תיקון 13 לחוק הגנת הפרטיות

משמעותו, השלכותיו וחסרונותיו

רחל אריאלי הרשקוביץ

מרץ 2026

הצעה לסדר 62

המכון הישראלי לדמוקרטיה

המכון הישראלי
לדמוקרטיה

תיקון 13
לחוק הגנת הפרטיות

משמעותו, השלכותיו וחסרונותיו

רחל ארידור הרשקוביץ

הצעה לסדר 62
מרץ 2026

Reforming Privacy Law in Israel:
Assessing Amendment 13 and What It Still Fails to Cover

Rachel Aridor Hershkovitz

עריכת הטקסט: לילך צ׳לנוב
עיצוב הסדרה והעטיפה: סטודיו Alfabees
ביצוע גרפי: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים

מסת״ב 978-965-519-519-4

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע״ר), 2026
נדפס בישראל, תשפ״ו/2026

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר – כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו״ל.

המכון הישראלי לדמוקרטיה
רח׳ פינסקר 4, ת״ד 4702, ירושלים 9104602
טל׳: 02-5300888
אתר האינטרנט: www.idi.org.il

כל פרסומי המכון ניתנים להורדה חינם, במלואם או בחלקם, מאתר האינטרנט.

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

הדברים המובאים במסמך זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.

תוכן העניינים

תקציר 7

מבוא 9

פרק 1. תיקון 13 – מטרות והיסטוריה חקיקתית 20

פרק 2. החידושים העיקריים בתיקון 13 לעניין הרחבת תחולת חוק הגנת הפרטיות 25

פרק 3. החידושים העיקריים בתיקון 13 לעניין רישום מאגר מידע 51

פרק 4. החידושים העיקריים בתיקון 13 לעניין עיבוד מידע 64

פרק 5. החידושים העיקריים בתיקון 13 לעניין חובות בעל השליטה או המחזיק 86

פרק 6. החידושים העיקריים בתיקון 13 לעניין זכויות נושא המידע 110

פרק 7. עם הפנים קדימה – מה נותר עוד לתקן? 114

סיכום 138

תקציר

מסמך זה מנתח את תיקון מס' 13 לחוק הגנת הפרטיות על רקע הצורך בעדכון מקיף של דיני הפרטיות בישראל והתאמתם לעידן הדיגיטלי. התיקון נועד לחזק את ההגנה על מידע אישי ולהתאימה לסטנדרטים בינלאומיים מתקדמים, לנוכח התעצמות השימוש במידע, התפתחות טכנולוגיות מתקדמות והתגברות איומי הסייבר. במסגרת זו, המסמך סוקר את השינויים העיקריים שמביא התיקון, ובהם השינויים בהגדרת המונחים המרכזיים בחוק, הרחבת סמכויות האכיפה והפיקוח של הרשות להגנת הפרטיות, שינוי מודל רישום מאגר מידע ברשות להגנת הפרטיות, הוספת חובת מינוי ממונה הגנת פרטיות, ביטול המגבלה על תקופת ההתיישנות ועיגון פסיקתם של פיצויים לדוגמה.

לצד הצגת תרומתו של התיקון, המסמך מצביע על מגבלותיו. שינוי ההגדרות, הנחוץ וההכרחי, אכן הוביל להרחבת תחולת החוק, אולם לא נעשה עדכון מקביל של ההסדרים המהותיים. בעקבות זאת נותרו פערים מהותיים ביחס להסדרים המקובלים בעולם, ובמיוחד ביחס למסגרת האירופית, וכן גבר חוסר הוודאות המשפטית בדבר המותר והאסור בעיבוד מידע אישי. פער זה, בין הרחבת התחולה לבין היעדר רפורמה מהותית, עלול להכביד על פעילות המשק, להקשות על אכיפה אפקטיבית, ואף לפגוע בהגנה על פרטיות בפועל, בשל קושי בפרשנות החוק וביישומו.

לפיכך, המסמך מדגיש כי אף שהתיקון הוא צעד חשוב לקראת מודרניזציה רגולטורית, אין בו כדי להשלים רפורמה כוללת הנדרשת להתמודדות עם אתגרי עיבוד המידע בעידן של בינה מלאכותית, כלכלת נתונים ושירותים דיגיטליים חוצי גבולות. משום כך המסמך מציג המלצות להשלמת המהלך החקיקתי באמצעות קביעת מסגרת מהותית ברורה ומאוזנת לעיבוד מידע אישי, שתאזן בין ההגנה על זכויות יסוד לבין צורכי חדשנות, ביטחון וסייבר, ותספק ודאות רגולטורית למחוקק, לרשויות האכיפה ולשוק.

מבוא

חוק הגנת הפרטיות הישראלי נחקק בשנת 1981.[1] הצעת החוק (להלן: הצעת חוק 1980) שהובילה לחקיקתו לא עסקה כלל בעיבוד מידע או במאגרי מידע,[2] אלא הייתה ממוקדת אך ורק במופעי פגיעה בפרטיות שבין אדם לאדם, המכונים "הפרטיות הקלאסית". למשל, פגיעה העלולה להיווצר בעקבות חיטוט במכתביו של אחר, או עקב שימוש שאדם עושה במכשירים טכנולוגיים למטרות האזנה, התחקות ובילוש מרחוק.[3] בהצעת החוק נקבע שהסכמתו של אדם, במפורש או מכללא, היא תנאי להכשרה מראש של כל פגיעה בפרטיות.[4]

במהלך הדיונים בהצעת החוק 1980 בוועדת החוקה, חוק ומשפט של הכנסת (להלן: ועדת החוקה) התעורר החשש שהנוסח המוצע חסר ויש לתת את הדעת גם ל"עניין המחשבים".[5] לפיכך החליטה ועדת החוקה למנות ועדת מומחים ציבורית בראשות יו"ר הוועדה דאז, ח"כ דוד גלס, לגיבוש התייחסות בחוק גם לנושא זה. בעקבות המלצות ועדת מומחים זו, החליטה ועדת החוקה לשלב, כבר בהצעת חוק 1980, את פרק ב, ובו עשרה סעיפים שמטרתם "מניעת פגיעה באזרח באמצעות מידע המרוכז במחשבים".[6] המצב שעמד לנגד עיני ועדת החוקה בזמנו היה אגירת מידע אישי על אדם באמצעות מחשבים. למשל, מידע

1 חוק הגנת הפרטיות, התשמ"א–1981, ס"ח התשמ"א עמ' 128, התשע"ז עמ' 986 (להלן: חוק הגנת הפרטיות לפני תיקון 13).

2 הצעת חוק הגנת הפרטיות, תש"ם–1980 (להלן: הצעת החוק 1980).

3 סעיף 2 לחוק הגנת הפרטיות, התשמ"א–1981, ס"ח התשמ"א עמ' 128, התשע"ז, בעמ' 986, התשפ"ד 1430 (להלן: חוק הגנת הפרטיות), כולל את התיקונים שהוספו לו בחוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד–2024, ס"ח התשפ"ד עמ' 1430 (להלן: תיקון 13). הסעיף מגדיר פגיעה בפרטיות כרשימה סגורה של מופעים.

4 סעיף 1 להצעת החוק 1980, לעיל ה"ש 2, קבע כי "לא יפגע אדם בפרטיות זולתו ללא הסכמתו". "הסכמה" הוגדרה בסעיף 3 כך: "'הסכמה' – במפורש או מכללא".

5 פרוטוקול מס' 265 ועדת החוקה חוק ומשפט, יום ב', י"ד בשבט התשמ"א, 19 בינואר 1981, בעמ' 18–19.

6 פרוטוקול מס' 271 מישיבת ועדה החוקה, חוק ומשפט, יום רביעי, ל' בשבט התשמ"א, 4.2.1981, בעמ' 8.

שמפלגה אוספת בסקר מדלת לדלת, או מידע שרופאה בקופת חולים מעדכנת על מטופליה בעת בדיקתם.[7] לפיכך, כבר במהלך הדיונים בהצעת חוק 1980 עוגנו בפרק ב בחוק הגנת הפרטיות הוראות המחייבות רישום של מאגר מידע, מגבילות את השימוש במידע רק למטרה שלשמה הוקם או נועד מאגר המידע, ובלבד שמדובר במטרה חוקית, ומעגנות את זכויות נושא המידע לעיין במידע האישי האגור במאגר מידע ולתקנו במידת הצורך.[8] כך, חוק הגנת הפרטיות שנחקק ב־1981, בסיומם של הדיונים בוועדת החוקה בהצעת חוק 1980, מאסדר שני סוגים של הזכות לפרטיות בחוק אחד. פרק א לחוק הגנת הפרטיות עוסק בנושאים הנוגעים לפרטיות הקלאסית, לפני הדיגיטיזציה וטכנולוגיות עיבוד המידע. הכוונה בעיקר להגנה על אדם מפני חדירה למרחב הפיזי שלהם, מפני התערבות בבחירותיהם האישיות ובהחלטות הנוגעות לאורחות חייהם ולענייניהם הפרטיים. הזכות לפרטיות בהקשר הזה נקשרת בעיקר למאמרם הנודע של עורכי הדין האמריקאים, לואיס ברנדס, שלימים מונה לשופט בבית המשפט העליון בארצות הברית, ועמיתו סמואל וורן, משנת 1890, שבו הגדירו את הזכות לפרטיות כזכות להיעזב במנוחה (the right to be left alone). השניים, שסלדו מכתבות רכילות שפורסמו בעיתונות המקומית עליהם ועל חבריהם, ביקשו ליצור באמצעות הזכות לפרטיות כלי למניעת חשיפה זו.[9] פרק ב בחוק הגנת הפרטיות עוסק בעולם הפרטיות המידעית המודרנית,[10] זו הנוגעת להגנה על המידע, לזהות הדיגיטלית של האדם ולשליטתו במידע האישי הנאסף על אודותיו. כל זאת אף שבמרבית המדינות החקיקה המגנה על הזכות לפרטיות אינה דואלית. הפרטיות הקלאסית מעוגנת בנפרד מחקיקת הפרטיות המודרנית, המוקדשת בעיקרה להגנה על מידע (data protection).

7 פרוטוקול 272 מישיבת ועדת החוקה, חוק ומשפט, יום ב', ה' באדר א', 9 בפברואר 1981, בעמ' 11–12.

8 פרוטוקול מס' 271, לעיל ה"ש 6, בעמ' 11.

9 Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 Ariz. L. Rev. 1 (1979)

10 מיכאל בירנהק **פרטיות חוקתית** (אוניברסיטת בר אילן ונבו, התשפ"ג–2023).

השנים חלפו, הטכנולוגיה כדרכה המשיכה להתפתח, ואילו המשפט נותר מאחור. רק ב־1996 נחקק תיקון חשוב לחוק הגנת הפרטיות בנושא מאגרי מידע (להלן: תיקון 4).[11] תיקון 4 עסק בעיקר בדרכים להביא לשיפור אבטחת המידע לנוכח התגברות דליפות מידע ממאגרי מידע. במסגרת זו הוספו לחוק הגנת הפרטיות הוראות בדבר רישום מאגרים, הורחבו סמכויות הרשם, הוגדר "מידע רגיש", הוספו סעיפים העוסקים ב"מחזיק", עוגן מעמדו של מנהל מאגר, והוטלה חובת אבטחת מידע. לצד זו חודדה הגדרת "מאגר מידע", ובעקבותיה הוצאו מאגרי מידע לשימוש אישי ומאגרי מידע לשימוש עסקי המיועדים אך ורק ליצירת קשר עם לקוחות מתחולת חוק הגנת הפרטיות. כן הוספו לחוק הגנת הפרטיות הוראות לעניין דיווח ישיר.[12]

התיקון החשוב הבא לחוק הגנת הפרטיות, תיקון לעניין עיבוד מידע אישי, נחקק ב־2007 (להלן: תיקון 9).[13] תיקון 9 עסק בשלושה עניינים מרכזיים: פרטיותו של המת, עיגון פיצוי ללא הוכחת נזק בגין פגיעה בפרטיות, והוספת יסוד הידיעה לדרישת ההסכמה.[14] עוד הובהר בתיקון 9, שמכתב או כתב, שהעתקתו או שימוש בתוכנו ללא רשות הם פגיעה בפרטיות לפי סעיף 2(5) לחוק הגנת הפרטיות, כוללים גם מסר המועבר או נשמר באמצעים אלקטרוניים או אופטיים.[15]

11 חוק הגנת הפרטיות (תיקון מס' 4) (מאגרי מידע), התשנ"ו–1996 (להלן: תיקון 4). נציין כי בשנת 1985 התקבל תיקון לחוק הגנת הפרטיות, אולם תיקון זה עסק במסירת מידע על ידי גופים ציבוריים. ראו חוק הגנת הפרטיות (תיקון), התשמ"ה–1985.

12 ראו בתיקון 4, לעיל ה"ש 11, בסעיף 1 המתקן את סעיף 3 בחוק הגנת הפרטיות ומוסיף הגדרה ל"מחזיק". סעיף 3 המתקן את סעיף 7 בחוק הגנת הפרטיות ומוסיף הגדרות למונחים "אבטחת מידע", "מידע רגיש", "מנהל מאגר" ומתקן את הגדרת "מאגר מידע", וסעיפים 4 ו־5 המוסיפים הוראות לעניין רישום מאגרי מידע וסמכויות הרשם לעניין זה.

13 חוק הגנת הפרטיות (תיקון מס' 9), התשס"ז–2017 (להלן: תיקון 9).

14 דברי שרת המשפטים דאז ציפי ליבני בעת הצגת החוק במליאת הכנסת, פרוטוקול ישיבת מליאת הכנסת, הכנסת ה־16 ישיבה 305, יום רביעי, כ' בכסלו התשס"ו, 21 בדצמבר 2005, בעמ' 127.

15 סעיף 1 בתיקון 9, לעיל ה"ש 13.

תיקון דרישת ההסכמה בתיקון 9 והפיכתה להסכמה מדעת נועד להבטיח שלפני שנושא המידע מסכים לפגיעה בפרטיותו יהיה בידו "מידע, הדרוש לו, באורח סביר, כדי להחליט האם להסכים או לא, והמידע ימסר לו בצורה מובנת".[16] כן הובהר בהצעת חוק תיקון 9 כי דרישת ההסכמה מדעת חשובה במיוחד לנוכח הפרקטיקה של הסכמי הוויתור על הפרטיות המקובלים ב"עידן האינטרנט".[17]

לצד תיקוני החקיקה התקבלו לאורך השנים כמה החלטות ממשלה המסדירות את הקמתה ואת פעולותיה של הרשות להגנת הפרטיות. ראשית, ב־2006 קיבלה הממשלה החלטה בדבר הקמתה של הרשות למשפט וטכנולוגיה, יחידה במשרד המשפטים, ובדבר אסדרת איתור ומינוי ראש הרשות, שימלא את תפקיד ה"רשם" לפי חוק הגנת הפרטיות.[18] לפי ההחלטה, הרשות למשפט וטכנולוגיה תאגד את כלל סמכויות הפיקוח והאכיפה לפי חוק הגנת הפרטיות, חוק חתימה אלקטרונית, התשס"א–2001 וחוק שירותי נתוני אשראי, התשס"ב–2002.[19] ב־2017 שונה שמה של הרשות למשפט וטכנולוגיה, והיא מכונה מאז "הרשות להגנת הפרטיות".[20] בשלהי 2022 קיבלה הרשות להגנת הפרטיות חיזוק חשוב למעמדה, אף שהיא נותרה יחידה בתוך משרד המשפטים. החלטת ממשלה 1890 עיגנה את עצמאות הרשות להגנת הפרטיות בכל הקשור להפעלת סמכויותיה על פי דין, מנתה את תפקידיה העיקריים של הרשות והגדירה את תנאי הכשירות לתפקיד ראש הרשות.[21]

16 הצעת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ו–2005, (להלן: הצעת חוק תיקון 9) דברי ההסבר לסעיף 3(2).

17 שם.

18 על פי סעיף 7 לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1, "רשם" הוא "מי שמינתה הממשלה בהודעה ברשומות לנהל את פנקס מאגרי מידע".

19 החלטת ממשלה 4660 (א) הקמת רשות משפטית לטכנולוגיות מידע והגנה על הפרטיות במשרד המשפטים; (ב) פטור ממכרז (מינוי באמצעות ועדה לאיתור מועמדים) למשרת ראש הרשות המשפטית לטכנולוגיות מידע והגנה על הפרטיות במשרד המשפטים (8.1.2006).

20 החלטת ממשלה 3019 שינוי שם הרשות למשפט טכנולוגיה ומידע במשרד המשפטים (7.9.2017).

21 החלטת ממשלה מס' 1890 עצמאות הרשות להגנת הפרטיות ותיקון החלטת ממשלה (2.10.2022).

עם זאת, החלטות ממשלה אלו לא עוגנו בחקיקה. משנת 2007 ועד אוגוסט 2024 לא התקבלה שום הצעה לתיקון ממשי לחוק הגנת הפרטיות, אף שבמהלך שנים אלו הוגשו כמה הצעות חוק פרטיות וממשלתיות לתיקונים למיניהם. כך, למשל, ב־2009 הגיש ח"כ אופיר פינס־פז הצעה להטלת איסור על מעקב של מעביד אחר עובדיו.[22] ב־2013 הגישו כמה חברי כנסת הצעה להטלת חובת דיווח על פריצה למאגר מידע. הצעות דומות הוגשו גם בשנים 2015 ו־2019.[23] ב־2015 הגישו כמה חברי כנסת הצעה להוספת הזכות להישכח. הצעות דומות הוגשו גם בשנים שאחר כך.[24] ב־2017 הגישו כמה חברי כנסת הצעה לאסדרת הזכות לפרטיות של קטינים. הצעות דומות הוגשו גם בשנים 2018–2021.[25] ב־2018 הגישו כמה חברי כנסת הצעה להארכת תקופת ההתיישנות בתביעות אזרחיות לפי חוק הגנת הפרטיות. הצעות ברוח זו הוגשו גם בשנים 2019 ו־2021.[26] ב־2022 הגיש ח"כ

22 הצעת חוק הגנת הפרטיות (תיקון – איסור מעקב של מעביד אחר עובדיו), התש"ע–2010.

23 הצעת חוק הגנת הפרטיות (תיקון – דיווח על פריצה למאגר מידע), התשע"ד–2013. הצעת חוק הגנת הפרטיות (תיקון – דיווח על פריצה למאגר מידע), התשע"ה–2015. הצעת חוק הגנת הפרטיות (תיקון־דיווח על פריצה למאגר מידע), התש"ף–2019.

24 הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התשע"ה–2015. ב־2016 הגישו ח"כ אורי מקלב ועופר שלח את הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התשע"ו–2016. בשנת 2017 הגישה ח"כ מרב בן ארי את הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התשע"ז–2017. ח"כ יזהר שי ועופר שלח הגישו הצעה דומה בשנת 2019. ראו הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התש"פ–2020. ב־2020 הגיש ח"כ שלח הצעה דומה. ראו הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח), התש"ף–2020.

25 ראו הצעת חוק הגנת הפרטיות (תיקון הגנה על פרטיותם של קטינים, התשע"ז–2017. ח"כ מיקי רוזנטל הגיש בשנת 2018 את הצעת חוק הגנת הפרטיות (תיקון – פרטיות תקינים), התשע"ח–2018. ח"כ אלהרר הגישה הצעות דומות בשנים שאחר כך. ראו הצעת חוק הגנת הפרטיות (תיקון – פרטיות קטינים), התש"ף–2019, הצעת חוק הגנת הפרטיות (תיקון – פרטיות קטינים), התש"ף–2020, הצעת חוק הגנת הפרטיות (תיקון – פרטיות קטינים), התשפ"א–2021. ב־2018 הגישו כמה חברי כנסת הצעה לתיקון חוק הגנת הפרטיות ולעיגונה של הזכות להישכח של קטינים. ראו הצעת חוק הגנת הפרטיות (תיקון – הזכות להישכח של קטינים), התשע"ח–2018.

26 ראו הצעת חוק הגנת הפרטיות (תיקון – תקופת ההתיישנות), התשע"ח–2018. ב־2019 הגיש ח"כ עמר בר לב הצעה דומה. ראו הצעת חוק הגנת הפרטיות (תיקון – תקופת ההתיישנות), התש"ף–2019. הצעה דומה הוגשה גם על ידי ח"כ מרב בן ארי בשנת 2021. ראו הצעת חוק הגנת הפרטיות (תיקון – תקופת ההתיישנות), התשפ"א–2021.

גלעד קריב הצעה לתיקון חשוב של הוראות חוק הגנת הפרטיות לעניין עיבוד מידע והתאמתן לדין הנוהג באיחוד האירופי ובמדינות נוספות.[27] לצד הצעות החוק הפרטיות האלה הגישה הממשלה בשלהי 2011 וב־2018 הצעות לתיקון חוק הגנת הפרטיות.[28] הצעות חוק ממשלתיות אלו היו הבסיס לתיקון 13.

שלל הצעות החוק שפורטו לעיל אומנם לא התגבשו לחוק, אך יש בהן כדי ללמד על הלך הרוח. הן מעידות על ההבנה בקרב חברי הכנסת ובמשרד המשפטים שהטכנולוגיה מתקדמת והמשפט נותר מאחור, ושיש צורך בעדכון חוק הגנת הפרטיות. עם זאת, מלבד הצעתו של ח"כ קריב משנת 2022,[29] הצעות החוק האחרות, לרבות הצעות החוק שהגיש משרד המשפטים ב־2011 וב־2018, לא ניסו לתקן תיקון מלא ומקיף בחוק הגנת הפרטיות לשם התאמתו למציאות הטכנולוגית העדכנית או לדין הבינלאומי בתחום, אלא כל אחת מהצעות החוק עסקה בנושא מסוים ומצומצם.

כך נותר חוק הגנת הפרטיות במדינת ישראל מתאים למציאות הטכנולוגית שנחקקה ב־2007, השנה שבה הושק האייפון של חברת אפל לצד הספר הדיגיטלי, קינדל, של אמזון.[30] אומנם הרשת החברתית פייסבוק כבר פעלה ב־2007, וכבר פעלו בה כ־50 מיליון משתמשים (לעומת 3.07 מיליארד משתמשים בחודש היום).[31] אולם טכנולוגיות אחרות, חשובות מבחינת עיבוד מידע אישי, הושקו

27 הצעת חוק הגנת הפרטיות (תיקון – חיזוק הזכות לפרטיות וההגנה עליה), התשפ"ג–2022.

28 הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2011 (להלן: תיקון 12), הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018.

29 הצעת חוק הגנת הפרטיות (תיקון – חיזוק הזכות לפרטיות וההגנה עליה), התשפ"ג–2022.

30 Tom Spring, *The Year in Tech: Top 2007 News and Trends,* PCWorld (Dec. 25, 2007)

31 *Number of Active Users at Facebook over the Years*, The Associated Press (Feb. 1, 2012); Naveen Kumar, Facebook Users Statistics (2025) – Latest Worldwide Data (Aug. 19, 2025)

רק שנים אחר כך. למשל, רשת המסרים המיידים ווטסאפ הושקה בשנת 2009 ואינסטגרם – בשנת 2010; טיקטוק הושקה לקהל הבינלאומי ב־2016, והגרסה הראשונה של מערכת ההפעלה אנדרואיד – בשלהי 2008. טכנולוגיות AI, כגון ChatGPT ו־Gemini, הופיעו שנים רבות אחר כך.

לצד החסר בחקיקה הראשית, בשנת 2018 נכנסו לתוקפן תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז־2017 (להלן: תקנות אבטחת מידע). תקנות אבטחת מידע נועדו לחזק את ההגנה על מידע אישי באמצעות דרישות אבטחת מידע שהוטלו על כל גוף, ציבורי או פרטי, המנהל או מעבד מידע אישי דיגיטלי. חובות אבטחת המידע הותאמו לפעילות עיבוד המידע בארגון, על בסיס ההנחה שרמת הסיכון לפגיעה בפרטיות מושפעת מגודל מאגר המידע, מרגישות המידע האגור בו וממספר המורשים לגשת אליו.[32] אף שהתקנות הציגו שינוי של ממש בדרישות אבטחת המידע, הן התמקדו אך ורק בנושא הזה. תקנות אבטחת מידע לא הביאו להשלמת החסר בחוק הגנת הפרטיות בכל הנוגע למותר ולאסור ביחס לעיבוד מידע אישי, אלא לקונקרטיזציה של דרישות אבטחת המידע.

זאת ועוד, בעוד מדינת ישראל קפאה על שמריה פחות או יותר בתחום הגנת הפרטיות של אזרחיה, התרחש שינוי חשוב במישור הבינלאומי. בשנת 2016 התקבלו באיחוד האירופי תקנות חדשות להגנת מידע, ה־GDPR.[33] ה־GDPR החליף את דירקטיבת הגנת המידע, שקדמה לו באיחוד האירופי,[34] וכלל כמה

32 ראו המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע), הרשות להגנת הפרטיות (2017, עודכן 2023).

33 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (להלן: GDPR).

34 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (להלן: דירקטיבת הגנת המידע).

חידושים מרכזיים. כך, הרחיב ה־GDPR את אגד זכויות נושא המידע ועיגן במסגרתו גם את זכות הניוד,[35] זכות המחיקה (המכונה הזכות להישכח),[36] והאיסור, המכונה גם הזכות של נושא המידע, על קבלת החלטות המבוססות על עיבוד אוטומטי של מידע אישי.[37] אשר לדרישת ההסכמה, היא לא הייתה הבסיס החוקי היחיד לעיבוד מידע אישי כבר לפי דירקטיבת הגנת המידע, שנחקקה בשנת 1995.[38] עם זאת, ה־GDPR חיזק עוד יותר את דרישת ההסכמה וקבע כי הסכמה המכשירה עיבוד מידע חייבת להיות מרצון חופשי, מסוימת, מדעת וחד־משמעית. נוסף על כך, עוגנה זכות נושא המידע לחזור בו מהסכמתו בכל עת. כך הבהיר ה־GDPR שמנגנון ה־opt-out (שבמסגרתו נעשה שימוש במידע אישי בהנחה שנושא המידע יסכים לו, ועל נושא מידע שאינו מסכים לנקוט פעולה אקטיבית כדי להביע את סירובו לשימוש במידע אישי על אודותיו) לקבלת הסכמה אינו מקובל, וכן שהישענות על הסכמה כבסיס חוקי לעיבוד מידע צריכה להיעשות במשורה, משום שעל בעל השליטה להביא בחשבון שנושא המידע יכול לחזור בו מהסכמתו בכל עת, ולכן הוא לא יוכל להמשיך ולעבד את המידע האישי שלו, אלא אם כן יש בסיס חוקי אחר שעליו הוא יוכל להישען לשם הצדקת עיבוד המידע.[39] נוסף על כך, עוגנו ב־GDPR הוראות לניהול סיכונים והערכתם טרם עיבוד מידע. בעל שליטה במידע נדרש לערוך תסקיר השפעה על הפרטיות בנסיבות מסוימות, לתעד את פעולותיו, ובתנאים מסוימים למנות ממונה הגנת פרטיות.[40] ה־GDPR גם מעגן את עקרון "העיצוב לפרטיות" (Privacy by Design, שלפיו יש לעצב את מערכות המידע להגנה הולמת על הזכות לפרטיות כבר משלב התכנון המוקדם של המערכות ולאורך כל מחזור החיים של איסוף המידע האישי

35 GDPR, לעיל ה"ש 33, בסעיף 20.

36 שם, בסעיף 17.

37 שם, בסעיף 22.

38 דירקטיבת הגנת המידע, לעיל ה"ש 34, בסעיפים 7 ו־8(2).

39 GDPR, לעיל ה"ש 33, בסעיפים 4(11), 6, 7.

40 שם, בסעיפים 35, 30 ו־37–39.

ועיבודו באמצעותן),[41] מטיל חובת דיווח על פרצת אבטחה,[42] ומסמיך את רשויות הגנת הפרטיות המדינתיות להטיל קנסות כבדים במקרה של הפרה.[43] לבסוף, התחולה האקס־טריטוריאלית של ה־GDPR ודרישת התאימות לשם התרת עיבוד מידע של אזרחי האיחוד האירופי על ידי גופים מחוץ לתחומי האיחוד, הובילו למה שמכונה "אפקט בריסל". באמצעות אפקט בריסל האיחוד האירופי משפיע ומעצב את רגולציית דיני הגנת המידע ברחבי העולם ברוח ה־GDPR.[44] כך, למשל, ביפן עודכן חוק הגנת המידע האישי בשנת 2020, כדי לזכות בהכרה בתאימות הדין ביפן לדין הנוהג באיחוד האירופי בכל הקשור בהגנת מידע אישי.[45] גם דרום קוריאה תיקנה בשנת 2020 את חוק הגנת הפרטיות שלה כדי לזכות בתאימות,[46] ובאותה שנה חוקקה קליפורניה שבארצות הברית חוק הגנת פרטיות במידע ברוח ה־GDPR.[47]

במכון הישראלי לדמוקרטיה זיהינו את הוואקום שנוצר בחקיקת הגנת הפרטיות במדינת ישראל, ובשנת 2016 הקמנו צוות של מומחים מהאקדמיה, מהתעשייה, מהחברה האזרחית ושל נציגים מהמגזר הציבורי כדי לעסוק בנושא. על בסיס עבודת הצוות הזה, בשנת 2019 פרסמנו הצעת חוק חדשה להגנת פרטיות במדינת ישראל. ההצעה משקפת את הלקחים שאפשר ללמוד מניסיונן של מדינות אחרות, בעיקר באיחוד האירופי, מאזנת בין הגנה על פרטיות לבין

41 שם, בסעיף 25.

42 שם, בסעיפים 33–34.

43 שם, בסעיפים 77–84.

44 Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford Univ. Press 2019)

45 Act on the Protection of Personal Information (Act No. 57 of May 30, 2003)

46 Personal Information Protection Act (Act No. 16930 of Feb. 4, 2020) (S. Korea)

47 California Consumer Privacy Act of 2018 (Cal. Civ. Code §1798.100 et seq.) (2018); California Privacy Rights Act of 2020 (Cal. Civ. Code §1798.100 et seq.) (2020) (להלן: CCPA).

חדשנות טכנולוגית בתחום עיבוד המידע האישי, ומקדמת תיקון מקיף לחוק הגנת הפרטיות הישראלי.[48] הצעתנו שימשה בסיס עיקרי להצעתו של ח"כ קריב לתיקון חוק הגנת הפרטיות ב־2022,[49] וסייעה בהבנת התיקונים הדרושים בחלק מהדיונים בוועדת החוקה בתיקון 13.

תיקון 13, שנכנס לתוקפו באוגוסט 2025 לאחר ציפייה דרוכה בציבור ובתעשייה, הוא אבן דרך חשובה בהתפתחותה ובשיפורה של הגנת הפרטיות במדינת ישראל.[50] התיקון כולל תיקונים נחוצים לחוק הגנת הפרטיות המיושן, ועם זאת, הוא אינו התיקון המלא והנחוץ לחוק הגנת הפרטיות, והחוק נותר חסר לעומת חקיקת הגנת הפרטיות במידע המקובלת במישור הבינלאומי ברוח ה־GDPR.

חקיקתו של תיקון 13 בוועדת החוקה ארכה כשמונה חודשים והשתתפו בה כמה שחקני מפתח, לרבות ועדת החוקה עצמה, מחלקת ייעוץ וחקיקה במשרד המשפטים, הרשות להגנת הפרטיות, גופים ביטחוניים וגופי אכיפת החוק, השלטון המקומי, החברה האזרחית, ועורכי דין מהמגזר הפרטי ומהתעשייה. צלילה לשיח בין נציגיהם של שלל גורמי המפתח במהלך הדיונים בוועדת החוקה, שברובם ככולם השתתפתי, מלמדת על המניעים המרכזיים של כל אחד מהשחקנים ושופכת אור על הקשיים שהתעוררו במהלך החקיקה ושחלקם מלווה את תיקון 13 גם עתה. למשל, מחלקת ייעוץ וחקיקה במשרד המשפטים עמדה על כך שיחקק תיקון חלקי לחוק הגנת הפרטיות, בציפייה ובהבטחה שתיקון עתידי לדין המהותי מחכה מעבר לפינה. הרשות להגנת הפרטיות התמקדה בעיקר בעיגונן של סמכויות אכיפה ופיקוח חשובות במהירות, כדי למלא את משימותיה גם במציאות של חוק חסר. לעומת זאת, ועדת החוקה שאפה לתקן תיקון שיקרב, עד כמה שאפשר, את דיני הגנת המידע בישראל לדינים הנהוגים באיחוד האירופי ובמדינות נוספות בעקבות אפקט בריסל, מתוך הבנת כובעה

48 רחל אריאדור הרשקוביץ ותהילה שורץ אלטשולר **הצעת חוק הגנת הפרטיות, התשע"ט־2019** (המכון הישראלי לדמוקרטיה 2019).

49 הצעת חוק הגנת הפרטיות (תיקון – חיזוק הזכות לפרטיות וההגנה עליה), התשפ"ג־2022.

50 תיקון 13, לעיל ה"ש 3.

הכפול של הרשות להגנת הפרטיות – רגולטור של המגזר הציבורי ושל המגזר הפרטי – ומתוך חשש מפני חולשתה של הרשות להגנת הפרטיות מול המגזר הציבורי. כמו כן, ועדת החוקה שמה דגש על הגנה על עסקים ישראליים בינוניים וקטנים מפני נטל רגולטורי שלא יוכלו לעמוד בו.

מטרת המסמך הזה היא להפנות זרקור להליך החקיקה, שכן הבנתו נחוצה לשם התווית גבולות הפרשנות הנאותה של הוראות תיקון 13 ושל סמכויות הנתונות מעתה לרשות להגנת הפרטיות. המסמך נועד לספק לעוסקים בתחום כלים להבנה מהותית של החוסרים שנותרו בהגנה על הזכות לפרטיות בישראל על בסיס הליך החקיקה עצמו, וכן לבחון בעין ביקורתית את השלכות תיקון 13, ולגבש תובנות בעניין תיקונים הנוספים הנחוצים לחוק הגנת הפרטיות. פרק 1 סוקר בקצרה את ההיסטוריה החקיקתית של תיקון 13, את מטרותיה של הצעת החוק הממשלתית,[51] ואת הנושאים המרכזיים שבהם התמקדה; פרק 2 מתמקד בכמה תיקונים עיקריים בתיקון 13 שיש בהם כדי לספק תובנות בעניין גבולות ההגנה על הזכות לפרטיות בישראל, ופרק 3 מספק מבט צופה פני עתיד על הנושאים שעדיין יש לתקן בחוק הגנת הפרטיות כדי לשפר מהותית את ההגנה על הזכות לפרטיות של אזרחי ישראל. פרק 4 מספק הסתכלות ממעוף הציפור על הליך החקיקה ועל התובנות שאפשר ללמוד ממנו.

אני מודה לצוות ההוצאה לאור של המכון הישראלי לדמוקרטיה על עבודתם המסורה בהוצאת מחקר זה לאור. תודה לד"ר תהילה שוורץ אלטשולר, לד"ר דנה בלאנדר, לעו"ד נעמה מנחמי ולעו"ד איה מרקביץ על הערותיהן מאירות העיניים.

51 הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב–2022, הצעות חוק הממשלה – 1496, ג' בשבט התשפ"ב, 5.1.2022 (להלן: הצעת החוק הממשלתית).

פרק 1

תיקון 13 - מטרות והיסטוריה חקיקתית

תיקון 13 מבוסס על הצעת חוק ממשלתית משנת 2011, שנועדה בזמנו לשפר את יכולות הפיקוח והאכיפה של ראש הרשות להגנת הפרטיות, על בסיס המלצותיה של ועדת שופמן מ־2007[52] והלקחים שהתווספו מאז לנוכח פעולתה של הרשות להגנת הפרטיות וההתפתחויות הטכנולוגיות.[53]

בשנת 2011, בעת הצגת תיקון 12 בוועדת החוקה, הסבירה עו"ד אורית קורן, אז המשנה ליועץ המשפטי לממשלה במשרד המשפטים, כי במשרד המשפטים שואפים לתקן חלקים נוספים בחוק הגנת הפרטיות, כדי לשפר ולעדכן את הטיפול במידע אישי במאגרי מידע. אחד החלקים האלה, שלדבריה באותה העת קודם על ידי משרד המשפטים, נוגע לצמצום חובת הרישום והחלפתה במקרים מסוימים בחובה לקיום סדרי ניהול וכללי עבודה בתוך הגוף השולט במאגר המידע, לצד קביעת חובות אבטחת מידע מפורטות. יו"ר ועדת החוקה דאז, ח"כ דוד רותם, סבר שעדיף להביא את כל התיקונים יחד וליצור קודקס אזרחי, ואף העיר כבר אז, ביוני 2012, ש"יש לכם אומנות איך למשוך חוקים במשך שנים".[54] נבואה שנדמה שהגשימה את עצמה.

באותו הדיון הסביר ראש הרשות להגנת הפרטיות דאז, עו"ד יורם הכהן, את מצבה הסבוך והעגום של הרשות. לדבריו הרשות מתמודדת עם גופים רבים ורבי עוצמה, מהמגזר הציבורי ומהמגזר הפרטי, המעבדים היקפים אדירים של מידע אישי בעזרת רגולציה ארכאית משנת 1981, ולכן נדרש לשיטתו עדכון סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות כמוצע בתיקון 12. עוד ציין עו"ד

52 משרד המשפטים, הצוות לבחינת החקיקה בתחום מאגרי המידע – דין וחשבון (ינואר 2007) (להלן: ועדת שופמן).

53 הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2011 (להלן: תיקון 12).

54 פרוטוקול מס' 633 מישיבת ועדת החוקה, חוק ומשפט, יום רביעי, ל' בסיון התשע"ב (20 ביוני 2012), בעמ' 3–4.

הכהן, כי לשיטת הרשות יש לקדם מעבר מחובות פורמליות, כגון חובת הרישום, לחובות מהותיות של ניהול תקין שבבסיסן תפיסת העיצוב לפרטיות לאורך כל מחזור חייו של המידע האישי.[55] בבואנו לבחון את עמדותיה של הרשות להגנת הפרטיות לאורך הליך חקיקת תיקון 13 יש לזכור כי דבריו של עו"ד הכהן הם תיאור מדויק למדי של סמכויות הרשות להגנת הפרטיות לפי החקיקה שהייתה תקפה ערב תיקון 13.

נוסף על כך, כבר אז, בדיון על תיקון 12, הצביעו יו"ר ועדת החוקה, ח"כ רותם, וח"כ דאז יצחק הרצוג על החשש שלרשות להגנת הפרטיות לא עומדות סמכויות אכיפה וענישה אפקטיביות מול גופי ממשל, אף שגופים אלו מחזיקים במידע אישי ורגיש רב, והמדינה אף כונתה בוועדת החוקה אז "המדליפה הכי הגדולה".[56] כפי שנראה בהמשך, חשש דומה הביע יו"ר ועדת החוקה, ח"כ שמחה רוטמן, גם בהליכי החקיקה של תיקון 13.[57]

הכנסת ה־18 התפזרה באוקטובר 2012, ומשום כך לא התגבש תיקון 12 לחוק. בתחילת 2018 הניחה הממשלה על שולחן הכנסת ה־20 את הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018 (להלן: תיקון 13 מ־2018). תיקון 13 מ־2018 התבסס רובו ככולו על תיקון 12, למעט הוספת פרק העוסק בפיקוח ובירור מינהלי בגופים ביטחוניים.[58] הכנסת ה־20 התפזרה בדצמבר 2018 וועדת החוקה כלל לא הספיקה לדון בו.

55 שם, בעמ' 4, 6, 13–14.

56 שם, בעמ' 15–17, 28–29.

57 פרוטוקול מס' 223 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ח בטבת התשפ"ד (9 בינואר 2024), בעמ' 115, דברי יו"ר ועדת החוקה, ח"כ רוטמן; פרוטוקול מס' 233 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, י"א בשבט התשפ"ד (21 בינואר 2024), בעמ' 43, דברי ח"כ רוטמן.

58 הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018 (להלן: תיקון 13 מ־2018), דברי ההסבר בעמ' 693.

