14/12/2023

לכבוד

יו"ר הוועדה - חבר הכנסת יולי יואל אדלשטיין

ועדת החוץ והביטחון

התייחסות מכון תכלית: תזכיר חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023

תזכיר חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023 (להלן: "התזכיר") מבקש להקים מנגנון שיאפשר לגופי מודיעין להתריע בפני חברות פרטיות המספקות שירותים דיגיטליים לציבור אודות חשש לתקיפת סייבר חמורה נגדן, ואף להנחות אותן במידה והן מתקשות להתמודד בעצמן עם המתקפה. מדובר במטרה ראויה, אשר נכון לקדמה על רקע אתגרי הסייבר במהלך מלחמת חרבות ברזל המתנהלת בקרקע, באוויר, בים וכן במרחב הדיגיטלי. מאחר ומדובר בשינוי פרדיגמה מהמצב הנוכחי – במסגרתו יחסי גופי מודיעין וחברות פרטיות מתבססים על מערכת יחסים שהיא יותר וולונטרית מאשר כופה – נבקש להסב את תשומת הלב למספר קשיים שעלולים להתעורר מן המתכונת המוצעת של המהלך.

תמצית עמדתנו

- **ישראל של אחרי השבעה באוקטובר היא מדינה שונה, וזאת אחרי שנחשפו כשלים ניהוליים שהובילו לטרגדיה אנושית מתמשכת. רגע שכזה בחיי מדינה מוביל לשינוי בתבניות החשיבה המקובלות, ופעמים רבות גם לשינויים מבניים ביחסי השלטון עם אזרחים, השוק הפרטי וגורמים נוספים. הזמן הנוכחי דורש גם אמצעים מיוחדים במהלך התמודדות עם מצב החירום שמדינת ישראל נקלעה אליו.**
- **למרות שמדובר בהוראת שעה, מדובר בשינוי דרמטי. בהתאם, יש לבחון כיצד המנגנון המוצע עלול להשפיע על השוק הטכנולוגי בישראל, אשר יש לו חשיבות אסטרטגית, כלכלית, ותדמיתית. חשוב כי המנגנון ישקף חלוקת סיכונים ואחריות ברורה בין גופי המודיעין לבין עצמם, ואל מול השוק הפרטי, מתוך הבנה כי כלל השחקנים הרלוונטיים הם בעלי אינטרס חשוב במשוואה (stakeholders).**
- **מבחינה מעשית, מכון תכלית ממליץ על: א) הגברת הוודאות לגבי רשימת השיקולים המובאים בסעיף 2(5) לתזכיר (שיקולי פרטיות, פגיעה כלכלית ורצף תפקודי), והבניה של הפעלת שיקול הדעת של העובד המוסמך בבואו לבצע איזון בינם; ב) חידוד חלוקת הסיכונים והאחריות בין גופי המודיעין והשוק הפרטי, במטרה למנוע אי הבנות, תקלות בתקשורת ובעיות בהתמודדות עם תקיפת סייבר חמורה; ג) ביחס לסעיף 4(5) לתזכיר, נציע להגדיר את המאגרים בהם יישמר מידע שייאסף על ידי גופי מודיעין, להבהיר אם**

התזכיר מסמיך העברת מידע ממאגר מידע ממשלתי אחד לאחר, לחדד מהו מועד "סיום הטיפול בתקיפת הסייבר" ולשקול קביעת סנקציה כלפי גורם שלטוני שלא יעמוד בדרישה למחיקת מידע; ד) ראוי לשקול מנגנון ערעור (בטרם מימוש האפשרות של פניה לבית משפט לעניינים מנהליים לפי סעיף 7 לתזכיר), לצורך יישוב אי הסכמות לגבי עצם או אופן הפעלת הסמכות החריגה.

