



17 במאי 2023
כ"ו באייר, התשפ"ג

היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק

תקציר מנהלים

בשנים האחרונות עברו ארגונים רבים למתכונת מלאה או חלקית של עבודה מרחוק. כתוצאה מכך חלה עלייה בשימוש ארגונים באמצעים טכנולוגיים למעקב אחר עובדיהם המבצעים את עבודתם מחוץ למקום העבודה.

במובחן ממעקב אחר עובדים במקום העבודה, מעקב במתכונת של עבודה מרחוק מתקיים, על-פי רוב, בביתו של אדם, קרי במרחב הפרטי והאינטימי ביותר שלו. מעקב שכזה "מכניס" את המעסיק לביתו של העובד, ומשכך מציב אתגר ממשי בכל הנוגע להגנה על פרטיותם של העובדים ובני ביתם ומשפחתם, לרבות קטינים.

הסיכונים לפרטיות במסגרת שימוש באמצעים טכנולוגיים למעקב בעבודה מרחוק הם רבים ומגוונים. סיכונים אלו כוללים איסוף מידע ללא הסכמת העובד; משטור ופגיעה בתחושת השליטה של העובד על פרטיותו; איסוף וחשיפה של מידע רגיש ועודף; דלף מידע; ושימוש לרעה במידע אישי.

במסמך זה סוקרת הרשות להגנת הפרטיות לראשונה באופן מקיף את נושא המעקב אחר עובדים בעבודה מרחוק, את הסיכונים המרכזיים לפרטיות במעקב שכזה, וכן את הוראות הדין הרלוונטיות. על יסוד כל האמור מציגה הרשות את עמדתה המשפטית והמקצועית בנושא, ואת הנחיותיה והמלצותיה למעסיקים.

להלן עיקרי עמדת הרשות:

- ככלל, דיני הגנת הפרטיות מאפשרים למעסיקים, תחת מגבלות, להשתמש באמצעים טכנולוגיים למעקב אחר עובדים בעת עבודה מרחוק.
- עם זאת, שימוש כאמור חייב להיעשות באופן סביר ומידתי, לצורך מטרה לגיטימית, וכן להיות בעל זיקה לאינטרסים הלגיטימיים של מקום העבודה. כמו כן, שימוש באמצעי מעקב צריך להיעשות תוך יידוע העובדים וקבלת הסכמתם לכך, ותוך הקפדה על כללי אבטחת המידע ועיקרון צמידות המטרה.
- בכל הנוגע לאמצעי מעקב שפגיעתם בפרטיות עשויה להיות גבוהה במיוחד (המפורטים בסעיף 9 למסמך) - שימוש באמצעים אלו עלול להביא לפגיעה חמורה בפרטיות, ועל כן הוא יכול להיעשות רק במקרים חריגים בהם קיימת תכלית מקצועית ספציפית המצדיקה זאת, ובכפוף לעמידה בדרישת המידתיות. כלל זה נכון ביתר שאת ביחס לשימוש בכל אמצעי לצילום העובד בסביבתו הביתית ולהאזנה לו.



- אמצעי מעקב שנבחר על-ידי מעסיק חייב להיות תואם לתכלית המעקב, וככלל אין לעשות שימוש במידע שנאסף לשם מטרה אחת, לצורכי מטרה אחרת. כמו כן, על מעסיקים לבחור את האמצעי שישומו יפגע בפרטיות העובדים במידה הפחותה ביותר האפשרית, מבין החלופות הרלוונטיות האפשריות.
- על מעסיק השוקל להשתמש באמצעים טכנולוגיים למעקב אחר עובדים בביתם להתחשב במידת הפגיעה בפרטיות העובדים ובני ביתם ומשפחתם. כמו כן, על המעסיק לפעול לכך שמידע אשר נאסף באופן אגבי על אודות בני ביתו של העובד (ואנשים אחרים שאינם רלוונטיים) לא יישמר במאגרי המידע שלו.
- לאור החשש לזליגת המעקב למרחב הפרטי-אנושי של העובד מחוץ לשעות העבודה, על מעסיק להימנע מלהשתמש באמצעי מעקב מעבר לשעות בהן מעמיד עצמו העובד לרשות המעסיק.
- על מעסיקים ליידע את עובדיהם על כך שהם עושים שימוש באמצעים טכנולוגיים למעקב אחר התנהלותם בעת עבודה מרחוק. יידוע זה צריך לכלול גם את המטרה שלשמה נעשה המעקב. בכל הנוגע לאמצעי מעקב שפגיעתם בפרטיות עובדים היא גבוהה במיוחד – מעסיקים אינם יכולים להסתפק ביידוע כללי, ועליהם לפרט בפני העובדים, בכתב ובשקיפות מלאה, על אופן ביצוע המעקב והשימוש במידע.
- הסכמת העובד היא קריטית. לכן, במצב בו לא ניתנה הסכמה של העובד, במפורש או מכללא, לכך שמידע אישי על אודותיו ייאסף לצרכי מעקב על עבודתו מרחוק, על מעסיקו להימנע מלאסוף עליו מידע אישי. עם זאת, בנסיבות בהן שימוש באמצעי מעקב מרחוק נעשה בהתאם לדרישות המידתיות והלגיטימיות המפורטות במסמך, רשאי מעסיק לדרוש מעובד כי ייתן הסכמתו לאיסוף המידע על אודותיו, וסירוב העובד לבקשה זו עלול להיות בעל השלכות מבחינת יחסי העבודה בין הצדדים.
- הסכמת העובד אינה יכולה 'להכשיר' שימוש בלתי מידתי באמצעי מעקב, או מעקב הנעשה למטרה שאינה מוגדרת, לגיטימית, ובעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה.
- על פי עיקרון צמצום המידע העודף, על מעסיקים להימנע, ככל הניתן, מאיסוף ושמירה של מידע על אודות עובדים שאינו הכרחי למטרת המעקב, או למטרת המאגר בו מידע זה נשמר. מעסיקים מחויבים לבחון, לפחות אחת לשנה, האם קיים צורך בהמשך שמירת מידע שכזה.
- מעסיקים רשאים לשמור מידע אישי על אודות עובדיהם הנאסף במסגרת מעקב אחריהם, אך ורק לתקופה התואמת את מטרת איסוף המידע ומטרת המאגר בו שמור המידע.



מבוא

1. בשנים האחרונות, וביתר שאת בתקופת ההתמודדות עם נגיף הקורונה, חלה עלייה במעבר ארגונים למתכונת של עבודה מרחוק, במסגרתה עובדים מבצעים את תפקידם באופן מקוון ומחוץ למקום העבודה, על-פי רוב כאשר הם בביתם.¹ לתופעה זו יתרונות רבים ומגוונים.
2. מצב זה, בשילוב ההתפתחות הטכנולוגית והרצון של מעסיקים לפקח על עובדיהם, מביא לשימוש מעסיקים באמצעים טכנולוגיים שונים ומתקדמים למעקב אחר התנהלות עובדים שנמצאים מחוץ למקום העבודה, ולרוב בביתם. לשימוש זה באמצעי מעקב השלכות משמעותיות על פרטיותם של עובדים.
3. מטרת המסמך היא להציב זרקור על תופעת המעקב של מעסיקים אחר עובדים במתכונת של עבודה מרחוק ועל הסיכונים לפרטיות הגלומים בה, לסקור את הרקע המשפטי הרלוונטי, להציג את פרשנות הרשות להוראות הדין והמלצות נוספות של הרשות בעניין זה.²
4. המסמך מיועד בעיקרו לארגונים במגזר הפרטי והציבורי אשר מעסיקים עובדים במתכונת, מלאה או חלקית, של עבודה מרחוק.³ המסמך מסתמך, בין היתר, על הנחיית הרשות להגנת הפרטיות בנושא 'שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה', ומפרש הנחיות אלו בהקשר של עבודה מרחוק.⁴
5. יובהר כי מסמך זה עוסק באמצעים טכנולוגיים העלולים להיות בשימוש מעסיקים לצרכי מעקב אחר עובדיהם בעת עבודה מרחוק. הוא אינו עוסק באמצעים טכנולוגיים שהשימוש בהם נדרש כחלק אינהרנטי מביצוע העבודה, אם מרחוק ואם במקום העבודה. עוד יובהר כי המסמך אינו מבקש להגביל או לצמצם את תופעת העבודה מרחוק, אלא להבטיח כי מתכונת עבודה זו תיושם תוך מתן התייחסות הולמת לפרטיותם של עובדים.

מעקב אחר עובדים במתכונת של עבודה מרחוק – רקע

6. מטבע הדברים, יכולתו של מעסיק לפקח על התנהלות עובדיו שעה שהם עובדים מחוץ למקום העבודה היא מוגבלת. במובן זה, מתכונת של עבודה מרחוק מציבה אתגר בפני ארגונים.

