הנחית רשם מאגרי מידע מס'

שימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהן

1. מטרה

1.1. לאחרונה הולך וגובר השימוש באמצעים טכנולוגיים לפיקוח ולמעקב חזותי או קולי מרחוק על שטחים ציבוריים ועל מתחמים פרטיים (להלן - **מצלמות מעקב**)[1].

1.2. מטרת הנחיה זו היא להבהיר את עמדת רשם מאגרי מידע (להלן - **הרשם**) ביחס לתחולת הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן - **החוק**) על שימוש במצלמות מעקב במרחב הציבורי, בפרט במקרים בהם הצילומים הנקלטים בהן נאגרים במאגרי מידע ממוחשבים.

2. רקע

2.1. מצלמות מעקב משמשות למגוון רחב של מטרות כגון הגנה על רכוש, מניעת עבירות וגילוין, הכוונת תנועה, שמירה על סדר ציבורי ואף פיקוח על עובדים.

2.2. למבט העוקב אחרי בני אדם יש כוח ממשמע וממשטר המשפיע על אופן התנהגותם. השפעה זו עשויה להיות חיובית, כאשר היא מצמצמת התנהגות עבריינית ומזיקה לזולת ולחברה כולה. אולם למעקב המתמיד יש גם השלכה שלילית: לשם המימוש העצמי וההתפתחות האישית זקוק כל אדם למרחב פרטי, בו יוכל להיות הוא עצמו ולהתנסות בחוויות ובהתנהגויות שאינן בהכרח מקובלות על החברה הסובבת אותו - בלא צורך לדווח לאחרים, להסביר ולהצטדק[2].

2.3. במערכות צילום והקלטה דיגיטליות המופעלות כיום קיימות תכונות בסיסיות המאפשרות מפתוח אוטומטי ואפשרויות שליפת מידע לפי פרמטרים כגון חתכי זמן הצילום ומיקומו. במקרים מסוימים אף קיימות יכולות זיהוי אוטומטיות, או אוטומטיות למחצה של אובייקטים שונים בתמונה, כגון פענוח מספר לוחיות זיהוי של כלי רכב או הפרדה של הפריטים המופיעים בתמונה (אנשים, כלי רכב, בעלי חיים וכדי).

---

[1] בעולם קיימים המונחים Closed Circuit Television (CCTV) ו-Video Surveillance.

[2] להרחבה על ההיבט הפסיכולוגי ועל הצדקות נוספות לזכות לפרטיות ראה מ. בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות", **משפט וממשל** יא תשס"ח 9, 57.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.4. בנוסף, גם תוכנות לזיהוי פנים אוטומטי הקיימות זה מכבר בשוק, עשויות לספק למערכות הצילום דיוק בזיהוי פנים ברמה הולכת ומשתפרת.

2.5. במסגרת הוראות פרק ב' לחוק חלות על בעל מאגר מידע, מנהלו והמחזיק בו מספר חובות מהותיות הקשורות באיסוף המידע, והן: חובת מתן הודעה למי שהמידע אודותיו (להלן - **נושא המידע**), האיסור על שימוש במידע למטרה שונה מזו לגביה ניתנה הסכמה, החובה לתת לנושא המידע זכות עיון במידע ותיקונו, חובת הסודיות ואבטחת המידע. על בעל מאגר המידע מוטלת גם חובת רישום מאגר המידע.

2.6. לפי הגדרות מידע ומאגר מידע בסעיף 7 לחוק, התחולה של פרק ב' בחוק היא על שמירת נתונים על אודות אדם, כאשר המידע אודותיו מזוהה או ניתן לזיהוי. לנוכח מאפייניהן המפורטים לעיל, חלק ניכר מן ההקלטות ממצלמות המעקב יכנסו לגדר "מאגר מידע" המתייחס למידע מזוהה, או ניתן לזיהוי, אודות אדם, כמשמעותו בסעיף 7 לחוק. בין אלה כלולות:

2.6.1. מערכות צילום המפעילות טכנולוגיות כגון זיהוי רכב לפי לוחית רישוי (LPR), אשר כבר כיום מספקות זיהוי אוטומטי ברמת דיוק גבוהה;

2.6.2. מערכות אשר לצד הקלט ממצלמות המעקב ניזונות גם ממידע ממאגרים נוספים, באופן בו הצלבת המידע משני המקורות ועיבודו מאפשרים רמה גבוהה של זיהוי האובייקטים המצולמים, למשל צילומים במקום עבודה המוצלבים עם מאגר התמונות המזוהות של העובדים;

2.6.3. מערכת מצלמות המפעילה זיהוי פנים אוטומטי ברמת דיוק ממוצעת מינימאלית; ככלל אצבע גרידא, צילומים ממערכת המספקת זיהוי ברמת דיוק ממוצעת של 20% לפחות – ודאי יחשבו ככוללים מידע (הניתן לזיהוי) אודות אדם, הנכנס לגדר "מאגר מידע" לצורך סעיף 7 לחוק;

2.6.4. מערכות המכילות יכולות ניתוח ושליפת מידע ויזואלי ברמה גבוהה, כגון האפשרות לזהות אובייקטים בתמונה ושליפת אובייקט זהה בתמונות נוספות וכד' המקלות מאוד על תהליך זיהוי אנשים.

2.7. זאת ועוד, עצם הידיעה על הימצאותו של אדם במקום נתון ובזמן נתון או עצם חזותו עשויות לכלול נתונים על צנעת אישותו (כגון עם מי הוא נמצא ובאילו נסיבות), על מצב בריאותו (כגון הימצאות במרפאה), על אמונתו הדתית (הימצאות בבית תפילה של עדה מסוימת או לבוש מסוים של המצולם) וכיו"ב. כל אלה הם נתונים העשויים ללמד את אחד מרכיבי הגדרת המונח "מידע" בסעיף 7 לחוק. קל וחומר שהנתונים הנאגרים בהקלטות מצלמות המעקב נכנסים לגדר "מידע" ואף "מידע רגיש" במערכות בעלות יכולת

טכנולוגית לעקוב אחרי אדם נתון לאורך מסלול תנועתו[3], או להסיק מידע רפואי מניתוח תמונתו החזותית או מצילום טרמי שלו.

