זכויות עובדים בעידן של הגנת הסייבר

כיום, כל ארגון נזקק לעמוד השדרה של הגנת סייבר. זאת על מנת להגן על המידע המצוי בידי הארגון, למנוע התקפות סייבר, כמו גם לנקוט אסטרטגיות של התקפה מפני האקרים פוטנציאלים. בעבר תחום "אבטחת המידע" הגן על ה"מידע הארגוני" ועל תהליכי העבודה בארגון המבוססות מידע. כיום פוטנציאל הפגיעה בהגנה על המידע התרחב מאוד בשל התלות הגוברת בתפקודם התקין של מחשבים והיכולת לשבש פעילות חיונית זו ולהגיע למידע מוגן באמצעות תקיפת מחשב. מגוון מטרות התקיפה התרחב וכך גם מושאי ההגנה אשר כוללים מעבר להגנה על המידע הארגוני אף פעילות תקינה שנועדה למנוע שיבוש שירותים חיוניים (כגון שירותים רפואיים), פגיעה בתשתיות (כגון חשמל, מים, תחבורה), מניעת נזק לאדם ולסביבה (כגון זיהום אוויר) ואינטרסים נוספים הנשענים היום, שלא כמו בעבר, על מערכות טכנולוגיות.

שינוי תפיסת ההגנה והפיתוחים הטכנולוגיים חייבו גם שינוי משמעותי בניהול הסיכונים באופן שלצד קיום עקרונות תפיסות אבטחת המידע המקובלות (הגנה פיזית, הגנה לוגית, הרשאות, מדיניות וכדומה) נדרש טיפול כולל וחוצה ארגון, הכולל ניטור רציף ומעמיק יותר של מערכות המידע ושל מרחב הסיכונים. זאת, על מנת לאפשר להנהלת הארגון קבלת החלטות רציפה לגבי המתח שבין התפקוד התקין של הארגון ושמירה על נכסיו לבין מניעת תקיפות, וכן הבנת היקף פוטנציאל הנזק והמשמעויות לנקיטת אמצעים למניעת הנזק, בעת שיש חשש לתקיפה.

ניטור זה פוגש שאלות הקשורות בקיומו של מרחב פרטי לגיטימי לעובדים גם במרחב הקיברנטי במקום העבודה. היקפו של מרחב זה הוא נושא לשיח תלוי הקשרי מגזר, מעסיק, פונקציה מיחשובית – הדעת נותנת כי קיומו מצומצם יותר בעניין מערכות המשרתות למשל תיקים רפואיים או תהליכים בטחונים, ורחב יותר בכל הקשור למערכות הניתנות לשימוש רחב יותר כגון גלישה באינטרנט. שאלות נוספות העולות בממשק שבין טכנולוגיה לחבירה היא כיצד משפיעה המגמה של מכשירים סלולרים של העובד הצורך במרחב פרטי נפרד במערכות המעסיק.

לשאלות אלה זיקה גם להיבטי הגנת הסייבר, משום שכפועל יוצא של תפיסות הגנת הסייבר מתקיים ניטור הגנתי הכולל את עובדות ועובדי הארגון וכן עובדות ועובדים של קבלני שירותים וקבלני כוח אדם שעובדים בו. בהמשך לכך עולות שאלות מורכבות ועדינות לגבי חובותיו של העובד ואחריותו, למול המעסיק, שפעמים רבות הינו בעצמו נאמן של צדדים שלישים – כגון "בעל מאגר מידע" לפי חוק הגנת הפרטיות או הדין האירופי וכן שאלות לגבי זכויות העובדים.

הזכות הראשונה שהפכה זה מכבר להיות "זכות על" שנדונה בעולם של טכנולוגיות חדשות היא **הזכות לפרטיות** העובדת והעובד. הסכם קיבוצי משנת 2007 קבע כי יראו כניטור סביר לצרכי הגנה ניטור המבוצע בהתאם לתקינת הגנת סייבר מקובלת. תזכיר חוק הסייבר מבקש להסדיר נושא זה באמצעות סעיף הגנה מפורש הקובע את מגבלותיו של ניטור סביר בארגון. בשורה של פסקי דין בתי הדין לעבודה עסק בשאלות מורכבות יותר שאינן ממוקדות בהגנת סייבר אלא באיזונים בין המרחב הפרטי של העובד וזכותו לפרטיות לבין אינטרסים לגיטימים אחרים של המעסיק במסגרת הפרורוגטיבה שלו. נבקש ללמוד מהלכות אלה גם לשאלות הרלוונטיות לעולם הגנת הסייבר.

לצד הזכות לפרטיות ישנו אגד נוסף של זכויות עובדות ועובדים שיש לתת עליהם את הדעת. **הזכות לאוטונומיה** של העובד/ת אשר תקשורת הרשת שלו, כולל התקשורת בעבודה, מנוטרת וחשופה, דבר המאפשר למעסיק לדעת בצורה יותר חדה מה העובד/ת עושיסות במהלך עבודתם – כיצד תוגן הזכות לאוטונומיה ומה תהיה מהות ההגנה?

המידע אודות אירועי הגנת סייבר, מלמד כי פעמים רבות העובדים מהווים שער הכניסה לתקיפה. בהקשר זה עולות שאלות הנוגעות **לחובות נזיקין במקרה של אירוע סייבר שנובע מרשלנותו של העובד/ת**. מי יהיה אחראי על פי הדין לנזק זה? והאם יש מקום לחשיבה מחודשת על הלכות החבות בנזיקין של עובדים ביחס למעסיקיהם?

שאלות משמעותיות עולות אף בכל הנוגע **לחובות תום הלב והאמון** – בין העובד והעובדת לבין הארגון וכן בין הארגון לעובדת ולעובד. למשל - מהי חובת הזהירות של המעסיק המחוייב במרחב פרטי וירטואלי לגיטימי כלפי העובד בעת שהוא מספק לו שירותי תקשורת? מה חובת הזהירות בין עובדים לבין עצמן בנושא זה?

לבסוף עולות שאלות חשובות לגבי חובות הארגון בנוגע לכל אחד מנושאים אלה **כלפי עובדות ועובדי קבלן**.

סוגיות אלה ונוספות יהיו במרכז מחקר שיתחיל השנה בשיתוף של ד"ר עינת אלבין והמרכז לחקר הסייבר בפקולטה למשפטים באוניברסיטה העברית. ביום 22.1.2020 יתקיים כנס השקה לפרוייקט.

מטרת הפרוייקט היא לעורר דיון ער בסוגיות אלו תוך התייחסות לכלל בעלי האינטרנט: רגולטורים, ארגוני עובדים, מעסיקים ונציגי תעשיית אבטחת הסייבר ולבחון את הפתרונות הנדרשים בשלבים השונים כדי למקסם את אבטחת הסייבר של הארגונים תוך צמצום הפגיעה בזכויות העובדות והעובדים.