14 בנובמבר 2023
א' בכסלו, התשפ"ד

פרטיות במוצרי IoT ביתיים ובבתים חכמים

נוסח מעודכן בעקבות תיקון 13

מבוא

1. אחת התופעות המתפתחות של השנים האחרונות היא העלייה בשימוש במוצרי IoT (האינטרנט של הדברים – Internet of Things) במרחב הביתי, וזאת במסגרת הפיכתם של בתים ל"חכמים".[1]

2. לשימוש במוצרי IoT במרחב הביתי יתרונות רבים. עם זאת, **לשימוש זה עשויות להיות השלכות משמעותיות על פרטיותם של משתמשים, בני ביתם, ושל כל הנכנסים בשערי המרחב הביתי החכם**. כפי שיפורט בהרחבה בהמשך, פעילותו של הבית החכם מחייבת איסוף ועיבוד של מידע אישי רב ורגיש העלול, בין השאר, לדלוף ולהיחשף ברבים. **שימוש במוצרי IoT ביתיים מהווה, הלכה למעשה, הכנסה של מערכות מעקב אל תחומי המרחב הפרטי והאינטימי ביותר של הפרט**, על כל המשמעויות הכרוכות בכך.

3. מטרת המסמך היא לסקור את סיכוני הפרטיות המרכזיים הכרוכים בשימוש במוצרי IoT ביתיים ובבתים חכמים, תוך התייחסות למצב המשפטי החל בישראל, ולהציג את עמדת הרשות בנושא. **המסמך כולל הנחיות והמלצות לחברות המספקות מוצרי IoT ביתיים ושירותים של בית חכם, וכן המלצות לציבור המשתמשים במוצרים ובשירותים אלו.**

רקע

4. ה"אינטרנט של הדברים" הוא מושג המיוחס לשימוש במכשירים חשמליים המצוידים בחיישנים הקולטים ואוספים מידע מהסביבה בה הם נמצאים (כגון נתוני תנועה, טמפרטורה, קול ומיקום), והמעבדים אותו למטרות שונות ולפעולות בעלות השפעה בעולם הפיזי (להלן: 'מוצרי IoT').[2]

5. מוצרים אלו מקושרים לרשת ולמוצרי IoT נוספים בטכנולוגיות חיבור שונות (כגון, Bluetooth, Wi-Fi), באופן המאפשר העברת ועיבוד מידע בהיקף רב ובאיכות גבוהה.[3]

6. בתים חכמים (או בתים מקושרים - Connected Home), הם בתים בהם נעשה שימוש במוצרי IoT ביתיים, המקושרים ביניהם והמחוברים לרשת, למטרות של שליטה ובקרה על המתרחש

---

[1] באתר נציבות הסחר הפדרלית האמריקנית (FTC) בנושא אבטחת מידע במכשירי IOT צוין כי אנליסטים מעריכים שעד שנת 2025, צרכנים ועסקים ברחבי העולם ישתמשו ביותר מ-20 מיליארד מכשירים המחוברים לאינטרנט.

[2] להרחבה ראו: איגוד האינטרנט הישראלי, "האינטרנט של הדברים (IoT) בישראל: תועלות, אתגרים והמלצות מדיניות" (פברואר 2022), (להלן: 'מסמך איגוד האינטרנט הישראלי').

[3] מאפיין זה מוגדר כ"קישוריות". להרחבה ראו: המכון הישראלי לדמוקרטיה **אדם, מכונה, מדינה: לקראת אסדרה של בינה מלאכותית**, 50 (2023).

במרחב הביתי, וזאת באמצעות עזר שליטה ייעודי, כמו הטלפון החכם. הדוגמאות בעניין זה רבות ומגוונות:

> כך, מערכות של בתים חכמים מאפשרות שליטה מרחוק על מוצרי חשמל כגון דודים חשמליים, תנורים, ומזגנים; מאפשרות לסייע בעמידה במטלות הבית באמצעות שימוש במכשירים כגון שואבי אבק רובוטיים ומקררים חכמים; מאפשרות מעקב אחר המתרחש בבית באמצעות שימוש במצלמות מעקב ביתיות ודלתות חכמות; מאפשרות שליטה על שירותי רשת (כגון ביצוע חיפוש מידע ברשת או השמעת מוסיקה) באמצעות עוזרים דיגיטליים כגון Siri או Alexa; וכן מאפשרות לייעל את צריכת החשמל והמים של משק הבית.[4] התקני IoT ייחודיים כגון "צעצועים חכמים" עשויים לשמש, בין היתר, לפיקוח ולבקרה על התנהלות ילדים במרחב הביתי.[5]

7. הטכנולוגיות המתפתחות של השנים האחרונות, כגון טכנולוגיות להעברת מידע בצורה מהירה המאפשרת קישוריות גבוהה בין רכיבים באמצעות רשתות האינטרנט והסלולר, טכנולוגיות מחשוב ענן (Cloud Computing), המאפשרות שימוש קל ונוח בפלטפורמות ענן לאחסון ולשיתוף מידע בהיקף כמעט בלתי מוגבל, וטכנולוגיית הבינה המלאכותית (AI) המאפשרת עיבוד מידע בהיקף עצום (לרבות מידע מסוג נתוני עתק – Big Data) והמשמשת, בין היתר, לעיבוד שפה טבעית (NLP), הביאו לעלייה באיכות ובזמינות השימוש במוצרי IoT במרחב הביתי.

בראייה צופה פני עתיד, סביר להניח כי היקף השימוש במוצרי IoT בכלל, ובבתים חכמים בפרט, ילך ויגבר, על כל המשמעויות הכרוכות בכך, לרבות בכל הנוגע לפרטיות ולאבטחת מידע.

IoT ובתים חכמים – אתגרי וסיכוני פרטיות

8. **שימוש במוצרי IoT בבתים חכמים כרוך מעצם טבעו באיסוף ובעיבוד מידע אישי רב ומגוון שמקורו בהתנהלות היומיומית של אנשים במרחב הביתי.**[6]

9. כך, מוצרי IoT ביתיים רבים מצלמים ומקליטים את הנעשה ברחבי הבית, **וכפועל יוצא מכך אוספים ומעבדים מידע אישי באופן ישיר ורחב היקף.**

> דוגמאות מרכזיות בעניין זה הן מצלמות מעקב ביתיות המצלמות את המתרחש ברחבי הבית באזורים ובמועדים שנקבעו להן, העזרים הדיגיטליים המאזינים באופן קבוע (Always on) למתרחש ברחבי הבית במטרה לקלוט את פקודות המשתמשים ולפעול לפיהן, והצעצועים

---

[4] למגוון דוגמאות לשימוש במכשירי IoT ביתיים ראו רועי צזנה **השולטים בעתיד: הון-שלטון, טכנולוגיה, תקווה**, 62-61 (2017).

