

מעקב טכנולוגי בדמוקרטיה: בין סיכול איומים לאיסוף מידע על הציבור

עמית כהן | גיליון 2195 | 3 בספטמבר 2026

בימים אלה מתרחבת בארצות הברית מחאה ציבורית נגד מצלמות Flock Safety לזיהוי לוחיות רישוי, ומחדדת את הדיון בגבולות השימוש בטכנולוגיות מעקב לצרכי ביטחון לאומי. מאמר זה משווה בין המערכת האמריקאית ל"עין הנץ" בישראל, ובוחן כיצד איסוף נתוני תנועה ויכולות הצלבה תורמים לסיכול איומים ולאכיפת חוק, אך גם מעוררים סיכונים לפרטיות, לאמון הציבור ולביטחון המידע. לבסוף מוצעים עקרונות למדיניות מאוזנת, המשלבת יעילות מבצעית, פיקוח, צמצום מידע והגנת סייבר, תוך שמירה על הלגיטימציה הדמוקרטית לאורך זמן.

גל ההתנגדות הציבורי למצלמות האוטומטיות לזיהוי לוחיות רישוי של חברת Flock Safety בארצות הברית חרג לאחרונה מביקורת של ארגוני זכויות אזרח ומהליכים במועצות מקומיות. לצד דרישות לביטול חוזים ולהגבלת הגישה למידע, מופצים ברשתות החברתיות סרטונים הקוראים לזהות את המצלמות ולהסירן, ובמספר מוקדים תועדה גם פגיעה פיזית בתשתית. התפתחות זו משקפת משבר אמון עמוק ביחס להתרחבותן של טכנולוגיות מעקב ממשלתיות ומסחריות במדינות דמוקרטיות.

בישראל התנהל דיון דומה סביב מערכת "עין הנץ" של משטרת ישראל, אם כי הוא היה מוגבל בעיקר לזירה [המשפטית](#) [המוסדית](#). שתי המערכות, האמריקאית והישראלית, נועדו לתמוך באיתור חשודים, בסיכול איומים ובחקירת פשיעה, אך הן גם אוספות ושומרות מידע על תנועת כלי רכב רבים שאינם קשורים לחשד מוקדם. השאלה המרכזית אינה אפוא האם טכנולוגיות מעקב נחוצות להתמודדות עם איומים, אלא כיצד ניתן לשמר את ערכן המבצעי מבלי להפוך אותן לתשתיות לאיסוף שיטתי של מידע על הציבור באופן שפוגע בפרטיות.

לגיטימציה של מערכות מעקב טכנולוגיות אינה נשענת רק על יעילותן המבצעית, אלא גם על יכולתה של המדינה להציב גבולות ברורים להפעלתן. ההשוואה בין המקרה האמריקאי למקרה הישראלי ממחישה כי כאשר גבולות אלה אינם ברורים לציבור, כלי שנועד להגן עליו עלול להיתפס כאמצעי המופעל נגדו. **המקרה הישראלי מחדד עוד כי עצם קיומה של מסגרת חוקית אינו מסיים את הדיון: יש לבחון אם ההסדרה מציבה בפועל מגבלות אפקטיביות על היקף האיסוף, השימוש במידע והרחבת המערכת לתכליות חדשות הפוגעות בפרטיות.**

ממצלמה נקודתית למאגר מידע מצטבר

מערכות אוטומטיות לזיהוי לוחיות רישוי (Automated License Plate Readers – ALPR) מתעדות את מספר הרישוי של הרכב, את מיקומו ואת מועד מעברו. מערכות מתקדמות מאפשרות לזהות גם את סוג הרכב, צבעו ומאפיינים חיצוניים נוספים. הנתונים מוזנים למאגר שבו ניתן לבצע חיפוש בזמן אמת או בדיעבד.

