המכון הישראלי
לדמוקרטיה

www.idi.org.il

29 יולי 2021

<u>חוות דעת בעניין תזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (מערכות צילום מיוחדות), התשפ"א-2021</u>

ד"ר תהילה שוורץ אלטשולר, עו"ד עמיר כהנא

1. רקע:

ב-28.1.2021 הגישו האגודה לזכויות האזרח ועמותת פרטיות ישראל, עתירה לבג"ץ נגד השימוש המשטרתי במערכת המעקב "עין הנץ" (בגץ 641/21 האגודה לזכויות האזרח נ' משטרת ישראל). מדובר במערכת אוטומטית לזיהוי לוחיות רישוי (LPR- license plate recognition) היוצרת מאגר מידע עצום, המתעד את תנועותיהם של אזרחים שנעים בכבישי הארץ ומשמש אותה לצרכים שונים. בעתירה נטען כי מדובר במנגנון מעקב קיצוני, שמאפשר למשטרה לקבל בלחיצת כפתור מידע פרטי רגיש על מיקומם של האזרחים הנוסעים בכבישי הארץ בזמן אמת וגם מאפשר לה לחזור אחורה כדי לשחזר את מקום הימצאו של אדם, את מסלול תנועתו, ולעיתים גם מגעים שקיים עם אחרים.

כל הפעולות האלה מתקיימות ללא הסדרה בחוק; ללא מערכת פיקוח שיפוטית וללא שקיפות ציבורית. הטענה של העותרים היתה כי מדובר בפגיעה בחירות ובפרטיות ולפיכך לפי חוק יסוד כבוד האדם וחירותו יש צורך בהסמכה מפורשת בחוק ובהסדר מידתי המתייחס לתכליות שאותן המשטרה מבקשת להשיג. מצב של "מסע דיג" בכבישים שבו כל נסיעה של כל אזרח מייצרת עבור המשטרה שביל פירורי לחם דיגיטלי לצרכים עתידיים לא מוגדרים איננו מידתי.

בדיון שהתקיים ב-27.5.2021 ציינה נשיאת בית המשפט העליון שאין מחלוקת שהמערכת פוגעת בפרטיות ולא ניתן להפעילה מכוח סמכויות כלליות של המשטרה. לכן, הורה בג"ץ למדינה לפרסם להערות הציבור בתוך 45 יום תזכיר חוק שמסדיר את מערכת המעקב "עין הנץ". בדיון גם הסתבר שלמרות שהמשנה ליועץ המשפטי לממשלה הורה לגבש חקיקה בנושא כבר בשנת 2015, הדבר לא התרחש בפועל.

ביום חמישי, ה- 8 ביולי, עלה תזכיר חוק לאתר התזכירים הממשלתי. אלא, שמדובר בתזכיר מפתיע ורחב הרבה יותר מזה שהתבקש על ידי בית המשפט העליון ונדון בעתירה ובתגובה לה. תזכיר החוק הוא רחב בשני הקשרים:

המכון הישראלי
לדמוקרטיה

א. תזכיר החוק עוסק במערכות הנקראות "מערכות צילום מיוחדות", שיש להן שני מאפיינים: מדובר במערכת שמאפשרת אגירה ועיבוד של נתונים או תמונות; ויש לה יכולת עיבוד שמאפשרת לזהות באופן חד ערכי אדם או חפץ בזמן אמת. למערכת יש יכולת איחזור מידע, עיבוד מידע או בדיקת התמונה וזיהוי האובייקט באמצעות יכולות הולכות ומשתכללות. כלומר, **התזכיר אינו עוסק רק במערכת של זיהוי לוחיות רישוי אלא במערכות של זיהוי פנים אנושיות.**

ב. התזכיר אינו עוסק רק בעניינים שנוגעים למה שניתן לחלץ מנתוני מיקום של רכב – שהם בעיקרם נתונים המיועדים לחיזוי וגילוי פשיעה, ואף לא במניעת פשעים הנוגעים לסיכון לחיים או לרכוש, אלא באכיפת הוראות המגבילות את חופש התנועה במרחב הציבורי, כגון איסורי כניסה וצווי הרחקה ממקומות ציבוריים. ליכולת אכיפה זו אפקט מצנן על מימוש חירויות יסוד נוספות, ובתוכן חופש הביטוי וחופש האסיפה. בפרט, עולה החשש מהכוונה לעשות שימוש במערכות זיהוי פנים על מנת לדבא הפגנות

הסדר בנוגע לזיהוי לוחיות רישוי דומה למעקב אחר נתוני תקשורת: מדובר בידיעה מי היה, היכן ומתי. השוואה בין תזכיר החוק, גם אם מתייחסים רק להקשר של זיהוי לוחיות רישוי, לבין מנגנוני הבקרה בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007, מלמדת על פער גדול בין שני החוקים. פוגעניותו של ההסדר בתזכיר הנוכחי מתבטאת בהיעדר מנגנוני פיקוח ראויים; בהצגת תכליות מבולבלת ורצופה סתירות פנימיות; בהיעדר הבחנה בין מניעת פשיעה, גילוי פשיעה ומחקר. יתרה מזאת, חוסר הבשלות של ההסדר בתזכיר הנוכחי מתבטאת בהותרת חלקים מהותיים לטיפול באמצעות תקנות ובכלל זה הוראות לגבי סוגים שונים של מערכות, דבר אשר עשוי לעקוף את הדיון הציבורי הנוקב בצורך בשימוש במערכות פוגעניות; אמות מידה לקביעת מקום להצבת המערכות; שמירת המידע ואבטחתו; תקופות שמירה ומחיקה; תנאים לגישה למידע או להעברתו; ויידוע הציבור בדבר הצבת המצלמות.

אולם, הדבר החמור ביותר בהצעת החוק הוא הניסיון לדחוף לתוכה **את השימוש במערכות זיהוי פנים לצרכי שיטור בהפגנות.** בין התכליות להצבה, הפעלה ושימוש במערכות צילום מיוחדות שבתזכיר מנויה אכיפת איסורי כניסה וצווי הרחקה ממקומות ציבוריים, בהם נעשה שימוש בין השאר בהקשרים של פעילות פוליטית. זהו העירוב הקיצוני ביותר בין כלים מעולם "האח הגדול" לבין דיכוי מחאה פוליטית והוא משקף זלזול בוטה בזכויות האדם הבסיסיות ביותר בדמוקרטיה - אוטונומיה, פרטיות, ביטוי וחירות, וגם חוסר מידתיות קיצוני בין האמצעי שנבחר כדי להשיג את התכלית של הסדר הציבורי לבין הפגיעה בזכויות אלה.

אנו קוראים **להסיר לאלתר מן התזכיר את ההתייחסות למערכות זיהוי פנים ולהתמקד במערכות זיהוי לוחיות רישוי וחפצים דוממים אחרים**. במקביל, אנו קוראים להקים וועדה ציבורית או בינמשרדית בהשתתפות מומחים, שתביא תוך זמן קצר המלצות בנוגע לשימוש במערכות זיהוי פנים. נשמח לעמוד לרשות כל וועדה כזאת.
נבהיר: הסרת ההתייחסות למערכות זיהוי פנים אין בה כדי להכשיר את ההסדר המוצע ביחס לזיהוי לוחיות רישוי, שגם הוא, כאמור, רחב ופוגעני יתר על המידה ונתייחס אליו בהמשך

המכון הישראלי
לדמוקרטיה

המסמך.

חוות הדעת שלנו תחולק לשלושה חלקים: החלק ראשון יעסוק במערכות זיהוי פנים. החלק השני יעסוק בהתנגדות במשפט המשווה לשימוש רחב במערכות כאלה על ידי רשויות אכיפת חוק. החלק השלישי יעסוק בהערות בנוגע לתזכיר החוק עצמו – אי הבהירות של תכליות השימוש במערכות; היעדר מנגנוני פיקוח ומנגנוני שקיפות מספקים; הותרת חלק מן העניינים המהותיים לקביעה בתקנות.

המכון הישראלי
לדמוקרטיה

חלק ראשון: מערכות זיהוי פנים

למערכות זיהוי פנים שלושה הקשרים בעייתיים:

1. איסוף המידע יוצר פגיעה בפרטיות אזרחים, מישטור התנהגותם ויצירת "אח גדול". זאת, ביחוד כשמדובר בדיכוי מחאה פוליטית.
2. עיבוד המידע יוצר חששות מפני יצירת "פרופילים עמוקים" על אזרחים ושימוש בו לצרכי מחקר יוצר חשש מפני זיהוי חוזר של המידע.
3. הטיות של מערכות זיהוי פנים יוצרות חששות לפגיעה בזכויות אזרחים ובהליך הוגן, בייחוד כשדובר בחיזוי פשיעה ובפגיעה בזכויות אזרח בזמן אמת.

א. מהו זיהוי פנים?

זיהוי פנים הוא תהליך אוטומטי של השוואת שתי תמונות שונות של פנים על מנת לבחון אם מדובר באותו אדם. אלגוריתמים לזיהוי פנים מבוססים על מערך כללים או תהליך לחישוב או ניתוח מאפיינים של פנים אנושיות. ניתן לראות שימוש הולך וגובר בטכנולוגיות זיהוי פנים לתכליות של ביקורת גבולות, ואף לאמצעי תשלום מקוונים, מערכות למיון ואינדוקס שלל התמונות המצולמות דרך קבע במכשירי הטלפון החכמים, או זיהוי פנים לתיוג חברים ברשת חברתית. מערכות לזיהוי פנים מאפשרות להשתמש בפרמטרים ביומטריים המאפיינים פנים של אדם מסוים בדרך לאימות זהותו, ואף כבסיס למפתח הצפנה, ובאמצעותם לנעול מכשירי קצה ולשלוט על גישה לחשבונות מקוונים. לכן, גם סוכנויות ביטחון ואכיפת חוק מגלות עניין גובר בטכנולוגיות לזיהוי פנים[1] במרחב מרושת במצלמות, מתוך ההנחה שביכולתן לזהות איומים ועבריינים[2] ואף להרתיע מביצוע פשיעה.[3]

---

[1] Clare Garvie, Alvaro M. Bedoya and Jonathan Frankle, *The Perpetual Line-Up - Unregulated police face-recognition in America*, Center on Privacy and Technology at Georgetown Law (2016); Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns* 105 VA. L. REV. ONLINE 57 (2019)

[2] Kyriakos N. Kotsoglou and Marion Oswald, *The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention* 2 FORENSIC SCIENCE INTERNATIONAL: SYNERGY 86-89 (2020)

[3] ר' לדוגמא הנחיית רשם מאגרי המידע מס' 4/2012, "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן", פס' 2.5-2.2.

עם זאת, מערכות זיהוי פנים אינן חסינות מפני מניפולציות. ניתן להערים על יכולותיהן ברמות שונות של תחכום – החל ממסכות פנים פשוטות וכלה בתמונות מזויפות יצירות מחשב (Deepfakes). מידה מספקת של תחכום (בהתאם לאלגוריתם בו נעשה שימוש).[4] מכאן, שמערכות זיהוי פנים אינן תרופת פלא טכנולוגית למיגור פשיעה, מאחר ש"השחקנים הרעים" מפתחים דרכים להתמודד איתה.

יחד עם ההתפתחות הטכנולוגית מגיעים גם אתגרים[5]. החשש הראשוני הוא מכך שפרטיות של כלל הציבור תיפגע, ואזרחים שומרי חוק עשויים להיות חשופים לסיכונים הנובעים בין השאר, מאבטחה לקויה וזליגה של מידע ביומטרי, ניצול לרעה של הגישה למידע על ידי בעלי סמכות, או טעיות בזיהוי. אבל מעבר לכך נשאלות שאלות כגון: באיזה שלב ניתן לומר שמערכת חכמה היא בעלת רמה מספקת של אחריותיות המאפשרת להסתמך על קביעותיה? מי יהיה הגוף שיבקר את המערכת? אחד המאפיינים של מערכות לומדות הוא שגם המתכננים שלהן אינם יכולים להסביר עד הסוף כיצד פועל תהליך הלמידה וכיצד הגיעו למסקנות שאליהן הגיעו. כיצד מממשים את עיקרון השקיפות השלטונית במצב כזה? כיצד תסביר המשטרה לציבור כיצד פועלות המערכות בהן היא משתמשת? האם מתקיים דיון ציבורי בהטיות של המערכות האלה? האם בידי חברי הכנסת מספיק ידע מקצועי ואוריינות דיגיטלית שיאפשרו להם לפקח על התהליכים הללו?

