פרטיות ובחירות

לקראת בחירות 2026

רחל ארידור הרשקוביץ | תהילה שוורץ אלטשולר

מרץ 2026

טיוטה

הצעה לסדר 64

המכון הישראלי לדמוקרטיה

המכון הישראלי
לדמוקרטיה

פרטיות ובחירות: לקראת בחירות 2026

רחל ארידור הרשקוביץ | תהילה שוורץ אלטשולר

מרץ 2026

הצעה לסדר 64

טיוטה

תוכן העניינים

חלק שלישי
המלצות לקראת הבחירות לכנסת ה־26

תקציר

הצעה לסדר זו בוחנת את האתגרים שמציב השימוש במידע אישי במסגרת תעמולת בחירות בעידן הנוכחי. השימוש במידע על בוחרים אינו תופעה חדשה, אך בשנים האחרונות התרחש שינוי עומק באופן ניהול קמפיינים פוליטיים: מעבר מתעמולה מבוססת נתונים לתעמולה המשלבת מאגרי מידע רחבי היקף, יכולות ניתוח מתקדמות מבוססות בינה מלאכותית של מאפיינים פסיכולוגיים ורגשיים של בוחרים, תוך טשטוש הגבולות בין מידע שנמסר ביודעין לבין מידע המוסק באמצעים אלגוריתמיים, וטכנולוגיות ליצירת תוכן מותאם אישית בהיקפים רחבים, באופן אוטומטי ובזמן אמת.

מאפיינים אלו לא רק מעצימים את האפקטיביות של תעמולת בחירות, אלא גם משנים באופן מהותי את אופי ההשפעה הפוליטית על ציבור הבוחרים. עקב כך הם גם יוצרים סיכונים משמעותיים לזכות לפרטיות, לאוטונומיה של הבוחר, לחשאיות הבחירות ולטוהר הבחירות.

על רקע הבחירות לכנסת ה־26, במחקר זה אנו מבקשות להניח תשתית מושגית ומעשית להתמודדות עם השפעותיה של תעמולה חישובית על פרטיות הבוחרים ועל טוהר הבחירות; ולהבהיר את גבולות הדיון הנורמטיבי לנוכח הפערים הקיימים בין דיני הפרטיות לבין דיני הבחירות, ולנוכח כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות.

ההצעה מציגה סט כלים יישומיים להתמודדות עם אתגרים אלה, ובהם עקרונות פעולה והכוונה רגולטוריים לגורמי הפיקוח הרלוונטיים ובראשם יו״ר וועדת הבחירות המרכזית והרשות להגנת הפרטיות, לצד שאלון בדיקה עצמית וניהול סיכוני פרטיות למפלגות ולגורמים המפעילים יישומוני בחירות. כלים אלו נועדו לסייע בזיהוי מוקדם של אתגרים הנובעים משימוש במידע אישי ובטכנולוגיות מתקדמות, ולחזק את היכולת להבטיח שימוש ראוי במידע במסגרת תעמולת בחירות, באופן המגן על פרטיות הבוחרים ועל תקינות ההליך הדמוקרטי.

מבוא

תעמולת בחירות נשענה מאז ומתמיד על מידע אישי אודות קהל הבוחרים. שימוש במידע אישי לשם הפצת תעמולה דיגיטלית מותאמת אישית גם הוא אינו חדש.[1] נשיא ארצות הברית ברק אובמה נחשב לראשון שעשה שימוש נרחב בפלטפורמות דיגיטליות כבר בקמפיין ההתמודדות הראשון לנשיאות בשנת 2008.[2] בקמפיין הבחירות לנשיאות ארצות הברית בשנת 2016 הופצו ברשתות חברתיות מסרי תעמולה אישיים לתמיכה בדונלד טראמפ בהתבסס על מידע אישי שנאסף אודותיהם בפייסבוק ועובד, ללא הסכמתם, על ידי חברת קיימברידג' אנליטיקה.[3] בקמפיין הבחירות לנשיאות ארצות הברית בשנת 2024 פיתח צוות הקמפיין של טראמפ אסטרטגיית פרסום דיגיטלית ממוקדת שבחנה כיצד מצביעים מתלבטים במדינות מפתח צורכים תוכן, לרבות תוכן פוליטי. בהתאם לממצאי ניתוח זה התמקד קמפיין הבחירות של טראמפ בכ־6.3 מיליון מצביעים בשבע מדינות מתנדנדות שאליהם הוצגו מסרי בחירות בפרסומות בשידורי סטרימינג, בדיוור ישיר ובהודעות טקסט. כך הצליח קמפיין הבחירות למשוך את תשומת ליבם של בוחרים מתלבטים במדינות מפתח תוך השקעת משאבים כספיים מינימליים יחסית.[4]

בגרמניה, בבחירות בשנת 2021, עשו כל המפלגות שימוש במיקרו־טרגטינג פוליטי בפייסבוק על מנת למשוך מצביעים. תלונות ששימוש כאמור הוא הפרת האיסור הקבוע ב־GDPR על שימוש במידע על דעה פוליטית,[5] הוגשו לנציבות הגנת המידע בגרמניה. אולם, במערכת הבחירות הפדרליות בשנת 2025 המשיכו המפלגות לעשות שימוש בטקטיקה זו, אך השתמשו לשם כך במידע אישי שאינו דעה פוליטית, כמו למשל מידע על להקות אהובות, במטרה להעריך את נטייתו הפוליטית של הבוחר.[6]

ההתפתחות הטכנולוגית של תעמולה ממוקדת אישית ומבוססת מידע אישי וחישוב מביאה עימה יתרונות אך גם חששות לא מעטים, ובראשם היכולת להשפיע על דעות פוליטיות ובעיקר על העדפות והתנהגויות של הבוחרים, כגון מניפולציה שתביא לדיכוי הצבעה של ציבור מסוים. יכולות אלה מעניקות למועמדים ולמפלגות יתרון על פני הבוחרים ומאיימות על תקינות הליך הבחירות ועל עקרון ההוגנות בבחירות.[7] משום כך, השאלה מהו היקף וסוג המידע האישי שמותר לעשות בו שימוש במסגרת

---

[1] *Daniel Kreiss & Shannon C. McGregor, The "Arms Race" in U.S. Digital Campaigning,* 35 POL. COMMC'N 155 (2018); DIDIER BIGO ET AL., EDS., DATA POLITICS: WORLDS, SUBJECTS, RIGHTS (2019); להרחבה באשר לסכנות לפגיעה באוטונומיה ובבחירה החופשית, ראו, תהילה שוורץ אלטשולר וגיא לוריא, **תעמולה דיגיטלית והאיום על הבחירות**, המכון הישראלי לדמוקרטיה, מחקר מדיניות 155 (דצמבר 2020) (להלן: "שוורץ אלטשולר ולוריא").

[2] Ed Pilkington & Amanda Michel, *Obama's team of tech gurus to unleash 'Holy Grail' of digital campaigning*, THE GUARDIAN (14 May, 2012)

[3] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, THE GUARDIAN (March 17, 2018); Joe Westby, *'The Great Hack': Cambridge Analytica is just the tip of the iceberg*, AMNESTY INTERNATIONAL (July 24, 2019)

[4] John Connors, *Trump's Digital Ad Strategy Redefined Political Campaigning in 2024*, CAMPAIGN NOW (Nov. 6, 2024); Makena Kelly, *Donald Trump's Win Cements a New Era for Campaigning Online*, WIRED (Feb. 8, 2025)

[5] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1 (EU), סעיף 9(1).

[6] Noyb, *Snap Election faster that German DPAs: Microtargeting continues to influence voters* (Feb. 21, 2025);

[7] Stephan Lewandowsky & Peter Pomerantsev, *Technology and Democracy: a Paradox Wrapped in a Contradiction inside an Irony*. MEMORY, MIND & MEDIA 1: e5 (2022), https://doi.org/10.1017/mem.2021.7

תעמולת בחירות ומהם השימושים המותרים למניפולציה על בוחרים במסגרת זו, מצויה היום בלב הדיון במדינות דמוקרטיות רבות.[8]

במערכות הבחירות האחרונות בישראל, כשלו הניסיונות להתמודד בזמן אמת, במהלך מערכת הבחירות עצמה, עם התפר שבין דיני הפרטיות ודיני הבחירות כפי שבא לידי ביטוי בשימושים במידע אישי, בעיקר באמצעות יישומוני בחירות, והשלכותיהם האפשריות על הגנה על זכות הבוחרים לפרטיות ועל עקרון טוהר הבחירות והוגנות הבחירות. אולם, טכנולוגיות תעמולה ממוקדת אישית המבוססות על מידע, לרבות מידע אישי, כמו גם הכללים המשפטיים המאסדרים שימוש במידע אישי השתנו דרמטית מאז מערכת הבחירות הקודמת בשנת 2022.

ראשית, כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות באוגוסט 2025,[9] צפויה להשפיע על השימוש שייעשה במידע אישי על אודות בעלי זכות ההצבעה בישראל במערכות הבחירות הבאות. תיקון 13 והמהלכים הנלווים לו מביאים עמם שינוי עומק בתפיסת ההגנה על מידע אישי בישראל, ומציבים סטנדרטים חדשים של אחריות, פיקוח וממשל נתונים.

שנית, היכולות הטכנולוגיות לניתוח מידע אישי, היסקים מבוססי מכונה, מיקרו־מיקוד והשפעה פוליטית השתכללו באופן ניכר בשנים האחרונות, בעיקר על רקע ההתפתחויות המואצות בתחום הבינה המלאכותית.

שלישית, החששות מפני דליפות מידע, מתקפות סייבר ושימושים עוינים בנתונים רגישים הפכו לנוכחים ומוחשיים במיוחד בתקופה הנוכחית, כאשר המלחמה וגם התפתחות טכנולוגיות בתחום הסייבר מחדדות את פגיעותן של מערכות מידע.

מטרת מחקר זה היא להבהיר בעיקר את התפר המחודש שבין דיני הפרטיות לדיני הבחירות והוא יחולק לארבעה חלקים. בחלק הראשון נעסוק ב"תעמולה חישובית" ובמאפייניה סביב המעבר לתעמולה מבוססת בינה מלאכותית, וכן ביישומוני הבחירות כמכשיר מרכזי לניהול בחירות ובפוטנציאל הטכנולוגי שהתווסף בשנים האחרונות בשל פיתוח יישומים מבוססי למידת מכונה. בחלק השני נעסוק במצב המשפטי הקיים בנושא פרטיות ובחירות, כפי שהתעצב במערכות הבחירות האחרונות. בחלק השלישי, נסקור את השינויים בחוק הגנת הפרטיות בעקבות תיקון 13 שיש בהם רלבנטיות לשימוש במידע אישי במסגרת תעמולת בחירות. בחלק הרביעי נציע המלצות ליישום ולשינוי: שאלון בחינה עצמית למפלגות ולמנהלי יישומים הקשורים לבחירות לעמידה בדרישות החוק, והמלצות לרשות להגנת הפרטיות וליו"ר ועדת הבחירות המרכזית.

[8] Judit Bayer, *Double harm to voters: data-driven micro-targeting and democratic public discourse*, 9(1) Cristina Blasi Casagran & Mathias Vermeulen, *Reflections on the murky legal practices of political micro-targeting from a GDPR perspective*, 11(4) INTERNATIONAL DATA PRIVACY ; INTERNET POLICY REVIEW (2020) (2021)

[9] חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות"); חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024 (להלן: "תיקון 13").

חלק ראשון

תעמולה דיגיטלית באמצעות מידע אישי

פרק ראשון
שימושים במידע אישי בקמפיינים של בחירות

1. מבוא

"תעמולה חישובית" משמעה מפלגות ומועמדים בקמפיין בחירות האוספים ומרכזים כמויות גדולות של נתונים דיגיטליים אישיים מזוהים על בוחרים, ומייחסים ערך אסטרטגי לצבירתם; מנתחים את הנתונים באמצעות שיטות חישוביות וכלים מתחום חקר ההתנהגות; ותוצרי הניתוח משמשים אותם באופן אוטומטי ליצירה ולהפצה בקנה מידה רחב של מסרים פוליטיים המותאמים אישית לבוחרים.[10]

יצירת הפרופילים משפיעה הן על הבוחרים נושאי המידע והן על החברה הדמוקרטית, בעיקר משום חוסר ההגינות האינהרנטי העולה מהחדירה למכמני נפשו של אדם תוך שימוש בטכנולוגיה והתאמת מסרים ל"מקומות הרכים" שבהם הוא עשוי להיות רגיש יותר להשפעה. העובדה שרוב הטכניקות האלה מתבצעות ללא ידיעת הבוחרים ומחוץ לרדאר התודעה שלהם, מאיימת על חופש הבחירה שלהם ויוצרת "מלכודת" על האוטונומיה שלהם בעוצמה ובאיכות שלא ידענו כמותן בעבר.[11] יש הטוענים כי בשנים האחרונות מצויות מפלגות בכל העולם הדמוקרטי במצב של "מרוץ חימוש של נתונים", שבו הן נשענות על ספקים מסחריים רבי עוצמה, בעוד הרגולציה והאכיפה נותרות בדיעבד, חלקיות ולעיתים עמומות. מצב זה פוגע בשקיפות, יוצר פערי כוח משמעותיים, ומערער את אמון הציבור בטוהר הליך הבחירות.[12] על כן, הגדרת גבולות הלגיטימיות של תעמולת הבחירות באמצעות תעמולה חישובית ואסדרתה חשובות מאוד, והתפר בין דיני הפרטיות – איסוף סוגים שונים של מידע; הגדרת הרמה והעומק של הפרופילים שמפלגות ומועמדים יכולים לבנות ולאגור; ניתוח וכיוונון עמוק ואישי של השפעה (מיקרו־טרגטינג) על בוחרים – לבין דיני הבחירות, הוא קריטי.[13]

באופן מסורתי קמפיינים פוליטיים מבוססים על שתי שאלות יסוד: האחת – האם מדובר בבוחר שבכוונתו לצאת ולהשתתף בהצבעה; והאחרת – האם אותו בוחר יצביע למפלגה שלה מיועד הקמפיין. כשמדובר בקמפיין דיגיטלי מבוסס נתונים, המטרה אפוא לפלח את הבוחרים לאחת מארבע קטגוריות: (א) אלה היוצאים להצביע ויצביעו למפלגה המועדפת; (ב) אלה היוצאים להצביע ויצביעו למפלגה אחרת; (ג) אלה שאינם יוצאים להצביע אבל תומכים במפלגה המועדפת; (ד) אלה שאינם יוצאים להצביע אבל תומכים במפלגות אחרות, ולמצוא את המתלבטים כדי להניע אותם לפעולה הרצויה. הפילוח נעשה

---

[10] The European Commission, *Study on the Impact of New Technologies on Free and Fair Elections*, September 2021, https://commission.europa.eu/document/4b280290-8848-4a21-aec5-b00baaf77e42_en; Katharine Dommett, Glenn Kefford & Simon Kruschinski, DATA-DRIVEN CAMPAIGNING AND POLITICAL PARTIES: FIVE ADVANCED DEMOCRACIES COMPARED, Chapter 1: Theoretical Frameworks, 20-43, Oxford University Press, 2023

[11] להרחבה ראו תהילה שוורץ אלטשולר "פרטיות – מלכת זכויות האדם בעולם דיגיטלי" **פרלמנט** 83 (2019).

[12] Jacob Ohrvik-Stott, *Moral Hazard: Voter Data Privacy and Politics in Election Canvassing Apps* (Open Rights Group, 2025)

[13] להרחבה ראו שוורץ אלטשולר ולוריא, לעיל ה"ש 1, עמ' 16–19.

באמצעות סוגים מגוונים של נתונים ומטרתו להתאים לכל חבר בקבוצה את המסרים המתאימים לו ביותר וכך להעביר בוחרים מקבוצה לקבוצה.[14]

2. מרכיבי קמפיינים של תעמולה חישובית

קמפיינים מבוססי נתונים[15] (Data-Driven Campaigning – DDC) או קמפיינים של תעמולה חישובית, מבוססים על שני מאפיינים מרכזיים – האחד הוא מיקוד (targeting), כלומר קביעה "מה" (איזה מסר) יישלח ל"מי" (אילו בוחרים) ו"מתי" (באיזה שלב של הקמפיין); והשני הוא בדיקה אמפירית (testing), כלומר מדידה שיטתית של ביצועי מסרים שונים והשוואתם זה לזה, באופן המאפשר להפיק תובנות המכוונות את המשך פעילות המיקוד.[16] כדאי להדגיש שאין מדובר רק במאפיינים טכנולוגיים, אלא תפקודיים. אכן, ארגונים פוליטיים אוספים כמויות גדולות של נתונים אישיים על בוחרים ויוצרים מהם מאגרי נתונים גדולים ומפורטים, ונתונים אלה עוברים ניתוח באמצעות כלים סטטיסטיים ומודלים אלגוריתמיים המאפשרים הפצה של מסרים מותאמים אישית או מיקרו־מכוונים בקנה מידה המוני.[17] אבל, במקביל, תוצאות הניתוחים האלה והמלצות המערכות הטכנולוגיות, הופכות לגורם מכריע בקבלת ההחלטות של ניהול הקמפיין, עד כדי כך שהן עשויות לקבוע בפועל את כיווני הפעולה הטקטיים והאסטרטגיים, לעיתים באופן אוטומטי ודטרמיניסטי וללא דיון אנושי שוטף. המערכת הארגונית של הקמפיין פועלת כך שהקצאת משאבים, בחירת קהלי יעד ועיצוב המסרים נקבעים בעיקר על בסיס הנתונים והמודלים האלגוריתמיים, ולא על פי שיקול דעת אנושי.

קמפיין פוליטי מבוסס נתונים כולל שלושה שלבים: (א) איסוף המידע על הבוחרים; (ב) ניתוח ועיבוד שלו; (ג) התאמת המסרים וטרגוט שלהם.

השלב הראשון בקמפיין פוליטי מבוסס נתונים הוא איסוף וגישה לנתונים על בוחרים, כאשר נתונים אלה צריכים להיות בעלי היקף ופירוט המאפשרים מיקוד אישי. כלומר, מדובר בכריית מידע על בוחרים ועיבודו למידע ממויין. הנתונים כוללים דמוגרפיה אישית (כגון גיל ומין), מאפיינים חברתיים (כגון השכלה), תכונות משוערות (כגון תחומי עניין או סוג אישיות), וכן מידע על התנהגות מקוונת ולא־מקוונת, למשל רכישות, מנויים, פעילות ברשתות חברתיות או נתוני מיקום. נתונים אלה יכולים להגיע מארבעה סוגי מקורות מרכזיים:

---

[14] שם.

[15] Rachel Gibson, Esmeralda Bon & Andrea Römmele, *Operationalizing Data-Driven Campaigning: Designing a New Tool for Mapping and Guiding Regulatory Intervention*, 45:5 POLICY STUDIES 692-708 (2024), DOI: 10.1080/01442872.2023.2259333; Hendrik Mildebrath, *The Arrival of E-voting and Campaign Technologies in Europe: Promise, Perils and Preparedness*, EPRS | European Parliamentary Research Service, May 2024, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762321

[16] Jessica Baldwin-Philippi, *The Myths of Data-Driven Campaigning*, 34(4) POLITICAL COMMUNICATION, 627–633 (2017). https://doi.org/10.1080/10584609.2017.1372999

[17] Elizabeth F. Judge & Michael Pal, *Voter Privacy and Big-Data Elections*, 58.1 OSGOODE HALL LAW JOURNAL 1-55 (2021), 1-55. DOI: https://doi.org/10.60082/2817-5069.3631

(1) רשומות ציבוריות כגון פנקסי בוחרים:

רשומות ציבוריות הן בראש ובראשונה פנקס הבוחרים אך יכולות להיות רחבות מזה ולכלול מאגרים אחרים הנמצאים בשליטת המדינה או הרשויות המקומיות. דוח של ארגון Human Rights Watch שפורסם לאחר הבחירות בהונגריה בשנת 2022 מצביע על שימוש בעייתי במידע אישי שנאסף על ידי המדינה לצרכים מינהליים, אך הוסב לשימוש פוליטי במסגרת קמפיין הבחירות של מפלגת השלטון פידס (Fidesz). לפי הדוח, הממשלה עשתה שימוש בפרטי קשר של אזרחים שנמסרו במסגרת פניות לשירותים ציבוריים שונים, כגון רישום לחיסוני קורונה, בקשות לקבלת הטבות מס או רישום לארגונים מקצועיים, כדי להפיץ מסרים פוליטיים התומכים במפלגת השלטון ובמדיניותה.

הדוח מדגיש כי שימוש חוזר לצרכים אלקטורליים במידע (repurposing) שאזרחים מסרו לממשלה לצורך קבלת שירות ציבורי מסוים, פוגע באמון הציבורי ויוצר ערבוב בין משאבי המדינה לבין פעילות מפלגתית. לפי ממצאי הדוח, טשטוש הגבולות בין הממשלה לבין מפלגת השלטון, יחד עם שליטה מוסדית של הממשלה בגופים ציבוריים, תרם לכך שהשימוש במידע זה לא נאכף באופן אפקטיבי על ידי רשויות הפיקוח. המקרה ההונגרי מדגים כיצד מאגרי מידע ממשלתיים עשויים להפוך למשאב אסטרטגי במערכות בחירות מבוססות נתונים. כאשר ממשלות מחזיקות במידע אישי בהיקף רחב על אזרחים, האפשרות להסב מידע זה לשימוש פוליטי מעניקה יתרון משמעותי למפלגת השלטון.[18]

רשומות ציבוריות המצויות בידי המדינה עשויות לכלול בנוסף גם מידע סטטיסטי ומידע מרשם האוכלוסין, כגון מידע דמוגרפי וכלכלי. למשל, גזע, מוצא אתני, גיל הילדים או מצב משפחתי. נדגיש כי יכולות זיהוי חוזר של מידע מותמם התעצמו מאוד ולכן למידע זה יש ערך גם לצורך הגעה אל בוחרים מזוהים.[19]

(2) מאגרי מידע מסחריים של חברות פרטיות:

מאגרי מידע מסחריים של חברות פרטיות עשויים לכלול מידע שנאסף מהמשתמש עצמו או מגופים שהעניקו לו שירותים. החל בהיסטוריית קניות בסופרמרקט המגיעה מחברות מרכולים או היסטוריית אשראי המגיעה מחברת האשראי, עובר ב"שביל פירורי לחם דיגיטליים" – פעילות דיגיטלית הכוללת שימוש ביישומונים סלולריים, היסטוריית גלישה ונתוני מיקום, וכלה בשימוש במוצרים דיגיטליים לבישים כגון שעונים חכמים או מכשירים אחרים שמקושרים לרשת האינטרנט באמצעות מכשירי ה־GPS בטלפונים שלהם, בלוטות' ורשתות WiFi, והכול בזמן אמת וברמות דיוק גבוהות.[20]

השגת מידע על גולשים אינו נעשה רק באמצעות מעקב ישיר אחריהם, אלא גם באמצעות ניתוח של מאגרי מידע גדולים כדי לאתר אנשים ששעשויים להיות בעלי מאפיינים דומים לאנשים שיש עליהם מידע אישי כתוצאה ממעקב ישיר אחריהם. הטכניקה של "אפיון דומים" (Look-alike Modelling) מאפשרת

---

[18] *Trapped in a Web, The Exploitation of Personal Data in Hungary's 2022 Elections*, Human Rights Watch, 2022, https://www.hrw.org/report/2022/12/01/trapped-web/exploitation-personal-data-hungarys-2022-elections

[19] Lucas Georges, Gabriel Charpentier & Pierre Lison, *Re-identification of De-identified Documents with Autoregressive Infilling* (May 2025), https://doi.org/10.48550/arXiv.2505.12859

[20] פרסומאי שעבד עם מפלגת הליכוד טען בריאיון לאחר הבחירות במרץ 2020 שבליכוד ידעו היכן המצביעים נמצאים ברמת דיוק של 15 מטר, וכך הם הסיקו אם הם נשארו בבית או יצאו להצביע. כשנשאל על כך מאוחר יותר, הכחיש את עצם קיומם של המעקבים. ראו איתמר ב"ז "ידענו לעקוב אחרי הטלפון של כל אחד, זה היה בדאטה שלנו, האם הוא הלך לאזור הקלפי או נשאר בבית" **העין השביעית** 7.3.2020, https://www.the7eye.org.il/364201

למשווקים "לשבט" לקוחות בעלי מאפיינים דומים. המפלגה מעלה את פרטי המידע הידועים לה על קבוצת אנשים שהזדהו כתומכי המפלגה, הם קבוצת המקור (Seed / Source Audience). האלגוריתם של הפלטפורמה מנתח את פרטי המידע שהוזנו על קבוצת המקור, מזהה דפוסים במאפיינים אלה ולאחר מכן מחפש בבסיס המשתמשים הקיים בפלטפורמה את המשתמשים עם פרופילים דיגיטליים דומים. קבוצות המשתמשים הדומות מקוטלגות בדרך כלל לפי רמת הדמיון או הזהות בין מאפייניהם למאפייני קבוצת המקור. שיטה זו מכונה בפלטפורמות של חברות מטא וטיק־טוק "Lookalike Audiences", ובפלטפורמת הפרסומות של גוגל "Similar Audiences". עם זאת, גם חברות עצמאיות המפתחות יישומוני בחירות ייעודיות עושות שימוש באלגוריתמים דומים.[21] בדרך זו יכול מנהל הקמפיין הפוליטי להגדיל ביעילות את קהל היעד למסרי התעמולה שלו.[22] בנוסף, יישומוני בחירות שונים מבקשים ממי שמתקין אותם לאפשר גישה אל כל אנשי הקשר שלו, וכך המערכת יוצרת "עץ" של קשרי חברות בין בוחרים המסייע גם כן בגיבוש קבוצת הדומים והגדלת קהל היעד.

(3) מאגרי מידע פנימיים של מפלגות המבוססים על פעילות שטח וסקרים או על פנקסי בוחרים או מידע על בוחרים מבחירות קודמות שלא נמחקו.

(4) מידע הנאסף מהאינטרנט, לרבות אפשרויות מיקוד המוצעות על ידי רשתות חברתיות וכוללות מידע כגון מי חבר של מי, מי משפיע על מי, עמדות פוליטיות בפוסטים, תחומי עניין של גולשים, מידת האינטראקציה של המשתמש ותגובותיו לתוכן המפורסם ברשת החברתית (engagement) לרבות זמן צפייה, תגובות, לייקים או שיתופים, השתייכות לקבוצות, האשטגים ועוד. הנתונים עשויים להיאסף ולהישמר במאגרי מידע פנימיים של הקמפיין או באמצעות ספקים חיצוניים.[23]

השלב השני בקמפיין פוליטי מבוסס נתונים הוא ניתוח הנתונים ויצירת "פרופיל" לכל בוחר. יש שיטות שונות לניתוח נתונים ליצירת פרופיל באמצעות תוכנות ניתוח למטרות של חיזוי, מדרוג (רייטינג) וניקוד (סקורינג). אלו מיועדות בעיקר לסיווג ולחלוקה של הבוחרים על בסיס מערכת מדויקת של מאפיינים וסמנים של מידע דמוגרפי והתנהגותי. בשל היקף הנתונים הגדול, שיטות הניתוח הן לרוב אוטומטיות וכמותיות, אם כי לעיתים נעשה גם קידוד אנושי של נתונים איכותניים. המדובר בניתוח נתונים המוכר מהעולמות הפרסום המסחרי. פלטפורמות האינטרנט הגדולות, בעיקר מטא וגוגל, מציעות מגוון רחב של כלי עיבוד למידע פרטי, והיתרון התחרותי שלהן הוא לרוב הקשר בין הזהות בעולם האמיתי (כתובת דוא"ל או מספר טלפון), הנדרשת כתנאי להצטרפות לרשת חברתית או לקבלת שירותים אחרים, ובין פרדיגמת הטירגוט שלהן.[24]

---

[21] למשל חברת Aristotle האמריקאית מציעה מערכת לניהול קמפיין פוליטי הכוללת, בין השאר, מידע על מצביעים לשם העברת מסרי תעמולה מותאמים אישית. ראו באתר החברה, https://www.aristotle.com/data

[22] Hunt Allcott *et. al.*, *The Effect of Political Advertising on Facebook and Instagram before the 2020 US Election*, NATIONAL BUREAU OF ECONOMIC RESEARCH, Working Paper 33818 (2025), https://www.nber.org/papers/w33818

[23] להרחבה ראו שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 23–35, וכן Dominik Bär, Francesco Pierri, Gianmarco De Francisci Morales & Stefan Feuerriegel, Systematic Discrepancies in the Delivery of Political Ads on Facebook and Instagram, PNAS Nexus, page 247 (2024), https://doi.org/10.1093/pnasnexus/pgae247

[24] Rachel Kraus, *How Well Does "Microtargeted Psychographic Advertising" Work Anyway?* MASHABLE (Mar. 24, 2018), https://mashable.com/2018/03/24/how-microtargeted-ads-affect-behavior/

השלב השלישי בקמפיין פוליטי מבוסס נתונים הוא יישום תוצאות הניתוח לצורך תקשורת פוליטית מותאמת אישית. זו כוללת (1) עיצוב של מסרים מותאמים אישית, ו־(2) הפצה מותאמת אישית לבוחרים. אחד הכלים המרכזיים בשלב זה הוא פרסום ממוקד (micro-targeted advertising) ברשתות חברתיות, באמצעות מערכות התאמה אוטומטיות של פלטפורמות ; שימוש בפלטפורמות סטרימינג דיגיטליות ; או הפצה מתואמת לא אותנטית ברשתות חברתיות של תכנים כגון פוסטים, ציוצים, סרטונים והודעות טקסט שנועדו להיות מופצים מחדש ברשת באופן ויראלי ולתת לגולשים תחושה כוזבת שהגיעו אליהם באופן אורגני. אבל, נקודות ההשקה עם מושא הקמפיין יכולות לכלול נקודות השקה הנעות מטלוויזיה מסורתית חכמה ועד לפרסום מותאם אישית על גבי משקפיים חכמים. זאת, כדי להתאים תכנים לאנשים ספציפיים ולפלטפורמות ספציפיות ; לדייק את מועד ההפצה, למשל סמוך להתרחשותם של אירועים ואת מיקומה הגיאוגרפי, למשל כאשר מושא הקמפיין נמצא במקום מסוים ; וליצור "קריאייטיב דינמי", כלומר לתפור מסרים באופן מתפתח, לאורך זמן ובאופן שמתאים בכל פעם מחדש למושא המסר. מאפיין מרכזי של שלב זה הוא אופיו המחזורי והניסויי – ביצועי המסרים נמדדים באופן שיטתי, בזמן אמת, והתוצאות משמשות לשיפור מודלי הניתוח, איסוף הנתונים ועיצוב המסרים.[25]

מודלים חישוביים מתקדמים משמשים לחיזוי התנהגות בוחרים. למשל, חישוב הסתברויות תגובה (propensity scoring) לצורך הערכת הסיכוי שבוחר מסוים יגיב למסר מסוים או שמסר יניע אותו לפעולה מסוימת. טירגוט ברשתות חברתיות למשל מבוסס על עיבוד המידע ואיתור קשרים עם המשתמשים בהתבסס על גיל, מגדר, מוצא אתני, אזור בחירה, תחומי עניין והפרופיל הרגשי שלהם, ועל ידי כך שיפור היכולת למצוא את נקודות ההשפעה עליהם. פעולה זו של עיבוד מידע מכונה גם "טרגוט פסיכוגרפי".[26]

שאלת האפקטיביות של מיקרו־טירגוטים המבוססים על מאפייני ניתוח פסיכוגרפי הייתה מושא למחקרים שונים, שחלקם הראו אפקטיביות בינונית בלבד.[27] כך גם טענו מפעילי חברת "קיימברידג' אנליטיקה" לאחר שהתגלה השימוש שעשו בפלטפורמה של פייסבוק בבחירות 2016 בארצות הברית.[28] בחלק הבא נראה כיצד עמדות אלה משתנות לאור ההתפתחות בתחום מערכות מבוססות בינה מלאכותית מתקדמות יותר.

---

[25] Katherine Haenschen, T*he Conditional Effects of Microtargeted Facebook Advertisements on Voter Turnout*, 45(4) POLITICAL BEHAVIOR 1661–1681 (2023), https://doi.org/10.1007/s11109-022-09781-7; Kevin Joyal-Desmarais et al., *Appealing to Motivation to Change Attitudes, Intentions, and Behavior: a Systematic Review and Meta-Analysis of 702 Experimental Tests of the Effects of Motivational Message Matching on Persuasion*, 148(7-8) PSYCHOLOGICAL BULLETIN 465–517 (2022), https://doi.org/10.1037/bul0000377

[26] Rachel Kraus, *How Well Does "Microtargeted Psychographic Advertising" Work Anyway?* MASHABLE (Mar. 24, 2018), https://mashable.com/2018/03/24/how-microtargeted-ads-affect-behavior

[27] Haenschen, לעיל ה"ש 25 ; Joyal-Desmarais, לעיל ה"ש 25 ; Alexander Coppock, Seth Hill & Lynn Vavreck, *The Small Effects of Political Advertising are Small Regardless of Context, Message, Sender, or Receiver: Evidence from 59 Real-time Randomized Experiments*, 6(36) SCIENCE ADVANCES (2020), DOI: 10.1126/sciadv.abc4046.

[28] Emma Woollacott, *Cambridge Analytica Did Not Influence Brexit Referendum*, FORBES (8.10.2020), https://www.forbes.com/sites/emmawoollacott/2020/10/08/cambridge-analytica-did-not-influence-brexit-referendum/#1adee04234fe

עוד נעיר כי חלק מן המגע עם בוחרים פוטנציאליים אינו דיגיטלי. המונח "Canvassing" מתאר את מערך הפעילות המפלגתי הישיר מול בוחרים, בדרך כלל מדלת לדלת, בטלפון או בפגישות קהילתיות, שבו פעילים ומתנדבים משוחחים עם בוחרים, שואלים שאלות (למשל: האם תצביע? מדוע אתה מתלבט?) ומעבירים מסרים פוליטיים מותאמים.[29] המיוחד ב־Canvassing בעולם של פוליטיקה חישובית הוא שמתנדבים או עובדי מפלגה נשענים על אפליקציות ייעודיות שמציגות להם שכבות מידע על הבוחר, מאפשרות להזין נתונים, ומסנכרנות אותם למאגרי המידע המרכזיים של המפלגה. כלומר, מדובר במפגש פיסי־אנושי אשר מוזן, מנותב ומעובד דרך תשתיות נתונים דיגיטליות.[30]

3. מתעמולה מבוססת נתונים לתעמולה מבוססת בינה מלאכותית

העשור האחרון התאפיין בהתבססותם של קמפיינים פוליטיים על איסוף וניתוח שיטתי של מידע אישי על בוחרים. כפי שתואר לעיל, מודל התעמולה החישובית (ה־Data Driven Campaigning) נשען על איסוף כמויות גדולות של מידע על אזרחים, ניתוחו באמצעים סטטיסטיים ואלגוריתמיים, ושימוש בתובנות המתקבלות לצורך התאמת מסרים פוליטיים והפצתם לקהלי יעד שונים. אולם, טכנולוגיות למימוש מהלכי תעמולה חישובית התפתחו באופן דרמטי בארבע השנים האחרונות, ולכן יוצרות שוני איכותי בינן לבין מה שהיה מקובל במסעות תעמולה פוליטיים בעבר, ובכלל זה במערכת הבחירות האחרונה בישראל.

אם התעמולה החישובית בעשור וחצי האחרונים התמקדה בעיקר באיסוף מידע על בוחרים ובהתאמת מסרים פוליטיים לקבוצות יעד שונות, הרי שטכנולוגיות בינה מלאכותית מאפשרות אוטומציה של תהליך ההשפעה הפוליטית כולו. מערכות בינה מלאכותית מסוגלות לייצר מסרים פוליטיים מותאמים אישית, לנתח תגובות רגשיות של בוחרים, לבצע ניסויים בזמן אמת ולשפר את האפקטיביות של הקמפיין באופן מתמשך. במקביל, הן מאפשרות הסקת מידע חדש על בוחרים מתוך עקבות דיגיטליים זמינים, גם כאשר מידע זה לא נמסר במפורש.

בחלק זה נסקור את אבני הבניין הטכנולוגיות האלה ואת השלכותיהן. נדגיש, כי עניינו בעיקר בהיבטים הנוגעים לשימושי דאטה, פרטיות ויצירת "מלכודות על האוטונומיה" של בוחרים.

א. שינוי אופי הפגיעה בפרטיות בעידן הבינה המלאכותית

בליבת הדיון בפרטיות בעידן הדיגיטלי קיימות הפעולות של איסוף מידע אישי, שמירתו, עיבודו, חשיפתו או דליפתו.[31] אבל, אתגרי הפרטיות הכרוכים במפגש עם מערכות מבוססות בינה מלאכותית מתקיימים בכמה מישורים נוספים. חלקם מוכרים יחסית מן הספרות, כגון האפשרות שמודלים "יספגו" מידע אישי

---

[29] Jacob Ohrvik-Stott, *Moral Hazard: Voter Data Privacy and Politics in Election Canvassing Apps* (Open Rights Group, 2025)

[30] לסקירה עדכנית יחסית של החברות העוסקות בתחום על כל גווניו, ראו בדוח הזה: *Political Tech Landscape Report, Spring 2025*, Higher Grounds Labs, https://highergroundlabs.com/political-tech-landscape-report-2024/

[31] Grace Billiris, Assif Gill & Madhushi Bandara, *Privacy in the Age of AI: A Taxonomy of Data Privacy Risks in AI Systems, Australasian Conference on Information Systems*, UniSC & AAIS (2025), https://doi.org/10.48550/arXiv.2510.02357

מתוך מאגרי נתונים ויחזרו עליו בשלב מאוחר יותר תוך פרסום לא מורשה של מידע אישי ; או האפשרות שמשתמשים יזינו למערכות מידע רגיש מבלי להבין כי הוא נשמר, מעובד או משמש לשיפור המודל.[32]

ואולם, מאמרים עדכניים מצביעים על כך שמוקד הסיכון המרכזי הוא יכולתן של מערכות להסיק מידע חדש על אדם מתוך נתונים קיימים. במובן זה, הבינה המלאכותית משנה את אופי הפגיעה בפרטיות מדיון לגבי גישה לנתון אישי קיים, אל עבר היכולת לייצר מידע פרטי חדש על אדם באמצעות ניתוח, חיבור והיסק.[33]

מערכות בינה מלאכותית מסוגלות ללמוד מדפוסים לשוניים, חזותיים והתנהגותיים, ולהסיק מהם מסקנות על מאפיינים אישיים גם כאשר הללו לא נמסרו להן במפורש. ניסוח של משפט, סוג השאלות שאדם שואל, בחירות לשוניות מסוימות או תמונה הנראית תמימה לכאורה, עשויים לשמש בסיס להסקת מסקנות על הכנסה, מצב בריאותי, מוצא אתני, מיקום גאוגרפי או תכונות אישיות. במצבים אלה אדם אינו מוסר בהכרח מידע רגיש, אך המערכת מסוגלת להרכיב מהנתונים שיש בידה פרופיל אישי ומידע רגיש באמצעות הסקה אלגוריתמית. כך, השאלה אינה רק מי נחשף למידע, אלא גם מי מסוגל "לקרוא" את האדם מתוך העקבות הדיגיטליים שהוא מותיר אחריו. המערכת לא רק אוספת מידע על אנשים ; היא מייצרת מידע על אנשים. זהו שינוי עמוק באופייה של הפגיעה בפרטיות : מעבר ממידע גלוי למידע מוסק.[34]

היבט מטריד במיוחד הוא שקשה מאוד לזהות, לתעד ולפקח על היסקים ישירים ועקיפים כאלה. בעוד שניתן לעקוב אחר איסוף נתונים או אחר שמירתם במאגרי מידע, תהליך ההיסק מתרחש בתוך המערכת עצמה ואינו מותיר בהכרח עקבות ברורים. מבחינה זו, דיני הפרטיות הקיימים, הבנויים במידה רבה סביב שליטה על מידע אישי קיים, מעניקים מענה חלקי בלבד למצבים שבהם המידע הרגיש לא נאסף אלא נוצר מתוך נתונים שגרתיים, חלקם מידע אישי וחלקם אף עשוי להיות מידע בלבד שכשלעצמו לא מביא לזיהויו של אדם. הם אינם מעניקים מענה גם לתרחישים שבהם המידע שעליו מבוסס תהליך ההיסק אינו שייך למושא ההיסק אלא לאדם שלישי שנתוניו הם שנמצאים במערכת.

מנגנון משלים אך שונה הוא איגום מאפיינים ישיר או Attribute Aggregation.[35] כאן אין מדובר בהסקת מידע מתוך נתון בודד, אלא באיסוף, חיבור וניתוח של פיסות מידע מפוזרות ממקורות ציבוריים שונים כדי להרכיב פרופיל אישי מלא. המידע על אדם אמנם כבר קיים ברשת, אך הוא מפוזר במקטעים, ורק באמצעות מערכות בינה מלאכותית ניתן לאתר, לאחד ולעבד אותו באופן אוטומטי. זהו מצב שבו המערכת מאתרת מאפיינים מדויקים על אדם באמצעות חיפוש וניתוח רחבים של מידע ציבורי, לרבות

---

[32] Y. Yao, J. Duan, K. Xu, Y. Cai, Z. Sun & Y. Zhang, *A Survey on Large Language Model (LLM) Security and Privacy: The Good, the Bad, and the Ugly*, 4(2) HIGH-CONFIDENCE COMPUTING 100211 (2024), doi: 10.1016/j.hcc.2024.100211

[33] Ethan Mendes, Yang Chen, James Hays, Sauvik Das, Wei Xu & Alan Ritter, *Granular Privacy Control for Geolocation with Vision Language Models*, In PROCEEDINGS OF THE 2024 CONFERENCE ON EMPIRICAL METHODS IN NATURAL LANGUAGE PROCESSING 17240–17292, Association for Computational Linguistics (2024), http://aclanthology.org/2024.emnlp-main.957/

[34] (2025), Niloofar Mireshghallah & Tianshi Li, *Position: Privacy is Not Just Memorization!* https://doi.org/10.48550/arXiv.2510.01645

[35] שם.

באמצעות מערכות "חיפוש" מבוססות סוכנים או ניתוח עמוק על ידי צ'אטבוטים שאומנו לכך.[36] מידע שנאסף ממקורות שונים עשוי לאפשר לענות על שאלות הנראות שוליות – למשל, מה שמו של חתול המחמד של אדם מסוים – אך שאלות כאלה עשויות לשמש בהמשך לשחזור סיסמאות, השתלטות על חשבונות או יצירת פרופיל אישי עמוק יותר היוצר זיהוי חד ערכי עם אדם מסוים. המשמעות היא שגם מידע פומבי, שכל אחד מפריטיו כשלעצמו נראה תמים, עשוי להפוך באמצעות מערכות AI לתמונה אישית שלמה, עשירה ורגישה. בכך מיטשטש הגבול בין מידע "ציבורי" לבין מידע שראוי להגנת פרטיות: הפגיעה אינה נעוצה בהכרח בסודיותו של כל נתון בודד, אלא ביכולת לחבר את העקבות הדיגיטליים (digital footprints) לכדי פרופיל אישי מדויק ומזוהה.[37]

התפתחות נוספת בעלת משמעות היא מה שניתן לכנות "דמוקרטיזציה של יכולות מעקב". אם בעבר איסוף, סינתזה וניתוח של כמויות גדולות של מידע פתוח ברשת היו דורשים משאבים טכנולוגיים גבוהים, מומחיות מקצועית וגישה לכלי מודיעין או דאטה מתקדמים, הרי שכיום מערכות בינה מלאכותית וסוכנים מורידים את חסמי הכניסה לכך באופן דרמטי. היכולת לאסוף מידע ממקורות גלויים, לנתח אותו ולהסיק ממנו מסקנות נעשית זמינה גם לשחקנים חסרי ידע טכני מוקדם. במובן זה בינה מלאכותית לא רק מעצימה יכולות מעקב קיימות; היא גם מפזרת אותן ומרחיבה את מספר השחקנים המסוגלים להפעילן.[38]

בהקשר של תעמולה חישובית, המשמעות היא שהפגיעה בפרטיות אינה עוד תוצר בלעדי של מאגרי מידע מפלגתיים גדולים או של פלטפורמות טכנולוגיות ענק. ככל שכלים מבוססי סוכנים הופכים נגישים יותר, כך גם יכולת המעקב, האיגום והפרופיילינג מתפשטת לשחקנים קטנים יותר: קמפיינים מקומיים, פעילים ומתנדבים; חברות בינוניות וקטנות וגם גורמים זרים. השינוי, אם כן, אינו רק טכנולוגי אלא גם מבני: הוא משנה את מאזן הכוחות בין מי שאוספים מידע על בוחרים לבין הבוחרים עצמם.

