



הגנת הפרטיות: סוגיית ההסכמה לאיסוף ולעיבוד של מידע אישי

כתיבה: רועי גולדשמידט | אישור: יובל וורגן

עריכה לשונית: מערכת דברי הכנסת

תאריך: כ"ב בסיון תשפ"ב, 21 ביוני 2022

מבט משווה

תוכן עניינים

מבוא ותמצית.....	1
1. מהי הסכמה ומה משמעותה בהקשר של הגנת הפרטיות בישראל?.....	3
2. ממצאים על מידת היעילות של מסמכי מדיניות פרטיות והסכמה.....	5
וחשש משימוש במידע אישי.....	5
3. מהן מגבלות האפקטיביות של הסכמה כיום?.....	7
3.1 טכנולוגיות חדשות – אתגרים חדשים.....	7
3.2 מהו מידע אישי או מזוהה הראוי להגנת פרטיות?.....	8
3.3 "מעטים קוראים, מעטים עוד יותר מבינים".....	8
3.4 "הסכמה היא משמעותית אם אפשר לסרב לה".....	9
4. עקרונות ההסכמה לפי ה-GDPR של האיחוד האירופי.....	11
5. הסכמה לפי חוק ההגנה על מידע אישי ומסמכים אלקטרוניים של קנדה (PIPEDA).....	13
6. הסכמה במסגרת חוק פרטיות הצרכן בקליפורניה – ארה"ב (CCPA).....	15

מבוא ותמצית

על שולחנה של ועדת החוקה, חוק ומשפט של הכנסת מונחת הצעת חוק ממשלתית לתיקון חוק הגנת הפרטיות. כמו כן מונחת על שולחן הכנסת הצעת חוק פרטית של יושב-ראש הוועדה, חבר הכנסת גלעד קריב. לקראת דיוני החקיקה ביקש מאיתנו צוות הייעוץ המשפטי של הוועדה להציג מידע על סוגיית ההסכמה בהקשר של פרטיות ודוגמאות לנושא ההסכמה בעולם. מסמך זה אינו סקירה משפטית.

חוק הגנת הפרטיות הישראלי קובע: **"לא יפגע אדם בפרטיות של זולתו ללא הסכמתו"**. הסכמה מוגדרת בחוק: "הסכמה מדעת, במפורש או מכללא", אך החוק אינו מגדיר בפירוט מהי הסכמה. לפי הרשות להגנת הפרטיות, הדרישה להסכמה מדעת מטילה על מבקש המידע "חובת יידוע" – חובה להציג לאדם נתונים בנוגע לאיסוף המידע על אודותיו ובנוגע לשימוש בו, כך שתוצג בפניו תמונה מלאה בטרם יחליט אם להסכים למסור מידע.

לפי בארוקס וניסנבאום, האינטרנט בכלל ועידן נתוני העתק – ביג דאטה בפרט, הפכו את ההסכמה לעיקרון שקשה ולעיתים אף בלתי אפשרי לפעול לפיו, וגם האפקטיביות של הסכמה כבר אינה כלי שימושי להגנת הפרטיות. למרות האימוץ של מסמכי מדיניות פרטיות באינטרנט, יש ראיות רבות כי משתמשים אינם קוראים או מבינים את המסמכים האלה.

מגבלות האפקטיביות של הסכמה

מודל ההסכמה כאמצעי להכשרת השימוש במידע אישי עוצב בסביבה טכנולוגית שונה במידה ניכרת מזו שאנו חיים בה כיום:

- מורכבות התנועה של מידע ונתונים מקשה על היכולת להסביר אותם למשתמש בעת שזה נדרש להסכים לאיסוף או לשימושים.
- המעבר לאיסוף באמצעים שאינם מבוססי מסך מעורר שאלה: כיצד אפשר להביע הסכמה לעיבוד מידע על ידי חיישנים?
- חלק מן הגופים האוספים מידע ונתונים ("אגרגטורים") אינם מוכרים למשתמש.
- הריבוי בדרישות הסכמה יוצר עומס יתר של דרישות ושל מידע, וכפועל יוצא מנטרל את המשמעות של תהליך ההסכמה מצד המשתמשים – הם נעשים קהים לנגישות של אחרים למידע האישי שלהם, ובפועל מבינים פחות ומייחסים פחות חשיבות להגנת פרטיותם דווקא בשל ריבוי בקשות ההסכמה.

הסכמה היא משמעותית אם ניתנת הבחירה שלא להסכים לה: למתן שירותים פיזיים או דיגיטליים נדרשת גישה למידע ולנתונים למיניהם, ולעיתים קרובות אף מבקשים להעבירם לצדדים שלישיים כדי לספק שירות. לפי בירנהק, מעקרון ההסכמה נגזר שלנושא המידע תהיה אפשרות אמיתית של בחירה; לשיטתו, ההחלטה שלא למסור מידע אישי ובשל כך לא לקבל גישה לשירות מסוים איננה בחירה במובן המלא של המושג.

במצב שבו הסכמה היא עילה לגיטימית לאיסוף מידע או לעיבודו גם כאשר מדובר במידע אישי ורגיש, או בשימושים שהלגיטימיות שלהם מוטלת בספק – עולה השאלה אם אין למחוקק מקום לשקול נקיטת עמדה פטרנליסטית ולהגן על זכויות מסוימות של נושא המידע – ללא זיקה לשאלת ההסכמה. עם זאת, יצוין כי פתרונות פטרנליסטיים מסוג זה

עלולים לפגוע באוטונומיה של הפרט לקבל החלטות, והם עלולים גם להוביל לאסדרה שתגביל חשיפת מידע גם אם יש אינטרס ציבורי לחושפו.

הסכמה ברגולציית הגנת הפרטיות האירופית (GDPR)

הסכמה צריכה להיות חופשית, ספציפית, מודעת, ועליה להיות ביטוי חד-משמעי (Unambiguous) לרצון של נושא המידע – אותו הוא מבטא בהצהרה או בנקיטת פעולה המסמנים את הסכמתו לעיבוד המידע הנוגע לו.

התנאים לתוקף ההסכמה: המחזיק יוכל להראות (demonstrate) שנושא המידע הסכים לעיבוד המידע שלו; אם ההסכמה ניתנת כחלק מהצהרה כתובה הנוגעת גם לנושאים אחרים, בקשת ההסכמה תוצג באופן מובחן, נגיש ובשפה פשוטה וברורה; נושא המידע יוכל לחזור בו מהסכמתו בכל עת, ובאותה קלות שבה הוא היה יכול להביע את הסכמתו; הסכמה תיחשב "חופשית" כל עוד היא לא הייתה תנאי למימוש חוזה או למתן שירות – למעט אם מדובר בעיבוד שהוא תנאי הכרחי לקיום החוזה או למתן השירות.

לא כל עיבוד של מידע אישי דורש הסכמה, שכן לפי ה-GDPR הסכמה היא רק אחד משישה בסיסים חוקיים לעיבוד מידע אישי – היינו עילות לגיטימיות לעיבוד מידע אישי. כדי שאיסוף, אגירה או עיבוד יהיו חוקיים, די בקיומה של עילה אחת לפחות. עם זאת, יש להגדיר אותה, ואין "להחליף עילה" למפרע.

הסכמה לפי חוק ההגנה על מידע אישי ומסמכים אלקטרוניים של קנדה

החוק הקנדי, שבו מוסדרת הגנת הפרטיות אל מול המגזר הפרטי, עוסק בידיעה ובהסכמה כדרישה או כבסיס העיקרי הנותן לגיטימיות לאיסוף, לשימוש ולהעברה של מידע אישי. ארגונים נדרשים לדווח ליחידים איזה מידע הם אוספים, כיצד הם מתכוונים להשתמש בו ולאיזו מטרה – כדי לאפשר ליחידים להחליט אם להסכים או לסרב לאיסוף ולעיבוד של המידע על אודותיהם ובכך לאפשר להם לשלוט בתפוצת המידע הנוגע להם. **כדי שההסכמה תיחשב למשמעותית (Meaningful) לפי החוק, יש לספק ליחידים הסבר ברור בנוגע למה נאסף; כיצד משתמשים במידע; ועם מי חולקים אותו.** הסכמה תקפה רק אם אפשר לצפות מהיחידים שהארגון משרת, להבין את דפוס ההתנהלות עם המידע (איסוף, שימוש והפצה), את מטרתו ואת השלכותיו. עוד יצוין כי לפי החוק הקנדי, הסכמה – גם מפורשת – איננה מכשירה **כל** סוג של איסוף מידע או לכל מטרה. לפי החוק איסוף, עיבוד או שיתוף של מידע אישי הוא חוקי רק כאשר הוא נעשה למטרה שהאדם הסביר יראה בה מטרה הולמת בהינתן הנסיבות הספציפיות.

