אסדרה של אבטחת סייבר בציוד קצה

מאת

אסף אבידן*

איומי סייבר על ציוד קצה בתקשורת, כגון הטלפון החכם, הם בעלי משמעות רבה בימינו, לא רק עבור המשתמש הפרטי אלא גם לפרטים וארגונים נוספים ברשת, בשל כך שהם עשויים להביא להחצנות שליליות לגורמים אלה.

מאמר זה בוחן את הצורך וההצדקות לאסדרה (רגולציה) של אבטחת סייבר בציוד קצה, דהיינו האם על המדינה באמצעות הרגולטור הרלוונטי, להתערב על מנת להבטיח קיומה של אבטחת סייבר בציוד מסוג זה, מי הוא הרגולטור הרלוונטי, מהו סוג האסדרה הנדרש, אם בכלל, מה הן ההצדקות ומהו המסד משפטי לביסוס התערבות רגולטורית.

מספר מגמות מקבילות הפכו את הסוגיה של אבטחת סייבר בציוד קצה (להלן: **בעיית האבטחה**) לבעלת חשיבות אשר חורגת מעולמו של המשתמש הפרטי. מגמה אחת היא ההתפתחות הטכנולוגית, שהביאה לכך שרשת האינטרנט, רשתות במקום העבודה, רשתות ביתיות וציוד הקצה המחובר אליהן הפכו חלק בלתי נפרד מההתנהלות היום־יומית ומהחיים הדיגיטליים המודרניים. כך ניתן לראות מצבים בהם ציוד קצה פרטי מחובר לרשת ארגונית בלא בקרה, בניגוד לבקרה הקיימת בדרך כלל על ציוד ארגוני שמחובר לאותה רשת. לא פעם מאוחסן בציוד קצה מידע אישי ועסקי רב או שניתן להגיע באמצעותו לאחסון בענן או ברשת ביתית או ארגונית, כמו גם למשתמשים אחרים ולציוד נוסף שמחובר לאותה רשת. על כן בעיית האבטחה בציוד הקצה ופגיעות שלו למתקפות סייבר יוצרת, מעבר לפגיעה המיידית במשתמש או בבעלים של ציוד הקצה, גם החצנות שליליות ופוטנציאל לפגיעה משמעותית באחרים וברשת.

מגמה נוספת היא ההתגברות של מתקפות הסייבר (מצד גורמים פרטיים ומדינתיים) והעלייה הניכרת בכמות ובתחכום המתקפות, בנזקים הכלכליים שנגרמים מהן ובנזקים הפוטנציאליים שלהן, במעגלים הולכים ונרחבים. לא פעם גם נעשה שימוש בציוד קצה כ"בסיס" להוצאת מתקפות כאלה, באמצעות נוזקות (Malware), דהיינו תוכנות זדוניות, המתוקנות בו (באופן לא רצוני או לא מכוון מבחינת המשתמש), ומקנות לתוקף שליטה בציוד הקצה ובמידע, או שהן

---

* עו"ד ומהנדס אלקטרוניקה. מוסמך במשפט וטכנולוגיה, הפקולטה למשפטים, אוניברסיטת חיפה, ועמית מחקר במרכז סייבר מדיניות ומשפט (CCLP) של אוניברסיטת חיפה, שהמחקר עליו מתבסס מאמר זה נערך בתמיכתו האדיבה.

נמצאות במצב המתנה להוראה מרחוק להוצאת המתקפה לפועל במועד שקובע התוקף.

התמודדות עם כל אלה דורשת מאמץ מתמשך וקבוע, שלא לומר סיזיפי, של עדכוני תוכנה ועדכוני אבטחה, ויש בה לעיתים מורכבות הנוצרת בשל האקוסיסטם (מכלול הגורמים המעורבים) של ציוד הקצה. פעולות אלה דרושות כדי להבטיח שציוד הקצה יהיה מוגן, ככל האפשר, מפני איומי סייבר ולא יהיה נקודת חולשה שדרכה ניתן יהיה לחדור למערכות נוספות ולמשתמשים אחרים ולפגוע ברשת.

מגמה נוספת, שיש לה השפעה על אבטחת סייבר בציוד קצה ועל המורכבות שהוזכרה לעיל, שבעיית האבטחה יכולה לשמש אמצעי להמשגת הקושי שהיא יוצרת, היא המגמה של מעבר ממוצרים לשירותים. גם הטלפון החכם, אף שהוא מוצר, מהווה למעשה פלטפורמה שעיקרה תוכן ושירותים. ציודי קצה, כגון ממירים ונתבים, כבר לא נרכשים על ידי המשתמשים, אלא הם חלק מהשירות שנותנים ספקי שירותי הטלוויזיה, ידיאו לפי דרישה (VoD) או שירותים של חיבוריות לאינטרנט. יתרה מכך, עם התגברות התופעה של האינטרנט של הדברים (IoT), צפויים סוגי ומספר ציודי הקצה לגדול בצורה משמעותית. יש גם לצפות שחלק הארי שלהם לא יהיה בבעלות המשתמשים, אלא יינתן להם כחלק מהשירות שהם צורכים. חשיבותה של אבטחת הסייבר בציוד קצה באה לידי ביטוי ביתר שאת נוכח מגמה זו. כפי שנטען במאמר, לעניין זה יש גם משקל במסגרת השיקולים של אסדרת אבטחת הסייבר וביחס לשאלה מיהו הגורם המתאים ביותר להיות מושא של אסדרה כזו.

המאמר פותח במבוא המתאר את הבעיה באופן כללי. הפרק הראשון עוסק בטקסונומיה והגדרות של מרחב הסייבר ואבטחת סייבר. לאחר מכן המאמר פונה לסקירת המסגרת הנורמטיבית החלה על ציוד קצה ובחינת מעמדו של הטלפון החכם וההחצנות השליליות של היעדר אבטחת סייבר או היותה לקויה. הפרק השני במאמר עוסק במקורות, הגורמים והסיבות לבעיית האבטחה. פרק זה מתאר את הכשלים העיקריים העומדים ביסודה. יש לכך חשיבות רבה הן להבנה של מצב האבטחה בטלפונים חכמים ובציוד קצה בכלל והן לבחינת השאלה אם פתרונות קיימים מדיסציפלינות משפטיות שונות נותנים להם מענה – שאלה זו נדונה בפרק השלישי. הפרק הרביעי במאמר עוסק באסדרה ובפתרונות אפשריים לבעיית האבטחה על ידי סוגים שונים של אסדרה. בפרק החמישי והאחרון במאמר מובאיסדברי סיכום על בסיס הניתוח ומכלול המסקנות העולות מהפרקים הקודמים.

בעוד שיש בספרות עיסוק באבטחת סייבר באופן כללי ובאבטחת סייבר בתשתיות קריטיות, ובעוד שהרגולציה הקיימת עוסקת בעיקר באבטחת סייבר של תשתיות אלה ושל ארגונים או של מרחב הסייבר בהיבט התשתית הטכנית שלו והתכנים שבו, טרם הוקדש דיון מעמיק לשאלת הרגולציה של אבטחת סייבר בציוד קצה ובמגזר האזרחי הפרטי, ומכאן חשיבות המאמר. חשיבות נוספת עשויה להיות בעת הזו, נוכח שתי התפתחויות שחלו בתחום: (1) העובדה שהצעת חוק הסייבר, שאמור לכלול בתוכו פרק של רגולציה, קורמת עור וגידים

ונמצאת בעבודה, כאשר הטיפול בסיכוני הסייבר, שהיה עד כה בידי רגולטורים מגזריים, אמור להיות מתוכלל על ידי גורם מרכזי – מערך הסייבר הלאומי; [1] (2) פורסמה על ידי רשות הסייבר הלאומית הגרסה הראשונה של תורת ההגנה בסייבר לארגון, אלא שגם אם יש בה התייחסות מסוימת לציוד קצה, עיקר המיקוד בה הוא באבטחת סייבר של ארגונים.

החשיבות בעת הזו היא גם נוכח היעד ששם לעצמו משרד התקשורת לשנים 2017–2018, תחת הכותרת של התאמת הרגולציה על שוק הטלקום בישראל לעידן המודרני, וכן היעד של סיום כתיבת מסמכי הסדרה בנושא הגנת הסייבר.[2] במאמר קודם עסק המחבר בסוגיית האסדרה של הועדת תדרים אלקטרומגנטיים בישראל לצורך שימוש ללא רישיון במוצרים אלחוטיים בשוק הביתי והמשרדי, לרבות ציוד קצה, והשפעתה על השימוש בציוד זה ועל הציבור בכללותו.[3] במאמר הנוכחי נדון היבט אחר של אסדרה, הנוגע במישרין לציוד הקצה ולרגולציה של תחום שונה – אבטחת סייבר בציוד קצה.

מבוא; א. אבטחת סייבר בציוד קצה; 1. מרחב הסייבר, מתקפות סייבר והסיכונים הכרוכים בהן; 2. ציוד קצה והמסגרת הנורמטיבית החלה עליו; 3. אסדרה של ציוד קצה בישראל – ״אישור סוג״; 4. מעמדו המרכזי של הטלפון החכם בחיים הדיגיטליים, האיומים וההחצנות השליליות של בעיית האבטחה. **ב. קיומה של בעיית האבטחה, הכשלים והסיבות לקיומה**; 1. כשלים ביסוד בעיית האבטחה – מבוא; 2. כשלים ביסוד בעיית האבטחה – דיון פרטני; (א) אחוז התקנה נמוך של אמצעי אבטחת סייבר; (ב) עדכונים וטלאים (Patches) במערכות ההפעלה ובאפליקציות; (ג) חשיפה לאפליקציות זדוניות וחולשות באפליקציות לגיטימיות; (ד) חשיפה במגוון חזיתות לקישורים זדוניים; (ה) חיבוריות קבועה (Always Connected) ונגישה לטלפון באמצעות מספר ממשקי קישוריות אלחוטית; (ו) אי־קבלת תמיכה שוטפת ממערך IT בארגונים; (ז) חשיפות למתקפות חומרה בשל פגיעות פיזית; (ח) חולשות מובנות בפרוטוקול הסלולרי; (ט) הגורם האנושי; (י) נוזקה המגיע עם הטלפון החכם (מותקנת מראש); (יא) סיכום – כשלים עיקריים וסיבות אפשריות. **ג. התמודדות עם בעיית האבטחה באמצעות דיסציפלינות משפטיות שונות**; 1. הגנת הפרטיות והמידע – רגולציית הגנה המידע של האיחוד האירופאי; 2. הגנת הפרטיות והמידע – תקנות אבטחת מידע; 3. דיני נזיקין; 4. דיני הגנת הצרכן – חובת

---

1 הצעת החוק טרם פורסמה בעת כתיבת מאמר זה, אולם ביום 20.6.2018 פורסם תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע״ח–2018 (להלן: **תזכיר חוק הסייבר**). אפשר למצוא את התזכיר באתר ״קשרי ממשל״ של ממשלת ישראל: http://www.tazkirim.gov.il/pages/tazkirim.aspx (כל אתרי האינטרנט המוזכרים במאמר זה נצפו לאחרונה בנובמבר 2018, אלא אם נאמר אחרת במפורש).

2 **ספר תוכניות העבודה של משרדי הממשלה לשנים 2017-18** (2017), יעד 5.1 בעמ׳ 663, ניתן לצפייה באתר: http://www.plans.gov.il/pdf2017/index.html).

3 אסף אבידן ״הועדת תדרים לשימוש במוצרי צריכה מחשוב ובקרה ללא רישיון״ **דין ודברים** ח 345 (תשע״ה).

יידוע; 5. אחריות למוצרים פגומים; 6. דיני הגנת הצרכן – חובת גילוי ואחריות יצרן. **ד. אסדרה כמענה לבעיית האבטחה;** 1. אסדרה – כללי (בקצירת האומר); 2. אסדרה עצמית; 3. אסדרה על דרך של הנחיה והעברת מידע ויישומו על בסיס התנדבותי; 4. אסדרה באמצעות ״אישור סוג״. **ה. דברי סיכום.**

מבוא

מתקפות סייבר ומתקפות על מערכות מחשוב דרך האינטרנט אינן דבר חדש, וכבר בשנת 1988 גרמה ״תולעת״ אינטרנט (the "Morris Worm") להאטה וקריסה של מערכות מחשוב מרכזיות ותחנות עבודה שהיו מחוברות לרשת.[4] עם זאת, בשל ההתפתחויות הטכנולוגיות מרחיקות הלכת שחלו מאז, הן רשת האינטרנט והן הציוד המחובר אליה התרחבו והפכו חלק בלתי נפרד מההתנהלות היום־יומית ומהחיים המודרניים. לא פעם מאוחסן בציוד כזה מידע אישי ועסקי רב, או אפשר להגיע באמצעותו לאחסון בענן או ברשת ביתית או ארגונית, כמו גם למשתמשים אחרים ולציוד המחוברים לאותה רשת.

מרחב הסייבר הוא מרחב מאתגר, לא רק מפני היותו פגיע, אלא בשל התלות, הן של החברה והן של המדינה, במרחב זה, מאחר שהוא ״[...] מאפשר, מצד אחד, זרימת מידע, המסייעת ברוב המקרים ליצירת פריחה כלכלית ורווחה חברתית, ומצד שני, הוא נתון לאיומים ביטחוניים, פליליים ומסחריים״.[5]

נוכח עובדות אלו, ונוכח מתקפות סייבר בהיקפים הולכים וגדלים (מצד גורמים פרטיים ומדינתיים), התחכום המתגבר של המתקפות, הנזקים הכלכליים שנגרמים מהן ויתרה מכך – הנזקים הפוטנציאליים שלהן, הפכה הסוגיה של אבטחת הסייבר לנושא מרכזי ורב משקל בסדר היום של מדינת ישראל כמו גם של מדינות אחרות ברחבי העולם.[6] בארצות הברית העידו מנהל המודיעין הלאומי (Director of National

---

4 לתיאור מפורט של המקרה ראו: Jonathan Zittrain, *The Future of the Internet and How to Stop It* (2008) pp 36-37.

5 גבי סיבוני ועידו סיון־סביליה, רגולציה במרחב הסייבר, מזכר 180 (אוגוסט 2018), המכון למחקרי ביטחון לאומי, אוניברסיטת תל אביב (להלן: **סיבוני וסביליה**), בעמ׳ 21, ניתן לצפייה באתר: http://www.inss.org.il/he/wp-content/uploads/sites/2/2018/08/memo180CyberRegulation_6.pdf.

6 כך למשל, בתחילת שנת 2017 פורסם כי אותרה נוזקה (maleware), שפועלת רק בזיכרון המחשב או המכשיר הנייד וכלל אינה משאירה אחריה עקבות. Shaun Waterman, New malware works only in memory, leaves no trace (9.2.2017), ניתן לצפייה באתר: https://www.cyberscoop.com/kaspersky-fileless-malware-memory-attribution-detection/. בארצות הברית דיווחו ה־FBI וה־DHS בחודשים מאי 2017 עד אוגוסט 2018 על מאמצים הולכים ומתגברים של ממשלת צפון קוריאה ליצור מתקפות סייבר על גורמים שונים בארצות הברית, US-CERT, North Korean Maclicious Cyber Activity (9.8.2018), ניתן לצפייה באתר: https://www.us-cert.gov/ncas/current-activity/2018/08/09/North-Korean-Malicious-Cyber-Activity/. מדיווחים נוספים של ה־US CERT עולה כי

Intelligence)[7] ומנהל ה־FBI בפני הקונגרס כי מתקפות סייבר הן האיום החמור ביותר על הביטחון הלאומי שחווה ארצות הברית.[8] ממשלת ישראל הכירה באיום הממשי של מתקפות סייבר הן על תשתיותיה ועל המגזר הציבורי והן על המגזר האזרחי, הכרה שמצאה ביטוי בכמה החלטות שמטרתן קידום היכולת הלאומית במרחב הסייבר והגנת הסייבר.[9]

מתקפות סייבר על מתקני רשת ותשתיות קריטיות בארצות הברית מבוצעות מטעמם ובחסותם של הגורמים הבאים: US-CERT, Alert (TA18-106A), Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices (16.4.2018), **ניתן לצפייה באתר**: https://www.us-cert.gov/ncas/alerts/TA18-106A **וכן** US-CERT, Alert (TA18-074A), Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (15.3.2018), **ניתן לצפייה באתר**: https://www.us-cert.gov/ncas/alerts/TA18-074A. בתזכיר חוק הסייבר, לעיל, הערה 1, נכתב בפרק המבוא כדלקמן: ״בשנים האחרונות ניכרת עלייה משמעותית בשכיחותם של איומי סייבר ובחומרתם, בעולם כולו. מגמה זו מיוחסת במידה רבה למאפיינים הייחודיים של המרחב אשר מקלים על הפעילות העוינת בתוכו: קבועי הזמן הקצרים המאפיינים את השתנות המרחב ואת הנעשה בו, חוסר הרלוונטיות של המרחק הפיזי לפעילות במרחב, וכתוצאה מכך חשיפה לאיומים מכל העולם בסבירות דומה, האנונימיות היחסית המתאפשרת בו, היעדר כוח ביטחוני החוצץ בין התוקף לנתקף, עלות נמוכה לפיתוח יכולות פעולה במרחב ועליית ׳שטח הפנים׳ לתקיפה כתוצאה מהתרחבותו המהירה של מרחב זה. איומים אלו עלולים להוביל לפגיעה בתוך המרחב (למשל במידע או בתפקוד), לפגיעה בעולם הפיסי (למשל פגיעה במערכות רפואיות או בתשתיות אנרגיה), לפגיעה תפקודית משקית קשה, ואף לפגיעה בחיי אדם. תקיפות הסייבר הולכות והופכות מתוחכמות יותר, ותוצאותיהן קשות יותר ומורכבות יותר לטיפול. כתוצאה מכך עולה הסיכון לפגיעה בביטחון האישי, בפעילות המשק ובביטחון המדינה, באופן המחייב התייחסות ברמה הלאומית״. בדוח הפורום הכלכלי לשנת 2018 נקבע כי מתקפות סייבר הן אחד מחמשת הסיכונים הגלובליים (במקום השלישי) מבחינת הסבירות להתקיימותו (Likelyhood) ובמקום השישי מבחינת ההשפעה שלו (Impact) על הכלכלה העולמית. **ראו** World Economic Forum, The Global Risks Report 2018 13th Edition (17/01/2018), **ניתן לצפייה באתר**: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf. **ראו גם** פרק 2.2 (״הערות וכימות הסיכון לאינטרס הציבורי (במצב הקיים)״ במסמך ״הערכת השפעות רגולציה – פרק האסדרה בחוק הסייבר״, המצורף כחלק מתזכיר חוק הסייבר (להלן: **מסמך השפעת הרגולציה**).

7 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE **ניתן לצפייה באתר**: https://www.dni.gov/index.php#content.

8 Stephanie K. Pell & Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy", 28 *H Harv. J.L. & Tech.* (2014) p.64, footnote 340.

9 החלטה מס׳ 3611 של הממשלה ה־32, ״**קידום היכולת הלאומית במרחב הקיברנטי**״ (7.8.2011) (להלן: **החלטה 3611**), **ניתנת לצפייה באתר**: https://www.gov.il/he/Departments/policies/2011_des3611; החלטה מס׳ 2443 של הממשלה ה־33, ״**קידום**

מאמר זה מתמקד באבטחת סייבר בציוד קצה בתקשורת, ולשם ניתוח הבעיה הוא מצטמצם לניתוח מצב האבטחה בטלפון הסלולרי החכם,[10] שהינו ציוד מסוג זה,[11] וגם דוגמה מובהקת לנקודת תורפה אפשרית מבחינת אבטחת סייבר.

הטעם לכך שהטלפון החכם הוא דוגמה לחשיבות של אבטחת הסייבר בציוד קצה הוא העובדה שהוא הפך להיות מרכז החיים הדיגיטליים של משתמשים רבים, תפקיד שבעבר הלא רחוק מילא המחשב האישי.[12] הטלפון החכם גם הפך חלק מהרשת הארגונית, נוכח הכנסת מכשירים ניידים פרטיים על ידי עובדים לתוך הרשת של מקום העבודה.[13] על כן, כפי שנטען ומודגם במאמר זה, הטלפון החכם הוא נקודת תורפה

אסדרה לאומית והובלה ממשלתית בהגנת הסייבר״ (15.2.2015) (להלן: **החלטה 2443**), ניתנת לצפייה באתר: https://www.gov.il/he/Departments/policies/2015_des2443; החלטה מס׳ 2444 של הממשלה ה־33, **״ההיערכות הלאומית להגנת הסייבר״** (15/02/2015). (להלן: **החלטה 2444**). ניתנת לצפייה באתר: https://www.gov.il/he/Departments/policies/2015_des2444.

10 ראו ערך ״טלפון חכם״ בוויקיפדיה: טלפון חכם ״הוא מחשב כף יד המשלב יכולות של טלפון סלולרי, נגן מוזיקה דיגיטלי, מצלמה משוכללת, מכשיר איתור לווייני ועוד. בטלפון החכם ניתן להתקין יישומים מתקדמים, בדומה לאלה המותקנים במחשב שולחני. בדומה למחשב שולחני, גם לטלפון החכם יש מערכת הפעלה. לעיתים קרובות הטלפון החכם, כמו כל מחשבי כף היד, נכלל תחת קטגוריית ה־Pocket PC״. ניתן לצפייה באתר: https://he.wikipedia.org/wiki/%D7%98%D7%9C%D7%A4%D7%95%D7%9F_%D7%97%D7%9B%D7%9D. מדובר אפוא במכשיר רט״ן – רדיו טלפון נייד (ההגדרה בסעיף 1 לחוק התקשורת (בזק ושידורים), תשמ״ב–1982, ס״ח 1060, להלן – **חוק התקשורת**), אך בעל יכולות נרחבות בהרבה מהמכשירים הסלולריים בדורות הראשונים, ששימשו רק לצורך שיחות קוליות או הודעות טקסט.

11 בית המשפט העליון הכתיר את הטלפון החכם בתואר ״ציוד הקצה האולטימטיבי״ – פסה״ד בבג״ץ 6414/15 **ענק הבטיחות נ׳ משרד התקשורת** (פורסם בנבו, 2016) (להלן: **פס״ד ענק הבטיחות**), סעיף 29 בעמ׳ 8.

12 יש לציין שלאחרונה הגבולות בין הטלפון הנייד והמחשב האישי הולכים ומטשטשים, כאשר מחשבים ניידים מצוידים באותם מעבדים שעושים בהם שימוש בטלפונים החכמים והם צפויים להיות מצוידים גם בקישוריות סלולרית בדור 5 ולהיות "Always Connected" – ראו כתבות בעניין: Cherlynn Low, Samsung is making a Snapdragon-powered PC (6.4.2018) ניתן לצפייה באתר: https://www.engadget.com/2018/06/04/samsung-snapdragon-850-pc; Chuong Nguyen, Google prepares an always-connected Chromebook to take on Microsoft (5.6.2018) ניתן לצפייה באתר: https://finance.yahoo.com/news/google-prepares-always-connected-chromebook-221400906.html?guccounter=1; Devindra Hardawa, Intel and Sprint team up to sell 5G PCs in 2019 (6.5.2018) ניתן לצפייה באתר: https://www.engadget.com/2018/06/05/intel-sprint-5g-pcs/.

13 התנהלות המכונה BYOD (Bring Your Own Device) – ראו James Careless, Establishing a Realistic BYOD Governance Policy (31.12.2012), ניתן לצפייה באתר: http://www.kmworld.com/Articles/Editorial/Features/Establishing-a-realistic-BYOD-governance-policy-86784.aspx.

מבחינת אבטחת סייבר, ויש בכך כדי להעמיד בסיכון לא רק מידע אישי של בעל המכשיר או המשתמש בו, אלא גם מידע ארגוני ועסקי וכן משתמשים אחרים ברשת שאליה הוא מחובר.

בספרות יש עיסוק באבטחת סייבר באופן כללי ובאבטחת סייבר בתשתיות קריטיות,[14] והרגולציה הקיימת מתמקדת באבטחת סייבר של תשתיות אלה ושל ארגונים. עם זאת, טרם הוקדש דיון מעמיק לשאלת הרגולציה של אבטחת סייבר במגזר האזרחי־הפרטי בכלל ובציוד קצה בפרט, ומכאן חשיבותו של מאמר זה.

היעדר אבטחת סייבר או אבטחת סייבר לקויה בציוד קצה (לעיל, **בעיית האבטחה**), דורשים מענה במטרה למנוע את התוצאות וההחצנות השליליות של בעיית האבטחה. לאור ניתוח הגורמים לבעיית האבטחה והכשלים שעומדים ביסודה, נטען במאמר כי אי־אפשר לסמוך על המשתמש, הבעלים של ציוד הקצה או המחזיק שלו, שיהיה הגורם העומד בפרץ ואחראי על וידוא קיומה של אבטחת סייבר בציוד הקצה והיותה מעודכנת. מדובר במשימה מתמשכת, יום־יומית, הדורשת לעיתים מודעות ומיומנות או הבנה טכנולוגית שאינן קיימות בהכרח אצל צרכנים ומשתמשים רבים.

עניין זה מתקשר להיבט רחב יותר של שתי מגמות שכבר מתחוללות וצפויות להתגבר, אשר ניתן להמשיג אותן דרך בעיית האבטחה: האחת היא המעבר ממוצרים לשירותים, והאחרת – הכמות והמגוון של ציוד הקצה שקיים, ועוד צפוי להיות קיים, עם הרחבת יישום האינטרנט של הדברים (IoT). כך למשל, צרכנים כבר כמעט אינם רוכשים תקליטורים של מוזיקה או סרטים אלא צורכים שירותי תוכן,[15] מגמה שקיימת גם בשוק התוכנה ואף צפויה להתרחב לשוק הרכב והתחבורה החכמה.[16] ביחס לציוד קצה, צרכנים כבר אינם הבעלים של הממירים של ספקי שירותי הטלוויזיה והווידיאו על פי דרישה ואף לא של נתבי xDSL, אלא מקבלים את המכשירים הללו מספקי השירותים כחלק מהשירות ורק כל עוד השירות עצמו נצרך. עם התרחבות תופעת ה־IoT אפשר לצפות להימצאותם של מכשירים רבים שהם בגדר ציוד קצה, בלא שלצרכן או למשתמש

---

14 לדיון נרחב בסוגיית אבטחת סייבר בתשתיות קריטיות, ראו אלדר הבר וטל ז׳רסקי ״דרכי הגנה על תשתיות חיוניות במרחב הסייבר בישראל״ **משפט וממשל** יח 100 (2017) (להלן: **הבר וז׳רסקי**).

15 באמצעות אפליקציות של תחנות רדיו או הוט למשל, או אפליקציות של שירותים כגון Spotify ו־Netflix.

16 שירותי SaaS (Software as a Service) ושירותי ענן הם כבר שירותים נפוצים, ובתחום התחבורה החכמה אף מדובר על CaaS (Car as a Service) ועל MaaS (Mobility as a Service) ראו: Riasanow, Tobias; Galic, Gabriela; and Böhm, Markus, "Digital Transformation in the Automotive Industry: Towards A Generic Value Network" (2017), *In Proceedings of the 25th European Conference on Information Systems (ECIS)*, p. 3191 (Research-in-Progress) ניתן לצפייה ב: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1065&context=ecis2017_rip.

הסופי יש בעלות בהם או שליטה עליהם. הטלפון החכם הוא לאמיתו של דבר שילוב של בעלות ושירות, אך גם בו הדגש הוא בשירותים ובהתכנים ופחות בבעלות במוצר.[17]

בהתאם לכך, מאמר זה מבקש לבחון את הצורך וההצדקות לאסדרה של אבטחת סייבר בציוד קצה, דהיינו לבחון אם על המדינה להתערב, באמצעות הרגולטור הרלוונטי, על מנת להבטיח את קיומה של אבטחת סייבר בציוד מסוג זה, מיהם הרגולטורים הרלוונטיים, מהו סוג האסדרה הנדרש, אם בכלל, מהן ההצדקות ומהו המסד משפטי לביסוס התערבות רגולטורית כזו.

הפרק הראשון במאמר עוסק בכמה הגדרות וטקסונומיות של ציוד קצה ושל אבטחת סייבר, תוך התמקדות בדין הישראלי. בהמשכו, הפרק מתאר את בעיית האבטחה (כאמור הבעיה של היעדר אבטחת סייבר בציוד קצה או היותה לקויה), ההשלכות והתוצאות האפשריות וההחצנות השליליות הנובעות מבעיה זו. מכאן המאמר פונה, בפרק השני שלו, לדיון במקורות, בכשלים ובגורמים האפשריים לבעיה. בפרק השלישי נדונים דרכי התמודדות והפתרונות האפשריים לבעיית האבטחה מכוחן של דיסציפילנות משפטיות שונות, כגון דיני נזיקין, דיני הגנת הפרטיות ודיני הגנת הצרכן. הפרק הרביעי עוסק ברגולציה ובפתרונות רגולטוריים לבעיית האבטחה, לרבות בשיטות אסדרה הנהוגות כיום בתחום של אבטחת הסייבר והטלפונים החכמים.

הפרק החמישי והאחרון במאמר מכיל סיכום קצר של המסקנות ביחס לדרכי ההתמודדות האפשריות.