---

[4] Parmy Olson, *Faces are the next target for fraudsters*, THE WALL STREET JOURNAL (7.7.2021)

[5] United States Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, 11-13 GAO-20-522 (13.7.2020); Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology And The Growing Lack Of Privacy* 23 J. SCI. & TECH. 889 97-100 (2017); IAN BERLE, FACE RECOGNITION TECHNOLOGY: COMPULSORY VISIBILITY AND ITS IMPACT ON PRIVACY AND THE CONFIDENTIALITY OF PERSONAL IDENTIFIABLE IMAGES 17-23 (2020); איתן לשם "'משמר הלילה' של סין: מערכת לזיהוי פנים תמנע מקטינים לשחק כשאסור" **THEMARKER** (11.7.2021); לדוגמאות של שימוש בטכנולוגיית זיהוי פנים בישראל ר' מיכל רז-חיימוביץ, למנוע שימוש של קטינים: אפליקציות הקורקינטים של ווינד תפעיל טכנולוגיה לזיהוי פנים, **גלובס** (14.10.2020); ניצן שפיר, "'שימוש בטכנולוגיית זיהוי פנים לבעלי תו ירוק בהבימה ובאצטדיון בלומפילד פוגע בפרטיות ואינו חוקי'" **גלובס** (20.5.2021). יוער כי כותביו של דוח של מרכז המחקר והמידע של הכנסת מציינים כי למיטב ידיעתם, אין גורם בגופי המטה הממשלתיים אליו הם פנו שציין כי נציגיו עושים היום שימוש בטכנולוגיות זיהוי פנים. רועי גולדשמידט, "השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי", **מרכז המחקר והמידע של הכנסת**, בעמ' 8 (14.12.2020). עם זאת, הן הצבא והן המשטרה סרבו לבקשת חופש המידע של האגודה לזכויות אדם, שבקשה מידע בנוגע לשימוש שאלו עושות בטכנולוגיות זיהוי פנים. ר' "שימוש בטכנולוגיות לזיהוי פנים על ידי המשטרה והצבא", **אתר האגודה לזכויות האזרח בישראל** https://www.acri.org.il/post/ 523.

המכון הישראלי
לדמוקרטיה

ב. החששות מפני שימוש במערכות זיהוי פנים על ידי גורמי אכיפת חוק

השימוש במערכות זיהוי הפנים לצרכי שיטור הוא אחד הנושאים השנויים ביותר במחלוקת בעולם המערבי היום. אך לפני כחודש פרסם האיחוד האירופי טיוטת חקיקה המבקשת לאסור על פרקטיקה זו למעט בכללים מהודקים ביותר. בארצות הברית מדובר באחת המחלוקות החברתיות הבוערות לאחר הריגתו של פלויד ג'ורג' על ידי שוטר באמצע 2020. בערים רבות בעולם המערבי, הוגבל באופן משמעותי השימוש במערכות כאלה. חברות הטכנולוגיה הגדולות ובראשן אמזון, IBM ומייקרוסופט הודיעו שיפסיקו לייצר ולהשקיע בחברות המפתחות מערכות זיהוי פנים לתכליות שיטור, או שימנעו מלספקן לסוכנויות אכיפת החוק.[6] זאת, לאור ההבנה של ההטיות הרבות הנלוות לשימוש בהן. לפיכך, הניסיון להעביר מתחת לרדאר וללא שום עבודת הכנה מקיפה ומדוקדקת חקיקה העוסקת בזיהוי פנים לצרכי שיטור, במסווה של טיפול בעיקוב אחר לוחות רישוי של כלי רכב, הוא ניסיון שיש להתנגד אליו.

נדגיש: אין מדובר רק בשאלה אלו אמצעי אבטחה יש לנקוט או ביצד לעבד את המידע או לשמור עליו, אלא **שעצם הצילום**, בהינתן היכולות הטכנולוגיות הקיימות, מהווה פגיעה בפרטיות שלא נלקחה בחשבון בעשור האחרון, עת הותקנו מצלמות בכל קרן זווית. נוכח היכולת להסיק מהנתונים המצטברים הללו מידע על ההיבטים הפרטיים ביותר של חיינו, אחד המאפיינים של פרטיות בעידן הדיגיטלי הינו הצורך להגן על הפרט מפני איסוף מידע על אודותיו במרחב הציבורי – בין אם עסקינן בניטור הפעילות המקוונות שלו ובין אם עסקינן ברישות הרחובות במערכות צילום נבונות הבולשות אחריו. ממש כמו רעות חברתיות אחרות, מעישון ועד שיח לא מוגבל ברשתות החברתיות, מחלחלת בשנתיים האחרונות ההבנה בעולם המערבי שלצילום המונים ישנן השלכות בעייתיות שראוי להתמודד איתן.

יתרה מזאת, השימוש במצלמות ופיענוח תכני תמונה ווידיאו לצורך זיהוי פנים איננו מוגבל רק לשימושים משטרתיים ורק למערכות שיוצרו לטובת זיהוי פנים. השימוש המדובר עולה – ויעלה בשנים הקרובות - בהקשרים רחבים של מערכות המצלמות שבהן רושתו ערי ישראל וכבישיה בעשור האחרון.

להלן, ננסה לתמצת את החששות מפני שימושים במערכות נבונות לזיהוי פנים:

1. **אפקט מצנן:** ישנו חשש מפני **האפקט המצנן** שבהצבת מערך של מצלמות חכמות במרחב הציבורי, המנטרות תדיר את הפעילות האנושית שבו. אפשר שלמערכות אלו יהיו

---

[6] Alex Hern, *IBM quits facial-recognition market over police racial-profiling concerns*, THE GUARDIAN (9.6.2020) available on https://www.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns; Jay Greene, *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*, THE WASHINGTON POST (11.6.2020) available on https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/; Jeffrey Dastin, *Amazon extends moratorium on police use of facial recognition software*, REUTERS (18.5.2021) available on https://www.reuters.com/technology/exclusive-/amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18

יכולות זיהוי אוטומטיות של פעילות חריגה או חשודה.[7] אפשר שיהיה ביכולתן לזהות איומים ביטחוניים או כוונות עברייניות בהתבסס על שפת גוף או הבעות פנים, לעתים בלתי מודעות.[8] כבר עתה, בהעדר יכולות אלו, שרמת הדיוק והביול שלהן עשויה להיות בלתי מספקת,[9] למבט בוחן-הכל של עדשת המצלמה במרחב הציבורי ישנו אפקט ממשטר וממתן המונע מהאזרחים במרחב להתנהג באופן חופשי מתוך חשש שהם נתונים תחת מעקב,[10] ובין השאר לממש את הזכויות הפוליטיות שלהם מחשש שיתויגו על ידי המכונה, והדבר יפגע בהם בעתיד. בשילוב עם הפוטנציאל לחיזוי פשיעה על בסיס ביומטרי וזיהוי אלגוריתמי של חריגות, האפקט הממשטר מתעצם, עד שבתרחישי הקצה שלו הוא נוטל את האנושיות מהמרחב הציבורי.[11]

2. יכולות ניתוח חדשות וקטגוריות חדשות של מידע שניתן לאסוף:

פריסה רחבת היקף של מערכות זיהוי פנים תרחיב את השימוש ב**קטגוריות חדשות של מידע**. מערכות נבונות המנתחות נתונים חזותיים עשויות לייצר מידע אוטומטי אודות רגשות של פרטים הנקלטים בעדשותיהן,[12] או על מאפייני התנהגותם במרחב. מערכות אלו עשויות לנתח את טיב האינטראקציה החברתית של יחידים וקבוצות הנקלטים בעדשת המצלמה ואת אופי הקשרים ביניהם. אלה אינן יכולות שהיו קיימות בעבר ושילובן במסגרת פרקטיקות של פיקוח ומשטור המרחב הציבורי מאיים **להעמיק את אופי הפרופילים האישיותיים** שניתן לבנות באופן אוטומטי וחסר אבחנה לאזרחים החולפים בעל כורחם על פני עדשת המצלמה, ובהתאמה את מידת הפגיעה בפרטיות המתלווה לכך. יש לתת את הדעת לכך שמערכות זיהוי

---

[7] Patrick Tucker, *Here Come AI-Enabled Cameras Meant to Sense Crime Before it Occurs* , DEFENSE ONE (24.4.2019) available in https://www.defenseone.com/technology/2019/04/ai-enabled-cameras-detect-crime-it-occurs-will-soon-invade-physical-world/156502

[8] לדוגמא ר' Louise Marie Jupe & David Adam Keatley, *Airport artificial intelligence can detect deception: or am i lying?* 33 SECURITY JOURNAL 622-635 (2020)

[9] ר' למשל James Vincent, *AI 'Emotion Recognition' Can't be Trusted*, THE VERGE (25.7.2019) available on https://www.theverge.com/2019/7/25/8929793/emotion-recognition-analysis-ai-machine-learning-facial-expression-review

[10] ר' בהקשר זה פס' 17-20 לפסק דינו של השופט הרמלין בעניין מקומיים (ת"א), תיק חנייה 72118789 **מדינת ישראל נ' מזרחי** (פורסם בנבו, 7.10.2018).

[11] לפי עדויות של בני המיעוט האויגורי ששהו במחנות 'חינוך מחדש' בסין, נדרש מהם שלא להביע רגשות כלל לאורך שהותם במתקנים אלה. הוראה זו נאכפה – כך נאמר להם - באמצעות רישות המחנות במערך של מצלמות חכמות, וסנסורים שמסוגלים לעקוב השוהים בהם. בין אם יכולות טכניות אלו אכן פותחו ונפרסו על ידי המשטר הסיני, עצם התחושה שהם מצויים תחת עינם האלקטרונית הבולשת של אמצעים כאלו נראה שהתיש ורוקן את רוחם של הכלואים. ר' למשל GEOFFREY CAIN, THE PERFECT POLICE STATE, Chap. 13-14 (2021)

[12] לאחרונה, לדוגמא, דווח כי חברת המצלמות 'קאנון' התקינה במשרדיה שבבייג'ינג מערכת זיהוי פנים המתירה כניסה רק לעובדים 'שמחים'. James Vincent, *Canon put AI cameras in its Chinese offices that only let smiling workers inside*, THE VERGE (17.6.2021) The Verge available on https://www.theverge.com/2021/6/17/22538160/ai-camera-smile-recognition-office-workers-china-canon

פנים לא מוגבלות לזיהוי פנים בלבד – מערכות צילום נבונות עשויות, בהתבסס על נתונים ויזואלים, להפיק מידע ביחס למאפייני תנועה, מגדר, שיוך אתני,[13] או רגשות. הן עשויות לנתח מידע בקונטקסט רחב יותר – לזהות מאפייני תנועה של התקהלויות חשודות, או של אירועים אלימים.

3. **טעויות ושגיאות:** במסגרת קטגוריות חדשות אלו של מידע, וגם במסגרת קטגוריות ישנות שעד כה טרם הופקו בהסתמך על נתוני חוזי, כגון זהות אתנית, השקפה דתית, עמדות פוליטיות,[14] נטייה מינית,[15] מבנה אישיות, או נטייה לאלימות, יש סיכון מוגבר להפקת נתונים החשופים ל**טעויות והעדר סימובין מדעי.**[16] הפערים בין היכולות המיוחסות למערכות אלו על ידי המפתחים שלהן לבין רמת האמינות האפקטיבית שלהן עשויים להיות בלתי מבוטלים. שיוך חד חד ערכי של רגשות אנושיים או של התנהגויות חברתיות מורכבות ורבות מימדים – מדדים ביומטריים חדשים, שהגדרתם עמומה - לאנשים הנקלטים בעדשת המצלמה בהתבסס על מערכות לומדות **שלא נבדקו ביאות**, עשוי להביא לטעויות מרחיקות לכת בזיהוי ובדיוק.[17]

איכותם של אלגוריתמים כרוכה באופיו של בסיס הנתונים עליו הם מתאמנים – ככל שאלגוריתמים אלו מפותחים באמצעות למידת מכונה, מאגר התמונות ששימש לפיתוחם יקבע אם הם יצליחו לזהות פנים של בני אדם ממוצא אסיאתי ברמת דיוק טובה יותר מפנים מערביות, למשל.[18] לאחרונה ציין הממונה על היישומים הביומטריים כי ישנם קשיים

---

[13] אושרית גן-אל, "ניו יורק טיימס: רשויות בסין משתמשות בזיהוי פנים לניטור מיעוטים" **גלובס** (15.4.2019); עודד ירון "'לא יכול להסביר את זה' בביר בוואווי התפטר בעקבות פיתוח 'אזעקת אויגורים' **הארץ** (16.12.2020).

