

20 ביוני 2023

לכבוד
הוועדה לביטחון לאומי
בראשות חבר הכנסת צביקה פוגל

התייחסות מכון תכלית: מערכת עין הנץ והצעת חוק לתיקון פקודת המשטרה (מס' 40) (מערכות צילום מיוחדות), התשפ"ג-2023

חברי ועדה נכבדים,

אנו מבקשים להתייחס להצעת חוק לתיקון פקודת המשטרה (מס' 40) (מערכות צילום מיוחדות), התשפ"ג-2023, אשר בא להסדיר בין היתר את השימוש במערכת "עין הנץ" לזיהוי לוחיות רישוי. המערכת מבוססת על טכנולוגיה לזיהוי אוטומטי של לוחיות רישוי (Automatic License Plate Reader - ALPR) ומאפשרת השוואה מיידית בין הקלט מהמצלמות האוטומטיות אל מול מאגרי מידע קיימים. מאז קליטת המערכת בישראל, בשנת 2013, תפוצתה התרחבה והיא פרוסה ברחבי הארץ, בטרם הוסדר השימוש בה כדין. כעת, הצעת החוק שבנדון באה לתחם את השימוש במערכת ולהציע איזון בין ההגנה על הפרטיות לבין האינטרס הציבורי במניעת וגילוי עבירות. אולם, הצעת החוק אינה נותנת מענה לסיכונים מרכזיים בתפעול טכנולוגיה מסוג זה. לשם כך, אנו מציעים להידרש לשתי סוגיות נוספות במסגרת החוק דנן: (1) אבטחת המידע שנאסף במערכת; (2) הגברת הפיקוח על השימוש במידע והעברתו.

1. רקע

1.1. טכנולוגיה לזיהוי אוטומטי של לוחיות רישוי

טכנולוגיית זיהוי פנים הינה אפליקציית מחשב הכוללת אלגוריתם שמסוגל לזהות או לאמת זהותו של אדם, באופן אוטומטי או אוטומטי למחצה, בהתבסס על תמונה או סרטון וידאו. טכנולוגיה לזיהוי אוטומטי של לוחיות רישוי (ALPR) מתבססת על טכנולוגיה זו, כאשר המצלמות מוצבות ברחובות ובכבישים ומתעדות באופן אוטומטי את הנוסעים בדרכים. לצד היתרונות הרבים שיש לשימוש במערכות מסוג זו, כגון דיוק, יעילות, חסכון בכוח אדם, והגברת אכיפת החוק, ישנם סיכונים גם כן.

חשש ראשון הינו שגיאות וכשלים של אמצעי הזיהוי. כך, בהקשר של זיהוי פנים, ביצוע כושל של המערכת עלול להביא לזיהוי שגוי ובכך להטרדת אנשים תמימים (False Positive Identification Rate – FPIR), ומאידך עלול לגרום להחמצת זיהוי חשודים (False Negative Identification Rate – FNIR)¹. חשש זה בא לידי ביטוי בשימוש במערכת

¹ מערך הסייבר הלאומי, היחידה להזדהות וליישומים ביומטריים, זיהוי פנים במרחב הציבורי בישראל עקרונות למדיניות וקריאה לאסדרה, בעמ' 4 (יולי, 2021) (להלן: "דו"ח מערך הסייבר הלאומי"); ר' גם Hasan, Md Rezwan, Richard Guest, and Farzin Deravi, "Presentation-Level Privacy Protection Techniques for Automated Face Recognition-A Survey." *ACM Computing Surveys*, p.1 (2023), <https://dl.acm.org/doi/pdf/10.1145/3583135>, בעמ' 8.

לזיהוי פנים ספציפית במרחב הציבורי בבריטניה, לדוגמה, שם נמצא כי שיעורי התראות השווא עמד על כ-90%². כישלון זה עלול לנבוע ממספר גורמים, ובינם בדיקה בלתי מיומנת של תוצרי המערכת, תזוזה של אנשים, הצבה לא נכונה של מצלמות, מאפיינים מיוחדים של קהל היעד שלא נלקחו בחשבון, הטיות דמוגרפיות של האלגוריתם ועוד.³

חשש שני הוא בהיבט של מעקב טכנולוגי והחשש לפגיעה בפרטיות. השימוש במערכות אלו עשוי להביא לאגירת יתר של תמונות פנים של אנשים רבים, אשר יתועדו במקומות שונים, באופן שעלול לשמש בפועל למעקב אחריהם, תיעוד תנועותיהם, תיעוד עמדתם הפוליטית, הרגלי הצריכה שלהם וכן הלאה. אף קיים חשש שהמידע עצמו ישמש גם למטרות נוספות אשר לא נקבעו או הובהרו מראש.

בנסיבות אלה, לא יכולה להיות מחלוקת על כך שהשימוש במערכות זיהוי פנים מאיימת להפר זכות יסוד מוגנת – הזכות החוקתית לפרטיות.⁴ בית המשפט העליון עמד זה מכבר בפסיקתו על כך שהזכות לפרטיות היא "מהחשובה שבזכויות האדם",⁵ וכי היא "אחת מהחירויות המעצבות את אופיו של המשטר בישראל כמשטר דמוקרטי".⁶ פגיעה זו בזכות לפרטיות מתבטאת במישורים שונים. לדוגמה, עצם המעקב אחרי המצולמים יכול להניב פרטי מידע אחרים ולמשל הרגלי צריכה ונטייה מינית, ובכך מהווה פגיעה בפרטיותם ולו מעצם היוודעותם לאדם שמקבל את הנתונים.⁷ כמו כן, נוכח העובדה שהפרט יודע שלמדינה שליטה במידע אישי שלו ויש ביכולתה לעקוב אחריו, ניתן לטעון כי נוצר אפקט מצנן ביחס להתנהגות הפרט וכי הוא ישנה את התנהגותו בעקבות זאת.⁸

חשש שלישי מקורו בסיכון הטמון בדליפת מידע ביומטרי מהמאגרים העלול להביא לשימוש לרעה בידי גורמים לא מורשים וזאת, ללא פיקוח ובקרה אפקטיביים.⁹ מדובר בחשש מתמשך לגבי מאגרים ביומטריים המנוהלים בישראל, שהועלה על ידי הממונה על היישומים הביומטריים במערך הסייבר הלאומי, ועל ידי מבקר המדינה.

