תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018

שינויים מוצעים על ידי איגוד האינטרנט הישראלי (ע"ר) - 09/08/2018

פרק א': פרשנות

הגדרות

1. בחוק זה -

" איום סייבר" - סיכון ממשי להתרחשות תקיפת סייבר;

" אינטרס חיוני" – כל אחד מאלה:

(1) ביטחון המדינה, ביטחון הציבור או ~~בטיחותו~~בריאותו;

(2) חיי אדם;

(3) פגיעה משמעותית בכלכלת המדינה;

(4) תפקודן התקין של תשתיות, מערכות או שירותים חיוניים, -בשגרה או בחירום, שיש סיכון ממשי כי פגיעה בהם תגרום נזק משמעותי לפעילותו התקינה של המשק בישראל, מסוג שייקבע בתקנות~~בשגרה או בחירום~~, ובכלל זה שירותי האינטרנט והתקשורת;

~~(5) תפקודם התקין של ארגונים המספקים שירותים בהיקף משמעותי;~~

(5)~~(6)~~ מניעת סכנה ניכרת לסביבה ~~או לבריאות הציבור~~;

(6)~~(7)~~ מניעת פגיעה משמעותית בפרטיות בהיקף שקבע שר המשפטים בצו, באישור ועדת החוקה חוק ומשפט של הכנסת~~או בנפש מידע משמעותי~~;

(7)~~(8)~~ אינטרס שקבע ראש הממשלה בצו לאחר התייעצות עם השר הנוגע בדבר ובאישור ועדת הכנסת לחוק.

"ארגון" – מוסד כהגדרתו בסעיף 35 לפקודת הראיות;

"ארגון מפוקח" – ארגון הפועל בתחום שמפוקח על ידי רשות מאסדרת כמשמעותה בסעיף 47, או על ידי המערך לפי סעיף 57 או 61;

"בית המשפט" – שופט בית משפט מחוזי שנשיא אותו בית המשפט המחוזי הסמיכו לדון בבקשות על פי חוק זה;

"גוף מיוחד" – כל אחד מאלה:

(1) צבא ההגנה לישראל;

(2) שירות הביטחון הכללי;

~~(3) משטרת ישראל;~~

(3)~~(4)~~ המוסד למודיעין ולתפקידים מיוחדים;

~~(5)~~(4) הממונה על הביטחון במערכת הביטחון;

"גורם אחראי במערך" – עובד מערך בכיר שהוסמך לפי חוק זה לבצע את הפעולות הקבועות בחוק זה או לפיו;

"הגנת הסייבר" - מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות אבטחת מידע;

"המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר" – נדרשת הגדרה

"ועדת הכנסת לחוק" – ועדה משותפת לוועדת חוק ובטחון, ועדת חוקה, חוק ומשפט וועדת הכלכלה של הכנסת"

"חומר מחשב, מחשב, פלט, שפה קריאת מחשב, תוכנה" – כהגדרתם בחוק המחשבים;

"חוק האזנת סתר" – חוק האזנת סתר, התשל"ט-1979;[1]

"חוק הגנת הפרטיות" – חוק הגנת הפרטיות, התשמ"א-1981;[2]

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995;[3]

"חוק הסדרת הבטחון" – חוק הסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998

"חוק נתוני תקשורת" - חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007;

"חוק התקשורת" – חוק התקשורת (בזק ושידורים), התשמ"ב -1982;[4]

"חפץ" - לרבות חומר מחשב ופלט, כהגדרתם בחוק המחשבים;

"מידע" – מידע כהגדרתו בחוק המחשבים ובלבד שאינו מאפשר במישרין לזהות אדם;

" מידע בעל ערך אבטחתי" - מידע שיש בו כדי לסייע לאיתור תקיפת סייבר, התמודדות עמה או מניעתה ובכלל זה אחד מאלה:

(1) סממנים (indicators) - נתונים המצביעים על תקיפת סייבר או איום סייבר;

(2) מידע על חולשות במערכות ממוחשבות, ברכיביהן, בנהלים הקשורים במערכות אלה או בתהליכים הקשורים אליהן, אשר ניתן לנצל כדי לייצר תקיפת סייבר;

(3) מידע על תוכנות ~~או נוזקות~~ או אמצעים אחרים ~~שמטרתן~~ המאפשרים ~~יצירת~~ תקיפת סייבר ~~או גרימת נזק~~;

(4) מידע על שיטות ~~ואמצעים~~ לביצוע תקיפת סייבר;

---

[1] ס"ח התשל"ט, עמ' 118; התשע"ז, עמ' 1060
[2] ס"ח התשמ"א, עמ' 128; תשע"ז, עמ' 986
[3] ס"ח התשנ"ה, עמ' 366; התשע"ב עמ' 514
[4] ס"ח התשמ"ב, עמ' 218; התשע"ו, עמ' 1177

(5) מידע על שיטות ואמצעים להתמודדות עם תקיפות סייבר.

"מידע בעל ערך אבטחתי רגיש" – מידע בעל ערך אבטחתי אשר עובד המערך סימן הגבלות על הפצתו, וכל עוד המידע לא פורסם לרבים כדין;

" מידע לא מזוהה" – מידע שלא מאפשר זיהוי של יחיד או ארגון באמצעים סבירים;

" מידע מוגן" – כל אחד מאלה:

(1) מידע שחוק הגנת הפרטיות חל עליו;

(2) תוכן שיחה כהגדרתה לפי חוק האזנת סתר, למעט מידע בשפה קריאת מחשב או כתב שלא נועד לפענוח חזותי בידי אדם;

(3) מידע שהוא סוד מקצועי או סוד שהוא בעל ערך כלכלי, לרבות סוד מסחרי שפרסומו עלול לפגוע פגיעה ממשית בערכו, וכן מידע הנוגע לעניין מסחרי או מקצועי הקשור לעסקו של אדם, שגילויו עלול לפגוע פגיעה ממשית באינטרס מקצועי, מסחרי או כלכלי.

"סייבר" –רשתות תקשורת ציבוריות, לרבות אינטרנט, המקשרות בין מחשבים והתקני מיחשוב.

"עובד מוסמך" – עובד המערך שהוסמך לפי חוק זה לביצוע פעולה בחומר מחשב או פעולות אחרות לפי חוק זה, לאחר שעבר הכשרה הכשרה מקצועית מקיפה ומתאימה בתחום מיחשוב, אבטחת מידע, הגנת הפרטיות, חקירת מחשב והפעלת סמכויותיו לפי חוק זה, ~~מתאימה מהסוג~~ שקבע ראש המערך בכללי המערך;

"פעולה בחומר מחשב" – הפעולות המנויות להלן:

(1) חדירה לחומר מחשב;

(2) העתקה של חומר מחשב;

(3) הקלטה או ניטור של תקשורת בין מחשבים;

(4) מתן הוראות למחשב בשפה קריאת מחשב;

(5) שינוי חומר מחשב ובלבד שאין בו שינוי של מידע שהוא רשומה מוסדית או מידע הניתן ~~לפענוח חזותי~~להבנה בידי אדם; לעניין זה, "רשומה מוסדית" - כהגדרתה בסעיף 35 לפקודת הראיות;

(6) דיווח למערך בשפה קריאת מחשב על איתור סממנים ומאפייניהם;

(7) התקנת מחשב או התקן אחר ברשת תקשורת או במחשב של ארגון לשם ביצוע הפעולות המנויות בסעיפים (1) עד (6).

"פקודת סדר הדין הפלילי" - פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969;

"פקודת הראיות" – פקודת הראיות [נוסח חדש], התשל"א-1971;[5]

"תקיפת סייבר" - פעילות שיש חשש ממשי כי נועדה לפגוע באינטרס חיוני באמצעות אחד מאלה~~שנועדה לפגוע בשימוש במחשב או בחומר מחשב השמור בו, ובין היתר~~:

(1) שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;

(2) מחיקת חומר מחשב, שינויו, שיבושו או הפרעה לשימוש בו;

(3) אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;

(4) חדירה שלא כדין לחומר מחשב כמשמעותה בחוק המחשבים;

(5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר;

(6) גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הדלפתו של מידע כאמור;

(7) הפרעה או מניעת נגישות של מחשב לרשת תקשורת.

פרק ב': מערך הסייבר הלאומי ייעודו ותפקידיו

מערך הסייבר הלאומי וייעודו

2. (א) מערך הסייבר הלאומי ~~הוא גוף בטחוני מבצעי ה~~פועל במשרד ראש הממשלה לפי הוראות חוק זה והחלטות הממשלה (להלן בחוק זה ~~–~~ "המערך");

(ב) ייעוד המערך הוא הגנת מרחב הסייבר ~~וקידום ישראל כמובילה עולמית בתחום הסייבר~~הישראלי מפני תקיפות סייבר והתמודדות עם תקיפות סייבר כאשר הן מתרחשות;

(ג) ראש הממשלה הוא השר הממונה על מערך הסייבר הלאומי.

תפקידי המערך

3. תפקידי המערך הם:

(א) לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה הלאומיים האופרטיביים כנגד תקיפות סייבר;

(ב) לקדם את יכולת ההתמודדות של ישראל עם תקיפות סייבר;

~~(ג) לקדם מדיניות ומובילות ישראלית בתחום הסייבר בהתאם למדיניות הממשלה והחלטותיה;~~

~~(ד)~~(ג) לקדם שיתופי פעולה בתחום הגנת הסייבר במישור הבינלאומי ולערוך הסכמי שיתוף פעולה בתחום הגנת הסייבר;

~~(ה)~~(ד) לייעץ לממשלה וועדותיה בתחום הגנת הסייבר;

[5] דיני מדינת ישראל, נוסח חדש 18 ,עמ' 421; ס"ח תשע"ז, עמ' 388

~~(ו)~~(ה) לבצע כל תפקיד אחר בתחום הגנת הסייבר שיקבע ראש הממשלה.

ראש המערך

4. (א) הממשלה, לפי הצעת ראש הממשלה, תמנה את ראש המערך, בהתאם להוראות חוק שירות המדינה (מינויים), התשי"ט-1959[6] (להלן – "חוק המינויים") לתקופת כהונה אחת בת שש שנים.

(ב) ראש המערך יהיה מופקד על ניהול המערך ועל ביצוע תפקידיו לפי חוק זה.

(ג) לראש המערך יהיו כל הסמכויות הנתונות לפי חוק זה לעובדי המערך.

(ד) ראש המערך רשאי לאצול סמכות שניתנה לו לפי חוק זה, לעובד בכיר במערך.

(ה) אחת לשנה ימסור ראש המערך ~~לראש הממשלה~~ממשלת ישראל, דוח מצב הגנת הסייבר הלאומית (להלן – "דוח מצב הגנת הסייבר הלאומית") שיכלול סקירה וניתוח לגבי מצב הגנת הסייבר בישראל, פעילויות שננקטו בשנה החולפת ופעילויות שנדרש לנקוט בעתיד.

(ו) לא יאוחר מחודשיים לאחר קבלת דוח מצב הגנת הסייבר הלאומית תדון הממשלה על-יסודו במצב הגנת הסייבר בישראל, באסטרטגיית הגנת הסייבר הלאומית ובעדכונה במידת הצורך.

~~(ה)~~(ז) גרסה לא מסווגת של דוח מצב הגנת הסייבר הלאומית תפורסם לציבור בסמוך לדיון בממשלה.

היבטים ארגוניים של המערך

5. (א) על אף האמור בחוק המינויים, רשאי ראש הממשלה, לאחר התייעצות עם שר האוצר ועם נציב שירות המדינה, לקבוע בתקנות או בכללים הוראות אחרות מאלה החלות בשירות המדינה, לעניין ארגון וניהול כוח אדם במערך, והכל בכפוף להוראות חוק יסודות התקציב, התשמ"ה-1985[7] (להלן – "חוק יסודות התקציב") ולהוראות חוק התקציב השנתי.

