



תאריך: 3 בנובמבר 2010
כ"ו חשוון תשע"א
סימוכין: 015-99-2010-004346

הנדון: מצלמות מעקב - הדין החל ואופן השימוש

מבוא

1. במהלך העשורים האחרונים, הולך וקונה אחיזה בעולם השימוש באמצעים טכנולוגיים המיועדים לפיקוח ולמעקב חזותי וקולי מרחוק על שטחים ציבוריים ועל מתחמים פרטיים כאחד. טכנולוגיות אלה מכונות לעיתים Closed Circuit Television (CCTV) ופעמים Video Surveillance; לצורך הנוחות הן יכוננו להלן "מצלמות מעקב".
2. מצלמות מעקב עשויות לשמש למגוון רחב של מטרות המשקפות מידה משתנה של לגיטימיות ושל אינטרס ציבורי, כדוגמת הגנה על אנשים ועל רכוש, מניעת עבירות וגילויין, הכוונת תנועה, שמירה על סדר ציבורי ואף פיקוח על עובדים. למצלמות המעקב השפעה מהותית על המרחב הציבורי ועל פרטיות המשתמשים בו; לא בכדי השימוש בהן זכה לתשומת לב ציבורית ערה והוכפף לרגולציה מפורטת באירופה במיוחד, וכן במקומות אחרים בעולם.
3. מסמך זה מיועד להבהיר את תחולתם של דיני הפרטיות והגנת המידע על השימוש במצלמות מעקב ולהציג עקרונות בסיסיים וראשוניים לתנאים לשימוש בהן, בדגש על פרישתן על ידי רשויות ציבוריות והחלתן יכולת המעקב שלהן על המרחב הציבורי.
4. למבט העוקב אחרי בני אדם יש כוח ממשמע וממשטר המשפיע על אופן התנהגותם. השפעת כוחה הממשטר של עדשת המצלמה על המצולמים עשויה להיות חיובית, כשהיא מונעת מהם לנהוג באופן עברייני ומזיק לזולתם 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 ולהצטדק¹.
5. טכנולוגיית המעקב באמצעות מצלמות הנשלטות ממוקד מרוחק, באופן בו כל אדם הנמצא בתחום הכיסוי של המצלמה עשוי להיות תחת מבט בוחן בכל רגע נתון, מעצימה את יכולת הפיקוח ומחילה אותה על אוכלוסיות גדולות בצורה שלא הייתה אפשרית ללא השימוש

¹ להרחבה על ההיבט הפסיכולוגי ועל הצדקות נוספות לזכות לפרטיות ראה מ. בירנהק, שליטה והסכמה: הבסיס היוני של הזכות לפרטיות, משפט וממשל יא תשס"ח 9, 57.



במצלמות המעקב. קיומן של מצלמות המעקב פוגע בצורך הפסיכולוגי למרחב הפרטי, ולכן מצדיק לנהוג בזהירות ובמשורה בהתקנת המצלמות ובשימוש בהן, במיוחד בכל הנוגע להשפעתן על ילדים².

6. כבר בפתח הדברים נבקש להדגיש שני סוגים של מקומות המחייבים זהירות בהפעלת מצלמות המעקב. כפי שיפורט להלן, קיימת בעיה מיוחדת בהצבת מצלמות מעקב **ברשות הרבים** בשל הקושי בהשגת הסכמת המצולמים הפוטנציאליים לפגיעה בפרטיותם הגלומה בהפעלת המצלמה. במקרים רבים גם עולה שאלה מקדמית של הגורם הרשאי לצלם במרחב הציבורי, וככל שהצילום מחייב הסכמה, האם ההסכמה לצילום במקומות ציבוריים היא חופשית ואמיתית – וזאת אם לאזרחים אין חופש בחירה ואין אפשרות פרקטית להימנע מכניסה לאזור המצולם. קושי זה מחייב הקפדה מיוחדת וריסון רב יותר בשימוש במצלמות ברשות הרבים. יש להדגיש שלא רק שטחים פתוחים הנמצאים בבעלות הציבור (כגון כבישים, פארקים וכיכרות העיר) נחשבים ל"רשות הרבים" לצורך זה, אלא גם מתחמים שהבעלות עליהם היא אמנם פרטית, אך יש לציבור הרחב גישה חופשית אליהם, למשל מרכזי קניות. במאמר מוסגר יצויין כי בניגוד לצילום הוידאו המאפשר יכולת התחקות רציפה ומתמדת, צילום ה- stills האקראי או הבודד הנעשה ברשות הרבים, לא יפגע בד"כ בזכות הפרטיות (בניגוד לצילום ברשות היחיד – ראה סעיף 2(3) לחוק).

7. כאמור, תשומת לב מיוחדת יש להקדיש גם לשימוש במצלמות מעקב **במקומות בהם נוהגים להתכנס ילדים**, כגון מוסדות חינוך או מתנ"סים. בהיעדר הסכמה מפורשת לפי חוק להפעלת המצלמה, 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. לפיכך יש לנקוט זהירות יתרה בהתקנת מצלמות במקומות כינוס של ילדים, ובאתרים אותם פוקדים ילדים מזהים על בסיס קבוע - למשל בתי ספר - יש לבקש הסכמה מפורשת ואינדיבידואלית של הורי הילדים כתנאי לשימוש במצלמות המעקב, ויש לצמצם ככל האפשר את עצם השימוש במצלמות, ולהקפיד על מיקומן ועל השימוש במידע הנאסף באמצעותן.

² מצלמות המעקב המודרניות הן למעשה הגשמה של מתקן "פאן אופטיקון" – מבנה היקפי המאפשר למשטר קבוצה גדולה של אנשים, למשל אסירים, באמצעות משגיח אחד המצוי במרכז המבנה כ"רואה ואינו נראה" בעל יכולת מעקב מתמיד אחרי המפוקחים שבהיקף - שהגה הפילוסוף האנגלי בנתהאם במאה ה-18. ראה בירנהק, ה"ש 1 לעיל, בעמ' 61.