² ראה כתבה של <https://www.bbc.com/news/technology-44089161>; BBC, בנוסף, ראה כתבה בה דווח כי משטרת ניו ג'רזי עצרה אדם חף מפשע למשך עשרה ימים בשל טעות בזיהוי של מערכת זיהוי פנים: <https://futurism.com/the-byte/lawsuit-claims-facial-recognition-ai-sent-wrong-man-jail>.

³ דו"ח מערך הסייבר הלאומי, לעיל ה"ש 1, בעמ' 8.
⁴ ס' 7 לחוק יסוד: כבוד האדם וחירותו; רועי גולדשמידט, "השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי", מרכז המחקר והמידע של הכנסת, 14 בדצמבר 2020 (להלן: דו"ח מרכז המחקר והמידע של הכנסת), בעמ' 19. הצעת החוק אף היא מציינת כי השימוש במערכות המוצעות מהווה פגיעה בפרטיות, וראה למשל בעמ' 122.

⁵ דנ"פ 1062/21 אור"י נ' מדינת ישראל, פס' 48 לפסק דינה של הנשיאה חיות (נבו 11.1.2022); ע"פ 1302/92 מדינת ישראל נ' נחמיאס, פ"ד מט(3) 353, 309 (1995).

⁶ שם, רע"א 2558/16 פלונית נ' קצין התגמולים – משרד הביטחון, פס' 39 לפסק דינה של השופטת ברק-ארז (נבו 5.11.2017); ע"א 8954/11 פלוני נ' פלונית, פס' 67-68 לפסק דינו של השופט סולברג (נבו 24.5.2014).

⁷ בג"ץ 3809/08 האגודה לזכויות האזרח נ' משטרת ישראל, פס' 7 לפסק דינה של הנשיאה ביניש (28.5.2012). ראה גם את דברי השופטת ד' ברק-ארז ברע"א 2558/16 פלונית נ' קצין התגמולים, בפס' 43 לפסק דינה (5.11.2017): "עצם פעולת המעקב, אותה התחקות אחר אדם בלא ידיעתו, תוך חדירה למרחב האישי-פרטי שלו, מהווה פגיעה באוטונומיה של הפרט ואף בכבודו".

⁸ ראה בג"ץ 6732/20 האגודה לזכויות האזרח נ' הכנסת, פס' 5 לפסק דינה של השופטת ברון (נבו 1.3.2021), שם נקבע כי עצם האפשרות של השימוש באיכוני השב"כ לצורך איתור חולי קורונה ואנשים בא עמם במגע יוצרת תחושת מעקב ואפקט של "משטור" ולכך השלכות על הפרט נוכח ההנחה שהוא יימנע מלפעול בחופשיות תחת פיקוח המשטר.

⁹ דו"ח מערך הסייבר הלאומי, לעיל ה"ש 1, בעמ' 8-9; דו"ח מרכז המידע והמחקר של הכנסת, לעיל ה"ש 4, בעמ' 20-21.

1.2. מערכת עין הנץ

על פי דו"ח מרכז המחקר והמידע של הכנסת, מערכת עין הנץ, בדומה למערכות זיהוי פנים, מבוססת על מערך מצלמות המותקנות בכבישים ברחבי הארץ אשר עוקבות, מצלמות ומזהות באופן אוטומטי ובכל שעות היממה לוחיות רישוי באמצעות טכנולוגיות עיבוד תמונה מתקדמות (ALPR).¹⁰ טכנולוגיה זו מאפשרת לתעד ולקרוא מתוך התמונות והווידאו שנאספו את פרטי לוחיות הרישוי של כלי רכב ומצליבה אותם עם נתונים שנמצאים במאגר מידע מסוים שמתופעל על ידי המשטרה. כתוצאה מכך, נוצר מאגר הכולל מידע על מיקום של עוברי דרך רבים.¹¹

משטרת ישראל עושה שימוש במערכת עין הנץ זה מכבר ביחידות שונות וביניהן, יחידת מג"ב, אגף התנועה ואגף המבצעים.¹² כחלק מהשימוש במערכת המשטרה מתפעלת מאגר מידע אשר כולל רשימה של כלי רכב שנגנבו, הורדו מהכביש, צילומי וידאו ותמונות סטילס שנאספו באמצעות המצלמות הפרושות ברחבי הארץ, לרבות תמונות הרכב, הנוסעים שבתוכו ומספר לוחית הרישוי.¹³ יודגש כי תמונות הנוסעים ברכב הן תמונות תקריב שבהן נראים בבירור פניהם של הנוסעים.¹⁴

בשנת 2020 חשף תחקיר של 'וואלה', כי משטרת ישראל אוגרת מידע למשך חודשים רבים על תנועת הרכבים בכבישים.¹⁵ כאמור, המערכת מסוגלת לזהות את פניהם של הנהגים והנוסעים ברכב ואוגר את הפרטי הרכבים החולפים במאגר מידע נרחב.¹⁶ המערכת כיום משמשת את המשטרה לזיהוי רכבים על בסיס לוחית הרישוי שלהם, ובהתאם לתנאים מוגדרים מראש, משווה את לוחית הרישוי למאגר הנתונים של המשטרה. התיעוד מהמערכת הוגש משכבר כראיה בבית המשפט,¹⁷ אך חוקיותן וקבילותן של ראיות מעין אלו מוטלת בשאלה.¹⁸

ועדיין, כי בשנים האחרונות ניתן לראות עלייה משמעותית בשימוש בראיות מתוך המאגר שנוצר בעקבות פעילות מערכת עין הנץ. כך, לדוגמה, במ"ת (שלום ב"ש) 57000-02-23 מדינת ישראל נ' שטרית (10.5.2023), כמו גם במ"ת (מחוזי חי') 46950-01-23 מדינת ישראל נ' עאשור (28.2.2023), תיעוד וצילום ממאגר מערכת עין הנץ סייע לבסס תשתית ראייתית נגד הנאשם לצורך החלטה על מעצר עד תום ההליכים.¹⁹ על רקע היעדר חקיקה המסדירה את השימוש בכלי זה, הגישה האגודה לזכויות האזרח בינואר 2021 עתירה למתן צו על תנאי למשטרה להסביר מדוע היא

¹⁰ מכרז לאספקת מערכת LPR (מס' 35/2012), עמ' 24 (17.10.2012) (להלן: "המכרז").