(ב) ראש הממשלה רשאי לקבוע בכללים משרות או תפקידים במערך אשר נדרשת בהם מומחיות מיוחדת ועקב כך, על אף האמור בכל דין, ניתן להעסיק בהם גם מי שאינו עובד המדינה, לתקופה קצובה.

(ג) מבלי לגרוע מהוראות חוק שירות המדינה (משמעת), התשכ"ג-1963[8], רשאי ראש הממשלה לקבוע בתקנות הוראות נוספות בדבר משטר ומשמעת שיחולו במערך.

(ד) ראש ~~המערך~~ הממשלה יקבע ב~~נהלי המערך~~תקנות הוראות לעניין כשירות והכשרה של גורם אחראי ועובד מוסמך כתנאי להפעלת סמכויות לפי חוק זה.

סודיות

6. (א) עובד המערך וכן הפועל מטעם המערך לפי הוראות חוק זה, בעבר או בהווה, לא יגלה, במעשה או במחדל, לא ימסור ולא יפרסם~~יפשוט~~ מידע מוגן שהגיע אליו בתוקף תפקידו או במסגרת פעילותו במערך, למי שאינו רשאי לקבלו~~, אלא אם כן נדרש לכך כדין~~

[6] ס"ח התשי"ט, עמ' 86; התשע"ה עמ' 105
[7] ס"ח התשמ"ה, עמ' 60; התשע"ד עמ' 300
[8] ס"ח התשכ"ג, עמ' 50; התשע"ה, עמ' 105

~~או קיבל היתר לכך בכתב בהתאם להוראות שקבע ראש המערך לפי חוק זה~~ כדין;

(ב) עובד המערך וכן הפועל מטעם המערך לפי הוראות חוק זה, בעבר או בהווה המגלה או המפרסם מידע מוגן לפי חוק זה ~~שהגיע אליו בתוקף תפקידו או במסגרת פעילותו במערך, למי שאינו רשאי לקבלו, בלא היתר לפי~~בניגוד ל~~-~~סעיף (א), דינו - מאסר שלוש שנים; הביא אדם לגילוי או לפרסום כאמור ברשלנות, דינו - מאסר שנה;

(ג) אין בסעיף זה כדי לגרוע מסמכות שר לפי סעיפים 44 ו-45 לפקודת הראיות, או מסמכויות הצנזור לפי תקנות ההגנה (שעת חירום), 1945, או מכל סמכות אחרת למניעת פרסום לפי כל דין;

(ד) אין בהוראות סעיף זה כדי לגרוע מתחולת הוראות פרק ז' בחלק ב' לחוק העונשין, התשל"ז-1977.[9]

הגבלות על עובדי המערך

7. (א) ראש הממשלה רשאי לקבוע בתקנות הגבלות על עובדי המערך והפועלים מטעם המערך בתקופת עבודתם במערך ועבורו, ולאחריה, ככל שהדבר דרוש לשם מילוי תפקידי המערך, להבטחת טוהר המידות במערך, ולהבטחת אמון הציבור במערך.

(ב) עובד המערך לא יהיה חבר בארגון עובדים ולא ייטול חלק בפעולות להקמתו, לקיומו או לניהולו של ארגון עובדים; עבירה על הוראת סעיף זה תיחשב כעבירת משמעת; בסעיף קטן זה, "ארגון עובדים" - כל התארגנות או נציגות, בין קבועה ובין ארעית, שבין מטרותיה או פעולותיה נמנה הטיפול בארגון המערך, בניהולו, במשטר ובמשמעת ובתנאי השירות של עובדי המערך, או ייצוג של עובד המערך בנושאים אלה.

סייג לאחריות

8. עובד המערך או הפועל מטעם המערך בתפקידים ייעודיים להגנת סייבר מסוג שקבע ראש הממשלה לא יישא באחריות פלילית או אזרחית למעשה או למחדל שעשה בתום לב ובאופן סביר במסגרת תפקידו ולשם מילויו; ואולם אין בהוראות סעיף זה כדי לגרוע מאחריות משמעתית לפי כל דין.

ממונה הגנת הסייבר במערך

9. (א) ראש המערך ימנה מבין עובדי המערך, ~~עובד~~ ממונה הגנת סייבר ~~שיפקח~~ שיהא אחראי על קיום הגנת הסייבר במערך הסייבר ~~שיהיה ממונה הגנת הסייבר~~.

(ב) ראש המערך יוודא כי לממונה הגנת הסייבר יש את האמצעים והסמכויות הנדרשים למילוי תפקידו.

(ג) ממונה הגנת הסייבר לא ימלא תפקיד אחר אשר עלול להעמידו בניגוד עניינים במילוי תפקידו לפי סעיף זה.

מפקח פרטיות פנימי במערך

10. (א) ראש המערך, בהתייעצות עם רשם מאגרי מידע לפי חוק הגנת הפרטיות (להלן – "הרשם"), ימנה ~~מבין עובדי המערך~~ מפקח פרטיות פנימי (להלן – "המפקח הפנימי"), שהוא בעל התאמה בטחונית מספקת לצורך מילוי תפקידו ועומד ב~~בהתאם ל~~תנאי כשירות והכשרה שיורה עליהם הרשם, בהתייעצות עם ראש המערך.

[9] ס"ח התשל"ז, עמ' 226; התשע"א, עמ' 80

(ב) המפקח הפנימי ימונה לתקופת כהונה אחת שלא תעלה על שבע שנים.

(ג) לא תופסק כהונתו של המפקח הפנימי והוא לא יועבר מתפקידו אלא ~~בהתייעצות~~ בהסכמת ~~עם~~ הרשם או ביוזמת הרשם.

~~(ד)~~(ד) הופסקה כהונתו של המפקח הפנימי ביזמת הרשם, לא יועסק המפקח הפנימי בתפקיד אחר במערך למשך חמש שנים מיום הפסקת הכהונה.

~~(ה)~~(ה) המפקח הפנימי יהיה עובד המערך הכפוף ישירות לראש המערך או לעובד בכיר במערך הכפוף ישירות לראש המערך, והוא יונחה מקצועית בידי הרשם.

(ו) המפקח הפנימי לא ימלא תפקיד נוסף ולא יעסוק בעיסוק נוסף העלולים להעמיד אותו בחשש לניגוד עניינים במילוי תפקידו לפי סעיף זה ולפי סעיף 11.

~~(ז)~~(ז) ראש המערך יקצה למפקח הפנימי את המשאבים הדרושים לו לשם מילוי תפקידיו ויישם במערך את תכנית העבודה השנתית שהכין המפקח כאמור בהוראת סעיף 11(1) לעיל.

תפקידי מפקח הפנימי

11. המפקח הפנימי יפקח על יישום הוראות ~~חוק~~ דיני הגנת הפרטיות במערך, יקיים בקרה על ביצוען ובכלל זאת -

(א) יכין תכנית עבודה שנתית שתובא לאישור ראש המערך, הרשם והוועדה המפקחת לפי סעיף 13 לפיקוח על קיום הוראות ~~חוק~~ דיני הגנת הפרטיות, ולבירור הפרות ~~חוק~~ דיני הגנת הפרטיות במערך;

~~(א)~~(ב) ימליץ לראש המערך בדבר הוראות ונהלים הדרושים לדעתו לשם ההגנה על פרטיות;

~~(ב)~~(ג) יבדוק את נהלי המערך בתחום הפרטיות, ~~ו~~עמידתם בהוראות חוק הגנת הפרטיות ויישומם בפועל;

~~(ג)~~(ד) יברר הפרות בתחום הוראות חוק הגנת הפרטיות, ~~בהתאם להנחיות הרשם~~;

~~(ד)~~(ה) ידווח לרשם בלא דיחוי, ~~בכפוף להוראות ההתאמה הביטחונית והמידור החלות על המערך~~, על ממצאים של פעולות הפיקוח הבדיקה והבירור שביצע;

~~(ה)~~(ו) יקיים בקרה על אופן תיקון ליקויים שהתגלו בממצאי הפיקוח והבירור;

~~(ו)~~(ז) יקיים הכשרה והדרכה של עובדי המערך בנושאי פרטיות;

~~(ז)~~(ח) יגיש לראש המערך, לוועדה המפקחת ולרשם דין וחשבון שנתי על אופן ביצוע תכנית הפיקוח ועל קיום הוראות החוק במערך.

~~(ח)~~(ט) יסייע לראש המערך בקיום הוראות סעיפים 17(ג) ו – 38.

סמכויות המפקח הפנימי

12. לצורך מילוי תפקידו רשאי המפקח הפנימי –

(1) לדרוש מכל עובד של המערך או כל הפועל מטעמו למסור לו כל ידיעה ומסמך;

(2) לדרוש מכל עובד של המערך או כל הפועל מטעמו להציג בפניו או למסור לו עותק מחומר מחשב;

(3) להיכנס למקום, לערוך בו חיפוש ולתפוס חפץ;~~יהיו למפקח הפנימי הסמכויות לפי סעיף 15 לחוק להסדרת הביטחון בגופים ציבוריים, תשנ"ח – 1998[10] (להלן – החוק להסדרת הביטחון)~~

ועדה מפקחת על מערך הסייבר הלאומי

13. (א) ~~ראש~~ הממשלה ~~ימנה~~ תמנה ועדה שתפקח על פעילות המערך לפי הוראות פרק ג' לחוק זה לעניין השפעת הפעילות על הזכויות החוקתיות בישראל, ובפרט הזכות לפרטיות (להלן – "הוועדה").

(ב) ~~נציג ראש מערך הסייבר הלאומי ישמש כמזכיר הוועדה.~~ מערך הסייבר הלאומי יעמיד לרשות הועדה את האמצעים הנדרשים לפעולתה על פי דרישתה.

(ג) הרכב הוועדה יהיה כדלקמן:

(1) שופט בית משפט מחוזי או בית המשפט העליון בדימוס או משפטן בכיר אחר בעל כשירות לכהן כשופט ~~מחוזי~~ בית המשפט העליון, שהם בעלי ניסיון והבנה בסוגיות של משפט וטכנולוגיות מידע – יו"ר;

(2) נציג היועץ המשפטי לממשלה;

(3) נציג מקרב הציבור בעל מומחיות, רקע וניסיון בתחומים הנוגעים לענייני הגנת הסייבר והביטחון של מדינת ישראל;

(4) נציג מקרב הציבור בעל ידע וניסיון מובהקים בתחומי זכויות האדם והגנת הפרטיות על בסיס המלצת רוב דיקני בתי הספר למשפטים בישראל;

(5) נציג מקרב הציבור בעל מומחיות רקע וניסיון בתחומי טכנולוגית המידע על בסיס המלצת רוב דיקני בתי הספר למדעי המחשב בישראל;

(ד) חבר הוועדה יהיה בעל התאמה בטחונית.

(ה) לא יגלה אדם דבר מדיוני הוועדה או מכל חומר שנמסר לה, אלא אם הסמיך אותו לכך ראש הממשלה, או באישור היועץ המשפטי לממשלה או נציגו.

(ו) חבר ועדה במילוי תפקידיו לפי חוק זה לא יהא נתון לכל מרות זולת מרות ~~החוק~~ הדין ויפעיל שיקול דעת עצמאי.

תפקידי הוועדה

14. (א) הוועדה תגיש ל~~ראש ה~~ממשלה אחת לשנה, וכן בכל עת אחרת שלדעתה הדבר נדרש, דין וחשבון מטעמה על פעילות המערך בהתאם להוראות חוק זה.

~~(א)~~(ב) הממשלה תדון בדין וחשבון מטעם הוועדה ביחד עם דוח מצב הגנת הסייבר הלאומית.

~~(ב)~~(ג) לצורך ביצוע תפקידיה תקבל הוועדה דיווחים עיתיים על פעילות המערך וביצוע תפקידיו שיאפשרו לעמוד על ההשפעה של פעילות המערך על הזכות לפרטיות וזכויות חוקיתיות אחרות בפעילות המערך, ובכלל זה:

~~10 ס"ח התשנ"ח, עמ' 348; התשע"ז, עמ' 494~~

(1) נתונים על שימוש בסעיפי הסמכות לפי החוק;

(2) נתונים על פעילות מערך הגילוי והזיהוי לפי סעיף 17;

(3) אירועים שבהם עלה חשש להפרת הוראות החוק בתחום הפרטיות בידי עובד המערך או מטעמו;

(4) הנחיות פנימיות בתחום ההגנה על הפרטיות וזכויות חוקתיות אחרות ואופן מימושן;

(5) תוכנית העבודה והדוח השנתי של מפקח הפרטיות הפנימי של המערך.

