

ל' אב תשפ"א
8 אוגוסט 2021

הנדון: הערות הרשות להגנת הפרטיות לתזכיר חוק פקודת המשטרה [נוסח חדש] (תיקון מס'....) מערכות צילום מיוחדות, התשפ"א - 2021

1. להלן התייחסותנו לתזכיר החוק שבנדון, שעיקרה הוצגו בפני הגורמים הרלבנטיים עוד בטרם פרסומו לציבור. לחקיקה המוצעת תהיה השפעה מכרעת לא רק על פרטיות הציבור אלא גם על אופן המימוש של זכויות אדם אחרות. עמדתנו מתמקדת בסוגיות הנוגעות לפרטיות ומתבססת על המומחיות שפיתחה הרשות בהסדרה בפועל של היבטי הפרטיות של השימוש בטכנולוגיות מידע מעקב בכלל, ובמערכות צילום בפרט.¹

2. התזכיר מסדיר את השימוש בטכנולוגיה כדוגמת זיהוי פנים אוטומטי וזיהוי אוטומטי של לוחיות רישוי (LPR), המאפשרת להתחקות אחר המיקום ומסלול התנועה של אנשים, לרבות בזמן אמת. תיעוד קבוע של מסלול תנועתו של אדם מאפשר להסיק מידע רב ורגיש אודותיו. לשימוש בטכנולוגיה מסוג זה השפעה משמעותית על הזכות לפרטיות, שהיא במקרים רבים תנאי בלעדי אין לאפשרות לממש זכויות אדם נוספות. מעקב קבוע וגורף אחר כלל האוכלוסיה מוביל לאבדן האנונימיות במרחב הציבורי והיכולת להיטמע בהמון, ולמבט הממשטר של המערכת אפקט מצנן על חירויות חיוניות לקיומה של חברה דמוקרטית.

פגיעה בזכויות יסוד בטכנולוגיית זיהוי אוטומטי של אנשים

3. מיקום מערכות זיהוי אנשים כגון זיהוי פנים במרחב הציבורי, במקרים מסוימים, מאפשר ללמוד רבות על אורחות חייו של אדם לרבות דעה פוליטית (השתתפות בהפגנות או ביקור במוסדות מפלגתיים), דת (ביקור במקומות פולחן דתי), מצב רפואי או נפשי (ביקור במרפאות), נטייה מינית (ביקור במקומות מפגש של להט"בים) ועוד.

4. מערכות זיהוי פנים עלולות לגרום לחלק מהציבור להימנע מלהגיע למקומות בהם הן מוצבות וכפועל יוצא מכך להימנע מהשתתפות בהפגנות, התקהלויות, כניסה למקומות בהם מתקיים פולחן דתי, כניסה למקומות בהם ניתן טיפול רפואי ואף כניסה למקומות בהם ניתנים שירותים ציבוריים (כגון תחנות רכבת וכיו"ב).

¹ בין היתר פרסמה הרשות לאורך השנים [הנחיה בנושא השימוש במצלמות במרחב הציבורי](#), [הנחיה בנוגע למצלמות במקום העבודה](#), [המלצות בנושא היבטי פרטיות בשימוש ברחפנים](#), וכללים ליישום החקיקה בנוגע להתקנת מצלמות בפעוטונים. כמו כן, הרשות הייתה מעורבת בהליכי חקיקה ספציפיים בעניין התקנת מצלמות במוסדות סיעודיים, ובעניין שימוש במצלמות לאכיפת איסור הנסיעה בנתיבי תחבורה ציבורית; והביעה עמדה בסוגיית התקנת מצלמות בתחנות קלפי.

