

העותרת: האגודה לזכויות האזרח בישראל (ע"ר 580011567)

ע"י ב"כ עוה"ד רוני פלי ו/או דן יקיר ו/או אבנר פינצ'וק ו/או
עודד פלר ו/או שרון אברהם-ויס ו/או גיל גן-מור ו/או גדיר
ניקולא 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 סנא אבן ברי
ו/או רעות שאער

מהאגודה לזכויות האזרח בישראל

נחלת בנימין 75 תל אביב 65154

טל': 054-4502944 ; פקס: 03-5608165

דוא"ל: roni@acri.org.il

- נגד -

המשיב: הממונה על יישום חוק חופש המידע בצה"ל

באמצעות פרקליטות מחוז ירושלים (אזרח)

עתירה מינהלית

בית המשפט הנכבד מתבקש להורות למשיב למסור לעותרת את המידע שביקשה מכוח חוק חופש המידע, שעניינו השימוש שעושה צבא ההגנה לישראל (להלן – **צה"ל** או **הצבא**) בטכנולוגיה לזיהוי פנים בשטחים הנתונים לשליטתו בגדה המערבית (להלן – **השטחים** או **הגדה המערבית**).

הבקשה מצורפת ומסומנת ע/1.

להלן טעמי העתירה:

רקע – טכנולוגיה לזיהוי פנים

1. עניינה של העתירה בסירובו הגורף והמוחלט של הצבא לחשוף כל פרט על השימוש שהוא עושה **בטכנולוגיה לזיהוי פנים** בגדה המערבית (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 כזה 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, מאגר היתרי הכניסה לישראל) 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 או הצבא.
11. צה"ל מעולם לא הודה שהוא עושה שימוש בטכנולוגיה זו בשטחים, למרות שלפי כתבה שפורסמה באתר The Marker ביולי 2019, ולפי כתבה נוספת שפורסמה ברשת NBC, באוקטובר 2019, הטכנולוגיה של חברת AnyVision משמשת את כוחות הביטחון למעקב אחר פלסטינים בגדה המערבית וגם ברחובות ירושלים המזרחית, שם חל החוק הישראלי. הכתבה ברשת NBC 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>

<https://www.themarket.com/technation/premium-1.7497279>

12. לא קשה להבין מדוע גורמי הביטחון בגדה המערבית, ובכללן, הצבא, ירצו בטכנולוגיה זו, אשר יש לה פוטנציאל לשרת את מטרותיהם. הטכנולוגיה יכולה לטייב את עבודתם ולקדם את המטרות הביטחוניות שבאחריותם. אך בה בעת, לשימוש בזיהוי פנים יש פוטנציאל מסוכן ביותר לפגוע בזכויות יסוד של תושבים פלסטינים ושל אזרחים ותושבי קבע ישראלים הגרים בהתנחלויות, בירושלים המזרחית או נעים בשטח הנתון לשליטת הצבא, פוטנציאל הגובר לאין ערוך כאשר הטכנולוגיה מוכנסת לשימוש ללא פיקוח ושקיפות.

13. מטבע הדברים השימוש בטכנולוגיה הזו מעוררת חששות כבדים, שנמנה כאן בקיצור רב:

14. ראשית, הטכנולוגיה, אם היא מדויקת, היא טומנת בחובה פוטנציאל לפגיעה אדירה בזכות החוקתית לפרטיות ולצנעת הפרט וביכולת של אזרחים ותושבים מוגנים לשמור על אנונימיות במרחב הציבורי.

15. כאן המקום לציין, כי במשפט הישראלי מעוגנת הזכות לפרטיות בסעיף 7 לחוק יסוד כבוד האדם וחירותו. לפי הפסיקה, מאות אלפי אזרחים ישראלים, שגרים בהתנחלויות נהנים מהגנות חוקי היסוד, וגם הם עלולים להיפגע מהשימוש בטכנולוגיה. כך גם לגבי תושבים ישראלים בירושלים המזרחית. הפלסטינים תושבי הגדה המערבית אינם נהנים מהגנה של חוק היסוד, מאחר שתחולתו בשטחים נותרה בפסיקה בצריך עיון (ראו בג"ץ 1661/05 המועצה האזורית חוף עזה נ' כנסת ישראל (9.6.2005)). עם זאת, המפקד הצבאי כפוף לדין הישראלי ולהגבלות שהדין מטיל על פעולות השלטון.