2.8. בצילום באמצעות מצלמות מעקב גלומה גם פגיעה בזכות לפרטיות עצמה, המעוגנת בפרק א' לחוק[4] ובסעיף 7(א) לחוק יסוד: כבוד האדם וחירותו[5]. לפיכך, כוחם של העקרונות המפורטים בהנחיה זו, שאינם שאובים אך ורק מפרק ב' לחוק הגנת הפרטיות, יפה גם למצלמות שאינן "מאגר מידע" לפי סעיף 7 לחוק.

2.9. עקרון בסיסי בחוק הגנת הפרטיות הוא שאין פוגעים בפרטיות של אדם ללא הסכמתו (סעיף 1 לחוק). לגבי רשויות המדינה כבר קבע בית המשפט[6] כי "פגיעה בזכות לפרטיות, כמו פגיעה בזכויות האחרות הקבועות בחוק-יסוד: כבוד האדם וחירותו, מותרת רק "בחוק ההולם את ערכיה של מדינת-ישראל, שנועד לתכלית ראויה ובמידה שאינה עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו". לטעמנו גם הצבת מצלמות במרחב הציבורי בידי גורם פרטי, ראוי לבחון באספקלריא החוקתית, שכן בשל טיבה ותחום השפעתה, ברוב המקרים כלל לא ניתן לקבל הסכמה מכל מי שפרטיותו תיפגע בשל המצלמה בוודאי שלא הסכמה מפורשת (לכל היותר אפשר יהיה לייחס להם הסכמה מכללא לפגיעה בפרטיותם)[7].

2.10. בשל האיסור בסעיף 1 לחוק לפגוע בפרטיותו של אדם ללא הסכמתו, כאשר מוצבת מצלמת מעקב יש ליידע את הציבור על כך באופן ברור, על מנת לאפשר למעוניין בכך להימנע מהצילום, ובמקביל לייחס לאנשים המצולמים הסכמה מכללא לאיסוף המידע על אודותם ולשימוש בו. הדרישות באשר למקום פרסום ההודעה לציבור, תוכנה של ההודעה ואופן הפרסום נגזרים מהגדרת המונח "הסכמה" בסעיף 3 לחוק הקובע שההסכמה תהיה מודעת.

---

[3] לעניין זה ראו הגדרת "מידע בעל רגישות מיוחדת", בהצעת חוק לתיקון הגנת הפרטיות (סמכויות אכיפה) (תיקון מס' 12), התשע"ב-2011, הצעות חוק 16.11.2011;

[4] צילום אדם במצלמה ברשות הרבים, עשוי להגיע כדי "בילוש או התחקות...העלולים להטרידו..." לפי סעיף 2(1) לחוק, והוא לכל הפחות יוצר סיכון לפגיעה בפרטיות שעניינה "פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול ..להשפילו" לפי סעיף 2(4), שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה לפי סעיף 2(9), ובנסיבות מסוימות אף כדי פרסומו של עניין הנוגע לצנעת חייו שהאישיים של אדם או למצבו הבריאותי לפי סעיף 2(11) לחוק. תחום הכיסוי של מצלמה המוצבת ברשות הרבים, עלול להיכנס לגדר "צילום אדם כשהוא ברשות היחיד" לפי סעיף 2(3) לחוק.

[5] "כל אדם זכאי לפרטיות ולצנעת חייו".

[6] בג"צ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים**, פ"ד נח(4) 842.

[7] בדומה לכך, המבחנים החוקתיים לפגיעה בזכות לפרטיות הוחלו גם בנסיבות בהן הפוגע בפרטיות הוא גורם פרטי שאיננו כפוף ישירות לחוק היסוד, אולם קיימים פערי כוחות בינו לבין נושא המידע - המעיבים על יכולתו של האחרון לתת הסכמה מדעת, חופשית ומרצון לפגיעה בפרטיותו. כך למשל ביחסי עובד מעביד, ראו דב"ע 97 /70-4 **אוניברסיטת תל אביב – ההסתדרות הכללית החדשה**, פד"ע ל' 385, 411. ראו גם ע"ע (ארצי) 90/08 **איסקוב נ' מדינת ישראל - הממונה על חוק עבודת נשים**, (פורסם בנבו, 8.2.2011).

3. הנחיה

3.1. לאור האמור לעיל, עמדת רשם מאגרי מידע לעניין השימוש הראוי במצלמות מעקב בהתאם להוראות חוק הגנת הפרטיות הינה כדלקמן:

3.1.1. <u>קבלת ההחלטה על הצבת מצלמות מעקב</u>

3.1.1.1. שימוש במצלמות מעקב במרחב הציבורי, במיוחד בידי רשויות ציבוריות, חייב לעמוד בתנאי פסקת ההגבלה החוקתית[8]. לשם ביסוס התכלית הראויה והמידתיות, **יש לקבל את ההחלטה על השימוש במצלמת מעקב באופן מושכל ומודע, לאחר בחינת הצרכים והחלופות לשימוש במצלמה**;

3.1.1.2. בטרם קבלת ההחלטה על עצם השימוש במצלמה יש לערוך **תסקיר של השלכות השימוש במצלמה על זכויות הציבור[9], ובמיוחד על הזכות לפרטיות[10]**; ככל שתחום הכיסוי רחב יותר, והיקף האנשים המושפעים צפוי להיות גדול יותר – כך צריכה להיות הבדיקה המכינה עמוקה ומקיפה יותר. במסגרת הבדיקה יש להתייחס לנושאים הבאים:

