גילוי דעת 3/17: שיתוף מידע לצורך התמודדות עם איומי סייבר

א. מבוא

עניינו של גילוי דעת זה בשיתוף מידע בין גופים מסחריים לצורך התמודדות עם איומי סייבר. לאור התגברות איומי הסייבר בשנים האחרונות, הולך וגובר הצורך של גופים וארגונים בשיתוף מידע שעשוי להועיל להם בהתמודדות עם איומים אלו, בייחוד בין גופים הפועלים בענף מסוים.

שיתוף מידע בין מתחרים עשוי להוות, בנסיבות מסוימות, הסדר כובל על פי חוק ההגבלים העסקיים, התשמ"ח-1988 (להלן: "**חוק ההגבלים העסקיים**"). לאור החשיבות המשקית בשיתוף מידע בין גופים מסחריים בהתגוננות מול איומי הסייבר, והצורך להגן על תשתיות חשובות במדינת ישראל, הממונה על הגבלים עסקיים רואה חשיבות להבהיר את עמדתה בעניין זה.

ב. אבטחת סייבר – רקע

ההתפתחות הטכנולוגית בעשורים האחרונים ובייחוד התפתחות האינטרנט והמערכות הממוחשבות הביאה בכנפיה בשורה של יעילות וחדשנות בניהול חיי המעשה של העולם המודרני, אך בד בבד הביאה גם לתלות רבה של המשק במערכות אלו. כתוצאה מן התלות במערכות הממוחשבות, אנו חשופים לאיומים חדשים על שלמותן ותקינותן של מערכות אלה, בדמות מתקפות ואיומי סייבר מצד גורמים פרטיים ומצד מדינות וארגוני טרור.

מטרתן של מתקפות סייבר היא לאסוף מידע, לפגוע במידע או להשבית שירותים והן עשויות להיות מכוונות כלפי תשתיות ומערכות חשובות במשק, כדוגמת מערכת הבנקאות ושוק ההון, מערכות תקשורת, וכן כלפי גופים שלטוניים.

מתקפות סייבר התפתחו בשנים האחרונות והפכו להיות מורכבות ומשוכללות יותר, ובמקביל החלו להתפתח דרכי התמודדות עם מתקפות אלו. דרכי התמודדות אלו שמות דגש על מניעה מראש של המתקפה, בין היתר על ידי איתור איומי סייבר פוטנציאלים ונטרולם טרם המתקפה ועל שמירה על מערכות האבטחה, על ידי איתור חולשות במערכת ודרכים אפשריות לפגיעה בהן. הצורך של ארגונים עסקיים להתמודד עם איומי סייבר מציב בפניהם אתגר משמעותי, בין היתר מאחר שהיקף המידע העומד בפני ארגון בודד אינו מספק לצורך קבלת תמונת מצב מיטבית של איומי הסייבר נגדו, וקיים צורך ממשי בגישה למידע אודות איומי סייבר שהתרחשו או שעשויים להתרחש בארגונים אחרים. לאור זאת, החלו לקום ברחבי העולם מערכות לשיתוף מידע בין ארגונים וגופים.[1]

---

[1] לדוגי בבריטניה מופעלת מערכת לאומית לשיתוף מידע בסייבר המופעלת על ידי ה- National Cyber Security Centre (NCSC); בארה"ב פועלים כ – 20 מיזמים לשיתוף מגזרי בענפים שונים הנקראים Information Sharing and Analysis Centers (ISACs) המאוגדים על ידי ארגון גג בשם National Council of ISACs (NCI), וכן פועלים גופים פרטיים המספקים מערכות לשיתוף מידע בסייבר כגון מערכת "TruSTAR" המופעלת על ידי חברת CyberPoint International LLC.

