

הזכות לפרטיות בעבודה: עיון מחודש בפרשת איסקוב ענבר ויישומה

מאת

עינת אלבין וגיל עומר*

לפני כעשור קבע בית הדין הארצי לעבודה את אחת מההלכות המרכזיות בכל הנוגע לזכות לפרטיות בעבודה בעידן של טכנולוגיות חדשות – הלכת **איסקוב ענבר**. מאמר זה בוחן את ההלכה ואת יישומה בבתי הדין לעבודה כדי לראות אם וכיצד מוגנת זכותם של עובדים לפרטיות. בעולם דיגיטלי, שבו צעדי העובדים מנוטרים או שמבוצע אחריהם מעקב, ומידע רב נאסף עליהם, הזכות לפרטיות היא אחת מהזכויות החשובות בעבודה, בעיקר לאחר תקופת הקורונה. המחקר מאמץ מתודולוגיה של ניתוח איכותני של פסקי הדין שניתנו בבתי הדין לעבודה בעשור שחלף מאז אומצה ההלכה (51 פסקי דין). הוא מראה כי מבחני ההלכה מיושמים בפסיקה באופן חלקי, ובייחוד כי הפסיקה מאמצת הבחנה גסה בין מידע עסקי לפרטי ובוחרת באופן חלקי את השאלה אם הפרטיות נפגעה; כי פעמים רבות מבחני הלגיטימיות, המידתיות, השקיפות וצמידות המטרה הוחלו בצמצום, ולעיתים נדירות נבחנה לגביהם הטכנולוגיה עצמה; וכי משקל רב מושם על עקרון ההסכמה, מה שמייצר קושי הן לאור תאוריות של דיני עבודה והן לאור תאוריות של דיני פרטיות. עוד מראה המחקר, שאין נקבעות סנקציות בעלות משקל על מעסיקים שאינם מקפידים על הגנת הזכות לפרטיות של עובדיהם באופן שוטף – לא באמצעות קביעת פיצויים ניכרים על פגיעה בפרטיות ולא במניעת סעדים. המאמר טוען כי נדרשת חשיבה מחודשת על ההלכה ועל יישומה בכמה הקשרים, ומציע דרכים שבהן ניתן להגן טוב יותר על הזכות בעתיד אגב הכרה בחשיבותה בעידן של ימינו.

מבוא. א. הלכת איסקוב ענבר. ב. מתודולוגיה ותיאור הנתונים. 1. בניית מאגר פסיקה. 2. שיטת המחקר. ג. ממצאים. 1. יישום מבחני איסקוב ענבר. 2. השלכות הפגיעה בפרטיות. 3. ממצאים נוספים. ד. דיון. 1. הדגש שניתן לשאלת ההסכמה. 2. שאלת הפגיעה

* עינת אלבין היא מרצה בכירה בפקולטה למשפטים באוניברסיטה העברית בירושלים המתמחה בדיני עבודה. גיל עומר היא תלמידה לתואר שלישי בכלכלה באוניברסיטת תל אביב. אנו מודות למיכאל בירנהק ולתמי קצביאן על קריאה של גרסה קודמת למאמר זה ועל מתן הערות מצוינות. כמו כן אנו מודות לקרן ויגשל, לתמי קריכלי-כץ ולשגית מור על סיוע מתודולוגי, וליסמין יונס ולכרמל הס על עבודתן המצוינת. אנו מודות גם למרכז פלדמן לחקר הסייבר באוניברסיטה העברית על מתן מענק מחקר שאפשר מחקר זה. נבקש לציין כי המחקר על המאמר הסתיים לפני כשנתיים, בשנת 2022, והוא אינו מתייחס לחקיקה ו/או פסיקה שהתקבלה מאז.

בפרטיות. 3. נחיצותו של דיון טכנולוגי. 4. הרתעת המעסיק מפני הפגיעה בזכות הפרטיות. ה. סיכום. נספח - תוצאות יישום הלכת איסקוב ענבר.

מבוא

השימוש הגובר בטכנולוגיות חדשות בעולם העבודה מעלה שאלות משפטיות כבדות משקל, בין השאר בכל הנוגע לזכות לפרטיות. במציאות שבה המידע האישי על עובדות ועובדים נאסף תדיר בידי מעסיקים לצרכים שונים,¹ בעיקר לאחר תקופת הקורונה שבה נעשה שימוש מוגבר בטכנולוגיות חדשות בעבודה; יש חשיבות לבחון לעומק מהי מידת ההגנה שמעניקים בתי הדין לעבודה מפני פגיעה בזכות לפרטיות העובדים ומהן ההשלכות על המעסיק שפגע בזכות העובדים לפרטיות. מאמר זה עוסק בשאלות אלה אגב ניתוח של 51 פסקי הדין שניתנו בבתי הדין לעבודה – האזוריים והארצי – המפנים להלכה המרכזית שמנחה את הדין בתחום – הלכת איסקוב ענבר.²

הזכות לפרטיות בעבודה הפכה להיות אחת מהזכויות המהותיות בדיני העבודה כיום. זכות זו מעסיקה את קובעי וקובעות המדיניות,³ את בתי הדין לעבודה,⁴ ואף את המחוקק,⁵ והיא מציפה שאלות רבות – תאורטיות ויישומיות – בעיקר בעקבות אימוצן של טכנולוגיות מידע דיגיטליות חדשות וקיומם של אתגרים חדשים העומדים בפני ארגונים.⁶ מדובר באחת מזכויות האדם החשובות בחברה ליברלית-דמוקרטית. אכן, יש רבים

¹ צרכים אלה כוללים: הגנת סייבר, מעקב אחר שעות עבודה של העובדים והעובדות, אחר מצבם הבריאותי, בחינת הפרודוקטיביות של העובדים ואיכות עבודתם, כשירותם לתפקיד והעלאה בתפקיד ועוד. טכנולוגיות שמשמשות בהן בעולם העבודה כוללות טכנולוגיות של כוח אדם (People Analytics), הגנת סייבר, אמצעי זיהוי של עובדות ועובדים בכניסה לעבודה וביציאה ממנה, מבחני התאמה ועוד, אשר חלק מהם כבר נדונו בפסיקה. ראו למשל דב"ע (ארצי) 4-70/97 אוניברסיטת תל-אביב – ההסתדרות הכללית החדשה, פד"ע ל 385 (1998); עס"ק (ארצי) 7541-04-14 הסתדרות העובדים הכללית החדשה – עיריית קלנסווה (נבו 15.3.2017).

² ע"ע (ארצי) 90/08 איסקוב ענבר – הממונה על חוק עבודת נשים (נבו 8.2.2011).

³ הרשות להגנת הפרטיות (לשעבר רמו"ט – הרשות למשפט, טכנולוגיה ומידע) עסקה כמה פעמים בעבר בשאלת הזכות לפרטיות בעבודה ופרסמה כמה מדריכים בנושא, לרבות הנחיית רשם מאגרי מידע 5/17 "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה" (17.10.2017) (להלן: הנחיית מצלמות מעקב ביחסי עבודה), וכן, הרשות להגנת הפרטיות היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק (17.5.2023). כמו גם מערך הסייבר הלאומי (ראו למשל מערך הסייבר הלאומי מסמך המלצות: שיטת עבודה מומלצות למערכת ניהול התקנים ניידים (MDM/EMM) (14.1.2021), הכולל התייחסות לשמירה על פרטיות העובד), ארגוני עובדים (לפירוט על הסכם קיבוצי שנחתם בין הסתדרות העובדים הכללית לבין לשכת התיאום של הארגונים הכלכליים בנושא שימוש עובדים במחשב בפרק א ראו להלן) ועוד.

⁴ ראו לעניין זה את החלטות בית הדין הארצי לעבודה בפרשות כגון פרשת אוניברסיטת-תל אביב, לעיל ה"ש 1, ופרשת עיריית קלנסווה, לעיל ה"ש 1, וכמובן פרשת איסקוב ענבר, לעיל ה"ש 2.

⁵ ראו למשל תקנה 7 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017 (העוסקת באבטחת מאגרי מידע בניהול כוח אדם); תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח–2018 (להלן: תזכיר חוק הסייבר).

⁶ HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 1 (2009) (להלן: NISSENBAUM, PRIVACY IN CONTEXT).

הטוענים כי הזכות לפרטיות איבדה ממעמדה בעידן של טכנולוגיות חדשות שבהן כבר "אין פרטיות". דברים מעין אלו נאמרו גם בבית הדין האזורי לעבודה בתל-אביב בפסק דין **אקספו** שבו אמרה השופטת יפית זלמנוביץ גיסין:⁷

בשולי הדברים ובאשר לזכות לפרטיות – בעידן הנוכחי נדמה שלמושג הפרטיות יש מעט מאד מקום בחיינו. כאשר עובד, אך לא רק, מקבל טלפון נייד ממעסיקו, מוריד לטלפון אפליקציות (יישומונים) אשר חלקן מבצעות מעקב אחר מיקומו, מידע שמתרגם מיד לפרסומות והצעות לרכישת מוצרים בקרבת מקום, חלקן אחר השימוש שאנו עושים באפליקציות מסוימות ותדירות השימוש על מנת להציע לנו אפליקציות דומות/פרסומות/מוצרים ועוד, ספק אם העובד או כל אדם אחר למעשה, לטעון כי קיימת לו זכות לפרטיות במה שהפך להיות המרחב האישי-הציבורי של חייו.

ואולם, מחקרים מראים כי הזכות לפרטיות עדיין מהותית ונמצאת בנפשו של האדם. הזכות לפרטיות חשובה מאוד אף מבחינות חברתיות, הגנה על מהותה של אזרחות ועל דמוקרטיה ליברלית, חדשנות, צמיחה אנושית ועוד.⁸ חברה דמוקרטית נשענת על פומביות לצורך הגנה מפני השלטון ועל פרטיות כמגן על חיים אישיים וקבוצתיים.⁹ כדי לקיים דמוקרטיה ליברלית וחדשנות יש חשיבות בקיומם של מרחבים מרווחים שבהם הצמיחה העצמית מתרחשת.¹⁰ אלו המרחבים של פרטיות. דברים אלה חשובים ביותר בהקשר של עבודה. הגנה על הזכות לפרטיות אינה מגינה רק על זכויות הפרט (מלבד הפרטיות, ההגנה היא אף על הזכות לאוטונומיה ועל הזכות לכבוד)¹¹ אלא גם על אינטרסים חברתיים וכלכליים רחבים יותר של עובדות ועובדים. היא מייצרת מרחבים שיאפשרו להם להתבטא ללא חשש, לשוחח ביניהם, לפתח רעיונות חדשניים, להתאגד ועוד. אף ניתן לטעון כי בהקשר של עבודה, לזכות לפרטיות יש חשיבות רבה יותר. אף שכולנו חיים בחברת מעקב (surveillance society),¹² הרי שבעבודה איסוף המידע עלינו מקיף, וחשוב מכך,

⁷ סע"ש (אזורי ת"א) 18279-06-16 **אקספו ניהול בע"מ – כהן**, פס' 31 להחלטה של השופטת זלמנוביץ-גיסין (נבו 26.3.2017).

⁸ ראו Jolie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2013); CLARISA VELIZ, *PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA* (2021); Valerie Steeves, *Reclaiming the Social Value of Privacy, in LESSONS FROM THE IDENTITY TRAIL: AUTONOMY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY* 191 (Jan Kerr, Carole Lucock & Valerie Steeves eds., 2009).

⁹ ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967).

¹⁰ Cohen, *What Privacy is For*, לעיל ה"ש 8.

¹¹ ראו מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9 (2017) (להלן: בירנהק "שליטה והסכמה"); VELIZ, לעיל ה"ש 8. בארצות הברית מודגש מאוד היות הזכות קשורה לאוטונומיה של הפרט, ובאירופה – לכבוד האדם.

¹² על חברת מעקב, ראו SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019); VELIZ;

לאיסוף המידע ולהימצאותו בידי המעסיק יש משמעות ייחודית בשל מערכת היחסים בין הצדדים שאינה שוויונית, שהיא לעיתים קרובה ואף אינטימית, וכן בשל הצדדים שהמעסיק יכול לנקוט בעקבות החשיפה למידע פרטי, כגון פיטורים, מניעת קידום, פגיעה בשכר ועוד. הכתיבה בדיני העבודה מחדדת את היות כוחו של המעסיק דומה לכוחה האוטוריטטיבי של המדינה,¹³ ואולם בפועל יש מצבים שבהם המגבלות החלות על פי דין על מעסיקים באשר לפגיעה בפרטיות עובדיהם פחותות מאלה החלות על המדינה כלפי אזרחיה.¹⁴

הזכות עוגנה לראשונה בחקיקה ראשית בשנת 1981, עם חקיקתו של חוק הגנת הפרטיות,¹⁵ והיא מעוגנת בחוק-יסוד: כבוד האדם וחירותו, שבו נקבע בין היתר כי "כל אדם זכאי לפרטיות ולצנעת חייו".¹⁶ ההסדרים החקיקתיים קובעים הגנות כלליות החלות גם על יחסי עבודה, ואולם הם אינם מתייחסים להקשר של עבודה באופן ייחודי ומפורש, והזכות לפרטיות בעבודה פותחה בעיקר בפסיקתם של בתי הדין לעבודה. פסק הדין המרכזי העוסק בסוגיית הפרטיות בהקשר של יחסי עבודה בעידן הטכנולוגי הוא **איסקוב ענבר**,¹⁷ אשר ניתן בשנת 2011. מאז ניתן מספר רב יחסית של פסקי דין אשר הרחיבו את הדיון בפרטיות לסוגיות נוספות,¹⁸ או יישמו את הלכת **איסקוב ענבר** בהקשרים הדומים לאלה שעלו בפסק הדין.

כאמור, במאמר זה נבחן את יישום הלכת **איסקוב ענבר** בבתי הדין לעבודה בישראל – בתי הדין האזוריים וכן בית הדין הארצי. לשם כך ניתחנו את כל פסקי הדין של בתי הדין לעבודה שנמצאו באתר "נבו" ושעסקו בזכות לפרטיות והפנו להלכה האמורה כשהם מיישמים או מפתחים אותה. מדובר ב-51 פסקי דין, כאשר המתודולוגיה שבה השתמשנו היא ניתוח טקסט איכותני של פסקי הדין. לאור הניתוח שעשינו בחנו אם ההלכה, ובעיקר יישומה, אכן נותנים הגנה טובה לזכות לפרטיות בהקשר של עבודה אגב הכרה בייחודה של מערכת היחסים הלא שוויונית הקיימת בין העובדים לבין המעסיק ולפערי הידע שבין הצדדים.

לעיל ה"ש 8, בפרק ההקדמה. כן ראו Mariano-Florentino Cuéllar & Aziz Huq, *Economies of Surveillance*, 133 HARV. L. REV. 1280 (2020).

¹³ PAUL DAVIES & MARK FREEDLAND, *KAHN FRUEND'S LABOUR AND THE LAW* (3d ed. 1983).

¹⁴ למשל, פרק ג לתזכיר חוק הסייבר מגביל את סמכות הרשות להגנת הסייבר לפעול רק כאשר יש יסוד סביר להניח שמתרחשת או עשויה להתרחש תקיפת סייבר שעלולה לגרום לפגיעה באינטרס חיוני. הגבלה דומה אינה קיימת על מעסיקים.

¹⁵ פרק ב לחוק הגנת הפרטיות, התשמ"א-1981.

¹⁶ ס' 7(א) לחוק-יסוד: כבוד האדם וחירותו.

¹⁷ פרשת **איסקוב ענבר**, לעיל ה"ש 2.

¹⁸ ראו למשל את פסק הדין בפרשת **עיריית קלנסווה**, לעיל ה"ש 1. בית הדין הארצי בעניין זה קבע כי אומנם הלכת **איסקוב ענבר** (לעיל ה"ש 2) נקבעה בקשר לשימושי מחשב במקום העבודה, אך היא מתאימה, בשינויים המחוייבים, גם בנוגע לאפשרויות העומדות למעסיק במעקב אחר שעות עבודה באמצעות שעון ביומטרי.

יצוין כי המחקר האקדמי סביב שאלת ההגנה על הזכות לפרטיות, בין השאר בתחום של עבודה,¹⁹ התרחב מאוד בשנים האחרונות. מחקר זה עוסק בגישות תאורטיות שונות ובהגדרות מגוונות לזכות לפרטיות, בדוקטרינות העולות מגישות תאורטיות שונות אלה ובהתאמתן לאתגרי הטכנולוגיה.²⁰ אחת הנקודות החשובות שעולות מהמחקר, ואף מצויה בלב הדוקטרינה המשפטית, נוגעת להבחנה בין הקשרים שונים של פרטיות (קשרים אינטימיים, למשל, אל מול נוכחות ציבורית, או דרישות ייחודיות בהקשר של יחסים שונים, כגון יחסי תאגיד וצרכן ועובד-מעסיק), כאשר על הקשרים שונים חלים דינים שונים.²¹ בירנהק הציע בספרו לסווג את הזכות לפרטיות כאוסף של מעגלים קונצנטריים, כאשר במעגל הפנימי נמצא האדם, המעגל השני הוא של קשרים בין-אישיים, מעגל שלישי הוא של קשרי קהילה והמעגל החיצוני ביותר – של המדינה. כך, בכל מעגל הצדקת הזכות לפרטיות, שממנה נגזר היקף ההגנה על הזכות, עשויה להיות שונה:²² במעגל המדינה הפרטיות נועדה לרסן כוח שלטוני, במעגל הבין-אישי הפרטיות מאפשרת אמון בין אדם לחברו (למשל בין רופא למטופל), ואילו במעגל הפנימי הפרטיות מאפשרת שליטה של אדם בעצמו.²³ מכאן עלתה לא אחת הטענה שבהקשר של עבודה נדרשת התייחסות מיוחדת לזכות לפרטיות בשל מערכת היחסים הייחודית שבין עובד לבין מעסיק

¹⁹ בעברית, ראו למשל מיכאל בירנהק "מעקב בעבודה: טיילור, בנת'האם והזכות לפרטיות" **עבודה, חברה ומשפט** יב 9, 34 (2010); שלי ולך "מישהו מתבונן בך: מעקב אחר עובדים במקום העבודה וזכות העובד לפרטיות" **ספר אלישבע ברק-אוסוסקין** 473 (2012).

²⁰ ראו למשל Matthew Finkin, *The Conception of the Employee as a Person in Western Law*, 23 COMP. LAB. L. & POL'Y J. 577, 580–586 (2002); Virginia Mantouvalou, *Work and Private Life: Sidabras and Dziautas v. Lithuania*, 30 EUR. L. REV. 573, 575–582 (2005); MARTA OTTO, *THE RIGHT TO PRIVACY IN EMPLOYMENT* (2016); Ugo Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection?*, in GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGY 159 (Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., 2017); Lucas D. Inrona, *Workplace Surveillance, Privacy, and Distributive Justice*, 30 COMPUT. & SOC'Y 33 (2000) Frank Hendrickx, *Privacy 4.0 at Work: Regulating Employment, Technology and Automation*, 41 COMP. LAB. L. & POL'Y J. 147 (2019); Antonio Aloisi & Elena Gramano, *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*, 41 COMP. LAB. L. & POL'Y J. 95 (2019); Tammy Katsabian, *Employee's Privacy in the Internet Age: Towards a New Procedural Approach*, 40 BERKELEY J. EMP. & LAB. L. 203 (2019).

²¹ כך, למשל, חוק הגנת הפרטיות מייצר הבחנות בין ספרה פרטית לספרה ציבורית בכל הנוגע לפרטיות, ואף מעניק הגנה ייחודית לפרטיות בהקשרים מסוימים ולא אחרים. לגישה קונטקסטואלית לפרטיות, ראו גם Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 148 (2004). על חלוקת דיני הפרטיות למקטעים משפטיים לפי אפיקי זרימת המידע, ראו מיכאל בירנהק "פרטיות בעיר הדיגיטלית" **מחקרי משפט** לד 1 (2021).

²² מיכאל בירנהק [מרחב פרטי] הזכות לפרטיות בין משפט לטכנולוגיה (2011).

²³ שם, בעמ' 115–125.

הכוללת פערי כוחות בין הצדדים וכפיפות של העובד למעסיק.²⁴ לגישתנו, ניתן לחזק טענה זו אף על בסיס הקשר הקיים בין פרטיות לבין אוטונומיה,²⁵ הואיל ואוטונומיה בהקשר של עבודה מומשגת אחרת מאוטונומיה בתחומי משפט אחרים. למשל, בניגוד לתפיסה הרווחת במשפט כי חופש מושג באמצעות היעדר התערבות חקיקתית ומתן חופש חוזי לצדדים להגיע להסכמות באשר לרצונם, חוקרים מעולם העבודה הראו כיצד דווקא התערבות בחופש החוזי באמצעות חקיקה קוגנטית היא שאפשרה מעבר מעבודה בכפייה לעבודה חופשית.²⁶ אוטונומיה, כך נטען, מושגת ביצירת יכולות אגב התערבות שוקית.²⁷ מכאן שבחינת ההגנה על פרטיות שנועדה לאפשר אוטונומיה כאשר מדובר ביחסי עבודה צריכה להיות שונה ביחס לכל מערכת יחסים אחרת שאותה מסדיר המשפט. במילים אחרות, יש לרסן את הפגיעה הפוטנציאלית בפרטיות כדי להגן על הזכות וליצור מרחב אוטונומי לעובדים.²⁸ כך ככלל, ובהקשר של טכנולוגיות חדשות בפרט, שכן אלה מעוררות שאלות ייחודיות בהקשר של עבודה.²⁹

בחינת שאלות המחקר שלנו וניתוחן מובילים אותנו לטעון שתי טענות עיקריות בנוגע לזכות לפרטיות בעבודה בעידן של טכנולוגיות חדשות. אף שמצאנו שב-39% מהמקרים שהובאו לפני בתי הדין לעבודה ניתנה הגנה מלאה על הזכות לפרטיות של העובד, עדיין מצאנו כמה קשיים בנוגע ליישום הלכת **איסקוב ענבר**. טענתנו הראשונה היא אפוא כי יש לבחון מחדש הלכה זו, ובעיקר כי נדרשת חשיבה מעמיקה ורחבה יותר על המבחינים שאימצה הפסיקה, הן בכל הנוגע להגדרת הפגיעה בפרטיות, הן בכל הנוגע למבחן ההסכמה המבוסס על הרעיון של פרטיות כשליטה, או במילים אחרות, שאדם יכול להסכים למסירת המידע הפרטי שלו, ואז אין מדובר בפגיעה בפרטיות, והן באופן יישומם של מבחינים חוקתיים ומנהליים שאומצו כדי להגן על הזכות. כך, למשל, הניתוח מראה שבתי הדין לעבודה כמעט שאינם בוחנים את השאלה אם הפרטיות אכן נפגעה, למעט

²⁴ ראו את הספרות המוזכרת לעיל בה"ש 19–20, וכן את עמדת קבוצת העבודה של ה-GDPR (Opinion 2/2017 on Data Processing at Work (17/EN WP 249) (June 8, 2017) <http://bit.ly/3lS7oSg> (להלן: Opinion 2/2017)).

²⁵ ראו Mathew Finkin, *Privacy and Autonomy*, 21 EMP. RTS. & EMP. POL'Y J. 589, 615 (2017); Ibo Van De Poel, *Core Values and Value Conflicts in Cybersecurity: Beyond Privacy v Security*, in THE ETHICS OF CYBERSECURITY 45, 54 (2020).

²⁶ ROBERT J. STEINFELD, COERCION, CONTRACT, AND FREE LABOR IN THE NINETEENTH CENTURY 1–28 (2001).

²⁷ ראו SIMON DEAKIN & FRANK WILKINSON, THE LAW OF THE LABOUR MARKET, ch. 5 (2005); Brian Langille, *Labour Law's Theory of Justice*, in THE IDEA OF LABOUR LAW 104 (Guy Davidov & Brian Langille eds., 2011). ראו גם את המאמרים אצל Brian Langille ed., CAPABILITY APPROACH TO LABOUR LAW (2019).

²⁸ נציין כי כאשר אין מדובר בטכנולוגיות חדשות, יש לעיתים מקום לחשיבה מורכבת יותר על הזכות לפרטיות שבו בלבד עם ריסון כוח המעסיק גם פותחת מרחב אינטימי, תומך שיש בו אמון, שבו העובדת והעובד ירגישו בנוח (ולא רק מחויבות) לחשוף מידע פרטי אודותיהם לפני המעסיק. מקרים אלה כוללים גילוי דבר היריון, מוגבלות או קושי אחר – בריאותי ואישי – שעשוי להשפיע על העבודה.

²⁹ ראו למשל את הדיון במאמרים המוזכרים לעיל בה"ש 20.

יצירת הבחנה קלה ולא מספקת בין מרחבים טכנולוגיים שונים שבהם מבוצעת הפעילות (למשל סוגים שונים של תיבות דוא"ל) ובין מידע פרטי למידע עסקי. כאשר יש גישה למידע פרטי, הנחת בתי הדין היא שמדובר בפגיעה בפרטיות, ולא הועלתה השאלה אם מידע שמסווג כעסקי הוא אכן כזה ואם הוא עשוי להיות פרטי. כמו כן אין דיון מעמיק באופן שבו הטכנולוגיה עצמה פוגעת בפרטיות, אם בכלל. כפי שנטען, יש חשיבות רבה בהגדרת הפגיעה בפרטיות לא רק כדי להבין לעומק על מה בדיוק ניתנת ההגנה, אלא גם לצורך יישומם של העקרונות והמבחנים האחרים שאומצו בפסיקה.

המחקר אף מראה כי מבחן ההסכמה נדון אחרת בהקשרים שונים, וניתן לו משקל רב, דבר שהוא מפתיע נוכח אמירות, הן בהלכת איסקוב ענבר והן בהלכות נוספות, על משמעותה של הסכמה ביחסי עבודה שבהם הצדדים אינם זהים מבחינת כוח המיקוח שלהם, וכאשר לעובדים כפיפות אינהרנטית למעסיק. שני אלה מפחיתים מיכולתם של העובדים להביע אי-הסכמה (או במילים אחרות לסרב). מלבד זאת, המשקל שניתן לשאלת ההסכמה בעייתי בעידן של טכנולוגיות חדישות שבהן יש קשיים אמיתיים לתת הסכמה מלאה, הן בשל מורכבותו של המידע הטכנולוגי והן בשל הבאת המידע ובקשת ההסכמה בדרך הדומה לאופיו של חוזה אחד. קשיים אלה מובילים לכך שהכוח בניהולה וביישומה של הטכנולוגיה מצוי בידי המעסיק, דבר שאף מגביר את הפרוגטיבה הניהולית שלו.³⁰ האיחוד האירופי אף הוא קבע כי יש לתת משקל קטן לשאלת ההסכמה בכל הנוגע לאיסוף מידע על עובדות ועובדים ולשימוש בו.³¹ לפיכך אנו נטען כי אין לתת להסכמת העובד את המשקל הנכבד שניתן לה, וכי הדגש צריך להיות על העקרונות האחרים. כמו כן נחדד שיש להרחיב את ההגנה הקוגנטית על פרטיות בעבודה.