3.1.1.2.1. **התכלית אותה מבקשים להשיג באמצעות מצלמות המעקב**. מטרת הצבת המצלמות חייבת להיות מוגדרת באופן חד, ספציפי ומפורש – ולאחר שנקבעה המטרה אין להשתמש בצילומים למטרות זרות. במסגרת הגדרת המטרה כאמור, יש לבחון האם יש בסיס עובדתי לקיומה של בעיה שפתרונה מצריך הצבת מצלמות מעקב. בהקשר זה, **על תכלית הפגיעה בזכות "ראויה"**. בטרם תחליט על התקנת המצלמה, על הרשות השלטונית לבחון אם התכלית המיועדת להתקנת המצלמה מצויה בכלל בתחום סמכותה. רק אם התשובה לכך היא חיובית, תוכל הרשות להמשיך הלאה לבחינת השיקולים המפורטים בהמשך הנחיה זו להלן;

3.1.1.2.2. **מידתיות השימוש במצלמות מעקב לשם השגת המטרה הרצויה**, בשים לב לשלושת מבחני המשנה שהוכרו בפסיקה כקונקרטיזציה של עקרון המידתיות:

3.1.1.2.2.1. האם מצלמות המעקב הן בכלל האמצעי המתאים והיעיל להשגת המטרה הרצויה;

3.1.1.2.2.2. האם ניתן להשיג את המטרה הרצויה באמצעי שהוא פחות פוגעני בפרטיות;

---

[8] הסמכה מפורשת בחוק, תכלית ראויה ועמידה במבחן המידתיות.

[9] הצבת מצלמת מעקב בשטח ציבורי עלולה להשפיע גם על אינטרסים אחרים של ציבור המשתמשים בו, בנוסף על הזכות לפרטיות: כך לדוגמא, מצלמה המופעלת לפי תזוזה עלולה למנוע משומרי שבת לעבור בתחום הכיסוי שלה.

[10] תהליך זה נקרא תסקיר השפעה על הפרטיות (privacy impact assessment). לדוגמא ראו "Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks" שפרסם The Treasury Board of Canada בכתובת: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrldtb-eng.asp.

3.1.1.2.2.3. התקנת מצלמות מעקב תהיה מידתית רק אם התועלת שתצמח ממנה גוברת על פגיעה בפרטיות שתיגרם בעטיה. לעניין יישום מבחן משנה זה, יצוין כי בשל טיבן והיקף השפעתן על הציבור, מצלמות המעקב יגרמו בדרך כלל לפגיעה משמעותית בפרטיות, ועל כן מה שנותר לבדוק הוא בעיקר את התועלת שתופק מהתקנתן. ככל שהתועלת תהיה פחותה יותר כך יימצא שהתקנת מצלמות המעקב אינה מידתית.

3.1.1.2.3. **כאשר מבקשים להתקין מצלמות מעקב במקומות בהם מצויים קטינים, כגון מוסדות חינוך או מתנ"סים, יש לנקוט בזהירות יתרה**. בהיעדר הסמכה מפורשת לפי חוק להתקנת מצלמות, ספק אם ניתן להסתפק ביידוע פסיבי של הילדים המצולמים באמצעות שלטי אזהרה, כבסיס להכשרת המצלמה: שהרי בעיקרון ילדים אינם כשירים לביצוע פעולות משפטיות כדוגמת מתן הסכמה (ולו מכללא) לפגיעה בפרטיותם, ויש לבחון הצורך בקבלת הסכמה מפורשת ואינדיבידואלית של הורי הילדים כתנאי לשימוש במצלמות המעקב, צמצום ככל האפשר של עצם השימוש במצלמות, והקפדה על מיקומן ועל השימוש במידע הנאסף באמצעותן;

3.1.1.2.4. **קבלת הכרעה נכונה בדבר התקנת מצלמת מעקב במרחב הציבורי בידי רשות שלטונית מצריכה גם קיום שימוע ציבורי פומבי**[11], ואם שימוע איננו אפשרי אזי לכל הפחות ראוי להיוועץ בכל הרשויות ושאר בעלי העניין הנוגעים בדבר או העשויים להיות מושפעים מהתקנתן של מצלמות ספציפיות (ועדי עובדים, ארגונים חברתיים, ארגוני צרכנות, נציגים של בעלי עסקים מקומיים). מעת לעת על הרשויות לחזור ולבחון האם הנסיבות שהצדיקו את הצבתן של המצלמות לכתחילה עדיין עומדות בתוקפן, והאם המשך השימוש במצלמות עומד במבחן המידתיות. בנספח א' להנחיה מוצגת דוגמא לפירוט הנתונים אותם ראוי להציג בעת עריכת שימוע כאמור על ידי רשות שלטונית.

3.1.2. <u>הפעלת מצלמות מעקב: מיקום, כיסוי ופונקציונליות</u> - בתכנון מערכת מצלמות מעקב ובשימוש בהן ההגנה על פרטיות הציבור צריכה לשמש שיקול מרכזי. יישומה

[11] כך דורשות למשל הנחיות נציב הגנת הפרטיות של מוסדות האיחוד האירופי (EDPS) מחודש מרץ 2010, בכתובת: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf; ובאופן כללי: אפרת וקסמן, דנה בלאנדר, <u>דגמים של שיתוף אזרחים</u>, המכון הישראלי לדמוקרטיה, 2002, עמ' 54-45.

