



המכון הישראלי
לדמוקרטיה

www.idi.org.il

18 דצמבר, 2023

ו' טבת, תשפ"ד

לכבוד

ח"כ יולי אדלשטיין

וועדת החוץ והביטחון של הכנסת

א.כ.,

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

ביום 06.12.24 פורסמה הצעת חוק התמודדות עם תקיפת סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד - 2023 (להלן: "הצעת החוק").

הצעת החוק מיועדת להחליף את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד – 2023 (להלן: "תקש"ח סייבר") שאושרו על ידי הממשלה ביום 27.11.23, ומכאן חשיבותה. הדרך הנכונה להתקין הוראות לעניין הגנת סייבר היא בחקיקה ראשית והשימוש בתקנות שעת חירום צריך להיות מוגבל למצב שבו הכנסת אינה מתפקדת. משום כך, אנו מברכות על פרסום הצעת החוק בסמוך לאישורו של תקש"ח סייבר מתוך כוונה להביא לחקיקתה המהירה - בתום תוקפן של תקש"ח סייבר.¹

במהלך מלחמת חרבות ברזל נגלה במרחב הסייבר כמרחב הרביעי ללוחמה. מאז תחילת הלחמה התעצמו תקיפות הסייבר בתדירותן ובמורכבותן והן משמשות כלי להשגת הישגים מבצעיים במרחבי הלוחמה האחרים. לצד זאת, אין בישראל מסגרת חקיקתית מלאה ומקיפה להגנת מרחב הסייבר. בנסיבות אלו, ברורה נחיצותה של הסמכת גופי המדינה הרלוונטיים להתערב בניהול הסיכונים בקרב גופים במגזר הפרטי המשמשים כספקי שירותי אחסון ושירותים דיגיטליים, ובלבד שהתערבות זו מוגבלת ונעשית לשם הגנה על ביטחון המדינה וביטחון הציבור.

אולם, לצד הבנת הצורך בהסמכה כאמור, יש לזכור כי מדובר בהתערבות רחבה וחודרנית של רשויות מדינה בהתנהלותם של גופים פרטיים, מה שמעורר חשש מפני פגיעה בזכויות לקניין ולפרטיות ובאוטונומיה של עסקים. כמו כן, יש בכך פוטנציאל למדרון חלקלק באשר למעורבות המדינה במגזר הסייבר הפרטי, שלה השלכות כלכליות והשלכות על פיתוח טכנולוגי.

עם זאת, לדעתנו, בהתחשב בנחיצות הטיפול בסוגיה, הצעת החוק מציגה הסדר מאוזן המביא בחשבון את ההבדלים בין אסדרת המגזר הציבורי והביטחוני לבין אסדרת המגזר הפרטי:

¹ לפי תקנה 9 לתקש"ח סייבר.

