

## דרושה בינה אנושית: מחשבות על השימוש הגובר של משטרת ישראל בטכנולוגיות לאיסוף מידע אישי

מאת

טל מימרון וגל דהן\*

### 1. מבוא

לאחרונה, אנו עדים למרוץ חימוש של משטרת ישראל בכלים טכנולוגיים רבי עוצמה לצורכי איסוף מידע אישי. הסיפור שלנו מתחיל לפני שנה וחצי, עם חשיפתו של תומר גנון מכלכליסט כי משטרת ישראל רכשה את רוגלת פגסוס מחברת NSO.<sup>1</sup> גילוי זה הוביל לסערה ציבורית, ולהקמת צוות בדיקה בהובלת המשנה ליועמ"ש עמית מררי. לאחר שדו"ח מררי פורסם, למדנו כי הרוגלה שנרכשה היא לא פגסוס, אלא תוכנה שהותאמה במיוחד עבור משטרת ישראל בשם סייפן, וכי היא הוכנסה לשימוש מבלי שהמשטרה, הפרקליטות או בתי המשפט הפנימו את יכולותיה מרחיקות הלכת.<sup>2</sup>

פרשת פגסוס סייפן הייתה יריית הפתיחה לדיון ציבורי מתמשך לגבי השימוש של משטרת ישראל בכלים טכנולוגיים – דוגמת מערכת עין הנץ, ומערכת לאיתור

\* ד"ר טל מימרון הוא ראש תוכנית במכון תכלית, מנהל המחקר של מרכז פדרמן לחקר הסייבר באוניברסיטה העברית, ומרצה במכללה האקדמית צפת.

מר גל דהן הוא חוקר במכון תכלית, ועורך המשנה של כתב העת "חוקים" באוניברסיטה העברית, אשר משלים בימים אלה תואר בוגר במשפטים (LL.B) באוניברסיטה העברית.

<sup>1</sup> תומר גנון "חברת NSO בשירות משטרת ישראל: פריצות לטלפון של אזרחים ללא פיקוח או בקרה" כלכליסט (18.1.2022).

<sup>2</sup> דין וחשבון הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים 56 (2022) (להלן: דו"ח מררי).

חשודים בנתב"ג, המבוססת על בינה מלאכותית.<sup>3</sup> אין לכחד, השימוש במערכות אלו אכן מביא לשיפור במישור המבצעי, ומשכך הוא נושא חשיבות רבה. ואולם, אין לקבל שימוש בלתי מוגבל באמצעים טכנולוגיים מסוג אלו. שימוש לרעה בכלים טכנולוגיים בידי רשויות האכיפה מקעקע את שלטון החוק, ומעלה חששות לגבי פגיעה בחירויות יסוד של אזרחי מדינת ישראל ובמיוחד באשר לזכות לפרטיות, הזכות לכבוד, הזכות לשוויון, חופש התנועה וחופש הביטוי.

ברשימה זו נתייחס לכלים הטכנולוגיים השונים לאיסוף מידע אישי בהם עושה שימוש משטרת ישראל, ונבקש להציע איזון בין האינטרסים על הכף – הגנה על ביטחון לאומי, אך לא במחיר של פגיעה בחירויות הפרט דוגמת הזכות לפרטיות, קידום וביסוס חדשנות טכנולוגית, שיקולים כלכליים כבדי משקל, ותדמיתה הבין לאומית של מדינת ישראל. הפתרון שנציע כולל מיסוד שני נתיבי פיקוח משלימים לאלו הקיימים, האחד בשלב הפיתוח של טכנולוגיות לאיסוף מידע אישי, והשני לאחר הכנסתן לשימוש מבצעי.

## 2. מקרי המבחן

### א. פרשת פגסוס-סייפן

תוכנת פגסוס היא מוצר הדגל של חברת NSO, והשימוש בה מאפשר גישה למחשבים ולמכשירים אישיים במטרה לאסוף מידע, לצורכי ריגול, מעקב ומניעת פשיעה. בשנים האחרונות, הצטברו עדויות על שימוש לרעה לכאורה בפגסוס ברחבי העולם, ובפרט נגד פעילים פוליטיים, עיתונאים ופעילי זכויות אדם.<sup>4</sup> ידיעות אלו יצרו משבר אמון ביחס לתעשיית הסייבר ההתקפי בישראל, אשר יש לה חשיבות עצומה עבור כלכלת ישראל ותדמיתה הבינלאומית,<sup>5</sup> ואף הובילו למהלכים משפטיים ודיפלומטיים שונים ביחס לטענות לשימוש ברעה בפגסוס.<sup>6</sup>

<sup>3</sup> אלו, יש להוסיף גילוי אודות רכישה לכאורה עלידי משטרת ישראל מחברת הסייבר הישראלית "רייזון" תוכנה המאפשרת לאתר מיקום ומסלול תנועה של משתמשי סלולר, וזאת ללא בחינה מקדימה או אישור של היעוץ המשפטי לממשלה, בניגוד להמלצת ועדת מרזי, אשר הבהירה כי על המשטרה לקבל את אישור היעוץ המשפטי לממשלה טרם רכישה של מערכת טכנולוגית בעלות יכולת חדשה מבחינת איסוף מידע. ראו תומר גנון "בניגוד להנחיות מרזי: המשטרה רכשה תוכנת מעקב חדשה ללא אישור היועמשי" **כלכליסט** (28.5.2023).

