29 ביולי, 2021

לכבוד
<u>המשרד לביטחון הפנים</u>

<u>הנדון: תגובה לתזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (תיקון מס')(מערכות צילום מיוחדות), התשפ"א-2021</u>

פרטיות ישראל (ע"ר)[1] מתכבדת להגיש את תגובתה לתזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (תיקון מס')(מערכות צילום מיוחדות), התשפ"א-2021 (להלן: "**תזכיר החוק**" או "**התזכיר**").

1. <u>הקדמה</u>

1.1. ב-8 ביולי 2021 פרסם משרדכם באתר התזכירים הממשלתי את תזכיר החוק. התזכיר מבקש להסמיך את משטרת ישראל להציב מצלמות מיוחדות במרחב הציבורי, ולאגור באופן נרחב מידע המאפשר זיהוי חד ערכי בזמן אמת של כל אדם, רכב או חפץ אחר במרחב הציבורי (להלן: "**מערכות המעקב**"). תכליתו המוצהרת של התזכיר היא סיוע למשטרה במאבק בפשיעה, מניעת עבירות ושמירה על שלום הציבור וביטחונו. אף על פי שמדובר בתכלית ראויה וחשובה, ההסדר המוצע בתזכיר אינו מידתי ועלול להוות פתח לאכיפה מגמתית, אפליה בין תושבים וקבלת החלטות אכיפה מהותיות הרחק מעינו הבוחנת של הציבור.

1.2. תזכיר החוק פורסם בתגובה לעתירה לבג"ץ 641/21 **האגודה לזכויות האזרח נ' משטרת ישראל** שהגישה פרטיות ישראל (עותרת מס' 2) ביחד עם האגודה לזכויות האזרח נגד השימוש במערכת לזיהוי לוחיות רישוי, "עין הנץ" (להלן: "**העתירה**"). הטענה המרכזית בעתירה היא שהמשטרה מפעילה בחשאי <u>וללא הסמכה חוקית</u>, מערכת אוטומטית שעוקבת ומתעדת את תנועת הנוסעים בישראל. במסגרת הדיון בעתירה, ובהתאם להחלטת בג"ץ מיום 27 במאי 2021, התחייבה משטרת ישראל לפרסם בתוך 45 יום תזכיר חוק בנושא הנדון בעתירה.

1.3. קשה להגיב לתזכיר החוק מבלי להתייחס לאירועים שקדמו לפרסומו: משבר הקורונה האיץ בעולם כולו, ובישראל בפרט, תהליכי דיגיטציה במגזר הציבורי. מיד עם פרוץ המשבר, מדינת ישראל החלה לבחון אמצעי איכון סלולריים לצורך התמודדות עם משבר הקורונה. במרץ 2020, הממשלה הסמיכה את השב"כ לאכן חולי קורונה לצורך איתור מגעים עם חולים; באפריל 2020, משטרת ישראל ביקשה לאכן את כל החייבים בבידוד כדי למנוע הפרות ובמקביל החלה להפעיל רחפנים לצורך אכיפת חובת הבידוד. בנובמבר 2020, המשטרה פרסמה מכרז למערכת שמנטרת בזמן אמת ורצוף את תנועת האזרחים, לצורך איתור ואכיפת התקהלויות שנערכו בניגוד לתקנות הקורונה; בדצמבר 2020 פעילי סייבר חשפו כי המשטרה מנטרת את תעבורת האינטרנט של גולשים ואתרים מסוימים; ביולי 2021 השר לביטחון הפנים ומשטרת ישראל החלו בהפעלת אמצעי אכיפה אלקטרוניים נגד מבודדים, ללא פרסום של אופן הפעלת הטכנולוגיה וסוגי המעקב שמשמשים לצורך האכיפה.

---

[1] פרטיות ישראל היא עמותה רשומה, הפועלת במטרה לשמור ולקדם את הזכות לפרטיות בישראל. עם מייסדי העמותה נמנים מיטב המומחים בארץ בתחום הפרטיות. העמותה פועלת בהיבטים מגוונים ובהם קידום מהלכים להתאמת החקיקה לאתגרי הפרטיות של המאה ה-21, נקיטת צעדים משפטיים לצורך שמירה והגנה על הזכות לפרטיות, עידוד וקידום יוזמות טכנולוגיות המקדמות שילוב של פרטיות וחדשנות (Privacy by Design ו-Privacy Enhancing Technologies) והגברת המודעות לחשיבות הזכות לפרטיות בקרב הציבור הרחב בכלל והצעירים בפרט.

1.4. מרצף האירועים הנ"ל אנו למדים על מטרה לא מוצהרת של תזכיר החוק: הגברת יכולות המודיעין האזרחי של המשטרה, לצורך שליטה והכוונת הסדר הציבורי. מערכות המעקב מציידות את המשטרה ביכולות טכנולוגיות מתקדמות שמשמשות היום את רשויות הביטחון לצורך פעולות סיכול ומניעת טרור (שב"כ, צה"ל וכיו"ב), ואילו כעת המשטרה מבקשת להשתמש במערכות אלו נגד כלל תושבי ישראל.

1.5. כבר בפתח הדברים נציין כי מנוסח התזכיר עולה כי הוא נועד בראש ובראשונה לעגן בדיעבד סמכות לפגיעות קשות בפרטיות שכבר נגרמו בפועל כתוצאה משימוש במערכת "עין הנץ" ומפרויקטים נוספים מבוססי מידע שהופעלו בשנה האחרונה על-ידי רשויות האכיפה, כמוזכר לעיל. התזכיר לא עורך הבחנה בין שימוש בזמן אמת לבין שימוש בדיעבד במידע שנצבר אגב השימוש במערכות המעקב, או בין שימוש שיש בו פגיעה קשה בזכות לפרטיות לבין שימוש שאין בו פגיעה (לדוגמה: איתור רכב גנוב). משכך, אנו סבורים כי התזכיר, כפי שפורסם, אינו בשל דיו ונעדר סעיפים רבים שנוגעים למורכבות בהפעלת מערכות מעקב מתקדמות, והמאגרים שנצברים אגב השימוש בהם.

1.6. **תזכיר החוק מעניק למשטרה סמכות רחבה לעשות שימוש בשלל אמצעי מעקב טכנולוגיים לצורך ניטור והתחקות אחר כלל תושבי ישראל בכל זמן נתון, ללא הבחנה בין שימוש מותר לבין שימור אסור, ובין מבצעי עבירה לעוברי אורח. התזכיר נעדר איזונים מהותיים, מנגנוני פיקוח, בקרה ותיעוד נאותים, וכן הסדרים ראייתיים בדבר ההסתמכות על מידע שמופק מתוך מערכת טכנולוגית.**

פרטיות ישראל מתנגדת לתזכיר החוק המוצע בשל הפגיעה הגורפת, המתמשכת והרחבה בזכויות החוקתיות של כלל תושבי ישראל, כפי שיורחב בהרחבה להלן בתגובתנו.

2. <u>הסיכונים הגלומים בתזכיר החוק</u>

2.1. <u>**הסמכה למעקב מתמיד ומתמשך**</u>. מערכות המעקב מאפשרות למשטרה לתעד, לנתח ולזכור את תנועתם היומיומית של מיליוני אנשים במרחב הציבורי, מבלי שהיו חשודים בביצוע עבירה. דרך כך, המשטרה יוצרת מאגר מידע אימתני שדרכו ניתן לשלוף בכל רגע נתון מידע רב על כל תושב בישראל (וגם על מי שאינו תושב). המידע שנאגר במערכות המעקב אינו מידע סטטי (לדוגמה: ישראל ישראלי עבר ברחוב סוקולוב בעיר רעננה בשעה 10:04), אלא מידע דינאמי שממנו ניתן להסיק מידע רגיש ואינטימי על אודות אורחות חייו של אדם: דפוסי התנהגות, דפוסי נהיגה, הרגלים ותחביבים, קשרים חברתיים ומשפחתיים, מצב הרפואי (הפיזי והנפשי), אמונתו של אדם, מצב כלכלי, נטיות מיניות ועוד - כל אלה יוצרים תמונת חיים אינטימית אודות כל אדם שנתפס בעיניה הבוחנת של מערכות המעקב של המשטרה.

