המכון הישראלי
לדמוקרטיה

www.idi.org.il

אמיר אלשטיין
יו"ר הוועד המנהל
הנשיא העשירי ראובן ריבלין
יו"ר של כבוד
יוחנן פלסנר
נשיא

חברי הוועד המנהל
עו"ד ליאת אהרנסון
פרופ' ורד וניצקי-סרוסי
ד"ר חן ליכטנשטיין
מזל מועלם
שגריר לשעבר סלי מרידור
פרופ' פאדיה נאסר אבו-אלהיג'א
עו"ד אבי פישר
ד"ר מיכל צור
יוסי קוצ'יק

המועצה הבינלאומית
פרופ' רונלד דניאלס, יו"ר
השופטת רוזלי סילברמן אבלה, קנדה
אן אפלבאום, ארה"ב
השופטת דורית בינישׁ, ישראל
השופט סטיבן ברייר, ארה"ב
פרופ' משה הלברטל, ישראל
פרופ' כריסטוף מרקשיס, גרמניה
ד"ר שרון נזריאן, ארה"ב
השופט אברהם סופר, ארה"ב
ברט סטפנס, ארה"ב
פרופ' גרהרד קספר, ארה"ב
האורייט שלייפר, ארה"ב

סגני נשיא
פרופ' סוזי נבות, מחקר
ד"ר ישי [ג'סי] פרס, אסטרטגיה

עמיתים בכירים
פרופ' תמר הרמן
פרופ' נתן זוסמן [אורח]
פרופ' עמיחי כהן
מר תומר לוטן [אורח]
פרופ' יותם מרגלית
פרופ' דניאל סטטמן
פרופ' בני פורת
פרופ' קרנית פלוג
פרופ' מרדכי קרמניצר
פרופ' גדעון רהט
ד"ר תהילה שוורץ אלטשולר
פרופ' יובל שני

מייסדים
ד"ר אריק כרמון
ברנרד מרכוס [1929-2024]
מזכיר המדינה ג'ורג' שולץ [1920-2021]

י"ג אדר, תשפ"ו

02 מרץ 2026

לכבוד

עו"ד ליאת גורפינקל כהנים

היועצת המשפטית

<u>מערך הסייבר הלאומי</u>

באמצעות: <u>אתר התזכירים הממשלתי</u>

ג.נ.,

הנדון: **<u>תזכיר חוק הגנת הסייבר הלאומית, התשפ"ו – 2026</u>**

ביום 22 בינואר, 2026 פורסם תזכיר חוק הגנת הסייבר הלאומית, התשפ"ו – 2026 (להלן: "התזכיר"). התזכיר, מסמך ההשוואה הבינלאומית ומסמך ה-RIA המצורפים אליו, משקפים עבודת הכנה מקיפה ומשמעותית. התזכיר מביא בחשבון את כשלי השוק הנלווים להגנת הסייבר בישראל ובעולם,[1] לצד מאפייני מרחב הסייבר וצרכי הביטחון הייחודיים של מדינת ישראל, ומציג מסגרת לאסדרת הגנת הסייבר הלאומית ופיקוח עליה במתווה "ביזורי מנוהל".

לצד יתרונותיו התזכיר מעורר מספר שאלות וקשיים, עליהם נרצה להצביע בחוות דעתנו.

חלק א' לחוות הדעת עוסק בהיבטים המבניים של התזכיר ומתווה האסדרה המוצע בו, תוך בחינת השלכות אפשריות על הסמכויות המוקנות בו לגורמים שונים, ממעוף הציפור. **חלק ב'** עוסק בחובות המוטלות על ארגונים במגזרי המשק. **חלק ג'** דן בסמכויות המוקנות למערך הסייבר הלאומי ולרשויות המוסמכות ובמספר הוראות פרטניות. **חלק ד'** מציג את עיקרי המלצותינו.

נשמח לעמוד לרשותכם בכל עניין,

בכבוד ובברכה

ד"ר רחל ארידור הרשקוביץ — ד"ר תהילה שוורץ אלטשולר

התוכנית לדמוקרטיה בעידן המידע, המכון הישראלי לדמוקרטיה

---

[1] רחל ארידור הרשקוביץ, תהילה שוורץ אלטשולר ועידו סיון סביליה, *מהו סייבר? חלק א: על מרחב הסייבר, תקיפות סייבר והגנת סייבר* (מחקר מדיניות 171, **המכון הישראלי לדמוקרטיה**, אוקטובר 2021), עמ' 30-27.

העתק:

- עו"ד גלעד סממה, ראש הרשות להגנת הפרטיות.
- עו"ד אביטל סמפולינסקי, המשנה ליועצת המשפטית לממשלה למשפט ציבורי-חוקתי.
- עו"ד לירון מאוטנר לוגסי, ראש אשכול פרטיות ומידע, ייעוץ וחקיקה (ציבורי – חוקתי), משרד המשפטים.
- תא"ל (מיל) יוסי כראדי, ראש מערך הסייבר הלאומי

<u>תקציר</u>

מדינת ישראל נתונה תחת איומי סייבר הולכים וגוברים. מלחמת "חרבות ברזל" לוותה כבר מתחילתה בעלייה ניכרת בתקיפות הסייבר נגד ארגונים וחברות בישראל, ובמחצית הראשונה של שנת 2025 מדינת ישראל אף דורגה בין שלוש המדינות המותקפות ביותר בעולם במרחב הסייבר.

על אף איומי הסייבר הגוברים, הגנת הסייבר במדינת ישראל היא חלקית, אינה מעוגנת בחוק יחיד ואחיד העוסק בהגנת מרחב הסייבר, ומנוהלת על ידי מספר גופים הפועלים במקביל. תשתיות קריטיות מונחות על ידי השב"כ, המלמ"ב ומערך הסייבר הלאומי (מס"ל); משרדי ממשלה מונחים על ידי יה"ב, וארגונים מהמגזר הפרטי שאינם תשתיות קריטיות, מונחים רק במידה והם כפופים לרגולטור מגזרי בתחום פעולתם ובהתאם להחלטתו.

לפיכך האסדרה והפיקוח על הגנת הסייבר הם מורכבים. הממשלה ויחידות הסמך שלה מאוסדרות על ידי יה"ב. גופי תמ"ק כפופים לשב"כ, למלמ"ב ולמס"ל, אולם רמת הגנת הסייבר שלהם ואופן ביצועה נסתר מהעין. ארגונים מהמגזר הפרטי שנתונים לאסדרה מגזרית של משרד ממשלתי כלשהו כפופים להנחיית יחידות הסייבר המגזריות ברגולטורים המגזריים. אולם, רמת הגנת הסייבר הנדרשת על ידי הרגולטורים המגזריים אינה אחידה וכן יש שונות בפעילותן של היחידות המגזריות.

כתוצאה מכך, ארגונים פרטיים שאינם גופי תמ"ק ואינם מאוסדרים בשגרה על ידי רגולטור מגזרי כלשהו או שהרגולטור המגזרי אינו מטיל עליהם דרישות בתחום הגנת הסייבר, אינם נתונים בכלל תחת רגולציית הגנת סייבר. בנוסף, גם במקומות לגביהם קיימת אסדרה, חסרים תמריצים או סנקציות. מצב זה טומן בחובו מגוון סכנות מבחינת רמת הגנת הסייבר הלאומית בישראל, עליהן הצביע מבקר המדינה לאורך השנים.

מתוך היכרות עם החוסרים העמוקים בהגנת מרחב הסייבר בישראל, ובמטרה לבלום ולטפל במתקפות סייבר על חברות המעניקות שירותים דיגיטליים ומחוברות לגופים רבים במשק, לרבות מערכות החיוניות לביטחון המדינה ולתפקוד המשק, חוקקה ממשלת ישראל בדצמבר 2023 את חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד – 2023.

אולם, הוראת השעה אינה מספקת פתרון ארוך טווח לבעייתיות הקיימת באסדרה החסרה של הגנת הסייבר במדינת ישראל. נדרשת אסדרת הגנת סייבר מקיפה בישראל שעקרונותיה צריכים להיות:

א. אסדרה ביזורית המותאמת למאפייניו וצרכיו של כל מגזר משק.
ב. אסדרה דינמית דיה כדי להשתנות בעת הצורך ובייחוד בהתקיים שינויים טכנולוגיים.
ג. אסדרה המספקת תמריצים לארגונים פרטיים ולמשרדי הממשלה לציית להוראות הגנת הסייבר הרלוונטיות להם.
ד. אסדרה המעגנת באופן בהיר את פעילותן של יחידות הסייבר המגזריות ומעניקה להן כלי פיקוח ואכיפה מותאמים לצרכי הגנת סייבר.

תזכיר חוק הגנת הסייבר הלאומית, התשפ"ו – 2026 משקף לפיכך אסדרה נחוצה ביותר של הגנת הסייבר בישראל. המתווה המוצע בו משקף "אסדרה ביזורית מנוהלת", ומבקש להציג רגולציה מותאמת לצורך בביזוריות אך בה בעת גם להכרח בפיקוח על פעולותיהן של היחידות המגזריות ויצירת מסגרת אחידה והוליסטית להגנת סייבר בכלל המשק. המתווה מכיר בחשיבותם של הרגולטורים המגזריים, מסדיר את סמכויותיהם ואף נותן בידיהם אמצעי אכיפה מינהליים. בה בעת,

המתווה מכיר בחסרונות אסדרה ביזורית מלאה, הן בשל הפערים שהיא עלולה ליצור והן בשל הקושי להפעיל אותה במצבי קיצון. לכן, המתווה מעניק למערך הסייבר הלאומי סמכויות לפיקוח מסוים על הרגולטורים המגזריים בשגרה באמצעות הנחיה מקצועית של היחידות המגזריות. ההנחיה המקצועית של היחידות המגזריות המוסדרת בתזכיר[2] אינה דומה לזו הניתנת לפי החוק להבטחת הביטחון בגופים ציבוריים,[3] שכן היא לא ניתנת לארגון מסוים המוגדר בגוף מונחה, אלא ממוענת ליחידה המגזרית האמונה על הגנת הסייבר ברשות המוסמכת. במודל כזה של הנחיה מקצועית מחייבת, גוף מרכזי קובע סטנדרטים, מתודולוגיות ועקרונות יישום אחידים, על מנת להבטיח רמת הגנה מינימלית אחידה ולמנוע פערי אכיפה, והגופים הסקטוריאליים שומרים על אוטונומיה תפקודית והעצמאות הרגולטורית שלהם נשמרת.

בנוסף, התזכיר מקנה למס"ל סמכויות לניהול הגנת הסייבר הלאומית בעת תקיפות סייבר חמורות או סיכון משמעותי להן. זאת נוכח יכולותיו הייחודיות של מס"ל, מומחיותו בתחום הגנת הסייבר, היותו גורם מקשר למול גורמי ביטחון כגון צה"ל והשב"כ, ויכולתו לגבש תמונת מצב לאומית כוללת של איומי הסייבר וצרכי ההגנה באופן דינמי ומהיר.

לדעתנו מתווה אסדרה זה הוא נכון, מאוזן ומתאים לצרכי הגנת הסייבר הלאומיים. הוא אינו מציג מודל של "רגולטור-על", שהוצע בתזכיר החוק הקודם שפרסם מערך הסייבר בשנת 2018, וסברנו כי הוא משקף הסדר שגוי. מנגד, הוא משמר בידי מס"ל סמכויות חיוניות, נוכח מאפייניה הביטחוניים של מדינת ישראל והאיומים הנשקפים לה ממרחב הסייבר. ההסדר המוצע בתזכיר דומה במידה רבה לזה הנהוג במרחבים אחרים בישראל וגם במדינות המערב, ובראשן מדינות האיחוד האירופי בהתאם לדירקטיבת NIS2. לכן, טענות לפיהן מדובר בפגיעה חמורה בתעשייה, אינן הגיוניות, בייחוד ככל שמדובר בתעשיות הטכנולוגיה הכפופות גם כך לדרישות תאימות מצד הרגולציה האירופית.

עם זאת, לדעתנו יש מקום לשפר ולתקן את התזכיר במספר נושאים:

1. **שקיפות ועצמאות מערך הסייבר :** מערך הסייבר הלאומי הוא רגולטור ייחודי המאסדר את המגזר הציבור אך גם את המגזר הפרטי. כבזה יש לפעול להגברת שקיפות פעולותיו כאמצעי להגברת אמון הציבור בו. כן יש לספק בידו כלים לפעולה עצמאית גם למול משרדי הממשלה אותם הוא מאסדר.
2. **הרגולטור המגזרי:** המבנה הארגוני של הרגולטור המגזרי המעוגן בחוק הוא מורכב ואינו בהיר מספיק. יש להבהיר שהיחידה המגזרית בכל רשות מוסמכת היא בעלת המומחיות בתחום הגנת הסייבר ועל כן החלטות בתחום זה צריכות להתקבל על ידה. במקביל יש לצמצם את סמכות ההחלטה הבלעדית של הגורם המאסדר שהוא השר. זאת על מנת למזער את הסיכון ליחסי קח-תן עם ארגונים פרטיים. כן יש לבחון הוספת מגזרים נוספים שאינם מנויים כיום ברשימת מגזרי המשק, כמו, למשל, מגזר הפיננסים והביטוח. לחילופין יש לספק בידי מס"ל כלים לבחינת מדיניות הגנת הסייבר במגזרים שאינם מנויים על מגזרי המשק לשם הבטחת התאמתה לצורכי הגנת הסייבר הלאומית ועדכונה מעת לעת.
3. **התזכיר אינו כולל תמריצים מספקים לנקיטת רמת הגנת סייבר ראויה, על כן, לדעתנו:**

---

[2] סעיף 5 לתזכיר חוק הגנת הסייבר הלאומית, התשפ"ו – 2026 (להלן: "התזכיר").
[3] סעיף 10 לחוק להסדרת הביטחון בגופים ציבוריים, לעיל ה"ש 17.

א. יש להחיל את מודל האכיפה המינהלית ובראשו העיצומים הכספיים גם על משרדי ממשלה ורשויות מקומיות.
ב. יש להרחיב את אחריות נושאי המשרה בארגון גם לנקיטת רמת הגנת סייבר מתאימה בעת שגרה.
ג. יש להרחיב את מודל הפטור מחובות לפי התזכיר במקרה של אימוץ תקינה טכנולוגית בינלאומית מוכרת ומחייבת, למגזרים נוספים מאלה המנויים בתזכיר.

תיקונו של התזכיר כמוצע על ידנו יקל גם על הוכחת עמידתו בדרישות האיחוד האירופי בנושא התרת פגיעה בפרטיות על ידי רשויות אכיפת חוק וביטחון, ושמירה על ההכרה בתאימות הדין הישראלי מול הדין האירופי.

פירוט המלצותינו נמצא בטבלה בסוף המסמך.

1. מבוא

מדינת ישראל נתונה תחת איומי סייבר הולכים וגוברים. מלחמת "חרבות ברזל" לוותה כבר מתחילתה בעלייה ניכרת בתקיפות הסייבר נגד ארגונים וחברות בישראל,[4] ובמחצית הראשונה של שנת 2025 מדינת ישראל אף דורגה בין שלוש המדינות המותקפות ביותר בעולם במרחב הסייבר.[5]

מבין תקיפות הסייבר החמורות שהתרחשו מפרוץ המלחמה ניתן למנות את תקיפת הסייבר שהתרחשה באמצע חודש נובמבר 2023 על חברת Signature-IT המספקת פתרונות לקנייה מקוונת ושירותי אחסון לאתרים. תקיפה זו בוצעה על פי הדיווחים על ידי קבוצת האקרים פרו-חמאסית המכונה Cyber Toufan Operation. מומחים סבורים שקבוצה זו בעלת יכולות גבוהות כשל מדינה. רק שבועות אחרי חשיפתה החלו להתברר פרטים אודות חומרת התקיפה, שהובילה לפגיעה משמעותית במשרדי ממשלה וחברות וארגונים גדולים במשק, להשבתת אתרי האינטרנט שלהם במהלך תקופת הקניות של חודש נובמבר, ולדלף מידע אישי.

כך, למשל, אתר האינטרנט של חברת "שפע אונליין" שסיפקה שירותי רכישה מקוונת מענקית הריהוט "איקאה" הפסיק את פעילותו לחלוטין, החנות המקוונת של חברת "הום סנטר" לא היתה זמינה במשך מספר שבועות, כמו גם החנויות המקוונות ומערכות המיחשוב של חברות כגון קרביץ, קל גב וכתר פלסטיק; אתר המנויים של רשות הטבע והגנים; מערכות המיחשוב ומאגרי המידע של חברות כמו חברת התעופה ישראייר, אסם, טויוטה ישראל, פיליפ מוריס, יונילוור, קוקה קולה וחברת הסייבר ראדוור. בחלק מן החברות האלה גם דלף מידע אישי אודות לקוחותיהן לרשת האינטרנט, וכך פורסמו כשלושה מיליון רשומות שהכילו לפחות שמות, כתובות דוא"ל, מספרי טלפון, כתובות מגורים ואף ארבע ספרות אחרונות של כרטיסי אשראי. בנוסף, טענו התוקפים גם לפגיעה במאגרי המידע של משרד העבודה והרווחה, משרד הבריאות, רשות החדשנות ומערכת התשלומים הממשלתית. עוד נפגע ארכיון המדינה ואתר האינטרנט שלו שב לפעילות חלקית רק כעבור שנתיים, בדצמבר 2025.[6]

---

[4] שירי חביב ולדהורן, *"מזהים יותר תקיפות סייבר כנגד ארגונים וחברות בישראל"*, **גלובס** (16.10.2023).

[5] Microsoft, *Microsoft Digital Defense Report 2025: Lighting the path to a secure future* (2025), בעמ' 10.

[6] רפאל קאהאן, *האקרים פרצו לאתרים של חברות גדולות, נתונים אישיים של מיליונים דלפו לרשת*, **Ynet** (19/11/2023); סתיו נמר, *אתר הום סנטר נפגע; האקרים: פרצנו גם לאתר ישראייר*, **מעריב** (17/11/2023); מערכת ICE, *רמי לוי בצרות: ישראייר תחת מתקפת סייבר חמורה*, **ICE** (16/11/2023); דניאלה גינזבורג, *המלחמה הקשטה: מתקפת סייבר על חברות ישראליות, האקרים תוקפים את נכסי חמאס ואיראן*, **ישראל היום** (19/11/2023); רפאל קאהאן, *מתקפת סייבר אותרה בחברת "ראדוור"*, **Ynet** (20/11/2023); איתמר מינמר ושי רינגל, *האקרים פרצו ל-Radware, מחברות הסייבר הוותיקות בישראל*, **N12** (21/11/2023); ינון בן שושן, *איקאה בהודעה ללקוחות: ייתכן שמידע אישי שלכם דלף*, **וואלה** (04/12/2023); מעריב אונליין, *מתקפת סייבר באתר ארכיון המדינה: "משבשת את שירותי החיפוש והעיון"*, **מעריב** (08/12/2023); מערכת 12N, *מתקפת סייבר באתר ארכיון המדינה: "מידע רב נמחק"*, **N12** (08/12/2023); עמרי ברק, *בשבועות האחרונים: אחת ממתקפות הסייבר הגדולות ביותר בתולדות המדינה*, **N12** (11/12/2023); יוסי הטוני, *אלה החיים? – ארכיון המדינה נפרץ בסייבר*, **אנשים ומחשבים** (11/12/2023).

תקיפות סייבר משמעותיות נוספות בשנים האחרונות בישראל נגעו לבתי חולים ולקופות חולים בישראל. כך, בסוף חודש נובמבר 2023 דווח על תקיפת סייבר על בית החולים זיו בצפת. על פרטי התקיפה הוטל צו איסור פרסום והובהר שהתקיפה נבלמה ולא הביאה לפגיעה במטופלים, אך היא גרמה לדלף מידע רפואי חסוי. בעמוד הטלגרם של קבוצת ההאקרים האיראנית שלקחה אחריות על התקיפה, נטען כי יש בידה למעלה מ-500 גיגה-בייט של מידע הכולל 700 אלף מסמכים רפואיים, מתוכם 100 אלף של חולים הקשורים לצה"ל.[7] בסוף דצמבר 2023 דווח על חשד לתקיפת סייבר על בית החולים בנהריה ועל בית החולים פוריה בטבריה, ובתחילת פברואר 2024 דווח על ניסיון לתקיפת סייבר נגד בית החולים רמב"ם בחיפה.[8] משרד הבריאות מצידו הבהיר שארגוני הבריאות חווים תקיפות סייבר מידי יום, אך מרכז הסייבר של משרד הבריאות מצליח לבלום כמעט את כולן.[9]

גל נוסף של תקיפות סייבר כוון אל עיריות ומועצות מקומיות, והוביל לשיבוש משמעותי בשגרת חייהם של אזרחים. כך, בחודש ינואר 2024 הותקפה מערכת המחשבים בעיריית מודיעין עילית והובילה להשבתת שירותים לזמן מה. בחודש מאי באותה שנה התרחשה תקיפת סייבר נוספת על עיריית מודיעין עילית שהובילה לחסימת הגישה לכל מערך המחשוב של העירייה ולשיתוקה.[10] בחודש מרץ 2024 היתה זו המועצה האזורית גולן שחוותה תקיפת סייבר על מערכותיה. כתוצאה מכך, המענה האנושי לציבור בנושאים שונים היה חלקי ומוקד התחבורה במועצה סיפק מידע מוגבל בלבד.[11] בתחילת יוני 2024 הותקפה המועצה האזורית מעלה יוסף וביישומון המועצה שודרה אזהרה שקרית לציבור: "אם הרחובות לא יפונו ואתם רוצים לעמוד נגד היהודים, נפרס מאה אלף כוחות מילואים!!".[12] עיריית בת ים עדכנה גם כן בתחילת חודש יוני 2024 שמערכותיה היו

---

[7] סתיו נמר, *חשד למתקפת סייבר על המרכז הרפואי זיו בצפת: "האירוע זוהה ונבלם"*, **מעריב** (27/11/2023); מערכת ice, *מתקפת סייבר על בית חולים בצפון: מידע רגיש הודלף*ice , (29/11/2023); ינון בן שושן, *אחרי מתקפת הסייבר: בבית החולים זיו מאשרים שדלף מידע*, **וואלה** (23/11/2023); סתיו נמר, *פרסמו מידע רגיש: איראן וחיזבאללה אחראיות לתקיפת הסייבר בבהי"ח "זיו"*, **מעריב** (18/12/2023); יוסי הטוני, *נחשפו פרטים חדשים על מתקפת הסייבר על בי"ח זיו בצפת*, **אנשים ומחשבים** (28/01/2024); יהודה קונפורטס, *כמה חודשים לאחר שנפרץ, אתר ארכיון המדינה עדיין מושבת*, **אנשים ומחשבים** (11/03/2024); עופר אדרת , *מערך הסייבר: ארכיון המדינה עלול להימחק*, **הארץ** (12/03/204).

[8] דניאל סיריוטי, *המרכז הרפואי לגליל בנהריה: התקלה במערכות המחשוב אינה מתקפת סייבר* , **חדשות מבזק לייב** (24/12/2023); נתן וסרמן, *חשד: מתקפת סייבר נגד בית החולים פוריה*, **מעריב** (26/12/2023); אדי גל, *המרכז הרפואי לגליל בנהריה: מערכת המחשוב קרסה ליותר מ-12 שעות*, **ידיעות ברמיאל** (29/12/2023); עמי רוחקס דומבה, *תקיפת סייבר נגד בית החולים רמב"ם*, **IsraelDefense** (05/02/2024).

[9] ישי אלמקייס, *"מערכת הבריאות עוברת מתקפות סייבר באופן יומומי, בולמים כמעט את כולן"*, **מקור ראשון** (09/01/2024).