במחצית השנייה של 2020 פרסם משרד המשפטים את תזכיר חוק הגנת הפרטיות (תיקון מס') (הגדרות וצמצום חובת הרישום), התש"ף–2020 (להלן: תזכיר חובת רישום). תזכיר זה מבוסס על תזכיר דומה שפרסם משרד המשפטים ב־2012, אך לא הבשיל להצעת חוק.[59] תזכיר חובת רישום לא עסק בסמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות, אלא התמקד בצמצום חובת הרישום כדי למקד את פעולות האכיפה של הרשות להגנת הפרטיות במאגרים המאיימים על הזכות לפרטיות. כן נועד תזכיר חובת רישום להתאים את ההגדרות הקבועות בחוק הגנת הפרטיות והנוגעות למידע אישי להתפתחויות הטכנולוגיות, החברתיות והמשקיות שהתפתחו מאז נחקק, וכן להסדרים בינלאומיים מודרניים הקיימים בעולם, ובראשם ה־GDPR. משרד המשפטים חזר בתזכיר חובת רישום על עמדתו המכירה אומנם בצורך לתקן את חוק הגנת הפרטיות, אך מתעקשת על חקיקתו בשלבים נפרדים. כך צוין בתזכיר כי –

> בחודשים הקרובים, בכוונת משרד המשפטים לפרסם תזכיר חוק נוסף שישלים את מהלך התיקון המהותי הנדרש לשם עדכון החוק הקיים והתאמתו למציאות בת זמננו. תיקון זה צפוי לכלול סוגיות מהותיות כגון הרחבה של הבסיסים המשפטים המותרים לעיבוד מידע, מעבר להסכמה והסמכה בחיקוק, הרחבה ועדכון של רשימת הזכויות המוקנות לנושאי המידע והסדרים המשקפים אחריותיות של בעל מאגר ומחזיק. דחיית הסדרתן של סוגיות אלה לתזכיר נוסף ונפרד נובעת מן המורכבות הרבה שלהן, המחייבת איזון עדין בין אינטרסים וזכויות, ומחוסר הרצון לעכב את קידום שאר הצעות החוק הדחופות והבשלות שעל הפרק.[60]

ידיעות על קיומו של "תזכיר חוק נוסף", "תיקון 15" בפי נציגי מחלקת ייעוץ וחקיקה במשרד המשפטים והרשות להגנת הפרטיות, והתפיסה שיש לדון בו

59 תזכיר חוק הגנת הפרטיות (תיקון מס') (צמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב–2012.

60 תזכיר חוק הגנת הפרטיות (תיקון מס') (הגדרות וצמצום חובת הרישום), התש"ף–2020.

בנפרד, נשמעו גם במהלך הדיונים בוועדת החוקה בתיקון 13.[61] אולם, לצערי, עד לכתיבת שורות אלו תזכיר חוק מקיף טרם פורסם לציבור.

הצעת החוק הממשלתית שגובשה לבסוף לכדי תיקון 13 (להלן: הצעת החוק הממשלתית), שילבה את תזכיר חובת רישום ואת תיקון 13 מ־2018 (המבוסס, כאמור, ברובו על תיקון 12 מ־2011). מטרותיה של הצעת החוק הממשלתית שיקפו את השילוב הזה ואת שאיפת משרד המשפטים להתאים את חוק הגנת הפרטיות המיושן מ־1981 לאתגרים ולסכנות העכשוויות בהגנה על מידע אישי. הצעת החוק הממשלתית נועדה לשפר את יכולות הפיקוח והאכיפה של הרשות להגנת הפרטיות, לצמצם את היקף חובת הרישום, ולהתאים את הגדרות המונחים הקשורים להגנה על מידע אישי ממוחשב להתפתחויות טכנולוגיות, חברתיות, משקיות ומשפטיות בתחום בארץ ובעולם.[62] במובן זה הייתה הצעת החוק הממשלתית רזה למדי. אולם במהלך הדיונים בוועדת החוקה, ועל פי דרישותיה, הוספו להצעת החוק הממשלתית נושאים לא מעטים, עד שהתגבשה לכדי תיקון 13.

עם זאת, חשוב להבהיר כי תיקון 13 הותיר את הדואליות של חוק הגנת הפרטיות בישראל בעינה – בפרק א הוא מאסדר את נושאי הפרטיות הקלאסית ובפרק ב את הפרטיות המידעית.

פיצול זה, לצד העובדה שבתיקון 13 אין הוראות מהותיות בנוגע לבסיסים חוקיים לעיבוד מידע אישי, מוביל להותרת ההישענות, שהייתה מקובלת עד כה, על ההוראות מפרק א, מעולם הפרטיות הקלאסית, לשם התווית גבולות המותר והאסור בעולם הפרטיות המידעית המודרנית. כך, עיבוד מידע אישי מותר כל עוד הוא אינו עולה כדי אחד ממופעי הפגיעה בפרטיות המפורטים בסעיף 2 בחוק הגנת הפרטיות, המשקפים בעיקרם את עולם הפרטיות הקלאסית,

61 ראו, למשל, פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 57, דברי עו"ד יוסוב עמיר; עמ' 112, דברי עו"ד אידלמן בתגובה לדיון בנושא הזכות להישכח; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 8–9, 12–13, דברי עו"ד יוסוב עמיר.

62 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר, בעמ' 420.

ודי בהסכמתו מדעת של נושא המידע כדי לעבד מידע שהוא בבחינת "פגיעה בפרטיות". אם נעשה עיבוד מידע שאינו עולה כדי "פגיעה בפרטיות", ובהקשר הזה מדובר בנסיבות מצומצמות מאוד לנוכח הפרשנות המרחיבה שניתנה לסעיף 2 לחוק הגנת הפרטיות, המונה את מופעי הפגיעה בפרטיות, לא נדרשת כלל הסכמת נושא המידע.[63] הותרת דואליות זו בעינה, בלי לעדכן את ההוראות המהותיות בנוגע לבסיסים החוקיים לעיבוד מידע אישי וליצור אסדרה מקיפה של הזכות לפרטיות מידעית, עוררה קשיים וחששות לאורך כל הליך חקיקת תיקון 13 ומשפיעה אף על פרשנותו של התיקון ועל השלכותיו.

63 סעיפים 1 ו־2 לחוק הגנת הפרטיות, לעיל ה"ש 3.

פרק 2

החידושים העיקריים בתיקון 13 לעניין הרחבת תחולת חוק הגנת הפרטיות

תחולת חוק הגנת הפרטיות נדמית למסע בין שלושה שערים שרק העובר בשלושתם ייכנס לעולם חוק הגנת הפרטיות ויהיה חייב לציית להוראותיו. תיקון 13 אינו משנה את אסטרטגיית שלושת השערים, אולם הוא מרחיב מאוד כל אחד ואחד מהם על ידי שינוי המונחים המרכיבים אותם, כפי שיפורט להלן.

2.1. השער הראשון: הגדרת "מידע אישי" ו"ידיעה על ענייניו הפרטיים של אדם"

"מידע" הוגדר בחוק הגנת הפרטיות לפני תיקון 13 בצמצום – מעין רשימת מכולת של סוגי מידע מסוימים שתוכנם נחשב "אישי" במיוחד ועל כן ראוי להגנה:

> "מידע" – נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו;[64]

בהצעת החוק הממשלתית הוצע להחליף הגדרה זו בהגדרה הזאת:

> "מידע" – נתון הנוגע לאדם מזוהה, או לאדם הניתן לזיהוי, במישרין או בעקיפין, באמצעים סבירים, לרבות מזהה ביומטרי, מספר זהות או כל נתון מזהה ייחודי אחר;[65]

64 סעיף 7 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

65 סעיף 3(3) להצעת החוק הממשלתית, לעיל ה"ש 51, המתקן את סעיף 7 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

בדיונים בוועדת החוקה הסכימו מרבית הנוכחים מהמגזר הפרטי והציבורי שהגדרה רחבה של המושג "מידע" באמצעות הביטוי "ניתן לזיהוי" רצויה ואף תואמת את ההגדרה המקובלת באיחוד האירופי.[66] הגדרה זו משקפת נכונה את ההבנה שבעידן נתוני העתק והיכולות הטכנולוגיות המתקדמות להצלבת נתונים, עשויות פיסות מידע המקובצות יחד להביא לזיהויו של אדם. נטען כי ההגדרה הרחבה תחייב בעלי שליטה במאגרי מידע לבחון בכובד ראש שימוש שהם מבקשים לעשות במידע אישי. עם זאת, לצד תמימות הדעים בדבר הצורך בהגדרה רחבה של המונח "מידע", התעורר חששה של ועדת החוקה, וגם של כמה עורכי דין מהמגזר הפרטי, מפני הרחבת יתר של תחולת חוק הגנת הפרטיות, שתביא בסופו של דבר לזילות הגנת הפרטיות. הדרך הטובה ביותר להתמודד עם חשש זה, העירו עורכי הדין, היא לתקן את הדין המהותי בחוק הגנת הפרטיות ולהטיל אחריות ברורה ומדורגת על בעלי שליטה במידע להגנת הפרטיות, על פי סוג המידע שהם מחזיקים, רגישותו והיקפו.[67]

לפיכך, כדי להגביר את התאימות להוראות ה־GDPR ולספק דוגמאות למשמעות שיש לצקת לנתון שיאפשר את זיהוי של אדם במאמץ סביר, הוספה להגדרת "מידע" בהצעת החוק הממשלתית רשימה פתוחה של נתונים שייחשבו נתון המאפשר את זיהוי של אדם במאמץ סביר.[68] כך אומצה בתיקון 13 ההגדרה הזאת ל"מידע אישי":

66 GDPR, לעיל ה"ש 33:

> "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

67 פרוטוקול מס' 197 מישיבת ועדת החוקה, חוק ומשפט, יום שני, כ"ח בכסלו התשפ"ד (11 בדצמבר 2023), בעמ' 6–8, דברי יו"ר ועדת החוקה, ח"כ רוטמן, עו"ד שגיא, עו"ד אתגר וד"ר רחום־טוויג.

68 שם, בעמ' 28–30.

> נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי;[69]

זאת ועוד, קריאת כיוון לפרשנות הגדרת "מידע אישי" בתיקון 13 אפשר לשאוב מההגדרה המקבילה ב־GDPR. ב־GDPR הובהר שיש להביא בחשבון את כל האמצעים שסביר שבעל השליטה במידע או כל אדם אחר יעשה בהם שימוש בניסיון להצליב נתונים ולהביא לזיהויו, במישרין או בעקיפין, של אדם מסוים. סבירות השימוש תיבחן מתוך שימת לב לעלות האמצעי, משך הזמן הנדרש לשם הזיהוי, הטכנולוגיה הזמינה, לציבור או רק לבעל השליטה במידע, בעת עיבוד המידע, וכן להתפתחויות טכנולוגיות הצפויות במהלך כל משך חיי המידע, כלומר לאורך כל התקופה שבה המידע עתיד להיות מעובד.[70] מאחר שעיבוד כולל גם אחסון המידע, המדובר למעשה בהגדרה צופה פני עתיד, על פי משך הזמן שבו תכנן בעל השליטה במידע לאחסן את המידע. נוסף על כך, בבחינת סבירות מאמצי הזיהוי יש להביא בחשבון גם את מטרת עיבוד המידע ואת אופן העיבוד. אם אי אפשר להשיג את מטרת עיבוד המידע בלי לזהות זיהוי כלשהו את נושאי המידע, סביר להניח שבידי מעבד המידע או בעל השליטה בו יהיו האמצעים הסבירים לזיהויו של אדם. הגוף האמון באיחוד האירופי על הפרשנות של הוראות ה־GDPR הציג כמה דוגמאות לכך.[71] למשל, מידע הנאסף באמצעות טכנולוגיית מעקב וידאו אינו מידע מזהה כשלעצמו, וזיהוי על בסיסו נעשה בנסיבות מצומצמות בלבד. אולם, מטרת השימוש בטכנולוגיה למעקב בווידאו היא זיהויו של אדם בנסיבות מסוימות, למשל בעת ביצוע עבירה. משום כך, המידע הנאסף באמצעות טכנולוגיה למעקב בווידאו צריך להיחשב מידע ניתן

69 סעיף 2(5) לתיקון 13, לעיל ה"ש 3, המתקן את סעיף 3 בחוק הגנת הפרטיות.

70 GDPR, לעיל ה"ש 33, Recital 26

71 Article 29 Data Protection Working Party לדירקטיבת הגנת המידע האירופית, לעיל ה"ש 33. עם כניסת ה־GDPR, לעיל ה"ש 33, לתוקף הוחלף גוף זה ב־European Data Protection Board (EDPB), שמונה לפי סעיף 68 ל־GDPR.

לזיהוי. דוגמה נוספת עסקה במאגר מידע של חברת תחבורה ציבורית שכלל מידע על ציורי גרפיטי המופיעים על כלי התחבורה שברשותה. מאגר המידע כלל גם את הסימן הייחודי שיוצר הגרפיטי הטביע עליו. הסימן כשלעצמו אינה מזהה, אולם חברת התחבורה מחזיקה את מאגר המידע במטרה להצליח ביום מן הימים לזהות את האדם האחראי לריסוס הגרפיטי המזיק. כלומר, חברת התחבורה עצמה צופה שבעתיד המידע יהיה בר זיהוי . משום כך, לפי הפרשנות שניתנה באיחוד האירופי, יש לראות בנתונים על אודות ציור הגרפיטי עצמו, נסיבות ביצועו והסימן הייחודי שהוטבע בו, כאל מידע ניתן לזיהוי, כלומר "מידע אישי" שהוראות ה־GDPR חלות עליו. כמו כן, בבחינת סבירות המאמץ לזיהוי חוזר יש לתת את הדעת לאמצעים הטכנולוגיים והארגוניים שננקטו, אם ננקטו, כדי למנוע זיהוי.[72]

במהלך הדיונים בוועדת החוקה בהגדרת "מידע אישי" ובשאלת מבחן המאמץ הסביר לזיהוי, התעוררה גם שאלת תחולת הגדרת "מידע" בחוק הגנת הפרטיות על מידע מותמם ועל פעילות ההתממה עצמה.[73] הנושא לא הוכרע בוועדת החוקה, אך בשל חשיבותו יש מקום להתעכב עליו בכל זאת. הרשות להגנת הפרטיות הגדירה שהתממה (או "עילום נתונים") היא "הסרת מאפיינים או שינוי ערכים על מנת לצמצם או למנוע זיהוי של נושא המידע".[74] לכאורה, הגדרה זו של הרשות להגנת הפרטיות מסתפקת בצמצום בלבד של אפשרות הזיהוי החוזר. עם זאת, יש לקרוא אותה במשולב עם הגדרת "מידע אישי". כלומר, שהיא כוללת בתוכה את מבחן הזיהוי הסביר. פרשנות זו גם תואמת את הגדרת מידע מותמם ב־GDPR. ה־GDPR אינו מציין שיטת התממה מסוימת, אך מדגיש שמידע מותמם הוא מידע מזהה שעובד והפך לבלתי ניתן לזיהוי לצמיתות ובאופן בלתי

72 Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP136 (Adopted June 20, 2007), 15-17

73 פרוטוקול מס' 197, לעיל ה"ש 67, עמ' 8-10.

74 הרשות להגנת הפרטיות, מדריך לטכנולוגיות מגבירות – פרטיות (23 בפברואר 2025).

הפיך.[75] גם ה־CCPA בקליפורניה אינו מסתפק בצמצום הסיכון לזיהוי חוזר אלא מגדיר מידע בלתי ניתן לזיהוי (deidentified) – מידע שאי אפשר לעשות בו שימוש סביר כדי להסיק ממנו מידע על או מידע המקושר בדרך כלשהי לנושא המידע, ובלבד שהארגון המעבד את המידע (1) נוקט אמצעים סבירים להבטיח שלא יהיה אפשר לקשר את המידע עם נושא המידע; (2) מתחייב בציבור שיחזיק ויעשה שימוש במידע בפורמט הבלתי ניתן לזיהוי שלו ולא ינסה לזהות את נושאי המידע (פרקטיקה המכונה זיהוי חוזר), אלא אם כן מטרת הזיהוי החוזר היא לקבוע אם הליך הסרת המזהים עומד בדרישות החוק; (3) חייב חוזית כל צד שלישי המקבל ממנו את המידע לציית להוראות אלו.[76]

גם חוזר מנכ"ל משרד הבריאות בנושא שימוש שניוני במידע בריאות משנת 2018 הגדיר "התממה" – "תהליך להפחתת הסיכון לזיהוי הפרט מתוך מידע בריאות [...]". כלומר, ההגדרה נותנת את הדעת למבחן סבירות הזיהוי החוזר. נוסף על כך, "מידע ניתן לזיהוי" מוגדר – "מידע בריאות ללא פרטים המזהים באופן חד־חד ערכי אדם, אך העשוי להביא לזיהוי מחדש של אדם באמצעות שימוש באמצעים סבירים או במידע אחר, הזמינים לציבור הרחב". הגדרה זו אף תוחמת את מבחן המאמץ הסביר בגבולות האמצעים הקיימים בידי הציבור ואינה מרחיבה את המבחן, כמו GDPR, לאמצעי סביר שבידי גורם כלשהו, אף אם אין מדובר בטכנולוגיה הזמינה לציבור הרחב.[77] צמצום זה עשוי לתת מענה לביקורת שלפיה מבחן המאמץ הסביר לזיהוי חוזר רחב מידי ויוביל להחשבת כל פריט מידע מותמם למידע אישי מזוהה.

לצד סוגיות אלו יש לתת את הדעת גם לביטוי "ידיעה על ענייניו הפרטיים של אדם" המופיע בסעיף 2(9) לחוק הגנת הפרטיות. לנוכח שימור המודל הדואלי של חוק הגנת הפרטיות בישראל והיעדר תיקון של הדין המהותי בכל הקשור לבסיסים חוקיים לעיבוד מידע, נותר ביטוי זה רלוונטי גם לעיבוד

75 סעיף הקדמה 26 ל־GDPR, לעיל ה"ש 33.

76 CCPA, לעיל ה"ש 47, בסעיף 1798.140(m).

77 משרד הבריאות, חוזר המנהל הכללי, נושא: שימושים משניים במידע בריאות, א' בשבט תשע"ח, 17 ינואר 2018, מס' 1/2018, בסעיפים 4.5–4.7.

מידע לאחר תיקון 13. בפסיקה פורש הביטוי "ידיעה על ענייניו הפרטיים של אדם" בהרחבה, אם כי פרשנות מרחיבה זו לא נעשתה בנסיבות של מאגרי מידע דיגיטליים.[78] נוסף על כך, פרשנות מרחיבה זו ניתנה לפני שהרשות להגנת הפרטיות החזיקה בסמכויות פיקוח ואכיפה מינהלית המוענקות לה בתיקון 13. עתה, כשבידה סמכויות אכיפה מינהלית, עשויה הרשות להגנת הפרטיות לפרש את המונח "ידיעה על ענייניו הפרטיים של אדם" בהרחבה, להטיל קנסות מינהליים ולמנוע פעולות עיבוד מידע רבות. לפי עמדת משרד המשפטים, אין פער של ממש בין המונח "מידע אישי" לביטוי "ענייניו הפרטיים של אדם". ועדת החוקה הסכימה עקרונית לפרשנות זו, אולם חשוב לתת את הדעת להערת יו"ר הוועדה, ח"כ רוטמן, בעניין זה. לדבריו, נוכח אימוץ ההגדרה הרחבה ל"מידע אישי" בתיקון 13 והייחוד לכאורה של סעיף 2(9) לנושא הפרטיות הקלאסית, יש לאמץ מעתה פרשנות מצומצמת ביותר ותלוית הקשר לביטוי "ענייניו הפרטיים של אדם":[79]

> לדעתי הפרשנות של המושג ידיעה על ענייניו הפרטיים של אדם [...] וזה באמת תלוי הקשר [...] מצד אחד. מצד שני צריך להיזהר שזה לא יהיה כחומר ביד היוצר, בוודאי כל המקומות שמפנים ל־2(9) [...] אני חושב שידיעה על ענייניו הפרטיים של אדם [...] צריכה להיות הרבה יותר צרה בהרבה מאד הקשרים.[80]

78 פרשת **ונטורה**, פסק הדין המוביל בפרשה, עסקה ברישומו של מאגר מידע ובו מידע על המחאות, שטרות והתחייבויות שלא כובדו, כדי להפיצו בקרב בעלי עסקים. רשם מאגרי המידע סירב לרשום את מאגר המידע בנימוק שמדובר בפגיעה בפרטיות לפי סעיף 2(9) לחוק הגנת הפרטיות. נפסק שיש לפרש את הביטוי "ענייניו הפרטיים של אדם" שבסעיף 2(9) לחוק הגנת הפרטיות, לעיל ה"ש 3, בהרחבה, על פי מובנם הטבעי והרגיל – "כל מידע הקשור לחייו הפרטיים של אותו אדם, לרבות שמו, כתובתו, מספר הטלפון שלו, מקום עבודתו, זהות חבריו, יחסיו עם אשתו ויתר חברי משפחתו וכדומה". ראו ע"א 439/88 **רשם מאגרי מידע נ' משה ונטורה**, פ"ד מח(2) 808, בעמ' 820–822.

79 פרוטוקול מס' 197, ה"ש 67 לעיל, בעמ' 31–35, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

80 שם, בעמ' 32, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

לצד תיקון הגדרת "מידע אישי", תיקון 13 יוצר שינוי מהותי בכל הקשור לקטיגוריות מיוחדות של מידע אישי בנושאים הנחשבים רגישים מבחינת נושא המידע. כמו דעה פוליטית או מצבו הבריאותי, הפיזי או הנפשי, של אדם. השינוי בתיקון 13 לא התמצה רק בשינוי המונח עצמו מ"מידע רגיש" בחוק הגנת הפרטיות[81] ל"מידע בעל רגישות מיוחדת" בתיקון 13.[82] תיקון 13 מרחיב את קטיגוריות המידע הנחשבות "מידע בעל רגישות מיוחדת". עם זאת, אין באפיון ש"מידע אישי" הוא "מידע בעל רגישות מיוחדת" כדי להשפיע על תחולת חוק הגנת הפרטיות. יתרה מזו, בהיעדר תיקונים מהותיים לחוק הגנת הפרטיות, נפקות הרחבת הגדרת "מידע בעל רגישות מיוחדת" מצומצמת. היא עדיין בעלת חשיבות לתחולתן של מגוון חובות, כגון חובת מסירת ההודעה,[83] חובות מכוח תקנות אבטחת מידע,[84] וגובה העיצומים הכספיים שתוכל הרשות להגנת הפרטיות להטיל בגין הפרות שונות.[85] משום כך לא מצאתי לנכון לעסוק במסמך זה במהות הקטיגוריות של "מידע בעל רגישות מיוחדת".

81 ראו סעיף 7 לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1, הגדרת "מידע רגיש".

82 סעיף 2(5) בתיקון 13, לעיל ה"ש 3, המתקן את סעיף 3 בחוק הגנת הפרטיות הגדרת "מידע בעל רגישות מיוחדת".

83 סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א(ב) לחוק הגנת הפרטיות.

84 תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: תקנות אבטחת מידע). במהלך הדיונים בתיקון 13 הובהר שיבוצעו התאמות בתקנות אבטחת מידע כדי להבטיח את תאימותן לתיקון 13 בכל הקשור להגדרת מידע בעל רגישות מיוחדת. ראו פרוטוקול מס' 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ד בטבת התשפ"ד (26 בדצמבר 2023), בעמ' 58.

85 פרוטוקול מס' 203 מישיבת ועדת החוקה, חוק ומשפט, יום שני, ו' בטבת התשפ"ד (18 בדצמבר 2023), בעמ' 3.

2.2. השער השני: הגדרת "מאגר מידע"

"מאגר מידע" הוא השער השני שהנכנס בו מגדיל את סיכוייו לחוב בהוראות חוק הגנת הפרטיות. בחוק הגנת הפרטיות לפני לתיקון 13 הוגדר "מאגר מידע" כך:

> אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –
>
> (1) אוסף לשימוש אישי שאינו למטרות עסק; או
>
> (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

גם על פי הצעת החוק הממשלתית הגדרת "מאגר המידע" היא שער כניסה שני לתחולת חוק הגנת הפרטיות, אם כי בתיקונים מסוימים. בטרם אעמוד על התיקונים, חשוב להבין שבעולם הפרטיות המידעית כל ארגון, פרטי או ציבורי, עוסק בעיבוד נתונים, לרבות מידע אישי, ומאגד אותם באופנים שונים על פי צרכיו ומטרות העיבוד. אולם, הותרת הביטוי "מאגר מידע" כתנאי לתחולת הוראות חוק הגנת הפרטיות היא ארכאית, אינה תואמת את משטר הגנת הפרטיות המקובל בעולם,[86] ואף מובילה לצמצום החשיבות והמשמעות שיש בהרחבת הגדרת "מידע אישי". יתרה מזו, הותרתה בעינה פוגעת בהגנה על מידע אישי כשלעצמו, בין שהוא חלק ממאגר מידע, בין לאו,[87] ועשויה לאפשר

86 למשל, חוקי הגנת המידע באיחוד האירופי, באוסטרליה, בסינגפור ובקליפורניה אינם כוללים כלל הגדרה של המונח "מאגר מידע" (dataset). ראו GDPR, לעיל ה"ש 33; Privacy Act 1988 (Cth) (Austl.); Personal Data Protection Act 2012, No. 26 of 2012 (Sing.); CCPA, לעיל ה"ש 47, בסעיף 1798.100–1798.199. הגדרת המונח "personal information bank" בקנדה היא אוסף או מקבץ של מידע אישי המצוי בידי משרדי הממשלה. ההגדרה רלוונטית אך ורק לעניין רישום המאגר. ראו סעיפים 3, 10–11 ל-Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.)

87 פרוטוקול מס' 197, לעיל ה"ש 67, בעמ' 35–40.

לארגון לאגד את הנתונים שברשותו באופן שיפחית את גובה העיצום הכספי העשוי להיות מוטל עליו אם יפר את הוראות חוק הגנת הפרטיות, משום שגובה העיצום הכספי שהרשות מוסמכת להטיל לפי תיקון 13 קשור או תלוי, בנסיבות מסוימות, בגודל מאגר המידע בארגון.[88]

עם זאת, הקריאות למחוק כליל את הגדרת "מאגר מידע" מחוק הגנת הפרטיות נדחו, וועדת החוקה דנה בתיקונים שהוצעו להגדרה בהצעת החוק הממשלתית. הצעה זו ביקשה להתאים את הגדרת "מאגר מידע" להתפתחויות הטכנולוגיות ולשיפור ביכולות עיבוד המידע והצלבתו, ולהפחית באמצעות הגדרה רחבה של המונח את הסיכון להיעדר הגנה על מידע אישי בנסיבות שבהן הוא אינו נופל בגדרי ההגדרה. לפיכך הוצע להשמיט את הסייג הקבוע בפסקה (2) להגדרה. הוסבר ש"אוסף הכולל רק שם מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו", ושאין לבעל השליטה בו אוסף נוסף בשליטתו, הוא בפועל קבוצה כמעט ריקה. למשל, מכתובת דוא"ל ניתן להסיק נתונים אישיים על נושא המידע, כמו למשל הכשרתו המקצועית, מעמדו האישי, ואולי אף את דעותיו ואמונותיו. כלומר, יכולות עיבוד המידע והצלבתו מאפשרות ליצור אפיון שיש בו פגיעה בפרטיות גם על בסיס כתובת דוא"ל בלבד. לפיכך, הצעת החוק הממשלתית הציעה להגדיר "מאגר מידע" כך:[89]

> אוסף פרטי מידע המוחזק באמצעי דיגיטלי, למעט אוסף לשימוש אישי שאינו למטרות עסק.

ועדת החוקה חששה מהנטל הכבד שיוטל על עסקים קטנים וזעירים בעקבות ההגדרה הזאת. עסקים אלו ייאלצו לעמוד בחוק הגנת הפרטיות על שלל החובות שהוא מטיל. למשל, לפי ההגדרה הזאת גם רשימה תפוצה שמית של לקוחותיה של מכולת שכונתית, שיש בה רק שם וכתובת דוא"ל, עלולה להיחשב מאגר

88 ראו סעיף 33 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 23כו לחוק הגנת הפרטיות.

89 הצעת החוק הממשלתית, לעיל ה"ש 51, בסעיף 3(3) המתקן את סעיף 7 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1, ודברי ההסבר בעמ' 426.

מידע. בעקבות זאת, בעל המכולת השכונתית עלול לחוב, בין השאר, בהיווצות עם יועץ אבטחת מידע. אף שוועדת החוקה הבינה את הסכנות הנלוות לצמצום הגדרת מאגר מידע ולהחרגת רשימות הכוללות רק שם ודרכי תקשורת, היא סברה שהצמצום וההחרגה נדרשים לשם הגנה על עסקים קטנים וזעירים, וישמשו גם להכוונת התנהגות. כך, עסקים יתאמצו וימזערו את השימוש שהם עושים במידע אישי כדי ליהנות מההחרגה. אם בכל זאת יגרמו בעלי עסקים כאלה לפגיעה בפרטיות, לפי ועדת החוקה יהיה אפשר לתבוע אותם במסגרת ההוראות העוסקות בפרטיות הקלאסית בפרק א לחוק הגנת הפרטיות, אם כי פתרון זה מוגבל, שכן במרבית המקרים התביעה תידחה בנימוק של פגיעה קלת ערך.[90]

נציגי הרשות להגנת הפרטיות הסבירו בדיון שההתפתחויות הטכנולוגיות מאפשרות להפיק אפיונים שיש בהם פגיעה בפרטיות גם מנתונים טריוויאליים, כגון מען או כתובת דוא"ל, או מהצלבתם עם מידע הזמין לכל באינטרנט. עוד טענו נציגי משרד המשפטים, שנתונים כגון מספר טלפון או כתובת דוא"ל הם אמצעי מרכזי במתקפות סייבר מסוג "פישינג" (דיוג),[91] העלולות לגרום לנזקים חמורים, ועל כן חשוב להגדיר גם רשימות הכוללות רק שם ודרכי תקשורת כ"מאגרי מידע" ולחייבן בהוראות חוק הגנת הפרטיות, בעיקר בהוראות העוסקות באבטחת מידע. אולם, ועדת החוקה דחתה טענות אלו בשם הרצון להגן על עסקים קטנים וזעירים. עמדה זו – החשש שאם תחולת חוק הגנת הפרטיות תהא רחבה מידי, יאבד החוק מערכו המעשי: "אם כל דבר הוא פגיעה בפרטיות, אז שום דבר הוא לא פגיעה בפרטיות" – חזרה ועלתה לאורך כל הדיונים בתיקון 13.

90 פרוטוקול מס' 197, לעיל ה"ש 67, בעמ' 35–46, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

91 מתקפת "פישינג" (דיוג) היא אחת השיטות הקלות והנפוצות להתחיל מתקפת סייבר. מדובר בהודעות המבקשות מהנמען פרטים אישיים, כגון כרטיס אשראי, סיסמה או קוד, או קוראת לו ללחוץ על קישור או לפתוח קובץ. מטרתה לגרום לנמען למסור פרטים אישיים כדי לאסוף מידע אישי, לגנוב כסף, להשתלט על חשבון ברשת החברתית או להיכנס למערכת הארגון שבו עובד הנמען. ראו מערך הסייבר הלאומי, "פישינג".

כך, למשל, ועדת החוקה השתמשה בדוגמת המכולת – אם בעלי מכולות ידעו שממילא כל מאגר מידע שיחזיקו יהיה כפוף להוראות חוק הגנת הפרטיות, הם יאספו מידע אישי רב יותר על לקוחותיהם. מרביתם אומנם לא יעמדו בכל דרישות חוק הגנת הפרטיות, אך בה בשעה יימלטו מציפורני הרגולציה לנוכח משאבי הפיקוח והאכיפה המוגבלים של הרשות להגנת הפרטיות. לעומת זאת, אם בעלי המכולות ידעו שאם יחזיקו רק מאגר מידע הכולל שם וכתובת של לקוחותיהם הם לא ייכנסו לגדר תחולת חוק הגנת הפרטיות, יהיה להם תמריץ להחזיק רק במאגרי מידע רזים כאלה. גם אם מאגרים אלו ייפרצו וידלפו, הנזק, לשיטת ועדת החוקה, יהיה קטן לעומת הנזק הפוטנציאלי שבדליפת מאגרי המידע המלאים שעשויים בעלי המכולות להחזיק אם הגדרת מאגר מידע תיוותר רחבה, כפי שהוצע בהצעת החוק הממשלתית.[92]

לפיכך, ההגדרה שאומצה בתיקון 13 היא:[93]

> "מאגר מידע" – אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי, למעט אחד מאלה:
>
> (1) אוסף לשימוש אישי שאינו למטרות עסק;
>
> (2) אוסף הכולל רק שם, מען ודרכי התקשרות, לגבי 100,000 בני אדם או פחות, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם;

בהשוואה לנוסח החריג לפני תיקון 13, הנוסח החריג שאומץ לבסוף מצומצם יותר:

92 פרוטוקול מס' 197, לעיל ה"ש 67, בעמ' 34, 46, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

93 סעיף 2(4) לתיקון 13, לעיל ה"ש 3, הממקן את סעיף 3 בחוק הגנת הפרטיות.

פסקה (2) להגדרת "מאגר מידע" בסעיף 3 לחוק הגנת הפרטיות לפני לתיקון 13	**פסקה (2) להגדרת "מאגר מידע" בתיקון 13**
אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף	אוסף הכולל רק שם, מען ודרכי התקשרות, לגבי 100,000 בני אדם או פחות, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם

צמצום זה נובע מכמה סיבות:

(1) ההגדרה בתיקון 13 קובעת רף מספרי שלא היה בהגדרת "מאגר מידע" לפני התיקון – האוסף המוחרג יכול לכלול מידע על עד 100,000 נושאי מידע.

(2) ההגדרה לפני התיקון דרשה שהאוסף המוחרג מהגדרת מאגר מידע "אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו". ההגדרה בתיקון 13 אינה עוסקת בשאלה הפרשנית אם האוסף מוביל לפגיעה בפרטיות, אלא מסתפקת בכך שהאוסף אינו כולל נתונים העשויים להיחשב "מידע אישי" נוסף על נושאי המידע. מאחר שהגדרת "מידע אישי" בתיקון 13 היא רחבה,[94] משמעות הדרישה הזאת היא להבטיח שהאוסף המוחרג יכלול שם, מען ודרכי תקשורת בלבד.

(3) ההגדרה לפני התיקון הסתפקה בדרישה שלבעל השליטה אין ולא יהיה "אוסף נוסף" על נושאי מידע כלשהם. ההגדרה בתיקון 13 מספקת תנאים ברורים יותר וקובעת שנדרש שלבעל השליטה אין ולא יהיה אוסף אחר הכולל

94 ראו הדיון בפרק 2.1 לעיל.

פרטי מידע אישי אחרים על אותם נושאי מידע. בפועל, מספר העסקים שיחזיקו באוסף הכולל רק שם ודרכי תקשורת, בלי להחזיק גם ברשימות נוספות, למשל של הזמנות, של חשבוניות או של קבלות – מצומצם, אף שוועדת החוקה הבהירה שהאפשרות לגשת לפרטי מידע רלוונטיים נוספים על אותם נושאי מידע, למשל דרך חיפוש באינטרנט, אינה רלוונטית לבחינה אם יש בידי בעל השליטה אוסף נוסף כאמור.[95]

עם זאת, אף שהחריג שאומץ בסופו של דבר בתיקון 13 מצומצם יותר, בכל זאת, נפקותו המעשית היא שמאגרים העומדים בתנאיו, כלומר כוללים רק שם, מען ודרכי תקשורת של עד 100,000 נושאי מידע, ושלבעל השליטה אין אוסף נוסף הכולל פרטי מידע אישי נוספים על אותם נושאי מידע, אינם מחויבים באבטחת מידע. לכך עשויות להיות השלכות שיש לתת עליהן את הדעת בעיקר בהיבטי הגנת הסייבר. מאז 7 באוקטובר נחזתה עלייה במתקפות הסייבר נגד מדינת ישראל, לרבות מתקפות העושות שימוש בבינה מלאכותית ומאפשרות חיקוי של דפוסי תקשורת רגילים. כך, באמצעות פנייה המתחזה לפנייה לגיטימית בדוא"ל עשויות להתפתח מתקפות סייבר חמורות.[96] למשל, בקיץ 2025 קיבלו משתמשי אתר הזמנות הנופש הפופולרי "בוקינג", הודעות בדוא"ל ובווטסאפ ולפיהן יש בעיה מסוימת בהזמנה, וכדי להבטיח את הזמנתם הם מתבקשים לשוב ולמלא פרטי כרטיס אשראי באמצעות קישורית שסופקה בהודעה. ההודעות היו מפורטות, נראו לגיטימיות ונשלחו לכאורה מעובד בחברה עצמה. לקוחות תמימים מילאו את פרטיהם ונותרו ללא מקום לינה, וחמור מכך הפסידו אלפי שקלים.[97] משום כך, היעדר חיוב באבטחת מידע גם במקרה שבו הרשומה כוללת רק שם ודוא"ל עשוי להקל על שגשוגן ממילא של מתקפות "פישינג" כאלה.

95 פרוטוקול מס' 197, לעיל ה"ש 67, בעמ' 45–48.

96 יוסי הטוני "רוב הארגונים הספיקו להיפגע ממתקפות סייבר מבוססות AI" **אנשים ומחשבים** (10.3.2025).

97 איריס ליפשיץ־קליגר "הונאות, פישינג ושירות לקוי: מה עובר על בוקינג?" **ynet** (8.7.2025).

2.3. השער השלישי: הגדרת בעלי התפקידים הנושאים בחובות לפי החוק

מי שמעבד נתונים שהם בבחינת מידע אישי ושמורים ב"מאגר מידע", כהגדרת מונחים אלו בחוק הגנת הפרטיות, חייב לציית לחוק זה. אולם, כדי להבין מה נכלל באותה חבות, מה משמעות תחולת חוק הגנת הפרטיות והאחריות המוטלת במסגרתו, יש לבחון איזה תפקיד ממלא מי שמעבד את המידע האישי במאגר המידע.

2.3.1. בעל שליטה במאגר מידע

חוק הגנת הפרטיות לפני תיקון 13 ציין את "בעל מאגר מידע" בלי להגדירו.

הצעת החוק הממשלתית ביקשה להוסיף את הביטוי "בעל שליטה במאגר מידע" במקום המונח "בעל מאגר מידע",[98] ולהגדירו כך:

> "בעל שליטה במאגר מידע" – מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוסמך בחיקוק לנהל מאגר מידע או שבעל תפקיד בו הוסמך לכך כאמור;[99]

בדברי ההסבר הודגש שהחלפת הביטוי מ"בעל מאגר מידע" ל"בעל שליטה במאגר מידע" משקפת את העובדה שהמבחן אינו שליטה קניינית אלא שליטה במטרות העיבוד ובהיבטים מרכזיים הנוגעים לאופן העיבוד. עוד הוסבר

98 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 423.

99 סעיף 3(2) להצעת החוק הממשלתית, לעיל ה"ש 51, המתקן את סעיף 7 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

כי ההגדרה המוצעת אף עולה בקנה אחד עם המונח המקביל Controller ב־GDPR.[100]

ה־GDPR מגדיר controller בסעיף 4(7):

> "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

לפי הגדרה זו של ה־GDPR, בעל השליטה (ה־controller) הוא מי שקובע גם את מטרות העיבוד וגם את האמצעים שבהם הוא יעובד. לאורך השנים העניק בית הדין האירופי לצדק (European Court of Justice, ECJ) פרשנות מרחיבה לדרישות אלו, ייחס משקל רב יותר לבחינה מיהו הגורם הקובע את מטרות העיבוד, והסתפק אף בהשפעה מועטה של הגורם הזה על קביעת אמצעי העיבוד. הרציונל שעמד בבסיס הפרשנות המרחיבה הזאת היה ההנחה שככל שיותר גורמים יוגדרו בעלי שליטה ויישאו באחריות לציית להוראות ה־GDPR, כך תשתפר הגנת הפרטיות המצרפית,[101] משום שלפי ה־GDPR נטל החובות והאחריות המוטל על מעבד המידע נמוך מזה המוטל על בעל שליטה בו, שכן בעל שליטה הוא שנחשב האחראי העיקרי לעיבוד מידע.[102] כך, לדוגמה, פסק ה־ECJ בשנת 2018, שמנהלי עמוד מעריצים ברשת החברתית פייסבוק הם בעלי שליטה במשותף עם פייסבוק עצמה. נימוק לכך היה שמנהלי עמוד המעריצים

100 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 423.

101 Case C-2010/16, *Wirtschaftsakademie Schleswig-Holstein* (2018), ECLI:EU:C:2018:388, paras 26-28

102 סעיף הקדמה 83 ל־GDPR, לעיל ה"ש 51.

