טיוטת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מספר 4), התשפ"ו-2026 – הסמכת ועדת שרים לענייני חקיקה

הצעת להחלטה

מחליטים:

א. לאשר עקרונית את טיוטת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 4), התשפ"ו-2026 (להלן – **טיוטת החוק**), המצורפת.

ב. להסמיך את ועדת השרים לענייני חקיקה לאשר על דעת הממשלה את נוסחה הסופי של טיוטת החוק.

דברי הסבר

רקע כללי

מתחילת הלחימה במסגרת מבצע "חרבות ברזל", החל מיום 7 באוקטובר 2023, ניכרת עלייה בהיקף ובעוצמה של תקיפות הסייבר כנגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלו היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עלולות להוביל לפגיעה בחיי אדם. תקיפות סייבר אלו, לפי עמדת גורמי המקצוע, הולכות והופכות מתוחכמות ומורכבות יותר.

ספקים רבים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שהם מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות למשרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות, ארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שעשוי להיגרם מתקיפה כנגד ספקים אלה עלול להתפשט ולהשפיע על חברות רבות במשק. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או לפגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום 27 בנובמבר 2023, את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, ובסמוך לכך, ביום 26 בדצמבר 2023 חוקק החוק אשר החליף את תקנות שעת החירום: חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023 (להלן – **החוק**). החוק הוארך שלוש פעמים וכן תוקן ביום 14 באוגוסט 2025, תיקון אשר כלל את ניתוק הזיקה של החוק לפעולות הצבאיות המשמעותיות שעל נקיטתן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה, בסמוך לאחר אירועי השבעה באוקטובר, כך שהפעלת הסמכויות מכוח החוק לא תהא תלויה במצב הלחימה במסגרת חרבות ברזל. החוק בתוקף עד ליום 31 בינואר 2026.

נוכח מאפייניו הייחודיים של מרחב הסייבר ולנוכח ההערכות המקצועיות של גופי הביטחון (להלן – **הגופים**) באשר לחומרת איומי הסייבר במגזר השירותים הדיגיטליים והסיכונים הנשקפים מהם, עמדת הגופים היא כי יש צורך לשמר את הסמכויות והכלים הנדרשים לצורך ההתמודדות עם תקיפות במרחב הסייבר שנקבעו בחוק. הסמכויות והכלים החיוניים, אשר נקבעו בחוק לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור ומניעת פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור. על כן, ובמקביל להשלמת עבודת מטה לקידום הסדר קבע במסגרת חוק הגנת הסייבר הלאומית, מוצע להאריך את תוקפה של הוראת השעה לתקופה של שנה נוספת, עד ליום 31 בינואר 2027. כמו כן, מוצע תיקון טכני הנדרש בנוסח סעיף 8 לחוק לעניין דיווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת כהתאמה לתיקונים קודמים שכבר בוצעו בחוק.

נתונים כלכליים וההשפעה על משק המדינה

א. בהסתמך על הערכות ואומדנים של טווחי ההשפעה הכלכלית מכיוונים שונים וכן על מחקרים ודוחות מהמקובלים בעולם בתחום, הנזקים הרחבים מתקיפות סייבר, במצב שגרה, במדינת ישראל, מוערכים בכ-12 מיליארד ₪ בשנה.

ב. נתח התוצר השנתי של ספקי שירותי אחסון ושירותים דיגיטליים שהפדיון השנתי שלהם מתחת ל-100 מלש"ח, המוגדרים כעסקים קטנים ובינוניים בסקטור, נאמד בכ-50 מיליארד ₪ בשנה, המהווה כ-2.4% מהתוצר הישראלי.

ג. מאחר שקיים מתאם גבוה בין שווי הנזק של תקיפת סייבר לערך הכלכלי של הארגון, ניתן להניח כי קיים קשר חזק בין סך הנזק של תקיפות סייבר במדינת ישראל (שחושב על בסיס התוצר הישראלי) לנתח התוצר של ספקי שירותי אחסון ושירותים דיגיטליים.