¹¹ שם, בעמ' 27; דו"ח מרכז המחקר והמידע של הכנסת, לעיל ה"ש 4, בעמ' 7.

¹² המכרז, לעיל ה"ש 10, בעמ' 25.

¹³ שם; ראה את העתירה שהגישה האגודה לזכויות האזרח בישראל בעניין השימוש במערכת "עין הנץ" (בג"ץ 641/21).

¹⁴ שם.

¹⁵ שם.

¹⁶ בג"ץ 641/21 האגודה לזכויות האזרח בישראל נ' משטרת ישראל, פס' 1 (עתירה למתן צו על תנאי 28/01/2021).

¹⁷ בש"פ 4877/21 מדינת ישראל נ' מחמוד גאבר, פס' 5 לפסק הדין (נבו) 08.08.2021.

¹⁸ בש"פ 2561/21 מדינת ישראל נ' שאהין, פס' 4 לפסק הדין (נבו) 22.04.2021.

¹⁹ ראה עוד מיני רבים: מ"ת (שלום ב"ש) 48373-01-23 מדינת ישראל נ' לטיף (נבו) 19.2.2023; מ"ת 44808-05-20 (מחוזי ב"ש) מדינת ישראל נ' קטיפאן (נבו) 10.6.2020; מ"ת (שלום חי') 5518-09-20 מדינת ישראל נ' חטיב (נבו) 15.10.2020.

לא חודלת מהשימוש בעין הנץ ובמאגרי המידע של מערכת זו.²⁰ על המשטרה לעדכן את בית המשפט אודות התקדמות הליך החקיקה עד ליום ה-30.07.2023.²¹

2. סקירה משווה

מסביב לעולם, מדינות מפעילות מערכות ALPR לאחר הסדרה מפורשת שלהן בדיון. נציג כעת סקירה משווה שתעיד על הסוגיות המרכזיות שדורשות מענה בעת שימוש בטכנולוגיה מרחיקת לכת זו.

2.1. האיחוד האירופי

התקנות להגנת הפרטיות של האיחוד האירופי (GDPR) נכנסו לתוקף בשנת 2018, ואלו מציעות כללים בכל הנוגע לשימוש ועיצוב מערכות זיהוי טכנולוגיות. גם מעבר לגבולות האיחוד האירופי, הוראות ה-GDPR תרמו רבות לשיח המשפטי אודות ההגנה על פרטיות ובפרט בהקשר הנוכחי.²² חובה חשובה העולה מן ה-GDPR היא החובה למנות מפקח על הגנת הפרטיות בתוך כל רשות ציבורית או פרטית אשר הפעולות העיקריות שלה כוללות מעקב אחר אנשים או עיבוד נתוני זיהוי.²³ כיום, לשם ההמחשה, ישנן 27 רשויות המפקחות על הגנת פרטיות באיחוד האירופי.

כמו כן, לאחרונה הוצעה באיחוד האירופי המסגרת החוקית הראשונה שמתייחסת לסיכונים שבשימוש בבינה מלאכותית (Artificial Intelligence – AI). במסגרת זו, הוצע כי יאסר השימוש במערכות זיהוי פנים במרחב הציבורי למען זיהוי מרחוק ב"זמן אמת", אלא במקרים הכרחיים ולמטרות מסוימות: חיפוש ממוקד למציאת קורבנות פשע (למשל מציאת קטינים ונעדרים); התמודדות עם מצבי חירום הנוגעים לביטחון הציבור ומניעת מתקפת טרור; איתור וזיהוי נאשם שיש להעמידו לדין בגין פשעים חמורים. עוד נקבע כי אף טרם ייעשה שימוש במקרים חריגים אלו יש לשקול את נסיבות האירוע, פוטנציאל הנזק בשימוש במערכת וההשלכות האפשריות על זכויות הפרט.²⁴

2.2. בריטניה

בריטניה הייתה מן המדינות הראשונות להפעיל מערכות ANPR (Automatic Number Plate Recognition) ומפעילה כיום מעל 11,000 מצלמות, ברמה הארצית, למעקב אחר פשיעה ופעולות טרור.²⁵ מערכות ה-ANPR

²⁰ בג"ץ 641/21 האגודה לזכויות האזרח בישראל נ' משטרת ישראל (עתירה למתן צו על תנאי 28/01/2021)

²¹ בג"ץ 641/21 האגודה לזכויות האזרח בישראל נ' משטרת ישראל, החלטה של הנשיאה חיות (נבו 20.04.2023).

²² Almeida, D., Shmarko, K. & Lomas, E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI Ethics* 2, 377–387 (2022).
²³ לדוגמה, פרשת Bridges v. South Wales Police. התובע, פעיל זכויות אדם, טען כי המערכת לזיהוי פנים שהמשטרה השתמשה בה באסיפות ציבוריות פוגעת בזכותו לכבוד אדם ופרטיות המידע בהתאם לחקיקה הפנימית המיישמת את ה-GDPR. בנוסף, טען כי בחינת ההשלכות (data privacy impact assessment או DPIA), אשר חובה לבצע על פי ה-GDPR, לא נעשה באופן ראוי. בית המשפט מצא לטובת התובע, ופרשה זו מוכיחה את החשיבות במסגרת חוקית רחבה וגם הוראות ספציפיות המדייקות את השימוש בטכנולוגיות אלו, שכן חלק משמעותי של טענות התובע נשענו על היעדר DPIA כראוי.

²³ שם.