אמיר אלשטיין

יו"ר הוועד המנהל

הנשיא העשירי ראובן ריבלין

יו"ר של כבוד

יוחנן פלסנר

נשיא

ברנד מרכוס

יו"ר בינלאומי

חברי הוועד המנהל

עו"ד ליאת אהרנסון

אלי גרוני

פרופ' ורד וניצקו-טרוס

ד"ר חן ליכטנשטיין

מזל מועלם

שגיר לשעבר סלי מרידור

פרופ' מאריה נאסר אבו-אלהיג'א

עו"ד אבי פישר

ד"ר מיכל צור

יוסי קוצניק

המועצה הבינלאומית

פרופ' רונלד דניאלס, יו"ר

השופטת רוזלי סילברמן אבלה, קנדה

אליזא אברמס, ארה"ב

שגיר לשעבר מרטין אינדיק, ארה"ב

אן אפלכאוס, ארה"ב

פרופ' ורנון בוגדנו, בריטניה

השופטת דורית ביניש, ישראל

השופט סטיבן ברייד, ארה"ב

השופט סלים ג'ובראן, ישראל

ד"ר ג'וזף ג'ופה, גרמניה

פרופ' משה הלברטל, ישראל

פרופ' מייקל וולצר, ארה"ב

פרופ' רוברט מנוקין, ארה"ב

פרופ' כריסטוף מקשיט, גרמניה

השופט אברהם סופר, ארה"ב

ברט סטפנס, ארה"ב

פרופ' ארווין קוטלר, קנדה

פרופ' גרהרד קספר, ארה"ב

פרופ' יהודה ריינהרץ, ארה"ב

פרופ' גבריאלה שלו, ישראל

סגני נשיא

פרופ' סוזי נבות, מחקר

פרופ' חרנית פלוג, מחקר

ד"ר ישי ג'סיין פרס, אסטרטגיה

עמיתים בכירים

פרופ' איתי אטר

פרופ' תמר הרמן

פרופ' נתן זוסמן (אורח)

פרופ' עמיחי כהן

פרופ' יותם מרגלית

פרופ' דניאל סטטמן

פרופ' בני פורת

פרופ' יובל פלדמן

פרופ' מרדכי קרמניצר

פרופ' גדעון רהט

ד"ר תהילה שוורץ אלטשולר

פרופ' יובל שני

מייסדים

ד"ר אריק ברמון

מזכיר המדינה ג'ורג' שולץ (1920-2021)



המכון הישראלי לדמוקרטיה

(1) הגופים עליהם חלות הוראות הצעת החוק מוגדרים באופן שקוף וברור יחסית, כ"ספקי שירותי אחסון או שירותים דיגיטליים", וזאת לעומת יצירת רשימה חסויה שהוצעה בנוסח הקודם.²

(2) הצעת החוק מבחינה בין ענייני צבא וביטחון "טהורים" לבין תקיפות סייבר על המגזר הפרטי והאזרחי, לרבות תשתיות קריטיות אזרחיות. ההבחנה נעשית באמצעות הגבלת סמכות המלמ"ב לספקים של משרד הביטחון ו"מפעלי מערכת הביטחון" שהם מפעלים המייצרים מוצרים עבור מערכת הביטחון כפי שיוגדרו בצו על ידי שר הביטחון,³ דבר שמוותר את הטיפול במגזר הפרטי בידי מערך הסייבר ושב"כ. הצעת החוק גם קובעת כי את שיתופי הפעולה ומאבקי הסמכות ינהלו הגופים המפקחים באופן פנים-ממשלתי, ולא מול לקוח הקצה שאליו יוכל לפנות רק גוף אחד לצורך מתן הוראות.

(3) סמכות מתן ההוראות לגופים האזרחיים – הספקים – מוגבלת לנסיבות של חשש ממשי לתקיפת סייבר חמורה המוגדרת באופן ברור ומוגבל. ההגדרה שמה את הדגש על האדוות וההשלכות העלולות להתעורר כתוצאה מגילוי של תקיפת סייבר חמורה אצל ספק ספציפי, ולא רק על האירוע הנקודתי.⁴ הגדרת "תקיפת סייבר חמורה" היא אמנם רחבה אבל מתבססת על הגדרות מוכרות בחקיקה דומה ובהצעות קודמות. ייתכן שבתום המלחמה יהיה מקום לחדד אותה יותר.

(4) הפעלת הסמכות למתן הוראות היא הדרגתית.

א. תחילה ניתנת לספק הזדמנות להסביר כיצד הוא פועל על מנת להתמודד עם התקיפה או לחילופין להצהיר כי מערכותיו פועלות בהתאם לסטנדרט אבטחה אמריקני מוכר.⁵ העובדה שאימוץ תקינה טכנולוגית בינ"ל מעניקה חסינות למפוקחים, מהווה תמריץ יעיל לתעשייה לנהל את סיכוני הסייבר באופן אחראי ומאוזן. זהו בדיוק הכיוון הנכון גם לאסדרה טכנולוגית עתידית.