ב. יצירת תוכן פוליטי מבוסס מכונה

בינה מלאכותית יוצרת (Generative Artificial Intelligence) מאפשרת יצירת תוכן חדש – כגון טקסט, תמונות, קוד, מוזיקה או וידאו – באמצעות אלגוריתמים מתקדמים של למידה חישובית. טכנולוגיה זו

---

[36] OpenAI: *Introducing Deep Research* (Feb. 2025), https://openai.com/index/introducing-deep-research.

[37] Robin Staab, Mark Vero, Mislav Balunovic & Martin Vechev, *Beyond Memorization: Violating Privacy via Inference with Large Language Models* (2024), arXiv preprint arXiv:2310.07298, 2024

[38] Zheyuan Liu, Guangyao Dou, Mengzhao Jia, Zhaoxuan Tan, Qingkai Zeng, Yongle Yuan & Meng Jiang, *Protecting Privacy in Multimodal Large Language Models with mllmu-bench*, In PROCEEDINGS OF THE 2025 CONFERENCE OF THE NORTH AMERICAN CHAPTER OF THE ASSOCIATION FOR COMPUTATIONAL LINGUISTICS 4105–4135 (2025), https://doi.org/10.48550/arXiv.2410.22108. מנגד כדאי לציין שיש המזהירים מפני תפיסה שגויה שלפיה הזמינות של כלים אלה מייצרת שוויון, הואיל ובפועל רק שחקנים בעלי תשתיות הפצה, גישה לנתונים ויכולת להגיע לקהלים גדולים יכולים לממש את יתרון האלגוריתמי. ראו: Felix M. Simon & Sacha Altay, *Don't Panic (Yet): Assessing the Evidence and Discourse Around Generative AI and Elections*, Knight First Amendment Institute at Columbia University (2025), DOI: 10.13140/RG.2.2.23142.33602

נשענת על מודלים גנרטיביים הלומדים דפוסים ממאגרי נתונים עצומים, ולאחר מכן מייצרים תוכן חדש, מקורי ובעל מאפיינים דומים למידע שעליו התאמנו.[39]

בלב התחום עומדים מודלים גדולים של שפה (Large Language Models – LLMs), מודלים המבוססים על רשתות נוירונים המאומנים על כמויות אדירות של טקסטים כדי להבין ולהפיק שפה טבעית. המודלים פועלים בעיקר באמצעות ארכיטקטורת Transformer שמאפשרת להם לנתח הקשרים רחבים ולהגיב בצורה קוהרנטית ורלוונטית. דוגמאות מרכזיות כוללות את Claude של Anthropic, Gemini של Google, וכן את GPT של OpenAI.[40] מודלים אלה משמשים כבסיס למערכות צ'אט, מנועי חיפוש, עוזרים אישיים, כלים לכתיבה, תרגום וסיכום טקסטים, והולכים ותופסים מקום מרכזי בחיי היומיום ובמגוון מקצועות, תחומים ושימושים – החל מכתיבת תכנים שיווקיים, סיכומי ישיבות, עזרה משפטית, וכלה ביצירת תמונות, הפקת מוזיקה, סימולציות, עיצוב גרפי, עריכת וידאו ויצירת דמויות דיגיטליות.

ככל שהמחקר והמסחור בתחום מתקדמים, כך גוברת חדירתם של כלים גנרטיביים לתוך תהליכים עסקיים, ממשלתיים וחינוכיים. היתרונות הבולטים של בינה מלאכותית יוצרת כוללים אוטומציה של משימות שגרתיות, שיפור חוויית לקוח ועובד, הגדלת קצב היצירה והתפוקה, והנגשת כלים מתקדמים לאנשים ללא הכשרה טכנית.[41] תכונות אלה הופכות את הבינה המלאכותית היוצרת לטכנולוגיה בעלת פוטנציאל משמעותי גם בתחום הקמפיינים הפוליטיים.

בינה מלאכותית מולטי־מודלית (Multimodal Artificial Intelligence) מתייחסת למערכות בינה מלאכותית המסוגלות לעבד ולשלב מידע ממקורות שונים, טקסט, תמונה, שמע, וידאו ונתונים מבניים, לצורך יצירת הבנה רחבה, אינטואיטיבית ומקיפה של סיטואציה או שאלה,[42] וליצור תוכן המשלב בין ערוצי מדיה שונים. בעוד שמערכות AI מסורתיות התמקדו לרוב בסוג מידע אחד בלבד, הבינה המולטי־מודלית מאפשרת לאחד את כל ערוצי המידע, באופן הדומה יותר לזה שבו בני אדם תופסים את העולם: באמצעות שפה כתובה, ראייה ודיבור.

היישומים כוללים מערכות חיפוש מידע משולבות, תרגום קונטקסטואלי (כגון שלטים בתמונה), אבחון רפואי משולב טקסט וסריקות,[43] ניתוח רגשות בשיחות, וכן ממשקים אינטראקטיביים, דוגמת מערכות

---

[39] Adam Zewe, *Generative AI Explained*, MIT NEWS (Nov. 9, 2023), https://news.mit.edu/2023/explained-generative-ai-1109

[40] Stefan Feuerriegel, Jochen Hartmann, Christian Janiesch & Patrick Zschech, *Generative AI. Business & Information Systems Engineering* (2023), http://dx.doi.org/10.2139/ssrn.4443189

[41] *MIT Technology Review Insights, Humans at the Heart of Generative AI* (2023) https://www.technologyreview.com/2023/11/01/1080463/humans-at-the-heart-of-generative-ai/

[42] Tadas Baltrušaitis, Chaitanya Ahuja & Louis-Philippe Morency, *Multimodal Machine Learning: A Survey and Taxonomy*, 41(2) IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 423-443 (2019), doi: 10.1109/TPAMI.2018.2798607

[43] Adam Zewe, *Making AI Models More Trustworthy in High-Stakes Settings*, MIT NEWS (May 1, 2025), https://news.mit.edu/2025/making-ai-models-more-trustworthy-high-stakes-settings-0501

ניהול שיחה המזהות גם טון דיבור וגם הבעות פנים.[44] בעוד שבעידן התעמולה החישובית מבוססת הנתונים התמקדו קמפיינים פוליטיים בעיקר בהתאמת מסרים קיימים לקהלי יעד שוני (microtargeting), הרי שהטכנולוגיות הגנרטיביות מאפשרות שלב נוסף: **ייצור אוטומטי של מסרים פוליטיים מותאמים אישית**. במקום לבחור מבין מספר מצומצם של מסרים שנכתבו מראש, מערכות בינה מלאכותית מסוגלות לייצר אין סוף טקסטים, תמונות, סרטונים, קטעי קול ודמויות דיגיטליות, בעלי ארבעה מאפיינים חשובים:

(1) מתאימים להקשר המסוים שבו נחשף הבוחר למסרים ולבועת התקשורת שהוא נמצא בתוכה.

(2) מתאימים למאפיינים פסיכולוגיים ורגשיים ספציפיים של הבוחר אליו מיועד המסר ולסגנון השיח שלו,[45] ולא רק למאפייני קהלי יעד קבוצתיים.

(3) מיוצרים באופן מתמשך וטמפורלי, למשל בדמות שיחה שאינה מוכתבת מראש או תכנים המשתנים בזמן אמת ותוך כדי פעולה

(4) אמינים ברמה שבני אדם מתקשים לזהות שהיא יצירת מכונה, ונראים "אנושיים" לא פחות מתכנים שנוצרו על ידי בני אדם.[46]

התפתחות זו משנה באופן מהותי את מבנה הקמפיינים הפוליטיים. ראשית, היא מאפשרת מעבר מהתאמה של מסרים קיימים לייצור אוטומטי ומהיר של מסרים מותאמים אישית. שנית, היא מפחיתה באופן משמעותי את עלויות הפקת התעמולה הפוליטית. אם בעבר יצירת קמפיין דרשה צוותי קריאייטיב, הפקת וידאו וכתיבת תכנים בהיקף רחב, הרי שכיום ניתן לייצר גרסאות רבות של מסרים פוליטיים באמצעים אוטומטיים ובעלות נמוכה יחסית. שילוב זה בין אוטומציה לירידת עלויות מאפשר להפעיל קמפיינים פוליטיים בהיקפים גדולים בהרבה מבעבר, אך מותאמים אישית ובאופן מדוייק למספר רב של בוחרים ספציפיים.

נדגיש כי ענייננו במסמך זה אינו בהיבטים של עצם יצירת התכנים על ידי מכונות, כלומר ביכולת ההבחנה בין תוכן אותנטי לבין תוכן יציר מכונה או בשימוש בבינה גנרטיבית לצורך הפצת דיסאינפורמציה. אנו גם לא עוסקים בצעדי מדיניות והגנה בהקשר זה, ביניהם: סימון תכנים יצירי מכונה, מערכות זיהוי

---

[44] Jiahui Pan, Weijie Fang, Zhihang Zhang, Bingzhi Chen, Zheng Zhang, Shuihua Wang, Multimodal Emotion Recognition Based on Facial Expressions, Speech, and EEG, 27(5) IEEE OPEN JOURNAL OF ENGINEERING IN MEDICINE AND BIOLOGY 396–403 (2023). DOI: 10.1109/OJEMB.2023.3240280

[45] חלק מעניין זה נובע גם מכך שכיום פלטפורמות צ'אטבוטים מבוססי מודלים גדולים של שפה אינן מגבילות את יכולות המיקוד והטירגוט כפי שמחוייבות למשל לעשות פלטפורמות המדיה החברתיות. ראו Almog Simchon, Matthew Edwardsc & Stephan Lewandowsky, *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3 PNAS NEXUS 1–5 (2024), https://doi.org/10.1093/pnasnexus/pgae035

[46] Angus R. Williams, Liam Burke-Moore, Ryan Sze-Yin Chan, Florence E. Enock, Federico Nanni, Tvesha Sippy, Yi-Ling Chung, Evelina Gabasova, Kobi Hackenburg & Jonathan Bright, *Large Language Models Can Consistently Generate High-Quality Content for Election Disinformation Operations*, 20(3) PLOS ONE e0317421 (2025), https://doi.org/10.1371/journal.pone.0317421

Josh A Goldstein, Jason Chao, Shelby Grossman, Alex Stamos & Michael Tomz, *How Persuasive is AI-generated Propaganda?*, , 3(2) PNAS NEXUS 34 (2024), https://doi.org/10.1093/pnasnexus/pgae034

ראו גם Yoshua Bengio, *International AI Safety Report*, 2nd edition, 50-57 (February 2026), https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

מתמשכות של פעילות מתואמת לא אותנטית ברשתות חברתיות, חיזוק מנגנוני אימות זהות ומקור (provenance) של תוכן, פיתוח כלים לסימון תוכן חשוד עבור משתמשים וכיוצא בכך.[47] לצד זאת, יש לתת את הדעת לכך שהשימוש בכלי בינה מלאכותית כגון ChatGPT או Gimini עשוי להוביל לחשיפת מידע אישי, לרבות מידע בעל רגישות מיוחדת, על הבוחרים. זאת משום ששיתוף מידע אישי עם כלים אלו עלול להוביל לפגיעה בפרטיות.[48]

ג. מחשוב חישתי וניתוח רגשות בוחרים

מחשוב חִישָׁתִי (Affective Computing) הוא תחום מתפתח בבינה מלאכותית שמטרתו ליצור מערכות המסוגלות לזהות, לפרש, לדמות ולהשפיע על רגשות אנושיים. תחום זה, שהוצג לראשונה על ידי החוקרת רוזלינד פיקרד (Picard) בשנות ה־90 של המאה ה־20,[49] חותר לא רק לניתוח נתונים "קרים", אלא גם להבנה של מצבים רגשיים, חוויות סובייקטיביות ואותות ביולוגיים כדי לשפר את איכות האינטראקציה בין מכונה לאדם.[50]

בניגוד למערכות בינה מלאכותית מסורתיות, המתמקדות בניתוח אנליטי או סטטיסטי, מערכות מחשוב חישתי שואפות להוסיף רובד רגשי לממשק. הן משתמשות בחיישנים ביומטריים, מצלמות, מיקרופונים ורכיבי עיבוד אותות כדי לנתח מאפיינים כמו הבעות פנים, תנועות עיניים, נימת קול, קצב לב ולחץ דם. טכנולוגיות אלו נשענות על שילוב בין עיבוד שפה טבעית (NLP), ראייה ממוחשבת ואלגוריתמים של למידת מכונה.

יישומי מחשוב חישתי כוללים תחומים מגוונים, למשל זיהוי עייפות, תסכול או עניין בקרב תלמידים, והתאמת קצב הלמידה או סוג התוכן בהתאם; ניטור סימפטומים של דיכאון, חרדה או מצבים פסיכולוגיים אחרים, המבוסס על טון דיבור או שפת גוף ומתן סיוע "פסיכולוגי" "טיפולי" מותאם; שיפור חוויית משתמש ולקוח על ידי תגובה מותאמת רגשית בזמן אמת; עיבוד רגשות של קהל בזמן צפייה ביצירות מדיה שונות, התאמת מוסיקה למצב רוח ויצירת שירה או סיפורת בעלות גוון רגשי מותאם אישית.

מערכות אלו אינן מסתפקות בעיבוד קוגניטיבי אלא שואפות לדמות התנהגות רגשית, ובכך חוצות את הגבול שבין כלי ניתוח לאובייקט של קשר. כך, לדוגמה, בעוד שמערכות NLP סטנדרטיות יזהו תבניות תחביריות או מילים טעונות, מערכות מחשוב חישתי מזהות שהטון העדין או ההבעה הנלווית מרמזים על אירוניה, עצב או חרדה ומתאימות את תגובתן בהתאם. כך, נוצרות אפשרויות לשינוי התנהגות

---

[47] בהקשר זה ראו שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 39–53, וכן לאחרונה החלטת יו"ר ועדת הבחירות לכנסת ה־26 בעניין תב"כ 12/26 **מפלגת "בנט 2026" ואח' נ' הליכוד – תנועה לאומית ליברלית** (29.01.2026) ובעניין תב"כ 15/26 **מפלגת "בנט 2026" ואח' נ' הליכוד – תנועה לאומית ליברלית** (12.02.2026).

[48] Lyana Calyanis, *Road to the 2026 midterm elections: Four ways the political landscape is changing*, NATIONBUILDER (Dec. 11, 2025); Zelly Martin, Dean Jackson, Inga Kristina Trauthing & Samuel C. Woolley, *Political Machines: Understanding the Role of AI in the U.S. 2024 Elections and Beyond*, Center for Media Engagement The University of Texas at Austin (June 6, 2024)

[49] Rosalind W. Picard, AFFECTIVE COMPUTING 3 (MIT Press 1997)

[50] Sitara Afzal, Haseeb Ali Khan, Imran Ullah Khan, Md. Jalil Piran & Jong Weon Lee, *A Comprehensive Survey on Affective Computing: Challenges, Trends, Applications, and Future Directions*, 111 IEEE J. 1 (2024), https://doi.org/10.48550/arXiv.2305.07665

אנושית בהסתמך לא רק על ניתוח מידע אלא גם על הבנה וניהול של מחוות גוף פיזיות ותגובות רגשיות.[51] מערכות אלה מעוצבות במכוון ליצירת חיבור רגשי עם המשתמש, ולכן עלולות לעודד תלות או אשליה של אינטימיות.[52] אחת הדוגמאות הבולטות היא שימוש גובר בצ׳טבוטים רגשיים, שמלווים אנשים בשיחות יומיומיות, מייעצים להם, ואפילו מחליפים שותפים לשיחה או חברים. מערכות כמו Replika, מאפשרות למשתמשים לפתח מערכת יחסים עם ישות דיגיטלית שנבנתה על פי העדפותיהם הרגשיות.[53]

טכנולוגיות מחשוב חישתי ומודלים מולטי־מודליים מאפשרים למערכות בינה מלאכותית לזהות, לפרש ולהגיב לרמזים רגשיים כגון טון דיבור, הבעות פנים, תנועות גוף, פניות לשוניות ומאפייני אינטראקציה אחרים, ברמת רזולוציה הולכת וגדלה.[54] יכולות אלו מאפשרות להתאים מסרים לא רק לפרופיל הדמוגרפי או ההתנהגותי של הבוחר, אלא גם למצבו הרגשי בזמן נתון. היכולת לזהות מצבי פגיעות רגשית, כגון בדידות, מצוקה או חוסר ביטחון, עשויה לשמש הן לשיפור שירותים והן ליצירת מנגנוני השפעה שאינם שקופים למשתמש. כאשר מערכת מזהה מצב רגשי ומגיבה אליו בזמן אמת, נוצר קשר שאינו סימטרי: המשתמש עשוי לפרש את התגובה כתקשורת אותנטית, בעוד שבפועל מדובר במנגנון המבוסס על דפוסים אלגוריתמיים או על מטרות מערכתיות שאינן ידועות לו. מבחינה זו, מיפוי והכוונת רגש הופכים ל״שובר שוויון״ טכנולוגי: הם משנים את גבולות האינטראקציה בין אדם למערכת דיגיטלית, מרחיבים את מרחב הפגיעות הרגשית, ומאפשרים השפעה על עמדות והתנהגויות בדרכים שאינן מבוססות רק על מידע או טיעון אלא גם על ניהול מצבים רגשיים.

לתוך מערך זה נוסף גם הסיכון המתפתח הנוגע ליחסים בין אנשים ומכונות. דוח סיכוני הבינה המלאכותית של פרופ׳ בנג׳יו מציין תופעות כגון הטיית אוטומציה (Automation Bias) – מצב שבו אנשים מפתחים אמון יתר במערכת ומפסיקים להפעיל שיקול דעת עצמאי גם כאשר היא שוגה; וכן ויתור מרצון על משאבים פנימיים של הבנה, תכנון, שיקול דעת ואפילו אינטימיות רגשית, כלומר תלות קוגניטיבית ורגשית הולכת ומעמיקה של אנשים במכונות.[55]

לצד הפוטנציאל החיובי של הטכנולוגיות האלה – למשל בקידום התנהגויות פרו־חברתיות כגון התחסנות או השתתפות בבחירות – הן מעוררות גם חששות משמעותיים ברמה האישית והחברתית. בתחום הצרכנות, התאמה פסיכולוגית של מסרים עלולה לעודד רכישה של מוצרים שאנשים אינם זקוקים להם או אינם יכולים להרשות לעצמם. ברמה החברתית הרחבה יותר, שימוש במודלים לשכנוע מותאם אישית

[51] Roddy Cowie & Marc Schroder, *Privacy and Ethical Considerations in Affective Computing*, 36 AI & SOCIETY 271, 275 (2021)

[52] Rhiannon Williams, *The AI Relationship Revolution is Already Here*, 128(2) MIT TECHNOLOGY REVIEW 20-27 (2025), https://www.technologyreview.com/2025/02/13/1111366/ai-relationships-chatbots-parenting-self-care-dating-marriage-mental-health/

[53] Kate Darling, *It's No Wonder People Are Getting Emotionally Attached to Chatbots*, WIRED (Jan. 8, 2024), https://www.wired.com/story/its-no-wonder-people-are-getting-emotionally-attached-to-chatbots/

[54] Ayşe A. Bozdağ, *The AI-Mediated Intimacy Economy: A Paradigm Shift in Digital Interactions*, 40(4) AI & SOCIETY 2285–2306 (2024), https://doi.org/10.1007/s00146-024-02132-6

[55] Yoshua Bengio, *International AI Safety Report*, 2nd edition 50-57. (February 2026), https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

עשוי להחריף מחלוקות חברתיות ולתרום לבעיות של בריאות נפשית כגון בדידות או התמכרות.[56] לכן, נטען שמחקר עתידי נדרש לבחון כיצד ניתן להסדיר את השימוש במודלים גנרטיביים באופן שימנע ניצול לרעה שלהם, למשל בקידום רכישה כפייתית או בפרקטיקות שיווק מניפולטיביות.[57]

התפתחויות אלה משמעותית במיוחד לגבי האפקטיביות של תקשורת והשפעה פוליטית.[58] אם תעמולה חישובית בעידן הנתונים התמקדה בעיקר בזיהוי דפוסי התנהגות של בוחרים – מי יוצא או לא יוצא להצביע, הרי שטכנולוגיות אלה מאפשרות למערכות לנסות לזהות גם את מצבם הרגשי של הבוחרים. בכך מתרחשת תזוזה ממיקוד התנהגותי למיקוד רגשי. מערכות מסוג זה יכולות, למשל, להתאים מסר פוליטי כך שיעורר תחושת תקווה, פחד, הזדהות או כעס, בהתאם למאפייני הנמען ולתגובותיו. ההשפעה הפוליטית של יצירת תכנים מותאמים אישית ומבוססים על מחשוב חישתי, עשויה לשקף גם מציאות פרשנית שונה עבור מושאי מידע שונים, שאינם עולים בהכרח לכדי דיסאינפורמציה, אבל משפיעים על עמדות ורעיונות.[59] התאמה כזו עשויה לגרום לאנשים לפתח עמדות חיוביות יותר כלפי מועמדים או סוגיות מאשר היו מפתחים בלעדיה. כאשר יכולות אלה פועלות בתוך סביבות מידע מקוונות שכבר נוטות ליצור "מערות הדהוד" ולחזק הטיות אישוש, כלומר חשיפה בעיקר לתכנים התואמים את תפיסות העולם הקיימות של המשתמש, הן עלולות להעמיק עוד יותר את ההסתגרות של אנשים בעולמות מידע אישיים ומבודדים החסרים מציאות משותפת עם אחרים.[60]

גם אם בעבר הועלו ספקות לגבי האפקטיביות של מיקרו־טירגוט פוליטי המבוסס על התאמה לתכונות אישיות, מחקרים מן השנתיים האחרונות מלמדים שיישומו באמצעות טכנולוגיות מבוססות בינה מלאכותית חישתית הוא אפקטיבי באופן עקבי ובהקשרים ניסויים שונים.[61] כן נמצא שהדבר עשוי לשנות את האופן שבו בוחרים צורכים מידע פוליטי[62] ושקשרים רגשיים עם מכונה עלולים לאפשר השפעה פוליטית עמוקה, סמויה ומתמשכת.[63]

---

[56] Matz, S.C., Teeny, J.D., Vaid, S.S. et al. , *The Potential of Generative AI for Personalized Persuasion at Scale*, 14(4692) SCIENTIFIC REPORTS (2024), https://doi.org/10.1038/s41598-024-53755-0

[57] Timothy Aylsworth, *Autonomy and Manipulation: Refining the Argument Against Persuasive Advertising*, 175(4) JOURNAL OF BUSINESS ETHICS 689–699 (2022) http://www.jstor.org/stable/45407148

[58] Hause Lin et. al.,*Persuading Voters Using Human-Artificial Intelligence Dialogues*, 648 NATURE 394–401 (2025), https://doi.org/10.1038/s41586-025-09771-9

[59] Almog Simchon, Matthew Edwardsc & Stephan Lewandowsky, *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3 PNAS NEXUS 1-5 (2024), https://doi.org/10.1093/pnasnexus/pgae035

[60] Tory Higgins, SHARED REALITY: WHAT MAKES US STRONG AND TEARS US APART, Epilogue: It Begins With Shared Relevance (Oxford University Press, 2019)

[61] Almog Simchon, Matthew Edwardsc and Stephan Lewandowsky, The Persuasive Effects of Political *Microtargeting in the Age of Generative Artificial Intelligence*, 3 PNAS NEXUS 1-5 (2024), https://doi.org/10.1093/pnasnexus/pgae035

[62] Felix M. Simon & Sacha Altay, *Don't Panic (Yet): Assessing the Evidence and Discourse Around Generative AI and Elections*, Knight First Amendment Institute at Columbia University (2025), DOI: 10.13140/RG.2.2.23142.33602

[63] שם.

ד. סוכני בינה מלאכותית וקמפיינים אוטונומיים

סוכן בינה מלאכותית (AI Agent) הוא מערכת בינה מלאכותית בעלת התנהגות מכוונת מטרה, יכולת קבלת החלטות אוטונומית, הסתגלות לסביבה משתנה וביצוע פעולות המשנות את המציאות. מערכות אלו מסוגלות לבצע סדרת פעולות לשם השגת מטרות מוגדרות, בין אם באופן חד־פעמי ובין אם בתהליך רציף של תכנון, למידה, התאמה וביצוע. סוכן כזה קולט מידע מהסביבה באמצעות חיישנים או קלטים אחרים, מעבד נתונים בזמן אמת, מתכנן רצפי פעולות, מקבל החלטות באופן עצמאי ולומד מניסיון. לעיתים הוא גם משתף פעולה עם סוכנים אחרים או עם בני אדם כדי לבצע משימות מורכבות בצורה מיטבית.[64]

סוכני בינה מלאכותית שונים מהותית ממודלי שפה גנרטיביים פשוטים דוגמת ChatGPT הפועל כתוכנת צ׳אט סטטית. בעוד שצ׳אטבוטים רגילים מייצרים תגובה טקסטואלית לבקשה אנושית, סוכנים פועלים כישויות עצמאיות, הם מקבלים מטרה כללית, בונים לה תוכנית פעולה, מבצעים שלבים, ומפעילים כלים חיצוניים לשם השלמת המשימה. כך למשל, סוכן יכול לא רק להציע טיסות לחו״ל אלא גם להזמין את הכרטיסים, למלא פרטים בטפסים, ולעדכן את היומן של המשתמש, ללא התערבות אנושית שוטפת.[65]

השימוש בסוכני בינה מלאכותית הופך נפוץ יותר במגוון תחומים: חברות כמו OpenAI, Anthropic, Google DeepMind, וכן ענקיות כמו LinkedIn ו־Stripe מפתחות ומשלבות סוכנים כחלק ממערכות שירות, סיוע אישי, ניתוח מידע וייעול תהליכים. המטרה המרכזית היא לאפשר למערכות לפעול באופן עצמאי, להפחית את העומס האנושי ולייעל תהליכים עסקיים, תוך שמירה על רמה מינימלית של פיקוח והתערבות מצד המשתמש.

ייחודם של סוכני הבינה המלאכותית טמון ביכולתם לפעול בזמן אמת, לקבל החלטות בתנאים משתנים ולהתמודד עם סביבות בלתי צפויות. יכולת זו נשענת על שילוב בין מודלים גדולים של שפה, מנגנוני זיכרון, גישה לכלים חיצוניים ומנגנוני למידה מתקדמים כגון למידת חיזוק. יחד, רכיבים אלו מאפשרים לסוכנים לבצע אינטגרציה בין סוגי מידע שונים ולפעול באופן רציף להשגת מטרות מורכבות ורב־תחומיות.

בהקשר זה מתחדדת ההבחנה בין סוכן בינה מלאכותית (AI Agent) לבין המושג הרחב יותר של בינה מלאכותית אייג׳נטית – ״סוכנות בינתית״(Agentic AI).[66] בעוד שסוכן הוא כלי ממוקד משימה, שפועל לרוב בתוך מסגרת פעולה מוגדרת ומונחה על ידי קלט אנושי ראשוני, הרי שבינה מלאכותית אייג׳נטית שואפת למודל פעולה עצמאי לחלוטין של מערכת שאינה מגיבה בלבד אלא גם יוזמת, לומדת, מסתגלת, ובמובנים מסוימים שואפת להשגת מטרות. סוכנות בינתית מתאפיינת באוטונומיה גבוהה, בפתרון בעיות

---

[64] Will Douglas Heaven, *OpenAI Launches Operator, an Agent that Can Use a Computer for You*. MIT TECHNOLOGY REVIEW (2025, January 23), https://www.technologyreview.com/2025/01/23/1110484/openai-launches-operator-an-agent-that-can-use-a-computer-for-you/

[65] Rhiannon Williams, *OpenAI's New Agent Can Compile Detailed Reports on Practically Any Topic*, MIT TECHNOLOGY REVIEW (2025, February 3), https://www.technologyreview.com/2025/02/03/1110826/openais-new-agent-can-compile-detailed-reports-on-practically-any-topic/

[66] Sahin Ahmed, *AI Agents vs. Agentic AI: What's the Difference and Why It Matters*, MEDIUM (17.6.2025) https://medium.com/@sahin.samia/ai-agents-vs-agentic-ai-whats-the-difference-and-why-it-matters-8e61d8a43b06

יצירתי, בלמידה מתמשכת, וביכולת לקבוע ולשנות את מטרותיה בהתאם לשינויים בסביבה או ביעדים.[67]

כאשר סוכנים רבים פועלים יחד במסגרת מערכת מרובת סוכנים (Multi-Agent Systems) נוצרת אפשרות לתיאום מורכב בין ישויות דיגיטליות רבות. שילוב בין מודלים לשוניים גדולים לבין מערכות סוכנים אוטונומיים יוצר תופעה חדשה המכונה "נחילי בינה מלאכותית (AI swarms)".[68] מדובר במערכות של סוכנים דיגיטליים רבים הפועלים יחד באופן מתואם, בעלי זהות מתמשכת וזיכרון, המסוגלים לתקשר ביניהם, להתאים את התנהגותם בזמן אמת ולחדור לקהילות מקוונות תוך חיקוי התנהגות אנושית.

בהקשר הפוליטי, מערכות מסוג זה עשויות לשנות באופן מהותי את אופן הפעלתם של קמפיינים להשפעה על דעת הקהל. בעוד שבעבר מבצעי השפעה פוליטיים התבססו על צוותים אנושיים או על רשתות בוטים פשוטות, הרי ששילוב של סוכני בינה מלאכותית מאפשר הפעלה אוטונומית ומתמשכת של מערכות השפעה. סוכנים כאלה יכולים ליצור ולהפיץ מסרים, לנתח תגובות של משתמשים, לבצע ניסויים בזמן אמת ולשפר באופן מתמשך את האפקטיביות של הקמפיין.

מחקרים עדכניים מצביעים על מספר יכולות מרכזיות המאפיינות מערכות "נחיל" כאלה.[69] ראשית, הן מאפשרות תיאום דינמי בזמן אמת: אלפי פרסונות דיגיטליות יכולות לפעול במקביל ולתאם ביניהן מסרים ונרטיבים בהתאם לתגובות הציבור. שנית, הן מסוגלות למפות רשתות חברתיות ולחדור לקהילות שונות באמצעות למידה של השפה, הסגנון והקודים התרבותיים שלהן. שלישית, הן מסוגלות לחקות התנהגות אנושית בצורה משכנעת – באמצעות שימוש בשפה טבעית, באווטארים דיגיטליים ובדפוסי פעילות מגוונים – ובכך להימנע מגילוי על ידי מערכות זיהוי בוטים. רביעית, הן מבצעות אופטימיזציה מתמשכת של המסרים באמצעות ניתוח נתוני מעורבות של משתמשים וניסוייA/B – השוואה בין תוצאות בקנה מידה רחב. לבסוף, מערכות אלו יכולות לפעול לאורך זמן רב, להשתלב בהדרגה בקהילות מקוונות ולשנות את השיח הציבורי מבפנים.

עוד יש לציין את החשש מפני יציאה משליטה של מערכות סוכנים, בדרכן לבצע באופן אופטימלי את המשימה שניתנה להן.[70] נחילי סוכנים שתכליתם ליצור שינוי בדעת הקהל או בדעתם של בוחרים ספציפיים עלולים ליצור ריבוי קולות מזויפים לצורך יצירת אשליה של קונצנזוס ציבורי; סוגי מציאות שונים לאנשים שונים לצורך העמקת קיטוב חברתי; הצפת המרחב הציבורי בתוכן מזויף או עוין; או "הרעלת" תשתית המידע של רשת האינטרנט כדי להשפיע על נגישות למידע של צ'אטבוטים או על מאגרי המידע שעליהם מתאמנים מודלים של בינה מלאכותית, וכיוצא באלה. אבל, לא פחות מכך הם עלולים

---

[67] שם.

[68] Daniel Thilo Schroeder, Meeyoung Cha, Andrea Baronchelli, Nick Bostrom, Nicholas A. Christakis, David Garcia, Amit Goldenberg, Yara Kyrychenko, Kevin Leyton-Brown & Jonas R. Kunst, *How Malicious AI Swarms Can Threaten Democracy*, 391 (6783) SCIENCE 354-357 (2026), DOI: 10.1126/science.adz1697

[69] שם.

[70] Yoshua Bengio, *International AI Safety Report* ,2nd edition, 76-83 (February 2026), https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026,

ליצור קמפיינים של הטרדה ממוקדת נגד עיתונאים, פוליטיקאים או פעילים אזרחיים; ומתקפות סייבר מסוג hack and leak הכוללות הפצת מידע אישי.[71]

כך או כך, התפתחות זו מסמנת מעבר נוסף בתעמולה החישובית: המעבר מקמפיינים פוליטיים המתוכננים ומנוהלים בעיקר על ידי בני אדם – גם אם בנקודת הקצה של הפעלת הקמפיין נמצאת למשל רשת בוטים, אל קמפיינים שבהם חלקים גדולים מתהליך ההשפעה מבוצעים מקצה לקצה ובאופן אוטונומי על ידי מערכות בינה מלאכותית. במודל זה, סוכנים דיגיטליים יכולים לבצע חלקים משמעותיים משרשרת ההשפעה – החל ביצירת מסרים, דרך התאמתם לקהלים שונים, ועד ניתוח תגובות הציבור ושיפור מתמיד של האסטרטגיה. כך משתנים באופן מהותי ההיקף, המהירות ויכולת ההתאמה של מבצעי השפעה פוליטיים, והתעמולה החישובית מתקרבת למצב של אוטומציה של "מעגל השכנוע".

ה. סיכום: אוטומציה של השפעה פוליטית בקנה מידה רחב

ההתפתחויות שתוארו לעיל מצביעות על שינוי מצטבר במבנה של תעמולה חישובית לכיוון תהליך של סגירת "מעגל השכנוע". נתונים על משתמשים נאספים או מוסקים מתוך פעילותם הדיגיטלית; מערכות בינה מלאכותית מנתחות נתונים אלה ומייצרות פרופילים אישיים; על בסיס פרופילים אלו נוצר תוכן פוליטי מותאם אישית; והתגובות של המשתמשים למסרים הללו מוזנות חזרה למערכת לצורך שיפור מתמשך של האסטרטגיה. כך נוצר תהליך דינמי של אופטימיזציה בזמן אמת, שבו המסרים עצמם, דרכי הפצתם והקבוצות שאליהן הם מכוונים משתנים באופן מתמיד בהתאם לתגובות הציבור.

המאפיין הראשון של התפתחות זו הוא האוטומציה. אם המודל הקלאסי של קמפיינים מבוססי נתונים נשען על איסוף מידע על בוחרים ועל התאמת מסרים לקבוצות יעד שונות, תוך הפעלת שיקול דעת אנושי בכל אחד משלבי השרשרת, הרי טכנולוגיות של בינה מלאכותית מאפשרות אוטומציה של כל מרכיב בתהליך ושל התהליך כולו.

המאפיין השני הוא היקף הפעולה – ה"סקייל". מערכות בינה מלאכותית מאפשרות לייצר כמויות אין סופיות של תוכן מכל סוג, לבצע ניסויים רבים במקביל ולהפעיל מערכות השפעה באופן אוטונומי לאורך זמן וכל זאת ללא הצורך בהשקעת המשאבים שנדרשה בעבר לכוח אדם, מומחיות ותשתיות טכנולוגיות. הפחתת העלויות הדרמטית מאפשרת להפעיל קמפיינים פוליטיים בהיקפים גדולים בהרבה מבעבר, ולהפיץ מסרים מותאמים ליחידים.[72] החידוש בהיבט זה אינו בהבדל בין מסר מותאם למסר לא מותאם, שהוא אינו דרמטי ברמת הפרט ואינו מוביל לשינוי מיידי בעמדות פוליטיות, אלא ביכולת ההרחבה, כלומר בהבחנה בין אפקטיביות נקודתית לבין אפקט מצטבר בקנה מידה גדול. גם אם אפקט השפעה נקודתי אינו גדול, כאשר הוא מיושם על מאות אלפי או מיליוני בוחרים, מופעל באופן אוטומטי ומשולב במערכות הפצה קיימות, עלול להפוך למשמעותי מבחינה אלקטורלית. שינוי של אלפים בודדים מתוך מאה אלף בוחרים שנחשפים לקמפיין עשוי להיות מכריע בבחירות צמודות – תרחיש ריאלי במדינות

---

[71] Schroeder, ה"ש 68 לעיל.

[72] Almog Simchon, Matthew Edwardsc and Stephan Lewandowsky, *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3 PNAS NEXUS 1-5 (2024), https://doi.org/10.1093/pnasnexus/pgae035; Matz, S. C., Teeny, J. D., Vaid, S. S. et al., *The Potential of Generative AI for Personalized Persuasion at Scale*, 14(4692) SCIENTIFIC REPORTS (2024), https://doi.org/10.1038/s41598-024-53755-0

דמוקרטיות רבות. כלומר הסיכון הדמוקרטי אינו נובע מעצם ביצוע ההמניפולציה אלא מהאוטומציה, הזמינות, המהירות, ההיקף של המסרים והתחכום של התאמתם לאדם מסוים.[73]

התוצאה היא שינוי עמוק בתעמולה החישובית, המשנה את היחסים בין מידע, כוח פוליטי ופרטיות, ומרחיב את יכולתם של שחקנים שונים – מפלגות, קבוצות לחץ ואף גורמים חיצוניים – להפעיל מנגנוני השפעה מתקדמים על בוחרים. במובן זה, התעמולה החישובית בעידן הבינה המלאכותית אינה רק שיפור של הכלים הקיימים, אלא שלב חדש בהתפתחותם של קמפיינים פוליטיים דיגיטליים.

4. יישומוני בחירות

יישומוני ניהול בחירות הם יישומונים שמפותחים בהזמנת המפלגות ומטרתם לייצר מעורבות של בוחרים ולסייע למפלגות ולמתמודדים לנהל את מערכת הבחירות. ליישומוני ניהול בחירות שימוש כפול: האחד – איסוף מידע על בוחרים; והאחר – הפעלה של המתנדבים והמטה. יישומונים אלה כוללים כמות עצומה של מידע פרטי,[74] וייחודם בכך שיש בהם קשר מזהה בין אדם ובין עמדותיו הפוליטיות. מאגר המידע עליו מבוסס היישומון בנוי בצורת שכבות.

שכבת הבסיס היא מידע מפנקס הבוחרים (המכונה "מידע פנקס") שנמסר ממשרד הפנים למפלגה המתמודדת בבחירות מכוח חוק הבחירות לכנסת.[75] מדובר בפרטי המידע האלה: שם פרטי ושם משפחה, שם האב או האם, כתובת, מספר הזהות של כל בעלי זכות הבחירה במדינה, כלומר כל האזרחים מעל גיל 18, הקלפי שאליה משויך כל אזרח ומספרו בקלפי. אזרח אינו יכול לסרב להיכלל במרשם האוכלוסין ובפנקס הבוחרים ואינו יכול לסרב שפרטיו יועברו אל המפלגות.

בשכבה השנייה נאגמים ומעובדים פרטי מידע נוספים כגון תאריך לידה, מספר טלפון וכתובת דוא"ל, קישורים לעמודי פייסבוק ורשתות חברתיות אחרות, קשרי משפחה ושפת הדיבור. עוד נמצאים בשכבה זו פרטי מידע מעובד שנרכשים מסוחרי מידע (data brokers), שעיסוקם העיקרי הוא עיבוד מידע אישי לשם מכירתו או העמדתו לשימוש צדדים שלישיים.

בשכבה השלישית נמצא מידע בדבר הזיהוי הפוליטי של בוחרים: מידת התמיכה במפלגה והאם בכוונתו של הבוחר נושא המידע להצביע ביום הבחירות. למעשה זו שכבת המידע החשובה ביותר לשימוש אפקטיבי ביישומון, משום שהיא בתורה תשמש כדי להכין את תוכנית הפעולה המותאמת אישית בנוגע לכל בוחר ובוחרת. האם המפלגה תפנה אליו ביום הבחירות? באיזה שלב של היום? מי יפנה ובאילו טכניקות?

את פרטי המידע בשתי השכבות הנוספות, מעבר לשכבת הבסיס, מזינים משתמשים שהורידו את היישומון מחנות היישומים או באמצעות אתר אינטרנט לגיוס תומכים.[76] פעילי המפלגה שהתקינו את היישומון מזינים את פרטיהם וכן ממלאים פרטים על אנשים אחרים. בין היתר התבקש מי שהתקין את

---

[73] Matz, et al., שם.

[74] תהילה שוורץ אלטשולר ורחל אריאדור הרשקוביץ "חוות דעת בנושא יישומוני הבחירות" **אתר המכון הישראלי לדמוקרטיה** (פברואר 2020) https://www.idi.org.il/media/13963/havad.pdf. בקביעה שמדובר במאגר מידע תומכת גם קביעתה של הרשות להגנת הפרטיות, ראו סעיף 4 להנחיות הרשות להגנת הפרטיות "אחריות המפלגות לקיום הוראות חוק הגנת הפרטיות בשימוש באפליקציות ובספקים חיצוניים לצורך ניהול מערכת בחירות" (11.2.2020).

[75] סעיף 39(א) לחוק הבחירות לכנסת [נוסח משולב], תשכ"ט-1969.

[76] ראו למשל אתר מפלגת הליכוד בכתובת www.likud-2020.co.il

היישומון להזין לתוכו מידע על חבריו ועל קרוביו ברמות שונות של פירוט. דליפת המידע מיישומון אלקטור בעת ששימש את קמפיין הליכוד בבחירות מרץ 2020, חשפה בין השאר כי במידע נכללו גם תיאורים פרטניים על אנשים וכן על הדרך שבה יש לשכנע אותם כגון "אביו פעיל ליכוד מוכר" או "לחיץ כמו בקבוק קטשופ".[77]

משימושים בעבר ביישומונים עולה שהמערכת מחלקת את האנשים שבמאגר המידע לארבע קבוצות בהתאם למידת תמיכתם במועמד או ברשימה שהיישומון פועל לבחירתו: תומכים, תומכים פוטנציאלים, לא ידוע או לא תומך.[78] מיון האזרחים שפרטיהם נמצאים במאגר המידע בהתאם למידת תמיכתם משפיע על ההתמקדות במסרים ובטיפול מצד עובדי הקמפיין.[79] נתוני זמן האמת ביום הבחירות מוצגים גם כן בחלוקה לארבע קבוצות אלה.[80]

שכבת המידע הרביעית נוגעת לסטטוס ההצבעה, כלומר לשאלה מי הצביע ומי טרם הצביע ביום הבחירות עצמו. משקיפים וחברי ועדות קלפי מטעם המפלגה, הנמצאים בקלפי כחוק, מעדכנים באופן שוטף באמצעות היישומון אם בעל זכות בחירה פלוני הצביע בקלפי. סטטוס ההצבעה מספק אפוא מידע חשוב ביותר למפלגה – מי מבעלי זכות ההצבעה לפי פנקס הבוחרים בחר לממש את זכותו הדמוקרטית ולהצביע בבחירות.[81]

מאגר המידע שביישומון מתעדכן כל העת. כך, ניתן באמצעות היישומון לשפר את פרופיל האישיות של בעל זכות הבחירה שהמידע הוא אודותיו ולמטב את המסרים המותאמים אישית אליו ואת פלטפורמת העברתם לשם השגת המטרה המבוקשת על ידי המפלגה. בנוסף, היישומון מאפשר לשלוח לבוחרים מסרים שיניעו אותם לפעולה כמתנדבים בקמפיין הבחירות, וכך לאפשר תעמולת בחירות בעלות נמוכה ובהיקפים גדולים יותר ממה שהיה מקובל קודם לכן.[82]

יישומוני הבחירות מאפשרים למפלגות ליצור מאגרי מידע עצומים הכוללים פרטי מידע רגישים ביותר שיוצרים זיהוי חד ערכי בין עמדתו הפוליטית של אדם לבין זהותו ומאפשרים ליצור פרופיל אישיות מדויק של האדם שהמידע אודותיו. בכך טמונה סכנה עצומה לא רק למניפולציות על הבוחרים ויצירת מלכודות אוטונומיה ביום הבחירות עצמו.[83] קיומם של מאגרי מידע רגישים כל כך טומנת סיכון לשימוש

---

[77] עומר כביר "מכונת קישוש הקולות של הליכוד בפעולה: 'חשוב ללחוץ עליו ולפנות אליו מניפולטיבית'" **כלכליסט** 17.2.2020, https://www.calcalist.co.il/internet/articles/0,7340,L-3793971,00.html

[78] ראו בסרטון "מערכת לניהול בחירות – אלקטור", https://www.youtube.com/watch?v=scQo5KWRBxc.

