הכנסת

מרכז המחקר והמידע

סוגיית הפרטיות בטלפונים חכמים

מוגש לוועדת המדע והטכנולוגיה

כתיבה: רועי גולדשמידט

אישור: יובל וורגן, ראש צוות

י״ב בתמוז תשע״ו

18 ביולי 2016

הכנסת, מרכז המחקר והמידע

קריית בן-גוריון, ירושלים 91950

טל׳: 02 - 6408240/1

פקס: 02 - 6496103

www.knesset.gov.il/mmm

תמצית

מסמך זה נכתב לבקשת ועדת המדע והטכנולוגיה של הכנסת לקראת דיון משותף של הוועדה עם ועדת החוקה, חוק ומשפט בנושא "ההגנה על הפרטיות באינטרנט ובטלפונים חכמים".

בשל היקפו של הנושא כמו גם בשל העובדה כי טלפונים חכמים הם זירה מועצמת של סוגיית הפרטיות, כפי שיובהר להלן, המסמך מתמקד בנושא הפרטיות בטלפונים חכמים. יצוין כי המסמך אינו עוסק בסקירה משפטית של סוגיית הפרטיות באינטרנט ובטלפונים חכמים, וכן אינו עוסק בניטור מידע אישי מצד רשויות מדינתיות בישראל או בעולם.

<u>מן המסמך עולים בין השאר הדברים הבאים</u>:

- פרטיות היא מושג עמום, סבוך ויחסי. הגבולות בין הפרטי לציבורי משתנים תדיר בין חברה לחברה ולעתים קרובות בין פרטים שונים באותה החברה, וכך גם חוקרים שונים מדגישים היבטים שונים בתפיסת מושג הפרטיות. וסטיין מגדיר פרטיות כיכולתו של הפרט לשלוט במידע על אודותיו. שליטה זו באה לידי ביטוי בקביעה **איך, מתי ולמי יימסר המידע על האדם, מהם השימושים המותרים בו ומהי התפוצה שלו.** ניסנבאום שמה את הדגש בפענוח הפרטיות בעידן המידע במושג "Contextual Integrity" או בתרגום, "יושרה הקשרית". היא גורסת כי **מה שמגדיר את השמירה או ההפרה של הפרטיות הוא השמירה או ההפרה של ההקשר שבמסגרתו נוצר מועבר או נמסר המידע.**

- החקיקה העיקרית שקובעת כיום את המסגרת ואת הכללים בנוגע להגנה על פרטיותו של אדם היא חוק הגנת הפרטיות ולעומתה חוק יסוד כבוד האדם וחירותו מגדיר את הזכות לפרטיות בקווים כלליים בלבד. מהתייחסויות של גופים הנוגעים בדבר, בהם המועצה הציבורית להגנת הפרטיות, הרשות למשפט טכנולוגיה ומידע (רמו"ט) במשרד המשפטים ואיגוד האינטרנט, עולה כי **החקיקה בתחום הגנת הפרטיות בישראל מיושנת ודורשת עדכון והתאמה לאתגרי עידן המידע**.

- בשנת 2015 74% מהמבוגרים בישראל דיווחו כי ברשותם טלפון חכם – שיעור זה מציב את ישראל במקום השלישי בעולם בשיעור החדירה של טלפונים חכמים, אחרי דרום קוריאה (88%) ואוסטרליה (77%).

- **טלפונים בכלל וטלפונים חכמים בפרט כוללים מידע רב שניתן להגדירו כמידע אישי – מידע הניתן לשיוך לאדם מסוים כאשר האדם ניתן למעשה לזיהוי בצורה ישירה או עקיפה.** בין פרטי המידע האישי ניתן למנות את: נתוני המיקום של המכשיר; פרטי אנשי הקשר, אמצעי זיהוי ייחודיים של המכשיר, רישומי השיחות, הודעות טקסט, פרטי דוא"ל, היסטוריית גלישה באינטרנט, היסטוריית חיפוש במנועי חיפוש, תמונות וסרטוני וידאו, מידע ביומטרי השמור על גבי המכשיר ועוד.

- **העקבות הדיגיטליות של המשתמש קיימות בשכבות מידע שונות ובשליטה של גורמים שונים בשרשרת, וקשה לשלוט בהן ובתפוצה שלהן או למחוק אותן כליל.**

- חברות וגופים שונים עוסקים כיום בכרייה של המידע האישי הגלוי והסמוי, למטרות שונות בהן: פרסום ממוקד, דירוג של לקוחות לפי מדדים שונים, בחינת אמינות לווים ועוד. המודל

הרווח באינטרנט שבו שירותים ניתנים "חינם" הוא בבחינת זרז לשימוש במידע האישי כמטבע עובר לסוחר.

- **סביבת המשתמש של הטלפון החכם מבוססת על מספר לא מבוטל של ספקי שירות בשכבות שונות של המוצר**: החברה המייצרת את החומרה – הטלפון עצמו; החברה המפתחת את מערכת ההפעלה שעל גביה פועל המכשיר; חברות התקשורת המפעילות (ספקי שירותי השיחות והגישה לאינטרנט); חנויות האפליקציות; מפתחי האפליקציות ולבסוף צדדים שלישיים שונים (רשתות מפרסמים ועוד). **לכל גורם בשרשרת האמורה יכולה להיות השפעה על פרטיות המשתמש**.

- מבדיקה שערך בשנת 2014 פורום בין-לאומי המאגד רשויות להגנת פרטיות בעולם (בהן רמו"ט), אשר כללה כ-1,200 אפליקציות בתחומים שונים, עלה כי:

  - 75% מהאפליקציות דרשו הרשאות גישה למידע אישי אחד או יותר; בקשות ההרשאה הנפוצות ביותר היו לנתוני מיקום, זיהוי המכשיר, גישה לחשבונות אחרים, מצלמה, ואנשי קשר;

  - ביחס לישראל, עלה ש-70% מהאפליקציות לא פירטו מדיניות פרטיות טרם ההתקנה; רוב האפליקציות הפנו לאתר אינטרנט או כלל לא התייחסו לנושא, וכי קיימות שאלות באשר לנחיצות ההרשאות לשם מימוש מטרותיהן של האפליקציות.

  מנתונים אלה עולה כי הפרה של פרטיותם של המשתמשים, בגירים וקטינים כאחת, כמו גם יידוע לא מספק באשר לאיסוף מידע אישי, איסוף לא מידתי ועוד, אינם תופעה שולית, אלא מייצגים סוגיה אמיתית שהיקפה נרחב.

- מחוות דעת שפרסמה קבוצה עבודה של נציבות האיחוד האירופי בנושא הגנת מידע, עולה כי **הסיכונים העיקריים למידע של משתמשי הקצה בטלפונים חכמים נובעים מהעדר השקיפות והמודעות ביחס לשימושים שיכולים להיעשות במידע האישי שלהם על ידי האפליקציות, בשילוב עם העדר הסכמה משמעותית מצד משתמש הקצה, בטרם נעשה עיבוד או שימוש במידע**. זאת לצד אבטחת מידע חלשה, נטייה לאיסוף מאסיבי של מידע, וגמישות יתרה (או "אלסטיות") בהגדרת המטרות של איסוף המידע.

- חוות הדעת כוללת הוראות והמלצות באשר לדרכי הפעולה ההכרחיות ורצויות של הגורמים השונים כדי לשמר את פרטיות המשתמשים. כך למשל, ביחס למפתחי האפליקציות, צוין כי עליהם: לספק למשתמשים מדיניות פרטיות קריאה, מובנת ונגישה בקלות; להיות מודעים לכך שהסכמה אינה מקנה לגיטימציה לעיבוד מידע אישי בהיקפים נרחבים ולא מידתיים; להגדיר משך זמן סביר לשמירת המידע ותנאים קבועים מראש למועד מחיקת מידע של משתמש לא פעיל.

- מחקר שבוצע עבור רשות התקשורת הבריטית העלה כי למרות שצרכנים טוענים כי הם מודאגים באשר למידע האישי שלהם ולשימוש בו, הם נוטים שלא להקדיש תשומת לב לתנאי שימוש או למדיניות פרטיות. משאבי הזמן המוגבלים והמורכבות של מסמכי תנאי שימוש הם ההסברים הרווחים בספרות לשיעורי הקריאה הנמוכים שלהם. בין הפתרונות המוצעים לייעול מנגנון תנאי השימוש: פישוט השפה ושימוש בשפה יומיומית, שימוש בטכנולוגיות מסייעות שונות כמו כלי רשת, מנגנוני יידוע פשוטים או כאלה המיידעים את המשתמש תוך כדי הפעולה שלו ברשת באשר להשלכותיה, ועוד.

- **מלבד ההתייחסות לצורך החיוני בעדכון החקיקה הישראלית בתחום הגנת הפרטיות, וכן התייחסות של רמו"ט לכך שבכוונתה לפרסם "הנחיות שוק" הנוגעות לתחום זה, לא עלה מתשובות הגופים הנוגעים בדבר לפנייתנו כי מתוכננים או נדונים כיום צעדי מדיניות נוספים בתחום**. על-פי איגוד האינטרנט, ישנם חסמים שונים למימוש יעיל של ההגנה על הפרטיות בישראל בהם: העדר מודעות מספקת בקרב הציבור והמחוקקים באשר לחשיבות סוגיית הפרטיות ובאשר לדפוסי איסוף המידע האישי הנהוגים באינטרנט כיום; משטר רגולציה חסר משאבים הנעדר סמכויות מספקות לניהול רגולציה אפקטיבית. לטענת האיגוד, יש להפקיד את קידום החקיקה בתחום הגנת הפרטיות בידי הרגולטור לנושא – רמו"ט, ולא בידי מחלקת ייעוץ וחקיקה המופקדת על כך כיום.

- מושג הפרטיות עצמו מצוי כיום במשא-ומתן חברתי, תרבותי ומסחרי ער. יש המדגישים את היתרונות שבוויתור על הפרטיות עבור משתמש הקצה כפרט ועבור השוק כמכלול, ולעומתם כאלה הגורסים כי אין לראות בזירה של האינטרנט עולם נפרד שאיננו כפוף לכללים החלים בזירות אחרות ולא רואים ברשת גורם המשדד כליל את הזכות לפרטיות. בשל האמור **נראה כי יש מקום לדון בשאלות הנוגעות למידת השליטה שלנו במידע אודותינו, לשקיפות המידע באשר לדפוסי האיסוף והניטור של מידע אישי ולשימושים בו, למידת הבחירה שיש כיום למשתמשי הרשת ולמשתמשי טלפונים חכמים ביחס לאיסוף המידע האישי שלהם, ולהסכמה המודעת לאיסוף זה. בנוסף, נראה כי יש מקום לדון בשאלה האם יש להטיל מגבלות על סוג המידע הנאסף, מידת הפירוט שלו, ההצדקות לאיסופו ומשך שמירתו**.

1. חדירתם לשוק של מכשירי טלפון ניידים ומכשירי טלפון חכמים

על פי נתוני איגוד הטלקומוניקציה הבינלאומי (ITU), בשנת 2015 שיעור המנויים לקו טלפון נייד עמד על 97 מנויים לכל 100 אנשים (יתכן יותר ממנוי אחד לאדם) **ושיעור המנויים לאינטרנט בפס רחב בטלפון הנייד עמד על 47 מנויים לכל 100 אנשים (גידול חד לעומת שיעור של כ-5 מנויים לכל 100 אנשים בשנת 2007). על פי אומדן ה-ITU בשנת 2015, יותר מ-40% מאוכלוסיית העולם עשתה שימוש באינטרנט והצמיחה הגדולה בשימוש בו היא באמצעות טלפונים חכמים ולא באמצעות אינטרנט קווי בפס רחב.**[1]

על פי נתוני ה-ITU היו בישראל בשנת 2015 כ-121 קווי טלפון נייד על כל 100 אנשים; ביותר מ-82% ממשקי הבית היה מחשב, וביותר מ-71% ממשקי הבית יש גישה לאינטרנט. יותר מ-71 אחוז מהאנשים עושים שימוש באינטרנט ושיעור הבעלות על אינטרנט בפס רחב בטלפון הנייד בישראל עמד על 52%.

על פי נתונים שפרסם מרכז המחקר PEW[2], שיעורי השימוש באינטרנט והבעלות על טלפונים חכמים בישראל גבוהים יותר: כ-86% מהמבוגרים בישראל (מגיל 18 ומעלה) דיווחו בשנת 2015 על שימוש באינטרנט או על בעלות על טלפון חכם (מקום 7 בעולם). 74% מהמבוגרים בישראל דיווח כי ברשותם טלפון חכם – שיעור זה מציב את ישראל במקום השלישי בעולם בשיעור החדירה של טלפונים חכמים, אחרי דרום קוריאה (88%) ואוסטרליה (77%).

---

[1] International Telecommunication Union, "Measuring the Information Society report 2015", accessed: 18 July 2016.

[2] Jacob Pousther and Rhonda Stewart, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies", Pew Research Center, 22 February, 2016, accessed: 18 July 2016.

