*המאמר טרם עבר עריכה טכנית ולשונית, ולכן צפויים שינויים מסוימים בנוסח הסופי.

הזכות למידע פרטי של עובדים בעידן של הגנת סייבר

מאת

עינת אלבין* וגיל עומר**

הגנת סייבר הפכה בשנים האחרונות למאמץ מהמעלה הראשונה. חברות וכן ממשלת ישראל מאמצות מדיניות ורוכשות תוכנות להגנה על הסייבר לשלל מטרות, ביניהן הגנה על מאגרי מידע ועל מערכות ממוחשבות, מתן שירות שוטף, והגנה על אינטרסים ביטחוניים, חברתיים וסביבתיים. ואולם, ההגנה על הסייבר נעשית, בין היתר, על ידי ניטור פעולות של עובדות ועובדים - איסוף מידע רב אודותיהם, כולל מידע פרטי, עיבודו, הסקת מסקנות ולעיתים העברת המידע לידיים שלישיות. פעולות אלו פוגעות בזכות הבסיסית להגנה על מידע פרטי. מאמר זה עוסק במתח העדין שבין חשיבות ההגנה על המרחב הקיברנטי לבין זכות העובדים להגנה על מידע פרטי. בעודו נע בין החובות המשפטיים שיש למעסיקים, העדר האחריות של חברות הטכנולוגיה להגן על פרטיות המידע, והתפקיד שממלא הרגולטור – מערך הסייבר הלאומי והרשות להגנת הפרטיות - כמו גם על החשש מגישת הביטחוניזציה לגבי הגנה על הסייבר, המאמר מצביע על הפררוגטיבה המועצמת שיש למעסיק לפגוע במידע הפרטי של העובדים. הוא גם מראה כי דיני הגנת הפרטיות בעבודה, כפי שאלה פותחו על ידי בתי הדין לעבודה בשני פסקי דין מרכזיים – איסקוב ענבר וקלנסווה – ומיושמים בפסיקה הישראלית – לא נותנים מענה מלא להגנה על הזכות מידע פרטי בעידן של הגנת סייבר. המאמר מסכם עם הטענה לפיה יש לכייל את הכלים הקיימים על מנת להתאימם לאתגר של הגנת סייבר וכן לאמץ כלים משפטיים נוספים מעולם דיני העבודה וכן מהדין האירופאי לצורך ההגנה על מידע פרטי. כלים אלה עשויים להיות רלוונטיים גם למקרים נוספים בהם מידע פרטי של עובדים נפגע, מעבר להגנת סייבר.

א. מבוא

הזכות להגנה על מידע פרטי הפכה בשנים האחרונות לאחת מהזכויות היותר נדונות בשיח המשפטי, האקדמי והפרקטי, בין השאר בכל הנוגע לספירת העבודה.[1] הדאגה מפני העדר הגנה על מידע פרטי גברה בעידן הדאטה והשימוש בטכנולוגיות האוספות פיסות מידע רב על עובדים, מעבדות אותו, מגיעות למסקנות ומשייכות את המידע לאדם מסוים. הקשר ייחודי ומאתגר בדיון על הגנה על מידע פרטי של עובדים מגיע מהכיוון של הגנה על המרחב הקיברנטי, או מה שמכונה "הגנת סייבר".[2] אין מחלוקת, כי הגנת סייבר הנה מטרה חשובה והכרחית בעולם הדיגיטלי, בעיקר נוכח הסכנות האמיתיות והגוברות לפגיעה משמעותית דרך מרחב זה במאגרי מידע, וכן במערכות ממוחשבות שפגיעה בהן עשויה לגרום לא רק לנזק עסקי, אלא גם לנזק ביטחוני, סביבתי וחברתי. הגנה על המרחב הקיברנטי כוללת גם הגנה על מידע על עובדים ועל אינטרסים המשותפים למעסיקים ולעובדים. ואולם, הגנת הסייבר נעשית כיום, בין היתר, על ידי טכנולוגיות המבוססות על איסוף, עיבוד ואף פיזור מידע על עובדים,[3] דבר המעורר שאלות בדבר המתח בין הגנת הסייבר לבין זכותם של העובדים להגנה על המידע הפרטי שלהם. זו מטרתו של המאמר. הוא מבקש לשאול כיצד ניתן לאזן בצורה טובה יותר בין הגנת המרחב הקיברנטי להגנה על המידע הפרטי של העובדים.

---

* מרצה בכירה בפקולטה למשפטים האוניברסיטה העברית ומנהלת אקדמית של מרכז מינרבה לזכויות אדם.
** תלמידת תואר שלישי בכלכלה באוניברסיטת תל-אביב. בוגרת תואר ראשון במשפטים, תואר שני במנהל עסקים מהאוניברסיטה העברית ותואר שני מחקרי בכלכלה מאוניברסיטת תל-אביב (תכנית משותפת עם האוניברסיטה העברית).
ברצוננו להודות למיכאל בירנהק ותמי קצביאן על ההערות המועילות שהעבירו לגרסה קודמת של מאמר זה, לעו"ד עמית אשכנזי ולעו"ד טל מזרחי ממערך הסייבר הלאומי, למשתתפות ולמשתתפים בסדנת הסייבר של האוניברסיטה העברית, ולמשתתפות והמשתתפים בסדנת כיווני משפט לתואר שני במרכז האקדמי למשפט ולעסקים, על נקודות מצוינות שהעלו בדיונים שהתקיימו על טיוטות המאמר. כמו כן אנו מודות לד"ר נטע רוזן-שיף, למר אורי אלבין, מר גדי פרל, ומר אלי כהן על סיוע בחשיבה בנוגע לטכנולוגיה עצמה. לבסוף, נבקש לומר תודה ליסמין יונס ולכרמל הס על עבודת מחקר מצוינת. המאמר נתמך על ידי מענק ממרכז פדרמן לחקר הסייבר באוניברסיטה העברית.

[1] ראו למשל: מיכאל בירנהק "מעקב בעבודה: טיילור, בנת'האם והזכות לפרטיות" **עבודה, חברה ומשפט** יב 9, 34 (2010); שלי ולך "מישהו מתבונן בך: מעקב אחר עובדים במקום העבודה וזכות העובד לפרטיות" **ספר אלישבע ברק** 1 (2012);
LAB. L. & .Matthew W. Finkin, *Menschenbild: The Conception of the Employee as a Person in Western Law*, 23 COMP Y J., 577, 580–86 (2002); Virginia Mantouvalou, *Work and Private Life: Sidabras and Dziautas v. Lithuania*, 30 EUR. ׳POL L. REV. 573, 575–82 (2005); MARTA OTTO, THE RIGHT TO PRIVACY IN EMPLOYMENT (2016); Ugo Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection?, in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGY 159 (Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds., 2017); Matthew T. Bodie, Miriam A. Cherry, Marcia L. McCormick & Jintong Tang, *The Law and Policy of People Analytics,* 88 U. Colo. L. Rev. 961 (2017); Lucas D. Introna, *Workplace Surveillance, Privacy, and Distributive Justice*, 30 COMPUT. & SOC'Y 33 (2000); Frank Hendricks, *Privacy 4.0 at Work: Regulating Employment, Technology and Automation*, 41 COMP. LAB. L. & POL׳Y J. 147 (2019); Valerio De Stefano, *Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection* (ILO, working paper No. 246, 2018); Antonio Aloisi & Elena Gramano, *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context,* 41 COMP. LAB. L. & POL׳Y J. 95 (2019); Tammy Katsabian, *Employee's Privacy in the Internet Age*, 40(2) BERKELEY J. EMP. & LAB. L. 203 (2019).

[2] במאמר זה לא נעסוק בהתקפת סייבר, אלא רק בהגנה.

[3] יצוין כי המתח בין הגנה על המרחב הקיברנטי לבין הגנה על הפרטיות אינו ייחודי רק לפרטיותם של עובדים. כך למשל, טכנולוגיות הגנת הסייבר אוספות מידע רב גם על לקוחות וספקים. ואולם, אנו מתמקדות בהקשר הייחודי של יחסי עבודה.

כאמור, הגנת סייבר הנה אחד האתגרים הגדולים ביותר של העידן הנוכחי.[4] גם ממשלת ישראל קבעה כי מדובר במאמץ לאומי ממדרגה ראשונה והקימה את מערך הסייבר הלאומי.[5] חברות מקימות יחידות להגנת סייבר ומשתמשות בטכנולוגיות מתקדמות לשם השגת מטרה זו, ולמעסיקים ישנן חובות להגנה על מידע של עובדים ושל לקוחות.[6] במקביל, שוק פיתוח תוכנות להגנת סייבר פורח ומגוון השירותים המוצעים למעסיקים להשגת ההגנה הטובה ביותר גדל בצורה משמעותית בשנים האחרונות.[7]

טכנולוגיות הגנת הסייבר מעמידות במתח חובות וזכויות משפטיות, ומחייבות חשיבה מסודרת בהקשר של דיני העבודה. החובות להגנת סייבר נגזרות מתחיקה, כגון תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות אבטחת מידע"), החלות על בעלי מאגרי מידע, וכן החוק להסדרת הביטחון בגופים ציבוריים, תשנ"ח-1998 ("החוק להסדרת הביטחון") הקובע כללי אחריות והתנהלות להגנה על מערכות ממוחשבות חיוניות, לרבות המידע האגור בהן. מעבר לדברי חקיקה אלה, מעסיקים אמונים על פעילותו השוטפת של העסק דבר שמחייב הגנה על המרחב הקיברנטי, ועשוי לחשוף את החברה ונושאי המשרה בה לקנסות ותביעות משפטיות.[8] פריצת סייבר עשויה לפגוע במתן שירות שוטף ותקני, ובמקרים מסוימים, כאמור, אף עשויה לפגוע באינטרסים ביטחוניים, חברתיים וסביבתיים רחבים יותר. הרצון שהעסק יפעל באופן שוטף וללא תקלות, והגנה על אינטרסים רחבים יותר משותפים גם לעובדים. מידע רגיש רב על העובדים מצוי במאגרי המידע,[9] פרנסתם תלויה בהתנהלותו התקינה של העסק, ובהיותם חלק מהחברה הם אף צריכים להיות מוטרדים מהסכנות הביטחוניות, החברתיות והסביבתיות שישנן מפריצה למרחב הקיברנטי.

ואולם, בה בעת, טכנולוגיות הגנת הסייבר עצמן מבוססות על ניטור אחר פעולות במרחב הקיברנטי, איתור סכנות לפגיעה במרחב זה, וזאת תוך איסוף מידע רב אודות הפעילות ברשת ועיבודו על בסיס ניתוח שמבקש לזהות אנומליה בתעבורה.[10] עובדות ועובדים, כמשתמשי קצה במערכות הארגון, הנם מבין הגורמים העיקריים שפעולותיהם עשויות להיות מנוצלות לפגיעה במרחב הקיברנטי ולכן מידע רב נאסף סביב פעולותיהם ברשת.[11]

---

[4] בישראל דבר זה נאמר במספר החלטות ממשלה: החלטה 3611 של הממשלה ה-32 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011) (להלן: החלטה 3611); החלטה 2443 של הממשלה ה-33 "קידום אסדרה בלאומית והובלה ממשלתית בהגנת הסייבר" (15.2.2015) (להלן: החלטה 2443); החלטה 2444 של הממשלה ה-33 "ההיערכות הלאומית להגנת הסייבר" (15.2.2015) (להלן: החלטה 2444). לגבי מקומות אחרים בעולם ראו:
Barack Obama, President of the United States, The White House, Washington, DC: Remarks by the president on securing our nation's cyber infrastructure (May 29, 2009); Advisory: COVID-19 exploited by malicious cyber actors, United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). (8.4.2020); Marios Panagiotis Efthymiopoulos, *A cyber-security framework for development, defense and innovation at NATO,* 8 J. INNOVATION & ENTREPRENEURSHIP 1, 7 (2019); ALP USTUNDAG & EMRE CEVIKCAN, INDUSTRY 4.0: MANAGING THE DIGITAL TRANSFORMATION 268-269 (2018).

[5] "מערך הסייבר הלאומי" **gov.il** (21.02.2022) https://www.gov.il/he/departments/israel_national_cyber_directorate/govil-landing-page.

[6] לפירוט החובות המשפטיים ראו פרק ב של מאמר זה.

[7] בשנים 2016-2021, שיעור הצמיחה השנתי המורכב (CAGR) בשוק הגנת הסייבר העולמי עמד על כ-10.8%. ראו: *Cybersecurity – Worldwide,* STATISTA (Sept. 3 2022), https://www.statista.com/outlook/tmo/cybersecurity/worldwide#cost.

[8] ראו דיון בפרק ב להלן.

[9] כולל תעודת הזהות של העובד, מצבו המשפחתי, מצבו הרפואי, פרטים אודות חשבון הבנק שלו, חסכונותיו השונים, חובות, גובה ההכנסה, ועוד ועוד.

[10] ראו פירוט בפרק א להלן.

[11] מחקרים מראים כי מעל ל-60% מפריצות אבטחת מידע נגרמות (בכוונה או שלא בכוונה) על ידי עובדים. ראו:

איסוף המידע נעשה באמצעות ניטור אחר פעילות שעוברת דרך עמדות קצה (end points), כגון המחשב של העבודה (בין אם מדובר במחשב נייד או במחשב שולחני), דוא"ל, תוכנות שמחברות לרשת וירטואלית פרטית (vpn), ואף בסלולר. כך, הטכנולוגיות (ובעצם המעסיק המשתמש בהן), אוספות באופן קבוע רסיסי מידע מהמקורות השונים, מכינות אותו, כורות מידע (data mining), מעבדות אותו, ומסיקות מסקנות. לאחר מכן, המידע אף עשוי להיות מפוזר לאחרים כמו למשל למערך הסייבר הלאומי, למשטרה ועוד.[12] אנו נראה כיצד בכל אלה יש כדי לפגוע בפרטיות המידע של העובדים. זאת ועוד, המידע נשמר בתוך המערכות, והנו נגיש למעסיק. מעבר לכך, בידי המעסיק הכוח לבחור באיזו דרך הוא משקף לעובדים במקום העבודה את האופן שבו התהליך נעשה ואת הפגיעה הפוטנציאלית בפרטיות. גם בכך, לגישתנו, עשויה להיות פגיעה בזכות לפרטיות.

מעסיקים משתמשים בטכנולוגיות מידע לשלל תכליות, כגון מעקב אחר שעות עבודה והגנה על הקניין הרוחני של המעסיק, והגנת סייבר הנה אחת מהתכליות הלגיטימיות ביותר לניטור אחר ושימוש במידע. לפיכך לדיון על הגנת מידע פרטי של עובדים במקרה של הגנת סייבר ישנם שני יתרונות. היתרון הראשון הוא שהדיון שלנו מראה שגם במקרה שבו יש תכלית לגיטימיות ביותר, ישנם אמצעים משפטיים שניתן לאמץ להגנה על הזכות הבסיסית לפרטיות ולמידע פרטי של העובדים, טובים מאלה שקיימים כיום בדין. היתרון השני הוא שמהמקרה של הגנת סייבר ניתן לגזור הגנות גם למקרים אחרים שבהם ישנה תכלית לגיטימית לשימוש בטכנולוגיות מידע על מנת לספק הגנה טובה יותר לזכויות האמורות. במילים אחרות, כל מה שמוצע להגנה על המידע הפרטי בהקשר של סייבר, הנו רלוונטי לכל תכלית לגיטימית אחרת של המעסיק לשימוש בתוכנות מבוססות דאטה.

במאמר נראה, כי המסגרת המשפטית הקיימת מעניקה היתר רחב במיוחד לביצוע פעולות של הגנת סייבר, אשר כמעט ואינן מרוסנות, ונצביע על ארבע סיבות מרכזיות לכך: האחת היא קיומן של חובות משפטיים המוטלים על ארגונים (במקרה שלנו המעסיק) להגנה על המרחב; השניה היא הפררוגטיבה הרבה שיש למעסיק במסגרת הדין הקיים לבצע כמעט כל פעולה להגנה על מרחב זה; השלישית היא תפיסת ביטחוניזציה חזקה שקיימת בכל הנוגע להגנת סייבר; והרביעית קשורה לכך שהדין הישראלי כיום אינו מטיל אחריות משפטית על חברות הטכנולוגיה לדאגה לזכות לפרטיות המידע של עובדות ועובדים שנאסף ומעובד על ידי טכנולוגיות. גם אנשי המחשוב של המעסיק, החשופים למידע, מתמקדים בתכליות של הטכנולוגיה (כאן הגנת סייבר) ולא בהכרח שוקלים לעומק את הפגיעה בזכות. כתוצאה מכך, שיקולים הנוגעים להגנה על המידע הפרטי בעת פיתוח הטכנולוגיה, השמתה במקום העבודה והשימוש בה, כמעט ואינם נשקלים.

Tasha Tobertson, *Experts: Employees Commit Most Data Breaches,* SHRM (Nov. 22, 2016), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employees-commit-most-data-breaches.aspx; Saket Modi, *How Likely Is Your Employee To Cause A Data Breach?* FORBES (Sep. 13, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/09/13/how-likely-is-your-employee-to-cause-a-data-breach/?sh=63a89e182c63.

[12] ראו את הדילמות כפי שהן תוארו על ידי תהילה שוורץ אלטשולר מהמכון הישראלי לדמוקרטיה: https://www.idi.org.il/articles/23988.

לעומת ההגנה המשמעותית שניתנת להגנת סייבר, אנו חוששות שההגנה שניתנת לזכות לפרטיות המידע של העובדים שנאסף, מעובד ומפוזר בעקבות פעולות הניטור, חיוורת יותר. קושי מרכזי אחד נוגע לאופן שבו עשויות להיות מיושמות הלכות הגנת הפרטיות בעבודה אשר נקבעו בשני פסקי דין מרכזיים בתחום - הלכת איסקוב ענבר[13] והלכת קלנסווה[14] – על המקרה של הגנת סייבר.[15] קושי נוסף נובע מכך שהלכות אלה אינן מספיקות למתן הגנה מיטבית לאור ההיתר הנרחב לפגיעה בזכות למידע פרטי של העובדים במקרה של הגנת סייבר. על מנת להתמודד עם שני הקשיים האמורים, המאמר מציע אופנים שבהם יש לפרש את עקרונות הדין שאומצו בפסיקה בהקשר המסוים של הגנת מידע פרטי בעת פעולה להגנה על הסייבר וכן מציע מספר כלים משפטיים נוספים שניתן לאמץ לדין הקיים.

יצוין, כי אחת הנקודות החשובות שעולות מהדיון האקדמי סביב הזכות להגנה על מידע פרטי, ואף מצויה בלב הדוקטרינה המשפטית, נוגעת להבחנה בין הקשרים שונים של פרטיות (מידע אינטימי, למשל, אל מול מידע שהנו יותר ציבורי, או מידע שנאסף בהקשר של יחסים מסוימים, כגון יחסי עובד-מעסיק).[16] מכאן עלתה לא אחת הטענה שבהקשר של עבודה נדרשת התייחסות מיוחדת לזכות להגנה על מידע פרטי, וזאת לאור מערכת היחסים הייחודית שבין עובד לבין מעסיק הכוללת פערי כוח בין הצדדים, ויחסי כפיפות או תלות.[17] הגנה על מידע פרטי לא נועדה רק להגן על זכויות הפרט (מעבר לפרטיות מדובר בזכות לאוטונומיה ולכבוד),[18] אלא גם על אינטרסים חברתיים וכלכליים רחבים יותר, תוך יצירת מרחבים שיאפשרו לעובדות ולעובדים להעביר מידע פרטי ללא חשש, להתכתב ביניהם, לפתח רעיונות חדשניים, להתאגד ועוד. להגנה על פרטיות המידע בעבודה ישנה חשיבות יתרה, שכן ידיעתם של עובדים שמידע רב נאסף עליהם, מעובד ואף נגיש למעסיק פוגעת בחופש הפעולה שלהם ולה השפעה מרסנת. הפגיעה שעשויה להיות כאשר המידע הפרטי אודות עובדים נאסף, מעובד, נשמר, מפוזר וכן נגיש למעסיק, הנה רבה ואף מעלה קשיים ייחודיים בשל מערכת היחסים המשמעותית, ארוכת הטווח ולעיתים אף הקרובה, בין עובדים לבין מעסיקיהם.[19] היא בעיקר עשויה להיות פוגענית במיוחד נוכח הכוח שיש למעסיק על העובד והאפשרות לפגוע בפרנסתו, בקידומו המקצועי, מימושו האישי ועוד תוך שימוש באותו המידע.

כיום קיים בישראל ואקום חקיקתי בכל הנוגע לזכות לפרטיות בעבודה, שכן אין דבר חקיקה שעוסק בהקשר הייחודי של עבודה ומתווה כללים לגבי הגנה על מידע פרטי או על פרטיות בספירה זו. לכן חשיבותן של ההלכות

---

[13] ע"ע (ארצי) 90/08 **איסקוב ענבר נ' הממונה על חוק עבודת נשים ואח'** (נבו 8.2.2011).

[14] עס"ק (ארצי) 7541-04-14 **הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי נ' עיריית קלנסווה** (נבו 15.3.2017).

[15] ראו דיון על פסקי דין אלו בפרק ד למאמר.

[16] כך, למשל, חוק הגנת הפרטיות, התשמ"א-1981, מייצר הבחנות בין ספירה פרטית לספירה ציבורית בכל הנוגע לפרטיות ואף מעניק הגנה ייחודית לפרטיות בהקשרים מסוימים ולא אחרים.

[17] ראו Otto, לעיל ה"ש 1 ; בירנהק, **מעקב בעבודה**, לעיל ה"ש 1 ; Hendricks, **Privacy 4.0 at Work**, לעיל ה"ש 1 ; Frank Hendricks, *Protection of Workers' Personal Data: General Principles* (ILO, Working Paper No. 62, 2022) ; וכן את עמדת קבוצת העבודה המפורטת בפרק ה למאמר זה.

[18] בארה"ב דגש רב מושם על היות הזכות קשורה לאוטונומיה של הפרט, ובאירופה לכבוד האדם. ראו: מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 37-36 (התשס"ח).

[19] דוגמא להבחנה זו ניתן לראות בפעולות של עובדי אפל. על מנת לקדם התאגדות, עובדי אפל לא השתמשו באייפונים ובאפליקציית המסרים המובנית של אפל, אלא באפליקציות שיחה מוצפנות, שהותקנו על גבי מכשירי אנדרואיד שונים, "כדי למנוע מעקב מצד אפל", ראו: אושרי אלקסלסי "עובדי אפל רוצים להתאגד, אז ברור שהם עושים את זה באנדרואיד" **Geektime** (21.02.2022) https://www.geektime.co.il/apple-employees-trying-to-unionize-using-android-phones/ .

שנקבעו. ואולם, ההצעות שאנו מעלות נשענות על שני אדנים: האחד, כי נדרש לטייב את דיני הגנת הפרטיות בישראל בהקשר של עבודה והשני, כי דיני ההגנה על מידע פרטי בעבודה שפותחו על ידי בתי הדין התבססו יתר על המידה על דיני הגנת פרטיות, תוך התאמתם בצורה מסוימת לעולם של עבודה, ואולם יש להשלימם על ידי כלים נוספים מעולם דיני העבודה.[20] כך למשל, דיני ההגנה על הזכות למידע פרטי מציעים אוסף של עקרונות כלליים, כגון לגיטימיות, מידתיות, צמידות המטרה ושקיפות שנועדו לרסן את הפררוגטיבה של מי שאוסף, מעבד ומפזר את המידע, גם אם בעל המידע נותן הסכמה לאיסוף ועיבוד המידע. ואולם, דיני העבודה בעת הגנתם על זכויות מעניקים הגנה רחבה מזו על ידי יצירת כללים קוגנטיים וכן על ידי מתן כוח בידי העובדים – גם כוח אישי וגם כוח קיבוצי, ואינה נשענת באופן מוחלט על עקרונות כלליים.[21] אם כן, הכלים שאנו מציעות נועדו לחדד את, ולהוסיף על, ההגנות המשפטיות הקיימות בדין על מנת להקנות הגנה משמעותית יותר למידע הפרטי בהקשר של עבודה.

כמובן, ההגנה על הזכות למידע פרטי אינה מוחלטת ויש לאזנה אל מול החובות המשפטיים של המעסיק ואל מול ההגנה החשובה על המרחב הקיברנטי. אנו נצביע על כך שהדין הישראלי מספק קו מחשבה מועיל ליצירת חריגים מההגנה על מידע פרטי – בעיקר דרך החוק להסדרת הביטחון וכן תזכיר חוק הסייבר.[22] זה יהיה סדר טיעוננו:

פרק ב של המאמר יניח את היסודות להבנה הטכנולוגית והמשפטית של הגנת סייבר בישראל כיום, זאת תוך עיון בספרות טכנולוגית, תיאורטית וביקורתית. אנו נדון בהגדרה של הגנת סייבר ובאפיוניה, וכן בטכנולוגיה של הגנת סייבר, המבוססת, בין השאר, על זיהוי אנומליה בתעבורה, ונראה כיצד היא עשויה לפגוע בזכות להגנה על מידע פרטי, תוך שימוש בטקסונומיה שהציע אחד החוקרים הבולטים של פרטיות, דניאל סולוב. **פרק ג** יסקור את המסגרת המשפטית הקיימת בכל הנוגע להגנת סייבר אשר תדון על פי הדינים שחלים על שלושה שחקנים מרכזיים: החברות שמגינות על המרחב הקיברנטי שלהן - במקרה שלנו המעסיקים, חברות פרטיות המפתחות טכנולוגיות להגנת סייבר וכן הרגולטור - מערך הסייבר הלאומי והרשות להגנת הפרטיות. נראה כיצד מסגרת משפטית זו מקנה עליונות להגנה על הסייבר ומאפשרת פררוגטיבה רחבה בידי מעסיקים להשתמש באופן כמעט בלתי מוגבל בטכנולוגיות הגנת סייבר, גם אם הן פוגעות בזכות למידע פרטי. גם נטען, שבתי הדין לעבודה מייחסים להגנת סייבר חשיבות רבה, דבר שעשוי אף להפחית עוד יותר את ריסון הפררוגטיבה המעסיקית. **בפרק ד**, ועל רקע שני הפרקים הקודמים, נבחן את ההגנה המשפטית שניתנת כיום לזכות לפרטיות מידע בהקשר הייחודי של עבודה בדין הישראלי. ננתח את ההלכות המרכזיות שחלות על הזכות למידע פרטי בעידן הטכנולוגי, שהנן, כאמור, הלכת איסקוב ענבר שניתנה על ידי בית הדין הארצי לעבודה בשנת 2011,[23] וכן הלכת קלנסווה משנת 2017.[24] כמו כן נבחן את האופן שבו המבחנים הקיימים בדין הישראלי יתמודדו עם שאלת ההגנה על מידע פרטי בהקשר של הגנת סייבר.