לאחרונה, בית המשפט העליון התייחס, במסגרת הליך אזרחי, להיקף הפגיעה בפרטיות שעלולה להיגרם כתוצאה מחשיפת נתוני מיקום: "הפגיעה הטמונה בגילוי נתוני מיקום ללא הסכמתו של מושא האיכון, באה לידי ביטוי, בעיקרו של דבר, בעצם חשיפת תנועותיו של הפרט והיותן מושא לתשומת לבו של אדם אחר. זאת, אף אם אין הפרט מבקש לחסות נתון ספציפי זה או אחר מתוך נתונים אלה....כמו כן, מיקום עשויים ללמד רבות על אורחות חייו ומאפייניו של מושאם, כך שחשיפתם לזולת עשויה אף להסב לו נזקים של ממש במגוון תחומים" (רע"א 2404/21 **פלונית נ' פלוני**, השופטת וילנר בפס' 17 (22.7.21)).

2.2. <u>**הפעלת מערכות מעקב טכנולוגיות שקולה לאיסוף נתוני תקשורת ביומטריים**</u>. בדומה לאיכון סלולרי, שמאפשר לנטר היכן אדם שהה, כמה זמן, ועם מי, על-ידי איסוף אותות סלולאריים (טריאנגולציה) מחברות התקשורת. מערכות המעקב מאפשרות לפענח מידע דומה, ולעיתים אף מידע זהה, מצילום אנשים במרחב הציבורי: היכן אדם שוהה, מתי, לאורך כמה זמן, כמה פעמים

שהה שם בעבר, עם מי הוא שוהה במקום ועוד. הצילום אף עלול ללמד נדבך נוסף שלא קיים באיכון סלולרי והוא הנדבך הרגשי: ממערכות זיהוי פנים ניתן היום ללמוד על מצבו הרגשי של אדם ע"י ניתוח תווי הפנים ו/או שפת הגוף.

חוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת), תשס"ח-2007 (להלן: "**חוק נתוני תקשורת**") קובע כי רשויות חקירה רשאיות לקבל לידיהן נתוני תקשורת בצו שיפוטי, או ללא צו שיפוטי במקרים דחופים (הצלת חיים או מניעת עבירה מסוג פשע), לתקופה מוגבלת של עד 24 שעות. כבר שנחקק חוק נתוני תקשורת בשנת 2008, כינו אותו "חוק האח הגדול", בעקבות כך שהוא מעניק לרשויות החקירה בישראל לבלוש ולהתחקות אחר כל אדם בישראל, בחלק מהמקרים בצו שיפוטי במעמד צד אחד, ובמקרים אחרים בלא צו שיפוטי כלל.

כעת תזכיר החוק מייתר במידה רבה את הצורך בהשגת צווים לפי חוק נתוני תקשורת, ומאפשר חיפוש רחב היקף בנבכי חייו של כל אדם. כך לדוגמה, אם המשטרה מעוניינת להשיג מידע על מיקום של אדם, במקום לפעול להשגת צו שיפוטי (לפי ההסדר הקבוע בחוק נתוני תקשורת), תזכיר החוק מאפשר לה כעת להשתמש, ללא הגבלה או פיקוח, במערכת שמאפשרת לה לזהות את כל העוברים והשבים בתאי שטח מצולמים ברחבי ישראל, בכל נקודת זמן.

בשנת 2009, נחקק חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, תש"ע-2009 (להלן: "**החוק הביומטרי**"), המחייב כל אזרח למסור תמונות פנים (באיכות שמאפשרת הרכשה ביומטרית) לרשות האוכלוסין לצורך הנפקת תעודת זהות ו/או דרכון. החשש העיקרי מהחוק הביומטרי היה השימוש הנרחב שהמשטרה תעשה במאגר הביומטרי. באופן דומה לחוק נתוני תקשורת, גם באשר לחוק הביומטרי - מומחי פרטיות בארץ ובעולם הביעו חשש מפני חדירה לפרטיותם של אזרחים חפים מפשע: נציבת הגנת הפרטיות של מדינת אונטריו, קנדה, ד"ר אן קאווקיאן, מומחית בעלת שם עולמי באבטחת מידע ואמצעים טכנולוגיים להבטחת פרטיות, ציינה במכתב למועצה הציבורית להגנת הפרטיות, כי השימושים במאגר הביומטרי בישראל צפויים להתרחב עקב תופעת "שינוי ייעוד זוחל" (mission creep), והדבר עלול להוביל ליצירתה של "מדינת משטרה".[2]

תזכיר החוק בעניינו משלב ומעצים חששות, סיכונים ואתגרים שעלו בעקבות החוק הביומטרי וחוק נתוני תקשורת. בחסות התזכיר, המשטרה תפעיל ותנהל מאגר מידע בלתי מוגבל בהיקפו שמכיל נתוני מיקום ביומטריים של תושבי ישראל, ותוכל להצליב אותם עם מאגרי מידע נוספים (שאינם ידועים לציבור). אם בעבר סברנו כי אנחנו בפתחו של מדרון חלקלק אל עבר מדינת מעקב, תזכיר החוק מהווה כעת נקודת אל-חזור מדאיגה שמאפשרת למשטרת ישראל להתחקות אחר כל אדם בכל רגע נתון, בלא ביקורת שיפוטית, פרלמנטרית או מנהלית.

בית המשפט העליון התייחס לפגיעה הנרחבת בזכות לפרטיות ולתחושת המעקב שנגרמת עקב איסוף נתוני מיקום בבג"ץ שעסק בחוק נתוני תקשורת: "ברי, כי מעקב אחר אדם, גם אם הוא לצורך חקירה פלילית, יכול שיעלה פרטים אחרים, שידיעתם מהווה פגיעה בפרטיותו ובצנעת הפרט של האדם, כגון בעיות בריאותיות, הרגלי צריכה, העדפותיו המיניות, וכיוצא באלה. בכל אלה יש כדי לפגוע בפרטיות האדם מעצם היוודעם לאחר המקבל את הנתונים, ובוודאי יש בהם פוטנציאל לפגיעה בפרטיותו כאשר יכול שיעשה בהם שימוש לצרכי חקירה", ובהמשך: "**אין ספק כי לתחושת המעקב - הידיעה כי עיניהן של רשויות החקירה פקוחות ויכולות לבחון כל אדם בכל מקום ובכל שעה - השפעה "ממשמעת" על התנהלותו של האדם, גם במרחב הפרטי**" [ההדגשות

---

[2] "החוק הביומטרי – "מדרון חלקלק למדינת משטרה"", YNET 10.08.2009; "המאגר הביומטרי - מדרון חלקלק למדינת משטרה", LAW.CO.IL (11.08.2009)

נוספו] (בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל**, הנשיאה בינייש בפס' 7, 28.5.2012).

פרטיות ישראל סבורה כי אופן יישום החוק צריך להיות כפוף הן לביקורת שיפוטית והן לביקורת פרלמנטרית, בדומה לחוק נתוני תקשורת (ובפרט סעיפים 3 ו-14 לחוק נתוני תקשורת).