קובעים קריטריונים לאיסוף מידע, לרבות קהל היעד. עם זאת, מנהלי העמוד אומנם מסייעים לפייסבוק באיסוף מידע אישי על נושאי מידע, אולם בפועל אין להם כל אפשרות לגשת למידע האישי שנאסף, והם מקבלים רק תמצית ניתוחים סטטיסטיים אנונימיים של המידע.[103] דוגמה נוספת היא החלטת ה־ECJ בשנת 2019, שלפיה מפעיל אתר אינטרנט שהטמיע באתר את הכפתור Like של פייסבוק הוא בעלים במשותף של המידע האישי שפייסבוק אוספת באמצעות הכפתור הזה. הנימוק לכך הוא שהמפעיל הוא הגורם המאפשר לפייסבוק לאסוף מידע על כל מי שמבקר באתר שלו, וכך לדעת בית המשפט הוא משפיע על איסוף המידע האישי ועל העברתו. אולם גם כאן למפעיל אתר האינטרנט לא הייתה כלל גישה למידע שנאסף או השפעה על השימושים שעושה פייסבוק במידע הזה.[104] פרשנות מרחיבה כזאת אף עשויה להוביל להחלת החובות המיוחסות לבעל שליטה במידע גם על יצרן מכשיר צריכה חכם הקובע מראש את מסגרת השימושים במכשיר, אף שהמידע האישי הנאסף נשמר על גבי המכשיר עצמו והגישה אליו מוגבלת למשתמש במכשיר בלבד.[105]

אולם בקווים המנחים המעודכנים של ה־European Data Protection Board (EDPB), שאומצו ביולי 2021, הובהר שבעל השליטה הוא המשפיע על מטרות העיבוד ועל אמצעי העיבוד. עם זאת, במקרה שבו בעל השליטה מתקשר עם מעבד (processor) לשם ביצוע העיבוד, מובן שגם המעבד יוכל לקבל החלטות ביחס לעיבוד. אולם אז יש לקבוע קווים מנחים בנוגע לרמת ההשפעה על המטרות והאמצעים המקימה חבות על בעל השליטה, ולהגדיר את היקף ההחלטות שמעבד יוכל לקבל בעצמו. כנקודת מוצא נקבע שרק בעל השליטה יכול לקבוע את מטרות העיבוד. בנוגע לאמצעי העיבוד, ה־EDPB מבחין בין אמצעים חיוניים לאמצעים לא חיוניים. אמצעים חיוניים (Essential means)

103 ראו Case C-2010/16, *Wirtschaftsakademie Schleswig-Holstein* (2018), ECLI:EU:C:2018:388, paras 37

104 Case C-40/17 *Fashion ID* 2019 ECLI:EU:C:2019:629

105 Alan Dahi & Marcelo Corrales Compagnucci, *Device Manufatures as Controllers – Expanding the Concept of "Controllership" in the GDPR,* 47 Comp. L. & Sec. Rev. (2022)

הם אמצעים הקשורים קשר הדוק למטרת העיבוד ולהיקפו. למשל, סוג המידע שיעובד, משך העיבוד, סוגי מקבלי המידע או מורשה הגישה למידע ולתוצרי העיבוד, וקטגוריות נושאי המידע. האמצעים החיוניים בשילוב עם מטרת העיבוד הם שמשפיעים על חוקיות העיבוד, על נחיצותו ועל מידתיותו. ולכן, קביעת האמצעים החיוניים צריכה להיות אחריותו של בעל השליטה בלבד. אמצעים לא חיוניים (non-essential means) נוגעים יותר להיבטים הפרקטיים של יישום ההחלטות הקשורות למטרת העיבוד ולאמצעים החיוניים לעיבוד. למשל, בחירת התוכנה שתשמש לעיבוד המידע ואמצעי אבטחת המידע שיש לנקוט. אלו, לפיכך, יכולים להיות נתונים לשיקול דעתו של המעבד. עם זאת, גם אם המעבד מקבל החלטות מסוימות ביחס לאמצעים הלא־חיוניים, על בעל השליטה לפרט בהסכם ביניהם נושאים מסוימים, למשל דרישות אבטחת מידע. ומכל מקום, בעל השליטה נותר האחראי לציות להוראות ה־GDPR, ועל כן עליו להחזיק ביכולת להראות שעיבוד המידע, גם אם נעשה על ידי המעבד, נעשה למטרה חוקית, והוא נחוץ ומידתי על פי דרישות ה־GDPR.[106]

להמחשת ההבחנה בין אמצעים חיוניים לאמצעים לא חיוניים, ובעצם להבחנה בין ארגון שההחלטות שהוא מקבל מקימות לו חבות בשל היותו בעל שליטה, לעומת ארגון שההחלטות שהוא מקבל מקימות לו חבות של מעבד בלבד, מספק ה־EDPB כמה דוגמאות. למשל ניהול שכר. מעסיק א שוכר את ארגון ב לניהול תשלום השכר לעובדיו. מעסיק א מספק הוראות ברורות – למי לשלם, גובה השכר לכל עובד, תאריך התשלום, פרטי חשבון הבנק שאליו יש להעביר את התשלום, משך הזמן שבו יש לשמור את המידע, המידע שיש לחשוף בפני רשויות המס וכדומה. במקרה כזה עיבוד המידע הוא למטרת תשלום המשכורות, ולכן לארגון ב', ששירותיו הושכרו לשם ניהול תשלומי השכר, אסור לעשות שימוש במידע לכל מטרה אחרת. שיקול הדעת שלו מוגבל רק בנושאים מסוימים, כגון באיזו תוכנה להשתמש, או למי מעובדיו להעניק הרשאת גישה לשם ניהול תשלומי השכר. לפיכך מעסיק א הוא בעל השליטה במידע הנדרש לשם תשלום

106 EDPB Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR (2021) (להלן: EDPB Guidelines 07/2020), בעמ' 14–15, סעיפים 37–41.

השכר לעובדיו, ואילו ארגון ב הוא מעבד בלבד. לשם תשלום השכר עצמו מועבר גם מידע רלוונטי מארגון ב', המחשב את חישובי השכר, לבנק המעבד את המידע שהועבר אליו לשם ביצוע הפעולות הבנקאיות הנדרשות לתשלום השכר. במסגרת פעולות אלו הבנק הוא שמחליט, בנפרד ממעסיק א, מה המידע שיעובד ולמשך כמה זמן יישמר. למעסיק א אין כל השפעה על המטרות והאמצעים שישמשו את הבנק בעיבוד המידע, ולכן הבנק צריך להיחשב בעל שליטה ביחס לעיבוד המידע הזה.[107]

דוגמה נוספת היא מוקד טלפוני. ארגון מסוים מחליט להעביר למיקור חוץ את מוקד שירות הלקוחות הטלפוני שלו. בהתקשרות עם ספק המוקד הטלפוני נקבע שעל הספק לנקוט את האמצעים הטכנולוגיים והארגונים המתאימים לאבטחת המידע, כנדרש ב־GDPR, וכי עליו לעשות שימוש במידע האישי המסופק לו על לקוחות הארגון אך ורק למטרותיו של הארגון ולפי הוראותיו. אולם הארגון אינו מספק לספק המוקד הטלפוני הוראות כלשהן בנוגע לתוכנה שבה יבוצע העיבוד או לאמצעי אבטחת המידע שעליו לנקוט. ספק המוקד הטלפוני מקבל מידע מזוהה על הרכישות של הלקוחות ועל דרכי ההתקשרות עימם, ומשתמש בתוכנה שלו ובתשתית טכנולוגית משלו כדי לנהל את המידע האישי הנוגע ללקוחותיו של הארגון. כך, ספק המוקד הטלפוני קובע את האמצעים הלא־חיוניים ביחס לעיבוד, ואילו הארגון נותר בעל השליטה הקובע את מטרות העיבוד ואמצעי העיבוד החיוניים.[108]

למרות הבהרה זו של ה־EDPB בנוגע לפרשנות הנכונה של הגדרת בעל שליטה ב־GDPR, נציגי משרד המשפטים והרשות להגנת הפרטיות נותרו בעמדתם, שלפיה "בעל שליטה" בישראל צריך להיות מי שקובע את מטרות העיבוד בלבד. לטענתם, הגדרה זו משקפת את המצב בפועל, שכן לדבריהם לרוב בעל השליטה במאגר המידע אינו קובע מהם האמצעים לעיבוד המידע. קביעה זו נעשית

107 שם, בעמ' 15–16, סעיף 40.

108 שם, בעמ' 16, סעיף 41.

בידי מי שמבצע את העיבוד בפועל, המכונה בחוק הגנת הפרטיות "מחזיק".[109] יתרה מזו, ההגדרה ש"בעל השליטה במאגר המידע" הוא מי שקובע אך ורק את מטרות העיבוד ממזערת את הסכנה שבגלגול האחריות להפרת הוראות חוק הגנת הפרטיות למחזיק רק משום שהוא מי שקבע את אמצעי העיבוד.[110]

לפיכך, הגדרת "בעל שליטה במאגר מידע" שאומצה בתיקון 13 היא:[111]

> "בעל שליטה" במאגר מידע – מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר מידע.

בשנים הבאות יהיה עלינו לבחון אם צדקו נציגי משרד המשפטים והרשות להגנת הפרטיות בעמדתם, והגדרה רחבה זו של בעל שליטה חיזקה את הגנת הפרטיות בישראל, או שמא הביאה לאכיפת יתר נגד גורמים שאין להם כל שליטה בעיבוד המידע האישי בפועל. אם כך, יהיה צורך בבחינה מחודשת של ההגדרה ובאימוץ מתווה ברוח ה־GDPR, כפי שפורש על ידי ה־EDPB, שלפיו בעל השליטה הוא מי שקובע את מטרות העיבוד ואת אמצעי העיבוד החיוניים.[112]

2.3.2. מחזיק

בעולם הפרטיות המידעית מקובל להבחין בין בעל השליטה במאגר המידע, שנידון לעיל, לבין ישות משפטית נפרדת שבעל השליטה מעביר אליה את מאגר המידע לשם ביצוע חלק מפעולות עיבוד המידע. למשל, משרד עורכי דין הוא בעל השליטה במידע האישי על עובדיו, אולם הוא מעביר מידע אישי עליהם לחברה המספקת שירותי ניהול שכר, כדי שתחשב את השכר שיש לשלם לכל

109 ראו הדיון בסעיף 2.3.2 להלן.

110 פרוטוקול מס' 210, ה"ש 84 לעיל, בעמ' 83–85.

111 סעיף 2(3) לתיקון 13, לעיל ה"ש 3, המתקן את סעיף 2 בחוק הגנת הפרטיות.

112 ראו לעיל הדיון בטקסט הנלווה לה"ש 102–109.

עובדת ועובד ותנהל את תשלום השכר. החברה המספקת שירותי ניהול שכר היא לפיכך ה"מחזיק" במאגר המידע על העובדים.

בחוק הגנת הפרטיות לפני תיקון 13 הוגדר "מחזיק" כך:

> "מחזיק, לענין מאגר מידע" – מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש.[113]

הצעת החוק הממשלתית ביקשה לעדכן את הגדרת "מחזיק" כך:

> "מחזיק", לעניין מאגר מידע – מי שהתקשר עם בעל שליטה במאגר מידע למתן שירות לבעל השליטה או למתן שירות מטעם בעל השליטה, וקיבל מבעל השליטה במאגר המידע, במסגרת ההתקשרות, הרשאה לעשות שימוש במידע שבמאגר לצורך מתן השירות;[114]

לפי דברי ההסבר, ההגדרה המוצעת ל"מחזיק" משקפת את מהות התפקיד, כפי שעולה גם מתקנה 15 לתקנות אבטחת מידע. תקנה זו מאסדרת את התקשרותו של בעל שליטה עם גורם חיצוני לשם מיקור חוץ של עיבוד המידע, ומיועדת לחדד את ההבחנה בין בעל השליטה במאגר המידע, מחד גיסא, לבין מורשה גישה למאגר המידע, מאידך גיסא. כן מבהירה ההגדרה המוצעת בהצעת החוק הממשלתית שאין צורך בהחזקת עותק פיזי של מאגר המידע כדי להיחשב מחזיק.[115] עם זאת, בדיונים בוועדת החוקה עלה החשש שההגדרה המוצעת, המחייבת התקשרות בין המחזיק לבעל השליטה, עלולה לגרום להתפלפלויות מיותרות בשאלה מהי ההתקשרות הנדרשת לשם הטלת

113 ראו הגדרת המונח "מחזיק" בסעיף 3 לחוק הגנת הפרטיות לפני לתיקון 13, לעיל ה"ש 1.

114 סעיף 2(1) להצעת החוק הממשלתית, לעיל ה"ש 51, המתקן את הגדרת "מחזיק" בסעיף 3 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

115 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 423–424.

חבות של מחזיק. למשל, האם גורם שקיבל רק שם משתמש וסיסמה, אך טרם ביצע כל פעולת עיבוד נחשב כבר למחזיק? האם נדרש שיבצע עיבוד בפועל כדי להיחשב מחזיק?[116] כן התעוררה השאלה אם לפי ההגדרה המוצעת עובד בארגון עלול להיחשב מחזיק בעצמו. לשיטת נציג הרשות להגנת הפרטיות, הדרישה שמחזיק יהיה גורם שהתקשר עם בעל השליטה נועדה להבהיר שאין כוונה לראות בעובד של בעל השליטה מחזיק.[117] עוד הוצגו בדיון בוועדת החוקה ההנחיות של ה־EDPB בכל הקשור להבחנה בין מעבד לבעל שליטה לפי ה־GDPR. נטען כי הנחיות אלו מבהירות שהמעבד צריך להיות גורם חיצוני לבעל השליטה המעבד מידע אישי בשמו של בעל השליטה. עוד מובהר בהן שעובד של בעל שליטה אינו יכול להיחשב מחזיק.[118]

ואכן, ההגדרה ל"מחזיק" שאומצה לבסוף בתיקון 13 דומה להגדרת "מעבד" (processor) ב־GDPR,[119] והיא מבהירה שמדובר בגורם חיצוני לבעל השליטה. כך, למשל, חשב השכר העובד במשרד עורכי דין המעבד מידע במאגר המידע על עובדי המשרד אינו מחזיק, אלא אחד ממורשי הגישה למאגר המידע. כן הושמטה הדרישה לקיומה של התקשרות בין בעל השליטה למחזיק:

> "מחזיק", לעניין מאגר מידע – גורם חיצוני לבעל השליטה במאגר המידע המעבד בעבורו מידע;[120]

116 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 90, דברי ד"ר רחל אריאלי הרשקוביץ, בעמ' 98 דברי יו"ר ועדת החוקה, ח"כ רוטמן.

117 שם, בעמ' 90–97, ובעמ' 98, דברי יועמ"ש הרשות להגנת הפרטיות, עו"ד אידלמן.

118 שם, בעמ' 98, דברי עו"ד דלית בן ישראל ועו"ד עמרי רחום טוויג; EDPB Guidelines 07/2020, לעיל ה"ש 107.

119 סעיף 4(8) ל־GDPR, לעיל ה"ש 33, הגדרת "processor":

> "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

120 סעיף 2(5) לתיקון 13, לעיל ה"ש 3, המתקן את הגדרת "מחזיק" בסעיף 3 בחוק הגנת הפרטיות.

2.3.3. מנהל מאגר

"מנהל מאגר" הוגדר בחוק הגנת הפרטיות לפני לתיקון 13 כך:

> "מנהל מאגר" – מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;[121]

הצעת החוק הממשלתית הותירה את המונח "מנהל מאגר" בעינו ולא שינתה את הגדרתו. אולם לאורך הדיונים בוועדת החוקה נמתחה על כך ביקורת. נטען שההתייחסות בחוק ל"מנהל מאגר" משקפת תפיסה ארכאית, וכי אין צורך בבעל תפקיד נוסף לצד בעל שליטה ומחזיק, שהם ממילא הנושאים העיקריים בחובות לפי חוק הגנת הפרטיות. מכל מקום, אם תוטל אחריות אישית, היא תוטל לפי דיני החברות, וסביר שמי שיישא בה יהיה מנכ"ל הארגון או הגוף. בפועל, החובה למנות בעל תפקיד בארגון למנהל מאגר והחשש מפני אחריות אישית גורמת לקושי רב במציאת בעלי תפקידים בארגון המוכנים להתמנות לתפקיד. יתרה מזו, חוק הגנת הפרטיות מטיל אחריות על מנהל מאגר, אך אינו מטיל עליו במפורש כל חובה או תפקיד. החובות המוטלות על מנהל מאגר מפורטות בתקנות אבטחת מידע ובתקנות העברת מידע בין גופים ציבוריים. משום כך, בפועל, בעיקר בארגונים גדולים, חובותיו של מנהל מאגר ממולאות בידי כמה אנשים בארגון ולא בידי אדם אחד.[122]

נציג משרד המשפטים עמד על ההבדל בין מנהל מאגר, שהוא אדם, לבין בעל שליטה או מחזיק שהם לרוב ארגונים או גופים ציבוריים. עוד טען הנציג שאף שהאחריות מוטלת על בעל השליטה או המחזיק, למשל לפי תקנה 17 לתקנות אבטחת מידע, יש צורך במינוי אדם שימלא את המשימות המוטלות בחוק, ולפי הגדרת "מנהל מאגר", מדובר ממילא במנהל הפעיל של הארגון שהוא בעל

121 ראו הגדרת המונח "מנהל מאגר" בסעיף 7 לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

122 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 61–62; פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 25–31.

השליטה. נציג הרשות להגנת הפרטיות הסביר שבכל הקשור לאבטחת מידע ולנוכח חשיבות הנושא חשוב למנות מנהל מאגר.[123]

יו"ר ועדת החוקה עמד על כך שלא תמיד "מנהל מאגר" הוא בהכרח אדם מסוים, למשל בחברות ניהול, וכן על היותה של ההגדרה הקיימת טאוטולוגית. יתרה מזו, בדיון נשאל מדוע דווקא בנושאים הקשורים בהגנה על הפרטיות יש צורך לחרוג מדיני האחריות התאגידית הכלליים ולדרוש מינויו של אדם מסוים בארגון לתפקיד מנהל מאגר. לשיטת ועדת החוקה ונציגי המגזר הפרטי והחברה האזרחית שנכחו בדיון, אף שייתכן שיש צורך בהטלת אחריות אישית על אדם כאמצעי להגברת הציות לדרישות אבטחת מידע, המסגרת המשפטית הקיימת של "מנהל מאגר" אינה מתאימה לכך ואינה מובילה לתוצאה זו. לשם כך יש צורך בתיקון חוק הגנת הפרטיות ובהטלת חובה למנות ממונה הגנת פרטיות, כפי שקבוע ב־GDPR.[124] נציג משרד המשפטים לא חלק על הטענה שמינוי ממונה הגנת פרטיות בארגון יאיין את הצורך במנהל מאגר, אולם הוא סבר שכל עוד אין תיקון כזה, אין מקום להסיר את תפקיד מנהל המאגר מחוק הגנת הפרטיות.[125]

לצד הצורך ביציקת תוכן אמיתי הקשור לאבטחת מידע לתפקיד "מנהל מאגר" בארגונים מהמגזר הפרטי, או לחלופין בחיוב במינוי ממונה על הגנת הפרטיות בהם, עמדה ועדת החוקה על החשיבות שבמינוי מנהל מאגר בגופים ציבוריים, שבהם כללי האחריות התאגידית אינם מתאימים בהכרח. למשל, אי אפשר לצפות מהעומדים בראש משרד המשפטים, השר או מנכ"ל המשרד, או בראש מועצה מקומית או עירייה, להיות מעורים בכל הקשור למאגר המידע שבשליטת הגוף.[126] עם זאת, לנוכח טענות מצד נציגת השלטון המקומי בדבר

123 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 61–62, דברי עו"ד עמית יוסוב עמיר; פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 28, דברי עו"ד גרסון.

124 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 62, דברי יו"ר ועדת החוקה, ח"כ רוטמן; פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 28, דברי יו"ר ועדת החוקה, ח"כ רוטמן, ובעמ' 30–32; ס' 37 ב־GDPR, לעיל ה"ש 33.

125 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 38–39 דברי עו"ד יוסוב עמיר.

126 שם, בעמ' 32–34, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

היעדר תקציבים למימון מספר רב של בעלי תפקידים ייעודיים לנושא מאגרי מידע והגנת פרטיות הובהר שלא מוטלת על גוף ציבורי חובה למנות מנהל מאגר. בהיעדר מינוי כזה תחול החובה על מנכ"ל הרשות המקומית, שרשות מקומית חייבת ממילא במינויו.[127]

לפיכך, ההגדרה שאומצה בסופו של דבר בתיקון 13 מאיינת את תפקיד מנהל מאגר בארגונים מהמגזר הפרטי ומותירה אותו רלוונטי רק בארגונים במגזר הציבורי.

> "מנהל מאגר" – בעל שליטה במאגר מידע, ולעניין גוף ציבורי כהגדרתו בסעיף 23 – המנהל הכללי של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שהמנהל הכללי הסמיכו לנהל את המאגר.[128]

נוסף על כך, לצד שינוי הגדרת "מנהל מאגר" ובעקבותיו הוחלט על הוספת מתווה למינוי ממונה הגנת פרטיות בתיקון 13.[129]

2.4. הגדרת "עיבוד" ו"שימוש"

תחולת חוק הגנת הפרטיות אינה מותנית בעשיית פעולה במידע אישי העונה להגדרות "עיבוד" או שימוש". יתרה מזו, "פגיעה בפרטיות" המוגדרת בסעיף 2 לחוק הגנת הפרטיות אינה מזכירה כלל שימוש במידע אישי או עיבוד שלו. ההחלטה אם הפעולה הנעשית במידע אישי מתאימה להגדרת אחד ממופעי הפגיעה בפרטיות היא עניין לפרשנות. כך, גם חובת הרישום המוטלת על גופים

127 פרוטוקול מס' 334 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ז באייר התשפ"ד (4 ביוני 2024), בעמ' 25–28.

128 סעיף 2(5) בתיקון 13, לעיל ה"ש 3, המתקן את סעיף 3 בחוק הגנת הפרטיות.

129 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 16, דברי עו"ד יוסוב עמיר; ראו הדיון בסעיף 5.3 להלן.

ציבוריים אינה מותנית בשימוש או בעיבוד.[130] גם חובת אבטחת המידע המוטלת על בעל שליטה או מחזיק אינה מותנית בעיבוד או בשימוש במידע אישי.[131]

למרות זאת, חשוב לדעתי להבין את משמעות הפעולות העונות להגדרה "עיבוד" או "שימוש" ואת היקפן לשם הבנת חלק מהחובות המוטלות על פי חוק הגנת הפרטיות, וכן מתוך ציפייה שבתיקון נוסף עתידי לחוק הגנת הפרטיות יוסדרו גם בסיסים חוקיים לעיבוד מידע אישי, כמו ב־GDPR.[132]

המונח "עיבוד" לא הופיע כלל בחוק הגנת הפרטיות לפני תיקון 13, ו"שימוש" הוגדר כך:

> "שימוש" – לרבות גילוי, העברה ומסירה.[133]

הצעת החוק הממשלתית ביקשה להוסיף את המונח "עיבוד" ולהגדירו "איסוף או שימוש".[134] עוד הוצע להוסיף להגדרת "שימוש" גם את פעולת האחסון.[135] לפי דברי ההסבר, אף שההגדרה של "שימוש" הייתה רשימה פתוחה של פעולות, המכנה המשותף לפעולות שצוינו בה הוא שמדובר בפעולות הקשורות להוצאת מידע או להפצתו. משום כך יש צורך בהבהרה שגם עצם אחסון מידע במאגר מידע הוא שימוש במידע, אף אם לא נלוות לו פעולות נוספות. אשר להגדרת "עיבוד", בדברי ההסבר צוין כי המטרה היא לכרוך את שתי הפעולות במידע

130 סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א לחוק הגנת הפרטיות.

131 סעיף 15 בתיקון 13, שם, המתקן את סעיף 17 לחוק הגנת הפרטיות.

132 סעיף 6(1) ו־9(1) ל־GDPR, לעיל ה"ש 33.

133 סעיף 3 לחוק הגנת הפרטיות לפני לתיקון 13, לעיל ה"ש 1.

134 סעיף 3(4) להצעת החוק הממשלתית, לעיל ה"ש 51, המציע לתקן את סעיף 7 לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

135 סעיף 2(2) להצעת החוק הממשלתית, לעיל ה"ש 51, המציע לתקן את סעיף 3 לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

אישי, איסוף ושימוש, בהגדרה אחת הדומה להגדרת המונח עיבוד (processing) ב־GDPR.[136]

ועדת החוקה סברה שההבחנה בין "עיבוד" ל"שימוש" והגדרתם בנפרד אינה הכרחית, שכן בפועל מדובר במונחים שמשמעותם זהה, כפי שאין הבדל רב בין "איסוף" לבין "אחסון", שכן אי אפשר לאסוף מידע בלי לאחסן אותו.[137] עם זאת, הוחלט להותיר את שני המונחים כמונחים חלופיים המתארים רשימה פתוחה של פעולות הנעשות במידע אישי, כדי להימנע, לעת עתה, מלתקן את כל החוק, התקנות והחוקים הקשורים העושים שימוש במונח "שימוש".[138] לפיכך, ההגדרה שאומצה מונה רשימה פתוחה של פעולות, והיא שואבת השראה מהגדרת המונח עיבוד (processing) ב־GDPR:[139]

> "עיבוד", "שימוש" – כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו;[140]

136 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 425; סעיף 4(2) ל־GDPR, לעיל ה"ש 33, הגדרת processing:

> "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

137 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 19–25.

138 שם, בעמ' 20, דברי עו"ד יוסוב־עמיר "סיבה נוספת, שהיא גם קצת קזואיסטית, אבל היא חשובה ומרכזית, שכרגע תקנות אבטחת מידע משתמשות במילה "שימוש". המטרה היא להבהיר. בסוף, אין פה משמעות נורמטיבית עמוקה. כל פעולה זה עיבוד. אבל אנחנו לא רוצים שייווצרו כל מיני פערים נוסחיים, כל מיני שאלות".

139 ראו סעיף 4(2) ל־GDPR, לעיל ה"ש 33.

140 סעיף 2(6) לתיקון 13, לעיל ה"ש 3, המתקן את סעיף 3 לחוק הגנת הפרטיות.

פרק 3

החידושים העיקריים בתיקון 13 לעניין רישום מאגר מידע

לאחר הבנת השינויים החשובים בתחולת חוק הגנת הפרטיות בעקבות תיקון 13, בתת־הפרק הזה נבחן את השינויים העיקריים שחולל התיקון ביחס לחובות המוטלות על בעל שליטה או מחזיק, האחריות המוטלת על כל אחד מבעלי התפקידים, וכיצד נקבע אם עיבוד המידע הוא חוקי. לנושאים אלו חשיבות גדולה בבחינת השלכות תיקון 13 על הגנת הפרטיות המצרפית של אזרחי מדינת ישראל. כן יש בהן כדי לשפוך אור על החוסרים שעדיין נותרו בו לעומת החקיקה הבינלאומית, בעיקר ה־GDPR, וכן לשם הבהרת חובות בעל שליטה ומחזיק והמותר והאסור בעיבוד מידע אישי, ומחייבים תיקון נוסף בהקדם.

3.1. צמצום חובת הרישום

חוק הגנת הפרטיות לפני תיקון 13 הטיל חובת רישום על מאגר מידע שיש בו מידע על למעלה מ־10,000 נושאי מידע, או מידע רגיש, או מידע על נושאי מידע שלא נמסר על ידם, מטעמם או בהסכמתם. כן חויבו ברישום מאגרי מידע של גופים ציבוריים או מאגרים המשמשים לשירותי דיוור ישיר. ראש הרשות להגנת הפרטיות היה רשאי לסרב לרשום מאגר מידע. לסמכות זו הייתה חשיבות, שכן היה אסור לנהל או להחזיק מאגר מידע החייב ברישום ללא רישומו.[141]

הצעת החוק הממשלתית הכירה בצורך לצמצם את היקף חובת הרישום כדי למקד את הפעילות הרגולטורית "במאגרים המציבים איומים משמעותיים לפרטיות". לפיכך הוצע בה שחובת הרישום תוטל על מאגר מידע הכולל מידע

141 סעיף 10(א)(1) לחוק הגנת הפרטיות לפני לתיקון 13, שם.

על 100,000 נושאי מידע ומעלה ומתקיים בו גם אחד מהתנאים האלה: (1) מאגר המידע כולל מידע שלא נמסר על ידי או מטעם נושא המידע או בהסכמתו; (2) המאגר הוא של גוף ציבורי; או (3) מטרתו העיקרית של מאגר המידע היא שירותי דיוור ישיר. כן הוצע להטיל חובת רישום על מאגר מידע הכולל מידע בעל רגישות מיוחדת על 500,000 נושאי מידע ומעלה.[142]

נציגי החברה האזרחית והמגזר הפרטי שנכחו בדיוני ועדת החוקה עמדו על החשש שחובת הרישום, גם לאחר צמצומה, עדיין רחבה מידי. הועלו גם השגות בדבר הצורך בחובת רישום ביחס למגזר הפרטי, לנוכח היעדר חובה דומה במרבית מדינות המערב, ומתאם בין קיומה של חובת רישום לבין תמ"ג נמוך לנפש, דירוג נמוך של המדינה בפיתוח ההון האנושי, ודירוג נמוך במדד הדמוקרטיה העולמי.[143] נוסף על כך, נטען כי חובת הרישום אינה מותאמת למציאות הטכנולוגית הקיימת, ואינה מספקת הגנה אמיתית ומהותית לזכות לפרטיות. בראשית שנות ה־70 הייתה הטלת חובת רישום מקובלת, לנוכח מיעוט מאגרי המידע והעובדה שהרישום אפשר לרשות האחראית למקד את תשומת לבה בסיכונים האמיתיים לזכות לפרטיות, אולם שפע מאגרי המידע היום הופכים חובה זו לנטל בירוקרטי, ואין אפשרות אמיתית להסיק תובנות בדבר רמת הסיכון לזכות לפרטיות המשתקפת מעצם קיומו של מאגר המידע.[144]

142 סעיף 4 בהצעת החוק הממשלתית, לעיל ה"ש 51, המציע לתקן את סעיף 8 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

143 ראו רחל אריאלי הרשקוביץ ותהילה שוורץ אלטשולר "קול קורא בנושא תיקון חוק הגנת הפרטיות" **המכון הישראלי לדמוקרטיה** (דצמבר 2020); רבקי דב"ש "השוואת הסדרים בחקיקת מידע אישי – חובת הרישום" **המכון הישראלי למדיניות טכנולוגיה** (ינואר 2022, עדכון יוני 2022).

144 זהו ההסבר שניתן ב־GDPR, לעיל ה"ש 33, לביטול חובת ההודעה שהייתה קיימת לפי דירקטיבת הגנת המידע. ראו סעיף הקדמה 89 ל־GDPR:

> Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and

עוד נטען כי חיוב בחובת רישום מאגרי מידע שהמידע שבהם לא נמסר על ידי או מטעם נושא המידע או בהסכמתו יוביל להחלת חובת רישום רחבה, מתוך חוסר הבנה של התפתחויות טכנולוגיות. כך, לדוגמה, כבר היום יש מאגרי מידע רבים הכוללים מידע שלא נמסר בידיעת נושא המידע או בהסכמתו. למשל, מידע שמקבלת חברת ביטוח ממבוטח שלה כחלק מדיווח על תאונת דרכים שהיה מעורב בה כולל גם מידע על הנהגים והעדים הנוספים בזירה. סביר שמידע כזה על צדדים שלישיים הועבר לחברת הביטוח ללא ידיעת הצדדים השלישיים או הסכמתם.[145]

הרשות להגנת הפרטיות הסבירה במהלך הדיונים בוועדה החוקה שחובת הרישום הכרחית לפעולות האכיפה שתנקוט, משום שבהיעדר רישום תתקשה הרשות לזהות מהם מאגרי המידע המצריכים את בחינתה המעמיקה לנוכח רגישות המידע האישי האגור בהם או סוג עיבוד המידע המבוצע.[146] טענה זו, שכאמור הייתה נכונה כנראה בראשית שנות ה־70, מוטלת היום בספק. הבחינה אם מאגר המידע חוקי או לא חוקי יכולה להיעשות באמצעות חיוב בעריכת תסקיר השפעה על הפרטיות ומינוי ממונה על הגנת פרטיות בארגון. כך יובטח שהארגון יבחן מראש את השלכות עיבוד המידע שהוא מבקש לעבד על הזכות לפרטיות, על פי כללים ברורים. זאת בניגוד לחובת רישום המאפשרת לארגון להימלט מציפורני הרשות להגנת הפרטיות באמצעות יצירת מאגרי מידע שאינם עומדים בסף המספרי המחייב את רישומם, וככלל לעבד מידע באין מפריע עד

---

replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

145 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 103–104.

146 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 70–90.

להגעה לסף המספרי המחייב רישום, או עד קבלת תשובת ראש הרשות להגנת הפרטיות לבקשת הרישום.[147]

לצד החששות מהותרת חובת רישום על מרבית הארגונים במגזר הפרטי, עמדה ועדת החוקה על חשיבות הותרת חובת הרישום על גופים ציבוריים. המדינה אוספת בכפייה מידע אישי רב על אזרחיה, ועל כן כחלק מעקרון חופש המידע עליה לספק לאזרח מידע מדויק על המידע שהיא מחזיקה עליו, ולאפשר לו לממש את זכויותיו ביחס אליו.[148] נוסף על כך, בוועדת החוקה הוצע להותיר את חובת הרישום על סוחרי מידע (data brokers) המעבדים מידע אישי לשם מכירתו לצדדים שלישיים,[149] בדומה לחובה המקובלת בקליפורניה שבארצות הברית.[150]

לפיכך, חובת הרישום שעוגנה בתיקון 13 התמקדה בשני סוגים של בעלי שליטה במאגר מידע:[151]

(1) **גופים ציבוריים.** הטלת חובת הרישום על גופים ציבוריים מיועדת להגביר את השקיפות של גופים אלו כלפי האזרחים, ולהקל על מימושן של זכויות נושא המידע במידע האישי על אודותיו האגור במאגרי המידע האלה. מאגרי מידע הכוללים רק מידע אישי על עובדיו של הגוף הציבורי מוחרגים מחובת הרישום.[152] עם זאת, ההחרגה מצומצמת רק למידע אישי על עובדי הגוף הציבורי בפועל, ולכן היא לא תחול, למשל, על מאגר מידע של מועמדים לעבודה בגוף הציבורי.[153]

147 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 105, דברי רחל אירידור הרשקוביץ.

148 שם, בעמ' 107, 108, דברי יו"ר הוועדה, ח"כ רוטמן.

149 שם, בעמ' 106–107.

150 Cal. Civ. Code §1798.99.82 (West 2024)

151 ראו סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א לחוק הגנת הפרטיות.

152 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 107.

153 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 61–62.

(2) **גופים שמטרתם "העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר", ביחס למאגרי מידע שבשליטתם, המונים מידע אישי על מעל 10,000 אנשים.**[154] אף שתיקון 13 אינו מציין זאת במפורש, בדיונים בוועדת החוקה היה ברור שהכוונה לסוחרי מידע (data brokers). הובהר שאין הכוונה למצב שבו בעל שליטה במידע, שמטרתו העיקרית אינה איסוף מידע אישי לשם מסירתו או מכירתו לאחר, מוכר מאגר מידע שברשותו לאחר. למשל, רשת קמעונאית שמחזיקה במועדון לקוחות לשם מתן הטבות וחיזוק הקשר עם הלקוח. אם הרשת מחליטה בנסיבות מסוימות למכור את מועדון הלקוחות, למשל בשל הפסקת פעולותיה או כחלק ממיזוג, אין מדובר במטרתה העיקרית של הרשת, ועל כן היא אינה חבה בחובת הרישום.[155]

הצעת החוק הממשלתית ביקשה לשמר גם את הגורם שעליו מוטלת חובת הרישום באמצעות שימור נוסח סעיף 8(א) מחוק הגנת הפרטיות לפני תיקון 13: "לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה: (1) המאגר נרשם בפנקס; [...]". אולם בדיון בוועדת החוקה עלה החשש שחובת הרישום תפורש גם כחובה המוטלת על מחזיק במאגר מידע, ותוביל להטלת נטל שמחזיק לא יוכל לעמוד בו. ועדת החוקה הציעה בתחילה שהפרשנות לחובה שתוטל על המחזיק לא תהיה שחובתו להגיש בקשה לרישום מאגר מידע, אלא שחובתו לוודא שבעל השליטה במאגר המידע מילא את חובתו לרשום מאגר מידע. אולם, במהלך הדיון בוועדת החוקה הובהר שגם לפי פרשנות זו יהיה מדובר בחובה שמחזיק לא יוכל לעמוד בה. כך, למשל, מחזיק שהוא ספק שירותי ענן אינו יודע מהו תוכן מאגר המידע המאוחסן אצלו, ולכן לא יוכל לבדוק אם מדובר במאגר מידע החייב ברישום ואם בעל השליטה בו עמד בחובתו זו.[156] לפיכך, וכחלק מניסיון רחב יותר להבחין בין חובות מהותיות המוטלות על המחזיק לעומת חובות המוטלות על בעל השליטה במאגר מידע, הובהר כי חובת רישום מאגר המידע מוטלת על בעל השליטה במאגר מידע בלבד.[157]

154 ראו סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א לחוק הגנת הפרטיות.

155 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 66–69.

156 שם, בעמ' 62–63.

157 ראו סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א(א)(2) לחוק הגנת הפרטיות.

3.2. חובת הודעה לרשות להגנת הפרטיות

לצד צמצום חובת הרישום ביקשה הצעת החוק הממשלתית להטיל חובת הודעה על בעל שליטה במאגר מידע הכולל מידע בעל רגישות מיוחדת על יותר מ־100,000 נושאי מידע אך פחות מ־500,000.[158] הנימוק לכך היה שצמצום חובת הרישום יפגע ביכולתה של הרשות להגנת הפרטיות לאתר עיבודי מידע המפרים את הוראות חוק הגנת הפרטיות. חובת מסירת ההודעה תאפשר לרשות להגנת הפרטיות להתגבר על פגיעה זו שכן היא תספק לה את המידע הדרוש למיטוב הפיקוח והאכיפה לפי החוק,[159] ותאפשר לה להשאיר "רמה מינימלית של הגנה על פרטיות".[160] ועדת החוקה קיבלה את עמדת הרשות להגנת הפרטיות בדבר הפגיעה הפוטנציאלית ביכולת הפיקוח שלה לנוכח צמצום חובת הרישום, והציעה כי חובת ההודעה תחול על כל מאגר מידע גדול של מידע בעל רגישות מיוחדת שאינו חייב ברישום.[161] לפיכך נקבע שחובת ההודעה תוטל על בעל שליטה במאגר מידע שבמאגר המידע שברשותו יש מידע בעל רגישות מיוחדת על 100,000 נושאי מידע או יותר. שר המשפטים, באישור ועדת החוקה, מוסמך לפטור סוגים של מאגרי מידע או של בעלי שליטה במאגר מידע מחובה זו.[162] מאחר שמידע בעל רגישות מיוחדת מוגדר בהרחבה, חובת מסירת ההודעה עשויה, למשל, לחול על מפלגה, תנועה או עמותה המחזיקה במאגר מידע הכולל מידע על דעות פוליטיות, אמונות דתיות או השקפות עולם של למעלה מ־100,000 נושאי מידע.[163]

158 סעיף 5 בהצעת החוק הממשלתית, לעיל ה"ש 51, המוסיף את סעיף 8(ג1) לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

159 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 95–97.

160 שם, בעמ' 75, דברי עו"ד גרסון.

161 שם, בעמ' 70.

162 ראו סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א(ב)(1), (3) לחוק הגנת הפרטיות.

163 ראו סעיף 2(5) בתיקון 13, שם, המתקן את סעיף 3 בחוק הגנת הפרטיות, הגדרת "מידע בעל רגישות מיוחדת".

על ההודעה לכלול את פרטי בעל השליטה במאגר המידע ואת דרכי ההתקשרות עימו, מידע על זהותו של הממונה על הגנת הפרטיות, אם מינויו נדרש לפי חוק הגנת הפרטיות, ודרכי ההתקשרות עימו, והעתק ממסמך הגדרות המאגר. ההעתק יספק לרשות להגנת הפרטיות מידע על פעולות איסוף המידע של בעל השליטה במאגר המידע, מטרות עיבוד המידע, סוגי המידע הכלולים במאגר, העברת המידע שבמאגר מחוץ למדינה, פעולות עיבוד מידע באמצעות מחזיק, והסיכונים העיקריים לאבטחת מידע והתמודדות בעל השליטה עימם.[164] על בעל השליטה במאגר המידע לעדכן את הרשות בדבר שינוי באחד מהפרטים האלה או על שינוי במסמך הגדרות המאגר.[165]

בגרסה הראשונה של חובת ההודעה כפי שהוצגה בדיונים בוועדה החוקה ביקשה הרשות להגנת הפרטיות לקבל כחלק מהדיווח גם "פרטים בדבר אופן קבלת ההסכמה לעיבוד המידע או מקור הסמכות המתיר עיבוד כאמור, ככל שעיבוד המידע כרוך בפגיעה בפרטיות". לשיטתה, פרטים אלו יאפשרו לה לבור את המוץ מן התבן ולמקד את מאמצי הפיקוח והאכיפה רק במאגרי המידע שיעוררו חשש לפגיעה בפרטיות מבין ההודעות הרבות שיקבלו.[166] ועדת החוקה ראתה בדרישת פרטים אלו נטל רגולטורי מיותר החותר גם תחת מטרת הוועדה להקל את הנטל הרגולטורי עם צמצום חובת הרישום. יתרה מזו, מדובר בפריט מידע שיחייב כל בעל שליטה במידע החב בחובת הודעה לפנות לעו"ד לקבל את חוות דעתו בעניין מקור הסמכות המתיר את עיבוד המידע, בעיקר במצב המשפטי הנוכחי, שבו ההסכמה היא הבסיס המשפטי החוקי היחיד לעיבוד מידע אישי העולה כדי פגיעה בפרטיות. נוסף על כך, ועדת החוקה סברה שהרשות להגנת הפרטיות רשאית ממילא לדרוש פרטים כאלה אם

164 תקנה 2(א)(1) לתקנות אבטחת מידע, לעיל ה"ש 84; פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 77.