ב. רק אם הספק אינו מספק תצהיר כאמור או שאינו נוקט פעולות הולמות לדעת העובד המוסמך, אזי קמה לעובד הסמכות למתן הוראות. אולם, גם אז עליו לתת לספק הזדמנות להשמיע את טענותיו בטרם יחויב בביצוע ההוראות.⁶

(5) התחשבות בשיקולי מידתיות, פרטיות ועלות: בעת קבלת החלטה בדבר מתן ההוראות ותוכן ניתן משקל לזכות לפרטיות, לשיקולי מידתיות, לעלות הכלכלית הכרוכה ביישום

² ראו הגדרת המונחים "ספק", "שירותי אחסון" ו"שירותים דיגיטליים" בסעיף 1 להצעת החוק.

³ ראו הגדרת המונח "עובד מוסמך" בסעיף 1 להצעת החוק.

⁴ ראו הגדרת המונחים "תקיפת סייבר" ו"תקיפת סייבר חמורה", סעיף 2 והרישא של סעיף 3 להצעת החוק.

⁵ סעיף 3(2), (3) הצעת החוק.

⁶ סעיף 3(4) להצעת החוק.



ההוראות ולהשלכותיהן על פעילותו הרציפה של הספק ושל צדדים שלישיים.⁷ התחשבות בשלושת טיפוסים השיקולים האלה יוצרת מעגל הגנה נכון – חוקתי, חוקי ועסקי.

(6) שקיפות: הצעת החוק קובעת כי יש להעביר אל המפוקח תשתית עובדתית ומקצועית, ככל האפשר, כבר בעת היידוע הראשוני בדבר חשש ממשי לתקיפת סייבר חמורה. יש להעביר גם הודעה על כוונה לתת הוראות, וגם אם ניתן להעביר אליו הוראות בעל פה, יש למסור לו תיעוד בכתב תוך פרק זמן סביר ממתן ההוראה.⁸ לתפיסתנו, שקיפות מול המפוקח היא הדרך הנכונה ביותר ליצור איזון מול הרשות המעניקה הוראות והיא עדיפה על פני סודיות ודיווח רק לגורמי פיקוח-על. מכל מקום, הצעת החוק כוללת גם חובת דיווח ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת.⁹

(7) שימוע וערעור: למפוקח ניתנת הזדמנות להשמיע את טענותיו קודם לקבלת החלטה בדבר מתן הוראות, וכן ניתנת אפשרות לערער על ההוראות הניתנות לו בפני בית המשפט לעניינים מינהליים.¹⁰

על אף היות ההסדר המוצע בהצעת החוק מאוזן, חשוב לדעתנו לתת את הדעת לנושאים המפורטים להלן על מנת לשפרו ולתת מענה מלא לחששות אפשריים:

1. פרום הדיון

הצעת החוק עוסקת ברגולציה של גופים אזרחיים ומעוררת חשש מפני פגיעה בזכויות לקניין ולפרטיות ובאוטונומיה של עסקים. כמו כן, יש בכך פוטנציאל למדרון חלקלק באשר למעורבות המדינה במגזר הסייבר הפרטי, שלה השלכות כלכליות והשלכות על פיתוח טכנולוגי. על מנת להתמודד עם חששות אלו ולאינם ראוי יהיה לקיים את הדיון בהצעת החוק באופן שקוף ופתוח לציבור. הטלת חיסיון על הדיונים בהצעת החוק מנוגדת לאופיו של מערך הסייבר כגוף אזרחי ולצורך לאמץ נורמות התנהלות המתאימות לעבודה עם גופים אזרחיים.

2. חלוקת סמכויות ברורה בין השב"כ לבין מערך הסייבר

הצעת החוק מסמיכה בסמכות זהה עובד מוסמך ממערך הסייבר ומהשב"כ - להודיע לספק שירותי איחסון או שירותים דיגיטליים אודות חשש לתקיפת סייבר חמורה ולתת לו הוראות בנושא.¹¹ עוד מובהר, וטוב שכך תוקן בהצעת החוק לעומת הנוסח שהוצע בתזכיר החוק,¹² כי

⁷ סעיף 3(5)(א),(ב) להצעת החוק.