5. כפועל יוצא מהאמור לעיל, החשש מפני אובדן האנונימיות כתוצאה מזיהוי אוטומטי של אדם במרחב הציבורי, עלול לפגוע בחופש התנועה של חלקים מהציבור ואף לשמש, בנסיבות מסויימות, כאפקט מצנן על מימוש הזכות להפגין (ובכך לפגוע בחופש הביטוי), להתאגד, לקיים פולחן דתי, לקבל טיפול רפואי או טיפול נפשי, להתקהל במקומות מפגש של הקהילה הלהטב"ית, לשהות במרחב הציבורי וכדומה.
6. טכנולוגיות של ניתוח פנים, עשויות לאפשר ניתוח מצב רוח ותחושות של העוברים ושבים, והכל תוך יצירת פרופיל של אדם הכולל את מאפייני פניו יחד עם מידע נוסף אשר נאסף לגביו.
7. ניתוח זיהוי פנים מתבסס על הסתברויות, ולכן המערכת עלולה לטעות. ההשלכות של טעות בזיהוי עלולות להיות הרסניות במיוחד אם המערכת תזהה בטעות עוברי אורח תמימים כפושעים מבוקשים או כגורמים אסורי כניסה.
8. כך למשל, במחקר שערכה ACLU (American Civil Liberties union) נמצא כי מערכת בשם Rekognition של חברת Amazon זיהתה בשוגג 28 חברי קונגרס כאנשים שנעצרו בגין ביצוע פשע, כאשר שיעור גבוה במיוחד מהטעויות בוצעו לגבי נושאי מידע בעלי צבע עור שחור².
9. בפסק דין שניתן בשבועות האחרונים עמד בית המשפט העליון על הפגיעה הקשה בפרטיותו של אדם כתוצאה מגילוי נתוני המיקום שלו ללא הסכמתו:
- "נתוני מיקום עשויים ללמד רבות על אורחות חייו ומאפייניו של מושאם, כך שחשיפתם לזולת עשויה אף להסב לו נזקים של ממש במגוון תחומים".** עוד נקבע בפסק הדין כי **"הפגיעה הטמונה בגילוי נתוני מיקום ללא הסכמתו של מושא האיסוף, 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"**³.

² ACLU, Jacob Snow, Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots, July 26, 2018:

<https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>

³ רע"א 2404/21 פלונית נ' פלוני (22.07.2021), פסקה 17 לפסק-דינה של השופטת וילנר.

הערות כלליות לתזכיר החוק

10. מעקב ותיעוד קבוע ושיטתי אחר תנועות התושבים לא רק שפותח פתח לניצול לרעה של המידע הרגיש הנאגר על אנשים ספציפיים, אלא גם גורם לציבור תחושה שהוא נתון למעקב, אשר יוצרת אפקט מצנן והשפעה שלילית של ממש על יכולת הציבור לממש את זכויות האזרח שלו ולקיים חברה דמוקרטית.

11. לעניין זה חשוב להדגיש שאין הכרח כי המצלמות המיוחדות יכסו את כל שטחי הארץ. די בכך שהציבור מודע לקיומן של המצלמות, אך אינו יכול לדעת אל נכון היכן ומתי הוא מתועד. החשש הוא שתלך ותרווח בציבור התחושה מרפת הידיים כי פוטנציאלית הכל נתונים למעקב קבוע ומתמיד, בכל מקום ובכל שעה.

12. בעולם כזה גם עלולה להיאבד האפשרות להיטמע ברחובה של עיר ללא מבט חיצוני מפקח וממשטר, ולהיפגע יכולתם של התושבים לממש את אישיותם ואת זכויות האדם המוקנות להם. זהו קו פרשת מים, שינוי מהותי ומשמעותי החורג בסדרי גודל משיפור גרידא ביכולת המעקב "הידנית" המוקנית ממילא למשטרה במרחב הציבורי. די בכך שזכיר שמעקב קבוע המלווה ביכולת זיהוי אוטומטית מתעד באופן גורף את כלל התנהלותם של המצולמים, מבלי ששום פרט הקשור אליהם יישכח, או יוצב בהקשר המתאים בחלוף הזמן.

13. מכאן שבחברה דמוקרטית, תיעוד קבוע ומזוהה של תנועות התושבים בידי השלטון, הינה פעולה חריגה ופוגענית אותה יש לבצע **בחרדת קודש**, בזהירות המתחייבת מהשפעותיה השליליות על הזכות לפרטיות ועל מימושן של זכויות יסוד אחרות במרחב הציבורי, ובמידה המינימאלית הנדרשת.

14. הטכנולוגיות אותן מבקש התזכיר להסדיר הן במהותן מערכות לאיסוף "נתוני מיקום" בידי רשויות המדינה, על כלל הציבור או חלק גדול ממנו לרבות החפים מפשע, הדומות דמיון של ממש לסמכויות האיסוף ועיבוד המידע המוקנות כיום רק לשירות הביטחון הכללי, ורק לתכליות ביטחוניות מצומצמות (על רגישותם של נתוני מיקום, מהם ניתן ללמוד על קיומם של קשרים אישיים ומפגשים חברתיים, ראו בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת** (1.3.21), פסקה 18 לפסק דינה של הנשיאה חיות. ראו גם מהעת האחרונה רע"א 2404/21 **פלונית נ' פלוני** (22.7.21), פסקה 17 לפסק הדין, שציטוט ממנה הובא לעיל בפסקה 9).