מדינת ישראל רואה חשיבות רבה בסיוע לגופים במשק בהתמודדות עם איומי סייבר והחליטה על הקמת המרכז הלאומי להתמודדות עם איומי סייבר (להלן: "**CERT**") על ידי הרשות הלאומית להגנת הסייבר, שייעודו הוא חיזוק החוסן של המשק הישראלי בהתמודדות עם איומי סייבר.[2] בנוסף, רגולטורים ענפיים פרסמו הוראות ועקרונות הנוגעים לאופן ניהול סיכוני הסייבר בגופים המפוקחים על ידם המתייחסות בין היתר לחשיבות שיתוף מידע בין הגופים.[3]

בין יתר פעולותיו, ייסד ה-CERT מערכת לשיתוף מידע בעל ערך אבטחתי בין גופים שונים, שתספק גם ערך מוסף מעבר להעברת המידע גרידא כגון, סינון המידע, ניתוח ועיבוד המידע וכן, מתן כלים וסיוע בהתמודדות עם איומי סייבר. כיום, שיתוף מידע בעל ערך אבטחתי צפוי להתבצע באמצעות המערכת לשיתוף מידע שהוקמה על ידי ה-CERT, אך יתכן שבעתיד יוקמו מערכות נוספות לשיתוף מידע בעל ערך אבטחתי.

ג. העברות מידע בין מתחרים ושיתוף מידע בעל ערך אבטחתי

העברות מידע בין מתחרים עשויות בנסיבות מסוימות להוות הסדר כובל כמשמעו בסעיף 2 לחוק ההגבלים העסקיים כפי שנקבע בהחלטות קודמות של הממונה על הגבלים עסקיים.[4]

החשש התחרותי העיקרי העולה מחילופי מידע בין מתחרים הוא מפני הקטנת חוסר הוודאות של המתחרים בשוק בנוגע לפעולות העסקיות של מי מהם, דבר שעשוי להוביל ליצירת התאמה ביניהם בנוגע להתנהלות העסקית שלהם באופן שעשוי לפגוע בתחרות. החשש האמור מתקיים בדרך כלל בנוגע להעברת מידע על הפעילות העסקית – מסחרית של הצדדים, כגון מידע על מחירים, עלויות, כמויות או תכניות עסקיות.[5] מידת ההשפעה של העברות מידע בין מתחרים על היכולת ליצור התאמה בין מתחרים תלוי בגורמים נוספים, וביניהם מידת התחרות השוררת בשוק הרלוונטי והגורמים המעבירים את המידע.

שאלת סיווגו של הסדר לשיתוף מידע בין מתחרים תחת הגדרת הסדר כובל, כמשמעו לפי סעיף 2 לחוק ההגבלים העסקיים, תלויה, אם כן, בראש ובראשונה בסוג המידע המועבר בין המתחרים, ובשאלה האם העברתו מעלה חשש לפגיעה בתחרות בין הצדדים.

---

[2] החלטה מספר 2444 של הממשלה ה – 33 "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.2015).

[3] ר' לדוגמה הוראות ניהול בנקאי תקין 361 "ניהול הגנת הסייבר" (16.3.2015).
www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf.
וכן, חוזר גופים מוסדיים 2016-9-14 "ניהול סיכוני סייבר בגופים מוסדיים" (31.8.2016)
mof.gov.il/hon/documents/mosdiym/memos/h_2016-9-14.pdf.

[4] כך לדוגמה החלטה לפי סעיף 14 לחוק ההגבלים העסקיים, התשמ"ח-1988 בדבר מתן פטור מאישור הסדר כובל להסדר בין World Liner Data Limited ובין Limited Container Trade Statistics ובין חברות ספנות בינלאומיות (17.4.2016) **הגבלים עסקיים** 500965; והחלטה לפי סעיף 14 לחוק ההגבלים העסקיים, התשמ"ח-1988 בדבר מתן פטור בתנאים מאישור הסדר כובל להסדר שצדדים לו כלל חברה לביטוח בע"מ, מגדל חברה לביטוח בע"מ, הראל חברה לביטוח בע"מ, מנורה מבטחים ביטוח בע"מ, הפניקס חברה לביטוח בע"מ וסומך חייקין- KPMG (4.4.2011) **הגבלים עסקיים** 5001769; וכן, גילוי דעת מאת הממונה על הגבלים עסקיים: פטור לחילופי מידע הכרחיים לפתרון בעיות שנת ה-2000 בתחום מערכות המחשוב (2.3.1999) **הגבלים עסקיים** 3002201 (להלן: "**גילוי דעת בעניין באג 2000**").