הניתוח מעיד גם שיש קושי ביישומם של המבחנים החוקתיים והמנהליים שאימצה הפסיקה. כך למשל בכל הנוגע לעקרון המידתיות, המחקר שלנו מראה שבתי הדין לעבודה כמעט שאינם מביאים בחשבון את האפיונים הספציפיים של הטכנולוגיות הנדונות ואינם בוחנים לעומק אם הן עומדות בדרישת המידתיות. אין ניכרת בפסקי הדין התעמקות בטכנולוגיה עצמה, ואין מועלות בהם שאלות הנוגעות לאופן שבו הטכנולוגיה אוספת את המידע, למקורות איסוף המידע, לעיבוד המידע ולדרך הסקת המסקנות, כמו גם לאופן שבו המידע מופץ. מלבד זאת, הפסיקה כמעט שאינה מייצרת הבחנות בין מטרות שונות לשימוש בטכנולוגיה (הגנת סייבר, מעקב, ניהול עובדים, ניהול פגישות מרחוק וכד') אלא בכל הנוגע לשאלה אם מדובר במטרה לגיטימית. היא אף אינה עושה הבחנות בין עסקים שונים (עסקים גדולים או קטנים, חשיבות השימוש בטכנולוגיה בעסקים אלה ועוד), כפי שראוי שתעשה. הגדרת התכלית של השימוש בטכנולוגיה היא מהותית ככלל לשאלת לגיטימיות הפגיעה בפרטיות, אך היא מהותית אף לבחינת המבחנים האחרים, למשל לצורך יישום מבחן צמידות המטרה. חוסר הגדרתה במפורש עשוי לשמש אחד ההסברים

³⁰ Valerio De Stephano, *Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection* (ILO working paper No. 246, 2018); Brishen Rogers, *The Law & Political Economy of Workplace Technological Change*, 55 HARV. C.R.-C.L. L. REV.1 (2020).

³¹ Opinion 2/2017, לעיל ה"ש 24.

לממצא שיוצג במאמר – כי בתי הדין לעבודה ממעטים ליישם את מבחן צמידות המטרה על אף חשיבותו הרבה. גם מבחן השקיפות והדרישה לקביעת מדיניות דורשים, לגישתנו, בחינה מחודשת. ההנחה המונחת כעת בבסיס מבחן השקיפות היא כי מתן מידע על מדיניות המעסיק תאפשר לעובד לסרב לה או להביע עמדתו כלפיה. בשל הביקורת שנעלה בעניין מבחן ההסכמה, נראה כי מטרתו של מבחן השקיפות צריכה להיות שונה, כפי שנפרט במאמר זה וכפי שעולה מדרישות השקיפות הקיימות בדין האירופי.

הטענה הנוספת שנעלה בעקבות הממצאים היא שהפרדיגמה הקיימת כיום במשפט העבודה קובעת כללים שמיושמים לרוב אקס פוסט ולא אקס אנטה. על המשפט בישראל – בין שזה המחוקק ובין שאלה בתי הדין לעבודה – לפעול לשמירה על הפרטיות לכל אורך חיי העבודה. כיום ההגנה על הפרטיות נעשית לרוב כאשר הדבר נדון בהקשר של גילוי מסמכים וקבילות ראיות, כאשר פעמים רבות המידע הפרטי כבר מצוי בידי המעסיק, אשר לא הקפיד על הגנת הזכות באופן שוטף ובמידה מספקת. הסדרה שכזו יכולה להיעשות בידי המחוקק, דרך אימוץ כללים ברורים יותר בנוגע לפרטיות בעבודה והחלת דרישות של אחריותיות המעסיק (accountability), או בבתי הדין לעבודה, שיכולים: א. לקבוע פיצויים גבוהים על הפרת הזכות לפרטיות; ב. למנוע מתן סעד למעסיקים שאינם מגינים באופן שוטף ובמידה מספקת על הזכות לפרטיות בעבודה.

המאמר בנוי כך: פרק א יציג את הלכת **איסקוב ענבר**. הוא יתאר את עובדות פסק הדין ואת ההלכה שנקבעה; פרק ב יציג את המתודולוגיה שאימצנו לניתוח פסקי הדין; פרק ג יציג את ממצאי המחקר האמפירי; פרק ד יעלה לדיון קשיים ביישומה של הלכת **איסקוב ענבר**, כפי שאלה תוארו בקצרה במבוא זה, אגב התייחסות לתאוריות של פרטיות, של דיני העבודה והפניה מועטה לדין האירופי; פרק ה יסכם.

א. הלכת איסקוב ענבר

בפסק דין **איסקוב ענבר** דן בית הדין הארצי לעבודה במאוחד בשני ערעורים – בעניין **איסקוב ענבר** (ע"ע 90/08) ובעניין **אפיקי מים** (312/08) – שעסקו בשאלת כשירותן הראייתית של תכתובות שנלקחו מתיבת דוא"ל שסופקה במקום העבודה. נוסף על זה דן בית הדין הארצי בהסכם קיבוצי כללי שנחתם בין ההסתדרות הכללית החדשה לבין לשכת התיאום של הארגונים הכלכליים, שבמסגרתו נקבעו עקרונות לשימוש שעושה העובד במחשב במקום העבודה.

פרשת **איסקוב ענבר** עסקה בתביעת המערערת לפיטורים שלא כדין במהלך היריון. המחלוקת נגעה למועד כניסת הפיטורים לתוקף. המעסיקה צירפה התכתבויות דוא"ל ששלחה איסקוב ענבר לתמיכת טענתה שהמערערת עסקה בחיפוש מקום עבודה חלופי עוד טרם ההודעה על ההיריון. בית הדין האזורי לעבודה בתל אביב קיבל את הגשת תכתובות הדוא"ל כראיה בקובעו שהמערערת נתנה הסכמה מכללא לחדירה לתיבת הדוא"ל שלה במקום העבודה. הנימוקים שניתנו לקביעתו של בית הדין האזורי כללו את העובדה שהתיבה ניתנה לצורכי עבודה, כי העירוב של הודעות פרטיות ומקצועיות נעשה

בידי העובדת, וכן שהמעסיקה יידעה את העובדים שהיא מבצעת ניטור של תיבות הדוא"ל מעת לעת.³²

בפרשת **אפיקי מים** הביע בית הדין האזורי לעבודה בנצרת עמדה הפוכה. לפי בית הדין, מכיוון שחדירה של המעסיקות לתכתובת הדוא"ל הפרטית של עובד באמצעות השרת שלהן או מציאתה בחיטוט בפח האשפה והגשתה כראיה, הם פגיעה חמורה בפרטיותו, הרי שכל עוד לא ויתר העובד במפורש על ציפייתו הסבירה לפרטיות ולמניעת גישה לתיבת הדוא"ל שלו במקום העבודה, אין לראות בו מי שהסכים מכללא למסירת המידע למעסיק. בית הדין האזורי קיבל את בקשת העובד שלא לקבל תכתובת דוא"ל שהגישו המעסיקות לתמיכה בתביעתן על נזקים כספיים ואחרים שגרם להן העובד.³³

בערעור לפני בית הדין הארצי לעבודה התקבל ערעורה של איסקוב ענבר, וקבילותן של תכתובת הדוא"ל נפסלה,³⁴ ונדחה ערעור המעסיקות בעניין **אפיקי מים**.³⁵ הנחת המוצא שקיימת בפסק דינו של בית הדין הארצי היא שלמחשב במקום העבודה יש ממד אישי של המשתמש. לעיתים תכופות הממד האישי הוא עיקר העיקרים לבעליו, בהיותו חולש על מרחב המחיה המוחשי והמטאפיזי של המשתמש. זאת, נוכח ייחודה של הפעילות במחשב שלא אחת היא בבחינת עדות ממקור ראשון ושותפות למצבים ולאירועים בעלי חשיבות אישית ואינטימית. זהו מידע פרטי השייך לעובדת ולעובד ומוגן בזכות החוקתית לפרטיות. כפי שאמרה השופטת נילי ארד: "בהיות המחשב 'המגירה האישית של בעליו' המכילה מידע כמוס, פרטי ואישי, נחשבת חדירה בלתי מורשית למחשב 'כחיטוט בחפציו האינטימיים' של בעליו, ופלישה לטריטוריה זו מהווה פגיעה בזכותו החוקתית לפרטיות".³⁶ במקביל, פסק הדין מחדד כי זכות הקניין של המעסיק במקום העבודה והפררוגטיבה הניהולית שלו מקימות לו זכות להגן על רכושו הפיזי והווירטואלי האצור ברשת. לכן המעסיק רשאי לנקוט אמצעים מוגברים של אבטחת המידע שנצבר ברשת, הנקלט בה והיוצא ממנה. במסגרת זו רשאי המעסיק לפקח על פעילותם של העובדים כדי לוודא שלא יעשו שימוש לא מורשה, או לא חוקי, בכלי העבודה הווירטואלי ובמידע המופקד בידם. כמו כן רשאי המעסיק לדרוש מן העובדים כי יקדישו זמנם לעבודה ולא יסטו ל"שדות זרים" הפזורים לרוב על פני הרשת הווירטואלית העולמית, בין היתר על דרך קביעת האסור והמותר בשימושים שהעובדים עושים בסביבת העבודה הממוחשבת.

פסק הדין מבקש לאזן בין זכות העובד לפרטיות ובין זכותו הקניינית והפררוגטיבה הניהולית של המעסיק. הוא עושה זאת, בין השאר, תוך בחינת השאלה מתי הפרטיות נפגעת וכן באימוץ עקרונות נוספים. בחינת השאלה מתי הפרטיות נפגעת נעשית בבית הדין אגב סרטוט קו הגבול בין רכושו של המעסיק לבין המרחב הווירטואלי הפרטי

³² ע"ב (אזורי ת"א) 10121/06 **איסקוב ענבר** – הממונה על חוק עבודת נשים (נבו 15.7.2007).

³³ ע"ב (אזורי נצ) 1158/06 **אפיקי מים** – אגודה חקלאית שיתופית לאספקת מים בבקעת בית שאן בע"מ נ' פישר (נבו 9.4.2008).

³⁴ פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 72 לפסק דינה של השופטת ארד.

³⁵ שם, בפס' 88.

³⁶ שם, בפס' 6.

והאישי של העובד באמצעות ההבחנה בין תיבת דוא"ל חיצונית-פרטית שבבעלות העובד לבין תיבות דוא"ל שהמעסיק מקצה לעובד. את תיבות הדוא"ל שהמעסיק מקצה לעובד מחלק בית הדין לסוגים האלה: תיבה מקצועית, המיועדת לצורכי עבודה בלבד ואסורה לשימוש אישי של העובד; תיבה מעורבת, המיועדת לצורכי עבודה, אך המעסיק מתיר לעובד לקיים בה תכתובת אישית; תיבה אישית, שהועמדה לרשות העובד לצרכיו האישיים בלבד. בית הדין מייצר הבחנה גם בין מידע עסקי המצוי בתיבות לבין מידע פרטי. כנקודת מוצא בית הדין מסכים כי מעסיק רשאי לנטר פעילות עסקית אך אינו רשאי לגשת אל מידע פרטי. בתוך כך קובע בית הדין את המסגרת הנורמטיבית הבאה:³⁷

ראשית, על המעסיק להנהיג **מדיניות ברורה** במקום העבודה בכל הנוגע להקצאת מרחב וירטואלי בשימושי המחשב במקום העבודה וניהול תיבות דוא"ל במקום העבודה. על המעסיק לקבוע בבירור את ההבחנה בין המרחב הווירטואלי והטכנולוגיות הווירטואליות המיועדות לצורכי עבודה, לבין המרחב הווירטואלי והטכנולוגיות העומדות לרשות העובד גם לצרכיו האישיים. המעסיק צריך ליידע את העובדים בבירור בדבר המדיניות. כמו כן בית הדין קובע כי על המעסיק לתת ביטוי מפורש למדיניות בחוזה האישי עם העובד, וכי ראוי שהמדיניות תגובש בהסכמת העובדים על דרך של הסכם או הסדר קיבוצי.

שנית, בכפוף לתנאים שנקבעו בפסק הדין, המעסיק רשאי לקיים פעולות ניטור ומעקב אחר נתוני תקשורת ותוכן **בתיבה המקצועית**, למעט מקרים שבהם מדובר בתכתובת אישית. אם מדובר בתכתובת אישית שאסור לקיימה בתיבה מקצועית, המעסיק רשאי להיכנס לתכתובת רק בהתקיים תנאים חריגים המצדיקים זאת וכפוף להסכמה מפורשת, מראש, מדעת ומרצון חופשי של העובד.

שלישית, בשונה מהתיבה המקצועית, המעסיק אינו רשאי לקיים פעולות מעקב אחר תכתובת בתיבה האישית או בתיבה מעורבת שהוא הקצה אותה, אלא בהתקיים נסיבות חריגות המצדיקות זאת וכפוף לעקרונות ולתנאים שנקבעו בפסק הדין, וכפוף להסכמת העובד. דרישת ההסכמה משתנה לפי סוג התיבה: כשמדובר **בחדירה לתיבה המעורבת** נדרשת הסכמתו הספציפית של העובד לכל פעולת חדירה של המעסיק לתוכן התכתובת האישית שלו, בשונה מתכתובתו המקצועית באותה תיבה; אשר ל**תיבה האישית**, נדרשת הסכמתו הספציפית והמפורשת של העובד, מרצון ומדעת, לכל פעולה ופעולה שבכוונת המעסיק לנקוט, לרבות ניטור ספציפי ומעקב הכולל חדירה לתיבה האישית לשם קבלת נתוני תקשורת ותוכן, וחדירה לתוכן תכתובת הדוא"ל האישי של העובד ועיון בה, וכיוצ"ב.

רביעית, המעסיק אינו רשאי לקיים פעולות מעקב וניטור אחר **התיבה החיצונית-פרטית** שבבעלות העובד. התיבה הפרטית, על יישומיה והתכתובת שבה, היא רכוש הפרטי של העובד, כמוה כמכוניתו או ביתו. כשהמעסיק סבור שהתקיימו נסיבות המצדיקות פעולות מסוג זה, עליו לפנות לבית הדין בבקשה לסעד מסוג "צו אנטון פילר" לחיפוש ולתפיסה בתיבה הפרטית, לפי העניין.

שם, בפס' 54.

כד בכד עם בחינת השאלה מתי מדובר בפגיעה בפרטיות, בית הדין קובע כי ההגנה על המידע הפרטי כפופה להסכמת העובד וכן לעקרונות תום לב, גילוי, שקיפות, לגיטימיות, מידתיות וצמידות המטרה. מדובר במבחנים מצטברים, שהיעדר אחד מהם עולה כדי פגיעה בזכות. להלן פירוט העקרונות והדרישות שנקבעו בפסק הדין:

דרישת ההסכמה: כפי שניתן לראות מהדיון שהתקיים למעלה, גם כאשר יש מידע פרטי בתוך תיבה מקצועית או מעורבת נדרשת הסכמה של העובד למסירת המידע לידי המעסיק. בהתייחס לסעיף 1 לחוק הגנת הפרטיות, וכדי לקיים את דרישת ההסכמה, בית הדין קובע כי ההסכמה תינתן מראש, מדעת ומרצון חופשי, הן באשר למדיניות הכללית הנוגעת אצל המעסיק בנושא, והן הסכמה ספציפית באשר לפעולות מעקב וחדירה לתכתובת אישית. ואולם, בית הדין גם מאפשר גישה למידע פרטי במשורה וללא הסכמה בהתקיים תנאי הסף המצטברים האלה: 1. שהחדירה למידע הפרטי תיעשה במקרים חריגים, וכאשר יש חשש רציני או ביסוס סביר לפעילות פלילית או other wrongdoings מצד העובד; 2. לא תותר חדירת המעסיק לתכתובת דוא"ל אישית של העובד, אלא אם המעסיק מילא אחר התנאים המוקדמים, של הבאת המדיניות הנוגעת לידיעת העובדים, כפי הנדרש ממנו על פי עקרונות תום הלב, השקיפות, המידתיות, הסבירות וצמידות המטרה; 3. מכוח עקרונות הלגיטימיות והמידתיות יידרש המעסיק לחדירה לתכתובת הדוא"ל האישית של העובד רק לאחר שמוצו כל אפשרויות המעקב, כגון מעקב באמצעות זיהוי נתוני תקשורת או אמצעים חלופיים אחרים שפגיעתם בזכויות לכבוד ולפרטיות של העובד פחותה.

עקרון הלגיטימיות ועקרון צמידות המטרה: עקרון הלגיטימיות נשאב מהזכות לפרטיות ומהפרשנות להגנות החלות בחוק הגנת הפרטיות ומחובות תום הלב וההגינות ומתקנת הציבור החלה ביחסי עבודה. העיקרון מגדיר את תכלית המעקב אחר נתוני תקשורת ואת תוכן והנסיבות שבהן ייעשה שימוש במידע שהפיק המעסיק מחדירתו לתכתובת הדוא"ל האישית של העובד. עקרון הלגיטימיות כולל דרישה להגבלת איסוף המידע במעקב למטרות חיוניות למקום העבודה והגבלת השימושים אשר ייעשו בהמשך באותו מידע. בהתקיים נסיבות חריגות ויוצאות דופן, שיש בהן כדי לגרום פגיעה חמורה באינטרסים של המעסיק או של מקום העבודה, כגון התנהלות פלילית של העובד או התנהלות פוגענית אחרת של העובד, יכול שתימצא הצדקה לקיום מעקב וניטור תכתובת אלקטרונית, לרבות מעקב אחר נתוני תקשורת ותוכן של העובד, כפוף לעקרונות הנוספים שנקבעו בפסק הדין. עקרון צמידות המטרה נובע מעקרון הלגיטימיות, והוא נועד להבטיח את השליטה על חדירת המעסיק למידע הפרטי של העובד על דרך הגבלת השימושים שניתן לעשות באותו מידע, באופן ש"מטרת האיסוף הראשונית מוצמדת למידע גם בגלגוליו הבאים".³⁸

עקרון השקיפות: עקרון השקיפות (transparency), החל מכוח חובות תום הלב והגילוי המוגברות ביחסי עבודה, מחייב את המעסיק להביא לידיעת העובדים, בפירוט ובבירור, את המדיניות בדבר שימושי מחשב במקום העבודה ולפרט את הנסיבות

שם, בפס' 20–21, 23.

המצדיקות ניטור כללי ומעקב ספציפי אחר עובד, את טכנולוגיות המעקב ומהותן.³⁹ אומר בית הדין כי "במסגרת עקרון השקיפות ויישומו, יש לכלול בהתקשרות החוזית עם העובד את מדיניות המעסיק בנוגע לשימוש בטכנולוגיות המידע המותקנות במחשב ובסביבת העבודה. מן הראוי הוא כי מדיניות זו תעוגן בתקנון החל במקום העבודה, ובהסכמה עם ארגון העובדים או נציגות העובדים במסגרת הסכם קיבוצי, או הסדר קיבוצי".⁴⁰

עקרון המידתיות: לפי חוק-יסוד: כבוד האדם וחירותו ופרשנותו ביחס לדיני עבודה, עקרון המידתיות נועד לאזן בין הזכויות החוקתיות והאינטרסים של המעסיק והעובד. על פי עקרון המידתיות, יש לבחון: (1) טכנולוגיות חלופיות למעקב הפוגעות במידה הפחותה ביותר בפרטיות העובדים; (2) מהו היחס הראוי בין התועלת שבהגשמת מטרתה הראויה של מדיניות המעקב לבין הנזק והפגיעה בזכויות העובד שנוצרו ממדיניות המעקב. במסגרת שילוב עקרון המידתיות ועקרון הלגיטימיות יש לבחון שהחזירה לתחום הפרט על ידי המעסיק היא לתכלית ראויה, אינה עולה על הנדרש, וכי המעקב מידתי לסיכון שהצדיק קיום המעקב מלכתחילה וחיוני לאינטרס לגיטימי של מקום העבודה.⁴¹

ב. מתודולוגיה ותיאור הנתונים

שאלות המחקר שלנו הן אלה: מהי מידת ההגנה שבתי הדין לעבודה מעניקים מפני פגיעה בזכות לפרטיות העובדים בעידן של טכנולוגיות חדשות, ומהן ההשלכות המשפטיות שהמעסיק חשוף להן מפגיעה בפרטיות עובדיו. כדי לבחון שאלות אלה חקרנו כיצד בתי הדין לעבודה יישמו ופיתחו את הלכת **איסקוב ענבר** מאז התקבלה בשנת 2011. המתודה המרכזית שבה השתמשנו היא ניתוח איכותני של פסקי הדין. נעזרנו בשיטת ניתוח תוכן קלאסי, שיטה המפעילה פרוצדורות כדי לבצע היסקים תקפים מתוך טקסט.⁴² לפי התאוריה והנסיבות המתוארות במבוא בנינו מסגרת קידוד (קטגוריזציה של הנתונים הגולמיים) וכללים שלפיהם ניתחנו את הטקסט של פסקי הדין וההחלטות אגב בדיקת מהימנות כללים אלו ושינויים ותיקונם כמתבקש. באמצעות שיטה זו קיבלנו הן תיאורים מספריים של תכונות מסוימות שעלו בפסקי הדין שבדקנו והן ממצאים על דפוסים ועל הבדלים שהבחנו בהם בפסקי הדין.

בפרק זה נציג את מסגרת המחקר שערכנו ואת הקווים הכלליים שהנחו אותנו בקידוד פסקי הדין.

1. בניית מאגר פסיקה

לצורך המחקר בנינו מאגר פסיקה שכולל 51 פסקי דין. פסקי הדין נבחרו לאחר חיפוש במאגר המשפטי "נבו" (www.nevo.co.il), אשר העלה כי עד חודש נובמבר 2020

³⁹ שם, בפס' 24–25.

⁴⁰ שם, בפס' 24.

⁴¹ שם, בפס' 22.

⁴² מרטין ו' באואר וג'ורג' גאסקל **מחקר איכותני: שיטות לניתוח טקסט, תמונה וצליל** 151–174 (אורית פרידלנדר מתרגמת, דוד לויין ומוטי רגב עריכה מדעית של המהדורה העברית 2011).

התקבלו בבתי הדין לעבודה 83 פסקי דין והחלטות ביניים שאזכרו את פסק הדין **איסקוב ענבר**. מתוכם בחרנו רק את אלה שעסקו בזכות לפרטיות במקום העבודה. מדובר ב-51 החלטות ופסקי דין (ראו את מספרי ההליכים בנספח מס' 1), שאותם ניתחנו.

בחרנו לתחום את המדגם שלנו להחלטות ופסקי דין שהתקבלו בבתי הדין לעבודה (אף שיש פסקי דין של בית המשפט העליון ושל בתי המשפט המחוזיים שהזכירו את ההלכה), שכן בתי דין אלו הם שמיישמים את ההלכה תדיר, כשהם עוסקים יום-יום במערכת היחסים הייחודית של עבודה. ייתכן שיש בכך חסרונות, שכן כפי שנראה בהמשך, בתי הדין לעבודה בוחנים את הזכות בעיקר בהקשר הפרוצדורלי שנוגע לגילוי מסמכים וקבילות ראיות, ופחות בעניין המהותי של הפגיעה בפרטיות כעולה נזיקית, ואולם עדיין מדובר בערכאה שאמורה להיטיב להבין את ייחודיותו של ההקשר של עבודה יותר מבתי המשפט האחרים ולפתח את הדין בהתאם. פסק דין **איסקוב ענבר** עסק בנושאים נוספים, כגון הגדרת זכות הקניין של המעסיק ותוקפו של כתב ויתור.⁴³ מכיוון שבחרנו להתמקד בזכות לפרטיות, פסקי הדין וההחלטות שלא עסקו במישורין בזכות לפרטיות "נפסלו". לפיכך מאגר הפסיקה שיצרנו מייצג את ההחלטות ואת פסקי הדין שפורסמו הרלוונטיים לשאלת המחקר שלנו עד למועד שבו ביצענו את החיפוש.

מתוך פסקי הדין וההחלטות שעוסקים בפרטיות, רק שני פסקי דין התקבלו בבית הדין הארצי לעבודה,⁴⁴ והיתר בבתי הדין האזוריים, מרביתם (37 פסקי דין והחלטות) התקבלו בבית הדין האזורי לעבודה בתל אביב, 3 פסקי דין והחלטות בבית הדין האזורי בנצרת, 1 בירושלים, 6 בחיפה ו-2 בבאר שבע.

הקידוד של פסקי הדין נעשה, בין השאר, על פי סוג הסעד המבוקש. קידוד זה העלה כי סוגיות הנוגעות לזכות לפרטיות נעשו בכל הנוגע לאלה: (1) גילוי מסמכים – בקשות לגילוי ועיון במסמכים הכרוכות בפגיעה בפרטיות, כגון בקשה לנטר התכתבויות דוא"ל של עובד ובקשה לעיין במחשבו (17 פסקי דין);⁴⁵ (2) בקשות לפסילת ראיות בטענה שהתקבלו אגב פגיעה בפרטיות (20 פסקי דין);⁴⁶ (3) פיצויים – בקשות לפיצוי בגין פגיעה בפרטיות (13 פסקי דין);⁴⁷ (4) הסדרת פרקטיקה – מקרים שבהם המעסיק מבקש להנהיג

⁴³ פרשת **איסקוב ענבר**, לעיל ה"ש 2.

⁴⁴ ראו ע"ע (ארצי) 40711-04-17 **פישר תעשיות פרמצבטיות בערבון מוגבל – שטר** (נבו 4.3.2018); פרשת **עיריית קלנסווה**, לעיל ה"ש 1.