2.3. **<u>היעדר מנגנוני ריסון, פיקוח ובקרה</u>.** תזכיר החוק קובע באופן כללי מאוד מסגרת משפטית להצבה, הפעלה ושימוש מותר בטכנולוגיות מעקב מתקדמות. בניגוד לדברי חקיקה ברחבי העולם,[3] האוסרים על שימוש בטכנולוגיות זיהוי פנים, למעט במקרים חריגים ומוגבלים, תזכיר החוק קובע מסגרת רחבה להפעלה ולשימוש במערכות המעקב, ללא הגבלות מהותיות. רמז להגבלות המתוכננות מצוי בסעיף 10יב לתזכיר, שקובע כי השר לביטחון הפנים יתקין תקנות בנושאים הנוגעים לאיסוף המידע, הגישה אליו ואופן שמירתו. **נעלמת מעינינו הסיבה לכך שהיבטים מהותיים כגון: מגבלות על הצבת המצלמות והשימוש במידע, יוסדרו בחקיקה משנית, ולא בחקיקה ראשית.**

הנושאים שעתידים להיות מוסדרים בתקנות הם בבחינת מעט מדי. התזכיר אינו כולל הסדרי פיקוח ובקרה אפקטיביים על אופן יישום הוראות החוק, ובפרט על מנעד המקרים בהם ניתן להשתמש במערכות. סעיפים 10ג ו-10ו לתזכיר מונים שורה רחבה של מטרות לשמן ניתן להשתמש במערכות המעקב: החל במקרים בהם יש חשש לפגיעה ברכוש, עובר בחקירת דפוסי פשיעה ועד לגילוי עבירות מסוג עוון. הצידוקים לשימוש במערכות המעקב הם רחבים, ובפועל מאפשרים למשטרה להשתמש במערכות המעקב כמעט עבור כל מטרה, ללא התייחסות להיבטים חשובים נוספים, כגון:

א. סוגי העבירות בגינן ניתן להפעיל את מערכות המעקב;

ב. סוגי המידע שניתן לאסוף באמצעות מערכות המעקב;

ג. אופן תיעוד הגישה למידע שנאגר אגב השימוש במערכות המעקב;

ד. קביעת הרף הראייתי שמאפשר למשטרה להשתמש במערכות המעקב;

ה. קביעת אמות מידה לבחינת המשקל הראייתי של תוצרי מערכות המעקב, בהתחשב בהטיות הקיימות במערכות הטכנולוגיות;

ו. חובת יידוע בדבר אופן כיול מערכות המעקב, שיעור הדיוק שלהן והבקרות שהוטמעו לצורך מניעת התאמות שגויות;

ז. פירוט מדויק של פעולות החקירה שנוגעות לשימוש בפלט ממערכות המעקב (לדוגמה: הצילום שבו השתמשו לצורך תהליך הזיהוי);

ח. הענקת זכות ערעור על החלטות ו/או התאמות שהתקבלו ממערכות המעקב.

בנוסף, סעיף 3 לתוספת הרביעית (הוראת המעבר) קובע כי עד כניסת התקנות כאמור לתוקפן, תמשיך המשטרה לעשות שימוש במערכת LPR באופן בו נעשה שימוש במערכת המעקב עובר לקביעת התקנות. **משמעות הדבר כי התזכיר מבקש להכשיר בחקיקה שימוש בלתי חוקי שנעשה**

---

[3] ראו: (1) בקליפורניה נחקק חוק זמני שתוקפו עד ה-1.1.23 (AB-1215 Law enforcement: facial recognition and other (2019-2020).biometric surveillance); (2) במיין נחקק לאחרונה חוק האוסר שימוש בטכנולוגיית זיהוי פנים או טכנולוגיות מעקב אחרות, אלא במקרים מוגבלים (LD 1585; HP 1174 An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials); (3) בווירג'יניה נחקק חוק שאוסר על רשויות אכיפה חוק מקומיות לרכוש או להשתמש במערכות זיהוי פנים, אלא בחקיקה (VA HB2031 - Facial recognition technology; authorization of use by local law); (4) בערים בולטימור, סן פרנסיסקו, אוקלנד ועוד, נחקקו חוקים מקומיים דומים שאוסרים על השימוש בטכנולוגיות זיהוי פנים).

כיום (ובשנים האחרונות) במערכות לזיהוי לוחיות רישוי, ללא קביעת אמות מידה, איזונים, מנגנוני פיקוח ובקרה.

פרטיות ישראל סבורה כי על תזכיר החוק לכלול הגבלות מחמירות יותר על השימוש בטכנולוגיות מעקב וכן לקבוע מנגנוני פיקוח ובקרה הדוקים על השימוש (כפי שמתוארים להלן בפרק ההמלצות), כדי להבטיח שמירה על הזכות לפרטיות, הזכות להליך הוגן וחזקת החפות.

2.4. **<u>הסמכה בלתי מוגבלת לשימוש בטכנולוגיות מעקב מתקדמות</u>**. תזכיר החוק מבקש להסמיך את המשטרה לעשות שימוש <u>בכל</u> טכנולוגיה לעיבוד נתונים שבאפשרותה לזהות ולהתחקות אחר אדם, ואינו מצומצם "רק" למערכות לזיהוי פנים או לוחיות רישוי (LPR). נפרט: סעיף 10ב לתזכיר קובע כי ההרשאה להצבה, הפעלה ושימוש בטכנולוגיה מוגבלת לסוגי המערכות המפורטות בתוספת הרביעית. השר לביטחון הפנים, בהתייעצות עם שר המשפטים, רשאי לתקן את התוספת הרביעית מבלי להידרש לתיקון חקיקה, ואף מבלי לפרסם על כך הודעה ברשומות. דברי ההסבר מלמדים כי הוראה זו נועדה לצורך שמירה על חסיון האמצעים והמערכות, על אף שהיעדר פרסום ברשומות אינו מונע את פירוט המערכות בנוסח החוק, ובין כה ראוי כי אמצעי האכיפה של המשטרה יהיו גלויים וחשופים לציבור.

הוראה זו מהווה רובד נוסף של היעדר הבקרה והפיקוח על השימוש של המשטרה בטכנולוגיות מתקדמות. פוטנציאל השימוש שקיים בהגדרה של "מערכת צילום מיוחדות" רק הולך וגובר לאור הגידול במצלמות הפזורות ברחבי הארץ, השיפור הטכנולוגי ביכולת ניתוח וידאו והיכולת להעשיר את המידע על דרך הצלבה עם מאגרי מידע נוספים המצויים בידי המשטרה וגורמים נוספים. כך לדוגמה, לתוך הגדרה זו ניתן ליצוק בעתיד מערכות נוספות: מערכות בינה מלאכותית לניתוח נתונים המופקים מהמצלמות, מערכות שמאפשרות לפענח תנועת שפתיים, מערכות שיודעות לצלם או להתחבר למכשירי טלפון ועוד. מערכות אלו יוכלו להיכנס לשימוש אופרטיבי ומבצעי של המשטרה (ושל גופים ציבוריים נוספים), ללא הליך חקיקה וללא ביקורת ציבורית או פרלמנטרית.

2.5. **<u>העברת מידע לגופי ביטחון נוספים</u>**. לצד הקביעה כי מידע שנאגר ממערכות המעקב יהיה חסוי, תזכיר החוק קובע כי משטרת ישראל רשאית למסור מידע, ביומטרי או אחר, ממאגר מערכות המעקב לגופי ביטחון נוספים, כגון: אגף המודיעין בצה"ל, שב"ס, שב"כ ועוד. הוראה זו מרחיבה באופן בלתי מידתי את מורשי הגישה למידע, ללא פיקוח או הגבלה על השימוש במידע על-ידי אותם גופים. כך תזכיר החוק בורא מציאות שבה גופי ביטחון שאמונים על סיכול טרור, פעילויות מודיעין, ניהול ושמירה על בטחון אסירים, ובטחון חוץ-מדינתי – אוספים מידע ועוקבים אחר אזרחים חפים מפשע.