[5] כך לדוגמה החלטה לפי סעיף 14 לחוק ההגבלים העסקיים, התשמ"ח-1988 בדבר מתן פטור בתנאים מאישור הסדר כובל להסדר שצדדים לו כלל חברה לביטוח בע"מ, מגדל חברה לביטוח בע"מ, הראל חברה לביטוח בע"מ, מנורה מבטחים ביטוח בע"מ, הפניקס חברה לביטוח בע"מ וסומך חייקין- KPMG (4.4.2011) **הגבלים עסקיים** 5001769;

ככל ששיתוף המידע אינו נוגע לפעילותם העסקית של הצדדים אלא אך ורק למידע הנדרש לצורך הגנת סייבר, כגון מידע אודות איומי סייבר, סממנים,[6] חולשות,[7] פוגענים ונוזקות[8] וכן מתודולוגיות וכלי התמודדות עם איומי סייבר (להלן: "**מידע בעל ערך אבטחתי**"), רשות ההגבלים העסקיים לא תראה בהעברתו כפעולה העלולה למנוע או להפחית את התחרות בעסקים וזאת אף אם העברת המידע נעשית בין מתחרים.

הרציונל בבסיס עמדה זאת הוא כי מידע בעל ערך אבטחתי הוא מטבעו מידע טכני, ואינו כולל מידע מסחרי או מידע שנוגע לפעילות העסקית של מי מהצדדים,[9] בעוד שהחשש מפני התאמת הפעילות המסחרית בין מתחרים כתוצאה משיתוף מידע ביניהם עולה במקרים של שיתוף של מידע רגיש תחרותית, הנוגע לפעילות העסקית של הצדדים.[10] יתירה מכך, לשיתוף מידע בעל ערך אבטחתי עשויה אף להיות השפעה פרו תחרותית על המשק, שכן הוא עשוי לעזור לכלל הגופים, גדולים וקטנים, לאבטח את התשתיות ואת מערכות המידע שלהם מפני איומי סייבר ולייעל את מערכות האבטחה שלהם.[11]

ד. גישה חופשית למערכות שיתוף מידע

במקביל להחלפת מידע בעל ערך אבטחתי באמצעות פלטפורמות המופעלות על ידי רשויות שלטוניות (כגון ה-CERT), החלפה של מידע כאמור עשויה להתבצע גם במסגרת מיזמים משותפים בין גופים העוסקים בשוק או בענף מסוים. בדומה למיזמים משותפים אחרים, גם מיזמים אלו עשויים לספק למשתתפים בהם ערך, באופן המשפיע על יכולת ההתחרות שלהם. לפיכך, מניעת גישה למיזם מאחד או יותר מהמתחרים עלולה להפחית את יכולת ההתחרות של אותם גופים, להעלות את חסמי הכניסה לשוק ולעיתים אף למנוע כניסה של גופים חדשים לתחום,[12] ועל כן עשויה להוות, כשלעצמה, הסדר כובל.

---

[6] נתונים אודות פעילות אשר ממנה ניתן להסיק כי התרחש, עלול להתרחש או מתרחש אירוע סייבר.

[7] תורפות במערכות ממוחשבת או רכיביהן או בנהלים הקשורים אליהן אשר ניתן לנצלן בכדי לייצר אירוע סייבר.

[8] יכולות וכלים אשר נעשה בהם שימוש כדי לנצל חולשה.