[10] מנחם קולדצקי, *מתקפת סייבר השביתה את מחשבי עיריית מודיעין עילית*, **המחדש** (23/01/2024); עומר בן יעקב, *מתקפת סייבר השביתה עירייה גדולה והוסתרה מהציבור. וזה רק קצה הקרחון*, **הארץ** (22/05/2024).

[11] אורי שמיר, *מתקפת סייבר על מחשבי מוא"ז גולן*, **גליל עולה מרכז הגליל והגולן** (18/03/2024).

[12] שקד שדה, *"לעמוד נגד היהודים": הודעת הפייק המצמררת שקיבלו תושבי הגליל* , **מעריב** (01/06/2024).

נתונות לתקיפת סייבר, אולם זו נבלמה שכן העירייה נקטה לטענתה את הצעדים הדרושים על מנת להתגונן כראוי.[13]

בתחילת אפריל 2024 סבלו הן משרד המשפטים והן משרד הביטחון מתקיפת סייבר על מערכותיהם. לפי פרסומים, תקיפת הסייבר על משרד המשפטים הובילה לדלף מידע שכלל בעיקרו תכתובות דוא"ל עד לשנת 2022. משרד המשפטים ומערך הסייבר הלאומי (להלן: "מס"ל" או "המערך") הבהירו ש"לא זוהתה חדירה למערכות המשרד" ולכן נראה שעיקר המסמכים שקבוצת ההאקרים פרסמה הם תוצר של חדירה לא חוקית לשרתים שבשימוש משרד המשפטים או הנהלת בתי המשפט, שהתרחשה בעבר. עם זאת, צו איסור פרסום הוטל על חקירת התקיפה ועל כן לא ניתן להבין באמת את ממדיה וחומרתה. באשר לתקיפה על משרד הביטחון, נטען שזו בוצעה באמצעות חדירה לשרתי צד שלישי, ושלא היתה חדירה למערכות הפנימיות של המשרד.[14] גם משרד החינוך חווה מתקפת סייבר כאשר פורטל עובדי ההוראה המאפשר עבודה מרחוק נפרץ והושבת לתקופה ממושכת.[15]

על אף איומי הסייבר הגוברים, הגנת הסייבר במדינת ישראל היא חלקית, אינה מעוגנת בחוק יחיד ואחיד העוסק בהגנת מרחב הסייבר, ומנוהלת על ידי מספר גופים. גופים אלה הם:[16]

(1) **שב"כ:** מנחה מקצועית גופי תשתיות מדינה קריטיות (תמ"ק) המנויים בתוספות הראשונה, השניה שאינם מופיעים בחמישית, והרביעית לחוק להסדרת הביטחון בגופים ציבוריים.[17]

(2) **מערך הסייבר הלאומי:** מאסדר את גופי תמ"ק המנויים בתוספת השניה והחמישית לחוק להסדרת הביטחון בגופים ציבוריים,[18] וכן מנחה את יחידות הסייבר המגזריות ואת היחידה להגנת הסייבר בממשלה ("יה"ב"), בהתאם להחלטת ממשלה 2443.[19]

(3) **היחידה להגנת הסייבר בממשלה:** הוקמה לפי החלטה 2443, פועלת בכפיפות לממונה על התקשוב הממשלתי, אך מונחית מקצועית על ידי מס"ל. תפקידה לספק הכוונה והנחיה מקצועית פנימית של משרדי הממשלה ויחידות הסמך בתחום הגנת הסייבר, לרבות ניהול סיכונים, הבנת תוכנית להגנת סייבר והקצאת משאבים למימושה, וגיבוש מדיניות ארגונית, נהלים ושיטות עבודה בנושא. כן עליה לפקח על ביצוע הדרישות

---

[13] מנחם הירשמן, *מתקפת סייבר על נכסי העירייה נבלמה בזמן*, **השבוע בחולון בת ים** (10/06/2024).

[14] טובה צימוקי, *בצל החשש מנקמה איראנית: דליפת סייבר נרחבת במשרד המשפטים*, **Ynet** (05/04/2024); טובה צימוקי, רפאל קאהאן ולירן תמרי, *ב"יום ירושלים האיראני": דליפת סייבר ממשרד המשפטים*, **Ynet**(05/04/2024); עמיר קורץ, *דליפת המסמכים ממשרד המשפטים – כתוצאה מפריצה "משנים קודמות"*, **Ynet** (06/04/2024); יוסי הטוני, *יום ירושלים האיראני בסייבר: יותר דיבורים, פחות מעשים*, **אנשים ומחשבים** (07/04/2024); רפאלה גויכמן, *מתקפת סייבר על משרד הביטחון: בשבוע האחרון הוכפל מספר המתקפות של האיראנים על ישראל*, **The Marker** (09/04/2024).

[15] יוסי הטוני, *משרד החינוך חווה מתקפת סייבר*, **אנשים ומחשבים** (31/01/2024).

[16] דוח שנתי של מבקר המדינה, 74א (טבת התשפ"ד, ינואר 2024), עמ' 634-633.

[17] ראו הגדרת "קצין מוסמך" בסעיף 1 לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח – 1998 (להלן: "החוק להסדרת הביטחון בגופים ציבוריים").

[18] שם, שם.

[19] החלטת ממשלה 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת סייבר" (15.02.2015) (להלן: "החלטה 2443").

המקצועיות בהתאם להכוונה ולהנחיה שנתנה, ולהתוות תהליכי שיתוף מידע פנים ממשלתיים, לרבות דיווח ל-CERT הלאומי.[20]

(4) **יחידות סייבר מגזריות:** אלו הן יחידות שהוקמו לפי החלטת ממשלה 2443, ופועלות בתוך כל אחד ממשרדי הממשלה הרלוונטיים ובכפיפות אליהם. תפקידן לספק הכוונה והנחיה מקצועית בתחום הגנת הסייבר למשק האזרחי, לרבות הגדרת מדיניות ודרישות האסדרה, בהתאם לסמכויות הרגולטוריות המופעלות על ידי המשרד הממשלתי בו הן פועלות ולמאפייני הגופים המאוסדרים על ידו. כן, עליהן לפקח ולבקר את ביצוע דרישותיהם המקצועיות על ידי הגופים המקצועיים, לרבות לעמוד על הפערים בין הנדרש למבוצע ולבצע התאמות. בנוסף, אחראיות היחידות המגזריות על בנייה והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר המאוסדר, לרבות דיווח אודות אירועי סייבר ל-CERT הלאומי. כמו כן, עליהן ליזום ולממש פעילות רוחבית, לרבות הקמת תשתיות והפעלת מנגנונים שמטרתם שיפור הגנת הסייבר במגזר המאוסדר על ידן. מס"ל מספק ליחידות אלו הנחיה מקצועית.[21]

(5) **הממונה על הביטחון במשרד הביטחון** (להלן: "מלמ"ב): אחראי על הנחיית ארגונים וחברות פרטיות המנויים בסעיפים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים, שהוגדרו בצו כמבצעות פרויקטים מוסווים.

(6) **הרשות להגנת הפרטיות:** מנחה ומייעצת לכלל המשק בהתאם לסמכויותיה לפי חוק הגנת הפרטיות, התשמ"א – 1981 ותקנות אבטחת מידע.[22]

מבחינת הגנת מרחב הסייבר הישראלי, מארג גופים זה משקף את התמונה הבאה:

- הגנת הסייבר של הממשלה על משרדי ויחידות הסמך שלה מאוסדרת על ידי יה"ב.
- גופי תמ"ק כפופים לשב"כ, למלמ"ב ולמס"ל, ולאור העובדה שגופים אלה הם חסויים לחלוטין אין לדעת את רמת התפקוד שלהם בהגנה על תשתיות קריטיות.
- ארגונים במגזר הפרטי אשר נתונים לאסדרה מגזרית של משרד ממשלתי כלשהו, כפופים להנחיית יחידות הסייבר המגזריות ברגולטורים המגזריים. בחלוף עשור מהחלטת ממשלה 2443 אשר נטעה את ניצני האסדרה הביזורית, מתגלה חוסר אחידות משמעותי בסמכויות ובמשאבים בין היחידות המגזריות השונות.[23] רק חלק ממשרדי ההמשלה הקימו יחידות מגזריות מתפקדות בעוד אחרים הקימו יחידות זמניות או נמנעו מהקמתן כלל.[24]
- כלל המשק, במגזרים הממשלתי, הציבורי והפרטי, כפופים להוראות הרשות להגנת הפרטיות, המתמקדת רק במידע אישי והגנה על פרטיות, ואינה עוסקת בהגנה על מרחב הסייבר בהיבט השמירה על הרציפות התפקודית של כל ארגון וארגון.

כתוצאה מכך, **ארגונים פרטיים שאינם גופי תמ"ק ואינם מאוסדרים בשגרה בנושא הגנת סייבר על ידי רגולטור מגזרי כלשהו, אינם נתונים בכלל תחת רגולציית הגנת סייבר.**

---

[20] נספח ה' להחלטה 2443, שם.

[21] נספח ג' להחלטה 2443, שם.

[22] חוק הגנת הפרטיות, התשמ"א – 1981 (להלן: "חוק הגנת הפרטיות"); תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 (להלן: "תקנות אבטחת מידע").

[23] החלטת ממשלה מס' 2443, לעיל ה"ש 19.

[24] רון גילרן, *חוק הגנת הסייבר הלאומית, התשפ"ו – 2026: דו"ח הערכת השפעות אסדרה (RIA)*, **מערך הסייבר הלאומי, אגף אסטרטגיה והתעצמות** (ינואר 2026), בעמ' 7.

מצב זה טומן בחובו מגוון סכנות, עליהן הצביע מבקר המדינה לאורך השנים. כך, למשל, בינואר 2024 הצביע מבקר המדינה על כשל משמעותי בניהול סיכוני סייבר של שרשרות אספקה, וקבע כי 55% ממשרדי הממשלה ומגופי התמ"ק אינם עובדים לפי מתודולוגיית שרשרת האספקה של מס"ל, 41% מהם לא ביצעו ביקורות סייבר על הספקים המהותיים שלהם בשלוש השנים שקדמו לדו"ח המבקר, 57% מהם לא כללו במכרזי ההתקשרות שלהם עם ספקים דרישה ליישום מתודולוגית שרשרת האספקה, ו- 43% מהם כלל אינם מערבים ממונה הגנת סייבר בהליכי הרכש.[25]

יתרה מכך, המבקר קבע כי אף לא אחד מ-13 הספקים המהותיים שנותנים שירותים לכמה גופי תמ"ק, עבר תשאול על ידי מומחה הגנת סייבר בהתאם למתודולוגית הגנת הסייבר בשרשרת האספקה של מס"ל.[26] עוד נמצא ש - 77% ממשרדי הממשלה וגופי התמ"ק שהשיבו לשאלותיו של המבקר לא ביצעו תהליך של איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון, על אף המלצות המתודולוגיה של מס"ל לעשות כן כשלב הראשון למזעור סכנת הסייבר הנשקפת משרשראות אספקה.[27] עוד מצא מבקר המדינה שחברות אחסון אתרים וחברות אינטגרציה ו-IT, מונחות על ידי אגף ה-CERT במס"ך, אך הן מחויבות רק להוראות חוק הגנת הפרטיות ותקנות אבטחת מידע ביחס ל"מחזיק" **ואינן מחויבות בכלל לקיים את שלל ההנחיות שהן מקבלות ממס"ל. עקב כך, אותם כשלים שהתגלו בהן בעבר ממשיכים להתגלות גם באירועי סייבר הבאים.[28]**

מבקר המדינה הצביע גם על היעדר תיאום בין הגופים האסדרתיים הפועלים בתחום שרשרת האספקה – מס"ל, יה"ב, שב"כ, מלמ"ב, יחידות הסייבר המגזריות, והרשות להגנת הפרטיות – ועל כך שלכל אחד מגופים אלה תקן והנחיות משלו בנוגע להגנת סייבר בשרשרת האספקה. כתוצאה מכך עשוי להיווצר נטל רגולטורי מיותר או בלבול בנוגע להוראות אבטחת המידע שעל ארגון לחייב ספק בהסכם ההתקשרות עמו.[29]

בדו"ח מיוחד בנושא הגנת סייבר ממאי 2023, מצא מבקר המדינה ליקויים בהגנת סייבר במספר משרדים ממשלתיים ומוסדות המעניקים שירות לציבור. כך, נמצא שבמערכת "אביב" ובמערכת "רותם" שבידי רשות האוכלוסין מאגרי מידע הכוללים תמונות פנים של מיליוני ישראלים וזרים, שהינן באיכות היכולה לשמש לשם השוואה ביומטרית. על אף זאת, מאגר המידע אינו מאובטח ברמה הנדרשת למידע רגיש מסוג זה.[30] ליקויים נמצאו גם במערכות המידע שבידי השב"ס, שלא פעל כלל לפי הכללים המחייבים בתחום, לא קיבל ליווי והנחייה בתחום המסווג, וזאת על אף שבתחום הלא מסווג והרגיש פחות כן הונחה על ידי היחידה המגזרית של המשרד לביטחון פנים.[31] ליקויים נמצאו גם בהגנת הסייבר של המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה אשר

---

[25] המבקר הגדיר "שרשרת אספקה" כ"כלל המשאבים והתהליכים הקשורים בספקים, בלקוחות ובקבלני ביצוע, אשר דרושים לצורך אספקת מוצר או שירות בארגון." ראו דוח שנתי של מבקר המדינה, 74א, לעיל ה"ש 16, עמ' 617.

[26] דוח שנתי של מבקר המדינה, 74א, לעיל ה"ש 16, עמ' 622.

[27] דוח שנתי של מבקר המדינה, 74א, לעיל ה"ש 16, עמ' 619, 697-698.

[28] דוח שנתי של מבקר המדינה, 74א, לעיל ה"ש 16, עמ' ,623, 628, 671.

[29] דוח שנתי של מבקר המדינה, 74א, לעיל ה"ש 16, עמ' 627 – 628, 719-718.

[30] דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע – מאי 2023 (מאי 2023), עמ' 275.

[31] דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע, שם, עמ' 307-305, 364, 368.

מחזיק במאגר מידע בנוגע לכ-3 מיליון חייבים, וזאת על אף שיה"ב הצביעה על ליקויים משמעותיים ודרשה את תיקונם.[32]

ממצאים מטרידים נוספים עולים בדו"חות מבקר המדינה לגבי מוכנות בתי החולים בישראל. המבקר ביצע בדיקת חדירות לבית חולים מסוים. הבדיקה חשפה מספר ליקויי אבטחה בתחום הסגמנטציה ובקרת זרימה, בקרת גישה לרשת, הגנת עמדות ושרתים, תוכנה לא עדכנית וגישה לא מאובטחת. על אף שהנהלת אותו בית חולים תיקנה חלק מהליקויים, היא הגיעה למסקנה שהעלות הכוללת לתיקון הליקויים יכולה להסתכם ביותר מעשרה מיליון ש"ח לשנה באופן שוטף. לפיכך המליץ המבקר למשרד הבריאות, שפועל כמאסדר של המוסדות הרפואיים לרבות בתחום אבטחת המידע, לבצע מבדקי חדירות לכלל המוסדות הרפואיים בארץ באופן עיתי ויפעל להטמיע את ממצאי בדיקת החדירות שערך המבקר בכלל המוסדות הרפואיים.[33]

מתוך היכרות עם החוסרים העמוקים בהגנת מרחב הסייבר בישראל, אישרה ממשלת ישראל בנובמבר 2023, סמוך לאחר פרוץ מלחמת חרבות ברזל, תקנות לשעת חירום (חרבות ברזל) התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד – 2023. נוכח הבעייתיות שבאסדרה במסגרת תקש"ח, הוחלט לחוקק את ההסדר שעוגן בתקש"ח בחקיקה ראשית המוגבלת בזמן, דהיינו בהוראת שעה. חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד – 2023, התקבל ב 26.12.23, במטרה לבלום ולטפל במתקפות סייבר על חברות המעניקות שירותים דיגיטליים ומחוברות לגופים רבים במשק, לרבות מערכות החיוניות לביטחון המדינה ולתפקוד המשק, מתוך הבנה שבמצב החקיקתי הנוכחי אין גורם ממשלתי אחד האמון על אסדרת פעילותן.[34]

ברור לכל שחקיקת תקנות שעת חירום או הוראות שעה אינה מספקת פתרון ארוך טווח לבעייתיות הקיימת באסדרה החסרה של הגנת הסייבר במדינת ישראל. לפיכך, אין מחלוקת שהתזכיר נחוץ ביותר.

כפי שכבר כתבתנו במסמכים קודמים[35] העקרונות המנחים בגיבושה של אסדרת הגנת סייבר צריכים להיות:

א. אסדרה ביזורית המותאמת למאפייניו וצרכיו של כל מגזר משק.
ב. אסדרה דינמית דיה כדי להשתנות בעת הצורך ובייחוד בהתקיים שינויים טכנולוגיים.
ג. אסדרה המספקת תמריצים לארגונים פרטיים ולמשרדי הממשלה לציית להוראות הגנת הסייבר הרלוונטיות להם.

---

[32] דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע, שם, עמ' 380-378.
[33] דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע, שם, עמ' 433-430.
[34] חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד – 2023 (להלן: "הוראת השעה"). תוקפה של הוראת השעה הוגבל תחילה ל- 7 חודשים מיום פרסומה. הוראת השעה תוקנה מעת לעת ותוקפה של הוראת השעה הוארך לעת עתה עד ל 31 בינואר 2027. ראו חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 4), התשפ"ן - 2026.
[35] רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר, *מהו סייבר? חלק ב: אתגרי האסדרה של הגנת הסייבר* (מחקר מדיניות 173, **המכון הישראלי לדמוקרטיה**, ינואר 2023), עמ' 201-194.

ד. אסדרה המעגנת באופן בהיר את פעילותן של יחידות הסייבר המגזריות ומעניקה להן כלי פיקוח ואכיפה מותאמים לצרכי הגנת סייבר.

לצורך הגשמת עקרונות אלה, אנו סבורות שמודל האסדרה הביזורי הוא נכון. עם זאת, האסדרה צריכה לתת מענה לחסרונותיו של מודל האסדרה הביזורי ובראשם:

(1) הצורך באחידות וחשש מפני רמות שונות של הגנה, הגדרות שונות והיעדר קישוריות. זאת נוכח מימצאי מבקר המדינה בבדיקותיו לאורך השנים לפיהן משרדי הממשלה עצמם אינם מקיימים פעמים רבות את מתודולוגיית ההגנה המוצעת על ידי מערך הסייבר, ולא כל יחידות הסייבר המגזריות מצליחות, פעמים רבות עקב תקצוב חסר, לספק הנחיה לארגונים המאוסדרים על ידי המשרד הממשלתי בו הן פועלות, לפקח או לאכוף אותן.

(2) מניעת נפילה בין הכיסאות ולחילופין כפילות רגולטורית על מנת למנוע מצבים כפי שמצא מבקר המדינה בבדיקותיו לאורך השנים בהן ארגון היה נתון להנחיה של מספר רגולטורים. אף שכל רגולטור מנחה את אותו הארגון בתחום פעילות שונה הרלוונטי לאותו רגולטור, התוצאה היא נטל רגולטורי ולעיתים אף חוסר התאמה בתקינה הנדרשת על ידי כל רגולטור.

(3) הצורך בפעילות חוצת מגזרים בתרחישי קיצון. במתווה הנוכחי ארגונים רבים במגזר הפרטי אינם מאוסדרים בנושא ההגנת סייבר על ידי אף גורם תחת המתווה הביזורי, על אף שפעילותם הרציפה של חלקם עלולה להיות חיונית מבחינה כלכלית או ציבורית. עקב כך קיים קושי משמעותי ביצירתה של "כיפת סייבר" לכלל המשק.

המתווה המוצע בתזכיר משקף "אסדרה ביזורית מנוהלת", ומבקש להציג רגולציה מותאמת לצורך בביזוריות אך בה בעת גם להכרח בפיקוח על פעולותיהן של היחידות המגזריות ויצירת מסגרת אחידה והוליסטית להגנת סייבר בכלל המשק. המתווה מכיר בחשיבותם של הרגולטורים המגזריים, מסדיר את סמכויותיהם ואף נותן בידיהם אמצעי אכיפה מינהליים. בה בעת, הוא משמר בידי מס"ל את ניהול הגנת הסייבר הלאומית בשגרה באמצעות הנחייה מקצועית של היחידות המגזריות ובנסיבות קצה באמצעות התערבות ומתן הוראות לארגון ספציפי. זאת נוכח יכולותיו הייחודיות של מס"ל, מומחיותו בתחום הגנת הסייבר, היותו גורם מקשר למול גורמי ביטחון כגון צה"ל והשב"כ, ויכולתו לגבש תמונת מצב לאומית כוללת של איומי הסייבר וצרכי ההגנה באופן דינמי ומהיר.

ההנחיה המקצועית של היחידות המגזריות המוסדרת בתזכיר[36] אינה דומה לזו הניתנת לפי החוק להבטחת הביטחון בגופים ציבוריים,[37] שכן היא לא ניתנת לארגון מסוים המוגדר כגוף מונחה אלא ממוענת ליחידה המגזרית האמונה על הגנת הסייבר ברשות המוסמכת. במודל כזה של הנחיה מקצועית מחייבת, גוף מרכזי קובע סטנדרטים, מתודולוגיות ועקרונות יישום אחידים, על מנת להבטיח רמת הגנה מינימלית אחידה ולמנוע פערי אכיפה, והגופים הסקטוריאליים שומרים על אוטונומיה תפקודית והעצמאות הרגולטורית שלהם נשמרת.

---

[36] סעיף 5 לתזכיר חוק הגנת הסייבר הלאומית, התשפ"ו – 2026 (להלן: "התזכיר").
[37] סעיף 10 לחוק להסדרת הביטחון בגופים ציבוריים, לעיל ה"ש 17.

מתווה האסדרה הביזורית המנוהלת המוצע בתזכיר הוא לדעתנו נבון וראוי. הוא אינו מציג מודל של "רגולטור-על", שהוצע בתזכיר החוק הקודם שפרסם מערך הסייבר בשנת 2018,[38] וסברנו כי הוא משקף הסדר שגוי. זאת משום שהוא אינו מותאם לתרבות הפוליטית והרגולטורית בישראל, המאופיינת בהיעדר שיתוף פעולה בין הרגולטורים השונים, התרבות הארגונית ורמת האוריינות הדיגיטליות השונות של כל אחד מהרגולטורים המגזריים, והסכנה לפוליטיזציה או סקיוריזציה.[39]

ההסדר בתזכיר משמר בידי מס"ל סמכויות חיוניות, נוכח מאפייניה הביטחוניים של מדינת ישראל והאיומים הנשקפים לה ממרחב הסייבר.[40] המתווה דומה במידה רבה לזה הנהוג במרחבים אחרים בישראל וגם במדינות המערב, ובראשן מדינות האיחוד האירופי בהתאם לדירקטיבת NIS2.[41]

חוק הגנת הפרטיות קובע הסדר מיוחד לפיקוח על ציות להוראות החוק בגופים ביטחוניים. לפי הסדר זה, בגופים בטחונים ימונה מפקח פרטיות פנימי, שיונחה מקצועית על ידי ראש הרשות להגנת הפרטיות. כך מובטח שהמפקח הפנימי יפעל בהתאם לדרישות הרשות להגנת הפרטיות וכפי שמפקחים מטעמה פועלים.[42] מודל דומה מצוי גם בתקנות אבטחת מידע, במסגרתן יראו מי שעומד בהנחיה של רשות מוסמכת, המוגדרת כגוף ציבורי המוסמך לתת הנחיות בעניין אבטחת מידע, כמי שמקיים את הוראות תקנות אבטחת מידע, ובלבד שראש הרשות להגנת הפרטיות אישור את הנחיית הרשות המוסמכת.[43] כך מובטחת רמת אבטחת מידע מספקת גם בקרב ארגונים המונחים על ידי רשויות מוסמכות מגזריות.

