



פברואר 2025
שבט, תשפ"ה

גילוי דעת בנושא הסכמה בדיני הגנת הפרטיות

הקדמה

1. עיקרון ההסכמה הוא עיקרון מרכזי בדיני הגנת הפרטיות הישראלים. מטרת גילוי הדעת היא להבהיר את עמדת הרשות להגנת הפרטיות (להלן: 'הרשות') בעניין יישום העיקרון בראי המציאות הדיגיטלית המתפתחת, וכן ביחס לתחולת חוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות' או 'החוק') בנושא.
2. גילוי הדעת משקף את הפרשנות המשפטית שתשמש את הרשות בעת ולצורך הפעלת מגוון הסמכויות המסורות לה בחוק, לרבות הפיקוח על מילוי הוראות החוק והתקנות שמכוחו, רישום מאגר במרשם מאגרי המידע לרבות ביטול או התלייה של רישום קיים, והטלת קנס מינהלי או עיצום כספי בגין הפרת הוראות החוק.

כללי

3. חוק הגנת הפרטיות קובע כי איסוף ושימוש במידע אישי (להלן גם: 'עיבוד') הכרוכים בפגיעה בפרטיות יכולים להיעשות מכוח הסכמה בדין או בהסכמת נושא המידע.¹
4. עיקרון ההסכמה הוא עיקרון מרכזי בדיני הגנת הפרטיות. על-פי עיקרון זה, עיבוד מידע מכוח הסכמתו של אדם יכול להיעשות רק בנסיבות בהן עומדת לו האפשרות להחליט איזה מידע הנוגע אליו ייחשף, למי, ולאיילו מטרות.²
5. עיבוד מידע על אודות אדם ללא קבלת הסכמתו מהווה פגיעה באוטונומיה שלו וביכולתו לשלוט במידע הנוגע אליו.³ הסכמה משקפת אפוא את יכולת השליטה של אדם במידע שעל אודותיו.⁴
6. דרישת ההסכמה נכללת מפורשות בחוק הגנת הפרטיות. סעיף 1 לחוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". משמעות הוראה זו היא כי על הפוגע בפרטיותו של אדם, באחת הדרכים המנויות בסעיף 2 לחוק, מבלי שניתנה לכך הסכמה בדין, מוטל הנטל לשכנע באופן פוזיטיבי כי הפגיעה נעשתה בהסכמה, נטל בו יתקשה לעמוד אם לא ישמור תיעוד של מתן ההסכמה.

¹ יצוין כי סעיף 18 לחוק הגנת הפרטיות קובע כי במצבים מסוימים עשויה לעמוד הגנה משפטית לגורם הפוגע שלא כדין בפרטיותו של אדם. יובהר כי ההגנות הקבועות בסעיף 18 לחוק פורשו בפסיקה בצמצום רב והן כפופות גם לדרישות סטטוטוריות כגון חובת תום הלב ודרישת סבירות (ראו סעיף 20 לחוק). ראו לדוגמה רע"פ 4743/20 **מרדכי לייבל נ' מדינת ישראל** (נבו 21.7.22). עוד יצוין כי בהתאם לפסיקת בית המשפט העליון, רשות מנהלית אינה רשאית להסתמך מראש על ההגנות שבסעיף 18 לחוק הגנת הפרטיות לצורך קביעת מדיניות כללית הכרוכה בפגיעה בפרטיות. לעניין זה ראו: רע"א 2558/16 **פלונית נ' קצין התגמולים – משרד הביטחון**, פסקה 59 לפסק הדין (נבו 5.11.2017).

² תפיסה זו ידועה בשם "פרטיות כשליטה". להרחבה ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה**, 108-89 (2010).

³ בג"ץ 2109/20 **שחר בן מאיר נ' ראש הממשלה** (פורסם בנבו, 26.4.2020), בפס' 38 לפסק דינה של הנשיאה א' חיות.

⁴ מיכאל בירנהק **פרטיות חוקתית** (2023), בעמ' 252.



7. היבט ההסכמה עשוי לבוא לידי ביטוי באופן עקיף גם בסעיף 8(ב) לחוק, הקובע כי לא ישתמש אדם במידע שבמאגר מידע אלא למטרה שלשמה הוקם המאגר.⁵ בהיעדר הסמכה בדין, שימוש במידע למטרה מסוימת יכול להיעשות רק על יסוד ההסכמה שניתנה למטרה ספציפית זו.
8. בתיקון מס' 13 לחוק הגנת הפרטיות נחקק בין היתר סעיף 8(ד1), המבהיר כי חל איסור על עיבוד מידע אישי במאגר אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע". למען הסר ספק יובהר כי הוראה זו תחול על מידע שנאסף שלא מתוקף ההסכמה תקפה לפי החוק, אלא אם קיימת הסמכה בדין לאיסופו.⁶
9. חוק הגנת הפרטיות מגדיר, בסעיף 3, כי על ההסכמה לעיבוד מידע אישי הכרוך בפגיעה בפרטיות להיות "מדעת", בין אם מתקבלת "במפורש" או נלמדת "מכללא". להלן נפרט על רכיבים מרכזיים אלו של דרישת ההסכמה בדיני הגנת הפרטיות, תוך התייחסות לרכיב הרצון החופשי בהסכמה, לסוגיית הפגיעה בפרטיות בהיעדר ההסכמה, ולמתן האפשרות לחזרה מהסכמה.

הסכמה מדעת

10. הסכמה מדעת (informed consent) נועדה להבטיח כי הסכמתו של אדם לפגיעה בפרטיותו ניתנה מתוך בחירה אמיתית ואוטונומית.⁷
11. מקורו של מושג זה הוא בהקשר הרפואי, ולפיו, על מטפל למסור למטופל את כל המידע הרפואי הנדרש לו, באורח סביר, לשם קבלת החלטה ביחס לטיפול רפואי אותו הוא מבקש או נדרש לעבור.⁸
12. בדיני הגנת הפרטיות, משמעות הדבר היא שבעת בקשה לקבלת ההסכמה לפגיעה בפרטיות, אדם צריך להיות מודע לזכותו לסרב לבקשה (לרבות מודעות להשלכות החלטתו),⁹ לאחר שהובא בפניו כל המידע הדרוש לו, באורח סביר ובצורה מובנת, כדי לקבל החלטה בנושא.¹⁰

⁵ סעיף זה מבטא את עיקרון צמידות המטרה.

⁶ חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, אושר על-ידי הכנסת באוגוסט 2024, וייכנס לתוקפו ביום 14.8.2025.

⁷ רע"פ 10141/09 אברהם בן חיים נ' מדינת ישראל (פורסם בנבו, 6.3.2012) (להלן: 'עניין בן חיים'), בפס' 27 לפסק דינה של הנשיאה (בדימ"ד) ביניש.

⁸ עיקרון זה קבוע בסעיף 13(ב) לחוק זכויות החולה, התשנ"ו-1986, הקובע כי "לשם קבלת ההסכמה מדעת, ימסור המטפל למטופל מידע רפואי הדרוש לו, באורח סביר, כדי לאפשר לו להחליט אם להסכים לטיפול המוצע". להרחבה ראו ע"א 2781/93 דעקה נ' בית החולים "כרמל" חיפה, פ"ד נג' (4) 526 (1999).

⁹ עניין בן חיים, לעיל הי"ש 7, בפס' 27.

¹⁰ השינוי בהגדרת "ההסכמה" בחוק הגנת הפרטיות, לפיו ההסכמה לפגיעה בפרטיות צריכה להיות "מדעת", התקבל במסגרת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ז-2007. בדברי ההסבר לתיקון צוין כי "התיקון המוצע נועד להבטיח כי ההסכמה הניתנת לפגיעה בפרטיות תהיה ההסכמה מדעת. היינו, שבידי האדם המסכים לפגיעה בפרטיות יהיה מידע, הדרוש לו, באורח סביר, כדי להחליט האם להסכים או לא, והמידע ימסר לו בצורה מובנת" (ה"ח הממשלה 2,30, 232).