15. בניגוד לחוק נתוני תקשורת⁴, ההסדר המוצע יסמך לראשונה את המשטרה **עצמה** לאסוף מידע רגיש על איכוני כלל התושבים, או חלק בלתי מסוים מהם, ללא צורך בצו שיפוטי. אמנם סוג נתוני הקלט שונה, ושוני יש גם בתווך בו הם נאספים – המרחב הפיזי לעומת המרחב הווירטואלי – אבל קיים דמיון רב בתכלית השימוש ובהשפעה שיש לה על הציבור ועל החברה.

16. הגם שהיקף פריסת המצלמות המיוחדות צפוי להיות מצומצם, הרי שלהפעלתן פוטנציאל גבוה יותר לפגיעה בפרטיות, מפני שבמרחב הציבורי (בניגוד למרחב הווירטואלי) אין לציבור ציפייה להיות נתון למעקב תמידי, קל וחומר שלא ביחס לטכנולוגיות מעקב המתבססות על זיהוי אוטומטי של **הפנים** של האנשים המתהלכים לתומם ברחוב.

17. לאור האמור לעיל, סבורה הרשות שהמגבלות על השימוש בטכנולוגיות המיוחדות המוצעות בתזכיר אינן מספיקות, אינן הולמות את פוטנציאל הפגיעה המהותית הגלום במערכת, וחסרות אף את האיזונים, הבקורות והערובות הקבועים בהסדרים ספציפיים אחרים (כגון בחוק שירות הביטחון הכללי ובחוק נתוני תקשורת).

18. קושי מהותי ומרכזי מוצאת הרשות בכך שמטרות השימוש במידע שנאסף מהמצלמות, המפורטות בסעיף 10 לטיטת התזכיר – רחבות בהרבה מהמטרות הלגיטימיות **להצבת המצלמה המפורטות בסעיף 10ג**, במידה המרוקנת מתוכן את המגבלות על עצם התקנת המצלמה. כך למשל, מתיר סעיף 10א(3) שימוש במידע מהמערכת המיוחדת לשם "גילוי עבריינים והעמדתם לדין" – ללא מגבלה על סוג העבירה שנעברה על ידם וחומרתה.

19. זהו תקדים הפורץ את גדר האיזונים והבלמים הנוהגים כיום: לראשונה תוסמך המשטרה לקבל לשימושה "נתוני מיקום" **על כל אדם** שנקלט במצלמות המיוחדות, לרבות מי שלא היה חשוד במועד הצילום. בניגוד להסדר הקיים בחוק שירותי הביטחון הכללי ובנהלים מכוחו – השימוש יתאפשר לחקירת **כל** עבירת עוון ופשע ולגילוי כל עברייני באשר הוא, ולא יוגבל רק לצרכי הליבה החיוניים ביותר לשלום הציבור ובטחון המדינה. כמו כן, בניגוד להסדר הקיים בסעיפים 3 ו-4 לחוק נתוני תקשורת, **לא תידרש המשטרה לצו שיפוטי ולא תוכפף לבקרה חיצונית על אופן הפעלת שיקול דעתה.**

20. יובהר כי הקושי עליו אנו מצביעים אינו גלום בתשתית טכנולוגית כזו או אחרת, אלא בשימוש שעושים במידע הנאסף באמצעותה. לפיכך וככל שחוק זה יקודם, חשוב שיכלול מתווה להגבלת השימוש במידע מזוהה ברמה הנורמטיבית, אשר יהווה איזון בין מכלול השיקולים וההגנה על זכויות האדם בדגש על זכותו לפרטיות.

⁴ חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007.