מבחינה ביטחונית ואכיפתית, מדובר ביכולת בעלת ערך רב. המערכת יכולה לספק התרעה כאשר רכב הקשור לעבירת תנועה, לפיגוע, לחטיפה, לגניבה או לפשיעה חמורה עובר בנקודה מסוימת, לקצר את משך האיתור ולסייע בחיבור בין זירות ובזיהוי קשרים בין חשודים. ואולם, ככל שמספר המצלמות גדל והמידע נשמר לאורך זמן, משתנה מהות המערכת: היא אינה משמשת עוד רק לזיהוי רכב מבוקש, אלא מאפשרת לשחזר מסלולים, לאתר מקומות שהייה ולזהות דפוסים חוזרים. לוחית הרישוי אמנם מתייחסת לכאורה לרכב ולא לאדם, אך ניתן להצליב אותה בקלות עם מאגרי בעלות ומידע משטרתי.

מכאן, שנתוני תנועה עשויים לא רק לשמש לחקירת פשעים אלא גם [לחשוף](#) מידע על מקום העבודה, קשרים אישיים, ביקורים במוסדות רפואיים, השתתפות בפעילות פוליטית או דתית והרגלים יומיומיים.

השינוי המרכזי הוא אפוא המעבר ממעקב המבוסס על חשד קונקרטי לאיסוף מידע מקדים על אוכלוסייה רחבה. במקום שחשד קונקרטי יוביל לאיסוף מידע, המידע נאסף ונשמר מראש כדי שניתן יהיה להשתמש בו אם יתעורר בעתיד חשד. ההבדל אינו טכנולוגי בלבד; הוא משנה את יחסי הכוח בין המדינה לבין האזרח. המשמעות המוסדית של שינוי זה היא שרוב המידע במערכת אינו בהכרח מידע על חשודים, אלא מידע על אזרחים שלא קיים לגביהם חשד. לכן השאלה אינה רק מי רשאי לעיין במאגר, אלא האם עצם ריכוזו של מידע כזה בידי גוף אכיפה יוצר יכולת מעקב רחבה מן הנדרש לצורך המבצע. החשש משימוש חורג אינו תיאורטי: בארצות הברית תועדו מאות חיפושים ברשת Flock הקשורים להפגנות ולארגונים אקטיביסטיים, וכן שימוש במערכת במסגרת [חקירה](#) הנוגעת להפלה עצמית. מאגר כזה הוא גם יעד בעל ערך למתקפות סייבר; [בעבר](#) נחשפו נתוני לוחיות רישוי במתקפה על קבלן של רשות פדרלית, ובמוצרי Flock עצמם התגלו חולשות אבטחה.

מחאה נגד Flock Safety בארצות הברית

חברת Flock Safety מפעילה רשת רחבה של מצלמות לזיהוי לוחיות רישוי עבור משטרות, רשויות מקומיות, שכונות וגופים פרטיים בארצות הברית. המודל האמריקאי מבוסס: כל רשות מחליטה באופן עצמאי אם להתקשר עם החברה ואם לאפשר לרשויות אחרות גישה לנתונים שאספה. כאשר השיתוף מופעל, חוקרים מרשות אחת יכולים לבצע חיפוש גם במידע שנאסף באמצעות מצלמות של רשויות אחרות, ולעיתים במספר רב של מדינות, באמצעות אותה תשתית טכנולוגית. לפי Flock, השיתוף אינו אוטומטי, וכל רשות קובעת את הרשאות הגישה שלה; עם זאת, ניתוחים של Electronic Frontier Foundation מצביעים על [היקף רחב של שימוש ברשת Flock](#) ועל האפשרות לבצע חיפושים במידע הנאסף באמצעות מספר רב של גופי אכיפה ברחבי ארצות הברית.