[79] שם.

[80] שם.

[81] שחר סמוחה "המצביע האוטומטי: 'הציבור לא מבין את עומק המניפולציה שעושים עליו'" **שומרים** (29.9.2022).

[82] שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 54.

[83] ענת בן דוד "מיום הבוחר ליום העוקב" **העין השביעית** (18.2.2020); שחר סמוחה "המצביע האוטומטי: 'הציבור לא מבין את עומק המניפולציה שעושים עליו'", **שומרים** (29.9.2022).

עתידי, מורשה ושאינו מורשה,[84] במידע האגור בהם כתנאי מוקדם לקבלה לעבודה, לקבלת שירות מהמדינה, לאינטראקציה חברתית ועוד.[85]

אחד מהיישומונים בהם נעשה שימוש במסגרת קמפיינים פוליטיים במדינות שונות, כמו, למשל, צרפת ובריטניה ואף פרלמנט האיחוד האירופי הוא היישומון של חברת NationBuilder האמריקאית. הפלטפורמה של NationBuilder מציעה חבילת כלים משתנה, בהתאם לבחירת הלקוח (מפלגה, מועמד או ארגון אחר) למעקב אחר התנהגות בוחרים, לניהול קמפיינים ולהנעת ציבור לפעולה באמצעות פעילות הסברה וגיוס. שלל כלים אלו נשענים על מסד נתונים מרכזי, שהינו ייחודי לכל לקוח של המערכת, המאחד מידע ממקורות שונים כגון רשומות פנימיות של מפלגות, מאגרי מידע ציבוריים, מאגרי מידע של צדדים שלישיים המספקים למשל נתונים דמוגרפיים, ניתוחים ניבויים ומידע הנלמד מאינטראקציות שיווקיות ודיגיטליות של משתמשים.[86] על בסיס מידע זה יוצרת הפלטפורמה פרופילי בוחרים. כן מפעילה הפלטפורמה מערכת אנליטיקה המודדת את רמת המעורבות של כל בוחר על בסיס מגוון פעילויות, למשל פעילות ברשתות חברתיות או השתתפות בקמפיין ומאפשרת לסווג ולדרג בוחרים לפי יותר משמונים משתנים שונים של פעילות. כל מאפשרת פלטפורמת NationBuilder למפלגות לבצע קמפיינים מדוייקים ומבוססי נתונים.[87]

חבילת הכלים המסופקת ללקוח על ידי פלטפורמת NationaBuilder משתנה בהתאם לבחירתו ולמחיר אותו הוא מוכן לשלם.[88] כך, הלקוח יכול לבחור האם ברצונו להצליב בין חשבונות ברשתות חברתיות לבין כתובות הדוא"ל של אנשים שזוהו כתומכים במסד הנתונים, להוסיף נתונים ממקורות שונים וכן לעשות שימוש במודלים ניבויים וניתוחים מותאמים אישית. כן יכול הלקוח לבחור לשלב במסגרת הכלים המוצעים לו גם חיבור לתהליכי פרסום המסופקים על ידי Amazon Advertising ו־Google Ads ; לקבל הצעות לשיתוף פעולה עם שותפים כגון חברות ייעוץ ; או לקבל גישה ללוחות מחוונים וגישה לשירותי אנליטיקה של צדדים שלישיים.[89] הפלטפורמה עושה שימוש בכלי בינה מלאכותית לשם התאמת מסרי תעמולה מותאמים לבוחרים בהתאם לתחומי העניין שלהם ולהיסטורית הקשר שלהם עם המפלגה, וכן מספקת למפלגה מידע בזמן אמת, שניתן לפילוח ומיון על מנת לקבל החלטות על בסיס מידע מלא בנוגע לאסטרטגיית התעמולה הנכונה.[90]

---

[84] מאגרים אלו כבר נפרצו במערכות בחירות קודמות. ראו חגי עמית "לגנץ פרצו לטלפון? בליכוד חשפו מיליון ישראלים ברשת לפי זהותם הפוליטית" **דה מרקר** (9.9.2019) ; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27/01/2021) ; **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021) ; **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – אלקטור** (27.1.2021).

[85] להרחבה, ראו, למשל, שוורץ אלטשולר ולוריא, לעיל ה"ש 1, עמ' 54 ; ענת בן דוד "מיום הבוחר ליום העוקב" **העין השביעית** (18.2.2020).

[86] Fenwick McKelvey & Jill Piebiak, *Porting the Political Campaign: The NationBuilder Platform and the Global Flows of Political Technology*, 20(3) NEW MEDIA & SOCIETY 901-918

[87] ראו באתר החברה : https://support.nationbuilder.com/en/articles/2362765-understanding-social-capital

[88] ראו גם באתר החברה : https://marketing.nationbuilder.com/for-political-campaigns

[89] ראו גם באתר החברה : https://nationbuilder.com/apps_and_integrations

[90] NationBuilder, *World-class software for political parties, optimized for Europe*, https://nationbuilder.com/political_party_software

דוח של ארגון זכויות האדם הדיגיטליות הבריטי Open Rights Group מינואר 2025 שסקר את היישומונים שבהם השתמשו שלוש המפלגות הגדולות בבחירות האחרונות בבריטניה, מצא שני סוגים עיקריים של יישומונים.[91] הסוג אחד הוא יישומונים ייעודיים לפעילי שטח המאפשרים גישה למידע על בוחרים, הזנת נתונים בזמן אמת לאחר שיחות פנים אל פנים עם בוחרים, וסינכרון עם מאגרי מידע מרכזיים של המפלגה. ביישומונים אלה נעשו גם שימושים בשירותי אנליטיקה ותשתיות של חברות חיצוניות, ובהן Microsoft Visual Studio App וכן רכיבי תוכנה של Google (Firebase, Crashlytics). הסוג השני הוא יישומונים לניהול מדיה חברתיות ובכללם ניתוח סנטימנט וזיהוי ישויות ופרופיילינג. ביישומונים אלה נעשו שימושים גם בשירותי מעקב אחר מיקום וזיהוי משתמשים באמצעות נתוני WIFI. באחד מן היישומונים נרשמה מעורבות עמוקה של חברת Experian, אחת משלוש חברות דירוג האשראי והדאטה הגדולות בעולם, מה שמלמד על שימוש בשכבות מידע ממקורות מסחריים. הדוח טוען כי מדיניות הפרטיות של היישומונים אינה מספקת פירוט לגבי היקף השיתוף והכיוון שלו – כלומר האם נתוני canvassing הכוללים מידע לגבי דעה פוליטית, נגישים ל־Experian לצרכים שמעבר לפעילות המפלגתית עצמה.

פרק שני
פרטיות ובחירות בישראל: המצב המעשי והמשפטי

דיני תעמולת הבחירות הקיימים בישראל אינם נותנים מענה לשאלה אם יש סוגים של מידע אישי שאסור להשתמש בו במסעות תעמולה, או אם יש טכניקות שרמת ההשפעה והמניפולציה שהן יכולות ליצור גדולה כל כך עד שיש לאסור אותן. בהקשר זה קיים אפוא חלל חוקי ואכיפתי בנושא של פרטיות ובחירות.

הזכות החוקתית לפרטיות, המעוגנת בסעיף 7 לחוק־יסוד: כבוד האדם וחירותו, היא לפי הניסוח בחוק היסוד והפסיקה סביבה, זכות בעלת ממד אינדיבידואלי ועוסקת בעיקר במניעת כניסה למרחב הפרטי ובשליטתו של הפרט על המידע האישי שלו. לכן המצב המשפטי במדינת ישראל, כמו שבא לידי ביטוי בפסיקה בעניין יישומוני הבחירות,[92] איננו כולל התייחסות חוקתית לכך שהשימוש בטכניקות איסוף של מידע אישי ועיבודו כדי לבצע מניפולציה על בוחרים, מציב איום משמעותי על האינטרס הציבורי הקולקטיבי בקיום הליך דמוקרטי תקין, הוגן וטהור.

איסוף מידע אישי אודות בוחרים פוטנציאלים לשם העברת מסרי תעמולת בחירות בפלטפורמות דיגיטליות צבר תאוצה החל **מהבחירות לכנסת ה־21** באפריל 2019. אז עשתה מפלגת הליכוד שימוש בתוכנת המסרים המיידים של פייסבוק באמצעות בוט שהופעל בדף הפייסבוק של ראש הממשלה בנימין נתניהו, וניהל שיחות לכאורה אישיות עם מצביעים פוטנציאלים תוך כדי איסוף ועיבוד מידע אישי עליהם מהמידע הזמין בפייסבוק והמידע שנמסר על ידם תוך כדי השיחה. הבוט מיפה את המצביעים עמם שוחח בהתאם למידת תמיכתם במפלגת הליכוד, המריץ תומכים לסייע בהפצת תעמולה וגיוס תומכים והמשיך בניסיונות שכנוע של מי שהוגדרו כמתלבטים. פייסבוק מצאה שהשימוש בבוט מפר את כללי השימוש בפלטפורמה, וביניהם איסור על שידול, ודרשה לחדול מהשימוש בו.[93] לטענת מי שעמד בראש קמפיין הדיגיטל של הליכוד באותה העת, הצ׳אט־בוט תרם משמעותית להצלחת קמפיין הבחירות של הליכוד. המידע שנאגר באמצעות הבוט שהופעל במערכת הבחירות לכנסת ה־21 נשמר על ידי הליכוד, לטענתה לפי הכללים המחייבים של פייסבוק.[94]

באותה מערכת בחירות הסתבר גם כי קיים גם חלל חוקתי בשאלה אם עצם היציאה להצביע היא מידע אישי שחוסה תחת הזכות לפרטיות. אף שאין מחלוקת שעמדתו הפוליטית של אדם ותוכן ההצבעה מאחורי הפרגוד בחדר הקלפי הם מידע אישי רגיש, בכל הנוגע לשאלה אם המידע על עצם היציאה להצביע הוא מידע פרטי –אין קביעה ברורה. בעתירה בעניין עדאלה נטען כי סימון דיגיטלי של המצביעים, והבנה בזמן אמת מי לא יצא להצביע, עלולים להביא לידי חשש מפני פגיעה במעמדו המקצועי, החברתי או האישי עקב חשיפה ציבורית כי נמנע מלממש את חובתו האזרחית להצביע. בנוסף, מהימנעותו של פלוני להצביע בבחירות אפשר להסיק גם על עמדותיו הפוליטיות. כך למשל אי־הצבעה יכולה ללמד על חוסר אמון במוסדות השלטון. ניתן גם להפעיל עליו לחץ מבוסס מיקום, כך למשל כשידוע שאדם הוא סטודנט ונמצא על יד מוסד הלימודים והרחק ממקום הקלפי, אפשר לעודד אותו לצאת להצביע בקלפי נגישה ולזייף את העובדה שאיננו בעל מוגבלות (שכן הכללים הקיימים אינם דורשים להציג תעודה כלשהי על

---

[92] תב״כ 14/23 **בן מאיר ואח׳ נ׳ הליכוד – תנועה לאומית ליברלית ואח׳** (18.2.2020).

[93] ינון בן שושן ״פייסבוק אסרה על נתניה להפיץ מספרי טלפון״ NEXTER (8.4.2019); עמרי ברק ״פייסבוק נגד נתניהו: יאוסף מידע״ N12 (18.8.2019).

[94] אמיר בן דוד ״שלום, קוראים לי ביבי ואני בוט״ **זמן ישראל** (16.5.2019).

מוגבלות בקלפי). בכיוון ההפוך ייתכן מצב שבו הודעות שקריות מגיעות במכוון אל בוחרים ספציפיים, כמו למשל הודעה שמיועדת למי שאינו תומך המפלגה שבקלפי המסוימת שאליה הוא משתייך התורים ארוכים וכיוצא באלה.

בעניין עדאלה סבר השופט מלצר כי:

> "זוהי שאלה נכבדה שטרם הוכרעה בפסיקה, וטעונה עוד ליבון ואינני רוצה לקבוע בה מסמרות, במיוחד בשים לב לכך שרשימת הבוחרים שהצביעו איננה, לכאורה, חסויה בפני סיעות הכנסת ששלחו נציגים לוועדת הקלפי."[95]

בבחירות **לכנסת ה־22**, שהתקיימו בחודש ספטמבר 2019, המשיך הליכוד לעשות שימוש בבוט שהופעל מדף הפייסבוק של ראש הממשלה בנימין נתניהו ודימה שיחה במסנג'ר. משתמשים שזוהו כתומכי ליכוד התבקשו באמצעות הבוט, לבצע שיחות טלפון לאנשים, להעביר להם את המסרים ולעדכן את הבוט לאחר מכן במידת התמיכה של נמען השיחה במפלגה. הטלפנים לא תודרכו שעליהם להסביר לנמעני השיחה שהמידע שהם מוסרים נאסף ונשמר במאגר מידע של הליכוד.[96] עוד נחשף בתקשורת כי מאגר מידע עצום שמטרתו לקטלג את בעלי זכות הבחירה בישראל לפי האוריינטציה הפוליטית שלהם דלף לרשת האינטרנט.[97]

במערכת **הבחירות לכנסת ה־23** השתמשו מפלגות רבות ביישומוני בחירות ייעודיים, שמטרתם לאסוף מידע על בוחרים, לקטלג אותם לפי מידת התמיכה שלהם במפלגה (תומך, מתלבט, לא תומך או לא יודע), ולהפיץ מסרים מותאמים אישית.

עם חשיפת השימוש שעשו מפלגות הליכוד, ש"ס וישראל ביתנו ביישומון "אלקטור" במערכת הבחירות לכנסת ה־23 הוגשה ליו"ר ועדת הבחירות המרכזית עתירה בבקשה למנוע או להגביל את השימוש ביישומון בטענה להפרת חוק הבחירות, חוק הגנת הפרטיות ותקנות אבטחת מידע. בעתירה נטען שהמידע המועלה ליישומון גלוי לכל אדם, ללא כל פיקוח ובקרה, ושהופצו סיסמאות כניסה ליישומון ברשתות החברתיות ובקבוצות ווטסאפ. נטען בעתירה כי הופצו סרטונים מטעם תנועת הליכוד בהם נקראו תומכי המפלגה להוריד את יישומון אלקטור ובסרטון פורסם מספר טלפון. כל המעוניין יכול היה לשלוח מסרון למספר הטלפון ולקבל בתגובה קישורית עם סיסמה להתקנת היישומון ולהפעלתו. מרגע זה קיבל המתקין גישה לכל מידע הפנקס והמידע המטויב שצורף לו, ולמעשה יכול היה לחפש מידע על כל אחד מבעלי זכות הבחירה בישראל, ללא קשר להתמודדות מפלגת הליכוד בבחירות ולכל צורך שהוא. לכן, נטען כי מדובר בפגיעה בפרטיות של כל הרשומים במידע הפנקס ובעקרון צמידות המטרה בחוק הגנת הפרטיות, וכן בעבירה על חוק הבחירות, שכן יש לקבל היתר לשם העברת מידע הפנקס לגורם אחר. עוד נטען שמידע הפנקס ביישומון נשמר גם לאחר הבחירות בניגוד לדין, שטיוב המידע אודות כל בוחר באמצעות היישומון יוצר מאגר נתונים חדש ועשיר יותר על גבי מידע הפנקס ועל כן אסור לפי החוק, וכי השימוש ביישומון ביום הבחירות מהווה הפרה של חשאיות הבחירות ואסור על פי חוק.[98] כן נטען כי השימוש ביישומון ללא הגבלות הרשאה, עלול להביא לפגיעה בביטחון המדינה, ולאפשר לגורמי ביון זרים

---

[95] ה"ש 7/22 **עדאלה המרכז המשפטי לזכויות המיעוט הערבי בישראל ואחרים נ' הליכוד ואחרים** (26.8.2019), בפסקה 60 להחלטה.

[96] איתמר ב"ז "סממנים של מדינת מעקב" **העין השביעית** (9.9.2019).

[97] חגי עמית "לגנץ פרצו לטלפון? בליכוד חשפו מיליון ישראלים ברשת לפי זהותם הפוליטית" **דה מרקר** (9.9.2019).

[98] תב"כ 14/23 **בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'** (18.2.2020), פסקה 1 להחלטה.

לחשוף סיפורי כישוי של סוכני ביון ישראלים בחו״ל.[99] הבקשה הוגשה למתן צו מניעה, מכוח סעיף 17ב לחוק הבחירות (דרכי תעמולה), התשי״ט – 1959 (להלן: ״חוק דרכי תעמולה״) להפסקת השימוש ביישומון על ידי המפלגות.

יו״ר ועדת הבחירות המרכזית לכנסת ה־23, השופט ניל הנדל, הצביע על היעדר התאמת חוק דרכי תעמולה, שנחקק בשנת 1959, לשימוש שנעשה בטכנולוגיה לצרכי תעמולת בחירות וגם למעמדה של הזכות לפרטיות המהווה מאז חקיקת חוק־יסוד: כבוד האדם וחירותו, בשנת 1992, זכות יסוד חוקתית. לשיטתו, היעדר התאמה זה מחייב בחינה נורמטיבית מעמיקה של ההסדרים הקבועים בחוק דרכי תעמולה ולכן הצהיר כי יפעל להקמת ועדה לבחינת הנושא בתום הבחירות, שתעסוק ב״מכלול הסוגיות המתעוררות בנקודת המפגש שבין פרטיות וטכנולוגיה בדיני הבחירות״.[100] עם זאת, נוכח הפרשנות שהעניק בית המשפט העליון לסעיף 17ב לחוק דרכי תעמולה,[101] סבר כב׳ השופט הנדל שידיו כבולות ואין בידו להוציא את צו המניעה המבוקש. חוק הגנת הפרטיות אינו מבין החוקים המנויים במפורש בסעיף 17ב לחוק דרכי תעמולה, ולפיכך הכתובת למניעת הפרת הוראות חוק הגנת הפרטיות ותקנות אבטחת מידע ולשמירה על פרטיותם של אזרחי ישראל, גם בתקופת בחירות, היא הרשות להגנת הפרטיות וכן שרת הפנים.[102] על החלטה זו של יו״ר ועדת הבחירות המרכזית הוגשה עתירה לבג״ץ, אולם גם זו נדחתה על הסף ובית המשפט העליון אישר את פסיקתו של השופט הנדל.[103] השופטים קבעו כי הדרך להתמודד עם הסוגיה של אבטחת המידע ביישומוני הבחירות היא באמצעות הגשת תביעה אזרחית, והדרך לערור על החלטותיה של הרשות להגנת הפרטיות היא בבית משפט לענייניים מינהליים. עם זה קבע השופט שטיין כי מדובר בסוגיה מטרידה, ולנוכח חשיבותן הציבורית של הטענות שהעלו העותרים בחר שלא להשית עליהם הוצאות משפט.[104] השופטים לא דנו לגופה בטענה שאיסוף המידע על מי שטרם יצא להצביע הוא הפרה של העיקרון המעוגן בסעיף 4 לחוק־יסוד: הכנסת בדבר חשאיות הבחירות.[105]

לאחר הדיון בעתירה האמורה ולפני מתן ההחלטה בה, בפברואר 2020, אירע אירוע אבטחת מידע במערכות המידע של יישומון הבחירות של חברת אלקטור במסגרתו התאפשרה גישה למערכות המידע של החברה ודלף לרשת האינטרנט קובץ המכיל את מידע הפנקס לכנסת ה־23 על אודות כ־6.5 מיליון בעלי זכות בחירה בישראל. מאגר המידע כלל לא רק פרטי מידע המופיעים במידע הפנקס, כגון שם פרטי, שם משפחה, שם אב או אם, כתובת, ומספר ת.ז., אלא גם שכבות מידע אישי ולעיתים רגיש נוספות כגון מספר טלפון, כתובת דוא״ל, מצב רפואי ודעה פוליטית ומידת תמיכה במפלגה. המידע אף פורסם ברשת האפלה (dark web).[106] כשבוע אחרי חשיפת פרצת המידע הראשונה, נודע על שני כשלי אבטחה חדשים

---

[99] שירות כלכליסט ״תמיר פרדו: ׳אלקטור היא הקורונה הביטחונית של מדינת ישראל – הסירו אותה׳״ **כלכליסט** (26.2.2020); יוסי מילמן ״למי אירגן צריכה להודות על חשיפת פנקס הבוכרים? שבעה גופים״ **הארץ** (17.2.2020).

[100] תב״כ 23/14 **בן מאיר ואח׳ נ׳ הליכוד ואח׳** (18.2.2020).

[101] דנג״ץ 1525/15 **ח״כ ד״ר אחמד טיבי נ׳ מפלגת ישראל ביתנו ואח׳** (נבו, 23.8.2017).

[102] תב״כ 13/23 **בן מאיר ואח׳ נ׳ הליכוד ואח׳**, ועדת הבחירות המרכזית לכנסת ה־23 (18.2.2020).

[103] בג״ץ 1311/20 **בן מאיר ואח׳ נ׳ הליכוד – תנועה לאומית ליברלית ואח׳**, (נבו, 25.2.2020).

[104] אורי ברקוביץ׳ ״בג״ץ דחה על הסף את העתירה נגד אפליקציית המרצת הבוחרים אלקטור״ **גלובס** 25.2.2020, https://www.globes.co.il/news/article.aspx?did=1001319767; איתמר ב״ז ״בג״ץ דחה את העתירה נגד הליכוד ו׳אלקטור׳״ **העין השביעית** 25.2.2020. https://www.the7eye.org.il/362895

[105] ענת בן-דוד ״מיום הבוחר ליום העוקב״ **העין השביעית** 18.2.2020. https://www.the7eye.org.il/361904

[106] עומר כביר ״פרצת האבטחה באפליקציה של הליכוד: הפרטים האישיים של כל הבוחרים נחשפו״ **כלכליסט** 9.2.2020; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ״א-**

נוספים במערכת היישומון אלקטור שהובילו לחשיפת כל מאגרי המידע שהעלו המפלגות שעשו באותה העת שימוש ביישומון – הליכוד וישראל ביתנו, לרבות מידע הפנקס. זאת לצד חשיפת קוד המקור של היישומון עצמו.[107]

אירוע זה שווה ערך למעשה לדליפת מרשם האוכלוסין והוא ארוע סייבר חמור ביותר. הרשות להגנת הפרטיות פתחה בחקירת אירוע דלף המידע ביישומון אלקטור מספר ימים לאחר חשיפתו. בחקירת אירוע דלף המידע על ידי הרשות להגנת הפרטיות נמצא שמערכת אלקטור אפשרה את יצוא המידע שבמערכת על ידי הפקת דוחות לפי בקשת כל משתמש. לכל משתמש ביישומון ניתנה הרשאה לבצע 50 שאילתות חיפוש, כלומר כל פעיל מפלגה שהתקין את היישומון הורשה לבצע 50 הצלבות בין אנשי הקשר שלו לבין הבוחרים המופיעים בפנקס הבוחרים, ולהזין לגביהם מידע נוסף המצוי בידו.[108] עם הורדת היישומון הוצגה בפני המשתמש הודעה לפיה ביכולתו להזין אך ורק פרטי מידע על אנשים שנתנו את הסכמתם לכך. בשטח, הפעילים לא יישומו את דרישת ההסכמה כנדרש.[109]

בינואר 2021 פרסמה הרשות את ממצאי חקירתה. נקבע שהליכוד, ישראל ביתנו וחברת אלקטור הפרו את הוראות חוק הגנת הפרטיות ותקנות אבטחת מידע. אולם הרשות להגנת הפרטיות הצהירה שבכוונתה להטיל קנס מינהלי רק על חברת אלקטור.[110] החלטת הרשות ניתנה כ־11 חודשים אחרי אירוע דלף המידע, ובהיעדר סמכות להטיל קנסות בגין מרבית ההפרות שנמצאו, הוטל בסופו של יום קנס אך ורק על חברת אלקטור.[111]

בבחירות לכנסת ה־24 בשנת 2021, עשה הליכוד שימוש ביישומון שכונה בתחילה "ליכוד נט", ומאוחר יותר הוחלף שמו ל"ניצחון 22", אשר פותח על ידי חברת אלקטור ושימוש למטרה דומה.[112] מקורב לחברת "אלקטור" טען באותה העת כי המערכת בה נעשה שימוש עברה שינויים משמעותיים ולא סבלה מדליפות מידע. לפי המידע שמסר, המשתמשים ביישומון החדש אינם נחשפים למספר ת.ז של כלל הבוחרים שפרטיהם מופיעים במאגר המידע שביישומון על בסיס מידע הפנקס. בנוסף, גם כתובת המגורים הנגישה לכלל הציבור כוללת רק את שם הרחוב ולא את מספר הבית. כן, המשתמש ביישומון

1981 – מפלגת ישראל ביתנו (27/01/2021) ; **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021) ; **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – אלקטור** (27.1.2021).

[107] ראו עומר כביר "לא תיקנו: ספר הבוחרים שוב דלף מאלקטור" **כלכליסט** (16.2.2020). פרצת האבטחה הובילה להגשת שתי תביעות אזרחיות נגד אלקטור ומפלגת הליכוד בטענה להפרת הוראות חוק הגנת הפרטיות. אלו הוגשו עוד לפני שהרשות להגנת הפרטיות סיימה את חקירתה בנושא, אולם שתיהן הסתיימו בפשרה חסויה כשנתיים אחר כך. ראו אורן פרסיקו "תביעה נוספת נגד "אלקטור" הסתיימה בפשרה" **העין השביעית** (5.6.2023) ; אורן פרסיקו "תביעה נגד הליכוד בגין הפרת חוקי הפרטיות הסתיימה בפשרה" **העין השביעית** (17.9.2022).

[108] הרשות להגנת הפרטיות, מחלקת אכיפה, קביעת הפרה של חוק הגנת הפרטיות, התשמ"א-1981 (27.1.2021) (סימוכין 008-2021-00000712 ; 2021-00000695).

[109] ענת ציגלמן "האפליקציה שמכריעה את הבחירות וכל האמצעים כשרים. כמעט" **שומרים** (18.3.2021).

[110] חוק הגנת הפרט 128, התשע"ז עמ' 986, התשפ"ד 1430 (להלן: "חוק הגנת הפרטיות"); תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז–2017 (להלן: "תקנות אבטחת מידע"); מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27/01/2021) ; **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021) ; **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – אלקטור** (27/01/2021) ;

[111] הרשות להגנת הפרטיות, מחלקת אכיפה, קביעת הפרה של חוק הגנת הפרטיות, התשמ"א-1981 (27.1.2021) (סימוכין 008-2021-00000712 ; 2021-00000695).

[112] שוקי טאוסיג "קמפיין בהסוואה? **העין השביעית** (18.9.2022).

אינו יכול לאתר מידע אישי על אנשים אחרים באמצעות היישומון. באפשרותו ליצור באמצעות היישומון שיחה למספר טלפון של בוחר אחר רק אם הוא הוסיף את מספר הטלפון של המשתמש האחר. עוד נמסר כי כל מפלגה יכולה להוסיף שכבות מידע וקטיגוריות כרצונה.[113]

כבר בפתח שנת **הבחירות לכנסת ה־*26***, בינואר 2026, הגיע לפתחה של ועדת הבחירות המרכזית נושא הקשור בשימוש ביישומוני בחירות, כאשר הוגשה עתירה הטוענת כי הפרקטיקה של תיעוד מצביעים המבוצע על ידי חברי ועדת הקלפי ומשקיפים, והכנסת המידע לתוך יישומוני הבחירות המפלגתיים, היא פגיעה בחשאיות הבחירות ופגיעה בזכות הבוחר לפרטיות. לפי סעיף 79 לחוק הבחירות לכנסת, משקיף רשאי להוסיף בפרוטוקול ועדת הקלפי את הערותיו העובדתיות הנוגעות לפעולות הוועדה ולבדוק את תא ההצבעה מעת לעת כדי לוודא שיש כמות פתקים מספקת לרשימה שהוא מייצג או לכל רשימה אחרת.[114] לפי תקנות 58, 60(ב) ו־61 לתקנות הבחירות התשל"ג-1973, ה"זהותון" – הרשימה הכוללת את שמות הבוחרים ואת מספרי תעודות הזהות שלהם – מסופקת לחברי ועדת הקלפי כאמצעי עזר לזיהוי הבוחרים בקלפי. ואולם החוק אינו מסמיך את חברי ועדת הקלפי או את המשקיפים להשתמש בפרטים אישיים אלה לצורך העברתם בחזרה אל מרכזי המפלגות.

סעיף 45א לתקנות הבחירות קובע כי ביום הבחירות, בשעה שבה מצביע מצוי בקלפי ובעת ספירת הקולות, אין לשוחח במכשיר טלפון נייד או מכשיר קשר בחדר שבו פועלת ועדת קלפי, אלא לצורך ניהול ההצבעה בקלפי או במקרי חירום. ניתן לפרש כלל זה כקביעה שלפיה השימוש במכשיר טלפון נייד בעיקרון אסור, אלא לצורך ניהול ההצבעה. בנוסף, אם נציגי המפלגות ממלאים במקום הקלפי תפקיד ציבורי על פי דין כחברי ועדת הקלפי או כמשקיפים, הרי שמכוח עקרון החוקיות אסור להם לבצע פעולות שלא הוסמכו במפורש בדין לעשותן.

נעיר כי כבר בחוות דעת שהגשנו בעניין **תב"כ 14/23 בן מאיר ואח' נ' הליכוד תנועה לאומית ליברלית ואחרים**, סברנו כי אין לאפשר שימוש באפליקציות על ידי חברי וועדות קלפי ומשקיפים לצורך הוצאת פרטי בוחרים בזמן אמת אל מוח מרכזי ואיגומם עם מאגרים מרכזיים. זאת, הן בשל היעדר סמכות והן בשל הפגיעה בפרטיות הבוחרים ובחשאיות הבחירות. סברנו כי ליו"ר ועדת הבחירות הסמכות ליתן החלטות והוראות בעניינים אלה, וזאת הן לאור פרשנות נצרכת למילוי החלל שבין האסדרה והטכנולוגיה ולמניעת ניצולו לרעה, והן בשל פרשנות סעיף 17ב לחוק התעמולה וסעיף 118 לחוק הבחירות.[115]בחוות דעת שהוגשה לוועדת הבחירות המרכזית במסגרת ההליך הנוכחי, הסבירו מומחי פרטיות כי המידע אודות הצבעתו של פלוני בקלפי מגיע לחברי ועדת הקלפי ומשקיפים כחלק מתפקידם לפקח ולשמור על טוהר הבחירות. תיעוד עצם ההגעה להצביע מוגדר כ"חומר רגיש" בתוספת הראשונה לכללי הבחירות לכנסת (עיון בחומר בחירות) תשע"ח–2018, אמור להתבצע רק בעותקים קשיחים ולא דיגיטליים, ולפי סעיף 79א לחוק הבחירות לכנסת [נוסח משולב], התשכ"ט–1969, חובה להשמידו לאחר תום המועד להגשת ערעורי בחירות. לפיכך, תיעוד עצם ההצבעה לתוך יישומוני בחירות מפלגתיים הוא חריגה מסמכותם לפי דין של המשקיפים וחברי ועדת הקלפי, מהווה פגיעה בפרטיות הבוחרים ובעקרון חשאיות

---

[113] שחר סמוחה "המצביע האוטומטי: 'הציבור לא מבין את עומק המניפולציה שעושים עליו'" **שומרים** (29.92022).

[114] ועדת הבחירות המרכזית לכנסת ה־21 מטה ההדרכה **תדריך ונוהלי עבודה למזכיר ולבעלי תפקידים בוועדות הקלפי** 2 (2019).

[115] רחל אריידור הרשקוביץ ותהילה שוורץ אלטשולר, חוות דעת ליו"ר וועדת הבחירות במסגרת **תב"כ 14/23 בן מאיר ואח' נ' הליכוד תנועה לאומית ליברלית ואחרים**, 13.2.2020, באתר המכון הישראלי לדמוקרטיה.

הבחירות, ויוצר אפקט מצנן על ההצבעה או אי ההצבעה אשר פוגם באמון הציבור בטוהר הבחירות.[116] נכון לכתיבת שורות אלו העתירה עודה תלויה ועומדת.

לסיכום, מנגנוני ההגנה על השימוש האסור במידע פרטי על אזרחי ישראל לצורך השפעה על הבחירות – אינם מספקים. מצד אחד, השימוש במידע מפנקס הבוחרים באמצעות יישומוני בחירות אינו מצוי תחת אסדרה של חוקי הבחירות ובעתירות שהוגשו בנושא לבג"ץ ולוועדת הבחירות המרכזית לא התקיים דיון מהותי. העתירה נדחתה בבג"ץ בנימוק שאינו הערכאה המתאימה,[117] ובוועדת הבחירות המרכזית בנימוק שאין ליו"ר הוועדה סמכות להכריע בנושא אלא נדרש שינוי חקיקתי.[118] אולם שינוי שכזה טרם בוצע. זאת, על אף שהשימושים במידע אישי על בוחרים אינם מהווים רק פגיעה בפרטיות אלא בעיקר עשויים לפגוע בעיקרון חשאיות הבחירות,[119] ולסכן את טוהר ההליך הדמוקרטי ואת מימושה המלא של הזכות לבחירות שוות והוגנות,[120] נושא שאין מחלוקת שהוא מצוי בתחום סמכותו הטבעית של יו"ר ועדת הבחירות המרכזית.[121]

בנסיבות אלו, יש חשיבות רבה לתחולתו של חוק הגנת הפרטיות ושל תקנות אבטחת מידע על שימוש במידע אישי לצורך תעמולת בחירות ולכלים שהוא מעניק לרשות להגנת הפרטיות לצורך אסדרת שימוש זה. ראשית, יודגש שכפי שקבעה הרשות להגנת הפרטיות במכתבי קביעת ההפרה בפרשת אלקטור, העובדה שהשימוש ב"מידע הפנקס" מוסדר במסגרת חוק הבחירות אינה מפקיעה את תוכן מידע הפנקס מתחולת חוק הגנת הפרטיות.[122]

אכן, לקראת הבחירות לכנסת ה־23 ולכנסת ה־24 פרסמה הרשות להגנת הפרטיות במשרד המשפטים מספר מסמכים חשובים הנוגעים לתחולת הוראות חוק הגנת הפרטיות על השימוש הנעשה על ידי המפלגות או מטעמן במידע אישי, לרבות מידע מפנקס הבוחרים, וביישומונים לניהול מערכת בחירות.[123]

---

[116] מיכאל בירנהק ונועה דיאמונד "הצבעה בבחירות כמידע פרטי: חוות דעת של הקליניקה לפרטיות" הקליניקה לפרטיות, התוכנית לחינוך משפטי קליני ע"ע אלגה צגלה, הפקולטה למשפטים ע"ש בוכמן, אוניברסיטת תל אביב (פברואר 2026).

[117] בג"ץ 1311/20 **בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'** (נבו, 25.2.2020).

[118] תב"כ 14/23 **בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'** (נבו, 18.2.2020).

[119] בימים אלו תלויה ועומדת עתירה בנושא בפני יו"ר ועדת הבחירות המרכזית. ראו ה"ש 17-26 **בן מאיר נ' היועצת המשפטית לממשלה ואח'** (פברואר 2026).

[120] כך, למשל, נטען שבמערכת הבחירות לנשיאות ארה"ב בשנת 2016 שלח טראמפ מסרים אישיים בטכניקת מיקרו־טרגרטינג, לכ־3.5 מיליון בוחרים אפרו אמריקאים, שעיבוד המידע האישי אודותיהם מצא שהם נוטים שלא להצביע. המסרים כללו מודעות בדבר ייחסה הקלוקל של המועמדת היריבה, הילארי קלינטון, לאפרו־אמריקאים. מטרת שליחת מסרים אלו הייתה לעודד בוחרים אלו שלא לממש את זכותם להצביע בבחירות לנשיאות ארצות הברית. ראו Channel 4 News Investigations Team, *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016*, CHANNEL 4 NEWS (Sep. 28, 2020)

[121] בג"ץ 1311/20 **בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'** (נבו, 25.2.2020).

[122] ראו מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27/01/2021), סעיפים 9.1, 10.2; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 9.5, בעמ' 4.

[123] הרשות להגנת הפרטיות, **ריענון הוראות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־23 מגבלות השימוש במידע מפנקס הבוחרים ומגבלות השימוש במידע אישי** (להלן: "הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים"); ; הרשות להגנת הפרטיות, **דרישות חוק הגנת הפרטות לקראת הבחירות לכנסת ה־24: מגבלות השימוש בפנקס הבוחרים ובמידע**

הרשות הדגישה שעל המידע שנמסר למפלגות במסגרת מידע הפנקס, כמו גם המידע שנאסף על ידי מפלגות במסגרת קמפיין בחירות, חלות הוראות חוק הגנת הפרטיות לצד חוק הבחירות. המפלגות הן הנושאות באחריות כ"בעלות מאגר". ספקי השירות החיצוניים עמם מתקשרת המפלגה לשם עיבוד המידע באמצעות יישומון או בדרך אחרת או אחסון בלבד נושאים באחריות לפי חוק הגנת הפרטיות כ"מחזיק".[124] בין ההוראות המחייבות בחוק הגנת הפרטיות מנתה הרשות את הוראות תקנות אבטחת מידע ביחס למאגר מידע ברמת אבטחה גבוהה או בינונית,[125] וכן את עקרון צמידות המטרה ואיסור שימוש במידע שלא למטרה לשמה הוקם המאגר. על בסיס שילוב הוראות אלו עם הוראת סעיף 39(ב) לחוק הבחירות, הבהירה הרשות שאין לעשות שימוש במידע הפנקס למטרות שאינן קשורות להתמודדות בבחירות ולקשר עם הבוחר, לרבות העברתו לצד שלישי לשימושים אחרים. הפרת איסור זה היא עבירה שדינה מאסר שנתיים לפי סעיף 118א לחוק הבחירות ובנסיבות מסוימות אף עשויה להיות עבירה לפי חוק הגנת הפרטיות.[126]

יתרה מכך, לעמדת הרשות אין לעשות שימוש בפנקס הבוחרים ממערכות בחירות קודמות או ממערכות בחירות לרשויות מקומיות, ויש לבער את כל עותקי המידע שמקורם במידע הפנקס, בין שהם בידי המפלגה או בידי ספקיות עמן התקשרה, וכן כל נגזרת של מאגרי מידע אלו, בתום הבחירות.[127]

בנוסף הדגישה הרשות להגנת הפרטיות שאין לעשות שימוש במידע אישי על אדם או לפרסם אותו שלא בהסכמתו מדעת של אותו האדם, או למטרה החורגת ממטרת השימוש שהוסברה לו בעת קבלת הסכמתו. הרשות הדגישה שבהיעדר הסכמת הבוחרים להזנת פרטיהם ביישומונים או במאגרי המידע של המפלגה, במיוחד אינדיקציות בדבר תמיכתם או אי תמיכתם במפלגה כזו או אחרת, שימוש במידע האישי הוא הפרה של עקרון צמידות המטרה ופגיעה בפרטיות לפי סעיף 2(9) לחוק הגנת הפרטיות והוא בלתי חוקי. עוד הבהירה הרשות שכל סחר במידע כאמור ללא הסכמת האדם שהמידע אודותיו אינו חוקי. ולפיכך, בעת התקשרות עם צד שלישי לשם רכישת מידע אישי על בוחרים יש לוודא את חוקיות מקורות המידע.[128]

עוד הבהירה הרשות שעל הודעות הנשלחות לבוחרים מטעם מפלגות, רשימות או מתמודדים, המפולחות על בסיס מאפיין אישי, חלות הוראות חוק הגנת הפרטיות בנושא דיוור ישיר. זאת משום ש"דיני הדיוור הישיר חלים על כל פניה לאדם המתבססת על אפיון אישי, וזאת בכל מדיה, טכנולוגיה או פורמט, לרבות בהודעות SMS, ברשתות חברתיות ובאפליקציות מסרים מיידים," ובניגוד לחוק דואר זבל, [129] "הוראות

אישי אחר ואחריות המפלגות על אפליקציות וספקים חיצוניים (7.1.2021) (להלן: דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24).

[124] דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בסעיפים 7–10, 24–25.

[125] דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בסעיף 17.4.

[126] הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 123, סעיפים 8–10; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בסעיפים 11–12, 17.1.

[127] דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בסעיפים 17.3, 17.7; הרשות להגנת הפרטיות, דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־25: מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר ואחריות המפלגות על אפליקציות וספקים חיצוניים.

[128] הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 123, סעיפים 17–18; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, לעיל ה"ש 123, בסעיף 17.2.

[129] סעיף 30א לחוק התקשורת, התשס"ח–2008 (להלן: "חוק דואר זבל").

חוק הגנת הפרטיות בנושא דיוור ישיר חלות גם על תעמולה פוליטית ולמעשה על כל סוג של פניה מפולחת לאדם, בלי קשר לתוכנה ולמהותה." במסגרת זו עומדת לבוחר הזכות שפרטיו יימחקו ממאגר מידע.[130]

על אף הבהרותיה של הרשות להגנת הפרטיות, בדוח מבקר המדינה מיום 12.7.2022 נמצא שאף מפלגה לא רשמה את מאגר המידע הכולל את המידע מפנקס הבוחרים לאחר טיוב ועדכון הנתונים בו. יתרה מכך, שש מהסיעות והמפלגות ביצעו טיוב של נתוני המאגרים הללו באמצעות חברות מסחריות, מבלי לבדוק את מידת חוקיות המידע שרכשו מהחברות לצרכיי הטיוב ומבלי לוודא שנושאי המידע נתנו את הסכמתם לאיסוף, העברה ועיבוד המידע האישי אודותיהם.[131] בנוסף, התפרסם בתקשורת כי חלק מן המפלגות עשו שימוש במידע הנמצא ברשותן באשר לשאלה מי מן האזרחים יצאו להצביע בבחירות האחרונות, על אף שמדובר במידע שלפי הדין ולפי התחייבויותיהן שנחתמו על ידן כתנאי לקבלת המידע, היה עליהן למחוק בתום מערכת הבחירות הקודמת.[132]

עד לחקיקת תיקון 13 לא היו בידי הרשות להגנת הפרטיות, המוסמכת לדאוג לפרטיותם של אזרחי המדינה בתקופת בחירות, כלי אכיפה מספקים כדי להבטיח שהמפלגות יעמדו בדרישות חוק הגנת הפרטיות בעת השימוש במידע אישי ורגיש ביישומונים לניהול בחירות. אומנם, היבט זה השתנה באופן מהותי עם חקיקת תיקון 13 לחוק הגנת הפרטיות, שבו נעסוק בהמשך. אולם עדיין החוסר המהותי בהסדרים בחוק הגנת הפרטיות כמו גם ההסדר להקפאת סמכויות הפיקוח והאכיפה של הרשות בתקופת בחירות,[133] יוצרים קושי באכיפה הנדרשת בזמן אמת לשם מזעור הפגיעה בפרטיות.