<sup>4</sup> הדיווחים התייחסו למדינות שונות וביניהן איחוד האמירויות, אל-סלבדור, בחריין, הונגריה, הודו, ירדן, מקסיקו, מרוקו, ספרד, צרפת, פולין, קזחסטן, רואנדה וערב הסעודית. ראו למשל עומר כביר "סייזן לאב: פגסוס ריגלה אחר עיתונאים ופעילי זכויות אדם במקסיקו עד 2021" **כלכליסט** (3.10.2022); Omer Benjakob, *The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware*, **HAARETZ** (5.4.2022).

<sup>5</sup> הסכום המוערך של הייצוא הביטחוני בשנת 2020 עמד על כ-8 מיליארד דולרים, כאשר הסכום אף עלה בשנת 2021 לשיא של 11.5 מיליארד דולרים. מתוך סכום זה, כ-10% מההכנסות מבוססות על טכנולוגיות סייבר. ראו מערכת אתר משרד הביטחון, "חוזי הייצוא הביטחוני ב-2020: 8.3 מיליארד דולר" **אתר משרד הביטחון** (1.6.2021); מערכת אתר משרד הביטחון, "2021: שנת שיא בייצוא הביטחוני של ישראל" **אתר משרד הביטחון** (12.4.2022).

<sup>6</sup> כך, למשל, הפרלמנט האירופאי הקים ועדת חקירה שמתמקדת בהשפעה של פגסוס וטכנולוגיות מעקב דומות על זכויות יסוד, וחברת NSO הוכנסה לרשימה השחורה של מחלקת המסחר

זמן לא רב לאחר גילויים אלו, התעורר חשד כי משטרת ישראל השתמשה גם היא ברוגלת פגסוס, לריגול ולאיסוף מידע וראיות, אחר דמויות פוליטיות שונות ופקידים בכירים, אולי אף ללא אישור שיפוטי.<sup>7</sup> בעקבות הביקורת הציבורית שהתעוררה נוכח הפרסומים, הוקמה ועדת מררי, אשר קבעה כי ההכנסה של מערכת האזנות רחבת היקף נעשתה בלי שהובנה לאשורה על ידי מקבלי ההחלטות.<sup>8</sup> ועדיין, קבע הדו"ח כי המשטרה לא השתמשה במערכת בניגוד לצו שיפוטי.<sup>9</sup>

לאחר אימוץ הדו"ח, אשר זכה לביקורת בשל היותו סלחני לכאורה לגבי המחדלים שנתגלו, החל רצף דיונים של ועדת החוקה, חוק ומשפט של הכנסת ביחס לפרשה, במסגרתם התעוררו מתחים רבים בין חברי הוועדה ובין נציגי המשטרה והפרקליטות, ובין נציגי המשטרה והפרקליטות עצמם. דיונים אלו הוכיחו את חשיבותם במובן של שקיפות ציבורית, וגם בזכות העובדה שהם הובילו לגילויים חדשים. למשל, נתחוו כי הפרקליטות מבצעת בדיקת עומק באשר לשימוש בראיות הנובעות משימוש ברוגלות, ואף החליטה למשוך ראיות שהוגשו במסגרת תיק רצח כפול המתנהל בימים אלו, היות שאלו נשאבו בניגוד לחוק.<sup>10</sup>

בסיום סבב הדיונים, קראה ועדת החוקה לממשלה להקים ועדת חקירה ממשלתית או ועדת בדיקה ממשלתית, בראשות שופט, בנושא הפעלת רוגלות על-ידי משטרת ישראל.<sup>11</sup> ואכן, ממש לאחרונה, הכריז שר המשפטים, יריב לוין, על הקמת ועדת בדיקה ממשלתית, בראשות שופט בדימוס, אשר תבדוק את התנהלות המשטרה, הפרקליטות ומערכות הפיקוח, ביחס לפעולות רכש, כמו גם הפעלת אמצעי מעקב ואיסוף טכנולוגיים.<sup>12</sup>

פרשת פגסוס-סייפן מעידה על חשיבות הגברת הפיקוח על אופן ההכנסה לשימוש של טכנולוגיות חדשות, על-ידי משטרת ישראל, במטרה להפעיל סמכות שלטונית כנגד אזרחי ישראל. חשיבות זו מתחדדת על רקע העובדה שישנו פיתוי רב יותר לעשות שימוש בטכנולוגיות באקלים רגיש פוליטי וביטחוני – כמו במחוזותינו.<sup>13</sup>

האמריקאית. לבסוף, חברות טכנולוגיה מובילות בעולם תובעות את NSO בשל שימוש לרעה ופריצה למערכות שלהן, ובפרט אפל ומטה. ראו למשל: *WhatsApp v. NSO Group, et al*, No. 4:19-cv-7123 (N.D. Cal. 29.10.2019); *Apple Inc. v. NSO Group Technologies Limited* No. 3:21-cv-09078 (N.D. Cal. 23.11.2021).

<sup>7</sup> גנון, לעיל ה"ש 1.

<sup>8</sup> דו"ח מררי, לעיל ה"ש 2, בעמ' 56.

<sup>9</sup> שם, בעמ' 4 ר 32. לביקורת על דו"ח מררי, ראו רועי פלד "שתי הערות ושתי טענות בעקבות קריאה בדוח מררי" *ICON-S-IL Blog* (9.10.2022).

<sup>10</sup> חן מענית "הפרקליטות משכה ראיות מתיק רצח כי הושגו ראיות על ידי שימוש ברוגלות שלא כד"ן" *הארץ* (05.06.2023).

<sup>11</sup> מתן וסרמן "ועדת החוקה לממשלה: הקימו ועדת חקירה על פרשת פגסוס ו-NSO" *מעריב* (13.6.2023).

