

העותרת: האגודה לזכויות האזרח בישראל (ע"ר 580011567)
ע"י ב"כ עוה"ד גיל גן-מור ו/או דן יקיר ו/או אבנר פינצ'וק
ו/או עודד פלר ו/או שרון אברהם-ויס ו/או דבי גילד-חיו ו/או
עביר ג'ובראן דכוור ו/או משכית בנדל ו/או טל חסין ו/או
אן סוצ'יו ו/או רוני פלי ו/או סנא אבן ברי ו/או רעות שאער

מהאגודה לזכויות האזרח בישראל
רחוב נחלת בנימין 75, תל-אביב 65154
פקס: 03-5608165; דוא"ל: gil@acri.or.il

- נ ג ד -

המשיבה: משטרת ישראל
באמצעות פרקליטות מחוז ירושלים (אזרחי)

עתירה מנהלית

בית המשפט הנכבד מתבקש להורות למשיבה למסור לעותרת את המידע שביקשה מכוח חוק חופש המידע, ושעניינו השימוש שעושה המשטרה בטכנולוגיה לזיהוי פנים במשטרה, וכן מצלמות המעקב ומאגרי המידע שבהם נעזרת המשטרה לצורך כך.
שלוש הבקשות מכוח חוק חופש המידע מצורפות ומסומנות ע/1-3/ע.

ואלו הם טעמי העתירה

רקע: שימוש משטרה בטכנולוגית זיהוי פנים

1. עניינה של עתירה זו בסירובה הגורף והמוחלט של משטרת ישראל לחשוף כל מידע על השימוש שהיא עושה בטכנולוגיה לזיהוי פנים (Facial Recognition Technology) (להלן – הטכנולוגיה או FRT).
2. טכנולוגיה לזיהוי פנים היא טכנולוגיה ביומטרית - טכנולוגיה ממוחשבת, המאפשרת זיהוי חד-ערכי של אדם על פי מאפיין אנושי ביולוגי או התנהגותי ייחודי, הניתן למדידה ממוחשבת, והיכול לשמש לאימות ולזיהוי. הטכנולוגיה מאפשרת להפיק מתצלום פניו של אדם נתונים מתמטיים ייחודיים, בעזרת מיפוי ומדידה של המרחק בין העיניים, מרחק בין המצח והסנטר, מבנה האף והסנטר וכיוצא באלה נתונים מדידים, שמסתכמים לבסוף לביטוי מתמטי חד-חד ערכי. כלומר, ביטוי מתמטי מסוים שיתקבל שוב ושוב כל אימת שהמערכת תוזן בתמונת הפנים של אותו אדם.

3. מערכות זיהוי פנים שונות זו מזו ביכולת לזהות אנשים ואין מערכת אחד שתשיג דיוק של 100 אחוזים בכל התנאים. ההשוואה מבוססת על הסתברויות ולכן ההשוואה בין שתי תמונות לא תסתכם בתשובות של "כן" או "לא" אלא בתוצאה של שיעור ההתאמה.
4. מערכות זיהוי פנים יכולה **לאמת זהות** של אדם מוכר. טלפונים חכמים רבים משתמשים כיום בזיהוי שכזה כדי לאפשר לבעל הטלפון לפתוח את הנעילה: הטלפון קולט את הפנים של מי שנועץ בו מבט ומשווה אותם לתווי הפנים השמורים של בעל הטלפון. יישום אחר של הטכנולוגיה נועד ל**זהות** אדם לא מוכר באמצעות השוואה של תמונתו למאגר תמונות קיים. למשל, שוטר ישתמש במערכת כדי לזהות חשוד לא מוכר, שצולם באחת ממצלמות המעקב שפרוסות במרחב הציבורי.
5. הזיהוי יכול להתבסס על השוואה אוטומטית ממוחשבת של תמונות ממצלמות אבטחה, למשל, והשוואתן למאגרים ציבוריים שיועדו לצרכים שונים (המאגר הביומטרי, מאגר רישיונות נהיגה) או פרטיים (פרופיל ברשתות חברתיות).
6. הטכנולוגיה הינה טכנולוגיה חדשה יחסית, המאפשרת לזהות אדם בעזרת בינה מלאכותית (אלגוריתם), באמצעות השוואה אוטומטית של תמונות או סרטונים של אותו אדם למאגר תמונות מזוהה. כלומר – הטכנולוגיה מאפשרת, למשל, לעבד תמונה של אדם אנונימי והשוואתה עם מאגר תמונות מזוהה, וזאת גם בלי שהאדם נתן מיוזמתו את נתוניו הביומטריים וגם ללא הסכמה לביצוע הזיהוי.
7. הטכנולוגיה מתבססת על אלגוריתם שמשמש לעיבוד תמונה באמצעות ניתוח מאפיינים ביומטריים ייחודיים (למשל – המרחק בין העיניים).
8. הטכנולוגיה מסוגלת לזהות אדם בהתבסס על תמונות גם ממצלמות רגילות, וגם מצלמות ייחודיות בעלות יכולות צילום ברמה הניתנת לעיבוד ביומטרי, נטרול עיוותים, אור או הבעות פנים, עיבוד של צילום חלקי וכן התבייתות אוטומטית על פנים בתוך קהל.
9. פיתוח נוסף של הטכנולוגיה נועד לאבחן באופן אוטומטי, באמצעות אלגוריתם, "רגשות" כמו כעס, עצבנות וכדומה, מצפיה בתמונה או סרטון (Affect Recognition).
10. זיהוי פנים אוטומטי – Automatic (or Live) Face Recognition (AFR) - מתבצע באמצעות השוואה בזמן אמת של "אחד לרבים" (one to many), כלומר, השוואה בין תצלום (סטילס או וידאו) של אדם שחולף על פני המצלמה אל מול "רשימת מבוקשים" (watch list). רשימה כזו עשויה לכלול פנים של חשודים, של נעדרים, ואנשים אחרים שמעניינים את המשטרה.
11. משטרת ישראל מעולם לא הודתה שהיא עושה שימוש בטכנולוגיה זו, למרות שבדף האינטרנט של **מנהל הטכנולוגיות** (מנ"ט) האחראי למתן מענה טכנולוגי למימוש יעדי משטרת ישראל, נכתב שהוא אחראי, בין היתר, על "כלים ביומטריים" ובכלל זה "הרחבת השימוש באמצעי זיהוי שונים: טביעות אצבע, זיהוי פנים, דנ"א, מאגרי תמונות לאימות זיהוי ושיפור ההרתעה" (ר' בקישורית: <https://bit.ly/3ih5kMI>).

12. גם לפי כתבה שפורסמה ברשת NBC, באוקטובר 2019, הטכנולוגיה של חברת AnyVision משמשת את משטרת ישראל למעקב אחר חשודים בגדה המערבית וגם ברחובות ירושלים המזרחית, שם חל החוק הישראלי. הכתבה כוללת סרטון שיווקי, שהחברה מפיצה בחו"ל, ובו היא מדגימה את השימוש שנעשה בטכנולוגיה שלה בסמטאות העיר העתיקה בירושלים.



<https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116>

13. זאת ועוד, מבקר המדינה מתח לאחרונה ביקורת חריפה על האופן שבו מתנהלים מאגרי מידע ביומטריים במדינה, ובמסגרת זו התייחס גם למאגר תמונות ב"איכות ביומטרית" שהוקם במשרד התחבורה (איכות ביומטרית היא איכות גבוהה המאפשרת לעבד את התמונות בטכנולוגיה ביומטרית - השוואה ביומטרית וחיפוש במאגר ביומטרי). המאגר הוקם עוד בשנת 2006 אבל עד עצם היום הזה לא טרחו לעגן את פעילותו בחקיקה מתאימה. מכל מקום, ולענייננו, מסתבר שהמשטרה מקבלת מידע ממאגר התמונות הביומטרי באופן שוטף. "המשטרה מסרה למשרד מבקר המדינה כי המגזרים המשתמשים במאגר תמונות רישיונות הנהיגם הם כל אלה הנדרשים לזיהוי אדם – סיור, תנועה, ואגף החקירות והמודיעין, והזיהוי נדרש במגוון מצבים... " (ר' מבקר המדינה, **דוח שנתי 2017**, עמ' 261-252 (מאי 2020)). לאור זאת מתגבר החשש, שמאגר התמונות של רשות הרישוי (שהוא עצמו אינו חוקי) ישמש גם לעיבודים וחיפושים ביומטריים.

14. לא קשה להבין מדוע גורמי ביטחון שונים, לרבות משטרה, ירצו בטכנולוגיה זו, שיכולה לטייב את עבודתם ולקדם את המטרות החברתיות שבאחריותם. אך בה בעת, לשימוש בזיהוי פנים יש פוטנציאל מסוכן לפגוע בזכויות יסוד חוקתיות.

15. ראשית, השימוש בטכנולוגיה פוגע, וטומן בחובו פוטנציאל לפגיעה חמורה עוד יותר בפרטיות ובצנעת הפרט, וביכולת של אזרחים לשמור על האנונימיות במרחב הציבורי.