13. עיקרון זה, כמו גם חובת היידוע שבסעיף 11 לחוק הגנת הפרטיות, מחייבים את מבקש ההסכמה לספק ולהציג לאדם נתונים שונים על אודות איסוף המידע והשימוש בו, ובכלל זה פירוט בדבר מטרת איסוף המידע ובדבר זהות הגורמים אליו הוא עשוי להיות מועבר.¹¹
14. תוקף ההסכמה והיקפה תלויים, במידה רבה, במידע שהועבר לאדם נושא המידע, ושעל-פיו הוא נתן את הסכמתו.

כך למשל, רשת מרכולים המשתמשת בתמונת לקוח במסגרת מסע פרסום נרחב על-גבי חלונות ראווה, אוטובוסים ובעיתונות, תיחשב כפוגעת בפרטיות הלקוח אם מתוך המידע שנמסר לו במועד קבלת הסכמתו לצילום לא ניתן היה ללמוד על הסכמה שהתמונה תפורסם באמצעי מדיה רחבים יותר מפרסום בחלונות הראווה בסניפים.¹²

15. סוג המידע שעל אוסף ומעבד המידע לספק לאדם לשם קבלת הסכמתו, והיקפו, תלויים בהקשר הפנייה.

לדוגמה, בעניין קלנסווה קבע בית הדין הארצי לעבודה כי מעסיקה לא קיבלה הסכמה מדעת לאיסוף מידע ביומטרי של עובדות לצרכי רישום נוכחות במקום העבודה, וזאת, בין היתר, משום שלא הציגה בפני העובדות פרטים רלוונטיים באשר לטיב ולאופן השימוש בשעון ביומטרי, לא פרסמה מדיניות ברורה, גלויה ומידתית בנושא, ולא שיתפה את העובדות (או נציגיהן) בקביעת מדיניות זו.¹³

בעניין סמל, אשר עסק בפרסום תמונות עירום ללא הסכמה, קבע בית משפט השלום כי לשם קבלת הסכמה מדעת בהקשר זה היה על המפרסם לספק למצולם מידע הדרוש לו לשם קבלת החלטתו, לרבות בדבר פרסומו של המידע המצולם ודרך פרסומו.¹⁴

דוגמה נוספת ניתן למצוא בעניין ברובצ'יק, בו קבע בית הדין האזורי לעבודה בתל-אביב כי מעסיקה פגעה באופן בלתי מידתי בפרטיות עובדת כאשר גרמה לה לעבור בדיקת פוליוגרף בלא לקבל הסכמה מדעת. בקביעתו זו הסתמך בית הדין, בין היתר, על כך שלעובדת לא ניתן כל

¹¹ סעיף 11 לחוק הגנת הפרטיות קובע כי "פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצוינו בה – (1) אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; (2) המטרה אשר לשמה מבוקש המידע; (3) למי יימסר המידע ומטרות המסירה". לפי בירנהק, את הביטוי "הסכמה מדעת" יש לקרוא ולפרש על רקע הבנה של הפרטיות כשליטה. לגישתו, מימוש שליטתו של אדם ביחידה האוטונומית שלו אפשרי רק כאשר הוא יודע ומבין את משמעות הפעולה המבוקשת. בירנהק, לעיל ה"ש 2, בעמ' 100.

¹² ת"א (ירושלים) 20901-08 רומן מינקין נ' קו אופ ישראל רשת סופרמרקטים בע"מ (פורסם בנבו, 20.2.11).

¹³ עס"ק (ארצי) 7541-04-14 הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי נ' עיריית קלנסווה (פורסם בנבו, 15.3.17), (להלן: "עניין קלנסווה"), בפס' 144 לפסק דינו של השופט איטח. במסגרת עמדת היועץ המשפטי לממשלה, שהוגשה בהליך זה, צוין בנוסף כי: "על היידוע להיות מפורש וספציפי, שכן ללא מידע ספציפי וברור בנוגע לפגיעה שעלולה להיגרם לפרטיותו ואף ביחס לחוסר הוודאות בה היא מתאפיינת, לא ניתן לייחס להסכמת עובד את יסוד ה"דעת" (פס' 65 לעמדת היועץ המשפטי לממשלה). לעניין זה ראו גם ע"ע (ארצי) 90/08 טלי איסקוב ענבר - מדינת ישראל - הממונה על חוק עבודת נשים ואח' (פורסם בנבו, 8.2.11), (להלן: "עניין איסקוב"), בפס' 30 של השופטת ארד.

¹⁴ בפסק הדין קבע כי "משמעותה של הסכמה מדעת בהקשר זה הינה כי בידי האדם היה במועד מתן ההסכמה את המידע הדרוש לו באורח סביר כדי להחליט אם להסכים למסירת המידע, פרסומו, דרך פרסומו ולשימושים שיעשו בו, ובכלל זה להעברתו לצדדים שלישיים". ראו ת"א (הרצליה) 21945-07-14 פלוני נ' אריאל סמל (פורסם בנבו, 31.1.16), פס' 42 לפסק דינו של השופט סלע.



הסבר לגבי מהות הבדיקה, לגבי הספקות הקיימים ביחס לרמת תקפותה ומהימנותה, ביחס לאופן שבו היא מתבצעת, ביחס לשימוש שיש בכוונת הנתבעת לעשות בתוצאותיה, או ביחס לזהות הגורם אשר יבצע את הבדיקה והכשרתו.¹⁵

16. מתוך כך שהסכמה חייבת להיות "מדעת" הרי שהסכמה שניתנה מבלי שלאדם הייתה האפשרות הסבירה להבין את משמעות הסכמתו והשלכותיה, לא תיחשב הסכמה תקפה. לכן, יש להקפיד כי תוכן ההסכמה והמידע הנלווה לה יוצגו באופן ברור, נגיש ומובן.

במקרים ששירות מסוים מופנה בעיקרו לאוכלוסייה בעלת מאפיינים ייחודיים, כגון אנשים עם מוגבלות, יש לתת על כך את הדעת במסגרת אופן הצגת המידע הנדרש לצורך קבלת ההסכמה, ואופן קבלתה.¹⁶

כך למשל, על אפליקציות חדשות שמכוונות לאוכלוסייה של ליקוי ראייה להציג את המידע הרלוונטי לקבלת ההסכמה לשימוש באפליקציה (לרבות איזה מידע נאסף בעת השימוש באפליקציה, למי הוא עשוי להיות מועבר ולאילו מטרה), ככל הניתן באופן שיהיה נגיש עבורם, למשל תוך שימוש בכיתוב בגודל פונט מתאים, באמצעים קוליים או באמצעים ויזואליים (תמונות, אימוג'ים) העשויים לסייע להם להבין את משמעות הסכמתם.

17. כאמור, ביטוי ספציפי של רכיב ההסכמה מדעת ניתן למצוא בסעיף 11 לחוק הגנת הפרטיות, הקובע כי בעת פנייה לאדם לשם איסוף מידע שנועד להיכלל במאגר מידע, יש לפרט בפני נושא המידע אם חלה עליו חובה חוקית למסור את המידע או שמסירת המידע תלויה בהסכמתו, את המטרה שלשמה מבוקש המידע, וכן למי הוא יימסר ולשם איזו מטרה.¹⁷ במסגרת תיקון מס' 13 לחוק הגנת הפרטיות נקבע כי חובת היידוע לפי סעיף 11 כוללת גם את החובה להודיע לאדם מה היא "תוצאת אי-ההסכמה".

יובהר כי לגישת הרשות אין בעמידה בתנאי סעיף 11 כדי להבטיח עמידה בדרישה לקבל הסכמה מדעת, שכן עמידה בתנאי הסעיף היא דרישת המינימום המתחייבת מהוראות החוק, וכפי שפורט לעיל, במקרים מסוימים מבקש ההסכמה יהיה מחויב בפירוט נרחב יותר מהקבוע בסעיף זה על מנת לעמוד בדרישת החוק להסכמה מדעת לפגיעה בפרטיות.

ככלל, עמדת הרשות היא כי בנסיבות בהן קיימים פערי כוח בין צדדים, או כאשר מדובר בפעולה בעלת פוטנציאל לפגיעה קשה בפרטיות או בנסיבות מורכבות אחרות (כגון שימוש בטכנולוגיה חדשה שהשלכות השימוש בה אינן ברורות דיין) – יש לראות בחובה זו כחובה מוגברת, ועל מבקש ההסכמה יהא להקפיד להציג באופן בולט ופשוט את כלל הנתונים

¹⁵ סעי' (תל אביב-יפו) 51013-11-14 ויקטוריה ברובצ'וק - טופ טן אביזרי אופנה בע"מ (פורסם בנבו, 15.12.16), בפס' 15 לפסק דינה של השופטת רות.

