שאלות לדיון – שולחן העגול

במסגרת השולחן העגול נבקש להעלות כמה שאלות לדיון על מנת שאלו ינחו אותנו בהמשך תהליך החשיבה והמחקר על נושא יום העיון. השאלות המפורטות פה מטה הנן רשימה ראשונית בלבד והנכם מוזמנים להעלות נקודות נוספות במהלך הדיון עצמו.

<u>הזכות לפרטיות</u>:

1. **האם האופן שבו מוגדרת כרגע ההגנה על הפרטיות במסגרת תזכיר חוק הסייבר מספקת?** על פי סעיף 64 לתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018 ("**התזכיר**") מתייחס לתנאים <u>מצטברים</u> על פיהם לא יראו פעולה שמבצע ארגון ל**מטרת הגנת הסייבר**, כפגיעה אסורה בפרטיות עובדים או לקוחות, האזנת סתר או חדירה אסורה לחומר מחשב, כדלקמן:
"(1) לארגון יש מדיניות הגנת סייבר בהתאם להוראות או תקן מקובל ביחס לצרכי הגנת סייבר בארגון, בשים לב לאיומי הסייבר שלהם הוא חשוף;
(2) לארגון יש מדיניות גישה ושימוש במידע המעובד לצורכי הגנת הסייבר, המגבילה את האיסוף, השימוש ועיבוד המידע להיקף הנדרש לצורכי הגנת הסייבר;
(3) הארגון הודיע לעובדיו, ללקוחותיו ולגורמים אחרים שמידע עליהם עשוי להיאסף במסגרת פעילות זו, פרטים על הפעילות, על מטרותיה, ועל השימוש במידע."

2. **האם יש מקום להחיל את דרישת ההסכמה הקבועה בחוק הגנת הפרטיות שאומצה לגבי עובדים בפרשת איסקוב גם בעידן של הגנת סייבר מוגברת?** סעיף 1 לחוק הגנת הפרטיות, קובע כי פגיעה בזכות לפרטיות מתרחשת כאשר אין הסכמה. מבחן זה אומץ אף הוא בפסיקה, אשר רואה פרטיות כשליטה של האדם על חשיפת המידע אודותיו, ועל כן דורשת את הסכמתו של העובד למדיניות הניטור במסגרת הארגון.[1] עולה השאלה: האם בעידן בו הגנת הסייבר הפכה להיות משימה לאומית ממדרגה ראשונה,[2] וניתן גיבוי ולגיטימציה לנקיטת פעולות שנועדו להגן על המרחב הקיברנטי, יש עוד מקום לדבר על הסכמה של העובד. זאת הואיל והגיבוי והלגיטימציה שניתנת במסגרת תזכיר החוק והנה אף רציונאלית מגדילה את פערי הכוח בין הצדדים ליחסי העבודה, וקשה עד מאד לראות מצב שבו העובד אינו מסכים למדיניות הסייבר בארגון. **האם קיימות אפשרויות אחרות להגדרת הפגיעה בפרטיות של עובדים כיום?**

3. **האם יש מקום לתקן את חוק הגנת הפרטיות ולהתייחס באופן ספציפי לפגיעה בעובדים?** בפרשת **קלנסווה**,[3] בית הדין הארצי לעבודה התייחס לכך שחוק הגנת הפרטיות נותן מענה בעיקר לפגיעה מצד אמצעי התקשורת ורשויות השלטון ומענה חלקי בלבד לפגיעה מצד גורמים אחרים, דוגמת מעסיקים. על רקע כך, ציין בית הדין, "אולי הגיעה השעה להשלימו".

4. החשיפה למידע פרטי אף עשויה להוביל לפגיעה בזכויות נוספות, כמו למשל **הזכות לשוויון והגנה מפני אפליה מטעמים פסולים**.[4] כך, למשל, חשיפה למידע רגיש, כגון היות אישה בהריון או עובד שלקה במחלה כלשהי, עשוי להוביל להחלטה שיש עמה הפליה. האם יש לראות בחשיפה למידע שכזה כפגיעה בפרטיות או שמא יש להתמודד עמו תחת זכויות אחרות, כגון הזכות לשוויון?

---

[1] **איסקוב**, עמוד 17.