מבנה זה מאפשר פריסה מהירה, אך גם יוצר רשת מעקב רחבה ללא החלטה פדרלית מפורשת להקימה. ניתוח שערך Electronic Frontier Foundation ליותר מ-12 מיליון חיפושים שביצעו כ-3,900 גופי אכיפה ברשת Flock מצא כי למעלה מחמישים גופי משטרה, משרדי שריף, גופי אכיפה מדינתיים ורשויות פדרליות ביצעו במהלך 2025 מאות חיפושים שנקשרו [להפגנות ולפעילות אקטיביסטית](#). בחלק מהמקרים נועדו החיפושים לאתר כלי רכב שנחשדו באיום, בתקיפה או בפגיעה במשתתפים; אולם במקרים רבים הוזנו כסיבת החיפוש רק המילה "מחאה" או שמה של ההפגנה, ללא ציון עבירה קונקרטית. ממצאים אלה ממחישים כיצד תשתית שנועדה לחקירת עבירות יכולה לשמש גם למיפוי כלי רכב ואנשים הנמצאים בסביבת פעילות פוליטית. מקרים אלה ממחישים כי הסיכון אינו מוגבל לפגיעה בפרטיות במובנה הצר. היכולת למפות ולשחזר בדיעבד נוכחות של כלי רכב בסביבת מחאות ופעילות פוליטית עשויה להשפיע גם על חופש הביטוי וההפגנה, ובפרט על נכונותם של אזרחים להשתתף בפעילות פוליטית חוקית.

על רקע זה התרחבה ההתנגדות למערכת. האיגוד האמריקאי לחירויות (Union ACLU – American Civil Liberties) השיק את קמפיין "Get the Flock Out", הקורא להגביל את פריסת המצלמות ואת השימוש במידע הנאסף באמצעותן. לצד פעילות ממוסדת זו, המחאה קיבלה ביטוי גם ברשתות החברתיות וברחוב (כפי שניתן לראות בתמונות להלן): מופצים סרטונים המסבירים כיצד לזהות את המצלמות וקוראים להסרתן, ובחלק מהמקרים תועדה גם פגיעה ישירה בצידוד. ביולי 2026, למשל, ניזוקו מצלמות בניו יורק ובקונטיקט, ואילו במקומות אחרים כוסו מצלמות לאחר שהרשויות החליטו להפסיק את השימוש בהן.



פוסטים ברשת אינם יכולים לבדם להעיד על היקף ההתנגדות בציבור האמריקאי. עם זאת, הצטברות האירועים מצביעה על שינוי באופי הוויכוח: ההתנגדות אינה מכוונת עוד רק לתנאי השימוש במערכת, אלא לעצם קיומה של תשתית המאפשרת לאסוף ולחבר מידע על תנועת הציבור. המצלמה הופכת, מבחינת המתנגדים, לסמל מוחשי של מעקב ממשלתי ותאגיד.

למחאה ולביקורת הציבורית הייתה גם השפעה מוסדית. רשויות אחדות [ביטלו](#) או לא חידשו את התקשרותן עם Flock, Safety ואחרות השעו את פעילות המצלמות או עצרו את הרחבת השימוש בהן לצורך בחינה מחודשת של סוגיות הנוגעות לפרטיות, לשיתוף מידע ולפיקוח. מנגד, [החברה](#) ורשויות אכיפה התומכות במערכת ממשיכות להדגיש את תרומתה לחקירת עבירות ולביטחון הציבור, וטוענות כי הגישה למידע מוגבלת, החיפוש מתועדים והשיתוף נתון להחלטת הרשויות המקומיות. הביקורת לא הביאה אפוא לנסיגה כוללת מן הטכנולוגיה, אלא למעבר מאימוץ מהיר לדרישה גוברת לשקיפות, לפיקוח ולהגבלת השימוש במידע.

“עין הנץ”: הדגם הישראלי

מערכת “עין הנץ”, הנמצאת בשימוש משטרת ישראל מאז 2015, נועדה לזהות אוטומטי לוחיות רישוי בכבישי הארץ. בדומה ל-Flock, היא מאפשרת לאתר כלי רכב ולבצע חיפוש במידע שנאסף. היא מסייעת, לטענת המשטרה, בפענוח פשעים, באיתור עבריינים ובהצלת חיים.

המערכת הופעלה במשך שנים בטרם הוסדרה בחקיקה ייעודית ובטרם התקיים דיון ציבורי מלא על היקף השימוש בה. הביקורת התמקדה בכך שהיא יוצרת מאגר נרחב המתעד את תנועתם של נהגים, לרבות מי שאינם חשודים בעבירה, וכן באפשרות לבצע חיפוש בדעבד במידע שנאסף.