16. שטח הגדה המערבית, אליו מתייחסת בקשת חופש המידע, נתון תחת משטר כיבוש של ישראל מזה למעלה מ-50 שנה. המסגרת המשפטית המסדירה את הכיבוש הישראלי בשטחים הינה דיני התפיסה הלוחמתית (Law of Belligerent Occupation) המהווים חלק מהדין הבינלאומי ההומניטארי. במסגרת שליטתו בשטח כבוש חב המפקד הצבאי חובות הגנה וזהירות מיוחדות כלפי האוכלוסייה האזרחית, הנתונה תחת שליטתו. בנוסף, חלות במקביל הגנות בסיסיות שנובעות מדיני זכויות האדם במשפט הבינלאומי (על תחולת דיני זכויות האדם ראו **International Court of Justice, Legal**

**Consequences of the Construction of a Wall in the Occupied Palestinian Territory,
 ((2004) Advisory Opinion**

17. סעיף 17 לאמנה בדבר זכויות אזרחיות ופוליטיות (1966) קובע שחל איסור פגיעה שרירותית או בלתי-חוקית בפרטיות. הטענה שהאמנה חלה על פעולות ביון ומעקבים היא יחסית חדשה, אולם בעשור האחרון מתייחסים לאמנה כאל מקור לזכות לפרטיות. ב-2016 האו"ם אימץ גרסה חדשה של הזכות לפרטיות בעידן הדיגיטלי, לפיה מעקבים המוניים ובלתי מאובחנים מהווים הפרה של סעיף WATERS, BENJAMIN G. "AN INTERNATIONAL RIGHT TO PRIVACY: ISRAELI". 17 (CAP. UL REV, INTELLIGENCE COLLECTION IN THE OCCUPIED PALESTINIAN TERRITORIES." (2016) 677 (להלן : WATERS) 2.

18. פעולותיה של ישראל בשטחים תחת כיבוש צריכים להתאים למטרות והיעדים של האמנה, ובכל מקרה להיות סבירים ומידתיים. מעקב אחרי אזרחים לא מעורבים אינו סביר או מידתי ולכן מנוגד לסעיף 17 לאמנה.

19. לפי סעיף 43 לאמנת האג, הדין החל בשטח הכבוש הוא הדין שחל ערב הכיבוש. סעיף 18 של החוקה הירדנית מ-1952 מעגן את הזכות לפרטיות על כן גם לפי עקרונות הדין הבינלאומי ההומניטרי עומדת לפלסטינים הזכות לפרטיות. (ראה WATERS ע' 592).

20. הפגיעה הפוטנציאלית בפרטיות כתוצאה משימוש בטכנולוגיה היא ברורה: 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'שימוש 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 (אדצ') 7541-04-14 **הסתדרות העובדים הכללית החדשה נ' עיריית קלנסווה** 56 (15.3.2017)].

21. לזיהוי פנים יש מאפיין 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).

22. כאשר FTR משולבת עם מערך ענק של מצלמות מעקב, כפי שקיים בשטחים, ועם יכולות אחסון ומחשוב גדולות, הצבא יכול לייצר בעזרתה מעקב רציף אחר אינדיבידואלים מסוימים, אך אפשר גם 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 unimaginable. 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>).

23. המרחב הציבורי בגדה מרושת במספר הולך וגדל של מצלמות מעקב, וכל אחת מהן אפשר לחבר למערכת זיהוי פנים וכך לזהות אדם שעובר ממקום למקום. בניגוד למצלמות האבטחה הרגילות, המערכת אינה מזהה רק אירועים חריגים, אלא יכולה לזהות באופן מתמשך, אוטומטי ורציף את אנשים, ולייצר מאגר מידע עצום ובו מידע אישי ואינטימי על כל מי שמצולם. ממאגר זה ניתן לדלות את המידע בלחיצת כפתור.

24. מכאן ש-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.

25. 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 האישיות שלו, נטייתו המינית, השקפותיו הפוליטיות, האם הוא תומך בשלטון או מתנגד לו, ועוד ועוד (ר' מיכאל בידנהק "פרטיות במשבר – הנדסה חוקתית והנדסת פרטיות" (יתפרסם במשפט וממשל 2020)).

26. 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.

27. 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. אמנם המשטר בגדה המערבית אינו משטר דמוקרטי, ואף רחוק מכך, אך ישנן זכויות שעודן עומדות גם לתושבים המוגנים בשטח הכבוש, ואלה עלולות להיפגע.

28. כך למשל, פגיעה בחירות יכולה 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>).

29. בשטח הנתון לשליטת הצבא, שימוש בחיווי אוטומטי של FRT ללא כל אינדיקציה נוספת, עלול להוביל להחשדה שגויה של פלסטינים, וגם בלי שהדבר יועמד לבירור בהליך פלילי, להוביל לשלילה של חירויות רבות התלויות לחלוטין בצבא: יציאה מהאזור, תנועה בתוך האזור, היתר כניסה לישראל לצורך עבודה, רישיון לחצות את חומת ההפרדה לשטחים חקלאיים ועוד ועוד.