165 ראו סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א(ב) לחוק הגנת הפרטיות.

166 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 73, דברי עו"ד אידלמן.

תראה בכך צורך מתוקף סמכותה לפקח על מילוי הוראות חוק הגנת הפרטיות לדרוש מכל אדם הנוגע בדבר למסור לה כל ידיעה או מסמך.[167]

3.3. סירוב, התלייה או ביטול רישום מאגר מידע

חוק הגנת הפרטיות לפני תיקון 13 העניק לראש הרשות להגנת הפרטיות, שכונה בו "רשם",[168] סמכות רחבה לסרב לרשום מאגר מידע. סירוב כאמור כמוהו כמניעה מוחלטת של עיבוד מידע המבוקש בבקשת הרישום:

> 10(א) הוגשה בקשה לרישום מאגר מידע –
>
> (1) ירשום אותו הרשם בפנקס, תוך 90 ימים מיום שהוגשה לו הבקשה, זולת אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או במסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין;

הצעת החוק הממשלתית ביקשה לשמר את הסמכות הרחבה הזאת של ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע, אך מתוך היפוך ברירת המחדל.[169] במקום ברירת המחדל, שלפיה אסור לבעל שליטה במאגר מידע להשתמש במידע שבמאגר לפני רישומו, הוצע שמרגע הגשת בקשה לרישום מאגר המידע יוכל בעל השליטה בו לעשות שימוש במידע האגור בו עד קבלת החלטה בבקשת הרישום. אם לא התקבלה החלטה בתוך 90 ימים מיום שהוגשה

167 סעיף 33 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 23י(א)(2) לחוק הגנת הפרטיות. פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 73–74, דברי יו"ר הוועדה, ח"כ רוטמן.

168 ראו סעיף 1(2) לתיקון 13, לעיל ה"ש 3.

169 סעיף 10(א)(1) בחוק הגנת הפרטיות לפני לתיקון 13, לעיל ה"ש 1, והתיקונים שהוצעו לו בסעיף 7(1) להצעת החוק הממשלתית, לעיל ה"ש 51.

בקשת הרישום, יכול בעל השליטה במאגר המידע לעשות בו שימוש אף ללא רישומו.[170]

הרשות להגנת הפרטיות הסבירה במהלך הדיונים בוועדת החוקה כי נעשה שימוש מצומצם בסמכות ראש הרשות לסרב לרשום מאגר מידע, וכי לרוב היא משתמשת בכלי זה כדי להכווין את התנהגות הארגונים בכל הקשור להגנה על הזכות לפרטיות. רישום מאגר המידע מותנה בכך שמבקש הרישום יפעל על פי ההנחיות שמנחה אותו הרשות להגנת הפרטיות בתגובה לבקשתו לרישום מאגר מידע.[171]

ועדת החוקה סברה שהסמכת ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע היא בעייתית. בהיעדר דין מהותי, החלטת ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע מבוססת על שיקול דעת רחב ונסתר שלו בשאלה אם המאגר מידע עשוי לשמש לפעילות בלתי חוקית או כמסווה לה, או שהמידע שבו התקבל בניגוד לכל דין. כך, למשל, במקרה של מאגר מידע הכולל מידע אישי שנאסף במהלך שיחות עם נציגי שירות לקוחות, מדובר בהחלטת ראש הרשות, על פי שיקול דעתו המוחלט בהיעדר דין מהותי ברור בשאלה אם המשך השתתפות נושא המידע בשיחה עם נציג שירות לאחר הודעה ש"השיחות מוקלטות לצורכי בקרה ושיפור השירות" מלמדת על הסכמתו מדעת לעיבוד המידע האישי שלמדה עליו בינה מלאכותית במהלך השיחה. בדיון בוועדת החוקה הועלה החשש שבהתחשב בסמכויות הפיקוח והענישה המשמעותיות שיוקנו לרשות בתיקון 13, תהפוך סמכות סירוב זו של הרשם לכלי רב עוצמה ומעורפל בידי הרשות להגנת הפרטיות, בניגוד לאופן שבו אמורה רשות שלטונית לפעול.

חשש זה מפני מתן סמכויות אכיפה וענישה מינהלית ופלילית בידי הרשות להגנת הפרטיות בהיעדר דין מהותי ברור בדבר המותר והאסור בעיבוד מידע

170 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר לסעיף 7(1) עד (3) עד (4) ו(6), בעמ' 431.

171 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 109, דברי עו"ד אידלמן.

אישי, מלבד דרישת ההסכמה הנתונה לפרשנות, חזר ועלה לאורך כל הדיונים בהצעת החוק הממשלתית ובתיקון 13 בוועדת החוקה.[172]

בסופו של דבר, סמכות ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע נותרה בעינה גם לאחר תיקון 13,[173] אולם ועדת החוקה פעלה לצמצום השימוש בה. לדוגמה, לצד חובת מסירת ההודעה ביקשה הרשות להגנת הפרטיות לעגן את סמכות ראש הרשות להגנת הפרטיות להורות לבעל שליטה במאגר מידע שאינו חייב ברישום לפי חוק הגנת הפרטיות לרשום את מאגר המידע בכל זאת "אם שוכנע כי הדבר דרוש לשם הבטחת קיום הוראות חוק זה לגבי מאגר המידע" ומטעמים מיוחדים שירשמו.[174] סמכות זו נגזרה מהסמכות שהוענקה כבר לרשם להורות על רישומו של מאגר מידע, גם אם מאגר זה פטור מחובת הרישום לפי הוראות החוק.[175] בדיון בוועדת החוקה הסביר היועץ המשפטי לרשות להגנת הפרטיות כי מטרת הסמכות הזאת היא לאפשר לרשות להגנת הפרטיות לפעול על בסיס המידע שתקבל מכוח חובת ההודעה, אך בלי להתחיל בהליך אכיפה. לשיטתו, אם במסגרת חובת ההודעה תקבל הרשות להגנת הפרטיות מידע על מאגר המצריך תשומת לב מיוחדת, היא תורה לבעל השליטה במאגר המידע שעליו לרשום את מאגר המידע. במסגרת הליך הרישום תוכל הרשות לתת לבעל השליטה במאגר המידע הנחיות, כפי שעשתה עד תיקון 13 מכוח סמכות ראש הרשות לסרב לרשום מאגר מידע,[176] בדבר הפעולות שעליו לנקוט כדי לקיים את

172 ראו למשל את דברי יו"ר ועדת החוקה, ח"כ רוטמן, בהתייחסו לקשיים הפרשניים הנלווים לסעיף 8 בהצעת החוק הממשלתית, לעיל ה"ש 51, ואת בקשתו להוסיף לחוק הגנת הפרטיות את סעיף 10ב ("איסור שימוש במידע ממאגר מידע בניגוד למטרה שלשמה נמסר": "הבעיה העקרונית ובאופן מעשי שאף אחד לא יודע מה מותר ומה אסור בתחום עיבוד המידע [...] אני מאחל לכם הצלחה באיך להגדיר את הבלתי־מוגדר. ואנחנו נעשה זאת, נגדיר את אשר לא ניתן להגדרה". ראו פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 60.

173 סעיף 6 בתיקון 13, לעיל ה"ש 3, המתקן את סעיף 10 בחוק הגנת הפרטיות.

174 סעיף 4(7) להצעת החוק הממשלתית, לעיל ה"ש 51, המתקן את סעיף 8(ה) בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

175 סעיף 8(ה) לחוק הגנת הפרטיות לפני לתיקון 13, לעיל ה"ש 1, וכן הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 430.

176 סעיף 10(א)(1) בחוק הגנת הפרטיות לפני לתיקון 13, לעיל ה"ש 1.

הוראות החוק "ובלי שזה יהיה הליך אכיפה". כך תוכל הרשות להגנת הפרטיות לפעול בסד זמנים קצר יותר מהליך אכיפה, ואולי אף למנוע פגיעה בפרטיות עוד לפני התרחשותה, או לעצור הפרות שייחשבו יעילות בעיני בעל השליטה במאגר המידע.[177] עמדתה זו של הרשות להגנת הפרטיות ממחישה יותר מכול את הקושי האמיתי שלה לפעול כדי להגן על הזכות לפרטיות בהיעדר הוראות חוק מהותיות המותאמות לעיבודי מידע דיגיטליים בהיקפים נרחבים הנעשים היום. חסר זה מוביל אותה לחפש דרכים להבהיר לבעלי שליטה במידע כיצד עליהם לפעול, מה מותר ומה אסור להם לעשות בכל הקשור בעיבוד מידע אישי, אף שאין בנמצא הוראות חוק ברורות בנושא.

ועדת החוקה סירבה, ובצדק, לתת סמכות שכזאת לראש הרשות להגנת הפרטיות. לשיטתה, סמכות זו פירושה הליך אכיפה לכל דבר, אך ללא שקיפות או כללים ברורים בעניין הסיבות לנקיטתו, והיא תאפשר לרשות להגנת הפרטיות להביא להפסקת עיבוד מידע במאגר מידע בנימוק של אי־רישום המאגר, גם במקרים שבהם לא נמצאה הפרה של הוראות חוק הגנת הפרטיות.[178] ועדת החוקה הבהירה שהרישום הוא חובה טכנית, ואי אפשר להעמיס עליה חובות מהותיות בדבר המותר והאסור בעיבוד מידע אישי בדרך של פרשנות.[179]

מנגד, ועדת החוקה חששה שכוחו של ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע לא יעמוד לו אם בעל השליטה במידע יהיה גוף ציבורי הכפוף, במישרין או בעקיפין, למשרד המשפטים ולייעוץ המשפטי לממשלה, שכן הרשות להגנת הפרטיות, למרות הכרת הממשלה בעצמאות שיקול דעתה,[180] כפופה

177 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 90, דברי עו"ד אידלמן, בעמ' 91, דברי עו"ד גרסון.

178 שם, בעמ' 91, דברי יו"ר ועדת החוקה, ח"כ רוטמן: "אתה בעצם אומר לו: לא מצאתי, אבל אני מורה לך להפסיק את ההפרה כי לא מצאתי. כי אני לא רוצה לנקוט נגדך הליך אכיפה, אז אני נוקט נגדך הליך אכיפה שאסור לך להחזיק את המאגר".

179 שם, בעמ' 94, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

180 החלטה מספר 1890 של הממשלה מיום 2.10.2022, **עצמאות הרשות להגנת הפרטיות ותיקון החלטת ממשלה**.

בהחלטותיה למשרד המשפטים. כדי להסיר את החשש הזה עמדה ועדת החוקה על כך שאם תהיה מחלוקת בסוגיות הקשורות בהחלטות אכיפה של הרשות להגנת הפרטיות תובא הסוגיה בפני בית המשפט, גם אם בעל השליטה או המחזיק הוא גוף ציבורי, והיא לא תופנה למנגנון יישוב סכסוכים פנימי בתוך הממשלה.[181]

סמכות נוספת שהרשות להגנת הפרטיות עמדה על שימורה היא סמכות ראש הרשות להתלות את רישומו של מאגר מידע או לבטלו אם מחזיק או בעל השליטה במאגר מידע הפר הוראה מהוראות החוק:[182]

> 10(ו) הפר מחזיק או בעל של מאגר מידע הוראות של חוק זה או התקנות לפיו או לא מילא אחרי דרישה שהפנה אליו הרשם, רשאי הרשם להתלות את תוקפו של הרישום לתקופה שיקבע או לבטל את רישומו של מאגר מידע בפנקס, ובלבד שקודם להתליה או לביטול ניתנה לבעל המאגר הזדמנות להשמיע את טענותיו.[183]

בוועדת החוקה עלה החשש שסמכות זו תפגע בשירות הניתן לאזרח, למשל, ברשויות מקומיות, שכן משמעותה היא שיש בסמכות ראש הרשות להגנת הפרטיות למנוע עיבוד מידע במאגר מידע אם מצא שהמחזיק שעימו התקשרה הרשות המקומית הפר את הוראות החוק. הרשות להגנת הפרטיות הבהירה כי השימוש שייעשה בסמכות להתלות את רישומו של מאגר מידע או לבטלו לחלוטין ייעשה במשורה, אולם אין היא מוכנה לוותר עליה לטובת הסתפקות בכלי האכיפה המינהלית ובהטלת עיצומים כספיים בלבד. לשיטתה, סמכות

181 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 116, סעיף 33 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף סעיף 23מה בחוק הגנת הפרטיות.

182 סעיף 10(ו) לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 39–43.

183 סעיף 10(ו) לחוק הגנת הפרטיות לפני תיקון 13, שם; סעיף 7(5) להצעת החוק הממשלתית, לעיל ה"ש 51, המציע לתקן את סעיף 10(ו) בחוק הגנת הפרטיות לפני תיקון 13.

זו היא בין הכלים האפקטיביים היחידים שיש בידה כדי להתמודד עם הפרות נמשכות מצד גופים ציבוריים. עם זאת, לא הוצגו בפני ועדת החוקה נתונים בדבר השימוש בסמכות זו על ידי הרשות להגנת הפרטיות. ועדת החוקה קיבלה עמדה זו, אך ביקשה להתוות את שיקול דעתו של ראש הרשות באמצעות הדרישה שהתלייה או ביטול רישומו של מאגר מידע תיעשה רק אם ראש הרשות "שוכנע כי הדבר נדרש בנסיבות העניין".[184] לפיכך, סעיף 10(ו) תוקן כך:

> 10(ו) הפר בעל שליטה במאגר מידע או מחזיק במאגר מידע הוראות של חוק זה או התקנות לפיו, או לא מילא אחר דרישה שהפנה אליו ראש הרשות, רשאי ראש הרשות להתלות את תוקפו של הרישום לתקופה שיקבע או לבטל את רישומו של מאגר המידע במרשם, אם שוכנע כי הדבר נדרש בנסיבות העניין, ובלבד שקודם להתליה או לביטול ניתנה לבעל השליטה במאגר או למחזיק במאגר הזדמנות להשמיע את טענותיו.[185]

184 פרוטוקול מס' 233, ליעיל ה"ש 57, בעמ' 39–43.

185 סעיף 8(7) בתיקון 13, ליעיל ה"ש 3, המתקן את סעיף 10(ו) בחוק הגנת הפרטיות.

פרק 4

החידושים העיקריים בתיקון 13 לעניין עיבוד מידע

4.1. עקרון צמידות המטרה

לפני תיקון 13 פורשו שני סעיפים בחוק כמעגנים את עקרון צמידות המטרה. משמעותו של העיקרון הזה היא שעיבוד המידע חייב להיעשות אך ורק (בצמידות) למטרה מסוימת. לפי פרשנות זו, סעיף 2(9) לחוק הגנת הפרטיות הוא הסעיף הראשון העוסק בעיקרון צמידות המטרה, וזו לשונו –

> 2. פגיעה בפרטיות היא אחת מאלה: [...]
> (9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסר;

סעיף החוק השני הרלוונטי לעניין עקרון צמידות המטרה הוא סעיף 8(ב) לחוק הגנת הפרטיות לפני לתיקון 13:

> 8(ב) לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

מאחר שצמצומה של חובת הרישום הוביל לצמצום המקרים שעליהם יחול סעיף 8(ב) ושבגין הפרתו תוכל הרשות להגנת הפרטיות להטיל עיצומים כספיים, הוצע בהצעת החוק הממשלתית לבטל את סעיף 8(ב) ובמקומו להוסיף את

סעיף 10ב המעגן במפורש איסור כללי להשתמש במידע ממאגר מידע שלא למטרה שלשמה נמסר:[186]

> 10ב. לא ישתמש בעל שליטה במאגר מידע או מחזיק במאגר, במידע, לרבות ידיעה על ענייניו הפרטיים של אדם אף שאינה בגדר מידע, ממאגר מידע, שלא למטרה שלשמה נמסרו, ולא ירשה לאחר מטעמו לעשות שימוש במידע או בידיעה כאמור.[187]

משרד המשפטים הסביר לאורך הדיונים שהוא מכיר בצורך לתקן את הדין המהותי בחוק הגנת הפרטיות ברוח ה־GDPR, ולהוסיף הוראות לעניין בסיסים חוקיים לעיבוד מידע וזכויות נושא המידע. אולם את זאת בכוונתו לעשות רק בתיקון עתידי. תיקון 13 ממוקד רובו ככולו בעיגון סמכויות אכיפה מינהליות לרשות להגנת הפרטיות ובהתאמת ההתאמות המינימליות הנדרשות בדין המהותי כדי לאפשר את העיגון הזה. אין בכוונת משרד המשפטים לתקן בתיקון 13 תיקונים בדין המהותי שיעוררו קשיים בתחום המותר והאסור בעיבוד מידע. לפיכך, סעיף 10ב המוצע רק מייבא, בשינויים מסוימים, את עקרון צמידות המטרה מסעיף 2(9) שבפרק א לחוק הגנת הפרטיות גם לעולם מאגרי המידע שבפרק ב'.[188]

ועדת החוקה חששה מהיווצרות מצב משפטי שבו עיבודי מידע שלא למטרה שלשמה נמסר המידע יותרו מכורח ההגנות,[189] העשויות לחול כאשר מופרת

186 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 428; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 5, דברי עו"ד יוסוב עמיר; פרוטוקול מס' 298 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ט"ז באדר ב' התשפ"ד (26 במרץ 2024), בעמ' 6–8, 23–24, דברי עו"ד יוסוב עמיר, עו"ד אידלמן ועו"ד גרסון.

187 סעיף 8 להצעת החוק הממשלתית, לעיל ה"ש 51, המציע להוסיף את סעיף 10ב לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

188 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 60, דברי עו"ד יוסוב עמיר; פרוטוקול מס' 298, לעיל ה"ש 187, בעמ' 2–3, דברי עו"ד יוסוב עמיר.

189 ההגנות מפורטות בפרק ג לחוק הגנת הפרטיות, לעיל ה"ש 3.

הוראת סעיף 2(9) לחוק הגנת הפרטיות. בעקבות זאת עלולה להיגרם פגיעה גדולה מאוד בזכות לפרטיות. להמחשה נתנה ועדת החוקה את הדוגמה הזאת: נושא מידע רוכש בקביעות פלסטרים ממכולת שכונתית. בעל המכולת מזהה כל צרכן לפי מספר צרכן שהוא מעניק לו ומנהל לעצמו וביוזמתו רישום של רכישותיו. את רישום הזה שומר בעל המכולת בקובץ שמור ומוגן בענן של חברת גוגל. חברת גוגל ניגשת למידע האגור על גבי הענן ומסיקה שלנושא המידע יש בעיה של קרישת דם ושולחת לו פרסומות על טיפולים המוצעים לבעיה זו. לכאורה, גוגל עושה שימוש במידע שלא למטרה לשמה נמסר, אולם היא תוכל להתגונן בטענה שהפגיעה בפרטיות נעשתה במהלך עיסוקה הרגיל של גוגל בהיותה מוכרת פרסומות, ולא דרך פרסום ברבים, כהוראת ההגנה הקבועה בסעיף 18(2)(ד) לחוק הגנת הפרטיות.[190]

נוסף על כך, ועדת החוקה העלתה את החשש שסעיף 10ב המוצע עשוי לעורר קשיים פרשניים בשאלה מהי המטרה שלשמה נמסר המידע. למשל, בעל שליטה ה"מגרד" מידע (data scraping) ממקורות גלויים באינטרנט ויוצר מאגר מידע, שהמידע שבו כלל לא נמסר לו. ביחס לדוגמה זו הסביר נציג הרשות להגנת הפרטיות שהתשובה מורכבת, שכן יש לבדוק מאילו אתרים נאסף המידע ומה היו תנאי השימוש שלהם, אולם הוא הכיר בעובדה שהוראת סעיף 10ב לא תחול על אדם העומד בכיכר העיר ויוצר בעצמו מאגר מידע על האנשים החולפים בה, משום שהמידע במאגר כאמור כלל לא נמסר לו.[191]

משרד המשפטים הסביר שגם היום, לנוכח הפרשנות המרחיבה של הוראת עקרון צמידות המטרה בסעיף 2(9) לחוק הגנת הפרטיות, עשויות פגיעות בפרטיות להיחשב מותרות מכוח ההגנות הקבועות בפרק ג לחוק. כמו כן, אם המידע לא נמסר מנושא המידע, עקרון צמידות המטרה המוצע בסעיף 10ב, ואף העיקרון

190 ההגנות הקבועות בסעיף 18(2)(ג) או 18(3) לחוק הגנת הפרטיות, לעיל ה"ש 3. פרוטוקול מס' 298, לעיל ה"ש 187, בעמ' 3–6, 23–24, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

191 פרוטוקול מס' 298, לעיל ה"ש 187, בעמ' 6–8, דברי יו"ר ועדת החוקה, ח"כ רוטמן, דברי עו"ד גרסון.

החל כיום לפי סעיף 2(9), אינו חל, שכן עקרון צמידות המטרה בסעיפים אלו מוגבל למידע שנמסר מנושא המידע בלבד. אם המידע נאסף ולא נמסר, מכל מקום אין שאלה מהי מטרת השימוש במידע, והמגבלות החלות על מידע הן מכוח סעיפי חוק אחרים, כגון חובת הסודיות הקבועה בסעיף 16 לחוק הגנת הפרטיות. אם כי בדוגמה של בעל המכולת לא ברור שהמידע על רכישותיו של הלקוח נאסף על ידי בעל המכולת ולא נמסר לו על ידי נושא המידע.[192]

גם לאחר ההסברים שסיפק משרד המשפטים נותרה עמדת ועדת החוקה בעינה. לשיטתה, הוראת סעיף 10ב המוצע יוצרת אי־בהירות גדולה, שכן במצב המשפטי הקיים לא ברור מה מותר ומה אסור. לכאורה, מי שאוסף מידע ממקורות גלויים ברחוב, אף אם עשה שימוש באמצעים טכנולוגיים לשם כך, כל עוד לא פגע בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות, לא יהיה כפוף לעקרון צמידות המטרה, משום שהמידע לא נמסר לו.[193]

נוסף על כך, בדיון בוועדת החוקה התקשו הנוכחים לעמוד על הצורך בסעיף 10ב ובשינוי המשפטי שייווצר בהיעדר תיקון לדין המהותי. נטען כי סעיף 10ב יוצר עקרון צמידות מטרה ביחס לעיבוד מידע אישי בהגדרתו הרחבה בתיקון 13, שהיא רחבה יותר מהפרשנות שניתנה עד כה לביטוי "ידיעה על ענייניו הפרטיים של אדם". בעקבות זאת, אם לא הוספו לחוק הגנת הפרטיות הוראות המאפשרות עיבוד מידע לפי בסיסים חוקיים לבד מהסכמה, מוטלת על בעל שליטה ומחזיק חובת צמידות מטרה רחבה יותר. כמו כן, עקרון צמידות המטרה גם אינו מאפשר גמישות לשם עיבוד מידע למטרה הדומה למטרה שלשמה נמסר המידע, כמו המנגנון הקבוע ב־GDPR.[194] כך, למשל, לכאורה הוראת סעיף 10ב עשויה למנוע מבעל שליטה להתמים מידע אישי, לאבטח אותו או לערוך מחקרים שטרם חשבו עליהם בעת מסירת המידע. כל זאת בתנאי שהתממה, אבטחת מידע או מחקרים מדעיים חדשניים הם שימושים שלא צוינו במטרות

192 שם, בעמ' 6–8, 23–24, דברי עו"ד יוסוב עמיר, עו"ד אידלמן ועו"ד גרסון.

193 שם, בעמ' 6–14, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

194 סעיף 5(1)(b) ב־GDPR, לעיל ה"ש 33; פרוטוקול מס' 298, לעיל ה"ש 187, בעמ' 15–17 דברי עו"ד רחום טוויג.

השימוש בעת מסירת המידע. אף ההגנות הקבועות בחוק הגנת הפרטיות לא יסייעו במקרה זה, שכן התממה או אבטחת מידע אינן עניין אישי כשר של בעל השליטה. יתרה מזו, ההגנות הקבועות בסעיף 18 לחוק הגנת הפרטיות, ובראשן הגנת תום הלב, יביאו דווקא להגנה פחותה על הזכות לפרטיות. לבעל שליטה שומר חוק יהיה תמריץ נמוך לבחון מראש אם מכלול השימושים שהוא מבקש לעשות עשוי להיחשב מנוגד למטרה שלשמה נמסר המידע, משום שבחינה עשויה לפגוע באפשרותו העתידית לטעון להגנת תום הלב.[195]

עוד הוצע בדיון בוועדת החוקה לוותר על הוראת סעיף 10ב המוצעת לחלוטין כדי להימנע מהקשיים הפרשניים שהיא מעוררת, לשמר את הוראת סעיף 8(ב) הקובעת צמידות מטרה למטרות המאגר ביחס למאגרי מידע שבכל זאת יחויבו ברישום, בעוד שעל יתר מאגרי המידע יחולו ממילא הוראת צמידות המטרה לפי סעיף 2(9) לחוק הגנת הפרטיות.[196]

לנוכח השאלות הפרשניות הקשות שעלו (למשל, מהי המטרה שלשמה נמסר המידע, מתי מידע ייחשב שנמסר ומתי ייחשב שנאסף ללא פנייה לנושא המידע), דרשה ועדת החוקה ממשרד המשפטים לנסח מחדש את הוראת סעיף 10ב, ומכל מקום הבהירה שעקב העמימות הנלוות לשאלה מהי המטרה שלשמה נמסר המידע לא יהיה אפשר להטיל עיצום כספי מיד עם גילוי הפרתו (מה שמכונה "עיצום חד שלבי"), אלא יהיה צורך לספק התראה בגין הפרתו, ורק אם אחרי מתן ההתראה לא תתוקן ההפרה, יהיה ניתן להטיל בגינה עיצום כספי (המכונה "מנגנון דו־שלבי להטלת עיצום כספי").[197]

בעקבות דרישת ועדת החוקה ויתר משרד המשפטים על הוספת סעיף 10ב. במקומה ביקש משרד המשפטים לתקן את הוראת סעיף 8(ב) בחוק הגנת

195 פרוטוקול מס' 298, ליל ה"ש 187, בעמ' 25–29, בעמ' 40, דברי עו"ד שגיא.

196 שם, בעמ' 14–15, דברי ד"ר אריאל הרשקוביץ, בעמ' 27, דברי עו"ד שגיא ועו"ד רחום טוויג, בעמ' 31 דברי עו"ד אור־חוף.

197 שם, בעמ' 44, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

הפרטיות לפני תיקון 13 לנוכח צמצום חובת הרישום. לפיכך, הוצע שעקרון צמידות המטרה המעוגן בסעיף האוסר על שימוש במידע ממאגר מידע שלא למטרה שלשמה הוקם המאגר יישמר אך יחול על כלל מאגרי המידע ולא רק על המאגרים החבים ברישום. אומנם, נציג משרד המשפטים הכיר בכך שהניסוח המוצע יעורר שאלות פרשניות, שכן כיצד תדע הרשות להגנת הפרטיות מהן המטרות לשמן הוקם המאגר אם בעל השליטה אינו נדרש לדווח לה עליהן עם הקמת המאגר כחלק מחובת רישום. אולם, הקושי האכיפתי מתגמד לנוכח חשיבות שימורו של עקרון צמידות המטרה בשתי מערכות הדינים הקיימות בחוק הגנת הפרטיות: הפרטיות הקלאסית, המוחלת גם על מידע באמצעות הפרשנות המרחיבה של הביטוי "ידיעה על ענייניו הפרטיים של אדם" בסעיף 2(9). מערכת הדינים השנייה היא הוראות פרק ב לחוק הגנת הפרטיות העוסקות בעיבוד מידע במאגר מידע, כלומר בפרטיות המידעית.[198]

גם על הצעה זו נמתחה ביקורת. ראשית נטען שהדרישה שעיבוד המידע ייעשה רק למטרה שלשמה הוקם המאגר היא דרישה סתמית, שכן למעשה גבולותיו של מאגר מידע אינם ברורים, ועל כן לא ברור מתי מוקם המאגר ומהי המטרה שנקבעה בעת הקמתו. יתרה מזו, בעל שליטה יכול לשנות את המטרות שלשמן הוקם המאגר בכל עת, כרצונו, כל עוד המטרה עומדת בגבולות המטרה שסופקה לנושא המידע בעת קבלת הסכמתו לאיסוף המידע. כאשר מדובר במאגר מידע הכולל מידע שלא נאסף ישירות מנושא המידע, גם מגבלה זו על שינוי המטרה שלשמה הוקם המאגר אינה קיימת. יתרה מזו, הוסבר כי במצב המשפטי שייווצר לאחר התיקון תהיה בחוק התייחסות לשלוש מטרות שונות זו מזו: בסעיף 2(9) לחוק הגנת הפרטיות מדובר במטרה שלשמה נמסרה הידיעה על ענייניו האישיים של אדם; בסעיף 8(ב) לפי התיקון המוצע – במטרה שלשמה הוקם המאגר; ובסעיף 11 לחוק הגנת הפרטיות המטיל את חובת יידוע נושא המידע – במטרה שלשמה מבוקש המידע. היחס בין המטרות אינו ברור, ויש חוסר בהירות פרשני בעניין מהות עקרון צמידות המטרה.[199]

198 פרוטוקול מס' 347 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ב בסיון התשפ"ד (18 ביוני 2024), בעמ' 2–3, דברי עו"ד יוסוב עמיר ועו"ד אידלמן.

199 שם, בעמ' 3–4, דברי עו"ד שגיא, דברי ד"ר חי.

לנוכח הקושי לאכוף עקרון צמידות מטרה מהותי כאשר נדרשת צמידות למטרה לשמה הוקם המאגר, הוצע לשנות את נוסח התיקון המוצע לסעיף 8(ב) ולדרוש שצמידות המטרה תהא למטרת המאגר על פי תקנה 2 בתקנות אבטחת מידע. במובן זה עקרון צמידות המטרה הנדרש יהיה אומנם פרוצדורלי, אך הוא יחייב את בעל השליטה לנסח כנדרש את מטרותיו במסמך הגדרות המאגר הנדרש לפי תקנות אבטחת מידע, מתוך היוועצות עם עו"ד בנושא. בדרך זו יישמר עקרון צמידות המטרה גם ביחס למאגרי מידע בפרק ב לחוק הגנת הפרטיות, אך לא יעורר קשיים פרשניים לנוכח החוסרים בדין המהותי בחוק הגנת הפרטיות.[200] עוד הוצע להוסיף לעקרון צמידות המטרה את הדרישה שהמטרה תהא מסוימת ומפורשת, כמו ב־GDPR,[201] כדי להגביר את השקיפות כלפי נושא המידע, לאפשר לו להבין לאיזו מטרה מעובד המידע האישי על אודותיו ולמזער את הסיכון שבעל השליטה יסתפק בניסוח מטרה כללית ומעורפלת בסגנון "לכל מטרה חוקית".[202]

לפיכך, הנוסח שהתקבל לבסוף בתיקון 13 הוא:

> 8(ב) לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין.[203]

הנוסח שהתקבל יוצר קישור למסמך מטרות המאגר, שבו נדרש בעל השליטה לפרט את מטרות המאגר, וכן מחייב שהמטרה תהא כדין. דרישה זו מסמלת את החיוב שהמטרה תהיה מסוימת ומפורשת.[204]

200 שם, בעמ' 7, דברי ד"ר אריאל הרשקוביץ.

201 בסעיף 5(1)(b) ל־GDPR, לעיל ה"ש 33.

202 פרוטוקול מס' 347, לעיל ה"ש 199, בעמ' 8–9, דברי עו"ד אור־חוף, בעמ' 13–14, דברי עו"ד מאוטנר לוגסי.

203 סעיף 4 בתיקון 13, לעיל ה"ש 3, המחליף את סעיף 8 בחוק הגנת הפרטיות.

204 סעיף 33 לתיקון 13, שם, המוסיף את סעיף 23כה(א) לחוק הגנת הפרטיות.

4.2. איסור עיבוד מידע אישי שנצבר או נאסף בניגוד להוראות חוק זה או כל דין אחר המסדיר עיבוד מידע והגנת תקנת השוק

הצעת החוק הממשלתית ביקשה להוסיף את ההוראה הזאת:[205]

> 8א. (א) לא ינהל אדם ולא יחזיק מאגר מידע אם המידע הכלול בו נוצר, התקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין המסדיר עיבוד מידע, אלא אם כן המידע נמסר לו בהתאם לדין, לא היה עליו לדעת על אי־החוקיות כאמור ובנסיבות העניין הפגיעה בפרטיות היא קלת ערך.
> (ב) מצא הממונה כי אדם ניהל או החזיק מאגר מידע בניגוד להוראות סעיף קטן (א) (בסעיף קטן ה – הפרה), רשאי הוא להודיע לו שמעשיו מהווים הפרה ולהורות לו להפסיק את ההפרה בתוך תקופה שיורה.

הוראה זו כוונה לשלב איסוף המידע, טרם עשיית השימוש בו, ובכך היא משלימה את עקרון צמידות המטרה שבסעיף 2(9) לחוק הגנת הפרטיות העוסק בשימוש במידע בניגוד למטרה לשמה נמסר. הוראה זו היא נגזרת מסמכות ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע אם לדעתו סביר שהמאגר משמש או עלול לשמש לפעולה בלתי חוקית, להסוואתה של פעולה, או שהמידע שבו נוצר, התקבל, נצבר או נאסף בניגוד לדין, ומשלימה אותה. כל זאת משום שהאיסור הקבוע בה יחול ללא קשר לתחולת חובת הרישום על מאגר המידע ולהפעלת סמכות ראש הרשות בהקשר הזה.[206]

205 סעיף 5 להצעת החוק הממשלתית, לעיל ה"ש 51, המציע להוסיף את סעיף 8א לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

206 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 430–431 וסעיף 7(1) המציע לתקן את סעיף 10(א)(1) בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1, וכן הדיון בסעיף 3.3 לעיל.

האיסור המוצע והקביעה שאי־ציות לו הוא הפרה, עוררו קושי שנבע מעיגונן של סמכויות אכיפה מינהלית משמעותיות לרשות להגנת הפרטיות בתיקון 13 וקביעת איסורים והפרות, בלי לתקן את הדין המהותי. ועדת החוקה חששה שהתשובה לשאלה מתי ייחשב שאיסוף, קבלה, צבירה או מסירה של מידע אישי למאגר מידע הם בניגוד לדין אינה ברורה.[207] חוסר בהירות זה רלוונטי במיוחד לארגונים מהמגזר הפרטי שמרביתם לא יחובו עתה ברישום, ואף לא יידרשו להודיע לנושא המידע לפי סעיף 11, שכן המידע שייאסף בהם לא ייאסף במסגרת פנייה לאדם.[208] עקב כך, נקודת המפגש הראשונה שלהם עם הרשות להגנת הפרטיות תהיה שאלת הפרת האיסורים בכל הקשור לניהול מאגר מידע ועיבוד חוקי של המידע שבו.[209] אולם היא תהיה גם מנת חלקם של גופים ציבוריים. אומנם אלו חייבים עתה ברישום, ולראש הרשות להגנת הפרטיות יש סמכות לסרב לרשום את מאגר המידע שברשותם ובכך למנוע את עיבוד המידע האישי על ידם טרם התחלתו,[210] אולם הרישום הוא טכני ואינו ערובה לחוקיות ניהול מאגר המידע ועיבוד המידע שבו.

בהיעדר בסיסים חוקיים לעיבוד מידע לבד מהסכמה, הקביעה אם המידע נאסף, נתקבל, נמסר או נצבר בניגוד לדין תלויה בפרשנות שתינתן לחוקים העוסקים בעיבודי מידע, לרבות לדרישת ההסכמה ולתחולת מופעי הפגיעה בפרטיות על נסיבות עיבוד מידע מסוימות.[211] לפיכך, כפי שהייתה לרשם סמכות לסרב לרישום מאגר מידע, גם כאן מדובר בסמכות רחבה לרשות להגנת הפרטיות שתופעל על פי שיקול דעתה ולפרשנותה.[212]

207 פרוטוקול מס' 233, ליל ה"ש 57, בעמ' 2, דברי עו"ד מנחמי, בעמ' 3, דברי יו"ר ועדת החוקה, ח"כ רוטמן; בעמ' 13, דברי עו"ד מרקביץ.

208 ראו הדיון בסעיף 3.1 לעיל.

209 סעיף 4 לתיקון 13, ליל ה"ש 3, המתקן את סעיף 8 בחוק הגנת הפרטיות.

210 ראו הדיון בסעיף 3.1 לעיל.

211 סעיף 1 ו־2 בחוק הגנת הפרטיות, ליל ה"ש 3.

212 פרוטוקול מס' 210, ליל ה"ש 84, בעמ' 117–118.

משרד המשפטים הבהיר כמה פעמים לאורך הדיונים שתיקון 13 אינו מוסיף איסורים ואינו מחדש בכל הקשור לעיבוד מידע. כפי שלפני תיקון 13 הוסמך ראש הרשות להגנת הפרטיות לסרב לרשום מאגר מידע אם סבר שהוא אינו חוקי, כך גם עתה. אבל כעת שאלה זו נבחנית במנותק משאלת הרישום. ביחס לארגונים מהמגזר הפרטי, כל מה שלא נאסר במפורש – מותר. ביחס לגופים ציבוריים, כל מה שנקבע שבסמכותם לעשות לפי חוק ועומד בהוראות חוק־יסוד: כבוד האדם וחירותו – מותר. למשל, אסור לעבד מידע במאגר מידע אם המידע נאסף, התקבל, נצבר, או נמסר מתוך הפרת סעיף 2(3) לחוק הגנת הפרטיות – צילום אדם ברשות היחיד ללא הסכמתו. אין לעבד מידע במאגר אם הוא נאסף ללא הודעה לנושא המידע על פי הוראת סעיף 11 לחוק הגנת הפרטיות או בניגוד להוראות פרק ד לחוק הגנת הפרטיות לעניין העברת מידע בין גופים ציבוריים,[213] ובלבד שבעל השליטה במאגר המידע או מי שממנו הוא קיבל את המידע שבמאגר המידע אינם יכולים ליהנות מאף אחת מההגנות המפורטות בחוק הגנת הפרטיות.[214]

הבהרה זו של משרד המשפטים לא סיפקה את ועדת החוקה, והיא עמדה על כך שבהיעדר בסיסים חוקים לעיבוד מידע אישי מדובר בשאלה פרשנית.[215] לכן נותר חשש מסוים מפני סמכות רחבה ומעורפלת לרשות להגנת הפרטיות שבצידה עיצום כספי.[216]

חשש נוסף שעלה בדיונים בוועדה החוקה נגע לכך שהצעת החוק הממשלתית ביקשה להטיל את האיסור על בעל השליטה ועל המחזיק. נטען שהמחזיק מקבל מאגר מידע שלם מבעל השליטה, ולרוב אינו יודע ואין ביכולתו לדעת אם המידע שבמאגר נאסף, נצבר, התקבל או נמסר בניגוד לחוק. הטלת איסור עיבוד מאגר

213 שם, בעמ' 119–120, דברי עו"ד יוסוב עמיר; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 2–3, 4, 5 דברי עו"ד יוסוב עמיר.

214 ההגנות המפורטות בסעיפים 18–20 לחוק הגנת הפרטיות, לעיל ה"ש 1.

215 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 117–118.

216 שם, בעמ' 120–123; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 11, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

מידע אם המחזיק ידע או היה עליו לדעת שהמידע שבו נאסף, נצבר או נתקבל בניגוד לחוק תוביל את המחזיק לברר בירורים שאינם מעניינו או מסמכותו. למשל, ספק שירותי עיבוד נתונים לבתי חולים מחזיק מאגר מידע שבבעלות בית החולים. הטלת איסור כאמור על המחזיק תוביל את אותו הספק לבדוק אם בית החולים אסף מידע על מטופליו כדין. כלומר, הטלת האיסור על המחזיק תטיל עליו בפועל חובה לערוך בדיקת נאותות לבעל השליטה, חובה שאינה מוטלת עליו לפי ההסדר לפני תיקון 13, ואף אינה מוטלת עליו בהסדרים הבינלאומיים כמו ה־GDPR. יתרה מזו, לרוב המחזיק, למשל במקרה של ספק שירותי ענן, אינו יודע ואינו יכול לדעת מהו המידע המוחזק במאגר המידע שהוא מעבד. לפיכך נטען כי די באיסור עיבוד מידע ללא הרשאה או בחריגה מהרשאה,[217] ואין צורך בהרחבת היקף האחריות של המחזיק מעבר לכך. כך, למשל, אם הרשות להגנת הפרטיות קובעת שהמידע שבמאגר המידע נאסף על ידי בית החולים שלא כדין, והיא תורה לבעל השליטה להפסיק את העיבוד, הוראה זו תועבר על ידי בעל השליטה למחזיק. אם המחזיק ימשיך בעיבוד המידע למרות הוראה שכזאת, עיבוד המידע ייעשה ללא הרשאה.[218] ועדת החוקה קיבלה לבסוף את העמדה הזאת.[219]

לצד האיסור הוספה בהצעת החוק הממשלתית הגנה שכונתה "תקנת השוק": אם המידע נמסר לאדם על פי דין, לא היה עליו לדעת על אי־החוקיות, ובנסיבות העניין הפגיעה בפרטיות היא קלת ערך, לא יחול האיסור ועיבוד המידע האישי שבמאגר המידע לא ייחשב הפרה.[220] בעקבות הדיונים בוועדת החוקה פוצלה הגנה זו, והיא מוענקת בשני מצבים:

217 סעיף 10ג להצעת החוק הממשלתית, לעיל ה"ש 51.