¹ לפי ד"ר נטלי שפר, המתבססת על סקר "גאלופ" מחודש אוקטובר 2020, כ- 55% מכלל העובדים עברו למתכונת של עבודה מרחוק, באופן מלא או חלקי. שפר מציינת בעניין זה כי "למעשה, כיום כלל משימות העבודה בארגונים מתבצעות מרחוק, החל מראיונות עבודה, דרך ישיבות שבועיות, וכלה בהערכות עובדים". ראו: [נטלי שפר "עבודה מרחוק ניהול מקרב: אתגרים והמלצות בעבודה מרחוק" חידושים בניהול 9, 20 \(2021\)](#).

² המסמך אינו עוסק בהקשרים של אבטחת מידע ארגוני והגנה מפני תקיפות סייבר במתכונת של עבודה מרחוק. להרחבה בנושאים אלה ראו: [הרשות להגנת הפרטיות "דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית" \(24.3.20\)](#); [מערך הסייבר הלאומי "המלצות הגנה לארגונים ועסקים לעבודה מהבית בעקבות התפשטות נגיף הקורונה" \(11.3.20\)](#).

³ הכוונה היא למצבים בהם העבודה מרחוק מהווה תחליף זמני או קבוע לעבודה במקום העבודה, ולא למעקב אחר עובדים שתפקידם דורש, מעצם מהותו ובמצב העניינים הרגיל, לקיים מתכונת של עבודה מחוץ למקום העבודה (כגון נהגים, שליחים, סוכני מכירות). להרחבה בעניין מעקב אחר מיקום עובדים שכאלו ראו טיוטת גילוי דעת מטעם [הרשות להגנת הפרטיות בנושא "איסוף נתוני מיקום של עובדים באמצעות אפליקציות ייעודיות ומערכות איכון ברכב"](#).

⁴ הנחיית רשם מאגרי מידע מסי' 5/17 "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה".



7. על מעסיקים מוטלת למעשה חובה חוקית לפקח על שעות העבודה של עובדיהם, וחובה זו חלה מטבע הדברים גם במתכונת של עבודה מרחוק.⁵ לשם כך, מעסיקים עשויים להשתמש באמצעים לדיווח נוכחות מקוון, המאפשרים לעובד לדווח מרחוק על שעות עבודתו. אמצעים אלו עשויים, בין היתר, לאפשר זיהוי ביומטרי של העובד על בסיס טביעת האצבע שלו או באמצעות מערכות לזיהוי פנים (Facial Recognition).⁶
8. כמו כן, קיימים כיום אמצעים טכנולוגיים שונים ומגוונים המאפשרים למעסיקים לקיים מעקב אחר התנהלות עובדיהם שעה שאלו נמצאים מחוץ למקום העבודה, לרבות בביתם. הטכנולוגיה מאפשרת ניטור מרחוק אחר כלל התנהלותו של אדם, לרבות לצורך בחינת הפרודוקטיביות של העובד, אופן התנהלותו, ושעות עבודתו בפועל. עם זאת, שימוש ברבים מאמצעים אלו עלול לחרוג בהרבה ממה שמתחייב או מותר על פי דין.
9. בין אמצעי המעקב האמורים, שפגיעתם בפרטיות גבוהה במיוחד ושהשימוש בהם יחרוג על-פי רוב במידה משמעותית מהנחוץ והמותר על פי דין, ניתן לציין את הכלים הבאים:⁷
- א. כלי סריקה ופיקוח על אתרי האינטרנט בהם גולש עובד,⁸ ועל תוכן הדואר האלקטרוני שלו (ככל שמדובר על תיבה שאינה לשימוש מקצועי בלבד);
- ב. אמצעים לשליטה על מצלמות הרשת ועל חיישנים לקליטת שמע (מיקרופון) שבמכשירים הדיגיטליים של העובד, לצילום העובד ולהאזנה לו ולסביבתו;
- ג. אמצעים לניטור תנועת העכבר ואופן השימוש של העובד במקלדת המחשב (מערכות לרישום הקשות - Keyloggers);
- ד. אמצעים לצילום מסך המחשב של העובד (Screenshots);⁹
- ה. אמצעים למעקב אחר תנועת עיניים (Eye Tracking) בעת שימוש העובד במחשב, לבחינת התכנים בהם הוא צופה בזמן היותו מול המחשב;¹⁰

⁵ מעסיקים חייבים לנהל רישום שוטף של שעות העבודה והמנוחה השבועית של העובדים. לעניין זה ראו סעיף 25 לחוק שעות עבודה ומנוחה, התשי"א-1951. במקרה של מחלוקת על המעסיק מוטל הנטל להוכיח שהעובד לא עמד לרשות העבודה במשך שעות העבודה השנויות במחלוקת. להרחבה ראו: [זרוע העבודה, "חובת רישום שעות עבודה ומנוחה שבועית" \(18.1.2021\)](#).

⁶ ביומטריה היא מונח המשמש לתיאור תכונה או תהליך. השימוש במידע ביומטרי הוא לצורך זיהוי אדם באמצעות מנועי השוואה ביומטריים, "על פי מה שהוא", ולא על פי המסמך או המידע שיש לגביו. הזיהוי מתבצע בשיטות אוטומטיות של זיהוי אדם בהתבסס על מאפיינים ביולוגיים (אנטומיים ופיזיולוגיים) והתנהגותיים, הניתנים למדידה. להרחבה ראו: [הרשות להגנת הפרטיות "זיהוי ביומטרי – שאלות ותשובות" \(27.10.2020\)](#).

⁷ הסקירה מבוססת, בין היתר, על פרסומים ברשת של חברות המציגות כלי ניטור ומעקב אחר עובדים. להרחבה ופירוט על חלק מהכלים המפורטים, ראו: [Drew Harwell, Managers turn to surveillance software, always-on webcams to ensure employees are \(really\) working from home, THE WASHINGTON POST \(Apr. 30, 2020\)](#); [Ryan Morris-Reade, VMware research shows employee surveillance could increase staff turnover, IT BRIEF \(Nov. 15, 2021\)](#).

⁸ למעט שימוש סביר ומידתי בכלי סריקה ופיקוח לצרכי אבטחת מידע והגנת סייבר בארגון.
⁹ לעניין זה ראו לדוגמה: [Lora Jones, 'I monitor my staff with software that takes screenshots', BBC NEWS \(Sep. 29, 2020\)](#).

¹⁰ להרחבה ראו: [Ian Taylor Logan, For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection, 123 PENN ST. L. REV. 779 \(2019\)](#).



1. אמצעים לאיסוף נתוני מיקום של עובד המותקנים במכשיריו הדיגיטליים או ברכבו.¹¹
10. מבחינה טכנולוגית, אמצעי מעקב מרחוק יכולים להיות מיושמים באופן סמוי, קרי מבלי שהעובד מודע לכך. אמצעים אלו יכולים להיות מופעלים באופן נקודתי או רציף ומתמשך. כמו כן, חלק מהאמצעים עלולים להיות מיושמים גם לאורך כל שעות היממה, קרי גם לאחר שעות העבודה.¹²

מעקב אחר עובדים במתכונת של עבודה מרחוק – סיכונים מרכזיים לפרטיות עובדים

11. לשימוש מעסיקים באמצעי מעקב אחר עובדיהם במתכונת של עבודה מרחוק עשויות להיות השלכות משמעותיות בכל הנוגע לפרטיות העובדים. מעצם טבעו, לעיתים שימוש שכזה כרוך באיסוף מידע אישי ורגיש על אודות העובדים ובני ביתם.
12. **במובחן ממעקב אחר עובדים במקום העבודה, מעקב במתכונת של עבודה מרחוק מתקיים, על-פי רוב, בביתו של אדם, קרי במרחב הפרטי והאינטימי ביותר שלו. במקרים רבים המעקב למעשה "מכניס" את המעסיק לביתו של העובד.** מעקב מסוג זה עשוי להוות חדירה של גורם חיצוני למרחב הפרטי-אנושי של אדם, באופן העמוק ביותר, ובמידה שלרוב אינה מתקיימת במסגרת של מעקב במקום העבודה.
13. להלן יפורטו הסיכונים המרכזיים לפרטיות עובדים המועסקים במתכונת של עבודה מרחוק:

א. איסוף ושמירת מידע אישי ללא הסכמה – כאמור, מבחינה טכנולוגית, מעקב אחר עובדים יכול להתבצע ללא ידיעתם או הסכמתם. **איסוף מידע אישי ושמירתו במאגר מידע, הנעשים ללא הסכמה, מהווים פגיעה בפרטיות, וזאת ללא קשר לשאלת אופן השימוש במידע זה, ואבטחתו.** נקודה זו נובעת מן השילוב בין סעיף 1 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות' או 'החוק') הקובע ש"לא יפגע אדם בפרטיות של זולתו ללא הסכמתו", לבין שורת המעשים והמחדלים אותם מגדיר סעיף 2 לחוק כפגיעה בפרטיות. כפי שציינה פרופ' גביזון, עצם איסוף המידע ללא הסכמה מהווה אובדן שליטה ופגיעה בכבוד.¹³

בית המשפט העליון, בהתייחסותו לסוגיית איכוני השב"כ בתקופת הקורונה, ציין בעניין זה כי: "הזכות לפרטיות כוללת בחובה לא רק הגנה מפני "גילוי" מידע הנוגע לאדם לצדדים שלישיים. ההגנה על זכות זו חייבת להתייחס גם לפעולות הקודמות לגילוי במישור הזמן – איסוף המידע. הטלת הגבלות על איסוף מידע הנוגע לאדם ועל אגירתו באופן אלקטרוני

¹¹ ככלל, עמדת הרשות היא כי מעסיק יהיה רשאי לעשות שימוש במערכת האוספת נתוני מיקום של עובד רק כאשר מדובר באיסוף נתונים לתכלית לגיטימית וחיונית למקום העבודה, העומדת בדרישת המידתיות. להרחבה ראו ה"ש 3. ¹² Adam Satariano, *How My Boss Monitors Me While I Work From Home*, THE NEW YORK TIMES (May 6, 2020).