[14] Michal Kosinski, *Facial recognition technology can expose political orientation from naturalistic facial images*, NATURE (11.1.2021) available on https://www.nature.com/articles/s41598-020-79310-1

[15] Sam Levin, *New AI can guess whether you're gay or straight from a photograph*, THE GUARDIAN (7.9.2017) available on https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

[16] ר' לדוגמא Khalida Sarwari, *You think you can read facial expressions? you're wrong*, NEWS@NORTHEASTERN (19.7.2019)

[17] ר' למשל David Leslie, Understanding bias in facial recognition technologies: an explainer, The Alan Turing Institute (2020); Will Knight "*Job Screeing Serice Halts Facial Analysis of Applicants*" WIRED (12.1.2021)

[18] כך למשל, מחקר מצא שרמת הדיוק של אלגוריתמים לזיהוי פנים שפותחו במדינות מזרח אסיאתיות לזיהוי תווי פנים אסיאתיים היא רבה יותר מרמת הדיוק לזיהוי תווי פנים מערביים, ולהפך. P. Jonathon Phillips,

בהרכשת תמונות פנים של תושבים בעלי גון עור כהה – ובהתאמה, העדר כיול ראוי למערכות ביומטריות עשוי להשפיע על הדיוק ומרווח הטעות שבשימוש בהן.[19]

4. **אפליה:** אלגוריתמים לזיהוי פנים עשויים להתבסס על מאגר נתונים חלקי או מוטה, ובהתאמה לסבול מהטיות בזיהוי. כאשר מאגר הנתונים ממנו לומדת המכונה אינו מהווה מדגם מייצג של כלל האוכלוסייה, המכונה תיטה לטעויות במקרים של ייצוג חסר (כך למשל, מצלמות שאומנו לזהות פנים בהתבסס על מאגר תמונות של אנשים לבנים, זיהו תווי פנים אסיאתיים כ'ממצמצים')[20] או ייצוג יתר.[21] נוכח מגוון היישומים הפוטנציאליים לטכנולוגיה זו, להטיות אלו, גם אם נעשו בתום לב, יש השלכות הרות גורל וביכולתן להנציח פערים ואפליה כלפי מיעוטים.[22] למשל, אלגוריתם זיהוי פנים שאומן על מאגר תמונות של אנשים ממוצע מערבי ומשמש לזיהוי חשודים בפשע, עשוי לדייק פחות ביחס לזיהוי של חשודים עם רקע אתני אחר. מערכות לזיהוי פנים שתהליך האימון שלהן היה בעיקר על פנים של אנשים בהירי עור, מבצעות טעויות כשהן נדרשות לזהות פנים של כהי עור.

5. **אביפת יתר:** מערכות זיהוי פנים ומערכות צילום נבונות עשויות **לעודד אביפת יתר,** מאחר שרישות המרחב במצלמות חכמות מאפשר ניטור מתמיד של ספקטרום שלם של עבירות באמצעות זיהוין בזמן אמת וזיהוי העבריין. פלוני השליך פסולת שלא בפח האשפה? פלונית החנתה את רכבה כחצי דקה מעבר לזמן המותר? פלוני חצה מעבר חצייה שומם באור אדום בשעה מוקדמת לפנות בוקר? הפיתוי שבקלות שבאכיפה האוטומטית של עבירות כאלו עשוי להיות רב.

Fang Jiang, Abhijit Narvekar, Julianne Ayyad, and Alice J. O'Toole, *An Other-Race Effect for Face Recognition Algorithms*, National Institute of Standards and Technology (2010)

[19] דו"ח הממונה על היישומים הביומטריים מס' 11 (21.6.2021), בעמ' 6.

[20] Odelia Lee, "*Camera Misses the Mark on Racial Sensitivity*" GIZMODO (15.5.2009) available at https://gizmodo.com/camera-misses-the-mark-on-racial-sensitivity-5256650

[21] ניתן לשער שאלגוריתמים לזיהוי פנים של 'עבריינים' שיאומנו באמצעות מאגרי תמונות של עבריינים בארצות הברית, ייטו לזהות אנשים כהי עור כעבריינים, בשל ייצוג היתר של מגזר זה במאגר. למען הסר ספק, לא ידוע לנו על מערכות לזיהוי 'עבריינים' על סמך מראם בלבד, אך הנסיון בארצות הברית במודלים לחיזוי פשיעה, הערכת סיכון ורצדיזיביזם מראה כי על פי רוב מודלים לוקים בהטיות. ר' בהקשר זה Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CA. L. REV. 671 687 (2016)

[22] Fabio Bacchini and Ludovica Lorusso,*"Race, Again: How Face Recognition Technology Reinforces Racial Discrimination."* 17 Journal of Information, Communication & Ethics in Society 321-335 (2019); Evan Selinger and Brenda Leong, *The Ethics of Facial Recognition Technology* in THE OXFORD GANDBOOK OF DIGITAL ETHICS (CARISSA VELIZ, ED., forthcoming 2021)

6. **שימוש לרעה:** חשש נוסף, הרלוונטי ביחס למערכות מעקב באשר הן, הוא מ**שימוש לרעה על ידי בעלי סמכות**. כך למשל, לאחרונה דווח כי חברת פייסבוק פיטרה עשרות מהנדסים שניצלו את גישתם למידע על מנת לעקוב אחר נשים.[23] בסמוך להקמת ה'כלי' של השב"כ היו בין עובדי הארגון שהתפתו לעשות בו שימוש חורג.[24] גם במשטרת ישראל היו מקרים של ניצול לרעה של גישה למידע על ידי בעלי סמכות, תוך הפרת החוק.[25] פוטנציאל דומה לניצול לרעה יש גם למערך מצלמות חכמות לזיהוי פנים או לוחיות רישוי.

7. **חשש מדליפת מידע:** הקמת מאגרי מידע רחבי היקף המתעדים נתוני זיהוי פנים מייצר סיכונים הנוגעים גם ל**דלף מידע**, כדברי השופטת ברק-ארז, "מידע – דרכו לדלוף, גם כאשר נעשים מרב המאמצים שהדבר לא ייעשה. אם כן, הסכנה של דליפת מידע מבטאת ממד נוסף של פגיעה בזכות לפרטיות."[26] אין להשוות בין חשש מדליפה של נתוני לוחיות רישוי, מספרי ברטיס אשראי או אפילו נתוני מיקום – לבין חשש מדליפה של נתונים ביומטריים כגון תמונות פנים.

---

[23] Theo Wayt, Facebook reportedly fired 52 employees who were caught spying on users, New York Post (13.7.2021)

[24] רונן ברגמן ועידו שברצטוך, "'הכלי', מאגר המידע הסודי של השב"כ, אוסף נתונים על כל אזרחי מדינת ישראל ויודע: איפה הייתם, עם מי דיברתם, ומתי עשיתם את זה" **ידיעות אחרונות** (25.3.2020).

[25] ר' שי לוי "מאגר ביומטרי? השוטרים יכולים להפיץ מידע אישי על כל אחד מאיתנו" **מאקו** 21.10.13; ת"פ (בש) 16908-06-11 **מדינת ישראל – המחלקה לחקירות שוטרים נ' רצאבי** (פורסם בנבו, 16.10.2013); ת"פ (חי') 18599-03-17 **מדינת ישראל נ' פארס**, 3 (פורסם בנבו, 10.12.2017); ת"פ (י-ם) 44139-07-15 **מדינת ישראל נ' מלכה** (פורסם בנבו, 20.9.2015); לדוגמאות הנוגעות למאגרי מידע של רשויות אחרות ראו ע"פ (חי') 616/05 **מדינת ישראל נ' שווגר** (פורסם בנבו, 25.6.2006); ת"פ (ת"א) 2928-06 **מדינת ישראל פרקליטות מחוז ת"א (פלילי) נ' משעול** (פורסם בנבו, 10.05.2012); ת"פ (מרכז) 36669-07-14 **מדינת ישראל נ' גרנביץ** (פורסם בנבו, 5.11.2018).

[26] בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת**, פס' 14 לפסק הדין של השופטת ברק-ארז (אר"ש 1.3.2021)

חלק שני: חקיקה משווה לגבי שימוש בטכנולוגיות זיהוי פנים בשירות רשויות אכיפת חוק

כאמור, בשל האופנים שבהם השימושים במערכות זיהוי פנים עשוי לפגוע בזכויות אדם,[27] מתנהל בשנים האחרונות ויכוח ער במדינות המערב בנוגע לשימושים אלה על ידי רשויות אכיפת חוק וחוקיותם. בינה מלאכותית מתחילה לשמש מנוע למערכות חיזוי פשיעה ומערכות פיקוח חכמות ורשויות אכיפת חוק מבקשות להטמיע אותן כחלק מהפעילות השגרתית. מערכות אלה זקוקות לאיסוף מידע – מצולם, מוקלט ומוסרט – ומסוגלות להעניק ניתוח חכם אשר יצליב את כל תכונותיו ופעילויותיו של אזרח, ואז קיימת כמובן האפשרות שאותו אדם יסומן כראוי לחקירה מעמיקה יותר, יילקח למעצר או יינקטו נגדו אמצעים אחרים. אין מדובר רק בפשיעה "רגילה" של גניבת אופניים: המערכות יובלו לסמן את מי לעצור לבדיקה מיוחדת; וגם את מי לעכב בדרכו להפגנה ומתי אדם עלול להוות איום לא רק לסובבים אותו אלא לאותו מונח אמורפי בשם "שלום הציבור" או "יציבות הממשל."

א. ארצות הברית:

בדו"ח שפורסם בשנת 2019 בעניין יכולות וידיאו אנליטיקס על ידי האגודה לזכויות האזרח בארצות הברית[28] נטען כי יש לצמצם באופן משמעותי את השימוש במצלמות לניטור המוני בגלל היכולות החדשות. בעיר סן פרנסיסקו נאסר במאי 2019 על שימוש במצלמות רחוב בגלל החשש לזיהוי פנים[29] וכך גם בסאמרוויל, מסצ'וסטס ובאוקלהומה סיטי. הדיון לגבי העניין בערים אחרות בארצות הברית נמצא בעיצומו. הרשות הפדרלית לסחר (FTC) אותתה על עניין רגולטורי בסוגיה זו ופרסמה המלצות לשימוש הוגן בבינה מלאכותית.[30] המלצות אלו מצביעות על מספר מקורות סטטוטוריים שמהם הרשות הפדרלית יכולה לינוק את סמכותה

---

[27] ר' לדוגמא את הסקירה של ארגון INCLO: International Network of Civil Liberties Organizations, In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World (2021)

[28] Jay Stanley, The Dawn of Robot Surveillance AI, Video Analytics, and Privacy (2019) available on https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf

[29] Shirin Ghaffary, *San Francisco's facial recognition technology ban, explained*, Vox (14.5.2019) available on https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained

[30] Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, Federal Trade Commission Business Blog (19.4.2021) available on https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

לאסור על הטיות בבינה מלאכותית, ועל פרקטיקות נאותות (שקיפות, הוגנות, הסברתיות, חסינות ואחריותיות).[31]

ב. בריטניה

נציבת הפרטיות הבריטית פרסמה בשנת 2020 הודעה לפיה בכוונתה לחקור את השימוש במצלמות רחוב במתחם קינגס קרוס המפורסם, המאפשרות זיהוי פנים.[32] וזאת על אף שבבריטניה, פורסמה כבר בשנת 2017 אסטרטגיה לאומית למצלמות מעקב, שמטרתה להבטיח שהשימוש במצלמות מעקב משקף איזון נכון וראוי בין הצורך של החברה הבריטית בביטחון לבין הזכות לפרטיות[33] ומופעל רק לשם הגשמת מטרה לגיטימית, כאשר הוא נחוץ להשגת צורך דחוף, מידתי, ושקוף.[34] כן נקבע כי הוא חייב לעמוד במחויבויות הבינלאומיות הרלוונטיות, שבראשן תקנות הגנת המידע של האיחוד האירופי (GDPR). בבריטניה ובקנדה העניין נדון[35] ואף הוגשו תביעות הנוגעות לחוקיות השימוש בפרקטיקה זאת.