בעקבות עתירות וביקורת ציבורית, בינואר 2024 הוסדר השימוש במערכת בחקיקה ייעודית, ובספטמבר אותה שנה אושרו תקנות מפורטות שנועדו לקבוע את התנאים להפעלתה, את אופן השימוש במידע ואת מנגנוני הפיקוח על המערכת. בכך, שונה המקרה הישראלי מן המודל האמריקאי המבוסס: בישראל נעשה ניסיון להסדיר ברמה הלאומית את השימוש בתשתית המעקב ולהציב לה מסגרת משפטית מוסדרת. ואולם, עצם קיומה של הסדרה אינו מסיים את הדיון. השאלה המרכזית היא האם המגבלות שנקבעו מצמצמות בפועל את היקף האיסוף והשימוש במידע, ובייחוד את האפשרות לעשות שימוש במידע שנאסף על אזרחים שלא קיים לגביהם חשד מוקדם.

המחלוקת סביב “עין הנץ” נמשכה גם לאחר השלמת ההסדרה. הביקורת המשפטית התמקדה, בין היתר, בהיקף המידע שנשמר, באפשרויות החיפוש והניתוח בדעבד ובמידת הפיקוח על השימוש [במערכת](#). בכך, הופכת “עין הנץ” למקרה מבחן

חשוב למדיניות ציבורית: לא רק כיצד להסדיר טכנולוגיית מעקב לאחר שכבר הוטמעה, אלא כיצד לוודא שהמסגרת המשפטית מציבה גבולות מהותיים ליכולות שהטכנולוגיה מאפשרת.

מעבר לפגיעה בפרטיות, יכולת מעקב מצטברת עשויה להשפיע גם על חופש הפעולה במרחב הדמוקרטי. חשש זה הועלה גם במסגרת הביקורת המשפטית על "עין הנץ", שבה נטען כי האפשרות לתעד ולשחזר תנועת אזרחים עלולה ליצור אפקט מצנן על חופש הביטוי, ההפגנה [וההתארגנות](#). הניסיון האמריקאי, שבו תועדו שימושים ב-Flock בהקשר של הפגנות ופעילות אקטיביסטית, ממחיש כי הסיכון להרחבת השימוש למרחבים של פעילות פוליטית אינו תיאורטי בלבד.

ההבדל המרכזי בין המקרים הוא במבנה השליטה במערכת. בישראל מדובר במערכת ארצית וריכוזית המופעלת בידי משטרת ישראל, ולכן האחריות להפעלה, לאבטחת המידע ולפיקוח מרוכזת בעיקר בידי גוף מדינתי אחד. מבנה זה מאפשר חיבור מהיר בין זירות ותגובה אפקטיבית לאיומים החוצים גבולות מקומיים, אך גם מרכז בידי המשטרה יכולת רחבה לשחזר את תנועותיהם של אזרחים.

בארצות הברית, לעומת זאת, המערכת מבוססת על התקשרויות נפרדות של רשויות מקומיות וגופים פרטיים עם ספק טכנולוגי מסחרי. המידע נאסף באופן מבוזר, אך ניתן לשיתוף ולחיפוש באמצעות תשתית משותפת. דגם זה מצמצם את קיומו של מרכז מדינתי אחד, ויוצר פערי מדיניות בין רשויות, תלות בחברה פרטית וקושי לפקח באופן אחיד על הגישה למידע ועל השימוש בו. מבחינה ביטחונית, ההבדל הוא אפוא בין ריכוז כוח ומידע בידי המדינה לבין פיזור האחריות לצד חיבור טכנולוגי רחב בין גופים רבים. למרות ההבדלים, שני הדגמים מאפשרים איסוף מצטבר של מידע גם על מי שלא התעורר לגביהם חשד מוקדם; השוני הוא בזהות הגורם המרכז את הכוח ובאופן שבו האחריות, הפיקוח והסיכון מפוזרים בין המדינה, הרשויות המקומיות והספק הפרטי.