[5] Eldar Haber, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399 (2019).

[6] פלדמן והבר טענו בעניין זה כי "IoT is driving society into an "always-on" era in which, more so than ever before, individuals are constantly surrounded by devices that capture their daily routines, including highly sensitive data". ראו: Dan Feldman & Eldar Haber, *Measuring and Protecting Privacy in the Always-On Era*, 35 BERKELEY TECH. L. J. 197, 1999 (2020).

החכמים המחוברים לרשת והמתקשרים עם ילדים, ובמסגרת זו אוספים עליהם מידע כגון שמם, גילם והתחביבים המועדפים עליהם.[7]

10. מוצרי IoT ביתיים אחרים אוספים מידע שמכוחו ניתן, באופן **עקיף**, ללמוד רבות על התנהלות של הפרט, **ולהסיק ממנו מידע אישי "חדש" רב ורגיש על אודותיו.**

כך לדוגמה, מידע הנאסף על-ידי המקרר החכם בדבר מוצרים המאוחסנים בו עלול ללמד על הרגלי התזונה של אדם ומכאן, בין היתר, על מצבו הרפואי או על אמונותיו בכל הנוגע לתזונה, שמירת כשרות, צמחונות וכן הלאה.

מידע על אודות זמני הכניסה והיציאה מדלתות חכמות או על היקף צריכת החשמל בבית בשעות מסוימות עלולים להעיד על מועדי השהות של אדם בביתו. מידע זה עשוי להיות רלוונטי, לדוגמה, למעסיקים, המבקשים לדעת אם אדם אכן עובד מביתו כפי שהוא מצהיר, או שמא הוא נמצא מחוצה לו.

מידע מהטלוויזיה החכמה - כגון נתוני שעות הפעלתה והתכנים המוצגים בה - עשוי ללמד רבות על אורחות חייו של אדם, אמונותיו ותחומי העניין שלו. כך לדוגמה, מידע על אודות שימוש בטלוויזיה במהלך שישי-שבת עשוי ללמד, בסבירות גבוהה, האם מדובר באדם דתי.

11. כפי שעולה באופן מובהק מהדוגמאות, מידע הנאסף במסגרת שימוש במוצרי IoT ביתיים הוא, במקרים רבים, מידע רגיש ביותר העלול להעיד רבות על אדם ועל אורחות חייו.

12. מעבר לכך, **מידע אישי "חדש" עלול להיווצר גם מתוך הקישוריות שבין מוצרי ה-IoT הביתיים ועיבוד המידע הנאסף ממספר מוצרי IoT שונים**.

כך לדוגמה, עיבוד מידע המגיע מנתוני צפייה בטלוויזיה חכמה בשילוב עם מידע המגיע משימוש אדם במוצרי מטבח (כגון נתונים בדבר מועד פתיחת מקרר והמוצר שהוצא ממנו במועד זה), יכול ללמד על מידת ואופן ההשפעה של פרסומות למזון המשודרות בטלוויזיה, על הרגלי האכילה והצריכה של אדם, באופן העשוי גם להעיד רבות עליו ועל אופיו. מידע זה עשוי להיות בעל ערך רב למפרסמים המבקשים לייצר "פרופילים" מדויקים על אודות משתמשים באמצעות כריית ועיבוד מידע על אודותיהם ממקורות שונים.[8]

13. לאור כל האמור, שימוש במוצרי IoT ביתיים יוצר אתגרי וסיכוני פרטיות ייחודיים. אתגרים וסיכונים אלו יפורטו להלן:

---

[7] The Future of Privacy Forum & The Family Online Safety Institute, *Kids & The Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots* (Dec. 2016); Samuel Gibbs, *Privacy fears over 'smart' Barbie that can listen to your kids*, THE GUARDIAN (13, Mar. 2015).

[8] תופעה זו מוגדרת כ"פרופיילינג". להרחבה בנושא ראו: מיקי זר "אנשים שקראו מאמר זה התעניינו גם ב....': על הקשר בין פרטיות לפרופיילינג", **משפט, חברה ותרבות – כרך ב**, 69 (מיכאל בירנהק עורך, 2019).

איסוף ועיבוד מידע אישי ללא יידוע והסכמת לקוחות

א. הסכמה

14. בהיעדר הסמכה בדין, איסוף מידע אישי והשימוש בו יכולים להיעשות אך ורק בהסכמתו של אדם, אשר צריכה להיות הסכמה "מדעת", ואשר יכולה להינתן מפורשות או להילמד באופן משתמע מהתנהגותו.[9] איסוף מידע אישי מחייב את אוסף המידע להציג בפני נושא המידע נתונים שונים בדבר איסוף המידע ואופן השימוש בו.[10] השימוש במידע, לרבות עיבודו, יכול להיות אך ורק למטרה שלשמה ניתנה ההסכמה.[11]

15. **שימוש במוצרי IoT ביתיים מעלה את החשש כי חברות ותאגידים המעניקים שירותים שונים של בתים חכמים יעשו שימוש במידע האישי והרגיש הנאסף על ידי מוצרי הבית החכם למטרות נוספות ושונות מאלו שלשמן ניתנה הסכמת המשתמש – קרי, ללא הסכמה.**

> כך לדוגמה, בשנת 2017 פורסם כי נציבות הסחר הפדרלי בניו-ג'רזי הגיעה לפשרה עם יצרנית טלוויזיות חכמות, לתשלום קנס בסך 2.2 מיליון דולר בגין איסוף מידע ושימוש בו ללא הסכמה. לפי הפרסום באתר הנציבות, **החברה התקינה בטלוויזיות המיוצרות על-ידה תוכנה שאספה נתוני צפייה של 11 מיליון לקוחות, והעבירה מידע זה לצדדים שלישיים (כגון חברות פרסום), ללא יידוע הלקוחות וקבלת הסכמתם לכך**.[12] דוגמה נוספת ניתן לראות בפרסום בדבר הפשרה שהושגה בין ה-FTC האמריקני לחברת אמזון, לפיו **החברה השתמשה במידע שהתקבל ממצלמות אבטחה ביתיות לצרכי אימון האלגוריתם שלה, וזאת מבלי שהיא קיבלה את הסכמת המשתמשים לכך**.[13]

ב. יידוע ושקיפות

16. מטבע הדברים, יידוע על אודות איסוף מידע, כנדרש על-פי הוראות סעיף 11 לחוק הגנת הפרטיות, אמור, ככלל, להיעשות **בטרם** מתן ההסכמה לאיסוף המידע.