---

[20] לדיון רחב יותר בעניין זה ראו: Einat Albin, *Protecting the Personal Data of the Human Labourer: A Labour Law Paradigm* (draft with author).

[21] שם.

[22] תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018 (להלן: תזכיר חוק הסייבר).

[23] פרשת **איסקוב ענבר**, לעיל ה"ש 13.

[24] פרשת **קלנסווה**, לעיל ה"ש 14.

פרק ה יראה כיצד הדין הקיים נשען ברובו על העקרונות הכלליים שפותחו להגנה על מידע פרטי ונציע לאמץ לוגיקה חזקה יותר של דיני העבודה, כולל שורה של כללים קונקרטיים ועקרונות שאומצו בהקשר של זכויות עבודה אחרות, ביניהם זכויות קוגנטיות להגנה על פרטיות וזכויות קולקטיביות של ארגוני עובדים או נציגות של עובדים. בנוסף נציע אימוץ של הסדרים הקיימים בדין האירופי, ה- GDPR, ובמסמך העקרונות של ארגון העבודה הבינלאומי, ושניתן למצוא אותם גם במקורות השוואתיים נוספים,[25] כגון מחיקת מידע, הזכות להישכח, אחריותיות (accountability) וצמצום המידע, כדי להגדיל את כוחם של העובדים בהגנה על המידע הפרטי שלהם. בהקשר זה יתייחס הפרק גם לנייר הדעה שנכתב על ידי קבוצת העבודה בנושא אבטחת מידע (ה- data protection working party),[26] להסכם המסגרת שנחתם בשנת 2020 בין ארגוני העובדים האירופאים לבין ארגוני המעסיקים בעניין דיגיטציה שחשוב אף הוא בכל הנוגע לסייבר,[27] ולדו"ח שיצא מטעם ארגון העבודה הבינלאומי לגבי הגנה על מידע.[28] בפרק זה גם נראה כיצד ניתן ליישם את הכללים והעקרונות הנוספים שאנו מציעות בהקשר הייחודי של הגנה על מידע פרטי בעת ההגנה על המרחב הקיברנטי. **פרק ו** האחרון יסכם.

ב. הגנת סייבר

"הגנת סייבר" היא "מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות אבטחת מידע".[29] מדובר במונח שכוונתו הרחבה היא הספקת הגנה על המרחב הקיברנטי.[30] הוא מתייחס לכל הכלים, מדיניות, ניהול סיכונים, צעדים שניתן לנקוט בהם, שנועדו להגן על מרחב זה, על הארגון (חברה/מפעל/מקום עבודה) ועל נכסי המשתמשים.[31] הכללת התחום של אבטחת מידע בתוך הגנת הסייבר משקפת את התפתחות תחום הידע בנושא אשר החל מהגנה על הערך של שמירת סודיות המידע והתפתח לכלול הכרה בפוטנציאל נזק רחב יותר, ובו האפשרות לשבש פעילויות דרך תקיפת מחשב וכן הרחבה של מגוון מטרות התקיפה.[32]

בישראל, על פי תקנות אבטחת מידע, על ארגונים (במקרה שלנו "מעסיקים"), כמחזיקים, בעלים או מנהלים של מאגרי מידע, מוטלות חובות שונות להגן על פרטיות נושאי המידע שעלולים להיפגע מחשיפתו, לפי רמת האבטחה החלה על מאגרי המידע שברשותם (רמת אבטחה בסיסית, בינונית או גבוהה). חובות אלו כוללות, בין היתר, חובה לנהל באופן מאובטח ומעודכן את מאגרי המידע שלהם,[33] חובה למנות ממונה על אבטחת מידע,[34] קביעה במסמך

---

[25] סיכום טוב של מגוון המקורות בהם ניתן למצוא את העקרונות הרלוונטיים נמצא בדו"ח של **ILO:** Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17.

[26] Working Party, Opinion 2/2017 on data processing at work (17/EN WP 249) (June 8, 2017).

[27] ETUC, BUSINESSEUROPE, CEEP & SMEunited, *European Social Partners Framework Agreement on Digitalization* (June 2020).

[28] Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17.

[29] ס' 1 לתזכיר חוק הסייבר, לעיל ה"ש 22.

[30] המונח "מרחב קיברנטי" הוא מרחב מטאפורי של מערכות מחשב ורשתות מחשב והוא המונח העברי ל-cyberspace.

[31] *Definition of cybersecurity*, THE INTERNATIONAL TELECOMMUNICATIONS UNION (last visited Aug. 25, 2022) https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[32] תזכיר חוק הסייבר, לעיל ה"ש 22, בעמ' 3-4. Rossouw von Solms & Johan van Niekerk, *From Information Security to Cyber Security*, 38 Comput & Sec. 97 (2013).

[33] תקנה 13 לתקנות אבטחת מידע.

[34] שם, בתקנה 3.

נוהל אבטחת מידע וקביעת הרשאות גישה למידע בהתאם למידה הנדרשת לביצוע התפקיד בלבד.[35] כמו כן, תקנות אבטחת מידע כוללות הוראות מפורטות ביחס לניהול כוח אדם, הקובעות, כי בהליכי מיון עובדים ושיבוצם לא תינתן הרשאה למידע, אלא אם בעל המאגר (המעסיק לענייננו) נקט אמצעים סבירים המקובלים בהליכים אלו לבירור שבעל ההרשאה מתאים לקבלת גישה למידע המצוי במאגר.[36] עם זאת, ניתן לראות כי במקרים מסוימים, תקנות אלו מטילות סטנדרט נמוך יותר של אבטחת מידע (רמת אבטחה בסיסית) כאשר המידע הוא אודות המועסקים או הספקים של בעל מאגר המידע והוא משמש לניהול העסק בלבד.[37]

מעבר להגנה על מידע, הגנת סייבר נעשית למטרות נוספות. למשל, הגנה מפני הטרדה ברשת,[38] הגנה על אינטרסים עסקיים ועל קניין רוחני, כמו במקרה של הפצה לא חוקית של סרטים ברשת או של יצירות אחרות,[39] הגנה על תשתיות שמספקות מים, חשמל ושאחראיות על המרחב האווירי, הגנה מפני סכנות סביבתיות, סכנות ביטחוניות ואף הגנות על האדם עצמו. תכלית מרכזית נוספת של הגנת סייבר היא הגנה על מערכות ממוחשבות. כך גם קבע המחוקק הישראלי כאשר הסדיר רגולציה ייחודית להגנה על תשתיות חיוניות, אשר פגיעה בהן עלולה לגרום נזקים נכבדים ונרחבים למדינת ישראל במסגרת החוק להסדרת הביטחון. חוק זה מבדיל בין פעולות לאבטחת מידע לבין פעולות לאבטחת מערכות ממוחשבות חיוניות, לרבות המידע האגור בהן, תוך קביעה אילו גופים (פרטיים וציבוריים) נופלים תחת כל קטגוריה וכפופים להסדרה בחוק.[40] הוא נועד להגן על מערכות ממוחשבות בכל הנוגע להגנת סייבר של תשתיות חיוניות והגנה על המשכיות תפקודית של מערכות חשובות אלו.[41] באופן הזה, הגנת סייבר נותנת מענה להגנה על אינטרסים רחבים,[42] וסטנדרטים חדשים נכנסים לתמונה כדי לוודא שהגנת הסייבר נעשית בצורה מיטבית.

האיום על המרחב הקיברנטי כמובן שאינו המשגתי בלבד. מדי שנה מיליוני אנשים נופלים קורבן לפשעי סייבר,[43] והאיומים על הביטחון הם אמיתיים. אלה מגיעים מיחידים, ארגונים ואף ממדינות.[44] הסוגים השונים של תקיפות סייבר כוללים, בין היתר, השתלטות על מערכות מחשוב במטרה להסב נזק, גניבה של מידע ומתקפת כופר

---

[35] שם, בתקנה 8.
[36] שם, בתקנה 7.
[37] שם, בס' 2(1) לתוספת הראשונה.
[38] אחת התופעות המשמעותיות שמתמודדים איתה היום ברשת היא מה שמכונה cyber bullying. על זה ראו: Nigel Martin & John Rice, *Cybercrime: Understanding and Addressing the Concerns of Stakeholders*, 30 COMPUT. & SEC. 813 (2011).
[39] Von Solms & Van Niekerk, לעיל ה"ש 32, בעמ' 100.
[40] סעיף 1 לחוק להסדרת הביטחון.
[41] אלדד הבר וטל זיו־רסקי "דרכי ההגנה על תשתיות חיוניות במרחב הסייבר בישראל" **משפט וממשל** יח (תשע"ז).
[42] שם.
[43] מטבע הדברים, קיים קושי לאמוד את היקף תקיפות הסייבר, מפני שחלק ניכר אינו מדווח. על-פי דוח מבקר המדינה בעניין התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת, בשנת 2015 נפגעו בישראל כ-230,000 בני אדם מפשיעת סייבר, ראו: מבקר המדינה **התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת** (2017); מסקר של הלשכה המרכזית לסטטיסטיקה ומערך הסייבר הלאומי, עולה כי אחד מכל חמישה עסקים בישראל חווה תקיפת סייבר, ראו: מערך הסייבר הלאומי "סקר הגנת סייבר" **סייבר ישראל – מערך הסייבר הלאומי** (20.7.2021) https://www.gov.il/he/departments/news/cyberweeknews. לנתונים נוספים, ראו: Chuck Brooks, *Alarming Cybersecurity Stats: What You Need To Know For 2021*, FORBES (Mar. 2, 2021), https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=3a4945e258d3.
[44] כך לדוגמא, נושא זה עלה לאחרונה לכותרת לאור דיווחים על מלחמת סייבר כחזית נוספת במלחמה בין רוסיה לאוקראינה. ראו: טל מימרן "המלחמה בין רוסיה לאוקראינה מוכיחה: חזית הסייבר היא שובר השוויון החדש" **גלובס** (24.2.2022). https://www.globes.co.il/news/article.aspx?did=1001403486; יוסי הטוני "רוסיה תקפה בסייבר – שוב – את רשת החשמל באוקראינה" **אנשים ומחשבים** (14.4.2022), https://www.pc.co.il/news/361176/; בישראל, לאחרונה קבוצה פרו איראנית השביתה את אתר רשות שדות התעופה ליותר מחצי שעה במתקפת סייבר. ראו: אסף גלעד "אתר רשות שדות התעופה הושבת במתקפת סייבר" **גלובס** (20.4.2022) https://www.globes.co.il/news/article.aspx?did=1001409814.

(ransomware).[45] אחת הדרכים הנפוצות ביותר לבצע התקפת סייבר נעשית על ידי הנדוס חברתי (social engineering), תוך הפעלת טריקים ומניפולציות, אשר פעמים רבות נעשות כלפי עובדים, ובנייה על האמון שלהם, על מנת שאלה יחדרו למרחב הקיברנטי של המעסיק.[46] כמו כן יש שימוש נרחב בסחיטת סייבר (cyber extortion). הפגיעה במרחב הסייבר אף התרחבה בשנים האחרונות בעת מגפת הקורונה.[47]

בוחסק וגובן , שני חוקרים אמריקאים מובילים בתחום של הגנת סייבר, חידדו כי בכל המערכות להגנת סייבר יש לפחות תוכנת אנטי וירוס ומערכת זיהוי התפרצות.[48] מערכות זיהוי ההתפרצות עוזרות לגלות, לקבוע ולזהות שימוש לא מאושר, העתקה, שינוי והשמדה של מערכות מידע, כאשר הפגיעה בהגנה יכולה להגיע מחוץ לארגון ומתוכו.[49] הן עושות זאת דרך ניתוח של מידע, כאשר ניתוח המידע כולל מספר שלבים: איסוף המידע (data collection), הכנת המידע, כריית המידע (data mining), ואחר כך ניתוח המידע והסקת מסקנות.[50] זיהוי אנומליה בתעבורת המידע ברשת נעשית במגוון של מתודות אשר אוספות את המידע ממקורות רבים.[51] כך, למשל, מדפי מידע של מספר חברות המפתחות ומוכרות תוכנות להגנת סייבר (להלן: חברות הסייבר),[52] מודגשת פעילותן ככזו שעוקבת אחר אימיילים, קול, צ'טים, רשתות, גישה פיסית של עובדים למקומות, זהויות, איסוף מידע מכוח אדם ועוד.[53] בתוכנות להגנת סייבר ישנם שלושה סוגים עיקריים של אופנים שבהם המידע מנותח. הראשון מאתר פגיעות ידועות מראש וזאת על ידי יצירת חותמת של אותה פגיעה, תוך עדכון תדיר שלה על פי מדריך מסוים. השני הוא על ידי זיהוי אנומליה, דהיינו זיהוי התנהגות חריגה ברשת, והשלישי מערב את שני האופנים האמורים.[54]

השלבים השונים של ניתוח המידע והאופן בו הם מבוצעים עשויים לעלות כדי פגיעה בפרטיות. על מנת לחדד את הפגיעה בזכות למידע פרטי של העובדים נשתמש בטקסונומיה שהציע דניאל סולוב, אחד החוקרים הבולטים בתחום, שנועדה להראות מדוע בעיות הנוגעות לפרטיות הנן פוגעניות וגורמות לנזק.[55] לצורך כך, התמקד סולוב *בסוגים שונים של פעולות* שיוצרות כשלעצמן פגיעות בפרטיות, עם התמקדות מיוחדת במידע פרטי. הטקסונומיה שהוא מציע נועדה לאפשר לקובעי מדיניות ולבתי משפט לאזן בצורה טובה יותר בין פרטיות לבין אינטרסים

---

[45] נוזקת כופר (ransomware) היא תוכנה זדונית המתוכננת למנוע ממשתמש גישה למערכות מחשב או לקבצי מידע ומשמשת לסחוט מהמשתמש כסף על מנת שתוסר המגבלה. ראו: מערך הסייבר הלאומי "התמודדות עם נוזקה מסוג כופרה-Ransomware" **סייבר ישראל – מערך הסייבר הלאומי** (7.8.2019) https://www.gov.il/he/departments/publications/reports/ransomware ; ראו למשל דוגמאות לפשעי סייבר מרכזיים כלפי כלי רכב חכמים: חיים ויסמונסקי, מאי הר-שי, "התמודדות משפטית עם איומי סייבר לכלי רכב "חכמים"", **חוקים** יג (197), 207-214 (2020).

[46] על הנדוס חברתי והגנת סייבר ראו: FILIPE BREDA, HUGO BARBOSA & TELMO S. MORIAS, SOCIAL ENGINEERING AND CYBER SECURITY (2017).

[47] בשנת 2020 נרשם מספר שיא של תקיפות סייבר על חברות, ממשלות ויחידים. ראו: Brooks, לעיל ה"ש 43.

[48] Anna L. Buczak & Erhan Guven, *A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection* 18(2) IEEE COMMC'TS SURV. & TUTORIALS 1153 (2016).

[49] שם.

[50] שם ; Bodie et al., לעיל ה"ש 1, בעמ' 8-9 ;
Jeremias Adams-Prassl *What if Your Boss was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work* 41(1) COMP. LAB. L. & POL'Y. *J.* 123 (2019).

[51] Buczak & Guven, לעיל ה"ש 48 ;
Abdun N. Mahmood & Jiankun Hu, *A Survey of Network Anomaly Detection Techniques* 60 J. OF Ahmed Mohiuddin, NETWORK AND COMPUT. APPL. 19 (2016).

[52] בחנו את דפי המידע של החברות הבאות: Forcepoint, CyberArk, Imperva, FireEye, Symantec.

[53] *Forcepoint Behavioural Analytics Overview*, FORCEPOINT (Feb. 22, 2022), https://www.forcepoint.com/sites/default/files/resources/files/ueba-regulatory-surveillance.pdf.

[54] Buczak & Guven, לעיל ה"ש 48.

[55] Daniel Solove, *A Taxonomy of Privacy*, 154(3) PENN. L. REV. 477 (2006), 480.

מתנגשים.[56] סולוב מכיר בכך שאי אפשר לבחון פרטיות בניתוק מההקשר החברתי, אשר טעון בקונפליקטים וחיכוכים. פרטיות, לגישתו, איננה סוג של חופש מחיכוכים חברתיים, אלא היא מגנה מפני שורה של פעולות קשורות שמשפיעות על אנשים בצורה שלילית.[57] עוד מדגיש סולוב, כי גם אם פעולה הנה פוגענית או בעייתית, אין זה אומר שהמשפט צריך לתת לה מענה, מכיוון שיכולות להיות סיבות טובות להימנע מלעשות זאת.[58] לכן המטרה שלו איננה לומר מתי המשפט צריך להתערב ומתי לא, שכן מענה לשאלה זו צריך להינתן בכל הקשר ספציפי ונפרד, אלא היא נועדה להגדיר את אותן הפעולות שעולות כדי פגיעה בפרטיות והנזק שנגרם. נזק זה יכול לנוע מפגיעה בגוף אבל הוא כולל גם פגיעה ברגשות, פגיעה בכבוד, ואפשרות לפגיעה עתידית בפרט.[59] סולוב מציע ארבע קבוצות של פעולות פוגעניות ואנחנו נתעכב על שלוש מתוכן שהן הרלוונטיות ביותר להקשר של מאמר זה: 1. איסוף המידע (שכולל את השלבים של איסוף המידע, הכנת המידע ומציאת המידע לפי בוחזק וגובן), 2. עיבוד המידע (הכולל ניתוח המידע והסקת מסקנות לפי בוחזק וגובן) ו-3. פיזור המידע.[60]

<u>איסוף המידע</u>: לפי סולוב איסוף מידע לכשעצמו עולה כדי פגיעה ונזק בפרט גם אם מידע זה לא נחשף לציבור. בדיון שלו עוסק סולוב בשני סוגים של איסוף מידע – מעקב וחקירה[61] – שהנם דומים לסוג הפעולות שמבצעות טכנולוגיות לאבטחת סייבר. לפי סולוב, לניטור מידע באופן רציף יש השפעות בעייתיות, שיכולות ליצור תחושות חרדה או אי נעימות, ואף עשוי לגרום לאנשים לשנות את התנהגותם, כולל צינזור עצמי או זהירות יתר הנובעים מכך שהמידע נאסף באופן קבוע.[62] הכוח החברתי של פיקוח מקובל בדיני עבודה,[63] ולכן השאלה היא שאלה של מידה על מנת למנוע את התופעות השליליות של פיקוח, כגון פגיעה ביוזמה, יצירה, ועוד.[64] סולוב מציין שגם ניטור שהפרט אינו מודע לו עשוי לעלות כדי פגיעה, לאור אפקט הצינון לו הוא גורם,[65] וכאשר מדובר בניטור שכולל מידע פרטי או שנעשה במרחב הפרטי, כגון על מחשבים בבית, המורכבות הנה גדולה יותר, לא רק מבחינת הפרט אלא גם מבחינה משפטית. זאת הואיל והמשפט עושה הבחנה בין מידע פרטי ומרחבים פרטיים לבין מרחבים ציבוריים ומידע עסקי.[66] אמנם טכנולוגיות להגנת סייבר לא נועדו לעקוב אחרי העובדים, ואולם עצם איסוף המידע באופן קבוע עשוי לגרום לאותו האפקט, בעיקר לאור כך שמידע זה נגיש למעסיק. בהקשר של סייבר יש גם היבט של חקירה של המידע, ולא רק של מעקב אחר העובדים,[67] שכן התוכנות מבקשות לאתר ולזהות אפשרות לתקיפות סייבר ולכן חוקרות את המידע לצורך מטרה זו, דבר שאף הוא פוגע בפרטיות.

---

[56] שם, בעמ' 483-481.
[57] שם, בעמ' 484.
[58] שם.
[59] שם, בעמ' 486.
[60] הפעולה הרביעית שמציין סולוב מתויגת על ידו כפלישה ("invasion") וכוללת הפרעה והתערבות בהחלטות, ראו: שם, בעמ' 549.
[61] שם, בעמ' 504-491.
[62] שם, בעמ' 494-493.
[63] בירנהק, מעקב בעבודה, לעיל ה"ש **שגיאה! מקור ההפניה לא נמצא.**.
[64] Solove, לעיל ה"ש 55, בעמ' 494.
[65] שם, בעמ' 495.
[66] ראו דיון נרחב יותר בשאלת פרטיות המידע בפרק ד להלן.
[67] על הפגיעות במקרה של חקירה ראו Solove, לעיל ה"ש 55, בעמ' 504-499.

כפי שציינו לעיל, ההגנה על המרחב הקיברנטי כוללת איסוף מידע ממקורות רבים כגון תכתובות דוא״ל, צ׳טים, הקלטות וידאו ואודיו, מהרשת, ועוד, וזאת מבלי שבהכרח מבוצעת הבחנה בין מידע עסקי לפרטי. מעבר לכך, גם מידע עסקי עשוי להיות מוגדר כמידע פרטי.[68] חיפוש האנומליה ברשת נעשה על מה שמכונה נקודות קצה, הכוללות את מחשבו האישי של העובד, כולל מחשב נייד ונייח. כלי ניטור רץ על המחשב ובודק את התעבורה, בין השאר באתרים שהעובד נכנס אליהם. אלה עשויים לכלול את אתר חשבון הבנק של העובד, רשתות חברתיות, אתר קופת החולים ועוד. מעבר למחשב, נעשית בדיקה על טכנולוגיות שמחברות לרשת וירטואלית פרטית (vpn). הכוונה למצבים שבהם טכנולוגיה יוצרת חיבור מוצפן בשביל לגלוש ברשתות אחרות, למשל, חיבור בין המחשב הביתי לבין הרשת של מקום העבודה לצורך כניסה למאגרי המידע. טכנולוגיה זו נקראת man in the middle, או במקרה של עבודה the employer in the middle. ברגע שהעובד משתמש בטכנולוגיה האמורה, המעסיק יכול לדעת כל מה שהוא עושה ברשת, שכן הטכנולוגיות דורשות סרטיפיקט של העובד על מנת לוודא הרשאת כניסה לרשת הוירטואלית הפרטית. גם המידע שעובר דרך הדוא״ל של העובד נאסף באופן תדיר, ומעבר לכל זאת, כיום ישנה הרחבה של שימוש בטכנולוגיות הגנת הסייבר גם לסלולר. יצוין, כי לעיתים, מותקנת בטלפון הנייד תוכנה שמחלקת את הטלפון לשני אזורים – חצי פרטי וחצי של העבודה. החצי הפרטי אינו מנוטר. תוכנות שכאלה, כמו למשל התוכנות cytrix או mobile iron, מסייעות בהגנה על החצי הפרטי של העובדים.

מעבר לכך, טכנולוגיות הגנת הסייבר עצמן משתמשות בכלים נוספים להגנה, שאף הם מבוססים על איסוף מידע פרטי ועשויים לפגוע בפרטיות. למשל, על מנת להגן על הארגון התוכנה מבקשת אמצעי זיהוי של משתמשים. אמצעים מוכרים הנם וידוא כפול ומשולש על ידי כניסה עם סיסמא ואח״כ דרישה לסיסמא נוספת שמאומתת דרך הטלפון ; אמצעי זיהוי ביומטריים, שכוללים טביעות אצבעות ואמצעים לזיהוי פנים, על אף שאלה נתונים במחלוקת משפטית וציבורית בישראל ;[69] קוד שעובר על האימיילים ומחפש זיהוי של מי ששלח אותו, ועוד. בנוסף, טכנולוגיות להגנת סייבר מציגות לעיתים רבות את האפשרות של ניטור לפי תוכן - רשימת מילים שהשימוש בהן נתפס כבעייתי והלקוח (המעסיק) בורר מתוכן מילים שנראות לו מתאימות. כך, למשל, לא מוגבל חיפוש לפי מילים שעשויות לפגוע בפרטיות או בזכויות אחרות של עובדות ועובדים – הריון, התארגנות עובדים, ועד, מחלה מסוימת ועוד.

מכל האמור לעיל עולה שטכנולוגיות הגנת הסייבר אוספת מידע רב, פרטי ועסקי, ממקורות מידע שונים ועל גבי אמצעים טכנולוגיים מגוונים, וכפי שפירט סולוב, עצם האיסוף עצמו מעלה חששות כבדים לפגיעה בפרטיות. נוסיף על סולוב ונציין, כי הפגיעה בפרטיות אף עשויה להיות גדולה יותר במערכות יחסים לא סימטריות, כגון יחסי עבודה, שבהן העובד לא אוטונומי להחליט את החלטותיו על המידע, אלא נמצא ביחסי כפיפות למעסיק. יחסי כפיפות אלה מקנים למעסיק פררוגטיבה על ניהול הליך איסוף המידע, הטכנולוגיות בהן הוא משתמש, על יישום הכללים המשפטיים הנוגעים למגבלות על איסוף המידע, וכן על האופן שבו האיסוף מוצג לעובד.[70]

---

[68] ראו דיון נרחב יותר בשאלת פרטיות המידע בפרק ד להלן.
[69] ראו למשל את הדיון בפרשת **קלנסווה**, לעיל ה״ש 14.
[70] Hendricks, **Privacy 4.0 at Work**, לעיל ה״ש 1 ; De Stefano , לעיל ה״ש 1 ; Bodie et al., לעיל ה״ש 1.

<u>עיבוד המידע</u>: הליך עיבוד המידע מתייחס לשימוש במידע, איחסונו וביצוע מניפולציות לגביו, לאחר שזה נאסף.[71] תהליך עיבוד המידע מתייחס לשלב שלאחר איסופו ונוגע לדרכים השונות שבהן מידע מחובר יחד, מוביל להסקת מסקנות ומחבר אותם לאנשים מסוימים שלהם שייך המידע. אגרגציה, תהליך שבו פיסות מידע רבות נאספות יחד ויוצרות תמונה של האדם, היא אחת הפגיעות המשמעותיות בפרטיות. זאת הואיל והיא מייצרת פרופיל שלם של האדם והשלם נהיה גדול יותר מסך חלקיו, שכן המידע שנאסף יחד מאפשר גילוי פרטים חדשים שפיסת מידע כזו או אחרת אינה מעלה. [72] מידע זה מגיע לממדים חדשים בעידן הטכנולוגי הנוכחי בו המידע שנאסף על אנשים רחב בהרבה מבעבר והיכולות הטכנולוגיות לנתח אותו במהירות על פי קוד עלתה בעשרות מונים ומקנה כוח רב בידי אלה שהמידע המצרפי נמצא בידם.