30. פעילות הצבא בשטח הכבוש אינה פעילות צבאית רגילה מול צבא עוין, וחלק ניכר מפעולות הצבא במקום הן פעולות שיטור ואכיפת חוק מול אוכלוסיה אזרחית. מטבעה, מערכת טכנולוגית כמו FRT, מהווה בסיס למעקב המוני, החל גם על התושבים המוגנים בשגרת חייהם, הזכאים, גם תחת משטר כיבוש, לפרטיות וצנעת הפרט, ואשר השימוש בה עלול להשפיע על מגוון עצום של אינטראקציות של הצבא מול האוכלוסייה האזרחית. לכן גם אם בבסיס השימוש מטרות צבאיות, היא יכולה בקלות להפר את עקרון ההבחנה בין לוחמים לאזרחים, ולהשפיע מאוד על חיי היומיום של תושבים חפים מפשע.

31. עוד יש להוסיף, כי לטכנולוגיה המאפשרת מעקב מתמשך אחר תנועות של אזרחים אפקט ממשמע וממשטר הגורם לאדם להימנע מפעילויות שונות שהוא חופשי לעשות. אדם שיודע שמהלכיו מנוטרים וחשופים לעיני השלטון ישנה את התנהגותו ואף ייזהר בהתבטאויותיו, ועל אחת כמה וכמה תושב מוגן בשטח כבוש (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)).

32. **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) <https://bit.ly/33cmnJd>: MIT_News systems בקישורית: 11.2.2018.

33. 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/33jlU8i>).

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

34. **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. הסמכה מפורשת נדרשת גם בפעילות הצבא מול התושבים הפלסטינים. הקפדה על עיקרון החוקיות נדרשת גם כדי להטיל מגבלות על השימוש בטכנולוגיה, למשל – ביחס לצורך בצו שיפוטי, ולהבחין בין שימוש לגיטימי לשימוש פסול. כך, למשל, שימוש במידע אישי רגיש שנאסף באמצעות הטכנולוגיה על אדם חף מפשע, כדי להפעיל עליו לחץ לשמש כמודיע או משתף פעולה הוא בוודאי שימוש פסול.

35. חקיקה שתעגן ותגביל שימוש בזיהוי פנים היא צו השעה. נשיא מייקרוסופט, ברד 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.**"

36. נשיא מייקרוסופט הזהיר מפני "מרוץ לתחתית" של יצרני טכנולוגיה מתחרים, שייאלצו 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.

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

38. 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 הצבא בשקיפות.

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

הבקשה לפי חוק חופש המידע והסירוב הגורף למסור מידע

40. ביום 27.2.2020 הגישה העותרת בקשה לפי חוק חופש המידע שכותרתה מצלמות בעלות התאמה לטכנולוגיה לזיהוי פנים בגדה המערבית (1/ע), ובה מפורטות 17 שאלות אודות השימוש שעושה הצבא בטכנולוגיה לזיהוי פנים בגדה המערבית. בבקשה נתבקשו נתונים אודות השימוש, אודות פרישתן של המצלמות בשטחים הכבושים, ובפירוט במחסומים, בכבישים, בכפרים ובערים פלסטיניות, ליד בתי חולים ובתי ספר ובהתנחלויות ומאחזים. בנוסף, נתבקשו המשיבים למסור את העתקי הנהלים להפעלת

הטכנולוגיה לזיהוי פנים ואת הסכם ההתקשרות עם ספק הטכנולוגיה. שאלות נוספות נגעו למאגר התמונות עצמו, למשך הזמן בו נשמרת התמונה במאגר ולזהות הגופים בעלי גישה אליו.

41. לאחר בקשת ארכה ותזכורת נוספת, התקבל ביום 9.7.2020 מענה מאת הממונה על חופש מידע בדובר צה"ל, ובו שתי פסקאות. בראשונה נמסר כי "הוראות חופש המידע אינן חלות על רשויות באזור יהודה ושומרון... עם זאת, "... אין באמור כדי לגרוע מתחולת המשפט המנהלי הישראלי על פעולתן של רשויות האזור, לרבות עקרונות חופש המידע במובנם הרחב. אין בתשובה זו כדי ללמד על תחולת חוק חופש המידע, התשנ"ח-1998. הפסקה השנייה כללה סירוב גורף למסור ולו פרט אחד מן המידע הרחב שנתבקש בבקשה המפורטת: "לאחר בחינת בקשתך, לא נוכל להעביר לידך את המידע המבוקש, מאחר שמסירתו עלולה לחשוף שיטות פעולה מבצעיות של צה"ל ולהוביל לפגיעה בביטחון המדינה, זאת ברוח הוראות סעיף 9(א)(1) לחוק וסעיף 2(4) לצו חופש המידע (נושאים שרשות ציבורית לא תמסור מידע לגביהם), התשנ"ט-1999".