האם אוסף הצילומים השמור שנוצר משימוש במצלמת מעקב הוא "מאגר מידע"?

8. צילום והקלטה דיגיטליים המשלבים יכולת מפתוח אוטומטית ואפשרויות אחזור לפי פרמטרים כגון חתכי זמן הצילום ומיקומו – הם תכונות בסיסיות במערכות צילום כיום. יכולות זיהוי אוטומטיות, או אוטומטיות למחצה של אובייקטים שונים בתמונה, כגון פענוח לוחיות זיהוי של כלי רכב או הפרדה של הפריטים המופיעים בתמונה (אנשים, כלי רכב, בעלי חיים וכד') גם הן טכנולוגיות מוכחות בהן משתמשים באופן שגורתי.

9. גם האפשרות לזיהוי ממוחשב של פני האנשים הנקלטים במצלמות המעקב – כבר איננה בגדר מדע בדיוני: יכולות אלה הולכות ומשתפרות וקיימות כיום לא רק אצל רשויות ביטחון ושיטור, אלא אף מוצעות למכירה בשוק הפרטי וחלקן אף מופץ ברשת האינטרנט לתיג של תמונות ברשתות חברתיות. מערכות זיהוי הפנים האוטומאטי הקיימות כיום אמנם עדיין אינן בשלות, אולם בנסיבות מסוימות עשוי הדיוק בזיהוי להגיע עד 95%³. עם התפתחות הטכנולוגיה, צפוי שדיוק זיהוי הפנים ילך וישתפר בעתיד הקרוב.

10. לנוכח מידת האמינות המשתנה במערכות הזיהוי האוטומאטי הקיימות היום, לא ישים לקבוע במסמך זה מסמרות לגבי כל סוגי מצלמות המעקב שהמידע הנקלט בהן יהיה ניתן לזיהוי ולשיוך לאדם ספציפי. עם זאת, לפחות במקרים המפורטים להלן אין לדעתנו כל ספק שצילומיהן המוקלטים של מצלמות המעקב יכנסו לגדר "מאגר מידע" המתייחס למידע מזוהה, או ניתן לזיהוי, אודות אדם, כמשמעותו בסעיף 7 לחוק הגנת הפרטיות, תשמ"א – 1981 ("חוק הגנת הפרטיות")⁴:

10.1. מערכות צילום המפעילות טכנולוגיות כגון זיהוי רכב לפי לוחית רישוי (LPR), אשר כבר כיום מספקות זיהוי אוטומאטי ברמת דיוק גבוהה⁵;

10.2. מערכות אשר לצד הקלטת מצלמות המעקב ניזונות גם ממידע ממאגרים נוספים, באופן בו הצלבת המידע משני המקורות ועיבודו מאפשרים רמה גבוהה של זיהוי האובייקטים המצולמים; למשל צילומי מצלמה המוצבת במפעל, המוצלבים עם מאגר התמונות המזוהות של עובדי המפעל;

10.3. כל מערכת מצלמות המפעילה זיהוי פנים אוטומאטי ברמת דיוק ממוצעת מינימאלית; ככלל אצבע גרידא, נציין שלדעתנו מערכת המספקת זיהוי ברמת דיוק

³ Brian C. Lovell, Reliable Face Recognition for Intelligent CCTV, *National ICT Australia (NICTA)* : http://www.nicta.com.au/_data/assets/pdf_file/0009/14949/Reliable_Face_Recognition_for_Intelligent_CCTV.pdf

⁴ יצוין כי הדיגיטיזציה של מצלמות המעקב על יכולת השמירה והאחזור הגלומות בה, הציפה והידדה באופן מהותי את בעיית הפרטיות והגנת המידע בצילומי מצלמות המעקב, בהשוואה למצלמות המעקב האנלוגיות בהן השתמשו בעבר.

⁵ LPR משמשת כבר כיום בפועל בהניונים ובכבישי אגרה.



- ממוצעת של 20% לפחות – ודאי נחשבת למידע הניתן לזיהוי "על אדם", הנכנס לגדר "מאגר מידע" לצורך סעיף 7 לחוק.
11. עצם הידיעה על הימצאותו של אדם במקום נתון ובזמן נתון או עצם חזותו – עשויות לכלול נתונים על צנעת אישיותו (כגון עם מי הוא נמצא ובאילו נסיבות), על מצבו בריאותו (כגון הימצאותו במרפאה), על אמונתו הדתית (הימצאותו בבית תפילה של עדה מסוימת או לבוש מסוים של המצולם) - וכיוצ"ב 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, או להסיק מידע רפואי מניתוח תמונתו החזותית או מצילום טרמי שלו.
12. כפי שנקבע בפסק הדין בעניין **התנועה לחופש המידע נ' רשות החברות הממשלתיות**⁶ "את תוכנו של הביטוי "ענייניו הפרטיים של אדם" יש לצקת בכל מקרה בהתאם למכלול הנתונים הרלוונטיים, ותוך מחויבות להגנה על יכולתו של האדם לקיים את האוטונומיה שלו ואת המרחב הפרטי הנתון לו". כדי להגן על האוטונומיה של בני האדם, מחייבות יכולות העיקוב ואחזור המידע המתקדמות הקיימות כיום במרחב הציבורי – להחיל על השימוש במצלמות מעקב את דיני הגנת המידע. לא מכבר קבע בית המשפט העליון שרשת האינטרנט היא **"כיכר העיר החדשה"**, ובתור שכזו יש לבצר ולעגן בה את הזכות לאנונימיות הנגזרת מן הזכות לפרטיות⁷; קל וחומר שיש הצדקה להגן על פרטיות המידע הנאסף אודות אדם בקשר לפעילותו ב"**כיכר העיר הישנה**", במיוחד כאשר הקדמה הטכנולוגית הופכת את המידע לנגיש יותר ולבר איחזור על נקלה.
13. גם באירופה הרגולציה של מצלמות המעקב נעשית באספקלריה של חוקי הגנת המידע⁸. הועדה המייעצת שהוקמה לפי **האמנה** האירופית בנושא עיבוד מידע אישי⁹, הצהירה שקולות ותמונות נחשבים ל"מידע אישי" ככל שהם מספקים מידע על אדם הניתן לזיהוי אפילו