פרטיות ישראל סבורה כי הסדר העברת מידע ביומטרי רגיש בין גופים ציבוריים (ביטחוניים או שלא ביטחוניים), צריך להיות מוסדר בחקיקה ייעודית או בתקנות, ביחס לכל רשות שדרוש לה המידע לצורך מילוי תפקידה, ובהתאם לסמכויות המקנות לה בדין. בנוסף, לאור רגישות והיקף המידע במערכות המעקב, אנו סבורים כי העברת מידע ביומטרי על אודות אזרחים צריכה להתבצע בכפוף לאישור של ועדת הפנים והגנת הסביבה בכנסת, תוך בחינת הצדקת שיתוף המידע.

2.6. **<u>הצלבת מידע בין מאגרים</u>**. הצלבת מידע מתוך מערכות המעקב עם מאגרי מידע נוספים המצויים בידי המשטרה וגורמים נוספים מאפשרת להעשיר ולטייב את המידע, ודרך כך ליצור הקשרים שונים למידע ולהסיק אי אלו מסקנות אודות נושא המידע, בלא ידיעתו.

ראוי כי תזכיר החוק יקבע מסגרת משפטית בנוגע לסוגי מאגרי המידע שניתן להצליב מהם מידע, וכן הוראות בדבר זכאותו של מי שנפגע כתוצאה מהחלטה שתקבלה באמצעות מערכות המעקב,

לקבל פירוט של מאגרי המידע מולם הוצלב מידע על-ידי המשטרה. המטרה למנוע מצב שבו הגופים הציבוריים המנויים בתזכיר משתפים ביניהם מידע מודיעיני כדי לבנות פרופיל מידע על חשוד, ללא שיש בידו את הכלים והיכולת להבין את החשדות ו/או האישום נגדו.

2.7. **<u>סיכון ביצירת עותקי מידע אגב השימוש במאגר מערכות המעקב.</u>** ישנם כיום מאות מאגרי מידע ציבוריים שכוללים מידע אישי רב על אודות אזרחים, כאשר מתוכם ישנו מספר בלתי ידוע של מאגרי מידע שמכילים מידע ביומטרי (טביעות אצבע, דגימות קול ותמונות פנים).

דו"ח מבקר המדינה בנושא מאגרים ביומטריים[4] הצביע על ליקויים באופן ניהול מאגר התמונות במשרד התחבורה. אחד הליקויים המרכזיים בדו"ח המבקר הוא השימוש התדיר במאגר רישיונות הנהיגה במשרד התחבורה על-ידי שלל גופים, בהם משטרת ישראל, בדרך של הסדר עוקף החוק הביומטרי.

נסביר: החוק הביומטרי מאפשר למשטרה לקבל תוצאות זיהוי ביומטרי או מידע ביומטרי בצו שיפוטי. על מנת לקבל מידע מהמאגר שלא על-ידי צו, נדרש להתקין תקנות. משנחקק החוק ועד לעצם היום הזה, המדינה לא התקינה תקנות שהקנו למשטרה גישה למידע מהמאגר הביומטרי. כאשר קוראים את דו"ח המבקר, ניתן להבין מדוע – למשטרה יש עותק של מאגר רישיונות הנהיגה, שמתעדכן ברמה יומיומית, שמכיל תמונות באיכות שמאפשרת הרכשה ביומטרית. כלומר, העברת המידע בין רשויות שונות ומשרדי הממשלה מתוקף תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986, מאפשרת למשטרה לקבל מידע עשיר ורב על אודות אזרחי ישראל, ולעיתים אף בלא להידרש להשגת צו שיפוטי (כפי שמחויב בחוק נתוני תקשורת ובחוק הביומטרי).

מכאן ללמדנו שרשויות המדינה מיומנות היטב ביצירת מאגרי מידע רגישים, אך לעיתים שוכחים (במכוון או בשוגג), את הצורך לפקח, לבקר ולנהל את מאגרי המידע, בהתאם להוראות החוק.

מיצירת מאגר ביומטרי נוסף במשטרת ישראל, עולה סיכון כפול: המשטרה תקבל לידיה מידע ממאגרי מידע ציבוריים רבים (לצורך העשרת המידע), ומהצד השני תמסור מידע לגופים ציבוריים אחרים (כמפורט לעיל), וכך ייווצרו עותקים של מאגרי מידע רגישים (ובחלקם ביומטריים), באופן שיקשה לעקוב ולפקח אחר הנעשה בהם.

2.8. **<u>אבטחת מידע.</u>** מאגר ביומטרי הוא מאגר רגיש מטיבו (ראו בהמשך); דו"ח המבקר הגדיר את מאגר רישיונות הנהיגה במשרד התחבורה כבעל רמת סיכון גבוהה, בעקבות המידע הביומטרי שניתן לחלץ ממנו. המאגר שמשטרת ישראל מבקשת ליצור, בחסות תזכיר החוק, יהיה אחד מהמאגרים הרגישים (אם לא הרגיש ביותר) במדינת ישראל. מעבר לסיכוני הפרטיות שנגזרים מניהול מאגר כזה, ישנם סיכונים ביטחוניים רבים.

מאגר כזה עלול להפוך למטרה אטרקטיבית עבור מי שמבקש לפגוע במדינת ישראל. מתקפת סייבר אחת יכולה לפתוח עבור גורמים זרים פתח למעקב אחר שיירת ראש הממשלה בכל רגע נתון, ארגוני פשיעה ישמחו לקבל מן המאגר מידע מפורט אודות יעדיהם, והסיכונים עוד רבים. תזכיר החוק צריך לכלול הסדרים מחמירים לאבטחת המידע במאגר, ובעיקר בכל הנוגע לשלל ההיבטים המוזכרים בתגובתנו להלן: הגבלת גישה למידע, הגבלת העברת המידע ויצירת עותקים שלו ומחיקת המידע באופן תדיר.

2.9. **<u>היעדר שקיפות.</u>** המשטרה היא גוף אכיפה אזרחי שמטרתו להעמיד עבריינים לדין, ככזו פעילותה לא יכולה לחסות תחת חשאיות מוחלטת ועליה לפעול בשקיפות במקומות ההכרחיים והנדרשים. אמון הציבור בפעולות של רשויות המדינה בכלל ומשטרת ישראל בפרט הולך ונשחק, ומתרבים

[4] מבקר המדינה, היבטים בהסדרת השימוש במאגרים ביומטריים (2020) (להלן: "**דוח המבקר**").

החששות מפגיעה במרקם החיים הדמוקרטיים, בייחוד לאור הפעלה של מערכות מעקב חודרניות כמו המערכות נשוא התזכיר. על כן, בכל הנוגע למערכות מעקב אזרחיות - על המשטרה חלה חובה מוגברת לנהוג בשקיפות ותוך כבוד לפרטיותם של האזרחים. לא רק על-ידי הצבת שילוט בנוגע למיקום המצלמות, אלא גם על-ידי פרסום של מפת המצלמות שמשמשות את המשטרה; איסור על הצבת מצלמות חשאיות (אלא לתקופה מוגבלת, ובצו שופט); ומתן זכות עיון במידע לאדם שנפגע כתוצאה משימוש במערכות המעקב.

באופן רחב יותר, ישנה חשיבות מכרעת להגברת השקיפות באשר לאופן השימוש במערכות מעקב אוטומטיות שאוספות מידע נרחב על כלל האוכלוסייה. באמצעות הגברת חובות השקיפות, ניתן למנוע מראש שימוש חורג, בלתי מידתי ופוגעני במערכות המעקב.