בדומה, ה-EDPB, הרשות המוסמכת באיחוד האירופי לוודא אחידות ביישום הוראות ה-GDPR בין המדינות, מוסמכת לפרסם החלטות מחייבות לפתרון מחלוקת בין רשויות להגנת פרטיות מדינתיות בנוגע לפרשות ויישום הוראות ה-GDPR, וכן לפרסם הנחיות, המלצות וקוים מנחים באשר לפרשנות וליישום של הוראות ה-GDPR.[44]

---

[38] תזכיר חוק הגנת הסייבר ומעירך הסייבר הלאומי, התשע"ח – 2018; תהילה שוורץ אלטשולר ורחל ארידור הרשקוביץ, הערות על תזכיר חוק הסייבר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח – 2018, **המכון הישראלי לדמוקרטיה** (11 ביולי, 2018).

[39] ראו רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר, *מהו סייבר? חלק ב*, לעיל ה"ש 35, עמ' 162-180.

[40] רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר, *מהו סייבר? חלק ב*, לעיל ה"ש 35, עמ' 19-21, 162-165.

[41] 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, 2022 OJ. (L. 333) 80(להלן: "דירקטיבת NIS2"). גם בטאיוואן מסגרת רגולטורית דומה, אם כי היא חלה רק על רשויות ממשלה, תאגידים בבעלות מדינתית, ארגונים בשליטה מדינתית, וספקי תשתיות קריטיות שאינם בבעלות מדינתית. ראו Cyber Security Management Act (Taiwan), Presidential Order Hua-Zong Yi Yi-Zi No. 10700060021 (June 6, 2018), as amended by Presidential Order Hua-Zong Yi Yi-Zi No. 11400095391 (Sept. 24, 2025) (R.O.C. statut).

[42] סעיף 23בא לחוק הגנת הפרטיות, לעיל ה"ש 22.

[43] תקנה 20(ב) לתקנות אבטחת מידע, לעיל ה"ש 22.

[44] סעיפים 65 ו-70 ל- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 (להלן: "V").

גם בדירקטיבת NIS2 ניתנה ל ENISA, הרשות להגנת הסייבר האירופית, קיימת סמכות לספק למדינות החברות ולרשויות הגנת הסייבר המדינתיות והמגזריות הנחיות באשר לסטנדרט הגנת הסייבר המתאים ליישום הוראות הדירקטיבה.[45] כן מוסמכת ENISA לפקח ולבחון את מדיניות הגנת הסייבר של המדינות החברות באיחוד האירופי.[46]

<u>חלק א': אסדרת הגנת הסייבר – היבטים מבניים</u>

2. הדנ"א של מערך הסייבר הלאומי: רגולטור היברידי כלל מגזרי עם היבטים ביטחוניים, והצורך באמון הציבור

מערך הסייבר הלאומי הוא רגולטור ייחודי. בדומה לרשות להגנת הפרטיות, הוא אחראי לאסדרת הגנת הסייבר בכלל המגזרים, הפרטי והציבורי. כגוף ציבורי המספק שירות לציבור, על מס"ל לפעול מקצועיות, חוסר פניות ושקיפות, כדי להבטיח את אמון הציבור בו ואת שיתוף הפעולה של המגזרים השונים עמו.[47]

לצד תפקודו של מס"ל כרגולטור, הוא אמור להימצא בקשר רציף עם ארגונים ביטחוניים כדוגמת השב"כ, להתמודד עם איומים ביטחוניים ולאסדר את הגנת הסייבר הלאומית הכוללת של מדינת ישראל. בכובעו זה נדרש חיסיון על חלק מפעולותיו. לתפיסתנו, התזכיר אינו משקף איזון מספק בין שני היבטים מנוגדים אלו.

2.1. שקיפות

2.1.1. החרגה מחוק חופש המידע, תשנ"ח – 1998 וחשיפת מידע לציבור

בסעיף 58 לתזכיר מוצע לתקן את חוק חופש המידע, תשנ"ח – 1998 (להלן: "חוק חופש המידע") כך שיוחרגו מתחולתו פעילות חטיבות מס"ל העוסקות בהגנת הסייבר מול המשק, או בהגנת הסייבר של מס"ל, וכן פעילות יחידת הביטחון בו. אומנם, החרגה זו מצטרפת לזו הקיימת כבר עתה בחוק חופש המידע לפיה הוראות חוק חופש המידע לא יחולו על "מערך הסייבר הלאומי כהגדרתו בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח – 1998, ויחידות הביטחון ברשויות ציבוריות, והכל בעניינים המונחים על ידי אותו מערך לפי החוק האמור" ועל מידע שנוצר, שנאסף או שמוחזק בידיהם.[48] אולם, מאחר שהתזכיר מבקש ליצור מתווה חדש לאסדרה ביזורית מנוהלת, יש מקום לבחון בעת מחדש את החרגת מס"ל מתחולת חוק חופש המידע. החרגה של שלל פעולותיו האזרחיות של מס"ל מתחולת חוק חופש המידע היא גורפת מידי בעיקר נוכח חריגי הביטחון ושיטות הפעולה הקיימים ממילא בסעיף 9 לחוק חופש המידע.

לכן, אנו מציעות לוותר על ההחרגה הגורפת של מס"ל מחוק חופש המידע, ואם יש צורך בכך להחריג רק את פעולות היחידות הבטחוניות שבו, והשאר יוכפפו לחריגים הרגילים של החוק. בנוסף, אנו מציעות לבחון מחדש גם את סעיף 48 לתזכיר ולקבוע שרשימת המומחים החיצוניים, שתפקידם לסייע לעובד מוסמך במס"ל או ברשות מוסמכת להפעיל את סמכויותיו השונות לפי

---

[45] סעיף 25 לדירקטיבת NIS2, לעיל ה"ש 41.
[46] סעיף 18 וסעיף הקדמה 49 לדירקטיבת NIS2, לעיל ה"ש 41.
[47] ראו רחל ארידור הרשקוביץ, תהילה שוורץ אלטשולר ועידו סיון סביליה, *מהו סייבר? חלק א*, לעיל ה"ש 1, *בעמ' 57-53*.
[48] סעיף 14(א)(17) לחוק חופש המידע, תשנ"ח – 1998 (להלן: "חוק חופש המידע").

התזכיר, תפורסם לציבור על מנת לאפשר ביקורת ציבורית על אפשרות הימצאותם בניגוד עניינים.[49]

2.1.2. דיווח שנתי

סעיף 55 (ב) לתזכיר מעגן חובת דיווח שנתית של מס"ל ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת. נושאי הדיווח מוגבלים וכוללים רק את מספר הארגונים החיוניים שגורם מאסדר החריג מרשימת הארגונים החיוניים, מספר הארגונים שלא עמדו בתבחינים אך גורם מאסדר החליט להוסיפם לרשימת הארגונים החיוניים, והכל בחלוקה למגזרים ותוך פירוט הנימוקים להחלטה. בנוסף יש לדווח על מספר ההוראות שניתנו לפי סעיף 10(ה) לתזכיר, המסמיך את ראש מס"ל לתת הוראות לנקיטת אמצעים להתמודדות או מניעת סיכון סייבר משמעותי לכל ארגון חיוני, סוגי הארגונים להם ניתנו, מהות ההוראות, והאם ניתן אישור ראש הממשלה טרם נתינת ההוראות.[50]

הדיווח השנתי חיוני להגברת שקיפות פעולות מס"ל וכן על מנת לתת בידי היועמ"ש, ועדת חו"ב של הכנסת, והציבור בכללותו, מידע לגבי מידת ההתערבות של מס"ל במגזר הפרטי, מידת ההתערבות של הרגולטורים המגזריים בקרב הגופים המאוסדרים על ידם, יעילות מודל האכיפה המינהלית ומתן התמריצים השונים. משום כך, אנו מציעות להרחיב את חובת הדיווח בשני הקשרים:

א. דיווח אגרגטיבי על מספר ההוראות שנתן לפי סעיפים 15, 16 או 17.

ב. מספר העיצומים הכספיים, ביחס לאילו הפרות וגובה העיצום; מספר המקרים בהם הוטלה אחריות אישית על נושאי משרה בתאגיד; ומספר הארגונים אשר הגישו תצהיר ואישור עמידה בתקן וקיבלו פטור למשך שנתיים מעמידה בחובות הקבועות בתזכיר.

מאחר ומדובר באסדרה ביזורית מנוהלת, הרי שגם הרשויות המוסמכות מחזיקות במידע חיוני. משום כך אנו מציעות לחייב בדיווח שנתי ישירות ליועמ"ש ולוועדת חו"ב של הכנסת גם את היחידות המגזריות ברשויות המוסמכות. דיווחים אלו צריכים להיות אגרגטיביים ולכלול מידע בנוגע למספר ההוראות שנתנו לפי סעיפים 15 ו – 16, וכן נתונים בדומה למה שהצענו בסעיף ב' לעיל.

אנו מציעות שהדיווחים יתפרסמו לציבור, וזאת משני טעמים. ראשית, הדבר יאפשר ביקורת ציבורית על פעולות הרשויות המוסמכות ומס"ל. שנית, הדבר יתרום להסברה, חינוך והרתעה של הארגונים המאוסדרים, שייחשפו לסנקציות המוטלות על מפירים.

2.1.3. מינוי ראש מס"ל

היבט נוסף שיש בו כדי להשפיע על אמון הציבור הוא מינוי ראש מס"ל. לפי סעיף 4 לתזכיר, מינוי ראש מס"ל הוא באישור הממשלה, אולם התזכיר אינו מפרט את תנאי הכשירות לתפקיד ואינו דורש את פרסומו.

---

[49] סעיף 23יח(י) לחוק הגנת הפרטיות, לעיל ה"ש 22.
[50] סעיף 55(ב)(1), (2) לתזכיר, לעיל ה"ש 36.

תפקיד ראש מס"ל מנוי בתוספת השניה לחוק שירות המדינה (מינויים), תשי"ט – 1959 (להלן: "חוק שירות המדינה (מינויים)"), הקובע כי המינוי יעשה באישורה ובתנאים שתקבע.[51] כלומר, גם חוק המינויים אינו קובע את תנאי הכשירות לתפקיד ראש מס"ל אלא מותיר זאת לקביעתה של הממשלה. חקיקת התזכיר מהווה הזדמנות לעגן בחוק את תנאי הכשירות לתפקיד ראש מס"ל בהתאם להחלטת הממשלה בנושא. לשם השוואה, חוק הגנת הפרטיות אינו קובע גם כן את תנאי הכשירות לתפקיד ראש הרשות להגנת הפרטיות, אלא מפנה להחלטות הממשלה בנושא המצורפות בתוספת לחוק.[52] לעומת זאת, בחוק השב"כ מפורטים תנאי הכשירות לתפקיד ראש השב"כ ואף נדרש פרסום מינויו ברשומות.[53] אף שלאור סעיף 23 לחוק שירות המדינה (מינויים) מינויים באישור הממשלה נעשים בתנאים שהממשלה קובעת, אנו סבורות שהבהרת תנאי הכשירות לתפקיד ושקיפות ביחס למינוי ראש מס"ל יגבירות את אמון הציבור.

2.2. עצמאות במינויים, בתקציבים ובייעוץ המשפטי

סעיף 2(א) לתזכיר קובע שמס"ל יפעל "ביחידה עצמאית במשרד ראש הממשלה". אנו סבורות כי בגוף המוסמך לפעול גם מול משרדי ממשלה וביניהם משרד ראש הממשלה, אין די בקביעה זו. לכן אנו מציעות להוסיף הוראות המבהירות את עצמאותו של המערך כמפורט להלן:

- עצמאות תקציבית.[54]
- עצמאות בהפעלת סמכויותיה בהתאם לחוק.[55]
- עובדי מס"ל יהיו עובדי מדינה הכפופים להוראותיו של ראש מס"ל, לצד שמירת עצמאות ראש מס"ל לחתום על חוזים מיוחדים עם עובדים.[56]
- עצמאות הייעוץ המשפטי של מס"ל. עצמאות היעוץ המשפטי חשובה במיוחד שעה שיהיה בסמכות מס"ל להפעיל אמצעי אכיפה מינהליים גם על גופים ציבוריים המיוצגים על ידי משרד המשפטים או היעוץ המשפטי לממשלה.[57]

2.3. תפקידי מס"ל

סעיף 3 לתזכיר מונה את תפקידי מס"ל. דברי ההסבר מוסיפים שיישמרו גם תפקידי מס"ל שנקבעו בחוקים אחרים ובהחלטות ממשלה.

מבין התפקידים המנויים בסעיף 3 לתזכיר, נבקש להעיר לגבי התפקידים הבאים:

(1) סעיף 3(א)(1) לתזכיר: "ליזום ולקדם מדיניות ואסטרטגיה לאומית בתחום הגנת הסייבר." המונח "אסטרטגיה לאומית בתחום הגנת הסייבר "אינו מוגדר. יש מקום להבהיר בדברי

---

[51] סעיף 23 לחוק שירות המדינה (מינויים), תשי"ט – 1959 (להלן: "חוק שירות המדינה ("מינויים").
[52] ראו הגדרת "ראש הרשות" ו"הרשות" בסעיף 3 לחוק הגנת הפרטיות, לעיל ה"ש 22.
[53] ראו סעיף 3 לחוק שירות הביטחון הכללי, תשס"ב – 2002.
[54] בדומה למשל לסעיף 41א(ג) לחוק התחרות הכלכלית, תשמ"ח -1988, ולסעיף 19ב לחוק הגנת הצרכן, תשמ"א – 1981.
[55] ראו למשל סעיף 2(ב) להצעת חוק התקשורת (שידורים), התשפ"ו – 2025.
[56] בדומה לסעיף 41ב לחוק התחרות הכלכלית, לעיל ה"ש 54.
[57] הוראה בדבר עצמאות מינוי יעוץ משפטי ניתן למצוא בסעיף 33 להצעת חוק התקשורת (שידורים), התשפ"ו – 2025.

ההסבר האם הכוונה לאסטרטגיה הלאומית להגנה בסייבר שהמערך מפרסם מידי שנה או לתפיסת הגנה רחבה יותר.

(2) סעיף 3(א)(2) לתזכיר: "לרכז תמונת מצב של רמת הגנת הסייבר הלאומית "המונח "רמת הגנת הסייבר הלאומית" אינו מוגדר ויש מקום להבהירו בדברי ההסבר על מנת לספק תמונה כללית למה הכוונה, לפי אילו מגזרים תבחן?

(3) סעיף 3(א)(4) לתזכיר: "לפעול להעלאת המודעות בציבור להתנהגות בטוחה במרחב הסייבר, ולפרסם התרעות והמלצות לציבור להעלאת רמת הגנת הסייבר". יש לבחון מדוע העלאת מודעות הציבור, שהיא חלק מחינוך הציבור, צריכה להיות חלק מתפקידיו של מס"ל.

(4) סעיף 3(א)(5) לתזכיר: "לקדם ולעודד מחקר ופיתוח של תחום הגנת הסייבר". תפקיד זה עשוי להציב את מס"ל בניגוד העניינים משום שארגון שמפתח בתחום הגנת הסייבר עשוי להיות גם ארגון מאוסדר לפי התזכיר. נוסף על כך, עידוד מחקר ופיתוח מצוי ממילא בתחומה של הרשות לחדשנות.

(5) סעיף 3(א)(6) לתזכיר: "לקדם בחינת והטמעת טכנולוגיות מתפתחות להגנת סייבר".[58] הגדרת התפקיד אינה ברורה. אם הכוונה לעידוד תקינה טכנולוגית בתחום, הדבר דומה להסדר בדירקטיבת NIS2 בנוגע לקביעת מנגנון לעידוד גופי תקינה לגיבוש תקנים המתרגמים לשפה טכנית טכנולוגית את דרישות ההגנה המשפטיות. אבל יש לתת את הדעת לביקורת על מודל זה בדירקטיבת NIS2: נטען שמנגנון המפנה לגופי תקינה פרטיים לשם תרגום ההוראות המשפטיות הקבועות בדירקטיבה בעצם מעביר לגופי התקינה הפרטיים את הסמכות להתוות מדיניות ראויה. זאת על אף שהם אינם מצוידים במומחיות מתאימה ובכלים מספיקים על מנת להביא בחשבון שיקולים הנוגעים לשמירה על זכויות יסוד בעת תירגום הדרישות המשפטיות לשפה טכנית וקביעת סטנדרט להתנהגות בתקן. יתרה מכך, תזכיר קובע דרישות רמת הגנה בסיסית, המפורטות בחלק א' לתוספת הרביעית לתזכיר, ומפנה להוראות הרלוונטיות באחד התקנים הבינלאומיים המנויים בחלק ב' לתוספת הרביעית כאמצעי לעמידה בדרישות הגנה בסיסית. נוסף על כך, ארגון מהמגזרים המנויים בתוספת השישית לתזכיר רשאי להגיש תצהיר ואישור בדבר יישום הנחיות הגנת הסייבר בהתאם לתקן הבינלאומי המנוי בסעיף 52(ד) לתזכיר, ואלו יהוו אישור מספק לעמידתו של הארגון בדרישות הגנת הסייבר הבסיסית בתזכיר ויקנו לו פטור מחובות מסוימות המנויות בתזכיר.[59] כלומר, מודל התקינה בתזכיר מסתמך על תקנים בינלאומיים קיימים בתחום, אשר אושררו ברמה הבינלאומית כמתאימים מבחינת הגנת הסייבר הנדרשת ומבחינת כיבוד זכויות יסוד. כך מתגבר התזכיר על הביקורת בנוגע להיעדר התייחסות לזכויות אדם מבלי להשקיע משאבים כלכליים לשם גיבוש ואישור תקינה חדשה על ידי גופי תקינה מקומיים.

3. מודל האסדרה הביזורית המנוהלת – ההיבט הביזורי

התזכיר קובע מסגרת אסדרה ביזורית מנוהלת במסגרתה מחולק מרחב הסייבר לעשרה מגזרי משק, שעל כל אחד מהם מופקדת "רשות מוסמכת" - רגולטור מגזרי. כפי שציינו לעיל, מסגרת

---

[58] סעיף 3(5), (6) לתזכיר, לעיל ה"ש 36.

[59] סעיף 52(א), (ב) לתזכיר, לעיל ה"ש 36.

אסדרה זו נכונה ומתאימה לצרכי הגנת הסייבר חוצת המגזרים.[60] עם זאת, המתווה המוצע בתזכיר מעורר מספר קשיים.

3.1. החלוקה למגזרי משק

מגזרי המשק עליהם חל התזכיר מנויים בתוספת הראשונה והשנייה לתזכיר. המדובר ברשימה של 10 מגזרי משק וכן משרדי הממשלה. לראש הממשלה יש סמכות, לאחר שקילת המלצת ראש מס"ל, בהתייעצות עם השר הממונה ושר האוצר, ובאישור ועדת חו"ב של הכנסת, לשנות את רשימת מגזרי המשק.[61] עם זאת, רשימת מגזרי המשק המנויה כרגע בתזכיר מעוררת קשיים.

3.1.1. המגזר הציבורי

התזכיר חל רק על משרדי ממשלה ועל רשויות מקומיות. אולם לא ברור מהי תחולתו על גופי ממשל או תאגידים סטטוטוריים אחרים שאינם מוגדרים כמשרדי ממשלה ואינם נתונים להנחיה מכוח החוק להסדרת הביטחון בגופים ציבוריים כ"גופים מונחים".[62] לא מצאנו התייחסות לסוגיה זו בדברי ההסבר או במסמך ה-RIA שצורף לתזכיר, על אף שמדובר בסוגיה חשובה. אנו מציעות להוסיף את כלל הגופים הממשלתיים או הציבוריים שאינן מונחים או לחילופין להבהיר בדברי ההסבר האם נותרו גופים ממשלתיים או ציבוריים שאינם נדרשים לרמת הגנת הסייבר הבסיסית ואינם גופים מונחים, ואם כן מדוע וביצד תושג רמת הגנת סיביר לאומית מספקת בהיעדרם.

3.1.2. מגזרי משק חסרים במגזר הפרטי

אין בתזכיר או במסמך הערכת ההשפעות הנלווה לו, התייחסות להסדרה הקיימת במגזרים שאינם נמנים על "מגזרי המשק" עליהם חל התזכיר. אכן, בדברי ההסבר לתזכיר מוסבר כי התזכיר מהווה השלמה להסדרה הלאומית הקיימת לעניין תשתית מדינה קריטית בהתאם לחוק להסדרת הבטחון בגופים ציבוריים, וכן כהשלמה להסדרים המגזריים במגזרי המשק השונים ככל שקיימים.[63] עם זאת, אנו סבורות שהיעדר התייחסות באמור מותיר פתח להגנת סייבר חסרה במגזרים אלו, מבלי שמס"ל יכול להשפיע עליה ולוודא את עדכונה מעת לעת.

בנוסף, כמה מגזרים אינם מנויים ברשימת מגזרי המשק בתוספת השנייה, על אף שמדובר במגזרים הנמצאים ברשימת המגזרים המאוסדרים במדינות אחרות. כך, למשל, מגזר הפיננסים והביטוח נמנה על המגזרים המאוסדרים בגרמניה, אוסטרליה והולנד. מגזרי יצרני תרופות וציוד רפואי וכן מגזר ההשכלה הגבוה והמחקר, נמנים על המגזרים המאוסדרים באוסטרליה.[64]

---

[60] ראו הדיון בסעיף 1 לעיל.

[61] סעיף 9 לתזכיר, לעיל ה"ש 36.

[62] ראו הגדרת "גוף מונחה" בסעיף 1 לתזכיר, לעיל ה"ש 36.

[63] התזכיר, לעיל ה"ש 36, דברי ההסבר בנושא "כללי".

[64] ראו רון גילרן, *חקיקה לאומית להגנת סייבר: השוואה בינ"ל: מוגש כחלק מדו"ח הערכת השפעות רגולציה (RIA) במסגרת עבודת המטה סביב תזכיר חוק הגנת הסייבר הלאומית*, **מערך הסייבר הלאומי – משרד ראש הממשלה, אגף מדיניות וממשל**. נציין כי האוניברסיטה העברית, אוניברסיטת תל אביב, אוניברסיטת חיפה, הטכניון, מכון וייצמן, אוניברסיטת בר-אילן ואוניברסיטת בן-גוריון מנויות בתוספת השלישית לחוק להסדרת הביטחון בגופים ציבוריים, לעיל ה"ש 17, ועל כן נתונות לדרישות בנוגע לאבטחה פיזית בלבד. ראו הגדרת "פעולות אבטחה" בסעיף 1 לחוק להסדרת הבטחון בגופים ציבוריים.

3.1.3. גופים מונחים וגופים המנויים בתוספות לחוק להסדרת הביטחון בגופים ציבוריים.

החוק להסדרת הביטחון בגופים ציבוריים חל על גופי תמ"ק המנויים בתוספות לחוק, ומחייבם לדרישות הגנת סייבר מחמירות יותר מאלו הנדרשות לפי התזכיר. כך, גופי תמ"ק המנויים בתוספות הראשונה, השניה שאינם מופיעים בחמישית, והרביעית לחוק להסדרת הביטחון בגופים ציבוריים נתונים להנחיית השב"כ. גופי תמ"ק המנויים בתוספת השניה והחמישית לחוק להסדרת הביטחון בגופים ציבוריים נתונים להנחיית מס"ל ואלו המנויים בסעיפים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים נתונים להנחיית מלמ"ב.