⁶ ע"מ 9341/05 - התנועה לחופש המידע נ' רשות החברות הממשלתיות ואח'. תק-על 2009(2), 2008, עמ' 2021 – פסקה 23.
⁷ רע"א 4447/07 רמי מור נ' ברק אי.טי.סי. [1995] החברה לשרותי בזק בינלאומיים בע"מ, פסקאות 13 – 16.

⁸ *A review of the increased use of cctv and video – surveillance for crime prevention in Europe – European Parliament, Directorate General Internal Policies Policy Department C, april 2009.* <http://www.statewatch.org/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf>

⁹ *Council of Europe Convention No. 108/1981 for the protection of individuals with regard to automatic processing of personal data.*



בעקיפין¹⁰. סעיף 14 למבוא **לדירקטיבת האיחוד האירופי על הגנת המידע**¹¹, קובע במפורש את תחולתה של הדירקטיבה על עיבוד של *sound and image data relating to natural persons*, ובשים לב להתפתחויות (אשר כבר בשנת 1995 היו) צפויות בטכנולוגיות של הקלטה, אחסון, עיבוד ושידור של מידע מסוג זה, אף דורש סעיף 33 לדירקטיבה מנציבות האיחוד לשוב ולבחון מעת לעת את אופן יישומה היעיל על עיבודן של הקלטות קול ותמונה הנוגעות לאדם. הועדה המייעצת של רשויות הגנת המידע במדינות החברות באיחוד, שהוקמה לפי סעיף 29 לדירקטיבה, קבעה במפורש שהדירקטיבה חלה גם על עיבוד קול ותמונה **באמצעות מצלמות מעקב**, ואף הציגה פרשנות מרחיבה לפיה נתוני קול ותמונה הקשורים לאדם הניתן לזיהוי נחשבים ל- "personal data" גם אם אינם כוללים דווקא את פני האנשים נשואי המידע אלא מידע אחר בעל זיקה אליהם (כגון לוחיות רישוי של מכוניות או קוד סודי של כרטיס בנקאי שנתפס בעדשת המצלמה), ובלי קשר לסוג מערכת המעקב ולמגוון האפשרי של מאפייניה הטכנולוגיים; כדי להסיר ספק גם הבהירה ועדת סעיף 29 שזיהויו של המידע לאדם ספציפי – שהוא תנאי לתחולתה של הדירקטיבה – יכול להיות מושג גם בעקיפין באמצעות הצלבת הצילומים עם מידע המוחזק בידי צד שלישי, או עם מידע המושג בטכנולוגיות אחרות ממצלמות מעקב¹².

התנאים המוקדמים לפגיעה בפרטיות: הסכמת הנפגע וחוקתיות

14. ראינו אם כך שבמקרים מסויימים, הצילומים המבוצעים ומוקלטים באמצעות מצלמת מעקב הם "מידע" אישי אשר אחזקתו וניהולו של אוסף שלהם כפופים להוראות פרק ב' לחוק ובפרט לחובת ההודעה למי שהמידע אודותיו (להלן – נשוא המידע), לאיסור על שימוש במידע למטרה שונה ללא הסכמה, לחובה לתת זכות עיון במידע ותיקונו המוקנית לנשוא המידע, לחובת הסודיות ואבטחת המידע המוטלת על מנהל המאגר ומחזיקו ולחובת הרישום.

¹⁰ ARTICLE 29 Data Protection Working Party (hereinafter "wp29"), Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, p. 5 s. 2b.

¹¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

¹² ראה חוות דעתה של WP29, ה"ש 6 לעיל, עמ' 15 סעיף 6.



15. באיסוף המידע באמצעות מצלמות מעקב גלומה גם פגיעה בזכות לפרטיות עצמה, המעוגנת בפרק א' לחוק הגנת הפרטיות¹³ ובסעיף 7(א) לחוק יסוד: כבוד האדם וחירותו¹⁴. לפיכך, כוחם של העקרונות המפורטים במסמך זה, שאינם שאובים אך ורק מפרק ב' לחוק הגנת הפרטיות, יפה גם למצלמות שאינן "מאגר מידע" לפי סעיף 7 לחוק.

16. עקרון בסיסי בחוק הגנת הפרטיות הוא שאין פוגעים בפרטיות של אדם ללא הסכמתו (סעיף 1 לחוק). לגבי רשויות המדינה כבר קבע בית המשפט¹⁵ **שלא די בהסכמת הנפגע** 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".

17. לכאורה אפשר היה לטעון שדרישת החוקתיות אינה צריכה לחול על **גורם פרטי** שאיננו "רשות מרשויות השלטון", המבקש להתקין מצלמת מעקב ברשות הרבים או במרחב הציבורי. אולם בשל טיבה ותחום השפעתה, ברוב המקרים כלל לא ניתן לקבל הסכמה מכל מי שפרטיותו תיפגע בשל המצלמה בוודאי שלא הסכמה מפורשת, ולכל היותר אפשר יהיה לייחס להם הסכמה מכללא לפגיעה בפרטיותם (ראו פירוט בהמשך). בשים לב לכך, יש מקום לטעון שגם הצבת מצלמות במרחב הציבורי בידי גורם פרטי, ראוי לבחון באספקלריא החוקתית¹⁶.