עם זאת, יידוע משתמשים על מדיניות איסוף ושימוש במידע על-ידי מוצרי IoT ביתיים ושמירתו במאגרי מידע נעשה, על-פי רוב, באמצעות צירוף פיזי של מסמכי תנאי שימוש

---

[9] סעיף 1 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות' או 'החוק') קובע כי לא יפגע אדם בפרטיות של זולתו ללא הסכמתו. סעיף 3 לחוק קובע כי על ההסכמה להיות "מדעת", ולהתקבל "במפורש או מכללא".

[10] ראו סעיף 11 לחוק הגנת הפרטיות; להרחבה ראו הרשות להגנת הפרטיות בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (יולי 2022).

[11] עיקרון זה מוגדר כ"עיקרון צמידות המטרה". פרופ' בירנהק מציין בעניין זה כי: "לפי עיקרון זה, מותר להשתמש במידע שנאסף למטרה מסוימת, רק לאותה מטרה: השימוש צמוד למטרה". ראו: מיכאל בירנהק **פרטיות חוקתית** (2023), בעמ' 68.

[12] FTC, *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11Million Smart Televisions without Users' Consent*, (Feb. 6, 2017).

[13] Makena Kelly, *Amazon's Ring agrees to pay $5.8 million to settle FTC spying suit / The FTC claims Ring workers and hackers unlawfully spied on customers*, THE VERGE (May. 31, 2023).

ומדיניות פרטיות למכשיר, או באמצעות פרסומם באופן מקוון ללקוחות שרכשו את המכשיר.[14] משמעות הדבר היא שבמרבים רבים, **יידוע לקוחות על מדיניות הפרטיות של מוצרי IoT ביתיים – ובכלל זה פרטים בדבר המידע הנאסף ואופן השימוש בו – נעשה רק לאחר מועד רכישת המוצרים ועם התחלת התקנתם**.

17. בנוסף, מסמכי מדיניות הפרטיות ותנאי השימוש עלולים להיות ארוכים ומנוסחים בשפה משפטית מסורבלת וקשה להבנה. כמו כן, תנאי השימוש עלולים גם להשתנות עם הזמן, באופן המשנה מהותית את מדיניות איסוף המידע והשימוש בו, שלאורה התקבלה ההסכמה המקורית לשימוש במוצר. **מצב עניינים זה מעלה את החשש כי משתמשים במוצרי IoT ביתיים עלולים להתקין ולהשתמש במכשירים האמורים מבלי שהם מבינים את משמעות הדבר בכל הנוגע לפגיעה בפרטיותם או בפרטיות בני ביתם, כגון ילדיהם הקטינים**.

ג. יידוע והסכמה לשימוש בטכנולוגיות של בינה מלאכותית

18. קושי מיוחד בהקשרי הסכמה ויידוע במערכות של בתים חכמים מתקיים ביחס לשימוש מערכות אלו בטכנולוגיות של בינה מלאכותית.

19. ככלל, מוצרי IoT מאפשרים איסוף מידע רחב היקף. על מנת להתמודד עם עומס המידע, ועל מנת להפיק מהמידע את התובנות הנדרשות למימוש מטרות איסופו, גובר הצורך להשתמש בטכנולוגיות של בינה מלאכותית לעיבוד המידע.[15]

20. טכנולוגיות של בינה מלאכותית נועדו לעבד מידע ממגוון מקורות באופן "עצמאי", משתנה, ולעתים שלא על-פי קריטריונים מוגדרים מראש.[16] משכך, **טכנולוגיות אלו מציבות אתגר בכל הנוגע ליידוע נושאי מידע בדבר אופן השימוש שלהן במידע על אודותיהם, וביחס לקבלת הסכמתם לשימוש במידע בנסיבות אלו**.[17]

דלף מידע אישי

21. שימוש במוצרי IoT במרחב הביתי כרוך באיסוף ובשמירה של מידע אישי רב ורגיש שמקורו בהתנהלות במרחב הביתי והפרטי. בנסיבות אלו, דלף מידע ממוצרים אלו או ממאגרי המידע בהם נשמר המידע, עלול להוות פגיעה קשה בפרטיותו של כל מי שמתגורר באותו בית.

---

[14] פרסום זה יכול להיעשות במסגרת הפנייה לאתר אינטרנט של החברה המספקת את המוצר או לאפליקציה ייעודית במסגרתה מפורטים תנאי השימוש במוצר ומדיניות הפרטיות שלו.

[15] המכון הישראלי לדמוקרטיה, לעיל ה"ש 3, בעמ' 51 ; צזנה, בעמ' 206.

[16] טכנולוגיות מסוג זה הוגדרו לא פעם כ'קופסה שחורה'. מושג זה מתייחס למנגנון אשר הקלט והפלט שלו ידועים, אולם דרך פעולתו לא ידועה. ראו : נתי פרל "החלטה על קיומו של 'חשד סביר' בעולם ה- Big-Data : מהנמקה אנושית לאלגוריתם לחיזוי פשיעה" **דין ודברים** יד 237, 253 (2019).

[17] להרחבה ראו : הרשות להגנת הפרטיות, מסמך חובת היידוע, לעיל ה"ש 10, סעיפים 18-22.

22. דלף מידע עלול להיגרם, בין היתר, כתוצאה מחדירה של גורמים לא מורשים למוצרי ה-IoT או למאגרי המידע.[18] חדירות שכאלו עלולות להיגרם כתוצאה מהחיבור של מוצרי ה-IoT הביתיים לרשת, ובשל אי-אבטחה מספקת של המוצרים ומאגרי המידע.[19]

23. דלף מידע (וחשיפתו ברבים) עלול להיגרם, בין היתר, גם כתוצאה מהעברתו של המידע הנאסף על-ידי מוצרי ה-IoT הביתיים לאחסון בשירותי ענן, ולשימוש בו במסגרת "אימון" טכנולוגיות של בינה מלאכותית שנועד, על-פי רוב, לשיפור וייעול פעילות המוצרים.

כך לדוגמה, על-פי פרסומים שונים, תמונות של אישה יושבת בשירותים - אשר צולמו על-ידי שואב אבק רובוטי שפעל בביתה ושלצורך פעילתו צילם את המרחב הביתי - דלפו ופורסמו ברשת. מתוך התחקיר שנעשה עלה כי שואב האבק שלח את התמונות לשירותי ענן לצורך אחסונן, משם הועברו התמונות לחברה המתמחה בעיבוד התמונות לצורכי אימון בינה מלאכותית, ובסופו של דבר הודלפו התמונות לעמוד פייסבוק על-ידי עובדי החברה.[20]

24. לאור רגישותו של המידע הנאסף במסגרת שימוש במוצרי IoT ביתיים, אירוע של דלף מידע ממוצר IoT ביתי בודד (או ממאגר מידע בו שמור המידע הנאסף על ידי המכשיר) עלול לגרום לפגיעה קשה בפרטיות.