התזכיר, בתורו, יוצר הפרדה ברורה בין מגזרי משק הנתונים לתחולתו, לבין גופים מונחים המוחרגים ממנו ונתונים להסדרה בהתאם לחוק הסדרת הביטחון בגופים ציבוריים. הפרדה זו היא חשובה שכן מגבירה את הוודאות במשק ומונעת נטל בירוקרטי מיותר.

עם זאת, התזכיר הוא הזדמנות לבחון מחדש את רשימת הגופים המנויים בתוספות לחוק להסדרת הביטחון בגופים ציבוריים ולהבטיח שהיא קוהרנטית ומדויקת. דווקא משום שהחוק להסדרת הביטחון בגופים ציבוריים מטיל דרישות מחמירות יותר בהשוואה לתזכיר, חשוב להבטיח שהחלוקה בין גופים הנתונים לאסדרה לפי התזכיר למול אלו הנדרשים לציית לחוק להסדרת הבטחון בגופים ציבוריים, היא הגיונית ושוויונית.

לעת עתה, לא בטוח שאלו הם פני הדברים. כך, למשל, מד"א מוגדרת כגוף מונחה, שכן נמנית על הגופים המנויים בתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, ואילו ארגון מקביל - איחוד הצלה ייחשב לפי התזכיר כארגון בלבד החייב ברמת הגנת סייבר ראויה בהתאם לפעילותו בלבד.[65]

לפיכך, אנו מציעות לערוך בחינה מקיפה של רשימת הגופים המנויים בתוספות לחוק להסדרת הביטחון בגופים ציבוריים לעומת גופים בעלי מאפיינים דומים אשר יוגדרו כארגונים חיוניים לפי התזכיר או כארגונים בלבד, ולהבטיח שהחלוקה בין גופים המאוסדרים לפי החוק להסדרת הביטחון בגופים ציבוריים לאלו שיאוסדרו לפי התזכיר תהיה הגיונית וקוהרנטית.

3.1.4. גופים מיוחדים

התזכיר מוציא מגדר תחולתו גופים מיוחדים, עליהם נמנית גם המשטרה.[66] אולם למשטרה מאפיינים המייחדים אותה לעומת שאר הגופים המיוחדים המנויים בהגדרה (מס"ל, משרד הביטחון ומלמ"ב, צה"ל, שב"כ והמוסד). המשטרה מחזיקה במידע אישי על כל אזרחי המדינה והנגישות למידע אישי זה פתוחה לבעלי תפקידים רבים במשטרה.[67]

אנו מציעות שלא להחריג את המשטרה מגדר תחולת התזכיר כגוף מיוחד ולחלופין לקבוע כיצד תעשה הגנת הסייבר במשטרה ומי יפקח עליה, במידה שזו אכן מוחרגת מתחולתו.

---

[65] ראו הגדרת "ארגון" בסעיף 1, וסעיף 10(א) לתזכיר, לעיל ה"ש 36.
[66] סעיף 1 לתזכיר הגדרת "גופים מיוחדים" ו"גוף ממשלתי", לעיל ה"ש 36.
[67] ראו דבריו של יו"ר ועדת חוקה, ח"כ רוטמן בנושא בעת בחינת מתווה מפקח הפרטיות הפנימי במשטרה במסגרת חוק הגנת הפרטיות (תיקון 13), התשפ"ד – 2024. פרוטוקול מס' 265 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"א באדר התשפ"ד (20 בפברואר 2024), עמ' 5.

3.2. הרגולטור המגזרי

התזכיר משמר את מבנה האסדרה הביזורית בהתבסס על החלטת ממשלה 2443 מלפני כעשור, על ידי פירוט סמכויותיהם של הרגולטורים המגזריים, כלי האכיפה שיועמדו לרשותם ומאפייני הגופים שיאוסדרו על ידי כל אחד מהם.

לפי התזכיר, על כל מגזר משק תהא אחראית רשות מוסמכת כמפורט בטור ג' בתוספת הראשונה או השנייה לתזכיר. ברשות המוסמכת תפעל יחידה מגזרית בהתאם להנחיה המקצועית של מס"ל. האסדרה של הרשות המוסמכת מופקדת בידי "גורם מאסדר", שהוא השר או גורם אחר המנוי בטור ה' בתוספת הראשונה.[68] בנוסף מפרט התזכיר שורה של בעלי תפקידים ברשות המוסמכת, שהקשר בניהם ובניהם לבין היחידה המגזרית, אינו ברור. כך, בכל רשות מוסמכת יש "גורם מסמיך", שמנוי בטור ד' בתוספת הראשונה או השניה לתזכיר, "ממונה", שהוא עובד בכיר ברשות מוסמכת שמוסמך להטיל עיצומים לפי התזכיר, מנהל בכיר ועובד מוסמך מגזרי.[69]

אנו סבורות שההסדר המוצע בתזכיר ביחס לרגולטורים המגזריים אינו ברור דיו ועלול להוביל לחוסר בהירות ולהימנעות הרגולטור המגזרי מפעולה או לכפילות בפעולות הננקטות על ידו. יש על כן מקום להבהיר את היחס בין בעלי התפקידים השונים ברשות המוסמכת, להתייחס לכשלים אפשריים בתפקודם וכן להבהיר את חלוקת הסמכויות ביניהם.

3.2.1. הגורם המאסדר – השר הממונה, והבעייתיות הנובעת מכך

לכל רשות מוסמכת יש גורם מאסדר שהוא "השר, או גורם אחר המנוי בטור ה' בתוספת הראשונה, האמון על האסדרה של רשות מוסמכת ביחס למגזר משק, המנוי בטור ב' לצדו".[70] התזכיר למעשה מעניק סמכויות החלטה לגורם פוליטי. אנו סבורות כי מתן חלק מסמכויות אלה בידי גורם פוליטי עלול לפתוח פתח להשפעה פוליטית וליחסי קח-ותן עם המגזר הפרטי, כמפורט להלן :

- **סמכות לפי סעיף 8(ב) לתזכיר לקבוע שארגון הוא ארגון חיוני או שאינו ארגון חיוני:**

המדובר בסמכות הגורם המאסדר לקבוע שארגון אינו ארגון חיוני, גם אם הוא עומד בתבחינים להגדרת ארגון חיוני לפי סעיף 8(א)(2) לתזכיר, ובכך לפטור את הארגון מהחובות המוטלות על ארגון חיוני לפי התזכיר, ובראשן חובת הבטחת רמת סייבר בסיסית. וכן הסמכות ההפוכה לקבוע שארגון הוא ארגון חיוני ולהטיל עליו את כל החובות המוטלות על ארגון חיוני לפי התזכיר, אף אם אינו עומד בתבחינים לפי סעיף 8(א)(2) לתזכיר.

אומנם, סמכות הגורם המאסדר בהקשר זה מותנית בקיומן של נסיבות מיוחדות ובשמיעת עמדת הוועדה המייעצת, אולם, אין די בכך כדי למנוע חשש מיחסי קח-ותן בין ארגון פרטי לגורם פוליטי. חלופות אפשריות הן קביעה כי יש לקבל את אישור הוועדה המייעצת להחלטת הגורם המאסדר; הפקדת ההחלטה בידי הוועדה המייעצת בלבד; החלפת הגורם המאסדר בוועדה המורכבת מבעלי תפקידים ברשות המוסמכת כגון הממונה האחראי על העיצומים ועל כן מחזיק בתפיסה רחבה

---

[68] ראו הגדרת "רשות מוסמכת", "גורם מאסדר" ו"יחידה מגזרית בסעיף 1 ו 5 לתזכיר, לעיל ה"ש 36.

[69] ראו הגדרת המונחים בסעיף 1 לתזכיר, לעיל ה"ש 36.

[70] ראו הגדרת "רשות מוסמכת", "גורם מאסדר" בסעיף 1 לתזכיר, לעיל ה"ש 36

באשר לרציפות התפקודית במגזר המשק, יחד עם מנהל בכיר ביחידה המגזרית האמונה על שיקולי הגנת הסייבר וכן מנהל בכיר נוסף מהרשות המוסמכת.

- **הסמכות לקבוע דרישות הגנת סייבר נוספות על אלו הקבועות בתוספת הרביעית לפי סעיף 10(ג) לתזכיר:**

מדובר בסמכות לשנות את התקנות או התוספת לחוק ולהטיל דרישות הגנת סייבר נוספות על אלו החלות לפי התזכיר, ועל כן לאמיתו של דבר היא צריכה להיות בידי הגורם המאסדר. אולם, על מנת למזער את הסיכון ליחסי קח ותן בין גורם פוליטי לבין ארגון מהמגזר הפרטי אנו מציעות להתנות את החלטת הגורם המאסדר בהתייעצות עם מנהל בכיר ביחידה המגזרית, במידה שמדובר במגזר משק המאוסדר על ידי רשות מוסמכת, וכן באישור החלטתו של הגורם המאסדר על ידי ועדת כנסת רלוונטית. נציין כי מתווה דומה קבוע בסעיף 41 לתזכיר ביחס לסמכותו של הגורם המאסדר להוסיף הפרות לתוספת החמישית בהתאם לדרישות הנוספות שיטיל לפי סעיף 10(ג) לתזכיר.

- **סמכות לקבוע סכומי עיצומים מופחתים לפי סעיף 28(ב) לתזכיר:**

סכומי העיצומים קבועים ביחס לכל הפרה בתוספת הרביעית לתזכיר, אולם הגורם המאסדר מוסמך לקבוע מקרים, נסיבות ושיקולים שבשלהם ניתן יהיה להטיל סכומי עיצומים מופחתים ואף לקבוע את שיעור העיצומים המופחתים. גם סמכות זו היא סמכות הכרוכה בשינוי התוספת לחוק ועל כן צריכה להיות נתונה בידי הגורם המאסדר. הסמכות מותנית בהתייעצות עם ראש מס"ל והסכמת שר המשפטים. אנו מציעות להתנותה גם כן באישור ועדת כנסת רלוונטית, כפי שנעשה, למשל, בנוגע לסמכות מקבילה הנתונה בידי שר המשפטים לפי חוק הגנת הפרטיות.[71]

- **הוספת מגזר משק לתוספת השישית לפי סעיף 52(ג) לתזכיר:**

הגורם המאסדר מוסמך, לאחר התייעצות עם ראש מס"ל, להוסיף מגזר משק לתוספת השישית. כך, יובל לאפשר לארגונים חיוניים מאותו המגזר להגיש תצהיר על עמידה בתקן טכנולוגי שהגורם המאסדר יקבע או יוסיף עליו, לשם קבלת פטור מציות להוראות התזכיר.[72] מדובר בסמכות לתקן את התוספת לתזכיר ועל כן היא חייבת להתבצע על ידי הגורם המאסדר. אך, אנו מציעות להוסיף חובת התייעצות עם הרשות המוסמכת או היחידה המגזרית ברשות המוסמכת וכן להתנות את החלטת הגורם המאסדר בקבלת אישור ועדת הכנסת הרלוונטית.

3.2.2. מנהל בכיר ברשות מוסמכת

"מנהל בכיר ברשות מוסמכת "מוגדר כ"עובד בכיר ברשות מוסמכת אשר דרגתו ראש אגף לפחות, אשר הגורם המסמיך הסמיכו לעניין זה." התזכיר מסמיך "מנהל בכיר ברשות מוסמכת" במגוון סמכויות, אולם אינו מבהיר את הקשר בינו לבין היחידה המגזרית, שהיא בעל המומחיות בתחום הגנת הסייבר. אף שיתכנו מקרים בהם יהיה צורך בקבלת החלטה על ידי מנהל בכיר שאינו חלק מהיחידה המגזרית,[73] חלק מהסמכויות המוקנות בתזכיר למנהל בכיר ברשות מוסמכת צריכות

---

[71] ראו סעיף 36ב לחוק הגנת הפרטיות, לעיל ה"ש 22.
[72] למעט חובת הדיווח לפי סעיף 11 לתזכיר, לעיל ה"ש 36.
[73] ראו הצעתינו בסעיף 3.2.1 לעיל.

להיות נתונות בידי בעל תפקיד, יתכן מנהל בכיר, ביחידה המגזרית, שהיא בעלת המומחיות בתחום הגנת הסייבר:

- הגדרת תקיפת סייבר חמורה היא בסמכותו של מנהל בכיר (סעיף 14(א)).
- דיווח על תקיפת סייבר משמעותית יעשה למנהל בכיר (סעיף 11).
- מתן הוראות לארגון חיוני להתמודדות עם תקיפת סייבר חמורה הוא בסמכות מנהל בכיר (סעיף 15(א)), אבל ההוראות עצמן יועברו לארגון החיוני מהמגזר הפרטי על ידי עובד מוסמך מגזרי, ולארגון חיוני מהמגזר הציבורי על ידי המנהל הבכיר עצמו.[74]
- מנהל בכיר הוא המוסמך לאשר את עבודתו של מומחה חיצוני לפי סעיף 48(ד) לתזכיר או להתיר פרסום פומבי ברבים של זהות ארגון לפי סעיף 49(ג) לתזכיר.

3.2.3. היחידה המגזרית: תפקידים ומבנה ארגוני

היחידה המגזרית היא יחידה בתוך הרשות המוסמכת ותפקידה לפעול "לקידום הגנת הסייבר במגזר המשק בהתאם להנחיה המקצועית של מערך הסייבר הלאומי."[75] הוראה על הקמתן של יחידות מגזריות עוגנה כבר בהחלטת ממשלה 2443,[76] ועתה מוצעת בתזכיר רשימה פתוחה של תפקידיה וסמכויותיה. עם זאת, תפקידי היחידה המגזרית וסמכויותיה מעוררים את הקשיים הבאים:

3.2.3.1. היעדר מועדים קבועים ועיתיים למיפוי שוטף של הארגונים החיוניים במגזר המשק.

כחלק מתפקידי של היחידה המגזרית עליה "למפות באופן שוטף את הארגונים החיוניים במגזר המשק".[77] אולם התזכיר אינו קובע מעדים קבועים ועיתיים לביצוע מיפוי שוטף כאמור, דבר העלול ליצור בעיה שכן תיתכן חוסר אחידות ברמת התפקוד של היחידות המגזריות במגזרי המשק השונים, וכתוצאה עלולים להיות מגזרי משק בהם לא יבוצע פיקוח מספיק על עמידתם של ארגונים הצריכים להיחשב ארגונים חיוניים לפי התבחינים שבתוספת השלישית לתזכיר בחובות לפי התזכיר. כתוצאה עשויים להיות ארגונים במגרי משק מסוימים שלא יעמדו ברמת הגנת הסייבר הבסיסית הנדרשת בניהם והגנת הסיבר הלאומית תיפגע. לפיכך, לשם הבטחת מיפוי מלא ועדכני של הארגונים החיוניים במגזר המשק, אנו מציעות לקבוע שעל היחידה המגזרית לקיים מיפוי עתי בפרקי זמן קצרים (למשל, אחת לרבעון). זאת על מנת להבטיח שהגדרת הארגונים החיוניים במגזר המשק תהא עדכנית ותואמת להתפתחויות הדינמיות בתחום הגנת הסייבר והטכנולוגיה.

3.2.3.2. היעדר הגדרה לנתוני רמת הגנה בסייבר בארגונים החיוניים

במסגרת תפקידיה, על היחידה המגזרית "לרכז את נתוני רמת ההגנה בסייבר בארגונים החיוניים במגזר המשק ולשתפם עם מערך הסייבר הלאומי באופן שוטף, ולכל הפחות אחת לרבעון[78]." אולם התזכיר אינו כולל הגדרה מהם "נתוני רמת ההגנה בסייבר ."כתוצאה, עשויה להיות שונות במידע

---

[74] סעיפים 15(א) ו 16(א) לתזכיר, לעיל ה"ש 36.
[75] סעיף 5 לתזכיר, לעיל ה"ש 36.
[76] החלטת ממשלה 2443, לעיל ה"ש 19.
[77] סעיף 5(ב) לתזכיר, לעיל ה"ש 36.
[78] סעיף 5(ג) לתזכיר, לעיל ה"ש 36.

המועבר מכל יחידה מגזרית למס"ל ועקב כך יחסרו למס"ל הנתונים הדרושים לשם הנחיה מקצועית מתאימה של היחידה המגזרית ולשם גיבוש תמונת מצב כוללת של הגנת הסייבר הלאומי. לפיכך, אנו מציעות להוסיף בתזכיר הגדרה ברורה ל"נתוני רמת ההגנה בסייבר בארגונים החיוניים" שהיחידה המגזרית נדרשת לשתף עם מס"ל.[79]

3.2.3.3. היעדר התייחסות למיקום הארגוני של היחידה המגזרית ולתקנים הנחוצים לפעילותה

התזכיר חסר התייחסות למיקומה הארגוני של היחידה המגזרית בתוך הרשות המוסמכת ולתקני כוח האדם הנדרשים לצורך פעילותה. היעדר התייחסות כאמור הוא בעייתי כי לא ברור מהו המעמד שניתן לה ולהחלטותיה, האם החלטותיה גוברות על החלטותיהן של יחידות אחרות ברשות המוסמכת במקרה של סתירה בניהן, וביצד תשמור היחידה המגזרית על מומחיותה ועצמאותה בקבלת החלטות הנוגעות להגנת סייבר, גם כאשר הן לא עולות בקנה אחד עם אינטרסים כלכליים וארגוניים של הרשות המוסמכת. לכן אנו מציעות להסדיר בחוק המוצע התזכיר את מיקומה הארגוני של היחידה המגזרית, לקבוע שהיחידה המגזרית תדווח ישירות לגורם המסמיך או לעובד בכיר הכפוף ישירות אליו, שהעובדים בה יהיו בעלי הידע והכישורים הנדרשים בתחום הגנת הסייבר לצד הבנה הולמת של תחומיה אסדרתה של הרשות המוסמכת, וכי לא ימלאו תפקידים נוספים או יהיו כפופים לנושא משרה ברשות המוסמכת אם מילוי התפקיד או הכפיפות כאמור עלולים להעמידן בחשש לניגוד עניינים במילוי תפקידיה של היחידה המגזרית לפי התזכיר.

4. מודל האסדרה הביזורית המנוהלת – ההיבט הניהולי

כאמור, לאסדרה ביזורית יתרונות רבים, שכן היא מאפשרת את התאמת דרישות הגנת הסייבר לצרכיו ומאפייניו של כל מגזר. אולם, כפי שהסברנו לעיל,[80] למתווה האסדרה המבוזר יש מספר חסרונות. בעיקר, ביזוריות היתר עלולה להוביל להיעדר הגנת סייבר מספקת בחלק מהמגזרים. משום כך, נדרש שמס"ל ישמר בידו גם סמכויות לפיקוח על הרשויות המוסמכות ולהבטחת אסדרת הגנת סייבר אחידה ככל הניתן בהתחשב במאפייני המגזרים השונים.

4.1. הנחייה מקצועית של היחידות המגזריות

היחידה המגזרית פועלת, לפי סעיף 5 לתזכיר, בהתאם להנחיה המקצועית של מס"ל.

כאמור, חוסר האחידות הנוכחי בסמכויות ובמשאבים של היחידות המגזריות כפי שנמצא בדוחות המבקר ובמסמך ה-RIA, מלמדים על נחיצותה של ההנחיה המקצועית של היחידות המגזריות.[81] אולם, לצד ההנחיה המקצועית, התזכיר מאפשר למס"ל להתערב רק בשני מקרים:

- סיכון סייבר משמעותי העלול לאפשר תקיפת סייבר חמורה נגד ארגונים חיוניים.[82]
- חשש לתקיפת סייבר חמורה שיש חשש שתתפשט במהירות לארגונים רבים, לכמה מגזרי משק או תפגע בביטחון המדינה או בטחון הציבור.[83]

---

[79] סעיפים 5(ג) ו-(ט) לתזכיר, לעיל ה"ש 61.
[80] ראו הדיון בסעיף 1 לעיל.
[81] ראו הדיון בטקסט הנלווה לה"ש 22 - 33 לעיל.
[82] סעיף 10(ה) לתזכיר, לעיל ה"ש 36. ראו הדיון בסמכות זו בסעיף 9.1 להלן.
[83] ראו סעיפים 10(ה) ו 17 לתזכיר, לעיל ה"ש 36.

כלומר, לבד מההנחיה המקצועית, מס"ל אינו מחזיק בסמכויות פיקוח לשם הבטחת יישום הוראות התזכיר על ידי היחידות המגזריות באופן רצוף בשגרה.

אנו סבורות כי אף שהמודל הביזורי הוא עדיף, הנתק שהתזכיר יוצר בין הרגולטורים המגזריים לבין מס"ל רחב מידי. לכן אנו מציעות לחייב את היחידה המגזרית לקבל את אישור מס"ל לתוכנית העבודה השנתית או הרב שנתית שלה, ולא להסתפק רק בהתייעצות עמו.[84] כך, ניתן יהיה להבטיח שבידי מס"ל תהיה היכולת לבחון את תפקודה השנתי של היחידה המגזרית ולהכווינה לא רק בעתות משבר אלא גם בשגרה, לשם שיפור הגנת הסייבר הלאומית ומניעת מצבים בהם הגנת הסייבר במגזרי משק מסוימים תהיה חסרה.

4.2. פיקוח על האסדרה במגזרים שאינם נמנים על מגזרי המשק

כאמור, קיימים מגזרים שאינם נמנים על מגזרי המשק ועל כן אין למס"ל סמכות לפקח על הגנת הסייבר בהם, אלא רק על גופים מונחים, במידה והם קיימים באותו המגזר.[85] היעדר פיקוח מינימלי על ארגונים במגזרים שאינם מבין מגזרי המשק ושאינם גופים מונחים היא פתח מסוכן לפגיעה משמעותית בהגנת הסייבר הלאומית. על מנת למנוע זאת, אנו מציעות לאמץ הסדר דומה לזה הקבוע בדירקטיבת NIS2,[86] המאפשר למס"ל סמכות שבשיקול דעת לבדוק באופן עתי את ההסדרה המגזרית במגזרים שאינם מנויים על רשימת מגזרי המשק, וזאת במטרה להבטיח שהיא מספיקה ועדכנית.

4.3. חובת התייעצות עם מס"ל בקביעת אסדרה עתידית

סעיף 51 לתזכיר מחייב שכל אסדרה, כהגדרתה בחוק עקרונות האסדרה, תשפ"ו – 2021, לעניין הגנת סייבר או שיש לה השפעה משמעותית על הגנת סייבר תיקבע רק לאחר התייעצות עם ראש מס"ל. כלומר, כל הוראה לעניין הגנת סייבר שנקבע בחיקוק, נוהל, הנחיה, חוזר, גילוי דעת או הוראה דומה אחרת, חייבת להיקבע לאחר התייעצות עם ראש מס"ל . מדובר בסעיף חשוב וחיוני, שכן הוא מבטיח שהגוף המקצועי שבידו המומחיות בתחום הגנת הסייבר הלאומית יהיה מעורב, באופן המוגבל להתייעצות בלבד, בכל אסדרה עתידית בתחום.[87]

בדין הישראלי מוכרת חובת התייעצות עם גורמים מקצועיים לפני קביעת הוראה או חקיקת משנה. כך, למשל, חוק הגנת הצרכן מחייב שתקנות לפיו יקבעו בהתייעצות עם הממונה על הגנת הצרכן או לפי הצעתו.[88] חוק שכר מינימום מחייב את שר האוצר להתייעץ עם ארגון העובדים הגדול במדינה ועם ארגוני מעבידים יציגים או נוגעים בדבר לשם קביעת הוראות לעניין חישוב שכר מינימום.[89]

בארצות הברית ובאיחוד האירופי נדרשת התייעצות עם הרשות המקצועית בתחום לפני גיבוש סטנדרטים מחייבים, בכמה דברי חקיקה. כך, לדוגמא, בארצות הברית ה – National Environmental Policy Act of 1969 מחייב כל רשות פדרלית המבקשת להציע חקיקה או פעולה

---

[84] ראו סעיף 5(ח) לתזכיר, לעיל ה"ש 36.
[85] ראו הדיון בסעיף 3.1.2 לעיל.
[86] ראו סעיף 4(1) לדירקטיבת NIS2, לעיל ה"ש 41.
[87] "אסדרה" כהגדרתה בחוק עקרונות האסדרה, תשפ"ב – 2021.
[88] סעיף 37(א1) לחוק הגנת הצרכן, תשמ"א – 1981;
[89] סעיף 18(ג) לחוק שכר מינימום, תשמ"ז – 1987.