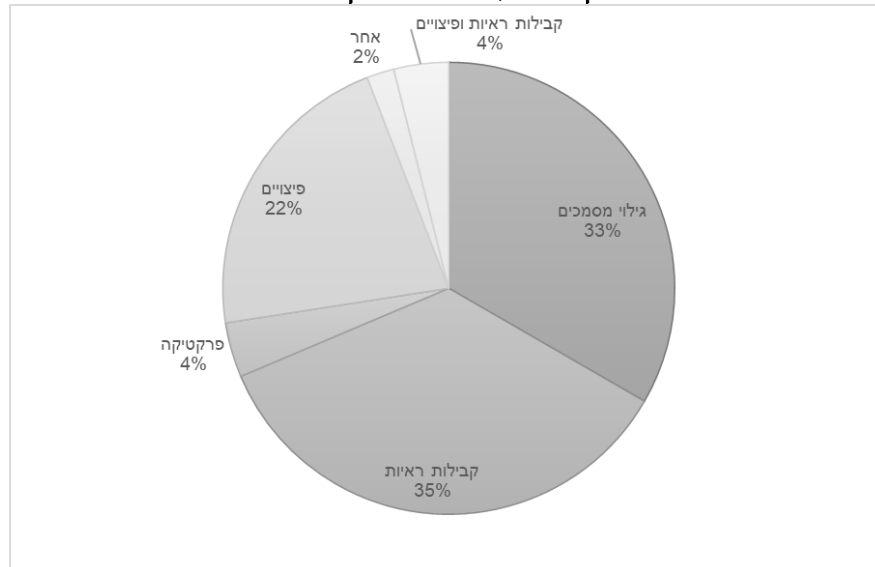
⁴⁵ בכמה פסקי דין צוין כי הכללים שנקבעו בפרשת **איסקוב ענבר**, לעיל ה"ש 2, אינם מתאימים בהקשר לגילוי מסמכים, כי אז המבחן המרכזי הוא מבחן הרלוונטיות, ויש לשקול באופן פרטני את אינטרס הגילוי במונחי הוגנות, יעילות וקידום חקר האמת לעומת אינטרס הפרטיות. ראו פרשת **שטר**, לעיל ה"ש 44, בפס' 13 לפסק דין, והדיון בדרישת המדיניות להלן.

⁴⁶ מתוכם שני פסקי דין עסקו הן בבקשה לפסילת ראיות והן בבקשה לפיצוי בגין פגיעה בפרטיות, ולכן אלו נספרו בשתי הקטגוריות.

⁴⁷ לרבות במסגרת טענה ליחסי עבודה פוגעניים. כך לדוגמה בעניין סע"ש (אזורי ת"א) 21426-11-16 **מנשה – אודיס מפעלי סינון בע"מ** (נבו 16.1.2019), במסגרת תביעה לפיצוי לא ממוני בשל העסקה פוגענית, נטען כי הנתבעת פגעה בפרטיות התובע (עובד לשעבר) מכיוון שניטרה התכתבויות הדוא"ל של עובדיה.

הסדר מובנה הכרוך בפגיעה בפרטיות (2 פסקי דין);⁴⁸ (5) אחר – כאשר לא נתבע סעד מוגדר בקשר להגנה על הפרטיות (פסק דין אחד). דבר זה מעלה את מה שצינינו קודם, כי הדיון בבתי הדין לעבודה בזכות הוא בעיקר פרוצדורלי ופחות מהותי, ממצא בעייתי בפני עצמו בשל הפגיעה בפרטיות המתחוללת מדי יום בעולם העבודה.

דיאגרמה 1. אזכור הלכת איסקוב ענבר, לפי סעד מבוקש

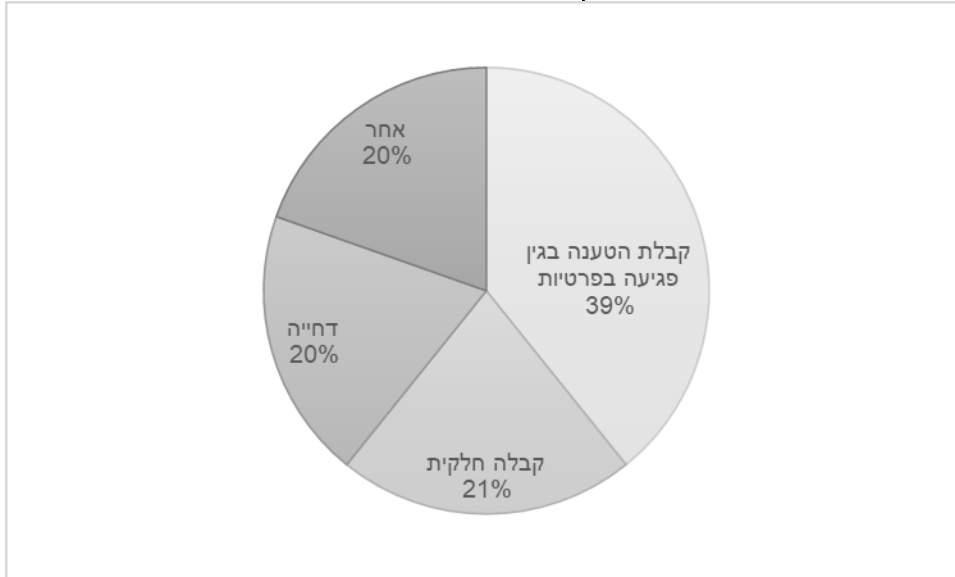


מסיווג פסקי הדין עולה כי במרבית המקרים (63%) בית הדין דן במקרה לאחר שהפגיעה בפרטיות כבר נעשתה. המקרים שבהם הפגיעה בפרטיות נבחנה "אקס אנטה" (37%), אירעו בהליכים שבהם ביקש המעסיק את גילוי המסמכים מראש בבית הדין (בניגוד לשימוש בהם בדיעבד) וכן במקרים שבהם המעסיק ביקש להנהיג הסדר מובנה הכרוך בפגיעה בפרטיות (כמו למשל הטמעת מערכת נוכחות באמצעות שרון ביומטרי). יצוין כי במסגרת אותם המקרים שבהם הפגיעה בפרטיות נבחנה "אקס אנטה" עלתה לא אחת הטענה מצד העובד כי מכיוון שלמעסיק יש גישה חופשית למידע המצוי במחשבו ובתיבת הדוא"ל שבבעלותו, סביר כי המעסיק כבר צפה במסמכים המבוקשים בגילוי

⁴⁸ בפרשת **עיריית קלנסווה**, לעיל ה"ש 1, דן בית הדין בשאלה אם ניתן לחייב עובדים למסור טביעת אצבע לשם רישום שעות בשעון נוכחות ביומטרי. בעניין ס"ק (אזורי ת"א) 19-06-2019 **הסתדרות העובדים הכללית הסתדרות עובדי המדינה – מדינת ישראל** (נבו) 8.10.2020. דן בית הדין בנוהל שהמדינה התקינה שעניינו "תפיסת ניהול לתפעול מערכת לאיכוון ורישום נסיעות ברכב ממשלתי". יצוין כי בעס"ק (ארצי) 46575-10-20 **הסתדרות העובדים הכללית הסתדרות עובדי המדינה – מדינת ישראל** (נבו) 9.3.2021 (להלן: עס"ק **הסתדרות העובדים הכללית**), בית הדין הארצי לעבודה נתן תוקף של פסק דין להסכמת הצדדים לביטול פסק דינו של בית הדין האזורי לעבודה מיום 8.10.2020.

המסמכים. קרי, שהפגיעה בפרטיות כבר התרחשה. עם זאת סיווגנו מקרים אלו כ"אקס אנטה" לפי סוג ההליך והסעד המבוקש.

דיאגרמה 2. תוצאות יישום הלכת איסקוב ענבר



בבחינת תוצאות ההחלטות ופסקי הדין⁴⁹ עלה כי ב-20 מקרים קיבלו בתי הדין את הטענה לפגיעה בפרטיות ופסקו בגין זה סעד. ב-11 מקרים קיבלו בתי הדין חלקית את טענת העובד לפגיעה בפרטיות. דוגמה לקבלה חלקית היא כאשר בית הדין התיר ניטור תיבת דוא"ל מקצועית אך דחה ניטור תיבת דוא"ל פרטית במסגרת הליכי גילוי מסמכים.⁵⁰ ב-10 מקרים נוספים נדחתה הטענה בגין פגיעה בפרטיות, כאשר ב-9 מתוכם קבע בית הדין כי לא הייתה כלל פגיעה בפרטיות, או שהפגיעה בפרטיות זניחה. לקטגוריה "אחר" נכנסו מקרים שבהם בית הדין דן בסוגיית הפרטיות אך לא הכריע בה, ולכן לא היה אפשר לסווגם לקטגוריות האחרות.

כמו כן מצאנו שמתוך כלל ההליכים שנבדקו בית הדין פסק פיצויים בגין פגיעה בפרטיות ב-6 מקרים, בסכומים הנעים בין 4,000 ש"ח ל-50,000 ש"ח. יש לציין כי עד היום לא הוכרה זכותו של עובד לתבוע תביעה נזיקית על הפרת זכותו לפרטיות מכוח חוק הגנת הפרטיות בבתי הדין לעבודה. בכמה וכמה פסקי דין אזוריים נקבע כי בית הדין אינו מוסמך ליתן סעד בתביעה שעילתה בחוק הגנת הפרטיות, הואיל ולבתי הדין לעבודה, ככלל, אין סמכות לדון בתביעות נזיקיות, כאשר פגיעה בפרטיות היא עוולה נזיקית לפי

⁴⁹ ראו את מספרי ההליכים בסיווג לפי תוצאות בנספח למאמר.

⁵⁰ ס"ש (אזורי ת"א) 14400-03-13 ברמן – אקספיריורס בע"מ (נבו 30.3.2017).

סעיף 4 לחוק הגנת הפרטיות.⁵¹ עם זאת נפסק כי היעדר הסמכות הוא במסגרת תביעה נזיקית בלבד. במקרים שבהם נפסק פיצוי, בתי הדין ראו בו פיצוי על בסיס הפרת חוזה, באומרים כי הקפדה על פרטיות העובד היא תנאי משתמע בכל חוזה עבודה.⁵²

2. שיטת המחקר

בניתוח ההחלטות ופסקי הדין בחנו את האופן שבו בתי הדין מיישמים את המבחנים המשפטיים ואת העקרונות שנקבעו בפסק דין **איסקוב ענבר**. בחנו את האופן שבו בתי הדין הגדירו פגיעה בפרטיות וכן את ששת המבחנים והעקרונות הנוספים: (1) הסכמה, (2) לגיטימיות, (3) מידתיות, (4) צמידות המטרה, (5) שקיפות ו- (6) קביעת מדיניות. יצוין כי יישום המבחנים והעקרונות תלוי במידה רבה בנסיבות ההליך המובא לפני בית הדין, בזהות הצדדים להליך, בשנת קבלת פסק הדין ובערכאה הרלוונטית. לפיכך ניתוח פסקי הדין נעשה בשיטות המשלבות קידוד וניתוח תוכן איכותני. כל הנתונים קודדו לאחר קריאה מעמיקה של פסק הדין ונסיבותיו.

את שאלת המחקר חילקנו לכמה תתי-שאלות שהנחו אותנו בניתוח פסקי הדין וההחלטות.

1. אופן יישום המבחנים והעקרונות שנקבעו בהלכת איסקוב ענבר: בבחינת יישום כל מבחן ועיקרון הגדרנו שאלות שהנחו אותנו בניתוח הפסיקה. לדוגמה, במסגרת יישום מבחן המידתיות בחנו מתי בתי הדין מאזכרים את המבחן ומיישמים אותו; אם בתי הדין בחנו טכנולוגיות חלופיות, ואילו צעדים נקטו בתי הדין כדי להקטין את הפגיעה בזכות. ביישום מבחן הלגיטימיות בדקנו אילו תכליות הוכרו בבתי הדין כלגיטימיות לאיסוף מידע ואילו תכליות הוכרו כלגיטימיות לשימוש במידע; אם בתי הדין בחנו את הקשר בין התכלית לבין הפגיעה בפרטיות; אם יתר המבחנים והעקרונות יושמו בצורה שונה על פי כל תכלית ותכלית. בנוגע למבחן ההסכמה בדקנו באיזה אופן בתי הדין לעבודה בוחנים את דרישת ההסכמה וכיצד הם מיישמים את מבחן ההסכמה שנקבע בהלכת **איסקוב ענבר** – הסכמה שניתנת מדעת ומרצון חופשי. בין היתר בדקנו באיזה אופן, אם בכלל, התקבלה ההסכמה: האם במסגרת הסכם ההעסקה? האם התקיים משא ומתן? נוסף על בחינת כל מבחן ועיקרון בנפרד בדקנו אם בתי הדין יישמו את כלל התנאים שנקבעו בהלכת **איסקוב ענבר**, ואם הושם דגש על עקרונות מסוימים יותר מאחרים.

2. התייחסות בית הדין לדרישת התנאים המצטברים: במקרים שבהם בתי הדין הכירו בפגיעה בפרטיות די היה לעיתים ביישום חלק ממבחניה ומעקרונותיה של הפסיקה כדי לקבוע כי הייתה פגיעה בזכות. בהקשר זה בחנו את המבחנים ואת העקרונות

⁵¹ לסקירת פסקי דין אלו, ראו סע"ש (אזורי ת"א) 20739-08-16 חננאל – מועצה מקומית באר יעקב, פס' 254 לפסק הדין (נבו 16.11.2020); ס"ע (אזורי ת"א) 29090-05-12 גורליק – אנבינדר, פס' 29 לפסק הדין (נבו 21.4.2014).

⁵² שם.

שנבדקו וכן את אופן יישומם על פי אותן השאלות שהנחו אותנו בניתוח הפסיקה שתוארו לעיל.

3. השלכות הפגיעה בפרטיות עובדים והגבלותיה: פיתוח הפסיקה תלוי בהליך המובא לפני בית הדין, ובייחוד בסוג הסעד המבוקש. לפיכך בחנו מה היו הסעדים שהתבקשו ומה היו תוצאות ההליך. כמו כן הבחנו אם הפגיעה בפרטיות כבר נעשתה או שמדובר בבקשה לבית הדין והפגיעה בפרטיות נבחנת "אקס אנטה". כפי שנראה בהמשך, חלוקה זו חשובה ביישום הכללים השונים שנקבעו בהלכת איסקוב ענבר. כך לדוגמה דרישת המידתיות מקבלת משמעות שונה כאשר מדובר בבקשה לגילוי מסמכים או בהסדרה מראש של פרקטיקה הכרוכה בפגיעה בפרטיות, שכן אז בית הדין יכול לתור אחר האמצעי שפגיעתו פחותה במסגרת ההליך. לעומת מקרים שבהם הפגיעה בפרטיות כבר נעשתה ובית הדין מתבקש לפסוק פיצויים בגין פגיעה זו. שאלה שעניינה אותנו בהקשר זה היא אם פסיקת בתי הדין יכולה להרתיע מפני פגיעה בפרטיות שלא כדין, ולכן בחנו הן את סכום הפיצויים שנפסקו (כאשר הם אכן נפסקו) בגין פגיעה בפרטיות והשלכות נוספות (כגון השפעה על הסעד המבוקש, ובין השאר פסילת ראיות).

4. אפיון הצדדים להליך: בחנו אם קיימים דפוסיים שונים בסוגי המקרים המובאים לפני בתי הדין, כגון אם מדובר במעסיק פרטי או ציבורי, מהי צורת ההעסקה, אם העובדים מאוגדים, ומהו מקומו של העובד בהיררכיה הארגונית. ההשערה שלנו הייתה כי ככל שתפקידו של העובד בכיר יותר, בתי הדין ייחסו משמעות רבה יותר להסכמה חוזית שניתנה לפגיעה בפרטיותם. גם סברנו כי לעובדים בתפקידים בכירים יותר תהיה אפשרות ממשית להתנגד לשימוש של המעסיק במידע הפרטי עליהם. במעט מקרים הובאו טענות הנוגעות לפגיעה בפרטיות של צדדים שלישיים (עובדים אחרים) ושל המעסיק, והבחנו בין יישומם של כללי הלכת איסקוב ענבר במקרים אלו לבין מקרים שבהם הפגיעה היא בזכות לפרטיות של עובד (או עובד לשעבר) שהוא צד להליך.⁵³ התמקדנו בהליכים שבהם נפגעה הפרטיות של העובדים שהיו צד להליך.

5. הגדרת פגיעה בפרטיות ומידת הפגיעה בפרטיות: בדקנו כיצד בתי הדין מגדירים פגיעה בפרטיות. האם סוג המידע משפיע על בחינה זו?⁵⁴ ההשערה שלנו הייתה כי כאשר מדובר במידע עסקי במהותו, בתי הדין לא יגדירו מידע זה כפרטי ולא יבחנו אותו דרך הכללים של פגיעה בפרטיות.⁵⁵ גם איסוף מידע אנונימי (דרך ניטור) אינו

⁵³ כך לדוגמה בעניין סע"ש (אזורי ת"א) 31869-03-19 הילטון ליכט – ג'ונס לאנג לאסאל ישראל בע"מ (נבו) 14.7.2020, ג'ונס לאנג לאסאל ישראל בע"מ ביקשה להוציא מתיק בית הדין טבלה המציגה משכורות ונתונים נוספים אודות עובדיה, בטענה לפגיעה בפרטיות עובדים אלו.

⁵⁴ דניאל סולוב, למשל, מציע טקסונומיה של פגיעה בפרטיות לפי סוגי מידע שונים. לא כל מידע הינו מידע שצריך להיות מוגדר כפרטי ולא בכל פעם, לכן, עשויה להיות פגיעה בפרטיות. גם מיכאל בירנהק מדגיש את החשיבות שיש לבחינת שאלת הפגיעה בפרטיות. ראו לעניין זה Daniel Solove, *A Taxonomy of Privacy*, 154 PENN. L. REV. 477 (2006); בירנהק "שליטה והסכמה", לעיל ה"ש 11, בעמ' 27.

⁵⁵ זאת, בניגוד להלכה בדין האירופאי שקבעה כי גם מידע עסקי יכול להיות פרטי. ראו Case C-92/09, Volker und Markus Schecke GbR & Hartmut Eifert v. Land Hessen, 2010

בהכרח עולה כדי פגיעה בפרטיות, ואולם תיתכן פגיעה שכזו, ומכאן החשיבות בבחינת שאלת הפגיעה בפרטיות לעומק.⁵⁶ בחנו כיצד בתי הדין הגדירו פגיעה בפרטיות והבחינו בין סוגים שונים של פגיעה בפרטיות, כגון ניטור הודעות דוא"ל לעומת איכון מיקום העובד או מסירת טביעת אצבע לשם רישום שעות בשעון נוכחות ביומטרי. בחלק זה רצינו לבחון אם בתי הדין מתייחסים לפגיעות שונות בחומרה רבה מזו שבה הם מתייחסים לאחרות.

כדי לשמור על מהימנות הקידוד, מרבית פסקי הדין וההחלטות נבחנו וקודדו תחילה בנפרד בידי כל אחת מאיתנו. במקרים שבהם ההתרשמות שלנו הייתה שונה, בחנו שנית את ההחלטה הרלוונטית והגענו להסכמות. לאחר הקידוד הראשוני חידדנו את השאלות המנחות (כמפורט לעיל) ועברנו על פסקי הדין וההחלטות פעם נוספת כדי לאשש את מסקנותינו – בכל הנוגע ל-20 מפסקי הדין של המאגר. לאחר מכן המשיכה גיל עומר לבדה את מלאכת הקידוד והניתוח של יתרת פסקי הדין.

ג. ממצאים

בפרק זה נסקור את הממצאים שעלו מהניתוח שעשינו. יצוין כי ממצאים אלה מספקים תמונה מעניינת על האופן שבו בתי הדין לעבודה מיישמים את הלכת **איסקוב ענבר**, חלקה חיובית מאוד, וחלקה בעייתית. במסגרת הדיון נצביע על כל סוגי הממצאים ונתעמק בקשיים שביישום ההלכה ובפיתוחה. דיון מעמיק בעיקרי הממצאים ובקשיים האמורים ייערך בפרק הבא של המאמר.

1. יישום מבחני הלכת איסקוב ענבר

(א) סוג המידע והגדרת פגיעה בפרטיות בבתי הדין לעבודה

במרבית פסקי הדין וההחלטות שבדקנו סוג המידע שנדון היה התכתבויות דוא"ל (33% מפסקי הדין) או עיון במחשב (22% מפסקי הדין), כאשר עיון במחשב כולל הן עיון במסמכים השמורים במחשב, הן גלישה באינטרנט ממחשב העבודה (עיון בהיסטוריית גלישה) והן עיון בתיבת דוא"ל. נוסף על זה כמה פסקי דין עסקו בהתכתבויות ממכשיר הטלפון הנייד (12%) ובשימוש במצלמות במקום העבודה (6% מפסקי הדין). יתר פסקי

59 || E.C.R. I-11063. בפסק דין זה נקבע שמידע על אנשים שמקבלים הטבות מקרנות אירופאיות הנו אמנם מידע הנוגע לפעילות בעלת אופי מקצועי ואולם הוא כולל מידע פרטי. דבר זה גם נפסק בפסק דינו של בית המשפט העליון בע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' ורדי (נבו 23.1.2013). השערתנו הייתה שונה מהדין האירופאי ומהלכת בית המשפט העליון לאור ההבחנה שבוצעה בפסק דין **איסקוב ענבר** בין מידע מקצועי לבין מידע פרטי.

⁵⁶ לעניין מטא-דאטה ופגיעה בפרטיות, ראו Paula Kift & Helen Nissenbaum, *Metadata in Context – An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, 13 ISJLP 333 (2016). יש לציין בהקשר זה כי בית המשפט העליון ראה בפרשת **בן מאיר** שימוש במגה-דאטה כפגיעה בפרטיות, ראו בג"ץ 2109/20 **בן מאיר נ' ראש הממשלה** (נבו 26.4.2020).

הדין עסקו בסוגים שונים של מידע, כגון איכון מכשיר נייד לאיתור מקום הימצאותו של העובד,⁵⁷ מידע ביומטרי⁵⁸ וגילוי מסמכים רפואיים.⁵⁹

בפסק דין **איסקוב ענבר** סרטט בית הדין את הגבולות בין המרחב הווירטואלי הפרטי של העובד במקום העבודה לבין המרחב שהוא קניינו של המעסיק באמצעות סיווג תיבות דוא"ל (מקצועית, מעורבת, אישית ותיבה חיצונית-פרטית) וכן לפי תוכן ההתכתבות. להבחנות אלו יש השלכות, על פי הלכת **איסקוב ענבר**, על סיווג פעולות מעקב וניטור כפגיעה בפרטיות. מבדיקת פסקי הדין וההחלטות במאגר עולה כי אכן סיווג פעולה כפרטית נעשה בעיקר על פי תוכן ההתכתבות וכן על פי סיווג הפלטפורמה שבה מצוי המידע. קרי, כשמדובר במידע עסקי ובפלטפורמה המשמשת לצורכי עבודה (מסמכים על מחשב בעבודה או תיבת דוא"ל מקצועית), נטייתם של בתי הדין היא לקבוע כי ניטור מידע זה אינו פוגע בפרטיות או שהפגיעה היא ברף הנמוך. לעומת זאת כשמדובר בתוכן שאינו מקצועי ובפלטפורמה שאינה מקצועית (לדוגמה גלישה באתרי אינטרנט שאינם מקצועיים או במידע רפואי על העובד), נטייתם של בתי הדין היא לפסוק כי מדובר בפגיעה בפרטיות.

כך לדוגמה בעניין **מנגלוס** קיבל בית הדין כראיה חוות דעת של מומחה מחשבים שלפיה סמוך לעזיבתם של כמה עובדים, שותפים ועורכי דין במשרד עורכי דין, הם מחקו והעתיקו קבצים רבים מהמחשבים במשרד לענן (דרופבוקס).⁶⁰ בית הדין נימק זאת בכך שלא הוכח כי המומחה פרץ לתיבות דואר אישיות, וכי המומחה טען (טענה שלא נסתרה) כי הגדיר את החיפוש ככזה שיכוון למסמכים הנוגעים ללקוחות המשרד ולא למסמכים פרטיים.⁶¹ דוגמה נוספת היא בעניין **חננאל**, שם פסק בית הדין כי השארת מידע רפואי של עובדת גלוי לעיני כול היא פגיעה אסורה בפרטיות. בית הדין הדגיש כי "מידע אודות מצבו הבריאותי של אדם הוא היבט מובהק ומרכזי של צנעת חייו ומידע שכזה מצוי בליבת הזכות לפרטיות, בעוד גילוי ללא הסכמת בעל המידע, מהווה פגיעה חמורה בפרטיותו".⁶²

בעניין **רמי חי**, מצד אחד קיבל בית הדין בקשה לעיין במסמכים שהעובד, אשר נטען נגדו שגלש באתרים פורנוגרפיים ושמר תמונות של תלמידים שהיו במחשב שלו במהלך העסקתו כחלק מהליך גילוי מסמכים, ומצד אחר לא אפשר עיון בהיסטוריית הגלישה של העובד מכיוון שמדובר בחדירה חמורה למרחב הווירטואלי הפרטי והאינטימי שלו.⁶³ מלבד זאת, בתי הדין מבצעים הבחנה בין מעקב במרחב ציבורי לזה שבמרחב פרטי הן

⁵⁷ לדוגמה בפרשת **שטור**, לעיל ה"ש 44.

⁵⁸ פרשת **עיריית קלנסווה**, לעיל ה"ש 1.

⁵⁹ לדוגמה בפרשת **חננאל**, לעיל ה"ש 51.

⁶⁰ סע"ש (אזורי ת"א) 25953-12-14 **ד"ר שלמה כהן ושות'**, **משרדי עורכי דין – מנגלוס**, פס' 22 לפסק הדין (נבו 18.1.2015).

⁶¹ שם.

⁶² פרשת **חננאל**, לעיל ה"ש 51, בפס' 262 לפסק הדין.

⁶³ סע"ש (אזורי ת"א) 79357-01-19 **רמי חי – ויצו – הסתדרות עולמית לנשים ציוניות (ע"ר)**, פס' 42–43 לפסק הדין (נבו 11.6.2020).

במרחבים הווירטואליים והן במרחבים הפיזיים. בעניין **אברמסון** כחן בית הדין את הפגיעה הנגרמת ממעקב של חוקר פרטי אחר עובד ברשות הרבים (במרחב הפיזי), וקבע כי זו עולה כדי פגיעה קטנה בפרטיות יחסית למעקב בבית פרטי או לעיון בתיבת דוא"ל של עובד שבה הוא כותב את צפונות ליבו בין היתר למקורכיו וליקיריו.⁶⁴ הבחנה דומה נעשתה גם לעניין צילום העובד במרחב הציבורי (כגון צילומי אבטחה בכניסה לבניין), שאז בית הדין פסק כי אין מדובר בפגיעה מובהקת בפרטיות, לעומת צילום בחדר הפרטי שהוא מרחב אישי במקום העבודה.⁶⁵

עם זאת במקרים רבים הבחנה בין העולם המקצועי לעולם הפרטי אינה פשוטה, והדבר מקשה על חידוד הפגיעה בפרטיות. בית הדין בעניין **שטטר** עמד על בעייתיות זו:⁶⁶

האתגרים שמציבות האפשרויות הטכנולוגיות חוצים ענפי משפט. הם לא פסחו, ובמידה רבה ביטויים אף גבר בתחום יחסי העבודה. זאת נוכח הטשטוש הגובר של קו הגבול בין חיי העבודה לחיים הפרטיים – מזה, וריבוי אמצעי התקשורת ובהם מחשבים וטלפונים ניידים אשר גורמים לכך שהמעסיק יכול לפקח על העובדים ולנטרם גם כשאינם נמצאים בחצרי המעסיק. בחלק מהמקרים הטשטוש בין העולם הפרטי והעולם המקצועי ובין רשות הרבים ורשות הפרט מוביל לכך כי מקום העבודה נהפך להיות מרחב נזיל שבו למעסיק יש פוטנציאל פיקוח בכל פעולה בכל נקודת זמן בכל מקום בעבודה ומחוצה לה.