ד. הנחה זו היא שמרנית, שכן מידת ההשפעה של הסקטור על נזקי סייבר רחבים צפויה להיות גבוהה מסקטורים אחרים (כגון קמעונאות) עקב היותו שרשרת אספקה דיגיטלית בסקטורים אחרים.

ה. בהמשך לכך ובהסתמך על אומדנים נוספים, ניתן להעריך שעבור מדינת ישראל מדובר בנזק פוטנציאלי של מאות מיליוני ש"ח בשנה עבור סקטור זה במצב שגרה ואף גבוה יותר במצב מלחמה עקב גידול בתקיפות.

נוכח כל האמור לעיל, בשל הדחיפות המתחייבת, ועל מנת לזרז את הליך החקיקה, מוצע לאשר עקרונית את טיוטת החוק בהתאם לנוסח שצורף להצעת ההחלטה, ולהסמיך את ועדת השרים לענייני חקיקה לאשר את נוסחה הסופי של הצעת החוק שתוגש לכנסת, וזאת על דעת הממשלה.

תקציב

אין.

השפעת ההצעה על מצבת כח האדם

לא רלוונטי.

עמדת שרים אחרים שההצעה נוגעת לתחום סמכותם

אין.

החלטות קודמות של הממשלה בנושא

החלטה מספר חק/654 של ועדת השרים לענייני חקיקה מיום 5.12.2023, אשר קיבלה תוקף של החלטת ממשלה ביום 5.12.2023 מספרה הוא 1117(חק/654)

החלטה מספר חק/1018 של ועדת השרים לענייני חקיקה מיום 19.5.2024, אשר קיבלה תוקף של החלטת ממשלה ביום 27.5.2024 ומספרה הוא 1774 (חק/1018)

החלטה מספר חק/1769 של ועדת השרים לענייני חקיקה מיום 9.3.2025, אשר קיבלה תוקף של החלטת ממשלה ביום 9.3.2025 ומספרה הוא 2858 (חק/1769)

החלטה מספר חק/2103 של ועדת השרים לענייני חקיקה מיום 14.7.2025, אשר קיבלה תוקף של החלטת ממשלה ביום 15.7.2025 ומספרה הוא 3238 (חק/2103)

<u>עמדת היועץ המשפטי של המשרד יוזם ההצעה</u>

מצורפת.

<u>סיווגים</u>

סיווג ראשי: 07חקיקה ממשלתית;

תחום פעולה עיקרי: 01 חוץ וביטחון

מגיש: ראש הממשלה

י"ב בטבת התשפ"ו
1 בינואר 2026

ירושלים, י"ב בטבת התשפ"ו
1 בינואר 2026
סימוכין: 7941216590

חוות דעת משפטית הנלווית להצעת החלטה לממשלה ולוועדות השרים

נושא הצעת ההחלטה:

טיוטת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מספר 4), התשפ"ו-2026 – הסמכת ועדת שרים לענייני חקיקה

תמצית ההצעה בהתייחס להיבטיה המשפטיים:

כמפורט בדברי ההסבר להצעת ההחלטה, מאז תחילת הלחימה במסגרת מבצע "חרבות ברזל", החל מיום 7 באוקטובר 2023, ניכרת עלייה בהיקף ובעוצמה של תקיפות הסייבר כנגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלו היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עלולות להוביל לפגיעה בחיי אדם. תקיפות סייבר אלו, לפי עמדת גורמי המקצוע, הולכות והופכות מתוחכמות ומורכבות יותר.