פדרלית בעלת השפעות משמעותיות על איכות הסביבה להיוועץ עם כל רשות פדרלית שלה סמכות שיפוט או מומחיות, ביחס להשפעה הסביבתית הרלוונטית.[90] בדומה, לפי ה – Endangered Species Act, על כל רשות פדרלית להתייעץ עם הרשות הפדרלית האמונה על שימור מינים בסכנה לפני מתן רישיון לפעולה העשויה לפגוע במינים כאלה.[91] בתחום הגנת הסייבר, ה Federal Information Security Modernization Act (FISMA) מחייב את השר לביטחון המולדת להתייעץ עם ראש מכון התקנים (National Institute of Standards and Technology (NIST, לפני קביעת הוראות מחייבות המבוססות על הסטנדרטים והקווים המנחים של NIST עצמו.[92]

באיחוד האירופי, דירקטיבת NIS2 מחייבת את נציבות האיחוד להתייעץ עם קבוצת שיתוף הפעולה (Cooperation Group) המורכבת מנציגי המדינות החברות באיחוד, נציגי הנציבות ו ENISA , לפני אימוץ חקיקה הקובעת דרישות הגנת סייבר טכניות במגזרים מסוימים. זאת, במטרה להבטיח אחידות מינימלית של רמת הגנת סייבר בין המדינות החברות באיחוד.[93] גם בגרמניה, רגולטורים מגזריים חייבים להתייעץ עם רשות הגנת הסייבר הפדרלית לפני שמטילים דרישות טכניות על גופים המאוסדרים על ידם לצורך הגנת סייבר.[94]

מדוגמאות אלו ניתן ללמוד שחובת ההתייעצות מקובלת במקרים שבהם נדרשת מומחיות מיוחדת המצויה בידיו של גוף מסוים, ומומחיות זו היא רלוונטית באופן חוצה מגזרים. יתרה מכך, חובת ההתייעצות משמשת כלי נוסף להשגת רמת הגנת סייבר לאומית אחידה, ויש בה כדי לתת מענה מסוים להיעדר הפיקוח של מס"ל על האסדרה במגזרים שאינם מנויים על מגזרי המשק, שכן היא מבטיחה שמס"ל יוותר בתמונה כגורם מייעץ גם באסדרה עתידית של תחום הגנת הסייבר במגזרים אלו. באופן זה משמרת חובת ההתייעצות שבסעיף 51 לתזכיר את מתווה האסדרה הביזורי, אך מעניקה למס"ל כלים לפיקוח ולניהול האסדרה, אם כי מדובר בכלי המוגבל להתייעצות בלבד. משום כך, מדובר בכלי רצוי וחשוב ויש להשאירו בעינו.

<u>חלק ב': החובות המוטלות על ארגונים במגזרי המשק</u>

---

[90] 42 U.S.C. §4332(c).
[91] 16 U.S.C. §1536(A)(2).
[92] 44 U.S.C. §3553(B)(5), (h)(2)(E).
[93] סעיף 14 לדירקטיבת NIS2, לעיל ה"ש 41.
[94] Theresa Ehlen et. al., *Germany implements NIS2 – What you need to know now*, **Freshfields** (Dec. 6, 2025).

5. רמת הגנת הסייבר הנדרשת והתמריצים לנקיטתה

5.1. רמת הגנת הסייבר הכללית על "ארגון"

לפי סעיף 10(א) לתזכיר מוטלת על כל ארגון חובת הגנת סייבר, וזאת בהתאם לסוג ואופי פעילותו של הארגון ולניהול סיכונים הולם. הגדרת "ארגון" היא רחבה וכוללת למעשה את כל הארגונים מהמגזר הפרטי ומהמגזר הציבורי, לרבות רשויות מקומיות.[95]

הוראת סעיף 10(א) היא לפיכך ליבת החוק. אומנם, כפי שנאמר בדברי ההסבר , אין מדובר בחובה חדשה, אלא זהו שיקוף המצב המשפטי הקיים.[96] יתרה מכך, במגזר הפרטי, הגנת סייבר עשויה להיחשב כחלק מציות לחובת הזהירות הכללית שארגון חב בה כלפי האורגנים שלו מכוח דיני החברות.[97] במסגרת חובת זהירות זו על נושאי המשרה בתאגיד לפעול ברמת מיומנות סבירה, בזהירות ותוך שיקול דעת מקצועי, במטרה להגן על טובת החברה. הפרת החובה, גם אם ברשלנות, עלולה להוביל לתביעה נזיקית נגד נושאי המשרה בתאגיד.[98] בחובת זהירות דומה מחזיקה גם רשות ציבורית מכוח דיני הנזיקין.[99] עם זאת, מכל מקום, אין כיום הוראה דומה באף לא אחד מדברי חקיקה ראשי העוסקים בהגנת סייבר. יתרה מכך, מאחר שמרחב הסייבר מאופיין בקישוריות גבוהה המובילה לסכנת התפשטות מהירה של תקיפות סייבר, ומכיוון שלגורם האנושי, או יותר נכון לרשלנותו, תפקיד משמעותי בהתפשטות תקיפות סייבר,[100] עיגונה של דרישה ברורה באמור בתזכיר היא חשובה. יש בה כדי להבהיר שבמדינת ישראל, המצויה בשלישיה הראשונה של המדינות המותקפות במרחב הסייבר,[101] על כל ארגון לפעול להגנת הסייבר.

אנו מציעות שבניסוח החובה בסעיף 10(א) לתזכיר, אפשר להסתפק בדרישה כי "ארגון אחראי להבטחת רמת הגנת סייבר בהתאם לסוג ואופי פעילותו תוך ניהול סיכון הולם", ולמחוק את הביטוי "ראויה לפעילותו" משום שהוא אינו ברור.

5.2. רמת הגנת סייבר על ארגון חיוני

התזכיר מחלק את הארגונים הקיימים במגזרי המשק לשני סוגים: "ארגון" ו"ארגון חיוני". "ארגון חיוני" מוגדר בסעיף 8(א) באחת משלוש חלופות:

(1) גוף ממשלתי;

(2) ארגון שמתקיימים לגביו התבחינים המגזריים המפורטים בתוספת השלישית, ושאינו גוף מונחה.

---

[95] סעיף 1 לתזכיר, לעיל ה"ש 36, הגדרת "ארגון".
[96] התזכיר, לעיל ה"ש 36, דברי ההסבר לסעיף 10(א).
[97] סעיף 252 לחוק החברות, תשנ"ט – 1999.
[98] אהוד גרא, חובת הזהירות של תאגיד כלפי האורגנים שלו (עא 566/65 כץ נ. ,קציף, בע'מ, כ' פדי (3) 533) ,**משפטים** כרך א, עמ' 408 – 410 .
[99] סעיפים 36-35 לפקודת הנזיקין [נוסח חדש].
[100] רחל אריזור הרשקוביץ, תהילה שוורץ אלטשולר ועידו סיון סביליה, *מהו סייבר? חלק א,* לעיל ה"ש 1, עמ' 26-23, 57-53.
[101] Microsoft, *Microsoft Digital Defense Report 2025: Lighting the path to a secure future* (2025)*,* בעמ' 10.

לדעתנו רשימת התבחינים בתוספת השלישית לתזכיר חסרה. במגזר הבריאות חסרה התייחסות לחברות המייצרות תרופות ולבתי מרקחת. במגזר שירותים דיגיטליים ושירותי אחסון חסרה התייחסות בתבחינים לצ'אט בוטים שמבוססים על מודלים גדולים של שפה ולמוצרים הכוללים רכיבים דיגיטליים (IoT).

(3) ארגון שגורם מאסדר קבע שהוא ארגון חיוני.

על "ארגון חיוני" כהגדרתו בתזכיר מוטלת חובה לעמוד בדרישות רמת הגנת סייבר בסיסית המפורטות בחלק א' לתוספת רביעית לתזכיר.[102]

מקום שארגון חיוני מוצא שהוא עומד בתבחינים ביותר ממגזר משק אחד, מאפשר התזכיר לארגון לפנות לגורמים המאסדרים במגזרי המשק הרלוונטיים ואלו יקבעו, בהתייעצות עם מס"ל, באיזה מגזר משק יוגדר הארגון כחיוני.[103] אנו סבורות כי הסדר זה הוא פתח ל"קמצנות רגולטורית" כלומר אי הסכמה של רשויות לוותר על סמכויותיהן, מה שעלול לגרום לכך שארגון יהיה נתון להוראותיהן של מספר רשויות מוסמכות בו זמנית. לחלופין, ארגון עשוי למצוא עצמו בין הכיסאות בהיעדר אחריות של רשות שכל אחת סומכת על רעותה. על מנת למנוע מצב זה, אנו מציעות לתת את סמכות ההחלטה בידי מס"ל, שבידו תמונת הגנת הסייבר הרחבה, תוך התייעצות עם היחידות המגזריות ברשויות המוסמכות הרלוונטיות, ומנהל בביר או הממונה בהן, המחזיקים בראייה מגזרית רחבה.

5.3. היעדר תמריצים מספיקים בתזכיר

התזכיר מעגן מספר תמריצים מרכזיים להבטחת נקיטת רמת הגנת סייבר בסיסית על ידי ארגון חיוני: אמצעי אכיפה מינהליים, קביעת אחריות לנושאי משרה ואפשרות לעמוד בתקן כחלופה לציות למרבית החובות. עם זאת, כל אחד ממנגנונים אלו אינו שלם ואנו סבורות כי הגנת סייבר מיטבית במדינת ישראל זקוקה להרחבה שלהם.

5.3.1. אמצעי אכיפה מינהליים

5.3.1.1. פטור לגופים ציבוריים ולרשויות מקומיות מאמצעי האכיפה המינהליים

אמצעי אכיפה מינהליים ובראשם עיצומים כספיים הם כלי המטיל סנקציה כלכלית במטרה למנוע מראש הפרה, נוכח הנזק הכספי הגבוה הצפוי בגינה. החל מתחילת שנות האלפיים, גבר השימוש בעיצומים כספיים בדין הישראלי,[104] בין השאר בחוק הגנת הצרכן,[105] בחוק התחרות הכלכלית,[106] ובדיני הגנת איכות הסביבה.[107]

---

[102] סעיף 10(ב) לתזכיר, לעיל ה"ש 36.
[103] סעיף 8(ה) לתזכיר, לעיל ה"ש 36.
[104] חנן מנדל, אורן פרז ושירה תם, *המעבר לעיצומים כספיים ככלי אכיפה בתחום הסביבתי*, **משפט וממשל כה**, עמ' 709-659 (תשפ"ג).
[105] סעיף 22ג לחוק הגנת הצרכן, לעיל ה"ש 54.
[106] סעיף 59ד לחוק התחרות הכלכלית, לעיל ה"ש 54.
[107] סעיף 11 לחוק הפיקדון על מכלי משקה, תשנ"ט – 1999; סעיף 130 לחוק תאגידי מים וביוב, תשס"א – 2001.

סעיף 23(א) קובע שהממונה ברשות המוסמכת יהיה רשאי להטיל עיצום כספי על ארגון חיוני המפר את אחת מההוראות המפורטות בתוספת הרביעית. אולם, הסעיף מחריג ארגונים חיוניים מקרב משרדי הממשלה ורשויות מקומיות ממנגנון העיצומים הכספיים. המשמעות היא שלארגונים חיוניים ממגזרים אלו לא יהיה תמריץ בדמות עיצום כספי לציות לדרישות הגנת סייבר. אכן, במדינות אירופה החקיקה בנושא אינה מטילה עיצומים כספיים על גופי ממשל,[108] אבל במדינת בישראל קיימת חקיקה המאפשרת הטלת עיצומים כספיים גם על גופים ציבוריים. למשל בחוק הגנת הפרטיות,[109] וחוק שוויון זכויות לאנשים עם מוגבלות, תשנ"ח – 1998.[110] גם בדיונים בוועדת החוקה בנוגע לתיקון 13 בחוק הגנת הפרטיות ציין יו"ר הועדה, כי נוכח הקושי הידוע של הרשות להגנת הפרטיות לפעול במישור הפלילי נגד גוף ציבורי, יש להעדיף את כלי האכיפה המינהלית של העיצומים הכספיים.[111]

זאת ועוד, כפי שפירטנו לעיל,[112] הגנת הסייבר במשרדי הממשלה וברשויות המקומיות לוקה בחסר.. לא כל משרדי הממשלה עומדים בדרישות החלטת ממשלה 2443,[113] להקמת יחידות מגזריות,[114] וחלקם אף לא עובדים לפי מתודולוגיית הגנת סייבר שהוצעו על ידי מס"ל בעבר.[115] כלומר, אסדרה בלתי פורמלית הנעדרת סנקציות הוביחה היעדר התכנות וולונטרית ליצירת סטנדרט הגנת סייבר נאותה בקרב כלל משרדי הממשלה והרשויות המקומיות והיא אינה כלי מספיק להבטחת הגנת הסייבר הלאומית.

לכן אנו מציעות שלא להחריג את מגזר משרדי הממשלה ואת הרשויות המקומיות ממנגנון האכיפה המינהלית, בכל הנוגע לעיצומים כספיים.

5.3.1.2. גובה העיצום ואופן חישובו

סכום העיצום הכספי המקסימלי נע בין 320,000 ל – 640,000 אלף ש"ח.[116] מדובר בסכום שאינו גבוה מספיק ולכן עשוי להיחשב על ידי ארגונים חיוניים מסוימים כמעודד הפרה יעילה. על מנת להימנע ממצב בו סכומי העיצום לא ירתיעו ארגונים חיוניים מפני הפרת הוראות החוק ואי עמידה בדרישות הגנת הסייבר הבסיסיות, אנו מציעות לקבוע תקרה מקסימלית גבוהה יותר מסכומים אלו,

---

[108] בדירקטיבת NIS2 הושארה ההחלטה האם להטיל עיצום כספי על גוף ציבורי לשיקול דעתה של על מדינה. ראו סעיף 34(7) לדירקטיבת NIS2, לעיל ה"ש 41. בגרמניה, למשל, ניתן להטיל עיצומים כספיים על תאגידים ממשלתיים, אך לא עם גופי ממשל פדרלי. הפרה המבוצעת על ידי גוף ממשלתי פדרלי תטופל באמצעות שיח בין רשות הפיקוח הרלוונטית והמשרד הפדרלי. ראו BSIG § 64 (Ger.).

[109] סעיף 23לט לחוק הגנת הפרטיות, לעיל ה"ש 22.

[110] סעיף 26ז לחוק שוויון זכויות לאנשים עם מוגבלות, תשנ"ח – 1998.

[111] פרוטוקול מס' 320 מישיבת ועדת החוקה, חוק ומשפט, יום חמישי, ח' באייר התשפ"ד (16 במאי 2024), עמ' 84 דברי יו"ר ועדת החוקה, ח"כ רוטמן.

[112] ראו הדיון הנלווה לטקסט הסמוך לה"ש 22 - 33 לעיל.

[113] החלטת ממשלה מס' 2443, לעיל ה"ש 19.

[114] רון גילרן, *חוק הגנת הסייבר הלאומית, התשפ"ו – 2026: דו"ח הערכת השפעות אסדרה (RIA)*, **מערך הסייבר הלאומי, אגף אסטרטגיה והתעצמות** (ינואר 2026), בעמ' 7.

[115] ראו דוח שנתי של מבקר המדינה, 74א, לעיל ה"ש 16, עמ' 622-619, 698-697. דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע, לעיל ה"ש 30, עמ' 45-42, 244-243, 265-263, 430-433. מבקר המדינה, דוח על הביקורת בשלטון המקומי, אבטחת מידע של מערכות גבייה ברשויות מקומיות (יולי 2024).

[116] סעיף 23 לתזכיר, לעיל ה"ש 36.

ייתכן שבדמות אחוז מסוים מהמחזור השנתי של הארגון החיוני המפר. בדרך זו ניתן יהיה להתאים את גובה העיצום גם לחומרת ההפרה וגם למאפייני הארגון החיוני המפר ויכולותיו הכספיות. כך, למשל, הקנס המקסימלי לפי דירקטיבת NIS2 עומד על 10 מיליון יורו או 2% מהמחזור השנתי העולמי הכולל בשנת הכספים הקודמת, הגבוה מבין השניים, ביחס לגופים חיוניים, ו- 7 מיליון יורו או 1.4$ ביחס לגופים חשובים.[117] סנקציה של אחוז מהמחזור קיימת בימים אלה גם בהצעת חוק השידורים, שם מוצע לחשב את העיצום הכספי לפי סכום בסיס של אחוז מההכנסה השנתית האחרונה.[118]

5.3.2. אחריות נושאי משרה

הטלת אחריות אישית על נושאי משרה בתאגיד היא תמריץ משמעותי להכוונת התנהגות נאותה של תאגידים גם בתחום הגנת הסייבר.[119]

סעיף 45 לתזכיר מטיל אחריות על נושא משרה בתאגיד. אולם אחריות זו מצומצמת רק לביצוען של פעולות שמטרתן למנוע עבירות לפי סעיף 44(א) לתזכיר. כלומר, אחריות נושא המשרה בתאגיד מצומצמת רק למניעת העבירות של אי נקיטת אמצעים בניגוד להוראת ראש מס"ל לפי סעיף 10(ה); או אי מילוי הוראה לפי סעיפים 15(א)(4), 16(א) או 17(ב) לתזכיר.

צמצום האחריות אך ורק לעבירות של אי ציות למתן ההוראות מצמצם את התמריץ של נושאי המשרה להבטיח הטמעת דרישות הגנת הסייבר הבסיסית לפי סעיף 10(ב) לתזכיר על ידי הארגון. ביקורת של הרשות לניירות ערך משנת 2023 מלמדת שדירקטוריונים של כ-70% מהחברות הציבוריות שנדגמו, לא קיבלו כלל דיווחים עיתיים באשר לסטטוס הגנת הסייבר בחברה. ביקורת זו מחזקת את הטענה בדבר היעדר תמריצים מספיקים לנושאי המשרה בארגון לוודא שהארגון מטמיע הגנת סייבר המתאימה לפעילותו ולסיכונים הצפויים לו.[120]

למשל, דירקטיבת NIS2 מטילה אחריות אישית רחבה יותר על נושאי המשרה בארגון מזו הקבועה בתזכיר, ודורשת שעל נושאי המשרה תהיה חובה לאשר את אמצעי ניהול הסייבר הננקטים על ידי הארגון ולפקח על הטמעתם. נוסף על כך, במטרה לצמצם את הנזק שבפיקוח נושאי משרה שאינם בעלי מומחיות בתחום הגנת הסייבר, מחייבת דירקטיבת NIS2 את נושאי המשרה לעבור הדרכות בנושא הגנת הסייבר.[121]

---

[117] סעיף 34 לדירקטיבת NIS2, לעיל ה"ש 41.

[118] סעיף 114 להצעת חוק התקשורת (שידורים), התשפ"ו – 2025.

[119] Megan Gale, Ivano Bongiovanni & Sergeja Slapnicar, *Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead*, 121 COMPUTER & SECURITY (2022); Jennider Arlen, *Directors' Caremark Liability for Fraudulent Disclosures to Customers about the Company's Cybersecurity: SolarWinds Reconsidered* (Feb. 6, 2025); Thomas Neeff, *Personal Liability for violation of the NIS 2 Directive,*TENIM (April 24, 2024).

[120] רון גילרן, *חקיקה לאומית להגנת סייבר: השוואה בינ"ל: מוגש כחלק מדו"ח הערכת השפעות רגולציה (RIA) במסגרת עבודת המטה סביב תזכיר חוק הגנת הסייבר הלאומית*, **מערך הסייבר הלאומי – משרד ראש הממשלה, אגף מדיניות וממשל**, עמ' 21.

[121] סעיף 20 לדירקטיבת NIS2, לעיל ה"ש 41; Michelle R. Lowry, Anthony Vance & Marshall D. Vance, *Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity,* 72(2) MANAGEMENT SCIENCE (May 23, 2025).

אנו מציעות להרחיב את האחריות המוטלת על נושאי המשרה ברוח דירקטיבת NIS2 ולכלול בה אחריות אישית גם על עמידה בדרישות הגנת הסייבר המפורטות בתוספת הרביעית, בהתאם לסעיף 10(ב) לתזכיר. כן מוצע לחייב נושאי משרה בארגונים חיוניים לעבור השתלמות בהגנת סייבר ,למשל השתלמות באמצעות לומדה המסופקת על ידי מס"ל.

5.3.3. תצהיר עמידה בתקן טכנולוגי כפטור מחובות רמת ההגנה הבסיסית

סעיף 52 לתזכיר מאפשר לארגון חיוני, ממגזר המנוי בתוספת השישית לתזכיר, להגיש תצהיר ואישור מתאים בדבר עמידה בהוראות תקן טכנולוגיה בינ"ל מקובל המפורט בתוספת.

ארגון חיוני שיגיש תצהיר ואישור על עמידה בתקן, יהיה פטור מהחובות החלים עליו לפי התזכיר, למעט חובת הדיווח לפי סעיף 11.

המבנה המשפטי של אימוץ תקינה טכנולוגית בינלאומית מקובלת והצהרה על כך, כהוכחה לעמידה בדרישות החוק בכל הקשור להטמעת אמצעים ופעולות להגנת סיביר ומתן פטור מציות להן, הוטמע כבר בחקיקת הוראת השעה ביחס לספקי שירות דיגיטליים ושירותי אחסון בזמן מלחמת חרבות ברזל.[122] מדובר במבנה מקובל באיחוד האירופי, שהרעיון שעומד בבסיסו הוא שבאמצעות הישענות על תקנים מקובלים ניתן לתמרץ את התעשיה ליצור הגנת סטנדרט מבלי להעלות באופן משמעותי מידי את הנטל הרגולטורי. כך, הרגולציה תבטיח את האינטרס הציבורי לצד עידוד יעילות.[123] דירקטיבת NIS2 קוראת למדינות החברות לאמץ תקינה מתאימה ככלי להוכחת ציות לדרישות הדירקטיבה.[124] כמו כן, חוק הבינה המלאכותית האירופי שנכנס לתקפו בשנת 2025, אימץ מודל לגיבוש תקינה טכנולוגית כתחליף ל לציות לדרישות החוק.[125]

לתקינה טכנולוגית בינ"ל מספר יתרונות ובראשם העובדה שהיא נקבעת בשיתוף מלא עם נציגי התעשייה, ועל כן מציבה סטנדרטים ישימים ומותאמים לטכנולוגיה הקיימת. כן היא ניתנת לעידכון לעיתים קרובות יותר מאשר חקיקה. משום כך, לאסדרה המתמרצת אימוץ תקינה ככלי לתרגום הדרישות המשפטיות לעולם הטכנולוגי יתרונות לא מעטים. עם זאת, לתקינה טכנולוגית עשויים להיות גם חסרונות. כך, למשל, מאז כניסת חוק ה-AI לתוקף נטען שגופי התקינה אינם מביאים

---

[122] הוראת השעה, לעיל ה"ש 34.

[123] OECD, *Reinforcing Regulatory Frameworks through Standards, Measurements and Assurance: Making Better Use of Quality Infrastructure in Policymaking,* OECD Publishing (2025).