של תפיסת "תכנון לפרטיות" (Privacy By Design) כבר במהלך התקנת מערכת המצלמות יסייע להפעיל אותן בהתאם לעקרון המידתיות החולש על פגיעה בזכויות חוקתיות כדוגמת הזכות לפרטיות. בהקשר זה יש לבחון את הנושאים הבאים:

3.1.2.1. **מיקום התקנת המצלמות וזווית הצילום** - יש להציב את המצלמה במקום ובזווית שיכסו במידת האפשר רק את השטחים הרלבנטיים, ויקלטו באופן המזערי האפשרי את השטח שאיננו רלבנטי למטרת הצבתה של המצלמה[12]. במקרים בהם לא ניתן למנוע צילומו של שטח הרחב מן הנדרש, יש לשקול שימוש בטכניקות הסוואה או ערבול של הצילומים העודפים, או להגביל את יכולת ההתמקדות של המצלמה[13];

3.1.2.2. **מספר המצלמות** - רצוי להתקין בכל אתר את מספר המצלמות המינימאלי החיוני להשגת המטרה המבוקשת. מספר מצלמות גדול מן הנדרש עלול להביא לשימוש לא יעיל ולעודף איסוף מידע הפוגע כשלעצמו בפרטיות העוברים ושבים;

3.1.2.3. **זמני הצילום** - כדי שפגיעת המערכת בפרטיות תהיה מידתית, יש לצמצם את פעילות המצלמות רק לזמנים בהם הצילום הוא רלבנטי למטרה המבוקשת. קיימים מנגנונים המאפשרים את הפעלת המצלמה רק כאשר יש תנועה במתחם המצולם;

3.1.2.4. **רזולוציית התמונה ואיכותה** - על איכות הצילום להתאים למטרה המבוקשת. במקרים בהם תכלית הצבת המצלמה אינה מחייבת זיהוי פנים של אדם ספציפי (למשל בבקרת תנועה), אזי איכות גבוהה של התמונה תהיה בלתי מידתית משום שתאסוף פרטי מידע עודפים שאינם חיוניים.

3.1.2.5. שימוש **בפונקציות מיוחדות** של מצלמת מעקב, כגון אלה המפורטות להלן, מחייב תשומת לב מיוחדת ויישום קפדני של מידתיות הפגיעה הנובעת מהשימוש בהן:

3.1.2.5.1. שילוב של מערכת מצלמות המעקב עם מידע השמור במאגרי מידע אחרים, לרבות מאגרים ביומטריים;

3.1.2.5.2. טכנולוגיות זיהוי פנים או זיהוי צורת הליכה;

3.1.2.5.3. יכולות מעקב דינמיות המופעלות על בסיס קול או על בסיס מאפיינים מיוחדים שהוגדרו מראש, כגון תנועה, לבוש, או שפת גוף של האובייקטים המצולמים;

3.1.2.5.4. צילום תרמי או אינפרה אדום המסוגל לקלוט תמונה בחשיכה או בתנאי תאורה קלושים;

---

[12] ראו למשל הנחיות נציבות המידע הבריטית (ICO) בנושא "CCTV Code of Practice" (סעיף 6): http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx. הגבלת תחום הכיסוי של הצילום בעלת חשיבות גם בשל האפשרות שבעת מתן זכות העיון בצילום מסוים, הפגיעה בפרטיות של צדדים שלישיים מצטמצמת.

[13] השוו הנחיות EDPS בה"ש 10 לעיל, והנחיות ICO בה"ש 11 לעיל.

3.1.2.5.5. מפתוח ותיוג מתוחכמים של התמונות המוקלטות המאפשרים לבצע בהן חיפוש אוטומטי;

3.1.2.6. אין להשתמש במצלמות מעקב לצורך הקלטת קול, אלא לפי הוראות חוק האזנת סתר, התשל"ט-1979.

3.1.3. <u>יידוע הציבור על הצבת מצלמת מעקב</u>

3.1.3.1. האיסור שבסעיף 1 לחוק לפגוע בפרטיותו של אדם ללא הסכמתו, ודרישת השקיפות המוטלת בסעיף 11 לחוק מחייבים ליידע את הציבור על הצבת מצלמת מעקב. **אמצעי היידוע המינימלי הוא הצגת שלטים בסמוך למקום בו המצלמה מותקנת, וכן בכניסה לאזור הכיסוי של המצלמה** (גם אם הכניסה ממוקמת הרחק ממיקומה הפיזי של המצלמה), כדי להתריע על קיום מצלמת מעקב בפני הציבור בטרם כניסתו לאזור המצולם. בבניינים או במתחמים מגודרים רצוי להציב שלט גם על דלת הכניסה לבניין/מתחם. החובה להציב שלטי אזהרה מקבלת משנה חשיבות ותוקף כאשר קשה להבחין בקיומה של המצלמה (בשל מיקומה או צורתה).

3.1.3.2. **שלט האזהרה חייב להיות קריא וברור**, לרבות מבחינת גודלו, ועליו לכלול את הפרטים הבאים:

3.1.3.2.1. ציור של מצלמה, או סמל גרפי מקובל אחר המעביר בצורה ברורה את המסר שהאתר מצולם (רצוי לקבוע סימול אחיד);

3.1.3.2.2. שמו של הארגון האחראי על הצבת המצלמה[14];

3.1.3.2.3. תיאור תמציתי של מטרת הצבת המצלמה, למשל: "בטיחות", "מניעת עבירות", "בקרת תחבורה";

3.1.3.2.4. אם קיים, כתובת אתר האינטרנט בו מצויה רשימת המצלמות ומדיניות השימוש בהן (כמפורט בסעיף 3.1.3.3 להלן), או מספר טלפון וכתובת דוא"ל למענה על שאלות בנוגע לשימוש במצלמה.

3.1.3.3. לקיום דרישת השקיפות לפי סעיף 11 לחוק, רצוי שהגורם האחראי על התקנת מצלמת המעקב **יפרסם גם רשימה מרוכזת של מקומות התקנת מצלמות מעקב באתר האינטרנט שלו**. בנספח ב' להנחיה מוצגת דוגמא למידת הפירוט שתוצג ברשימה.