כפי שמצוין בדברי ההסבר להצעת ההחלטה, ספקים רבים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שהם מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות למשרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות, ארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שעשוי להיגרם מתקיפה כנגד ספקים אלה עלול להתפשט ולהשפיע על חברות רבות במשק. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או לפגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום 27 בנובמבר 2023, את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, ובסמוך לכך, ביום 26 בדצמבר 2023 חוקק החוק אשר החליף את תקנות שעת החירום – חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023 (להלן – **החוק**). החוק הוארך שלוש פעמים וכן תוקן ביום 14 באוגוסט 2025, תיקון אשר כלל את ניתוק הזיקה של החוק מהפעולות הצבאיות המשמעותיות, כך שהפעלת הסמכויות מכוח החוק לא תהא תלויה במצב הלחימה. החוק בתוקף עד ליום 31 בינואר 2026.

נוכח מאפייניו הייחודיים של מרחב הסייבר ולנוכח ההערכות המקצועיות של גופי הביטחון (להלן – **הגופים**) באשר לחומרת איומי הסייבר במגזר השירותים הדיגיטליים והסיכונים הנשקפים מהם, עמדת הגופים היא כי יש צורך לשמר את הסמכויות והכלים הנדרשים לצורך ההתמודדות עם תקיפות במרחב הסייבר שנקבעו בחוק. לעמדתם, הסמכויות והכלים החיוניים, אשר נקבעו בחוק לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור ומניעת פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור. על כן, ובמקביל להשלמת עבודת מטה לקידום הסדר קבע במסגרת חוק הגנת הסייבר הלאומית, מוצע להאריך את תוקף החוק לתקופה של שנה נוספת, עד ליום 31 בינואר 2027. כמו

כן, מוצע תיקון טכני הנדרש בנוסח סעיף 8 לחוק לעניין דיווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, כהתאמה לתיקונים קודמים שכבר בוצעו בחוק.

נוכח כל האמור לעיל, בשל הדחיפות המתחייבת, ועל מנת לזרז את הליך החקיקה, מוצע לאשר עקרונית את טיוטת החוק בהתאם לנוסח שצורף להצעת ההחלטה, ולהסמיך את ועדת השרים לענייני חקיקה לאשר את נוסחה הסופי של הצעת החוק שתוגש לכנסת, וזאת על דעת הממשלה.

קשיים משפטיים, ככל שישנם, ודרכי פתרונם:

חוק יסוד: כבוד האדם וחירותו קובע שורה של זכויות מוגנות אשר אין פוגעים בהן אלא בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שאינה עולה על הנדרש. ההסדר המעוגן בחוק, שאת תקפו מבוקש להאריך, עלול לפגוע בזכויות מוגנות אלו, לרבות בחופש הקניין של הספקים, וכן בזכותם לפרטיות של לקוחות וצדדים שלישיים נוספים, ועל כן עליו לעמוד בתנאים שנקבעו בחוק היסוד.

תכלית התיקון, שאינו כולל שינוי מהותי של החוק, אלא מאריך את תוקפו, לצד תיקון טכני כאמור לעיל, היא לאפשר המשך הפעלה של הכלים והסמכויות שנחקקו לצורך הגנה מפני תקיפת סייבר חמורה שעלולה לפגוע בביטחון המדינה, ביטחון הציבור או לפגוע באופן חמור ברציפות אספקת שירותים חיוניים לציבור. תכלית זו היא ראויה וקשורה בקשר ישיר עם ההסדר המוצע. זאת, בשים לב למצב במרחב הקיברנטי, ונוכח הערכת הגורמים המקצועיים, כפי שמצוין בדברי ההסבר להצעת החלטה, בדבר היקף ועוצמת מתקפות הסייבר כנגד גופים אזרחיים במשק הישראלי, כחלק מהמתקפה המשולבת המכוונת כנגד מדינת ישראל, וקיומו של צורך מקצועי לשמר את הכלים החיוניים אשר הוקנו במסגרת החוק לצורך התמודדות עם תקיפות סייבר, וזאת במקביל להמשך עבודת המטה לגיבוש חוק הגנת הסייבר הלאומית, אשר נמצאת בשלבים מתקדמים.