[124] סעיפים 24-25, וסעיף הקדמה 80 לדירקטיבת NIS2, לעיל ה"ש 41. בהצעת החקיקה החדשה להגנת סייבר שפורסמה בינואר 2026 שילבה נציבות האיחוד האירופי את מנגנון הפטור כבסיס להוכחת ציות בגוף החוק עצמו. ראו סעיף 78 ל Proposal of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) (להלן: "להצעה לתיקון חוק הגנת הסייבר האירופית").

[125] סעיפים 40 – 49, סעיף הקדמה 121 ל - Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L) 1689 (להלן: "**חוק ה – AI**").

בחשבון היבטים הקשורים בביבוד זכויות אדם, וכן אין ביכולתם להתחשב בשיקולים גיאופוליטיים וכלכליים העשויים להיות רלוונטיים לקביעת תקינה מחייבת למערכות AI.[126]

אנו סבורות שהמנגנון הזה הוא מנגנון נכון וראוי משום שהוא מקל על הבנת הדרישות המשפטיות באמצעות אימוץ התרגום הטכנולוגי שלהן כפי שמופיע בתקן טכנולוגי בינלאומי מוסכם. נוסף על כך, ההישענות על תקן טכנולוגי בינלאומי מוסכם מאפשרת להתגבר על החשש שבאי מתן משקל מספיק לזכויות אדם. זאת משום שאין הוא מפנה לחשיבה מחודשת וליצירת תקינה על ידי גופי תקינה, אלא מתבסס על התקינה הבינלאומית הקיימת בתחום אשר הוכחה מזה מספר שנים בארץ ובעולם כמכבדת זכויות אדם ברמה מספקת.

החיסרון הוא, שלפי התזכיר המגזר היחיד הרשאי להנות כרגע ממנגנון תמרוץ התקינה הוא מגזר ספקי השירותים הדיגיטליים ושירותי האחסון המופיע בתוספת השישית לתזכיר. אומנם, לגורם מאסדר הסמכות להוסיף מגזרים נוספים למנגנון,[127] אך נוכח יתרונותיו של המנגנון כתמריץ לאימוץ הגנת סייבר מתאימה, אנו מציעות להוסיף כבר עתה מגזרים נוספים שקיימים לגביהם תקנים בינלאומיים מתאימים.

ניסוח סעיף 52 עלול להוביל למסקנה שארגון חיוני המספק אישור עמידה בתקן הנדרש פטור מכל הוראות התזכיר. בדומה למקובל בדירקטיבת NIS2 שם מובהר שציות לתקינה פוטר אך ורק מחובות הגנת הסייבר המנויות בסעיף 21 לדירקטיבת NIS2,[128] אנו מציעות להבהיר גם בתזכיר שהפטור נוגע רק לעמידה בדרישות הגנת סייבר בסיסית המפורטות בסעיף 10(ב) לתזכיר וחלות בעת שגרה ומהפעלת אמצעי אכיפה מינהלית לפי סעיפים 12 ו – 13 לתזכיר, ואינו מונע מהרשות המוסמכת או ממס"ל להפעיל את סמכויות מתן ההוראות בעת מתקפת סייבר חמורה בהתאם לתנאים הקבועים בסעיפים 10(ה), 15, 16 ו -17 לתזכיר.

6. חובת הדיווח

סעיף 11 לתזכיר מטיל על ארגון חיוני חובת דיווח כאשר מתרחשת נגדו תקיפת סייבר משמעותית, שמתקיים לגביה אחד מהתנאים המפורטים בסעיף 11(א)(1) – (3).

6.1. למי מועבר הדיווח?

לפי סעיף 11(א) לתזכיר על ארגון חיוני לדווח לשני גורמים במקביל – מנהל בכיר במס"ל ומנהל בכיר ברשות המוסמכת. בסעיף 11(ג) מובהר שהדיווח יעשה באופן מקוון באמצעות ה CERT שמפעיל מס"ל, אך הגורם המסמיך ברשות המוסמכת יכול לקבוע שהדיווח יועבר לרשות המוסמכת ורק אח"כ למס"ל. אנו סבורות שמירוץ סמכויות זה עלול להוביל לחוסר בהירות ולנטל רגולטורי מיותר.

---

[126] MelaNIE Gorney & Helene Herman, *A peek into European standards making for AI: between geopolitical and economic interests,* (Hal-04784034, 2024); Christine Galvagna, *Inclusive AI governance: Civil Society participation in standards development,* Ada Lovelace Institute, discussion paper (March 30, 2023).

[127] סעיף 52(ג) לתזכיר, לעיל ה"ש 36. לביקורת על הסמכת הגורם המאסדר לקבלת החלטה זו ראו הדיון בסעיף 3.2.1 לעיל.

[128] ראו סעיפים 24, 25, 32(4), 33(4) לדירקטיבת NIS2, לעיל ה"ש 41.

אכן, גם בדירקטיבת NIS2 ניתנת האפשרות לדווח ל-CSIRT או לרשות המוסמכת הרלוונטית. אולם בשבועות האחרונים הוגשה הצעה לתיקון הדירקטיבה, משום שחובת הדיווח ל CSIRT הרלוונטי או לרשות המוסמכת,[129] הובילה למצב בו ארגון חיוני נאלץ להעביר דיווח לרשויות הרלוונטיות להגנת הפרטיות ולרשויות הרלוונטיות להגנת הסייבר או ל - CSIRT בנפרד בכל מדינה חברה באיחוד. הצעת התיקון קובעת שדיווח על תקיפת סייבר הנדרש מכוח חקיקת הגנת סייבר וכדיווח על פירצת אבטחה במסגרת ה-GDPR, ייעשה למוקד אחד שיוקם וינוהל על ידי סוכנות הגנת הסייבר של האיחוד האירופי (ENISA) והיא תעביר אותו לכל הגורמים הרלוונטיים באיחוד.[130]

אף שבישראל אין מדובר בדיווח למעל 20 גורמים שונים, יש בתיקון המוצע באיחוד האירופי כדי להבהיר את חשיבות הדיווח לגורם אחד אשר יפיץ אותו לכל שאר הגורמים הרלוונטיים. לפיכך, אנו מציעות שהדיווח יעשה אך ורק באמצעות אתר האינטרנט של ה CERT המופעל על ידי מס"ל. בנוסף, יש לשקול איחוד של חובת הדיווח לפי התזכיר עם חובת הדיווח לפי תקנה 11(ד) לתקנות אבטחת מידע.

6.2. מועדי הדיווח

התזכיר מחייב דיווח בשני מועדים: באופן מיידי ובסמוך לאחר הטיפול בתקיפת הסייבר.[131] אנו סבורות שמסגרת זו אינה מספיקה כי מיד לאחר גילוי תקיפת הסייבר המשמעותית יתכן שאין בידי הארגון החיוני את מירב המידע באשר לתקיפה, מקורה ונזקיה. לכן, הסתפקות רק בדיווח מידי ובדיווח בעת סיום הטיפול בתקיפת הסייבר עלול להוביל להיעדר מידע חיוני בתקופת הביניים. מידע שעשויה להיות לו חשיבות להערכת רמת הגנת הסייבר הלאומית ולהחלטות הרשות המוסמכת בנוגע להפעלת סמכויותיה למתן הוראות לפי סעיפים 15, 16 ו-17 לתזכיר. סמכות הרשות המוסמכת לדרוש ידיעה או מסמך לפי סעיף 12 לתזכיר אינה נותנת מענה מספק להיעדר המידע בתקופת הביניים שבין הדיווח המיידי לדיווח המסכם, שכן הרשות המוסמכת עשויה להיות מוצפת בדיווחים ולאו דווקא תוכל להבטיח שהיא בוחנת ודורשת מידע נוסף מידע כאשר הוא נחוץ .

דירקטיבת NIS2 מחייבת דיווח רב שלבי בשלושה מועדים שונים: 24 שעות מרגע גילוי תקיפת הסייבר, 72 שעות ובסיום הטיפול בתקיפת הסייבר. בדרך זו מאזנת דירקטיבת NIS2 לאזן בין הצורך במתן התראה מיידית כדי לנקוט פעולות מהירות למיזעור התפשטות אפשרית של תקיפת סייבר, לבין הצורך לקבל מידע מפורט ככל האפשר לשם הבנת מקורותיה של תקיפת הסייבר והמניעים

---

[129] סעיף 23(1) לדירקטיבת NIS2, לעיל ה"ש 41.

[130] סעיף 15 להצעת לתיקון חוק הגנת הסייבר האירופית, לעיל ה"ש 124; Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directive 2002/58/EC. (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulation (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) (להלן: "חבילת התיקונים הדיגיטלית האירופית").

[131] סעיף 11(ב), (ד) לתזכיר, לעיל ה"ש 36.

שבבסיסה. הבנה מעמיקה זו נחוצה לשם גיבוש הדרכים לשפר את חוסן הסיביר של הארגון המותקף וארגונים הדומים לו, וכן של כלל המגזרים המאוסדרים.[132]

בהתאם לדירקטיבת 2NIS בשלב הראשון, ארגונים חיוניים וחשובים חייבים לספק, ללא דיחוי ולכל המאוחר בתוך 24 שעות מרגע גילוי תקיפת סייבר חמורה, התראה ראשונית ל - CSIRT המתאים, או כאשר הדבר מתאים - לרשות האחראית הרלוונטית. כעיקרון, ההתראה הראשונית צריכה לכלול רק מידע הנחוץ על מנת להביא למודעות של ה-CSIRT או הרשות הרלוונטית על תקיפה משמעותית, ולאפשר לארגון המותקף לפנות בבקשה לעזרה. במידת האפשר, יכלול הדיווח הראשוני מידע האם תקיפת הסייבר היא תוצאה של פעולה זדונית או בלתי חוקית והאם עשויה להיות לה השפעה חוצת גבולות.[133] הדיווח יתבסס על הערכה ראשונית של תקיפת הסייבר על ידי הארגון המותקף, אשר תביא בחשבון את הרשתות ומערכות המידע המושפעות מהתקיפה, בייחוד את החשיבות שלהן במתן השירות על ידי הגוף, את חומרת איום הסייבר ומאפייניו הטכניים וכל חולשה המנוצלת, כמו גם את ניסיונו של הארגון עם מתקפות דומות. אינדיקטורים כמו מידת ההשפעה על השירות או משך התקיפה או מספר מקבלי השירות המושפעים, עשויים לשחק תפקיד משמעותי בבחינה האם ההפרעה התפעולית לשירות היא חמורה.[134]

בשלב השני, בתוך 72 שעות מגילוי תקיפת הסייבר, יש להעביר ל-CSIRT דיווח אודותיה. על הדיווח לכלול, בנוסף על המידע שנכלל בהתראה הראשונית, גם עדכון מצב תקיפת הסייבר וההתמודדות עמה וכן הערכה ראשונית של חומרתה, השפעתה ואינדיקטורים לפגיעה.[135]

בשלב השלישי, לא יאוחר מחודש לאחר הגשת הדיווח, יש להעביר דו"ח סופי. אם בתוך פרק זמן זה הארגון עדיין מתמודד עם תקיפת הסייבר, עליו להעביר דו"ח התקדמות, ובהמשך דו"ח סופי. הדו"ח הסופי צריך לכלול תיאור מפורט של התקיפה, לרבות חומרתה והשפעתה, סוג האיום או הגורמים שסביר שהובילו לתקיפה, האמצעים למזעור הנזק שנעשה בהן שימוש ובמידה שרלוונטי ההשפעה חוצת הגבולות של התקיפה.[136] לאורך כל שלבי הדיווח רשאים ה -CSIRT או הרשות האחראית לבקש דוחות ביניים אשר יכללו עדכוני מצב רלוונטיים.[137]

נוכח חשיבות הדיווח להבטחת הגנת הסייבר הלאומית, אנו מציעות לשנות את מסגרת הזמנים לדיווח, ולאמץ מסגרת רב שלבית דומה לזו המעוגנת בדירקטיבת NIS2. כמו כן, מוצע להסמיך את מס"ל לדרוש דיווחים נוספים בתקופת הביניים שבין הדיווח השני לדיווח האחרון בסיום הטיפול

---

[132] Chapter D Additional Rules Implementing the Basic Act, Non-Binding Criteria for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union — 18 June 2019 (2019/C 223/01), C 223/1 of 3 .7.2019, בעמ' 5.

[133] דירקטיבת NIS2, לעיל ה"ש 41, סעיף הקדמה 102, סעיף 23(4)(a). בהצעת התיקון של החקיקה הדיגיטלית האירופית הוצע להאירך תקופה זו ל 96 שעות לשם האחדה עם דרישות ה-GDPR. ראו התיקונים הדיגיטלית האירופית, לעיל ה"ש 130.

[134] דירקטיבת NIS2, לעיל ה"ש 41, סעיף הקדמה 101; Chapter D Additional Rules Implementing the Basic Act, Non-Binding Criteria for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union — 18 June 2019 (2019/C 223/01), C 223/1 of 3 .7.2019, בעמ' 3-4.

[135] דירקטיבת NIS2, לעיל ה"ש 41, סעיף 23(4)(b).

[136] דירקטיבת NIS2, לעיל ה"ש 41, סעיף 23(4)(d), (e).

[137] דירקטיבת NIS2, לעיל ה"ש 41, סעיף 23(4)(c).

בתקיפת הסייבר, על מנת להבטיח שיהיה בידה את המידע המלא הנחוץ להערכת רמת הגנת הסייבר הלאומית.

6.3. דיווח לארגון אחר ודיווח למקבלי השירות

במסגרת מתן הוראות לארגון חיוני במקרה של תקיפת סייבר חמורה, על ארגון חיוני לדווח על תקיפת הסייבר לכל ארגון אחר העלול להיפגע מתקיפת הסייבר ישירות ובאופן ממשי, אלא אם העובד המוסמך המגזרי בהתייעצות עם מס"ל פטר אותו מחובת דיווח זו.[138] בהקשר זה אנו מציעות את החידודים הבאים:

- להבהיר האם חובת הדיווח היא לכל ארגון או רק לכל ארגון חיוני העלול להיפגע מתקיפת הסייבר ישירות ובאופן ממשי.
- לצמצם את סמכות מתן הפטור מחובת דיווח זו לבעל תפקיד ביחידה המגזרית ולא לכל עובד ברשות המוסמכת.
- לקבוע תנאים או נסיבות בהן יינתן פטור כאמור על מנת לא להותיר את הנושא לשיקול דעתו המלא של העובד המוסמך המגזרי. זאת על מנת להבטיח אחידות, עד כמה שאפשר, בנסיבות בהן יידרשו ארגונים חיוניים לדווח על תקיפת סייבר לארגונים אחרים.

לצד חובת ההודעה לארגון אחר שעלול להיפגע מהתקיפה ישירות ובאופן ממשי, התזכיר אינו כולל חובת הודעה לציבור בכלל, או לציבור מקבלי השירות של הארגון החיוני בפרט. חובה כזו קיימת בדירקטיבת NIS2,[139] וגם בתקנה 11(ד) לתקנות אבטחת מידע, שם ניתן לראש הרשות שיקול הדעת האם לחייב בדיווח למקבלי השירות בתנאים מסוימים. אנו סבורות שדיווח לציבור הכללי או לציבור מקבלי השירות הינו חיוני אף להגברת אמון הציבור במס"ל, שכן מבטיח שמס"ל תפעל להגברת השקיפות כלפי הציבור.

לכן אנו מציעות להוסיף סמכות למס"ל או לרשות המוסמכת לחייב את הארגון החיוני להעביר דיווח גם לציבור הכללי או לציבור מקבלי השירות שלו.

<u>חלק ג: אסדרת הגנת הסייבר – סמכויות הרשויות המוסמכות, מס"ל וראש חטיבת ההגנה בסייבר בצה"ל</u>

7. הגדרת "תקיפת סייבר חמורה" והגדרת "תקיפת סייבר משמעותית"

המונח "תקיפת סייבר חמורה" הוא מונח מפתח בתזכיר, והוא משמש תנאי מרכזי להפעלת הסמכויות הנתונות למס"ל ולרשות המוסמכת להתערב בהתנהלות ארגון חיוני.[140] עם זאת, הגדרת

---

[138] סעיף 15(ב)(1) לתזכיר, לעיל ה"ש 36.
[139] סעיף 23(1), (2) לדירקטיבת NIS2, לעיל ה"ש 41.
[140] ראו סעיפים 10(ה), 15, 16 ו – 17 לתזכיר, לעיל ה"ש 36.

"תקיפת סייבר חמורה "אינה ברורה דיה וכן נדמה שיש דמיון רב להגדרת "תקיפת סייבר משמעותית "המקימה חובת דיווח לפי סעיף 11 .

"תקיפת סייבר חמורה – "סעיף 14 לתזכיר	**תקיפת סייבר משמעותית – סעיף 11 לתזכיר**
(א) בסימן זה "תקיפת סייבר חמורה - "תקיפת סייבר שהיה למנהל בכיר ברשות מוסמכת חשש ממשי כי מתקיים לגביה אחד או יותר מהתנאים הבאים ביחס אליה:	(א) נודע לארגון חיוני שמתרחשת נגדו, בפועל, תקיפת סייבר משמעותית שמתקיים לגביה אחד מהמפורטים להלן, ידווח על כך למנהל בכיר במערך הסייבר הלאומי ולמנהל בכיר ברשות המוסמכת בהתאם להוראות סעיפים קטנים (ב) ו-(ג):
(1) תקיפת הסייבר עלולה לפגוע בזמינות, רציפות או מהימנות השירות שארגון חיוני מספק;	(1) התקיפה עלול לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות השירות של הארגון, לרבות בבטיחות של מערכת או תהליך חיוניים בארגון, בהתחשב בין השאר באלה: (א) מספר או סוג המשתמשים בשירות, שעלולים להיות מושפעים מהתקיפה; (ב) סוג הפגיעה והיקפה; (ג) משך הפגיעה
(2) תקיפת הסייבר עלולה לפגוע בזמינות, רציפות או מהימנות השירות שארגון חיוני מספק;	
(3) תקיפת הסייבר עלולה לאפשר גישה לגורם שאינו מורשה לנכס מידע משמעותי של הארגון החיוני;	(2) התקיפה עלולה להביא לפגיעה או גישה של גורם שאינו מורשה לנכס מידע משמעותי, ובכלל זה בדרך של פגיעה בתהליך הזדהות, שינויו או הוצאתו שלא כדין של מידע לרבות בדרך של העתקתו על ידי גורם באמור;
(4) תקיפת הסייבר בארגון חיוני בעלת מאפיינים המעידים על חומרת תקיפה מיוחדת, לרבות מיתאר התקיפה או זהות התוקף;	(3) יש חשש ממשי שהיא אינה מוגבלת לארגון הנתקף.
(5) תקיפת הסייבר בארגון חיוני עלולה לפגוע בביטחון המדינה, בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור בשל: (א) מאפייני התקיפה, לרבות מתאר התקיפה או זהות התוקף;	

"תקיפת סייבר חמורה – "סעיף 14 לתזכיר	תקיפת סייבר משמעותית – סעיף 11 לתזכיר
(ב) יומו של חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לארגון הנתקף.	

בין תקיפת סייבר חמורה לפי סעיף 14 לתזכיר לבין תקיפת סייבר משמעותית המקימה חובת דיווח לפי סעיף 11 לתזכיר מספר ההבדלים משמעותיים:

(1) הגורם הקובע את סוג התקיפה: בתקיפת סייבר משמעותית מנהל בכיר ברשות מוסמכת הוא שבוחן וקובע האם מדובר בתקיפת סייבר חמורה. לעומת זאת, היותה של תקיפת סייבר משמעותית נבחנית ונקבעת על ידי הארגון החיוני עצמו בעת בחינת השאלה אם עליו לדווח עליה.
(2) התרחשות התקיפה: תקיפת סייבר חמורה עשויה לכלול גם חשש ממשי לפעולה העשויה לעלות כדי תקיפת סייבר חמורה. לעומת זאת, תקיפת סייבר משמעותית מתייחסת אך ורק לתקיפות סייבר המתרחשות בפועל .
(3) תקיפת סייבר תחשב לחמורה אם היא עלולה לפגוע בביטחון המדינה, ביטחון הציבור או ברציפות אספקתם של שירותים חיוניים לציבור. שיקולים אלו כלל לא רלוונטיים ואינם אף בגדר ידיעתו של ארגון חיוני בבואו לקבוע האם חלה עליו החובה לדווח על תקיפת הסייבר ממנה הוא סובל .

הבדלים אלו בין תקיפת סייבר חמורה לבין תקיפת סייבר משמעותית הם משמעותיים ומצדיקים את ההבחנה בניהן. אולם, לצד ההבדלים, נראה שקיים דמיון מסוים בהגדרת התנאים לאפיונה של תקיפה כחמורה או משמעותית. כך, התנאים הקבועים בסעיפים 14(א)(א)(1) ו (2) דומים זה לזה וכן לתנאי המפורט בסעיף 11(א)(1). התנאי המפורט בסעיף 14(א)(3) דומה לזה המפורט בסעיף 11(ב). לדעתנו הניסוח של התנאים בסעיף 11(א) ו –(ב) הוא ברור ובהיר יותר. משום כך, לדעתנו בהגדרת תקיפת סייבר חמורה יש לאחר את סעיפים 14(א)(1) ו – (2) ולנסחם בדומה לתנאי שבסעיף 11(א). כן יש לשקול לאמץ את הנוסח הקבוע בסעיף 11(ב) על פני זה שבסעיף 14(א)(3).

בנוסף, התנאי הקבוע בסעיף 14(א)(4) אינו ברור. אם הכוונה לתקיפת סייבר העלולה, נוכח מיתאר התקיפה או זהות התוקף, הביא לפגיעה בביטחון המדינה או הציבור או ברציפות אספקתם של שירותים חיוניים לציבור, הרי שאלו נכללים ממילא בסעיף 14(א)(5), ולכן ניתן רק בקבוע בו. אם לא כך הדבר, ראוי להבהיר מדוע תקיפת הסייבר צריכה להיות מוגדרת חמורה ומצדיקה התערבות של מס"ל או הרשות המוסמכת בהתמודדותו של הארגון החיוני עם תקיפת הסייבר באמצעות מתן הוראות לפי סעיפים 15, 16 ו – 17 לתזכיר.

לשם השוואה, דירקטיבת NIS2 מגדירה "מתקפת סייבר משמעותית" החייבת בדיווח, ככזו הגורמת או עשויה לגרום להפרעה תפעולית משמעותית בשירות או לאובדן כלכלי לארגון או אם היא השפיעה או עשויה להשפיע על אנשים על ידי כך שתגרום לנזק חומרי או לא חומרי משמעותי.[141] בארצות הברית הדירקטיבה הנשיאותית מס' 41 משנת 2016, הגדירה תקיפת סייבר משמעותית כתקיפת סייבר, שלבד או בשילוב של מספר תקיפות סייבר, עלולה לגרום לנזק מופגן

[141] סעיף 23(1), (6), (11) לדירקטיבת NIS2, לעיל ה"ש 41.

(demonstrable harm) לאינטרסים של ביטחון לאומי, חירויות אזרח, בריאות הציבור או ביטחונו.[142]

בנוסף, וכפי שפירטנו לעיל,[143] אנו מציעות שההחלטה בדבר חומרתה של תקיפת סייבר תתקבל על ידי בעל תפקיד ביחידה המגזרית ברשות המוסמכת, המחזיקה במומחיות בתחום הגנת הסייבר, ולא בידיו של מנהל בכיר ברשות מוסמכת שאינו קשור ליחידה המגזרית.

8. סמכויות הרשות המוסמכת

8.1. סמכות מתן הוראות לגופים מהמגזר הפרטי ולגופים ממשלתיים

סעיפים 15 ו-16 לתזכיר מעגנים את סמכות הרשות המוסמכת לתת הוראות להתמודדות עם תקיפת סייבר חמורה במגזר הפרטי והממשלתי, אולם בניסוחם הנוכחי הם מעוררים מספר קשיים.