שיעורי הבעלות על טלפונים חכמים בישראל גדולים יותר בקרב בני הגילאים 18- 34 (87%) בהשוואה לבני 35 ומעלה (67%). בנוסף שיעורי הבעלות גבוהים יותר בקרב אלו שסווגו כבעלי רמת השכלה גבוהה יחסית (80% לעומת 68% בקרב אלו שסווגו כבעלי רמת השכלה נמוכה יחסית); ובקרב בעלי הכנסה גבוהה (83% לעומת 63%)[3].

76% מתוך הישראלים המדווחים על שימוש באינטרנט או על בעלות של טלפון חכם דיווחו כי הם משתמשים ברשתות חברתיות; 69% ממשתמשי האינטרנט דיווחו כי הם משתמשים באינטרנט מספר פעמים ביום, 19% דיווחו כי הם משתמשים אחת ליום, ו-11% דיווחו על שימוש אחת לשבוע או פחות.[4]

מן הנתונים עולה כי טלפונים ניידים הפכו זה מכבר למוצר צריכה בסיסי בחלק ניכר מהעולם בכלל ובישראל בפרט וכי שיעור ניכר מן המשתמשים מחזיקים בטלפון חכם. **מחקרים מן השנים האחרונות מלמדים שעיקר הגידול בשימוש במחשב ובאינטרנט הוא בשימוש במכשירי טלפון חכמים (להלן, סמארטפונים) ובמכשירי טאבלט** (מחשבי לוח, דוגמת אייפד) ולא בשימוש במחשבים אישיים (דסקטופים).

2. גישות למושג הפרטיות

פרטיות היא מושג עמום, סבוך ויחסי. הגבולות בין הפרטי לציבורי משתנים תדיר בין חברה לחברה ולעתים קרובות בין פרטים שונים באותה החברה. אף-על-פי שמקובל לראות בזכות לפרטיות זכות מודרנית, אפשר למצוא התייחסות לנושא הפרטיות כבר במשנה ובחוקי חמורבי.[5]

הניסוח המשפטי הבולט והמפורסם הראשון של הזכות לפרטיות הוא של **וורן וברנדייס,[6] שטענו בשנת 1890 כי הזכות לפרטיות היא "הזכות להיעזב במנוחה" (The right to be let alone)**, ומכוחה קמה זכותו של האדם לשלוט במידע פרטי על אודותיו.

הסוציולוג אלן וסטיין[7] מגדיר פרטיות כיכולתו של הפרט לשלוט במידע על אודותיו. שליטה זו באה לידי ביטוי בקביעה **איך, מתי ולמי יימסר המידע על האדם, מהם השימושים המותרים בו ומהי התפוצה שלו.** המשפטן מיכאל בירנהק מגדיר גישה זו **"פרטיות כשליטה"**. הדגש בגישה זו איננו בתביעה למידה כלשהי של גילוי או לשמירת סודיות כזאת או אחרת אלא בעצם היכולת של הפרט להכריע באשר למידת השימוש במידע עליו, מועדו ותנאיו. בירנהק מציין כי שני עקרונות נלווים מסייעים בעיגונה של הזכות לפרטיות: **עקרון ההסכמה** – האדם מסכים לאיסוף, עיבוד והעברה של מידע עליו, **ועקרון צמידות**

---

[3] לצורך המחקר הגדירו החוקרים הכנסה נמוכה ככזו הפחותה מההכנסה החציונית במדינה והכנסה גבוהה ככזו השווה להכנסה החציונית במדינה או גבוהה ממנה.

[4] Ibid.

[5] במשנה, במסכת בבא בתרא, נאמר כך: "לא יפתח אדם לחצר השותפים פתח כנגד פתח, חלון כנגד חלון". הגמרא הדנה בנושא משתמשת בביטוי "בעינא לאיצטנועי מינך" (רצוני להצטנע מפניך), שכפי הנראה הוא המקור למונח "צנעת הפרט". בחוקי חמורבי משנת 1760 לפני הספירה נקבע כי יצירת חור בקיר של אדם אחר היא עבירה. יש הגורסים כי בחוקים אלה אף קבוע כי מי שמקבל לחזקתו טובין או כסף למטרת שמירה עליהם מחויב לשמור בסוד את המידע על כך. ראו: "צנעת אדם: הזכות לפרטיות לאור ההלכה", איתמר ורהפטיג, תשס"ט, עמ' 86.

[6] Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review* Vol. 4, No. 5 (December 15, 1890).

[7] Alan F. Westin,"Social and Political Dimensions of Privacy", *Journal of Social Issues* Vol. 59, No. 2 (2003), pp. 431–453.

המטרה – השימוש במידע שנאסף הוא רק למטרות שלשמן הסכים האדם לגלותו, ולכן, למשל, המידע אינו מועבר לצד שלישי ואינו משמש למטרה אחרת מזו שלשמה נמסר.[8]

חוקרת התרבות הלן ניסנבאום שמה את הדגש בפענוח הפרטיות בעידן המידע במושג "**Contextual Integrity**" או בתרגום, "יושרה הקשרית". היא גורסת כי מה שמגדיר את השמירה או ההפרה של הפרטיות הוא השמירה או ההפרה של ההקשר שבמסגרתו נוצר מועבר או נמסר המידע. ברגע שמידע מנותק מן ההקשר החברתי והתרבותי הספציפי שבתוכו הוא נוצר או מופץ, ברגע שהנורמות המקובלות ביחס לשימוש ההולם במידע מופרות, הרי שמופרת הפרטיות.[9] החוקרות מרוויק ובויד טוענות כי ההקשר של המידע הדיגיטלי איננו קבוע ומובן מאליו ולכן הגבולות של הפרטי אינם ברורים ומוחלטים אלא מצויים במשא ומתן בין השחקנים השונים הנוטלים חלק באינטראקציה ברשת האינטרנט.[10] בניגוד לגישות של וסטיין ובירנהק, הדגש בגישה שלהן הוא על היעדר האוטונומיה של הפרט בעיצובה של פרטיותו וקיומה של דינמיקה בין שחקנים שונים המעצבים יחד את דפוסי הפרטיות.

2.1. פרטיות בחוק הישראלי

הזכות לפרטיות מעוגנת בחוק הישראלי הן בחוקים שונים הקובעים סעיפי סודיות הקשורים לצנעת חייו של יחיד, והן בחוק יסוד. החקיקה העיקרית שקובעת את המסגרת ואת הכללים בנוגע להגנה על פרטיותו של אדם היא חוק הגנת הפרטיות ולעומתה חוק יסוד כבוד האדם וחירותו מגדיר את הזכות לפרטיות בקווים כלליים בלבד.

חוק הגנת הפרטיות, התשמ"א -1981 שקדם לחוק-יסוד: כבוד האדם וחירותו, קובע בסעיף 1 תחת הכותרת "איסור הפגיעה בפרטיות" כך: "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו."

סעיף 2 לחוק קובע מה ייחשב לפגיעה בפרטיות: "(1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת; (2) האזנה האסורה על פי חוק; (3) צילום אדם כשהוא ברשות היחיד; (4) פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו; (5) העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו. לענין זה, "כתב" - לרבות מסר אלקטרוני כהגדרתו בחוק חתימה אלקטרונית; (6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו, לשם ריווח; (7) הפרה של חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם; (8) הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע; (9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה; (10) פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או (9); (11) פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני או למצב בריאותו, או להתנהגותו ברשות היחיד.

---

[8] מיכאל בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות", **משפט וממשל** יא (תשס"ח).

[9] Nissenbaum, H. "Privacy as contextual integrity", *Washington Law Review*, 79, 119-157. (2004).

[10] Alice E Marwick, Danah Boyd, "Networked Privacy: How Teenagers Negotiate Context in Social Media", New Media & Society, 2014 Vol. 16(7) 1051- 1067.

פרק ב' לחוק הגנת הפרטיות עוסק בהגנה על הפרטיות במאגרי מידע. החוק מגדיר חובת רישום של מאגרי מידע ומגדיר ישות משפטית לשם כך – רשם מאגרי מידע שבאחריותו ובסמכותו לאשר הקמה וניהול של מאגרי מידע וסייגים לשימוש בו. ומתייחס בפירוט גם לנושא דיוור ישיר.

חוק יסוד כבוד האדם וחירותו, התשנ"ב - 1992 קובע בסעיף 7 תחת הכותרת: "פרטיות וצנעת הפרט" כך: "**(א) כל אדם זכאי לפרטיות ולצנעת חייו. (ב) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו. (ג) אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו. (ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו.**"

ברור כי הזכות לפרטיות אינה מוחלטת, ולעיתים יש לאזנה מול ערכים מתנגשים אחרים, כגון חופש הביטוי או צרכים אחרים כגון בריאות, ביטחון, מניעת פשע, טרור. עמימותה של הזכות לפרטיות – זכות "לא מוחשית" להבדיל מחופש הביטוי, היכולות הטכנולוגיות המתפתחות תדיר ובמידה מסוימת גם השיח הביטחוני והחשש מפשיעה וטרור, גורמים כיום לצמצומה הלכה למעשה של הפרטיות בעולם הקיברנטי ומחוצה לו.

יצוין, כי התייחסויות לצורך בעדכונים ובתיקונים לחקיקה הישראלית הקיימת מובאות בהמשך המסמך בתשובותיהם של גורמים שונים בממשלה, והוא נידון גם בוועדת המדע והטכנולוגיה של הכנסת בשנת 2013 בדיון בנושא "הזכות לפרטיות בעידן הטכנולוגי".[11]

3. פרטיות בטלפונים חכמים[12]

טלפונים בכלל וטלפונים חכמים בפרט כוללים מידע רב שניתן להגדירו כמידע אישי. בהפשטה, **מידע אישי הוא מידע הניתן לשיוך לאדם מסוים כאשר האדם ניתן למעשה לזיהוי בצורה ישירה או עקיפה.** מידע אישי המצוי על גבי מכשירי טלפון חכמים עשוי להיות לא רק של המחזיק במכשיר אלא גם של צדדים שלישיים – לדוגמא, פרטי אנשי קשר או תמונות של אחרים המצויים על גבי המכשיר, תכתובת שלהם ועוד.

בין פרטי המידע האישי ניתן למנות את: נתוני המיקום של המכשיר; פרטי אנשי הקשר, אמצעי זיהוי ייחודיים של המכשיר, רישומי השיחות, הודעות טקסט, פרטי דוא"ל, היסטוריית גלישה באינטרנט, היסטוריית חיפוש במנועי חיפוש, תמונות וסרטוני וידאו, מידע ביומטרי השמור על גבי המכשיר ועוד.

בהינתן הצמידות של מכשירי טלפון חכמים למשתמש אחד לרוב, הרי שהמידע המצוי על גביהם, מרכז פרטי מידע ניכרים של הפרט: נתוני המיקום משקפים היכן המשתמש נמצא בכל רגע נתון, היסטוריית החיפוש משקפת ככלל במה הוא מתעניין או עסוק וכך גם תכתובות הדוא"ל, ההודעות והתמונות.

---

[11] פרוטוקול מס 29 של ועדת המדע והטכנולוגיה מה-10 בדצמבר 2013.

[12] European Commission, Article 29 Data Protection Working Party, "Opinion 02/2013 on Apps on Smart Devices" adopted on 27 February 2013, accessed: 18 July 2016.

בטלפונים חכמים קיימים מספר רב של חיישנים (סנסורים) בהם: ג'ירוסקופ, מצפן דיגיטלי, מד תאוצה (אקסלרומטר) – כל אלה יכולים לספק מידע על מהירות וכיוון התנועה של המכשיר; המצלמות – יכולות לספק צילומי תמונות ווידאו, והמיקרופון יכול להקליט קבצי קול. מכשירי טלפון חכמים גם מתחברים לרשתות תקשורת או למכשירים אחרים באמצעות פרוטוקולי תקשורת שונים Wi-Fi Bluetooth, NFC, Ethernet. לצד השימושים הישירים של סנסורים אלה כדי לספק למשתמש הקצה שירותים שונים, בסיסיים ומתקדמים, הם הופכים את הטלפון הנייד למכשיר מעקב וולונטארי רב עוצמה. **העקבות הדיגיטליות של המשתמש קיימות בשכבות מידע שונות ובשליטה של גורמים שונים בשרשרת, וקשה לשלוט בהן ובתפוצה שלהן או למחוק אותן כליל.**

נוסף על המידע הנאסף על המשתמש כחלק מעצם ביצוע הפעולות שלו באמצעות המכשיר והיישומים שעל גביו, הרי ש**משתמשים רבים בוחרים לחלוק מידע רב באמצעות רשתות חברתיות שונות: הם עשויים לחלוק את המיקום והפעילות שלהם בזמנים שונים, תמונות שלהם, עמדות ביחס לנושאים על סדר היום, העדפות תרבותיות, רשימה של חברים ועוד. מידע עשיר וזמין זה, איננו בבחינת עקבות פסיביות שמשאיר המשתמש, אלא הם ייצוג אקטיבי שלו – אך לא תמיד המשתמש מודע לתפוצה האפשרית של מידע זה ולקושי להגביל את הגישה אליו או למחוק אותו.**

חברות וגופים שונים עוסקים כיום בכרייה של המידע האישי הגלוי והסמוי, למטרות שונות בהן: פרסום ממוקד, דירוג של לקוחות לפי מדדים שונים, בחינת אמינות לווים ועוד. המודל הרווח באינטרנט שבו שירותים ניתנים "חינם" הוא בבחינת זרז לשימוש במידע האישי כמטבע עובר לסוחר בקרב חלק ניכר משרשרת ספקי השירותים השונים, הרואים במידע האישי אמצעי לגיטימי ליצירת תזרים הכנסות.