הניסיון האמריקאי ממחיש מדוע סוגיה זו חשובה גם בישראל. כאשר ניתן לזהות בדיעבד כלי רכב שנכחו באזור הפגנה או פעילות פוליטית, עצם קיומה של היכולת עשוי ליצור אפקט מצנן גם אם רוב השימושים במערכת חוקיים ומוצדקים. בחברה המאופיינת בקיטוב פוליטי, לפיכך, ההגנה על נתוני תנועה נוגעת לא רק לפרטיות אלא גם לתנאים המאפשרים השתתפות פוליטית חופשית.

איום, תמיכה ציבורית ולגיטימציה

הדיון במדיניות מעקב אינו מתקיים בחלל ריק. נכונות הציבור לתמוך באמצעי מעקב מושפעת מתפיסת האיום ומההקשר הביטחוני שבו הם מוצגים. [מחקר](#) שנערך ב-2021 במעבדה לפסיכולוגיה פוליטית באוניברסיטת חיפה באמצעות מציאות מדומה בחן כיצד חשיפה לטרור קונבנציונלי ולטרור סייבר משפיעה על התמיכה במדיניות מעקב. הממצאים הצביעו על תפיסת האיום הלאומי כמנגנון מרכזי: ככל שהאיום נתפס כחמור יותר, כך גברה התמיכה באמצעי מעקב נרחבים, וההבדלים בין סוגי הטרור הצטמצמו.

ממצאים אלה מסייעים להסביר מדוע הרחבת סמכויות מעקב עשויה לזכות בלגיטימציה ציבורית בתקופות של איום. כאשר הציבור תופס סכנה ביטחונית כמיידיה וחמורה, הוא עשוי לתת משקל רב יותר ליעילות המבצעית ולהיות נכון לקבל פגיעה רחבה יותר בפרטיות. ואולם, התמיכה הניתנת בתנאים של איום אינה בהכרח הסכמה יציבה ובלתי מוגבלת להפעלת המערכת לאורך זמן.

הקושי נובע מכך שבעוד שתפיסת האיום עשויה להשתנות, תשתיות המעקב שהוקמו על רקעה נוטות להישאר. המצלמות, המאגרים, מנגנוני השיתוף והיכולות הטכנולוגיות אינם מצטמצמים בהכרח עם דעיכת האיום, ולעיתים אף מורחבים לתכליות נוספות. כך עלול להיווצר פער בין התנאים שבהם הציבור תמך בהקמת המערכת לבין השימוש השגרתי שנעשה בה בהמשך.

הסיכון בהרחבת תכליות אמצעי הפיקוח אינו נוגע רק להוספת שימושים חדשים למערכת הקיימת, אלא גם להתפתחות הדרגתית של יכולות המעקב עצמן. תשתית שנועדה בתחילה לזיהוי ולאיתור כלי רכב עשויה, עם התפתחות יכולות ההצלבה והניתוח האוטומטי, לשמש גם לזיהוי דפוסי תנועה, ליצירת פרופילים ואף לאכיפה ממוכנת. משום כך, בחינת המידתיות של מערכת המעקב אינה יכולה להתבסס רק על השימושים המותרים בה כיום, אלא צריכה להביא בחשבון גם שימושים עתידיים שהארכיטקטורה הטכנולוגית מאפשרת.

לפיקר, תמיכה ציבורית בפיקוח אינה יכולה לשמש הצדקה להפעלה עתידית בלתי מוגבלת של מערכות מעקב. דווקא משום שתפיסת האיום משפיעה על נכונות הציבור לקבל אמצעים חודרניים, נדרשים גבולות מוסדיים ברורים שאינם תלויים רק בעמדות הציבור ברגע נתון.

משמעויות והמלצות לישראל

ההגנה על הפרטיות אינה מגבלה חיצונית על מדיניות הביטחון, אלא רכיב בה: היא מצמצמת את הנזק האפשרי מדליפת מידע, מחזקת את אמון הציבור ומסייעת לשמר לאורך זמן את הלגיטימציה של כלים מבצעיים חיוניים. מן ההשוואה בין המקרה האמריקאי לישראלי עולים מספר עקרונות לגיבוש מדיניות מעקב טכנולוגית המאזנת בין צרכי הביטחון הלאומי לבין הגנת הפרטיות והאמון הציבורי.