²⁴ נוסח ההצעה להלן: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>

²⁵ ראו להלן: <https://web.archive.org/web/20200118140655/https://www.police.uk/information-and-advice/automatic-number-plate-recognition>

נמצאות בשימוש המשטרה הבריטית מאז שנת 2002.²⁶ לשם ההמחשה, רק ב-13 החודשים הראשונים במערכת עצרה המשטרה הבריטית 180,543 רכבים על סמך התרעות ANPR.²⁷ עצירות לצורך בדיקה אלו, בתורן, הובילו ל-13,499 מעצרים, השבת 1,152 כלי רכב גנובים ותפיסה בשווי £380,000 של סמים לא חוקיים.

מספר המעצרים של שוטרים עם מערכות ANPR הייתה פי 10 ממספר המעצרים בקרב שוטרים ללא המערכת. מאגר המידע אוגר את הנתונים הנקלטים של כלל הרכבים המצולמים, לרבות הרכבים אשר אינם בעלי עניין בעת הצילום.²⁸ מידי יום, נקלטים כ-60 מיליון נתונים למערכת אשר נאגרים יחד עם מידע דומה, למשך שנה אחת.²⁹

בשנת 2012, ממשלת בריטניה חוקקה את ה- Protection of Freedoms Act הכולל הגבלות ביחס לאיסוף, שימוש ואחסון מידע על הפרט.³⁰ כתוצאה מכך, משרד הפנים של בריטניה התקין סטנדרטים ביחס לשימוש במצלמות והמידע הנאסף מהן- National ANPR Standards for Policing and Law Enforcement (להלן NASPLE).³¹ בהתאם, המידע הנאגר יכול לשמש רק לשם אכיפת החוק, בידי רשויות אכיפת החוק ואסורה השימוש בנתונים לצרכים נוספים.³² בנוסף, השימוש במידע חייב להיות בהתאם לרגולציה האירופית העוסקת בנושא.³³ האסדרה בתחום מגדירה את המידע שחובה לאסוף (מספר הרישוי, השעה ומיקום גיאוגרפי כללי (בטווח של 10 מטרים)), כמו גם את המידע שניתן לאסוף (צילום תומך של הרכב, צילום של לוחית הרישוי ומיקום GPS מדויק של הרכב).³⁴

בנוסף, מעוגנים הסדרים הכוללים חובה לבצע הערכת סיכונים ביחס להטמעת המערכת, ביצוע הערכה אסטרטגית (תוך התחשבות בביטחון לאומי, פשיעה מאורגנת, פשיעה מקומית ואמון הציבור ביעד) וביצוע הערכת ההשפעות על ההגנה על פרטיות מידע אישי.³⁵ בנוסף, מעוגנים דרישות ביחס לדיוק המצלמות, יכולות הסנכרון לרשתות נוספות, החיבור למאגרי מידע והגבלת הגישה אליהם.³⁶ לבסוף, מעוגנים תקני הניהול והגישה לנתונים ביחס לאיסוף, אחסון, העברה ומחיקה של הנתונים.³⁷

United Kingdom Home Office Police, **ANPR- Driving Down Crime- Denying Criminals the Use of the Road** (2004),²⁶ https://web.archive.org/web/20070108145008/http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/Driving_Crime_Down_-_Denyin1.pdf?view=Binary שם.

Police.uk, **Advice and Information, Road Safety, Automatic Number Plate Recognition (ANPR)**²⁸ <https://www.police.uk/advice/advice-and-information/rs/road-safety/automatic-number-plate-recognition-anpr/> שם.

Legislation.gov.uk. Section 2, **Protection of Freedoms Act 2012**. [online]³⁰ <http://www.legislation.gov.uk/ukpga/2012/9/section/2/enacted>

UK Home Office, **National ANPR standards for policing and law enforcement (NASPLE)**, 2021 (Version 2.4, July 2022),³¹ <https://www.gov.uk/government/publications/national-anpr-standards/national-anpr-standards-for-policing-and-law-enforcement-accessible-version#Annex-A> שם.

ANPR Data: Legal Basis, 5.1 חלק שם,³³

Data Standards, Core Data, 7.4 חלק שם,³⁴

ANPR Infrastructure Development, 8.5 חלק שם,³⁵

Infrastructure Standards, 8.7 חלק שם,³⁶

Data Access and Management Standards 9 חלק שם,³⁷

הגישה לנתונים תתבצע רק לצורכי חקירה ותהא מוגבלת לגורמים שגישתם למערכת חיונית לביצוע תפקידם. רוב הגורמים שיקבלו גישה יהיו חשופים למידע שנאגר עד 90 ימים מיום צילומם ובמקרים חריגים (כגון משימות לוחמה בטרור), ניתן לקבל גישה לנתונים עד טווח של שנה (באישור מפקד בכיר).³⁸

2.3. ארצות הברית

בניגוד לאירופה, לארצות הברית מסגרת מבוצרת, בעיקר בעקבות היעדר גוף פדרלי אשר מפקח על הגנת מידע, וכן היעדר חקיקה פדרלית המציבה רף אליו כל המדינות צריכות להגיע.³⁹ מחקר של מרכז ברנן לצדק ציין כי השימוש ב-ALPR ברחבי ארצות הברית נפוץ ביותר, עם 93% ממשטרות בערים של מעל מיליון תושבים המפעילות מערכת מסוג זה.⁴⁰ לפי דו"ח של מדינת קליפורניה, לדוגמה, במשטרת עיריית לוס אנג'לס יש מעל ל-320 מיליון תמונות של לוחיות רישוי, ובעיר סקרמנטו נאספו 1.7 מיליון תמונות בשבוע בלבד. אולם, יש רק 16 מדינות אשר התייחסו מפורשות בדין לשימוש במערכות ה-ALPR (בפרט, ולא באופן כללי כהתייחסות לטכנולוגיות לזיהוי פנים) ואגירת הנתונים הנקלטים.⁴¹ המדינות השונות אסדרו את השימוש במערכת במגוון רחב של שיטות רגולציה תוך איזונים שונים בין הצורך באכיפת החוק לבין הגנת הפרט.