¹³ גביזון טענה בעניין זה כי "אחת מהסכנות שבמאגרים שכאלה היא הידיעה שאתה – כל אחד מאיתנו, כל אחד מהאנשים – הוא מספר, הוא פרופיל, שכל אחד יכול להפעיל כפתור ולקבל אותו. הפגיעה הזאת היא פגיעה של כבוד. הפגיעה הזאת היא פגיעה של אבדן שליטה. הפגיעה הזאת היא פגיעה של היחס בין הפרט ופרטים אחרים לבין הממשלה או מחזיק המאגר". רות גביזון "הזכות לפרטיות" **זכויות האדם והאזרח בישראל** 305 (1992).



היא חלק אינטגרלי מהזכות לפרטיות אף כאשר הוא אצור במאגר המידע ואינו נחשף בפני כלל¹⁴.

חשוב לציין כי במערכת היחסים בין עובדים למעסיקים קיים גם חשש כי הסכמה הניתנת על-ידי עובד לפגיעה בפרטיותו אינה הסכמה הניתנת מתוך רצון חופשי. חשש זה נובע מפערי הכוחות הקיימים בין עובדים למעסיקים, ומכך שבמקרים רבים עובדים עלולים להניח כי סירובם לתת את הסכמתם ייתפס באופן שלילי על-ידי מעסיקהם, ויביא להגבלת קידומם או אף לפיטוריהם.¹⁵

סוגיית ההסכמה קשורה קשר הדוק לאלטרנטיבה העומדת בפני העובד. במצבים בהם אין לעובד ברירה אמיתית אלא לעבוד מרחוק (כגון בתקופת ההתמודדות עם נגיף הקורונה) קשה לראות בהסכמתו למעקב ככזו הניתנת מרצון חופשי. מנגד, במצב בו המעסיק מאפשר לעובד לבחור בין עבודה בביתו לבין עבודה במשרד, מבלי שלהחלטתו בנושא תהיה השפעה שלילית על המשך העסקתו או תנאי עבודתו – כך תגבר הנטייה לראות בהסכמת העובד, ככזו שניתנה מתוך רצון חופשי.

ב. איסוף וחשיפה של מידע רגיש – שימוש בכלים טכנולוגיים למעקב אחר עובדים שעה שהם עובדים מרחוק ובביתם (ובוודאי כאשר שימוש זה נעשה מעבר לשעות העבודה), עשוי להביא לאיסוף ולשמירה של מידע אישי ורגיש על אודות העובדים, שספק אם היה נאסף ונשמר במתכונת של עבודה "רגילה" במקום העבודה.

כך לדוגמה, בעת שימוש במצלמת הרשת או במיקרופון המותקנים במחשב הנייד או בטלפון החכם של העובד עלול מעסיק להיחשף לשיחות פרטיות שמקיים העובד עם אחרים (כגון בני משפחה או נותני שירותים) ולפעולות אחרות, העלולים לחשוף מידע רגיש על מצבו המשפחתי של העובד ומערכת היחסים שלו עם בני משפחתו, מצבו הכלכלי והבריאותי, וכן מידע הנוגע לצנעת חייו (כגון נטייתו המינית). מידע זה עלול לכלול גם נתונים על אודות בני ביתו של העובד (לרבות קטינים), וכן הלאה.

בנוסף, שימוש מעסיקים באמצעים לצילום מסך המחשב של העובד או לניטור אתרי האינטרנט בהם הוא גולש, עלול להביא לאיסוף ולשמירה של מידע רגיש הנובע מניטור זה, כגון מידע פיננסי, מידע רפואי או מידע אינטימי הנוגע לצנעת חייו של העובד.¹⁶

כמו כן, שימוש במערכות לניטור תנועת העיניים של העובד או באפליקציות לדיווח על נוכחות (המשתמשות בנתוני מיקום של עובדים או בנתונים ביומטריים) מביא, הלכה למעשה, לאיסוף ושמירה של מידע רגיש ביותר על אודות עובדים. בכל הנוגע למידע

¹⁴ בג"ץ 6732/20 האגודה לזכויות האזרח בישראל נ' הכנסת (פורסם בנבו, 1.3.2021), פסקה 12 לפסק דינה של השופטת ברק-ארז.

¹⁵ לאור כך, הסכמת עובדים לפגיעה בפרטיותם במסגרת יחסי עבודה נתפסת כהסכמה חשודה. להרחבה ראו מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה 253 (2010).

¹⁶ איסוף מידע שכזה עשוי להתרחש גם במסגרת מעקב במקום העבודה. עם זאת, ההנחה היא שעובד הנמצא בביתו עלול להרגיש בנוח יותר להיכנס לאתרים שהוא היה אולי נמנע מלהיכנס אליהם במקום העבודה.



ביומטרי, איסוף מידע שכזה טומן בחובו סיכונים משמעותיים לפרטיות. מכיוון שנתוני ביומטריה אינם ברי עדכון ותיקון, איסוף מידע שכזה יוצר סיכון בהקשר לחשיפת זהותו של אדם ויכולת ההתחזות אליו.

בנוסף, במקרים בהם עושה העובד שימוש במחשב האישי שלו כדי לייצר גישה למערכות התפעוליות של הארגון בו הוא מועסק, ייתכן כי מחשב זה משמש גם את בני הבית האחרים, אשר כלל אינם מודעים לתוכנות ולפונקציות הניטור המופעלות עליו. כאשר בפועל, בעת שהם עושים במחשב ביתי זה שימוש אישי, פעילותם מנוטרת ומתועדת.

ג. **איסוף ושמירת מידע עודף** – בהמשך לאמור בנקודה הקודמת, **ניטור התנהלות עובדים בביתם עלול להביא לאיסוף ולשמירה של מידע עליהם ועל אודות אחרים (לרבות מידע רגיש) אשר כלל אינו נדרש ואינו רלוונטי למטרת הפיקוח על משימותיו של העובד**. מידע שכזה מהווה מידע עודף, שאיסוף ושמירתו עלולים, בנסיבות מסוימות, להוות פגיעה בפרטיות.

ככלל, מידע כגון נתונים בדבר מצבו הכלכלי או המשפחתי של עובד, או מידע הנוגע לצנעת חייו (כגון נטייתו המינית) – אינם רלוונטיים למעסיקים המבקשים לפקח על עבודת עובדיהם מרחוק, ומשכך הם מהווים מידע עודף. איסוף ושמירה של מידע שכזה עלולים, בנסיבות מסוימות, להוות פגיעה בפרטיות.

ד. **דלף וזליגת מידע** – שימוש בכלים למעקב אחר התנהלות עובדים, הנעשה באופן שאינו מאובטח דיו, עלול להביא גם ל**זליגתו של מידע רגיש** הנאסף במסגרת ניטור זה.

מצב שכזה עלול להתרחש, לדוגמה, כתוצאה מפריצה לרשת האינטרנט הביתית של העובד (במיוחד אם מדובר ברשת אלחוטית, Wi-Fi), שאינה מאובטחת דיה), או כתוצאה מפריצה לאמצעי המעקב או למאגרי המידע של הגורמים המספקים את אמצעי המעקב למעסיקים, והמתפעלים אותם. זליגת מידע עלולה להתרחש גם כתוצאה מכשלי אבטחת מידע וכשלים אנושיים מצד המעסיקים והחברות המספקות את אמצעי המעקב.¹⁷

לאור כך שניטור התנהלותו של עובד שעה שהוא נמצא בביתו עלול להביא לאיסוף מידע רגיש ביותר, מובן כי זליגת מידע שכזה וחשיפתו ברבים עלולה להביא לפגיעה קשה בפרטיות. חשוב להדגיש כי בכל הנוגע למידע ביומטרי, זליגת מידע שכזה עלולה להביא לתוצאות קשות במיוחד, כגון התחזות לאדם במסגרת שימוש במערכות למשיכת כספים, קבלת גישה לטלפון הנייד שלו וכן הלאה.

ה. **שימוש לרעה במידע** – איסוף ושמירת מידע רגיש על אודות עובדים על ידי מעסיקיהם מעלה את החשש לשימוש לרעה במידע במסגרת יחסי העבודה. **מעסיקים עלולים**

¹⁷ ככלל, הסיכון לדלף וזליגת מידע גובר כאשר אמצעי המעקב מותקן במכשירים פרטיים של עובדים, במובחן ממכשירים מוסדיים, שעל פני הדברים אמורים להיות בעלי רמת אבטחה גבוהה יותר.