למאמר זה עשויה להיות חשיבות נוספת בעת הזו, נוכח העובדה שהצעת חוק הסייבר, שאמור לכלול בתוכו פרק של רגולציה, קורמת עור וגידים ונמצאת בשלב התזכיר.[18] הטיפול בסיכוני הסייבר היה עד כה בידי רגולטורים מגזריים. כעת הוא אמור להיות מתוכלל על ידי גורם מרכזי – מערך הסייבר הלאומי (בהתאם לכך, פורסמה הגרסה הראשונה של תורת ההגנה בסייבר לארגון,[19] שבה יש התייחסות מסוימת לציוד קצה). החשיבות בעת הזו מתחזקת גם נוכח היעד ששם לעצמו משרד התקשורת לשנים

---

17 כך למשל מי שרוכש טלפון של אפל או טלפון אנדרואיד לא יכול להתקין עליו מערכת הפעלה אחרת וחברות הטלפונים מציעות מכשירים חדשים עם תוכנות שמעבירות את כל האפליקציות המותקנות מהטלפון הישן (גם אם הוא של יצרן אחר) לטלפון החדש כמו גם את כל התכנים שהיו בטלפון הישן. ראו Samsung Smart Switch, ניתן לצפייה באתר: http://www.samsung.com/il/support/smart-switch.

18 לעיל, הערה 1. יצוין כי על פי ספר תכניות העבודה של משרדי הממשלה לשנים 2017–2018 (בעמ׳ 504), הצעת חוק הסייבר הייתה אמורה להיות מונחת על שולחן הכנסת בשנת 2017. בינתיים פורסם כאמור תזכיר חוק הסייבר.

19 משרד ראש הממשלה מערך הסייבר הלאומי, **תורת ההגנה בסייבר לארגון גרסה 1.0** (אפריל 2018) (להלן: **תורת ההגנה בסייבר לארגון**). ניתן לצפייה באתר: https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_418_A4.pdf.

2017–2018 תחת הכותרת ״התאמת הרגולציה על שוק הטלקום בישראל לעידן המודרני״, וכן ״כתיבת מסמכי הסדרה בנושא הגנת הסייבר״.[20]

א. אבטחת סייבר בציוד קצה

בפרק זה מובאת תחילה סקירה כללית של ההיקף הנרחב (ההולך וגדל) של מתקפות סייבר והסיכונים הכרוכים בהן. לאחר מכן אתמקד בציוד קצה – תחילה בהגדרת ציוד קצה ותיאור המסגרת הנורמטיבית החלה עליו, ובסיום הפרק בקונקרטיזציה של בעיית אבטחת סייבר בציוד קצה, ההיבטים הייחודיים, ההשלכות של כשלים באבטחה והחצנות שליליות הנובעות מכשלים אלה.

בפרק הבא אדון במקורות לכשלי האבטחה בציוד קצה ובסיבות לקיומם של הכשלים הללו. כל אלה ישמשו יסוד לדיון בפתרונות ובכלים המשפטיים האפשריים לצורך מתן מענה לבעיית האבטחה, ובכללם אסדרה של אבטחת סייבר בציוד קצה.

1. מרחב הסייבר, מתקפות סייבר והסיכונים הכרוכים בהן

מתקפות סייבר ומתקפות על מערכות מחשוב דרך האינטרנט אינן דבר חדש, וכבר בשנת 1988 גרמה ״תולעת״ אינטרנט (the "Morris Worm") להאטה וקריסה של מערכות מחשוב מרכזיות ותחנות עבודה שהיו מחוברות לרשת.[21] עם זאת, בשל ההתפתחויות הטכנולוגיות מרחיקות הלכת שחלו מאז, הן רשת האינטרנט והן הציוד המחובר אליה התרחבו והפכו חלק בלתי נפרד מההתנהלות היום־יומית ומהחיים המודרניים. לא פעם מאוחסן בציוד כזה מידע אישי ועסקי רב, או ניתן להגיע באמצעותו לאחסון בענן או ברשת ביתית או ארגונית, כמו גם למשתמשים אחרים ולציוד המחוברים לאותה רשת.

נוכח עובדות אלו ונוכח מתקפות סייבר בהיקפים הולכים וגדלים (מצד גורמים פרטיים ומדינתיים), התחכום המתגבר של המתקפות,[22] הנזקים הכלכליים שהן גורמות ויתרה מכך – הנזקים הפוטנציאליים שלהן, הפכה אבטחת הסייבר לסוגיה מרכזית ורבת משקל בסדר היום של מדינת ישראל כמו גם של מדינות אחרות ברחבי העולם.

מרחב הסייבר מעלה סוגיות ואתגרים יחודיים בכל הנוגע להגנה עליו, בין היתר בשל היכולת של תוקף לפעול מרחוק מכל מקום בעולם, הקשר בין מרחב הסייבר למערכות

---

20 לעיל, הערה 2.
21 לעיל, הערה 4.
22 לעיל, הערה 6.

בעולם הפיזי (כגון ציוד קצה) והקשיים להפחית את פגיעותן של מערכות ורשתות סייבר מורכבות ואת ההשלכות של פגיעה כתוצאה של מתקפה.[23]

בארצות הברית העידו מנהל המודיעין הלאומי (Director of National Intelligence)[24] ומנהל ה־FBI בפני הקונגרס כי מתקפות סייבר הן האיום החמור ביותר על הביטחון הלאומי שחווה ארצות הברית.[25] ממשלת ישראל הכירה, כאמור לעיל, באיום הממשי של מתקפות סייבר הן על תשתיותיה ועל המגזר הציבור והן על המגזר האזרחי, הכרה שמצאה ביטוי בכמה החלטות שמטרתן קידום היכולת הלאומית במרחב הסייבר והגנת הסייבר.[26]

כדי לדון בהיקף של מתקפות סייבר יש להגדיר תחילה את מרחב הסייבר, שבו מתרחשות מתקפות אלה. ממשלת ישראל, במסגרת החלטותיה בנושא, הגדירה את מרחב הסייבר (ה״מרחב הקיברנטי״), כדלקמן:[27]

> המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה.

הגדרה זו היא הגדרה רחבה ביותר. על פי לשונה, ובניגוד לתפיסה הרווחת של המונח ״התקפת סייבר״, האינטרנט (המרשתת), אף שהוא מרחב הכלול בהגדרה, אינו הכרחי לקיומו של מרחב הסייבר. יוצא מכך שגם מתקפה באמצעות התקן נייד כמו זיכרון USB (דיסק־און־קי) על מערכת ממוחשבת המנותקת מהאינטרנט[28] היא מתקפה במרחב הסייבר, כהגדרתו על ידי ממשלת ישראל. יתרה מכך, ההגדרה רחבה גם בכך שהיא כוללת את המטה־דאטה **(״נתוני תעבורה ובקרה״)**,[29] וגם את המשתמשים (ראו דיון על

---

23 Department of Homeland Security, Cybersecurity Overview, ניתן צפייה באתר: https://www.dhs.gov/cybersecurity-overview.

24 לעיל, הערה 7.

25 לעיל, הערה 8.

26 לעיל, הערה 9.

27 החלטה 3611, הגדרת ה״מרחב הקיברנטי״.

28 כמו למשל המתקפה הידועה כתולעת Stuxnet, שחיבלה בשנת 2011 בתכנית הגרעין האיראנית וככל הנראה הוחדרה לכור הגרעיני באיראן באמצעות התקן USB נייד. ראו: Stuxnet, New Jersey Cybersecurity and Communications Integration Cell (10.8.2018) ניתן לצפייה באתר: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet.

29 ראו הגדרת ״נתוני התעבורה״ בסעיף 1 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס״ח–2007, ס״ח 2122, וכן הגדרת ״מתקן בזק״ (שם), הכוללת בתוכה גם ״ציוד קצה״. בעוד החוק הנ״ל מגדיר ״נתוני תקשורת״ ככאלה הכוללים גם ״נתוני מנוי״ ו״נתוני מיקום״ כהגדרתם בסעיף 1 לחוק, הרי שהלשון שנוקטת החלטה 3611 היא ״נתוני תעבורה ובקרה״. לא ברור מלשונה של הגדרה זו מהי התחולה של המונח ״נתוני בקרה״.

כך בהמשך המאמר). החלטה 3611 הגדירה גם את המונח אבטחת סייבר (״ביטחון קיברנטי״):[30]

> מדיניות, מנגנוני אבטחה, פעולות, הנחיות, ניהול סיכונים וכלים טכנולוגיים, שנועדו להגן על המרחב הקיברנטי ושנועדו לאפשר פעולה בו.

לשם השוואה, לפי הגדרת אבטחת סייבר של הממשלה הבריטית, שבה מוטמעת גם הגדרת מרחב הסייבר, משמעותה של אבטחה זו היא הגנה על מערכות מידע (חומרה, תוכנה והתשתית הכרוכה בהם), המידע המצוי בהן והשירותים שהן נותנות, מפני גישה בלתי מורשית, נזק או שימוש לרעה.[31] גם הגדרה זו רחבה ואינה דורשת חיבוריות לאינטרנט דווקא, אך אינה כוללת בתוך המרחב המוגן את המשתמשים.

היה אפשר לחשוב שבתוספת של הגנה על משתמשים בהגדרה הישראלית יש ממד ונדבך נוספים של הגנה, בכך שהיא כוללת לא רק הגנה מפני אובדן המידע או השחתתו, אלא גם מפני שימוש במידע הפוגע במשתמשים של מערכות המחשוב, שהם בעלי המידע (כגון הפצת מידע מביך במרשתת או שימוש בסיסמאות ושמות משתמש). ואולם, מבחינת הדברים אפשר להסיק שגם ההגדרה הבריטית כוללת בחובה הגנה מפני מקרים כגון אלה, בלא שהיא כוללת את המשתמשים, שכן יש בה, לפי לשונה, הגנה על שימוש לרעה במידע. כך גם באשר להבטחת קבלת שירותים ממערכות ממחושבות. בעוד בהגדרה הישראלית הם באים לידי ביטוי באמצעות הפגיעה במשתמשים, בהגדרה הבריטית הם מוטמעים בלשונה בלא צורך להוסיף את המשתמשים.

לא ברור למה כיוונה הממשלה בהוספה גם את המשתמשים להגדרה של מרחב הסייבר. יש להניח שאין כוונה להגנה פיזית על המשתמשים, אלא להגנה על המידע שלהם, על האינטרסים שלהם, על זכויותיהם ועל שירותים שהם מקבלים, העשויים להיפגע כתוצאה של מתקפה על מערכות מחשוב ורשתות תקשורת, כפי שהדבר בא לידי ביטוי בהגדרה הבריטית. אם כן, מחד גיסא, אין כל רבותא לעניין ההגנה בהוספת המשתמשים להגדרה הישראלית של מרחב הסייבר, אך מאידך גיסא היא מאפשרת החלה של כל האמצעים הכלולים בהגדרה זו גם על המשתמשים. הנפקות של עניין זה

---

30 לעיל, הערה 27, שם, הגדרת ״ביטחון קיברנטי״. לצורך הדיון, ההתייחסות למושג זה ולמושג אבטחת סייבר היא זהה.

31 HM Government, *National Cyber Security Strategy 2016-2021* הגדרת Cybersecurity בסעיף 2.11 בעמ׳ 15 – התרגום הוא של המחבר – במקור: "the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse" ניתן לצפייה באתר: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (נצפה לאחרונה במאי 2018).

והשלכותיה האפשריות של אסדרה על זכויות המשתמשים יידונו בהמשך המאמר, בפרקים הדנים באמצעים והכלים המשפטיים ובדרכי ההתמודדות האפשריות עם בעיית האבטחה.[32]

לעניין זה יש משמעות גם בהתייחס ל״נתוני תעבורה״, הכלולים אף הם בהגדרה הישראלית של מרחב הסייבר.[33] נתונים כמו יעד התקשורת, שעת התקשורת, משך התקשורת, גודל התקשורת או נפחה עשויים להיות מידע רב ערך לתוקפים שמבקשים לאסוף מידע לצורך כלשהו על היעד המותקף.

יש לציין שגם בהמלצות של איגוד התקשורת הבין־לאומי משנת 2008, ההגדרה של מרחב הסייבר או סביבת הסייבר (Cyber environmet) כוללת את המשתמשים.[34]

בהקשר של מתקפות סייבר, סיבוני ואסף[35] מחלקים את מרחב הסייבר לתתי־מרחבים לפי מניעי הפעולה – תת־המרחב הביטחוני, שהמניע העיקרי לפעולה בו הוא פוליטי־ביטחוני, ותת־המרחב הפלילי־אזרחי, שבו ארגוני פשע ופושעים בודדים מבצעים תקיפות למטרות כלכליות או למטרות נקם. אף כי מכשירי קצה יכולים כמובן לשמש גם גורמים ביטחוניים, יעסוק מאמר זה בתת־המרחב הפלילי־אזרחי בלבד.

סיבוני וסביליה מונים סיבות מספר לפגיעות של מרחב הסייבר:[36]

א. האסימטריה הקיימת בין העלות של יצירת מתקפה לעלות ההגנה מפני מכלול שלם של מתקפות;

ב. הישענות מרחב הסייבר על פרוטוקולי תקשורת מיושנים, שאינם נותנים מענה לסוגיית הפגיעות של המרחב ואף מאפשרים לפעול בו בצורה אנונימית;

ג. העובדה שמרחב הסייבר מאפשר ניצול של חולשות תוכנה וחומרה, הקיימות בשפע, כמו גם הזמינות של כלי התקיפה והיכולת לעשות שימוש חוזר בכלי תקיפה שהופעל בהצלחה;

ד. הקושי בגיבושו של שיתוף פעולה קולקטיבי לשם התגוננות ממתקפות סייבר, בשל שיתוף מידע חלקי בין גופים אזרחיים לבין עצמם ובין גופים אזרחיים לגופים ביטחוניים;

ה. אי־תמרוץ כלכלי וחוסר בכלים טכנולוגיים לפיתוח הגנה נאותה.

---

32 להלן, פרק ג ופרק ד.

33 לעיל, הערה 27.

34 ההגדרה בסעיף 3.2.4 היא כדלקמן: “**cyber environment**: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks”. ניתן לצפייה באתר: Recommendations ITU-T X.1205: Overview of Cybersecurity (4/2008), https://www.itu.int/rec/T-REC-X.1205-200804-I.

35 גבי סיבוני ועופר אסף, ״קוים מנחים לאסטרטגיה לאומית במרחב הסייבר״, **המכון למחקרי ביטחון** לאומי (2015), בעמ׳ 14.

36 **סיבוני וסביליה**, לעיל הערה 5.

מתקפות הסייבר לובשות צורה חדשה חדשות לבקרים, ופירוט כל סוגי המתקפות חורג מהיקפו של מאמר זה. עם זאת, חשוב לציין שהמגמה של יישום ה־IoT וחיבור של ציוד קצה נטול אבטחת סייבר לאינטרנט, מביאים לעלייה ניכרת במתקפות הרותמות ציוד קצה באמצעות נוזקה ועושות בו שימוש כרשת של בסיסים להוצאת מתקפות DDoS או RDoS.[37]

כלים שונים למתקפות סייבר הפכו זמינים לציבור הרחב ולא רק למדינות, ארגוני פשע והרשת האפלה ("Dark Web"), באופן שמאפשר גם לגורמים שאינם ״מתוחכמים״ להוציא לפועל מתקפות סייבר.

בפרסום של ה־US-CERT (United States Computer Emergency Readiness Team)[38] מחודש אוקטובר 2018[39] מפורטים כלי מתקפה כאלה. מדובר בפרסום בעקבות מחקר משותף, שערכו רשויות הגנת הסייבר בארצות הברית, אוסטרליה, קנדה, ניו זילנד ובריטניה. הכלים המפורטים בפרסום (Remote Access Trojan (RAT): JBiFrost, Webshell: China Chopper ,Credential Stealer: Mimikatz ,Lateral Movement Framework: PowerShell Empire ו־ C2 Obfuscation and Exfiltration: HUC Packet

---

37 RDoS – Ransom Denial of Service: מתקפת כופר שלפיה נשלחים איום ודרישת כופר כדי למנוע את השלב הבא, שהוא מתקפת DDoS (Distributed Denial of Service), מתקפה שבה התוקף מייצר תעבורת אינטרנט פיקטיבית בקצב ובכמות שגורמים לקריסה של האתר או השרת המותקפים או במטרה לגנוב מידע. תעבורה כזו נוצרת בדרך כלל באמצעות botnet – רשת של מחשבים או ציוד קצה המחוברים לאינטרנט, שעליהם מותקנת תוכנה המאפשרת את הפעלתם יחדיו לצורך ביצוע משימה, שלעיתים היא חוקית לחלוטין ודרושה לשם הפעלה תקינה של שירותי אינטרנט. בהקשר של מתקפות סייבר, הכוונה לרשת כזו שעל רכיביה מותקנת נוזקה העושה בהם שימוש לצורך שילוח מתקפות סייבר. ראו הסבר באתר חברת נורטון, ניתן לצפייה באתר: https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html. גם לסוג זה של מתקפת סייבר (DDoS) צורות אפשריות רבות – ראו פירוט באתר חברת CORERO, ניתן לצפייה באתר: https://www.corero.com/resources/glossary.html. לפי דוח של אותה חברה מנובמבר 2017, ההערכה הייתה שבאותה עת כמיליון מכשירי IoT היו בתהליך ״גיוס״ לבוטנט, שקיבלה את הכינוי "Reaper", בשל פגיעות בקוד שלהם וניצול חולשות אבטחה ידועות, ושחל גידול של 91% במספר המתקפות שחווים ארגונים ברבעון השלישי של 2017 ביחס לרבעון הראשון של אותה שנה, גידול המיוחס למגמה של יישום IoT (*Corero DDoS Trends Report, Q2-Q3 2017*). על פי אתר TechRepublic ניתן כיום לרכוש ״שירות״ של מתקפת DDoS בעלות של פחות מ־100$. ניתן לצפייה באתר: https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot.

38 ה־US-CERT הוא חלק מה־NCCCIC (National Cybersecurity and Communications Integration Center) האמריקאי, שמטרתו להקטין את הסיכונים המערכתיים הנובעים מאתגרי סייבר ותקשורת, כל זאת במסגרת במילוי תפקידיו כגוף הגנת הסייבר הלאומי, הנותן מענה לאירועי סייבר ומרכז מידע ומומחיות טכנית בתחום. ראו US-CERT, About Us, ניתן לצפייה באתר: https://www.us-cert.gov/about-us.

39 US-CERT, Alert (AA18-284A), Publicly Available Tools Seen in Cyber Incidents Worldwide, ניתן לצפייה באתר: https://www.us-cert.gov/ncas/alerts/AA18-284A.

Transmitter) מיועדים לשימושים שונים בידי התוקף – להתקנת קודים על פלטפורמת היעד כדי להקנות לתוקף גישה מרחוק ברמת מנהל הפלטפורמה (administrive control), לאסוף נתוני משתמש (שמות וסיסמאות) כדי לתת לתוקף גישה וכניסה לפלטפורמות, לאפשר התקדמות בתוך הרשת לאחר החדירה אליה ולמסך את זהות התוקף באמצעות התערבות והכוונה מחדש של התקשורת הממוחשבת, כך שלא ניתן יהיה לזהות מהיכן הגיעה המתקפה.

מבלי להקדים את המאוחר, יצוין כי הפרסום הנ״ל הוא נדבך נוסף בגישה הנוהגת בתחום הגנת הסייבר שלא על תשתיות חיוניות, בישראל כמו גם במדינות אחרות, דהיינו גישה של פרסום והנגשה של מידע והמלצות על הפעולות שיש לנקוט, בעיקר בארגונים, בלא כפייה או חיוב בדין לנקוט אמצעי כלשהו. הפרסום האמור מתאר כל אחד מהכלים, את מהות השימוש בו, יכולותיו, דוגמאות לשימוש בו, ולבסוף – האופן שבו אפשר לאתר שימוש בו ולהגן מפניו, הכול בגדר המלצה לא מחייבת.

יש לציין שהתוצאות של מתקפות סייבר יכולות להיות הרות אסון, הן ברמה הפיזית והן בנזק שנגרם לארגונים החשופים להם. כך לדוגמה, חברה הולנדית (DigiNotar) שעסקה בהנפקת אישורים דיגטליים[40] גילתה בחודש יוני 2011 שהיא הייתה מושא למתקפת סייבר (באופן שהתוקפים הנפיקו אישורים מזויפים), והגיעה בעקבות המתקפה ותוצאותיה למצב של חדלות פירעון שישה חודשים לאחר מכן.[41]

סיבוני וסביליה מציינים ש״חוסנו של המגזר הפרטי במרחב הסייבר קשור ישירות לביטחון הלאומי״.[42] עם זאת, גם חיבורם המקיף עוסק ברגולציה של גופי ביטחון, משרדי ממשלה, תשתיות קריטיות והמגזר הפרטי־העסקי, בניגוד ליחידים במגזר הפרטי, שהם המשתמשים בציוד הקצה, ורגולציה במגזרים האחרים אינה חלה עליהם.

כפי שאראה להלן, בפרק הדן בבעיית האבטחה בטלפון החכם (לאחר סקירה של המסגרת הנורמטיבית החלה על ציוד קצה), הטלפון החכם, בין השאר בשל היותו נפוץ

---

40 אחד השימושים הנפוצים של האישורים הללו הוא בפרוטוקול האינטרנטי המאובטח HTTPS, שבו התקשורת בין הדפדפן לאתר האינטרנט מוצפנת ונעשה שימוש במפתח ציבורי ומפתח פרטי. האישור הוא לבעלות במפתח הציבורי שנשלח לדפדפן על מנת שהתקשורת תוצפן באמצעותו, בעוד האתר יפענח אותה באמצעות המפתח הפרטי המתאים, המצוי רק בידו. אם האישור מזויף, המשמעות היא שאתר מתחזה מציג את עצמו כאתר הלגטימי, וכל משמעות הצפנת הנתונים, שנועדה למנוע התערבות במידע והגעתו ליעדים אחרים, מאבדת מערכה. מנפיק האישורים הינו צד שלישי, שהצדדים האחרים בוטחים בו וסומכים עליו ועל אמיתות האישורים שהוא מנפיק. לכן כל פגיעה באמינותו ובאמינות האישורים מביאה לכך שהדפדפנים יחסמו את האישורים של אותו מנפיק ולא יאפשרו שימוש בהם.

41 ערך DigiNotar בוויקיפדיה, ניתן לצפייה באתר: https://en.wikipedia.org/wiki/DigiNotar, וראו Microsoft Security Advisory 2607712 (29.8.2011), ניתן לצפייה באתר: Microsoft Security Advisory 2607712.

42 לעיל, **סיבוני וסביליה**, הערה 5, בעמ׳ 9.

כל כך ובשל השימוש הנרחב בו, הוא יעד למתקפות סייבר שעשויות להתחולל בערוצים שונים.

2. ציוד קצה והמסגרת הנורמטיבית החלה עליו

כדי לבחון את הסוגיה של אבטחת סייבר בציוד קצה, יש להבין תחילה מהו ציוד קצה ומהי המסגרת הנורמטיבית שחלה עליו. לאחר מכן יבוא דיון בבעיית האבטחה (קונקרטיזציה של אבטחת סייבר לציוד קצה) ובהחצנות השליליות שלה.

״ציוד קצה״ מוגדר בסעיף 1 לחוק התקשורת באופן הבא:

> ציוד בזק, לשימושו של מנוי, המתחבר או המיועד להתחבר מחצריו של המנוי או מכל מקום אחר לרשת בזק ציבורית באמצעות המישק המיועד לכך, לרבות ציוד רדיו טלפון נייד, מפענח או ממיר אפיקים ולרבות כל התקן אחר המותקן בחצרי המנוי והמיועד לשמש לקליטת שידורים בחצריו וכן ציוד קצה לווייני כהגדרתו בסעיף 6מג.

המונחים ״בזק״, ״רשת בזק ציבורית״ ו״מישק״ מוגדרים אף הם בסעיף 1 לחוק התקשורת, ובשל הצורך להבין את ההגדרה של ציוד קצה, שכוללת מונחים בלתי ברורים אלה, תובאנה הגדרותיהם כלשונן בחוק, כדלקמן:

״בזק״:

> שידור, העברה או קליטה של סימנים, אותות, כתב, צורות חזותיות, קולות או מידע, באמצעות תיל, אלחוט, מערכת אופטית או מערכות אלקטרומגנטיות אחרות;

״רשת בזק ציבורית״:

> מערכת של מיתקני בזק, המשמשת או המיועדת לשמש לאספקת שירותי בזק לכלל הציבור בכל הארץ או לפחות באזור שירות, הכוללת ציוד מיתוג וניתוב, ציוד תמסורת ורשת גישה, לרבות מערכת רדיו טלפון נייד ומערכת בזק בין־לאומית, ולמעט ציוד קצה.[43]

״מישק״:

> המפגש הפיזי בין יחידות בזק תפקודיות שונות לרבות באמצעי אופטי או אלחוט.

---

43 ״**אזור שירות**׳ – תחום גאוגרפי שבו חייב בעל רישיון כללי, על פי רישיונו, להקים, לקיים או להפעיל רשת בזק ציבורית ולספק באמצעותה שירותי בזק לכלל הציבור״ (סעיף 1 לחוק התקשורת).

משילוב ההגדרות הללו עולה כי ציוד קצה הינו מכשיר המשמש מנוי להתחבר לרשת ציבורית, בין שמדובר בחיבור חוטי (כגון נתב ביתי המתחבר לשקע טלפון של בזק בטכנולוגית xDSL, או נתב כזה המתחבר לרשת הכבלים), חיבור אלחוטי (כגון הטלפון החכם המחובר לרשת הסלולרית או מקלט לשידורי לווין) או חיבור אופטי (כגון נתב המתחבר לרשת סיבים אופטיים המגיעים עד הבית).

בפסק דין **ענק הבטיחות**[44] קבע בית המשפט העליון כי ״מבחינה לשונית, עולה מן ההגדרה כי ציוד קצה הוא ציוד ׳המיועד לשמש לקליטת שידורים׳. הדגש מושם אפוא בפעולת הקליטה״, וכן שמדובר בהתקן המצוי בקצה התשדורת ולא במהלכה. מטעם זה נקבע שם כי מגבר סלולרי, לדוגמה, אינו בגדר ציוד קצה, שכן הוא התקן ש״אינו מצוי ב׳קצה׳ התשדורת, אלא במהלכה של השרשרת המובילה מן הפלט אל הקלט״.[45]

עם זאת, ברור שההגדרה בחוק, שמקורה בתיקון מס׳ 5 לחוק הבזק משנת 1988,[46] לאחר שעברה שני תיקונים נוספים בשנים 2000 ו־2001,[47] אינה שוללת אפשרות שציוד הקצה גם משדר לרשת הציבורית ואינו רק קולט מידע ממנה. כאמור, בית המשפט העליון הגדיר בפסק הדין הנ״ל את הטלפון החכם כציוד הקצה ה״אולטימטיבי״, והדגש הושם בהיותו של הציוד ב״קצה״ הרשת, בלא לעסוק בסוגיה שהוא גם משדר ולא רק קולט.[48]

לסיכום, מההגדרה ומהפרשנות שניתנה לה עולה שמדובר במגוון של התקנים שמאפשרים חיבוריות לרשת ציבורית, לרבות חיבור לאינטרנט באמצעות מגוון הרשתות הציבוריות והטכנולוגיות הקיימות (על גבי קווי הטלפון, רשת הכבלים, הרשת הסלולרית וכו׳). עם זאת, כאמור לעיל, מפאת חשיבותו והדומיננטיות שלו בחיים הדיגיטליים המודרניים, הדגש במאמר זה הוא בטלפון החכם.

יצוין שההגדרה של ציוד קצה בחוק הישראלי דומה להגדרתו בדירקטיבה האירופאית בנושא ציוד רדיו וציוד מסוף בתקשורת והכרה ההדדית בתאימות שלהם, משנת 1999.[49] ציוד קצה מכונה שם ״ציוד מסוף תקשורת״ (telecommunications

---

44 לעיל, הערה 11, בעמ׳ 9.

45 שם.

46 חוק הבזק (תיקון מס׳ 5), תשמ״ח–1988, ס״ח 1260.

47 חוק ההסדרים במשק מדינת ישראל (תיקוני חקיקה להשגת יעדי התקציב והמדיניות הכלכלית לשנת התקציב 2000), תש״ס–2000, ס״ח 1724, בעמ׳ 21, וחוק הבזק (תיקון מס׳ 25), תשס״א–2001, ס״ח 1807.

48 פסק דין **ענק הבטיחות**, לעיל הערה 11. ההגדרה בסעיף 1 לחוק התקשורת, כמו גם פסק הדין, אינם עוסקת כאמור ביכולת ציוד הקצה – האלמנט הקולט – להיות גם בעל יכולת לשדר חזרה לרשת הבזק הציבורית, כמו במקרה של הטלפון הסלולארי, המוזכר במפרש בהגדרה (״רדיו טלפון נייד״).

49 Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999, on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

terminal equipment), וגם שם מדובר בכל התקן שמאפשר תקשורת ונועד להיות מחובר לרשת תקשורת ציבורית.[50]

מעבר לחשיבותו והדומיננטיות שלו בחיים הדיגיטליים המודרניים כאמור לעיל, הדגש בעבודה זו הוא בטלפון החכם גם מהטעם שבחינת מצבה של אבטחת הסייבר בטלפון החכם, ממשיגה את סוגיית האבטחה ואת חשיבותה בעידן ה־IoT.