המענה מצורף ומסומן נספח ע/2.

42. כך, וללא כל פירוט והנמקה דחה המשיב את הבקשה המפורטת. התשובה גורפת כדי כך, שלא פורט בה אפילו אלו סעיפים נדחו מכוח סעיף 9(א)(1) לחוק חופש המידע (להלן: **החוק**), ואלו סעיפים נדחו מכוח סעיף 2(4) לצו חופש המידע (נושאים שרשות ציבורית לא תמסור מידע לגביהם)(להלן: **הצו**, או **צו חופש המידע**). בנוסף, לא מסר הממונה ולו ברמז כל נימוק או הסבר מדוע לשיטתו יש לדחות את הבקשה על סמך הסעיפים שזכרו.

43. יצוין, כי צבא ארצות הברית דווקא השיב לבקשה על השימוש המבצעי שלו בטכנולוגיית זיהוי פנים. אמנם לא כל המידע שנתבקש נמסר, אך מידע אודות התקשרויות של הצבא עם גופים פרטיים בתחום זיהוי הפנים והשימוש בו באפגניסטן נמסרו לכותבי אתר "onezero" ואת הניתוח של המידע של המידע וכן חלק מן המידע עצמו ניתן למצוא כאן: <https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d>

טענת המשיב כי חוק חופש המידע לא חל על פעולותיו בשטחים הכבושים

44. הצבא הינו רשות שחל עליה חוק חופש המידע, גם בעת שהצבא פועל בשטח הכבוש. בפסק הדין בבג"ץ 6870/14 רגבים נ' ראש המינהל האזרחי (3.1.2017) (להלן: פרשת רגבים) עלתה השאלה אודות תחולתו של החוק על המינהל האזרחי, כלשונו. בית המשפט העליון קבע כי אין לבית המשפט לעניינים מנהליים סמכות לדון בעתירות לפי החוק, אך על המינהל האזרחי לפעול לאור עקרונות המשפט המינהלי לרבות עקרונות חופש המידע, וכי החלטותיו בבקשות למידע, גם אם לא מכוח החוק, נתונות לביקורת שיפוטית של בג"ץ. אולם בפסק דין מאוחר יותר, בפרשת יש דין (ע"מ 10014/16 יש דין – ארגון מתנדבים לזכויות אדם נ' המינהל האזרחי אי"ש (מיום 16.5.2019)) דנו שופטי הרוב בערעור על החלטת בית המשפט לעניינים מינהליים בעתירת חופש מידע נגד המינהל האזרחי בלי להכריע בשאלת תחולת החוק על המינהל האזרחי, לאור הסכמת הצדדים להכיר בסמכות בית המשפט לעניינים מינהליים. השופטת ברון, בעמדת יחיד, קבעה כי החוק חל גם על פעולות המינהל האזרחי בשטחים (פס' 6 לפסק דינה של השופטת ברון בפרשת יש דין).

45. בכל מקרה, תיקון 117 לחוק בתי משפט לעניינים מנהליים, התש"ס-2000, שנכנס לתוקפו בשנה החולפת, הקנה את הסמכות לדון ב"עתירות מינהליות בענייני האזור" לבית המשפט לעניינים מנהליים בירושלים.

46. כפועל יוצא מכך, לבית המשפט הנכבד סמכות עניינית לדון בסירוב של הצבא לתת מידע בין מכוח חוק חופש המידע ובין כביקורת על החלטה מינהלית בענייני האזור.

47. כאמור, העותרת סבורה כי חוק חופש המידע חל במקרה זה במלואו, ואין מקום להחיל את עקרונותיו באופן וולונטרי. גישת הצבא כאילו ניתן להוציא את פעולותיו בגדה המערבית מתחולת חוק חופש המידע חוטאת לעקרונות החוק. חוק חופש המידע אינו מתייחס למיקומם הפיזי של המידע ושל הרשות, אלא לשאלה האם גוף מחויב למסור מידע אם לאו, בהתאם לסעיף 2 לחוק. כמו במידע על פעולות הצבא בתוך שטחי ישראל, גם בכל הנוגע לפעולותיו בשטחים הכבושים, מחזיק הצבא במידע כנאמן הציבור. נאמנות זו אינה נעצרת בקו הירוק, ומצויה בכל מקום שבו הממשל הישראלי והמשיב עצמו מבצע פעולות. עקרון זה חל גם מחוץ לשטחים שישראל שולטת בהם, כמו למשל בפסק הדין בע"מ 2975/15 הוצאת עיתון 'הארץ' נ' משרד החוץ (פרסם 6.6.2016) שם פסק בית המשפט העליון כי על משרד החוץ למסור מידע הנוגע לארוחה שהתקיימה בבית שגריר ישראל בווינגטון.