למשל, בקליפורניה השימוש במערכת מותרת ל-Highway Patrol וניתן לאגור מידע לתקופה שלא עולה על 60 ימים אלא אם המידע משמש כראיה בתיק פלילי.⁴² חשוב לציין, כי בקליפורניה ישנה חקיקה כללית המעגנת את החובה להגן על מידע (חוק הזכות לפרטיות - CCPA), אך אין בה התייחסות לגורמי אכיפת החוק.⁴³ במקביל, ישנן הצעות חוק להגביר את השימוש בטכנולוגיות לזיהוי פנים למטרות אכיפת החוק. יש לציין עוד כי יש מספר ערים בתוך קליפורניה, כגון ברקלי, בהן השימוש בטכנולוגיות לזיהוי פנים אסור. במיין, בדומה, השימוש במערכות ALPR אסורה למעט למטרות בטיחות ציבורית (Public Safety Purposes). כאשר נעשה שימוש במערכת, המידע הנאסף חסוי וישמש לצורכי אכיפת חוק בלבד וימחק תוך 21 ימים.⁴⁴ לבסוף, בניו המפשייר, החוק מגביל את השימוש במערכת לרשויות אכיפת החוק תחת הגבלות ולמטרות מוגדרות ומצמצמות ובלבד. ברמה המעשית, הנתונים הנקלטים לא ייאגרו וימחקו תוך 3 דקות ברגע קריאתם אלא אם הצילום הוביל למעצר או לדו"ח תנועה.⁴⁵

³⁸ Police.uk, ANPR, לעיל ה"ש 28.

³⁹ ראו לעיל ה"ש 22 (Almeida).

⁴⁰ Brennan Center for Justice, [Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use](https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations), 10.09.2020, available at: <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>.

⁴¹ National Conference of State Legislatures, [Automated License Plate Readers: State Statutes \(Updated February 03, 2022\)](https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes), <https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes>

Calif. Veh. Code § 2413⁴²

⁴³ ראו לעיל ה"ש 22 (אלמיידה).

⁴⁴ 29-A M.R.S.A. § 2117-A(2)

⁴⁵ N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130.

מעניין לראות, כי מחקר שפרסם המרכז לזכויות אדם באוניברסיטת וושינגטון הדגיש שהשימוש ב-ALPR מסכן בעיקר אוכלוסיות מוחלשות.⁴⁶ דוגמה בולטת היא האיום על זכויות מהגרים בארצות הברית. ערים רבות אימצו חוקי "sanctuary" אשר מגבילים את היכולת של עובדי הציבור בהם לשתף פעולה עם גורמי הגירה פדרליים, במטרה לסייע למהגרים הנמצאים בגבולותיה. אולם, המחקר מראה כי גוף אכיפת ההגירה (ICE) מסוגל לעקוף חוקים אלו תוך השימוש במערכות פרטיות ובפרט מערכות ALPR. במסגרת תביעה שהתנהלה בקליפורניה, הראו כי ICE השתמש במנוע חיפוש של תכנת ALPR אלפי פעם בחודש, למהלך שבע חודשים בשנת 2018.

דוגמה נוספת שעולה במחקר היא החשש שישתמשו במידע על מנת לאכוף חוקים נגד הפלות - גם במדינות שבהן הפלה חוקית. עוד מראה המחקר, כי בגלל ש-ALPR אוסף מידע באופן רחב ולא ממוקד - מרבית המידע שנשמר הוא על נהגים שלא מהווים סכנה לביטחון הציבור.⁴⁷ ככלל, לפי התיקון הרביעי לחוקת ארצות הברית, יש קושי לאפשר חיפוש ללא-חשש (suspicionless) של מאגרי מידע.⁴⁸

3. הצעת החוק הנוכחית

הצעת החוק, כמתואר בדברי ההסבר, נועדה לאזן נכונה בין ההגנה על הזכות החוקתית לפרטיות לבין "האינטרס הציבורי במניעת עבירות, גילוי, איתור מבצעים והבאתם לדין, ושמירה על הסדר הציבורי וביטחון הנפש והרכוש".⁴⁹ יצוין כבר עתה כי הצעת החוק מציעה לקבוע מסגרת כללית משותפת למגוון רחב של טכנולוגיות צילום מיוחדות, וביניהן מערכות כמו "עין הנץ" ומערכות זיהוי פנים, ואף כאלו שיתכן ועדיין לא נוצרו. בהתאם לכך, סעיף 10א להצעת חוק מציע לקבוע כי מערכת צילום מיוחדת הינה מצלמה אחת או יותר, בעלת מעבד ממוחשב המאפשר אגירה ועיבוד של נתונים או תמונה, באופן שיכול לזהות בזמן באופן חד ערכי, ובכך להתחקות או לבלוש אחר אדם.

סעיף 10ג המוצע, קובע כי מצלמה נייחת במערכת צילום מיוחדת לא תופעל באופן המאפשר צילום אדם כאשר הוא ברשות היחיד. ואולם, במקרה של מצלמות ניידות, שמטבען מיקומן משתנה ולא ניתן לשלוט בכל רגע נתון במרחב המצולם על ידן, מוצע לסייג את הכלל האמור ולקבוע שיחול "ככל הניתן".

⁴⁶ Washington State - Center for Human Rights, **Who's Watching Washington: Dangers of Automated License Plate Readers to Immigrant and Reproductive Rights**, 07.12.2022, available at: <https://jsis.washington.edu/humanrights/2022/12/07/whos-watching-washington/>

⁴⁷ המחקר חיפש האם יש מגבלות כראוי על שיתוף מידע ממערכות ALPR ומצא כי בווינגטון מרבית המועצות האזוריות מאפשרים שיתוף מידע עם כל גורם אכיפת החוק מדיני או פדרלי ללא מגבלות. כמו כן, הוסיף המחקר כי הנתונים שאוגרו שומשו לאיתור רכבים גנובים מעט מאוד - בבלינגהם 0.000027%, במונרו 0.00032%, ובברמטון 0.00189%. בפרשת קרפנטר נ' ארצות הברית, בעניין איסוף מידע מהיסטוריית מכשיר נייד, מצא בית המשפט כי "ההיקף, העומק והיסודיות" של המידע לצד האופן האוטומטי של אסיפתו מחייבים צו ברמה של probable cause. עוד נתון מעניין מפרשת קרפנטר הוא שבית המשפט קבע שאנשים לא משתפים את המיקום שלהם באופן הסכמי - אלא מדובר בחלק בלתי נפרד מהחזקת מכשיר נייד, שזה נחשב למשהו הכרחי ביותר להשתתפות בחברה המודרנית. על אף האמור, המאמר מצא שבתי המשפט טרם אימצו את הלכת קרפנטר על ALPR ובמקום נוקטים בגישה לא אחידה ביחס למקרים אלו.