18. סוגיה חוקתית נוספת נוגעת ל**זהות הגורם האחראי על הפעלת המצלמות**. כפי שיפורט בהרחבה להלן, אחת התכליות המרכזיות להפעלת מצלמות מעקב **במרחב הציבורי**, והתכלית הלגיטימית היחידה בהקשר של אכיפת חוק היא התמודדות עם אלימות ועם פשיעה חמורה. השאלה האם ראוי ורצוי "להפריט" את הסמכויות המיועדות לטיפול בבעיות אלה, ולהעבירן מטיפול המשטרה לגורמים נוספים, כגון הרשויות המקומיות היא בעיה נכבדת וקשה, החורגת בהרבה מגבולות מסמך זה. מפאת קוצר היריעה, די אם נדגיש בשלב זה שבדומה

¹³ צילום אדם במצלמה ברשות הרבים, עשוי להגיע כדי "בילוש או התחקות... העלולים להטרידו..." [סעיף קטן 2(1) לחוק]. והוא לכל הפחות יוצר סיכון לפגיעה בפרטיות שעניינה "פרסום תצלומי של אדם ברבים בנסיבות שבהן עלול... להשפילו" [ס"ק 4(4)], שימוש בידעיה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה [ס"ק 9(9)], ובנסיבות מסוימות אף כדי פרסומו של עניין הנוגע לצנעת חייו שהאישיים של אדם או למצבו הבריאותי [ס"ק 11(11)]. מובן גם שתחום הכיסוי של מצלמה **המוצבת** ברשות הרבים, עלול להכנס לגדר "צילום אדם כשהוא ברשות היחיד" [סעיף 2(3) לחוק].

¹⁴ "כל אדם זכאי לפרטיות ולצנעת חייו".

¹⁵ בג"צ 8070/98 האגודה לזכויות האזרח נ' משרד הפנים ואח'.

¹⁶ 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 נשוא המידע - המעיבים על יכולתו של האחרון לתת הסכמה מדעת, חופשית ומרצון לפגיעה בפרטיותו. כך למשל ביחסי עובד מעביד - ראה דב"ע 97/70-4 **אוניברסיטת תל אביב** - ההסתדרות הכללית החדשה, פד"ע ל' 385, 411.



להפרטת השימוש בכוח, גם הפרטת השימוש באמצעי הפוגע באופן חמור בפרטיות – איננה עניין של מה בכך והשלכותיה על חירויות האדם עשויות להיות עמוקות ונרחבות.

קבלת ההחלטה על הצבת מצלמות מעקב

19. שימוש במצלמות מעקב במרחב הציבורי, במיוחד בידי רשויות ציבוריות, חייב אם כך לעמוד בתנאי פסקת ההגבלה החוקתית: הסמכה מפורשת בחוק, תכלית ראויה ועמידה במבחן המידתיות. לשם ביסוס התכלית הראויה והמידתיות, חייבת ההחלטה על השימוש במצלמת מעקב להתקבל באופן מושכל ומודע, לאחר בחינת הצרכים והחלופות לשימוש במצלמה. הצבת מצלמת מעקב איננה החלטה שניתן לקבל כלאחר יד רק משום שאפשר להציב אותה, כגון שהתפנה תקציב לרכישתה או שארע אירוע נקודתי שגורם ללחץ לעשות כן.

20. במלים אחרות, בטרם קבלת ההחלטה על עצם השימוש במצלמה יש לערוך **תסקיר של השלכות השימוש במצלמה על זכויות הציבור**¹⁷, ובמיוחד **על הזכות לפרטיות**¹⁸; ככל שתחום הכיסוי רחב יותר, והיקף האנשים המושפעים צפוי להיות גדול יותר – כך צריכה להיות הבדיקה המכינה עמוקה ומקיפה יותר.

21. בשלב הראשון, יש להצביע על התכלית שאותה מבקשים להשיג באמצעות מצלמות המעקב. מטרת הצבת המצלמות חייבת להיות מוגדרת באופן חד, ספציפי ומפורש – ולאחר שנקבעה המטרה אין להשתמש בצילומים למטרות זרות. הגדרת מטרה כללית ומעורפלת כגון "מניעת עבירות" או "בטחון הציבור" לא תספיק, וראוי לציין את התכליות ברמת פירוט גבוהה יותר, כגון "צמצום אלימות נוער הקשורה לשכרות באזור בילוי מסוים", או "אבטחת כניסה למתקן בטחוני רגיש ספציפי". הגדרת המטרה ברמת רזולוציה זו מחייבת כמובן לבחון האם עובדתית קיימת בכלל בעיה שפתרונה מצריך הצבת מצלמות מעקב: אם לדוגמה המטרה היא מניעת מקרי אלימות במקום מסוים – יש צורך לאסוף נתונים ותייעוד על חומרת האלימות ועל שכיחות התופעה והיקפה, ולוודא האם מדובר בהתרחשות חד פעמית ומקרית או בתופעה קבועה או חוזרת.

¹⁷ הצבת מצלמת מעקב בשטח ציבורי עלולה להשפיע גם על אינטרסים אחרים של ציבור המשתמשים בו, בנוסף על הזכות לפרטיות: כך לדוגמה, מצלמה המופעלת לפי תזוזה עלולה למנוע משומרי שבת לעבור בתחום הכיסוי שלה.
¹⁸ תהליך זה נקרא תסקיר השפעה על הפרטיות (privacy impact assessment). להרחבה בנושא זה ראו באתר האינטרנט של המשרד להגנת המולדת האמריקאי (DHS) ב-

http://www.dhs.gov/files/publications/gc_1209396374339.shtm



22. פסקת ההגבלה בחוק היסוד דורשת גם שתכלית הפגיעה בזכות תהיה "ראויה". קשה להגדיר על דרך החיוב באופן כולל וממצה מהי התכלית "הראויה". וודאי שקיום התפקיד המוטל על רשות ציבורית בחוק הוא תכלית ראויה; ברור גם שהגנה על שלומו ובטחונו של הציבור היא תכלית ראויה. אך קשה יותר להגדיר במדויק מהי תכלית ראויה למצלמות מעקב שהתקין גוף פרטי שאינו ממלא תפקיד שהוטל עליו בחוק.