48. גם אם החוק לא חל על פעולות הצבא בשטחים, החוק אינו יוצר הסדר שלילי לגבי חשיפת מידע בהתבסס על מקורות אחרים ואם החוק לא חל, אין זה אומר שלא מוטלת על הרשות חובה לשקול את מסירת המידע מכוח דיני המשפט המינהלי הכלליים, ודיני השקיפות, ודומה שגם המשיב מבין זאת כי הוא מחיל באופן וולונטרי את עקרונות החוק על עצמו, ומנמק את החלטותיו על סעיפי החוק.

49. החלטה על אי מסירת מידע, ככל החלטה מינהלית, נתונה לביקורת על פי כללי המשפט המינהלי – סבירות, מידתיות וכדומה. יפים לעניין זה דבריו של המשנה לנשיאה רובינשטיין בדנ"מ 8020/15 האגודה לזכויות האזרח בישראל נ' משרד ראש הממשלה (החלטה מיום 8.6.2016):

"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 (ע"מ 2975/15 הוצאת עיתון 'הארץ' נ' משרד החוץ, פסקה 41 (6.6.16)), בלא שאכנס לפירוט זה או אחר בשקלא וטריא שבפסק הדין. כאמור, החרגת המידע המבוקש מכוח סעיף 14 משמעה כי המידע לא נבחן לגופו; וכפי שציינה השופטת ברון בפסק הדין נשוא העתירה, חרף טענת המדינה כי המידע חוסה תחת סעיף 9(1) וסעיף 9(4) לחוק ולכן אין על הרשות למסור, טענה זו, לרבות עמידה בנטלי הראיה במקרה הקונקרטי, לא נבחנה. לטעמי, נוכח חשיבותה של זכות הציבור לדעת לקיומו של משטר דמוקרטי תקין, ייטיבו הרשויות השונות אם יטמיעו כאמור את עקרונות השקיפות, ויואלו למסור מידע מבוקש ככל שביטחון המדינה מאפשר זאת, גם אם חוק חופש המידע אינו מחייב לעשות כן. ניתן, והדברים ידועים, לערוך פרפרזות 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 בידינו: 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. לדעתי, ככל שיגבר הגילוי

הוולונטרי, כן יגבר האמון באותם מקרים שבהם עומדת הרשות על אי גילוי הלגיטימי של מידע בסייגים שבחוק".

50. מכאן שלעמדת העותרת חוק חופש המידע חל במלואו על המשיב, אך אם טענה זו לא תתקבל, למשיב יש שק"ד למסור את המידע, גם אם לדידו הוא אינו חייב לעשות זאת, ושיקול דעת זה נתון לביקורת שיפוטית מכוח הזכות הכללית לקבלת מידע במשפט המינהלי.

הטעמים לאי מתן המידע

51. את הסירוב המהותי למסור מידע תולה המשיב בשני סעיפים. סעיף 9(א)(1) לחוק חופש המידע וסעיף 4(2) לצו חופש המידע (נושאים שרשות ציבורית לא תמסור מידע לגביהם). כאמור בראשית טיעון זה, המשיב לא פרט אלו סעיפים בבקשה דחה לפי הראשון ואלו לפי השני.

סעיף 9(א)(1) לחוק

52. אין מחלוקת באשר למעמדה של הזכות לקבלת מידע מרשות ציבורית כאחת מזכויות היסוד במשטר דמוקרטי. זכות זו עומדת לעותרת גם ביחס לפעולות הצבא. 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**, [פורסם בנבו] פסקה 18 (18.7.2017); פרשת **יש דין** פסקה 5 לפסק דינה של השופטת ברון (16.5.2019)).

53. סעיף 9(א)(1) לחוק חופש המידע מאפשר לרשות שלא למסור מידע אשר בגילוי יש חשש לפגיעה בביטחון המדינה, ביחסי החוץ שלה, בביטחון הציבור או בביטחון או בשלומה של אדם.