הסכמה בחוק פרטיות הצרכן בקליפורניה – ארה"ב

בנובמבר 2020 עברה במשאל עם הצעה 24 לחוק "הזכויות לפרטיות", אשר בעקבותיה תוקן חוק פרטיות הצרכן – ה-CCPA, ונוספו זכויות חדשות בנוגע להגנה על פרטיות. כמו כן, מתוקפה מוקמת בקליפורניה "הסוכנות להגנה על פרטיות" שאמורה להיות גוף אכיפה של החוק. בניגוד למיעוט האזכורים של מונח ה"הסכמה" (Consent) בגרסתו הקודמת של החוק, בחוק המעודכן מוגדרת הסכמה בפירוש ובפירוט, ומאוזכר בו נושא ההסכמה בהקשרים רבים. **בחוק המעודכן נתפסת הסכמה ככזו הניתנת מדעת ומבחירה חופשית, למטרה מסוימת ובאמצעות פעולה מפורשת.** לפי החוק, ההסכמה לא יכולה להינתן באופן נרחב וכללי, ואסור לנסות להשיגה באמצעים מניפולטיביים.

על שולחנה של ועדת החוקה, חוק ומשפט של הכנסת מונחת הצעת חוק ממשלתית לתיקון חוק הגנת הפרטיות.¹ נוסף לכך מונחת על שולחן הכנסת הצעת חוק פרטית של יושב-ראש הוועדה, חבר הכנת גלעד קריב.² לקראת דיוני החקיקה ביקש מאיתנו צוות הייעוץ המשפטי של הוועדה להציג מידע על סוגיית ההסכמה בהקשר של פרטיות וגישות לנושא ההסכמה במדינות נוספות.³ בסקירה שלהלן יוצגו שאלות ותשובות כדי לנסות להאיר את סוגיית ההסכמה, את אתגריה ואת דפוסי ההתמודדות עימה המקובלים או מוצעים בעולם. נבהיר כי סקירה זו אינה משפטית. הדוגמאות להסדרת הנושא במדינות הנסקרות נבחרו הן על רקע היותן מייצגות שלל גישות באשר לסוגיה, הן על בסיס זמינותו של מידע בנושא ממקורות רשמיים או מחקריים. בדוגמאות אלו אין משום התיימרות לייצג את כלל הגישות הרווחות בנושא זה.

1. מהי הסכמה ומה משמעותה בהקשר של הגנת הפרטיות בישראל?

בסעיף 1 לחוק הגנת הפרטיות נקבע: **"לא יפגע אדם בפרטיות של זולתו ללא הסכמתו"**; בסעיף 3 לחוק מצוין כי ההסכמה יכולה להיות במפורש או מכללא; **בתיקון לחוק משנת תשס"ז נוספה להגדרת הסכמה המילה "מדעת"**: **"הסכמה: הסכמה מדעת, במפורש או מכללא"**, כך לפי נוסח החוק.⁴ עם זאת, אין בחוק הגדרה מפורטת להסכמה.⁵

לפי טיוטת מסמך של הרשות להגנת הפרטיות במשרד המשפטים ממאי 2022, הדרישה להסכמה מדעת מטילה על מבקש המידע "חובת יידוע" – חובה להציג לאדם נתונים בנוגע לאיסוף המידע על אודותיו ובנוגע לשימוש בו, כך שתוצג בפניו תמונה מלאה בטרם יחליט אם להסכים למסור את המידע. היקף היידוע ותוכנו עשויים להיות מושפעים מן ההקשר הספציפי ובין השאר מרגישות המידע, מאופי מערכת היחסים בין הצדדים וממידת היכולת של הפרט להתנגד לבקשה.⁶

ההסכמה משנה את המעמד של "צמצום" הפרטיות, והופכת אותה מפגיעה והפרה של החוק לפרקטיקה לגיטימית

¹ הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022.

² הצעת חוק הגנת הפרטיות (תיקון – חיזוק הזכות לפרטיות וההגנה עליה), התשפ"ב-2022 (3179/24/9).

³ יצוין כי בהצעת החוק הממשלתית אין התייחסות לנושא ההסכמה, אך בהצעת החוק של יו"ר הוועדה מוצע בין השאר להוסיף להגדרת הסכמה את המילים "ומרצון חופשי", והסכמת נושא המידע היא בין ההנמקות המתירות פגיעה בפרטיות ועוד.

⁴ חוק הגנת הפרטיות, התשמ"א-1981.

⁵ מיכאל בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות", **משפט וממשל**, י"א, תשס"ח, עמ' 73-9.

⁶ משרד המשפטים, הרשות להגנת הפרטיות, **"חובת יידוע במסגרת איסוף ושימוש במידע אישי – טיוטה להערות הציבור"**, 2 במאי 2022.

סאני כלב מבהיר במאמרו כי משמעותו של סעיף 1 לחוק היא שוויתור על פרטיות בהסכמה שולל את עצם הפגיעה בה – כלומר ההסכמה משנה את המעמד של "צמצום" הפרטיות והופכת אותה מפגיעה והפרה של החוק לפרקטיקה לגיטימית.⁷ לדבריו, הסכמה כביטוי לאוטונומיה מאפשרת לאדם לוותר על זכויותיו או להתיר פגיעה בהן. בהקשר של הסכמה לפגיעה בפרטיות מצוין כלב כי הדין הישראלי מתיר לפרט לקבוע את מסגרת פרטיותו ואת מידת ההגנה עליה – ובכלל זה גם את הזכות לוותר על פרטיותו. עם זאת, האוטונומיה של האדם בהחלטות אלה מוגבלת – למשל אין די בהסכמתו כדי להתיר חיפוש במחשבו ללא חשד סביר וללא צו.⁸

"הסכמה מדעת", שלשיטתם של בירנהק וכלב התפתחה רבות בהקשר הרפואי, מוגדרת: **"הסכמה תקפה, שניתנה על ידי אדם הכשיר לקבל החלטה בעניין הנדון, מתוך רצון חופשי, בלי אונס או כפייה ועל בסיס מידע מלא ורלוונטי שהובן על ידו"**.⁹ הסכמה מדעת נועדה לשמר את האוטונומיה של החולה ואת הגדרתו כסובייקט שיש לו זכויות על גופו, לאפשר לו להשתתף בתהליכי קבלת ההחלטות הנוגעים לו ובכך גם לתמרץ את הרופאים לפעול בצורה מחושבת ומיטבית לטובתו ולצמצם טעויות, רשלנות או אינטרסים זרים בתהליך הטיפול. יצוין כי גם בהיבט הרפואי ההסכמה והאוטונומיה של האדם על גופו מוגבלת – למשל אדם אינו רשאי להסכים לסחר באיבריו. עם זאת, **נראה כי אפשר להחיל את עקרונות ההסכמה מדעת בהקשר הרפואי גם להקשר של פרטיות – וההנחה כי אדם המבין איזה מידע נאסף עליו, מה נעשה במידע שלו ולאילו מטרות, יוכל לקבל החלטות מחושבות יותר, כך שישרתו את טובתו.**

בגישה שמקובל לתאר במושג "פרטיות כשליטה", ממקד בירנהק את הגרעין של תפיסת הפרטיות בעצם השליטה של אדם במידע עליו. **בפעולות איסוף, עיבוד, שמירה, העברה לצד שלישי, פרסום ועוד יש משום פגיעה בפרטיות אם הם נעדרים הסכמה של מושא האיסוף (בניסוח המקובל בחוק – "נושא המידע"), ולשיטתו אין בהן משום פגיעה בפרטיות אם מושא האיסוף מסכים לפעולות אלו.**¹⁰

לפי עקרונות השימוש
ההוגן נדרש כי נושא
המידע יעודכן
בפרטים אלו:
מי אוסף עליו מידע;
מה המידע הנאסף;
כיצד משתמשים
במידע,
אם הוא מופץ,
ואם איסוף המידע
הוא הכרחי או
אופציונלי.