23. בשלב השני של הבדיקה המקדימה יש לבחון את מידתיות השימוש במצלמות מעקב לשם השגת המטרה הרצויה, בשים לב לשלושת מבחני המשנה שהוכרו בפסיקה כקונקרטיזציה של עקרון המידתיות¹⁹. ראשית, צריך לוודא האם מצלמות המעקב הן בכלל האמצעי המתאים והיעיל להשגת המטרה הרצויה.

24. שנית, יש לבחון האם ניתן להשיג את המטרה הרצויה באמצעי שהוא פחות פוגעני בפרטיות; כך למשל, אם לצורך מניעת עבירות אלימות בפארק ציבורי, אפשר להגביר את סיורי המשטרה, להגביר את התאורה, או לסגור את הפארק בלילות – יש להימנע משימוש במצלמות מעקב; ובדומה לכך יש להימנע מהתקנת מצלמות מעקב בכניסה למתקן המחזיק מאגר מידע רגיש, אם אפשר להגביר את אבטחתו באמצעים פיזיים כגון סורגים, דלתות משוריינות והתקנת מערכת בקרת גישה תלוית סיסמה או כרטיס חכם.

25. שלישית, התקנת מצלמות אבטחה תהיה מידתית רק אם התועלת שתצמח ממנה תהיה שקולה לפגיעה בפרטיות שתיגרם בעטייה. לעניין יישומו של מבחן משנה זה יש לציין שבשל טיבן והיקף השפעתן על הציבור, מצלמות המעקב יגרמו בדרך כלל לפגיעה משמעותית בפרטיות²⁰. הואיל וכך, מה שנוטר לבדוק הוא בעיקר את התועלת שתופק מהתקנתן. כך למשל, התקנת מצלמות מעקב לצורך מניעת עבירות פעוטות של ניקיון וסדר ציבורי – תהיה בלתי מידתית גם אם היא יעילה וגם אם אין אמצעי פוגעני פחות להשגת המטרה, מפני שהפגיעה החמורה בפרטיותם של באי המקום עולה פי כמה מונים על התועלת לציבור משמירה על המתקנים והניקיון; ומאידך שימוש במצלמות למניעת אלימות חמורה, תעמוד במבחן המידתיות השלישי משום התועלת הממשית שהיא מביאה לציבור.

¹⁹ בג"צ 1715/97 לשכת מנהלי ההשקעות נ' שר האוצר, פסקה 17 לפסק דינו של הנשיא ברק.
²⁰ גם בנסיבות רגילות התקנת מצלמת מעקב תגרום להשפעה משמעותית על פרטיות הציבור; קל וחומר שמצלמה תגרום לפגיעה קשה בפרטיות במקומות בהם קיימת ציפייה מוגברת לפרטיות: חדרי שירותים, מלתחות וכד'. לכן במקומות אלה קשה יהיה להצדיק התקנת מצלמת מעקב גם אם תועלתן תהיה ניכרת.



26. כאמור במבוא למסמך זה, הצבה של מצלמות אבטחה במקומות בהם מצויים קטינים מחייבת זהירות יתרה. שימוש במצלמות במקומות כינוס של קטינים עלול גם להשפיע בצורה משמעותית על תחושת החופש והאוטונומיה שלהם, החיונית לצורך התפתחות תקינה.

27. משום פולשנותן של המצלמות ובשל השפעתן על ציבור רחב, ועל מנת לשפר את היכולת לבחון האם קיים צורך אמיתי במצלמות והאם ישנן חלופות להתקנתן, אנו סבורים כי קבלת הכרעה נכונה בדבר התקנת מצלמת מעקב במרחב הציבורי בידי רשות שלטונית – מחייבת גם קיום **שימוע ציבורי** פומבי²¹, ואם שימוע איננו אפשרי אזי לכל הפחות ראוי להיוועץ בכל הרשויות ושאר בעלי העניין הנוגעים בדבר או העשויים להיות מושפעים מהתקנתן של מצלמות ספציפיות. למשל: ועדי עובדים, ארגונים חברתיים, ארגוני צרכנות, נציגים של בעלי עסקים מקומיים.

28. מעת לעת על הרשויות לחזור ולבחון האם הנסיבות שהצדיקו את הצבתן של המצלמות לכתחילה עדיין עומדות בתוקפן, והאם **המשך** השימוש במצלמות עומד במבחן המידתיות.

מידתיות בהפעלת המצלמות: מיקום, כיסוי ופונקציונאליות

29. ככל שלאחר התהליך המתואר לעיל התקבלה ההחלטה המקדמית על עצם השימוש במצלמות המעקב²² - ההגנה על פרטיות הציבור צריכה לשמש שיקול מרכזי, שלא לומר ראשון במעלה גם בתכנון מערכת המצלמות ושימוש בהן. יישומה של תפיסת "תכנון לפרטיות" (Privacy By Design) כבר במהלך התקנת מערכת המצלמות יסייע להפעיל אותן בהתאם לעקרונות המידתיות החולש על פגיעה בזכויות חוקתיות כדוגמת הזכות לפרטיות.