אנו לא מצאנו דיון מעמיק במקרים מעין אלה על אף ההצבעה על הבעייתיות האמורה. כך, מלבד הבחנות כלליות בין הפרטי לבין המקצועי-עסקי בתי הדין כמעט לא דנים בשאלה אם הפרטיות נפגעה. למשל, בתי הדין לא שואלים אם מידע שנאסף באמצעות טכנולוגיות בינה מלאכותית על בסיס מטה-דאטה עולה כדי פגיעה בפרטיות, מה המשמעות של אנונימיות באיסוף המידע ואם ניתן לזהות את בעל המידע, אם יש באיסוף המידע ובעיבודו פגיעה בפרטיות, או שמא רק שמירתו והגישה אליו הם פגיעה שכזו; בתי הדין לא עיצבו כללים בנוגע למידע מעורב – עסקי ופרטי; בתי הדין לא עסקו בשאלה אם מידע הנוגע לתכליות, כגון פגיעה בסודות מסחריים או פתיחת עסק מתחרה, הוא עסקי או פרטי; בתי הדין גם נשענים על ההבחנות בין התיבות השונות כפי שאלו נקבעו בהלכת **איסקוב ענבר**, בלי לבחון בהכרח לעומק אם המידע הרלוונטי שנדון הוא פרטי או עסקי.⁶⁷

⁶⁴ ס"ע (אזורי י"ם) 50814-01-12 **אברמסון – מלם מערכות בע"מ**, פס' 13 לפסק הדין (נבו 11.9.2014).

⁶⁵ ראו סע"ש (אזורי ת"א) 45564-12-17 **כהן – אל על נתיבי אויר לישראל בע"מ**, פס' 19. ד לפסק הדין (נבו 9.3.2018); על"ח (אזורי ת"א) 1116-02-12 **דלל-גפנר – פריגו ישראל סוכנויות בע"מ**, פס' 17 לפסק הדין (נבו 18.8.2013).

⁶⁶ פרשת **שטטר**, לעיל ה"ש 44, בפס' 10 לפסק הדין.

⁶⁷ כך למשל בעניין סע"ש (אזורי ת"א) 24704-11-16 **זיפקום תקשורת בע"מ – חסקלוביץ'** (נבו 20.8.2019) אמר בית הדין כי "עפ"י ההלכה הפסוקה, אין מניעה כי המעסיק יחדור לתוכן התכתבות מקצועית בתיבת דוא"ל שהוא מעמיד לרשות עובדיו" (שם, בפס' 139 לפסק הדין).

(ב) מבחן ההסכמה

כאמור, קושי מרכזי ביישום הלכת **איסקוב ענבר** נוגע לדרישה בפסק הדין כי הסכמת העובד צריכה להיות מדעת ומרצון חופשי כאשר מדובר בתיבות הדוא"ל המעורבת והמקצועית. ואולם קביעה זו סותרת את האמירות גם בגוף פסק הדין כי בשל פערי הכוחות בין הצדדים קשה מאוד לתת הסכמה חופשית, וכן את הדרישה כי הסכמה תיבחן רק לאחר התקיימותם של כמה תנאי סף מצטברים, לרבות דרישת מדיניות.⁶⁸ עוד בחנו מצבים שבהם בתי הדין התייחסו לפרטיות כזכות קוגנטית שאי אפשר להתנות עליה, כמו במקרה של תיבה פרטית בהלכת **איסקוב ענבר**.

מצאנו שבתי הדין מעניקים משקל גדול יחסית למבחן ההסכמה. דרישת ההסכמה נדונה במישרין או בעקיפין בכ-70% מפסקי הדין וההחלטות, הן במקרים שבהם הוכרה הפגיעה בזכות לפרטיות וניתן סעד והן במקרים שבהם לא הוכרה הפגיעה בפרטיות. בקריאת פסקי הדין וההחלטות של בתי הדין הבחנו כי ניתן לחלק את המצבים שבהם נידונה דרישת ההסכמה לשני קצוות ולמצבי ביניים.

בקצה האחד בתי הדין קבעו במצבים מסוימים כי האיסור על הפגיעה בפרטיות הוא קוגנטי, ולא ניתן להתנות עליו בהסכמת כללית של העובד. המצבים העיקריים שבהם בתי הדין פסקו בגישה זו וקבעו כי מדובר בפגיעה אסורה בפרטיות שלא ניתן להתנות עליה כאמור הם למשל כאשר המעסיק ניטר או ביקש לנטר תיבת דוא"ל פרטית של העובד, גלישה של העובד באינטרנט, או חדר לחשבון הווטסאפ של העובד. כך למשל בעניין **סולימנוב** פסק בית הדין שמכיוון שמדובר בניטור של תיבת דוא"ל פרטית, אין משמעות לעובדה שהמעסיק הודיע לעובדים על ניטור המחשבים ולשאלה אם יש לראות בשתיקת העובדים להודעה זו כהסכמה. יתרה מזאת, בית הדין ציין כי גם אם ניתנה הסכמת העובד לחידרה לתיבת הדוא"ל הפרטית שלו, חזקה שהסכמה זו ניתנה מכורח ולא מרצון חופשי ולכן אינה תקפה. עם זאת נפסק כי אילו היה מדובר בתיבה מעורבת או בתיבה אישית שבבעלות המעסיק, היה מקום לבחון שאלות אלו.⁶⁹ בעניין **בירנבוים** הורה בית הדין על הוצאת ראיה ופסק כי כאשר מדובר בתיבת דוא"ל חיצונית-פרטית שבבעלות העובד, שאלת ההסכמה אינה רלוונטית, ולמעסיק אסור לחדור לתיבה זו או לעקוב אחר השימוש שהעובד עושה בה.⁷⁰ בעניין **רמי חי** דחה בית הדין בקשה לצפייה בהיסטוריית גלישה של עובד שפוטר וקבע כי בקשה זו "חורגת מגדר הליך גילוי מסמכים בתסיעה [בתביעה] אזרחית רגילה שבין עובד למעסיק", שכן תהא בכך חידרה אסורה אל המרחב הווירטואלי הפרטי והאינטימי של העובד.⁷¹ בעניין **גבע** קבע בית הדין כי חזקה שהעובד לא נתן הסכמתו לעיין בתכתובת אישית שנעשתה באמצעות הפייסבוק.⁷² בקצה האחר, במצבים מסוימים בתי הדין לא נדרשו כלל לשאלת ההסכמה או קבעו כי הסכמת העובד אינה רלוונטית. כך למשל בעניין **ברמן** קבע בית הדין כי מכיוון

⁶⁸ פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 41–43 לפסק הדין.

⁶⁹ פ"ה (אזורי ב"ש) 16-04-16 40066-04-16 **כרמל בידוד בע"מ נ' סולימנוב**, פס' 52 לפסק הדין (נבו) 13.08.2017.

⁷⁰ ס"ע (אזורי ת"א) 11-09-11 11371-09-11 **שיאולוגי בע"מ – נתן בירנבוים**, פס' 31–32 לפסק הדין (נבו) 4.11.2015.

⁷¹ פרשת **רמי חי**, לעיל ה"ש 63, בפס' 43–44 לפסק הדין.

⁷² ס"ע"ש (אזורי ת"א) 15-09-15 1575-09-15 **גבע – מזרחי**, פס' 15–16 (נבו) 29.9.2016.

שהחדירה לתיבת דוא"ל מעורבת נעשתה לאחר שהיו ראיות לפעילות אסורה מצד העובד ובשל חשש שהעובד ינסה להעלים ראיות ולשבש חקירה משטרתית, קבלת הסכמת הייתה מיותרת,⁷³ וזאת במסגרת הליך "אקס פוסט" שבו ביקש המעסיק להציג את הראיות. בעניין **אקספו** הבחין בית הדין בין עובד שעודנו מועסק ומטרת ניטור תיבת הדוא"ל היא אגירת מידע על העובד לשימוש עתידי במידת הצורך, לבין עובד לשעבר שהמעסיקה חוששת כי הקים עסק פרטי מתחרה בעודו מועסק אצלה או גזל את סודותיה. במקרה השני, וכאשר מדובר בתיבת דוא"ל מקצועית, פסק בית הדין כי אין צורך בהסכמה.⁷⁴ במילים אחרות, כאשר אופי המידע הוא עסקי, בין בשל תוכנו (לדוגמה מצגות עסקיות לעומת פרטים הנוגעים למשפחה או לחברים) ובין בשל הפלטפורמה שבה המידע מועבר (תיבת דוא"ל מקצועית לעומת תיבה פרטית), והמעקב נעשה לצורך הגנה על העסק, על סודותיו ומתוך נאמנות כלפיו, בתי הדין לעבודה אינם בוחנים את הסכמת העובד. זהו יישום בעייתי של ההלכה, שכן כאמור בהלכת **איסקוב ענבר** קבע בית הדין שלושה מבחני עזר למצבים שבהם הסכמת העובד אינה נדרשת, ואלה אינם מיושמים במלואם בבתי הדין. יישום בעייתי זה אף קשור, להערכתנו, לנקודה שהעלינו קודם לכן בנוגע להיעדרו של דיון מעמיק בשאלת הפגיעה בפרטיות, שכן גם בנוגע למידע פרטי המצוי בתיבה מעורבת או מקצועית נדרשת הסכמה ספציפית, מפורשת, מדעת ומרצון, על פי ההלכה.

שני הקצוות של קוגנטיות מחד גיסא, והיעדר דרישה להסכמה מאידך גיסא, מצויים גם בפסיקה ובהנחיות הרשות להגנת הפרטיות בנוגע לשימוש במצלמות מעקב במקום העבודה, בין אזורים ציבוריים לבין המרחב הפרטי של העובד. לפי ההנחיות, באזורים המסווגים כמרחב הפרטי של העובד אסור לצלם את העובד ללא ידיעתו ואסור להתקין מצלמות נסתרות, אפילו למטרה לגיטימית, גם אם התקבלה הסכמה עקרונית של העובד לביצוע צילומי סתר במשרדי העובדים.⁷⁵ לעומת זאת במקרים אחרים, כאשר המצלמות הוצבו במרחב הציבורי, פסק בית הדין כי לא נדרש לבצע פעולות מיוחדות להגנה על פרטיות העובדים.⁷⁶ ואולם, במקרה של מצלמות שהוצבו במרחב הציבורי ההנחה היא כי אין פגיעה ניכרת בפרטיות, מה שלא נכון למקרים שבהם לא נבחנה הסכמה שפורטו לעיל. רק במצבים מסוימים, שנופלים בתווך שבין שני קצוות אלה, עסקו בתי הדין באופן שבו יש ליישם את דרישת ההסכמה ולמשקל שיש לתת לשאלה אם ניתנה מראש, מדעת ומרצון חופשי. ואולם מהניתוח שלנו של פסקי הדין לא היה אפשר לראות כי בתי הדין קבעו הלכה ברורה וסדורה בעניין זה. נראה כי על בתי הדין לעבודה להמשיך ולפתח את מבחן ההסכמה במקרים האמורים. במספר המועט של המקרים שבהם נדון אופן יישום דרישת ההסכמה התייחסו בתי הדין לקריטריונים לביסוס ההסכמה. נוסף על כך, אף שהלכת **איסקוב ענבר** קבעה כי הסכמה תיבחן רק לאחר התקיימותם של כמה תנאי סף

⁷³ פרשת **ברמן**, לעיל ה"ש 50, בפס' 8 לפסק הדין.

⁷⁴ פרשת **אקספו**, לעיל ה"ש 7, בפס' 25–26 לפסק הדין.

⁷⁵ הנחיית מצלמות מעקב ביחסי עבודה, לעיל ה"ש 3.

⁷⁶ ראו פרשת **דלל-גפנר**, לעיל ה"ש 65; פרשת **אל-על**, לעיל ה"ש 65.

מצטברים, הרי שבתי הדין בחנו את התקיימותם של תנאים אלה במקרים מועטים בלבד מתוך פסקי הדין שכן דנו בדרישת ההסכמה.

הפיתוח המרכזי לדרישת ההסכמה היה בעניין **קלנסווה**. כאמור, בהלכת **איסקוב ענבר** קבע בית הדין כי הדרישה להסכמה כללית מדעת ומרצון למדיניות השימוש והמעקב שנקבעה בהסכם הקיבוצי היא תנאי הכרחי אך לא מספיק, וכי "נדרשת הסכמה מיוחדת של העובד, לכל פעולה ופעולה שבכוונת המעסיק לנקוט בחדירה לתכתובת ולקבצים אישיים בתיבת הדואר שהוקצתה לו, תוך שמירת זכותו שלא ליתן הסכמתו לחדירת המעסיק לאותה תיבה".⁷⁷ בעניין **קלנסווה** קבע בית הדין הארצי לעבודה שהשימוש בשעון ביומטרי לצורך מעקב אחר שעות עבודה אינו אסור קטגורית, אלא שהכשרת שימוש כזה, שיש בו משום פגיעה בפרטיות ובזכותן של העובדות לאוטונומיה על גופן, יכולה להיעשות באחת מהדרכים האלה: בחוק או בהסכמה שאינה נוגדת את תקנת הציבור,⁷⁸ בפרט, ככל שהפגיעה נעשית על דרך של הסכמה, נדרשת הסכמה מדעת ומרצון חופשי.⁷⁹ בית הדין דן אך אינו מכריע בשאלה אם הסכמה קיבוצית מייתרת את הצורך בהסכמה פרטנית. מצד אחד בית הדין אומר שהסדרה שכזו מעניקה יתרון ל"גודל" ומקילה על המעסיק במגעיו עם העובדים, ומצד אחר ניתן לטעון שהסדרה קיבוצית של השימוש בשעון ביומטרי טעונה הסכמה פרטנית, שכן מדובר בחדירה ליחידה האוטונומית של האדם.⁸⁰

עוד יישומים של שאלת ההסכמה היו בעניין **אנחין**, שם בית הדין פסק כי לא ניתן לבסס את הסכמת העובד לניטור תיבת הדוא"ל על סמך סעיף עם ניסוח גורף בהסכם העסקה.⁸¹ בדומה לזה, בעניין **בירנבוים** עולה כי לא ניתן לבסס הסכמה על "אזהרה" כללית שניתנה לכל העובדים, וכי נדרשת הסכמה ספציפית של העובד.⁸² בעניין **בובר**⁸³ הסכים התובע במהלך דיון בהליך לגלות את תיבת הדוא"ל שלו, הסכמה שקיבלה תוקף של החלטת בית הדין, ובהמשך ביקש לחזור בו מהסכמתו. בית הדין קיבל את בקשתו ופסק: "סבורני שאין הצדקה להותיר את ההחלטה על כנה ואין הצדקה לאפשר את העיון בתיבת הדוא"ל של התובע, רק בשל העובדה שהתובע נתן הסכמתו לענין זה וחזר בו מההסכמה".⁸⁴

⁷⁷ פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 33 לפסק הדין.

⁷⁸ בית הדין מפרט כי הסכמה שאינה נוגדת את תקנת הציבור בהקשר זה היא הסכמה מדעת ומרצון חופשי, העומדת במבחני תום הלב ובמבחני סעיף 30 לחוק החוזים (חלק כללי), התשל"ג-1973. ראו פרשת **עיריית קלנסווה**, לעיל ה"ש 1, בפס' 89 לפסק הדין.

⁷⁹ שם, בפס' 129-130.

⁸⁰ שם, בפס' 120-121.

⁸¹ סע"ש (אזורי ת"א) 14245-02-17 **אנחין – אליאסי**, פס' 40-42 לפסק הדין (נבו 22.7.2017).

⁸² פרשת **בירנבוים**, לעיל ה"ש 70, בפס' 32 לפסק הדין.

⁸³ סע"ש (אזורי ת"א) 30032-12-17 **בובר – בובר** (נבו 29.1.2019).

⁸⁴ שם, בפס' 6.

(ג) עקרון הלגיטימיות

כאמור, עקרון הלגיטימיות כולל דרישה להגבלת איסוף המידע באמצעים אלקטרוניים למטרות החיוניות למקום העבודה וכן הגבלת השימושים אשר ייעשו בהמשך באותו מידע.

בתי הדין הכירו במפורש בתכלית כלגיטימית בעיקר בכל הנוגע לתכליות לשימוש במידע ולא בנוגע לתכלית איסופו. תכליות שהוכרו במפורש כלגיטימיות קשורות לחשש לגזל סוד מסחרי, להגנת סייבר, לניהול העסק ולהגנה עליו, כגון לצורך שזון נוכחות (קלנסווה) ואבטחה (למשל מצלמות אבטחה). למשל, בעניין **הסתדרות עובדי המדינה**⁸⁵ פסק בית הדין כי התכליות שהציגה המדינה לצורך הטמעת מערכת איכון כלי רכב – תכלית כלכלית (חיסכון כספי שיווצר הודות לשיפור האפקטיביות של השימוש בכלי הרכב) ותכלית בטיחותית (שיפור הבטיחות באמצעות בקרת נהיגת כביש חריגה) הן ראויות.⁸⁶ ברוב המקרים היה אפשר לגזור מהפסיקה הכרה בתכליות לגיטימיות לשימוש במידע במסגרת טענות המעסיק כי ניטור תיבת דוא"ל ומסמכים נוספים נדרש כדי להוכיח טענותיו שהעובד פגע בעסק, בין היתר באמצעות הקמת עסק מתחרה במהלך עבודתו אצל המעסיק,⁸⁷ פגיעה בסודות מסחריים של החברה,⁸⁸ הפרת חובות סודיות או חובות אמונים⁸⁹ או הוכחת טענות בהקשרים נוספים הנוגעים ליחסי עבודה כגון קיומם של יחסי עובד-מעסיק.⁹⁰ תכליות אלו עורבבו פעמים רבות עם אינטרס הגילוי שבהליך המשפטי, עם יעילות הדיון ועם חקר האמת, ולעיתים עמדו בפני עצמן.

כאמור, כאשר בתי הדין עסקו בעקרון הלגיטימיות, הם לא הבחינו בין התכלית של איסוף המידע לבין התכלית של השימוש במידע, למרות חשיבותה של הבחנה זו ליישום מבחן הלגיטימיות וכן ליישום של מבחנים אחרים, בעיקר עקרון צמידות המטרה שנועד לוודא כי נעשה שימוש במידע רק למטרה שלשמה הוא נאסף. להלן סיכום התכליות העיקריות שהוכרו, במישרין או בעקיפין, בפסיקה כלגיטימיות לצורך ביצוע פעולות ניטור ומעקב הכוללות איסוף מידע פרטי ושימוש בו באמצעים טכנולוגיים.⁹¹

1. **חשש לגזל סודות מסחריים או הקמת עסק מתחרה בידי עובד.**⁹² למשל, בעניין **אקספו** התיר בית הדין ניטור תיבת דוא"ל מקצועית שהייתה בשימוש העובד במהלך עבודתו

⁸⁵ ע"ס **הסתדרות העובדים הכללית**, לעיל ה"ש 48. יצוין כי בפרשה זו בית הדין הארצי לעבודה נתן תוקף של פסק דין להסכמת הצדדים לביטול פסק דינו של בית הדין האזורי לעבודה מיום 8.10.2020.

⁸⁶ שם, בפס' 110.

⁸⁷ ראו סע"ש (אזורי ת"א) 22614-09-19 **ש. אנגל מהנדסים בע"מ – בוגרט** (נבו) 27.4.2020; פ"ה (אזורי חי') 15794-10-17 **אקספו אופנה בע"מ – הברפלד** (נבו) 4.2.2018.

⁸⁸ סע"ש (אזורי ת"א) 69292-03-18 **מאפי – פארמה בע"מ – טומוב ז"ל** (נבו) 9.12.2019.

⁸⁹ פרשת **אנחין**, לעיל ה"ש 81.

⁹⁰ סע"ש (אזורי ת"א) 38650-09-17 **אי.איי.סי – מרכז הפרסום הישראלי בע"מ – גולן** (נבו) 4.12.2018.

⁹¹ יצוין כי במקרים שבהם מדובר בהליך גילוי מסמכים, אינטרסים אלו מצטרפים לזכות המעסיק להשיג ראיות התומכות בעניינו בהליך וכן לאינטרס חקר האמת.

⁹² לדוגמאות, ראו סע"ש (אזורי ת"א) 41363-03-13 **יוסקוביץ – טלרד נטוורקס בע"מ** (נבו) 15.10.2017;

סע"ש (אזורי ת"א) 18515-02-18 **סערה – בלוקשתיל בע"מ** (נבו) 13.5.2020; סע"ש (אזורי ת"א) 12303-

09-18 **רוברגורפ ט.א.ק. בע"מ – באום** (נבו) 24.3.2020; סע"ש (אזורי ת"א) 26316-09-15 **סוריא – בן ארי**

- אצל התובעות בשל החשש של התובעות כי העובד הקים עסק מתחרה במהלך עבודתו.⁹³
2. חשש מפני פעילות פלילית או מזיקה של העובד כלפי העסק או כלפי אחרים.⁹⁴ בעניין **ברמן** התיר בית הדין שימוש בראיות שהושגו באמצעות חדירה לכתובת דוא"ל שהוקצתה לעובד לצורך עבודתו, מכיוון שהוכח שפעל לפגוע במעסיקה ו"נוכח החשש הלגיטימי מפני מעשים נוספים".⁹⁵
3. דיווח על נוכחות ומעקב אחריה.⁹⁶ בית הדין פסק כי מעקב אחר נוכחות הוא אינטרס לגיטימי של המעסיק המצדיק פגיעה מסוימת בפרטיות, הן כחלק מהניהול השוטף של העסק⁹⁷ והן כדי לגלות מעשה שלא כדין כגון דיווח נוכחות שקרי,⁹⁸ וכחלק מהליך גילוי מסמכים.⁹⁹ עם זאת בעניין **קלנסווה** קבע בית הדין הארצי כי בבחינת תכלית הפעלתו של אמצעי מעקב יש לבחון את ההקשר שבו האמצעי מיושם. כך למשל האמצעי של מסירת טביעת אצבע לשם רישום שעות בשעות נוכחות ביומטרי עשוי להימצא לא לגיטימי אצל מעסיקים מסוימים ועשוי להימצא ראוי כאשר מדובר במעסיקים אחרים, כגון מפעל ביטחוני.¹⁰⁰ בעניין **אברמסון**,¹⁰¹ במסגרת תביעה לפיצויים בגין פגיעה בפרטיות בשל מעקב וחקירה שביצעה הנתבעת, פסק בית הדין כי המעקב אחר העובד בוצע למטרה לגיטימית שנועדה להגן על אינטרס לגיטימי של המעסיק – לבדוק את טענותיו של עובד שלפיהן נבצר ממנו להתייצב לשימוע.¹⁰² בעניין זה הזמינה הנתבעת חקירה סמויה אחר העובד לאחר שהגיש אישורי מחלה רבים, ובכך דחה שיחת שימוע לפיטורי צמצום צפויים, דבר שעורר חשד אצל הנתבעת שמדובר באישורים פיקטיביים שמטרתם לסכל את עריכת השימוע.

(נבו 3.11.2016). כן ראו ת"פ (אזורי חי') 25861-02-16 **איסתא ישראל בע"מ – רוזנברג** (נבו 21.3.2016); פרשת **בירנבוים**, לעיל ה"ש 70; סע"ש (אזורי ת"א) 24960-02-19 **א.מ רכיבים (2005) בע"מ – מולדובן** (נבו 6.10.2020); פרשת **אקספו**, לעיל ה"ש 7.

93 שם, בפס' 28.

94 לדוגמאות, ראו פרשת **רמי חי**, לעיל ה"ש 63; פרשת **ברמן**, לעיל ה"ש 50.

95 שם, בפס' 8. מפסק הדין עולה כי לאחר שנתגלעה מחלוקת בנוגע לתנאי העסקתו נקט העובד כמה וכמה פעולות "מתוך כעס ונקמה", לרבות הסרת רישיונות של לקוחות החברה, התחזות בדוא"ל לעובד אחר כדי לחבל בשיתופי פעולה בין החברה ללקוחותיה והפצת חוזה עבודה של עובד אחר כדי להתסיס את יתר העובדים נגד החברה, בין היתר באמצעות שימוש בהרשאות ובסיסמאות שניתנו לעובד מתוקף תפקידו כבעל תפקיד בכיר בחברה לאבטחת מידע. עוד עולה מפסק הדין כי חדירת המעסיקה לתיבת הדוא"ל של העובד נעשתה לאחר שהיו בידיה ראיות לפעילות פלילית לכאורה או other wrongdoing ומתוך חשש שהעובד ינסה להעלים ראיות ולשבש חקירה משטרתית.

96 לדוגמאות, ראו פרשת **דלל-גפנר**, לעיל ה"ש 65; פ"ה (אזורי חי') 1274-04-17 **מרעי – המועצה המקומית פרדיס** (נבו 2.4.2018); פרשת **אברמסון**, לעיל ה"ש 64; פרשת **עיריית קלנסווה**, לעיל ה"ש 1.

97 שם.

98 פרשת **אל על נתיבי אוויר**, לעיל ה"ש 65; פרשת **אברמסון**, לעיל ה"ש 64.

99 פרשת **שטור**, לעיל ה"ש 44.

100 פרשת **עיריית קלנסווה**, לעיל ה"ש 1, בפס' 132 לפסק הדין.

101 פרשת **אברמסון**, לעיל ה"ש 64.

102 שם, בפס' 13.