ראשית, יש להתאים את היקף איסוף המידע לצורך המבצעי. זיהוי בזמן אמת של רכב הקשור לפיגוע, לחטיפה או לפשיעה חמורה עשוי להיות חיוני לסיכול איום, אך אינו מחייב בהכרח שמירה ממושכת של נתוני כלל הנהגים שעברו במקום.

שנית, יש לקבוע מדרג שימושים בהתאם לחומרת האיום ולתכלית הביטחונית. מניעת פיגוע, איתור אדם בסכנת חיים או חקירת פשיעה חמורה עשויים להצדיק שימוש רחב יותר במידע מאשר טיפול בעבירות שגרתיות. הבחנה זו נועדה לשמר את יכולתה המבצעית של המערכת, תוך מניעת הרחבה שגרתית של השימוש בה מעבר לתכליות שלשמן הוקמה.

שלישית, יש להבטיח תיעוד, פיקוח ושקיפות שאינם פוגעים בביטחון המבצעי. כל חיפוש במאגר צריך להיות מתועד ולכלול את זהות המשתמש, מטרת החיפוש והחקירה הרלוונטית. במקביל, ניתן לפרסם נתונים מצרפיים על היקף השימוש, השיתוף ואירועי החריגה, בלי לחשוף מיקומי מצלמות, שיטות חקירה או יכולות רגישות. פיקוח כזה עשוי לחזק את אמון הציבור ואת הלגיטימציה להמשך הפעלת המערכת.

רביעית, יש להתייחס למאגר עצמו כנכס מודיעיני רגיש וכיעד אפשרי למתקפות סייבר. צמצום משך שמירתו של מידע שאינו קשור לאיום או לחקירה חשוב לא רק להגנת הפרטיות, אלא גם לצמצום משטח התקיפה. מאגר הכולל היסטוריית תנועה של אוכלוסיות רחבות עשוי להיות בעל ערך לגורמי פשיעה, לארגוני טרור ולשירותי מודיעין זרים, בפרט כאשר הוא מאפשר לזהות דפוסי תנועה של אנשי מערכת הביטחון, בעלי תפקידים רגישים ותשתיות חיוניות.

חמישית, יש לקבוע שימושים אסורים ולא רק שימושים מפקחים. במדיניות טכנולוגית אי אפשר להניח שכל שימוש חדש ייבחן רק כשהטכנולוגיה כבר מאפשרת אותו. יש שימושים שהמחוקק צריך להחליט מראש שאינם לגיטימיים, או שהם מחייבים חקיקה חדשה ומפורשת.

סיכום

המחאה נגד Flock בארצות הברית והביקורת על "עין הנץ" בישראל משקפות מתח יסודי במדיניות הביטחון הלאומי של מדינות דמוקרטיות. מערכות לזיהוי לוחיות רישוי עשויות לסייע בסיכול טרור, בחקירת פשיעה ובהצלת חיים. ואולם, כאשר הן מחוברות למאגרים רחבים וליכולות הצלבה ושיתוף, הן יוצרות גם תשתית מידע רגישה, שהפעלתה הבלתי מבוקרת עלולה לפגוע בפרטיות, באמון הציבור ואף בביטחון המידע.

האתגר אינו לצמצם את יכולתה של המדינה להתמודד עם איומים, אלא להבטיח שהשימוש בטכנולוגיה יישאר מותאם לתכלית הביטחונית שלשמה הוקמה. מדיניות ברורה ביחס לאיסוף, לשמירה, לשיתוף ולפיקוח אינה רק דרישה להגנת זכויות; היא תנאי לשימור הלגיטימציה הציבורית, לצמצום סיכוני סייבר ולהמשך הפעלה אפקטיבית של המערכת.

המבחן של מדינה דמוקרטית אינו רק יכולתה לפתח ולהפעיל טכנולוגיות מעקב מתקדמות, אלא גם יכולתה לשלב בין צרכי הביטחון הלאומי, הגנת הפרטיות ושמירת אמון הציבור.

עורכי הסדרה: ענת קורץ, רינת חרש ואלדד שביט.