⁴⁸ Jenifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases*, National Security, Technology & Law at Hoover Institute, Aegis Series Paper No. 2104, available at: [lynch_webready.pdf\(hoover.org\)](lynch_webready.pdf(hoover.org)). בהתאם, השימוש הכוללני בחיפוש מסוג זה מקביל לצווים הכלליים שבעקבותם נוסח תיקון זה לחוקה - ועל כן יש להכיר בהם כהפרה מטבעם.

⁴⁹ הצעת החוק, בעמ' 123.

סעיף 10ח המוצע, קובע את זהות בעל הסמכות אשר בסמכותו לאשר הצבה והפעלה של מצלמה מיוחדת נייחת. הסעיף מבחין בין הצבה והפעלה של מצלמה לפרק זמן העולה על שלושה חודשים – שלגביה נדרש אישורו של קצין מוסמך, המוגדר בסעיף 10א כקצין משטרה בדרגת תת-ניצב ומעלה, לבין הצבה והפעלה של מצלמה לפרק זמן שאינו עולה על שלושה חודשים, שלגביה נדרש אישור של גורם מאשר המוגדר בסעיף 10א כקצין בדרגת ניצב משנה ומעלה ממערך החקירות והמודיעין של משטרת ישראל.

סעיף 10ז להצעת החוק, מונה את המטרות אשר לשם מימושן ניתן להורות על הצבה והפעלה של מערכת צילום מיוחדת, בין אם היא נייחת או ניידת, והן: מניעה, סיכול או גילוי של עבירות פשע או עבירות שעלולות לסכן את שלומו או ביטחונו של אדם, את שלום הציבור או את ביטחון המדינה וכן גילוי מעורבים בביצוע עבירות כאמור;⁵⁰ מניעת פגיעה חמורה בביטחון הנפש או הרכוש כאשר קיים חשש ממשי לפגיעה שכזו; איתור נעדר או אדם שיש חשש לשלמו; אכיפת איסורי כניסה שניתנו על פי דין וצוויו הרחקה ממקום ציבורי.

סעיף 10ט להצעה, מתווה את שיקול הדעת של הגורם המוסמך לאשר הצבה והפעלה של המצלמות, וזאת בשים לב לשני שיקולים מרכזיים: האחד, הצבת המצלמה נועדה להשגת מטרה, אחת או יותר, מהמטרות המפורטות בסעיף 10ז. השני, הצבת המצלמה הספציפית אינה פוגעת בפרטיותו של אדם במידה העולה על הנדרש. הסעיף מוסיף וקובע כי מצלמות נייחות מיוחדות יוצבו באופן הגלוי לעין אלא אם יקבע אחרת וכן שיש לבחון את האפשרות ליידע את הציבור בדבר הצבת המצלמה באמצעות שילוט מתאים או באופן מקוון.

סעיף 10י להצעת החוק, קובע כי הקצין המוסמך יבחן, אחת לשלוש שנים, את הצורך בהמשך הצבתה והפעלתה של כל מצלמה מיוחדת נייחת ואת התקיימות התנאים שפורטו לעיל.

אשר למצלמות ניידות, סעיף 10יב מציע לקבוע שהפעלתן תיעשה לפי נוהל שיקבע על ידי קצין מוסמך, ויסדיר את ההיבטים השונים הכרוכים בהפעלת מצלמות אלו. כמו כן, מוצע לקבוע כי הנוהל האמור ייקבע בהתאם למטרות המפורטות בסעיף 10ז ובאופן שבו לא תיפגע פרטיותו של אדם במידה עולה על הנדרש.

סעיף 10יג המוצע, מפרט את התנאים שבהם תהא רשאית המשטרה לעשות שימוש טכנולוגי בדיעבד במידע שנאגר מהמצלמות המיוחדות. תנאים אלו מציגים רשת רחבה יותר של מקרים ביחס למטרות ההצבה וההפעלה של מצלמה מיוחדת והם כוללים את המטרות המנויות בסעיף 10ז וכן לשם הצלה והגנה על חיי אדם; גילוי עבירות פשע ועבירות עוון המנויות בתוספת החמישית להצעת החוק, חקירתן או מניעתן וכן לצורך הליך פלילי; גילוי עבריינים בעבירות פשע ובעבירות המנויות בתוספת האמורה והעמדתם לדין; חילוט רכוש על פי דין; וחקירת דפוסים של ביצוע עבירות

⁵⁰ הצעת החוק מפנה, לדוגמה, לסעיפים 2 ו-10 לפקודת התעבורה [נוסח חדש] לעניין רישיון רכב שחלפה שנה ומעלה מיום שפקע תוקפו או רישיון נהיגה שחלפו שנתיים ומעלה מיום שפקע תוקפו או נהיגה בידי מי שלא החזיק מעולם ברישיון רכב.

כאמור (ובלבד שהמידע אינו כולל פרטים מזהים וכי הדבר אושר בידי קצין משטרה בדרגת ניצב משנה שהוסמך לעניין זה על ידי המפק"ל).

סעיף 10(ג) להצעת החוק, מציג הוראות בדבר שמירת המידע שנאגר בידי המשטרה, וקובע, בין היתר, הגבלות זמן לשמירת המידע, כאשר פרק הזמן המירבי לשמירת המידע לא יעלה על שנתיים לגבי מידע שנאסף ממצלמות מיוחדות נייחות, או על שנה לגבי מידע שנאסף ממצלמות מיוחדות ניידות. כמו כן, מוצע לקבוע כי בחלוף שישה חודשים מיום איסוף המידע ממצלמה נייחת, או לאחר שלושה חודשים מיום איסוף מידע ממצלמה ניידת, המידע שנאסף יופרד מכל מידע אחר במערכת והשימוש בו יתאפשר רק אם ניתן אישור לכך בידי גורם מאשר ולשם השגת מטרה מהמטרות המפורטות בסעיף 10(ג) בהתייחס לעבירות פשע חמור בלבד (סעיף 10(ג)(ב)).