ואולם, מעבר לכך, מכיוון שבמרבית המקרים מוצרי ה-IoT הביתיים מקושרים האחד לשני לשם העברת ושיתוף מידע ביניהם, ולאור כך שבמקרים רבים ההתחברות למערכות הבקרה והשליטה נעשית על-ידי משתמשים באמצעות חשבונותיהם ברשתות חברתיות, **הרי שמוצר IoT אחד עלול לשמש מעין "שער כניסה" (Gateway) למוצרי IoT ביתיים אחרים ולמאגרי מידע נוספים, וכן לחשבונות משתמשים ברשתות חברתיות**.

פריצה למוצר IoT אחד עלולה אפוא להביא לדלף מידע ממוצרי IoT נוספים, ממאגרי מידע ומחשבונות של רשתות חברתיות. מצב זה עלול להביא לדלף ולחשיפת מידע אישי רגיש בהיקף נרחב, ומכאן לפגיעה קשה ביותר בפרטיות משתמשים.

25. על-פי ההגדרה בסעיף 3 לחוק הגנת הפרטיות, נתונים הנוגעים לאדם מזוהה או לאדם הניתן לזיהוי מהווים "מידע אישי". מעבר לכך, מידע מסוגים שונים, לרבות כזה העלול להיאסף על אדם בביתו – כגון מידע על אודות צנעת חיי המשפחה של אדם, צנעת אישותו ונטייתו המינית, וכן מידע המתייחס למצב בריאותו, ומידע על דעותיו הפוליטיות, אמונתו הדתית והשקפת עולמו – מהווים על-פי ההגדרה שנחקקה בתיקון מס' 13 לחוק - 'מידע בעל רגישות מיוחדת'. כפי שיפורט, בעלי שליטה במאגר מידע, שבמאגריהם נשמר מידע אישי על אודות אדם,

---

[18] ממחקר שבוצע בבריטניה בשנת 2021 נמצא שמכשירי IoT ביתיים עשויים להיחשף לכ-12 אלף ניסיונות חדירה בשבוע. לכתבה בנושא ראו: Kristine Lazar, *On Your Side: Prevent hack attacks on your 'smart home' devices*, CBS Los Angeles (Feb. 1, 2023).

[19] שימוש בחיישנים פשוטים, זעירים מבחינה פיזית, וזולים מבחינה כלכלית, מגביר את הסיכון לפגיעה בפרטיות בכלל, ולדלף מידע בפרט, וזאת מכיוון שניתן לחדור למרבית חיישנים אלו בקלות יחסית.

[20] גלי פיאלקוב "שואב אבק רומבה צילם אישה בשירותים והתמונה הגיעה לפייסבוק" **אנשים ומחשבים** (22.12.2022).

מחויבים באבטחת המידע במאגר, בהתאם לכלל הדרישות הקבועות בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע").

מעקב (צילום משתמשים והאזנה להם) ללא הסכמה

26. כאמור, חלק ממוצרי ה-IoT הביתיים, כגון מצלמות ביתיות, מכשירי מוניטור בחדרי תינוקות ועזרים דיגיטליים, נועדו לצלם, להאזין ולהקליט את הנעשה ברחבי הבית החכם, וזאת בהתאם לרצון ולצרכי משתמשים.

27. עם זאת, **בשל כשלי אבטחה, גורמים עבריינים עלולים לפרוץ למוצרים אלו ולהשתלט עליהם מרחוק, במטרה לעקוב אחר משתמשים בתחומי המרחב הביתי, וזאת ללא ידיעתם או הסכמתם, ותוך פגיעה קשה בפרטיותם**.

הדוגמאות בעניין זה רבות ומגוונות. כך לדוגמה, באוקטובר 2022 הרשיע בית משפט השלום בתל-אביב אדם אשר, בין היתר, פרץ למצלמות אבטחה ביתיות לשם איתור וצפייה בתכנים אינטימיים.[21] דוגמה מרכזית אחרת היא פריצה למוניטורים "חכמים" המחוברים לרשת והמצוידים במצלמה ומיקרופון, לשם צילום, האזנה ויצירת קשר עם קטינים.[22]

28. **מעקב פסול וללא הסכמה יכול להתבצע גם על-ידי גורמים לא מורשים מתוך החברות המספקות שירותים של בית חכם**.

כך לדוגמה, במאי 2023 פורסם כי ה-FTC האמריקני הגיע לפשרה עם חברת אמזון על תשלום קנס בסך 5.8 מיליון דולר וזאת, בין היתר, בגין כך שלא מנעה מגורמים לא מורשים להשתמש במידע שנאסף ממצלמות של החברה המותקנות על עינית הדלת (Amazon Ring), ואפשרה מצבים בהם עובדי החברה צפו בחומרים המצולמים, ללא הרשאה או הסכמה.[23]

29. צפייה באדם ללא ידיעתו וקבלת הסכמתו לכך, מהווה פגיעה בפרטיות. ביצוע מעקב ללא הסכמה אחר אדם מהווה הפרה של סעיף 2(1) לחוק הגנת הפרטיות. צילום ללא הסכמה של אדם ברשות היחיד מהווה גם הפרה של סעיף 2(3) לחוק. בכל הנוגע להרשאות גישה למאגרי מידע, תקנות אבטחת מידע מחייבות בעלי שליטה במאגרים לקבוע הרשאות גישה למאגר המידע ולמערכות המאגר ואת אופן הזיהוי והאימות של בעלי ההרשאות, וזאת בהתאם להגדרות תפקיד ורמות האבטחה החלות על המאגר.[24]

---

[21] לפי הפרסום, במסגרת זו צפה הנאשם באחת מבנות המשפחה כשהיא מתהלכת בביתה ללא בגדים. במקרה אחר חדר למצלמה וצפה בבני זוג מקיימים יחסי מין, ובאישום אחר תיעד קטין כשהוא עירום. ראו: גלעד מורג "15 חודשי מאסר למתכנת שפרץ למצלמות אבטחה ותיעד נשים במצבים אינטימיים" **ynet** (26.10.22).

[22] איגוד האינטרנט הישראלי, לעיל ה"ש 2, בעמ' 46; Amy B. Wang, *'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say*, THE WASHINGTON POST (Dec. 20, 2018); Brooke Kato, *My baby cam was hacked — it was terrifying for me and my infant son*, NEW YORK POST (May. 9, 2023).