218 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 126; פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 41, 43–50.

219 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 50, דברי ח"כ רוטמן.

220 סעיף 5 בהצעת החוק הממשלתית, לעיל ה"ש 51, המציע להוסיף את סעיף 8א לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

האחד – בעל השליטה במאגר מידע לא ידע, או לפי מבחן אובייקטיבי לא היה עליו לדעת, שבמהלך חיי המידע שנמסר לו הופרה הוראת חוק הגנת הפרטיות או כל דין רלוונטי אחר.[221]

השני – הפגיעה בפרטיות היא קלת ערך. במקרה זה ההגנה תחול גם אם בעל השליטה ידע או היה עליו לדעת שהגורם שמסר לו את המידע פעל שלא כדין.[222]

במהלך הדיונים בוועדת החוקה התעורר החשש שהגנה שהוספה לא תחול אם בעל השליטה במאגר מידע "מגרד" מידע אישי (data scraping) ממקורות אחרים שבהם המידע פורסם, משום שפעולת גרידת מידע היא בפועל איסוף אקטיבי שלו, ואין גורם מזוהה המוסר את המידע לבעל השליטה במאגר המידע. כל זאת אף על פי שכאשר בעל שליטה במאגר מידע מגרד מידע אישי מאתרי אינטרנט שהמידע המפורסם בהם מתחזה לחוקי, הוא אינו יודע ולא היה עליו לדעת שהמידע האישי נוצר, התקבל, נצבר או נאסף באופן לא חוקי. כך, למשל, רשות המיסים אוספת מידע המפורסם ברשתות חברתיות, וכך מאתרת בעלי עסקים המעלימים מס. למשל, קוסמטיקאית הפועלת מחדר בביתה ואינה מדווחת על כך עלולה להיחשף אם תפרסם מידע על שירותיה בפייסבוק.[223] אם המידע על אודותיה יפורסם בלא ידיעתה או הסכמתה על ידי לקוחה שתפרסם עליה פוסט המלצה בפייסבוק, עלול המידע שייאסף בידי רשות המיסים להיחשב שנאסף שלא כחוק. ועדת החוקה פתרה חשש זה בקביעה שמוסר המידע הוא מי שמעלה את המידע לאתר אינטרנט, ושבכך הוא מוסר את המידע לכלל הציבור. מדברים אלו משתמע שהפרשנות הנכונה היא שהגנת תקנת השוק חלה גם כאשר מתבצעת גרידת מידע, ובלבד שבעל השליטה במאגר המידע לא ידע ולא היה עליו לדעת שהמידע שהוא מגרד נמסר על ידי גורם שפעל שלא כדין, ולחלופין גם אם בעל השליטה ידע או היה עליו לדעת על אי־החוקיות, הפגיעה היא קלת

221 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 39–58; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 17–21.

222 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 39–41.

223 נחמה פריזן "שטיינמץ עמינח: 'רשות המיסים עוקבת אחריכם גם ברשתות החברתיות'" **כלכליסט** (27.8.2019).

ערך.[224] למשל, בדוגמה של הקוסמטיקאית, רשות המיסים לא ידעה ולא היה עליה לדעת שפוסט ההמלצה פורסם שלא בהסכמתה של הקוסמטיקאית.

הוספת הגנת תקנת השוק לצד האיסור עצמו ולא כחלק מסעיפי ההגנות מעניקה לבעל השליטה במידע את שיקול הדעת לבחון ולהכריע בעצמו אם הפגיעה היא קלת ערך. ואולם, ועדת החוקה חששה שבהיעדר בסיסים חוקיים לעיבוד מלבד הסכמת נושא המידע במקרה של פגיעה בפרטיות, קביעת האיסור כחובה כללית ללא הגנת תקנת השוק בצמוד לה תעניק לראש הרשות להגנת הפרטיות בפועל שיקול דעת רחב לקבוע אם הייתה הפרה, ללא כללים ברורים ובהיעדר שקיפות. לפיכך הוחלט להותיר את הגנת תקנת השוק צמודה לאיסור.[225]

נוסח ההוראה שהתקבלה לבסוף בתיקון 13 הוא כדלקמן:

8(ד)(1) בעל שליטה במאגר מידע לא יעבד מידע אישי במאגר מידע ולא ירשה לאחר לעבד בעבורו מידע כאמור, אם המידע האישי הכלול במאגר המידע נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה או להוראות כל דין אחר המסדיר עיבוד מידע;

(2) נמסר מידע אישי לבעל שליטה במאגר מידע מגורם אחר, ובעל השליטה לא ידע ולא היה עליו לדעת כי אותו גורם פעל שלא כדין, לא יישא בעל השליטה במאגר המידע באחריות לפי סעיף קטן זה לעיבוד מידע אישי שבוצע לפני שידע או שהיה עליו לדעת כאמור;

224 פרוטוקול מס' 223, ליל ה"ש 57, בעמ' 56–58, ראו דבריו של ח"כ רוטמן בעמ' 57: "לקחת אותו מאחר. הוא מסר. בשנייה שהוא פרסם משהו בפומבי, בצורה שניתן לעשות עליו data scraping, הוא נמסר על ידי המחזיק בו לציבור. זה מה שהוא עשה. אז הוא נמסר, אתה אספת".

225 שם, בעמ' 52–53.

(3) הוראות פסקה (1) לא יחולו על הפרת דין קלת ערך בנסיבות העניין, ולעניין מידע אישי שנמסר כאמור בפסקה (2), אף אם בעל השליטה ידע או היה עליו לדעת.

נוסף על כך, לנוכח היעדר תיקון לדין המהותי, ועקב כך אי־הבהירות בנוגע למותר ולאסור בעיבוד מידע אישי, ביקשה ועדת החוקה לספק לבעל השליטה במאגר המידע ולמחזיק כלים להתמודד עם קביעה אפשרית של הרשות להגנת הפרטיות בדבר הפרת איסור זה. ראשית, האכיפה בגין הפרת האיסור על עיבוד מידע במאגר מידע שנצבר, נאסף, נתקבל או נמסר בניגוד לחוק היא דו־שלבית. אם ראש הרשות להגנת הפרטיות סובר שבעל השליטה במידע מפר את האיסור הזה, בסמכותו להודיע לבעל השליטה במידע שהוא מפר אותו ועליו להפסיק את ההפרה, רק לאחר מתן הזדמנות לבעל השליטה במאגר המידע להשמיע את טענותיו.[226] לבעל השליטה במאגר המידע אפשרות לערער על הוראה זו של ראש הרשות להגנת הפרטיות לבית משפט שלום.[227] אם בעל השליטה במידע אינו מגיש ערעור לבית המשפט או שערעורו נדחה, והוא אינו מקיים את הוראת ראש הרשות להגנת הפרטיות, אז בסמכות ראש הרשות להגנת הפרטיות להטיל עליו עיצום כספי.[228] אולם קודם להטלת העיצום על ראש הרשות להגנת הפרטיות למסור לבעל השליטה במאגר המידע הודעה על כוונת חיוב שלאחריה לבעל השליטה במאגר המידע האפשרות לטעון את טענותיו בפני ראש הרשות.[229] נוסף על כך, גם לאחר הודעה על כוונת חיוב, או אמצעי אכיפה אחר, שמורה לבעל השליטה במאגר המידע האפשרות להגיש ערעור לבית משפט השלום.[230]

226 סעיף 33 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 23כה(ב) לחוק הגנת הפרטיות.

227 סעיף 33 לתיקון 13, שם, המוסיף את סעיף 23כה(ו) לחוק הגנת הפרטיות.

228 סעיף 33 לתיקון 13, שם, המוסיף את סעיף 23כו(ה)(1)(ג) לחוק הגנת הפרטיות.

229 סעיף 33 לתיקון 13, שם, המוסיף את סעיף 23כז, 23כח לחוק הגנת הפרטיות.

230 סעיף 33 לתיקון 13, שם, המוסיף את סעיף 23מה לחוק הגנת הפרטיות.

כמו כן, ועדת החוקה הוסיפה לתיקון 13 את אפשרות לקבל חוות דעת מקדמית,[231] שניתן לעתור עליה לבית המשפט לעניינים מינהליים. אפשרות זו היא אפיק התמודדות נוסף עם יכולתה של הרשות להגנת הפרטיות להטיל עיצומים כספיים ולחסום עיבוד מידע על בסיס פרשנותה את דרישת ההסכמה או את מופעי הפגיעה בפרטיות שבסעיף 2 לחוק הגנת הפרטיות.[232]

עם זאת, סעיף 8(ד) שהתקבל בסופו של דבר בתיקון 13 ועיגן את איסור עיבוד המידע והגנת תקנת השוק עדיין מעורר קושי. כאמור, מידע במאגר המידע ייחשב ש"נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה או כל דין אחר המסדיר עיבוד מידע" אם הופרו הוראות מסוימות בחוק הגנת הפרטיות, כמו, למשל, סעיף 2, 11 או 23ד, או בדין אחר המסדיר עיבוד מידע. אולם, רק כאשר מופרת לכאורה הוראה מהוראות סעיף 2 לחוק הגנת הפרטיות, עומדת למפר הגנה מכוח סעיף 18 לחוק הגנת הפרטיות, ותיקון 13 אף הרחיבן והבהיר שהגנות אלו יחולו גם בהליך מינהלי.[233] כשהחשד הוא להפרת הוראות סעיף אחר, למשל, אי־מסירת הודעה לאדם כאשר נאסף ממנו מידע אישי על אודותיו לפי סעיף 11, לא תעמוד למפר כל הגנה,[234] למעט הגנת תקנת השוק, והאיסור לעבד את המידע שנתקבל מתוך ההפרה יעמוד בתוקפו. למשל, עיתונאי האוסף מידע אישי במהלך בילוש או התחקות מפר את סעיף 2(1) לחוק הגנת הפרטיות אך זכאי ליהנות מאחת מההגנות המעוגנות בסעיף 18 לחוק הגנת הפרטיות, ועל כן לא יימצא מפר את סעיף 8(ד)(1). אולם, אם איסוף המידע על

231 ראו הדיון בסעיף 4.5 לעיל.

232 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 14, 17 דברי יו"ר ועדת החוקה, ח"כ רוטמן. סעיף 24 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ט2 לחוק הגנת הפרטיות.

233 סעיף 25 לתיקון 13, שם, המתקן את סעיף 18 בחוק הגנת הפרטיות.

234 בדיוני ועדת החוקה אמר יו"ר הוועדה שלדעתו הרציונל למתן הגנה אינו תלוי בשאלה אם הפגיעה בפרטיות נעשתה בדרך של חשיפת פתק או שליחת דוא"ל, כלומר אם נעשתה בגבולות הפרטיות הקלאסיים או בעולמה של הגנת המידע. אלא כדי לקבוע אם תעמוד לרשות המפרה הגנת סעיף 18 יש לבחון את מהות ההפרה ואם היא פגיעה בפרטיות במהותה או אי־עמידה בדרישות טכניות, כמו למשל התקנת מערכת להגנת סייבר. ראו פרוטוקול מס' 351 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, י"ז בסיון התשפ"ד (23 ביוני 2024), בעמ' 23–27.

ידי העיתונאי לא הגיע לכדי בילוש או התחקות, אך נעשה ללא פנייה לאדם או יידוע שלו, כלומר מתוך הפרת סעיף 11 לחוק הגנת הפרטיות, לא יהיה זכאי העיתונאי להגנה כאמור ויימצא מפר את סעיף 8(ד)(1) לתיקון 13. יתרה מזו, בעל שליטה במאגר מידע המקבל מידע מעיתונאי יצטרך לבחון אם העיתונאי שהעביר לידיו את המידע עמד בהוראות החוק או נהנה מאחת מההגנות המפורטות בסעיף 18.[235]

4.3. איסור עיבוד ללא הרשאה

הצעת החוק הממשלתית ביקשה להוסיף איסור על שימוש או החזקה במידע ממאגר מידע בלא הרשאה.[236]

10ג. (א) לא ישתמש אדם במידע, לרבות ידיעה על ענייניו הפרטיים של אדם אף שאינה בגדר מידע, ממאגר מידע,[237] בלא הרשאה מאת בעל השליטה במאגר המידע או בחריגה מהרשאה כאמור.

(ב) לא יחזיק אדם במידע או בידיעה על ענייניו הפרטיים של אדם, ממאגר מידע, בלא הרשאה של בעל השליטה במאגר המידע או בחריגה מהרשאה כאמור; לעניין זה, "החזקה" – למעט החזקה באקראי ובתום לב.

235 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 17–21.

236 סעיף 8 בהצעת החוק הממשלתית, לעיל ה"ש 51, המציע להוסיף את סעיף 10ג לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

237 הניסוח המסורבל שהוצע כדי להבהיר כי איסור השימוש חל גם על מידע וגם על ידיעה על ענייניו הפרטיים של אדם נובע מהקושי להבחין בהבדל בין "מידע אישי" לפי ההגדרה הרחבה שאומצה בסעיף 2(5) בתיקון 13, לעיל ה"ש 3, המתקן את סעיף 3 בחוק הגנת הפרטיות, לבין "ידיעה על ענייניו הפרטיים של אדם" המופיעה בסעיף 2(9) לחוק הגנת הפרטיות. להרחבה ראו הטקסט הנלווה לה"ש 78–80 לעיל.

מטרת הוראה זו הייתה להבהיר שלמעט אחסון באקראי ובתום לב של מידע אישי, כל עיבוד מידע ממאגר מידע חייב להיעשות בהתאם להרשאה מבעל השליטה במאגר המידע.[238] בדיונים בוועדת החוקה הועלתה השאלה אם יש צורך בהגדרת מהות ההרשאה הנדרשת. מחד גיסא, מתן שם משתמש בלבד לא ייחשב מתן הרשאה לעיבוד מידע, מאידך גיסא, אין כוונה לחייב הרשאה פורמלית, כגון ייפוי כוח או "כתובה חתומה". ועדת החוקה קיבלה את עמדת משרד המשפטים שאין מקום להגדיר בחוק את מהות ההרשאה, והרשות להגנת הפרטיות רשאית לפרשה בגמישות, כפי שהיא עושה בהקשר של תקנות אבטחת מידע.

עם זאת, חלק מהנוכחים עמדו על כך שאיסור העיבוד ללא הרשאה ב־GDPR מבהיר במפורש שאפשר לעבד מידע אף בלא הרשאה, אם הדבר נדרש לפי חוק.[239] היעדר ציון מפורש של חריג זה בנוסח המוצע לסעיף 10ג בהצעת החוק הממשלתית עורר את חששם מצמצום עיבוד מידע לעיבוד שהתיר בעל השליטה בלבד. לפיכך, הובהר בדיון כי הוראת סעיף 35 בחוק הגנת הפרטיות, שלפיה "הוראות חוק זה לא יגרעו מהוראות כל דין אחר", עומדת בעינה. ולכן, אם יש דין ספציפי המתיר לעבד מידע באופן מסוים, עיבוד המידע בהתאם לדין זה אינו הפרה של איסור העיבוד ללא הרשאה.[240] כך, למשל, אם חברה המספקת שירות ניהול שכר מעבירה לבנק מידע אישי על עובדים לשם תשלום משכורותיהם, הבנק רשאי לעבד את המידע האישי שנמסר לו למטרות המותרות לו לפי החוק, למשל חוק מידע פיננסי,[241] אף אם ספקית שירותי ניהול השכר לא נתנה לא הרשאה לכך.

238 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 60.

239 סעיף 29 ל־GDPR, לעיל ה"ש 33.

240 הוראת סעיף 35 לחוק הגנת הפרטיות, לעיל ה"ש 3, מבהירה שהוראות חוק הגנת הפרטיות לא יגרעו מהוראות כל דין אחר, לרבות ביחס להרשאה בנוגע לעיבוד מידע. ראו גם פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 59–60.

241 חוק שירות מידע פיננסי, תשפ"ב–2021.

נוסף על כך, עקב הוספת המונח "עיבוד" בתיקון 13,[242] לא היה עוד צורך בהבחנה בין שימוש לבין החזקה, ולכן נוסח האיסור שהתקבל לבסוף הוא:

> 8(ג) לא יעבד אדם מידע אישי ממאגר מידע ללא הרשאה מאת בעל השליטה במאגר המידע או בחריגה מהרשאה כאמור.[243]

4.4. צו להפסקת פעולות עיבוד או למחיקת מידע אישי

במסגרת צמצום חובת הרישום וצמצום סמכות ראש הרשות לסרב לרשום מאגר מידע, להתלות את רישומו או לבטלו,[244] ביקשה ועדת החוקה להסדיר מנגנון מאוזן, שלא היה קיים בהצעת החוק הממשלתית, למתן הוראה להפסקת עיבוד מידע במאגר מידע בעקבות הפרת הוראות חוק הגנת הפרטיות.[245] מתוך הכרה בכך שהרשות להגנת הפרטיות היא רגולטור של המגזר הציבורי והפרטי כאחד, והחשש, שעליו עמדה ועדת החוקה פעמים רבות,[246] מפני חולשתה או חוסר יכולתה לפעול מול גופים ציבוריים, ההסדר שאומץ הוא צו הפסקה שיפוטי ולא מינהלי. אימוץ הסדר מינהלי נועד להפנות את הסוגיה לבית משפט לענייניים מינהליים ולמנוע מצב שבו הנושא ייפתר במסגרת מנגנון יישוב סכסוכים פנימי בתוך הממשלה. יתרה מזו, בקביעה שיהא זה צו שיפוטי ולא בסמכות ראש הרשות להגנת הפרטיות ביקשה ועדת החוקה לתת מענה לכך שחוק הגנת

242 ראו הדיון בסעיף 2.4 לעיל.

243 סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8(ג) לחוק הגנת הפרטיות.

244 ראו הדיון בסעיפים 3.1 ו־3.3 לעיל.

245 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 44–45, 91; פרוטוקול מס' 347, לעיל ה"ש 199, בעמ' 31–32, והדיון בסעיף 3.3 לעיל.

246 ראו הדיון בטקסט הנלווה לה"ש 181–182 לעיל.

הפרטיות חסר הוראות חשובות המבהירות את חוקיות עיבוד המידע בעידן הדיגיטלי, כגון בסיסי עיבוד חוקיים והגבלת מטרה.[247]

מטרת מנגנון צו הפסקת עיבוד היא לתת מענה למקרים שבהם יש לראש הרשות להגנת הפרטיות חשד סביר שמבוצעת, או עלולה להתבצע, הפרה חמורה של ההוראה האוסרת על שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה שלשמה נמסרה, על עיבוד מידע אישי במאגר מידע שלא למטרה שנקבעה לו כדין, ללא הרשאה או בחריגה ממנה, או למקרה שבו המידע האישי הכלול במאגר המידע נוצר, התקבל, נצבר או נאסף בניגוד לחוק הגנת הפרטיות או לכל דין אחר המסדיר עיבוד מידע, הפרת חובת אבטחת מידע, או מסירת מידע אישי מגוף ציבורי שלא בהסכמת נושא המידע, פרסומו או העמדתו לעיון רבים שלא לפי סמכות כדין (לפי סעיפים 2(9), 8(ב), (ג) או (ד), 17 או 23ב בחוק הגנת הפרטיות, בהתאמה). במקרה כזה יוכל ראש הרשות להגנת הפרטיות לפנות לבית המשפט לעניינים מינהליים בבקשה לתת צו לבעל השליטה במאגר המידע או למחזיק להפסיק את פעולות העיבוד הגורמות להפרה חמורה, או שיש חשש שיגרמו להפרה חמורה, של הוראות החוק האמורות, וכן, במידת הצורך, להורות על מחיקת המידע האישי שבמאגר המידע במלואו. בית משפט שהסוגיה תובא לפתחו יבחן אף הוא את סבירות החשד להפרה חמורה עכשיו או בעתיד, ואת מידתיות הסעד המבוקש בצו. במסגרת זו מחיקת מאגר מידע היא סעד קיצוני.[248]

ועדת החוקה עמדה על כך שהוראה להפסקה מוחלטת של עיבוד המידע במאגר המידע, שמשמעה בפועל מחיקת המידע, עשויה להביא להגנה על הזכות לפרטיות, אך בה בעת היא עלולה להוביל גם לפגיעה של ממש בחופש הביטוי. כך, למשל, מתן צו להפסקה מוחלטת של עיבוד המידע באתר אינטרנט המבקר את מערכת המשפט על ידי פרסום פומבי של פסקי דין. משום כך ביקשה ועדת

247 פרוטוקול מס' 347, לעיל ה"ש 199, בעמ' 31–38; פרוטוקול מס' 351, לעיל ה"ש 235, בעמ' 15–17, 33.

248 פרוטוקול מס' 347, לעיל ה"ש 199, בעמ' 31–32; פרוטוקול מס' 351, לעיל ה"ש 235, בעמ' 16–17.

החוקה לספק הגנה נוספת למקרים שבהם צו הפסקת עיבוד עלול להציב סיכון ממשי לחופש הביטוי, למשל, לחופש הביטוי של גופי תקשורת או גופי ביקורת.[249] לפיכך, בחינת הפגיעה האפשרית של הצו המבוקש בחופש הביטוי צוינה במפורש במתווה השיקולים שעל בית המשפט לשקול. נוסף על כך, נקבע שאם הצו ניתן במעמד צד אחד בלי שבעל השליטה או המחזיק שנגדם מוצא הצו מתגוננים בפני בית המשפט, לא יינתן צו מחיקה, ובכל מקרה תוקף הצו שינתן יהיה 48 שעות בלבד.[250]

לפיכך, נוסח הסעיף שאומץ בתיקון 13 הוא:[251]

23מט. (א) היה לראש הרשות יסוד סביר להניח כי מתבצעת או עומדת להתבצע במאגר מידע הפרה של הוראות לפי סעיף 2(9), 8(ב), (ג) או (ד), 17 או 23ב, רשאי הוא לבקש מבית משפט לעניינים מינהליים (בסעיף זה – בית המשפט) לתת צו לבעל השליטה במאגר המידע או למחזיק במאגר המידע, להפסקת פעולות עיבוד מידע הגורמות להפרה או שיש חשש שיגרמו להפרה (בסעיף זה – צו הפסקה), וכן רשאי בית המשפט להורות לשם כך על מחיקת המידע האישי שבמאגר המידע במלואו (בסעיף זה – צו מחיקה).

(ב) בית המשפט רשאי לתת צו לפי סעיף קטן (א), כפי שהתבקש או בשינויים, אם שוכנע כי התקיימו כל אלה:

(1) יש יסוד סביר להניח כי מתבצעת או עומדת להתבצע במאגר מידע הפרה כאמור באותו סעיף קטן;

(2) אין אמצעי אחר שפגיעתו פחותה למניעת ביצוע ההפרה;

249 פרוטוקול מס' 347, לעיל ה"ש 199, בעמ' 33, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

250 שם, בעמ' 38, 42; פרוטוקול מס' 351, לעיל ה"ש 235, בעמ' 17, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

251 סעיף 33 לתיקון 13, לעיל ה"ש 3 המוסיף את סעיף 23מט בחוק הגנת הפרטיות.

(3) הנזק שעלול להיגרם כתוצאה מההפרה עולה על הנזק שעלול להיגרם ממתן הצו הנוגע אליה, ובכלל זה הפגיעה בחופש הביטוי שעלולה להיגרם ממתן הצו;

(4) חומרת ההפרה מצדיקה את מתן הצו.

(ג) (1) צו לפי סעיף זה יינתן לאחר שניתנה לבעל השליטה במאגר המידע הזדמנות להשמיע את טענותיו לפני בית המשפט, ואם הצו מופנה כלפי מחזיק – גם למחזיק, ככל שהדבר ניתן, ובדרך המתאימה בנסיבות העניין.

(2) צו הפסקה שלא במעמד צמד כאמור בפסקה (1) יינתן לתקופה שלא תעלה על 48 שעות; בתקופה כאמור לא יינתן צו מחיקה.

(3) בית המשפט רשאי להאריך את תוקפו של הצו לאחר שניתנה לבעל השליטה במאגר המידע או למחזיק במאגר המידע, לפי העניין, הזדמנות להשמיע את טענותיו.

(ד) בית המשפט רשאי לדון מחדש בצו לפי סעיף זה אם ראה שהדבר מוצדק בשל נסיבות שהשתנו או עובדות חדשות שהתגלו לאחר מתן הצו.

(ה) על הליך לפי סעיף זה יחולו הוראות חוק בתי משפט לעניינים מינהליים, התש"ס–2000, בשינויים המחויבים; שר המשפטים, באישור ועדת החוקה, רשאי לקבוע הוראות לעניין סדרי דין בהליך לפי סעיף זה; עד לקביעת הוראות כאמור, יחולו הוראות תקנות האזרחות (סדרי הדין בבקשה לביטול אזרחות), התשע"ז–2017, בשינויים המחויבים.

4.5. חוות דעת מקדמית

בעבר נהגה הרשות להגנת הפרטיות לתת חוות דעת במענה לשאלות שנשלחו אליה בנוגע לפרשנות הוראות חוק הגנת הפרטיות. עם זאת, אסדרת האפשרות

לפנות לרשות להגנת הפרטיות לשם קבלת חוות דעת מקדמית "בעניין עמידת מאגר המידע בדרישות חוק זה או ההוראות לפיו לעניין עיבוד המידע במאגר המידע" לא הוצגה בהצעת החוק הממשלתית. במהלך הדיונים בוועדת החוקה החליטה הוועדה שיש לקבוע מסגרת ברורה בחוק, שמשולבים בה גם לוחות זמנים, לפנייה ולקבלה של חוות דעת מקדמית מהרשות להגנת הפרטיות, כדי ליידע את כלל הציבור הרלוונטי באפשרות קבלת מענה לשאלות הקשורות בחוק הגנת הפרטיות מהרשות להגנת הפרטיות. עיגונה של האפשרות לקבלת חוות דעת מקדמית בא גם במקום הצעת הרשות להגנת הפרטיות לעגן בתיקון 13 מנגנון לרישום וולונטרי, שבו ראתה הרשות נקודת מפגש בינה לבין מעבד המידע, שתאפשר לה לחוות את דעתה בשאלות הקשורות לחוקיות מאגר המידע. ועדת החוקה מצאה שאין ברישום כדי לתת מענה לתהייה של בעל שליטה או מחזיק אם עיבוד המידע שבמאגר המידע הוא חוקי, בעיקר בהיעדר שינוי בדין המהותי והוספת הוראות בדבר בסיסים חוקיים לעיבוד מידע אישי.[252]

עם זאת, הרשות להגנת הפרטיות חששה מעיגונו של מתווה שיחייב אותה לספק חוות דעת מקדמית בכל עת שתתבקש לעשות זאת, מה שעשוי להוביל להצפת הרשות בבקשות לחוות דעת מקדמית שרובן עשויות להיות מיותרות, ולבזבוז משאביה היקרים. לפיכך נקבע כי רק בעל שליטה או מחזיק עכשוויים, או מי שעתיד לשלוט או להחזיק במאגר מידע בעתיד הנראה לעין, יוכלו לפנות בבקשה לקבלת חוות דעת מקדמית. נוסף על כך, עוגנו סוגים של בקשות, שביחס אליהן ועל פי הנסיבות שיפורטו בנוהל על ידי ראש הרשות, תהיה הרשות רשאית לסרב לתת חוות דעת. למשל, אם הבקשה נגועה בחוסר ניקיון כפיים, או שהטיפול בה ידרוש הקצאת משאבים בלתי סבירה.[253]

252 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 109–110, דברי יו"ר ועדת החוקה, ח"כ רוטמן; פרוטוקול מס' 249 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ז בשבט התשפ"ד (6 בפברואר 2024), בעמ' 128–131.

253 פרוטוקול מס' 249, לעיל ה"ש 253, בעמ' 129, דברי יועמ"ש הרשות להגנת הפרטיות, עו"ד אידלמן, בעמ' 132 דברי ראש הרשות להגנת הפרטיות, עו"ד סממה וסגן יועמ"ש הרשות להגנת הפרטיות, עו"ד גרסון, בעמ' 131–133, דברי יו"ר ועדת החוקה, ח"כ רוטמן והיועצת המשפטית של ועדת החוקה, עו"ד מנחמי; סעיף 24 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ט2 לחוק הגנת הפרטיות.

פרק 5

החידושים העיקריים בתיקון 13 לעניין חובות בעל השליטה או המחזיק

5.1. חובת הודעה לנושא המידע

סעיף 11 לחוק הגנת הפרטיות לפני תיקון 13 עיגן את חובת ההודעה לנושא המידע, כך:

> 11. 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.

תיקון חובת ההודעה לא נכלל בהצעת החוק הממשלתית, אלא נעשה ביוזמת ועדת החוקה שביקשה להשוותו עד כמה שאפשר להוראה המקבילה ב־GDPR.[254] במסגרת זו ביקשה הוועדה להחיל את חובת ההודעה בכל מקרה של עיבוד מידע אישי על אודות נושא מידע, ולא רק כאשר עיבוד המידע נעשה במסגרת פנייה אליו,[255] כפי שה־GDPR מחייב, בחריגים מסוימים, את בעל השליטה במידע

254 סעיפים 13 ו־14 ל־GDPR, לעיל ה"ש 33.

255 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 36, דברי עו"ד מנחמי.

להודיע לנושא המידע על איסוף המידע על ידו בעת איסוף המידע אם המידע האישי נאסף מנושא המידע עצמו,[256] ובתוך חודש מקבלת המידע האישי על אודות נושא המידע אם המידע אינו נאסף ישירות מנושא המידע.[257] גם חוק פרטיות הצרכנים בקליפורניה (California Consumer Privacy Act, להלן: CCPA) מטיל בחוק ובתקנות מכוחו חובת הודעה דומה על "business",[258] בעת איסוף המידע או לפניו.[259] בתקנות מכוחו של ה־CCPA מובהר שמטרת חובת ההודעה היא לספק לצרכנים כלים לשליטה ממשית בשימוש שעושים Business במידע האישי עליהם.[260] ה־CCPA אינו עוסק כלל בשאלה אם מידע אישי נאסף ישירות מנושא המידע או בדרכים אחרות, שכן חובת ההודעה היא חלק מזכות נושא המידע להיות מיודע (the right to be informed).[261] עם זאת, מובהר בו שאפשר ליישם את חובת ההודעה בעת איסוף המידע האישי או לפני כן באמצעות פרסום מדיניות פרטיות.[262] התקנות מכוחו של ה־CCPA מספקות דוגמאות לנסיבות שבהן תיושם חובת ההודעה באמצעות פרסום מדיניות פרטיות. כך, למשל, אם צד א מפעיל אתר אינטרנט ומאפשר לצד ב לשלוט באיסוף המידע האישי על הגולשים באתר האינטרנט שלו, על צד א לכלול מדיניות פרטיות באתר שלו, ועל צד ב לפרסם גם כן מדיניות פרטיות באתרים שבבעלותו, או לכלול את המידע הדרוש במדיניות הפרטיות של צד א. סוחרי מידע הרשומים במרשם סוחרי המידע אינם נדרשים לפרסם מדיניות פרטיות אם כללו את הפרטים הדרושים בבקשת הרישום, לרבות הסבר כיצד לקוחות יכולים לבקש opt-out ממכירה או משיתוף של מידע אישי על אודותיהם.[263]

256 GDPR, לעיל ה"ש 33 , בסעיף 13.

257 שם, בסעיף 14.

258 CCPA, לעיל ה"ש 47, בסעיף 1798.140(d) – הגדרת business

259 שם, בסעיף 1798.100(a).

260 ראו California Consumer Privacy Act Regulations, תקנה 7012(a)-(f).

261 ראו CCPA, לעיל ה"ש 47, בסעיף 1798.110.

262 שם, בסעיף 1798.100(b).

263 ראו California Consumer Privacy Act Regulations, בסעיף 7012(g)-(i). תוכנה של מדיניות הפרטיות מפורט בתקנה 7011.

ההיגיון שבחובת ההודעה בשני החוקים – ה־GDPR וה־CCPA – הוא זכות נושא המידע להיות מיודע, שהיא חלק מחובת השקיפות (transparency), שמטרתה להבטיח שבעלי השליטה במידע יפעלו בהגינות ובאחריותיות בכל הקשור לעיבוד מידע אישי על ידם או מטעמם. חובת שקיפות זו נועדה להגביר את אמון נושאי המידע בתהליך עיבוד המידע המשפיע עליהם על ידי הגברת ההבנה שלהם את התהליך ואת אתגריו ומתן כלים בידם לדרוש את זכויותיהם בקשר עליו. משום כך, חובת ההודעה חלה על כל בעלי השליטה במידע, ואין לשונות בין בעלי השליטה במידע כל משקל.[264]

ואולם, במהלך הדיונים בוועדת החוקה הובעה התנגדות, הן מצד נציגי המגזר הפרטי, הן מצד משרד המשפטים, לתיקון דומה של חובת ההודעה בחוק הגנת הפרטיות. הנימוק העיקרי להתנגדויות היה שתיקון 13 אינו כולל תיקון לדין המהותי. בעיקר, חסרה בתיקון הוספה של בסיסים חוקיים לעיבוד מידע, ובעקבות זאת רק עיבוד מידע המגיע כדי פגיעה בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות מחייב את קבלת הסכמת נושא המידע. חוק הגנת הפרטיות אינו עוסק במקרים אחרים של עיבוד מידע.[265] הרחבת חובת ההודעה בלא הרחבה דומה של הנסיבות שבהן מותר לבעל שליטה לעבד מידע אישי תטיל זרקור על כל המקרים האפורים שבהם ארגונים במגזר הפרטי וגופים ציבוריים מעבדים מידע אישי על נושאי מידע ללא יכולת ממשית לאתרם או לפנות אליהם לשם קבלת הסכמתם, אך לכאורה אינם מגיעים עד כדי פגיעה בפרטיות.

לבסוף תוקנה חובת ההודעה הקבועה בסעיף 11 לחוק הגנת הפרטיות כך:[266]

264 Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (Adopted on 29 Nov., 2017, as last Revised and Adopted on 11 April, 2018). ראו גם CCPA, לעיל ה"ש 47, בסעיף 1798.110.

265 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 36–38.

266 סעיף 8 לתיקון 13, לעיל ה"ש 3, המתקן את סעיף 11 בחוק הגנת הפרטיות.

11. פניה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע תלווה בהודעה שיצוינו בה –

(1) אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו ומהי תוצאת אי־ההסכמה;

(2) המטרה אשר לשמה מבוקש המידע;

(2א) שמו של בעל השליטה במאגר המידע, ודרכי ההתקשרות עמו;

(3) למי יימסר המידע ומטרות המסירה.

(4) קיומן של זכות עיון במידע האישי לפי סעיף 13 ושל זכות לבקש תיקון של המידע האישי לפי סעיף 14.

לפי תיקונים אלו נדרש שההודעה תכלול מידע בנוגע להשלכות אי־הסכמתו של נושא מידע לעיבוד מידע על אודותיו, את פרטי הקשר של בעל השליטה במידע, וכן מידע על זכויותיו של נושא המידע לעיין במידע האישי עליו ולבקש את תיקונו.[267] המדובר בתיקונים חשובים שיש בהם כדי לשפר את שקיפות עיבוד המידע, לבסס את הסכמתו מדעת של נושא המידע לעיבוד מידע אישי על אודותיו, וכן לצמצם את פערי הכוחות הקיימים לעיתים בין נושא המידע לבעל השליטה במאגר מידע. כך, למשל, באמצעות החיוב לפרט את תוצאותיה של אי־הסכמה לעיבוד מידע אישי יהיה אפשר להבהיר לנושא המידע שאי־הסכמתו לעיבוד מידע אישי על אודותיו לאו דווקא תוביל למניעת שירות או מוצר ממנו. לדוגמה, אם קופת חולים פונה בבקשה לאסוף מידע אישי לצורכי מחקר לפני בדיקת דם, אי־ההסכמה למסירת המידע האישי לא תוביל לאי־ביצוע בדיקת הדם לנושא המידע.[268] עם זאת, חובת ההודעה לא הורחבה כך שתחול בכל מקרה של עיבוד מידע אישי, גם אם העיבוד אינו מבוצע על בסיס פנייה לנושא המידע. עקב כך, הרחבתה עלולה להוביל לתוצאות מטעות במקרים מסוימים. למשל, אם נעשית פנייה לאדם לשם איסוף מידע אישי, אולם לא נדרשת הסכמתו לאיסוף ולעיבוד המידע, או אם ההסכמה שתינתן על ידו היא חסרת משמעות. הדוגמה הקלאסית לכך היא יחסי עבודה. אם מעסיק מודיע לעובדיו הודעה במסגרת מדיניות הגנת פרטיות בדבר איסוף ועיבוד המידע האישי שלהם, על

267 שם.

268 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 138–139.

העובד לא חלה חובה חוקית למסור את המידע. אולם נוכח יחסי הכוחות בין המעסיק לעובד להסכמת העובד ניתנת ממילא משקל נמוך,[269] ועל כן אין מקום לעסוק גם בתוצאות אי־ההסכמה. לו היו מוספים לחוק הגנת הפרטיות בסיסים חוקיים לעיבוד מלבד מהסכמה, מצב אבסורדי זה לא היה מתרחש.

5.2. חובת אבטחת מידע ומינוי ממונה אבטחת מידע

חובת אבטחת מידע היא החובה המוטלת על בעל שליטה ועל מחזיק כדי להגן על מידע אישי שברשותם מפני גישה, שימוש או חשיפה בלתי מורשים. חובה זו הוספה לחוק הגנת הפרטיות לפני כשני עשורים, בתיקון מס' 4, היא חובה כללית המוטלת על בעל מאגר המידע, המחזיק ומנהל המאגר,[270] והיא לא שונתה מאז. כך קבע סעיף 17 לחוק הגנת הפרטיות לפני תיקון 13:

> 17. בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.

הצעת החוק הממשלתית ביקשה לתקן את סעיף 17 ולהוסיף סמכות ספציפית לשר המשפטים להתקין תקנות גם בנושא האחריות לאבטחת מידע. סמכות ספציפית זו תתווסף לסמכות הכללית של השר להתקין תקנות המעוגנת בסעיף 36 לחוק הגנת הפרטיות. כן ביקשה הצעת החוק להציג הסדרים ייחודיים

269 להרחבה ראו רחל אריאלי הרשקוביץ **עובדים מרחוק: הזכות לפרטיות העובדים ושמירה עליה באמצעות דוקטרינת ההפרה התורמת** (מחקר מדיניות 202, המכון הישראלי לדמוקרטיה 2025), 54–75.

270 הצעת חוק הגנת הפרטיות (תיקון מס' 2) (מאגרי מידע), התשנ"ד–1994, דברי ההסבר בעמ' 153.

להתקנת תקנות בתחום הגנת הסייבר וביחס לאבטחת מידע בגופי ביטחון.[271] נוסח התיקון שהוצע היה –

9. בסעיף 17 לחוק העיקרי, האמור בו יסומן "(א)" ואחריו יבוא:

(ב) (1) השר רשאי לקבוע הוראות לעניין האחריות לאבטחת המידע הקבועה בסעיף קטן (א) ובסעיף 17ב(ב), ובכלל זה היקפה והחובות הכלולות בה, וכן לעניין דרכי אבטחת המידע כאמור, בין השאר בעניינים אלה:

(א) הגנה פיזית ולוגית על המאגר;

(ב) סדרי הניהול וכללי העבודה במאגר המידע ובקשר אליו, לרבות לעניין קביעה על הגבלות על גישה של מועסקים למידע.

(2) בתקנות לפי פסקה (1), יכול שייקבעו הוראות שונות לגבי מאגרים בעלי מאפיינים שונים.

(3) תקנות לפי פסקה (1) יותקנו בהסכמת ראש הממשלה, ולעניין תקנות כאמור שיחולו על גופים המנויים בפרטים 2 ו־3 בתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1988 (להלן: חוק להסדרת הביטחון בגופים ציבוריים) – גם בהתייעצות עם שר הביטחון.[272]

בדיון בוועדת החוקה הוחלט להסיר את מנהל המאגר מרשימת בעלי התפקידים האחראים לאבטחת מידע, מתוך תפיסה שהאחריות מוטלת בראש ובראשונה על בעל השליטה, ותפקיד מנהל המאגר רלוונטי, אם בכלל, רק בגופים ציבוריים. כמו כן עמדה ועדת החוקה על כך שכל התקנות שיתקבלו על ידי השר חייבות באישור הוועדה.[273] לפיכך, נוסח סעיף 17 המתוקן הוא:

271 הצעת החוק הממשלתית, לעיל ה"ש 51, דברי ההסבר בעמ' 433.

272 סעיף 9 להצעת החוק הממשלתית, לעיל ה"ש 51, המתקן את סעיף 17 בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

273 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 43–44, דברי עו"ד מנחמי; סעיף 15 לתיקון 13, לעיל ה"ש 3, המתקן את סעיף 17 בחוק הגנת הפרטיות.