להשתמש באמצעי המעקב שברשותם לאיסוף מידע רגיש על אודות עובדיהם, גם לשם השגת מטרות שאינן לגיטימיות.

כך לדוגמה, מעסיק עלול להשתמש במידע אישי שאסף ממערכות העובד כדי ללמוד על מצבו הרפואי (כגון אם עובדת מצויה בשלבים ראשוניים של הריון), או לבדוק האם עובד עוסק בחיפוש אחר מקום עבודה אחר. דוגמה אחרת עשויה להיות הפליית עובד על-ידי מעסיקו על יסוד עמדה פוליטית שלו שנחשפה במסגרת הקלטת דברים שהוא אמר בביתו במסגרת שיח שניהל עם בני משפחתו.

1. משטור ופגיעה בתחושת השליטה של אדם – מעקב וניטור רציף של עובדים על-ידי מעסיקיהם – החל מצילום העובד וחלקים מהמרחב הביתי שלו, דרך האזנה והקלטה של המתרחש בסביבת העבודה הביתית שלו לאורך שעות היום, וכלה במעקב אחר תנועת עינו כשהוא יושב מול המחשב - עלול להביא לפגיעה בפרטיות, בעוצמה המתבטאת בפגיעה בתחושת השליטה של עובד על חייו.¹⁸ לפגיעה זו עלולות להיות השלכות קשות. פרופ' בירנהק טען בעניין זה:

"הצורך בפרטיות במקום העבודה מיתרגם בפועל לצורך בזמן פנוי, כלומר הפסקה במהלך העבודה, לאפשרות לעסוק גם בעניינים שלא קשורים בעבודה, ובצורך שלא להיות נתון לתצפיות ויזואליות או אלקטרוניות. [...] העובד אינו יודע אם הוא נצפה בכל רגע נתון או לא, אבל יודע שהאפשרות קיימת. כאשר אנו מרגישים נתונים במעקב, אנו מתנהגים אחרת, ו"מצנזרים" את התנהגותנו. העין הבוחנת והעוקבת [...] גורמת לנו לתחושת אובדן שליטה בעצמנו: מישהו אחר, לא ידוע, מושך בחוטים שאליהם אנו קשורים, ושולט בגורלנו. במובן זה תחושת המעקב איננה רק תלונה כללית, אלא יש לה מחיר רפואי של ממש, של חרדות, דיכאון ..."¹⁹

משטור עובדים, כמתואר לעיל, עלול להביא למצב בו עובדים העובדים מביתם ימנעו מלבצע פעולות לגיטימיות, כגון לצאת להפסקת שתייה במטבח או ללכת לנוחיות, וזאת מחשש שברגעים אלו תופעל מערכת המעקב (לדוגמה באמצעות שימוש במצלמת המחשב), ומעסיקיהם יסיקו מכך שהם אינם מבצעים את עבודתם כנדרש.

14. עד כאן סקירת הסיכונים המרכזיים לפרטיות הקיימים בהקשר של מעקב מעסיקים אחר עובדיהם המועסקים במתכונת, מלאה או חלקית, של עבודה מרחוק. **אמנם, סיכונים אלו קיימים במידה מסוימת גם במתכונת של עבודה "רגילה" במקום העבודה. עם זאת, נראה כי**

¹⁸ היועץ המשפטי לממשלה עמד על סיכון זה בעמדה שהגיש בסעי' (ת"א-יפו) 45564-12-17 גליה כהן נ' אל על נתיבי אויר לישראל בע"מ (פורסם בנבו, 27.7.2022), (להלן: "עניין כהן"): "למצלמות יש כוח ממשטר העלול לכרסם מתחושת הכבוד והאוטונומיה שיש לעובד כאדם ... כאשר העובדים מרגישים כי הם נתונים למעקב, הם מתנהגים באופן שונה ומצנזרים את התנהגותם, דבר היוצר תחושה של חוסר שליטה" (פסי 49-50 לעמדת היועץ המשפטי לממשלה).
¹⁹ מיכאל בירנהק "מעקב בעבודה: טיילור, בנתיחהם והזכות לפרטיות" **עבודה, חברה ומשפט** יב 8, 34 (2008). ראו גם טל גולן "העין הבוחנת והצופה: הסדרה ומשטור של התנהגות עובדים במקום העבודה" **משפט, חברה ותרבות - מסדירים רגולציה: משפט ומדיניות**, 515 (2016).



מתכונת של עבודה מרחוק מקצינה את הסיכונים האמורים, לאור הצורך הגובר של מעסיקים לפקח על עובדים במתכונת העסקה שכזו, ולאור כך שמתכונת זו "מכניסה" את המעסיק אל תוך ביתו של העובד, על כל המשתמע מכך.

ניתוח אמצעי מעקב בראי מידת הפגיעה בפרטיות עובדים

15. לאור כל שפורט עד כה ניתן לחלק את אמצעי המעקב והפיקוח בעבודה מרחוק לשלוש קבוצות, וזאת על יסוד מידת הפגיעה האפשרית שלהם בפרטיות עובדים:²⁰

א. **אמצעים שאינם פוגעים בפרטיות עובדים** - אמצעים טכנולוגיים שנועדו להגבלת התנהלות עובדים בזמן עבודתם מרחוק אך שאינם כרוכים כלל באיסוף מידע על אודותיהם, כגון טכנולוגיות לחסימת גישה של עובדים לאתרי אינטרנט מסוימים או להגבלת יכולתם להוריד תוכנות (אפליקציות) למכשיריהם הניידים, וכן הלאה.

ב. **אמצעים שפגיעתם בפרטיות עובדים היא מועטה** - אמצעים שכרוכים באיסוף מידע שאינו אישי על התנהלות העובד, כגון אמצעים לניטור השימוש במערכות התפעוליות של הארגון, שבמסגרתם עלול להיאסף גם מידע אישי מסוים על אודות עובד.

ג. **אמצעים שפגיעתם בפרטיות עובדים היא גבוהה במיוחד** - אמצעים שיישומם כרוך במהותו באיסוף מידע אישי ורגיש על אודות עובדים, המהווים, במידה רבה, גם אמצעים למשטור העובד. תחת קבוצה זו ניתן לציין את האמצעים שפורטו בסעיף 9 למסמך זה, לרבות אמצעים למעקב אחר עובדים באמצעות מידע ביומטרי (זיהוי פנים, תנועת עיניים), אמצעים לאיסוף נתוני המיקום של העובד, ניטור רציף של התנהלות העובד במכשיריו (לרבות צילום מסך המחשב של העובד ומעקב אחר שימוש בעכבר ובמקלדת); ואמצעים לצילום העובד או להאזנה לסביבת העבודה שלו.²¹ ניטור וחדירה לתוכן אישי מתוך תיבות הדואר האלקטרוני של העובד (בין אם מדובר בתיבה מקצועית, אישית או מעורבת) מהווים גם הם אמצעי שפגיעתו בפרטיות העובד היא ברמה גבוהה במיוחד.

מעקב מעסיקים אחר עובדים – רקע משפטי

חוק הגנת הפרטיות

16. הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו אינן מעניקות התייחסות מיוחדת לסוגיית המעקב של מעסיקים אחר עובדיהם, ככלל או במתכונת של עבודה מרחוק בפרט. עם זאת, מספר מצבים המוגדרים בחוק כפגיעה בפרטיות, שהחוק אוסר עליה בהעדר הסכמה, עשויים להיות רלוונטיים לסוגיית המעקב של מעסיקים אחר עובדיהם.

²⁰ חלק מהאמצעים המפורטים עשויים להיות בשימוש מעסיקים גם במסגרת מעקב אחר עובדים במקום העבודה. עם זאת, ככלל, עמדת הרשות היא כי שימוש באמצעים אלו במסגרת עבודה מרחוק עלול להביא לפגיעה קשה יותר בפרטיות העובד, וזאת בשל החדירה למרחב האישי והמשפחתי במקום מגוריו של העובד.

²¹ אמצעים לצילום ולהאזנה יכולים להיות בשימוש נקודתי וזמני או בשימוש רציף ומתמשך. מטבע הדברים, ככל שהיקף השימוש ורציפותו יהיו נרחבים יותר – כך מידת הפגיעה בפרטיות העובד תהיה משמעותית יותר.



17. כך למשל, החוק קובע כי בילוש או התחקות אחרי אדם העלולים להטרידו (סעיף 12(1)), האזנה לאדם שלא מתוקף חוק (סעיף 22(2)), וכן צילום אדם שהוא ברשות היחיד (סעיף 2(3)), הנעשים ללא הסכמה, מהווים פגיעה בפרטיות. בנוסף, על-פי סעיפים 2(9) ו-8(ב) לחוק, שימוש ללא הסכמה במידע למטרה אחרת מזו שלשמה הוא נאסף או שלא למטרת המאגר בו הוא שמור, מהווה גם הוא פגיעה בפרטיות.²²

18. כפי שיפורט, חובות נוספות הקבועות בחוק (כגון חובת היידוע - סעיף 11 לחוק), וכן זכויות מסוימות העומדות על-פי החוק לנושאי מידע, כגון זכות העיון במידע (סעיף 13) ותיקונו (סעיף 14), עשויות גם הן להיות רלוונטיות בהקשר של מעקב מעסיקים אחר עובדיהם, לרבות במתכונת של עבודה מרחוק.