בחוק נקבעו מספר מנגנונים שמטרתם להבטיח שהכלים והסמכויות שהוקנו במסגרתו יופעלו באופן מידתי, ושהפגיעה בזכויות תהיה מצומצמת ככל הניתן. בין היתר, בטרם מתן הוראות להתמודדות עם התקיפה, ניתנת לספק הזדמנות לפעול באופן הולם לאיתור התקיפה, מניעתה או בלימתה; בנוסף, במסגרת מתן הוראות לספק נדרש לשקול את השפעתן האפשרית על הזכות לפרטיות, על פעילות הספק ועל צד שלישי, וכן את העלות הכלכלית המוערכת של יישום ההוראות ואת השפעתן האפשרית על הרציפות התפקודית של הספק. עתה כאמור מוצע להאריך את תוקפו של החוק לתקופה של שנה נוספת, כאשר בהקשר זה יובהר, כי אין בתיקון המוצע כדי לגרוע מכלל המנגנונים שנקבעו לשם צמצום הפגיעה בזכויות.

עמדת היועצים המשפטיים של משרדים אחרים שהצעת ההחלטה נוגעת להם:

הצעת ההחלטה תואמה עם היועצים המשפטיים של מערך הסייבר הלאומי, מערכת הביטחון ושירות הביטחון הכללי.

עמדת היועץ המשפטי של המשרד שהשר העומד בראשו מגיש את ההצעה:

בשים לב לכל האמור לעיל, אין מניעה משפטית לאישור הצעת ההחלטה.

אורלי פישמן אורן, עו"ד
משנה ליועצת המשפטית

רח' קפלן 3, הקריה, ירושלים 91919, טל: 02-6705463, פקס: 02-5605008
3 Kaplan St. Jerusalem 91919, Tel: +972 (2) 6705463, Fax: +972 (2) 5605008

טיוטת חוק

א. שם החוק המוצע

חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 4), התשפ"ו-2026

ב. מטרת החוק המוצע, הצורך בו, עיקרי הוראותיו והשפעתו על הדין הקיים

מתחילת הלחימה במסגרת מבצע "חרבות ברזל" (להלן – חרבות ברזל), ביום כ"ב בתשרי התשפ"ד (7 באוקטובר 2023), ניכרת עלייה בהיקף ובעוצמה של תקיפות הסייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עלולות להוביל לפגיעה בחיי אדם. תקיפות הסייבר, לפי עמדת גורמי המקצוע, הולכות והופכות מתוחכמות ומורכבות יותר. ספקים רבים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שהם מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות למשרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות, ארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שעשוי להיגרם מתקיפה כנגד ספקים אלה עלול להתפשט ולהשפיע על חברות רבות במשק. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או לפגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום י"ד בכסלו התשפ"ד (27 בנובמבר 2023), את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, ובסמוך לכך, ביום י"ד בטבת התשפ"ד (26 בדצמבר 2023) חוקק החוק אשר החליף את תקנות שעת החירום – חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023 (להלן – הוראת השעה).

הוראת השעה הוארכה שלוש פעמים וכן תוקנה ביום כ' באב התשפ"ה (14 באוגוסט 2025), תיקון אשר כלל את ניתוק הזיקה של הוראת השעה לפעולות הצבאיות המשמעותיות, והיא בתוקף עד ליום י"ג בשבט התשפ"ו (31 בינואר 2026).

נוכח מאפייניו הייחודיים של מרחב הסייבר ולנוכח ההערכות המקצועיות של הגופים באשר לחומרת איומי הסייבר במגזר השירותים הדיגיטליים והסיכונים הנשקפים מהם, עמדת הגופים היא כי יש צורך לשמר את הסמכויות והכלים הנדרשים לצורך ההתמודדות עם תקיפות במרחב הסייבר שנקבעו בחוק. הסמכויות והכלים החיוניים, אשר נקבעו בחוק לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור ומניעת פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור. על כן, ובמקביל להשלמת עבודת מטה לקידום הסדר קבע במסגרת חוק הגנת הסייבר הלאומית, מוצע להאריך את תוקפו של החוק לתקופה נוספת של שנה, עד יום כ"ג בשבט התשפ"ז (31 בינואר 2027). כמו כן, מוצע תיקון טכני הנדרש בסעיף הדיווח כהתאמה לתיקונים שכבר בוצעו בחוק.

