א.נשים מנהלים א.נשים
באמצעות מכונות

המכון הישראלי
לדמוקרטיה

עובדים מרחוק

הזכות לפרטיות העובדים ושמירה עליה באמצעות דוקטרינת ההפרה התורמת

מחקר מדיניות 202

רחל אריזור הרשקוביץ

המכון הישראלי
לדמוקרטיה

מחקר מדיניות 202

עובדים מרחוק

הזכות לפרטיות העובדים ושמירה עליה באמצעות דוקטרינת ההפרה התורמת

רחל אריזור הרשקוביץ

יולי 2025

Remote Workers: Protecting Workers' Right to Privacy through the Doctrine of Contributory Infringement

Rachel Aridor-Hershkovitz

עריכת הטקסט: גלית שמאע
עיצוב הסדרה: סטודיו Alfabees
עיצוב העטיפה: mootagoc.com
ביצוע גרפי: רונית גלעד, ירושלים
הדפסה: גרפוס פרינט, ירושלים

מסת"ב: 978-965-519-484-5

נדפס בישראל, תשפ"ה/2025

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים:
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

המחקר רואה אור במימון קרן תובענות ייצוגיות במסגרת קול קורא 88/2024 למחקרים בתחום הפרטיות.

תוכן העניינים

תקציר

מגפת הקורונה הביאה להיווצרותו של דפוס עבודה חדש: עבודה משולבת (היברידית), ובמסגרתה מחלק העובד את ימי עבודתו בין המשרד הביתי לבין מרחב העבודה של המעסיק. מעסיקים נאלצו לפתע להתמודד עם הצורך לשמור על יעילות הארגון בהיעדר יכולת לפקח פיזית על העובד, ובעקבות זאת החלו טכנולוגיות למעקב אחר עובדים לפרוח לא רק בקרב עובדי הצווארון הכחול, שם היו נהוגות גם בעבר ברמות חודרנות שונות, אלא גם בקרב עובדי הצווארון הלבן. שגשוגן של טכנולוגיות למעקב אחר עובדים הוביל להתמקדות הולכת וגוברת ב"נראות העובד", שמשמעותה המעשית היא חשיפת העובד, תפוקותיו, מחשבותיו וסביבתו למעסיק מתוך טשטוש גובר והולך בין המרחב העסקי, המרחב הפרטי והמרחב הציבורי.

עם זאת, הצגתן של טכנולוגיות למעקב אחר עובדים באופן חד־ממדי שכזה חוטאת לאמת, שכן לחלקן מטרות לגיטימיות, ובראשן החתירה לשיפור שוק העבודה בעידן ההיברדי. מדובר, אם כן, בטכנולוגיות דו־שימושיות שיכולות לשמש להגשמת אינטרסים ציבוריים וארגוניים לגיטימיים וחשובים לצד התרת פגיעה חמורה בזכות העובד לפרטיות.

מחקר זה מתמקד בסוגיית הפגיעה בזכות העובד לפרטיות עקב שימוש בטכנולוגיות מעקב מתוך הכרה בדו־שימושיותן. המחקר סוקר חלק מן הטכנולוגיות למעקב אחר עובדים הקיימות כעת בשוק ומציג את אפשרויות הפגיעה בפרטיות שהן מאפשרות. בהמשך, נבחנים היקפה של זכות העובד לפרטיות בארצות הברית, באיחוד האירופי ובישראל והסעדים הקיימים לעובד שפרטיותו נפגעה בעקבות השימוש בטכנולוגיות מעקב.

על בסיס סקירה זו מציע המחקר לאמץ גישה שונה לבחינת הפגיעה בפרטיות העובד, שאינה מניחה, כנקודת מוצא, שהעובד נמצא במרחב השייך למעסיק, אלא מביאה בחשבון את מידת החודרנות שמאפשרות טכנולוגיות המעקב הן מבחינת היקפי המידע האישי שהן חושפות לעיני המעסיק והן מבחינת המרחבים החדשים שאליהן הן מעניקות למעסיק גישה. כך, למשל, טכנולוגיית מעקב יכולה להיות מותקנת במרחב פיזי של המעסיק, לדוגמה על המחשב הנייד שהוא מספק לעובד, ולאפשר איסוף מידע אישי ממרחבים דיגיטליים ואף פיזיים אישיים של העובד. לפיכך, בבחינת הפגיעה בזכות העובד לפרטיות יש לתת את הדעת למרחב הפיזי שנמצא בו העובד בעת הפגיעה בפרטיות, המרחב שמותקנת בו טכנולוגיית המעקב והמרחב הדיגיטלי או הפיזי שנאסף ממנו המידע האישי, רגישות המידע האישי המעובד, היקפו ותדירות איסופו. מדובר במנעד: ככל שהמרחב הפיזי שנמצא בו העובד, כלומר המרחב שמותקנת בו טכנולוגיית המעקב, המרחב, שנאסף ממנו המידע האישי פרטיים יותר, וככל שהמידע הנאסף רב יותר ורגיש יותר, כך הפגיעה בזכות העובד לפרטיות צריכה להיחשב חודרנית יותר ומידתית פחות. מתן משקל למנעד זה במסגרת בחינת חוקיות הפגיעה בזכות העובד לפרטיות יבטיח שהכלל המשפטי לא יהיה מוגבל לנסיבות מסוימות או לטכנולוגיה מסוימת.

לצד בחינת הפגיעה בזכות העובד לפרטיות, המחקר בוחן את האפשרות להטיל אחריות ולדרוש סעד לא רק מן המעסיקים המשתמשים בטכנולוגיות למעקב אחר עובדיהם, אלא גם ממפתחי אותן טכנולוגיות, באמצעות אימוצה של דוקטרינת ההפרה התורמת המוכרת מדיני זכויות היוצרים לדיני הגנת הפרטיות. אימוץ הדוקטרינה ישמש כלי נוסף בארגז הכלים העומד לרשותו של העובד לשם הגנה על זכותו לפרטיות. אומנם אימוץ כזה עלול להוביל לכשל אכיפה הנוגע לסמכות השיפוט והדין החל ולפגיעה באינטרסים נוספים לנוכח רוחבה של הזכות לפרטיות, אך הוא יביא לחיזוק נחוץ לזכות של הפרטיות הנתונה זה

שנים מספר במגננה מול התפתחויות טכנולוגיות חדשניות המתייחסות למידע אישי כאל נכס סחיר.

מהלך כזה עשוי להשיב את המשקל הראוי לערכים שבבסיס הזכות לפרטיות הנגזרת מן הזכות לכבוד ובעלת חשיבות לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו ללא התערבות זרה. יש אינטרס ציבורי חשוב באימוץ דוקטרינת ההפרה התורמת, שכן היא עשויה לתמרץ את החברות המפתחות לפעול למזעור הפגיעה האפשרית בזכות לפרטיות ולהגברת הפיקוח על השימושים הנעשים בה, למשל על ידי צמצום חלק מן התכונות האפשריות של טכנולוגיית המעקב. כך למשל יצומצמו סוגי המידע האישי שהיא אוספת ומעבדת, יצומצם מגוון התובנות שהיא יכולה להפיק על ידי שימוש בבינה מלאכותית או יוגבלו השימושים האפשריים בתובנות אלו במסגרת ניהול משאבי האנוש בארגון, (החל בהחלטות בדבר גיוס מועמדים לעבודה, ניוד עובדים, קידומם וכלה בפיטורים).

מבוא

במרץ 2020, בעודנו מסתגרים בבתים חמושים במסכות ובתכשירי חיטוי, עוקבים בדאגה אחר מדד החולים היומי ואחר מספר המתים ההולך ועולה בעקבות מגפת הקורונה העולמית, המשיך שוק העבודה לתפקד ללא הפרעות ניכרות. לצד הדאגה לבריאותנו ולבריאות קרובי משפחתנו וההסתגלות למציאות שנדמתה כשאובה מסרטי מדע בדיוני, החל במרדף אחר מסיכות ונייר טואלט וכלה במרדף אחר ביצים ערב חג הפסח, העתיק חלק ניכר מן הציבור את חייו למרשתת (רשת האינטרנט) ונדרש להמשיך לעבוד כרגיל. עבור חלק גדול מן העובדים ממשיך מתווה העבודה מרחוק בחלק מימי השבוע גם לאחר מגפת הקורנה. דפוס עבודה זה זכה לכינוי "עבודה היברידית".

המעבר לשגרת עבודה מרחוק מלווה בחשיפה גוברת של העובד – על תפוקותיו, מחשבותיו וסביבתו – לעיני המעסיק באמצעות טכנולוגיות מעקב. מעסיקים, שלפתע נשמטה מידיהם האפשרות לעקוב אחר התנהלות העובד במקום העבודה, תרו אחר דרכים להבטיח את יעילותו גם בעת העבודה מרחוק בביתו, ותעשיית טכנולוגיות המעקב אחר עובדים הפכה למשגשגת. כך החלו להופיע מגוון טכנולוגיות שהופעלו לעיתים בהיחבא וללא מודעות העובד: לדוגמה, טכנולוגיות שעקבו אחר התקשורת של העובדים בינם לבין עצמם ובינם לבין המעסיק בערוצי התקשורת הדיגיטליים השונים, וניתחו מידע זה במטרה לעמוד על בריאותו הנפשית של כל עובד;[1] טכנולוגיות שעקבו אחר הקלקות העכבר והקשות המקלדת של העובד או צילמו באופן עיתי את מסך המחשב של העובד; מעסיקים שחייבו עובדים להשאיר את מצלמת המחשב פתוחה ופועלת במשך כל שעות העבודה; טכנולוגיות שעקבו אחר תנועות העין של העובד כדי לאמוד את רמת תשומת הלב שלו לעבודה; טכנולוגיות שעקבו אחר היסטוריית הגלישה של העובד ופעילותו ברשתות חברתיות כדי להעריך את רמת יעילותו בעבודה ולבחון אם בכוונתו לעזוב את מקום העבודה. יש אף טכנולוגיות העוקבות אחר טון הדיבור של העובד במטרה להעריך את רמת מעורבותו בשיח העבודה. אלו התווספו על מגוון טכנולוגיות מעקב שהיו בשימוש עוד קודם מגפת הקורונה, כגון: כלים המתבססים על בינה מלאכותית שהקליטו ועיבדו את שיחות הטלפון שניהלו נציגי שירות לקוחות; טכנולוגיות לְבִישׁות שעקבו אחר תנועותיו וקצב פעימות הלב של עובד מחסן או עובד ברשת מזון מהיר והעריכו את מידת יעילותו; וכן מערכות איכון גלובליות (Global Positioning System – GPS),

1 Mark Pesce, *Every Move You Make*, Cosmos (Oct. 7, 2022)

המשלבות מצלמות ובינה מלאכותית במטרה לעקוב אחר מיקומם ותפקודם של שליחים.[2] הביקוש לטכנולוגיות למעקב אחר עובדים עלה במידה ניכרת בתקופת מגפת הקורונה, וקצב אימוצן של טכנולוגיות אלו המשיך להיות גבוה גם עם סיום המגפה ואימוץ מתווה עבודה היברידי במקומות עבודה רבים, בעיקר בקרב עובדי הצווארון הלבן שהיו רגילים עד אז למרחב פעולה יותר בהשוואה לעמיתיהם ממעמד הצווארון הכחול, שהיו נתונים גם קודם לכן למעקב קפדני יותר אחר שעות העבודה שלהם ותפוקותיהם.

טכנולוגיות למעקב אחר עובדים הן דו־שימושיות, כלומר יכולים להיות להן שימושים חוקיים בצד שימושים לא חוקיים. דוגמאות לשימושים חוקיים הן טכנולוגיות למעקב אחר עובדים אשר עוזרות לעובדים לגלות ערנות להרגלי העבודה שלהם ולנצל טוב יותר את זמן העבודה שלהם, מקנות למעסיק כלים למעקב ולהערכת תפוקות העובד ויעילותו לשם שימור מתווה העבודה ההיברידי,[3] מאפשרות חישוב שעות עבודה ושכר ביעילות ובאופן חוצה גבולות, למשל עבור מעסיק בינלאומי, מקילות על גביית תשלום מלקוחות או מספקות הגנת סייבר. אולם, לצד השימושים החוקיים, יכולים כאמור להתבצע בטכנולוגיות מעקב גם שימושים פוגעניים ובלתי חוקיים. טכנולוגיות המעקב עלולות לפגוע קשות בזכות העובדים לפרטיות, בראש ובראשונה בעובדים מוחלשים, בעיקר נותני שירותים עצמאיים המועסקים בחברות פלטפורמה (platform based gig workers), כגון נהגים בחברת אובר או שליחי וולט. הפגיעה בפרטיות מעמיקה את פערי המידע בין המעסיק לבין עובדיו, ומעניקה למעסיק יכולות שליטה מרחיקות לכת על העובדים, ובכלל זאת מחלישה את יכולתם לשפר את תנאי העסקתם או להתאגד לפעולה משותפת למול המעסיק.[4]

2 Kathryn Zickuhr, *Workplace Surveillance is Becoming the New Normal for U.S. Workers*, 4 (Washington Center for Equitable Growth, Aug. 2021)

3 זאת על רקע המגמה המסתמנת של הפסקת מתווה העבודה ההיברידי בנימוק לירידה בתפוקות הארגון. ראו למשל, Russ Kennedy, *Stop Blaming your Problems on Hybrid Work. Outdated Tech is the Real Issue*, FastCompany (Nov. 14, 2024); Lauren Hirsch, *Executive and Research Disagree about Hybrid Work. Why?* The Seattle Times (Oct. 14, 2024)

4 שם.

התמודדות עם השימושים הבלתי חוקיים המבוצעים בטכנולוגיות מעקב במטרה למנוע או למזער את הפגיעה בפרטיות היא אתגר משמעותי העומד בפני החברה ותחום המשפט בישראל ובעולם. דיני הגנת הפרטיות בארץ ובעולם נשענים, רובם ככולם, על עקרונות ניהול מידע הוגן (Fair Information Practices — FIPs) שגובשו בסוף שנות ה־70 ובראשית שנות ה־80 של המאה הקודמת, אגב שילוב מועט בלבד של רעיונות חדשים, כגון עיצוב לפרטיות (Privacy by Design), על אף הפיכתו של מידע אישי לנכס סחיר בעל ערך רב ולבסיס כלכלת המידע בשנים האחרונות.[5] נוסף על כך, וליתר דיוק בעקבות עליית קרנו של מידע אישי כנכס סחיר בעל ערך רב, נשחק ונחלש מעמדה של הזכות לפרטיות בשנים האחרונות. לפיכך, הכלים העומדים לרשותו של נפגע בודד מצומצמים ואינם יעילים.

מדובר, אם כן, בשדה לא חרוש ויש צורך בפיתוחם של כללים משפטיים לשימוש הוגן ומידתי בטכנולוגיות מעקב בכלל, ובמסגרת יחסי העבודה בפרט, ובכך עוסק מחקר זה.[6] לצד בחינת המתווה המתאים לבחינת פגיעה בזכות העובד לפרטיות עקב שימוש בטכנולוגיות מעקב, מחקר זה מבקש לבחון שימוש בכלי הלקוח מתחום המשפט האזרחי – דוקטרינת ההפרה התורמת (contributory liability) – לצורך התמודדות עם הפגיעה בפרטיות הנגרמת בעקבות שימוש לרעה בטכנולוגיות מעקב. מדובר בדוקטרינה שמקורה בדיני הנזיקין, אך היא פותחה בבתי המשפט ככלי להטלת אחריות על יצרנים ועל מפתחי מוצרים וטכנולוגיות בגין הפרת זכויות יוצרים שמבצעים המשתמשים. בדרך זו מבקש המחקר להצביע על כלי שבאמצעותו יוכלו החברה ותחום המשפט לסמן את קו הגבול שבין שימוש חוקי לבין שימוש בלתי חוקי או רצוי מן הבחינה החברתית

5 Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 Yale J. L & Tech. 256, 260–261 (2020)

6 כך למשל, העיר בית המשפט העליון במסגרת פסק דין אשר בחן את חוקיות השימוש בתיעוד ממצלמות הכניסה לחנייה לשם הערכת יעילותה של עובדת. באותה פרשה הפנה בית המשפט העליון את הזרקור לבית הדין הארצי לעבודה כמי שמחזיק את המומחיות המתאימה לקביעת ההלכה בנושא השימוש בטכנולוגיות מעקב במסגרת יחסי עבודה. ראו אפרת נוימן "עובדת אל על נתפסה במצלמות ופוטרה: גם בג"ץ לא עזר לה" **דה מרקר** (20.9.2023).

בטכנולוגיה למעקב אחר עובדים. סימון קו ברור והגדרת הדרכים לאכיפתו המשפטית יכולים לשמש מצפן עבור מפתחי טכנולוגיות חדשניות.

בבסיס אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות ניצבת השאלה אם יצרן טכנולוגיה דו־שימושית אחראי לשימוש בלתי חוקי, שעושה משתמש הקצה, ומוביל לפגיעה לא חוקית בזכותו של אדם לפרטיות? סוגיית אחריותו של גורם ביניים להפרת זכות הנעשית על ידי צד שלישי המשתמש בטכנולוגיה פרי פיתוחו – אינה חדשה. בית המשפט בארצות הברית עסק בשאלת אחריותו של יצרן טכנולוגיה דו־שימושית לשימוש לא חוקי הגורם לפגיעה בזכויות יוצרים הנעשה בטכנולוגיה שלו כבר לפני 40 שנים בפסק הדין הנודע בפרשת **סוני**.[7] עם זאת, הדיון לא עסק בטכנולוגיית מעקב המאפשרת פגיעה בזכות היסוד לפרטיות. מחקר זה מבקש לבחון האם – ואם כן, באילו תנאים – ניתן לאמץ את דוקטרינת ההפרה התורמת לתוך עולם טכנולוגיות המעקב והזכות לפרטיות, ומהם שיקולי המדיניות הרלוונטיים לאימוץ כזה?

בפרק הראשון של המחקר אבחן את הזכות לפרטיות ואעמוד על הצדקותיה התאורטיות, על הערכים שבבסיסה ועל חשיבותה. בהמשך אדון בהיקפה של זכות העובד לפרטיות למול הפררוגטיבה הניהולית של העובד ואבחן כיצד טכנולוגיות מעקב אחר עובדים משפיעות על האיזון ביניהן. אסקור את היקפה של זכות העובד לפרטיות וההגנה הניתנה לה בארצות הברית, באיחוד האירופי ובישראל. **בפרק השני** אציג את דוקטרינת ההפרה התורמת ואת שלבי התפתחותה בדיני זכויות היוצרים בארצות הברית, באיחוד האירופי ובישראל. **בפרק השלישי** אעסוק בהרחבה בשיקולי המדיניות בעד ונגד אימוצה של דוקטרינת ההפרה התורמת שתוביל ליצירתה של עוולה חדשה בדיני הגנת הפרטיות מתוך הרחבת מעגל האחראים לפגיעה בזכות העובד לפרטיות. דיון זה בבסיס העיוני להצדקת אימוצה של דוקטרינת ההפרה התורמת חיוני כשלב ראשוני ומקדמי לפני החלטה בדבר קליטתה של הדוקטרינה בדיני הגנת הפרטיות. **בפרק הרביעי** אבחן את תנאיה של דוקטרינת ההפרה התורמת ויישומם בנסיבות של טכנולוגיות מעקב אחר עובדים. בין השאר יעסוק פרק

7 *Sony Corp. Of America v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984) (להלן: פרשת **סוני**).

זה בהשלכותיו האפשריות של השימוש בטכנולוגיות מעקב לצורך מעקב מקיף וממושך המתנהל בו זמנית בכמה מרחבים, ואגב טשטוש הגבולות בין המרחב הפיזי הפרטי של העובד לבין מרחב העבודה במציאות של עבודה מרחוק, על בחינת הפגיעה בפרטיות העובד. **הפרק החמישי** ייוחד לסיכום ולמסקנות.

אני מודה להוצאה לאור של המכון הישראלי לדמוקרטיה, לתמר שקד ולעורכת הלשון גלית שמאע על עבודתן המסורה בהבאת מחקר זה לאור. תודה לד"ר תהילה שוורץ אלטשולר, לד"ר דנה בלאנדר ולפרופ' סוזי נבות על הערותיהן החשובות, ולעו"ד איה מרקביץ שהאירה את עיניי כתמיד והצביעה על הצורך במחקר זה.

פרק 1
מבוא לזכות היסוד לפרטיות, יישומה וגבולותיה במסגרת יחסי עבודה

1.1. המשגת הזכות לפרטיות

במהלך השנים הוצגו מגוון גישות תאורטיות להבנת חשיבותה ולהגדרת הזכות לפרטיות והערכים שבבסיסה.[8] הראשונים לעשות זאת היו עורכי הדין האמריקנים, לואיס ברנדס, שלימים מונה לשופט בבית המשפט העליון בארצות הברית, וחברו סמואל וורן, שהגדירו, בשנת 1890, את הזכות לפרטיות כזכות להיעזב במנוחה (the right to be left alone).[9] בהמשך, התפתחה התאוריה העיקרית להמשגת הזכות לפרטיות כשליטתו האקטיבית של אדם (המכונה בעגה המשפטית "נושא המידע"), בזרימת המידע על אודותיו בכל שלב בשרשרת הפעולות הקשורות באיסוף המידע ובעיבודו. תאוריה זו נשענת על ראיית הזכות לפרטיות כמבוססת על עקרון העל של כבוד האדם.[10]

תפיסת הפרטיות כגישה היא תאוריה נוספת להבנת הזכות לפרטיות. לפי תאוריה זו הזכות לפרטיות היא זכות עצמאית המבוססת על יכולתו של אדם למנוע גישה של אחרים אליו בשלושה מישורים: (א) סודיות: הגבלת הנגישות של אחרים למידע אישי על אודות נושא המידע; (ב) נגישותם הפיזית של אחרים לנושא המידע; (ג) אנונימיות: המידה שבה נושא המידע הוא מושא לתשומת

8 להרחבה ראו רחל ארידור הרשקוביץ **פגיעה בפרטיות באמצעות נוזקות מעקב: אחריות תורמת של היצרן** (מחקר מדיניות 197, **המכון הישראלי לדמוקרטיה** 2024), עמ' 51–62.

9 Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 Ariz. L. Rev. 1 (1979)

10 Alan F Westin, Privacy And Freedom (1967); מיכאל בירנהק **[מרחב פרטי]: הזכות לפרטיות בין משפט לטכנולוגיה** (תשע"א), עמ' 89–99.

ליבם של אחרים.[11] גישה תאורטית נוספת מציעה להגדיר את הזכות לפרטיות בהתבסס על זיהוי מצבים הנחשבים פגיעה בפרטיות ועל סיווגם לקטגוריות. מקובל להכיר בארבע קטגוריות של פרטיות, בהתאם לסוג הפעילות שמדובר בה: (א) פרטיות במקומות (בבחינת "ביתו של אדם – מבצרו"); (ב) פרטיות בתקשורת; (ג) פרטיות במידע; (ד) פרטיות בקבלת החלטות. חוק הגנת הפרטיות, התשמ"א–1981 (להלן: חוק הגנת הפרטיות) מאמץ חלקית את גישת הקטגוריות בהגדירו מקרים של פגיעה בפרטיות, אם כי אלו אינם חופפים לארבע הקטגוריות המקובלות.[12]

דניאל סולוב הציע בשנת 2008 להגדיר את הזכות לפרטיות בהתאם למענה המשפטי למצבים שבהם נפגעת הפרטיות. הצעתו התבססה על ההבנה שאי־אפשר להעניק לזכות לפרטיות הגדרה אחת אחידה שתספק מענה מתאים לכל פגיעה אפשרית בזכות. ניתן למצוא חפיפה מסוימת בין הצעתו של סולוב לבין תאוריות הקטגוריות של פרטיות.[13] סולוב מונה ארבע קבוצות של בעיות שעימן הזכות לפרטיות מבקשת להתמודד. כל אחת מן הקבוצות הללו כוללות כמה מצבי פגיעה: (א) איסוף מידע: מעקב וחקירה; (ב) עיבוד מידע: צבירת מידע, זיהוי על בסיס מידע, אבטחת מידע, היעדר שקיפות כלפי נושא המידע ושימושים נוספים במידע; (ג) הפצת מידע: הפרת אמון, גילוי מידע, חשיפת מידע, הגברת תפוצה של מידע, סחיטת מידע, גניבת זהות ועיוות מידע; (ד) חדירה לחייו האישיים של אדם: מצבים של פלישה לחייו של אדם או התערבות בהחלטותיו.[14] ככלי משלים להגדרת הזכות לפרטיות בהתבסס על רשימת מצבי הפגיעה הללו, הוסיפו דניאל סולוב ודניאל ציטרון רשימת נזקים הנגרמים עקב פגיעה בזכות לפרטיות.[15]

11 Ruth Gavison, *Privacy and the Limits of Law*, 89(3) The Yale Law Journal 421 (1980); רות גביזון "הזכות לפרטיות ולכבוד" **בלי הבדל ... זכויות האדם בישראל: קובץ מאמרים לזכרו של ד"ר חמן שלח ז"ל** 68 (רות גביזון עורכת, 1988).

12 סעיף 2 לחוק הגנת הפרטיות, התשמ"א–1981.

13 בירנהק, [מרחב פרטי], **לעיל** ה"ש 10, 83–85.

14 Daniel Solove, Understating Privacy (2008)

15 Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. 793 (2022)

תאוריה נוספת להמשגת הזכות לפרטיות הציעה הלן ניסנבאום בשנת 2010. לשיטתה, הזכות לפרטיות נלמדת מן ההקשר: כאשר הפרט מבקש לממש את זכותו לפרטיות אין הוא מעוניין להגביל את זרימת המידע על אודותיו או לשלוט במידע על אודותיו, אלא בהבטחה שהמידע יועבר בצורה ראויה ותואמת את הקשר הרלוונטי. לפיכך, ניסנבאום מציעה מנגנון שהיא מכנה "פרטיות הקשרית" (contextual integrity), אשר יבטיח זרימת מידע ראויה על אודות הפרט בכל תחום מתחומי החיים, בהתאם לנורמות הנהוגות בתחום שבו מתרחשת זרימת המידע, ובלי להיות תלוי טכנולוגיה ספציפית, זמן או מקום. הקביעה מהי הנורמה השלטת בנסיבות מסוימות תיעשה בהתאם למצב הקיים (סטטוס קוו).[16]

כל אחת מהגישות התאורטיות להמשגת הזכות לפרטיות טומנת בחובה קשיים מסוימים. כך, למשל, הגדרת הזכות לפרטיות על פי החלוקה לקטגוריות, כפי שנהוג כיום בחוק הגנת הפרטיות,[17] בעייתית נוכח טשטוש הגבולות בין המרחב הפרטי לבין מרחב הציבורי. אף התמקדות בפרטיות כגישה נתקלת בקשיים נוכח התפתחויות טכנולוגיות המאפשרות פגיעה במידה כזו או אחרת באוטונומיה ובמרחב הפרטי של האדם בלי לחדור פיזית לגופו או למרחבו הפיזי, ואף להגיע לחשיפת זהותו בלי לעבד מידע אישי שנאסף ישירות מנושא המידע, או אף ללא פרטי מידע מזהים כשלעצמם. גם גישת הפרטיות ההקשרית עלולה לרוקן את הזכות לפרטיות מתוכֶן ככל שהיא נשענת על המצב הקיים ועל מבחן הציפייה הסבירה. ולבסוף, גם אימוץ גישת הפרטיות כשליטה נתקל בקשיים אמיתיים נוכח הקושי המעשי לקבל הסכמה מדעת לכל איסוף מידע, עיבודו או שימוש בו.

עם זאת, עצם הניסיונות המרובים להמשיג את הזכות לפרטיות מעידים על חשיבותה ועל היותה זכות המאופיינת בעמימות רבה, טיבה נטול צורה, וגבולותיה מושפעים ממערכת היחסים הדינמית שבין הנורמות המקובלות

16 Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010)

17 סעיף 2 לחוק הגנת הפרטיות, התשמ"א–1981.

בחברה לבין תחומי המשפט והטכנולוגיה.[18] מדובר בזכות מורכבת החולשת על מגוון נרחב, ולעיתים מופשט, של פעולות, תופעות וחשיבויות. במובן הרחב ביותר ניתן לומר שפרטיות היא היכולת של הפרט להגדיר, בתנאיו שלו, את עצמו ואת מהותו כלפי העולם.

בעולם דיגיטלי מאוגמות על כל אחד ואחד מאיתנו כמויות מידע אישי עצומות אשר משמשות גופים מדינתיים ומסחריים לבניית פרופילים אישיותיים, פסיכולוגיים והתנהגותיים מדויקים למדי. פרופילים אלו משמשים ליצירת "מלכודות אוטונומיה", שבמסגרתן מוצעות לנושא המידע מגוון מצומצם של אפשרויות פעולה, כגון מזון שכדאי לו להזמין, נתיב נסיעה מועדף או סרט מוצע לצפייה בערב שישי. אפשרויות פעולה אלו הן יצירת מערכת ממוחשבת המנתחת את מאפייני אישיותו של נושא המידע בהתבסס על המידע האישי שנאסף עליו. המלצות פעולה אלו מהוות הלכה למעשה ויתור מצד נושא המידע על חלק מתהליכי קבלת ההחלטות האישי שבעבר היה מבצע בעצמו, והפקדתם בידי מערכות ממוחשבות אלו. אולם, אם לא נדע להציב גבולות או שלא נוכל להציבם, מערכות אלו ימליצו לנו גם מה לחשוב, למי להצביע ובמי להאמין. הסכנה לפרטיות וכלל לדמוקרטיה בנסיבות אלו ברורה. החלטות מהותיות כבר לא יהיו נתונות באמת בידי הפרט, האוטונומי, אלא יוכתבו לו, אף בלי שנתן עליהן את הדעת, על ידי תאגידים מסחריים או המדינה. כדי למנוע הידרדרות שכזו מציעה תהילה שוורץ אלטשולר להתייחס לזכות לפרטיות כאל זכות קבוצתית המגינה מפני מלכודות אוטונומיה ומבטיחה שיח ציבורי עשיר ומתפקד החיוני להליך דמוקרטי תקין.[19]

היקפה הרחב של הזכות לפרטיות אף הוביל להקבלת הפגיעה בה לתופעות כמו ההתחממות הגלובלית ושינוי האקלים, שהפילוסוף הבריטי טימותי מורטון כינה "היפר־אובייקט". מדובר בתופעות רחבות, שקשה לאדם להגדיר במלואן ולהבין את הסכנה הטמונה בהן לטווח הארוך. לכן במקום לנקוט פעולות לשם הגנת הזכות לפרטיות, מרבית הציבור בוחר בנוחות המיידית גם במחיר של

18 מיכאל בירנהק **פרטיות חוקתית** 25–26 (2023).

19 תהילה שוורץ אלטשולר "פרטיות: מלכת זכויות האדם בעולם דיגיטלי" **פרלמנט** 83 (המכון הישראלי לדמוקרטיה, 2019).

פגיעה בהן. למשל, אנשים ימשיכו להשתמש במזגן בימים חמים, על אף הידיעה ששימוש רב במכשירים צורכי חשמל גורם לפגיעה באיזון המובילה להתחממות הגלובלית. באופן דומה, מרביתנו נמשיך להשתמש ביישומון ניווט בטלפון הנייד, אף בידיעה שהיישומון אוסף עלינו מידע אישי ורגיש ומוכֵר אותו למרבה במחיר תוך כדי פגיעה חמורה בפרטיותנו.[20]

1.2. פרטיות העובד והפררוגטיבה הניהולית של המעסיק

ככלל, לעובד, ככל נושא מידע אחר, שמורה הזכות לפרטיות. אולם, ככל זכות יסוד חוקתית אין הזכות לפרטיות זכות יחידה או מוחלטת, אלא יש לאזנה למול זכויות יסוד ואינטרסים אחרים הראויים להגנה. במסגרת יחסי עובד-מעסיק למול זכות העובד לפרטיות ניצבת הפררוגטיבה הניהולית של המעסיק, הנשענת על זכות היסוד שלו לקניין. מכוח הפררוגטיבה הניהולית המעסיק אוסף מידע אישי רב על אודות העובד. בהקשר זה מקובלים שני מונחים, שהובנו לעיתים כבעלי משמעות זהה, לתיאור איסוף מידע על העובד על ידי המעסיק: "מעקב" (surveillance) ו"ניטור" (monitoring). התחושה העולה מן המונח ניטור חיובית יותר מזו המיוחסת למונח מעקב. ניטור נחשב מוגבל לבחינת פעולות העובד הקשורות במישרין לעבודתו, ואילו מעקב עשוי לכלול איסוף מידע, לרבות מידע אישי ומידע אישי רגיש, באופן חודרני יותר ושוטף, ממכלול פעולותיו של העובד, בין שהן קשורות לעבודתו ובין שלאו. כן עשוי המונח "מעקב" ללמד שאיסוף המידע נעשה בחשאי, בלי שהעובד מודע אליו כלל. בשיח הציבורי המונח "מעקב" מיוחס לרוב למאפיינים דיסטופיים, לדימוי של פנאופטיקון דיגיטלי הכולל מעקב א־סימטרי תמידי ושיטתי אחר העובד. מבחינת הפגיעה בפרטיות ניתן להתייחס לניטור ולמעקב כפעולות הממוקמות ברצף: מעקב ממוקם

20 TIMOTHY MORTON, HYPEROBJECTS (2013); Charlie Warzel, *Privacy Is Too Big to Understand*, NEW YORK TIMES (April 16, 2019)

בקצה המרוחק ומתאר פגיעה חמורה בפרטיות, ואילו ניטור ממוקם מרוחק מעט מנקודת קיצון זו.[21] במחקר זה המונח "מעקב" כולל כל פעולה של איסוף מידע אישי על אודות עובד, בין שהוא מכונה ניטור ובין שמעקב.

מעקב שמנהל מעסיק אחר עובדיו אינו תופעה חדשה. תחילתו במהפכה התעשייתית ומאז הוא נחשב אמצעי המעיד על יעילות המעסיק. זו דרכו של המעסיק להפיק מהמשאב האנושי את המרב למען רווחי העסק. תחילה, בוצע המעקב באמצעות תכנון המרחב הפיזי במקום העבודה: עיצוב המפעל בהתאם למודל הפנאופטיקון ובהמשך אימוץ השיטה של מרחב עבודה פתוח במשרד (open space), תוך מתן חשיבות רבה לעבודה משותפת, לשקיפות ולפתיחות, בלי לתת את דעתם לכרסום המתמשך בזכותם של העובדים ליהנות ממרחב פרטי מסוים, אשר יאפשר להם לנהל שיחה פרטית למשל עם רופא, עם פקיד בנק או עם מחנכת הכיתה של בתו, גם במקום העבודה.[22] ההתפתחויות הטכנולוגיות במהלך השנים הובילו לשכלול שיטות המעקב ולהעצמת חודרניותן. כך, החלו חברות שילוח לעקוב אחר נהגיהן באמצעות חיישן מיקום שהותקן ברכב, והשימוש המשולב למטרות פרטיות ועסקיות בטכנולוגיות תקשורת דוגמת דוא"ל פתח למעסיק צוהר למעקב אחר רחשי ליבו של העובד.[23] כן, נדרשו מעסיקים רבים לפגוע במידה מסוימת בזכות העובדים לפרטיות נוכח חובתם להגנת סייבר של מערכותיהם הממוחשבות, המנטרת פעמים רבות את תעבורת האינטרנט.[24]

21 Sara Riso, *Monitoring Surveillance of Workers in the Digital Age*, Euro found (Dec. 15, 2021)

22 Tracy Brower, *Why Privacy at Work is Important (Even if You Don't Have Any Secrets)*, FastCompany (Dec. 19, 2019); Katherine Hoppe, *From Utilitarianism to Fordism: How Americans Brought the Panopticon Home*, 44 Hastings Comm. Ent. L. J. 195, 197 (2022)

23 Murray Brown & Normann Witzleb, *Big Brother at Work*: *Workplace Surveillance and Employee Privacy in Australia*, 34 Australian Journal Of Labour Law 170 (2021); Hoppe, **לעיל** ה"ש 22, עמ' 197; Riso, **לעיל** ה"ש 21.

24 Dan Amiga, *Employees Deserve Online Privacy Too: Here's How to Deliver It to Them*, Forbes (Feb. 2, 2023)

כך, הפך המעקב לרכיב בלתי נפרד מחיי העבודה. עובדים מצפים שתפוקתם בעבודה תיבחן על בסיס איסוף מידע על תפקודם במהלך שעות העבודה. המעקב אף נחשב התנהגות ניהולית טובה וחלק מזכותו של המעסיק להבטיח חלוקת משאבים יעילה להגנה על סודות מסחריים, לניהול סיכונים ולציות עובדיו לחוק.[25]

עם זאת, נדמה שבמהלך השנים נטו המעסיקים לאמץ תפיסה מרחיבה, ולעיתים אף שגויה, של הפררוגטיבה הניהולית שלהם, אגב פגיעה לא מידתית בזכות העובדים לפרטיות.[26] מגמה זו לא התקבלה בהשלמה בקרב העובדים. לפי סקר בינלאומי שערכה בשנת 2022 חברת המחקר העולמית פורסטר, 72% מהעובדים שהשתתפו בסקר אינם מעוניינים שמידע אישי על אודותיהם ישמש, ללא הסכמתם, כחלק מפרויקטים של ניתוח כוח אדם. יותר ממחצית מהעובדים שהשתתפו בסקר היו מעוניינים בהגנה טובה יותר על זכותם לפרטיות ואף העידו כי הם נוקטים צעדים מעשיים למען הגבלת כמות המידע האישי שהם חולקים עם מעסיקיהם.[27] יתרה מכך, חיזוק התקשורת, הרשמית והאישית, בין כלל העובדים וההנהלה, נחשב גורם חשוב בהגברת יעילות העובד במקום העבודה. חיזוק כזה מושפע מכמה גורמים שונים, וביניהם הגברת הנראות והנגישות במרחב הפיזי, מספר העובדים השוהים יחד באותו מרחב, מידת הפתיחות בחלל העבודה וכן גם מידת ההגנה על פרטיותו של העובד במרחב.[28]

25 Kirstie Ball, *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations*, 4 (2021) Publication Office of the European Union; Riso, **לעיל** ה"ש 21.

26 האגודה לזכויות האזרח **זכויות האדם בישראל: תמונת מצב – 2013**, עמ' 86–87 (2013); Enza Iannopollo & Heidi Shey, *The Future of Work: Employee Privacy*, Forrester (Jan. 28, 2022); Amiga, **לעיל** ה"ש 24.

27 Iannopollo & Shey, **לעיל** ה"ש 26.

28 Hossein Motamed Chaboki, *The Impact of Visibility and Privacy in the Workplace on Organizational Productivity as Conducted Through Informal Interactions*, 7(5) J. of Business & Management 82 (2013)

1.3
טכנולוגיות למעקב אחר יעילות העובד

נדמה שהתפיסה המרחיבה של הפררוגטיבה הניהולית של המעסיק, והפגיעה החמורה בזכות העובד לפרטיות שהתאפשרה במסגרתה, הגיעה לשיאה בעת מגפת הקורונה והסגרים שנכפו על אוכלוסיית העולם. עובדים רבים, שעד פרוץ המגפה ביצעו את עבודתם ממשרדיו של המעסיק, החלו לעבוד בשיטה של "עבודה מרחוק", מבתיהם הפרטיים, תוך כדי שימוש במחשבים אישיים שלהם או שסופקו להם על ידי המעסיק ובטכנולוגיות תקשורת מרחוק דוגמת זום. בהיעדר פיקוח פיזי ישיר על העובדים, ונוכח השינוי המיידי בדפוסי העבודה ללא הכנה או הבנה מעמיקה של ההשלכות, לא היו בידי מרבית המעסיקים כלים להבטיח שהמשאבים שהם מעמידים לרשות העובדים, החל במחשב האישי וכלה בתשלום המשכורת, אכן ישמשו אותם לצורכי העבודה ולשם ביצוע משימותיהם ביעילות יחסית, בהתחשב בנסיבות הנלוות להסתגרות הכללית שכפתה מגפת הקורונה. לפיכך, ביקשו המעסיקים למצוא דרכים אחרות לפקח על יעילות העובדים. ואכן, הביקוש העולמי לתוכנות מעקב אחר עובדים עלה ב־108% באפריל 2020 וב־70% במאי 2020, לעומת הביקוש לתוכנות אלו בשנת 2019.[29]

חברת Hubstaff האמריקנית מתהדרת בכך שהטכנולוגיה שהיא מפתחת מסייעת להתייעלות צוותי עבודה בכל מקום. לדברי החברה, הטכנולוגיה שפיתחה מאפשרת למעסיק לעקוב אחר תוצריו והספקו של כל עובד, בלי להפריע לעובד עצמו. כן ניתן לעקוב אחר יכולת הצוות לעמוד ביעדים שהוצבו בפניו, הרווחיות של כל פרויקט ומידת ניצול התקציב בכל שלב. באמצעות המעקב מבליטה הטכנולוגיה את הישגיהם של העובדים המצטיינים ומאפשרת למעסיק להעניק להם הטבות כתגמול חיובי על השקעתם. החברה מדגישה כי פרטיותם של העובדים עצמם חשובה לה, וכי הטכנולוגיה שפיתחה

29 Ball, **לעיל** ה"ש 25, עמ' 54; Riso, **לעיל** ה"ש 21.

דווקא מסייעת לעובדים, בהעניקה למעסיק כלים לראות את עבודתו הטובה של העובד, בלי להטריד את העובד. כן מבטיחה הטכנולוגיה מעקב מדויק אחר שעות העבודה לשם חישוב שכר חף מטעויות. טכנולוגיית המעקב שלה מעניקה לעובד אף כלים לשלוט במעקב של המעסיק עליהם: (א) העובד יכול לשלוט בהגדרת שעות העבודה שבמהלכן יהיה נתון למעקב. לטענת החברה, הדבר דומה להחתמת שעון נוכחות בעבודה; (ב) צילום המסך ותיעוד אתרי האינטרנט שבהם מבקר העובד מבוצעים רק אם המעסיק בחר בכך; (ג) המעקב שקוף: העובד מקבל הודעות כאשר נלקח תצלום מסך של מחשבו האישי, מתי שעון הנוכחות שלו התחיל ולאיזה פרויקט; (ד) על העובד להסכים למעקב אחר מיקומו הגאוגרפי באמצעות מכשיר הטלפון הנייד שברשותו; (ה) לעובד ניתנת מעין "זכות עיון" במידע הנאסף עליו, וכן ברירת המחדל של טכנולוגיית המעקב היא שלעובד מוענקת, לתקופת זמן מוגדרת ומוגבלת, גם זכות למחוק תיעוד שבוצע עליו; (ו) החברה מתחייבת שמידע אישי שנאסף על העובד לא יימכר בשום מקרה לצדדים שלישיים.

* ראו באתר החברה Hubstaff, Power up with work from home software.

מגמת השגשוג והגידול בשימוש בטכנולוגיות מעקב אחר עובדים המשיכה במסגרת מתווה העבודה המשולב, אשר הפך למתווה עבודה שכיח בשנים שלאחר מגפת הקורונה. לצד הצורך הגובר בכלים לפיקוח על עובדים מרחוק, הפכו טכנולוגיות המעקב אחר עובדים לחודרניות, לזולות ולזמינות יותר מאשר בעבר.[30] כשנתיים וחצי מפרוץ מגפת הקורונה העולמית נמצא שאחת מכל שלוש חברות בגודל בינוני עד גדול בארצות הברית בעיקר, אולם גם באירופה ובישראל, אימצה סוג מסוים של טכנולוגיה למעקב אחר עובדים למטרת ניהול עובדים ומשימות ולהגברת היעילות, מצד העובד והמעסיק כאחד.[31] מדובר בקצב אימוץ

30 Amy Vatcha, *Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees*, 15(1) IS CHANNEL 4 (2020); Isabel Ebert, Isabelle Wildhaber & Jeremias Adams-Prassl, *Big Data in the Workplace: Privacy Due Diligence as a Human Rights-based Approach to Employee Privacy Protection*, BIG DATA & SOCIETY 1 (2021)

31 ניתוח אנושי, people analytics, מוגדר פרקטיקה לניהול משאבי אנוש, מחקר וחדשנות, העושה שימוש בטכנולוגיות מידע, כלי ניתוח והדמיה של נתונים תיאוריים וחזויים לשם הפקת תובנות בנוגע לדינמיקה בצוות העבודה, לגבי הצוות בכללותו

טכנולוגיה חסר תקדים, אשר שינה את מאפייני סביבת העבודה בעיקר בקרב עובדי הצווארון הלבן, שהיו רגילים למרחב גדול יותר בהשוואה לעמיתיהם ממעמד הצווארון הכחול, שחויבו גם בעבר בהחתמת שעון נוכחות כל אימת שנכנסו ויצאו מסביבת העבודה.[32]

חברת InterGuard האמריקנית משווקת את טכנולוגיית המעקב אחר עובדים שבפיתוחה ככלי אשר יאפשר למעסיק לדעת האם עובדיו "עובדים קשה או בקושי עובדים". מניעת "גנבת זמן" מצד העובד מוצגת כמטרה המרכזית אשר תוביל לחיסכון בכסף למעסיק ולהגברת יעילות העובד. מטרה זו מושגת באמצעות מעקב אחר זמני הכניסה והיציאה של העובד מהמערכת, צביעת זמנים פרודוקטיביים שלו לצד זמנים שאינם פרודוקטיביים, בחינת פעילותו ברשת האינטרנט ותצלומי מסך עיתיים. המידע מעובד ומוצג גרפית לצד מדדים המציגים את העובד היעיל ביותר בצוות ואת העובד הכי פחות יעיל. הטכנולוגיה גם מתריעה בזמן אמת כאשר העובד מקליד במחשבו מילים שאינן קשורות לעבודה: למשל, הימורים ברשת, תשלום חשבונות או חיפוש עבודה, משתמש ביישומונים או באתרים שהמעסיק הגדירם מראש כאתרים לא פרודוקטיביים, או מתנהג באופן החורג מהתנהגותו השגרתית

* ראו באתר החברה Employee Monitoring Made Simple, InterGuard.

טכנולוגיות המעקב אחר עובדים, אשר החלו עוד לפני הקורונה, הן חלק מתעשייה משגשגת המורכבת מחברות רבות המספקות כלים טכנולוגיים המעורבים בכל שלב משלבי העסקתו של עובד, החל במיונו, עובר בגיוסו, העסקתו, קידומו וניודו

ועובדים יחידים, שניתן לעשות בהן שימוש לשם הגברת הפרודוקטיביות של הארגון וניהולו הארגוני. ראו Aizhan Tursunbayeva, Stefano Di Lauro, & Claudia Pagliari, *People Analytics: A Scoping Review of Conceptual Boundaries and Value Propositions*, 43 International Journal of Information Management 224 (2018)

32 Christopher Mims, *More Bosses Are Spying on Quiet Quitters. It Could Backfire*, The Wall Street Journal (Sep. 17, 2022); Miriam Klöpper & Sonja Köhne, *People Analytics and the Promise of the Good Life: A Critical Transformative Perspective*, Wirtschaftsinformatik Proceedings 4 (2022)

בארגון וכלה בסיום העסקתו עקב פיטורין, התפטרות או פרישה.[33] טכנולוגיות המעקב אחר עובדים השתפרו והשתכללו במהלך השנים, ובעיקר בעקבות מגפת הקורונה. אין הן מתמצות עוד באיסוף מידע אישי באמצעות תוכנות המותקנות על המחשב או הטלפון הנייד של העובד או על מכשיר לביש שהוא עונד. חלק מטכנולוגיות המעקב הקיימות כיום משלבות, לצד איסוף המידע האישי, גם ניתוח אנושי, המשלב מידע אישי על אודות העובד ונתונים חיצוניים כגון נתוני תעבורת תקשורת, ומעבד אותם באמצעות בינה מלאכותית. מטרת הניתוח האנושי היא להפיק תובנות לגבי מצבו הנפשי של העובד או למאפייני אישיותו. תוכנות אלו משמשות לשיפור קבלת החלטות בנוגע לניהול עובדים ולחלוקת משימות, ומאפשרות ניהול צוותי עבודה מרחוק.[34] כל זאת לכאורה באופן אובייקטיבי יותר ממעסיק שעלול להיות מוטה לפי מגדר או מוצא אתני.

חברת Tele Link Soft הקפריסאית מפתחת ומשווקת את Kickidler, טכנולוגיה למעקב אחר עובדים בזמן אמת. הטכנולוגיה מאפשרת מעקב אחר הקשות מקלדת ועכבר, מעקב אחר משך הזמן שבו העובד עוסק במשימות בעבודה, משך הזמן שהוא מבזבז באתרים וביישומונים שהמעסיק הגדיר בלתי קשורים לעבודתו, ומשך הזמן שהוא כלל אינו נמצא ליד המחשב. התוכנה מצלמת בווידאו את צג המחשב של העובד כדי לבחון מה העובד עושה בשעות העבודה, ומאפשרת למעסיק שליטה מרחוק במחשבים שהוא מספק לעובדים לצרכיי העבודה. החברה מדגישה את השימוש המשולב בטכנולוגיית המעקב המסופקת על ידה הן לשם הגברת יעילות העובד והן לשם הגנת סייבר ומניעת אירועים מבפנים על בסיס חולשת הגורם האנושי. טכנולוגיית המעקב מעבדת את המידע שהיא אוספת לצורך חישוב אוטומטי של שעות העבודה של העובד, ניתוח מידת יעילותו ומעקב אחר יעילות כלל העובדים במהלך היום.