3.1. הגורמים הנוטלים חלק בעיבוד מידע אישי בטלפונים חכמים[13]

סביבת המשתמש של הטלפון החכם מבוססת למעשה על מספר לא מבוטל של ספקי שירות בשכבות שונות של המוצר: החברה המייצרת את החומרה – הטלפון עצמו; החברה המפתחת את מערכת ההפעלה שעל גביה פועל המכשיר; חברות התקשורת המפעילות (ספקי שירותי השיחות והגישה לאינטרנט)**; חנויות האפליקציות; מפתחי האפליקציות ולבסוף צדדים שלישיים שונים** (רשתות מפרסמים ועוד). יצוין, כי גם במקרים בהם אין הורדה של אפליקציה- יישום ייעודי למכשיר טלפון נייד, יכול להיאסף מידע באמצעות אתרי אינטרנט שונים בכלים שונים.

לכל גורם בשרשרת האמורה יכולה להיות השפעה על פרטיות המשתמש בהתאם לאלמנטים שונים כמו דרישות המערכת (לאילו נתונים ומידע היא מבקשת גישה, מתי ולשם מה); ברירות המחדל של האיסוף (האם המשתמש מספק את המידע אילולי הוא מביע סירוב, או להפך, לא מספק את המידע אילולי הוא מסכים לכך) ועוד. **עם זאת, נראה כי <u>לשני סוגים של גופים יש שליטה גדולה יחסית ברמת איסוף המידע האישי וההגנה על פרטיות המשתמשים והם לרוב גם חולשים על לפחות שתיים מן השכבות – לחברות המפתחות את מערכת ההפעלה של המכשירים; ול-"חנויות האפליקציות" (App-store או</u>**

[13] European Commission, Article 29 Data Protection Working Party, "Opinion 02/2013 on Apps on Smart Devices" adopted on 27 February 2013, accessed: 18 July 2016.

Market). השליטה של החברות המפתחות מערכות הפעלה נובעת ממיעוטן היחסי של יצרניות מערכות ההפעלה הנפוצות ברוב המכשירים[14] דבר היוצר שליטה רבה בשוק ובסביבת הפיתוח של יישומים שונים. השליטה של "חנויות האפליקציות" נובעת מכך שהן בבחינת "שומר סף" עבור רבים מן המשתמשים כיוון שהן יכולות לאשר או למנוע את ההרשאה של מפתחי האפליקציות להציג את מרכולתן למשתמשי הקצה בערוצי ההפצה המרכזיים של אפליקציות- חנויות האפליקציות הרשמיות.

ריבוי הגורמים בשרשרת מבהיר במידה מסוימת את המורכבות היחסית של השליטה בפרטיות, הן מבחינת משתמש הקצה והן מבחינת הרגולטור או גורמים נוספים. בהינתן ההנחה כי לכל משתמש מותקנות מספר אפליקציות על גבי מכשיר הרי שהסדרת פרטיותו של המשתמש צריכה כיום להתממש אל מול מספר רב של גורמים, החל מחברות רב-לאומיות המספקות חומרה, תוכנה או שירות אינטרנטי, עבור דרך חברות תקשורת במדינה, המספקות תשתית, וכלה בחברות קטנות או אפילו אנשים פרטיים, המפתחים אפליקציות. **ניתן לטעון כי ההגנה על פרטיות המשתמשים טובה אך ורק במידה שבה טובה החוליה החלשה ביותר בשרשרת – מספיק יישום אחד שמפר את הפרטיות ואוגר מידע אישי באופן בעייתי כדי לפגוע בפרטיות המשתמש ולהפוך את המידע האישי שלו למידע סחיר.**

3.2. נתונים על פרטיות באפליקציות לטלפונים חכמים

הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים (רמו"ט), הממונה על יישום חוק הגנת הפרטיות ועל ההגנה על המידע האישי בישראל, נוטלת חלק בפורום בינלאומי המאגד רשויות דומות לה בעולם. כחלק מפעילות הפורום מבוצעת גם אחת לשנה פעילות משותפת של סקירת מצב הפרטיות בהיבטים שונים. על פי נתונים שנאספו בשיתוף של 26 רשויות הגנת פרטיות ברחבי העולם. להלן יוצגו עיקרי הממצאים של פעילות זו.

הנתונים שנאספו בשנת 2014 עסקו באיסוף מידע אישי באמצעות אפליקציות לטלפונים ניידים והתבססו על בדיקה של 1,211 אפליקציות בתחומים שונים בהם: משחקים, בריאות/כושר, חדשות ובנקאות. הבדיקות בוצעו על אפליקציות חינמיות ובתשלום, בסביבות אנדרואיד וגם במכשירים של אפל.[15]

- **75% מהאפליקציות דרשו הרשאות גישה למידע אישי אחד או יותר; בקשות ההרשאה הנפוצות ביותר היו לנתוני מיקום, זיהוי המכשיר, גישה לחשבונות אחרים, מצלמה, ואנשי קשר;**
- 59% מן האפליקציות לא כללו התייחסות לנושא הפרטיות טרם הורדת האפליקציה.

[14] שתי מערכות ההפעלה הנפוצות הן: 1) מבוססות אנדרואיד – שהיא מערכת ההפעלה שמובילה חברת גוגל; ו- 2) IOS מבית אפל.

[15] הרשות למשפט, טכנולוגיה ומידע, משרד המשפטים, "דוח רשם מאגרי מידע לשנת 2014", עמ' 34-33. כניסה: 18 ביולי 2016;

- אפליקציות רבות לא כללו, טרם ההתקנה, מידע מספק באשר לעילת איסוף המידע או השימושים שלו, או כללו קישורים למדיניות פרטיות שלא התייחסה לאפליקציה עצמה. בחלק מן המקרים הופנה המשתמש לחשבונות לא פעילים ברשתות חברתיות או דרשו כניסה עם שם משתמש כדי לצפות במידע.

- **מנתוני הבדיקה של רמו"ט ביחס לישראל, עלה ש-70% מהאפליקציות לא פירטו מדיניות פרטיות טרם ההתקנה; רוב האפליקציות הפנו לאתר אינטרנט או כלל לא התייחסו לנושא, וכי קיימות שאלות באשר לנחיצות ההרשאות לשם מימוש מטרותיהן של האפליקציות.**

בעקבות ממצאי הבדיקות נשלחה פנייה על ידי כמה רשויות הגנת פרטיות, בתוכן ישראל, אל שבע חנויות אפליקציות מובילות, בהן גוגל פליי ואפל-סטור, הקוראת להן לחייב את מפתחי האפליקציות להפנות למדיניות פרטיות, טרם התקנת האפליקציה, כדי ליידע את המשתמש באשר למידע האישי הנאסף ומטרות האיסוף ולאפשר לו לבחון את הסכמתו.[16]

בשנת 2015, בוצעה על ידי הפורום של רשויות הגנת הפרטיות סקירה שבחנה את פרטיותם של ילדים ברשת ובאפליקציות. [17] בסקירה נבחנו 1,494 אפליקציות ואתרי אינטרנט ממוקדים או בשימוש נפוץ בקרב ילדים[18], ולהלן עיקרי ממצאיה:

- **67% מהאפליקציות או האתרים אספו פרטי מידע אישי של ילדים**;

- **ב-31% מהאתרים/אפליקציות בלבד היו אמצעים יעילים להגבלת איסוף המידע האישי מילדים**. ברבים מן האתרים/יישומים הנפוצים בקרב ילדים, נטען במדיניות הפרטיות שלהם כי הם אינם מיועדים לילדים ולא הוטמעו אמצעים לשם הגבלת האיסוף של מידע אישי, זאת למרות שבפועל האתרים/יישומים הופנו או היו בשימוש רב בקרב ילדים.

- **כמחצית מהאתרים/אפליקציות חלקו מידע אישי עם צדדים שלישיים.**

- **ב-22% מן האתרים/אפליקציות סיפקו לילדים אפשרות לציין את מספר הטלפון שלהם ו-23% מן האתרים נתנו להם אפשרות להעלות תמונות או וידאו.**

- **71% מן האתרים לא סיפקו אפשרות נגישה למחוק את החשבון והמידע שבו.**

<u>מן הנתונים המוצגים לעיל עולה כי הפרה של פרטיותם של המשתמשים, בגירים וקטינים כאחת, כמו גם יידוע לא מספק באשר לאיסוף מידע אישי, איסוף לא מידתי ועוד, אינם תופעה שולית, אלא מייצגים סוגיה אמיתית שהיקפה נרחב.</u>

---

[16] שם.

[17] 2015 Global Privacy Enforcement Network (GPEN), Annual Report, pp: 11, March 2016, accessed: 18 July, 2016.

[18] במאמר מוסגר, יצוין כי למרות שנושא זה ראוי למיקוד נפרד, התפיסה המקובלת רואה באיסוף מידע אישי מקטינים, בעיה חמורה יותר בשל המגבלות על יכולתם להביע הסכמה מדעת לאיסוף.

4. הסדרת ההגנה על הפרטיות בטלפונים חכמים

נראה כי ריבוי הגורמים והשונות ביניהם לא אמורים בהכרח ליצור שונות בנורמות החברתיות ומכוחן באלו המשפטיות, ביחס למידע האישי שבו הם מחזיקים. לפיכך, יש הטוענים כי ישנה חשיבות בהסדרה או בהבהרה של המעמד של מידע אישי לפי קריטריונים ברורים, בהם לדוגמא: קיומה של הסכמה מדעת של משתמש הקצה, ההרשאות שמקנה המשתמש לשימוש במידע, מטרות האיסוף, המידתיות של השימוש במידע, השאלה למי המידע מועבר, היכן הוא נשמר ועוד - כל זאת, ללא זיקה הכרחית לשאלה מי הוא הגוף המחזיק במידע. במצב הדברים הקיים, קיימת שונות מובנית במידת הפיקוח והרגולציה על שחקנים שונים בשוק התקשורת. ככלל, מידת הרגולציה על האינטרנט נמוכה משמעותית מזו המוחלת על מדיה מסורתית יותר דוגמת שידורי טלוויזיה או רדיו - למרות שאלה מבוצעים כיום גם על גבי רשת האינטרנט, ולכן עשויה להיות חשיבות "להשוואת תנאי המשחק" בין שחקנים שונים באשר לדרישות הרגולטיביות מהם בהיבטים שונים, בתוכם גם בסוגיות של פרטיות.

להלן נציג התייחסויות נבחרות לסוגיית ההסדרה של תחום ההגנה על הפרטיות בטלפונים חכמים, כפי שהן מוצגות בשתי חוות דעת של קבוצת עבודה הפועלת במסגרת נציבות האיחוד האירופי, וכן בדוח שנכתב עבור רשות התקשורת הבריטית.

4.1. עמדת קבוצת העבודה של נציבות האיחוד האירופי בנושא הגנת מידע ופרטיות בעניין אפליקציות במכשירי טלפון חכמים[19]

בפברואר 2013 פרסמה קבוצת העבודה של הנציבות האירופית לתחום הגנת המידע חוות דעת רשמית בעניין השימוש באפליקציות במכשירי טלפון חכמים. למרות שחלפו כ-3 שנים מאז פרסום זה, הוא מציג מידע רלבנטי, בפרספקטיבה מקיפה יחסית בנושא ולכן יוצגו להלן סוגיות ועקרונות עיקריים ממנו.

- **הסיכונים העיקריים למידע של משתמשי הקצה בטלפונים חכמים נובעים מהעדר השקיפות והמודעות ביחס לשימושים שיכולים להיעשות במידע האישי שלהם על ידי האפליקציות, בשילוב עם העדר הסכמה משמעותית (Meaningful Consent) מצד משתמש הקצה, בטרם נעשה עיבוד או שימוש במידע. אבטחת מידע חלשה, נטייה לאיסוף מאסיבי של מידע, וגמישות יתרה (או "אלסטיות") בהגדרת המטרות של איסוף המידע, תורמים גם הם לסיכוני הפרטיות שבאקו סיסטם[20] של אפליקציות לטלפונים ניידים.**
- ביטוי מסוים להיעדר השקיפות יכול להימצא בהעדרה של מדיניות פרטיות עבור האפליקציה והעדר יידוע מספק של המשתמשים באשר לסוג המידע האישי שהאפליקציה יכולה לגשת אליו. **הסכמה חופשית ומודעת לשימוש במידע האישי** קשורה ישירות למידת השקיפות. **לעתים קרובות, מרגע שמשתמש מתקין אפליקציה על גבי המכשיר הטלפון הנייד, מצטמצמת ההסכמה לאישור סמלי בלבד באמצעות סימון אישור בתיבה של תנאי השימוש, זאת למרות**

[19] European Commission, Article 29 Data Protection Working Party, "Opinion 02/2013 on Apps on Smart Devices" adopted on 27 February 2013, accessed: 18 July 2016.