<sup>12</sup> אברהם בלוח "בעקבות פרשת פגסוס: לוין הודיע על הקמת ועדת בדיקה ממשלתית" *מעריב* (20.7.2023).

<sup>13</sup> ראו לעניין זה למשל טל מימרן וליאור וינשטיין "הממשלה מפקירה את הפרטיות" *העין השביעית* (29.10.2022); בג"ץ 2109/20 בן מאיר נ' ראש הממשלה (נבו) (26.04.2020).

כיום, הרגולטור העיקרי אשר מפקח על שוק הסייבר ההתקפי הוא משרד הביטחון, אשר אחראי על מתן רישיון שיווק וייצוא של מוצרים אלה, אך יכולתו לפקח מוגבלת מכובעו הכפול (מפקח ולקוח פוטנציאלי) ובשל תופעות דוגמת הדלת המסתובבת (מעבר של בכירים ברגולטור לתעשייה, ולהיפך). במישור הטכנולוגי, קשה במיוחד לפקח על ייצור, שיווק או שימוש בכלי סייבר מאחר ואלו יכולים להיות משוכפלים ולפעול ברחבי העולם בו זמנית – להבדיל מכלי נשק רגילים שמוגבלים למיקום פיזי אחד. בנוסף, עובד ממורמר של חברה טכנולוגית יכול לנסות ולמכור מוצר בשוק השחור, וכן ניתן להעתיק קוד, או לפתח תוכנות נגזרות שיכולות להביא לפגיעה זדונית.

כפי שניתן לראות, שוק הרגולטור סובל מתת-פיקוח, ונדרש ליותר פיקוח על מנת לוודא בטווח הארוך שמירה על אינטרסים כלכליים ותדמיתיים של מדינת ישראל, וזאת לצד קידום הגנה מיטבית על זכויות אדם. תעשיית הסייבר ההתקפי בישראל משמשת חלק ניכר מסל מוצרי הייצוא הצבאי עליהם נסמכת כלכלת ישראל. כמו כן, תדמיתה של ישראל בתור מעצמה טכנולוגית חשובה גם בכדי לקדם יחסים דיפלומטיים עם מדינות וגם כדי לשמר מאזן הרתעה מול גורמי אויב. בהתאם, בפרק המסכם של רשימה זו נציע מנגנונים לחיזוק הפיקוח על שוק חשוב זה.

## ב. השימוש במערכת עין הנץ

מערכת נוספת המעוררת דאגה בקרב הציבור, היא מערכת עין הנץ אשר רותמת את היכולות של טכנולוגיית זיהוי פנים – העושה שימוש באלגוריתם שמסוגל לזהות או לאמת בהתבסס על תמונה או סרטון וידאו זהות של בן אדם, או לוחית רישוי במקרה של מערכת זו, באופן אוטומטי או אוטומטי למחצה.<sup>14</sup> מערכת עין הנץ מבוססת על מערך מצלמות המותקנות בכבישים ברחבי הארץ אשר עוקבות, מצלמות ומזהות באופן אוטומטי ובכל שעות היממה לוחיות רישוי באמצעות טכנולוגיות עיבוד תמונה מתקדמות (Automatic License Plate Reader).<sup>15</sup>

שנים רבות שמשטרת ישראל עושה שימוש במערכת זו ביחידותיה השונות וביניהן, יחידת מג"ב, אגף התנועה ואגף המבצעים – זאת בטרם הוסדר השימוש במערכת בחקיקה. כחלק מן השימוש במערכת מתפעלת המשטרה מאגר מידע אשר כולל רשימה של כלי רכב שנגנבו, הורדו מהכביש, צילומי וידאו ותמונות סטילס שנאספו באמצעות המצלמות הפרושות ברחבי הארץ, לרבות תמונות הרכב, מספר לוחית הרישוי ותמונות תקריב של הנוסעים בתוכו שבהן נראים בכירור פניהם של הנוסעים.<sup>16</sup>

<sup>14</sup> מערך הסייבר הלאומי – היחידה להזדהות וליישומים ביומטריים זיהוי פנים במרחב הציבורי בישראל עקרונות למדיניות וקריאה לאסדרה 4 (יולי, 2021) (להלן: דו"ח מערך הסייבר הלאומי).

<sup>15</sup> רועי גולדשמידט, "השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי", מרכז המחקר והמידע של הכנסת, 14 בדצמבר 2020 (להלן: דו"ח מרכז המחקר והמידע של הכנסת); ראו גם את עתירת האגודה לזכויות האזרח בישראל כנגד שימוש המשטרה במערכת עין הנץ (בג"ץ 641/21), בפס' 16, 19, <https://www.acri.org.il/post/488>.

<sup>16</sup> שם.

בשנים האחרונות, ניתן לראות עלייה ניכרת בשימוש בראיות מתוך המאגר שנוצר בעקבות פעילות מערכת עין הנץ.<sup>17</sup> כך, לדוגמה, במ"ת (שלום ב"ש) 57000-02-23 **מדינת ישראל נ' שטרית** (10.5.2023), תיעוד וצילום ממאגר מערכת עין הנץ סייע לבסס תשתית ראייתית נגד הנאשם לצורך החלטה על מעצר עד תום ההליכים.