פיקוח מעסיקים על עובדים בראי החוק והפסיקה

19. למעסיק פררוגטיבה ניהולית הנגזרת מזכות הקניין לנהל את עסקו ומכוחה הוא רשאי להחליט על שימוש באמצעים טכנולוגיים במקום העבודה, כדי להגן על אינטרסים לגיטימיים של עסקו, ובכלל זה אבטחה ופיקוח על העובדים.²³ בהקשר זה יצוין כי בהתאם להלכה הפסוקה פיקוח מסוים של מעסיק על עובדיו הוא חלק אינהרנטי מחוזה העבודה ולגביו רואים את העובדים כמסכימים מכללא. מעבר לכך, מעסיק אף מחויב מכוח הוראות בחקיקה לפקח על שעות העבודה של העובדים, בין היתר לצורך תשלום שכרו. לעניין זה ראו סעיף 25 לחוק שעות עבודה ומנוחה, התשי"א-1951 שקובע חובת ניהול פנקס שעות עבודה, וסעיף 24 לחוק הגנת השכר, התשי"ח-1958 והתוספת לחוק הקובעים חובה לפרט בתלוש השכר פרטים לגבי ימי העבודה ושעות העבודה בפועל.

20. עם זאת, בהתאם להלכה הפסוקה, הפררוגטיבה הניהולית ואופן הפעלתה כפופים לדרישות הסבירות, המידתיות, תום הלב וההגינות.²⁴ לעניין הפגיעה בפרטיות, בעניין **איסקוב**²⁵ ו**קלנסווה**²⁶ נקבע כי מכוח זכות הקניין הנתונה למעסיק והפררוגטיבה הניהולית הנגזרת ממנה, רשאי מעסיק לפקח על פעילות העובדים במטרה לוודא שלא יעשו שימוש בלתי מורשה או בלתי חוקי בכלי העבודה הווירטואלי המופקד בידם, ורשאי הוא לקבוע את טכנולוגיות המעקב על פעולות העובדים במקום העבודה. כל זאת בכפוף לעקרונות תום לב, גילוי, שקיפות, לגיטימיות, מדתיות וצמידות למטרה. כמו כן, הפסיקה מבחינה בין אמצעי פיקוח שונים במקום העבודה, הפוגעים במידה שונה בפרטיות העובד ובהתאם לכך ולנסיבותיו של כל מקרה, משתנה גם צורת

²² סעיפים אלו מבטאים את עיקרון צמידות המטרה.

²³ אינטרסים לגיטימיים יכולים לנבוע מסיבות שונות. כך לדוגמה, מעקב אחר נהיגת עובדים ברכבים ממשלתיים יכול לנבוע לא רק מהצורך לעקוב אחר מיקום העובדים ואופן ביצוע עבודתם, אלא גם מהרצון להביא לצמצום תאונות דרכים ופגיעה בציבור העלולה להיגרם מתוך כך. אינטרס מסוג אחר למעקב אחר התנהלות עובדים ברשת עשוי לנבוע מצרכי אבטחת מידע של הארגון.

²⁴ ראו דב"ע (ארצי) נד/4-1 ההסתדרות הכללית של העובדים בא"י – התעשייה האווירית לישראל בע"מ, פד"ע כט 601 (1996) (להלן: 'עניין רמת'א'), בעמ' 635.

²⁵ ע"ע (ארצי) 90/08 **טלי איסקוב ענבר נ' מדינת ישראל - הממונה על חוק עבודת נשים** (פורסם בנבו, 8.2.2011) (להלן: 'עניין איסקוב').

²⁶ ע"ע (ארצי) 7541-04-14 **הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי - עיריית קלנסווה** (פורסם בנבו, 15.3.2017) (להלן: 'עניין קלנסווה').



ההסכמה הנדרשת מהעובד לשימוש המעסיק באמצעים השונים באיזוניה למול זכויות המעסיק.

21. פיקוח על עובדים רלבנטי גם כאשר עבודת העובד נעשית מחוץ לחצרי המעסיק, על מנת לפקח על העבודה וכן לצורך תשלום שכרו של העובד עבור השעות בהן עבד והעמיד עצמו לרשות המעסיק, ובכלל זה היכולת לדעת האם העובד זכאי לתשלום בגין שעות נוספות.²⁷ במקרה של עבודה מרחוק, הצורך האמור גובר אף ביתר שאת נוכח שהות העובד באופן ממושך מחוץ לחצרי המעסיק, במקרים רבים במרחב הפרטי של העובד. על כן, ביתר שאת גובר הצורך באיזונים בין הצורך של המעסיק בפיקוח אחר עבודת העובד במסגרת הפררוגטיבה הניהולית שלו מצד אחד, לבין האתגרים והחשש לפגיעה מוגברת בפרטיות בנסיבות אלה מצד שני.

הנחיות הרשות להגנת הפרטיות

22. הנחיית הרשות להגנת הפרטיות בנושא 'שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה' מפרטת את עמדת הרשות בנושא שימוש מעסיקים במצלמות למעקב אחר עובדים במקום העבודה. ההנחיה מנתחת את העקרונות שנקבעו בעניין **איסקוב**, ומבהירה כי ההסדר הספציפי שנקבע שם בנושא מעקב אחר הודעות דוא"ל חל, בשינויים המחויבים, גם ביחס לשאר סוגי הפעילות הדיגיטאלית של עובדים.²⁸ **עמדת הרשות היא כי העקרונות העומדים ביסוד ההנחיה האמורה, המבקשים לאזן בין הפררוגטיבה של המעסיק לפקח על עובדיו לבין זכותם לפרטיות, רלוונטיים גם, ואולי אף ביתר שאת, כאשר המעקב נעשה במתכונת של עבודה מרחוק.**

23. מסמך נוסף רלוונטי לענייננו הוא טיוטת גילוי הדעת של הרשות שפורסמה להערות הציבור בנושא 'איסוף נתוני מיקום של עובדים באמצעות אפליקציות ייעודיות ומערכות איכון ברכב'. במסמך זה הבהירה הרשות כי שימוש מעסיקים במערכת האוספת נתוני מיקום של עובדים ייעשה רק כאשר מדובר בתכלית לגיטימית וחיונית למקום העבודה בהתאם לסוג העבודה וטיב תפקידו של העובד, ורק בהעדר חלופה אחרת שאינה אוספת נתוני מיקום, ושכוחה להגשים את תכלית איסוף הנתונים. הרשות הבהירה גם כי ככלל, יהיה קשה להצביע על אינטרס של מעסיק שבכוחו להצדיק איסוף רציף של נתוני מיקום, ככל שמדובר בעובד שעיקר עבודתו בפעילות משרדית רגילה.²⁹

²⁷ לגבי המבחן לשעת עבודה, ראו למשל ע"ע (ארצי) 45431-09-16 גורביץ נ' מדינת ישראל (פורסם בנבו, 16.1.2018) פס"כ 35.

²⁸ לעיל הי"ש 25, בפס"כ 11.

²⁹ לעיל הי"ש 3, בעמ' 3.



מעקב אחר עובדים בעבודה מרחוק – עמדת הרשות להגנת הפרטיות

כללי

24. באופן כללי, דיני הגנת הפרטיות מאפשרים למעסיקים, תחת מגבלות, להשתמש באמצעים טכנולוגיים למעקב ולפיקוח אחר התנהלות עובדיהם במקום ובשעות העבודה. **שימוש זה חייב להיעשות באופן סביר ומידתי, לצרכי מטרה לגיטימית ובעל זיקה לאינטרסים הלגיטימיים של מקום העבודה, תוך יידוע העובדים וקבלת הסכמתם לכך, ותוך הקפדה על כללי אבטחת המידע ועיקרון צמידות המטרה.**³⁰

25. לגישת הרשות, העקרונות שנקבעו בפסיקה - שנועדו לאזן בין זכויות המעסיקים וצרכי מקום העבודה לבין זכויות העובדים, ולצמצם את הפגיעה בפרטיותם של עובדים במסגרת מעקב במקום העבודה - חלים ביתר שאת בעת שמדובר במעקב אחר עובדים במתכונת של עבודה מרחוק, וזאת בשל השימוש הגובר באמצעים טכנולוגיים, אשר מגביר את הסיכון לפגיעה בפרטיות העובד, ועוצמתה, בתוך ביתו שלו, ובפרטיותם של אלו המתגוררים עמו.