21. הסיכונים המהותיים לזכות לפרטיות ולזכויות אדם אחרות עליהם הצבענו רלבנטיים לשני סוגי מערכות הצילום המיוחדות שאת השימוש בהן מציע התזכיר להתיר. עם זאת העוצמה והחומרה של הסיכונים שהזכרנו גדולות פי כמה וכמה מונים בכל הנוגע לטכנולוגיית זיהוי פנים:

א. בנוסף להתחקות אחר המיקום ומסלול התנועה של התושבים, טכנולוגיה זו, הנעזרת בעיבודי וידאו מתוחכמים ובבינה מלאכותית, מאפשרת גם לבנות פרופיל אישי מקיף ורגיש ביותר על התושבים, הכולל נתונים כגון הרגליהם החברתיים והדתיים, האנשים עימם הם מתרועעים, מצבם הרפואי, תחושותיהם, מצבם הנפשי, נטיותיהם המיניות ועוד;

ב. כיוון שהיא מנטרת את תנועתו של האדם עצמו ולא של כלי הרכב, המערכת צפויה להחמיר במידה ניכרת את תחושת המעקב ואת האפקט המצנן שלה על הציבור;

ג. תווי פנים הם נתון ביומטרי חד ערכי הייחודי לכל אדם ובלתי ניתן להחלפה. משכך עצם איסופם יוצר סיכון אבטחה גבוה ביותר ופוטנציאל גבוה לשימוש לרעה באופן בלתי הפיך במקרה של דליפת המידע או גניבתו, הן על ידי גורמים עברייניים הן על ידי גורם עוין אחר, לרבות במישור הלאומי (כגון מתקפת סייבר על ידי מדינה אחרת).

22. סיכוני הפרטיות והאבטחה כבדי המשקל הייחודיים לשימוש בטכנולוגיית זיהוי פנים, וכן היבטים תפעוליים נוספים המיוחדים לשימוש במערכות ביומטריות, מחייבים שמלוא הסוגיות המהותיות הכרוכות בשימוש בה תיקבענה בחקיקה ראשית.⁵

בכל הנוגע למערכות זיהוי פנים – שפגיעתן בפרטיות היא בסדר גודל שונה – עמדת הרשות היא שלא ניתן להסתפק בחקיקת משנה להסדרת אופן הפעלתה, וזאת אף אם יוחלט שדי בה לשם הסדרת היבטים מסוימים של השימוש במערכות LPR. לכן מציעה הרשות להפריד את ההסדרה של שני סוגי המערכות ולייחד חקיקה ראשית נפרדת למערכות זיהוי פנים.

הערות לסעיפים קונקרטיים בתזכיר החוק

23. בסעיף 10א הגדרת המונח "גוף ציבורי" – לא ברור כיצד חלק הגופים המנויים בהגדרה רלבנטיים למטרות הצבת המערכות המיוחדות המנויות בסעיף 10ג. כמו כן את סמכות השר להוסיף בצו גוף ציבור נוסף, יש להבנות בחוק ולצמצם אותה רק לגופים הפועלים למטרות בטחון המדינה או למטרות ספציפיות אחרות שיוגדרו בחוק.

⁵ לעניין זה ראו גם עמדת מערך הסייבר הלאומי בנושא "זיהוי פנים במרחב הציבורי – קריאה להסדרה":

https://www.gov.il/he/departments/general/face_recognition

24. הגדרת "מערכת צילום מיוחדת" – בשל עקרון הניטרליות הטכנולוגית, ראוי לדעתנו להגביל ולהסדיר בחקיקה ראשית מפורטת ומאוזנת לא רק את השימוש "במערכות צילום מיוחדות" – אלא גם במערכות אחרות האוספות נתונים באמצעות **חיישנים אחרים שאינם ויזואליים** דווקא. בהתאם לכך יש להוסיף לרישא של ההגדרה את המונח "חיישן", כך שהרישא תיקרא כך:

"מערכת איסוף מיוחדת" - חיישן, לרבות מצלמה, אחד או יותר, שמתקיימים בהם כל התנאים הבאים:...."

25. גם בהגדרות הנוספות הכוללות את המילה "מצלמה" ובמופעים שלהן בהמשך התזכיר – יש לתקן ל-"חיישן" – מתקן טכנולוגי האוסף נתונים ויזואליים, קוליים או אחרים, באופן המאפשר זיהוי אדם, או התחקות או בילוש אחריו".

26. **בסעיף 10ב** - בהמשך להערתנו בדבר הצורך להסדיר בחקיקה ראשית את מלוא ההיבטים הכרוכים בשימוש במערכות זיהוי פנים, ולהערתנו להגדרת "מערכת צילום מיוחדת" אנחנו מציעים לתקן את נוסח הסעיף כדלקמן:

"משטרת ישראל רשאית להציב, להפעיל ולהשתמש רק במערכת איסוף מיוחדת המנויה בתוספת הרביעית או בחוק בהתאם להוראות פרק זה ובלבד שנקבעו תקנות כאמור בסעיף 10ב; השר, בהסכמת שר המשפטים ובאישור ועדת הפנים והגנת הסביבה של הכנסת, רשאי לתקן את התוספת הרביעית."