ג. האיחוד האירופי:

ביולי 2019, אימצה מועצת הגנת המידע האירופית (The European Data Protection Board, להלן: "EDPB") הנחיות לעניין עיבוד מידע אישי ממצלמות וידיאו (הכוונה היא למידע

---

[31] ר' גם Andrew Smith, *Using Artificial Intelligence and Algorithms*, FEDERAL TADE COMMISSION BUSINESS BLOG (8.4.2021) available on https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms

[32] Kevin Rawlinson, *ICO opens investigation into use of facial recognition in King's Cross*, THE GUARDIAN (15.8.2019) available on https://www.theguardian.com/technology/2019/aug/15/ico-opens-investigation-into-use-of-facial-recognition-in-kings-cross

[33] *Surveillance* Camera Commissioner, A National Surveillance Camera Strategy for England and Wales (March 2017)

[34] כן ר' לאחרונה Information Commissioner, *The use of live facial recognition technology in public places* (18.6.2021)

[35] Joe Devansan, *EU privacy debate rages regarding facial recognition firm Clearview AI*, TECHHQ (1.6.2021) available on https://techhq.com/2021/06/eu-privacy-debate-rages-regarding-facial-recognition-firm-clearview-ai/; *Legality of collecting faces online challenged*, BBC NEWS (27.5.2021) available on https://www.bbc.com/news/technology-57268121; Amir Ali, *RCMP violated Canadian privacy act with facial recognition technology*, DHNEWS (10.6.2021) available on https://dailyhive.com/vancouver/rcmp-violated-canadian-privacy-act-with-facial-recognition-technology

העלול להביא לזיהויו של אדם, ובכלל זה פניו או מספר הרכב שבו הוא נוסע), שמהן עולה כי היא מניחה שצילומים כאלה הם פגיעה בפרטיות ולכן לפני התקנת מערכת מצלמות ומעקב יש לבחון באופן זהיר האם האמצעי של מעקב הווידאו הוא האמצעי המתאים, הראוי והנחוץ להשגת המטרה, שצריכה להיות ברורה ספציפית ומדוייקת ("שמירה על ביטחונכם", כך נכתב בהנחיות, אינם הגדרת מטרה העומדת בדרישות אלו).[36] נקודת המוצא של ההנחיות היא שיש לבחון קיומם של אמצעים אחרים, שפגיעתם בפרטיות פחותה, להשגת מטרת המעקב. תפיסה של מעקב באמצעות וידאו כברירת מחדל מסכנת את הנורמות החברתיות הקיימות ועלול להוביל לאיון הזכות לפרטיות. לפי ההנחיות יש להגדיר ולציין במפורש ובכתב את מטרת המעקב המצולם ביחס לכל מצלמה שנעשה בה שימוש, בהתאם לסעיף 5(1)-(2) ל-GDPR. תיאור המטרה צריך להיות **מדוייק, ברור, שקוף וספציפי**. כך, למשל, ההנחיות מבהירות **שקביעה שהמטרה היא "ביטחון" או "ביטחונו של המצולם" אינה עומדת בתנאי ה-GDPR.**

על מנת לבצע מעקב וידאו יש להיכנס לגדר אחד הבסיסים הלגיטימיים הקבועים בסעיף 6. לענייננו רלבנטי סעיף 6(1)(e) ל-GDPR באשר המעקב הוא אינטרס ציבורי או מימוש סמכות רישמית. לפני התקנת מערכת מעקב מצולם יש לבחון באופן זהיר האם זהו האמצעי המתאים, הראוי והנחוץ להשגת המטרה ולא סביר להגשים את המטרה באמצעות אמצעי אחר שפגיעתו בזכויות ובחירויות של נושא המידע פחותה. בנוסף יש לפעול לפי עיקרון מיזעור המידע (data minimization) על מנת להקטין את הסיכון שיאסוף באמצעות הסרטון מידע שיביא לגילוי מידע רגיש. לצד מבחן הנחיצות, יש להבטיח שעיבוד המידע האישי עומד בשאר דרישות ה-GDPR, לרבות המגבלה על איחסון ודרישת המידתיות.

מידע ביומטרי לפי סעיף 9 כולל מידע שמעובד באופן ספציפי במטרה להביא לזיהויו של אדם.[37] המבחן הוא מבחן משולש: (1) טיב המידע: מידע הקשור למאפיינים פיזיים, פסיכולוגיים או התנהגותיים של אדם. (2) הדרך והאמצעים לעיבוד המידע: המידע הוא תוצר של עיבוד טכנולוגי ספציפי. (3) מטרת העיבוד: זיהוי ייחודי של אדם. לפי ההנחיות נקודת המוצא היא ששימוש במידע ביומטרי, במיוחד במערכות לזיהוי פנים (facial recognition) מגביר את הסיכון לזכויותיו של נושא המידע. משום כך, בעת הפעלת מעקב הכולל מערכות לזיהוי פנים על בעל שליטה במידע לפעול בהתאם לעיקרון החוקיות, הנחיצות, המידתיות ומיזעור המידע הקבועים ב-GDPR. בראש ובראשונה על בעל שליטה במידע לבחון האם ניתן להשיג את אותה מטרה לגיטימית של עיבוד המידע באמצעות שימוש באמצעים שפגיעתם בפרטיות פחותה.

על בעל שליטה במידע לבחון כל העת האם מעקב הווידאו שהתקין עלול להביא לגילוי של מידע רגיש. למשל, אם מסרטון מעקב הווידאו ניתן להסיק על דעותיו הפוליטיות של אדם כיוון שהסרטון מראה שאותו אדם השתתף באירוע פוליטי מסוים או הפגין או שבת. במקרה

---

[36] EDPB Plenary meeting, 09-10 July 2019, Guidelines 3/2019 on processing of personal data through video devices (version for public consultation) Adopted on 10 July 2019

[37] שם, בעמ' 15.

שהסרטון עלול להוביל לגילוי מידע רגיש על בעל השליטה במידע למצוא בסיס לגיטימי לפי סעיף 9 ל-GDPR לעיבוד המידע האישי וכן יהיה עליו לציית לדרישות אבטחת מידע מחמירות יותר. בנוסף, חלות שאר הזכויות של ה GDPR ובכללן זכות העיון, זכות המחיקה: לנושא המידע הזכות לדרוש את מחיקת המידע בהתאם לסעיף 17 ל-GDPR; הזכות להתנגד כאשר עיבוד המידע מבוסס על סעיף 6(1) ל-GDPR – עיבוד למטרה שיש בה אינטרס ציבורי.

שמירת סרטוני הוידאו צריכה להיעשות רק אם היא נחוצה ומידתית להגשמת המטרה ולתקופה הנחוצה להגשמת מטרת עיבוד המידע והמידע שנשמר צריך לעמוד בדרישת מיזעור המידע. כך למשל כאשר מעקב הוידאו הוא למטרה של גילוי ונדליזם פרק הזמן הראוי לשמירת המידע לא יעלה על מספר ימים כאשר עדיף שמחיקת המידע בתום התקופה הסבירה תעשה באופן אוטומטי. כבל שהסרטונים ישמרו לפרק זמן ארוך יותר (מעל 3 ימים) ההצדקות לגיטימיות מטרת העיבוד ונחיצות השמירה צריכות להיות חזקות יותר.

לבסוף, על בעל שליטה במידע להטמיע אמצעי הגנה ואבטחת מידע טכניים וארגוניים לכל אורך שלבי השימוש (כלומר איחסון, העברה ועיבוד) ועל האמצעים להיות מידתיים ביחס לסכנה הנשקפת לזכויות נושא המידע עקב הרס, אובדן, שינוי, גילוי, עיון או שימוש בלתי מורשה או מקרי.

לאור כל האמור אין זה מפתיע כי **תקנות הבינה המלאכותית האירופיות המוצעות** שפורסמו במאי 2021 מקדישות תשומת לב מיוחדת לטכנולוגיות אלה ומציעות לאסור **על זיהוי ביומטרי לצרכי אכיפת חוק, אלא בהגבלות מחמירות ביותר**[38]**.** במסגרת גישת ניהול הסיכונים של תקנות הבינה המלאכותית האירופיות המוצעות, מערכות נבונות מחולקות לארבע רמות סיכון: מערכות אסורות, מערכות בסיכון גבוה, מערכות שעליהן חלות חובות שקיפות מיוחדות, ומערכות בסיכון נמוך. במסגרת המערכות הבעייתיות ביותר – כלומר המערכות האסורות, תקנות הבינה המלאכותית האירופיות מציעות לאסור על השימוש והפריסה של מערכות בינה מלאכותית שנתפסות כמסוכנות באופן קיצוני ושאינן עולות בקנה אחד עם ערכי היסוד האירופיים.[39] אחד האיסורים הבולטים הוא על השימוש במערכות זיהוי ביומטריות בזמן אמת במרחבים ציבוריים לתכליות של אכיפת חוק, אלא אם הדבר נחוץ לחיפוש ממוקד

---

[38] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 (21.4.2021) available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulationeuropean-approach-artificial-intelligence . (להלן: "הצעת תקנות הבינה המלאכותית האירופיות"). בס' 3(33) לתקנות מגדיר מידע ביומטרי כמידע שמקורו מתהליכי עיבוד טכניים הנוגעים, בין השאר, לזהותו הייחודית של אדם, לדוגמת דמותו. ס' 5(2) לתקנות אוסר על שימוש במערכות זיהוי ביומטריות (למעט חריגים מסוימים) וס' 52(2)מטיל על מערכות אלו חובות שקיפות ייחודיות. כמו כן, מערכות זיהוי ביומטריות מוגדרות כמערכות בסיכון גבוה (ס' 1 בתוספת III לתקנות).

[39] ר' ס' 5(1) להצעת תקנות הבינה המלאכותית האירופיות.

אחר קורבנות פוטנציאלים מסוימים של פשע (כגון, ילדים חטופים), מניעת איום ספציפי, מוגדר, משמעותי ומיידי על חייהם או שלומם של אנשים, או מתקפת טרור וכן לתכליות של איתור, זיהוי ותביעה של עבריינים בעבירות חמורות.[40] התקנות מוסיפות סייגים על השימוש במערכות זיהוי ביומטריות במקרים חריגים אלה. יש להביא בחשבון את עוצמת האיום הפוטנציאלי המצדיק את השימוש בהן, כמו גם את ההשלכות הרוחב החברתיות שבהפעלתן. כמו כן, יש להבטיח כי כל הסתייעות פרטנית במערכת זיהוי ביומטרית כאמור יהיה בכפוף לצו שניתן על ידי גורם שיפוטי או גוף מנהלי עצמאי.[41]

העולה מן האמור לעיל הוא כי ההסדר המוצע בתזכיר הוא מתירני ורחב ביחס להסדרים קיימים או כאלה הנמצאים על שולחנם של מקבלי החלטות במדינות המערב. הוא יוצר פגיעה רחבה ועמוקה בזכויות אזרחי מדינת ישראל ביחס לעמיתיהם במדינות המתוקנות. יתרה מזאת, הוא עלול להפוך את מדינת ישראל לחצר האחורית של ניסויים בשימושים במערכות אלה, המתבצעים כבר כמה שנים כאמצעי שיטור בשטחים.[42]

---

[40] ס' 5(1)(d) להצעת תקנות הבינה המלאכותית האירופיות.