[130] הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 123, סעיפים 16-13 ; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, לעיל ה"ש 123, בסעיף 17.6.

[131] מבקר המדינה, פרסום דוחות מימון המפלגות – יולי 2022.

[132] שוקי טאוסיג "תיעוד מכנס מתנדבי הליכוד: נביא לכם טלפונים של כל מי שלא הצביע למפלגה" **העין השביעית**, 22.7.2022.

[133] ראו פרק ד'5 לחוק הגנת הפרטיות, לעיל ה"ש 110.

חלק שני

תיקון 13 והשפעתו על השימוש במידע אישי אודות בעלי זכות הצבעה במהלך קמפיין בחירות

מבוא

תיקון 13 הוא אבן דרך בהתפתחות הגנת הפרטיות במדינת ישראל, והוא כולל תיקונים משמעותיים ונחוצים לחוק הגנת הפרטיות. בתיקון נוסף גם הסדר מיוחד לאכיפת הוראות חוק הגנת הפרטיות בתקופת בחירות. לכלל השינויים האלה השפעה ישירה ומשמעותית על השימוש במידע אישי על אודות בעלי זכות הבחירה בישראל בתקופת בחירות ; סמכויות הרשות להגנת הפרטיות ; וגם על הפעולות שניתן לנקוט – הן באמצעות רשויות השלטון והן באמצעות אכיפה פרטית – כדי לשפר את ההגנה על הזכות לפרטיות מפני פגיעה בהן על ידי מתמודדים ומפלגות.

בפרק זה נסקור תחילה את השינויים שהתקבלו בתיקון 13 להגדרות המונחים "מידע אישי", "מידע בעל רגישות מיוחדת" ו"מאגר מידע" ונעמוד על השלכותיהם מבחינת תחולת חוק הגנת הפרטיות על השימוש שעושות מפלגות ומפעילי יישומוני בחירות במידע אישי אודות הבוחרים. בהמשך נעמוד על הגדרות בעלי התפקידים הרלוונטיים לעיבוד מידע אישי לפי תיקון 13, על החובות המרכזיות המוטלות עליהם והאחריות בה נושאים, ונבחן את יישומן של הוראות אלו על מפלגות ומפעילי יישומוני בחירות. כן נעמוד על ההגבלות והאיסורים שהוספו לחוק הגנת הפרטיות בתיקון 13 על עיבוד מידע אישי במאגר מידע והחלתן על השימוש שעושות מפלגות ומפעילי יישומונים במידע אישי על בוחרים, לצד בחינת הזכויות המוקנות לבוחרים, נושאי המידע, בעקבות תיקון 13. לבסוף, נבחן את כלי הפיקוח והאכיפה המינהלית המוקנים בתיקון 13 לרשות להגנת הפרטיות בשגרה ובמהלך תקופת בחירות ונעמוד על השלכות מנגנון זה על הרשות להגנת הפרטיות, ציבור הבוחרים ועדת הבחירות המרכזית.

פרק שלישי
מידע אישי, מידע בעל רגישות מיוחדת ומאגר מידע לפי חוק הגנת הפרטיות

חוק הגנת הפרטיות מושתת על הבחנה בין נתון למידע אישי; בין מידע אישי לבין מידע בעל רגישות מיוחדת; ובין אוסף פרטי מידע אישי או מידע בעל רגישות מיוחדת לבין מאגר מידע. הבחנות אלו הן שערי הכניסה לתחולת חוק הגנת הפרטיות. רק אם הנתון עונה להגדרת מידע אישי ונאסף באוסף העונה להגדרת מאגר מידע, יחולו הוראות חוק הגנת הפרטיות.

אם המידע האישי שבמאגר המידע נכנס לגדר אחת מהקטיגוריות שהוגדרו על ידי המחוקק כמידע בעל רגישות מיוחדת, הרי שמדובר במידע אישי מיוחד ששימוש לא מורשה או חוקי בו טומן סכנה גדולה יותר לזכות לפרטיות, ועל כן מוטלות ביחס לשימוש בו, שמירתו והעברתו, דרישות מחמירות יותר.

1. הגדרת "מידע"

תיקון 13 הרחיב את ההגדרה של המונח "מידע" שמהווה את התנאי הראשון לתחולת חוק הגנת פרטיות והוא מוגדר כעת כך:

> "מידע אישי" – "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;".[134]

להגדרה זו משמעות כפולה. ראשית, מידע אישי מוגדר באופן רחב הכולל גם נתון הנוגע ל"מצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי" של אדם. כלומר, מרבית המידע המצוי בידי מפלגה, הן זה שמקורו במידע הפנקס (שם, מספר זהות וכתובת מגורים), והן מידע מטויב שהוסף על ידי פעילי מפלגה ומשתמשי יישומוני הבחירות השונים (למשל מידע המתאר את נכותו של אדם, או הסטטוס החברתי או התרבותי שלו), נחשב מידע אישי.

נוסף על כך, מדובר במידע של אדם מזוהה או מי ש"ניתן לזהותו במאמץ סביר". כלומר, גם אם מדובר במידע מותמם, יש להביא בחשבון אפשרות שעיבוד המידע המותמם והצלבתו עם נתונים אחרים עשוי להביא לזיהויו, במישרין או בעקיפין, של אדם מסוים. עם זאת, ככל שהדברים אמורים במידע הנוגע לבחירות,[135] המידע איננו מותמם אלא ההיפך – יש חשיבות דווקא להיותו מידע מזוהה, וככזה הוא מועבר באמצעות פנקס הבוחרים ונבנות על גבו שכבות נוספות של מידע מזוהה.

---

[134] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[135] ראו גם את התכלית למסירת מידע פנקס הבוחרים שנמצאת בסעיף 39(ג) לחוק הבחירות, לעיל ה"ש 75.

2. מידע בעל רגישות מיוחדת

אפיון מידע אישי כ״מידע בעל רגישות מיוחדת״, אינו משפיע על תחולת חוק הגנת הפרטיות, אלא על החובות המוטלות על מי שמבקש לעבד מידע הנמנה על קטיגוריות אלו. למשל, מי שבבעלותו מאגר מידע שבו מידע בעל רגישות מיוחדת על 100,000 נושאי מידע ומעלה, חייב להודיע על כך לרשות להגנת הפרטיות.[136] כן, חלות עליו דרישות אבטחת מידע מחמירות יותר,[137] ובמקרה שהוא או מי שמעבד בעבורו את המידע במאגר המידע מפר הוראה מהוראות חוק הגנת הפרטיות, הוא עשוי לשאת בסכום עיצום כספי גבוה יותר מזה שהיה מוטל עליו אם במאגר המידע לא היה מידע בעל רגישות מיוחדת.[138]

תיקון 13 יצר שינוי משמעותי בהגדרת בקטיגוריות המידע האישי שנחשבות ״מידע בעל רגישות מיוחדת״, משום שהוא הוסיף סוגי מידע בעל רגישות מיוחדת שלא נכללו קודם לכן בחוק ושעשויות להיות רלבנטיות ביחס למידע האישי שבשליטת מפלגה או שמוסק על ידה. להלן, נסקור את סוגי המידע האלה.

(1) מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישותו ועל נטייתו המינית[139]

המדובר בפרטי מידע המעידים באופן ישיר, ולא עקיף או על דרך ההיסק, על צנעת אישותו של אדם, נטייתו המינית וצנעת חיי המשפחה שלו. תיבה אחרונה זו כוללת את כל אותם סוגי מידע והתנהגויות שאינן נופלים לגדר צנעת אישותו או נטייה מינית, אך מתרחשים בצנעת הפרט. למשל, התנהלות בין בני זוג, יחסים בין הורים וילדיהם, שיטות חינוך במשפחה, אלימות כלכלית, החלטות הנוגעות להרחבת המשפחה או להמשך התא הזוגי.[140]

כלומר, פרטי מידע המופיעים ביישומון בחירות או במאגר מידע של מפלגה כגון תלות של בן באביו, למשל ״אביו פעיל ליכוד, עשוי לחשוש להצביע בשונה מאביו״; מידע על נטייה מינית; מידע לגבי פנייה של בני זוג ליועץ זוגי או לגישור לפני גירושין או על שיטות חינוך במשפחה יחשבו כמידע בעל רגישות מיוחדת תחת קטגוריה זו.

(2) מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי כהגדרתו בחוק זכויות החולה[141]

קטגוריה זו כוללת כל מידע הקשור לבריאות הפיזית או הנפשית של נושא המידע בעבר, בהווה או בעתיד, לרבות מידע הנאסף במסגרת מתן שירותי רפואה אבל איננה מוגבלת רק למידע הנוצר או נאסף בנסיבות

---

[136] סעיף 8א(ב) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[137] תקנות אבטחת מידע, לעיל ה״ש 110. במהלך הדיונים בתיקון 13 הובהר שיבוצעו התאמות בתקנות אבטחת מידע על מנת 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), עמ׳ 58.

[138] פרוטוקול מס׳ 203 מישיבת ועדת החוקה, חוק ומשפט, יום שני, ו׳ בטבת התשפ״ד (18 בדצמבר 2023), עמ׳ 3.

[139] סעיף 3 בחוק הגנת הפרטיות, לעיל ה״ש 9.

[140] ראו פרוטוקול מס׳ 203 מישיבת ועדת החוקה, חוק ומשפט, יום שני, ו׳ בטבת התשפ״ד (18 בדצמבר 2023), 12–13; פרוטוקול מס׳ 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י״ד בטבת התשפ״ד (26 בדצמבר 2023), עמ׳ 3–7.

[141] סעיף 3 בחוק הגנת הפרטיות, לעיל ה״ש 9.

של יחסי מטפל-מטופל .[142] כלומר, כל מידע על מצב בריאותו של אדם, על מחלה ספציפית של אדם, נכותו, או הימצאותו בטיפולי פוריות ייחשב ללא ספק כמידע המתייחס למצב בריאותו של אדם. מדדים בריאותיים של אדם כפי שנאספים על ידי יישומוני כושר שונים או שעונים חכמים ייחשבו גם כן כמידע בעל רגישות מיוחדת.[143] מנגד, הערתו של פעיל מפלגה, שאינו איש מקצוע, שאדם הוא "לחיץ כמו קטשופ" לא בהכרח תחשב כמידע המתייחס למצב בריאותו של אדם, אך הדבר יהיה תלוי נסיבות.

(4) מידע אישי שהוא מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב[144]

"מזהה ביומטרי" מוגדר כ"נתון ביומטרי המשמש לזיהוי אדם או לאימות זהותו, או אמצעי ביומטרי שניתן להפיק ממנו נתון כאמור; לענין זה, "ביומטרי" – מאפיין אנושי, פיזיולוגי או התנהגותי, ייחודי, הניתן למדידה ממוחשבת".[145] אולם, לא כל מזהה ביומטרי הוא מידע בעל רגישות מיוחדת, שכן נוכח טכנולוגיות מתקדמות הקיימות כבר, עשויים מאגרי תמונות וסרטונים באיכות רגילה להכיל מזהים ביומטריים.[146] לפיכך, בדומה ל־GDPR,[147] נקבע בתיקון 13 כי רק מזהה ביומטרי, שאכן משמש או מיועד לשמש לזיהוי אדם או לאימות זהותו, יחשב כמידע בעל רגישות מיוחדת.[148] בהתאם להגדרה זו סביר שתמונת סלפי, למשל, שמשתמש ביישומון בחירות צילם והעלה למאגר המידע, לא תחשב מידע בעל רגישות מיוחדת. אולם, צילום של תעודת זיהוי, רישיון נהיגה או דרכון ביומטרי שיועלה על ידי משתמש למאגר המידע ביישומון הבחירות עשוי להיחשב כמידע בעל רגישות מיוחדת.

(5) מידע אישי על מוצאו של אדם[149]

מידע על מוצאו של אדם כולל רק מידע על מוצאו הגזעי או האתני של אדם.[150] קטגוריה זו אינה כוללת מידע על השתייכות לאומית או מידע על אזרחות זרה שיש לאדם. לפיכך, מידע בנוגע לזהות התרבותית־חברתית של אדם, כלומר למוצאו האתני, או ביחס לקטגוריה החברתית־היסטורית (גזע במובן race) של אדם יחשב מידע בעל רגישות מיוחדת. כך, למשל, ציון העובדה שאדם הוא אשכנזי, ספרדי, תימני, אתיופי או רוסי הנאמרת בהקשר העדתי תרבותי תחשב כמידע על מוצאו, ולכן כמידע בעל רגישות מיוחדת. למשל, העובדה שאדם מחזיק באזרחות גרמנית לא תחשב כמידע על מוצאו של אדם, לעומת זאת היותו "יקה" כן נופלת לגדר קטגוריה זו של מידע בעל רגישות מיוחדת.[151]

---

[142] ראו הגדרת מידע רפואי בסעיף 2 לחוק זכויות החולה, תשנ"ו–1996 (להלן: "חוק זכויות החולה") כ"מידע המתייחס באופן ישיר למצב בריאותו הגופני או הנפשי של מטופל או לטיפול הרפואי בו;".

[143] פרוטוקול מס' 203 מישיבת ועדת החוקה, חוק ומשפט, יום שני, ו' בטבת התשפ"ד (18 בדצמבר 2023), עמ' 17–19.

[144] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[145] סעיף 3 לחוק הגנת הפרטיות, לעיל ה"ש 9

[146] פרוטוקול מס' 203 מישיבת ועדת החוקה, חוק ומשפט, יום שני, ו' בטבת התשפ"ד (18 בדצמבר 2023), עמ' 23.

[147] סעיף 9(1) ל-GDPR, ה"ש 5 לעיל.

[148] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[149] שם.

[150] סעיף 9(1) ל-GDPR, ה"ש 5 לעיל.

[151] פרוטוקול מס' 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ד בטבת התשפ"ד (26 בדצמבר 2023), בעמ' 39–42.

(6) מידע אישי על אודות עברו הפלילי של אדם[152]

קטגוריה זו עוסקת בעברו הפלילי של אדם במובן הרחב, שכן היא אינה קושרת זאת למידע מהמרשם הפלילי או למידע פלילי שיש צורך לפנות למשטרה לשם קבלתו. משום כך, בהחלט יתכן שציון במאגר מידע שבשליטת מפלגה שפלוני ישב בכלא או שהוא עבריין מורשע יחשב כמידע הנופל תחת קטגוריה זו.[153]

(7) מידע אישי על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם או השקפת עולמו[154]

קטגוריה זו עוסקת בדעות פוליטיות ואמונות דתיות ופילוסופיות,[155] ואינה מצומצמת רק להזדהות המפלגתית. הקביעה האם מידע הוא פוליטי תעשה בהתאם לשאלה האם הוא מחזיק בעמדה ידועה לגבי נושא השנוי במחלוקת פוליטית. השקפת עולמו של אדם בקטגוריה זו היא מידע המלמד באופן מהותי על אופיו של אדם, והיא אינה כוללת למשל העדפה שלו לצבע מסוים.

בהתאם להגדרה זו, מידע בנוגע למידת תמיכתו של אדם במפלגה (תומך, לא תומך, מתלבט) נוגע לליבת הדעה הפוליטית של אדם ועל כן ייחשב למידע בעל רגישות מיוחדת. אולם, גם פרטי מידע נוספים עשויים להיחשב כמידע בעל רגישות מיוחדת לפי קטגוריה זו. למשל, מידע על כך שאדם שומר שבת יחשב מידע על אמונתו הדתית. מידע על השתתפותו של אדם בהפגנות בעד גיוס חרדים לצה"ל או נגד רפורמה בחקלאות או בשוק החלב עשויה להיחשב כמידע על השקפת עולמו

נציין בהקשר זה כי בפרשת "אלקטור" טענה מפלגת הליכוד שלא אספה מידע רגיש על בעלי זכות בחירה אלא ערכה מעין "מחקר דעת קהל" שנועד למצות את פוטנציאל המצביעים שלה. לטענת הלכוד, מידע בדבר תמיכת אדם במפלגה ואף התפקדותו למפלגה אינו מלמד בהכרח על דעותיו הפוליטיות, "שכן הבוחר בוחר מאחורי פרגוד ואין איש יודע כיצד בחר והאם הצבעתו בפועל שיקפה את תיאורו כ"תומך" או "לא תומך"."[156] אולם, בקביעת ההפרה דחתה, בצדק, הרשות להגנת הפרטיות טענות אלו והבהירה כי "אין חובה שמידע, כגון דעותיו הפוליטיות של אדם, יהיה אמין באופן מוחלט, אלא די שניתן יהיה לייחס לו אמינות ברמה סבירה ואף פחות מכך" על מנת להיחשב מידע רגיש.[157]

---

[152] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[153] במידה שמדובר במידע שגוי, יתכן גם שיהיה מדובר במידע שהוא בבחינת לשון הרע לפי חוק איסור לשון הרע, תשכ"ה–1965.

[154] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[155] ראו סעיף 9(1) ל-GDPR, לעיל ה"ש 5.

[156] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 9.8, בעמ' 5.

[157] שם, סעיף 10.7, בעמ' 11.

(8) מידע אישי שהוא הערכת אישיות שנערכה מטעם גורם מקצועי שכדרך עיסוק מחווה דעתו על אישיותו של אדם, או שנערכה באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים[158]

קטגוריה זו של מידע בעל רגישות מיוחדת נועדה לתת מענה למאפייני האישיות שאינם נכללים בקטגוריות אחרות של "מידע בעל רגישות מיוחדת". אולם, אין הכוונה לכל מאפיין אישיות, אלא רק לאלו ש"גורם מקצועי", שכדרך עיסוק מספק חוות דעת על מאפייני האישיות של אדם, מנה אותם, או במאפייני אישיות שהופקו באמצעות טכנולוגיה ייעודית לכך. הסיפא של הסעיף מספקת קריאת כיוון נוספת לפיה הכוונה היא לקווי אופי מהותיים, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים.[159]

לפיכך, מאפייני אישיות מהותיים כגון אופי חרדתי, נטייה לכעס, קלות דעת ברכישת מוצרים לאחר אימון ספורטיבי, או אימפולסיביות לאחר צפייה בסרטונים, שנקבעו על ידי גורם מקצועי העוסק בניתוח מאפייני אישיות של אדם או באמצעות טכנולוגיה ייעודית לכך, יהוו מידע בעל רגישות מיוחדת לפי קטגוריה זו. גם סיווגים של מאפייני אישיות מהותיים שנעשו על ידי מערכת בינה מלאכותית עשויים להיכלל בקטגוריה זו. לעומת זאת, חיווי דעה שמשתמש מזין על אדם אחר ביישומון, לא תחשב כהערכת אישיות.

(9) מידע אישי שהוא נתוני מיקום ונתוני תעבורה, כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת) שנוצרו על ידי ספק מורשה כהגדרתו בחוק האמור, לגבי אדם, ונתונים על אודות מיקומו של אדם שיש בהם כדי ללמד על מידע לפי פסקאות (1) עד (7) ו-(11)[160]

בתיקון 13 הובהר שנתוני תעבורה ומיקום יחשבו כבעלי רגישות מיוחדת רק אם יש בהם כדי ללמד על מידע רגיש אחר, [161] או נוצרו על ידי ספק מורשה, כהגדרת מונחים אלו בחוק נתוני תקשורת.[162] לכן, ארגונים שאינם חברת תקשורת, למשל חברה המוכרת תוכנה לבתי עסק ומנהלת תקשורת עם לקוחותיה, אינם נכללים בכך.[163]

בהתאם להגדרה זו, נתון בנוגע למיקומו של בוחר, גם אם אין מדובר במעקב רציף, עשוי להיחשב מידע בעל רגישות מיוחדת אם הוא מלמד על מידע מקטיגוריות אחרות של מידע רגיש המנויות בסעיף. למשל, ציון שאדם נמצא במועדון ריקודים בערב שישי עשוי ללמד על אמונתו הדתית או השקפת עולמו, ועל כן יחשב כנכלל בקטגוריה זו.

---

[158] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[159] פרוטוקול מס' 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ד בטבת התשפ"ד (26 בדצמבר 2023), עמ' 27–39; פרוטוקול מס' 223 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ח בטבת התשפ"ד (9 בינואר 2024), עמ' 3–7.

[160] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[161] פרוטוקול מס' 203 מישיבת ועדת החוקה, חוק ומשפט, יום שני, ו' בטבת התשפ"ד (18 בדצמבר 2023), עמ' 42, דברי יו"ר ועדת חוקה, ח"כ רוטמן.

[162] סעיף 1 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007 (להלן: "חוק נתוני תקשורת").

[163] פרוטוקול מס' 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ד בטבת התשפ"ד (26 בדצמבר 2023), עמ' 8–16.

(10) מידע אישי על נתוני שכר של אדם ועל פעילותו הפיננסית[164]

קטגוריה זו מצומצמת רק למידע על אודות נתוני שכר ופעילות פיננסית, שנאסף או מופק על ידי שחקנים, מוסדיים ושאינם מוסדיים, מהשוק הפיננסי. לדוגמה, מוסד אקדמי המעניק זכאות למלגה על בסיס מצבו הפיננסי של אדם, או עסקים המספקים שירות לניהול יעיל וכלכלי של משק הבית.[165]

לפיכך, אם מאגר מידע של מפלגה או יישומון בחירות כולל מידע אודות נתוני שכר של בעל זכות בחירה או פעילות פיננסית שלו, הוא ייכנס לקטגוריה הזאת. מנגד, אמירות כלליות לפיהן פלוני "מרוויח כמו בהייטק", עונד שעון רולקס, "טחון", בונה ארמון או רוכש מכוניות פאר, לא יכנסו לגדר קטגוריה זו.

3. מאגר מידע

העובדה שמפלגה מחזיקה בנתונים הנכנסים תחת הגדרת "מידע אישי",[166] אינה מספיקה כשלעצמה לשם החלת הוראות חוק הגנת הפרטיות על עיבוד המידע, אלא על המידע להיות מאוגד ב"מאגר מידע".[167] תיקון 13 דייק וצמצם במידה מסוימת את הגדרת "מאגר מידע" וכעת הוא מוגדר כך:

> "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;"[168]

לפי הגדרה זו, אוסף פרטי מידע לשימוש אישי בלבד לא יחשב מאגר מידע. בנוסף, אוסף הכולל רק שם מען ודרכי תקשורת על 100,000 נושאי מידע ומטה, שכשלעצמו לא ניתן להפיק ממנו נתונים שיחשבו כ"מידע אישי", ושלבעליו אין אוסף אחר הכולל פרטי מידע על אותם נושאי מידע, יוחרג מהגדרת מידע אישי.

כל מפלגה מקבלת לידיה עם תחילת תקופת הבחירות את המידע הפנקס שכולל את מספרי הזיהוי של כל אחד מבעלי זכות הבחירה בישראל והיקפו עולה על 100,000 איש. לכן, כל מפלגה מחזיקה במאגר מידע. גם אם מפלגה תפצל את מידע הפנקס לאוספים נפרדים הכוללים רק שם, מען ודרכי תקשורת על עד 100,000 בעלי זכות בחירה כל אחד, היא תתקשה להימלט מהגדרת "מאגר מידע". זאת משום שהחריג להגדרת "מאגר מידע" מחייב שלא יהיה אצל בעל האוסף או אצל תאגיד בשליטתו אוסף נוסף הכולל פרטי מידע אישי אחרים ביחס לאותם נושאי מידע. סביר שבידי מפלגה קיימים פרטי מידע נוספים על

---

[164] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[165] פרוטוקול מס' 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ד בטבת התשפ"ד (26 בדצמבר 2023), עמ' 44–49.

[166] ראו דיון בהגדרת "מידע אישי" בסעיף 0 לעיל.

[167] לביקורת על הותרת המונח "מאגר מידע" כשער כניסה לתחולת הוראות חוק הגנת הפרטיות ראו רחל ארידור הרשקוביץ **תיקון 13 לחוק הגנת הפרטיות: משמעות התיקון, השלכותיו וחסרונותיו** (הצעה לסדר 62, המכון הישראלי לדמוקרטיה, בהכנה).

[168] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

בעלי זכות הבחירה בישראל, כגון מידת תמיכתם במפלגה או האם נדרשים לסיוע בהגעה לקלפי ביום הבחירות.

באשר למפעיל יישומון בחירות, הרי שלכאורה אם יחזיק אך ורק באוספי מידע הכוללים רק שם, מען ודרכי תקשורת על עד 100,000 בעלי זכות בחירה כל אחד, הוא עשוי להימלט מהגדרת "מאגר מידע". אולם, מהמידע שפורסם בציבור באשר ליישומון אלקטור, נראה שהחזקת אוספי מידע דלים שכאלו אינה סבירה, שכן מפעיל יישומון הבחירות לא יוכל לסייע באמצעותם במיקוד והמרצת תעמולת הבחירות למפלגה ששוכרת את שירותיו. זאת ועוד, גם אם מפלגה אחת מסתפקת במאגר מידע קטן, אם מפעיל יישומון הבחירות מספק שירותים למפלגות נוספות הרי שהוא ממילא מחזיק מאגרי מידע הכוללים פרטי מידע נוספים, על אותם נושאי מידע, קרי כל בעלי זכות הבחירה בישראל. משום כך, נראה שגם מפלגה וגם מפעיל יישומון בחירות מחזיקים במאגרי מידע.

4. עיבוד ושימוש במידע

"עיבוד" ו"שימוש" במידע הם מונחים חלופיים המתארים רשימה רחבה ופתוחה של פעולות, בדומה למונח עיבוד (processing) ב־GDPR.[169] "עיבוד", "שימוש" משמעם כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו.[170] בשל רוחב ההגדרה נקודת המוצא היא שכל פעולה הנעשית במידע אישי תחשב כשימוש או עיבוד.

5. סיכום

כל מפלגה ורשימת מועמדים, מקבלת לידיה עם תחילת תקופת הבחירות את מידע הפנקס, הכולל שם, מען ומספק זהות של בעלי זכות הבחירה בישראל. על בסיס מידע הפנקס מוסיפה המפלגה שכבות נתונים נוספים. מאחר ומידע אישי מוגדר בהרחבה, הרי שמידע הפנקס ושכבות הנתונים הנוספות – נופלים לגדר הגדרת מידע אישי. יתרה מכך, פעמים רבות אף מדובר במידע בעל רגישות מיוחדת. למשל, מידע על דעה פוליטית או על מצב רפואי. אוסף המידע האישי והמידע בעל הרגישות המיוחדת שבשליטת המפלגה ומועבר על ידה למפעילי יישומוני בחירות הוא מאגר מידע כהגדרתו בחוק. הפעולות שמבצעים המפלגות ומפעילי יישומוני בחירות במידע אישי ובמידע בעל רגישות מיוחדת שבמאגרי המידע הן עיבוד או שימוש.

[169] ראו סעיף 4(2) ל-GDPR, לעיל הערה 5.

[170] סעיף 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

פרק רביעי
בעלי תפקידים וחובותיהם

1. בעלי תפקידים רלוונטיים

עיבוד נתונים המהווים מידע אישי ב"מאגר מידע", מקים חבות. על מנת להבין מה נכלל בגדר אותה חבות, יש להבין את סוג התפקידים לפי החוק שממלאות מפלגות, רשימות מועמדים ומפעילי יישומוני בחירות.

1.1. בעל שליטה במאגר מידע

בקביעת הפרת חוק הגנת הפרטיות בפרשת "אלקטור", שניתנה עוד לפני תיקון 13, דחתה הרשות להגנת הפרטיות את טענותיהן של מפלגות הליכוד וישראל ביתנו בדבר היותה של המדינה "בעלת המאגר" ביחס למידע הפנקס. הטענה התבססה על כך שהמפלגה היא הבעלים אך ורק של המידע המטויב, המהווה אחוז קטן של מידע הפנקס,[171] או מחזיקה בזכות שימוש מוגבלת במידע הפנקס.[172] הרשות להגנת הפרטיות קבעה שאף שהמדינה היא בעלת מאגר מרשם האוכלוסין, ממנו נגזר מידע הפנקס שנמסר למפלגות, הרי שמרגע מסירת מידע הפנקס למפלגה, נוצר מאגר מידע חדש שהמפלגה, ולא המדינה, היא שמחליטה האם ובאיזה אופן להשתמש בו לקידום מטרותיה הפוליטיות. העובדה שהשימוש במידע הפנקס מוגבל לפי חוק הבחירות, אינה גורעת מאחריות המפלגה כבעלת המאגר.[173]

לפי תיקון 13 "בעל שליטה" במאגר מידע, הוא "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".[174] בעל השליטה במאגר המידע קובע רק את מטרות העיבוד, כאשר האמצעים לעיבוד המידע נקבעים על פי רוב על ידי מי שמעבד בפועל את המידע ונקרא ה"מחזיק".[175]

בהתאם להגדרה זו על אף שמפלגות מקבלות את מידע הפנקס מכוח חוק הבחירות לכנסת[176] המגביל את השימושים לצורכי התמודדות בבחירות וקשר עם ציבור הבוחרים,[177] כלומר, קובע מסגרת מטרות חוקית לשימוש במידע פנקס, עדיין כל מפלגה יכולה לקבוע מטרות שימוש כרצונה בתוך מסגרת זו. לכן, המפלגה היא בעלת השליטה במאגר המידע, בין אם מדובר רק במאגר מידע אחד הכולל את מידע הפנקס והמידע המטוייב המוסף על ידה, או בשני מאגרי מידע נפרדים, האחד כולל רק את מידע הפנקס, והשני כולל

---

[171] ראו למשל, מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27/01/2021), סעיף 9.1.

[172] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27/01/2021), סעיף 9.6, בעמ' 4.

[173] ראו דיון בטקסט הנלווה לה"ש 124–126.

[174] סעיף 2 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[175] ראו הדיון בטקסט הנלווה לה"ש 178–181 להלן.

[176] סעיף 39(ב) לחוק הבחירות לכנסת, ה"ש 75 לעיל.

[177] סעיף 39(ג) לחוק הבחירות לכנסת, שם.

מידע מטוייב וחלקים ממידע הפנקס. לחילופין, המפלגות הן גוף שהוסמך בחיקוק (חוק הבחירות) לעבד מידע במאגר מידע, ולכן עונות גם כן להגדרת בעל שליטה במאגר המידע.

1.2. "מחזיק"

בהחלטה לגבי ההפרה בפרשת אלקטור קבעה הרשות להגנת הפרטיות שאלקטור היא "מחזיק" ושאין בעובדה שמאגר המידע היה מצוי בידי אלקטור לתקופה קצרה ולא כדרך קבע, כדי לשנות את קביעה זו. זאת, משום שבתקופה זו חברת אלקטור הייתה רשאית לבצע פעולות עיבוד מידע במאגר בהתאם לדרישת המפלגה.[178] קביעה זו נותרת בעינה גם לפי ההגדרה המעודכנת למונח "מחזיק" בתיקון 13. גם לאחר תיקון 13 מבחין חוק הגנת הפרטיות בין בעל שליטה במאגר מידע לבין מי ש"מחזיק בו", המוגדר כגורם חיצוני לבעל השליטה במאגר המידע, המבצע במידע שבמאגר המידע פעולות עיבוד בהתאם למטרות העיבוד שקובע בעל השליטה. אולם, אופן העיבוד עצמו והאמצעים עמם יעובד המידע נתונים לשיקול דעתו והחלטתו של המחזיק.[179] כך, למשל, משרד עורכי דין הוא בעל השליטה במידע האישי אודות עובדיו. אולם, אם הוא מעביר לחברה המספקת שירותי ניהול שכר מידע אישי אודות עובדיו , החברה המספקת את שירותי ניהול השכר היא ה"מחזיק" במאגר המידע. לעומת זאת, חשב השכר העובד במשרד עורכי דין לא יחשב למחזיק, שכן הוא אינו גורם חיצוני לבעל השליטה (משרד עורכי הדין). בנוסף, לפי הגדרת "מחזיק" שתוקנה בתיקון 13 אין צורך בהחזקת עותק פיזי של מאגר המידע על מנת להיחשב כמחזיק[180] ולא נדרשת הוכחת התקשרות בין בעל השליטה למחזיק.[181]

לפיכך, כל גורם חיצוני למפלגה, כלומר כל מי שאינו עובד המפלגה, שהמפלגה העבירה לו את מאגר המידע לשם עיבודו עבורה, יחשב כ"מחזיק". פרק הזמן של עיבוד המידע, אופן ההתקשרות בין המפלגה לאותו גורם, או השאלה מי קובע את אמצעי העיבוד – אינם רלוונטיים לכך שמדובר ב"מחזיק".

1.3. מנהל מאגר

מנהל מאגר לפי תיקון 13 הוא "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."[182]

---

[178] ראו למשל, מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27/01/2021), סעיפים 10.3, 10.5 ו־10.11, בעמ' 13 ; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27/01/2021), סעיף 10.4 בעמ' 10 ; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – חברת אלקטור תוכנה בע"מ** (27.1.2021), סעיפים 9.4 ו־10.5, בעמ' 4 ו־11.

[179] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[180] 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"), דברי ההסבר בעמ' 424-423.

[181] זאת בניגוד לדרישת ההתקשרות שהופיעה בהגדרת "מחזיק" בהצעת החוק הממשלתית, שם, סעיף 2(1):

> "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;"

[182] סעיף 3 בחוק הגנת הפרטיות, לעיל ה"ש 9.

הואיל ומפלגה או מפעיל יישומון בחירות אינם "גוף ציבורי" כהגדרתו בסעיף 23 לחוק הגנת הפרטיות או בצו הגנת הפרטיות (קביעת גופים ציבוריים), תשמ"ו – 1986 (להלן: "צו קביעת גופים ציבוריים"), לאחר תיקון 13 אין משמעות לתפקיד מנהל מאגר במפלגה או במפעיל יישומון בחירות.

פרק חמישי

החובות המרכזיות המוטלות על מפלגות כבעלות שליטה ועל מפעילי יישומוני בחירות כמחזיקים

חוק הגנת הפרטיות מטיל מספר חובות על בעל שליטה במאגר מידע ועל מחזיק שנסקור אותן להלן.

1. חובת רישום מאגר מידע

תיקון 13 צמצם משמעותית את חובת רישום מאגרי מידע שהייתה נהוגה קודם לכן. חובת הרישום בסעיף 8א לחוק מוטלת עתה על גופים ציבוריים, אלא אם כן מאגר המידע כולל מידע אישי על עובדי הגוף הציבורי בלבד ; ועל בעלי שליטה המעבדים מידע אישי לשם מכירתו לצדדים שלישיים כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, דהיינו סוחרי מידע, ויש במאגר מידע אישי על יותר מ־10,000 בני אדם.[183]

חובת רישום מוטלת רק על בעל שליטה במאגר מידע, ועל כן אינה רלבנטית ביחס למפעיל יישומון בחירות. באשר לחבותה של מפלגה, כבעלת השליטה במאגר המידע, ברישום מאגר מידע, נדרשת בחינה מעמיקה. על מפלגה לעבד את המידע במאגר המידע בהתאם לסעיף 39(ג) לחוק הבחירות, לפיו היא מתחייבת שהשימוש שתעשה במידע הפנקס, לרבות העברתו לאחר, יוגבל רק "לצורכי התמודדותה בבחירות ולצורכי קשר עם ציבור הבוחרים". כלומר, מטרתו העיקרית של איסוף המידע לא יכולה להיות לשם מסירתו לאחר כדרך עיסוק או בתמורה. העברת המידע מהמפלגה למפעיל יישומון בחירות, היא במסגרת יחסי בעל שליטה ומחזיק ואינה מהווה מסירה כדרך עיסוק או בתמורה. יתרה מכך, מפלגה שתמסור את מידע הפנקס או נגזרותיו לאחר כדרך עיסוק או בתמורה עשויה להפר את הוראות חוק הבחירות.

עם זאת, ניסוח חובת הרישום בסעיף 8א(א)(1)(א) מעורפל מעט וקובע כי חובה זו תחול כאשר מטרתו העיקרית של מאגר המידע "היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר". "דיוור ישיר" מוגדר כ"פנייה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר המידע".[184] לפיכך, וכפי שהבהירה הרשות להגנת הפרטיות בהבהרות שפרסמה לפני הבחירות לכנסת ה־23 וה־24,[185] מסרי תעמולה חישובית מותאמים אישית למאפייניו של בוחר עשויים להיחשב כדיוור ישיר. אולם חובת הרישום חלה רק אם מטרתו העיקרית של מאגר המידע היא "**שירותי** דיוור ישיר". אלו מוגדרים כ"מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא;".[186] מפלגה מבצעת דיוור ישיר בעצמה או באמצעות מפעיל יישומון בחירות, אך אינה מספקת **שירותי** דיוור ישיר לאחרים. משום כך, נראה לנו שלא חלה עליה חובת הרישום מטעם זה.

---

[183] סעיף 8א(א)(1) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[184] הגדרת "דיוור ישיר" בסעיף 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

[185] הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 123, סעיפים 13-16 ; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, לעיל ה"ש 123, בסעיף 17.6.

[186] סעיף 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

באשר לשאלה האם חלה על מפלגה חובת רישום כגוף ציבורי, מפלגה אינה "גוף ציבורי" כהגדרתו בפסקה (1) להגדרת "גוף ציבורי שבסעיף 23 לחוק הגנת הפרטיות.[187] אולם, מפלגה נחשבת כגוף דו מהותי, שכן פעולותיה עשויות להיות בחלקן בעלות אופי פרטי ובחלקן בעלות אופי שלטוני ציבורי. כך לצד עקרונות מהמשפט הפרטי העלולים לכל על ענייניה ופעולותיה של המפלגה, עשויים לחול עליה גם כללים וחובות מכוח המשפט הציבורי.[188]

בית המשפט העליון הכיר בכך שפעולותיה של מפלגה בכל הקשור לענייניה הפרטיים, לרבות פעולותיהם של טריבונלים הפועלים מטעמה, הינם נושאים פרטיים בהם המפלגה צריכה להנות מחופש פעולה יחסי. זאת משום שלכל מפלגה מאפיינים פוליטיים ברורים ושונים וכל אחת פועלת לקידום ערכים ועקרונות בהתאם לצו מצפונם ואמונתן של חבריה. במובן זה פעולותיה של מפלגה הן אמצעי חשוב למימושן של זכויות יסוד של חבריה ותומכיה, בעיקר חופש ההתאגדות הפוליטי, חופש הביטוי והזכות לבחור ולהיבחר.[189]

עם זאת, בפרשת **ערוץ 14** קבע בית המשפט העליון שלהחלטתה של מפלגת מרצ שלא להתיר לכתבי ערוץ 14 לסקר את פעילותה במטה המפלגה ביום הבחירות לכנסת ה־25 מאפיינים ציבוריים מובהקים, התומכים בהטלת חובות מהמשפט הציבורי על המפלגה בראשם החובה לנהוג בשוויון ולכבד את חופש העיתונות. זאת משום שסיקור אירוע הבחירות המרכזי במטה המפלגה משקף מפגש בין חופש הביטוי, חופש העיתונות וזכות הציבור לדעת. חסימת כניסתו של כלי תקשורת מסוים אחד בלבד לאירוע בעל גוון ציבורי ניכר שקולה לפגיעה ב"גרעין הקשה" של חופש העיתונות. כאשר מנגד חיובה של המפלגה לכבד את חופש הגישה של כלל אמצעי התקשורת לסיקור כמוה כהבטחת חופש הגישה למקומות שבהם מתקיימת פעילות ציבורית, גם אם המקומות הם בבעלות פרטית, אינה מהווה פגיעה משמעותית בחופש הפעולה או בחופש הביטוי של המפלגה. זאת לעומת כיבוד החלטותיה של מפלגה שהן בעלות מאפיינים פרטיים יותר שלא לקיים ראיונות יזומים או למסור מידע באופן העלול להתפרש כתמיכת המפלגה בערוץ תקשורת מסוים.[190]

עם זאת, אין בפסיקה או בחקיקה קביעות מהותית קשיחות באשר לשאלה אילו נורמות מהמשפט הציבורי חלות על המפלגה. בית המשפט העליון הגביל את פסיקתו בפרשת **ערוץ 14** לנסיבות המקרה שהובא בפניו – הבטחת גישה של כלל אמצעי התקשורת לזירה הציבורית.[191]

לפיכך, בבחינת תחולת חובת הרישום על מפלגה, מכוח היותה גוף דו־מהותי, יש לבחון (1) מהי תכלית הטלת חובת הרישום על גוף ציבורי והאם היא תקפה גם ביחס לעיבוד מידע אישי על ידי מפלגה ו־(2) האם עיבוד מידע אישי על בוחרים במאגר מידע על ידי מפלגה הוא בעל אופי ציבורי.

באשר לתכלית הטלת חובת הרישום על גופים ציבוריים, הסבירה ועדת החוקה במהלך הדיונים בנושא בתיקון 13, כי המדינה אוספת בכפייה מידע אישי רב על אזרחיה ועל כן כחלק מעקרון חופש המידע עליה

---

[187] סעיף 23(1) לחוק הגנת הפרטיות, לעיל ה"ש 9: "משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין."

[188] בג"ץ 7232/22 **ערוץ יהודי ישראלי בע"מ נ' מרצ – השמאל של ישראל בראשות זהבה גלאון ואח'**, (31.10.2022), סעיף 19 לפסק דינה של השופט ברק ארז.

[189] שם, סעיף 20 לפסק דינה של השופט ברק ארז.

[190] שם, סעיפים 22-24 לפסק דינה של השופט ברק ארז.

[191] שם, סעיף 25, 27 לפסק דינה של השופט ברק ארז.

לספק לאזרח מידע מדויק על המידע שהיא מחזיקה אודותיו ולאפשר לו לממש את זכויותיו ביחס אל מידע זה.[192]

באשר למידע האישי שיש בידי המפלגה, החזקתה של מפלגה במידע הפנקס ידועה ומוסדרת בחוק הבחירות, לרבות זכותו של בוחר לדרוש את הסרת פרטיו ממידע הפנקס באינטרנט, או לדרוש את תיקונו.[193] מידע אישי נוסף שמפלגה מוסיפה על גבי מידע הפנקס הוא מידע שהיא אוספת ישירות מהבוחרים, באמצעות צדדים שלישיים או סוחרי מידע או באמצעות מערכות בינה מלאכותית המפיקות מידע מוסק. בהקשר למידע זה, לא ברור שמתקיימת תכלית הטלת חובת הרישום על גופים ציבוריים, שכן אין מדובר במידע הנאסף בכפייה מהאזרחים. זאת ועוד, עיבוד המידע האישי לא בהכרח מבטא מאפיינים ציבוריים בולטים, אלא דווקא ניתן להקבילו להחלטותיה של מפלגה באיזה ערוץ תקשורת להתראיין על מנת להגביר את המסרים העשויים להוביל להגברת התמיכה בה.

כמו כן, תחולת חובת הרישום הוגבלה בחוק הגנת הפרטיות רק לגופים המפורטים בפסקה (1) להגדרת "גוף ציבורי" בסעיף 23 לחוק הגנת הפרטיות. כלומר, רק ל"משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין;". לעומת זאת, גופים ששר המשפטים קבע בצו שהם גופים ציבוריים,[194] מוחרגים במפורש מתחולת חובת הרישום.[195] החרגה זו עשויה ללמד דווקא על רצונות של המחוקק להימנע מהרחבת יתר של חובת הרישום.

אומנם, אין קביעות נורמטיביות ברורות באשר לחובות מן המשפט הציבורי שיש להחיל על גוף דו־מהותי והנושא אמור להיקבע בהתאם לנסיבות כל מקרה,[196] אולם העובדה שלבד מהמידע המופיע במידע הפנקס, המידע האישי במאגר המידע שבידי המפלגה לא נאסף על ידה בכפייה, הימנעותו של המחוקק מהרחבת חובת הרישום גם על גופים ששר המשפטים יכריז עליהם כגופים ציבוריים, בשילוב העובדה שחובת הרישום אינה מספקת הגנה מהותית לזכות לפרטיות,[197] תומכים לדעתנו באי החלת חובת הרישום על מפלגות.