27. **בסעיף 10ג (תכליות להצבה והפעלה)** – בסעיף קטן (ב) יש למחוק את הרישא "חקירת דפוסי פשיעה בעבירות מסוג פשע". "חקירת דפוסי פשיעה" היא תיבה כללית ומעורפלת מדי המאפשרת התחקות אחרי חפים מפשע למטרות מודיעין כלליות, גם כשאין ראיה או חשד לעבירה ספציפית. לחלופין יש להגביל את תחולת הרישא רק לעבירות מסוג "פשע חמור" שיוגדרו מראש בחוק.

28. **בסעיף 10ג(ה)** יש להגדיר במדויק מהם "איסורי הכניסה וצווי ההרחקה" אותם ניתן יהיה לאכוף באמצעות המערכת המיוחדת.

29. **בסעיף 10ד(ב)** יש להוסיף בסיפא "לפי תוצאות תסקיר השפעה על פרטיות שייערך בטרם ההתקנה של כל מערכת צילום מיוחדת בנפרד, ויכלול בין השאר התייחסות למידת הפגיעה בפרטיות הצפויה לציבור הנוהג לשהות במקום המיועד להצבת המצלמה, בשים לב לאוכלוסיות מיוחדות⁶ או למתקנים רגישים המצויים בקרבתו".⁷

⁶ כגון קטינים וחוסים.

⁷ כגון מרפאת הפלות, מרפאה לבריאות הנפש, או מוסדות רפואיים אחרים, ארגוניים פוליטיים וכיוצא באלה.

30. **בסעיף 10ד(ג) – מהטעמים שפרטנו לעיל, בפועל עצם הצבת המצלמה תקנה למשטרה אפשרות להשתמש במידע הנקלט בה, ואשר מהותית שקול ל"נתוני מיקום", לצורך חקירה של כל עבירת עוון ופשע, ללא הבחנה לעניין מידת חומרתה. להשוואה, חוק נתוני תקשורת דורש צו שיפוטי לשם קבלת מידע מסוג זה. לפיכך ראוי כי ההחלטה על הצבת המצלמות תימסר להכרעת גורם בלתי תלוי** חיצוני למשטרה, כגון שופט בדימוס, או ועדה ציבורית. **בנוסף, יש למסד פיקוח חיצוני ואפקטיבי על החלטות "הקצין המוסמך", אשר יחייב העברת דיווח עיתי על ההחלטות ונימוקיהן, וכן דיווח כאמור לוועדה המוסמכת בכנסת.**

כמו כן, לא ברור מהם גבולות "מתווה ההפעלה" בסעיף זה ומה שיקול הדעת המסור לקצין המוסמך; יש להבנות את תוכן המתווה בחוק או לכל הפחות בתקנות, ולכלול בו בין השאר דרכי יישום של עיקרון העיצוב לפרטיות בעת התקנת המערכת והפעלתה, למשל בשטח הכיסוי של המצלמות, הרזולוציה המקסימאלית שלהן, ימי השבוע והשעות בהן יופעלו וכד'.

31. **סעיף 10ד(ד) - השימוש במצלמות ניידות** צופן סיכון גבוה יותר לפרטיות בשל אקראיות האזורים המצולמים, ובשל ההסתברות הגבוהה יותר לצלם מקומות שהם בבחינת רשות היחיד ואזורים רגישים אחרים. סיכון זה צריך לבוא לידי ביטוי בהוראות מתווה ההפעלה. ככל שההחלטה על הפעלה ספציפית של מצלמה ניידת תתקבל בידי דרגים נמוכים יותר – כך יש להבנות ולהתוות מראש את גבולות שיקול דעתם.

32. **סעיף 10ד(ה) - שקיפות.** יש להבטיח כי ברירת המחדל תהיה יידוע לא רק על האיזור בו הוצבה המצלמה (לא בהכרח מיקומה המדויק) – אלא גם על מאפייניה המיוחדים ועל הגורם המפעיל אותה. כפי שהסברנו, אחת מן ההשלכות השליליות ביותר להתקנת מערכות זיהוי אוטומטי היא תחושת המעקב הנוצרת בציבור. הקפדה על שקיפות בדבר סוג המערכת נדרשת כדי למתן במידת מה את נזקיה המוחשיים של תחושת המעקב. את הנסיבות בהן יידוע לא יתאפשר, ראוי להבנות מראש בחקיקת משנה או לפחות בנהלים.