סמכויות הוועדה

15. (א) לצורך ביצוע תפקידיה לפי חוק זה יהיו לוועדה ביחס למערך כל הסמכויות הנתונות לוועדת חקירה לפי סעיפים 9 – 13 ו- 17 לחוק ועדות חקירה, התשכ"ט-1968. ~~רשאית הוועדה לאסוף מידע ומסמכים, ויהיו ליו"ר הוועדה, הסמכויות הבאות:~~

~~(1) להזמין אדם לבוא בפניה ולמסור מידע או מסמכים שברשותו; מי שהוזמן להעיד או להציג מסמך או מוצג אחר בפני הוועדה, חייב להתייצב בפני הוועדה ולמסור לה מידע או מסמך.~~

~~(2) להסמיך אדם הכשיר לכך לדעת הוועדה, ובלבד שהוא בעל התאמה בטחונית, לאסוף חומר הדרוש לביצוע תפקידיה ויהיו נתונות לו הסמכויות לפי פסקה (1).~~

(ב) ראתה הוועדה במסגרת פעילותה שעולה חשש להפרת הדין בידי גורם או אדם מסוים, תחדל מטיפול לגביו ותעביר את המשך הטיפול לגורם המוסמך לכך.

פרק ג': סמכויות המערך

סימן א': כללי

סמכויות המערך

16. (א) לצורך מילוי תפקידיו מוסמך המערך, לבצע את הפעולות המנויות להלן, בין היתר באמצעות המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר:

(1) לקבל ולאסוף מידע בעל ערך אבטחתי ~~ומידע שעשוי לשמש להפקת מידע בעל ערך אבטחתי~~;

(2) לעבד מידע לצורך הפקת מידע בעל ערך אבטחתי בהתאם להוראות חוק זה;

(3) להעביר, לשתף ולהפיץ מידע בעל ערך אבטחתי לכלל המשק ולארגונים הפועלים בו בהתאם להוראות חוק זה, ובלבד שלא יפיץ מידע מוגן;

(4) לסייע לארגונים וליחידים להתמודד עם אירועי סייבר בהתאם להוראות חוק זה.

(ב) ראש הממשלה בהסכמת שר המשפטים באישור ועדת הכנסת לחוק יקבע

בתקנות הוראות לעניין איסוף מידע, עיבודו, העברתו, שיתופו והפצתו לפי פסקאות (1) עד (3).

מערך גילוי וזיהוי

17. (א) המערך יפעיל מערך גילוי וזיהוי בתחום הגנת הסייבר לצורך גילוי מוקדם וביצוע של תקיפות סייבר וסיוע בהתמודדות עמן; המידע שייאסף ויעובד במערך הגילוי והזיהוי ישמש למטרה זו בלבד.

(ב) מערך הגילוי והזיהוי יאסוף מידע בזמן אמת מהגופים המנויים בסעיף 18 (להלן בסעיף זה – הארגונים) לשם עיבודו למידע בעל ערך אבטחתי;

(ג) מערך הגילוי והזיהוי יפעל בהתאם לעקרונות האלה:

(1) ~~איסוף ה~~המידע שיאסף מהארגונים י~~האמוקד ב~~מידע בעל ערך אבטחתי בלבד;

(2) עיבוד ~~ה~~מידע למידע בעל ערך אבטחתי יבוצע בחצרי הארגון וככל הניתן בזמן אמת ו~~,~~באופן ממוחשב אוטומטי ויהיה גלוי לביקורת מתמדת של פעילותו של נושא משרה מטעם הארגון;

~~(2)~~(3) איסוף מידע יתבצע באמצעים שקוד מקור התוכנה שלהם זמין באופן חופשי לעיון ובדיקת הציבור הרחב. ראש המערך, באישור היועץ המשפטי לממשלה, רשאי להתיר שימוש באמצעים אחרים אם שוכנע שאינם אוספים מידע מוגן;

~~(3)~~(4) איסוף המידע ועיבודו ייעשה בהתאם להוראות סעיף 38.

(ד) מערך הסייבר הלאומי יפרסם המלצות לעניין אופן מסירת הודעה לעובדי הארגונים, ללקוחות ~~ועובדי הארגונים~~ ולציבור בדבר פעילות מערך הגילוי והזיהוי;

(ה) ראש הממשלה ושר המשפטים, באישור ועדת הכנסת לחוק, יקבעו בתקנות הוראות לעניין אופן איסוף, עיבוד, שמירה וביעור של המידע במערך הגילוי והזיהוי והשימוש בו, וכן רשאים הם לקבוע בכללים הוראות נוספות לעניין מערך הגילוי והזיהוי אשר פרסומם יהיה חסוי משיקולי הגנה על סודיות, שיטות ואמצעים.

ארגונים שייכללו במערך הגילוי וזיהוי

18. מערך הגילוי והזיהוי יכלול את הארגונים האלה:

(א) משרדי הממשלה;

(ב) גוף מבוקר כהגדרתו בסעיף 9 לחוק מבקר המדינה (נוסח משולב), התשי"ח-1958,[11] שראש המערך קבע באישור ועדת החוק לכנסת ששיתופו יתרום תרומה של ממש לגילוי תקיפות סייבר ולהתמודדות עמן ~~ולמעט הגופים המיוחדים~~;

~~(ב)~~(ג) הגופים המיוחדים, לגבי מערכות שלהם המחוברות לסייבר.

~~(ג)~~(ד) ארגון המנוי בתוספת החמישית לחוק להסדרת הביטחון, לגבי המערכות

[11] ס"ח התשי"ח, עמ' 92; התשנ"ח, עמ' 352

שהוגדרו כמערכת ממוחשבת חיונית בניהולו.

~~(ד)~~(ה) בעל רישיון לאספקת שירותי בזק בסיסיים או בעל היתר כללי כהגדרתם ~~ו~~ בחוק התקשורת; ואולם היה בעל רישיון מנוי בתוספת הרביעית לחוק להסדרת הביטחון, לא יחולו עליו הוראות סימן זה אלא באישור הקצין המוסמך לפי אותו חוק; ניתן לבעל הרישיון צו לפי סעיף 13(ב) לחוק התקשורת, לא יחולו עליו הוראות סימן זה אלא לאחר אישור הגורם המוסמך לפי אותו סעיף ולאחר שראש המערך התייעץ עם ראש שירות הביטחון הכללי לפי חוק שירות הביטחון הכללי, התשנ"ב-2002,[12] (להלן – חוק שירות הביטחון הכללי);

~~(ה)~~(ו) ארגון אחר שביקש להצטרף למערך הגילוי והזיהוי וראש מערך הסייבר אישר את הצטרפותו; ראש הממשלה בהתייעצות עם שר המשפטים יקבע בתקנות באישור ועדת הכנסת לחוק את אופן הגשת הבקשה, וכן הוראות בדבר מסירת הודעה ללקוחות ועובדי הארגון אודות פעילות מערך הגילוי והזיהוי.

~~(ו)~~(ז) ארגון אחר מהמנויים לעיל, שקבעו ראש הממשלה ושר המשפטים בצו, באישור ועדת הכנסת לחוק, לאחר שראש המערך חיווה דעתו כי הארגון מספק שירותים בהיקף משמעותי בישראל ושיתופו במערך הגילוי והזיהוי יתרום תרומה של ממש לגילוי ולזיהוי של תקיפות סייבר ולהתמודדות עמן במסגרת הגנת הסייבר בישראל.

חובת יידוע ארגון על תקיפת סייבר

19. היה למערך יסוד להניח כי ארגון מסוים מהווה, או מיועד להיות, יעד לתקיפת סייבר, יעביר המערך לאותו ארגון בלא דיחוי את כל המידע בעל הערך האבטחתי הדרוש לו באופן סביר כדי להיערך לתקיפת הסייבר ולהתגונן מפניה. ראש המערך יקבע כללים לעניין מסירת מידע בעל ערך אבטחתי שיישאר חסוי משיקולי הגנה על סודיות, שיטות ואמצעים.

סימן ב': סמכויות לטיפול בתקיפות ובאיומי סייבר

הוראות כלליות

~~19.~~20. (א) הפעלת הסמכויות לפי פרק זה תיעשה רק בידי מי שהוסמך לביצוע הפעולה לפי הוראות חוק זה או שנקבעו לפיו.

(ב) הפעלת סמכויות תיעשה לאחר שבעל הסמכות מסר לארגון מידע על אודות הצורך בפעולה והשפעותיה על הארגון.

(ג) הפעלת סמכויות כלפי ארגון תיעשה אם התקיים האמור להלן -

(1) יש יסוד סביר להניח שמתרחשת או עשויה להתרחש תקיפת סייבר שעלולה לגרום לפגיעה באינטרס חיוני.

(2) הפעלת הסמכות נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה;

[12] ס"ח התשס"ב, עמ' 179, התשע"ד, עמ' 667

(3) בעל הסמכות שקל את השפעת הפעלת הסמכויות על הארגון ועל הזכות לפרטיות;

(4) בעל הסמכות נוכח כי הפעלת הסמכות אין בה כדי לפגוע בפעילות הארגון או בזכות לפרטיות במידה העולה על הנדרש בנסיבות העניין.

(ד) לא תופעל סמכות לפי פרק זה אם ניתן להסתפק בהפעלת סמכות שחומרתה פחותה ממנה. בכלל זה:

(1) לא ייתפס חפץ אם ניתן להסתפק בקבלת ידיעה או מסמך, או – בהעדר אפשרות להסתפק בקבלת ידיעה או מסמך - בהעתקת החפץ;

(2) לא ייתפס חפץ אם ניתן להסתפק בהמצאתו לבדיקה;

(3) לא ייכנס בעל סמכות למקום אם יכול היה להסתפק בקבלת ידיעה, מסמך או חפץ, ולא ייכנס למקום בלא הסכמת הארגון אם יכול היה לקבל את הסכמתו;

(4) לא יסתייע בעל סמכות במומחה אם יכול היה להסתייע בעובדי הארגון;

(5) לא יבצע בעל סמכות פעולה במחשב או בחומר מחשב, לא יבקש צו להתיר פעולה כזו ולא יורה ראש המערך על ביצוע פעולה כזו, אם אפשר היה להסתפק במתן הוראות לארגון לגבי ביצוע פעולות כאמור.

~~(ד)~~(ה) הופעלה סמכות לפי פרק זה וחלפו תשעים ימים מעת שהופעלה הסמכות האמורה – לא תופעל הסמכות או סמכות נוספת לפי פרק זה בארגון אלא אם נוכח ראש המערך כי יש יסוד סביר להניח שתקיפת הסייבר עדיין מאיימת על אינטרס חיוני והפעלת הסמכויות בארגון נדרשת להתמודדות עמה או לאיסוף מידע עליה;

~~(ה)~~(ו) הוראות סעיפים (ג) ו- (ד) יחולו בשינויים המחויבים אם הפעולה בארגון נעשית לבקשת הארגון, והוראות סעיף 35 יחולו בשינויים המחויבים ולפי ההקשר.

