רשומות

הצעות חוק

ה ממ ש ל ה

י׳ באדר התשפ״ה | 1849 | 10 במרץ 2025

עמוד

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס׳ 2), התשפ״ה–2025 664

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס׳ 2), התשפ״ה–2025

תיקון סעיף 12

1. בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, התשפ״ד–2023[1], בסעיף 12, במקום ״עד יום ב׳ בניסן התשפ״ה (31 במרץ 2025)״ יבוא ״עד יום ט׳ בחשוון התשפ״ו (31 באוקטובר 2025)״.

דברי הסבר

כללי ביום כ״ב בתשרי התשפ״ד (7 באוקטובר 2023), פתחו ארגוני טרור במתקפה רצחנית נגד כוחות הביטחון ואזרחי מדינת ישראל. מתקפה זו גבתה את חייהם של מאות אזרחים ושיבשה את מערך החיים בחזית ובעורף במדינה. בעקבות מתקפה זו הכריז שר הביטחון, באותו היום, על מצב מיוחד בעורף, מכוח סמכותו לפי סעיף 9ג(ב)(1) לחוק ההתגוננות האזרחית, התשי״א–1951. בהתאם לסעיף 9ג(א)(5) לאותו חוק, החליטה ועדת החוץ והביטחון של הכנסת, ביום כ״ז בתשרי התשפ״ד (12 באוקטובר 2023), לאשר את ההכרזה בשטחה של כל מדינת ישראל, והכרזה זו מוארכת מזמן לזמן. כמו כן, הוכרז בצבא הגנה לישראל (להלן – צה״ל) על מבצע ״חרבות ברזל״, וועדת השרים לענייני ביטחון לאומי החליטה על נקיטת פעולות צבאיות משמעותיות בהתאם לסעיף 40 לחוק־יסוד: הממשלה, והודיעה לגביהן לוועדת החוץ והביטחון של הכנסת ביום כ״ג בתשרי התשפ״ד (8 באוקטובר 2023) (להלן – הפעולות הצבאיות המשמעותיות).

במהלך תקופת הפעולות הצבאיות המשמעותיות המתמשכות מאז המועד האמור, ניכרת עלייה בהיקף ובעוצמה של תקיפות סייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, גם בכלכלה ובתפקודו התקין של המשק הישראלי. תקיפות סייבר עלולות להביא לפגיעה במרחב הסייבר, לפגיעה בעולם הפיזי (למשל פגיעה במערכות רפואיות או בתשתיות אנרגיה), לפגיעה קשה בתפקוד המשק, ואף לפגיעה בחיי אדם. תקיפות הסייבר הולכות והופכות מתוחכמות יותר, ותוצאותיהן קשות יותר ומורכבות יותר לטיפול.

חברות המספקות שירותים דיגיטליים ושירותי אחסון, כהגדרתם בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ״ד–2023 (להלן – החוק), מתאפיינות בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות משרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות, ארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שנגרם מתקיפת חברות אלה עלול להתפשט ולהשפיע על חברות רבות במשק.

נוסף על כך, למרות רגישותן וחשיבותן המשקית של חברות אלה, אין כיום גורם ממשלתי האמון על הסדרת פעילותן בכל הנוגע להגנת הסייבר. לעניין חברות כאמור המחזיקות או מעבדות מידע אישי, קיימת הסדרה של פעילות זו על ידי הרשות להגנת הפרטיות במשרד המשפטים. בנסיבות אלה, ספקים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר. בייחוד בתקופת הלחימה הנוכחית, תקיפות סייבר חמורות נגד ספקים אלה עלולות להביא לפגיעה רחבה בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים.

כדי להתמודד עם הקושי 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). בסמוך לאחר מכן, ביום י״ד בטבת התשפ״ד (26 בדצמבר 2023), פורסם ברשומות החוק אשר החליף את תקנות שעת החירום. החוק נחקק כהוראת שעה למשך שבעה חודשים מיום פרסומו, וביום י״ז בתמוז התשפ״ד (23 ביולי 2024), הוארכה תקופת תוקפו עד יום ב׳ בניסן התשפ״ה (31 במרץ 2025) (ראו: חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון), התשפ״ד–2024 (ס״ח התשפ״ד, עמ׳ 1098)).

החוק מסמיך עובד מוסמך במערך הסייבר הלאומי, בשירות הביטחון הכללי או בממונה על הביטחון במערכת הביטחון (להלן – הגופים) להודיע לספק על קיומו של חשש לתקיפת סייבר חמורה נגדו, ובהמשך לכך, במקרים מסוימים, לתת לספק הנתקף הוראות לצורך איתור התקיפה, מניעתה או בלימתה. הכול, במטרה לאפשר התמודדות עם התגברות והתעצמות תקיפות הסייבר אגב הלחימה המתמשכת במסגרת הפעולות הצבאיות המשמעותיות ובמהלכן.

[1] ס״ח התשפ״ד, עמ׳ 410 ועמ׳ 1098.