[23] ראו לעיל ה"ש 13.

[24] ראו לדוגמה תקנה 8 לתקנות אבטחת מידע.

פגיעה בפרטיות אורחים ונותני שירותים במרחב הביתי

30. שימוש במוצרי IoT ביתיים ללא יידוע מספק של הלקוחות המשתמשים בהם, עלול להביא לכך שמידע על אודות גורמים שאינם נחשבים לקוחות השירות (קרי גורמים חיצוניים שאינם מתגוררים בבית כגון אורחים ונותני שירותים) ייאסף, יעובד ואף יועבר לגורמים שלישיים (כגון חברות פרסום), מבלי שהם מודעים לכך, וללא קבלת הסכמתם.

כך לדוגמה, אדם העוסק בניקיון בתים עשוי להיות מצולם על-ידי מצלמה ביתית בזמן עבודתו בבית לקוח, באופן החושף אותו למעקב מקוון מצד בעלי הבית ובאופן המביא לאיסוף מידע על אודותיו ושמירתו במאגר מידע, וכל זאת מבלי שהוא מודע לכך, ומבלי שהוא נתן הסכמתו לצילום ולשימוש במידע אישי הנוגע אליו. דוגמה אחרת עשויה להיות קטינים המתארחים בבית חבריהם, כשבעת האירוח הם מצולמים ומוקלטים על-ידי מוצרי IoT ביתיים, וזאת ללא ידיעתם או ידיעת הוריהם.

31. שימוש במוצרי IoT ביתיים ביחס למי שכלל אינם מודעים לאיסוף ולשימוש שנעשה במידע האישי אודותיהם עלול להוות הפרה של הוראות סעיף 2(1) לחוק הגנת הפרטיות, האוסר על בילוש או התחקות אחרי אדם ללא קבלת הסכמתו לכך, הפרה של סעיף 2(2) האוסר על האזנה אסורה אם מדובר במוצרי IoT המקליטים קול, וכן הפרה של סעיף 2(3) האוסר על צילום ללא הסכמה של אדם כשהוא ברשות היחיד.

איסוף והחזקת מידע עודף

32. כחלק מפעילותם עלולים מוצרי IoT לאסוף ולהחזיק מידע עודף שאינו נדרש לשם השירות או הפעולה להם הם נועדו.

כך לדוגמה, עוזרים דיגיטליים כגון Siri או Alexa, המאזינים באופן קבוע למתרחש במרחב הביתי ואשר אמורים להתחיל לפעול ולהקליט את המתרחש בבית רק עם קליטתן של מילות הפעלה מסוימות, עלולים לטעות בזיהוי מילות ההפעלה האמורות, ומכאן להקליט שיחות גם במצבים בהם לא התבקשו לעשות כן, ובאופן שאינו נדרש.[25]

33. נקודה זו נכונה במיוחד בכל הנוגע להחזקת מידע ללא הגבלת זמן. כך לדוגמה, בחודש מאי 2023 פורסם כי חברת אמזון תשלם קנס בסך 25 מיליון דולר בגין שמירת הקלטות קול של ילדים, אשר הוקלטו במסגרת שימוש בעוזרת הדיגיטלית 'אלקסה', וזאת ללא הגבלת זמן, ושלא לצורך מימוש המטרה שלשמה נאסף המידע מלכתחילה.[26]

---

[25] עידן בן טובים "אלקסה הקליטה בחשאי שיחה פרטית של משתמש ושלחה אותה לעובד בחברה שלו" GEEKTIME (27.5.18); https://moniotrlab.khoury.northeastern.edu/publications/smart-speakers-study-pets20/.

[26] FTC, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*, (May. 31, 2023)

34. בעניין זה יובהר כי איסוף והחזקת מידע עודף שאינו נדרש למטרת השירות עלולים, במקרים מסוימים, להפר את הוראות סעיף 2(9) ו-סעיף 8(ב) לחוק הגנת הפרטיות.[27]

המלצות למשתמשים במערכות ומוצרי "בית חכם"

35. מוצרי IoT ביתיים עלולים לאסוף מידע אישי ואינטימי רגיש ביותר על התנהלותכם והתנהלות בני משפחתכם בין קירות הבית ולהשתמש בו למטרות שונות, כולל מטרות מסחריות, גם במצבים שלא שיערתם בדעתכם. במצבים מסוימים, מידע שכזה עלול גם להיחשף ברבים.

36. בשל החשש לצילום ולהקלטה של אורחים או נותני שירותים ברשות היחיד ללא ידיעתם ותוך ביצוע עבירה לפי סעיף 2(3) לחוק הגנת הפרטיות, **ראוי ליידע את כלל באי הבית בדבר השימוש במוצרי IoT ביתיים העלולים להקליט או לצלם אותם ברשות היחיד, וזאת במיוחד במצב בו הצילום וההקלטה נעשים בחדרי שירותים ומקלחות**. יידוע שכזה יכול להיעשות בעל-פה או בדרכים אחרות.[28]

37. ראוי להימנע מהתקנת מוצרי IoT בעלי יכולת צילום והקלטה בחדרי השינה של הבית או בחדרי שירותים ומקלחות, שכן המידע הנאסף במרחבים אלו הוא בעל פוטנציאל לפגיעה ברף הגבוה ביותר בפרטיותו של אדם, והסיכון לפגיעה שכזו מתעצם בהינתן שהמידע המצולם והמוקלט נשמר במאגרי החברה המספקת את המוצר.

38. בעת הגדרת מרחבי הפעילות של מוצרי IoT ניידים (כגון שואבי אבק רובוטיים) ניתן להגביל את תנועתם וימנע מהם לפעול במרחבים ביתיים רגישים.

39. בעת התקנת מערכות ומוצרי בית חכם הקפידו לשנות את סיסמאות ברירת מחדל של המכשירים לסיסמאות חזקות וייעודיות, והקפידו לעדכן ולשנות סיסמאות אלו מעת לעת.

אם מוצרי ה- IoT הביתיים שלכם מחוברים לרשת באמצעות Wi-Fi, הקפידו כי סיסמת הכניסה לרשת הביתית תהא סיסמה חזקה. הקפידו גם שלא לשתף סיסמה זו עם גורמים שאינכם מכירים או בוטחים בהם.

בעת הגדרת סיסמאות הקפידו שלא להשתמש בנתונים ידועים או פשוטים לגילוי (כגון תאריך לידה, מספר טלפון נייד, שמות ילדיכם או שמות חיות מחמד שברשותכם).

---

[27] להרחבה ראו: הרשות להגנת הפרטיות "צמצום מידע (Minimization Data) - מסמך מדיניות" (25.3.2021).