ראשית, הפעלת הסמכות מותנית בקביעתו של מנהל בכיר ברשות מוסמכת שקיים חשש ממשי להתרחשותה העכשווית או העתידית של תקיפת סייבר חמורה הדורשת את מעורבותו. מאחר ומדובר בהחלטה המחייבת הבנה של תחום הגנת הסייבר אנו מציעות שהיא תתקבל על ידי בעל תפקיד ביחידה המגזרית ולא על ידי מנהל בכיר אחר ברשות המוסמכת.

נוסף על כך, הפעלת הסמכות במגזר הפרטי ובמגזר הממשלתי מותנית בכך שמנהל בכיר ברשות מוסמכת קובע שמדובר ב"תקיפת סייבר חמורה הדורשת את מעורבותו". בדברי ההסבר ניתנות דוגמאות למקרים בהם מדובר בתקיפה כאמור, ומובהר שלא כל תקיפת סייבר חמורה תיחשב לכזו הדורשת את מעורבות הרשות המוסמכת. אנו סבורות שאין להסתפק בדוגמאות בדברי ההסבר, לכן אנו מציעות לפרט בלשון החוק תנאים, נסיבות או שיקולים אשר בהתקיימותם יחליט המנהל הבכיר ברשות המוסמכת שאכן מדובר בתקיפת סייבר חמורה הדורשת את מעורבות הרשות המוסמכת. זאת, על מנת להגביר את הוודאות והבהירות בהפעלת הסמכות ואת אחידות בהפעלת הסמכות בכלל הרשויות המוסמכות.

כאשר מדובר בארגון חיוני במגזר הפרטי, ניתנת לו תחילה הזדמנות לפעול בעצמו לאיתור התקיפה, מניעתה או בלימתה,[144] אך אם העובד המוסמך המגזרי מצא ש"הארגון לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה" הוא רשאי, בהתקיים התנאים הנוספים המפורטים בסעיף 10(א)(4) לתזכיר, לתת לארגון הוראות.

אנו מציעות להוסיף תנאים או שיקולים שעל העובד המוסמך המגזרי לשקול בבואו לקבל החלטה האם הארגון החיוני פעל באופן הולם. זאת, על מנת להבטיח אחידות בהפעלת הסמכות למתן הוראות בין הרשויות המוסמכות .

---

[142] Presidential Policy Directive 41, United States Government Coordination of Cyber Incidents (July 26, 2016) (להלן: "דירקטיבה נשיאותית 41"). במאי 2026 אמור להיכנס לתוקפו תיקון ל Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), אולם הוא לא צפוי לשנות את הגדרת תקיפת סייבר משמעותית. ראו Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 91 Fed. Reg. 6794 (proposed Feb. 13, 2026) (to be codified at 6 C.F.R. pt. 226).

[143] ראו הדיון בסעיף 3.2.2 לעיל.

[144] סעיף 15(א)(2) לתזכיר, לעיל ה"ש 36.

בעת מתן הוראות לארגון חיוני במגזר הפרטי, על העובד לשקול את השפעתן האפשרית של ההוראות על פעילות הארגון החיוני ועל צדדים שלישיים, לרבות הזכות לפרטיות; את העלות הכלכלית המוערכת של יישום ההוראות; ואת השפעתן האפשרית על הרציפות התפקודית של הארגון. כן עליו להורות על נקיטת האמצעי שפגיעתו פחותה.[145]

לעומת זאת, בעת מתן הוראות לגוף ממשלתי, נדרש העובד המוסמך המגזרי לבחון רק את ההשפעה האפשרית של ההוראות על פעילות הגוף הממשלתי ועל צד שלישי, לרבות על הזכות לפרטיות וכן להורות על נקיטת האמצעי שפגיעתו פחותה.[146] היעדר ההתחשבות בעלות הכלכלית המוערכת של יישום ההוראות ובשאלת הפגיעה ברציפות התפקודית ביחס לגופים ממשלתיים - אינו ברור, שכן גם בגופים ממשלתיים יש לתת את הדעת לשיקולים אלה, כפי שעולה גם מסעיף 10(ה) לתזכיר לעניין השיקולים שעל ראש מס"ל לשקול בעת הפעלת סמכותו למתן הוראות לנקיטת אמצעים. לבן אנו מציעות להוסיף לרשימת השיקולים שעל העובד המגזרי לשקול בעת קבלת החלטה האם לתת הוראות לגוף ממשלתי גם את העלול הכלכלית המוערכת של יישום ההוראות ואת פגיעתם האפשרית ברציפות התפקודית של הגוף.

לבסוף, בעוד שבמקרה של מתן הוראות לארגון מהמגזר הפרטי, על העובד המגזרי לקבוע את המועד האחרון לביצוע ההוראה ועל הארגון חובה לעמוד במסגרת זמנים זו,[147] אין הוראה דומה ביחס לגוף ממשלתי. אנו מציעות לתקן זאת. אין סיבה שהוראות לגוף ממשלתי בנסיבות של תקיפת סייבר חמורה הדורשת את מעורבות הרשות המוסמכת, לא יהיו תחומות בזמן.

8.2. חוות דעת מקדמית

סעיף 47 לתזכיר מעגן מנגנון של פנייה לרשות מוסמכת על ידי ארגון חיוני לשם קבלת חוות דעת מקדמית על אופן יישום דרישה המנויה בתוספת הרביעית.

מדובר בהסדר חשוב ומבורך שיש בו כדי להגביר את הוודאות והבהירות בנוגע ליישום הוראות החוק בתחום טכנולוגי מורכב כמו הגנת סייבר. עם זאת, אנו מציעות:

- להבהיר שמתן המענה לבקשה לחוות דעת מקדמית ייעשה על ידי היחידה המגזרית ברשות המוסמכת, שלה המומחיות הנדרשת בתחום הגנת הסייבר.
- לקבוע מסגרת זמנים למתן חוות דעת במטרה להבטיח שהרשות המוסמכת תתייחס כראוי לחובתה זו, ובד בבד לאפשר לרשות המוסמכת לסרב לתת חוות דעת בנסיבות מסוימות.
- לחייב את הרשות המוסמכת לעדכן את מס"ל במתן חוות הדעת ותוכנה, שכן למס"ל הראייה הרוחבית של הגנת הסייבר הלאומית.
- לחייב פרסום של חוות דעת מקדמיות, תוך הסרת פרטים מזהים או פרטים שיש בהם לחשוף נושאים ביטחוניים, על מנת להבטיח שבידי כל הארגונים החיוניים יהיה מידע נגיש

---

[145] סעיף 15(א)(5) לתזכיר, לעיל ה"ש 36.
[146] סעיף 16(ב) לתזכיר, לעיל ה"ש 36.
[147] סעיף 15(5)(ג), (6) לתזכיר, לעיל ה"ש 36.

וזהה בנודע לאופן היישום של דרישות הגנת הסייבר הבסיסית וכן לאפשר ביקורת חיונית מצד הציבור ומומחי טכנולוגיה.

9. סמכויות מס"ל

נוסף על סמכות ההנחיה המקצועית של היחידות המגזריות וחובת ההתייעצות עם מס"ל בכל מקרה של אסדרה עתידית בתחום הגנת הסייבר ,הסמכויות המוקנות למס"ל בנסיבות קיצון בעת חשש לתקיפת סייבר חמורה או לסיכון סייבר משמעותי העלול להוביל לתקיפת סייבר חמורה הן נדבך נוסף בהיבט הניהולי של האסדרה הביזורית המוצע בתזכיר. על נחיצות הסמכויות הניהוליות נוכח אי הצלחת המודל הוולונטרי נעדר הסנקציות הקיים עד כה בישראל עמדנו כבר בראשית חוות דעתנו, ואנו סבורות שהסמכויות הנוספות המוקנות למס"ל לשם התערבות באמצעות מתן הוראות לנקיטת אמצעים או מתן הוראות בעת תקיפת סייבר חמורה משקפות את נחיצות זו ומציגות איזון יחסית ראוי בין ההיבט הביזורי להיבט הניהולי של אסדרת הגנת הסייבר הלאומית בישראל.

9.1. סמכות מתן הוראות לנקיטת אמצעים לפי סעיף 10(ה) לתזכיר

מדובר בסמכות קיצונית הניתנת למס"ל להתערב ולתת הוראות לכל ארגון חיוני. אולם, סמכות זו מוגבלת לנסיבות חריגות ולראש מס"ל. להלן הערותינו לגבי הצורך לחדד אותה עוד:

- על ראש מס"ל למצוא ש"מתקיים סיכון סייבר משמעותי העלול לאפשר תקיפת סייבר חמורה". אנו סבורות כי יש פגם בכך שהמונח "סיכון סייבר משמעותי" אינו מוגדר. על מנת להבטיח וודאות ובהירות בהפעלת הסמכות אנו מציעות להוסיף בחוק תנאים או נסיבות המקימות "סיכון סייבר משמעותי".

- לשם הפעלת הסמכות יש צורך באישור ראש הממשלה. אם מתן ההוראה אינו סובל דיחוי, יכול ראש מס"ל להפעיל את סמכותו, אולם ההוראה שייתן תהא תקפה ל-48 שעות בלבד. בעוד אישור ראש הממשלה הוא סביר ורלוונטי כאשר מדובר בארגון חיוני מהמגזר הממשלתי, התניית הפעלת סמכות קיצונית ביחס לארגון חיוני מהמגזר הפרטי - באישור ראש הממשלה, שהוא גורם פוליטי, היא בעייתית ועלולה להוות פתח ליחסי קח תן בין ראש הממשלה למגזר הפרטי. אנו מציעות שאישור כאמור יינתן על ידי יועמ"ש הממשלה.

- טרם מתן ההוראה על ראש מס"ל לשקול את ההשפעה על פעילות הארגון החיוני ועל צדדים שלישיים, לרבות הזכות לפרטיות, את העלות הכלכלית המוערכת של יישום ההוראות ואת השפעתן האפשרית על הרציפות התפקודית של הארגון, ולהבטיח את מידתיות ההוראה. אנו מציעות להבהיר בניסוח הסעיף שהכוונה היא לבחינת השפעת מתן ההוראות על פעילות הארגון ולא בחינת השפעת התממשות הסיכון המשמעותי לתקיפת סייבר חמורה.

- אנו מציעות לקבוע לוח זמנים ליישום ההוראות הניתנות בהקשר זה, בעיקר מאחר ואי ציות למתן ההוראה הוא עבירה פלילית והפרה מינהלית.[148]

[148] סעיפים 23(ב)(1), 44(א)(1) לתזכיר, לעיל ה"ש 36.

9.2. סמכות מתן הוראות לארגון חיוני ולספק שירותים דיגיטליים ושירותי אחסון

סעיף 17 מעניק לעובד מוסמך או למנהל בכיר במס"ל את הסמכויות המוקנות למנהל בכיר ברשות מוסמכת - לקבוע האם מדובר בתקיפת סייבר חמורה לפי סעיף 14, לתת הוראות לארגון חיוני מהמגזר הפרטי ומהמגזר הממשלתי וכן לספק שירותים דיגיטלים ושירותי אחסון, גם אם אינו ארגון חיוני. מדובר בסמכות חריגה בשני היבטים: האחד – התערבות מס"ל בהתנהלות הרשויות המוסמכות ופגיעה בעיקרון האסדרה הביזורית, והשני – מתן הוראות גם לארגון שאינו חיוני, אם הוא במגזר ספקי השירותים הדיגיטליים ושירותי האחסון. לפיכך, אנו סבורות שסמכות זו צריכה להינתן במשורה ובנסיבות מוגבלות.

לפי סעיף 17(ב) לתזכיר הפעלת הסמכות לפי סעיפים 15 או 16 כלפי ארגון חיוני תיעשה:

(1) לבקשת רשות מוסמכת.

(2) אם ראש מס"ל קבע שקיים חשש שתקיפת הסייבר החמורה מקיימת את אחד מארבעת המאפיינים הבאים:

(א) מתפשטת במהירות לארגונים רבים.

)ב(מתפשטת ליותר ממגזר משק אחד. לכאורה נראה שיש חפיפה בין תנאי זה לתנאי העוסק בהתפשטות במהירות של תקיפת הסייבר לארגונים רבים. אנו מציעות להבהיר שהכוונה אינה לעצם התפשטות תקיפת הסייבר אלא לכך שהיא מוכוונת מראש או תוקפת בפועל בו זמנית יותר ממגזר משק אחד.

(ג) תפגע בבטחון המדינה.

)ד(תפגע בבטחון הציבור.

בניגוד לקביעת הנסיבות בהן רשאי עובד מוסמך או מנהל בכיר במס"ל להפעיל את הסמכות לתת הוראות לפי סעיפים 15 או 16 לתזכיר, סעיף 17 לתזכיר אינו קובע תנאים או נסיבות בהן יהיה רשאי עובד מוסמך או מנהל בכיר במס"ל לקבוע שמדובר בתקיפת סייבר חמורה לפי סעיף 14 לתזכיר. לכן, לכאורה, הם רשאים לקבוע בכל עת שתקיפת הסייבר נגד ארגון חיוני או ספק שירותים דיגיטליים ושירותי אחסון היא חמורה, וכן לא ברור האם קביעה שכזו מחייבת רשות מוסמכת ותגבר על קביעה סותרת של מנהל בכיר ברשות מוסמכת. לכן אנו מציעות להבהיר בתזכיר באילו נסיבות רשאי יהיה עובד מוסמך או מנהל בכיר במס"ל לקבוע שתקיפת סייבר על ארגון חיוני שאינו במגזר משק המאוסדר על ידי מס"ל היא תקיפת סייבר חמורה, והאם קביעתו זו תחייב את הרשות המוסמכת בכל מקרה.

באשר להפעלת סמכויות אלו ביחס לספק שירותים דיגיטליים או שירותי אחסון שאינם עונים להגדרת ארגון חיוני, סמכות זו קיימת כבר היום לפי הוראת השעה.[149] כמו כן, לפי דברי ההסבר, סמכות זו נדרשת בשל המאפיינים הייחודיים של מגזר משק זה, החיבוריות הגבוהה של ספקי שירותי אחסון וספקי שירותים דיגיטליים העלולה להיות מנוצלת על ידי תוקפים לגרימת נזק רחב

[149] סעיף 3 להוראת השעה, לעיל ה"ש 34.

היקף, ופוטנציאל הנזק למשק הגלום בתקיפת סייבר חמורה נגד ארגונים במגזר זה גם אם אינם ארגונים חיוניים.

גם דירקטיבת NIS2 חלה, נוסף על ארגונים המוגדרים כחיוניים לפי מדד כמותי במגזרי משק מסוימים, גם על ארגונים שאינם עומדים במדד הכמותי הפועלים באחד מהמגזרים המנויים כאשר: (1) מדובר בארגונים המספקים שירותי רשתות תקשורת אלקטרוניות ציבוריות, שירותי תקשורת אלקטורניים הזמינים לציבור, ספקי שירותי אמון,[150] או ספקי שמות מתחם ושמות מתחם מהרמה הגבוה (TLD); (2) ארגונים שהם הספק היחיד של שירות החיוני לשימור פעילות חברתית או כלכלית קריטית במדינה; (3) כאשר הפרעה לשירות המסופק על ידי הארגון עשויה להשפיע באופן משמעותי על ביטחון הציבור, אבטחתו או בריאותו; (4) הפרעה לשירות המסופק על ידי הארגון עשויה להוביל לסיכון מערכתי משמעותי, בייחוד במגזרים בהם השפעה כאמור עשויה להיות חוצת גבולות; (5) ארגון שהוא גוף ציבורי של הממשלה המרכזית כהגדרתה המדינה החברה בחוק מקומי או גוף מדינתי אזורי, כפי שיקבע על ידי הממשלה המרכזית בחוק, שלהפרעה לשירות שלו עשויה להיות השפעה משמעותית על פעילות חברתית או כלכלית קריטית.[151]

לכן, לדעתנו, החלתה על ארגונים שאינם חיוניים במגזר השירותים הדיגיטליים ושירותי האחסון - מוצדקת.

9.3. סמכות סיוע בהגנת סייבר

סעיף 42 לתזכיר מעגן את סמכות מס"ל לספק סיוע לארגון המעוניין בכך, ובלבד שמס"ל קבע שיש אינטרס לאומי בסיוע לו בשגרה, או שיש אינטרס לאומי בסיוע לו אגב תקיפת סייבר נגדו או באמצעותו.[152] מדובר בסמכות **וולונטרית** המסופקת לבקשתו של כל ארגון, גם כזה שאינו ארגון חיוני, מהמגזר הפרטי או הציבורי, וגם אם אינו ממגזר משק המנוי בתזכיר. למרות זאת, יש לקבוע קריטריונים, בחוק עצמו או בנוהל שיפורסם בציבור, ל"אינטרס לאומי" המצדיק את מתן הסיוע, על מנת לשחרר את ראש מס"ל מלחצים פוליטיים בעת קביעתו זו.

10. תיעוד הוראות הניתנות במסגרת סמכויות הרשות המוסמכת ומס"ל

סעיף 50 בתזכיר קובע שעל עובד מוסמך מגזרי או עובד מוסמך במערך הסייבר לתעד בכתב הוראות שניתנו לארגון לפי סעיפים 15, 16 ו 17 לארגון ולמסור לארגון נוסח כתוב של ההוראות שאינו מכיר מידע מסווג ברמת "שמור "ומעלה, בהקדם האפשרי לאחר מתן ההוראה. הקושי שמעורר הסעיף נעוץ בכך שכאשר רשות מנהלית נותנת הוראות לארגון המאוסדר על ידה במגזר הפרטי עליה לתעד זאת ולהעביר אותה בכתב לארגון, אולם הסעיף אינו מחייב לתעד הוראה הניתנת על ידי ראש מס"ל לפי סעיף 10(ה). לפיכך, אנו מציעות לקבוע שכל הוראה הניתנת על ידי עובד מוסמך מגזרי או עובד

---

[150] ספקי שירותי אמון מוגדרים כספקים של שירותים אלקטרונים בתשלום הכוללים יצירה, אימות, ואישרור של חתימה אלקטרונית, אימות אתר אינטרנט או שימור חתימה אלקטרונית. ראו Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, בסעיף 3.

[151] דירקטיבת NIS2, לעיל ה"ש 41, סעיף (2)2, סעיפי הקדמה 7, 11, 32, 93.

[152] סעיף 42(ו) לתזכיר, לעיל ה"ש 36.

מוסמך במס"ל לפי סעיפים 10(ה), 15, 16 ו-17 תהיה מתועדת באופן מלא ככל האפשר ונוסח כתוב שלה יימסר לארגון.

11. סמכות ראש חטיבת הגנה בסייבר בצה"ל להכריז על תקיפת סייבר חמורה

סעיף 18 מאפשר לראש חטיבת הגנה בסייבר בצה"ל להיכנס בנעליו של מנהל בכיר ברשות מוסמכת, ולקבוע שמדובר בתקיפת סייבר חמורה לפי סעיף 14 לתזכיר. לדעתנו יש לחייב את ראש חטיבת ההגנה בסייבר בצה"ל לעדכן את מס"ל ואת הרשות המוסמכת הרלוונטית בקביעתו, על מנת למנוע אי בהירות וכפל סמכויות.

12. סודיות, הגבלת שימוש ומחיקה

סעיף 49 לתזכיר קובע חובת סודיות על מידע אישי המגיע לאדם לפי החוק המוצע בתזכיר, וכן מגביל את שמירת מידע אישי כאמור ומחייב את מחיקתו, בהתאם לעיקרון הנחיצות והגבלת המטרה, שהם עמודי יסוד בהגנת הפרטיות.

12.1. שמירת מידע אישי

סעיף 49(ב) מתיר שמירה של מידע אישי, בהיקף המזערי הנדרש, מעבר לשנתיים, אם הוא "חיוני לזיהוי מאפייני תקיפת סייבר או להתמודדות עם תקיפת סייבר או חשש לה או שהוא נדרש להליכים לפי פרק ה' או פרק ז'". לכאורה, מידע אישי בהתאם לתנאים אלו עשוי להישמר לעד והדבר בעייתי נוכח החשש מפני חשיפתו ופגיעה בפרטיות. לכן אנו מציעות לקבוע שמידע אישי שימשיך להישמר גם לאחר שנתיים מעת קבלתו, יימחק מידע כאשר לא יהיה חיוני יותר לזיהוי מאפייני תקיפת הסייבר, להתמודדות עמה או עם חשש לה או לא יהיה דרוש עוד להליכים לפי פרקים ה או ז לתזכיר.

12.2. כתובת IP

בדברי ההסבר לסעיף 49 נאמר כי "לעניין חוק זה כתובת IP לא תחשב מידע אישי". הטעם לכך הוא שכתובת IP היא מידע חיוני לכל הפעולות הכרוכות בהגנת סייבר. עם זאת המדובר בקביעה מוזרה ובעייתית.

תיקון 13 לחוק הגנת הפרטיות הרחיב את הגדרת "מידע אישי" ועתה "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי" במאמץ סביר, במישרין או בעקיפין, הוא מידע אישי.[153] הרחבת הגדרת "מידע אישי" נעשתה, בין השאר, לשם הגברת התאימות עם ה-GDPR, וכך משמש ה-GDPR כמקור לקבלת השראה לפרשנות הוראות חוק הגנת הפרטיות. ה-GDPR, ואף פסיקה שהתקבלה לאחר חקיקתו באיחוד האירופי קובעים במפורש כי כתובת IP היא מידע אישי.[154]

---

[153] סעיף 3 לחוק הגנת הפרטיות, לעיל ה"ש 22.

[154] סעיף הקדמה 30 ל-GDPR, לעיל ה"ש 44, וכן Case C-582/14, Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779 (Oct. 19, 2016).

למרות זאת, באיחוד האירופי מתאפשר עיבוד של כתובת IP לצורכי הגנת סייבר מתוקף הבסיסים החוקיים לעיבוד מידע אישי, בפרט האפשרות לעבד מידע אישי לצורך ציות לחוק או לשם הגשמת אינטרס לגיטימי של בעל השליטה במידע.[155]

חוק הגנת הפרטיות, גם לאחר תיקון 13, אינו כולל בסיסים חוקיים המתירים עיבוד מידע אישי לבד מהסכמת האדם שהמידע אודותיו. לפיכך, לא ניתן לעבד כתובת IP, המהווה מידע אישי, ללא הסכמת האדם שהמידע אודותיו, גם כאשר עיבוד המידע נעשה לצורך הגנת סייבר.[156]

הפתרון המוצע לכך בתזכיר – הבהרה בדברי ההסבר לתזכיר שכתובת IP לא תיחשב מידע אישי לעניין החוק המוצע בתזכיר, סותר את המצב המשפטי ויתקשה לעמוד בבחינה משפטית בבית משפט. על מנת לאפשר עיבוד כתובת IP לשם הגנת סייבר אנו מציעות לעגן בתזכיר במפורש הוראה המאפשרת זאת, על אף המגבלות האמורות בחוק הגנת הפרטיות, בנוסח הבא:

"עיבוד כתובת IP אינו פוגע בפרטיות ואינו מפר את חוק הגנת הפרטיות, התשמ"א – 1981, כל עוד הוא נעשה בהיקף שאינו עולה על הנדרש לשם ביצוע חוק זו או למטרת ביצוע סמכות של אדם להגנת סייבר לפי דין, או לפי צו בית משפט."