⁷ סאני כלב, "אני מחליט עליי" – פרטיות של ילדים בעידן הדיגיטלי והזכות לחזור מהסכמה הורית, **עיוני משפט** (מ"א) 2018, עמ' 61–112. שם.

⁹ עפרה גולן, "דרישת הסכמה מדעת כביטוי לכבוד האדם", **שערי משפט** ב, 171, 172 – ראו כלב, הערת שוליים 62.

¹⁰ מיכאל בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות", **משפט וממשל**, י"א, תשס"ח, עמ' 9–73.

לפי בארוקס וניסנבאום, שורשי המרכזיות של מושג ההסכמה בחקיקה הנוגעת לפרטיות, מקורם בעקרונות השימוש ההוגן במידע (FIPPS), שאימצה נציבות הסחר הפדרלית, ה-FTC, בארה"ב ב-1998.¹¹ בתמצית העקרונות הללו דורשים כי נושא המידע יקבל התראה, כלומר יעודכן בפרטים אלו: מי אוסף עליו מידע; מה המידע הנאסף; כיצד משתמשים במידע, אם הוא מופץ, ואם איסוף המידע הוא הכרחי או אופציונלי. עם זאת, לפי בארוקס וניסנבאום, האינטרנט בכלל ועידן נתוני העתק – ביג דאטה בפרט, הפכו את ההסכמה לעיקרון שקשה ולעיתים אף בלתי אפשרי לפעול לפיו, וגם האפקטיביות של הסכמה כבר אינה כלי שימושי להגנת הפרטיות. לדבריהם, **למרות האימוץ של מסמכי מדיניות פרטיות באינטרנט, שנראה כמעט כמו העתקה של חוזים מודפסים לרשת, הרי שישנן ראיות רבות כי משתמשים אינם קוראים או מבינים מסמכים אלו.** כמו כן, כדי להסכים מדעת נדרש לדעת את הפרטים האלה: מה נאסף, עם מי חולקים את המידע, לאילו מטרות חולקים אותו ובאילו מגבלות עושים זאת. לא זו בלבד שמדיניות פרטיות – ובפרט מדיניות פרטיות שנדרשת להיות פשוטה וברורה – אינה כוללת לרוב תשובות מספקות על השאלות הללו, אלא שלטענת ניסנבאום ובארוקס, איסוף הנעשה כחלק מהפקתם, מתאפיין בתנועה רב-כיוונית ובעת האיסוף לא תמיד ברורים השימושים שלו או הערך שלו ומכאן גם התפוצה שלו – לכן עולים קשיים נוספים בקבלת הסכמה מדעת, כלומר הסכמה אמיתית ובעלת משמעות.¹²

2. ממצאים על מידת היעילות של מסמכי מדיניות פרטיות והסכמה

חשש משימוש במידע אישי

ממחקרים בנושא עולה כי היעילות של ההסכמה אינה ברורה, וכי ספקי שירות בתחום מעצבים לעיתים קרובות את פלטפורמות ניהול ההסכמה (CMP) באופן שעשוי לעודד בחירה באפשרויות הפוגעות בפרטיות הגולש.

במחקר מקיף שפורסם בשנת 2018, נבחנו מסמכי "מדיניות פרטיות" (privacy policy) של 191 אתרים פופולריים, ועלה כי הם הכילו 2,716 מילים בממוצע¹³, כי ב-82% מהמסמכים היה הטקסט מעוצב ברווח בודד בין השורות, וכי רק בתשעה מתוך 191 המסמכים היו "כפתורים" נגישים הניתנים לזיהוי בקלות, שאפשרו לשנות את ברירת המחדל בקלות (opt out buttons); ב-82% מהמסמכים לא נמצא שום אלמנט גרפי, ובמסמכים שנמצא בהם אלמנט גרפי לרוב היה מדובר בסמל החברה או בסמל של הסמכה כחברה המגינה על המסחר (TRUSTe). לפי המאמר, מניתוח מסמכי המדיניות עולה כי הם אינם מעוצבים באופן המתייחס לשאלות עד כמה

¹¹ Solon Barocas and Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent", In Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum (Editors), **Privacy, Big Data, and the Public Good – Framework for Engagement**, Cambridge, 2014, pp. 44–75.

¹² שם.

¹³ כמחצית מהמילים במסמך זה.

הם קריאים, ניתנים להבנה ונגישים. כמו כן, מסמכים ארוכים ומסובכים קשים יותר לקריאה אם הם מוגשים בטקסט צפוף, כתובים בגופן קטן ולרוב ללא הבחנה בצבע או בגודל הגופן בין הטקסט לכתורות או לכתורות המשנה. בשל האמור, לפי המאמר ייתכן כי העיצוב של מסמכי המדיניות הללו מעודד את המשתמשים לוותר על קריאתם עוד בטרם הם מתחילים בה.¹⁴

במחקר מ-2020 נבחנה ההסכמה לשימוש בעוגיות מעקב (cookies)¹⁵ באינטרנט, ונמצא כי ביותר ממחצית מהפלטפורמות שנבחנו לא הייתה אפשרות לדחות את כל העוגיות; ביותר מ-70% מהמקרים, כאשר הייתה אפשרות לדחות את כל העוגיות, היא הוצגה במיקום נסתר מהאפשרות לקבל את כל העוגיות. באתרים שפירוטו כחלק מתהליך ההסכמה את מספרם של עוקבי צד שלישי (Third party trackers) אחר דפוסי הגלישה, היה החציון 315 עוקבים.¹⁶

לפי סקר שערך מכון המחקר פיו (Pew) בשנת 2019 בקרב אזרחים אמריקאים בוגרים, כ-79% מן המשיבים היו מודאגים מן השימושים של חברות במידע שלהם, ו-64% היו מודאגים מן השימושים של הממשלה במידע שלהם. רוב המשיבים גם חשים כי אין להם שליטה או כי יש להם מעט שליטה על אופני השימוש במידע האישי שלהם. **למרות החשש שהמשיבים הביעו באשר לפרטיותם, רק כחמישית מהמשיבים ציינו כי הם תמיד (9%) או לעיתים קרובות (13%) קוראים את מדיניות הפרטיות בטרם הם מאשרים אותה.** 38% מהמשיבים ציינו כי לעיתים הם קוראים מסמכי מדיניות כאלה, ו-36% ציינו כי הם אינם קוראים אף פעם את מסמכי מדיניות הפרטיות טרם אישורם. נוסף על כך, **גם בקרב המשיבים כי הם קוראים את מסמכי מדיניות הפרטיות, רק 22% ציינו כי הם קוראים את כל המסמך טרם אישורם.** עוד עלה מן הסקר כי **63% מן המשיבים ציינו כי הם מבינים מעט או לא כלום בנוגע לחוקים ולתקנות המגינים על פרטיות המידע שלהם.**¹⁷

¹⁴ Ari Ezra Waldman, "Privacy, Notice and Design", **Standard Technology Law Review** (21), pp. 74–127, 2018.

¹⁵ עוגיות (Cookies) הן קובצי טקסט קטנים שאתרי אינטרנט מתקינים במחשב (או בהתקן קצה אחר) של המשתמש בעת שהוא גולש באינטרנט, והן מעובדות ונשמרות באמצעות הדפדפן.

¹⁶ Midas Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1–13, April 2020.