[28] על-פי סעיף 18 לחוק הגנת הפרטיות, פעולה של צילום אדם ברשות היחיד ללא ידיעתו והסכמתו עשויה להיות מוגנת מבחינה משפטית, אך זאת רק בנסיבות בהן הצילום נעשה מתוך חובה חוקית, מוסרית, חברתית או מקצועית, או כאשר הוא נעשה לשם הגנה על עניין אישי כשר של המצלם, וכל זאת רק כשהצילום היה נדרש ומידתי בנסיבות העניין.

40. בעת רישום והתקנה של מערכות בית חכם, הימנעו מלקשר מערכות אלו לחשבונותיכם שברשתות חברתיות.

41. בעת רכישת מוצרי IoT ביתיים:

- העדיפו רכישה של מוצרים מחברות המבטאות הכרה בחשיבות של הגנה על פרטיות ואבטחת מידע במוצריהן;
- העדיפו רכישה של מוצרים מחברות המציעות הגנת פרטיות וסייבר מתקדמת. כך לדוגמה, העדיפו מוצרים המקפידים על הצפנת המידע הנאסף, והדורשים אימות דו-שלבי כדי לגשת לאפליקציות התפעול של המוצרים;
- בחנו את מדיניות הפרטיות של המוצרים השונים המוצעים בשוק, והעדיפו רכישה של מוצרים המאפשרים לכם שליטה משמעותית ככל הניתן במידע הנאסף.

42. הקפידו לבצע עדכוני תוכנה למוצרי ה- IoT הביתיים בהתאם להוראות היצרן.

43. עשו שימוש במוצרי ה-IoT הביתיים רק בעת הצורך, והקפידו לכבות מכשירים אלו כאשר הם אינם נדרשים.

44. חלק ממוצרי ה-IoT יכולים לפעול באופן לא מקוון וללא העברת מידע ברשת. מוצרים מסוימים מאפשרים גם להגביל את העברת המידע ליצרן. שקלו ברצינות לעשות שימוש באפשרויות אלו.

45. שליטה מרחוק במוצרי ה-IoT הביתיים חושפת את המשתמשים לאירועי חדירה על ידי גורמים לא מורשים למוצרים ומגבירה את הסיכון לפגיעה בפרטיות. לפיכך, שקלו היטב האם ובאיזו מידה תרצו להשתמש באפשרות זו.

46. ככל שהדבר אפשרי, מומלץ להתקין תוכנת אנטי וירוס על מוצרי ה-IoT בטרם חיבורם לרשת.

47. עשו שימוש בזכותכם לעיין במידע על אודותיכם שנשמר במאגרי המידע של החברות המספקות עבורכם את שירותי הבית החכם. אם נתקלתם במידע שאינו נכון, מדויק או שלם, זכותכם לפנות בבקשה למחיקתו ממאגרי החברה.

<u>הנחיות והמלצות לחברות המספקות שירותי ומוצרי "בית חכם"</u>

<u>אבטחת מידע</u>

48. ככלל, חברות המספקות שירותים ומוצרים של בית חכם (אם במסגרת הספקת מוצר אחד ואם במסגרת שירות המאגד מספר מוצרי IoT ביתיים) שבמסגרתם נאסף מידע אישי הנשמר במאגרי החברה המספקת, הן בעלות השליטה במאגרים, לפי חוק הגנת הפרטיות, ביחס לכלל

המידע האישי הנאסף על ידי מוצריהן ונשמר אצלן, על כל המשתמע מכך. בין היתר חלה על חברות אלו החובה לאבטח את מאגריהן בהתאם לכלל הדרישות הקבועות בתקנות אבטחת מידע.[29]

49. כפי שפורט קודם לכן, שימוש במוצרי IoT ביתיים ובבתים חכמים מביא לאיסוף מידע אישי ואף מידע בעל רגישות מיוחדת בהתאם להגדרה החדשה בחוק, על בני הבית ועל אלו הפוקדים אותו. מידע זה כולל, מעצם טבעו, מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד. מידע זה כולל, על-פי רוב, גם מידע ממנו ניתן ללמוד, בקלות יחסית, על מצב בריאותו של האדם ועל מצבו הכלכלי, על הרגלי הצריכה שלו, על אישיותו, דעותיו הפוליטיות, אמונותיו הדתיות, וכן הלאה.

50. בשל כך, ולאור הקבוע בתוספת הראשונה לתקנות אבטחת מידע, **מאגרים בהם מידע הנאסף ממוצרי IoT ביתיים אצל החברה המספקת, הם מאגרי מידע שחלה עליהם רמת האבטחה הבינונית לפי התקנות. עם זאת, מאגרים שכאלו, אשר מוחזק בהם מידע על 100,000 איש ומעלה, או שמספר בעלי ההרשאה להם עולה על 100, הם מאגרים אשר חלה עליהם רמת האבטחה הגבוהה, וזאת בהתאם לאמור בתוספת השנייה לתקנות.**[30]

51. לאור החשש לשימוש פסול במידע על-ידי בעלי הרשאות למאגרים, על החברות לפעול להסדרת והגבלת הרשאות הגישה של עובדיהן למאגרי המידע ולמוצרי הבית החכם, והכל כמפורט בתקנות 7 עד 11 לתקנות אבטחת מידע.

52. בנוסף, על-פי האמור בתקנה 14 (ג) לתקנות אבטחת מידע, על החברות לעשות שימוש באמצעים שמטרתם לזהות את המשתמשים, ואשר מאמתים את הרשאתם לביצוע פעילות מרחוק במאגרי המידע ואת היקפה, כגון על ידי קביעת סיסמאות כניסה חזקות ומורכבות למערכות ולמוצרי הבית החכם (להבדיל מסיסמאות פשוטות וגנריות).

53. כמו כן, לאור סיכוני הפרטיות שפורטו לעיל, מומלץ כי חברות יפעלו לצמצום סיכונים אלו באמצעים ותהליכים שונים, כגון:

- הטמעת תהליכים של הנדסת פרטיות (Privacy by Design) ותפיסה של "פרטיות כברירת מחדל" (Privacy by Default), שמשמעותם עיצוב מערכת הבית החכם להגנה

[29] חובות אבטחת המידע לפי התקנות חלות גם על גורמים המחזיקים במאגר המידע, בהתאם להגדרת "מחזיק" בחוק הגנת הפרטיות, כגון ספקי שירות ענן וכו' (ראו תקנה 19 לתקנות אבטחת מידע).