¹⁶ עיקרון זה קבוע, בין היתר, בסעיף 12 לתקנות הגנה המידע האירופאיות (להלן: 'GDPR'), אשר כולל התייחסות ספציפית לצורך להגשת מידע עבור קטינים. לעניין כללי הנגשה של מסמכים עבור אנשים עם מוגבלות ראו לדוגמה תקנות שוויון זכויות לאנשים עם מוגבלות (התאמות נגישות לשירות), התשע"ג-2013.

¹⁷ להרחבה ראו עמדת הרשות להגנת הפרטיות בעניין "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (יולי, 2022).



הרלוונטיים להחלטה, וככל הניתן בנפרד משאר רכיבי ההתקשרות. העדר פירוט מספק במסגרת הליך קבלת ההסכמה עלול להביא לפגיעה בתוקפה של ההסכמה.

18. עוד יובהר כי הדרישה שהסכמה תהיה מדעת, כפי שפורט לעיל בחלק זה, חלה הן ביחס להסכמה הניתנת באופן מפורש והן ביחס להסכמה מכללא, קרי הסכמה משתמעת הנלמדת מהתנהגותו של אדם.

הסכמה מרצון חופשי

19. על-פי מהותה, הסכמה לפגיעה בפרטיות חייבת להינתן מתוך רצון חופשי.¹⁸ כך לדוגמה, בעניין **איסקוב**, אשר עסק בסוגיית חדירת מעסיק לחשבונות דואר אלקטרוני של עובדת, קבע בית הדין הארצי לעבודה כי: **"קיומו של רצון חופשי כתנאי להכרה בהסכמה הוא פועל יוצא מההגנה על הזכות החוקתית לפרטיות האוסרת חדירה למרחב הווירטואלי הפרטי שלא בהסכמתו של אדם"**.¹⁹ על חשיבות הרצון החופשי בהסכמה לפגיעה בפרטיות ניתן ללמוד גם מעמדת היועץ המשפטי לממשלה שהוגשה לבית המשפט המחוזי בעניין **גרינברג**, שם נאמר כי **"יש להבטיח כי ללקוח קיימת אפשרות בחירה אמיתית (ההדגשה במקור), על מנת שניתן יהיה לומר כי הסכמתו ניתנה מרצון חופשי"**.²⁰

20. בהקשר הרפואי נפסק כי רצון חופשי מהווה אחד מיסודות ההסכמה מדעת, וכי יסוד זה נשען על זכותו של מטופל לאוטונומיה ולקבלת החלטות עצמאיות באשר לטיפול לו הוא זקוק.²¹

21. רצון חופשי מהווה אחד מרכיבי ההסכמה גם בדיני הגנת המידע האירופיים. כך, סעיף 4(11) לרגולציית הגנת המידע של האיחוד האירופי (GDPR) מגדיר הסכמה ככזו אשר, בין היתר, ניתנת באופן חופשי ("freely given").

22. דוגמה לפגיעה ברכיב הרצון החופשי בדיני הגנת הפרטיות ניתן לראות בשימוש בכלים עיצוביים ו"טקטיקות אפלות" (dark patterns), שנועדו להקשות על נושא המידע להבין את משמעות הסכמתו ולהשפיע באופן פסול על החלטתו. שימוש שכזה עלול להצביע על כך שההסכמה שהתקבלה בנסיבות שכאלו אינה הסכמה מדעת, ואינה כזו המבטאת את רצונו החופשי של נושא המידע.²²

¹⁸ בירנהק, ה"ש 4, בעמ' 381.

¹⁹ עניין איסקוב, לעיל ה"ש 13, בפס' 30 של השופטת ארד.

²⁰ עמדת היועץ המשפטי לממשלה בת"צ (מרכז) 22141-03-15 פנחס יוסף גרינברג נ' חברת סלקום ישראל בע"מ (פורסם בנבו, 5.3.20), (להלן: 'עניין גרינברג'), בפס' 55. העמדה זמינה באתר נבו.

²¹ ע"א 1303/09 מרגלית קדוש נ' בית החולים ביקור חולים, סה(3) 164 (פורסם בנבו, 5.3.12), בפס' 3 לפסק דינו של המשנה לנשיאה א' ריבלין.

²² בירנהק, לעיל ה"ש 4, בעמ' 252. להרחבה ודוגמאות בנוגע לאופן השימוש בטקטיקות אפלות להשפעה על משתמשים ראו איגוד האינטרנט הישראלי **"התמודדות עם מניפולציות של רשתות חברתיות כלפי משתמשים (dark patterns)"** (28.4.22).



כך למשל, אפליקציה של משחק רשת המיועדת לילדים, ה"מקפיצה" בזמן המשחק ובאופן קבוע בקשה לאיסוף נתוני מיקום, ש"מקפיאה" את המשחק ומפריעה למהלכו התקין, שאינה מאפשרת גישה למידע על מטרת השימוש בנתוני המיקום אלא באמצעות "יציאה" מהמשחק, ואשר אינה מעניקה אפשרות פשוטה לביטול הקפיצה החוזרת של ההודעה – עשויה להיחשב כאפליקציה העושה שימוש בטקטיקה אפלה לקבלת הסכמה.

23. סוגיית הרצון החופשי בדיני הגנת הפרטיות מתעוררת בעיקר במצבים בהם קיימים פערי כוח בין מבקש ההסכמה לבין נושא המידע. במצבים שכאלו הסכמה לפגיעה בפרטיות עלולה להיחשב כ"חשודה"²³, קרי כזו שקיים ספק האם ועד כמה ניתן לראותה כהסכמה שניתנה מתוך רצון חופשי, כן ואמיתי.

24. עמדה המבטאת את הקושי בהסתמכות על הסכמה הניתנת במצבים של פערי כוחות ניתן לראות בפסיקת בית המשפט העליון בעניין דיין:

"כאשר אדם מתבקש למסור מידע אודות חקירה פלילית במסגרת מכרז (או במצבים קרובים, כדוגמת ראיון עבודה) והוא מוסר מידע זה מרצונו, ניתן לכאורה לטעון כי הזכות לפרטיות אינה נפגעת, מאחר שאדם זכאי למסור מידע פרטי, כל עוד הדבר נעשה בהסכמה. אולם, לאמיתו של דבר, הסוגיה מורכבת יותר. **כאשר אדם נדרש למסור מידע לצורך השתתפות במכרז (או במצבים דומים) הוא מצוי במצב של תלות המצמצם את מרחב הבחירה העומד לרשותו.** אין להניח, שבעל מכרז (או מעביד) יוכל לדרוש גילוי של כל פרט הנוגע לחייו האישיים של המועמד, ולהצדיק את הדרישה בכך שהדבר נעשה 'מרצונו' (ההדגשות אינן במקור).²⁴

25. דוגמאות מרכזיות למצבים של הסכמה "חשודה", הן הסכמה הניתנת ביחסי עבודה (בין מעסיקים לעובדים ולמועמדים לעבודה),²⁵ הסכמה הניתנת לקבלת שירות חיוני (כגון שירותי תחבורה ציבורית, שירותי בריאות או שירותי טכנולוגי חיוני), וכן הסכמה הניתנת בהיעדר כל אלטרנטיבה סבירה. להלן מוצגות דוגמאות ספציפיות להסכמות חשודות:

דוגמה #1: רשת לממכר מוצרי פארם, המפעילה חנות באזור גיאוגרפי מרוחק שבו אין לתושבי האזור חלופה סבירה אלא לערוך את קניותיהם בחנות זו, המתנה את אפשרות לקוחותיה לרכוש מוצרי פארם בהצטרפות למועדון לקוחות, הכרוכה באיסוף מידע אישי רב על אודותיהם.

²³ בירנהק, לעיל ה"ש 4, בעמ' 381.