[14] "בעל המאגר" בלשונו של חוק הגנת הפרטיות; ציון זהותו של הארגון בשלט מיותרת כאשר היא ברורה מנסיבות העניין, למשל כשמצלמה מוצבת בתוך חנות או בכניסה למתקן מאובטח.

3.1.4. <u>שמירת הצילומים ומחיקתם</u>

3.1.4.1. שמירת הצילומים לאחר שהם אינם נחוצים עוד מהווה הפרה של עקרון הגבלת המטרה[15] ויוצרת סיכוני אבטחת מידע מיותרים, ומשום כך גם פוגעת בזכות החוקתית לפרטיות במידה העולה על הנדרש..

3.1.4.2. בראש ובראשונה יש לבחון בקפידה האם מטרת התקנת המצלמות בכלל מחייבת הקלטה של הצילומים, או שמא ניתן להסתפק בצילום חי בלבד. הקלטה שאינה נחוצה להגשמת המטרה אינה עומדת במבחני המידתיות.

3.1.4.3. ככל שקיים צורך להקליט, יש לקבוע את משך התקופה בה יישמרו ההקלטות. משך שמירת הצילומים יקבע בכל מקרה בנפרד לפי מבחני המידתיות, בהתאם למטרה הספציפית של התקנת המצלמה ולרגישות המידע הנקלט בעדשתה.

3.1.4.4. כדי למנוע תקלות מומלץ לתכנן את מערכת ההקלטה מראש לפי תפיסת *"תכנון לפרטיות"* (Privacy By Design) כך שהצילומים המוקלטים יימחקו אוטומטית לאחר פרק הזמן המוגדר. כדי לחסוך במשאבים אפשר גם לתכנן את ההקלטה כך ש"תדרוס" צילומים ישנים.

3.1.5. <u>זכות העיון של המצולם</u> – אופן מתן זכות העיון במידע מוסדר בסעיף 13 לחוק ובתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981, אולם לעיון בצילומים במצלמות המעקב יש להתייחס למאפיינים ייחודיים:

3.1.5.1. אופיו של המידע האגור במאגר **מחייב שזיהויו של מבקש העיון בצילומים יעשה גם לפי תמונה**;

3.1.5.2. כיוון שעל פי רוב בשלב הראשון, האנשים המצולמים לא יהיו מזוהים ולא ניתן יהיה לערוך בהקלטות חיפוש ממוחשב לפי שם, **על הבקשה לעיון במאגר להיות קונקרטית וספציפית יותר מן הרגיל**: ניתן לדרוש ממבקש העיון שיפרט את התאריך ואת השעה המדויקים בה הוא מבקש לעיין והסבר מדוע הוא מבקש לעיין במידע ממועדים אלה;

3.1.5.3. מתן זכות עיון בצילומים לפלוני עשוי לחשוף אותו למידע עודף לעניין זכות העיון שלו **ועלול לפגוע בפרטיות של אנשים אחרים**. לכן, **כאשר בצילום בו מבקש נושא המידע לעיין מופיעים גם אנשים אחרים, יש לנהוג בבקשה במשנה זהירות**: אפשרות אחת היא למחוק מהסרט את הדמויות האחרות או לטשטש אותן, אפשרות אחרת שתתאים יותר למצלמה שהותקנה באזור בו הציפיה לפרטיות היא פחותה – היא לאפשר למבקש העיון לצפות בהקלטה במתקני מפעיל המצלמה אך להימנע מלמסור לו העתק שלה[16].

---

[15] הקבוע בסעיפים 2(9) ו- 8(ב) לחוק, והפרתו היא עבירה על סעיפים 5 ו- 31א לחוק.

[16] סעיף 2(א) לתקנות העיון מאפשר להעניק את זכות העיון בתדפיס או במצג; לענייננו "תדפיס" קרי – העתק מן ההקלטה. לפי בג"צ 2303/90 **פיליפוביץ נ' רשם החברות**, פ"ד מו(1) 410, ובג"צ 7256/95 **פישלר נ' מפכ"ל המשטרה**,

3.1.6. <u>אבטחת מידע</u> - סעיף 17 לחוק מטיל אחריות לאבטחת המידע במאגר על בעל מאגר המידע, מנהל מאגר המידע והמחזיק בו. אבטחת מידע מוגדרת בסעיף 7 לחוק כהגנה על שלמות המידע ומניעת חשיפתו העתקו או שימוש בו ללא רשות כדין. על הגורמים האחראים לאבטחת המידע מוטל לנקוט בכל האמצעים הדרושים להשגת רמה נאותה שלה לפי דרישות הדין והרגולציה המעודכנים למועד הרלבנטי[17], כאשר המינימום הנדרש הוא נקיטת אמצעי האבטחה המפורטים בסעיף 3 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986. באופן כללי, אבטחת המידע במערכת מצלמות מעקב המופעלת בידי גוף פרטי או ציבורי כאחד, מחייבת:

3.1.6.1. קיום הגנה פיזית ולוגית על המערכת[18];

3.1.6.2. קביעת נהלים ברורים להקלטת הצילומים, לעיבודם ולהפצתם ולאבטחת המידע בהם;

3.1.6.3. קביעת רשימת מורשי גישה, והטלת מגבלות על גישתם למידע[19];

3.1.6.4. הקפדה בבחירת העובדים שיהיו בעלי גישה למידע, הדרכה נאותה שלהם בדבר נהלי אבטחת המידע ובדבר חובותיהם לפי הנהלים ולפי החוק, והחתמת העובדים על התחייבות לסודיות ולהימנע ממסירת תוכן הצילומים לגורמים בלתי מוסמכים;

3.1.6.5. מפעיל מערכת המצלמות צריך לנקוט משנה זהירות אם הוא נעזר בשירותי מיקור חוץ[20], שכן שימוש בקבלנים אינו מסיר את האחריות ממפעיל מצלמות המעקב לקיום כל החובות החלות עליו מכוח החוק, במיוחד לעניין פעולות רגישות יותר כגון העתקת הצילומים, מחיקתם או עריכתם אותן עדיף שיבצע מזמין השירות ולא עובדי הקבלן. ביחס לרשות שלטונית יצוין שבדומה להפרטת השימוש בכוח, גם הפרטת השימוש באמצעי הפוגע באופן חמור בפרטיות – כדוגמת הפעלת אמצעי מעקב במרחב הציבורי - איננה עניין של מה בכך והשלכותיה על חירויות האדם עשויות להיות עמוקות ונרחבות;

פ"ד נ(5) 1 ישנה אמנם עדיפות לקיים את זכות העיון באמצעות מסירת "תדפיס" – אולם במקרה שלפנינו זכותם החוקתית של האנשים האחרים המופיעים בצילום עשויה להטות את הכף לכיוון עיון באמצעות מצג דווקא.