לצד היתרונות הגלומים בשימוש במערכת עין הנץ, לשימוש נלווים גם סיכונים הדורשים לתת עליהם את הדעת. **החשש הראשון** נוגע לשגיאות ולכשלים 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).<sup>18</sup> חשש זה בא לידי ביטוי בבריטניה, שם נמצא כי שיעורי התראות השווא כתוצאה משימוש במערכת לזיהוי פנים במרחב הציבורי עמד על כ-90%.<sup>19</sup>

**החשש השני** הוא בהיבט של מעקב טכנולוגי ופגיעה בפרטיות. השימוש בעין הנץ צפוי להוביל לאגירת מידע אישי באופן שעלול לשמש בפועל למעקב אחרי האנשים המתועדים, גם לצורך מטרות אשר לא נקבעו או הובהרו מראש, למשל נטייה מינית או הרגלי צריכה של אדם, תוך הפרה של הזכות החוקתית לפרטיות.<sup>20</sup> "מהחשבה שבזכויות האדם" ו"אחת מהחירויות המעצבות את אופיו של המשטר בישראל כמשטר דמוקרטי".<sup>21</sup> לכך יש להוסיף את האפקט המצנן שעתיד להיווצר ביחס להתנהגות הפרט, מתוך חשש לשימוש לרעה במערכת זו (כפי שעלה ביחס לטכנולוגיות מעקב אחרות, למשל השימוש בכלי של השב"כ בזמן משבר הקורונה).<sup>22</sup>

**החשש השלישי** מקורו בסיכון של דליפת מידע ביומטרי מהמאגר של מערכת עין הנץ, אשר עלול להביא לשימוש לרעה בכלים ויכולות בידי גורמים לא מורשים, ללא פיקוח ובקרה אפקטיביים.<sup>23</sup> מדובר בחשש מתמשך לגבי מאגרים ביומטריים

<sup>17</sup> ראו מיני רבים: מ"ת (מחוזי חי') 46950-01-23 **מדינת ישראל נ' עאשור** (נבו 28.2.2023); 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).

<sup>18</sup> דו"ח מערך הסייבר הלאומי, לעיל ה"ש 14, בעמ' 8.  
<sup>19</sup> Chris Fox, [Face Recognition police tools 'staggeringly inaccurate'](#), BBC (15.5.2018).

<sup>20</sup> ס' 7 לחוקיסוד: כבוד האדם וחירותו; דו"ח מרכז המחקר והמידע של הכנסת, לעיל ה"ש 15, בעמ' 19.

<sup>21</sup> דנ"פ 1062/21 **אוריך 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); בג"ץ 3809/08 **האגודה לזכויות האזרח נ' משטרת ישראל**, פס' 7 לפסק דינה של הנשיאה ביניש (נבו 28.5.2012); ראו גם את דברי השופטת דפנה ברק-ארז ברע"א 2558/16 **פלונית נ' קצין התגמולים**, בפס' 43 לפסק דינה (נבו 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".

<sup>22</sup> ראו בג"ץ 6732/20 **האגודה לזכויות האזרח נ' הכנסת**, פס' 5 לפסק דינה של השופטת ברון (נבו 1.3.2021), שם קבעה השופטת ברון כי עצם האפשרות של השימוש באיכוני השב"כ לצורך איתור חולי קורונה ואנשים באו עמם במגע יוצרת תחושת מעקב ואפקט של "משטור" ולכן השלכות על הפרט.

<sup>23</sup> דו"ח מערך הסייבר הלאומי, לעיל ה"ש 14, בעמ' 8-9; דו"ח מרכז המידע והמחקר של הכנסת, לעיל ה"ש 15, בעמ' 20-21.

המנוהלים בישראל, שהועלה על-ידי הממונה על היישומים הביומטריים במערך הסייבר הלאומי,<sup>24</sup> ועל-ידי מבקר המדינה.<sup>25</sup>

במטרה להתמודד עם חששות אלו, גובשה הצעת חוק שתהווה מסגרת משפטית עבור הפעלתן של מערכות צילום מיוחדות, וביניהן מערכת עין הנץ.<sup>26</sup> הצעה זו מנסה לתחם את השימוש במערכות צילום מיוחדות ומציעה איזון בין ההגנה על הפרטיות ובין האינטרס הציבורי במניעת עבירות וגילויין.

הצעת החוק קובעת רשימה סגורה של תכליות אשר יצדיקו הצבה של מערכת צילום מיוחדת. בין תכליות אלו ניתן למנות מטרות כמו איתור נעדר שיש חשש לשלומן או מניעה, סיכול או גילוי של עבירות פשע או עבירות שעלולות לסכן את שלומן או ביטחונן של אדם, את שלום הציבור או את ביטחון המדינה וכן גילוי מעורבים בביצוע עבירות כאמור.<sup>27</sup> עוד קובעת ההצעה כי אחת לשלוש שנים תיבחן מחדש הצבתה של כל אחת מן המערכות שהוצבו.<sup>28</sup>

הצעת החוק אף מעגנת מגבלות באשר לשימוש טכנולוגי בדיעבד של המשטרה במאגר הנתונים וביניהן הוראות אשר מגבילות את משך הזמן בו ניתן לשמור תיעוד במאגר, וכן רשימה סגורה של תכליות אשר רק לשם הגשמתן ניתן להשתמש במאגר.<sup>29</sup> ההצעה מוסיפה ומעגנת חובת דיווח, אחת לשנה, ליועצת המשפטית לממשלה אודות נתוני פעילות המערכות דוגמת מספר המערכות שהופעלו ופירוט בדבר המקרים שבהם נעשה שימוש במערכות לשם טיפול באירוע המסכן חיים או אירוע שיש בו סכנה לביטחון המדינה.<sup>30</sup>

אין ספק, הצעת חוק זו היא מהלך חשוב ומבורך, אשר מבקש לקדם שימוש סדור בטכנולוגיות צילום מיוחדות תוך איזון בין שיקולים רלוונטיים. עם זאת, דומה כי הצעת החוק אינה נותנת מענה לשני סיכונים מרכזיים בתפעול טכנולוגיה מסוג זה.