²⁴ ע"א 8189/11 רפאל דיין נ' מפעל הפיס (פורסם בנבו, 21.2.13), בפס' 34 לפסק דינה של השופטת ברק-ארז.

²⁵ להרחבה על הסכמה חשודה ביחסי עבודה ראו עניין איסקוב, לעיל ה"ש 13, בפס' 30 לפסק דינה של השופטת ארד. כמו כן ראו עמדת הרשות להגנת הפרטיות בעניין "היבטי פרטיות בוויטור על סודיות רפואית וחשיפת מידע רפואי בקבלה לעבודה" (מרץ, 2023).



דוגמה #2: מעסיק המבקש לפקח על פעילות עובדיו בזמן עבודתם מהבית, ולשם כך מבקש את הסכמתם לשימוש במערכת המצלמת אותם בביתם באופן רציף, בכל שעות העבודה.²⁶

דוגמה #3: חברת טכנולוגיה המבקשת "לאמן" את מערכות זיהוי הפנים שלה ופונה לשם כך לאוכלוסיות מעוטות יכולת בהצעה למתן תשלום סמלי בעבור שימוש בתמונותיהם.

דוגמה #4: מלון המבקש את הסכמת האורחים לשימוש במערכת לזיהוי פנים, אך אינו מציין זאת מראש במסגרת הליך הזמנת החדרים המקוון.

דוגמה #5: רשות מקומית או חברה המעניקה שירות חיוני מחליטה כי פניות למוקד השירות שלה יתקבלו רק באמצעות פנייה בתוכנת וואטסאפ, באופן שיחייב למעשה חלקים בציבור להשתמש בתוכנה זו ומכאן גם להעניק "הסכמה" לאיסוף ולשימוש במידע על אודותיהם.²⁷

26. לגישת הרשות, **במצבים מסוימים, בהם קיים חשש אינהרנטי כי ההסכמה שניתנה היא "חשודה", הנטל להראות כי הסכמה לפגיעה בפרטיות ניתנה מתוך רצון חופשי של אדם עשוי להיות מוטל על כתפיו של מבקש ההסכמה.**

במקרים שכאלו יכול מבקש ההסכמה לנקוט אמצעים שונים - כגון העמדת חלופה סבירה או אי-התניית קבלת השירות במתן הסכמה לאיסוף מידע שאינו נדרש - על מנת להראות כי ההסכמה מבטאת את רצונו החופשי ואת בחירתו האמיתית של נושא המידע.

כל האמור נכון במיוחד במקרים של מתן שירות חיוני או ביחס למקומות בהם ניתנים שירותים שכאלו.

כך למשל, חברה המפעילה שירותי תחבורה ציבורית אשר מבקשת לעבור לשימוש באמצעי תשלום מתקדמים, האוספים מידע רציף על נתוני המיקום של ציבור הנוסעים, תוכל להמשיך ולהעמיד לציבור את האפשרות לשלם באמצעים אחרים, שאינם אוספים נתונים אלו, או באמצעים שעושים זאת תוך שמירה על האנונימיות של המשתמש.²⁸

27. ויודגש שבמצב בו אדם כלל אינו יכול לסרב לפעולה הפוגעת בפרטיותו, יהיה קשה לראות בהסכמתו ככזו שניתנה מתוך רצון חופשי, והדבר עשוי להשליך על תוקפה של הסכמה זו.²⁹

תפיסה זו באה לידי ביטוי בפסיקת בית המשפט העליון בעניין **גוטסמן**, שם ציין בית המשפט כי "על-אף שהסכמה לצורך פגיעה בפרטיות ניתן להסיק משורה של מקרים ודרכי התנהגות,

²⁶ להרחבה על סוגיית הגנה על פרטיות במתכונת של עבודה מרחוק ראו עמדת הרשות להגנת הפרטיות בעניין "**היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק**" (מאי, 2023).

²⁷ צוין כי על-פי **תנאי השימוש** של אפליקציית וואטסאפ, תוכן ההתכתבות עם חשבון וואטסאפ 'עסקי', גם כאשר המשתמש הנוסף הוא חשבון פרטי והתכתובת כוללת מידע אישי, עשוי להיות מועבר לחברת פייסבוק (מטא) לצורך שימוש בו למטרות שונות, כולל הצגת פרסומות ומטרות מסחריות אחרות.

²⁸ להרחבה ראו מסמך המדיניות של הרשות להגנת הפרטיות בנושא "**היבטי פרטיות ביישומים (אפליקציות) לתשלום ותיקוף שימוש בשירותי תחבורה ציבורית**" (יולי, 2020).

²⁹ כך לדוגמה, קופת חולים המציבה מצלמות בתוך סניפיה מחייבת למעשה מטופלים להסכים להיות מצולמים גם אם הם לא רוצים בכך, שכן אין להם אפשרות אמיתית לבחור שלא להיכנס לסניפים. לפיכך ניתן לטעון כי ההסכמה הניתנת במצב שכזה היא לא חופשית אלא כזו הניתנת מחוסר ברירה.



מוטב להפעיל משנה זהירות בקביעה כי נתקבלה הסכמה לפרסום.³⁰ בית המשפט המשיך וציטט בהקשר זה את דבריה של פרופ' רות גביון, לפיהם "יש להיזהר ולא להפעיל את הכוח המצדיק של ההסכמה על מקרים בהם ברור כי אין הסכמה ממש והשימוש בהסכמה הוא לכן קונסטרוקטיבי ופיקטיבי".³¹

28. תפיסה זו באה לידי ביטוי בעניין **בנק לאומי**, שם קבע בית המשפט המחוזי בירושלים, כי התנייה של בנק את פתיחת החשבון בו בויתור מראש על חובת הסודיות כלפי החברות הקשורות לתאגיד הבנקאי, אינה הוגנת ומקפחת את הלקוחות.³²

29. יובהר שבנסיבות בהן הסכמה ניתנת במסגרת יחסי עבודה,³³ או כאשר על מבקש ההסכמה חלים כללי המשפט הציבורי (כגון משרד ממשלתי, רשות מקומית) – הפגיעה בפרטיות כפופה גם לעמידה בדרישת המידתיות.

הסכמה במפורש או מכללא

30. על-פי סעיף 3 לחוק הגנת הפרטיות, הסכמה לפגיעה בפרטיות יכולה להינתן במפורש (כלומר בצורה מפורשת) או להילמד מכללא, כלומר שלא במפורש ובאופן משתמע.

31. הסכמה מפורשת יכולה להינתן בכתב או בעל-פה, ומשמעותה היא שאדם הסכים באופן מפורש, ולפיקך מובהק וחד-משמעי, לפגיעה בפרטיותו בהקשר שבו התבקשה ההסכמה. על-פי רוב, חתימה על חוזה, לחיצה אקטיבית על רובריקת אישור מסמך תנאי שימוש, ואמרה בעל פה מהווים הסכמה מפורשת. גם מחווה גופנית כגון הנהון בתגובה לשאלה מפורשת עשויה להיחשב כהסכמה מפורשת, אם כי בנסיבות מסוימות, וכפי שיפורט בהמשך, עלול להתקיים קושי להסתמך על סוג הסכמה שכזו.

לדוגמה, לחיצה על כפתור "אני מסכים" בתחתית מסמך תנאי שימוש בעת הורדת אפליקציה, מהווה הסכמה מפורשת לתנאי השימוש, לרבות בנוגע לתנאים המתייחסים לאיסוף ואופן השימוש במידע אישי.

32. הסכמה מכללא היא הסכמה משתמעת, קרי כזו הניתנת ללמידה מתוך הנסיבות, הסיטואציה, ודרכי ההתנהגות של האדם נושא המידע, וזאת על יסוד הפרשנות הסבירה והמקובלת של אותה התנהגות.

³⁰ ע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' אריה ורדי (פורסם בנבו, 23.1.13) (להלן: 'עניין גוטסמן'), בפס' 30 לפסק דינו של השופט פוגלמן.

³¹ רות גביון "איסור פרסום הפוגע בפרטיות", בתוך זכויות אזרח בישראל – קובץ מאמרים לכבוד חיים ה. כהן, 177, 199 (1982).