סעיף 10(ב) להצעת החוק, קובע כי אדם שהגיע לידי מידע כאמור בפרק זה, ישמור אותו בסוד, לא ימסור ולא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא אך לפי הוראות הצעת החוק.

סעיף 10(ז) להצעה, מסדיר את אופן העברת מידע שנאסף ממערכות הצילום לידי גופים ציבוריים, כהגדרתם בסעיף 10א. בפרט, מוצע כי מידע יועבר לגופים אלו רק בשני מצבים: האחד, בהתאם לבקשתו של הגוף הציבורי לשם מילוי תפקידו וזאת בלבד שהמידע נדרש לשם מטרה מהמטרות בסעיף 10(ז) או לצורך "הגנה על ביטחון המדינה"; השני, במצב בו מסירת המידע לגוף הציבורי דרושה למטרה למען הגשמת מטרה מהמטרות בסעיף 10(ג).

סעיף 10(כא) המוצע, קובע כי המשטרה חבה בחובת דיווח, אחת לשנה, ליועצת המשפטית לממשלה באשר לנתונים שונים הנוגעים לאופן השימוש במערכת המפורטים בתוספת השישית וכוללים, בין היתר, את מספר המצלמות המיוחדות שהופעלו; מספר הצילומים ששימשו כראיה בתיק חקירה ומתוכם מספר התיקים שהוגש בהם כתב אישום; המקרים שבהם נעשה שימוש במערכות לשם טיפול באירוע המסכן חיים או אירוע שיש בו סכנה לביטחון המדינה; מספר המקרים שבהם נעשה שימוש במידע שנאגר במערכות למטרות המנויות בסעיף 10(ג)(א), שאינן כלולות במטרות המנויות בסעיף 10(ז); מספר מורשי הגישה למידע שנאגר במערכות, בפילוח לפי תפקידם ופירוט הרשאות הגישה שלהם.

סעיף 10(כב) מוסיף ומציע לקבוע שהשר לביטחון לאומי ידווח אחת לשנה לוועדה לביטחון לאומי של הכנסת באשר לנתונים שונים (רשימה זו מצומצמת ביחס לרשימה המופיעה בתוספת השישית) וביניהם מספר הצילומים ששימשו כראיה בתיק חקירה, ומתוכם מספר התיקים שהוגש בהם כתב אישום; מספר מורשי הגישה למידע שנאגר במערכות בפילוח לפי תפקידם; מספר החפצים שזוהו במערכות.

אנו מברכים על הצעד החשוב של אסדרת השימוש בטכנולוגיות צילום מיוחדות, ובפרט עין הנץ, בחקיקה. צעד זה מבקש לקדם שימוש סדור בטכנולוגיות אלו תוך איזון שיקולים רלוונטיים. כמו כן, יש בהצעת החוק התייחסות לנושאים מרכזיים וחשובים וכן מענים לסיכונים קיימים מסויימים. הצעת החוק מגבילה את המטרות שלשמן ניתן להשתמש במידע הנאסף, מתווה את שיקול הדעת של הגורמים המוסמכים וקובעת מנגנון להעברת מידע. יחד עם זאת, יש שני נושאים בולטים אשר לדעתנו נדרשים לקבל התייחסות בהצעת החוק, שכן הם מעוררים סיכונים ממשיים ביחס לזכות לפרטיות: אבטחת מידע, ופיקוח על השימוש במידע והעברתו.

4.1. רמת אבטחה מספקת

כאמור, המידע הנאסף ממערכת עין הנץ כולל תמונות ומיקום מדויק של כמעט כל עוברי דרך בישראל. ישנה חשיבות רבה כי תהיה הגנה מרבית ומיטבית על המידע הרגיש הזה. אך, כפי שנלמד מהביקורת המתמשכת על ניהול המאגרים הביומטריים באחריות מדינת ישראל, נראה כי לא ננקטו פעולות לשמירה אפקטיבית על מידע זה.

בדיווחו של הממונה על היישומים הביומטריים רועי פרידמן, משנת 2022, עולות מספר בעיות הנוגעות לאופן ניהול המידע, ובפרט לסוגיית האבטחה של המאגרים.⁵¹ חשוב לציין כי הדאגות שהועלו בדו"ח זה אינן ראשוניות, אלא מדובר בסוגיות חוזרות בדיווחיו של הממונה, שאף הועלו בעבר על ידי מבקר המדינה. העלה הממונה בעיות מהותיות הנוגעות לניהול מידע ביומטרי בישראל, ובפרט העברת תמונות לגופים ממלכתיים אחרים ושלא על פי חוק, אי הערכות לפקיעת הוראת השעה המסדירה את הניהול של המאגרים הביומטריים בישראל, פגם בכיול מערכת ההשוואה הביומטרית ועוד. פערים אלו מעידים על בעיות עם אופן הניהול התקין של מאגר ביומטרי עצום ורגיש, מה שחושף את אזרחי ישראל לפגיעה אפשרית בזכותם החוקתית לפרטיות. דאגה מיוחדת העולה מן הדו"ח, נוגעת לרמת האבטחה של מאגרי מידע ביומטרי בישראל.

מעבר לחששותיו של הממונה על היישומים הביומטריים, ראוי לציין גם את הביקורת המקיפה שביצע מבקר המדינה בשנת 2020 בנושא ניהול מאגרים ביומטריים בישראל ושימוש במידע הנאגר בהם.⁵² בין היתר, ציין מבקר המדינה כי נדרשת אסדרת המאגרים הביומטריים הממשלתיים בחקיקה וכן לוודא את עמידת המאגרים הביומטריים בעקרונות המדיניות הלאומית ליישומים ביומטריים ובקווים המנחים ליישומה. כפי שניתן לראות, מבקר המדינה מחזק את החששות שמופיעים בדיווחיו של הממונה על יישומים ביומטריים. בעוד כמות המידע שיש במאגרים הביומטריים רק גדל מאז שפורסמו מסקנות מבקר המדינה, קשה לומר שרמת ההגנה עליו השתפרה במקביל.