א. <u>אתגרי העת הנוכחית – מלחמת חרבות ברזל</u>

מתקפת ה-7 באוקטובר טלטלה את מדינת ישראל ואת אזרחיה. על פי חברת אבטחת הסייבר קלאודפלייר, לצד מתקפה אכזרית זו התבצעו תקיפת סייבר במטרה למנוע העברת מידע חיוני ולשבש התרעות צבע אדום.[1] מאז, נרשמה עלייה משמעותית בתקיפות הסייבר כנגד אתרים ישראלים – הן גופים ציבוריים והן חברות פרטיות.[2]

בעידן הנוכחי, למידע אישי ישנו ערך כלכלי רב, אשר שחקנים שונים, דוגמת חברות פרטיות, יכולים לנצל בקלות. כאשר מדובר במדינות אויב, למידע אישי יש ערך אסטרטגי ולפעמים גם צבאי. בנוסף, החשש איננו רק מדליפת מידע, אלא ישנן סכנות נוספות כגון זיוף, זיהוי מטעה ועוד.[3] למידע אישי יש חשיבות גם בהקשר של הגנה על הפרטיות, אשר מהווה בסיס חשוב להגנה על כבוד האדם[4], האוטונומיה שלו[5], כמו גם למימוש שאר החירויות שלו.[6]

מאחר וגופי מודיעין נדרשים לפעול לילות כימים בכדי לשמור על אזרחי המדינה, ראוי כי יוקנה סל כלים מספק להתמודדות עם האיומים המרחפים מעל ראשינו, גם אם הדבר מהווה שינוי תפיסתי (פרדיגמטי) במובן של טיב היחסים בינם לבין שוק הטכנולוגיה בישראל. בפרט, ראוי להרחיב את סמכויות מערך הסייבר הלאומי העומד בחזית של מדיניות אבטחת הסייבר במדינת ישראל, במיוחד כאשר הדבר מחזק את רמת הביטחון של אזרחי ישראל. יחד עם זאת, חשוב לוודא שהמהלך מבוסס על עקרונות מקובלים של שיתופי פעולה בין גופי שלטון לשוק הפרטי, באופן אשר יהיה בר-יישום, בר-קיימא, ובעל פוטנציאל לחזק את היחסים בין השחקנים הרלוונטיים השונים.

ב. <u>שיתוף פעולה בין שחקנים בעלי אינטרס בהתמודדות עם תקיפות סייבר (Multi-stakeholders)</u>

המרחב הדיגיטלי הוא מבוזר וכולל שחקנים רבים (multi-stakeholders) – דוגמת ספקי האינטרנט, חברות הגנת סייבר, גופי ביטחון ומודיעין מדינתיים, ואף ארגונים בינלאומיים. מחקרים מראים כי ביחסים בין השחקנים השונים, יש חשיבות

---

[1] עומר יואכימיק "מתקפות סייבר מאז פרוץ המלחמה בין ישראל וארגון הטרור חמאס" **קלאודפלייר בלוג** (26.10.2023), https://blog.cloudflare.com/he-il/cyber-attacks-in-the-israel-hamas-war-he-il/ .

[2] יוסי הטוני "40 ימים למלחמה: יותר מ-1,200 אירועי סייבר נגד ישראל" **אנשים ומחשבים** (15.11.2023), https://www.pc.co.il/featured/397891/.

[3] Tal Mimran and Yuval Shany, Israel, *Cyberattacks and International Law*, **Lawfare** (30.12.2020), https://www.lawfareblog.com/israel-cyberattacks-and-international-law; *Biometric Authentication Benefits and Risks*, **Identity Management Institute**, https://identitymanagementinstitute.org/biometric-authentication-benefits-and-risks/.

[4] Beizaras and Levickas v. Lithuania, App. No. 41288/15 ECHR, para.117 (2020).

[5] Reklos and Davourlis v. Greece, App. No. 1234/05 ECHR, para. 38 (2009).

[6] *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Hum. Rts. Comm., para. 11, (1988), https://www.refworld.org/docid/453883f922.html. להרחבה בנושא, ראו: מיכאל בירנהק **פרטיות חוקתית** (2023), בעמ' 83.

להסכמה על אופן חלוקת הסיכונים ומקסום היכולות הייחודיות של כל גוף[7]. גם בתזכיר דנן, חשוב כי יוסדר מנגנון של שילוב כוחות בין בעלי העניין השונים, באופן אשר ימקסם את היתרונות היחסיים של כל אחד.