דברי הסבר

החוק קובע תנאים ושלבים מפורטים ומדורגים להפעלת הסמכות למתן הוראות לספק, וכן קובע הוראות לעניין תוכן ההוראות לספק. מבנה זה של ההסדר בא להבטיח כי הוראות כאמור יינתנו רק בהתקיים תקיפת סייבר חמורה, כהגדרתה בחוק, ובנסיבות שבהן ספק לא פעל באופן הולם ובתוך פרק זמן סביר שניתן לו לטיפול בתקיפת הסייבר החמורה ולא הגיש תצהיר בדבר יישום הנחיות אבטחה בתקן רלוונטי כקבוע בחוק. כמו כן, מבנה זה של ההסדר נועד להבטיח שיינתנו רק ההוראות החיוניות הנחוצות להתמודדות עם תקיפת הסייבר החמורה.

כמפורט בדברי ההסבר להצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023 (הצ"ח הממשלה, התשפ"ד, עמ' 358), הנחת העבודה של גורמי הממשלה הנוגעים בדבר, ערב חקיקת החוק, הייתה שלאחר חקיקתו מרבית הספקים יטפלו בתקיפת סייבר חמורה באופן הולם, בוודאי בעת לחימה, ואם יבקשו זאת, יינתנו להם סיוע והכוונה על ידי הגופים. בה בעת, החוק נועד להקנות סמכות, בתקופת החירום הכרוכה בפעולות הצבאיות המשמעותיות, לתת הוראות לספקי שירותים דיגיטליים או שירותי אחסון שלא יפעלו כך, לנוכח הנסיבות והסיכונים שפורטו לעיל.

הניסיון שהצטבר בתקופה שחלפה מאז חקיקת החוק, מאשש את הנחת העבודה המתוארת לעיל. מאז נחקק החוק, חל שיפור ניכר בהתמודדות ספקים עם תקיפות סייבר חמורות. ספקים שבוצעה נגדם תקיפת סייבר חמורה ועודכנו על כך, טיפלו בתקיפה באופן הולם ובפרק זמן סביר כמוגדר בחוק, לעיתים בסיוע והכוונה מצד הגופים, ובהתאם לכך, עד כה לא נדרשה הפעלת הסמכות למתן הוראות מכוח סעיף 3(4) לחוק.

כמו כן, הניסיון שהצטבר בתקופה זו מלמד על חשיבותו של החוק ועל כך שההסדר שנקבע בו, ובכלל זה תהליך הפעלת הסמכות והבניית שיקול הדעת, הוא מאוזן ומידתי. כך, הסמכות מופעלת רק כאשר האינטרס הציבורי מחייב זאת.

יודגש כי במקביל לעלייה המשמעותית בהיקפי התקיפות, ניכרת מגמה ברורה של החמרה בסוג ובחומרה של התקיפות כלפי מרחב הסייבר הישראלי ובעיקר כלפי ספקי שירותי אחסון ושירותים דיגיטליים. בתקופת אירועי הלחימה, ובייחוד בתקופה שחלפה מאז הוארך תוקפו של החוק, התרחשו תקיפות סייבר משמעותיות נגד ספקים במגזר השירותים הדיגיטליים שבשלהן גם הוכרזה תקיפת סייבר חמורה בהתאם לחוק. ההתעצמות, הכוונות והניסיונות של התוקפים בתקופה זו, מחייבים לפעול בצורה המהירה והיעילה ביותר מול מגזר זה. לפיכך, ובשל כל המפורט לעיל, קיים צורך מבצעי ממשי להאריך את תוקפו של החוק כמוצע בהצעת חוק זו.

סעיף 1 כאמור, החוק נקבע כהוראת שעה ועומד בתוקף עד יום ב' בניסן התשפ"ה (31 במרץ 2025). בשל הימשכות הפעולות הצבאיות המשמעותיות, על הסיכונים והאתגרים של הסייבר הכרוכים במצב לחימה זה כמפורט בחלק הכללי של דברי ההסבר, ובמטרה לאפשר המשך התמודדות עם תקיפות סייבר במגזר השירותים הדיגיטליים ושירותי האחסון במצב לחימה זה, ובשים לב לאיזונים הקבועים בחוק כפי שפורטו, מוצע להאריך את תקופת תוקפו של החוק כך שהוא יעמוד בתוקף עד יום ט' בחשוון התשפ"ו (31 באוקטובר 2025). יודגש כי לפי סעיף 2 לחוק, אחד התנאים לכך שמנהל מוסמך יוכל לקבוע כי תקיפת סייבר מסוימת היא תקיפת סייבר חמורה, הוא שהתקיפה התרחשה במהלך תקופת הפעולות הצבאיות המשמעותיות, כך שאם תקופה זו תסתיים לפני תום תקופת הארכת התוקף המוצעת, ממילא לא יהיה ניתן להפעיל את הסמכות מכוח החוק, גם אם החוק עצמו יהיה בתוקף. מכאן שבפועל, הנפקות המשפטית של ההארכה המוצעת מוגבלת לתקופת ההארכה או לתקופת הפעולות הצבאיות המשמעותיות, לפי התקופה שתסתיים ראשונה.