[41] ס' 5(2) להצעת תקנות הבינה המלאכותית האירופיות,. על פיקוח אקס אנטה לתכליות של מעקב מקוון, ר' עמיר כהנא ויובל שני, **פיקוח על מעקב מקוון בישראל** 46-44 (2020)

[42] אמיתי זיו, "חשיפה: הסטארט-אפ הישראלי המסקרן שפועל בחשאי בשטחים ועוקב אחרי פלסטינים" **TheMarker** (14.7.2019) https://www.themarker.com/technation/.premium-1.7497279 (14.7.2019)

חלק שלישי: הערות לתזכיר החוק

א. מהות הפגיעה בפרטיות

אין חולק ששימוש במצלמות המסוגלות ליצור זיהוי חד ערכי של אדם ולפיכך לגלות אדם מסויים במקום מסויים ובזמן מסויים מהווה פגיעה של ממש בזכות החוקתית לפרטיות. זאת, בייחוד כשניתן יהיה להצליב מגעים עם אנשים אחרים וסוגי מידע אחרים עם הזיהוי הזה. ואולם, ראוי להתייחס לטענה העולה מתזכיר החוק ועלתה גם בתגובת המדינה לבג"ץ. טענה זו היא שהצילום ברשות הרבים איננו בעייתי ואיננו מהווה פגיעה בפרטיות. לכן, סעיף 10ד (א) קובע כי "מערכת צילום מיוחדת תוצב, תכוון ותופעל כך שיצולם המרחב הציבורי בלבד ולא רשות היחיד", בעוד שביחס למערכת צילום מיוחדת שהיא מצלמה ניידת יחול האמור "ככל הניתן". לאור ההתפתחויות הטכנולוגיות של השנים האחרונות בתחום זיהוי פנים ועיבוד ווידיאו באמצעים מבוססי למידת מכונה, הגישה המקובלת בעולם בדבר הזכות לפרטיות בעידן הדיגיטלית רואה את עצם הצילום ההמוני במרחב ציבורי כפוגע בזכות לפרטיות. זאת, משום שהוא משנה באופן מהותי את התוצרים שניתן להפיק ממצלמות מעקב המוני ברשות הרבים. כבר היום מצלמות זיהוי פנים אינן משמשות רק לצורך זיהוי אדם מסויים במקום מסוים ובזמן מסוים, אלא לצורך מימוש היכולת לעבד פרופיל התנהגותי-פסיכולוגי על אודות אדם בהסתמך על הצילומים, ולחלץ מידע על ההיבטים הפרטיים ביותר של חייו.

לכן, אנו סבורים שהתפיסה לגבי האיזון בין היתרונות והחסרונות בצילום המוני ברשות הרבים, צריכה להשתנות.[43] חוק הגנת הפרטיות איננו עוסק באופן מפורש בצילום ברשות הרבים, בגלל העובדה שהוראותיו נוסחו בעידן טכנולוגי מוקדם, לפני המהפכה הדיגיטלית. חוות הדעת של הרשות להגנת הפרטיות בעניין הצבת מצלמות ברשות הרבים משנת 2012, המתמקדת בעיקר בשמירה על מאגר המידע שנוצר ופחות באמירה בהירה שלפיה עצם הצילום הוא פגיעה בפרטיות,[44] גם היא לתפיסתנו, מיושנת ויש לעדכן אותה בגלל השינויים הטכנולוגיים. כך או כך, הזכות לפרטיות כמשמעה בחוק יסוד כבוד האדם וחירותו חלה גם כאשר מדובר בשימוש באמצעים אלה במרחב הציבורי.

בדונו בחוק הסמכת השב"כ, קבע בית המשפט העליון שאיכון נשאי קורונה והיחידים עמם באו במגע קרוב מהווה פגיעה בפרטיותם.[45] השופטת ברון ציינה כי "המסר הטמון בשימוש בכלי זה הוא שכל תושב ואזרח בישראל מצוי במעקב מתמיד, משל היה דמות בספרו של

---

[43] ראו גם: תהילה שוורץ אלטשולר, "היזהרו: יש חור שחור שמאפשר לעשות עלינו ניסויים" **TheMarker** (14.7.2019) https://www.themarker.com/technation/.premium-1.7499515

[44] הנחיה מס' 2012/4 של רשם מאגרי המידע.

[45] בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת**, פס' 16-10 לפסק דינה של השופטת ברק-ארז; פס' 6 לפסק דינו של השופט הנדל. ר' התייחסויות דומות בבג"ץ 2109/20 **בן מאיר נ' ראש הממשלה** (26.4.2020), בפס' 36 לפסק דינה של הנשיאה חיות.

ג'ורג' אורוול "1984". עצם האפשרות של השימוש באיכוני השב"כ יוצרת תחושת מעקב ואפקט של משטור ("המבט הממשמע", כלשון הוגה הדעות מישל פוקו) – ולכך השלכות אף במישור החירות של הפרט, שכן ההנחה היא שהוא יימנע מלפעול בחופשיות תחת עיניו הפקוחות של המשטר."[46] דברים דומים נאמרו גם ביחס לסמכויות המשטרה לקבל נתוני תקשורת,[47] והם יפים גם ביחס למערך מצלמות לזיהוי לוחיות רישוי. איסוף מסוג זה הוא מטבעו גורף וחסר אבחנה ויש להבטיח שהשימוש יהיה נקודתי וממוקד ככל הניתן. אולם, הדברים שהובאו כאן תקפים פי כמה כשמדובר במערכת לזיהוי פנים המופעלת על ידי המשטרה. זאת, משום שהיא עוסקת באיסוף גורף של נתוני מיקום מבלי שניתן לטעון שמדובר במישהו אחר שהשתמש ברכב או מישהו אחר שלקח את המכשיר הסלולרי – הואיל ומדובר בזיהוי ביומטרי.

ב. סעיף התכליות ועניין דיכוי ההפגנות:

סעיף 10ג לתזכיר מונה את התכליות שלשמן מותר להציב ולהפעיל מערכת צילום מיוחדת, נייחת, נפרשת או ניידת. סעיף 10ו קובע את המטרות לשימוש במידע שנאסף (הצלת חיי אדם או הגנה עליהם; גילוי עבירות עוון ופשע, חקירתן או מניעתן; גילוי עבריינים והעמדתם לדין; חילוט רכוש על פי דין; ושוב – אכיפת איסורי כניסה וצווי הרחקה ממקומות ציבוריים).

ב.1. היחס בין סעיף התכליות וסעיף המטרות:

הכפילות בין שני הסעיפים היא בעייתית משום שבמובנים מסוימים תכליות הפעלת המצלמות רחבות הרבה יותר מאלה של מטרות השימושים במידע – למשל בהקשר של זיהוי דפוסי פשיעה וחיזוי פשיעה, ואם כך הדבר, מדוע איסוף המידע מותר לפי התכליות אבל השימוש בו למטרות זיהוי דפוסים לא מופיע במטרות של סעיף 10ו(א). מנגד, תכליות האיסוף הן לצורך צר של עבירות העלולות לסכן את החיים או הרכוש בעוד שהשימוש במידע שנאסף יכול להיות למטרות גילוי או אף מניעה של עבירות עוון או פשע. כך נוצר מצב שלפיו המשטרה מרחיבה מאד את השימושים במידע שנאסף, למטרות החורגות מן התכלית שלשמה נאסף. זוהי פגיעה קשה בעיקרון צמידות המטרה ואיננה משקפת את הבנת עיקרון המידתיות בפגיעה בזכות לפרטיות שהתזכיר עצמו כולל. בדברי ההסבר נאמר כי "הוחלט שאין מקום להגביל את המשטרה בשימוש בראיות שנאספו על ידה מכוח סמכות על פי דין, בדומה למצב החוקי הקיים בדברי חקיקה אחרים, אף ביחס למידע שהוא רגיש יותר" ואולם לא הוסבר באיזה מידע רגיש יותר מדובר וכך או כך עולה שהפיצול בין התכליות לבין המטרות מנסה לטשטש את העובדה הפשוטה שהשימושים בתוצרי הצילום ישמשו את המשטרה למטרות רחבות ביותר של פגיעה בפרטיות אזרחים ובזכויות האדם האחרות שלהם.

ב.2. סעיף התכליות:

באשר לסעיף התכליות כשלעצמו, אמנם, סעיף 10ד (ב) קובע שלא תהיה פגיעה בפרטיות

---

[46] בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת**, פס' 5 לפסק דינה של השופטת ברון

[47] בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (פורסם באר"ש, 28.5.2012) פס' 7 לפסק דינה של הנשיאה בדימ' ביניש

במידה העולה על הנדרש, אבל מידה העולה על הנדרש היא פונקציה של תכלית הפגיעה. לדעתנו, רשימת התכליות המופיעה בחוק רחבה למעלה מן הצורך, בארבעה היבטים שיפורטו להלן:

- **מניעת פשיעה:** ס"ק א עוסק ב"מניעה או סיכול של עבירות שעלולות לסכן את שלומו או בטחונו של אדם, את שלום הציבור או את בטחון המדינה" בעוד שס"ק ג עוסק ב"מניעת פגיעה חמורה בביטחון הנפש או הרכוש, ומצב שבו יש חשש ממשי לפגיעה כאמור". סעיף ג' הוא הגיוני אבל אין בו צורך לאור ההגדרה המרחיבה של סעיף א'. אנו סבורים שתפיסה רחבה של שימוש במצלמות זיהוי פנים לצורך מניעת עבירות העלולות לסכן את "שלום הציבור" תפגע קשה בזכות לפרטיות ותייצר אווירת שיטור.[48] יתרה מזאת, האיזון שבין הזכות לפרטיות לבין האינטרס הציבורי של הגנה על שלום הציבור צריך להיות איזון של וודאות קרובה ובוודאי לא יכול להתמצות בניסוח העמום, המתאים לחקיקה מנדטורית, "עלול".[49] לכן, לדעתנו יש להסיר את סעיף קטן א ולהותיר את סעיף קטן ג' בלבד.

- **איתור דפוסי פשיעה:** ס"ק ד מתאר תכלית מבולבלת: "חקירת דפוסי פשיעה בעבירות מסוג פשע, וכן גילוי עבירות מסוג פשע ומבצעיהן". ראשית, יודגש כי יש להבחין באופן מפורש בין גילוי עבירות מסוג פשע, לבין מחקר בנוגע לדפוסי פשיעה (שיתכן שניתן יהיה להסיק ממנו בעתיד לגבי חיזוי פשיעה).
באשר לגילוי עבירות, יש לפעול בהשראת חוק סדר הדין הפלילי וחוק נתוני תקשורת. אם מדובר במצלמת זיהוי פנים שממנה ניתן להסיק למשל על מצב רגשי של אדם, אין לאפשר שימוש בה ללא צו של שופט בית משפט מחוזי. כניסה לנבכי רגשותיו של אדם היא חודרנית הרבה יותר מאשר האזנה לשיחות הטלפון הפרטיות שלו.
באשר לשימוש במידע לצרכי מחקר והבנת דפוסי פשיעה, עמדתנו החד משמעית היא כי אם אין הכרח בדבר, אסור להשתמש במידע אישי לצרכי מחקר. בדיוק כפי שהדבר קיים לגבי מידע רפואי, שימוש שניוני במידע – בדרך שאיננה קשורה לנשוא המידע – אלא מיועדת להבנת תהליכים, דפוסים, סיוע לאחרים ולאנושות וכיו"ב - צריך להתבצע על מידע מותמם.
באם מדובר בתמונות פנים, אין מדובר במידע שניתן להתמים אותו וככזה לתפיסתנו אסור למדינה לעשות שימוש בתמונות שהושגו בכפיה מאזרחים שאין נגדם כל חשד מוקדם על מנת לבצע מחקרים. אכן, ניתן לחשוב על מחקרים אגרגטיביים בנוגע לדפוסי פעילות או מאפיינים כללים ואולם לצורך אלה אין צורך במערכות זיהוי פנים ובוודאי שאינם מצדיקים איסוף מידע לכתחילה.
אנו סבורים כי החששות המרכזיים אינם עצם השימוש הפנימי במידע למטרות מחקר

---

[48] ר' בהקשר עניין דנפ 2316/95 גנימאת נ' מדינת ישראל, פ"ד מט(4) 589 (1995), פס' 2 לפסק דינה של השופטת דורנר: "... הקניית מעמד של זכות יסוד למכלול האינטרסים הפרטיים המאוגדים בערך הכללי של 'שלום הציבור'... עשויה להביא לשלילת המשמעות של זכויות היסוד של הפרטים האינדיווידואליים. " עקרון זה יישום בעניין בג"ץ 8070/98 **האגודה לזכויות האזרח בישראל נ' משרד הפנים**, פ"ד נח(4) 842 (2004), בפס' 5 לפסק דינה של השופטת דורנר, ביחס לאיזון בין האינטרס הקולקטיבי של לקוחות הבנקים לקבל שירות יעיל לבין הזכות לפרטיות.