⁸ סעיפים 3(1), (4), ו-4 להצעת החוק.

⁹ סעיף 7 להצעת החוק.

¹⁰ סעיפים 3(4), 9 להצעת החוק.

¹¹ בהתאם להגדרות המונחים "עובד מוסמך", "ספק", "שירותי איחסון" ו"שירותים דיגיטליים" בסעיף 1 להצעת החוק, והוראות סעיפים 2 ו-3 להצעת החוק לעניין הסמכות.



הפעלת הסמכות כלפי ספק לעניין תקיפה מסוימת או לעניין כמה תקיפות המתרחשות באותו המועד, תעשה על ידי עובד מוסמך מקרב גוף אחד בלבד. כלומר, לכאורה, לא יתכן מצב בו ספק יקבל במקביל הוראות הן מהשב"כ והן ממערך הסייבר.¹³ אולם, מצב בו מתקיים מירוך סמכויות בין שני גופים ממשלתיים אינה מצב מקובל בהתנהלות למול גופים אזרחיים והצעת החוק אינה מפרטת מהו המנגנון לפיו מתבצעת חלוקת הסמכויות וכיצד ימנע מצב בו מפוקח יקבל בתקופה מסוימת הוראות מגוף אחד וכעבור תקופת זמן יאלץ להתמודד עם הוראותיו ונורמות ההתנהלות של גוף אחר. ככל שחלוקת הסמכויות בין השב"כ למערך הסייבר ברורה ראוי שתפורט באופן ברור בהצעת החוק.

3. דיווח לרשות להגנת הפרטיות

הצעת החוק ממוקדת באיתור תקיפת סייבר חמורה, כהגדרתה בסעיף 1 להצעת החוק, מניעתה או בלימתה ומטיל על מערך הסייבר, השב"כ ומלמ"ב חובה לדווח ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת על מקרים בהם ניתנו הוראות לספק שירותי איחסון או שירותים דיגיטליים בהתאם להוראות הצעת החוק.¹⁴ אולם, תקיפת סייבר חמורה עלולה להוביל לפגיעה במידע אישי. לעיתים איסוף המידע האישי אודות אזרחי המדינה הוא אחת ממטרות תקיפת הסייבר, ככלי ליצירת קשר ישיר עם האזרחים, כחלק מלוחמת תודעה או מתוך ניסיון לפגוע בעורף.¹⁵ משום כך, לדעתנו, לצד הדיווח ליועצת המשפטית לממשלה ולוועדת חוץ וביטחון, יש לחייב גם במתן הודעה לראש הרשות להגנת הפרטיות על מנת שהרשות תחל בחקירת תקיפת הסייבר, תבחן את רמת הגנת הפרטיות שננקטה על ידי הספק ואת הצורך במתן מידע לציבור נושאי המידע במידת האפשר, בהתאם לתקנות אבטחת מידע. היעדר ממשק בין החקיקה הזאת לבין חוק הגנת הפרטיות ותקנות אבטחת מידע עלול להוביל לבעיות בהמשך ואנו מציעות לטפל בכך כבר עכשיו.

4. הערה צופה פני עתיד – טיפול בשרשראות אספקה

לפי מחקר של פורום הכלכלה העולמי (World Economic Forum), 39% מהארגונים במגזר הפרטי נפגעו מתקיפות סייבר על צדדים שלישיים בשרשרת האספקה שלהם. מתקיפות סייבר על גופים בשרשראות אספקה היוו את הגורם השני בחשיבותו לתקיפות סייבר בשנת 2021. אולם, למרות חשיבותם הגדולה בהגנת סייבר, הרי שב 66% מתקיפות הסייבר על ספקים בשרשראות אספקה, הספקים לא ידעו או לא נקטו בשקיפות בנוגע להיותם מותקפים. כתוצאה מכך, קרוב ל-62% מתקיפות סייבר על לקוחותיהם של ספקים בשרשראות אספקה נגרמו עקב

¹² סעיף 5 תזכיר חוק התמודדות עם תקיפת סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023 (להלן: "התזכיר").