* ראו באתר החברה – Kickidler overview.

33 Wilneida Negron, *Little Tech Is Coming for Workers,* Coworker.org (2021)

34 כך למשל תוכנת Microsoft 360. בסוף שנת 2020 עוררה מיקרוסופט ביקורת ציבורית חריפה עקב שילוב כלי לדירוג היצרניות של העובדים בתוכנת Microsoft Workplace Analytics. ראו Alex Hern, *Microsoft Productivity Score Feature Criticized as Workplace Surveillance*, The Guardian (Nov. 26, 2020)

טכנולוגיות מעקב יכולות לאסוף מידע אישי על אודות עובד לא רק באמצעות תוכנות ייעודיות המותקנות לשם כך על המחשב או הטלפון הנייד של העובד. כך, למשל, במקומות עבודה העושים שימוש ברובוטים כסוג של עובד המסייע לעובד האנושי (corobot), מבוססת עבודת הרובוט על איסוף מידע רב מסביבת העבודה שלו, לרבות מידע אישי על עמיתיו האנושיים שבסביבתו. בכך, מנהל הרובוט גם מעקב אחר העובדים האנושיים.[35] גם טכנולוגיה מסוג "האינטרנט של הדברים" (Internet of Things – IoT) עשויה לאפשר מעקב אחר עובדים. לדוגמה, חברת המשתלות האיטלקית "Centro Seia" התקינה טכנולוגיה מסוג האינטרנט של הדברים במפעל השתילים שלה. הטכנולוגיה מנטרת בזמן אמת את איכות העבודה ומהירותה ואת מידת בזבוז הצמח בכל חיתוך של שתיל, במטרה לזהות במהירות שתיל מזוהם ולמנוע את התפשטות הזיהום לשתלים נוספים וכן ככלי להתמודדות עם האיסור האירופי על שימוש בחומרי הדברה מסוימים ולציות לו. אולם, בעקיפין עוקבת הטכנולוגיה אחר ביצועיו של כל עובד. החברה אף השתמשה במידע הנאגר באמצעות הטכנולוגיה כדי לתגמל עובדים שביצועיהם היו טובים בשיבוץ למשמרות נוחות יותר, במענקים כספיים ובקידום לתפקידי פיקוח.[36]

חברת Prodoscore האמריקנית מפתחת ומשווקת את טכנולוגיית המעקב Employee Productivity Monitoring – EPM המשמשת לבחינת יעילות העובדים. בהתבסס על פרדיגמת ה"נראות" (visibility), משלבת EPM ניתוח אנושי באמצעות בינה מלאכותית ועיבוד שפה טבעית ומספקת למעסיק מדדים בנוגע לתפוקת העובד במקום העבודה בעת שהות פיזית לעומת עבודה מרחוק, באילו כלים נעשה שימוש במסגרת העבודה, על מי מהעובדים מוטל עומס יתר, מי הם העובדים הבולטים בצוות. המדדים מאפשרים למעסיק למטב את קבלת החלטותיו בניהול העובדים והחברה, לתגמל עובדים טובים ולסייע לעובדים שמתקשים. כך מעניקה EPM לעובדים גמישות מבחינת מקום העבודה הפיזי ושעות העבודה, לצד אחריותיות. החברה אינה מפרטת מהו המידע שהיא אוספת וכיצד הוא מניע את רכיבי הבינה המלאכותית

35 Riso, **לעיל** ה"ש 21.

36 Anna Menenti, *Centro Seia*, European Monitoring Centre on Change (Nov. 26, 2021)

בטכנולוגיית המעקב לשם יצירת המדדים. עם זאת, מובהר ש־EPM אוספת רק מידע הקשור לפעילותו המקצועית של העובד ואינה חשופה לפרטי מידע אחרים, כגון, רשימת ההאזנה ביוטיוב, או העובדה שהעובד בודק את תוצאות משחקי הספורט של הקבוצה האהודה עליו באתר חדשות ספורט. החברה מכירה בכך שהמידע האישי הנאסף על העובדים עלול לשמש למטרות שאינן "טובות לארגון" ולכן היא מדריכה את משתמשיה כיצד לעשות שימוש מוסרי, מועיל, ואחראי במידע. במסגרת זו החברה מזכירה ללקוחותיה, המעסיקים, "לא לשכוח להיות אנושיים", ולכבד את פרטיות עובדיהם על ידי כך שיימנעו מלהשתמש במידע לשם ניגוח עובדים זה בזה, יגלו רגישות כלפי העובד ויעקבו אחר מגמות בדפוסי העבודה של העובד לאורך זמן. כלומר, המיקוד אינו בנקודת זמן בודדת אלא על המעסיק ללמוד את המגמות העולות מהמדדים שטכנולוגיית המעקב מספקת.

* ראו Why Employee Productivity־ו ,Prodoscore, How Prodoscore Works Monitoring, וכן Prodoscore, Prodoscore's Pledge, באתר האינטרנט של החברה.

1.3.1. יתרונות טכנולוגיות למעקב אחר עובדים

לטכנולוגיות מעקב במקומות עבודה מגוון יתרונות. במקרים מסוימים מעקב אחר העובדים הכרחי למניעת עבירות או נועד למען עמידה בדרישות רגולטוריות. כמו כן יכולות טכנולוגיות מעקב לאתר התנהגויות לא נאותות בסביבת מקום העבודה, מצד העובדים עצמם או מצד לקוחות הפונים לעובדים, וכך להבטיח את ביטחון העובדים האחרים. טכנולוגיות מעקב גם עשויות להגביר את ביטחונם של עובדים הנדרשים לבלות מרבית מעבודתם לבד, בדרכים או בבתי לקוחות. נוסף על כך הן יכולות לשמש כלי ללימוד. לדוגמה, טכנולוגיות לבישות עשויות לאפשר לעובד לבצע משימות מורכבות שהוא אינו מנוסה בהן תחת הדרכה ופיקוח של עובד מנוסה יותר ממנו, וכך לרכוש מיומנות נוספת במקום העבודה. עובדים אף יכולים להשתמש במידע שנאסף עליהם כדי להתייעל, להשתפר או לבוא בדרישות למעסיק אם עמדו ביעדים שהציב להם.[37] כמו כן, טכנולוגיות מעקב המשלבות ניתוח אנושי מאפשרות למעסיק לנהל

37 Riso, **לעיל** ה"ש 21.

מרחוק צוות עובדים מגוון בהעדפותיו ובמאפייניו. כך למשל אפשר באמצעותן לנהל עובדים המועסקים בשעות שונות, במדינות שונות ואף בשפות שונות, לשייך לכל אחד ואחד מהם משימה מתאימה ולפעול בשיתוף פעולה מלא בין אנשי הצוות למען סיום מוצלח של משימה.[38] כן עשויות טכנולוגיות מעקב להסב את תשומת ליבו של המעסיק למידת הלחץ של העובד ולסכנה לשחיקתו וכן נוטות לניתוח הישגיו של העובד ורמת יצרניותו לכאורה באופן אובייקטיבי יותר ממעסיק העשוי להיות מוטה לפי מגדר או מוצא אתני.[39]

חברת VeriClock הקנדית מאפשרת למעסיק לעקוב אחר זמני התחברות העובד למערכת ויציאתו ממנה, אחר מיקומו הגאוגרפי בעת התחברותו ובמהלכה עד התנתקותו. כמו כן היא מאפשרת לעובד לצלם את עצמו, בתמונה או בסרטון, לפני העבודה, במהלכה ובסיומה. על אף השונות בעומק המעקב ובהיקפו, החברה משווה את המוצר שלה למערכת נוכחות פיזית המוצבת במקום העבודה.

* ראו באתר האינטרנט של החברה – Get Up To Speed: Employee Time Tracking. For Anyone. From Anywhere

ולבסוף, ובכך טמון היתרון העיקרי שלהן בעיני המעסיקים, מסייעות טכנולוגיות מעקב אחר עובדים להערכת היעילות והפרודוקטיביות של מקום העבודה ושל העובד עצמו בהתבסס על פרדיגמת שליטה חדשה יחסית המכונה "נראות" (visibility). משמעות הנראות היא שקיפות מלאה כמעט של העובד כלפי המעסיק בהתבססו על המידע האישי הרב על ביצועי העובד, התנהגותו ומיקומו, שאוספת ומעבדת טכנולוגיית המעקב. השקיפות מאפשרת למעסיק ללמוד על מאפייני אישיותו ועל מצבו הנפשי של העובד וכך להטיל עליו משימות מתאימות עבורו, לנקוט פעולות אשר יתמרצו אותו או יגבירו את יעילותו ולהימנע מהעמסת יתר על עובד מסוים בהיסח הדעת. כך יכול המעסיק לקבל במהירות ובעלות נמוכה יחסית הערכת פרודוקטיביות אמינה לגבי העובד, ועל ידי כך להמשיך לאפשר עבודה במתווה היברידי.[40]

38 Ali Aslan Gümüsay et al., *Why Big Brother Should Not Be Watching You at Work*, Human Resource (July 15, 2022)

39 Klöpper & Köhne, **לעיל** ה"ש 32, עמ' 4.

40 Ebert et al., **לעיל** ה"ש 30, עמ' 3; Reid Blackman, *How to Monitor Your*

1.3.2. חסרונות טכנולוגיות למעקב אחר עובדים

בצד היתרונות הטמונים באותה "נראות" המתבטאים בשימושים המוצדקים והראויים בטכנולוגיות המעקב אחר עובדים, יש לתת את הדעת לכך שמדובר בטכנולוגיות דו־שימושיות העשויות לספק למעסיק מידע עודף שאין לו צורך בו, אך הוא עשוי לעשות בו שימוש לרעה, או מלכתחילה לעשות בטכנולוגיות המעקב שימוש למטרות לא חוקיות. בחסות המעטה המכובס של נראות, מדובר בשקיפות חד־כיוונית המאפשרת להעמיק את פערי המידע בין העובד לבין המעסיק. יש לכך מגוון חסרונות, כגון: פגיעה ביחסי האמון בין העובד לבין המעסיק ובתחושת השייכות והנאמנות של העובד לארגון; פגיעה במוטיבציה של העובד לתת מעצמו לטובת מקום העבודה; יצירת תחושת מעקב תמידית המשפיעה על תחושת המסוגלות של העובד ומובילה להגברת הלחץ שהוא נתון בו; אפליה לרעה בין העובדים, בעיקר כאשר מדובר בטכנולוגיות מעקב המשתמשות בבינה מלאכותית לשם הפקת מדדי יעילות שונים; העמקת פערי המידע והכוח בין העובד למעסיק; פגיעה ביכולתם של עובדים, בעיקר עובדים מן המעמד הנמוך, להתאגד כדי להגן על זכויותיהם; והחיסרון שאתמקד בו במחקר זה, ואשר מהווה את הבסיס המאפשר את מרבית הפגיעות האחרות, פגיעה ניכרת בזכות העובד לפרטיות.[41]

Employees While Respecting Their Privacy, Harvard Business Review (May 28, 2020)

41 ראו Ball, **לעיל** ה"ש 25, עמ' 36–37, 41; Maren Gierlich-Joas, Mena Angela Teebken, & Thomas Hess, *A Synthesized Perspective on Privacy and Transparency in the Digital Workplace*, 55 Hawaii International Conference on System Sciences 5191, 5192 (2022); Pauline T. Kim & Matthew T. Bodie, *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, 35 ABA Journal Lab. & Emp. Law 289, 293–301 (2021); Sonja Köhne & Miriam Klöpper, *Working from Home but Never Alone: Why People Analytics Have to Be Designed with the Employee in Mind*, Digital Society Blog, The Alexander von Humboldt Institute for Internet and Society (April 12, 2021); כמו כן ראו Vatcha, **לעיל** ה"ש 30, עמ' 5; Mims, **לעיל** ה"ש 32; Ebert et al., **לעיל** ה"ש 30, עמ' 3; Riso, **לעיל** ה"ש 21; Blackman, **לעיל** ה"ש 40; Klöpper & Köhne, **לעיל** ה"ש 32, עמ' 4; Negron, **לעיל** ה"ש 33; Zickuhr, **לעיל** ה"ש 2, עמ' 10–11.

טכנולוגיית המעקב של חברת Veriato האמריקנית משתמשת בבינה מלאכותית לצורך ניתוח דפוסי התנהגותו של העובד. הטכנולוגיה מתריעה אוטומטית כל אימת שהיא מזהה פעילות לא שגרתית או פעילות שהוגדרה אסורה. כך, מאפשרת הטכנולוגיה ניהול יעיל של העובדים, הגברת הנראות של כל עובד לצד הגברת האבטחה והתמודדות עם אירועי סייבר שמקורם בגורם האנושי. לטענת החברה לטכנולוגיה שלה יתרון משמעותי על פיקוח אנושי, שכן היא מבצעת מעקב אובייקטיבי ונטול דעות קדומות. עם זאת, החברה מעודדת את לקוחותיה לנהוג בשקיפות מלאה בנוגע לשימוש שהם עושים בטכנולוגיית המעקב, היקף המעקב המבוצע ומטרותיו, במטרה לגבש תמיכה רחבה בקרב העובדים לשימוש בה.

* ראו באתר האינטרנט של החברה – Monique Zubicki, *The Myths and Truths of Employee Monitoring*, (Veriato Blog [Oct. 20, 2022])

דוגמה ליום בחייו של עובד הנתון למעקב טכנולוגי חודרני ניתן למצוא בתיאור יום בחייה של רינה, העובדת באחד ממחסניה של חברת אמזון בארצות הברית. עם הגעתה למקום העבודה בבוקר, רינה מעבירה את תג העובד שלה. החיישנים בתג העובד מאפשרים לה לעבור את דלת הכניסה, ומאותו רגע קולטת טכנולוגיית המעקב את מיקומה לאורך כל שעות העבודה. בטרם היא מתחילה את עבודתה, ניגשת רינה לחדר המנוחה הקרוב ככל הניתן לעמדת העבודה שבה היא מוצבת כדי לאחסן במקררים שבו את קופסת האוכל שלה. היא אינה רוצה לבזבז משלושים הדקות המוקדשות להפסקת הצוהריים שלה זמן על הליכה בטלה בתוך מתחם המחסן הענק. תפקידה של רינה לבחון את הפריטים החולפים במסוע בקצב של 1,800 פריטים בשעה. קצב עבודתה וטיבה מנוטרים על ידי סורקים דיגיטליים משולבים בבינה מלאכותית המוצבים על המסוע נוסף על מפקח אנושי. כל הפסקה שרינה נוטלת, לרבות הליכה לשירותים, שאינה במסגרת ההפסקה היומית המוקצבת לה, נמדדת ונחשבת כנטילת חופשה. כאשר מואטת תנועת המוצרים על המסוע על רינה לפנות בבקשה לקבל משימה חדשה, אחרת ייחשב זמן האטת המסוע כזמן חופשי גם כן. עובד שנרשמות לו דקות חופשה רבות מדי מסתכן בפיטורים. בסוף יום העבודה

על רינה לעבור דרך כמה חיישנים שתפקידם למנוע גניבת מוצרים על ידי העובדים.[42]

טכנולוגיית המעקב DeskTime פותחה על ידי חברה מלטביה ומאפשרת למעסיק לצוות עובדים לפי פרויקטים ולקבוע את השעות במהלך היום שבהן הוא מעוניין שכל עובד יעבוד. הטכנולוגיה גם עוקבת אחר פעילותו של כל עובד במחשב, מרגע הפעלתו ועד לכיבויו, באופן אוטומטי, ללא צורך בהתחברות אקטיבית מצידו וללא קשר לשעות העבודה המוגדרות שלו. במסגרת זו הטכנולוגיה אוספת מידע על אודות משך בזמן שבו שהה העובד בכל אתר אינטרנט, לאילו אתרים הוא גולש, באילו יישומונים משתמש, אילו קבצים פתח וכמה זמן היה עסוק בכל קובץ, ומתייגת את שעות עבודתו לשעות יצרניות, שעות ניטרליות ושעות שאינן יצרניות. הטכנולוגיה מצלמת את המסך של העובד מדי פעם במהלך שעות העבודה כדי לאפשר למעסיק לדעת איזה שימוש עשה העובד בפועל במחשבו במהלך שעות העבודה. המעסיק יכול לבחור אם להפעיל שימוש זה לגבי כלל העובדים או רק לגבי עובדים מסוימים. הטכנולוגיה מאפשרת לעובד להגדיר מראש פרקי זמן "פרטיים" במהלך היום שבהם הוא עוסק בפעילות שאינה קשורה בעבודה ובמהלכה התוכנה לא תעקוב אחר פעילותו. כמו כן כדי למנוע תופעה של עובדים אשר עובדים יותר מדי שעות ועלולים להגיע לתשישות, התוכנה מאפשרת למעסיק לשלוח התראות לעובדים שעליהם לצאת להפסקה או לקחת "זמן פרטי".

* ראו באתר האינטרנט של החברה – The ultimate all-in-one time tracker for your business

תיאור זה ממחיש במדויק כיצד המעקב הטכנולוגי ההדוק על העובד מוביל להפיכתו לקובץ נתונים בלבד (המכונה "datafication of employment"), מעין קובץ אקסל המלמד על דקות העבודה, התפוקה, ההפסקה, וייתכן אף מאפיינים בריאותיים או על מאפייני אישיות המשפיעים על תפוקותיו. התייחסות זו פוגעת באופן ממשי בזכות היסוד לפרטיות, בין שלפי תפיסת הפרטיות הצרה

42 Wilmeida Negron & Aiha Nguyen, *The Long Shadow of Workplace Surveillance*, Stanford Social Innovation Review (Sep. 6, 2023)

המתמקדת בהבנת הפרטיות כשליטתו של אדם במידע הנוגע לו ובין שבמובנה הרחב כזכות חשובה וחיונית לעצמאות הפרט, ובכלל זאת למחשבתו החופשית וליכולתו לקבל החלטות עצמאיות. לא זו אף זו, הפיקוח המתמיד של המעסיק על כל תנועותיו ופעולותיו של העובד מאפשר לו למנוע מפגשים בין העובדים, לשלוט במסרים המועברים בהן ובכך למזער את הסיכוי שהעובדים ייפגשו, ישוחחו על נושאים שמטרידים אותם ואולי אף יתארגנו כדי לבוא מאוחדים אל המעסיק בדרישות למען הגנה על זכויותיהם.[43]

מגפת הקורונה ומתווה העבודה ההיברידי שממשיך אחריה הובילו להתרחבות השימוש בטכנולוגיות מעקב גם לעובדים במקצועות חופשיים ולעובדי הצווארון הלבן. השימוש בטכנולוגיות מעקב אחר העובדים הנמנים עם המגזרים האלה מאתגר עוד יותר את תפיסת פרטיות העובד. אם בעבר עסק הדיון בשאלת פרטיות העובד בגידורם של איי פרטיות במרחב הציבורי שבמקום העבודה הפיזי, כאשר העבודה מבוצעת מהבית מתהפכות הנסיבות, והעבודה, שעד כה נחשבה מרחב ציבורי, נכנסת למרחב הפרטי ביותר של העובד. השימוש בטכנולוגיות מעקב בנסיבות אלו מוביל לכך שהבית אינו משמש עוד רק כמרחב הפרטי והמוגן של העובד.[44] בכך מְטשטשות טכנולוגיות המעקב אחר עובדים את הגבול בין המרחב הפרטי לבין המרחב הציבורי, והופכות את נראותו של העובד, על יכולותיו, ביצועיו, מאפייניי אישיותו ותחושותיו, לרשימה ארוכה של נתונים כמו גיליון אקסל גדול.

טשטוש הגבולות והחדירה החמורה למרחב הפרטי של העובד עומדים בניגוד גמור לתחושתם של עובדים רבים כאילו העבודה מרחוק מאפשרת להם עצמאות נרחבת יותר מאשר זו שנהנו ממנה, כאשר שהו פיזית במקום העבודה. תחושה מזויפת זו אף מתעצמת ככל שהשימוש בטכנולוגיות המעקב נעשה באופן

43 Sam Adler-Bell & Michelle Miller, *The Datafication of Employment: How Surveillance and Capitalism Are Shaping Workers' Future Without Their Knowledge*, The Century Foundation (2018); Negron, **לעיל** ה"ש 33.

44 Qingqin Zhang, *Workplace Surveillance and Protection of Worker's Privacy in Covid-19*, a paper presented in Queen Mary Postgraduate Law Conference (2021)

חשאי או בלי שהוסבר כראוי לעובדים.[45] יתרה מכך, גם כאשר המעסיק מיידע את העובד בדבר השימוש שהוא עושה בטכנולוגיות מעקב, העובד לא בהכרח מבין או יודע מהו המידע האישי שנאסף עליו ומהו היקפו, השימוש בו ומטרותיו. החברות המפתחות טכנולוגיות מעקב משתמשות במילים כלליות ומכובסות דוגמת "ניטור פרודוקטיביות", הקפדה על שעות עבודה ומניעת בזבוז זמן. רק חברות מעטות טורחות להבהיר במדויק מהו המידע האישי והרגיש הנאסף על אודות העובד, כיצד הוא מעובד ונשמר ולאילו מטרות.[46]

החברה הבריטית Analog Republic משווקת את טכנולוגיות המעקב אחר עובדים Sneek. הטכנולוגיה מאפשרת למעסיק לצלם את עובדיו, באמצעות המצלמה המותקנת במחשבם בפרקי זמן שיקבע. הטכנולוגיה גם מאפשרת לנהל שיחות וידאו עם כל אחד מהעובדים, ומתירה לכל עובד לסמן אם הוא פנוי לשיחה או עסוק. בתיאור הטכנולוגיה בעמוד הבית, מרגיעה החברה את המשתמשים, שאולי מוטרדים מכך שהם מצולמים באמצעותה מדי כמה דקות, באמירה "Yes, we all pick our noses, there's no shame". אמירה שיותר מכול מלמדת על מידת החודרנות שמאפשרת הטכנולוגיה. כמו כן, בהסבר בנוגע לאפשרות הסימון "עסוק" או "זמין לשיחה", מעירה החברה, ספק בצחוק וספק ברצינות, שסימון אי־זמינות לשיחה משמעותו "well that obviously means you're in the toilet".

* ראו באתר האינטרנט של החברה – Human contact for remote teams.

גם טכנולוגיית מעקב, המוגבלת לכאורה להפקת מדדי יעילות בלבד, נדרשת לאסוף כמויות עצומות של מידע. למשל, הפקת מדדי יעילות על סמך עיבוד שפה טבעית (Natural Language Processing – NLP) מחייבת איסוף כמויות גדולות של דוגמיות תקשורת אנושית.[47] לפיכך, טכנולוגיות המעקב עלולות לחרוג ממעקב המתמקד בביצועיו של העובד ונתפס כמוצדק וכחודרני במידה

45 Ball, **לעיל** ה"ש 25, עמ' 73; Gierlich-Joas et al., **לעיל** ה"ש 41, עמ' 5195; Köhne & Klöpper, **לעיל** ה"ש 41.

46 Vatcha, **לעיל** ה"ש 30, עמ' 6; Ebert et al., **לעיל** ה"ש 30, עמ' 1–2.

47 Kim & Bodie, **לעיל** ה"ש 41, עמ' 302.

ראויה,[48] לאיסוף מידע אישי שנחשב לא נחוץ לצורך הערכת ביצועיו בעבודה, ולכן נתפס כחודרני וכפוגעני יותר.[49] משום כך, בפועל, טכנולוגיות למעקב אחר עובדים עשויות להיות חודרניות ביותר ולפגוע קשות בפרטיות העובדים. בעוד בעבר ההגבלות על פרטיותו של עובד במקום העבודה הפיזי היו ברורות, פגיעה בפרטיות העובד באמצעות טכנולוגיות מעקב, המאפשרות חדירה לביתו הפרטי ולמחשבותיו, היא בגדר עליית מדרגה מבחינת היקף הפגיעה האפשרי בחסות מה שמקובל לכנות "הפררוגטיבה של המעסיק".[50]

חברות הטכנולוגיה עצמן מודות בכך שבצד היתרונות הרבים הטמונים בטכנולוגיית המעקב אחר העובדים, הן עשויות גם לשמש לרעה. נשיא חברת Prodoscore אף דימה את טכנולוגיית המעקב שהוא משווק לרובה, אשר יכול לשמש למטרות ראויות ולמטרות רעות.[51] ואולם, נדמה שהנהירה לדיגיטציה של סביבת העבודה ולשימוש הגובר בטכנולוגיות מעקב עובדים נעשית בלי להבין לעומק את האתגרים הכרוכים בכך, ובעיקר בלי לתת את הדעת לאיזון הנחוץ בין פרטיות העובד לבין יעילות הארגון.[52]

1.4
האיזון בין הזכות לפרטיות לבין הפררוגטיבה הניהולית של המעסיק: סקירת משפט משווה

לצד ההכרה בפררוגטיבה הניהולית של המעסיק, כחלק מזכות היסוד החוקתית שלו לקניין, חשוב להגן גם על זכות העובד לפרטיות החיונית לאוטונומיה שלו וכן על חשיבתו היצירתית וחדשנותו. בחלק זה נבחן אם וכיצד האסדרה החקיקתית

48 Ball, **לעיל** ה"ש 25, עמ' 53–54.

49 Daniel M. Ravid *et. al.*, *EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring*, 46(1) Journal of Management 100, 102 (2020); **שם**, עמ' 12, 22–23, 35.

50 Hoppe, **לעיל** ה"ש 22, עמ' 198.

51 Mims, **לעיל** ה"ש 32.

52 Gierlich-Joas et al., **לעיל** ה"ש 41, עמ' 5198.

הקיימת בארצות הברית, באיחוד האירופי ובישראל, מגינה על זכות העובד לפרטיות מפני הסכנה שבשימוש לרעה בטכנולוגיות מעקב. בחינה זו תסייע להערכת האפשרויות העומדות בפני עובד המבקש להתגונן מפני פגיעה בלתי חוקית בפרטיותו באמצעות טכנולוגיות מעקב ותחזק את הבנת הצורך באימוצה של דוקטרינת ההפרה התורמת ככלי נוסף בארגז הכלים שבידי עובד שפרטיותו נפגעה.

1.4.1. ארצות הברית

בארצות הברית, עיגונה החוקי של הזכות לפרטיות והיקפה תלויים בסוג מקום העבודה. במקומות עבודה ציבוריים, מעוגנת זכותו של עובד לפרטיות מכוח התיקון הרביעי לחוקה.[53] היקפה של הזכות לפרטיות נקבע לפי מבחן הציפייה הסבירה, אשר פורש כמעניק זכות מצומצמת ביותר לפרטיות העובד במקום עבודתו. במהלך השנים התירו בתי המשפט פגיעה בפרטיותם של עובדים מנימוקים של הבטחת יעילות כלכלית או בטיחות בעבודה, ואף קבעו כי הודעה מטעם המעסיק על קיומה של טכנולוגיית מעקב אחר העובד במקום העבודה מבטלת לחלוטין את זכותו של העובד לפרטיות במקום העבודה.[54]

במקומות עבודה פרטיים, ההכרה בזכות העובדים לפרטיות מבוססת על המשפט המקובל, והיקפה נקבע בהתאם לחוק במדינה שמאוגדת בה החברה המעסיקה, בהתאם לפרשנותו בפסיקה ובהתאם למבחן הציפייה הסבירה. הלכה למעשה מדובר בזכות צרה. הזכות לפרטיות המבוססת על המשפט

53 U.S. Constitution, Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issues, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

54 Hoppe, **לעיל** ה"ש 22, עמ' 204–205; Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees,* 42 J. Marshall L. Rev. 83 (2008); Kim & Bodie, **לעיל** ה"ש 41, עמ' 304–305.

המקובל כוללת הגנה מפני חדירה למקום שמסתגר בו אדם, גילוי פומבי של מידע פרטי מביך על אדם, פרסום המעמיד אדם באור שלילי ומסחור בשמו של אדם. פגיעה בפרטיות נחשבת עוולה נזיקית ביותר מארבעים מדינות בארצות הברית. הוכחתה של העוולה הנזיקית מחייבת שהפגיעה בפרטיות היא מכוונת, מהווה פגיעה בציפייתו הסבירה של העובד לפרטיות וכשלעצמה מהווה פגיעה ממשית בעיני האדם הסביר.[55] אולם, במהלך השנים העניקו בתי המשפט המדינתיים הגנה רבה יותר לזכות הקניין של המעסיק ולאינטרס הכלכלי שלו על פני הזכות לפרטיות. במסגרת זו הכירו בתי המשפט בהיעדר ציפייה סבירה לפרטיות היכן שהמעסיק מחזיק במדיניות ברורה של מעקב אחר העובד או כאשר הסכים העובד לפגיעה בפרטיותו.[56]

בית המשפט העליון בניו ג'רזי דן בשנת 2010 בזכותה של עובדת לפרטיות במידע אישי על אודותיה, שנאסף באמצעות טכנולוגית המעקב שהותקנה בהיחבא במחשב הנייד שסיפק לה מקום העבודה וצילמה באופן עיתי את מסך המחשב. אחד התצלומים היה של תכתובת שניהלה העובדת עם עורך דינה באמצעות תוכנת דואר אלקטרוני מוגנת בסיסמה וכלל מידע אישי שלא היה ידוע קודם לכן למעסיק. בית המשפט פסק שלעובדת הייתה ציפייה סבירה לפרטיות בנושא תכתובת הדואר האלקטרוני שלה, שכן היא הגנה עליה באמצעות שם משתמש וסיסמה, ולפיכך פגע המעסיק בפרטיותה.[57]

בקליפורניה זוכה הזכות לפרטיות לעיגון בחוקת המדינה,[58] ופגיעה בה נחשבת עוולה נזיקית. בפרשנות שניתנה לזכות בבתי המשפט בקליפורניה נפסק שלעובד ציפייה סבירה, במידה מוגבלת, לפרטיות במקום העבודה. אולם, עוד נקבע שלמעסיק אינטרס גובר ליצירת סביבת עבודה בריאה ובטוחה. כך, למשל, נפסק שלעובדים במעון ילדים ציפייה סבירה לפרטיות במשרד שהם עובדים בו, מאחורי דלתיים סגורות. אולם, התקנת מצלמת מעקב במשרד, אשר הופעלה

55 **שם**.

56 Hoppe, **לעיל** ה"ש 22, עמ' 204–205.

57 Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 990 (2010)

58 Cal. Const. art. I §12: "Every natural person has the right to be let alone and free from governmental intrusion into person's private life except as otherwise provided herein"

רק בשעות הלילה, אחרי שהמעסיק גילה שאחד מהמחשבים במשרד שימש בשעות אלו לצפייה באתרי פורנו, אינה חדירה פוגענית לפרטיות העובד. נפסק כי אינטרס המעסיק ביצירת סביבת עבודה בריאה ובטוחה לילדים החוסים במעון גוברת על זכות העובדים לפרטיות. עוד נקבע שהסכמת העובד לפגיעה בפרטיותו מאיינת את ציפייתו הסבירה לפרטיות ומונעת ממנו לטעון שהמעסיק חדר לפרטיותו באופן פוגעני.[59] יתרה מכך, בקליפורניה, בקונטיקט ובדלאוור די בהודעה מטעם המעסיק בדבר קיומה של טכנולוגיית מעקב אחר העובדים כדי להכשירה ולאיין את ציפייתו הסבירה של העובד לפרטיות במקום העבודה, למעט מקומות הנחשבים פרטיים באופן מסורתי כמו השירותים במקום העובדה או ביתו הפרטי של העובד. טכנולוגית מעקב המותקנת על גבי מחשבו של העובד ומנטרת את שגרת חייו בביתו, עשויה להוביל לפגיעה בפרטיות, שהיא עוולה נזיקית, ובלבד שהעובד מוכיח שהמידע שנאסף עליו הוביל לפגיעה ממשית ומכוונת בפרטיותו הגוברת על אינטרס המעסיק בהגברת היעילות ובהבטחת סביבת עבודה ראויה.[60]

נוסף על כך, זכותם לפרטיות של עובדים במקומות עבודה ציבוריים ופרטיים זוכה להגנה מסוימת גם בחוק יחסי העבודה הפדרלי, ומעקב לא סביר אחר עובד יכול להיחשב פרקטיקת העסקה בלתי הוגנת. עם זאת, במרבית המקרים מדובר במעקב שמבצע המעסיק כאשר מתעורר חשדו להתאגדויות עובדים במסגרת ארגוני עובדים, ולאו דווקא מעקב קבוע במסגרת מהלך העסקים הרגיל והשגרתי.[61]

סקירת פעולות האכיפה שביצעה במהלך השנים נציבות המסחר הפדרלית (Federal Trade Commission, להלן: FTC) לגבי טכנולוגיות מעקב מסחריות, מלמדת על עמדת ה־FTC, כרשות אכיפה פדרלית, בנושא זכות העובד לפרטיות. כך, בשנת 2013 הגישה ה־FTC תלונה נגד חברת DesignerWare בגין איסוף לא הוגן, ולפיכך בלתי חוקי, של מידע אישי. באותן נסיבות דובר בחברה אשר פיתחה, שיווקה ותפעלה את טכנולוגיית המעקב "PC Rental Agent" לשימושן של

59 Hoppe, **לעיל** ה"ש 22, עמ' 206–208.

60 Kim & Bodie, **לעיל** ה"ש 41, עמ' 305.

61 National Labor Relations Act, 29 U.S.C. §§151–169; Hoppe, **לעיל** ה"ש 22, עמ' 208–209.

חברות בתעשיית השכרת ציוד וריהוט ביתיים ורכישתם (Rent-to-own stores). הטכנולוגיה הותקנה על מחשבים טרם השכרתם. השוכר לא יכול היה לאתרה על גבי המחשב המושכר או להסירה. התוכנה אפשרה לבעל רישיון השימוש בה להפסיק מרחוק את פעילות המחשב השכור כאשר הלקוח השוכר לא עמד בתשלומי השכירות או הפר את חוזה ההשכרה, לאתר את מיקומו הגאוגרפי של המחשב, ולהפעיל מרחוק תוסף לתוכנה המכונה "Detective Mode". תוסף זה אפשר לבעל רישיון השימוש לעקוב בחשאי, וללא ידיעת המשתמש במחשב המושכר, אחר הפעילות המבוצעת באמצעות המחשב המושכר, לרבות מעקב אחר הקלדות, הקלקות עכבר, תצלומי מסך של הפעילות המבוצעת במחשב ושימוש במצלמת המחשב לשם צילום כל מי שנתפס באמצעותה. המידע שנאסף באמצעות התוסף הועבר לשרתיה של חברת DesignerWare ומשם, באופן לא מוצפן, לכתובת הדוא"ל, שציין בעל רישיון השימוש. פעמים רבות כלל המידע שנאסף מידע פרטי, סודי ואישי. למשל, מעקב אחר ההקלדות חשף סיסמאות גישה של המשתמש לחשבונותיו בשירותי דואר אלקטרוני, ברשתות חברתיות וכן במוסדות פיננסיים. תצלומי מסך שביצע התוסף חשפו לעיתים מידע רפואי, תכתובות דואר אלקטרוני אישיות עם רופאים, עם מעסיקים ועם עורכי דין. התצלומים שביצע התוסף באמצעות מצלמת המחשב חשפו את כל מי שהיה בעת הצילום בטווח המצלמה, לרבות ילדים וזוגות במצבים אינטימיים. החברה אומנם המליצה ללקוחותיה ליידע את שוכרי המחשב בדבר קיומה של התוכנה על גבי המחשב המושכר, אולם לא חייבה אותם לעשות כן, וגם לא נקטה שום צעד כדי לקבוע אם חנות השכרת הציוד פעלה בהתאם להמלצותיה. יתרה מכך, החברה המליצה ללקוחותיה להפעיל את התוסף בחשאי. אומנם, החברה הבהירה שהשימוש בתוסף הוא לצורך איתור מחשב שאבד או נגנב ולצורך זיהוי האדם שמשתמש בו. עם זאת, היא לא ניטרה את איסוף המידע ולא הגבילה את גישת בעל רישיון השימוש רק למקרים שבהם אכן השימוש בתוסף נועד לאיתור מחשב אבוד או גנוב.[62]

במקרה אחר, במרץ 2020, הגישה ה־FTC תלונה נגד חברת Retina-X Studios בנימוק שבפעולותיה פגעה בפרטיות ובסודיות של מידע אישי, בעיקר הנוגע

62 Comp., In re DesignerWare, LLC, F.T.C. File No. 1123151 (April 11, 2013)

לילדים. החברה פיתחה ושיווקה רישיונות שימוש בטכנולוגיות שאפשרו מעקב, לרוב חשאי, אחר משתמש במכשיר טלפון נייד או במחשב. הטכנולוגיות שווקו ככלי למעקב הורים אחר ילדיהם או מעסיקים אחר עובדיהם, אך החברה לא נקטה שום אמצעי כדי להבטיח שהשימוש בטכנולוגיה יוגבל למטרות אלו בלבד. טכנולוגיית המעקב "MobileSpy", שנועדה להתקנה על מכשירי טלפון ניידים של עובדים וילדים, אספה הודעות טקסט, מסרונים שנשלחו בתוכנות מסרונים, היסטוריית התקשרות, הקלדות, מיקום גאוגרפי, תמונות, רשימת אנשי קשר, תצלומי מסך והיסטוריית גלישה של המכשיר שהותקנה בו. גרסת הפרמיום שלה אפשרה גם מעקב מרחוק ובזמן אמת אחר מסך המכשיר הנייד. טכנולוגיית המעקב "PhoneSheriff", שנועדה למעקב אחר ילדים, אספה פרטי מידע אישי, כגון מיקום גאוגרפי, הודעות טקסט, היסטוריית התקשרויות, תמונות, אנשי קשר, היסטוריית גלישה, רשימות, קובצי מוזיקה, לוח שנה ויומן, יישומונים שהותקנו על גבי המכשיר, תקציר שימוש במכשיר, היסטוריית תכתובות דוא"ל ותצלומי מסך של כל פעילות אשר בוצעה באמצעות היישומון "Snapchat". טכנולוגיית המעקב "TeenShield" אפשרה מעקב אחר מכשירי טלפון ניידים ואספה נתונים על תאריך הלידה של המשתמש במכשיר, מיקום, מסרונים, היסטוריית התקשרות, תמונות, אנשי קשר, היסטוריית גלישה והיסטוריית תכתובות דוא"ל. לשם התקנת כל אחת מטכנולוגיות המעקב נדרש בעל הרישיון להחזיק במכשיר הנייד פיזית ולפרוץ חלק מהגנות היצרן שהוטמעו בו. משום כך, קבע ה־FTC כי הגבלת השימוש למעקב אחר ילדים או עובדים היא מס שפתיים בלבד וכי לא זו הייתה כוונתה האמיתית של החברה. יתרה מכך, ברירת המחדל של כל אחת מטכנולוגיות המעקב הייתה חשיפת דבר קיומה למשתמש במכשיר. עם זאת, בעל רישיון השימוש יכול היה לבחור להתקינה בחשאי בלי ליידע את המשתמש במכשיר בדבר קיומה. במקרה זה, נבצר מן המשתמש במכשיר להסירה. ה־FTC הסיק שחברת Retina-X Studios הסבה נזק של ממש למשתמשי המכשירים הניידים שכן אפשרה למחזיק ברישיון השימוש לעקוב אחר המשתמשים בחשאי, לאסוף לגביהם מידע אישי ללא רשות ולעקוב בחשאי אחר תנועותיהם הפיזיות ואחר פעולותיהם ברשת האינטרנט. מכלול מידע זה שימש את המחזיקים ברישיון השימוש בטכנולוגיות המעקב לביצוע מעקב אחר משתמשי המכשירים הניידים, אגב גרימת נזק נפשי, רגשי, פיננסי, חברתי ואף פיזי, לרבות מוות. יתרה מכך, אף אם הניחה החברה שמוצריה משמשים למטרות חוקיות לצורך מעקב של הורים אחר ילדיהם או מעסיקים אחר עובדיהם, היא

לא נקטה את האמצעים הנאותים כדי להגן כראוי על המידע האישי שנאסף באמצעות טכנולוגיות המעקב שפיתחה, ולמנוע גישה לא מורשית אליהן.[63]

במקרה אחר בחן ה־FTC את טכנולוגיית המעקב של חברת Support King, אשר אפשרה לבעל רישיון השימוש בה לעקוב בחשאי אחר כל פעולותיו של אדם במכשיר הטלפון הנייד שלו, לרבות מיקומו הגאוגרפי ומידע אישי רגיש על אודותיו. עם התקנתה במכשיר אספה טכנולוגיית המעקב מידע אשר כלל מסרונים, היסטוריית התקשרויות, מיקום גאוגרפי, היסטוריית גלישה, אנשי קשר, תמונות, לוח שנה, קבצים שהורדו למכשיר הנייד והודעות. כן יכלו מפעיליה לחסום מרחוק יישומונים שהותקנו על המכשיר הנייד, לקבל דוח בנוגע לשימוש שנעשה במכשיר הנייד וליצור תכתובות טקסט מזויפות הנחזות להיות ממשתמש המכשיר עצמו. גרסת הפרימיום שלה אפשרה גם איסוף מידע הכולל תכתובות דוא"ל, התקשרויות וידאו, פעילות המבוצעת באמצעות יישומונים, לרבות רשתות חברתיות, תמונות שהמשתמש במכשיר שיתף ביישומונים המיועדים לכך ומידע ששלח ביישומוני היכרויות. גרסה נוספת של טכנולוגיית המעקב, המכונה "Xtreme", אפשרה לבעל הרישיון בה גם להשתמש מרחוק ובחשאי במצלמה ובמיקרופון של המכשיר. התקנת טכנולוגיית המעקב התאפשרה רק למי שהחזיק פיזית במכשיר, והיה בעל הרשאות "מנהל" בתוכנת ההפעלה של המכשיר הנייד. עם זאת, לאחר התקנתה, טכנולוגיית המעקב לא הוצגה כיישומון במכשיר הנעקב ובעל רישיון השימוש אף יכול היה לבחור להסירה מרחוק. עם התקנתה הוצגה על גבי המסך הודעה מפורשת, ולפיה השימוש בטכנולוגיית המעקב נעשה לצורך מעקב אחר ילדים או עובדים, אולם חברת Support King לא נקטה שום אמצעי כדי להבטיח שהשימוש אכן יוגבל רק למטרות אלו. יתרה מכך, לפי ה־FTC, האפשרות להגביל את השימוש למטרה זו היא בגדר מס שפתיים בלבד, משום שהתקנת טכנולוגיות המעקב חייבה את המתקין לבצע פעולות אשר פגעו באחריות היצרן למכשיר הטלפון וסביר שהורה או מעסיק לא ירצו בהן, בייחוד לנוכח קיומן של חלופות המאפשרות מעקב אחר ילדים או עובדים בלי לדרוש זאת. עוד טען ה־FTC שהחברה לא נקטה אמצעי הגנת מידע והגנת סייבר נאותים, עובדה שאפשרה מתקפת סייבר וחשיפת פרטיהם של יותר מ־2,000 משתמשי מכשירים שהותקנה בהם טכנולוגיית המעקב. כמו

63 Compl., In re Retina-X Studios, LLC, F.T.C. File No. 172-3118 (Mar. 26, 2020)

כן, נטען שטכנולוגיית המעקב של החברה אפשרה התעללות במי שהטכנולוגיה הותקנה על מכשירו הנייד, והסבה נזקים כספיים, בריאותיים ונפשיים חמורים. העובדה שמשתמש במכשיר נייד כלל לא ידע ולא יכול היה לדעת על קיומה של תוכנת המעקב על מכשירו העצימה נזקים אלו. חומרתן של הנזקים גוברת על התועלת שהפיקו בעלי רישיון השימוש בטכנולוגיית המעקב וכן על אינטרס הציבור בקיומו של שוק תחרותי.[64]

לצד פעולות אכיפה אלו פרסם ה־FTC באוגוסט 2022 להערות הציבור הצעת אסדרה בנושא שיטות למעקב מסחרי ולהגנת מידע הפוגעות בצרכנים ובעובדים (להלן: ההצעה).[65] בהצעה סוקר ה־FTC את הסכנות שבשיטות המעקב המסחרי (commercial surveillance), הכולל איסוף המידע האישי מצרכנים ומעובדים על ידי חברות מסחריות, אגירתו, עיבודו, שמירתו, העברתו ומסחורו, ומתאר את ההשפעה על בטיחותם של נושאי המידע ועל בריאותם הנפשית, את פגיעותם של ילדים ונוער ואת החשש מאפליה על בסיס מגדר או מוצא אתני. כמו כן נקבע שלמרות כמה פעולות אכיפה שנקט ה־FTC בשנים האחרונות,[66] נראה שתופעת המעקב המסחרי שכיחה ביותר ואין די בפעולות אכיפה בודדות כדי לספק לצרכנים הגנה נאותה. לפיכך יש צורך באימוץ כלל משפטי אשר יספק ודאות משפטית בדבר סטנדרט להגנת הפרטיות ויאפשר ל־FTC להטיל עונשים כבדים יותר על חברות המפירות אותו.[67] בהצעה ביקש ה־FTC את תגובות הציבור

64 Comp., In re Support King, LLC, F.T.C. File No. 192-3003 (Dec. 20, 2021)

65 Federal Trade Commission, Advance Notice of Proposed Rulemaking: Commercial Surveillance ANPR, R111004 (Aug. 22, 2022, 16 CFT chapter undef, 2022-17752)

66 ראו למשל Comp., In re Support King, LLC, F.T.C. File No. 192-3003 (Dec. 20, 2021); Compl., In re Retina-X Studios, LLC, F.T.C. File No. 172-3118 (Mar. 26, 2020); Comp., for Permanent Injunction and Other Equitable Relief, FTC v. CyberSpy Software, LLC., No. 6:08-cu-01872 (M.D. Fla. Filed Nou. 5, 2008)

67 Federal Trade Commission, Advance Notice of Proposed Rulemaking: Commercial Surveillance ANPR, R111004 (Aug. 22, 2022, 16 CFT chapter undef, 2022-17752), 51276, 51280; מוגדר בהצעה ככולל גם עובדים "consumer" מכל סוג.

בשלושה נושאים עיקריים: (א) אופיין ושכיחותן של שיטות מעקב מסחרי מזיקות ושל הגנת מידע חסרה; (ב) איזון בין העלויות לבין התועלות של שיטות אלו מבחינת הצרכן ומבחינת התחרות בשוק, וכן האיזון בין עלות לתועלת של כל כלל משפטי אפשרי לאסדרתן; (ג) הצעות להגנה על צרכנים מפני מעקב מסחרי שכיח ומזיק ומפני פרקטיקות הגנת מידע קלוקלות.[68]

עיון בפעולות האכיפה ובקול הקורא להערות הציבור מלמד שה־FTC מייחס חשיבות למודעותו של אדם להיותו נתון במעקב ולמנגנוני הגנת הסייבר ואבטחת המידע. נדמה כי ה־FTC אינו מציב קווים אדומים בנוגע להיקף המעקב האפשרי שרשאי המעסיק לבצע אחר עובדיו או לעצם המעקב עצמו. לפיכך, מבחינת התמונה הכוללת, היקפה של הזכות לפרטיות במקומות עבודה מצומצם ומוגבל בארצות הברית. בתי המשפט מדגישים במידה רבה הן את האינטרס של המעסיק ביצירת סביבת עבודה בטוחה והן את השיקול הכלכלי כגוברים על זכות העובד לפרטיות או כמאיינים את ציפייתו הסבירה של עובד לפרטיות במקום העבודה מלכתחילה. לפיכך רק עובדים בעלי כוח מיקוח רב הנובע מכישוריהם, מניסיונם או מהיותם מאוגדים נהנים הלכה למעשה מהגנה על זכותם לפרטיות במקום העבודה. באווירה שכזו ההגנה על פרטיות העובד בתנאים שבהם נעשה שימוש בטכנולוגיות מעקב היא מצומצמת ביותר.[69]

1.4.2. האיחוד האירופי

1.4.2.1. ההגנה על הזכות לפרטיות לפי ה־GDPR

לפי דיני האיחוד האירופי, זכותו של עובד לפרטיות מבוססת, בראש ובראשונה, על עיגונה של הזכות לפרטיות בסעיף 8 לאמנת זכויות האדם האירופית,[70]

68 **שם**, עמ' 51281.