[30] יובהר, כי גם לאחר כניסת תיקון מס' 13 לחוק לתוקפו, רמת האבטחה של מאגרי מידע לעניין תקנות אבטחת מידע, עודנה נקבעת על פי האמור בתוספת הראשונה ובתוספת השניה לתקנות אלו. ההגדרות לרמות האבטחה הנכללות בתוספת השלישית לחוק (אשר נחקקה בתיקון מס' 13), רלוונטיות אך ורק לעניין סכום העיצום הכספי שניתן להטיל בהתאם להוראות התוספת השלישית.

אופטימאלית על הפרטיות ולצמצום איסוף המידע ועיבודו למינימום ההכרחי, כבר משלב התכנון המוקדם ולאורך כל מחזור החיים של איסוף המידע והשימוש בו.[31]

על-פי תפיסה זו, על חברות להגדיר, מלכתחילה, את הגדרות השימוש במוצרי ה-IoT הביתיים, באופן שיאפשר הגנה חזקה יותר על פרטיות משתמשים.

דוגמה ליישום תפיסה זו היא הגדרה מלכתחילה של "בידוד" מוצרי ה- IoT ברשתות מוגנות ונפרדות משלהם, באופן שיצמצם את אפשרות החדירה ממכשיר אחד למשנהו.

- שימוש באמצעים לחיזוק ההגנה על המידע האישי הנאסף במסגרת שימוש במוצרים אלו (כגון שימוש בכלים להצפנת המידע ותעבורת התקשורת אל המוצר וממנו, ובכלים להתממת המידע). בעניין זה יובהר כי תקנה 14(ב) לתקנות אבטחת מידע קובעת את החובה לוודא כי העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

- פישוט אמצעי השליטה של משתמשים במידע הנוגע אליהם ובהגדרות ההפעלה של מוצרי הבית החכם;

- עדכון משתמשים פוטנציאליים, בטרם רכישת המוצר או השירות, בדבר סיכוני הפרטיות ואבטחת המידע הכרוכים בשימוש במוצרי IoT ביתיים.[32]

- קביעת נוהל לשליחת הודעת תזכורת למשתמשים לעדכון סיסמאות כניסה למוצרים.

דגש מיוחד ראוי לשים בהקשרים האמורים על "צעצועים חכמים" ומוצרי בית חכם המיועדים לשימוש ילדים.

54. בנוסף, הרשות להגנת הפרטיות מבקשת להדגיש כי עריכת תסקיר השפעה על פרטיות בשלב מוקדם של תכנון מערכות המידע הינה דרך יעילה ואפקטיבית למזער את הסיכון לפגיעה בפרטיות במסגרת מתן שירותי בית חכם.[33] עריכת תסקיר שכזה היא חלק מתפיסה רחבה יותר של עיצוב לפרטיות.[34] הרשות מבקשת להדגיש בהקשר זה גם את התועלת שבמינוי ממונה הגנת פרטיות בארגון, שבין יתר תפקידיו, הינו גם הגורם המתאים והיעיל לבחינת הצעדים הננקטים בארגון למזעור הסיכון לפגיעה בפרטיות.[35]

---

[31] הרשות להגנת הפרטיות "עיצוב לפרטיות (Privacy By Design)" (אוגוסט 2021).

[32] המלצה זו מתיישבת עם האמור בטיוטת הנחייה מטעם הרשות להגנת הצרכן ולסחר הוגן, לפיה קמה חובה לגלות לצרכן, בטרם רכישה של מוצר IoT, כי מדובר במוצר שעלול להיות מנוצל לרעה על ידי גורם זדוני לצורך ביצוע תקיפת סייבר. ראו: הרשות להגנת הצרכן ולסחר הוגן "טיוטת הנחיה: חובת גילוי לגבי סיכוני מוצרי IoT "האינטרנט של הדברים" (אוגוסט 2022).

[33] ראו מדריך עזר לביצוע תסקיר השפעה על הפרטיות שפרסמה הרשות להגנת הפרטיות (אוגוסט 2021).

[34] דוגמה לעיצוב לפרטיות בהקשר זה ניתן לראות בתכנון מערכת למפגש וירטואלי בין מטופל למטפל המציעה למטופל, עם התחלת המפגש ובאופן אוטומטי, להשתמש ברקע המטשטש את אפשרות הצילום של כל המתרחש מאחוריו.

[35] להרחבה ראו מסמך "מינוי ממונה הגנה על פרטיות בארגון ותפקידיו", מטעם הרשות להגנת הפרטיות (ינואר 2022).

חובת היידוע

55. **על חברות המספקות שירותים של בית חכם, והאוספים ומעבדים במסגרת זו מידע אישי, להקפיד לעמוד בחובת היידוע, כנדרש על-פי הוראות סעיף 11 לחוק הגנת הפרטיות**. חובה זו חלה בשלב איסוף המידע גם על גורמים האוספים מידע אישי באמצעות מערכות המבוססות על טכנולוגיה של בינה מלאכותית.

56. לשם כך, על חברות להקפיד להציג בפני משתמשים נתונים על המטרה לשמה מבוקש המידע, למי יימסר המידע (כגון ספקים, חברות למתן שירותי ענן, גורמים מסחריים וכו'), את פירוט מטרות המסירה האמורה, וכן את תוצאות אי-ההסכמה לאיסוף המידע. בנוסף, יש ליידע את המשתמשים בדבר שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עמו, וכן ליידע אותם על קיומן של זכות עיון במידע האישי לפי סעיף 13 לחוק, ובדבר הזכות לבקש את תיקון המידע לפי סעיף 14 לחוק. יש להקפיד על כך גם בכל הנוגע לצעצועים חכמים ומוצרי בית חכם המופנים לילדים, וזאת בשל סיכוני הפרטיות שאמצעים אלו יוצרים, והעדר מודעות מספקת של הוריהם לסיכונים אלו.

57. ראוי כי הצגת הנתונים תיעשה בטרם תתקבל הסכמת המשתמשים לשירות, או לכל הפחות במסגרת הליך קבלת ההסכמה.

58. בשירותים בהם הפעלת השירות נעשית באופן מקוון (לדוגמה, במסגרת הורדת ושימוש באפליקציה לניהול מערכות של בית חכם), ראוי כי נתונים אודות אופן השימוש במידע יוצגו במסגרת זו ובאופן מקוון.

59. בכל הנוגע למוצרי IoT ביתיים אשר השימוש בהם יכול להיעשות ללא הפעלה מקוונת (כגון שימוש במצלמות מעקב המתחברות באופן ישיר למערכת שליטה במחשב הביתי), יש צורך כי פירוט נתוני המידע כנדרש על-פי הוראות סעיף 11 לחוק ייעשה באופן שיאפשר למשתמש הפוטנציאלי להיחשף למידע לפני שהוא רוכש את המוצר.[36]

הסכמה ועיקרון צמידות המטרה

60. ככלל הסכמה לפגיעה בפרטיותו של אדם, גם הסכמה לשימוש בשירותי בית חכם ובמוצרי IoT ביתיים נדרשת על פי חוק הגנת הפרטיות להיות **הסכמה מדעת**.