בסעיף 17 לחוק העיקרי –

(1) האמור בו יסומן "(א), ובו, במקום הרישה עד המילים "מנהל מאגר מידע" יבוא "בעל השליטה במאגר מידע ומחזיק במאגר מידע";

(2) אחרי סעיף קטן (א) יבוא:

"(ב) (1) שר המשפטים, בהסכמת ראש הממשלה ובאישור ועדת החוקה, רשאי לקבוע תקנות לעניין האחריות לאבטחת המידע הקבועה בסעיף קטן (א) ובסעיף 17ב(ב), ובכלל זה היקפה והחובות הכלולות בה, וכן לעניין דרכי אבטחת המידע כאמור, בין השאר בעניינים אלה:

(א) הגנה פיזית ולוגית על המאגר;

(ב) סדרי הניהול וכללי העבודה במאגר המידע ובקשר אליו, לרבות לעניין קביעה של הגבלות על גישה של מועסקים למידע.

(2) בתקנות לפי פסקה (1), יכול שייקבעו הוראות שונות לגבי מאגרי מידע בעלי מאפיינים שונים.

(3) תקנות לפי פסקה (1) שיחולו על גופים המנויים בפרטים 2 ו־3 בתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים – יותקנו גם בהתייעצות עם שר הביטחון.

נוסף על כך, בנושא אבטחת מידע הוצע בהצעת החוק הממשלתית לתקן גם את סעיף 17א בחוק הגנת הפרטיות לפני תיקון 13, שפירט את נסיבות ספציפיות של אבטחת מידע בידי מחזיק:

17א. (א) מחזיק מאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר.

(ב) מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מהמאגרים נקבעו הזכרים

> בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

השינוי העיקרי שהוצע בהצעת החוק הממשלתית בהקשר הזה הוא ביטולו של סעיף קטן 17א(ב),[274] מתוך הבנת הנטל שההוראה מטילה על מחזיקים והעובדה שחלות עליהם חובות עדכון אחרות במסגרת הצעת החוק הממשלתית, כגון החובה לדווח על שינוי בפרט מהפרטים הנכללים בבקשת הרישום.[275]

במהלך הדיון בוועדת החוקה טענו נציגי המגזר הפרטי כי גם ההוראה בסעיף קטן 17א(א) מיותרת, מכיוון שהרשאות גישה נקבעות ממילא בתקנה 15 לתקנות אבטחת מידע. ההוראה בסעיף 17א(א) אינה מתאימה לעולם הדיגיטלי כיום שבמסגרתו ההחלטה בדבר מורשי גישה היא בניהול עצמי של בעל השליטה, באמצעות ממשק ייעודי להוספה והסרה של מורשי גישה. משום כך, הדרישה שהמחזיק יוודא שמורשי הגישה יהיו רק מי שנקבעו בהסכם עם בעל השליטה מטילה נטל כבד על מחזיקים, ויתרה מזו, היא אינה בת־ביצוע. נציג משרד המשפטים הסביר שאומנם נושא הרשאות הגישה מוסדר בתקנות אבטחת מידע, אולם לדעתו, אף שאין הדבר מצוין בבירור בלשון הסעיף, מהות הוראת סעיף 17א(א) היא לחייב מחזיק להבטיח הפרדה בין מאגרי מידע, כדי לוודא שלכל בעל שליטה תהא גישה אך ורק למאגרים שלו. ועדת החוקה קיבלה את עמדת נציגי המגזר הפרטי בנושא וקבעה כי סעיף 17א כולו מיותר, שכן הנושא מטופל טיפול מקיף בתקנות אבטחת מידע. לפיכך בוטל הסעיף במלואו.[276]

אשר לחובה למנות ממונה אבטחת מידע, קבע סעיף 17ב בחוק הגנת הפרטיות לפני תיקון 13 כי –

274 סעיף 10 בהצעת החוק הממשלתית, לעיל ה"ש 51, המציע לתקן את סעיף 17א בחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

275 הצעת החוק הממשלתית, לעיל ה"ש 51 לעיל, דברי ההסבר בעמ' 434; פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 44, דברי עו"ד אידלמן.

276 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 45–46.

17ב. (א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן: הממונה):
(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;
(2) גוף ציבורי כהגדרתו בסעיף 23;
(3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.
(ב) בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).
(ג) לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.[277]

צמצום חובת הרישום[278] הובילה למעשה לצמצום חובת אבטחת המידע לפי סעיף 17ב(א)(1), שכן מספר מאגרי המידע החייבים ברישום צומצם.[279] נוסף על כך, בדיון בוועדת החוקה הסבירו נציגי המגזר הפרטי שפעמים רבות המחזיק כלל אינו יודע אם מאגרי המידע שברשותו חייבים ברישום. למשל, ספק שירותי אחסון מספק שירותי אחסון מוצפנים ואינו יודע אם מאגר המידע שאוחסן בשרתים שלו חייב ברישום לפי חוק הגנת הפרטיות.[280] תחילה ביקשה ועדת החוקה לבחון להטיל את חובת מינוי ממונה אבטחת מידע על בעל שליטה, על פי רגישות המידע שבמאגר או מספר נושאי המידע, בלי קשר לחובת הרישום, ולגזור מחובת בעל השליטה את חובת מינוי ממונה אבטחה על ידי המחזיק, בהנחה שבעל השליטה יודע פרטים אלו על המאגר שבשליטתו, ומתוך רצון להימנע מלהטיל על מחזיק חובה לבדוק את תוכן המידע במאגר המידע

277 סעיף 15 בתיקון 13, לעיל ה"ש 3, המתקן את סעיף 17 בחוק הגנת הפרטיות.

278 ראו דיון בסעיף 3.1 לעיל; פרוטוקול מס' 334, לעיל ה"ש 128 לעיל, בעמ' 16–23.

279 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 16–24.

280 פרוטוקול מס' 265 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"א באדר התשפ"ד (20 בפברואר 2024), בעמ' 49–51, דברי עו"ד שגיא.

שהוא מחזיק.[281] אולם, במהלך הדיונים ונוכח הוספת חובת מינוי ממונה הגנת פרטיות,[282] חששה ועדת החוקה מפני ריבוי גורמים מקבלי החלטות הנושאים באחריות לנושא הגנת פרטיות ואבטחת מידע. כך, למשל, כאשר עירייה היא בעלת השליטה, יהיה עליה למנות כמה בעלי תפקידים: מנכ"ל העירייה או מי מטעמו הוא מנהל המאגר, בעל תפקיד שנותר רלוונטי בגופים ציבוריים; כן יהיה על העירייה למנות ממונה הגנת פרטיות וממונה אבטחת מידע. מאחר שסביר שעיבוד המידע, לפחות בכל הנוגע לאחסון, ייעשה בדרך של מיקור חוץ, הרי שגם מחזיק, ממונה הגנת פרטיות וממונה אבטחת מידע שימונו על ידו יהיו רלוונטיים לשאלת האחריות להגנת פרטיות ולאבטחת מידע באותו המאגר.[283]

לפיכך, ולנוכח תפיסתה של ועדת החוקה שבכל הנוגע למגזר הפרטי די בקביעת חובת אבטחת מידע ויש לצמצם את מידת התערבותה של המדינה בהתנהלותו של ארגון מהמגזר הפרטי, נבחנה גם האפשרות לבטל לחלוטין את חובת מינוי ממונה אבטחת מידע במגזר הציבורי בגופים שאינם מעבדי מידע גדולים. אולם, בסופו של דבר החליטה ועדת החוקה לעדכן את רשימת הגופים החבים במינוי ממונה אבטחת מידע, מכמה נימוקים. ראשית, הוועדה סברה שיש להמתין ולהפיק לקחים מהשלכות תיקון 13, ובעיקר מצמצום חובת הרישום והחיוב במינוי ממונה הגנת פרטיות. שנית, הוועדה הסבירה שצמצום חובת הרישום מביא ממילא לצמצום נפקותה המעשית של חובת מינוי ממונה אבטחת מידע, וגם כך החובות המהותיות לעניין אבטחת מידע הקבועות בתקנות אבטחת מידע. ולבסוף, ועדת החוקה נתנה דעתה להשלכות השליליות העלולות להיות לביטול החיוב במינוי ממונה אבטחת מידע על החשיבות שייחסו לנושא ארגונים במגזר הפרטי.[284]

281 שם, בעמ' 52–53, דברי עו"ד מנחמי ודברי יו"ר ועדת החוקה, ח"כ רוטמן.

282 ראו דיון בסעיף 5.3 להלן.

283 פרוטוקול מס' 336 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ז באייר התשפ"ד (4 ביוני 2024), בעמ' 29–38.

284 פרוטוקול מס' 334, ליל ה"ש 128, בעמ' 17–20, דברי יו"ר ועדת החוקה, ח"כ רוטמן; פרוטוקול מס' 336, ה"ש 284 לעיל, בעמ' 37–39, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

לפיכך עודכנה בתיקון 13 הגדרת הגופים החייבים במינוי ממונה אבטחת מידע, והם כוללים עתה בעלי שליטה בחמישה מאגרי מידע לפחות החייבים ברישום או במסירת הודעה לרשות להגנת הפרטיות, או מחזיקים של מאגרי מידע כאמור.[285]

לשון סעיף 17ב לאחר תיקון 13 היא:

17ב. (א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע:
(1) בעל שליטה בחמישה מאגרי מידע החייבים ברישום או בהודעה לפי סעיף 8א או מחזיק בחמישה מאגרי מידע כאמור;
(2) גוף ציבורי כהגדרתו בסעיף 23;
(3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.
(ב) בלי לגרוע מהוראות סעיף 17, הממונה על אבטחת המידע יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).
(ג) לא ימונה כממונה על אבטחת מידע מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

5.3. חובת מינוי ממונה הגנת פרטיות

חובת מינוי ממונה על הגנת פרטיות היא חובה חדשה בדין הישראל, והיא לא נכללה כלל בהצעת החוק הממשלתית. עם זאת, כבר בתחילת הדיונים בוועדת החוקה עמדו נציגי החברה האזרחית על חשיבות ממונה הגנת פרטיות בארגון

285 ראו סעיף 17 לתיקון 13, לעיל ה"ש 3, המתקן את סעיף 17ב בחוק הגנת הפרטיות; פרוטוקול מס' 249, לעיל ה"ש 253, בעמ' 117–118; פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 37–39.

בהיותו אמצעי למזעור סיכוני הפגיעה בפרטיות.[286] במהלך הדיונים בנוגע לתפקיד "מנהל מאגר" והצורך בו,[287] עמדה גם ועדת החוקה על הצורך בהוספת חובת מינוי ממונה הגנת הפרטיות, ואילו נציג משרד המשפטים הסביר שהנושא אמור להיכלל בתיקון 15 העתידי לחוק הגנת הפרטיות.[288] ועדת החוקה עמדה על דרישתה לצמצם את החיוב במינוי מנהל מאגר לגופים ציבוריים בלבד ולהוסיף מנגנון לחיוב במינוי ממונה הגנת הפרטיות, בין השאר לנוכח הצורך ליישר קו עם רגולציה בינלאומית בנושא והחשש מפני הפיכתה של מדינת ישראל לחצר האחורית לפגיעה בפרטיות.[289]

משרד המשפטים נענה לדרישת ועדת החוקה להוספת ההוראות בנוגע למינוי ממונה הגנת פרטיות כבר בתיקון 13, כדי ליצור בעל תפקיד בגוף פרטי ובגוף ציבורי שיהיה בעל הידע, המומחיות, הכישורים והסמכויות להבטיח את מילוי הוראות חוק הגנת הפרטיות בכל הקשור לעיבוד מידע אישי בגוף שהוא עובד בו.[290] אולם, לפני הצגת הצעת משרד המשפטים להוספת הוראות אלו נעשתה עבודת הכנה מקיפה. במסגרת עבודה זו נערכו כמה מפגשים מקוונים בהשתתפות היועצת המשפטית של ועדת החוקה, עו"ד נעמה מנחמי, נציגי אשכול פרטיות ומידע, ממחלקת ייעוץ וחקיקה (ציבורי חוקתי) במשרד המשפטים, עו"ד לירון מאוטנר לוגסי, ועו"ד עמית יוסוב עמיר, נציגי הייעוץ המשפטי ברשות להגנת הפרטיות, ובראשם עו"ד ראובן אידלמן, חוקרים ומומחים אקדמיים בתחום הפרטיות (ובהם כותבת המחקר הזה), ועורכי דין מהתעשייה ומהמגזר הפרטי.[291] מפגשים אלו היו דוגמה להתוויית רגולציה על בסיס שיח שיתופי עם גורמים מרכזיים

286 ראו, למשל, פרוטוקול 190 מישיבת ועדת החוקה, חוק ומשפט, יום שני, כ"א בכסלו התשפ"ד (4 בדצמבר 2023), בעמ' 4–5, דברי עו"ד גבע, נציגת המועצה להגנת הפרטיות; פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 105.

287 ראו הדיון בסעיף 2.3.3 לעיל.

288 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 29–39; פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 8, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

289 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 24, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

290 פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 16.

291 פרוטוקול מס' 334, לעיל ה"ש 128 , בעמ' 16, דברי עו"ד יוסוב עמיר.

שכל הצדדים והציבור בכללותו מרוויחים ממנו. המפגשים אפשרו לנציגי משרד המשפטים והרשות להגנת הפרטיות להציג את עמדותיהם ואת חששותיהם מקביעת הסדרים רגולטוריים בלתי מספקים, לנציגי המגזר הפרטי לשקף את המתרחש בפרקטיקה ואת הלך הרוח של לקוחותיהם בנושא מינוי ממונה הגנת הפרטיות, ולנציגי החברה האזרחית לתרום מהידע שלהם על רגולציות מקבילות במשפט המשווה ועל השלכותיהם, ולשקף את אינטרס הציבור בהתוויית רגולציה מתאימה. כך, למשל, בתחילה סברו במשרד המשפטים וברשות להגנת הפרטיות שממונה הגנת הפרטיות צריך לבוא במקום ממונה אבטחת מידע. אולם לאחר השיח המשותף והעמדה הנחרצת שהציגו מרבית המשתתפים בדבר חשיבות תפקיד ממונה אבטחת מידע בארגון, הוחלט במשרד המשפטים שחובת מינוי ממונה אבטחת מידע, שהייתה קיימת כבר בחוק הגנת הפרטיות לפני תיקון 13,[292] לא תבוטל עקב הוספת חובת מינוי ממונה הגנת פרטיות.[293] בתום המפגשים פורסמה להערות הציבור הצעת משרד המשפטים בשיתוף עם הייעוץ המשפטי של ועדת החוקה להוספת הוראות בנוגע למינוי ממונה הגנת פרטיות ששימשה בסיס לדיון בנושא בוועדת החוקה.[294]

לפי ההצעה שהוצגה בוועדת החוקה, ארגון יחוב במינוי ממונה הגנת פרטיות בהתקיים אחד מהתנאים האלה:

17ב1 חובת מינוי ממונה על הגנת הפרטיות

(א) הגופים המפורטים להלן חייבים במינוי ממונה על הגנת הפרטיות:

(1) בעל שליטה או מחזיק במאגר מידע הכולל מידע בכל רגישות מיוחדת על אודות 200,000 אנשים או יותר.

(2) מי שמחזיק במאגרי מידע שונים של חמישה בעלי שליטה שונים או יותר.

292 ראו הדיון בסעיף 5.2 לעיל.

293 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 17, דברי עו"ד יוסוב עמיר.

294 פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 16.

(3) גוף ציבורי כהגדרתו בסעיף 23, למעט גוף ביטחוני כהגדרתו בסעיף 23יח.

(4) בעל שליטה במאגר מידע הכולל מידע על אודות 100,000 אנשים או יותר ומתקיים בו אחד מאלה:

(א) המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה.

(ב) מטרתו העיקרית של המאגר היא איסוף מידע אישי לצורך מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר כהגדרתו בסעיף 3.

(ב) שר המשפטים רשאי לקבוע, באישור ועדת החוקה, סוגים נוספים של גופים עליהם תחול חובת מינוי ממונה על הגנת הפרטיות.[295]

תנאים אלו שיקפו דרישות פורמליסטיות בלבד ועוררו את החשש שגם במקרים שבהם לא ייעשה עיבוד מידע מהותי ולא תהיה סכנה אמיתית לפרטיות, בכל זאת יוטל על ארגונים נטל בירוקרטי וכלכלי כבד של מינוי בעל תפקיד ייחודי לממונה הגנת הפרטיות. למשל, כאשר עירייה עושה מיקור חוץ זניח שבמסגרתו מעבירים רשימת טלפונים ושמות של תושבי העיר כדי לשלוח להם סקר ומאגר המידע נמחק בתוך זמן קצר לאחר הסקר.[296]

יתרה מזו, ועדת החוקה חששה שהכללים הפורמליסטים יובילו לחיוב סטטוטורי במינוי ממונה הגנת פרטיות, ועקב כך עלול להיווצר ריבוי בעלי תפקידים בלא מנגנון הכרעה או קביעת אחריות ברורה ביניהם. למשל, כאשר עירייה עושה מיקור חוץ למאגר מידע שברשותה, ללא קשר לרגישות המידע שבמאגר, היקפו או מטרות העיבוד, יהיו לפחות ארבעה בעלי תפקידים שתהיה להם דעה בנוגע להגנת הפרטיות ולאבטחת המידע בו – ממונה הגנת פרטיות וממונה אבטחת מידע מצד המחזיק, וכן שני בעלי התפקידים האלה מצד בעל השליטה. אף

295 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 28–29.

296 שם, בעמ' 33.

שוועדת החוקה הכירה בחשיבות שיש גם לממונה אבטחת מידע וגם לממונה הגנת פרטיות מבחינת שיפור רמת הגנת הפרטיות בארגון, נחיצותה של החובה הסטטוטורית במינוי ממונה הגנת הפרטיות הן אצל בעל השליטה, הן אצל המחזיק, לא הייתה בעיניה ברורה דיה. יתרה מזו, הוועדה סברה שמינוי סטטוטורי הוא התערבות יתר של המחוקק בניהול הפנימי של הארגון. לשיטתה, אם בעל שליטה הוא גוף ציבורי ממילא הוא יחוב במינוי ממונה הגנת פרטיות, ועדיף להשאיר לשיקול דעתו את השאלה אם יש צורך במינוי ממונה הגנת פרטיות גם אצל המחזיק שעימו הוא מתקשר. חיוב סטטוטורי במינוי בכל מקרה שמאגר המידע כולל למעלה מ־200,000 נושאי מידע מוציא מידי בעל השליטה או המחזיק את שיקול הדעת בנוגע לניהול הסיכונים ולא בהכרח יביא לשיפור בהגנת הפרטיות. למשל, לפי תנאי המינוי שהוצעו, עירייה או מועצה מקומית תחזיק ברוב המקרים מאגרי מידע על למעלה מ־200,000 נושאי מידע. במצב זה, לא רק שהיא צריכה להחזיק ממונה הגנת פרטיות בהיותה גוף ציבורי, יהיה עליה גם לחייב את המחזיק שהיא מתקשרת עימו לצורך עיבוד המידע להחזיק ממונה הגנת פרטיות וממונה אבטחת מידע, בלי קשר לסוג המידע שהיא מעבירה אליו, היקפו או מטרות העיבוד.[297] מנגד, עורכי הדין מהמגזר הפרטי עמדו על חשיבות חיוב סטטוטורי במינוי ממונה הגנת פרטיות בעיקר במקרים שבהם בעל השליטה אינו ארגון גדול וחזק אלא דווקא הצד החלש במערכת היחסים עם המחזיק. למשל, חברת סטרט־אפ המתקשרת לקבלת שירותי אחסון עם Amazon Web Services.[298]

לפיכך ביקשה ועדת החוקה לבחון אם ומתי יש להבחין בין חבות בעל שליטה לחבות מחזיק, וכן האם וכיצד להטיל חובת מינוי ממונה הגנת פרטיות על מחזיק שאינו יודע כלל מהו המידע המוחזק על ידו. למשל, מחזיק המספק שירותי ענן מוצפנים בלבד ואינו יכול, וגם איננו רוצים לאפשר לו, לדעת מה מוחזק במאגר המידע שאוחסן בשרתיו.[299]

297 שם, בעמ' 35–38, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

298 שם, בעמ' 39, דברי עו"ד רבינוביץ.

299 שם, בעמ' 42.

נוסף על כך, נציגי המגזר הפרטי והחברה האזרחית הדגישו בדיון את החשיבות שבעיגונם של מדדים מהותיים, ברוח ה־GDPR,[300] המתמקדים בבחינת ליבת הפעילות המבוקשת ובסיכון שהיא מסכנת את הזכות לפרטיות, ואת היותם התנאים שלפיהם תוטל על בעל שליטה או על מחזיק חבות מינוי ממונה הגנת פרטיות. כך, למשל, ניתן לבחון את סוג המידע במאגר המידע, את מטרות עיבוד המידע ואת סוגי העיבוד המבוקשים כמדדים מהותיים להטלת חובת מינוי ממונה הגנת פרטיות. התמקדות במדדים המהותיים תאפשר קורלציה נכונה בין מידת הסיכון הטמון בעיבוד המידע לזכות לפרטיות לבין ניהול סיכונים ראוי.[301] נציגי משרד המשפטים והרשות להגנת הפרטיות הדגישו כי אימוץ הוראות ברוח ה־GDPR להטלת חובת מינוי ממונה הגנת פרטיות טומן בחובו סיכון שיש לתת עליו את הדעת, משום שכלל פורמליסטי נוקשה יהיה קל לאכיפה ונהיר יותר, ואילו כללים המתמקדים בהיבטים המהותיים של פעולות העיבוד עושים שימוש במונחים עמומים שיחייבו פרשנות. פרשנות זו תינתן על ידי הרשות להגנת הפרטיות, והיא תוכל להטיל קנסות מינהליים בהתאם. התוצאה, חששה ועדת החוקה, תהא מתן שיקול דעת מוחלט כמעט לרשות להגנת הפרטיות לקבוע כיצד על כל ארגון לנהל את הסיכונים הטמונים בפעולותיו לזכות לפרטיות, ואם למנות ממונה הגנת פרטיות אם לאו. המדובר בשיקול דעת כמעט מוחלט, שכן ניתן לערער על החלטה מינהלית שתקבל הרשות להגנת הפרטיות. אולם, במרבית המקרים בתי המשפט ייטו שלא להתערב בשיקול דעתה המקצועית של הרשות.[302]

הפשרה שהתקבלה לבסוף שיקפה את רצון הרשות להגנת הפרטיות בכלל פורמליסטי וקל לאכיפה, לצד השאיפה לאמץ הסדר עמום הבוחן את המאפיינים המהותיים של פעולת העיבוד והסיכון שנשקף ממנה לזכות לפרטיות, אך מתוך מזעור החשש ממתן שיקול דעת מוחלט לרשות להגנת הפרטיות. כך, התנאים לחיוב במינוי ממונה הגנת הפרטיות הם שילוב של כלל פורמליסטי לצד תנאים כלליים וגמישים ברוח ה־GDPR:

300 סעיף 37(1) ל־GDPR, לעיל ה"ש 33.

301 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 40–42.

302 שם, בעמ' 44–46.

17ב1. (א) הגופים המפורטים להלן חייבים במינוי ממונה על הגנת הפרטיות:

(1) בעל שליטה במאגר מידע שהוא גוף ציבורי כהגדרתו בסעיף 23 או מחזיק במאגר מידע כאמור, למעט גוף ביטחוני כהגדרתו בסעיף 23כ;

(2) בעל שליטה במאגר מידע שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, ויש במאגר מידע אישי על יותר מ־10,000 בני אדם;

(3) בעל שליטה במאגר מידע או מחזיק במאגר מידע שעיסוקיו העיקריים כוללים פעולות עיבוד מידע או כרוכים בפעולות כאמור, אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר, ובין היתר ספק מורשה המספק שירות רדיו טלפון נייד לפי חוק התקשורת (בזק ושידורים), התשמ"ב–1982, וספק שירות חיפוש מקוון או מי שעיסוקו העיקרי כרוך בפעולות אלה;

(4) בעל שליטה במאגר מידע או מחזיק במאגר מידע שעיסוקו העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר, ובין השאר תאגיד בנקאי כהגדרתו בחוק הבנקאות (שירות ללקוח), התשמ"א–1981, מבטח כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ"א–1981, בית חולים כללי כמשמעותו בפקודת בריאות העם, 1940, וקופת חולים כהגדרתה בחוק ביטוח בריאות ממלכתי, התשנ"ד–1994.

(ב) לעניין פסקאות (3) ו־(4) שבסעיף קטן (א) – עיבוד מידע בהיקף ניכר יהיה בין השאר בשים לב למספר בני האדם שמידע מעובד לגביהם, לשיעורם באוכלוסייה מסוימת, להיקף המידע, לכמותו ולטווח של סוגי המידע המעובד,

למשך ולתדירות של פעולות העיבוד, למשך שמירת המידע
ולתחום הגיאוגרפי של פעולות העיבוד.[303]

לפי הכלל הפורמליסטי, כל אחד משלושת הגופים הבאים חב בחובת מינוי ממונה הגנת פרטיות:[304]

(1) בעל שליטה במאגר מידע, שהוא גוף ציבורי כהגדרתו בסעיף 23 לחוק הגנת הפרטיות (למשל רשות מקומית או משרד ממשלתי), למעט גוף ביטחוני כהגדרתו בסעיף 23כ בחוק הגנת הפרטיות (למשל, צה"ל או משטרת ישראל);

(2) מחזיק של בעל שליטה במאגר מידע שהוא גוף ציבורי כאמור;

(3) בעל שליטה במאגר מידע שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, כלומר סוחר מידע, ובלבד שבמאגר המידע יש מידע אישי על יותר מ־10,000 נושאי מידע.

לצד הכלל הפורמליסטי, חלה חובת מינוי ממונה הגנת פרטיות בהתקיים אחד מהתנאים המהותיים. תנאים אלו שואבים השראה, עד כדי זהות, מהוראות ה־GDPR. משום כך יהיה אפשר להישען בבחינת תחולתם על פרשנותם באיחוד האירופי. נוסף על כך, הם חלים בצדק על בעל שליטה במאגר מידע ועל מחזיק, משום שמחזיק ממלא תפקיד מפתח בעיבוד המידע האישי, ויש לו השפעה רבה על היקף הגנת הפרטיות ועל הציות לחוק.

(1) בעל שליטה במאגר מידע או מחזיק, "ש**עיסוקיו העיקריים** כוללים פעולות עיבוד מידע או כרוכים בפעולות כאמור, אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר".[305] הסעיף אף כולל דוגמאות לבעלי שליטה במאגר מידע או מחזיקים כאמור – ספק מורשה של

303 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב1 לחוק הגנת הפרטיות.

304 סעיף 18 לתיקון 13, שם, המוסיף את סעיף 17ב1(א)(1),(2) לחוק הגנת הפרטיות.

305 סעיף 18 לתיקון 13, שם, המוסיף את סעיף 17ב1(א)(3) לחוק הגנת הפרטיות.

שירותי טלקומוניקציה, ספק שירות חיפוש מקוון, או מי שפעולות אלו הן עיסוקו העיקרי. בטיוטת גילוי הדעת שפרסמה הרשות להגנת הפרטיות להערות הציבור ביולי 2025, סיפקה הרשות דוגמאות נוספות לנסיבות של "ניטור שוטף ושיטתי" של בני אדם. למשל, התחקות אחר פעילות נושא המידע באתרי אינטרנט וביישומונים, ביישומוני מעקב אחר מיקום פיזי או בנתוני בריאות, ובמכשירי "האינטרנט של הדברים" (IoT), כגון כלי רכב חשמליים, מאגר צילומים של מצלמות מעקב וספקי אינטרנט.[306] לעומת זאת, עסק קטן המנטר רק את עובדיו באופן פנימי ולא שוטף עשוי שלא להיות חייב במינוי ממונה הגנת פרטיות.

(2) בעל שליטה במאגר מידע או מחזיק "ש**עיסוקו העיקרי** כולל עיבוד מידע בעל רגישות מיוחדת ב**היקף ניכר**". גם כאן הסעיף מספק דוגמאות – תאגיד בנקאי, מבטח, בית חולים וקופת חולים.[307] כמו בפרשנות המקובלת של המונחים באיחוד האירופי,[308] בטיוטת גילוי הדעת בנוגע למינוי ממונה הגנת הפרטיות הבהירה הרשות שהכוונה היא רק לגופים שעיבוד המידע בעל הרגישות המיוחדת בהיקף ניכר הוא חלק מרכזי בהגשמת המטרות הארגוניות או העסקיות שלהם. נוסף על כך, לדעת הרשות להגנת הפרטיות הדרישה שעיבוד המידע בעל רגישות מיוחדת בהיקף ניכר ייחשב עיסוקו העיקרי של הארגון חלה גם אם העיבוד כאמור הוא חלק אינהרנטי מפעילות הליבה של הארגון, אף אם אינו חיוני להגשמתה. עם זאת, הרשות מבהירה כי אם עיבוד המידע בעל הרגישות המיוחדת בהיקף ניכר נעשה "רק לצורך ביצוע מטרות עזר משניות כגון העסקת עובדים, אם אינן בעלות זיקה ישירה למטרות המרכזיות של הארגון", הוא לא יביא להטלת חובת מינוי ממונה הגנת פרטיות.[309]

306 הרשות להגנת הפרטיות, גילוי דעת: מינוי ממונה על הגנת הפרטיות בארגון לפי דרישות תיקון 13 לחוק הגנת הפרטיות, טיוטה להערות הציבור (23 ביולי, 2025) (להלן: גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות), בסעיף 9.8.

307 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב1(א)(4) לחוק הגנת הפרטיות; פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 6–15; פרוטוקול מס' 351, לעיל ה"ש 235 לעיל, בעמ' 36–54.

308 Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017)

309 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 307, בסעיף 9.6.

אשר לביטוי "בהיקף ניכר" המופיע תחת הכלל המהותי, בתיקון 13 מופיעה רשימה פתוחה של קריטריונים שלפיהם ייקבע אם עיבוד המידע עולה כדי "היקף ניכר": מספר נושאי המידע, שיעורים באוכלוסייה מסוימת, היקף המידע, כמותו, טווח סוגי המידע המעובד, משך פעולת העיבוד ותדירותה, משך שמירת המידע והתחום הגאוגרפי של פעולת העיבוד.[310] בטיוטת גילוי הדעת בנוגע למינוי ממונה הגנת הפרטיות הבהירה הרשות שמדובר ברשימה פתוחה של קריטריונים, ואין הכרח שכולם יתקיימו יחד כדי להכיר בכך שעיבוד המידע עולה כדי עיבוד מידע בהיקף ניכר.[311]

במסמך הזה המליצה הרשות להגנת הפרטיות גם לארגונים שאינם כפופים לחובת מינוי ממונה הגנת הפרטיות שהוספה בתיקון 13 לשקול מינוי כאמור. הרשות ציינה, ובצדק, שמינוי ממונה הגנת פרטיות בארגון צפוי להביא לשיפור הגנת הפרטיות והציות לחוק בארגון. משום כך היא ממליצה לגופים דו־מהותיים, הכפופים לחלק מנורמות המשפט הציבורי, למנות ממונה הגנת פרטיות אף אם אינם חבים בכך לפי החוק.[312]

אשר לחשש שקביעת תנאים מהותיים העושים שימוש במושגי שסתום תעניק בפועל שיקול דעת מוחלט ובלתי שקוף לרשות להגנת הפרטיות הציעה ועדת החוקה שהחובה למנות ממונה הגנת פרטיות תהיה חובה רכה ביחס לגופים מהמגזר הפרטי. כלומר, לא יהיה אפשר להטיל על ארגונים פרטיים שאינם סוחרי מידע עיצום כספי בגין הפרת החובה הזאת. במקום זאת, אם יימצא שארגון פרטי שאינו סוחר מידע הפר הוראה אחרת מהוראות חוק הגנת הפרטיות, העובדה שמינה ממונה הגנת פרטיות תהיה שיקול מקל להפחתת העיצום או להתחשבות בהטלתו. כך יהיה אפשר להפיק לקחים בעניין הצורך במינוי ממונה הגנת פרטיות עד לתיקון העתידי של הדין המהותי בחוק הגנת הפרטיות ויינתן מענה לחשש מעודף רגולציה וממתן שיקול דעת מוחלט לרשות להגנת

310 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב1(ב) לחוק הגנת הפרטיות.

311 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 307, בסעיף 9.10.

312 שם, בסעיף 9.12.

הפרטיות. עוד העירה ועדת החוקה, שעל הרשות להגנת הפרטיות לפרסם בהנחיות את הפרשנות שבדעתה לתת לכללים המהותיים למינוי ממונה הגנת פרטיות, ושכללים אלו צריכים לשאוב השראה מפרשנות ההוראות המהותיים ב־GDPR.[313]

נוסף על כך, תיקון 13 קובע גם הוראות בדבר תפקידיו של ממונה הגנת הפרטיות והכישורים הנדרשים לכך. ככלל, על ממונה הגנת הפרטיות לפעול "להבטחת קיום ההוראות לפי חוק זה [...] ולקידום השמירה על הפרטיות ואבטחת המידע במאגרי מידע".[314] המדובר בניסוח רחב שמטרתו להבהיר שלצד הצורך להבטיח ציות להוראות חוק הגנת הפרטיות, על הממונה על הגנת הפרטיות לפעול להגנה על הזכות לפרטיות במובנה הרחב.[315] ועדת החוקה דחתה את הצעת משרד המשפטים והרשות להגנת הפרטיות להסמיך את שר המשפטים לקבוע בתקנות, באישור ועדת החוקה, פעולות נוספות שעל הממונה על הגנת הפרטיות לבצע, בנימוק שיש להפחית עד כמה שאפשר את ההתערבות הרגולטורית בהתנהלות השוק הפרטי, ואין מקום לאסדרת העיסוק או מקצוע ממונה הגנת הפרטיות בחקיקה.[316] בטיוטת גילוי הדעת בנוגע למינוי ממונה הגנת הפרטיות הסבירה הרשות להגנת הפרטיות שהממונה על הגנת הפרטיות בארגון הוא מעין מתאם של תהליכי ציות, הן לדרישות המתחייבות מדיני הגנת הפרטיות, הן לדרישות הנובעות מפרקטיקות רצויות לפי רוח הדין והרציונלים שבבסיסו.[317]

313 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 46–49, דברי יו"ר ועדת החוקה, ח"כ רוטמן; פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 6–15. כך, פרט 2(4) לתוספת החמישית לחוק הגנת הפרטיות שהוספה בתיקון 13, לעיל ה"ש 3, קובע כי מינוי ממונה הגנה על הפרטיות בארגון שנדרש לכך מכוח סעיפים 17ב1(א)(3) או (4) לחוק הגנת הפרטיות עשוי לזכות את הארגון בהפחתה בסך 10%, ככל שיוטל עליו עיצום כספי בשל הפרות אחרות של החוק.

314 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב2(א) לחוק הגנת הפרטיות.

315 פרוטוקול מס' 336, לעיל ה"ש 284 לעיל, בעמ' 23–26.

316 שם, בעמ' 22, דברי יו"ר ועדת החוקה, ח"כ רוטמן, יועמ"ש ועדת החוקה, עו"ד מנחמי, ובעמ' 29, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

317 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 307, בסעיף 14.

נוסף על כך, ממונה על הגנת פרטיות נדרש להחזיק בידע בדיני הגנת הפרטיות בישראל, שהם ליבת פעילותו, לצד הבנה הולמת בטכנולוגיה ובאבטחת מידע והיכרות עם תחומי הפעילות של הגוף שבו הוא משמש, והכול על פי הנדרש לנוכח "אופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו". בטיוטת גילוי הדעת בנוגע למינוי ממונה הגנת הפרטיות הרשות להגנת הפרטיות מבהירה שנדרש ידע מעמיק בדיני הגנת הפרטיות בישראל. לשיטתה, ידע מעמיק כאמור נרכש באמצעות ניסיון, אך רצוי גם שמי שמתמנה לתפקיד זה בארגון יעבור גם הכשרה בסיסית בתחום. הכשרה בסיסית, לפי הרשות, אפשר לרכוש בקורסים מטעם הרשות או בחסותה, אך היא יכולה להירכש גם בדרך אחרת, כל עוד אפשר להוכיח לימודים או ניסיון מעשי באסמכתאות רשמיות.[318]

כמו כן, בתיקון 13 נקבע במפורש שממונה הגנת הפרטיות בארגון לא חייב להיות עובד בבעל השליטה במאגר המידע או במחזיק.[319] עם זאת, בטיוטת גילוי הדעת בנוגע למינוי ממונה הגנת הפרטיות הרשות להגנת הפרטיות מציינת כי "אופטימאלית רצוי שהממונה יהיה עובד הארגון וחלק אינטגרלי מן הארגון".[320]

ברוח ה־GDPR,[321] תיקון 13 מחייב בעל שליטה במאגר מידע ומחזיק, החייבים במינוי ממונה הגנת פרטיות, לספק לו את "התנאים והמשאבים הדרושים למילוי נאות של תפקידו ויוודאו שהוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות".[322] מטרת הוראה זו היא להבטיח שממונה הגנת הפרטיות בארגון יהיה בעל תפקיד מהותי, וכי מילוי מוצלח של תפקידו יהיה גם אינטרס של בעל השליטה או המחזיק. להוראה זו מתווספת גם הדרישה שהממונה על הגנת הפרטיות ידווח ישירות למנכ"ל בעל השליטה או המחזיק או לעובד הכפוף לו ישירות. הדיווח למנכ"ל או לעובד הכפוף ישירות למנכ"ל מבטיח את רמת הקשב

318 שם, בסעיף 12.2.

319 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב3(א) ו־(ב) לחוק הגנת הפרטיות; פרוטוקול מס' 336, לעיל ה"ש 284 לעיל, בעמ' 26–29.

320 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 307, בסעיף 16.

321 ראו סעיף 37(1)–(2) ל־GDPR, לעיל ה"ש 33.

322 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב2(ב) לחוק הגנת הפרטיות.

הנדרשת להערותיו של הממונה על הגנת הפרטיות בארגון. תיקון 13 בוחר במכוון בדרישת דיווח של ממונה הגנת הפרטיות, ואינו מחייב שבעל התפקיד יהיה כפוף לבעל תפקיד בכיר בארגון, כדי להימנע מהתערבות יתר בפררוגטיבה הניהולית של המעסיק, לצד הבנת הקושי הפרקטי של עובד להגביל או למנוע פעולות שהדרג הניהולי הבכיר בארגון מבקש לבצע.[323]

תיקון 13 אוסר על הממונה על הגנת הפרטיות למלא תפקיד נוסף בארגון או להיות כפוף לנושא משרה בארגון אם מילוי התפקיד הנוסף או הכפיפות עלולים להעמידו בחשש לניגוד עניינים.[324] הרשות להגנת הפרטיות מבהירה כי תפקידים הכוללים "את הסמכות או האחריות לקבוע מדיניות בעניין עיבוד המידע האישי בארגון, לרבות קביעת מטרות העיבוד וקבלת החלטות מהותיות לגבי שיטות ואמצעי העיבוד" הן בהכרח תפקידים המעמידים את הממונה בניגוד עניינים האסור לפי החוק. כן מציעה הרשות להגנת הפרטיות לקבוע כלל אצבע, ולפיו תפקידים בכירים, כגון מנהל שיווק, מנהל לקוחות, מנהל כספים, מנהל מערכות מידע או CTO, הם בהכרח תפקידים המעמידים את הממונה על הגנת הפרטיות בארגון בניגוד עניינים.[325] עמדה זו עולה בקנה אחד עם הפרשנות שניתנה לאיסור ניגוד העניינים המוטל על ממונה על הגנת פרטיות בארגון לפי ה־GDPR.[326]

אף שתיקון 13 אינו קובע זאת, הרשות להגנת הפרטיות הבהירה בטיוטת גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות שחובה להיוועץ עם הממונה על הגנת הפרטיות. לפי הרשות, יש להתייחס לחוות דעתו בכובד ראש, ואם

323 פרוטוקול מס' 336, לעיל ה"ש 284, בעמ' 35, דברי יו"ר ועדת החוקה, ח"כ רוטמן, בעמ' 36, דברי עו"ד רבינוביץ ויו"ר ועדת החוקה, ח"כ רוטמן.

324 סעיף 18 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ב(3)(ג) לחוק הגנת הפרטיות.

325 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 307, בסעיף 20.