3. <u>מסגרת נורמטיבית</u>

3.1. הזכות לפרטיות היא זכות יסוד חוקתית בשיטה המשפטית בישראל. היא מעוגנת בסעיף 7 לחוק-יסוד: כבוד האדם וחירותו ולפיכך היא בעלת מעמד חוקתי על-חוקי. בית המשפט העליון הגדירה "אחת החירויות המעצבות את אופיו של המשטר בישראל כמשטר דמוקרטי" (בג"ץ 2109/20, 2135/20, 2141/20, 2187/20 **בן מאיר ואח' נ' ראש הממשלה ואח'** (26.4.2020)) ונאמר עליה שהיא "מן החשובות שבזכויות" (ע"א 1697/11 **א. גוטסמן אדריכלות בע"מ ואח' נ' ורדי** (23.1.2013)). היקפה של הזכות החוקתית לפרטיות נקבע על פי פרשנות תכליתית של סעיף 7 בחוק-יסוד: כבוד האדם וחירותו (בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי בנתניה**, פ"ד סא(1) 581 (2006)). חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") מסדיר באופן פרטני את ההגנה על הזכות לפרטיות ואת המסגרת המשפטית לאיסוף ושימוש במידע אישי. החוק חל גם על המדינה (סעיף 24 לחוק הגנת הפרטיות). לצדו, מוגנת הזכות בחקיקה פרטיקולרית, כדוגמת חוק זכויות החולה, תשנ"ו-1996.

3.2. נתוני מיקום ומידע ביומטרי מוגדרים בחקיקה כמידע רגיש במיוחד שמקים חובות הגנת פרטיות ואבטחת מידע מוגברים (ראו: תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 שלפיהן מידע ביומטרי ומידע בדבר מיקום מגבירים את רמת אבטחת המידע הנדרשת ממאגר וכן את תזכיר חוק הגנת הפרטיות (תיקון מס') (הגדרות וצמצום חובת הרישום), התש"ף -2020 שלפיו מידע ביומטרי ונתוני מיקום מוגדרים כ"בעל רגישות מיוחדת").

4. <u>מערכת זיהוי לוחיות רישוי (LPR) - סקירה</u>

4.1. מערכת זיהוי לוחיות רישוי (LPR) (בפרק זה: "**המערכת**" או "**מערכת LPR**") קוראת באופן אוטומטי את לוחיות הרישוי של הרכבים שעוברים על פני המצלמות הפרושות ברחבי הארץ ומשווה את מספרי הלוחיות שפוענחו. על הטכנולוגיה ועל השימושים השונים בה על ניתן ללמוד ממכרז המשטרה לאספקת מערכת LPR. כך לדוגמה תוארה הטכנולוגיה הדרושה במסמכי מכרז המשטרה: "טכנולוגיות עיבוד תמונה מתקדמות המאתרות, עוקבות, מצלמות ומזהות לוחיות רישוי של כלי רכב בזמן אמת, הפועלות 24/7 בכל ימות השנה במשימות רבות" (משטרת ישראל, מכרז לאספקת מערכת LPR (מס' 35/2012), סעיף 1.2 עמ' 24 (17.10.2012) להלן: "**מכרז המשטרה**").

4.2. למערכת LPR שני שימושים עיקריים – האחד, יצירת התרעות בזמן אמת של כלי רכב ונהגים "מבוקשים" והשני, יצירת מאגר מידע על תנועת כלי רכב שהמערכת זיהתה, לרבות מיקום ומועד שבו עברו, לשם התחקות, תיעוד ומעקב בעתיד.

4.3. מערכת LPR מסוגלת לאתר ולזהות, באופן אוטומטי ובזמן אמת, רבבות כלי רכב ביום (סעיף 1.4.1.4 למכרז המשטרה). כל אימת שיש התאמה בין לוחית הרישוי שנקראה במערכת לבין זו

שמופיעה ברשימת ה"מבוקשים", המערכת תציג לשוטר בשטח את המידע לצורך עיכוב נהג הרכב. מערכת LPR נמצאת כיום בשימוש של יחידות שונות במשטרה, לרבות, אגף התנועה, סיירי אגף המבצעים, שוטרי מג"ב, יחידות אח"ם ואג"ם ייעודיות (עמ' 25 למכרז המשטרה).

4.4. רשימות המבוקשים אינן כוללות רק כלי הרכב (רכב גנוב, ללא רישוי וכו') אלא גם בעלי הרכב. כך, המכרז מונה בין "משימות" המערכת – "איתור רכב עברינ/מבוקשי פשע, או מבוקשים על רקע בטחוני, או ע"י יחידה מסוימת" (סעיף 1.2 למכרז, עמ' 24) וכן "איתור רכבים שבעליהם העבריינים דרושים לחקירה ו/או צריכים להיות מובאים לדין, נהגים מורדים מהכביש שממשיכים לנהוג, עברייני תנועה כבדים..." (סעיף 1.8 למכרז, עמ' 26). ההתרעות נוגעות אף למקרים שבהם "כלי רכב הקשורים לעבריינים מבוקשים... או מבוקשים על רקע בטחוני" (סעיף 2 למכרז, עמ' 27).

4.5. המידע באשר לרבבות הנהגים שחולפים מדי יום על פני מצלמות "עין הנץ", בין אם מדובר ברכב "מבוקש" ובין אם לאו, נאגר בידי המשטרה לצורך שימוש מאוחר. מידע זה כולל: מספר לוחית הרישוי, צילומי וידאו וסטילס, לרבות תמונת הרכב והנוסעים בתוכו וכן תמונות ממוקדות של לוחית הרישוי, שעליהן מוטבעים מועד הצילום ומיקום מדויק של המצלמה (ליאור אילן, חוות דעת מומחה – מערכת 'עין הנץ', 6.11.2019).

4.6. משמעות הדבר כי שילוב בין מערכת לזיהוי פנים לבין מערכת LPR, יעניק רובד נוסף של מידע והוא תנועת הנוסעים ברכב, ולא רק תיעוד של בעל הרכב (במערכת LPR) או תנועת הולכי רגל ברחובות ובמתחמים ציבוריים (במערכת לזיהוי פנים).

4.7. מעיון בפרוטוקולים של דיונים פליליים שבהם הובאו ראיות ממערכת "עין הנץ" עולה, כי השימוש במערכת נעשה באופן **שגרתי** ולא מבוקר על ידי חוקרים ובוחני תנועה **בתיקי חקירה מסוגים שונים**: גניבת רכבים, פשעים חמורים, תאונות דרכים ועוד.

4.8. בפועל, הגישה למידע על תנועות של כלי-רכב במערכת "עין הנץ" נעשית ללא הגבלה או בקרה, כך שלמעשה לכל שוטר או חוקר, שמעורבים בתיקי חקירה, יש גישה למידע בדבר תנועתם היומיומית של מאות אלפי אזרחים במדינת ישראל. המידע מהמערכת מסייע לקביעת המיקום של חשודים ונאשמים בזמנים שונים בעבר **בדומה לאיכון טלפון נייד שמבוצע בהתאם לחוק נתוני תקשורת.**

4.9. **תזכיר החוק אינו נותן מענה למרבית הסיכונים שעולים משימוש המשטרה במערכת LPR, כפי שהוזכרו ותוארו בהרחבה בעתירה. היעדר ההגבלות על השימוש במערכת, בצירוף סעיף 3 לתוספת הרביעית לתזכיר, ממחישים כי תזכיר החוק נועד בעיקר להכשיר בדיעבד את הפגיעה בפרטיות, ולאפשר למשטרה להמשיך לעשות שימוש נרחב ובלתי מוגבל במערכת.**

5. <u>מערכת זיהוי פנים - סקירה</u>[5]

5.1. זיהוי פנים היא שיטה לזיהוי או אימות זהותו של אדם באופן ייחודי וחד-חד ערכי. מערכות זיהוי פנים יכולות להשתמש בתמונה, וידאו או צילום בזמן אמת של אדם, כדי לפענח את זהותו. טכנולוגית זיהוי פנים היא ענף בתחום הטכנולוגיה הביומטרית, שמאפשרת לזהות ולמדוד אדם לפי מאפיינים ביולוגיים מולדים או מאפיינים התנהגותיים כגון: טביעת אצבע, פנים, קשתית, קול או סגנון הליכה.