ג. להלן נוסח טיוטת החוק המוצעת ודברי הסבר

הצעת חוק מטעם הממשלה:

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 4), התשפ"ו-2026

תיקון סעיף 8	1.	בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), התשפ"ד- 2023[1] (להלן – החוק העיקרי), בסעיף 8(א), בפסקה (4), במקום "פגיעה בקיום האספקה והשירותים החיוניים" יבוא "פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור".
תיקון סעיף 12	2.	בסעיף 12 לחוק העיקרי, במקום "עד יום י"ג בשבט התשפ"ו (31 בינואר 2026)" יבוא "עד יום כ"ג בשבט התשפ"ז (31 בינואר 2027)".

דברי הסבר

כללי מתחילת הלחימה במסגרת מבצע "חרבות ברזל" (להלן – חרבות ברזל), ביום כ"ב בתשרי התשפ"ד (7 באוקטובר 2023), ניכרת עלייה בהיקף ובעוצמה של תקיפות הסייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עלולות להוביל לפגיעה בחיי אדם. תקיפות הסייבר, לפי עמדת גורמי המקצוע במערך הסייבר הלאומי, בשירות הביטחון הכללי (להלן – שב"כ) ובממונה על הביטחון במערכת הביטחון (להלן – מלמ"ב), הולכות והופכות מתוחכמות ומורכבות יותר.

ספקים רבים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שהם מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות למשרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות, ארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שעשוי להיגרם מתקיפה כנגד ספקים אלה עלול להתפשט ולהשפיע על חברות רבות במשק. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או לפגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום י"ד בכסלו התשפ"ד (27 בנובמבר 2023), את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023 (להלן – תקנות שעת החירום הראשונות), ובסמוך לאחר מכן, ביום י"ד בטבת התשפ"ד (26 בדצמבר 2023) פורסם ברשומות חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023 (להלן – החוק), אשר החליף את תקנות שעת החירום הראשונות. יצוין כי החוק הוארך שלוש פעמים בחוק

---

[1] ס"ח התשפ"ד, עמ' 410; התשפ"ה, עמ' 798.

התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון), התשפ"ד-2024, מיום י"ז בתמוז התשפ"ד (23 ביולי 2024), בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 2), התשפ"ה-2025, מיום ב' בניסן התשפ"ה (31 במרץ 2025), וכן בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 3), התשפ"ה-2025, מיום כ' באב התשפ"ה (14 באוגוסט 2025), במסגרתו גם תוקן החוק, כך שהוא עומד בתוקף עד יום י"ג בשבט התשפ"ו (31 בינואר 2026).

החוק מסמיך מנהל מוסמך במערך הסייבר הלאומי, בשב"כ או במלמ"ב (להלן – הגופים), וכן את ראש חטיבת ההגנה בסייבר בצבא ההגנה לישראל, לקבוע כי תקיפת סייבר היא תקיפת סייבר חמורה, אם יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה או בביטחון הציבור, או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור; ובהמשך לכך – נתונה לעובד מוסמך באחד הגופים הסמכות להודיע לספק, כהגדרתו בחוק, על קיומו של חשש לתקיפת סייבר חמורה כנגדו או באמצעותו. אם הספק הנתקף לא הגיש תצהיר לפי החוק, וכן לא פעל באופן הולם ובתוך פרק זמן סביר שניתן לו לטיפול בתקיפת הסייבר החמורה, מסמיך החוק את העובד המוסמך לתת לספק הנתקף הוראות לצורך איתור התקיפה, מניעתה או בלימתה, תוך שהחוק קובע תנאים למתן ההוראות כאמור.