ניתן להסתכל לדוגמה על חברת מיקרוסופט, שהקימה תכנית ביטחון ממשלתית כבר ב-2003, לפיה היא משתפת ממשלות במידע לגבי איומים, במטרה לחזק את שיתוף הפעולה עם גורמי שלטון בהתמודדות עם תקיפות סייבר.[98] ועדיין, לעיתים שיתוף הפעולה אינו מתרחש באופן חלק, במיוחד כאשר כללי המשחק אינם ברורים ולא נתקבלו באמצעות הסכמה. למשל, בפרשת *מיקרוסופט נ' ארצות הברית*, החברה סירבה לספק לגופי המודיעין האמריקנים מידע בטענה שמדובר במידע שמוחזק מחוץ לגבולותיה של מדינה ולכן העברתו היא בניגוד לדין הבינלאומי.[10]

תיק זה עורר עניין רב, וחברות ביג-טק כמו גוגל ואמזון הגישו חוות דעת "ידיד בית המשפט" בכדי להשפיע על התוצאה. אמנם, בסופו של יום, הדין האמריקני תוקן באופן שייתר את ההכרעה השיפוטית, אך דוגמה זו מעידה על החשיבות של הגדרת כללי התנהלות ברורים.[11] לאחר הפרשה, הציעה מייקרוסופט עקרונות מנחים לשיתוף פעולה: עיצוב אסטרטגיה רוחבית לשיתוף מידע ושיתוף פעולה בין הגורמים השונים המתבססת על התמודדות עם איומים ממשיים, זיהוי מצבים פגיעים ושיתוף במידע שיכול למנוע מתקפות סייבר, התחשבות בהשפעה על זכויות אדם, מניעת חסמים חקיקתיים ורגולטוריים בפני שיתוף הפעולה, וקביעת מגבלות על הגישה של הממשלה למידע מוגן.[12]

ג. <u>הצעות קונקרטיות לגבי המנגנון המוצע בתזכיר</u>

ניכר כי הושקעה חשיבה רבה בהבניית מנגנון הפעולה בתזכיר, שהביאה בחשבון אינטרסים מגוונים, בתקווה לצמצם ככל הניתן פגיעה כלכלית, הפרעה לרצף תפקודי או איום על זכויות אדם. הדבר בולט לאור קיומו של מסלול פעולה הדרגתי, המשמר אוטונומיה של חברות ומעודד אותן להתמודד עם האתגר בעצמן, בטרם הפעלת סמכות פולשנית. המחשה נוספת ניתן למצוא בהצבת רף גבוה להתערבות בסעיף 2 (חשד *ממשי*, ביחס לתקיפת סייבר *חמורה*), בהגדרה בסעיף 2(5) של

---

[7] Tobias Liebetrau and Linda Monsees, *Assembling Publics: Microsoft, Cybersecurity and Public-Private Relations*, 11(3) POL. & GOV. 1, 2 (2023), available at: https://doi.org/10.17645/pag.v11i3.6771; *Multistakeholder Participation at the UN: The Need for Greater Inclusivity in the UN Dialogues on Cyber Security, A study by Paris Call Working Group 3 on Advancing the UN Negotiations with a Strong Multistakeholder Approach* (November 2021), p. 23, at https://cybertechaccord.org/uploads/prod/2021/11/ParisCall-WG3-Study-FINAL.pdf .

[8] Microsoft, *Information Sharing and Exchange*, (21.11.2023) https://learn.microsoft.com/en-us/security/gsp/informationsharingandexchange. החברה גם הצהירה שהיא מחלקת תוכנות מטעמה לממשלות להתמודדות עם מתקפות סייבר. ראו: Sean Lyngaas, *Microsoft is giving out free cybersecurity tools after an alleged Chinese hack*, **CNN** (19.7.23), available at: https://edition.cnn.com/2023/07/19/tech/microsoft-free-cybersecurity-tools-china-hack/index.html.

[9] Assaf Lubin, *The Lawfare Podcast: Asaf Lubin on Cyber Espionage and International Law*, **Lawfare** (21.7.23), available at: https://www.lawfaremedia.org/article/the-lawfare-podcast-asaf-lubin-on-cyber-espionage-and-international-law;

[10] Jay Butler, *Corporate Commitment to International Law*, 53 NYU J. INT'L L. & POL. 433, 470 (2021); Brief for Appellant at 33, 51, In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2014) (No. 14-2985-cv); Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 188 (2018).

[11] United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018); Consolidated Appropriations Act, Pub. L. No. 115-141, §§ 103, 105, 132 Stat 1213, 1213-24 (2018).

[12] Microsoft, *In cybersecurity, information is power – Cybersecurity Policy and Resilience Paper*, https://www.microsoft.com/en-us/cybersecurity/content-hub/in-cybersecurity-information-is-power.