בהקשר של טכנולוגיות הגנת הסייבר, אלה, כאמור, לרוב מבקשות להתחקות אחר מה שקורה ברשת על מנת לאתר התנהגות אנושית שהיא אנומלית במרחב הקיברנטי. הטכנולוגיות בנויות כך שהן מגדירות התנהגויות מסוימות כבעייתיות, ועל ידי ניטור פעולות ברשת מבצעות ניתוח התנהגותי תוך שימוש בצירופי מידע ומגיעות למסקנות לגבי התנהגות חריגה. ישנן מספר מתודות טכנולוגיות לביצוע קורלציה בין המידע שנאסף לבין עיבודו והתחזיות שהטכנולוגיה מגיעה אליהן.[73] לצורך כך הטכנולוגיה צריכה להגדיר לעצמה מהי התנהגות נורמאלית, ובעקבות זאת לזהות חריגות.[74] כך יתכן שאם, למשל, עובדת נוהגת לעבוד בכל יום בשעות מסוימות ובאחד מהימים עובדת בשעות חריגות, המערכת תזהה התנהגות זו כחריגה. אם קצב ההקלדה של העובדת משתנה אזי, גם אז, המערכת תזהה זאת כהתנהגות חריגה. גם ההגדרה של מה חריג או לא עשוי להוביל לפגיעה בפרטיות, שכן, למשל, הקלדה חריגה עשויה להעיד על בעיה בריאותית כלשהי. בהקשר זה יצוין, שעל פי מחקרים, מידת הדיוק של המתודות האמורות לעיתים אינה גבוהה.[75]

חשש נוסף בתהליך עיבוד המידע נוגע לשימוש למטרה שניונית, או במילים אחרות שימוש למטרה אחרת מהמטרה שלשמה נאסף מידע זה. שימוש כזה הנו בעייתי מאד שכן הוא שולל מהאדם את השליטה במידע שהוא כן הסכים למסור למטרה מסוימת, ויתכן ואם היה יודע כי המידע ישמש למטרה אחרת לא היה מסכים למסור אותו. עובדות המקרה בהלכת איסקוב ענבר הנם דוגמא מובהקת לכך שמידע שנאסף מתכתובות דוא"ל לצורך הגנה או שמירה של מאגרי מידע ונשמר אצל המעסיק, שימש אחר כך את המעסיק למטרה אחרת.[76]

<u>פיזור המידע</u>: החששות לפגיעה בפרטיות בהקשר של פיזור המידע נוגעות להעברת המסקנות לידיים שלישיות.[77] במקרה של הבטחת סייבר פעמים רבות המידע עצמו, עיבודו והמסקנות שהוסקו חשופים אך ורק בפני מנהל מערכות המידע בארגון (המנמ"ר). ואולם ברגע שישנו חשש לפגיעה פוטנציאלית במרחב הקיברנטי מידע זה יועבר

---

[71] Solove, לעיל ה"ש 55, בעמ' 504-523.
[72] שם, בעמ' 506.
[73] Buczak & Guven , לעיל ה"ש 48.
[74] לגבי האופן שבו הטכנולוגיה מגדירה התנהגות כ"נורמאלית" ראו: שם.
[75] שם, פרק 4.
[76] פרשת **איסקוב ענבר**, לעיל ה"ש 13. פסק דין איסקוב ענבר עסק בשאלת כשירותן הראייתית של תכתובת שנלקחו מתיבת דוא"ל שסופקה במקום העבודה, ראו הרחבה בפרק ד להלן.
[77] Solove, לעיל ה"ש 55.

לצדדים שלישיים בתוך הארגון. בנוסף, מידע עשוי לעבור גם לידיים של רשויות מחוץ לארגון, כמו למשל למערך הסייבר הלאומי. דבר זה בעייתי, שכן גם אם עובד נתן את הסכמתו לאיסוף מידע לצורך הגנת סייבר, אזי הוא לא בהכרח נתן את ההסכמה כי המידע יעבור לצד שלישי.

כפי שציינו לעיל, עצם הפגיעה בפרטיות המידע אינה בהכרח מובילה למסקנה שיש לנקוט בצעדים משפטיים למנוע אותה, שכן יתכנו אינטרסים כבדי משקל לפגיעה האמורה. ואולם, אנו סבורות כי בהקשר של הגנת סייבר – למרות התכלית החשובה של הגנה זו – המדובר בפגיעה בלתי מידתית וכי ניתן להשיג את ההגנה על הסייבר תוך מתן הגנה מיטבית יותר למידע הפרטי של העובדים. את הטענה הזו נבסס לאחר שנראה, כי המסגרת המשפטית הקיימת כיום מעניקה משקל רב להגנת הסייבר אשר מאיינת חשיבה מספקת על ההגנה על המידע הפרטי של העובדים.

ג. המסגרת המשפטית הקיימת

חוקרים שעסקו בזכות לפרטיות בעבודה הראו את המתח בין הפררוגטיבה המעסיקית לבין הזכות לפרטיות, בפרט בהקשר של טכנולוגיות חדשות ואת הכוח המועצם של המעסיק בהקשר זה. הנדריקס ציין, שהואיל ויחסי עבודה הם יחסים שמאופיינים בכפיפות אינהרנטית או תלות של העובד למעסיק, אזי החופש של העובד מוגבל בכך שהמעסיק רשאי לנהל ולכוון את העבודה וכן לקבוע את התנהגותו של העובד, לאסוף מידע ולשלוט ולמשמע אותו.[78] כך, בעוד הזכות לפרטיות מבוססת על הרעיון של הזכות להיעזב במנוחה,[79] יחסי העבודה מאפשרים למעסיק שלא להניח לעובדיו למנוחה.[80] דה סטפנו הראה כיצד הפררוגטיבה הניהולית של המעסיק מועצמת, דרך חוזה העבודה, בהקשר של טכנולוגיות חדשות, דבר אשר מגדיל את האוטוריטה של המעסיק אל מול העובד.[81] רוג׳רס הדגים כיצד דיני העבודה מקנים זכויות נרחבות למעסיקים להטמיע טכנולוגיות חדשות במקום העבודה ולאסוף מידע על עובדים, ואף טען, כי דינים אלה מנתבים פיתוח של טכנולוגיות המפעילות כוח על עובדים.[82] רכבי הדגיש דברים דומים.[83]

בפרק זה נראה כיצד הדין הישראלי הנוגע להגנת סייבר מאשש את אמירותיהם של הכותבים האמורים. המסגרת המשפטית הקיימת מעניקה משקל רב להגנה על המרחב הקיברנטי ואף מקנה למעסיק פררוגטיבה ניהולית רבת עוצמה לצורך מטרה זו. אכן, ההגנה על הסייבר מאפשרת למעסיק שלא להניח לעובדיו במנוחה, היא מגדילה את האוטוריטה הניהולית שלו מולם על ידי הקניית כוח דרך חוזה העבודה לנהל את העסק, כולל את המרחב

---

[78] Hendricks, **Protection of Workers' Personal Data**, לעיל ה״ש 17, בעמ׳ 8; Hendricks , **Privacy 4.0 at Work**, לעיל ה״ש 1 .

[79] כך הגדירו את הזכות וורן וברנדייס במאמרם המפורסם:
Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Har. L. Rev. 193 (1890). זאת למרות, שכיום הגישה השלטת לגבי הזכות לפרטיות הנה פרטיות כשליטה – ראו עוד בפרק ה להלן.

[80] Hendricks, **Privacy 4.0 at Work**, לעיל ה״ש 1.

[81] De Stefano, לעיל ה״ש 1.

[82] Brishen Rogers, *Beyond Automation: The law & Political Economy of Workplace Technological Changes*, (Roosevelt Institute, Working Paper, 2019); Brishen Rogers (2019) *The Law and Political Economy of Workplace Technological Change* 55 Harv. CRCL Law Review 531.

[83] Gali Racabi, *Abolish the Employer Prerogative, Unleash Work Law*, 43 BERKLEY J. EMP & LAB. L.79 (2022).

הקיברנטי, ולבסוף המסגרת המשפטית הקיימת נוטה להקנות זכויות נרחבות למעסיקים להטמיע טכנולוגיות הגנת סייבר כרצונם שמפעילות כוח על העובדים. נראה את הדברים בשני אופנים. הראשון, על ידי תיאור המסגרת המשפטית שחלה כיום על שלושת השחקנים הראשיים שמעצבים את הדין לגבי האופן בו עובדות תוכנות הסייבר בישראל: הארגון (המעסיק), חברות הטכנולוגיה המפתחות את טכנולוגיות הגנת הסייבר, והרגולטור - מערך הסייבר הלאומי והרשות להגנת הפרטיות. השני, על ידי חידוד הטיעון כי לאור החובות המשפטיות שחלות על מעסיקים, התפיסה של הגנת סייבר דומה לערך של ביטחון לאומי, דבר המגביר עוד יותר את המשקל שניתן להגנת סייבר.

1. המסגרת המשפטית להגנת סייבר

א. הארגון (<u>המעסיקים</u>):

כפי שצוין בפרק הקודם, למעסיקים עצמם ישנה מחויבות על פי דין להגן על מאגרי המידע שלהם וכן על תקינות מערכות המחשוב ולנקוט במכלול פעולות להשגת מטרה זו. מחויבות זו מעוגנת הן בתקנות אבטחת המידע והן בחוק להסדרת הביטחון. מעבר לכך, מעסיקים, גם פרטיים וגם ציבוריים עליהם לא חלות כל החובות הקבועות בחוק להסדרת הביטחון, מבקשים לעשות כל שביכולתם על מנת להגן על תקינות מערכות המחשוב כדי לספק שירות רציף ויעיל ללקוחותיהם, וכן למנוע מפגעים חברתיים, ביטחוניים וסביבתיים. במקרים מסוימים, אי נקיטת אמצעים למניעת מתקפות סייבר שיפגעו במערכות עשוי להיחשב כהפרת חובות של החברה והדירקטוריון שלה כלפי הנפגעים ועולה כדי עוולה נזיקית. כך למשל, בעמדה משפטית שפרסמה רשות ניירות ערך, נאמר שבמקרים מסוימים חלים על תאגיד חובות דיווח בקשר עם סיכוני סייבר, הכוללים את הסברי הדירקטוריון ביחס לסיכונים אלו או התממשותם.[84] גם גרוס ציין, כי מתוקף תפקידו הפיקוחי, הדירקטוריון אחראי על ניהול הסיכונים של החברה, וכי גם החברה וגם נושאי המשרה בה צפויים לתביעות משפטיות וקנסות במקרה של נזק סייבר.[85] לאחרונה פורסם הסדר פשרה בתביעה ייצוגית כנגד חברת הביטוח שירביט, בעקבות אירוע אבטחת מידע במהלכו הצליחו קבוצת ההאקרים Black Shadow לגנוב מידע רב ופרטים אישיים של לקוחות ומבוטחים. במסגרת ההסדר, נקבע כי שירביט תפצה את הקבוצה המיוצגת בכ-5 מיליון ש"ח.[86] עוד בעניין שירביט, רשות שוק ההון קבעה כי בשנים 2018-2020, רמת ניהול סיכוני הסייבר שנעשתה בשירביט לא עלתה בקנה אחד עם רמה ההולמת גוף מוסדי והטילה על החברה עיצום כספי בסך 10.7 מיליון ש"ח.[87] בנוסף, ישנו פיקוח רגולטורי על חברות הפועלות בענפים מסוימים, כגון בסקטור הפיננסי.[88]

---

[84] **עמדה משפטית מספר 105-33: גילוי בנושא סייבר** (עמדה משפטית, רשות ניירות ערך 2018), https://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D%20%D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/Staf_Positions/SLB_Decision/Reports/Documents/SLB_105-33_cyber.pdf

[85] יוסף גרוס **דירקטורים ונושאי משרה בעידן הממשל התאגידי** 212 (מהדורה חמישית 2018).

[86] ת"צ (מחוזי מרכז) 6615-12-20 **שור נ' שירביט חברה לביטוח בע"מ** (נבו 3.10.2023).

[87] "רשות שוק ההון, ביטוח וחיסכון הטילה עיצום כספי בסך של 10,720,000 ש"ח על שירביט חברה לביטוח בע"מ" **gov.il** (30.11.2021) https://www.gov.il/he/departments/news/press_0009.

[88] במספר תחומים כגון מידע רפואי ונתוני אשראי. ראו למשל: חוק נתוני אשראי, התשע"ו-2016; חוזר מנכ"ל משרד הבריאות 2019/09 "אמות מידה לניהול רשומות מטופל במערכת הבריאות" (15.12.2019).

לרוב, למעסיקים אין ידע ייחודי בעניין הגנת סייבר כך שהם סומכים על אנשי מקצוע – בין אם של חברות הסייבר ובין אם על עובדים שלהם המתמחים בהגנת סייבר (לרוב המדובר במנמ"ר או Chief Information Security Officer - CISO). השיקולים של חברות הסייבר ושל אנשי המקצוע בתוך הארגון הנם של מתן הגנה מקסימאלית למרחב הקיברנטי. אמנם המעסיק מחויב להגן על המידע הפרטי במערכות, ולכן הגנה על המרחב הקיברנטי תראה גם על ידי בתי הדין כתכלית לגיטימית.[89] ואולם ההסתמכות הבלעדית על אנשי המקצוע וחברות הטכנולוגיה הנה בעייתית נוכח העובדה שלחברות הסייבר אין כיום חובות אתיות או משפטיות לתכנן את הטכנולוגיה שלהם או לעצב אותה מחדש כשהם מתקינים אותה אצל מעסיק מסוים תוך התחשבות בזכויות העובדים (או כל זכות אדם אחרת).[90] כך, החובות החלות על מעסיקים להגן על מידע פרטי (של לקוחות, של עובדים) ועל העסק עצמו, כמו גם על מטרות חברתיות אחרות, אל מול "צדדים שלישיים" שעשויים לפגוע במרחב הקיברנטי, מעצימות, אם כן, את מתח הפרטיות ביחסים הדו-צדדיים המתקיימים בין העובדים לבין המעסיק. ההסתמכות על אנשי מקצוע שאינם נותנים די משקל לזכות למידע הפרטי של העובדים מעצימה מתח זה.

זאת ועוד, אחת החובות המשפטיות הבסיסיות שיש למעסיקים להגנה על פרטיות המידע של עובדיהם על ידי טכנולוגיות (במקרה זה תוכנות להגנת סייבר) הנה שקיפות בכל הנוגע למדיניות הארגון לגבי אופן איסוף המידע, עיבודו ופיזורו לצדדים נוספים.[91] לשקיפות יש משקל מכריע לפי הדין הקיים, ואולם, בדין הישראלי ההחלטה בדבר האופן בו המידע מועבר לעובדים נותרת בידיים של המעסיק, מבלי שנקבעו כללים מכוונים בעניין זה.[92] למיטב ידיעתנו, טרם נעשה מחקר הבוחן עד כמה מתמלא כלל השקיפות על ידי מעסיקים במשק הישראלי - האם מעסיקים מוסרים את המידע האמור לעובדים או לאו, ואם כן באיזה אופן. ואולם, אם מסתכלים על מקרים אחרים בהם מידע טכנולוגי מועבר לציבור, אזי ניתן לראות שפעמים רבות אופן העברת המידע כולל מידע טכנולוגי רב שפעמים רבות אינו מובן דיו. מחקרים מראים כי במצב זה ישנו קושי אמיתי של בעלי המידע להחליט כיצד לנהוג. זאת הן בכל הנוגע לשאלה האם יסכימו למסירת המידע או לא, וכן לאופן בו יתנהלו עם המידע הפרטי שלהם – לתוך אילו אתרים ייכנסו, איזה מידע פרטי יהיה על המחשב האישי שלהם או בתיבות הדוא"ל שלהם וכיצד מידע ממקורות אלה מגיע לגורם האוסף ומעבד את המידע, ועוד.[93]

מעבר לכך, האופן בו מוצג המידע בהקשרן של טכנולוגיות חדשות דומה פעמים רבות לחוזים אחידים, שאין אפשרות ממשית לשנות או לנהל עליהם משא ומתן. מעבר לכך, חוזים אחידים מכילים פעמים רבות תניות מקפחות,[94] אשר המחקר האקדמי הראה כי הם לא בהכרח מכילים את רצונם של שני הצדדים.[95] עוד עולה

---

[89] ראו דיון בהגנת סייבר כתכלית לגיטימית בפרק ד להלן.

[90] למעט חובות שנגזרות כתוצאה מתחולת דין זר על חברות מקומיות או חברות שאימצו סטנדרטים שכאלה באופן וולנטרי (בעקבות דרישת לקוחות וכדומה). ראו פירוט של העדר חובות אלה בדיון בתת פרק הבא, תחת הכותרת "חברות הסייבר".

[91] ראו בהרחבה דיון בעקרונות ההלכתיים בפרק ד להלן.

[92] בניגוד, למשל, לתקנון למניעת הטרדה מינית שמפרט מה על המעסיק לפרסם בהקשר זה לציבור העובדות והעובדים.

[93] Lori Andrews, *The Fragility of Consent*, 66(1) Loy. L. Rev. 11 (2020); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Washington U. L.Q. 1461 (2019).

[94] על תניות מקפחות ראו: אייל זמיר **פירוש והשלמה של חוזים** 40-39 (1996).

[95] עצם היות החוזה אחיד עם פוטנציאל לתניות מקפחות והדין המכיר בכך, משקפים זאת. שם.

מהמחקר שדווקא במקרים בהם החוזה שקוף הוא פעמים רבות חד צדדי ולא נוהל עליו משא ומתן עם הצד השני,[96] ומעל לכל זאת שאנשים אינם מיודעים בדבר הכתוב בחוזים אלה לאור משך הזמן המועט בו הם מגללים את המידע מטה ועושים וי על קופסת ההסכמה.[97] מעבר לכך, הגורם שמעביר את המידע אף יכול להחליט כיצד לסגנן את המידע המועבר דבר שעשוי להטות את האופן בו יבינו את המדיניות. על אף, שכאמור, אין למיטב ידיעתנו מחקרים הבוחנים שאלות אלו בהקשר של תעסוקה, אין סיבה להניח כי יש הבדל מהותי בספירה זו.

ב. <u>חברות הסייבר</u>:

בשנים האחרונות, פעילותן העסקית של חברות המפתחות תוכנות להגנת סייבר, מוכרות אותן, ומשימות אותן אצל מעסיקים תוך התאמתן לצרכיו של כל מעסיק ספציפי, גדל מאד.[98] הכוח של חברות המפתחות את הטכנולוגיה נשען על יכולתן להציע טכנולוגיה חדישה יותר ואפקטיבית יותר למתן הגנת סייבר בארגון, דבר שאף נשקל בעת מכירת התוכנות וכן השמתן אצל מעסיקים. בכך החברות נותנות מענה לחובותיו המשפטיים של המעסיק לגבי ההגנה כפי שפורטו בתת-חלק הקודם. בהיות חברות הטכנולוגיה מונעות על פי דרישות שוק, אזי ככל שמדיניות הסייבר של המדינה נהיית יותר נוקשה ומחייבת, חברות אלה מרוויחות יותר שכן המוצרים שלהם נהיים מוצרים חיוניים.[99] כך, למשפט יש חלק משמעותי בכיוון ועיצוב הטכנולוגיה.

ההשפעה שיש לחברות הסייבר על התהליך של איסוף ועיבוד המידע הנה גדולה, ולה השלכות ישירות על זכותם של העובדים לפרטיות. ואולם, מבחינה משפטית או אתית, אין כיום חבות על החברות המפתחות את הטכנולוגיה לדאגה לזכויות אדם באופן כללי, ולזכויות עובדים בפרט, ואין להן כל אחריות להגן על הזכות למידע פרטי. העדר אחריות זו זכתה לביקורת.[100] בהיותה מודעת לחשיבות של חברות טכנולוגיה להשפעה על זכויות אדם, הספרות והפרקטיקה עוסקים בשנים האחרונות בחשיבה על אחריות חברתית של תאגידים טכנולוגיים לזכויות אדם, כולל זכויות עבודה.[101] כמו כן מושם דגש על הרעיון של הנדסת פרטיות (privacy by design) שמסיט את כובד המשקל של ההגנה על הפרטיות ממשתמש הקצה (במקרה שלנו המעסיק) אל החברה שמתפתחת את הטכנולוגיה.[102]

---

[96] Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 U. CHI. L. REV. 165 (2011); Eyal Zamir & Yuval Farkash, *Standard Form Contracts: Empirical Studies, Normative Implications, and the Fragmentation of Legal Scholarship: Comments on Florencia Marotta-Wurgler's Studies* 12(1) JERUSALEM REV. LEG. STUD. 137.

[97] שם.

[98] STATISTA, *Cybersecurity – Worldwide*, לעיל ה"ש 7.

[99] Natalie Green, *CyberSecurity and Human Rights*, Carolina Rossini & Public Knowledge.

[100] Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 U. PENN L. REV. 633 (2017).

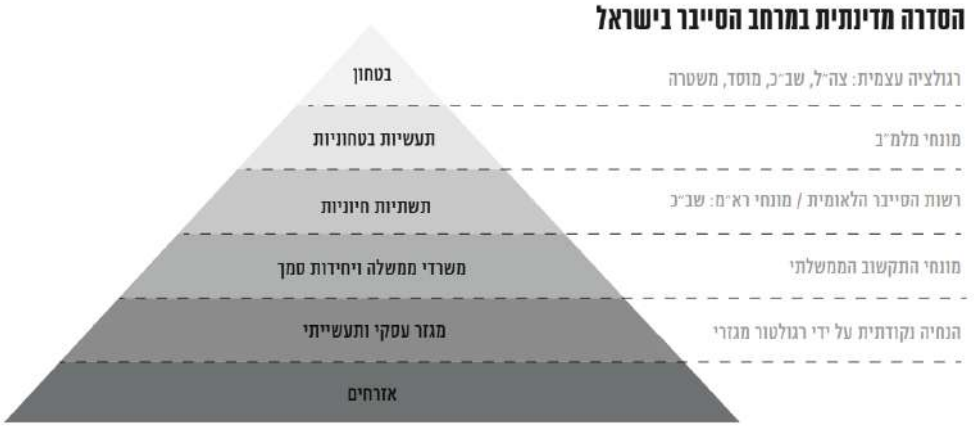
[101] Daniel Kreiss & Shannon C. McGregor, *Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google with Campaigns During the 2016 U.S. Presidential Cycle*, 35 Pol. Commc'n 155 (2018); Irene Pollach, *Online Privacy as a Corporate Social Responsibility: An Empirical Study*, 20 Bus. Ethics: A Eur. Rev. 88 (2011).

[102] על הרעיון של הנדסת פרטיות ראו בהרחבה מיכאל בירנהק, "הנדסת פרטיות ציבורית: המקרה של העברת מידע ממרשם האוכלוסין למפלגות" **דין ודברים** י"ב, 15.

לאחרונה, האיחוד האירופי מקדם חקיקה אשר תטיל אחריות משפטית על חברות המפתחות טכנולוגיות בינה מלאכותית, כולל בהקשר של סייבר, כאשר ישנה סכנה להפרת זכויות אדם ובין השאר זכויות עבודה.[103] על אף שהועלתה ביקורת על הגישה המאומצת בהצעתו של האיחוד,[104] חשיבה מורכבת יותר על האחריות של החברות הללו בעת פיתוח הטכנולוגיה, שכלולה, ועיצובה מחדש בעת השמתה אצל מעסיק הנה חיונית. בישראל, טרם נדרשו לסוגיה הנדונה, דבר שיתכן והנו הכרחי בהינתן המלצתו של מערך הסייבר להגדיל את האוטומציה בתחום.[105] כך יוצא, שהכריכה שנעשית בין הדרישות המשפטיות החלות על ארגונים (מעסיקים) להגנה על מאגרי המידע שלהם, החובות בדירקטוריונים, המשגת ההגנה על הסייבר כאתגר של ביטחון לאומי כמתואר בהמשך, והשימוש בטכנולוגיות אלה ללא כל אחריות משפטית או אתית, מגדילים את כוחן של חברות הסייבר. היא אף מעצימה את כוחם של מעסיקים להצדיק את השימוש שנעשה בטכנולוגיות האמורות.

ג. <u>הרגולטור</u>:

במזכר של המכון למחקרי בטחון לאומי (INSS), סיבוני וסבילה טוענים כי במדינות מערביות ובכללן ישראל, אין מענה רגולטורי הולם למגזר העיסקי-אזרחי, המשמש פעמים רבות כחוליה החלשה במרחב הסייבר, וממחישים זאת באמצעות התרשים הבא:



כפי שניתן לראות בתרשים, המגזרים הנתונים תחת הנחיות רגולטוריות מחייבות אינם כוללים את המגזר האזרחי הפרטי, למעט אם מדובר בתשתיות חיוניות, אשר פגיעה בהן עלולה לפגוע במהלך התקין בישראל ולהסב נזק לביטחון הלאומי, כגון תעופה, מים וגז ; ולמעט מגזרים המונחים על ידי רגולטור מגזרי דוגמת שוק ההון ומוסדות בריאות.[106]

---

[103] *Proposol for a Regulation of the European Parliament and of the Council Concerning Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,* COM (2021) 206 final (Apr. 21, 2021). (להלן: The Proposed Artificial Intelligence Act).

[104] Valerio De Stefano, *"The EU Proposed Regulation on AI: A Threat to Labour Protection?",* REGULATING FOR GLOBALIZATION (Apr. 16, 2021), http://regulatingforglobalization.com/tag/artificial-intelligence/.

[105] על המלצה זו ראו דיון בעמוד הבא.

[106] גבי סיבוני ועידו סיון-סבילה, רגולציה במרחב הסייבר, מזכר 180 (אוגוסט 2018), 79-91, המכון למחקרי ביטחון לאומי, אוניברסיטת תל אביב: https://www.inss.org.il/he/wp-content/uploads/sites/2/2018/08/memo180CyberRegulation_6.pdf .

בהתאם לחוק להסדרת הביטחון, האחריות להנחיית גופים אשר להם מערכות חיוניות הוטלה על נציג מערך הסייבר הלאומי.[107] יריית הפתיחה להקמת מערך הסייבר הלאומי הייתה בשנת 2011 בעקבות החלטת ממשלה שקבעה כי יש לקדם את היכולת להגן על תפקודו התקין הבטוח של מרחב הסייבר תוך שהיא מגדירה זאת כ"יעד ביטחוני חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי".[108] המערך כולל בתוכו את הרשות הלאומית להגנת הסייבר ואת המטה להגנת הסייבר.[109] למעט סמכות רגולטוריות כלפי גופים המנויים בחוק להסדרת בטחון, עד היום אין למערך הסייבר סמכויות מעבר למה שניתנו לו על ידי החלטות הממשלה, וזאת בשל העדר קידום תזכיר חוק הסייבר. לכן, ולאור העובדה כי הסייבר הינו מרחב המופעל בעיקרו על ידי פרטים וארגונים אזרחיים, המערך פועל על בסיס שיתוף פעולה הסכמי עם הארגונים המחויבים להגן על המרחב הקיברנטי שלהם. בעת חשש להתקפת סייבר פונה המערך אל הארגון ומבקש כי יינתן לו לסייע בהתמודדות עמה. במסגרת תפקיד זה עשוי המערך להיחשף למידע פרטי על העובדים.