4. ניהול שוטף של העסק. כאמור, בעניין הסתדרות עובדי המדינה פסק בית הדין כי התכליות שהציגה המדינה לצורך הטמעת מערכת איכון כלי רכב – תכלית כלכלית ותכלית בטיחותית הן ראויות.¹⁰³
5. הגנת סייבר ואבטחה.¹⁰⁴ ניתן לטעון כי הגנת סייבר ואבטחה הן אמצעי ולא תכלית בפני עצמן, וניתן לראות בהגנת סייבר ובאבטחה תכלית כללית המאגדת תחתיה מספר תכליות, כגון הגנה על מאגרי מידע; שמירה מפני פגיעה במטרות חברתיות, סביבתיות וביטחוניות; הגנה על סודות, על קניינו של המעסיק ועוד.¹⁰⁵ ואכן, הדיון בהגנת סייבר ובאבטחה כתכליות בפסקי הדין הוא מועט. ייתכן שפער זה נובע מהנקודה שצינו קודם לכן, ולפיה בתי הדין לעבודה אינם מבחינים בין תכלית איסוף המידע לבין תכלית השימוש במידע. זאת, הואיל וניטור קבוע של הדוא"ל הוא פעמים רבות לצורך הגנה על הסייבר אך השימוש במידע נעשה לתכליות אחרות. תכלית הגנת סייבר נדונה רק בעניין אודיס,¹⁰⁶ אך כמה פסקי דין התייחסו להתקנת מצלמות אבטחה.¹⁰⁷ מפסק הדין בעניין אודיס עולה כי בית הדין רואה בהתקנת מערכת ניטור לצורכי אבטחת מידע תכלית לגיטימית. במסגרת תביעה לפיצויים בגין יחסי עבודה פוגעניים טען התובע כי החברה פגעה בפרטיותו ובפרטיות העובדים בכלל בכך שאולץ לחתום על מסמך המאפשר לה לחדור לתיבת הדוא"ל ולבצע מעקב אחר הודעות דוא"ל אישיות.¹⁰⁸ בית הדין פסק כי הנתבעת פעלה בצורה לגיטימית כשהזהירה את עובדיה כי ייתכן שהמידע שהם בוחרים להעלות במחשביה יהיה חשוף, בעקבות התקנת מערכת אבטחת מידע אשר מנטרת קבצים והודעות דוא"ל שיוצאים ממחשבי החברה ונכנסים אליהם.¹⁰⁹
6. גילוי מסמכים היא תכלית לגיטימית נוספת שבתי הדין מזכירים, ואולם פה ההלכה אינה ברורה דייה ואינה חד-משמעית. בפועל איתרנו שני אופנים עיקריים שבהם בתי הדין לעבודה מתייחסים להלכת איסקוב ענבר בהליכים אלה, ועליהם נפרט בהרחבה בתת-הפרק "ממצאים נוספים".

¹⁰³ עס"ק הסתדרות העובדים הכללית, לעיל ה"ש 50, בפס' 110 לפסק הדין.
¹⁰⁴ יצוין כי מטרה זו הוכרה כלגיטימית גם על-ידי ה-GDPR. סעיף 49 להוראות המבוא ל-GDPR קובע כי עיבוד מידע לצורכי הגנת הסייבר, המוגבל והפרופורציונלי למידה הנדרשת לאבטחת המידע, הוא אינטרס לגיטימי של הגורם השולט במידע. ראו Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data; Directive 95/46/EC, 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 (להלן: GDPR).
¹⁰⁵ עינת אלבין וגיל עומר "זכות העובדים להגנה על מידע פרטי בעידן של הגנת סייבר" משפט וממשל כח (2024).

¹⁰⁶ פרשת אודיס, לעיל ה"ש 47.

¹⁰⁷ לדוגמאות, ראו פרשת דלל-גפנר, לעיל ה"ש 65; פרשת אל-על, לעיל ה"ש 65.

¹⁰⁸ פרשת אודיס, לעיל ה"ש 47, בפס' 13 לפסק הדין.

¹⁰⁹ שם, בפס' 79–80.

נציין כי ההתייחסות בפסיקה למבחן הלגיטימיות היא דלה, ואנו דלינו את רובה מדיוני רקע בפסקי הדין. במקרים שבהם בתי הדין אינם מקבלים במלואן טענות בגין פגיעה בפרטיות, היעדרו של דיון זה בעייתי, שכן שאלת הלגיטימיות היא קריטית לצורך ההגנה על הפרטיות. מלבד זאת, מכיוון שבתי הדין אינם בוחנים את שאלת הלגיטימיות ישירות ובמדויק, הם אף אינם מנמקים בצורה מעמיקה מדוע המטרה לגיטימית. למשל, אם אכן לגיטימי לעקוב אחרי עובד כדי לבדוק את טענותיו כי נבצר ממנו להגיע לשימוע כפי שנקבע בעניין **אברמסון**¹¹⁰ או אם לגיטימי לאסוף מידע לצורך ניהול הליך משפטי. חשיבות הדיון בשאלת הלגיטימיות נובע גם מכך שעקרון צמידות המטרה וכן עקרון המידתיות ויישומו תלויים בהגדרת המטרה הלגיטימית. אם נחזור לעניין **אברמסון**, בית הדין כמעט שלא בחן את מידתיות האמצעי שנבחר אלא רק אמר כי מדובר בפגיעה קטנה יחסית בפרטיות מכיוון שמדובר במעקב ברשות הרבים ולא בחדירה לדוא"ל. עוד אמר בית הדין, שהיה אפשר למצוא דרך פוגענית פחות, כמו למשל שהמעסיקה יכלה להעמיד רופא מטעמה, ואולם פסק כי אין בכך לשלול דרכים כמו אלה שנקטה המעסיקה.¹¹¹ שאלות מעין אלו ניתן לשאול רק כאשר התכלית הלגיטימית של המעקב והניטור נדונים במפורש. באשר לממצאים אלה חשוב לזכור את אמירתו של בית הדין הארצי לעבודה בעניין **קלנסווה**: "חשוב לעמוד על בהירות בעניין התכלית ולזכור שלעיתים התכלית המוצהרת מסתירה תכלית אמיתית אחרת."¹¹² אין לנו אלא להסכים.

(ד) עקרון צמידות המטרה

עקרון צמידות המטרה נדון לעומק רק במעט מאוד פסקי דין מאלה שסקרנו. אומנם בחלק מפסקי הדין שסקרנו שאלת צמידות המטרה לא הייתה רלוונטית משום שהוכרה הפגיעה בפרטיות ללא קשר למבחן זה, ועדיין מדובר בממצא מטריד. פסקי הדין שכן דנו בעקרון צמידות המטרה עסקו בהסדרת פרקטיקה הכרוכה בפגיעה בפרטיות (שעון ביומטרי ואיכון כלי רכב). בעניין **הסתדרות המדינה** הצביע בית הדין על כוונת המדינה להשתמש במידע המועבר גם למשאבי אנוש של המשרד, גם כדי לאתר הפרות משמעת של העובדים, אך פסק כי אם הסנקציות המשמעתיות הן אמצעי להשגת התכלית הכלכלית והבטיחותית, אין בכך כדי לאיין את עקרון צמידות המטרה.¹¹³

בעניין **אנחין** ניתן לראות יישום של הלכת **איסקוב ענבר** שלפיה "קביעת מטרה כוללנית, חסרת זיקה לאינטרסים הלגיטימיים של מקום העבודה, לא תוכר כ'תכלית ראויה' המצדיקה מעקב אחר תכתובת אי-מייל של העובד, איסוף מידע ושימוש במידע שהפיק המעסיק מאותה תכתובת".¹¹⁴ באותו עניין פסק בית הדין כי אין בניסוח גורף בהסכם העסקה המתיר ניטור דוא"ל כדי לענות על עקרון צמידות המטרה, שכן לפי עיקרון

¹¹⁰ פרשת **אברמסון**, לעיל ה"ש 64.

¹¹¹ שם, בפס' 13.

¹¹² פרשת **עיריית קלנסווה**, לעיל ה"ש 1, בפס' 132 לפסק הדין.

¹¹³ עס"ק **הסתדרות העובדים הכללית**, לעיל ה"ש 48, בפס' 120–122 לפסק הדין.

¹¹⁴ פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 20 לפסק הדין.

זה, על המעסיק לפרט מראש אילו שימושים ייעשו במידע ולמי יועבר המידע, אם אכן יועבר.¹¹⁵

ניתן לראות יישום של עקרון צמידות המטרה הכולל כאמור הגבלת השימוש במידע למטרה שלשמה נאסף בהנחיה מס' 5/17 של רשם מאגרי המידע שהוזכרה בעניין גליה כהן.¹¹⁶ בעניין זה פסק בית הדין כי על פי הנחיית רשם מאגרי המידע, מצלמות שמעסיק התקין לצורכי בקרת כניסה, למטרות ביטחוניות או לשמירה על שלום העובדים, אינן יכולות לשמש למטרת ניהול ומשמעת. עם זאת נפסק שמכיוון שהצילומים נעשו ברשות הרבים, כאשר העובדת צולמה נכנסת לבניין ויוצאת ממנו, אין מדובר בפעולות הפוגעות במובהק בפרטיות, ולכן בית הדין פסק כי אין לפסול את הראיות.¹¹⁷

בעניין קלנסווה הדגיש השופט אילן איטח את החשש מאובדן השליטה כאשר מדובר במידע ביומטרי ופסק שעצם החשש מהשימוש במידע ביומטרי שלא למטרה שלשמה נמסר הוא פגיעה בפרטיות: "מסירת טביעת אצבע, גורמת לאדם שמסר אותה לאבד את שליטתו על מידע הייחודי לו באופן מובהק, המאפשר זיהוי חד ערכי שלו ומהווה חלק מגופו. השילוב של אופיו הייחודי של המידע מחד, ואובדן השליטה עליו מאידך, הוא-הוא היוצר את הפגיעה הן בפרטיות והן באוטונומיה".¹¹⁸

כאשר הפגיעה בפרטיות נעשית בפיקוחו של בית הדין במסגרת בקשה לגילוי מסמכים, בית הדין יכול להגביל את השימושים שנעשים במידע ובכך ליישם את עקרון צמידות המטרה. כך למשל בעניין אקספו הגביל בית הדין את השימוש במידע שיתקבל מניטור תיבת דוא"ל רק למסגרת ההליך הנדון.¹¹⁹ עם זאת אף שההליך הוא "סביבה מבוקרת", ההחלטה שניתנה באקספו מדגימה את הקושי שביישום עקרון צמידות המטרה רטרואקטיבית על ידי בית הדין, לאחר שהפגיעה בפרטיות לכאורה כבר נעשתה.

הקושי בהיעדר יישומו של מבחן צמידות המטרה מתחדד נוכח מה שעלה מהניתוח שלנו בנוגע לעקרון הלגיטימיות. כאשר בתי הדין לעבודה אינם מבחינים בין תכלית לגיטימית לאיסוף מידע לבין תכלית לשימוש במידע, אזי עולה בעיה של החלת עקרון צמידות המטרה. למשל, מידע שנאסף לצורך הגנה על הסייבר אמור לשמש רק למטרה זו. זה יישומו הנכון של עקרון צמידות המטרה, שכן כפי שציינו לעיל, הלכת איסקוב ענבר קבעה את עקרון צמידות המטרה לתכלית שלמענה נאסף המידע. קשה לראות, למשל, בית דין שקובע כי מעסיק יכול לאסוף מידע פרטי לצורך קיום הליכים משפטיים (גילוי מסמכים), ולכן החלת עקרון צמידות המטרה הייתה אמורה להוביל לאיסור על שימוש במידע שנאסף למטרה אחרת לתכלית זו, אלא במקרים שבהם השימוש הותר לפי הלכת איסקוב ענבר.

¹¹⁵ פרשת אנוחין, לעיל ה"ש 81, בפס' 41 לפסק הדין.

¹¹⁶ פרשת אל-על, לעיל ה"ש 65.

¹¹⁷ שם, בעמ' 13-14.

¹¹⁸ פרשת עיריית קלנסווה, לעיל ה"ש 1, בפס' 113 לפסק דינו של השופט איטח.

¹¹⁹ פרשת אקספו, לעיל ה"ש 7, בפס' 35 לפסק הדין.

(ה) עקרון המידתיות

בכחינת יישום דרישת המידתיות בדקנו אם בתי הדין בחנו אם היה אפשר להשתמש באמצעי מידתי יותר בלי לפגוע בזכות לפרטיות ולעצב את הטכנולוגיה כך שתפגע בפרטיות פחות, ואם נבחנו טכנולוגיות חלופיות. כפי שציינו לעיל, על פי הלכת **איסקוב ענבר**, עקרון המידתיות מחייב לבחון: (1) טכנולוגיות חלופיות למעקב הפוגעות במידה הפחותה ביותר בפרטיות העובדים; (2) את היחס הראוי בין התועלת שבהגשמת מטרתה הראויה של מדיניות המעקב לבין הנזק והפגיעה בזכויות העובד כתוצאה ממדיניות המעקב.

בניתוח הפסיקה שאזכרה את הלכת **איסקוב ענבר** הבחנו כי המקרים המעטים שבהם היה דיון מעמיק בנוגע לעיצוב הטכנולוגיה הרלוונטית היו כאשר המעסיקים ביקשו להסדיר פרקטיקות הכרוכות בפגיעה בפרטיות וכן הייתה מעורבות של ארגון עובדים. במקרים אלו אף הוכרה הפגיעה בזכות לפרטיות – בעניין **קלנסווה** ובעניין **הסתדרות עובדי המדינה**. בעניין **קלנסווה** קבע בית הדין כי ככלל שימוש בטביעת אצבע לשם הקפדה על דיווחי נוכחות אמינים אינו מידתי מכיוון שיש אמצעים אחרים, פוגעניים פחות, להשגת המטרה, כגון כרטיס נוכחות ומצלמות, שהסיכונים הכרוכים בשימוש בהם פחותים במידה ניכרת מהשימוש בשעון הביומטרי.¹²⁰ בעניין **הסתדרות עובדי המדינה** דן בית הדין בהסדרת פרקטיקה של התקנת מערכת מעקב ברכבי מדינה המופעלת באמצעות כרטיס חכם שעליו מקודדים פרטי העובד, המאפשר לאסוף מידע על השימוש שנעשה ברכב ועל נהיגתו של העובד לפי נוהל שהציגה המדינה. בית הדין בחן אם הנוהל עומד בדרישות המידתיות וחילק מבחן זה לשניים: במובן הרחב – השוואה לאמצעים טכנולוגיים שונים וחלופיים ובחירה באמצעי שפגיעתו פחותה, ובמובן הצר – השוואה בין האמצעי המוצע לבין הפגיעה בפרטיות ובחינה אם התועלת שבמעקב עולה על הפגיעה בפרטיות. בית הדין דן בסעיפים השונים בנוהל וקבע באשר לכל סעיף וסעיף אם הוא מידתי. כך למשל קבע בית הדין שצפייה במידע על מסלול נסיעתו של עובד במקרה של איחור חד-פעמי אינה מידתית, שכן לא הוצגו מדוע אין אמצעים חלופיים הפוגעניים פחות לביצוע מעקב זה, וכי נדרש לקבוע מספר מצטבר של איחורים שיהוו חריג שבגיננו כן יהיה אפשר לצפות במידע זה.¹²¹

דוגמה לפסיקה נוספת שבה נבחן אם יש אמצעי חלופי פוגעני פחות היא עניין **מאפי**,¹²² שם נימק בית הדין את דחיית בקשת החברה לגילוי ועיון במסמכים שהיו שמורים בתיבת דוא"ל של עובדת שהלכה לעולמה שהייתה בבעלות החברה, בכך שמדובר בבקשה גורפת (ניטור תיבה ששימשה את המנוחה במשך שמונה שנים) ובכך שקיימים אמצעים חלופיים להוכחת טענות החברה.¹²³

¹²⁰ פרשת **עיריית קלנסווה**, לעיל ה"ש 1, בפס' 132 לפסק הדין.

¹²¹ עס"ק **הסתדרות העובדים הכללית**, לעיל ה"ש 48, בפס' 127–128 לפסק הדין.

¹²² פרשת **מאפי**, לעיל ה"ש 88. סקירת עובדות פסק הדין מתוארת בהרחבה בעמ' 37 להלן.

¹²³ פרשת **מאפי**, לעיל ה"ש 88, בפס' 41 לפסק הדין.

נוסף על זה ניתן לראות מהמקרים שסקרנו שההשלכות המעשיות של עקרון המידתיות ובחינת אמצעים שפגיעתם פחותה הן שונות כאשר מדובר במקרים שבהם הפגיעה בפרטיות כבר נעשתה ונבחנת בדיעבד, לעומת מקרים שבהם הבחינה נעשית אקס אנטה. הדיון בעקרון המידתיות היה נרחב ומעמיק יותר בהליכים שבהם הפגיעה בפרטיות נבחנת אקס אנטה לעומת מקרים שבהם נבחנה פעולת המעסיק בבית הדין **לאחר** שהפגיעה בפרטיות לכאורה התרחשה ("אקס פוסט"). למשל, במסגרת תביעה לפיצויים בגין פגיעה בפרטיות ובבקשות לפסילת ראיות בטענה שהתקבלו תוך פגיעה בפרטיות, שאלות המידתיות – אם המעסיק נקט צעדים למנוע או למזער את הפגיעה בפרטיות ואם נבחנו אמצעים חלופיים – הועלו במספר קטן של מקרים, ולעיתים אף נקבע כי הן אינן רלוונטיות. כדוגמה ניתן את פסק הדין בעניין **אברמסון**, שם פסק בית הדין כי אף שלמעסיקה עמדה אפשרות פוגענית פחות – להעמיד את התובע לבדיקה רפואית מטעמה – הייתה הפגיעה קטנה מכיוון שביצוע המעקב אחריו באמצעות חקירה סמויה של משרד חקירות התבצעה ברשות הרבים. בית הדין פסק כי קיומה של דרך חלופית זו אינו בהכרח פוסל את השימוש בדרך של חקירה סמויה כפי שבחרה הנתבעת.¹²⁴

דוגמה נוספת היא עניין **יוסקוביץ**,¹²⁵ שם החרימה המעסיקה מחשב שהיה בשימוש עובד מתוך חשש שהעובד ימחק או יעתיק קבצים לצורך מיזם פרטי שהקים. בית הדין דחה את תביעת העובד לפיצויים בגין פגיעה בפרטיות ופסק שמכיוון שהמעסיקה איפסה את סיסמאות המחשב, מה שימנע גם מהעובד וגם מהחברה לגשת לחומר המצוי בו, היא נקטה פעולות סבירות להגן על פרטיות העובד.¹²⁶ באותו מקרה לא התקיים דיון בשאלת המידתיות. לבסוף, בעניין **גליה כהן** קבע בית הדין כי הפגיעה בפרטיות, אם התרחשה, היא קטנה ביחס לאינטרס המעסיק (גילוי דיווח שקרי של שעות עבודה), ובית הדין לא בחן אמצעים פוגעניים פחות.¹²⁷ בכל המקרים הללו, על אף חשיבות מבחן המידתיות, הוא לא נדון לעומק, ואנו סבורות שאם כן היה נדון, אזי ייתכן שתוצאות פסקי הדין היו אחרות. בניגוד למקרים אלה, כאשר הפגיעה בפרטיות נבחנה "אקס אנטה", במסגרת הליכי גילוי מסמכים, למשל בבקשות לנטר תיבת דוא"ל של עובד לשעבר, דחו בתי הדין בקשות לניטור תיבת דוא"ל ולעיון בה מהטעם שהבקשה רחבה וגורפת מדיי, ועל כן אינה מתיישבת עם עקרון המידתיות,¹²⁸ ובחנו אם קיימים אמצעים פוגעניים פחות להגשמת המטרה שלשמה הוגשה הבקשה תוך יישום אמצעים אלו בהליך הנדון. אמצעים אלו כוללים למשל הגבלת היקף הגילוי והגבלת מילות החיפוש בניטור תיבת הדוא"ל. כך, למשל, בעניין **אקספון**¹²⁹ התיר בית הדין ניטור תיבת דוא"ל מקצועית שהייתה בשימוש העובד במהלך עבודתו אצל התובעות, אך הגביל את הניטור לפי מילות חיפוש ומינוי

¹²⁴ פרשת **אברמסון**, לעיל ה"ש 64, בפס' 13 לפסק הדין.

¹²⁵ פרשת **יוסקוביץ**, לעיל ה"ש 92.

¹²⁶ שם, בפס' 39.

¹²⁷ פרשת **אל-על**, לעיל ה"ש 65.

¹²⁸ פרשת **מאפי**, לעיל ה"ש 88, בפס' 41 לפסק הדין.

¹²⁹ פרשת **אקספון**, לעיל ה"ש 7. נכון למועד כתיבת שורות אלו, ערעור על פסק הדין בעניין **אקספון** מתנהל בבית הדין הארצי לעבודה.

מומחה מחשבים שאינו עובד של התובעות, אשר יבצע את הניטור.¹³⁰ עם זאת לא שאל בית הדין אם היה אפשר לנקוט אמצעי מידתי יותר כדי לא לפגוע בפרטיות וקבע כי מכיוון שמדובר בעובד לשעבר, אין לצפות מהמעסיקות לבחון אמצעים פוגעניים פחות בנסיבות העניין.¹³¹

דוגמה נוספת מצויה בעניין **בונגרט**, שם קיבל בית הדין חלקית את בקשת החברה להשתמש בקבצים השמורים במחשב שנועד לשימוש העובדת, כדי להוכיח את נסיבות הפיטורים של העובדת. בית הדין התיר את העיון ואת הגשת המסמכים כפוף לכך שהחברה תעביר ראשית את המסמכים לעובדת, ואם העובדת תסבור שיש במסמכים מסמך אישי, או שהשימוש בו בהליך פוגע בפרטיותה, היא רשאית להגיש לבית הדין בקשה להתנגד להגשתם בהליך. כמו כן התנה בית הדין את החלטתו בהתייבות החברה בתצהיר כי השימוש במסמכים אלה יהיה למטרת ניהול הליך זה בלבד.¹³² ניתן לסכם ולומר כי כאשר הבחינה נעשית "אקס אנטה", הדיון בפגיעה בפרטיות הוא מהותי בהרבה מבמקרים שבהם הוא נבחן "אקס פוסט".

(ו) עקרון השקיפות ודרישת מדיניות

מבדיקת הפסיקה עולה כי הדיון בנוגע לשקיפות ולמדיניות נכרך במקרים רבים ביישום דרישת ההסכמה ועלה בשני הקשרים עיקריים: הראשון, לצורך סיווג תיבות הדוא"ל. בעניין **מאפי** פסק בית הדין כי מכיוון שלא הוגדרה מדיניות בנוגע לשימוש בתיבת דוא"ל שבבעלות המעסיק, לא מן הנמנע כי היא שימשה גם לצרכים פרטיים, ולכן יש לסווגה כתיבה מעורבת.¹³³ מנגד, בעניין **באום**¹³⁴ סיווג בית הדין את תיבת הדוא"ל כתיבה מקצועית על בסיס הסכם ההעסקה שהיה כתוב בו במפורש כי העובד מנוע מלעשות שימוש פרטי בתיבת הדוא"ל, וכי הוא מותר על כל טענה לפגיעה בפרטיות בהקשר זה.¹³⁵ בית הדין פסק כי אף שהתיבה מסווגת כתיבה מקצועית, נדרש לבחון אם קיימת הצדקה לגילוי המידע הפרטי.¹³⁶ בדומה לזה, בעניין **בונגרט** פסק בית הדין כי מכיוון שהחברה הציגה מסמך האוסר על עובדים לעבוד בעבודות פרטיות במחשבי החברה, ניתן לראות במסמכים השמורים על גבי מחשב החברה לכל היותר "תיבה מעורבת".¹³⁷ דיון זה תואם את פסק הדין ב**איסקוב ענבר**, שלפיו, על פי עקרון השקיפות, אם המדיניות הנוהגת במקום העבודה בנוגע לשימוש בטכנולוגיות מידע לא הובאה לידיעתו של העובד, קמה לעובד ציפייה סבירה לפרטיות בשימוש בטכנולוגיות המידע במקום העבודה, לרבות לצרכיו הפרטיים.¹³⁸

¹³⁰ שם, בפס' 30.

¹³¹ שם, בפס' 26.

¹³² פרשת **בונגרט**, לעיל ה"ש 87, בפס' 17–21 לפסק הדין.

¹³³ פרשת **מאפי**, לעיל ה"ש 88.

¹³⁴ פרשת **רובורופ**, לעיל ה"ש 92.

¹³⁵ שם, בפס' 20–21.

¹³⁶ שם, בפס' 21.

¹³⁷ פרשת **בונגרט**, לעיל ה"ש 87, בפס' 16 לפסק הדין.

¹³⁸ פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 24–25 לפסק הדין.

האופן השני שבו נדונה דרישת המדיניות הוא כדרישה מחייבת של הלכת **איסקוב ענבר** שהיעדר התקיימותה מביא לפגיעה בפרטיות שהשלכותיה הן קביעת בית הדין כי לא ניתן לבצע מעקב וניטור אחר העובדים. לדוגמה, בעניין **גרטי**,¹³⁹ במסגרת תביעה שנוגעת לשאלת קיום יחסי עובד-מעסיק, דחה בית הדין בקשה לעיין בתיבת דוא"ל שהוקצתה לתובע וקבע כי גם אם היה מדובר בתיבת דוא"ל מקצועית, הרי שלא הוצג נוהל מדיניות בנוגע לשימוש בתיבה זו שלפיו קיימת אפשרות לבצע פעולות ניטור ומעקב בה מצד המעסיק.¹⁴⁰ בעניין **קלנסווה** העניק בית הדין משקל מכריע לדרישת המדיניות ופסק כי לא התקיימה הסכמה מדעת, מכיוון שהעירייה לא קבעה מדיניות ברורה בכל הנוגע לשימוש בשעון, וממילא לא שיתפה את העובדות או את ועד העובדים בכך.¹⁴¹ בעניין **סעדה**¹⁴² התייחס בית הדין להיעדר יידוע כתנאי סף וקבע שמכיוון שהמעסיק לא הנהיג מדיניות ברורה בנוגע לשימוש בטכנולוגיות ולא יידע את עובדיו בדבר פעולות מעקב, אין טעם להיכנס לשאלת קיומם של תנאים אחרים, לרבות עקרון הלגיטימיות והמידתיות, שהם תנאים מצטברים להתרת ניטור ומעקב מצד המעסיק.¹⁴³

גם בעניין **אנחין**, העוסק בבקשה לניטור התכתבויות דוא"ל של עובד שפוטר כדי להוכיח שהפר חובות סודיות המוטלות עליו כלפי המעסיק, ניתנה לדרישת המדיניות משקל מכריע.¹⁴⁴ בית הדין דחה בעניין זה את הבקשה ופסק כי לא התקיימו התנאים שנקבעו בהלכת **איסקוב ענבר** המתירים למעסיק לנטר את תיבת הדוא"ל של עובדו, וקבע כי מכיוון שלא הייתה למעסיק מדיניות ניטור, לא התקיימו תנאי המידתיות ועקרון הלגיטימיות.¹⁴⁵

עם זאת יצוין כי ברוב רובם של המקרים שבהם לא הוכרה פגיעה בפרטיות או הוכרה חלקית, לא מנעו בתי הדין גילוי מידע במקרה שבו לא הייתה מדיניות מצד המעסיק אף שמדיניות היא תנאי לעקרון השקיפות ולדרישת ההסכמה.¹⁴⁶ יתור על כן, במקרים אחרים נקבע שדרישת המדיניות אינה רלוונטית כלל. בעניין **שטטר**¹⁴⁷ קבע בית הדין הארצי לעבודה שדרישת המדיניות שנקבעה בהלכת **איסקוב ענבר** ובעניין **קלנסווה** רלוונטית למקרים שבהם המעסיק מבקש להנהיג הסדר מובנה הכרוך בפגיעה בפרטיות (כפי שנדון בעניין **קלנסווה**), או כאשר המעסיק מבקש גישה ישירה למחשב העובד שתהיה בלתי אמצעית (כפי שנדון בעניין **איסקוב ענבר**).¹⁴⁸ לפיכך לפי פסק הדין, דרישה זו אינה רלוונטית כאשר מדובר בבקשה לגילוי מסמכים, שאז האיזון נעשה בין פגיעה בפרטיות

¹³⁹ סע"ש (אזורי ת"א) 71727-10-18 גרטי – לב הדקל - סוכנות לביטוח (2004) בע"מ (נבו 12.4.2020).