2. חובת הודעה לרשות להגנת הפרטיות

בתיקון 13 התווספה חובת מתן הודעה לרשות לפרטיות. חובה זו מוטלת על בעל שליטה שבמאגר המידע שברשותו יש מידע בעל רגישות מיוחדת על 100,000 נושאי מידע או יותר. על ההודעה שנמסרת לרשות לכלול את פרטי בעל השליטה ודרכי ההתקשרות עמו, מידע על זהותו של הממונה על הגנת הפרטיות בארגון ודרכי ההתקשרות עמו, והעתק ממסמך הגדרות המאגר. המדובר במסמך הנדרש מבעל השליטה לפי תקנות אבטחת מידע. על בעל שליטה לפרט במסמך הגדרות מאגר נושאים שונים, כגון מטרות השימוש במאגר המידע, סוגי המידע שבמאגר, האם מבוצע עיבוד מידע באמצעות אחר, מהם סיכוני

---

[192] שם, בעמ' 107, 108, דברי יו"ר הוועדה, ח"כ רוטמן.

[193] סעיפים 26(ה), 40(א) לחוק הבחירות, לעיל ה"ש 75.

[194] סעיף 23(2) לחוק הגנת הפרטיות, לעיל ה"ש 9: "גוף ששר המשפטים קבע בצו, באישור ועדת החוקה, ובלבד שבצו ייקבעו סוגי המידע והידיעות שהגוף יהיה רשאי למסור ולקבל."

[195] סעיף 8א(א)(1)(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[196] פרשת **ערוץ 14**, לעיל ה"ש 188, סעיף 25, 27 לפסק דינה של השופט ברק ארז.

[197] 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).

האבטחה למאגר וכיצד הוא מתמודד עמם. כן עליו לשמור את המסמך אצלו ולעדכנו מידי שנה לפחות.[198] בעל השליטה נדרש להעביר את מסמך מטרות המאגר לעיונה של הרשות להגנת הפרטיות כחלק מחובת ההודעה, במטרה לספק לה את המידע הנחוץ לה להערכת חוקיותו של מאגר המידע ולפעולות הפיקוח והאכיפה המינהלית הנדרשות ביחס אליו. על בעל השליטה במאגר המידע לעדכן את הרשות בדבר שינוי באחד מהפרטים הללו או על שינוי במסמך הגדרות המאגר.[199]

מאחר ומידע הפנקס כולל מידע אישי על כל בעלי זכות הבחירה בישראל, כלומר מעל 100,000 אנשים ומעלה, ועליו מוספים פרטי מידע אישי נוספים שחלקם עשוי להיות מידע בעל רגישות מיוחדת (למשל, מידע על דעה פוליטית, השקפת עולם או נטייה מינית), חובת ההודעה לרשות חלה על מפלגות כבעלות שליטה.

3. חובת אבטחת מידע וחובת מינוי ממונה אבטחת מידע

חובת אבטחת מידע המוטלת על בעל שליטה ומחזיק להגן על מידע אישי המצוי ברשותם מפני גישה, שימוש או חשיפה בלתי מורשים, אינה חדשה.בפרשת אלקטור, כפרו מפלגת הליכוד וחברת אלקטור בקביעה כי הפרו חובה זו. מפלגת הליכוד טענה ש"לא קיימת מערכת שהיא חסינה לאירועי אבטחה וכי העולם הרשתי אינו חסין מפני אירועים של אבטחת מידע."[200] אלקטור מצידה טענה שמאחר ואין אפשרות לחסינות מלאה מאירועי אבטחה בעולם התוכנה, "המדד הנכון לבחינת רמת האבטחה ... הינו המהירות שבה מאותרת פרצת אבטחה ומנוטרלת".[201] הרשות להגנת הפרטיות דחתה טענות אלו וקבעה שגם אם "לא ניתן להבטיח כי העולם הרשתי יהיה חסין לחלוטין מפני אירועים של דליפת מידע או פריצה בלתי מורשית למערכות", על בעל המאגר והמחזיק "לנקוט באמצעים מקובלים להגנה מקסימלית על המידע".[202] בנוסף קבעה הרשות שמפלגה, כבעלת שליטה במאגר מידע, נושאת באחריות גם על התנהלותו של המחזיק, דהיינו אלקטור, בכל הקשור לעיבוד מידע במאגר מידע, ואינה יכולה להסתפק בהצהרות המחזיק כי הוא עומד בהוראות החוק והתקנות. כן אין בעובדה שאלקטור הייתה בפיקוח הרשות להגנת הפרטיות בעבר, בשנת 2018, כדי להעניק אישוש מספק לרמת אבטחת המידע הנוכחית של מערכותיה. לפי הרשות להגנת הפרטיות, על מנת לעמוד בחובות אבטחת מידע המוטלות על בעל מאגר מידע, לרבות אלו הקבועות בתקנות אבטחת מידע, על בעל מאגר האחריות לבחון את סיכוני אבטחת המידע הכרוכים בהתקשרות עם המחזיק ולנקוט בעצמו את אמצעי הבקרה והפיקוח על ציות המחזיק לחוק הגנת הפרטיות ולתקנות מכוחו לאורך כל ההתקשרות ביניהם.[203]

---

[198] תקנה 2(א)(1) לתקנות אבטחת מידע, ה"ש 110 לעיל; פרוטוקול מס' 223, לעיל ה"ש 159, עמ' 77.

[199] ראו סעיף 8א(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[200] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 9.14, בעמ' 6.

[201] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – חברת אלקטור תוכנה בע"מ** (27.1.2021), סעיף 9.7.4 בעמ' 6.

[202] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 10.10, בעמ' 13 ; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – חברת אלקטור תוכנה בע"מ** (27.1.2021), סעיף 10.8 בעמ' 13.

[203] ראו למשל, מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27.1.2021), סעיף 10.12 בעמ' 13 ; מחלקת האכיפה הרשות להגנת

תיקון 13 הוסיף לחובת אבטחת מידע מספר הבהרות, ביניהן ביטול סעיף 17א לחוק הגנת הפרטיות שחייב מחזיק של מאגר מידע של בעלים שונים לעקוב אחר מורשי הגישה למאגר. זאת בנימוק שהנושא מוסדר בתקנות אבטחת מידע.[204]

בנוסף, בתיקון 13 עודכנה החובה למנות ממונה אבטחת מידע והיא חלה, בין השאר, על בעל שליטה ומחזיק בחמישה מאגרי מידע החייבים ברישום או בהודעה לרשות להגנת הפרטיות.[205]

כבעלת שליטה במאגר מידע מפלגה אחראית לאבטחת המידע שבמאגר המידע שבשליטתה, ומפעיל יישומון בחירות כמחזיק אחראי לאבטחת המידע במאגרי המידע שבחזקתו.[206] בנוסף, מפלגה תהיה חייבת למנות ממונה אבטחת מידע רק אם תחזיק חמישה מאגרי מידע (למשל אם תפצל את מאגר המידע שברשותה), שכל אחד מהם מקים את חובת ההודעה לרשות. כלומר, כל אחד מהחמישה יכלול מידע בעל רגישות מיוחדת על 100,000 איש לפחות.[207]

מפעיל יישומון בחירות המחזיק בחמישה מאגרי מידע החייבים בהודעה לרשות להגנת הפרטיות,[208] בין אם מאגרים אלו הם של אותה מפלגה או של מפלגות שונות, חייב במינוי ממונה אבטחת מידע.

4. חובת מינוי ממונה הגנת פרטיות

חובת מינוי ממונה הגנת פרטיות היא חובה חדשה שהוספה בתיקון 13 וחלה על בעל שליטה במאגר מידע ועל מחזיק, בהתקיים אחד מהתנאים הקבועים בחוק:[209]

(1) בעל שליטה, 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); חובת מינוי ממונה הגנת פרטיות אינה מצומצמת רק לגופים ציבוריים מסוימים המנויים בסעיף 23(1) לחוק הגנת הפרטיות, ועל כן חלה גם על גופים ששר המשפטים יקבע בצו שהם גופים ציבוריים.[210]עובדה זו עשויה להיות רלוונטית בבחינה האם ניתן להטיל את חובת מינוי ממונה הגנת הפרטיות על מפלגה על בסיס אפיונה כגוף דו־מהותי.

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

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

הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 10.9, בעמ' 12.

[204] פרוטוקול מס' 233 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, י"א בשבט התשפ"ד (21 בינואר 2024), בעמ' 45–46.

[205] ראו סעיף 17ב בחוק הגנת הפרטיות, לעיל ה"ש 9; פרוטוקול מס' 249 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ז בשבט התשפ"ד (6 בפברואר 2024), עמ' 118-117; פרוטוקול מס' 336 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ"ז באייר התשפ"ד (04 ביוני 2024), עמ' 39-37.

[206] בהתאם להוראת סעיף 17(א) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[207] לפי סעיף 8א(ב)(1), (3) לחוק הגנת הפרטיות, לעיל ה"ש 9. ראו הדיון בסעיף 2 לעיל.

[208] לפי סעיף 8א(ב)(1), (3) לחוק הגנת הפרטיות, לעיל ה"ש 9. ראו הדיון בסעיף 2 לעיל.

[209] סעיף 17ב1(א)(1),(2) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[210] סעיף 23(2) לחוק הגנת הפרטיות, לעיל ה"ש 9.

(4) בעל שליטה במאגר מידע או מחזיק, "**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**."[211]

החוק מספק דוגמאות לבעלי שליטה או מחזיקים כאמור, למשל ספק מורשה של שירותי טלקומוניקציה, ספק שירות חיפוש מקוון או מי שפעולות אלו הן עיסוקו העיקרי. בטיוטת גילוי דעת בנושא מנתה הרשות להגנת הפרטיות דוגמאות לנסיבות של "ניטור שוטף ושיטתי" של בני אדם. למשל, התחקות אחר פעילות נושא המידע באתרי אינטרנט ויישומונים, יישומוני מעקב אחר מיקום פיזי או נתוני בריאות, מכשירי אינטרנט של דברים (IoT) כגון כלי רכב חשמליים, מאגר צילומים של מצלמות מעקב וספקי אינטרנט.[212] לעומת זאת, עסק קטן שמנטר רק את עובדיו באופן פנימי ולא שוטף עשוי שלא להיות חייב במינוי ממונה הגנת פרטיות.

(5) בעל שליטה או מחזיק "ש**עיסוקו העיקרי** כולל עיבוד מידע בעל רגישות מיוחדת ב**היקף ניכר**".

החוק מספק מספר דוגמאות לבעל שליטה או מחזיק העונים לגדר תיאור זה, כמו תאגיד בנקאי, חברת ביטוח, בית חולים וקופת חולים.[213] בטיוטת גילוי דעת של הרשות לפרטיות הובהר שהכוונה היא לגופים שעיבוד המידע בעל הרגישות המיוחדת בהיקף ניכר הוא חלק מרכזי בהגשמת המטרות הארגוניות או העסקיות שלהם, או חלק אינהרנטי מפעילות הליבה של הארגון, אף אם אינו חיוני להגשמתה. עם זאת, כאשר 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", אין מדובר בארגון שזהו עיסוקו העיקרי.[214]

החוק מונה גם רשימה פתוחה של קריטריונים לפיהם ניתן לקבוע האם עיבוד המידע נעשה ב"היקף ניכר": מספר נושאי המידע, שיעור נושאי מידע באוכלוסייה מסוימת, היקף המידע, כמותו, טווח סוגי המידע המעובד, משך פעולת העיבוד ותדירותה, משך שמירת המידע והתחום הגיאוגרפי של פעולת העיבוד.[215] הרשות להגנת הפרטיות הבהירה בטיוטת גילוי הדעת שאין הכרח שכל הקריטריונים יתקיימו במצטבר כדי להכיר בכך שעיבוד המידע עולה כדי עיבוד מידע בהיקף ניכר.[216]

הוראות החוק עוסקות גם בכישורים הנדרשים לשם מינוי ממונה הגנת פרטיות ובהגדרת תפקידיו, מתוך התפיסה שביצוע ראוי של תפקידיו של ממונה הגנת הפרטיות היא אינטרס של בעל השליטה או המחזיק. תפקיד הממונה הוא להבטיח ציות להוראות חוק הגנת הפרטיות וכן לפעול להגנה על הזכות לפרטיות במובנה הרחב.[217] ממונה נדרש להחזיק בידע בדיני הגנת הפרטיות בישראל, לצד הבנה הולמת בטכנולוגיה

---

[211] סעיף 17ב1(א)(3) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[212] 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.

[213] סעיף 17ב1(א)(4) לחוק הגנת הפרטיות, לעיל ה"ש 9; פרוטוקול מס' 336, לעיל ה"ש 205, עמ' 6–15; פרוטוקול מס' 351 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, י"ז בסיון התשפ"ד (23 ביוני 2024), עמ' 36–54.

[214] גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 212, בסעיף 9.6. פרשנות זו עולה בקנה אחד גם עם הפרשנות האירופית בנושא. ראו Article 29 Data Prot. Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017).

[215] סעיף 17ב1(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[216] גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 212, בסעיף 9.10.

[217] סעיף 17ב2(א) לחוק הגנת הפרטיות, לעיל ה"ש 9; פרוטוקול מס' 336, לעיל ה"ש 205, עמ' 23–26.

ובאבטחת מידע, וכן בהיכרות עם תחומי הפעילות של הגוף בו משמש כממונה. הכל בהתאם לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו באותו ארגון. הרשות להגנת הפרטיות הוסיפה כי נכון לדרוש גם ניסיון משמעותי וכן הכשרה בסיסית בתחום.[218]

החוק קובע כי יש לספק לממונה את התנאים והמשאבים הדרושים למילוי נאות של תפקידו ולוודא שהוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות. [219] במטרה להבטיח שיהיה בעל תפקיד מהותי. הממונה מדווח ישירות למנכ"ל בעל השליטה או המחזיק, או לעובד הכפוף לו ישירות, על מנת לוודא שניתן קשב ראוי להערותיו של הממונה. הרשות להגנת הפרטיות קבעה שיש להתייחס לחוות דעתו של ממונה על הגנת הפרטיות בארגון כאל מי שיש חובה לפי חוק להיוועץ עמו, כלומר להתייחס לדעתו בכובד ראש, ובמידה שמוחלט שלא לפי חוות דעתו – לנמק את הסיבות לכך.[220]

החוק גם אוסר על הממונה למלא תפקיד נוסף בארגון או להיות כפוף לנושא משרה בארגון, אם מילוי אלה עלולים להעמידו בחשש לניגוד עניינים.[221] הרשות להגנת הפרטיות הבהירה שתפקידים הכוללים "את הסמכות או האחריות לקבוע מדיניות בעניין עיבוד המידע האישי בארגון, לרבות קביעת מטרות העיבוד וקבלת החלטות מהותיות לגבי שיטות ואמצעי העיבוד" הם בהכרח תפקידים היוצרים ניגוד עניינים כזה. בנוסף, מציעה הרשות לקבוע כלל אצבע לפיו תפקידים בכירים כגון מנהל שיווק, מנהל לקוחות, מנהל כספים, מנהל מערכות מידע או מנהל טכנולוגיות ראשי הם תפקידים היוצרים ניגוד עניינים מול תפקיד הממונה.[222]

לצד התנאים הקבועים בחוק הגנת הפרטיות למינוי ממונה הגנת הפרטיות המליצה הרשות להגנת הפרטיות בטיוטת גילוי הדעת למנות ממונה באופן וולנטרי גם כאשר התנאים למינוי לא מתקיימים. זאת משום שמינוי צפוי לשפר את הגנת הפרטיות והציות לחוק בארגון.[223]

מבחינת מפלגה, היא אינה גוף ציבורי או סוחר מידע, וכן אינה אוספת מידע אישי לצורך מתן שירותי דיוור ישיר, אף שהיא בהחלט מבצעת דיוור ישיר.[224] עם זאת, יש לבחון האם אפיונה של מפלגה כגוף דו־מהותי עשוי להקים את חובת מינוי ממונה הגנת פרטיות. אומנם, התבחינים הללו להטלת חובת מינוי ממונה הגנת הפרטיות על גוף ציבורי או סוחר מידע, נקבעו על ידי ועדת החוקה במהלך הדיונים על תיקון 13 תוך התבססות על התנאים להחלתה של חובת הרישום ומתוך רצון ליצור, לצד כללים מהותיים ומעורפלים ברוח ה־GDPR, גם כללים פורמליסטיים, שהאכיפה והפיקוח על הציות להם תהיה ברורה וקלה. עם זאת, תכליתה של חובת מינוי ממונה הגנת פרטיות בארגון היא הגברת הציות לחוק הגנת הפרטיות בקרב ארגונים מהמגזר הפרטי והציבורי ובתוך כך שיפור ההגנה על הזכות לפרטיות בישראל.[225] עיבוד מידע אישי, בעל רגישות מיוחדת, בהיקפים המבוצעים על ידי מפלגות, מעורר את החשש, שאינו

---

[218] גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 212, בסעיף 12.2.

[219] סעיף 17ב2(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[220] גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, ה"ש 212 לעיל, בסעיף 15.1.

[221] סעיף 17ב(3)(ג) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[222] גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, ה"ש 212 לעיל, בסעיף 20. עמדה זו עולה בקנה אחד עם הפרשנות שניתנה לאיסור ניגוד העניינים המוטל על ממונה על הגנת פרטיות בארגון לפי ה־GDPR. ראו Article 29 Data Prot. Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017)

[223] שם, בסעיף 9.12.

[224] ראו הדיון בטקסט הנלווה להי"ש 185–186.

[225] פרוטוקול מס' 336, לעיל ה"ש 205, בעמ' 16.

תיאורטי,[226] לפגיעה בפרטיות העשויה להוביל לפגיעה בחשאיות הבחירות ובהגינותם ובזכות לבחור. משום כך, מדובר בפעולה העשויה להיחשב כבעלת מאפיינים ציבוריים מובהקים המצדיקים את החלת חובת מינוי ממונה הגנת פרטיות על מפלגה במסגרת החלתה על גופים ציבוריים ועל בסיס אפיונה של מפלגה כגוף דו־מהותי. היעדר הגבלת החובה למינוי ממונה הגנת פרטיות אך ורק לגופים ציבוריים המנויים בסעיף 23(1) לחוק הגנת הפרטיות עשוי אף הוא לתמוך בהרחבה זו למפלגות. עם זאת, כאמור, החלת חובות על מפלגה כגוף דו־מהותי צריכה להיבחן בנסיבות כל מקרה ומקרה.[227]

לצד השאלה האם חובת מינוי ממונה הגנת פרטיות עשויה לחול על מפלגה בשל אפיונה כגוף דו־מהותי יש לבחון גם את התנאים הנוספים להטלתה. אומנם, עיסוקה העיקרי של המפלגה אינו כולל פעולות עיבוד מידע או כרוך בפעולות עיבוד מידע, שנוכח טיבן היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם. אולם, התנאי האחרון הקבוע בחוק למינוי ממונה הגנת פרטיות עשוי להיות רלוונטי למפלגה כבעלת שליטה, אם כי ההכרעה בשאלת התאמתו למפלגה אינה חד משמעית. לפי תנאי זה, בעל שליטה שעיסוק עיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר, חייב למנות ממונה הגנת פרטיות. אפשר להניח בסבירות גבוהה שמפלגה מעבדת מידע בעל רגישות מיוחדת בהיקף ניכר. אולם, נדרש גם שעיבוד זה הוא חלק מרכזי בהגשמת המטרות הארגוניות שלה. עיבוד מידע שהוא אינהרנטי לפעילות בעל השליטה יחשב לחלק מרכזי בהגשמת המטרות הארגוניות או העסקיות שלה, גם אם אינו חיוני להגשמתן. לפיכך, בבחינת נסיבות עיבוד המידע האישי על ידי מפלגות בשנים האחרונות, בהחלט יתכן שניתן לומר שהוא הפך לחלק אינהרנטי בפעולות שמפלגה נוקטת לשם התמודדות בבחירות לכנסת ולתקשורת עם ציבור הבוחרים. זאת על אף שאין מדובר בפעולה שבלתה אין, שכן מפלגה יכולה להתמודד בבחירות וליצור קשר עם ציבור הבוחרים אף מבלי לעבד מידע אישי בעל רגישות מיוחדת בהיקף ניכר אודותיהם.[228] בכל מקרה, גם אם מפלגה אינה חייבת במינוי ממנה הגנת פרטיות, מינוי כאמור יהווה שיקול מקל להפחתת העיצום או להתחשבות בהטלתו.

באשר למפעיל יישומון בחירות, הוא יחוב במינוי ממונה הגנת פרטיות אם ייקבע שמפלגה חייבת במינוי ממונה הגנת פרטיות מכורח היותה גוף דו־מהותי ועל בסיס סעיף 17ב1(א)(1) המטיל חובת מינוי על גוף ציבורי או על מחזיק במאגר מידע שבשליטת גוף ציבורי. אפשרות נוספת לחיובו של מפעיל יישומון במינוי ממונה הגנת פרטיות מבוססת על העובדה שמפעיל יישומון בחירות מעבד את מידע הפנקס ומידע מטויב, לרבות מידע בעל רגישות מיוחדת, המוסף לו. עיבוד מידע זה נעשה על ידי מפעיל היישומון בהיקף ניכר, שכן מדובר במאגרי מידע הכוללים את כל בעלי זכות הבחירה בישראל. יתרה מכך, עיבוד המידע כאמור הוא חלק מרכזי בהגשמת מטרותיו העסקיות של מפעיל יישמון בחירות, שהרי זו ליבת השירות שהוא מספק למפלגה. משום כך, סביר שמפעיל יישומון בחירות יחוב בחובה למנות ממונה הגנת פרטיות לפי החלופה הקבועה בסעיף 17ב1(א)(4) לחוק הגנת הפרטיות.

---

[226] הפרת הזכות לפרטיות כבר התרחשה במערכות בחירות בעבר כפי שמוכיחה פרשת **אלקטור**. ראו הדיון בטקסט הנלווה להע״ש 98–111.

[227] פרשת **ערוץ 14**, לעיל הע״ש 188, סעיף 25, 27 לפסק דינה של השופט ברק ארז.

[228] החלופה הקבועה בסעיף 17ב1(א)(4) לחוק הגנת הפרטיות, לעיל הע״ש 9.

פרק שישי
הגבלות ואיסורים על עיבוד המידע האישי במאגר מידע

1. הסכמה מדעת

סעיף 1 לחוק הגנת הפרטיות קובע שכל הפוגע בפרטיותו של אדם באחת מן הדרכים המנויות בסעיף 2 לחוק, בניהן שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה (סעיף 2(9)) או בילוש או התחקות אחרי אדם העלולים להטרידו (סעיף 2(1)), מבלי שהוסמך לעשות זאת בדין, נושא בנטל לשכנע באופן פוזיטיבי שהפגיעה בפרטיות נעשתה בהסכמת נושא המידע.[229]

דרישת ההסכמה חוזרת גם בסעיף 11(1) לחוק העוסק בחובת ההודעה לנושא המידע ומחייב שבעת פנייה לאדם לקבלת מידע אישי אודותיו לשם עיבודו במאגר מידע, על הפונה לציין גם האם חלה על האדם חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן מה עשויה להיות תוצאת אי ההסכמה.[230] כן נכללת דרישת ההסכמה בעקיפין בסעיף 8(ב) לחוק הגנת הפרטיות העוסק בעקרון צמידות המטרה ומחייב שעיבוד מידע אישי יעשה אך ורק בהתאם למטרת המאגר שנקבעה כדין. זאת משום שבהיעדר הסמכה בדין שימוש במידע למטרה מסוימת יכול להיעשות רק מכוחה של הסכמת נושא המידע. סעיף 8(ד)(1) האוסר על עיבוד מידע אישי במאגר מידע אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע" מתייחס לדרישת ההסכמה על דרך השלילה. האיסור מתייחס לעיבוד מידע אישי שנאסף אגב פגיעה בפרטיות ללא הסכמה תקפה ובהיעדר הסמכה בדין.[231]

סעיף 3 לחוק הגנת הפרטיות מגדיר "הסכמה" תקפה כהסכמה המתקבלת מדעת, מרצון חופשי, במפורש או מכללא.

"מדעת"

הדרישה שההסכמה תהיה מדעת נועדה להבטיח שלנושא המידע הייתה בחירה אמיתית ואוטונומית. היא נדרשת בין אם ההסכמה ניתנת במפורש ובין אם היא ניתנת מכללא. על מנת לעמוד בדרישה כי ההסכמה תהא מדעת יש להבטיח שהאדם מודע לזכותו לסרב לבקשה לספק מידע אישי אודותיו לאחר שניתן לו כל המידע הנחוץ לו, באורח סביר ובצורה מובנית, לשם החלטה האם לספק מידע אישי אודותיו אם לסרב לה. במסגרת זו נדרש לספק לאדם נתונים על אודות איסוף המידע והשימוש בו לרבות מטרות איסוף המידע וזהות הגורמים אליהם המידע האישי עשוי להיות מועבר. לעמדת הרשות, די בציון סוג הגורמים אליהם יועבר מידע אישי בהתאם לשיוך המקצועי שלהם, אך אין להסתפק בזיהוי כללי שאין

---

[229] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה בדיני הגנת הפרטיות (25 בפברואר, 2026), בעמ' 2 (להלן: "גילוי דעת בנושא הסכמה").

[230] שם, וכן ראו הדיון בסעיף 1 בפרק החמישי.

[231] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה, לעיל ה"ש 229, בעמ' 2.

בו כדי ללמד על השימוש שיעשה במידע האישי על ידי אותו גורם. למשל, ניתן להסתפק באמירה שהמידע האישי יועבר לחברות פרסום, אך ציון שהמידע יועבר לחברות טכנולוגיה אינו מספק. כן יש לפרט את כלל סוגי המידע וכלל מטרות עיבוד המידע כך שנושא המידע יוכל להבין איזה מידע אישי נאסף על בסיס הסכמתו ולאילו שימושים. בהקשר זה הרשות הבהירה פירוט חלקי תוך שימוש בביטויים כגון "וכיו"ב" או "בין היתר", אינו מספק. בנוסף, יש להקפיד שתוכן המידע המסופק לאדם בעת בקשה לקבל את הסכמתו לאיסוף מידע אישי אודותיו יוצג באופן ברור, נגיש פשוט ומובן. הסכמה שניתנה מבלי שהייתה לאדם אפשרות סבירה להבין את משמעותה והשלכותיה לא תיחשב להסכמה תקפה. כך, למשל, אתר אינטרנט שמדיניות הפרטיות שלו ומסמך תנאי השימוש אינם נגישים באופן סביר למשתמשים או שהאמור בהם מוצג בצורה מסורבלת, ארוכה וקשה להבנה עשוי להיחשב כמי שלא סיפק את המידע הדרוש באופן ברור וסביר לשם קבלת הסמכה מדעת לפגיעה בפרטיות.[232]

זאת ועוד, פרטי המידע שיש לפרט בהודעה לנושא המידע לפי סעיף 11 לא בהכרח מספקים לשם עמידה בדרישת ההסכמה מדעת. במקרים של פערי כוחות משמעותיים בין הצדדים, כאשר מדובר בפעולה שעשויה לפגוע קשות בזכות לפרטיות או בנסיבות מורכבות אחרות כגון שימוש בטכנולוגיה חדשה שהשלכותיה אינן ברורות, חובת ההסכמה מדעת מחייבת פירוט רחב יותר של מידע מאשר זה הנדרש במסגרת חובת ההודעה שבסעיף 11 לחוק. על מבקש המידע בנסיבות כאמור לפרט באופן בוטל ופשוט את הנתונים המהותיים הרלוונטיים לנושא המידע לשם קבלת החלטה האם להסכים לעיבוד מידע אישי אודותיו.[233]

עוד הבהירה הרשות שכאשר מבקש המידע הוא ספק שירות והמידע האישי המבוקש הוא למטרות השונות באופן מהותי מתכלית העסקה העיקרית או מידע בעל רגישות מיוחדת שסביר שאינו תואם את ציפיית הלקוח, יש להציג את המידע והמטרות הללו באופן בולט ובנפרד ככל הניתן מרכיבי ההתקשרות לצורך מתן השירות. למשל, אם חברה המשווקת מזון בריאות אוספת ממשתמשים הנרשים לאתר שלה נתוני מיקום ומסלולי תנועה, הרי שמדובר במידע שמרבית המשתמשים אינם מצפים שיאסף מהם במסגרת מתן שירות לרכישת מזון. משום כך, על החברה להציג את עובדת איסוף נתוני המיקום ומסלולי התנועה באופן בולט ומודגש בתנאי השימוש שלה, בעמוד הבית הראשי או בהודעה קופצת בעת הרישום לאתר על מנת לבסס את הדרישה שההסכמה היא מדעת. כמו כן, לעמדת הרשות, במתן שירות המיועד לאוכלוסיה בעלת מאפיינים ייחודיים כגון אנשים עם מוגבלויות יש לתת לכך את הדעת באופן הצגת המידע לשם ביסוס דרישת ההסכמה מדעת. למשל, יישומון המכוון לאוכלוסיה של ליקוי ראייה נדרש להציג את המידע באופן ויזואלי נגיש או באמצעים קוליים העשויים לסייע בהבנת משמעות ההסכמה.[234]

הסכמה מדעת יכולה להינתן באופן אקטיבי ומפורש (opt-in) של נושא המידע, למשל סימון ברובריקה המתירה שימוש במידע. אך גם הסכמה פסיבית (opt-out) במסגרתה נושא המידע נמנע מסימון ברובריקה האוסרת על שימוש במידע אישי שאינו הכרחי למתן השירות, כאשר ההסכם מבהיר שאי הסימון מבטא קבלה של כל תנאי ברירת המחדל בהסכם, עשויה להיחשב הסכמת מדעת. עם זאת, הסכמה אקטיבית מלמדת על מודעות גבוה יותר לרכיבי ההסכמה ועל כן בנסיבות מסוימת תידרש הסכמה מסוג זה על מנת לקיים את דרישת ההסכמה מדעת. נסיבות אלו כוללות מקרים בהם עיבוד

[232] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 3–5.

[233] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 7.

[234] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 5–6.

המידע הוא למטרות פרופיילינג שאינו קשור ישירות בתכלית העסקה, ובעיקר אם מדובר בנסיבות הן קיימים פערי כוחות בין הצדדים, מבוצע בהקשר של שירותי דיוור ישיר, אינו נחוץ למתן השירות או מבוקש למטרות השונות מהותית ממטרות ההסכם שלגביהן ניתנה הסכמה כללית ומפורשת.

"מרצון חופשי"

הדרישה שההסכמה ניתנת מרצון חופשי נועדה להבטיח שלנושא המידע בחירה אמיתית האם להסכים לעיבוד המידע האישי אודותיו או לסרב לה. היותה של ההסכמה "מדעת" אינה מלמדת בהכרח שהיא עומדת גם בדרישה שהיא תינתן גם מרצון חופשי. בגילוי הדעת בנושא הסכמה הבהירה הרשות ששימוש בכלים עיצוביים וטקטיקות אפלות (dark patterns) שמטרתן להקשות על נושא המידע להבין את משמעות הסכמתו ולהשפיע באופן פסול על החלטתו, עלול ללמד על כך שההסכמה אינה מבטאת את רצונו החופשי של נושא המידע ואינה הסכמה מדעת. לדוגמה יישומון משחק רשת לילדים מקפיץ בזמן המשחק באופן קבוע בקשה לאיסוף נתוני מיקום שמקפיאה את המשחק, אינה מאפשרת לבטל את הקפיצה החוזרת של ההודעה ומנגד אינה מאפשרת גישה למידע בנוגע למטרות השימוש אלא ביציאה מהמשחק, תחשב כפרקטיקה הפוגעת בהיותה של ההסכמה מרצון חופשי.[235]

בנוסף, לעמדת הרשות בנסיבות בהן קיים חשש אינהרנטי שההסכמה לא ניתנה מרצון חופשי, בעיקר בנסיבות של פערי כוחות בין נושא המידע למבקש ההסכמה. למשל, במסגרת יחסי עבודה, התקשרות של צרכן עם מונופול עסקי או עם ספק שירות חיוני, על מבקש ההסכמה מוטל להראות שההסכמה ניתנה מרצון חופשי. למשל, מבקש ההסכמה יכול להראות שהציג חלופות סבירות להסכמה, לא התנה את מתן השירות במתן הסכמה לאיסוף מידע שאינו נדרש באופן סביר לשם מתן השירות, או שקיימות חלופות אחרות לקבלת אותו השירות מגורמים אחרים.[236]

במפורש או מכללא

חוק הגנת הפרטיות מכיר הן בהסכמה הניתנת במפורש, כלומר הסכמה בכתב או בעל פה באופן מובהק וחד משמעי לפגיעה בפרטיות בהקשר שבו התבקשה ההסכמה. במסגרת זו הסכמה מפורשת מוכרת בחתימה על חוזה, לחיצה אקטיבית על רובירקת אישור במסמך תנאי השימוש, אמירה בעל פה, ובמקרים מסוימים גם מחווה גופנית כגון הנהון בתגובה לשאלה מפורשת.[237]

אולם, חוק הגנת הפרטיות מכיר גם בהסכמה מכללא כהסכמה תקפה. הכוונה להסכמה משתמעת הנלמדת מהנסיבות, ההקשר ודרכי ההתנהגות של נושא המידע, בהתבסס על הפרשנות הסבירה והמקובלת של התנהגות כאמור. למשל, פעילות פומבית של אדם במפלגה פוליטית מהווה הסכמה מכללא לחשיפת דעתו הפוליטית. כך גם השתתפות בתהלוכה במרחב הציבורי מהווה הסכמה מכללא לפרסום תמונתו של האדם בדיווח חדשותי בדבר קיום התהלוכה. גם בהקשרים דיגיטליים מכירה הרשות להגנת הפרטיות בנסיבות בהן הסכמה מכללא היא תקפה. למשל, המשך גלילה באתר אינטרנט, לאחר שהוצג בפני המשתמש המידע הנדרש לשם קבלת הסכמתו מדעת לאיסוף מידע אודותיו עם כניסתו לאתר היא

[235] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה, שם, בעמ' 8–9.

[236] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 9–10.

[237] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 12.

הסכמה מכללא לאיסוף המידע, ובלבד שקיים קשר סביר בין מטרות איסוף המידע ועיבודו לבין מאפייני השירות.[238]

עם זאת, לעמדת הרשות, כפי שאף באה לידי ביטוי בפסיקה, ככל שהפגיעה בפרטיות חמורה יותר או ככל שהמידע המעובד הוא מידע בעל רגישות מיוחדת, כן יפחת הסיכוי להכיר בהסכמה מכללא לפגיעה ויש להוכיח הסכמה מפורשת. כן אין בעובדה שאדם הסכים לגילוי מידע אישי מסוים לגורמים מסוימים כדי לתמוך בקיומה של הסכמה מכללא שלו לגילוי אותו המידע לגורמים אחרים. בנוסף, שתיקתו של אדם או היעדר מחאה מצדו לעיבוד מידע אודותיו יחשב כהסכמה מכללא לעיבוד המידע רק בנסיבות בהן ניתן ללמוד שנושא המידע באמת התכוון להסכים לעיבוד המידע, ובלבד שגם ניתן להוכיח שהוא היה מודע לכל המידע הנדרש לשם הוכחת הסכמה מדעת.[239]

זאת ועוד, נקיטת פעולות לחיזוק הליך קבלת ההסכמה, כגון העדפת הסכמה מפורשת על פני הסכמה מכללא, שימוש במנגנון הסכמה אקטיבית על פני הסכמה פסיבית ושימוש בכלים טכנולוגיים ועיצוביים לפישוט ולהנגשת דרישת ההסכמה והמידע הנחוץ לשם קבלתה, אף שאינן נדרשות לפי החוק, יסייע בהוכחת תקפותה של ההסכמה.[240]

חזרה מהסכמה

בגילוי הדעת בנוגע להסכמה הכירה הרשות להגנת הפרטיות בזכות נושא המידע לחזור בו מהסכמתו במקרים מסוימים, אף שזכות זו אינה מעוגנת בחוק הגנת הפרטיות. עמדת הרשות נשענה על פסיקת בשופט בית המשפט העליון סולברג בעניין פלוני לפיה ככל שהפגיעה בפרטיות חמורה יותר כך יטה בית המשפט להימנע מלאכוף את הסכמתו של נושא המידע לפגיעה בפרטיותו ויעדיף את סעד הפיצויים.[241] אולם, נוכח היעדר עיגון בחוק לזכות החזרה מהסכמה הבהירה הרשות להגנת הפרטיות שכאשר נושא המידע מבקש לחזור בו מהסכמה שנתן כדין לעיבוד מידע אישי אודותיו על בעל השליטה לשקול להיענות בחיוב להסכמה, במיוחד כאשר עיבוד המידע יפגע קשות בפרטיות נושא המידע ובעל השליטה אינו יכול להצביע על אינטרסים לגיטימיים ומשמעותיים להמשך עיבוד המידע. למשל, כאשר עיבוד המידע הכרחי לקיום חובות רגולטוריות, דרישות אבטחה, התגוננות בהליך משפטי או היעדר אפשרות טכנולוגית להפסיק את עיבוד המידע. עם זאת, חזרה מהסכמה אינה פוגעת בחוקיות עיבוד המידע שבוצע קודם לה ולא בהכרח תוביל למחיקת המידע האישי שכבר נאסף.

עוד המליצה הרשות, שבמקרים בהם התנהגותו של נושא המידע עשויה ללמד שהוא מבקש לחזור בו מהסכמתו או שההסכמה שנתן מלכתחילה הייתה נקודתית או לזמן מוגבל, יפנה בעל השליטה מיוזמתו לנושא המידע על מנת לבחון האם הסכמתו עומדת בעינה. למשל, כאשר אדם לא עשה שימוש ביישומון שהתקין על מכשיר הנייד שלו לפרק זמן ממושך (למשל שנה), מומלץ ליידע אותו שעיבוד המידע אודותיו באמצעות היישומון נמשך ולבחון האם הוא עדיין מסכים לכך.[242]

---

[238] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 12.

[239] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה, שם בעמ' 14–15.

[240] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה שם, בעמ' 10.

[241] ע"א 8954/11 **פלוני נ' פלונית** (נבו, 20.4.2014).

[242] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה, לעיל ה"ש 229, בעמ' 15–16.

המידע במאגר המידע אותו מעבדים מפלגה ו/או מפעיל יישומון בחירות הוא מידע בעל רגישות מיוחדת בהיקף נרחב. זאת ועוד, כחלק מעיבוד המידע מבוצע גם פרופיילינג על הבוחרים מתוך כוונה להתאים להם מסרי תעמולה מותאמים אישית באמצעות דיוור ישיר. לפיכך, על מפלגה ומפעיל יישומון בחירות לקבל את הסכמת הבוחרים, נושאי המידע, לעיבוד המידע אודותיהם. ההסכמה צריכה להיות מדעת, ולפיכך על המפלגה ומפעיל יישומון הבחירות להבטיח שבידי הבוחרים נושאי המידע כל המידע הנחוץ להם, לרבות מידע על סוגי המידע הנאספים אודותיו, השימוש שיעשה בו, מטרותיו וסוגי הגורמים אליהם עשוי המידע להיות מועבר. המידע צריך להיות מוצג באופן ברור, נגיש פשוט ומובן. מאחר ועיבוד המידע הוא למטרות פרופיילינג, עדיף שההסכמה תתקבל באמצעות פעולה אקטיבית מצד הבוחרים נושאי המידע (opt-in). כן נדרשת המפלגה ו/או מפעיל יישומון הבחירות להוכיח שההסכמה ניתנת מרצונו החופשי של הבוחר נשוא המידע, כאשר שימוש בכלים עיצוביים וטקטיקות אפלות שמטרתן להקשות על הבנת משמעות ההסכמה, למשל טענה שהבוחר חייב לתת את הסכמתו לעיבוד המידע האישי באופן הפוגע בפרטיותו על מנת לממש את זכותו לבחור, יפגע בתקפותה של ההסכמה כהסכמה מרצון חופשי. בנוסף, מוצע למפלגה או למפעיל יישומון בחירות להעדיף קבלת הסכמה מפורשת ולא מכללא. זאת משום שבמקרים בהם המידע האישי הנאסף משמש להסקת דעתו הפוליטית של הבוחר ולנקיטת תעמולת בחירות בהתאם המדובר בפגיעה חמורה בזכות לפרטיות. ככל שהפגיעה חמורה יותר בזכות לפרטיות הסיכוי להכרה בהסכמה מכללא כהסכמה תקפה פוחת. לבסוף, נוכח חומרת הפגיעה בפרטיות מוצע שהמפלגה ו/או מפעיל יישומון הבחירות יעמידו לרשות הבוחרים נשואי המידע מנגנון לחזרה מהסכמה, בהתאם להמלצת הרשות בנושא.

2. צמידות המטרה

עקרון צמידות המטרה הוא עקרון יסוד בדיני הגנת הפרטיות עוד לפני תיקון 13 ומחייב שעיבוד מידע ייעשה אך ורק למטרה לשמה נאסף המידע. בסעיף 2(9) לחוק הגנת הפרטיות, עוד לפני התיקון, נקבע ששימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסר, הוא פגיעה בפרטיות שתותר רק בהסכמת נושא המידע.[243] סעיף 11 חייב לפרט במסגרת פנייה לקבלת מידע אישי את המטרה שלשמה מבוקש המידע.

סעיף 8(ב) לחוק הגנת הפרטיות, שתוקן בתיקון 13, מהווה נדבך נוסף בעקרון צמידות המטרה וקובע כי "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין".[244] כלומר, עיבוד מידע חייב להיעשות בהתאם למטרת המאגר המפורטת במסמך מטרות המאגר, ומטרה זו צריכה להיות חוקית, מסוימת ומפורשת.[245] נעיר כי חוק הגנת הפרטיות אינו מבהיר על מי מוטלת החובה לפעול בהתאם לעקרון צמידות המטרה לפי סעיפים אלו – בעל שליטה ו/או מחזיק.[246]

לכן, על מפלגה לקבוע מטרות עיבוד מפורשות, מסוימות וחוקיות לעיבוד המידע במאגרי המידע שלה. קביעה שהמידע יעובד "לכל מטרה חוקית" אינה עומדת בדרישה זו. כל עיבוד מידע אישי חייב להיעשות

---

[243] סעיפים 1, 2(9) ו־8(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[242] סעיף 8(ב) בחוק הגנת הפרטיות, לעיל ה"ש 9.

[245] סעיף 23כה(א) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[246] לביקורת על כך ראו רחל אירידור הרשקוביץ **תיקון 13 לחוק הגנת הפרטיות: משמעות התיקון, השלכותיו וחסרונותיו** (הצעה לסדר 62, המכון הישראלי לדמוקרטיה, בהכנה)

אך ורק למטרות שנקבעו. בנוסף, מטרות עיבוד המידע צריכות להיכלל הן במסמך מטרות המאגר והן בכל פנייה לאדם לשם קבלת מידע אישי. על מפעיל יישומון בחירות להבטיח שעיבוד המידע המבוצע על ידו הוא אך ורק למטרות שהגדירה המפלגה כבעל שליטה במסמך מטרות המאגר, בפנייה לאדם לשם קבלת מידע אישי ממנו ובמטרות לשמן נמסרה ידיעה על ענייניו הפרטיים של אדם.