**הראשון**, נוגע לאבטחת המידע. כאמור המידע הנאסף ממערכת עין הנץ כולל תמונות ומיקום מדויק של כמעט כל עוברי דרך בישראל, ומשכך ישנה חשיבות רבה כי תהא הגנה מרבית ומיטבית על מידע רגיש שכזה. אך, כפי שנלמד מהביקורת המתמשכת על ניהול המאגרים הביומטריים באחריות מדינת ישראל, נראה כי לא ננקטו פעולות לשמירה אפקטיבית על מידע מסוג זה. למשל, בדיווחו של הממונה על היישומים הביומטריים, משנת 2022, הועלו בעיות מהותיות הנוגעות לניהול מידע ביומטרי בישראל, ובפרט ביחס לאי היערכות לפקיעת הוראות השעה שמסדירה את ניהול המאגרים הביומטריים בישראל ופגם בכיול מערכת ההשוואה הביומטרית, ובנוסף הזהיר הממונה לגבי רמת האבטחה הלקויה ביחס למאגרי מידע אישי וביומטרי בישראל.<sup>31</sup> ויובהר - אבטחת מידע בישראל היא

<sup>24</sup> דו"ח הממונה על היישומים הביומטריים – מס' 12, הממונה על היישומים הביומטריים במערך הסייבר הלאומי (18.05.22).

<sup>25</sup> מבקר המדינה, היבטים בהסדרת השימוש במאגרים ביומטריים, דוח שנתי 70 (04.05.2020).

<sup>26</sup> [הצעת חוק לתיקון פקודת המשטרה \(מס' 40\) \(מערכות צילום מיוחדות\). התשפ"ג:2023.](#)

<sup>27</sup> שם, בס' 10 י.

<sup>28</sup> שם.

<sup>29</sup> שם, בס' 10 יג.

<sup>30</sup> שם, בס' 10 כא.

<sup>31</sup> דו"ח הממונה על היישומים הביומטריים, לעיל ה"ש 24.

לא עניין תיאורטי. אתרי הממשלה, כמו גם אתרים של חברות פרטיות, נתונים בסיכון מתמיד של תקיפות סייבר וניסיונות גניבת מידע מצד שחקנים זדוניים (פליליים, וגם כאלה המגיעים ממדינות אויב ובפרט איראן).

השני, נוגע לפיקוח על השימוש במידע והעברתו לגופים ממלכתיים אחרים. אכן, קיים חשש כי המידע שנאסף ישמש למטרות זרות או יועבר לגופים אחרים ולא לצורך מימוש היעדים שלשםם נאסף. אומנם, הצעת החוק מגבילה את השימושים המותרים של מידע זה, וכן מציבה מנגנון העברת מידע. ועדיין, לדעתנו מדובר בסוגיה רגישה הדורשת רמה גבוהה יותר של פיקוח על מנת לוודא שהשימושים היחידים במידע זה תואמים את דרישות החוק, ובפרט במקרה של העברת מידע ממאגר אחד לאחר. לשם כך, ישנו צורך במנגנון פיקוח מוגבר ומקיף אשר יפקח על אופן איסוף, שמירה ומחיקה של המידע, כמו גם על השימוש במידע והעברתו.

### ג. השימוש במערכת איתור חשודים בנמל התעופה בךגוריון

כלי טכנולוגי נוסף של משטרת ישראל, אשר חשוב להביא גם אותו בחשבון, הוא מערכת מבוססת בינה מלאכותית לאיתור חשודים בנתב"ג. מערכת זו בונה פרופיל עברייני, ומנסה לאתר בין הנכנסים לישראל חשודים לעיכוב.<sup>32</sup> כאשר אדם מסומן בידי המערכת, אשר מייצרת רשימת חשודים המכונה "רשימת ההכללה", הוא יעוכב עם הגעתו לנתב"ג על-ידי שוטר, ויעבור חיפוש פיזי או באמצעות מכונת שיקוף. זאת, גם אם אין מידע מודיעיני שלפיו מדובר באדם שעבר על החוק.<sup>33</sup>

הקריטריונים אשר על פיהם פועלת המערכת אינם ידועים ואלו יכולים להיות מגוונים – למשל מקום מגורים, תחום עיסוק, או מוצא אתני. כמו כן, לא ברור מהיכן נשאב המידע האישי המנותח בידי המערכת, ובפרט האם מדובר במידע שניתנה הסכמה להעברתו, והאם הוא מועבר ממאגרים ממשלתיים בלבד או גם ממאגרים פרטיים. עוד קשה לדעת כיצד המערכת מקבלת החלטות ביחס לנתונים שבפניה, בשל תופעה המתוארת כתופעת "הקופסה השחורה" (Black-Box), ועניינה במצב בו המידע המוזן למערכת ידוע, וכך גם התוצאה אליה הגיעה המערכת, אך דרך פעולת המערכת הפנימית אינה ידועה למי שמושפע ממנה, או אף אינה ניתנת להבנה.<sup>34</sup>

השימוש במערכת מסוג זה בנתב"ג מעלה אתגרים שונים.

ראשית, קשה לקבל מצב בו אלגוריתם מקבל החלטה על בסיס נתונים שאינם ידועים, דרך הליך קבלת החלטות שאינו גלוי לציבור, ומבלי להסביר מדוע אדם – לעיתים נורמטיבי לחלוטין – צריך להיות מעוכב. לשם ההשוואה, בטיוטת החוק בנושא בינה מלאכותית המוצעת באיחוד האירופי, מוצע כי תהיה חקיקה נוקשה ביחס למערכות הפועלות על בסיס בינה מלאכותית עם סיכון גבוה, כמו המערכת

<sup>32</sup> תומר גנון "האלגוריתם שיעצור אתכם בנחיתה בנתב"ג" כלכליסט (10.11.2022).