16. נתונים ביומטריים שונים במהותם מנתונים מינהליים הקשורים למחזור החיים של האדם. נתונים מינהליים הם ברי עדכון ותיקון (כגון שם, כתובת, מצב משפחתי). נתונים ביומטריים מאפיינים את

האדם עצמו, ולפיכך, במרבית המקרים, אינם ברי עדכון ותיקון בצורה פשוטה. עצם הנטילה והשימוש במידע הביומטרי של אדם מסבה פגיעה בפרטיות, כפי שהטעים אפילו היועץ המשפטי לממשלה בדיוני חקיקה ובניירות עמדה שהוגשו לבתי המשפט. כך, למשל, התייצב היועץ המשפטי לממשלה בהליך בעניין שעון נוכחות ביומטרי במקום העבודה ובין היתר אמר את הדברים הבאים:

"היועמ"ש מזכיר את אופיו הייחודי של המידע הביומטרי ומציין כי 'מרגע שנחשף, או שנעשו בו שימושים אחרים שלא כדין – לא ניתן להשיב את הגלגל לאחור'. נוכח אפיון זה, היועמ"ש סבור שעצם חיובו של עובד להוציא משליטתו מידע ביומטרי ולהעבירו למעסיק לשימוש במערכת זיהוי ביומטרית, פוגע בזכותו לפרטיות. הפגיעה נגרמת מעצם אובדן השליטה על נתון מזהה כה רב עוצמה, והיא אינה מתמצה בחשש משימוש לרעה בנתון זה. פגיעה נוספת ונפרדת בפרטיות נגרמת מחשש משימוש לרעה או שלא כדין בנתונים הביומטריים ומהסיכון שידלפו. בהמשך ישיר לכך מוסבר ש'השימוש באמצעים ביומטריים צובר תאוצה, אך סיכוניו והיכולת למזערם טרם הובררו כל צרכם', וככל שיתרחב השימוש כאמור, כן יגדל הסיכון שייעשה במידע שימוש לרעה, חרף אמצעי האבטחה הקיימים. לכן מידת הנזק שעלול להיגרם כתוצאה מדליפת הנתונים היא "גדולה ביותר, עד כדי בלתי הפיכה" [עס"ק (ארצ'י) 7541-04-14 **הסתדרות העובדים הכללית החדשה נ' עיריית קלנסווה** פס' 56 (15.3.2017)].

17. לזיהוי פנים יש מאפיון ייחודי, בשונה מטביעות אצבע ונתונים ביומטריים דומים, בכך שניתן לזהות באמצעותם אנשים, גם ללא רצונם וללא ידיעתם. ניתן לצלם אנשים במצלמות אבטחה, כשהם עוברים ברחוב וחולפים מול המצלמה, או במתקנים ציבוריים אחרים, ולבדוק צילומים אלו מול "רשימות מעקב" (Watchlist).

18. כאשר FTR משולבת עם מערך ענק של מצלמות מעקב ועם יכולות אחסון ומחשוב גדולות, הממשלה יכולה לייצר בעזרתה מעקב רציף אחר אינדיבידואלים מסוימים. אפשר לעקוב אחרי כל אחד בכל מקום, ולעקוב אחרי כולם בכל המקומות. בכל זמן או כל הזמן. באופן כזה FTR יכולה לאפשר מעקב המוני בקנה מידה חסר תקדים. וכפי שהזהיר נשיא מייקרוסופט, בראד סמית, לפני כשנתיים:

"... Unprecedented, but not unimagined. As George Orwell described in his novel '1984,' one vision of the future would require that citizens must evade government surveillance by finding their way secretly to a blackened room to tap in code with hand signals on each other's arms – because otherwise cameras and microphones will capture and record their faces, voices and every word. Orwell sketched that vision nearly 70 years ago. Today technology makes that type of future possible (Brad Smith "Facial recognition: It's time for action" Dec.6,2018 at <https://bit.ly/2GFSQQs>).

19. המרחב הציבורי שלנו מרושת במספר הולך וגדל של מצלמות מעקב, וכל אחת מהן אפשר לחבר למערכת זיהוי פנים וכך לזהות אדם שעובר ממקום למקום. בניגוד למצלמות האבטחה המוכרות לנו, המערכת אינה מזהה רק אירועים חריגים, אלא יכולה לזהות באופן מתמשך, אוטומטי ורציף

את אנשים, וליצר מאגר מידע עצום ובו מידע אישי ואינטימי על כל מי שמצולם. ממאגר זה ניתן לדלות את המידע בלחיצת כפתור.

20. FTR מעלה את המעקב לדרגות חדשות ומפחידות. היא מאפשרת מעקב אוטומטי ורצוף אחר אנשים בזמן שהם טרודים בענייני היומיום שלהם, ומעניק לרשויות אפשרות לעקוב אחר כל מהלך ותנועה שלנו. היא מפרה את עקרון הנחיצות והמידתיות. מעקב צריך להיות נחוץ ומידתי בכל מקרה שהוא מתבצע. בהתאם לזאת המעקב חייב להיות מצומצם לטיפול בעבירות חמורות בלבד.

21. אגירת מידע על מיקומיו של אדם מסוים לאורך זמן, באמצעות זיהוי תווי פניו כל אימת שהוא עובר על פני מצלמה, מאפשרת להתחקות אחר אינספור נתונים שהם בליבת הזכות לצנעת הפרט: אמונותיו, מעגליו החברתיים, חיי האישות שלו, נטייתו המינית, השקפותיו הפוליטיות, האם הוא תומך בשלטון או מתנגד לו, ועוד ועוד (ר' מיכאל בירנהק "פרטיות במשבר – הנדסה חוקתית והנדסת פרטיות" (יתפרסם במשפט וממשל 2020)).

22. השימוש בטכנולוגיה אף מעורר חשש לזליגת מידע שניתן בהסכמה למטרה אחרת, בניגוד לחוק. למשל – אדם נתן תמונתו בהסכמה לצורך רישיון הנהיגה כדי ששוטר יוכל לדעת שהוא אכן הנהג, וקיים חשש שתמונתו תשמש ללא הסכמתו לזיהויו באמצעות הטכנולוגיה בעת שהוא עובר ברחוב.

23. **שנית**, אם הטכנולוגיה מדויקת, וביתר שאת – אם היא לא מדויקת, היא טומנת בחובה **פוטנציאל לפגיעה נרחבת בחירויות היסוד: חופש הביטוי, חופש הדת, חופש ההתאגדות, חופש ההפגנה ואפילו בזכות לחירות**. לטכנולוגיה המאפשרת מעקב מתמשך אחר תנועות של אזרחים אפקט ממשמע וממשטר הגורם לאדם להימנע מפעילויות שונות שהוא חופשי לעשות. אדם שידוע שמהלכיו מנוטרים וחשופים לעיני השלטון ישנה את התנהגותו ואף ייזהר בהתבטאויותיו (על האפקט הממשמע של מעקב ר' בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (מיום 28.5.2012), בפסקה 7; מיכאל בירנהק **מרחב פרטי – הזכות לפרטיות בין משפט לטכנולוגיה** 182 ו-429 (2011)).

24. לא קשה לתאר, למשל, איזה אפקט מצנן יהיה לשימוש בטכנולוגיה לזיהוי פנים אם יעשה בה שימוש בהפגנות, או במצעדי גאווה. מעקב מקיף וכולל עלול להרתיע אנשים מלהשתתף באירועים ציבוריים. הוא יכול לדכא השתתפות במחאות פוליטיות או בקמפיילים למען שינוי חברתי. הוא עלול להחניק התנהגות לא קונפורמית. האפקט המצנן שנוצר מהווה הפרה של חופש האסיפה, חופש ההתאגדות וחופש הביטוי (לעניין האפקט המצנן של מעקב אחר פעילי מחאה ראו פסיקת בית המשפט האירופי לזכויות אדם בעניין **Catt v United Kingdom** (2019) 69 EHRR 7; וראו עוד פס' 10, 61 ו-94 להערה מס' 37 של וועדת האו"ם לעניין האמנה לזכויות אזרחיות ופוליטיות - **General comment No. 37 Article 21: right of peaceful assembly**).

25. הפגיעה בחירות יכולה גם להתרחש כתוצאה מכשל טכנולוגי בזיהוי, כאשר האינדיקציה מבוססת על אלגוריתם, ללא שיקול דעת אנושי. כך, למשל, לא מזמן נרעשה ארה"ב ממעצר שגוי שבוסס על טעות בזיהוי של הטכנולוגיה לזיהוי פנים של משטרת דטרויט. אדם שחור בשם רוברט ג'וליאן בורצ'אק וויליאמס נעצר בחשד לביצוע עבירה של גניבה מחנות, בהתבסס על צילום ממצלמת אבטחה בחנות. לאחר מכן התברר שמדובר היה בזיהוי שגוי של אלגוריתם של טכנולוגיה לזיהוי

פנים, וכי זיהוי שגוי זה היה האינדיקציה היחידה לכך שמר וויליאמס הוחשד בגניבה (ר' כתבה בעניין בניו-יורק טיימס מיום 24.6.2020, Wrongfully Accused by an Algorithm, באתר: <https://nyti.ms/3idc11W>).