33. **סעיף 10 - תנאים לשימוש במידע.** מהנימוקים שפרטנו בהרחבה בפרק ההערות הכלליות, אנו סבורים שאין להשתמש במידע לתכליות השונות מאלה שאושרו לצורך הצבת המצלמות. לפיכך, את סעיף 10א(2) יש לצמצם לעבירות פשע בלבד, וכך גם את סעיף 10א(3) בעניין גילוי עבריינים. לחלופין, ובדומה לאיזון הקיים בחוק נתוני תקשורת, יש להתנות את השימוש במידע לחקירת עבירות עוון בקבלת אישור ערכאה שיפוטית, שתערוך את האיזון ההולם בין התועלת הצפויה משימוש זה, לבין הנזקים הגלומים בה לחברה, למול הזכות לפרטיות והיכולת לממש זכויות נוספות.

34. **סעיף 10(ו)ב) - שימוש במידע לצורך מחקר.** הרשות מתנגדת לעשיית שימוש במידע הרגיש הנאסף במצלמות המיוחדות באופן שחורג מתכליות הליבה החיוניות הנקובות בסעיף 10ג לתזכיר; ודאי שלא למטרות הרחבות והכלליות בסעיף 3 לפקודת המשטרה, כגון "קיום הסדר הציבורי". יש בכך משום בנאלזציה של שימוש באמצעי מעקב כה חריג ופוגעני, שאינה מייחסת משקל מספיק למחיר החברתי והדמוקרטי הכרוך בשימוש בו. לכל הפחות יש להתנות שימוש למחקר רק מידע שעבר אנונימיזציה מלאה כך שיוסרו ממנו **גם פרטים הניתנים לזיהוי** בנוסף על הסרת המזהים הישירים. בנוסף, את הקריטריונים להחלטה על עריכת המחקר ומתכונתו אין להותיר בידי קצין משטרה, בכיר ככל שיהיה, אלא ראוי לקבוע בתקנות או בנוהל שיאושר בידי היועץ המשפטי לממשלה.

35. **לסעיף 10(ג) יש להוסיף את הרישא:** "מבלי לגרוע מהוראות חוק הגנת הפרטיות, התשמ"א-1981 ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017".

36. **סעיף 10(ד) – עמדתנו היא שראוי לקבוע כבר בחקיקה הראשית את תקופת המקסימום לשמירת מידע** שאינו דרוש לחקירה ספציפית. עיגון משך השמירה המקסימאלי בחקיקה ראשית מקובל בדברי חקיקה אחרים ויש לו חשיבות יתרה כשעסקין במידע שבפנינו, שהשלכותיו הפוטנציאליות על פרטיות התושבים וזכויותיהם הן ברמה הגבוהה ביותר ומשעסקין בתיעוד גורף, קבוע ושיטתי אחר ציבור שלם שמלכתחילה אין בו מתום או זיקה כלשהי לעבירה שנחקרה.

37. עמדת הרשות היא כי **מידע הנקלט במצלמות הניידות אין לשמור כלל, או לחלופין לפרקי זמן קצרים ביותר**. זאת מפני שחלק גדול ממידע זה נקלט באופן אקראי בנסיבות שאינן מקיימות את התכליות הכלליות להצבת מצלמות נייחות, ואף לא את התכליות שיצדיקו את הפעלת המצלמה הניידת הנוגעת בדבר.

38. **בסעיף 10ו יש להוסיף סעיף קטן נוסף:** "(ו) אחת לשנה תמסור המשטרה לוועדת חוקה חוק ומשפט של הכנסת דין וחשבון בדבר היקף השימוש במידע שנאסף לפי פרק זה, נסיבותיו, משך שמירת המידע ומחיקתו, והכל בנפרד לגבי כל סוג של מערכת מיוחדת המנויה בתוספת הרביעית".

39. **בסעיף 10ח יש להבהיר שהתנאים בסעיף קטן (א) למסירת מידע לגוף ציבורי – הם מצטברים.** בסעיף קטן (ב) יש להגביל את מסירת המידע לגוף ציבורי אך ורק לעילות הפעלת מערכות הצילום הנקובות בסעיף 10ג לתזכיר.