69 Hoppe, **לעיל** ה"ש 22, עמ' 210; Kim & Bodie, **לעיל** ה"ש 41, עמ' 312.

70 European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15 (להלן: אמנת זכויות האדם האירופית).

לצ'רטר האירופי לזכויות יסוד[71] ועל אמנת ליסבון.[72] עם זאת, היקפה של זכותו של העובד לפרטיות על בסיס דברי החקיקה הללו נתון לפרשנות. ואכן, במסגרת סמכויותיו לאכוף את הוראות אמנת זכויות האדם האירופית, בית המשפט האירופי לזכויות אדם (European Court of Human Rights – ECtHR) עיצב במהלך השנים את גבולותיה של זכות העובד לפרטיות. כך, בשנת 1993 נפסק שהזכות לפרטיות כוללת הגנה על חייו האישיים של אדם, וזו כוללת לא רק את קשריו של נושא המידע עם המעגל הקרוב אליו, אלא גם את זכותו של אדם לפתח מערכות יחסים עם אנשים מחוץ למעגל זה.[73] ברוח זו נפסק ששיחות טלפון, תכתובות דוא"ל והיסטוריית הגלישה ברשת האינטרנט המבוצעות ממקום העבודה עשויות ליהנות מהגנה מכוח הזכות לפרטיות, ובלבד שהמעסיק לא יידע את העובד מראש שהתקשרויות אלו מנוטרות על ידיו. כן הובהר שמגבלות על פרטיות העובד חייבות להיות מידתיות למען השגת אינטרס לגיטימי של המעסיק.[74]

בהמשך אף נפסק שמעקב של מעסיק אחר השימוש שעושה עובד ברשת האינטרנט, לרבות מעקב אחר תכתובת פרטית של העובד באמצעות תוכנת מסרים מיידיים, אינו מידתי להשגת האינטרס הלגיטימי של המעסיק ולכן הוא בגדר פגיעה לא חוקית בזכות העובד לפרטיות.[75] לפסיקות אלו עשויה להיות חשיבות רבה בבחינת זכותו לפרטיות של עובד במציאות העבודה מרחוק, שכן הן מאפשרות הרחבת הזכות לפרטיות מעבר למעגל הפנימי המצומצם של חייו האישיים של אדם, גם למעגלים נוספים אשר הופכים לרלוונטיים כאשר מיטשטשת ההבחנה בין ביתו וחייו הפרטיים של העובד לבין מרחב עבודתו.[76]

71 Charter of Fundamental Rights of the European Union (2016/c 202/02) (להלן: הצ'רטר האירופי לזכויות יסוד).

72 The Treaty on the Functioning of the European Union (TFEU) (להלן: אמנת ליסבון).

73 *Niemietz v. Germany* (1993) 16 E. H. R. R 97, [27]–[29]

74 *Halford v. United Kingdom* (1997) 24 E.H.R.R. 523, [1]–[2]; Copland v. United Kingdom (2007) 45 E.H.R.R. 37, [39]–[49]

75 Bărbulescu v. Romania [2016] IRLR 235

76 Zhang, **לעיל** ה"ש 44.

היקפה של זכות העובד לפרטיות מושפע גם מתקנות הגנת הפרטיות (General Data Protection Regulation; להלן: GDPR), המונות כמה נסיבות שבהן מותרת פגיעה בזכות לפרטיות.[77] כך, למשל, מותרת פגיעה בפרטיות בעקבות עיבוד מידע אישי על העובד אם נדרש הדבר לפי חוק,[78] למשל לפי חוקי עבודה. כן מותר לעבד מידע אישי על עובד אם המידע נחוץ לצורך עמידה בהתחייבות חוזית של המעסיק לפי חוזה שהעובד הוא צד לו.[79] על רקע תלותו של העובד במעסיק, הסכמתו של העובד לפגיעה בפרטיותו[80] תותר רק במקרים נדירים שבהם אין להסכמה שום השפעה על זכויותיו או על חובותיו של העובד בעבודה.[81]

הצדקה נוספת, לפי ה־GDPR, העשויה לאפשר פגיעה בזכותו של עובד לפרטיות היא נחיצות הפגיעה למען הגשמת אינטרס לגיטימי של בעל השליטה במידע, כלומר המעסיק.[82] אינטרס עסקי לגיטימי אפשרי הוא הגנת סייבר, מניעה של אובדן מידע אישי, למשל על אודות לקוחות, מניעה של אובדן קניין רוחני או רכוש פיזי, מניעת התנהגות לא חוקית או לא הולמת מצד העובד או שיפור יעילות העובד וביצועיו. כך נתונה הפררוגטיבה של המעסיק בחסות הצדקת האינטרס הלגיטימי.

בחוות דעתה משנת 2017 התייחסה המועצה האירופית להגנת מידע (European Data Protection Board, להלן: EDPB) לאפשרות המעסיק להישען על הצדקת

77 סעיפים 6 ו־9 ל־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, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (להלן: GDPR).

78 **שם**, ס' 6(1)(c).

79 **שם**, ס' 6(1)(b).

80 **שם**, ס' 6(1)(a).

81 **שם**, ס' 43(1) הקדמה; Article 29 Data Protection Working Party, *Opinion 2/2017 on Data Processing at Work*, 17/EN WP 249 (June 8, 2017); Pauline T. Kim & Matthew T. Bodie, *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, 35 ABA JOURNAL LAB. & EMP. LAW 289, 309 (2021)

82 ס' 6(1)(f) ל־GDPR.

האינטרס הלגיטימי הקבועה ב־GDPR. אף שחוות הדעת פורסמה בשנת 2017, לפני מגפת הקורונה ולפני שגשוג טכנולוגיות המעקב אחר עובדים, הקווים המנחים שנקבעו בה חשובים להבנת האיזון שבין צורכי המעסיק לבין זכות העובד לפרטיות.[83]

לפי חוות הדעת, במציאות הטכנולוגית כיום, הישענות על הצדקת האינטרס הלגיטימי של ה־GDPR כמכשירה את השימוש בטכנולוגיות מעקב במסגרת יחסי עובד–מעסיק לשם מימוש האינטרס לגיטימי של המעסיק בשיפור היעילות והגנה על נכסיו, עלולה להתיר מעקב חודרני ולא מוצדק על העובד, משלוש סיבות עיקריות: הסיבה הראשונה, עלותה הנמוכה של טכנולוגיית המעקב לצד היכולת הטכנולוגית המשתפרת לאסוף מידע רב יותר ומגוון יותר, מגבירות את הסיכון לעיבוד לא ראוי של מידע אישי. למשל, טכנולוגיות המותקנות כחוק כדי להגן על נכסי המעסיק, כגון מצלמות וידאו במקומות העבודה או מערכות מעקב אחר נתוני מיקום, עשויות לאפשר מעקב לא חוקי אחר זמינות העובד, ביצועיו והתנהגותו. הסיבה השנייה, חוסר השקיפות הגובר של טכנולוגיות המעקב מעורר שאלות בנוגע למודעותם של העובדים להיותם נעקבים. הסיבה השלישית, טשטוש הגבולות הגובר בין המרחב הביתי לבין מרחב העבודה, בעיקר כאשר מדובר בעובדים העובדים מרחוק או נדרשים לנסיעות עבודה, מגביר את הסיכון לגלישה למעקב על חייו הפרטיים של העובד. הסכנה אף גוברת על רקע הופעת טכנולוגיות האוספות הקלקות, עוקבות אחר תנועות העכבר, שימוש ביישומונים והיסטוריית הגלישה, ואף מצלמות מדי פעם את מסך העובד או את העובד עצמו, תוך כדי תיעוד סביבת העובד והנוכחים בה. כמו כן, מעקב אחר השימוש שהעובד או אחד מבני ביתו עושה במחשב מעבר לשעות העבודה, בעיקר אם מדובר במחשב פרטי של העובד ובאמצעותו הוא מתחבר לעבודה, עלול להוביל לפגיעה חמורה בפרטיותו של העובד.

לפיכך, כדי להישען על הצדקת האינטרס הלגיטימי הקבועה ב־GDPR, על המעסיק להבטיח את מידתיות הפגיעה ונחיצותה. כן עליו לעמוד בעקרון מזעור המידע, כלומר לאסוף רק מידע הכרחי להגשמת התכלית – האינטרס הלגיטימי, לעבד את המידע באופן הגון כלפי העובד ולפעול בשקיפות. בבחינת מידתיות הפגיעה בפרטיות העובד, ה־EDPB מייחסת חשיבות לשונות בין המרחבים

83 Article 29 Data Protection Working Party, **לעיל** ה"ש 81.

שבהם מתרחשת הפגיעה: המרחב הפיזי של העובד, המרחב הפיזי של המעסיק, המרחב הדיגיטלי של המעסיק או המרחב הדיגיטלי האישי של העובד. ככלל ניתן לומר שככל שהמעקב חודרני יותר, כך יתקשה המעסיק להצדיק את הפגיעה בפרטיות העובד בטענה למידתיות ולנחיצות למען הגשמת אינטרס לגיטימי שלו.[84] דוגמאות למעקב חודרני הן: איסוף מקיף ומסיבי של מידע אישי ללא מגבלות, כולל באזורים רגישים כגון שירותים או חדרי הלבשה; שימוש במידע שמתקבל עקב המעקב לקבלת החלטות אוטומטיות בנוגע לביצועיו של העובד ללא מעורבות אנושית; מעקב חשאי מתמשך ללא חשד סביר למעשה עבירה.

לפי ה־EDPB כדי להישען על הצדקת האינטרס הלגיטימי לפי ה־GDPR, וכצעד מקדים טרם הטמעת טכנולוגיית מעקב העלולה לפגוע בזכות העובד לפרטיות, על המעסיק לבצע הערכת אינטרס לגיטימי (legitimate interest assessment). אף שהערכה כזו אינה נדרשת במפורש ב־GDPR, אי־ביצועה יקשה על המעסיק להוכיח ציות לעקרון האחריותיות. נוסף על כך, כאשר עיבוד המידע עלול להוביל לסיכון ממשי לזכויות ולחירויות אדם, למשל במקרה של מעקב שיטתי ומקיף של העובד או שימוש במידע אישי רגיש בהיקפים גדולים, על המעסיק לבצע, לפי ה־GDPR, תסקיר השפעה על הפרטיות (data protection impact assessment).[85]

לצד המסגרת הכללית לבחינת פגיעה בפרטיות העובד למען הגשמת האינטרס הלגיטימי של המעסיק, בחנה ה־EDPB גם נסיבות מעקב ספציפיות. כך, למשל, ציינה כי בשם האינטרס הלגיטימי של המעסיק להגן על מערכות המחשב של העסק ועל המידע האגור בהן, רשאי המעסיק להתקין מערכת להגנת סייבר, הכוללת: מעקב אחר כלל התקשורת היוצאת במטרה לאתר פרצות אבטחה, סינון אתרי אינטרנט ותכנים, מעקב אחר גישת עובד מזוהה למערכת ומעקב אחר השימוש במכשירים וביישומונים, ובלבד שהפגיעה בפרטיות עומדת בדרישת הנחיצות, המידתיות והשקיפות. אולם, לפי ה־EDPB, ככלל עדיף שטכנולוגיות להגנת סייבר יתמקדו במניעה, למשל בחסימת הגישה לאתרי אינטרנט חשודים, ופחות בניטור תעבורת האינטרנט הקיימת. כחלק מדרישת

84 Ball, **לעיל** ה"ש 25, עמ' 72–73; ס' 13–14 ל־GDPR; Article 29 Data Protection Working Party, **לעיל** ה"ש 81, עמ' 3–4, 9–10.

85 Ball, **לעיל** ה"ש 25, עמ' 72–73; ס' 13–14 ל־GDPR.

המידתיות הציעה ה־EDPB שהמעסיק יאפשר לעובד לסמן ביישומון לוח השנה "פגישות פרטיות", שהמעסיק לא יוכל לנטר את תוכנן, ימנע מהפעלת טכנולוגיית המעקב בשעות הערב והלילה, או ימנע מסריקת ספריות מסוימות במחשב, כגון ספריית התמונות שצולמו באמצעות המכשיר.[86] כמו כן המערכות, המיועדות להגנת סייבר ומנטרות את כלל הפעילות המבוצעת ברשת המעסיק, יימנעו מניטור פעילות באתרי בנק או בריאות, כדי לאפשר לעובדים לבצע פעולות חשובות, שהם זכאים לבצע באתרים שכאלו. כן הוצע כי יוצבו במקום העבודה עמדות מחשב חופשיות מטכנולוגיות מעקב ושאינן מחוברות לרשת המעסיק, שבאמצעותן יוכלו העובדים לבצע פעילות פרטית שהם זכאים לבצעה בזמן העבודה. דוגמה נוספת היא מערכת למניעת אובדן מידע (data loss prevention) המנטרת את כל תכתובות הדוא"ל היוצאת מרשת המחשב של המעסיק כדי להבטיח שאינה כוללת, במכוון או שלא במכוון, מידע אישי על אודות לקוחות. כחלק מדרישת המידתיות, הציעה ה־EDPB כי הכללים שלפיהם תקבע המערכת מהי תכתובת דוא"ל חשודה יהיו ברורים וידועים לעובדים, וכי כאשר תזהה המערכת תכתובת חשודה, היא תשלח אזהרה לכותב הדוא"ל עוד בטרם העברת התכתובת, כך שיוכל לבחור אם להימנע משליחתה.[87]

עוד ציינה ה־EDPB כי מעקב אחר הבעות הפנים של העובד הוא בלתי מידתי וככלל על המעסיק להימנע משימוש בטכנולוגיות לזיהוי פנים (facial recognition). עם זאת, ה־EDPB הכירה בכך שמעקב אחר תנועותיו של העובד, למשל באמצעות מעקב אחר נתוני המיקום של העובד או רכב העבודה המשמש אותו, עשוי לעמוד בדרישת הנחיצות. כך למשל כאשר מטרת המעקב היא להבטיח את בטיחותו של העובד או של העובדים שהוא מסיע. אולם, טכנולוגיות מעקב אלו יכולות לאסוף גם פרטי מידע נוספים כמו דפוסי הנהיגה של העובד. לפיכך, אף אם השימוש בטכנולוגיות מעקב אחר מיקום נחוץ לשם הגשמתו של אינטרס לגיטימי של המעסיק, עליו להפעיל את הטכנולוגיה באופן מידתי ושקוף. לדוגמה, לאפשר לעובד לכבות את המעקב במקרים מסוימים, כגון ביקור אצל רופא. כמו כן על המעסיק להימנע מעיבוד המידע למטרות שאינן קשורות בהבטחת בטיחות העובד, כגון הערכת ביצועיו של העובד. כן על המעסיק ליידע את העובד בבירור

86 Article 29 Data Protection Working Party, **לעיל** ה"ש 81.

87 **שם**.

על קיומה של טכנולוגיית מעקב למשל ברכב העבודה המשמש אותו. המעקב אחר המיקום צריך להיות מוגבל לשעות העבודה המוסכמות בלבד. אם קיימת הצדקה להמשך המעקב מעבר לשעות העבודה, יש להטמיע מגבלות נוספות על עיבוד המידע. למשל, שהמעקב יופעל רק אחרי שהמערכת מזהה את יציאתו של הרכב מאזור מוסכם או מהמדינה, כדי למנוע גניבה, או שנתוני המעקב ייחשפו בפני המעסיק רק על ידי בקשה פעילה מצידו.[88]

גם כאשר הפגיעה בפרטיות העובד מותרת, על המעסיק למלא אחר דרישות ה־GDPR, לרבות כיבוד זכויות העובד לעיון במידע, לתיקונו ולמחיקתו. עוד חייב המעסיק לאחסן את המידע באופן מאובטח ולתקופה הנחוצה בלבד,[89] ולהראות שנקט את האמצעים הראויים כדי להבטיח איזון הולם בין זכויות העובד לבין האינטרס הלגיטימי של המעסיק. עוד נדרש המעסיק לכבד את זכות העובד להתנגד להחלטה בעניינו המתקבלת על בסיס עיבוד ממוכן של מידע אישי אודותיו, ללא התערבות אנושית משמעותית. זכות זו עשויה להיות רלוונטית לטכנולוגיות מעקב רבות אשר מדרגות את העובד בהתאם לרמת יעילותו ומעניקות לו הטבות על בסיס דירוג זה.[90]

ה־GDPR אף מסמיך את המדינות החברות באיחוד לקבוע, בחוק או בהסכמים קיבוציים, כללים ספציפיים שמטרתם להבטיח הגנה על זכויות העובד וחירויותיו בעת עיבוד מידע אישי על אודותיו בהקשר של יחסי עובד־מעסיק. כל כלל שכזה חייב לכלול אמצעים מתאימים וייחודיים להגנה על כבודו של העובד, על האינטרסים הלגיטימיים שלו ועל זכויות היסוד שלו, בייחוד לגבי שקיפות העיבוד, העברת מידע אישי בין חברות קשורות ומערכות מעקב במקום העבודה.[91]

1.4.2.2. ההגנה על הזכות לפרטיות וחוק ה־AI

לצד דברי החקיקה העוסקים במפורש בזכות לפרטיות, ייתכן שניתן ללמוד גם מהאסדרה של בינה מלאכותית על המסגרת המשפטית הרלוונטית לשימוש

88 שם.

89 Ball, **לעיל** ה"ש 25, עמ' 72–73.

90 Ebert t al., **לעיל** ה"ש 30, עמ' 4; ס' 22(1) ל־GDPR.

91 ס' 88 ל־GDPR; Article 29 Data Protection Working Party, **לעיל** ה"ש 81, עמ' 8–9.

בטכנולוגיות מעקב. נציבות האיחוד האירופי הגישה הצעת חוק בנושא כבר בשנת 2021. במהלך שנת 2023 התקיימו דיונים לגבי נוסחה הסופי וההצעה אומצה לכדי חוק במרץ 2024.[92]

חוק ה־AI מדרג מערכות בינה מלאכותית לארבע רמות סיכון – לא מקובל, גבוה, מוגבל או מינימלי – בהתאם להערכת הסיכון שהשימוש בהן ואופיו עלולים להטיל על בריאות הציבור, על ביטחונו או על זכויות יסוד כגון: הזכויות לכבוד, לפרטיות, לשוויון, לחופש ביטוי, לחופש אספה, לסעד יעיל ולחזקת החפות וכן לעקרון המִנהל התקין. מערכות בינה מלאכותית המופעלות במקומות עבודה, כגון מערכות למיון ולגיוס עובדים ולניהול תפוקות עובדים, מדורגות ברמת סיכון גבוה.[93] לפיכך גם טכנולוגיות מעקב אחר עובדים, המשלבות מערכות בינה מלאכותית המספקות תובנות בנוגע ליעילותו של העובד ולהתאמתו לביצוע משימות שונות, עשויות להיכלל ברמת סיכון זו.

מערכות בינה מלאכותית המדורגות ברמת סיכון גבוה מותרות לשיווק ולשימוש בשוק האיחוד האירופי אך ורק בכפוף לציות לדרישות המהותיות והמִנהליות המפורטות בחוק ה־AI. אי־עמידה בדרישות תוביל לחסימת השיווק והשימוש

92 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels, 21.4.2021 (COM[2021] 206 final, 2021/0104 [COD]); הצעת החוק אומצה כלשונה על ידי הפרלמנט האירופי במרץ 2024. ראו European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on Laying down Harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending Certain Union Legislative Acts (COM[2021]0206 – C9-0146/2021 – 2021/0106(COD)) (להלן: חוק ה־AI); Gian Volpicelli, *ChatGPT Broke the EU Plan to Regulate AI*, Politico (March 3, 2023); Spencer Feingold, *The European Union's Artificial Intelligence Act, Explained*, World Economic Forum (March 28, 2023)

93 עמ' 13 וס' 5.2.3 לדברי ההסבר, ס' 6(2) לחוק ה־AI וסעיף 4 ל־ANNEX III לחוק ה־AI; Daniel Stander, *THE EU's Proposed Artificial Intelligence Act*, XIII(116) National Law Review (April 26, 2023)

בטכנולוגיה בשוק האיחוד האירופי.[94] הדרישות הללו כוללות מגוון דרישות משפטיות הקובעות סטנדרט מינימלי במכלול נושאים הקשורים למידע, לרבות ממשל נתונים (data governance), תיעוד המידע ושמירתו, שקיפות ויידוע המשתמשים, פיקוח אנושי, דיוק ואבטחה.[95] להלן פירוט כמה מן הדרישות.

אחת הדרישות היא שמערכות בינה מלאכותית המשלבות מודלים של למידת מידע על בסיס אימון, תיקוף ובחינה של מידע ישתמשו רק במערכי נתונים (data sets) העומדים בדרישות ניהול ראוי של מידע המפורטות בחוק ה־AI. יש לבצע פעולות כגון אלה: בניית מערכי נתונים הכוללים רק את המידע הרלוונטי לפעולות העיבוד; הערכה מוקדמת של מערכי הנתונים הדרושים, ובכלל זאת זמינותם, כמותם והתאמתם לצרכים; בחינה מראש של הטיות אפשריות; זיהוי פערים וחוסרים אפשריים במידע ובחינת הדרכים להתמודד עימם.[96]

עוד נדרש שהתיעוד הטכני של מערכות בינה מלאכותית בסיכון גבוה יבוצע לפני החדרתן לשוק ויישמר מעודכן כל העת. התיעוד הטכני חייב לאפשר לרשויות המדינתיות האחראיות להעריך על בסיסו את מידת הציות של המערכת לדרישות הטכניות הקבועות בחוק ה־AI.[97]

כן מחויבות מערכות בינה מלאכותית בסיכון גבוה לאפשר תיעוד אוטומטי של אירועים (logs) במהלך הפעילות השגרתית של המערכת. התיעוד האוטומטי צריך להיעשות כך שיאפשר מעקב אחר פעילות המערכת לכל אורך חייה וניטור התרחשויות אשר עשויות לסכן את הבריאות, את הבטיחות או את זכויות היסוד של האנשים שעליהם היא מופעלת או לשנות באופן משמעותי את המערכת.[98]

חובה נוספת היא חובת השקיפות ויידוע המשתמשים. לפי חובה זו יש לתכנן ולפתח מערכות בינה מלאכותית בסיכון גבוה באופן המבטיח שאופן פעולתן

94 הוראות חוק ה־AI בנוגע למערכות המסווגות בסיכון גבוה ייכנסו לתוקפן 36 חודשים מחקיקת החוק. ראו ס' 179 לדברי ההסבר לחוק ה־AI.

95 **שם**, ס' 5.3.3 לדברי ההסבר וההוראות הקבועות ב־Title III, Chapter 2.

96 **שם**, ס' 10.

97 **שם**, ס' 11.

98 **שם**, ס' 12.

שקוף במידה המאפשרת למשתמש בהן לפרש את הפלט של המערכת, לקבל הסבר לגביו וכן להשתמש בו כראוי.[99]

עוד מוטלת החובה לעצב ולפתח מערכות בינה מלאכותית בסיכון גבוה באופן אשר יאפשר פיקוח אנושי יעיל במהלך כל תקופת השימוש במערכת. מטרת הפיקוח האנושי היא למנוע או למזער סיכונים לבריאות, לבטיחות או לזכויות יסוד שיכולים לנבוע מהשימוש במערכת, אגב הבאה בחשבון גם שימוש לרעה במערכת. ההנחה היא שבאמצעות הפיקוח יוכל המשתמש להבין את יכולותיהן ומגבלותיהן של המערכות הללו, וכך יוכל להבטיח פרשנות נכונה של הפלט שלהן ואף להחליט, בנסיבות מתאימות, להימנע משימוש בהן, להתערב בפעולתן או לעצור אותה לחלוטין.[100]

כן מטיל חוק ה־AI מגוון דרישות על גורמים שונים לאורך חיי המוצר, החל בספקי מערכות בינה מלאכותית בסיכון גבוה, עבור ביבואנים, במפיצי ובנציגים המורשים וכלה במשתמשים. דרישות אלו נגזרות מדרישות סטנדרט המינימום המשפטי שפורטו לעיל.[101]

כמו כן, כתנאי לשיווק מערכת הבינה המלאכותית בסיכון גבוה באיחוד האירופי, עליהם לבצע בחינת תאימות (conformity assessment), במטרה להבטיח שהמערכת עומדת בדרישות הצעת חוק ה־AI. עוד מוטלת עליהם החובה להחזיק במערכת לניהול איכות (quality management system) ובמערכת לניטור פעולת מערכת הבינה המלאכותית בסיכון גבוה. מטרת מערכות אלו להבטיח את הציות לדרישות הצעת חוק ה־AI ולפקח עליו. לצד מערכות אלו, ספקים או יצרני מוצר אשר מוטמעת בו מערכת בינה מלאכותית בסיכון גבוה נדרשים לקבוע מנגנון לדיווח לרשויות המתאימות על תקלות חמורות בפעולתה של המערכת המוטמעת. כמו כן, עם היוודע לסַפָּק שמערכת הבינה המלאכותית בסיכון גבוה ששיווק אינה עומדת בדרישה מדרישות חוק ה־AI,

99 **שם**, ס' 13.

100 **שם**, ס' 14.

101 **שם**, Title III, Chapter 3.

עליו לפעול מייד לתיקון היעדר הציות, להפסקת פעולת המערכת או לאיסופה מהלקוחות.[102]

יבואן או מפיץ של מערכת בינה מלאכותית בסיכון גבוה חייבים לוודא שהמערכת עברה הערכת התאמה לדרישות חוק ה־AI לפני שיווקה בשוק, שספק המערכת סיפק את התיעוד הטכני הנדרש ושהמערכת משווקת בצירוף התיעוד והנחיות השימוש המתאימות.[103]

על משתמש במערכת בינה מלאכותית בסיכון גבוה החובה לפעול בהתאם להוראות הנלוות למערכת. כמו כן, אם המשתמש הוא השולט בנתוני הקלט שבהם משתמשת המערכת, עליו להבטיח שהנתונים יהיו רלוונטיים בהתחשב במטרה המיועדת של המערכת. ניתן לראות בכך התחייבות לפעול בהתאם לעקרון צמידות המטרה ולהימנע מאיסוף מידע שאינו נחוץ לשם הגשמתה. כן מוטלת על המשתמש החובה לנטר את פעילות המערכת וליידע את הספק או את המפיץ אם יש לו סיבה להאמין ששימוש בהתאם להוראות עלול להוביל לסיכון לבריאות, לביטחון או לזכויות יסוד של האנשים הרלוונטיים, או כאשר זיהה התרחשות של אירוע חמור או תקלה שיכולים לפגוע בזכויות יסוד. כן מחויבים המשתמשים במערכות בינה מלאכותית בסיכון גבוה לשמור את תיעוד האירועים שהתרחשו במהלך הפעילות השגרתית של המערכת.[104]

עוד מרחיב חוק ה־AI את תחולת החובות המוטלות על ספק מערכת בינה מלאכותית בסיכון גבוה וקובע כי אלו יחולו גם על מפיץ, על יבואן, על משתמש או על כל צד שלישי שנכנס בנעליו של הספק, בהתקיים אחת הנסיבות האלה:

(**א**) האדם החדיר לשוק מערכת בינה מלאכותית בסיכון גבוה תחת שמו או סימן מסחרי שלו.

(**ב**) האדם שינה את המטרה המיועדת של מערכת בינה מלאכותית בסיכון גבוה הקיימת כבר בשוק.

102 **שם**, ס' 16–25.

103 **שם**, ס' 26–27.

104 **שם**, ס' 29.

(**ג**) האדם שינה באופן ממשי את מערכת הבינה המלאכותית בסיכון גבוה.[105]

חוק ה־AI מחייב גם הטמעה של מערכת לניהול סיכונים לאורך כל חיי מערכת הבינה המלאכותית בסיכון גבוה. על המערכת לזהות ולנתח סיכונים ידועים וצפויים הקשורים במערכת הבינה המלאכותית בסיכון גבוה, להעריך את הסיכונים שעלולים להיגרם בעת שהיא משמשת למטרותיה המוגדרות, וכן מתוך התחשבות בשימוש לרעה שסביר לצפותו, להעריך סיכונים אפשריים נוספים בהתחשב בניתוח המידע שנאסף מניטור השימוש במערכת הבינה המלאכותית בסיכון גבוה לאחר שיווקה ולאמץ אמצעים מתאימים לניהול הסיכונים.[106] לאחר שיווקן של המערכות בשוק האירופי נתונות מערכות הבינה המלאכותית בסיכון גבוה לפיקוח מצד כל אחת מרשויות הפיקוח הלאומיות המדינתיות (market surveillance authorities). מטרת הפיקוח היא להבטיח את המשך עמידתן של המערכות בדרישות החוק.[107] חוק ה־AI אף מחייב את המדינות החברות להטיל סנקציות בגין הפרת החובות הקבועות בה וכן קובעת רף מרבי לקנסות מִנהליים בגין הפרת החובות הקבועות בה.[108]

1.4.3. ישראל

1.4.3.3. זכות העובד לפרטיות: פסיקות בתי המשפט

פסק הדין המוביל בישראל בנושא גבולותיה של זכות העובד לפרטיות ניתן על ידי בית הדין הארצי לעבודה בשנת 2011 בפרשת **איסקוב**.[109] באותה פרשה הכיר בית הדין הארצי בזכות המעסיק, הנגזרת מהזכות החוקתית לקניין

105 **שם**, ס' 28.

106 **שם**, ס' 9.

107 **שם**, ס' 49, 19, 65–66.

108 **שם**, ס' 71.

109 ע"ע (ארצי) 8/90 **טלי איסקוב ענבר נ' מדינת ישראל** (פורסם בנבו, 2011), עמ' 10–14 (להלן: פרשת **איסקוב**). באותה פרשה טענה העובדת לפיטורים שלא כדין מפני שהמעסיק הסתמך על תכתובת דוא"ל שמצא בתיבת דוא"ל חיצונית של העובדת, ולפיה חיפשה העובדת עבודה אחרת בעת שהעסיקה עדיין.

ולחופש עיסוק, לנהל את מפעלו כרצונו בהתאם לפררוגטיבה הניהולית שלו. כנגזרת מזכותו זו, למעסיק נתונה גם הזכות לקבוע את הכללים אשר יחולו על השימוש שעושה עובד בכלי העבודה שהמעסיק נותן בידיו, לרבות אמצעי תקשורת טכנולוגיים. כן רשאי המעסיק לנהל מעקב, לרבות מעקב אלקטרוני, אחר השימוש שעושה העובד במחשב במקום העבודה ובמסגרתו.[110] עם זאת, לצד ההכרה בזכותו זו של המעסיק במסגרת הפררוגטיבה הניהולית שלו, הכיר בית הדין הארצי לעבודה גם בזכותו החוקתית של העובד לפרטיות, המשולה לענגת מרחב פרטי המלווה את העובד כל העת. נפסק כי היקפה של זכות העובד לפרטיות משתנה בהתאם לציפייתו הסבירה של העובד לפרטיות. בעלותו של המעסיק במרחב הפיזי של מקום העבודה ובמרחב הדיגיטלי שבו משתמש העובד אינה מתירה לו לפגוע בזכות העובד לפרטיות במקום העבודה. זכותו זו של העובד כוללת גם את פעולותיו האישיות של העובד בתיבת הדוא"ל שהוקצתה לו במקום העבודה. פערי הכוחות המובָנים ביחסי עובד ומעסיק, שהותו של העובד במקום העבודה במרבית שעות היממה, "עירוב התחומים וטשטוש האבחנה, ההולך ופושט, בין חיי העובד בעבודה ומחוצה לה" וטיב יחסי עבודה המושתתים על אמון הדדי ועל תפקוד העובד במסגרתם – מחייבים, לדעת בית הדין, הגנה על זכות העובד לפרטיות.[111]

יתרה מכך, בית הדין הארצי קבע כי הערך החוקתי האובייקטיבי של הזכות לפרטיות ומהותם של יחסי עבודה המבוססים על אמון, על הגינות ועל חובות הדדיות ומוגברות לתום לב – מחייבים מתן פרשנות מצומצמת להיקף ההגנות המוענקות בחוק הגנת הפרטיות לפוגע בזכות לפרטיות, לרבות ההגנה שלפיה נעשתה הפגיעה בפרטיות למען הגנה על עניין אישי כָּשֵׁר של הפוגע, המעסיק.[112]

עם זאת, בית הדין בפרשת **איסקוב** הכיר בכך שככל זכות יסוד גם הזכות לפרטיות אינה מוחלטת ויש לאזנה מול זכותו החוקתית של המעסיק לקניין

110 דב"ע 3-223 **פלסטין פוסט בע"מ נ' יחיאל**, פד"ע כז 436 (1994); ע"ע (ארצי) 44776-05-16 **סירטו נ' הפניקס קרנות פנסיה מאוזנות ווזיקות בע"מ** (פורסם בנבו, 2018).

111 פרשת **איסקוב**, **לעיל** ה"ש 109, עמ' 18, 47.

112 ס' 18 לחוק הגנת הפרטיות; פרשת **איסקוב**, **לעיל** ה"ש 109, עמ' 18.

ומול הפררוגטיבה הניהולית שלו במקום העבודה. איזון זה צריך להיעשות מתוך התחשבות באופי העבודה וטיבה, בדרישות התפקיד ומהותו, בסביבת העבודה, במדיניות הכללית במקום העבודה ובצורך בהגנה מפני עבירות ונזקים מצידו של העובד.[113] לפיכך, נפסק שפגיעה בזכות יסוד החוקתית לפרטיות, כבכל זכות חוקתית אחרת, צריכה לעמוד בדרישות הסבירות, המידתיות, תום הלב, השקיפות, ההגינות וצמידות המטרה. בהתאם לכללים אלו הבחין בית הדין הארצי בפרשת **איסקוב** בין שני מרחבים דיגיטליים: הראשון, המרחב הדיגיטלי העסקי – תיבת דוא"ל המסופקת לעובד על ידי המעסיק; השני, המרחב הדיגיטלי האישי והפרטי – תיבת דוא"ל חיצונית פרטית של העובד. לגבי כל אחר ממרחבים דיגיטליים אלו קבע בית הדין הארצי תנאים שונים לפגיעה בפרטיות העובד.

פגיעה בפרטיות העובד על ידי חדירה לתכתובת דוא"ל שהוא מנהל במרחב הדיגיטלי שמספק לו המעסיק, דהיינו תיבת דוא"ל המסופקת לעובד על ידי המעסיק, תותר בהתקיים התנאים המצטברים האלה:

(**1**) **נסיבות מיוחדות**. קיומן של נסיבות מוגבלות ויוצאות דופן שבהן ההגנה על אינטרסים לגיטימיים של המעסיק מצדיקה פגיעה בפרטיותו של העובד.

(**2**) **חשש**. קיים חשש כבד לפעילות בלתי חוקית מצד העובד.[114]

(**3**) **שקיפות ויידוע**. המעסיק קבע, טרם התחלת המעקב, מדיניות וקוד התנהגות ברורים בנוגע לשימוש במרחב הדיגיטלי שהוא מספק ויידע את העובד על אודותיהם. בית הדין הארצי לעבודה ציין שראוי שמדיניות זו תיקבע תוך כדי שיתוף נציגות העובדים או ארגוני העובדים והיוועצות עימם במטרה לגבש מדיניות מוסכמת. עוד הציע בית הדין למנות נאמני פרטיות בטכנולוגיות מידע במקום העבודה, כדי לעודד את הטמעת מדיניות המעסיק בנושא. במסגרת מדיניות זו על המעסיק להבחין בין שימושים לצורכי עבודה לבין שימושים לצרכים פרטיים, שאותם רשאי העובד לבצע באמצעות המחשב שניתן לו במקום העבודה. כך, למשל, מעסיק רשאי לקבוע שתיבת הדוא"ל

113 ס' 18 לחוק הגנת הפרטיות; פרשת **איסקוב**, **לעיל** ה"ש 109, עמ' 22–23.

114 **שם**, עמ' 27–28.

שהוא מקצה לעובד יכולה לשמש אך ורק לצורכי העבודה ואין הוא מתיר לעובד לנצלה לצרכיו הפרטיים. במצב זה רשאי המעסיק גם לבצע מעקב אחר נתוני התקשורת ותוכנה של תכתובות הדוא"ל ולגבותם, ובלבד שיידע את העובד במפורש ובבירור במדיניות זו ועמד בחובות הנוספות המפורטות לעיל. אי־ציות המעסיק לעקרון השקיפות, כלומר אי־הבאה לידיעת העובד ולהסכמתו מדעת ומרצון של מדיניות המעסיק בנוגע לשימוש במרחב הדיגיטלי או אי־הנהגת מדיניות ברורה האוסרת שימוש במרחב הדיגיטלי לצרכים פרטיים מקימות לעובד ציפייה סבירה לפרטיות בשימוש במרחב הדיגיטלי של המעסיק, לרבות לצרכיו הפרטיים. במקרה כזה אין המעסיק רשאי לנהל מעקב אחר תכתובת הדוא"ל של העובד או לחדור לתוכנן, כל עוד העובד משתמש בטכנולוגיה לצרכיו הפרטיים בתום לב ובלי לפגוע בעבודתו ובצורכי מקום העבודה.[115]

(**4**) **לגיטימיות**. מטרת המעקב אחר נתוני תקשורת ותוכנה והנסיבות שבהן רשאי המעסיק לעשות שימוש במידע שהפיק מחדירתו לתכתובת דוא"ל של עובד כפופות לעקרון הלגיטימיות, אשר מחייב שאיסוף המידע במסגרת המעקב והשימוש בו ייעשו אך ורק למטרות חיוניות למקום העבודה. לא ייתכן ביצוע מעקב לשם השגת מטרה כוללנית, שאין בינה לבין האינטרסים הלגיטימיים של מקום העבודה שום קשר. כן לא ייתכן מעקב ממניעים פסולים או לא מוגדרים.[116]

(**5**) **מידתיות**. על המעסיק לבחון טכנולוגיות חלופיות למעקב הפוגעות במידה הפחותה ביותר בזכות העובד לפרטיות. אם לא מצא המעסיק חלופות ראויות, על המעקב להיעשות באופן המאזן בין התועלת שבהגשמת המטרה הראויה שלו לבין הנזק והפגיעה בזכות העובד לפרטיות בעקבותיו. בין השאר, על המעסיק להימנע מפגיעה בזכות לפרטיות העולה על הנדרש באופן החושף בפניו מידע אישי של העובד שאינו קשור לצורכי העובדה.[117]

115 **שם**, עמ' 28–29, 35–37, 49–50.

116 **שם**, עמ' 30–31.

117 **שם**, עמ' 32–34.

(6) **צמידות מטרה**. המעקב והשימוש בתוצריו נדרשים לעמוד בעקרון צמידות המטרה. כלומר, אין לנהל מעקב או לעשות שימוש בתוצריו מעבר למטרתו הראשונית.[118]

(7) **הסכמה**. קבלת הסכמה מפורשת, מדעת ומרצון חופשי של העובד לקיום פעולות מעקב וחדירה לתיבת דוא"ל שהֻקצה המעסיק לשימושו האישי של העובד. הסכמה כאמור תהיה תקפה רק אם קיים המעסיק את תנאי הסף המצטברים המנויים לעיל.

הסכמת העובד מורכבת משני ראשים: (1) הסכמה כללית למדיניות המעקב שהמעסיק הציג בפניו; (2) כאשר מדובר בחדירה למרחב הדיגיטלי שמספק המעסיק לעובד אך הוא התיר לו לעשות בו גם פעולות לצרכים אישיים, בנסיבות פסק הדין הכוונה היא לחדירה לתיבת דוא"ל שהוגדרה מלכתחילה תיבת דוא"ל מעורבת שבה רשאי העובד לעשות שימוש לצורכי העבודה ולצרכים אישיים, נדרשת הסכמתו הספציפית של העובד לכל פגיעה בפרטיות. כאשר מדובר בחדירה למרחב הדיגיטלי שהעמיד המעסיק לרשות העובד ושהוגדר מראש לצורכי עבודה בלבד, לא נדרשת הסכמת העובד לפגיעה בפרטיות. כאשר מדובר בחדירה למרחב הדיגיטלי שהעמיד המעסיק לרשות העובד ושהוגדר מראש לצרכים פרטיים בלבד, בנסיבות פסק הדין הכוונה היא לתיבת דוא"ל שמספק המעסיק לעובד אך הוגדרה מראש אישית בלבד, נדרשת הסכמה ספציפית, מפורשת, מדעת ומרצון חופשי של העובד לכל פעולה שבכוונת המעסיק לנקוט, לרבות מעקב. הסכמת העובד לניטור אוטומטי מחשש לווירוסים אינה שקולה להסכמה למעקב שמטרתו איסוף נתוני תקשורת ותוכן.[119]

אם מתקיימים כל התנאים המפורטים לעיל, למעט הסכמת העובד, על המעסיק לפנות לבית הדין האזורי לעבודה בבקשה לסעד שיתיר לו חדירה לתכתובת הדוא"ל של העובד.[120]

118 **שם**, עמ' 34–35.

119 **שם**, עמ' 39–40, 53–54.

120 **שם**, עמ' 55.

פגיעה בפרטיות העובד על ידי חדירה לתכתובת דוא"ל שהוא מנהל במרחב הדיגיטלי הפרטי שלו, כלומר תיבת דוא"ל חיצונית ופרטית של העובד, מחייבת צו בית משפט לחיפוש ולתפיסה של ראיות פוטנציאליות, מסוג צו אנטון פילר.[121] צו כזה יינתן בנסיבות חריגות ביותר בהתקיים התנאים המצטברים האלה:

(**1**) קיומן של נסיבות חריגות.

(**2**) על המעסיק מוטל נטל מוגבר להוכיח לכאורה את טיב העילה ואת סיכויי התביעה.

(**3**) על המעסיק לבסס חשש ממשי סביר או חשש ברמה של ודאות קרובה, שהנכסים הדרושים לבירור התובענה ונמצאים בחזקתו של העובד, ייעלמו או יושמדו.

(**4**) על המעסיק לבסס טענה ולפיה העלמת הנכסים שעלולה להתרחש אם לא יקבל צו כמבוקשו, תכביד באופן ממשי על בירור ההליך העיקרי באופן שיסב לו נזק חמור או שקרוב לוודאי כי בירור התביעה יסוכל.[122]

כן הבהיר בית המשפט בפרשת **איסקוב** שהחיוב בקבלת צו בית משפט יעמוד בעינו אף אם התיר המעסיק לעובד להשתמש במרחב הפיזי והדיגיטלי של מקום העבודה כדי לגשת למרחב הדיגיטלי הפרטי של העובד. כמו כן נפסק כי הסכמתו של עובד לחדירה של המעסיק לתכתובת דוא"ל האישית שניהל בתיבת דוא"ל חיצונית ופרטית אינה תקפה.[123]

במרוצת השנים מאז פסיקת בית הדין הארצי לעבודה בפרשת **איסקוב**, הוספו כמה סייגים לתנאים שנקבעו בה לעניין פגיעה בפרטיות העובד. כך, בפרשת **עיריית קלנסווה** בחן בית הדין הארצי לעבודה את דרישת המעסיק מהעובד לחתום על כרטיס נוכחות ביומטרי והוסיף לעקרונות שלפיהם נבחנת חוקתיות הפגיעה בפרטיות העובד גם התחשבות באופי העבודה וטיבה, דרישות התפקיד

121 צו מסוג אנטון פילר הוא צו לתפיסת חומרים וראיות בהליך אזרחי.

122 **שם**, עמ' 60.

123 **שם**, עמ' 56–58.

ומהותו, סביבת העבודה, המדיניות הכללית במקום העבודה והצורך בהגנה מפני עבירות ונזקים מצד העובד.[124]

בפרשת **זינגר**, כחמש שנים לאחר פרשת **איסקוב**, דובר בחדירה לתכתובת דוא"ל של עובד באמצעות תיבת דוא"ל חיצונית פרטית שלו, שהושארה פתוחה ונגישה על מחשב של המעסיק במקום העבודה. כלומר דובר בחדירה למרחב הדיגיטלי האישי של העובד שהיה נגיש באמצעות המרחב הפיזי והדיגיטלי של המעסיק. בית המשפט העליון לא התמקד בתנאים שצריכים לחול לגבי הפגיעה בפרטיות בכל אחד מהמרחבים, אלא בחר להבחין בין מעקב יזום שמעסיק עורך אחר עובדיו לבין חשיפה מקרית ובתום לב של תכתובת דוא"ל פרטית של עובד. נפסק שיש לבחון כל מקרה לגופו ולהכריע באיזון שבין זכות העובד לפרטיות לבין האינטרס הלגיטימי של המעסיק בהתאם למידת הפגיעה בפרטיות העובד ולמידת הדחיפות שיש בהגנה על האינטרס הלגיטימי של המעסיק. בנסיבות אותה פרשה נפסק שכאשר חשיפה מקרית, סבילה ובתום לב של תכתובת דוא"ל בתיבה חיצונית פרטית של העובד מובילה לחשד שהוא גזל מהמעסיק סכום כסף, נסוגה זכותו של העובד לפרטיות מפני האינטרס הלגיטימי של המעסיק, והאחרון רשאי להשתמש בתכתובת הדוא"ל שנחשף אליה במקרה כראיה לצורך הגנה על עניין אישי כשר שלו, ללא צו שיפוטי.[125] בפסיקה זו ייחס בית המשפט העליון חשיבות רבה לנסיבות המעקב (שנעשה בתום לב ובאופן מקרי), ולחשש מפני עבירה או מפני פגיעה באינטרס הלגיטימי של המעסיק, מתוך התעלמות מהעובדה שדובר בחדירה למרחב דיגיטלי פרטי של העובד, ומההבחנה שעשה בנושא בית הדין הארצי לעבודה בפרשת **איסקוב**.

בפרשת **אקספו** פנה מעסיק לבית הדין האזורי לעבודה בתל אביב בבקשה להתיר לו לנטר את תיבת הדואר האלקטרוני המקצועית, שהעמיד לרשות עובד לשעבר במהלך העסקתו של האחרון בחברה, ולעיין בהודעות הדוא"ל. המעסיק נימק את בקשתו בחשד שהעובד גזל ממנו הכנסה. חשד זה התעורר מקריאת

124 עס"ק (ארצי) 7541-04-14 **הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי נ' עיריית קלנסווה** (פורסם בנבו, 2017) (להלן: פרשת **קלנסווה**).

125 רע"א 2552/16 **זינגר נ' יהב חמיאס טכנולוגיות (1990) בע"מ ואח'** (פורסם בנבו, 2016) (להלן: פרשת **זינגר**).

תכתובת דוא"ל, שמוענה לעובד אך לאחר עזיבתו הועברה אוטומטית לתיבת הדוא"ל של מחליפו בחברה, וממנה נלמד שהעובד קיבל תשלום עבור עבודה פרטית שביצע עבור חברה אחרת בעת שעדיין עבד אצל המעסיק. בית הדין האזורי הבהיר שלעובד, ואף לעובד לשעבר, יש ציפייה סבירה לפרטיות גם ביחס למרחב הדיגיטלי העסקי, בנסיבות המקרה – תיבת דוא"ל מקצועית המוקנית לו לשם עבודתו על ידי המעסיק. אולם, בהתאם לפסיקת בית המשפט העליון בפרשת **זינגר**, בעת בחינת מידת הפגיעה בפרטיות העובד ותום ליבו של המעסיק יש לתת את הדעת לנסיבות המקרה כגון הצורך במעקב ומטרתו וכן תפקידו של העובד. מאחר שמטרת הפגיעה בפרטיות העובד, או עובד לשעבר, היא הגנה על אינטרס לגיטימי של המעסיק ומאחר שבנסיבות פסק הדין דובר בעובד שכיהן בתפקיד בכיר בחברה ועל כן הנזק שהוא עשוי להסב לחברה גדול, והוכח קיומה של ראשית ראיה לחשד לגזל מצד העובד, הרי שאין לחייב את המעסיק בקבלת הסכמת העובד למעקב או במיצוי החלופות שפגיעתן בפרטיות העובד פחותה. לא כך הדבר כאשר המעסיק מבקש לקיים מעקב מראש לצורך אגירת מידע אישי על העובד שאולי ישמש אותו בבוא העת. במקרה כזה חלה הלכת **איסקוב** במלואה, ועל המעסיק לקבל את הסכמת העובד ולמצות קודם את כלל האמצעים שפגיעתם בפרטיות העובד פחותה או לפנות לקבלת צו שיפוטי.[126]

בפרשת **אופטיקה הלפרין** בחן בית המשפט השלום בהרצלייה את מידת הפגיעה בפרטיות העובד בעקבות מעקב שניהלה אחריו המעסיקה, אופטיקה הלפרין. המעקב בוצע באמצעות "מערכת ניהול עובדים מבוסס מיקום" שהותקנה במכשיר הטלפון הנייד שהועמד לרשותו של כל עובד, שהוצמד לו רכב מטעם המעסיקה. השליטה הבלעדית במערכת הייתה בידי המעסיקה. כלומר, דובר בחדירה לפרטיות העובד במרחבים הדיגיטלי והפיזי שהקנתה לו המעסיקה – מכשיר הטלפון הנייד והרכב – שברור שהעובד עשה ורשאי היה לעשות באותם המרחבים גם שימושים אישיים פרטיים. מערכת ניהול העובדים הוגדרה כך שהמעקב אחר מיקום העובד לפי מכשיר הטלפון הנייד שהעניקה לו המעסיקה ייעשה במהלך שעות העבודה בלבד, כלומר בעת שהמרחב הפיזי והדיגיטלי היו אמורים לשמש את העובד למטרות עבודה. המידע שהועבר למעסיקה התמצה בהודעה, שנשלחה בזמן אמת למנהלו של העובד בחברה, כל אימת שהעובד

126 סע"ש (ת"א) 18279-06-16 **אקספו ניהול בע"מ נ' משה כהן** (פורסם בנבו, 2017).