[20] המושג "אקו-סיסטם" מתבסס על הרעיון של זיקות בין אלמנטים שונים בסביבה הטבעית שגוררים השפעה הדדית בין האלמנטים השונים. עם זאת, בהקשר העסקי מקובל לדבר על "אקו-סיסטם" כסביבה עסקית הכוללת תחומים קרובים או המשפיעים אחד על השני.

שמשתמשי יישומים מעוניינים באפשרויות מורכבות או מדורגות (granular) יותר ולא באפשרות בינארית של "הכל או לא כלום".

- סיכון נוסף לפרטיות המידע נובע מהתעלמות, מכוונת או כזו הנובעת מבורות, מעיקרון **צמידות המטרה (Purpose Limitation)**. **עקרון זה קובע כי איסוף ועיבוד של מידע אישי יבוצע לשם מטרה ספציפית ולגיטימית שהמשתמש מודע אליה**. במקרה שמטרת האיסוף שונתה, יש להודיע על כך למשתמש ולקבל את הסכמתו מחדש. בניגוד לעקרון זה, עשויות לדוגמא אפליקציות להפיץ מידע אישי הנאסף על ידם למספר רב של "צדדים שלישיים" מסיבות שאינן מוגדרות או כאלה המוגדרות בצורה נרחבת מידי כמו לשם "מחקר שוק".
- עקרון נוסף שנזנח לעיתים קרובות הוא זה של **"צמצום מידע" (Data Minimization)**. לפיו המידע הנאסף אמור להיות זה הדרוש לשם המשימות הקונקרטיות של היישום. בניגוד לעיקרון זה, כאמור, אפליקציות רבות מבקשות גישה למידע אישי רב שאין לו זיקה ישירה לעניינן.
- על פי חוות הדעת, **בטלפונים חכמים, בניגוד לנוהג רווח במחשבים שולחניים (דסקטופ), ישנן אפשרויות מוגבלות יחסית להתקין תוכנות המגבילות את העיבוד של מידע אישי.** בנוסף, בעוד דפוס השירות והניטור הרווח במחשבי דסקטופ כולל שימוש ב"עוגיות" (Cookies) - אותן יכול משתמש הקצה למחוק, הרי שבסביבת מובייל, מקובל להשתמש באמצעי זיהוי ייחודיים שונים של המכשיר (כדי לספק שירותים שונים, וכדי לספק למשתמשים פרסומות המפולחות לקבוצה ייעודית), אותם אין אפשרות למחוק. כפועל יוצא, **יש לצדדים שלישיים (לדוגמא ספקי תשתיות פרסום, חברות העוסקות בניטור תעבורה ברשת ועוד), את הפוטנציאל לעבד כמויות גדולות של מידע אישי ללא שליטה של משתמש הקצה בכך.**
- באשר ל**הסכמה מדעת, זו חייבת להינתן בצורה "חופשית, מפורשת ומודעת".** ביחס לטלפונים חכמים, כדי שההסכמה תהיה חופשית, צריכה להיות למשתמש אפשרות לסרב, ולא להתקין את היישום. מסך טלפון המציג למשתמש אך ורק אפשרות לאשר כי הוא מסכים (ולא מציג אפשרות סירוב), איננו מהווה הסכמה מספקת.
- **הסכמה מפורשת משמעה כזו שבה יש זיקה בין עילת ההסכמה לאיסוף המידע האישי לבין המטרה של האפליקציה והסכמה איננה היתר כללי לביצוע ניטור כולל.** לדוגמא: אפליקציית מסעדות, המבקשת גישה לנתוני מיקום לשם המלצה על מסעדות סמוכות, נדרשת לבקש גישה לנתוני המיקום כדי לספק את השירות. אך ההסכמה האמורה, איננה מקנה לה גישה קבועה אל נתוני המיקום, אלא בעת שבו המשתמש מפעיל את היישום. במידה והיישום דורש גישה קבועה לנתוני המיקום, נדרש לשם כך כי היישום יספק מידע נוסף וכן הסכמה נפרדת לאיסוף זה. **במקרה של אפליקציית תקשורת המבקשת לגשת אל רשימת אנשי הקשר, יש לאפשר למשתמש לבחור עם אילו מהמשתמשים הוא מעוניין לתקשר, ולא להקנות כברירת מחדל גישה אל כל אנשי הקשר.**
- **<u>קיימות דוגמאות של ניטור או עיבוד מידע באופן לא מידתי: לדוגמא, אם אפליקציית שעון מעורר מאפשרת למשתמש לתת הוראה קולית לשעון המעורר להפסיק את פעולתו, ההסכמה שלו היא להאזנה למיקרופון של המכשיר בעת שהשעון פועל. ניטור או האזנה בזמן אחר, יוגדר ככל הנראה כבלתי מידתי ופסול.</u>**

- **יש להקנות למשתמש הקצה גישה למידע הנאסף אודותיו**, אפשרות לבקש את תיקון המידע – אם הוא אינו נכון, או את מחיקתו. במידה ומשתמש מבקש גישה למידע, יש למחזיק במידע (מי שעוסק באיסוף, ניטור או עיבוד המידע) לספק לו מידע על העיבוד של המידע ועל מקורו.

חוות הדעת כוללת הוראות והמלצות באשר לדרכי הפעולה ההכרחיות ורצויות של הגורמים השונים כדי לשמר את פרטיות המשתמשים, בחלוקה לפי הגורם הספציפי, להלן יוצגו עיקריהן של ההוראות שהוגדרו כ"הכרחיות"[21]:

<u>ביחס למפתחי האפליקציות</u>, נכתב בין השאר כי מחובתם:

- לספק למשתמש אפשרות להביע את הסכמתו או סירובו באופן נפרד לאיסוף של פרטי מידע אישיים שונים, בפרט: נתוני מיקום, אנשי קשר, מזהה ייחודי של המכשיר, פרטי אשראי או אמצעי תשלום, רישומי שיחות והודעות, היסטוריית גלישה, דוא"ל, גישה למידע מרשתות חברתיות ומידע ביומטרי.
- להיות מודעים לכך ש**הסכמה אינה מקנה לגיטימציה לעיבוד מידע אישי בהיקפים נרחבים ולא מידתיים**, ולכבד את עיקרון צמצום המידע ולאסוף רק את המידע הדרוש לשם ביצוע מטרותיה של האפליקציה.
- **לספק למשתמשים מדיניות פרטיות קריאה, מובנת ונגישה בקלות** שתכלול לפחות את המידע הבא: מי הגוף האוסף את המידע; אילו קטיגוריות של מידע נאספות ומעובדות, לאילו מטרות נדרש האיסוף; האם המידע האישי מועבר לצדדים שלישיים ומי הם; ומה הן זכויות המשתמש להסיר את הסכמתו ולמחוק את המידע.
- **להגדיר משך זמן סביר לשמירת המידע ותנאים קבועים מראש למועד מחיקת מידע של משתמש לא פעיל.**
- **באשר לאפליקציות לילדים, יש לקבוע אמות מידה מחמירות ביחס לאיסוף המידע;** להימנע מעיבוד מידע אישי של ילדים למטרות פרסום ממוקד ומאיסוף מידע מן הילדים אודות קרובי משפחה או חברים.

ביחס ל<u>חנויות האפליקציות</u> נכתב בין השאר כי חובה עליהן:

- **על החנויות לאכוף את חובת מסירת המידע מצד מפתחי האפליקציות כולל:** לאיזה מידע האפליקציה נגישה, לאיזו מטרה, והאם המידע מועבר גם לצדדים שלישיים.
- **לספק מידע באשר לתהליכי הבקרה של החנות על האפליקציות הנמכרות/ניתנות להורדה בה, בין השאר ביחס להגנה על הפרטיות והשמירה על המידע.**

[21] הן מוגדרות כ- Must – חובה, ולא כהמלצה בלבד. במסמך מוצגות גם המלצות בדבר פרקטיקות רצויות, אך אלה לא נסקרות כאן.

ביחס לחברות המפתחות מערכות הפעלה וליצרנים נכתב כי מחובתם:

- יש לעדכן את ממשקי הפיתוח, הכללים בחנויות האפליקציות וממשקי המשתמש כדי שאלה יספקו למשתמש הקצה שליטה מספקת ויאפשרו לו להביע את הסכמתו ביחס למידע המעובד על ידי האפליקציות.
- להטמיע מנגנונים לקבלת הסכמה מדעת במערכות ההפעלה, בשלב ההתקנה הראשונית או הפעלת אפליקציות לראשונה.
- לעשות שימוש בעקרונות של "פרטיות בעיצוב" (Privacy By Design) כדי למנוע ניטור סמוי של המשתמש.
- לאפשר גישה מדורגת למידע, לחיישנים ולשירותים שונים על גבי המכשירים כך שמפתחי האפליקציות ייגשו אך ורק למידע הנדרש למטרת האפליקציה.
- לספק למשתמשים אמצעים ידידותיים ויעילים למנוע איסוף מידע אישי על ידי מפרסמים או צדדים שלישיים אחרים. **ברירת המחדל צריכה להיות של מניעת ניטור**.

ביחס לצדדים שלישיים, חובה עליהם:

- לא למנוע או לעקוף את פעולתם של מנגנונים למניעת מעקב (Tracking).
- על מפרסמים להימנע מלהציע פרסום שלא כחלק מן האפליקציה, ולא לשנות את ברירות המחדל הקבועות של הדפדפן, או באמצעות התקנה של אייקונים (סמלילים) על גבי המסכים של המכשיר.
- יש להימנע משימוש במזהים אישיים של המכשיר לשם מעקב.

4.2. עמדת קבוצת העבודה של נציבות האיחוד האירופי בנושא הגנת מידע ופרטיות בעניין נתוני מיקום[22]

במאי 2011 פרסמה קבוצת העבודה של נציבות האיחוד האירופי בנושא הגנת מידע ופרטיות נייר עמדה בעניין "שירותי מיקום על גבי מכשירי סלולר חכמים"[23], להלן נקודות עיקריות ממסמך זה:

- נתוני מיקום ממכשירי סלולר חכמים הם מידע אישי. השילוב בין מידע אודות נקודות Wi-Fi ופרטי המידע הספציפיים של כרטיס רשת (כתובת MAC) הם מידע אישי ודורשים התייחסות מתאימה.

[22] European Commission, Article 29 Data Protection Working Party, ", Opinion 13/2011 on "Geolocation Services on Smart Mobile Devices", Adopted on May 16, 2011, accessed: 18 July 2016.

[23] בהקשר זה יצוין כי ועדת המדע והטכנולוגיה של הכנסת דנה בנושא "השימוש בנתוני מיקום במכשירי סלולר חכמים – פרטיות ושימושיות" בעקבות הצעה לסדר היום של חה"כ איתן כבל, ראו פרוטוקול הוועדה מס' 108 מה-21 בנובמבר 2011. כמו כן, ראו: מרכז המחקר והמידע של הכנסת, "שמירתם של נתוני מיקום מכשירים סלולריים חכמים והשימוש בהם", רועי גולדשמידט, 20 בנובמבר 2011.