¹⁴⁰ שם, בפס' 19.

¹⁴¹ פרשת **עיריית קלנסווה**, לעיל ה"ש 1, בפס' 144 לפסק הדין.

¹⁴² פרשת **סעדה**, לעיל ה"ש 92.

¹⁴³ שם, בפס' 107.

¹⁴⁴ פרשת **אנחין**, לעיל ה"ש 81, בפס' 5-8 לפסק הדין.

¹⁴⁵ שם, בפס' 40-42.

¹⁴⁶ ראו בפרק א לעיל.

¹⁴⁷ פרשת **שטטר**, לעיל ה"ש 44.

¹⁴⁸ שם, בפס' 13.

לבין אינטרס הגילוי וכפוף לנסיבות כל מקרה וכשקיימת אפשרות לתור אחר המנגנון שימזער את הפגיעה בפרטיות.¹⁴⁹

כמו כן, בעניין **המועצה האזורית פרדיס**,¹⁵⁰ במסגרת תביעה בגין פיתורים של מנכ"ל המועצה, פסק בית הדין כי אין בהלכת **איסקוב ענבר** כדי לחסום בקשות כגון בקשת המועצה לעיין בדוחות איתורן פנגו של המנכ"ל בטענה שאלו יאפשרו לה להוכיח שדיווח על ביצוע עבודה בשעה שלא שהה במקום העבודה, וכי בבחינת בקשות מעין אלו יש לשקול את אינטרס הגילוי אל מול מנגנון הממזער את הפגיעה בפרטיות.¹⁵¹

דרישת השקיפות, שמטרתה היא יידוע העובד בדבר העובדה שנאסף עליו מידע ובדבר סוג המידע שנאסף, היא חשובה כמובן. עם זאת יודגש כי הן בפסק דין **איסקוב ענבר** והן ביישומו בבתי הדין לעבודה היא נכרכת עם סוגיית ההסכמה. בעניין **בלקאר**¹⁵² עלה כי בית הדין מתייחס לעקרונות השקיפות כמעין סף נמוך יותר לדרישת ההסכמה. בית הדין ציין כי המעסיק לא קיבל את הסכמת העובדת להתקנת אמצעי מעקב וניטור "ואף לא הודיע לה על אמצעי הפיקוח שהתקין במחשבי המשרד".¹⁵³ בעניין **אודיס**, במסגרת טענת התובע ליחסי עבודה פוגעניים, ציין בית הדין כי המעסיקה פעלה לפי הדרישות שנקבעו בהלכת **איסקוב ענבר** כשהודיעה לעובדיה והזהירה אותם מראש שישתכחן שהמידע האישי שלהם יהיה חשוף אם יבחרו להעלות מידע אישי במחשביה.¹⁵⁴ במילים אחרות, נראה כי כאשר העובד יודע על מדיניות החברה באשר לאיסוף המידע, אזי בתי הדין רואים בכך מתן הסכמה כללית לאיסוף המידע, לעיבודו ולשימוש בו. ברצוננו לחדד כי למבחן ההסכמה בפסק הדין רבדים נוספים, התלויים אף בשאלות הנוגעות לספרה שבה המידע נאסף – היותה ספרה פרטית או ציבורית-עסקית (בהקשר של הלכת **איסקוב ענבר** הכוונה היא להבחנה בין סוגי תיבות הדוא"ל השונות) – ואולם התפיסה הבסיסית שלפיה שקיפות כרוכה בהסכמה סותרת את ההלכה והיא אף בעייתית, כפי שנפרט בפרק הבא.

2. השלכות הפגיעה בפרטיות

כאמור, פסק דין **איסקוב ענבר** עסק בשאלת כשירותן הראייתית של תכתובות שהתקבלו תוך פגיעה בפרטיות. ואכן, כפי שניתן לראות לעיל בדיאגרמה מס' 3, מרבית המקרים שבהם בתי הדין אזכרו את הלכת **איסקוב ענבר** עסקו בבקשות לגילוי מסמכים ולפסילת ראיות.

עם זאת בכ-13 פסקי דין שבחנו דנו בתי הדין בהשלכה אפשרית נוספת לפגיעה בפרטיות במקום העבודה – פסיקת פיצויים. ואולם, כאשר נפסקו פיצויים, היו הפיצויים נמוכים יחסית לסכום הקבוע בחוק הגנת הפרטיות, שלפיו בית המשפט רשאי לפסוק פיצוי

¹⁴⁹ שם.

¹⁵⁰ פרשת **מרעי**, לעיל ה"ש 96.

¹⁵¹ שם, בפס' 15.

¹⁵² סע"ש (ת"א) 16-06-60161 **בלקאר – בלקין** (נבו 27.8.2019).

¹⁵³ שם, בפס' 75.

¹⁵⁴ פרשת **אודיס**, לעיל ה"ש 47, בפס' 82 לפסק הדין.

ללא הוכחת נזק, בסכום של עד 50,000 ש"ח.¹⁵⁵ סכומים אלו עשויים, לעמדתנו, שלא להרתיע מעסיקים מלפגוע בפרטיות. ייתכן ששיעורם הנמוך של הפיצויים (כאשר נפסקים) נובע מכך שמדובר בעוולה נזיקית לפי חוק הגנת הפרטיות וסמכותו של בית הדין לדון בה טרם הוכרה.¹⁵⁶ לפיכך כאשר נפסקו פיצויים בגין פגיעה בפרטיות נימקו זאת בתי הדין בהיותם פיצוי בגין עוגמת נפש, בגין הפרת מחויבות חוזית של המעסיק להקפיד על פרטיותו של העובד או בגין הפרת זכות יסוד חוקתית.

כך, למשל, בעניין **גורליק** פסק בית הדין כי בסמכותו לפסוק פיצויים בגין פגיעה בפרטיות ללא הוכחת נזק, מכיוון שגם אם בית הדין אינו מוסמך לפסוק פיצוי לפי לחוק הגנת הפרטיות, "הרי שניתן לייחס את הפיצוי אותו פסקנו לתובעת בגין הפגיעה בפרטיותה כפיצוי על עוגמת הנפש שנגרמה לה בשל הפרת מחויבותו החוזית של המעסיק כלפיה". בית הדין פסק לתובעת פיצויים בסך 20,000 ש"ח בגין פגיעה בפרטיותה.¹⁵⁷ בדומה לזה, בעניין **זוחוביצקי** פסק בית הדין לתובע 20,000 ש"ח בגין עוגמת הנפש שנגרמה לו מפגיעה בפרטיותו.¹⁵⁸ בעניין **גרידנב** צוין כי אם תוכח פגיעה בפרטיות, ניתן לפסוק פיצוי מכוח הפרת זכות יסוד חוקתית.¹⁵⁹ בעניין **בלקאר** ציין בית הדין כי אינו מוסמך לפסוק פיצויים לפי חוק הגנת הפרטיות, אך נעזר בעמדת המחוקק בדבר סכום הפיצוי הראוי בגין פגיעה בפרטיות ללא הוכחת נזק כפי שעולה בחוק, וקבע את סכום הפיצויים ל-50,000 ש"ח.¹⁶⁰ לעומת זאת בעניין **באר יעקב** קבע בית הדין את הפיצוי "על רקע הנסיבות ובשים לב לכך שלא הוכח כי הפגיעה בפרטיות נעשתה בכוונת מכוון" לסך של 5,000 ש"ח.¹⁶¹ בדומה לזה, בעניין **סוריא** היה סכום הפיצויים בנסיבות העניין 4,000 ש"ח.¹⁶²

כאמור, מתוך כלל ההליכים שנבדקו פסק בית הדין פיצויים בגין פגיעה בפרטיות בשישה מקרים, בסכומים הנעים מ-4,000 ש"ח ל-50,000 ש"ח.

לעמדתנו, חשוב להסדיר את סמכות בית הדין לפסוק פיצויים בגין פגיעה בפרטיות הן כדי להגביר את השימוש בכלי זה להרתעת מעסיקים והן כדי ליעיל את הדיון בשאלות של

¹⁵⁵ ס' 29 לחוק הגנת הפרטיות. על פי חוק בית הדין לעבודה, התשכ"ט-1969, אין לבית הדין סמכות לדון בתביעות נזיקיות למעט בעילות ספורות בקשר לסכסוך עבודה. ראו שם, בס' 24(א), 24(א)(ב).

¹⁵⁶ ראו לעיל ה"ש 51.

¹⁵⁷ עניין **גורליק**, לעיל ה"ש 51, בפס' 29-30 לפסק הדין. קביעה דומה ניתן לראות בפסקי דין נוספים. ראו סקירה בעניין זה המוצגת בפרשת **חננאל**, לעיל ה"ש 51.

¹⁵⁸ סע"ש (אזורי חי') 6017-09-16 **חקי – המחדש תעשיות (מנת"ש) בע"מ**, פס' 68 לפסק הדין (נבו) (25.12.2018).

¹⁵⁹ פ"ה (אזורי ת"א) 50861-03-20 **מעבדות ים המלח בע"מ – גרידנב**, פס' 22 לפסק הדין (נבו) (21.11.2020).

¹⁶⁰ פרשת **בלקאר**, לעיל ה"ש 152, בפס' 107-108 לפסק הדין. סכום דומה (40,000 ₪) נפסק גם בעניין **סעדה**, לעיל ה"ש 92, בגין פגיעה בפרטיות העובד.

¹⁶¹ פרשת **חננאל**, לעיל ה"ש 51.

¹⁶² פרשת **סוריא**, לעיל ה"ש 92.

פגיעה בפרטיות במסגרת יחסי עובד-מעסיק, בדומה לסמכות שניתנה לבתי הדין לעבודה במסגרת הדין לדון ולפסוק פיצויים נזיקיים בגין לשון הרע¹⁶³ ובגין הטרדה מינית.¹⁶⁴ מבחינת תוצאות ההחלטות ופסקי הדין שעסקו בקבילות ראיות בטענה שהושגו תוך פגיעה בפרטיות מצאנו כי מבין 20 פסקי דין שעסקו בפסילת ראיות, בכ-60% מהמקרים קיבל בית הדין במלואה או בחלקה את הבקשה לפסילת ראיות.

3. ממצאים נוספים

(א) זהות הצדדים

הגדרנו כ-40% מן העובדים (או עובדים לשעבר) שהיו צד להליכים שאותם בדקנו "עובדים בכירים". מדובר בעובדים בתפקידים בכירים, כגון מנכ"לים, סמנכ"ל ומנהלים בכירים¹⁶⁵ או עובדים בתפקידי מפתח החשופים למידע עסקי רגיש.¹⁶⁶ להבחנה זו יש חשיבות, שכן פיתוח המבחנים שנקבעו בהלכת **איסקוב ענבר** תלוי במידה רבה בסוג המקרים המובאים לבתי הדין. כאשר מדובר בעובד בכיר, בעל חובות אמון וסודיות, הפגיעה באינטרסים של המעסיק מתעצמת, ונוסף על זה ניתן אף לטעון כי יש לתת משקל רב יותר להסכמה בשל פערי כוחות פחות משמעותיים. דוגמה להתייחסותו הייחודית של בית הדין לתפקיד הבכיר ניתן לראות בפסיקה בעניין **אקספו**:¹⁶⁷

מאחר והנתבע שימש בתפקיד בכיר בנתבעות, ועל כך אין חולק, טיב ואופי העבודה שלו, דרישות התפקיד ומהותו היו לכאורה בעלי אופי של משרה מיוחדת של אימון אישי. את חובות הזהירות מחד ויחסי האימון מאידך, שמצופים מעובד במשרה בכירה יש, לעניות דעתי, לקחת בחשבון בעת בחינת בקשה כגון זו שעומדת בפני. וודאי כאשר עובד בכיר אשר יכול להסב למעסיקתו נזק גדול מדובר, נזק שיכול ויהיה גדול מן הנזק שיכול עובד זוטא אשר אינו חשוף לכל סודותיה העסקיים להסב. אף שיקול זה ילקח בחשבון בעת בקשת מעסיקה זו או אחרת להגן על קניינה מפני עבירות ונזקים מצידו של העובד.

בעשרה פסקי דין והחלטות מתוך המאגר שלנו התייחסו בתי הדין לשאלת ביסוס ההסכמה במסגרת חוזית בין הצדדים להליך בקשר לפעולות מעקב או ניטור (למשל דיון בתנאים בהסכם ההעסקה בנוגע למעקב אחר תיבת הדוא"ל). בשישה מהמקרים הללו היה מדובר בעובדים שסיווגו כעובדים בכירים, ובשני מקרים נוספים הייתה מעורבות של ארגוני עובדים. בכל יתר פסקי הדין במאגר הדיון בשאלת ההסכמה לא היה קשור להסכמה חוזית.

¹⁶³ ס' 24 (א) לחוק בית הדין לעבודה.

¹⁶⁴ ס' 10 לחוק למניעת הטרדה מינית, התשנ"ח-1998.

¹⁶⁵ ראו פרשת **מרעי**, לעיל ה"ש 96; פרשת **בובר**, לעיל ה"ש 83.

¹⁶⁶ לדוגמה, גישה לפרטי לקוחות. ראו פרשת **אנחין**, לעיל ה"ש 81; פרשת **איסתא**, לעיל ה"ש 92.

¹⁶⁷ פרשת **אקספו**, לעיל ה"ש 7, בפס' 27 לפסק הדין.

הבחנה נוספת שעלתה מבדיקת פסקי הדין היא שרק בשני מקרים הייתה מעורבות של ארגוני עובדים: בעניין קלנסווה ובעניין הסתדרות עובדי המדינה. בשני הליכים אלו ראינו כי בית הדין בחן לעומק את המבחנים שנקבעו בהלכת איסקוב ענבר ונכנס "בעובי הקורה" של הטכנולוגיה הנדונה בכל מקרה ובתנאים לביסוס דרישת ההסכמה כאמור.

(ב) מעורבות מומחים בהליך

מפסקי הדין וההחלטות עולה כי כמעט שלא הייתה מעורבות של מומחים לצורך בחינת הטכנולוגיה שבה נעשה שימוש ולא נשאלו שאלות בנוגע לעיצובה של הטכנולוגיה. המקרים היחידים שבהם היו מעורבים מומחים היו אלה שבהם בית הדין הורה למנות מומחה מחשבים לצורך ביצוע פסק הדין (למשל לביצוע ניטור בתיבת דוא"ל),¹⁶⁸ וכאשר הוגשה חוות דעת מטעם המעסיק לתמיכה בטענה שעובדים ביצעו פעולות אסורות במחשב (העתיקו מידע רגיש ממחשבי החברה).¹⁶⁹ בעניין קלנסווה, שבו כאמור ארגון עובדים (ההסתדרות) היה צד להליך, פסק בית הדין כי במסגרת שיקולי תכלית, מידתיות וסבירות היה על המעסיק להוכיח את טיב מערכת הזיהוי הביومترית, את תוקפה ואת מהימנותה באמצעות הצגת חוות דעת של מומחה בלתי תלוי.¹⁷⁰

(ג) יישום מבחני איסקוב ענבר בבקשות לגילוי מסמכים

ממצא נוסף שעלה מהמחקר נגע לשתי הגישות הקיימות בעניין גילוי מסמכים – כאשר האחת עושה איזון בין אינטרסים שונים מבלי לבחון את הפגיעה בפרטיות לעומק, והשנייה רואה בגילוי מסמכים מטרה לגיטימית ובוחנת את שאלת הפגיעה בפרטיות לפי הלכת איסקוב ענבר.

הגישה הראשונה היא בקביעה כי הליך הניתוח במקרים של גילוי מסמכים אינו נוגע להלכת איסקוב ענבר, מכיוון שנעשה בהם איזון בין פגיעה בפרטיות לבין אינטרס הגילוי (הוגנות, יעילות הדיון וקידום חקר האמת), ועל כן השאלה המשפטית החשובה אינה הפגיעה בפרטיות אלא רלוונטיות המסמכים להליך עצמו, בניסיון לתור אחר מנגנון שימזער את הפגיעה בפרטיות. דברים אלה נאמרו מפורשות בבית הדין הארצי בעניין שטטר:¹⁷¹

אנו סבורים כי הלכת איסקוב וקלנסווה רלבנטיות כאשר מבקש המעסיק מראש להנהיג פרקטיקה הכרוכה בפגיעה בפרטיות (ענין קלנסווה) או גישה ישירה למחשב העובד ולקבל ממנו מידע מלא לרבות כזה הכרוך בפגיעה בפרטיות בצורה בלתי אמצעית (ענין איסקוב). המכנה המשותף לשני אלה הוא שהפגיעה בפרטיות מובנית בהסדר, ולכן נדרש המעסיק ליתן ביטוי למדיניותו על מנת שהעובדים יוכלו לכלכל צעדיהם. הלכות אלה לא נקבעו בהקשר לגילוי מסמכים, כשבהקשר זה יש לשקול באופן

¹⁶⁸ ש.ם.

¹⁶⁹ פרשת מנגלוס, לעיל ה"ש 60.

¹⁷⁰ פרשת עיריית קלנסווה, לעיל ה"ש 1, בפס' 132 לפסק הדין.

¹⁷¹ פרשת שטטר, לעיל ה"ש 44, בפס' 13 לפסק הדין.

פרטני את אינטרס הגילוי במונחי הוגנות, יעילות וקידום חקר האמת מול אינטרס הפרטיות, וגם – וזה העיקר – את היכולת לתור בנסיבותיו המיוחדות של כל מקרה ומקרה אחר מנגנון מזעור הפגיעה בפרטיות, כפי שנערוך להלן.

בדומה לזה, בעניין **המועצה האזורית פרדיס**,¹⁷² במסגרת תביעה בגין פיתורים של מנכ"ל המועצה, פסק בית הדין כי אין בהלכת **איסקוב ענבר** כדי לחסום בקשות כגון בקשת המועצה לעיין בדוחות איתורן פנגו של המנכ"ל בטענה שאלו יאפשרו לה להוכיח שדיווח על ביצוע עבודה בשעה שלא שהה במקום העבודה, וכי בבחינת בקשות מעין אלו יש לשקול את אינטרס הגילוי אל מול מנגנון הממזער את הפגיעה בפרטיות.¹⁷³

לפי הגישה השנייה שאיתרנו, גילוי מסמכים הוא תכלית לגיטימית שעשויה להוביל לפגיעה בפרטיות, שאז בתי הדין בוחנים את שאלת הפגיעה בפרטיות לפי מבחני הלכת **איסקוב ענבר**. דוגמה לניתוח כאמור ניתן לראות בהחלטה שניתנה בעניין **מאפי**.¹⁷⁴ בעניין **מאפי**, במסגרת תביעה בגין פיתורין שלא כדין שהגישה עובדת לשעבר שהלכה לעולמה לאחר הגשת כתב התביעה ותביעה שכנגד שהגישה החברה, הוגשה בקשה לגילוי ועיון במסמכים ששמורים בתיבת דוא"ל של העובדת שבבעלות החברה לצורך הוכחה כי המנוחה נכנסה ללא רשות לתיבות דוא"ל של עובדים אחרים וצירפה הודעות דוא"ל אלו, הכוללות סודות מסחריים ועסקיים של החברה, לכתב התביעה שלה.¹⁷⁵ בית הדין פסק כי אף שהמסמכים המבוקשים רלוונטיים לבירור ההליך, ההיתר לניטור תיבת הדוא"ל של העובדת, שבית הדין סיווגה כתיבה מעורבת,¹⁷⁶ יינתן כפוף להתקיימות הדרישות שנקבעו בהלכת **איסקוב ענבר**, חשש לשימוש לא ראוי של העובדת או לפעילות פלילית.¹⁷⁷ דהיינו, במקרה שכזה, כאשר המידע נאסף לצורך תכלית לגיטימית אחרת (ייתכן שתכלית זו היא שימור הזיכרון הארגוני, התנהלות עסקית או הגנה על מאגרי מידע), אזי השימוש בו הוגבל לפי הלכת **איסקוב ענבר**. קרי, על אף עמידה במבחן הרלוונטיות של המסמכים דחה בית הדין את הבקשה על בסיס הכללים שנקבעו בהלכת **איסקוב ענבר**, ובייחוד דרישת המידתיות. בית הדין ציין שהחברה יכולה לפנות לעובדים אחרים שמהם נשלחו כביכול הודעות הדוא"ל הרלוונטיות, וכפוף להסכמתם, לבחון אם הוצא מתיבת הדוא"ל שלהם מידע בידי העובדת לשעבר.¹⁷⁸ אופן ניתוח דומה ניתן לראות בפסיקת בתי הדין לעבודה בעניין **אנחין** ובעניין **גרטי**.¹⁷⁹

¹⁷² פרשת **מרעי**, לעיל ה"ש 96.

¹⁷³ שם, בפס' 15.

¹⁷⁴ פרשת **מאפי**, לעיל ה"ש 88.

¹⁷⁵ שם, בפס' 1–8 לפסק דינו של השופט שביון.

¹⁷⁶ מכיוון שלא הוצג נוהל מדיניות ביחס לשימוש בתיבה. ראו שם, בפס' 36.

¹⁷⁷ שם, בפס' 37–38.

¹⁷⁸ שם.

¹⁷⁹ בפרשת **אנחין**, לעיל ה"ש 81, בחן בית הדין בקשה של מעסיק לנטר תיבת דוא"ל של עובד הן בהיבט של דרישת הרלוונטיות – זיקה ישירה בין המסמכים המבוקשים לבין ההליך – והן באשר לעמידה בכללים שנקבעו באיסקוב ענבר בדבר תיבה מעורבת. בית הדין פסק כי לא התקיימו התנאים שנקבעו בפרשת **איסקוב**

על פי הגישה הראשונה, שהלכת איסקוב ענבר אינה נבחנת בה, הזכות לפרטיות עשויה להיפגע יותר, דבר שאינו בהכרח מוצדק. לפיכך אנו סבורות שדרך הניתוח השנייה שתוארה מגינה טוב יותר על הזכות לפרטיות ויצרת קוהרנטיות בין הדין החל בהליכי גילוי מסמכים למבחני הלכת איסקוב ענבר.

ד. דיון

מהתיאור לעיל עולים קשיים מסוימים בהלכת איסקוב ענבר, ובעיקר ביישומה ובפיתוחה בבתי הדין לעבודה. בפרק זה נצביע על הקשיים העיקריים ונדון בהם לאור תאוריות של הגנת פרטיות ודיני עבודה.

טרם קיומו של הדיון נבקש שוב לחדד את שכתבנו במבוא למאמר: הזכות לפרטיות בעבודה היא אחת הזכויות החשובות ביותר הקיימות כיום. זכות זו מאפשרת את קיומו של מרחב בלתי חדיר שבו עובדות ועובדים יכולים לנהל את חייהם האישיים, ומלבד זאת – אף יכולים להביע את דעתם ללא חשש, להיות יצירתיים ולהתאגר באיגוד עובדים.¹⁸⁰ בספרה שבה כמעט כל פעולה של העובד נתונה בניטור או במעקב, וכאשר עובדים יודעים כי המעסיק יכול בקלות רבה לאסוף מידע רב עליהם, זכויות אישיות וגם אינטרסים חברתיים רחבים יותר נפגעים. מתן לגיטימציה לאיסוף מידע ללא הגבלה וללא סנקציות ברורות הוא אפוא פגיעה מהותית לא רק בפרט אלא גם באינטרסים הרחבים האמורים. לכן יש חשיבות רבה בהפניית תשומת לב מצד המשפט להקנות לעובדים הגנה תוך ריסון כוח המעסיק בשימוש בטכנולוגיות הפוגעות בזכות לפרטיות. כיום מעסיקים יכולים לעשות כמעט הכול בכל הנוגע למידע הפרטי של העובדים. הטכנולוגיות החדשות מגדילות את הפרוגטיבה המעסיקית במקום העבודה,¹⁸¹ והמעסיקים אף חשים כי הם יכולים לעשות במידע כרצונם, ברגע שנלקח.¹⁸² לפיכך עבודה היא אחת הספרות החשובות ביותר שבה יש להגן על הזכות לפרטיות.

ענבר (לעיל ה"ש 2) המתירים זאת (שם, בפס' 40–42). בעניין **גרטי**, לעיל ה"ש 139, במסגרת תביעה שנוגעת לשאלת קיום יחסי עובד–מעסיק, בחן בית הדין הן את מידת הרלוונטיות של המסמכים המבוקשים והן עמידה בכללים שנקבעו בהלכת **איסקוב ענבר** (לעיל ה"ש 2). בית הדין ציין כי נקודת המוצא היא "גילוי מרבי ורחב ככל האפשר של המידע הרלוונטי למחלוקת" אך דחה בקשה לעיין בתיבת דוא"ל שהוקצתה לתובע וקבע כי גם אם היה מדובר בתיבת דוא"ל מקצועית, הרי שלא הוצג נוהל מדיניות בנוגע לשימוש בתיבת זו שלפיו קיימת אפשרות לבצע פעולות ניטור ומעקב בה מצד המעסיק (עניין **גרטי**, לעיל ה"ש 139, בפס' 19).

¹⁸⁰ דוגמה לחשש זה ניתן לראות בפעולותיהם של עובדי אפל. כדי לקדם התאגדות עובדי אפל לא השתמשו באיפונים ובאפליקציית המסרים המובנית של אפל אלא באפליקציות שיחה מוצפנות, שהותקנו על גבי מכשירי אנדרואיד שונים "כדי למנוע מעקב מצד אפל", ראו: אושרי אלקסלסי "עובדי אפל רוצים להתאגר, אז ברור שהם עושים את זה באנדרואיד" Geektime (21.2.2022) <http://bit.ly/3K4XEMd>.

¹⁸¹ ראו De Stephano, לעיל ה"ש 30; Rogers, לעיל ה"ש 30.

¹⁸² Eric Rosenbaum, *Companies Are Collecting More Data on Employees, And Not At All Confident They Are Doing It Responsibly*, CNBC (Mar. 28, 2022), <https://tinyurl.com/2vfcekes>.