[49] וראו בעניין זה בג"ץ 73/53 **חברת "קול העם" בע"מ נ' שר הפנים** פ"ד ז 871, 882 887 (1953)

מודיעיני אלא נוגעים: (1) ליישום המידע במערכות חיזוי פשיעה משטרתיות, מה שעשוי ליצור אפקט של חוסר שקיפות וקופסאות שחורות, ולהגביר הטיות (2) לדליפה של המידע (3) לשימושים לא מורשים בו על ידי גורמים המשטרה (4) למיקור חוץ של המחקר לגורמים חיצוניים על החששות הנוגעים לזיהוי חוזר של המידע (5) לחוסר יכולת לתקף את המחקרים והמודלים על ידי אנשים חיצוניים בשל רגישות המידע.

לפיכך, יש להגדיר בצורה מדוייקת את סוגי המחקרים ואת היישום הפוטנציאלי שלהם ולא להשאיר זאת כ"מחקר".
נוסף על כך, יש לתת את הדעת על כך שהצבת מצלמות במרחב הציבורי לצורך 'מחקר' או זיהוי דפוסי התנהגות עלול לשמש עילה המצדיקה לכאורה ניטור קבוע של תאי שטח גאוגרפיים שלמים: שכונות מסוימות, או ערים מסוימות, עליהם תפקח באופן מתמיד העין החוקרת של מערכות הצילום. מעקב כזה, שנועד לזהות גורמים עוינים במרחב בהסתמך על דפוסי ההתנהגות שלהם, הפעילה ארצות הברית בפקיסטן במסגרת חיסולים באמצעות כטב"מים,[50] גם אם ניתן אולי לקבל תיעוד כזה בזמן סכסוך חמוש בשטח אויב, לא ניתן לקבל זאת ככלי שיטור שמופעל בשגרה בסביבה אזרחית. נזכיר כי עצם פריסת מערכות אלו בשכונות מסוימות וברחובות מסוימים עשוי לתייג אותם כ"איזורים מוכי פשיעה", ולהנציח בהם את התווית הזו (מעין אפקט פרומתיאוס); או כ"איזורי מלחמה", מה שעלול ליצור ביטחוניזציה של המרחב האזרחי – למשל שימוש מוגבר בהן ביישובים ערביים או בסמוך להם, על כל המשתמע מכך.

נדגיש כי אם אכן מדובר בשימושים לצורך אימון מערכות לחיזוי פשיעה, אנו מתנגדים לכך בתוקף וסבורים שלא ניתן יהיה בשום מקרה לכלול אימון כזה בגדר "מחקר" ויהיה הכרח בעבודת מטה שתגדיר מסגרת ייחודית בחוק תהליכי עבודה סדורים המיועדים למזער סיכוני הטיות וליצור גופי פיקוח ובקרה על תהליכי מחקר ואימון כאלה.

- **מחקר:** סעיף 10ו(ב) לתזכיר קובע כי המשטרה תהא רשאית לעשות שימוש במידע שנאגר ממערכת צילום מיוחדת לצורך מחקר בקשר לתפקידים האמורים בסעיפים 3 ו-5 לפקודת המשטרה ובלבד שהמידע מהמאגר המועבר לצורך המחקר אינו כולל פרטים מזהים. מחקר באמור יאושר בידי קצין משטרה בדרגת ניצב משנה ומעלה שהמפקח הכללי הסמיכו לעניין זה. זוהי חריגה משמעותית מעיקרון צמידות המטרה. גם אם ניתן היה לחשוב – וכאמור, לתפיסתנו מדובר בהסדר בלתי מידתי – שהמשטרה יכולה לאסוף ולעבד נתונים רגישים הקשורים לתכליות המנויות בתזכיר, הקביעה לפיה המשטרה יכולה לעשות שימוש

[50] Nina Franz, *Targeted Killing and pattern-of-life analysis: weaponised media*, 39 MEDIA, CULTURE & SOC. 111-121 (2017)

במידע אישי רגיש של אזרחים לצרכי מחקר כלליים, בנוגע לכלל תפקידיה, היא בלתי מתקבלת על הדעת. כפי שנכתב לעיל, סוגיית המידתיות תלויה בתכלית ואיננה מנותקת ממנה. לא ניתן לומר שטיפול במידע רגיש הוא מידתי אם באיבחת קולמוס הורחבו תכליות השימושים למחקר ביחס לכלל תפקידי המשטרה. יתרה מזאת, החשש הוא שהמשטרה תשתמש בסמכויות העומדות לרשותה כדי לבצע "מסעות דיג" ולאסוף מידע על אזרחים רק כדי לבצע מחקרים.

אם נאספו נתונים ויש רצון לעשות בהם שימוש שניוני למטרות שאינן אכיפת חוק אלא למטרות מחקר, תתכבד המשטרה ותבקש את הסכמתם של מושאי המחקר, כפי שמקובל בכל מחקר אחר על נתונים ביומטריים של בני אדם, ומקום בו אי אפשר להשיג את הסכמתם – יש להקים מערך של פיקוח משפטי ואתי, בדומה למערך וועדות הלסינקי לגבי מידע בריאות ולמערך וועדות האתיקה המוסדיות הקיימות לגבי מחקר במוסדות אקדמיים. . אין להסכים עם תפיסה שלפיה מרגע שהמשטרה אספה נתונים פרטיים על אזרחים נתונים אלה הופכים לרכושה שלה. הנתונים נאספו בכפיה מאזרחים, למטרת אכיפת חוק ולא למטרת מחקר והשליטה בכל שימוש אחר בהם צריכה להיות בידי אזרחים. לא מתקבל על הדעת שמחקרים אלה יאושרו על ידי קצין בדרגת ניצב משנה שהוסמך לכך על ידי המפכ"ל, הואיל והקצין ואף המפכ"ל אינם אנשי מחקר בנתונים ואין סיבה להניח שיש להם את המומחיות המעמיקה בהבנה של מחקרים כאלה. המשטרה תצטרך גם להקים וועדות אתיקה מיוחדות, כפי שקיים במערכת הרפואית או במערכת האוניברסיטאית. וועדות אלה יכללו מומחי מחקר, מומחי התממה ומומחי אבטחת מידע. וועדות אלה יהיו בעלות הסמכות לפטור מהסכמה של מושאי המידע רק אם ישוכנעו שהמידע איננו בר זיהוי מחדש. יש לקבוע חובת פרסום למחקרים שייעשו במידע זה. בנוסף, יש לאסור בכל מקרה העברה של נתונים אלה, גם אם עברו התממה, לצרכי מחקר לאף גוף מחוץ למשטרה – מחקרי, מסחרי או ציבורי.

בנוסף, סעיף 10 י לתזכיר קובע בנוסף כי כל מגבלות ההסדר לא יחולו על הפקת מידע סטטיסטי ומצטבר ממידע שנאגר ממערכות צילום מיוחדות. בדברי ההסבר נכתב כי "מאחר שהתממת המידע מאיינת את הפגיעה בפרטיות, מוצע להבהיר כי ההוראות המיוחדות הקבועות בפרק זה לא יחולו על מידע סטטיסטי ומצטבר שהופק ממערכות הצילום המיוחדות".

זהו חוסר הבנה שורשי ביחס לשאלה מהי התממה של מידע המלמד, שוב, על מידת חוסר הבשלות של התזכיר. מידע מותמם הוא מידע אישי, פרטני, לאחר שהוסרו ממנו מזהים אישיים. לעומת זאת, מידע סטטיסטי הוא מידע מקובץ. המונח "מצטבר" איננו מונח ברור בהקשר זה. הקביעה לפיה התממה של מידע "מאיינת את הפגיעה בפרטיות" היא קביעה שגויה, לא מקובלת במחקר ויתרה מזאת – לא מקובלת גם בכללים העוסקים במחקר במידע מותמם. כך, למשל, בשימושים שניוניים במידע בריאות מובהר כי מחקר בנתונים מותממים חייב לקבל אישור ועדות אתיקה ואף את הסכמת מושאי המידע בשל היכולת לבצע זיהוי חוזר

של הנתונים[51]. עד לפני כחמש שנים התפיסה המקובלת היתה שמידע שעבר התממה איננו מעורר חשש לפגיעה בפרטיות ולכן אין צורך לבקש הסכמה ממושאי המידע. במהלך השנים האחרונות, עם פרסום עוד ועוד מחקרים בכתבי עת מובילים המלמדים על האפשרות לבצע "זיהוי חוזר" של מאגרים שעברו התממה, תפיסה זו אינה יכולה להיות תקפה עוד והנחת העבודה צריכה להיות כי **אין מאגר מותמם שמוגן באופן מוחלט מפני זיהוי חוזר**. היכולת לקחת מאגר אנונימי של נתוני מיקום סלולריים, למשל, ולזהות באמצעותו אנשים, הוכחה כבר בשנת 2013 במאמר בכתב העת נייצ'ר. תחקיר רחב שפורסם אך לאחרונה הראה כיצד ניתן לאחזר זהות לפי נתונים אנונימיים באפליקציות סלולריות[52].

יוער כי אפילו מידע מקובץ עשוי להיות בר זיהוי חוזר, אם הוא בקבוצות יחסית קטנות. לעיתים ניתן "לבנות מחדש" את חלק מהנתונים המקוריים ששימשו ליצירת המידע בעזרת הטבלאות בלבד (reconstruction attack). כך עולה למשל ממחקרם של תומר אשור[53] ואחרים לגבי אפשרות לזהות בוחרים ספציפיים לפי מידע קבוצתי מקלפיות.

- **סיכול הפגנות:** ס"ק ה קובע כאחת התכליות את "אכיפת איסורי כניסה וצווי הרחקה ממקומות ציבוריים". לא זו אף זו, עניין זה מופיע גם בסעיף המטרות של השימושים במידע שנאסף. דומה, שלהבדיל משאר העניינים הנוגעים לאכיפת חוק, חשוב היה למנסחי התזכיר להודיע כי הם מתכוונים להשתמש במערכות זיהוי פנים לאכיפת הוראות המגבילות את חופש התנועה במרחב הציבורי, דבר המעלה חשש מפני הסתייעות בתכלית זו לשם דיכוי הפגנות ומחאות פוליטיות.

הזכות להפגין היא זכות יסוד במשטר דמוקרטי, הנגזרת מהזכות לחופש ביטוי.[54] היא זכות יסוד שיש בה כדי לעצב את אופיו של המשטר – ולא בכדי משטרים אוטוריטריים מדכאים הפגנות ביד ברזל. "לזכות ההפגנה והאסיפה מוכר מקום של כבוד בהיכל זכויות היסוד של

---

[51] משרד הבריאות, חוזר המנהל הכללי בנושא: שימושים משניים במידע בריאות, ינואר 2018 https://www.health.gov.il/hozer/MK01_2018.pdf ; משרד הבריאות, חוזר המנהל הכללי בנושא: שיתופי פעולה המבוססים על שימושים משניים במידע בריאות, ינואר 2018 https://www.health.gov.il/hozer/MK02_2018.pdf

[52] https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/

[53] Ashur T., Dunkelman O., Talmon N. (2017) Breaching the Privacy of Israel's Paper Ballot Voting System. In: Krimmer R. et al. (eds) Electronic Voting. E-Vote-ID 2016. Lecture Notes in Computer Science, vol 10141. Springer, Cham. https://doi.org/10.1007/978-3-319-52240-1_7

[54] בג"ץ 2557/05 **מטה הרוב נ' משטרת ישראל** פ"ד סב(1) 200 (2006),פס' 10 לפסק דינו של הנשיא (בדימ') ברק.