30. **מיקום התקנת המצלמות וזווית הצילום** הם נתונים בעלי השפעה מכרעת על הפגיעה בפרטיות. יש להציב את המצלמה במקום ובזווית שיכסו במידת האפשר רק את השטחים הרלבנטיים, ויקלטו באופן המזערי האפשרי את השטח שאיננו רלבנטי למטרת הצבתה של המצלמה²³. כך למשל, כשמצלמה מוצבת במטרה לנטר את התנהגותם של באי פארק ציבורי

²¹ כך דורשות למשל הנחיות נציב הגנת הפרטיות של מוסדות האיחוד האירופי (EDPS) מהודש מרץ 2010; ראה בקישור הבא בעמ' 13 בסעיף 4:

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, דגמים של שיתוף אזרחים, המכון הישראלי לדמוקרטיה, 2002, ובעמ' 45-54.

²² מובן שההפרדה בין שלב ההחלטה על עצם השימוש במצלמות ובין שלב התקנתן והשימוש בהן – עשויה להיות מלאכותית; אותם מבחני מידתיות עשויים לשמש בשני השלבים גם יחד בערבוביה.

²³ ראה 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



– יש להקפיד שלא תכוון לבתים וחצרות פרטיים השוכנים בסמוך אליו, או כשמצלמה מוצבת לצורך בקרת כניסה למבנה, יש לוודא שצילום השטח הציבורי הסובב את השער יהיה מוגבל ומצומצם. 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 המצלמה²⁴.

31. **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.

32. **זמני הצילום** – כדי שפגיעת המערכת בפרטיות תהיה מידתית, יש לצמצם את פעילות המצלמות רק לזמנים בהם הצילום הוא רלבנטי למטרה המבוקשת. כך למשל, מצלמות אבטחה של בתי עסק או משרדים אפשר להגביל רק לשעות בהם העסקים סגורים ואינם מאוישים; אפשר לתכנת את המנגנון כך שהמצלמה תפעל רק כאשר יש תנועה במתחם הרגיש יותר של האזור המצולם, כפי שהוגדר מראש (בדומה לאזעקת נפח).

33. **גם רזולוציית התמונה ואיכותה** הם משתנים המשפיעים על מידת פגיעתה של המצלמה בפרטיות המצולמים. אם לדוגמה תכלית הצבת המצלמה איננה מחייבת זיהוי פנים של אדם ספציפי (למשל בבקרת תחבורה), אזי איכות גבוהה של התמונה תהיה בלתי מידתית משום שתאסוף פרטי מידע עודפים שאינם חיוניים. על איכות הצילום להתאים למטרה המבוקשת.

34. שימוש **בפונקציות מיוחדות** של מצלמת מעקב בעלות השלכה על הפרטיות, מחייב תשומת לב מיוחדת ויישום קפדני של מידתיות הפגיעה הנובעת מהם. לדוגמה מדובר בפונקציות מצלמה כגון –

34.1. שילוב של מערכת הצילום עם מידע השמור במאגרי מידע אחרים, לרבות מאגרים ביומטריים;

34.2. טכנולוגיות זיהוי פנים או זיהוי צורת הליכה;

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

34.4. צילום תרמי או אינפרא אדום המסוגל לקלוט תמונה בחשיכה או בתנאי תאורה קלושים;

²⁴ השווה הנהיות EDPS ה"ש 19 לעיל, בעמ' 27, והנהיות ICO ה"ש 21 לעיל.



- 34.5. מפתוח ותיוג מתוככמים של התמונות המוקלטות המאפשרים לבצע בהן חיפוש אוטומאטי ;
- 34.6. אין להשתמש במצלמות מעקב לצורך הקלטת קול, אלא לפי הוראות חוק האזנת סתר, תשל"ט - 1979.

יידוע הציבור על הצבת המצלמה

35. החובה ליידע את הציבור על הצבת מצלמת מעקב, נובעת מן האיסור שבסעיף 1 לחוק לפגוע בפרטיותו של אדם ללא הסכמתו. יידוע הציבור מאפשר למעוניין בכך להימנע מהצילום, ובמקביל לייחס לאנשים המצולמים הסכמה מכללא לאיסוף המידע אודותם ולשימוש בו, בכפוף לסייגים המפורטים להלן. מקום פרסום ההודעה לציבור ותוכנה של ההודעה נגזרים מהגדרת המונח "הסכמה" בסעיף 3 לחוק הקובע שההסכמה תהיה מודעת.
36. כיוון שבמקרים רבים הציבור הצפוי להיקלט בעדשות המצלמה איננו מוגדר או מזוהה מראש, במיוחד כאשר מדובר במצלמות המוצבות במרחב הציבורי, אמצעי היידוע המינימאלי הוא הצגת שלטים בסמוך למקום בו המצלמה מותקנת. בנוסף על שלט בקרבת המצלמה עצמה, יש להציב את השלט גם בכניסה לאזור הכיסוי של המצלמה (גם אם פירושו של דבר הוא התקנת השלט הרחק ממיקומה הפיזי של המצלמה), כדי להתריע לציבור בטרם כניסתו לאזור המצולם. בבניינים או במתחמים מגודרים רצוי להציב שלט גם על דלת הכניסה. במקומות בהם מופעלת באופן שוטף מערכת כריזה, ניתן לשלב בה הודעות קוליות על עצם הפעלת מצלמות המעקב במתחם. החובה להציב שלטי אזהרה מקבלת משנה חשיבות ותוקף כאשר קשה להבחין בקיומה של המצלמה (בשל מיקומה או צורתה).
37. בנוסף לחובת קבלת הסכמה מדעת מן האובייקטים המצולמים, מיועדת ההודעה על הצבת המצלמות למלא גם אחר דרישת השקיפות המוטלת בסעיף 11 לחוק על מי שאוסף מידע. הוראת סעיף 11 חלה גם במקרים בהם איסוף המידע החזותי במצלמות אינה מחייבת הסכמה אלא מבוצעת לפי הסמכה בחוק. מסיבה זו, יחד עם שלטי ההודעה באתר הצילום, טוב יעשה הגורם האחראי על הצבת מצלמות המעקב אם יפרסם גם רשימה מרוכזת של מקומות התקנתן באתר האינטרנט שלו; בפרסום המרוכז הנ"ל, ניתן לפרט בהרחבה את מטרות הצבת המצלמה, השימוש בצילומים, הגורמים להם עשויים הצילומים להימסר, משך הזמן בו ישמרו הצילומים ופרטי התקשרות לצורך מימוש זכות העיון בהקלטות לפי סעיף 13 לחוק.