1. הדגש שמושם בשאלת ההסכמה

חוקרות וחוקרים חלוקים בעמדותיהם בדבר המתווה העיוני שבבסיס הזכות לפרטיות. הדין התאורטי עוסק רבות בשאלה זו, בעיקר כדי לבסס את חשיבותה של הזכות ולדאוג כי יינתן לה משקל בהתנגשותה עם זכויות נוספות; לקבוע את היקף ההגנה על הפרטיות; לצורך עיצוב הכללים המשפטיים למימושה.¹⁸³ הדין הישראלי מאמץ בסיס עיוני מרכזי לזכות, זה שמגדיר **פרטיות כשליטה**.¹⁸⁴ משמעותה של פרטיות כשליטה, כפי שהגדיר אותה בירנהק, היא שליטת האדם במידע על אודותיו.¹⁸⁵ גישה זו אינה מאפיינת רק את המשפט בישראל, וניתן למצוא אותה גם בארצות הברית וכן באירופה.¹⁸⁶ כך, גם באיסקוב **ענבר** אמר בית הדין הארצי לעבודה כי:

מן הערכים החוקתיים-אובייקטיביים לכבוד ולפרטיות, ובמסגרת המרחב הווירטואלי הפרטי במקום העבודה ובמהלכה, נגזרות זכויותיו של העובד לביטוי האוטונומיה האישית שלו, להגדרה עצמי ולאנונימיות. זאת, באופן המקנה לעובד שליטה על חשיפת המידע אודותיו ומניעת התחקות אחריו (tracing). שכן, מעקב אחר העובד במקום העבודה, חדירה למחשב ולדואר האלקטרוני שלו במקום העבודה, ואיבוד השליטה על הפרטיות במידע האישי שלו, עלולים לגרום לפגיעה בכבוד האדם של העובד, בפרטיותו ובאוטונומיה שלו.¹⁸⁷

הקושי המרכזי שבאימוץ הבסיס העיוני של פרטיות כשליטה הוא בכך שהמשפט כרוך את רעיון השליטה עם הפרדיגמה של פרטיות כתלוית הסכמה.¹⁸⁸ בהקשרים רבים הקשורים לטכנולוגיות חדשות יש במבחן ההסכמה קשיים לא מעטים.¹⁸⁹ כמה מחקרים

¹⁸³ ראו לעניין זה Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Ruth E. Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

¹⁸⁴ ראו בירנהק "שליטה והסכמה", לעיל ה"ש 11, בעמ' 68–72; פרשת **בן מאיר**, לעיל ה"ש 56, בפס' 37 לפסק דינה של הנשיאה חיות; פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 11 לפסק הדין; פרשת **קלנסווה**, לעיל ה"ש 1, בפס' 113 לפסק הדין.

¹⁸⁵ בירנהק "שליטה והסכמה", לעיל ה"ש 11.

¹⁸⁶ ראו Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) (להלן: Solove, *the Consent Dilemma*); Stephen Breen, Karim Ouazzane & Preeti Patel, *GDPR: Is Your Consent Valid?*, 31 BUS. INFO. REV. 19 (2020). כן ראו GDPR, לעיל ה"ש 104, בס' 7.

¹⁸⁷ פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 11 לפסק הדין.

¹⁸⁸ Anita Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861 (2000).

¹⁸⁹ ראו סיכום טוב של חלק מהביקורות אצל 20 JULIE E. COHEN, *Turning Privacy Inside Out*, THEORETICAL INQUIRIES L. 1 (2019).

מהשנים האחרונות חידדו את הבעיות הטמונות במבחן ההסכמה ככלל¹⁹⁰ ובעולם הדיגיטלי בפרט.¹⁹¹ ביקורות על מרכזיותו של מבחן ההסכמה המצויה בלב ליבה של הגישה העיונית האמורה עלו בדיונים על האסדרה האירופית,¹⁹² בספרות האקדמית,¹⁹³ בין השאר בכל הנוגע לפרטיות בעבודה.¹⁹⁴ כך, למשל, קבוצת העבודה בנושא אבטחת מידע (ה-data protection working party) של האיחוד האירופי התייחסה להקשר של עבודה וקבעה בנייר דעה משנת 2017 כי הסכמה כמעט שאינה יכולה לשמש בסיס משפטי לצורך עיבוד מידע בעבודה, אלא אם כן עובדים יכולים לסרב לעיבוד המידע ולמסירתו בלי שתהיה לכך תוצאה שלילית עליהם.¹⁹⁵ ואולם, מכיוון שנדיר שעובדים יהיו במצב שבו הם יכולים לתת הסכמה חופשית מלאה, להיות חופשיים לסרב או לשנות את דעתם, בשל מהותה של מערכת יחסי עובד-מעסיק,¹⁹⁶ אזי לבד מבמקרים חריגים מאוד יצטרכו מעסיקים להשתמש בתשתית משפטית שונה מזו של הסכמה. תשתית זו תכלול בחינתה של החיוניות באיסופו ובעיבודו של המידע לצורך אינטרס לגיטימי, וכן כללים הנוגעים למידתיות המידע שנאסף והמחויבות לבחון אם עיבוד המידע נחוץ לצורך השגת המטרה הלגיטימית וכן אם ננקטו צעדים שימעיטו ככל הניתן את הפגיעה בזכות לפרטיות.¹⁹⁷ ואכן, אחת השאלות המתמיהות בהקשר של הלכת איסקוב ענבר, ובעיקר יישומה, היא הדגש שמושם בשאלת ההסכמה בהקשר של פרטיות, כאשר בהקשרים אחרים של הגנה על זכויות עבודה בסיסיות, וכן על זכויות אדם, בתי הדין לעבודה ממעיטים מאוד מערך ההסכמה.¹⁹⁸

¹⁹⁰ לדין מעניין מאוד שהיה לאחרונה על מהותה של הסכמה ועל האופנים השונים שבהם יכולה להינתן הסכמה ובחינת תקפות ההסכמה, ראו Nancy Kim, *Consentability: Consent and IT Limits* (2019).

¹⁹¹ ראו Paul Schwartz, *Internet Privacy and the State*, 32 *CONN. L. REV.* 815 (2000); Lori Andrews, *The Fragility of Consent*, 66 *LOY. L. REV.* 11 (2020); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 *WASH. U. L. REV.* 1461 (2019). כן ראו Solove, *the Consent Dilemma*, לעיל ה"ש 186; VELIZ, לעיל ה"ש 8. לדין מורחב בספרות זו ואחרת הנוגעת לשאלת ההסכמה ראו אלבין ועומר, לעיל ה"ש 105.

¹⁹² ראו Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 *INT'L* Alessandro Mantelero, *The Future of Consumer Data*; *DATA PRIV. L.* 250 (2014) *Protection in the E.U.: Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, 30 *COMPUT. & SOC'Y L. REV.* 643 (2014).

¹⁹³ ראו Solove, *the Consent*; 188; Allen, לעיל ה"ש 8; Cohen, *What Privacy is For*; *Dilemma*, לעיל ה"ש 186.

¹⁹⁴ Frank Hendrickx, *Privacy, Data Protection and Measuring Employee Performance: The Triggers of Technology and Smart Work*, 9 *EUR. LAB. L. J.* 99 (2018); (להלן: Hendrickx, *Employee Performance*).

¹⁹⁵ *Opinion 2/2017*, לעיל ה"ש 24, בעמ' 3.

¹⁹⁶ שם, בעמ' 4, 23.

¹⁹⁷ שם.

¹⁹⁸ דוגמאות בולטות לכך הן כמובן אוסף החוקים הקוגנטיים דיני העבודה; החלטות שיפוטיות הנוגעות לזכויות אדם בסיסיות, כגון חופש העיסוק, בהן נקבע כי ההסכמה כמעט אין משקל (ראו לעניין זה את

גם בתאוריות של דיני עבודה נתונה ההסכמה ביחסי עבודה בסימן שאלה כאשר מדובר בזכויות עבודה ואדם בסיסיות. דיני העבודה מניחים קיומם של פערי כוחות בין הצדדים ליחסי עבודה לאור התלות והכפיפות של העובד למעסיק שלו. אלה מייצרים, כפי שקהאן-פרוינד ציין,¹⁹⁹ פערי מיקוח בין העובד לבין המעסיק, המצדיקים את קיומם של ארגוני עובדים וכן התערבות רגולטורית בתוכנו של חוזה העבודה מתוך הנחה כי בשל פערי מיקוח אלה הסכמתו של עובד לתנאים המוצעים לו תיעשה לאו דווקא מתוך בחירה חופשית. גם פערי המידע בין הצדדים ליחסי העבודה, בעיקר בכל הנוגע לטכנולוגיות חדשות, מונעים מן העובד לתת הסכמה חופשית מדעת ומרצון, או לסרב, לאיסוף המידע אודותיו. לעובד אין הכלים לדעת אם יש טכנולוגיות מידתיות יותר להשגת התכליות הרלוונטיות לעסק. הקושי בהשאת מרחב להסכמה אף מתעצם נוכח מחקרים נוספים שהראו כי לא המעבר מעבודות לחוזה בדיני העבודה הוא שאפשר את מה שמכונה "עבודה חופשית", דהיינו עבודה שאינה כוללת כבילה ותלות גדולה במעסיק. סטיינפלד הראה כי במאה התשע-עשרה, בעת המעבר של המשפט מראיית מערכת היחסים כמערכת יחסים של עבדות לעבר תפיסה חוזית, גרמו כבלי השוק והכלכלה לכך שעובדים לא היו חופשיים לבחור. הוא המשיך והראה כי דווקא חוקי המגן המתערבים בחופש החוזים בין הצדדים הם שאפשרו יותר חופש לעובדים, ובעקבות זאת – מימוש הרעיון של עבודה חופשית בניגוד לעבודה בכפייה.²⁰⁰ דברים אלה נכנסו אף לתוך הכתיבה בנוגע לזכות לפרטיות בעבודה אגב חידוד הקושי הקיים במבחן ההסכמה.²⁰¹

כפי שצינו לעיל, הלכת **איסקוב ענבר** בעצמה התייחסה לתפיסה זו של דיני העבודה. כמה אמירות בפסק הדין מדגישות כי בשל פערי הכוחות בין הצדדים קשה מאוד לתת הסכמה חופשית.²⁰² בשל תובנות ואמירות אלה קשה מאוד להבין את ההלכה הקובעת כי יש לקבל את הסכמת העובד, וכי זו צריכה להיות מדעת ומרצון חופשי. קשה עוד יותר להבין את דיון העומק שמבצעת ההלכה לאור נקודת מוצא זו שמייצרת הבחנות בין תיבות דוא"ל שונות, בהתכתבות עם הבחנה בין ספרות פרטיות לציבוריות-עסקיות, בהדגישה את היכולת לתת הסכמה מדעת ומרצון חופשי בכל אחת מהן, למעט זו של התיבה הפרטית-חיצונית. זהו החלק החשוב ביותר בפסק הדין, וכפי שהראינו, זה החלק שבתי הדין לעבודה מדגישים על אף הסתירה הפנימית האמורה.

הממצאים שלנו, אשר מראים כי בתי הדין מתייחסים בשלושה אופנים למבחן ההסכמה, חשובים בהקשר זה. בתי הדין יכולים להגדיל את מספר המקרים שבהם הם מתייחסים לפרטיות כקוגנטית, ולכן לא ניתן להשיג הסכמה לפגיעה בפרטיות. נוסף על זה, וכפי שצינו קודם לכן, חשוב כי בתי הדין יפתחו את ההלכה בדבר הסכמה שניתנת

החלטת בית הדין הארצי לעבודה בעניין ע"ע (ארצי) 164/99 פרומר וצ'ק פוינט – רדגארד בע"מ, פר"ע לד 294 (1999). דוגמה נוספת הם מצבים שבהם יש הסכמה למעשים המוגדרים כהטרדה מינית במצב של יחסי מרות בעבודה, ראו ע"ע 274/06 פלונית נ' אלמוני (נבו 26.3.2008).

¹⁹⁹ DAVIES & FREEDLAND, לעיל ה"ש 15.

²⁰⁰ ראו STEINFELD, לעיל ה"ש 26, בעמ' 1–28.

²⁰¹ לכתיבתו של הנדריקס בעניין זה, ראו Hendrickx, *Employee Performance*, לעיל ה"ש 194.

²⁰² פרשת **איסקוב ענבר**, לעיל ה"ש 2, בפס' 28 לפסק הדין.

מראש מדעת ומרצון, דבר שלא נעשה לעומק עד היום.²⁰³ מלבד זאת, כאשר בתי הדין יבחנו בצורה ברורה יותר את שאלת התכלית הלגיטימית ויחדדו את השאלה מתי נעשית פגיעה בפרטיות, יצטמצמו להערכתנו המקרים שבהם תתאפשר פגיעה בפרטיות בלי לדרוש את הסכמת העובד כלל. לבסוף – תובנות אלה מחדדות את הטענה כי יש לתת להסכמה משקל קטן ביותר ביחס למבחנים ולעקרונות האחרים שבית הדין מאמץ בהלכת **איסקוב ענבר**. עיקר המשקל הדיוני צריך לעבור לבחינת המבחנים והעקרונות האחרים באופן המוצע במאמר זה.

עוד נבקש לציין כי נקודת המוצא המצביעה על פערי הכוחות בין הצדדים ליחסי העבודה הקשורים לתלות ולכפיפות של העובד למעסיקו אף מצדיקים מתן מידע בידי עובדים. ההנחה היא כי ככל שהמידע שיהיה בידי העובד רב יותר, כך יצטמצמו פערי הכוחות ויאפשרו ניהול משא ומתן מבוסס יותר. לכן שקיפות כערך היא חשובה. ואולם שקיפות לבדה אינה בהכרח מספקת, וחשוב מזה – לא שקיפות היא שתאפשר איזון כוח מלא בין הצדדים, ואין בה כדי להצביע על הסכמה מלאה וחופשית. לשקיפות מטרה מצומצמת יותר והיא מתן ידע בידי העובד על המדיניות שחלה עליו. או במילים אחרות, על האופן שבו מרחב האוטונומיה שלו מצטמצם בידי המעסיק.²⁰⁴ כאשר שקיפות מלווה בפעילות של ארגוני עובדים, אזי יש לה קשר הדוק יותר לאפשרות לאזן את פערי הכוחות, כמו שעולה מהרעיון שבבסיס ה- information and consultation directive של האיחוד האירופי.²⁰⁵ ואולם עדיין נותרת פתוחה השאלה אם העובד נתן הסכמה מדעת ומרצון בשל המידע המצוי בידו. כמו כן עולה השאלה אם הסכמה קיבוצית מספקת כדי לפגוע בזכות האישית לפרטיות, נקודה שבית הדין הארצי לעבודה השאיר בפרשת **קלנסווה** בצריך עיון.²⁰⁶ שאלה זו מורכבת ותלויה נסיבות, ולכן בחרנו לא להתעמק בה במאמר זה.

²⁰³ יש לציין בהקשר כי ישנם מחקרים רבים העוסקים באופן בו ניתן לוודא הסכמה מיועדת אמיתית. ראו למשל Luiza Jarovsky, *Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs)*, 4 EUR. DATA PROT. L. REV. 447 (2018); Raul Pardo and Daniel Le Metayer, *Analysis of Privacy Policies to Enhance Informed Consent* Lecture Notes in Computer Sciences (2019).

²⁰⁴ מחקרים מהתחום של חוזים אישיים הראו כי התרומה של גילוי מידע לצמצום פערי הכוחות מוגבלת מאוד. ראו Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 Eyal Zamir & Yuval Farkash, *Standard Form Contracts*; U. CHI. L. REV. 165 (2011) *Empirical Studies, Normative Implications, and the Fragmentation of Legal Scholarship: Comments on Florencia Marotta-Wurgler's Studies*, 12 JERUSALEM REV. LEG. STUD. 137 (2015).

²⁰⁵ Directive 2002/14/EC, of the European Parliament and of the Council of 11 March 2002 establishing a General Framework for Informing and Consulting Employees in the European Community – Joint Declaration of the European Parliament, the Council and the Commission on Employee Representation, O.J. (L 80), 29–34

²⁰⁶ פרשת **עיריית קלנסווה**, לעיל ה"ש 1.

לבסוף נבקש לציין כי השארת מבחן ההסכמה על כנו מעניקה כוח לעובדים בכירים שתאורטית יש להם כוח רב יותר לסרב למסירת המידע הפרטי אודותיהם. ואכן, כפי שהממצאים שלנו מראים, כמעט מחצית מהמקרים שהגיעו לפתחם של בתי הדין לעבודה בנוגע לשאלת הפגיעה בפרטיות נגעו למצבים שבהם נדון מידע פרטי של עובדים בכירים. לפיכך הדין הקיים עשוי לפגוע יותר בעובדים מוחלשים שלהם כוח מיקוח קטן בהרבה.

2. שאלת הפגיעה בפרטיות

ממצא שעולה מהמחקר נוגע לשאלה אם נבחנת הפגיעה בפרטיות ובאיזה אופן. הממצאים מראים כי שאלה זו נדונה בבתי הדין חלקית בלבד. בחלק מן המקרים יצרו בתי הדין הבחנה בין מידע פרטי לבין מידע עסקי, הבחנה שהיא חשובה מאוד, שכן על פני הדברים ניתן להניח כי אין פגיעה בפרטיות כאשר המעסיק אוסף מידע עסקי מהעובד. ואולם, היו מקרים שבהם הבחנה שכזו לא נעשתה כלל. מלבד זאת, בתי הדין נשענים יתר על המידה על זהות הפלטפורמה (מקצועית, מעורבת או פרטית) כדי לקבוע אם הייתה פגיעה בפרטיות אף שבכולן עשוי להיות מידע פרטי או עסקי. נוסף על זה, בתי הדין עדיין לא התמודדו בצורה מעמיקה עם מצבים מטושטשים של פרטי ועסקי. כך, בתי הדין אינם נכנסים בעובי הקורה ושואלים: מהי בדיוק הפגיעה בפרטיות? למשל, האם כאשר איסוף המידע נעשה במסגרת טכנולוגיה של מטא-דאטה שאוספת מידע לא מזוהה מדובר בפגיעה בפרטיות? האם מדובר בפגיעה זהה לאיסוף מידע לא אנונימי מהמחשב הפרטי של העובד? יצוין כי היעדר התייחסות מעמיקה לשאלה מהי בדיוק פגיעה בפרטיות אינו מאפיין רק את פסיקת בתי הדין לעבודה. לאחרונה ביקר מיכאל בירנהק את בית המשפט העליון על שגם הוא אינו עוסק בשאלה זו לעומק.²⁰⁷

המחלוקת בדבר הבסיס העיוני של הזכות לפרטיות הובילה חלק מהחוקרים להציע טקסונומיה לזכות ולא הגדרה אחת ברורה. אחד הסיווגים המעניינים ביותר שהוצעו בשנים האחרונות בנוגע למידע הוא של דניאל סולוב.²⁰⁸ נקודת המוצא של סולוב היא שהמונח "פרטיות" מצוי באי-סדר, אינו מובן ומעורפל, וכי אין כל אפשרות למצוא ערך אחד לזכות. לגישתו, הפרה של פרטיות כוללת כמה וכמה מצבים, או במילים אחרות, משפחה של מצבים שקשורים זה לזה, אבל אינם כוללים ערך מוגן אחד.²⁰⁹ המשותף למצבים אלה הוא שמדובר בפעולות שמסיגות גבול ופוגעות.²¹⁰ הטקסונומיה שהוא מציע נועדה לאתר את המצבים האמורים ולהשליט בהם סדר כדי להצביע על הפגיעה שגורמת הפרה של פרטיות. הדגש שסולוב שם בפגיעה יכול מאוד לסייע לבתי הדין להגדיר הגדרה מדויקת יותר את הפגיעה שנעשית לפרטיות בכל מקרה ומקרה, דבר שכפי שהמחקר שלנו

²⁰⁷ ראו מיכאל בירנהק "פרטיות במשבר: הנדסה חוקתית והנדסת פרטיות" *משפט וממשל* כד 149, 158 (2021); Michael Birnhack, *Constitutional Privacy in Israeli Law*, in OXFORD HANDBOOK ON THE ISRAELI CONSTITUTION (Aharon Barak, Barak Medina & Yaniv Roznai eds., forthcoming 2023).

²⁰⁸ שם, בעמ' 480–481, Solove, *A Taxonomy of Privacy*, לעיל ה"ש 54.

²⁰⁹ שם, בעמ' 481–480.

²¹⁰ שם, בעמ' 484.

הראה לא נעשה עד היום. הטקסונומיה המוצעת כוללת ארבעה מצבים פוגעניים ובהם תתי-מקרים המכילים פגיעות נוספות: (1) איסוף מידע; ²¹¹ (2) עיבוד מידע; ²¹² (3) פיזור מידע; ²¹³ (4) פלישה. ²¹⁴ בנוגע לכל אחת מקבוצות אלה הוא מקיים דיון מעמיק על הפגיעה. למשל, לא כל איסוף מידע הוא פוגעני, אבל יש מצבים שבהם הוא עשוי להיות כזה, כמו למשל כאשר אדם נתון בסוג של מעקב, ²¹⁵ בשל ההשפעה שעשויה להיות למעקב על ההתנהגות האנושית. נוסף על זה, עיבוד מידע כולל כמה וכמה מצבים, ובהם שימור המידע (ובין השאר בעיות של שמירת מידע), צירוף מידע (אגרגציה), שיוך מידע לאדם מסוים (זיהוי), מניפולציה על המידע, שימוש משני, חיפוש במידע ועוד.

בכל אלה יכולים להיות מצבים שפוגעים בזכות הפרטיות, ואולם אלה לא נדונו לעומק בפסיקת בתי הדין. כך, למשל, בכל הנוגע לאיסוף המידע עולה שאלה חשובה – מאין נאסף המידע, שכן הוא יכול להיאסף ממקורות רבים, כגון תכתובות דוא"ל, צ'טים, הקלטות וידאו ואודיו, ועוד מידע שנמצא ברשת. מכיוון שאיסוף המידע נעשה בלי לבצע הבחנה בין מידע עסקי לבין מידע פרטי, המידע שנאסף עשוי להיות מידע פרטי ביותר, ושמירתו בידי המעסיק, כשבידיו היכולת לגשת אליו, היא פגיעה בפרטיות של העובד. מלבד זאת, גם מידע עסקי עשוי להיות מוגדר כמידע פרטי.

גם בכל הקשור לעיבוד המידע יכולה להיות פגיעה בפרטיות. הליך עיבוד המידע מתייחס לשימוש במידע לאחר שזה נאסף. ²¹⁶ ניתן להצביע על שלוש סכנות ממשיות לפרטיות בעת הליך עיבוד המידע. אלה סוכמו בידי בודי ואחרים והוצגו כשלוש פגיעות אפשריות: אגרגציה, שימוש שניוני (או במילים אחרות היעדר צמידות מטרה) ודיוק. ²¹⁷ הראשונה, אגרגציה, היא פגיעה בפרטיות שנובעת מצירוף המידע על משתמש ספציפי. כאשר המערכת לוקחת פיסות מידע כאלה ואחרות ומאחדת אותן, אפשר לקבל תמונה הרבה יותר רחבה על האדם. למשל: צירוף של פיסות מידע על פעילויות ברשתות החברתיות עם פעילות כללית ברשת ובעבודה יוצר תמונה רחבה מזו שניתן ללמוד מכל אחד מהחלקיקים לבדם. השנייה, שימוש שניוני, מתייחסת למצבים שבהם משתמשים במידע למטרה שונה מזו שלשמה נאסף מידע זה. שימוש כזה הוא בעייתי מאוד, שכן הוא שולל מהאדם את השליטה במידע שהוא כן הסכים למסור למטרה מסוימת. עובדות המקרה בהלכת **איסקוב ענבר** הן דוגמה מובהקת לכך שמידע שנאסף מתכתובות דוא"ל לצורך הגנה על מאגרי מידע ונשמר אצל המעסיק שימש אחר כך את המעסיק למטרה אחרת לגמרי. השלישית נוגעת לדיוק. בודי וחבריו טוענים כי אי הדיוק לכשעצמו הוא פגיעה בפרטיות, שכן איסוף המידע נעשה לצורך הגעה למסקנות מסוימות, ומסקנות אלה

²¹¹ שם, בעמ' 491–505.

²¹² שם, בעמ' 505–525.

²¹³ שם, בעמ' 525–552.

²¹⁴ שם, בעמ' 552–562.

²¹⁵ ראו דיון מעניין מאוד על מעקבים, שם, בעמ' 491–499.

²¹⁶ שם, בעמ' 505.

²¹⁷ Matthew T. Bodie et al., *The Law and Policy of People Analytics*, 88 U. COLO. L.

REV. 961, 36–39 (2017).

עשויות לפגוע בעובד (למשל במקרה של הגנת סייבר, להגדיר את העובד כמי שיש בו סכנה לבטיחות הסייבר בארגון אף שידוע כי טכנולוגיות הגנת סייבר אינן אמינות לחלוטין). בשל העובדה שמוסקות מסקנות, עובדים צריכים לתת אמון בהיותו של המידע מדויק ובהיותם של האלגוריתמים שמגיעים להחלטות אמינים. לפיכך דיוק זה עיקרון חשוב בהגנה על פרטיות מידע. כך גם באשר לפיזור המידע. החששות לפגיעה בפרטיות בהקשר של פיזור המידע הם מפני העברת המסקנות לידיים שלישיות שייחשפו אף הן למידע הפרטי.

ההבחנה שבתי הדין עושים בין מידע עסקי, שאליו אמורה להיות למעסיק גישה ללא כל מגבלה, לבין מידע פרטי היא חשובה, אך ראשית ראינו כי היא אינה נעשית בכל המקרים, ושנית הראינו כי היא חלקית בלבד וודאי שהיא אינה מספקת לצורך השאלה אם אירעה פגיעה בפרטיות, מכיוון שכפי שסולוב מראה לנו, גם איסוף מידע פרטי אינו בהכרח תמיד פוגעני, ויש לתת את הדעת לאופנים שבהם כן נפגעת הפרטיות כפי שפורט לעיל. שלישית, יש לבחון את טיב המידע הנאסף בדקדוק רב יותר בשל הטשטוש הקיים בין הפרטי לבין העסקי, למשל אם הקמתו של עסק מתחרה היא דבר עסקי או פרטי. אף שבתי הדין לעבודה מתייחסים למעשה שכזה בחומרה המצדיקה פגיעה בפרטיות, הרי שייתכן שיש מקום לבחינה אחרת של פעילות שכזו – גם לאור הפריזמה של פרטיות. כאמור, הגנה על הזכות לפרטיות נועדה, בין השאר, לאפשר יזמות ופיתוח עסקי. ג'ולי כהן כתבה כי כדי לקדם חדשנות, נדרשת סובייקטיביות דינמית של הפרט. סובייקטיביות שכזו צומחת רק בתוך מרחבים מרווחים השייכים לפרט. אלו המרחבים של פרטיות, שעליהם יש להגן.²¹⁸ אין מחלוקת כי אם הקמתו של עסק חדש כרוכה במידע עסקי קודם השייך למעסיק, עולות שאלות חשובות של סודות מסחריים, ואולם יש לחדד את ההבחנות הללו במסגרת הדיון על פגיעה בפרטיות. דוגמה נוספת היא סיווג התכתבות בין חברים לעבודה הכוללת מידע פרטי ועסקי.

