



רשומות

הצעות חוק

ה מ מ ש ל ה

27 במאי 2024

1754

י"ט באייר התשפ"ד

עמוד

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון
(הוראת שעה – חרבות ברזל) (תיקון) (הארכת תוקף), התשפ"ד-2024 1004

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון) (הארכת תוקף), התשפ"ד–2024

תיקון סעיף 12 1. בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023¹, בסעיף 12, במקום "עד תום שבעה חודשים מיום פרסומו" יבוא "עד יום ב' בניסן התשפ"ה (31 במרץ 2025)".

ד ב ר י ה ס ב ר

נוסף על כך למרות רגישותן וחשיבותן המשקית של חברות אלה, אין כיום גורם ממשלתי האמון על הסדרת פעילותן בכל הנוגע להגנת הסייבר. לעניין חרבות ברזל כאמור המחזיקות או מעבדות מידע אישי, קיימת הסדרה של פעילות זו על ידי הרשות להגנת הפרטיות. 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 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). ובסמוך לכך, ביום י"ד בטבת התשפ"ד (26 בדצמבר 2023) חוקק החוק אשר החליף את תקנות שעת החירום. החוק מסמיך עובד מוסמך במערך הסייבר הלאומי, בשירות הביטחון הכללי או במלמ"ב (להלן – הגופים) להודיע לספק על קיומו של חשש לתקיפת סייבר חמורה נגדו, ובהמשך לכך, במקרים מסוימים, לתת לספק הוראות לצורך איתור התקיפה, מניעתה או בלימתה. הכול במטרה לאפשר התמודדות עם התגברות והתעצמות מתקפות הסייבר אגב הלחימה המתמשכת במסגרת הפעולות הצבאיות המשמעותיות ובהלכן. החוק קובע תנאים שונים ושלבם מפורטים ומדורגים עד למתן הוראות לספק, וכן קובע הוראות לעניין ההוראות לספק עצמן, כל זאת, במטרה להבטיח כי הוראות כאמור יינתנו רק בהתקיים תקיפת סייבר חמורה בהגדרתה בחוק, ובנסיבות שבהן ספק לא פעל באופן הולם ובתוך פרק זמן סביר שניתן לו לטיפול בתקיפת הסייבר החמורה, או לא הגיש תצהיר בדבר יישום הנחיות אבטחה בתקן רלוונטי בקובע בחוק; כמו כן, במטרה להבטיח כי כאשר יינתנו הוראות, יינתנו רק ההוראות החיוניות והשקולות הנחוצות להתמודדות עם תקיפת הסייבר החמורה.

בל"ל 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 ושייבה את מערך החיים בחזית ובעורף במדינה. בעקבות מתקפה זו הכריז שר הביטחון, באותו היום, על מצב מיוחד בעורף, מכוח סמכותו לפי סעיף 99(ג)(ב)(1) לחוק ההתגוננות האזרחית, התשי"א–1951. בהתאם לסעיף 99(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).

במסגרת הפעולות הצבאיות המשמעותיות המתמשכות מאז המועד האמור, מתגברות ומתעצמות 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 לגרום 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 גופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות וארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שנגרם מתקיפה כנגד חברות אלה עלול להתפשט ולהשפיע על חברות רבות במשק.

¹ ס"ח התשפ"ד, עמ' 410.

דברי הסבר

מופעלת סמכות לצורך הגנה, רק כאשר האינטרס הציבורי, בשים לב למצב הלחימה, מחייב זאת.

סעיף 1 בשים לב לאמור בחלק הכללי לדברי ההסבר, לנוכח מטרות החקיקה, לנוכח המשך מצב הלחימה, על סיכוני ואתגרי הסייבר הכרוכים בו והצורך המבצעי לאומי הנגזר מכך, כדי לאפשר המשך התמודדות חיונית עם תקיפות סייבר במגזר השירותים הדיגיטליים ושירותי האחסון במצב לחימה זה, ובשים לב לאיזונים הקבועים בחוק כפי שפורטו, מוצע להאריך את הוראת השעה עד יום ב' בניסן התשפ"ה (31 במרץ 2025). יודגש כי לפי סעיף 2 לחוק, אחד התנאים המצטברים להפעלת סמכותו של מנהל מוסמך לקבוע כי תקיפת סייבר מסוימת היא תקיפת סייבר חמורה, הוא התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות; כך שאם תסתיים תקופת הפעולות הצבאיות המשמעותיות לפני תום התקופה המוצעת, ממילא לא יהיה ניתן להפעיל את הסמכות מכוח החוק, גם אם החוק עצמו יעמיד בתוקפו. מכאן שמשמעות ההארכה המתבקשת בפועל, לנוכח נוסח החוק, היא לתקופה של ההארכה המוצעת או עד תום "חרבות ברזל", לפי המוקדם.

כפי שנכתב בדברי ההסבר להצעת החוק (הצ"ח הממשלה – 1688, התשפ"ה, עמ' 358) עוד טרם חקיקתו, הנחת העבודה של גורמי הממשלה הנוגעים בדבר הייתה שלאחר חקיקתו, מרבית הספקים יטפלו באופן הולם בתקיפת הסייבר החמורה, בוודאי בעת לחימה, ואם יבקשו אף יינתן להם סיוע והכוונה על ידי הגופים. בה בעת, החקיקה נועדה להקנות סמכות, בתקופת החירום הכרוכה בפעולות הצבאיות המשמעותיות, לתת הוראות לספקי שירותים דיגיטליים או שירותי אחסון אשר לא יפעלו כך, נוכח הנסיבות והסיכונים שפורטו כאמור.

התקופה שחלפה מאז חקיקת החוק, מאששת את הנחת העבודה האמורה. בתקופת החוק ועד למועד זה חל שיפור ניכר בהתמודדות ספקים עם תקיפות סייבר חמורות. ספקים אשר כלפיהם בוצעה תקיפת סייבר חמורה ועודכנו על כך, טיפלו בתקיפה באופן הולם ובפרק זמן סביר כמוגדר בחוק, לעיתים תוך שניתן להם סיוע והכוונה על ידי הגופים, ובהתאם עד כה לא נדרש מתן הוראות מכוח סעיף 3(4) לחוק.

בתקופה זו אוששה חשיבות החוק והאיזון המידתי הקבוע בו וכן הבניית התהליך ושיקול הדעת, שלפיהם