26. **עמדת הרשות היא כי שימוש מעסיקים באמצעי מעקב שפגיעתם בפרטיות גבוהה במיוחד (כגון אלו אשר צוינו בסעיף 9 לעיל) מעלה חשש ממשי לחריגה מהוראות הדין.** על מעסיקים המבקשים לעשות שימוש באמצעים שכאלו מוטל הנטל להצביע על הצורך בשימוש זה, ועל העדרה של חלופה אחרת העשויה לתת מענה מספק לצורך האמור תוך פגיעה פחותה בזכות לפרטיות. כמו כן, על מעסיקים להראות כי ההחלטה על שימוש באמצעים אלו התקבלה רק לאחר בחינה מעמיקה של היחס הראוי בין התועלת שתצמח מהם, לבין הנזק והפגיעה בזכות העובד ובני ביתו לפרטיות.³¹

בכל הנוגע לאמצעי המעקב שפורטו לעיל בסעיף 9, עמדת הרשות היא כי שימוש באמצעים אלו עלול להביא לפגיעה חמורה בפרטיות, ושימוש זה יכול להיעשות רק במקרים חריגים בהם קיימת תכלית מקצועית ספציפית המצדיקה זאת, ובכפוף לעמידה בדרישת המידתיות, המפורטת להלן.

להלן יפורטו דגשי הרשות:

מידתיות, לגיטימיות ועיקרון צמידות המטרה

27. **כלל, שימוש מעסיקים באמצעי מעקב אחר עובדים יכול להיעשות רק לשם מטרה מוגדרת ולגיטימית בעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה.** אם מעסיק אינו יכול להצביע על מטרה מוגדרת הנובעת מצורך לגיטימי של מקום העבודה – אין הוא רשאי לעשות שימוש באמצעי מעקב אחר העובד.

³⁰ ראו עניין איסקוב, לעיל הי"ש 25.

³¹ בין היתר, השאלה האם מדובר באמצעי מעקב שהמעסיק עושה בו שימוש גם במקום העבודה (קרי לא רק במתכונת של עבודה צחוק) עשויה להוות שיקול רלוונטי בעת ניתוח נחיצות השימוש באמצעי זה.



28. על מעסיקים חל איסור להשתמש באמצעים דיגיטליים למעקב אחר עובדים (או במידע שנאסף במסגרתם) למטרות פסולות, כלליות, או למטרות שאינן קשורות ישירות לאינטרסים הלגיטימיים של מקום העבודה.

כך לדוגמה, למעסיקים אסור להשתמש במידע שנאסף כתוצאה משימוש באמצעי מעקב שנועדו לבחינת שעות עבודתו של עובד, שלא למטרה לשמה נמסר,³² וברי שלא לשם בחינת מצבו המשפחתי, אופן התנהלותו במרחב הביתי, דעותיו הפוליטיות וכיוצא באלה.

29. ככלל, מעקב אחר עובדים במתכונת של עבודה מרחוק אמור להתבצע במסגרת שעות העבודה. לאור החשש לזליגת המעקב למרחב הפרטי-אנושי של העובד מחוץ לשעות העבודה, על מעסיקים להימנע מלהשתמש באמצעי מעקב מעבר לשעות בהן מעמיד עצמו העובד לרשות המעסיק.

30. אמצעי מעקב שנבחר על-ידי מעסיק צריך להיות תואם לתכלית המעקב. כך לדוגמה, מעסיק המבקש לנטר את היקף שעות העבודה של עובד, צריך לעשות שימוש באמצעים התואמים מטרה זו (כגון אמצעים לבחינת שעות ההתחברות וההתנתקות של העובד מהמערכת המשרדית), ולא באמצעים שנועדו לתכליות אחרות, כגון למעקב אחר פרודוקטיביות העובד במסגרת ניטור תכני האתרים בהם הוא גולש בשעות העבודה.

31. על מעסיקים השוקלים להשתמש באמצעים דיגיטליים למעקב אחר עובדים בביתם להתחשב במידת הפגיעה בפרטיות העובדים ובני ביתם, שעה שהם בוחנים האם ובאילו אמצעים להשתמש. במסגרת זו יש לשקול, בין היתר, את סוג אמצעי המעקב והשלכתו על פרטיות העובד ובני ביתו, משך תקופת ביצוע המעקב (מעקב זמני או לתקופה ארוכה); רציפות המעקב (ניטור רציף לאורך שעות העבודה או ניטור מדגמי בנקודות זמן ספציפיות); המכשיר בו משתמש העובד ושלגביו מתבצע המעקב (כגון מחשב נייד פרטי או מחשב של המעסיק), וכן הלאה.

32. על מעסיקים המבקשים לפקח על עובדיהם במהלך עבודה מרחוק לבחון את החלופות האפשרויות העומדות בפניהם, ולבחור את החלופה מבין החלופות הרלבנטיות להגשמת התכלית שישומה יפגע בפרטיות העובדים במידה הפחותה ביותר האפשרית.

33. כך למשל, מעסיק המבקש למנוע מעובדו לגלוש במחשב שהקצה להם לאתרי אינטרנט מסוימים, רצוי שיעשה שימוש באמצעים טכנולוגיים לחסימת גישה לאתרים אלו (blocking), ולא באמצעים לניטור או פיקוח על האתרים בהם גולשים העובדים. כמו כן, מערכות לדיווח עצמאי על שעות עבודה יחשבו ככלל כחלופה הפוגעת פחות בפרטיות עובדים מאשר אמצעים טכנולוגיים למעקב אחר התנהלותם, כגון אמצעים למעקב אחר מיקום עובדים או אמצעים לצילום העובדים ותיעוד פעילותם. שימוש (ובוודאי שימוש רציף) באמצעי מעקב טכנולוגיים 'חודרניים' שפגיעתם בפרטיות העובדים היא ברף הגבוה,³³ ללא הצדקה ובנסיבות בהן מטרת

³² ראו גם עניין דב"ע 70-4/97 אוניברסיטת תל אביב - ההסתדרות הכללית החדשה ואח', פד"ע ל' עמ' 385, עמ' 411. יצוין כי במקרים חריגים עשויה לקום למעסיק הגנה מכוח סעיף 18 לחוק, בהתקיים התנאים הקבועים בסעיף 20 לחוק.

³³ ראו לעניין זה את החלוקה המוצעת בפסקה 13 למסמך זה.



המעקב יכולה הייתה להיות מושגת באמצעים 'רכים' יותר – חורג לכאורה מדרישת המידתיות ועלול להוות פגיעה אסורה בפרטיות והפרה של הוראות הדין.

יידוע עובדים

34. בהתאם לפסיקה,³⁴ פגיעה בפרטיות במקום העבודה דורשת יידוע העובדים. לפיכך, על מעסיקים ליידע את עובדיהם על כך שהם עושים שימוש באמצעים טכנולוגיים למעקב אחר התנהלותם במתכונת של עבודה מרחוק. יידוע זה צריך לכלול גם את המטרה שלשמה נעשה השימוש באמצעי המעקב.³⁵ חובה זו חלה אף מכוח חובות תום הלב המוגברות שחלות על הצדדים ליחסי עבודה.

35. מעסיקים המבקשים להשתמש באמצעי מעקב שפגיעתם בפרטיות עובדים היא גבוהה – כגון אמצעים למעקב אחר פעילות העובד במחשבו ותכתובת הדואר האלקטרוני של העובד, או אמצעים מבוססים מידע ביומטרי (כגון שימוש בחיישן לקליטת שמע או מערכת לניטור תנועת עיניים) – אינם יכולים להסתפק ביידוע כללי, ועליהם לפרט בפני העובדים, בכתב ובשקיפות מלאה, על אופן ביצוע המעקב והשימוש במידע.

על מעסיק לפרט, לדוגמה, על אופן השימוש באמצעי המעקב, על סוג המידע שייאסף, תדירות ומועדי המעקב, השימוש שייעשה במידע שייאסף, היכן הוא יישמר ולכמה זמן, וכן הלאה. הרשות ממליצה כי יידוע עובדים ייעשה בשפה פשוטה וברורה, תוך התייחסות למאפיינים ייחודיים של עובדים, כגון שפתם, מוגבלותם אם ישנה וכן הלאה.

36. כמו כן, בהתאם לפסיקת בית הדין בעניין איסקוב, על מעסיקים לקבוע את המדיניות הנוהגת במקום העבודה בהקשרים אלו, לרבות תוך ציון כללי האסור והמותר בשימוש במחשב ובשימושי בעת העבודה מרחוק. בפסיקה אף נאמר כי מן הראוי לעגן עקרונות אלה במפורש בחוזה העבודה ובתקנון הנהגה במקום העבודה, ותוך היוועצות עם נציגות העובדים.

הסכמת עובדים

37. חוק הגנת הפרטיות דורש הסמכה בחוק או הסכמה מדעת של אדם לפגיעה בפרטיותו. על ההסכמה להיות מדעת ולהינתן מרצון חופשי, במפורש או מכללא.³⁶

38. בעניין איסקוב וקלנסווה, נפסק שלאור פערי הכוחות, נקודת המוצא היא שהסכמת העובד אינה תמיד חופשית, ומסיבה זו יש "לדקדק" בדרישת ההסכמה, ובמידתיות הפגיעה.³⁷

³⁴ ראו לדוגמה, פס' 111 לפסק הדין בעניין קלנסווה, לעיל ה"ש 26.