<sup>33</sup> ראו לשם השוואה, בג"ץ 4797/07 האגודה לזכויות האזרח נ' רשות שדות התעופה (החלטה מיום 22.5.2012).

<sup>34</sup> Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J. L. & TECH. 889, 893, 901 (2018)



לאיתור חשודים של משטרת ישראל, והוגדרו חובות דוגמת פיקוח אנושי, בקרת איכות, שמירת מידע, הסברתיות, חובת דיווח ועוד.<sup>35</sup>

**שנית**, קיים חשש של הסתמכות יתר על המערכת בקבלת ההחלטות, ללא מעורבות אנושית מספקת או יכולת לקבל הסבר על אופן גיבוש המסקנות לגבי חשוד כזה או אחר.<sup>36</sup> הרי, הטיות ודעות קדומות חברתיות באות לידי ביטוי במסגרת קבלת החלטות אוטומטית או מבוססת אלגוריתם, וזאת מכיוון שהמתכנת "מוריש" תכונות לקוד שהוא כותב.<sup>37</sup> על רקע זה, מתחדד הצורך בהסברתיות ('שקיפות' אלגוריתמית), ביחס לקבלת החלטות המבוססת על בינה מלאכותית.<sup>38</sup>

**שלישית**, ולבסוף, המערכת, אף אם היא מבוססת על בינה מלאכותית לצורך ביצוע חישובים והיסקים ברמת אוטומציה גבוהה, בעצם נבנתה לקבל החלטות על בסיס אותו ההיגיון של שיטת הפרופיילינג, כאשר על בסיסו היא נוקטת מספר צעדים קדימה באמצעות יכולת גבוהה לשקלל נתונים רבים, ולהחליט מהר יותר (לעומת בן אנוש). חשוב לציין, כי גם אם יכולת ההערכה הסטטיסטית של המערכת מדויקת ויעילה יותר משל בני אנוש, עדיין לא הוכח ברמה המחקרית כי יש טעם או ערך בקבלת החלטות בצורה זו. למעשה, קבלת החלטות על בסיס פרופיילינג דווקא הוכחה כלא יעילה מבחינה מבצעית,<sup>39</sup> ונתגלה כי יש לה השפעות שליליות ארוכות טווח ברמה החברתית (תחושת ניכור, איבוד אמון במערכת אכיפת החוק, וכתוצאה מכך היעדר נכונות לשתף פעולה עם השלטונות באופן שמקשה על התמודדות יעילה עם פשיעה).<sup>40</sup>

<sup>35</sup> גל דהן "הצעת הרגולציה של האיחוד האירופי בתחום הבינה המלאכותית Artificial Intelligence Act" **מכון תכלית** (יולי, 2023), בעמ' 3-5.

<sup>36</sup> Zana Bucinca, Maja Barbara Malaya, and Krzysztof Z. Gajos, *To Trust to Think: Cognitive Forcing Functions Can Reduce Overreliance on AI in AI-assisted Decision-making*, Proceedings ACM Hum. Comput. Interact. Vol. 5, pp.188: 4-5 (2021).

<sup>37</sup> ראו למשל גדי פרל "[האלגוריתם של המשטרה בנתב"ג חייב להיות שקוף לציבור](#)" **כלכליסט** (15.12.2022). כפי שמציין פרל, "תוכנה היא יציר סובייקטיבי שמשקף את הערכים של המתכנת ואת המידע שהזינו לתוך התוכנה [...] לענייננו – תוכנה שלמדה משוטר איך לאכוף, רק תטמיע את הדפוסים של השוטר. אם הוא היה גוען, גם היא תהיה".

<sup>38</sup> Nagy Adam, Hilligoss Hannah, Achten Nele, Fjeld Jessica, Srikumar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY (2020).

<sup>39</sup> Badi Hasisi, Yoram Magalioth, and Liav Orgad, *Ethnic Profiling in Airport Screening: Lessons from Israel 1968-2010*, 14 AM. L. & ECON. REV.517 (2002); ראו גם Nicola G. Persico & Petra Todd, *Passenger Profiling, Imperfect Screening, and Airport Security* (January 12, 2005).

<sup>40</sup> ראו למשל Bernard E. Harcourt, *The Shaping of Chance: Actuarial Models and Criminal Profiling at the Turn of the Twenty-First Century*, 70 U. CHI. L. REV. 105 (2003).



### 3. דיון ומבט קדימה

השימוש בכלים טכנולוגיים מתקדמים על-ידי משטרת ישראל מייצר אתגרים ניכרים ומעלה שאלות הנוגעות לפגיעה בחירויות הפרט (דוגמת הזכות לפרטיות והזכות לחירות) ללא כל הסמכה חוקית, וכן חששות בדבר ניצול לרעה של אמצעים אלו בידי הרשויות. המצב הקיים מתאפיין בחוסר שקיפות מצד רשויות האכיפה בכל הנוגע להיקף השימוש בטכנולוגיות אלו, מהות ההכשרה של מפעילי הטכנולוגיה וכן אי-בהירות באשר למנגנוני הפיקוח על השימוש בכלים אלו. מצב זה מביא, בין היתר, לערעור אמון הציבור ברשויות האכיפה.