התפיסה של מערך הסייבר היא כי הארגון הוא האחראי להגן על עצמו, אך לצורך הגנה על מרחב הסייבר נדרש שיתוף פעולה בין הממשלה למשק ובין הארגונים לבין עצמם. בין תפקידיו, כפי שמוצג באתר מערך הסייבר, על המערך להכווין את הציבור והמשק הישראלי להיערך לקראת איומי סייבר.[110] כך למשל, בחודש יולי 2021, פרסם מערך הסייבר מדריך יישומי להגנת הסייבר של הארגון.[111] מדריך זה מציג מתודולוגיה סדורה לניהול סיכוני סייבר בארגון, תוך התאמת האמצעים לפוטנציאל הנזק של הארגון. בהתייחסות לשיקולי הגנת הפרטיות, מצוין במדריך כי "ככלל, הגנת סייבר היא פעולה לגיטימית שאין בה כל פגיעה חריגה בפרטיות. עם זאת, המימוש שלה בפועל צריך להתבצע תוך התייחסות מעמיקה להיבטי פרטיות ועמידה בעקרונות מקובלים". ביצוע איזון בין האינטרסים השונים של הארגון, באופן שיאפשר להנהלת הארגון לקבל החלטות באופן מושכל, מוטל על-פי המדריך על מנהל הגנת הסייבר בארגון, ה-CISO, שעליו לערב את היועץ המשפטי, ולפעול לצמצום הן את סיכוני הסייבר והן את הפגיעה בפרטיות. כמו כן, המדריך שם דגש על שימוש בתהליכי אוטומציה וצמצום הצורך במעורבות יד אדם למקרים חריגים בלבד, על מנת להקטין את החשיפה של הגורמים השונים למידע אישי. הצמצום במעורבות יד אדם הנו חיובי במובן זה שהוא יכול לסייע במניעת הפצת המידע, ואולם הוא מעורר, במקביל, קשיים בכמה רמות: מבחינת השאלה מי יישא באחריות משפטית במידה וההחלטה הנה שגויה וגורמת נזק, המשקל שיש לתת בעת פיתוח הטכנולוגיה לפגיעה בזכויות אדם, ביניהן זכויות עבודה והזכות לפרטיות, השותפות של ארגוני עובדים

---

[107] ס' 10 לחוק להסדרת הביטחון.

[108] החלטה 2444, לעיל ה"ש 4.

[109] בשנת 2011 התקבלה החלטת ממשלה 3361 של הממשלה ה-30 "הסכם שיתוף פעולה בין רשות ניירות ערך הישראלית לבין רשות ניירות ערך ההולנדית (AFM)" (06.03.2005), שעסקה בהקמת מטה הסייבר הלאומי, בכפיפות לראש הממשלה. בהתאם להחלטת ממשלה מס' 2444, לעיל ה"ש 4, הוקמה הרשות הלאומית להגנת הסייבר, אשר החלה לפעול בשנת 2016, כגוף האופרטיבי להגנת הסייבר, בעוד מטה הסייבר הלאומי פעל כגוף המדיניות ובניין הכוח. בסוף שנת 2017, בהחלטת ממשלה 3270 של הממשלה ה-34 "איחוד יחידות מערך הסייבר הלאומי" (17.12.2017), הוחלט על איחוד שני הגופים לכדי יחידה ארגונית אחת – מערך הסייבר הלאומי. לפרטים נוספים ראו: מערך הסייבר הלאומי "אודות מערך הסייבר הלאומי" **gov.il** (01.07.2021) https://www.gov.il/he/Departments/about/newabout.

[110] שם.

[111] מערך הסייבר הלאומי "תורת ההגנה בסייבר 2.0" **gov.il** (19.07.2021) https://www.gov.il/he/departments/general/cyber_security_methodology_2.

בתהליך, האופן שבו ייאסף המידע ויתבצע עיבוד הנתונים ועוד. בנוסף, מסמכים שונים, בעיקר אירופאים,[112] וכן של ארגון העבודה הבינלאומי,[113] הדגישו את החשיבות שהחלטות לגבי אנשים יתקבלו על ידי אנשים ולא על ידי מכונות.

עיקר המיקוד של האסדרה בישראל הינו באבטחת סייבר של ארגונים ושל תשתיות חיוניות בפרט, כאשר הטיפול בסיכוני סייבר, אמור להיות מתוכלל על ידי מערך הסייבר הלאומי, כמפורט לעיל. עם זאת, לאחרונה ישנו עיסוק בספרות באסדרה של אבטחת סייבר בציוד קצה.[114] לאור השינויים הטכנולוגיים בעידן הדיגיטלי המודרני, פעמים רבות מחובר ציוד קצה פרטי לרשת ארגונית, כדוגמת טלפון חכם או מחשב נייד של עובד המחובר לרשת של מקום העבודה, ובכך הרשת הארגונית ומשתמשים נוספים נחשפים לסיכוני סייבר, כאשר ציוד הקצה משמש כבסיס למתקפות הסייבר.[115] במאמרו בנושא, אבידן טוען כי גם אם תזכיר חוק הסייבר יתגבש לכדי חוק, אין די במתן הנחיות או הוראות לארגונים ויש להחיל אמצעים רגולטוריים גם על היצרנים ושותפיהם של ציוד הקצה, על מנת לאבטחו למשל באמצעות עדכון מערכות הפעלה, התקנת תוכנה לשיפור אבטחה וכדומה.[116] גישה דומה יש להפעיל, לדעתנו, לגבי הפגיעה בזכויות, כולל הזכות למידע פרטי, גישה, אשר, כפי שציינו לעיל, מקודמת כיום על ידי האיחוד האירופי ומדינות נוספות בעולם.[117]

רגולטור מרכזי נוסף האמון על קידום של ציות לדיני הגנת המידע, בהתאם לדיני הגנת הפרטיות הנו הרשות להגנת הפרטיות. [118] במסגרת זו, הרשות להגנת הפרטיות מופקדת על פיקוח ואכיפת חלק מהחובות המשפטיות המוטלות על מעסיקים המפורטות לעיל, באמצעות הליכים פליליים ומנהליים. בפרט, בכל הנוגע להגנה על מידע אישי במאגרי מידע דיגיטליים. כמו כן, הרשות פרסמה מספר ניירות הנוגעים להגנת הזכות לפרטיות בעבודה הכוללים, בין היתר: הנחיות בנוגע לשימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה,[119] הנחיות בנוגע לתחולת חוק הגנת הפרטיות על הליכי מיון וגיוס עובדים,[120] דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית, [121] הנחיות בדבר איסוף ושימוש במידע ביומטרי לדיווח ולבקרת נוכחות עובדים במקום העבודה,[122]

---

[112] ה- GDPR קובע כלל שכזה, וגם ההסכם בין הצדדים האירופאיים ליחסי עבודה מיוני 2020 ובו נאמר כי: Support the development of a human-oriented approach to integration of digital technology.

[113] ראו דיונים עם human in command ב- ILO, *Global Commission on the Future of Work, Work for a Brighter Future* (2019).

[114] ראו: אסף אבידן, "אסדרה של אבטחת סייבר בציוד קצה", **דין ודברים** יד (2019). מההגדרה של "ציוד קצה" בסעיף 1 לחוק התקשורת (בזק ושידורים), תשמ"ב-1982, ומהפרשנות שניתנה לה בפסיקה, עולה כי שמדובר במגוון התקנים המצוים בקצה התשדורת שמאפשרים חיבור לרשת תקשורת ציבורית, לרבות חיבור לאינטרנט. ראו: אסף אבידן, בעמ' 29-31.

[115] שם, בעמ' 17-22.

[116] שם, בעמ' 80.

[117] The Proposed Artificial Intelligence Act, לעיל ה"ש 103; The National Institute of Standards and Technology in the US Department of Commerce, "AI Risk Management Framework" at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; The White House's Blueprint for an AI Bill of Rights

[118] ראו: משרד המשפטים "אודות הרשות להגנת הפרטיות" **gov.il** (15.08.2019) https://www.gov.il/he/departments/about/about_ppa.

[119] משרד המשפטים "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה" **gov.il** (17.10.2017) https://www.gov.il/he/departments/policies/workplace_camera.

[120] משרד המשפטים " הליכי מיון לקבלה לעבודה ופעילות מכוני מיון" **gov.il** (28.02.2012) https://www.gov.il/he/departments/policies/recruitment_guidelines.

[121] משרד המשפטים " דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית" **gov.il** (24.03.2020) https://www.gov.il/he/departments/publications/reports/corona_work.

[122] משרד המשפטים "איסוף ושימוש במידע ביומטרי לדיווח ולבקרת נוכחות עובדים במקום העבודה" **gov.il** (15.2.2024) https://www.gov.il/he/Departments/publications/reports/biometric_workplace.

והיבטי פרטיות במעקב אחר עובדים בעבודה מרחוק.[123] ואולם עד היום הרשות לא נתנה את הדעת למתח המתואר במאמר זה. בעמדות לעיל הרשות מחדדת את חשיבות ההגנה על מאגרי המידע אל מול צדדים שלישיים וכן את הכללים הנוגעים למעקב אחר עובדים, אך לא נדרשת לאיזון בין הגנה על מאגרי המידע ועל אינטרסים נוספים במסגרת הגנה על הסייבר, לבין הזכות להגנה על מידע פרטי. כך למשל, בעמדת הרשות בנוגע למעקב אחר עובדים בעבודה מרחוק, ישנו פירוט של אמצעי מעקב שפגיעתם עשויה להיות גבוהה במיוחד, הכוללים כלי סריקה ופיקוח על אתרי האינטרנט בהם גולש העובד.[124] בעמדה מצויין כי השימוש באמצעים אלו יחרוג על-פי רוב מהמותר על-פי דין, למעט שימוש סביר ומידתי לצרכי אבטחת מידע והגנת סייבר. מעבר לדרישה כי השימוש באמצעים אלו לצרכי סייבר יהיה סביר ומידתי, אין בעמדה הנחיות כיצד לבצע איזון זה.[125]

2. בין הגנה לביטחוניזציה

הלן ניסנבאום, אחת הכותבות הבולטות בתחום של טכנולוגיה ומשפט, ציינה כי "הגנה" אינו מונח טכני, אלא מונח עשיר, מורכב, ובעל תפיסות שונות ואף מתחרות, המושתתות על ערכים נבדלים שמשפיעים ישירות על הטכנולוגיה ועל האופן שבו אנחנו מתייחסים להגנה.[126] תפיסה אחת של הגנה היא זו שנוגעת להגנה טכנית על מחשבים, אשר שורשיה בשדה המדעי והטכנולוגי. תפיסה זו עוסקת בצורך בהגנה על פעילות תקנית של מתן שירותים, איומים על אמיתות המידע, וחשש לסודיות של מידע, כגון אפשרות גישה לתכנים של אימיילים, גישה לא מאושרת למאגרי מידע ועוד. תפיסה שניה של הגנה מחברת בין הגנה על מחשבים לבין ביטחון לאומי,[127] ורואה את ההגנה כמשהו חיוני וקריטי למדינה, תשתיותיה ואזרחיה. הגדרתו של איום כאיום בטחוני מצדיקה שימוש באמצעי הגנה יוצאי דופן ומחמירים, שיש בהם דחיפות ושהם נתפסים כאמצעי חירום.[128] הם מאפשרים התגמשות עם מדיניות קיימת (משפטית או אחרת) בשל איפיונם ככאלה. כך, יש קשר ישיר בין הערך אותו אנחנו מגדירים (הגנה על מערכות מחשוב או הגנת סייבר על בסיס רעיון של ביטחון לאומי) לבין עיצוב הטכנולוגיה והאמצעים שננקטים.

גם הדין הישראלי עושה הבחנה שכזו בין הגופים הכפופים לחוק להסדרת הביטחון ואלה שלא. החוק להסדרת ביטחון, מבחין בין גופים שונים לפי חיוניותם, וזאת דרך רשימות המצויות בתוספות לחוק. החוק קובע הוראות שונות לגבי גופים המנויים בכל אחת מהתוספות,[129] מאפשר לשר לפטור גוף ציבורי המנוי בתוספת השלישית מהחובה למנות ממונה ביטחון ואף קובע שבכך לא יחולו על אותו גוף ציבורי הוראות החוק,[130] וקובע מהן מערכות ממוחשבות חיוניות.[131] גם הצעת חוק הסייבר והצעת החוק המקוצרת מגבילים את פעילות מערך הסייבר רק למה

---

[123] משרד המשפטים "היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק" **gov.il** (17.10.2023) https://www.gov.il/he/departments/publications/reports/remotework

[124] שם, בסעיף 9 לעמדה.

[125] שם, בה"ש 8 לעמדה.

[126] Helen Nissenbaum, *Where Computer Security meets National Security*, 7 ETHICS & INFO. TECH. 61 (2005).

[127] שם, בעמ' 63.

[128] שם, בעמ' 69.

[129] ס' 2, 2א לחוק להסדרת הביטחון.

[130] ס' 2(ב) לחוק להסדרת הביטחון.

[131] ס' 2א לחוק להסדרת הביטחון.

שמוגדר כ"אינטרס חיוני".[132] זו אף עמדתו של האיחוד האירופי, אשר חוקק בשנת 2016 חקיקה המחייבת את המדינות החברות באיחוד לגבש מדיניות הגנת סייבר, לקבוע הסדרה לתשתיות ולהקים מערך לאומי שמטרתו טיפול באירועי סייבר.[133] השיח הביטחוני במסמך זה הנו מועט ביותר וכולל אמירות כגון החשיבות הרבה שיש להגנה על מידע וחיוניותן לתקינות שוקית (סעיף 1); וכן החיבור בין הגנה על תפקוד המדינה ובמיוחד ביטחונה (סעיף 1(6)). בנוסף, בשנת 2015 ה- OECD החליט לשנות את גישת ההגנה על המרחב הקיברנטי, תוך שהוא נפרד מהמונח "הגנת סייבר" ועבר לשימוש במונח "הגנה דיגיטלית", באומרו כי יש להתייחס אל הגנה על מרחב זה והסיכונים המצויים בו כאל כל מרחב וסיכון כלכלי אחר, ולא כמשהו שהוא שונה מבחינה מהותית.[134]

לאור זאת, יש לבחון היטב את סוגי ההגנה השונים שניתנים על ידי מערכות הגנת הסייבר בארגון, והאם הם מאמצות את ההבחנה האמורה, זאת בעיקר כאשר המדובר באפשרות לפגוע באחת מהזכויות המוכרות של עובדים שנחשבים כאוכלוסייה פגיעה. המשגה שגויה של "הגנה" כקשורה לאיום על המדינה או על תשתיות עשויה להפוך הגנה על מאגרי מידע קטנים (כגון מאגר מידע של לקוחות במכולת או אפילו בבנק) לעניין שנתפס כבעיה ביטחונית.[135] יש להיזהר מלטעות כי מדובר בהכרח בהגנה העולה כדי "ביטחון לאומי" בכל אחד מהמצבים של הגנה על המרחב הקיברנטי. וירוסים שנכנסים למרחב הקיברנטי ומשבשים פעילות ועשויים אף לאסוף מידע, או לגרום לפיחות ההגנה על המידע; ספאמים; פריצות לא מאושרות לתוך המרחב ועוד, אינם בהכרח איומים שעשויים להוביל לפגיעה מעבר לזמינות במתן שירותים ופגיעה באמיתות המידע, פגיעה שהיא כלכלית ושוקית גרידא. אמנם, פעמים רבות לא ניתן למיין מראש את הנזקים הפוטנציאליים לכאלו שמהווים סיכון רק לעסק לבין פגיעות המהוות סיכון מדינה והבחנה כזו היא נזילה. אולם, תפיסה כוללת של ביטחוניזציה עשויה לייצר לגיטימציה עודפת לפגיעה בפרטיות בכלל, ובמידע הפרטי של העובדים בפרט. אנו סבורות כי גם בהקשר של עבודה יש לפתח חשיבה יותר מידתית ומאוזנת שכזו. בדיון בהמשך נחדד את חשיבות ההבחנה האמורה בין הגנת סייבר לתכליות עסקיות להגנה ביטחונית בהקשר של עבודה.

ד. הגנת הפרטיות בדין הישראלי

בהקשר של עבודה, הזכות לפרטיות נדונה לראשונה בישראל בכל הנוגע לצורך להגן על מאגרי מידע במסגרת חוק הגנת הפרטיות.[136] מאוחר יותר, כאשר נדרשה התמודדות יותר מעמיקה עם הפגיעה הפוטנציאלית בזכות של העובדים כתוצאה מהתפתחותה של טכנולוגיית המידע, היכולת לנטר אחר עובדים וצרכים המצדיקים ניטור שכזה,

---

[132] ס' 19(ג)(1) לתזכיר חוק הסייבר, לעיל ה"ש 22; הצעת חוק הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לצורך חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א-2021. ראו הגדרה של "אינטרס חיוני" בס' 1 לתזכיר חוק הסייבר.

[133] Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, O.J. (L 194) 1.

[134] OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, 4 (2015).

[135] Helen Nissenbaum, *Digital Disaster, Cyber Security and the Copenhagen School*, 53(4) INT'L STUD. Q. & Lene Hansen 1155, 1156 (2009).

[136] סימן ב' בפרק א' לחוק הגנת הפרטיות.

נחתם הסכם קיבוצי בין הסתדרות העובדים הכללית לבין לשכת התיאום של הארגונים הכלכליים, ואולם טרם יישומו נתן בית הדין הארצי לעבודה את הלכת איסקוב ענבר.[137] כמה שנים מאוחר יותר, הגיעה הלכת קלנסווה המשלימה.[138] בפרק זה נציג את ההלכות האמורות ואת הנקבע בהן ונבחן האם הן ויישומן על ידי בתי הדין לעבודה מספקים לצורך ההגנה על הזכות לפרטיות המידע של העובדים בהקשר המורכב של הגנת סייבר ולאור המשקל הרב שיש לתת להגנה זו, כפי שאלה שורטטו בפרק הקודם.

בפרשת איסקוב ענבר, בית הדין הארצי לעבודה ביקש לאזן בין זכות העובד לפרטיות ובין זכותו הקניינית והפררוגטיבה הניהולית של המעסיק. זאת, במקרה שבו המעסיקה ניטרה אחר תיבת הדוא"ל של העובדת ולאחר מכן הוציאה משם תכתובות על מנת להגיש אותן כראיות בהליך משפטי שהתנהל בין הצדדים לתמוך בטענה כי במועד פיטוריה של איסקוב ענבר היא לא הייתה בהריון.[139] באותה פרשה נדון מקרה נוסף – אפיקי מים – שגם שם הגיש המעסיק לבית הדין תדפיסים של תכתובות דוא"ל שהופקו מהשרת האלקטרוני של החברות כראיה.[140] בפסק הדין, בית הדין הארצי לעבודה ביקש לשרטט את קו הגבול בין הערך החוקתי-אובייקטיבי לקניין של המעסיק, אשר ממנו גם נגזרת הפררוגטיבה הניהולית שלו, וכן חופש העיסוק של המעסיק, לבין המרחב הווירטואלי הכולל, בנוסף למידע עסקי, גם מידע פרטי ואישי של העובד. בית הדין מגדיר את המידע הפרטי המצוי במרחב הוירטואלי "כמרחב הפיסי האישי השמור לאדם"[141] ואומר כי "הפעילות במחשב כמוה כעשיית המשתמש בביתו".[142]

במסגרת זו, בית הדין ערך הבחנה בין תיבת דוא"ל מקצועית של העובד המיועדת לצרכי עבודה בלבד, תיבת דוא"ל מעורבת, המיועדת לצרכי עבודה אך המעסיק מתיר לעובד לקיים בה תכתובת אישית, ותיבת דוא"ל אישית שהעובד פתח לעצמו.[143] לגבי האחרונה קובע בית הדין כי המעסיק אינו רשאי לערוך ניטור או מעקב אחרי תיבת דוא"ל חיצונית-פרטית של העובד, גם אם זה נתן את הסכמתו.[144] בית המשפט העליון אימץ עמדה זו בעניין זינגר וקבע כי המעסיק אינו רשאי לנטר או לעקוב אחרי תיבת דוא"ל חיצונית-פרטית גם אם זו הושארה בשוגג פתוחה על מסך המחשב.[145]

בדיון על זכויות הקניין וחופש העיסוק של המעסיק וכן הפררוגטיבה הניהולית וחוזה העבודה בין הצדדים, מדגיש בית הדין בפרשת איסקוב ענבר, כי למעסיק יש זכות יתר לקבוע את האמצעים הטכנולוגיים שיהיו במקום העבודה, על מכלול יישומיהם ואת השימוש שיעשה בהם, וזאת בשל היותם חלק בלתי נפרד מסביבת העבודה ואמצעי הייצור.[146] כן נאמר כי "זכות הקניין של המעסיק במקום העבודה והפררוגטיבה הניהולית שלו, מקימות לו זכות

---

[137] על ההשתלשלות המפורטת של מהלך הדברים בישראל ניתן ללמוד מעניין **איסקוב ענבר**, לעיל ה"ש 13, פס' 5 לפסק דינה של השופטת נילי ארד.
[138] פרשת **קלנסווה**, לעיל ה"ש 14.
[139] שם, פס' 3 לפסק דינו של השופט אילן איטח.
[140] שם, פס' 4 לפסק דינו של השופט אילן איטח.
[141] שם, פס' 6 לפסק דינו של השופט אילן איטח.
[142] שם.
[143] שם, פס' 54 לפסק דינו של השופט אילן איטח.
[144] שם.
[145] רע"א 2552/16 **יהודה זינגר ואחרים נ' חברת יהב חמיאס טכנולוגיות (1990) בע"מ ואחרים**, פס' 42-45 לפסק דינו של השופט סולברג (נבו 10.5.2016).
[146] פרשת **איסקוב ענבר**, לעיל ה"ש 13, פס' 8 לפסק דינה של השופטת נילי ארד.

להגן על רכושו הפיזי והווירטואלי האצור ברשת. **אי לכך, רשאי המעסיק לנקוט באמצעים מוגברים של אבטחת המידע שנצבר ברשת, הנקלט בה והיוצא ממנה**. במסגרת זו, רשאי המעסיק לפקח על פעילותם של העובדים כדי לוודא שלא יעשו שימוש בלתי מורשה, או בלתי חוקי בכלי העבודה הווירטואלי והמידע המופקד בידם" (הדגשה לא במקור – ע.א., ג.ע.). [147] כמו כן נאמר, כי המעסיק רשאי לקבוע את מדיניות השימוש בטכנולוגיות העומדות לרשות העובדים, כולל השימוש בתיבות הדוא"ל וכל זאת בכפוף לעקרונות תום לב, גילוי, שקיפות, לגיטימיות, מידתיות וצמידות המטרה (להלן: העקרונות ההלכתיים). [148] לבסוף, מחדד בית הדין את זכותו של המעסיק לבצע מעקב אחר העובדים, כולל איסוף ועיבוד מידע, דבר שהוא אומר "הפך לחלק בלתי נפרד של סביבת העבודה המודרנית". [149] זאת, כאמור, גם בכפוף לעקרונות הסבירות, מידתיות, תום לב והגינות. בקביעת האיזון בין הפגיעה בזכות לפרטיות לבין זכויות אלה של המעסיק מתמקד בית הדין בשלוש סוגיות משפטיות מרכזיות: שאלת פרטיות המידע, דרישת ההסכמה, כאשר בית הדין קובע כי ההסכמה הנדרשת בהקשר של עבודה היא הסכמה מדעת, מראש ומרצון חופשי נוכח אופיים הייחודי של יחסי עבודה ויחסי הכוח בין הצדדים. [150] עוד ציין בית הדין את המחויבות לאותם העקרונות ההלכתיים, ללא קשר לשאלת ההסכמה. [151]

בפרשת קלנסווה בית הדין עסק בשאלה האם רשות מקומית רשאית לחייב את עובדיה למסור טביעת אצבע לשם רישום שעות נוכחות בשעון ביומטרי. [152] בית הדין הארצי המשיך את הקו שנקבע באיסקוב ענבר, חזר על עקרונות ההלכה, וביניהן זכות הקניין של המעסיק וזכותו לפררוגטיבה ניהולית על מנת להגן על הקניין שלו וזכותו לנהל את העסק כראות עיניו, כמו גם זכויות העובדים לעבוד, פרטיות ואוטונומיה. [153] בנוסף, עסק בית הדין בשלוש הסוגיות המשפטיות של פגיעה בפרטיות, הסכמה ושמירה על העקרונות ההלכתיים, ואף הדגיש את הצורך לוודא את טיבה של המערכת הטכנולוגית, את תוקפה ומהימנותה, [154] תוך הפנייה להלכה קודמת בעניין אוניברסיטת תל-אביב. [155] בית הדין בקלנסווה השאיר ב"צריך עיון" שאלה חשובה הנוגעת למשמעותה של הסכמה קיבוצית לפגיעה בפרטיות, והאם זו מספקת במקום הסכמה אישית. [156]

שתי ההלכות שרטטו את עמדת דיני העבודה בישראל להגנה על מידע פרטי. לפיהן, נקודת המוצא היא של פררוגטיבה מעסיקית להטמיע טכנולוגיות במקום העבודה וכן לאסוף מידע על עובדות ועובדים. זאת תוך יצירת ריסונים לפי שלושת המבחנים של: הבחנה בין מידע עסקי למידע פרטי; דרישת ההסכמה; וכן עמידה בשורת העקרונות ההלכתיים. בפרק זה נבחן את השאלה שהצגנו לעיל: האם ההלכות שנקבעו, ובהם שלושת המבחנים האמורים, מספקות לצורך ההגנה על הזכות לפרטיות המידע של העובדים בהקשר המורכב של הגנת סייבר. הואיל

---

[147] פרשת **איסקוב ענבר**, לעיל ה"ש 13, פס' 8 לפסק דינה של השופטת נילי ארד.
[148] שם.
[149] שם, פס' 10 לפסק הדין.
[150] שם, פרק רביעי לפסק הדין.
[151] שם, פס' 43-41 לפסק הדין. עקרונות אלה אף מעוגנים בחוק הגנת הפרטיות, למשל עיקרון צמידות המטרה מעוגן בסעיפים 2(9) ו-8(ב) לחוק ועקרון השקיפות בסעיף 11 לחוק.
[152] פרשת **קלנסווה**, לעיל ה"ש 14.
[153] שם, פס' 22 לפסק דינו של השופט אילן איטח.
[154] שם, בעמ' 36.
[155] דב"ע (ארצי) 97-70-4 **אוניברסיטת תל-אביב נ' ההסתדרות הכללית החדשה, האגף לאיגוד מקצועי** (נבו 17.6.1998).
[156] פרשת **קלנסווה**, לעיל ה"ש 14, פס' 145 לפסק דינו של השופט אילן איטח.