בבחינת הפרת עקרון צמידות המטרה יש לתת את הדעת לכך שאין לעשות שימוש במידע אישי כאשר האדם עליו נאסף המידע לא נתן הסכמה תקפה, מדעת ומרצון חופשי, למטרת השימוש או לגורמים להם יועבר המידע.[247] עיבוד מידע אישי בנסיבות כאמור עלול להביא להפרת עקרון צמידות המטרה. למשל, כאשר מידע על עמדתו הפוליטית של אדם מעודכן ביישומון בחירות על ידי בן משפחה או עמית לעבודה על בסיס שיחה שקיימו, מבלי שמעדכן המידע ביקש את הסכמתו של האדם להזנת מידע זה ביישומון בחירות. זאת, משום שסביר שהמידע נמסר בשיחה הפנימית, לא למטרה של עדכון ביישומון בחירות ולא לעיבוד מידע לשם יצירת פרופיילינג והתאמת מסרי תעמולה מותאמים אישית. משום כך, לא מתקיימים היסודות מדעת, מרצון חופשי והסכמה המפורשת הנדרשים על מנת להכיר בהסכמה תקפה.[248] לעומת זאת, כאשר אדם מעדכן ביישומון בחירות ששכנו אינו תומך במפלגה מסויימת על בסיס שלט תמיכה במפלגה אחרת שמציב השכן במרפסת ביתו הגלויה לרחוב ולציבור בכללותו, ניתן לומר שאין פגיעה בעקרון צמידות המטרה, שכן ניתן להסיק על הסכמתו של השכן לשימוש במידע אודות עמדתו הפוליטית למטרות תעמולת בחירות. השכן יתקשה לטעון שהביע את עמדתו הפוליטית בפני שכנו בלבד ולא ציפה שיעשה בה שימוש למטרות שונות כגון עדכון מפלגה בעמדותיו.

עקרון צמידות המטרה מופר גם כאשר אדם מעדכן ביישומון בחירות מידע על עמדותיו הפוליטיות, מתוך ידיעה והבנה שמטרת עיבוד המידע היא הצלחת המפלגה בבחירות הקרובות, והמפלגה אינה מוחקת את המידע ומשתמשת בו גם במערכת בחירות אחרת כמה שנים לאחר מכן. זאת משום שבהיעדר הבהרה ברורה שיעשה שימוש במידע האישי בכל מערכת בחירות עתידית, הרי שימוש במידע במערכת בחירות הבאה אחרי זו שבמהלכה התקבלה הסכמה תקפה לעיבוד המידע היא שימוש למטרה שונה שלגביה לא נתן הבוחר הסכמה מדעת. יתרה מכך, נראה שלפי עמדת הרשות להגנת הפרטיות בגילוי הדעת בנוגע להסכמה חלוף השנים אף מצדיק פנייה מחודשת לנושא המידע לשם בחינה האם הוא הסכמתו לשימוש במידע האישי אודותיו לצורכי תעמולת הבחירות עדיין עומדת בעינה.[249]

נוסף על כך, למפעיל יישומון בחירות חייבת להיות שליטה מלאה על שימושים הנעשים ביישומון, כדי לממש את עקרון צמידות המטרה. למשל, אם כל המעוניין יכול לשלוח מסרון למספר טלפון ולקבל בתגובה קישורית להתקנת היישומון ולפיכך לקבל גישה לכלל המידע (מידע פנקס ושכבות מידע נוספות) ולחפש בתוך המאגר מידע על כל מי שנמצא בו, ללא קשר למטרת המאגר שהתוותה המפלגה בהתאם למסגרת המותרת לה בחוק הבחירות, מדובר בהפרת עקרון צמידות המטרה. אין מדובר בחשש בעלמא, אלא באירועים שדווחו בתקשורת במערכות בחירות קודמות.[250]

---

[247] ראו למשל, מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27.1.2021), סעיף 10.3, בעמ' 9 ; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 10.7 בעמ' 11.

[248] ראו הדיון בטקסט הנלווה לה"ש 229–242 לעיל.

[249] ראו הדיון בטקסט הנלווה לה"ש 242 לעיל.

[250] שוורץ אלטשולר ולוריא, לעיל ה"ש 1, עמ' 70–106.

3. מידתיות עיבוד המידע

הדרישה שפגיעה בפרטיות תעמוד בדרישת המידתיות מקורה בעיגונה של הזכות לפרטיות כזכות יסוד חוקתית בחוק־יסוד: כבוד האדם וחירותו.[251] משום כך, עיבוד מידע המבוצע על ידי גוף שחלים עליו עקרונות המשפט הציבורי חייב להיעשות בהתאם לדרישת המידתיות. כן נקבע בפסיקה שדרישת המידתיות חלה גם על פגיעה במסגרת יחסי עבודה.[252]

דרישת המידתיות חלה גם על בעל שליטה או מחזיק הפוגעים בזכות לפרטיות ומבקשים להישען על הגנת תום הלב לפי סעיף 18(2) ו 20(ב) לחוק הגנת הפרטיות. זאת משום שחזקת תום הלב תחול רק בשעה שהפגיעה נעשתה בהתאם לעקרון המידתיות והנחיצות.

בפועל, על מנת לעמוד בדרישת המידתיות, יש להוכיח התאמה בין היקף וסוג המידע המעובד לאינטרס הציבורי שהוא מטרת העיבוד, ולהראות שעיבוד המידע האישי המבוצע נחוץ להשגת המטרה והוא האמצעי שפגיעתו בזכות לפרטיות פחותה, ושבאיזון בין הפגיעה בזכות לפרטיות לבין התועלת מהשגת האינטרס הציבורי שבבסיס מטרת העיבוד, גוברת האחרונה.[253]

בבחינה האם מפלגה או מפעיל יישומון בחירות חייבים לעבד מידע אישי אודות בוחרים בהתאם לעקרון המידתיות, יש לתת את הדעת לא רק לשאלה האם ברצונן להישען, במידה והנושא יגיע לבית המשפט, על הגנת תום הלב. עקרון המידתיות עשוי לחול, גם על גוף שחלים עליו עקרונות מהמשפט הציבורי. כלומר, כאשר אפיונה של המפלגה כגוף דו־מהותי מצדיק גם את החלת דרישת המידתיות מהמשפט הציבורי.

אף שההכרעה בנושא תתקבל לגופו של כל מקרה,[254] לדעתנו עיבוד המידע האישי על ידי מפלגה, נוכח סוג המידע – מידע בעל רגישות מיוחדת – והיקפו, הוא בעל מאפיינים ציבוריים מובהקים. זאת משום שקמפיינים פוליטיים מבוססי נתונים ובינה מלאכותית מאפשרים איסוף, ניתוח והיסק של מידע על בוחרים בהיקפים ובעומק שלא היו אפשריים בעבר, וכן יצירה והפצה של מסרים פוליטיים מותאמים אישית בקנה מידה רחב. יכולות אלה מעוררות חשש הולך וגובר לפגיעה בפרטיות הבוחרים, להגדלת פערי הכוח בין מפלגות לאזרחים, ולפגיעה בזכות לבחור באופן חופשי ואוטונומי ועקב כך פגיעה בהוגנות הבחירות, חשאיות הבחירות וטוהר הבחירות. לפיכך, לדעתנו לשם מזעור סיכון כאמור יש לחייב את המפלגה לעבד מידע אישי אודות בוחרים בהתאם לעקרון המידתיות.

4. איסור עיבוד מידע אישי שנצבר או נאסף בניגוד להוראות החוק או כל דין אחר המסדיר עיבוד מידע והגנת "תקנת השוק"

סעיף 8(ד) לחוק הגנת הפרטיות, שנוסף אליו במסגרת תיקון 13, אוסר על בעל שליטה לעבד מידע אישי במאגר מידע, או להתיר לאחר לעשות כן עבורו, אם המידע הכלול במאגר המידע "נוצר, התקבל, נצבר

---

[251] סעיף 7 לחוק-יסוד: כבוד האדם וחירותו.

[252] בג"ץ 8298/22 **הסניגוריה הציבורית נ' היועצת המשפטית לממשלה** (נבו, 31.08.2025).

[253] להרחבה ראו **אהרון ברק, מידתיות במשפט: הפגיעה בזכות החוקתית הגבלותיה** (נבו, 2010); ולעניין המבחן האחרון למידתיות במובנה הצר ע"א 8954/11 פלוני נ' פלונית (נבו, 24.4.2014) סעיפים 118-136 לפסק דינו של השופט סולברג.

[254] פרשת **ערוץ 14**, לעיל ה"ש 188, סעיף 25, 27 לפסק דינה של השופט ברק ארז.

או נאסף בניגוד להוראות חוק זה או להוראות כל דין אחר המסדיר עיבוד מידע". "הוראות חוק זה" כוללות את סעיף 2 המונה מופעי פגיעה בפרטיות; ובניהן עקרון צמידות המטרה, סעיף 11 המטיל חובה לתת הודעה בעת פנייה לאדם לשם קבלת מידע אישי ממנו; וסעיף 23ד המאסדר מסירת מידע אישי על ידי גוף ציבורי.[255]

סעיף 8(ד) כולל, לצד האיסור, גם הגנה המכונה "תקנת השוק", לפיה האיסור לא יחול באחת מהנסיבות הבאות:

(1) בעל השליטה במאגר מידע לא ידע, או לפי מבחן אובייקטיבי לא היה עליו לדעת, שהופרה הוראת חוק הגנת הפרטיות או כל דין רלוונטי אחר בקשר למידע שנוצר, התקבל, נצבר או נאסף במאגר המידע.[256]

(2) הפגיעה בפרטיות היא קלת ערך. במקרה זה ההגנה תחול גם אם בעל השליטה ידע או היה עליו לדעת שהופרה הוראת חוק הגנת הפרטיות או כל דין רלוונטי אחר בקשר למידע שנוצר, התקבל, נצבר או נאסף במאגר המידע.[257]

הוראה זו, וגם ההגנה הצמודה אליה, אינן מעניקות תשובה בהירה לגבי מעמדו של מידע שהגיע למאגר מידע באמצעות "גירוד" מידע אישי (data scraping) ממקורות גלויים – למשל אתרי אינטרנט או רשתות חברתיות. בנסיבות אלו אין גורם מזוהה אשר מוסר לבעל השליטה את המידע; יש להניח שהמידע המפורסם בהם הוא חוקי; וקשה לומר שבעל השליטה יודע או שעליו לדעת שהמידע האישי נוצר, התקבל, נצבר או נאסף באופן לא חוקי. נדגיש, כי אין מדובר במידע שהמפלגה עצמה משיגה באמצעות "גירוד", אלא בקנייה של מידע מסוחרי מידע, המגרדים מידע הקיים ברשת האינטרנט לשם יצירת מסרים מותאמים אישית לצרכים מסחריים ועתה גם פוליטיים.

חוסר בהירות זה מתגבר הואיל ובדיונים בוועדת החוקה נקבע שהגנת "תקנת השוק" חלה גם כאשר מתבצע גירוד מידע, ובלבד שבעל השליטה במאגר המידע לא ידע ולא היה עליו לדעת שהמידע המגורד על ידו נמסר על ידי גורם שפעל שלא כדין, ולחילופין גם אם בעל השליטה ידע או היה עליו לדעת על אי החוקיות, הפגיעה היא קלת ערך.[258]

לעומת זאת, בטיוטת הנחיית הרשות להגנת הפרטיות בנושא בינה מלאכותית, עמדה הרשות על כך שכאשר מערכות מבוססות בינה מלאכותית מגרדות מידע – אפילו כזה שנושא המידע פרסם על עצמו ברשת חברתית, ובוודאי ממידע הזמין ברשת האינטרנט – לא ניתן להסיק הסכמה מדעת לעיבוד המידע רק מעצם הימצאות המידע באופן זמין ופתוח ברשת האינטרנט. הרשות סברה כי לא ניתן להניח שלנושא המידע הייתה ציפייה סבירה לשימושים שעשויים להתבצע באמצעות מערכות בינה מלאכותית ולסכנות הטמונות בהם. לכן הציעה הרשות לחייב בעלי שליטה המאפשרים שיתוף מידע אישי ברשת האינטרנט,

---

[255] ס' 1 ו 2 בחוק הגנת הפרטיות, לעיל ה"ש 9.

[256] פרוטוקול מס' 223, לעיל ה"ש 159, עמ' 39–58; פרוטוקול מס' 233, לעיל ה"ש 204/202, עמ' 17–21.

[257] פרוטוקול מס' 223, לעיל ה"ש 159, עמ' 39–41.

[258] פרוטוקול מס' 223, לעיל ה"ש 159, עמ' 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."

לנקוט אמצעים נאותים למניעת פעולות אסורות של גירוד מידע.[259] משמעות הנחייה זו היא שמידע שנאסף בדרך של גירוד מידע באינטרנט, מבלי לקבל את הסכמתו מדעת של נושא המידע, עשוי להיחשב כשימוש במידע שלא למטרה לשמה נמסר, כלומר כפגיעה בפרטיות לפי סעיף 2(9) לחוק הנעשית ללא הסכמה מדעת של נושא המידע. עיבוד מידע ממאגר מידע הכולל מידע שנאסף בדרך גירוד כזו יהיה, לכן, הפרה של האיסור הקבוע בסעיף 8(ד) לחוק הגנת הפרטיות. אומנם, הנחיה זו זכתה לביקורת לא מעטה ובזמן כתיבת מחקר זה לא פורסמה בגרסתה הסופית. קבלתה כלשונה משמעה ביטול ההכרה בהסכמה מכללא, והחמרת דרישת ההסכמה באופן שיהפוך אותה לכמעט בלתי ניתנת להשגה. בהיעדר בסיסים חוקיים אחרים לעיבוד מידע אישי לבד מהסכמה, עלול שינוי זה של דרישת ההסכמה לשתק לחלוטין את החדשנות בתחום הבינה המלאכותית בישראל וליצור הטיה לרעת ישראל במודלים שיפותחו במדינות אחרות. זאת לצד מתן סמכות עוצמתית לרשות להגנת הפרטיות, שלא הייתה בכוונת המחוקק לתת לה, וללא בחינה מעמיקה של השלכותיה. ודוק, נושא גירוד המידע הוצג מספר פעמים בדיוני ועדת החוקה שעסקו בתיקון 13, ומעולם לא הוסכם שם על פרשנות כפי שמוצגת בטיוטת ההנחיה.[260] עם זאת, יש לתת את הדעת כי עמדה זו של הרשות, לפיה יש לקבל את הסכמתו מדעת של כל אדם לשם איסוף ועיבוד מידע אישי אודותיו ביישומונים או מאגרי מידע של מפלגות, וכי סחר במידע כאמור ללא הסכמת האדם שהמידע אודותיו אינו חוקי, אינה חדשה, והייתה בין הדגשים שמסרה הבחירות למפלגות במסמכיה לקראת הבחירות לכנסת ה־23 וה־24.[261]

עקב חוסר הבהירות באשר לתחולת האיסור הקבוע בסעיף 8(ד), האכיפה בגין הפרתו היא דו שלבית. בשלב הראשון, כאשר ראש הרשות להגנת הפרטיות סבור שבעל השליטה במידע מפר איסור זה, עליו לתת לו להשמיע את טענותיו, ולאחר מכן בסמכותו להודיע לו שעליו להפסיק את ההפרה.[262] לבעל השליטה במאגר המידע אפשרות לערער על הוראת ראש הרשות לבית משפט שלום.[263]

בשלב השני, אם בעל השליטה לא מגיש ערעור או שערעורו נדחה, והוא אינו מקיים את הוראת ראש הרשות, אז בסמכות ראש הרשות להטיל עליו עיצום כספי.[264] קודם להטלת העיצום, על ראש הרשות למסור לבעל השליטה הודעה על כוונת חיוב, שלאחריה לבעל השליטה במאגר המידע האפשרות לטעון

---

[259] סעיפים 6.3.4 ו־10 בטיוטת הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית (28.4.2025). לביקורת על הנחייה זו, ראו רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר "טיוטת הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית – חוות דעת" המכון הישראלי לדמוקרטיה (29.7.2020).

[260] פרוטוקול מס' 233, לעיל ה"ש 204 פרוטוקול מס' 298 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ט"ז באדר ב התשפ"ד (26 במרץ 2024); פרוטוקול מס' 210 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ד בטבת התשפ"ד (26 בדצמבר 2023). לביקורת על הנחייה זו ראו, למשל, רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר "טיוטת הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית – חוות דעת" המכון הישראלי לדמוקרטיה (29.7.2020).

[261] הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 123, סעיפים 17–18; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, לעיל ה"ש 123, בסעיף 17.2.

[262] סעיף 23כה(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[263] סעיף 23כה(ו) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[264] סעיף 23כו(ה)(1)(ג) לחוק הגנת הפרטיות, לעיל ה"ש 9.

את טענותיו בפני ראש הרשות.[265] גם לאחר הודעה על כוונת חיוב, או אמצעי אכיפה אחר, שמורה לבעל השליטה האפשרות להגיש ערעור לבית משפט השלום.[266]

האיסור הקבוע בסעיף 8(ד) מוטל על בעל שליטה ואינו רלוונטי ביחס למחזיק. משום כך, הוא אינו רלוונטי למפעיל יישומון בחירות אלא רק למפלגה. במסגרתו, על מפלגה לבחון האם **מידע שבמאגר המידע שבשליטתה נחשב כזה ש"נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה או להוראות כל דין אחר המסדיר עיבוד מידע**". הואיל וסוגי המידע שבידי מפלגות הם שונים, נחלק אותם לכמה מקטעים:

(1) <u>מידע פנקס ממערכת בחירות קודמת</u>

סעיף 39(ג) לחוק הבחירות מתיר למפלגה או לסיעה לעשות שימוש במידע הפנקס רק לאחר שתתחייב בכתב כי השימוש יהיה "לצורכי התמודדותה בבחירות ולצורכי קשר עם ציבור הבוחרים".[267] "כתב ההתחייבות" שעל מפלגה או סיעה לחתום עליו על מנת לקבל לידה את מידע הפנקס, לפי תקנות הבחירות לכנסת, תשל"ג – 1973 (להלן: "תקנות הבחירות"), קובע שהמפלגה מתחייבת ש"השימוש במידע הפנקס יהיה אך ורק לצורך התמודדות בבחירות **הקרובות** לכנסת ולצורכי קשר עם ציבור הבוחרים של הסיעה או המפלגה האמורה ולא לכל צורך אחר".[268]

הרשות להגנת הפרטיות הבהירה במסמכיה לקראת הבחירות לכנסות ה־24 וה־25 כי "אין לעשות שימוש בפנקסי עבר, פנקסים מהבחירות לרשויות המקומיות וכד'".[269] הרשות חזרה על העמדה שמידע הפנקס ניתן למפלגה **כפיקדון זמני למערכת בחירות ספציפית** גם בקביעות ההפרה שפרסמה בעניין אלקטור שם ציינה כי "הזכות שמעניק חוק הבחירות למפלגות להשתמש בפנקס הבוחרים מוגבלת למטרת התמודדות במערכת בחירות ספציפית ורק כל עוד היא מתקיימת. הפנקס נמסר למפלגות כפיקדון זמני אותו הן נדרשות להחזיק או להשמיד עם תום הקמפיין."[270]

יתכן שאפשר לטעון ששימוש במידע הפנקס מותר לפי סעיף 39(ג) גם לצורכי "קשר עם ציבור הבוחרים". הקשר עם ציבור הבוחרים אינו מוגבל למערכת בחירות ספציפית, ולכן לכאורה מפלגה אינה חייבת למחוק את מידע הפנקס בתום מערכת הבחירות, אלא רשאית לשמור אותו ולעשות בו שימוש למטרה זו, וזאת בניגוד לעמדת הרשות בנושא. אולם, כך או כך, בכל מקרה, בכל הקשור לשימוש לצורכי התמודדות בבחירות, כתב ההתחייבות אליו מפנה סעיף 39(ג) לחוק הבחירות, קובע במפורש שהשימוש מוגבל למערכת בחירות ספציפית.

---

[265] סעיפים 23כז, 23כח לחוק הגנת הפרטיות, לעיל ה"ש 9.

[266] סעיף 23מה לחוק הגנת הפרטיות, לעיל ה"ש 9.

[267] סעיף 39(ג) לחוק הבחירות, לעיל ה"ש 75.

[268] תקנה 6א(ג) לתקנות הבחירות לכנסת, תשל"ג–1973 (להלן: "תקנות הבחירות"), סעיף א בנוסח כתב התחייבות שבתוספת לתקנות, בטופס ה1.

[269] דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, לעיל ה"ש 123, בסעיפים 17.3, 17.7; ס' 16.5 למסמך הרשות להגנת הפרטיות, דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־25: מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר ואחריות המפלגות על אפליקציות וספקים חיצוניים.

[270] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 10.3, בעמ' 8.

לפיכך, שימוש במידע הפנקס ממערכות בחירות קודמות במערכות בחירות שאחריהן, מנוגד לסעיף 39(ג) לחוק הבחירות. משום כך, מאגר מידע המשמש לצורכי התמודדות בבחירות עתידיות שכולל את מידע הפנקס ממערכות בחירות קודמות, כולל מידע שנוצר בניגוד לחוק הבחירות ולכן אסור לעבד אותו לפי סעיף 8(ד).

(2) <u>מידע שנאסף במערכת בחירות קודמת</u>

כאשר אדם מעדכן ביישומון הבחירות של מפלגתו כי הוא תומך במפלגה, הוא עושה זאת מתוך ידיעה והבנה שמטרת עיבוד המידע אודותיו הוא הצלחתה של המפלגה בבחירות הקרובות. לפיכך, שימוש שמפלגה עושה במידע כאמור במערכת הבחירות הבאה, מבלי לקבל לשם כך את הסכמתו המפורשת, מדעת ומרצון חופשי של הבוחר,[271] עשוי להוות הפרה של עקרון צמידות המטרה.

(3) <u>מידע שנאסף ללא הסכמת נושא המידע או מבלי לתת לו הודעה</u>

כפי שכבר הובהר לעיל, איסוף מידע אישי ישירות מאדם, במסגרת פנייה אליו, מחייב מתן הודעה מבעל השליטה בה מפורטים פרטים שונים, ביניהם מטרת עיבוד המידע. כמו כן, איסוף ועיבוד מידע אישי העולה כדי פגיעה בפרטיות מחייב קבלת הסכמה מדעת ומרצון חופשי של נושא המידע.

א. איסוף מידע לתוך יישומוני בחירות: מהמידע שפורסם אודות יישומון הבחירות אלקטור[272] נלמד שלעיתים מידע אישי אודות בוחר נאסף ללא ידיעתו, למשל מידע המוזן על ידי בן משפחה, שכן או חבר, שהתקין את היישומון על מכשירו האישי. עדכון מידע בעל רגישות מיוחדת כדעה פוליטית או מידע אישי אחר המשמש להסקת דעתו הפוליטית של הבוחר ללא ידיעתו או ללא הסכמתו לעיבוד המידע על ידי מפעיל ישומון בחירות או מפלגה לצורכי תעמולת בחירות מותאמת אישית עשוי להיחשב לפגיעה עקרון צמידות המטרה או לבילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת", שהיא פגיעה בפרטיות לפי סעיפים 2(1) ו 2(9) לחוק הגנת הפרטיות. לפיכך, לשם עיבוד מידע כאמור נדרשת הסכמתו מדעת, מרצון חופשי ועדיף במפורש של הבוחר נושא המידע.[273] הרשות להגנת הפרטיות אף ציינה במכתבי קביעת ההפרה בפרשת אלקטור שאין לעשות שימוש במידע אישי כאשר האדם עליו נאסף המידע לא הסכים לכך מדעת ומרצון חופשי, לאחר שהוסברו לו מטרות השימוש ולמי יימסר המידע.[274] אולם, מהמידע שפורסם בציבור לא נמצא שמפלגות שעשו שימוש ביישומוני בחירות או מפעילי יישומון בחירות ביקשו את הסכמתם של בעלי זכות בחירה למשל לתיוגם כתומכים במפלגה, מתנגדים לה או מתלבטים.[275]

ב. גירוד מידע מאתרי אינטרנט ורשתות חברתיות. נוכח עמדת הרשות במסמכי ההבהרה לקראת הבחירות לכנסת ה־23 וה־24, ובטיוטת הנחיית הרשות להגנת הפרטיות בנוגע לבינה מלאכותית,

---

[271] ראו הדיון בטקסט הנלווה לה"ש 229–242 לעיל.

[272] ראו סמוחה, ה"ש 113 לעיל.

[273] ראו הדיון בטקסט הנלווה לה"ש 229–242 לעיל.

[274] ראו, למשל, מחלקת האכיפה של הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות, התשמ"א-1981 – מפלגת ישראל ביתנו** (27.1.2021), סעיף 10.3, בעמ' 9; מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.01.21), סעיף 10.7, בעמ' 11.

[275] שוורץ אלטשולר ולוריא, לעיל ה"ש 1, עמ' 70.

בהחלט יתכן שגם פרקטיקה זו תחשב כאיסוף מידע אישי המחייב את קבלת הסכמתו התקפה של נושא המידע. במידה שאיסוף המידע האישי הוא מאתר אינטרנט שלא מפרט את אפשרות גירוד מידע לשם שימוש על ידי מפלגות במסגרת תעמולת בחירות כחלק ממטרות השימוש האפשריות בעת קבלת הסכמת משתמש האתר למדיניות השימוש באתר, הרי שניתן יהיה לטעון שהמשתמשים לא נתנו את הסכמתם לגירוד המידע.[276] עם זאת, לדעתנו, פרשנות שכזו אינה רצויה, ונכון לכתיבת שורות אלו אף אין לגביה הכרעה ברורה בחוק או בפסיקה.[277]

לטעמנו, מפלגות לא יוכלו ליהנות מהגנת תקנת השוק בהקשרים שנידונו למעלה. מפלגה תתקשה לטעון שלא ידעה כי עליה למחוק את מידע הפנקס ממערכת הבחירות הקודמת או שלא ידעה ולא היה עליה לדעת שיש לקבל את הסכמת בעלי זכות הבחירה לעיבוד מידע אישי עליהם או שחובה עליה לתת הודעה במסגרת פנייה לאיסוף מידע אישי מאדם או לציית לעקרון צמידות המטרה. זאת, לפחות בשל כך שלמפלגות נערכים תדרוכים מטעם הרשות להגנת הפרטיות בפתח כל מערכת בחירות,[278] וכן נוכח קביעת ההפרה של הרשות להגנת הפרטיות בעניין אלקטור שפורסמה בציבור.[279] בנוסף, באשר להגנה המבוססת על קלות הערך שבפגיעה בפרטיות, נראה כי אין זה המצב בכל הקשור לעיבוד מידע אישי על ידי מפלגה הנעשה בהיקפים נרחבים ביותר וביחס למידע אישי בעל רגישות מיוחדת.

5. איסור עיבוד מידע במאגר מידע ללא הרשאה

סעיף 8(ג) שהוסף לחוק הגנת הפרטיות בתיקון 13 קובע כי –

> "8(ג) לא יעבד אדם מידע אישי ממאגר מידע ללא הרשאה מאת בעל השליטה במאגר המידע או בחריגה מהרשאה כאמור."[280]

מטרת הסעיף היא להבהיר שלמעט אחסון באקראי ובתום לב של מידע אישי, כל עיבוד מידע ממאגר מידע חייב להיעשות בהתאם להרשאה מבעל השליטה במאגר המידע.[281] עם זאת, תיקון 13 לא סיפק פרשנות ברורה למהות ההרשאה הנדרשת.[282]

האיסור על עיבוד ללא הרשאה מוטל על מחזיק ולא על בעל שליטה, אבל על מפלגה כבעלת שליטה במאגר המידע, מוטל לקבוע במפורש מהו עיבוד המידע שהיא מתירה למחזיק לבצע במאגר המידע.

על מפעיל יישומון בחירות, כמחזיק של מאגר מידע שבשליטת מפלגה, לעבד את המידע במאגר המידע אך ורק במסגרת, בהיקף ובאופן שהותר לו על ידי המפלגה.

---

[276] ראו הדיון בטקסט הנלווה להי"ש 259–261 לעיל.

[277] ראו הטקסט הנלווה להי"ש 260 לעיל.

[278] ראו, למשל, הרשות להגנת הפרטיות, דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־25: מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר ואחראיות המפלגות על אפליקציות וספקים חיצוניים, https://www.gov.il/BlobFolder/reports/elaction_guidelines_3/he/elaction_4.pdf.

[279] מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27.1.2021); **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021); **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – אלקטור** (27.1.2021).

[280] סעיף 8(ג) לחוק הגנת הפרטיות, לעיל הי"ש 9.

[281] פרוטוקול מס' 223, לעיל הי"ש 159.

[282] סעיף 29 ל-GDPR, לעיל הי"ש 5.

פרק שביעי
כיבוד זכויות נושא המידע

לפי חוק הגנת הפרטיות, לנושא המידע, כלומר לאדם שמידע אישי אודותיו מועבד על ידי בעל שליטה או מחזיק, זכות לעיין במידע האישי על אודותיו, ולבקש תיקון של המידע האישי או מחיקתו במידה שאינו מדוייק, שלם או נכון. יש לו גם זכות לקבל הודעה,[283] וכן זכות לקבל פרטי מידע מסוימים בצירוף להודעת דיוור ישיר וכן לדרוש את מחיקת המידע האישי או להגביל את העברתו לצדדים שלישיים.[284] תיקון 13 לא הרחיב משמעותית את זכויות נושא המידע, למעט הרחבה מסוימת של זכות נושא המידע לקבל הודעה. כן נוספו שני כלים משמעותיים לרשות נושא המידע – פיצויים לדוגמה וביטול מגבלת ההתיישנות. לכלים אלו עשויה להיות השפעה גם על מפלגה ומפעיל יישומון בחירות.

1. חובת מתן הודעה לנושא המידע

חובת מתן הודעה לנושא המידע קבועה בסעיף 11 לחוק הגנת הפרטיות וחלה בנסיבות בהן נעשית פניה לאדם כדי לאסוף מידע אישי על אודותיו לשם עיבודו במאגר מידע, בין אם המידע נאסף מכוח הסכמת נושא המידע או מכוח הסמכה בדין. הרשות להגנת הפרטיות אף הבהירה שחובת היידוע תחול גם כאשר הפנייה לאדם לקבלת מידע אישי אודותיו מבוצעת בעקבות פנייתו של אותו האדם לקבלת שירות מסוים. מנגד, חובת היידוע לא חלה בעל השימוש במידע או העברתו. כלומר, היא לא מחייבת צדדים שלישיים שמידע אישי מועבר אליהם מתוקף הסכמת נושא המידע, או בעת העברת מידע בין גופים ציבוריים.[285] כלומר, כאשר המידע האישי אודות בוחרים מקורו במאגר מידע שנרכש מסוחר מידע, המפלגה או מפעיל היישומון אינם חייבים ליידע את הבוחרים שפרטיהם מופיעים במאגר. עם זאת, אין בכך כדי לשנות את דרישת הרשות שהמידע שאסף סוחר המידע נאסף בהסכמת נושאי המידע.[286]

לעומת זאת, הרשות להגנת הפרטיות הבהירה בהנחייתה בנושא כי נדרש יידוע של נושא המידע כאשר איסוף המידע מבוצע באמצעות מערכות לקבלת החלטות המבוססות על בינה מלאכותית. כלומר, כאשר המידע נאסף באמצעות גירוד מידע מרשת האינטרנט או שאיבה, באמצעות טכנולוגיית בינה מלאכותית, של פרטים על אנשי קשר ממכשיר טלפון נייד של אדם שהתקין את יישומון הבחירות, כן נדרשת הודעה.[287]

באשר לתוכן ההודעה, תיקון 13 הרחיב את תוכן ההודעה שיש למסור לנושא המידע בעת פנייה אליו. כך, יש לכלול בהודעה מידע בנוגע להשלכות אי הסכמתו של נושא מידע לעיבוד מידע אודותיו, את פרטי

---

[283] ס' 13, 14 ו־11 לחוק הגנת הפרטיות, לעיל ה"ש 9.

[284] סעיף 17ו לחוק הגנת הפרטיות, לעיל ה"ש 9.

[285] הרשות להגנת הפרטיות, חובת יידוע במסגרת איסוף ושימוש במידע אישי, נוסח מעודכן בעקבות תיקון 13 (18 ביולי 2022), בסעיפים 4, 5, 25.

[286] לעניין זה ראו גם את הטקסט הנלווה לה"ש 128 לעיל.

[287] עם זאת, נושא חוקיות גירוד מידע מרשת האינטרנט באמצעות בינה מלאכותית אינה ברורה לאשורה. ראו הדיון בטקסט הנלווה לה"ש 259–260 לעיל.

הקשר של בעל השליטה במידע וכן מידע אודות זכויותיו של נושא המידע לעיין במידע האישי אודותיו ולבקש את תיקונו.[288]

החובה אינה מבחינה האם הפונה הוא בעל השליטה במאגר המידע או המחזיק. לפיכך, על מפלגה או מפעיל יישומון בחירות הפונים לאדם לשם איסוף מידע אישי, לספק לו הודעה שבה יצויין:

- האם חלה עליו חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו ובהסכמתו
- מה תהא תוצאת סירובו למסור את המידע. במסגרת זו, ובכפוף לנסיבות העניין וזהות הצדדים, על בעל השליטה או המחזיק לפרט גם את החלופות העומדות בפני נושא המידע במידה שזה מסרב למסור את המידע האישי אודותיו. הרשות להגנת הפרטיות הבהירה דרישה זו באמצעות דוגמא. כאשר רשות מקומית מבקשת לספק לתושביה שירותים ציבוריים באופן מקוון ולשם כך היא מבקשת מהם לספק לה מידע אישי, עליה להבהיר שתושב שאינו מעוניין למסור את המידע יוכל לקבל את השירותים המסוימים רק באופן פיזי במשרדי הרשות. כמו כן, אם סירוב למסור מידע עשוי להשפיע על זכויות נושא המידע, יש לפרט זאת.[289]
- המטרה לשמה מבוקש המידע
- שמה של המפלגה ודרכי ההתקשרות עמה
- למי יימסר המידע ומטרות המסירה
- זכויותיו של נושא המידע לעיין במידע המעובד על אודותיו ולדרוש את תיקונו בהתאם לסעיפים 13 ו־14 בחוק הגנת הפרטיות.

2. הודעה בעת פנייה בדיוור ישיר

כל פנייה בדיוור ישיר חייבת לכלול ציון שמדובר בדיוור ישיר, זהותו ומענו של בעל השליטה, פירוט המקורות מהם קיבל בעל השליטה את המידע האישי, וכן הודעה על זכותו של מקבל הפנייה בדיוור ישיר להימחק מהמאגר, בצירוף המען אליו יש לפנות על מנת לממש את זכות מחיקה זו.[290]

מסרי תעמולה חישובית מותאמים אישית למאפייניו של בוחר עשויים להיחשב כדיוור ישיר, כפי שקבעה גם הרשות להגנת הפרטיות שפרסמה לפני הבחירות לכנסת ה־23 וה־24.[291] החובה אינה מוטלת במפורש על בעל שליטה או מחזיק, ולפיכך הן מפלגה והן מפעיל יישומון בחירות חבים בה. כן עליהן לתת את הדעת לכך שההודעה צריכה לכלול גם את פירוט מקורות המידע.

---

[288] סעיף 17ו לחוק הגנת הפרטיות, לעיל ה״ש 9.

[289] הרשות להגנת הפרטיות, חובת יידוע, לעיל ה״ש 285, סעיפים 14–15.

[290] סעיף 17ו(א) לחוק הגנת הפרטיות, , לעיל ה״ש 9.

[291] הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה״ש 123, סעיפים 13-16 ; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, לעיל ה״ש 123, בסעיף 17.6. כן ראו הטקסט הנלווה להי״ש 185–186.

3. זכות המחיקה ממאגר מידע המשמש לדיוור ישיר והזכות להגביל את העברת המידע לצדדים שלישיים

אדם שקיבל פנייה בדיוור ישיר רשאי לדרוש מבעל השליטה במאגר המשמש לדיוור ישיר למחוק את המידע האישי אודותיו. כן הוא רשאי לדרוש מבעל השליטה במאגר מידע שבו מצוי המידע על פיו בוצעה פנייה בדיוור ישיר שלא למסור את המידע האישי אודותיו לאדם, לסוג בני אדם או לאנשים מסוימים, לפרק זמן מוגבל או קבוע. דרישות אלו צריכות להיעשות בכתב ולבעל השליטה אין שיקול דעת האם להיענות להן. עליו לפעול בהתאם לדרישה ולהודיע על כך לדורש בתוך 30 ימים מקבלת הדרישה. בהיעדר הודעה בתוך פרק זמן זה רשאי האדם לפנות לבית משפט השלום בבקשה שיורה לבעל השליטה לפעול בהתאם לדרישתו.[292]

זכות המחיקה חלה על בעל שליטה במאגר מידע המשמש לדיוור ישיר, והזכות להגביל את מסירת המידע חלה על בעל שליטה במאגר מידע שבו מצוי המידע שעל פיו בוצעה הפנייה בדיוור ישיר. בהנחה שתעמולה חישובית מותאמת אישי היא דיוור ישיר, הרי שהוראות אלו מחייבות מפלגה כבעלת שליטה במאגר המשמש לדיוור ישיר או שבו מידע לפיו בוצעה הפנייה בדיוור ישיר. עליה להיענות לבקשת מחיקה או לבקשה להימנע ממסירת המידע האישי לצדדים שלישיים בהתאם לבקשה, למשל במידה שבוחר מבקש למנוע העברת מידע אודותיו לספק יישומון בחירות או לספק טכנולוגיה המשמשת להפצת מסרים מותאמים אישית.

4. פיצויים לדוגמה

סעד הפיצויים לדוגמה מתבסס על מודל דומה בחוק הגנת הצרכן,[293] ומטרתו לייצר מנגנון הרתעתי ביחס להפרת הוראות החוק, כחלופה למנגנון התביעות הייצוגיות שבשנים האחרונות שימש לעתים להגשת תביעות סרק.[294] התיקון קובע פיצויים מוסכמים בסכום מירבי של 10,000 ש״ח לטובת נושא המידע בגין הפרת הבאות על ידי בעל השליטה או מחזיק:[295]

- **חובת מתן הודעה לנושא המידע:** מחזיק או בעל שליטה הפונים לאדם לקבלת מידע אישי לשם עיבודו מבלי למסור הודעה כנדרש לפי בסעיף 11 לחוק הגנת הפרטיות, בתנאי שנושא המידע פנה לבעל השליטה בדרישה לקבל הודעה כאמור ובקשתו לא נענתה בחלוף 30 ימים.[296]
- **זכות עיון:** בעל שליטה במאגר מידע אשר לא כיבד את זכות העיון של נושא המידע.[297]

---

[292] סעיף 17ו(ב), (ג), (ד), (ה) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[293] 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 חוקה, עו״ד מנחמי; ס׳ 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.

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

[295] סעיף 15א לחוק הגנת הפרטיות, לעיל ה״ש 9. להלן יפורטו רק סעיפי ההפרות הרלוונטיים למפלגה ו/או למפעיל יישומון בחירות.

[296] סעיף 15א(א)(2) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[297] סעיף 15א(א)(3) לחוק הגנת הפרטיות, לעיל ה״ש 9.

- **זכות תיקון:** בעל שליטה במאגר מידע אשר הסכים לבקשת תיקון שהגיש נושא המידע, אך לא ביצע אותה או לא הודיע על השינויים שיש לבצע בעקבותיה לכל מי שקיבל ממנו את המידע, במסגרת הזמן הקבועה בחוק הגנת הפרטיות.[298]
- **זכות תיקון:** בעל שליטה במאגר מידע אשר סירב לבקשת תיקון, אך לא הודיע על כך לנושא המידע שביקש את התיקון במסגרת הזמנים הקבועה בחוק הגנת הפרטיות.[299]

בפסיקת גובה הפיצוי לדוגמה על בית המשפט להימנע מלהביא בחשבון את גובה הנזק שנגרם לנושא המידע אבל להביא בחשבון מגוון שיקולים אחרים, כגון עידוד התובע למימוש זכויותיו, היקף ההפרה וחומרתה, התנהגות המפר, נסיבותיו האישיות ויכולתו הכלכלית וכן אמצעי אכיפה נוספים או תשלום נוסף שהוחלו עליו לגבי אותן הפרות.[300]

על מפלגה או מפעיל יישומון לתת את הדעת לכך שתביעה לפיצויים לדוגמה עשויה להיות מוגשת **בכל עת**, במסגרת תקופת ההתיישנות הקבועה בחוק הגנת הפרטיות ובהתאם לסד הזמנים המתואר בסעיף 15א לחוק הגנת הפרטיות. זאת, בניגוד לפעולות חקירה ואכיפה מצד הרשות להגנת הפרטיות המוגבלות בקיומן ובהיקפן במהלך תקופת בחירות לפי פרק ד'5.[301]

המקרים בהם יוכל אדם לפנות בתביעה לפיצויים לדוגמה בגין עיבוד מידע אישי אודותיו על ידי מפלגה ו/או מפעיל יישומון בחירות הם:

- מפלגה ו/או מפעיל יישומון בחירות האוספים מידע אישי באמצעות פנייה לאדם מבלי למסור לו הודעה כנדרש לפי סעיף 11, ומבלי להיענות לדרישתו לקבל הודעה כאמור בתוך 30 יום מדרישתו.
- מפלגה שאינה מכבדת את זכותו של האדם לעיון.
- מפלגה מסכימה לבקשת תיקון שהגיש לה אדם שפרטיו במאגר המידע שלה, אך לא ביצעה את התיקון או לא הודיעה על כך לצדדים שלישיים אליהם העבירה את המידע.
- מפלגה מסרבת לבקשת תיקון שהגיש לה אדם שפרטיו נמצאים במאגר המידע שלה, אך לא מודיעה על כך למבקש בהתאם לנדרש בחוק.

5. תקופת התיישנות

תקופת ההתיישנות על תביעה אזרחית בגין פגיעה בפרטיות הייתה לאורך שנים קצרה משמעותית מזו הנהוגה ביחס לתביעות נזיקיות רגילות,[302] ועמדה על שנתיים בלבד.[303] בתיקון 13 הוחלט להשוות את תקופת ההתיישנות לשבע שנים כמקובל בגין תביעות אזרחיות.[304]

---

[298] סעיף 15א(א)(4) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[299] סעיף 15א(א)(5) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[300] סעיף 15א(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[301] סעיף 23נח לחוק הגנת הפרטיות, לעיל ה"ש 9, וכן הדיון בטקסט הנלווה להי"ש 305– 322.

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

[303] סעיף 26 לחוק הגנת הפרטיות, לעיל ה"ש 9.

[304] סעיף 34 לתיקון 13, ה"ש 9 לעיל, המבטל את סעיף 26 בחוק הגנת הפרטיות לפני תיקון 13.

לפיכך, תביעה נגד מפלגה או מפעיל יישומון בחירות בגין הפרת הוראות חוק הגנת הפרטיות ופגיעה בפרטיות עשויה להיות מוגשת במהלך 7 שנים מיום התרחשותה בלי קשר לתקופת בחירות או למועד התרחשותה של הפגיעה.

פרק שמיני

פיקוח ואכיפה מצד הרשות להגנת הפרטיות, בזמן רגיל ובתקופת בחירות

תיקון 13 נועד מראשיתו לשפר את יכולות הפיקוח והאכיפה של ראש הרשות להגנת הפרטיות, ואכן סמכויות האכיפה והפיקוח שהוספו בו רחבות. אומנם את חלקן מנועה הרשות להפעיל בתקופת בחירות, אלא אם התקבל לכך אישור יושב ראש ועדת הבחירות המרכזית, אך הגבלת סמכויות האכיפה והפיקוח של הרשות בתקופת הבחירות אינה מתן פטור מחקירה ואכיפה. מדובר רק בהשהיה, ובסיום תקופת הבחירות הרשות רשאית לפעול, ומפלגה או מפעיל יישומון עשויים להיות צפויים לעיצומים כספיים או אמצעי אכיפה מינהלית אחרים. בפרק זה נבהיר את סמכויות הפיקוח האלה.