26. **שלישית**, השימוש בטכנולוגיה טומן בחובו **פוטנציאל ממשי לפגיעה בשוויון**. הפגיעה עשויה להיגרם מכשלים טכנולוגיים באלגוריתם, כאשר מידע שנאסף עד כה מצביע על הטיות קשות ביכולת הזיהוי של שחורים לעומת לבנים, נשים לעומת גברים. ב 2018 בדק חוקר ב-MIT תוכנות של שלושה יצרנים שונים ומצא טעויות ב 21-25% מהמקרים שבהם נבדקו פנים של אישה עם עור כהה. לעומת זאת, שיעור הטעות בקרב בהירי עור היה פחות מ-1% (Study finds gender and skin-type bias in commercial artificial-intelligence systems בקישורית: <https://bit.ly/33cmnJd>: MIT_News 11.2.2018).

27. מחקר מקיף אחר שערך מכון התקנים האמריקני מצא כי טכנולוגיה לזיהוי פנים סובלת מהטיה מובהקת המובילה לזיהויים שגויים של אנשים ממוצא אפריקני ואסייתי (לדיווח על תוצאות המחקר ר' כתבה בניו-יורק טיימס מיום 19.12.2019: <https://nyti.ms/33jIU8i>).

Face Recognition Vendor Test, National Institute of Standards and Technology Dec.2019
<https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

28. כאשר הטכנולוגיה מהווה בסיס לחקירה משטרתית ההטיה עלולה להוביל לפגיעה בקבוצות מיעוט שונות והפללה שגויה שלהם באופן לא פרופורציונאלי. חשש נוסף הוא משימוש בטכנולוגיה למשטור ומעקב אחר קבוצות מיעוט שונות, ושיטור יתר שלהן, באמצעות הצבת מצלמות המחוברות לטכנולוגיה בשכונות או באזורים המזוהים עם אותן קבוצות מיעוט.

29. **רביעית**, השימוש בטכנולוגיה ללא שקיפות מינימלית מעוררת **סימני שאלה סביב חוקיות השימוש בה**, והיעדר הקפדה על שלטון החוק. הכנסת טכנולוגיה הפוגעת בזכויות חוקתיות מחייבת הסמכה מפורשת בחוק, כמצוות חוק יסוד: כבוד האדם וחירותו, ואם היא נעשית ללא הסמכה כזו על פני הדברים היא לא חוקית. הקפדה על עיקרון החוקיות נדרשת גם כדי להטיל מגבלות על השימוש בטכנולוגיה, למשל – ביחס לצורך בצו שיפוטי, ולהבחין בין שימוש לגיטימי לשימוש פסול. אם הטכנולוגיה מופעלת ללא מסגרת חקיקתית ייעודית שמסדירה את השימוש, הדבר פותח את הדלת בפני אפשרויות של ניצול לרעה, כמו שימוש בתווי הפנים שלנו מבלי לידע אותנו ומבלי לקבל את הסכמתנו.

30. הכנסת לשימוש של הטכנולוגיה ללא הסדרה בחוק עשויה ליצור הלכה למעשה "מסלול עוקף" לעקרונות ולהגבלות שעוגנו **בחוק המאגר הביומטרי** (חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, תש"ע-2009). החוק מסדיר את הפעלתו של מאגר ביומטרי מדינתי במשרד הפנים, ובין היתר, קובע הוראות מיוחדות לעניין השימוש שמותר למשטרה לעשות במאגר המידע הביומטרי. שימוש כזה לצורך זיהוי מותנה בצו שיפוטי, ועמידה בקריטריונים הקבועים בחוק.

31. אמנם, קיים חוק נוסף שמסדיר את השימוש שעושה המשטרה במידע ביומטרי לצרכי חקירה, הלא הוא חוק סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף ונטילת אמצעי זיהוי), תשנ"ו-1996. אלא

שספק רב אם חוק זה אכן מתייחס לשימוש ב-FRT ולבטח שאינו מתיר להשתמש ב-AFR, דהיינו, זיהוי עוברים ושבים בזמן אמת.

32. חקיקה שתעגן ותגביל שימוש בזיהוי פנים היא צו השעה. נשיא מייקרוסופט, בראד סמית, פרסם קריאת השכמה לכל המדינות, שיתעוררו ויקדמו את פני הסכנה שטמונה בפיתוח בלתי מבוקר של טכנולוגיות לזיהוי פנים:

"We believe it's important for governments in 2019 to start adopting laws to regulate this technology. The facial recognition genie, so to speak, is just emerging from the bottle. Unless we act, we risk waking up five years from now to find that facial recognition services have spread in ways that exacerbate societal issues. By that time, these challenges will be much more **difficult to bottle back up.**"

33. נשיא מייקרוסופט הזהיר מפני "מרוץ לתחתית" של יצרני טכנולוגיה מתחרים, שיאלצו לבחור בין אחריות חברתית (פיתוח אחראי של FRT) לבין הצלחה בעסקים. הדרך היחידה לעצור את המרוץ לתחתית היא באמצעות חקיקה, כדי שזו תבטיח תחרות עסקית בריאה ואת שלטון החוק.

34. **חמישית**, שיתוף הפעולה בין המשטרה לבין חברות פרטיות המפתחות את הטכנולוגיה ואולי אף מפעילות אותה עבור המשטרה מעורר חשש בפני עצמו להפרטה של סמכויות שלטוניות, זליגת מידע לגורמים פרטיים, או הפעלת סמכויות שלטוניות רגישות על ידי גורמים הפועלים למטרת רווח.

35. לאור כל האמור, לא יכולה להיות מחלוקת כי השימוש ההולך וגובר בטכנולוגיה כה משמעותית ובעלת פוטנציאל לפגיעה קשה בחירויות הפרט על ידי רשויות השלטון בכלל, ורשויות אכיפת החוק בפרט מחייב דיון ציבורי פתוח, שקוף ורציני. הצעד הראשון וההכרחי לכך הוא לחייב את המשטרה בשקיפות.

36. העותרת הינה עמותה להגנה על זכויות האדם, ארגון זכויות האדם הוותיק בישראל, והיא פועלת קרוב לחמישים שנה ללא מטרת רווח למימוש מטרותיה, ובכלל זה למנוע מרשויות המדינה לפגוע ללא הצדקה בזכויות חוקתיות, ובכלל זה בזכויות לפרטיות, לחירות ולשוויון. מטרת העותרת בבקשת חופש המידע שהגישה ובעתירה זו הינה לאפשר לדיון זה להתקיים, שלא לומר – להתחיל להתקיים.

הפניה למשטרה והסירוב הגורף

37. ביום 22.6.2020 פנתה העותרת בבקשת חופש מידע ביחס לשימוש בטכנולוגיה לזיהוי פנים במשטרה, אך ביום 25.6.2020 השיב רפ"ק יניב ארקוס, קצין מדור תלונות ציבורי ארצי במשטרה, כי "עפ"י התייחסות הגורמים הרלוונטיים, מדובר בבקשה שאינה מתאימה מבחינת היקפה לחופש מידע. אודה לך על צמצום הבקשה על מנת שאלו יבחנו בקשתך ומתן מענה בהקדם".

העתק הבקשה והתשובה מצורפים ומסומנים ע/4 ו-ע/5.

38. לכן ביום 30.6.2020 הגישה העותרת 3 בקשות נפרדות שכל אחת ממוקדת בתחום אחר, **ע/1-3/ע**.
הבקשה הראשונה עניינה בעצם השימוש בטכנולוגיה בשורות המשטרה. הבקשה השנייה עוסקת
בשימוש במצלמות המחוברות לטכנולוגיה, והשלישית – במאגרי תמונות שבידי המשטרה, העשויות
לשמש לצרכי זיהוי פנים.

39. ביום 26.7.2020 דחתה המשטרה את כל הבקשות באופן גורף ולא מסרה אפילו בדל מידע ואף לא
הייתה מוכנה להודות או להכחיש את עצם השימוש בטכנולוגיה לזיהוי פנים.

40. המשטרה נימקה את סירובה בשני טעמים:

ראשית, כי הבקשות לקבלת המידע אינן חוסות תחת חוק חופש המידע, שכן ככל ואכן קיימת מערכת
מעין זו, הרי שתהיה תחת מערכי המודיעין והחקירות, ולפי הוראות סעיף 14(א)(9) לחוק, הוראותיו
לא יחולו על גופים ועל מידע שנוצר, שנאסף או שמוחזק בידי מערכי המודיעין והחקירות של משטרת
ישראל.

שנית, נטען, כי חשיפת המידע המבוקש בבקשות עשויה לספק אינדיקציה באשר לפעילות משטרת
ישראל ובכך לפגום ביעילות עבודתה של משטרת ישראל וכן להביא לחשיפת שיטות פעולה שלה
ובתוך כך לפגיעה בפעולות האכיפה של המשטרה, ומכאן שבהתאם להוראות סעיף 9(ב)(1) לחוק אין
חובה למסור את המידע, שכן הסעיף קובע כי רשות ציבורית אינה חייבת למסור מידע אשר גילויו
עלול לשבש את התפקוד התקין שלה; וכך גם מכוח סעיף 9(ב)(8)(א) לחוק, הקובע כי רשות ציבורית
אינה חייבת למסור מידע על שיטות עבודה של רשות ציבורית העוסקת באכיפת החוק העלול לגרום
לפגיעה בפעולות האכיפה.