הטכנולוגיות שנסקרו לעיל מציגות יכולות מבצעיות מרחיקות לכת. להבדיל מחיפוש או האזנת סתר, רוגלות דוגמת פגסוס־סייפן אינן מוגבלות לאיסוף מידע חד-ממדי, וביכולתן לגשת לכלל המידע וחומר המחשב שזמינים דרך המכשיר, אף אם חומר זה הופק או נצבר לפני שנים רבות. אף מערכת איתור החשודים בנתב"ג מציגה יכולות מבצעיות מיוחדות, שכן ביכולתה לבצע עיבוד רב של נתונים בזמן קצר – כזה המקשה על פיקוח אנושי יעיל בזמן אמת. ועדיין, חרף היכולות שמציגות הטכנולוגיות שנסקרו, אשר ספק אם נעשתה בחינה מעמיקה של ההשלכות הרחבות של השימוש בהן, ישנה אי ודאות לגבי שיעורי ההצלחה של השימוש בכלים אלו.

חשוב לזכור כי צווי האזנת סתר זוכים לאישור נרחב יחסית מצד בתי המשפט. כך, בשנת 2020 מתוך 3,692 בקשות שהוגשו – רק 26 נדחו, כ-0.7% מכלל הבקשות.<sup>41</sup> מגמה זו החריפה בשנת 2021, בה אישרו בתי המשפט למשטרה 3,350 בקשות מתוך 3,359 בקשות להאזנת סתר – למעלה מ-99% מכלל הבקשות שהוגשו באותה שנה.<sup>42</sup> נתונים אלו, בהינתן כי חלק מצוים אלו אישרו שימוש ברוגלות לאיסוף מידע אישי, מעידים על פוטנציאל הפגיעה העצום בחירויות הפרט, וזאת טרם הסכנה המצויה בשימושיה ובניגוד לצו ברוגלה (כפי שנתגלה לאחרונה שאכן קרה בפועל).

נושא ההכשרה חשוב אף הוא. בעוד ברור כי עצם השימוש בטכנולוגיות מתקדמות דורש מומחיות והכשרה מיוחדת עבור המפעילים של כלים אלו, לא ידוע מהן ההכשרות המתבצעות למפעילי הטכנולוגיות, וכן מה היחס בין ההיבט הטכני של ההדרכה ובין שיקולים אתיים ומשפטיים. מעבר לכך, לא ברור אם קיימים מנגנוני פיקוח פנימיים שתפקידם לעקוב אחר השימוש בטכנולוגיות לאיסוף מידע לאחר הכנסתן לשימוש.

חרף הדיון הציבורי הגובר בנושא, חוסר השקיפות ביחס להפעלת כלים טכנולוגיים מצד משטרת ישראל עדיין מותיר אותנו בפני שאלות ללא מענה. בין אלו, ניתן לתהות מה עולה בגורל המידע האישי הנאסף, במובן של שמירה עליו והעברתו ממאגר מידע אחד לאחר, והאם נתונים אלו נשמרים כחומר מודיעיני לשימוש

<sup>41</sup> יהושע (ג'וש) בריינר "ככירים במשטרה: שופטים שמאשרים האזנה לא יודעים באיזה כלי המשטרה תשתמש" **הארץ** (19.1.2022).

<sup>42</sup> צבי זרחיה ותומר גנון "היקף השימוש ברוגלות הוסתר גם בדיווחי האזנות סתר לשנת 2021" **כלכליסט** (20.6.2022).

עתידי לצורכי חקירות אחרות (או שמא אלו נמחקים לאחר תקופה מוגדרת, כפי שדורשים מנגנוני האיזון של הזכות לפרטיות).

אין ספק, ישנה חשיבות לכלים טכנולוגיים לצורכי אכיפת החוק. ועדיין, חשוב לשמור על איזון בין כלל השיקולים הרלוונטיים. לשם כך, אנו מציעים מיסוד של שני מנגנוני פיקוח: האחד, פיקוח בשלב הייצור, השימוש או המכירה של הכלים הטכנולוגיים; השני, פיקוח מעת לעת על-ידי הכנסת.

#### א. פיקוח בשלבי הפיתוח

סעיף 36 לפרוטוקול הראשון של אמנת ג'נבה, מחייב לערוך בדיקת חוקיות לנשקים או לטכנולוגיה שיש להם יישום ביטחוני טרם השימוש או הרכישה שלהם, בין אם ממדינה ובין אם מחברה פרטית.<sup>43</sup> מקובל לומר כי הדרישה מכוח סעיף 36 חלה גם ביחס לכלי סייבר התקפיים אשר יכולים לחדור למערכות מחשב, סלולרי, מכשירי Internet of Things ועוד.<sup>44</sup>

כיום, טכנולוגיות נבחנות רק בשלב מאוחר, ובמועד זה ישנו קושי לערוך שינויים מהותיים במאפייני הטכנולוגיה, בין היתר בשל שיקולים כלכליים של פיתוח הטכנולוגיה והתועלת הכלכלית של מתן הרישיון לטכנולוגיה כמו שהיא. לעומת זאת, מיסוד מנגנון פיקוח ברוח סעיף 36 האמור תייצר תמריץ להגביר את הציות לנורמות חוקיות, ובפרט זכויות אדם, באופן שלא פוגע כלכלית בצורה אנושה במפתחים, שכן הדבר נעשה טרם שהושקעו כספים בפיתוח מתקדם.