38. שלט האזהרה חייב להיות קריא וברור, לרבות מבחינת גודלו, ועליו לכלול את הפרטים הבאים:
- 38.1. ציור של מצלמה, או סמל גרפי מקובל אחר המעביר בצורה ברורה את המסר שהאתר מצולם (רצוי לקבוע סימול אחיד);
- 38.2. שמו של הארגון האחראי על הצבת המצלמה²⁵;
- 38.3. תיאור תמציתי של מטרת הצבת המצלמה, למשל: "בטיחות", "מניעת עבירות", "בקרת תחבורה";
- 38.4. כתובת אתר האינטרנט בו מצויה רשימת המצלמות ומדיניות השימוש בהן (כמפורט בסעיף 32 לעיל), או מספר טלפון וכתובת דוא"ל למענה על שאלות בנוגע לשימוש במצלמה.

אופן ומשך שמירת הצילומים ומחיקתם – זכות העיון של המצולם

39. אסור לשמור את הקלטות הצילומים למשך זמן ארוך יותר ממשך הזמן הנחוץ במישרין לצורך הגשמת מטרת התקנת המצלמה. שמירת הצילומים לאחר שהם אינם נחוצים עוד - הינה הפרה של עקרון הגבלת המטרה²⁶ ויוצרת סיכוני אבטחת מידע מיותרים, ומשום כך גם פוגעת בזכות החוקתית לפרטיות במידה העולה על הנדרש.
40. לפיכך בראש ובראשונה על מפעיל המערכת לבחון בקפידה האם מטרת התקנת המצלמות אכן מחייבת בכלל להקליט את הצילומים, או שמא אין סיבה שלא להסתפק בצילום חי בלבד. הקלטה שאינה נחוצה להגשמת המטרה אינה עומדת במבחני המידתיות. אם מסתבר שקיים צורך להקליט, על מפעיל המצלמה לקבוע את משך השמירה בהתאם לשיקולים המפורטים להלן.
41. משך שמירת ההקלטות תלוי במטרה של התקנת כל מצלמה ומצלמה באופן ספציפי, וברגישות המידע הנקלט בעדשתה, ולכן קשה לקבוע מסמרות בדבר פרק הזמן המדויק בו מוצדק לשומרן. משך שמירת הצילומים יקבע בכל מקרה בנפרד לפי מבחני המידתיות. עם זאת בהכללה ניתן לומר שבמצלמות מעקב המותקנות במרחב הציבורי למטרת מניעת עבריינות, כדוגמת המצלמות המוצבות בערים בארץ במסגרת תכנית "עיר ללא אלימות", קשה להצדיק שמירת מידע למשך למעלה משבוע ימים; את תקופת שמירת ההקלטות במצלמות מסוג זה אפשר להאריך אם במהלך אותה תקופה מתקיימת באזור המצולם

²⁵ "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.

²⁶ הקבוע בסעיפים 2(9) ו-8(ב) לחוק הגנת הפרטיות, והפרתו היא עבירה על סעיפים 5 ו-31 לחוק.



התרחשות המעלה אפשרות ממשית שיהיה צורך לגיטימי לשימוש בצילומים, או אם נפתחת חקירה רשמית שלצרכיה ההקלטות עשויות להיות רלבנטיות. מובן כי מיד כשמסתיים הצורך להאריך את תקופת השמירה – יש למחוק את ההקלטות כפי שצריך היה לעשות מלכתחילה. 42. כדי למנוע תקלות מומלץ לתכנן את מערכת ההקלטה מראש לפי עקרון "הפרטיות באמצעות תכנון" (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.

43. סעיף 13 לחוק הגנת הפרטיות מקנה לכל אדם את הזכות לעיין במידע המוחזק אודותיו במאגר מידע. זכות זו חלה גם על מאגר המידע הכולל הקלטות צילומי מערכת המעקב. מובן שהחובה לאפשר עיון במידע תקפה רק כל עוד המידע נשמר במערכת – ולכן גם זה שיקול בו צריך מפעיל המצלמה להתחשב בבואו לקבוע את משך זמן שמירת הצילומים.

44. אופן מתן זכות העיון במידע מוסדר בסעיף 13 לחוק הגנת הפרטיות ובתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-1981, אולם ראוי להעיר מספר הערות ביחס לעיון בצילומים במצלמות המעקב:

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

44.2. כיוון שעל פי רוב בשלב הראשון, האנשים המצולמים לא יהיו מזוהים ושלא ניתן יהיה לערוך בהקלטות חיפוש ממוחשב לפי שם – על הבקשה לעיון במאגר להיות קונקרטי 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;

44.3. מתן זכות עיון בצילומים לפלוני – עלול לפגוע בפרטיות של אנשים אחרים, שכן המידע אודותם הוא מידע עודף לעניין זכות העיון של המבקש. לכן כאשר בצילום בו מבקשים 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 במשרדי מפעיל המצלמה אך להימנע מלמסור לו העתק שלה;²⁷

²⁷ 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, ובג"צ 7256/95 פישלר נ' מפכ"ל המשטרה, ישנה אמנם עדיפות לקיים את



44.4. צמצום הפגיעה בפרטיות של צדדים שלישיים בעת מתן זכות העיון במאגר הצילומים, הוא עוד נימוק לצמצום מראש את זווית הצילום ואת האזור המצולם.