העתק תשובה המשטרה מיום 26.7.2020 מצורף ומסומן **ע/6**.

41. ציון הסעיפים הנ"ל מלמד גם כי **גם לעמדת המשיבה אין מדובר** ב"מידע שנאסף או שנוצר לצורכי
חקירה ולגבי מידע מודיעיני", שכן אחרת הייתה מציינת את סעיף 14(א)(8); ואין מדובר במידע
שמקים "חשש לפגיעה בביטחון המדינה, ביחסי החוץ שלה, בביטחון הציבור או בביטחון או בשלומו
של אדם", שכן אחרת הייתה מציינת את סעיף 9(א)(1); ואף אין בחשיפת המידע המבוקש משום
"פגיעה בהליכי חקירה או משפט או בזכותו של אדם למשפט הוגן"; שכן אחרת הייתה מציינת את
סעיף 9(ב)(8)(ב) לחוק.

42. סירוב הגורף של המשטרה לתת כל מידע על השימוש בטכנולוגיה הוא חריג בנוף הבינלאומי.
משטרות רבות בעולם, לא רק שלא מסתירות את השימוש בטכנולוגיה לזיהוי פנים אלא גם מציגות
לציבור מיוזמתן את השימוש שהן עושות בטכנולוגיה.

43. כך, למשל, באתר משטרת ניו יורק יש **דף ייעודי ובו שאלות ותשובות** על השימוש בטכנולוגיה של
משטרת ניו יורק. הדף מפנה את הגולשים גם **לנוהל המפורט** של המשטרה. ור' גם **דיווח בעלון הרשמי**
של משטרת לוס-אנג'לס על הכנסת הטכנולוגיה לשימוש ועל האופן שבה משתמשים בה.

44. באנגליה, משטרת לונדון Metropolitan Police מפרסמת באתר האינטרנט שלה דף מידע ברור ובו השימוש שהיא עושה בטכנולוגיה, וגם הבסיס החוקי לשימוש זה, כולל הנהלים. נוהל המשטרה לשימוש בטכנולוגיה גלוי ומפורסם.

יתרה מזאת, בממשלת בריטניה יש נציב לענייני מצלמות מעקב (פונקציה המזכירה את הרשות להגנת הפרטיות אצלנו), והנציב פירסם במרץ 2019 הנחיה מפורטת אודות הטכנולוגיה והשימוש בה על ידי המשטרות בבריטניה.

Surveillance Camera Commissioner "The police use of Automated Facial Recognition Technology with Surveillance Camera System" (March 2019).

45. לא רק שמשטרות אחרות בעולם חושפות באופן יזום את השימוש שהן עושות בטכנולוגיה, גם מתקיים סביב הנושא דיון ציבורי ער, בתקשורת, בבתי המחוקקים וגם בערכאות שיפוטיות, דיון בו יכול הציבור לקבוע את גבולות הלגיטימיות של השימוש בטכנולוגיה, מתי היא מותרת ומתי לא.

46. למשל, לאחרונה פסק בית המשפט לערעורים בוילס בתביעה שהוגשה נגד השימוש שעושה משטרת דרום וילס בטכנולוגיה. משטרת דרום וילס החלה באופן גלוי ולא חשאי להפעיל פיילוט בו היא צילמה אנשים במרחבים ציבוריים, והתמונות עובדו והשוו בו זמנית למאגר תמונות משטרת דרום וילס. המצלמות הייחודיות שבהן השתמשה משטרת דרום וילס מסוגלות לצלם 50 תמונות פנים בשנייה ואלו עובדים באמצעות מחשב ומושווים למאגר תמונות משטרת דרום וילס. תמונות של אנשים שיש נגדם צו מעצר, תמונות של מי שנמלט ממשמורת, תמונות של חשודים, תמונות של אנשים הזקוקים להגנה, תמונות של אנשים שנדרשים לצרכי איסוף מודיעין, וכדומה. אם יש התאמה, מועברת התראה למשטרה, ואם אין התאמה, התמונה נמחקת מהמאגר. ההערכה היא שצולמו כך מעל חצי מיליון איש, ואחד מהם הוא התובע, באירוע בקרדיף.

בית המשפט לערעורים פסק כי המשטרה הפרה את החוק, שכן הפעילות המשטרתית לא הייתה מבוססת על הסמכה מפורשת דיה בחוק, וכן כי המשטרה לא ערכה תסקיר על הגנת המידע, כנדרש בחוק המקומי, וכן כי לא בחנה את ההטיות של הטכנולוגיה מבחינת מגדר וצבע עור (ר': EWCA Civ [2020] 1058 R (Bridges) -v- CC South Wales).

47. דוגמה זו רק מדגישה עד כמה חשובה השקיפות המשטרתית בשימוש בטכנולוגיה, על מנת לפקח על פעילותה ולמנוע שימוש לא חוקי בטכנולוגיה. וכבר נאמר:

"הנגישות למידע היא תנאי ליכולת הציבורית לפקח על רשויות השלטון, לגבש עמדה מושכלת באשר לפעילותן, לגלות מעורבות בעשייה השלטונית ולקחת חלק בכינונה ובעיצובה של תרבות שלטונית ראויה... היא מאפשרת מימוש זכויות אזרחיות ופוליטיות". אין הציבור יכול להשיג פיקוח אפקטיבי על פעילות הרשות מבלי שיינתן לו מידע רלבנטי לפעולתה, בגדרי שקיפות; אי אפשר לגלות מעורבות בעשייה השלטונית ללא מידע זה; וקשה לראות כיצד יכולים ציבור ופרטים בתוכו להגשים את חרותם הבסיסית וזכויותיהם, מבלי שתינתן גישה למידע הנצבר ברשויות השלטונית השונות" (ר' עע"ם 3908/11 הנהלת בתי המשפט נ' עיתון דה מרקר בע"מ (22.9.2014), בפסקה 22 לחוות דעתה של השופטת ארבל).

תחולת סעיף 14(א)9 על הבקשות מושא העתירה

48. לטענת המשיבה, סעיף 14(א)9 לחוק פוטר אותה מהחובה לחשוף את המידע המבוקש, שכן לטענתה "ככל ואכן קיימת מערכת מעין זו, הרי שתהיה תחת מערכי המודיעין והחקירות", ועל פי הסעיף, הוראות החוק לא חלות על "מערכי המודיעין והחקירות של המשטרה", ועל מידע שנוצר, שנאסף או שמוחזק בידיהם.

49. הפרשנות של סעיף זה צריכה להיות צרה ככל הניתן כדי למנוע מהמשטרה להתחמק מחובתה לחשוף מידע תוך הסתתרות מאחורי סעיף החרגה גורף. ביחס לגופים ביטחוניים חשאיים, כמו המוסד והשב"כ, האיסור הגורף נועד למנוע פגיעה בביטחון המדינה. ביחס לאיסור על קבלת מידע ממערכות המודיעין והחקירות של המשטרה, המטרה של הסעיף לפי דברי ההסבר של הצעת החוק הייתה למנוע מגורמים העוסקים בפשיעה להשיג מידע כדי לקדם את מטרותיהם הבלתי חוקיות, וכך יש להבין את הסעיף. כך נכתב בהצעת החוק:

"תיאורטית היה ראוי כי החוק המוצע יחול על כל הרשויות הציבוריות במדינה ועל כל המידע שבידיהן, עם זאת, אין להתעלם מכך שבפני מדינת ישראל עדיין ניצבות סכנות ביטחוניות של ממש מצד גורמים עוינים, אשר עלולים לנסות לעשות שימוש בחוק המוצע לצרכים העלולים לפגוע במדינה. הניסיון במדינות אחרות מלמד, שגורמים העוסקים בפשיעה עשו ניסיונות להשיג מידע בתחומים הנוגעים לאכיפת החוק, בכדי לקדם את מטרותיהם הבלתי חוקיות. לגבי מידע בעניינים ביטחוניים שונים או בעניינים הנוגעים לאכיפת החוק, קיים חשש, כי עצם מתן מענה למבקש מידע לפיו המידע המבוקש על ידו חסוי, מסתיר את העובדה שאכן קיים מידע, ובכך עלול להיגרם נזק לעניין חיוני ביותר. על כן יש הכרח להוציא גופים מסוימים מתחולת החוק בכדי להבטיח למידע שבידם יתר הגנה" (הצ"ח 2523 מיום 7.3.1996).

50. חריג גורף זה ביחס למערכי המודיעין והחקירות של המשטרה, מערכים העוסקים במגוון רחב ביותר של סוגיות, מעורר קושי כפול, שכן ברור כי לגבי חלק ניכר מהמידע המוחזק בידי מערכים אלו, כלל אין סכנה שיהווה בסיס לקידום מטרות בלתי חוקיות מצד גורמי פשיעה ואין חשש בחשיפתו, ובנוסף, דווקא לגבי מערכים אלו של המשטרה, הפועלים באופן רצוף מול תושבי המדינה, ומול חשודים שעומדת להם חזקת החפות, קיים צורך חיוני של ממש בשקיפות.