האדם".[55] נוכח חשיבות הזכות להפגין, למשל, ההגבלות שהוטלו במהלך התפרצות נגיף הקורונה בשנת 2020, החריגו הפגנות כפעילות מותרת.[56] לאור המעמד המיוחד של הזכות להפגין החילה הפסיקה קריטריונים מחמירים על מנת לבחון את האיזון בינה לבין אינטרסים וזכויות הניצבים מולם, ובתוכם שמירה על שלום הציבור והסדר הציבורי.[57] לכן, על המשטרה, בבואה להתערב בזכות להפגין, לנקוט בזהירות מפליגה על מנת שלא לגרום לאפקט המצנן את חופש הביטוי הפוליטי, ובפרט את חופש הביטוי של אלה "שכלי הביטוי הממלכתיים והמסחריים אינם עומדים לרשותם".[58]

לתפיסתנו, עצם הפעולה של פריסת מערכות מעקב חזותיות המתעדות פעילות פוליטית יש בה כדי לייצר אפקט מצנן על אזרחים המבקשים להשמיע את קולם תוך הטמעות בהמון המפגינים, לבקר מתנגד משטר בביתו או לנקוט במחאה יחידנית מול מבנה שלטוני. האפקט המצנן מתגבר שבעתיים כאשר מערכות אלו ניחנות ביכולת לזהות את המפגינים בזמן אמת או בדיעבד.[59] משטרים אוטוריטריים מפעילים כבר עתה (או נחשדים כמפעילים) מערכות כאלו על מנת להרתיע מפגינים מפני התנגדות למשטר.[60] מערכות לזיהוי פנים הופעלו בבולטימור ובאוקלנד שבארצות הברית במהלך מחאות 'Black Lives Matters' בשנת 2015 וכן במהלך המחאות שלאחר הריגתו של ג'ורג' פלויד ב-2020 וזכתה לביקורת שקרעה את החברה האמריקנית.[61]

ג. **הפיקוח על הצבת המצלמות ועל השימוש בהן:** לפי סעיף 10ד ס"ק ג,ד לתזכיר, הצבה והפעלה של מצלמות נייחות ונפרשות תיעשה באישור קצין מוסמך בדרגת תת ניצב,

---

[55] בג"ץ 153/83 **לוי נ' מפקד המחוז הדרומי של משטרת ישראל**, פ"ד לח(2) 393, 398 (1984)

[56] עע"מ 1775/20 **התנועה למען איכות השלטון בישראל נ' עיריית ירושלים** (פורסם בנבו, 24.09.2020), בפס' 36 לפסק דינו של המשנה לנשיאה מלצר.

[57] בג"ץ 5078/20 **טלי פדידה ואח' נ' משטרת ישראל** (פורסם בנבו, 19.8.2020), פס' 19-20 לפסק דינו של השופט פוגלמן

[58] בג"ץ 153/83 **לוי נ' מפקד המחוז הדרומי של משטרת ישראל**, פ"ד לח(2) 393, 398 (1984)

[59] ר' לדוגמא Monika Zalnieriute, *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, 22 COLUMBIA SCI. & TECH. L. REV. 22-23 (2021, Forthcoming)

[60] למשל, דווח כי רוסיה עושה שימוש במערכות זיהוי פנים על מנת לבצע מעצרי מנע של מתנגדים פוליטיים. Gleb Stolyarov and Gabrielle Tétrault-Farber, *"Face control": Russian police go digital against protesters,* REUTERS (11.2.2021). ר' גם *"Russia: Police target peaceful protesters identified using facial recognition technology"* AMNESTY INTERNATIONAL (27.4.2021). בהונג קונג, דווח כי מפגינים ופעילים פוליטיים המתנגדים לרשויות הסיניות חוששים, חרף הכחשת הממשל, כי ברחבי העיר מוצבות מערכות לזיהוי פנים שיופנו נגדם. Sidney Fussell, *Why Hong Kongers Are Toppling Lampposts*, THE ATLANTIC (30.8.2019)

[61] *"Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color"* ACLU (11.10.2016) available on https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target; Maya Shwayder, *Police facial recognition tech could misidentify people at protests, experts say*, DIGITAL TRENDS (2.6.2021) available on https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification/

וקביעת מתווה הפעלה של מצלמות ניידות תאושר על ידי קצין מוסמך בדרגת תת ניצב. הגורם שיוסמך לאשר הצבתן של מצלמות נפרסות שהן חלק ממערכת צילום מיוחדת, שהצבתן באמור ארעית, לפרק זמן שלא יעלה על 3 חודשים, יהיה קצין משטרה בדרגת ניצב משנה. כפי שכבר נאמר לעיל, התזכיר אינו דורש פניה פרטנית לאישור שיפוטי בטרם יוצבו מצלמות או בטרם ייעשה שימוש במידע שנאסף. בכך, הוא משאיר את כלל הסמכויות בידי המשטרה ללא כל מערך פיקוח. בעניין זה אפשר להבחין בין איסוף המידע, המהווה לרוב "מסע דיג" ואיננו מוכוון אפילו לתפוס אדם קונקרטי, לבין עיבוד המידע, ולכל הפחות לקבוע כי עיבוד המידע הפרטני לאחר שנאסף ייעשה באישור נשיא בית משפט מחוזי על בסיס יסוד לחשד ממשי לעבירה.

נזכיר כי בעניין **האגודה לזכויות אזרח** קבע בית המשפט כי פרשנות מידתית של חוק נתוני תקשורת היא כזו המתירה מעקב ממוקד (targeted), לבירור חשד קונקרטי, ולא לאיסוף מודיעין כללי.[62] באמור, הבקרות וההגבלות שצריך שיחולו על שימוש בנתונים שמקורם במערכות צילום מיוחדות, צריכות להיות מחמירות מאלו החלות על השגת נתוני תקשורת, נוכח פוטנציאל הפגיעה בפרטיות שבצידן.

ככל שמערכות צילום מיוחדות אלו נועדו להשתלב במערכים טכנולוגיים של חיזוי פשיעה ומניעתה, ומרבית האיסוף בהן יהיה אוטומטי, הרי שיש להסדיר בחוק את לא רק את הגישה האנושית הפרטנית לנתונים שבמערכות אלו, אלא את תהליכי העיבוד, הלמידה והחיזוי עצמם, ואת הבקרות עליהן. כיוון פעולה בהקשר זה יהיה למידה מהוראות תקנות הפרטיות האירופיות (GDPR) לגבי החובה להכניס גורם אנושי לתהליך קבלת ההחלטות (סעיף 22 לתקנות); תיעוד של המערכת והבטחת יכולות מעקב בדיעבד אחרי תהליכים (tracability); וממשל נתונים תקין.

עוד נוסיף כי לתפיסתנו, יש צורך בהתייחסות רוחבית לכל המקורות שמהם יגיע ניתוח וידיאו וזיהוי פנים מעבר לאלה שבהם המשטרה עושה שימוש. כתבנו קודם כי נכון להקים וועדה שתעסוק בכך. נציע, כי הסדר מוסדי רחב יותר לפיקוח על זיהוי ביומטרי דרך מערכות נבונות לא יכול להסתפק בפיקוח של בית משפט המאשר חיפוש אחר חשוד ויהיה צורך בהקמת נציב פיקוח מיוחד שיהיו לו הסמכויות המנהליות והיכולות הטכניות לבדוק שתהליכי השימוש במידע, ובמיוחד במקרה של פיתוח מודלים על בסיס המידע הזה, שומרים על אמות מידה טכניות נאותות כדי להבטיח עמידה בסטנדרטים בסיסיים של אתיקת AI.

ד. **מגבלות על השימושים ועל שימושים לרעה:** התזכיר קובע בסעיף 10ו(ג) כי שמירת המידע שנאגר ממערכת צילום מיוחדת תיעשה בדרך שתבטיח הגנה מפני שימוש לא מורשה במידע, שיבושו, חשיפתו או העתקתו בלא רשות כדין. ואולם, התזכיר איננו קובע ביצד יהיה להגן על המידע ומעדיף להעביר את קביעת הכללים האלה לתקנות. לתפיסתנו, יש

---

[62] בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (פורסם באר"ש, 28.5.2012) פס' 20 לפסק דינה של הנשיאה בדימ' ביניש

לקבוע בחוק קריטריונים בהירים להגנה על המידע ולהרשאות השימוש בו. זאת, בשל:

א. הרגישות הגבוהה ביותר של המידע הכולל תמונות פנים, שהוא למעשה מידע ביומטרי. בהקשר זה נפנה לסעיף 25 לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, תש"ע-2009 הקובע כי נתוני זיהוי ביומטריים יישמרו (1) בדרך שתבטיח הגנה מפני דליפת מידע מהמאגר או פריצה אליו, וכן מפני העברה, חשיפה, מחיקה, שימוש, שינוי או העתקה בלא רשות כדין; (2) בדרך שתמנע שימוש בהם בניגוד להוראות לפי חוק זה; (3) בדרך שתבטיח הגנה על פרטיותם של התושבים שהאמצעים והנתונים באמור מתייחסים אליהם, ותאפשר בקרה ופיקוח על אופן השימוש במאגר, לרבות שימוש החורג ממסגרת ההרשאה לפי סעיף 13. בנוסף קובע החוק כי כל פעולה המבוצעת במאגר הביומטרי תתועד באופן שיאפשר פיקוח ובקרה על אופן ביצועה, על מועד ביצועה ועל מבצע הפעולה. אנו סבורים כי נדרש כאן ניסוח המקיים לכל הפחות דרישות ברמה דומה לאלה.

ב. הידע המצטבר בספרות לגבי חשיבותו של "הגורם האנושי" בהבטחת סייבר והכשל בהטמעת מערכות רגישות ללא הכשרה מספקת. חולשת הגורם האנושי נובעת מחוסר הבנה של העובדים בארגון באשר לחשיבות אבטחת המידע ובאשר להשלכות התנהגויותיהם על הסיכון למתקפת סייבר, וכן מהיעדר מודעות העובדים בנושאים אלו, התעלמות או חוסר אכפתיות בנוגע לרמת הסיכון האפשרית או פעולה בתנאי לחץ ובחוסר תשומת לב, והכול במסגרת קבלת הרשאות גישה רחבות שלא לצורך.[63] העקרונות והנהלים שיש לאמץ כדי להפחית את הסיכון הנשקף מהגורם האנושי עשויים להיות שונים מארגון לארגון. עם זאת, הדעה הרווחת היא שרק כך אפשר למזער את הפגיעה הפוטנציאלית של הגורם האנושי כחוליה החלשה במערכת הגנת הסייבר.

ג. ניסיון החיים המצטבר לפיו המשטרה איננה פועלת בכל חומרת הדין בטיפול בשוטרים המועלים בתפקידם ומחפשים מידע במאגרים באופן בלתי מורשה. נוכח העובדה שמדובר בסמכות חריגה המאפשרת שימוש במידע אישי רגיש על אזרחים מן השורה ללא הסכמתם וללא צו בית משפט, נזכיר כי גישה ללא הרשאה למאגרי מידע ולמערכות מידע משטרתיות היא רעה חולה בתוך משטרת ישראל. החל משנת 2016 עולה כי בכל קובצי החלטות של בית הדין למשמעת של המשטרה ישנם תיקים העוסקים בגישה בלתי מורשית של שוטרים למערכות המידע המשטרתיות ובשאילתות שלא כדין למאגרי מידע משטרתיים[64]. למרבה הצער נציין גם כי הענישה על עבירות חמורות אלה אינה תמיד גבוהה ולעתים מזומנות מסתיימת בעסקות טיעון, הורדה בדרגה לתקופה קצובה בלבד, נזיפות וקנסות ולא מעבר

---

[63] *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from* Israel Levy, *The Human Factor: The Unspoken Threat in Cybersecurity*, IT *Within*, KASPERSKY; PROPORTAL (April 19, 2017); Lee Hadlington, *The "Human Factor" in Cybersecurity: Exploring the Accidental Insider*, *in* PSYCHOLOGICAL AND BEHAVIORAL EXAMINATIONS IN CYBER SECURITY 46, 47 (John McAlaney, Lara A. Frumkin, & Vladlena Benson, eds., 2018); Mohd Anwar et al., *Gender Difference and Employees' Cybersecurity Behaviors*, 69 COMPUTERS IN HUMAN BEHAVIOR 437 (2017)

[64] ביד"מ 7/2019; ביד"מ 72/2018.

לכך, ובהתחשבות יתר בנסיבות האישיות של השוטרים ולא בחומרת המעשה[65]. איש מאלה שהועמדו לדין על מעשים אלה, שיש בהם הניצול המחפיר ביותר של כוחם של שוטרים לפגיעה בפרטיות אזרחים – לא סולק משורות המשטרה.