- **מידע מיקום מטלפונים ניידים חכמים חושף פרטים אינטימיים על בעליהם ולכן נדרשת הסכמה מדעת.** הסכמה זו לא יכולה להינתן כחלק מחתימה על תנאים כלליים. על ההסכמה להיות ספציפית ותואמת את עילת איסוף המידע. במידה ועילת איסוף המידע משתנה, נדרשת הסכמה חוזרת.
- **ברירת המחדל ביחס לאיסוף נתוני מיקום צריכה להיות שהם אינם נאספים. מנגנונים הדורשים פעולה אקטיבית כדי למנוע את האיסוף (Opt-Out Mechanism) לא מהווים אמצעי הולם לקבלת הסכמה מדעת של המשתמש.**
- **קבלת הסכמתם מדעת של מועסקים וילדים הינה בעייתית.** על מעסיקים לאמץ טכנולוגיות נתוני מיקום כאשר היישום שלהן הוא למטרה לגיטימית וניתנת להוכחה וכאשר לא ניתן להשיג את המטרה באמצעים פולשניים פחות. ביחס לילדים, על ההורים לבחון את הצידוק של שימוש באמצעים אלה ולכל הפחות ליידע את הילדים על כך. ככל הניתן, יש לאפשר לילדים לקחת חלק בהחלטה על השימוש של ההורים בנתוני מיקום.
- יש מקום להגביל בזמן את ההסכמה ולהזכיר למשתמשים את הסכמתם לפחות אחת לשנה. בנוסף, יש להעניק למשתמשים מידע על מידת הדיוק של מידע המיקום.
- יש לאפשר למשתמשים לוותר על הסכמתם לשימוש בנתוני מיקום בקלות ללא השלכות שליליות על השימוש שלהם במכשירי הקצה.
- ביחס למיפוי נקודות Wi-Fi: לחברות יש אינטרס לגיטימי באיסוף ועיבוד ההכרחי של כתובות MAC ונקודות Wi-Fi למטרת אספקת שירותים מבוססי מיקום. איזון האינטרסים בין זכויות המחזיק במידע וזכויות המשתמש דורש שהמחזיק במידע יאפשר למשתמש שלא לחלוק נתוני מיקום (Opt-Out) בקלות ולצמיתות, ללא דרישת מידע אישי נוסף.
- **המידע באשר לסוג הנתונים שנאספים : צורת האיסוף, משך האיסוף, מטרותיו ועוד, צריך להיות ברור, מקיף וקל להבנה גם למשתמש הפשוט.**
- לצדדים שלישיים, דוגמת דפדפנים ואתרי רשתות חברתיות, יש תפקיד מפתח ביחס לנראות ולאיכות המידע באשר לשימוש בנתוני מיקום.
- המחזיקים השונים בנתוני מיקום במכשירי סלולר צריכים לאפשר ללקוחותיהם **גישה לנתוני המיקום שלהם בפורמט קריא ולהתיר להם את האפשרות לתיקון או מחיקת המידע** בלי לדרוש מידע אישי נוסף. למשתמשים יש זכות לגשת, לתקן או למחוק פרופילים אפשריים המבוססים על נתוני המיקום שלהם. מומלץ לאפשר גישה מאובטחת למידע האמור באמצעות האינטרנט.
- על ספקי נתוני מיקום או שירותים מבוססי מיקום להגדיר **מדיניות שמירה על נתוני מיקום**. מדיניות זו תבטיח כי נתוני מיקום או פרופילים שנבנו על סמך נתוני מיקום ימחקו לאחר אחרי זמן הולם.
- במידה ומפתחי מערכות הפעלה ו/או המחזיקים בתשתית נתוני מיקום מחזיקים בפרטים ספציפיים המאפשרים זיהוי חד ערכי (כתובת MAC, או כתובת זיהוי זמנית דוגמת UDID) הקשורים לנתוני המיקום האמורים, פרטי הזיהוי הייחודיים יישמרו ללא יותר מ-24 שעות, למטרות תפעוליות.

4.3. סוגיות עקרוניות הקשורות להסכמה מדעת ומדיניות פרטיות

מחקר שבוצע עבור רשות התקשורת הבריטית (OfCom) מספק מידע ותובנות מעניינות, המכניסות הקשר צרכני והתנהגותי מורכב יותר להמלצות לרגולציה ולפרקטיקות ראויות - דוגמת המסמכים של קבוצת העבודה של הנציבות בענייני הגנת פרטיות במידע. להלן יוצגו בקצרה כמה מן הסוגיות שמעלה דוח זה, שפורסם במאי 2015 תחת הכותרת "מידע אישי ופרטיות".[24]

- **<u>נדיר שצרכנים קוראים תנאי שימוש</u>**: הדוח מציין כי מחקרים רבים מצביעים על כך שצרכנים, בסביבות לא דיגיטליות, ובמידה רבה עוד יותר בסביבות דיגיטליות, נוטים לאשר תנאי שימוש בלי לקרוא אותם. זאת גם במקרים שבהם עשויות להיות לאישור (הסכמה) השלכות על איסוף, ניתוח ושימוש במידע אישי שלהם. סקרי צרכנים מצביעים באופן עקבי על כך ש**למרות שצרכנים טוענים כי הם מודאגים באשר למידע האישי שלהם ולשימוש בו, הם נוטים שלא להקדיש תשומת לב לתנאי שימוש או למדיניות פרטיות.** גם במקרים בהם הצרכנים ניגשים להסכם תנאי השימוש, הם לרוב לא קוראים אותם, וזמן הצפייה הממוצע בתנאי שימוש עומד על הרבה פחות מדקה אחת.

- **משאבי הזמן המוגבלים של המשתמשים והמורכבות של מסמכי תנאי שימוש** הם ההסברים הרווחים בספרות לשיעורי הקריאה הנמוכים שלהם. מסמכים אלה מתאפיינים באריכות רבה ובשימוש בז'רגון משפטי שאיננו ברור לחלק ניכר מן האנשים. מחקרים שבחנו את רמת הקריאה הנדרשת להבנת מסמכי תנאי שימוש גורסים כי להבנתם נדרשת השכלה ברמה אוניברסיטאית לפחות. יתרה מכך, צרכנים רבים מפרשים את המונח "מדיניות פרטיות" ככזה המעגן את זכויות הפרטיות שלהם ולא ככזה המפרט מהי מידת פרטיות המידע ולכן עצם קיומה של מדיניות כזו גורם להם לספק יותר מידע אישי. כמו כן, משתמשים מתקשים להבין את ההשלכות של הניתוח והעיבוד של המידע האישי שלהם, בין השאר בשל ההתפתחות המתמדת של זרימות המידע בין מערכות איסוף מידע, רשתות פרסום (Ad Networks) וצדדים שלישיים.

- **<u>אין לצרכנים אפשרות להתחמק מניטור אך הם מתמודדים איתו בדרכים שונות</u>:** ספקי שירות ואפליקציות רבות עושים שימוש במדיניות פרטיות של "הכל או לא כלום" ולכן מקשים להגביל את מידת האיסוף; חוזקם של חלק מהספקים מקשה על צרכנים לעבור בין שירותים משיקולי פרטיות – לדוגמא כאשר רוב החברים של המשתמש עושים שימוש בשירות רשת חברתית מסוים, הוא מתקשה לעזוב אותו ולהחליף שירות, גם אם הוא מתנגד למדיניות הפרטיות, כיוון שזה יפגע באפשרות התקשורת עם חבריו. בנוסף, **טכנולוגיות מעקב מתוחכמות כמו מה שמכונה "טביעת אצבע של המכשיר" – שיטה המבוססת על זיהוי ייחודי של המכשיר בהתבסס על השילוב הייחודי של כלל היישומים המותקנים על גביו יחד עם פרטי מידע נוספים גלויים, או זמינים בקלות, מקשה מאוד על נטרול אפשרות המעקב והניטור.** עם זאת,

[24] René Arnold, Annette Hillebrand and Martin Waldburger, "Personal Data and Privacy - Final Report", WIK-Consult GmbH, Study for Ofcom, 26 May 2015, accessed: 18 July, 2016.

מחקרים מצביעים על כך שמשתמשים מפעילים טכניקות התנגדות לפרסום, באמצעות התעלמות מודעת ממנו, או באמצעות שימוש בכלים טכנולוגיים דוגמת כלי החוסם פרסומות. ישנן טענות כי התפתחותו של שוק משני שיעניק כלים טובים יותר לשליטה במידע, או יאפשר לשלם יותר בעבור שירותים השומרים על פרטיות יכול להועיל, עם זאת, כפי הנראה אי-הוודאות של צרכנים באשר לשימוש במידע האישי שלהם, מונע התפתחותו של שוק כזה.

- **<u>קיימות אפשרויות וניסיונות לייעל את מנגנוני תנאי השימוש והיכולת לסרב או להביע הסכמה</u>.** פישוט השפה ושימוש בשפה יומיומית, שימוש בטכנולוגיות מסייעות שונות כמו כלי רשת, מנגנוני יידוע פשוטים או מנגנונים המיידעים את המשתמש תוך כדי הפעולה שלו ברשת באשר להשלכותיה, שימוש באייקונים (סמלילים) המשקפים למשתמש את הגישה או השימוש במידע האישי ועוד, הם בין האפשרויות הנבחנות כדי לשפר רמת הנגישות של תנאי השימוש והיכולת של המשתמש לממש את רצונו ולהביע את הסכמתו. **עם זאת, קיימת בעיה מובנית המכונה "פרדוקס השקיפות" לפיו ככל שהמדיניות מפורטת יותר היא מאפשרת למשתמש לשלוט יותר במידע אודותיו, אך פחות משתמשים יקראו מדיניות כזו או יבינו אותה.**

- **עידוד לפעולה ולנקיטת עמדה** ביחס להיבטי פרטיות במידע אישי היא אחת הגישות הנידונות על ידי כלכלים התנהגותיים ופסיכולוגים. הרעיון בגישה זו הוא לא להכריע עבור האנשים, אלא לסייע להם לקבל החלטה מושכלת באמצעות שיקוף ההשלכות של הוויתור על פרטיות המידע האישי שלהם.

5. התייחסות גופי ממשלה בישראל וגופים נוספים לסוגיית הפרטיות

מרכז המחקר והמידע של הכנסת פנה אל משרדי ממשלה בעלי זיקה לנושא ואל גופים נוספים בבקשה למידע והתייחסות לנושא הדיון, להלן עיקרי תשובותיהם:

5.1. הרשות למשפט, טכנולוגיה ומידע (רמו"ט) במשרד המשפטים[25]

מרכז המחקר והמידע של הכנסת פנה אל רמו"ט שהיא כאמור הרגולטור לעניין ההגנה על הפרטיות במידע בישראל בבקשה למידע באשר לפעילותה בהיבטים שונים בהם: קביעת כללים או הנחיות ביחס לאיסוף מידע אישי בטלפונים חכמים, דרישות הגנה על פרטיות ועוד. להלן עיקרי תשובת רמו"ט:

הרשות למשפט טכנולוגיה ומידע (רמו"ט), שהיא הרשות להגנת מידע אישי בישראל, מקפידה לעקוב אחר השינויים הטכנולוגיים, החברתיים והמשקיים הנובעים מעידן המידע, ולקבוע בהתאם את סדר העדיפות של פעילותה הרגולטורית ואת המיקוד שלה.

רמו"ט נטלה חלק בפעילות אכיפה משותפת יחד עם 26 רשויות הגנת מידע אישי ופרטיות ברחבי העולם שחברות ברשת שיתוף פעולה באכיפת הגנת הפרטיות (GPEN) – ממצאי פעילות זו נסקרים לעיל במסמך. כפועל יוצא מן הפעילות, כאמור לעיל, הייתה שותפה רמו"ט למכתב שהופנה על ידי מספר

[25] עו"ד ניר גרסון, ממונה משפט וטכנולוגיה, הרשות למשפט, טכנולוגיה ומידע, משרד המשפטים, מכתב, 17 ביולי 2016.

רשויות הגנת פרטיות לחנויות אפליקציות מובילות הקורא להן להפנות את המשתמשים למדיניות פרטיות טרם התקנת האפליקציות.

רמו"ט פעילה גם בבחינה של בקשות לרישום מאגרי מידע, המוגשות לה בין השאר על ידי אפליקציות ושירותי אינטרנט. וכן, בפרסומים של קווים מנחים על סיכונים ברשת והתמודדות איתם, המלצות כיצד להגן על מידע אישי ברשת ובטלפונים חכמים.

יצוין, כי חלק ניכר מן הדוגמאות שציינה רמו"ט בתשובתה קשורות לפעילות שנעשתה לפני מספר שנים, בהן: פעילות ניטור מצב ההגנה על מידע אישי באפליקציות- בשיתוף גופים מקבילים מן העולם, והפיקוח על מאגרי המידע של חברת גוגל לצורך הפעלת שירות גוגל "Street view" (פעולות שנעשו בשנים 2014 ו- 2011 בהתאמה).

על פי התשובה, רמו"ט עתידה לפרסם הנחיות שוק בהיבטים הקשורים להגנה על הפרטיות באינטרנט בחודשים הקרובים.

עם זאת, באשר לחוק ולכלים שהוא מקנה לרשות נכתב כך:

"הרשות פועלת על פי חוק אשר מאז חוקק לראשונה ב- 1981 עבר רק תיקונים מוגבלים בהיקפם, והינו ארכאי ואינו מתאים למסגרת ההגנה על המידע האישי על פי המציאות הטכנולוגית היום. כפועל יוצא מכך, פועלת רמו"ט כאשר "ידיה קשורות מאחורי הגב' עם סט חסר של כלי אכיפה מיושנים."