[17] בנוסף על התקנות התקפות, פרסמה רמו"ט ביום 10.1.10 טיוטת תקנות מפורטות בעניין אבטחת מידע בגופים ציבוריים ופרטיים כאחד. גם בטרם כניסת התקנות החדשות לתוקף, ניתן להיעזר בהן כדוגמא לפרקטיקה ראויה. ראו: הרשות למשפט, טכנולוגיה ומידע, משרד המשפטים "**נייר עמדה בנושא תקנות אבטחת מידע להגנה על פרטיות**". בכתובת: http://www.justice.gov.il/MOJHeb/News/takanotavtachatmeida.htm

[18] במערכות מצלמות רבות יש אפשרות גישה מרחוק אל המחשב המכיל את המידע המצולם, על גבי רשת האינטרנט. במערכות אלה סיכוני אבטחה הנובעים מקישוריות לאינטרנט. יש לתת את הדעת לסיכונים אלה בעת שמירה של המידע.

[19] ההרשאה לצפייה בצילומי המצלמה ולהקלטתם תהיה רק על בסיס צורך לדעת, ורק במידה הנדרשת; רשימת הרשאות הגישה צריכה להיות מפורטת ומדויקת בשים לב לסוגים השונים של הפעולות שניתן לבצע במערכת מצלמות המעקב ובצילומם הנאגרים בה, למשל: רשות לראות את הצילום בזמן אמת; צפייה בצילומים המוקלטים; הרשאה להעתיק את ההקלטות; הרשאה לשליטה במערכות הזום והכוונון של המצלמה; יכולת מחיקה או עריכה של הצילומים.

[20] ראו הרשות למשפט, טכנולוגיה ומידע, משרד המשפטים "הנחיית רשם מאגרי מידע 2/2011 בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" בכתובת: http://www.justice.gov.il/MOJHeb/ILITA/Hanchayot/HanchayotDB/HanhayotDB.htm במחלקת ייעוץ וחקיקה במשרד המשפטים מתבצעת בימים אלה עבודת מטה במטרה לפרסם הנחיית יועץ משפטי לממשלה בנושא היבטי הפרטיות של מיקור חוץ של עבודות ושירותים מגופים ציבוריים.

3.1.6.6. קיום מערכת ניטור שתאפשר תיעוד ובקרה של כל ניסיונות הגישה למערכת: מי נחשף למידע, לאיזה סוג של מידע ומתי;

3.1.6.7. לבחון את יישומם של אמצעים משפרי פרטיות (privacy enhancing technologies) לצורך מניעה של שימוש לא ראוי במידע[21].

3.1.7. <u>הגבלת השימוש במידע</u> - אין לעשות שימוש בצילומים, ובכלל זה העברה, מסירה או גילוי לגורמים שאינם קשורים לארגון מציב המצלמות או למטרה המקורית של השימוש בצילומים. קל וחומר, שאסור גם למסור את הצילומים ממצלמת המעקב לפרסום באמצעי התקשורת, אלא במקרים קונקרטיים שבהם יש נימוקים מיוחדים ויוצאי דופן לכך.

3.2. כלי עזר ליישום האמור בהנחיה זו מצוי ב<u>**נספח ג'**</u>.

3.3. שימוש במצלמות מעקב בניגוד לאמור בהנחיה זו עלול להוות הפרה של חוק הגנת הפרטיות. פגיעה בפרטיות לפי סעיף 4 לחוק מהווה עוולה אזרחית ולפי סעיף 5 לחוק מהווה עבירה פלילית. כמו כן, סעיף 31א לחוק מונה עבירות אחריות קפידה לפי החוק.

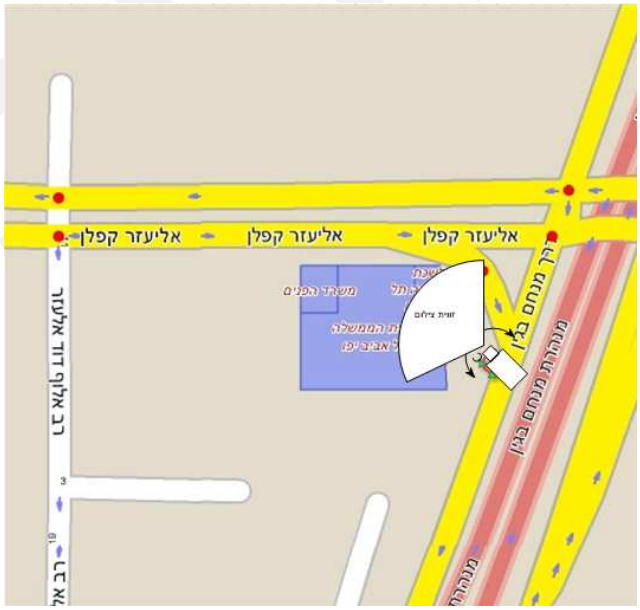
[21] בין אמצעים אלה ניתן למנות:
- אמצעים לאנונימיזציה של המידע המצולם (data anonnymization);
- אמצעים להצפנה של המידע המצולם (data encryption);
- אמצעים למזעור המידע המצולם (data minimization);
- אמצעים לוידוא זהותם של משתמשים במידע המצולם (identity systems);
- אמצעים להגבלת השימוש במידע המצולם על ידם (digital rights management);
- אמצעים למעקב וניטור אחר השימוש במידע המצולם.