³⁵ ראו סעיף 11 לחוק הגנת הפרטיות. לעמדת הרשות להגנת הפרטיות בעניין יישום הוראות סעיף 11 ראו "חובת יידוע במסגרת איסוף ושימוש במידע אישי".

³⁶ סעיפים 1 ו-3 לחוק הגנת הפרטיות.

³⁷ בפסק הדין בעניין קלנסווה נקבע כך: "הצורך בהגנה על זכות העובד לפרטיות נובע מעיקרו מפערי הכוחות האינהרנטיים ביחסים שבין הצדדים ליחסי העבודה, מן ההכרה במציאות לפיה העובד נמצא במקום העבודה חלק ניכר משעות היום, מעירוב התחומים וטשטוש האבחנה בין חיי העובד בעבודה ומחוצה לה, ומטיבם של יחסי העבודה המושתתים על אמון הדדי ועל תפקוד העובד במסגרתם" (פסקה 110 לפסק הדין, המפנה גם לפסק הדין בעניין איסקוב).



בהתאם לכך, במסגרת קבלת הסכמתם על המעסיק לגבש מדיניות ברורה וליידע את העובדים על טיב המעקב והיקפו.

39. ככלל, שימוש מעסיקים באמצעים דיגיטליים למעקב אחר עובדים, הכרוך בעצם מהותו באיסוף מידע אישי על אודותיהם, צריך להיעשות על יסוד קבלת הסכמה מראש מטעם העובדים, בין מפורשת ובין מכללא (קרי הסכמה הנלמדת מהתנהגות העובד בתנאי שהוא מודע לקיומם של אמצעי המעקב). **היה ולא ניתנה הסכמת העובד, במפורש או מכללא, לכך שמידע אישי על אודותיו יאסף לצרכי מעקב על עבודתו מרחוק, ימנע מעסיקו מלאסוף עליו מידע אישי.**³⁸ לחובת היידוע שצוינה לעיל משקל חשוב לצורך הבטחת עמידה בדרישה זו.

40. יודגש כי אין בהסכמת עובדים כדי 'להכשיר' שימוש שאינו מידתי באמצעי מעקב, או כזה הנעשה שלא למטרה מוגדרת ולגיטימית, בעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה. כאמור, הפרורוגטיבה הניהולית לפקח אחר עובדים אינה בלתי מוגבלת והיא כפופה לאמות מידה של סבירות, תום לב והגינות. עם זאת, בנסיבות בהן שימוש באמצעי מעקב מרחוק נעשה בהתאם למבחני המידתיות והלגיטימיות שפורטו לעיל, רשאי מעסיק לדרוש מעובד כי ייתן הסכמתו לאיסוף המידע על אודותיו, וסירוב עובד לבקשה זו עלול להיות בעל השלכות מבחינת יחסי העבודה בין הצדדים.³⁹

41. בכל הנוגע לשימוש באמצעי מעקב שאינם כרוכים במהותם באיסוף מידע אישי על אודות עובדים (כגון ניטור נתוני תקשורת בלבד בתיבת הדואר המקצועית של העובד) – שימוש זה אפשרי ללא קבלת הסכמת העובד, אולם יש ליידעו על כך, וזאת בכפוף לעקרונות הלגיטימיות והמידתיות שצוינו קודם לכן.⁴⁰

שימוש באמצעים לצילום העובד ולהאזנה לסביבתו

42. שימוש באמצעים לצילום עובד ולהאזנה לסביבתו שעה שהוא בביתו עלול להביא לפגיעה קשה בפרטיות העובד ובני ביתו. מטבע הדברים, שימוש באמצעים אלו עלול להביא לאיסוף מידע אישי, פרטי ורגיש על אודות העובד ובני ביתו (לרבות קטינים), שאינו רלוונטי לצרכי מקום העבודה, בוודאי כאשר הצילום וההאזנה נעשים באופן רציף ולאורך חלקים ניכרים משעות היום.

43. כאמור, סעיף 2(1) לחוק הגנת הפרטיות קובע כי בילוש או התחקות אחרי אדם, העלולים להטרידו, מהווים פגיעה בפרטיות. כמו כן, על-פי סעיפים 2(2) ו-3(2) לחוק, האזנה שאינה מכוח חוק או צילום אדם שהוא ברשות היחיד, הנעשים ללא הסכמה, מהווים גם הם פגיעה בפרטיות. לאור כך ובהתבסס על פסיקת בית הדין לעבודה בעניין איסקוב, הרשות מדגישה כי שימוש

³⁸ השופטת ארד ציינה בעניין זה כי: "דרישת ההסכמה מראש ומדעת של העובד, עולה ביתר שאת בהתקיים חשש לפגיעה בפרטיותו, נוכח פעולותיו של המעסיק". ראו עניין איסקוב, לעיל ה"ש 25, בפסקאות 29-30 לפסק דינה של השופטת ארד.

³⁹ מסמך זה מתמקד בסוגיית הפגיעה בפרטיות, ואין הוא עוסק בשאלת סבירות סירובו של עובד לבקשה מידתית ולגיטימית של מעסיק לשימוש באמצעי מעקב מרחוק, או במשמעותו של סירוב לבקשה שכזו במישור יחסי העבודה.

⁴⁰ עניין איסקוב, לעיל ה"ש 25, בפסקה 38 לפסק דינה של השופטת ארד.



באמצעים לצילום ולהאזנה לעובד שעה שהוא בביתו, לא יכול להיעשות אלא לאחר קבלת הסכמה חופשית ומדעת מצד העובד.

44. לאור החזירה למרחב הפרטי של העובד כתוצאה משימוש באמצעים האמורים, החשש שהסכמתו עלולה שלא לבטא את רצונו החופשי,⁴¹ ולאור כך שהסכמת העובד לצילום או להקלטת סביבת עבודתו עלולה להביא לאיסוף מידע רגיש גם על אחרים (כגון בני ביתו של העובד, לרבות קטינים שלא נתנו הסכמתם לאיסוף המידע) – עמדת הרשות היא שעל מעסיקים להימנע משימוש באמצעים שכאלו, אלא במקרים קיצוניים בהם קיים צורך חיוני לכך, וכאשר אמצעים אחרים שבהם נעשה שימוש לא הועילו.⁴²

45. מכל מקום, בנסיבות בהן נעשה שימוש באמצעים לצילום עובד או להאזנה לסביבתו, על המעסיקים לוודא כי שימוש באמצעים האמורים יעשה רק במהלך שעות העבודה ותוך הימנעות, ככל האפשר, מאיסוף מידע על אודות אחרים. על המעסיק לפעול לכך שמידע אשר נאסף באופן אגבי על אודות בני ביתו של העובד (ואנשים אחרים שאינם רלוונטיים לתכלית המעקב) לא יישמר כלל במאגרי המידע שלו.

איסוף מידע מתיבה פרטית-חיצונית שבבעלות העובד

46. בהתאם לקביעת בית הדין בעניין איסקוב, מעסיקים אינם רשאים לעשות באמצעי מעקב לחזירה או לאיסוף מידע מתיבת דוא"ל פרטית-חיצונית הנמצאת בבעלות העובד (כגון דוא"ל מסוג Gmail) - לרבות לנתוני תקשורת של העובד בתיבה הפרטית ולנתוני תוכן של התכתובת הפרטית שלו בתיבה – אלא מכוח צו שיפוטי.

47. כדי לעמוד בדרישה זו, מומלץ כי מעסיקים המאפשרים לעובדיהם להיכנס לתיבות הדואר הפרטיות-חיצוניות שלהם בעת עבודתם מהבית ומתוך המחשב של מקום העבודה, יימנעו מלהשתמש באמצעי מעקב כגון תוכנות לצילום מסך – וזאת מתוך החשש כי במהלך המעקב ייאסף מידע שמקורו בתיבת הדואר הפרטיות-חיצוניות של העובד.

48. הרשות מבהירה כי בהתאם לקביעת בית הדין בעניין איסקוב, אין בהסכמת עובד כדי להתיר למעסיק לחדור לתיבת דוא"ל פרטית-חיצונית שלו או לאסוף מידע מתוך תיבה זו.

צמצום מידע עודף

49. כפי שצוין, מעקב אחר עובדים כאשר הם בביתם עלול להביא לכך שמעסיקים יאספו מידע רגיש רב על אודות העובדים ובני ביתם, שאינו נדרש לצרכי המעקב ואינו תואם למטרת האיסוף.

⁴¹ שם, בפסקה 43 לפסק דינה של השופטת ארד.

⁴² יובהר כי עמדה זו אינה מתייחסת למקרים שבהם השימוש באמצעים האמורים נעשה שלא למעקב אחר התנהלות העובד אלא מסיבות אחרות, כגון לשם מתן תמיכה טכנית לעובד מרחוק או לשם קיום פגישות וירטואליות של עובד מביתו הנערכות כחלק מעבודתו.