3. אסדרה של ציוד קצה בישראל – ״אישור סוג״

ההגדרה של ציוד קצה הוכנסה לראשונה לחוק התקשורת במסגרת שינוי חקיקה שנועד להתמודד עם הפרעות לרשת הבזק הציבורית – אז בעיקר רשת הטלפוניה הקווית – באמצעות ציוד שחובר אליה ולא היה מותאם למערכת הבזק בישראל. הדבר נועד למנוע נזק לרשת ולמנויים האחרים, ״המתבטא, בין השאר, בחיוג מוטעה ובעומס על הרשת״.[51] מכוח התפיסה של צורך להבטיח שציוד הקצה הוא ״תקני״ הוכנס לחוק באותו תיקון גם המונח ״אישור סוג״.[52] מדובר באישור שנותן משרד התקשורת לציוד קצה והדרוש גם לשם יבוא ציוד כזה לארץ, כדי לאפשר חיבור של ציוד קצה תקני ומתאים לרשת, בלא לחייב כל מי שמחזיק בציוד מאותו סוג להגיש בקשה ולהצטייד ברישיון לפי החוק.[53]

עד שנת 2012 נדרש לקבל ממשרד התקשורת רישיון סחר ואישור סוג על מנת לייבא ציוד קצה לישראל ולסחור בו. באותה שנה הוציא שר התקשורת צו,[54] שנועד להקל יבוא של ציוד קצה סלולרי (טלפונים, טאבלטים בעלי קישוריות סלולריות ונתבים ומודמים סלולריים). בצו נקבעו כמה תנאים לפטור של ציוד קצה סלולרי מאישור סוג.[55] בין

---

50 שם, ההגדרה ב־Article 2(b).

51 הצעת חוק הבזק (תיקון מס׳ 5), תשמ״ז–1987, ה״ח 1822. ראו דברי ההסבר לסעיף מס׳ 1.

52 אישור סוג מוגדר בסעיף 1 לחוק התקשורת כדלקמן: ״אישור שניתן לפי חוק זה לדגם של ציוד קצה לשם חיבורו לרשת הבזק של בעל רשיון כללי לרבות אישור כאמור המעיד על כך שציוד הקצה שלגביו ניתן האישור תואם במאפייניו העיקריים דגם של ציוד קצה שלגביו ניתן אישור סוג קודם״. לפי סעיפים 4א–4ג לפקודת הטלגרף האלחוטי [נוסח חדש], תשל״ב–1972, דמ״י 25, קיימת חובת קבלת רישיון לשם ייצור מכשיר אלחוטי, החזקתו, הפעלתו או התקנתו, וחובה זו מותנית, בין היתר, בקיומו של אישור סוג.

53 לעיל, הערה 51, בדברי ההסבר לסעיפים 2 ו־3. ציוד שטרם קיבל אישור סוג לא יחובר לרשת בטרם קיבל אישור כאמור ממעבדה שהוסמכה לכך (סעיף 4א(ב) לחוק התקשורת), וחובת הרישוי, לעיל הערה 52.

54 צו התקשורת (בזק ושידורים) (פטור מרישוי לציוד קצה הפועל בשיטה התאית (רט״ן)), תשע״ב–2012, ק״ת 7159 (להלן: **צו 2012**). הצו הותקן בהתאם להוראות סעיף 4א(ד3) לחוק התקשורת, הקובע כי ״ציוד קצה שהוא ציוד רדיו טלפון נייד, העומד בתנאים שקבע השר בצו, אינו טעון אישור סוג; השר רשאי לקבוע בצו תנאים למתן פטור מאישור סוג לסוגים מסוימים נוספים של ציוד קצה, כפי שיקבע״.

55 שם, בסעיף 2.

היתר, ציוד הקצה הסלולרי נדרש לקיים דרישות של דירקטיבה של האיחוד האירופאי,[56] על דרך של הפניה אליה והצהרה על עמידה בדרישותיה.[57] בשנת 2014 הותקן צו פטור נוסף,[58] אשר חל על סוגים שונים של ציוד קצה, למעט ציוד קצה סלולרי. גם צו 2014 דורש עמידה בדרישות מסוימות, הקבועות בתקינה אירופאית או אמריקאית, על דרך של הפניה והצהרה. בדרך זו יכול משרד התקשורת, ובפועל כך הוא עושה, לדרוש שציוד קצה המיובא לישראל והמופץ בישראל יעמוד בתקינה עולמית קיימת, במקום להעמיד דרישות תקינה חדשות. ההנחה היא שהיצרנים הגדולים, וגם אחרים, ממילא עומדים בתקינה זו, שכן השווקים המרכזיים שלהם הם באותן מדינות שבהן היא חלה.

עולה מכל האמור שאישור סוג או הפטור ממנו, תוך התניה בעמידה בתקינה זרה, הוא אמצעי שבידי שר התקשורת להכפפת ציוד הקצה לרגולציה שמפורטת בצווים שהוא מוציא תחת ידו. אמצעי זה יכול להיות מסגרת פוטנציאלית להחלת דרישות מחייבות על ציוד קצה בתחום הגנת הסייבר, דהיינו לרגולציה של הגנת סייבר בציוד קצה. ואולם, זאת אפשרות אחת מבין אפשרויות מספר, כפי שעולה מהדיון בפרקים העוסקים בדרכי התמודדות עם הסוגיה.[59]

4. מעמדו המרכזי של הטלפון החכם בחיים הדיגיטליים, האיומים וההחצנות השליליות של בעיית האבטחה

עמדתי על כך שמתקפות סייבר הן בעיה בהיקף נרחב, שאינה ייחודית לציוד קצה. עם זאת, לציוד קצה שהוא טלפון חכם יש מאפיינים ייחודיים, שבגללם הוא חשוף למתקפות מסוגים שונים אשר בחלקן ייחודיות לו. ואולם, רובו של דיון זה עוסק בטכנולוגיה ומובא בפרק הבא.

---

56 Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. ניתנת לצפייה באתר: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999L0005. יש לציין שבשנת 2014 בוטלה הדירקטיבה הנ״ל והוחלפה בדירקטיבה חדשה, אך צו 2012 נותר על כנו בלא שההפניה תוקנה. הדירקטיבה החדשה היא: Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC. ניתנת לצפייה באתר: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053.

57 על סמך הצהרת מי שביקש לייבא את הציוד לארץ ולסחור בו היה מונפק ״אישור פטור״, שנדרש לשם שחרור הציוד מהמכס.

58 צו התקשורת (בזק ושידורים) (פטור מאישור סוג לציוד קצה), תשע״ד–2014, ק״ת 7423 (להלן: **צו 2014**).

59 להלן, פרק ג ופרק ד של מאמר זה.

פרק זה דן במעמדו המיוחד של הטלפון החכם בחיים הדיגיטליים המודרניים ובסיכונים וההחצנות השליליות של מצב שבו אבטחת הסייבר בטלפון החכם לקויה.

הטלפון החכם, מכשיר המצוי כיום בליבת המערכת האקולוגית של טכנולוגיית המידע ואשר אנשים פרטיים וגופים עסקיים מסתמכים עליו ועל פעולתו התקינה, הוא גם תשתית אזרחית חיונית בשעה של אסון טבע, פעולות איבה ומלחמה.[60] פגיעה מכוונת בתשתית הזו באמצעות מתקפת סייבר עשויה להעצים את הכאוס בעיתות כאלה ואף להחריף את הפגיעה שהן גורמות. בעוד ספקי התשתית הסלולרית יכולים להיערך למקרה שבו נגרמים נזקים לתשתית עצמה כתוצאה של אסון טבע או אירוע חירום אחר,[61] הפגיעה באמצעות מתקפת סייבר במכשירים עצמם בעת משבר עשויה להשאיר את הציבור ואת גורמי ההצלה בלא יכולת לתקשר. מתקפת סייבר דרך ציוד הקצה עשויה להביא אף לפגיעה בתשתית עצמה ולגרום לנזק רחב היקף, מעבר לנזק הפרטני למידע האגור בציוד הקצה, להשבתתו או לניצולו לרעה לשם הפצה במשתמשים אחרים. בישראל, ספקי התשתית הסלולרית מנויים בתוספת השנייה ובתוספת הרביעית לחוק להסדרת הביטחון בגופים ציבוריים, תשנ״ח–1998, והם מנויים גם בתוספת השנייה של אותו חוק (להלן: **חוק הביטחון**). יוצא מכך שעל פי הוראות חוק הביטחון, המדינה יכולה לחייב את ספקי התשתית הסלולרית, שהם גופים פרטיים, להקים ולנהל מערך אבטחה לשמירה על תשתית זו, הן בהיבט של אבטחה פיזית והן בהיבט של אבטחת מערכות המידע,[62] או להכפיף אותן למנגנון אבטחה חיצוני.[63]

התשתית הסלולרית היא רק דרך חיבוריות אחת של הטלפון החכם לרשתות תקשורת. הטלפון החכם הפך להיות מרכז החיים הדיגיטליים של משתמשים רבים, תפקיד שבעבר הלא רחוק מילא המחשב האישי. בית המשפט העליון הכיר בחשיבותו הרבה של המחשב האישי המחזיק מידע אישי ועסקי רב ובהיותו ״חלק בלתי נפרד, ומהותי ביותר, ממרקם החיים האנושי המודרני״.[64] הדברים הללו יפים ביתר שאת לטלפון החכם,

---

60 תקשורת היא אחת התשתיות הקריטיות לפי הגדרת ה־PCCIP (President's Commission on Critical Infrastructure Protection) האמריקאי – ראו: Eun Ho Oh, Abhijeet Deshmukh & Makarnd Hastak, "Disaster Impact Analysis Based on Inter-Relationship of Critical Infrastructure and Associated Industries", *International Journal of Disaster*, 1 (2010).

61 Gerard O'Reilly, Ahmad Jrad, Ramesh Nagarajan, Theresa Brown & Stephen Conrad, "Critical Infrastructure Analysis of Telecom for Natural Disasters", *IEEE Netowrks 2006, 12th Intenational Telecommunications Netwrok Strategy and Planing Symposium* (2006).

62 הגדרת ״פעולות אבטחה״ בסעיף 1 לחוק הביטחון.

63 במקרה של ספקי תשתית הסלולר – נציג השב״כ (סעיף קטן 2(ב)(1) להגדרת ״קצין מוסמך״ בסעיף 1 לחוק הביטחון). לדיון נרחב בסוגיית אבטחת סייבר של תשתיות חיוניות ותחולת החוק, ראו **הבר וז׳רסקי**, לעיל, הערה 13.

64 רע״פ 8464/14 **מדינת ישראל נ׳ ניר עזרא** (פורסם בנבו, 2015), בעמ׳ 7.

שבנוגע אליו יש לעיתים תחושה שהוא אף הפך חלק בלתי נפרד מהמשתמשים עצמם ולא רק ממרקם חייהם. רבים משתמשים בו לאורך שעות רבות במהלך היממה (לא בפונקציונליות שלו כטלפון), באופן שאפילו יצרני המכשירים, כמו Apple למשל, מקיימים שיח על דרכים להפחתת השימוש הזה.[65]

הוזלת המכשירים בשל כניסת שחקנים חדשים לשוק, כגון חברת Xiaomi הסינית ואחרים, הביאו לגידול ניכר בכמות הטלפונים החכמים, שהפכו להיות הפלטפורמה העיקרית לגלישה באינטרנט. כבר ב־2015 דווח ש־68% מהמבוגרים בארצות הברית היו בעלי טלפון חכם,[66] מספר שעלה ל־77% ב־2017, ובגילאים 18–29 מספר בעלי טלפון חכם עומד כבר על 92%.[67] הטלפון החכם גורם גם לשינויים חברתיים וצמצום פערים דיגיטליים,[68] ואף מהטעם הזה הוא בעל מעמד מרכזי בחייהם של רבים. השימושים בטלפון החכם שונים ומגוונים – קבלת התראות על חדשות, חיפוש עבודה, מציאת בני זוג, קריאת ספרים דיגיטליים, פלטפורמה ל־e-commerce ולביצוע רכישות ועסקאות ברשת ועוד. עובדה זו הופכת את הטלפון לחלק בלתי נפרד מהחיים המודרניים של כל אדם ולא רק של גיקים ומומחי טכנולוגיה.[69]

מכשיר הטלפון החכם אינו נופל מהמחשב האישי, ובימינו אף עולה עליו, בכל הקשור ליכולות החישוב שלו וכמות המידע האישי והעסקי האגור בו או שאפשר להגיע אליו באמצעותו. עם התפתחותה הבלתי פוסקת של הטכנולוגיה, הוא מציע שירותים ויכולות נוספים. בסוף 2017 דווח כי כ־46% מהמבוגרים בארצות הברית עושים שימוש בעוזרים וירטואליים המופעלים על ידי קול, בעיקר באמצעות הטלפונים החכמים שלהם.[70] הטכנולוגיה של ״בינה מלאכותית״ (AI) מביאה לכך שיכולותיו שמוקנות של

---

65 ראו: Rory Cellan-Jones, Tech Tent – Glued to our phones (8.6.2018), על כך שנושא זה היה בין הנושאים שדובר עליהם בנאום הפתיחה המרכזי של כנס המפתחים העולמי של אפל ביוני 2018. ניתן לצפייה באתר: https://www.bbc.com/news/technology-44412033

66 Pew Research Center, Technology Device Ownership: 2015 (29.10/2015), ניתן לצפייה באתר: http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015.

67 Pew Research Center, 10 facts about smartphones as the iPhone turns 10 (28.6.2017), ניתן לצפייה באתר: http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones.

68 כך לדוגמה הוא מסייע לשחורים והיספנים לצמצם את הפער הדיגיטלי שהיה קיים בשל כך שבעלי המחשבים הניידים בקהילות הללו היה נמוך בהשוואה לקהילת הלבנים. Pew Research Center, Smartphones help blacks, Hispanics bridge some – but not all – digital gaps with whites (31.8.2017), ניתן לצפייה באתר: http://www.pewresearch.org/fact-tank/2017/08/31/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/.

69 לעיל, הערה 66.

70 Pew Research Center, Nearly half of Americans use digital voice assistants, mostly on their smartphones (12.12.2017), ניתן לצפייה באתר: http://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/.

הטלפון החכם, כיום ובעתיד, הן מגוונות וכוללות, למשל, גם מה שהיה נראה כמדע בדיוני לפני שנים לא רבות – שיחות טלפון שמבוצעות על ידי הטלפון עצמו, בלי התערבות יד אנוש, עבור בעל הטלפון.[71] כמו כן, ״מחשוב ענן״ מאפשר לקבל באמצעות הטלפון החכם עוצמת מחשוב של חוות שרתים ושטח אחסון מידע שהוא כמעט בלתי מוגבל.

עם זאת, קלות החדירה לטלפון החכם באמצעים טכנולוגיים הופכת אותו לנקודת חולשה שתוקפים יכולים לנצל לשם השתלטות על המכשיר, הגעה לאותו מידע רצוי, חדירה לרשתות שהוא מחובר אליהן והפעלת מגוון היכולות שלו באופן שמשרת את התוקף. כל אלה מתאפשרים בעוד האמצעים הננקטים על ידי בעלי המכשירים לוקים בחסר. כך למשל, מסקר משנת 2016 עולה כי כשליש מבעלי המכשירים אפילו לא נועלים אותם למניעת גישה פיזית לא מורשית.[72] מגוון אפשרויות החיבור האלחוטיות של הטלפון החכם, היותו מחובר באופן קבוע לאינטרנט באמצעות רשת בזק ציבורית (הרשת הסלולרית), היותו מחובר לרשת ביתית או ארגונית באמצעות חיבור WiFi והיכולת להתחבר אליו גם באמצעות Bluetooth, כל אלה הופכות את הטלפון החכם לגורם סיכון משמעותי לניצול פרצות באבטחת סייבר או חוסר מוחלט של אבטחת סייבר, גם לאחרים המחוברים לאותם רשתות.

הסיכון הנובע מבעיית האבטחה אינו מתמצה בפגיעה במידע האגור בטלפון החכם או בנטילתו, אלא בפגיעה רחבה הרבה יותר – חדירה דרכו גם לרשת הארגונית שאליה הוא מחובר באמצעות WiFi, חדירה למידע השמור בענן והפעלת הטלפון החכם לשירות התוקף, לעיתים באופן שבו ייראה כאילו בעל המכשיר הוא שביצע את הפעולה (בין שמדובר בשיחה ובין שמדובר במשלוח הודעה) לשם גנבת זהות ודיוג של מידע רגיש. בעוד מערכת המחשוב בארגון מנוהלת ונשלטת על ידי הארגון, התחברות באמצעות מכשיר נייד שאינו תחת ניהולו של מנהל הרשת עשויה להביא לכך שבשל אי־מוגנותו

---

71 מנכ״ל גוגל חשף בחודש מאי 2018 בכנס I/O 2018 יכולת נוספת ל״עוזר הוירטואלי״ שלה, תחת השם Duplex. המשמעות של המונח Duplex בתקשורת הוא יכולת תקשורת דו כיוונית בין שתי נקודות קצה. בכנס הושמעה שיחת טלפון שערך העוזר הוירטואלי עם מספרה, בשיחה שנשמעה רגילה לחלוטין ובלא שלבן האנוש בצד השני של הקו היה מושג שהשיחה מבוצעת על ידי עוזר וירטואלי. ראו: Chris Welch, Google just gave a stunning demo of Assistant making an actual phone call (8.5.2018), ניתן לצפייה באתר: https://www.theverge.com/2018/5/8/17332070/google-assistant-makes-phone-call-demo-duplex-io-2018. ניתן להקשיב לשיחה הנ״ל וכן לשיחה של Duplex עם מסעדה ולדוגמאות נוספות, בבלוג של גוגל בנושא בינה מלאכותית. Yaniv Leviathan, 7.9.32 Google Duplex: An AI System for Accomplishing Real- World Tasks Over the Phone (8.5.2018), ניתן לצפייה באתר: https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html.

72 לעיל, הערה 67.

של המכשיר הנייד והיותו נקודת חולשה תיגרם פגיעה לרשת כולה, למאגרי המידע הארגוניים ולמשתמשים אחרים המחוברים אליה.

בדוח משולב על מצבן של מתקפות הסייבר בשנת 2016 והתחזיות לשנת 2017, שפרסמה חברת אבטחת המידע קספרסקי (Kaspersky),[73] מתוארת שורה של מתקפות ואיומי סייבר שהתגלו בשנת 2016 בטלפונים ניידים, לרבות סוסים טרויאנים ונוזקות (Malware), דהיינו תוכנות זדוניות המותקנות בו באופן לא רצוני או לא מכוון מבחינת המשתמש, שהופיעו כאפליקציות תמימות ב־Google Play. חלק מהמתקפות הצליחו להתגבר על תכונות אבטחה שהוספו בגרסאות מתקדמות של Android (מערכת ההפעלה של הטלפון). איום נוסף שהלך והתגבר ב־2016 היו מתקפות על ידי נוזקות כופר (Ransomware), כולל כאלה שמתקינות קוד פתיחה חדש לטלפון, שאינו מאפשר למשתמש לעשות שימוש במכשיר.

בתחזית איומי הסייבר לשנת 2017 מתוארת בדוח קספרסקי שורה ארוכה של איומי סייבר שצפויה הייתה להתרחש בשנת 2017. מצוין בדוח כי בעוד המתקפות על טלפונים סלולריים עד אותה עת היו בעיקרן ״משלימות״ למתקפות על מחשבים ומבוססות על כלים בהתאם, הרי שיש צפי לעלייה ניכרת של מתקפות ריגול ממוקדות טלפונים סלולריים. הדבר נובע הן מהעובדה שהחיים הדיגיטליים של המשתמשים עוברים מהמחשב האישי לטלפון החכם, והן מחוסר תשומת לב לסוגיית האבטחה בהם, אי־עדכון של מערכות ההפעלה על ידי המשתמשים והקושי להשיג כלים לניתוח פורנזי של מערכות ההפעלה שלהם.[74] ואכן, בסקירה של מעבדות קספרסקי מחודש מרץ 2018 נמצא שבשנת 2017 התגלו בתחום המובייל כ־6 מיליון חבילות התקנה פוגעניות, כ־95 אלף סוסים טרויאנים לגנבת מידע בנקאי וכ־545 אלף סוסים טרויאנים של מתקפות כופר.[75]

בסקירה של חברת צ׳קפוינט, בדוח המגמות של מתקפות סייבר לאמצע שנת 2018,[76] מתוארת מגמה מרכזית שנצפתה בשנה זו, והיא מתקפות לצורך ניצול כוח המחשוב של הפלטפורמה המותקפת לכריית מטבעות קריפטוגרפיים ולשימושים אחרים בתחום הקריפטו. הדבר מתבצע בדרכים שונות, כגון על ידי התקנת נוזקה שמתחזה לאפליקציה לגיטימית בטלפון ומשתמשת בכוח המחשוב שלו לפעולות כרייה של מטבעות וירטואליים, בדרך של מודעות המפתות התקנה של תוכנת הכרייה אגב הבטחות שווא לתגמול למתקין, ונוזקות שעושות דיוג של פרטי הכניסה לארנקים הקריפטוגרפיים של

---

73 Kaspersky Security Bulletin (2016). ניתן לצפייה באתר: https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf.

74 שם, בעמ׳ 9 ובעמ׳ 66.

75 Roman Unuchek, Mobile malware evolution 2017 (7.3.2017), ניתן לצפייה באתר: https://securelist.com/mobile-malware-review-2017/84139.

76 Checkpoint's Cyber Atatck Trends – 2018 Mid-Year Report, ניתן לצפייה באתר: https://pages.checkpoint.com/cyber-attack-2018-mid-year-report.html.

המשתמשים, המותקנים על המכשיר הנייד. על פי פרסום באתר Techcrunch, אפליקציה שהתחזתה לתת שירות של של ארנק בשם MyEtherWallet.com, אחד מהארנקים הפופולריים ביותר לאחסון המטבע הוירטואלי Ether ומטבעות אחרים, הצליחה לא רק להיכנס לתוך ה־AppStore של אפל, אלא אף הגיעה לראש טבלת ההורדות. לאחר דיווחים של משתמשים על האפליקציה היא הוסרה על ידי אפל.[77]

על פי מסמך המלצות של איגוד התקשורת הבין־לאומי, מידע מסקרים שערכו ארגונים ברחבי העולם מלמד כי בעוד נוזקות שנועדו ליצור botnets[78] יועדו בעבר לתקוף מחשבים אישיים ורשתות מחשבים, הן מועתקות במהירות לשם מתקפות מסוג זה על טלפונים חכמים, והאיום הולך וגדל במהירות ברחבי העולם.[79] הסיבה לכך היא השימוש הנרחב בטלפונים חכמים והגלישה המרובה באינטרנט.

גם אם בית המשפט העליון הישראלי רואה כאמור בטלפון הנייד את ציוד הקצה ה״אולטימטיבי״, הרי שיש דוגמאות נוספות לציוד קצה שעשוי להיות מושא לרגולציה של אבטחת סייבר. עם אלה נמנים נתבים (ראוטרים), המתחברים מצד אחד לרשת בזק ציבורית (רשת סלולרית או רשת הטלפוניה באמצעות xDSL או רשת הכבלים), ומצד אחר מאפשרים חיבוריות לאינטרנט על ידי קישוריות אלחוטית באמצעות Wi-Fi או חיבור חוטי (Ethernet). גם נתבים כאלה הם נקודת תורפה משמעותית מבחינת אבטחת סייבר ויכולת של תוקפים לחדור דרכם לרשתות ארגוניות וביתיות,[80] ותוקפים אכן מנצלים חולשות באבטחת סייבר של נתבים לשם חדירה לרשתות וביצוע מתקפות

---

77 Brian Heater and Jon Russel, Apple let a knockoff version of one of the world's biggest crypto wallets into the App Store (11.12.2017) (נצפה לאחרונה באוקטובר 2018): https://techcrunch.com/2017/12/11/apple-knockoff-myetherwallet-ios.

78 קבוצת מכשירים המחוברים לאינטרנט (מחשבים, טלפונים חכמים, מצלמות וכו׳), שנוצרה על ידי הידבקות בנוזקה אשר הופכת אותם לרשת בידי תוקף כדי לבצע באמצעות כוח המחשוב שלהם והקישוריות האינטרנטית שלהם, מתקפות סייבר.

79 Recommendation ITU-T X.1213: Security capability requirements for countering smarthphone-based botnet (09/2017), ניתן לצפייה באתר: https://www.itu.int/rec/T-REC-X.1213-201709-I.

80 חברות המייצרות נתבים מפרסמות חדשות לבקרים הודעות על ליקויי אבטחה ותיקונים שלהם – לדוגמה הודעת חברת NetGear באשר לפגיעות של נתבים מתוצרתה. ראו: NETGEAR Product Vulnerability Advisory: Potential security issue associated with remote management (06/01/2017), ניתן לצפייה באתר: http://kb.netgear.com/29960/NETGEAR-Product-Vulnerability-Advisory-Potential-security-issue-associated-with-remote-management. ראו גם US-CERT, Security Tip (ST15-002), Home Network Security (23/05/2018), ניתן לצפייה באתר: https://www.us-cert.gov/ncas/tips/ST15-002. עוד ראו כתבה על נוזקה בשם VPNFilter, המיועדת לתקיפת נתבים בעלת יכולת להתגבר על ההצפנה המקובלת (SSL) ולהפוך את התקשורת ללא מוצפנת: Jon Fingas, Data-stealing router malware bypasses web encryption (06/06/2018), ניתן לצפייה באתר: https://www.engadget.com/2018/06/06/router-malware-bypasses-web-encryption.

באמצעותם, כפי שהיה בכמה מתקפות DDoS מאז ספטמבר 2016, באמצעות נוזקה הקרויה Mirai.[81] צעדי המנע שעליהם המליץ ה־CERT האמריקאי ביחס לאותה מתקפה מוטלים רובם ככולם על כתפי המשתמשים בציוד הקצה, כגון עדכון התוכנה והתקנת טלאי תוכנה (דהיינו קובץ התקנה לשם תיקון או מעקף של תקלה בתוכנה, הדורשת תיקון מיידי), ביטול הפונקציונליות של פרוטוקול ה־UPnP ועוד.[82] צעדים אלה הם בבחינת גזרות שהציבור אינו יכול לעמוד בהן. כפי שאראה בהמשך המאמר, להנחת העבודה שאבטחת סייבר בציוד קצה תוסדר על ידי המשתמשים אין אחיזה במציאות, והיא חושפת את אותם משתמשים, צדדים שלישיים ואת האינטרנט למתקפות סייבר ולנזקים.

להיותו של ציוד קצה נטול אבטחת סייבר או בעל אבטחת סייבר לוקה בחסר עשויות להיות החצנות שליליות. החצנה או השפעה חיצונית ״היא הפעולה של חברה או של יחיד המשפיעה על חברה או על יחיד אחרים שלא דרך השוק״.[83] ״החצנות שליליות, הן עלויות של פעולה או עסקה המוטלות על מי שאינם צדדים לעסקה, או אף על החברה כולה״.[84] זיהום אוויר וזיהום מים הן הדוגמאות הקלסיות להחצנות שליליות.[85]

ההחצנות הנובעות מהיעדר אבטחת סייבר עשויות להיות כבדות משקל ונוגעות הן לשוק הפרטי והן למגזר העסקי. כפי שיובהר להלן, הן צפויות להתעצם ולהחריף והן עשויות להצדיק את הסדרתה של סוגיית אבטחת הסייבר בציוד קצה בדרך של אסדרה.

ההחצנות הללו יכולות לבוא לידי ביטוי בנזקים ופגיעות בעולם הממשי בשל פעולות תקיפה, שיביאו, לדוגמה, להשתלטות מרחוק על רכב דרך אפליקציה המותקנת בטלפון החכם ושימוש ברכב למטרות טרור או לגרימת תאונות ונזקים פיזיים למטרות אחרות. יצרני רכב רבים מציעים כבר היום אפליקציות שמאפשרות פעולות שונות בכלי רכב המחוברים לאינטרנט, כמו פתיחה וסגירה של הרכב, דיאגנוסטיקה של הרכב, מציאת המיקום שלו ועוד.[86] מצד אחד מדובר באפליקציות שימושיות מאוד לבעלי הרכב, אך מן הצד האחר זהו פתח למתקפות סייבר מסוג חדש, דרך הטלפון החכם. בבדיקה שערכו

---

81 ראו לעיל, הערה 37, להסבר על מתקפת DDoS. פרטים על המתקפה באמצעות ניצול IoT ניתן למצוא באתר ה־CERT האמריקאי. ראו US-CERT, Alert (TA-16-288A), Heightened DDoS Threat Posed by Mirai and Other Botnets, ניתן לצפייה באתר: https://www.us-cert.gov/ncas/alerts/TA16-288A.

82 שם.

83 אבי שמחון, ״פרק א: הקדמה כללית״, **הגישה הכלכלית למשפט** (אוריאל פרוקצ׳יה עורך, תשע״ב) 39, בעמ׳ 49.

84 רונן אברהם, ״פרק יח: ביטוח״, **הגישה הכלכלית למשפט** (אוריאל פרוקצ׳יה עורך, תשע״ב) 925, בעמ׳ 974.