¹⁷ Pew Research Center, "[Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information](#)", November 2019.

מסקר של איגוד האינטרנט ועמותת פרטיות ישראל מינואר 2022, שנערך בקרב מדגם מייצג של ישראלים מעל גיל 18, עלו בין השאר הממצאים הבאים: 64% מן המשיבים מרגישים כי אין להם שליטה על המידע האישי עליהם ברשת; 57% מן המשיבים הביעו חשש שרשויות המדינה ישתמשו במידע עליהם ללא ידיעתם והסכמתם; 69% מן המשיבים הביעו חשש ממה שחברות וארגונים מסחריים יוכלו לעשות במידע שלהם בעתיד; 85% מן המשיבים הביעו רצון לדעת כיצד חברות וארגונים מסחריים משתמשים במידע על אודותיהם; 58% מן המשיבים ציינו כי פרסום ממוקד או מותאם אישית מטריד אותם.¹⁸

3. מהן מגבלות האפקטיביות של הסכמה כיום?

להלן נציג בקצרה את המגבלות ואת הביקורות הרווחות באשר להסכמה בהקשר של פרטיות ושל הגנת מידע:

3.1 טכנולוגיות חדשות – אתגרים חדשים

כאמור לעיל, מודל ההסכמה כאמצעי להכשרת השימוש במידע אישי או פרטי כפי שעוצב ברגולציות פרטיות במדינות רבות, עוצב בסביבה טכנולוגית שונה במידה ניכרת מהסביבה הטכנולוגית שאנו חיים בה כיום. "האינטרנט של הדברים" (IoT) ובכללו מחשוב לביש, חיישנים המותקנים במרחב הביתי או מערכות חישה המופעלות יותר ויותר במרחב הציבורי, מצלמות, דפוס גלישה ברשת, נתוני מיקום, שימוש באפליקציות רבות בטלפון החכם ועוד, יוצרים שרשראות הפצה ותנועה של מידע אישי שכבר אינו נחלתם הבלעדית של שני צדדים לעסקה, אלא טביעת אצבע דיגיטלית המלווה את התנועה של הפרט במרחב הדיגיטלי והפיזי.

מורכבות התנועה של מידע ונתונים מקשה להסביר אותם למשתמש בעת שזה נדרש להסכים לאיסוף או לשימושים. כמו כן, חלק מן הגופים האוספים מידע ונתונים ("אגרגטורים") אינם מוכרים למשתמש, שכן לרוב הם אינם מתנהלים ישירות מולו אלא רק מול חברות או גופים אחרים, שהם מקורות לאיסוף או להפצה מחודשים של המידע. לפיכך יש קושי להבהיר למשתמש מי אוסף או משתמש במידע; איזה מידע נאסף; לאיזו מטרה המידע נאסף – כיוון שלא תמיד המטרה ברורה ומוגדרת כבר בשלב האיסוף.

המעבר לאיסוף באמצעים שאינם מבוססי מסך, כגון חיישנים הפזורים במרחב הביתי ואף יותר מכך במרחב הציבורי – מעורר שאלה: כיצד אפשר להסכים לעיבוד מידע על ידי חיישנים – בפרט אם בחלק מן המקרים קשה או בלתי אפשרי לסרב לו? גם אם מדובר בחיישנים חכמים במרחב הביתי, כגון רמקולים "חכמים", טלוויזיות "חכמות", שעונים "חכמים" וכו', לעיתים קרובות נבנים מנגנוני הסכמה כחלק מתנאי השימוש בשלב ההפעלה הראשוני, והם נבנים בדרך שבה קשה עד בלתי אפשרי להפריד בין שימושים הכרחיים לתפעול של היישום לשימושים משניים במידע.

¹⁸ איגוד האינטרנט הישראלי, "תחושות ועמדות הציבור הישראלי ביחס לפגיעה בפרטיות", פברואר 2022.

עידן ה"אינטרנט של הדברים" ונתוני העתק יוצר שרשראות הפצה ותנועה של מידע אישי שכבר אינו נחלתם של שני צדדים לעסקה, אלא טביעת אצבע דיגיטלית המלווה את הפרט במרחב הדיגיטלי והפיזי

3.2 מהו מידע אישי או מזוהה הראוי להגנת פרטיות?

מידע או נתונים חוסים תחת המטרייה של הגנת הפרטיות אם הם קשורים לנושא מידע ספציפי, ומכאן משתמע כי מידע שאינו מזוהה (מידע אנונימי או מידע שעבר "התממה"), אינו מוגן באותו אופן. יש לזכור כי השימוש בנתוני עתק יכול לזמן תובנות מחקריות או טובין חברתיים רבים, ולכן אם אין פגיעה בזכויות של נושא המידע, או בהתאם לעילות אחרות (שאליהן נתייחס בהמשך) או בכפוף להסכמה של נושא המידע, הרי שהשימוש יכול להיות ראוי וחיוני. עם זאת, החיבור של הרבה פיסות מידע אנונימיות על נושא מידע – גם כאשר הוא נותר כביכול אנונימי ומקבל רק מספר סידורי שרירותי המאפשר לקשור את פריטי המידע לאותו פרט – יוצר מצב שבו גם בהיעדר שם או מספר זיהוי נוצר "פרופיל ייחודי" של משתמש. בארקוס וניסנבאום אף טוענים כי חלק מן החברות בוחרות במודע שלא לשמור שם משתמש או מידע המאפשר זיהוי, ובכך הן נמנעות ממצב שבו הן כפופות לחוקי הפרטיות במלואם ובפרט אינן נדרשות להסכמה של המשתמש החוסה כביכול תחת מעטה אנונימיות – אך בפועל נהפך למשתמש בעל פרופיל מובחן, ובכלל זה העדפות, דפוסי צריכה, תחומי עניין, מצב בריאותי וכדומה. עוד הם טוענים כי גם אם רק מעטים מסכימים, אפשר ללמוד גם על אחרים – אף שסירבו לחלוק מידע, באמצעות מתאימים או שיטות למידת מכונה מתקדמות, ובכך לחשוף מידע גם על מי שסירב לספק אותו.¹⁹

יצוין כי יש מחקרים שקראו תיגר על עצם ההנחה כי אפשר לבצע התממה בלתי הפיכה של מידע.²⁰

עוד יצוין כי לצד היתרונות בשימוש בנתוני עתק יש חשש משימושים לרעה בהם: תמחור מפלה; פרסום מבוסס יצירת פרופילים גזעיים, אי-דיוקים והטיות מכונה – כל אלה צפויים לפגוע יותר באוכלוסיות חלשות או מודרות דווקא.²¹

3.3 "מעטים קוראים, מעטים עוד יותר מבינים"

כאמור, גם כאשר מסמכי מדיניות פרטיות מונגשים על גבי מסך המחשב או הטלפון, הם מעוצבים בעיקרם כטקסט חוזי, ארוך, משפטי ודקדקני. כפועל יוצא הם אינם נהירים לרוב המשתמשים, וכפי שהוצג לעיל, יש מחקרים המצביעים על כך שמעט משתמשים קוראים אותם ומעטים עוד יותר מבינים אותם.

¹⁹ Solon Barocas and Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent", In Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum (Editors), **Privacy, Big Data, and the Public Good – Framework for Engagment**, Cambridge, 2014, pp. 44–75.

²⁰ Rocher, L., Hendrickx, J.M. & de Montjoye, YA, "Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models", **Nature Communications**, 10, 3069 (2019).

²¹ רועי גולדשמידט, "אפלייה אלגוריתמית במערכות המבוססות על בינה מלאכותית", מרכז המחקר והמידע, יוני 2020.