התקרב לאחד מסניפי רשת המעסיקה. המידע לא נשמר במערכת. בית משפט השלום קבע שהמידע שנאסף באמצעות המערכת הוא טכני בעיקרו, וממילא לא נשמר במערכת ולא נמסר לצד שלישי. עוד נקבע כי תכלית המעקב היא ייעול ושיפור השירות שמעניקה המעסיקה ללקוחותיה, ועל כן מדובר בתכלית לגיטימית. לפיכך, נפסק שהפגיעה בפרטיות העובד היא מזערית ולא נדרשת הסכמת העובד לפגיעה אלא די בהודעה מראש. אף שהודעה זו לא ניתנה לתובע, הסיק בית משפט השלום מהנסיבות כי התובע היה מודע לקיומה של מערכת המעקב במהלך העסקתו, ודחה לפיכך את תביעתו לפגיעה בפרטיותו שלא כדין.[127]

לאחר סיום כתיבת מחקר זה התקבל בבית הדין הארצי לעבודה פסק הדין בפרשת **אלקנר** המציג מתווה תלת־שלבי לבחינת החוקיות של פגיעה בפרטיות העובד.[128] לפי מתווה זה יש לבחון תחילה את תכלית הפגיעה בפרטיות. אם מדובר בתכלית לגיטימית, יש להמשיך ולבחון את מידתיות הפגיעה. במסגרת בחינת המידתיות יובאו בחשבון שיקולים כגון המרחב שבו מבוצעת הפגיעה בפרטיות, סוג המידע הנאסף, מאפייניו האישיים של העובד והתנהלות המעסיק בסמוך לפגיעה בפרטיות. בשלב השלישי והאחרון תיבחן מידת השקיפות שנוקט המעסיק והסכמתו של העובד. בהקשר זה מציין בית הדין כי ככל שהפגיעה בפרטיות מידתית ומזערית, תידרש הסכמה חלשה יותר, אם בכלל. ולהפך, ככל שהפגיעה בפרטיות העובד חמורה יותר, תידרש הסכמה מפורשת, ספציפית, מדעת ומרצון חופשי. בית הדין אף מציין כי יהיו מצבים שבהם הפגיעה בפרטיות תהא חמורה כל כך שלא ניתן יהיה להכשירה באמצעות הסכמת העובד.

127 ת"א (שלום הרצליה) 28882-50-88 **ביידר נ' אופטיקה הלפרין בע"מ ואח'** (פורסם בנבו, 2013).

128 ע"ע 41179-01-24 **ד"ר מרק פרידמן בע"מ נ' אלקנר ואח'** (פורסם בנבו, 26.3.2025) (להלן: פרשת **אלקנר**).

1.4.3.4. זכות העובד לפרטיות: הנחיות הרשות להגנת הפרטיות

1.4.3.4.1. שימוש במצלמות בהקשר של יחסי עבודה

לצד פסיקות בתי המשפט, ניתן ללמוד על היקפה של זכות העובד לפרטיות גם מעמדת הרשות להגנת הפרטיות (להלן: הרשות או הרשות להגנת הפרטיות) בנושא. באוקטובר 2017 פרסמה הרשות הנחיה בנוגע ל"שימוש במצלמות בהקשר של יחסי עבודה, בין במרחב הציבורי ובין במקומות עבודה אחרים, שאינם 'רשות הרבים' במובנה הקלאסי ואינם פתוחים לציבור הרחב".[129] ההנחיה פורסמה לפני מגפת הקורונה, שהגבירה את השימוש בטכנולוגיות למעקב אחר עובדים במתווה העבודה ההיברידי, ועל כן מתמקדת בפגיעה בפרטיות העובד הנגרמת ממצלמות המותקנות במרחבים פיזיים שבבעלות המעסיק: עמדת העבודה האישית של העובד, אזורי מנוחה, אזורים "ציבוריים" ואזורים הפתוחים לקבלת קהל.[130] הנחת המוצא של ההנחיה היא שהעובד מבלה את מרבית שעות היום במקום העבודה. משום כך, מצלמת וידאו המותקנת במקום העבודה עשויה לתעד "באופן מקיף ומתמשך את כלל התנהלותו של העובד במהלך יום העבודה ולא רק את פעילותו המקצועית". על כן עלול התיעוד לכלול "מידע רגיש ומקיף במיוחד, ולפגוע באורח חמור בפעילות הפרטית, המהווה חלק מהמרחב הפרטי המלווה את העובדים גם במקום העבודה, וזאת מבלי שיש בידיהם יכולת להשפיע באופן משמעותי על מיקום המצלמות או על מתכונת הפעלתן".[131] בכך משקפת ההנחיה את ההבנה שנוכח שעות העבודה הרבות שהעובד מבלה במרחב הפיזי שבבעלות המעסיק, הוא עשוי לשמש אותו גם לשם ביצוע פעולות אישיות ופרטיות. יתרה מכך, בהערת שוליים מתייחסת הרשות לשימוש בטכנולוגיות מעקב במרחב הדיגיטלי של המעסיק הנגיש מהמרחב הפיזי האישי של העובד וקובעת כי צילום עובד בעמדת עבודה מרוחקת, לרבות

129 הרשות להגנת הפרטיות, מדינת ישראל, משרד המשפטים **הנחיית רשם מאגרי מידע מס' 5/17 שימוש במצלמות מעקב במקום העבודה במסגרת יחסי עבודה** (17.10.2017), ס' 2.

130 **שם**, ס' 3.

131 **שם**, ס' 4.

בביתו, נחשב צילום ב"רשות היחיד" שבה יש לעובד ציפייה סבירה לפרטיות.[132] אומנם מדובר בהערת שוליים, ולפיכך המשקל שיש לייחס לה אינו ברור, אולם יש בה כדי להצביע על עמדה המייחסת עננת פרטיות רחבה יותר לעובד בעת עבודה במרחב הפיזי האישי שלו, אף אם העבודה והמעקב מבוצעים שניהם במרחב הדיגיטלי של המעסיק.

לפי ההנחיה, שימוש בטכנולוגיות מעקב במקום העבודה, כלומר במרחב הפיזי של המעסיק, חייב להיעשות בהתאם לדרישות האלה במצטבר:[133]

(**1**) **לגיטימיות**. המעסיק רשאי להתקין ולהשתמש בטכנולוגיות מעקב במקום העבודה, תוך כדי איסוף מידע אישי על אודות עובדיו ועיבודו, רק למטרות מוגדרות וחיוניות למקום העבודה, העולות בקנה אחד עם התכלית העסקית של המעסיק, דרושות לפי חוק או מחויבות על ידי רשות או גורם פיקוח מוסמך. הרשות מונה בהנחיה מגוון תכליות, אשר עשויות לעמוד בעקרון הלגיטימיות: הגנה על ביטחון הנוכחים בעסק, שמירה על תכולת העסק והרכוש שבו, אבטחת מידע אישי רגיש הנדרשת לפי חוק, וכן ככלי לניהול העובדים ולפיקוח על המשמעת במקום העבודה ואיכות השירות המסופקת על ידי העובדים ללקוחות.[134]

(**2**) **מידתיות**. מידתיות הפגיעה בפרטיות העובד עקב שימוש בטכנולוגיות מעקב תיבחן בהתחשב בתכלית השימוש במעקב: מיקום התקנת המצלמה, שטח הכיסוי שלה, מספר המצלמות המוצבות, זמני הצילום, רזולוציית התמונה, משך שמירת התיעוד, הציפייה הסבירה של העובד לפרטיות באותו אזור, קיומו של אמצעי חלופי שפגיעתו בפרטיות פחותה להשגת אותה מטרה ומידת השקיפות שבמסגרתה פעל המעסיק. כך, התקנת מצלמה בחלל עבודה סגור לציבור שמתבצעת בו עבודה החורגת מפעילות משרדית שגרתית עשויה להיות מידתית אם היא מותקנת למטרה לגיטימית, כגון שמירת שלום הפועלים המועסקים או לבקרת איכות מוצר רגיש או בעל פוטנציאל נזק המיוצר בו, ובלבד שהתקנת המצלמה היא האמצעי היעיל להבטחת מטרות אלו ואין אמצעי שפגיעתו בזכות לפרטיות פחותה. לעומת זאת, הרשות מתקשה לקבל

132 **שם**, הערת שוליים 26.

133 **שם**, ס' 13.

134 **שם**, ס' 15–16.

את הטענה שלמעסיק אינטרס המצדיק התקנת מצלמות מעקב במשרד ובכל עמדה שבה העבודה היא בגדר פעילות משרדית רגילה, הכוללת הקלדה במחשב או ניהול שיחת טלפון. לשיטתה, התקנת מצלמה במקומות אלו תוביל לפגיעה לא מידתית ולא סבירה בפרטיות העובד: "צילום וידאו קבוע של חדר או עמדת המחשב בה מבצע עובד משרדי את עבודתו, לשם אכיפת כללי משמעת פנימיים כגון משך ההפסקות המותרות או איסור שיחה בטלה עם עמיתיו – פוגע בפרטיותו במידה בלתי מוצדקת העולה על הנדרש". אחד הנימוקים לכך הוא שלדעת הרשות המעקב אינו האמצעי המתאים ביותר להגברת היעילות במקום העבודה או לאכיפת משמעת.

ככלל, לעמדת הרשות, לעובד ציפייה סבירה לפרטיות במרבית ממרחבי העבודה, לרבות "עמדות עבודה בהם שוהה העובד לשם ביצוע עבודתו, ואשר איננו פתוח לכניסה חופשית של הציבור", לרבות "בשינויים המחויבים ... גם עמדות עבודה המרוחקות מהקמפוס הארגוני של המעסיק".[135] אזור מנוחה, כגון מטבחון או כל חלל אחר שאינו זירת ביצוע עבודה ואינו פתוח לקהל הלקוחות, ואשר משמש את העובדים לצורך הפסקה משגרת העבודה, נחשב לדעת הרשות כאזור שבו ציפייתו הסבירה של העובד לפרטיות גבוהה, ועל כן צילום בו יותֵר רק במידה מצומצמת למטרה חיונית מאוד. ציפייתו הסבירה של עובד לפרטיות מגיעה לשיאה בחדר השירותים או במלתחות, ועל כן הצבת מצלמות שם אינה מידתית. לעומת זאת, באזורים ציבוריים, כגון מסדרונות, מבואת הכניסה למשרד או מתחמים הפתוחים לציבור הרחב, אין לעובד ציפייה סבירה לפרטיות, ועל כן הצבת מצלמות בהם מותרת כל עוד מטרתה לגיטימית והיא נעשית בשקיפות ובמידתיות.[136]

(**3**) **שקיפות**. לשיטת הרשות, על המעסיק לגבש מדיניות ברורה ומפורטת בנוגע לאופן השימוש במצלמות המעקב, היקפו ומטרותיו, ולרעננה מעת לעת בהתאם "למגמות המתפתחות בתחום". על המעסיק לפעול לגיבוש מדיניות זו תוך היוועצות, ככל הניתן, עם העובדים או נציגיהם. עוד על המעסיק לוודא שהמדיניות מוצגת באופן קבוע לידיעת העובדים. דרישת השקיפות עומדת בעינה שמדובר באזור שבו יש לעובד ציפייה סבירה לפרטיות ובין שלאו, למשל באזור ציבורי. חריגה מדרישת השקיפות והתקנת מצלמות באזורים שבהם יש

135 **שם**, ס' 29.2 וה"ש 26.

136 **שם**, ס' 29.2–29.4.

לעובד ציפייה סבירה לפרטיות תתאפשר רק בנסיבות יוצאות דופן שקיים בהן חשד מוחשי וממשי לביצוע עבירות פליליות חמורות או התנהגויות אסורות של העובד הגורמות למעסיק נזק כבד, כאשר אין אמצעי אחר למנוע את העבירות, ורק בתנאי שהצילום הוא נקודתי ומוגבל בזמן ובתחום הכיסוי. התקנת מצלמות באזור ציבורי ללא יידוע העובדים תותר אפוא רק אם מסוגל המעסיק להצביע על תכלית חיונית המצדיקה צילום בסתר של העובדים באזור הציבורי, אם הצילום עומד בדרישת המידתיות ואם יידע המעסיק את העובדים על כוונתו זו ושקל את עמדתם בנושא. להסכמת העובד לפגיעה בפרטיותו באמצעות מצלמות במרחב העבודה, אף אם תהא זו הסכמה ספציפית, אין משקל רב בשל פערי הכוחות המובְנים שבין מעסיק לעובד.[137]

(**4**) **צמידות מטרה**. מעסיק רשאי להשתמש בתיעוד ממצלמות שהותקנו במקום עבודה אך ורק למטרה המוגדרת והלגיטימית שלשמה הותקנו, אחרי שעמדה התקנתם בעֶקרון הלגיטימיות ובדרישת המידתיות והשקיפות. כך, למשל, תיעוד ממצלמות שהותקנו למטרת בקרת כניסה למפעל למטרות ביטחוניות או ביטחון העובדים אינו יכול לשמש את המעסיק למטרות ניהול, משמעת או מעקב אחר יעילות העובד. חריגה מעקרון צמידות המטרה תותר רק בהתאם להוראות הדין או בהתאם לדרישת רשות מוסמכת.[138]

בית הדין הארצי לעבודה הטמיע את מתווה זה של הרשות להתקנה של מצלמות במקום העבודה. נפסק כי התקנת מצלמות במגרש החנייה של מקום העבודה והשימוש בתיעודן היו מידתיים ואינם מהווים פגיעה בפרטיות העובדת שכן השימוש שעשה המעסיק במצלמות היה לגיטימי למטרת פיקוח על דיווחי הנוכחות של העובדים, המעסיק פעל בשקיפות מלאה ובתום לב: המצלמות היו גלויות; דבר התקנתן היה ידוע לנציגות העובדים; המעסיק פרסם מראש נוהל שימוש במצלמות לעובדים וכן הציב שלטים המעידים כי המקום מצולם.[139]

137 **שם**, ס' 20–25.

138 **שם**, ס' 26–28.

139 ע"ע (ארצי) 1680/10/22 **כהן נ' אל על נתיבי אויר לישראל בע"מ ואח'**, (8.5.2023).

1.4.3.4.2. מעקב אחר נתוני מיקום

באוגוסט 2021 פרסמה הרשות טיוטת גילוי דעת בדבר מעקב טכנולוגי אחר מיקום עובדים במסגרת יחסי העבודה. גילוי הדעת מציע מתווה דומה לזה שהוצג בהנחיה שעסקה במצלמות במקום העבודה לבחינת חוקיותה של הפגיעה בפרטיות העובד בעקבות מעקב אחר נתוני המיקום שלו. נקודת המוצא של גילוי הדעת היא שנתוני מיקום עשויים לחשוף מידע אישי ורגיש על העובד, נושא המידע, ולמעקב מתמיד אחר מיקומו של עובד יכול להיות אפקט מְמַשטר. לפיכך, הבהירה הרשות כי שימוש בטכנולוגיית מעקב אחר מיקום עובד יכול להיעשות רק לתכלית לגיטימית, ספציפית וחיונית למקום העבודה העומדת במבחן המידתיות. כלומר על המעסיק לבחון את תועלת השימוש בטכנולוגיה למען השגת תכליתו העסקית למול הפגיעה בפרטיות העובד, למצות את אפשרות השימוש באמצעים אחרים שפגיעתם בפרטיות פחותה להשגת אותה התכלית, קודם להטמעת טכנולוגיית המעקב, ולהבטיח שסוג העבודה וטיב תפקידו של העובד מצדיקים איסוף רציף של נתוני המיקום שלו. אם מדובר בעובד המבצע עבודה משרדית רגילה, יתקשה המעסיק, כך לפי הרשות, להצביע על עניין לגיטימי שלו המצדיק את הפגיעה בפרטיותו של העובד. עוד ציינה הרשות כי מידתיות השימוש בטכנולוגיית מעקב תתבטא בצמצום השימוש בה אך ורק לאיסוף מידע הרלוונטי לתכלית הלגיטימית של המעסיק. כך, לדוגמה, טכנולוגיית המעקב תוגבל לאיסוף נתוני מיקום בשעות העבודה בלבד, למעקב אחר הגעתו של העובד למקומות מסוימים הרלוונטיים למעסיק ולא תכלול מעקב רציף אחר מסלול תנועותיו, או תאפשר לעובד להפסיק את המעקב לפרקי זמן שיקבע, למשל כאשר הוא מבקש לבקר במרפאה. אפשרות נוספת היא שמירת הנתונים באופן לא מזוהה ומוצפן ואֵחזורם למידע מזהה רק בהתקיים תנאים המצדיקים זאת. למשל, קיום חשד סביר שהעובד אינו ממלא אחר משימותיו. אם השימוש בטכנולוגיית המעקב נעשה לתכלית לגיטימית, נקודתית וחיונית למעסיק, ועומד בדרישת המידתיות, על המעסיק להבטיח עמידה בדרישות האלה:

(**1**) **צמידות המטרה**. לא יוּתָר שימוש במידע למטרה החורגת מן המטרה הראשונית שלשמה נאסף.

(**2**) **שקיפות**. קביעת מדיניות ברורה ושקיפות מלאה כלפי העובד.

(**3**) **הסכמת העובד**. אם מדובר במעקב אחר העובד במהלך כל שעות עבודתו, גם מחוץ לחצריו של המעסיק, יש לקבל את הסכמתו המפורשת של העובד למעקב.

(**4**) **מידתיות ונחיצות**. על המעסיק להימנע מאיסוף נתוני המיקום מחוץ לשעות העבודה המוגדרות.

(**5**) **אבטחת מידע** על המעסיק להבטיח את אבטחת המידע הראויה והנאותה.[140]

1.4.3.4.3. מעקב אחר עובדים בעבודה מרחוק

במאי 2023 פרסמה הרשות מסמך מפורט העוסק בהיבטי פרטיות במעקב אחר מועסקים בעבודה מרחוק. המסמך מתבסס, בין השאר, על הנחיית הרשות בנוגע למצלמות במקום העבודה ומפרש אותה בהקשר של עבודה מרחוק.

הנחת המוצא של הרשות בבחינת השימוש בטכנולוגיות מעקב בעת עבודה מרחוק היא שמדובר בחדירה ממשית ועמוקה למרחב הפרטי של האדם, שאינה מתקיימת בדרך כלל במסגרת יחסי עובד-מעסיק במקום העבודה, ויכולה להוביל למגוון פגיעות אפשריות בזכות לפרטיות. למשל, שימוש בטכנולוגיות מעקב בעת עבודה מרחוק עלול להביא לאיסוף ולשמירה של מידע אישי על העובד ועל בני ביתו בחשאי, בלי שהעובד מודע לכך וממילא לא הסכים לכך. המידע עלול לכלול מידע רגיש שספק אם היה נחשף לעיני המעסיק לולא היה העובד מועסק מרחוק וכן סביר שאינו נדרש או רלוונטי למטרת הפיקוח על משימותיו של העובד. למשל, מעקב באמצעות מצלמת הרשת או המיקרופון המותקנים במכשיר הטלפון החכם של העובד או במחשבו עלולים לחשוף מידע רגיש על העובד או על בני ביתו, על מצבם הבריאותי או הנפשי וכן על היחסים הפנים־משפחתיים. צילום מסך המחשב של העובד או מעקב אחר הרגלי הגלישה שלו עלולים לחשוף מידע אישי רגיש, לרבות מידע פיננסי, מידע רפואי או מידע אינטימי הנוגע לצנעת חייו. זאת ועוד, איסוף המידע האישי הרב ושמירתו מגבירים את הסיכון לדלף מידע ואף עלולים לשמש לרעה בידי המעסיק. לדוגמה, מעסיק הנחשף באמצעות המעקב למצבה הרפואי של עובדת הנמצאת בשלבי היריון ראשוניים, או מפלה עובד על בסיס עמדתו הפוליטית כפי שנחשפה משיח שקיים העובד עם בני משפחתו בביתו. ולבסוף, מעקב רציף

140 הרשות להגנת הפרטיות **גילוי דעת: איסוף נתוני מיקום של עובדים באמצעות אפליקציות ייעודיות ומערכות איכון ברכב** (טיוטה להערות הציבור, 31.08.2021).

אחר העובד בביתו, החל בצילום העובד והמרחב הביתי שלו, דרך האזנה והקלטה של המתרחש בביתו במהלך שעות היום, וכלה במעקב אחר תנועות עיניו כאשר הוא יושב מול המחשב, עשוי להביא לפגיעה בתחושת השליטה של האדם על חייו ולעורר תחושת משטור תמידית. עובד המודע להיותו נתון במעקב חודרני כל כך על ידי מעסיקו עלול להימנע מלבצע פעולות לגיטימיות במהלך עבודתו מביתו, כגון הפסקת שתייה.[141]

הרשות חזרה בהנחיה על הדרישות שהגדירה בעבר לבחינת חוקיותה של פגיעה בפרטיות העובד: מעסיק רשאי להשתמש בטכנולוגיות למעקב אחר עובדיו ועקב כך לפגוע בפרטיותם, ובלבד שהשימוש הוא מידתי וסביר, לצורכי מטרה לגיטימית ובעל זיקה לאינטרסים הלגיטימיים של מקום העבודה, בהתאם לעקרון צמידות המטרה, נעשה בשקיפות אגב יידוע העובדים וקבלת הסכמתם לכך ומתוך הקפדה על כללי אבטחת המידע.[142] בכך נדמה שהרשות מחילה את התנאים שנקבעו בפרשת **איסקוב** לגבי חדירה לפרטיות המתרחשת במרחב הדיגיטלי העסקי (תיבת דוא"ל שמספק המעסיק לעובד לצורכי עבודתו) על חדירה לפרטיות המתרחשת במרחב הפיזי של העובד, באמצעות, כך נראה, המרחב הדיגיטלי העסקי (המחשב שהמעסיק מספק לעובד).

לצד קביעה זו הרשות מציינת שקיימים סוגים של טכנולוגיות מעקב שהשימוש בהן עלול לפגוע קשות בזכות לפרטיות ולעורר חשש ממשי מחריגה מהוראות הדין. עם טכנולוגיות מעקב אלו נמנים: כלי סריקה ופיקוח על אתרי האינטרנט שבהם גולש העובד ועל תוכן הדוא"ל שלו בתיבה שאינה לשימוש מקצועי בלבד; אמצעים לשליטה במצלמות הרשת ובחיישנים לקליטת שמע במכשירים הדיגיטליים של העובד, למטרות צילומו או האזנה לו ולסביבתו; כלים לניטור תנועות העכבר של העובד ואופן השימוש שלו במקלדת; אמצעים לצילום מסך של העובד; אמצעים למעקב אחר תנועת העיניים של העובד בעת השימוש במחשב ולבחינת התכנים בהם העובד צופה בזמן היותו מול המחשב; וכן אמצעים לאיסוף נתוני מיקום של העובד המותקנים ברכבו או במכשיריו הדיגיטליים.[143]

141 הרשות להגנת הפרטיות **היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק** (מאי 2023), עמ' 1, 5–9.

142 **שם**, עמ' 12.

143 **שם**, עמ' 4–3.

מדובר, אם כן, בטכנולוגיות מעקב המאפשרות חדירה הן למרחב הדיגיטלי של העובד (תיבת דוא"ל שאינה לשימוש מקצועי בלבד, תנועות העכבר שלו והקלקות המקלדת שמבצע, תנועות העיניים שלו והתוכן בו הוא צופה על גבי מסך המחשב), והן למרחב הפיזי האישי של העובד (באמצעות מצלמת הרשת, מיקרופון המכשיר וחיישן המיקום שלו). עם זאת, הרשות לא הבחינה בין שני המרחבים הללו וקבעה כלל אחיד, ולפיו השימוש בהן יותֵר רק במקרים חריגים ובכפוף לדרישות האלה:

(**1**) **לגיטימיות**. השימוש בטכנולוגיות המעקב נעשה למען תכלית מקצועית מוגדרת ולגיטימית, בעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה, המצדיקה את השימוש בהן.

(**2**) **מידתיות**. (א) השימוש בטכנולוגיה מותר רק אם אין חלופה אחרת להגשמת התכלית הלגיטימית, שפגיעתה בזכות לפרטיות פחותה. למשל, מעסיק המבקש למנוע גלישה של עובדיו לאתרי אינטרנט מסוימים, עדיף שיעשה שימוש בטכנולוגיות לחסימת גישה ולא בטכנולוגיות מעקב אחר הרגלי הגלישה של העובד; (ב) קיים יחס ראוי בין התועלת שתצמח מהשימוש בטכנולוגיה למול הנזק והפגיעה בזכות העובד ובני ביתו לפרטיות. במסגרת זו על המעסיק לשקול את סוג האמצעי, משך תקופת המעקב, רציפותו, סוג המכשיר שיתבצע באמצעותו המעקב (מחשבו הפרטי של עובד או מחשב שסיפק לו המעסיק). על המעסיק להימנע מלהשתמש בטכנולוגיות המעקב מעבר לשעות שבהן העובד מעמיד את עצמו לרשות המעסיק. בדרישה זו נדמה שיש ניסיון להחיל על המרחב הדיגיטלי של המעסיק, בו מבצע העובד את עבודתו גם כאשר הוא נמצא פיזית בביתו, את המגבלות הקיימות לו היה מדובר במרחב דיגיטלי הנגיש רק במקום העבודה הפיזי; (ג) טכנולוגיית המעקב שבה מבקש המעסיק להשתמש תואמת את תכלית המעקב. למשל, מעסיק המבקש לפקח על היקף שעות העבודה של העובד צריך להשתמש בטכנולוגיות המתאימות למטרה זו, כגון טכנולוגיות המנטרות את שעות ההתחברות של העובד אל המערכת המשרדית וההתנתקות ממנה, ולא בטכנולוגיות שנועדו למטרות אחרות, כגון מעקב אחר יעילותו של העובד במסגרת ניטור הרגלי הגלישה שלו ברשת האינטרנט.

(**3**) **שקיפות כלפי העובד ויידוע העובד**. על המעסיק ליידע את העובד לגבי השימוש בטכנולוגיות המעקב ומטרתו. אם המעסיק מבקש להשתמש בטכנולוגיות מעקב שפגיעתן בפרטיות העובד גבוהה, חובת היידוע אינה

מתמצה ביידוע כללי. על המעסיק לשקף לעובד בכתב בשפה ברורה ופשוטה, בהתאם לשפתו ולמוגבלותו, אם קיימת, את אופן ביצוע המעקב והשימוש במידע שייאסף באמצעותו, לרבות מידע בנוגע לסוג המידע שייאסף, תדירות המעקב ומועדיו וכן היכן יישמר המידע ולכמה זמן. במסגרת חובת השקיפות על המעסיק לקבוע מדיניות ברורה בנוגע לפעולות שלעובד מותר או אסור לעשות באמצעות המחשב וביישומיו בעת עבודה מרחוק. ראוי שמדיניות זו תגובש מתוך היוועצות עם נציגות העובדים ותעוגן בחוזה העבודה ובתקנון הנוהג במקום העבודה.[144]

(**4**) **הסכמת העובד**. נוכח פערי הכוחות המובְנים ביחסי עבודה, יש לדקדק בדרישת ההסכמה ובמידתיות הפגיעה. ככלל, הרשות מבחינה בין מצבים שבהם אין לעובד אפשרות אחרת אלא לעבוד מרחוק, כגון, בתקופת סגרי הקורונה, לבין מצבים שבהם נתונה לעובד הבחירה אם לעבוד ממקום העבודה או מרחוק. במסגרת החלופה הראשונה לא ניתן לתת משקל רב להסכמת העובד, שכן קשה לקבלה כהסכמה חופשית ומרצון נוכח פערי הכוחות בין העובד למעסיק ועל רקע היעדר יכולת בחירה בידי העובד. מבחינת העובד, סירובו למעקב עלול להוביל לפיטוריו. לעומת זאת, בחלופה השנייה שבה נתונה בחירה בידי העובד, תגבר לדעת הרשות הנטייה לראות בהסכמתו למעקב הסכמה תקפה, חופשית ומרצון. בהנחה שקיימת בידי העובד חלופה אמיתית, על מעסיק לקבל הסכמה, במפורש או מכללא על בסיס יידוע ברור ומפורש של העובד, לאיסוף מידע אישי על אודותיו באמצעות טכנולוגיית מעקב. הסכמת העובד אינה יכולה בשום מקרה להכשיר פגיעה שאינה מידתית או שאינה לגיטימית ובעלת זיקה לאינטרסים הלגיטימיים של מקום העבודה, בזכותו לפרטיות. עם זאת, אם השימוש שמבקש המעסיק לעשות בטכנולוגיית מעקב עומד בדרישות הלגיטימיות והמידתיות, אזי אי־הסכמתו של העובד לאיסוף המידע האישי על אודותיו במסגרת זו עשויה להיות בעלת השלכות מבחינת יחסי העבודה. שימוש בטכנולוגיות מעקב שאינו כרוך באיסוף מידע אישי על העובד, לדוגמה ניטור נתוני תקשורת בלבד בתיבת הדואר המקצועית של העובד, המבוצע בהתאם לעקרונות הלגיטימיות והמידתיות, אינו מחייב את הסכמת העובד, אלא די ביידוע שלו בלבד.[145]

144 **שם**, עמ' 12–14.

145 **שם**, עמ' 14–15.

(5) **צמצום מידע עודף**. על המעסיק להימנע ככל הניתן מאיסוף מידע על עובד ומשמירתו, שאינו הכרחי למטרת המעקב או למטרת המאגר שנשמר בו המידע. ככל שמשך זמן שמירת המידע ארוך יותר, כך גדל הסיכון לפגיעה בפרטיות העובד ובני ביתו. לפיכך, לעמדת הרשות על המעסיק לשמור את המידע הנאסף באמצעות טכנולוגיות מעקב אך ורק לתקופה התואמת את מטרת איסוף המידע או את מטרת המאגר שבו שמור המידע.

(6) **אבטחת מידע ועיצוב לפרטיות**. האחריות לאבטחת המידע הנאסף באמצעות טכנולוגיית מעקב מוטלת על המעסיק כבעל מאגר המידע. כדי לעמוד בחובה זו הרשות ממליצה שהמעסיק יבצע תסקיר השפעה על הפרטיות טרם התחלת השימוש בטכנולוגיית מעקב במטרה למזער את הסיכון לפגיעה בפרטיות ולפרצות אבטחה. כן ממליצה הרשות למנות ממונה הגנת פרטיות בארגון, אשר יסייע בבחינה ובתכנון של הצעדים הדרושים לצורך מזעור הסיכון לפגיעה בפרטיות העובדים.

(7) **כיבוד זכויות העובד כנושא המידע**. בהתאם לחוק הגנת הפרטיות, על המעסיק להתיר לעובד לעיין במידע אישי שנאסף על אודותיו באמצעות טכנולוגיות מעקב ואף לדרוש את תיקונו או את מחיקתו אם מצא שאינו נכון, שלם, ברור או מעודכן.

(8) **איסור העברה לצדדים שלישיים**. הרשות להגנת הפרטיות הבהירה שהמידע שנאסף באמצעות טכנולוגיות מעקב מיועד אך ורק לצורכי המעסיק לשם פיקוח על העובד בשעות העבודה. משום כך אין להעבירו לצדדים שלישיים, לרבות מעסיקים עתידיים, אלא בהסכמת העובד או לפי חוק.[146]

עוד הבהירה הרשות ששימוש באמצעים לצילום העובד ולהאזנה לסביבתו בעת עבודתו מרחוק, ובעיקר כזה הנעשה באופן רציף ובמהלך מרבית שעות היום, עלול להוביל לאיסוף מידע אישי, פרטי ורגיש על אודות העובד ובני ביתו, לרבות קטינים, שאינו רלוונטי לצורכי מקום העבודה. הסכמת העובד לשימוש כאמור עשויה להיות שלא מרצון חופשי וכן אין בה כדי להכשיר פגיעה בפרטיותם של אחרים, שאינם העובד עצמו. משום כך, לפי עמדת הרשות ניתן להשתמש באמצעים לצילום העובד ולהאזנה לו בעת עבודה מרחוק רק במקרים קיצוניים שבהם קיים צורך חיוני לכך וכאשר אמצעים אחרים לא הועילו. כמו כן, השימוש

146 שם.

באמצעים אלו צריך להיות מוגבל לשעות העבודה, תוך כדי הימנעות ככל האפשר, מאיסוף מידע על אודות אחרים. על המעסיק להימנע משמירת מידע אגבי שנאסף תוך כדי הפעלת אמצעים אלו על מי שאינם העובד.[147] בכך קובעת הרשות את התנאים להכשרת חדירה למרחב האישי של העובד ובני ביתו לשם מיצוי הפררוגטיבה הניהולית של המעסיק.

לצד דרישות אלו, הרשות חזרה על הלכת **איסקוב** והבהירה שהמעסיק אינו רשאי להשתמש באמצעי מעקב לחדירה לתיבת דוא"ל חיצונית פרטית של העובד או לאיסוף מידע ממנה, לרבות נתוני התקשורת של העובד, אלא מכוח צו שיפוטי. משום כך המליצה הרשות למעסיק המתיר לעובד לגשת לתיבת דוא"ל חיצונית פרטית של העובד בעת עבודה מרחוק או במקום העבודה, להימנע מלהשתמש בטכנולוגיות מעקב המאפשרות צילום מסך העובד.[148] לעמדה זו כמה משמעויות: האחת, הרשות מבחינה בין פעולות שהעובד עושה במרחב הדיגיטלי בשירותים שאינם מחייבים הזדהות וסיסמה, למשל האתרים שבהם גולש העובד ברשת האינטרנט באמצעות מחשב המעסיק או בעת שעות העבודה מרחוק, לבין תיבת הדוא"ל החיצונית הפרטית של העובד. בעוד הפעילות בשירותים שאינם מחייבים הזדהות אינה נחשבת מרחב דיגיטלי אישי, פעילות בשירות המוגבל בסיסמה, כגון תיבת הדוא"ל החיצונית הפרטית שלו, נחשבת המרחב הדיגיטלי האישי שלו. השנייה, הרשות מבחינה בין חדירה למרחב הדיגיטלי האישי של העובד לבין חדירה למרחב הפיזי האישי של העובד. לכאורה, לפי עמדה זו, זכות העובד לפרטיות לגבי פעולותיו ברשת האינטרנט בשירותים שאינם מחייבים הזדהות ובמרחב הפיזי שלו מצומצמת יותר מאשר זכותו לפרטיות במרחב הדיגיטלי האישי שלו.

עמדת הרשות בהנחיה העוסקת בהיבטי הפרטיות הנלווים למעקב אחר עובדים בעת עבודה מרחוק זוכה לביקורת חריפה בטענה שמדובר בהכשרת פגיעה בפרטיות, שאין לה כלל הסמכה בחוק. נטען כי החוק אינו מתיר למעסיק להשתמש באמצעים טכנולוגיים לשם מעקב אחר עובד שעובד מרחוק, כי הנחיית הרשות בנושא עלולה להוביל לפגיעה חמורה בעובדים אשר היא בגדר חריגה מתחום מומחיותה של הרשות וכי נדרשת אסדרה ראויה של התחום שהוא תחום

147 **שם**, עמ' 16–18.

148 **שם**, עמ' 16.

חדש. אסדרה שכזו ראוי שתבוצע רק לאחר שיח עם ארגוני עובדים ומעסיקים בשיתוף מומחים בדיני פרטיות. לפי עמדה זו העבודה מרחוק טומנת בחובה יתרונות הן לחברה בכללותה והן למעסיקים. מן הבחינה החברתית, עבודה מרחוק מובילה להשבחת ההון האנושי, לקידום מוביליות חברתית, להקלה על תשתיות התחבורה, להגנה על הסביבה ולקידום רווחת הפרט, בעיקר באמצעות איזון בין חיי המשפחה לעבודה. מבחינת המעסיקים, לעבודה מרחוק יתרונות כלכליים המתבטאים, למשל, בהפחתת ההוצאות הקשורות בתחזוקת משרדים פיזיים ואף בעלייה בפריון העובד. המעסיק משקלל יתרונות אלו מול החסרונות הטמונים בעבודה מרחוק, ובראשם אובדן שליטה מלאה על זמנו של העובד והוא זה שמחליט אם להתיר לעובד לעבוד במתכונת עבודה מרחוק. משום כך, לפי עמדה זו, הנחת המוצא של הרשות, ולפיה עבודה מרחוק היא הטבה גרידא לעובד העשויה בנסיבות מסוימות להצדיק פגיעה בפרטיות, אינה נכונה. הנחת המוצא הנכונה, לפי ביקורת זו, היא שבעת בחירה במתן היתר לעבודה מרחוק נדרש המעסיק להפנים שהוא מוותר בכך על מגוון אמצעים העומדים לרשותו במרחב הפיזי שבבעלותו לשליטה בעובד. טכנולוגיות למעקב אחר העובד אינן ניתנות לייבוא למרחב הביתי של העובד. יתרה מכך, ההלכה שנקבעה בפרשת **איסקוב** בדבר סמכותו של המעסיק לעשות שימוש באמצעי מעקב מסוימים, בהתאם לאיזון בין הפגיעה בזכות העובד לפרטיות לבין הפררוגטיבה הניהולית של המעסיק, אינה חלה כאשר מדובר במרחב האישי של העובד. לפי עמדה זו, במרחב האישי של העובד אין למעסיק שום סמכות להפעיל אמצעי מעקב אחר העובד, ואין לתת להסכמתו של העובד בנסיבות אלו שום משקל. תמיכה בעמדה זו ניתן למצוא בפסיקת בית הדין האזורי לעבודה משנת 2006, ולפיה צילום פנים דירתה של עובדת, גם אם דירה זו שימשה אותה לצורך פרנסה, ואף אם מטרת הצילום הייתה הגנה על אינטרס לגיטימי של המעסיק, היא פגיעה חמורה בפרטיות העובד ואין להתירה.[149]

במסגרת הביקורת שנמתחה על עמדת הרשות המתבטאת בהנחיה הוסבר עוד כי חובת המעסיק לנהל פנקס שעות לעובדיו, לפי חוק שעות עבודה ומנוחה,

149 נועה דיאמונד ומיכל תג'ר **התייחסות הקליניקה לזכויות עובדים.ות והקליניקה לפרטיות למסמך הרשות "היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק"** טיוטה שפורסמה להערות הציבור ביום 25.12.2022 (18.1.2023); הכותבות מפנות לעב' (אזורי ת"א) 6702/02 **בן דוד נ' איפרגן** (נבו 30.7.2006).

אינה חלה על עובדים שתנאי עבודתם אינם מאפשרים פיקוח כאמור, ובכללם עבודה מהבית, ולכן אין בה כדי להצדיק מעקב פוגעני. יתרה מכך, אף אם החובה לנהל פנקס שעות עבודה חלה על מעסיק לגבי עובדים שהתיר להם לעבוד מהבית, אין בה כדי להצדיק או להתיר ניהול מעקב טכנולוגי על העובד. זאת ועוד, עמדת משרד העבודה היא שלצורך עמידה בחובת המעסיק לנהל פנקס שעות עבודה אין הכרח בתיעוד טכנולוגי, וניתן אף להסתפק בדיווח ידני של שעות העבודה על ידי העובד מרחוק.[150]

1.5
סיכום ביניים: הזכות לפרטיות בראי המשפט המשווה

הזכות לפרטיות היא זכות יסוד חוקתית, שההגנה עליה חיונית לשם שמירה על הערכים שבבסיסה, בעיקר על האוטונומיה של הפרט ועל יכולתו לקבל החלטות עצמאיות ומושכלות, ובתוך כך על שיח ציבורי עשיר ומתפקד ההכרחי להליך דמוקרטי תקין.

גם עובד זכאי ליהנות מזכות לפרטיות, אם כי זו, ככל זכות יסוד חוקתית, אינה זכות מוחלטת. בנסיבות של יחסי עבודה מאוזנת זכות העובד לפרטיות אל מול זכות היסוד החוקתית של המעסיק לקניין, המתבטאת בתפיסת הפררוגטיבה הניהולית של המעסיק. בחלוף הזמן הפך בהדרגה המעקב שניהלו מעסיקים אחר עובדיהם למקובל ולמצופה, במסגרת זכותו של המעסיק להביא למרב את יעילות עסקיו ורווחיותם. אולם הקִדמה הטכנולוגית הובילה לאימוץ תפיסה מרחיבה, ולעיתים אף שגויה, של הפררוגטיבה הניהולית של המעסיק, אגב פגיעה בלתי מידתית בזכות העובד לפרטיות. תפיסה מרחיבה זו הגיעה לשיאה בעת משבר הקורונה עת מעסיקים רבים תרו אחר דרכים אשר יבטיחו להם המשך תפקוד יעיל ותקין של העסק, תוך כדי שמירה על רווחיותו, גם בעת עבודה מרחוק. טכנולוגיות המעקב שהפכו לנפוצות מאוד בקרב מעסיקים רבים ברחבי העולם בתקופת הקורונה ולאחריה מטשטשות את הגבול בין המרחב הפרטי לבין המרחב הציבורי והופכות את יכולותיו של העובד, ביצועיו,

150 דיאמונד וחג'יר, **לעיל** ה"ש 149.

מאפייני אישיותו, מצבו הבריאותי והנפשי, דעותיו ותחושותיו, לשקופים בפני המעסיק. כך עשויות טכנולוגיות למעקב אחר עובדים להיות חודרניות ביותר ולפגוע קשות בפרטיות העובדים. בעוד ההגבלות על פרטיותו של עובד במקום העבודה הפיזי הן ברורות, פגיעה בפרטיות העובד באמצעות טכנולוגיות מעקב המאפשרת חדירה לביתו הפרטי ולמחשבותיו, היא בגדר עליית מדרגה מבחינת היקף הפגיעה המותר בחסות מה שמקובל לכנות הפרוגטיבה של המעסיק.

מסקירת המשפט המשווה המובאת בקצרה ב**לוח 1: דוקטרינת ההפרה התורמת – סקירת משפט משווה** עולה מציאות מורכבת מבחינת התשתית המשפטית הקיימת להתרת שימוש יעיל ונדרש בטכנולוגיות מעקב אחר עובדים לשם מימוש היתרונות הגלומים במתווה עבודה היברידי לצד הגנה נאותה על פרטיות העובדים.[151] ניתן להצביע על טווח הגנה: בקצה האחד, הגנה מזערית בארצות הברית, שבמסגרתה יתקשה העובד להוכיח פגיעה בפרטיותו עקב שימוש בטכנולוגיית מעקב על ידי המעסיק, כל עוד המעסיק יידע אותו על כך. בקצה השני, הגנה ברמה גבוהה באיחוד האירופי המורכבת מהוראות ה־GDPR ומפרשנותן באופן המכפיף טכנולוגיית מעקב לארבע דרישות – הלגיטימיות, המידתיות, עקרון צמידות המטרה והשקיפות – לצד דרישות חוק ה־AI המחייבות למנוע או למזער סיכון לזכות לפרטיות כבר משלב פיתוח הטכנולוגיה, עובר בשיווקה וכלה בשימוש בה. במרכז, לכאורה, ממוקמת מדינת ישראל. עם זאת, גם לאחר עדכון חוק הגנת הפרטיות, שייכנס לתוקפו בחודש אוגוסט 2025,[152] ההגנה על פרטיות העובד בישראל אינה מספקת נוכח פערי הכוחות בין עובד למעסיק והקושי להסתמך על הסכמת העובד. זאת ועוד, הנחיות של הרשות, שלהן תוקף פרשני בעיקר, המליצו להתיר שימוש בטכנולוגיות מעקב אחר עובדים בעת עבודה מרחוק בכפוף לדרישת הלגיטימיות, המידתיות, השקיפות, עקרון צמידות המטרה, הסכמת העובד והגנה על אבטחת המידע. עם זאת נראה שהנחיית הרשות הקבילה את השימוש בטכנולוגיות מעקב אחר עובד בעת עבודה מרחוק למעקב שמנהל מעסיק אחר עובד באמצעות חדירה לתיבת דוא"ל של המעסיק. הקבלה זו אינה נקייה מספקות שכן בעוד שימוש

151 Ebert et al., **לעיל** ה"ש 30, עמ' 4.

152 חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד–2024, ס"ח 3287 מיום 14.08.24 (להלן: תיקון 13).

בטכנולוגיית מעקב בעת עבודה מרחוק מתנהל אומנם על גבי תשתית דיגיטלית שבבעלות המעסיק (המחשב שבאמצעותו מתחבר העובד מרחוק ובמקרים מסוימים חיבור האינטרנט המשולם על ידי המעסיק), הוא חודרני בהרבה ממעקב ממוקד אחר תכתובת דוא"ל בלבד וכן מתנהל במרחב הפיזי הפרטי של העובד.

יש לתת את הדעת גם לכך שתעשיית טכנולוגיות המעקב אחר עובדים מורכבת ברובה מחברות טכנולוגיה קטנות רבות, עובדה שיכולה להקשות על רשויות הגנת הפרטיות, גם באיחוד האירופי, לפקח על פעילות החברות ובמידת הצורך לפעול למניעה מראש או להפסקה של פגיעה בפרטיות על ידי הטכנולוגיה שהן מפתחות. יתרה מכך, מאחר שמדובר כאמור בחברות רבות וקטנות, הן נמלטות פעמים רבות מרדאר הפיקוח.[153]

לא זו אף זו, עובדים רבים נרתעים מלהתלונן על מעסיקיהם ומלנהל נגדם הליך משפטי. הרתיעה אינה נובעת רק מן העלות הכספית הכרוכה בניהול תביעה משפטית, אלא גם ואולי בעיקר מהחשש לנהל תביעה נגד מקור הפרנסה העיקרי, ומההשלכות של ניהול תביעה כאמור על המוניטין של העובד בעתיד לכשירצה להתקבל לעבודה במקומות אחרים. גם ניסיונותיהם של עובדים להביא לשינוי פנימי של מדיניות הפרטיות באמצעות פנייה והידברות עם המעסיק כושלים על פי רוב. מרבית המעסיקים מעדיפים לדכא כל ביקורת או התנגדות בנושא באמצעות איומים בפגיעה בשכר ואף בפיטורים. יתרה מכך, השימוש בטכנולוגיות מעקב מקשה על העובדים להתאגד לשם תיאום ציפיות, למתוח ביקורת על מדיניות המעסיק ולהתייצב מולו בדרישה לשיפור תנאי ההעסקה.[154]

בנסיבות אלו, נדמה שיש צורך בחשיבה ובבחינה מחודשת של האיזון הראוי בין הפררוגטיבה של המעסיק וזכותו לנהל עסק יעיל ומצליח לבין היקפה של זכות העובד לפרטיות. בהיעדר שינוי חקיקתי מתאים השאלה הנבחנת במחקר זה, אם עובד שפרטיותו נפגעה יכול לקבל סעד יעיל יותר מכוח הכלי החלופי של דוקטרינת ההפרה התורמת – הופכת משמעותית עוד יותר.

153 Negron & Nguyen, **לעיל** ה"ש 42.

154 האגודה לזכויות האזרח, **לעיל** ה"ש 26, עמ' 86–87.

לוח 1
ההגנה על זכות העובד לפרטיות: סקירת משפט משווה

	ארצות הברית		האיחוד האירופי	ישראל
	מקום עבודה במגזר הציבורי	מקום עבודה במגזר הפרטי		
מקור ההגנה על זכות העובד לפרטיות	מכוח התיקון הרביעי לחוקה.	משפט מקובל, חקיקה מדינתית.	ECHR, צ'רטר האירופי לזכויות יסוד, אמנת ליסבון, ה־GDPR וחוק ה־AI.	ס' 7 לחוק יסוד: כבוד האדם וחירותו, חוק הגנת הפרטיות.
היקף ההגנה על זכות העובד לפרטיות	מצומצם. לפי מבחן הציפייה הסבירה.	מצומצם. פגיעה בפרטיות היא עוולה נזיקית. הוכחתה מחייבת פגיעה ניכרת, לפי מבחן האדם הסביר, וכן פגיעה בציפייה הסבירה של העובד לפרטיות.	נרחב יחסית. ההגנה חלה גם על המרחב הדיגיטלי של המעסיק וגם על המרחב הדיגיטלי האישי, כולל את קשריו החברתיים של העובד, תכתובות דוא"ל, היסטוריית הגלישה ברשת האינטרנט, ותכתובת בתוכנת מסרים מיידיים.	משתנה. בפרשת **איסקוב** נקבע כי היקף ההגנה ישתנה בהתאם לציפייתו הסבירה של העובד לפרטיות. אומצה הבחנה בין פרטיות במרחב דיגיטלי של המעסיק (תיבת דוא"ל המסופקת לעובד על ידי המעסיק) לבין זכות רחבה יותר לפרטיות במרחב דיגיטלי אישי של העובד (תיבת דוא"ל חיצונית פרטית שלו). בפרשת **זינגר** ניתן משקל רב יותר לתום ליבו של המעסיק ולאינטרס הלגיטימי שלו מאשר למאפייני המרחבים הדיגיטליים – האישי והמקצועי. בהנחיית הרשות לעניין שימוש בטכנולוגיות מעקב בעת עבודה מרחוק הוחלו התנאים שנקבעו בפרשת **איסקוב** בנושא המרחב הדיגיטלי של המעסיק גם על חדירה למרחב הפיזי האישי של העובד ועל חדירה למרחב דיגיטלי אישי שאינו מוגן בסיסמה.
הצדקות לפגיעה בפרטיות	יעילות כלכלית; יצירת סביבה עבודה בריאה ובטוחה; מיוחסת חשיבות רבה ליידוע העובד כמאיין את ציפייתו הסבירה לפרטיות או כבסיס להכשרת הסכמתו לפגיעה.		לפי חוק, לשם ביצוע התחייבות חוזית שהעובד הוא צד לה, אינטרס לגיטימי של המעסיק ובמקרים מצומצמים ביותר – הסכמת העובד.	תכלית לגיטימית של המעסיק ובנסיבות מסוימות – הסכמת העובד.