85 Scot N. Arnold, *Imposing Values: Liberalism and Regulation* (2009) p. 142.

86 Which car manufacturers offer connected smartphone apps? ניתן לצפייה באתר: https://www.cartelligent.com/blog/which-car-manufacturers-offer-connected-smartphone-apps.

מעבדות קספרסקי בשנת 2017 לשבע אפליקציות כאלה נמצאו בהן בעיות אבטחה, אף כי צוין שבאותה עת לא היה ידוע על קוד פוגעני שמיועד לאפליקציות מסוג זה. עם זאת גם צוין שקל מאוד לערוך שינויים בקוד פוגעני קיים כדי ליצור מתקפה על רכב מחובר.[87]

כמו כן, הבאת מכשירים ניידים פרטיים על ידי עובדים לתוך הרשת של מקום העבודה (BYOD – Bring Your Own Device) הפכה למציאות שגרתית בארגונים רבים,[88] וזאת לאור הפיכת הטלפון הנייד למכשיר שאינו מיועד רק לשיחות קול כמו בעבר, אלא כאמור לעיל, למכשיר שהוא חלק מהותי בחייו של אדם בעידן שאנו חיים בו. היעדר אבטחת סייבר בטלפון נייד יכול כמובן להביא לפגיעה בבעלים של המכשיר, אך אם הוא מחובר לרשת ארגונית, או אף בעצם חיבורו לרשת הסלולרית, מתקיימת החצנה שלילית; עשויה להיות לכך השפעה הרת אסון על הארגון ומשאביו, על משתמשים אחרים, על רשתות ומשאבים אחרים דרך משתמשים אחרים ואף על התשתית הסלולרית.

יתרה מכך, השימוש בטלפון החכם אינו מוגבל לטריטוריה מסוימת. בעת נסיעה למדינה אחרת, הטלפון החכם ממשיך למלא את ייעודו בעת שהוא מחובר לתשתיות התקשורת באותה מדינה. דיני התקשורת הבין־לאומית מסדירים את השימוש הזה, אך אין בנמצא הסדרה או אסדרה בין־לאומיות של אבטחת סייבר.[89] פייק וורל, במאמרם על רגולציה של מרחב הסייבר, מסבירים את הקושי להשיג אמנות בין־לאומיות בתחום אסדרת הסייבר בשל פערים במשטרי החקיקה והאכיפה בין מדינות.[90] המשמעות היא שההחצנות השליליות אינן מוגבלות גאורפית גם מהטעם של התניידות ציוד קצה בין מדינה למדינה.

נוכח ההחצנות השליליות של אבטחת סייבר לקויה או חוסר מוחלט באבטחת סייבר במכשירים שהם ציוד קצה, עולה השאלה שהיא מושא המאמר על היבטיה השונים – האם נדרשת רגולציה, שאינה קיימת כיום, אשר תבטיח קיום הגנת סייבר והאם היא תצליח לתת מענה לסוגיה – אם התשובה חיובית – מי הרגולטור שצריך לעסוק בכך? בבד בבד עימה תעלה השאלה אם הסוגיה יכולה להיות מוסדרת באמצעות כלים משפטיים אחרים, כגון עוולת הרשלנות ותביעות של גורמים פרטיים,[91] ואולי שילוב של

---

87 Mikhail Kuzin & Victor Chebyshev, Mobile apps and stealing a connected car (16.2.2017), ניתן לצפייה באתר: https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576.

88 לעיל, הערה 13.

89 ראו דבורה האוסן־כוריאל ״דיני הטלקומוניקציה הבינלאומית ודיני סייבר בינלאומיים״, **משפט בינלאומי** (רובי סיבל ויעל רונן עורכים, תשע״ו) בעמ׳ 615.

90 J. Feick & R. Werle, "Regulation of Cyberespace", *The Oxford Handbook of Regulation* (R. Baldwin, M. Cave & M. Lodge eds., 2010) 523, p. 541 (להלן: **פייק ו־וורל**).

91 ראו לדוגמה המקרה שנדון בפסק הדין *Remijas v. Neiman Group*, LCC, No. 14-3122, (7th Cir. 2015).

כלים משפטיים, הן רגולטוריים[92] והן אחרים. כפי שאראה להלן, בעיית האבטחה אכן קיימת בטלפונים חכמים, וביסודה כשלים מספר, שיתוארו בפרק הבא.

ג. קיומה של בעיית האבטחה – הכשלים והסיבות לקיומה

בפרק זה של המאמר אעמוד על הכשלים שעומדים ביסודה של בעיית האבטחה, תוך ניתוח הסיבות לקיומם. ניתוח זה חשוב לשם בחינת הפתרונות המשפטיים השונים הקיימים והתאמתם למתן מענה לכשלים הללו.

1. כשלים ביסוד בעיית האבטחה – מבוא

המתקפות על הטלפון החכם יכולות להתבצע בשורה של חזיתות לוגיות ופיזיות, כפי שמפורט בקטלוג האיומים על הטלפון החכם של ה־NIST,[93] ובין היתר בחזיתות הבאות:

1. חולשות ופגיעות באפליקציות: בקטגוריה הזו כלולות הן פגיעות של האפליקציות עצמן, גם אם הן לגיטימיות (לעיתים בתלות במערכת ההפעלה), והן התקנה תמימה של אפליקציות זדוניות;

2. פגיעות בשל אימות (Authentication) לא מאובטח דיו: אימות של המשתמש לשם שימוש במכשיר (לדוגמה, פריצה ב-Brute-force שניתנת לצמצום באמצעות pin code ארוך יותר וכדומה), אימות בשירות מרחוק שאליו נכנסים באמצעות הטלפון ואימות בעת התחברות לרשת;

3. פגיעות בשל מאפייני הרשת הסלולרית: כל מכשיר מתקשר עם תחנת הבסיס הקרובה אליו ברשת שאליה הוא מחובר והפרוטוקול שלה (רשת GSM, CDMA

---

92 מקרה רשת מלונות Windhem, שבו נקטה נציבות הסחר הפדרלית בארצות הברית, ה־FTC (Federal Trade Commission) הליכים נגד הרשת, בטענה שהיעדר הגנת סייבר כמקובל במגזר המלונאות הינו תחרות לא הוגנת (אף ששם היה מדובר באי־יישום הפרוטוקול הבסיסי לסליקת כרטיסי אשראי, פרוטוקול PCI-DSS). *Federal Trade Comission v. Wyndham Worldwide Corporation, et al.*, 2:13-CV-01887-ES-JAD (New Jersey, 2015), ניתן לצפייה באתר: https://www.ftc.gov/system/files/documents/cases/151209wyndhamstipulated.pdf.

93 NIST Mobile Threat Catalogue, ניתן לצפייה באתר: https://pages.nist.gov/mobile-threat-catalogue וכן: (DRAFT) NISTIR 8144, Assessing Threats to Mobile Devices & Infrastructure (September 2016), ניתן לצפייה באתר: https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf וכן Christopher Brown et al. *Assessing Threats to Mobile Devices & Infrastructure* (Draft) NIST (September 2016), ניתן לצפייה באתר: https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf.

וכדומה). חלק מהאיומים משותפים לכלל סוגי הרשתות, וחלקם ספציפיים לסוגי רשתות מסוימים. גם כאן יש כמה אפשרויות לפגיעות בתחומים מספר, שחלקם נוגעים למכשירים וחלקם לתחנות הבסיס עצמן ולרשת, כגון האזנה לתקשורת בין הטלפון לתחנת הבסיס, מתקפות באמצעות תחנות בסיס זדוניות[94] ועוד.

4. פגיעות באחסון וגיבוי חיצוני: כולל חדירה למידע מהטלפון המגובה על מחשב פגיע ופגיעות באחסון המבוצע בענן על ידי אפליקציות;

5. חולשות במערכות החומרה והתוכנה של הטלפון: כולל במערכת ההפעלה, בדרייברים (התוכנה שמתפעלת חומרה כמו המצלמה), בתוכנה שמעלה את מערכת ההפעלה (Boot Firmware) ועוד.

6. פגיעות כתוצאה מחיבור המכשיר למחשב או למטען באמצעות חיבור USB.

חלק מהאיומים שפורטו לעיל קשורים בכשלים בפרוטוקול התקשורת הסלולרי או בתוכנה/חומרה של המכשירים, שלמשתמש אין כל יכולת השפעה עליהם. הכשלים העיקריים באבטחת סייבר של טלפונים חכמים, אשר תלויים במשתמש, עשויים להיות נעוצים בגורמים רבים ושונים, ובין היתר באלה:

1. אחוז נמוך של התקנות אמצעים לאבטחת סייבר בטלפונים חכמים;

2. אי־ביצוע עדכונים וטלאים (Patches) במערכות ההפעלה ובאפליקציות של הטלפונים;

3. התקנת אפליקציות זדוניות בחנויות האפליקציות, שמותקנות בתמימות על ידי משתמשים, ופגיעות באפליקציות לגיטימיות;

4. לחיצה על קישורים זדוניים המגיעים במגוון של אפשרויות (בדואר אלקטרוני, רשתות חברתיות, SMS ו־MMS);

5. פגיעות בשל גישה לטלפון באמצעות כמה ממשקי קישוריות אלחוטית, שחלקם פועלים באופן קבוע;

6. אי־קבלת תמיכה שוטפת ממערך ה־IT בארגונים גם במקרה של שייכות לארגונים;

7. חשיפה למתקפות חומרה בשל פגיעות פיזית מוגברת;

8. חולשות בפרוטוקול הסלולרי;

9. הגורם האנושי.

הדיון הפרטני להלן בכל אחד מהכשלים הללו נועד לאפשר התקדמות לשלב הבא, אשר דן בסיבות ובגורמים לכשלים אלה. הדבר יאפשר לבחון את האמצעים המשפטיים שעשויים לתת מענה לאותם כשלים ובכך גם לבעיית האבטחה.

---

94 מדובר במיקרו־תחנת בסיס שאפשר לרכוש במרשתת או אף לבנות בצורה עצמאית: How to Build Your Own Rogue GSM BTS for Fun and Profit (31.3.2016), ניתן לצפייה באתר: https://www.evilsocket.net/2016/03/31/how-to-build-your-own-rogue-gsm-bts-for-fun-and-profit.

2. כשלים ביסוד בעיית האבטחה – דיון פרטני

(א) אחוז התקנה נמוך של אמצעי אבטחת סייבר

ממחקר של קספרסקי שפורסם בחודש אוקטובר 2016, אשר נערך בקרב כ־12,000 משיבים מ־21 מדינות, נמצא כי רק כ־53% מבעלי טלפון חכם התקינו עליו אמצעי אבטחת סייבר.[95] אף כי אין נתונים עדכניים, אפשר להניח שכיום המצב דומה. בחינה של עשר תוכנות ההגנה המובילות ב־2018 לאנדרואיד, לפי אתר TechRadar,[96] מעלה נתונים כדלקמן:[97]

שם התוכנה	מספר הורדות (מיליון)
Avast Mobile Security	100
Bitdefender Antivirus Free	1
AVL	0.1
McAfee Security & Power Booster Free	10
Kaspersky Mobile Antivirus	50
Sophos Free Antivirus and Security	1
Norton Security and Antivirus	10
Trend Micro Mobile Security Antivirus	1
AhnLan V3 Mobile Security	5
Avira Antivirus Security	10

95 Only half of the World's Mobile Devices Are Protected from Cybercrime, According to a Kaspersky Lab Study (26.10.2016), ניתן לצפייה באתר: https://www.kaspersky.com/about/press-releases/2016_only-half-of-the-worlds-mobile-devices-are-protected-from-cybercrime.

96 Nate Draek, The best Android antivirus in 2018, ניתן לצפייה באתר: https://www.techradar.com/news/best-security-apps-and-antivirus-for-android.

97 בדיקה שערך הכותב ב־Google Play ביום 20.5.2018.

התוצאות שמודגמות בטבלה לעיל אינן שונות גם בנוגע לתוכנות הגנה אחרות, כגון MalwareBytes (10 מיליון הורדות בלבד). אין כמובן לדעת אם הורדה משמעה בהכרח גם התקנה וכן אם התקנה נשארת פעילה גם בחלוף תקופת הניסיון ללא תשלום (בחלק מהתוכנות) או בכלל, ולפיכך מספר המכשירים שמותקנת בהם תוכנת הגנה פעילה עשוי אף להיות נמוך יותר. כך או כך, מדובר במספר כולל שהוא בטל בשישים ביחס לכמות הטלפונים בשוק – לפי הכרזה של מנכ״ל גוגל, כבר בשנת 2017, עבר מספר מכשירי האנדרואיד הפעילים בחודש את ה־2 מיליארד![98]

אם כן, כשל ראשון ומשמעותי הגורם לקיום בעיית האבטחה הוא שיעור נמוך ביותר של התקנת תוכנות הגנה בטלפונים החכמים.

הסיבות לכשל הזה יכולות להיות נעוצות במספר גורמים אפשריים:[99]

1. חוסר מודעות של בעלי המכשירים לסיכוני הסייבר שהם חשופים אליהם במכשיר ללא תוכנת הגנה ואי־הערכה נכונה של הסיכונים הכרוכים בכך;[100]
2. קושי לבחור את התוכנה הרצויה מבין תוכנות ההגנה;
3. קושי להתקין את תוכנות ההגנה;
4. חששות מפני פגיעה בפרטיות – ייתכן שחלק מהמשתמשים חוששים שתוכנת ההגנה, אשר עשויה להזדקק לאישור הרשאה כ״משתמש־על״ (Superuser) בטלפון, חשופה לכל התכנים ועלולה בעצמה להיות מקור לפגיעה אפשרית בפרטיות;
5. אדישות – יש להניח שהסיבה העיקרית לכך היא אדישות, דהיינו ההתעלמות מהצורך לנקוט פעולה אקטיבית להתקנת תוכנת הגנה;
6. כמו כן, ייתכן שילוב של אדישות וחוסר מודעות.

בישראל, על פי פרסומים של חלק מהמפעילים הסלולריים, אפשר היה לחשוב שאין צורך בהתקנת תוכנת הגנה. אחדות מהחברות מפרסמות שהן נוקטות אבטחת סייבר רשתית ומציעות גם שירות הגנה למכשירים. כך למשל, חברת פלאפון מפרסמת את שירות ״פלאפון סייבר״, אשר לטענת החברה מספק ״מעטפת הגנה מתקדמת לגלישה בטוחה ברשת הסלולארית ובגלישת WiFi בארץ ובחו׳ל״.[101] השירות מוצע ברמת "BASIC" (״שירות אבטחה וסייבר רשתי המגן על לקוחות פלאפון בעת גלישה ברשת הסלולרית בארץ ובחו״ל. השירות ניתן ללא צורך בהתקנת אפליקציה וללא השפעה על זמן הסוללה וביצועי המכשיר״), וברמת "TOTAL" (״שירות אבטחה וסייבר עם

---

98 Ben Popper, Google announces over 2 billion monthly active devices on Android (17/05/2017), ניתן לצפייה באתר: https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users.

99 הואיל והמחקר שעליו מבוסס מאמר זה הוא מחקר עיוני, אין בידי המחבר תוצאות אמפיריות באשר לסיבות לכשלים.

100 לעיל, **פייק ו־וורל**, הערה 90, בעמ׳ 542.

101 פלאפון סייבר, שאלות ותשובות, ניתן לצפייה באתר: https://www.pelephone.co.il/digitalsite/heb/content-products/pelephonecyber.

אפליקציית Norton Mobile security שנותן לך הגנה גם בגלישת WiFi, ויכולות הגנה נוספות כמו התראות על אפליקציות זדוניות שמותקנות על המכשיר, איתור המכשיר במקרה של אובדן או גנבה ואפשרות לנעול ולמחוק את המכשיר מרחוק״). לפי האמור באתר של חברת פלאפון, שירות BASIC הוא שירות ״רשתי״; טיבו המדויק אינו ברור,[102] אך ברור שהוא אינו מספק הגנה על המכשיר בעת גלישה ב־WiFi או בעת חיבור המכשיר באמצעות ממשק אחר (בין שאלחוטי, כגון ה־Bluetooth, ובין שחוטי, כגון ה־USB). גם לא ברור אם ביכולתו לסנן תוכנות זדוניות בעת לחיצה על קישורים וכיוצא באלה (אין באתר פרטים). שירות TOTAL הוא שילוב של השירות הרשתי עם תוכנת הגנה של נורטון של חברת סימנטק, שיש להתקינה בטלפון. כל משתמש יכול להתקין את תוכנת ההגנה הזו (או אחרת) בעצמו בנפרד, בלא להכפיף את עצמו לתנאי השירות, תנאי השימוש ומדיניות הפרטיות של חברת פלאפון, ועל כן לא ברור מה התועלת בשירות הזה.[103] עיון בתנאי השירות של TOTAL מעלה כי הוא ״לא יסנן תכנים ׳נגועים׳ במקרה בו מכשירך הכיל וירוס/תוכנה זדונית/רוגלה וכדומה, טרם הפעלת השירות ו/או ככל שהועברו תכנים נגועים בווירוס למכשירך בערוצים אחרים, אך השירות ישלח התראה למכשירך״.[104] מדובר אפוא בשירות מוגבל ביותר, שלפי האמור לעיל אינו מבצע אפילו סריקה של הטלפון בעת ההתקנה (Scan) לסילוק תוכנות זדוניות שכבר נמצאות בו, כפי שמבצעות תוכנות הגנה אחרות, ואינו מגן מפני תוכנות זדוניות וחדירות דרך ממשקים אחרים מאשר הסלולרי וה־WiFi.

חברת סלקום מפרסמת את שירות ״סייבר 360״ לעסקים, שההגנה שלו, לפי הטענה, ״ממשיכה גם בסלולרי״ (מכונה ״סייבר מובייל״).[105] השירות הזה מיועד לעסקים ולא למנויים פרטיים, ואין באתר פירוט שאפשר ללמוד ממנו מהו היקף השירות שניתן ובמה בדיוק מדובר, פרט לאמירה הכללית שמדובר ב״שירות הגנה בזמן אמת לטלפונים חכמים מאיומי סייבר ידועים ולא ידועים שמטרתו למנוע גנבת מידע, חדירה לרשת הארגונית ומניעת שירות״.[106]

---

102 באתר חברת פלאפון אין פרטים על טיבו של השירות ומהות ההגנה הרשתית, וכל שניתן הוא לבדוק באמצעות קבלת מסרון אם הוא חל על מספר טלפון נייד, אך ברור שהתשובה חיובית אם המכשיר הוא ברשת פלאפון ושלילית אם לא.

103 השירות כפוף הן לתנאי השירות של חברת פלאפון והן לתנאי השירות של Norton Symantec. עמוד תנאי השירות, פלאפון סייבר, ניתן לצפייה באתר: http://www.pelephone.co.il/digital/corporate/tos.aspx?id=5871&appid=159, כמו גם למדיניות הפרטיות של חברת פלאפון. עמוד מדיניות ופרטיות של פלאפון, ניתן לצפייה באתר: https://www.pelephone.co.il/DigitalSite/heb/support/general_info/privacypolicy/.

104 תנאי השירות באתר חברת פלאפון, לעיל הערה 103.

105 סייבר 360 של חברת סלקום, ניתן לצפייה באתר: https://business.cellcom.co.il/cyber/home.

106 סייבר 360 של חברת סלקום, לוח מחוונים, ניתן לצפייה באתר: https://business.cellcom.co.il/cyber/demo.

גם חברת פרטנר מפרסמת את שירות CyberGuard, שהוא "שירות הגנה רישתי מפני אתרים זדוניים".[107] כמפורט בתנאי השירות,[108] מדובר על הגנה "בשימוש על גבי הרשת הסלולארית בלבד" (סעיף 3(א) לתנאי השירות), וכן ש"ככל שמכשירך הכיל וירוס/תוכנה זדונית/רוגלה וכיוצ"ב ('וירוס') טרם הפעלת השירות ו/או ככל שהועברו תכנים נגועים בוירוס למכשירך בערוצים אחרים (כגון, בעת העברת תכנים באמצעות חיבור התקן USB, Bluetooth וכדומה), השירות לא יסנן תכנים אלו" (סעיף 3(ג) לתנאי השירות). על כן גם כאן מדובר בהגנה חלקית בלבד ובלתי מספקת.

מכל האמור לעיל עולה כי שירותי אבטחת הסייבר שמציעות חברות הסלולר בישראל הם חלקיים בלבד, ואין בהם מענה מלא לבעיית האבטחה. העובדה שטלפון חכם אינו מגיע מצויד מראש באבטחת סייבר איננה נמנית כנראה עם הגורמים שמשפיעים על משתמשים בקשר להחלפת מותגים של טלפונים חכמים,[109] וגם עובדה זו יכולה להעיד על חוסר מודעות או אדישות של המשתמשים לצורך בהתקנת הגנת סייבר בטלפון החכם.

(ב) עדכונים וטלאים (Patches) במערכות ההפעלה ובאפליקציות

מערכת ההפעלה של הטלפון החכם היא התוכנה המותקנת עליו ומאפשרת את הפונקציונלית שלו בשילוב החומרה שלו. במקרה של אפל, היא הגורם שמייצר הן את מערכת ההפעלה והן את החומרה, דהיינו את המכשיר עצמו. לעומת זאת, מערכת ההפעלה אנדרואיד של חברת גוגל מותקנת על מגוון רחב של טלפונים ממגוון של יצרנים.

שתי מערכות ההפעלה הנפוצות בטלפונים החכמים הן כאמור Android של גוגל ו־iOS של חברת אפל. ב־2016 פורסם שסמסונג, יצרנית טלפונים חכמים מובילה, שוקלת לעשות שימוש במערכת הפעלה משל עצמה בשם Tizen,[110] אך למיטב ידיעת המחבר הדבר טרם קרה עד היום.

---

107 באתר חברת פרטנר (נצפה לאחרונה ב־26.5.2018): https://www.partner.co.il/-2/AppsPartner/CyberGuard.

108 תנאי השירות של CyberGuard של חברת פרטנר, ניתנים לצפייה באתר: https://www.partner.co.il/globalassets/documents/partnerdoc/pb5dev_19209.pdf.

109 כך מפני שאבטחת סייבר גם אינה תכונה שיצרנים עושים בה שימוש במסגרת התחרות בשוק. לגורמים להחלפת מותג ראו: Abhijeet Jain, Varsha Seshadri & Vidushi Changulani, "Anylysis of factors affecting Brand Switching in the Smartphone Industry", 3 *Imperial Journal of Interdisciplinary Research* (2017).

110 Samsung considers using Tizen in all products (13.6.2016), ניתן לצפייה באתר: http://www.koreatimes.co.kr/www/news/tech/2016/06/133_206894.html. מדובר במערכת הפעלה בקוד פתוח, שפותחה במיוחד לצורך שוק המובייל והמכשירים המחוברים, כפרויקט במסגרת ה־Linux Foundation. ראו Tizen – About, ניתן לצפייה באתר: https://www.tizen.org/about.

אף על פי שקיימות רק שתי מערכות הפעלה ולכאורה הדבר היה אמור להביא לכך שהעדכונים שלהן ייעשו בקלות ותוך זמן קצר מהיותם זמינים, הרי שהמצב בשטח מלמד על בעייתיות רבה ועל כך שמדובר בכשל שהוא גורם מרכזי לבעיית האבטחה. בפועל נעשות התאמות למערכות ההפעלה למכשירים השונים, והבעיה של עדכונים וטלאים למערכת ההפעלה מקבלת רמת סיבוכיות גבוהה באופן ניכר ביחס לקיומן של שתי מערכות הפעלה, אף בהתחשב בכך שלהן עצמן יש גרסאות שונות.

על פי דוח האיומים על טלפונים חכמים ל־Q2/2017 שפרסמה חברת האבטחה זימפריום, ב־94% ממכשירי האנדרואיד הותקנה גרסה ישנה משתי הגרסאות האחרונות של מערכת ההפעלה, ו־23% ממכשירי ה־iOS לא עודכנו במשך 45 ימים למרות קיומה של גרסה מעודכנת זמינה להתקנה.[111] על פי דוח האיומים של החברה ל־Q4/2017,[112] אפל עדכנה ברבעון הרביעי של 2017 ובשני החודשים הראשונים של 2018 את מערכת ההפעלה שלה עשר פעמים (!!!), כדי לפתור לא פחות מ־72 CVEs;[113] העדכון כלל תיקון לחולשה שאפשרה לתוקף דרך WiFi לבצע התקפת Krack,[114] וכן תיקון כנגד בעיית Meltdown & Spectre.[115] באותו דוח מצוין כי גוגל שחררה באותה תקופה חמישה עדכונים לאנדרואיד, ובסך הכול תוקנו 161 CVEs. מהדוח הנ״ל עולה החשיבות הרבה של עדכון מערכת ההפעלה והתקנת טלאים בהקדם האפשרי, ולעיתים בתכיפות ובתקופות זמן קצרות.

אלא שמתברר כי מצב העדכונים של מערכות ההפעלה רחוק מאוד מלהיות מספק. ה־FTC, נציבות הסחר הפדרלית בארצות הברית,[116] ערכה בשנת 2016 בדיקה של בעיית האבטחה בהקשר של עדכון מערכות ההפעלה בטלפונים חכמים, באמצעות צווים לקבל

---

111 Zimperium, Mobile Threat Data Q2 2017 (5.9.2017), ניתן לצפייה באתר: https://blog.zimperium.com/mobile-threat-data-q2-2017.

112 Zimperium, Global Threat Report Q4/2017, ניתן לצפייה באתר: https://get.zimperium.com/whitepaper_q4-2017-threat-report.

113 Common Vulnerabilities and Exposures – סדרת רשומות הכוללת מספר מזהה, תיאור ולפחות הפניה אחת לפרסום על פגיעות אבטחת סייבר ידועה. ראו באתר: https://cve.mitre.org.

114 KRACK – Key Reinstallation attaCK – חולשה בפרוטוקול ה־WPA2 שמאבטח את רשת ה־WiFi. לעיל, הערה 112 בעמ׳ 6.

115 ניצול חולשות קריטיות שנתגלו במעבדים ומאפשרת את גנבת המידע שהם מעבדים, כך שתוכנה זדונית יכולה לקרוא נתונים בזיכרון של תוכנה אחרת. השם Meltdown מקורו בכך שהנוזקה ממוסמת את גבולות ההגנה והבידוד בין יישומי המשתמש למערכת ההפעלה. לפי הדוח של מגלה הבעיה, כל המעבדים של אינטל משנת 1995 סובלים מהחולשה הזו, וכך גם מעבדים של ARM שמשמשים בטלפונים חכמים. לעיל, הערה 112 בעמ׳ 8.

116 Federal Trade Commission – נציבות הסחר הפדרלית שאחראית, בין היתר, על הגנה על צרכנים וסחר הוגן: https://www.ftc.gov (להלן ולעיל: **FTC**).

מידע שהופנו לשמונה יצרני טלפונים חכמים.[117] הדבר נעשה בעת ובעונה אחת עם פנייה של ה־FCC,[118] באמצעות צווים דומים שנשלחו לספקי השירות בעלי התשתיות וספקי שירות וירטואליים.[119] הממצאים שעלו מהתשובות לצווים והמסקנות רוכזו בדוח של ה־FTC שפורסם בפברואר 2018.[120]

מדוח ה־FTC עולה כי הזמן הממוצע לשחרור עדכונים של מערכות ההפעלה למשתמשים הוא ארוך, כ־18 חודשים בממוצע, לעומת מגמה של התארכות זמן ההחזקה במכשיר של כ־29 חודשים בממוצע. הדוח גם מגלה מצב של חוסר שקיפות מוחלט בנושא, בנוגע למכשירים שמקבלים עדכונים ואלה שלא, באשר למשך הזמן שעדכונים כאלה ניתנים מאז רכישת המכשיר ולתדירות העדכונים וזמינותם.

עוד עולה מדוח ה־FTC כי האקוסיסטם של הטלפון החכם, הכולל גורמים רבים בשרשרת,[121] מקשה את הוצאת העדכונים בצורה סדירה ומהירה. דוח ה־FTC אף מצביע על מורכבות נוספת בנושא, הנובעת מכך שקיימת מטריצה של דגמים של מכשירים בשל התאמות לפלחי שוק ודרישות של ספקיות השירות, וכל פרט במטריצה הזו דורש התאמה מיוחדת של גרסת מערכת ההפעלה או הטלאי שרוצים לשחרר, וכל גרסה כזו דורשת בדיקת התאמה ספציפית.

יש לציין כי השילוב של המצב שתואר לעיל יחד עם הסתמכות של המשתמשים על יצרני המכשירים ועל ספקי השירות הסלולרי, וההנחה ששני האחרונים נוקטים אמצעים להגן על המידע בטלפונים החכמים, מעצים את הכשל ומחריף את בעיית האבטחה.[122]

---

117 הודעה לעיתונות של ה־FTC: FTC, to Study Mobile Device Industry's Security Update Practices (09/05/2016), **ניתנת לצפייה באתר:** https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices. הצו פורסם באתר הנציבות. FTC Matter No. P165402 ORDER TO FILE A SPECIAL REPORT, **ניתן לצפייה באתר:** https://www.ftc.gov/system/files/attachments/press-releases/ftc-study-mobile-device-industrys-security-update-practices/160509mobilesecuritymodelorder.pdf.

118 נציבות התקשורת הפדרלית בארצות הברית – Federal Communications Commission. **ניתן לצפייה באתר:** https://www.fcc.gov.