³² ע"ש (י-ם) 195/97 היועץ המשפטי לממשלה נ' בנק לאומי לישראל פ"מ תשס"ג(1) 481 (2004), בפס' 282. בית המשפט דחה בעניין זה את טענת הבנק כי הלקוחות הנם אנשים "בוגרים ועצמאים ומבינים היטב על מה הם חותמים", כך שהתנייה אינה מקפחת אותם. בית המשפט ציין כי אם הלקוח יזקק לאשראי או לכל שירות אחר מחברות הקשורות לתאגיד הבנקאי, כי אז יוכלו נותני אותם שירותים להתנות את מתן השירותים בויתור על הסודיות הבנקאית, ומכאן שאין צורך בויתור גורף מראש על הסודיות הבנקאית, הנובעת בין היתר מחוק הגנת הפרטיות, כתנאי לפתיחת חשבון.³³ ראו עניין איסקוב, לעיל ה"ש 13.



33. בתי המשפט קבעו לא פעם כי התנהגותו של אדם יכולה להיחשב כהסכמה מכללא לפגיעה בפרטיותו. כך לדוגמה, פעילותו הפומבית של אדם במפלגה פוליטית נחשבת על-פניו כמבטאת הסכמה מכללא לחשיפת דעתו הפוליטית. גם אדם שמתתף בצילומים לצרכי פרסום ושיווק פעילות בה הוא לוקח חלק, ובמסגרת זו גם משתף פעולה עם צוות הצילום, יתקשה לטעון בשלב מאוחר יותר כי לא נתן הסכמתו לצילומים.³⁴ באופן דומה, אדם הלוקח חלק בתהלוחה המתקיימת באופן פומבי במרחב הציבורי נחשב ככזה שהעניק הסכמה מכללא לפרסום תמונתו לעניין הדיווח התקשורתי בדבר קיום התהלוחה.³⁵

בעניין **ונטורה** ציין בית המשפט העליון כי מספר חשבון הבנק של אדם נמנה עם ענייניו הפרטיים ופרסומו ללא הסכמה יהיה פגיעה בפרטיות. עם זאת, כאשר אדם מושך שיק לטובת פלוני, ועליו מודפסים שמו, כתובתו, וחשבון הבנק, הרי שיש לראות בכך הסכמה בהתנהגות להעברת אותו מידע לידיעתו של כל אדם שאותו שיק יוסב לו בדרך הרגילה, ואין בפעולות הללו, ככלל, משום פגיעה אסורה בפרטיותו.³⁶

34. עם זאת, **פסיקת בתי המשפט צמצמה במקרים שונים את האפשרות להסתמך על התנהגותו של אדם כהסכמה משתמעת לפגיעה בפרטיותו.**

כך, במספר פסקי דין נקבע כי אין בעצם יחסי נישואין כדי להוות הסכמה משתמעת לפגיעה בפרטיות בין בני זוג, וכי שאלת ההסכמה המשתמעת לפגיעה בפרטיות בהקשר זה צריכה להיבחן ביחס לנסיבותיו של כל מקרה ומקרה.³⁷ בעניין **גוטסמן** קבע בית המשפט העליון, בין היתר, כי אין בעובדה שאדם הסכים לגלות פרטים מסוימים לגורמים מסוימים, כדי להוות הסכמה משתמעת לגילוי אותם פרטים לגורמים אחרים.³⁸ כמו כן, בעניין **זינגר** קבע בית המשפט העליון כי העובדה שאדם השאיר את תיבת הדואר האלקטרוני שלו פתוחה על גבי מחשבו, אינה מהווה הסכמה שאחר יעיין בהודעותיו.³⁹ בעניין **פלונית** נקבע כי הימצאותה של אישה בחוף ים כשחלק גופה העליון חשוף, אינו מהווה הסכמה מכללא לפרסום תמונתה.⁴⁰

³⁴ ת"א (חיפה) 24285-09-14 **יוחאי פורטל נ' ירון זוננשין** (פורסם בנבו, 1.8.2016). לפסיקה דומה בעניין צילום מתעמלת בחדר-כושר ופרסום תמונתה בעיתון לצרכי שיווק ראו ת"א (פתח-תקווה) 1591/07 **יעקובסון נ' אביגד** (פורסם בנבו, 16.9.08). לביקורת על החלטה זו ראו בירנהק, לעיל ה"ש 2, בעמ' 102.

³⁵ ת"א (ירושלים) 6023/07 **שגב ישראל אפריאט נ' ידיעות אחרונות בע"מ** (פורסם בנבו, 5.1.08), (להלן: 'עניין אפריאט').

³⁶ ע"א 439/88 **רשם מאגרי מידע נ' משה ונטורה** (פורסם בנבו, 27.7.94), בעמ' 822.

³⁷ בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי בנתניה**, (פורסם בנבו, 14.5.06). ראו גם: תמ"ש (ראשון לציון) 17772-01-10 **פלוני נ' אלמוני** (פורסם בנבו, 11.11.13); תמ"ש (פתח תקווה) 19229-07-11 **פלונית נ' פלוני** (פורסם בנבו, 14.12.15); תלה"מ (ירושלים) 1118-09-17 **ד.מ. נ' ת.מ.** (פורסם בנבו, 21.5.19); תלה"מ (תל אביב-יפו) 47127-07-21 **פלונית נ' פלוני** (פורסם בנבו, 27.12.23).

³⁸ עניין גוטסמן, לעיל ה"ש 30.

³⁹ רע"א 2552/16 **זינגר נ' חברת יהב חמיאס טכנולוגיות (1990) בע"מ** (פורסם בנבו, 10.5.16).

⁴⁰ ת"א (נתניה) 5680/02 **פלונית נ' שניידר אליעד** (פורסם בנבו, 6.2.06). לפסיקה דומה בה נדחתה טענה להסכמה לפרסום על יסוד העדר הסתייגות ראו: ת"א (תל אביב-יפו) 50267/05 **פלונית נ' חדשות ערוץ 10** (פורסם בנבו, 29.10.08). לדיון בדבר פגיעה בפרטיות במצב של התנגדות לצילום ולפרסום הצילום ברבים ראו רע"א 6902/06 **מנשה דרור צדיק נ' הוצאת עיתון הארץ בע"מ** (פורסם בנבו, 13.8.08).



כפי שנקבע בהתאם לנסיבות המקרה בעניין **כהן**, שפת גוף כגון הנהון ראש או הבעת פנים אינה מהווה בהכרח מסד ראייתי עובדתי מספק לרמה הנדרשת להוכחה ברורה ומודעת של הסכמה לצילום או לשימוש בתמונות לצרכים מסחריים.⁴¹ בהקשר זה ממליצה הרשות לנקוט זהירות בהסתמכות על הסכמה הניתנת בדרך של מחווה פיזית או תנועת גוף ולקחת בחשבון את הצורך לתעד אותה לשם הוכחת מתן ההסכמה.

35. ככלל, שתיקתו של אדם, או העדר מחאה מצדו לאיסוף או שימוש במידע הנוגע אליו, כשלעצמם, לא יכולים ללמד על הסכמה תקפה לפי דיני הגנת הפרטיות. כלומר, לגישת הרשות, שתיקה או העדר מחאה יכולים ללמד על הסכמה לפגיעה בפרטיות רק כאשר ניתן להוכיח כי לנושא המידע עמדה המודעות הנדרשת למתן ההסכמה, ורק כאשר קיימות נסיבות אחרות מהן ניתן ללמוד כי נושא המידע אכן התכוון להעניק את הסכמתו.