	ארצות הברית	האיחוד האירופי	ישראל
תנאים להכשרת פגיעה בפרטיות	יידוע העובד והסכמתו.	פגיעה בזכות העובד לפרטיות מותרת ובלבד שהיא מידתית, נחוצה לשם השגת אינטרס לגיטימי של המעסיק ומבוצעת בשקיפות ובהוגנות מתוך שמירה על עקרון מזעור המידע. לשונות בין המרחבים (פיזי של מעסיק, פיזי אישי של העובד, דיגיטלי של המעסיק ודיגיטלי אישי) ניתן משקל בעת בחינת מידתיות הפגיעה בפרטיות. על המעסיק לבצע הערכת אינטרס לגיטימי. כאשר הפגיעה עשויה להוביל לסיכון ממשי, על המעסיק לבצע תסקיר השפעה על הפרטיות. על המעסיק לכבד את זכויות העובד כנושא מידע לפי ה־GDPR, לרבות זכות העיון, התיקון והמחיקה.	כאשר הפגיעה היא במרחב הדיגיטלי של המעסיק (תכתובת דוא"ל בתיבה של המעסיק): נסיבות מוגבלות ויוצאות דופן, חשש כבד מפעילות לא חוקית של העובד; שקיפות כלפי העובד ויידועו; מטרת הפגיעה לגיטימית; מידתיות הפגיעה, צמידות מטרה והסכמת העובד. כאשר הפגיעה מתרחשת במרחב הדיגיטלי האישי של העובד (תכתובת דוא"ל בתיבה חיצונית פרטית): צו מבית המשפט; קיומן של נסיבות חריגות; המעסיק עומד בנטל הוכחה מוגבר להוכיח לכאורה את טיב העילה ואת סיכויי התביעה; חשש ממשי סביר או ברמה של ודאות קרובה שהנכסים הדרושים לבירור התובענה יושמדו; וכן שהעלמת הנכסים תקשה על בירור התביעה ותסב לו נזק חמור. בפרשת **אלקנר** נקבע מבחן תלת־שלבי המורכב מבחינת לגיטימיות תכלית הפגיעה בפרטיות העובד, מידתיות הפגיעה והסכמת העובד. מידת ההסכמה הנדרשת עומדת ביחס ישר למידתיות הפגיעה בפרטיות. בבחינת הפגיעה בפרטיות יובאו בחשבון גם אופי העבודה וטיבה, דרישות התפקיד ומהותו, סביבת העבודה, המדיניות הכללית במקום העבודה והצורך בהגנה מפני עבירות ונזקים מצד העובד. לפי הרשות, כאשר הפגיעה בפרטיות מתרחשת עקב חדירה למרחב הפיזי האישי של העובד או למרחב הדיגיטלי של המעסיק או למרחב האישי שאינו מוגן בסיסמה, תחול הלכת **איסקוב** ביחס לפגיעה במרחב הדיגיטלי של המעסיק.
שימוש בבינה מלאכותית	אין התייחסות.	טכנולוגיות מעקב אחר עובדים הכוללות מערכות בינה מלאכותית יהיו כפופות לדרישות נוספות לפי חוק ה־AI ויחולו על יצרני מערכות, על ספקים ועל משתמשים. למשל, דרישות הנוגעות לממשל נתונים, לחובת שקיפות ולחובת פיקוח אנושי יעיל.	אין התייחסות.

פרק 2

דוקטרינת ההפרה התורמת: משפט משווה

בפרק הקודם סקרתי את היקפה של זכות העובד לפרטיות ועמדתי על הסכנה הגוברת לפגיעה חמורה בה בעקבות השימוש הגובר בטכנולוגיות למעקב אחר עובדים. פגיעה זו עלולה להוביל לפגיעות חמורות נוספות, למשל, ביכולתם של עובדים מן המעמד הנמוך להתאגד. סקירת המשפט המשווה בסוגיה עוררה את החשש שאין כיום בעולם מסגרת משפטית מקיפה ויעילה להתמודדות עם פגיעה חמורה בפרטיות העובד: רמת הגנת הפרטיות שנהנה ממנה עובד בארצות הברית היא הנמוכה ביותר, עובד ישראלי נהנה מהגנת פרטיות נרחבת יותר ואילו עובד ממדינות האיחוד האירופי צפוי ליהנות מהגנת פרטיות נרחבת אף יותר. עם זאת, נוכח הפער המוכר בין המשפט לבין הדינמיות המאפיינת את שוקי הטכנולוגיה והשגשוג של תעשיית טכנולוגיות המעקב אחר עובדים, יש מקום לבחון אם עשויים לעמוד לרשות העובד כלים משפטיים אחרים כדי לתבוע את נזקו או כדי להרתיע מפני פגיעה חמורה בפרטיותו שעלולה להיגרם משימוש לא חוקי בטכנולוגיות מעקב אחר עובדים, ובתוך כך להביא לשינוי הארכיטקטורה של טכנולוגיות מעקב כך שיאזנו באופן ראוי בין התועלות הטמונות בהן, למשל לשם המשך מתווה העבודה ההיברידי, לבין הפגיעה בזכות העובד לפרטית. אחד הכלים המשפטיים האפשריים הוא דוקטרינת ההפרה התורמת מדיני זכויות היוצרים, שבה יעסוק פרק זה.

דוקטרינת ההפרה התורמת עוסקת בשאלה: "האם יצרן של טכנולוגיה דו־שימושית אחראי לשימושים הלא חוקיים שעושים המשתמשים במוצר? ואם כן, באילו תנאים?".

שאלה זו התעוררה בארצות הברית בשנות ה־80 של המאה ה־20 בהקשר של הפרת זכויות יוצרים. הקושי שהציבה שאלה זו מלכתחילה לפני בתי המשפט היה היעדר מערכת יחסים מתמשכת וישירה של פיקוח כלשהו בין יצרן הטכנולוגיה לבין משתמשי הקצה בה, בניגוד, למשל, למערכת היחסים בין משכיר אולם אירועים לשוכר, או בין מעסיק לעובד, אשר יוצרת מנגנוני פיקוח ושליטה של המשכיר או של המעסיק על מעשיהם של השוכרים או העובדים. הדיונים בסוגיית אחריותו של יצרן טכנולוגיה להפרות זכויות היוצרים המבוצעות בידי

המשתמשים בה הובילו לפיתוח דוקטרינת ההפרה התורמת, תחילה בארצות הברית ובהמשך גם באירופה ובישראל, כפי שיתואר להלן.

2.1. בארצות הברית: מסוני ועד גרוקסטר

דוקטרינת ההפרה התורמת בדיני זכויות יוצרים היא הרחבה יציר המשפט המקובל של עקרון האחריות הקבוע בדיני זכויות היוצרים. שורשיה הנורמטיביים נעוצים בהיעדר איסור מפורש בדין על הטלת אחריות על מפר תורם וכן בעובדה שעקרון האחריות התורמת מקובל בדיני הנזיקין ובדיני הפטנטים.[155] ראשיתה של הדוקטרינה בשנת 1911, אז פסק בית המשפט העליון בארצות הברית שחברה שהעסיקה עובד במטרה שיכתוב תסריט המבוסס על ספר אחראית להפרה הישירה שביצע העובד, וכן להפרה הישירה שביצעה חברת הפקת הסרטים שרכשה ממנה את התסריט.[156] בפסקי הדין שניתנו בשנים הבאות התבססה הדוקטרינה כאפיק להטלת אחריות על מי שמספק לאחֵר אמצעים להפרה, מודע להפרה, שולט על השימוש ביצירות מוגנות בזכות יוצרים או מתיר שימוש כאמור ללא רשות בעל זכות היוצרים.[157] ההכרה במודעותו של גורם הביניים התבססה, רובה ככולה, על הקשר בינו לבין המפר הישיר, על ההיכרות ביניהם ועל יכולתו של גורם הביניים לשלוט במעשיו של המפר הישיר.[158]

155 John M. Moye, *How Sony Survived: Peer-to-Peer Software, Grokster, and Contributory Copyright Liability in the Twenty-First Century*, 84 N.C. L. Rev. 646, 653 (2006); 39 U.S.C.A. §271(C) (1994)

156 ראו Connie Davis Powell, *The Saga Continues: Secondary Liability for Copyright Infringement Theory, Practice and Predictions*, 3(1) Akron Intell. Prop. J., 189, 191 (2016), המחאר את פסק הדין בפרשת Kalem Co. v. Harper Bros., 222 U.S. 55 (1911).

157 Powell, **לעיל** ה"ש 155, עמ' 191–192.

158 Methaya Sirichit, *Catching the Conscience: An Analysis of the Knowledge Theory Under §512(c)'s Safe Harbor & the Role of Willful*

בשנת 1976 נחקק חוק זכויות יוצרים חדש בארצות הברית,[159] אולם אף שבית המשפט כבר פיתח את דוקטרינת ההפרה התורמת, המחוקק לא שילב בחוק הוראות המעגנות אותה. עם זאת, לפי היסטוריית החקיקה נראה שהמחוקקים ביקשו להכיר בדוקטרינת ההפרה התורמת באמצעות ההכרה המפורשת בזכות הבלעדית של בעל זכות היוצרים להתיר את השימוש ביצירתו.[160]

בפרשת **סוני** (1984) הכיר בית המשפט בקיומה של דוקטרינת ההפרה התורמת שפותחה בפסיקות בית המשפט בעבר ובחיזוק שניתן לה בהיסטוריה החקיקתית של חוק זכויות היוצרים משנת 1976, אולם הבהיר שהנסיבות שמולו שונות, משום שאין מדובר במערכת יחסים של מודעות, שליטה או פיקוח, המאפיינים למשל בעל אולם קונצרטים, בעל אולם אירועים או בעל חנות המוכרת קלטות ריקות ומעניקה שירות הקלטה והעתקה.[161] בפרשת **סוני** דובר ביצרן של מכשיר טכנולוגי המאפשר העתקה, לצד שימושים אחרים חוקיים, ועלול להימצא אחראי תורם להפרת זכויות היוצרים בידי לקוחותיו אף אם אין ביניהם מערכת יחסים מתמשכת של פיקוח כלשהו.[162]

הטכנולוגיה שנדונה באותה פרשה הייתה מכשיר הווידיאו של חברת סוני, Betamax. בשנות ה־80 היה ה־Betamax המכשיר החדשני הראשון שאפשר למשתמשיו להחזיק בבתיהם ספריות וידיאו אישיות שלא היו מביישות ארכיון טלוויזיה עשיר. בעלי זכויות היוצרים של כמה תוכניות טלוויזיה ששודרו באותה

Blindness in the Finding of Red Flags, 23 Alb. L.J. Sci. & Tech. 85, 99–100 (2013)

159 Copyright Act of 1976, 17 U.S.C. §§ 101–1332 (2012)

160 ראו Powell, **לעיל** ה"ש 155, עמ' 191–192.

161 Moye, **לעיל** ה"ש 154, עמ' 653; Jane C. Ginsburg, *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 Ariz. L. Rev. 577, 580 (2008)

162 David G. Post, Annemarie Bridy & Timothy Sandefur, *Nice Questions Unanswered: Grokster, Sony's Staple Article of Commerce Doctrine, and the Deferred Verdict on Internet File Sharing*, 2004 Cato Sup. Ct. Rev. 234, 240–241 (2004–2005)

העת בערוצי השידור הציבוריים עמדו לפני דילמה קשה: זכויות היוצרים שלהם הופרו בהיקף נרחב אולם בידי מפירים בודדים רבים, וניהול תביעה נגד כל אחד ואחת מהם לא היה מעשי או משתלם כלכלית. בעלי זכויות היוצרים החליטו אפוא לתבוע את חברת סוני.[163]

בית המשפט העליון בארצות הברית התבסס בפסק דינו על דוקטרינת ההפרה התורמת מדיני הפטנטים,[164] ולפיה כאשר ניתן לעשות בטכנולוגיה שימוש מסחרי חוקי משמעותי (commercially significant non-ifringing uses), הוכחת מודעותו בכוח של היצרן לאפשרות השימוש הלא חוקי בטכנולוגיה שייצר אינה מספקת לשם הטלת אחריות תורמת. באמצעות יצירת חריג של "שימוש חוקי משמעותי" ביקש בית המשפט לאזן בין הגנה על זכות היוצרים והאינטרס של יוצרים לשלוט בשימוש ביצירותיהם לבין האינטרס של החברה לעודד חדשנות וזרימה חופשית של רעיונות, מידע ומסחר. יישום דוקטרינת ההפרה התורמת והחריג לה בנסיבות המקרה הוביל את בית המשפט למסקנה שמכשיר הווידיאו של סוני, שתכליתו העיקרית היא לאפשר שימוש הוגן משמעותי בדמות הקלטה וצפייה מאוחרת (time shifting), אינו יכול לשמש בסיס להטלת אחריות תורמת על סוני בגין השימושים המפירים הנעשים באמצעותו.[165] פסק הדין בפרשה אותת לציבור שבית המשפט מבקש לעודד חדשנות כל עוד מטרתה של הטכנולוגיה החדשנית היא שימוש לגיטימי ולא הפרת זכויות יוצרים.[166]

163 פרשת **סוני**, **לעיל** ה"ש 7, עמ' 442.

164 Patent Act of 1952, 35 U.S.C. §271; Charles W. Adams, *A Brief History of Indirect Liability for Patent Infringement*, 22(3) Santa Clara High Tech. L.J. 369 (2006)

165 פרשת **סוני**, **לעיל** ה"ש 7, עמ' 423, 428, 441.

166 Moye, **לעיל** ה"ש 154, עמ' 659; Diane Leenheer Zimmerman, *Daddy, Are We There Yet – Lost in Grokster-Land*, 9 N.Y.U. J. Legis. & Pub. Pol'y 75, 78 (2005). נציין שבדין הישראלי, החריג שנקבע בפרשת **סוני** (**לעיל** ה"ש 7) אינו מקובל, לכאורה, כפי שמעידה אמירתו של השופט ריבלין בפרשת **שוקן** שלפיה אפשר להטיל אחריות תורמת גם כאשר ההפרה הישירה חוסה תחת חריג השימוש ההוגן. ראו ע"א 5977/07 **האוניברסיטה העברית בירושלים נ' בית שוקן להוצאת ספרים בע"מ** (נבו 15.11.2010), פס' 24 לפסק דינו של השופט ריבלין (להלן: פרשת **שוקן**). לביקורת על עמדה זו ראו אורית פישמן אפורי "אחריות תורמת להפרת זכויות יוצרים בישראל: מהפורום בהר הצופים לפורום המקוון" **הפרקליט** נב 3, 47–48 (תשע"ג).

עם זאת, בית המשפט לא הגדיר היקף ברור לחריג "שימוש חוקי משמעותי" או לנסיבות שבהן מותר יהיה להישען על מודעותו בכוח של היצרן לשימושים מפירים כבסיס להטלת אחריות תורמת עליו.[167] כך נוצרה עמימות בדבר תנאיה של דוקטרינת ההפרה התורמת.[168]

התפתחות האינטרנט וטכנולוגיות שאפשרו הצגת תמונות וקישורים לחומרים המוגנים בזכות יוצרים הובילה לחקיקת ה־Digital Millennium Copyright Act (להלן: DMCA) בשנת 1998.[169] ה־DMCA כולל, בין השאר, הוראות המכונות "נמלי ביטחון" (safe harbors), הקובעות באילו תנאים יהיו ספקי שירותי אינטרנט הנמנים עם אחת מארבע קטגוריות המוזכרות בחוק,[170] פטורים מאחריות ישירה, עקיפה או תורמת להפרת זכויות יוצרים המבוצעות באמצעות השירותים שהם מספקים.[171] כדי ליהנות מהחסינות שמספקים נמלי הביטחון, נדרשים ספקי שירותי האינטרנט למיניהם, בין השאר, להטמיע מנגנון "הודעה והסרה", להוכיח שהם אינם מודעים בפועל לשימוש המפר, אינם שולטים בו, אינם מפיקים רווח ישיר ממנו, ומסירים כל שימוש מפר מייד עם היוודע דבר קיומו.[172] בתי המשפט פירשו את דרישת המודעות בפועל כמתקיימת רק בעקבות קבלת הודעה מבעל זכות היוצרים על אודות השימוש המפר במסגרת מנגנון הודעה והסרה. בספרות הוצע להכיר במודעות בכוח של הספק כאשר אפשר להוכיח שפעל באופן לא אחראי או ציני, אולם עמדה זו לא התקבלה בפסיקה. נפסק שאין די בהוכחת

167 Elizabeth Miles, *In re Aimster & MGM, Inc. v. Grokster, Ltd.: Peer-to-Peer and the Sony Doctrine*, 19 Berkeley Tech. L.J. 21, 22 (2004); Craig A. Grossman, *From Sony to Grokster, The Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War Between Content and Destructive Technologies*, 53 Buff. L. Rev. 141, 164 (2005); Moye, **לעיל** ה"ש 154, עמ' 656–657.

168 Post et al., **לעיל** ה"ש 161, עמ' 244–246.

169 Digital Millenium Copyright Act (DMCA), 17 U.S.C. §§101–1332 (2006)

170 **שם**, ס' 512.

171 **שם**.

172 **שם**, ס' 512(c)(1)(A), (B)(i).

מודעות כללית לכך שהשירות עשוי לשמש גם להפרת זכויות יוצרים או שיש בשרתיו של הספק גם תכנים המפירים זכויות יוצרים. עוד נקבע ש"עצימת עיניים" יכולה להקים מודעות בכוח מצד ספק השירותים רק אם אפשר להוכיח שהיא הייתה מכוונת, ולשם כך נדרש כי יחזיק במידע על הפרה ספציפית שממנה הוא מעלים עין.[173] לפיכך, ניתן לומר שדרישת המודעות לפי ה־DMCA מצומצמת למודעות בפועל בלבד.[174]

אולם ככל שהיקף השימוש באינטרנט גדל לא הצליחו בעלי זכויות היוצרים לנטר תכנים המפירים את זכויותיהם ולהודיע על הימצאם לכל אחד מספקי השירותים האינטרנטיים, ופנו לערכאות המשפטיות.[175]

כ־17 שנים לאחר פסיקת בית המשפט העליון בפרשת **סוני** דן בית המשפט לערעורים במחוז התשיעי בארצות הברית בתוכנת שיתוף הקבצים נאפסטר (Napster). נאפסטר אפשרה שיתוף מבוזר של קבצים, בין השאר קובצי שירים מוגנים בזכויות יוצרים, בין משתמשי הקצה שלה. נאפסטר עקבה אחר כלל משתמשיה, ידעה מי מהם מחובר לפלטפורמה בכל רגע נתון ומהם קובצי המוזיקה הזמינים במחשבו האישי, וכן תחזקה מפתח (אינדקס) של קובצי השירים הזמינים לשיתוף ומיקומם. המפתח שיצרה היווה מנוע חיפוש נוח למציאת קובצי מוזיקה ולהורדתם המהירה ממחשבי משתמשי נאפסטר האחרים. נפסק שניתן לעשות שימוש חוקי משמעותי בטכנולוגיה של נאפסטר, אף שהחברה לא הוכיחה שבאמת נעשה שימוש כזה. אולם בית המשפט לערעורים במחוז התשיעי מצא שנאפסטר הייתה מודעת לשימושים המפירים ויכלה לפקח עליהם באמצעות המפתח שניהלה. נפסק שכאשר גורם הביניים מחזיק במודעות בפועל להפרה ספציפית של זכות היוצרים, העובדה שהטכנולוגיה היא דו־שימושית ועשויים להיעשות באמצעותה שימושים חוקיים

173 UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1108 (C.D. Cal 2009); Sirichit, **לעיל** ה"ש 157, עמ' 186–187.

174 **שם**, עמ' 125–144.

175 Michael Harrigan, *Beyond a Reasonable Doubt: How Blockchain Technology Can Shift the DMCA's Burden of Notification Away from Copyright Owners*, 39 Ent. & Sports Law. 145, 146–147 (2023)

משמעותיים – אינה רלוונטית. לפיכך, נפסק כי נאפסטר אחראית תורמת להפרת זכויות היוצרים בידי משתמשיה.[176]

הפרשה הבאה שהגיעה לפתחו של בית המשפט לערעורים במחוז התשיעי עסקה בפלטפורמה נוספת לשיתוף קבצים – גרוקסטר. החברה החזיקה בשרת מרכזי ששמר את פרטי משתמשי הקצה וסייע במציאת משתמשים אחרים, אך לא אספה שום מידע בנוגע לתעבורת קבצים. מרגע הורדת תוכנת שיתוף הקבצים למחשב של משתמש הקצה, למפתחיה של גרוקסטר לא הייתה שום שליטה בתצורה שלה או באופן השימוש בה. במובן זה גרוקסטר דומה למכשיר הווידיאו של סוני, שעם רכישתו על ידי משתמש הקצה איבדה סוני כל יכולת לשלוט על השימושים הנעשים בו.[177]

בית המשפט לערעורים במחוז התשיעי פסק שאם מוכח שימוש חוקי משמעותי, אזי נדרשת מודעות ממשית להפרה ספציפית בשלב שבו גורם הביניים יכול להפסיק, למנוע או למזער את ההפרה הישירה. עוד נפסק שגם שיעור נמוך של שימושים חוקיים (בפסק הדין דובר ב־10%) מספיק להכרה בקיומו של שימוש חוקי משמעותי. לפיכך נפסק שמפתחיה של גרוקסטר אינם נושאים באחריות תורמת להפרות הנעשות באמצעות התוכנה.[178] בית המשפט לא ייחס שום חשיבות לכך שמפתחיה של גרוקסטר בחרו במכוון לעצבה באופן המונע מודעות מצידם, כדי לצלוח את הפרשנות של בית המשפט לדוקטרינת ההפרה התורמת בפרשת **נאפסטר**.[179]

176 A & M Records, Inc. V. Napster, Inc., 239 F.3d 1004, 1020–1022 (9th Cir. 2001); Bryan H. Choi, *The Grokster Dead-End*, 19(2) Harv. J.L. & Tech 393, 395 (2006) (להלן: פרשת **נאפסטר**); Grossman, **לעיל** ה"ש 166, עמ' 198–200; Ginsburg, **לעיל** ה"ש 160, עמ' 582.

177 Miles, **לעיל** ה"ש 166, עמ' 42; Choi, **לעיל** ה"ש 175, עמ' 395–396.

178 MGM Studios Inc. v. Grokster, Ltd., 380 F.3d 1154, 1160–1161 (9th Cir. 2004), *vacated*, 125 S. Ct. 2746 (2005)

179 Moye, **לעיל** ה"ש 154, עמ' 666; Miles, **לעיל** ה"ש 166, עמ' 27; Choi, **לעיל** ה"ש 175, עמ' 395.

באותן שנים שבהן פרשות **נאפסטר** ו**גרוקסטר** נדונו בבית המשפט לערעורים במחוז התשיעי, נידון גם המקרה של איימסטר, המספקת פלטפורמה לשיתוף קבצים, בבית המשפט לערעורים במחוז השביעי. איימסטר הצפינה את הקבצים המועברים על גבי הפלטפורמה שלה, כך שלא יהיה אפשר לדעת אילו קבצים מועברים בין משתמשיה. על אף הצפנת הקבצים, בית המשפט לערעורים במחוז השביעי פסק בפרשת **איימסטר** כי התקיים יסוד המודעות החיוני להוכחת אחריות להפרה תורמת, משום שהחברה עצמה עיניים כלפי הפרות אפשריות (willful blindness).[180] לפי פסק הדין, כוונתה הרעה של איימסטר מלכתחילה לבנות את תוכנת שיתוף הקבצים כך שלא יתאפשר לחברה המפתחת אותה לקבל מידע בנוגע לשימושים הנעשים בה, היא בגדר עצימת עיניים מכוונת ומעידה על מודעות גורם הביניים להפרה.[181] בכך חרג בית המשפט במחוז השביעי מהפרשנות המקובלת עד אז לדוקטרינת ההפרה התורמת, שלפיה נדרשת מודעות בפועל להפרה הישירה לשם הטלת אחריות תורמת.[182]

גם באשר לחריג לאחריות להפרה תורמת שנקבע בפרשת **סוני** בחר בית המשפט במחוז השביעי בפרשנות שונה מזו שנתן בית המשפט במחוז התשיעי בפרשות **נאפסטר** ו**גרוקסטר**. נפסק שאין די בהוכחת היכולת של המוצר או הטכנולוגיה לאפשר שימוש חוקי משמעותי, אלא יש להוכיח שהמוצר או הטכנולוגיה אכן שימשו בפועל לשימושים חוקיים משמעותיים ושאי־אפשר באמצעים סבירים כלכלית למנוע כליל או להפחית במידה ניכרת את השימושים המפירים. בהתאם לפרשנות זו נפסק שאיימסטר לא הצליחה להוכיח שימוש חוקי כלשהו בפלטפורמה שלה.[183]

ההתדיינות המשפטית בנוגע לאחריות התורמת של גרוקסטר להפרת זכויות היוצרים הגיעה לפתחו של בית המשפט העליון האמריקני בשנת 2004, והוא התבקש לחוות את דעתו באשר לתנאים ולנסיבות שבמסגרתם מפיץ של מוצר

180 In re Aimster Copyright Litigation, 334 F.3d 643, 655 (7th Cir. 2003), *cert. Denied*, 540 U.S. 1107 (2004) (להלן: פרשת **איימסטר**).

181 Sirichit, **לעיל** ה"ש 157, עמ' 107–108.

182 ראו Powell, **לעיל** ה"ש 155, עמ' 194–195.

183 פרשת **איימסטר**, **לעיל** ה"ש 179, עמ' 648.

דו־שימושי ייחשב אחראי להפרת זכות יוצרים שמבצע צד שלישי המשתמש במוצר. משהסכים לדון בפרשה ציפו רבים שבית המשפט העליון יישב אחת ולתמיד את המחלוקת הפרשנית בין הערכאות הנמוכות באשר למידת המודעות הנדרשת להטלת אחריות תורמת, וכן באשר לרף השימוש החוקי המשמעותי הפוטר מאחריות תורמת לפי החריג שנקבע בפרשת **סוני**. לצד ציפייה זו גבר החשש שבית המשפט יצמצם את החריג אשר נקבע בפרשת **סוני**, וכך תיגרם פגיעה של ממש בחדשנות.[184]

אולם בפסיקתו לא הכריע בית המשפט העליון בין הפרשנויות השונות שהוצעו בבתי המשפט במחוז השביעי ובמחוז התשיעי, והמחלוקת באשר למהותה של דרישת המודעות ולרף הוכחת השימוש החוקי המשמעותי הנדרש נותרה בעינה.

השופט סוֹטֶר, אשר כתב את פסק הדין בשם כלל שופטי ההרכב, מתח ביקורת על הפרשנות שנתן בית המשפט במחוז התשיעי בפרשת **גרוקסטר** לדרישת המודעות בפועל, וקבע כי הדרישה להוכיח מודעות בפועל להפרה ספציפית כתנאי להחלת אחריות תורמת היא שגויה. עם זאת, השופט סוֹטֶר נמנע מלקבוע אמת מידה כמותית ל"שימוש חוקי משמעותי" הפוטר מאחריות תורמת לפי החריג שנקבע בפרשת **סוני**, וכתב כי סוגיה זו תזכה להתייחסותו בעתיד אם זו תידרש. השופטת גינסבורג, שלעמדתה הצטרף גם השופט קנדי, הסכימה עם תוצאת פסק הדין, אך התייחסה באופן ספציפי לשאלת היקף השימוש החוקי המשמעותי הנדרש כדי ליהנות מהחריג שאומץ בפרשת **סוני**. לעמדתה יש להעניק פרשנות מחמירה יותר מזו שהייתה מקובלת עד אז לחריג פרשת **סוני**, ולחייב הוכחה ממשית לקיומו של שימוש חוקי משמעותי במוצר. לשיטתה, בפרשת **גרוקסטר** לא הוכח באופן סביר שימוש חוקי משמעותי. ובכל מקרה, אף אם תוכנות שיתוף הקבצים שימשו גם למטרות חוקיות, מספר השימושים החוקיים מתגמד לעומת הכמות העצומה של ההפרות שתוכנות אלה אפשרו. השופט בְּרֶיֶר, שלעמדתו הצטרפו השופטים אוקונור וסטיבנס, הסכים גם הוא עם תוצאת פסק הדין, אולם חלק על ניסיונה של גינסבורג להציע פרשנות

184 Moye, **לעיל** ה"ש 154, עמ' 673; Zimmerman, **לעיל** ה"ש 165, עמ' 84; Alfred C. Yen, *Third-Party Copyright Liability After Grokster*, 91 Minn L. Rev. 184, 188 (2005)

מחמירה יותר לחריג פרשת **סוני**. לשיטתו של ברֵייֶר, גם בפרשת **סוני** עצמה שיעור השימושים החוקיים, אשר בית המשפט העליון דאז הכיר בהם כמקיימים את חריג השימוש החוקי המשמעותי, היה נמוך ועמד על 10% לערך. משום כך, לדעתו עמדה גרוקסטר בדרישת קיומו של שימוש חוקי משמעותי, ואין מקום להחמרת הפרשנות המוענקת לחריג זה שכן הוא עדיין משקף את האיזון הנכון והראוי בין האינטרס של בעל זכות היוצרים בהגנה על זכותו לבין אינטרס הציבור בקידום חדשנות.[185]

במקום להכריע בשאלות הקשורות לתנאים להחלתה של דוקטרינת ההפרה התורמת במקרה של יצרן טכנולוגיה דו־שימושית, בחר בית המשפט לפתח בסיס חלופי להטלת אחריות תורמת להפרת זכות יוצרים – "תאוריית השידול". לפי תאוריה זו, כאשר קיימות ראיות ברורות לכך שהמניע העיקרי ליצירת הטכנולוגיה והפצתה הוא עידוד השימוש בה לשם הפרת זכות יוצרים, יוצר הטכנולוגיה חב באחריות תורמת להפרת זכות היוצרים בידי המשתמשים בה. אם כן, תאוריית השידול מחייבת את בתי המשפט לצלול לבחינה סובייקטיבית של הסוגיה אם מפתחי הטכנולוגיה שידלו את המשתמשים להפר זכויות יוצרים. לפי פסק הדין של בית המשפט העליון בפרשת **גרוקסטר**, אפשר ללמוד על הכוונה מן הארכיטקטורה של הטכנולוגיה, דהיינו מהתקנה או מאי־התקנה של מסנני תוכן בלתי חוקי, או מן המודל העסקי של החברה שמפיצה את הטכנולוגיה. אם כן, תאוריית השידול מאפשרת למפתחי טכנולוגיה להמשיך להישען על החריג שנקבע בפרשת **סוני** כדי לפתח טכנולוגיות חדשניות, ובית המשפט שומר בכך על מסגרת המעודדת חדשנות.[186]

185 MGM Studios Inc. V. Grokster, Ltd., 125 S. Ct. 2764, 2777–2778 (2005) (להלן: פרשת **גרוקסטר**); Yen, **לעיל** ה"ש 183, עמ' 188, 223.

186 Pamela Samuelson, *Three Reactions to MGM v. Grokster*, 13 Mich. Telecomm. & Tech. L. Rev. 177, 186 (2006); Ginsburg, **לעיל** ה"ש 160, עמ' 586–590.

2.2
באיחוד האירופי

דוקטרינת ההפרה התורמת באיחוד האירופי עשויה טלאים־טלאים מדברי חקיקה שונים, שכל אחד מהם עוסק בהיבט אחר של אחריות תורמת להפרת זכויות קניין רוחני.[187] המקור הראשון הוא EU Directive Enforcement of Intellectual Property Rights (להלן: דירקטיבת האכיפה), אשר קובעת כי על המדינות החברות באיחוד האירופי לקבוע בחקיקה אמצעים יעילים לאכיפת זכויות קניין רוחני, ובהם סעדים, לרבות צווי ביניים, נגד מתווכים שהשירות שלהם משמש צדדים שלישיים להפרת זכויות קניין רוחני, למעט זכויות יוצרים.[188] EU Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (להלן: דירקטיבת חברת המידע) מספקת מקור נוסף לדוקטרינת ההפרה התורמת באמצעות הוראה המתייחסת אל מתווכים כאל מונע הנזק היעיל, ועל כן מחייבת את המדינות החברות באיחוד האירופי לקבוע בחקיקה סעדים נגד מתווכים שהשירות שלהם משמש צדדים שלישיים להפרת זכויות יוצרים.[189] דומה שזהו סטנדרט המינימום לאחריות תורמת להפרת זכויות קניין רוחני. עם זאת, מתווכים המספקים תשתית פיזית להעמדה לרשות הציבור של יצירות מוגנות מוחרגים מגדרי האחריות התורמת.[190] מקור חקיקה נוסף המלמד על היקפה של דוקטרינת ההפרה התורמת באיחוד האירופי הוא

187 Christina Angelopoulos, *Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe*, Inter'l Rev. Intell. Prop. & Competition L. 253 (2013)

188 סעיפי הקדמה 3, 9–10 וסעיפים 9 ו־11 ל־Directive 2004/48, of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 157) 45

189 ס' הקדמה 59 וס' 8(3) ל־Directive 2001/29, of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10

190 ס' 8 ל־WIPO Copyright Treaty (WCT) (1996)

דירקטיבת ה־E-Commerce, אשר קובעת "נמלי ביטחון" המגבילים את יכולתן של המדינות החברות להטיל אחריות תורמת על ספקי שירותי אינטרנט.

לפי הוראות אלה, ספק שירותי אחסון לא יישא באחריות תורמת להפרה שמבצע משתמש הקצה באמצעות שירות האחסון בהתקיים שני תנאים: (א) הספק לא היה מודע בפועל להפרה, או לעובדות או לנסיבות שמהן עולה ההפרה בבירור; (ב) עם היוודע דבר ההפרה או העובדות או הנסיבות שמהן היא עולה הסיר הספק מייד את התוכן המפר או מנע גישה אליו.[191] עוד אוסרת דירקטיבת ה־E-Commerce על המדינות החברות באיחוד האירופי להטיל על ספק שירות אינטרנט חובה לנטר את התוכן המאוחסן או המועבר על גבי התשתית שהוא מספק.[192] עם זאת, נמלי הביטחון מוגבלים למקרים שבהם פעילות ספק השירות היא טכנית, אוטומטית ופסיבית מטבעה. ספק אקטיבי שהמודל העסקי שלו מבוסס על האינטרסים שלו באחסון תוכן מפר, הנותן העדפה לאחסון או העברה של תוכן מפר, או שאפילו מפרסם שימוש לא חוקי שכזה בפלטפורמה שלו, אינו זכאי ליהנות מחריג האחריות שכן הוא אינו ניטרלי באשר לתוכן המועבר או המאוחסן, כלומר אינו פועל באופן טכני גרידא, אוטומטי וסביל.[193] עמדה זו קיבלה חיזוק גם בפרשנות של בית הדין לצדק של האיחוד האירופי (להלן: CJEU) לסעיף 14 לדירקטיבת ה־E-commerce.[194] כמו כן, דירקטיבת ה־E-commerce מאפשרת למדינות החברות להגביל את יישומם של נמלי הביטחון במקרה של סעד של צו מניעה – כלומר אפשר לקבוע בחוק מדינתי כי על ספק

191 ס' 14 ל־Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on CertainLegal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market 1 (L 178) O.J. 2000, ("Directive on Electronic Commerce") (להלן: דירקטיבת ה־E-commerce).

192 **שם**, ס' 15.

193 **שם**, ס' הקדמה 42 וס' 15.

194 CJEU, Joined Cases C-236/08 to C-238/08, Google France SARL and Google Inc. v. Louis Vuitton Malletier SA and Others, par. 106 (23.3.2010); Opinion of AG Maduro, pars. 137 et seq. (22.9.2009)

שירות אינטרנט לסיים הפרה או למנוע אותה מרגע שהוא מקבל עליה הודעה.[195] ביוני 2021 נכנסה לתוקף ה־EU Directive on Copyright in the Digital Single Market (להלן: דירקטיבת ה־DSM), שחוללה שינוי מסוים בדוקטרינת ההפרה התורמת באיחוד האירופי בהגדירה מחדש את היקף האחריות הישירה של ספק תוכן שיתופי באינטרנט (online content-sharing service providers).[196] מדובר בספק שירותי מידע חברתיים ש"מטרתו העיקרית, או אחת ממטרותיו העיקריות", היא לאחסן תכנים רבים המוגנים בזכות יוצרים ולהעניק לציבור גישה אליהם.[197] התכנים מועלים בידי משתמשיו, אך מאורגנים ומקודמים על ידי הספק עצמו במטרה להפיק רווח מהנגשתם לציבור המשתמשים. ההגדרה של ספק תוכן שיתופי באינטרנט אינה כוללת ספקים אשר מטרתם העיקרית אינה זו, למשל: ספקים של פלטפורמות המאחסנות ומעניקות גישה לחומרים חינוכיים ומדעיים שלא למטרות רווח; ספקים של שירותי תקשורת מסורתיים, כגון חברות המספקות שירותי חיבור לרשת האינטרנט; ספקי שירותי ענן בין־עסקיים ושירותי ענן, כגון גוגל דרייב או דרופבוקס; ספקי פלטפורמות שוק מקוון שמטרתם העיקרית היא לאפשר מסחר מקוון בין המשתמשים ולא מתן גישה ליצירות המוגנות בזכות יוצרים; ספקי פלטפורמה לפיתוח תוכנות קוד פתוח, כגון גיטהאב (GitHub); וספקי פלטפורמות לאנציקלופדיה מקוונת שלא למטרות רווח.[198]

לפי דירקטיבת ה־DSM, הנגשה לציבור של תוכן המוגן בזכויות יוצרים על גבי פלטפורמה של ספק תוכן שיתופי באינטרנט מהווה העמדה לרשות הציבור על

195 ס' הקדמה 45 וס' 12(3), 13(3); סעיף 14(3) לדירקטיבת ה־E-commerce, **לעיל** ה"ש 190.

196 ראו ס' 17 ל־Directive 2019/790, of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directive 96/9/EC and 2001/29/EC, 2019 O.J. (L 130) 92

197 ס' 6(2) לדירקטיבת DSM. השאלה אם מדובר בספק המעניק גישה לכמות גדולה של תכנים תיבחן באופן כמותי בכל מקרה ומקרה, תוך כדי הערכה של כמות התוכן המוגן בזכויות יוצרים שהספק מאחסן ומנגיש ושל מספר המשתמשים בשירות שהוא מספק. ראו **שם**, ס' הקדמה 63.

198 **שם**, ס' הקדמה 61–62.

ידי הספק, ומחייבת אותו לקבל רישיון לשם כך מבעל זכות היוצרים.[199] בהיעדר רישיון מבעל זכות היוצרים יהא ספק תוכן שיתופי אחראי להפרת זכות היוצרים, אלא אם כן עמד בתנאים האלה:

(**1**) הספק נקט פעולות סבירות לקבלת רישיון מבעל זכות היוצרים.[200]

(**2**) הספק נקט מאמצים סבירים בהתאם לסטנדרטים גבוהים של חריצות מקצועית המקובלים בתעשייה, כדי להבטיח את אי־זמינותן של יצירות, שבעל זכויות היוצרים בהן הודיע לו על הימצאותן בשירות ללא אישורו.[201]

(**3**) ובכל מקרה, הספק פעל מייד עם קבלת הודעה מפורטת מבעל זכות היוצרים להסרתם של התכנים המפירים או לחסימת הגישה אליהם, וכן נקט מאמצים סבירים למניעת העלאה חוזרת של התכנים המפירים לשירות שלו.[202]

עמידתו של הספק בכל אחד מתנאים אלו תיבחן בהתאם לעקרון המידתיות ולשיקולים נוספים המנויים בדירקטיבת ה־DSM כגון סוג השירות המסופק, קהל היעד שלו והיקפו, סוג היצירות המועלות לשירות על ידי משתמשיו, זמינותם של אמצעים יעילים לעמידת ספק התוכן השיתופי בדרישות אלו ועלותן.[203]

בחקיקת דירקטיבת ה־DSM ביקשה נציבות האיחוד האירופי להחמיר את כללי האחריות החלים על ספקים של תוכן שיתופי באינטרנט כדי לתמרץ אותם לפנות לקבלת רישיון מבעל זכות היוצרים ולהטמיע בשירות שהם מספקים כלים טכנולוגיים לזיהוי אוטומטי של תוכן, וכך להקטין את היקף התוכן המפר זכויות יוצרים שמשתמשי הקצה מעלים לרשת האינטרנט.[204] על משטר האחריות שנקבע בדירקטיבה זאת נמתחה ביקורת רבה בטענה שהוא לא ברור, מעורפל ועשוי להתפרש כמטיל חובת ניטור כוללני ומתמיד של התכנים על ידי ספק

199 **שם**, ס' הקדמה 64 וסעיף 17(1).

200 **שם**, ס' 17(4)(a).

201 **שם**, ס' 17(4)(b).

202 **שם**, ס' 17(4)(c).

203 **שם**, ס' 17(5).

204 Pamela Samuelson, *Pushing Back on Stricter Copyright ISP Liability Rules*, 27 Mich. Tech. L. Rev. 299, 302–303 (2021)

השירות באופן הפוגע בזכויות יסוד של המשתמשים, כגון הזכות לחופש ביטוי והזכות לפרטיות.[205]

למרות הביקורת, באפריל 2022 דחה ה־CJEU את טענת פולין שלפיה יש לבטל את משטר האחריות הקבוע בדירקטיבת ה־DSM בנימוק שהוא מטיל חובת ניטור תוכן ולכן פוגע בזכות לחופש ביטוי. ה־CJEU הכיר בכך שהחובה לנקוט פעולות סבירות להבטחת אי־זמינותן של יצירות המוגנות בזכות יוצרים ללא אישור בעליהן מחייבת הלכה למעשה ספקי תוכן שיתופי באינטרנט לנטר תוכן קודם שהמשתמשים מעלים אותו לשירות שלהם, וכך מגבילה את זכות היסוד של משתמשי הפלטפורמה לחופש ביטוי. עם זאת, הזכות לחופש ביטוי אינה זכות מוחלטת, אלא יש לבחון את הפגיעה בה בהתאם לעקרון המידתיות. כן מבהיר ה־CJEU שכל פתרון טכנולוגי ליישום החובה לנקוט אמצעים סבירים חייב להבחין בבירור בין תוכן חוקי לבין תוכן שאינו חוקי.

נוסף על כך מצא ה־CJEU שדירקטיבת ה־DSM כוללת אמצעי הגנה מספקים על הזכות לחופש ביטוי, וכן שפגיעתה בזכות לחופש ביטוי היא נחוצה ומידתית לשם הגנה על זכויות קניין רוחני.[206] כך, למשל, הדרישה שעמידתו של הספק בדרישות לפטור מאחריות תיבחן בהתאם לעקרון המידתיות ומתוך התחשבות בשיקולים נוספים, כגון סוג השירות, קהל היעד שלו והיקפו.[207] כן מונְחות המדינות החברות להתייחס באופן שונה לספק תוכן שיתופי הפועל באיחוד האירופי פחות משלוש שנים והרווח השנתי שלו נמוך מ־10 מיליון אירו. ספק שכזה יחויב אך ורק בנקיטת פעולות סבירות לקבלת רישיון מבעלי זכויות היוצרים כדי לזכות בפטור מאחריות להפרת זכויות יוצרים בידי משתמשיו.[208]

דירקטיבת ה־DSM גם מבהירה שעל המדינות החברות להבטיח שכל שיתוף פעולה בין בעלי זכויות היוצרים לבין ספקי תוכן שיתופי לא יפגע בזמינותן

205 **שם**, עמ' 313–330.

206 Case C-401/19 Action for annulment under Article 263 TFEU, brought of 24 May 2019, Republic of Poland, Judgment of the Court (Grand Chamber) (26 April 2022)

207 דירקטיבת ה־DSM, ס' 17(5)(a).

208 **שם**, ס' 17(6).

של יצירות המוגנות בזכויות יוצרים, בנסיבות שבהן השימוש ביצירות נעשה למטרות ציטוט, ביקורת, סקירה, קריקטורה או פרודיה.[209] עוד נדרשים ספקי תוכן שיתופי להחזיק במנגנון תלונות ויישוב סכסוכים בכל הקשור להסרת תוכני משתמשים על ידם, ולהבטיח שכל החלטה בדבר הסרת תוכן או חסימת הגישה אליו מאושרת בידי גורם אנושי. על המדינות החברות להבטיח שמשתמשים הסוברים כי זכויותיהם נפגעו עקב הסרת תכנים שהעלו או עקב חסימת הגישה אליהם יוכלו לפנות לערכאות משפטיות בבקשת סעד.[210] זאת ועוד, על נציבות האיחוד לקיים מפגשים בהשתתפות ספקי תוכן שיתופי ובעלי זכויות יוצרים כדי לגבש קווים מנחים באשר לסטנדרט הפעולות הסבירות שעל ספקי תוכן שיתופי לנקוט לשם קבלת פטור מאחריות להפרת זכויות יוצרים.[211]

מאחר שמשטר האחריות והחריג לאחריות הקבוע בדירקטיבת ה־DSM מוגבלים רק לספקי תוכן שיתופי באינטרנט, על שאר ספקי השירות חל משטר אחריות שונה המורכב מהוראות דירקטיבת חברת המידע, דירקטיבת האכיפה ונמלי הביטחון שבדירקטיבת ה־E-Commerce. היקפה של אחריות זו והחריגים לה נדונו ביולי 2021 בפסק הדין של ה־CJEU בשתי פרשות שהדיון בהן אוחד: פרשות **יוטיוב** ו־*Cyando*. בשתי הפרשות תבעו בעלי זכויות יוצרים את הבעלים והמפעילים של פלטפורמות שיתוף קבצים, יוטיוב של גוגל ו־Uploaded של חברת Cyando, בגין הפרת זכויות יוצרים שביצעו לטענתם משתמשי הקצה של הפלטפורמות. בעניין **יוטיוב** טענו בעלי זכויות היוצרים כי יצירות מוגנות הועלו לשירות והועמדו בו לרשות הציבור ללא אישורם. בעניין פרשת *Cyando*, נטען כי שירות אחסון הקבצים שלה, Uploaded, אפשר הפרת זכויות יוצרים בידי משתמשי קצה אשר אחסנו קבצים המוגנים בזכויות יוצרים על השירות ושיתפו באתרי אינטרנט שונים (בלוגים ופורומים) קישורים לקבצים אלו, ללא אישור מבעלי זכויות היוצרים. בעלי זכויות היוצרים פנו לבתי המשפט האזוריים במחוז המבורג ובמחוז מינכן אחרי שהיצירות המוגנות שבבעלותם הוסרו מהפלטפורמות בעקבות פנייתם, אך שבו והועלו בידי משתמשי הקצה.

209 **שם**, ס' 17(7).

210 **שם**, ס' 17(9).

211 **שם**, ס' 17(10).

לפיכך, בעלי זכויות היוצרים ביקשו מבית המשפט להוציא צו האוסר על החברה להעמיד לרשות הציבור את היצירות המוגנות, להורות לכל אחת מהחברות להעביר לידיהם מידע על ההפרות ועל הרווחים בגינן, וכן לשלם להם פיצוי כספי בגין הנזקים שנגרמו להם עקב הפרת זכויות היוצרים. בעלי זכויות היוצרים ערערו על החלטת בית המשפט המחוזי לערכאת בית המשפט המחוזי הגבוה, ובהמשך ערערו התובעים והנתבעים לבית המשפט הפדרלי לצדק בגרמניה. זה האחרון השהה את הדיון בערעור, ופנה בבקשה ל־CJEU לפרש את היקף האחריות התורמת של ספק שירות.[212]

ה־CJEU בחן את אופן פעולתן של הפלטפורמות יוטיוב ו־Uploaded, והכיר בכך שהן יכולות לשמש לצרכים חוקיים אך גם לצרכים בלתי חוקיים: קובצי וידיאו המשותפים באמצעות יוטיוב ו־Uploaded עשויים לכלול יצירות המוגנות בזכויות יוצרים, והיכולת לאחסן ולשתף קבצים גדולים באמצעות פלטפורמת Uploaded הופכת אותה כלי שימושי לשיתוף קבצים המוגנים בזכויות יוצרים.[213]

לפיכך נפסק שמשתמשי הפלטפורמות מפירים את זכות ההעמדה לציבור, שהיא אחת מהזכויות באגד זכויות היוצרים ביצירות המוגנות, כאשר הם מעלים אל הפלטפורמה תכנים המוגנים בזכויות יוצרים ללא רשות בעלי הזכויות, ובוחרים לשתף יצירה זו עם ציבור המשתמשים האחרים: במקרה של יוטיוב באמצעות מתן הרשאות צפייה ציבוריות, ובמקרה של Uploaded באמצעות העתקת הקישור לקבצים והצגתו בבלוגים ובפורומים. עוד נקבע שתרומתם של ספקי השירות להפרה הישירה שהמשתמשים מבצעים היא חיונית שכן בהיעדרה ההפרה אינה יכולה להתבצע. ואולם, בית המשפט קבע כי ספק שירות ייחשב אף הוא אחראי להפרת זכות ההעמדה לציבור רק אם יוכח כי תרומתו לא הייתה רק חיונית אלא גם מכוונת.[214] לפי פסק הדין, בבחינת כוונתו של ספק השירות לתרום תרומה חיונית להפרה הישירה בית המשפט צריך לשקול כמה שיקולים:

212 Judgement of the Court (Grand Chamber) of 22 June 2021 Frank Peterson v. Google LLC and Others and Elsevier Inc. v. Cyando AG, Joint Cases C-682/18 and C-683/18 (להלן: פרשות **יוטיוב** ו־*Cyando*).