לדברי נציג הרשות, כדי שהיא תוכל לתת מענה הולם לאתגרי הפרטיות העכשוויים, לתפקד בצורה תקינה, להוות רגולטור יעיל ומשפיע במשק ולהיות חלק מרכזי במערך הגנת מידע אישי בישראל – **יש חובה לערוך תיקונים משמעותיים בחוק הגנת הפרטיות ובתקנות שנקבעו מכוחו.**

נציג הרשות ציין כי מספר הצעות לתיקון החוק, עומדות על הפרק, חלקן לטענתו בשלבים מתקדמים של בשלות: **הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב-2011** עברה בקריאה ראשונה בכנסת ה - 18 אך הדיון בה לא הסתיים גם במהלך כהונתה של הכנסת ה-19, ולכן לא היה ניתן להחיל עליה שוב דין רציפות - כדי לחדש כעת את הליכי חקיקתה נדרשת התגייסות של כל הגורמים הרלבנטיים; **תקנות הגנת הפרטיות (אבטחת מידע), התשע"ו – 2016** הונחו זה מכבר על שולחן ועדת החוקה של הכנסת וממתינות לאישורה.

עוד ציין נציג הרשות כי **קיים צורך דחוף וממשי קיים גם בתיקון ועדכון של הוראות הדין המהותי של חוק הגנת הפרטיות,** וכן בהמשך הליכי החקיקה של תזכיר חוק הגנת הפרטיות (צמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב – 2012.

5.2. המועצה הציבורית להגנת הפרטיות[26]

המועצה הציבורית להגנת הפרטיות מורכבת מנציגי ציבור מהאקדמיה ומהמגזר הפרטי ומנציג עובד מדינה שעוסקים בתחום הפרטיות, והיא ממונה על ידי שר המשפטים. על פי חוק, המועצה נדרשת להגיש

[26] עו"ד אורית פודמסקי, דוא"ל ושיחת טלפון, 12 ביולי 2016.

לוועדת החוקה חוק ומשפט של הכנסת את הערותיה על דוח רשם מאגרי המידע. אך בנוסף, המועצה גם משמשת כיועצת לשרת המשפטים. בשנים האחרונות המועצה לא פעלה, לאחר שמינוי חבריה הסתיים ולא מונתה מועצה חדשה. בסוף שנת 2015 מונתה לעמוד בראש המועצה עו"ד אורית פודמסקי.

מרכז המחקר והמידע של הכנסת פנה אל המועצה בשאלות ביחס להגנה על הפרטיות באינטרנט ובטלפונים חכמים ובדבר שאלת הצורך בחקיקה או תקינה עדכניות בתחומים אלה. **יו"ר המועצה, עו"ד פודמסקי ציינה בתשובתה כי המועצה טרם נדרשה לסוגיות אלה בפירוט ולכן איננה יכולה להציג עמדה רשמית של המועצה.**

עם זאת, בהערות המועצה להגנת הפרטיות לדוח רשם מאגרי מידע משנת 2014 שהוגשו כאמור לוועדת החוקה, חוק ומשפט בינואר 2016 נכתב כעמדת המועצה, בין השאר כך: "מצבה הנוכחי של הזכות לפרטיות בישראל רחוק מלהשביע רצון, וזקוק לחיזוק נמרץ. המועצה עוקבת בדאגה אחרי מגמות שונות בשוק שבהן מידע נאסף, מעובד, מועבר לשימושים חדשים ולגרומים אחרים, ללא בקרה מספקת, פעמים רבות תוך הפרה בוטה של החוק והתעלמות ממנו. המועצה מוטרדת מאוד מקיפאון בחקיקה בתחום וקוראת לקידומה המהיר, כמו גם להגברת האכיפה הציבורית והפרטית.[...] "**לקיפאון החקיקתי יש מחיר. החוק הקיים כמעט שאינו רלוונטי למציאות הטכנולוגית-עסקית-חברתית. הפער בין החוק שהולדתו לפני עידן האינטרנט לבין המציאות מביא לכך שהאכיפה והכוונת השוק כמעט שאינן מתקיימות.**"[27]

עוד נכתב בהערות המועצה לדוח, כי האיחוד האירופי הכיר במשטר הגנת הפרטיות במידע בישראל כמשטר משפטי "מספק", בין השאר בהינתן הבטחות לקדם חקיקה ברוח דוח ועדה שבראשה עמד המשנה ליועמ"ש באותה עת, עו"ד יהושע שופמן, שהגישה דוח ובו המלצות קונקרטיות לחקיקה בשנת 2007. לפי המועצה, הקיפאון החקיקתי עלול לגרום לאירופים לשנות את עמדתם ולפגוע בעסקים המספקים שירותי מידע לאיחוד האירופי.

5.3. משרד התקשורת[28]

מרכז המחקר והמידע פנה אל משרד התקשורת בבקשה למידע האם המשרד קבע כללים ביחס לאיסוף של מידע אישי של משתמשי קצה על ידי חברות התקשורת וביחס להיבטי פרטיות אחרים בשימוש בטלפונים חכמים ובאינטרנט.

על פי תשובת נציג המשרד, המשרד מפקח אך ורק על ספקי תקשורת כהגדרתם בחוק וברישיונות השונים שהמשרד מנפיק, אך אינו מפקח על יישומים המסופקים על גבי האינטרנט דוגמת רשתות חברתיות, חברות מערכות הפעלה וכו'.

---

[27] הרשות למשפט, טכנולוגיה ומידע, המועצה הציבורית להגנת הפרטיות, "הערות המועצה הציבורית לדוח רשם מאגרי המידע לשנת 2014", 20 בינואר 2016. כניסה: 18 ביולי 2016.

[28] יאיר חקאק, מנהל האגף לתכנון מדיניות, משרד התקשורת, מכתב, 17 ביולי 2016.

ההגנה על פרטיות המנויים מופיעה כחובה ברישיונות של ספקי תקשורת, כך למשל, ברישיון כללי אחוד למתן שירותי בזק נכתב תחת הכותרת "הגנה על פרטיות המנוי":

[...] "אין בעל הרישיון רשאי להאזין לטלפון או לתקשורת אחרת של מנוי ללא אישור בכתב של המנוי, פרט לשם בקרה על טיב, לשם בקרה על טיב השירות ואיכותו, או מניעת הונאות. [...] בעל הרישיון שלוח וכל מי מטעמו אינם רשאים לגלות רשימות או מסמכים בהם רשומים שם ומען של מנוי או כל מידע אחר הנוגע אליו, לרבות פרטי החשבון, תנועת שיחות זמניהן ויעדן לאדם כלשהו פרט למנוי או למי שהסמיך המנוי לכך."

בתשובת המשרד לא צוינה פעילות אחרת כלשהי, להעלאת המודעות של משתמשי טלפונים ניידים לסוגיית פרטיות המידע האישי שלהם ולא צוינה כל פעילות אחרת בעניין ההגנה על הפרטיות, או הפיקוח על פעילות ספקי התקשורת בנושא. לא ברור מתנאי הרישיון האם כאשר משתמש מביע הסכמה לאיסוף מידע אישי שלו ולהעברתו –באמצעות תנאי השימוש עליהם הוא חותם אל מול ספקית הטלפוניה, יכול מידע כזה להיות מועבר ומנותח. יצוין, כי פרקטיקות כאלה נהוגות בחו"ל בקרב ספקיות תקשורת שונות,[29] ולכן גם ספקיות התקשורת יכולות ליטול חלק בשלל מערכי הניטור של משתמשי טלפונים ניידים, כאמור לעיל. יצוין כי מפאת הזמן הקצר, לא פנה מרכז המחקר והמידע של הכנסת לספקיות עצמן, בעניין זה.

5.4. מטה הסייבר הלאומי[30]

מרכז המחקר ומהידע של הכנסת פנה אל מטה הסייבר הלאומי בשאלות באשר לטיפול של המטה בסוגיית הגנת הפרטיות במובייל ובאינטרנט ולהשלכות ככל שישנן על אבטחת המידע של אזרחי ישראל.

על פי תשובת נציג היועץ המשפטי של מטה הסייבר הלאומי, יש להבחין בין סוגיית הפרטיות במידע ובין תחום הגנת הסייבר. תחום הגנת הסייבר עוסק באופן רוחבי וכולל במניעת תקיפות מחשב, שעלולות להביא לגניבת מידע או דלף מידע ולשיבוש אופן הפעולה התקין של מחשבים; בהתמודדות עם תקיפות ובהתאוששות מהן. לעומת זאת, תחום הגנת הפרטיות, עוסק בעיקרו בהסדרה של התנאים המשפטיים לאיסוף מידע אישי ולעיבודו ובעקרונות המשפטיים הקשורים בפעילותו של מי שאוסף מידע. אכן, במקרים מסוימים עשויה תקיפת סייבר לגרום לפגיעה בפרטיות, אך ככלל, תחומי העיסוק והמיקוד שלהם הם שונים.

בהתאמה לאמור, מערך הסייבר הממשלתי, הכולל את מטה הסייבר הלאומי ואת הרשות הלאומית להגנת הסייבר, ממוקד בסוגיות ההגנה על מרחב הסייבר. במסגרת זו נתקבלו בפברואר 2015 שתי החלטות ממשלה המגדירות את ההיערכות המדינתית הכוללת שמטרתה העלאת רמת הגנת הסייבר והגדרת תחומי האחריות להגנת הסייבר ברמה הלאומית, לצד שמירת מרחב הסייבר פתוח ומאפשר

[29] כך לדוגמא, חברת "ורייזון", חברת תקשורת אמריקנית גדולה, שבין השאר בבעלותה מפעילת סלולר וספקית אינטרנט, פרסמה, באוקטובר 2011, מכתב ללקוחותיה ובו פרטים על שינויים במדיניות הפרטיות שלה. על-פי המידע שפרסמה, "ורייזון ויירלס", מפעילת הסלולר של "ורייזון", החברה מפעילה "תוכניות פרסום חדשות" ובמסגרתן ייעשה שימוש במידע שייאסף ממכשירי הסלולר, ובין השאר כתובות אתרים שאליהם גלש הלקוח; מלות חיפוש שהלקוח השתמש בהן; מיקום המכשיר הסלולרי; אפליקציות המותקנות על גבי המכשיר ודפוסי שימוש. נוסף על כך, ייאספו נתונים על שימוש במוצרים ובשירותים של "ורייזון" וכן מידע דמוגרפי ומידע על תחומי עניין, המתקבל מחברות אחרות.

[30] עו"ד עמית אשכנזי, היועץ המשפטי, מטה הסייבר הלאומי, מכתב, 14 ביולי 2014.

זרימה של ידע, הון ושירותים, מחולל חדשנות ותורם לרווחה חברתית, תוך שמירה על זכויות יסוד ובהן הזכות לפרטיות וחופש הביטוי.

כחלק מפעילות הרשות הלאומית להגנת סייבר פועל ה-CERT הלאומי (המרכז הלאומי להתמודדות עם איומי סייבר) שנמצא בהקמה, ה- CERT נועד לספק סיוע למשק האזרחי בהגנת סייבר והוא פועל לסייע בהגנה ובהתמודדות עם תקיפות סייבר. **הרשות הלאומית להגנת סייבר, תקדם בחקיקה, תקינה והנחיות את הגנת הסייבר במשק הישראלי וניתן להניח כי פעילות זו תשפיע בעקיפין גם על ההגנה על מידע.**

5.5. איגוד האינטרנט הישראלי[31]

מרכז המחקר והמידע פנה אל איגוד האינטרנט בשאלות בעניין הנידון, להלן עיקרי תשובת מנכ"ל הארגון.[32]

באשר לפעילות איגוד האינטרנט בנושא הגנת הפרטיות בטלפון הנייד ובאינטרנט צוין בתשובת האיגוד כי הוא פועל בתחומים אלה בהיבטים שונים בהם: הפעלת מרכז לאינטרנט בטוח, העוסק במתן תמיכה, ייעוץ וטיפול בפגיעות ברשת, ובהגברת המודעות לשימוש נבון – ובתוך כך הגנת הפרטיות באינטרנט; בנוסף, נכתב כיום באיגוד מסמך הצעה למדיניות לאומית בנושא "פרטיות קטינים".

באשר לשאלת הסיכון לפרטיות משתמשי הקצה בשל היקפי האיסוף של מידע אישי צוין בתשובת האיגוד בין השאר:

- איסוף ואגירה של מידע, הן באופן ישיר הקשור לזהות של אדם (כגון מספר טלפון), והן באופן שניתן להסיק ממנו על זהותו של האדם, מעלים את פוטנציאל הפגיעה בפרטיות. מומחי פרטיות מציינים כי עצם איסוף המידע ושמירתו במאגר מידע, הם בגדר פגיעה בפרטיות כיוון שכאשר אדם יודע שמידע מסוים שמור לגביו, וכי אחר יוכל לעשות בו שימוש, הוא ישנה את התנהגותו וזאת גם אם לא יעשה כל שימוש בפועל במידע.
- מידע רב נאסף על משתמשים ישראלים ברשת, בין השאר על ידי תאגידים ישראלים וזרים, גופי מדינה ישראלים ויש להניח שגם גופי מדינה זרים, על ידי גופים ללא מטרות רווח וכן גם על ידי יחידים. העובדה כי בדין הישראלי אין חובת מחיקה מוגדרת של מידע, ועלויות נפחי האחסון של מידע דיגיטלי הולכות וקטנות באופן דרמטי, הם בין הגורמים למידת האיסוף הרבה ולמיעוט המגבלות עליו.
- היקפי האיסוף המידע והשימוש בו מעלים את הסיכון לפרטיות של האזרחים. עם זאת, המודעות בקרב הציבור בישראל לנושאי הפרטיות לעומקם אינה גבוהה, וזאת אף שהמסגרת החקיקתית בישראל מספקת הגנה חוקתית לפרטיות וכי בסקרים, סוגיית הפרטיות מועלת באופן קבוע כחשש עיקרי בהקשר לשימוש באינטרנט.