51. מכאן שיש לנקוט בפרשנות מצמצמת של סעיף 14 בכלל, ושל החרגה של מערכי המודיעין והחקירות במשטרה במיוחד, כדי לאזן בין התכלית של שקיפות וחופש מידע מצד אחד לבין החשש משימוש לרעה בחוק לקידום מטרות בלתי חוקיות. הצורך בפרשנות מצמצמת כדי להימנע ככל הניתן מפגיעה בחופש המידע עולה גם מקיומה של "שכבת הגנה" נוספת בחוק לצורך המשטרתי למנוע ניצול לרעה של החוק: סעיף 14(א)8 מוציא מתחולת החוק "מידע שנאסף או שנוצר לצורכי חקירה ולגבי מידע מודיעיני", וכן בדמות סעיף 9(ב)8 לחוק המסייג את החובה למסור "מידע על אודות שיטות עבודה ונהלים של רשות ציבורית העוסקת באכיפת החוק, או שיש לה סמכות חקירה או ביקורת או ברור תלונות על פי דין, אם גילוי עולל לגרום לאחד מאלה: (א) פגיעה בפעולות האכיפה או הביקורת או

בירור התלונות של הרשות; (ב) פגיעה בהליכי חקירה או משפט או בזכותו של אדם למשפט הוגן; (ג) גילוי או מתן אפשרות לגלות את קיומו או זהותו של מקור מידע חסוי".

52. דומה כי סעיפים 14(א)(8) ו-9(ב)(8) מזקקים את אותם מקרי ליבה בהם קיים חשש ממשי מחשיפת מידע לגורמים המבקשים לשבש את החקירות נגדם. סעיף 14(א)(9) לעומת זאת מנוסח באופן כוללני וגורף הרבה מעבר לאותם מקרים, ולכן חיוני לפרשו על דרך הצמצום.

53. הדרישה לפרשנות מצמצמת של סעיף 14 התקבלה גם בבית המשפט בעניין **עציון**, שם ציין בית המשפט הנכבד כך:

"אמת נכון הדבר, שהוראת סעיף 14 לחוק מצויה בספר החוקים והיא שרירה וקיימת, חרף ביקורתו של פרופ' סגל עליה, וברי כי יש לפסוק על-פיה. עם זאת, הלכה ברורה היא, שכאשר סעיף בחוק אינו עולה בקנה אחד עם מטרת החוק בכללו, הרי שיש לפרשו פרשנות מצמצמת, ולא להרחיב את תחולתו מעבר למתחייב על-פי לשונו הברורה של הסעיף (ראה א' ברק פרשנות במשפט, כרך א, תורת הפרשנות הכללית, בעמ' 131-132 ופרשנות במשפט, כרך ב, פרשנות החקיקה, בעמ' 84-85)).

גם בלא הפטור הגורף שמעניק סעיף 14 ומעבר לו, מעניק החוק לרשות שלטונית סמכות לסרב להעניק את המידע המבוקש מטעמים אחרים... נוכח דברי הביקורת שהובאו לעיל על סעיף 14 האמור ונוכח כוונת המחוקק ותכליתו הברורה של החוק – אין מקום להחיל פרשנות מרחיבה של סעיף 14, כפי שמבקשת המדינה, ובמיוחד לאור העובדה שהחוק העניק למדינה אמצעים אחרים, כמו אלה שבסעיף 9, כדי להשיג את המטרה של שמירה על ביטחונה או על יתר המטרות שבסעיף 9 לחוק.

ועוד זאת: סעיף 14 לחוק הוא סעיף הפותח פתח שיכול לגרום לעקיפתו של החוק. כפי שמציין פרופ' ברק בספרו פרשנות במשפט, כרך ב, פרשנות החקיקה [8], בעמ' 574, גם עקיפה תמימה, שלא בכוונת זדון, יש למנוע, ויש לפרש חוק באופן המקיים חזקה שתכליתו היא למנוע עקיפתו" (ה"פ (י-ם) 282/00 **עציון נ' סמנכ"ל משרד לביטחון פנים**, פ"ד תשס"א(1), 1 (2000)).

54. ובדומה לזה פסק בית המשפט העליון כי "ככלל, חשוב לחזור ולהזכיר כי כמו בהקשרים אחרים יש להיזהר מפרשנות מרחיבה לחריגים לתחולתו של חוק חופש המידע, שהרי גילוי המידע הוא הכלל ואילו החיסיון הוא החריג לו" (עע"ם 1786/12 **ג'ולאני נ' המשרד לביטחון פנים**, פ"ד סו(3) 362, 382 (2013) (להלן – עניין ג'ולאני)).

55. בעניין אחר, סורבה בקשת המידע, שהגישו קרובי משפחה של מפגעים, על יסוד הפטור המוחלט שבסעיף 14(א)(8), אך בית המשפט קבע כי "יש ממש בטענת העותרים, כי מדובר בטפסים ואישורים סטנדרטיים, הנוגעים להליכי קבורה, ואשר אינם תולדה של הליכי חקירה. מסקנה זו מתחזקת עוד יותר, נוכח הכלל בדבר הפרשנות המצמצמת לסייגים למסירת המידע" (עת"ם (י-ם) 26445-08-16 **המוקד להגנת הפרט נ' משרד הבריאות** (27.3.2018)).

56. גם בחוק האמריקאי, המקביל לחוק חופש המידע, ישנה החרגה של בקשות חופש המידע ביחס למטרה, אך היא מצומצמת ומזכירה יותר את סעיף 9 מאשר את סעיף 14. ההחרגה חלה רק כאשר

חשיפת המידע תפגע בחקירה משטרתית אשר החשוד לא מודע לקיומה של החקירה וסביר להניח שחשיפת המידע תפריע להליך החקירה; כאשר מדובר בחשיפת מקור מודיעיני; החריג השלישי חל רק על ה-FBI ולא על המשטרה הכחולה, והוא עוסק במידע של גורם מודיעיני זר או גורמים העוסקים בסיכול טרור (ר' סעיף 8(C) לחוק חופש המידע האמריקאי, Freedom of Information Act).

57. יתרה מזאת, כאשר למבקש המידע עניין אישי, פרטני, במידע שבחזקת מערך החקירות המשטרתית, כבר נקבע כי זכותו לקבל את המידע צריכה להיות מאוזנת עם האינטרס הציבורי באי חשיפתו. כך, למשל, נפסק שיש לאפשר לנאשמים וחשודים לעיין בחומר החקירה נגדם, אם הם מעוניינים לשנות את סעיף סגירת התיק (בג"ץ 10271/02 פריד נ' משטרת ישראל פ"ד טב(1) 106 (2006)). בדומה נפסק כי עניין אישי בחומרי חקירה לצורך ביסוס טענה של הגנה מן הצדק בשל אכיפה בררנית מצדיק במקרים מסוימים חשיפת מידע על תיקים אחרים, מכוח סעיף 108 לחוק סדר הדין הפלילי (ר' בג"ץ 4922/19 נוה נ' פרקליטות מחוז מרכז (פלילי) (9.12.2019)).

58. גם כשלא מדובר במתן מידע שיש בו עניין אישי, אלא במתן מידע בשל עניין ציבורי, המשטרה בעצמה אינה רואה בכל מידע הקשור למודיעין וחקירות מידע שלעולם אין לגלותו. המשטרה אף חשפה בעבר עשרות נהלי אכיפה במסגרת הידברות עם הסניגוריה הציבורית, והיא חושפת מפעם לפעם מידע המתבקש לא רק על ידי גורמים פרטיים במסגרת זכות העיון הפרטנית שלהם, אלא גם במענה לבקשות חופש מידע מכוח החוק ואף בפרסומים מטעמה (למשל – המשטרה מסרה נתונים אודות מעצרים וכתבי אישום שהוגשו בשנים 2018 ו-2019 נגד תושבי ירושלים המזרחית בכלל ונגד תושבי שכונת עיסאווייה בפרט במענה לעתירת העותרת (ר' עת"ם 70983-01-20 האגודה לזכויות האזרח בישראל נ' המשטרה (14.8.2020)).

59. זאת ועוד – סעיף 14 כורך יחד את השב"כ ואת מערכי המודיעין והחקירות של המשטרה וגורמים נוספים, שדינם שונה, וקיימת חשיבות בפיתוח תורת פרשנות מורכבת. כאשר מדובר על השב"כ, או על יחידות ביטחוניות הפועלות תחת אחריותו, ניתן להבין את הגיונה של דרישת החיסיון הרחב המתבטאת בסעיף 14 לחוק חופש המידע. השב"כ גוף חשאי הפועל על בסיס מידע מודיעיני חסוי למטרות של ביטחון המדינה, המפורטות בחוק השב"כ. מיקוד הפעילות שלו היא בגורמים העוינים למדינה, וייתכן ואין מנוס מהקפדה על חשאיות גם בעת אכיפת החוק על ידי השב"כ וזרועותיו. גם הפיקוח עליו ועל האמצעים שלו הוא חשאי. זהו מחיר כבד בשקיפות, שכציבור אנו משלמים ככורח המציאות (ר' למשל עת"ם (ת"א) 1555/06 התנועה לחופש המידע נ' רשות שדות התעופה (מיום 12.11.2006) (עתירה שבה נתבקש מידע על נהלי הבידוק של השב"כ בנתב"ג והיא נדחתה על בסיס סעיף 14, רק לאחר שחלק מהמידע כן נמסר לעותרת).