213 **שם**, פס' 45 לחוות דעתו של ה־Advocate General.

214 **שם**, פס' 60-83 לפסק הדין.

(**1**) ספק השירות ידע או היה עליו לדעת באופן כללי שמשתמשי הפלטפורמה מעמידים באמצעותה לרשות הציבור יצירות המוגנות בזכות יוצרים שלא כחוק. אולם אין די במודעות בפועל או בכוח, אלא נדרש שלמרות ידיעה זאת נמנע ספק השירות מלספק אמצעים טכנולוגיים מתאימים כדי למנוע הפרת זכות יוצרים, כמצופה ממפעיל זהיר.[215] ה־CJEU פסק שיוטיוב נקטה אמצעים אמינים ויעילים כדי להתמודד עם הפרת זכויות יצרים, כמו יידוע המשתמשים כמה פעמים בכך שהעלאת תכנים המפירים זכויות יוצרים היא אסורה, וכן אימוץ מגוון אמצעים טכנולוגיים כדי למנוע הפרת זכויות יוצרים על גבי הפלטפורמה שלה, כמו הליכי יידוע והתראה שונים לדיווח על תכנים מפירים וכן תוכנות לאימות תוכן ולהכרת תוכן.[216]

(**2**) ספק השירות סיפק למשתמשיו כלים לשיתוף לא חוקי של התכנים המפירים או עודד במודע שיתוף כאמור, כפי שאפשר ללמוד מן המודל הכלכלי של ספק השירות.[217] ה־CJEU בחן את אופן פעולתה של פלטפורמת Uploaded ופסק כי מפעילת הפלטפורמה Cyando כלל לא יצרה, בחרה או בדקה את התכנים שהמשתמשים שלה מעלים, ואף לא צפתה בהם, ועל כן לא סיפקה להם כלים להפרת זכות יוצרים. יתרה מכך, Cyando סיפקה רק למשתמש הקצה עצמו קישור לתוכן שהעלה, ולא נתנה בידיו כלים המאפשרים לו לשתף את התוכן עם הציבור.[218]

אם נמצא שספק השירות תרם תרומה חיונית ומכוונת להפרה הישירה של זכות היוצרים, על ה־CJEU לבחון את תחולת החריג לאחריות התורמת – נמל הביטחון הקבוע בסעיף 14 לדירקטיבת ה־E-Commerce. בפרשות **יוטיוב** ו־*Cyando* נפסק שספק שירות יוכל ליהנות מהחריג לאחריות תורמת להפרת זכות יוצרים בידי משתמש הקצה רק בהתקיים אחד התנאים האלה:

215 **שם**, פס' 84.

216 **שם**, פס' 90–96.

217 **שם**, פס' 60–83.

218 **שם**, פס' 98–99.

(**1**) הוא אינו מודע בפועל להפרת זכות יוצרים ספציפית ואין ביכולתו לשלוט בתכנים המועברים באמצעות השירות שהוא מספק.

(**2**) הוא אינו מודע לעובדות או לנסיבות שהובילו להפרת זכות היוצרים, או פעל להסרת התכנים המפירים או למניעת גישה אליהם מייד כאשר למד עליהם.[219]

היעדר מודעות בפועל או בכוח או שליטה כאמור ייתכנו רק כאשר ספק שירות הוא ניטרלי לתכנים.[220] בפרשת *eBay*, למשל, נפסק שהחברה אינה יכולה ליהנות מנמל הביטחון הקבוע בסעיף 14 לדירקטיבת ה־E-commerce שכן היא פועלת למיטוב מודעות הפרסומת של לקוחותיה, וכך יכולה להיחשף למידע הנוגע להצעה למכירה של מוצר המפר זכויות קניין רוחני, או להשיג שליטה במידע כזה.[221]

עם זאת, משטר האחריות החל על ספקי שירות לפי דירקטיבת ה־E-Commerce ופסיקת ה־CJEU בפרשות **יוטיוב** ו־*Cyando* עומד להשתנות בעקבות ה־Digital Service Act (להלן: ה־DSA), שאושר בפרלמנט האירופי באוקטובר 2022 ונכנס לתוקף בינואר 2024.[222] ה־DSA נועד להתאים את המשטר המשפטי בתחום הקניין הרוחני להתקדמויות הטכנולוגיות שהתרחשו מאז כניסתה לתוקף של דירקטיבת ה־E-Commerce לפני עשרים שנה, ובראשן הופעת הפלטפורמות האינטרנטיות, המשמשות כיום כמתווכות העיקריות, כמקור מידע וכמעצבות השיח. ה־DSA הוא נדבך נוסף בניסיון להתאים את אירופה לעידן הדיגיטלי, להגן על הצרכנים ברשת האינטרנט, להבטיח את זכויות היסוד שלהם וליצור מרחב סייבר פתוח ושקוף שבמסגרתו תשגשג החדשנות. הוראות ה־DSA מחליפות את הוראת נמלי הביטחון שבדירקטיבת ה־E-Commerce,[223] ומטרתן ליצור אחידות

219 **שם**, פס' 103–118.

220 **שם**, פס' 104–111.

221 CJEU, C-324/09, L'Oreal SA and Others v. eBay International AG and Others (12.7.2011)

222 סעיף 93 ל־Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Service Act), 2022 O.J. (L 277) 1

223 **שם**, ס' 89.

במשטר האחריות של מתווכים[224] – ספקי שירות המוגדרים "צינורות העברה" (mere conduit), ספקי שירות העברה או מטמון (caching services) או ספקי שירות אחסון. מתווכים עשויים לכלול ספקי רשת אלחוטית מקומית, ספקי שמות מתחם, רשמי שמות מתחם, ספקי רשתות וירטואליות פרטיות, מנועי חיפוש, ספקי שירותי ענן, ספקי שירותי דוא"ל וספקי שירותי Voice Over IP.[225] ה־DSA משמר את עקרונות דירקטיבת ה־E-Commerce באשר להחרגת ספק שירות ניטרלי מאחריות תורמת וכן בכל הנוגע לאחריות המפר הישיר.

ה־DSA מדגיש שהכתובת הראשונה והמרכזית להתמודדות עם תכנים ועם פעולות בלתי חוקיות צריכה להיות משתמשי הקצה המבצעים את הפעולה הבלתי חוקית, ולא ספקי השירות המשמשים כמתווכים.[226] כן משמר ה־DSA את העיקרון שלפיו לא חלה על מתווכים חובת ניטור אקטיבית, ומובהר שפעולותיו הוולונטריות של הספק לאיתור ולזיהוי של תוכן בלתי חוקי, וכן פעולות שהספק נוקט משנתגלה תוכן כזה, המבוצעות בתום לב ובאופן זהיר, אובייקטיבי ומידתי, מתוך התחשבות בזכויותיהם של כלל הצדדים ונקיטת אמצעי זהירות למניעת טעויות והסרה בלתי מוצדקת של תכנים חוקיים, אינן מלמדות כשלעצמן על מודעותו של הספק לתוכן או על שליטה בתוכן המועבר או המועלה בידי המשתמשים לשירות שהוא מספק.[227]

כך, נקבע שלא תוטל אחריות תורמת להפרת זכות יוצרים על ספק המשמש צינור העברה בלבד בהתקיים התנאים האלה: (א) הספק אינו יוזם את העברת התוכן; (ב) הספק אינו בוחר את מקבל התוכן; (ג) הספק אינו בוחר או משנה את התוכן המועבר. כלומר ספק הממלא תפקיד פעיל המאפשר לו שליטה במידע או מודעות לתוכנו, או ספק שירות המשתף פעולה במכוון עם המשתמש לשם פעילות לא חוקית, לא יוכל ליהנות מהחריג לאחריותו לתוכן לא חוקי שהמשתמשים מעלים. עם זאת, ה־DSA מבהיר שהעובדה שהשירות מאפשר

224 **שם**, ס' 2(a).

225 **שם**, ס' הקדמה 28–29, ובהגדרת "intermediary service", ס' 3.

226 **שם**, ס' הקדמה 27.

227 **שם**, ס' 7–8 וס' הקדמה 26 ו־30.

להצפין את התכנים המועברים או לעשות בהם שימוש אנונימי אינה מלמדת, כשלעצמה, על כך שהשירות מכוון לאפשר פעולות בלתי חוקיות.[228]

ספק המספק שירותי מטמון לא יישא באחריות להעברה, לתיווך ולאחסון זמני של תוכן מפר, אשר בוצעה רק למטרה של העברת מידע באופן יעיל ובטוח למשתמשים אחרים של השירות לפי בקשתם, בהתקיים התנאים האלה: (א) אינו משנה את התוכן המועבר; (ב) מציית להוראות ה־DSA בנוגע למתן גישה לתוכן; (ג) אינו מפריע לשימוש חוקי בטכנולוגיה המוכרת בתעשייה לשם השגת מידע על השימוש בתוכן; (ד) פועל להסרת התוכן המפר או לחסימת הגישה אליו מייד כאשר נודע לו שהמידע הוסר ממקור ההעברה או שהגישה אליו נחסמה, או אם רשות משפטית הורתה על הסרתו או על חסימת הגישה אליו.[229]

על ספק שירותי אחסון לא תוטל אחריות תורמת לאחסון תוכן מפר אם לא היה מודע לפעילות הבלתי חוקית או לתוכן המפר, או לא היה מודע לנסיבות שברור מהן שמתרחשת התנהגות לא חוקית או שהתוכן אינו חוקי, כלומר היעדר מודעות בפועל או בכוח, או אם פעל להסרת התוכן הבלתי חוקי או למניעת הגישה אליו מייד כשנודע לו על קיומו. מודעותו של הספק יכולה לנבוע מפעולות שהוא מבצע בעצמו או מהודעה ממי שנפגע מהתוכן הבלתי חוקי. ואולם, עצם העובדה שהספק יודע שהשירות שהוא מציע משמש לאחסון תוכן בלתי חוקי, שהוא מתייג אוטומטית את התכנים המועלים לפלטפורמה שלו או שהוא מאפשר חיפוש בתוכן ומספק המלצות לתוכן על בסיס הפרופיל האישי שהוא מגבש על כל אחד ממשתמשיו, אינה מלמדת על מודעותו בפועל לקיומו של תוכן בלתי חוקי. כמו כן, הסרת התוכן או חסימת הגישה אליו צריכות להיעשות מתוך התחשבות הספק בזכויות בסיסיות של המשתמשים, לרבות הזכות לחופש ביטוי.[230]

228 **שם**, ס' 4 וס' הקדמה 18, 20–21.

229 **שם**, ס' 5.

230 **שם**, ס' 6 וס' הקדמה 22.

2.3 בישראל

הבסיס לדוקטרינת ההפרה התורמת בדין הישראלי מובא בסעיף 12 לפקודת הנזיקין, אשר מאפשר הטלת אחריות משפטית על המייעץ או על המשדל למפר הישיר.[231] כלומר לשם הטלת אחריות משפטית לא נדרשת מערכת יחסים הדוקה בין המפר הישיר למפר התורם, המאפיינת למשל יחסים של עובד ומעסיק או מרשה ושלוח; די בהוכחת קיומה של מערכת יחסים רחוקה יותר המקיימת קשר כלשהו בין המפר הישיר לבין המפר התורם. להטלת אחריות תורמת לעוולה נזיקית שתי הצדקות מרכזיות: האחת, הטלת אחריות על מונע הנזק היעיל; השנייה, הרצון לפצות את הניזוק בהתבסס על עקרון הכיס העמוק, כלומר האחריות מוטלת על מי שיש בידיו האמצעים לעמוד בפיצוי הנדרש לניזוק. עם זאת, המשקל שניתן להצדקה זו הצטמצם במהלך השנים נוכח המשמעות של הטלת אחריות משפטית בהתאם ליכולת הכלכלית.[232]

חדירתה של דוקטרינת ההפרה התורמת לדיני הקניין הרוחני בישראל הייתה הדרגתית. תחילה נסקרה דוקטרינת ההפרה התורמת בפרשת **רגבה** באשר לשאלת האחריות להפרת פטנט. השופטים באותה פרשה חיוו את דעתם שאימוצה של הדוקטרינה בדיני הפטנטים בישראל, תוך כדי קביעת תנאים מגבילים להוכחתה, עשוי להיות בגדר התפתחות חיובית. עם זאת, הם בחרו להימנע מלהכריע בסוגיה והשאירו אותה ב"צריך עיון".[233]

בתחילת שנות האלפיים חל שינוי בעמדת בית המשפט העליון והוא הכיר בקיומה של דוקטרינת ההפרה התורמת בדיני הפטנטים בפסק דינו בפרשת **רב**

231 ס' 12 לפקודת הנזיקין [נוסח חדש], נ"ח התשכ"ח 266: "לענין פקודה זו, המשתף עצמו, מסייע, מייעץ או מפתה למעשה או למחדל, שנעשו או שעומדים להיעשות על ידי זולתו, או מצווה, מרשה או מאשרר אותם, יהא חב עליהם".

232 פישמן אפורי, **לעיל** ה"ש 165, עמ' 41–42.

233 ע"א 7614/96 **צחורי ובניו תעשיות בע"מ נ' רגבה: מושב שיתופי חקלאי**, פ"ד נד(3) 721, 741–742 (2000).

בריח. בית המשפט העליון אזכר בפסיקתו את סעיף 12 לפקודת הנזיקין, הקובע את עקרונות האחריות התורמת במקרה של עוולה נזיקית, והציג את האפשרות לייבא את הדוקטרינה לחוק הפטנטים באמצעות הקביעה כי הפרת פטנט היא בבחינת הפרת חובה חקוקה לפי סעיף 63 לפקודת הנזיקין.[234] אולם ההכרה בקיומה של דוקטרינת ההפרה התורמת בפסק הדין בפרשת **רב בריח** התבססה בעיקרה על התפתחותה בפסיקה בארצות הברית ובגרמניה.[235] נפסק כי לשם הטלת אחריות תורמת להפרת פטנט יש להוכיח את קיומם של התנאים האלה: (א) קיום הפרה ישירה; (ב) הרכיבים שבגינם הוגשה התביעה הם חלק מהותי מן ההמצאה המוגנת בפטנט; (ג) קיום יסוד נפשי – הנתבע ידע בפועל, או שהיה עליו לדעת לפי הנסיבות ובהתאם למבחן האדם הסביר, על ההפרה הישירה; (ד) אין שימוש משמעותי אחר מן השימוש המוגדר בפטנט.[236]

דוקטרינת ההפרה התורמת יובאה לדיני זכויות היוצרים בישראל רק כעבור עשור, בפסק דינו של בית המשפט העליון בפרשת **שוקן**.[237] באותה פרשה נבחנה אחריותה של האוניברסיטה העברית בירושלים לשכפול ולהפצה של יצירה ללא אישור בעל זכויות היוצרים בה – הוצאת שוקן – בידי נציג תא סטודנטיאלי באוניברסיטה תוך כדי שימוש במשאבים שהאוניברסיטה העמידה לרשותו. השופט ריבלין עמד על כך שחוק זכויות היוצרים מכיר בהפרה תורמת באופן מוגבל בהקשר של בעל מקום בידור, כגון תיאטרון או אולם שמחות, וכן בהפרת הזכות לביצוע פומבי; אולם אין החוק מכיר באפשרות העקרונית להטלת אחריות מכוח דוקטרינת ההפרה התורמת.[238]

234 ע"א 1636/98 **רב בריח בע"מ נ' בית מסחר לאביזרי רכב חבשוש (1987) בע"מ**, פ"ד נה(5) 337 (2001), פס' 23 לפסק דינו של השופט אנגלרד (להלן: פרשת **רב בריח**); מיכאל בירנהק "לידתה של עוולה: הפרה תורמת בדיני פטנטים" **טכנולוגיות של צדק: משפט, מדע וחברה** 169, 173 (שי לביא עורך, 2003).

235 פרשת **רב בריח**, **לעיל** ה"ש 233, פס' 25–30 לפסק דינו של השופט אנגלרד; פישמן אפורי, **לעיל** ה"ש 165, עמ' 12.

236 פרשת **רב בריח**, **לעיל** ה"ש 233, פס' 31–35 לפסק דינו של השופט אנגלרד.

237 פרשת **שוקן**, **לעיל** ה"ש 165.

238 ס' 49 לחוק זכות יוצרים, התשס"ח–2007; פרשת **שוקן**, **לעיל** ה"ש 165, פס' 12 לפסק דינו של השופט ריבלין.

בבוחנו את יתרונותיה של דוקטרינת ההפרה התורמת ציין השופט ריבלין כי ייבואה לדיני זכויות היוצרים יאפשר לבעל זכות היוצרים להרחיב את מעגל הנתבעים האפשריים ו"להיפרע ממי שהייתה לו יד בהפרת זכותו", גם כשמדובר במי ש"אינו מבצע את ההפרה בעצמו, אך הוא מאפשר ומתיר את פעילותו המפירה של גורם אחר, או אף מסייע ומעודד את אותה הפעילות. הוא משמש מעין 'גורם ביניים', בשרשרת ההפרה – בטווח שבין המפר הישיר (מפר 'הקצה'), לבין בעל הזכות".[239]

בהמשך פנה השופט ריבלין לסקור את ההצדקות לעיגונה החוקי של זכות היוצרים ואת הרלוונטיות שלהן להכרה בדוקטרינת ההפרה התורמת. ראשית, השאיפה לתגמל את היוצר ולהגן על האינטרסים הקניינים הלגיטימיים שלו מצדיקה גם הטלת אחריות על גורמי ביניים שפעולתם מביאה לפגיעה בזכויותיו של היוצר. כך יוכל היוצר להיפרע מכל מי שהיה מעורב בהפרת זכויותיו. שנית, החשש מפני פגיעה בתמריצי של היוצר ליצור וההשלכות של פגיעה זו על החברה ועל החדשנות עומדים בבסיס ההכרה בזכות היוצרים וההגנה עליה, ורלוונטיים גם להצדקת ההכרה במפר תורם. זאת נוכח כשל השוק, שהופך את אכיפת זכות היוצרים נגד כל אחד מהמפירים הישירים ליקרה ולבלתי יעילה כלכלית ומוביל לאכיפת חסר העלולה לפגוע בתמריץ של היוצר להמשיך וליצור. מתן כלי בידיו של בעל זכות היוצרים לתבוע את המפר התורם, שהוא גוף יחיד ומוכר, פותר כשל שוק זה ומבטיח גמול ראוי ליוצר והמשך ההגנה על תמריציו. הצדקה נוספת להטלת אחריות על המפר התורם נעוצה בהיותו מונע הנזק הזול, דהיינו הגורם שיכול לפקח ביעילות ובאופן פשוט וזמין יחסית על המפירים הישירים.[240]

עוד נשען השופט ריבלין על ההכרה בדוקטרינת ההפרה התורמת בפסיקה בארצות הברית ובפסיקת בית המשפט העליון בפרשת **רב בריח**. דיני הפטנטים ודיני זכויות יוצרים משתייכים לאותה "משפחת" דינים, ועל כן הם עשויים להשפיע זה על זה, אגב התאמה למאפייניו הייחודיים של כל משטר. כן מציין השופט ריבלין את הוראת סעיף 12 לפקודת הנזקין כצינור הקליטה של

239 **שם**, פס' 11–12.

240 **שם**, פס' 13–15.

הדוקטרינה לדיני זכויות היוצרים, שכן הפרת זכות יוצרים נחשבת עוולה אזרחית שפקודת הנזקין חלה עליה, בשינויים המתחייבים נוכח תכלית חוק זכויות יוצרים – המשקף איזון עדין בין גמול ליוצר על השקעתו והבטחת תמריצים להמשך היצירה, לבין הגנה על זכויות המשתמשים ועידוד פלורליזם במרחב הציבורי.[241] לפיכך נקבעו בפסק הדין בפרשת **שוקן** שלושה תנאים מצטברים לתחולתה של אחריות תורמת להפרת זכות יוצרים. תנאים אלו מבטאים יישום זהיר של דוקטרינת ההפרה התורמת ומזעור הפגיעה במשתמשים ובמרחב הציבורי:[242]

(**1**) **קיומה בפועל של הפרה ישירה**. משמעות דרישה זו היא שהטלת אחריות על מפר תורם תתאפשר רק כאשר אכן מופרת זכות היוצרים. עם זאת, תנאי זה עשוי להתקיים אף אם פעולתו של המפר הישיר חוסה תחת אחד מהחריגים הקבועים בחוק זכות יוצרים, כגון חריג השימוש ההוגן, משום שהגנות אלו מונעות מהמפר לשאת באחריות להפרה, אך אינן מאיינות את עצם ההפרה. נוסף על כך, ייתכן שהנזק הנגרם מפעולתו של כל אחד מהמפירים הישירים אינו גדול, ואף עשוי לחסות תחת אחת מן ההגנות הקבועות בחוק זכות יוצרים, אולם הנזק המצטבר הנגרם מההפרה על ידי כל המפירים הישירים הוא גדול, וחוסר היכולת של בעל זכות היוצרים לקבל פיצוי בגינו הוא כשל אכיפה שדוקטרינת ההפרה התורמת באה לפתור.[243]

(**2**) **מודעותו של המפר התורם להפרה הישירה**. לדרישת המודעות כמה הצדקות. ראשית, היא עולה בקנה אחד עם הדרישות שנקבעו בפסיקה להוכחת אחריות מכוח סעיף 12 לפקודת הנזיקין. שנית, מנקודת מבטה של החברה בכללותה, הטלת אחריות על מונע הנזק היעיל תיתכן רק כאשר היה

241 **שם**, פס' 18, 20–23 לפסק דינו של השופט ריבלין, ופס' 3 לפסק דינו של השופט דנציגר; סעיף 52 לחוק זכות יוצרים: "הפרה של זכות יוצרים או זכות מוסרית היא עוולה אזרחית, והוראות פקודת הנזיקין [נוסח חדש] יחולו עליה, בשינויים המחוייבים ובכפוף להוראות חוק זה".

242 **שם**, פס' 18, 20–23 לפסק דינו של השופט ריבלין; פישמן אפורי, **לעיל** ה"ש 165, עמ' 8–10.

243 פרק ד' לחוק זכות יוצרים; פרשת **שוקן**, **לעיל** ה"ש 165, פס' 24 לפסק דינו של השופט ריבלין.

ביכולתו למנוע את ההפרה. יכולת זו מותנית במודעותו של המפר התורם לעצם ביצועה של ההפרה על ידי המפר הישיר. הצדקות אלו מחייבות ידיעה ממשית וקונקרטית כחלק מדרישת המודעות, ואין די בידיעה קונסטרוקטיבית כללית. זאת משום שהסתפקות בידיעה בכוח בלבד עשויה להטיל נטל כבד מדי על כתפי גורמי הביניים, להצר את פעולתם החופשית בשוק ולהטלת אחריות רבה מדי עליהם. ואולם, אין צורך בהוכחת ידיעת המפר התורם על כל אחת ואחת מההפרות הספציפיות, שכן דרישה שכזו הייתה יוצרת את אותו כשל אכיפה שבו נתקל בעל הזכות למול המפירים הישירים הרבים: גם גורם הביניים אינו מודע לפעילותו של כל אחד ואחד מהמפירים הישירים. לפיכך נפסק שדי במודעות בפועל לקיומה של פעילות מפירה.[244]

(**3**) **קיומה של תרומה משמעותית, ניכרת וממשית לביצוע ההפרה.**[245] דרישה זו נשענת על לשון סעיף 12 לפקודת הנזיקין, המציג כמה פעולות אשר עשויות ללמד על תרומה משמעותית של גורם הביניים להפרה: שיתוף, סיוע, ייעוץ, פיתוי, ציווי, הרשאה או אשרור של ההפרה הישירה.

קיומו של תנאי זה ייבחן לפי נסיבות המקרה, ובית המשפט יביא בחשבון את מכלול פעולותיו של גורם הביניים, את מעורבותו בשרשרת האירועים שהביאה להפרה ואת יכולתו למנוע אותה בנקיטת אמצעים סבירים. אם המפר התורם יכול למנוע את ההפרה במאמצים סבירים אך נמנע מכך, הרי שמתקיים תנאי זה והימנעותו מפעולה נחשבת תרומה משמעותית. בחינה זו תואמת את תאוריית מונע הנזק היעיל: אם המפר התורם נדרש לנקוט אמצעים יקרים ובלתי סבירים כדי למנוע את ההפרה, לא עומדת עוד ההצדקה הכלכלית להטיל עליו אחריות תורמת שכן אינו מונע הנזק היעיל. לפיכך, סבירות האמצעים נמדדת במונחים כלכליים של עלותה של פעולת מניעת הנזק. אם העלות אינה זניחה, אין הצדקה להטילה דווקא על גורם הביניים.[246] בספרות הוצע כי בבחינת סבירות האמצעים שגורם הביניים נקט יש לתת משקל לקוד הפעולה המקובל בענף הרלוונטי. לשם הגברת הוודאות המשפטית בהחלת דוקטרינת ההפרה התורמת, יש לצאת

244 **שם**, פס' 25.

245 **שם**, פס' 23.

246 **שם**, פס' 26–27.

מנקודת הנחה שציות לסטנדרט הפעולה המקובל בתעשייה מלמד על סבירות האמצעים שנוקט גורם הביניים.[247]

עוד הבהיר השופט ריבלין בפרשת **שוקן** שאין צורך בהוכחת קשר סיבתי במובנו הצר, כלומר בהוכחה שפעילות המפר התורם הייתה תנאי הכרחי לקיומה של ההפרה הישירה, אלא די בהיותה חלק אינטגרלי ומשמעותי בשרשרת הפעולות שהובילו להפרה הישירה.[248] על פרשנות זו נמתחה ביקורת בנימוק שהיא עלולה לפגוע בוודאות המשפטית ולהביא לתחולה רחבה מדי של דוקטרינת ההפרה התורמת. למשל, יהיה אפשר לטעון שיש להטיל על חברת החשמל אחריות תורמת להפרת זכות יוצרים, שכן ללא חשמל לא היה אפשר להפעיל את המחשבים שבאמצעותם בוצעה ההפרה. מנגד, גם דרישה שמעורבותו של המפר התורם תהיה ישירה עד כדי הגדרתו כמעוול במשותף אינה רצויה, שכן היא עלולה לרוקן מתוכן את דוקטרינת ההפרה התורמת. הוצע שדרישת התרומה המשמעותית תפורש כדרישה להוכחת מעורבות גבוהה מאוד עד כדי הפרה ישירה על ידי גורם הביניים – כלומר להבחין בין גורם ביניים המספק אמצעים היקפיים בלבד ותרומתו פסיבית לבין גורם ביניים הפועל באופן אקטיבי לשם ביצוע הפעולות המפירות. לצד זאת הוצע שאם בשירות שגורם הביניים מספק נעשה גם שימוש חוקי משמעותי, אזי לא מתקיים קשר סיבתי בין מעשה ההפרה לפעולותיו של גורם הביניים ולא מתקיים תנאי התרומה המשמעותית.[249]

בפרשת **שוקן** נפסק שתנאי התרומה המשמעותית, הממשית והניכרת לא התקיים לגבי האוניברסיטה העברית בירושלים. אומנם תרומתה של האוניברסיטה להפרת זכויות היוצרים הייתה תרומה שבמחדל, והיא לא פעלה כלל למניעת ההפרה. עם זאת, האוניברסיטה אינה בגדר מונע הנזק היעיל; היא אינה יכולה לפקח באמצעים סבירים על פעולותיהם של התאים הסטודנטיאליים

247 פישמן אפורי, **לעיל** ה"ש 165, עמ' 50–61.

248 פרשת **שוקן**, **לעיל** ה"ש 165, פס' 26–27 לפסק דינו של השופט ריבלין.

249 פישמן אפורי, **לעיל** ה"ש 165, עמ' 50–61.

או של כל סטודנט וסטודנט, ולמנוע את הפרות זכויות היוצרים שנגרמות בשל מעשיהם.[250]

בפרשת **א.ל.י.ס.** (2011) יישם בית המשפט המחוזי את דוקטרינת ההפרה התורמת בעניין הפרת זכות יוצרים. באותה פרשה הגישה חברה העוסקת בהגנה על זכויות יוצרים בסרטים תביעה נגד מפעילי אתר אינטרנט שבו מתנהלים פורומים מקוונים, ובהם שני פורומים שהכניסה אליהם מותנית ברישום ובתשלום דמי חבר – פורום אחד שכותרתו "הורדות" ופורום שני שנקרא "סרטים וטלוויזיה". בתביעה נטען כי משתמשי הפורומים, ובעיקר הפורומים שבתשלום, מציבים בהם קישורים לאתרי אינטרנט שמהם אפשר להוריד באופן בלתי חוקי סרטי קולנוע המוגנים בזכויות יוצרים, ועל מפעילי האתר לשאת באחריות תורמת להפרה הישירה. בפסק דינו עמד בית המשפט המחוזי על הצורך באיזון בין השיקולים והאינטרסים הבאים: היותו של גורם הביניים מונע הנזק הזול למול האינטרס שלו שלא לשאת בעלות ניטור תוכן בעת מתן השירות על ידו, האינטרס של בעל זכות היוצרים להגן על זכויותיו ביעילות, והאינטרס החברתי בהגנה על חופש הביטוי ובהימנעות מצינון פעילות חברתית רצויה באמצעות יצירת מנגנוני אחריות ופיקוח יקרים. עוד הצביע בית המשפט על היעדר הסדר הולם בחוק לאחריות ספק שירות, שבעטיו נאלץ בית המשפט להפעיל כללים מהמשפט הפרטי ולהתאימם לנסיבות המקרה ולטכנולוגיה הרלוונטית.[251]

בפסיקתו בפרשת **א.ל.י.ס.** הדגיש בית המשפט המחוזי כי הבסיס הסטטוטורי להחלת דוקטרינת ההפרה התורמת בדיני זכויות היוצרים בישראל הוא סעיף 12 לפקודת הנזיקין באמצעות "צינור הקליטה" הקבוע בסעיף 52 לחוק זכויות היוצרים, אשר מבהיר שהפרת זכות יוצרים היא עוולה אזרחית שפקודת הנזיקין חלה עליה – זאת לצד הצדקות נורמטיביות נוספות, לרבות פתרון לכשל השוק

250 פרשת **שוקן, לעיל** ה"ש 165, פס' 28 לפסק דינו של השופט ריבלין.

251 ת"א (מחוזי מר') 09-08-567 **א.ל.י.ס. אגודה להגנת יצירות סינמטוגרפיות (1993) בע"מ נ' רוטר. נט בע"מ** (נבו 8.8.2011), פס' 18–19, 21 לפסק הדין (להלן: פרשת **א.ל.י.ס.**).

הפוגע בהגנה על זכות היוצרים ובתמריץ היוצר להמשיך וליצור וכן עקרון מונע הנזק היעיל.[252]

בבחינת קיומם של התנאים להחלת דוקטרינת ההפרה התורמת, כפי שנקבעו בפרשת **שוקן**, הגיע בית המשפט המחוזי למסקנה כי בנסיבות המקרה בפרשת **א.ל.י.ס.** דרישת המודעות של גורם הביניים תתקיים רק אם בעל זכות היוצרים הודיע לו על קיומה של יצירה מפירה. הנימוק לצמצומה של דרישת המודעות באופן זה היה שבנסיבות המקרה, הטלת אחריות תורמת ללא הודעה קודמת מבעל זכות היוצרים משמעה החלת חובה רחבה של ניטור תכנים על גורם הביניים. החלת חובת ניטור כזו אינה עולה בקנה אחד עם פסיקת בית המשפט העליון בפרשת **שוקן**, שהדגישה שנדרשת מודעות בפועל ולא בכוח. חובת ניטור אף אינה רצויה מן הבחינה החברתית, שכן היא הופכת את גורם הביניים לעורך תוכן ובכך מגבירה את החשש מצנזורה ומפגיעה בחופש הביטוי של ציבור המשתמשים באתר.[253] בקביעה זו אימץ בית המשפט את פרשנות דרישת המודעות שבה דגל בית המשפט במחוז התשיעי בפרשת **גרוקסטר**. אולם, פרשנות זו נדחתה במפורש בידי בית המשפט העליון האמריקני בפרשת **גרוקסטר** בפסק הדין בראשותו של השופט סוטֶר.[254]

בפסק דינו בפרשת **א.ל.י.ס.** הבהיר בית המשפט המחוזי גם את המבחנים הראויים לקביעה אם הנתבע הוא מונע הנזק היעיל, כלומר את סבירות האמצעים שעל הנתבע לנקוט כדי למנוע את ההפרה. המבחן הראוי, לפי פסק הדין, הוא מבחן דו־ראשי: בחלקו האחד זהו מבחן יעילות הבוחן אם עלויות הפיקוח המצטברות שבעל זכות היוצרים צריך לשאת בהן כדי להגן על זכויותיו גבוהות יותר מעלויות הפיקוח המצטברות שעל הנתבע לשאת בהן, במקרה זה מפעיל אתר הפורומים. בחלקו השני זהו מבחן של צדק חלוקתי, אשר בודק אם הסטת עלויות הפיקוח המצטברות מבעל זכות היוצרים לנתבע או לגורמים כמותו, במקרה של פסק הדין – בעלי אתרים שבהם מתנהלים פורומים שהגולשים מפרסמים בהם קישורים לאתרים המאפשרים העתקה ללא רשות של יצירות מוגנות, היא הסטה מוצדקת. במסגרת מבחן הצדק החלוקתי, בית המשפט מביא בחשבון

252 **שם**, פס' 45–47.

253 **שם**, פס' 43, 45–46.

254 ראו דיון בטקסט הנלווה, לעיל ה"ש 183–184.

את אינטרס הציבור ואת הערך החברתי שבפעילותו של הנתבע, כפי שבא לידי ביטוי בחריג השימוש החוקי המשמעותי שנקבע בפרשת **סוני**.[255]

בדומה להתפתחות דוקטרינת ההפרה התורמת בארצות הברית ובאיחוד האירופי, וכן ברוח פסיקת בית המשפט העליון בפרשת **שוקן**, בית המשפט המחוזי מבהיר בפסק דינו בפרשת **א.ל.י.ס.** שתיתכן הטלת אחריות תורמת על גורם ביניים גם כאשר לא ניתנה לו הודעה כנדרש, בשני מצבי קיצון או חריגים מרכזיים:[256]

הראשון הוא "חריג העידוד": בדומה לפסיקת בית המשפט העליון בארצות הברית בפרשת **גרוקסטר**, כאשר גורם הביניים מעודד באופן אקטיבי את הפרת זכות היוצרים, הרי שהוא מודע להפרה וגם תורם לה תרומה משמעותית, ולכן עליו לשאת באחריות תורמת להפרה. בבחינת העידוד מצד גורם הביניים יביא בית המשפט בחשבון, בין השאר, את שם השירות שגורם הביניים מספק, את אופן שיווקו בציבור ואת הנחיות השימוש בו.[257]

השני הוא "חריג הפורום הפסול": כאשר פורום מסוים מבין הפורומים המופעלים באתר משמש רובו ככולו להצבת קישורים לאתרים מפירים, ובעל האתר מודע לכך, אף אם לא עודד זאת, עליו לחסום את הגישה לפורום. אם לא עשה כן, עליו לשאת באחריות תורמת להפרת זכות היוצרים. הקביעה אם פורום משמש רובו ככולו להצבת קישורים לאתרים מפירים תישען על בחינת היקף הקישורים לאתרים המפירים בהשוואה להיקף שאר הפעילות בפורום, וכן על בחינה מוחלטת – מספר הקישורים המפירים שפורסמו בפורום. עוד ישקול בית המשפט את שאלת הגישה לפורום: אם מדובר בפורום סגור, שהגישה אליו מוגבלת למשתמש רשום או למשתמש המשלם דמי שימוש, יקשה על בעל זכויות היוצרים לפקח ביעילות על פעילותו ולנטר את הצגת התכנים המפירים. משום כך, פורום סגור שמתקיים בו כלל האצבע שהציג בית המשפט, ולפיו בפורום יש יותר מעשרה קישורים לאתרים מפירים וההודעות הכוללות קישורים כאמור הן יותר מרבע מהתוכן המהותי בפורום, חשוד כפורום פסול, וקמה

255 פרשת **א.ל.י.ס.**, **לעיל** ה"ש 250, פס' 48, 50–51.

256 **שם**, פס' 55.

257 **שם**, פס' 56.

חזקה שלפיה מפעיל הפורום מודע להפרות ותורם להן משמעותית. לפיכך הוא עלול לשאת באחריות תורמת אם לא יצליח להפריך את החזקה. כאשר הכניסה לפורום פתוחה לכלל הגולשים, בית המשפט מחמיר יותר בקביעה אם זהו פורום פסול, וכלל האצבע שנקבע הוא שמחצית מהתוכן המהותי בפורום כולל קישורים לאתרים מפירים.[258] בפרשת **א.ל.י.ס.** התייחס בית המשפט רק לנסיבות המקרה שלפניו, אולם אפשר להבחין כי חריג זה הוא תמונת מראה של חריג השימוש החוקי המשמעותי מפרשת **סוני**: שם דובר בקיומו של שימוש חוקי משמעותי, ושופטי בית המשפט העליון בפרשת **גרוקסטר** נמנעו מלקבוע אמות מידה כמותיות ברורות לקיומו של החריג,[259] ואילו כאן ההתמקדות היא במרכזיותו של השימוש הבלתי חוקי תוך כדי ניסיון להגדירו באופן כמותי.

2.4
סיכום ביניים: דוקטרינת ההפרה התורמת בראי המשפט המשווה

טכנולוגיות דו־שימושיות מציבות זה כמה עשורים אתגרים משפטיים לפני בעלי זכויות היוצרים. אלו ביקשו להיעזר ביצרני הטכנולוגיה לשם אכיפת זכויותיהם, תוך כדי התמודדות עם כשל האכיפה שנבע מקיומם של מפירים ישירים רבים ומפוזרים, וניצול היותם של יצרני הטכנולוגיה הדו־שימושית מונע הנזק הזול. הטלת אחריות תורמת על יצרני הטכנולוגיה סיפקה את האפיק המתאים להפיכתם לזרוע האכיפה הארוכה של בעלי זכות היוצרים, תוך כדי איזון בין ההגנה על זכות היוצרים ובין אינטרס הציבור בעידוד חדשנות וזרימה חופשית של רעיונות, מידע ומסחר.

מסקירת המשפט המשווה המובאת בקצרה בלוח 2 להלן עולה שבשלושת המשטרים המשפטיים שנבדקו – בארצות הברית, באיחוד האירופי ובישראל –

258 **שם**, פס' 57.

259 ראו את הטקסט הנלווה, **לעיל** ה"ש 185.

אומצו הסדרים דומים, בפסיקה או בחקיקה, בנוגע להיקפה של האחריות התורמת של גורם הביניים להפרת זכות יוצרים בידי המשתמשים בשירותים. עם זאת, המגמה הברורה העולה מסקירת המשפט המשווה היא קיומו של מרוץ "חתול ועכבר" בין המשפט ובעלי זכויות היוצרים לבין מפתחי הטכנולוגיה: האחרונים למדו בכל שלב מהו הכלל המשפטי ופיתחו דרכים יצירתיות כדי לעקוף אותו ולהמשיך לאפשר למשתמשיהם להפר זכויות יוצרים בלי לשאת באחריות תורמת לכך.

ואולם, לאחר האימוץ של דוקטרינת ההפרה התורמת ושל מדיניות ההודעה וההסרה בחקיקה ובפסיקה בערכאות הגבוהות בסוף שנות התשעים ובתחילת שנות האלפיים, פחתו מאוד תביעות מצד בעלי זכויות יוצרים נגד מפעילים של טכנולוגיות דו־שימושיות המאפשרות הפרת זכות יוצרים, ונדמה גם שהצטמצם פיתוחן של טכנולוגיות המזלזלות באופן בוטה בזכויות יוצרים. גם בגזרת החקיקה נרשמת יציבות, ויוזמות החקיקה האחרונות באיחוד האירופי נוגעות בעיקר לאחריות של פלטפורמות אינטרנטיות להבטחת מרחב סייבר בטוח והגון עבור הצרכנים, ואינן מתמקדות דווקא בהפרת זכויות יוצרים. בד בבד התפתחו מודלים טכנולוגיים ועסקיים המאפשרים צריכת יצירות מוגנות בזכויות יוצרים בקלות ובעלות נמוכה בכל רחבי העולם תוך כדי כיבוד זכויות היוצרים לצד עידוד חדשנות ותחרות בשוק – למשל באמצעות שירותי מוזיקה בתשלום דוגמת ספוטיפיי, דיזר ואפל מיוזיק או שירותי טלוויזיה דוגמת נטפליקס.

הזכות לפרטיות אינה זוכה לשדולה חזקה כמו זכות היוצרים. עד כה לא ידוע על מקרים שבהם עובדים שפרטיותם נפגעת התאגדו לפעולה משותפת נגד הפגיעה החמורה בזכותם החוקתית, כפי שעשו בעלי זכויות היוצרים לפני כשלושים שנה עם הופעת תוכנות שיתוף הקבצים. עם זאת, התהליך שהתרחש במשפט ובטכנולוגיה לגבי זכות היוצרים עשוי דווקא לחזק את העמדה שלפיה יש להפקיד בידי בעלי הזכויות כלים משפטיים נוספים בדמות דוקטרינת ההפרה התורמת, כדי לחזק את ההגנה על הזכות לפרטיות ולהביא, בסופו של דבר, להתפתחויות טכנולוגיות אשר יכבדו את הזכות וכן ייתנו מענה הן לצרכיהם העסקיים של המעסיקים בפיקוח על עובדיהם לשם הגברת יעילותם, והן לצורכי החברה הקשורים בקדמה וביעילות כלכלית ומימוש היתרונות הטמונים במתווה עבודה היברידי.

לוח 2
דוקטרינת ההפרה התורמת: סקירת משפט משווה

ארצות הברית	יציר המשפט המקובל. התנאים להחלתה: (1) **הוכחת הפרה ישירה**. יש להוכיח שמתבצעת הפרה של זכות יוצרים מוגנת. (2) **מודעות גורם הביניים**. כאשר קיים שימוש חוקי משמעותי, נדרשת הוכחת מודעותו להפרה, אך לא ברור אם די בהוכחת עצימת עיניים. עם זאת, לא ברור אם יש צורך בהוכחת שימוש חוקי משמעותי בפועל או שדי בהוכחת היתכנות טכנולוגית לשימוש חוקי כאמור. בהיעדר שימוש חוקי משמעותי, די בהוכחת מודעות בכוח להפרה ספציפית. אין די בהוכחת מודעות כללית לקיומם של שימושים מפירים. (3) **תרומה משמעותית**. אין די בהוכחה שגורם הביניים שימש "צינור" גרידא לפעילות מפירה או שהפיק תועלת מן הפעילות המפירה. מנגד, מתן משאבים או תשתית לפעילות מפירה מספיקים להוכחת דרישת התרומה המשמעותית. בשנת 1998 גובש ה־DMCA הכולל "נמלי ביטחון" להחרגת ספקי שירות אינטרנטיים מאחריות ישירה, עקיפה או תורמת להפרת זכויות יוצרים שמבצעים משתמשיהם. ספקי השירות נדרשים לעמוד בכמה תנאים כדי ליהנות מהגנת נמל הביטחון הרלוונטי לעיסוקם, וביניהם מדיניות "הודעה והסרה" והוכחת היעדר מודעות בפועל או בכוח להפרה. בפסיקה פורשה מודעות בכוח כמתקיימת בנסיבות מצומצמות שבהן ההפרה ברורה, כפי שאפשר לרוב להוכיח בהתבסס על הודעה מטעם בעל זכות היוצרים. ספק השירותים אינו נדרש לבחינה נוספת כדי לאשש את דבר קיומה של ההפרה. הלכה למעשה, פרשנות זו מובילה להקבלה מלאה כמעט בין מודעות בכוח לבין מודעות בפועל. עוד נפסק כי רק עצימת עיניים מכוונת לנוכח מידע על הפרה ספציפית תוכר כמודעות בכוח.
באיחוד האירופי	לפי דירקטיבת ה־DSM, סטנדרט האחריות המוטל על ספק תוכן שיתופי באינטרנט הוא מחמיר. עליו לפעול מראש לקבלת רישיון מבעל זכות היוצרים ולהטמיע אמצעים טכנולוגיים למזעור הפרות, בהתאם למבחני סבירות ומידתיות. הספק יימצא אחראי להפרה בכפוף למודעות בפועל בעקבות הודעה מתאימה מבעל זכות היוצרים. ספקי תוכן שיתופי באינטרנט שמטרתם העיקרית היא לאפשר הפרת זכויות יוצרים לא יורשו ליהנות מהגנת דירקטיבת ה־DSM. לפי דירקטיבת ה־DSA, ספק שירותי אחסון לא יישא באחריות תורמת להפרת זכויות יוצרים המבוצעת על ידי משתמשיו אם יוכיח היעדר מודעות בכוח או בפועל או יוכיח שפעל להסרת התוכן מייד עם רכישת מודעות בפועל. מודעות כללית לכך שהשירות המסופק על ידיו יכול לשמש להפרת זכות יוצרים אינה מַספקת לשם הכרה במודעות בכוח.

ישראל	דוקטרינת ההפרה התורמת נשענת על סעיף 12 לפקודת הנזיקין. התנאים להחלתה לפי פסק הדין של בית המשפט העליון בפרשת **שוקן**: (א) קיומה של הפרה ישירה; (ב) מודעות ממשית וקונקרטית לקיומה של פעילות מפירה. לא נדרשת מודעות ממשית על כל הפרה ספציפית; (ג) תרומה משמעותית, ניכרת וממשית לביצוע ההפרה. בפרשת **א.ל.י.ס.** פירש בית המשפט המחוזי את דרישת המודעות כמחייבת הודעה בדבר קיומה של הפרה, ופסק כי בהיעדר מודעות, תוטל אחריות תורמת רק בנסיבות קיצון מוגבלות: המפר התורם שידל את ההפרה הישירה; או התקיים חריג "הפורום הפסול", שהגדרתו מבטאת ניסיון של בית המשפט המחוזי לקבוע היקף כמותי לשימוש לא חוקי.

פרק 3

אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות: בסיס עיוני ושיקולי מדיניות

בפרקים הקודמים התמקדנו בחשיבותה של הזכות לפרטיות במסגרת יחסי עבודה, סקרנו את השימוש הגובר בטכנולוגיות מעקב אחר עובדים, עמדנו על החשש מפגיעה חמורה בזכות העובד לפרטיות, ותיארנו את התפתחות דוקטרינת ההפרה התורמת ככלי משלים להגנה על זכות היוצרים. בפרק זה נעסוק בסוגיה העיקרית למחקר זה: האם ניתן לאמץ את דוקטרינת ההפרה התורמת לדיני הפרטיות כמענה לפגיעה החמורה בזכות לפרטיות בעקבות השימוש בטכנולוגיות מעקב במסגרת יחסי עבודה? אם כן – מהם שיקולי המדיניות המצדיקים אימוץ כזה ומהן השפעותיו האפשריות לחיוב ולשלילה?

אימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים נשען על דוקטרינת האחריות התורמת מפקודת הנזיקין,[260] שדיני זכויות היוצרים נחשבים חוקי לוויין שלה.[261] בישראל, פגיעה בפרטיות היא עוולה אזרחית, והוראות פקודת הנזיקין חלות עליה.[262] לפיכך, ניתן, לכאורה, לאמץ את דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות מתוך שימוש באותו בסיס נורמטיבי – צינור הקליטה הקבוע בסעיף 12 לפקודת הנזיקין שלשונו:

> לעניין פקודה זו, המשתף עצמו, מסייע, מייעץ או מפתה למעשה או למחדל, שנעשו או שעומדים להיעשות על ידי זולתו, או מצווה, מרשה או מאשרר אותם, יהא חב עליהם.