ובתי הדין לעבודה לא עסקו ישירות בסוגיית הגנת הסייבר, אלא בפסקי דין מעטים בלבד,[157] דבר מתמיה בפני עצמו נוכח השימוש הנרחב שיש בטכנולוגיות הגנת סייבר, נבחן את השאלה דרך האופן שבו הפסיקה הקיימת – לא רק הלכות איסקוב ענבר וקלנסווה - אלא גם פסקי דין של בתי הדין לעבודה - התייחסה לשאלת פרטיות המידע שנאסף על ידי טכנולוגיות בעולם העבודה באופן כללי.

1. שאלת פרטיות המידע

השאלה האם הפרטיות נפגעת הנה מהותית לבחינת הזכות. הראינו בפרק א של המאמר מה עשוי לעלות כדי פגיעה בפרטיות בהקשר של הגנת סייבר. זאת בכל הנוגע לאיסוף המידע, עיבודו במטרה לזהות אנומליה בהתנהלות ברשת, פיזורו, שימורו בידי המעסיק ואופן הצגת הדברים בעת יישום דרישת השקיפות. דיון מעמיק שכזה על מהותה של פגיעה בפרטיות המידע בהקשר של טכנולוגיות חדשות כמעט ולא התקיים עד היום על ידי בתי הדין לעבודה, למעט במספר מקרים בודדים.[158] זאת, על אף חשיבותו הרבה בעולם הדיגיטלי בו אנו חיים. מהפסיקה בישראל ניכר שבתי הדין יוצרים, בעיקר, שני סוגים של הבחנות. האחת, הבחנה בין הספירות (מרחב פרטי ומרחב עסקי), והשנייה, בין מידע עסקי למידע פרטי. כעיקרון, מידע עסקי הנו מידע שבתי הדין לעבודה מאפשרים למעסיק לנטר, לאסוף, לעבד, ואף לגשת אליו, בניגוד למידע פרטי שלגביו, כאמור, נדרשת הסכמה וכן חלים העקרונות ההלכתיים.[159] הבחנות אלה אינן מספקות משלוש סיבות עיקריות:

ראשית, פסיקה של בית הדין האירופי לזכויות אדם הכירה גם במידע בעל אופי מקצועי ככזה שיכול להיות מידע פרטי.[160] דברים דומים נקבעו על ידי בית המשפט העליון בפרשת א. גוטסמן אדריכלות בע"מ נ אריה ורדי.[161] לאור פסקי דין אלה ניתן לשער, כי גם מידע עסקי שנאסף על ידי טכנולוגיות להגנת סייבר עשוי לעלות כדי פגיעה בפרטיות במידה ויש בו משהו פרטי המזוהה עם אדם מסוים.

---

[157] פרשת **איסקוב ענבר**, לעיל ה"ש 13, וכן בפרשת סע"ש (אזורי ת"א) 16-11-21426 **מנשה נ' אודיס מפעלי סינון בע"מ** (נבו 16.1.2019).

[158] למשל, פרשת **קלנסווה**, לעיל ה"ש 14; וכן בס"ק (אזורי ת"א) 19-06-2994 **הסתדרות העובדים הכללית הסתדרות עובדי המדינה נ' מדינת ישראל** (נבו 8.10.2020), שם בית הדין דן בנוהל שהמדינה התקינה שעניינו "תפיסת ניהול לתפעול מערכת לאיכון ורישום נסיעות ברכב ממשלתי". יצויין כי בעס"ק (ארצי) 20-10-46575 **הסתדרות העובדים הכללית הסתדרות עובדי המדינה ואח' נ' מדינת ישראל** (נבו 9.3.2021) בית הדין הארצי לעבודה נתן תוקף של פסק דין להסכמת הצדדים לביטול פסק דינו של בית הדין האזורי לעבודה מיום 8.10.2020.

[159] כך למשל, בעניין **מנגלוס**, בית הדין קיבל כראיה חוות דעת של מומחה מחשבים לפיה סמוך לעזיבתם של מספר עובדים, שותפים ועורכי דין במשרד עורכי דין, הם מחקו והעתיקו קבצים רבים מהמחשבים במשרד לענן (דרופבוקס). בית הדין נימק זאת בכך שלא הוכח, כי המומחה פרץ לתיבות דואר אישיות וכי המומחה טען (טענה שלא נסתרה) כי הגדיר את החיפוש באופן שיכוון למסמכים הנוגעים ללקוחות המשרד ולא למסמכים פרטיים. ראו סע"ש (אזורי ת"א) 14-12-25953 **ד"ר כהן ושות'- משרדי עורכי דין נ' מנגלוס**, פס' 22 לפסק-הדין (נבו 18.1.2015). בעניין **באום**, בית הדין מאפשר שימוש במסמכים שנלקחו מתיבת דוא"ל מקצועית במסגרת ההליך מהטעם שמדובר במסמכים הקשורים בעניינים מקצועיים, הפגיעה בפרטיות, ככל שקיימת, אינה מהותית. ראו סע"ש (אזורי ת"א) 18-09-12303 **רובוגרופ ט.א.ק. בע"מ נ' באום** (נבו 24.03.2020).

[160] *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 2010 E.C.R. I-11063. בפרשה זו נקבע שמידע על אנשים שמקבלים הטבות מקרנות אירופאיות הנו אמנם מידע הנוגע לפעילות בעלת אופי מקצועי ואולם הוא כולל מידע פרטי.

[161] ע"א 1697/11 **א. גוטסמן אדריכלות בע"מ נ' ורדי** (נבו 23.1.2013). פרשה זו עסקה באדריכל שתכנן בית מגורים ללקוח. בעקבות סירובו של הלקוח לפרסם תמונות של הבית באתר האינטרנט של משרדו, האדריכל פרסם הדמיות ממוחשבות של הבית. בית המשפט העליון פסק כי על אף שלא נמסרו פרטים מזהים בנוגע לבעל הבית ולא מופיעים חפציו האישיים, ההדמיות חושפות חללים אישיים בבית המלמדים על אורחות חייו של הלקוח וכן ניתן לקשר בין הפרסום לבין הלקוח. משום שלא התקבלה הסכמתו של הלקוח, בית המשפט העליון קבע כי פרסומן מהווה פגיעה בפרטיות, ראו פס' 15 לפסק דינו של השופט פוגלמן.

שנית, ההבחנה בין העסקי לפרטי אינה ברורה דיה ונשענת על הנחות יסוד שאינן בהכרח מצביעות על תוכן המידע – אם פרטי או עסקי. למשל, כפי שהראנו במקום אחר, לא נשאלה בפסיקת בתי הדין לעבודה השאלה האם הקמת עסק מתחרה הנו עניין פרטי או עסקי, למרות שזו שאלה ראויה בהחלט.[162]

שלישית, בבסיס הדיון המשפטי קיימת הנחה שברגע שמדובר בתיבה מקצועית המידע בה הוא עסקי.[163] ואולם, לאור הטשטוש ההולך והגובר בין מידע פרטי לבין מידע עסקי יתכנו מצבים שבהם גם מידע בתיבה המקצועית יהיה מידע פרטי. מתיו בודי, חוקר אמריקאי מוביל בתחום של עבודה ופרטיות, הצביע על כך שהטשטוש בין סוגי המידע נובע משתי סיבות עיקריות: האחת היא ערבוב בין מידע עסקי למידע פרטי במסגרת אותה פיסת המידע – למשל התכתבות דוא"ל עם קולגה יכולה להיות בנוגע לענייני עבודה אך גם לכלול דיון אישי. השניה היא שהעובדים הופכים להיות חלק כל כך משמעותי מהחברה, כך שהם עצמם, וכל דבר שהם מעבירים בטכנולוגיות שלה, הופך לנכס עבור החברה מבחינת המידע שהיא אוספת והיכולת שלה לנתחו ולעבד נתונים.[164] דבר זה מתחבר גם לדיני קניין רוחני שקובעים כי כל דבר שנעשה על ידי העובד, כולל פטנטים, המצאות, יוזמות וכד', הופך לקניין של המעסיק.[165] בהקשר של איסוף מטה-דאטה בית המשפט העליון בפרשת האגודה לזכויות האזרח בישראל , קבע כי השגת נתוני תקשורת – מידע הנוגע למסר המועבר, כגון נמען, היקף השיחה, מיקום המנוי, כתובת וכדומה, מהווים פגיעה בפרטיות.[166] באופן דומה, בפרשת בן מאיר, קבע בית המשפט העליון כי הסמכת השב"כ לנטר ולעשות שימוש בנתוני תקשורת מובילה לפגיעה חמורה בפרטיות.[167] לאור הלכות אלה נראה כי איסוף ועיבוד מידע, פיזורו ושימורו, גם בתיבה מקצועית או מעורבת או עמדות קצה מקצועיות או מעורבות אחרות, עולים כדי פגיעה בפרטיות.

מסקנה זו מתחזקת נוכח תזכיר חוק הסייבר אשר עושה הבחנה בין "מידע טכנולוגי טהור שניתן להסיק ממנו במישרין או בצירוף מידע אחר, מידע על אדם" כגון נתוני תקשורת או מטה דאטה,[168] לבין "מידע טכנולוגי טהור שלא ניתן להסיק ממנו מסקנות על אדם".[169] לפיכך, בהקשר של סייבר, כאשר הגישה למידע והזיהוי שלו עם נקודת קצה מסוימת או עם כתובת אימייל או עם סרטיפיקט שזוהה דרך מערכות של רשת וירטואלית פרטית (vpn), ומטרתה לזהות אנומליה ברשת תוך איתור אותו אדם שמהווה סכנה למרחב ועל בסיס הגדרת התנהלותו הקודמת

---

[162] ממצא זה וממצאים נוספים שיפורטו בפרק זה הנוגעים ליישום של הלכת איסקוב ענבר על ידי בתי הדין לעבודה נשענים בחלקם על ניתוח שעשינו בעינת אלבין וגיל עומר, "הזכות לפרטיות בעבודה: עיון מחודש בפרשת איסקוב ענבר ויישומה", עתיד להתפרסם בכתב העת ***משפטים*** נג (2023). במאמר זה בחנו את הלכת איסקוב עינבר ואת יישומה על ידי בתי הדין לעבודה בתקופה של עשור מאז אומצה ההלכה (51 פסקי דין).

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

[164] Matthew T. Bodie, Employment as Fiduciary Relationship, 105 GEO. L.J. 819,

[165] ס' 134-131 לחוק הפטנטים, תשכ"ז-1967; ס' 34 לחוק זכות יוצרים, תשס"ח-2007; ראו גם דיון ב- Bodie, שם.

[166] בג"ץ 08/3809 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (נבו 28.5.2012), פס' 7 לפסק דינה של הנשיאה בינייש.

[167] בג"ץ 20/2109 **בן מאיר נ' ראש הממשלה** (נבו 26.4.2020), פס' 35 לפסק דינה של הנשיאה חיות.

[168] לעניין מטה דאטה ופגיעה בפרטיות ראו: Paula Kift & Helen Nissenbaum, *MetaData in Context – An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, 13 ISJLP 333 (2017).

[169] תזכיר חוק הסייבר, לעיל ה"ש 22, בדברי ההסבר.

כנורמאלית מתוך מטרה לזהות את אותה האנומליה, אזי נראה, כי, ככלל, מדובר במידע שניתן להסיק ממנו מסקנות על אדם.

2. דרישת ההסכמה

על אף ההסתייגויות של בית הדין הארצי לעבודה מדרישת ההסכמה הן באיסקוב ענבר והן בקלנסווה,[170] עצם השארת דרישת ההסכמה כחלק מבחינת הפגיעה בפרטיות מחייבת התייחסות אליה על ידי בתי הדין. ואכן, בתי הדין לעבודה נותנים במסגרת פסיקתם משקל רב לדרישת ההסכמה. במקום אחר הראינו כי פסיקת בתי הדין לעבודה פועלת בשלוש דרכים שונות בכל הנוגע לשאלת ההסכמה. דרך אחת כוללת מצבים לגביהם נקבע, כי האיסור על הפגיעה בפרטיות הוא קוגנטי ולא ניתן להתנות עליו בהסכמה כללית של העובד. למשל, כאשר המעסיק ניטר או ביקש לנטר תיבת דוא"ל פרטית של העובד,[171] או גלישה של העובד באינטרנט,[172] או כאשר המעסיק צילם מסך של התכתבות ווטסאפ של העובד.[173] הדרך השניה כוללת מצבים בהם בתי הדין כלל לא נדרשים לשאלת ההסכמה או קבעו כי הסכמת העובד אינה רלוונטית. זאת, כאשר המעקב נעשה לצורך תכלית של הגנה על העסק, סודותיו ונאמנות כלפיו – ביטחון העסק. נציין, כי מקרים אלה נוגדים את הפסיקה בפרשת איסקוב ענבר. הדרך השלישית כוללת את אותם המקרים בהם בתי הדין מזכירים כי ההסכמה צריכה להינתן מראש, מדעת ומרצון חופשי אך עד היום לא נקבעה הלכה ברורה וסדורה בענין הפרשנות שיש לתת לאותה מידת הסכמה נדרשת, ונראה כי בתי הדין לעבודה לא הצליחו לפתח את מבחן ההסכמה במקרים אלו.[174] זה אינו בכדי. הספרות כאמור הצביעה על הקושי הגדול שקיים להשיג הסכמה שכזו בכל הנוגע לטכנולוגיות חדישות ככלל, כולל טכנולוגיות להגנת סייבר, ובהקשר של עבודה בפרט.[175] דוגמא מעניינת לכך היא המקרה של קלנסווה, שם בית הדין הארצי לעבודה קבע שהשימוש בשעון ביומטרי לצורך מעקב אחר שעות עבודה אינו אסור קטגורית, אלא, שהכשרת שימוש כזה, שיש בו משום פגיעה בפרטיות וזכותן של העובדות לאוטונומיה על גופן, יכולה להיעשות באחת מהדרכים הבאות: בחוק או בהסכמה שאינה נוגדת את תקנת הציבור, וככל שהפגיעה נעשית על דרך של הסכמה, נדרשת הסכמה מדעת ומרצון חופשי. בית הדין דן ביסודות ההסכמה, ואולם לא קובע כיצד ניתן לבחון שאכן תושג הסכמה שכזו.[176]

---

[170] פרשת **איסקוב ענבר**, לעיל ה"ש 13, פס' 43-41 לפסק דינה של השופטת נילי ארד; פרשת **קלנסווה**, לעיל ה"ש 14, פס' 118-114 לפסק דינו של השופט אילן איטח.

[171] ראו למשל: פ"ה (אזורי ב"ש) 16-04-40066 **כרמל בידוד בע"מ נ' סולימנוב** (נבו 13.8.2017).

[172] ראו למשל: בעניין **בלקאר**, עלה כי המעסיק ניטר אחר כל פעולה ופעולה שהעובדת עשתה במחשב במשך שנים. בית הדין פסק כי התקנת תוכנה המסוגלת לעקוב אחר פעילותו של עובד במחשב מותנית בהסכמה מפורשת של העובד, וגם אם המעסיק קיבל הסכמה מפורשת, אין בכך כדי להקנות לו רשות לעקוב אחר פעילות פרטית של העובד, הכוללת גלישה לכל אתר. ראו: סע"ש (אזורי ת"א) 60161-06-16 **בלקאר נ' בלקין**, פס' 108-101 לפסק הדין (נבו 27.8.2019); בעניין סע"ש (אזורי ת"א) 79357-01-19 **חי נ' ויצו - הסתדרות עולמית לנשים ציוניות (ע"ר)**, פס' 43-42 לפסק הדין (נבו 11.6.2020), בית הדין מצד אחד קיבל בקשה לעיין במסמכים שהעובד, אשר נטען כנגדו שגלש באתרים פורנוגרפיים ושמר תמונות של תלמידים, שהיו במחשב שלו במהלך העסקתו כחלק מהליך גילוי מסמכים, אך מצד שני לא איפשר עיון בהיסטוריית הגלישה של העובד מכיוון שמדובר בחדירה חמורה למרחב הווירטואלי הפרטי והאינטימי שלו.

[173] ראו למשל: סעש (נצ') 19-12-60673 **נסאר נ' המכללה הארצית להכשרה מקצועית סכנין בע"מ** (נבו 23.8.2020).

[174] אלבין ועומר, לעיל ה"ש 162.

[175] על מגוון קשיים אלה ראו את הדיון בתת פרק ג.1 לעיל, וכן את ההפניות הרלוונטיות.

[176] בית הדין מפרט כי הסכמה שאינה נוגדת את תקנת הציבור, בהקשר זה, הינה הסכמה מדעת ומרצון חופשי, העומדת במבחני תום הלב ובמבחני סעיף 30 לחוק החוזים (חלק כללי), התשל"ג-1973. ראו פרשת **עיריית קלנסווה**, לעיל ה"ש 14, פס' 89 לפסק דינו של השופט אילן איטח.

מכיוון שהתכלית של הגנת סייבר לא נדונה באופן ישיר על ידי בתי הדין לעבודה,[177] אזי כך גם בתי הדין לא עסקו בשאלת ההסכמה בהקשר מסוים זה. ואולם אנו מניחות, כי הכרה בלגיטימיות של תכליות הגנת הסייבר והיותה מעוגנת בחובות משפטיים, תוביל לכך שלא תידרש הסכמתו האישית של העובד לאיסוף המידע הפרטי אודותיו, עיבודו והפצתו לגורמים רלוונטיים במערכת. כפי שנפרט בפרק הבא, אנו סבורות כי אין בכך בהכרח בעיה, שכן לעמדתנו יש לתת משקל מועט מאד למבחן ההסכמה ולשים דגש משמעותי יותר על העקרונות ההלכתיים וכן על עקרונות נוספים שאנו מציעות לאמץ.

לבסוף, בעניין איסקוב ענבר, בית הדין הדגיש את חשיבות המעורבות של ארגוני עובדים בהטמעת העקרונות שנקבעו בהלכה זו (פס' 26 לפסק הדין): "מן הראוי הוא, כי עקרונות אלה יבואו לידי ביטוי בתקנון במקום העבודה, וכי יוסדרו במשותף עם ארגון העובדים או נציגותם במסגרת הסדר קיבוצי או הסכם קיבוצי, בדומה לביטויים בפועל בהסכם הקיבוצי הכללי. **ככל שעיקרים ועקרונות אלה מעוגנים בהסכם הקיבוצי** הרי הם מהווים חלק מחוזה העבודה האישי שבין המעסיק לעובד". בעניין קלנסווה, בית הדין דן, אך לא מכריע, בשאלה האם הסכמה קיבוצית מייתרת את הצורך בהסכמה אישית.[178] עמדתנו היא, כפי שגם נרחיב בהמשך, שהסכמה קיבוצית בכל הנוגע לאיסוף, עיבוד והפצה של מידע פרטי לצורך הגנה על פרטיות המידע, בין השאר בהקשר של הגנת סייבר, הנה נחוצה ומוצדקת.

3. העקרונות ההלכתיים

כאמור, בשתי ההלכות המובילות, אימץ בית הדין הארצי לעבודה שורה של עקרונות הלכתיים, ולאור עמדתנו בכל הנוגע להפחתת השימוש בדרישת ההסכמה, חשיבותם של עקרונות אלה הנה רבה ומשמעותית להגנה על המידע הפרטי שנאסף.

הגנת סייבר כתכלית לגיטימית: כאמור, התכלית של הגנת סייבר לא נדונה באופן ישיר על ידי בתי הדין לעבודה אך אנו סבורות כי התכלית של הגנת סייבר הנה תכלית לגיטימית וראויה לאיסוף מידע, עיבודו וכן הפצתו. הגנת סייבר הנה גם תכלית לגיטימית לשימוש במידע במידה ואכן ישנה סכנה אמיתית לפגיעה במרחב הקיברנטי. לפיכך, ניתן לראות בהגנת סייבר כאגד של תכליות או כאמצעי להגנה על תכליות אלו. גם ה- GDPR קובע כי הגנת סייבר מהווה אינטרס לגיטימי,[179] ובשתי הפרשות שנדונו על ידי בתי הדין לעבודה בישראל נאמרו דברים דומים.[180] ואולם, גם פה, יש לתת את הדעת למספר נקודות מהותיות:

---

[177] במספר מקרים ניתן לראות כי הנחת המוצא היא שתכלית הגנת סייבר הינה לגיטימית. כך למשל, בעניין אודיס, בית הדין פסק כי המעסיק פעל בצורה לגיטימית בכך שהזהיר את העובדים כי ייתכן והמידע שהם בוחרים להעלות במחשביהם יהיה חשוף, אך בית הדין לא בחן במקרה זה את אופן הצגת המידע והאפשרות לפגוע בפרטיות בצורה יותר מידתית ועוד. ראו: **פרשת אודיס**, לעיל ה"ש 157, פס' 79-80 לפסק הדין.

[178] פרשת **עיריית קלנסווה**, לעיל ה"ש 14, פס' 120-121 לפסק דינו של השופט איטח.

[179] ס' 49 ל-GDPR.

[180] בפרשת איסקוב ענבר אמר בית הדין הארצי לעבודה כי המעסיק רשאי לנקוט באמצעים מוגברים של אבטחת המידע שנצבר ברשת, הנקלט בה והיוצא ממנה. במסגרת זו, רשאי המעסיק לפקח על פעילותם של העובדים כדי לוודא שלא יעשו שימוש בלתי מורשה, או בלתי חוקי בכלי העבודה הווירטואלי והמידע המופקד בידם. ראו: פרשת **איסקוב ענבר**, לעיל ה"ש 13, פס' 8 לפסק דינה של השופטת נילי ארד. בפרשת אודיס בית הדין ראה בהתקנת מערכת ניטור לצרכי אבטחת מידע כתכלית לגיטימית, ופסק כי המעסיק פעל בצורה

ראשית, לעיתים יש מקום לעשות הבחנה בין תכליות שונות של הגנת סייבר לצורך חידוד חשיבותה של התכלית. אי אפשר להשוות, למשל, בין הגנה על רשימת לקוחות של מכולת להגנה על הכור הגרעיני, הכולל מידע רב על עובדות ועובדים של הכור, על מידע בטחוני רגיש ושלו תכליות חברתיות, סביבתיות ובטחוניות מהותיות ושלו הסדרה ייחודית במסגרת החוק להסדרת הביטחון. אמנם, לפגיעה בתכליות עסקיות יכולה להיות השלכה רחבה יותר על הציבור הרחב ולעתים גם על הביטחון וגם זאת יש לשקול בהערכת הסיכונים ובהגדרת התכלית בכל מקרה ומקרה.

שנית, גם אם המדובר בתכלית לגיטימית, אזי ישנה חשיבות אמיתית לדאגה כי לא יעשה איסוף, עיבוד, הפצה או שימוש במידע לכל תכלית אחרת. דבר זה נגזר מעיקרון צמידות המטרה. לעיקרון צמידות המטרה – הגבלת השימוש במידע שנמסר למטרה לשמה נמסר – יכול להיות תפקיד מפתח בהגנה על עקרון הלגיטימיות וחידודו. על פי עיקרון זה, ככל שמעסיק מנטר אחר תיבות דוא"ל של עובדיו לצורכי הגנת סייבר, ראוי להגביל את הניטור לצורך זה בלבד, ולאחר מכן את השימוש במידע שנאסף גם למטרה זו בלבד, ולא להתיר עיון כולל בתוכן המידע לכל מטרה אחרת. ואולם, כפי שהראנו במקום אחר, בתי הדין ממעטים ליישם את עיקרון צמידות המטרה.[181]

ואכן ניתן לראות במקרים רבים, וכפי שאירע בעניין איסקוב ענבר, כי מעסיקים ביקשו להשתמש במידע שנאסף למטרה מסוימת, כראיה במסגרת ההליכים בבתי הדין לעבודה.

בהקשר זה, נציין את אמירתו של בית הדין הארצי לעבודה בעניין קלנסווה: "חשוב לעמוד על בהירות בעניין התכלית ולזכור שלעתים התכלית המוצהרת מסתירה תכלית אמיתית אחרת".[182] הבחנה חשובה נוספת היא ההקשר בו טכנולוגיית הסייבר מיושמת. בעניין קלנסווה, בית הדין הארצי קבע כי בבחינת תכלית הפעלת אמצעי מעקב יש לבחון את ההקשר בו האמצעי מיושם. לדוגמא, שימוש בשעון ביומטרי לצרכי רישום שעות עשוי להימצא בלתי לגיטימי אצל מעסיקים מסוימים ועשוי להימצא ראוי כאשר מדובר במעסיקים אחרים, כגון אלה הכפופים לחוק להסדרת הביטחון.[183]

עקרון המידתיות: על פי ההלכות עקרון המידתיות מחייב לבחון: (1) טכנולוגיות חלופיות למעקב (במקרה של סייבר ניטור) הפוגעות במידה הפחותה ביותר בפרטיות העובדים; (2) מהו היחס הראוי בין התועלת שבהגשמת מטרתה הראויה של מדיניות המעקב (ניטור), לבין הנזק והפגיעה בזכויות העובד כתוצאה ממדיניות המעקב (ניטור). למרות קביעות חד משמעיות אלה בדבר העיקרון וחשיבות החלתו, הפסיקה שניתנה עד היום על ידי בתי הדין לעבודה מיעטה לעסוק בשאלת מידתיות הטכנולוגיה.[184] חריגים לכך הנם פסקי הדין קלנסווה,[185] משרד ראש

לגיטימית בכך שהזהיר את העובדים כי ייתכן והמידע שהם בוחרים להעלות במחשביהם יהיה חשוף. ראו: **פרשת אודיס**, לעיל ה"ש 157, פס' 80-79.

[181] אלבין ועומר, לעיל ה"ש 162.

[182] פרשת **עיריית קלנסווה**, לעיל ה"ש 14, פס' 132 לפסק דינו של השופט איטח.

[183] שם, פס' 132.

[184] ראו אלבין ועומר, לעיל ה"ש 162.

[185] **קלנסווה**, לעיל ה"ש 14.

הממשלה,[186] שטטר,[187] וכן פסק דין של בית המשפט המחוזי בעניין עובדי הסיעוד של נכי צה"ל.[188] במקרה הספציפי של הגנת סייבר, בחינת מידתיותה של הטכנולוגיה תאפשר בחינה מדוקדקת של מכשירי הקצה (end points) מהם נאסף המידע, את האפשרות לבחור לרכוש טכנולוגיה שעושה הבחנות בין מרחבים עסקיים לפרטיים בצורה טובה יותר, או להנדס טכנולוגיה באופן המגן טוב יותר על פרטיות המידע של העובדים בעת ההגנה על הסייבר,[189] ועוד. גם שאלת מחיקת המידע וצמצום איסוף המידע חיונית בהקשר זה.[190] התעמקות בהיבטים הטכנולוגיים לצורך יישום מבחן המידתיות יאפשר לבתי הדין לקחת חלק פעיל יותר בבחינת השאלה האם ניתן היה לעצב את הטכנולוגיה בצורה מידתית יותר, באופן שאינו פוגע בצורה נרחבת בזכות למידע פרטי של העובדים, על בחינת רלוונטיות המידע הנאסף לצורך הגנת סייבר וכן על היקפו, תוך איסוף כמות המידע שמספק לצורך השגת המטרה של הגנת סייבר. במילים אחרות, בתי הדין יכולים לוודא, תוך שימוש במינויים של מומחי טכנולוגיה, כי טכנולוגיות הגנת הסייבר אוספות מידע פרטי בצורה המצומצמת ביותר שניתן ומעבדות אותו בדרכים שמגנות בצורה הטובה ביותר על הפרטיות.