61. לפיכך, ולנוכח סיכוני הפרטיות העלולים להיווצר בשל אי-הבנת משתמשים את השלכות השימוש במערכות של בית חכם על פרטיותם, על חברות להקפיד כי בעת קבלת הסכמה לשימוש במוצרי IoT ביתיים יוצג בפני המשתמשים, **בצורה תמציתית, פשוטה, נגישה ומובנת**, כל

[36] כך לדוגמה, פירוט שכזה יכול להיות מפורסם על-גבי הקופסה בה נמכר המכשיר, באופן שיאפשר למשתמש הפוטנציאלי לבחון את הדברים או להשוות בין מכשירי IoT ביתיים שונים, לפני רכישתו את המוצר.

המידע הרלוונטי בנוגע לאיסוף מידע אישי על ידי המוצר והשימושים שייעשו במידע על אודותיהם, לרבות ההשלכות האפשריות של שימוש במוצרים אלו על פרטיותם.

הקפדה יתרה יש להקפיד בנסיבות בהן הסכמה לשימוש במוצרי IoT ביתיים מהווה גם הסכמה ליצירת "פרופיל" על משתמשי המוצר, וזאת על יסוד עיבוד מידע שמקורו ממוצרי IoT שונים.

62. בנסיבות בהן איסוף המידע או עיבודו נעשים באמצעות טכנולוגיות של בינה מלאכותית, **יש לפרט על אופן פעולת המערכות האמורות, ככל שהדבר רלוונטי לגיבוש ההסכמה, וככל שפירוט זה אפשרי מבחינה משפטית, טכנולוגית, ומסחרית**. בהקשר זה מומלץ כי יוסבר לנושאי המידע על אודות פרטי המידע בהם עשויות הטכנולוגיות האמורות להשתמש במסגרת עיבוד המידע על אודותיהם, והמקור של פרטי מידע אלו (כלומר, איזה מידע נאסף ועם איזה מידע נוסף יכול מידע זה להיות מוצלב ומועבד).

63. **יש להקפיד כי השימוש במידע הנאסף במסגרת מוצרי ה- IoT הביתיים ייעשה אך ורק למטרות שלשמן התקבלה ההסכמה מלכתחילה. שימוש במידע למטרה שונה מהמטרות המקוריות, העלול גם להיות חורג מהציפיות הסבירות של משתמשים, מחייב קבלת הסכמה נפרדת, ובהעדר הסכמה כזו הוא מהווה הפרה של סעיפים 2(9) ו-8(ב) לחוק הגנת הפרטיות**.

64. ראוי לאפשר לנושאי מידע לחזור בהם מהסכמתם לאיסוף ושימוש במידע על אודותיהם. לפיכך, מומלץ כי חברות יאפשרו לנושאי מידע להודיע, באופן פשוט הדומה לאופן קבלת ההסכמה, על רצונם לחזור בהם מהסכמתם ולהפסיק את השימוש במידע על אודותיהם שנאסף במסגרת שירותי הבית החכם.

<u>עיון, צמצום ומחיקת מידע</u>

65. <u>עיון במידע</u> - בהתאם להוראות סעיף 13 לחוק הגנת הפרטיות, על חברות המספקות מוצרי IoT לאפשר למשתמשים לעיין במידע האישי על אודותיהם המוחזק במאגרי מידע שבשליטתן.

לאור החשש שצוין קודם לכן בדבר איסוף מידע אישי רגיש מעבר לנדרש (ושלא בהתאם לצפיית המשתמשים או כוונתם), **רצוי כי חברות המספקות שירותים של בית חכם יאפשרו ללקוחותיהם גישה קלה, ככל האפשר, לעיון במידע על אודותיהם השמור במערכות של הבית החכם ובמאגרי המידע**.[37]

66. <u>מחיקת מידע</u> - בהתאם להוראות סעיף 14 לחוק הגנת הפרטיות, לנושאי מידע עומדת הזכות לפנות בבקשה לעדכון ולמחיקת מידע אשר לגישתם אינו נכון, שלם, ברור או מעודכן.

[37] להרחבה ראו: <u>הרשות להגנת הפרטיות "סעיף 13 לחוק הגנת הפרטיות: זכות העיון הפרטית" (אוגוסט, 2023)</u>.

לאור האמור, נוכח רגישותו של המידע הנאסף במסגרת שימוש במוצרי IoT ביתיים וסיכוני הפרטיות הכרוכים בהחזקת ובשמירת מידע זה לאורך זמן, וכן לנוכח הסבירות שמידע שייאסף במסגרת שימוש במוצרי IoT ביתיים יהיה במקרים מסוימים שגוי או לא מעודכן,[38] **ראוי כי חברות ישקלו בחיוב בקשות משתמשים למחיקת מידע על אודותיהם, או על אודות ילדיהם הקטינים**.

67. צמצום מידע עודף - איסוף, החזקה ושימוש במידע עודף שאינו נדרש למטרה שלשמה התקבלה הסכמה עלולים, במקרים מסוימים, להפר את הוראות סעיף 2(9) וסעיף 8(ב) לחוק הגנת הפרטיות, ולייצר סיכוני פרטיות מיותרים.

על-פי תקנה 2(ג) לתקנות אבטחת מידע, על בעל השליטה במאגר מידע לבחון, אחת לשנה, אם המידע הנשמר על-ידו במאגר מידע אינו רב מן הנדרש למטרות המאגר.

לאור האמור, **על חברות המספקות שירותים ומוצרים של בתים חכמים לבחון, לכל הפחות אחת לשנה, האם המידע הנאסף על-ידן במסגרת מתן השירותים, אינו חורג מהנדרש**. דגש מיוחד יש לתת בהקשר זה למוצרים העלולים, מעצם טבעם ובשל מורכבות השימוש בהם, להביא לאיסוף מידע עודף שאינו נדרש, כדוגמת עוזרים דיגיטליים.

[38] מידע שנאסף במסגרת מוצרי IoT ביתיים עלול להיות שגוי או לא מעודכן ומכאן להביא גם למסקנות מוטעות לגבי אדם. כך לדוגמה, שינוי בסטאטוס אישי של בני זוג או מעבר של אדם נוסף לבית (כגון עובד סיעודי העובר להתגורר עם אדם מבוגר), עלולים להביא לאי-דיוקים ביחס למידע הנאסף ולמסקנות הנובעות מעיבודו.