50. על פי עיקרון צמצום המידע העודף, על מעסיקים להימנע ככל הניתן מאיסוף ושמירה של מידע על אודות עובדים שאינו הכרחי למטרת המעקב, או למטרת המאגר בו מידע זה נשמר.⁴³

51. מכוח תקנה 2(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'התקנות' או 'תקנות אבטחת מידע') על מעסיקים, בכובעם כבעלי מאגרי המידע, לבחון, אחת לשנה, אם המידע שהם שומרים במאגר אינו חורג מן הנדרש ביחס למטרותיו.

בעניין זה יובהר כי לגישת הרשות להגנת הפרטיות ייתכנו מצבים בהם רצוי שבדיקה כזו תיערך מספר פעמים לאורך השנה וזאת, בין היתר, כתלות בסוג המידע השמור ומטרת איסופו. במקרה זה, לאור כך שמידע הנאסף במסגרת מעקב עבודה מרחוק עשוי להיות מידע רגיש במיוחד, מומלץ כי הבחינה תיעשה במסגרת פרקי זמן קצרים יותר מהקבוע בתקנות, קרי מספר פעמים בשנה.

תקופת שמירת המידע

52. במקרים מסוימים עלולים ארגונים לשמור מידע שנאסף על אודות עובדים במסגרת מעקב אחר התנהלותם בביתם לאורך זמן, וזאת ללא כל הצדקה או תכלית ראויה.

53. ככלל, עמדת הרשות היא שעל ארגונים לשמור מידע על עובדיהם הנאסף במסגרת מעקב אחריהם, אך ורק לתקופה התואמת את מטרת איסוף המידע או מטרת המאגר בו שמור המידע.

54. בעניין זה יצוין כי שמירת מידע לאורך זמן מגבירה את הסיכון לפגיעה בפרטיות. ככל שמידע הנאסף במסגרת שימוש באמצעי מעקב נשמר על ידי המעסיק לתקופה ארוכה יותר – כך גובר הסיכון כי מידע זה ידלוף או ייחשף ויפגע קשות בפרטיות העובדים ובני ביתם.

אבטחת מידע ועיצוב לפרטיות

55. על-פי סעיף 17 לחוק הגנת הפרטיות, מעסיקים, כבעלי המאגרים בה נשמר המידע, הם הגורם האחראי על אבטחת המידע המוחזק במאגר.

56. תקנות אבטחת מידע קובעות כי מידת רגישותו של המידע השמור במאגר מהווה קריטריון ביחס לאופן יישום היבטים שונים של אבטחת מידע, כגון אופן ההתמודדות עם אירועי אבטחת מידע והאבטחה הפיזית והסביבתית של מאגר המידע. מידת רגישותו של המידע משפיעה גם על רמת אימות הזהות הנדרשת בעת מתן גישה מרחוק למאגר.⁴⁴

57. על מעסיקים לפעול לאבטחת המידע הנאסף לשם וכתוצאה משימוש באמצעי מעקב אחר עובדים בהתאם להנחיות האמורות.

58. הרשות מבקשת להדגיש את החשיבות בעריכת תסקיר השפעה על פרטיות, טרם השימוש באמצעים למעקב אחר עובדים. תסקיר הוא תהליך אשר נועד לסייע לארגון באיתור, הערכה

⁴³ עיקרון זה מושתת על הוראות סעיף 9(2) ו-8(ב) לחוק הגנת הפרטיות. להרחבה ראו [טיוטת מסמך מדיניות הרשות להגנת הפרטיות בנושא צמצום מידע](#).

⁴⁴ ראו לעניין זה תקנה 9 לתקנות אבטחת מידע.



וניהול של סיכונים לפרטיות בפרויקטים או פעילויות עסקיות וארגוניות אחרות הכוללות איסוף ושימוש במידע אישי.⁴⁵ לגישת הרשות, עריכת התסקיר בשלב מוקדם היא הדרך היעילה והאפקטיבית למזער את הסיכון לפגיעה בפרטיות וסיכוני אבטחת המידע, ורצוי כי ארגונים המבקשים להשתמש באמצעים למעקב אחר עובדים (במקום העבודה ובמתכונת של עבודה מרחוק), יפעלו לעריכת תסקיר שכזה.

הרשות מבקשת להדגיש בהקשר זה גם את התועלת הרבה שבמינוי ממונה הגנת פרטיות בארגון, שבין יתר תפקידיו, הוא גם הגורם המתאים והיעיל לתכנון ולבחינת הצעדים הננקטים בארגון למזעור הסיכון לפגיעה בפרטיות העובדים.⁴⁶

עיון במידע ותיקונו

59. סעיף 13 לחוק הגנת הפרטיות קובע את זכותו של אדם לעיין במידע על אודותיו המוחזק במאגר מידע. הסעיף קובע כי על בעל מאגר לאפשר עיון במידע המוחזק על-ידו, וזאת בהתאם לבקשה המוגשת לו מטעם נושא המידע.

60. הרשות מבקשת להדגיש כי מידע אישי על אודות עובדים, שנאסף במסגרת מעקב אחריהם בעודם עובדים בביתם, הוא מידע שיש לאפשר לעובד לעיין בו, בהתאם להוראות סעיף 13 ובכפוף לסייגים המפורטים בו.

61. בהתאם להוראות סעיף 14(א) לחוק, עובד שעיון במידע על אודותיו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות למעסיק בבקשה לתקן את המידע או למוחקו.

העברת מידע לצדדים שלישיים

62. המידע הנאסף על-ידי מעסיקים במסגרת שימושם באמצעי מעקב – ככל ששימוש זה נעשה על-פי מבחני המידתיות ובהסכמת העובד – נועד אך ורק לשימוש המעסיקים ולצרכי פיקוח על עובדיהם בשעות העבודה.

63. לפיכך, חל איסור על מעסיקים להעביר מידע זה לצדדים שלישיים, לרבות מעסיקים עתידיים או פוטנציאליים של עובדיהם, אלא בהסכמת העובדים או מתוקף חובה שבדין.

סיכום

64. למעבר ארגונים למתכונת מלאה או חלקית של עבודה מרחוק יש יתרונות רבים. עם זאת, השימוש של ארגונים באמצעים דיגיטליים לפיקוח על התנהלות עובדיהם העובדים במתכונת שכזו, מהווה אתגר בכל הנוגע להגנה על פרטיותם של עובדים אלו.

65. במסמך זה סקרה הרשות את הסיכונים לפרטיות הכרוכים בשימוש באמצעים טכנולוגיים למעקב אחר עובדים ואת הוראות הדין הרלוונטיות, וכן הציגה הנחיות והמלצות בנושא זה.

⁴⁵ ראו מדריך עזר לביצוע תסקיר השפעה על הפרטיות שפרסמה הרשות להגנת הפרטיות (אוגוסט 2021).
⁴⁶ להרחבה ראו עמדת הרשות להגנת הפרטיות בעניין "מינוי ממונה הגנה על פרטיות בארגון ותפקידיו" (ינואר 2022).



66. לגישת הרשות, העקרונות שנקבעו בפסיקה ואשר נועדו לאזן בין צרכי המעסיקים לזכותם לפרטיות של עובדים - חלים ביתר שאת שעה שמדובר במעקב במתכונת של עבודה מרחוק, וזאת בשל הסיכון לפגיעה ממשית בפרטיות העובד ובני ביתו.

67. ככלל, למעסיקים עומדת הפררוגטיבה להשתמש באמצעים טכנולוגיים למעקב ולפיקוח אחר התנהלות עובדיהם במקום ובשעות העבודה, צורך שגובר ביתר שאת מקום שבו מתאפשרת עבודה מרחוק, לעיתים מתוך רצון של העובדים לאיזון עבודה-בית. עם זאת, הגברת הצורך מביאה גם להגברת הצורך להבטיח כי שימוש זה ייעשה באופן סביר ומידתי, לצרכי מטרה לגיטימית ובעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה, תוך יידוע העובדים בדבר המעקב, ותוך הקפדה על כללי אבטחת המידע ועיקרון צמידות המטרה. ככל שמדובר באמצעים שהשימוש בהם כרוך באיסוף מידע אישי על אודות עובדים – אין להשתמש באמצעים אלו ביחס לעובדים שלא נתנו הסכמתם לאיסוף מידע על אודותיהם, במפורש או מכללא.

68. שימוש מעסיקים באמצעי מעקב שפגיעתם בפרטיות גבוהה במיוחד, כגון אלו אשר פורטו בסעיף 9 לעיל, מעלה חשש ממשי לחריגה מהוראות הדין. בנוגע לאמצעים לצילום או להאזנה לעובד – עמדת הרשות היא שאין לעשות שימוש באמצעים אלו, למעט במצבים קיצוניים המחייבים זאת.

69. למעסיקים המאפשרים לעובדיהם להיכנס לתיבות הדוא"ל הפרטיות-חיכוניות שלהם במהלך עבודתם מהבית מומלץ להימנע מלהשתמש באמצעי מעקב לצילום מסך, וזאת מתוך החשש כי במהלך המעקב ייאסף מידע שמקורו בתיבת הדוא"ל הפרטית-חיכונית של העובד – מידע שחל איסור לאוספו אלא מכוח צו שיפוטי.