שיקולים רחבים אשר על העובד המוסמך להעריך (פרטיות, פגיעה כלכלית ורצף תפקודי), ובהבהרה בסעיף 3(4) כי יינתנו הוראות רק אם הדבר חיוני לאיתור התקיפה, מניעתה או בלימתה.

ועדיין, ישנו מקום לקדם ודאות רבה יותר לגבי אופן הפעלת הסמכות מכוח התזכיר, בכדי להבנות שיתוף פעולה יעיל במהלך התמודדות עם מצבי קיצון דוחקים ועם דילמות שעלולות להתעורר במהלך תקיפת סייבר חמורה. **ראשית**, לא מוגדר כיצד אמור נציג גופי המודיעין – במיוחד ככל שמדובר באיש מחשוב – להביא בחשבון את כלל השיקולים המפורטים בסעיף 2(5), מהי ההיררכיה בין השיקולים וכיצד נכון לאזן בינם. לא מובן מאליו שאדם שאינו משפטן יוכל לעשות זאת, וגם כאשר מדובר במשפטן חשוב לזכור כי לא מדובר באדם עם היכרות מעמיקה עם אופן הפעולה והמבנה של החברה הפרטית אשר את עניינה עליו לשקול.

שנית, חשוב להגדיר כללי משחק ברורים יותר, אגב הבהרת חלוקת הסיכונים והאחריות בין השחקנים הרלוונטיים, במטרה למנוע תקלות בתקשורת ובעיות מעשיות. למשל, התזכיר לא מגדיר מהי חלוקת אחריות בין גופי המודיעין השונים שמוסמכים לפעול מכוח החוק, ולא בטוח שהמגבלה שהוגדרה בסעיף 5 (לפיה רק גוף מודיעין אחד ינחה את החברה הפרטית) תעמוד במבחן מעשי (במובן שניתן לדמיין מצב בו חברה פרטית תצטרך לפעול בשיתוף פעולה עם מספר גופים שלטוניים במקביל). בנוסף, ברמה הטכנית, לא ברור האם הנחיות צריכות להתקבל בכתב (מה שעלול לייצר פתח לפגיעה נוספת בחברות – במקרה של תקיפת סייבר ובצידה הונאה ביחס להפעלת סמכות מכוח החוק המוצע). לבסוף, לא ברורה ההבחנה בתזכיר בין היקפי הסמכות של גופי המדינה והחובה מנגד של חברות פרטיות במהלך השלבים השונים של התמודדות עם תקיפת סייבר, מה שמשאיר פתח לאי הבנות, תקלות בתקשורת ואף לבעיות מעשיות בהתמודדות עם תקיפת סייבר חמורה לאורך תהליך מורכב (זיהוי ובדיקה ראשוני, בלימת האיום, שיקום וניקוי המערכת, חזרה לשגרה).

שלישית, בעוד יש לברך על ההכללה בסעיף 4(ב) המוצע של דרישה למחיקת מידע שהתקבל לאחר סיום הטיפול בתקיפת הסייבר החמורה, למעט מידע חיוני לזיהוי מאפייני התקיפה (אשר יישמר בהיקף המזערי הנדרש), יש מקום לחידוד נוסף ביחס לניהול מידע. למשל, חשוב להגדיר במפורש היכן יישמר מלכתחילה מידע שייאסף כתוצאה מהפעלת הסמכות החריגה, באילו מקרים ניתן יהיה להעביר את המידע שייאסף ממאגר מידע ממשלתי אחד לאחר (אם בכלל), ומהו מועד "סיום הטיפול בתקיפת הסייבר החמורה". לבסוף, ראוי לשקול קביעת סנקציה כלפי גורם שלטוני אשר לא יעמוד בדרישה זו.

רביעית, חשוב לייצר מנגנון שיאפשר התמודדות עם אי הבנות, חילוקי דעות ויצירת קווים מנחים לשיתוף פעולה יעיל בין כל הצדדים המעורבים. המלצתנו היא לשקול מיסוד מנגנון ליישוב אי הסכמה (למשל ביחס להפעלת סמכות מכוח סעיפים 2(5) ו-4(ב) לתזכיר), או אפילו ערעור על החלטה (בטרם מימוש האפשרות של פניה לבית משפט לעניינים מנהליים, בהתאם לסעיף 7 לתזכיר). מנגנון שכזה נחוץ על מנת לאזן בין האינטרסים וההבנה המקצועית של חברות פרטיות (שיכולות שלא להסכים לגבי קיומו של חשש, או אופן ההתמודדות עמו), ובכדי לסמן את הדרך קדימה לשיתוף פעולה יעיל מכוח התזכיר (באמצעות הגדרת קווים מנחים באשר לדילמות שיעלו).