1. סמכות ראש הרשות להגנת הפרטיות בתקופת בחירות: ההסדר הכללי

תיקון 13 הוסיף לחוק הגנת הפרטיות את פרק ד'5 המתווה הסדר מיוחד להפעלת סמכויות פיקוח ואכיפה מינהלית בתקופת בחירות לכנסת,[305] ביחס למאגר מידע שמפלגה[306] היא בעלת השליטה בו.[307] ההסדר מונע מראש הרשות, מפקח או חוקר להפעיל סמכויות מסוימות בתקופת בחירות כאשר מדובר בהפרות הנוגעות למאגר מידע שמפלגה היא בעלת השליטה בו, ושמפלגה או מחזיק מטעמה ביצעו. מועד ביצוע ההפרה לא משנה, וגם אם ההפרה בה נחשדת מפלגה אירעה לפני תחילת תקופת הבחירות, מרגע שהחלה תקופת הבחירות לא תוכל הרשות להפעיל את אחת מהסמכויות המפורטות להלן, ללא אישור יו"ר ועדת הבחירות המרכזית.[308]

דברי ההסבר של החוק וכן דברי יו"ר ועדת החוקה של הכנסת, מלמדים כי תכלית ההגבלה היא למנוע ניצול לרעה של סמכויות הפיקוח והאכיפה המינהלית שניתנו לרשות בתיקון 13, לצורך ניגוח פוליטי של מפלגה או מפלגות מסוימות.[309]

נעיר, כי אנו סבורות שמדובר בהסדר בעייתי, המעניק הגנה לזכות להיבחר, כלומר למפלגות ולפועלים מטעמן, אך אינו מספק הגנה מספקת על הבוחרים ועל זכותם לבחור ללא שיופעלו עליהם מניפולציות מבוססות מידע אישי. ההסדר אינו מתייחס למקרים שבהם עלולה להתקיים פגיעה משמעותית בזכות

---

[305] "תקופת בחירות לכנסת" מוגדרת כ"תקופה שתחילתה ביום הקובע, כהגדרתו בחוק מימון מפלגות, התשל"ג–1973, וסיומה ביום פרסום תוצאות הבחירות לפי סעיף 11 לחוק-יסוד: הכנסת;". ראו סעיף 23נח לחוק הגנת הפרטיות, לעיל ה"ש 9.

[306] "מפלגה" מוגדרת כך: "כהגדרתה בחוק המפלגות, התשנ"ב–1992, ולעניין החלק מתקופת בחירות לכנסת המתחיל ביום שלאחר המועד האחרון להגשת רשימת מועמדים לכנסת לוועדת הבחירות המרכזית, - מפלגה כאמור שהגישה רשימת מועמדים המשתתפת בבחירות לכנסת;". ראו סעיף 23נח לחוק הגנת הפרטיות, לעיל ה"ש 9.

[307] ההסדר חל גם במהלך תקופת בחירות לרשויות מקומיות ביחס למאגר מידע שמועמד בבחירות לרשות המקומית הוא בעל השליטה בו. סעיף 23נט לחוק הגנת הפרטיות, לעיל ה"ש 9.

[308] פרוטוקול מס' 313 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ח' בניסן התשפ"ד (16 באפריל 2024), בעמ' 13.

[309] הצעת החוק הממשלתית, לעיל ה"ש 180, דברי ההסבר בעמ' 441; פרוטוקול מס' 313 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ח' בניסן התשפ"ד (16 באפריל 2024), בעמ' 5–6, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

לפרטיות ונדרשת פעולה דחופה לשם עצירת הפגיעה בזמן אמת, וכך עלול להיווצר מצב שבו ההגנה על הזכות לפרטיות מגיעה מעט מידי ומאוחר מידי, והשהיית הבירור והחקירה עלולה לפגוע ביכולת הרשות להגנת המציאות להפעיל כלי אכיפה בדיעבד. הגנת המפלגות באמצעות הסדר זה צורמת עוד נוכח היעדר הכלים שיש בידי אזרח מן השורה שמפלגה פוגעת בזכותו לפרטיות במהלך תקופת בחירות. זה האחרון אינו יכול לפנות ליו"ר ועדת הבחירות המרכזית בעתירה להפסקת ההפרה, משום שחוק הבחירות אינו מסמיך את יו"ר ועדת הבחירות לדון בנושאים הקשורים לחוק הגנת הפרטיות.[310]

הסדר ראוי יותר – כחלופה לצורך לפנות ליו"ר ועדת הבחירות – היה למשל מאפשר למפלגה להגיש ערעור לבית משפט השלום על הוראת ראש הרשות להפסקת הפרה, לפי סעיף 23כה לחוק הגנת הפרטיות, כך שמרגע הגשת הערעור ועד החלטת בית המשפט לא תידרש המפלגה להפסיק את ההפרה.[311]

כך או כך, הסמכויות שהפעלתן בתקופת בחירות דורשת שראש הרשות לפרטיות יקבל אישור מראש מיושב ראש ועדת הבחירות המרכזית הן:[312]

(1) סמכות להיכנס למקום למטרות פיקוח על ביצוע הוראות לפי פרקים ב', ד' ו־ה', ופיקוח על ביצוע הוראות שראש הרשות מוסמך להורות על הפסקתן לפי סעיף 23כה, לרבות הוראות הקשורות בחובת ההודעה לרשות להגנת הפרטיות לפי סעיף 8א(ב), איסור עיבוד שלא למטרה שנקבעה למאגר לפי סעיף 8(ב), עיבוד בחריגה מהרשאה לפי סעיף 8(ג), חובת הודעה לאדם נושא המידע לפי סעיף 11, חובת ההודעה בעת פנייה בדיוור ישיר לפי סעיף 17ו, כיבוד זכות העיון, התיקון והמחיקה והגבלת העברת מידע אישי בהקשר של דיוור ישיר לפי סעיפים 13, 14 ו־17ו בהתאמה, איסור על עיבוד מידע במאגר מידע אם המידע נוצר, התקבל, נצבר או נאסף בניגוד לחוק לפי סעיף 8(ד), חובת אבטחת מידע לפי סעיף 17 ועיבוד מידע תוך הפרת הוראות מסוימות בתקנות אבטחת מידע, ביצוע הוראות הקשורות לדיוור ישיר, או הוראות הקשורות במינוי ממונה הגנת פרטיות.[313]

(2) סמכות לפנות לבית משפט בבקשה לצו חיפוש ותפיסה או צו חדירה לחומר מחשב כאשר יש לו יסוד סביר להניח שבוצעה הפרה של הוראות סעיף 23כה.[314]

(3) סמכות לפנות לבית משפט לעניינים מינהליים לתת צו להפסקת פעולות עיבוד מידע הגורמות או שיש חשש שיגרמו להפרת עקרון צמידות המטרה בסעיף 2(9), האיסור על עיבוד מידע שלא למטרה שנקבעה לו בדין לפי סעיף 8(ב) , האיסור על עיבוד מידע ללא הרשאה לפי סעיף 8(ג), האיסור על עיבוד מידע שנוצר בניגוד לחוק לפי סעיף 8(ד) או חובת אבטחת מידע לפי סעיף 17.[315]

(4) סמכות לתפוס כל חפץ שיש לחוקר יסוד סביר להניח שהוא קשור לעבירה של פגיעה במזיד בעקרון צמידות המטרה או שהוא קשור לעבירה על הוראות פרק ב' או עבירה לפי פרק ד'4, הכוללות בין השאר הכללה בכוונה להטעות פרטים שגויים בהודעה לרשות לפי סעיף 8א(ב),

---

[310] תב"כ 13/23 **בן מאיר ואח' נ' הליכוד ואח'**, ועדת הבחירות המרכזית לכנסת ה־23 (18.2.2020), וכן הדיון בטקסט הנלווה להע"ש 101–105 לעיל.

[311] סעיף 23כה(ו) לחוק הגנת הפרטיות, לעיל ה"ש 9. ראו גם פרוטוקול מס' 313 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ח' בניסן התשפ"ד (16 באפריל 2024), בעמ' 13–15 דברי ד"ר אריאל-הרשקוביץ, דברי עו"ד אור-חוף.

[312] סעיף 23נט(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[313] סעיף 23נט(א)(1) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[314] סעיף 23נט(א)(2) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[315] סעיף 23נט(א)(3) לחוק הגנת הפרטיות, לעיל ה"ש 9.

ומסירת פרטים לא נכונים בכוונה להטעות באשר למסירת המידע האישי במסגרת הודעה לנושא המידע לפי סעיף 11.[316]

(5) סמכות לבקש מבית משפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב ולבצעו, כאשר יש לחוקר יסוד סביר לחשד שנעברה עבירה של פגיעה במזיד בעקרון צמידות המטרה, עבירה על הוראות פרק ב' או עבירה לפי פרק ד'4.[317]

(6) סמכות למסור הודעה על כוונה להטיל עיצום כספי כאשר יש לו יסוד סביר להניח שמקבל ההודעה הפר הוראה מההוראות המנויות בסעיף 23כו לחוק הגנת הפרטיות, לרבות אי מתן הודעה לרשות או עדכונה לפי סעיף 8א(ב), אי כיבוד זכות העיון או התיקון לפי סעיפים 13 ו־14, אי כיבוד זכות נמען בדיוור ישיר להימנע מהעברת מידע אודותיו לאנשים מסוימים לפי סעיף 17ו(ד), אי מתן הודעה לנושא מידע לפי סעיף 11, פנייה בדיוור ישיר מבלי לספק פרטים הנדרשים לפי סעיף 17ו(א), או עיבוד מידע ממאגר למטרה שאינה כדין או עיבוד מידע שלא למטרה שנקבעה לפי סעיף 8(ב).[318]

(7) סמכות למסור לאדם התראה מינהלית אם יש לו יסוד סביר להניח כי אותו אדם הפר אחת מההוראות המנויות בסעיף 23כו לחוק הגנת הפרטיות והתקיימו הנסיבות שקבע שר המשפטים.[319]

(8) סמכות למסור לאדם הודעה על אפשרותו להגיש כתב התחייבות ולהפקיד ערבון במקום עיצום כספי, ובלבד שלראש הרשות יסוד סביר להניח שמקבל ההודעה הפר הוראה מהוראות סעיף 23כו לחוק הגנת הפרטיות והתקיימו הנסיבות שקבע שר המשפטים.[320]

לפני מתן אישור, על יושב ראש ועדת הבחירות המרכזית לתת למפלגה הזדמנות להשמיע את טענותיה, אלא אם מדובר בהפעלת סמכות לפי סעיפים (1)-(5) לעיל וטעמי דחיפות מצדיקים קבלת החלטה מבלי לתת למפלגה הזדמנות לטעון את טענותיה, או שיהיה בכך כדי לסכל את מטרת הפעלת הסמכות המבוקשת. במקרה כזה על יושב ראש ועדת הבחירות המרכזית לפרט את נסיבות העניין או טעמי הדחיפות אשר הצדיקו את אי מתן האפשרות למפלגה לטעון את טענותיה.[321] יושב ראש ועדת הבחירות המרכזית רשאי להתנות בתנאים את האישור להפעלת אחת מהסמכויות האלה.

המבחן שבו על יושב ראש ועדת הבחירות המרכזית להשתמש בהחלטה לגבי מתן היתר להפעיל את סמכות האכיפה, הוא מבחן מידתיות. כלומר, יו"ר ועדת הבחירות צריך להשתכנע שהפעלת הסמכות לא תפגע באופן מהותי ביכולתה של המפלגה להתמודד בבחירות או לנהל את הקשר עם ציבור הבוחרים, ושפגיעה זו לא תעלה בעוצמתה על הסיכון לפגיעה בפרטיות ופגיעה באינטרס הציבורי העומד בבסיס הפעלת הסמכות.[322] להלן, נבהיר את הסמכויות המוגבלות בתקופת בחירות, ולאחר מכן נעסוק בסמכויות שאינן מוגבלות.

---

[316] סעיפים 23נט(א)(4), 23נד, 23נו לחוק הגנת הפרטיות, לעיל ה"ש 9.

[317] סעיף 23נט(א)(5) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[318] סעיף 23נט(א)(6) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[319] סעיף 23נט(א)(7) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[320] סעיף 23נט(א)(8) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[321] סעיף 23נט(ג) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[322] סעיף 23נט(ד) לחוק הגנת הפרטיות, לעיל ה"ש 9.

2. סמכויות הרשות להגנת הפרטיות, המוגבלות בתקופת בחירות

2.1. סמכויות פיקוח, אכיפה ובירור מינהלי

מפקח מטעם הרשות להגנת הפרטיות מוסמך לבצע כל אחת מהפעולות המפורטות בסעיף 23י לחוק, ובכללן כניסה למקום או דרישה מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך או עותק מחומר מחשב,[323] לשם פיקוח על הוראות החוק לפי פרקים ב׳, ד׳ ו־ה. הוראות אלה כוללות בין השאר הוראות בדבר חובת אבטחת מידע,[324] חובת מינוי ממונה הגנת פרטיות,[325] חובת מתן הודעה לרשות להגנת הפרטיות בדבר קיומו של מאגר מידע,[326] חובת מתן הודעה לאדם בעת פנייה אליו לשם קבלת מידע לעיבודו,[327] חובת צירוף הודעה לפנייה בדיוור ישיר,[328] איסור עיבוד שלא למטרה שנקבעה למאגר,[329] או כיבוד זכויות נושא המידע לעיון, תיקון, ומחיקה והגבלת העברת מידע אישי בהקשר של דיוור ישיר.[330]

כן מוסמך מפקח מטעם הרשות לבצע כל אחת מהפעולות המפורטות בסעיף 23י לחוק לשם פיקוח על ביצוע הוראות שבגין הפרתן רשאי ראש הרשות להגנת הפרטיות להורות על הפסקת ההפרה,[331] כגון עקרון צמידות המטרה,[332] איסור עיבוד מידע ללא הרשאה מבעל השליטה,[333] או לשם פגיעה בפרטיות.[334] כמו כן, בסמכותו של המפקח להחליט לפתוח בהליך בירור מינהלי אם יש לו יסוד סביר להניח שבוצעה הפרה של אחת מהוראות אלו,[335] או אחת מהוראות החוק שבגין הפרתה ניתן להטיל עיצום כספי.[336] במסגרת בירור מינהלי רשאי מפקח לפנות לבית משפט בבקשה לקבל צו חיפוש ותפיסה או צו חדירה לחומר מחשב ולבצעו בהתאם להוראות בית המשפט.[337] כמו כן, במקרים בהם לראש הרשות יסוד סביר לחשד שניתן אף לפתוח בחקירה פלילית בגין המעשה או המחדל הנחקרים, בסמכותו להחליט האם לקיים בירור מינהלי או חקירה פלילית.[338]

---

[323] סעיף 23י לחוק הגנת הפרטיות, לעיל ה״ש 9.

[324] סעיף 17 בחוק הגנת הפרטיות, לעיל ה״ש 9, וכן הדיון בטקסט הנלווה להי״ש 200–208לעיל.

[325] סעיף 17ב לחוק הגנת הפרטיות, לעיל ה״ש 9, וכן הדיון בטקסט הנלווה להי״ש 209–228 לעיל.

[326] סעיף 8א(ב)(1), (3) לחוק הגנת הפרטיות, לעיל ה״ש 9, וכן הדיון בטקסט הנלווה להי״ש 198–199 לעיל.

[327] סעיף 11 לחוק הגנת הפרטיות, לעיל ה״ש 9, וכן הדיון בטקסט הנלווה להי״ש 285–289 לעיל.

[328] סעיף 17ו לחוק הגנת הפרטיות, לעיל ה״ש 9, וכן הדיון בטקסט הנלווה להי״ש 290–291 לעיל.

[329] סעיף 8(ב) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[330] סעיפים 13, 13א, 14 ו־17ו לחוק הגנת הפרטיות, לעיל ה״ש 9.

[331] סעיף 23כו בחוק הגנת הפרטיות, לעיל ה״ש 9, והדיון בטקסט הנלווה להי״ש 341–346 לעיל.

[332] סעיף 2(9) ו־8(ב) בחוק הגנת הפרטיות, לעיל ה״ש 9, וכן הדיון בטקסט הנלווה להי״ש 243–250 לעיל.

[333] סעיף 8(ג) לחוק הגנת הפרטיות לפני תיקון 13, ה״ש 1 לעיל, וכן הדיון בטקסט הנלווה להי״ש 280–282 לעיל.

[334] סעיף 2 לחוק הגנת הפרטיות, לעיל ה״ש 9.

[335] סעיף 23כה לחוק הגנת הפרטיות, לעיל ה״ש 9.

[336] סעיף 23כו לחוק הגנת הפרטיות, לעיל ה״ש 9.

[337] סעיפים 23יד, 23טו לחוק הגנת הפרטיות, לעיל ה״ש 9.

[338] סעיף 23טז לחוק הגנת הפרטיות, לעיל ה״ש 9.

בנוסף, במקרה של חשד לפגיעה במזיד בעקרון צמידות המטרה לפי סעיף 2(9) או עבירה אחרת לפי חוק הגנת הפרטיות, רשאי החוקר לחקור כל אדם הקשור לעבירה, לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא קשור לעבירה או לבקש מבית המשפט צו חיפוש ותפיסה.[339]

אולם, בתקופת בחירות לא יכול ראש הרשות או מפקח או חוקר מטעמו להיכנס למקום, לתפוס כל חפץ או להגיש בקשה לצו חיפוש ותפיסה או צו חדירה למחשב.[340]

2.2. צו להפסקת פעולות עיבוד או למחיקת מידע אישי

סעיף 23מט שהוסף בתיקון 13 מעגן מנגנון למתן הוראה להפסקת עיבוד מידע במאגר מידע בעקבות הפרת אחת מהוראות החוק המפורטות בו. מטרתו היא לתת מענה למקרים בהם יש לראש הרשות להגנת הפרטיות חשד סביר שמבוצעת או עלולה להתבצע הפרה חמורה ולהפסיק אותה באופן מיידי. מקרים אלה הם:

- הפרת איסור על שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה (סעיף 2(9)).[341]
- הפרת איסור על עיבוד מידע אישי במאגר מידע שלא למטרת המאגר שנקבעה לו כדין (סעיף 8(ב)).[342]
- הפרת איסור על עיבוד מידע ללא הרשאה או בחריגה ממנה (סעיף 8(ג)). למשל, כאשר מפעיל יישומון בחירות, שהוא מחזיק במאגר מידע של מפלגה, יעבד מידע ממאגר המידע של המפלגה לצורך שליחת פרסומות מותאמות אישית למוצר צריכה.
- הפרת איסור על עיבוד מידע במאגר מידע כאשר המידע האישי הכלול במאגר המידע נוצר, התקבל, נצבר או נאסף בניגוד לחוק או לכל דין אחר המסדיר עיבוד מידע (סעיף 8(ד)).[343]
- הפרת חובת אבטחת מידע (סעיף 17).
- מסירת מידע אישי מגוף ציבורי שלא בהסכמת נושא המידע או פרסומו שלא בסמכות כדין (סעיף 23ב).

במקרים אלה יוכל ראש הרשות לפנות לבית המשפט לעניינים מינהליים בבקשה לתת צו לבעל השליטה במאגר המידע או למחזיק, להפסיק את פעולות העיבוד הגורמות להפרה או שיש חשש שיגרמו להפרה, ובמידת הצורך להורות על מחיקת המידע האישי שבמאגר המידע במלואו. בית משפט שהסוגייה תובא לפתחו יבחן את סבירות החשד לביצוע עכשווי או עתידי של ההפרה, ואת מידתיות הסעד המבוקש בצו. במסגרת זו מחיקת מאגר מידע היא סעד קיצון.[344] בית המשפט יבחן גם את מידת הפגיעה האפשרית של הצו המבוקש על הזכות לחופש הביטוי. כן ייתן בית המשפט למפלגה או למפעיל יישומון הבחירות

---

[339] סעיף 23נא(א) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[340] סעיף 23נט(א)(1), (2), (4), (5) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[341] ראו הדיון בטקסט הנלווה להע"ש 243–250 לעיל לעניין הפרה אפשרית של עקרון צמידות המטרה על ידי מפלגה או מפעיל יישומון בחירות.

[342] שם.

[343] שם.

[344] פרוטוקול מס' 347 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, י"ב בסיון התשפ"ד (18 ביוני 2024), בעמ' 31–32; פרוטוקול מס' 351, לעיל ה"ש 213, בעמ' 16–17.

הזדמנות להציג את טענותיהם. צו שניתן במעמד צד אחד מבלי שמפלגה או מפעיל היישומון התגוננו, יעמוד על 48 שעות ובכל מקרה לא יינתן צו מחיקה במעמד צד אחד.[345]

אומנם, בתקופת בחירות לא יכול ראש הרשות להפעיל את סמכותו זו לבקשת צו הפסקה אלא באישור יו"ר ועדת הבחירות המרכזית.[346] אך חשוב להבין שאם ישתכנע יו"ר ועדת הבחירות המרכזיות שיש להפעיל סמכות זו, ובית המשפט ישתכנע שהחשד לביצועה של הפרה הוא סביר וכי הסעד הוא מידתי, הרי שהסעד של הפסקת עיבוד המידע או מחיקת המאגר במקרה קיצון משמעות שיתוק מלא של כלל הפעולות הנשענות על עיבוד המידע שבמאגר המידע.

2.3. הטלת עיצום כספי, התראה מינהלית או דרישת כתב התחייבות והפקדת עירבון

סעיף 23כו, שהוסף לחוק בתיקון 13, מעגן את סמכות ראש הרשות להגנת הפרטיות להטיל על מפלגה או על מפעיל יישומון עיצום כספי בגין הפרת הוראה מההוראות המפורטות בסעיף, כמפורט להלן:[347]

הסעיף בחוק הגנת הפרטיות המופר	על מי יוטל העיצום	ההפרה	סכום העיצום
8א(ב)	בעל שליטה	אי מתן הודעה לרשות להגנת הפרטיות או אי עדכון הרשות בשינוי באחד מהפרטים שיש לכלול בהודעה כאמור.	150,000 ש"ח או כפל הסכום אם במאגר המידע היה מידע אישי על אודות מיליון בני אדם ומעלה.
13	בעל שליטה	סירוב לבקשתו של נושא לעיין במידע אישי אודותיו האגור במאגר המידע	15,000 ש"ח
14(ב)	בעל שליטה	תיקון מידע אישי בעקבות מימוש זכות התיקון על ידי נושא המידע, מבלי ליידע על התיקון את כל מי שקיבל את המידע	15,000 ש"ח
14(ג)	בעל שליטה	אי מתן הודעה לנושא המידע על סירוב לבקשת התיקון	15,000 ש"ח
14(ד)	מחזיק	אי תיקון מידע אישי שבהחזקתו	15,000 ש"ח
11	בעל שליטה ומחזיק	פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע מבלי למסור לו הודעה כנדרש	מכפלה של 50 ש"ח במספר בני האם שאליהם נעשתה פנייה או דרישה מכפלה של 100 ש"ח או הפנייה או הדרישה היא לגבי מידע בעל רגישות מיוחדת. או 30,000 ש"ח בהוראות ראש הרשות
11	בעל שליטה ומחזיק	פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר, והפנייה נעשתה לקבוצה בלתי מסוימת של בני אדם, ללא מתן הודעה כנדרש בסעיף 11 לחוק הגנת הפרטיות	2 ש"ח לכל אדם שיש עליו מידע אישי במאגר או 4 ש"ח אם המידע הוא בעל רגישות מיוחדת או 20,000 ש"ח ביחס למידע אישי ו־ 40,000 ש"ח ביחס למידע בעל רגישות

[345] שם, בעמ' 38, 42; פרוטוקול מס' 351, לעיל ה"ש 213, בעמ' 17, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

[346] סעיף 23נט(א)(3) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[347] סעיף 23כו לחוק הגנת הפרטיות, לעיל ה"ש 9. להלן יפורטו רק הפרות העשויות להיות רלוונטיות למפלגה כבעלת שליטה ו/או למפעיל יישומון בחירות כמחזיק.

הסעיף בחוק הגנת הפרטיות המופר	על מי יוטל העיצום	ההפרה	סכום העיצום
			מיוחדת, בהוראת ראש הרשות להגנת הפרטיות
17ב(א)	בעל שליטה ומחזיק	אי מינוי ממונה אבטחת מידע	2 ש״ח לכל אדם שיש עליו מידע אישי במאגר או 4 ש״ח אם המידע הוא בעל רגישות מיוחדת. או 20,000 ש״ח ביחס למידע אישי ו־ 40,000 ש״ח ביחס למידע בעל רגישות מיוחדת, בהוראת ראש הרשות להגנת הפרטיות.
17ב1(א)(1) או (2)	בעל שליטה ומחזיק	אי מינוי ממונה הגנת פרטיות	2 ש״ח לכל אדם שיש עליו מידע אישי במאגר או 4 ש״ח אם המידע הוא בעל רגישות מיוחדת. או 20,000 ש״ח ביחס למידע אישי ו־ 40,000 ש״ח ביחס למידע בעל רגישות מיוחדת, בהוראת ראש הרשות להגנת הפרטיות.
17ו(ב), (ד)	בעל שליטה ומחזיק	לא נענה לדרישתו של אדם שמידע המתייחס אליו יימחק ממאגר המשמש לדיוור ישיר	15,000 ש״ח
17ו(ג), (ד)	בעל שליטה	לא נענה לדרישתו של אדם שמידע אישי אודותיו שעל פיו בוצעה פניה בדיוור ישיר לא יימסר לאדם, לסוג בני אדם או לאנשים מסוימים	15,000 ש״ח
17ו(א)	בעל שליטה ומחזיק	פניה לאדם בדיוור ישיר מבלי לציין בפניו שמדובר בדיוור ישיר, לספק את זהותו ומענו של בעל השליטה, לפרט את המקורות מהם קיבל בעל השליטה את המידע שבמאגר ולספק לנמען הפניה מידע בדבר זכותו להימחק מהמאגר	מכפלה של 50 ש״ח במספר בני האם שאליהם נעשתה פנייה או דרישה מכפלה של 100 ש״ח או הפנייה או הדרישה היא לגבי מידע בעל רגישות מיוחדת. או 30,000 ש״ח בהוראות ראש הרשות
23כה(ד)	בעל שליטה ומחזיק	הפרת הוראה להפסקת הפרה הוראות הקשורות במינוי ממונה הגנת פרטיות	2 ש״ח לכל אדם שיש עליו מידע אישי במאגר או 4 ש״ח אם המידע הוא בעל רגישות מיוחדת. או 20,000 ש״ח ביחס למידע אישי ו־ 40,000 ש״ח ביחס למידע בעל רגישות מיוחדת, בהוראת ראש הרשות להגנת הפרטיות.
23כה(א)	בעל שליטה ומחזיק	אי מילוי הוראת ראש הרשות להפסקת הפרה עקב הפרת עקרון צמידות המטרה שבס׳ 2(9) לחוק הגנת הפרטיות או בגין עיבוד מידע אישי למטרה שמהווה פגיעה בפרטיות לפי ס ; 2 לחוק הגנת הפרטיות	4 ש״ח לכל אדם שיש עליו מידע אישי במאגר או 8 ש״ח אם המידע הוא בעל רגישות מיוחדת. או 20,000 ש״ח ביחס למידע אישי ו־ 40,000 ש״ח ביחס למידע בעל רגישות מיוחדת, בהוראת ראש הרשות להגנת הפרטיות.
23כה(ב)	בעל שליטה	אי מילוי הוראת ראש הרשות להפסקת הפרה עקב הפרת האיסור על עיבוד, או הרשאה לאחר לעבד, מידע במאגר	4 ש״ח לכל אדם שיש עליו מידע אישי במאגר או 8 ש״ח אם המידע הוא בעל רגישות מיוחדת.

הסעיף בחוק הגנת הפרטיות המופר	על מי יוטל העיצום	ההפרה	סכום העיצום
		מידע שנוצר, התקבל, נצבר או נאסף בניגוד לחוק הקבוע בסעיף 8(ד) לחוק הגנת הפרטיות או	או 20,000 ש״ח ביחס למידע אישי ו־ 40,000 ש״ח ביחס למידע בעל רגישות מיוחדת, בהוראת ראש הרשות להגנת הפרטיות.
8(ג)	מחזיק	עיבוד מידע אישי ללא הרשאה או בחריגה מהרשאה	4 ש״ח לכל אדם שיש עליו מידע אישי במאגר או 8 ש״ח אם המידע הוא בעל רגישות מיוחדת. או 200,000 ש״ח בהוראת ראש הרשות להגנת הפרטיות.
8(ב)	בעל שליטה ומחזיק	עיבוד מידע אישי במאגר מידע שלא בהתאם למטרה שנקבעה בנסיבות שבהן היה ניתן לקבוע כדין מטרה כאמור.	לפי פרט 1 בתוספת השלישית לחוק הגנת הפרטיות לאחר תיקון 13.
23י(א)(2) או (3)	בעל שליטה ומחזיק	אי מסירת מסמך או עותק מחומר מחשב לבקשת מפקח	300,000 ש״ח
תקנות לפי סעיף 36	בעל שליטה ומחזיק	הפרת הוראה מהוראות תקנות שהותקנו לפי סעיף 36 לחוק הגנת הפרטיות. אם ההפרה מבוצעת על ידי מחזיק, ראש הרשות רשאי למסור הודעה לבעל השליטה ולהורות לו שיפעל להפסקת ההפרה על ידי המחזיק. אם המחזיק לא מפסיק את ההפרה ובעל השליטה לא מבצע את שנדרש ממנו על ידי ראש הרשות לשם הפסקת ההפרה, יראו אותו כמפר.	בהתאם למפורט בתוספת הרביעית לחוק הגנת הפרטיות.
23כה(ג)	בעל שליטה ומחזיק	אי מילוי הוראה להפסקת הפרת תקנות מתקנות אבטחת מידע בהתאם למפורט בחלק ב׳ לתוספת הרביעית	בהתאם למפורט בתוספת הרביעית לחוק הגנת הפרטיות.

במקום להטיל עיצום כספי, ראש הרשות רשאי למסור לבעל שליטה או מחזיק התראה מינהלית. זאת, כאשר יש לו יסוד סביר להניח כי ישנה הפרת הוראה מההוראות המפורטות בטבלה שלעיל.[348] מפר שמקבל התראה מינהלית רשאי לפנות לראש הרשות להגנת הפרטיות בבקשה לבטל את ההתראה.[349] עם זאת, המשך ההפרה, לאחר קבלת התראה, ייחשב כהפרה נמשכת אשר תוביל להטלת עיצום כספי. כמו כן, הפרה של אותו הסעיף במהלך שנתיים לאחר קבלת ההתראה המינהלית, תיחשב כהפרה חוזרת שגם בגינה ניתן להטיל עיצום כספי.[350]

[348] סעיף 23לו לחוק הגנת הפרטיות, לעיל ה״ש 9.

[349] סעיף 23לז לחוק הגנת הפרטיות, לעיל ה״ש 9.

[350] סעיף 23לח לחוק הגנת הפרטיות, לעיל ה״ש 9.

אפיק חלופי נוסף לעיצום כספי הוא כתב התחייבות והפקדת עירבון, כאשר התקיימו נסיבות המתאימות לפי קביעת שר המשפטים.[351] בכתב ההתחייבות נדרש המפר להתחייב להפסיק את הפרת הוראת החוק הרלוונטית, ולהימנע מהפרה נוספת של אותה הוראה, במהלך תקופה שתקבע על ידי ראש הרשות להגנת הפרטיות, ולא תעלה על שנתיים. כן רשאי ראש הרשות לדרוש בכתב ההתחייבות תנאים נוספים שעל המפר לעמוד בהם לשם הקטנת הנזק שנגרם מההפרה או למניעת הישנותה. בנוסף על כתב ההתחייבות על המפר להפקיד עירבון בסכום העיצום הכספי שראש הרשות היה רשאי להטיל עליו.[352]

בעל שליטה או מחזיק שהוטל עליו עיצום כספי, נמסרה לו התראה מינהלית או שהוא נדרש לחתום על כתב התחייבות ולהפקיד עירבון, יכול לערער על החלטת ראש הרשות להגנת הפרטיות בתוך 45 ימים בפני בית משפט השלום.[353] כן יש להביא בחשבון את חובת ראש הרשות להגנת הפרטיות לפרסם את דבר הטלת עיצום כספי באתר האינטרנט של הרשות להגנת הפרטיות.[354]

כלומר, במקרה של הפרה של אחד הסעיפים המפורטים בטבלה שלעיל, עשויים מפלגה או מפעיל יישומון לחוב בתשלום עיצום כספי או להידרש לחתום על כתב התחייבות והפקדת עירבון. עם זאת, בתקופת בחירות מנועה הרשות מלמסור הודעה על כוונת חיוב, התראה מינהלית או הודעה על האפשרות להגיש כתב התחייבות ולהפקיד עירבון.[355] כלומר הרשות להגנת הפרטיות לא תוכל להטיל על מפלגה או מפעיל יישומון בחירות סנקציות מינהליות במהלך תקופת בחירות, אך אם הן בגין הפרות שהתרחשו קודם לכן.

2.4. האפיק הפלילי

פעולות מסוימות של הפרת החוק עשויות לעלות כדי עבירה פלילית. למשל, הפרעה לראש הרשות, לחוקר או למפקח במילוי תפקידו;[356] הכללת פרטים לא נכונים בהודעה לרשות להגנת הפרטיות לפי סעיף 8א(ב) או במענה לדרישה של מפקח או מומחה חיצוני, מתוך כוונה להטעות את ראש הרשות, מפקח או מומחה חיצוני;[357] עיבוד מידע ללא הרשאה מבעל השליטה בניגוד לסעיף 8(ג);[358] ופנייה לאדם לקבלת מידע אישי לשם עיבודו תוך מסירת פרטים לא נכונים, בכוונה להטעות את אותו אדם באשר למסירת המידע האישי.[359] אומנם הרשות להגנת הפרטיות עשתה שימוש מצומצם יחסית בסמכויותיה הפליליות עד כה,[360] אולם בהחלט יתכן שראשי מפלגה או מפעילי יישומון בחירות יהיו נתונים לחקירה פלילית ואף

[351] סעיף 23לט לחוק הגנת הפרטיות, לעיל ה"ש 9.

[352] סעיף 23מ לחוק הגנת הפרטיות, לעיל ה"ש 9.

[353] סעיף 23מה לחוק הגנת הפרטיות, לעיל ה"ש 9.

[354] סעיף 23מו לחוק הגנת הפרטיות, לעיל ה"ש 9.

[355] סעיף 23נט(א)(6)-(8) לחוק הגנת הפרטיות, לעיל ה"ש 9.

[356] סעיף 23נג לחוק הגנת הפרטיות, לעיל ה"ש 9.

[357] סעיף 23נד לחוק הגנת הפרטיות, לעיל ה"ש 9.

[358] סעיף 23נה לחוק הגנת הפרטיות, לעיל ה"ש 9.

[359] סעיף 23נו לחוק הגנת הפרטיות, לעיל ה"ש 9.

[360] בשנת 2023 קיבלה הרשות להגנת הפרטיות 34 פניות המעלות חשד לעבירה פלילית, נפתחו 10 תיקי חריקה פלילית בגין חשד לעבירות של סחר או שימוש במידע רגיש בניגוד לחוק, נמשכה חקירתם של 5 תיקי חקירה משנת 2022 ו־3 מהם הועברו לעיון הפרקליטות לקבלת הכרעה בדבר הגשת כתב אישום. הוגש כתב אישום אחד. ראו הרשות להגנת הפרטיות, דו"ח פעילות לשנת 2023 (25.11.2024), עמ' 20–21.

להגשת כתב אישום במידה וימצא חשד סביר לעבירות פליליות כאמור. עם זאת, סמכויות אלו מוגבלות בעת תקופת בחירות.[361]

3. סמכויות הרשות להגנת הפרטיות שאינן מוגבלות בתקופת בחירות

3.1. סמכות להורות על הפסקת הפרה

סעיף 23כה שהוסף בתיקון 13 מסמיך את ראש הרשות להורות לבעל שליטה או למחזיק להפסיק הפרה של אחת מהוראות החוק הבאות:

- עקרון צמידות המטרה בסעיף 2(9) לחוק: שימוש בידיעה על ענייניו הפרטיים של אדם במאגר מידע שלא למטרה לשמה נמסר. למשל, כאשר מפלגה או מפעיל יישומון בחירות עושים שימוש במערכת בחירות עכשווית במידע מטויב שבוחר עדכן על עצמו במערכת בחירות קודמת מבלי לקבל את הסכמתו התקפה לכך.[362]
- עיבוד מידע אישי במאגר מידע למטרה שמהווה פגיעה בפרטיות כהגדרתה בסעיף 2 לחוק הגנת הפרטיות. לדוגמה, כשמפלגה או מפעיל יישומון שולחים מסרים פוליטיים מותאמים אישית לבוחר על בסיס עיבוד מידע אישי , שהוזן, ללא ידיעתו או הסכמתו של הבוחר, על ידי משתמש ביישומון, באופן העולה כדי בילוש או התחקות העלולים להטרידו.[363]
- עיבוד, או מתן הרשאה לאחר לעבד, מידע במאגר מידע שנוצר, התקבל, נצבר או נאסף בניגוד לחוק תוך הפרת סעיף 8(ד) לחוק הגנת הפרטיות. למשל, כאשר מאגר המידע של המפלגה המשמש לצורכי התמודדות בבחירות כולל את מידע הפנקס ממערכת הבחירות הקודמת, בניגוד לסעיף 39(ג) לחוק הבחירות.[364]
- עיבוד מידע בניגוד להוראות תקנות אבטחת מידע המנויות בחלק ב׳ לתוספת הרביעית לחוק הגנת הפרטיות.
- הפרת הוראות הקשורות במינוי ממונה הגנת פרטיות, כישוריו, כפיפותו, או הימצאותו בניגוד עניינים.

הוראה על הפסקת הפרה תינתן רק לאחר שראש הרשות נותן לבעל השליטה או למחזיק הזדמנות להשמיע את טענותיו ומודיע לו לאחריה כי מעשיו מהווים הפרה. אופן הפסקת ההפרה ופרק הזמן במהלכו יידרש בעל השליטה או המחזיק להפסיקה ייקבעו על ידי ראש הרשות. בעל שליטה או מחזיק רשאי לערער לבית משפט השלום בתוך 45 ימים מקבלת הוראה כאמור.

סמכות ראש הרשות להורות על הפסקת הפרה זו אינה מוגבלת בתקופת בחירות, ונפקותה המעשית היא הפסקת עיבוד המידע לחלוטין או עד לתיקון ההפרה. כלומר, גם בתקופת בחירות עשויים מפלגה או מפעיל יישומון בחירות למצוא עצמם מנועים מלבצע פעולות המבוססות על עיבוד מידע במאגר מידע.

---

[361] סעיף 23נט(א)(4), (5) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[362] ראו הדיון בטקסט הנלווה לה״ש 243–250 לעיל.

[363] שם.

[364] שם.

למשל, כאשר מאגר המידע ביישומון הבחירות מבוסס על מידע הפנקס ממערכת בחירות קודמת. עם זאת, מפלגה או מפעיל יישומון בחירות רשאים לערער לבית משפט השלום על הוראת ראש הרשות להפסקת הפרה וכך לקנות עוד זמן, שהוא קריטי בתקופת בחירות, ולהמשיך את ההפרה עד לקבלת הוראה אחרת מבית המשפט.

במידה שהמפלגה או מפעיל היישומון ממשיכים להפר על אף הוראתו של ראש הרשות להפסיק את ההפרה, רשאי ראש הרשות להטיל עליהם עיצום כספי. אולם סמכות זו מוגבלת בתקופת הבחירות.[365]

[365] סעיף 23נט(א)(6) לחוק הגנת הפרטיות, לעיל ה"ש 9.

חלק שלישי

המלצות לקראת הבחירות לכנסת ה־26

מבוא

הניתוח בפרקים הקודמים מצביע על פער הולך ומתרחב בין היכולות הטכנולוגיות המשמשות כיום בקמפיינים פוליטיים, לבין המסגרת המשפטית המסדירה את השימוש במידע אישי במערכות בחירות. קמפיינים פוליטיים מבוססי נתונים ובינה מלאכותית מאפשרים איסוף, ניתוח והיסק של מידע על בוחרים בהיקפים ובעומק שלא היו אפשריים בעבר, וכן יצירה והפצה של מסרים פוליטיים מותאמים אישית בקנה מידה רחב. יכולות אלה עשויות לפגוע בפרטיות הבוחרים, ליצור פערי כוח משמעותיים בין מפלגות לבין אזרחים ולהציב אתגרים חדשים לעקרונות היסוד של הליך הבחירות הדמוקרטי, ובראשם הוגנות הבחירות, חשאיות הבחירות וטוהר הבחירות.

כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות מסמנת שינוי משמעותי בתפיסת ההגנה על מידע אישי בישראל, אולם יישומו בהקשר של תעמולת בחירות מעורר שאלות פרשניות ומעשיות שטרם הובהרו. בהיעדר הנחיות ברורות וכלים יישומיים, קיים חשש כי השימוש בטכנולוגיות אלה יתרחב מבלי שתתקיים בקרה מספקת על השלכותיו על פרטיות הבוחרים ועל תקינות ההליך הדמוקרטי.

על רקע זה מוצעות להלן המלצות מדיניות ויישום שמטרתן להבהיר את גבולות השימוש במידע אישי במסגרת קמפיינים פוליטיים, לחזק את יכולת האכיפה והפיקוח של הרשות להגנת הפרטיות ושל ועדת הבחירות המרכזית. הפרק הבא יכלול שאלות בחינה עצמית למפלגות ולמי שפועלים מטעמן כדי לספק להם כלים מעשיים לעמידה בדרישות הדין.

פרק עשירי
המלצות לרשות להגנת הפרטיות

כל עוד לא החלה "תקופת בחירות" לכנסת,[366] עומדים לרשות הרשות להגנת הפרטיות כלי הפיקוח, הבירור והאכיפה המינהלית המעוגנים לאחר תיקון 13 בחוק הגנת הפרטיות. אנו מציעות שהרשות תעשה בהם שימוש כבר עתה, במטרה לשפר את הגנת הפרטיות של בעלי זכות הבחירה, כמפורט להלן:

א. פתיחה בהליכי פיקוח ובירור מינהלי לשם בחינת ציות המפלגה לחובת ההודעה לרשות,[367] והטלת עיצום כספי, התראה מינהלית או כתב התחייבות, על מפלגות שהפרו את חובת ההודעה לרשות.[368]

ב. פתיחה בהליכי פיקוח ובירור מינהלי לבחינה האם עיבוד מידע נעשה בהתאם להוראות תקנות אבטחת מידע,[369] ובמקרים מתאימים גם פניה לבית משפט לעניינים מינהליים בבקשה להוצאה צו להפסקת עיבוד המידע,[370] הוראה למפלגה כבעלת השליטה ולכל מחזיק מטעמה להפסיק את ההפרה במקרים המתאימים, [371] והטלת עיצום כספי, התראה מינהלית או הטלת חובה לכתבה התחייבות עקב הפרת הוראות תקנות אבטחת מידע.[372]

ג. פתיחה בהליכי פיקוח ובירור מינהלי לבחינת מינוי ממונה הגנת פרטיות וציות לדרישות כשירותו ומילוי תפקידיו.[373] הפרת החובה למנות ממונה הגנת פרטיות בארגון או אי עמידה בדרישות כשירות המינוי והתנאים למילוי תפקידו, מקימים לרשות להגנת הפרטיות את הסמכות להורות למפלגה כבעלת השליטה ולכל מחזיק מטעמה להפסיק את ההפרה.[374] כן מוסמך ראש הרשות להגנת הפרטיות להטיל על מפלגה או מחזיק מטעמה עיצום כספי, למסור לה התראה מינהלית או לדרוש את חתימתה על כתב התחייבות והפקדת עירבון עקב הפרת הוראות תקנות אבטחת מידע.[375]

נוסף על סמכויות האכיפה אנו מציעות כי נוכח החידושים שבתיקון 13 וטענות מפלגות בעבר כי אכיפת חוק הגנת הפרטיות היא חדשנית והן לא הבינו את השלכותיה,[376] נכון כבר עכשיו, בטרם החלה תקופת

---

[366] "תקופת בחירות לכנסת" מוגדרת כ"תקופה שתחילתה ביום הקובע, כהגדרתו בחוק מימון מפלגות, התשל"ג–1973, וסיומה ביום פרסום תוצאות הבחירות לפי סעיף 11 לחוק-יסוד: הכנסת;". ראו סעיף 23נח לחוק הגנת הפרטיות, לעיל ה"ש 9.