ביצוע פעולה בהסכמה

21. (א) גורם אחראי במערך רשאי להורות על ביצוע פעולה בארגון הדורשת אישור בית המשפט לפי סימן זה אף בלא צו כאמור, אם הארגון הסכים לביצוע הפעולה והתקיים האמור להלן:

(1) נותן ההסכמה הוא גורם מוסמך מטעם הנהלת הארגון;

(2) לפני מתן ההסכמה הסביר הגורם האחראי לנותן ההסכמה, בלשון המובנת לו ובכתב, את כל אלה -

(א) מהי הפעולה שהארגון מתבקש להסכים לה, וכמה זמן תימשך;

(ב) כי אין על הארגון חובה על פי חוק להסכים לביצוע הפעולה;

(ג) הנסיבות המצדיקות את ביצוע הפעולה;

(ד) השפעת ביצוע הפעולה על הארגון ועל ארגונים נוספים ככל שישנם;

(ה) מידת הפגיעה בפרטיות או אפשרות לפגיעה אחרת באדם או

בארגון כתוצאה מביצוע הפעולה, קיומה של אפשרות לצמצום הפגיעה והדרכים לכך;

(ו) את זכותו של הארגון שלא להסכים לביצוע הפעולה, והעובדה שהארגון לא יפגע מעצם אי הסכמתו

(ב) ארגון שנתן הסכמה לביצוע פעולה לפי סעיף זה רשאי לחזור בו מהסכמתו ואם חזר בו תופסק לאלתר כל פעולה שבוצעה מכוח הסכמתו; אין בחזרה מהסכמה כדי לפגוע בחוקיות הפעולות שנעשו עד לחזרה מההסכמה.

דרישת מידע ומסמכים

22. ~~20.~~ (א) עובד מוסמך רשאי לדרוש מכל ארגון הנוגע בדבר למסור לו ~~כל~~ ידיעות ~~ה~~ או ~~מסמך~~ מסמכים, ובכלל זה עותק של חומר מחשב, אם יש לו יסוד סביר להניח כי הם ~~ה~~ נדרשים לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה.

(ב) לא ידרוש עובד מוסמך ולא יקבל ידיעות או מסמכים מארגון שפעילותו טעונה רישיון לפי הוראות כל דין, שאינו רשיון לפי חוק רישוי עסקים, התשכ"ח-1968, או שהיא כפופה לחובת סודיות או חיסיון מקצועיים אלא בהסכמת אותו ארגון, ואם לא קיבל אותה הסכמה - בהסכמת הגורם המוסמך על-פי דין ליתן לארגון רישיון לפעילותו.

(ג) לא ידרוש עובד מוסמך ולא יקבל ידיעות או מסמכים המכילים מידע מוגן ממשרד ממשרדי הממשלה או מרשות של המדינה, המקבלים מידע ומסמכים מהציבור או מארגונים לפי הוראות כל דין, אלא באישור בכתב של היועץ המשפטי לממשלה או מי שהוא הסמיך לכך, שיינתן לאחר שהיועץ מצא כי התועלת להגנה בסייבר ממסירת המידע עולה על הנזק העלול להיגרם לאירגון, לצדדים שלישיים ולאינטרס הציבורי מאי-מסירת המידע.

(ד) לא ידרוש עובד מוסמך ולא יקבל ידיעות או מסמכים, ובכלל זה עותק של חומר מחשב, שיש בהם מידע מוגן אלא בכפוף לקבלת צו בית משפט מכוח חוק נתוני תקשורת או סעיף 43 לפקודת סדר הדין הפלילי, לפי העניין.

מינוי איש קשר בארגון שיש בו תקיפת סייבר

23. ~~21.~~ עובד מוסמך רשאי להורות לארגון למנות איש קשר שיקבל הוראות מהמערך ויעביר את המידע הנדרש אל המערך או אל מי שהוסמך לכך מטעמו לפי הוראות סימן זה.

כניסה למקום

24. ~~22.~~ (א) גורם אחראי במערך רשאי להיכנס למקום או להורות לעובד מוסמך להיכנס למקום, אם היה לו יסוד סביר להניח שבמקום נמצא מחשב או חומר מחשב שבו מידע בעל ערך אבטחתי הדרוש לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה, ושתקיפה זו מתרחשת בעת כניסתו, או שיש יסוד סביר להניח כי היא צפויה להתרחש בסמוך לאחריה, והיא מיועדת לפגוע באינטרס חיוני;

(ב) על אף האמור בסעיף קטן (א) בכל אחד מהמקרים המפורטים להלן, לא ייכנס גורם אחראי במערך או עובד מוסמך למקום אלא בהסכמת המחזיק במקום או על פי צו של בית משפט ~~לא ייכנס גורם אחראי במערך או עובד מוסמך למקום המשמש למגורים אלא בהסכמת המחזיק במקום או על פי צו של בית משפט השלום; אולם רשאי ראש

~~המערך להורות לגורם אחראי או לעובד מוסמך להיכנס למקום המשמש למגורים גם בלא צו מאת בית משפט, אם היה לו יסוד סביר להניח שבמקום נמצא מחשב או חומר מחשב שבו מידע בעל ערך אבטחתי כאמור בסעיף קטן (א) שנדרש למניעת סכנה ממשית ומידית לשלום הציבור או ביטחונו, ואין דרך אחרת להשיגו בנסיבות העניין.~~

(1) כשהכניסה איננה בקשר לתקיפה המתרחשת בזמן הכניסה או שיש יסוד סביר להניח כי היא צפויה להתרחש בסמוך לאחריה;

(2) כשהמקום משמש למגורים;

(3) כשהכניסה עלולה להימשך יותר מאשר 12 שעות;

(4) כשבעל המקום כפוף לחובת סודיות לפי הוראות כל דין;

(ג) על אף האמור בסעיף (ב) לעיל, רשאי ראש המערך להורות לגורם אחראי או לעובד מוסמך להיכנס למקום גם בלא צו מאת בית משפט, אם היה לו יסוד סביר להניח שבמקום נמצא מחשב או חומר מחשב שבו מידע בעל ערך אבטחתי כאמור בסעיף קטן (א) שנדרש למניעת סכנה ממשית ומידית לשלום הציבור או ביטחונו, ואין דרך אחרת להשיגו בנסיבות העניין.

תפיסת חפץ לצורך טיפול בתקיפה

25~~23~~. (א) עובד מוסמך רשאי לתפוס חפץ שיש לו יסוד סביר להניח שיש בו מידע בעל ערך אבטחתי, שבדיקתו המידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה.

(ב) לא יתפוס עובד מוסמך חפץ כאמור בסעיף קטן (א) אלא לאחר שנתן למחזיק בו הזדמנות להשמיע טענותיו. סבר הגורם האחראי כי הדבר יביא לפגיעה משמעותית ביכולת לאתר תקיפת סייבר, להתמודד עמה או למנוע אותה, ויש סכנה ממשית ומידית לשלום הציבור או ביטחונו, רשאי הוא לתפוס את החפץ ולתת למחזיק להשמיע טענותיו בפניו בהזדמנות הראשונה.

(ג) נתפס חפץ לפי סעיף זה, יחזירו העובד המוסמך לארגון שממנו נתפס לאחר שביצע בו את הבדיקה, בהקדם האפשרי ולא יאוחר מחמישה עשר ימים מיום שנתפס.

(ד) בית משפט השלום רשאי להורות -

(1) כי החפץ יוחזר לארגון, לבקשתו;

(2) על הארכת תקופת ההחזקה של החפץ מעבר לאמור בסעיף קטן (ג), לבקשת העובד המוסמך, אם סבר כי בנסיבות העניין קיים צורך בהארכת התקופה לשם איתור תקיפת הסייבר, טיפול בה או מניעתה.

המצאת חפץ לבדיקה

26~~24~~. היה לעובד מוסמך יסוד סביר להניח שחפץ שנמצא בחזקתו או בשליטתו של ארגון מכיל מידע בעל ערך אבטחתי ובדיקתו המידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה, ולא ניתן לפעול על פי הסמכויות הקבועות בסעיפים 22 ו-23, רשאי הוא להורות על הצגתו או המצאתו בשעה, במקום ובאופן הנקובים בהוראה; לעניין זה, יראו חפץ כנמצא בשליטתו של ארגון - אם הארגון יכול להשיגו במאמץ סביר.

הסתייעות במומחה

27.~~25.~~ (א) לצורך ביצוע פעולות ובדיקות לפי פרק זה, רשאי עובד מוסמך להסתייע במומחה שהוא בעל ניסיון, ידע או אמצעים הדרושים לביצוע הפעולות והבדיקות האמורות (להלן, בסעיף זה – "המומחה החיצוני"), ובלבד שהעובד המוסמך יהיה נוכח במקום ביצוע הפעולות והבדיקות בידי המומחה החיצוני, בעת ביצוען, ויפקח עליו. ~~בסעיף זה "מומחה" – גם מי שאינו עובד ציבור.~~

(ב) כמומחה חיצוני יכול להתמנות גם מי שאינו עובד ציבור, ולבד שאין ניגוד עניינים המונע ממנו ביצוע תפקידו.

(ג) בביצוע תפקידיו לפי סעיף זה יחול על המומחה החיצוני הדין החל על עובד הציבור.

(ד) על אף האמור בסעיף (א) לעיל, אם לארגון, או למי הפועל מטעמו, הניסיון, הידע או האמצעים הדרושים לביצוע הפעולות והבדיקות האמורות, יסתייע העובד המוסמך במומחה מטעם הארגון לפעולות ובדיקות בחצרי הארגון.

(ה) הסתייע העובד המומחה במומחה מטעם הארגון לפעולות ובדיקות חלף שימוש במומחה חיצוני, יוחזרו עלויות הפעולות והבדיקות לארגון כפי שהיה משולם למומחה חיצוני;

סמכות מתן הוראות

28.~~26.~~ (א) עובד מוסמך רשאי לתת לארגון הוראות, ובכלל זה הוראות לגבי ביצוע פעולות בחומר מחשב של הארגון, שהן חיוניות לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה - ואשר בלעדי ביצוען קיימת ודאות קרובה כי ייגרמו לארגון, לצדדים שלישיים או לאינטרס חיוני נזקים בלתי הפיכים.

(ב) בהוראה שייתן, יפרט העובד המוסמך את התמצית העובדתית והמקצועית להחלטתו ליתן את ההוראה לפי סעיף קטן (א) ככל שאין בכך כדי לפגוע או לעכב את הטיפול בתקיפה, לחשוף מקורות מידע, שיטות או אמצעים.

~~(ב)~~(ג) לא יתן עובד מוסמך הוראה לפי סעיף קטן (א) אלא לאחר שנקט בכל האמצעים הסבירים כדי לוודא שאין בביצוע ההוראה כדי לגרום נזק לארגון, לקוחותיו או לצדדים שלישיים, ובכלל זה נתן לארגון הזדמנות נאותה להשיג בפניו על ההוראה.

~~(ג)~~(ד) נתקבלה הוראה מעובד מוסמך כאמור בסעיף קטן (א) יבצע אותה הארגון במועד הקבוע בה וידווח על אופן ביצועה לעובד המוסמך. השיג הארגון על הוראה שנתן העובד המוסמך כקבוע בסעיף (ג), ועמד העובד המוסמך על הוראותיו על אף השגות הארגון, יהיה הארגון רשאי להביא את השגותיו בפני ראש המערך בתוך 48 שעות ממועד קבלת ההוראה ועד אז לא יהיה חייב למלאה.

~~(ד)~~(ה) לא יגלה אדם תוכן הוראה שניתנה לארגון, פרטים הקשורים בתקיפה או בטיפול בה שנמסרו לארגון, אלא אם התיר זאת העובד המוסמך ~~ו~~בתנאים שיקבע ובכפוף לכל דין, לרבות כזה המחייב את הארגון בהודעה על אודות התקיפה לציבור; העובד המוסמך רשאי להנחות את הארגון בדבר אופן ההגנה על סודיות הפעילות לפי פרק זה כלפי עובדיו ואחרים.