60. לעומת זאת, המשטרה היא גוף אזרחי נתון לפיקוח הפועל לפי כללים מפורסמים, פקודות ונהלים. אלו חושפים מטיבם את אמצעי המשטרה ויכולותיה. כך, למשל, קובע חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007 את המסגרת החוקית שלפיה יכולה המשטרה לקבל נתוני תקשורת מחברות התקשורת, ואף אחד לא העלה על דעתו שיש להטיל מטה חשאיות על החוק, שמא עבריינים ידעו כי ביכולתה של המשטרה לאכף את מיקומם אם יסתובבו עם טלפון נייד. בדומה לזה, אין להעלות על הדעת שהמשטרה הייתה מונעת מידע על עצם השימוש שהיא עושה

בהאזנות סתר או בנתונים גנטיים. לבטח שכך הוא בעידן שבו מתקיים דיון משפטי וציבורי אפילו על אמצעי המעקב של שירות הביטחון הכללי (ר' בג"ץ 2109/20 שחר בן מאיר ואח' נ' ראש הממשלה (26.4.2020)).

61. כעניין של שגרה מועבר חומר חקירה לחשודים העומדים למשפט, ובכלל זה מועברת תמונה מקיפה ביותר של אמצעי הפעולה של המשטרה, טכנולוגיות שבידה, נהלים תרגילי חקירה ועוד. רק במקרים חריגים המשטרה פועלת לקבל חסיון על חומרי חקירה. ברור כי מעצם קיומם של משפטים פליליים בישראל נחשפת בפני גורמים רבים ומגוונים תמונה נרחבת של עבודת המשטרה, האופן שבו היא אוספת מודיעין והאופן שבו היא חוקרת פשעים, לרבות טכנולוגיות שהיא עושה בהן שימוש.

62. כבר אירעו מקרים בהם התברר שהמשטרה הסתירה מידע ללא צורך מבצעי. כך, לדוגמה, בעניין נגדי, ביקש נאשם לעיין בנוהל "השוואת עקבות נעליים וצמיגים" של אגף החקירות והמודיעין (מס' נוהל 370.39.00). המשטרה התנגדה לבקשה וטענה, כי לא מדובר בחומר חקירה שיש לנאשם זכות לקבלו. לאחר שהשופט עיין בנוהל במעטפה סגורה והתברר שמדובר בנוהל שנרשם עליו כי "נוהל זה הותר לעיון הציבור" טענה המשטרה, כי היה על הנאשם לעתור לקבלו לפי חוק חופש המידע. ניתן רק לנחש כי פניה כזו הייתה נתקלת בחומה הבצורה של סעיף 14 לחוק. למרבה המזל, השופט הורה להעביר את הנוהל לידי הנאשם וקבע, כי "באופן עקרוני, ניתן היה לומר כי ראוי ונכון היה שנוהל זה יהיה נגיש במרשתת לעיון הציבור, כפי שמונגשים אין סוף נהלים של גופים שונים, פרטיים וציבוריים, בכללם גם של רשויות האכיפה בכלל, ומשטרת ישראל בפרט" (ר' ת"פ 19-01-36741 מדינת ישראל נ' נגדי (החלטה מיום 5.12.2019)).

63. מכאן שהתפיסה כאילו קיים אינטרס ציבורי חיוני בהטלת ערפל מוחלט על מערכי המודיעין והאכיפה של המשטרה, בדומה לשב"כ, היא תפיסה המעוררת קושי רב, ואין לה אחיזה במציאות.

64. כדי ליישב בין סעיף 14(א)(9) לחוק לבין הזכות למידע והאינטרס הציבורי באור השמש כגורם מחטא, יש צורך בפרשנות מצמצמת. על כן ראוי לקבוע כי רק כאשר המידע מוחזק באופן בלעדני בידי מערכי המודיעין והחקירות חל סעיף 14(א)(9), ולעומת זאת, כאשר מדובר במידע המוחזק בידי גורמים רבים במשטרה, הסעיף לא יחול. כך פסק בית המשפט הנכבד בעניין עציין:

"עולה מן המקובץ, שיש לקבוע כי סעיף 14 אינו מוציא מתחולתו של החוק עניינים הנוגעים באופן כללי לעבודת אחד הגופים החוסים בצלו, אלא רק מידע שנוצר, נאסף או מוחזק באופן בלעדי על-ידי אחד הגופים הללו.... כאשר מידע נוצר בידי גוף שאינו חסוי ומוחזק בידי שתי רשויות שלטוניות – האחת חסויה והשנייה אינה חסויה – לא ייהנה המידע מחיסוי אוטומטי, ואם ברצונה של הרשות השלטונית השנייה לסרב לבקשתו של האזרח ליתן לו את המידע המבוקש, עליה להצביע על אחד הטעמים המנויים בסעיפים 8 או 9 לחוק, או לדאוג לכך שתוצא תעודת חיסיון על-פי סעיף 44 לפקודת הראיות... אכן, ברוב המקרים שבהם המידע נוגע לפעילותו של גוף חסוי, הרי הוא נוגע גם לביטחון המדינה או ליחסי החוץ שלה, ואז נתונה הרשות לרשויות המדינה לסרב, מטעמים ענייניים, למסור את המידע האמור – אם מתקיים אחד מן הטעמים שבסעיף 9 לחוק. ואולם, בכך בלבד שגוף חסוי היה מעורב בכל צורה שהיא בדיון מסוים, אין כדי להוציא את כל הדיון, על כל היבטיו, מתחולת החוק".

65. לעניין זה המשיבה לא ביססה את הטענה כי המידע המבוקש מוחזק רק על ידי מערכי המודיעין והחקירות. למעשה – המשיבה אף לא הסכימה להודות האם בכלל היא משתמשת בטכנולוגיה לזיהוי פנים או שוקלת להשתמש בטכנולוגיה זו. המשיבה טוענת כי "ככל ואכן קיימת מערכת מעין זו, הרי שתהיה תחת מערכי המודיעין והחקירות". עמימות מכוונת זו מייצרת "ספק" שעובד לטובת העותרת (ר' קביעה דומה בעניין **ג'וליאני** בעמ' 382).

66. ברור כי מידע על עצם השימוש בטכנולוגיה חדשה אינו מוחרג מחוק חופש המידע, גם אם הטכנולוגיה תשמש בסופו של דבר גם את מערך המודיעין והחקירות. מדובר בהחלטה אסטרטגית של המשטרה לרכוש את הטכנולוגיה או לפתח אותה, ולכן המידע לגביה קיים במטה הראשי, במינהל הטכנולוגיות ובמינהל הרכש, במחלקה המשפטית שמעורבת מן הסתם בנהלי ההפעלה של הטכנולוגיה, ואם הטכנולוגיה משמשת לחקירות, הרי שתוצריה יועברו למחלקת התביעות ולפרקליטות כדי לבסס אשמה בתיקים פליליים. מכאן שהמידע אודות טכנולוגיה לזיהוי פנים במשטרה אינו מוחזק באופן בלעדי במערך המודיעין והחקירות, ולכן המשטרה אינה פטורה באופן גורף ממתן המידע.

התייחסות לנימוקים נוספים לאי מתן המידע

67. בעוד שסעיף 14(א)9 היה הנימוק המרכזי להחלטתה שלא לגלות את המידע המבוקש, המשיבה מפנה גם לסעיף 9(ב)1 לחוק, שלפיו אין היא חייבת למסור מידע, שגילויו עלול לשבש את התפקוד התקין שלה; וכן גם לסעיף 9(ב)8(א) לחוק, הקובע כי רשות ציבורית אינה חייבת למסור מידע על שיטות עבודה של רשות ציבורית העוסקת באכיפת החוק העלול לגרום לפגיעה בפעולות האכיפה. המשיבה נימקה בקיצור רב כי לעמדתה חשיפת המידע המבוקש בבקשות עשויה לספק אינדיקציה באשר לפעילות משטרת ישראל ובכך לפגום ביעילות עבודתה של משטרת ישראל וכן להביא לחשיפת שיטות פעולה שלה ובתוך כך לפגיעה בפעולות האכיפה של המשטרה. להלן נראה, שנימוקים אלה אינם משכנעים כלל, וחולשתם מקרינה גם על הניסיון להידחק בצלו של החריג שבסעיף 14 לחוק.

68. אין מחלוקת באשר למעמדה של הזכות לקבלת מידע מרשות ציבורית כאחת מזכויות היסוד במשטר דמוקרטי. לכן, קובע חוק חופש המידע בבסיסו כי נקודת המוצא היא גילוי המידע, תוך שעל הרשות לערוך איזונים מול אינטרסים שונים, בהתאם לסייגים הקבועים בחוק ולכללי המשפט המנהלי (ר' עע"מ 1704/15 **האוניברסיטה העברית נ' העמותה למדע מוסרי**, בפיסקה 18 (18.7.2017); עע"מ 10014/16 **יש דין נ' המינהל האזרחי איו"ש**, בפיסקה 5 לחוות דעת השופטת ברון (16.5.2019)).