השימוש בנתוני עתק יכול לזמן תובנות מחקריות או טובין חברתיים רבים, ולכן אם אין פגיעה בזכויות של נושא המידע, או בכפוף להסכמה של נושא המידע, הרי שהשימוש יכול להיות ראוי וחיוני

יש הטוענים כי הריבוי
בדרישות הסכמה
יוצר מצב של עומס
יתר של בקשות
הסכמה, עומס יתר
של מידע וכפועל יוצא
גורם לאובדן
המשמעות של תהליך
ההסכמה

שרמר, קוסטר ואחרים אף גורסים כי הריבוי בדרישות הסכמה יוצר מצב של עומס יתר, וכפועל יוצא מנטרל את המשמעות של תהליך ההסכמה מצד המשתמשים - הם נעשים קהים לנגישות של אחרים למידע האישי שלהם, ובפועל מבינים פחות ומייחסים פחות חשיבות להגנת פרטיותם דווקא בשל ריבוי בקשות ההסכמה.²²

במצב שבו הסכמה היא עילה לגיטימית לאיסוף מידע או לעיבודו, גם כאשר מדובר במידע אישי ורגיש, או בשימושים שהלגיטימיות שלהם מוטלת בספק, עולה השאלה אם אין למחוקק מקום לשקול נקיטת עמדה פטרנליסטית ולהגן על זכויות מסוימות של נושא מידע - ללא זיקה לשאלת ההסכמה. במילים אחרות, כל עוד הסכמה יכולה לשמש עילה לגיטימית גם לפרקטיקות פסולות, מתבקש לשאול אם אין מקום לנקוט עמדה ערכית שאינה מתירה כל סוג של איסוף בהינתן הסכמה, אלא רק בתנאים מסוימים, כגון איסוף מידתי בזיקה לשירות, שהמשתמש היה יכול להניח שייעשה במידע שלו. לפי כלב, **חסרונות אפשריים לפתרונות פטרנליסטיים כאלה: הם עלולים לפגוע באוטונומיה של הפרט לקבל החלטות, והם עלולים גם להוביל לאסדרה שתגביל חשיפת מידע גם אם יש אינטרס ציבורי לחושפו.**²³

יצוין כי לפי בירנהק, "עקרון צמידות המטרה" - היינו שמידע הנאסף למטרה מסוימת מותר לשימוש רק למטרה שלשמה נאסף, הוא עיקרון משלים לעקרון ההסכמה - כלומר ההסכמה, בפרט מדעת, ניתנת למטרה מסוימת, ושימושים בה למטרות אחרות הם אסורים. עם זאת, גם בירנהק מציין כי יש חשש שהאוסף יגדיר את מטרת האיסוף בצורה כללית ורחבה, ובכך יאפשר שימושים נרחבים במידע.²⁴

3.4 "ההסכמה היא משמעותית אם אפשר לסרב לה"

למתן שירותים פיזיים או דיגיטליים נדרשת גישה למידע ולנתונים, ולעיתים קרובות אף מבקשים להעבירם לצדדים שלישיים כדי לספק שירות. בכך למעשה מצמצמים ולעיתים אף מבטלים את המשמעות של הסכמה לאיסוף או לעיבוד של מידע. אומנם בחלק מן המקרים הדרישה למידע נועדה לאפשר את עצם הספקת השירות, אך במקרים אחרים אין כל זיקה בין המידע המבוקש לשירות עצמו, וזה מתבקש כאמצעי להפקת רווח משיתוף או ממכירה של המידע האישי.²⁵

²² Bart W. Schermer, Bart Custer, Simone Van der Hof, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection", **Ethics and Information technology**, (16), 2014, pp. 171-182.

²³ סאני כלב, "אני מחליט עליו" - פרטיות של ילדים בעידן הדיגיטלי והזכות לחזור מהסכמה הורית, **עיוני משפט** (מ"א) 2018, עמ' 61-112.

²⁴ מיכאל בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות", **משפט וממשל**, י"א, תשס"ח, עמ' 9-73.

²⁵ ביטוי מקובל לדפוס השימוש האמור הוא הביטוי הזה: "אם אתה לא משלם עבור המוצר, אתה המוצר".

לדברי בירנהק, "כלל נוסף שנגזר מעקרון ההסכמה הוא שלמושא המידע תהיה אפשרות אמיתית של בחירה". אם נותנים לאדם אפשרות בחירה שאין בה ממש – כמו האפשרות שלא למסור מידע אישי, אך בשל כך גם לא לקבל גישה לשירות מסוים, הרי שאין זו בחירה במובן המלא של המושג.²⁶

בהקשר זה ראוי לציין כי ככל הנראה בשל האימוץ של הרגולציה האירופית ה-GDPR הרי שאתרי אינטרנט רבים דורשים כיום ממשתמשים את אישור מדיניות הפרטיות שלהם ובפרט אישור על השימוש שהם עושים ב"עוגיות" (cookies) לצורכי איסוף מידע על משתמשים. ככלל, בשל הנחיות החוק אמורים האתרים שלא להשאיר את דפוסי האיסוף הנרחבים כברירת מחדל, אלא רק איסוף שהוא הכרחי לצורכי התפעול של השירות.²⁷

רשת האינטרנט עדיין מתאפיינת באיסוף מידע אישי. שומרי סף ספציפיים, בפרט ענקיות הרשת, שולטים בצומתי מידע ובתשתיות מידע המקנים להם יתרון מבחינת תחרות

ככלל, באופן המממש את עקרון הבחירה, גם אתרים או שירותים אינם אמורים להתנות את האפשרות להשתמש בשירותי האתר בהסכמה לאיסוף נרחב – בכך בפועל הם מאפשרים בחירה והסכמה משמעותית יותר. עם זאת, יצוין כי יש אתרים המנסים לעצב את מנגנוני ההסכמה והאישור לאיסוף באופן שימקסם את חלקם של המשתמשים המאשרים אותו, בין השאר באמצעים גרפיים או אחרים, וכך רק מי שנכנס בפועל להגדרות האיסוף יוכל לצמצם את היקפו. דוגמה זו מראה מחד את כוחה של הרגולציה האירופית בהשפעה על השימוש בכלי איסוף מידע על גולשים, ומאידך את המגבלות שלה – הבאות לידי ביטוי בקשות ההסכמה הן בניסיונות לעקוף את הצורך בה. כמו כן, נראה כי האקו-סיסטם של האינטרנט עדיין מתאפיין באיסוף מידע אישי נרחב כחלק ישיר או עקיף מאספקת שירותים; שומרי סף ספציפיים – בפרט הדומיננטיים, כמו חלק מענקיות הרשת – שולטים בצומתי מידע ובתשתיות מידע היוצרים אצלם יתרון מבחינת תחרות, והם אוספים מידע ופוגעים הן בתחרותיות של שחקנים אחרים הן ביכולת להגן על פרטיות המשתמשים מפניהם.²⁸

²⁶ שם.

²⁷ רועי גולדשמידט, "[על עוגיות וטכנולוגיות זיהוי מקוון נוספות](#)", מרכז המחקר והמידע של הכנסת, מרץ 2021.

²⁸ שם.

4. עקרונות ההסכמה לפי ה-GDPR של האיחוד האירופי²⁹

להלן נסביר בקצרה את העקרונות של הסכמה ברגולציית הגנת הפרטיות האירופית.³⁰

לא כל עיבוד של מידע אישי דורש הסכמה, שכן לפי ה-GDPR הסכמה היא רק אחת משישה בסיסים חוקיים לעיבוד מידע אישי – היינו עילות לגיטימיות לעיבוד מידע אישי. להלן חלק מהעילות המופיעות בסעיף 6 לרגולציה:

- **הסכמה למטרה או מטרת ספציפיות;**
 - קיומו של חוזה או היערכות לחוזה שנושא המידע הוא צד לו;
 - קיום חובה משפטית של המחזיק במידע;
 - הגנה על אינטרס חיוני של נושא המידע או של אדם אחר;
 - מימוש אינטרס או משימה ציבורית (בעיקר, אך לא רק בידי גוף ציבורי);
 - אינטרס לגיטימי של המחזיק או של צד שלישי, למעט אם הוא מנוגד לאינטרסים או לזכויות יסוד וחירויות של נושא המידע – בפרט אם מדובר בקטין.
- כדי שאיסוף, אגירה או עיבוד יהיו חוקיים, די בקיומה של עילה אחת לפחות. עם זאת, יש להגדיר אותה, ואין "להחליף עילה" למפרע.