---

[31] עו"ד יורם הכהן, מנכ"ל איגוד האינטרנט, מכתב, 15 ביולי 2016.

[32] יצוין, כי מנכ"ל איגוד האינטרנט היה יו"ר רמו"ט ואחד ממייסדיה ולכן הוא מצוי בסוגיות הפרטיות עוד טרם תפקידו באיגוד.

באשר לחסמים המרכזיים למימוש יעיל של הגנה על הפרטיות, ציין עו"ד יורם הכהן כי קיימים מספר רב של חסמים בהם: 1) **העדר מודעות בציבור** ובקרב המחוקק על החשיבות של ההגנה על הפרטיות למשטר הדמוקרטי; 2) **העדר הבנה בציבור ואצל המחוקקים להשלכות של המודלים הכלכליים והעסקיים של האינטרנט** על האזרחים ובחינה מעמיקה של האיזון הנכון בין שימושיות ואיסוף מידע נרחב; 3) **העדר דיון ציבורי ותקשורתי נרחב בסוגיות הקשורות לפרטיות**; 4) **חקיקה לא עדכנית** – לטענת הכהן, השינוי האחרון בחוק הגנת הפרטיות מ-1981 הקשור ישירות לסוגיות של מידע ממוחשב נעשה בשנת 1996; תקנות אבטחת מידע נוסחו בשנת 1986 – טרם חדירת האינטרנט לשימוש נפוץ; 5) **משטר רגולציה חסר משאבים**- לטענת הכהן חסרות: סמכויות לניהול רגולציה אפקטיבית, חוק ברור ומודרני, ומשאבים כספיים להפעלת מסגרת רגולטורית וביצוע מחקרים ועידוד טכנולוגיות משפרות פרטיות; 6) **הפקדת קידום תהליך החקיקה בידי מחלקת ייעוץ וחקיקה** – ולא בידי הרשות למשפט טכנולוגיה ומידע שהוא הרגולטור בתחום זה; 7) **מודל העסקים באינטרנט** לפיו "המנצח לוקח הכל" גורר דומיננטיות של שחקן יחיד מה שמונע למעשה אפשרות בחירה ומגביל את היכולת "להסכים לעיבוד מידע אישי" בהעדר חלופה אחרת; 8) **הבינלאומיות של האינטרנט והעדרו של משטר משפטי גלובאלי** מקשים על יצירת רגולציה ואכיפה אחידה ומובילים גופים בעלי פוטנציאל הפרת פרטיות לפעול במדינות בהן הרגולציה מקלה יחסית.

הכהן מציין כאמור כי המסגרת החוקית והרגולטורית בישראל איננה מספקת מענה הולם ומסכם את דבריו כך: " על הכנסת לדרוש ממשרד המשפטים להציג תוך פרק זמן קצר הצעת חוק לחוק הגנת מידע אישי, אשר יסדיר מחדש את הכללים לפיהם יש לאסוף ולעבד מידע אישי כגון: הכנסת חובה לעיצוב לפרטיות (Privacy By Design) בכל תכנון, יישום והפעלה של מערכת המנהלת מידע אישי או חובת הודעה על כשל אבטחת מידע (breach notification notice) וכן מסגרת רגולטורית עדכנית ואפקטיבית של רשות להגנת מידע אישי, אשר תתוקצב באופן ראוי התואם את היקף המשימות".

5.6. חברת גוגל[33]

מרכז המחקר והמידע של הכנסת פנה אל חברת גוגל בבקשה למידע על תפיסת האיזון בין פרטיות המשתמשים לשיתוף המידע האישי והשפעותיו על השירות למשתמש הקצה ועל כלכלת האינטרנט וסביבת המובייל וכן באשר לשאלות כיצד גוגל פועל לשמירת פרטיותם של משתמשיה. להלן יוצגו עיקרי תשובת גוגל.

על פי תשובת נציגת גוגל, החברה מקדישה מאמצים רבים לוודא כי המשתמשים במוצריה מוגנים היטב ומודעים היטב באשר לשליטה במידע שהם חולקים. לדבריה, החברה מעוניינת להעצים את צרכניה באמצעות המידע שהיא מספקת להם, כך שהם יוכלו להחליט בשקיפות מלאה כיצד הם רוצים להתנהל. לשיטתם, קל למצוא, להבין ולנהל את הגדרות המשתמש והכלים המגדירים את דפוסי השימוש במוצרי החברה. משתמשים המחוברים (Signed In) לשירותי גוגל יכולים לשלוט במידע בחשבון שלהם[34],

[33] נעה אלפנט, מנהלת מדיניות בכירה, גוגל ישראל, מכתב, 17 ביולי 2016.

[34] https://myaccount.google.com/intro?hl=iw

להשתמש בכלי לבדיקת פרטיות[35] ולשלוט במודעות הפרסומיות שהם רואים. ביחס למשתמשים שאינם מחוברים, לדברי נציגת גוגל, אלה נחשפים גם כן למודעות פרסומיות באמצעות "עוגיות" או מזהים אנונימיים אחרים. נציגת גוגל מציינת בתשובתה כי החברה איננה משתמשת בטכניקת "טביעת אצבעות"[36] כדי לספק מודעות ממוקדות וכי אמצעי הזיהוי האמורים מסייעים לחברה להגן על שירותיה, למנוע הונאות ולספק פרסומות רלבנטיות. המדיניות של החברה אוסרת על מפרסמים ומפיצים לעסוק בפעילויות הפולשות לפרטיות המשתמשים.

5.7. חברת פייסבוק[37]

מרכז המחקר והמידע של הכנסת לא פנה אל חברת פייסבוק לקראת דיון זה, עם זאת, להלן תוצג תשובת פייסבוק לפנייה של ועדת המדע והטכנולוגיה לקראת הדיון. בהקשר זה יצוין כי בלי להכריע באשר לטענות בדבר ביצוע האזנה של פייסבוק למשתמשיה, שבעקבותיהן הגישו כמה חברי כנסת הצעות לסדר היום בנושא[38], ובלי לבטל מכוח השוק הניכר שלה, הדיון בעניין פייסבוק הוא מופע ספציפי אחד של סוגיית הפרטיות ברשת האינטרנט שמסמך זה עוסק בה בהרחבה.

לעניין הטענות שהועלו במקורות שונים בתקשורת, בחו"ל ובישראל, בדבר האזנות של פייסבוק למשתמשיה ושימוש בתוכן לשם פרסום ממוקד, על פי תשובת פייסבוק לפניית הוועדה, החברה איננה משתמשת במיקרופון של הטלפון לשם עדכון פרסומות או "פיד החדשות" שלה. הפרסומות מוצגות בהתאם לתחומי העניין של המשתמשים ומידע נוסף בפרופיל שלהם, ולטענתה לא בהתבסס על האזנה לדיבור בסמוך למכשיר.

לטענת החברה, הגישה למיקרופון של הטלפון הנייד של משתמשיה נעשית בכפוף לאישור של המשתמש לשימוש זה וכאשר המשתמש מפעיל יישום של פייסבוק בו נדרש שימוש בתוכן קולי. שימוש כזה יכול להתרחש בעת הקלטת וידאו או במקרה של שימוש ביישום המאפשר למשתמש לשתף מוזיקה או תוכן קולי אחר בעדכוני הסטאטוס שהוא מעלה.

6. עמדות של משתמשים ביחס לפרטיות

מרכז המחקר PEW עוסק במחקר בתחומי האינטרנט וטכנולוגיה, ובחן במספר מחקרים עמדות בציבור ביחס לסוגיות של פרטיות, פיקוח ומעקב. להלן יוצג בקצרה מידע משני מחקרים שונים.[39] למרות,

---

[35] https://myaccount.google.com/intro/privacycheckup/1

[36] טכניקה שכאמור לעיל, מזהה משתמשים באופן חד ערכי על פי צירוף המאפיינים הייחודיים של המידע המצוי על גבי המכשיר (אפליקציות, פרטי מכשיר ועוד).

[37] Simon Milner, Policy Director, Europe, the Middle East and Africa, Facebook, reply to Ms Anat Levi, Managing Director, The Knesset, Science and Technology Committee, 28 June, 2016.

[38] "האזנות שמבצעת הרשת החברתית פייסבוק למשתמשיה – פגיעה חמורה בפרטיות" הצעות לדיון מהיר של חברי הכנסת מיכל רוזין ; רויטל סויד ; עליזה לביא ; ניסן סלומינסקי (מס' 4076 ; 4077 ; 4096 ; 4104).

[39] Jan Lauren Boyles, Aaron Smith and Mary Madden, "Privacy and Data Management on Mobile Devices", Pew Research Center, 5 September, 2012, accessed: 18 July 2016. Mary Madden, Lee Rainie, "Americans'

שייתכן וקיימת שונות מסוימת בתפיסות בעניין בקרב הציבור במדינות שונות, מחקרים אלה, הממוקדים בציבור האמריקאי מספקים אינדיקציה לנושא. בנוסף, יוצג לאחר מכן, מחקר על עמדות והתנהגויות של משתמשי רשת בישראל.

בסקר שפורסם בשנת 2012, עלו הממצאים הבאים:

- **54% ממשתמשי אפליקציות <u>החליטו שלא להתקין</u> אפליקציה לטלפון שלהם כאשר גילו כמה מידע אישי הם יצטרכו לחלוק כדי להשתמש בה.**

- **30% ממשתמשי אפליקציות <u>הסירו אפליקציה</u> שכבר הותקנה על גבי הטלפון שלהם כיוון שהם גילו כי היא אוספת מידע אישי שהם לא רצו לחלוק.**

- סה"כ, שתי הקבוצות (שלא התקינו או שהסירו), מייצגות כ-57% ממשתמשי האפליקציות שבחרו שלא להשתמש באפליקציות מסיבות דומות של פרטיות מידע אישי.

- לא נמצאה שונות משמעותית בשיעורי ההסרה או אי-השימוש באפליקציות לנייד משיקולי פרטיות בהתאם למשתנה הגיל של המשתמש, או בהתאם לסוג מערכת ההפעלה/מכשיר שבו נעשה שימוש.

- **32% ממשתמשי טלפונים ניידים מחקו את היסטוריית הגלישה או החיפוש שלהם מהטלפון הנייד; וכ- 19% מהמשתמשים בטלפון נייד נטרלו את הגישה אל נתוני המיקום שלהם כיוון שהם חששו מגישה של חברות או אנשים אחרים למידע זה.**

- **בקרב משתמשי טלפונים חכמים היה שיעור האנשים שמחקו את היסטוריית הגלישה או החיפוש שלהם גבוה יותר והוא הגיע לכ- 50% מהמשתמשים; 30% ממשתמשי הטלפונים החכמים נטרלו את הגישה לנתוני המיקום שלהם.**

- שיעורי מחיקת ההיסטוריה או נתוני הגלישה בטלפונים ניידים בקרב משתמשים מבוגרים נמוכים בצורה מובהקת מאלה של צעירים. כמו כן, גברים מוחקים יותר מנשים (37% לעומת 28%); הורים מוחקים יותר ממי שאינם הורים (39% לעומת 29%).

- 15% ממשתמשי טלפונים חכמים דיווחו כי חוו הפרה של פרטיותם בשל גישה של אדם אחר אל מכשיר הטלפון שלהם, לעומת זאת, רק 8% מהמשתמשים בטלפון נייד לא חכם דיווחו על חוויה דומה.

Attitudes About Privacy, Security and Surveillance", Pew Research Center, 20 May, 2015, accessed: 18 July 2016.