סעיף 9(ב)1

69. הגבלת מידע על בסיס סעיף 9(ב)1, תיעשה רק במקרים שבהם קיימת ודאות קרובה לפגיעה ממשית באינטרס הרשות. זהו לא סעיף שמעניק פטור גורף מהחובה למסור מידע. ההלכה הנוהגת היא כי יש לפרש את הגבלת מסירת המידע בצמצום. כך, למשל, הסביר בית המשפט:

"הוראת סעיף 9(ב)1 – לשונה רחבה וכוללנית. ההוראה מתירה לרשות הציבורית שלא למסור מידע 'אשר גילויו עלול לשבש את התפקוד התקין של הרשות הציבורית או את יכולתה לבצע את תפקידיה'. בצדק נאמר על הוראה זו, כי היא 'פותחת שער לשיבושה של הזכות לקבלת מידע עצמה'... פרשנות הסעיף צריכה,

אפוא, להתאים עצמה לאמות המידה המנחות את החוק ולעקרונות הכלליים והחוקתיים המקובלים במשפטנו. כלל ידוע ומושרש הוא במשפטנו, כי בהתנגשות בין זכות חוקתית מוגנת לבין אינטרס ציבורי, גובר האחרון על הראשונה רק במקום בו קיימת הסתברות ראויה – לרוב, 'ודאות קרובה' – לפגיעה ממשית באותו אינטרס ציבורי... הנוסחה שהתגבשה בפסיקה הענפה בנוגע לחופש הביטוי ולמגבלותיו נכונה גם לענייננו. עמד על כך פרופ' א' ברק, בציינו: '...האם כל שיבוש בתפקידה של הרשות מצדיק מניעת מסירתו של מידע? דומה שהתשובה הינה כי בגדרי האיזון החיצוני ועל רקע תכליתו של החוק, רק שיבוש קשה, רציני וחמור אשר הסתברות התרחשותו היא ודאות קרובה, מאפשר מניעת מידע' ... אכן, קיים אינטרס ציבורי חשוב בשמירה על תקינות פעולתה של הרשות הציבורית, אולם רק מקום בו קיימת ודאות קרובה לפגיעה באינטרס זה – תקום עילה מספקת להגבלת חופש המידע, כמרכיב של חופש הביטוי. ודוק: מקום בו ניתן להפחית את הפגיעה בתקינות פעולתה של הרשות, מבלי לאיין את חופש המידע – מוטב וראוי לעשות כן. ההגבלה על חופש המידע היא בבחינת אמצעי אחרון, וחובה היא על הרשות הציבורית, בטרם תחליט שלא למסור מידע שגילוי מתבקש, לבחון אמצעים שפגיעתם בחופש המידע – פחותה" (עע"ם 6013/04 **משרד התחבורה נ' חברת החדשות הישראלית**, פ"ד ס(4) 60, 86-87 (2006); לעניין זה ראו גם: זאב סגל הזכות לדעת באור חוק חופש המידע 199 (2000); אהרן ברק "חופש המידע ובית-המשפט" קריית המשפט ג 95, 103-102 (2003); יונתן ארבל ותהילה שוורץ-אלטשולר **מידע רוצה להיות חופשי: הטמעת חוק חופש המידע בישראל** 188-186 (2008).

70. המשיבה לא הציגה נימוק כלשהו מדוע חשיפת המידע המבוקש ייפגע **בוודאות קרובה** בעבודת המשטרה, וכפי שצינו לעיל - משטרות רבות בעולם חשפו את השימוש בו הן עושות בטכנולוגיה. למצער היה על המשיבה לציין בפירוט איזה פרט מהמידע המבוקש מעורר לעמדתה חשש ברמה של קרוב ודאי לפגיעה בתפקוד התקין של הרשות.

סעיף 9(ב)(8)(א)

71. על פי סעיף זה רשות העוסקת באכיפת החוק אינה חייבת למסור מידע על אודות שיטות עבודה ונהלים, אם גילוי עולל לגרום לפגיעה בפעולות האכיפה. סעיף זה לא יכול להצדיק את תשובת המשטרה לבקשה, שכן חלק גדול מהמידע המבוקש אין בו לפגוע בפעולות אכיפה מסוימות, אלא מידע כללי על השימוש בטכנולוגיה, על התקשרויות עם גורם חיצוני, על מאגרי התמונות שמשים את המשטרה, על האופן שבו הטכנולוגיה מיושמת, נבחנת ומפוקחת וכדומה.

72. כדי לטעון לסמכות להסתיר מידע מהציבור על המשטרה לנמק איזה פרט מהמידע שנתבקש יפגע בפעולות אכיפה, וכיצד, אך פירוט כזה לא נמסר, וכפי שנפסק: "רשות ציבורית אינה רשאית להסתפק בסירוב לקוני לבקשה למסירת מידע ועליה לפרט את הטעמים לכך, על מנת לאפשר למבקש המידע לעמוד על טעמים אלה ולשקול את מהלכיו. פירוט הטעמים לסירוב מאפשר גם לבית המשפט לעמוד על השיקולים ששקלה הרשות ועל האיזון הפנימי שערכה ביניהם, בהעבירו את ההחלטה תחת שבט ביקורתו" (ר' עע"ם 9738/04 **המועצה להשכלה גבוהה נ' הוצאת עיתון הארץ** (19.12.2006)).

החובה להפעיל שיקול דעת למסירת מידע גם אם סעיפים 14 או 9 לחוק חופש המידע חלים

73. החוק קובע שגם לגבי מידע שאין חובה למסור, ואף אם אסור למסור אותו לפי סעיפים 8 ו-9 לחוק, הרשות צריכה בכל זאת לשיקול את מסירת המידע, ולו באופן חלקי, מכוח סעיפים 10 ו-11 לחוק.
74. סעיף 10 מדגיש את העניין הציבורי במידע כשיקול מכריע למסור מידע גם אם קיים טעם לא למסור אותו. בענייננו לא יכולה להיות מחלוקת שיש עניין ציבורי מובהק בשקיפות בשימוש בטכנולוגיה, שכפי שמוסבר במבוא עתירה, שנויה במחלוקת ציבורית ויש לה השלכות מרחיקות לכת על זכויות יסוד ועל ביטחון הציבור.
75. סעיף 11 לחוק מחייב את הרשות, גם אם יש לה עילה לא למסור את המידע, למסור אותו בכל זאת תוך השמטת פרטים, תוך עריכת שינויים או תוך התניית תנאים בדבר דרך קבלת המידע והשימוש בו.
76. בתשובה הלקונית של המשטרה לא ניתנה הדעת לסעיפים 10 ו-11 ולא ניתן כל נימוק מדוע לא תפעל המשטרה על פיהם. זה בפני עצמו מחייב התערבות בהחלטה.
77. הגם שסעיפים 10 ו-11 מתייחסים לסעיפים 8 ו-9, יש לחייב את המשיבה לשיקול שיקולים דומים גם ביחס למידע שאין למסור מחמת סעיף 14, היינו – שמדובר בגורם שהחוק לא חל עליו.
78. החוק אינו יוצר הסדר שלילי לגבי חשיפת מידע בהתבסס על מקורות אחרים ואם החוק לא חל, אין זה אומר שלא מוטלת על הרשות חובה לשיקול את מסירת המידע מכוח דיני המשפט המינהלי הכלליים, ודיני השקיפות, והחלטה על אי מסירת מידע, ככל החלטה מינהלית, נתונה לביקורת על פי כללי המשפט המינהלי – סבירות, מידתיות וכדומה. לכן מי שבידו בקשה לחוק חופש המידע מהרשות, שסעיף 14 חל לגביה, שמורה לו הזכות לקבל התייחסות לדרישה גם מכוח חוק חופש המידע וגם מכוח דיני המשפט המינהלי. יפים לעניין זה דבריו של המשנה לנשיאה רובינשטיין:

"העובדה שאין חובה להעביר את המידע מכוח חוק חופש המידע, אין בה כדי לומר כי הרשות אינה רשאית לעשות כן; ראו לעניין זה את הדברים שהביאה השופטת ברק ארז בדבר מדיניות ה"גילוי מרצון" (voluntary disclosure), דהיינו שלא מכוח חובה חוקית, הנהוגה בהקשרים מסוימים בארצות הברית... נוכח חשיבותה של זכות הציבור לדעת לקיומו של משטר דמוקרטי תקין, ייטיבו הרשויות השונות אם יטמיעו כאמור את עקרונות השקיפות, ויאיילו למסור מידע מבוקש ככל שביטחון המדינה מאפשר זאת, גם אם חוק חופש המידע אינו מחייב לעשות כן. ניתן, והדברים ידועים, לערוך פרפרוזות המאזנות בין חופש המידע לבין צרכי הביטחון. וכמובן, השב"כ, ככל רשות אחרת ציבורית אחרת, הוא נאמן הציבור; ועל פני הדברים, ובזהירות המתבקשת אולם מהיכרות מקרוב עם המאטריה, לא אחת – לא בשמים היא **מסירת מידע בגדרי האיזון, וזאת גם אם אין במקרה נתון חובה סטטוטורית** לעשות זאת מכוח חוק חופש המידע. יהא כלל זה נקוט בדינו: **ככל שבידי הרשות לשתף את הציבור במידע, עליה לעשות כן**, בין על פי דין בין על פי שיקול דעת ועל פי השכל הישר. נהוג לדבר על אמון הציבור; זהו כמובן מושג עמום ולעתים חמקמק, אך **עדיף עשרת מונים גילוי יזום על**