לפי הגדרת ה-GDPR (4.11), הסכמה צריכה להיות חופשית, ספציפית ומודעת, ולהביא לידי ביטוי באופן חד-משמעי (Unambiguous) את רצון נושא המידע. ביטוי זה ניתן באמצעות הצהרה או נקיטת פעולה המסמנות את הסכמתו לעיבוד המידע הנוגע לו.

²⁹ GDPR.EU, "[What Are the GDPR Consent Requirements?](#)", accessed: May 19th 2022.

המכון הישראלי למדיניות טכנולוגית, "[מבט השוואתי על מודלים של הגנת הפרטיות - לקראת תיקוני החוק בישראל: סיכום ותובנות מהמפגש הראשון בנושא בסיסים חוקיים לעיבוד מידע](#)", פברואר, 2022.

ראו גם: ירון אונגר, "[התקנות האירופיות בעניין הגנת מידע \(GDPR\)](#)", הכנסת, הלשכה המשפטית תחום חקיקה ומחקר משפטי, 12 ביוני 2018.

³⁰ יצוין כי המסמך אינו עוסק בחקיקת "השווקים הדיגיטליים", ה-Digital Markets act. אומנם החקיקה האמורה (שטרם הושלמה) עוסקת בהגדרתם של שחקנים דומיננטיים בשווקים הדיגיטליים, שהם בגדר "שומרי סף" (gatekeepers) ובקביעת כללים ומגבלות על פעילותם כדי למנוע מהם לנצל את כוח השוק שלהם ולפגוע בתחרות, אך גם נושא ההסכמה זוכה להתייחסות – ראו [טיוטת חקיקה](#) מ-11 במאי 2022.

אלה התנאים לתקפותה של ההסכמה:

- המחזיק יוכל להראות (demonstrate) שנושא המידע הסכים לעיבוד המידע שלו;
- אם ההסכמה ניתנת כחלק מהצהרה כתובה הנוגעת גם לנושאים אחרים, בקשת ההסכמה תוצג באופן מובחן, נגיש, ובשפה פשוטה וברורה.
- נושא המידע יוכל לחזור בו מהסכמתו בכל עת, ובאותה קלות שבה הוא היה יכול להביע את הסכמתו. (החזרה מהסכמה אינה משנה את חוקיות העיבוד של המידע הנעשה טרם החזרה מהסכמה).
- הסכמה תיחשב "**חופשית**" כל עוד היא לא הייתה תנאי למימוש חוזה או לאספקת שירות – למעט אם מדובר בעיבוד שהוא תנאי הכרחי לקיום החוזה או לאספקת השירות.

בהסכמה **ספציפית** הכוונה היא כי אין די בהגדרה כללית שמאזכרים בה פריטי מידע הנאספים למטרות מגוונות, אלא יש לפרט את מטרת איסוף המידע באשר לכל פריט מידע שנאסף. לדוגמה, אין די בניסוח "המידע והנתונים משמשים לצורכי שיווק" בעת איסוף של כתובת IP וכתובת דוא"ל, אלא יש לציין מהן המטרות של איסוף כתובות ה-IP, ומהן המטרות של איסוף כתובות הדוא"ל, ויש לאפשר למשתמש – נושא המידע, להסכים רק לחלק מהאיסוף ורק לחלק מהמטרות – כלומר להיות מסוגל להבחין בין עילות איסוף, וכן יש לאפשר סירוב מוחלט.

הסכמה **מדעת** פירושה שנושא המידע יודע מי אוסף עליו מידע, אילו פעולות עיבוד בכוונתו לבצע במידע, מהן מטרות העיבוד, וכן כי יש באפשרותו לסגת מהסכמתו בכל עת. את בקשת ההסכמה וההסברים באשר לעיבוד ולעילותיו יש לנסח בשפה ברורה וללא שימוש במונחים משפטיים או טכניים, כדי שמי שניגש לשירות יוכל להבינם.

הסכמה **חד-משמעית** או שאינה משתמעת לשתי פנים היא כזאת שבה אין כל ספק שהמשתמש הסכים. לכן הסכמה שהושגה באמצעות "תיבות מסומנות מראש", או הסכמה שהמשתמש לא נדרש לנקוט שום פעולה כדי להביעה – אינן תקפות.

לפי ה-GDPR,
הסכמה מדעת
פירושה שנושא
המידע יודע מי אוסף
עליו מידע, אילו
פעולות עיבוד
בכוונתו לבצע
במידע, מהן מטרות
העיבוד,
וכן כי יש באפשרותו
לסגת מהסכמתו בכל
עת

5. הסכמה לפי חוק ההגנה על מידע אישי ומסמכים אלקטרוניים של קנדה (PIPEDA)³¹

החוק הפדרלי העיקרי שבו מוסדר נושא ההגנה על פרטיות במגזר הפרטי בקנדה³², הוא חוק ההגנה על מידע אישי ומסמכים אלקטרוניים, משנת 2000, Personal Information Protection and Electronic Documents Act (להלן – "החוק" או "החוק הקנדי").³³ להלן נסביר בקצרה את עקרון ההסכמה בחוק. המידע מבוסס בעיקרו על מסמך נרחב בנושא פרטיות והסכמה של משרד הנציב לענייני פרטיות של קנדה³⁴ (הגוף המקביל לרשות להגנת הפרטיות בישראל).

החוק הקנדי רואה בידעיה ובהסכמה דרישה או בסיס הלגיטימיות העיקרי לאיסוף, לשימוש ולהעברה של מידע אישי. ארגונים³⁵ נדרשים לדווח ליחידים (individuals) איזה מידע הם אוספים, כיצד הם מתכוונים להשתמש בו ומה מטרת השימוש – כדי לאפשר ליחידים להחליט אם להסכים או לסרב לאיסוף המידע על אודותיהם ולעיבודו, ובכך לאפשר להם לשלוט במידע הנוגע להם ובתפוצתו.

לפי החוק הקנדי, כדי שהסכמה תיחשב למשמעותית (Meaningful), יש לספק ליחידים הסבר ברור באשר ל"מה" נאסף; "כיצד" משתמשים במידע; ו"עם מי" חולקים אותו

כדי שהסכמה תיחשב משמעותית (Meaningful) לפי החוק, יש לספק ליחידים הסבר ברור בנוגע ל"מה" נאסף; "כיצד" משתמשים במידע; ו"עם מי" חולקים אותו. הסכמה תקפה רק אם אפשר לצפות מיחידים שהארגון משרת, להבין את דפוס ההתנהלות עם המידע שלהם (איסוף, שימוש והפצה), את מטרתו ואת השלכותיו.

לפי עמדת משרד נציב הפרטיות הקנדי, כחלק מהעדכון של יחידים הנדרש לשם הסכמתם, יש לעדכן אותם אם יש חשש לשימוש לרעה או לנזק שעלול להיגרם מאיסוף, מעיבוד או משיתוף של מידע – בתנאי שמדובר בסיכון של ממש לנזק של ממש (נזקי גוף, השפלה, פגיעה במוניטין, אובדן עבודה, גנבת זהות ועוד). יצוין כי אם מדובר בסבירות גבוהה לסיכון, הרי שאיסוף המידע ועיבודו יוגדרו כלא הולמים וכלא ראויים לבקשת הסכמה.³⁶

³¹ Office of Privacy Commissioner of Canada, "[Consent and Privacy](#)", 2016.

³² במגזר הציבורי החוק הרלוונטי הוא חוק הפרטיות (Privacy Act), והוא חל על סוכנויות ועל משרדי הממשל הפדרלי. ראו הסבר קצר [באתר](#) נציב הגנת הפרטיות הקנדי.