דוקטרינת ההפרה התורמת בדיני זכויות יוצרים משמשת כלי משפטי להרחבת מעגל האחראים בנזיקין. כך, גורמי הביניים, למשל יצרני מוצר טכנולוגי, ספקי הגישה לאינטרנט, בעלי אתרים שבהם מועבר מידע, מפעילי פלטפורמות רשתות חברתיות ומנועי חיפוש, עשויים לשאת באחריות תורמת להפרת זכות היוצרים

260 ס' 11 ו־12 לפקודת הנזיקין [נוסח חדש], התשכ"ח–1968.

261 פישמן אפורי, **לעיל** ה"ש 165, עמ' 10; בירנהק, לידתה של עוולה, **לעיל** ה"ש 233, עמ' 173.

262 ס' 4 לחוק הגנת הפרטיות, התשמ"א–1981.

שמבצעים משתמשי הקצה. ההכרעה בשאלת הטלת אחריות תורמת על גורמי הביניים, כלומר בשאלה אם ראוי שישמשו שומרי סף הנושאים באחריות להתנהגות פסולה שלא הם ביצעו, מתקבלת בהתאם לשיקולי מדיניות ויעילות אכיפה.[263] אימוצה של דוקטרינת ההפרה התורמת לדיני זכויות יוצרים סימן את האיזון הראוי, לפי שיקולי מדיניות, בין חדשנות טכנולוגית לבין הזכות הקניינית של יוצרים.[264] הקביעה אם נתבע חב באחריות תורמת להפרת זכות יוצרים היא בסופו של דבר קביעה המבוססת על איזון בין המחיר החברתי והכלכלי שבפגיעה בזכות יוצרים לבין המחיר הכלכלי והחברתי שבהפיכת צדדים שלישיים לזרוע האכיפה הארוכה של בעל זכות היוצרים ולפגיעה בחדשנות ובשימושים מותרים אפשריים.[265]

אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יוביל לתוצאה זהה של הרחבת מעגל האחראים להפרת הזכות לפרטיות מעבר למפר הישיר. מן הבחינה הזו אימוצה מחזק את הזכות לפרטיות באמצעות יצירת עוולה חדשה המשנה את האיזון הקיים בין הזכות לפרטיות לבין אינטרס הציבור לחדשנות טכנולוגית וזכות הקניין של המעסיק. משום כך, בבואנו להכריע בדבר קליטתה של עוולת ההפרה התורמת החדשה לדיני הגנת הפרטיות יש לבחון תחילה את הבסיס העיוני להצדקת אימוצה ואת שיקולי המדיניות ויעילות האכיפה הרלוונטיים, ולהתמודד עם הקשיים המשמעותיים שאימוץ זה עלול לעורר.[266] בעת בחינה זו אעמוד על הדומה ועל השונה בין זכות היוצרים, שהיא זכות קניינית במהותה, לבין הזכות לפרטיות, ובעיקר בהקשר של זכות העובד לפרטיות.

263 פישמן אפורי, **לעיל** ה"ש 165, עמ' 4.

264 Moye, **לעיל** ה"ש 154, עמ' 653.

265 Yen, **לעיל** ה"ש 183, עמ' 214.

266 בדומה למה שהתרחש עם ייבואה של העוולה לדיני הפטנטים ומאוחר יותר לדיני זכות היוצרים. ראו בירנהק, לידתה של עוולה, **לעיל** ה"ש 233, עמ' 186–196.

3.1
שיקולי מדיניות להצדקת אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכלל ובהקשר של יחסי עבודה בפרט

3.1.1. חיזוק הזכות לפרטיות והערכים שבבסיסה

בדומה לדוקטרינת ההפרה התורמת, שהביאה להרחבת זכות הקניין הרוחני, בפטנט או ביצירה,[267] אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יוביל לחיזוק הזכות לפרטיות באמצעות הרחבת מעגל האחראים להפרתה. בעקבות ההתפתחויות הטכנולוגית המלוות אותנו בעשורים האחרונים נשחקה הזכות לפרטיות,[268] ולכן הכרחי לחזקה. מדובר בזכות חשובה לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו ללא התערבות זרה.

שוקי המידע מאופיינים בכמה כשלי שוק המונעים הגנה ראויה לזכות לפרטיות ומצדיקים התערבות חיצונית, שמטרתה לחזק את הזכות לפרטיות. ראשית, לפגיעה בזכות לפרטיות מגוון החצנות שליליות שלחברות המסחריות אין תמריץ למנוע אותן. אחד הכשלים הוא שעיבוד מידע אישי על אודות אדם עשוי להשפיע על צד שלישי. כך למשל, בדיקת דנ"א של אדם עשויה להוביל לחשיפת פשע שביצע קרוב משפחתו בעבר.[269] החצנה שלילית נוספת נובעת משימוש במכשירים מסוג האינטרנט של הדברים, המסוגלים לאסוף ולנתח

267 **שם**, עמ' 193–195.

268 ראו למשל Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019)

269 יוסף ישראל "איחוד משפחות וסודות אפלים: בדיקות ה־DNA שמסעירות את העולם" **רשת 13** (1.10.2019).

מידע אישי לא רק של בעל המכשיר אלא גם של כל מי שבסביבתו או מתקשר עימו.[270]

כשל שוק משמעותי נוסף, המשמש להצדקת רגולציה לחיזוק הזכות לפרטיות, הוא מידע א־סימטרי. לרוב מנוסחת מדיניות הפרטיות של החברות המסחריות בהרחבה ובצורה מעורפלת. מאחר שעיקר מטרתן של החברות במתן השירות או המוצר היא איסוף מידע אישי על צרכניהן, אין להן תמריץ ליצור מדיניות פרטיות ברורה וקצרה שתאפשר לצרכנים ללמוד בקלות ובבהירות איזה מידע נאסף עליהם ולאילו מטרות הוא משמש. לפיכך, התעמקות במדיניות הפרטיות ומאמץ להבין את היקף איסוף המידע האישי והשימוש הצפוי בו כרוכים בעלויות גבוהות, אשר מובילות צרכנים בדרך כלל להימנע מלשאת בהן וגורמות להם להסכים באופן עיוור. יתרה מזאת, קשה עד בלתי אפשרי לאתר בדיעבד איזו חברה אחראית לשימוש מזיק במידע אישי, ולכן בדרך כלל השוק אינו מצליח להזהיר צרכנים מפני חברות שנהגו בעבר בחוסר הוגנות.[271]

לבסוף, כשל שוק מוכר, המאפיין גם הוא שוקי מידע אישי, הוא הפעולה הקולקטיבית: כדי להגן על הזכות לפרטיות, למשל, באמצעות מאבק בחברה מסחרית במטרה שתשנה את מדיניות הפרטיות שלה, או באמצעות מעבר לרשת חברתית מתחרה המגינה טוב יותר על הזכות לפרטיות מתוך שימור יתרונותיו של אפקט הרשת (network effect), יש צורך בפעולה משותפת של מספר רב של יחידים. אולם, אין זה אפשרי כאשר מדובר ביחידים מבוזרים. וכך, בעוד להצלתה של זכות היוצרים נרתמו תאגידי ענק בעלי כוח וממון שהיה בכוחם לנהל מאבקים משפטיים ארוכים ולהפעיל שדלנים בבתי המחוקקים בארצות הברית, כל אחד ואחד מאיתנו, המחזיק בזכות החוקתית לפרטיות, אינו משופע במשאבים כספיים ואנושיים, ברצון או במודעות לנזק שעשוי להיגרם לו, כדי לצאת להגנת פרטיותו. וכך, המאבק להגנתה של הזכות לפרטיות נותר נחלתם של מעטים: ארגוני חברה אזרחית ופעילי זכויות אדם.[272]

270 Lev-Aretz & Strandburg, *Privacy Regulation and Innovation Policy*, **לעיל** ה"ש 5, עמ' 280–287.

271 **שם**, עמ' 285–287, 289–290.

272 ראו למשל Zuboff, **לעיל** ה"ש 267; Yafit Lev-Aretz & Katherine J.

ההחצנות השליליות ושלל כשלי השוק שתוארו לעיל מובילים למסקנה שאין בכוחות השוק כדי להעיד על העדפותיהם האמיתיות של הצרכנים בנוגע לשימוש במידע אישי על אודותיהם וכדי לספק הגנת פרטיות ראויה. נוסף על כך, היכולת לאסוף, לעבד, לנתח ולהסיק מסקנות באופן ממוחשב מכמויות עצומות של מידע אישי ממקורות שונים – מאפשרת לחברות להסיק מידע אישי מהמידע שאספו הן מנושא עצמו המידע והן ממקורות אחרים, שאין לנושא המידע שום שליטה בהם. בעקבות זאת מתעצמים כשלי השוק שתוארו לעיל, ותיקונם על ידי השוק עצמו הופך לבלתי אפשרי. למשל, אף אם חברות יפעלו בשקיפות מלאה בנוגע למידע שהן אוספות מנושא המידע ולמידע שהן משלבות ממקורות אחרים, ללא הבנת האלגוריתם אשר משמש את החברה לעיבוד המידע ולהסקת מסקנות ממנו, נבצר מן הצרכן להעריך מראש מהו המחיר המעשי שיגבה ממנו השימוש במידע אישי על אודותיו. משום כך, בחירותיו של הצרכן לא ישקפו את העדפותיו האמיתיות בשאלת ההגנה על פרטיותו. זאת ועוד, איסוף ועיבוד נתוני העתק ממקורות שונים מקשה לאתר את האחראי לפגיעה בפרטיות. כן מעמיקה ההחצנה השלילית העוסקת בפגיעה בצדדים שלישיים, כלומר בנושאי מידע שכלל לא הסכימו לאיסוף ולעיבוד מידע אישי על אודותיהם, אולם ניתן להסיקו מאיסוף ומעיבוד של מידע אישי על אנשים דומים להם, קרובים אליהם או שייכים לאותם קבוצה חברתית או מקצועית או לאותו אזור גאוגרפי.[273]

כוחות השוק מתייחסים למידע אישי כאל כל סחורה אחרת, ולכן מתעלמים מערכים חשובים העומדים בבסיס הזכות לפרטיות, ונפגעים בעקבות שימוש לא ראוי במידע אישי. הזכות לפרטיות אינה זכות קניינית כזכות היוצרים. מדובר בזכות יסוד חוקתית הנגזרת מזכותו של אדם לכבוד ולאוטונומיה. שלל הגישות התאורטיות מלמדות שמדובר בזכות חיונית למימוש כבודו של האדם, לגיבוש זהותו ותפיסתו העצמית, לקבלת החלטות עצמאית ולהגנה מפני מבטו המְמַשטר של האחר. כמו כן מדובר בזכות חיונית לשם הגנה על זכויות אחרות,

---

Strandburg, *Regulation and Innovation: Approaching Market Failure from Both Sides*, 3.8:1 Yale J. on Regulation Bulletin (2020)

273 Lev-Aretz & Strandburg, *Privacy Regulation and Innovation Policy*, **לעיל** ה"ש 5, עמ' 291–296.

כגון הזכות לחופש ביטוי ולשוויון.[274] האותות (סיגנלים) שהשוק מספק, על בסיס ההיצע הקיים בשוק הטכנולוגיה והביקוש של הצרכנים לטכנולוגיות מסוימות, בנוגע להיקף ורמת הגנת הפרטיות המבוקשת על ידי הצרכנים או הרצויה מן הבחינה החברתית מטעים ומעודדים דווקא טכנולוגיות מעקב ואיסוף מידע. בה בעת חסרים תמריצים לפיתוח תחומי חדשנות רצויים חברתית, שלשם פיתוחם דווקא נדרשת הגנת פרטיות המאפשרת חשיבה יצירתית ועצמאית.[275] לפיכך, כוחות השוק אינם מסוגלים להתוות הגנה ראויה לזכות לפרטיות. מציאות זו מצדיקה יוזמות רגולטוריות לחיזוק הגנת פרטיות במידע.

חיזוק הזכות לפרטיות טומן בחובו משמעות יתרה דווקא בישראל. הזכות לפרטיות מעוגנת אומנם כזכות יסוד חוקתית בחוק יסוד: כבוד האדם וחירותו,[276] אולם היקפה ואכיפתה מותווים באמצעות חוק הגנת הפרטיות, שעל אף עדכונו בתיקון 13 הוא עדיין חסר בראי המשפט המשווה ואינו מותאם באופן מלא למציאות הדיגיטלית.

בשנים האחרונות דומה שישראל הופכת ל"חצר האחורית" של מדינות המערב הדמוקרטיות בכל הקשור להגנת הפרטיות. התקנתן של תקנות הגנת הפרטיות לשימור מעמד הנאותות במאי 2023[277] דווקא מדגישה את חולשתה של הזכות לפרטיות בישראל ומגבירה את החשש ממיצובה של ישראל כ"חצר אחורית". המטרה היחידה של תקנות אלה היא לעמוד בדרישות האיחוד האירופי להכרה בתאימות דיני הגנת הפרטיות בישראל לדינים הנהוגים באיחוד האירופי. מסיבה זו התקנות מעניקות זכויות יתר רק לנושאי מידע שהמידע עליהם מגיע לישראל מן האזור הכלכלי האירופי.[278] לפיכך נושאי מידע שמקור המידע עליהם הוא

274 WESTIN, **לעיל** ה"ש 10; בירנהק, [מרחב פרטי], **לעיל** ה"ש 10, 89–99.

275 Julie E. Cohen, *Symposium: Privacy and Technology: What Privacy is For*, 126 HARV. L. REV. 1904, 1918–1927 (2013)

276 ס' 7 לחוק יסוד: כבוד האדם וחירותו.

277 תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג–2023 (להלן: תקנות הגישור).

278 האזור הכלכלי האירופי מוגדר ככולל את המדינות החברות באיחוד וכן את איסלנד, נורווגיה וליכטנשטיין.

ישראל, כלומר כל נושאי המידע הנמצאים במדינת ישראל, אינם זכאים לאותן הזכויות, ונשארים נתונים להגנה מצומצמת יותר מצד חוק הגנת הפרטיות הקיים.[279] במצב זה מותר, למשל, לבצע בישראל מחקרי נתונים המשתמשים במידע אישי על אודות אזרחים, בתנאים מקילים יותר מאלה הנדרשים במדינות אחרות.

אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יעניק לנושא המידע כלי אזרחי לתבוע את נזקו מהגורמים אשר תרמו לפגיעה בפרטיותו ולקבל סעד אפקטיבי שעשוי להרתיע מפני סיוע דומה לפגיעה בפרטיות בעתיד. כך, עקב בצד אגודל, ניתן יהיה לחזק את הזכות לפרטיות על רקע ההתפתחויות הטכנולוגיות, ובישראל גם על רקע חולשתו של המחוקק בנושא. אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הזכות לפרטיות אף עולה בקנה אחד עם מגמת החקיקה הבינלאומית, שהאיחוד האירופי הוא ממוביליה,[280] לחזק את הזכות לפרטיות במידע נוכח הדיגיטציה הגוברת של חיי היום יום והפיכתו של מידע אישי למטבע סחיר רב ערך.

3.1.2. עקרון מונע הנזק היעיל ביחסי עבודה

אחת ההצדקות לאימוץ דוקטרינת ההפרה התורמת לדיני זכויות היוצרים עסקה בהיותו של הנתבע, יצרן הטכנולוגיה, מונע הנזק היעיל.[281] עקרון מונע הנזק היעיל נשען על שני מבחנים: המבחן הראשון בוחן אם גורם הביניים אשר פיתח את הטכנולוגיה ששימשה לרעה לשם הפרת זכויות היוצרים ההמונית והחמורה, הוא גם הגורם שסביר להטיל עליו את האחריות לעצירתה או למניעתה של ההפרה. סבירות הטלת האחריות נבחנה לפי יכולתו של גורם הביניים, מן הבחינה הכלכלית, לעצור את ההפרה או למנוע אותה מראש. אם גורם הביניים הוא צוואר הבקבוק או החוליה בשרשרת הפעולות המובילות להפרת זכות

279 להרחבה ראו רחל אריאלי הרשקוביץ ותהילה שוורץ אלטשולר **טיוטת תקנות הגנת הפרטיות עלולה לפגוע בעיקרון השוויון ולהביא לזעם בציבור, חוות דעת לקראת הדיון בוועדת החוקה של הכנסת** (המכון הישראלי לדמוקרטיה, 19.4.2023).

280 עם חקיקת ה־GDPR בשנת 2016 וכניסתן לתוקף במאי 2018.

281 מקובל לעשות שימוש גם במונח "מונע הנזק הזול".

הקניין הרוחני וביכולתו לפקח ביעילות ובאופן פשוט וזמין יחסית על המפירים הישירים, להפסיק את שיווק הטכנולוגיה או לשנותה באופן אשר ימנע את המשך השימושים לרעה בה, הרי שסביר לראות בו מונע הנזק היעיל.[282]

המבחן השני לבחינת היותו של גורם הביניים מונע הנזק היעיל, נשען על שיקולים של צדק חלוקתי ובוחן אם קיים אינטרס ציבורי המצדיק את הסטת עלויות הפיקוח המצטברות מבעל זכות היוצרים לגורם הביניים.[283]

יישום מבחנים אלו לדיני הגנת הפרטיות במסגרת יחסי עבודה מציג תמונה מורכבת. נדמה שאכן מפתחי טכנולוגיות המעקב אחר עובדים עונים להגדרת מונע הנזק היעיל במונחי יעילות כלכלית, בהיותם צוואר הבקבוק או החוליה בשרשרת הפעולות המובילות לפגיעה החמורה בזכות לפרטיות. גם מבחינת שאלת הצדק החלוקתי, נדמה כי קיים אינטרס ציבורי המצדיק את הסטת עלויות הפיקוח והאכיפה ממי שזכותם לפרטיות נפגעת, דהיינו עובדים בודדים, אל אלו המעניקים במודע למעסיקים כלים למשטור חודרני של העובד באמצעות מעקב ממושך ורציף עליו ומסייעים בכך להפיכת מקום העבודה לזירת מעקב הנראית שאובה ממשטרים אפלים. זאת בעיקר לאור העובדה שקיימים אמצעים אחרים, שפגיעתם בפרטיות העובד פחותה, לשם שיפור יעילותו של העובד ורווחיות המעסיק.

עם זאת, בעוד במקרה של הפרת זכויות יוצרים עמדו בעלי הזכויות מול מפירים רבים, מבוזרים ולעיתים אף אנונימיים, במקרה של פגיעה בפרטיותו של עובד – זהות הפוגע הישיר ידועה, איתורו קל והוא אף עשוי להיות בעל כיס עמוק, שכן מדובר במעסיק עצמו. למרות נסיבות מקלות אלו, יש לתת את הדעת לקושי האובייקטיבי של העובד לתבוע את המעסיק שלו עצמו. פעולה כזו עלולה להוביל מיידית לפיטוריו, ויתרה מכך – לפגוע במוניטין של העובד בעתיד ולפגוע בסיכוייו להתקבל לעבודה אצל מעסיקים אחרים. לפיכך, סביר שבנסיבות של יחסי עבודה, העובד מורתע מפני הגשת תביעה אף אם זכותו נפגעת באופן חמור. אולם, אין בכך כדי להצדיק פתרון של תביעת יצרן טכנולוגיות המעקב,

282 פישמן אפורי, **לעיל** ה"ש 165, עמ' 41–42, 50–61; פרשת **שוקן**, **לעיל** ה"ש 165, פסקה 13–15 לפסק דינו של השופט ריבלין.

283 פרשת **א.ל.י.ס.**, **לעיל** ה"ש 250.

שכן ניתן להתגבר על הקושי של עובד מסוים לתבוע את מעסיקו באמצעות תביעה המוגשת על ידי ארגון עובדים. עם זאת, חלק ניכר מהעובדים שפרטיותם נפגעת עקב שימוש בטכנולוגיות מעקב אינם מאוגדים. משום כך, תביעה נגד יצרן הטכנולוגיה – בין על ידי העובד עצמו ובין בשמו על ידי ארגון חברה אזרחית – הופכת לאפשרות הישימה יותר בנסיבות של יחסי עבודה.

ככל טכנולוגיה דו־שימושית גם לטכנולוגיות למעקב אחר עובדים שימושים ראויים ורצויים בצד שימושים פוגעניים. אימוץ דוקטרינת ההפרה התורמת דווקא עשוי לתמרץ את החברות המפתחות לפעול למזעור הפגיעה האפשרית בזכות לפרטיות, על ידי צמצום חלק מהתכונות האפשריות של טכנולוגיית המעקב. כך למשל יצומצמו סוגי המידע האישי שהיא אוספת ומעבדת, ויצומצם מגוון התובנות שהיא יכולה להפיק על ידי שימוש בבינה מלאכותית. כמו כן, אימוצה של דוקטרינת ההפרה התורמת עשוי להוביל את מפתחי טכנולוגיות המעקב להגביר את אכיפת רישיון השימוש במטרה להבטיח שימוש ראוי.

3.1.3. גורם הביניים כבעל כיס עמוק

גורם הביניים, מפתח הטכנולוגיה שאפשרה את הפרת זכות היוצרים, הוא בעל כיס עמוק, ועובדה זו הצדיקה אימוץ של דוקטרינת ההפרה התורמת לעולם זכויות היוצרים. לעומת המפירים הבודדים הרבים, ניצב גורם הביניים – למשל חברות סוני, נאפסטר או גרוקסטר – כבעל האמצעים לעמוד בפיצוי הנדרש לבעל זכות היוצרים בגין הפגיעה בזכותו.[284]

בהקשר של פגיעה בפרטיות, לגורם הביניים, מפתח טכנולוגיות המעקב אחר עובדים, אין בהכרח כיס עמוק יותר מאשר למעסיק שהוא הפוגע הישיר בזכות לפרטיות. עם זאת, במהלך השנים ניתן משקל פחות להצדקה זו נוכח המשמעות שבהטלת אחריות משפטית בהתאם ליכולת הכלכלית,[285] ולכן להצדקה זו עשוי להינתן משקל מועט במכלול השיקולים הנבחנים בעת אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות.

284 בירנהק, לידתה של עוולה, **לעיל** ה"ש 233, עמ' 200–201.

285 פישמן אפורי, **לעיל** ה"ש 165, עמ' 41–42.

3.2
שיקולי מדיניות נגד אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכלל ובהקשר של יחסי עבודה בפרט

3.2.1. פגיעה בחדשנות

בתחום דיני הקניין הרוחני בכלל והגנה על זכות היוצרים בפרט מקובל לעסוק באיזון בין חדשנות לבין זכות היוצרים. מחד גיסא, החדשנות נתפסת כמאיימת על זכות היוצרים. כך, למשל, תוכנות שיתוף הקבצים פגעו ביכולתם של בעלי זכויות היוצרים לקבל תגמול עבור השקעתם, ובכך איימו לפגוע במידה רבה בתמריצים להמשיך וליצור. מאידך גיסא, ההצדקות התאורטיות לזכות היוצרים הלקוחות מעולם הניתוח הכלכלי של המשפט, מדגישות את חיוניותה של זכות היוצרים, מן הבחינה הכלכלית והתועלתנית, להשגת חדשנות. זכות היוצרים מספקת את התמריצים הנחוצים להשקעה בחדשנות. תובנות מנוגדות אלו משקפות את האיזון המוטמע בזכות היוצרים בין הקניית הגנה לאינטרס הפרטי הקנייני של היוצר, הממציא או מפתח התוכנה, לבין האינטרס הציבורי: התקדמות טכנולוגית והתפתחות חברתית ותרבותית. כמעט כל פיתוח חדש, מכל סוג, נשען על פיתוחים קודמים המצויים בנחלת הכלל, וההגנה המוענקת בזכות היוצרים לאינטרס הפרטי מכרסמת ביכולת להגיע לפיתוח הבא ומאיימת על ההתקדמות החברתית והתרבותית. מנגד, ההגנה על האינטרס הפרטי חיונית לשם שמירה על תמריצי היוצרים והמפתחים להשקיע מלכתחילה בפיתוחים חדשים.[286]

אימוץ דוקטרינת ההפרה התורמת לדיני זכויות היוצרים התבסס מלכתחילה על ההבנה שטכנולוגיות דו־שימושיות מאתגרות את האיזון הראוי שביקש המחוקק

286 מיגל דויטש **עוולות מסחריות וסודות מסחריים** (2002).

להציב בין אינטרס הציבור – עידוד חדשנות וזרימה חופשית של רעיונות, מידע ומסחר והימנעות מפגיעה במנוע המוביל של הכלכלה המודרנית – לבין הזכות הקניינית של היוצרים לשלוט בניצול יצירותיהם. במובן זה דוקטרינת ההפרה התורמת משמשת כלי חשוב להשבת האיזון הראוי המגולם בזכות היוצרים.[287]

כפי שבסוף שנות ה־90 של המאה ה־20 טענו בעלי זכויות היוצרים כי ההתפתחויות הטכנולוגיות מובילות לפגיעה כה קשה בזכות היוצרים עד כדי הפרת האיזון הראוי בינה לבין חדשנות, כך נדמה שהחדשנות בתחום איסוף מידע ועיבודו עלולה להפר את האיזון הראוי בינה לבין הזכות לפרטיות, ואף מאיימת על עצם קיומה של זכות חשובה זו.[288] עם זאת, הרחבת מעגל האחראים להפרת הזכות לפרטיות, עם אימוץ דוקטרינת ההפרה התורמת, תחזק לכאורה את הזכות לפרטיות ובכך מעוררת את החשש כי האיזון בין חדשנות לפרטיות יופר דווקא בעקבות הפגיעה הצפויה בחדשנות. הרחבת היקפה של הזכות לפרטיות, כך נטען, אינה תואמת את הציפייה הסבירה של נושא המידע לפרטיות, תפגע בזרימה החופשית של מידע, שהוא חומר הגלם הבסיסי לחדשנות הטכנולוגית כיום, וכך תוביל לפגיעה אנושה בחדשנות שהיא בעלת ערך ורצויה מן הבחינה החברתית.[289]

לפי עמדה זו, כדי למנוע פגיעה חמורה בחדשנות, מוצדק להתעלם לחלוטין מהפרות הזכות לפרטיות ולתמוך ברגולציה חלשה להגנה על הזכות לפרטיות

287 Moye, **לעיל** ה"ש 154, עמ' 659; Zimmerman, **לעיל** ה"ש 165, עמ' 78. אציין שלכאורה בדין הישראלי, החריג שנקבע בפרשת **סוני** אינו מקובל, לנוכח אמירתו של השופט ריבלין בפרשת **שוקן** ולפיה ניתן להטיל אחריות תורמת גם כאשר ההפרה הישירה חוסה תחת חריג השימוש ההוגן. ראו פסקה 24 לפסק דינו של השופט ריבלין בפרשת **שוקן**, **לעיל** ה"ש 165. לביקורת על עמדה זו ראו פישמן אפורי, **לעיל** ה"ש 165, עמ' 47–48.

288 Tal Zarsky, *The Privacy-Innovation Conundrum*, 19 Lewis & Clark L. Rev. 115, 117–118 (2015)

289 Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, NBER Working Paper Series (Working Paper 17124, 2011); Ashley Johnson, *Balancing Privacy and Innovation in Smart Cities and Communities*, Information Technology & Innovation Foundation (March 6, 2023); Zarsky, **לעיל** ה"ש 287, עמ' 140–141; Lev-Aretz & Strandburg, *Privacy Regulation and Innovation Policy*, **לעיל** ה"ש 5.

בשוקי מידע.[290] התומכים בעמדה זו מביאים כדוגמה את הפער הקיים בתחום טכנולוגיית המידע בין ארצות הברית לבין האיחוד האירופי. לשיטתם, הסיבה לחדשנות רבה יותר בארצות הברית לעומת האיחוד האירופי בתחום זה היא חקיקת הגנת פרטיות חלשה יותר בארצות הברית לעומת זו הקיימת באיחוד האירופי. עם זאת, לעמדה זו אין סימוכין במחקרים. זאת ועוד, הפער בחדשנות בשוקי המידע בין ארצות הברית למדינות האיחוד האירופי עשוי דווקא ללמד על הצורך בסטנדרט פרטיות גלובלי אחיד, בדומה לזה הקיים בנושא זכות היוצרים. סטנדרט אחיד יאפשר חדשנות רצויה וראויה חברתית מבחינת הגנת הפרטיות, בלי להעניק יתרון בתחום ליזמים ממדינות שאינן מעניקות הגנה מתאימה לזכות יסוד חשובה זו.[291]

זאת ועוד. הטיעונים בדבר קשר חיובי בין חדשנות לפרטיות נדחים בדרך כלל. כך, נטען שפגיעה בפרטיות וחיים תחת מעקב – רציף או לאו – מובילים לתחושת משטור ולחשש מפני חשיפה. תחושות אלו פוגעות ביצירתיות. מאחר שחדשנות היא תוצר של יצירתיות, הגנה על הפרטיות חיונית גם כשלעצמה לשם עידוד החדשנות. עם זאת, על טיעון זה נמתחה ביקורת בנימוק שמדובר בטיעון ספקולטיבי שאינו מגובה בנתונים אמפיריים ונשען על התפיסה הרומנטית של היוצר או של הממציא הבודד. כלל לא ברור שהיצירתיות הנדרשת לחדשנות מקורה בעיקר ביחיד ובהגנה על פרטיותו, ולא בהשקעה בחינוך ובהשכלה גבוהה של שיעור ניכר מהציבור וביצירת מרחב אשר יאפשר שיח פתוח בין עמיתים במקום העבודה.[292]

290 Cohen, **לעיל** ה"ש 274, עמ' 1918–1927.

291 Goldfarb & Tucker, **לעיל** ה"ש 288; Johnson, **לעיל** ה"ש 288; Zarsky, **לעיל** ה"ש 287, עמ' 140–141; Lev-Aretz & Strandburg, *Privacy Regulation and Innovation Policy*, **לעיל** ה"ש 5.

292 Margaret Steen, *Privacy and Innovation*, Markkula Center for Applied Ethics at Santa Clara University (Feb. 1, 2023); M. Ryan Calo, *The Unknown Unknowns: The Role of Innovation in Privacy,* Yale ISP Symposium 2010–2011; Julie E. Cohen, *The Surveillance Innovation Complex: The Irony of Participatory Turn*, The Participatory Condition (Darin Barney et al. eds., 2015); Cohen, **לעיל** ה"ש 274, עמ' 1918–1927.

קשר חיובי אפשרי נוסף בין חדשנות להגנה על הזכות לפרטיות מתבטא בחיוניותה של הזכות לפרטיות לשם יצירת יחסי אמון, הסכמה ושקיפות בין נושא המידע, המשתמש או הצרכן, לבין החברה המסחרית המספקת את הטכנולוגיה החדשנית. ההנחה היא שכאשר לקוחות ידעו שמידע אישי עליהם נחשף שלא כדין, הם יימנעו מלתת אמון בחברות המסחריות המפתחות את הטכנולוגיות החדשניות ומפעילות אותן. הימנעות שכזו תפחית את מספר המשתמשים או הצרכנים המתעניינים בטכנולוגיות חדשניות, בעקבות זאת יפחת התמריץ ליצור טכנולוגיות חדשניות, והחדשנות ככלל תפגע. גם על טיעון זה נמתחה ביקורת בנימוק שאין בנמצא הוכחות לכך שהגנה על פרטיות המשתמשים או הימנעות ממנה משפיעה על אמון המשתמשים באופן המוביל להימנעות משימוש במוצר טכנולוגי ובכך גם לפגיעה בחדשנות.[293]

הגנה על הזכות לפרטיות חיונית לשם הגברת התחרות בשוק ומכאן גם של החדשנות. עמדה זו מצביעה על כך שכוח השוק המונופוליסטי הנשלט בידי חברות הטכנולוגיה הגדולות בשוק מבוסס על איסוף, על החזקה ועל עיבוד של כמויות עצומות של מידע אישי. חקיקה המגינה על מידע אישי ומסדירה את השימוש בו עשויה לפיכך לצמצם את יכולתן של חברות לאסוף, להחזיק או לעבד כמויות עצומות של מידע אישי. כתוצאה יצומצם כוחן גם של החברות הגדולות הנשענות על איסוף מידע אישי רב ויופחתו חסמי הכניסה לשוק בפני חברות אחרות, קטנות יותר וחדשניות. עם זאת, גם על עמדה זו נמתחה ביקורת בנימוק שייתכן שדווקא דילול ההגנה על הזכות לפרטיות תקל על המסחר במידע אישי וכך יוכלו גם חברות חדשות וקטנות לחדור לשוק ולרכוש כוח שוק אשר יאפשר להן להתחרות בחברות הגדולות.[294]

יתרה מכך, בניגוד לזכות היוצרים, שמעצם טבעה מעודדת קִדמה וחדשנות ומשמשת כלי להשגתן, הזכות לפרטיות אינה מבוססת על אינטרסים תועלתניים כלכליים אלא על תפיסת כבוד האדם, האוטונומיה האישית שלו, והגנה מפני חדירה פוגענית מדי מצד המדינה ומצד האחרים. אינטרסים ציבוריים כלכליים, שעליהם מגינה החדשנות, הם משניים בחשיבותם לעומת ערכים אלו.

293 Zarsky, **לעיל** ה"ש 287, עמ' 132.

294 **שם**, עמ' 135–136.

ההתנגשות בין חדשנות לבין פרטיות, מבטאת הלכה למעשה התנגשות בין זכות חוקתית לבין אינטרס ציבורי מנוגד ויש לאזן ביניהם, תוך כדי מתן במה לחשיבותו של כל אחד מהם. אולם, איזון זה אינו יכול לצאת מנקודת הנחה שלזכות לפרטיות ולאינטרס הציבורי בחדשנות במשקל זהה,[295] ובכל מקרה, אין מקום לבטל את הזכות לפרטיות ואת הערכים שבבסיסה, בשם החדשנות הטכנולוגית.[296] חיזוק לטענה שהזכות לפרטיות לא נסוגה או נעלמה כדי לפנות מקום לחדשנות, ניתן למצוא בהתנהלותו של מייסד הרשת החברתית פייסבוק, מארק צוקרברג. בשנת 2010 הכריז צוקרברג כי פרטיות אינה נורמה חברתית יותר. אנשים, לדבריו אז, מעדיפים את הנורמה החברתית של פתיחות ושיתוף במידע אישי עם אחרים, על פני הנורמה החברתית הדועכת של פרטיות.[297] במרץ 2019, לאחר חשיפת כמה שערוריות שנגעו לזכות לפרטיות, ובראשן קיימברידג' אנליטיקה שבמסגרתה נחשף כי מטא העניקה לחברת הייעוץ הפוליטי קיימברידג' אנליטיקה גישה למידע אישי על 87 מיליון משתמשי הרשת החברתית פייסבוק,[298] שינה צוקרברג את עמדתו. ברשומה שפרסם ברשת החברתית הבהיר צוקרברג שמעתה תקפיד פייסבוק לשמור על פרטיות משתמשיה. אומנם, לשיטתו מדובר בפרטיות מצומצמת בין משתמשים, ולא בין המשתמש לבין פייסבוק עצמה, אולם ניתן לראות בכך את תחילתה של ההבנה שהזכות לפרטיות אינה נורמה חברתית שחלפה מהעולם.[299]

דווקא כשלי השוק המאפיינים שוקי מידע אישי רלוונטיים גם להצדקת אימוצה של דוקטרינת ההפרה התורמת מתוך חיזוק הזכות להגנת הפרטיות ויצירת איזון ראוי מחודש בינה לבין אינטרס הציבור בחדשנות.[300] השפעתה של רגולציה

295 **שם**, עמ' 143–146.

296 בירנהק, פרטיות חוקתית, **לעיל** ה"ש 18, 36–37.

297 Bobbie Johnson, *Privacy no Longer a Social Norm, says Facebook Founder*, The Guardian (Jan. 11, 2010)

298 Alex Hern, *Cambridge Analytica: How did it Turn Clicks Into Votes?*, The Guardian (May 6, 2018)

299 Alex Hern, *Mark Zuckerberg's Privacy Blogpost: What He Did and Didn't Say*, The Guardian (March 7, 2019)

300 להרחבה בעניין כשלי השוק המאפיינים שוקי מידע, ראו את הדיון **לעיל** בסעיף 3.1.1.

על החדשנות תלויה במתווה ובדרישות של אותה רגולציה. רגולציה, המתוכננת היטב תביא בחשבון את עלויות הציות וחשיבות הגנה על התמריצים הכלכליים לחדשנות, ועל כן פגיעתה הצפויה בחדשנות בעלת תועלת חברתית אמורה להיות מזערית, אם בכלל.[301]

3.2.2. כשל אכיפה

ההצדקה העיקרית לאימוץ דוקטרינת ההפרה התורמת לדיני זכויות היוצרים או הפטנטים הייתה קיומו של כשל אכיפה, שהתבטא בקיומם של מפירים יחידים רבים, שאת חלקם היה קשה לאתר, ושתביעת כל אחד מהם בנפרד יקרה והתועלת הצפויה ממנה נמוכה. אימוץ זה אִפשר לבעל זכות היוצרים או הפטנט לפנות בתביעה לקבלת סעד מן הגורם שסיפק את הכלים שאפשרו את ההפרה ההמונית של זכויותיו – יצרן הטכנולוגיה.[302]

דווקא במקרה של הפרת פרטיות בעלי הזכויות הנפגעים הם רבים, מבודדים וחלשים כלכלית מול הפוגעים ומפתחי הטכנולוגיות המאפשרות את הפגיעה. מדובר בכשל שוק של היעדר יכולת לפעול באופן קולקטיבי,[303] ולאו דווקא בכשל אכיפה.

עם זאת, דווקא אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יכול להוביל לכשל אכיפה אחר הנובע מהיעדר הגדרה אחידה ומקובלת לפגיעה בפרטיות במרבית המדינות. שלל הגישות התאורטיות לזכות לפרטיות מלמד על כך שמדובר בזכות עמומה ומשתנה, שקשה להמשיגה באופן אחיד וברור.[304] זאת בניגוד לזכות היוצרים, שגבולותיה והיקפה ברורים ומוסכמים במרבית מדינות העולם, ומשקפים את האיזון הראוי בין האינטרס הפרטי של היוצר לבין האינטרס הציבורי בחדשנות המבוססת על נחלת הכלל. בהיעדר הגדרה אחידה וברורה, מעשה שעשוי להיחשב פגיעה בזכות לפרטיות במדינה אחת,

301 Lev-Aretz and Strandburg, *Privacy Regulation and Innovation Policy*, **לעיל** ה"ש 5, עמ' 275-276, 291-296.

302 בירנהק, לידתה של עוולה, **לעיל** ה"ש 233, עמ' 200-201.

303 להרחבה ראו את הדיון בטקסט הנלווה, **לעיל** ה"ש 272.

304 בירנהק, פרטיות חוקתית, **לעיל** ה"ש 18, 68.

עשוי להיות מותר וחוקי במדינה אחרת. היעדר הגדרה אחידה עלול להטיל נטל כבד על החברות המפתחות שייאלצו להחזיק מערך משפטי מורכב אשר יכיר את דיני הגנת הפרטיות לצד דיני העבודה בכל המדינות בכל המדינות הרלוונטיות, יטמיע דרישות חוזיות מתאימות בכל עסקה לרכישת רישיון שימוש בטכנולוגיית המעקב ויחזיק במנגנון טכנולוגי וחוזי לאיתור פגיעות אפשריות בפרטיות המבוצעות באמצעות הטכנולוגיה.

עם זאת, חקיקת ה־GDPR באיחוד האירופי הובילה למה שמכונה "אפקט בריסל" – האחדה יחסית ומבורכת של סטנדרט ההגנה על הזכות לפרטיות בקרב מרבית המדינות.[305] בהנחה שמגמת ההאחדה של דיני הגנת הפרטיות ברוח ה־GDPR תמשיך ותעמיק, עשוי כשל אכיפה זה להצטמצם.

3.2.3. אינטרסים ציבוריים נוספים

בעוד שבעת בחינת אימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים התמקד הדיון בניתוח כלכלני תועלתני של השלכות אימוץ הדוקטרינה והסתיים בבחינת האיזון הראוי בין זכות היוצרים לבין אינטרס הציבור בחדשנות, הדיון באימוצה של הדוקטרינה לדיני הגנת הפרטיות אינו מתמצה בנקודה זו.

עומקה ורוחבה של הזכות לפרטיות מובילים לכך שגם חיזוקה עלול לפגוע בקשת רחבה של זכויות או של אינטרסים. כך, למשל, אימוץ דוקטרינת ההפרה התורמת עלול לפגוע באינטרס הציבור בכללותו ובאינטרס המעסיק באופן פרטני לשכלל את שוק העבודה בעידן הפוסט־קורונה. יש לתת את הדעת לפגיעות אפשריות אלו בבואנו לבחון את הבסיס העיוני לאימוץ דוקטרינת ההפרה התורמת ושיקולי המדיניות הנלווים לו. אולם, בה בעת, יש לתת את הדעת להשלכות השליליות לעיתים של טכנולוגיות מעקב אחר עובדים. בעיקר, יוצרות טכנולוגיות מעקב אלו שקיפות חד־כיוונית ומובילות להעמקת פערי המידע בין העובד למעסיק, להחרפת פערי הכוחות ביניהם ולפגיעה ביכולתם של עובדים, בעיקר עובדים

305 Cedric Ryngaert & Mistale Taylor, *The GDPR as Global Data Protection Regulation*, 114 American Journal of International Law 5 (2020)

מהמעמד הנמוך, להתאגד כדי להגן על זכויותיהם. בנסיבות אלו, הסיכון לניצול לרעה של עובדים גובר.[306]

נקודת המוצא בבחינת שיקולי מדיניות אלו היא שמדובר באינטרסים. משום כך, באיזון מול הזכות החוקתית לפרטיות, יש לתת להם משקל פחות, על אף חשיבותם הציבורית הגדולה. במסגרת זו פגיעה בזכות החוקתית לפרטיות לשם הגשמת אחד האינטרסים החשובים הללו בכל זאת צריכה לעמוד בדרישת המידתיות. כלומר, על הפגיעה בפרטיות להיות לא רק לתכלית ראויה, אלא גם יש להוכיח שהאמצעי שננקט ומוביל לפגיעה הוא המתאים והיעיל להגשמת האינטרס. כן יש להוכיח שהתועלת השולית מהשימוש באמצעי הנבחר עולה על הנזק שבפגיעה בזכות לפרטיות.[307] עמידה במבחנים אלו תיבדק במסגרת יישום דוקטרינת ההפרה התורמת בכל מקרה ומקרה.

3.3. סיכום ביניים: שיקולי המדיניות בנוגע לאימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות במסגרת יחסי עבודה

אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יוביל לחיזוק הזכות לפרטיות, אשר נחוץ ביותר לנוכח הפגיעה המהותית בחשיבות הזכות ובהגנה עליה בשנים האחרונות עם הקִדמה הטכנולוגית. האימוץ עשוי להשיב את

306 ראו Ball, **לעיל** ה"ש 25, עמ' 36–37, 41; Gierlich-Joas et al., **לעיל** ה"ש 41, עמ' 5192; Kim & Bodie, **לעיל** ה"ש 41, עמ' 293–301; Vatcha, **לעיל** ה"ש 30, עמ' 5; Mims, **לעיל** ה"ש 32; Ebert et al., **לעיל** ה"ש 30, עמ' 3; Riso, **לעיל** ה"ש 21; Blackman, **לעיל** ה"ש 40; Klöpper & Köhne, **לעיל** ה"ש 32, עמ' 4; Köhne & Klöpper, **לעיל** ה"ש 41; Negron, **לעיל** ה"ש 33.

307 מרדכי קרמניצר ורענן סוליציאנו קינן **קבלת החלטות בימי הקורונה בראי הפסיקה: ההחלטה להשתמש באיכוני השב"כ כמקרה מבחן** (על חוקיות 02, המכון הישראלי לדמוקרטיה, נדיב מרדכי עורך, 2021), עמ' 8.

המשקל הראוי לערכים שבבסיס הזכות לפרטיות הנגזרת מהזכות לכבוד ומשמעותית לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו וללא התערבות זרה. כן תפתור דוקטרינת ההפרה התורמת את כשלי השוק המאפיינים שוקי מידע.

כן נראה שמפתחי טכנולוגיות המעקב הם מונע הנזק היעיל. הם נמצאים בעמדת המפתח למניעת הפגיעה בפרטיות או להפסקתה, ואינטרס הציבור מצדיק את הסטת עלויות הפיקוח והאכיפה מעובדים בודדים אל הגורמים שמחזיקים באמצעים הסבירים כלכלית למנוע את הפגיעה החמורה בזכות העובד לפרטיות. אומנם, זהותו של הפוגע הישיר ידועה, איתורו קל והוא אף עשוי להיות בעל כיס עמוק, מפני שמדובר במעסיק עצמו. עם זאת עובדים רבים מורתעים מפני תביעת המעסיק לנוכח ההשלכות הקשות העלולות להיות למהלך שכזה על העסקתם הנוכחית ועל המוניטין שלהם בעתיד במקומות עבודה אחרים. נוסף על כך, סביר שהטלת אחריות תורמת על יצרני טכנולוגיית המעקב תוביל אותם לדייק את השימושיות של הטכנולוגיה ולהימנע מפגיעה שלא כדין בזכות העובד לפרטיות.

בראש הטיעונים נגד אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות ניצב הטיעון בדבר הפגיעה בחדשנות. אולם, בחינת הטיעון מובילה לטעמי למסקנה שאין לייחס לו משקל רב. שיקול הפגיעה בחדשנות הוצג גם בנוגע לאימוצה של דוקטרינת ההפרה התורמת לדיני זכות היוצרים, אולם בהיות זכות היוצרים זכות קניינית המיועדת להגנה על תמריצי היוצר להמשיך וליצור, אימוץ דוקטרינת ההפרה התורמת נתפס ככלי לחיזוק זכות היוצרים מול פגיעת הטכנולוגיה בה וכאמצעי להשבת האיזון הדרוש לקידום חדשנות. אף שיש הטוענים לקשר חיובי, במובנים מסוימים, בין פרטיות לחדשנות נוכח חיוניותה של הפרטיות למחשבה חופשית ויצירתית, ליצירת יחסי אמון בין המשתמש לחברה המפתחת ולהגברת התחרות בשווי המידע האישי, נדמה שהזכות לפרטיות אינה נחשבת חיונית לחדשנות בבחינה תועלתנית כלכלית. זאת ועוד, הזכות לפרטיות מגינה על ערכים בסיסיים של כבוד האדם ועל האוטונומיה האישית שלו, בעוד חדשנות מגינה על אינטרסים ציבוריים כלכליים, המשניים בחשיבותם לערכים שמגינה עליהם הפרטיות. לפיכך, בהתנגשות בין פרטיות לחדשנות אין מדובר בגורמים שקולים, אלא יש לתת את הדעת למשקל הרב יותר שיש לתת לזכות היסוד לפרטיות מול האינטרס הכלכלי בחדשנות.

אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יכול להוביל גם לכשל אכיפה הנוגע לסמכות השיפוט והדין החל, משום שאין הגדרה אחידה ומקובלת לפגיעה בפרטיות בקרב מרבית המדינות, ומעשה המותר במדינה אחת יכול להיחשב פגיעה בפרטיות במדינה אחרת. עם זאת, חקיקת ה־GDPR ו"אפקט בריסל" שהגיע בעקבותיה עשויים להביא להאחדה יחסית של הגדרת הזכות לפרטיות במרבית מדינות העולם ולריכוך כשל אכיפה זה.

רוחבה של הזכות לפרטיות מוביל לכך שחיזוקה עלול לפגוע גם באינטרסים נוספים ובעיקר באינטרס המעסיק, ואולי אף הציבור בכללותו, בשכלולו בייעולו של שוק העבודה בעידן הפוסט־קורונה. אולם, על אף חשיבותם הרבה של אינטרסים אלו, יש לזכור שמדובר באינטרסים שמשקלם פחות לעומת הזכות החוקתית לפרטיות. כמו כן, וללא קשר לאיזון הדרוש שבין האינטרסים לזכות החוקתית לפרטיות, הסיכון לניצול לרעה של עובדים עקב העמקת פערי המידע והכוחות ביניהם לבין המעסיקים בעקבות שימוש בטכנולוגיות מעקב, מצדיק לדעתי את אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות. ההגנה על האינטרסים הציבוריים החשובים תיעשה כחלק מבחינת מידתיות הפגיעה בפרטיות בעת הוכחת קיומה של הפרת הזכות לפרטיות כתנאי הראשון ביישום דוקטרינת האחריות התורמת.

לפיכך, סקירת שיקולי המדיניות הרלוונטיים מעידה על כך שאימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות – אפשרי.

פרק 4

דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות: התנאים להחלתה וליישומה בנושא טכנולוגיות למעקב אחר עובדים

בפרק הקודם בדקתי את הבסיס העיוני לאימוצה של דוקטרינת ההפרה התורמת ואת שיקולי המדיניות הנלווים לכך. מצאתי שאף על פי שלאימוצה עשויים להיות יתרונות משמעותיים בכל הקשור לחיזוק הזכות לפרטיות והערכים שבבסיסה, עלולים להיות לו גם חסרונות, כגון פגיעה מסוימת בחדשנות, פגיעה בוודאות המשפטית עקב כשל אכיפה ופגיעה באינטרס הציבורי בשכלול שוק העבודה בעידן הפוסט־קורונה. עם זאת, מכלול השיקולים הוביל למסקנה שהיתרונות הטמונים באימוצה של דוקטרינת ההפרה התורמת עולים על חסרונותיה, וההתמודדות הנכונה עם האחרונים ראוי שתיעשה בעת יישום הדוקטרינה בנסיבות כל מקרה ומקרה. את זאת אפנה לעשות עתה.