36. **גם במקרים בהם הסתמכות על הסכמה מכללא היא אפשרית, רצוי שלא להסתפק בהסכמה שכזו, אלא לפנות לאדם לקבלת הסכמתו המפורשת. זאת בעיקר במקרים של איסוף ושימוש מידע רגיש או נקיטת פעולה העלולה להביא לפגיעה קשה בפרטיות.**

בהקשר זה יפים דברי בית המשפט המחוזי בעניין **שטנגר**, בו נדחתה עתירה לגילוי מידע על שכם של פרקליטים המועסקים בוועדת האתיקה המחוזית, תוך שנקבע כי "יש לזכור, כי הזכות לפרטיות הינה זכות חוקתית, כך שנראה כי מן הראוי הוא לצמצם את השימוש בדוקטרינת ההסכמה מכללא אשר באה להגבילה".⁴²

37. כמו כן יש לזכור, כי הסכמה מכללא לשימוש במידע למטרה אחת, אין בה בכדי להתיר שימוש במידע למטרה אחרת. על כן, **מי שאסף מידע על אודות אדם למטרה מסוימת על יסוד הסכמה מכללא, אינו רשאי להשתמש במידע למטרות אחרות, אלא לאחר קבלת הסכמה חדשה לכך מנושא המידע.**

דוגמה: סטודנטים צולמו במהלך שיעור בקמפוס של מוסד להשכלה גבוהה. הצילום נעשה בידיעתם ובהסכמה מכללא לעצם הצילום, אך מבלי שנאמר להם אילו שימושים ייעשו בו בהמשך. לאחר מספר שנים, מצלם התמונה מבקש להשתמש בה לצרכים מסחריים ולפרסמה כחלק מקמפיין שיווקי לחברה לשיפור ציוני בגרויות. במצב עניינים זה, אין להסתמך על

⁴¹ תא"מ (עפולה) 50830-07-13 **אופיר כהן נ' שארבל קמוע** (פורסם בנבו, 8.9.19). פסיקת בית המשפט עסקה בהקשר זה בהעברת תמונות שצולמו במסגרת קמפיין פרסומי לאתר הפייסבוק העסקי של אשת הצלם בהיעדר הסכמת המצולמת או אימה לכך.

⁴² עת"מ (תל אביב-יפו) 36541-12-12 **חיים שטנגר נ' ועד מחוז תל-אביב והמרכז של לשכת עורכי הדין בישראל** (פורסם בנבו, 25.2.14), בפרק 3 לפסק הדין. בית המשפט קבע בעניין זה כי: "אף אם זכותם לפרטיות של הפרקליטים המועסקים על ידי ועדת האתיקה המחוזית הינה מסויגת ויש לראותם כמי שהסכימו למסירת פרטים אישיים מסוימים לציבור אותו הם משרתים, הרי שהמידע המבוקש בגדר עתירה זו נוגע לענייניו הפרטיים ביותר של אדם, אשר חשיפתו מדורגת במקום גבוה במדרג הפגיעות בפרטיות ואיני סבורה כי יש לראות את המשיבים 4-7 כמי שהסכימו מכללא לחשיפתו בעצם מינויים לתפקיד זה".



ההסכמה מכללא לצילום, ועל מצלם התמונה לפנות לסטודנטים במטרה לקבל את הסכמתם המפורשת לפרסום התמונה למטרה האמורה, תוך פירוט מטרת הפרסום.⁴³

הסכמה אקטיבית (Opt-in) או פסיבית (Opt-out)

38. ככלל, הסכם בין צדדים במסגרתו ניתנת הסכמה אקטיבית ומפורשת לפגיעה בפרטיות, יכול לכלול הוראות ספציפיות במתכונת המלמדת על רמת מודעות גבוהה יותר לפגיעה בפרטיות, ביחס לחלק מהתנאים המפורטים בו. הסכמות אלו יכולות להינתן בשתי צורות:

האחת, על יסוד פעולה אקטיבית של אדם מתוכה ניתן ללמוד על הסכמתו (Opt-in), כגון סימון ברובריקה המתירה שימוש במידע למטרה ספציפית אחרת מהמטרה לה ניתנה ההסכמה הכללית.

השנייה, על יסוד התנהגות פסיבית (Opt-out), כגון הימנעות מסימון ברובריקה שאוסרת על שימוש במידע אישי שאינו הכרחי למתן השירות, וזאת כאשר ההסכם מבהיר כי העדר הסימון מבטא קבלה של כלל תנאי ברירת המחדל הקבועים בו.⁴⁴

עם זאת, כפי שיפורט להלן, איסוף המידע ושימוש בו מכוח הסכמה אקטיבית דווקא, קרי במתכונת של Opt-in, יכול ללמד על מודעות גבוהה יותר לרכיבי ההסכמה. בנסיבות מסוימות, מתכונת זו היא שתגשים את הדרישה להסכמה מדעת.

39. כך, בעמדת היועץ המשפטי לממשלה בעניין **גרינברג**,⁴⁵ נאמר כי שימוש במידע אישי (כגון נתוני מיקום) למטרות "פרופיילינג" שאינו קשור ישירות בתכלית העסקה, מחייב קבלת הסכמה אקטיבית לכך מצד האדם נושא המידע, ולא ניתן להסתפק בעניין זה בהסכמה פסיבית, במיוחד במצבים של פערי כוח בין הצדדים, ובשים לב לקושי ליידע אותם באופן אקטיבי בדבר משמעות הסכמתם לאיסוף ועיבוד מידע על אודותיהם.

40. חובת קבלת הסכמה אקטיבית מסוג Opt-in חלה, לעמדת הרשות להגנת הפרטיות, גם בהקשר של **שירותי דיוור ישיר**.⁴⁶ בהקשר זה עמדת הרשות להגנת הפרטיות היא שבחובה אחיד, הסכמת לקוח לשימוש במידע על אודותיו למטרת שירותי דיוור ישיר, שאיננה קשורה בתכלית

⁴³ לעניין דומה ראו: ת"א (תל אביב-יפו) 43369-03-18 **שרית יחיא נ' המכללה האקדמית ספיר** (פורסם בנבו, 12.3.20). בעניין זה נקבע כי הסכמת המצולמים ניתנה לעצם הצילום שלהם, ואולם לא לשימוש בתצלומים למטרות שונות, לרבות מטרות פרסום.

⁴⁴ מיכאל בירנהק הסביר את הבדל בין המושגים באופן הבא: "שתי האפשרויות הן opt out לעומת opt in. במצב הראשון בררת-המחדל היא שהמידע ייאסף וייעשו בו שימושים ככל שאוסף המידע מפרט, ואדם שמתנגד לכך צריך לבצע פעולה יזומה של שינוי בררת-המחדל. במצב השני בררת-המחדל היא שהמידע לא ייאסף, אלא אם כן האדם מסכים שהוא ייאסף... במצב של opt out האפשרות לשינוי בררת-המחדל כלולה בחוזה מפורש, ואז ההסכמה היא מפורשת...". ראו: מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 53-54 (התשס"ח).

⁴⁵ לעיל הי"ש 20.

⁴⁶ ראו הנחיית הרשות להגנת הפרטיות מס' 2/2017 "**פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר**" **שירותי דיוור ישיר**.



העסקה, צריכה להיות במתכונת של Opt-in, באמצעותה מביע הלקוח באופן אקטיבי אינדיקציה מפורשת להסכמתו לשימוש המבוקש.

41. מעבר לכל האמור, כאשר הסכם כולל סעיפים למתן הסכמה לאיסוף מידע אישי שאינו נדרש למתן השירות, או לשימוש בו למטרות השונות מהותית ממטרת ההסכם (שלגביה ניתנה הסכמה כללית ומפורשת), רצוי שההסכמה הנפרדת לסעיפים אלו תיעשה במתכונת של הסכמה אקטיבית (Opt-in) ולא באופן פסיבי (Opt-out).

42. גם במקרים אחרים שאינם נוגעים להסכמה המאפשרת פגיעה בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות, ואשר בהם ניתן לעיתים להסתפק בהעדר התנגדות - לא תמיד ניתן להסתפק בהעדר ההתנגדות של אדם, ועל מבקש המידע לפנות בבקשה לקבלת הסכמה אקטיבית.

כך, בפסיקת בית המשפט העליון נקבע כי ככלל, במצבים של פנייה לרשות ציבורית על יסוד הוראות חוק חופש המידע, התשנ"ח-1998, למסירת מידע אישי על אדם, החוסה תחת חוק הגנת הפרטיות, נדרשת הסכמתו האקטיבית של נושא המידע לצורך מסירת המידע.⁴⁷

חזרה מהסכמה

43. הסכמה לפגיעה בפרטיות עשויה, במקרים מסוימים, לכלול גם את זכותו של אדם לחזור בו מהסכמתו, כלומר, לבקש את הפסקת השימוש במידע על אודותיו.