³³ יצוין כי בנובמבר 2020 הגיש שר החדשנות, המדע והתעשייה הקנדי הצעה לחקיקת שני חוקים חדשים: חוק להגנת פרטיות הצרכן וחוק בנושא בית משפט להגנה על מידע ועל נתונים אישיים. ההצעה נועדה בין השאר לעדכן את ה-Pipeda, אך לא נתקבלה כחוק בשל פיזור הפרלמנט הקנדי (ראו [כאן](#)). להרחבה בעניין הצעת החוק ראו מסמך ספריית הפרלמנט הקנדי, ובפרט ראו עמ' 7-12 על השינויים המוצעים למודל ההסכמה בין ה-Pipeda לחוק המוצע:

Sabrina Charland, Alexandra Savoie and Ryan Van Den Berg, "[Legislative Summary Bill C-11: An Act to Enact the Consumer Privacy Protection Act and The Personal Information and Data Protection Tribunal Act and to Make Consequential and Related Amendments to Other Acts](#)", Parliamentary Information and Research Service – Canada, December 2020.

³⁴ Office of Privacy Commissioner of Canada, "[Consent and Privacy](#)", 2016.

³⁵ הסקירה של נציב הפרטיות הקנדי מתייחסת לארגונים בלי לפרט אותם. לפי נוסח החוק, ב"ארגונים" הכוונה לאגודה, לשותפות, לאדם ולאגוד מקצועי. במקור: organization includes an association, a partnership, a person and a trade union. לעיון בנוסח החוק ראו [כאן](#).

³⁶ Office of Privacy Commissioner of Canada, "[Guidelines for obtaining Meaningful Consent](#)", May 2018, Revised: August 2021

אף שהעקרונות הבסיסיים של לגיטימציה לשימוש במידע אישי הם ידיעה והסכמה, יש בחוק חריגים לחובות אלה על סמך ההבנה כי לא בכל הנסיבות ניתן לבקש הסכמה. דוגמה לחריגים: מצב חירום המאיים על חיו, על בריאותו או על ביטחונו של אדם; חשש לפגיעה בחקירה אם יבקשו הסכמה לאיסוף מידע, ועוד.

יצוין כי בחוק מפורטים חריגים בנפרד באשר לאיסוף מידע ללא ידיעה והסכמה; שימוש במידע ללא ידיעה והסכמה; וחשיפה (Disclosure) של מידע ללא ידיעה והסכמה.

עוד יצוין כי לפי החוק הקנדי, הסכמה – גם מפורשת – אינה מכשירה כל סוג של איסוף מידע או כל מטרת איסוף. לפי החוק, פעולות איסוף, עיבוד או שיתוף מידע אישי הן חוקיות רק אם האדם הסביר יראה במטרתן הולמת בהינתן הנסיבות הספציפיות.

אין למנוע שירות בשל סירוב (אי-הסכמה) למסור מידע נוסף למידע הנדרש לשם אספקת השירות. כדי שמידע ייחשב כנדרש לאספקת השירות, הוא צריך לשמש למטרה מפורשת, ספציפית ולגיטימית. עם זאת, יש לידע את הפרט על השלכות של חזרה מהסכמה, בפרט במקרים שזו תגרור פגיעה או מניעה של אספקת השירות המבוקש.

לפי עמדת נציב הפרטיות הקנדי, החוק מכיר בכך שסוג ההסכמה יכול להיות שונה בין השאר בהינתן מידת רגישות המידע והציפיות הסבירות של הפרט באשר לשימוש במידע. אף שהסכמה מפורשת (Express) היא סוג ההסכמה הרצוי והראוי ביותר, והיא בגדר דרישה כאשר מבקשים גישה למידע רגיש, בתנאים מסוימים ומוגדרים גם הסכמה משתמעת (Implied) תיחשב להסכמה תקפה.

יצוין כי אין בחוק הקנדי הגדרה רשמית למידע רגיש. אומנם מידע בריאותי, מידע פיננסי, עמדות פוליטיות, מידע על גזע, נטייה מינית ועוד ייחשבו לרוב כפריטי מידע רגישים, אך גם מידע לא רגיש יכול להיחשב רגיש, אם הצלבתו עם פריטי מידע אחרים מביאה לחשיפת מידע רגיש על הפרט. מאידך, גם מידע רגיש יכול להיחשב כרגיש פחות בסיטואציה מסוימת – למשל אם המידע האמור כבר נהפך לנחלת הכלל.³⁷

לפי מסמך הנחיות של נציב הפרטיות של קנדה ושל נציג הפרטיות של מחוז (province) אלברטה בקנדה, אין די בהעתקה של חוזה כתוב אל פורמט דיגיטלי כדי להפוך אותו לכלי לקבלת הסכמה בסביבת אינטרנט, אלא יש למצוא דרכים לנצל את המדיום כדי להעביר מסרים ברורים – לדוגמה: להצמיד הסבר לבקשה של פריט מידע כך שהוא "יקפוץ" בעת בקשה של המידע; להשתמש בסרטוני וידאו להדגמה של עקרונות, או להציג "רענון" של עיקרי השימוש במידע

³⁷שם.

גם מידע לא רגיש
יכול להיחשב כרגיש
אם הצלבתו עם
פריטי מידע אחרים
מביאה לחשיפת
מידע רגיש על הפרט.
מאידך, גם מידע
רגיש יכול להיחשב
כרגיש פחות, למשל
אם המידע כבר נהפך
לנחלת הכלל

האישי של המשתמש מדי פעם. יש גם להתאים את מועד החשיפה למידע בנושא – בדגש על נקודות החלטה.³⁸

לפרטים יש זכות לחזור בהם מהסכמתם לאיסוף מידע אישי על אודותיהם בכפוף למגבלות חוקיות או חוזיות. על הארגון ליישם את החזרה מהסכמה, ועליו להביא לעצירת כל איסוף מידע אישי או שימוש נוסף בו. כמו כן, במקרים מסוימים משמעותה של חזרה מהסכמה³⁹ היא שיש למחוק מידע אישי שארגון מחזיק. לדוגמה, אם משתמש מחק את חשבונו ברשת חברתית, יש למחוק את המידע האישי שלו באתר – למעט אם הוא מוחזק כדי לממש חובות חוקיות אחרות של המחזיק.⁴⁰

6. הסכמה במסגרת חוק פרטיות הצרכן בקליפורניה – ארה"ב (CCPA)

חוק פרטיות הצרכן של קליפורניה, California Consumer Privacy Act (CCPA), שנחקק בשנת 2018 ונכנס לתוקף ב-2020, נועד לעגן את זכויותיהם של צרכנים תושבי קליפורניה אל מול גופים מסחריים (ולא אל מול רשויות מדינה). בנובמבר 2020 עברה במשאל עם בקרב אזרחי קליפורניה הצעה 24 לחוק "הזכויות לפרטיות" – California Privacy Rights Act; מתוקף חוק זה תוקן חוק פרטיות הצרכן – ה-CCPA, נוספו זכויות חדשות באשר להגנה על פרטיות, והוקמה בקליפורניה "הסוכנות להגנה על פרטיות" (California Privacy Protection Agency) שנועדה להיות גוף אכיפה של החוק.⁴¹ החקיקה החדשה אמורה ברובה להיכנס לתוקף בראשית 2023.

יצוין כי לא כל גוף מסחרי כפוף לחובות מתוקף החוק, אלא רק עסקים העומדים בתנאים המפורטים בחוק, בין השאר עסקים שהמחזור השנתי שלהם גדול מ-25 מיליון דולר, או שהם עוסקים בסחר או בשיתוף במידע אישי של 100,000 צרכנים או משקי בית לפחות, או שמחצית המחזור השנתי שלהם לפחות מבוססת על מכירה או על שיתוף של מידע אישי של אזרחי קליפורניה.⁴²

³⁸ שם.

³⁹ הדבר אינו מצוין במפורש בסקירה, אך משתמע מן הדברים כי יש זיקה בין בקשה למחיקת חשבון לחזרה מהסכמה.

⁴⁰ שם.

⁴¹ CCPA, [About CCPA](#), accessed: May 22 2022.

⁴² Attorney General of the State of California, "[California Consumer Privacy Act \(CCPA\)](#)", accessed May 22 2022.