נספח א' – <u>נתונים הנדרשים לרשות שלטונית בעת קבלת הכרעה בדבר התקנת מצלמת מעקב במרחב הציבורי</u>

חלק א' – פרטים אודות איסוף – מיקום המצלמה

1. המיקום המבוקש להתקנת המצלמה והשטח המכוסה על ידה. מומלץ להכין מפה המציגה את מיקום המצלמה, השטח המכוסה על ידה ואתרים רגישים הנכללים בשטח המכוסה (להלן דוגמא).
2. תקופת הניטור באמצעות המצלמה.
3. שם המוקד הצופה במצלמה ופרטי קשר שלו.
4. מטרת הצבת המצלמה במיקום זה.
5. אתרים רגישים הנכללים בשטח המכוסה.
6. הסיבות להצבת המצלמה במיקום המבוקש וצילום השטח המכוסה:
7. החלופות שנבדקו להצבת מצלמה.
8. האם יש אפשרות שלא לצלם אתרים רגישים בשטח המכוסה - יש לפרט חלופות אחרות שאינן מחייבות תיעוד אתרים רגישים בשטח המכוסה.
9. מאפייני המצלמה - סוג המצלמה, יכולות צילום (רזולוציה), תנאי צילום וכד'.
10. זוויות הצילום של המצלמה.
11. שעות פעילות המצלמה.

דוגמא למפה:



חלק ב' – פרטים אודות עיבוד המידע

1. שם מנהל מאגר המידע
2. שם הממונה על אבטחת המידע והגנה על הפרטיות במאגר המידע
3. תקופת שמירת המידע במאגר ומטרות השמירה

4. מורשי הגישה למידע – פירוט שם, תפקיד, סוג הרשאה ומטרה
5. "מחזיקים" במאגר המידע - האם יש ארגונים נוספים שמספקים שירותי עיבוד למידע או שיש להם גישה למידע.
6. אבטחת המידע - פירוט אמצעים שננקטים באופן שגרתי במאגר המידע למניעת שימוש לרעה במידע

נספח ב' – פרטים שיש למסור אודות הפעלת מצלמת מעקב במסגרת קיום חובת השקיפות לפי סעיף 11 לחוק הגנת הפרטיות, התשמ"א-1981

1. תיאור מערכת המצלמה וסוג המצלמה
2. מטרות הצבת המצלמה
3. השטח המכוסה על ידי המצלמה
4. שעות הפעלת המצלמה
5. פרטי הגורם האחראי לצפייה ושמירה של המידע
6. פרטי מנהל מאגר המידע
7. פרטי הממונה על אבטחת המידע במאגר המידע
8. תקופת שמירת המידע במאגר המידע
9. מטרות שמירת המידע
10. הגורמים בעלי הרשאת גישה למידע לצורך מטרות שמירת המידע
11. פרטי התקשרות לצורך מימוש זכות העיון בהקלטות לפי סעיף 13 לחוק

נספח ג' - רשימת בדיקה לקיום הוראות ההנחיה בהתקנת ושימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהן

נושא	סעיף בהנחיה	תוכן הבדיקה	הערות
קבלת ההחלטה על הצבת מצלמות מעקב	3.1.1.2	עריכת תסקיר של השלכות השימוש במצלמה על זכויות הציבור , ובמיוחד על הזכות לפרטיות	בתסקיר יש להתייחס לנושאים: תכלית השימוש במצלמות המעקב; מידתיות השימוש במצלמות המעקב; בחינת מקרים מיוחדים כגון הצבת מצלמות מעקב במקומות בהם מצויים קטינים; עריכת שימוע ציבורי פומבי במקרים מסוימים (ראו נספח א' להנחיה לעניין זה)
הפעלת מצלמות מעקב: מיקום, כיסוי ופונקציונליות	3.1.2.1	מיקום המצלמות וזווית הצילום במקום ובזווית שיכסו במידת האפשר רק את השטחים הרלבנטיים, ויקלטו באופן המזערי האפשרי את השטח שאיננו רלבנטי למטרת הצבתה של המצלמה	
	3.1.2.2	רצוי להתקין בכל אתר את מספר המצלמות המינימאלי החיוני להשגת המטרה המבוקשת	
	3.1.2.3	יש לצמצם את פעילות המצלמות רק לזמנים בהם הצילום הוא רלבנטי למטרה המבוקשת	
	3.1.2.4	על איכות הצילום להתאים למטרה המבוקשת	
	3.1.2.5	שימוש בפונקציות מיוחדות של מצלמת מעקב, כגון אלה המפורטות להלן, מחייב תשומת לב מיוחדת ויישום קפדני של מידתיות הפגיעה הנובעת מהשימוש בהן	
	3.1.2.6	אין להשתמש במצלמות מעקב לצורך הקלטת קול, אלא לפי הוראות חוק האזנת סתר, התשל"ט-1979	
יידוע הציבור על הצבת מצלמת מעקב	3.1.3.1	יש ליידע את הציבור על הצבת מצלמות מעקב, אמצעי היידוע המינימלי הוא הצגת שלטים בסמוך למקום בו המצלמה מותקנת, וכן בכניסה לאזור הכיסוי של המצלמה	