צו לפעולות למניעת תקיפת סייבר או לטיפול בה

27.29. (א) ~~שופט~~ בית משפט ~~השלום~~ רשאי להתיר בצו לעובד מוסמך, על פי בקשת גורם שהסמיך ראש המערך (להלן – "גורם אחראי במערך"), לבצע פעולה במחשב או בחומר מחשב של ארגון, אם שוכנע כי יש יסוד סביר להניח כי מתרחשת תקיפת סייבר או שיש איום סייבר שכתוצאה מהם עלולה להיגרם פגיעה באינטרס חיוני (להלן בסעיף זה – "צו ביצוע פעולות");

(ב) בהחלטה למתן צו ביצוע פעולות, יתחשב בית משפט ~~השלום~~, בין השאר, באלה:

(1) חומרת הנזק אשר עלול להיגרם בשל תקיפת הסייבר אשר בקשר אליה מתבקש הצו וההסתברות להתרחשותה;

(2) השפעת הפעולות המבוקשות על הארגון שהצו חל עליו ועל גורמים נוספים שעשויים להיות מושפעים מהצו, ככל שישנם;

(3) מידת הפגיעה בפרטיות ובזכויות חוקתיות אחרות כתוצאה מביצוע הפעולות המבוקשות ו~~מידת~~ פגיעה אחרת בארגון או באדם.

(4) צעדים שנקט המערך או יכול היה לנקוט קודם לבקשת הצו ואשר היו עשויים לייתר את הצו, לרבות בקשת הסכמה לפי סעיף 35 או מתן הוראות לפי סעיף 26, ואם ננקטו צעדים כאמור - האם הארגון לא פעל לפי ההוראות או שפעל לביצוען ברשלנות רבתי;

(5) מידת היכרותו של העובד המוסמך עם מערכות המחשב שבקשר עימן התבקש הצו והאם יוכל העובד המוסמך לפעול בהן ביעילות ובמקצועיות בלא חשש שייגרם שיבוש, תקלה או נזק אחר כלשהו;

(ג) לבד מנימוקין, צו לביצוע פעולות יגדיר בבירור את כל אלה

(1) שם הארגון ומקום ביצוע הפעולות;

(2) מערכות המחשב שביחס אליהן ניתן הצו;

(3) מהות הפעולות בחומר מחשב שהותרו – ובפרט, ככל שהותרה העתקת חומר מחשב, איזה חומר יועתק ולכמה זמן יישמר;

(4) הוראות בדבר שיתוף הארגון בביצוע הפעולות;

(ד) צו לביצוע פעולות יעמוד בתוקף למשך ימים מיום שניתן.

(ה) לא יינתן צו ביצוע פעולות בארגון שפעילותו דורשת רישיון לפי הוראות כל דין, שאינו רשיון לפי חוק רישוי עסקים, התשכ"ח-1968, או בארגון הכפוף לחובת סודיות מקצועית, אלא מטעמים מיוחדים שיירשמו.

בקשת הצו

28.30. (א) בקשה לצו ביצוע פעולות כאמור בסעיף 27 תוגש בכתב על ידי ה~~ג~~גורם ה~~א~~אחראי במערך (להלן – "המבקש"), ויפורטו בה שם הארגון ומגזר פעילותו, תיאור מערכות המחשב שבקשר עימן התבקש הצו, הפעולות שנקט המערך קודם לבקשת הצו, הסיבות בגינן לא ניתן להסתפק בפעולות אחרות זולת מתן הצו, פירוט הפעולות השונות שנדרש

לבצע במחשב או בחומר מחשב, מידת היכרותו של העובד המוסמך עם מערכות המחשב שבקשר עימן התבקש הצו והסיכון לגרימת שיבוש, תקלה או נזק אחר בשל הפעולות המבוקשות בצו; הבקשה תיתמך בתצהיר של ~~הגורם האחראי במערך~~המבקש.

(ב) המשיב בבקשה הינו הארגון שבמחשביו מבקשים לבצע פעולות כאמור; הדיון במתן הצו יתקיים במעמד הצדדים שזומנו לדיון, ואולם רשאי בית המשפט לתת צו לביצוע פעולות במעמד צד אחד אם הוא סבור שהמשיב הוזמן כדין ולא התייצב לדיון.

הדיון בבקשה

~~29.~~31. (א) בדיון בבקשה למתן צו לפי סעיף 27 או 32, רשאי המבקש לבקש לפרט או להציג בפני בית המשפט בלבד עובדות או מידע שעליהם הוא מבסס את בקשתו (להלן בסעיף זה – "חומר חסוי"); בקשה כאמור תוגש בכתב בצירוף נימוקים.

(ב) בית המשפט רשאי להיענות לבקשה כאמור בסעיף קטן (א) ולהסתמך על החומר החסוי אם מצא כי חשיפת החומר החסוי עלולה לפגוע או לסכל את אפשרות איתור תקיפת הסייבר, התמודדות עמה, או לפגוע באינטרס בטחוני או אינטרס ציבורי אחר; החומר החסוי יסומן, יוחזר למבקש לאחר העיון והדבר יירשם בפרוטוקול.

(ג) בית המשפט יודיע למבקש ולמשיב על החלטתו בבקשה לפי סעיף קטן (א), ורשאי הוא לקבוע שנימוקי ההחלטה, כולם או מקצתם, יהיו חסויים.

(ד) החליט בית המשפט שלא להיעתר לבקשה בדבר אי-גילויו של החומר החסוי לפי סעיף קטן (א), רשאי המבקש להודיע כי הוא חוזר בו מהגשת החומר החסוי, ומשעשה כן לא יועמד החומר לעיון המשיב והשופט יתעלם ממנו לצורך החלטותיו.

(ה) החליט בית המשפט שלא להיעתר לבקשה בדבר אי-גילויו של החומר החסוי לפי סעיף קטן (א), רשאי המבקש לערער על החלטת בית המשפט בעניין זה בתוך חמישה עשר ימים ממועד מתן ההחלטה, לפני בית משפט של ערעור אשר ידון בערעור בשופט אחד.

(ו) הודיע המבקש לבית המשפט שהחליט כאמור בסעיף קטן (ה), כי הוא שוקל להגיש ערעור כאמור באותו סעיף קטן, לא יעביר בית המשפט את החומר החסוי למשיב עד להכרעה בערעור.

(ז) החליט בית המשפט להיעתר לבקשה בדבר אי-גילויו של החומר החסוי לפי סעיף קטן (א), רשאי הארגון לערער על החלטת בית המשפט בעניין זה בתוך חמישה עשר ימים ממועד מתן ההחלטה, לפני בית משפט של ערעור אשר ידון בערעור בשופט אחד.

~~(ז)~~(ח) בדיון בערעור לפי סעיף קטן (ו) ו-(ז), רשאי בית המשפט לעיין בחומר החסוי ולקבל פרטים נוספים מהמבקש בלי לגלותם למשיב.

~~(ח)~~(ט) ראש הממשלה ושר המשפטים רשאים לקבוע הוראות נוספות בתקנות, באישור ועדת הכנסת לחוק, לעניין סדרי הדין לפי פרק זה.

ערעור על החלטת בית משפט

~~30.~~32. מי שהיה צד להליך למתן צו לפי סעיף 27 רשאי לערער על החלטת בית המשפט בתוך שלושים ימים ממועד מתן ההחלטה, לפני בית משפט שלערעור אשר ידון בערעור בשופט

אחד, שיהיה מוסמך לבטלו או לשנות תנאים בו. הוגש ערעור על החלטת בית המשפט, יעוכב ביצוע הצו עד להכרעה בערעור.

ביצוע הצו

31.33. ניתן צו לפי סעיפים 27 או 32 וביצועו לא עוכב, יבצע העובד המוסמך את הפעולות המנויות בצו לאחר שמסר על כך הודעה לאיש קשר מטעם הארגון, ו~~כל הניתן~~בנוכחותו. להודעה יצרף העובד המוסמך את הצו.

צו לביצוע פעולות בחומר מחשב לצורך בקרה מדגמית

32.34. (א) ~~שופט~~ בית המשפט ~~השלום~~ רשאי להתיר בצו, לצורך בקרה מדגמית, ביצוע פעולה במחשב או בחומר מחשב של ארגון אם סבר כי יש סיכוי של ממש לאתר באמצעותן תקיפת סייבר בארגון, בשים לב למאפייני הפעילות בארגון (להלן בסעיף זה – "צו פעולות לצורך בקרה מדגמית").

(ב) בהחלטה למתן צו פעולות לצורך בקרה מדגמית, ~~נחשב~~ ישקול בית משפט השלום, בין השאר, באלה:

(1) נחיצות הצו והפעולות מכוחו לצורכי הגנת הסייבר;

(2) השפעת הפעולות המבוקשות על הארגון שהצו חל עליו ועל גורמים נוספים שעשויים להיות מושפעים מהצו, ככל שישנם;

(3) מידת הפגיעה בפרטיות ובזכויות חוקתיות אחרות כתוצאה מביצוע הפעולות המבוקשות והאפשרות לפגיעה אחרת בארגון או באדם.

(4) צעדים שנקט המערך או יכול היה לנקוט קודם לבקשת הצו ואשר היו עשויים לייתר את הצו, לרבות בקשת הסכמה לפי סעיף 35 או מתן הוראות לפי סעיף 26, ואם ננקטו צעדים כאמור - האם הארגון לא פעל לפי ההוראות או שפעל לביצוען ברשלנות רבתי;

(5) מידת היכרותו של העובד המוסמך עם מערכות המחשב שבקשר עימן התבקש הצו והאם יוכל העובד המוסמך לפעול בהן ביעילות ובמקצועיות בלא חשש שייגרם שיבוש, תקלה או נזק אחר כלשהו;

(ג) לבד מנימוקין, צו לביצוע פעולות יגדיר בבירור את כל אלה

(1) שם הארגון ומקום ביצוע הפעולות;

(2) מערכות המחשב שביחס אליהן ניתן הצו;

(3) מהות הפעולות בחומר מחשב שהותרו – ובפרט, ככל שהותרה העתקת חומר מחשב, איזה חומר יועתק ולכמה זמן יישמר;

(4) הוראות בדבר שיתוף הארגון בביצוע הפעולות;

(ד) צו פעולות לצורך בקרה מדגמית יעמוד בתוקף למשך ____ ימים מיום שניתן.

(ה) לא יינתן צו פעולות לצורך בקרה מדגמית בארגון שפעילותו דורשת רישיון לפי הוראות כל דין, שאינו רשיון לפי חוק רישוי עסקים, התשכ"ח-1968, או בארגון הכפוף לחובת סודיות מקצועית, אלא מטעמים מיוחדים שיירשמו.

בקשת הצו והדיון בה

35.~~33.~~ (א) בקשה לצו פעולות לבקרה מדגמית תוגש בכתב על ידי גורם אחראי במערך ויפורטו בה שם הארגון ומגזר פעילותו, הפעולות שנקט המערך קודם לבקשת הצו, הסיבות בגינן לא ניתן להסתפק בפעולות אחרות זולת מתן הצו, הפעולות המבוקשות והקשר בינן לבין תכלית הבקרה המדגמית בהתאם לסעיף 32 וזהות מבצען; הבקשה תיתמך בתצהיר של הגורם האחראי במערך;

(ב) המשיב בבקשה הינו הארגון שבמחשביו מבקשים לבצע פעולות כאמור; הדיון במתן הצו יתקיים במעמד הצדדים שזומנו לדיון , ואולם רשאי בית המשפט לתת צו לביצוע פעולות במעמד צד אחד אם הוא סבור שהמשיב הוזמן כדין ולא התייצב לדיון.

(ג) בית המשפט ידון בבקשה לפי סעיף זה בדלתיים סגורות, אלא אם הורה אחרת.

(ד) גילוי הוראות לפי סעיף זה או פרטים הקשורים בפעילות לפיו אשר נמסרו לארגון אסור אלא אם התיר זאת הגורם האחראי.

(ה) על ערעור על החלטת בית המשפט יחולו הוראות סעיף 30 לחוק זה, בשינויים המחויבים לפי העניין

פעולה בחומר מחשב אינה האזנת סתר או חדירה שלא כדין

36.~~34.~~ פעולה שנעשתה כדין לפי הוראות סעיפים 26 ,17, 27, 35 או 36 לא תיחשב כהאזנת סתר או כחדירה שלא כדין לחומר מחשב כמשמעותן בחוק האזנת סתר או בחוק המחשבים, בהתאמה.