[2] בשנת 2010 מינה ראש הממשלה נתניהו צוות מיוחד לגיבוש תכנית קיברנטית לאומית אשר בחן את המרכיבים החיוניים להתמודדותה של ישראל במרחב הסייבר. מסקנת הצוות הצביעה על פוטנציאל לאיום מהותי על תפקוד המדינה, מוסדותיה ואזרחיה, וכי היערכות מדינת ישראל לאתגרי הסייבר הינם משימה לאומית. על בסיס מסקנה זו, התקבלה בשנת 2011 החלטת ממשלה מס׳ 3361 שעסקה בהקמת מטה הסייבר הלאומי, בכפיפות לראש הממשלה. בהתאם להחלטת ממשלה מס׳ 2444, 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 (החלטת ממשלה מס׳ 3270) הוחלט על איחוד שני הגופים לכדי יחידה ארגונית אחת – מערך הסייבר הלאומי. לפרטים נוספים אודות מערך הסייבר הלאומי ראו: https://www.gov.il/he/departments/about/newabout).

[3] עס״ק (ארצי) 14-04-7541 **הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי - עיריית קלנסווה** (פורסם בנבו, 15.3.2017) (״**קלנסווה**״).

[4] ראו שם, עמוד 18.

5. **האם יש לשאוב השראה בכל הנוגע להגנת הפרטיות של עובדים מה- GDPR האירופאי?** הרגולציה של האיחוד האירופי להגנת מידע האישי, General Data Protection Regulation ("**GDPR**") נכנסה לתוקף בשנת 2018 והחליפה את הדירקטיבה בנושא הגנת המידע האישי משנת 1995.[5] ה-GDPR קובע את העקרונות לעיבוד מידע אישי, כגון שקיפות ביחס לעיבוד המידע ושהמידע רלוונטי למטרה לשמה נאסף, וכן התנאים להסכמתו של מושא המידע לעיבוד מידע פרטי שלו.[6] לפי ה-GDPR, מושאי המידע נהנים מזכויות שונות ביחס למידע האישי כגון זכות גישה למידע האישי וקבלת מידע בנוגע למידע הנאסף (לרבות המטרה לשמה נאסף ופרטים בנוגע לגורם השולט במידע),[7] זכות לתקן מידע לא מדויק,[8] והזכות למחוק את המידע האישי (הזכות להישכח).[9] סעיף 49 להוראות המבוא ל-GDPR, קובע כי עיבוד מידע לצרכי הגנת הסייבר, **<u>המוגבל והפרופורציונאלי</u>** למידה הנדרשת לאבטחת המידע, מהווה **אינטרס לגיטימי** של הגורם השולט במידע. כמו כן, 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, המבוססים על **הסכמת העובד**, ובהתייחס להקשרים שונים כגון גיוס עובדים, ביצוע הסכם העבודה, ניהול, שוויון בעובדה וסיום יחסי עבודה.

<u>הזכות לאוטונומיה</u>

6. לצד הזכות לפרטיות ישנו פוטנציאל לפגיעה בזכות לאוטונומיה של העובדת והעובד. ישנם מצבים בהם בתי הדין לעבודה עסקו בשאלת השימוש של המעסיק במידע שהשיג על העובד במרחב הוירטואלי ואולם בחנו זאת לא דרך הפגיעה בפרטיות אלא בזכויות אחרות – כגון האוטונומיה לפרסם דעה וחופש הביטוי.[10] זאת במקרים בהם העובד חשף את המידע מרצונו (כמו למשל בפייסבוק). יתכן והדיון במקרים אלה דרך הזכות לחופש ביטוי ולאוטונומיה נובע מההמשגה של פרטיות בדין הישראלי שבבסיסה רעיון השליטה במידע, וההנחה כי מרגע בו העובדת פרסמה מידע בפייסבוק היא כביכול ויתרה של שליטה שכזו. **האם ראוי להמשיך לראות פעולות שכאלה כפגיעה באוטונומיה?**