[9] Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cyber Security Information (April 10, 2014) P.7.
www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

[10] כך לדוגי נקבע כי חילופי מידע הנוגעים לפתרון בעיות שנת ה- 2000 אינם מעלים חשש לפגיעה בתחרות, גילוי דעת בעניין באג 2000, עמ' 6.

[11] Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cyber Security Information (April 10, 2014) P.6-7.
www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.
Letter from Joel I. Klein, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, to Barbara Greenspan, Assoc. Gen. Counsel, Electric Power Research Inst. (Oct. 2, 2000), *available at* www.justice.gov/atr/public/busreview/6614.html.

[12] והשוו לאמור בסעיף 39 לגילוי דעת 3/14 "בעניין איגודים עסקיים ופעילותם" (4.9.2014) **הגבלים עסקיים** 500682 - "כאשר חברות באיגוד העסקי מקנה גישה לנכס, מידע או שירות שעשויה להיות לו השפעה משמעותית על כושר התחרות של העוסק או כשהיא עשויה להקנות גישה לפעילות כלכלית משמעותית או להקל עליה משמעותית הרי אי קבלתו לאיגוד או הוצאתו ממנו עלולה לחסום או להגביל את יכולת התחרות בענף ובכך למנוע או להפחית את התחרות בעסקים ואף להוות החרמה" כמו כן, במספר החלטות הממונה למתן פטור מאישור הסדר כובל, הותנה מתן הפטור בתנאים אשר יאפשרו גישה חופשית ושוויונית לגופים העוסקים בתחום, כך לדוגי החלטה לפי סעיף 14 לחוק ההגבלים העסקיים, התשמ"ח-1988 בדבר מתן פטור בתנאים מאישור הסדר כובל שצדדים לו ארגון התעופה הבינלאומי (International Air Transport Association) וחברות תעופה (20.10.2015) **הגבלים עסקיים** 500864; והחלטה לפי סעיף 14 לחוק ההגבלים העסקיים התשמ"ח-1988 בדבר מתן פטור בתנאים מאישור הסדר כובל להסדר שבין איגוד חברות הביטוח בישראל וחברות ביטוח להפעלת מערכת סליקה (31.8.2015) **הגבלים עסקיים** 500852.

מאחר שמערכות לשיתוף מידע בעל ערך אבטחתי עשויות לשפר את יכולת ההתמודדות של גופים עם איומי סייבר ולייעל את מערך ההגנה שלהם, מניעת גישה, ללא הצדקה סבירה, למערכת בה משותף מידע בין גופים בשוק או ענף מסוים מגופים הפועלים באותו שוק או ענף, שהמידע רלוונטי עבורם (בשים לב למאפייניהם הרלבנטיים , כגון תחומי הפעילות שלהם, היקפי פעילותם וכו'), עלולה להשאירם בנחיתות תחרותית אל מול המתחרים שלהם ובכך עלולה להביא לפגיעה בתחרות.

ה. סוף דבר

שיתוף מידע בעל ערך אבטחתי מהווה חלק משמעותי מיכולת ההתמודדות של גופים עם איומי סייבר ומדינת ישראל רואה חשיבות רבה בעידוד גופים במשק לשתף ביניהם מידע בעל ערך אבטחתי.

רשות ההגבלים העסקיים רואה אף היא חשיבות בעידוד שיתוף מידע בעל ערך אבטחתי, במקום בו הדבר לא עלול לפגוע בתחרות. גילוי הדעת מציג כללים לניתוח תחרותי של שיתוף מידע בעל ערך אבטחתי, באופן שייתן אמות מידה להערכה של הסדרי שיתוף מידע ובכך יגדיל את הוודאות של גופים המעוניינים לקחת חלק בשיתוף מידע בעל ערך אבטחתי מבלי לחשוש מהפרה של הוראות חוק ההגבלים העסקיים.

מיכל הלפרין

הממונה על הגבלים עסקיים

ירושלים, כ"ט בתמוז התשע"ז

23 ביולי 2017