בסקר שפורסם בשנת 2015 עלו הממצאים הבאים:

- 93% מן הבגירים דיווחו כי יש חשיבות עבורם לשאלה מי ייגש למידע אודותיהם: 74% מתוכם דיווחו כי הדבר חשוב להם מאוד ו-19% מתוכם גרסו כי הדבר חשוב להם במידה מסוימת.
- 90% מן הבגירים טענו כי קיימת חשיבות בשליטה על איזה מידע ייאסף עליהם: 65% מתוכם ייחסו לכך חשיבות רבה ו- 25% ייחסו לכך חשיבות מסוימת.
- 88% ציינו כי חשוב להם שלא יצפו בהם או יאזינו להם ללא אישורם (67% ציינו שזה חשוב מאוד היתר ציינו כי זה חשוב במידה מסוימת);
- עם זאת, שיעור נמוך יותר של 63% גרסו כי יש חשיבות להתהלך ברבים בלא שיזהו אותם (34% גרסו כי זה חשוב מאוד ו-29% חשבו כי זה חשוב במידה מסוימת).
- **76% מקרב הבגירים חשו "לא בטוחים לגמרי" או "כלל לא בטוחים" ביחס לכך שתיעוד הפעילות שלהם באינטרנט, הנשמר על ידי מפרסמים באתרים בהם הם מבקרים, יישאר פרטי ובטוח.**
- **69% מן הבגירים גרסו כי הם אינם בטוחים שתיעוד השימוש שלהם ברשתות חברתיות בהן הם משתמשים יישאר פרטי ובטוח.**
- **66% ציינו כי הם אינם בטוחים כי תיעוד השימוש שלהם במנועי חיפוש ובאתרי צפייה ושיתוף וידאו (Online Video Sites) יישאר פרטי ובטוח.**
- **באשר לתפיסת השליטה של אנשים באיסוף מידע אישי עליהם ובשימוש בו: 38% גרסו כי יש להם "שליטה מסוימת"; 37% גרסו כי "יש להם מעט שליטה", ו-13% גרסו כי "אין להם שום שליטה".**
- **59% מן המשתמשים דיווח כי הסירו "עוגיות" או היסטוריית גלישה; ו-57% סירבו לספק מידע אישי שלא היה קשור לעסקה שביצעו.**
- **25% עשו שימוש בדוא"ל חלופי או שם משתמש זמני[40]; 24% סיפקו מידע מטעה על עצמם; ו-23% בחרו שלא להשתמש באתר אינטרנט שדרש שימוש בשם אמיתי.**
- **10% מן המשתמשים דיווח כי הם הצפינו את השיחות/הודעות הטקסט/ דוא"ל שלהם; ו-9% עשו שימוש בשירותים שמאפשרים לגלוש באופן לא מזוהה (שרת פרוקסי, רשת וירטואלית פרטית –VPN, או אמצעים דומים).**

<u>בהכללה, עולה מן הנתונים דלעיל תמונת מצב על פיה מחד, אנשים מייחסים חשיבות לא מבוטלת לסוגיות של פרטיות, ומאידך, כי הם חשים שיש להם שליטה מועטה יחסית בתפוצת המידע אודותיהם, באיסופו ובהעברתו על ידי שחקנים שונים הקשורים לרשת האינטרנט.</u>

[40] אמצעי הנתפס על ידי המשתמשים ככזה המאפשר להם להסתיר או להגביל את הגישה למידע על פעילותם ברשת.

במאי 2014 פורסם מחקר בנושא "**פרטיות באינטרנט בישראל**" שבוצע על ידי חוקר מהמכללה למינהל ובמימון חברת מיקרוסופט[41], להלן יוצגו עיקרי הממצאים העולים ממנו:

תפיסות ועמדות

- **54% מהגולשים באינטרנט מודעים לכך שגופים מסחריים מתעדים את הרגלי הגלישה שלהם ומשתמשים בו למטרות מסחר.**
- 48% מהגולשים גורסים כי המידע שהם מוסרים באינטרנט מועבר לגורמים נוספים.
- **40% מהגולשים ציינו כי הם אינם יודעים איזה מידע אישי נאסף עליהם באמצעות האינטרנט**.
- **48% מן הגולשים ציינו כי חשים חסרי אונים מול איסוף המידע עליהם בעת הגלישה.**
- 57% מן הגולשים טענו כי הם יודעים כיצד להגן על פרטיותם באינטרנט.
- **64% מן הגולשים מתנגדים למודל העסקי של העברת מידע שנאסף עליהם לגורמים אחרים; 57% הביעו התנגדות לכך שאתר מכירות יציע להם הצעה לחופשה יוקרתית יותר בעקבות זיהוי הגלישה ממכשיר טלפון נייד יקר; 53% הביעו התנגדות לקבלת הצעת מחיר משתלמת יותר על בסיס מידע שהושג מתכתובת דוא"ל עם אדם אחר; ו- 48% התנגדו לפרסומות מותאמות אישית על בסיס היסטוריית חיפוש**.

התנהגויות ברשת

- 53% מהגולשים דיווחו שמעולם לא החליפו סיסמה לשירות הדוא"ל שלהם ו- 36% נוהגים להחליף סיסמה.
- 61% לא גלשו מעולם כאשר הדפדפן שלהם במצב "פרטיות" (שנועד להגביל את אפשרות הניטור של הגלישה) ואילו 24% דיווחו כי הם נוהגים לגלוש במצב פרטיות או באמצעות תוכנות מונעות זיהוי.
- 45% מהגולשים ביטלו פעם אחת או יותר את התקנתה של תוכנה או אפליקציה בשל דרישה לספק מידע אישי רב. פרקטיקה של הסרה בשל דרישה למידע אישי רב, מקובלת יותר בקרב גולשים צעירים מאשר בקרב מבוגרים.

התנהגויות ברשתות חברתיות

- **80% מהגולשים בישראל עושים שימוש ברשת חברתית כלשהי;**
- 96% מהגולשים בגילאי 15- 17 משתמשים ברשת חברתית כלשהי;
- **51% מהמשתמשים ברשתות חברתיות נוהגים לשתף תמונות או סרטונים של עצמם; 43% מהמשתמשים ברשתות חברתיות מתייגם את עצמם או אחרים בתמונות; ו-46% מאפשרים לאפליקציות או יישומים שונים לתעד את מיקומם.** פרקטיקות אלה של שיתוף בתמונות, של תיוג ושל שיתוף מיקום, נפוצות יותר ככל שגיל הגולשים צעיר יותר.

[41] יובל דרור וסער גרשון, "פרטיות באינטרנט הישראלי", מאי 2014, המכללה למינהל.

<u>מן המחקר עלה כי אין זיקה ממשית בין תפיסות ביחס לפרטיות, לבין ההתנהגות בפועל. כך לדוגמא, למרות שכ-50% מן המשיבים ציינו כי הם חשים חסרי אונים אל מול האיסוף המסחרי של מידע אישי עליהם, לא נמצאה שונות בשיעורי השימוש בתיוג בתמונות או שיתוף המיקום; למרות ש-53% מהגולשים מודעים לכך שחברות מתעדות את הרגלי הגלישה שלהם ומשתמשות במידע, אין שונות במידת שיתוף המידע האישי בתמונות וסרטונים, בתיוג, ובהקניית גישה לנתוני מיקום, בין המודעים לאיסוף ולמטרותיו, לאה שאינם מודעים לו.</u> תופעה זו איננה ייחודית למקרה הישראלי, והיא מכונה "פרדוקס הפרטיות.

דיון

בעבר נדמה היה כי רשת האינטרנט מאפשרת פרטיות חסרת תקדים. ביטוי אנונימי בסוגיות שונות, רכישות ותשלום חשבונות, זהות מקוונת פיקטיבית, חיפוש מידע בנושאים רבים ועוד – את כולם יכול היה האדם לקיים מחדרו הפרטי, ללא צורך בחשיפה ישירה. ואולם, הפרטיות באינטרנט היא בעיקרה אשליה: מנגנוני איסוף מידע רבים פועלים ברשת ובטלפונים החכמים זה מכבר ומנגנונים מתקדמים יותר מפותחים כל העת גם ביישומים שונים הקשורים לקונספט "האינטרנט של הדברים" (IOT – ראו התייחסות להלן) או ליישומי ערים חכמות ועוד.

מנגנוני האיסוף והניטור מתעדים לא רק את האתרים שבהם אנו גולשים, העסקאות שאנו מבצעים, ותחומי העניין שלנו, אלא גם את המיקום שלנו, מהירות וכיוון התנועה, תכתובת הדוא"ל, תחלופת המסרים המידיים, התמונות שאנו מצלמים וחולקים, אנשי הקשר שלנו ועוד, לעיתים קרובות הם ידעו לזהות את חתימת הקול שלנו, את טביעת האצבע ואת תווי הפנים שלנו ושל יקירנו.

למרות אשליית הפרטיות, אנו מותירים אחרינו "טביעת רגל" דיגיטלית (Digital Footprint), הולכת וגדלה, כמעט בכל פעילות דיגיטלית. הקלות היחסית שבאיסוף מידע על אדם ומסות המידע הנצברות הופכות גם פריטי מידע טריוויאליים לבעלי משמעות ולכאלה המאיימים על הפרטיות.

מכשירים מתקדמים דוגמת שעונים חכמים, צמידים לפעילות גופנית, משקפיים מתקדמים, רמקולים ביתיים, טלוויזיות חכמות, מקררים חכמים, תרמוסטטים, מחשוב לביש ועוד (המהווים חלק ממצב שבו שלל מכשירים המחוברים לרשת האינטרנט מאפשרים שליטה מרחוק, ניטור ואיסוף מידע לשימושים ישירים ועקיפים – מצב שנהוג לתארו באמצעות המונח "האינטרנט של הדברים"), לצד מערכות ניטור המונים – דוגמת מצלמות וחיישנים שונים שמוצבים במרחב הציבורי, כולם צפויים להציב אתגרים עצומים לתפיסת הפרטיות הישנה, כאשר הם יתווספו למנגנוני הניטור הקיימים זה מכבר ויאפשרו לדעת כמעט כל פרט על אורחות חיינו. הם יספקו לנו מחד ערך מוסף כזה או אחר, ומאידך יגדילו את הניטור ועיבוד המידע האישי לממדים חסרי תקדים.

ניתן לטעון כי הפרטיות היא המטבע שבו אנו משלמים עבור שלל הטובין המוצעים לנו כביכול חינם אין כסף, אך לא ברור עד כמה אנו מודעים למחירים האמיתיים של הוויתור עליה או האם אנו מוכנים לגלם את מחירה האמיתי בצריכה שלנו.

מודלים של שימוש במידע אישי כוללים כבר כיום יצירת מנגנוני אקרדיטציה ואומדן ערך על פי המידע האישי שלנו והעברה שלהם לשחקנים שונים במשק, דוגמת חברות ביטוח, מעסיקים, שירותי בנקאות

ועוד.[42] אופייה הדינמי של הטכנולוגיה ושל יכולות הניטור עשויות לאפשר שלל שימושים נוספים במידע האישי שטרם ניתן לאמוד את השלכותיו.

מאידך, מושג הפרטיות עצמו מצוי כיום במשא-ומתן חברתי, תרבותי ומסחרי ער. לא רק גופים מסחריים בעלי עניין אלא גם חלק ממשתמשי הקצה רואים בתפיסת הפרטיות שטרם ימי האינטרנט תפיסה אנכרוניסטית. גורמים אלה מדגישים את היתרונות שבוויתור על הפרטיות עבור משתמש הקצה כפרט ועבור השוק כמכלול. הם מציינים כי למרות שאנשים מדווחים על עניין רב בפרטיותם, הם אינם מוכנים לוותר על האפשרויות המתקדמות שעידן המידע האישי המנוטר מאפשר להם ואינם מוכנים גם לשלם עבור כל המוצרים שהתרגלו לקבל בחינם. הם מדגישים את תרבות שיתוף המידע האישי ואת חופש הביטוי שעידן זה מאפשר. לשיטתם, שיח הפרטיות, הוא בעיקרו פטרנליסטי ומנסה לעגן ולקבוע עמדות נורמטיביות דווקא בעידן בו נושא הפרטיות עובר תהליך שינוי - כאשר קיימות שלל עמדות התלויות בין השאר במעמד, גיל, מגדר, ושיוך חברתי המשפיעות על תפיסת הפרטיות.[43]

מולם ניצבים מי שגורסים כי אין לראות בזירה של האינטרנט עולם נפרד שאיננו כפוף לכללים החלים בזירות אחרות ולא רואים ברשת גורם המשדד כליל את הזכות לפרטיות. לשיטתם, יש מקום לשיח ער בנושא הפרטיות ואף לקביעת עמדות נורמטיבית באשר לאיזון הרצוי בין ערכים וזכויות שונות, במקום להותיר את האינטרנט כזירה פרוצה שהכללים היחידים החלים בה הם כללי היד הנעלמה של השוק החופשי.

בלי לנקוט עמדה בסוגיות מורכבות אלה, נראה כי **יש מקום לדון בשאלות הנוגעות למידת השליטה שלנו במידע אודותינו, לשקיפות המידע באשר לדפוסי האיסוף והניטור של מידע אישי ולשימושים בו, למידת הבחירה שיש כיום למשתמשי הרשת ולמשתמשי טלפונים חכמים ביחס לאיסוף המידע האישי שלהם, ולהסכמה המודעת לאיסוף זה. בנוסף, נראה כי יש מקום לדון בשאלה האם יש להטיל מגבלות על סוג המידע הנאסף, מידת הפירוט שלו, ההצדקות לאיסופו ומשך שמירתו.**

[42] תהילה שוורץ אלטשולר, "פרטיות בעידן של שינוי", המכון הישראלי לדמוקרטיה, 2012, עמ' 14

[43] שיזף רפאלי ורמי מיקולינסקי, " "חי או מת: שאון דיגיטלי", עם עובד, (טרם פורסם).