ביום י"ז בסיוון התשפ"ה (13 ביוני 2025) החלה המערכה מול איראן, במסגרת מבצע "עם כלביא", וזאת בעקבות החלטתה מאותו היום של ועדת השרים לענייני ביטחון לאומי על נקיטת פעולות צבאיות משמעותיות לפי סעיף 40 לחוק-יסוד: הממשלה. לנוכח המערכה נגד איראן והערכת הגופים באשר לחומרת איומי הסייבר והסיכונים הנשקפים מהם, ועל רקע הצורך המבצעי הדחוף בהקניית סמכויות וכלים חיוניים נוספים לשם התמודדות עם אותם איומים, הותקנו ביום כ"ז בסיון התשפ"ה (23 ביוני 2025) תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025 (להלן – תקנות שעת החירום השניות).

ביום כ' באב התשפ"ה (14 באוגוסט 2025) פורסם ברשומות חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 3), התשפ"ה-2025 (להלן – תיקון מס' 3) שתיקן את החוק, האריך את תוקפו עד יום י"ג בשבט התשפ"ו (31 בינואר 2026) וביטל את תקנות שעת החירום השניות. במסגרת התיקון עוגנו בחוק הכלים הנוספים אשר הותקנו בתקנות שעת החירום השניות, ועיקרם סמכות מנהל מוסמך לדרוש מספק להציג לו כל ידיעה או מסמך הנדרשים לשם בחינת התקיימותם של התנאים לקביעה כי תקיפת סייבר היא תקיפת סייבר חמורה; חובת דיווח של ספק למנהל מוסמך על תקיפת סייבר משמעותית נגדו; וחובת ספק הנתקף בתקיפת סייבר חמורה ליידע ארגון מקושר אשר עלול להיפגע מן התקיפה באופן ישיר וממשי. נוסף על כך, התיקון ניתק את הזיקה של החוק לפעולות הצבאיות המשמעותיות, שעל נקיטתן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה, בסמוך לאחר אירועי השבעה באוקטובר, כך שהפעלת הכלים והסמכויות מכוח החוק לא תלויה במצב הלחימה במסגרת חרבות ברזל.

סעיף 1 במסגרת תיקון מס' 3, תוקן סעיף 2 לחוק כך שנקבע בו כי מנהל מוסמך רשאי לקבוע כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי עומדת להתרחש היא תקיפת סייבר חמורה, אם מצא כי יש חשש ממשי שיש בה "כדי לפגוע בביטחון המדינה או בביטחון הציבור, או לפגוע באופן חמור ברציפות אספקתם

של שירותים חיוניים לציבור". בהמשך לתיקון האמור, נדרש תיקון טכני מקביל בנוסח סעיף 8 לחוק לעניין דיווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת על קביעות מנהל מוסמך לפי סעיף 2, כך שסעיף הדיווח יתאים לתיקון שנעשה בסעיף 2 לחוק.

סעיף 2 לנוכח מאפייניו הייחודיים של מרחב הסייבר ולנוכח ההערכות המקצועיות של הגופים באשר לחומרת איומי הסייבר במגזר השירותים הדיגיטליים והסיכונים הנשקפים מהם, עמדת הגופים היא כי יש צורך לשמר את הסמכויות והכלים הנדרשים לצורך ההתמודדות עם תקיפות במרחב הסייבר שנקבעו בחוק. הסמכויות והכלים החיוניים, אשר נקבעו בחוק לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור ומניעת פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור. על כן, ובמקביל להשלמת עבודת מטה לקידום הסדר קבע במסגרת חוק הגנת הסייבר הלאומית, מוצע להאריך את תוקפו של החוק לתקופה נוספת של שנה, עד יום כ"ג בשבט התשפ"ז (31 בינואר 2027).