5.2. טכנולוגית זיהוי פנים מפענחת תמונה של אדם ויוצקת ממנה תבנית (face template) שמכילה את המאפיינים הייחודיים שלו. התבנית היא למעשה ייצוג מתמטי של התמונה ויכולה לכלול לדוגמה: את המרחק בין העיניים, הצורה של הסנטר ועוד. כך, אלגוריתם יכול להשוות בין התבנית שנשמרה לבין תמונה של אדם, ולחשב את הדמיון בין שני הייצוגים הגרפיים. בניגוד לאמצעים ביומטריים

[5] פרק זה נכתב בסיוע הרב ובאדיבות ד"ר יאיר דוד; העמותה מבקשת להודות לד"ר יאיר דוד על הסיוע והעזרה באיסוף המידע, ריכוזו וכתיבתו.

אחרים כמו טביעת אצבע ו-DNA, שאינם משתנים במהלך חייו של אדם, מערכת זיהוי פנים צריכה לחשב פרמטרים נוספים, כגון: הזדקנות, ניתוחים פלסטיים, קוסמטיקה, תאורה וזווית הצילום.

5.3. **<u>כיצד מערכת לזיהוי פנים עובדת?</u>**

1. צילום אדם – בווידאו או בתמונה;
2. המערכת מעבדת את הצילום ומאתרת מאפיינים ייחודים של המצולם;
3. מתוך המאפיינים שחולצו, המערכת מקודדת תבנית שמכילה את המאפיינים שחולצו;
4. לבסוף המערכת עורכת השוואה של התבנית אל מול התמונה או התמונות שמצויות במאגר המידע, בשיטה של אימות או של זיהוי:

4.1. **אימות זהות (verification).** בשיטה זו המערכת מבקשת לאמת את הזהות של אדם על-ידי השוואה של תווי הפנים של מי שטוען לזהות, לבין התבנית שקיימת במאגר של בעל הזהות (one-to-one matching). דוגמה לכך היא זיהוי פנים בטלפון הנייד – המצלמה בטלפון מצלמת את תווי הפנים של מי שמנסה לגשת לטלפון, ומשווה את המאפיינים שחולצו מהצילום לתבנית הפנים השמורה במכשיר. באופן זה מתבצע אימות שבעל המכשיר הוא הבן אדם שמנסה לקבל גישה לטלפון.

4.2. **זיהוי (Identification).** בשיטה זו המערכת מחפשת התאמה בין תווי פנים של אדם לבין התבניות הקיימות בתוך מאגר (one-to-many matching). החיפוש נועד לזהות התאמה או התאמה פוטנציאלית בין האדם שאת זהותו מבקשים לדעת לבין רשימת בעלי הזהות במאגר. דוגמה לכך היא שימוש בתמונה של אדם לא מזוהה מזירת פשע, לצורך זיהויו.

5.4. מרשימת המטרות שמנויה בסעיפים 10ג ו-10ו לתזכיר, אנו למדים כי הפונקציונאליות הנדרשת למשטרת ישראל ולגופים הציבוריים עוסקת יותר בזיהוי מאשר באימות. משכך, ישנה חשיבות לתמונה הנדגמת באמצעות מערכות המעקב, לתמונה במאגרי המידע שקיימים במשטרה, וכמובן ליכולת ההתאמה בין שתי התמונות.

5.5. יכולת הזיהוי של המערכת תלויה במידה רבה באיכות התמונה ובתאימות של תמונת המצולם לתמונה במאגר המידע. ככל שאיכות הצילום נמוכה יותר או שהאדם עבר שינויים חיצוניים מהותיים – כך הדיוק בהתאמה עלול להיפגע. נוסף על כך, נמצא שהטכנולוגיה מייצרת לעתים קרובות מדי תוצאות המדגימות כי קיימת הטיה ברורה על סמך מאפיינים אתניים, גזעיים, מגדריים ואנושיים אחרים שמזוהים על ידי מערכות מחשב.[6] ההשלכות של הטיה כזו, יכולות לגרום לפגיעה עמוקה, במיוחד בחייהם, פרנסתם וזכויותיהם הבסיסיות של אנשים בקבוצות דמוגרפיות ספציפיות.

5.6. עם זאת, מאז שנות השמונים ועד היום השתפרו ביצועי מערכות הראיה הממוחשבות בזכות ההתפתחויות בתחומי החומרה ובתחומי התוכנה. מזעור חומרות המחשב מוכרות לכל במיוחד בזכות מכשירי כף היד. בתחום התוכנה ההתפתחויות המהותיות הן בשימוש בלמידת מכונה, ברשתות נוירונים, (שניתן ליישמן הן בחומרה והן בתוכנה), ובלמידה עמוקה, (Machin Learning, Neural networks, and Deep Neural networks).

5.7. תרומה חשובה מאוד לשיפור היכולת נעוצה בכמות המידע הזמין המשמש ללימוד המכונה שגדלה מאוד בזכות הרשתות החברתיות, השימוש הרב במצלמות הדיגיטליות במכשירים הניידים ובהגדלת יכולות הזיכרון של המחשבים הזעירים. ייתכן והתרומה המכרעת נובעת מפיתוח

[6] NISTIR 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (December 2019).

אלגוריתמים יעילים ללימוד הרשת וליכולת החישוב הגדולה הנדרשת, דבר שהביא לפריצת הדרך של השנים האחרונות.

5.8. דוגמה להתפתחות המואצת בתחום ניתן לראות בדו"ח מס' 11 של הממונה על היישומים הביומטריים (להלן: "**הדו"ח**").[7] הדו"ח התריע על כך שבעקבות שיפור משמעותי באלגוריתמיקה לזיהוי פנים, תמונות פנים באיכות מופחתת, שמוחזקות ברשות האוכלוסין בהתאם לסעיף 27 לחוק הביומטרי, יכולות לשמש לאימות ולזיהוי של אדם באופן ממוחשב. כלומר, ההתפתחות הטכנולוגית שהתרחשה בעשור האחרון, יצרה דה פקטו מאגר ביומטרי נוסף ולא חוקי מתמונות באיכות נמוכה.

5.9. מכאן, כי השילוב של מצלמות וידאו בתפוצה רחבה במרחב הציבורי עם מאגרי מידע ענקיים של תמונות פנים, החל מתמונות שהועלו לרשתות חברתיות, תמונות הנאספות בכניסות למרחבים כגון שדות תעופה, וכלה בתמונות שמקורן בתעודות זהות, דרכונים, רישיונות נהיגה וכיו"ב, מאפשרות לזהות בקלות אנשים ולעקוב אחר מקומות הימצאם ועל מפגשים חברתיים שהם מקיימים. כל זאת כאשר הזיהוי והצלבת המידע נעשים בחשאי ומבלי שניתנה הסכמת האנשים לכך.

5.10. ישנן אף מערכות המסוגלות לבצע זיהוי ואימות של אנשים גם כאשר התמונה חשוכה, והמצולם צולם בזוויות שבהן לא רואים באופן מלא את תווי הפנים (כמו לדוגמה כאשר אדם מצולם מגבוה). כשמדובר בטעויות בזיהוי, ישנם 2 מונחים חשובים:

- **False Negative ("זיהוי שלילי כוזב")** – כאשר המערכת לא מצליחה לזהות פנים של אדם מתוך המאגר או מול תמונה ספציפית. כלומר, המערכת לא תציג אף התאמה לתמונת הפנים, ולא יתרחש זיהוי או אימות של האדם על אף שתמונת האדם מצויה ביד הבודק.
- **False Positive ("זיהוי חיובי כוזב")** – כאשר המערכת מוצאת התאמה בין תמונה של אדם לבין תבנית במאגר, אבל ההתאמה שגויה ולא מדובר באותו אדם. כלומר, המערכת העלתה תמונה של "אלון", וזיהתה או אימתה אותו כ"שחר".