מסקירת דוקטרינת ההפרה התורמת בדיני זכויות יוצרים בפרק 2 עולה שלשם החלתה נדרשת הוכחתם של שלושה תנאים מצטברים:

(**1**) קיום הפרה ישירה.

(**2**) מודעות גורם הביניים להפרה.

(**3**) גורם הביניים העלה תרומה משמעותית, ניכרת וממשית לביצוע ההפרה הישירה.

בעת בחינת אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יש לבדוק את האפשרות ליישם כל אחד מהתנאים המצטברים הללו ולבחון את השלכותיו.

4.1
קיומה של הפרה ישירה: פגיעה בפרטיות העובד

תנאי זה, המחייב קיומה של הפרה ישירה, יכול להתקיים גם כאשר המפר הישיר נהנה מחריג השימוש ההוגן, משום שהגנות אלו מונעות מן המפר לשאת באחריות להפרה, אך אינן מאיינות את עצם ההפרה.[308]

בהקשר של יחסי עובד-מעסיק, תכלית הפגיעה בזכות העובד לפרטיות ממוסגרת תחת הפררוגטיבה הניהולית של המעסיק המבטאת את צרכיו הלגיטימיים. אולם, כפי שתואר בסעיף 1.4, עמדת המשפט המשווה בשאלת חוקיות הפגיעה בפרטיות העובד אינה אחידה. בארצות הברית נדמה שדי אם המעסיק יודיע מראש על מדיניות שימוש בטכנולוגיית מעקב חודרנית ויקפיד לעשות בה שימוש בשקיפות כדי לאיין את ציפייתו הסבירה של העובד לפרטיות בביתו ולגבי השימוש שהוא עושה במכשיר הטלפון הנייד שלו או במחשבו, וכדי להתיר שימוש בטכנולוגיות מעקב באופן חודרני אגב פגיעה חמורה בזכות העובד לפרטיות.

באיחוד האירופי ניתנת הגנה מקיפה וחזקה יותר לזכות העובד לפרטיות, בניסיון להתאימה לחדשנות הטכנולוגית הקיימת. אין די רק ביידוע ובשקיפות, אלא יש להוכיח שהפגיעה בפרטיות באמצעות טכנולוגיית מעקב מידתית ונחוצה למען הגשמת אינטרס לגיטימי של המעסיק. במסגרת בחינת מידתיות הפגיעה בפרטיות יש להביא בחשבון גם את המרחב שבו פועלת טכנולוגיית המעקב, אולם אין מדובר בשיקול היחיד. לצידו נבחנים גם היקף המעקב, משכו ותדירותו וכן השימוש שנעשה במידע הנאסף במסגרתו. מדובר בארגז כלים מקיף המביא בחשבון את טשטוש הגבולות בין המרחבים שבהם עשויה לפעול טכנולוגיית המעקב, אולם אינו תְּלוי טכנולוגיה ספציפית. ככל שהמעקב חודרני יותר מבחינת המרחב שבו הוא פועל, מקיף מבחינת המידע הנאסף וממושך יותר, וככל שהמידע הנאסף מהמעקב מעובד לשם קבלת החלטות אוטומטיות בנוגע

308 ראו את הטקסט הנלווה, **לעיל** ה"ש 243.

ליעילותו של העובד, כך תיחשב הפגיעה בזכות העובד לפרטיות מידתית פחות. לפיכך נפסק שטכנולוגיית מעקב שאוספת מידע מהמרחב הדיגיטלי העסקי בעת שהעובד ניגש אליו מהמרחב הפיזי של המעסיק, עשויה להיחשב מידתית. עם זאת, כאשר הטכנולוגיה אוספת מידע מן המרחב הדיגיטלי הפרטי של העובד, למשל תכתובת פרטית של העובד באמצעות תוכנת מסרים מיידיים, אף אם הוא ניגש אליו מהמרחב הפיזי של המעסיק, היא אינה מידתית. כך גם כאשר הטכנולוגיה אוספת מידע מהמרחב הפיזי האישי של העובד, למשל הבעות פניו, באמצעות המרחב הדיגיטלי או הפיזי (המחשב) העסקי.

בישראל, פגיעה בפרטיות צריכה לעמוד בתנאי פסקת ההגבלה שבחוק יסוד: כבוד האדם וחירותו (הפרטיות החוקתית) ולהיעשות בהתאם להוראות חוק הגנת הפרטיות (הפרטיות הסטטוטורית).[309] מאחר שמדובר ביחסי מעסיק-עובד ולכן במערכת שאינה שוות כוחות, קשה לייחס להסכמת העובד, הנדרשת כתנאי להכשרת הפגיעה לפי חוק הגנת הפרטיות, ערך רב. נוסף על כך, פגיעה בזכות חוקתית צריכה להיות קבועה בחוק או לפי הסמכה בחוק, לתכלית ראויה ובמידה שאינה עולה על הנדרש. אף בהנחה שייעול תפוקות העבודה ושוק העבודה בתקופת הפוסט־קורונה הוא תכלית ראויה, שאר התנאים להוכחת חוקתיות הפגיעה מעוררים קשיים. כפי שראינו בעת דיון במסמך הרשות בנושא היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק, קיומה של הסמכה בחוק המתירה הפעלת טכנולוגיות מעקב במסגרת יחסי עבודה מוטלת בספק,[310] ועל כן לא ברור האם ניתן לטעון שהפגיעה היא בחוק או לפיו. באשר למידתיות הפגיעה, הבחינה היא תלת־ראשית: (א) מבחן ההתאמה: האם האמצעי שננקט עשוי להביא להשגת התכלית? (ב) מבחן הצורך: האם האמצעי שנבחר הוא היעיל ביותר שפגיעתו בזכות היא הקטנה ביותר, ואין אמצעי אחר שיעילותו דומה אך פגיעתו בזכות לפרטיות קטנה יותר? (ג) מבחן המידתיות הצר: האם התועלת השולית שתושג מהשימוש באמצעי עולה על הנזק המתבטא בפגיעה בזכות? אולם, יישומם של מבחנים אלה בנושא פגיעה בפרטיות עובד עקב טכנולוגיות מעקב מגלה תמונה משפטית מעורפלת במקצת. הכללים המשפטיים לבחינת

309 מיכאל בירנהק "פרטיות בעיר הדיגיטלית" **מחקרי משפט לד** 1, 20 (התשפ"א-2021).

310 ראו את הדיון בטקסט הנלווה, **לעיל** ה"ש 149.

פגיעה בזכות העובד לפרטיות מתבססים על פרשנות שניתנה במהלך השנים על ידי בתי המשפט ועל ידי הרשות לחוק הגנת הפרטיות, ומתבססים על חוק מיושן שאף עדכונו לאחרונה בתיקון 13 אינו מספק נוכח חודרניות טכנולוגיות המעקב והשימוש בבינה המלאכותית המשולב בהן.

בפרשת **איסקוב** קבע בית הדין הארצי כלל משפטי המדרג את חומרת הפגיעה בפרטיות העובד ואת מידתיותה בהתאם למרחב הדיגיטלי שבו נמצא המידע האישי, שעיבודו פוגע בפרטיות. בקצה האחד, המרחב הדיגיטלי העסקי בלבד, בתווך המרחב הדיגיטלי העסקי, שהמעסיק התיר לעובד להשתמש בו גם לצרכים אישיים, ובקצה השני המרחב הדיגיטלי הפרטי הסגור של העובד. במרחב הדיגיטלי העסקי בלבד תותר פגיעה בפרטיות בהתאם לאיזון בין האינטרס הלגיטימי של המעסיק לבין זכות העובד לפרטיות, למידתיות, לשקיפות, ליידוע ולהוכחת חשש ממשי לפעילות בלתי חוקית מצד העובד. במרחב הדיגיטלי העסקי שבו המעסיק מתיר לעובד לעשות שימוש גם לצרכים הפרטיים, נדרשת הסכמת העובד לפגיעה ספציפית. ובמרחב הדיגיטלי הפרטי תותר פגיעה בפרטיות העובד רק בצו בית משפט, בהתקיים תנאים מסוימים.

בפרשת **זינגר**, חמש שנים לאחר פסיקת בית הדין הארצי בפרשת **איסקוב**, התעלם בית המשפט העליון ממדרג הפגיעה מבוסס המרחב שהוצגה בפרשת **איסקוב**. חוקיותה של הפגיעה בפרטיות העובד נבחנה בהתאם לדרישת הנחיצות, המידתיות והלגיטימיות תוך כדי ייחוס חשיבות רבה לתום ליבו של המעסיק, להגנה על האינטרס הלגיטימי של המעסיק ולחשש מפני עבירה מצד העובד. בית הדין האזורי לעבודה בפרשת **אקספו** אזכר את ההבחנה בין המרחבים והבהיר שלעובד ציפייה סבירה לפרטיות גם במרחב הדיגיטלי העסקי, אולם גם הוא ייחס משקל רב לאופי העבודה, תפקידו של העובד, ותום ליבם של העובד ושל המעסיק בבחינת חוקיותה של הפגיעה בפרטיות העובד.[311]

הרשות הציעה להתייחס לכל פגיעה בזכות העובד לפרטיות באמצעות טכנולוגיות למעקב אחר עובדים באותו האופן, בלי להבחין בין המרחבים השונים. לשיטתה פגיעה בפרטיות העובד עקב שימוש בטכנולוגיות מעקב בעת

311 להרחבה ראו הדיון בסעיף 1.4.3.1 לעיל.

עבודה מרחוק תותר אם היא נחוצה להגשמת תכלית לגיטימית של המעסיק ומידתית, אם המעסיק פעל בשקיפות, אם יידע את העובד על אודות השימוש בטכנולוגיות מעקב ואם יש לעובד בחירה אמיתית בין עבודה מרחוק לבין עבודה במקום העבודה פיזית, והעובד הסכים, מראש ומדעת, לפגיעה בפרטיות באמצעות טכנולוגיית המעקב. כן על המעסיק לעמוד בעקרון מזעור המידע, להבטיח אבטחת מידע ועיצוב לפרטיות, לכבד את זכויות נושא המידע ולהימנע מהעברת המידע האישי על אודות העובד לצדדים שלישיים ללא הסכמת העובד. מנגד, לצד קביעת מתווה זה, אשר אינו מתייחס למרחבים השונים שמתרחשת בהם הפגיעה בפרטיות, הרשות חוזרת על הלכת **איסקוב** ומבהירה שחדירה למרחב דיגיטלי פרטי של העובד, המגודר באמצעות שם וסיסמה, מחייבת צו שיפוטי.

לאחר סיום כתיבת מחקר זה התקבל בבית הדין הארצי לעבודה פסק הדין בפרשת **אלקנר**. בית הדין התווה שם מבחן תלת־שלבי לבחינת הפגיעה בפרטיות. בשלב הראשון נבדק אם תכלית הפגיעה בזכות העובד לפרטיות היא לגיטימית. בשלב השני נבדקת מידתיות הפגיעה, ובמסגרתה מובאים בחשבון שיקולים כגון המרחב שבו בוצעה. בשלב השלישי והאחרון בוחן בית הדין את מידת השקיפות שנקט המעסיק ואת הסכמת העובד. ככל שהפגיעה בפרטיות העובד חמורה יותר, כך דרישת ההסכמה תהא מקיפה יותר. עם זאת, במקרי קצה שבהם הפגיעה בפרטיות חמורה ביותר, הבהיר בית הדין כי לא ניתן יהיה להכשירה באמצעות קבלת הסכמת העובד. בית הדין בפרשת **אלקנר** הבחין בין נסיבות הפגיעה בפרטיות בפרשת **איסקוב**, שבה דובר על עיבוד מידע אישי לאחר איסופו, לבין נסיבות המקרה שלפניו. לשיטתו, בפרשת אלקנר נבחנו גבולות הזכות לפרטיות וטרם נעשה שימוש במידע אישי שנאסף. עם זאת, מפסק הדין לא ברור באילו נסיבות תחייב ההלכה מפרשת **איסקוב** ובאילו יש לפעול לפי המבחן התלת־שלבי שנקבע בפרשת **אלקנר**.[312]

העמדות השונות שהוצגו בדין הישראלי בנוגע לאופן בחינת חוקיותה של פגיעה בפרטיות עקב שימוש בטכנולוגיות מעקב במסגרת יחסי עבודה מדגימות את עיקר הקושי בבחינת סוגיה זו ואת הסכנה שבקביעת כללים מתוך התמקדות בפגיעה בפרטיות במרחב מסוים בלבד ואגב התעלמות מכך שייחוס הזכות

312 פרשת **אלקנר**, לעיל ה"ש 128.

לפרטיות למרחבים מסוימים הופך לקשה ולמורכב על רקע התפתחות הטכנולוגיה וטשטוש הגבולות בין המרחבים השונים.[313] נקודת המוצא במהלך השנים לבחינת פגיעה בפרטיות העובד הייתה שהעובד נמצא במרחב השייך למעסיק, בין שמדובר במרחב הדיגיטלי שהמעסיק מעמיד לרשותו ובין שבמרחב הפיזי, כלומר במקום העבודה עצמו או ברכב אשר המעסיק נתן לו לשימוש לצורכי עבודה או בעיקר לצורכי עבודה. אולם, הטכנולוגיות למעקב אחר עובדים מטשטשות את ההבחנה בין המרחבים, מאפשרות מעקב חודרני פי כמה מזה שבוצע בעבר במקומות עבודה, במרחבים שונים שלא היו קיימים בעבר ותוך כדי ביצועו בכמה מרחבים בעת ובעונה אחת. כך, לדוגמה, טכנולוגיית מעקב יכולה להיות מותקנת במרחב הפיזי של המעסיק, למשל במגרש החנייה או באולם העבודה הפתוח במקום העבודה, וכן על גבי חומרה שמספק המעסיק לעובד, כגון מחשב אישי או טלפון נייד, אך תוך חדירה למרחבים דיגיטליים ואף פיזיים אישיים של העובד.

יתרה מכך, בעת עבודה מרחוק הנסיבות המוכרות מתהפכות, והנחת המוצא לבחינת פגיעה בפרטיות העובד שלפיה הפגיעה מתרחשת בעת שהעובד נמצא במרחב השייך למעסיק אינה נכונה עוד. עתה העובד נמצא פיזית במרחב האישי שלו, ואליו הוא מכניס את המעסיק ואת מערכות המחשוב שלו. אולם, שוני זה אינו מלמד בהכרח על שינוי ביחסי הכוחות. העובד עודו נמצא במערכת יחסי עבודה לא שוויונית ותלוי במעסיק לפרנסתו.

לפיכך, ובדומה להלכה שנקבעה בפרשת **אלקנר**, בחינת מידתיות הפגיעה בפרטיות העובד עקב שימוש בטכנולוגיות מעקב צריכה להביא בחשבון את המשקל שיש לתת לכל אחד מהמרחבים הבאים:

(**1**) המרחב הפיזי שבו נמצא העובד בעת הפגיעה בפרטיותו, ועשוי להיות אחד מאלה:

א. מרחב ציבורי או מרחב ציבורי עסקי (למשל, אולם קבלת הפנים במפעל).

313 Tali Hatuka & Eran Toch, *Being Visible in Public Space: The Normalisation of Asymmetrical Visibility*, 54 Urban Studies 984, 992 (2017)

ב. מרחב עסקי בלבד (למשל, עמדת העבודה בחלל הפתוח בחברת הייי־טק, עמדת העבודה ליד מסוע במפעל, חלל עבודה משותף לכמה עובדים במועצה מקומית).

ג. מרחב עסקי־פרטי (למשל, חדר המנוחה במקום העבודה, המטבחון).

ד. מרחב פרטי בלבד (למשל, ביתו של העובד).

(**2**) המרחב הפיזי שעל גביו מותקנת או שממנו פועלת הטכנולוגיה המפירה את פרטיות, העשוי להיות אחד מאלה:

א. חומרה בבעלות המעסיק (למשל, מחשב או טלפון נייד שהמעסיק נותן לעובד למטרות עבודה בלבד).

ב. חומרה משולבת עסקית פרטית (למשל, מחשב או טלפון נייד שהמעסיק נתן לעובד למטרות עבודה והתיר לו להשתמש בו גם למטרות פרטיות).

ג. חומרה פרטית בלבד של העובד (למשל, טלפון או מחשב נייד פרטי של העובד בלבד, כרטיס סים של העובד שמותקן במכשיר טלפון נייד שנתן לו המעסיק ומאפשר תפעול שני כרטיסי סים בעת ובעונה אחת).

(**3**) המרחב הדיגיטלי שבו נמצא המידע האישי על אודות העובד שעיבודו פוגע בפרטיותו, העשוי להיות אחד מאלה:

א. מרחב דיגיטלי עסקי בלבד (למשל, יומן, תיבת דוא״ל, תוכנת התכתבות פנימית, מיקרוסופט 365).

ב. מרחב דיגיטלי משולב עסקי־פרטי (למשל, יומן או תיבת דוא״ל שהמעסיק מתיר לעובד להשתמש בהן למטרות עבודה ולמטרות פרטיות).

ג. מרחב דיגיטלי פרטי פתוח (למשל, היסטוריית הגלישה של העובד באתרי אינטרנט).

ד. מרחב דיגיטלי פרטי סגור (הכוונה לכל שירות דיגיטלי מוגן בסיסמה, למשל וואטסאפ, תיבת דוא״ל ענן ופרטי).

בצד ההתייחסות למרחבים, יש לתת את הדעת גם לרגישות המידע האישי המעובד, החל ממידע מידע אישי פתוח לציבור (תמונת העובד או פוסט שלו המוגדרים פתוחים לכלל הציבור), עובר במידע אישי שאינו רגיש ואינו פתוח לציבור וכלה במידע אישי רגיש (למשל, מדדים ביומטריים או פיזיולוגיים משעון

חכם או מעקב אחר תנועות העיניים של העובד). כן יש לתת את הדעת להיקף המידע האישי הנאסף ולתדירות איסופו. מכלול נתונים אלו מלמדים על מגוון התובנות שניתן להפיק ממנו ומהווים מדדים למידת החודרנות טכנולוגיית המעקב. מדובר במנעד. ככל שהמרחב הפיזי בו מצוי העובד בעת שמתרחשת הפגיעה בפרטיות (מקום העבודה פיזית, רכב של המעסיק, או ביתו של העובד), והמרחב בו מבוצעת הפגיעה (מקום העבודה פיזית, רכב של המעסיק, המרחב הווירטואלי המקצועי, האישי פרטי מוגן בסיסמה או פרטי שאינו מוגן בסיסמה, והמרחב הפיזי הפרטי של העובד) פרטיים יותר, והמידע שטכנולוגיית המעקב אוספת רגיש ורב יותר, כך ציפיתו הסבירה של העובד לפרטיות גבוהה יותר והפגיעה חודרנית יותר, ועל כן חמורה יותר ומידתית פחות. התייחסות למנעד זה במסגרת בחינת חוקיות הפגיעה בזכות העובד לפרטיות תבטיח שהכלל המשפטי לא יהיה מוגבל לנסיבות מסוימות או לטכנולוגיה מסוימת.

לדעתי להסכמת העובד, אין לתת שום משקל, לנוכח פערי הכוחות בין העובד לבין המעסיק וחולשת דרישת ההסכמה בנסיבות של פגיעה בפרטיות.[314]

4.2 מודעות גורם הביניים

טכנולוגיות למעקב אחר עובדים הן כאמור דו־שימושיות. הן יכולות לאפשר שימושים חוקיים, אולם גם שימושים המאפשרים מעקב מתמשך, חודרני ופוגעני. משום כך, הוכחת מודעות יצרן הטכנולוגיה לכך שנעשה בה שימוש לא חוקי היא מורכבת. בדומה למפתחי טכנולוגיות שיתוף הקבצים למיניהן, גם מפתחי טכנולוגיות למעקב אחר עובדים יטענו שהטכנולוגיה מיועדת לשימושים חוקיים ולגיטימיים, למשל מתן כלים לייעול העסק במתווה עבודה היברידי לנוכח איבוד השליטה הפיזי של המעסיק. יתרה מכך, בהיעדר כללים ברורים

314 להרחבה בנוגע לחולשת דרישת ההסכמה ראו רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר **הצעת חוק הגנת הפרטיות התשע"ט-2019** (המכון הישראלי לדמוקרטיה, יוני 2019), עמ' 13.

להגדרת פגיעה בזכות העובד לפרטיות ואף בהנחה שקיימים כללים ברורים לבחינת חוקיות פגיעה בפרטיות, כמו באיחוד האירופי, הרי שמדובר בשאלה של איזון בין הפררוגטיבה הניהולית של המעסיק לבין זכות העובד לפרטיות וכן בבחינה של מידתיות. לכאורה, מפתח טכנולוגיות מעקב יתקשה לאמוד מראש את האיזון הראוי בין הפררוגטיבה הניהולית של המעסיק המסוים שרכש רישיון שימוש לטכנולוגיית המעקב לבין השימוש שייעשה בטכנולוגיה זו בפועל, וכך לדעת אם מבקש הרישיון עומד לעשות בטכנולוגיה שימוש בלתי חוקי. עם זאת, סוגיה זו מזכירה את טענתם של מפתחי תוכנות לשיתוף קבצים שאין ביכולתם לדעת מראש אם משתמש הקצה זכאי ליהנות מחריג השימוש ההוגן אם לאו. גם במקרה של חריג השימוש ההוגן, שאלת חוקיות השימוש בטכנולוגיית שיתוף הקבצים נתונה לשיקול דעת בית המשפט. ואולם, נפסק שקיומם של שימושים חוקיים אינו רלוונטי לשאלת מודעות המפר התורם, מפני שזו נבחנת רק לגבי השימושים המפירים.

סקירת מקצת מטכנולוגיות המעקב הקיימות בשוק כיום מלמדת לדעתי על מודעות ממשית וקונקרטית של יצרני טכנולוגיות המעקב שנסקרו לאפשרות השימוש הבלתי חוקי שיכול להיעשות בטכנולוגיות שלהם. כך, למשל, חברת Hubstaff מציינת אומנם שפרטיות העובדים חשובה, אך בה בעת מעניקה למעסיק יכולת לשלוט בחודרנות המעקב שהוא מבצע. באפשרותו לבחור אם הטכנולוגיה תבצע תצלומי מסך עיתיים של מחשבו של העובד, כדי לעקוב אחר היסטוריית הגלישה שלו. מדרג חודרנות זה המוטמע בטכנולוגיה מלמד על מודעותה של החברה לאפשרות השימוש בטכנולוגיה שהיא משווקת לשם פגיעה בפרטיות העובד. יתרה מכך, מאחר ש־Hubstaff יודעת מתי המעסיק בוחר בהפעלת פונקציות אלו בטכנולוגיה, הרי שמודעותה היא מודעות ממשית וקונקרטית.[315] גם אמירתה, הומוריסטית לכאורה, של חברת Analog Republic Ltd המשווקת את טכנולוגיות המעקב אחר עובדים Sneek, ולפיה "כן, כולנו מחטטים באף, זו לא בושה"[316] מלמדת שהחברה מודעת באופן ממשי וקונקרטי

315 ראו את הדיון בסעיף 1.3 **לעיל**.

316 המשפט המקורי מובא באנגלית: "Yes, we all pick our noses, there's no shame", ראו באתר האינטרנט של החברה.

לרמת החודרנות והפגיעה בפרטיות האפשרית באמצעות טכנולוגיית המעקב שפיתחה.[317]

אף שבישראל נדונה בערכאת בית המשפט העליון רק שאלת המודעות בפועל, קיים חוסר אחידות בנוגע לפרשנותה בארצות הברית. בהיעדר שימוש חוקי משמעותי די בהוכחת מודעותו בכוח של גורם הביניים להפרה ספציפית, אך כאשר קיים שימוש חוקי משמעותי נדרשת הוכחת מודעות בפועל לשימוש מפר. עם זאת, היקף השימוש החוקי שיוכר כשימוש חוקי משמעותי אינו ברור. כן קיימת מחלוקת שטרם הוכרעה בין ערכאות הערעור בשאלה אם עצימת עיניים מכוונת מספיקה לשם הוכחת מודעותו של גורם הביניים לשימושים לא חוקיים.[318] באירופה, לעומת זאת, דרישת המודעות כוללת מודעות בפועל או מודעות בכוח העשויה להילמד מהנסיבות או מפעולות שנוקט ספק שירותי האינטרנט בעצמו. עם זאת, מודעות כללית לדו־שימושיות האפשרית של השירות אינה מספיקה לשם הקמת מודעות בכוח. במקרים מסוימים, למשל לגבי ספק תוכן שיתופי באינטרנט, ניתן משקל גם לכוונת הספק לצד שאלת מודעותו, להימנעותו מנקיטה מראש של אמצעים טכנולוגיים מידתיים וסבירים לשם מניעת הפרה לגבי ספק שירותים אינטרנטיים אחרים.[319]

חוסר האחידות בארצות הברית לצד ההכרה האירופית במודעות בפועל בנסיבות מסוימות יכולים לשמש בסיס להצדקת השימוש בדרישת המודעות כקרקע פורייה לקליטת שיקולי מדיניות הרלוונטיים להגנה על הזכות לפרטיות בעת הזו. כך, בנסיבות מסוימות, ייתכן שהרחבת דרישת המודעות למודעות בכוח לצד מודעות בפועל תהא מוצדקת.

כך, למשל, המלצתה של חברת Prodoscore למעסיקים "להיות אנושיים" לנוכח אפשרות השימוש לרעה במידע אישי הנצבר באמצעות הטכנולוגיה שלה על העובד, עשויה ללמד על מודעותה בכוח לפגיעה אפשרית בזכות לפרטיות.[320] כמו

317 ראו את הדיון בסעיף 1.3 **לעיל**.

318 ראו את הדיון בסעיף 2.1 **לעיל**.

319 ראו את הדיון סעיף 2.1 **לעיל**.

320 ראו את הדיון סעיף 1.3 **לעיל**.

כן ניתן לטעון שככל שטכנולוגיית מעקב מאפשרת מעקב חודרני יותר מבחינת מרחב הפגיעה בפרטיות, משך המעקב והיקף המידע הנאסף, ומפתחיה אף מעודדים או מצהירים על אפשרות לעשות שימושים כאמור, ניתן לראות בהם מודעים בכוח לאפשרות השימוש לרעה בטכנולוגיה שפיתחו.

4.3. תרומה משמעותית, ניכרת וממשית

דרישת התרומה המשמעותית בדוקטרינת ההפרה התורמת בדיני זכויות יוצרים התמקדה בשאלה אם בידי גורם הביניים אמצעים סבירים, מן הבחינה הכלכלית, למנוע את ההפרה הישירה. מפתחת טכנולוגיות למעקב אחר עובדים שמעניקה גם שירותי תמיכה טכניים, במהלך תקופת הרישיון, יכולה לנקוט צעדים למניעת שימוש בלתי חוקי בטכנולוגיה שלה. למשל, ניתן להטמיע בטכנולוגיה מנגנון Kill Switch לשם הפסקת השימוש בה, בטרם פקיעת רישיון השימוש, אם נמצא שנעשה בה שימוש בלתי חוקי. כמו כן, יכולה החברה המפתחת לחסום או להתנות באישור גורם מורשה בכיר, שימוש בפונקציות מסוימות בטכנולוגיית המעקב. כך, למשל, עושה חברת DeskTime המאפשרת למעסיק לבחור אם לצלם את המסך של מחשבו של העובד באופן עיתי לגבי כל העובדים, לגבי עובדים מסוימים המוגדרים על ידו או להימנע מכך לחלוטין.[321] כלומר, בידי חברה המפתחת טכנולוגיה למעקב אחר עובדים אמצעים סבירים מן הבחינה הכלכלית להפסיק או למנוע מלכתחילה את הפגיעה בזכות העובד לפרטיות.

321 ראו את הדיון סעיף 1.3 **לעיל**.

4.4
סיכום ביניים: התנאים להחלת דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות במסגרת יחסי עבודה

יישומם של התנאים המצטברים להוכחת עוולת ההפרה התורמת בדיני הגנת הפרטיות בנסיבות של שימוש בטכנולוגיות למעקב אחר עובדים תלוי בראש ובראשונה בשאלת ההפרה הישירה אשר מציגה נסיבות חדשות ולא מוכרות מבחינת המשפט והדין הנוהג. טכנולוגיות למעקב אחר עובדים מאפשרות מעקב וחדירה לקודש הקודשים הפרטי של העובד, ביתו. בד בבד הן מאפשרות מעקב חודרני בכמה מרחבים בו זמנית, המאפשר הצצה לנימי נפשו של העובד, בין שהוא עובד מרחוק ובין שהוא עובד פיזית במקום העבודה.

לפיכך, בבחינת מידתיות הפגיעה בפרטיות יש לעמוד על תכלית הפגיעה יש לתת את הדעת למרחבים שבהם אירעה הפגיעה, משכה, היקף המידע האישי שנאסף באמצעותה ומידת רגישותו.

באשר לדרישת המודעות, בחלק מהמקרים, ניתן להסיק על מודעות ממשית וקונקרטית של יצרן טכנולוגיות המעקב לשימוש הבלתי חוקי שיבוצע בטכנולוגיית המעקב שפיתח. במקרים אחרים, המידע השיווקי שמספקים יצרני טכנולוגיית המעקב אחר עובדים על הטכנולוגיות שיצרו מלמד דווקא על עצימת עיניים מכוונת העולה לכדי מודעות בכוח מצידם. חוסר האחידות הקיים בפרשנות דרישת המודעות בארצות הברית, והעובדה שבאיחוד האירופי הסתפק המחוקק, בתנאים מסוימים, בהוכחת מודעות בכוח באמצעות הוכחת עצימת עיניים מכוונת, עשויים להתפרש כבסיס להכרה בהוכחת עצימת עיניים מכוונת כמספקת גם במקרה של אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות.

לבסוף, ניתן ללמוד על תרומה משמעותית לפגיעה בפרטיות מצד החברות המפתחות את טכנולוגיות למעקב אחר עובדים בעקיפין, מכך שבמאמץ סביר

ביכולתן להגביל, למנוע או להפסיק שימוש בטכנולוגיה למעקב אחר עובדים אשר פוגע בזכות לפרטיות.

לפיכך, בהיעדר שיקולי מדיניות משמעותיים נגד אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות ביחס לטכנולוגיות למעקב אחר עובדים, נראה שאין מניעה מאימוצה. לא זו אף זו, הפגיעה החמורה בזכות העובד לפרטיות המתאפשרת באמצעות טכנולוגיות למעקב אחר עובדים הפועלות בחוסר שקיפות ומאפשרות חודרנות קיצונית תוך כדי טשטוש הגבולות בין מקום העבודה לבין מרחב הפרטי של העובד במתווה העבודה ההיברידי, וחולשת הזכות לפרטיות זה שנים אף מחייבות את חיזוקה באמצעות ייבוא דוקטרינת ההפרה התורמת בנסיבות הללו.

פרק 5

סיכום

טכנולוגיות למעקב אחר עובדים הן טכנולוגיות דו־שימושיות. מחד גיסא, הן משמשות להגשמת אינטרסים ציבוריים חשובים, כגון שכלול שוק העבודה בעידן פוסט־הקורונה ומתווה העבודה ההיברידי, הגנה על העובד מפני שחיקה וניצול יעיל וחכם של כוח העבודה. מאידך גיסא, הן עלולות לגרום לפגיעה חמורה בזכות העובד לפרטיות כאשר הן מאפשרות מעקב חודרני, חוצה מרחבים ורחב היקף אחר מידע אישי ורגיש על אודות העובד. בחינת פגיעה זו בפרטיות מחייבת שינוי גישה כפול: הן ברמת בחינת ההפרה הישירה של זכות העובד לפרטיות והן בשאלת האחריות להפרה חמורה זו.

באשר לבחינת ההפרה הישירה, ראשית, אין לדעתי לתת שום משקל להסכמת העובד, לנוכח פערי הכוחות בין העובד למעסיק וחולשת דרישת ההסכמה בנסיבות של פגיעה בפרטיות.[322] לדעתי נקודת המוצא שהייתה מקובלת במשך השנים לבחינת פגיעה בפרטיות העובד – ולפיה העובד נמצא במרחב השייך למעסיק – אם זה המרחב הדיגיטלי שהמעסיק מעמיד לרשותו או המרחב הפיזי, קרי מקום העבודה עצמו או רכב אשר ניתן לו על ידי המעסיק לשימוש לצורכי עבודה, או בעיקר לצרכי העבודה, אינה רלוונטית עוד. טכנולוגיות למעקב אחר עובדים מטשטשות את ההבחנה בין המרחב העסקי לבין המרחב הפרטי, מאפשרות מעקב חודרני פי כמה מזה שבוצע בעבר במקומות עבודה, במרחבים שונים שלא היו קיימים בעבר ותוך ביצועו בכמה מרחבים בו זמנית. כך, טכנולוגיית מעקב יכולה להיות מותקנת במרחב פיזי של המעסיק, למשל חומרה שהמעסיק מספק לעובד כגון מחשב נייד, ולאפשר איסוף מידע אישי ממרחבים דיגיטליים ואף פיזיים אישיים של העובד. משום כך, כחלק מבחינת מידתיות הפגיעה בפרטיות במסגרת הערכת חוקיותה, יש להביא בחשבון את המרחב הפיזי שבו נמצא העובד בעת הפגיעה בפרטיות, המרחב הפיזי שעל גביו מותקנת טכנולוגיית המעקב והמרחב הדיגיטלי שנאסף ממנו המידע האישי. כמו כן יש לתת את הדעת לרגישות המידע האישי המעובד, היקפו ותדירות איסופו.

322 להרחבה בנוגע לחולשת דרישת ההסכמה ראו אריאל הרשקוביץ ושוורץ אלטשולר, **הצעת חוק הגנת הפרטיות התשע"ט-2019, לעיל** ה"ש 312, עמ' 13.

ככל שהמרחב הפיזי בו מצוי העובד בעת שמתרחשת הפגיעה בפרטיות (מקום העבודה פיזית, רכב של המעסיק, או ביתו של העובד), והמרחב שמבוצעת בו הפגיעה (מקום העבודה פיזית, רכב של המעסיק, המרחב הווירטואלי המקצועי, האישי פרטי מוגן בסיסמה או פרטי שאינו מוגן בסיסמה, והמרחב הפיזי הפרטי של העובד) – פרטיים יותר והמידע שטכנולוגיית המעקב אוספת רגיש ורב יותר, כך ציפייתו הסבירה של העובד לפרטיות גבוהה יותר והפגיעה חודרנית יותר, ועל כן חמורה יותר ומידתית פחות. מתן משקל למנעד זה כחלק מבחינת חוקיות הפגיעה בזכות העובד לפרטיות יבטיח שהכלל המשפטי לא יהיה מוגבל לנסיבות מסוימות או לטכנולוגיה מסוימת.

באשר לשאלת האחריות, יש לדעתי מקום לאמץ את דוקטרינת ההפרה התורמת מדיני זכויות היוצרים לדיני הגנת הפרטיות, ככלי נוסף בארגז הכלים העומד לרשותו של העובד לשם הגנה על זכותו לפרטיות ועל הערכים החשובים שבבסיסה, ובראשם זכותו לכבוד ולאוטונומיה. אימוץ דוקטרינת ההפרה התורמת יחזק את הזכות לפרטיות הנתונה זה שנים מספר במגננה למול התפתחויות טכנולוגיות חדשניות המתייחסות למידע אישי כאל נכס סחיר, ויש בו כדי להשיב את המשקל הראוי לערכים שבבסיס הזכות לפרטיות הנגזרת מן הזכות לכבוד ומשמעותית לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו ללא התערבות זרה. כן תפתור דוקטרינת ההפרה התורמת את כשלי השוק המאפיינים שוקי מידע, ובראשם התמודדות עם החצנות שליליות, מידע א־סימטרי והקושי של נפגעים רבים ומבוזרים לפעול באופן קולקטיבי. חיזוק הזכות לפרטיות חשוב בייחוד בישראל, שנדמה שהופכת ל"חצר האחורית" של מדינות המערב הדמוקרטיות בכל הקשור להגנת הפרטיות. במסגרת יחסי עבודה, יוביל אימוץ דוקטרינת ההפרה התורמת לחיזוק העובד במערכת המאופיינת בפערי כוחות ניכרים בעיקר נוכח התפיסה המרחיבה של הפררוגטיבה הניהולית של המעסיק בשנים האחרונות.

אומנם, אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי להוביל לכשל אכיפה הנוגע לסמכות השיפוט והדין החל ולפגיעה באינטרסים נוספים נוכח רוחבה של הזכות לפרטיות. עם זאת, חקיקת ה־GDPR ו"אפקט בריסל" שהגיע בעקבותיו עשויים להביא להאחדה יחסית של הגדרת הזכות לפרטיות במרבית מדינות העולם ולריכוך הכשל האכיפה. באשר לפגיעה באינטרסים נוספים, ובראשם אינטרס המעסיק והציבור בכללותו בשכלול וייעול שוק

העבודה בעידן הפוסט־קורונה, יש לזכור שמדובר באינטרסים שמשקלם פחות לעומת הזכות החוקתית לפרטיות והסיכון לניצול לרעה של עובדים עקב החרפת פערי המידע והכוחות ביניהם לבין המעסיקים בעקבות שימוש בטכנולוגיות מעקב. הדבר מצדיק לדעתי את אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות. ההגנה על האינטרסים הציבוריים החשובים תיעשה במסגרת בחינת מידתיות הפגיעה בפרטיות.

אף שמפתחי טכנולוגיות למעקב אחר עובדים אינם בהכרח בעלי הכיס העמוק, קיים לדעתי אינטרס ציבורי מבחינת שיקולי צדק חלוקתי המצדיק את הסטת עלויות הפיקוח והאכיפה מעובדים בודדים אל אלו המעניקים למעסיקים כלים למשטור חודרני של העובד באמצעות מעקב ממושך ורציף עליו ומסייעים בכך להפיכת מקום העבודה לזירת מעקב הנדמית כלקוחה ממשטרים אפלים, וסביר שיש אף ביכולתם לפקח ביעילות ובאופן פשוט וזמין יחסית על המפירים הישירים, להפסיק את שיווק הטכנולוגיה או לשנותה באופן אשר ימנע המשך השימושים לרעה בה. זאת בעיקר לאור העובדה שקיימים אמצעים אחרים, שפגיעתם בפרטיות העובד פחותה, לשם שיפור יעילותו של העובד ורווחיות המעסיק.

לבסוף, שיקול מדיניות חשוב נגד אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בהקשר של טכנולוגיית מעקב אחר עובדים הוא זהותו של המפר הישיר. בניגוד להפרת זכות יוצרים שבמסגרתה עמדו בעלי הזכויות מול מפירים רבים, מבוזרים ולעיתים אף אנונימיים, במקרה של פגיעה בפרטיותו של עובד זהותו של הפוגע הישיר ידועה, איתורו קל והוא אף עשוי להיות בעל כיס עמוק, שכן מדובר במעסיק עצמו. עם זאת, עובדים רבים מורתעים מפני תביעת המעסיק הישיר שלהם הן נוכח הפגיעה הצפויה בפרנסתם ובמוניטין שלהם. כמו כן טכנולוגיות מעקב מקשות על יכולתם של עובדים להתאגד ולבוא בדרישות משותפות למעסיק. בעקבות זאת עובדים הנתונים תחת טכנולוגיות מעקב מוחלשים עוד יותר מבחינת יחסי הכוחות ביניהם לבין המעסיק. ולבסוף, קיים אינטרס ציבורי משמעותי באימוץ דוקטרינת ההפרה התורמת שכן היא עשויה לתמרץ את החברות המפתחות לפעול למזעור הפגיעה האפשרית בזכות לפרטיות, למשל על ידי צמצום חלק מהתכונות האפשריות של טכנולוגית המעקב, ממגוון המידע האישי שהיא אוספת ומעבדת, או מטווח התובנות שהיא יכולה להפיק על בסיס עיבוד מידע על ידי בינה מלאכותית. כן אימוץ

דוקטרינת ההפרה התורמת עשוי להוביל את מפתחי טכנולוגיות המעקב להגביר את הפיקוח על השימושים הנעשים בה במסגרת רישיון השימוש לשם הבטחת שימוש ראוי.

ההתחשבות בחששות המתנגדים לאימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יכולה להיעשות בבחינת יישומם של התנאים להחלת הדוקטרינה בכל מקרה ומקרה. קיומה של הפרה ישירה ייבחן בהתאם לחומרת הפגיעה על פני מנעד מרחבי הפגיעה, היקף המידע האישי שנאסף, רגישותו, משכו והשימושים שהטכנולוגיה מאפשרת לעשות בו.

מבחינת מודעות ממשית וקונקרטית, הרי שזו מתקיימת לגבי חלק ממפתחי הטכנולוגיות. זאת ועוד, ככל שטכנולוגיית מעקב מאפשרת מעקב חודרני יותר מבחינת מרחב הפגיעה בפרטיות, משך המעקב והיקף המידע הנאסף, ומפתחיה אף מעודדים או מצהירים על אפשרות לעשות זאת, ניתן לראות בהם כמי שעוצמים עיניהם במכוון עד כדי מודעות בכוח לביצוע פגיעה בפרטיות. חוסר האחידות הקיים בפרשנות דרישת המודעות בארצות הברית לצד ההכרה בחקיקה באיחוד האירופי בעצימת עיניים מכוּונת כמספקת, בנסיבות מסוימות, להוכחת דרישת המודעות, עשוי להוביל להכרה בעצימת עיניים כמספקת גם במקרה של אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות. יתרה מכך, לדעתי הצורך לחזק את הזכות לפרטיות וההשלכות השליליות של טכנולוגיות מעקב על מעמד העובד למול המעסיק אף מצדיקות את הרחבת דרישת המודעות כך שתכלול גם מודעות בכוח המתבטאת בעצימת עיניים מכוונת.

לבסוף, לדעתי מתקיימת דרישת התרומה הממשית להפרה מכיוון שמפתחות טכנולוגיות המעקב יכולות במאמץ סביר למנוע או להפסיק שימוש בטכנולוגיה למעקב אחר עובדים אשר פוגע בזכות לפרטיות.

לסיכום, ההמלצה המוצעת במחקר זה היא שבתי המשפט, ובעיקר בתי הדין לעבודה, יאמצו במקרים המתאימים את דוקטרינת ההפרה התורמת לשם הטלת אחריות על יצרן טכנולוגיה למעקב אחר עובדים. כמו כן, על ארגוני עובדים ועל עורכי דין בתחום דיני העבודה לפעול להגנה על זכות העובדים לפרטיות בהשתמשם בדוקטרינת ההפרה התורמת. ולבסוף, ראוי שיצרני טכנולוגיות

מעקב וכן עורכי דין המייעצים להם בשלבי הפיתוח הראשונים ישקלו לאמץ אמצעים טכנולוגיים וארגוניים להגנה על פרטיות העובד מתוך הכרה באפשרות שתוטל על יצרני הטכנולוגיה אחריות תורמת לפגיעה בפרטיות.

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy Paper 202

REMOTE WORKERS

Protecting Workers' Right to Privacy through the Doctrine of Contributory Infringement

Rachel Aridor-Hershkovitz

July 2025

Abstract

The Coronavirus pandemic created a new pattern of work: hybrid employment, where employees divide their workdays between the home office and the employer's workplace. Employers were suddenly confronted with the need to maintain the organization's efficiency in a reality in which they could not physically surveil workers. As a result, surveillance technologies began to develop not only among blue-collar workers, where they had been used in the past at varying levels of intrusiveness, but also among white-collar workers. The flourishing of technologies for surveilling employees led to an increasing emphasis on "worker visibility." In practical terms, this means the exposure of the worker's output, thoughts, and environment to the employer, leading to the growing blurring of the distinction between the workplace, the private domain, and the public domain.

However, a unidimensional description of technologies for surveilling employees is misleading. Some of these technologies have legitimate goals, particularly the desire to improve the job market in the hybrid era. Thus our subject actually relates to dual-use technologies that can be used to realize legitimate and important public and organizational

interests, but which may also lead to the grave violation of the worker's right to privacy.

This study focuses on the question of the violation of the worker's right to privacy due to the use of surveillance technology, recognizing its dual-use nature. The study reviews some of the employee surveillance technologies currently available in the market and describes the possible violation of privacy these permit. This is followed by an examination of the scope of the worker's right to privacy in the United States, the European Union, and Israel, as well as the existing reliefs available for workers whose privacy has been infringed due to the use of surveillance technology.

Based on this review, the study proposes the adoption of a different approach to examining the violation of workers' privacy. This approach does not assume as its starting point that the worker is present in a space that belongs to the employer, but rather takes into account the degree of intrusiveness made possible by surveillance technologies, both in terms of the scope of personal information they expose to the employer and in terms of the new domains to which they grant access to the employer. Thus a surveillance technology may be installed in the employer's physical domain—on the laptop the employer provides to the employee, for example—thereby permitting the collection of personal information from digital domains and even from the worker's physical surroundings. Accordingly, when examining the violation of the worker's right to privacy, it is important to take into account the physical domain in which the worker is present at the time of the violation, the domain in which the surveillance technology is installed, the digital or physical domain in which personal information is collected, the sensitivity of the processed personal information, and the scope and frequency of its collection. A spectrum thus emerges whereby the more private the physical domain where the employer is (i.e., the domain where the surveillance technology is installed) and the domain where the personal information is collected, and the more extensive and sensitive the information collected—the

more we will conclude that the violation of the worker's right to privacy should be considered intrusive and disproportionate. Addressing this spectrum when considering the legality of the violation of the worker's right to privacy will ensure that the legal rule will not be limited to certain circumstances or technologies.

In addition to examining the violation of the worker's right to privacy, the study also considers the possibility of imposing liability and claiming relief not only from employers who use technologies to surveil their employees, but also from the developers of these technologies. This would be possible through the adoption in privacy protection law of the contributory infringement doctrine, borrowed from intellectual property law. The adoption of this doctrine will serve as an additional tool in the toolbox available to employees in order to defend their right to privacy. This move is liable to cause an enforcement failure regarding jurisdiction and the applicable law and to damage additional interests due to the broad character of the right to privacy. However, it will provide the necessary strengthening of the right to privacy, which has been put on the defensive for years due to technological developments that regard personal information as a negotiable commodity.

The proposed move could restore the proper equilibrium of the values underlying the right to privacy, derived from the right to dignity—a right that is important for personal autonomy, self-definition, and the ability to take decisions without alien intervention. The adoption of the contributory infringement doctrine is in the public interest, since it may incentivize the companies that develop technologies to act to minimize the possible violation of privacy and to strengthen their supervision of the use of these technologies, such as by mitigating some of the potential characteristics of surveillance technology. For example, the types of personal collection the technology collects and processes could be restricted, as could the range of insights it provides, based on the use of artificial intelligence. Alternatively, the possible uses of these insights

could be restricted through the management of human resources in the organization, including decisions on recruitment, transfer, promotion, and dismissal.

Text Editor [Hebrew]: Galit Shamah
Series and Cover Design: Studio Alfabees
Typesetting: Ronit Gilad, Jerusalem
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-484-5

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-888
Website: en.idi.org.il

To order books:
Online Book Store: en.idi.org.il/publications
E-mail: orders@idi.org.il
Tel: (972)-2-5300-800

איך מגינים על פרטיות העובד בעידן שבו העבודה מתבצעת מהבית - והמעסיק רואה הכול?

בעידן שבו טכנולוגיות מעקב חודרות לכל היבט של סביבת העבודה, מחקר זה מציע כיוון חדש לחשיבה משפטית: החלת דוקטרינת ההפרה התורמת - המוכרת מדיני זכויות יוצרים - גם על דיני הגנת הפרטיות. באמצעותה ניתן להרחיב את גבולות האחריות לפגיעות בפרטיות הנגרמות משימוש בטכנולוגיות מעקב, לבחון מחדש את האיזון בין הפררוגטיבה הניהולית של המעסיק לבין זכות העובד לפרטיות ולחזק את ההגנה על זכות יסוד ההולכת ומתכרסמת.

ד"ר רחל אריאלי הרשקוביץ היא חוקרת בכירה בתוכנית "דמוקרטיה בעידן המידע" במכון הישראלי לדמוקרטיה; בעלת תואר שלישי במשפטים מהפקולטה למשפטים באוניברסיטת חיפה, בוגרת תואר ראשון במשפטים מאוניברסיטת חיפה ותואר שני במשפטים מאוניברסיטת ניו יורק. תחומי המחקר שלה הם פרטיות, הגנת סייבר, רשתות חברתיות ואתגרי המציאות הפיג'יטלית.

0 4500001334 6
דאנאקוד 450-1334

מחיר מומלץ: 45 ₪

יולי 2025 | מסת"ב: 978-965-519-484-5 | www.idi.org.il