7. עד היום הפסיקה הכירה בזכותו של עובד לאוטונומיה על גופו (עניין **דעקה**[11]), וכן למידע על גופו (פרשת **קלנסווה**). בכל הנוגע להתנהלות בעבודה הפסיקה חידדה את הפרוגטיבה של המעסיק לנהל את העסק שלו כרצונו, וכן לקבוע את נהלי העבודה של העובדים. יחד עם זאת, במציאות שבה הניטור עולה, עולות שאלות לגבי זכותו של העובד לאוטונומיה בהתנהלות במקום העבודה. שאלות אלה מעסיקות את העולם האקדמי הואיל וניטור המרחב הקיברנטי מאפשר איסוף מידע מן הסוג הזה ברזולוציה גבוהה ביותר. ברישן רוג'רס העלה לאחרונה את החשש כי בשל שימוש בטכנולוגיות חדישות במקום העבודה עובדים ימצאו את האוטונומיה שלהם בעבודה נפגעת.[12] פגיעה שכזו באוטונומיה תועדה על ידי החוקרת קרן לוי על ענף נהיגת המשאיות בארצות הברית, תוך שהיא מראה כי אמצעים טכנולוגיים הובילו לפגיעה באוטונומיה של העובדים בענף שבו ישנה תרבות של עבודה אוטונומית.[13] חשש זה אינו פוסח על המציאות הישראלית, בעיקר לאור קביעת בתי הדין לעבודה, אשר פסקו כי כאשר עיקר העבודה מתבצע **מחוץ לחצרי המעסיק** והיא מאופיינת בניידות גבוהה, מעסיקים רשאים, בהתאם לפררוגטיבה הניהולית שלהם ובכפוף להלכה שנקבעה בעניין איסקוב, להשתמש באמצעים טכנולוגיים על מנת לעמוד בחובתם לנהל יומן נוכחות (כגון

---

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (״**GDPR**״).

[6] סעיפים 5 - 7 ל-GDPR.

[7] סעיף 15 ל-GDPR.

[8] סעיף 16 ל-GDPR.

[9] סעיף 17 ל-GDPR.

[10] ראו למשל פסק הדין בעניינה של עביר רואשדה...

[11] ע״א 2781/93 **מיאסה עלי דעקה נ בית החולים ״כרמל״ חיפה**, נג (4) 526 (פורסם בנבו, 29.8.1999) (״**דעקה**״).

[12] Brishen Rogers, 'Beyond Automation: The Law & Political Economy of Workplace Technological Change'

[13] Levy.

מעקב אחר המיקום באמצעות טלפון נייד ו-GPS).[14] מעבר לכך, האמצעים הטכנולוגיים מאפשרים פיקוח עקיף ו"לא מורגש" של המעסיק על העובדים, באמצעות אמצעי מעקב שונים כגון מצלמות, מעקב אחר תכתובת דוא"ל, מעקב ברשתות החברתיות ועוד.[15] מגוון רב של אמצעי פיקוח וניטור, יחד עם כלים של בינה מלאכותית עשויים להניב מידע שאינו רלוונטי רק לעבודה עצמה, ואף לנתח את ההתנהגות והבחירות של העובדים. הטשטוש הגובר בין החיים הפרטיים והמקצועיים והממשק השוטף בין מכשירים טכנולוגיים ורשתות חברתיות, מאפשרים לאסוף מידע אישי על עובדים אשר קשה לכמת ולהגביל מראש.[16] **על כן עולות שאלות בכל הנוגע להכרה בזכות לאוטונומיה, והמבחנים שיש לאמץ כדי ליישמה** תוך שאנו עדיין מאפשרים את הפררוגטיבה הניהולית של המעסיק.

<u>אחריות נזיקית של עובדים</u>

8. המידע אודות אירועי הגנת סייבר, מלמד כי פעמים רבות העובדים (בכוונה או שלא), מהווים שער כניסה לתקיפות סייבר. מחקרים מראים כי ישנם מצבים בהם העובדים לא פועלים על פי מדיניות אבטחת המידע של הארגון ונוטים להעריך בחסר את הסכנות הכרוכות באירועי סייבר.[17] בהקשר זה עולות שאלות הנוגעות לחובות נזיקין של העובד ושל המעסיק במקרים של אירוע סייבר הנובעים מרשלנותו של העובד. על פי הדין מעסיק יכול לתבוע את עובדו בגין נזק שנגרם לעסק כתוצאה מפעילותו. זאת, לצד אפשרותו לתבוע את העובד על הפרת החוזה מצדו, כאשר מדיניות הבטחת הסייבר בארגון עשויה להיות חלק מחוזה זה. **האם יש מקום לאפשר תביעה נזיקית גם במקרה של אירוע סייבר? זאת לאור הנזקים המאוד גדולים שעשויים להיות וכן לאור המידע המועט, יחסית, שיש לעובד מן השורה על אפשרויות הפגיעה במאגרי המידע של הארגון ו/או בתשתיות ו/או באספקת השירותים. האם יש מקום להחיל חובת ביטוח על המעסיק לאירועי סייבר?.**