נושא	סעיף בהנחיה	תוכן הבדיקה	הערות
	3.1.3.2	שלט האזהרה חייב להיות קריא וברור, לרבות מבחינת גודלו	פרטים שיש לכלול בשלט: ציור של מצלמה, או סמל גרפי מקובל אחר; שם הארגון האחראי על הצבת המצלמה; תיאור תמציתי של מטרת הצבת המצלמה; אם קיים, כתובת אתר האינטרנט בו מצויה רשימת המצלמות ומדיניות השימוש בהן, או מספר טלפון וכתובת דוא"ל למענה על שאלות בנוגע לשימוש במצלמה.
	3.1.3.3	רצוי שהגורם האחראי על התקנת מצלמת המעקב יפרסם גם רשימה מרוכזת של מקומות התקנת מצלמות מעקב באתר האינטרנט שלו	בנספח ב' להנחיה מוצגת דוגמא למידת הפירוט שתוצג ברשימה
שמירת הצילומים ומחיקתם	3.1.4.2	יש לבחון בקפידה האם מטרת התקנת המצלמות בכלל מחייבת הקלטה של הצילומים, או שמא ניתן להסתפק בצילום חי בלבד	
	3.1.4.3	ככל שקיים צורך להקליט, יש לקבוע את משך התקופה בה יישמרו ההקלטות	משך שמירת הצילומים יקבע בכל מקרה בנפרד לפי מבחני המידתיות, בהתאם למטרה הספציפית של התקנת המצלמה ולרגישות המידע הנקלט בעדשתה
	3.1.4.4	מומלץ לתכנן את מערכת ההקלטה מראש לפי תפיסת "תכנון לפרטיות" (Privacy By Design) כך שהצילומים המוקלטים יימחקו אוטומטית לאחר פרק הזמן המוגדר	
זכות העיון של המצולם	3.1.5.1	בעת מימוש זכות העיון זיהויו של מבקש העיון בצילומים יעשה גם לפי תמונה	
	3.1.5.2	על הבקשה לעיון במאגר להיות קונקרטית וספציפית יותר מן הרגיל	
	3.1.5.3	כאשר בצילום בו מבקש נושא המידע לעיין מופיעים גם אנשים אחרים, יש לנהוג בבקשה במשנה זהירות	

נושא	סעיף בהנחיה	תוכן הבדיקה	הערות
אבטחת מידע	3.1.6.1	קיום הגנה פיזית ולוגית על מערכת מצלמות המעקב	
	3.1.6.2	קביעת נהלים ברורים להקלטת הצילומים, לעיבודם ולהפצתם ולאבטחת המידע בהם	
	3.1.6.3	קביעת רשימת מורשי גישה, והטלת מגבלות על גישתם למידע	
	3.1.6.4	הקפדה בבחירת העובדים שיהיו בעלי גישה למידע, הדרכה נאותה שלהם בדבר נהלי אבטחת המידע ובדבר חובותיהם לפי הנהלים ולפי החוק, והחתמת העובדים על התחייבות לסודיות ולהימנע ממסירת תוכן הצילומים לגורמים בלתי מוסמכים	
	3.1.6.5	יש לנקוט משנה זהירות בשירותי מיקור חוץ, שכן שימוש בקבלנים אינו מסיר את האחריות ממפעיל מצלמות המעקב לקיום כל החובות החלות עליו מכוח החוק, במיוחד לעניין פעולות רגישות יותר כגון העתקת הצילומים, מחיקתם או עריכתם אותן עדיף שיבצע מזמין השירות ולא עובדי הקבלן	ראו הנחיית רשם מאגרי מידע 2/2011 בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי
	3.1.6.6	קיום מערכת ניטור שתאפשר תיעוד ובקרה של כל ניסיונות הגישה למערכת: מי נחשף למידע, לאיזה סוג של מידע ומתי	
	3.1.6.7	לבחון את יישומם של אמצעים משפרי פרטיות (privacy enhancing technologies) לצורך מניעה של שימוש לא ראוי במידע	
הגבלת השימוש במידע	3.1.7	אין לעשות שימוש בצילומים, ובכלל זה העברה, מסירה או גילוי לגורמים שאינם קשורים לארגון מציב המצלמות או למטרה המקורית של השימוש בצילומים	

מידע לגבי ההנחיה

1. **מס' ההנחיה:**
2. **נושא ההנחיה:** שימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהן
3. **תאריך פרסום:**
4. **בתוקף מתאריך:**
5. **חוקים שאוזכרו**:

א. חוק יסוד: כבוד האדם וחירותו

ב. חוק הגנת הפרטיות, התשמ"א-1981

ג. חוק האזנות סתר, התשל"ז-1977

ד. תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981

ה. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986

6. **פסקי דין שאוזכרו**:

א. בג"צ 2303/90 **פיליפוביץ נ' רשם החברות**, פ"ד מו(1) 410

ב. בג"צ 7256/95 **פישלר נ' מפכ"ל המשטרה**, פ"ד נ(5) 1

ג. דב"ע 97/70-4 **אוניברסיטת תל אביב – ההסתדרות הכללית החדשה**, פד"ע ל' 385, 411

ד. בג"צ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים ואח'**, פ"ד נח(4) 842

ה. ע"ע 90/08 **איסקוב נ' מדינת ישראל – הממונה על חוק עבודת נשים**, (פורסם בנבו, 8.2.2011).

7. **מאמרים שאוזכרו**:

א. מ. בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות", **משפט וממשל** יא תשס"ח 9, 57

ב. אפרת וקסמן, דנה בלאנדר, <u>דגמים של שיתוף אזרחים</u>, המכון הישראלי לדמוקרטיה, 2002, עמ' 54-45

8. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.
9. **הנחיות רשם מאגרי מידע שאוזכרו**: הנחיית רשם מאגרי מידע 2/2011 בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי
10. **מילות מפתח:** אבטחת מידע, גילוי נאות, הסכמה מדעת, הסכמה מכללא, זכות עיון, מאגר מידע, מידע רגיש, מצלמות מעקב, שקיפות, CCTV.
11. **עדכונים**

גרסה	פרטים	תאריך