119 הודעה לעיתונות של ה־FCC: FCC Wireless Telecommunications Bureau Launches Inquiry into Mobile Device Security Updates – Partnership with FTC will examine how patches are distributed, **ניתנת לצפייה באתר:** https://docs.fcc.gov/public/attachments/DOC-339256A1.pdf.

120 Mobile Security Updates: Understanding the Issues (Ferbruary 2018) (להלן: **דוח ה־FCC**), **ניתן לצפייה באתר:** https://www.ftc.gov/reports/mobile-security-updates-understanding-issues.

121 יצרן המכשיר, ספקית מערכת ההפעלה, ספק המעבד של הטלפון (ה־SoC), ספק השירות הסלולרי, שותפים שלו ומעבדות בדיקה עצמאיות.

122 לפי המחקר, 70% סומכים על יצרני מכשירי הטלפון ו־68% על ספקיות השירות הסלולרי, בשיעור דומה לאלה הסומכים על חברות האשראי (69%), לעומת 66% שסומכים על ספקיות הדואר האלקטרוני 49% שסומכים על הרשויות הפדרליות ו־47% שסומכים על

(ג) חשיפה לאפליקציות זדוניות וחולשות באפליקציות לגיטימיות

חלק מ״חוכמתו״ של הטלפון החכם, ואולי עיקרה, נעוץ ביכולת של המשתמש להתקין עליו יישומים (אפליקציות), העושים שימוש במשאבים שלו (כגון במצלמה, חיישני תנועה, חיבורים אלחוטיים ועוד) ומקנים לו פונקציונליות נוספת. אפשר להתקין יישומים כאלה מחנויות האפליקציות (Play של גוגל ו־App Store של אפל), אך גם להורידן ממקורות אחרים, באמצעות הורדת קובצי APK[123] מאתרים שונים. לפי אתר Statista, מספר האפליקציות ב־Play בשנת 2018 עומד על 3.8 מיליון, ב־App Store של אפל על 2 מיליון וב־AppStore של אמזון על כ־630 אלף.[124]

על פי דוח של חברת המחקר Nielsen, בשנת 2014 הוקדש עיקר זמנם של המשתמשים בטלפונים החכמים (86%) לשימוש באפליקציות, לעומת גלישה באתרי אינטרנט (14% בלבד).[125] יש להניח שזה המצב גם כיום נוכח הגידול הרב בכמות האפליקציות והנוחות שהן מציעות לעומת הגלישה באתרים מותאמים, ועל אחת כמה וכמה באתרים שאינם מותאמים למובייל.

ההנחה שהורדת אפליקציה מהחנויות הרשמית של גוגל ואפל מבטיחה שמדובר באפליקציות שאינן נוזקה היא הנחה חסרת יסוד. בהתבסס על דיווחים של גוגל עצמה, בשנת 2015 נמצאו ב־Play 40,000 אפליקציות חשודות (PHA),[126] בשנת 2017 למעלה מ־150 אלף ובשנת 2018 הסירה גוגל מספר מדהים של 700,000 אפליקציות החשודות כזדוניות.[127] כאמור, באנדרואיד אפשר להוריד קובצי התקנה של אפליקציות גם ממקורות אחרים, שכלל אינם תחת פיקוח או סריקה של גוגל, וזהו פתח נוסף לכניסת אפליקציות זדוניות ולהתקנתן בטלפון.

---

123 Android PacKage – קובץ (container) שמשמש במערכת ההפעלה אנדרואיד להתקנת אפליקציות ותוכנות נוספות.

124 Number of apps available in leading app stores as of 3rd quarter 2018, ניתן לצפייה באתר: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores.

125 Nilsen, THE DIGITAL CONSUMER (February 2014), ניתן לצפייה באתר: http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2014%20Reports/the-digital-consumer-report-feb-2014.pdf.

126 Potentially Harmful Apps – אפליקציות שעשויות להיות מזיקות ולמעשה נוזקות המוסתרות באפליקציות שנראות תמימות.

127 Chris Welch, Google took down over 700,000 bad Android apps in 2017 (30/01/2018), ניתן לצפייה באתר: https://www.theverge.com/2018/1/30/16951996/google-android-apps-removed-security-2017.

גם כאשר מותקנות בטלפון אפליקציות לגיטימיות שאינן זדוניות, עשויות להתגלות בהן חולשות שמאפשרות את ניצולן על ידי תוקפים. כך למשל דיווחה חברת צ׳קפוינט את דבר קיומה של חולשה שכונתה FakesApp באפליקציית Whatsup. האפליקציה נמצאת בבעלות פייסבוק ולה מעל 1.5 מיליארד משתמשים ומעל מיליארד קבוצות דיון ועוברים בה כ־65 מיליון מסרים מדי יום. החולשה שנתגלתה מאפשרת לתוקף להתערב ולשנות תוכן של מסרים, הנשלחים הן בין משתמשים בודדים והן בקבוצות. יכולת כזו מקנה לתוקף אפשרות להפיץ דיסאינפורמציה ו־Fake News, שנראית למקבל כאילו הגיעה ממקור אמין.[128] כל זאת עומד בסתירה להודעה שמקבלים המשתמשים, שלפיה המסרים מוצפנים מקצה לקצה.

(ד) חשיפה במגוון חזיתות לקישורים זדוניים

הטלפון החכם משלב יכולות של טלפון סלולרי ושל מחשב כף יד. ככזה, הוא מאפשר למשתמש ליהנות משני העולמות הללו מחד גיסא, אך גם להיות חשוף למתקפות במגוון רחב של יותר של אמצעים מאידך גיסא.

המשתמש חשוף למסעות דיוג (Phishing) ולניסיונות לפתות אותו ללחוץ על קישורים שיגרמו להתקנת נוזקה על הטלפון. אלה מועברים לא רק בדואר אלקטרוני שמתקבל בטלפון, אלא גם במסרונים (SMS/MMS)[129] ובשירותי מסרים מיידיים (כמו WhatsUp ו־Telegram).

(ה) חיבוריות קבועה (Always Connected) וגישה לטלפון באמצעות כמה ממשקי קישוריות אלחוטית

כאמור לעיל, לטלפון החכם יש כמה ממשקים של חיבוריות אלחוטית, המופעלת לעיתים קרובות באופן קבוע וכל העת, תוך שאף אם הטלפון אינו בשימוש מתרחשת בו פעילות ברקע.[130] הטלפון מחובר כמובן לרשת הסלולרית באופן קבוע,[131] אך גם בקישוריות

---

128 פרסום באתר חברת צ׳קפוינט, Dikla Barda, Roman Zaikin and Oded Vanunu, FakesApp: A Vulnerability in WhatsApp, ניתן לצפייה באתר: https://research.checkpoint.com/fakesapp-a-vulnerability-in-whatsapp.

129 SMS: Short Messaging Service, MMS: Multimedia Messaging Service – שירות מסרוני טקסט ושירות מסרוני מולטימדיה.

130 העובדה שמסך הטלפון כבוי אין משמעותה שהטלפון אינו ממשיך לתפקד ולקבל מידע באמצעות ממשקי הקישוריות שלו, כפי שכל משתמש חווה – לאחר ש״מעירים״ את הטלפון יש בו הודעות חדשות ולעיתים עדכונים של אפליקציות ואף עדכוני תוכנה נעשים ברקע.

131 על פגיעות הרשת הסלולרית ראו בהמשך בסעיף (ח) בפרק זה.

Bluetooth,WiFi ו־NFC.[132] כל אחד מהממשקים הללו עשוי לשמש נקודת תורפה שבאמצעותה תתבצע חדירה של תוקף או לכל הפחות באמצעותה יועבר הפיתיון, אשר אם יצלח יביא לחדירה לטלפון החכם. לא פעם גם ערוצי הקישוריות האלחוטית הללו נמצאים במצב של Always On ומאפשרים לתוקפים לנצל אותם וחולשות שמתגלות בהם לביצוע מתקפות סייבר.[133]

(ו) אי־קבלת תמיכה שוטפת ממערך ה־IT בארגונים

לאוכלוסיות רחבות אין ממילא תמיכה ארגונית (סטודנטים, עסקים קטנים, עצמאים, פנסיונרים, בני נוער, אנשים שעובדים בבית וכו׳), אך גם מי שמועסק בארגון שנותן תמיכה מרכזית לפלטפורמות המחשוב שלו, לא בהכרח מקבל תמיכה לטלפון החכם הפרטי שלו.

השימוש בטלפונים חכמים פרטיים במקום העבודה נפוץ ביותר, והמצב של BYOD[134] הוא כבר עובדה קיימת. עם זאת, המכשירים הללו, בניגוד למערכות המחשוב הארגוניות לרבות מחשבים ניידים, אינם מקבלים תמיכה שוטפת ממערך מערכות המידע של הארגון. משכך, גם הארגון אינו מתקין על הטלפון החכם אמצעי הגנת סייבר ואינו דואג לעדכונים שוטפים של אמצעים אלה ולעדכונים במקרים של גילוי פרצות אבטחה ואיומי סייבר חדשים. יש ארגונים שמבצעים ניטור מסוים על התעבורה בטלפונים ניידים בשטח הארגון, אך לא יותר מכך.

מדריכים שמפרסמות רשויות שונות מיועדים בדרך כלל לארגונים,[135] וככאלה הם רלוונטיים לארגונים ולמי שהם מעסיקים (אם הם מיושמים), אך לא לאוכלוסיות אחרות.

(ז) חשיפה למתקפות חומרה בשל פגיעות פיזית

חלק נכבד מהטלפון החכם הוא המסך שלו, שהוא מטבעו רכיב פגיע לשבר כתוצאה של נפילה של המכשיר או חבטה שהוא סופג. גם רכיבים נוספים של המכשיר עשויים להינזק

---

132 NFC היא תקשורת בשדה קרוב (Near Field communication), דהיינו לטווחים קצרים ביותר (של כ־20 ס״מ), ומשמשת ליישומים כגון ארנק אלקטרוני (תשלום באמצעות הטלפון), קריאת כרטיסים חכמים (כמו רב־קו) ועוד. עם זאת, על ידי שימוש באמצעים טכניים בצד השני (כגון אנטנה מתאימה ומגבר), יש אפשרות ליצור תקשורת גם בטווחים גדולים יותר.

133 ראו לדוגמה חולשה ב־Bluetooth בעת חיבור בין התקנים. Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange – Vulnerability Note VU#304725 (17/08/2018), ניתן לצפייה באתר: https://www.kb.cert.org/vuls/id/304725.

134 Bring Your Own Device, ראו לעיל, הערה 13.

135 ראו **תורת ההגנה בסייבר לארגון**, לעיל, הערה 19, בסעיף 13 בפרק 6.2 העוסק ב״אבטחת טלפוניים סלולריים״.

עקב כך, ומשתמשים רבים חוו נזקים כאלה בגלל גודלו של הטלפון והעובדה שהוא נישא לכל מקום ובצמוד למשתמש. החלפת מסך או תיקוני חומרה הם עניין יום-יומי, ומעבדות לתיקונים טלפונים חכמים הפכו להיות נפוצות מאוד.

שוורץ ואחרים, מאוניברסיטת בן גוריון, הדגימו כיצד אפשר לבצע מתקפה באמצעות מודול של מסך מגע בעת החלפת מסך, למשל בשל שבירה שלו,[136] וזאת בשל חולשות ופגיעויות שקיימות במודול של מסכי המגע ובדרייבר שלו.[137] מתקפות כאלה יכולות לתעד את השימוש במסך המגע וגם לגרום לפעולות שמדמות לחיצות על מסך המגע ויכולות גם להביא להשתלטות על הטלפון, לצילום תמונה ושליחתה במייל בלא ידיעת המשתמש, לשינוי קישורים לקישורים זדוניים ועוד.

(ח) חולשות מובנות בפרוטוקול הסלולרי

הטלפון החכם מחובר לרשת הסלולרית בצורה אלחוטית ומתקשר על הרשת בפרוטוקול תקשורת מוגדר, כגון פרוטוקול ה־GSM שפותח תחילה להעביר קול בלבד ולאחר מכן נוספו לו יכולות להעביר Data, שאפשרו גם את החיבוריות של הטלפון החכם לאינטרנט.[138] לפרוטוקולים הללו יש חולשות מובנות שתוקפים מנצלים לרעה.[139] כך למשל, רצ׳יץ ואחרים[140] תיארו מתקפה באמצעות MMS[141] על ידי ניצול חולשות של הפרוטוקול, שתוצאתה ריקון הסוללה של המכשיר תוך זמן קצר והפיכתו לחסר שימוש עד לטעינתו מחדש.

מתקפות נוספות נעשות באמצעות מכשירים הקרויים IMSI Catchers,[142] המדמים תחנות בסיס של הרשת הסלולרית וגורמים לטלפונים להתחבר אליהם במקום לתחנת

---

136 Omer Shwartz et al., “From Smashed Screens to Smashed Stacks: Attacking Mobile Phones Using Malicious Aftermarket Parts”, *IEEE European Symposium on Security and Privacy Workshops* (2017), pp. 94–98.

137 דרייבר היא תוכנה שמפעילה התקן חומרה. החולשות דווחו ותוקנו על ידי טלאי של גוגל – ראו CVE-2017-0650, ניתן לצפייה באתר: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0650.

138 לסקירה היסטורית של התפתחות התקשורת הסלולרית ראו: ETSI, Mobile Communication Systems, ניתן לצפייה באתר: http://www.etsi.org/technologies-clusters/technologies/past-work/cellular-history.

139 על פגיעות הרשת הסלולרית בפרוטוקול ה־GSM ראו למשל: Ali Raheem, *An Investigation Into Authentication Security of GSM Algorithm for Mobile Banking* (2014).

140 Radmilo Racic at el., “Exploiting MMS Vulnerabilities to Stealthy Exhaust Mobile Phone’s Battery”, *IEEE Securecomm and Workshops* (2006).

141 לעיל, הערה 129.

142 IMSI (International Mobile Equipment Identity), הוא קוד השמור בכרטיס ה־SIM (Subscriber Identity Module) בטלפון ברשת GSM והינו מזהה ייחודי של המנוי. IMSI Catcher מדמה תחנת בסיס ומשדר אות חזק שגורם לטלפונים בסביבתו להתחבר

הבסיס, תוך ניצול חולשות בפרוטוקול הסלולרי. כך למשל, ה־DHS האמריקאי, בהתייחסו להימצאות מכשירים כאלה בוושינגטון הבירה, השיב שאין לו יכולת טכנית לזהות או לאתר את כל ההתקפות האלה.[143]

העיסוק בחולשות של הפרוטוקולים הסלולריים והדרך להתגבר עליהן חורג מהיקפו של מאמר זה, ולפיכך לא יהיה בו עיסוק בהמשך הדברים.

(ט) הגורם האנושי

"If there's a flaw it's human. It always is".[144]

בספרות הקיימת כבר עמדו על כך שהגורם האנושי הוא החוליה החלשה בכל מערכת של אבטחת סייבר.[145] הגורם האנושי הוא גם הגורם המקשר בין חלק ניכר מהכשלים שתוארו לעיל ומהסיבות לכשלים הללו.

בניסוי שערכו חוקרים מאוניברסיטת Friedrich-Alexander בגרמניה התברר שכ־56% מהאנשים לחצו על קישורים בהודעות אימייל שהם קיבלו מאנשים לא מוכרים ו־40% ממשתמשי פייסבוק לחצו על קישורים שנשלחו אליהם על ידי שולחים לא ידועים. הם עשו זאת אף על פי שידעו שהדבר עשוי להעמיד את המחשב או הטלפון שלהם בסכנה. הסיבה העיקרית לכך הייתה פשוטה ולא מפתיעה במיוחד: **סקרנות**.[146]

אליו ולא לתחנת הבסיס האמיתית, תוך שהם שואבים את כל המידע מהטלפון, כולל זהות המנוי. חלקם גם יכולים ליירט שיחות והודעות טקסט. גם גורמי אכיפת חוק עושים שימוש במכשירים כאלה.

143 מכתב ה־DHS בתשובה לשאלות של הסנטור Ron Wyden לגבי המצאות IMSI Catchers באזור וושינגטון DC וההשלכות של כך. The Department of Homeland Security's Response to Senator Ron Wyden's November 17, 2017 Letter (March 2018), **ניתן לצפייה באתר**: https://www.scribd.com/document/375529905/Wyden-Enclosure-3-26-18-1.

144 **מתוך הסרט** Minority Report (2012).

145 **ראו לדוגמה**: Man Ho Au & Raymond Choo, *Mobile Security and Privacy* (2017), Chapter 3.

146 One in two users click on links from unkown senders – FAU researchers investigate user behavior when unknown messages are received online (25/08/2016), **ניתן לצפייה באתר**: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders- **בניסוי השתתפו כ־1700 סטודנטים מ־FAU (בשני מחקרים) שאליהם נשלחו מיילים תחת שם בדוי. ההודעות נחתמו בשמות שהם נפוצים ביותר בקרב קבוצת היעד, ונכתב בהן שהקישורים הם לתמונות ממסיבת סוף השבוע. מי שלחץ על הקישור הגיע לעמוד שנרשם בו שהגישה נחסמה, וכך יכלו החוקרים למנות את מספר הלחיצות. לאחר מכן נשלח שאלון לכל הסטודנטים שהשתתפו לבירור הסיבה לכך שלחצו על הקישור.

העובדה שהגורם האנושי הוא החוליה החלשה רק מחזקת, לדעת המחבר, את הצורך במתן פתרון לבעיית האבטחה. מצד אחד, פתרון זה צריך לדרוש מעורבות מינימלית של הגורם האנושי, באופן שלא תידרש מעורבות כזו על מנת להבטיח רמה גבוהה של אבטחת סייבר בטלפון החכם. מן הצד השני, נדרש שכשל של הגורם האנושי, כמו לחיצה על קישור שבעקבותיו יהיה ניסיון להתקין תוכנה זדונית על הטלפון, לא יגרום באופן אוטומטי להצלחתה המיידית של התקפת הסייבר ולהתקנת אותו קישור, בדוגמה זו.

(י) נוזקה המגיעה עם הטלפון החכם (מותקנת מראש)

בדוח מגמות מתקפות הסייבר החצי־שנתי לשנת 2018 של חברת צ׳קפוינט[147] מתוארת מגמה חדשה, שנצפתה במחצית הראשונה של שנת 2018, של נוזקה מותקנת מראש (preinstalled malware). לטענת החברה, התגלתה נוזקת בוטנט למובייל, שהתחזתה לאפליקציית שירות מערכת ל־WiFi לגיטימית, והותקנה במיליוני מכשירים של יצרנים שונים, כולל Huawie, Xiaomi, Vivo וסמסונג. במקרה אחר, 42 דגמים של טלפונים זולים נמצאו ככאלה שנמכרו עם נוזקה הידועה בשם Triada banking trojan, שיש קושי רב להסיר אותה בלא למחוק לחלוטין את מערכת ההפעלה ולהתקינה מחדש.[148] מגמה מעין זו דורשת אמצעים מתאימים, שבוודאי אינם בידי המשתמש אלא בידי היצרנים של המכשירים, שעליהם להבטיח ששרשרת האספקה בייצור הטלפון אינה חשופה לתוקפים ששותלים נוזקות במהלך ייצור הטלפון.

(יא) סיכום – כשלים עיקריים וסיבות אפשריות

הטבלה הבאה מסכמת את הכשלים העיקריים והסיבות האפשריות לקיומם:

סוג הכשל	סיבות אפשריות
אחוז נמוך של התקנת תוכנת הגנה	אדישות ו/או חוסר מודעות של בעלי המכשירים/משתמשים לסיכוני הסייבר שהם חשופים אליהם; קושי לבחור מבין תוכנות ההגנה את התוכנה הרצויה; קושי להתקין את תוכנות ההגנה; חשש מפני פגיעה בפרטיות.

147 לעיל, הערה 76.

148 Catalin Cimpanu, Banking Trojan Found in Over 40 Models of Low-Cost Android Smartphones (2.3.2018), ניתן לצפייה באתר: https://www.bleepingcomputer.com/news/security/banking-trojan-found-in-over-40-models-of-low-cost-android-smartphones.

סוג הכשל	סיבות אפשריות
חשיפה לאיומים במגוון חזיתות	הגורם האנושי (סקרנות, חוסר מודעות); חיבוריות אלחוטית שמטבעה היא always on.
BYOD	המכשירים, בניגוד לעבר, הם בדרך כלל של המועסקים; לא בהכרח מקבלים תמיכת הגנה מהארגון, אבל מתחברים לרשת שלו; גם מי שמקבל תמיכה - אוכלוסייה מצומצמת (לא כוללת עסקים קטנים ועצמאים, ילדים ונוער, סטודנטים, פנסיונרים, לא מועסקים ועוד).
כשלים מובנים	חולשות בפרוטוקול הסלולרי ובפרוטוקול הטלפוניה הבסיסי המשמש גם כיום את כל ספקי השירות (SS7); חולשות בפרוטוקולים אלחוטיים אחרים; תקיפות חומרה; Always Connected, שמשמעו חשיפה מתמדת לאיומי סייבר.

ג. התמודדות עם בעיית האבטחה באמצעות דיסציפלינות משפטיות שונות

כסיכום ביניים עד כאן, אפשר להגיע למסקנות הבאות:

1. קיימת בעיית אבטחת סייבר בטלפונים חכמים;
2. בעיה זו עשויה לגרום לפגיעה הן בבעל המכשיר או המשתמש והן באחרים (החצנות שליליות);
3. מדובר באתגר אבטחה ייחודי למכשירי קצה ולכשלים שדורשים מענה שאינו תלוי רק במשתמש הקצה;
4. עולה כי שני הכשלים המרכזיים הם אי־התקנה של אמצעי אבטחת סייבר ואי־עדכון מערכות ההפעלה/טלאים;

בהתאם למסקנות הללו אבחן בפרק זה של המאמר אם קיימים אמצעים משפטיים פוזיטיביים מדיסציפלינות משפטיות שונות אשר יכולים לתת מענה לכשלים המרכזיים שביסוד בעיית האבטחה.

יצוין כי כאשר מדובר בציוד קצה מסוג אחר, ותחת המעטפת של IoT, הבעיה אף עשויה להיות חריפה יותר; בניגוד לטלפון החכם, בציוד קצה אחר שהוא ״טיפש״ המשתמש אינו יכול, בדרך כלל, לבצע עדכוני תוכנה או להתקין תוכנות אבטחה, ובחלק

ממכשירים אלה כלל אין מערכת הפעלה. הפתרון שרגולטורים נוקטים כיום לעיתים בנוגע לציוד כזה הוא הוצאת מכשירים כאלה מהשוק.[149]

אבחן להלן את השאלות, אם אפשר להחיל דיסציפלינות משפטיות שונות, כגון דיני הגנת הפרטיות, דיני נזיקין ודיני הגנת הצרכן, כדי לתת מענה לבעיית האבטחה, ואם דיסציפלינות כאמור עונות על הכשלים שביסוד בעיית האבטחה.

כפי שעולה מניתוח הסוגיה להלן, אין די בכל אלה בפני עצמם כדי לתת מענה לבעיית האבטחה, אך הם עשויים להיות חלק ממכלול הכלים המשפטיים להתמודדות איתה, ולעיתים עשוי להידרש שינוי חקיקה.

1. הגנת הפרטיות והמידע – רגולציית הגנה המידע של האיחוד האירופאי

חקיקה ואסדרה קיימות בתחום של הגנת הפרטיות המידע, ולפיכך אבחן להלן אם, ביישום מתאים, אסדרה זו עשויה לתת מענה לבעיית האבטחה. דוגמה לאסדרה כזו היא הרגולציה של הגנת המידע של האיחוד האירופי, ה־GDPR,[150] אשר נכנסה לתוקף במאי 2018. ה־GDPR מטילה חובות שונות הן על ה־Controller הן על ה־Processor.[151] בין היתר, מוטלת עליהם החובה ליישם אמצעים ארגוניים וטכניים כדי להבטיח את קיומה של אבטחה ברמה ההולמת את הסיכון, בין היתר על ידי שימוש בהצפנת המידע ופסאודו־אנונימיזציה,[152] יכולת להבטיח באופן שוטף סודיות, שלמות, זמינות ועמידות של המערכות ושירותי עיבוד המידע, יישום תהליך קבוע לבדיקה והערכה של האפקטיביות של האמצעים הטכניים והארגוניים שנועדו לוודא כי העיבוד מאובטח ועוד.[153]

הרגולציה גם קובעת שבעת הערכת הרמה הנדרשת של אבטחת המידע יש להביא בחשבון במיוחד את הסיכונים שנובעים מהעיבוד, תוך הדגשת פגיעה במידע ואיבודו,

---

149 Jane Wakefield, Germany bans children's smartwatches (17/11/2017), **ניתן לצפייה באתר**: https://www.bbc.com/news/technology-42030109.

150 Regulation (EU) 2016/679 of the European Parliament and 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 and repealing Directive 95/46/EC (General Data Protection Regulation) (להלן: **GDPR**), נכנסה לתוקף ב־EEA (Europe Economic Area) ב־25.5.2018.

151 ראו הגדרת מונחים אלה ב־Article 4 של ה־GDPR. ה־Controller הוא שקובע את מטרותיו של עיבוד המידע ואת האמצעים לביצועו, וה־Processor הוא שמבצע את העיבוד עבור ה־Controller ובהרשאתו.

152 עיבוד מידע באופן שאי־אפשר עוד לייחסו למושא מידע מסוים בלא שימוש במידע נוסף, ובלבד שמידע נוסף כזה שמור בצורה נפרדת וננקטים אמצעים טכניים וארגוניים להבטיח שהמידע האישי לא יהיה ניתן לייחוס לאדם מזוהה או לזיהוי (הגדרת pseudo-anonymization ב־Article 4 של ה־GDPR).

153 Article 32 של ה־GDPR.

שינויו, חשיפה בלתי מורשית שלו, וכן גישה אל מידע בעת שידורו, שמירתו או עיבוד שלו בכל דרך אחרת. ההגדרה של ״עיבוד״ ב־GDPR רחבה מאוד, ומפאת חשיבותה לענייננו, כפי שיובהר להלן, אביא אותה כלשונה, לרבות הגדרת המונח ״מידע אישי״ המוטמעת בה, כדלקמן:[154]

> "**processing**" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
>
> "**personal data**" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

כעולה מההגדרות הללו, אין ספק שבטלפון החכם מתבצע עיבוד של מידע אישי. הדבר בא לידי ביטוי, בין היתר, בשמירת מידע אישי בטלפון או באמצעותו, לרבות תמונות, מסמכים ובהם נתונים מזהים וכיוצא באלה, שמירת מידע אישי והעברתו באפליקציות של רשתות חברתיות ועוד, עיבוד נתוני המיקום (Geolocation) באמצעות הרשת הסלולרית, אמצעי הניווט בטלפון (GPS) ועל פי חיבוריות ה־Wi-Fi שלו. הוא גם עשוי לבוא לידי ביטוי בעיבוד מידע ביומטרי (כגון טביעת אצבע הדרושה לצורך שימוש בטלפון), שהינו מידע אישי מסוג המידע הכלול בקטגוריות המיוחדות, אשר אסורות בדרך כלל בעיבוד, אלא בהתקיים התנאים הקבועים ב־GDPR.[155]

אפשר לטעון כי מבצע העיבוד הוא מושא המידע עצמו, ועל כן הרגולציה כלל אינה חלה במקרה זה, שכן עיבוד כזה מוחרג מתחולתה המהותית, לפי לשונו של Article

---

154 Article 4 של ה־GDPR.

155 מידע ביומטרי מוגדר ב־Article 4 של ה־GDPR וכלול בסוגי המידע המפורטים ב־ Article 9. שאלת חוקיות העיבוד בנסיבות אלה היא מחוץ ליריעה של מאמר זה ואינה דרושה לשם הדיון.

2(2)(c) של ה־GDPR, המסייג את תחולתה, בין היתר, לעיבוד מידע שנעשה על ידי אדם במהלך פעילות שהיא אישית או פעילות של משק הבית (להלן: **פעילות מוחרגת**):[156]

> The regulation does not apply to the processing personal data:
>
> …
>
> (c) by a natural person in the course of a purely personal or household activity;

במבט ראשון מדובר בטיעון שובה לב, שהרי המשתמש הוא הבעלים של המכשיר (בדרך כלל), הוא ששומר את התמונות בטלפון, בין שהוא צילם אותן ובין שלא, הוא שמתחבר לרשתות החברתיות ועוד. אפשר אפוא לטעון שלכאורה מדובר בעיבוד על ידי אדם במהלך פעילות שבאופייה היא אישית.

אלא שבפסקת המבוא הרלוונטית של ה־GDPR מובהר בצורה שאינה משתמעת לשתי פנים הרגולציה חלה על ה־Controller וה־Processor, אשר מספקים את האמצעים לעיבוד המידע האישי עבור עיבוד במהלך הפעילות המוחרגת:[157]

> This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

מהאמור בפסקת המבוא הנ״ל עולה כי הן יצרני הטלפונים החכמים והן ספקי מערכות ההפעלה (גוגל ואפל), שמספקים את האמצעים לעיבוד המידע של הפעילות המוחרגת, כפופים ככאלה ל־GDPR, ועל כן גם הם מחויבים בחובות החלות על ה־Controller וה־Processor, לרבות נקיטת אמצעים לאבטחת המידע האישי בהתאם להוראת Article 32 של ה־GDPR.