326 Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017)

הארגון מחליט לפעול שלא לפי חוות הדעת שלו עליו לנמק את הסיבות לכך.[327] עמדה זו רצויה ועולה בקנה אחד עם המשקל שניתן לחוות דעתו של ממונה לפי ה־GDPR, שלפי הפרשנות המקובלת, מחייב את הארגון לתעד בכתב את נימוקיו שלא לאמץ את עמדת הממונה על הגנת הפרטיות. עם זאת, ב־GDPR יש מכלול הוראות דין מהותיות נוספות החסרות בחוק הגנת הפרטיות בישראל,[328] ושעל בסיסן פורשו ההוראות ביחס לממונה הגנת פרטיות, כמו למשל, הוראות ה־GDPR בנוגע לעריכת תסקיר השפעה על פרטיות וחובת התיעוד.[329] נוסף על כך, לא ברור שמתן משקל זה לעמדת הממונה על הגנת הפרטיות עולה בקנה אחד עם עמדת ועדת החוקה והעומד בראשה לאורך כל הדיונים. יו"ר ועדת החוקה, ח"כ רוטמן, חזר והדגיש את חששו מפני מתן משקל רב מידי ליועצים משפטיים וחיוב במינוי בעל תפקיד בחוק, שכן לשיטתו מדובר בהתערבות יתר בהתנהלות הפנימית בארגון פרטי. זו גם אחת הסיבות לכך שחובת מינוי ממונה הגנת פרטיות בגופים פרטיים, שאינם סוחרי מידע, אומצה כחובה רכה שאין עיצום ספציפי נגד הפרתה, אלא שקיומה הוא שיקול להפחתת עיצום ביחס להפרות אחרות.[330]

327 328 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 307, בסעיף 15.1.

328 תקנה 5 לתקנות אבטחת מידע, לעיל ה"ש 84, מחייבת כל בעל מאגר מידע להחזיק מסמך מעודכן של מבנה מאגר המידע, ובעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה חייב לעשות סקר סיכונים אחת ל־18 חודשים לפחות. עם זאת, אין מדובר בחובת עריכת תסקיר השפעה מקיף, כפי שהסבירה הרשות להגנת הפרטיות עצמה. ראו הרשות להגנת הפרטיות **תסקיר השפעה על פרטיות – מדריך עזר מתודולוגי** (נובמבר 2022).

329 ראו GDPR, לעיל ה"ש 33, סעיפים 5(2) ו־35(2); Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017); Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679*, WP248 rev.01 (Oct. 4, 2017)

330 ראו הטקסט הנלווה לה"ש 316 לעיל.

פרק 6

החידושים העיקריים בתיקון 13 לעניין זכויות נושא המידע

לפי חוק הגנת הפרטיות לנושא המידע זכות לעיין במידע אישי על אודותיו, לבקש תיקון המידע האישי או מחיקתו אם אינו מדויק, שלם או נכון, וזכות לקבל הודעה בעת פנייה אליו לקבלת מידע אישי על אודותיו.[331] תיקון 13 אומנם לא הרחיב מאוד את זכויות נושא המידע, אך הוסיף שני כלים חשובים העומדים בידי נושא המידע:

6.1. פיצויים לדוגמה

נושא הפיצויים לדוגמה לא נכלל בהצעת החוק הממשלתית אלא הוסף אליה ביוזמת ועדת החוקה, על בסיס מודל דומה בחוק הגנת הצרכן.[332] מטרת סעד הפיצויים לדוגמה היא לייצר מנגנון הממוקד בנושא המידע וזכויותיו, המנגנון משקף יסוד הרתעתי עונשי ביחס להפרתן ויכול להחליף את מנגנון התביעות הייצוגיות, ששימשו בשנים האחרונות פעמים רבות לרעה ולהגשת תביעות סרק.[333] נוסף על כך, ההסדר מאפשר לנושא מידע לתבוע גם גופים ציבוריים, למשל, אם נושא המידע מגלה שמאגר המידע שבידי הגוף הציבורי אינו רשום, או אם הוא מוצא ברישומי הרשות להגנת הפרטיות שהגוף הציבורי לא עדכן

331 סעיפים 13, 14 ו־11 לחוק הגנת הפרטיות.

332 פרוטוקול מס' 310 מישיבת ועדת החוקה, חוק ומשפט, יום שני, כ"ט באדר ב התשפ"ד (8 באפריל 2024), בעמ' 57, דברי יועמ"ש ועדת החוקה, עו"ד מנחמי; סעיף 31א בחוק הגנת הצרכן, תשמ"א–1981; פרוטוקול מס' 359 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, כ"ד בסיון התשפ"ד (30 ביוני 2024), בעמ' 4–5.

333 פרוטוקול מס' 320 מישיבת ועדת החוקה, חוק ומשפט, יום חמישי, ח' באייר התשפ"ד (16 במאי 2024), בעמ' 118, דברי יו"ר ועדת החוקה, ח"כ רוטמן; נטע סרוסי "אלפי תביעות נגד עסקים: הכירו את שיטת מצליח של עורכי הדין" **גלובס** (11.4.2024).

את הרשות להגנת הפרטיות שהוא מקבל דרך קבע מידע אישי.[334] ועדת החוקה ראתה באפיק הפעולה הזה אמצעי לעודד ציות בקרב גופים ציבוריים, על רקע משאבי האכיפה המוגבלים של הרשות להגנת הפרטיות ביחס לגופים ציבוריים והקושי להטיל עליהם עיצומים כספיים.[335] עם זאת, בהיעדר זכויות מהותיות משמעותיות לנושא המידע, לבד מזכות העיון והתיקון, יוצר מנגנון הפיצויים לדוגמה הקבוע בסעיף 15א זכות לקבלת פיצוי ללא הוכחת נזק במקרים שהוכחתם עשויה להיות מסורבלת מעט ולא אינטואיטיבית לנושא המידע, שכן הוא נדרש להוכיח שבעל השליטה במאגר המידע הפר חובה רגולטורית, כגון חובת הרישום, אף אם הפרתה אינה גורמת לו נזק ישיר.[336]

לפי ההסדר ייפסקו פיצויים מוסכמים בסכום מירבי של 10,000 ש"ח לטובת נושא המידע בתנאים מסוימים בגין הפרת הוראות מסוימות בחוק הגנת הפרטיות על ידי בעל השליטה במאגר מידע או מחזיק.[337] עם זאת, אם מדובר בהפרת חובת הרישום שבסעיף 8א, הפרת חובת יידוע נושא המידע שבסעיף 11, או החובה המוטלת על גוף ציבורי לפי סעיף 23ד(ג) לדווח לרשות להגנת הפרטיות על קבלה דרך קבע של מידע אישי, מימוש זכות התביעה מותנה בפעולה אקטיבית מצד נושא המידע: פנייה בדרישה לרשום מאגר מידע שלא נענתה בתוך 90 ימים, פנייה בדרישה לקבל הודעה לפי סעיף 11, או פנייה בדרישה להודיע לרשות על קבלה דרך קבע של מידע אישי על ידי גוף ציבורי – שלא נענו בתוך 30 ימים.[338]

334 סעיף 13 בתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 15א(א)(1) ו־(6) לחוק הגנת הפרטיות.

335 פרוטוקול מס' 310, לעיל ה"ש 333, בעמ' 63, דברי יו"ר ועדת החוקה, ח"כ רוטמן; פרוטוקול מס' 359 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, כ"ד בסיון התשפ"ד (30 ביוני 2024), בעמ' 4–5.

336 פרוטוקול מס' 310, לעיל ה"ש 333, בעמ' 53–63.

337 סעיף 13 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 15א לחוק הגנת הפרטיות.

338 סעיף 13 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 15א לחוק הגנת הפרטיות; תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א–1981; פרוטוקול מס' 310, לעיל ה"ש 333, בעמ' 53–63.

6.2. ביטול מגבלת ההתיישנות

תקופת ההתיישנות בתביעה אזרחית בגין פגיעה בפרטיות הייתה לאורך שנים קצרה בהרבה מהתקופה הנהוגה בתביעות נזיקיות רגילות,[339] ועמדה על שנתיים בלבד.[340] בעבר הונחו על שולחן הכנסת כמה הצעות חוק לביטול הגבלה זו על תקופת ההתיישנות, אולם הן לא התגבשו לחוק.[341] הצעת החוק הממשלתית לא עסקה כלל במגבלת ההתיישנות. הנושא עלה בדיונים בוועדת החוקה. כך, למשל, הודגש הפער בין שלוש השנים שבמהלכן ביקשה הצעת החוק הממשלתית להתיר לרשות להגנת הפרטיות לשמור מידע מדגמי לשם השלמת הליך פיקוח, לבין תקופת הזמן הקצרה יותר, של שנתיים, הנתונה לפי מגבלת ההתיישנות לנושא מידע מן השורה המבקש להגיש תביעה אזרחית בגין פגיעה בפרטיותו.[342] לפיכך ביקשה ועדת החוקה ליצור הלימה בין היכולת של הרשות להגנת הפרטיות להטיל עיצום כספי, לבין זכות נושא המידע להגיש תביעה בגין פגיעה בפרטיותו. הוועדה ביקשה לחזק את אפיק התביעות האזרחיות, בעיקר מכוח סעד הפיצויים לדוגמה שהוסף בתיקון 13,[343] ככלי לשיפור הגנת הפרטיות בישראל, אך בד בבד להימנע מהכבדת הנטל הרגולטורי על בעלי שליטה ומחזיקים העשויים להידרש מעתה לתת מענה לא רק לרשות להגנת הפרטיות אלא גם לנושאי מידע העשויים לנצל לרעה את מתווה הפיצויים לדוגמה.[344]

339 חוק ההתיישנות, התשי"ח–1958, קובע שתקופת ההתיישנות בנושאים אזרחיים, כגון הפרת חוזה, הסגת גבול, תקיפה, התרשלות ומטרד, עומדת על שבע שנים.

340 סעיף 26 לחוק הגנת הפרטיות לפני תיקון 13, לעיל ה"ש 1.

341 ראו הצעת חוק הגנת הפרטיות (תיקון – תקופת ההתיישנות), התשע"ח–2018. ב־2019 הגיש ח"כ בר לב הצעה דומה. ראו הצעת חוק הגנת הפרטיות (תיקון – תקופת ההתיישנות), התש"ף–2019. הצעה דומה הגישה גם ח"כ בן ארי ב־2021. ראו הצעת חוק הגנת הפרטיות (תיקון – תקופת ההתיישנות), התשפ"א–2021.

342 פרוטוקול מס' 249, לעיל ה"ש 253, בעמ' 64, דברי ד"ר ארידור הרשקוביץ.

343 ראו הדיון בסעיף 6.1 לעיל.

344 פרוטוקול מס' 310, לעיל ה"ש 333, בעמ' 65, דברי עו"ד מרקביץ והיועצת המשפטית של הוועדה, עו"ד מנחמי; פרוטוקול מס' 313 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ח' בניסן התשפ"ד (16 באפריל 2024), בעמ' 65–66, דברי יו"ר ועדת החוקה,

ואולם, היעדר התיקון לדין המהותי היה מכשלה גם בנושא מגבלת ההתיישנות. נטען כי בהיעדר כללים ברורים בנוגע לבסיסים חוקיים לעיבוד מידע, ומשום שכלל עיבוד המידע נשען על שאלת ההסכמה ועל פרשנות מופעי הפגיעה בפרטיות הקבועים בסעיף 2 לחוק הגנת הפרטיות, הארכת תקופת ההתיישנות לשבע שנים עלולה להקשות על התנהלותם של בעלי שליטה ומחזיקים המבקשים לעבד מידע. אלו יתקשו לכלכל את צעדיהם לנוכח חוסר הוודאות האינהרנטי בהיעדר תיקון לדין המהותי ולנוכח ההישענות על פרשנות הרשות להגנת הפרטיות ובתי המשפט העשויה להשתנות מעת לעת במהלך שבע שנים בהשפעת המשפט המשווה והשינויים הטכנולוגיים. עם זאת, ועדת החוקה לא השתכנעה שיש בכך כדי להצדיק את הפער בין אדם שנפגעת זכותו לשלמות גופו ותובע, למשל, בגין רשלנות רפואית, לבין אדם שנפגעה זכותו לפרטיות.[345] לפיכך, מגבלת ההתיישנות שהייתה קבועה בסעיף 26 לחוק הגנת הפרטיות לפני תיקון 13 בוטלה.[346]

ח"כ רוטמן; פרוטוקול מס' 320, לעיל ה"ש 334, בעמ' 118–119, דברי יו"ר ועדת החוקה, ח"כ רוטמן והיועצת המשפטית לוועדה, עו"ד מנחמי.

345 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 11, דברי עו"ד שגיא, בעמ' 12–13, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

346 סעיף 34 לתיקון 13, לעיל ה"ש 3, המבטל את סעיף 26 בחוק הגנת הפרטיות.

פרק 7

עם הפנים קדימה – מה נותר עוד לתקן?

אף שתיקון 13 הציג שינויים חשובים ונחוצים לחוק הגנת הפרטיות, הרבה מעבר למה שהובא בפני ועדת החוקה בהצעת החוק הממשלתית, חוק הגנת הפרטיות נותר חסר. חוסר זה מציב קשיים יום־יומיים ביישומו המעשי של החוק הישראלי ובגישור על הפערים בינו לבין המשפט המשווה. החוסר מורגש בעיקר מול החקיקה המקיפה במדינות אירופה, המציגה אמת מידה בינלאומית בכל הנוגע להגנת מידע אישי ולשימושים בבינה מלאכותית. כן מתעורר קושי אמיתי לבעלי שליטה ומחזיקים המבקשים לעבד מידע אישי, אך מתקשים להסתמך בעידן הדיגיטלי המודרני רק על הסכמתו מדעת של נושא המידע. בחלק זה אצביע על התיקונים הנחוצים לחוק הגנת הפרטיות כדי להביא את רמת הגנת הפרטיות במדינת ישראל לרמה המקובלת במדינות המערב הדמוקרטיות, ולאפשר עיבוד מידע אישי שהוא חלק מהתנהלות הכלכלה המודרנית, אם כי מתוך מתן הגנה מתאימה על נושאי המידע, שהם חסרי אונים נוכח עיבוד המידע האישי עליהם בהיקפים גדולים ושלא בידיעתם, וצמצום חוסר הוודאות של בעלי השליטה ומחזיקים המבקשים לעבד מידע.

7.1. הרחבת שער הכניסה לתחולת חוק הגנת הפרטיות – ביטול הגדרת "מאגר מידע"

בעולם עיבוד המידע הדיגיטלי "מאגר מידע" הוא יצור פיקטיבי – יצירתו מאולצת ומלאכותית ונובעת מהצורך להתמודד עם דרישות חוק הגנת הפרטיות בלבד.[347] לפיכך, הותרת הביטוי "מאגר מידע" בלשון החוק, בין התנאים לתחולת הוראות חוק הגנת הפרטיות היא ארכאית, אינה תואמת את משטר הגנת הפרטיות המקובל בעולם,[348] ואף מובילה לצמצום החשיבות והמשמעות שיש בהרחבת

347 ראו הטקסט הנלווה לה"ש 86–87 לעיל.

348 למשל, חוקי הגנת המידע באיחוד האירופי, בסינגפור, בקליפורניה ובאוסטרליה

הגדרה של "מידע אישי". יתרה מזו, הותרתה בעינה פוגעת בהגנה על מידע אישי כשלעצמו ובזכויות נושא המידע, בין שהמידע האישי הוא חלק ממאגר מידע בין לאו.[349]

זאת ועוד, הקושי הפרקטי להגדיר מהו "מאגר מידע" ולהבחינו מבין שלל המערכות המעבדות מידע שיש בידי ארגון נעשה קריטי לנוכח תג המחיר הגבוה שבצידו – תג המחיר בא לידי ביטוי בהסמכת הרשות להגנת הפרטיות בתיקון 13 להטיל עיצומים כספיים על מעשה או מחדל שביצועם קשור או תלוי בהגדרת מאגר המידע בארגון.[350]

אם המונח "מאגר מידע" יוותר גם לאחר תיקון מהותי של חוק הגנת הפרטיות, יש לתת את הדעת להחרגה מההגדרה של מאגרי מידע הכוללים רק שם, מען ודרכי תקשורת על פחות מ־100,000 איש. ייתכן שראוי להגן על עסקים קטנים וזעירים ולאפשר להם ליצור רשימות קשר מצומצמות בלי לחוב בהוראות חוק הגנת הפרטיות. אולם, הרף של 100,000 בני אדם או פחות גבוה יחסית לצורך האמיתי של עסקים שההגנה עליהם היא תכלית החריג. התוצאה בפועל היא שמי שמחזיק בפרטים כגון שם, כתובת, טלפון וכתובת דוא"ל, בלי כל מידע נוסף על נושאי המידע, לא יחוב כלל בחובות הקבועות בחוק הגנת הפרטיות, ובכלל זה חובת אבטחת המידע. במציאות שבה מדינת ישראל נתונה למתקפות סייבר בעוצמות משתנות כל העת,[351] יש לתת את הדעת גם להחרגת "אוסף אישי שאינו

אינם כוללים הגדרה של המונח "מאגר מידע" (dataset) כלל. ראו GDPR, לעיל ה"ש 33; Privacy Act 1988 (Cth) (Austl.); Personal Data Protection Act 2012, No. 26 of 2012 (Sing.); CCPA, לעיל ה"ש 47. בקנדה מוגדר המונח "personal information" "bank – אוסף או מקבץ של מידע אישי המצוי בידי משרדי הממשלה. ההגדרה רלוונטית אך ורק לעניין רישום המאגר. ראו סעיפים 3, 10–11 ל־Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.)

349 פרוטוקול מס' 197, לעיל ה"ש 67, בעמ' 35–40.

350 סעיף 33 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 23כו לחוק הגנת הפרטיות.

351 ראו, למשל, עומר כביר "זינוק במתקפות הסייבר: 'עברו מגניבת מידע לשיבוש ונזק'" **כלכליסט** (31.3.2024); ליאור נוביק "תקיפות סייבר: ישראל היתה המדינה המותקפת ביותר בשנת 2023" **מעריב** (7.4.2024).

למטרות עסק" מהגדרת "מאגר מידע", משום שמשמעות החרגה זו היא שאין חובת אבטחת מידע על אוסף זה מכוח חוק הגנת הפרטיות, ועל כן יש להבטיח שאין באוספים כגון אלו פוטנציאל נזק משמעותי להגנת הסייבר של המדינה.

7.2. בעל שליטה במאגר מידע, מחזיק ומנהל מאגר מידע: בחינה מחודשת של חלוקת האחריות

ראשית, יש לבחון אם ההגדרה הרחבה של "בעל שליטה" במאגר מידע, המתמקדת אך ורק בארגון הקובע את מטרות העיבוד, לא הובילה לאכיפת יתר מצד הרשות להגנת הפרטיות נגד גורמים שאין להם כל שליטה בעיבוד המידע האישי. אם תופעת אכיפת יתר אכן תתרחש, כפי שיהיה אפשר ללמוד מהדיווחים השנתיים שעל הרשות להגנת הפרטיות לספק לוועדת החוקה,[352] על ועדת החוקה לבחון מחדש את ההגדרה שאומצה בתיקון 13 למונח "בעל שליטה" ולאמץ מתווה ברוח ה־GDPR, כפי שפורש על ידי ה־EDPB, שלפיו בעל השליטה הוא מי שקובע את מטרות העיבוד ואת אמצעי העיבוד החיוניים.[353]

נוסף על כך, ה־GDPR מבהיר את חלוקת האחריות בין בעל השליטה במידע למעבד,[354] אך בחוק הגנת הפרטיות, גם לאחר תיקון 13, התמונה אינה ברורה

352 ראו סעיף 24 בתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ט3 לחוק הגנת הפרטיות.

353 ראו לעיל הדיון בטקסט הנלווה להערות שוליים 102–109.

354 לפי ה־GDPR, על בעל השליטה (controller) מוטלת האחריות להתקשר רק עם מעבד (processor) שבהתחשב באופי עיבוד המידע ובסכנות שמציב עיבוד המידע לזכויות נושאי המידע, יכול לספק לו ערבויות מספיקות לכך שיטמיע אמצעים טכניים וארגונים שיבטיחו שעיבוד המידע יעמוד בדרישות החוק וישמור על זכויותיו של נושא המידע. עוד מוטלת עליו החובה לפקח ולבדוק לאורך כל תקופת ההתקשרות עם המעבד שהוא אכן נוקט את האמצעים הראויים לעמידה בדרישות ה־GDPR ולכיבוד זכויות נושאי המידע. ההתקשרות בין בעל השליטה למעבד חייבת להיעשות בכתב, ראו סעיפי הקדמה 81–83 וסעיפים 28–36 ל־GDPR, לעיל ה"ש 33. בעל השליטה הוא שאחראי להוכחת הציות לעקרונות עיבוד המידע

לחלוטין. למשל, עקרונות צמידות המטרה בסעיפים 2(9) לחוק הגנת הפרטיות ו־8(ב), אינם קובעים על מי מוטלת האחריות לציית להוראת צמידות המטרה. לשון ההוראות היא כללית וראש הרשות להגנת הפרטיות מוסמך להפעיל את סמכויות האכיפה המינהליות שלו נגד כל אחד מבעלי התפקידים – בעל שליטה במאגר מידע או המחזיק.[355] אף חובת ההודעה לנושא המידע הקבועה בסעיף 11 לחוק הגנת הפרטיות מנוסחת בלשון כללית, "פניה לאדם", בלי לקבוע על מי מבעלי התפקידים מוטלת חובת ההודעה לנושא המידע, וכל אחד מהם עשוי לחוב בפיצוי לדוגמה בגין הפרתה.[356] היעדר אסדרה ברורה של מערכת היחסים וחלוקת האחריות בין בעל השליטה במאגר מידע לבין המחזיק עלולה להגביר את חוסר הוודאות בשוק ואת הקושי של הרשות להגנת הפרטיות לאכוף כהלכה את הוראות חוק הגנת הפרטיות.

כמו כן, מבט מעמיק בתקנות העברת מידע בין גופים ציבוריים מלמד שהחובות המוטלות על מנהל מאגר שקולות לאלו המוטלות על בעל המאגר או על המנהל הכללי בגוף.[357] ולכן אפשר לוותר לחלוטין על המונח "מנהל מאגר" בחוק הגנת

המפורטים בסעיף 5 ל־GDPR, לעמידה במגבלות המטרה ולעיבוד למטרות דומות לפי סעיף 6(4) ל־GDPR, לפנות לקבלת הסכמת נושא המידע לעיבוד המידע לפי סעיף 7(1) ל־GDPR, וכן לקבלת הסכמה חוקית מקטין לפי סעיף 8(2) ל־GDPR. כמו כן, מימוש זכויות נושא המידע, חובת עיצוב לפרטיות וחובת עריכת תסקיר השפעה על הפרטיות, הן באחריות בעל השליטה, לפי סעיפים 15–18, 25, 35 ל־GDPR. חובת תיעוד, חובת שיתוף פעולה עם נציבות הפרטיות המדינתית, חובת אבטחת מידע וחובת מינוי ממונה אבטחת מידע מוטלת במפורש על בעל השליטה ועל המעבד, לפי סעיפים 30–32, 37 ל־GDPR.

355 סעיף 2(9) לחוק הגנת הפרטיות, לעיל ה"ש 3: "פגיעה בפרטיות היא אחת מאלה: [...] (9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה". סעיף 8(ב) "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין". ראו סעיף 4 לתיקון 13, לעיל ה"ש 3, המחליף את סעיף 8 בחוק הגנת הפרטיות. ראו גם סעיף 24 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ט3 לחוק הגנת הפרטיות.

356 ראו סעיף 8 בתיקון 13, שם, המתקן את סעיף 11 לחוק הגנת הפרטיות.

357 תקנה 2(א)(7) לתקנות העברת מידע בין גופים ציבוריים מחייבת לציין את שמו של מנהל המאגר לצד שמו של המחזיק ושל ממונה אבטחת המידע בו; תקנה 3(1) קובעת שממונה אבטחה יהיה כפוף ישירות למנהל המאגר או למנהל הפעיל של בעל המאגר או המחזיק בו או לנושא משרה בכירה הכפוף ישירות למנהל המאגר; תקנה 3(3) מחייבת

הפרטיות. צמצום מספר בעלי התפקידים שגוף ציבורי חייב במינויים הוא בעל משמעות כלכלית, בעיקר אם מדובר בגופים ציבוריים קטנים, כמו רשויות מקומיות קטנות, ומונע אי־בהירות ומתחים ביחס לחלוקת הסמכויות והאחריות בניהם.[358]

7.3. הוספת בסיסים חוקיים לעיבוד מידע והחלשת ההסתמכות על דרישת ההסכמה

היעדר תיקון של הדין המהותי, ובראשו הוספת בסיסים חוקיים מלבד ההסכמה להתרת עיבוד מידע אישי, הוא חסר מהותי בתיקון 13. קודם כול, הצבת דרישת ההסכמה כציר שמסביבו סובבים כל עיבודי המידע "מכשירה" הסכמות שספק אם ניתנו מדעת ומרצון. יתרה מזו, להסכמת נושא המידע עלולות להיות השלכות שליליות על אחרים. למשל, הצטרפות לרשת חברתית מאפשרת לרשת לקבל את רשימת אנשי הקשר של המצטרף, תיוג פנים מאפשר ללמוד על אחרים המצולמים באותו התצלום, והסכמה למסירת מידע גנטי מאפשרת ללמוד על בני משפחה. בעקבות זאת, כבר היום קיימים מאגרי מידע רבים הכוללים מידע שלא נמסר בידיעה או בהסכמת נושא המידע. למשל, מידע שחברת ביטוח מקבלת ממבוטח שלה כחלק מדיווח על תאונת דרכים שהיה מעורב בה, כולל גם מידע על הנהגים והעדים בזירה. מידע כזה על צדדים שלישיים הועבר לחברת הביטוח ללא ידיעתם או הסכמתם. כך, הותרת דרישת ההסכמה, המוגדרת ומוסדרת בפרק א בחוק הגנת הפרטיות, כמדד היחיד והמרכזי להכשרת עיבוד מידע רק

את ממונה האבטחה להודיע למנהל המאגר על ממצאי תוכנית הבקרה השוטפת שיכין; תקנה 18(2) מחנה את שחזור הנתונים באישור מנהל המאגר, ולבסוף, תקנה 19 מבהירה שהחובות החלות לפי התקנות על בעל מאגר יחולו גם על מנהל המאגר, למעט חובות החלות גם על מחזיק.

358 פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 33–34.

בנסיבות שהן "פגיעה בפרטיות" לפי סעיף 2 לחוק הגנת הפרטיות, יוצרת אזור אפור ביחס למידע אישי שנאסף ללא הסכמת נושא המידע.[359]

כמו כן, במצב חוקי העכשווי רק עיבוד מידע אישי שנחשב פגיעה בפרטיות,[360] כהגדרתה בסעיף 2 בחוק הגנת הפרטיות, חייב להיעשות בהסכמת נושא המידע.[361] אולם יתכנו עיבודי מידע שאינם נופלים לגדר מופעי הפגיעה בפרטיות שבסעיף 2 לחוק הגנת הפרטיות, שיוכלו להיעשות ללא הסכמת נושא המידע. למשל, האם כאשר עובד מוריד לטלפון הנייד שקיבל מהמעסיק יישומונים העוקבים אחר דפוסי הצריכה שלו כדי להציג לו פרסומות מותאמות אישית, נעשה הטלפון למרחב אישי־ציבורי של חייו, ולכן המעסיק רשאי לנהל אחריו מעקב באמצעות הטלפון בלי שהדבר ייחשב פגיעה בפרטיות המחייבת את הסכמת העובד?[362] נוסף על כך, ההתמקדות בדרישת ההסכמה מובילה בעלי שליטה המבקשים לעבד מידע אישי בנסיבות שיש בהן קושי לקבל את הסכמת נשוא המידע לנסות ולהישען על סעיפי ההגנות שבחוק, שלא נועדו לשם כך.[363]

לפיכך, הישענות אך ורק על דרישת ההסכמה כדי להכשיר כל פגיעה בפרטיות מובילה בפועל להגנה חסרה על הזכות לפרטיות. הציבור מסתגל לכך שההסכמה היא חסרת ערך ממשי, והיא נהפכת לזכות שמוותרים עליה כלאחר יד וכדבר שבשגרה בלי להבין את השלכות הוויתור, שכן רק הוויתור עליה וההסכמה

359 פרוטוקול מס' 210, לעיל ה"ש 84, בעמ' 103–104.

360 שם, בעמ' 123, דברי עו"ד יוסוב עמיר: "חד משמעית לא מבקשים לקבוע שנדרשת הסכמה לעצם העיבוד [...] לא הצענו לקבוע שכל עיבוד מידע דורש הסכמה".

361 שם, בעמ' 107, דברי עו"ד אידלמן.

362 ראו הערת אגב של השופטת זלמנוביץ גיסין בסע"ש (ת"א) 18279-06-16 **אקספו ניהול בע"מ נ' משה כהן** (פורסם בנבו 2017), סעיף 31 לפסק הדין.

363 פרק ג לחוק הגנת הפרטיות. ראו גם רחל אריאלי הרשקוביץ ותהילה שוורץ אלטשולר, "חוות דעת: גילוי דעת של הרשות להגנת הפרטיות בנושא הסכמה בדיני הגנת הפרטיות – טיוטה להערות הציבור" **אתר המכון הישראלי לדמוקרטיה** (23.3.2025); רחל אריאלי הרשקוביץ ותהילה שוורץ אלטשולר, "חוות דעת: "טיוטת הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית" **אתר המכון הישראלי לדמוקרטיה** (3.8.2025).

לפגיעה בה הם שמאפשרים התנהלות שוטפת בעולם המידע שאנו חיים בו.[364] הפתרון הוא קביעת בסיסים חוקיים נוספים לעיבוד מידע בחוק, על פי המנגנון החקיקתי באיחוד האירופי, לצד הוספת הזכות לחזרה מהסכמה לנושא המידע.[365] זכות החזרה מהסכמה היא שתבטיח שמעבדי מידע יעדיפו לנסות ולעבד מידע מכוח אחד הבסיסים החוקיים האחרים לפני שיפנו לבקש את הסכמת נושא המידע כדי להכשיר את הפגיעה הצפויה בפרטיות עקב עיבוד המידע שהם מבקשים.[366]

7.4. חובת הרישום וחובת ההודעה לרשות להגנת הפרטיות

חובת הרישום וחובת ההודעה לרשות להגנת הפרטיות[367] הן חובות ארכאיות שאינן מקובלות במרבית המדינות.[368] יתרה מזו, תפיסת הרשות להגנת הפרטיות שחובת הרישום, ולאחר צמצומה – חובת ההודעה, חיוניות לשם הבטחת רמה

364 להרחבה על לעמדה זו ראו, למשל, Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 Boston University Law Review 593 (2024); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1207–08 (2016). לעמדה התומכת בדרישת ההסכמה, ראו Michael Birnhack, *In Defense of Privacy-as-Control (Properly Understood)*, 65 Jurimetrics (forthcoming 2025). ראו גם רועי גולדשמידט "הגנת הפרטיות: סוגיית ההסכמה לאיסוף ולעיבוד של מידע אישי" **הכנסת – מרכז המחקר והמידע** (21 ביוני 2022).

365 סעיפים 6, 9 ו־7(3) ל־GDPR, לעיל ה"ש 33.

366 ראו, למשל, אריאל הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 48, בעמ' 45–51, 61–63.

367 ראו הדיון בסעיפים 3.1 ו־3.2 לעיל.

368 ראו אריאל הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 144; דב"ש, לעיל ה"ש 144.

מינימלית של הגנת פרטיות[369] שמה דגש על פורמליזם על חשבון מהות ושגויה בבסיסה. גם חובת הרישום של סוחרי מידע וגם חובת ההודעה חלות רק לאחר שבעל השליטה במידע החל כבר בעיבוד מידע. חובת רישום של סוחרי מידע חלה רק אם מאגר המידע כולל מידע על 10,000 נושאי מידע, וחובת ההודעה חלה רק אם מאגר המידע כולל מידע בעל רגישות מיוחדת על 100,000 נושאי מידע. התפיסה בדבר חיוניותה של חובת ההודעה מניחה גם שלרשות להגנת הפרטיות יהיו הכלים והמשאבים המספיקים לשם בחינה מעמיקה של כל ההודעות שתקבל ולשם נקיטת פעולות אכיפה מיידיות ומהירות כדי להפסיק עיבודי מידע הפוגעים בזכות לפרטיות באופן המפר את חוק הגנת הפרטיות. הנחה זו אינה נקייה מספקות לנוכח ההיקפים העצומים של מידע בעל רגישות מיוחדת המעובדים בימינו דרך שגרה.

יתרה מזו, חובות הרישום ומתן ההודעה אינן כופות על בעלי השליטה במידע לבחון בעצמם, הרבה לפני שהם מתחילים בעיבוד מידע אישי, כיצד ביכולתם להשיג את שאיפותיהם העסקיות מתוך מזעור הפגיעה בזכות לפרטיות. ובמצב המשפטי הנוכחי, בהיעדר בסיסים חוקיים לעיבוד מידע בחוק בישראל, כל שעל בעל השליטה במידע לעשות הוא לקבל את הסכמתו מדעת של נושא המידע. ולכן תיקון 13 לא יביא לשינוי בתפיסת הזכות לפרטיות ומימושה, והיא תיוותר זכות שבצידה בעיקר דרישות פורמליות שהשוק ממלא באמצעות מסרים קופצים בדבר עדכון מדיניות הפרטיות ומלל רב שרובנו כלל לא טורחים לקרוא.

כדי לשנות את הגישה הזאת ולשפר מהותית את ההגנה על הזכות לפרטיות ראוי לאמץ, במקום חובת הודעה לרשות להגנת הפרטיות, חובת עריכת תסקיר השפעה על הזכות לפרטיות בנסיבות מסוימות ובתדירות קבועה. החובה לערוך תסקיר ההשפעה צריכה להיות ברורה ורחבה יותר מהחובה המוטלת כיום בעקיפין בתקנות אבטחת מידע.[370] חובה כזאת תיתן מענה טוב

369 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 75, דברי עו"ד גרסון.

370 תקנה 5 לתקנות אבטחת מידע, לעיל ה"ש 84, מחייבת כל בעל מאגר מידע להחזיק

יותר לחשש שהעלתה הרשות להגנת הפרטיות מפני עיבודי מידע פוגעניים, משום שבמסגרתה יהא על בעל השליטה במידע לערוך תסקיר תדיר כבר משלב הפיתוח של טכנולוגיית עיבוד המידע, ולא רק תסקיר חד־פעמי, אם מאגר המידע הוא של מידע בעל רגישות מיוחדת וחוצה את רף 100,000 נושאי מידע, הטכנולוגיה בוגרת ונעשה בה שימוש זמן מה. עריכת תסקיר גם תוביל לשינוי תפיסתו אצל בעל השליטה במאגר מידע. חובת ההודעה מציבה את בעל השליטה במאגר מידע במצב פסיבי – עליו לציית אומנם לדרישות החוק אולם הוא חייב לדווח לרשות רק אם המאגר שלו חוצה רף נושאי מידע מסוים וגבוה, ואז עליו להמתין ולראות אם הרשות להגנת הפרטיות תמצא בפעולות העיבוד שהוא מעבד פגם כלשהו. לעומת זאת, חובת עריכת תסקיר מחייבת את בעל השליטה במאגר המידע להתחשב בשיקולי פרטיות משלב הפיתוח ולאורך כל שלבי עיבוד המידע. אף שהתסקיר הוא תסקיר פנימי, בעל השליטה נדרש לתעד את עריכתו כדי להוכיח במידת הצורך שאכן נקט את כל הפעולות המתאימות למזעור הפגיעה בפרטיות. כלומר, לשם עמידת בחובת התסקיר יהיה על בעל השליטה במידע לנקוט גישה אקטיבית יותר ולבחון מקרוב את כל היבטי עיבוד המידע, ולא לצמצם את פעולותיו לפעולות ציות טכניות להוראות החוק.

אשר לחובת הרישום, אכן חובה זו לא חלפה לחלוטין מהעולם. בקליפורניה, שאימצה חוק הגנה פרטיות במידע ברוח ה־GDPR, חייבים סוחרי מידע ברישום. מטרת הרישום הזה היא להבטיח את שקיפות השימוש במידע אישי לעיני הציבור. אולם, חובת הרישום בקליפורניה נבדלת מזו המוחלת לפי תיקון 13 בכמה היבטים מרכזיים, כמפורט בלוח שלהלן:

מסמך מעודכן של מבנה מאגר המידע, ובעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה חייב בעריכת סקר סיכונים בכל 18 חודשים לפחות. עם זאת, אין מדובר בחובת קיום תסקיר השפעה מקיפה, כפי שהסבירה הרשות להגנת הפרטיות עצמה. ראו הרשות להגנת הפרטיות **תסקיר השפעה על פרטיות – מדריך עזר מתדולוגי** (נובמבר 2022).

חובת הרישום בקליפורניה	חובת הרישום לפי תיקון 13
חלה על כל בעל שליטה במידע שהוא סוחר מידע. מספר נושאי המידע שמידע על אודותיהם נמצא במאגר המידע אינו רלוונטי כלל לתחולת חובת הרישום.	חלה על בעלי שליטה במאגר מידע שהם גופים ציבוריים או סוחרי מידע שמאגר המידע שבשליטתם כולל מידע אישי על יותר מ־10,000 נושאי מידע.
הגדרה ברורה ל"סוחר מידע": (א) אוסף מידע אישי במודע; (ב) מוכר מידע אישי כאמור לצד שלישי. מכירה מוגדרת בהרחבה, והיא כוללת צורות שונות של שיתוף מידע בעבור רווח פיננסי או בעל ערך אחר; (ג) אין מערכת יחסים ישירה בין נושא המידע לסוחר המידע.	אין הגדרה מפורשת ל"סוחר מידע", ותיקון 13 אף אינו עושה שימוש במונח, והוא הופיע רק בדיונים בוועדת החוקה. חובת הרישום חלה על מי ש"אוסף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה."[371] הגדרה זו רחבה דייה כדי לכלול, למשל, את כל תעשיית הפרסום באינטרנט.[372]
חובה שנתית, שמטרתה להבטיח שבידי הציבור יהיה מידע מעודכן ככל הניתן על השימוש הנעשה במידע אישי על אודותיהם על ידי סוחרי מידע.[373]	חובה חד־פעמית. לראש הרשות סמכות למחוק מאגר מידע אם בעל השליטה הודיע לו על ביעורו. כן מוטלת על בעל השליטה חובה להודיע לראש הרשות על שינוי בפרטים שהוא נדרש לציין בבקשת הרישום או על הפסקת פעילות המאגר.[374]
מינואר 2026 על סוחרי מידע לפרט אם הם אוספים מידע אישי על קטינים, נתוני מיקום מדויקים ומידע בריאות.	אין חובה ספציפית.

371 סעיף 4 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 8א(א)(1)(א) לחוק הגנת הפרטיות.

372 פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 63–69.

373 CCPA, לעיל ה"ש 47, בסעיף 1798.99.82.

374 סעיף 9(ד) לחוק הגנת הפרטיות.

חובת הרישום בקליפורניה	חובת הרישום לפי תיקון 13
סנקציות בגין אי־רישום: קנס מינהלי; סוחר מידע אינו יכול למכור את המידע האישי שאסף שלא מנושא המידע ישירות בלי להודיע לנושא המידע, אלא אם נרשם כסוחר מידע.	סנקציות בגין אי־רישום: קנס מינהלי; אסור לסוחר מידע לעבד מידע במאגר מידע שמספר נושאי המידע בו עולה על 10,000 אם לא נרשם.
מינואר 2026: הוקם מנגנון מחיקה שיאפשר לנושאי מידע להגיש בקשה אחת למחיקת פרטים אישיים על אודותיהם ממאגרי מידע של סוחרי מידע. על סוחרי המידע להיכנס למאגר בקשות המחיקה בכל 45 ימים ולהיענות לכל בקשות המחיקה הרלוונטיות להם. כן עליהם להורות לכל ספקי השירותים שעימם הם עובדים למחוק את המידע האישי המבוקש. אם סוחר המידע אוסף מידע אישי חדש על לקוח שביקש את מחיקתו מהמאגר, אסור לסוחר המידע למכור מידע אישי או לשתף בו צד ג, ועליו לחדש את בקשת המחיקה בכל 45 ימים. מינואר 2028 יחויבו סוחרי מידע בביקורת חיצונית של צד שלישי עצמאי בכל שלוש שנים כדי לבחון את מידת הציות שלהם לבקשות מחיקה. תוצאות הבדיקה יוגשו לנציבות הפרטיות לפי דרישתה.[375]	זכות מחיקה מצומצמת בנסיבות האלה: (1) במסגרת הזכות לתקן מידע אישי, אם נושא המידע מצא שהוא אינו נכון, שלם, ברור או מעודכן.[376] (2) אם מאגר המידע משמש לדיוור ישיר.[377]

375 Senate Bill No. 362, ch. 709, 2023 Cal. Stat. (amending Cal. Civ. Code §§1798.99.80, 1798.99.81, 1798.99.82, 1798.99.84; adding §§1798.99.85, 1798.99.86, 1798.99.87, 1798.99.89) (approved Oct. 10, 2023). ראו גם Libbie Canter, Sarah Parker & Andrew Longhi, *California Amends Data Broker Law*, Privacy & Data Security (Nov. 1, 2023).

376 סעיף 14(א) לחוק הגנת הפרטיות.

377 סעיף 17ו(ב) לחוק הגנת הפרטיות.