54. לגבי החריג שבסעיף 9(א)(1) לחוק קבע בית המשפט כי יש להצביע על חשש לפגיעה בשלום הציבור וביטחונו ו"אין די בכל חשש, היינו באפשרות רחוקה, אלא רק בחשש בעל משקל הנאמד בהתאם לעוצמתו של הסיכון ולהסתברות התממשותו" (עע"מ 2975/15 **הוצאת עיתון 'הארץ' נ' משרד החוץ**, פסקה 26 (6.6.2016); ר' גם: בג"ץ 2007/11 **שני נ' המשרד להגנת הסביבה**, פסקה 4 (5.2.2012)). אין די, אם כך, בחשש כללי ובלתי מנומק, אלא נדרש לבחון את ההסתברות שהחשש יתממש ואת עוצמת הפגיעה שתיגרם בשל מסירת המידע.

55. בתשובה לא ניתן הסבר קונקרטי לחשש מפני פגיעה בביטחון המדינה כתוצאה ממסירת המידע. בטחון המדינה אינה מילת קסם, ויש לאזן בינו לבין זכויות ואינטרסים אחרים, לרבות זכות הציבור לדעת. בית המשפט העליון פסק כי, גם כאשר בענייני ביטחון עסקינן, "הכלל הוא... פומביות וגילוי. החריג לכלל הוא – חיסיון וסודיות. מאחר שהחריג לכלל מהווה הגבלה על נורמה חוקתית, החלתו באופן הפוגע בנורמה מותנית בתנאים מוקדמים שעיקרם תכלית ראויה ומידתיות" (בג"ץ 258/07 **גלאון נ' ועדת הבדיקה הממשלתית לבדיקת אירועי המערכה בלבנון 2006** (פורסם בנבו 6.2.2007), בפס' 3 לחוות דעתה של השופטת פרוקצ'יה).

56. בפרשת **גלאון** עסק בית המשפט במתח שבין זכות הציבור לדעת ופומביות הדיונים של ועדת הבדיקה הממשלתית לענייני מלחמת לבנון, לבין ביטחון המדינה. בפסקה 8 לפסק הדין נקבע כי גם כאשר מדובר במידע הנוגע לענייני ביטחון מובהקים, יש לבחון כל פרט מידע באופן מדוקדק, כדי לבדוק אם אכן קיימים טעמים ביטחוניים הכרחיים, המונעים את פרסום המידע:

"תוצאת האיזון בין פומביות הדיון לבין בטחון המדינה אינה ניתנת לקביעה מראש שכן היא תלויה בהערכת מידת הסיכון לביטחון ומידת ההסתברות שפגיעה כזו תתרחש בנסיבות העניין. לפיכך, התוצאה באשר לנקודת האיזון הראויה, נגזרת מנסיבותיו של כל מקרה לגופו. יודגש כי נוכח חשיבותו של עקרון פומביות הדיון, לא ניתן להסתפק בהערכה כוללתית וגורפת של הסיכון לביטחון הציבור הנשענת על טיבן הכללי של הסוגיות הנדונות. בהקשר זה, נדרשת בדיקה קונקרטית ופרטנית של נסיבות העניין על-מנת להכריע האם מתקיימת הצדקה לסטייה מהכלל בדבר פומביות הדיון"

57. הכללים לדחיית בקשה מפורטים גם בנוהל מס' 3.1 של היחידה הממשלתית לחופש מידע במשרד המשפטים "דרישות המענה בדחיית בקשת חופש מידע". הנוהל נועד להבהיר את הוראות סעיף 7 לחוק חופש המידע לפיו במקום בו החליטה רשות ציבורית לדחות בקשה על פי החוק, עליה לנמק את החלטתה וליידע את העותר על זכותו לעתור כנגד החלטתה לבית המשפט לעניינים מנהליים.

58. בנוהל מחולקים הסייגים למסירת מידע לפי סוג ההנמקה שיש לנמק בבואה לדחות את הבקשה. סעיף 9(א)(1) מסווג שם כ"סייג המגן על אינטרס מוכר (בטחון, סוד מסחרי וכד') ככל שיש חשש או עלולה להיות פגיעה בו אם יימסר המידע המבוקש. על כן, בהנמקה, יש להתייחס לתוצאות הצפויות מחשיפת המידע גם בהתייחס לרמת הוודאות הנדרשת לפגיעה כעולה מלשון הסעיף המסוים"

וכך מפורט בנוהל לגבי סעיף 9(א)(1):

"2.1 מידע אשר בגילוי יש חשש לפגיעה בביטחון המדינה, ביחסי החוץ שלה, בביטחון הציבור או בביטחונו או בשלמו של אדם" – לעניין הגנה על אחד הערכים המנויים בסעיף (בטחון, יחסי חוץ וכד'), אין צורך בהוכחת "ודאות קרובה" לפגיעה. לדברי בית המשפט העליון בבג"ץ 2007/11 ינאי שני נ' המשרד להגנת הסביבה ואח' לצורך ביסוס התקיימותו של הסייג על הרשות לבחון את החשש לפגיעה בהתייחס ל"מכפלת עוצמת הסיכון בהסתברותו" (תוחלת הסיכון) כך שכלל שעוצמת הסיכון גבוהה יותר, ניתן להסתפק ברמת הסתברות נמוכה יותר להתרחשות הסיכון כדי להקים חשש לפגיעה באינטרס המוגן, וככל שעוצמת הסיכון נמוכה, יש צורך ברמת הסתברות גבוהה להתרחשות הסיכון כדי להקים חשש לפגיעה באינטרס המוגן"