**הידרשות מאוחרת להדלפות וסחרור... " (דנ"ם 8020/15 האגודה לזכויות האזרח
בישראל נ' משרד ראש הממשלה (החלטה מיום 8.6.2016)).**

79. מכאן שלמשיבה יש שיקול דעת למסור את המידע, גם אם לדעתה היא אינה חייבת לעשות זאת מכוח חוק חופש המידע, ושיקול דעת זה נתון לביקורת שיפוטית. אכן, ניתן לטעון כי כל אימת שהרשות משתכנעת, שחל סעיף 14 לחוק, נסתם הגולל על הבקשה, ועמה גם על סמכותו של בית המשפט לעניינים מנהליים. אך עמדה מעין זו - אין בה לא הגיון ולא יעילות. שהרי ממילא יהיה על הרשות לשקול את מסירת המידע גם שלא על פי החוק. השאלה היחידה היא אפוא זו: האם במקרה שסעיף 14 פוטר את הרשות מתחולת החוק, נסגרת הדלת בפני עתירה מינהלית, ועל מבקש המידע לפנות לבג"ץ בעתירה שלא מכוח חוק חופש המידע, ולבקש ממנו להעמיד בביקורת שיפוטית את ההחלטה. העותרת סבורה שלא.
80. המחוקק ביקש להעביר את נושא חופש המידע בכללותו לערכאה המנהלית, בדרך יחיד, כדי להוציא את הצורך של בית המשפט העליון בשבתו כבית משפט גבוה לצדק להידרש להחלטות מנהליות בנוגע לבקשות הנוגעות לחשיפת מידע, שאינן מסוג הנושאים שנחוץ שבג"ץ יידרש להם כערכאה ראשונה במותב תלתא.
81. יתרה מזאת, פעמים רבות קיימת מחלוקת עובדתית או ראייתית שמחייבת בירור בערכאה המנהלית כדי לדעת האם סעיף 14 חל או לא. למשל - כאשר לא ברור האם הגוף המחזיק במידע פטור מהוראות החוק או לא. לא סביר שמי שמעוניין בביקורת שיפוטית יידרש להגיש שני הליכים מקבילים לשתי ערכאות - לערכאה המנהלית כדי לחלוק על הקביעה שסעיף 14 חל, ולבג"ץ כדי לטעון שאם הסעיף כן חל, עדיין יש לבחון לתת המידע מכוח כללי המשפט המנהלי. מדובר בדרישה לא הגיונית ולא יעילה, לא לעותר, לא לרשות ולא למערכת בתי המשפט, והיא עלולה לבזבז זמן שיפוטי יקר ואף להוביל לקביעות סותרות.
82. לכן יש להבהיר כי שיקול הדעת של רשות המתבקשת למסור מידע לא מסתיים אם היא סבורה שסעיף 14 חל, אלא עליה לשקול את מתן המידע חרף תחולת הסעיף. החלטה זו כפופה לביקורת שיפוטית של בית המשפט לעניינים מנהליים.
83. עמדה זו לא רק הגיונית ויעילה יותר, אלא מתבקשת מכוח סעיף 11 לחוק אשר קובע מסגרת בתוך החוק, להפעלת שיקול דעת נוסף כאשר הוראות החוק פוטרות את הרשות ממתן המידע, ואף כאשר מדובר במידע שאסור למסור! קל וחומר במידע שאין חובה למסור. שיקול דעת זה צריך לחול גם על מידע שמסירתו אינה מתחייבת מכוח סעיף 14 לחוק, שכן סעיף 9(א)(4) לחוק מתייחס במפורש למידע אשר אין לגלותו על פי כל דין.
84. במילים אחרות, אם המשיבה סברה שסעיף 14 חל על המידע המבוקש, כלומר - שהמידע שהתבקש הוא מידע שאין לגלותו מכוח כל דין, כלשון סעיף 9(א)(4), היה עליה בכל זאת לשקול למסור את המידע, ולו באופן חלקי, מכוח סעיף 11.

85. אם הפעילה הרשות שיקול דעת והחליטה לא למסור את המידע עליה לנמק את תשובתה, והיא אינה יכולה להסתפק בהפניה לסעיף 14 או לסעיף 9. החלטה זו נתונה לביקורת שיפוטית של בית המשפט לעניינים מנהליים. כמובן שגם מחדלה של הרשות להפעיל שיקול דעת מכוח סעיף 11 הינה "החלטה" הנתונה לביקורת של בית המשפט הנכבד (ר' סעיף 2 לחוק בתי המשפט לעניינים מנהליים הקובע כי החלטה של רשות" - החלטה של רשות במילוי תפקיד ציבורי על פי דין, **לרבות העדר החלטה וכן מעשה או מחדל**".

86. **מהכלל אל הפרט** – העותרת סבורה כי סעיף 14(א)(9) לא חל על בקשתה, ויש לפרש אותו הצמצום, אבל אם סעיף 14 כן חל, היה על המשיבה לשקול בכל זאת את מתן המידע מכוח סעיף 11 לחוק. משלא עשתה זאת הרשות, החלטתה היא שלא כדין, ויש לחייבה לתת את המידע ולמצער, לחייבה על לשקול מחדש את מתן המידע, ולו באופן חלקי.

87. אם הפעילה המשיבה שיקול דעת מכוח סעיף 11 היא לא נתנה לכך ביטוי בהנמקתה, והעותרת שומרת לעצמה את הזכות להוסיף טענות בעניין, אך כבר עתה נעמוד על כמה מהשיקולים שהיה על המשיבה לשקול.

87.1. היה על המשיבה לתת משקל לחשיבות העליונה בחשיפת טכנולוגיות בהם היא עושה שימוש, טכנולוגיה שיש בה פוטנציאל מובהק וברף הגבוה לפגיעה בפרטיות ובצנעת הפרט, בחירות ובשוויון. פוטנציאל זה לא רלוונטי רק לחשודים אלא גם לחפים מפשע, ולמעשה לכל הציבור שומר החוק בכללותו שמושפע מהפעלת הטכנולוגיה.

87.2. היה על המשיבה לתת משקל רב לאינטרס הציבורי של שקיפות המשטרה, שהיא תנאי לשמירה על שלטון החוק בגוף בעל סמכויות ניכרות, ולשמירה על אימון הציבור. ללא שקיפות נוצר חוסר אמון בפעילות המשטרה ובחוקיות האמצעים שלה, וקיים חשש לשימוש פסול או לא חוקי בטכנולוגיה, שכן אור השמש הוא המחטא הטוב ביותר.

87.3. היה על המשיבה לתת משקל רב לכך שחשיפת המידע, ולמצער – חלקו, יאפשר דיון ציבורי אודות הטכנולוגיה, טיבה ויעילותה. דיון זה הינו דיון עקר אם המשטרה פועלת במחשכים ולא חושפת את השימוש בטכנולוגיה. בהיעדר שקיפות נרמס חופש הביטוי, שכן קשה להתנגח עם ספינקס.

87.4. מנגד נראה שניתן משקל מופרז לאינטרס המשטרה בהגנה על המידע, כאשר משטרות רבות ברחבי העולם חושפות מיוזמתן את השימוש שהן עושות בטכנולוגיה, ואת הנהלים שמנחים אותן, ובמקומות רבים השימוש בטכנולוגיה מבוסס על חקיקה ראשית מפורשת.

סיכום

88. אם יש אמת בפרסומים על כך שמשטרת ישראל עושה שימוש בטכנולוגיה לזיהוי פנים, יהיה זה בלתי נתפס שהציבור לא ידע מכך, שלא ייערך דיון ציבורי בנושא, ושהכל ייעשה במחשכים וללא שקיפות. מדובר בטכנולוגיה ששימוש מוגבל, מפוקח וראוי עשוי להניב רווח לאינטרס הציבורי במיגור הפשיעה, ובטיוב עבודת המשטרה. אולם שימוש נרחב, לא מפוקח ולא ראוי בטכנולוגיה עשוי לתת

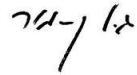
בידי המשטרה כח עצום לבלוש ולעקוב אחר אזרחים תמימים, ולא יעלה על הדעת במדינה דמוקרטית מתוקנת שכוח כזה לא יינתן לפי חוק מפורש, ותחת פיקוח ציבורי.

89. הניסיון של המשטרה לחמוק מהדרישה לשקיפות הוא לא חוקי, וגם לא סביר שהמשטרה תסתיר לחלוטין את המידע בנושא, ולא תעשה מאמץ לפרסם את המידע ולו באופן חלקי. זה גם חורג בצורה קיצונית ממה שעושות משטרות אחרות בעולם.

90. לבית המשפט סמכות להתערב בהחלטה, ולקבוע שלא ניתן להשתמש על דרך הסתם בסעיף 14 לחוק כדי להתחמק משקיפות, וכי בכל מקרה על המשיבה קיימת חובה לשקול את מתן המידע גם מכוח סעיף 11 לחוק.

מכל האמור, מתבקש בית המשפט הנכבד להורות כמבוקש בעתירה.

21 בספטמבר 2020



גיל גן-מור, עו"ד

ב"כ העותרת