---

156 לפי סעיף זה, הרגולציה אינה חלה על עיבוד מידע בידי אדם במהלך פעילות שהיא אישית או במסגרת משק ביתו "processing personal data…by a natural person in the course of a purely personal or household activity").

157 Recital 18 of the GDPR.

יתרה מכך, היצרנים וספקי מערכות ההפעלה של הטלפונים החכמים לא רק מספקים את האמצעים לעיבוד המידע, אלא מבצעים בעצמם עיבוד של מידע אישי כמשמעותו ב־GDPR, הנאסף באמצעות הטלפון החכם, ושל המידע האגור בו.

כך למשל, כדי להתמודד עם הבעיה שהמידע בטלפון נשמר באפליקציות המותקנות בו ואינו מגיע לידיה, הכריזה גוגל בשנת 2016 על הוספת שכבה למערכת ההפעלה אנדרואיד, שתאפשר לה להגיע למידע שמשתמשים שומרים או מעבירים באפליקציות. גוגל הכריזה על יכולת חיפוש חדשה – לא רק באינטרנט, אלא גם באפליקציות המותקנות בטלפון, לרבות אלה שמתוקנות בו מראש על ידי יצרנים.[158]

בנסיבות האלה אפשר לטעון, על בסיס האמור לעיל, כי יצרני הטלפונים וספקי מערכות ההפעלה שלהם מפירים את חובתם בעניין אבטחת המידע, בכך שאינם מספקים אמצעים כאלה ולא דואגים לעדכונים שוטפים שלהם.

אלא ש״אליה וקוץ בה״, שכן התחולה הטריטוריאלית של ה־GDPR מוגבלת רק לעיבוד מידע של מושאי מידע הנמצאים בתוך תחום האיחוד האירופאי.[159] בלא החלה של ה־GDPR על מושאי מידע בישראל אין אפוא לרגולציה זו תוקף ואי־אפשר לעשות בה שימוש לצורך אכיפתה של אבטחת סייבר בישראל.

2. הגנת הפרטיות והמידע – תקנות אבטחת מידע

בחודש מאי 2018 נכנסו לתוקף גם תקנות הגנת הפרטיות העוסקות באבטחת מאגרי מידע.[160] תקנות אבטחת מידע חלות על מאגרי מידע וקובעות את רמת האבטחה שחלה על מאגרי מידע בהתאם לפרמטרים שונים המפורטים בהן, כמו גם את החובות שחלות מכוח רמת האבטחה הרלוונטית.

בטלפון החכם עשוי להיות אגור ״מידע״ מסוג העונה על ההגדרה של מידע שיוצר ״מאגר מידע״, כמפורט בסעיף 7 לחוק הגנת הפרטיות.[161] מכוח כך הייתה אפשרות להחיל חובות של אבטחת מידע בהתבסס על תקנות אבטחת מידע, גם אם מדובר במאגר מידע המנוהל על ידי יחיד.[162]

---

158 Timo Mertens, A new way to search for content in your apps (30.8.2016), **ניתן לצפייה באתר**: https://blog.google/products/search/a-new-way-to-search-for-content-in-your/.

159 Article 3 של ה־GDPR. לאמיתו של דבר התחולה רחבה במעט מגבולות האיחוד האירופאי וכוללת גם שלוש מדינות נוספות, שיחד עם מדינות האיחוד יוצרות את ה־EEA (European Economic Area), אך אין בכך כדי להועיל, שכן התחולה עדיין מוגבלת ביותר ואין בהקשר הזה תחולה ל־GDPR על מושאי מידע המצויים בישראל.

160 תקנות הגנת הפרטיות (אבטחת מידע), תשע״ז–2017, ק״ת 7089 (להלן: **תקנות אבטחת מידע**).

161 חוק הגנת הפרטיות, תשמ״א–1981, ס״ח 1011 (להלן: **חוק הגנת הפרטיות**).

162 ההגדרה של ״מאגר המנוהל בידי יחיד״ בתקנה 1 לתקנות אבטחת מידע קובעת שמדובר במאגר שמנהל יחיד או בבעלות יחיד, ואשר רק היחיד, ולכל היותר שני בעלי הרשאה

אלא שגם בתקנות אבטחת מידע, בדומה ל־GDPR, יש החרגה של תחולן אם מדובר במאגר מידע שהוא ״אוסף לשימוש עצמי שאינו למטרות עסק״.[163] מהצד האחר אין בהן, כפי שיש ב־GDPR, התייחסות למי שמספק את האמצעים לעיבוד המידע לשימוש עצמי, דהיינו יצרני הטלפון וספקי מערכות ההפעלה.

משכך, ולמעט עסקים, אין לתקנות אבטחת מידע תחולה על מאגרי המידע השמורים בטלפון החכם, ובנוסחן כיום אין בהן משום פתרון להסדרת בעיית האבטחה או אסדרתה.

3. דיני נזיקין

קושי מבני אינהרנטי לדיני הנזיקין הוא שהם נותנים סעד בדיעבד ורק לאחר שהנזק כבר נגרם, ויש הרואים במטרתם את השבת המצב לקדמותו.[164] הסעד בדרך כלל גם אינו מחייב את המזיק לנקוט צעדים כלשהם מכאן והלאה, אלא מטרתו לפצות את הנפגע.[165] כידוע, בניגוד לדין האמריקאי והקנדי לדוגמה, המוסד של פיצוי עונשי אינו קיים בדין הישראלי. על פי פסיקת בית המשפט העליון, בתי המשפט לא ייטו לפסוק פיצויים עונשיים במסגרת הליך אזרחי אלא במקרים חריגים בלבד.[166] אם כן, בדיני הנזיקין בישראל לא קיים ההיבט ההרתעתי הנובע מפיצוי עונשי והדרוש לשם שינוי התנהגות שתביא להסרת הכשלים שביסודה של בעיית האבטחה. כאשר מדובר בכשל של אי־התקנת אמצעי אבטחה בטלפונים החכמים ואי־עדכון של מערכות ההפעלה, אפשר לטעון, לפי הגישה הכלכלית, כי דיני הרשלנות מיועדים לתמרץ את יצרני המכשירים לפתור את הכשלים הללו, אם עלותם נמוכה מתוחלת הנזק שיימנע אם יינקטו.[167] הואיל וכל המידע מצוי בידי היצרנים ולא מדובר בעלויות שאפשר להעריך אותן בקלות (כגון עלות של הצבת שלטי אזהרה או גידור של מכונה), לא ברור אם תמריץ כזה אכן קיים.

נוסף על כך, בתביעה נזיקית במקרה של נזק שנגרם כתוצאה של בעיה של אבטחת סייבר, עלול הניזוק – המשתמש או הצד השלישי – להיתקל בקשיים להוכיח את הסיבה

נוספים, רשאים לעשות בו שימוש ובאפשרותם לעשות בו שימוש, אך למעט כמה מקרים חריגים שאינם רלוונטיים לדיון כאן.

163 הגדרת ״מאגר מידע״ בסעיף 7 לחוק הגנת הפרטיות.

164 ישראל גלעד, **דיני הנזיקין – גבולות האחריות** (2012) (להלן: **גלעד**), עמ׳ 52. לדיון נרחב יותר על מטרות דיני הנזיקין, שם החל מעמ׳ 51.

165 אם כי לפי סעיפים 71 ו־72 לפקודת הנזיקין [נוסח חדש], דמ״י 10 (להלן: **הפקודה**), בית המשפט גם רשאי לתת ציווי ש״יכול שיהיה צו עשה או צו לא־תעשה, לשעה או לתמיד״, במגבלות סעיפים 73 ו־74 לפקודה. ראו גם הדיון בהסדרה באמצעות הטלת אחריות לאחר מעשה, **הבר וז׳רסקי**, בפרק ד(3)(1), בעמ׳ 39.

166 רע״א 9670/09 **פלונית נ׳ פלוני** (פורסם בנבו, 2009).

167 לדיון נרחב בנושא ובנוסחת לרנד הנד (נוסחת הרשלנות הכלכלית), ראו אריאל פורת, **נזיקין** (2013), בעמ׳ 94.

לנזק. קיימת גם שאלה אם בכלל מוטלת חובת זהירות בעניין ועל מי – על היצרן או על ספק מערכת ההפעלה, ואם הפגם שנוצל על ידי התוקף הוא במעבד – אם על יצרן המעבד, וכן הלאה. גם אם תוטל חובת זהירות,[168] יש ספק באשר להיקפה ותחולתה נוכח הדינמיות של התחום והעובדה שמתקפות הסייבר לובשות פנים חדשות מדי יום וההתמודדות איתן היא סוגיה מורכבת. עשויים גם להיות קשיים בהוכחת הקשר הסיבתי (דהיינו זיקה מספקת בין ההתנהגות הבלתי ראויה לנזק), וכן בשאלת האשם התורם של בעל המכשיר/המשתמש, אם לדוגמה האחרון לא התקין תוכנת הגנה, לא דאג לעדכן את מערכת ההפעלה או לחץ בעצמו על קישור תמים בהודעת דואר אלקטרוני, ובכך גרם להתקנת הנוזקה או להפעלתה.

לעיתים קרובות מדובר בנזק תוצאתי עתידי – שימוש במידע שנגנב לצורכי גנבת זהות וכיוצא בזה. בארצות הברית, לדוגמה, נדרש להראות קיומו של נזק ממשי או אפשרות ממשית לקיומו של נזק, עניין שעשוי להיות קשה להוכחה.[169] הוכחת הנזק ושיעורו הם יסוד אף בדין הישראלי במקרה של עוולת הרשלנות לפי סעיף 35 לפקודה,[170] והקושי הכרוך בכך במקרה של פגם באבטחת סייבר מקשה כאמור את השימוש בדיני הנזיקין ככלי משפטי למתן מענה לבעיית האבטחה ולכשלים ביסודה. כדי להקים אחריות נזיקיות לפי עוולת הרשלנות נדרש גם להראות שהתנהגותו של המזיק הייתה בלתי סבירה או רשלנית.

גם ההגנה בסעיף 5 לפקודה (הסתכנות מרצון) עשויה לשמש נתבעים במקרה של טלפון חכם שנפגע ממתקפת סייבר, בכל הנוגע לבעל המכשיר או המשתמש בו וביחס לנזקים שנגרמו לו. כך יכולה לעלות הטענה שהמשתמש ״ידע והעריך, או יש להניח שידע והעריך, את מצב הדברים שגרמו לנזק וכי חשף עצמו או רכושו למצב זה מרצונו״.[171]

---

168 לדיון נרחב בסוגיית חובת הזהירות והשיקולים להטלתה, ראו **גלעד**, בעמ׳ 643.

169 ראו הדיון בסעיף IV(A) להחלטת בית המשפט המחוזי בלוס אנג׳לס, בבקשת חברת סוני לדחייה על הסף של התביעה שהוגשה כנגדה על ידי עובדיה, שהמידע שלהם נגנב בעת פריצה למחשבי החברה. במקרה הזה המידע הועלה לאתר שיתוף של גנבי זהות ואצל חלק מהעובדים כבר התקבלו מכתבי איום, כך שנקבע שהתנאי מתקיים. *Michael Corona et al v. Sony Pictures Entertainment, Inc.*, Case 14-CV-09600 RGK (Central District of California, 2015), ניתן לצפייה באתר: http://www.krcomplexlit.com/wp-content/uploads/2015/09/OrdGrantPartDenyPartDefMotDismiss97061515.pdf.

170 לשם גיבוש עוולת הרשלנות נדרש נזק (ע״א 145/80 **שלמה ועקנין נ׳ המועצה המקומית, בית שמש**, פ״ד לז (1) 113, 139). ״נזק״ מוגדר בסעיף 2 לפקודה ״אבדן חיים, אבדן נכס, נוחות, רווחה גופנית או שם־טוב, או חיסור מהם, וכל אבדן או חיסור כיוצאים באלה״; ״נזק ממון״ מוגדר ״הפסד או הוצאה ממשיים הניתנים לשומה בכסף ואפשר למסור עליהם פרטים״.

171 לשון סעיף 5 הנ״ל.

מכל הדברים לעיל עולה כי בדיני הנזיקין אין מענה לכשלים ולבעיית האבטחה, והשימוש בהם עשוי להציב קשיים ניכרים, שמטילים בספק את יכולתם להיות הכלי המשפטי המתאים לשם פתרון בעיית האבטחה.

4. דיני הגנת הצרכן – חובת יידוע

בתחומים מסוימים, לרבות בתחום הטלפונים הסלולריים, ננקטת גישה של הטלת חובת יידוע מכוח חקיקה. המשמעות היא חובת פרסום מידע ואזהרות על אריזת המוצר או בעלון בתוך אריזת המוצר, באופן שיאפשר לצרכן (המתעניין) לקבל את המידע על הסכנות הפוטנציאליות הכרוכות בשימוש במוצר. מדובר בסוג של אסדרה בדרך של נורמה המחייבת גילוי.[172]

טלפונים ניידים, והטלפון החכם בכללם, פולטים קרינה אלקטרומגנטית (קרינה בלתי מיינת).[173] קרינה זו נובעת מהתקשורת הסלולרית עצמה וכן מהחיבוריות האלחוטית לטווח קצר (Wi-Fi ו־Bluetooth).

על פי ה־NCI האמריקאי,[174] אין קביעה נחרצת באשר לסיכונים הבריאותיים כתוצאה של קרינה כזו.[175] עם זאת, מקובל במקרים מעין אלה לנהוג בגישת ה״זהירות המונעת״, שלפיה ״[...] גם בהיעדר הוכחות מדעיות מספקות לקיום נזק בריאותי מגורם מסוים ו/או במצב בו ההוכחות לקיום הנזק הן חלשות מאוד, יש במקרים רבים הצדקה לנקוט בצעדים בעלויות סבירות לא גבוהות להפחתת ה׳סיכון׳. נקיטת אמצעים מסוג זה נחוצה ומומלצת מבלי להמתין לסיום המחקרים שהומלץ לבצעם וזאת על מנת להקטין את אי הודאות באשר לקיום/אי קיום נזק בריאותי מהגורם הנדון״.[176]

כחלק מאותו עיקרון המיושם בחקיקה צרכנית בישראל,[177] קיימת חובה לצרף לטלפונים סלולריים חדשים שנמכרים לציבור עלון בדבר הקרינה האלקטרומגנטית שלהם. לא ידוע למחבר מה שיעור המשתמשים המעיינים בעלון, ואם הם מעיינים בו –

---

172 ראו פרק ד׳ לדיון בסוגי האסדרה השונים.

173 להרחבה ראו: המשרד להגנת הסביבה – ״קרינה בלתי מיינת״, ניתן לצפיה באתר: https://www.gov.il/he/departments/topics/non-ionising.
וכן הגדרת ״קרינה בתדרי רדיו״ וההגדרות הנלוות לה, ניתן לצפיה באתר: https://www.gov.il/he/departments/guides/radio_frequency_radiation.

174 NIH, National Cancer Institute, ניתן לצפייה באתר: https://www.cancer.gov/about-nci/overview.

175 ראו ב: "Cell Phones and Camcer Risk" Why are the findings from different studies of cell phone use and cancer risk inconsistent?, ניתן לצפייה באתר: https://www.cancer.gov/about-cancer/causes-prevention/risk/radiation/cell-phones-fact-sheet#q5.

176 ת״א (חי׳) 6684-07 **ונטורה נ׳ דומוטק בע״מ** (פורסם בנבו, 2011), בעמ׳ 18.

177 תקנה 3(2) לתקנות הגנת הצרכן (מידע בדבר קרינה בלתי מיינת מטלפון נייד), תשס״ב–2002, ק״ת 6172.

כמה מהם מבינים את משמעות הנתונים שנמסרים בו, אך יש להניח שמדובר בשיעור נמוך ביותר.[178] הדבר נובע ממורכבות הנושא ומחוסר היכולת להבין את המשמעות של חשיפה לקרינה, שכאמור ממילא שנויה במחלוקת מדעית (חובה דומה, של צירוף עלון לאריזות, קיימת גם בנוגע לתרופות).[179] גורם אפשרי נוסף הוא העובדה שהטלפון החכם הפך להיות חלק בלתי נפרד מחיי היום־יום, והוא צמוד למשתמשים במשך רוב שעות היממה. בעקבות זאת נוצרה הערכת־יתר של ערכו של השימוש בטלפון החכם לעומת הנזק הפוטנציאלי ששימוש כזה עשוי לגרום. התוצאה היא שמשתמשים בוחרים במודע להתעלם ואף לא לקרוא כלל את האזהרות, שכן ממילא לא יהיה בכך כדי לשנות ולגרום להם לחדול משימוש או אף לשנות את הרגליהם ולהפחית את השימוש.

תופעה זו של קיום מידע שמשתמשים מתעלמים ממנו בשל היותו בלתי מובן לרובם או בשל העובדה שכך מקובל לנהוג, אינה ייחודית לעלונים בדבר קרינה אלקרטרומגנטית של טלפונים סלולריים. תופעה דומה אפשר למצוא בהתייחס לתנאי השימוש (Terms of Use) או הסכם רישיון שימוש למשתמש הקצה (EULA)[180] בתוכנות, אפליקציות ואתרי אינטרנט. כך לדוגמה, בניסוי שערכה חברת משחקי אונליין בריטית בשם Gamestation, היא הצליחה ״לאסוף״ 7,500 ״נשמות״ של משתמשים, לאחר שאלה הסכימו לתנאי השימוש שכללו סעיף שמקנה לחברה את הנשמות שלהם.[181]

דוגמה לניסיון לתת מענה לכשל מעין זה אפשר למצוא ברגולציית הפרטיות של האיחוד האירופאי, ה־GDPR,[182] הדורשת שהסכמתו של מושא המידע תתקבל באופן שמובחן מנושאים אחרים, בצורה נגישה, תוך שימוש בשפה בהירה וברורה, וקובעת שכל חלק של הצהרה על הסכמה שאינו עומד בתנאים אלה יהיה חסר תוקף מחייב.[183] הרגולציה נכנסה לתוקף בחודש במאי 2018, כך שבעת כתיבת מאמר זה עדיין אי־אפשר לבחון את ביטויה של הדרישה הזו בפועל ואת השפעתה בצורה מקיפה.

בניגוד לחובת היידוע האמורה אשר חלה על טלפונים סלולריים ביחס לקרינה אלקטרומגנטית, לא קיימת חובה חוקית דומה להתריע מפני חולשות הקיימות במכשיר למתקפות סייבר והתוצאות האפשריות שלהן.

כך או כך, לדעתי לא יהיה די בחובת יידוע מעין זו של הצרכן או המשתמש כדי לתת מענה לכשלים שעומדים ביסוד בעיית האבטחה ולתת מענה לגורמים לכשלים האלה כמפורט בפרקים הקודמים, כעולה גם מהניתוח בפרק ד׳ בסעיף 3 להלן, הדן באסדרה על

---

178 הואיל והמחקר שעליו מבוסס מאמר זה הוא מחקר עיוני, עניין זה לא נבדק אמפירית.

179 תקנה 20 לתקנות הרוקחים (תכשירים), תשמ״ו–1986, ק״ת 6468.

180 End User License Agreement – הסכם רישיון למשתמש קצה.

181 John Brownlee, GameStation EULA collects 7,500 souls from unsuspecting (16.4.2010), ניתן לצפייה באתר: http://www.geek.com/games/gamestation-eula-collects-7500-souls-from-unsuspecting-customers-1194091.

182 לעיל, הערה 150.

183 GDPR, Article 7(2).

דרך של הנחיה והעברת מידע. הטלת החובה על המשתמש הסופי, בציפייה שהוא יהיה הגורם שיעמוד בפרץ, אינה מוכיחה את עצמה במציאות.[184]

על משתמשים או מפעילי הרשת גם לא חלה חובה למסור מידע ולדווח על התקפות סייבר שהתרחשו. חובת גילוי כאמור היא בעלות חשיבות רבה לתחקור המקרים הידועים, לטיפול באירועי סייבר אחרים, להתאוששות מהם, לפיתוח אמצעי מנע והתגוננות, להפצת מידע על דבר המתקפה ודרכי ההתגוננות מפניה וכיוצא באלה. כיום עניינים אלה מטופלים על ידי גופי CERT (Cyber Event Readiness /Response Team), ומסירת המידע היא על בסיס התנדבותי.[185]

5. אחריות למוצרים פגומים

אפשר לבחון אם טלפון חכם שאינו מוגן מפני מתקפות סייבר הוא בבחינת ״מוצר פגום״ כהגדרתו בסעיף 3 לחוק האחריות למוצרים פגומים, תש״ם–1980 (להלן: **חוק המוצרים הפגומים**) ואם יש תחולה לחוק זה בהקשר האמור.

המגבלה בחוק המוצרים הפגומים היא שהוא עוסק רק בפיצוי בגין נזקי גוף. כך לפי סעיף 3(א)(1) שלו, הקובע כי ״מוצר פגום״ הוא מוצר ש״מחמת ליקוי בו הוא עלול לגרום לנזק גוף״ וכך על פי סעיף 2 שלו, המקים אחריות מוחלטת ליצרן בשל נזק גוף,[186] ומטיל עליו חובה ״לפצות את מי שנגרם לו נזק גוף כתוצאה מפגם במוצר שייצר [...]״.

יש לציין שמוצר נחשב כפגום לפי סעיף 3(א)(2) לחוק המוצרים הפגומים גם מטעם חלופי, שלפיו ״בנסיבות העניין נדרשות אזהרות או הוראות טיפול ושימוש מטעמי בטיחות והן לא ניתנו או שאינן מתאימות בהתחשב בסכנה הכרוכה במוצר״.

הטלפון החכם או מוצר קצה בפני עצמו אינו מוצר שמטבעו יכול לגרום לנזק גוף, ועל כן נדרשות אזהרות או הוראות טיפול ושימוש מיוחדות.[187] כך או כך, היותו של החוק מוגבל לנזקי גוף היא מגבלה משמעותית, שכן הנזקים שבדרך כלל נגרמים ממתקפות סייבר בטלפון שאבטחתו חסרה או לקויה הם נזקים כלכליים או נזקים לא

---

184 כאמור בהערות קודמות, המחקר שעליו מבוסס המאמר הוא מחקר עיוני ולא אמפירי, אך הכשל של אי־עדכון מערכות ההפעלה בטלפונים, אי־התקנת טלאי תוכנה לשיפור האבטחה והשיעור הנמוך של התקנת אמצעי הגנת סייבר בטלפונים חכמים, כמתואר לעיל המאמר זה, מעידים על כך שאין לסמוך על המשתמש הסופי לשם מתן מענה לבעיית האבטחה.

185 לדוגמה ה־CERT הישראלי. ראו מסמך עקרונות הפעולה של ה־CERT הלאומי (4.3.2015). ניתן לצפייה באתר: https://www.gov.il/BlobFolder/policy/principles/he/principles.pdf.

186 ת״א (ב״ש) 325/90 **מנדיל נ׳ שיש אשדוד**, פ״מ תשנ״ה(1) 242, 254.

187 לעניין החשש לנזק גוף מהקרינה הבלתי מיוננת שהוא פולט, ראו לעיל בפרק זה בסעיף 4.

ממוניים שאינם כרוכים בנזק גוף (כגון גנבת זהות, הפצה של תמונות אינטימיות וכיוצא באלה).

על כן חוק המוצרים הפגומים אינו נותן מענה לבעיית האבטחה ואינו גורם הרתעתי ליצרנים לתת מענה לכשלים שבבסיס בעיית האבטחה.

6. דיני הגנת הצרכן – חובת גילוי ואחריות יצרן

הדיון להלן בוחן אם דיני הגנת הצרכן בהיבט של חובת גילוי ואחריות היצרן למוצר יכולים לחול על בעיית האבטחה ולתת לה מענה. סעיף 4 לחוק הגנת הצרכן, תשמ״א-1981 (להלן: **חוק הגנת הצרכן**) קובע חובת גילוי של עוסק לצרכן.[188] יש לגלות ״כל פגם או איכות נחותה או תכונה אחרת הידועים לו, המפחיתים באופן משמעותי מערכו של הנכס״,[189] וכן ״כל תכונה בנכס המחייבת החזקה או שימוש בדרך מיוחדת כדי למנוע פגיעה למשתמש בו או לאדם אחר או לנכס תוך שימוש רגיל או טיפול רגיל״.[190] ואולם, החוק גם קובע בסעיף 4 כי ״תהא זו הגנה לעוסק אם הוכיח כי הפגם, האיכות או התכונה או הפרט המהותי בנכס היו ידועים לצרכן״.

לכאורה, לפי לשון החוק, חובת הגילוי רחבה דיה לכלול בתוכה גם חוסר או פגם באבטחת סייבר בטלפון חכם, ואפשר להטיל מכוחה חובת גילוי על יצרני הטלפונים החכמים, היבואנים והמפיצים שלהם. נשאלת השאלה אם יש יסוד להגנה האמורה בסעיף 4 לחוק הגנת הצרכן – הדרישה של נטל ההוכחה בדבר ידיעתם של רוכשי הטלפון על אודות הפגמים באבטחת הסייבר שלו, המוטלת, לפי הסעיף, על היצרן. כפי שפורט לעיל, הממצאים שונים לחלוטין – משתמשים סבורים (בטעות) שהיצרנים וספקי השירות הסלולרי נוקטים אמצעים כדי לשמור על המידע שלהם ולהגן על המכשירים, בעוד בפועל התמונה שונה.

אלא שגם אם תקוים חובת גילוי בנוגע לטלפונים חכמים בהתאם לדרישות סעיף 4 לחוק הגנת הצרכן, לא יהיה בכך כדי לתת מענה לבעיית האבטחה. אם יצרנים או יבואנים ומפיצים יצרפו לאריזת הטלפון החכם עלון אבטחת סייבר, עשויה להיות לו אותה השפעה כמו זו של העלון בעניין הקרינה הבלתי מיוננת.[191] לא יהיה בכך כדי לתת מענה לבעיית האבטחה ולכשלים שביסודה.[192]

מכוח סעיף 18א לחוק הגנת הצרכן תוקנו תקנות הגנת הצרכן (אחריות ושירות לאחר מכירה), תשס״ו-2006 (להלן: **תקנות השירות**).

---

188 ״מי שמוכר נכס או נותן שירות דרך עיסוק, כולל יצרן״ (סעיף 1 לחוק הגנת הצרכן).

189 סעיף 4(א)(1) לחוק הגנת הצרכן.

190 סעיף 4(א)(2) לחוק הגנת הצרכן.

191 הדיון לעיל, בפרק זה בסעיף (4).

192 לדיון בחובת גילוי בהקשר של הגנת סייבר על תשתיות קריטיות, ראו **הבר וז׳רסקי**, לעיל הערה 14, בפרק ד(2) בעמוד 36.

לפי סעיף 1 לתקנות השירות, ״טובין״ כוללים גם מוצרי אלקטרוניקה חדשים, דהיינו גם טלפונים ניידים,[193] ו״קלקול״ מוגדר ״ליקוי, פגם או קלקול״. זוהי הגדרה רחבה, היכולה להכיל גם ליקוי או פגם של חשיפה למתקפות סייבר ואבטחת סייבר לקויה.

על פי תקנה 2(א) לתקנות השירות, ״יצרן של טובין שנמכרו לצרכן יתקן, בעצמו או באמצעות אחר מטעמו, כל קלקול שנתגלה בטובין במהלך תקופת האחריות, בלא תמורה״, ותקופת האחריות היא, לפי תקנה 1 לתקנות השירות, ״תקופה של שנה מיום מסירת הטובין לצרכן [...]״ (יצרנים רשאים להאריך את תקופת האחריות, ולעיתים אף עושים זאת בפועל). על מוצרים המיוצרים בחו״ל (כמו הטלפונים החכמים) חלה תקנה 18, שקובעת כי ״בטובין מיובאים יראו את מי שייבא אותם כיצרן לענין תקנות אלה״, דהיינו החבות לתקן ליקויים ופגמים בטלפונים החכמים בישראל חלה על היבואן שלהם.[194]

אפשר לשאול אם מכוח תקנות השירות ניתן לטעון כי מכשיר טלפון חכם שגרסת מערכת ההפעלה שלו אינה מתעדכנת בתדירות גבוהה דיה כדי לתקן בעיות אבטחה שמתגלות בה ובלי תלות בביצוע פעולות על ידי המשתמש, הוא מכשיר שיש בו ״קלקול״. אפשר גם לשאול אם מכשיר שלא מותקנים בו אמצעי אבטחת סייבר מובנים שמתעדכנים בלא צורך בהתערבות המשתמש הוא מכשיר שיש בו קלקול.

לדעתי התשובות לכך שליליות. הפרשנות של ״קלקול״ היא פגם מובנה שמונע את הפונקציונליות הרגילה של המכשיר, כגון מצב שבו המכשיר אינו מאתחל את עצמו ו״נתקע״ במצב שבו לא ניתן לעשות בו שימוש.[195]

גם אילו היו התשובות חיוביות, הרי שחובת היצרן לפי תקנות השירות היא תיקון המכשיר, בעוד הנזקים שעשויים להיגרם מבעיית האבטחה הם כאמור נרחבים בהרבה (פגיעה ברשת שלמה, במכשירים נוספים ובצדדים שלישיים), וחובת התיקון לא תועיל גם להסרת הכשלים שביסוד בעיית האבטחה (כמתואר בפרק ב׳ בסעיף 2 לעיל). תקנות השירות מחילות חובת תיקון ל״כל קלקול שנתגלה בטובין במהלך תקופת האחריות״, כלומר רק לטובין הספציפיים ורק לפרק זמן מוגבל של תקופת האחריות.