ה. שקיפות:

סעיף 10ב לתזכיר קובע כי משטרת ישראל רשאית להציב, להפעיל ולהשתמש במערכת צילום מיוחדת "המנויה בתוספת הרביעית". התוספת הרביעית, שבה בעצם יש את רשימת המערכות, מתעדכנת באישור השר לביטחון פנים בהתייעצות עם שר המשפטים. אבל, "פרטים בתוספת הרביעית אינם טעונים פרסום ברשומות" – כלומר, אפשר לשכלל את המערכות, להוסיף מערכות חדשות - אבל אין צורך לעדכן על כך את הציבור. בדברי ההסבר נקבע כי הדבר נעשה "על מנת לשמור על חסיון האמצעים והמערכות". סעיף 10ד (ה) – קובע כי מערכות צילום מיוחדות נייחות ונפרשות שיוצבו לפי סעיף זה יוצבו בדרך שתהיה גלויה לעין, אלא אם קבע הקצין המוסמך כי נסיבות העניין מצדיקות הצבת המצלמות בדרך שאינה גלויה לעין וכן ש"הקצין המוסמך ייתן דעתו" באשר לאפשרות ליידע את הציבור על הצבת מצלמות באמצעות שילוט מתאים ככל שאין בכך כדי לפגוע בתכליות האמורות בסעיף 10ג – אבל אין שום חובה של שקיפות. אין גם חובת דיווח שנתית לכנסת או לכל רשות אחרת.

שקיפות היא ערך יסוד באתיקה של מערכות נבונות, לרבות מערכות צילום מיוחדות ובפרט כאלו שתכליתן הוא אכיפת חוק ושלתוצאות פעולתן השפעה מהותית על מושאיהן. תחת ערך השקיפות מתכנסים מספר עקרונות כגון הסברתיות (explainability), קוד פתוח ומידע פתוח וקיום אינטרקציה מיודעת עם בינה מלאכותית.[66] יש הממשיגים את עקרון השקיפות באמצעות עקרון ה'מפורשות' **(**explicability**)**, הממזג בין ההבנה של אופן פעולתה של מערכת הבינה המלאכותית לשאלת האחריותיות לפעולתה.[67] גם כאשר מערכת בינה מלאכותית פועלת לכאורה בשקיפות מלאה ורבבות שורות הקוד שלה פתוחות לעיון הציבור –

---

[65] ראו למשל בד"מ 16/175; בד"מ 18/18; בד"מ 18/44; שבכולם היו עונשים קלים בעסקות טיעון. ביד"ם 17/6 (הרצת 37 שאילתות שונות בארבעה מועדים) - נזיפה חמורה והורדה בדרגה למשך 10 חודשים מתוכם 3 בפועל; בביד"ם 17/4 ; ביד"ם 16/45 - נזיפה חמורה והורדה בדרגה למשך 6 חודשים.

[66] Jessica Fjeld, Nele Achten, Hanna Hiligoss, Adam Nagy and Madhulika Srikumar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, BERKMAN KLEIN CENTER RESEARCH PUBLICATION NO. 2020-1 41 (2020) available at https://cyber.harvard.edu/publication/2020/principled-ai.

[67] Luciano Floridi, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge, Robert Madelin, Ugo Pagallo, Francesca Rossi, Burkhard Schafer, Peggy Valcke, and Effy Vayena, *Ai4people–an ethical framework for a good ai society: (Opportunities, risks, principles, and recommendations*. 28 MINDS AND MACHINES 689–707 (2018)

אין ערב לכך שהדיוטות יצליחו להבין כיצד היא פועלת ולמי לייחס אחריות בגין תוצריה.[68] שקיפות נדרשת על מנת שהמשתמשים יוכלו לבטוח במערכות, ולפקח שפעולתן תקינה והוגנת. היכולות והמטרות של מערכות בינה מלאכותית צריכים להיות גלויים, וההחלטות אותן הן מקבלות צריכות להיות ניתנות להסבר. כשמדובר בקופסאות שחורות שלא ניתן להסביר את פעולתן – יידרשו אמצעים משלימים, ובתוכם היכולת לבקר את המערכת (auditability)[69] ולעקוב אחר תהליכים בה (traceability).[70]

אין זה מתחייב שהקרביים של מערכות אכיפה רגישות יהיו גלויים לעיני הציבור. ואולם, יש להבטיח שישנם מנגנונים עצמאיים המבקרים את תקינות המערכות; שישנו נציב תלונות עצמאי או אומבודסמן שבסמכותו לבדוק טענות של אזרחים על כשלים במערכות; וכן להבטיח דיווח שנתי פומבי לוועדת הפרלמנטרית המפקחת על ביקורות, בקרות ותקינות המערכת. מבלעדי כל אלה ספק אם יוכל הציבור לתת אמון במערכות הצילום המיוחדות וברשויות המפעילות אותן, ולהרגיש חופשי ונינוח במרחב הציבורי.

יתרה מזאת, השימוש במצלמות ופיענוח תכני תמונה ווידיאו לצורך זיהוי פנים איננו מוגבל רק לשימושים משטרתיים ורק למערכות שיוצרו לטובת זיהוי פנים. השימוש המדובר עולה – ויעלה בשנים הקרובות - בהקשרים רחבים של מערכות המצלמות שבהן רושתו ערי ישראל ובבישיה בעשור האחרון. התזכיר עצמו מתייחס לכך כשהוא קובע בסעיף 10ז כי "מבלי לגרוע מסמכות המשטרה לפי כל דין, שימוש כהגדרתו בפרק זה במידע שמקורו במערכות צילום שאינן מערכות צילום מיוחדות יעשה לשם התכליות הקבועות בסעיפים 10ג ו-10ו", כלומר, הוא משקף הבנה שלפיה בשנים הקרובות יתכן שניתן יהיה לעבד נתוני זיהוי ביומטריים ותמונות פנים גם מתוך מצלמות אחרות. במקביל, התזכיר מבקש לסייג את השימוש וקובע כי משטרת ישראל תהיה רשאית להציב ולהפעיל רק מערכות צילום מיוחדות שנקבעו בתוספת הרביעית לפקודה. בדברי ההסבר נאמר ש"ההסדר המבוקש הינו הסדר החל על משטרת ישראל, בעוד סמכותם של גורמים אחרים לעשות שימוש במצלמות מיוחדות ואופן השימוש על ידי גורמים אלו תבחן בהתאם לדין החל עליהם"[71].
לתפיסתנו, לא ניתן, כפי שהתזכיר מבקש, להותיר את הטיפול באלה – הן מערכות שבשימוש גורמים אחרים והן מערכות שניתן יהיה להפוך בעתיד למערכות זיהוי פנים - למועד מאוחר יותר, אלא נדרשת כבר בעת הזאת עבודת רוחב מעמיקה שתטפל בכל הקשרי זיהוי הפנים

---

[68] CHRISTOPH BARTNECK, CHRISTOPH LÜTGE, ALAN WAGNER AND SEAN WELSH, AN INTRODUCTION TO ETHICS IN ROBOTICS AND AI 36 (2021)

[69] ר' US Public Policy Council, Association for Computing Machinery, *Statement on Algorithmic Transparency and Accountability* (2017) available at https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf, בעמ' 2 (עקרון מס' 6).

[70]); AI HLEG, Ethics Guidelines for Trustworthy AI (8.4.2019) available at ; https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines, בעמ' 13. ל-traceability, ר' גם Defense Innovation Board, AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense (2019), בעמ' 8 (עקרון מס' 3).

[71]

למטרות אכיפת חוק ושיטור. עבודה כזאת לא נעשתה כאן וההסדר המגולם בהצעת החוק אינו בשל ובייחוד מבקש להנות מכל העולמות (על חשבון זכויות האזרח).

ו. תקופות שמירת המידע: סעיף 10ו (ד) תקופות שמירת המידע ייקבעו בתקנות, יוגבלו רק לפרק הזמן הנדרש להשגת המטרות לשמן הן הוצבו, בשים לב למידע הנוגע לתכליות המנויות בסעיף 10ג, לסוג מערכות הצילום המיוחדות, לאופן הצבת המצלמות ולמיקומן. בדברי ההסבר נוספו שיקולים שלא קיימים בתזכיר עצמו - א. האם המידע המצולם קשור לביצוע עבירה או לאיתור נעדר או שמדובר בעוברי דרך שנקלטו באקראי. ב. סוג מערכת הצילום המיוחדת בהתאם לסוגים שאושרו לשימוש והמנויים בתוספת הרביעית - האם מדובר במערכת צילום המזהה לוחיות רישוי של רכבים, זיהוי ביומטרי של בני אדם וכו'. ג. האם מדובר במידע ממצלמות נייחות, נפרשות או ניידות. ד. מיקומן של המצלמות עשוי להשפיע על משך השמירה – כך למשל, במקומות בהם הפגיעה בפרטיות גדולה יותר יישמר המידע לפרק זמן קצר יותר בעוד במקומות בהם אדם צפוי להידרש להזדהות, כגון במעברי גבול, ניתן יהיה לשמור את המידע לפרקי זמן ארוכים יותר.

ראשית, אנו סבורים שלכל הפחות יש צורך בקביעת תקופת שימור מירבית בחוק, שאליה יהיה כפוף שיקול הדעת המיניסטריאלי בהתקנת תקנות. יתר על כן, ניתן כבר עתה – ורצוי - לקבוע תקופת שימור מירבית בחוק עבור כל אחת מהתכליות המנויות בס' 10ג. כמו כן, נדרש להקים גורם טכני לפיקוח על תקינות המחיקה, שידווח לוועדת הפנים והגנת הסביבה באופן פומבי מדי שנה על סטטוס ביעור הנתונים, ועל מצב המלאי הקיים.

כמו כן, יש לתת את הדעת על כך שמידע שנעשה בו שימוש למטרות מחקר צריך כללי שימור נפרדים, בייחוד כאשר מדובר בפיתוח מודלים סטטיסטיים לשימוש המשטרה. בהתאם לתכליות של מודלים אלה, ייתכן ויידרש לשמור את בסיס הנתונים עליו התבססו לביקורת עתידית או רענון המודל, או לזיהוי בדיעבד של שגיאות או הטיות. הצורך לתת את הדעת על שאלות של מחקר מבוסס נתוני מערכות אלו, כש'מחקר' זה ותכליותיו לא מוגדרות, רק מדגיש עד כמה התזכיר אינו בשלולא מבוסס עבודת מטה רצינית.

ז. העברת מידע בין גופים ציבוריים:

בהתאם לסעיף 10ח לתזכיר, העברת מידע מן המשטרה לגופים ציבוריים אחרים מותרת לשימוש בהתאם לתכליות שבסעיף 10ג ולצורך מילוי תפקידו של הגוף. התכליות, כפי שכתבנו למעלה מנוסחות בצורה רחבה למעלה מן הצורך. גם בהתניית ההעברה לגוף הציבורי "לצורך מילוי תפקידו" - מדובר במשרעת רחבה של סמכות העברה. השורה התחתונה היא שמעתה תהיה לשב"כ, למוסד, ואפילו לאמ"ן, גישה ישירה למערכות ביומטריות על אזרחי מדינת ישראל. במגיפה הבאה לא יהיה צורך באיכוני השב"כ, אפשר יהיה להשתמש ישירות במערכות המשטרתיות. בנוסף, בהגדרת "גוף ציבורי" נכללים גם "כל גוף ציבורי אחר שקבע שר המשפטים בצו באישור ועדת הפנים והגנת הסביבה של הכנסת". למעשה, שר המשפטים יכול להכליל בצו גם גופים כמו משרד התחבורה (מחקרי תנועה מבוססי LPR); משרד הבריאות וגם רשות הטבע והגנים והמשטרה הירוקה. יוזכר: מדובר

במידע ביומטרי, מן הרגישים ביותר והפרטיים ביותר שאפשר להעלות על הדעת מבחינת יכולות הניתוח והעיבוד שלו. השימושים שיוכלו הגופים האלה לעשות במידע – ייקבעו בהנחיות או בנהלים פנימיים. למעלה מן הצורך, נזכיר את רמת הפירוט לה נדרש הסדר העברת נתוני האיכונים של נשאי הקורונה בין השב"כ למשרד הבריאות ואת העניין הציבורי הרב בו – התזכיר מציע כי העברת נתונים פולשניים לא פחות לא תהיה כרוכה אף בכך שהגוף המקבל את המידע יעמוד בסטנדרט המינימלי של התזכיר עצמו.