הניסיון המתואר לעיל מלמד על החשיבות של הגברת הפיקוח על כלים טכנולוגיים לאיסוף מידע אישי, ובמיוחד כאלו אשר יש להם יישום ביטחוני. חרף העובדה כי ישראל לא קיבלה על עצמה את הפרוטוקול הראשון לאמנת ג'נבה, גם מדינות שאינן חברות בפרוטוקול, מקיימות, מתוך הכרה בחשיבות של פיקוח על נשקים וכלים טכנולוגיים המאיימים על חירויות הפרט, מנגנון בדיקה ברוח סעיף 36 (הדוגמה הרלוונטית ביותר היא ארצות הברית). כמו כן, ישנה חובה חוקית לבצע הערכה מקדימה של חוקיות של כלים טכנולוגיים גם מכוח דיני זכויות האדם הבינלאומיים, ובפרט בראי האמנה בדבר זכויות אזרחיות ומדיניות,<sup>45</sup> אליה מדינת ישראל בחרה להצטרף בשנת 1991.

משכך, אנו סבורים כי ראוי למסד מנגנון פיקוח משלים לזה הפועל במסגרת משרד הביטחון, אשר יבחן את הטכנולוגיה עוד טרם מתן רישיון שימוש, שיווק או ייצוא. מנגנון זה נדרש לשקלל מספר תחומים: כלכלה, ביטחון, אתיקה, משפט ועוד.

<sup>43</sup> § 36 Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1977), 1125 U.N.T.S. 3

<sup>44</sup> לדיון באשר להיקף תחולת הסעיף, ראו: WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED Conflict 4 (2009).

<sup>45</sup> INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (entered into force 23 March 1976).

### ב. פיקוח פרלמנטרי קבוע על הכנסה לשימוש והפעלת טכנולוגיות על ידי משטרת ישראל

אחד מן התפקידים העיקריים של הרשות המחוקקת הוא פיקוח על הרשות המבצעת והממשלה העומדת בראשה. בנסיבות שנוצרו, אשר מעידות על האתגרים הרבים הנובעים מן ההכנסה לשימוש וההפעלה של כלים טכנולוגיים על-ידי משטרת ישראל, אנו סבורים כי ראוי למסד פיקוח פרלמנטרי קבוע אשר גם ייצר אפקט מצנן על שימושיהם בסמכות שלטונית, וגם ייצר שדה לדיון ציבורי משמעותי באשר לגבולות הראויים של השימוש בכלים אלו.<sup>46</sup>

ניתן, למשל, להקים ועדת משנה, אם תחת ועדת חוקה או ועדת המדע והטכנולוגיה. לחלופין, ניתן לקיים פיקוח תחת אחת הוועדות הקבועות – כפי שעשתה לאחרונה ועדת חוקה ביחס לפרשת פגסוססיפן.

אומנם, חברי הכנסת בישראל נמצאים תחת עומס עבודה משמעותי – כאשר עליהם לחלק את זמנם בין מספר ועדות ולצד זה להשתתף בהצבעות, שאילתות והצעות לדיון מהיר, וליזום חקיקה פרטית. ועדיין, ישנה חשיבות בפיקוח בעל אופי קבוע יותר, שלא יהיה תלוי בגילוי עיתונאי כזה או אחר, ואשר יהיה פתוח ככל הניתן, בשל החשיבות של שקיפות לשם חיזוק אמון הציבור. נדרש יותר מהמצב הקיים על מנת לוודא בטווח הארוך שמירה על אינטרסים כלכליים ותדמיתיים של מדינת ישראל, וזאת לצד קידום הגנה מיטבית על חירויות הפרט.

## 4. סיכום

חשיפתו של תומר גנון, ומה שבא בעקבותיה, הם אירוע מכונן בישראל, בדומה לפרשת סנודן בארצות הברית.<sup>47</sup> זו הזדמנות לקדם הליכי פיקוח יעילים, במקביל להסדרה החוקית של הטכנולוגיות שנסקרו, יגבירו את האמון בתעשיית הסייבר בישראל ויחזקו את הכלכלה. בהתאם, אנו מציעים לבסס שני מנגנוני פיקוח משלימים לאלו הקיימים: ראשית, הקמת מנגנון פיקוח על כלי סייבר התקפיים כבר בשלב הפיתוח הטכנולוגי הראשוני. פיקוח מוקדם יאפשר לבצע שינויים בטכנולוגיה אגב פיתוחה, תוך צמצום פגיעה כלכלית בתעשיית הסייבר. שנית, מיסוד פיקוח פרלמנטרי קבוע על הכנסה לשימוש והפעלה של טכנולוגיות על-ידי משטרת ישראל.

אחרי שנים בהן מדינת ישראל התנסתה עם טכנולוגיות על חשבון חירויות הפרט, לעיתים עם בסיס חוקי רעוע, אם בכלל, הגיע הזמן להגדיר מסלול מחדש ולהבהיר: בעוד הטכנולוגיה היא מנוף אדיר עם חשיבות עצומה – חירויות הפרט חשובות לא פחות, ולכן הפעלת כוח שלטוני הולכת יד ביד עם הליכי פיקוח, ביקורת, ודיון ציבורי.

ציטוט מוצע: טל מימרן וגל דהן "דרושה בינה אנושית: מחשבות על השימוש הגובר של משטרת ישראל בטכנולוגיות לאיסוף מידע אישי" **רשות הרבים** (28.7.2023)

<sup>46</sup> בנוסף, ראוי לשקול לבסס מנגנון דיווח מקיף יותר לוועדת חוץ וביטחון על עסקאות מכירה של רוגלות. זאת, לצד התייעצות עם גורמים מייצגים דוגמת מערך הסייבר הלאומי והרשות להגנת הפרטיות, במטרה לחזק את אמון הציבור.

<sup>47</sup> מערכת וואלה "אל גור: סנודן עשה שירות חשוב לארצות הברית" וואלה (11.06.2014).