40. **סעיף 10יא(ב) - הסייג בעניין אי תחולת מגבלות החוק בעת שימוש במערכות הצילום המיוחדות ב"חקירה" רחב מדי ועלול לרוקן מתוכן הלכה למעשה את הוראות סעיפים 10ג ו-10ו.** כך למשל, הסייג עשוי לכאורה לחול ביחס לכל שלב בחקירה. עמדת הרשות היא כי יש לצמצם את הסייג ולקבוע לו גבולות ברורים.

הצעת רגולציית הבינה המלאכותית של האיחוד האירופי

41. באירופה השימוש במערכות זיהוי פנים המוצבות במרחב הציבורי לצרכי אכיפה (Live Facial Recognition) נתון לביקורת קשה וככל הידוע לנו אין אף מדינה המשתמשת בשיטה זו למעט בריטניה. בינואר 2020 פורסם כי נציבות האיחוד האירופי שוקלת לפרסם המלצה לפיה עד להסדרת הנושא לא יהיה שימוש בזיהוי פנים במרחב הציבורי.⁸ אולם ההמלצה לא פורסמה בסופו של דבר.

42. עם זאת, ביום 21.4.2021 פרסמה נציבות האיחוד האירופי הצעת רגולציה לתחום הבינה המלאכותית הכוללת התייחסות למערכות זיהוי ביומטריות המוצבות במרחב הציבורי לצרכי זיהוי ואכיפה פלילית.⁹

א. לפי ההצעה, פרקטיקה זו תותר רק כאשר השימוש בה הכרחי לצורך אחד מאלה:

- איתור קורבנות פשיעה פוטנציאליים ספציפיים, לרבות ילדים נעדרים;
- מניעת סכנה מיידית חמורה וספציפית לחייו או לבטחונו של אדם או למניעת התקפת טרור;
- גילוי זיהוי או העמדה לדין של מבצע או חשוד בעבירה פלילית אשר עונשה שלוש שנים לפחות, והיא אחת מן העבירות המפורטות להלן: חברות בארגון פשיעה, סחר בבני אדם, ניצול מיני של ילדים לרבות פורנוגרפיה בהשתתפות ילדים, סחר בסמים, שחיתות, מרמה, הלבנת הון, פשעי מחשב, פשיעה הקשורה לאיכות הסביבה (סחר בזני חיות וצמחים מוגנים), רצח או פגיעה גופנית קשה, סחר באברי גוף, חטיפת בני אדם והחזקת בני ערובה, גזענות, שוד מאורגן או שוד באמצעות כלי נשק, סחר לא חוקי באומנות, מעשי נזק, סחיטה וסחר במוצרים פיראטיים, סחר במסמכים רשמיים, זיוף אמצעי תשלום, סחר לא חוקי בהורמוני גדילה וחומרים אחרים להאצת גדילה, סחר לא חוקי בחומרים גרעיניים ורדיואקטיביים, סחר לא חוקי ברכבים, אונס, הצתה, פשעים אשר בסמכות השיפוט של בית המשפט הפלילי הבינלאומי, אחזקה בלתי חוקית של כלי טיס או שיט, חבלה, זיוף מטבעות.

ב. בהחלטה לבצע זיהוי ביומטרי מרחוק בזמן אמת במרחב הציבורי כאמור יש להביא בחשבון את נסיבות המקרה, חומרתו, הסבירות להתרחשותו, חומרת הנזק אשר ייגרם מאי שימוש במערכת, והשפעות השימוש במערכת על זכויות אחרים.

⁸ <https://www.bbc.com/news/technology-51148501>

⁹ <https://ec.europa.eu/newsroom/dae/items/709090>



ג. הנחת מערכות ביומטריות במרחב הציבורי למטרות זיהוי בזמן אמת תותר רק אם היא חיונית ומידתית בהתייחס אל משך הזמן בו יעשה שימוש במערכת, מיקומה של המערכת וההיבט האנושי.

ד. כל שימוש במרחב הציבורי כאמור יהיה כפוף לצו שיפוטי או אישור של רשות מנהלית מוסמכת בלתי תלויה, אשר יינתנו מראש, בעקבות הגשת בקשה מנומקת. במקרים דחופים ניתן להשתמש במערכת ללא אישור מראש, אלא אישור בדיעבד.