~~ביצוע פעולה בהסכמה~~

~~35. (א) גורם אחראי במערך רשאי להורות על ביצוע פעולה בארגון הדורשת אישור בית המשפט לפי סימן זה אף בלא צו כאמור, אם הארגון הסכים לביצוע הפעולה והתקיים האמור להלן:~~

~~(1) נותן ההסכמה הוא גורם מוסמך מטעם הנהלת הארגון;~~

~~(2) לפני מתן ההסכמה הסביר הגורם האחראי לנותן ההסכמה, בלשון המובנת לו, את כל אלה -~~

~~(א) הנסיבות המצדיקות את ביצוע הפעולה;~~

~~(ב) השפעת ביצוע הפעולה על הארגון ועל ארגונים נוספים ככל שישנם;~~

~~(ג) מידת הפגיעה בפרטיות או אפשרות לפגיעה אחרת באדם או בארגון כתוצאה מביצוע הפעולה, קיומה של אפשרות לצמצום הפגיעה והדרכים לכך;~~

~~(ד) את זכותו של הארגון שלא להסכים לביצוע הפעולה;~~

~~(3) ארגון שנתן הסכמה לביצוע פעולה לפי סעיף זה רשאי לחזור בו מהסכמתו; אין בחזרה מהסכמה כדי לפגוע בחוקיות הפעולות שנעשו עד לחזרה מההסכמה.~~

סימן ג': סמכויות נוספות

פעולה דחופה בחומר מחשב להגנת סייבר

37.~~36.~~ (א) ראש המערך רשאי ~~להורות על הפעלת~~להפעיל סמכות המנויה בסימן ב', שלשם הפעלתה נדרש צו בית משפט, ללא צו כאמור, לתקופה שלא תעלה על עשרים וארבע שעות ובהסכמת היועץ המשפטי לממשלה, ובלבד שהתקיימו כל אלה:

(1) הפעלת הסמכות נדרשת בדחיפות לשם מניעת נזק ממשי לאינטרס חיוני כתוצאה מתקיפת סייבר, אין דרך אחרת למניעת הנזק האמור, ואין שהות לבקש מבית המשפט צו;

(2) הארגון סירב להתיר למערך לפעול, או סיכל את הפעלת סמכויותיו, בדרך אחרת;

(3)~~(2)~~ התקיימו יתר דרישות הסעיפים האמורים בפרק זה, ככל שהדבר אינו מסכל את ביצוע הפעולה.

(4) הסמכות תופעל על ידי ראש המערך בעצמו, או על ידי עובד בכיר הכפוף לו ישירות שסמכות ראש המערך הואצלה אליו;

~~(ב) ראש המערך ידווח באופן מיידי ליועץ המשפטי לממשלה על הסמכויות שהורה להפעילן לפי סעיף קטן (א) לא יאוחר משש שעות ממועד הפעלתן.~~

(ב)~~(ג)~~ ~~גורם אחראי~~מי שהפעיל את הסמכות לפי סעיף (א) יפנה לבית המשפט באופן מיידי ולא יאוחר מעשרים וארבע שעות ממועד הפעלת סמכות לפי סעיף זה בבקשה למתן צו לפי הוראות פרק זה, אשר תכלול דיווח על הפעלת הסמכות ופירוט הפעולות שבוצעו במסגרתה לפי סעיף זה.

(ג) הפעלת הסמכות מכוח סעיף זה תחדל בתום 24 שעות, אלא אם הוארכה קודם לכן בצו בית משפט.

ממשקים עם רשויות אחרות ורשויות מאסדרות בעת טיפול בתקיפה

38.~~37.~~ נוכח ראש מערך הסייבר בעת טיפול בתקיפת סייבר לפי פרק זה שמניעת הפגיעה באינטרס החיוני או צמצומה מחייב פעולה של בעל סמכות נוסף, יודיע על כך ללא דיחוי לאותו בעל סמכות; בעל הסמכות יקבע איש קשר לסיוע למניעת הפגיעה האמורה ולהיערכות להתמודדות עמה.

סימן ד': הגנה על הפרטיות ומידע מוגן שנאסף לפי פרק זה

עיצוב לפרטיות והגנה על מידע מוגן

39.~~38.~~ (א) מידע שבידי המערך יישמר ויעובד במערכות המחשב המשמשות לפעילות המערך (להלן בסעיף זה – המערכות) בהתאם להוראות אלה:~~לצורך הגנה על הפרטיות ושמירה על מידע מוגן ראש המערך אחראי ליישום העקרונות המנויים להלן במערכות המחשב המשמשות לפעילות המערך (להלן בסעיף זה – המערכות):~~

(1) בדרך שתבטיח הגנה מפני דליפת מידע או פריצה אליו, וכן מפני העברה, חשיפה, מחיקה, שימוש, שינוי או העתקה בלא רשות כדין;

(2) בדרך שתמנע שימוש בו בניגוד להוראות לפי חוק זה;

(3) בדרך שתבטיח הגנה על הפרטיות, ותאפשר בקרה ופיקוח על אופן

השימוש במאגר, לרבות שימוש החורג ממסגרת ההרשאה לפי הוראות חוק זה.

(ב) לצורך הגנה על הפרטיות ושמירה על מידע מוגן ראש המערך אחראי ליישום העקרונות המנויים להלן במערכות:

(1) עיצוב טכנולוגי של המערכות באופן שנאסף ונשמר המידע המוגן המינימלי הנדרש לקיום ייעוד המערך, והוא מעובד ככל הניתן באופן שהוא מידע לא מזוהה;

(2) עיצוב טכנולוגי של המערכות באופן שעיבוד מידע למידע בעל ערך אבטחתי נעשה ככל הניתן באופן אוטומטי או ללא שהוא חשוף לאדם;

(3) שילוב בקרות טכנולוגיות במערכות המאפשרות פיקוח על העמידה בהוראות החוק לעניין איסוף שימוש ועיון במידע מוגן, לרבות מועד ביצוען של פעולות וזהות מבצען.

~~(ב)~~(ג) ראש הממשלה ושר המשפטים יקבעו תקנות באישור ועדת הכנסת לחוק לעניין הוראות סעיף זה.

סודיות ואי גילוי

~~39.~~40. (א) לא יגלה אדם או ארגון מידע שנמסר לו אודות הוראה או מידע אחר הקשור בפעילות המערך אשר סומן בידי גורם אחראי כמידע מוגן, מידע בעל ערך אבטחתי רגיש או מידע בעל סיווג בטחוני.

(ב) בית המשפט רשאי להורות, לבקשת אדם הנוגע בדבר, על גילוי מלא או חלקי של מידע כאמור, לאחר ששמע את עמדת המערך ושקל את האינטרס הציבורי ואינטרס המבקש בגילוי המידע למול החשש לפגיעה בפעילות המערך או בהגנת הסייבר.

מסירת מידע

~~40.~~41. ראש המערך, עובד הכפוף לו, או מי שפועל מטעמו, לא יגלה ידיעה או מסמך שנמסרו לו, או שהגיעו לידיעתו, מכוח תפקידו או סמכויותיו או על בסיס מנגנון הקבוע בחוק זה, ~~לפי פרק זה,~~ אלא בהתאם להוראות חוק זה, ~~או לצורך הליך פלילי בשל עבירה חמורה או בשל הפרעה לעובד ציבור~~.

שימוש במידע שנמסר למערך

~~41.~~42. (א) מידע שנמסר למערך בהסכמה לפי הוראות פרק זה לא ישמש כראיה כנגד מוסרו בהליך אזרחי, מנהלי או פלילי ~~למעט בעבירות שקבע שר המשפטים בתוספת הראשונה לחוק~~.

(ב) על מידע מוגן ועל מידע אודות ארגון שנמסר למערך בידי ארגון יחול סעיף 9(א) לחוק חופש המידע התשנ"ח-1998[13] (להלן- חוק חופש המידע) ויראו אותו כמידע שאין למוסרו לפי אותו סעיף.

(ג) ראש הממשלה יקבע באישור ועדת הכנסת לחוק כללים לעניין העברת מידע בעל ערך אבטחתי לגופים המיוחדים לצורך מימוש הוראות חוק זה.

[13] ס"ח התשנ"ח עמ' 226; התשע"ו עמ' 1223

פרק ד': אסדרה לאומית בתחום הגנת הסייבר

מטרות הפרק

42.43. מטרות פרק זה הן:

(א) העלאת העמידות והחוסן של ארגונים במגזרי המשק לתקיפות סייבר, בין היתר באמצעות הנחייתם להיערכות ושמירה על כשירות מתאימה להתמודדות עם איומי סייבר ותקיפות סייבר;

(ב) להסדיר את ההנחיה בתחום הגנת הסייבר תוך קביעת מדיניות אחידה והתחשבות באינטרסים ציבוריים ומשקיים אחרים.

עקרונות על לאסדרה

43.44. (א) בעת קביעת הוראות אסדרה בתקנות, צווים והוראות בתחום הגנת הסייבר (להלן –האסדרה)~~ (להלן – האסדרה) ביד ראש מערך הסייבר הלאומי או בעל סמכות אסדרה~~ ישקלו השיקולים האלה:

(1) התאמת האסדרה לתקינה בינלאומית או תקינה מקובלת ונוהגת במדינות מפותחות בעלות שווקים משמעותיים, בשינויים המחוייבים לפי העניין;

(2) התאמת האסדרה לאיומי הגנת הסייבר בישראל המצדיקים שינויים ייעודיים;

(3) התאמת האסדרה להוראות כל דין בישראל;

~~(3)~~(4) באסדרה מגזרית - התאמת האסדרה למאפייני המגזר ולמאפייני פעילותם של הארגונים השונים במגזר;

~~(4)~~(5) קיום יחס הולם בין היקף ואופן האסדרה לסוגי הארגונים איומי הסייבר שלהם הם חשופים והסתברות התרחשותם.

(ב) קביעת אסדרה תיעשה לאחר בחינת מידע על העלויות הישירות הנובעות ממנה והשפעתה על פעילות עסקית, תחרות הוגנת ורווחת צרכנים; ראש הממשלה רשאי לקבוע תקנות לעניין אופן ביצוע סעיף זה.

המערך – גורם מסדיר לאומי

44.45. (א) ראש המערך ינחה את הרשויות המאסדרות לעניין אופן יישום הוראות חוק זה בתחום הגנת הסייבר ביחס לתחום הנתון לסמכותם.

(ב) אסדרה בתחום הגנת הסייבר תיקבע בהתאם לעקרונות לפי סעיף 43, ובאישור ראש מערך הסייבר הלאומי.

(ג) מי שרואה עצמו נפגע כתוצאה מהחלטה של מאסדר בתחום אסדרת הגנת הסייבר, רשאי לפנות בבקשה לבחינה חוזרת של ההחלטה לראש מערך הסייבר הלאומי; בחינה חוזרת כאמור תעסוק רק בהיבטי הגנת הסייבר של ההחלטה ולא בעמדתו של מאסדר לגבי עניינים אחרים שבסמכותו; ראש הממשלה יקבע בתקנות הוראות לעניין הגשת בקשה לבחינה חוזרת כאמור וסדרי הדיון בבקשה.

הנחיות בתחום הגנת הסייבר

45.46. (א) המערך יפרסם הנחיות בתחום הגנת הסייבר שיגובשו בהתאם לעקרונות המנויים בסעיף 43 ובכלל זה:

(1) מדיניות ונהלים לצורכי התמודדות עם איומי הסייבר בידי ארגון או עבורו;

(2) אמצעים מקובלים הנדרשים לצרכי הגנת הסייבר והתמודדות עם איומי סייבר;

(3) מצבי כוננות ודרישות הגנת הסייבר הנגזרות מהן בארגון;

(4) אופן הבדיקה של קיום הנחיות בתחום הגנת הסייבר בידי ארגון או עבורו;

(5) תהליכי הזדהות;

(6) אופן הדיווח למערך על תקיפות או איומי סייבר;

(ב) לא יפורסמו הנחיות בתחום הגנת הסייבר אלא אם ניתנה תחילה לציבור מספקת להגיב להן, וההנחיות ופרסומן היו על דעת הרשויות המאסדרות הנוגעות בדבר.