לפי תקנה 2(ג) לתקנות השירות פטור היצרן מחיוביו אם הוכיח ש״מקור הקלקול בנזק מכוון שגרם הצרכן״. לפי תקנה 8(2) רשאי היצרן לגבות תשלום בגין תיקון המכשיר אם הוכיח, לפני ביצוע התיקון, שהקלקול נגרם כתוצאה של ״זדון או רשלנות של הצרכן, לרבות שימוש בטובין בניגוד להוראות השימוש ובלבד שהוראות השימוש סבירות בנסיבות הענין [...]״.יצרנים יכולים אפוא לפטור את עצמם אף מחובת התיקון

---

193 ת״ק (תביעות קטנות רח׳) 41332-06-16 **בר נדב נ׳ סי.טי.אי גומובייל בע״מ** (פורסם בנבו, 2018).

194 רת״ק (מחוזי חי׳) 50000-02-15 **דל טכנולוגי׳ אנד סולושנס ישראל בע״מ נ׳ עמר גלבר** (פורסם בנבו, 2015).

195 שם, המקרה המתואר בפסק הדין.

בלא תשלום על ידי הנחיות בתנאי השימוש ביחס לגלישה זהירה, התקנת אפליקציות ואי-התקנת תוכנת הגנה על ידי המשתמש.

מכל האמור עולה שאין בדיני הגנת הצרכנות בנוסחם כיום כדי לתת מענה לבעיית האבטחה ולהביא להסרת הכשלים שביסודה. ואולם, ייתכן שיש בהם כדי להטיל על היצרנים או היבואנים חובת יידוע (ברורה ו״סבירה בנסיבות העניין״), שאינה קיימת מתוקף חוקים אחרים. ייתכן אפוא שמדובר בפתרון חלקי לבעיה.

ד. אסדרה כמענה לבעיית האבטחה

1. אסדרה – כללי (בקצירת האומר)

אסדרה של שווקים, לדוגמה בצורה של רישיונות או היתרים, היא אחת מהפרקטיקות הנושנות ביותר של מוסד המדינה. התפיסה המקובלת היא שאסדרה ניתנת לביצוע באמצעות מגוון מנגנונים וכלי רגולציה, ולא רק באמצעות סנקציות או כלים הידועים בשם הכולל ״ציוויים ובקרה״ (״Command & Control״).[196]

ההגדרה המדויקת של המונח ״רגולציה״ שנויה במחלוקת בין מלומדים. ההגדרות נעות בין מערכת של ציוויים ספציפיים, השפעה מכוונת של המדינה ועד לכל סוג של שליטה חברתית. סלזניק הגדיר אסדרה כשליטה מתמשכת וממוקדת, המופעלת על יד רשות ציבורית על פעילויות המוערכות על ידי הקהילה; בלק הגדירה אסדרה כשימוש מכוון בסמכות לשם השפעה על גוף אחר בהתאם למערכת של סטנדרטים, המערבת שימוש בכלים שונים של איסוף מידע ושינוי התנהגות.[197]

פייק ווורל, במאמרם על רגולציה של מרחב הסייבר, מציינים את ההגדרה של מינץ, הגורס כי רגולציה היא צורות שונות של פעולות קיבוציות מכוונות, בעניינים הכרוכים באינטרסים ציבוריים.[198] הם גם מציינים שרגולציה היא בעלת השפעה על טכנולוגיה אבל גם מושפעת ממנה. חדשנות טכנולוגית לא רק משנה את הנושאים, היעדים והנסיבות אלא גם את אופני הרגולציה ואת הכלים שלה.[199]

רגולציה, או אסדרה, ״היא כיום הגישה המרכזית של המדינה המודרנית להכוונת שווקים. עם זאת, אין בנמצא פירוש אשר הכל מסכימים עליו ביחס למושג ולתופעה מרכזית וחשובה זו, והמעיין בספרות הדיסציפלינות השונות ימצא לה הגדרות

---

196 R. Baldwin, M. Cave & M. Lodge, "Introduction: Regulation – The Field and the Developing Agenda", *The Oxford Handbook of Regulation* (R. Baldwin, M. Cave & M. Lodge eds., 2010) 3, pp. 4–5.

197 שם, בעמ׳ 12.

198 **פייק ו־וורול**, לעיל הערה 89, בעמ׳ 525.

199 שם.

שונות״.[200] במובן הצר של המונח, הכוונה היא ל״מערכת כללים מחייבים, לה נלווית רשות מפקחת העוסקת בפיקוח על הציות להם ובאכיפתם״.[201]

אם כן, במובן הצר והמשפטי של המונחג, הדגש מושם במרכיב הסמכות של המדינה וביכולות האכיפה שלה, לשם התערבות במשק במטרה להשפיע על התנהגות השחקנים בו.[202] הדגש הזה בא לידי ביטוי בהחלטת הממשלה 2118, העוסקת בהקטנת הנטל הרגולטורי, שם מוגדרת רגולציה כדלקמן:[203]

> רגולציה – חוק או תקנה בת פועל תחיקתי המהווה כלל התנהגות מחייב במסגרת פעילות כלכלית או חברתית, ושהוא בר אכיפה על ידי רשות מינהלית מוסמכת לפי דין. למען הסר ספק, חקיקה בתחום המסים והטלת אגרות או שינויים בשיעורן אינן בגדר רגולציה לעניי החלטה זו.

כאמור לעיל בפרק הדן בהגדרות מרחב הסייבר ואבטחת סייבר בהחלטות ממשלת ישראל,[204] המשתמשים מוגדרים כחלק מהמרחב, ולפיכך, לפי תפיסה זו, גם משתמשים (פרטיים) עשויים להיות מושא לרגולציה של אבטחת סייבר. ואולם, במובן המקובל של רגולציה, היא ״מתבצעת במסגרת יחסים מקצועיים בין רגולטורים למפוקחים״, ומושאי הרגולציה ״הם בעיקר תאגידים, חברות ועסקים, ולא יחידים, שבדרך כלל לא מקובל לראות בהם סובייקט לרגולציה מתמשכת וקבועה״.[205]

אפשר לחלק את צורות האסדרה לשלוש קטגוריות עיקריות – מתן היתרים ורישיונות, נורמות מחייבות ללא צורך בהיתר מוקדם ורתימת השוק.[206]

ברמה המקומית והגלובלית ניכרת התחזקות של המגמה ליישם ״רגולציה הסכמית״, שלפיה הרשות הרגולטורית אינה עושה שימוש באמצעי הכפייה שבידיה בצורה ישירה, אלא בעוד אמצעים אלה נמצאים ברקע, הרגולטור מעדיף להגיע להסכמה עם התעשייה.[207] מגמה זו אף מיושמת לעיתים מראש, כאשר לרגולטור כלל אין אמצעי אכיפה, והאסדרה מבוססת כולה על שיתוף פעולה מרצון של התעשייה. גישה זו היא

---

200 שרון ידין, **רגולציה: המשפט המנהלי בעידן החוזים הרגולטוריים** (2016) (להלן: **ידין**), בעמ׳ 22.

201 שם, בעמ׳ 24.

202 **תורת הערכת השפעות רגולציה (RIA), על פי החלטת ממשלה 4027 מיום 25.12.2011, גרסה 1.0** (2013) (להלן: **מסמך ה־RIA**), ניתן לצפייה באתר: http://www.pmo.gov.il/policyplanning/Regulation/Documents/RIA.pdf.

203 החלטה מס׳ 2118 של הממשלה ה־33, ״**הפחתת הנטל הרגולטורי – דיון בהחלטת שרים לענייני חברה וכלכלה מס. חכ/39 מיום 14.9.2014**״ (2013), בסעיף א׳. ניתנת לצפייה באתר: http://www.pmo.gov.il/policyplanning/Regulation/Documents/dec2118.pdf.

204 ראו לעיל, בסעיף 1 של פרק א.

205 **ידין**, לעיל הערה 200, בעמ׳ 25.

206 **מסמך ה־RIA**, בעמ׳ 70.

207 **ידין**, בעמ׳ 256.

העומדת בבסיס האסדרה המקובלת כיום של אבטחת סייבר בארגונים, באמצעות גופי ה־CERT וגופים מדינתיים אחרים.[208]

רגולציה יכולה להיות גם על דרך של מתן תמריצים וגם על דרך של אסדרה עצמית, דהיינו ״הענקת מעמד לארגון מסוים לקבוע את הכללים לגופים הכפופים לו ולאכוף אותם, ללא התערבות ממשלתית באכיפה״.[209]

בשוק תחרותי אידאלי מתקיימת ״יעילות פארטו״ (Pareto Efficienncy), דהיינו במצב שבו הרווחה של יחיד אינה יכולה לגדול באמצעות הפחתת הרווחה של אחרים, מתקיים מצב שבו כל הצדדים מרוויחים, או לכל הפחות אינם נפגעים, מהקצאה מחדש של משאבים, טובין, נכסים או משינויים בחקיקה. במצב בו לא קיימת יעילות פארטו מתקיים אפוא כשל שוק, שיש בו משום הצדקה להתערבות של המדינה בשוק.[210] כשל שוק כזה יכול לנבוע מארבע סיבות עקרוניות: (1) כוח שוק; (2) החצנות; (3) מוצרים ציבוריים; (4) חוסר או אי־שלמות של מידע.[211]

מן המפורט לעיל ומבחינת שלוש מתוך הסיבות הנ״ל של כוח השוק של יצרניות הטלפון ובמיוחד ספקיות מערכות ההפעלה, ההחצנות השליליות והבעיות, חוסר מידע (לאו דווקא בשל אי־קיומו אלא בשל אי־יכולת לעשות בו שימוש ממשי), עולה המסקנה שאכן מדובר בכשל שוק גם לפי ההגדרה הנ״ל.

הראיתי במאמר זה כי מודל השוק אינו נותן מענה לבעיית האבטחה, דהיינו כוחות השוק לבדם אינם מובילים למצב שבו מתקבלת תוצאה של מתן מענה ראוי לבעיית האבטחה,[212] וכך גם דיסציפלינות משפטיות אחרות.[213] על כן מתן פתרון לבעיית האבטחה בדרך של אסדרה נראה כמוצא אחרון, והשאלה שתידון להלן היא אם אכן אסדרה היא הכלי המתאים לכך ואיזה סוג של אסדרה.

כפי שאראה להלן, אף כי חלק מהמפעילות הסלולריות בישראל מציעות כאמור פתרונות אבטחה (שאינם מספקים), אין מדובר באסדרה עצמית ואין די באסדרה בדרך של הנגשת מידע.

---

208 ראו **תורת ההגנה בסייבר לארגון**, לעיל הערה 19, עקרונות הפעולה של ה־CERT הלאומי, לעיל הערה 183 – הדרישה ל״הסכמה מדעת של הארגון״, וכן עקרונות פעולת ה־CERT האמריקאי: US-CERT About US, ניתן לצפייה באתר: https://www.us-cert.gov/about-us.

209 **מסמך ה־RIA**, בעמ׳ 75.

210 C. Veljanovski, “Economic Approaches to Rgulation”, *The Oxford Handbook of Regulation* (R. Baldwin, M. Cave & M. Lodge eds., 2010) 17, p. 20. המונח ״יעילות פארטו״ קרוי על שם הכלכלן השוויצרי-איטלקי וילפרדו פארטו, והיא מבוססת על שתי הנחות יסוד: (1) היחיד הוא בעל היכולת הטובה ביותר לשפוט את מצב הרווחה שלו; (2) הרווחה הכוללת של החברה תלויה ברווחה של היחידים שמרכיבים אותה. הטענה היא שבחברות מערביות שני עקרונות אלה מתקיימים.

211 שם, בעמ׳ 20–21.

212 לדיון במודל השוק וכשליו, ראו **הבר וז׳רסקי**, לעיל הערה 14, בפרק ד(1) בעמ׳ 31.

213 לעיל, פרק ג.

העיסוק בספרות ברגולציה של מרחב הסייבר מתמקד בעיקר בשני תחומים:[214] (1) התשתית הטכנולוגית של הרשת בהיבטים טכניים, כגון DNS (Domain Name System), תאימות ברמת פרוטוקול ה־TCP/IP (פרוטוקול התקשורת של הרשת) והגישה לרשת (סוגיות כמו network neutrality); (2) התכנים באינטרנט.

בחינה השוואתית שערכו סיבוני וסביליה מלמדת ש״המגזרים הנתונים תחת הנחיות מחייבות״ בארצות הברית, האיחוד האירופי, בריטניה, צרפת, גרמניה וישראל, אינם כוללים את המגזר האזרחי הפרטי, ובדרך כלל גם לא את המגזר האזרחי העסקי, אלא אם כן מדובר בתשתיות קריטיות.[215] במסגרת התווית ״מודל מוצע לרגולציה של מרחב הסייבר בישראל״,[216] סיבוני וסביליה מציעים שלושה רבדים של רגולציה: (1) ״רגולציה עצמית״, מוצעת במסגרת המודל ככזו שתחול על ארגוני ביטחון (צה״ל, שב״כ וכו׳); (2) ״רגולציה מחייבת״, מוצעת ככזו שתושת על ״גופים אשר פגיעה בתשתיות שלהם משמעותה פגיעה חמורה בביטחון הלאומי של ישראל״, דהיינו מתקנים ותעשיות ביטחוניות רגישות, תשתיות קריטיות, ״מגזרי משק החיוניים לרציפות התפקודית בישראל״, ״בעלי עסקים פרטיים החייבים רשיון עסק או אישור ממשרדי התכנון השונים״ ו״מרחב הסייבר בכללותו״, באמצעות ״התערבות נקודתית בצמתי מפתח״ (כגון נותני שירותים של אחסון אתרים במרשתת, מטמיעי מוצרי אבטחה וכו׳); (3) ״רגולציה מבוססת תמריצים״, לשם עידוד מנגנונים של אבטחת סייבר בארגונים השונים.

אף על פי שסיבוני וסביליה עוסקים בהרחבה בסוגיית הרגולציה של מרחב הסייבר, ואף שנושא ה״מכשירים החכמים״ וה־IoT נדון שם, גם חיבור זה עוסק ברגולציה של אבטחת סייבר בארגונים ואינו נותן מענה למגזר האזרחי הפרטי (בניגוד לעסקי) בכלל, ולבעיית האבטחה בפרט.

2. אסדרה עצמית

על פי ההגדרה לעיל של אסדרה עצמית, אין בתחום הטלפוניה הסלולרית ארגון שקיבל מהמדינה מעמד שמאפשר לבצע אסדרה עצמית כזו. עם זאת, מפעילות הסלולר הגדולות מציעות למנוייהן אמצעי אבטחה שונים, שפורטו לעיל.[217] עם זאת, כאמור אין בשירותים הללו כדי לתת מענה לבעיית האבטחה.

אסדרה עצמית גם יכולה להיות כזו שבה התעשייה מכפיפה את עצמה מרצונה לעקרונות הנדרשים ונוקטת את פעולות הדרושות גם ללא ארגון שהגופים הרלוונטיים חברים בו והוא שגורם לחבריו לפעול כאמור. אלא שהציפייה שיצרניות הטלפונים החכמים יקבלו על עצמן את החובה להסדיר את הכשלים, ולו רק את אלה שנוגעים

---

214 **פייק ו־וורל**, לעיל, הערה 90.
215 **סיבוני וסביליה**, לעיל הערה 5, טבלת ההשוואה בעמ׳ 101–102.
216 שם, בפרק ד׳, החל מעמ׳ 120.
217 לעיל, פרק ב, בסעיף 2(א).

לעדכונים של מערכות ההפעלה והתוכנה באופן מקיף, זמין בתדירות הנדרשת ולאורך חיי המכשירים, היא ככל הנראה ציפייה שלא תתממש.

לפי פרסום באתר האינטרנט של BBC מה־31.5.2018, חברת סמסונג זכתה בהליך משפטי שניהל כנגדה ארגון צרכנים הולנדי, אשר טען כי יש להטיל על סמנסונג חובה לעדכן את מערכת ההפעלה במכשירים שלה במשך לפחות ארבע שנים לאחר המכירה, וכן כי סמסונג אינה משחררת עדכונים בתדירות הנדרשת.[218] על פי הפרסום, סמסונג טענה מנגד כי הלקוחות ההולנדים מקבלים עדכוני תוכנה במשך שנתיים מהמכירה, כי מידע על כך נמסר לצרכנים באתר ההולנדי של החברה וכי עדכוני התוכנה מופצים בתדירות ״סבירה״, לאחר שנבדקת התאמתם למכשירים של החברה. במילים אחרות, לאחר קבלת עדכון מגוגל בנוגע למערכת ההפעלה אנדרואיד, סמסונג מחליטה לאילו טלפונים לשחרר עדכון ולאילו לא. בעניין זה ראוי להזכיר את מורכבות העניין, כמפורט לעיל.[219] בהתאם לפרסום, בית המשפט דחה את התביעה כנגד סמסונג בקובעו שטענות ארגון הצרכנות בלתי קבילות, הואיל והן מתייחסות לעניין עתידי. להליך הייתה גם תוצאה חיובית, אם כי היא מוגבלת ביותר במשמעותה מבחינת פתרון בעיית האבטחה. סמסונג, ככל הנראה רק באתר ההולנדי שלה, מפנה כעת לעמוד מדיניות העדכונים שלה, דבר שיצר שקיפות בנוגע לעדכונים, אך כאמור כרגע רק להולנדים.

מדובר בנטל על יצרניות המכשירים שקשה להאמין שהן תקבלנה אותו על עצמן מרצונן. לשם כך יידרשו כנראה הליכים כגון זה שננקט בהולנד, או רגולציה שתחייב אותן לשקיפות באשר למצב עדכוני התוכנה או אף תחייב אותן לבצע עדכוני תוכנה בתדירות גבוהה ולאורך תקופה מסוימת.

מכל האמור לעיל עולה כי אסדרה עצמית, גם במובן של פעולה עצמאית של היצרניות או ספקיות מערכת ההפעלה, אין בה די והיא אינה נותנת מענה לבעיית האבטחה.

3. אסדרה על דרך של הנגשת מידע והנחיות, שיישומן הוא על בסיס התנדבותי

הגישה המקובלת להתמודדות עם הבעיה של אבטחת סייבר בשוק האזרחי, בניגוד לאבטחת סייבר של תשתיות קריטיות,[220] היא גישה של ״חינוך״ המשתמשים באמצעות העמדת מידע ופרסום מדריכים והנחיות. פעולות אלה נועדו להתוות התנהגות שתגביר את המודעות לנושא, והתקווה היא שאימוצה יביא לשיפור במצב האבטחה. אימוץ ההנחיות לפי הגישה הזו הוא על בסיס התנדבותי, ואין אכיפה של היישום שלהן.

---

218 Samsung won’t be forced to update old phones (31/05/2018), ניתן לצפייה באתר: https://www.bbc.com/news/technology-44316364.

219 ראו לעיל, פרק ב, בסעיף 2(ב).

220 ראו **הבר וז׳רסקי**, לעיל, הערה 14 וכן ראו **סיבוני וסבילייה**, לעיל הערה 5, טבלת ההשוואה בעמ׳ 101.

המידע וההנחיות נמסרים על ידי גופי תקינה מדינתיים, רשויות אכיפה וכאלה שיש להן נגיעה לתחום וכן רשויות ייעודיות, כגון ה־NCCIC בארצות הברית (The National Cyberscurity and Communications Integration Center) שכולל את ה־US-CERT (Computer Emeregency Readiness Team),[221] מערך הסייבר הלאומי בישראל,[222] ה־NCSC הבריטי (National Cyber Security Center)[223] וכיוצא באלה.

גופים אלה מרכזים מידע על נוזקות, חולשות ופגיעויות, אירועי סייבר, פתרונות ופעולות נדרשות, ומנגישים אותו למשתמשים.

(א) ארצות הברית

בארצות הברית פרסם ארגון התקינה והטכנולוגיה הלאומי (ה־NIST) מדריך לניהול אבטחת סייבר של מכשירים ניידים במגזר העסקי.[224] מטרת המדריך היא לסייע לארגונים בניהול מרכזי של אבטחת מידע במכשירים ניידים, כגון הטלפון הנייד ומחשבי לוח (שאף הם עשויים כמובן להיכנס להגדרה של ציוד קצה), תוך ציון מפורש שהוא אינו מיועד למחשבים ניידים כמו גם לטלפונים שאינם טלפון חכם (טלפוני ניידים מדורות קודמים). המסמך כולל המלצות לבחירה, הטמעה ושימוש באמצעים וטכנולוגיות של ניהול מרכזי. עם זאת, המסמך לא עודכן מאז שנת 2013, והדבר מדבר בעד עצמו. ייתכן שבתחילת העשור השני של שנות האלפיים עדיין היה מקובל לקבל מכשיר סלולרי מהמעסיק, אבל לקראת סוף העשור המגמה הזו נעלמה כלא הייתה, והמכשירים הם בדרך כלל של העובדים. המסמך גם אינו עוסק בהסדרה של אבטחת סייבר בטלפונים חכמים של הציבור הרחב, במנותק מארגונים.

רשויות וגופים נוספים בארצות הברית עוסקים גם הם בפרסום מדריכים שמטרתם להקנות ידע ולהכווין התנהגות. ה־FTC, כאמור לעיל הנציבות הפדרלית בארצות הברית, שאמונה על הגנת הצרכנים מפני סחר לא הוגן ובלתי תחרותי, פרסמה מדריך להגנת סייבר לעסקים קטנים[225] וכן מדריך להגנת סייבר למלכ״רים וקרנות.[226]

---

221 לעיל, הערה 39.

222 מערך הסייבר הלאומי במשרד ראש הממשלה, ניתן לצפייה באתר: https://www.gov.il/he/Departments/israel_national_cyber_directorate.

223 The National Cyber Secuirty Center הבריטי, ניתן לצפייה באתר: https://www.ncsc.gov.uk.

224 NISTSP 800-124 Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise (June 2013), ניתן לצפייה באתר: https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final.

225 New materials on cybersecurity for small business (18.10.2018), ניתן לצפייה באתר: https://www.consumer.ftc.gov/blog/2018/10/new-materials-cybersecurity-small-business.

226 Cybersecurity Resources for Non-Profits (25.10.2018), ניתן לצפייה באתר: https://www.consumer.ftc.gov/blog/2018/10/cybersecurity-resources-non-profits.

ה־NICC וה־US-CER,[227] הפועלים במסגרת ה־DHS האמריקאי (Department of Homeland Security), הם גורם מרכזי בריכוז מידע בנושא איומים ואבטחת סייבר והנגשתו, לרבות באמצעות מדריכים והנחיות כיצד מומלץ לפעול ואילו פעולות מומלץ לנקוט.[228]

מדובר במדריכים הכוללים הנחיות שהן בחלקן הנחיות התנהגותיות (כגון לא ללחוץ על קישורים ממקורות לא בטוחים, לבחור סיסמאות חזקות וכו׳), אך בחלקן גם טכניות (כגון התקנת תוכנות אבטחה).

(ב) אירופה

מדריכים ואזהרות מפורסמים על ידי גורמים שונים, כמו לדוגמה המשטרה האירופאית (ה־Europol), שמפרסמת מדריכים והנחיות שמטרתם להזהיר משתמשים מפני הסכנות השונות והמתקפות השונות, לרבות באמצעות המכשירים הסלולריים.[229]

ה־NCSC הבריטי, שמפרסם גם הוא מדריכים והנחיות, מדגיש שהמדריכים וההנחיות הללו הם בגדר ייעוץ בלבד, ואין בהם כדי לקבוע סטנדרטים או מדיניות מחייבת.[230] גם כאן ההתמקדות היא בארגונים ולא באבטחת סייבר של יחידים.

ENISA, שהיא הסוכנות של האיחוד האירופאי לאבטחת רשת ומידע, משמשת כמרכז למומחיות בתחום אבטחת סייבר, ובין תפקידיה היא מפרסמת המלצות בנושא.[231] במסמך של הסוכנות שעוסק בשיתוף פעולה בין גופי ה־CERT[232] של

---

227 בארצות הברית משמעות המונח CERT היא Computer Emergency Readiness Team, לעיל, הערה 39.

228 פרסומים באתר ה־NICC תחת "Publications" וכן תחת "Alerts & Tips". ראו גם לדוגמה הקמפיין Stop.Think.Connect של ה־DHS, שנועד להעלות את רמת המודעות של הציבור האמריקאי לסוגיה של אבטחת הסייבר. ניתן לצפייה באתר: https://www.dhs.gov/stopthinkconnect.

229 לדוגמה ראו: Europol, Be Aware of Fake Social Media Accounts and Fake Mobile Apps, ניתן לצפייה באתר: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/be-aware-of-fake-social-media-accounts-and-fake-mobile-apps.

230 ראו באתר ה־NCSC תחת "Guidance" שם נאמר כדלקמן: "We provide *advice*, not standards or policy. And because our guidance is advisory in nature, it provides a sound basis from which to make your own, informed decisions that are right for your organisation", ניתן לצפייה באתר: https://www.ncsc.gov.uk/guidance.

231 "פרסומים" באתר הסוכנות. ראו European Union Agency for Network and Information Secuirty (enisa) – Publications, ניתן לצפייה באתר: https://www.enisa.europa.eu/publications.

232 פירוש המונח, לפי הסוכנות באירופה, הוא Computer Emergency Readiness Team. למרות השוני הקל בין פירוש המונח בארצות הברית (לעיל, הערה 227), הרי שמבחינת המשמעות המעשית התפקוד של הגופים דומה.

מדינות האיחוד מתוארים השירותים שארגוני ה־CERT המדיניים באיחוד נותנים, כבסיס לשיתוף פעולה. אלה כוללים פרסום אזהרות והתראות, וכן "Security-Related Information Dissemination", נוסף על איסוף מידע, ניתוח אירועים ועוד.[233] מדובר בגופים שבין היתר מנחים ומנגישים מידע בנוגע לנוזקות, מתקפות ופגיעויות, למי שצורך את המידע הזה ויכול לעשות בו שימוש.

גם ה־CERT-EU של האיחוד האירופאי מפרסם הנחיות שונות ומאמרים בנושא אבטחת סייבר (White Papers),[234] אך הוא מתמקד באבטחת הסייבר של מוסדות האיחוד.[235]

(ג) איגוד התקשורת הבין־לאומי

ה־ITU (איגוד הטלקומוניקציה הבין־לאומי) הוא סוכנות של האומות המאוחדות, שעוסקת ומתמחה בתחום של טכנולוגיות המידע והתקשורת.[236] סקטור ה־ITU-T (ITU Telecommunication) באיגוד עוסק בלימוד שאלות הקשורות לעניינים טכניים ותעריפים של הפעלת שירותי תקשורת ואמון על הכנת המלצות בנושאים אלה, לשם יצירת סטנדרטים עולמיים בתקשורת.[237] בשנת 2008 פרסם הסקטור המלצות בתחום אבטחת הסייבר.[238] ההמלצות כוללות טקסונומיה של איומי אבטחת סייבר והמלצות, אך זאת מזווית הראייה של ארגונים ורשתות תקשורת, ולא מזו של יחידים או של מכשירי הקצה.

האיגוד עוסק בענייני תשתית, ואף שציוד הקצה הוא מהתשתית מקצה לקצה, ההמלצות מתייחסות בדרך כלל לתקשורת עם ציוד הקצה ולא לפגיעות של ציוד הקצה עצמו.[239] עם זאת לעיתים מתפרסמות גם המלצות ביחס לטלפונים חכמים. בשנת 2017 פרסם הארגון המלצות למניעת botnet[240] מבוססות טלפונים חכמים.[241] ההמלצות

---

233 CERT cooperation and its further facilitation by relevant stakeholders, WP2006/5.1 (CERT-D3), ניתן לצפייה באתר: https://www.enisa.europa.eu/publications/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders.

234 CERT-EU White Papers, ניתן לצפייה באתר: https://cert.europa.eu/cert/newsletter/en/latest_PublicationsAndNewsletters_.html.

235 ראו: CERT-EU About Us, ניתן לצפייה באתר: https://cert.europa.eu/cert/plainedition/en/cert_about.html.

236 International Telecommunnication Unioun (ITU), ניתן לצפייה באתר: https://www.itu.int/en/about/Pages/default.aspx.

237 הנושאים נקבעים על ידי ה־WTSA (World Telecommunication Standardization Assembly), המתכנס אחת לארבע שנים ובסמכותו גם לאשר את ההמלצות של ה־ITU-T.

238 לעיל, הערה 34.

239 ראו גם: Security in Telecomuniccations and Information Technology, ITU-T (2009), ניתן לצפייה באתר: https://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-E.pdf.

240 לעיל, הערה 78.

241 לעיל, הערה 79.

במסמך זה מופנות הן ליצרניות המכשירים והן למשתמשים, והן כוללות, בין היתר, את ההמלצות הבאות: המלצה שלמכשירים תהיה יכולת הצפנת מידע וגישה אליו על ידי המשתמש באמצעות סיסמאות, טביעות אצבע או אמצעים דומים, המלצה למשתמשים להתקין תוכנות הגנה, המלצה שמכשירי הטלפון החכמים יודיעו למשתמש על צריכת הספק מוגברת בלתי רגילה וכיוצא באלה. אין בהמלצות האלה התייחסות לאחת הסיבות המרכזיות לבעיית האבטחה – הסוגיה של עדכוני התוכנה בכלל ושל מערכת ההפעלה בפרט.