13. השלכות אפשריות על ההכרה האירופית בתאימות דיני הגנת הפרטיות בישראל

כאמור, התזכיר מעניק לרשויות המוסמכות ולמס"ל סמכות לדרוש מארגון חיוני להציג ידיעה או מסמך, לרבות פלט, הנחוץ לקביעה האם מדובר בתקיפת סייבר חמורה.[157] כן מוענקת בתזכיר סמכות לרשות מוסמכת ולמס"ל לתת לארגון חיוני או לספק שירותים דיגיטלים ושירותי אחסון הוראות לביצוע פעולות להגנת סייבר בחומר מחשב, ובכלל זה לבצע סריקה, עיבוד או הסרה של חומר מחשב הנוגע לתקיפת סייבר, או להתקין סוג תוכנה שפעולה מוגבלת לרשת הארגון, או הוראות למסור ידיעה, מסמך או העתק מחומר מחשב. הפעלת סמכויות אלו מדורגת בהתאם לתנאים הקבועים בתזכיר,[158] אולם בהפעלתן עלול להיות מועבר חומר מחשב הכולל מידע אישי. כאשר מדובר בארגון המעבד מידע אישי על אזרחי האיחוד האירופי העברה כאמור חייבת לעמוד בדרישות האיחוד האירופי בהתאם להכרת נציבות האיחוד האירופי בינואר 2024 בכך שדיני הגנת הפרטיות בישראל תואמים לסטנדרט האירופי (להלן: "החלטת התאימות").

להחלטת התאימות השלכות משמעותיות על פעילותם של ארגונים ישראלים בשוק האיחוד האירופי, שכן במסגרתה הם יכולים להעביר באופן חופשי מידע אישי ממדינות אירופה לישראל, ללא צורך במחויבות רגולטוריות נוספות. כלומר, העברת מידע מאירופה לישראל כפופה לאותן הדרישות כמו העברת מידע בתוך האיחוד האירופי.[159]

---

[155] סעיף 6(1)(c), (f) ל-GDPR, לעיל ה"ש 44; Eyup Kun, *Searching for the appropriate legal basis for personal data processing under the NIS 2 Directive: Legal obligation and/or legitimate interest?*, 56 COMPUTER LAW & SECURITY REVIEW (April 2025).

[156] סעיף 1 לחוק הגנת הפרטיות, לעיל ה"ש 49.

[157] סעיף 14 לתזכיר, לעיל ה"ש 36.

[158] סעיפים 15 ו-17 לתזכיר, לעיל ה"ש 36.

[159] נציבות האיחוד האירופי אישרה את ההכרה במדינת ישראל כמדינה בעלת מעמד תאימות (Adequacy) בתחום הגנת הפרטיות, **משרד המשפטים הרשות להגנת הפרטיות** (15.01.2024, עודכן 10.07.2025).

נציבות האיחוד האירופי מנטרת התפתחויות העשויות להשפיע על החלטת התאימות, לרבות חקיקה העוסקת בגישה של רשויות המדינה למידע אישי מטעמי ביטחון לאומי וביטחון הציבור.[160] לפיכך, לשם המשך ההכרה בתאימות דיני הגנת הפרטיות ומניעת פגיעה בהחלטת התאימות, התזכיר חייב לעמוד בדרישות האירופיות ביחס לפגיעה בפרטיות עקב העברת מידע אישי לרשויות אכיפת חוק או רשויות ביטחון ועיבודו כחלק משימוש באמצעי מעקב. דרישות אלו מפורטות ב - European Essential Guarantees, שקבעה ה-EDPB:[161]

א. עיבוד המידע צריך להיות מבוסס על כללים ברורים, מדויקים ונגישים.

עיבוד המידע צריך להיעשות למטרות מסוימות, בהסכמת נושא המידע או לפי בסיס אחר הקבוע בחוק. ההצדקה לפגיעה בפרטיות צריכה להיות מפורטת בחוק, לרבות התנאים והנסיבות בהן ניתן לעבד מידע תוך פגיעה בפרטיות, היקף הפגיעה ואמצעי המעקב בהם יעשה שימוש כמו גם אמצעי הגנה מינימליים. החוק צריך להעניק גם לאדם הנפגע זכויות אפקטיביות וסעדים ברי אכיפה במקרה של הפרתו על ידי רשות המדינה. המבחן לעמידתו של החוק בדרישות אלו הוא האם אדם יכול להסתמך עליו ולטעון להפרתו בפני בית משפט.[162]

ב. יש להדגים נחיצות ומידתיות עיבוד המידע לצורך הגשמת מטרות חוקיות.

הפגיעה בפרטיות צריכה להיות מידתית ונחוצה לשם מטרות שיש בהם אינטרס ציבורי, שמוכר על ידי האיחוד האירופי, או לשם הגנה על זכויות צדדים שלישיים.

במסגרת בחינת המידתיות, יבוצע איזון בין חומרת הפגיעה בזכות לפרטיות לבין חשיבות האינטרס הציבורי שלשם הגשמתו מבוצעת הפגיעה. ה-EDPB הבהיר עוד שביטחון לאומי הוא מטרה חשובה ביותר המצדיקה פגיעה משמעותית יותר בזכות לפרטיות, לעומת מטרה כגון התמודדות עם פשיעה. אולם, לשם כך יש להוכיח שהמדינה מתמודדת עכשיו או צפויה להתמודד עם סיכון משמעותי אמיתי לביטחון הלאומי.

מבחינת הוכחת הנחיצות, נדרש לא רק שהחוק יקבע כללים ברורים להפעלת סמכות הפוגעת בפרטיות ולהיקף הפגיעה. יש צורך בעיגון ברור של אמצעי הגנה מינימליים כך שיועמדו לרשות נושא המידע ערבויות מספיקות להגנה אפקטיבית על המידע האישי שלו מפני שימוש לרעה. שמירת מידע שהתקבל אגב פגיעה בפרטיות כאמור תוגבל גם כן בהתאם לנחיצותה.[163]

ג. יש צורך במנגנון פיקוח חיצוני

---

[160] סעיף 45(3) ל-GDPR, לעיל ה"ש 44.

[161] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board (EDPB) (Adopted on 10 November 2020), בעמ' 5-8.

[162] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board (EDPB) (Adopted on 10 November 2020), בעמ' 8-10.

[163] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board (EDPB) (Adopted on 10 November 2020), בעמ' 10-12.

הפגיעה בפרטיות על ידי רשויות המדינה צריכה להיות כפופה למערכת פיקוח יעילה, עצמאית וחסרת פניות, בראשות שופט או גוף עצמאי אחר (רשות מינהלית או גוף פרלמנטרי) אשר תינתן לו גישה לכל המסמכים הרלוונטיים, לרבות מסמכים חסויים. כן יש להביא בחשבון את מידת השקיפות של פעילות גוף זה.[164]

ד. יש צורך בסעד אפקטיבי זמין לאדם שזכותו לפרטיות נפגעה

לשם כך נדרש שאדם שזכותו נפגעה יוכל לפנות לבית משפט או לגוף הפיקוח העצמאי על מנת לקבל גישה למידע אישי שלו או לדרוש את תיקונו או מחיקתו.[165]

בבחינת התזכיר עולה החשש שהיבטים מצומצמים בו עלולים לשמש בסיס לטענה לאי עמידה בתנאי ה - European Essential Guarantees. התנאים להפעלת הסמכות אינם ברורים דיים, ובתוצאה קשה לומר שעיבוד המידע האישי מבוסס על כללים ברורים ומדויקם. הגדרת תקיפת סייבר חמורה צריכה להיות מדויקת יותר.[166] כן נדרשת הבהרה של התנאים להפעלת סמכות מתן ההוראות ובפרט מתי מתקיים סיכון סייבר משמעותי לתקיפת סייבר חמורה ומתי היא תחשב לכזו שמחייבת את מעורבותו של מס"ל או הרשות המוסמכת.[167]

נוסף על כך, ההחרגה הגורפת של מס"ל ופעולותיו מחוק חופש המידע, היעדר דיווח שנתי מצד הרשויות המוסמכות לוועדת חו"ב וליועמ"ש הכנסת, העובדה שהדיווח אינו כולל מידע בנוגע למספר ההוראות שניתנו לפי סעיפים 15, 16 ו-17 לתזכיר, והקביעה שהדיווחים יהיו חסויים עלולים לפגוע בתפקודם של ועדת חו"ב, יועמ"ש הכנסת בתי המשפט כמנגנון פיקוח עצמאי, שכן המידע אשר יוצג בפניהם עשוי להיות חסר וכן אינו חשוף לביקורת ציבורית. כך גם בידי האזרחים לא יהיה מידע מספק אשר יאפשר להם לפנות לבית משפט בבקשה לסעד אפקטיבי בטענה לפגיעה בפרטיותם. אולם, תיקון נושאים אלו כמוצע על ידנו,[168] עשוי להביא להגברת השקיפות ולחיזוק מנגנון הפיקוח העצמאי של ועדת חו"ב ויועמ"ש הכנסת, לצד קיומה של מערכת משפט עצמאית במדינה.

לבסוף, סעיף 49 לתזכיר קובע חובת סודיות ומנגנון למחיקת המידע בהתאם לעיקרון הנחיצות. אולם, יש להבהיר שעיקרון הנחיצות ימשיך לעמוד בעינו ויחייב את מחיקת המידע גם אם זו לא נעשתה בחלוף שנתיים ממועד איסופו. כן הקביעה התמוהה שכתובת IP לא תחשב למידע אישי לצורך התזכיר היא בעייתית ועלול לפגוע בדרישה לקיומו של סעד אפקטיבי בידי האדם שפרטיותו נפגעה. לדעתנו יש לקבוע הוראה מפורשת המתירה עיבוד כתובת IP תוך הכפפת עיבוד שכזה לעיקרון המידתיות והנחיצות.[169]

---

[164] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board (EDPB) (Adopted on 10 November 2020), בעמ' 12.

[165] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, European Data Protection Board (EDPB) (Adopted on 10 November 2020), בעמ' 13-15.

[166] ראו הצעתנו בסעיף 7 לעיל.

[167] ראו הצעתנו בסעיפים 8.1, 9.1, ו - 9.2 לעיל.

[168] ראו הצעותינו בסעיף 2.1 לעיל.

[169] ראו הדיון בסעיף 12 לעיל.

תיקון התזכיר בנושאים אלו כפי שמוצע על ידנו בחוות דעת זו, יוביל לדעתנו לעמידת התזכיר בתנאי ה - European Essential Guarantees המפורטים לעיל.

<u>חלק ד: סיכום והמלצות</u>

תזכיר החוק מציע מתווה מאוזן יחסית ל"אסדרה ביזורית מנוהלת" של המגזר הפרטי והציבורי לשם מיטוב הגנת הסייבר הלאומית בישראל. נוכח תקיפות הסייבר ההולכות וגוברות בהיקפן, כמותן ומורכבותן על מדינת ישראל בשנים האחרונות, הפיכתו של התזכיר לחקיקה ראשית נחוצה מאין כמותה. עם זאת, יש לתקן מספר נושאים בתזכיר על מנת לשפרו ולהביא לחקיקתו המהירה. בטבלה שלהלן נסכם בקצרה את ההערות והמלצות לתיקון כפי שפורטו בהרחבה בגוף חוות הדעת.

<u>טבלת סיכום ההערות וההמלצות לתיקון</u>

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
איזון המאפיין ההיברידי של מס"ל כגוף המאסדר את המגזר הציבורי והפרטי לצד היבטים ביטחוניים	2.12	להגביר את שקיפות פעולותיו של מס"ל, בין השאר ע"י וויתור על ההחרגה הגורפת של מס"ל וכל פעולותיו מחוק חופש המידע. לקבוע כי רשימת המומחים החיצוניים לפי סעיף 48 לתזכיר תפורסם בציבור. להרחיב את נושאי הדיווח השנתי של מס"ל ליועמ"ש הממשלה ולוועדת חו"ב של הכנסת, לחייב גם את הרשויות המוסמכות בדיווחים דומים, ולהבטיח שהדיווחים יהיו אגרגטיביים ויפורסמו לציבור. לעגן בחוק את תנאי הכשירות למינוי ראש מס"ל ולחייב את פרסום מינויו ברשומות.
איזון המאפיין ההיברידי של מס"ל כגוף המאסדר את המגזר הציבורי והפרטי לצד היבטים ביטחוניים	2.2	לעגן בחוק את עצמאות מס"ל לא רק כ"יחידה עצמאית במשרד ראש הממשלה", כלשון סעיף 2(א) לתזכיר, אלא גם מבחינת התקציבים, גיוס והעסקת עובדים, ועצמאות היעוץ המשפטי.
תפקידי מס"ל	2.32.3	להבהיר למה הכוונה "אסטרטגיה לאומית" ו"רמת הגנת הסייבר הלאומית". לבחון האם מתפקידו של מס"ל לפעול להעלאת המודעות בציבור.

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
		לבחון מחדש את תפקידי מס"ל לקדם ולעודד מחקר ופיתוח ולקדם בחינת והטמעת טכנולוגיות.
אסדרה ביזורית – חלוקה למגזרי משק	3.13.1	לבחון תחולת התזכיר על גופי ממשל או תאגידים סטטוטוריים שאינם מוגדרים כמשרדי ממשלה או נתונים להנחיה לפי החוק להסדרת הביטחון בגופים ציבוריים. לבחון הוספת מגזרים כגון מגזר הפיננסים והביטוח, מגזר יצרני התרופות וציוד רפואי. לבחון מחדש את רשימת הגופים המנויים בתוספת לחוק להסדרת הביטחון בגופים ציבוריים על מנת להבטיח קוהרנטיות. לבחון מחדש את החרגת המשטרה מתחולת התזכיר.
אסדרה ביזורית – הגורם המאסדר	3.2.1	יש להמיר את סמכות הגורם המאסדר לקבוע שארגון אינו ארגון חיוני בסעיף 8(ב) לתזכיר לסמכות של הוועדה המייעצת בלבד או ועדה המורכבת ממספר בעלי תפקידים ברשות המוסמכת כגון הממונה, מנהל בכיר ביחידה המגזרית ומנהל בכיר נוסף ברשות המוסמכת. להתנות את סמכות בגורם המאסדר לקבוע דרישות הגנת סייבר נוספות בסעיף 10(ג) לתזכיר בהתייעצות גם עם מנהל בכיר ביחידה המגזרית, במידה שמדובר במגזר משק המאוסדר על ידי רשות מוסמכת, וכן באישור החלטת הגורם המאסדר על ידי ועדת כנסת רלוונטית. להתנות את סמכות הגורם המאסדר לקבוע סכומי עיצומים מופחתים לפי סעיף 28(ב) לתזכיר באישור ועדת כנסת רלוונטית. להתנות את סמכות הגורם המאסדר להוסיף מגזר משק לפי סעיף 52(ג) לתזכיר בהתייעצות עם הרשות המוסמכת ובאישור ועדת הכנסת הרלוונטית.

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
אסדרה ביזורית – היבטים מבניים ברשות המוסמכת	3.2.2 - 3.2.3	למצב את היחידה המגזרית כבעלת סמכויות ההחלטה בכל הנושאים הנוגעים להגנת הסייבר או דורשים מומחיות בתחום. לקבוע בחוק את מיקומה הארגוני והתקנים הנדרשים לצורך עבודתה של היחידה המגזרית.
אסדרה ביזורית – תפקידי היחידה המגזרית	3.2.33.2.3	להטיל על היחידה המגזרית חובה למפות באופן עתי את הארגונים החיוניים במגזר המשק הרלוונטי לה. להגדיר מהם "נתוני רמת ההגנה בסייבר בארגונים חיוניים" המועברים מהיחידה המגזרית למס"ל על מנת להבטיח שהיחידה המגזרית תעביר את הנתונים הנחוצים למס"ל לשם קידום הגנת הסייבר הלאומית.
אסדרה ביזורית – ההיבט הניהולי – הנחיה מקצועית של היחידות המגזריות	4.1	לחזק את ההיבט הניהולי באסדרה הביזורית, נוכח חוסר האחידות בתפקוד היחידות המגזריות לאורך השנים, על ידי חיוב באישור מס"ל של תוכנית העבודה השנתית או הרב שנתית של היחידה המגזרית
אסדרה ביזורית – ההיבט הניהולי ביחס למגזרים שאינם נמנים על מגזרי המשק	4.2	לעגן סמכות שבשיקול דעת למס"ל לבדוק באופן עתי את ההסדרה המגזרית במגזרים שאינם נמנים על מגזרי המשק.
חובת הגנת סייבר	5.15.1	לתקן את סעיף 10(א): "ארגון אחראי להבטחת רמת הגנת סייבר בהתאם לסוג ואופי פעילותו תוך ניהול סיכון הולם"
הגדרת ארגון חיוני	5.25.2	להוסיף לרשימת התבחינים בתוספת השלישית חברות המייצרות תרופות ובתי מרקחת במגזר הבריאות, צ'אט בוטים שמבוססים על מודלים גדולים של שפה ולמוצרים הכוללים רכיבים דיגיטליים (IoT) במגזר שירותים דיגיטליים ושירותי אחסון. להסמיך את מס"ל בהתייעצות עם הרשויות המוסמכות הרלוונטיות, להחליט לאיזה מגזר

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
		ישתייך ארגון חיוני שעומד בתבחינים ביותר ממגזר אחד.
רמת הגנת סייבר בסיסית – תמריצים חסרים למגזר הציבורי ולרשויות מקומיות	5.3.1.15.3.1.1	אין לפטור משרדי ממשלה ורשויות מקומיות מעיצומים כספיים.
רמת הגנת סייבר בסיסית – תמריצים: גובה העיצום הכספי	5.3.1.25.3.1.2	לאמץ מגנון לקביעת סכום העיצום הכספי בהתאם לתקרה מקסימלית גבוהה או אחוז מהמחזור השנתי האחרון, הגבוה מבין השניים. אחרת סכומי העיצומים עשויים להיחשב כהפרה יעילה על ידי חלק מהארגונים.
רמת הגנת סייבר בסיסית – תמריצים: אחריות נושאי משרה	5.3.25.3.2	להרחיב את האחריות המוטלת על נושאי המשרה בארגון גם לפיקוח והבטחת ציות לחובות הגנת הסייבר הבסיסית.
רמת הגנת סייבר בסיסית – תמריצים: תקינה כחלופה לדרישות החוק	5.3.35.3.3	להוסיף מגזרים לתוספת השישית לתזכיר למודל הפטור על בסיס תקן. להבהיר שהפטור הוא רק מציות לחובת רמת הגנת הסייבר הבסיסית לפי סעיף 10(ה) וסמכויות הפיקוח המינהלי לפי סעיפים 12 ו 13, ואינו מאיין את הסמכויות לפי סעיפים 10(ה), 15, 16 ו -17 לתזכיר.
חובת הדיווח	6.1 - 6.2	להבהיר שהדיווח הוא לגורם אחד בלבד – מס"ל, אשר יפיץ את הדיווח לגורמים נוספים. לשקול שהדיווח למס"ל יחול גם על חובת הדיווח לפי תקנות אבטחת מידע. להוסיף מועדים לדיווחי ביניים לאחר הדיווח הראשוני והמיידי, ולשקול הסמכת מס"ל לדרוש דיווחי ביניים נוספים.
חובת דיווח לארגון אחר	6.36.3	להבהיר האם מדובר בחובת דיווח לכל ארגון או רק לארגון חיוני.

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
		לקבוע תנאים או נסיבות בהן ינתן פטור מחובת הדיווח לארגון אחר. ההחלטה בדבר פטור מחובת דיווח לארגון אחר צריכה להתקבל על ידי היחידה המגזרית. להוסיף סמכות שבשיקול דעת למס"ל או לרשות המוסמכת לחייב ארגון חיוני לדווח לציבור או לציבור מקבלי השירות.
הגדרת תקיפת סייבר חמורה	77	הסמכות לקבוע שמדובר בתקיפת סייבר חמורה צריכה להיות בידי היחידה המגזרית. יש לבחון מחדש את הגדרת תקיפת סייבר חמורה נוכח הגדרת תקיפת סייבר משמעותית בסעיף 11 ולוודא שאין חפיפה בין סעיפים 14(א)(1) ו (2) ו 14(א)(4) ו – (5) לתזכיר.
סמכות מתן הוראות לפי סעיפים 15 או 16 לתזכיר	8.18.1	החלטה בדבר קיומו של חשש ממשי להתרחשותה העבשווית או העתידית של תקיפת סייבר חמורה הדורשת את מעורבותו צריכה להתקבל על ידי בעל תפקיד ביחידה המגזרית. להבהיר בחוק מהם התנאים, הנסיבות או השיקולים שיובילו להחלטה שמדובר בתקיפת "סייבר חמורה הדורשת את מעורבותו". להוסיף תנאים או שיקולים שעל העובד המוסמך המגזרי לשקול בבואו לקבל החלטה האם הארגון החיוני פעל באופן הולם. להוסיף לשיקולים הנשקלים במתן הוראות בגוף ממשלתי גם את העלות הכלכלית של יישום ההוראות וההשפעה על הרציפות התפקודית. לקבוע מועד אחרון ליישום ההוראות על ידי הגוף הממשלתי.
חוות דעת מקדמית	8.28.2	להבהיר שחוות דעת מקדמית תינתן על ידי היחידה המגזרית.

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
		לקבוע לוח זמנים למתן מענה לבקשת חוות דעת מגזרית. להוסיף שיקולים או נסיבות במסגרתן יכולה רשות מוסמכת לסרב לתת חוות דעת מקדמית. לחייב את הרשות המוסמכת לעדכן את מס"ל בתוכן חוות הדעת המקדמית וכן לפרסמה בציבור.
סמכות מס"ל להורות על נקיטת אמצעים לפי סעיף 10(ה) לתזכיר	9.19.1	להסביר מהם התנאים או הנסיבות המקימים "סיכון סייבר משמעותי" כאשר ההוראות ניתנות לארגן חיוני מהמגזר הפרטי האישור צריך להינתן על ידי יועמ"ש הממשלה ולא ראש הממשלה. לקבוע לוח זמנים ליישום ההוראה לנקיטת אמצעים על ידי הארגון החיוני.
סמכות מס"ל לפי סעיף 17 לתזכיר	9.29.2	להבהיר את התנאי לפיו עובד מוסמך יהיה רשאי להפעיל את הסמכות לפי סעיף 15 או 16 אם תקיפת הסייבר תתפשט במהירות ליותר ממגזר משק אחד לפי סעיף 17(ב), ומה ההבדל בינה לבין האפשרות להתפשטות מהירה לארגונים רבים. להבהיר מתי יהיה עובד מוסמך במס"ל לפעול לפי סעיף 14 ומה קורה אם החלטתו תעמוד בסתירה עם קביעת מנהל בכיר ברשות מוסמכת.
סמכות מס"ל לספק סיוע בהגנת סייבר	9.39.3	להבהיר בחוק או בנוהל שיפורסם לציבור מהם הקריטריונים לקביעה שיש אינטרס ציבורי המצדיק מתן סיוע לארגון.
תיעוד ההוראות ומסירתן בכתב	1010	להבהיר שגם הוראה של ראש מס"ל לפי סעיף 10(ה) חייבת להיות מתועדת ולהימסר בכתב לארגון.
סמכות ראש חטיבת ההגנה בסייבר בצה"ל	1111	להוסיף חובה לעדכן את מס"ל בקביעת היות התקיפה תקיפת סייבר חמורה.

נושא	סעיפים רלוונטיים בחוות הדעת	המלצה
סודיות ושימוש במידע אישי	12	להבהיר שבכל מקרה בו נשמר מידע מעבר לשנתיים, יש למחוק אותו מיד כאשר אין בו צורך יותר. ההבהרה בדברי ההסבר לפיה כתובת IP לא תחשב מידע אישי לעניין חוק זה אינה תקפה. להוסיף הוראה המתירה עיבוד כתובת IP לצורכי החוק: "עיבוד כתובת IP אינו פוגע בפרטיות ואינו מפר את חוק הגנת הפרטיות, התשמ"א – 1981, כל עוד הוא נעשה בהיקף שאינו עולה על הנדרש לשם ביצוע חוק זו או למטרת ביצוע סמכות של אדם להגנת סייבר לפי דין, או לפי צו בית משפט."