מיפוי המרחב האזרחי – המערך

46.47. (א) ראש המערך ~~רשאי~~ יגבש ~~על~~ שיטה למיפוי חשיפת המשק לתקיפות סייבר שיש בהן כדי לפגוע באינטרס חיוני (להלן – השיטה).

(ב) השיטה תכלול התייחסות להיקף הפגיעה האפשרית באינטרס חיוני בשל תקיפת סייבר (להלן – תרחיש הנזק) בהתבסס, בין היתר, על שיקולים אלה:

(1) לעניין חומרת הפגיעה באינטרס חיוני -

(א) רמת השירות הנדרשת מסוגי ארגונים בשגרה ובחירום וטיב השירות ובכלל זה כפי שהוגדרו בידי רשות החירום הלאומית שהוקמה לפי החלטות הממשלה;

(ב) היקף הפגיעה האפשרית בחיי אדם;

(ג) גודל הציבור המשתמש בשירותי הארגון;

(ד) הנזק הכלכלי הצפוי;

(ה) היקף המידע המצוי בארגון, ורגישותו;

(ו) היקף הפגיעה בסביבה;

(ז) פגיעה משמעותית בפרטיות;

(ח) השפעה של תקיפת סייבר בארגון על תפקודם התקין של שירותי המיחשוב והאינטרנט בישראל;

(ט) השפעה של תקיפת סייבר בארגון על גורמי ייצור, משאבים, שירותים, תהליכים ומוצרים החיוניים לקיום האוכלוסייה, לכלכלת המדינה ולפעילות הגורמים המיוחדים בשגרה ובחירום.

(י) עמדת רשות מאסדרת לעניין איומי סייבר בארגונים מפוקחים על ידה;

(2) לעניין החשיפה לתקיפות סייבר – סוגים של איומי סייבר ביחס לפעילות ולהסתברות התרחשותם.

(ג) ראש המערך ידווח לראש הממשלה על השיטה;

(ד) ראש המערך יפרסם את עיקרי השיטה, באופן שאין בו, להנחת דעתו, כדי לסכן אינטרס חיוני.

(ה) ראש המערך יפעל לעדכון השיטה באופן מתמיד, בהתאם להתפתחויות טכנולוגיות, משקיות ואיומי הסייבר המתגלים.

הגדרת רשות מאסדרת

48.~~47.~~ (א) בפרק זה, "רשות מאסדרת" – שר, רשות או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים משקיים המופיעים בתוספת השנייה; ראש הממשלה רשאי להוסיף בצו תחומים משקיים לתוספת השנייה לאחר שהתייעץ עם השר הממונה על התחום, ככל שיש כזה.

(ב) במקרים שבהם בתחום מתחומי הפעילות המנויים לעיל יש יותר מרשות מאסדרת אחת אשר יש לה סמכות הנחיה בתחום הגנת הסייבר, רשאי ראש הממשלה לקבוע בתוספת השנייה, לאחר שהתייעץ עם השרים הנוגעים בדבר, את הרשות המאסדרת האחראית למימוש הוראות פרק זה באותו תחום (להלן – "רשות מאסדרת מובילה").

(ג) הרשות המאסדרת המובילה תפעל בתיאום עם הרשות המאסדרת האחרת בעלת הסמכות באותו תחום פעילות כאמור בסעיף קטן (ב).

תפקיד הרשות המאסדרת - מיפוי בתחום פעילותה

49.~~48.~~ (א) רשות מאסדרת, בהתייעצות עם ראש המערך, תגדיר תרחישי נזק בשל תקיפות סייבר בתחום הפעילות שעליו היא אחראית ואת מידת חומרתם בהתאם לשיטה.

(ב) רשות מאסדרת תסווג את הארגונים המפוקחים על ידה לפי חומרת תרחישי הנזק והקשר של הארגונים אליהם.

אסדרה מגזרית למניעה והתמודדות עם תקיפות סייבר

50.~~49.~~ (א) רשות מאסדרת בהתייעצות עם ראש המערך, תבחן את הצורך בקביעה או במתן הוראות בתחום הגנת הסייבר לארגונים המפוקחים על ידה, ככל שהדבר נדרש לצורך התמודדות עם תרחישי נזק שהוגדרו לפי סעיפים 46 או 48.

(ב) קביעת הוראות בתחום הגנת הסייבר בידי רשות מאסדרת תיעשה בהסכמה של ראש מערך הסייבר הלאומי.

(ג) נקבעה רשות מאסדרת מובילה לפי סעיף 47(ב) תבחן הרשות המאסדרת המובילה את הצורך בהוראות ביחס לארגונים מפוקחים במגזר שצוין בצו האמור.

הוראות למניעת תקיפות סייבר ולהתמודדות עמן

51.~~50.~~ הוראות והנחיות לפי פרק זה יכללו את הדרישות האלה:

(א) דרישות המבוססות על ההנחיות לפי סעיף 45;

(ב) דרישה כי ארגון מפוקח יהיה מסוגל להראות יישום אפקטיבי של המדיניות והנהלים, באמצעות הצהרה עצמית, חוות דעת מקצועית או סקר אבטחה מקצועי שבוצע

על ידי גוף חיצוני; דרישות כאמור ייקבעו על פי אמות מידה שתקבע הרשות המאסדרת בהסכמת המערך, ובהתאם לרמת הסיכון;

(ג) דרישה כי ארגון מפוקח יחזיק תיעוד מעודכן אודות מערכות המחשב המשמשות את הארגון ואבטחתן באופן המאפשר קבלת סיוע חיצוני במידת הצורך.

דרישות ארגוניות בתחום הגנת הסייבר – ממונה סייבר

51.52. (א) רשות מאסדרת רשאית להורות לארגון מפוקח, שרמת הנזק לפי תרחיש הנזק שאליו הוא חשוף היא גבוהה, למנות ממונה הגנת סייבר.

(ב) רשות מאסדרת, בהתייעצות עם ראש המערך, רשאית לקבוע כי ממונה הגנת הסייבר כאמור בסעיף קטן (א) יהיה בעל התאמה ביטחונית.

(ג) ראש הממשלה רשאי לקבוע בתקנות תנאים לגבי כשירותו, חובותיו ותפקידו של ממונה הגנת הסייבר בארגון.

דיווחים תקופתיים

52.53. רשות מאסדרת רשאית להורות לגבי ארגון מפוקח חובת דיווח תקופתי על אופן העמידה בהוראות לפי פרק זה.

יחידות הכוונה מגזריות

53.54. (א) לצורך מימוש האמור בחוק זה תהיה ברשות מאסדרת יחידת הכוונה להגנת סייבר.

(ב) ראש הממשלה יקבע תקנות לעניין תפקידים והכשרה הנדרשת ממי שמפעיל או מסייע להפעלת סמכויות אסדרה בתחום הגנת הסייבר ברשות מאסדרת.

(ג) על אף האמור בחוק המינויים, רשאי ראש הממשלה, לאחר התייעצות עם שר האוצר ועם נציב שירות המדינה, לקבוע בתקנות באישור ועדת החוק לכנסת או בכללים הוראות אחרות מאלה החלות בשירות המדינה, לעניין ארגון וניהול כוח אדם הנדרש למימוש תפקידי יחידת הכוונה להגנת סייבר הפועלת ברשות מאסדרת, והכל בכפוף להוראות חוק יסודות התקציב, ולהוראות חוק התקציב השנתי.

(ד) לא ימונה עובד או יועץ בתחום הגנת הסייבר ליחידת הכוונה מגזרית אלא בהסכמת הגורם האחראי במערך.

קיום הוראות הגנת סייבר כתנאי למתן היתר או רישיון וחידושו

54.55. (א) רשות מאסדרת שמוסמכת להעניק לארגון היתר או רישיון, ~~תעודה או כיוצא באלה (להלן - רישיון)~~, לפעילות לפי דין (להלן - רישיון), רשאית להתנות מתן הרישיון כאמור או חידושו באופן סביר בקיום ההוראות שניתנו לפי סעיף 50, ורשאית היא לקבוע ברישיון כאמור תנאים שעל הארגון לקיים כתנאי לשימוש בזכויות לפי הרישיון.

(ב) הרשות המאסדרת רשאית לדרוש כי ארגון שהיא נתנה לו הוראות לפי סעיף 50, יוכיח עמידה בדרישות הוראות אלה באמצעות חוות דעת של מומחה מתאים; הרשות המאסדרת, בהסכמה של ראש המערך, רשאית להורות על אמות מידה לגבי מומחה ולגבי חוות דעת כאמור.

סמכויות פיקוח

55.56. הוסמך אדם כמפקח ברשות מאסדרת והוקנו לו סמכויות פיקוח לפי אותו דין, יהא רשאי ~~הוא~~ להפעיל את סמכויות הפיקוח שהוקנו לו כאמור לשם פיקוח על ביצוע ההוראות לפי

חוק זה רק לאחר אישור של ראש המערך, או מי שהוא הסמיך לכך, כי יש בידי אותו אדם את הידע וההכשרה הנדרשים לשם הפעלת סמכות הפיקוח בהקשר להוראות חוק זה.

סמכות להתלות רישיון, להגבילו או לבטלו

57.~~56.~~ הוסמכה רשות מאסדרת בדין להתלות רישיון, לבטלו או להגבילו בשל הפרת תנאי הרישיון שניתן לפי דין או בשל הפרת הוראות הדין, יחולו סמכויות אלה, בשינויים המחויבים, גם בשל הפרת הוראות שנקבעו ברישיון או שניתנו לפי חוק זה.

הנחייה ופיקוח ישירים של המערך על ארגונים

58.~~57.~~ (א) המערך יפקח במישרין לפי הוראות פרק זה על מגזר משקי המוגדר בתוספת השלישית; ראש הממשלה רשאי לתקן את התוספת השלישית בצו ולהורות על פיקוח והנחייה ישירים בידי המערך על פעילות במגזר משקי שקבע, ובלבד שהתקיימו כל אלה:

(1) המגזר כולל ארגונים המקיימים פעילות החשופה לתקיפות סייבר שפגיעה בה יכולה לגרום לפגיעה באינטרס חיוני ;

(2) אין רשות מאסדרת בעלת סמכות, משאבים ויכולת ארגונית להנחות בתחום הגנת הסייבר בארגונים השייכים למגזר האמור;

(3) יש חשש סביר שלנוכח העדרה של רשות מאסדרת כאמור בפסקה (2), תתממש הפגיעה באינטרס החיוני המנוי בפסקה (1).

(ב) בסעיף זה "מגזר משקי" – ארגון או קבוצת ארגונים, שהפעילות העיקרית שלהם בעלת מאפיינים או צביון דומה.

סמכות מתן הוראות במסגרת הנחיה ישירה

59.~~58.~~ הורה ראש הממשלה על הנחיה ופיקוח ישירים על ידי המערך, כאמור בסעיף 57, יחולו הוראות סעיפים 49 עד 52 על המערך כמפורט להלן:

(א) המערך ימפה את המגזר שבו עליו לבצע הנחייה ופיקוח ישירים בהתאם לשיטה.

(ב) ראש המערך רשאי לתת הוראות לשם יישום הגנת הסייבר לארגונים במגזר האמור, ובכלל זה הוא רשאי להורות על מינוי ממונה הגנת סייבר וקבלת דיווחים תקופתיים.

סמכויות פיקוח במסגרת הנחיה ישירה

60.~~59.~~ לשם פיקוח על קיום הוראות לפי סעיף 58 יהיו לעובד מוסמך שמונה לכך סמכויות אלה:

(א) לדרוש מכל אדם למסור לו את שמו ומענו ולהציג בפניו תעודת זהות או תעודה רשמית אחרת המזהה אותו;

(ב) לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך שיש בהם כדי להבטיח או להקל על ביצוע הוראות פרק זה; בפסקה זו, "מסמך" - לרבות פלט, כהגדרתו בחוק המחשבים.

(ג) להיכנס למקום, ובלבד שלא ייכנס למקום המשמש למגורים אלא על פי צו של בית משפט.