בעוד שבאתר המובא מופיע הסף של 50,000 צרכנים, לפי התיקון לחוק, הרף הוגדל ל-100,000. עוד יצוין כי הגדרתו של עסק שונתה גם היא כחלק מהשינויים בחוק, ראו בסעיף ההגדרות בחוק בסעיף הגדרת עסק שמספרו 1798.140.

בחוק פרטיות הצרכן של קליפורניה, לאחר תיקונו, כאמור, בעקבות קבלת חוק הזכויות לפרטיות, מוגדרת הסכמה כך⁴³:

“Consent” means any freely given, specific, informed, and unambiguous indication of the consumer’s wishes by which the consumer, or the consumer’s legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including **by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent”.**

כפי שאפשר לראות בטקסט (ההדגשות אינן במקור), הסכמה צריכה להינתן מדעת ומרצון חופשי, למטרה מסוימת ובאמצעות פעולה מפורשת. כמו כן, נראה כי לפי הנוסח המדובר, ההסכמה לא יכולה להינתן באופן נרחב וכללי או להיות מושגת באמצעות כלים מניפולטיביים.

יצוין כי בעוד שלפני תיקונו, כאמור, בחוק פרטיות הצרכן אוזכר מעט המונח הסכמה, ואף נמנעו מלהגדירו⁴⁴; בעקבות התיקון הוטמע מושג ההסכמה במסגרת החוק בצורה ברורה יותר. להלן נתייחס לעיקרם של חלק מיישומי עקרון ההסכמה על סמך לשון החוק.

⁴³ California legislative Information, "[Title 1.81.5. California Consumer Privacy Act of 2018](#)", accessed: may 22 2022.

Keir Lamont and Jeewon K. Serrato, "[CPRA Law + Tech: Understanding Data, Decisionmaking, and Design](#)", Future of Privacy Forum, February 18th 2022, accessed: may 22 2022.

⁴⁴ ראו כאן.

- **הזכות לסרב למכירה או לשיתוף של מידע אישי לצדדים שלישיים:** לפי החוק, בגיר יכול להנחות עסק שלא למכור או לחלוק מידע אישי שלו עם צדדים שלישיים (היינו "אופט אאוט").⁴⁵ עם זאת, ביחס לקטינים מתחת לגיל 13 נדרשת הסכמה (היינו "אופט אין") כדי להתיר מכירה או שיתוף של מידע אישי עם צדדים שלישיים.⁴⁶ כלומר ברירת המחדל לפי החוק היא כי מכירה או שיתוף של מידע אישי של קטינים מתחת לגיל 13 איננה מותרת אלא אם נתקבלה הסכמה לכך.⁴⁷
- **הזכות להגביל שימוש וחשיפה (disclosure) של מידע אישי רגיש:**⁴⁸ לפי החוק, בגיר יכול להנחות עסק שלא להשתמש במידע אישי רגיש עליו, אלא אך ורק עבור אספקת השירות או המוצר ובאופן התואם לציפיות הסבירות של לקוח ממוצע של שירות מסוג זה. במקרה כזה על העסק להימנע מלהשתמש או לחשוף מידע כזה למעט עבור אספקת השירות כאמור, אלא אם כן הוא קיבל את הסכמת הלקוח לשימושים נוספים.⁴⁹
- **תמריצים להענקת גישה למידע:** אף שהחוק קובע איסור אפליה או נקמות (Retaliation) כלפי לקוחות המממשים את הזכויות שלהם במידע מתוקפן, עסקים יכולים להציע תמריצים או הטבות ללקוחות המסכימים לחלוק את המידע האישי שלהם ולאפשר שיתוף, שימוש ומכירה שלו. עסקים גם רשאים להציע תמחור שונה או איכות מוצרים שונה ללקוחות שונים כל עוד הדבר נעשה באופן סביר הקשור לערך שהמידע האישי מספק לעסק. "מסלול" הכולל תמריצים כאמור, יכול להינתן רק לאחר קבלת הסכמה במנגנון "אופט-אין". עסק רשאי להציע שוב ללקוח שסירב להצטרף למסלולי תמריצים כאמור רק בחלוף שנה מהסירוב.⁵⁰

⁴⁵ יצוין כי ההגדרה של מכירה לפי החוק היא נרחבת וכוללת בין השאר את הרכיבים האלה: השכרה, שחרור, גילוי, הפצה, העברה, תקשורת בכתב או בעל פה ועוד, של מידע אישי של צרכן לצד שלישי לתועלת כלכלית או אחרת. ראו California legislative Information, "Title 1.81.5. California Consumer Privacy Act of 2018", 1798.140.

⁴⁶ בחוק מוגדרים תנאים באשר לקטינים מתחת לגיל 13 ובגילי 13-16, ראו סעיף 1798.120.

⁴⁷ California legislative Information, "Title 1.81.5. California Consumer Privacy Act of 2018", 1798.120(d).

⁴⁸ לפי החוק, מידע אישי רגיש כולל בין השאר את הפרטים האלה: מידע החושף את פרטי מספר הביטוח הלאומי, מספר רישיון הנהיגה, מספר דרכון או מספר תעודה מזהה מדינתית, פרטי התחברות לשירות מקוון, מספר חשבון בנק, מספר כרטיס חיוב, מספר אשראי הכולל קוד גישה נוסף או סיסמה, נתוני מיקום מדויקים, מוצא אתני או גזעי, אמונות דתיות או פילוסופיות או חברות באיגוד, תכולת דואר או דוא"ל, הודעת טקסט – למעט אם העסק הוא הנמען של התכתובת, מידע גנטי של הצרכן, נתוני עיבוד מידע ביומטרי המאפשר זיהוי חד-ערכי, מידע אישי הנאסף או מנותח הנוגע לבריאותו של הצרכן, מידע אישי הנאסף או מנותח הנוגע לחיי המין של הצרכן או לנטייה המינית שלו. בתנאים מסוימים חלק מהמידע האמור, אם הוא זמין וגלוי, הוא לא ייחשב כמידע אישי או כמידע אישי רגיש. לפירוש ולהסתייגויות נוספות ראו את סעיף ההגדרות 1798.140.

⁴⁹ שם, 1798.121.

⁵⁰ שם, 1798.125(b)3.

• **"דף הסכמה"**: עסקים נדרשים לספק כלים זמינים באתרי האינטרנט שלהם כדי לאפשר ללקוחות לאסור על מכירה, שימוש או שיתוף המידע האישי שלהם ולהגביל את השימוש במידע אישי רגיש. ככל שהם מקיימים את הכללים הנוגעים לכך, עסקים רשאים גם להציע "דף הסכמה" והפניה (לינק) אליו, המאפשר למשתמש לבטל את אי-ההסכמה ולמעשה להתיר להם לאסוף ולמכור את המידע. עם זאת, "דף ההסכמה" חייב לאפשר הן את ההסכמה הן את הנסיגה ממנה – ביטולה – באותה קלות שימוש.⁵¹

• **חריג לחובת המחיקה**: אף שלפי החוק צרכן יכול לבקש מעסק או ממחזיקים נוספים במידע אישי למחוק אותו, אחד החריגים הקבועים בחוק הוא פטור מחובת מחיקה אם המידע משמש למחקר, ואם מחיקתו תמנע את האפשרות לערוך את המחקר או תפגע בתהליך, בהינתן כי המחקר עומד בכללי האתיקה והגנת הפרטיות וכי נתקבלה **ההסכמה מדעת** מצד הפרט.⁵²

יובהר כי האמור לעיל אינו ממצה את כלל האזכורים של נושא ההסכמה בחוק פרטיות הצרכן העדכני, ומתבסס על התיקונים שהוכנסו בגרסתו האחרונה – מרביתם ייכנסו לתוקף רק בינואר 2023. עוד יצוין כי מאתר הסוכנות להגנה על פרטיות משתמע כי לחקיקה עצמה מתלוות תקנות מפורטות.⁵³

⁵¹ שם, 1798.135.

⁵² שם, 1798.105 (d)6.

⁵³ CCPA, "[Regulations](#)", accessed: June 19, 2022.