הצעותינו לעיל נובעות מן העובדה שהתזכיר מייצר, במובן רחב, חשש של ערעור מרקם היחסים העדין בין גופים שלטוניים ובין השוק הטכנולוגי הפרטי. נכון להיום, שיתוף הפעולה בין גופי המודיעין לבין חברות פרטיות (בהקשר דנן) הוא בעל אופי וולונטרי, בהתבסס על קידום אינטרסים משותפים, אך בפנינו מעבר למסגרת פטרנליסטית לפיה הגורמים הפרטיים כפופים לגופים המדינתיים באופן מרחיק לכת. ההיגיון מאחורי המצב הקיים נובע מכך שאנו למדים הן מהניסיון המעשי, והן מהמחקרים בתחום, כי מנגנוני שיתוף פעולה וולונטריים בתחום הטכנולוגי מהווים מכפיל כוח.[13] הגדרה מחדש של מנגנון פעולה לא מוסכם עלול ליצור הרתעה בקרב השוק הטכנולוגי במדינת ישראל אשר יש לו חשיבות עצומה מבחינה אסטרטגית, צבאית, מדינית, תדמיתית ועוד, ואף להוביל להתנגדויות שיפגעו בהתמודדות עם האתגר החשוב של תקיפת סייבר חמורה. אמנם, המנגנון המוצע מוגבל מבחינה טמפורלית, אבל לא ניתן לשלול אפשרות שמהלך זה יהפוך לסוג של "פיילוט" במבט קדימה, או שפשוט הזמני יהפוך לקבוע (במסגרת מאבק רב-זירתי, ככל הנראה ארוך ביותר, שמדינת ישראל מובילה נגד חמאס).

ד. <u>סיכום</u>

מטרת החוק המוצע היא חשובה וראויה ביותר, וניכר שנעשתה עבודת מטה מקיפה המבקשת להביא בחשבון אינטרסים שונים ומגוונים, ולהבנות מנגנון מדורג אשר מכבד את האוטונומיה והזכויות של חברות פרטיות. ובכל זאת, ראוי כי התזכיר יקודם תוך שילוב עקרונות של הדדיות, חלוקת סיכונים ויצירת הסכמות גבי שיתופי פעולה, בכדי שלא לפגוע במרקם היחסים שבין גופי השלטון בישראל לבין השוק הטכנולוגי שיש לו חשיבות רבה.

בפרט, אנו מציעים מספר צעדים. **ראשית**, הגברת הוודאות לגבי אופן היישוב בין רשימת השיקולים המובאים בסעיף 2(5), ובמיוחד לגבי ההיררכיה בין השיקולים השונים והאופן הנכון שיש לאזן בינם. **שנית**, הבהרת חלוקת הסיכונים והאחריות בין השחקנים הרלוונטיים, במטרה למנוע תקלות בתקשורת ואף בעיות מעשיות בהתמודדות עם תקיפת סייבר חמורה. **שלישית**, בנוגע לסעיף 4(5), חשוב להגדיר היכן יישמר מידע שייאסף כתוצאה מהפעלת הסמכות מכוח החוק, האם תוקנה סמכות העברת המידע ממאגר מידע ממשלתי אחד לאחר (ככל שזו נחוצה), ומהו מועד "סיום הטיפול בתקיפת הסייבר החמורה". בנוסף, אנו מציעים לשקול סנקציה כלפי גוף מודיעין שלא יעמוד בדרישה למחיקת מידע מכוח סעיף 4(ב) לחוק המוצע. **רביעית**, ראוי לשקול מנגנון יישוב מחלוקות או לערעור (בהליך מקדים לפניה לבית משפט לעניינים מנהליים), ביחס לאי הסכמה על אופן הפעלת הסמכות החריגה מכוח התזכיר.

[13] Anna Bryden et. al., *Volunary agreements between government and business – A scoping review of the literature with specific reference to the Public Health Responsibility Deal*, 110(2-3) HEALTH POL. 186, (2013).

עו"ד עדן פרבר

חוקרת,

תַּכְלִית – המכון למדיניות ישראלית

ד"ר טל מימרן

ראש תכנית,

תַּכְלִית – המכון למדיניות ישראלית