נוהל " דרישות המענה בדחיית בקשת חופש מידע" :

<https://www.gov.il/he/departments/policies/regulation-3-1>

59. בהתאם לנוהל, אמור היה המשיב בנימוקו להציג את תרחיש הפגיעה שתגרום אם המידע יימסר לעותרת, כך לגבי כל סעיף מסעיפי הבקשה, וכן להראות כי אין אפשרות למזער את הפגיעה האפשרית במסירת מידע חלקי, או מענה בתנאים. המשיב לא עשה דבר מכל אלה והותיר את העותרת לנסות ולפרש בעצמה איך המידע אודות קיומן או העדרן של מצלמות ליד בתי ספר ובתי חולים בגדה המערבית יכול לפגוע בביטחון המדינה, או העברת העתק של הסכם ההיקשרות עם החברה המפעילה את המצלמות. תחת זאת לא נימק הממונה את סירובו ולו במילה, אלא הסתפק בהפניה לסעיף.

60. העותרת סבורה כי העברת מידע אודות היקף השימוש בטכנולוגיה של זיהוי פנים בגדה המערבית, והרגולציה המופעלת עליה אינה יוצרת סיכון ממשי לפגיעה בביטחון. קשה להבין איך מידע כגון זמן השארת תמונת קטין במאגר, שאלה אודות הפרטים השמורים, הסכם ההתקשרות עם החברה וכד' יוצרות סיכון לפגיעה בביטחון המדינה. נכון הדבר גם לגבי המידע הכמותי שהתבקש – כגון המספר

הכולל של מצלמות. לגבי המידע הגיאוגרפי שנתבקש – אם החשש הוא מפגיעה במצלמות הרי שיכול היה המשיב למסור חלק מהמידע, ובכל מקרה לנמק את החלטתו שלא למסור את המידע לכל סעיף מסעיפי הבקשה. המשיב לא עשה כן, והסירוב הגורף למסור מידע מעלה חשש שהבקשה כלל לא נבחנה לעומקה.

סעיף 2(4) לצו חופש המידע (נושאים שרשות ציבורית לא תמסור מידע לגביהם)

61. לטענת המשיבה, סעיף 2(4) לצו חופש המידע מצדיק סירוב להעביר את המידע לידי העותרת. לשונו של הסעיף:

2. רשות ציבורית לא תמסור, מטעמים של שמירה על בטחון המדינה, מידע בנושאים המפורטים להלן:

(4) שיטות פעולה מבצעיות ותורת לחימה, אופי התרגילים והאימונים של יחידות צה"ל ועצם קיומם.

62. העותרת לא ביקשה מידע אודות שיטות פעולה מבצעיות ולא על תורת לחימה או מידע כלשהו על יחידות צה"ל ואימוניהם. המידע שנתבקש היה אודות מצלמות המוצבות בגדה המערבית, מיקומן, מסד הנתונים אליו הן מחוברות, מידע אודות ההתקשרות עם חברה מסחרית אם קיימת. בהעדר כל נימוק כלל לא ברור מדוע בחר המשיב את הסעיף הנ"ל כבסיס לסירוב.

63. אך גם במקרה שחלק מהמידע שנתבקש כן נופל בגדרו של סעיף 2(4) לצו, דבר שיש לנמק בפירוט, הרי שוודאי שלא כל המידע המבוקש מצוי בגדרו. ודאי, כך למשל, שהסכם ההתקשרות עם חברה מסחרית אינו בגדר תורת לחימה או אימון. נכון הדבר גם לגבי מידע כללי לגבי הימצאותן או אי הימצאותן של מצלמות ליד בתי חולים.

64. גם במקרה זה, המשיב לא נימק החלטתו באופן ההולם את חובתו החוקית, ונראה שלא נערכה בחינה אמיתית של האפשרות למסור את המידע.

החובה להפעיל שיקול דעת למסירת מידע גם אם חלים סייגים למסירתו

65. החוק קובע שגם מידע שאין חובה ואף אסור למסור אותו לפי סעיפים 8 ו-9 לחוק, הרשות צריכה בכל זאת לשקול את מסירת המידע, ולו באופן חלקי, מכוח סעיפים 10 ו-11 לחוק.