מתן הוראות לארגון במגזר שמצוי בהנחיה ישירה של המערך

~~60.~~61. נוכח עובד מוסמך כי ארגון לא קיים הוראות ליישום הגנת הסייבר שניתנו לפי סעיף 58(2) רשאי הוא להורות לארגון לנקוט את הפעולות הנדרשות לשם כך.

מתן סמכויות לרשות מאסדרת לשם הנחיית ארגון ברמת סיכון גבוהה

~~61.~~62. (א) ראש הממשלה רשאי להורות בצו על הוספת רשות מאסדרת לתוספת הרביעית, אם נוכח, בהתייעצות עם השר הממונה וראש המערך, כי התקיימו שני אלה:

(1) תחת פיקוחה של הרשות המאסדרת נמצא ארגון שתקיפת סייבר בו עלולה לגרום לנזק חמור לאינטרס חיוני בהתאם למיפוי שנערך לפי סעיף 48;

(2) אין לרשות המאסדרת סמכויות על פי דין להורות לארגון ליישם הוראות הגנה בסייבר, ולפקח על ישומן, בהיקף הנדרש להתמודדות עם הסיכון.

(ב) לרשות מאסדרת המנויה בתוספת הרביעית יהיו נתונות הסמכויות המנויות בסעיפים 58, 59 ו – 60 לצורך קיום הוראות חוק זה.

הנחייה ישירה זמנית בידי המערך

~~62.~~63. (א) נוכח ראש המערך כי לעניין ארגון מסוים מתקיימים התנאים הבאים, רשאי הוא להכריז כי הארגון יהיה נתון להנחיה זמנית על ידי המערך:

(1) הארגון מקיים פעילות שחשופה לתקיפות סייבר שעלולות לגרום לפגיעה חמורה באינטרס חיוני;

(2) הארגון אינו כפוף להנחיה ופיקוח על פי דין של רשות מאסדרת, ועקב כך עלולה להתממש הפגיעה באינטרס החיוני המנוי בפסקה (1).

(ב) קבע ראש המערך כאמור, יהיו נתונות לעובד מוסמך הסמכויות לפי סעיפים 58, 59 ו – 60 כלפי הארגון.

(ג) הנחייה לפי סעיף זה תהיה לפרק זמן שלא יעלה על שלושה חודשים מהכרזה לפי סעיף (א).

<u>פרק ה': הוראות שונות</u>

הארגון והדירקטוריון

~~63.~~64. (א) דירקטוריון חברה מסוג שקבע ראש הממשלה בהתייעצות עם שר המשפטים (להלן – החברה), ידון לפחות אחת לשנה באלה:

(1) איומי הסייבר לפעילות החברה;

(2) הנזק שעלול להיגרם לתפקודה, לנכסיה, ללקוחותיה או לספקיה של החברה כתוצאה מהתרחשות תקיפת סייבר והסתברות התרחשות הנזק בשל תקיפת סייבר;

(3) משאבים שהוקצו לצורך צמצום החשיפה האמורה;

(4) הגורם האחראי בחברה על הגנת הסייבר, הסמכויות והמשאבים שניתנו לו לשם כך;

(5) אופן והיקף היישום של ההנחיות לפי סעיף 45;

(ב) הוראת סעיף זה לא תחול מקום שדירקטוריון חברה כפוף להוראות דומות של רשות מאסדרת.

פעילות מותרת לצורכי הגנת סייבר – הארגון

64.65. לא יראו פעולה שמבצע ארגון למטרת הגנת הסייבר של מחשבי הארגון כפגיעה בפרטיות, האזנת סתר, חדירה אסורה לחומר מחשב, אם מתקיימים בה כל אלה:

(א) לארגון יש מדיניות הגנת סייבר בהתאם להוראות או תקן מקובל ביחס לצרכי הגנת סייבר בארגון, בשים לב לאיומי הסייבר שלהם הוא חשוף;

(ב) לארגון יש מדיניות גישה ושימוש במידע המעובד לצורכי הגנת הסייבר, המגבילה את האיסוף, השימוש ועיבוד המידע להיקף המינימלי נדרש לצורכי הגנת הסייבר;

(ג) הארגון ~~הודיע~~ מסר לעובדיו, ללקוחותיו והודיע לגורמים אחרים שמידע עליהם עשוי להיאסף במסגרת פעילות זו, פרטים על הפעילות, על מטרותיה, ועל השימוש במידע;

בסעיף זה, "מחשבי הארגון" - מחשבים המצויים ברשותו כדין או בשימושו בהתאם לחוזה.

פעילות מותרת לצרכי הגנת הסייבר

65.66. לא יראו שיתוף של מידע שנאסף בארגון, עם ארגון נוסף או יותר, או עם מערך הסייבר הלאומי כפגיעה בפרטיות לפי חוק הגנת הפרטיות, אם מתקיימים כל אלה:

(א) המידע הוא מידע בעל ערך אבטחתי;

(ב) הארגון מסר פרטים על הפעילות, על מטרותיה, ועל השימוש במידע במסגרתה לעובדיו ולקוחותיו;

(ג) השימוש במידע הוא למטרת הגנת הסייבר בלבד.

~~(א) עובד המערך או מי שפועל מטעמו לא יישאו באחריות לפי חוק הגנת הפרטיות על פגיעה בפרטיות לפי חוק הגנת הפרטיות, שנעשתה באופן סביר במסגרת תפקידם ולשם מילוי.~~

שיתוף מידע לצורכי הגנה – פעולה מותרת

66.67. לא יראו שיתוף מידע בעל ערך אבטחתי בין שני ארגונים או יותר למטרת הגנת סייבר, כהפרה של הוראות חוק ההגבלים העסקיים, התשמ"ח-1988,[14] בתנאי שיתקיימו כל אלה:

(א) המידע אינו כולל נתונים על לקוחות, ספקים, כמויות או מחירים של הארגונים;

(ב) המידע אינו כולל מידע על איכות מוצר או שירות המסופק על ידי אחד הארגונים.

תחולת החוק על גופים נוספים

67.68. סמכויות מכוח חוק זה לא יופעלו לגבי הגופים המנויים להלן, אלא בהסכמת הגורמים המנויים לצדם –

(א) לשכת נשיא המדינה – בהסכמת מנהל הלשכה;

[14] ס"ח התשמ"ח, עמ' 128; התשע"ו, עמ' 126

(ב) הכנסת – בהסכמת יושב ראש הכנסת;

(ג) משרד מבקר המדינה – בהסכמת מבקר המדינה;

(ד) ועדת הבחירות המרכזית לכנסת – בהסכמת יושב ראש הוועדה;

(ה) מערכת בתי המשפט – בהסכמת נשיא בית המשפט העליון;

~~(ה) הגופים המיוחדים – בהסכמת ראש הגוף;~~

~~(ו) מערכת הביטחון והגופים המנויים בצו שר הביטחון לפי החוק להסדרת הביטחון – בהסכמת הממונה על הביטחון במערכת הביטחון.~~

סקרים משקיים ומגזריים בנושאי הגנת סייבר

~~68.~~69. (א) ראש המערך ~~או מי שהוא הסמיכו לכך,~~ יפעל לביצועם, באמצעות הלשכה המרכזית לסטטיסטיקה על פי פקודת הסטטיסטיקה [נוסח חדש], התשל"ב-1972 של ~~רשאי לערוך~~ סקרים לאומיים או מגזריים על מנת לאתר פערים ברמת הגנת הסייבר ולבירור רמת ההגנה במרחב הסייבר במרחב האזרחי.

(ב) ~~כל אדם חייב, לפי דרישתו של ראש המערך, או מי שהוא הסמיך לכך מבין עובדי המערך, למסור לו את המידע, המסמכים, ושאר התעודות שלדעת ראש המערך יש בהם כדי להבטיח או להקל את ביצועו של סעיף זה.~~ הסקרים שיבוצעו על פי סעיף זה יפורסמו לציבור על ידי הלשכה המרכזית לסטטיסטיקה.

הסדרים הסכמיים בתחום הגנת הסייבר

~~69.~~70. אין באמור בהוראות חוק זה כדי למנוע הסדרה של דרישות לקביעת נהלים ויישום אמצעי אבטחה הדרושים לשם הגנה בסייבר ~~פעולות הקבועות בו~~ באמצעות הסכמים, ובכלל זה במסגרת הסכמים שבין הגופים המיוחדים או משרד הביטחון לבין ספקיהם.

התקשרות עם גורמים מקבילים

~~70.~~71. (א) ראש המערך רשאי לחתום עם גוף בינלאומי הסכם לשיתוף פעולה ועזרה הדדית לשם התמודדות עם תקיפות סייבר או היערכות לקראתן, או לקידום שיתופי פעולה בתחום הסייבר במישור הבינלאומי; בסעיף זה - "גוף בינלאומי" – גוף העוסק בהגנת הסייבר במדינת חוץ, בין אם הוא רשות ממשלתית ציבורית או ארגון בינלאומי; ראש הממשלה יקבע בכללים באישור ועדת הכנסת לחוק הוראות לעניין פעילות לפי סעיף זה.

(ב) לא יועבר מידע מוגן לגוף בינלאומי אלא בהסכמת האדם או הארגון שהמידע הוא על אודותיו ~~אלא אם כן מדובר במידע בעל ערך אבטחתי ושוכנע ראש המערך, לאחר שנועץ במפקח הפנימי על הפרטיות, כי הוא ישמש אך ורק למטרה שלשמה נמסר~~.

~~הסמכה לביצוע פעולות לסיכול תקיפת סייבר הנמנית בין יעדי שירות הביטחון הכללי~~

~~71. (א) לצורך סיכול איומי טרור וריגול, כמשמעותם בסעיף 7 לחוק שירות הביטחון הכללי, רשאי ראש שירות הביטחון הכללי (להלן – ראש שב"כ), להסמיך בעלי תפקידים מבין עובדי שירות הביטחון הכללי (להלן – שב"כ) בסמכויות הנתונות לעובד מוסמך או גורם אחראי לפי סעיפים 19 עד 36 לחוק.~~

~~(ב) הפעלת סמכויות לפי סעיף (א) תיעשה לאחר שהתקיימו כל אלה:~~

~~(1) ראש שב"כ השתכנע כי יש תקיפת סייבר והתקיימו יתר התנאים הקבועים בסעיף 19 לחוק (להלן – התקיפה);~~

~~(2) ראש שב"כ השתכנע כי הפעלת הסמכות נדרשת לצורך סיכול איומי טרור או ריגול כמשמעותם בסעיף 7 לחוק שירות הביטחון הכללי, הנובעים מהתקיפה;~~

~~(3) ראש שב"כ או עובד בכיר שהוא מינה לכך התייעץ עם ראש מערך הסייבר הלאומי או עובד בכיר שהוא מינה לכך לענין הפעלת הסמכות לפי סעיף זה;~~

~~(ג) יתר הוראות החוק למעט סעיפים 13 עד 15 יחולו על הפעלת סמכויות לפי סעיף קטן (א) ומידע שנאסף באמצעותן.~~

איסור על גילוי מידע על פעילות המערך

72. פעילות מערך הסייבר לפי חוק זה אסורה בגילוי אלא בהתאם להוראות חוק זה או להוראות שיקבעו ראש הממשלה ושר המשפטים, באישור ועדת הכנסת לחוק.

תקנות

73. ראש הממשלה ממונה על ביצועו של חוק זה, והוא רשאי להתקין תקנות לביצועו באישור ועדת הכנסת לחוק, אלא אם נקבע אחרת בחוק זה..

תוספת ראשונה (סעיף 41)

תוספת שנייה (סעיף 47)

שר, רשות או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים המשקיים האלה:

(1) שירותים פיננסיים;

(2) שירותי בריאות ורפואה;

(3) תחבורה, תחבורה ציבורית, תובלה, תעופה, ושייט;

(4) הגנת הסביבה;

(5) ייצור אנרגיה והולכתה;

(6) מים וביוב;

(7) שירותי דואר ותקשורת, שירותי בזק ושידורים מסחריים

תוספת שלישית (סעיף 57)

תוספת רביעית (סעיף 61)