44. כך לדוגמה, בעניין אפריאט, נקבע כי אדם אשר העניק הסכמה לפרסום תמונתו אשר צולמה במסגרת השתתפותו במצעד הגאווה, רשאי לחזור בו מהסכמתו, בין שזו ניתנה במפורש ובין שמכללא, ומרגע שעשה כן, אין לעשות עוד שימוש בתמונה זו.

45. עמדה עקרונית המכירה בזכות לחזרה מהסכמה, במיוחד במקרים של פגיעה קשה בפרטיות, מצאה מקומה בפסיקת בית המשפט העליון בעניין פלוני,⁴⁸ שם ציין השופט סולברג כי:

"דומני, כי הסכמתו של אדם לפגיעה בפרטיותו, איננה סוף פסוק. מעמדה החוקתי של הזכות, אופייה האישי הקשה של הפגיעה בפרטיות, עשויים להציב את התרופות בגין חזרה מהסכמה, במקום שונה מזה שעל-פי דיני החוזים. יתכן שאכיפה לא תהא מוצדקת, בנסיבות של פגיעה קשה בפרטיות, לעומת פיצויים כספיים שיכול ותהיה הצדקה לפסוק בגין החזרה מן ההסכמה, אם זו גרמה לנזק. על-פי "מקבילית כוחות" בין עוצמת הפגיעה בפרטיות לבין תוקפה של ההסכמה, ככל שהפגיעה קטנה יותר כך

⁴⁷ ראו ע"מ 2820/13 רוזנברג נ' רשות האכיפה והגבייה (פורסם בנבו, 11.6.14), פסקה 20 לפסק דינו של השופט שהם. להבדיל, קבע בית המשפט כי בכל הנוגע למידע העלול לגרום נזק לצד שלישי, אך אינו מוגן לפי חוק הגנת הפרטיות, ניתן להסתפק בהעדר התנגדות של הצד השלישי, ולא נדרשת הסכמה אקטיבית. לעניין ראו גם ע"מ 1386/07 עיריית חדרה נ' שנירס בע"מ (פורסם בנבו, 16.7.2012).

⁴⁸ ע"א 8954/11 פלוני נ' פלונית (פורסם בנבו, 20.4.14). בהליך זה דחה בית המשפט העליון ערעור על החלטת בית המשפט המחוזי, שקיבל תביעה למתן צו מניעה לפיו יאסר על המערער לפרסם ולהפיץ ספר שכתב, המגולל את מערכת היחסים האינטימית שהתקיימה בינו לבין המשיבה.



גברו הסיכויים לקבלת סעד אכיפתי; ככל שהפגיעה קשה יותר, תיטה הכף להימנע מאכיפה, תוך מתן אפשרות לסעד של פיצויים".⁴⁹

46. לעמדת הרשות, במקרים בהם נעשה שימוש במידע על אדם מתוקף הסכמה שהתקבלה כדון, והאדם נושא המידע מבקש לחזור בו מהסכמתו ולהפסיק את השימוש במידע על אודותיו, יש לבחון בחיוב קבלת בקשה זו גם במקרים בהם ההסכמה איננה הדירה מלכתחילה כמפורט בסעיפים 44-45 לעיל, במיוחד במצבים בהם המשך השימוש במידע יפגע באופן קשה בפרטיות המבקש.

47. יובהר כי אין בחזרה מהסכמה בכדי לפגוע בחוקיות איסוף המידע והשימוש בו שקדמו לה, ככל שההסכמה לאיסוף ולשימוש במידע ניתנה כדון.

48. במקרים בהם התנהגותו של נושא מידע עשויה ללמד כי הוא מבקש לחזור בו מהסכמתו, או ללמד על כך שההסכמה מלכתחילה ניתנה באופן נקודתי או לזמן מוגבל, מומלץ כי בעל מאגר יפנה לנושא המידע על מנת לבחון האם הסכמתו עומדת בעינה.⁵⁰

כך למשל, במקרה בו אדם הוריד אפליקציית ניווט בעת שהותו בחו"ל, ואינו עושה שימוש באפליקציה למשך פרק זמן ממושך (למשל במשך שנה), מומלץ לפנות לאותו אדם לשם יידועו כי השימוש במידע על אודותיו נמשך מתוקף ההסכמה שהעניק עם הורדת האפליקציה, ולבחון האם הסכמתו עומדת בעינה.

סיכום: עיקרי הדגשים של הרשות להגנת הפרטיות בנושא הסכמה

49. כל פעולה המהווה פגיעה בפרטיותו של אדם לפי סעיף 2 לחוק הגנת הפרטיות, לרבות תוך איסוף ושימוש במידע אישי על אודותיו, חייבת להיעשות בהסכמתו או מכוח הסמכה בדון. ככלל, פגיעה בפרטיות בהיעדר הסמכה חוקית או הסכמה מהווה הפרה של הוראות החוק.

50. הסכמה לפגיעה בפרטיות, המתקבלת באופן מפורש או מכללא (קרי באופן משתמע), חייבת להיות מדעת. על כן, על מבקש ההסכמה לפעול באופן המבטיח כי האדם נושא המידע מודע לתוכן הבקשה, למטרותיה, ולהשלכות הסכמתו או סירובו לבקשה.

⁴⁹ שם, בפס' 160 לפסק דינו של השופט סולברג.

⁵⁰ להסדרה בדון של מנגנון ווידוא תוקף הסכמה שניתנה לתקופה קצובה בהקשר של מידע אישי פיננסי ראו סעיף 26(ב) לחוק שירות מידע פיננסי, התשפ"ב-2021, אשר קובע חובה אחת לשישה חודשים, לנקוט "פעולות הדרושות כדי לוודא כי הלקוח מודע לכך שאפשרות הגישה עומדת בעינה בהתאם להסכמתו כאמור".



51. על מבקש ההסכמה להקפיד להעמיד בפני אדם את הנתונים הרלוונטיים הדרושים לו, באורח סביר ובצורה מובנת, בקבלת החלטתו. סוג הנתונים והיקפם עשויים להשתנות בהתאם לנסיבות ובהן בין היתר: סוג המידע ורגישותו והשימושים המבוקשים במידע.
- לעמדת הרשות, עמידה בתנאי סעיף 11 לחוק היא דרישת המינימום המתחייבת לשם קיום חובת היידוע, ואולם אין בה כדי להבטיח את העמידה בדרישת ההסכמה מדעת. ככלל, **בנסיבות בהן קיימים פערי כוח בין צדדים, או כאשר מדובר בפעולה בעלת פוטנציאל לפגיעה קשה בפרטיות או בנסיבות מורכבות אחרות (כגון שימוש בטכנולוגיה חדשה שהשלכות השימוש בה אינן ברורות דיין) – יש לראות בחובה זו כחובה מוגברת, ועל מבקש ההסכמה יהא להקפיד להציג באופן בולט ופשוט את כלל הנתונים הרלוונטיים להחלטה, וכן להציגם ככל הניתן בנפרד משאר רכיבי ההתקשרות. העדר פירוט מספק במסגרת הליך קבלת ההסכמה עלול להביא לפגיעה בתוקפה של ההסכמה.**
52. **יש להקפיד כי תוכן ההסכמה יוצג באופן ברור, נגיש ומובן.** התייחסות מיוחדת יש לתת בהקשר זה לאוכלוסיות מיוחדות, כגון בני-נוער או אנשים עם מוגבלות.
53. במצבים מסוימים, בהם קיים חשש אינהרנטי כי ההסכמה שניתנה היא "חשודה", הנטל לשכנע כי הסכמה לפגיעה בפרטיות ניתנה מתוך רצון חופשי של אדם עשוי להיות מוטל על כתפיו של מבקש ההסכמה.
- לשם בחינת השאלה האם הסכמה ניתנה מתוך בחירה ורצון חופשי אמיתי ייבחנו, בין היתר, נסיבות מתן ההסכמה, מועד קבלתה, אופן הצגת הבקשה (לרבות שימוש מבקש המידע ב"טקטיקות אפלות" ובכלים עיצוביים שנועדו להקשות על נושא המידע), אופן קבלת ההסכמה (במפורש או מכללא; באופן אקטיבי או פסיבי), וזוהות הצדדים ויחסי הכוחות ביניהם.
- במקרים של הסכמה חשודה יכול מבקש ההסכמה לנקוט אמצעים שונים - כגון העמדת חלופה סבירה או אי-התניית קבלת השירות במתן הסכמה לאיסוף מידע שאינו נדרש - על מנת להראות כי ההסכמה מבטאת את רצונו החופשי ואת בחירתו האמיתית של נושא המידע.**
54. במצב בו אדם כלל אינו יכול, הלכה למעשה, לסרב לפעולה הפוגעת בפרטיותו, יהיה קשה לראות בהסכמתו ככזו שניתנה מתוך רצון חופשי, והדבר עשוי להשליך על תוקפה של הסכמה זו. וזאת ללא קשר לשאלה האם ההסכמה ניתנה במפורש או מכללא.
55. שינוי מהותי של תנאי שימוש במידע ללא קבלת הסכמה נוספת יחשב כשימוש במידע שלא על יסוד הסכמה שהתקבלה מדעת ומתוך רצון חופשי.
56. אופן קבלת ההסכמה עשוי להשפיע על תוקפה. גם במקרים בהם הסתמכות על הסכמה מכללא היא אפשרית, רצוי ככל הניתן לפנות לאדם לקבלת הסכמתו המפורשת, וזאת בעיקר במקרים של איסוף מידע רגיש או נקיטת פעולה העלולה להביא לפגיעה קשה בפרטיות.