נקודה רלוונטית נוספת בהקשר זה, נוגעת לשאלה מיהם הצדדים השלישיים אליהם מופץ המידע. מיישום מבחן המידתיות עולה כי רק הגורמים הרלוונטיים ביותר לצורך הגנה על המרחב הקיברנטי צריכים להיות אלה שמקבלים את המידע על זיהוי אנומליה ברשת, ומתוכם רק חלק קטן, יתכן והמנמ"ר עצמו בלבד יחד עם ממונה הפרטיות בארגון המעסיק,[191] רשאים להסתכל במידע הפרטי שנאסף לצורך זיהוי אותה אנומליה ובחינת מסקנת הטכנולוגיה כי עשוי להיות איום על המרחב. בהקשר זה יש אף להביא בחשבון את תוכן המידע הפרטי המופץ, האם הוא כולל מידע על אנשים נוספים מעבר לעובד (למשל בני משפחתו או חבריו) והאם הפצת מידע זה הנו נחוץ לצורך תכלית הגנת הסייבר.

לבסוף, יש לציין כי מבחן המידתיות מאפשר לבחון את התמונה במלואה, תוך הצמדת האמצעי הטכנולוגי שנבחר למטרה. למשל, בפסק דין של עמותת חברות הסיעוד, קבע בית המשפט המחוזי כי איסוף מידע על מקום הימצאם של העובדים על ידי החתמה סלולרית של נוכחות מבוססת מיקום, אינו פוגע בזכות לפרטיות של העובדים בצורה בלתי מידתית שכן למעסיק ישנה פררוגטיבה לוודא כי העובדים אכן עובדים בשעות עבודתם ונמצאים עם המטופל.[192] כך, במקרה של הגנת סייבר, ברי הוא כי ניטור המידע הפרטי לצורך זיהוי אנומליה ברשת הנו מידתי לצורך זיהוי של פגיעה אפשרית במרחב הקיברנטי.

עיקרון השקיפות ודרישת מדיניות: כאשר המעסיק מבקש להנהיג פרקטיקה הכרוכה בפגיעה בפרטיות, כמו הפעלת אמצעי הגנת סייבר, עיקרון השקיפות והדרישה לקביעת מדיניות מהווים כלים חשובים, שתיאורטית

---

[186] הסתדרות העובדים הכללית, לעיל ה"ש 158.
[187] ע"ע (ארצי) 40711-04-17 **פישר תעשיות פרמצבטיות בערבון מוגבל נ' שטטר** (נבו 4.3.2018).
[188] עת"מ (מינהליים ת"א) 28857-06-17 **עמותת חברות הסיעוד ואח' נ משרד הביטחון** (נבו 1.7.2019).
[189] ראו למשל לעניין זה את הסעד שקבע בית המשפט המחוזי בעניין **עמותת חברות הסיעוד** בכל הנוגע לפגיעה בפרטיות נכי צה"ל, שם.
[190] לדיון מעמיק יותר על שני אלה ראו בפרק הבא.
[191] על ההמלצה להעסיק ממונה פרטיות בארגון ראו: משרד המשפטים "מסמך המלצות - מינוי ממונה הגנה על הפרטיות בארגונים, תפקידיו ותחומי אחריותו" **gov.il** (24.01.2022) https://www.gov.il/he/Departments/publications/reports/dpo_doc_kit.
[192] עניין **עמותת חברות הסיעוד**, לעיל ה"ש 188.

לפחות, מאפשרים לעובדים לכלכל את צעדיהם בהתאם. השקיפות אף חשובה לצורך יצירת סביבת עבודה המגנה על הפרטיות, שכן היא מחייבת את המעסיק לכתוב את המדיניות בצורה ברורה תוך הבאה בחשבון את השיקול של פגיעה בזכות האמורה. זוהי אף דרישה המעוגנת בסעיף 11 לחוק הגנת הפרטיות. אולם, למרות החשיבות התיאורטית של כלים אלה, וכפי שכבר ציינו, מבחינה מעשית יש עמם בעייתיות.[193] בהקשר של עבודה ניתן להניח כי הבעיה חמורה ביתר שאת נוכח פערי הכוח בין הצדדים.

עם זאת, יש להיזהר מלכרוך את עיקרון השקיפות ודרישת המדיניות עם שאלת ההסכמה, דבר שבתי הדין עשו לא אחת.[194] לאור הקשיים שהעלינו ביחס למבחן ההסכמה, אנו סבורות כי אופן בחינת עיקרון השקיפות וההנחה העומדת בבסיסו - כי מתן מידע על מדיניות המעסיק תאפשר לעובד לסרב לה או להביע עמדתו לגביה - אינם מתאימים, ונראה כי מטרתו של מבחן השקיפות - יידוע העובדים בדבר העובדה שנאסף עליהם מידע וסוג המידע שנאסף – צריכה להיבחן בנפרד. קרי, שקיפות נדרשת הן על מנת שהעובד יוכל להבין למה הוא מסכים וכדי שההסכמה תהיה מדעת. ואולם, גם אם המידע הנו שקוף, אין זה אומר בהכרח שהעובד אכן נתן הסכמה שכזו. בנוסף, גם אם מבחן ההסכמה מתייתר, עדיין שקיפות נדרשת על מנת שהעובד יידע לכלכל את צעדיו במרחב הקיברנטי.

נקודה מעניינת נוספת שעולה מהפסיקה נוגעת למקרים בהם בתי הדין קבעו, כי דרישת המדיניות היא דרישה מחייבת שהעדר התקיימותה מביא לפגיעה בפרטיות שהשלכותיה הן שלא ניתן לבצע מעקב וניטור אחר העובדים וכן הימנעות ממתן סעד למעסיק או קביעת סנקציה.[195] אחת מן הסנקציות הללו היא קביעת פיצויים על הפגיעה בזכות לפרטיות. כיום הפיצויים שנקבעים על ידי בתי הדין עשויים, לדעתנו, שלא להרתיע מעסיקים מלפגוע בפרטיות,[196] דבר שיש לשנות. יש לקבוע פיצויים גבוהים מאד שיובילו מעסיקים לשנות את אופן איסוף, עיבוד והפצת המידע בצורה שלא תפגע בפרטיות ותגרום להם לעמוד בדרישות המשפטיות. יצוין כי גם על פי תזכיר חוק הסייבר, קיום מדיניות הגנת סייבר ויידוע העובדים על פעילות זו, מהווים תנאים הכרחיים לכך שפעולה של ארגון למטרת הגנת סייבר לא תחשב כפגיעה בפרטיות.[197]

לסיום פרק זה, נראה כי הדין הקיים בישראל בכל הנוגע להגנת הזכות לפרטיות של מידע פרטי הנאסף על ידי טכנולוגיות במקום העבודה עדיין אינו מספק דיו לצורך הגנה מיטבית על מידע פרטי בהקשר של הגנת סייבר. פררוגטיבת המעסיק להטמיע טכנולוגיות במקום העבודה וכן לאסוף מידע עסקי על עובדות ועובדים, לעבדו ואף להעבירו לצד שלישי מייצרת קשיים אמיתיים. כמו כן, האופן בו דיני הגנת הפרטיות מרסנים את האיסוף והשימוש במידע פרטי לפי שלושת המבחנים של: פגיעה במידע פרטי; דרישת ההסכמה; וכן עמידה בעקרונות ההלכתיים – אף הם אינם מספיקים לעולם העבודה. במסגרת הפרק הצענו שלל דרכים לטייב את העקרונות הקיימים על מנת

---

[193] ראו דיון בעמוד 15 לעיל.
[194] ראו דיון באלבין ועומר, לעיל ה״ש 162.
[195] ראו סע״ש (אזורי ת״א) 18515-02-18 **סעדה נ׳ בלוקשתיל בע״מ** (נבו 13.5.2020).
[196] אלבין ועומר, לעיל ה״ש 162.
[197] ס׳ 64 לתזכיר חוק הסייבר, לעיל ה״ש 22.

שאלו יתנו מענה הולם למקרה של פגיעה במידע פרטי בהקשר של הגנת סייבר. בפרק הבא, אנו מציעות לאמץ כלים משפטיים נוספים מהעולם של דיני העבודה ומהמשפט המשווה כדי לחזק את ההגנה על הזכות. לעמדתנו, יש להשתית את הדין של הגנה על פרטיות עובדים על תיאוריות של דיני עבודה אשר מצדיקות את אימוצם של אותם כלים נוספים.

ה. עבודה והזכות למידע פרטי

בתחילתו של פרק זה נראה כי מבחני הפסיקה שתוארו לעיל עוקבים אחר הרציונאלים של דיני הגנת הזכות לפרטיות, תוך התאמתם, על ידי בתי הדין לעבודה, לעולם העבודה. ואולם, נחדד, כי בדין הקיים חסרים כלים ספציפיים מעולם דיני העבודה, שיטיבו מאד עם ההגנה על זכויות עובדים. אימוצם של כלים מעולם דיני העבודה מוצדק לאור ההגנה הנפרדת והשונה שיש לתת לזכות בהקשר זה, והם יאפשרו, לעמדתנו, הגנה טובה יותר על הזכות למידע פרטי. לעמדתנו, על הכלים המוצעים - הנשענים על הסדרים שאומצו על ידי האיחוד האירופי במסגרת ה- GDPR, כולל עמדתה של קבוצת העבודה בתחום העבודה; מסמכי ארגון העבודה הבינלאומי; וכן הסכם המסגרת שנחתם בין ארגוני העובדים האירופאים ונציגי מעסיקים בנושא דיגיטציה - להתווסף לעקרונות המופעלים על ידי בתי הדין כיום. הדיון שלנו אף יתייחס באופן ספציפי לזכות להגנה על מידע פרטי בהקשר של הגנת סייבר.

1. הגנה על הזכות לפרטיות

דיני הגנת הפרטיות, בארץ ובעולם, נועדו להגן על בני אדם מפני אחרים – רשויות שלטון, אנשים, וחברות – בכל הנוגע למה שמוגדר כפגיעה בזכות לפרטיות, כולל מידע פרטי. המדובר בשורת דינים מעולמות המשפט החוקתי, המנהלי והנזיקי, שנקודת ההנחה בהם היא, שככלל, אין מניעה לבצע פעולות, כולל איסוף עיבוד ופיזור מידע, אלא כאשר אלה אסורות על פי דין. בכל הנוגע למידע, דיני הגנת הפרטיות תוחמים את ההגנה לכזו שחלה על מידע פרטי בלבד, דבר שנאמר מפורשות בחוק יסוד: כבוד האדם וחירותו בו נקבע ש"כל אדם זכאי לפרטיות ולצנעת חייו".[198] סעיף 1 לחוק הגנת הפרטיות קובע כי " לא יפגע אדם בפרטיות של זולתו ללא הסכמתו" וסעיף 2 לחוק הגנת הפרטיות מונה שורה של מצבים העולים כדי פגיעה בפרטיות. גם ה- GDPR האירופי יוצא מאותה נקודת מוצא, כפי שנאמר מפורשות בסעיף 1(1) שבו לפיו הרגולציה מניחה את הכללים הנוגעים להגנה על בני ובנות אדם בכל הנוגע לעיבוד מידע פרטי וכן בכל הנוגע לזרימתו של מידע פרטי.[199]

אמנם, ההגדרה של מידע פרטי הינה רחבה ואינה מסתכמת דווקא במובן של צנעת הפרט,[200] אך לצד תחימת ההגנה למידע פרטי, הן הדין הישראלי והן זה האירופי ממשיכים וקובעים כי ישנם מצבים בהם הפגיעה במידע פרטי אפשרית. זאת, למשל, במידה וניתנה הסכמה על ידי מי שהמידע הפרטי שלו או שלה. סעיף 1 לחוק הגנת הפרטיות

---

[198] ס' 7 לחוק-יסוד: כבוד האדם וחירותו, ס"ח התשנ"ב 150.

[199] Article 1(1) GDPR.

[200] ראו הגדרה ב-GDPR, שם. גם סיווג עניין כקשור ל"צנעת החיים האישיים" אינו חד וחלק. ראו: עניין **ורדי**, לעיל ה"ש 161, בפס' 14 לפסק דינו של השופט פוגלמן.

קובע, כאמור, כי אסור לפגוע בפרטיות הזולת "ללא הסכמתו", כאשר על פי סעיף 3 לחוק הסכמה פירושה: "הסכמה מדעת, במפורש או מכללא". גם ה- GDPR כולל דרישה להסכמה למסירת מידע פרטי. על פי ההגדרה הקבועה בסעיף 4(11) ל- GDPR הסכמה משמעה כל אינדיקציה שניתנת באופן חופשי, מפורש, מיודע, וחד משמעי של מי שהמידע שלו או שלה לעיבוד המידע האישי. כמו כן, סעיף 7 ל- GDPR קובע תנאים להסכמה שכזו. בירנהק הרחיב והסביר מדוע דרישת ההסכמה הנה חשובה בהקשר של פרטיות, שכן היא מתקשרת לתיאוריה של פרטיות כשליטה.[201] שני הדינים – הן הישראלי והן האירופי – מאפשרים פגיעה במידע פרטי כאשר האיסוף, עיבוד ופיזור המידע הפרטי נעשה לתכלית לגיטימית, בצורה מידתית, תוך הקפדה על צמידות המטרה, שקיפות ומבחנים נוספים.[202] זהו הבסיס הרעיוני של דיני הגנת הפרטיות.

בסיס רעיוני זה אומץ בדיני העבודה הישראליים תוך התאמתו להקשר המיוחד של עבודה, התאמה שעל היבטיה נרחיב בהמשך. כפי שתיארנו בפרק הקודם, בפרשת איסקוב ענבר בית הדין הארצי לעבודה קבע שלמעסיק ישנה פררוגטיבה להטמעת טכנולוגיות במקום העבודה כרצונו, כולל אלה המבוססות על איסוף מידע, כאשר האיזון בין פררוגטיבה זו לבין זכותם של העובדים מתחיל בהקשר של מידע פרטי. עמדה זו מניחה את הימצאותו של מידע פרטי רב ברשות המעסיק והיא גם נקודת ההנחה הקיימת בדיני ההגנה על הזכות לפרטיות. נקודת המוצא של הזכות לאסוף ולעבד כל מידע שהוא, ובמצבים מסוימים גם מידע פרטי, לתכליות של העסק, מעצימה מאד את פררוגטיבת המעסיק, שכן היא מעניקה לו כוח רב אל מול העובד. כוח זה הולך וגדל עם שיפור הטכנולוגיות האוספות מידע והשימוש בטכנולוגיות בינה מלאכותית שמגיעות למסקנות תוך הענקת כלי ניהולי נוסף בידי המעסיק.[203] במקרים מסוימים פררוגטיבה זו עוד יותר עוצמתית לאור חיוניותה של הטכנולוגיה כמו במקרה של הגנת הסייבר. המשמעות הנה שמידע פרטי יהיה ברשות המעסיק על רקע כוחו הרב לאסוף אותו, לעבד אותו ולהשתמש בו כמעט ללא מגבלה. הטשטוש ההולך והגובר בין מידע עסקי לבין מידע פרטי מגביר תוצאה בעייתית זו.

נקודת מוצא דומה של פררוגטיבה מעסיקית מצויה בדין הישראלי לגבי התנהלויות רבות נוספות במסגרת מקום העבודה. המעסיק רשאי לשכור לעבודה כל מי שהוא מעוניין בו, הוא יכול לשלם איזה שכר שהוא מסכים לו וכד'.[204] אבל לאור הכוח הרב של המעסיק בהתנהלות השוקית האמורה והפררוגטיבה הניהולית שלו, דיני העבודה קבעו

---

[201] בירנהק, מעקב בעבודה, לעיל ה"ש **שגיאה! מקור ההפניה לא נמצא.**; בירנהק, שליטה והסכמה, לעיל ה"ש 18.

[202] ראו דיון על ה- GDPR האירופאי בהמשך פרק זה.

[203] כיום חלק נכבד מהתוכנות להגנת סייבר מבוססות על בינה מלאכותית המוסיפה אתגר מיוחד להגנה על זכויות, כולל על הזכות למידע פרטי, ככלל ובעולם של דיני עבודה בפרט. אחד האתגרים העיקריים נוגעים להחלטות של תוכנות הבינה המלאכותית שלעיתים מחליפות החלטות מעסיקיות או מנתבות את החלטות המעסיק בדרך מסוימת (כמו למשל בכל הנוגע לחשש להתקפת סייבר). זאת בעוד שידוע כי תוכנות הגנת סייבר אינן מגיעות למסקנות שהן ב-100% נכונות וכי יש בהן הטיות. על האתגרים הללו של דיני העבודה כתבו כמה חוקרים, ראו למשל: Joe Atkinson & Philippa Collins, 'Algorithmic Management and a New Generation of Rights at Work' Institute of Employment Rights (January 2024); Adams-Prassl, Jeremias, Halefom Abraha, Aislinn Kelly-Lyth, Michael 'Six Silberman, and Sangh Rakshita. "Regulating algorithmic management: A blueprint." European Labour Law Journal 14, no. 2 (2023). לאור המורכבות שמתעוררת בהקשר של בינה מלאכותית החלטנו לא להיכנס לדיון עליה לעומק במסגרת מאמר זה.

[204] לעניין הפררוגטיבה של המעסיק ראו: רות בן ישראל, 'זכות היתר (הפררוגטיבה) הניהולית של המעביד: תבנית עיצובה בעידן הבתר-תעשייתי' **עיוני משפט כה(3)** 705; גיא דוידוב, 'הפררוגטיבה של המעביד ודיני החוזים: בעקבות פרשות נהרי וגרינשפן' **משפטים לח(2)** 417; וכן לדיון כללי שלא בהקשר הישראלי Gali Raccabi, 'Abolish The Employer Prerogative, Unleash Work Law' 43 BERKELEY J. EMP. & LAB. L. 79 (2022).

כללים קוגנטיים מאד ברורים שמגבילים אותה. מעסיק אינו יכול לשלם פחות משכר המינימום.[205] אסור לו לשלם שכר לא שווה לעובדת ולעובד.[206] אסור לו לא לקבל לעבודה אדם על בסיס הפליה או מטעמים אסורים נוספים.[207] במקרה של הגנה על הזכות לפרטיות, כללים ברורים שכאלה אינם קיימים בדין הישראלי, למעט מספר מקרים בודדים שקבעו בתי הדין לעבודה.[208] כפי שהראינו בחלק הקודם, מעסיק יכול שיהיה ברשותו מידע פרטי אם העובד הסכים לכך, או אם המידע הפרטי דרוש לתכלית ראויה, כאשר הפגיעה נעשית בכפוף לעקרונות ההלכתיים. אפשרות שכזו לפגוע בזכות עבודה לא קיימת לגבי אף זכות עבודה אחרת. מעסיק לא יכול להתנות על שכר המינימום, בין אם העובד או העובדת הסכימו, ובין אם המדובר בהפחתת שכר לתכלית ראויה, במידה ובשקיפות. אותו הדבר לגבי הפליה. מעסיק אינו רשאי להפלות מכל סיבה שהיא. בפרשת **פלוטקין** בית הדין אף קבע בכל החלטה של מעסיק שעשויה להיות נגועה בהפליה די בכך כדי לפסול את ההחלטה כולה.[209] על מנת להגן על ערך השוויון, אומר בית הדין, ולבסס ולהטמיע בקרב המעסיקים נורמות של שוויון יש למנוע מהם להביא כל שיקול הנגוע בהפליה. אכן, גם בחוק שכר מינימום וגם בחוק שוויון הזדמנויות בעבודה נקבעים חריגים. למשל, סעיף 18(ג) לחוק שכר מינימום קובע חריג שכזה,[210] וסעיף 2(ג) לחוק שוויון הזדמנויות בעבודה קובע כי: "אין רואים הפליה לפי סעיף זה כאשר היא מתחייבת מאפיים או ממהותם של התפקיד או המשרה". גם בחוק שכר שווה לעובדת ולעובד עשה המחוקק איזון בין חובת השוויון מחד לבין פררוגטיבת המעסיק מאידך.[211] ישנם גם חוקים הקובעים שכר מינימום מופחת, כמו למשל תקנות שכר מינימום מותאם,[212] וחוק עבודת נוער.[213] ואולם את כל האיזונים הללו ביצע המחוקק באופן ברור, כאשר נקודת המוצא הנה קוגנטיות שממנה ישנם חריגים, ולא להפך – העדר קוגנטיות למעט במקרים חריגים ביותר.

האם מוצדק לנהוג אחרת כאשר המדובר בזכות לפרטיות? נבחן שאלה זו על פי הסוגיות שהעלנו.

פררוגטיבת איסוף המידע: כאמור, למרות שגם ביתר התחומים של דיני העבודה למעסיק ישנה פררוגטיבה רחבה לניהול העסק, אזי כאשר מדובר בזכויות עבודה, דיני העבודה קבעו כללים קוגנטיים ברורים שמגבילים את אותה הפררוגטיבה. פגיעה בזכות במסגרת מתחם הקוגנטיות אינה אפשרית שכן העובד אינו יכול להסכים לה. מעט מאד הצדקות אחרות מוכרות לפגיעה בזכות. כפי שפירטנו לעיל, זה אינו המקרה בכל הנוגע לזכות לפרטיות. ישנם מקרים בודדים בהם בתי הדין לעבודה קבעו כי לא ניתן לתת הסכמה של העובד לפגיעה בפרטיות, כגון מעקב אחרי

---

[205] ס' 12 לחוק שכר מינימום, תשמ"ז-1987.
[206] ס' 12 לחוק שכר שווה לעובדת ולעובד, תשנ"ו-1996 (להלן: "חוק שכר שווה").
[207] ס' 2 לחוק שוויון הזדמנויות בעבודה, תשמ"ח-1988.
[208] ראו דיון בעמוד 26 לעיל על שלוש ההלכות בהם בתי הדין קבעו כללים קוגנטים להגנה על הפרטיות.
[209] דב"ע נו/3-129 **שרון פלוטקין ואח' נ אחים איזנברג בע"מ** פד"ע לו' תשנ"ט-תש"ס - 1999, 481; וראו גם ע"ע (ארצי) 07/363 **שרונה ארביב נ' פואמיקס בע"מ**.
[210] על פי הסעיף: "השר, לאחר התייעצות עם ארגון עובדים שעם חבריו נמנים רוב העובדים המאורגנים במדינה ועם ארגוני מעבידים שהם, לדעת השר, יציגים ונוגעים בדבר, ובאישור ועדת העבודה והרווחה של הכנסת, רשאי לקבוע הוראות משלימות לענין חישוב שכר מינימום יומי ושכר מינימום לשעה, ויכול שיקבע לענין זה הוראות השונות מהאמור בחוק זה".
[211] ס' 6 לחוק שכר שווה, לעיל ה"ש 206.
[212] תקנות שכר מינימום (שכר מותאם לעובד עם מוגבלות בעל יכולת עבודה מופחתת), תשס"ב-2002.
[213] חוק עבודת הנוער, תשי"ג-1953.

תיבת דוא"ל פרטית. ואולם, ההגנה הקוגנטית הנה מועטה ומצויה בשוליים של ההסדרים הנוגעים לפרטיות במקום העבודה. זוהי התאמה קלה של דיני הגנת הפרטיות להקשר של עבודה, ולעמדתנו היא אינה מספקת.

שאלת ההסכמה: שאלת העדרה של הגנה קוגנטית חזקה יותר על הזכות לפרטיות מזו שקיימת כיום בדין, כרוכה אף עם הדיון בשאלת ההסכמה. זאת הואיל וישנה הבחנה ברורה בין הזכות לפרטיות לבין זכויות העבודה האחרות, שלגבי האחרונות העובד אינו יכול לתת הסכמה לפגיעה בהן. ניתן לטעון, שבניגוד לזכויות העבודה האחרות שבהן ההסכמה היא חיצונית לזכות, או במילים אחרות הזכות קיימת עם ובלי קשר לשאלת ההסכמה, במקרה של הזכות לפרטיות שאלת ההסכמה אינהרנטית לקיומה של הזכות. זאת הואיל ואין פגיעה בפרטיות במקרה שבו האדם מוסר את המידע עליו לאחר באופן רצוני, מיודע ושלם. אנו סבורות כי אין בהבחנה זו כדי להצדיק את המשקל שניתן לשאלת ההסכמה בדין הישראלי בכל הנוגע לפגיעה בפרטיות בהקשר של עבודה. זאת גם בהנתן ההתאמות שביצע בית הדין להקשר של עבודה תוך כדי שקבע שהסכמה צריכה להיות מדעת, מראש ומרצון חופשי. כפי שהראינו בניתוח בפרק הקודם, לדרישת ההסכמה עדיין ניתן משקל רב על ידי בתי הדין לעבודה ולא נוצרה דוקטרינה שבוחנת לעומק מה הכוונה בהסכמה מדעת, מראש ומרצון חופשי ובמה היא שונה מדרישת ההסכמה הקבועה בחוק הגנת הפרטיות שקובע כי עליה להיות מדעת, במפורש או מכללא. המשקל הרב שניתן לשאלה ההסכמה בפסיקת בית הדין הארצי לעבודה אף סותר דינים אחרים בעולם, בעיקר את זה האירופי. בכל הנוגע ליישום ה- GDPR להקשר של עבודה ניתנה התייחסות מיוחדת על ידי קבוצת העבודה בנושא אבטחת מידע, ה- data protection working party, (להלן: "קבוצת העבודה"). נייר הדעה של הקבוצה משנת 2017 קבע בצורה מפורשת כי הסכמה כמעט ואינה יכולה לשמש כבסיס משפטי לצורך עיבוד מידע בעבודה, אלא אם עובדים יכולים לסרב לעיבוד ומסירת המידע מבלי שתהיה לכך תוצאה שלילית עליהם.[214] עוד קובע הנייר כי נדירים המצבים בהם עובדים יוכלו לתת הסכמה חופשית מלאה, לסרב בצורה חופשית או לשנות את דעתם, וזאת בשל המהות של מערכת יחסי עובד מעסיק. בנוסף, הדגיש נייר הדעה כי עובדים צריכים לקבל מידע אפקטיבי ומובן לגבי הניטור שנעשה עליהם ושכל העברה של מידע על עובדים צריך להיעשות כאשר ניתנת מידה מתאימה של הגנה על מידע. מכיוון שרק לעיתים נדירות יוכלו עובדים לקבל החלטה אוטונומית שמשקפת את רצונם החופשי, קובע הנייר כי למעט במקרים חריגים ביותר, מעסיקים יצטרכו להשתמש בתשתית משפטית שונה מזו של הסכמה, על מנת להמעיט את הפגיעה בזכות לפרטיות. אכן, גם אנחנו סבורות כי אין לתת משקל משמעותי לשאלת ההסכמה בהקשר של עבודה, במיוחד בכל הנוגע להגנת סייבר, וכי המשקל צריך לעבור להגנות אחרות. יחד עם זאת, אנו סבורות, שבמצב בו המשפט הישראלי ימשיך לשים דגש על שאלת ההסכמה, הרי שישנן כמה נקודות חשובות שיש לתת עליהן את הדעת. ראשית, שאלה חשובה שעולה נוגעת לשימוש במידע לצורך מטרה אחרת, כגון זה שנעשה באיסקוב ענבר. על פי הטקסונומיה של סולוב שהצגנו בחלק א של המאמר, שימוש שכזה עולה כדי פגיעה בפרטיות, שכן לא ניתנה עבורו הסכמה של העובד. כאן עמדתנו הנה חד משמעית, והיא כי אין לאפשר כל שימוש אחר במידע שנאסף לצורך התכלית של הגנת סייבר. דבר

[214] Working Party, לעיל ה"ש 26.