התעכבות על שאלת הפגיעה בפרטיות היא חשובה. היא תאפשר ביתר דיוק לבחון כבר בשלב מקדמי של הדיון המשפטי אם יש צורך לבחון את המבחנים ואת העקרונות בהלכת איסקוב ענבר אם לאו. הטקסונומיה של סולוב וכתובה ענפה נוספת בנוגע לפגיעה בפרטיות של טכנולוגיות חדשות²¹⁹ יכולות לסייע לבתי הדין להגיע להבחנות ברורות יותר בכל הנוגע לפגיעה בפרטיות.

3. נחיצותו של דיון טכנולוגי

היבט חשוב נוסף שעולה בכתובה האקדמית על פרטיות הוא היות הזכות לפרטיות תלויה טכנולוגיה. בירנהק למשל מראה כיצד ההשפעה בין פרטיות לבין טכנולוגיה היא "הדדית ודינאמית",²²⁰ כאשר טכנולוגיות אינן עשויות מקשה אחת, ועל כן יש טכנולוגיות

²¹⁸ Cohen, *What Privacy is For*, לעיל ה"ש 8.

²¹⁹ ראו Solove, *A Taxonomy of Privacy*, לעיל ה"ש 54; Bodie et al., לעיל ה"ש 217. כן ראו את הפירוט של שניהם באלבין ועומר, לעיל ה"ש 105.

²²⁰ בירנהק "שליטה והסכמה", לעיל ה"ש 11, בעמ' 18.

שמאפשרות פרטיות רבה יותר (למשל מצלמות שמוצבות בפתחם של בתים פרטיים) וטכנולוגיות שמובילות לפגיעה בפרטיות.²²¹ טענה נוספת שהועלתה בספרות בדבר היות פרטיות תלויה בטכנולוגיה היא שהגנה על הפרטיות יכולה להיעשות בצורה הטובה ביותר תוך התאמתה לטכנולוגיה מסוימת.²²² כך, רק כאשר נדע כיצד טכנולוגיה עובדת – מה המידע שנאסף ועל פי אילו קריטריונים; כיצד הוא מעובד; מה האופן שבו מגיעים למסקנות; אם, ובאילו נסיבות, המידע מפוזר ולידי מי – יהיה אפשר להגן על הזכות בדרך טובה יותר.²²³ אף הספרות בדבר הזכות לפרטיות מחדדת את מה שצינינו קודם – שיש לבחון את הטכנולוגיה עצמה, בעיקר בכל הנוגע ליישום מבחן המידתיות. מחקר אחר שעשינו – על הגנת הזכות לפרטיות בעידן של הגנת סייבר – הראה כיצד חיוני להבין את איסוף המידע ואת עיבודו ואת הסקת המסקנות בטכנולוגיה של הגנת סייבר.²²⁴ אף שיש סוגים רבים של טכנולוגיית הגנת סייבר, חלק גדול מהן פועל על פי ניתוח תנועה חריגה ברשת (כניסה לאתרים מסוימים, הקלדה בקצב אחר, העברת מידע ממחשב העבודה למחשב אחר וכדומה). טכנולוגיה זו מבוססת על איסוף מטא-דאטה, ניתוח ואנליזה של המידע ברשת והסקת מסקנות. הפרטים הנאספים – למשל באשר לקצב הקלדה – יכולים ללמד על הפרודוקטיביות של העובד, אם הוא חולה (במחלה המאיטה את קצב ההקלדה), אם מישוהו אחד השתמש במקלדת ועוד. אף שהמידע נאסף בכל הנוגע לתנועה ברשת, הרי שקל לשייך אותו לעובד כשיודעים שהוא שעובד על מחשב מסוים. לכן כדי להבין את הפגיעה בפרטיות יש להכיר את הטכנולוגיה. הבנה של מידתיות הפגיעה אף היא מחייבת היכרות עם הטכנולוגיה, שכן ייתכן שהתנהגות מסוימת מוגדרת כחריגה אף שאינה בהכרח כזו, או שהניתוח שנעשה להתנהגות כזו או אחרת בעייתי ועל כן גם אינו מידתי, וכן לצורך בחינת אמצעים פוגעניים פחות.

כפי שצינינו בפרק הקודם, בתי הדין לעבודה כמעט שאינם בוחנים שאלות הנוגעות למידתיות הטכנולוגיה עצמה ואף אינם נעזרים במומחים טכנולוגיים. כן עולה כי בתי הדין התעמקו בטכנולוגיה הנדונה ובחנו כיצד ניתן להתאימה כדי למזער את הפגיעה בפרטיות רק במקרים מועטים, וכאשר ארגוני עובדים היו מעורבים בהליך. ממצא זה חשוב במיוחד. ראשית, הוא משקף את העובדה שבתי הדין אינם מיישמים את הלכת איסקוב ענבר כהלכתה, שכן שם קבע בית הדין הארצי שיש לבחון את מידתיות הטכנולוגיה. שנית, עיקר הפגיעה בזכות לפרטיות קשורה לאופן שבו הטכנולוגיה עובדת ולבחינת השאלה לפי אילו פרמטרים היא אוספת מידע, מעבדת אותו ומסיקה מסקנות, אם הטכנולוגיה מוחקת את המידע הנאסף אחרי זמן מה כשתם הצורך בשימוש בו, אם יש

²²¹ שם.

²²² NISSENBAUM, PRIVACY IN CONTEXT, לעיל ה"ש 6.

²²³ לדיון בעניין זה בהקשר של עבודה, ראו Jeremias Adams-Prassl, *What if Your Boss was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, 41 COMP. LAB. L. & POL'Y J. 1 (2019).

²²⁴ אלבין ועומר, לעיל ה"ש 105.

צמצום של המידע הנאסף ועוד.²²⁵ לפיכך היעדרה של בחינה מעמיקה של הטכנולוגיה במבחן המידתיות לא תאפשר הגנה מיטבית על הזכות לפרטיות. הממצאים שלנו, שמראים שבתי הדין לעבודה כמעט שאינם בוחנים את הטכנולוגיה לעומק, מעידים אפוא שהזכות לפרטיות אינה מוגנת כיום בצורה המיטבית, הן בכל הנוגע לשאלת הפגיעה בפרטיות והן בנוגע למבחן המידתיות. ממצא נוסף שלנו, שהראה כי הטכנולוגיה נבחנה כאשר ארגוני עובדים היו מעורבים בתהליך, מצביע הן על חשיבותם של ארגוני העובדים, והן על כך שלבתי הדין ישנה היכולת לעסוק בשאלות טכנולוגיות. יצוין כי ראוי שיהיה שימוש יותר נרחב במומחים טכנולוגיים במסגרת ההליך המשפטי לבחינת השאלות האמורות.

4. הרתעת המעסיק מפני הפגיעה בזכות לפרטיות

עוד ממצא בעייתי שעולה מהמחקר נוגע להשלכות המעטות שיש לאי-הגנה על כללי הפסיקה בידי המעסיק ופגיעה בזכות לפרטיות. מצאנו כי לרוב (ב-63% מהמקרים) הדיון בזכות לפרטיות נידון בבית הדין לאחר שזו כבר נפגעה ("אקס פוסט"), בשלב שימוש בראיות או בבקשת סעד פיצויים. פנייה לבתי הדין לאחר שהזכות נפגעה משקפת כי במהלך חיי העבודה המעסיק אוסף בקלות את המידע הפרטי על העובדים ושיש לו גישה אליו. ידיעה של עובדים שהם כל הזמן נמצאים תחת עינו הפקוחה של המעסיק, גם בכל הנוגע לענייניהם הפרטיים, היא פגיעה קשה בזכות לפרטיות, כפי שתיארנו לעיל. מלבד זאת, דיון בבית הדין בדיעבד מחמיץ שיקולים של פגיעה עתידית בזכות לפרטיות בעבודה ויצירת הגנה על המרחב הפרטי של עובדים. כמו כן נראה כי במקרים רבים (כ-40% מהמקרים שבדקנו) טענות לפגיעה בפרטיות הובאו בידי עובדים שהועסקו בתפקידים בכירים בחברה. ניתן להניח כי יש מקרים רבים של פגיעה בפרטיות עובדים שלא הובאו לפני בתי הדין, ובהם מאזן הכוח שונה. נוסף על זה, ההשלכות שיש על המעסיק בשל היעדר ההגנה על הפרטיות הן מועטות מאוד. לבית הדין לעבודה אין סמכות לפסוק פיצוי על הפרה של הזכות לפרטיות מכוח החוק; ייתכן שכתלות בכך נקבעים סכומי פיצוי נמוכים לפי בסיסי פיצוי אחרים במקרים שבהם אכן נפסק פיצוי – בגין הפרת חוזה או עוגמת נפש; כמעט שאין מוטלות סנקציות על מעסיק שאינו מגן על חובותיו לפי דיני הגנת הפרטיות. מעסיק שכבר ניטר ואסף חומר – מורשה לעיתים להשתמש בו בצמצום; מעסיק שלא פרסם מדיניות – רק במקרים מועטים קבעו בתי הדין כי אין לתת לו את הסעד המבוקש; מעסיק שאינו בוחן את מידתיות הטכנולוגיה – כנדרש על פי הלכת איסקוב ענבר – אינו זוכה לביקורת שיפוטית. מלבד אלה היו כמה פסקי דין שבהם התייחסו בתי הדין לאי-קיומו של מבחן המידתיות בסלחנות. ואולם, יש חשיבות גדולה בהרתעה משמעותית על ידי בתי הדין מפני פגיעה בזכות זו בשל חשיבותה הרבה, בעיקר בספרת העבודה, כפי שפירטנו לעיל. כתיבה רבה מצויה בספרות של דיני העבודה על חשיבות אכיפתם של דיני העבודה, ורובה עוסקת בתפקיד המחוקק וכן זה של רשויות האכיפה בהגברת האכיפה של דיני העבודה. לידה יש כתיבה

²²⁵ ראו דיון מעמיק שאנו עורכות בשאלות אלה בכל הנוגע לטכנולוגיות להגנת סייבר, שם.

שאף מחדדת את תפקיד בתי הדין לעבודה בהגברת האכיפה.²²⁶ ואכן, כפי שציינו במבוא למאמר, ניתן להגביר את ההגנה על הפרטיות באמצעות אכיפת חובות המעסיקים או באמצעות חקיקה או בבתי הדין לעבודה. נתמקד פה בתפקיד שיכולים למלא בתי הדין בהקשר זה.

ראשית, בתי הדין לעבודה יכולים לפסוק פיצויים גבוהים יותר אגב הסתייעות בפיצויים שנקבעו בחוק הגנת הפרטיות כרף מסייע. עוד אנו סבורות, כפי שציינו לעיל, כי יש לתת סמכות לבתי הדין לעבודה לקבוע פיצויים נזיקיים בגין הפרת הזכות בדומה לסמכות שניתנה לו בהקשרים אחרים. מלבד זאת, רק במספר קטן של פסקי דין נמנעו בתי הדין ממתן סעד למעסיק כאשר הוא לא קבע מדיניות סדורה במקום העבודה. טיעונם היה כי הכללים שנקבעו בהלכת **איסקוב ענבר** הם תנאים מצטברים, וכי בהיעדר מדיניות, ממילא אין מתקיימים התנאים האחרים של הסכמה, מידתיות וצמידות המטרה.²²⁷ הלך חשיבה שכזה הוא ראוי ונכון. מעסיק שאינו פועל להגנת הפרטיות של עובדיו אל לו לקבל סעד מבתי הדין גם כאשר יש מטרה לגיטימית.

נקיטת צעדים שכאלה יאפשרו התמודדות עם ממצא נוסף שעלה מהמחקר והוא הקושי ביישום הדוקטרינה שנקבעה בהלכת **איסקוב ענבר** "אקס פוסט" בפסיקת בתי הדין, לעומת הסדרה "אקס אנטה" שמטרתה הגבלת איסוף מידע ושימוש בו באופן שוטף. כך למשל על פי הלכת **איסקוב ענבר**, המעסיק רשאי להיכנס לתיבת הדואר של העובד במקרים חריגים ובה בעת הוא מחויב בעקרון צמידות המטרה, דהיינו שהשימוש במידע יהיה רק לשם מטרת איסופו (למשל, במקרה של הגנת סייבר – רק לצורך ההגנה על הסייבר). ההלכה קובעת גם מידתיות לפעילות המעסיק. במקרים רבים המעסיקים מגישים בקשה לשימוש במסמכים בהליך לאחר שכבר נחשפו למידע האישי של עובדיהם, כלומר הפגיעה בפרטיות כבר נעשתה. כפי שציינו לעיל, הגנה על פרטיות נועדה לאפשר מרחבים חופשיים לפעולה עצמאית של עובדות ועובדים בעולם העבודה, כדי להגן על זכויותיהם כפרטים וגם לצורך מטרת חברתיות חשובות. ואולם עובדים שיודעים כי המידע אודותיהם נאסף, וכי השאלה המרכזית הופכת להיות אם מידע זה יהיה קביל כראיה בבית הדין לעבודה, נתונים במצב שבו אין להם אותו מרחב חופשי. הם נתונים תמידית בפיקוח, במעקב ובניטור. הממצא של המחקר שלנו אף מחדד את העובדה כי מעסיקים אינם רואים בעיה באיסוף המידע באופן שוטף. דבר זה מגדיל את הפררוגטיבה הניהולית שלהם ומצר את צעדי העובדות והעובדים. ברי הוא כי נקיטת צעדים שיגרמו שהזכות לפרטיות תישמר לאורך חיי העבודה – כמו הטלת פיצויים כספיים גבוהים וכן מניעת מתן סעד במקרה שבו המעסיק פוגע בפרטיות באופן שוטף – חיונית להשגת המטרה האמורה. אלו צעדים שבתו הדין לעבודה אכן יכולים לנקוט, והם אף עולים בקנה אחד עם הלכת **איסקוב ענבר**.

Guy Davidov & Edo Eshet, *Improving Compliance with Labor Laws: The Role of* ²²⁶
Courts, COMP. LAB. L. & POL'Y J. (forthcoming, 2022)

ראו דיון בתת פרק "עיקרון השקיפות ודרישת מדיניות".²²⁷

ה. סיכום

טכנולוגיות חדשות מאפשרות למעסיקים לנהל את העסק שלהם בצורה טובה יותר. לעיתים קרובות יש לטכנולוגיות אלה גם ערך רב לעובדות ולעובדים. עם זאת כפי שאמר ארגון העבודה הבינ-לאומי, יש לוודא כי בעת השימוש בטכנולוגיות חדשות יישמרו תנאי עבודה נאותים.²²⁸ לפיכך הגנה על זכויות עבודה ואדם בסיסיות חיונית בעידן זה, בין השאר בכל הנוגע לזכות לפרטיות. גם אם השינויים הטכנולוגיים מציבים אתגרים לא פשוטים להגנה על הפרטיות, כפי שבוודאי עולה מהניתוח שנעשה במאמר זה, הרי שאין בכך כדי להוריד מקרנה של הזכות לפרטיות, הן בשמירה על כבודו של הפרט והאוטונומיה שלו והן בשמירה על אינטרסים חברתיים וכלכליים רחבים יותר. ייתכן שאף להפך.

במאמר זה ביקשנו לבחון מהי מידת ההגנה שמעניקים בתי הדין לעבודה מפני פגיעה בזכות לפרטיות העובדים ומהן ההשלכות העומדות בפני המעסיק שפגע בזכות העובדים לפרטיות. בחנו זאת בדיון בהלכה המרכזית שמנחה את בתי הדין לעבודה בתחום זה – **איסקוב ענבר** – ויישומה בבתי הדין לעבודה בתקופה של כעשור מאז התקבל פסק הדין בשנת 2011. מהמחקר עלה כי אף שהמבחנים והעקרונות שהותוו בהלכת **איסקוב ענבר** הם ככלל ראויים, הרי שיש מצבים רבים שבהם יישום הלכת **איסקוב ענבר** ופיתוחה בבתי הדין לוקים בחסר. הצגנו מקרים שבהם העקרונות והמבחנים המשפטיים לא יושמו במלואם, והראינו את החסרים הקיימים בדיון על עקרונות המידתיות, הלגיטימיות וצמידות המטרה. בנוסף אף הבענו את הקושי שיש לנו בדגש שהושם בשאלת ההסכמה.²²⁹ הצענו במאמר כמה דרכים להתמודדות עם הבעיות האמורות, ואנו מקוות כי אלה יאומצו בעתיד בבתי הדין בבואם לבחון את שאלת ההגנה על הפרטיות וכן בחקיקה. נבקש לסכם באמירה הזאת: אחת המטרות החשובות ביותר של בתי הדין לעבודה בעידן של טכנולוגיות חדשות היא הגנה על הזכות לפרטיות. לפיכך יש חשיבות אמיתית ביישום ראוי של העקרונות והמבחנים שנקבעו בפסיקה, ולמתן משקל קטן למבחן ההסכמה אגב הגדלת ההגנה הקוגנטית על פרטיות. אך נוסף על זה, יש לוודא כי יש אכיפה ראויה של הזכות לפרטיות לאורך כל חיי העבודה, ולכן ישנה חשיבות להשלכות משמעותיות ניכרות על מעסיקים שפוגעים בזכות האמורה. בהיעדר השלכות שכאלה אין למעסיקים תמריץ ליישם את התנאים שנקבעו בהלכת **איסקוב ענבר**, ובייחוד בחינה של לגיטימיות התכלית שלשמה נאסף המידע, יישום עקרון צמידות המטרה, בחינת מידתיות הטכנולוגיה וכן קביעת מדיניות בכל הנוגע לשימוש בטכנולוגיות בסביבת העבודה והבאת המדיניות הנוהגת והנסיבות שבהן מתקיים ניטור ומעקב לידיעת העובדים. לפיכך ליד ההמלצות שהעלינו במסגרת מאמר זה ליישום נאות של העקרונות ושל המבחנים בפסיקה, הצענו להרחיב את האכיפה של הזכות לפרטיות וכן את ההרתעה מפני פגיעה

Int'l Lab. Org. (ILO), *Global Commission on the Future of Work: Work for a Brighter Future* (2019), <https://bit.ly/3zmCcho> ²²⁸

במקום אחר אנו טוענות כי יש מקום להשלים את המבחנים והעקרונות שנקבעו בפרשת **איסקוב ענבר** במבחנים נוספים שטרם אומצו בדיון הישראלי, ראו אלבין ועומר, לעיל ה"ש 105. ²²⁹

של המעסיק בפרטיות באופן שוטף, בין היתר באמצעות הטלת פיצויים כספיים גבוהים ומניעת מתן סעד בהיעדר מדיניות במקום העבודה או בפגיעה בפרטיות באופן שוטף. רק כך יהיה אפשר לייצר את אותו מרחב פעולה פרטי שהוא כה חיוני – לפרט ולחברה כולה – בעולם העבודה של ימינו.

נספח - תוצאות יישום הלכת איסקוב ענבר

א. פסקי הדין וההחלטות שבהם קיבלו בתי הדין את הטענה בגין פגיעה בפרטיות ופסקו בגין זה סעד:

1	עס"ק (ארצי) 7541-04-14 הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי – עיריית קלנסווה (נבו 15.3.2017)
2	פ"ה (אזורי חי') 1274-04-17 מרעי – המועצה המקומית פרדיס (נבו 2.4.2018)
3	סע"ש (אזורי ת"א) 20739-08-16 חננאל – מועצה מקומית באר יעקב (נבו 16.11.2020)
4	סע"ש (אזורי ת"א) 69292-03-18 מאפי – פארמה בע"מ – טומוב (נבו 9.12.2019)
5	סע"ש (אזורי ת"א) 14245-02-17 אנחין – אליאסי (נבו 22.7.2017)
6	סע"ש (אזורי חי') 6017-09-16 זוחוביצקי – המחדש תעשיות (מנת"ש) בע"מ (נבו 25.12.2018)
7	סע"ש (אזורי נצ') 2684-03-16 קוריטני – צדוק (נבו 9.3.2017)
8	סע"ש (אזורי ת"א) 30032-12-17 בובר – בובר (נבו 29.1.2019)
9	סע"ש (אזורי ת"א) 28766-11-12 בוטביניק – אינטלימיננד בע"מ (נבו 20.12.2015)
10	סע"ש (אזורי ת"א) 11641-03-15 אלבה פתרוןות טכנולוגיים מתקדמים בע"מ – שמעון אלמלם (נבו 28.6.2015)
11	סע"ש (אזורי ת"א) 18515-02-18 סעדה – בלוקשתיל בע"מ (נבו 13.5.2020)
12	סעש (נצ') 60673-12-19 נסאר – המכללה הארצית להכשרה מקצועית סכנין בע"מ (נבו 23.8.2020)

13	סע"ש (אזורי ת"א) 28119-07-17 אליאס – מאצ' ריטייל בע"מ (נבו 26.8.2018)
14	סע"ש (אזורי ת"א) 1575-09-15 גבע – מזרחי (נבו 29.9.2016)
15	סע"ש (אזורי ת"א) 29090-05-12 גורליק – אנבינדר (נבו 21.4.2014)
16	סע"ש (ת"א) 60161-06-16 בלקאר – בלקין (נבו 27.8.2019)
17	פ"ה (אזורי ב"ש) 40066-04-16 כרמל בידוד בע"מ – סולימנוב (נבו 13.8.2017)
18	סע"ש (אזורי ת"א) 38650-09-17 אי.איי.סי – מרכז הפרסום הישראלי בע"מ – גולן (נבו 4.12.2018)
19	סע"ש (אזורי ת"א) 26316-09-15 סוריא – בן ארי (נבו 23.4.2017) + סע"ש (אזורי ת"א) 26316-09-15 סוריא – בן ארי (נבו 3.11.2016)
20	סע"ש (אזורי ת"א) 11371-09-11 שיאולוגי בע"מ – בירנבוים (נבו, 4.11.2015)

ב. פסקי הדין וההחלטות שבהם קיבלו בתי הדין את הטענה בגין פגיעה בפרטיות חלקית בלבד:

1	ע"ע (ארצי) 40711-04-17 פישר תעשיות פרמצבטיות בערבון מוגבל – שטטר (נבו 4.3.2018)
2	סע"ש (אזורי ת"א) 969-08-15 ש.ז. – ל.א. בע"מ (נבו 18.4.2017)
3	ס"ק (אזורי ת"א) 2994-06-19 הסתדרות העובדים הכללית הסתדרות עובדי המדינה – מדינת ישראל (נבו 8.10.2020)
4	סע"ש (אזורי ת"א) 18279-06-16 אקספו ניהול בע"מ – כהן (נבו 26.3.2017)
5	סע"ש (אזורי ת"א) 71727-10-18 גרטי – לב הדקל – סוכנות לביטוח (2004) בע"מ (נבו 12.4.2020)

6	סע"ש (אזורי ת"א) 14400-03-13 ברמן – אקספיריורס בע"מ (נבו 30.3.2017)
7	פ"ה (אזורי חי') 15794-10-17 אקספוז אופנה בע"מ – הברפלד (נבו 4.2.2018)
8	סע"ש (אזורי ת"א) 24960-02-19 א.מ רכיבים (2005) בע"מ – מולדובן (נבו 6.10.2020)
9	סע"ש (אזורי ת"א) 22614-09-19 ש. אנגל מהנדסים בע"מ – בונגרט (נבו 27.4.2020)
10	סע"ש (אזורי ת"א) 79357-01-19 חי – ויצו – הסתדרות עולמית לנשים ציוניות (ע"ר) (פורסם נבו 11.6.2020)
11	סע"ש (אזורי ת"א) 17625-03-16 לויץ – אבידן (נבו 8.1.2018)

ג. פסקי הדין וההחלטות שבהם דחו בתי הדין את הטענה בגין פגיעה בפרטיות:

1	ס"ע (אזורי י-ם) 50814-01-12 מרדכי אברמסון – מלם מערכות בע"מ (נבו 11.9.2014)
2	ד"מ (אזורי ת"א) 15161-08-12 בן עזרא – חברת "דן" תחבורה ציבורית בע"מ (נבו 28.9.2013)
3	תע"א (אזורי ת"א) 9331-09-09 סלם – עיצובים גרפיקה ותקשורת שיווקית בע"מ (נבו 5.2.2013)
4	סע"ש (אזורי ת"א) 41363-03-13 יוסקוביץ – טלרד נטוורקס בע"מ (נבו 15.10.2017)
5	סע"ש (אזורי ת"א) 24704-11-16 זיפקום תקשורת בע"מ – חסקלוביץ' (נבו 20.8.2019)
6	סע"ש (אזורי ת"א) 12303-09-18 רובוגרופ ט.א.ק. בע"מ – באום (פורסם בנבו, 24.03.2020)
7	סע"ש (אזורי ת"א) 21426-11-16 מנשה – אודיס מפעלי סינון בע"מ (נבו 16.1.2019)

8	סע"ש (אזורי ת"א) 25953-12-14 ד"ר שלמה כהן ושות' – משרדי עורכי דין – מנגלוס (נבו 18.1.2015)
9	סע"ש (אזורי ת"א) 45564-12-17 כהן – אל על נתיבי אויר לישראל בע"מ (נבו 9.3.2018)
10	על"ח (אזורי ת"א) 1116-02-12 דלל גפנר – פריגו ישראל סוכנויות בע"מ (נבו 18.8.2013)

ד. אחר:

1	סע"ש (אזורי ת"א) 31869-03-19 הילטון ליכט – ג'ונס לאנג לאסאל ישראל בע"מ (נבו 14.7.2020)
2	ס"ע (אזורי ב"ש) 14692-02-10 שביט דמרי – ג'ין (נבו 4.8.2011)
3	תע"א (אזורי נצ') 1027/06 אפיקי מים – אגודה חקלאית שיתופית לאספקת מים בבקעת בית שאן בע"מ – פישר (נבו 26.6.2011)
4	סע"ש (אזורי ת"א) 31749-02-18 קלאסיק הוטל מנג'מנט בע"מ – נטלי ניקיטינה (נבו 11.9.2018)
5	סע"ש 25861-02-16 ת"פ (עבודה חיפה) איסתא ישראל בע"מ – רוזנברג (נבו 21.3.2016)
6	סע"ש (אזורי ת"א) 4394-05-14 בלוך – סינאל מלל פייוויי בע"מ (פורסם בנבו, 2.12.2014)
7	ע"ב (אזורי חי') 10596-11-08 סטאטוס סקול בע"מ – תיב"מ פלוס בע"מ (נבו 21.3.2012)
8	תע"א (אזורי ת"א) 22105-11-11 ג'ובני – שיא סיורים (1986) בע"מ (בפירוק) (נבו 20.3.2013)
9	סע"ש (אזורי חי') 32450-03-14 לפידות מדיקל יבוא ושיווק בע"מ – גרא (נבו 30.5.2018)
10	פ"ה (אזורי ת"א) 50861-03-20 מעברות ים המלח בע"מ – רימה גרידנב (פורסם בנבו, 21.11.2020)