9. **שאלה נוספת שעולה נוגעת לנזק שנגרם לצד שלישי**. כעקרון, בהתאם לסעיף 13 לפקודת הנזיקין, למעסיק יש אחריות שילוחית על נזקים שהעובד ביצע <u>תוך כדי עבודתו</u> או אם המעסיק הרשה או אישרר את המעשה (לרבות מחדל) של העובד. בהתאם לסעיף זה, יראו מעשה כאילו נעשה "תוך כדי עבודתו" של עובד, אם נעשה על ידי העובד "כשהוא מבצע את התפקידים הרגילים של עבודתו והכרוכים בה אף על פי שמעשהו של העובד היה ביצוע לא נאות של מעשה שהרשה המעביד". כן נקבע כי הגדרה זו אינה כוללת מעשים שהעובד עשה למטרותיו האישיות. יחד עם זאת הפסיקה קבעה כי כאשר הפעולות נעשות במהלך יום העבודה (למשל בעת הפסקת הצהריים) עדיין יש מקום לבחון את אחריותו השילוחית של המעסיק. **ואולם, עולה השאלה האם תהיה אחריות שילוחית כאשר אין בהכרח יחסי עבודה בין הצדדים?, כמו, למשל, עובדים בענף ההיי-טק אשר עובדים כעצמאיים תופעה רחבת היקף בענף ההייטק הישראלי (שעל חלקה ניתן מענה בפסק דין ניסים)[18]. שנית, האם פעולה של עובד בענייניו הפרטיים על מחשבו של המעסיק תוך כדי רשלנות במימוש הנחיות להגנת סייבר, תוגן במסגרת האחריות השילוחית של המעסיק?, באיזו מידה?. שלישית, עולות שאלות לגבי פגיעה בהגנת הסייבר כאשר העובד עובד על מחשבו שלו, או עושה פעולה רשלנית דרך המכשיר הנייד הפרטי שלו.**

---

[14] ע"ע (ארצי) 40711-04-17 **פישר תעשיות פרמצבטיות בערבון מוגבל - אברהם שטטר** (פורסם בנבו, 04.03.2018), פסקה 11 לפסק הדין.

[15] טל גולן, "העין הבוחנת והצופה: הסדרה ומשטור של התנהגות עובדים במקום העבודה" בתוך: **משפט, חברה ותרבות - מסדירים רגולציה: משפט ומדיניות**, 515 (2016, להלן: **גולן, התנהגות עובדים**).

[16] טל גולן, "העין הבוחנת והצופה: הסדרה ומשטור של התנהגות עובדים במקום העבודה" בתוך: **משפט, חברה ותרבות - מסדירים רגולציה: משפט ומדיניות**, 515 (2016, להלן: **גולן, התנהגות עובדים**).

[17] Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, pp.13-24.

[18] בעניין **מדינת ישראל נ' ניסים**, בית המשפט העליון מרחיב את האחריות השילוחית על-פי דיני נזיקין ביחס להגדרת "שליחות" על-פי חוק השליחות, תשכ"ח-1965, גם כאשר לא מתקיימים יחסי עובד-מעסיק. באותו מקרה, בית המשפט קבע כי ניתן לראות בנהג שהתרשל, על אף שהיה לו עסק ונהג בטנדר משלו, כשלוח של היחידה הצבאית בה פעל. זאת, משום שעם תחילת שירותו ועד לסיומו, היה חלק מהמערך הארגוני של הצבא והיה נתון לפיקוחו.

סוגיות נוספות

10. מהן החובות החוזיות בין הצדדים ליחסי העבודה בכל הנוגע להגנת סייבר, בעיקר כאשר המעסיק קבע מדיניות סייבר בארגון שהפכה להיות חלק מחוזה העבודה של הצדדים?

11. מהי אחריות המשתמש לזכויות של עובדי ועובדות קבלן – הן בכל הנוגע לפרטיות והן בכל הנוגע למעשי רשלנות נזיקיים?

12. האם יש מקום לעשות אבחנות בין מקומות עבודה גדולים וקטנים בכל הנוגע לחובות המעסיק (ראו למשל את ההבחנה בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017)?