זה עולה בבירור ממבחן צמידות המטרה שנקבע בפרשת איסקוב ענבר ואף מעוגן בסעיפים 2() ו-8(ב) לחוק הגנת הפרטיות אשר יישומו מתחייב במקרה של הגנת סייבר. אנו אף סבורות שיש לקבוע פיצויים משמעותיים במידה ועיקרון קוגנטי זה מופר.

שנית, אנו בדעה כי יתכן ובכל הנוגע למבחן ההסכמה על בתי הדין לפעול אחרת לפי זהות המעסיקים וחובותיהם המשפטיות בנוגע להגנת סייבר. זאת על פי התכליות השונות של הגנת הסייבר וכן לאור ההבחנה בין גופים ציבוריים ופרטיים שונים, וכן תוך מתן משקל שונה לסכנות השונות, כפי שפירטנו בחלק ג במאמר. במקרה בו מדובר במעסיק פרטי, קטן, שמבצע הגנת סייבר למטרה עסקית בלבד, יתכן ומוצדק יותר לדרוש הסכמה של עובד לאסוף את המידע הפרטי אודותיו לצורך הגנת סייבר. זאת, בניגוד למקרה שבו מדובר במעסיק ציבורי עם מידת סיכון גבוהה מאד לשיבוש מערכות שעשוי להוות סיכון ביטחוני וחברתי משמעותי. במקרה שכזה ייתכן כי הסכמת העובד לא צריכה להדרש.

שלישית, וכפי שנרחיב עוד בהמשך, אנו סבורות כי גם אם תכלית הגנת הסייבר הנה לגיטימית, ההבחנות בפסיקה בין המרחב הפרטי האישי לבין המרחב העסקי ציבורי (כפי שנעשו לגבי הבעלות על הטכנולוגיה, תיבות דוא״ל ולגבי הצבת מצלמות) רלוונטית מאד. יש לאסור ולהחיל דרישה קוגנטית על ניטור של האזורים הפרטיים – תיבה פרטית, קבוצת ווטסאפ שאינה מוקמת על ידי המעסיק, המחשב הפרטי של העובד והטלפון הסלולרי שלו. בנוסף, יש להשתמש בטכנולוגיות שעושות הפרדה טובה יותר בין מידע עסקי למידע פרטי ולוודא כי הגנת הסייבר נעשית, ככל הניתן, על מידע עסקי בלבד. בהקשר זה אתגר אמיתי מצוי בכל הנוגע למידע מעורב – עסקי ופרטי – לאור הטשטוש ההולך וגובר ביניהם, ואולם יצירת המרחבים השונים תקל במעט את ההתמודדות עם אתגר זה, גם אם לא באופן מוחלט.

העקרונות ההלכתיים: כאמור, בית הדין הארצי לעבודה קבע שורה של עקרונות שיחולו, גם במקרה בו ניתנה הסכמה, שירסנו את המעסיק מפגיעה בזכות העובד לפרטיות. גם בכך אימץ בית הדין את עמדת דיני הגנת הפרטיות הקובעים עקרונות שכאלה לפגיעה במידע פרטי גם אם ניתנת הסכמה.

גם ה- GDPR, שנכנס לתוקף בשנת 2018, קובע שורה של עקרונות דומים לאלה הקיימים בדין הישראלי, כגון שקיפות ביחס לעיבוד המידע ושהמידע רלוונטי למטרה לשמה נאסף,[215] מידתיות וצמצום המידע הנאסף,[216] תנאים להסכמתו של מושא המידע לעיבוד מידע פרטי שלו,[217] זכות גישה למידע האישי וקבלת מידע,[218] זכות לתקן מידע לא מדויק,[219] וכן חובה למחיקת המידע.[220] לפי ה-GDPR, מושאי המידע נהנים מזכויות נוספות מעבר לאלה שהדין

[215] ס׳ 5(1), 12 ו-13 ל- GDPR.
[216] ס׳ 5(1)(ג) ל- GDPR.
[217] הגדרת ״הסכמה״ בס׳ 4, וכן ס׳ 7 ל-GDPR.
[218] ס׳ 15 ל-GDPR.
[219] ס׳ 16 ל-GDPR.
[220] ס׳ 65 למבוא וכן ס׳ 17(1)(א) ל- GDPR שקובע כי מידע שאינו נדרש יותר לצורך המטרה שלשמה נאסף יימחק.

הישראלי אימץ, כגון זכות לחזור בך מההסכמה,[221] והזכות למחוק את המידע האישי (הזכות להישכח).[222] ה-GDPR לא רק קובע מגבלות על איסוף מידע פרטי, אלא הוא אף קובע הגנה על מידע פרטי, הכולל בין השאר מידע על עובדים המצוי ביד המעסיק.[223] כפי שציינו קודם לכן, פסיקה של בית הדין האירופי לזכויות אדם קבעה כי ההגנה על מידע פרטי כוללת, במקרים מסוימים, גם פעילות שלה אופי עסקי.[224]

ככלל, העקרונות הרחבים יותר שאומצו ב- GDPR מאפשרים הגנה טובה יותר על המידע, כולל על המידע של עובדות ועובדים, וכפי שציינו קודם לכן, ההתייחסות המיוחדת להקשר של עבודה הולידה התאמות טובות לספירה זו, מעבר לאלה הקיימות בדין הישראלי. דבר זה מאפיין גם את מסמך העקרונות של ארגון העבודה הבינלאומי.

כך, למשל, ה- GDPR קובע את עקרון האחריותיות (accountability), לפיו הגורם השולט במידע הוא האחראי ועליו להיות בעל יכולת להדגים ציות עם שאר העקרונות לעיבוד מידע.[225] גישה זו באה לידי ביטוי גם בניירות המדיניות של הרשות להגנת הפרטיות ומערך הסייבר, תוך מתן דגש לכך שהאחריות מוטלת על הארגונים (ולא על הרגולטור) ליצירת מנגנונים לניהול ולהגנה על מידע, כגון מינוי ממונה להגנה על מידע בארגון.[226] לאור עיקרון האחריותיות, מכיוון שהארגונים נמצאים בעמדה של כוח מבחינת ניהול המידע, יש להם אחריות ביחס לצעדים שננקטים על ידם להגנה על מידע האישי. אחריות זו כוללת, במידה מסוימת, שקיפות ויכולת להראות אילו צעדים ננקטו ומהן ההחלטות שהובילו להם.

סעיף 49 להוראות המבוא ל-GDPR, קובע כי עיבוד מידע לצרכי אבטחת מידע, המוגבל והפרופורציונאלי למידה הנדרשת לכך, מהווה אינטרס לגיטימי של הגורם השולט במידע. סעיף 88 ל-GDPR קובע כי המדינות החברות, באמצעות חוק או הסכם קיבוצי, יכולות לקבוע כללים ספציפיים לוודא את ההגנה על זכויות וחופשים של עובדים שעשויים להיפגע כתוצאה מהעיבוד של מידע פרטי. על כללים אלה לכלול אמצעים מותאמים וייחודיים כדי להגן על כבודו של נשוא המידע.[227] גם סעיף 155 להוראות המבוא ל-GDPR משאיר פתח לחקיקה או הסכמים ספציפיים הנוגעים לעיבוד מידע אישי של עובדים, ובפרט ביחס לתנאים על-פיהם ניתן לעבד מידע אישי בקונטקסט של יחסי עבודה בהתבסס על הסכמת העובד, ובהתייחס להקשרים שונים כגון גיוס עובדים, ביצוע הסכם העבודה, ניהול, שוויון בעובדה וסיום יחסי עבודה. ההתייחסות אינה בהכרח לאבטחת מידע, אלא למתן הסכמה לכל טכנולוגיה בעבודה שנוגעת לעיבוד מידע אישי. לפי נייר הדעה, על מעסיקים: א. לוודא כי המידע מעובד למטרה ספציפית ולגיטימית, כאשר מטרות אלה צריכות להיות הכרחיות ומידתיות; ב. להביא בחשבון את העיקרון של מגבלה

---

[221] ס' 7(3) ל- GDPR.

[222] ס' 17 ל-GDPR. יצוין כי בינואר 2022 הוגשה הצעת חוק הנועדה לעגן בחקיקה את זכותו של אדם לדרוש מחיקת מידע אודותיו במאגר. ראו: הצעת חוק הגנת הפרטיות (תיקון- מחיקה ממאגרי מידע), התשפ"ג- 2022, ה"ח פ/25/549.

[223] ס' 2-4, 32-39 ל- GDPR.

[224] Cases 92/09 & 93/09, **Volker und Markus Schecke GbR** & **Hartmut Eifert v. Land Hessen** E.C.R. 1-11063 (2010).

[225] ס' 5(2) ל-GDPR.

[226] "מסמך המלצות, לעיל ה"ש 191; משרד המשפטים "פיתוח מאובטח - עבודת מנהל הגנת סייבר CISO עם גופי הפיתוח בארגון" **gov.il** (27.04.2020) https://www.gov.il/he/departments/general/securedevelopment.

[227] וראו פרשנות של סעיף זה בפסק דין שניתן על ידי ה- CJEU, Case C-34/21, *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums*, 30 March 2023, ECLI:EU:C:2023:270.: EU's Court of Justice

לגיטימית על איסוף ועיבוד המידע תוך וידוא כי המידע אכן נדרש ומותאם למטרה הלגיטימית ואימוץ עקרון צמצום המידע הנאסף; ג. להחיל את עקרונות המידתיות והשיוריות בלי קשר ללגיטימיות המטרה; ד. להיות שקופים עם העובדים לגבי מטרות איסוף המידע, לאפשר להם גישה למידע שנאסף אודותם, לשמור על המידע מדויק ולא לשמור אותו לתקופה שעולה על הנדרש; ה. לנקוט בכל האמצעים הנדרשים כדי להגן על המידע.[228]

נייר הדעה אף התייחס לנושא השקיפות וקבע, כי עובדים צריכים להיות מודעים לכל ניטור מידע שמתרחש, בין אם הוא אירעי או קבוע, ובין אם הוא נלווה לפעילות אחרת של הארגון או לאו. צריך להביא לידיעת העובדים את מטרת הניטור ואת הנסיבות וכן לתת להם מידע כיצד ניתן להימנע ממצבים בהם המידע שלהם נתפס על ידי הארגון. עוד המליצה קבוצת העבודה על שיתוף עובדים בתהליך קביעת הכללים והמדיניות לגבי ניטור המידע בהנתן ולניטור מידע ישנו פוטנציאל להפר את זכויות הפרטיות של העובדים.[229]

בהסכם מיוני 2020 התייחסו השותפים האירופאים ליחסי העבודה לנושא ניטור המידע והצורך בשמירה על כבודו של העובד. הם הפנו לסעיף 88 של ה- GDPR והציעו מספר אמצעים שניתן לאמץ על מנת להגן על העובדים.[230] ראשית, הוצע לאפשר לנציגי העובדים להתייחס לנושאים הקשורים למידע, להגנה על פרטיות, לשאלות של הסכמה ולמעקב. שנית, לדאוג תמיד לקשור את איסוף המידע למטרה קונקרטית ושקופה. שלישית, לתת כלים בידי נציגי העובדים כדי שיוכלו למלא את תפקידם בעולם הדיגיטלי, כולל קביעת מדיניות משותפת ועוד. ההסכם אף כולל התייחסות למערכות של בינה מלאכותית ולעקרון של שליטה אנושית (human in command).[231]

רוח דומה מצויה גם בעקרונות ארגון העבודה הבינלאומי.[232] העקרונות המנחים של ארגון העבודה הבינלאומי נקבעו עוד לפני הפיתוחים הטכנולוגיים המשמעותיים של שני העשורים האחרונים וכניסתם לעולם העבודה, ביניהם בינה מלאכותית, ואולם הם עדיין משמשים כמקור נורמטיבי חשוב להגנה על מידע בהקשר של עבודה.[233] בין השאר, קובע המסמך את חשיבות רעיון צמידות המטרה בקובעו כי יש להשתמש במידע פרטי רק למטרה שלשמה הוא נאסף מלכתחילה,[234] וכי אין לעשות שימוש במידע פרטי שנאסף על ידי אמצעים טכניים או ארגוניים על מנת לוודא שימוש נכון במערכות אוטומטיות לניהול התנהגותם של העובדים.[235] עוד קובע המסמך את עקרון צמצום המידע,[236] ואת המטרה של שיפור הדרכים בהם ניתן להגן על פרטיות המידע של העובדים.[237] המסמך קובע את עיקרון השקיפות בפני עובדים ונציגיהם,[238] וכן את עיקרון השיתוף של עובדים ושל נציגיהם בעיצוב מדיניות הפרטיות במקום העבודה באופן מותאם לעקרונות.[239] הוראה חשובה ביותר במסמך העקרונות היא כי הזכות

---

[228] Working Party, לעיל ה"ש 26.
[229] שם.
[230] הסכם המסגרת של השותפים האירופאיים ליחסי עבודה קיבוציים, לעיל ה"ש 27, בעמ' 12.
[231] שם, 11.
[232] ס' 5.6-5.5, Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17.
[233] ראו למשל את ההפניה הנרחבת שעושה הנדריקס למסמך זה בדו"ח החדש של ארגון העבודה הבינלאומי, Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17.
[234] ס' 5.2, Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17.
[235] שם, בס' 5.4.
[236] שם, בס' 5(7)(a).
[237] שם, בס' 5(7)(b).
[238] שם, בס' 5(8).
[239] שם, בס' 5.11.

לפרטיות של העובדים הנה קוגנטית ואינה ניתנת לויתור.[240] לאחרונה הוציא ארגון העבודה הבינלאומי מסמך נוסף של עקרונות להגנה על מידע פרטי שכן עוסק, בין השאר, בבינה מלאכותית, ומדגיש עקרונות שלא נמצאו במסמך העקרונות משנת 1997, כגון אחריותיות וממשל על המידע הפרטי, וכן כללים בנוגע להחלטות אוטומטיות.[241]

נקודה נוספת שמצויה במסמכים נוגעת לזהות האנשים בארגון שיכולים לגשת למידע הפרטי שנאסף. לפי מסמך העקרונות של ארגון העבודה הבינלאומי מידע פרטי יכול להיות זמין אך ורק לאנשים מסוימים שלהם סמכות מפורשת מהמעסיק, וזאת רק לצורך שימוש במידע הפרטי למשימות מוגדרות.[242]

מסמכים אלה מלמדים אותנו כי בהקשר של עבודה עקרונות רבים קיימים על מנת לדאוג להגנה על הפרטיות של העובדים, וכי בכולם ישנה התייחסות משמעותית לחשיבות שילובם של ארגוני עובדים, או נציגות אחרת של העובדים, בתהליך. בכך הם משקפים התאמה טובה יותר להקשר של יחסי עבודה בהשוואה לדין הישראלי. על אף שהמסמכים האמורים לא עוסקים באופן ייחודי בהגנת סייבר, אפשר ללמוד מהם על האופן בו יש להתמודד עם האתגרים שמציבה ההגנה על הסייבר בתחום העבודה. ההתאמות של הדין האירופי וכן של מסמך העקרונות של ארגון העבודה הבינלאומי משמעותיים יותר מאלה של הדין הישראלי להגנה על הזכות של העובדים לפרטיות, אך אין בהן די. אנו בעמדה כי יש לאמץ כללים מסוימים של עבודה אשר יתנו מענה לפררוגטיבה המועצמת והכמעט בלתי מוגבלת של המעסיק להטמעת טכנולוגיות. זאת, הן על ידי קביעת כללים קוגנטיים ברורים וחד משמעיים, שימנעו מתן אפשרות להסכים למסירת מידע פרטי כאשר המדובר בכלל קוגנטי, והן על ידי מתן משקל משמעותי לכוח הקיבוצי. אנו אף סבורות כי במקביל יש לאמץ כללים נוספים מה- GDPR על מנת לתת כוח גדול יותר בידי העובדים להגן על המידע שלהם. הצעתנו זו אינה סותרת את דיני הגנת הזכות לפרטיות אלא רק מטייבת אותה ומוסיפה לה הגנות משפטיות שלא מצויות במידה מספקת כיום במסגרת הדין הקיים.

2. הגנת פרטיות בעבודה

במבוא למאמר זה ציינו כי אחת הנקודות החשובות שעולות מהדיון האקדמי סביב הזכות להגנה על מידע פרטי, ואף מצויה בלב הדוקטרינה המשפטית, נוגעת להבחנה בין הקשרים שונים של פרטיות, וביניהם ההקשר של יחסי עובד-מעסיק. ייחודיותו של הקשר זה עולה גם מעמדת בתי הדין לעבודה שמצאו לנכון להתאים את דיני הגנת הפרטיות לדיני העבודה (גם אם זה לא נעשה בצורה מספקת), וכן בדין האירופאי, כולל עמדת קבוצת העבודה והוראות סעיף 88 ל-GDPR. בנוסף, גם ארגון העבודה הבינלאומי מצא לנכון לתת דגשים מסוימים להגנה על הזכות בהקשר הייחודי של עבודה.

---

[240] שם, בס' 5.13.
[241] ס' 3.9, 4.2, Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17.
[242] שם, ס' 10.6.

זה אינו בכדי. הנחת המוצא של דיני העבודה היא פערי כוחות הקיימים בין הצדדים ליחסי עבודה לאור התלות והכפיפות של העובד למעסיק שלו, המצדיקים את קיומם של ארגוני עובדים וכן התערבות רגולטורית בתוכנו של חוזה העבודה.[243] פעולה קיבוצית תאזן את פערי המיקוח ועל כן הסכמה קיבוצית הנה רצויה. פערי המיקוח אף מצדיקים התערבות של הרגולטור ושל בתי הדין לעבודה.[244] הצדקה נוספת להתערבות בתוכנו של חוזה העבודה מצויה בנקודת ההנחה, שלאור העסקה הבסיסית בדיני העבודה בה עבודה נמכרת תמורת כסף, ניתן יהיה להתייחס לעובד כאל כל מצרך אחר.[245] לכן, על מנת לוודא שהיחס כלפי בן אנוש לא יהיה כאל מצרך רגיל, אלא יחס המשמר ערכים וצרכים אנושיים בסיסיים, ישנה הצדקה להתערבות בתוכנו של החוזה ולקביעת כללים קוגנטיים.[246]

הספרות של דיני העבודה אף הצדיקה התערבות בחופש החוזים של הצדדים על בסיס הטענה של אוטונומיה. המחקר הראה, כי המעבר מהסדרה משפטית שנעשתה בתקופת העבדות (או בתקופה של חוקי המשרת והאדון) להסדרה חוזית של מערכת יחסי העבודה במהלך המאה ה-19 הוא לא זה שאפשר את מה שמכונה "עבודה חופשית", דהיינו עבודה שלא כוללת כבילה ותלות גדולה במעסיק.[247] במציאות הכלכלית והחברתית של אותה המאה, עצם השינוי המשפטי מהגדרת העסקה בה עבודה נמכרת תמורת כסף כעבדות או אדון ומשרת לחוזה לא השפיעה כלל על מצבם של העובדים. דווקא חוקי המגן המתערבים בחופש החוזים בין הצדדים, הם שאפשרו יותר חופש לעובדים, וכתוצאה מכך – מימוש הרעיון של עבודה חופשית בניגוד לעבודה בכפייה. לבסוף, הספרות מצדיקה התערבות בחופש החוזים של הצדדים גם מטעמים פטרנליסטים ומטעמים של אינטרסים ציבוריים וכן אינטרסים מסדר שני. כך, גם אם העובד רוצה להסכים מסיבותיו שלו להסדר מסוים (למשל תמורת שכר גבוה יותר), עדיין ישנן הצדקות לפגיעה בחופש החוזים ולמנוע הסכמות בעניינים מעין אלה.[248] פה יש למתוח קו עדין בין הסדר שהוא קוגנטי שאין להתנות עליו כלל לבין הסדרים אחרים שיתכן וניתן יהיה לגבש בהם הסכמה.

תובנות תיאורטיות אלה מדיני העבודה הובילו חוקרים לטעון כנגד חלק מהעקרונות המאומצים בדיני הגנת הזכות לפרטיות. הדוגמא הבולטת ביותר לכך היא מבחן ההסכמה. הנדריקס הסביר, כי לאור העובדה שהנחת המוצא בדיני עבודה היא שיש מערכת יחסים של תלות וכפיפות בין העובד לבין המעסיק, אזי המסגרת המשפטית הקיימת, ובתוכה ההכרה בפררוגטיבה המעסיקית המעוגנת בתוך חוזה העבודה בין הצדדים ליחסי העבודה, מאפשרת למעסיק להשתמש בכוח אל מול העובדים. במובן זה הוא אומר, כי המשמעות של להיות מועסק הנה שהאוטונומיה האישית מוגבלת במידה מסוימת תוך מתן אפשרות למעסיק "לשלוט" בעובדים ואף לתת להם אפשרות לומר את דברם לגבי התנהגותם.[249] כך, בעוד הזכות לפרטיות כוללת את "הזכות שיניחו לך" אזי שבהקשר של עבודה יחסי

---

[243] Davis & Fruend, Labour and the Law; GUY DAVIDOV, A PURPOSIVE APPROACH TO LABOUR LAW, 52 (Oxford: Oxford University Press (2016).

[244] שם.

[245] ILO, *Declaration concerning the aims and purposes of the International Labour Organisation* (10 May 1944) [Declaration of Philadelphia]; HUGE COLLINS, EMPLOYMENT LAW, 26-3 (Oxford: Oxford University Press, 2003).

[246] David M. Beatty, *Labour is Not a Commodity,* in STUDIES IN CONTRACT LAW (Barry J. Reiter and John Swan eds., ; שם 1980), 313.

[247] ROBERT J STEINFELD, COERCION, CONTRACT, AND FREE LABOR IN THE NINETEENTH CENTURY 1-28 (2001).

[248] Guy Davidov, *Nonwaivability in Labour Law* 26-20 Oxford Journal of Legal Studies Hebrew University of Jerusalem Legal Research Paper) (2020).

[249] Hendricks, **Privacy 4.0 at Work**, לעיל ה"ש 1, 154.

העבודה מקנים למעסיק את הזכות שלא "להניח לעובדיהם".[250] ההתייחסות לזכות לפרטיות צריכה להיעשות מתוך נקודת מוצא זו. הנדריקס מוסיף ואומר, שגם זכויות ואינטרסים של גורמים מחוץ למערכת יחסי העבודה מצמצמים עוד את מרחב התמרון בין המעסיק לבין העובדים בכל הנוגע להגנה על הפרטיות.[251] למשל, הזכות והאינטרס של לקוחות ושל צדדים שלישיים נוספים שהמידע שלהם יהיה מוגן, כמו גם אינטרסים רחבים יותר (למשל הגנת סייבר בשל חשש לסכנה ביטחונית, סביבתית או חברתית). לאור זאת, בהקשר של עבודה, נקודת המוצא היא כי ניתן לפגוע בפרטיותם של העובדים לצורך השגת תכליות אלה, ולכן, עמדתו של הנדריקס הנה כי אין לתת משקל להסכמת העובד, וכי תפקידו של המשפט הוא בעיקר לבחון שאלות של לגיטימיות, מידתיות ושקיפות.[252] כתיבה נוספת בדיני העבודה חידדה את חשיבותם של כללים קוגנטיים גם בהקשר של פרטיות, ואף את הערך הרב שיש במעורבותם של ארגוני עובדים להגן על זכות זו של העובדים.[253]

סיבה נוספת לייחד את ההגנה על הפרטיות בהקשר של עבודה ביחס להקשרים אחרים בהם הזכות מוגנת, נובעת מהשוני הקיים בין יחסי עובד-מעסיק לבין צרכן-נותן שירות. המודל של צרכן אל מול נותן השירות הוא שעומד בבסיסם של חלק מדיני ההגנה על מידע פרטי, כמו ה- GDPR, והוא מניח בבסיסו אדם אוטונומי שיכול לעשות את בחירותיו כרצונו, ובעיקר, אדם שאין לו מחויבות כלשהי כלפי נותן השירות.[254] בניגוד לצרכן, לעובד ישנן חובות כלפי המעסיק כגון חובת נאמנות,[255] והחובה לפעול על פי הנחיותיו לאור הפררוגטיבה הרבה שיש למעסיק. מדובר בהרבה יותר מיחסים שבהם לאחד יש כוח גדול יותר מלאחר, אלא בפסיפס של דינים בהם ישנם לעובד חובות אל מול המעסיק ולמעסיק פררוגטיבה, בדומה לשל מדינה, לנהל את העובד.[256] שוני זה בין מערכות היחסים גם משתקף בדין הכללי אשר מבצע רגולציה הרבה יותר מהודקת על שוק העבודה בנוגע לשלל זכויות ואינו מבצע רגולציה זהה על שוק הצרכנים. הדוגמא המובהקת ביותר לכך היא איסור האפליה הקיימת בדיני עבודה שאינו חל על צרכנים.[257]

אם כן, התיאוריה של עבודה להגנת הפרטיות תצא מנקודת מוצא, כי יש להגביל את הפררוגטיבה של המעסיק לשלב כל טכנולוגיה שהוא מעוניין בה במקום העבודה ולאסוף מידע על עובדים, וזאת על ידי שורה של כללים שישיגו תוצאה זו תוך הכרה בחשיבות של כללים קוגנטיים, וכן מתן כוח קיבוצי ואישי לעובדות ועובדים. אימוץ תיאוריה של דיני עבודה תעודד את פיתוחם של ארבעה אמצעים שונים שאנו נדון בהם יותר לעומק בהקשר של סייבר: 1. הגדלת ההגנה הקוגנטית על הזכות למידע פרטי, תוך קביעת איסורים מוחלטים על מצבים שבהם הסכמה לא תאפשר גישה למידע פרטי לצורך הגנת סייבר; 2. הכרה בחשיבותם של ארגוני עובדים כמי שיכולים

---

[250] שם.
[251] שם.
[252] שם.
[253] Emanuele Dagnino and Ilaria Armaroli *A Seat at the Table: Negotiating Data Processing in the Workplace. A National Case Study and Comparative Insights* 41 Comp. Lab. L. & Pol'y J. 147 (2019); see also discussion in Abraha Halefom *A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace* 12(4) International Data Privacy Law 276 (2022).
[254] Michele Molè, *Lost in Translation* (הרצאה בכנס Privacy@Work in an Era of New Technologies, ירושלים, 30.5.2023-31).
[255] דוידוב, לעיל ה"ש 248.
[256] על הדמיון בין הכוח של המעסיק לנהל את העובד לכוח של המדינה ראו: PAUL DAVIES AND MARK R FREEDLAND, KAHN-FREUND'S LABOUR AND THE LAW 14-26 (1983).
[257] Katharine Bartlett & Mitu Gulati, *Discrimination by Customers*, 102 Iowa L. Rev. 223 (2016).