(ד) ישראל

גם בישראל הגישה היא של פרסום הנחיות והמלצות. כאמור, בשנת 2017 פרסמה הרשות הלאומית להגנת הסייבר בישראל מדריך ליישום הגנת סייבר, אך מדריך זה מתמקד באבטחת סייבר בארגונים.[242] תורת ההגנה שפורסמה במדריך, כפי שמצוין בה, אימצה את הרעיון של הגנה בשלבים (היערכות והגנה, איתור, הכלה, וההתאוששות) כפי שהיא באה לידי ביטוי ב־Cyber Security Framework של ה־NIST.[243]

ההתמקדות היא בעיקר במידע לארגונים, ולא לציבור הרחב שאינו חלק מהארגונים הללו. גם מהניתוח של סיבוני וסביליה עולה כי אין אסדרה מדינתית בתחום אבטחת סייבר ברובד של האזרח מן השורה. האסדרה חלה על מגזרים העסקיים, משרדי הממשלה ויחידות סמך, תשתיות חיוניות, תעשיות ביטחוניות והמגזר הביטחוני.[244]

מודל האסדרה בתזכיר חוק הסייבר,[245] כפי שהוא בא לידי ביטוי בפרק ד׳ של החוק המוצע, אף הוא מבוסס בעיקרו על הנחיה. במבוא של התזכיר נאמר כדלקמן:

> פרק האסדרה בחוק המוצע עוסק במכלול פעילות הממוקדת במניעה ובהיערכות למתקפות סייבר, על יסוד מנגנוני הנחיה ברמה הלאומית והמגזרית, אשר יאפשרו למדינה לחזק את החוסן המשקי.

הדבר בא לידי ביטוי בסעיף 45 לחוק המוצע, שלפיו מערך הסייבר הלאומי יפרסם הנחיות בתחום הגנת הסייבר, שיגובשו בהתאם לעקרונות המנויים בסעיף 43 של החוק (״עקרונות־על לאסדרה״) וכן לעקרונות המפורטים בסעיף 45. גם בדברי ההסבר לסעיף 48 לחוק מצוין במפורש כי ״הנחת העבודה היא ששמירה על תפקודן התקין של מערכות הארגון ונכסי המידע שלו הם אינטרס של הנהלת הארגון ובעליו. בהתאם לכך, מעת שיש

---

242 לעיל, הערה 19. ההתמקדות בארגונים באה לידי ביטוי גם בהחלטת הממשלה 2443, לעיל, הערה 9.

243 NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (16.4.2018), ניתן לצפייה באתר: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

244 **סיבוני וסביליה**, לעיל, הערה 5, בעמ׳ 81 (תרשים 6), וכן הניתוח בעמ׳ 81–91.

245 לעיל, הערה 1.

בידי הנהלות הארגונים כלים להיערך לאיומי סייבר, ניתן להניח כי ינקטו אמצעים לכך. לכן לא בהכרח נדרשת אסדרה מקום שאין תרחיש נזק אשר אין בו סיכון לאינטרס ציבורי חיוני או אינטרס מוסדר בהתאם לאסדרה מגזרית״.

יש לציין גם שלפי במבואר,[246] עודף מידע שנחשף בפני משתמשים ולקוחות בשל חובת גילוי רגולטורית אינו מביא לתוצאות המצופות, וזאת בשל רתיעה בגלל אי־הבנה ותפיסות לא נכונות, אלא אם כן חובת הגילוי עומדת בקריטריונים מסוימים.[247]

כך או כך, על פי הנתונים שהובאו לעיל ביחס למצב אבטחת הסייבר בטלפונים החכמים, ניכר שאין די בפעולות של הנגשת מידע לשם מתן מענה לבעיית האבטחה.

סעיפים 48 ו־49 לחוק המוצע מאפשרים ל״רשות מאסדרת״, כהגדרתה בסעיף 47 לחוק המוצע,[248] לקבוע הוראות בתחום הגנת הסייבר (בהסכמת ראש מערך הסייבר הלאומי), לסווג את **הארגונים המפוקחים** על ידיה לפי חומרת תרחישי הנזק ועוד.[249] ״שירותי דואר ותקשורת, שירותי בזק ושידורים מסחריים״ כלולים בסעיף 7 של התוספת השנייה לחוק המוצע, במסגרת התחומים המשקיים שבהם פועלות רשויות מאסדרות. שר התקשורת או רשות מאסדרת רלוונטית אחרת בתחום התקשורת, יהיו רשאים לפי החוק המוצע, בהסכמת ראש המערך, לתת הוראות (ולא רק הנחיות) לארגונים מפוקחים בתחום התקשורת.

בעניין זה יש לציין שיצרני הטלפונים החכמים ומערכות ההפעלה, כמו גם מפתחי האפליקציות ואחרים באקוסיסטם, אינם ארגונים המפוקחים על ידי משרד התקשורת. המפעילים הסלולריים ויבואני הציוד הם הגורמים המפוקחים. מצד אחד, סמכות כזו עשויה לכאורה לסייע במתן מענה לבעיית האבטחה בטלפונים חכמים חדשים על ידי מתן הוראות למפעילים וליבואנים, אם כי לא יהיה בה משום מענה לבעיית האבטחה בטלפונים שכבר נמצאים בשוק (בעניין זה דרושה אסדרה ספציפית בדרך אחרת). מן הצד האחר, נראה שהכוונה בתזכיר חוק הסייבר היא למתן הוראות לארגונים מפוקחים כיצד עליהם להתגונן ואילו אמצעים עליהם לנקוט כדי להגן על הארגון, ולא על המוצרים של הארגון, במקרה שבו עסקינן – ציוד קצה. הדברים עולים מדברי ההסבר לחוק בתזכיר, מהוראות כגון סעיף 51 לחוק המוצע בדבר ״מינוי ממונה הגנת סייבר

---

246 Jane Bambauer, Jonathan Loe & Alex Winkelman, “A Bad Education” (Draft, 2016) (להלן: **במבאואר**).

247 שם, הטענה היא שעל חובת הגילוי לעמוד בשלושה קריטריונים (מהותיות, פרופורציונליות והתאמה), על מנת שתהיה אפקטיבית.

248 ״שר, רשות או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים משקיים המופיעים בתוספת השנייה״ (סעיף 47 בחוק המוצע, תזכיר חוק הסייבר, הערה 1 לעיל).

249 ״ארגון מפוקח״ מוגדר בסעיף 1 לחוק המוצע – ״ארגון הפועל בתחום שמפוקח על ידי רשות מאסדרת כמשמעותה בסעיף 47 או על ידי המערך לפי סעיף 57 או 61״.

בארגון מפוקח, אם רמת הנזק בשל איומי הסייבר הנשקפת מפעילותו היא במדרג גבוה״[250] וממסמך השפעת הרגולציה, שמתמקד בבירור באסדרה של הגנה על ארגונים.

נראה אפוא שלא די גם בהוראות החוק המוצע, אם יתגבש להצעת חוק ויחוקק, כדי להביא לאסדרה שתיתן מענה מלא לבעיית האבטחה בטלפונים חכמים בפרט ובציוד קצה בכלל.

(ה) סיכום – אסדרה באמצעות הנחיה והנגשת מידע והטמעתו על בסיס התנדבותי

היעילות של אסדרה בדרך זו של הנגשת מידע מוטלת בספק, נוכח קשיים אחדים שעליה להתגבר עליהם. קושי ראשון הוא היכולת להבין ולהטמיע את ההנחיות, שחלקן הן הנחיות התנהגות כללית וחלקן הנחיות טכניות הדורשות הבנה טכנית וטכנולוגית. הבנה כזו אולי קיימת בארגונים, אבל לא בהכרח אצל יחידים.

קושי נוסף בגישה הזו הוא בכך שהמידע אינו מונגש לציבור בצורת Push, אלא מוטמעת בו הנחת יסוד שהציבור יחפש את המידע הזה, ימצא, יקרא, יפנים ויבצע אותו. הנחה זו דורשת הוכחה, וסביר להניח שמרבית הציבור לא פועל בדרך הזו, ועל כן האפקטיביות שלה נמוכה. קושי אחר הוא בכך שההתמקדות היא כאמור בעיקר במידע לארגונים, ולא בציבור הרחב שאינו חלק מהארגונים הללו.[251]

לדברי במבואר שנזכרו לעיל,[252] עודף מידע שנחשף בפני משתמשים ולקוחות בשל חובת גילוי רגולטורית אינו מביא לתוצאות המצופות, וזאת בשל רתיעה בגלל אי־הבנה ותפיסות לא נכונות, אלא אם כן חובת הגילוי עומדת בקריטריונים מסוימים.[253]

כך או כך, על פי הנתונים שהובאו לעיל ביחס למצב אבטחת הסייבר בטלפונים החכמים, ניכר שאין די בפעולות של הנגשת מידע לשם מתן מענה לבעיית האבטחה.

4. אסדרה באמצעות ״אישור סוג״

על פי החלטה 2443, שכותרתה ״קידום אסדרה לאומית והבלה ממשלתית בהגנת הסייבר״,[254] האסדרה ״תיעשה מתוך כוונה שלא להוסיף למשק עוד רגולטורים, אלא באמצעות העצמה של הרגולטורים הקיימים, וזאת באמצעות מגוון הכלים העומדים לרשותם וחיזוק כלים אלה [...]״.

---

250 לעיל, הערה 6.
251 ההתמקדות בארגונים באה לידי ביטוי גם בהחלטת הממשלה 2443, לעיל, הערה 9.
252 לעיל, **במבואר**, הערה 246.
253 לעיל, הערה 247.
254 לעיל, הערה 9.

שוק התקשורת בישראל בכלל ושוק הרט״ן (רדיו טלפון נייד) בפרט הם מושא לרגולציה של משרד התקשורת.[255] בחקיקה הראשית מוטלות, לדוגמה, מגבלות על יבואנים, מוכרים ומפיצים של טלפונים, כמו גם על מפעילי הרשתות, מלהגביל או לחסום את השימוש באינטרנט באמצעות הטלפון הסלולרי (סעיף 51ג לחוק התקשורת, עם הסייגים בס״ק (ג)). כאמור לעיל, על הטלפון הסלולרי חלה גם פקודת הטלגרף האלחוטי והצווים מכוחה, ונדרש גם לקבל אישור סוג או פטור מצורך באישור סוג לשם יבוא מכשירי קצה אלחוטיים. הפטור מאישור סוג ניתן כאמור לטלפונים חכמים בצורה גורפת, אם מכשירי הטלפון עומדים בדרישות טכניות של תקינה בין-לאומית,[256] אך אין התייחסות בדרישות הטכניות הנ״ל לנושא אבטחת סייבר.

אפשר לעשות שימוש באישור סוג לשם אסדרה של אבטחת הסייבר בטלפונים חכמים ולהביא באמצעותה להסרת שני הכשלים המרכזיים שעלו לעיל – עדכונים של מערכות ההפעלה והתקנתם של אמצעי אבטחת סייבר. אם שני אלה יוצבו כתנאי לקבלת פטור מאישור סוג בצו הפטור,[257] ויכללו גם את פירוט הדרישות המינימליות של תדירות עדכונים, משך הזמן לאספקת עדכונים, שקיפות ופרסום הנתונים הללו באתרי היצרנים,[258] הרי שלא תהיה ברירה בידי היצרנים והיבואנים והם יאלצו לנקוט את הצעדים המתחייבים ולהסיר את הכשלים המרכזיים הללו. לא מן הנמנע שהעלויות של פעולות אלה יושתו על המשתמשים ויבואו לידי ביטוי במחירי המכשירים, אך נראה שהעלות החלופית, של ההחצנות השליליות והסיכונים שיוצרת בעיית האבטחה, גבוהה לאין שיעור. אסדרה בצורה זו עשויה להתגבר על תמרון־החסר של היצרנים מלתת מענה לבעיית האבטחה. עם זאת יש לזכור כי ישראל אינה השוק המרכזי של יצרני הטלפונים החכמים ומערכות ההפעלה, ולא מן הנמנע שיכולתה לכפות בדרך זו פתרון על חברות ענק בין־לאומיות מוטלת בספק.

כך או כך, דרישה כזו עשויה לסייע במתן מענה לבעיית האבטחה בטלפונים חכמים חדשים, אך לא יהיה משום מענה לבעיית האבטחה בטלפונים שכבר נמצאים בשוק. בעניין זה דרושה אסדרה ספציפית בדרך אחרת.

לעיתים, בדגמים חדשים יחסית, מותקנת מראש בטלפונים חכמים תוכנת הגנה Anti-Malwaer ואף פלטפורמת הגנה (שלפי הטענה יש לה רבדים של תוכנה ושל חומרה), כגון Knox, המותקנת בדגמים מסוימים של חברת סמסונג כתוצאה של שיתוף

---

255 משרד התקשורת אף הקים את אגף טכנולוגיות עתידיות וסייבר, העוסק ״בכל הקשור לטכנולוגיות תקשורת עתידיות (טכנולוגיות שעדיין אינן נמצאות בשימוש בישראל), סייבר (אחריות המשרד בתחום הסייבר תגובש בתיאום עם מטה הסייבר הלאומי)״. ראו באתר המשרד, ניתן לצפייה ב: https://www.gov.il/he/Departments/Units//technologie.

256 ראו הדיון לעיל, פרק א, בסעיף 3.

257 **צו 2012,** לעיל, הערה 54.

258 בדומה למה שנעשה בהולנד בעקבות התביעה שהוגשה שם בעניין נגד סמנסוג – ראו לעיל, הערה 218.

פעולה שלה עם חברת MacAfee. לשם לאחסנת קבצים ומידע אפשר לעשות שימוש במחיצה מיוחדת בטלפון, שהגישה אליה היא רק באמצעי ביומטרי (סריקת עין או אצבע), עניין שבפני עצמו מעלה סוגיות של פרטיות ואבטחה, שהדיון בהן חורג ממסגרת מאמר זה.[259] התקנה של תוכנת הגנה כאמור ופלטפורמות כאלה בדגמים חדשים אף היא אינה רלוונטית למכשירים ישנים יותר, שלא יצאו לשוק עם תוכנה הגנה מותקנת מראש. כך או כך, עדיין קיימת הסוגיה של עדכון גרסאות של תוכנת ההגנה והשאלה אם העדכון מבוצע בצורה אוטומטית, או דורש פרואקטיביות של המשתמש וכן עדכון של מערכות ההפעלה. ייתכן שהמגמה של הגנת ציוד קצה באמצעות תוכנות הגנה בענן, בלא שנדרש עדכון מקומי, תיתן מענה לסוגיה הזו, ובאמצעים רגולטוריים אפשר לגרום לכך שפתרונות כאלה יתנו מענה גם למכשירים קיימים. לפי דוח של חברת המחקר פורסטר, מדובר במגמה שהולכת ומתרחבת,[260] אולם לא ניכר שהיא תפסה מקום מרכזי באבטחת סייבר של טלפונים חכמים.

לאסדרה ממשלתית יש יתרונות וחסרונות.[261] להערכתי, יתרונותיה של אסדרה שתעסוק בנושאים כמוצע לעיל גדולים מחסרונותיה, והיא לא תביא לפגיעה בחדשנות וביצירתיות; אולי להפך – יצרני המכשירים ויצרני מערכות ההפעלה יידרשו לחדשנות ויצירתיות כדי לתת מענה לבעיית האבטחה, שהיא בעייה דינמית, המשנה את פניה ומגלה מופעים חדשים ושיטות חדשות ומתוחכמות לתקיפת ציוד קצה וליצירת מתקפות סייבר שטרם נחוו בעבר.

עם זאת, אין להתעלם מהקושי של העמדת דרישה רגולטורית ישראלית מול ענקי הטכנולוגיה השולטים בשוק הטלפונים החכמים. בחודש יולי 2018 קנסה נציבות

---

259 ראה/י למשל מפרט Galaxy S9/S9+ באתר חברת סמסונג תחת הכותרת "Security", ניתן לצפייה באתר: http://www.samsung.com/global/galaxy/galaxy-s9/specs. נכתב שם שתוכנת ההגנה המותקנת עשויה להשתנות ממדינה למדינה בלא הסבר מדוע ומה התוכנות האחרות שיכול ויהיו מותקנות על המכשיר. אין גם התייחסות לעדכוני התוכנה. יש לציין שחוקרים מאוניברסיטת בן גוריון מצאו בעבר בעיות אבטחה ב־KNOX. ראו: Samsung Phone Studied for Possible Security Gap – Israeli Researchers Point to Alleged Vulnerability in Galaxy S4 (23/12/2013), ניתן לצפייה באתר: https://www.wsj.com/articles/samsung-phone-studied-for-possible-security-gap-1387820528.

260 Forrester, Mastering the Endpoint (2017), p.9. ניתן לצפייה באתר: https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/PDFs/McAfee/rp-forrester-mastering-endpoint_Q32017.pdf.

261 ליתרונות וחסרונות של אסדרה ממשלתית, ראו **הבר וז׳רסקי**, פרק ה׳, בעמ׳ 42. אפשר להתגבר על החששות לפגיעה בחדשנות (שם, בעמ׳ 46) על ידי כך שהאסדרה לא תכתיב את ״דרך ההתנהלות״, אלא תדרוש את קיומה של אבטחת סייבר, ועל השוק תוטל החובה לתת את המענה הטכנולוגי ההולם, שלא ייקבע לפרטיו על ידי הרגולטור. ראו גם הסייג לביקורת בעניין הפגיעה בחדשנות (שם, בעמ׳ 47).

האיחוד האירופאי את חברת גוגל בסכום של 4.34 מיליארד יורו (כ־5 מילארד דולר),[262] בשל פעולה של גוגל בניגוד לדיני ההגבלים העסקיים. הטעם לכך היה, שגוגלהטילה מגבלות לא חוקיות על יצרני מכשירים עם מערכת ההפעלה אנדרואיד. הדבר בא לידי ביטוי בדרישתה של גוגל שהיצרנים יתקינו מראש את אפליקציית החיפוש והדפדפן של גוגל (כרום), כתנאי לקבלת רישיון לחנות האפליקציות של גוגל (Play Store). גוגל שילמה להם תשלומים בתנאי שיעשו כן ומנעה מיצרנים שרצו להימנע מכך, למכור מכשירי טלפונים חכמים עם גרסת אנדרואיד שלא אושרה על ידי גוגל (Android Forks). יש לציין שהדבר עומד לכאורה גם בניגוד להצהרת גוגל באתר אנדרואיד, שלפיה "No manufacturer is required to pre-install any Google app on any Android device Ever." עוד יש לציין שמדובר במערכת הפעלה בקוד פתוח, שקוד המקור שלה זמין בחינם לכל אחד להורדה, לקסטומיזציה ולהפצה, מה שאמור לאפשר ליצרנים לבנות טלפונים חכמים בעלות נמוכה ולאפשר גישה לטלפונים חכמים בכל רחבי העולם.[263]

על פי פרסומים שונים, כתגובת־נגד, גוגל עומדת לשנות את תנאי הרישיון של האפליקציות שלה לאנדרואיד באירופה ובכוונתה להתחיל לגבות עבורן תשלום.[264] היצרנים יכולים, בהתאם, למכור טלפונים בלי ה־Play Store וכל יתר האפליקציות של גוגל, למכור טלפונים עם כל האפליקציול של גוגל אך למעט דפדפן כרום וחיפוש או למכור טלפונים עם כל האפליקציות של גוגל מותקנות מראש, כפי שהמצב היום ברוב הטלפונים מבוססי אנדרואיד. הטענה של גוגל היא שהסדרים שהיו לה סייעו לממן את פיתוח אנדרואיד, ולכן עליה להשיג מימון לכך בדרך אחרת. כמו כן פורסם שגוגל עומדת לערער על ההחלטה.

המקרה הנ״ל הוא רק דוגמה למאזן הכוחות ולמאבקים בין האיחוד האירופאי, המייצג 28 מדינות באירופה (כולל בריטניה לפני ה־Brexit), לענקית טכנולוגיה כמו גוגל. קשה להניח שרגולטור ישראלי, גם בשל גודל השוק הישראלי, יוכל לעמוד מול יצרני הטלפונים החכמים ומערכות ההפעלה ולכפות עליהם רגולציה שתיתן מענה מלא לבעיית האבטחה. עם זאת, המקרה של סמסונג והולנד[265] מלמד שגם במדינה קטנה

---

262 Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's serch engine (18/07/2018), ניתן לצפייה באתר: http://europa.eu/rapid/press-release_IP-18-4581_en.htm.

263 Android – Enabling Opportunity, ניתן לצפייה באתר: https://www.android.com/everyone/enabling-opportunity/#encouraging-openness.

264 Jacob Kastrenakes & Nilay Patel, Google will start charging Android device makers a fee for using its apps in Europe (16.10.2018), ניתן לצפייה באתר: https://www.theverge.com/2018/10/16/17984074/google-eu-android-licensing-bundle-chrome-search.

265 לעיל, הערה 218.

אפשר להגיע להישגים מסוימים שיכולים לשפר את מצב בעיית האבטחה, גם אם באופן חלקי.

למרות כל האמור לעיל ביחס ליחסי הכוחות וגודל השוק הישראלי, הרי שבאמצעות רגולציה, דהיינו דרך הדרישה/הפטור בעניין אישור סוג או רגולציה חדשה, יכול משרד התקשורת לכפות דרישות על היבואנים הישראלים. חלק מהפעולות הנדרשות לשם מתן מענה לבעיית האבטחה יכול להתבצע על ידיהם (כגון התקנת תוכנות אבטחה). הדבר דורש בחינה מעמיקה יותר של השאלה אילו אמצעים אפשר לכפות בנסיבות האלה, לאילו כשלים בבסיסה של בעיית האבטחה יינתן מענה ואם התועלת בכך תגבר על חסרונות אפשריים של הטלת העלויות הכרוכות בכך על הצרכנים. שאלות אלו כרוכות בניתוח נתונים שיש לאסוף מהשטח ובמענה לשאלות שהן מעבר להיקפו של מאמר זה ולמחקר העיוני שבבסיסו.

ה. דברי סיכום

ההנחה שאבטחת סייבר של ציוד קצה, יהא זה הטלפון החכם או סנסור ״טיפש״ המחובר לאינטרנט, היא עניין שיש להותירו בידי המשתמש בציוד הקצה, שלעיתים הוא הבעלים שלו ולעיתים קרובות, וביתר שאת בעתיד, הוא אינו הבעלים שלו אלא מקבל אותו כחלק מהשירות שאותו הוא צורך, היא הנחה חסרת יסוד. יתרה מכך, מדובר בהנחה מסוכנת, המסכנת גם את הרשת ומשתמשים אחרים.

המחקר שמאמר זה מבוסס עליו, הוא מחקר עיוני ולא אמפירי, אך הכשלים של אי־עדכון מערכות ההפעלה בטלפונים, אי־התקנת טלאי תוכנה לשיפור האבטחה והשיעור הנמוך של התקנת אמצעי הגנת סייבר בטלפונים חכמים, כמתואר לעיל, מעידים על כך שבאופן חד־משמעי לא ניתן לסמוך על המשתמש לשם מתן מענה לבעיית האבטחה.

מצד אחד, המשתמשים אינם עושים די כדי לאבטח את ציוד הקצה שברשותם ממגוון סיבות שפורטו במאמר, ומן הצד האחר הם עצמם מהווים כשל התורם לבעיית האבטחה. למעשה, אלה שני צדדים של אותו מטבע, שהמסקנה הנובעת ממנו היא שעל גורמים אחרים לשאת בנטל של פתרון בעיית האבטחה.

המסקנה מכך אינה צריכה להיות שהואיל והגורם האנושי הוא מרכזי בבעיית האבטחה, אין מה לעשות בנדון ובעיית האבטחה היא גזרה שיש לחיות איתה ועם ההחצנות השליליות שלה. נהפוך הוא, היותו של הגורם האנושי כשל אבטחתי רק מחזקת את הטענה שאין לתלות את התקווה לפתרון בעיית האבטחה במשתמש.

היכולת בעניין זה מצויה בידי היצרנים והשותפיהם שלהם לאקוסיסטם של ציוד הקצה. הם הגורם היעיל ביותר למתן מענה לבעיית האבטחה, ועליהם אפשר להחיל אמצעים רגולטוריים כדי לגרום להם לפעול בעניין ולהביא לשינוי במצב הקיים. כעולה

מהסקירה במאמר, כיום היצרנים אינם נוקטים את האמצעים הדרושים, בתדירות הדרושה, אין שקיפות בנוגע לעדכוני תוכנה במכשירים חדשים, ובמכשירים ישנים בעיית האבטחה אף מתעצמת.

קשה לראות כיצד יינתן מענה לבעיית האבטחה בלא התערבות רגולטורית Ex-ante. הרגולטור, שממילא מאסדר בישראל את שוק התקשורת ואת ציוד הקצה, הוא משרד התקשורת. כפי שהובהר לעיל, למשרד התקשורת יש את היכולת לעשות שימוש ב״אישור סוג״ כדי לכפות רגולציה של אבטחת סייבר בציוד קצה, ולתת מענה לפחות לשני הכשלים המרכזיים שעומדים בבסיס בעיית האבטחה. כשלים אלה רלוונטיים גם לציוד קצה אחר ואינם ייחודיים לטלפונים חכמים (בהקשר של הבעיה של עדכוני תוכנה ואי-התקנת אמצעי הגנת סייבר).

החוק המוצע בתזכיר חוק הסייבר עשוי לכאורה לאפשר מתן מענה מסוים לבעיית האבטחה. אלא שגם בחוק המוצע ההתמקדות בפרק הרגולציה היא בהנחיה של ארגונים, ולכל היותר במתן הוראות לארגונים, אך זאת רק ביחס להגנת הסייבר במערכות של אותם ארגונים, ולא במוצרים שהם מייצרים או מייבאים. על מנת ליצור בסיס משפטי לאסדרה של אבטחת סייבר במוצרי קצה מכוח חוק הסייבר המוצע, נדרש לבצע בו תיקונים שיאפשרו זאת.

אפשרות אחרת היא עריכת תיקונים בחקיקה הצרכנית, במטרה לגרום לכך שהיצרנים והיבואנים של המכשירים יהיו מחויבים בעדכוני תוכנה, בשקיפות בנושא כלפי הצרכנים או המשתמשים ובהתקנת אמצעי אבטחה ועדכונם.

הגישה הנוהגת של הנגשת מידע על דרך של Pull ולא של Push והתמקדות בארגונים אינה יכולה להביא למתן מענה לכשלים העומדים ביסודה של בעיית האבטחה. אין ספק שיש חשיבות רבה בהעמדת מידע לרשות הציבור, אך הדבר צריך להיעשות בצורת Push, ויש לעבור לחינוך פרואקטיבי של הציבור הרחב, ולא רק של ארגונים.

כאמור לעיל, ייתכן שחלק מהבעיה נובע מחוסר מודעות או אדישות, והסברה פרואקטיבית יכולה לתת מענה לבעיות אלה, כמו גם לבעיית הסקרנות שגורמת למשתמשים ליפול בפח שטומנים להם התוקפים.

שאלת המענה לבעיית האבטחה עשויה גם להיות שאלה של עלות – זו של הנזקים הנגרמים כתוצאה של בעיית האבטחה לעומת העלות של התקנת אמצעי אבטחה ופתרונות לבעיית האבטחה. עם צפי ששיעור הנזק מתקיפות סייבר יגיע ל-6 טריליון דולר בשנת 2021,[266] ועם צפי של גידול עצום בכמות המכשירים והסנסורים הניידים,[267] אפשר להניח שגם מההיבט הזה קיימת הצדקה כלכלית למתן מענה לבעיית האבטחה.

---

266 Cybersecurity Ventures, 2017 Cybercrime Report, ניתן לצפייה באתר: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

כמפורט עוד לעיל במאמר, בשל גודל השוק הישראלי ובשל יחסי הכוחות מול ענקיות הטכנולוגיה השולטות בשוק הטלפונים החכמים, ייתכן שלאחר תהליך בירור עם יבואני המכשירים, יש לבחון מה ניתן לביצוע במסגרת רגולציה מקומית. כך יהיה אפשר להבטיח שרגולציה כזו תהיה ניתנת ליישום מעשי, להבטיח שיתרונותיה יהיו גדוליםמחסרונותיה, ולבחון לאיזה סוג של מענה ולאילו כשלים העומדים ביסוד בעיית האבטחה רגולציה כזו מיועדת.

אם כן, המסקנה המתבקשת היא שעל משרד התקשורת, יחד עם מערך הסייבר הלאומי ואולי גורמים נוספים (כגון משרד החינוך, הרשות להגנת הצרכן ועוד), לתת את דעתם על הסוגיה, שנראה שאינה עומדת על סדר יומם. על כל אלה לנקוט צעדים רגולטוריים משולבים בתיקוני חקיקה ובפעילות הסברה פרואקטיבית, לשם מתן מענה, ולו חלקי, לבעיית האבטחה, על אחת כמה וכמה בשל התחזקות המגמה של יישום האינטרנט של הדברים.

---

267 Dr. Janusz Bryzek, Trillion Sensors Movement in Support of Abundance and Internet of Everything (6.3.2014), ניתן לצפייה באתר: https://cseweb.ucsd.edu/classes/sp14/cse291-b/notes/Janusz_Bryzek_SensorsCon2014.pdf.