"ברם סעיף 9 לחוק אינו סוף פסוק. "בתרשים הזרימה" – לשון בית המשפט העליון בפרשת אורון (ע"מ 615/15) [פורסם בנבו] – לאורכו מוליך אותנו החוק, הקובע, כאמור, כנקודת מוצא את הזכות לקבל מידע, יש לפנות, לאחר בחינת הסייגים לזכות (סעיפים 8-9 לחוק) למסנת הסבירות והמידתיות בה הרשות אמורה לעשות שימוש טרם מתן החלטתה (סעיפים 10-11 לחוק) ולבסוף למסנת שיקול הדעת השיפוטי (סעיף 17(ד) לחוק) המכוונת את בית המשפט לקבוע את נקודת האיזון בין הערכים והאינטרסים המתנגשים (עת"מ (ת"א) 19336-08-16 התנועה למען איכות השלטון בישראל נ' משרד הביטחון (פורסם בנבו, 11.12.2018), בפיסקה 16).

66. 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.

67. 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.

68. בתשובה הלקונית והתמציתית של המשיב לא ניתנה הדעת לסעיפים 10 ו-11 ולא ניתן כל נימוק מדוע לא יפעל המשיב על פיהם. זה בפני עצמו מחייב התערבות בהחלטה.

69. סעיפים 10 ו-11 מתייחסים לסעיפים 8 ו-9, והצו הוצא אף הוא מכוח סעיף 9, כפי שמצוין במפורש בצו, ולכן סעיפים 10 ו-11 חלים גם על החלטות מכוח הוראות צו.

70. אם הפעילה הרשות שיקול דעת והחליטה לא למסור את המידע עליה לנמק את תשובתה, והיא אינה יכולה להסתפק בהפניה לסעיף בחוק או בצו. החלטה זו נתונה לביקורת שיפוטית של בית המשפט לעניינים מנהליים. כמובן שגם מחדלה של הרשות להפעיל שיקול דעת מכוח סעיפים 10 ו-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**").

71. מהכלל אל הפרט – העותרת סבורה כי סעיף 4(2) לצו לא חל על בקשתה, ויש לפרש אותו בצמצום, ובוודאי שאינו חל על כל סעיפי הבקשה, אך גם לו היה חל היה על המשיבה לשקול בכל זאת את מתן המידע מכוח סעיפים 10 ו-11 לחוק. משלא עשתה זאת הרשות, החלטתה היא שלא כדין, ויש לחייבה לתת את המידע ולמצער, לחייבה לשקול מחדש את מתן המידע.

72. אם הפעיל המשיב שיקול דעת מכוח סעיפים 10 ו-11 הוא לא נתן לכך ביטוי משלא נימק את תשובתו כלל, והעותרת שומרת לעצמה את הזכות להוסיף טענות בעניין, אך כבר עתה נעמוד על כמה מהשיקולים שהיה על המשיב לשקול.

א. היה על המשיב לתת משקל לחשיבות העליונה בחשיפת טכנולוגיות בהם הצבא 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 המתגורר או מתנייע בשטחי הגדה המערבית, שמושפע מהפעלת הטכנולוגיה, פלסטינים וישראלים כאחד.

ב. היה על המשיב לתת משקל רב לאינטרס הציבורי של חובת הצבא כלפי תושבים מוגנים בגדה המערבית, ולכך שפעולותיו בשטח הכבוש כפופות גם לדין הבינלאומי ולהגנותיו, ולכן העניין במסירת המידע הוא רב יותר, ובמיוחד כאשר מדובר בטכנולוגיה שמשפיעה על חיי אזרחים שאינם מעורבים בלחימה, ואשר מהות היחסים בין הצבא לאזרחים אלו היא של ניהול חיי היומיום, שמירה על הסדר ופעילות מעין משטרתית.

ג. היה על המשיב לתת משקל רב לכך שחשיפת המידע, ולמצער – חלקו, יאפשר דיון ציבורי אודות הטכנולוגיה, טיבה ויעילותה. בהיעדר שקיפות נרמס חופש הביטוי, שכן קשה להתנגח עם ספינקס, ותיתכן פגיעה לא מידתית באמצעות הטכנולוגיה.

ד. מנגד נראה שניתן משקל מופרז לאינטרס הצבא בהגנה על המידע, כאשר צבא ארצות הברית, למשל, לא מסתיר לגמרי את השימוש שהוא עושה בטכנולוגיה.

מכל האמור, מתבקש בית המשפט הנכבד להורות כמבוקש בעתירה.

21 בספטמבר 2020

רוני פלי

רוני פלי, עו"ד
ב"כ העותרת