איננו זרים בישראל להשלכות מרחיקות הלכת של תקיפות סייבר על מאגרי מידע, כפי שקרה ביחס למתקפה על חברת הביטוח שירביט, על רקע ההתמודדות עם התפשטות מגפת הקורונה.⁵³ החשש איננו רק מדליפת המידע

⁵¹ דו"ח הממונה על היישומים הביומטריים - מס', 12, הממונה על היישומים הביומטריים במערך הסייבר הלאומי, 18.05.22, סימוכין 1313, [25 ci_bg_2060443.pdf \(knesset.gov.il\)](https://www.knesset.gov.il/25_ci_bg_2060443.pdf).

⁵² מבקר המדינה, היבטים בהסדרת השימוש במאגרים ביומטריים, דוח שנתי 70, 04.05.2020, [היבטים בהסדרת השימוש במאגרים ביומטריים](https://www.mevaker.gov.il/) (mevaker.gov.il).

⁵³ Tal Mimran and Yuval Shany, Israel, Cyberattacks and International Law, LAWFARE (Dec. 30, 2020), at <https://www.lawfareblog.com/israel-cyberattacks-and-international-law>.

הקיים, אלא ישנן סכנות נוספות אותן יש להביא בחשבון.⁵⁴ זאת, מאחר ומדובר במידע עם חשיבות אדירה, בעל ערך כלכלי רב, אשר שחקנים שונים, דוגמת חברות פרטיות, יכולים לנצל בקלות.

נראה כי החששות אשר הועלו על ידי הממונה על היישומים הביומטריים, כמו גם מבקר המדינה, טרם קיבלו מענה מוסדי, או חקיקתי. ראוי כי בעת אסדרת השימוש במערכות נוספות אשר במסגרתן נאגר מידע רגיש רב מאוד, יינתן מענה לחשש מרכזי זה לפיו המידע אשר נשמר אינו מבטח באופן מספק. אין מקום להמשיך לאסוף ולאגור מידע על אזרחי ישראל מבלי להבטיח רמת אבטחה מספקת.

4.2. פיקוח מוגבר על שימוש והעברת מידע

כפי שנלמד מן הסקירה המשווה, חשש מרכזי ביחס להפעלות מערכות מסוג עין הנץ הוא כי המידע שנאסף ישמש מטרות זרות או יועבר לגופים אחרים ולא לצורך מימוש היעדים שלשמן נאסף. אמנם, הצעת החוק מגבילה את השימושים המותרים של מידע זה, וכן מציבה מנגנון העברת מידע. ועדיין, מדובר בסוגיה רגישה הדורשת רמה גבוהה יותר של פיקוח על מנת לוודא שהשימושים היחידים במידע זה הוא על פי חוק.

כפי שעלה מפרשת פגסוס-סייפן, המשטרה נכונה לעשות שימוש בטכנולוגיות מתקדמות על מנת לאכוף את החוק – גם אם בהתבסס על הסכמה חוקית רעועה, אם בכלל, ולעיתים באופן מרחיק לכת אשר פוגע בפרטיות. לקח מרכזי שנלמד מפרשה זו, הוא הצורך בפיקוח חיצוני על הנעשה במשטרה על מנת לוודא שהטכנולוגיות אינן מנוצלות לרעה כלפי אזרחי ישראל. פיקוח שכזה צריך להגיע מצד הייעוץ המשפטי לממשלה, בשלב ההכנסה לשימוש של המערכת, ובהמשך על ידי הכנסת – אשר תפקיד מרכזי שלה הוא פיקוח על הממשלה, ובפרט ביחס להפעלת כוח שלטוני המאגיר את חירויות הפרט. ניתן לשייך פיקוח זה לאחת מוועדות הכנסת, להקים ועדת משנה מיוחדת או למנות ממונה מטעם הכנסת.

והנה, בפנינו מערכת טכנולוגית נוספת, אשר מובילה לאיסוף מידע רגיש על אינספור אנשים בישראל. ישנה חשיבות רבה בהבטחה שיעשה שימוש במידע זה אך ורק למטרות המפורטות בחוק. לשם הבטחת מטרה זו, ישנו צורך במנגנון פיקוח מוגבר ומקיף אשר יפקח על אופן איסוף, שמירה ומחיקת המידע, כמו גם על השימוש במידע והעברתו.

5. סיכום

מערכת עין הנץ מופעלת על ידי משטרת ישראל זה מכבר, והצעת החוק שבנדון באה להסדיר את השימוש בה ובמערכות דומות. כפי שנלמד, במדינות העולם יש שימוש נרחב בטכנולוגיה זו וגישות שונות להתמודדות עם הסכנות הכרוכות בה, ובעיקר שימוש לרעה במידע. הצעת החוק מהווה צעד חשוב לשמירה על פרטיות והבטחת שימוש הוגן בטכנולוגיה זו. אולם, נעדרת התייחסות לפן של אבטחת המידע הנאסף – המהווה כשל רוחבי ביחס למידע שנאסף

⁵⁴: at Identity Management Institute, Benefits and Risks, Biometric Authentication, למשל" ר
<https://identitymanagementinstitute.org/biometric-authentication-benefits-and-risks/>.

במדינת ישראל. כמו כן, נדרש מנגנון פיקוח מוגבר וחיצוני אשר יבטיח שלא יהיה ניצול לרעה של המידע הנאסף. נושאים אלו חשובים ביותר לניהול התקין של מערכת עין הנץ, ואנו מציעים שיקבלו מענה במסגרת הצעת החוק.



ד"ר טל מימרן

ראש תכנית,

תכלית – המכון למדיניות ישראלית



עו"ד עדן פרבר

חוקרת,

תכלית – המכון למדיניות ישראלית