לתת הגנה טובה לעובדים בהקשר של הגנת סייבר, וקביעת דרישה מהותית לקבלת הסכמה קיבוצית – בין אם של ארגון העובדים או של נציגות העובדים – להטמעת טכנולוגיות סייבר הנרכשות ועוברות לשימוש במקום העבודה ולקביעה משותפת לגבי הגנת הפרטיות באופן שוטף; 3. צמצום הפררוגטיבה המעסיקית בכל הנוגע להגנת סייבר, תוך יישום מותאם טכנולוגית של העקרונות ההלכתיים שאומצו בפסיקה, כגון לגיטימיות, מידתיות (כולל עקרון צמצום המידע), שקיפות, וכן אימוץ העיקרון הנוסף של אחריותיות; 4. מתן כלים אינדיבידואלים של כוח בידי העובדים על מנת שיוכלו לנהל בצורה טובה יותר את המידע אודותיהם שנאסף, מעובד ומופץ לצרכי הגנת סייבר, וביניהם הזכות לביטול ההסכמה, מחיקת המידע, וכן הזכות להישכח. לאור הדיון שקיימנו בחלקים א ו-ב של מאמר זה אנו סבורות כי ניתן לקבוע חריגים לכללים הקוגנטיים ולכוח של ארגוני העובדים במקרים מסוימים בהם יש חשיבות עליונה להגנת סייבר.

א. <u>הגדלת ההגנה הקוגנטית</u>

העקרונות הקוגנטיים מתכתבים עם תפיסת ההסכמה המצויה בלבו של חוק הגנת הפרטיות, שכן הסכמה מדעת כפי שדורש החוק מחייבת, לאור הכרה בייחודיות מערכת יחסי העבודה, הגנה קוגנטית משמעותית. להגנה הקוגנטית טעמים שונים,[258] וכולם רלוונטיים גם בהקשר של הזכות הגנה על מידע פרטי. המשמעות תהיה שאיסוף, עיבוד, ופיזור מידע פרטי – במקרים מסוימים - תהיה אסורה בצורה מוחלטת. במקרים מעין אלה ניתן יהיה לפנות לקבלת צו אנטון פילר מבית הדין לעבודה לצורך איסוף אותו מידע פרטי, בדומה לאופן בו נקבע בהלכת איסקוב ענבר לגבי הגישה לתיבת דוא"ל פרטית של העובד. בהקשר של הגנת סייבר היינו מציעות להחיל את הכללים הקוגנטיים הבאים: איסור על ניטור אימיילים בתיבה פרטית של העובדת או העובד; איסור ניטור אחר מידע המצוי במרחבים הפרטיים של המחשב והפלאפון של העובדים שאינם מצויים במקום העבודה עצמו (זאת תוך חיוב מעסיקים להתקין תוכנה שמפרידה בין מרחבים אלה). כמו כן אנו סבורות כי יש להטיל איסור קוגנטי לגשת אל המידע הפרטי שנאסף על ידי המעסיק שנמצא בשרתים שלו ועל המכשירים שלו, למעט לצורך התכלית של הגנת סייבר. דבר זה ניתן להשיג הן על ידי כללים משפטיים – כגון קביעת פיצויים משמעותיים להפרת עיקרון צמידות המטרה – והן באמצעים טכנולוגיים, למשל הצפנת המידע כך שהוא לא יכול להגיע לידיים של המעסיק לאחר תקופה מסוימת. כחלק מההגנה הקוגנטית יש לדרוש מהמעסיק שקיפות נגישה לכל עובדת ועובד בכל הנוגע לפגיעה האפשרית בפרטיות ומשמעויותיה המעשיות. זאת בדומה לשקיפות הנדרשת בחלק מחוקי המגן, כגון בכל הנוגע לתלושי שכר בחוק הגנת השכר,[259] בכל הנוגע לשכר מינימום,[260] ולהטרדה מינית.[261] כללי השקיפות צריכים להיות ברורים על מנת למנוע, ככל הניתן, הטיות במידע המדובר. כלל קוגנטי נוסף נוגע לזהות של מי שרשאי להיחשף

---

[258] דוידוב, לעיל ה"ש 248, 40; Ian Ayres, *A Theory of Mandatory Rules: Typology, Policy and Design,* 99 &Eyal Zamir (2020) TEX. L. REV. 283.

[259] ס' 24 לחוק הגנת השכר, התשי"ח-1958.

[260] ס' 6(ב) לחוק שכר מינימום, התשמ"ז -1987.

[261] ס' 7(ב) לחוק למניעת הטרדה מינית, התשנ"ח-1998; תקנה 2(ב) לתקנות למניעת הטרדה מינית (חובות מעסיק), תשנ"ח-1998.

למידע הפרטי שאליו המעסיק כן רשאי לגשת לצורך ההגנה על המרחב הקיברנטי, שצריך להנתן לאדם או לפונקציה אחת בארגון.

ב. <u>חשיבותם של ארגוני עובדים</u>

שיתוף של ארגוני העובדים בעת קביעת מדיניות הגנת הסייבר בארגון והשימוש בטכנולוגיות להגנת סייבר הנה קריטית. זאת כדי לאפשר הבאת קול של עובדים אל תוך השיח הטכנולוגי ולא רק את קולם של חברות הטכנולוגיה, מערך הסייבר הלאומי, המעסיקים ושל אנשי הטכנולוגיה בארגון שלהם, כפי שהראינו בפרק א, אינטרסים אחרים והעדר מחויבות מסדר ראשון לדאגה לזכויות העובדים. כאמור, ארגוני העובדים נועדו לתת כוח בידי העובדים, ורבים כבר הדגישו את חשיבות שיתופם בכל מה שנוגע לטכנולוגיות חדשות.[262] אנו סבורות כי בדומה למה שעשה המחוקק האירופי ב- GDPR אזי גם בהקשר הישראלי יש להדגיש את חובת שיתופם של ארגוני העובדים במקומות מאורגנים. כפי שהרחבנו בדיון על שאלת ההסכמה בפרק הקודם, נראה כי הסכמה קיבוצית עשויה להיות משמעותית מאד בהקשר של טכנולוגיות הגנת סייבר ולדעתנו, יש לחייבה במקומות עבודה מאורגנים ולעודד אותה במקומות עבודה אחרים, ולו עם נציגות של עובדים. זאת נוכח התרומה הרבה שיכולה להיות לארגוני עובדים להחלטות הנוגעות לשאלות כגון: מקורות איסוף המידע, כיצד יבוצע עיבוד המידע, כיצד ניתן לוודא את יצירתם של מרחבים אישיים ועסקיים במחשב או במכשיר נייד, מהם צרכי המעסיק הספציפי והתכליות של הגנת הסייבר, מי בתוך הארגון רשאי יהיה לצפות במידע, שאלות הנוגעות למחיקת המידע וכד'. ארגון העובדים או נציגות העובדים אף יכולים להחליט יחד עם המעסיק מהן המטרות הלגיטימיות שבהן לא בהכרח תידרש הסכמה אישית מטעם העובדים (כגון במקרה של הגנת סייבר). ואולם, עדיין יש לתת כוח בידי העובד להסיר את ההסכמה לאיסוף מידע פרטי עליו, כמפורט להלן.

המשמעות היא שגם ארגוני העובדים צריכים ללמוד היטב את המטריה על מנת לקחת חלק פעיל בעת הטמעת טכנולוגיות הגנת סייבר במקומות עבודה מאורגנים ולקבל הכשרות טכנולוגיות ומקצועיות לשם כך. מחקר שנעשה לאחרונה על מעורבות ארגוני עובדים בהטמעה ושימוש בטכנולוגיות חדשות במקום העבודה הראה כי כאשר מסגרת יחסי העבודה הקיבוציים מחייבת, כמו בגרמניה, בין השאר בכל הנוגע לטכנולוגיות חדשות, אזי הארגונים מעורבים בצורה מהותית בכל היבט של הטכנולוגיה, בעוד במודל אחר בו ניתן להיוועץ עמם, כמו באיטליה, התערבותם הנה מינימאלית, אד הוקית, ומרסנת בלבד.[263] חובת ההסכמה של ארגון העובדים כמובן מעלה את שאלת היחס בין הסכמה קיבוצית להסכמה אישית, שהושארה בקלנסווה בצריך עיון, ואנו לא ניגע בה במסגרת זו. יצוין, כי המלצותינו לגבי מעורבות ארגוני עובדים או נציגות עובדים הנן רק בכל הנוגע להגנה על זכויות עובדים, ובהקשר שלנו הזכות לפרטיות, ולא בכל הנוגע להיבטים אחרים של הטכנולוגיה.

ג. <u>צמצום הפררוגטיבה המעסיקית באמצעות עקרונות הלכתיים</u>

---

[262] ILO, **Work for a Brighter Future**, לעיל ה"ש 113; De Stefano, לעיל ה"ש 1.
[263] Dagnino and Armaroli, לעיל ה"ש 253.

בדומה לאופן שבו מרוסנת הפררוגטיבה המעסיקית בדיני העבודה ברבדים שפוגעים בזכויות מעל לרף שנקבע בחוקי המגן או בהסכמים קיבוציים, כך לעמדתנו יש להגן על מידע פרטי מעבר למרחב הקוגנטי ולמה שהוסכם במסגרת היחסים הקיבוציים. הדבר דומה להגנה שניתנת על שוויון בעבודה גם במקרים בהם חוק שוויון הזדמנויות לא חל, לאור תחולתו של עקרון השוויון הכללי. גם כאן, הגנה על מידע פרטי רלוונטית מאד, בעיקר בהקשר של הגנת סייבר שהנה תכלית לגיטימית לניטור אחר מידע, כולל מידע פרטי. כצעד ראשון יש, לגישתנו, לעשות הבחנה בין מקרים שנופלים לגדר "ביטחון לאומי", כגון אלה המוגדרים בחוק הבטחת הביטחון וכן בהצעת חוק הסייבר, לבין מצבים אחרים של אבטחת מידע והגנה על מערכות. בשני האחרונים, הגישה כלפי הגנה על המידע צריכה להיות כלכלית-עסקית. למרות ששתי המטרות – הן הגנה על ביטחון לאומי והן המטרה הכלכלית-עסקית - הנן מטרות לגיטימיות, יש לוודא כי התפיסה של ביטחון לאומי לא תצבע גם צעדים שנעשים לצורך הגנה על מידע בלבד. את מתחם זה – של הגנה על מידע – יש לתחום תוך החלת הכללים המשפטיים האחרים, ובעיקר יש לדאוג לכך שלא ינקטו צעדים בלתי מידתיים תחת הכסות של "הגנת סייבר" על בסיס תפיסה של ביטחון לאומי. יש לעשות הבחנות בין מעסיקים שונים, כפי שתיארנו במהלך הדיון בפרק א, וכן בין סוגי מידע שונים המצויים במאגר (לקוחות של מכולת אל מול לקוחות של בנק).

בנוסף, על מנת לצמצם את הפררוגטיבה המעסיקית, יש לבחון שאלות הנוגעות להבחנה בין המידע – אם הוא עסקי או פרטי – ולעסוק לעומק בשאלות של מתי ובאיזה אופן נפגעת הפרטיות באמצעות הטכנולוגיה, כפי שפירטנו בפרק ג לעיל. עוד יש לתהות לגבי היקף המידע וסוג המידע שצריך להיאסף; איזה מידע צריך להיות חשוף ולמי; מהו אורך הזמן שיש לשמור על המידע; ואילו זכויות נוספות עשויות להיפגע. שאלות אלו יובילו להדגשת חשיבותם של עקרונות הלגיטימיות והמידתיות, ולבחינה יותר מעמיקה שלהן על מנת לבחור אמצעים חלופיים (בין השאר טכנולוגיות חלופיות או עיצוב שונה של הטכנולוגיה, שפוגעות פחות בזכות לפרטיות) לצורך ההגנה על הסייבר.

יש לאמץ בהקשר זה עקרונות נוספים מהדין האירופי, וביניהם עקרון צמצום המידע, עיקרון מחיקת המידע וכן עיקרון האחריותיות (accountability). על פי הרשות להגנת הפרטיות עיקרון צמצום המידע מעוגן בדין הישראלי וזאת בסעיפים 9(2) לחוק הקובע חובת צמצום הן בשלב האיסוף והן בשלב שמירת המידע, וכן בסעיף 6 לתקנות הגנת הפרטיות (תנאי החזרת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986.[264] ניתן אף למצוא דיון בעקרון צמצום המידע בפרשת שטטר של בית הדין הארצי לעבודה בה נקבע כי נתוני איכון של עובדים יועברו לידיהם של העובדים בטרם הם עוברים לידי המעסיק, על מנת לאפשר לעובדים להשחיר מידע עודף שאינו רלוונטי לבחינת אופן התנהלותם בשעות העבודה. בית הדין השעין את קביעתו על עקרון המידתיות בקובעו כי: "השמטת מידע עודף מאפשרת גילוי חלקי של מידע מקום בו הגילוי הכולל והרחב פוגע פגיעה שאינה מידתית באינטרסים משפטיים הראויים להגנה לרבות הזכות לפרטיות ...אופן מסירת מידע זו תורמת למזעור הפגיעה

[264] משרד המשפטים "צמצום מידע (Minimization Data) - מסמך מדיניות - טיוטא להערות הציבור" **gov.il**, בעמ' 7 (25.03.2021) https://www.gov.il/he/departments/publications/Call_for_bids/data_minimization_public_hearing.

בפרטיות".[265] אנו גם סבורות כי ניתן לגזור את עיקרון צמצום המידע מעקרון המידתיות, בנוסף לאדנים המשפטיים שציינה הרשות להגנת הפרטיות. זו גם עמדה שהובעה במסמך האחרון שהוציא ארגון העבודה הבינלאומי.[266] משמעות העיקרון הנה כי אין לאסוף מידע שאינו נחוץ לצורך הגנת סייבר. על פי הרשות להגנת הפרטיות, עיקרון צמצום המידע קובע כי יש להימנע ככל הניתן מאיסוף ושמירה של מידע אודות אדם שאינו הכרחי למטרת האיסוף או למטרת המאגר בו הוא שמור, ולפיכך יש לאסוף ולשמור רק את המידע המינימאלי הנדרש וההכרחי למטרות האמורות.[267]

חובת מחיקת המידע, אף היא, יכולה להיגזר מעקרון המידתיות. כך, למשל, מחקרים מראים כי הזמן שלוקח לאתר התקפת סייבר הנו בממוצע 200 ימים.[268] המשמעות היא שניתן לאחר שנה להצפין את המידע ולהסתירו מהמעסיק, שכן הסיכוי שתידרש גישה למידע לאחר תקופה זו הנו נמוך לאור ממוצע זה, וכן לקבוע חובה למחיקת המידע לאחר פרק זמן של שנתיים או שלוש, שאז לא יהיה עוד צורך במידע שנאסף. מחיקת מידע הנו עיקרון קריטי וחשוב לצורך הגנה על הפרטיות. אין כל הגיון – טכנולוגי ומשפטי – בהחזקת מידע שנאסף לצרכי הגנת סייבר לפרקי זמן ממושכים ובלתי מוגבלים. עקרון האחריותיות אף הוא חשוב מאד להגנה על המידע. כך לדוגמא, בהתאם לעיקרון האחריותיות, יש לבחון אילו מנגנונים ארגוניים ננקטו בידי המעסיק, האם מנגנונים אלו תואמים לעקרונות המשפטיים שנקבעו על ידי הפסיקה, והאם למעסיק יש יכולת להדגים אילו צעדים הוא נקט להגנה מיטבית על פרטיותם של העובדים. עקרונות נוספים המצויים ב- GDPR צריכים להיות מאומצים על ידי בתי הדין לעבודה בישראל, הן כחלק מעקרונות הלגיטימיות, המידתיות וצמידות המטרה (כגון עקרון הצמצום ועקרון מחיקת מידע שאינו נחוץ יותר) או כחלק מכבוד האדם וחירותו (כגון הזכות להישכח).

אימוץ כללים אקס אנטה יגנו בצורה הטובה ביותר על הזכות לפרטיות. נקודה זו נוגעת לקושי ביישום הדוקטרינה שנקבעה באיסקוב ענבר "לאחר המעשה" בפסיקת בתי הדין. כך למשל, על פי הלכת איסקוב ענבר, המעסיק רשאי להיכנס לתיבת הדואר של העובד במקרים חריגים ובה בעת הוא מחויב בעקרון צמידות המטרה, דהיינו שהשימוש במידע יהיה רק לשם מטרת איסופו (במקרה של הגנת סייבר – רק לצורך ההגנה על הסייבר). ואולם, במקרים רבים, המעסיקים מגישים בקשה לשימוש במסמכים בהליך לאחר שכבר נחשפו למידע האישי של עובדיהם, כלומר הפגיעה בפרטיות כבר נעשתה.[269] בתי הדין לאו דווקא מקפידים על יישום העקרון של צמידות המטרה, ועליהם לוודא שכך נעשה. הכרה בעיקרון כקוגנטי כפי שאנו מציעות ישיג את המטרה האמורה. אך מעבר לכך, מעסיקים שלא עומדים בעקרונות האחרים באופן שוטף – אל להם לקבל סעד מבתי הדין. דרישת של צמצום המידע הנאסף, כמו גם מידתיות של הטכנולוגיה והבאה בחשבון של הזכות לפרטיות בעת הפעלתה והסקת מסקנות על פיה, צריכים

---

[265] עניין **שטטר**, לעיל ה"ש 187, פס' 16 לפסק הדין.
[266] Hendricks, **Protection of Workers' Personal Data**, לעיל ה"ש 17, בעמ' 27.
[267] "צמצום מידע (Minimization Data) - מסמך מדיניות - טיוטא להערות הציבור", לעיל ה"ש 264, בעמ' 4.
[268] Luke Irwin, *How long does it take to detect a cyber attack?* IT GOVERNANCE (Dec. 28, 2017), https://blog.itgovernance.asia/blog/how-long-does-it-take-to-detect-a-cyber-attack.
[269] ראו דיון באלבין ועומר, לעיל ה"ש 162.

להיות משמעותיים בהחלטות בתי הדין ובלעדיהם, כאמור, אין לתת סעד למעסיקים שלא פועלים על פיהם וניתן אף לקבוע פיצויים משמעותיים כאשר אלה מופרים.

ד. <u>מתן כלים של כוח אינדיבידואלי בידי העובדים</u>

מעבר לכל אלה, אנו מציעות לאמץ עקרונות המקנים כוח בידי העובדים שיאפשר להם לנהל את המידע אודותיהם. ה- GDPR מציע סל מעניין וחשוב של זכויות בהקשר זה, וביניהן: הזכות לביטול ההסכמה, וכן הזכות להישכח. את שתי הזכויות הללו ניתן לשאוב לדין הישראלי. רלוונטית ביותר לענייננו היא הזכות להישכח, אשר אותה ניתן לבסס על הזכות לפרטיות המעוגנת בחוק יסוד: כבוד האדם וחירותו, כך שכאשר עובד סבור כי הוא מבקש למחוק מידע פרטי הנמצא אצל המעסיק הוא יכול לבקש למחוק אותו באופן מיידי, וללא שהות. מידע זה אינו נחוץ עוד כאשר הטכנולוגיה כבר עשתה עליו אנליזה לצורך זיהוי אנומליה ולכן אם העובד סבור כי הוא אינו מעוניין שמידע זה יישאר בידי המעסיק, הוא יכול לבקש למחוק אותו ולהישכח.[270]

ניתן להעלות מספר קשיים לגבי ההצעות האמורות. ראשית, הסכמה מהווה יסוד של הזכות לפרטיות ואילו התיאוריה של עבודה מציעה כללים קוגנטים שלא ניתן להתנות עליהם בהסכמה. אנו סבורות, כפי שציינו לעיל, כי קוגנטיות הנה חלק מתפיסת ההסכמה ולכן לא סבורות שיש כאן קושי מיוחד. קושי נוסף הנו קביעת כללים קוגנטיים בעולם טכנולוגי שהוא דינאמי ומשתנה, דבר שמשנה את נקודות הקצה בהם משתמשים עובדים, וכן את סוגי המידע הפרטי שנאסף (כמו למשל פיתוחים טכנולוגיים הנשענים על איסוף מידע ביומטרי או מידע רגשי). כך למשל פרשת איסקוב ענבר עסקה בסיווג תיבות דוא"ל שהיום השימוש בהן נעשה במידה פחותה, בעוד עולה השימוש באמצעים טכנולוגיים אחרים. יתר על כן, יצירת מרחבים פרטיים, אותם למעסיק אסור לנטר, עשוייה להוביל ל"blind spots" שאפשר שינוצלו על ידי תוקפי סייבר. יחד עם זאת, כפי שבתי הדין לעבודה מקישים מההבחנה של איסקוב ענבר בכל הנוגע לתיבות הדוא"ל גם לטכנולוגיות אחרות (למשל ווטסאפים) ניתן יהיה להתמודד עם זה בדרך זו וכן לייצר כללים קוגנטים נוספים. הדגש שלנו הוא על הרעיון ולא בהכרח אופן היישום שלו. קושי נוסף שעמדנו עליו בפרק זה הוא שארגוני עובדים לא עוסקים עדיין בכל מה שקשור לטכנולוגיות חדישות ואין להם בהכרח את הידע הנדרש. לפיכך ישנה חשיבות להכשרות לארגוני עובדים, חשיפתם לתחום זה, הניסיון הנלמד מארגונים במדינות אחרות וכדומה. קושי זה יכול לפתוח פתח חשוב לפעילות קיבוצית שעדיין אינה מפותחת דיה כיום.

ו. סיכום

[270] ישנה כתיבה מרובה על הזכות להישכח ופסיקה המכירה בה. אנו לא נצליח במסגרת מאמר זה להיכנס לעובי הקורה ולהכריע באיזה אופן יש להכיר בזכות בהקשר של עבודה, ואולם ברצוננו לציין, כי בירנהק מתייחס לזכות כביטוי לשליטה של אדם במידע ואפשרותו לחזור בו מהסכמתו, ראו: מיכאל בירנהק, "מעגלים של פרטיות" **זכויות הקהילה הגאה בישראל: משפט, נטייה מינית וזהות מגדרית** 195 (ענב מורגנשטרן, יניב לושינסקי, ואלון הראל עורכים 2016); בפסק הדין Google Spain v. Gonzalez , הזכות הוכרה על ידי בית הדין של האיחוד האירופי בקשר לתביעתו של אזרח ספרדי שדרש ממנוע החיפוש גוגל להסיר קישור לאתר בו פורסמה כעשור קודם לכן הודעת אמת על פשיטת רגל שלו. ראו: *Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, 2014 Reports of Cases before the Court of Justice and the Court of First Instance 1 (2014); ראו גם: Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. RER. 1 (2017).

במאמר זה עסקנו באחת הסוגיות הבוערות והחשובות ביותר בשוק העבודה כיום: כיצד ניתן לתת הגנה טובה יותר על מידע פרטי של עובדים שנאסף, מעובד ומופץ באמצעות תוכנות להגנת סייבר. זאת, מבלי לפגוע בתכלית החשובה של הגנה על המרחב הקיברנטי, אשר כפי שראינו, נועדה להגן על מאגרי מידע ועל מערכות ממוחשבות במטרה לדאוג להתנהלותו השוטפת של העסק, ולעיתים גם על אינטרסים חברתיים, סביבתיים ובטחוניים, ואף גם על המידע הפרטי של עובדים. יחד עם זאת, יש אף לתת את הדעת לכך שההגנה האמורה נעשית תוך ניטור אחר מידע פרטי של עובדות ועובדים, תוך פגיעה בזכותם למידע פרטי במגוון של דרכים אשר פורטו בחלק א של המאמר. חובות משפטיים החלים על מעסיקים להגנה על מאגרי המידע ועל מערכות ממוחשבות מעצימים את הפררוגטיבה שיש למעסיק בכל הנוגע להטמעת ושימוש במערכות הגנת סייבר במקום העבודה. פררוגטיבה זו מתחדדת נוכח התלות שיש למעסיקים במומחים הטכנולוגיים - בחברות המפתחות ומטמיעות את התוכנות להגנת סייבר במקום העבודה וכן במנמ"ר – מומחים שלא בהכרח מביאים בחשבון בעת עבודתם את הפגיעה האפשרית בפרטיות העובדים ואף אינם מחויבים לכך על פי הדין. גם אופן הפעולה של מערך הסייבר הלאומי מגביר את הפררוגטיבה המעסיקית אל מול העובדים, כמו גם תפיסת הביטחוניזציה הקיימת כלפי הגנת סייבר.

לאור זאת בחנו האם המבחנים המשפטיים הקיימים בדין הישראלי לגבי הגנה על מידע פרטי, כפי שאלה נקבעו בהלכות של בית הדין הארצי לעבודה – איסקוב ענבר וקלנסווה – ופותחו ויושמו על ידי בתי הדין בישראל, מעניקים הגנה מספקת למידע הפרטי. מסקנתנו הנה, כי על אף חשיבותם של מבחנים אלה, הרי שהם נותנים לעובדים הגנה חלקית בלבד. הצענו דרכים בהם ניתן יהיה לשפר את יישום המבחנים האמורים ואולם ציינו כי קושי מרכזי בהגנה הקיימת טמון בכך שההגנה על הזכות לפרטיות בעבודה נעשית בדין על ידי אימוץ כלים מדיני הגנת הפרטיות, תוך ביצוע מספר התאמות לעולם של עבודה, ולא על כלים מעולם דיני העבודה. עמדתנו היא כי אם יאומצו כללים נוספים מעולם דיני העבודה, אותם פירטנו בחלקו האחרון של המאמר, אזי ניתן יהיה להגן טוב יותר על הזכות לפרטיות בעבודה מהאופן בו היא מוגנת כיום. כפי שחידדנו לאורכו של המאמר – אין להפחית בחשיבותה של הזכות למידע פרטי בימינו, גם במקרים קשים כגון זה של הגנת סייבר. להפך – חיוניות ההגנה על מידע זה רק עלתה.