5.11. כאשר בוחנים שימוש במערכת זיהוי פנים על-ידי רשויות אכיפה, אחד הפרמטרים החשובים ביותר הוא שיעור הזיהוי החיובי הכוזב, כדי לקבוע את עלות הסיכון של השימוש במערכת עבור המטרה שלשמה משתמשים בה. **אם התוצאה של זיהוי חיובי כוזב היא מעצר או חיפוש של אדם חף מפשע בעקבות טעות בזיהוי של המערכת, עלות הסיכון היא גבוהה ביותר, ועל כן יש לדאוג כי סוג המערכת בה ייעשה שימוש תהא מהימנה, וכן שכיול המערכת ייעשה באופן שיבטיח שיעור אפסי של טעויות מסוג אלו (גם במחיר של יכולת זיהוי נמוכה יותר).**

5.12. כבר כיום ישנן יכולות טכנולוגיות למעקב מטריד, וככל שיכולות אלו ילכו וישתפרו, ייוצר מצב בו מי שישלוט בטכנולוגיה ובמערכות יוכל בלחיצת כפתור לקבל את שמות כל המשתתפים בעצרת בכיכר או בהפגנה ברחובות, באם פני המשתתפים נמצאים במאגר שברשותו או במאגר שיש לו גישה תקשורתית אליו. לא רק זאת, ניתן יהיה להעשיר את המידע ולשייך לדוגמה את המשתתפים לקבוצות, מי עמד ליד מי, מי שוחח עם מי.

5.13. יתרה מכך, במחקר שבוצע באוניברסיטת סטנפורד ופורסם בכתב העת Nature נטען כי טכנולוגיית זיהוי פנים יכולה לחשוף את הנטייה הפוליטית של אנשים, בהתבסס על כך שלפניהם של אנשים ליברלים ואנשים שמרנים יש מאפיינים שונים. במחקר הוחל אלגוריתם לזיהוי פנים על יותר ממיליון תמונות פנים של אנשים שנטיותיהם ידועות, שהושוו לתמונות פנים של אנשים אחרים שידוע היה שהם ליברליים או שהם שמרניים. בכשלושת רבעי מקרים האלגוריתם זיהה נכון את

[7] היחידה להזדהות וליישומים ביומטריים, דוח מס' 11 של הממונה על היישומים הביומטריים - יוני 2021, (21.6.21)

הנטייה הפוליטית.[8] מחקרים מסוג זה מחזקים את החשש כי זיהוי פנים אוטונומי בשילוב יישומי בינה מלאכותית יכול, או **בעיקר עשוי להתיימר**, לסווג ולתייג אנשים לפי מאפיינים סובייקטיביים ואינטימיים כגון: יושר, רמת אינטליגנציה, דעה פוליטית, נטייה מינית, ונטייה לאלימות.

5.14. הסתמכות על מערכת זיהוי פנים אוטונומית, ללא שנעשית בקרת זיהוי אנושית, עשויה להביא את המשטרה לביצוע פעולות אכיפה נגד חפים מפשע. דוגמה לכך התרחשה בחודש דצמבר 2020 כאשר אדם בשם Nijeer Parks, שהוא אזרח אמריקני ממוצא אפרו-אמריקאי, תבע בתביעה אזרחית את משטרת וודבריג׳ בטענה שהוא נעצר למשך עשרה ימים כתוצאה מהסתמכות על זיהוי פנים שגוי ובלתי חוקי שנעשה באמצעות מערכת אוטונומית לזיהוי פנים. מקרים דומים למקרה של ניג׳ייר הולכים ומתרבים במקומות שבהם אין הגבלה על השימוש במערכות לזיהוי פנים.

6. <u>המלצות</u>

תזכיר החוק בנוסחו הנוכחו אינו עומד במבחני המידתיות, היות שהוא מבקש להכשיר מצב שבו כמעט כל יציאה של אדם למרחב הציבורי מייצרת למשטרה באופן אוטומטי שובל של מידע בלתי מוגבל לצרכים עתידיים ולא ידועים. התזכיר לא כולל מנגנונים מרסנים שמבטיחים כי הפגיעה בפרטיות תצומצם למינימום הנדרש, ולא הוטמעו בו מנגנוני בקרה שיפוטית, פרלמנטרית או מנהלית שיבטיחו כי לא ייעשה שימוש חורג במערכות המעקב.

להלן השינויים המהותיים שאנו סבורים שיש להטמיע בתזכיר החוק על מנת ליצור הסדר מידתי וראוי:

6.1. **איסור פוזיטיבי על שימוש במערכות מעקב, למעט חריגים.** דברי חקיקה במדינות וערים שונות בעולם קובעות איסור על שימוש בטכנולוגיות מעקב של זיהוי פנים, למעט במקרים חריגים, מוגבלים ומוגדרים מראש. אנו סבורים כי החוק בישראל צריך ליישר קו עם המקובל בעולם בנושא זה, ולקבוע איסור פוזיטיבי על השימוש בטכנולוגיות מעקב במרחב הציבורי, תוך ציון רשימה סגורה של מקרים חריגים בהם דרוש השימוש במערכות המעקב באופן מידתי, מבוקר ומוגבל.

6.2. **הסדרה נפרדת עבור טכנולוגיות מעקב שונות.** טכנולוגיות מעקב שונות פוגעות ומשפיעות על זכויות הפרט באופן שונה. דין מערכת לזיהוי לוחיות רישוי אינו כדין מערכת לזיהוי פנים: מערכת לזיהוי לוחיות רישוי לא פוגעת *בכל מקרה* בפרטיותו של אדם, ואילו טכנולוגיה לזיהוי פנים לא מאפשרת חדירה לסוד שיחו של אדם כפי שמערכת לפענוח שפת גוף ומילים עלולה לפגוע. על כן, אנו סבורים כי הסדרה של מערכת לזיהוי לוחיות רישוי צריכה להיות נפרדת להסדרה של מערכת לזיהוי פנים, ושל מערכות טכנולוגיות עתידות.

6.3. **הבחנה בין סוגים שונים של שימושים במערכות המעקב.** קיים הבדל יסודי בין צילום, ניטור והצלבת מידע בזמן אמת כאשר קיימת עילה למעקב, לבין איגום, ניטור והצלבת מידע בדיעבד לשימושים עתידיים ובלתי ידועים. כך לדוגמה: ניטור מרחב ציבורי במהלך אירועי אלימות אינו שקול לניטור מרחב ציבורי במהלך שגרה; ובדומה, ניטור כבישים שמועדים לעבירות או מצויים בסמוך למחסומים משטרתיים אינו דומה לניטור תנועת רכבים ברחובות הערים. התזכיר קובע תקופות זמן ארוכות למדיי (שלוש שנים) באשר לבחינה מחודשת של הצבת מצלמות במרחב הציבורי, בפרט ביחס למצלמות ניידות (דוגמת רחפנים). אנו סבורים כי יש לערוך הבחנה קפדנית ביחס לעבירות שניתן לאכוף באמצעות מערכות המעקב, הנסיבות שבהן ניתן יהיה לעשות זאת, וכן לקבוע הסדרים פרטניים ומוגבלים בפרקי זמן ותאי שטח המצולמים.