ככלל, שתיקתו של אדם, או העדר מחאה מצדו לאיסוף מידע הנוגע אליו, כשלעצמם, לא מהווים הסכמה תקפה לפי דיני הגנת הפרטיות.

57. מתן הסכמה בעל-פה היא עניין טעון הוכחה, ועל כן מומלץ כי מבקש ההסכמה יתעד אותה באמצעים הניתנים להצגתה, וזאת בעיקר במקרים של איסוף מידע רגיש או בנסיבות בהן קיימים פערי כוח בין הצדדים.

58. **הסכמה מפורשת או מכללא לשימוש במידע למטרה אחת, אין בה בכדי להתיר שימוש במידע למטרה אחרת.** על כן, גם מי שאסף מידע למטרה מסוימת על יסוד הסכמה מכללא, אינו רשאי להשתמש במידע למטרות אחרות, אלא לאחר קבלת הסכמה חדשה לכך מנושא המידע.

59. כאשר הסכם כולל סעיפים למתן הסכמה לאיסוף מידע אישי שאינו נדרש למתן השירות, או לשימוש בו למטרות השונות מהותית ממטרת ההסכם (שלגביה ניתנה הסכמה כללית ומפורשת), רצוי שההסכמה במסגרת סעיפים אלו תיעשה במתכונת של הסכמה אקטיבית נפרדת (Opt-in) ולא באופן פסיבי (Opt-out).

ואולם, במקרים בהם ההסכם כולל סעיפים למתן הסכמה לשימוש במידע אישי לצרכי "פרופיילינג" שאינו נדרש או קשור ישירות למטרת שירות בין צדדים שביניהם יש פערי כוח, וכן לעמדת הרשות להגנת הפרטיות גם בהקשר של שירותי דיוור ישיר – לא ניתן להסתפק בהסכמה פסיבית, ועל ההסכמה להתקבל במתכונת של הסכמה אקטיבית נפרדת (Opt-in).

60. במקרים בהם נעשה שימוש במידע על אודותיו של אדם מתוקף הסכמה שהתקבלה כדין, והאדם נושא המידע מבקש לחזור בו מהסכמתו ולהפסיק את השימוש במידע על אודותיו, יש לבחון בחיוב קבלת בקשה זו, גם במקרים בהם ההסכמה איננה הדירה מלכתחילה כמפורט בסעיפים 44-45 לעיל במיוחד במצבים בהם המשך השימוש במידע יפגע באופן קשה בפרטיות המבקש.

61. נזכיר, כי כל הפוגע בפרטיותו של אדם ללא הסכמתו ומבקש להסתמך לשם כך על הוראות סעיף 18(2) לחוק, צריך לעמוד בדרישת המידתיות (ראו סעיף 20(ב) לחוק). בכלל זה, עליו להיות מסוגל להצביע על כך שקבלת הסכמה לא הייתה אפשרית בנסיבות העניין, ואם לא כן הוא עלול להיות מוחזק כמי ש"פגע בודעין במידה גדולה משהיתה נחוצה באופן סביר" לצורך האינטרסים להם ניתנה ההגנה בסעיף 18.⁵¹

62. איסוף מידע אישי ושימוש בו הפוגעים בפרטיות, שאינם מלווים בהסכמה תקפה בהתאם לאמור במסמך זה או בהסמכה בדיון, מהווים עוולה אזרחית ועשויים להוות עבירה פלילית. מעבר לכך, במקרים אלו עשויה הרשות להפעיל את סמכויות האכיפה המוקנות לה בדיון וכן

⁵¹ להרחבה וליישום הוראות סעיף 18 באירועי חירום ראו: [הרשות להגנת הפרטיות "עקרונות הגנת פרטיות בהתמודדות עם אירועי חירום" \(ספטמבר, 2024\)](#).



לסרב לאשר רישום של מאגר מידע, כמו גם להשחות או לבטל רישום של מאגר קיים, שמשמעותם איסור על ניהול והחזקת מאגר המידע.⁵²

המלצות לחיזוק הליך קבלת הסכמה מקוונת⁵³

- בעת פנייה לקבלת הסכמה מקוונת ובניסוח מסמכי מדיניות פרטיות ותנאי שימוש, הדגישו והבליטו את ההיבטים המרכזיים והמשמעותיים ביותר הנוגעים לפרטיות, לאופן השימוש במידע הנאסף במסגרת השירות ולתכליות השימוש בו.
- השתמשו בדרכים יצירתיות וחדשניות לפישוט הליך קבלת ההסכמה, ובכלל זה:
 - השתמשו בסרטוני הסברה, תמונות ואימוג'ים;
 - השתמשו ב"באנרים קופצים" להבלטת הדגשים המרכזיים הנוגעים לפרטיות;
 - השתמשו בכלים אינטראקטיביים להגברת המעורבות של משתמשים בהליך קבלת ההסכמה.
- התאימו את טפסי קבלת ההסכמה והיידוע לסוגי המכשירים השונים (כגון מחשב נייד, טלפון חכם), בהם עשוי להיעשות שימוש למתן הסכמה.
- הציגו למשתמשים רמות שונות של פירוט בדבר איסוף המידע ואופן השימוש בו (מרמת הפירוט הבסיסית הנדרשת על-פי דין ועד רמת פירוט גבוהה ומפורטת), ואפשרו להם לשלוט על רמת הפירוט לה הם מבקשים להיחשף.
- הימנעו מקבלת הסכמה גורפת למתן שירות, ואפשרו למשתמשים להחליט איזה סוגי מידע הם מוכנים כי ייאספו, ולאילו מטרות.
- קיימת חשיבות של ממש בציפייה הסבירה של משתמשים בכל הנוגע לסוג המידע האמור להיאסף במסגרת מתן שירות מסוים, ולאופן השימוש בו. ככל שבכוונתכם לאסוף מידע ולהשתמש בו באופן החורג באופן מובהק מציפייה זו – הבהירו והדגישו זאת בטרם קבלת ההסכמה.

כך למשל, סביר להניח כי הורים המעניקים הסכמה לאיסוף נתוני מיקום של ילדיהם לאפליקציה שנועדה לספק הגנה על ילדים במרחב הפיזי, אינם מצפים כי האפליקציה תשתמש במידע לצורכי שיווק ופרסום מוצרים להורים. כאשר החברה מבקשת לעשות שימוש בנתוני המיקום לצרכים אלו, עליה לפעול באמצעים שונים להבהרת הדברים בצורה מפורשת, במסגרת קבלת הסכמת ההורים, בהסכמה נפרדת, לשימושים נוספים אלו.

⁵² ראו סעיף 10(ב2) לחוק הגנת הפרטיות.

⁵³ חלק זה מבוסס בחלקו על הנחיות נציב הפרטיות הקנדי. להרחבה ראו: Office of the Privacy Commissioner of Canada [Guidelines for obtaining meaningful consent](#) (13, Aug. 2021).