¹³ סעיף 5 להצעת החוק.

¹⁴ סעיף 7 להצעת החוק.

¹⁵ ראו, למשל, ממצאיה של חברת גוגל בעקבות מלחמת רוסיה אוקראינה. Google's Threat Analysis Group (TG), *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (Feb. 2023).



המכון הישראלי לדמוקרטיה

האמון שנתנו הלקוחות בספקים.¹⁶ נוכח הסיכון הגובר עקב חולשת גורמים שונים בשרשראות אספקה הטילו באיחוד האירופי על ארגוני תשתיות קריטיות להתמודד עם סיכוני הסייבר הנובעים מספקים בשרשראות אספקה, במטרה להביא, בין השאר, להטמעת הגנת סייבר נאותה על ידי הספקים עצמם.¹⁷ בארה"ב נדרשות סוכנויות ורשויות פדרליות לפעול רק לפי קווים מנחים להגנת סייבר שחוברו בתהליך שיתוף פעולה בין המגזר הציבורי לבין המגזר הפרטי. לפי קווים מנחים אלו, על הרשויות והסוכנויות הפדרליות להתקשר רק עם חברות תוכנה הפועלות לפי סטנדרטים מוכרים לפיתוח תוכנה מאובטחת, זאת במסגרת אסטרטגיית "אפס האמון" של הממשל.¹⁸

בישראל, אין אסדרה בחקיקה של פעילות מערך הסייבר ובכלל זה גם נושא הגנת סייבר בשרשראות אספקה אינו מאוסדר. בתום המלחמה ראוי שנושא זה יטופל באופן מקיף על מנת להגביר את חוסן הסייבר בישראל.

סיכום ההמלצות:

לדעתנו, ההסדר המוצע בהצעת החוק מאוזן וממוקד יחסית. עם זאת, יש לדעתנו להבהיר את הנושאים הבאים:

1. לקיים את כלל הדיונים בהצעת החוק באופן פתוח ושקוף לציבור ולא להטיל עליהם חיסיון. זאת בהתאם לנומרות ההתנהלות המצופות מגוף ממשלתי המאסדר גופים אזרחיים.
2. חלוקת סמכויות ברורה בין מערך הסייבר לבין השב"כ על מנת להגביר את הבהירות והשקיפות למול המגזר האזרחי, אשר יש בה כדי להשפיע במישרין על נכונותו לשתף פעולה עם גורמים אלו.

¹⁶ Enisa, Good Practices for Supply Chain Cybersecurity, 4 (June 2023)
¹⁷ סעיף 21 ל 14 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
¹⁸ NIST ;Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)
;Special Publication (SP) 800-218 , *Secure Software Development Framework (Version 1.1)*
NIST, *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e* (Feb. 4, 2022)



המכון הישראלי לדמוקרטיה

3. הכללת הרשות להגנת הפרטיות בקרב הגופים המדווחים, על מנת לאפשר לה להתחיל בחקירה בהתאם לסמכויותיה לשם הגנה על הזכות לפרטיות ועל אינטרס הציבור במקרה של תקיפת סייבר שמעורב בה דלף מידע פרטי.

נשמח לעמוד לרשותכם בכל עניין שיידרש,

בכבוד ובברכה

ד"ר תהילה שוורץ אלטשולר

ד"ר רחל ארידור הרשקוביץ,

ג'ה'ה א'ת'ס'ה'ר

כ'ה' א'ר'י'ד'ו'ר ה'ר'ש'ק'ו'ב'י'ץ

התוכנית לדמוקרטיה בעידן המידע

המכון הישראלי לדמוקרטיה

העתק:

- עו"ד ליאת גורפינקל, יועמ"ש מערך הסייבר הלאומי.
- עו"ד גלעד סממה, ראש הרשות להגנת הפרטיות.