אבטחת מידע והגבלת השימוש בו

45. המערכת המקליטה ואוגרת צילומים ממצלמות המעקב היא מאגר של מידע רגיש. סעיף 17 לחוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על הארגון שיזם את התקנת המצלמה ואחראי להפעלתה²⁸, על ארגון שיש לו גישה למאגר הצילומים ורשות להשתמש בהם²⁹, ועל נושאי המשרה שהופקדו על ניהול המאגר בארגונים אלה³⁰. אבטחת מידע מוגדרת בסעיף 7 לחוק כהגנה על שלמות המידע ומניעת חשיפתו העתקו או שימוש בו ללא רשות כדין.

46. על הגורמים האחראים לאבטחת המידע מוטל לנקוט בכל האמצעים הדרושים להשגת רמה נאותה שלה לפי דרישות הדין והרגולציה המעודכנים למועד הרלבנטי³¹. המינימום הנדרש הוא נקיטת אמצעי האבטחה המפורטים בסעיף 3 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו – 1986. באופן כללי אבטחת המידע במערכת מצלמות מעקב המופעלת בידי גוף פרטי או ציבורי כאחד, מחייבת:

46.1. קיום הגנה פיזית ולוגית על המערכת;

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

46.3. קביעת רשימת מורשי גישה, והטלות מגבלות על גישתם למידע;

46.4. 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;

46.5. מפעיל מערכת המצלמות צריך לנקוט משנה זהירות אם הוא נעזר בשירותי מיקור חוץ; קצרה היריעה מלפרט כאן את מלוא האמצעים הנוספים שעל מפעיל

זכות העיון באמצעות מסירת "תדפיס" – אולם במקרה שלפנינו זכותם החוקתית לפרטיות של האנשים האחרים המופיעים בצילום עשויה להטות את הכף לכיוון עיון באמצעות מצג דווקא.

²⁸ מי שנהוג לכנותו "בעל המאגר".

²⁹ "מחזיק" במאגר בלשון סעיף 3 לחוק הגנת הפרטיות.

³⁰ "מנהל מאגר" בלשון סעיף 7 לחוק הגנת הפרטיות.

³¹ בנוסף על התקנות התקפות הנוגעות לגופים ציבוריים, פרסמה הרשות ביום 10.1.2010 טיוטת תקנות מפורטות בעניין אבטחת מידע בגופים ציבוריים ופרטיים כאחד. גם בטרם כניסת התקנות החדשות לתוקף, ניתן להיעזר בהן כדוגמא לפרקטיקה ראויה.

<http://www.justice.gov.il/MOJHeb/ILITA/News/niyar+emda+takanot+avtachat+meida+lepratiyut.htm>



המצלמה ליישם³², אולם בתמצית עליו להקפיד בבחירת קבלן אמין, לכלול בחוזה עימו הוראות בדבר אבטחת מידע והגנה על המידע ולוודא שהקבלן מבצע בפועל את הוראות החוזה בנושאים אלה; להסיר ספק יודגש השימוש בקבלנים אינו מסיר את האחריות ממפעיל מצלמות המעקב;

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

46.7. יש לבחון את יישומם של אמצעים משפרי פרטיות (privacy enhancing technologies) לצורך מניעה של שימוש לא ראוי במידע³³.

47. 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; צפיה בצילומים המוקלטים; הרשאה להעתיק את ההקלטות; הרשאה לשליטה במערכות הזום והכוונן של המצלמה; יכולת מחיקה או עריכה של הצילומים. אם מפעיל המצלמה נעזר בשירותי מיקור חוץ, יש להקפיד על כך שהפעולות הרגישות יותר כגון העתקת הצילומים, מחיקתם או עריכתם לא תימסר לעובדי הקבלן אלא תעשה בידי מזמין העבודה עצמו.

48. 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.

³² 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; עד שתפורסם הנחיית היועץ, טוב יעשו מפעילי המצלמות אם בהוצאת עבודות למיקור חוץ - יפעלו לפי סעיף 14 לטיוטת תקנות האבטחה שפרסמה הרשות כמפורט בה"ש 26 לעיל.

³³ בין אמצעים אלה ניתן למנות:

- אמצעים לאנונימיזציה של המידע המצולם (data anonymization);
- אמצעים להצפנה של המידע המצולם (data encryption);
- אמצעים למזעור המידע המצולם (data minimization);
- אמצעים ליידוא זהותם של משתמשים במידע המצולם (identity systems);
- אמצעים להגבלת השימוש במידע המצולם על ידם (digital rights management);
- אמצעים למעקב וניטור אחר השימוש במידע המצולם.



49. יובהר שוב כי 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 אבטחה לפרסום באמצעי התקשורת, אלא במקרים קונקרטיים שבהם יש נימוקים מיוחדים ויוצאי דופן לכך – כגון איתור של עבריין.

סיכום

50. על הצבתן של מצלמות מעקב ועל השימוש בהן, חלות מגבלות הנובעות מן הפגיעה בפרטיות הגלומה בפעולתן. במקרים בהם אוסף הצילומים הנוצר עקב השימוש במצלמות מעקב הוא "מאגר מידע" כמשמעותו בסעיף 7 לחוק הגנת הפרטיות, חלות על הצילומים גם הוראות פרק ב' לחוק.

51. העקרונות המפורטים במסמך זה מיועדים לשמש כהנחיות ראשוניות ובסיסיות להפעלת מערך מצלמות המעקב והאבטחה ולשימוש בצילומים הנקלטים בהן, עד אשר יגובש הסדר ממצה ומקיף בסוגיה.

52. הפרת הוראות חוק הגנת הפרטיות הנוגעות להפעלת מצלמות מעקב המפורטות במסמך זה, עלולה להגיע כדי עבירה פלילית לפי סעיפים 5, 16 ו- 31 לחוק.

ניר גרסון, עו"ד
ממונה משפט וטכנולוגיה