הבדלים אלו בין חובת הרישום בקליפורניה לחובה שהוטלה בתיקון 13 מלמדים דווקא שיש מקום להרחיב את חובת רישום מאגרי המידע ביחס לסוחרי מידע, כמו החובה הנהוגה בקליפורניה. במסגרת זו יש להגדיר "סוחרי מידע" הגדרה ברורה בחוק, שתבטיח שחובת הרישום לא תהפוך לנטל בירוקרטי על ארגונים שאין הצדקה להטלתה עליהם, וכן להסיר את מגבלת 10,000 נושאי המידע היוצרת את חובת הרישום, ולחייב סוחרי מידע לפרט בבקשת הרישום את פרטי המידע בעלי הרגישות המיוחדת שהם אוספים.

7.5. חובת מינוי ממונה אבטחת מידע

עדכון החובה למנות ממונה על אבטחת מידע בתיקון 13 שימר את העיקרון שבעל שליטה במאגר מידע או מחזיק יהיה חייב למנות ממונה אבטחת מידע אם בשליטתו או בחזקתו חמישה מאגרי מידע לפחות החייבים ברישום או במסירת הודעה לרשות להגנת הפרטיות. אולם, עיקרון זה נשען על אמת מידה שרירותית ואינו נותן מענה מקיף לסכנות אבטחת המידע האפשריות. כך, למשל, בעל שליטה במאגר מידע שלו מאגר מידע אחד בלבד של מידע בעל רגישות מיוחדת על יותר מ־100,000 נושאי מידע לא יחוב במינוי ממונה אבטחת מידע, אף שסכנות האבטחה הטמונות במאגר כזה עשויות להיות חמורות בהרבה מהסכנות הצפויות לבעל שליטה במאגר מידע שלו חמישה מאגרי מידע מאגרי מידע קטנים שאינם כוללים מידע בעל רגישות מיוחדת כלל או אינם כוללים מידע בעל רגישות מיוחדת בהיקפים גדולים. זאת ועוד, חובת מינוי ממונה אבטחת מידע המוטלת על המחזיק מותנית בכך שמאגרי המידע שברשותו חבים ברישום או בדיווח, אולם חובות אלו אינן מוטלות כלל על מחזיק, והוא אף עשוי שלא להיות מודע כלל לכך שמאגרי המידע שבחזקתו חבים ברישום או בדיווח.[378] למשל, מחזיק הנותן רק שירותי אחסון אינו מודע כלל למהות מאגר המידע שהוא מחזיק, לרגישות המידע שבמאגר או למספר נושאי המידע שבו.

378 פרוטוקול מס' 249, לעיל ה"ש 253, בעמ' 117–127.

רוב מאגרי המידע שהוא מאחסן מוצפנים בכוונה, והוא אינו מודע כלל לתוכנם או למספרם. הוא מאחסן מידע בהתאם לנפח.[379]

ב־GDPR, למשל, אין חובה מפורשת למנות ממונה אבטחת מידע. ארגונים נוטים בכל זאת למנות ממונה אבטחת מידע מכורח החובה המוטלת עליהם לנקוט אמצעים טכניים וארגוניים ראויים להבטחת הגנה נאותה לנוכח הסיכונים הסבירים הצפויים.[380] הסדר דומה קיים גם בקליפורניה.[381] כך ייתכן שגם אצלנו אפשר לוותר על הטלת חובת מינוי ממונה אבטחת מידע שאינה מתאימה יותר לעיבודי המידע הדיגיטליים ולהסתפק בהוראת סעיף 17 לחוק הגנת הפרטיות המטילה על בעל שליטה במאגר מידע ועל מחזיק אחריות כללית לאבטחת מידע, מתוך בחינת עדכון הוראת סעיף 17 והכפפתה למבחן סבירות. עם זאת, יש להביא בחשבון כיצד יפרשו הארגונים במשק את ביטול חובת המינוי, ואת החשש שהוא יביא לזילות בתפיסת אבטחת המידע. בהקשר הזה יש לשקול שהאסדרה המקיפה של הנושא תיעשה דווקא בחוק הגנת סייבר ולא במסגרת חוק הגנת הפרטיות.[382]

7.6. צמידות מטרה מול הגבלת מטרה

עקרון צמידות המטרה הוא עיקרון ארכאי שאינו מתאים עוד למציאות עיבודי המידע הדיגיטליים הנוכחיים.[383] ב־GDPR לא משתמשים כלל במונח "צמידות מטרה", אלא במונח "הגבלת מטרה", מתוך הכרה בכך שיתכנו מטרות דומות שבעל השליטה במידע לא צפה אותן בעת איסוף המידע הראשוני. אולם מדובר

379 פרוטוקול מס' 265, לעיל ה"ש 281, בעמ' 49–53; פרוטוקול מס' 334, לעיל ה"ש 128, בעמ' 34–35.

380 סעיף 32 ל־GDPR, לעיל ה"ש 33.

381 CCPA, ה"ש 47 לעיל, בסעיף 1798.100(e).

382 להרחבה בסוגיה זו, ראו אריאל הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 98.

383 ראו הדיון בתת־פרק 4.1 לעיל.

במטרות הקרובות דיין למטרה הראשית והחוקית שבה נקב בעל השליטה במידע בתחילה, ולכן יש להתיר לבעל השליטה לעבד מידע למטרות דומות אלו אף אם העיבוד אינו "צמוד" למטרה הראשונית.[384]

ההבדל בין "צמידות מטרה" ל"הגבלת מטרה" הוא הבדל חשוב. דרישת הגבלת מטרה ברוח ה־GDPR מאפשרת גמישות בעיבוד המידע המתאימה לעידן המודרני, שבמסגרתו בעל השליטה במאגר המידע אינו יודע מראש, בעת איסוף המידע או הקמת מאגר המידע, את מכלול המטרות לשמן יוכל לעבד מידע אישי, חוסר ידיעה שיחמיר עוד יותר עם התגברות השימוש בבינה מלאכותית. כך, למשל, לפי עקרון צמידות המטרה, בעל שליטה האוסף מידע אישי לשם מציאת נתיב הנסיעה בתחבורה ציבורית המתאים למאפייניו של נושא המידע (גיל, מידת ניידות, חוסר סבלנות, רגישות לחום, חרדה סביבתית וכד'), לא יוכל לעשות שימוש במידע האישי גם לשם פרסום שירות מוניות מהיר. עם זאת, לפי עקרון הגבלת המטרה ייבחן הקשר בין המטרה הראשונית למטרה הנוספת המבוקשת, נסיבות איסוף המידע האישי ומערכת היחסים בין בעל השליטה לנושא המידע, רגישות המידע האישי שבו נעשה שימוש והשלכות עיבוד המידע הנוסף, ועיבוד המידע למטרת הפרסום עשוי להיות מותר.[385] בהיעדר חריג מיוחד המתיר עיבוד מידע למטרות מחקר,[386] ההבדל בין עקרון צמידות המטרה להגבלת המטרה נעשה משמעותי אף יותר, בעיקר בכל הקשור למחקר מדעי ורפואי. כך, למשל, בעל שליטה המעבד מידע אישי כחלק ממחקר לטיפול במחלת המעיים קרוהן, המגלה קורלציות העשויות ללמד על אפשרות לגילוי מוקדם של סרטן המעי הגס, לא יוכל לעשות במידע שימוש למטרה הנוספת על פי עקרון צמידות המטרה.

384 פרוטוקול מס' 298, לעיל ה"ש 187, בעמ' 25–28.

385 ראו סעיף 6(4) ל־GDPR, לעיל ה"ש 33 ; אריאל הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 48, בעמ' 51–52.

386 דומה לסעיף 5(1)(b) ל־GDPR, לעיל ה"ש 33.

זאת ועוד, הדרישה לצמידות העיבוד למטרה הנקבעת כדין עם הקמת המאגר מחזירה את הדיון בקושי לקבוע הלכה למעשה מתי מוקם מאגר מידע, שכן כאמור מאגר מידע הוא פיקציה, יציר המשפט.[387]

הניסוח הנוכחי של עקרון צמידות המטרה בחוק הגנת הפרטיות בעקבות תיקון 13 יוביל לכך שבעלי שליטה במאגרי מידע יבחרו לנסח רשימת מטרות ארוכה וחסרת גבולות, ככל העולה על רוחם בעת הקמת המאגר. בעלי השליטה יוכלו להשתמש בניסוח מעורפל שיאפשר בפועל עיבוד מידע לכל מטרה חוקית. לחלופין, אם אין מדובר במידע אישי שנאסף על בסיס הסכמת נושא המידע או במאגר מידע המוקם לפי חוק, יוכלו בעלי השליטה במאגר המידע להקים מאגר מידע חדש כל אימת שיבקשו לעבד מידע למטרה שלא נרשמה בתחילה. כדי למנוע מצבים כאלה, במקום הוראות צמידות המטרה שבחוק הגנת הפרטיות, יש לדעתנו לאמץ מתווה להגבלת מטרה שיאפשר עיבוד מידע אישי גם למטרות דומות, דומה לזה הנהוג ב־GDPR.[388]

7.7. הרחבת אגד זכויות נושא המידע

כדי לתת בידי נושאי המידע סט כלים להתמודדות עם עיבוד מידע אישי על אודותיהם ולהביא את הגנת הפרטיות במדינת ישראל לרמה הדומה מהותית לזו הנהוגה במרבית מדינות המערב, יש להרחיב את זכות העיון ואת זכות התיקון הנמצאות כבר היום בחוק הקיים, ולהוסיף זכויות נוספות, כגון –

387 פרוטוקול מס' 347, לעיל ה"ש 199, בעמ' 3–4.

388 ראו, למשל, הצעתנו בנושא משנת 2019, אריאל הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 48, בעמ' 51–52.

7.7.1. חובת הודעה לנושא המידע

כאמור,[389] תיקון 13 משמר את הניסוח הקיים בחוק הגנת הפרטיות לחובת מסירת הודעה לנושא המידע. לפיכך, החובה קמה רק כאשר פונים לנושא המידע. בכך מצומצמת חובת ההודעה לנסיבות שבהן המידע האישי נאסף ישירות מנושא המידע. אולם במציאות עיבוד המידע המודרנית מרבית המידע האישי לא נאסף ישירות מנושא המידע. למשל, ברשתות חברתיות, כאשר המידע האישי מגיע דרך צדדים שלישיים המסכימים לאיסוף מידע אישי על אודותיהם, או דרך גירוד מידע אישי המפורסם בפומבי באתרי אינטרנט.[390]

לפיכך, כדי לחזק את זכויות נושא המידע ולהבטיח שקיפות מירבית יש לתקן את חובת מסירת ההודעה לנושא המידע הקבועה בסעיף 11 לחוק הגנת הפרטיות. במסגרת התיקון יש לקבוע שחובה זו תחול במפורש על בעל שליטה במאגר מידע, שכן הוא הקובע איזה מידע ייאסף ולאילו מטרות ישמש. על החובה הזאת להבטיח גם את יידוע נושא המידע הן בנסיבות שבהן המידע האישי נאסף ישירות ממנו, הן בנסיבות הרווחות יותר שבהן נאסף המידע האישי על אודותיו בעקיפין. ייתכן שיש מקום לאמץ חריגים מצומצמים לחובת ההודעה לנושא המידע, ברוח החריגים הקבועים בסעיף 14 ל־GDPR. החרגת מצומצמת של גופי ביטחון מחובה זו, מובנת, אולם אין לקבל את הטענה שיש להחריג גם גופים ציבוריים. הנימוק שמרבית הגופים הציבוריים אינם יכולים לעמוד בחובת ההודעה לנושא המידע אינו ענייני ואינו מקובל.[391]

זאת ועוד, לפי עמדת הרשות, כפי שהוצגה בטיוטת הנחיית הבינה המלאכותית, חובת מסירת ההודעה לנושא המידע כוללת גם פרטי מידע שאינם מופיעים כלל במסגרת החובה לפי חוק הגנת הפרטיות. למשל, מידע על אודות הסיכונים

389 ראו הדיון בתת־פרק 5.1 לעיל.

390 ראו פרוטוקול מס' 223, לעיל ה"ש 57, בעמ' 140–142.

391 פרוטוקול מס' 233, לעיל ה"ש 57, בעמ' 37–38.

הכרוכים בעיבוד מידע אישי באמצעות בינה מלאכותית.[392] משום כך, ראוי לבחון בשנית, במסגרת תיקון עתידי, מהם פרטי המידע שיש צורך לכלול במסגרת חובת ההודעה לנשוא המידע וכיצד אפשר להציגם באופן קצר ותמציתי, כדי להבטיח שהודעה אכן תשרת את רציונל הגברת השקיפות ולא תהפוך לנטל בירוקרטי שאיש לא ייתן עליו את הדעת.

7.7.2. הוספת הזכות להתנגד לעיבוד מידע אישי

זכות זו תאפשר לנושא המידע להתנגד לעיבוד מידע אישי מסיבות הקשורות במצבו האישי, הכלכלי, הבריאותי או הנפשי, כאשר עיבוד המידע האישי או בעל הרגישות המיוחדת נעשה בהתאם לבסיס החוקי, שיוסף לחוק,[393] המתיר עיבוד מידע להגשמת אינטרס מהותי של בעל השליטה או של צד שלישי. למשל, במקרים שבהם עיבוד המידע האישי ערער את מצבו הנפשי של נושא המידע או גרם לו לנזק כספי ניכר. מטרת הוספת זכות זו היא להבטיח שהשימוש של בעל השליטה בבסיס החוקי המאפשר לו לעבד מידע אישי לשם הגשמת אינטרס מהותי שלו תיעשה בצמצום ורק לאחר שבעל שליטה במידע איזן כראוי בין ההגנה על האינטרס המהותי שלו למול זכות נושא המידע לפרטיות, והבטיח שהפגיעה בפרטיות עומדת במבחן המידתיות והסבירות. כך, הזכות להתנגד מחייבת את בעל השליטה לקיים איזון ובדיקות כאמור ולתעדן כדי שיהיה בידו להוכיח כי זכותו להמשיך ולעבד את המידע האישי למרות התנגדות נושא המידע.

הזכות להתנגד מבוססת על סעיף 21 ל־GDPR, אך יש לאמצה בצמצום רק למקרים שבהם העיבוד נעשה לפי הבסיס החוקי של הגשמת אינטרס מהותי של בעל השליטה. הצדקת התנגדות נושא המידע לעיבוד על בסיס מצבו הבריאותי, הנפשי, האישי או הכלכלי מבוססת על הפרשנות שניתנה למונח "particular situation" בסעיף 21 ל־GDPR.

392 הרשות להגנת הפרטיות "הנחייה – תחולת חוק הגנת הפרטיות על מערכות בינה מלאכותית" טיוטה להערות הציבור (28.4.2025).

393 בהתאם למוצע בסעיף 7.3 לעיל.

7.7.3. הוספת הזכות לקבל הסבר

הכוונה להעניק לנושא המידע זכות לקבל הסבר מידתי מבחינת היקפו אם ההחלטה בעניינו, המשפיעה על זכויותיו, מבוססת, במלואה או ברובה, על עיבוד אוטומטי של מידע אישי. מטרת זכות זו היא למנוע מצב קפקאי שבו מתקבלת החלטה בעניינו של נושא המידע שאינה ברורה לו ושמשפיעה על זכות או על חובה שלו על פי דין. בדרך זו תחוזק השקיפות בפעולותיהם של בעלי שליטה, והם יחויבו לשקול, ואף להנגיש, את הפרמטרים מתוך המידע האישי שנעשה בהם שימוש בעת קבלת החלטה בעניינו של אדם. לזכות זו מיוחסת חשיבות רבה עם התגברות השימוש בבינה מלאכותית לשם קבלת החלטות.

הזכות לקבל הסבר מבוססת על סעיף 22(1) ל־GDPR האוסר על קבלת החלטה יחידה שיש לה השלכות משפטיות או בעלות משמעות על נושא המידע ומבוססת רק על עיבוד אוטומטי של או על אפיון (profiling), כלומר החלטה המתקבלת אך ורק על ידי מכונה.[394] הפרשנות המקובלת של הוראה זו היא שמדובר באיסור על קבלת החלטות אוטומטיות ולא בזכות נושא המידע שלא להיות נתון להחלטות אוטומטיות מחזקת נושאי מידע המצויים במערכת יחסים המאופיינת בפערי כוחות, כמו יחסי עובד–מעביד המקשים על נושאי המידע להביע עמדה חופשית ולהתנגד באמת לפעולות של המעסיק, כגון שימוש בכלי ניהול אלגוריתמיים לשם קבלת החלטות אוטומטיות.[395] ה־GDPR מעגן כמה חריגים לאיסור על החלטות אוטומטיות. אולם, גם בהתקיים אחד החריגים על בעל השליטה להטמיע בכל זאת אמצעים מתאימים להגנה על הזכויות, החירויות והאינטרסים הלגיטימיים של נושא המידע.[396] כך, נדרש שלנושא המידע תהא הזכות לדרוש מעורבות אנושית

394 סעיף 22(1) ל־GDPR והפרשנות שניתנה לו ב־Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-making and Profiling for the Purpose of Regulation 2016/679, 17/EN 251rev.01 (6.2.2018), בעמ' 19.

395 Margot E. Kaminski, *The Right to Explanation, Explained,* 34 Berkeley Tech. L. J. 189, 201 (2019)

396 Margot E. Kaminski, *The Right to Explanation, Explained,* 34 Berkeley Tech. L. J. 189, 207, 209 (2019) ; Celine Castets-Renard, *Accountability of Algorithms in the GDPR and Beyond: A European Legal*

מצד בעל השליטה, להציג את נקודת המבט שלו בנוגע לעיבוד המידע ולהחלטה המבוססת על עיבוד זה, ואף לערער עליה.[397] בספרות נחלקות הדעות בשאלה אם אמצעים אלו כוללים גם את זכותו של נושא המידע לקבל הסבר בנוגע להחלטה בעניינו.[398] הרציונל שבסיס דרישת היידוע למתן הסבר הוא התפיסה ששקיפות הכרחית כדי לגבש אחריותיות. השקיפות כלפי נושא המידע היא שמאפשרת ביקורת על פעולות בעל השליטה, לרבות גופים ציבוריים, ומבטיחה שהארגון יכבד את נושא המידע, יציית לדרישות החוק ויפעל באחריות.[399]

7.7.4. הוספת זכות המחיקה של מידע אישי

הכוונה לעיגון מאוזן ומידתי בחוק של הזכות להישכח, כדי לאפשר לנושא המידע לדרוש את מחיקת המידע אם הוא חזר מהסכמתו לעיבוד המידע אישי על אודותיו, או אם התברר שהעיבוד נעשה בניגוד למטרה שלשמה נאסף או בניגוד לחוק. עיגון כאמור יכול להישען על זכות המחיקה בסעיף 17 ל־GDPR. הזכות לפי ה־GDPR חלה על המידע האישי שנאסף מנושא המידע, וכן על המסקנות או התובנות שהוסקו ממנו.[400] זכות זו מצומצמת רק לנסיבות האלה: המידע האישי אינו נחוץ עוד להשגת המטרה לשמה נאסף או עובד; נושא המידע חזר בו מהסכמתו; נושא המידע מתנגד לעיבוד מידע אישי על אודותיו ואין בסיסים לגיטימיים אחרים המתירים לבעל השליטה במידע להמשיך בעיבוד המידע האישי על פי ה־GDPR; נושא המידע הסכים לעיבוד במידע אישי על אודותיו כאשר היה קטין ולא היה מודע לחלוטין לסכנות הנלוות לעיבוד, ומאוחר יותר הוא מבקש להסיר את המידע האישי; המחיקה נדרשת על פי חוק; או כאשר

Framework on Automated Decision-Making, 30 Fordham Intell. Prop. Media & Ent. L. J. 91, 123-124 (2019)

397 GDPR, לעיל ה"ש 33, בסעיפים 22(2)(b), 22(3).

398 GDPR, שם, בסעיף הקדמה 71.

399 Kaminski, לעיל ה"ש 396, בעמ' 201-216; Castets-Renard, לעיל ה"ש 395, בעמ' 91, 109, 112.

400 Article 19 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01 (Oct. 3, 2017)

עיבוד המידע האישי אינו עומד בדרישות ה־GDPR. עם זאת, אין מדובר בזכות מוחלטת. סעיף 17(3) ל־GDPR מעגן כמה חריגים המאפשרים לבעל השליטה במידע לסרב לבקשת המחיקה של נושא המידע.

7.7.5. הוספת זכות לניוד מידע אישי

מטרת זכות הניוד היא לשכלל את השוק על ידי עידוד התחרות בין בעלי שליטה שונים ולחזק את שליטת נושא המידע במידע אישי על אודותיו על ידי מניעת "נעילת" (locking) המידע האישי שלו בפלטפורמת שירותי מידע אחת, וכך להקטין את תלותו של נושא המידע בבעל שליטה מסוים. המדובר בזכות חדשה שעוגנה בפעם הראשונה בסעיף 20 ל־GDPR. עם זאת, במסגרת תיקון עתידי של חוק הגנת הפרטיות רצוי לבחון אימוץ זכות רחבה יותר מהזכות האירופית. במסגרת זו זכות הניוד צריכה לחול על כל מידע אישי שנאסף על נושא המידע, בין בהסכמתו בין מכוח בסיס חוקי אחר. צמצום הניוד אך ורק למידע אישי שסופק על ידי נושא המידע עצמו, או נוצר על ידי בעל השליטה מתצפית על התנהגותו ופעולותיו של נושא המידע, עלול לפגוע בהשגת המטרה העיקרית של הזכות, שהיא הגברת התחרות בין בעלי שליטה במידע ומניעת מצב של "נעילת" מידע אישי על נושאי מידע בפלטפורמה אחת בלבד. נוסף על כך, בניסוח הזכות יש להבהיר שאין בה כדי להביא להפסקת עיבוד המידע האישי על ידי בעל השליטה או המעבד, וכי לשם כך על נושא המידע לחזור בו מהסכמתו, אם ניתנה, או לפנות בבקשה למימוש הזכות להישכח.

כמו כן, נוכח החשש שזכות הניוד עלולה להביא לפגיעה חמורה בעסקים קטנים ובינוניים דווקא, שלא יוכלו להתמודד עם העברת מידע אישי מהם בשלבי פעילותם הראשונית, ובתוך כך להעצים את כוחן של החברות הגדולות ולהחליש את התחרות, מוצע לקבוע כי בהחלטת השר, לאחר התייעצות עם ראש הרשות להגנת הפרטיות ובאישור ועדת החוקה יהיה אפשר להחריג בעלי שליטה במידע מסוימים מסיבות הקשורות בגודלם, במשך הזמן שחלף מרגע היווסדם או בנתח השוק שהם מחזיקים בו.

7.8. העצמת יכולות החקירה והאכיפה של הרשות להגנת הפרטיות: שיתוף פעולה בינלאומי

כחלק מתפקידי הרשות להגנת הפרטיות ראוי לאפשר לה במפורש בחוק לשתף פעולה, לרבות באמצעות העברת מידע אישי שנאסף במהלך הליך אכיפה ופיקוח, עם רשויות להגנת פרטיות ברחבי העולם, על בסיס ההבנה שפגיעה בזכות לפרטיות, בעיקר פרטיות במידע, עשויה להיות חוצת גבולות. כך, למשל, בפרשת קיימברידג' אנליטיקה נחשף מידע אישי על כ־47 אלף משתמשי פייסבוק מישראל.[401] משום כך, שיתוף פעולה בין רשויות הגנת פרטיות ברחבי העולם הוא כורח המציאות כדי לחקור פגיעה בזכות לפרטיות ולהביא לאכיפה יעילה של דיני הגנת הפרטיות. הוראות בדבר שיתוף פעולה כאמור יש גם ב־GDPR, המכיר בצורך להתיר העברת מידע אישי בין רשויות מדינתיות מנימוקים הקשורים באינטרס הציבור, למשל, בין רשויות מדינתיות להגבלים עסקיים, או בין רשויות מדינתיות להגנת הפרטיות מדינתיות, לשם ייעול אכיפת דיני הגנת הפרטיות.[402]

הצורך בשיתוף מידע אישי בין רשויות מדינתיות קיבל גם הכרה בינלאומית בעקבות החקירה המשותפת שניהלו רשויות הגנת הפרטיות בקנדה, אוסטרליה וה־FTC האמריקני, בנוגע לחשיפת מידע אישי ומידע רגיש על משתמשי אתר ההיכרויות אשלי מדיסון.[403] כך, בספטמבר 2017 נחתמה החלטה בדבר הצורך בבחינת עקרונות חקיקתיים שאימוצם יאפשר שיתוף פעולה בינלאומי במישור החקירתי. ההחלטה הדגישה כי שיתוף פעולה בינלאומי נועד להגביר את הציות

401 שגיא כהן "פייסבוק: מידע על 47 אלף ישראלים נחשף בפרשת קיימברידג' אנליטיקה" **ynet** (10.4.2018).

402 ראו סעיפי הקדמה 112 ו־116 וסעיף 50 ל־GDPR, לעיל ה"ש 33.

403 ראו FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation, FTC (Sep. 27, 2017)

לחוקי ההגנה על הפרטיות.[404] שיתוף במידע לצורכי אכיפה וחקירה בין רשויות מקובל בדין הישראלי בדיני ניירות ערך,[405] וניתן לאמץ הסדר דומה גם בחוק הגנת הפרטיות.[406]

7.9. תחולה אקס־טריטוריאלית

כמו בסעיף 3 ל־GDPR, מוצע לקבוע שבנסיבות מסוימות תחולת הוראות חוק הגנת הפרטיות הנוגעות לעיבוד מידע אישי תהיה אקס־טריטוריאלית, כדי למנוע מבעלי שליטה במידע להתחמק מציות להוראות הצעת החוק על ידי העברת מידע אישי על אודות נושאי מידע ישראלים לחוות שרתים הממוקמות במדינות שאינן מחייבות הגנת פרטיות ברמה דומה לזו שתידרש בחוק הגנת הפרטיות הישראלי.

נוסף על כך, וכמו בסעיף 27 ל־GDPR, מוצע לחייב בעלי שליטה מסוימים להחזיק נציגות מקומית בישראל, כדי לאכוף את הוראות החוק גם על תאגידי ענק בינלאומיים שאין להם נציגות משפטית מקומית, בד בבד עם הימנעות מפגיעה בתחרות והדרת שחקנים בינלאומיים מתחומי מדינת ישראל.

404 ראו 39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, 25–29 Sep. 2017, Resolution on exploring future options for International Enforcement Cooperation (2017)

405 סעיפים 54יא1–54יא9 לחוק ניירות ערך, תשכ"ח–1968.

406 כפי שהצענו בהצעת חוק הגנת הפרטיות מטעם המכון הישראלי לדמוקרטיה בשנת 2019. ראו אריאל הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 48, בעמ' 105–109.

7.10. סיכום ההצעות לתיקונים נוספים

נושא	התיקון המוצע
הגדרת "מאגר מידע" כשער התחולה הראשון לחוק הגנת הפרטיות	ביטול ההגדרה "מאגר מידע" והשימוש במונח לאורך החוק. חוק הגנת הפרטיות צריך לחול על כל מידע אישי, בין שהוא מאוגד במאגר מידע ובין לאו. לחלופין, קביעת רף נמוך יותר מ־100,000 נושאי מידע להחרגת מאגרי מידע המשמשים עסקים קטנים וזעירים. לחלופין מתן מענה מבחינת חובת אבטחת מידע גם לאוספי מידע אישי שלא יחשבו "מאגר מידע".
הגדרת "בעל שליטה" במאגר מידע	מעקב אם ההגדרה הקיימת עתה מובילה לאכיפת יתר נגד גורמים שאין להם כל שליטה בפועל על עיבוד מידע אישי, ובחינה אם יש צורך בהרחבת ההגדרה ברוח האיחוד האירופי.
יחסי הכוחות בין "בעל שליטה" לבין "מחזיק"	הגדרה ברורה בחוק הגנת הפרטיות בנוגע לנושאים שבאחריות כל אחד מבעלי התפקידים.
הגדרת "מנהל מאגר"	תיקון תקנות העברת מידע בין גופים ציבוריים, וביטול מלא של המונח "מנהל מאגר" גם בגופים ציבוריים.
הוספת בסיסים חוקיים לעיבוד מידע לבד מהסכמה	אימוץ מנגנון המתיר עיבוד מידע אישי בנסיבות מסוימות, דומה לזה המקובל ב־GDPR, כדי להחליש את ההישענות הבעייתית על דרישת ההסכמה.
הוספת זכות "חזרה מהסכמה"	כדי להחליש את ההישענות על הסכמת נושא המידע לשם עיבוד מידע יש להוסיף לזכויות נושא המידע את זכות החזרה מהסכמה. זכות זו תאפשר לו לחזור בו מהסכמתו לעיבוד מידע אישי בכל עת, ותוביל לכך שבעלי שליטה יעדיפו להישען על בסיסים חוקיים אחרים לעיבוד מידע אישי ולא על הסכמת נושא המידע.
חובת ההודעה לרשות להגנת הפרטיות	ביטול חובת ההודעה לרשות להגנת הפרטיות, ובמקומה הוספה של חובת עריכת תסקיר השפעה על הפרטיות.
חובת הרישום	הרחבת חובת הרישום המוטלת על סוחרי מידע, דומה לזו הנהוגה בקליפורניה.

נושא	התיקון המוצע
חובת מינוי ממונה אבטחת מידע	תיקון התנאים למינוי ממונה אבטחת מידע, או לחלופין, הסתפקות בהטלת חובה לאבטחת מידע על פי מבחן סבירות. לחלופין, בחינת העברת הנושא לחוק הגנת סייבר ייעודי.
צמידות מטרה	החלפת עקרון צמידות המטרה בחוק הגנת הפרטיות בהגבלת מטרה, דומה להסדר הקבוע ב־GDPR המכיר גם בעיבוד למטרות דומות.
הרחבת אגד זכויות נושא המידע	תיקון חובת ההודעה לנושא המידע, כך שתחול גם אם המידע האישי לא נאסף מתוך פנייה לנושא המידע. הוספת הזכות להתנגד לעיבוד מידע אישי, הזכות לקבלת הסבר, זכות המחיקה וזכות הניוד.
התרת שיתוף מידע בין רשויות חקירה	אימוץ הסדר ברוח ההסדר הקבוע בחוק ניירות ערך, שיתיר לרשות להגנת הפרטיות לשתף מידע, לרבות מידע אישי שנאסף בהליכי פיקוח וחקירה, לשם ניהול מאמצי פיקוח ואכיפה חוצי גבולות.
תחולה אקס־טריטוריאלית	הרחבת תחולת חוק הגנת הפרטיות הנוגעות לעיבוד מידע אישי לפי מיקום נושא המידע, דומה לתחולה האקס־טריטוריאלית של ה־GDPR, וחיוב בעלי שליטה מסוימים להחזיק נציגות מקומית בישראל.

סיכום

תיקון 13 – יתרונותיו וחסרונותיו

תיקון 13 מסמן שינוי חשוב בדיני הגנת הפרטיות בישראל. בתיקון הובהרו ועודכנו מונחי מפתח, צומצמה חובת הרישום, הוטלה חובת מינוי ממונה הגנת פרטיות, בוטלה מגבלת ההתיישנות, הוספו פיצויים לדוגמה וחוזקו סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות. בכך יש כדי לחזק את נושא המידע ולשפר את רמת הגנת הפרטיות בישראל.

עם זאת, תיקון 13 אינו ממצה ואינו מוביל להשוואת רמת הגנת הפרטיות בישראל לרמה הנהוגה במדינות האיחוד האירופי ובמדינות שאימצו חקיקה דומה ל־GDPR. גם אחרי התיקון דרישת ההסכמה נותרה התנאי הבלעדי להכשרת עיבוד מידע, כמו כן, לא נוספו לחוק בסיסים חוקיים לעיבוד מידע ולהרחבת זכויות נושא המידע, וכך נותרו בו חוסרים ניכרים. זאת ועוד, החיזוק החשוב לסמכויות הפיקוח, האכיפה והענישה של הרשות להגנת הפרטיות, לצד היעדר תיקון לדין המהותי, עלולים להביא לאי־בהירות ולבלבול בעניין תחולת הוראות חוק הגנת הפרטיות, פרשנותן והתאמתן לעיבודי המידע הדיגיטליים המתקדמים.

לפיכך, במצב הדברים הנוכחי, כדי להביא את דיני הגנת הפרטיות בישראל לרמת הגנה נאותה ומקבילה לרמה המקובלת במדינות האיחוד האירופי ובמדינות שאימצו חקיקה דומה ל־GDPR, ובה בעת לצמצם את הקושי ואת חוסר הוודאות הנלווים לאחר התיקון לעיבוד מידע אישי, יש צורך בתיקונים נוספים לחוק הגנת הפרטיות. תיקונים אלו יצמצמו את הפער בין דיני הגנת הפרטיות במדינת ישראל לדינים שבמדינות המערב, ועם זאת, יותאמו לתנאי הארץ ותושביה. כן חשוב שהתיקונים ישקפו את הלקחים שניתן להפיק כבר עתה מניסיונן של

מדינות האיחוד האירופי ביישום הוראות ה־GDPR ומהתאמתן לטכנולוגיות מתקדמות.[407]

זאת ועוד, בבחינת השינויים הנוספים הנדרשים בחוק הגנת הפרטיות יש לתת את הדעת גם להשפעת תיקון 13 על התנהלותם של גופים במגזר הפרטי ובמגזר הציבורי, ולבחון אם וכיצד אפשר לשפר עוד את הגנת הפרטיות בגופים אלו, ובד בבד לצמצם את הנטל הבירוקרטי המוטל עליהם. בחינת השפעת תיקון 13 כאמור יכולה להיעשות על בסיס הדיווח המקיף שעל הרשות להגנת הפרטיות למסור לוועדת החוקה בכל שנה.[408]

תובנות הקשורות להליך החקיקה

לצד ההתעמקות בחידושים שבתיקון 13 ובחסרונותיו, אפשר ללמוד מהליך החקיקה תובנות חשובות נוספות.

חשיבות השיח בין הגורמים הרלוונטיים. הליכי החקיקה שהובילו לאימוצו של תיקון 13 מצביעים על חשיבות השיח בין גורמי עניין, ובהם הרשות המבצעת (משרד המשפטים), הרגולטור הרלוונטי (הרשות להגנת הפרטיות), ונציגים מהחברה האזרחית, מהאקדמיה והמגזר הציבורי והפרטי. שיח כזה הביא לתיקון לשון הצעת החוק הממשלתית, להסרת סעיפי חוק בעייתיים ממנה ולהוספת הוראות חשובות שלא היו בה. השיח התקיים לא רק בין כותלי חדר הדיונים של ועדת החוקה. כך, למשל, לפני הצגת ההסדר בנוגע למינוי ממונה הגנת פרטיות התקיים שיח חשוב בין כל גורמי העניין, ושיח זה השפיע במידה מסוימת על ההסדר שהציג משרד המשפטים בסופו של דבר בוועדת החוקה עצמה.

407 חלק מהתיקונים פורטו בסעיף 7 לעיל.

408 סעיף 24 לתיקון 13, לעיל ה"ש 3, המוסיף את סעיף 17ט3 לחוק הגנת הפרטיות.

זאת ועוד, פתיחותם של הגורמים הממשלתיים, ובראשם מחלקת ייעוץ וחקיקה במשרד המשפטים והרשות להגנת הפרטיות לנהל שיח כאמור, להציג את עמדותיהם, לשמוע את העמדות מהשטח, וגם ביקורת, ראויה לציון, והיה לה משקל מכריע בליטוש התיקונים לחוק הגנת הפרטיות שאומצו לבסוף בתיקון 13.

חשיבות התשומות של ועדת הכנסת הדנה בחקיקה ממשלתית. תובנה חשובה נוספת נוגעת לתפקיד שמילאו ועדת החוקה עצמה, הייעוץ המשפטי של הוועדה ויו"ר הוועדה. בפני ועדת החוקה עמדה הצעת חוק ממשלתית, שלחקיקתה נלוותה גם דחיפות מסוימת, משום שהדיונים בה התקיימו לאחר 7 באוקטובר, תוך כדי המלחמה, לבקשת המל"ל.[409] נוסף על כך, באותו זמן התקיים גם שיח בין משרד המשפטים, הרשות להגנת הפרטיות ונציגי האיחוד האירופי, להכרה בתאימות הדין בישראל לדין המקובל באיחוד האירופי. להכרה זו חשיבות כלכלית רבה, ובין השאר, ניתן בשיח שהתקיים עם נציגי האיחוד האירופי גם משקל להבטחה לחוקק את תיקון 13.[410] למרות זאת, ועדת החוקה לא קיבלה את הצעת החוק הממשלתית ככתבה וכלשונה, ולאורך הדיונים הייתה קשובה לשיח בין גורמי העניין שהתנהל בחדר הוועדה בשאיפה להביא את הגנת הפרטיות בישראל לרמה הקרובה ביותר האפשרית במצב הנוכחי לזו המקובלת במדינות המערב, ובראשן האיחוד האירופי, מתוך בחינת ההסדרים המקובלים במשפט המשווה והתאמתם לתנאי הארץ ותושביה.[411] כך מילאה ועדת החוקה תפקיד חשוב באימוצם של הסדרים, דוגמת מינוי ממונה הגנת פרטיות, שלא הופיעו

409 פרוטוקול מס' 190 מישיבת ועדת החוקה, חוק ומשפט, יום שני, כ"א בכסלו התשפ"ד (4 בדצמבר 2023), בעמ' 5, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

410 פרוטוקול מס' 190 מישיבת ועדת החוקה, חוק ומשפט, יום שני, כ"א בכסלו התשפ"ד (4 בדצמבר 2023), בעמ' 11, דברי ניר ברנגה; פרוטוקול מס' 233 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, י"א בשבט התשפ"ד (21 בינואר 2024), בעמ' 47 דברי ראש הרשות להגנת הפרטיות, עו"ד סממה; הרשות להגנת הפרטיות, נציבות האיחוד האירופי אישרה שמדינת ישראל היא מדינה בעלת מעמד תאימות (adequacy) בתחום הגנת הפרטיות, (15 בינואר 2024).

411 פרוטוקול מס' 190, לעיל ה"ש 287 , בעמ' 23, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

בהצעת החוק הממשלתית ושהיה בהם כדי להביא לשיפור בהגנת הפרטיות של אזרחי מדינת ישראל.

עם זאת, מהתרשמות בלתי אמצעית של כותבת שורות אלו, שנכחה ברוב ישיבות ועדת החוקה שעסקו בתיקון 13, חשוב לציין שפעמים רבות מצא עצמו יו"ר ועדת החוקה, ח"כ רוטמן, לבד בדיונים. בחלק מועט מהדיונים נכחו חברי כנסת נוספים, אולם מעורבותם הייתה מועטה. אומנם הדיונים התקיימו במהלך מלחמת חרבות ברזל, אולם מצער שתיקון חוצה משק כמו תיקון 13, שיש לו השפעה של ממש על המגזר הפרטי והאזרחי, לא זכתה לקשב רב אצל מרבית המחוקקים.[412]

שיתוף ציבור. מהניסיון שנצבר בעת הדיונים בתיקון 13 בוועדת החוקה אפשר ללמוד שבגיבוש התיקונים הנוספים הנדרשים לחוק הגנת הפרטיות יש חשיבות גדולה לשיתוף ציבור. כבר עתה, בדיונים בתיקונים הנוספים הנדרשים, ראוי לשלב נציגים מגורמי מפתח רלוונטיים, כגון גופי הביטחון ואכיפת החוק, התעשייה, האקדמיה והחברה האזרחית. נציגים אלו צריכים להפגין מעורבות וידע בתחום. כך יוכלו לסייע בניסוח התיקונים הדרושים ולזרז את הליך קבלתה של הצעה לתיקון החוק. אין המדובר בשיתוף ציבור ברמה הנעשית כיום – פרסום טיוטת הנחיות או תזכיר חוק להערות הציבור בתוך זמן קצוב ובאופן פורמלי. שיתוף הציבור הנדרש במסגרת המוצעת יאפשר שיח בלתי אמצעי עם מומחים משלל התחומים הרלוונטיים, בפתיחות ובכנות. הניסוח הסופי יוותר כמובן מנת חלקה של הרשות להגנת הפרטיות ושל מחלקת ייעוץ וחקיקה במשרד המשפטים.

412 להרחבה על תפקיד ועדות הכנסת וכיצד יש לשפרן, ראו חן פרידברג, אביטל פרידמן ונעה גשן **איך משפרים את עבודת הכנסת ומחזקים את מעמדה? המלצות עיקריות** (המכון הישראלי לדמוקרטיה, מהדורה מעודכנת, 2024).

ד"ר רחל אריאלי הרשקוביץ היא חוקרת בכירה בתוכנית "דמוקרטיה בעידן המידע" במכון הישראלי לדמוקרטיה. דוקטור למשפטים מהפקולטה למשפטים באוניברסיטת חיפה; בעלת תואר ראשון מאוניברסיטת חיפה ותואר שני במשפטים מאוניברסיטת ניו יורק. תחומי המחקר שלה הם פרטיות, הגנת סייבר, רשתות חברתיות ואתגרי המציאות הפיג'יטלית.

המכון הישראלי לדמוקרטיה
www.idi.org.il