---

[8] Michal Konsinski, Facial recognition technology can expose political orientation from naturalistic facial images 11.01.2021,

6.4. **שימוש במערכת בכפוף לצו שיפוטי.** בדומה להסדר הקיים בחוק הביומטרי ובחוק נתוני תקשורת, אנו סבורים כי ראוי שהפעלה ושימוש במערכות המעקב ייעשה בצו בית משפט, כאשר קיימת עילה סבירה וביקורת שיפוטית להפעלה של המערכות. בנוסף, ולאור הרגישות הרבה בשימוש במערכות לזיהוי פנים, אנו סבורים כי כל חיפוש או מעצר של אדם צריך להתבסס על ראיות מצטברות, ולא להתבסס אך ורק על ראיות שהופקו ממערכות המעקב. זאת כדי למנוע מצב שבו בני אדם יועמדו לדין רק על סמך החלטה של מערכת טכנולוגית.

6.5. **קביעת אמות מידה להיבטי איסוף, שמירה ומחיקת המידע.** כפי שתואר בהרחבה לעיל, ניתן להעשיר מידע ממערכות המעקב על-ידי הצלבתו עם מאגרים נוספים, ודרך כך ניתן לחדור להיבטים האינטימיים ביותר בחייו של אדם. על כן, ראוי כי תזכיר החוק יקבע אמות מידה ברורות באשר לסוגי המידע שניתן להפיק ממערכות המעקב, או לחילופין, סוגי מידע שלא ניתן להפיק באמצעותן, אלא לאחר תהליך בחינה, בקרה ואישור (לדוגמה: דעות פוליטיות, אמונות דתיות, נטייה מינית – אלו סוגי מידע שהפקה שלהם מתוך מערכות המעקב מהווה סיכון משמעותי לפרט, ובהיבט רחב יותר – אין לאפשר איסוף מידע זה במדינה דמוקרטית).

בנוסף, יש לקבוע בחקיקה ראשית (ולא בתקנות), את דרכי שמירת המידע והגישה אליו על-ידי הגורמים השונים, בכלל זה יש להגביל העברת המידע בין גופים ציבוריים שונים. לבסוף, יש להגדיר בחקיקה את משך שמירת המידע ומחיקתו, בהתייחס לסוג המצלמה, מיקומה, והסיבה לשמה הוצבה. יודגש בהקשר זה כי תהליך מחיקה של מידע הוא תהליך מורכב שיש להיערך לו מראש. לראיה – המדינה החליטה על מחיקת מאגר רישיונות הנהיגה במשרד התחבורה, אך נכון לזמן כתיבת תגובתנו המאגר טרם נמחק. יתרה על כך, גם אם המאגר יימחק, כיצד מבטיחה המדינה כי גם עותקי המאגר הרבים יימחקו?

קביעת אמות המידה בעניין שמירת המידע על אזרחים שאינם חשודים בביצוע עבירה, קשורה במישרין להסדרה של סוגי השימושים השונים (כמפורט בסעיף 6.3), ולהבחנה בין שימוש בזמן אמת במידע לבין שימוש בדיעבד.

6.6. **קביעת אמות מידה לבחינת מהימנות המידע.** כפי שצוין לעיל, קיימות הטיות מבניות בטכנולוגיה לזיהוי פנים. לפיכך תזכיר החוק צריך לקבוע אמות מידה לבחינת מהימנות המידע, שכוללות (א) כיול המערכת באופן שתבטיח שיעור אפסי של False Positives; (ב) ביקורת תקופתית של מהימנות ואמינות מערכות המעקב על-ידי מומחים מקצועיים, ו-(ג) קביעת נוהל משטרתי בדבר אופן הפעלת המערכות, כדי למנוע מצב שבו מנסים לזהות אדם מתוך תמונה באיכות נמוכה (לדוגמה: זיהוי אדם על בסיס קלסתרון). בנוסף, כדי להבטיח מהימנות גבוהה יותר, יש לקבוע כי לא תתקבל החלטת אכיפה בנוגע לאדם, רק על בסיס פלט או תוצר של מערכות מעקב בלי בקרה אנושית.

6.7. **מנגנוני תיעוד ובקרה.** ישנם מקרים רבים של כשל אנושי בטיפול במידע רגיש. לעיתים הכשל מקורו בכוונת זדון ולעיתים נעשה בשוגג. עם זאת, קשה מאוד למנוע באופן מוחלט והרמטי כשל אנושי בשימוש במידע. על כן, יש להבטיח כי הגישה למידע והשימוש במערכות המעקב יהיה מתועד באופן שיזהה את בעל הגישה, מועד הגישה, סוג הפעולה שבוצעה, מאגרי המידע שבוצע בהם החיפוש, העבירה בגינה בוצע החיפוש ופירוט הראיות שמצדיקות את הפעלת המערכת. בנוסף, יש להבטיח כי כל שרשרת המידע שמובילה לחשוד תתועד באופן מדויק ומפורט, כדי למנוע טעויות בזיהוי שמקורן בעיבוד מידע אוטומטי.

6.8. **שקיפות וזכות ערעור.** תזכיר החוק בנוסחו הנוכחי ממחיש ביתר שאת את מעטה החשאיות והסודיות שאופף את השימוש של המשטרה במערכות מעקב מתקדמות. על המשטרה, כגוף אכיפה אזרחי, להנגיש ולפרסם את אופן הפעולה של מערכות המעקב, בכל מקום שניתן ואינו פוגע ביכולת

ההרתעה והבטחון, במטרה להגביר את אמון הציבור במערכות אלו, ולהבטיח כי לא נעשה בהם שימושים חורגים ובלתי מידתיים.

בנוסף, המשטרה צפויה להשתמש בתוצרים מהמערכת במסגרת הליכים פליליים (כפי שנעשה עד כה עם תוצרים ממערכת "עין הנץ"). מכאן שיש לאפשר לחשודים בביצוע עבירה, שמידע על אודותם התקבל מתוך מהערכת, לקבל עותק מפורט על אופן הסקת המסקנות של המערכת לצד הקניית זכות ערעור למי שנפגע כתוצאה מהשימוש במערכת.

6.9. **הנדסת פרטיות.** גישה זו מבקשת להטמיע את הגנת הפרטיות במערכת מלכתחילה, כבר בשלב המכרז והתכנון הטכנולוגי, ולא רק בדיעבד בשלב ההפעלה (כפי שמורה התזכיר באופן מעומעם). על כן, אנו סבורים כי יש לחייב כי כל מכרז ורכישה של מערכת מעקב יכלול חובה להטמעת אמצעים וכלים להנדסת פרטיות (Privacy by Design) ופרטיות כברירת מחדל (Privacy by Default).

6.10. **ממונה על הגנת הפרטיות.** לשם הבטחת יישום והטמעה של עקרונות להגנת הפרטיות בהצבה, הפעלה ושימוש במערכות המעקב, יש למנות ממונה הגנת הפרטיות (Data Protection Officer) שאמון על כלל נושאי הגנת הפרטיות במשטרת ישראל. תפקידיו של ממונה הגנת הפרטיות מפורטים בהרחבה בטיוטת הנחיית הרשות להגנת הפרטיות.[9]

6.11. **תסקיר השפעה על הפרטיות.** על משטרת ישראל וכל גוף שעושה שימוש במערכות מעקב לערוך באופן תקופתי תסקיר השפעה על הפרטיות", שסוקר את כל פעולות עיבוד המידע שמבוצעות ועתידות להתבצע בקשר עם מערכות המעקב ומאגרי המידע המקושרים להן, ודרך כך למפות את סיכוני הפרטיות שעולים מהשימוש במערכות וממאגרי המידע. . אופן עריכת התסקיר ואפיונו מפורטים בהרחבה במסמך הרשות להגנת הפרטיות בנושא.[10]

בכבוד רב,

עו"ד נעמה מטרסו, מנכ"לית

פרטיות ישראל (ע"ר)

[9] הרשות להגנת הפרטיות, "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו" (29.10.2020)
[10] הרשות להגנת הפרטיות, "תסקיר השפעה על הפרטיות" (18.10.2020)