[367] סעיף 23י לחוק הגנת הפרטיות, לעיל ה"ש 9, וכן הדיון בטקסט הנלווה לה"ש 198–199 לעיל.

[368] סעיפים 23כו, 23לו ו־23לט לחוק הגנת הפרטיות, לעיל ה"ש 9.

[369] סעיף 23י לחוק הגנת הפרטיות, לעיל ה"ש 9.

[370] סעיף 23 מט לחוק הגנת הפרטיות, לעיל ה"ש 9.

[371] סעיף 23כה לחוק הגנת הפרטיות, לעיל ה"ש 9.

[372] סעיפים 23כו, 23לו ו־23לט לחוק הגנת הפרטיות, לעיל ה"ש 9.

[373] סעיף 23י לחוק הגנת הפרטיות, לעיל ה"ש 9, וכן הדיון בטקסט הנלווה לה"ש 209–228 לעיל.

[374] סעיף 23כה לחוק הגנת הפרטיות, לעיל ה"ש 9.

[375] סעיפים 23כו, 23לו ו־23לט לחוק הגנת הפרטיות, לעיל ה"ש 9.

[376] ראו למשל, מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת ישראל ביתנו** (27/01/2021), סעיף 9.3 בעמ' 4. טענה דומה העלתה גם הליכוד. ראו מחלקת האכיפה הרשות להגנת הפרטיות משרד המשפטים, **הודעה בדבר קביעת הפרה של חוק הגנת הפרטיות התשמ"א-1981 – מפלגת הליכוד** (27.1.2021), סעיף 9.17, בעמ' 6.

בחירות, לתדרך את המפלגות בדבר החידושים בתיקון 13 והשלכותיו. בין השאר, חיוני, לדעתנו, להדגיש בפני נציגי המפלגות בפתח מערכת הבחירות לכנסת ה־26 את הנושאים הבאים:

(א) דרישת ההסכמה מדעת

חוק הגנת הפרטיות מתנה כל פגיעה בפרטיותו של אדם בקבלת הסכמתו תקפה, שמשמעה הסכמה מדעת, מרצון חופשי, במפורש או מכללא.[377] לטעמנו, יש לחדד בפני המפלגות כי את המשמעות המעשית של דרישת ההסכמה התקפה, ובכלל זה את הצורך להציג בפני האדם ממנו מתבקש המידע האישי את המידע הנחוץ לו לשם קבלת החלטה האם ברצונו להסכים למסירת המידע או לסרב לה. מידע זה אינו זהה בהכרח למידע שיש להציג בפני אדם בעת פנייה אליו מכוח חובת ההודעה שבסעיף 11 לחוק הגנת הפרטיות. על מנת לקבל הסכמה תקפה יש לתת בידי האדם מידע על כלל סוגי המידע המבוקשים, מטרות השימוש בהם וזהות סוגי הגורמים אליהם יועבר המידע. המידע צריך להיות מוצג בצורה פשוטה וברורה ונגישה, כך שלאדם תהיה אפשרות סבירה להבין את משמעותה והשלכותיה.[378]

כן יש להבהיר למפלגות שההסכמה צריכה להינתן באופן אקטיבי על ידי נשוא המידע ואין להסתפק בהסכמה פסיבית (opt out) זאת נוכח רגישות המידע הנאסף ועיבודו למטרות דיוור ישיר. בנוסף, על המפלגות להבין ששימוש בכלים עיצוביים וטקטיקות אפלות (dark patterns) שמטרתן להקשות על נושא המידע להבין את משמעות הסכמתו ולהשפיע באופן פסול על החלטתו, עלול לפגוע ברכיב הרצון החופשי ומכאן שבתקפותה של ההסכמה. יתרה מכך, חומרת הפגיעה בזכות לפרטיות עקב עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר וההשלכות האפשריות של עיבוד כאמור על הזכות לבחור מצדיקים דרישה שההסכמה תעשה במפורש ואין להסתפק בהסכמה מכללא.

במסגרת זו יש להדגיש בפני המפלגות שכל משתמש ביישומון לניהול בחירות, המזין פרטי מידע אישי או מידע בעל רגישות מיוחדת על אדם אחר, לרבות פרטים כגון כתובת דוא״ל או סטטוס תמיכה במפלגה, מזין מידע אישי ואף מידע בעל רגישות מיוחדת וחייב לקבל לפני הזנת הנתונים ליישומון, את הסכמתו התקפה, מדעת ומרצון חופשי, של נושא המידע. אין די בהצגת מסר, עם התקנת היישומון, לפיו באחריות המשתמש לקבל את הסכמת הבוחר אותו הוא מתשאל או שעליו הוא מזין מידע אישי לפני הזנתו ליישומון. על המפלגה לנקוט פעולות הסברתיות בקרב המשתמשים ביישומון, לצד הוספת חסמים טכנולוגיים שיש בהם כדי להעלות את המודעות לצורך בקבלת הסכמה תקפה. למשל, כל אימת שמשתמש ביישומון מבקש להזין מידע אישי אודות בוחר, תופיע חלונית בה יתבקש המשתמש לאשר שקיבל את הסכמתו נתקפה של הבוחר, תוך פירוט קצר של דרישות ההסכמה התקפה וההשלכות האפשריות על משתמש המאשר מבלי לקבל הסכמה כאמור בפועל.

(ב) הקפדה על עקרון צמידות המטרה

מטרות המאגר הנקבעות על ידי מפלגה חייבות לעמוד במסגרת המטרות החוקיות הקבועה בסעיף 39(ג) לחוק הבחירות, כלומר ״לצורכי התמודדות בבחירות ולצרכי קשר עם ציבור הבוחרים״.[379] עקרון צמידות

[377] להרחבה ראו הטקסט הנלווה לה״ש 229–242.

[378] הרשות להגנת הפרטיות, גילוי דעת בנושא הסכמה, לעיל ה״ש 229.

[379] ראו הדיון בטקסט הנלווה לה״ש 267–270 לעיל.

המטרה הוא עיקרון יסוד בדיני הגנת הפרטיות ומחייב שעיבוד מידע אישי במאגר המידע יעשה אך ורק למטרה לשמה נמסר המידע ולמטרת המאגר שנקבע כדין.[380] אולם, במערכת הבחירות לכנסת ה־23 פורסם ברבים אופן תקנת היישומון "אלקטור", ששימש את מפלגת הליכוד, ונעשו מאמצים נרחבים להגדיל את בסיס משתמשיו. כתוצאה כל אחד, פעיל במפלגה ואף אזרח זר, שאינו מתגורר כלל בישראל, יכול היה להתקין את היישומון ולחפש בו פרטים אודות 50 נושאי מידע. אפשרות זו היא שהובילה גם לאזהרתו של ראש המוסד לשעבר, מר תמיר פרדו, שהשימוש ביישומון אלקטור עלול להביא לפגיעה חמורה בביטחון המדינה.[381] בנוסף, אפשרותו של כל אחד להתקין את היישומון ולהשתמש בו לצרכיו מונעת מהמפלגה וממפעילי היישומון, המוגדרים כבעלי מאגר המידע והמחזיק בו, בהתאמה,[382] לעמוד בדרישת קיום המטרה.

משום כך, לדעתנו, יש לחזור ולהבהיר למפלגות את משמעות עקרון צמידות המטרה ואחריות המפלגה להבטיח שלא יעובד מידע אישי באופן המפר את עקרון צמידות המטרה, לרבות על ידי נקיטת אמצעים טכנולוגיים המונעים ממשתמשי יישומון בחירות לעשות שימוש במידע שבמאגר המידע שביישומון למטרות שונות מאלו שנקבעו על ידי המפלגה במסמך הגדרות המאגר. זאת לצד נקיטת צעדי אכיפה מהירים ומיידיים במידה שיתקבל מידע על שיווק דומה של יישומון לניהול בחירות במהלך מערכת הבחירות לכנסת ה־25.

(ג) דרישת אבטחת המידע

לדעתנו, יש לחדד בקרב המפלגות את משמעותן של דרישות תקנות אבטחת מידע. במסגרת זו חשוב להבהיר את הדרישה שיוענקו הרשאות גישה רק במידה הנדרשת לצורך מילוי תפקידו של מקבל ההרשאה,[383] וכן את החובה לוודא שמי שניגש למאגר המידע הוא מורשה הגישה באמצעות אימות זהותו. בהנחה שרמת האבטחה שחלה על מאגר המידע שבשליטת המפלגה היא בינונית או גבוהה,[384] אימות הזהות של מורשה הגישה צריך להיעשות ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. למשל, תעודה המכילה חתימה אלקטרונית מאובטחת.[385] על המפלגות להבין שדרישות אלו צריכות לחול על כל מי שמקבל מהן הרשאת גישה למאגר המידע, ולא רק על עובדי המפלגה או החברה המפעילה את היישומון. כלומר, יש להחילן גם על כל פעיל מפלגה או מתנדב המקבל הרשאת גישה לעשות שימוש ביישומון מטעם או לטובת המפלגה.

---

[380] סעיפים 2(9) ו8(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9. כן ראו הדיון בטקסט הנלווה להע"ש 243–250 לעיל.

[381] שירות כלכליסט "תמיר פרדו: 'אלקטור היא הקורונה הביטחונית של מדינת ישראל – הסירו אותה'" **כלכליסט** (26.2.2020); יוסי מילמן "למי איראן צריכה להודות על חשיפת פנקס הבוחרים? שבעה גופים" **הארץ** (17.2.2020).

[382] הרשות להגנת הפרטיות, מחלקת אכיפה, קביעת הפרה של חוק הגנת הפרטיות, התשמ"א – 1981 (27.01.21) (סימוכין 008-2021-00000695; 008-2021-00000712).

[383] תקנה 8(א) לתקנות אבטחת מידע, לעיל ה"ש 110.

[384] מאגר מידע שחלה עליו רמת האבטחה הבינונית הוא, למשל, מאגר מידע המכיל מידע בעל רגישות מיוחדת. מאגר מידע שחלה עליו רמת האבטחה הגבוה הוא כזה שחלה עליו רמת האבטחה הבינונית, אך יש בו מידע על 100,000 אנשים ומעלה או שמספר בעלי ההרשאה בו עולה על 100. ראו התוספת הראשונה והשניה לתקנות אבטחת מידע, לעיל ה"ש 110.

[385] תקנה 9 לתקנות אבטחת מידע, לעיל ה"ש 110. כן ראו הרשות להגנת הפרטיות, המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע).

כן יש להבהיר למפלגות את החובה לערוך, אחת ל־18 חודשים לפחות, סקר סיכונים לאיתור סיכוני אבטחת מידע במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה. על המפלגה כבעלת השליטה לדון בתוצאות הסקר ולפעול לתיקון הליקויים בו.[386] במסגרת סקר סיכונים נבחנות נקודות התרופה בתשתית הטכנולוגית במטרה למזער את הסיכון לזליגת מידע ולתקיפות סייבר העלולות לשבש את קמפיין הבחירות ובתוך כך גם לפגוע בזכות לפרטיות של הבוחרים.

(ד) עיצוב לפרטיות

"עיצוב לפרטיות" מבטא את התפיסה שכאשר מדובר במערכות לעיבוד מידע אישי, יש להבטיח הטמעה של אמצעי הגנה על הפרטיות בשלבי התכנון והפיתוח, בשלב ההטמעה וכן בשלב ההפעלה. במסגרת זו יש להבנות את הטכנולוגיה לצמצום איסוף מידע אישי ועיבודו למינימום הנחוץ להשגת מטרות העיבוד לאורך כל שלבי מחזור החיים של המידע, לשם מזעור הסיכונים לפרטיות.

חובת העיצוב לפרטיות אומצה בעשור השני של המאה ה־21 על ידי נציבי פרטיות ברחבי העולם כצעד יזום ומניעתי, ולא כסעד שלאחר מעשה, לאחר מחדל אבטחה או פגיעה בפרטיות. בשנת 2023 נכללה החובה בתקן בינלאומי להגנה על צרכנים.[387] אומנם, החובה אינה מעוגנת בחוק הגנת הפרטיות, אולם הרשות להגנת הפרטיות ממליצה לבעלי שליטה ומחזיקים לאמצה ככלי חיוני במזעור סיכוני פרטיות ולשם בניית אמון.[388]

הצעד הראשון בעיצוב לפרטיות הוא ביצוע תסקיר השפעה על פרטיות (Privacy Impact Assessment) במסגרתו יש לבחון באופן מקיף ושיטתי את השפעת השימוש בטכנולוגיה המבוקשת על פרטיות נושאי המידע, לזהות את הסיכונים לפרטיות לאורך כל מחזור החיים של המידע, ולהציע אמצעים טכנולוגיים וארגוניים למזעור סיכונים אלו. יש לעצב את טכנולוגיות עיבוד המידע בהתאם לממצאי התסקיר ומטרות העיבוד.[389]

לדעתנו, יש להבהיר למפלגות את חשיבות העיצוב לפרטיות ויתרונותיה ולעודדן לאמצה, תוך ביצוע תסקיר השפעה על הפרטיות, כבר בתחילת קמפיין הבחירות, בעת התקשרות עם מחזיק, פיתוח יישומון בחירות או בחירת פלטפורמה להפצת מסרי תעמולה על בסיס מידע אישי. המדובר בכלי שיבטיח מזעור הפגיעה בפרטיות במהלך קמפיין הבחירות, הגברת אמון הציבור במפלגות בכל הקשור לעיבודי מידע המבוצעים על ידן, וזאת תוך התאמת טכנולוגיית עיבוד המידע למטרות העיבוד של המפלגה.

(ה) דיוור ישיר

יש להבהיר למפלגות שכל פנייה אישית לבוחר, בין אם מבוצעת על ידי המפלגה או גורם אחר מטעמה, המבוססת על השתייכותו לקבוצת אוכלוסין שנקבע על פי אפיון אחד או יותר של בני אדם הכלולים במאגר, למשל פנייה לבוחרים שאופיינו כמתלבטים, היא דיוור ישיר כהגדרתו בחוק הגנת הפרטיות. ועל

[386] תקנה 5(ג) לתקנות אבטחת מידע, לעיל ה"ש 110.

[387] ISO 31700-1:2023 Consumer protection – Privacy by design for consumer goods and services

[388] הרשות להגנת הפרטיות, עיצוב לפרטיות (Privacy by Design) (פורסם 04.08.2021, עדכון אחרון 10.07.2025).

[389] הרשות להגנת הפרטיות, מדריך עזר מתודולוגי לעריכת תסקיר השפעה על הפרטיות – כלי שיסייע לארגונים במשק להעריך ולצמצם סיכונים לפרטיות (פרסום 23.11.2022, עדכון 7.12.2025).

כן חלות עליהן החובות החלות בעת משלוח דיוור ישיר – החובה לספק הודעה במסגרת הפנייה בדיוור ישיר הכוללת הבהרה שמדובר בדיוור ישיר וכן ציון זהותו ומענו של בעל השליטה, פירוט המקורות מהם קיבל בעל השליטה את המידע האישי, וכן הודעה על זכותו של מקבל הפנייה בדיוור ישיר להימחק מהמאגר, בצירוף המען אליו יש לפנות על מנת לממש את זכות מחיקה זו.[390]

כן על המפלגות לכבד את זכותו של בוחר לבקש את מחיקתו ממאגר המידע המשמש לדיוור ישיר ולהגביל את העברת המידע האישי אודותיו לצדדים שלישיים. במסגרת זו על המפלגות להבין שעליהן להחזיק במנגנון אשר יאפשר לבוחרים לממש את זכויותיהן אלו וכן שאין להן שיקול דעת האם להיענות לבקשה. מרגע קבלת בקשה מבוחר להימחק ממאגר המידע או להגביל את העברת המידע אודותיו לצדדים שלישיים על המפלגה להיענות לבקשה בתוך 30 ימים. בהיעדר מענה בתקופה האמורה זכאי הבוחר המבקש לפנות לבית משפט השלום בבקשה להורות למפלגה לכבד את בקשתו.[391]

(ו) כיבוד זכויות הבוחרים נושאי המידע

יש להבהיר למפלגה שעליה לכבד את זכויות הבוחרים נושאי המידע ליידוע בעת פנייה לאיסוף מידע אישי,[392] לעיבוד מידע אישי רק בהסכמה תקפה שלהם,[393] לדרוש עיון במידע אודותיהם ולבקש את תיקונו.[394] זאת בנוסף לזכויות העומדות להן במקרה של דיוור ישיר.[395] במסגרת זו יש להבהיר למפלגה מהן הפעולות שעליה לנקוט לשם כיבוד זכויות אלו וכן שעליה לוודא שגם מפעיל יישומון בחירות יכבד את זכויות אלו של נושא המידע.[396] כן על מפלגה לתת את הדעת לזכותו של בוחר נושא מידע שזכויותיו לא כובדו לפנות לבית משפט בבקשה לפיצויים לדוגמה ולהשפעת ביטול מגבלת על תקופת ההתיישנות על זכויות אלו.[397]

(ז) הבהרות לגבי נושאים שאין לגביהם הכרעה: החובות החלות על מפלגה כגוף דו־מהותי, מדיניות ביחס לגירוד מידע מאתרי אינטרנט ומידע מוסק

מפלגה היא גוף דו־מהותי, אולם אין קביעה ברורה באשר לחובות החלות עליה מן המשפט הציבורי בשל כך. על הרשות לבחון ולהבהיר מהן החובות לפי חוק הגנת הפרטיות שעל מפלגה לציית להן מכורח היותה גוף דו־מפלגי בכובעה כמבצעת פעולות בעלות מאפיינים ציבוריים מובהקים. למשל, האם חלה על מפלגה חובת רישום, חובה למנות ממונה הגנת פרטיות ומידתיות בעיבוד המידע האישי מטעם זה.

---

[390] סעיף 17ו(א) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[391] סעיף 17ו(ב)-(ה) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[392] ראו הדיון בטקסט הנלווה לה״ש 286–289 לעיל.

[393] ראו הדיון בטקסט הנלווה לה״ש 229–243 לעיל.

[394] סעיפים 13, 14 לחוק הגנת הפרטיות, לעיל ה״ש 9.

[395] ראו הטקסט הנלווה לה״ש 390–391 לעיל.

[396] סעיפים 13א, 14(ד) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[397] סעיף 15א לחוק הגנת הפרטיות, לעיל ה״ש 9 וכן הטקסט הנלווה לה״ש 293–304 לעיל.

בנוסף, נושא עיבוד מידע מרשתות חברתיות באמצעות גירוד מידע למטרות פוליטיות, לרבות איסוף מידע על דעה פוליטית או הסקת דעתו הפוליטית של אדם על בסיס מידע אישי אחר, הם נושאים שיש מחלוקת ציבורית בנוגע לדין המחייב. כך, למשל, בהיעדר בסיסים חוקיים לעיבוד מידע לבד מהסכמה בדין הישראלי, האם נדרשת הסכמה תקפה, מדעת ומרצון חופשי, לכל גירוד מידע? ואם כן, כיצד יש לבחון קבלתה של הסכמה כאמור? האם מאגרי המידע שנוצרו בעבר על בסיס גירוד מידע אינם חוקיים? על הרשות להתייחס לנושא בהנחיותיה בשים לב למגבלות חוק הגנת הפרטיות הקיים וכן השלכות קביעותיה לא רק על המרחב הפוליטי אלא גם על המרחב העסקי הפרטי.

פרק אחד עשר
המלצות ליו"ר ועדת הבחירות המרכזית

(א) סמכות יו"ר ועדת הבחירות המרכזית – כללי

סוגיות הקשורות בעיבוד מידע אישי באמצעות בינה מלאכותית לצורכי תעמולת בחירות, בהפצת מסרי תעמולת בחירות מותאמים אישית ובשימוש ביישומוני בחירות יהיו ללא ספק תפוח האדמה הלוהט בבחירות לכנסת ה־26. סוגיות אלה נשענות בעיקר על ההכרה בזכות לפרטיות כזכות חוקתית וכן על עיקרון חשאיות הבחירות, שנועד לשרת הן את האינטרס הפרטי של המצביע לשמור על סודיות הצבעתו (שהוא אינטרס שניתן לוותר עליו בהסכמה) והן את האינטרס הציבורי למנוע את קיומה של השפעה פסולה ולשמור על טוהר הבחירות.[398] למולן ניצבת הזכות החוקתית להיבחר, שמכוחה יכולות מפלגות לבצע פעולות שונות למטרת הצלחה בבחירות.

סעיף 17ב לחוק דרכי תעמולה מסמיך את יו"ר וועדת הבחירות להוציא צווי מניעה במטרה למנוע עבירה על הוראות החוק וכן על הוראות פרק י"א לחוק הבחירות לכנסת. רוב העתירות המוגשות ליו"ר וועדת הבחירות הן להוצאת צוו מניעה (תב"כ) ורוב החלטותיו בשנים האחרונות קשורות לעבירות על חוק דרכי תעמולה.399 בפרשת "שרלי הבדו" הגביל בית המשפט העליון במפורש את סמכות יו"ר ועדת הבחירות המרכזית להוציא צווי מניעה, רק לעבירות על אחד מהחיקוקים המנויים בסעיף 17ב לחוק דרכי תעמולה.400 חיקוקים אלה הם חוק התעמולה עצמו וכן העבירות המנויות בפרק י"א לחוק הבחירות לכנסת.

ברוח זו, במערכות הבחירות הקודמות, בחרה וועדת הבחירות המרכזית למשוך ידה מהסוגיות הנוגעות לשימושים במידע אישי והגנת הפרטיות סביב הבחירות. כך, יו"ר ועדת הבחירות המרכזית לכנסת ה־23, השופט ניל הנדל הכיר בכך שיש צורך בהסדרה נורמטיבית מעמיקה של הזכות לפרטיות הבוחרים, נוכח השימוש הגובר בטכנולוגיות לעיבוד מידע אישי במסגרת תעמולת בחירות והיעדר התייחסות של חוק התעמולה לסוגיות אלו. אולם קבע שוועדת הבחירות המרכזית אינה מוסמכת לדון בסוגיות אלו, שכן חוק הגנת הפרטיות אינו מבין החוקים המנויים במפורש בסעיף 17ב לחוק דרכי תעמולה. החלטתו אושרה גם על ידי בית המשפט העליון שהביע אף הוא חוסר נוחות נוכח הפגיעה האפשרית בזכות לפרטיות, אך החזיק בעמדה לפיה אין בסמכותה של ועדת הבחירות המרכזית להכריע בנושא.[401]

בפועל, חוסר ההכרעה מצד ועדת הבחירות המרכזית, כמוהו כהכרעה. עיבוד מידע אישי לצורכי תעמולה, באמצעות בינה מלאכותית ויישומוני בחירות ימשיך ויגבר עוד. בהקשר זה נציע שתי דרכים. הדרך האחת היא לטעון כי תיקון 13 יצר סמכות משלימה עבור יו"ר ועדת הבחירות לדון בענייני פרטיות

---

[398] בר"מ 3235/90 **עמאש נ' מנהל הבחירות למועצה המקומית ג'סר אלזרקא** (נבו, 1.3.2011).

[399] להרחבה ראו דנה בלאנדר, ועדת הבחירות המרכזית – מקצועית או פוליטית? **המכון הישראלי לדמוקרטיה** (מחקר מדיניות 175, יוני 2022), בעמ' 101–108.

[400] שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 76–79.

[401] תב"כ 13/23 **בן מאיר ואח' נ' הליכוד ואח'**, ועדת הבחירות המרכזית לכנסת ה־23 (18.2.2020); בג"ץ 1311/20 **בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח'**, (נבו, 25.2.2020). כן ראו הדיון בטקסט הנלווה לה"ש 98–105 לעיל.

ובחירות. הדרך השניה היא להרחיב את תחולת הפרשנות של סעיפים בפרק י״א לחוק הבחירות ולהתאימם לעידן הנוכחי.

(ב) סמכות יו״ר ועדת הבחירות לאור תיקון 13

אנו סבורות כי בבחינת סמכותה של ועדת הבחירות המרכזית לדון בנושאים אלו יש לתת את הדעת לשינוי שהתרחש מאז חקיקת תיקון 13 לחוק הגנת הפרטיות. כחלק מן התיקון הוענקה ליו״ר ועדת הבחירות המרכזית סמכות להכריע האם לאפשר לרשות להגנת הפרטיות להפעיל חלק מסמכויותיה בתקופת בחירות. במסגרת זו על יו״ר ועדת הבחירות המרכזית לבחון את מידתיות הפגיעה ביכולתה של המפלגה להתמודד בבחירות או לנהל את הקשר עם ציבור הבוחרים לעומת הסיכון לפגיעה בפרטיות ובאינטרס הציבורי העומד בבסיס הפעלת הסמכות.[402]

במובן זה, בעת חקיקת ההסדר המיוחד להגבלת סמכויותיה של הרשות להגנת הפרטיות בתקופת בחירות,[403] הכיר המחוקק בסמכותו של יו״ר ועדת הבחירות המרכזית לעסוק בנושאים הקשורים בהגנה על הזכות לפרטיות. כן הכיר המחוקק בהיותו יו״ר הוועדה הגורם שביכולתו לגשר בין הזכות להיבחר, לרבות זכויותיה של מפלגה להתמודד בבחירות וליצור קשר עם הבוחרים לפי חוק דרכי תעמולה וחוק הבחירות, לבין זכות הבוחר לפרטיות. לטעמנו ההסדר בתיקון 13 צריך להיות מתורגם להבנה כי ישנה סמכות ליו״ר ועדת הבחירות לדון בנושאים הקשורים בהגנת הפרטיות בתקופת הבחירות בנסיבות בהן נדרשת הכרעה מהירה תוך כדי תקופת הבחירות, וכאשר יש חשש שהמתנה להליך פיקוח ואכיפה מצד הרשות להגנת הפרטיות תוביל לפגיעה משמעותית בהיקפה ובחומרתה בזכות הבוחרים לפרטיות, שלא ניתן יהיה למנוע, למזער או לתקן בדיעבד. לכן, מדובר בהסדר חדש, שניתן לקרוא אותו אל תוך סעיף 17ב לחוק התעמולה.

נציין שעמדתנו זו הובעה גם במהלך הדיונים בתיקון 13 בנוגע להסדר הגבלת סמכויותיה של הרשות להגנת הפרטיות בתקופת בחירות, אולם ועדת החוקה בחרה שלא להכריע בסוגיה שכן דיוניה התמקדו לשיטתה רק בסמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות ולא באלה של ועדת הבחירות. לכן, אין לראות בכך הסדר שלילי ביחס לוועדת הבחירות.[404]

תיקון 13 לא יצר סתירה בין סמכות ראש הרשות להגנת הפרטיות להוציא צו להפסקת עיבוד[405] לבין הכרה בסמכותו של יו״ר וועדת הבחירות המרכזית לדון בנושאים הקשורים בחוק הגנת הפרטיות, אלא תוספת. סמכותו של ראש הרשות להגנת הפרטיות להוציא צו להפסקת עיבוד מידע אישי במאגר מידע במקרים שיש לו חשד סביר שמבוצעת או עלולה להתבצע הפרה חמורה,[406] לא מוגבלת בתקופת בחירות. המדובר בסמכות חשובה שיש בה לתת מענה מסוים לחששות העולים מעיבוד מידע אישי לצורכי תעמולת בחירות באמצעות טכנולוגיות מבוססות בינה מלאכותית ויישומוני בחירות. במסגרת סמכות זו רשאי ראש הרשות להגנת הפרטיות להורות על הפסקה מיידית של עיבוד מידע אישי כאשר יש לו חשד סביר

---

[402] ראו סעיף 23נט(ד) לחוק הגנת הפרטיות, לעיל ה״ש 9.

[403] סעיפים 23נח–23נט לחוק הגנת הפרטיות, לעיל ה״ש 9.

[404] פרוטוקול מס׳ 313 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, ח׳ בניסן התשפ״ד (16 באפריל 2024), בעמ׳ 4–8.

[405] סעיף 23מט לחוק הגנת הפרטיות, לעיל ה״ש 9.

[406] סעיף 23מט לחוק הגנת הפרטיות, לעיל ה״ש 9, וכן ראו הדיון בטקסט הנלווה להה״ש 341–346 לעיל.

שמבוצעת או עלולה להתבצע הפרה חמורה של הוראות שונות כגון עקרון צמידות המטרה, עיבוד בחריגה מהרשאה, הפרת חובת אבטחת המידע או הפרת האיסור על עיבוד מידע שנוצר, התקבל או נצבר בניגוד לדין.[407] אולם, כפי שטענו במהלך המחקר, אין בסמכות זו די. זאת נוכח החשש, שהוזכר במהלך הדיונים בוועדת החוקה בנוגע לתיקון 13,[408] מפני חולשתה של הרשות להגנת הפרטיות למול גורמי ממשל וגורמים מהמגזר הציבורי כיוון שעצמאותה מוסדרת רק בהחלטת ממשלה המופיעה בתוספת לחוק הגנת הפרטיות.[409]

בעידן הנוכחי יש חלון זמנים קצר ומצומצם ביותר למניעת פגיעה בפרטיות, שכן מרגע שניתנת הרשאת גישה למידע אישי לגורמים שונים או שמתגלה פרצת אבטחה, זליגת מידע אישי עשויה להיות עניין של טווח זמן קצר, ולאחריה קשה מאוד לאתר את המידע ולמנוע שימוש בו על ידי גורמים בלתי מוסמכים. יתרה מכך, בעוד שראש הרשות ממוקד בשיקולי פרטיות, ליו״ר ועדת הבחירות המרכזית ראייה רחבה יותר וסמכות לשקול את הפגיעה בזכות להיבחר לצד פגיעה אפשרית בזכות לבחור ובהוגנות הבחירות, כפי שלמעשה עולה מן ההסדרים בתיקון 13.

(ג) סמכות יו״ר ועדת הבחירות לתת פרשנות מותאמת־זמן ומציאות לסעיפים מתוך פרק י״א לחוק הבחירות

בחלק זה אנו מציעות לפרש את סעיפי החוק המפורטים להלן, מתוך פרק י״א לחוק הבחירות הנכלל בקרב הסעיפים שלגביהם ניתן לתת צווי מניעה מכוח סעיף 17ב לחוק התעמולה, באופן המתאים למציאות הנוכחית.

(1) סעיף 118א לחוק הבחירות: שימוש חורג במידע פנקס

סעיף 118א לחוק הבחירות קובע ש״העושה שימוש במידע פנקס או המוסר מידע ממדע פנקס כהגדרתו בסעיף 39 שלא לצורכי התמודדות בבחירות או לצורכי קשר עם ציבור הבוחרים, דינו – מאסר שנתיים או הקנס הקבוע בסעיף 61(א)(4) לחוק העונשין, התשל״ז-1977.״ הסעיף ממוקד בהפרה של עקרון צמידות המטרה מחוק הגנת הפרטיות,[410] וקובע שמדובר בעבירה פלילית. קביעה זו מתווספת להוראת סעיף 5 לחוק הגנת הפרטיות לפיה פגיעה במזיד בפרטיות לפי סעיף 2(9), כלומר הפרת עקרון צמידות המטרה עקב שימוש בידיעה על עניניו הפרטיים של אדם שלא למטרה לשמה הוא נמסר, היא עבירה שדינה מאסר 5 שנים.

---

[407] סעיף 23מט לחוק הגנת הפרטיות, לעיל ה״ש 9, וכן ראו הדיון בטקסט הנלווה להי״ש 341–346 לעיל.

[408] ראו, למשל, פרוטוקול מס׳ 223 מישיבת ועדת החוקה, חוק ומשפט, יום שלישי, כ״ח בטבת התשפ״ד (9 בינואר 2024), בעמ׳ 116.

[409] החלטת ממשלה מס׳ 1890 עצמאות הרשות להגנת הפרטיות ותיקון החלטת ממשלה (2.10.2022); וכן התוספת הראשונה לחוק הגנת הפרטיות, לעיל ה״ש 9.

[410] ראו הטסקט הנלווה להי״ש 243–250 לעיל.

עם זאת, סעיף 118א לחוק הבחירות נבדל מסעיף 5 לחוק הגנת הפרטיות, כמפורט להלן:

	סעיף 118א לחוק הבחירות	**סעיפים 5 ו2(9) לחוק הגנת הפרטיות**
תחולה	רק מידע הפנקס	ידיעה על ענייניו הפרטיים של אדם. כלומר כולל גם מידע הפנקס וגם מידע מטוייב.
העבירה	עיבוד שלא למטרת התמודדות בבחירות וקשר עם ציבור הבוחרים	עיבוד שלא למטרה לשמה נמסר. בכל מקרה המטרה צריכה לעמוד במסגרת החוקית של סעיף 39(ג) לחוק הבחירות. כלומר לצורכי התמודדות בבחירות או קשר עם ציבור הבוחרים. העיבוד הוא **במזיד**
עונש	שנתיים מאסר או קנס	חמש שנות מאסר או קנס
הגוף החוקר	המשטרה	הרשות להגנת הפרטיות
הפעלת הסמכות בתקופת בחירות	אם החקירה היא נגד רה"מ, שרים או אישי ציבור בכירים יש צורך באישור יועמ"ש.	נדרש אישור יו"ר ועדת הבחירות המרכזית

משמעות הבדלים אלו היא ששימוש במידע הפנקס שלא למטרה לשמה נמסר, היא עבירה שהעונש בגינה קל יותר מאשר הפרה בזדון של עקרון צמידות המטרה ביחס למידע מטויב או מידע הפנקס. כפי שפורט לעיל, חקירת העבירה החמורה יותר מחייבת אישור יו"ר ועדת הבחירות המרכזית. אבל, דווקא בתקופת בחירות חקירת העבירה הקלה יותר אפשרית ואינה דורשת אישורים נוספים, אלא אם מושא החקירה הוא ראש הממשלה, שר או איש ציבור בכיר אחר.

שמירת מידע ממידע הפנקס ממערכות הבחירות הקודמות היא ממילא הפרה של הוראת סעיף 39(ג) לחוק הבחירות ותקנות הבחירות,[411] שגם בגינה מוסמך יו"ר וועדת הבחירות להוציא צו מניעה לפי סעיף 17ב לחוק תעמולה, וזאת משום שהיא נופלת בגדר סעיף 126(6) לחוק הבחירות – "המפר הוראה מהוראות חוק זה שלא נזכרה בפרק זה".

אבל, בהקשר זה אנו מציעות להחיל את העבירה לפי סעיף 118א הן על מידע פנקס והן על מידע מטויב. זאת מתוך ההבנה שהבחנה בין סוגי המידעים ויצירת משטר משפטי שונה ביחס לחלק מהמידע במאגר המידע, היא יקרה ומסובכת. נעיר כי הדבר דומה, בשינויים המחויבים, לדיון שהתקיים בנוגע לתקנות מידע שהועבר לישראל מהאזור הכלכלי האירופי. באותו הקשר הוחלט כי נוכח הקושי המעשי והנטל הכלכלי והבירוקרטי שבהחלת משטרי פרטיות שונים על שני סוגי מידע שונים הנמצאים שניהם באותו מאגר מידע – מידע שהגיע מהאיזור הכלכלי האירופי ומידע שהגיע מישראל – יש להחיל את הוראות התקנות על כל מידע המצוי במאגר מידע שיש בו מידע שהתקבל מהאזור הכלכלי האירופי.[412] אכן, אין

[411] להרחבה ראו הטקסט הנלווה לה"ש 267 לעיל.

[412] תקנה 2(א) לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), תשפ"ג-2023; פרוטוקול מס' 66 מישיבת ועדת החוקה, חוק ומשפט, יום ראשון, ב' באייר התשפ"ג (23 באפריל 2023), בעמ' 20–27.

מדובר כאן בשני משטרים שונים, אך הטענה לפיה הפרדה בין סוגי מידע במאגר אחד היא קשה ליישום, צריכה להילקח בחשבון.

(2) סעיף 119(א)(3) לחוק הבחירות: הפרעה להצבעה ודיכוי הצבעה

סעיף 119(א)(3) לחוק הבחירות לכנסת אוסר על הפרעה לבחירות ומגדיר הפרעה כך: "המפריע לבוחר בהצבעה או המונע אותו מהצביע". לנוכח היכולת להשתמש במידע אישי כדי לתפור אישית מסרים שעשויים לדכא הצבעה ולדכא בוחרים מלצאת ולהצביע, ראוי לדעתנו שוועדת הבחירות המרכזית תבהיר כי מניעת הצבעה איננה רק חסימה פיזית של הגישה לקלפי, אלא גם מניעה שמבוססת על פעולות דיגיטליות מותאמות אישית לבוחר העלולות לגרום לאדם סביר להימנע מלהצביע. למשל, מסרים של שכנוע או מניפולציה, כמו למשל מסר שמבוסס על מידע אישי בנוגע למיקומו של המצביע ("אנחנו יודעים שאתה בדרך, אבל התור בקלפי שלך ארוך, לא להתקרב!"); למצב בריאותו ("אנחנו יודעים שאתה בקבוצת סיכון, ובקלפי יש חולה קורונה מאומת"); או ללאום שלו ("יש ליד הקלפי חברה שמחפשים להרביץ לערבים").

(3) סעיף 122(6) לחוק הבחירות

סעיף 122(6) לחוק הבחירות קובע ש"המשדל אדם להצביע או להימנע מלהצביע, בכלל או בעד רשימת מועמדים מסויימת, בדרך של השבעה, קללה, נידוי, חרם, נדר, התרת נדר, הבטחה להעניק ברכה, או מתן קמיע" עובר עבירה של שחיתות ואיום. לדעתנו על ועדת הבחירות המרכזית להבהיר שסעיף זה כולל גם איסור על מעשים של מניפולציה רגשית על בוחרים המבוססים על עיבוד מידע בעל רגישות מיוחדת אודות הבוחרים באופן המפר את הוראות חוק הגנת הפרטיות. בתקופה הנוכחית מניפולציה רגשית שמבוססת על איסוף ועיבוד של מידע אישי עשויה להיות פוגענית יותר מקללה או חרם, בעיקר משום שבוחרים אינם יודעים איזה מידע ידוע עליהם ואינם מודעים לעומק המניפולציה הרגשית עליהם. בכך, היא עלולה לפגוע משמעותית ברצון החופשי של הבוחר וביכולתו לממש בחופשיות את זכותו לבחור.

(ד) סימון תעמולה

על ועדת הבחירות המרכזית להבהיר לכלל המפלגות והסיעות את משמעות דרישת השקיפות בתעמולת בחירות לפי חוק דרכי תעמולה,[413] תחולתה ואופן יישומה המעשי על תעמולת בחירות המופצת על ידן באמצעות יישומוני בחירות או מותאמת אישית לבוחרים ומופצת בפלטפורמות דיגיטליות שונות כגון, למשל, הודעות SMS אישיות, מסרים בפלטפורמות סטרימינג או פודקסט.

[413] סעיף 2א1 לחוק הבחירות (דרכי תעמולה), התשי"ט-1959.

פרק שנים עשר

שאלון בחינה עצמית למפלגות ומי שפועלים מטעמן, לעמידה בדרישות חוק הגנת הפרטיות בעיבוד מידע על בוחרים

שאלון זה נועד לשמש כלי בחינה עצמית למפלגות ולמנהלי קמפיינים פוליטיים מטעמן, בדומה לתסקיר השפעה על פרטיות המקובל בדיני הגנת המידע בעולם. מטרתו לסייע בזיהוי מוקדם של סיכוני פרטיות הנובעים משימוש במידע אישי ובכלים טכנולוגיים וחישוביים מתקדמים במסגרת תעמולת בחירות וכן לספק מסגרת בסיסית לבחינת עמידת בדרישות דיני הגנת הפרטיות.

שלב ראשון: מיפוי המידע וחוקיות השימוש בו [D]

1. **מידע או נתון**

האם המידע בהם מותמם או מדובר במידע מזוהה או ניתן לזיהוי ולכן מידע אישי?

2. **אוסף נתונים או מאגר מידע**

האם אוסף פרטי המידע האישי עולה כדי הגדרת "מאגר מידע"?

3. מקור המידע וחוקיותו

אם המידע נאסף ישירות מהבוחרים, לרבות באמצעות מערכות לקבלת החלטות המבוססות על בינה מלאכותית,[414]

- האם הבוחרים מקבלים הודעה כנדרש לפי סעיף 11 לחוק, הכוללת הסבר האם חלה עליהם חובה חוקית למסור את המידע והשלכות סירוב למסור אותו, מטרת השימוש במידע, שמה של המפלגה ודרכי ההתקשרות עמה, הגורמים להם יימסר המידע, וזכויותיהם לגבי המידע שהם מוסרים?
- האם הבוחרים הסכימו מדעת, מרצון חופשי, ועדיף במפורש, לעיבוד המידע האישי למטרות הספציפיות שהגדירה המפלגה, לפי המבחנים המפורטים להלן?
- האם המפלגה ו/או מפעיל יישומון הבחירות מספקים לבוחרים את כל המידע הנחוץ להם לשם קבלת החלטה האם להסכים או לסרב לעיבוד המידע האישי אודותיהם?
- האם היישומון כולל מידע לבוחרים לגבי סוגי המידע הנאספים אודותיהם, השימוש שיעשה בהם, המטרות וסוגי הגורמים אליהם עשוי המידע להיות מועבר?
- האם המידע המסופק לבוחרים לשם קבלת הסכמתם מוצג באופן ברור, נגיש, פשוט ומובן?
- האם הבוחרים נדרשים לציין את הסכמתם באופן אקטיבי (opt-in)?
- האם נעשה שימוש בכלים עיצוביים שמטרתם להקשות על הבנת משמעות ההסכמה ובכך להקשות על נתינתה מרצון חופשי?
- האם הבוחר נתן את הסכמתו לעיבוד מידע אישי אודותיו במפורש?
- האם המפלגה ו/או מפעיל יישומון הבחירות מחזיקים במנגנון לחזרה מהסכמה?

[414] עם זאת נושא חוקיות גירוד מידע מרשת האינטרנט באמצעות בינה מלאכותית אינה ברורה לאשורה. ראו הדיון בטקסט הנלווה להע"ש 259–260 לעיל.

אם מקור המידע הוא צדדים שלישיים המזינים את המידע באמצעות יישומון בחירות או טכנולוגיה אחרת:

- האם הצדדים השלישיים סיפקו לבוחרים הודעה הכוללת הסבר האם חלה עליהם חובה חוקית למסור את המידע והשלכות סירוב למסור אותו, מטרת השימוש במידע, שמה של המפלגה ודרכי ההתקשרות עמה, הגורמים להם יימסר המידע, וזכויותיהם לגבי המידע שהם מוסרים?
- האם הסכמת הבוחרים היא הסכמה תקפה בהתאם לתבחינים שפורטו לעיל?

אם מקור המידע הוא סוחרי מידע מהם רכשה המפלגה את המידע:

- האם המפלגה וידאה שהמידע האישי שרכשה מסוחרי מידע הוא חוקי? למשל, שסוחר המידע ביקש את הסכמתם מדעת של נושאי המידע שמידע אודותיהם כלול במאגר הנרכש?
- אם המידע שנרכש מסוחרי מידע נאסף באמצעות גירוד מאתרי אינטרנט פתוחים, או באמצעות מערכות בינה מלאכותית אשר גירדו מידע או הסיקו מידע אישי על בסיס מידע קיים:
  - האם המפלגה וידאה שהבוחרים נושאי המידע נתנו הסכמה תקפה, בהתאם לתבחינים שפורטו לעיל לגירוד המידע?[415]

אם מקור המידע הוא מאגרי מידע קיימים של המפלגה

- האם מאגרי מידע אלו כוללים מידע פנקס ממערכות בחירות קודמות או נגזרות שלו?
- האם המפלגה יכולה למפות את מקורות המידע שבמאגר המידע המפלגתי ולהבטיח את חוקיותו מבחינת דרישת ההודעה לפי סעיף 11 ודרישת ההסכמה התקפה?

שלב שני: בחינת מטרות השימוש במידע

1. מטרות השימוש במידע

אם מדובר במידע הפנקס או נגזרותיו:

- האם מטרות השימוש תואמות את מסגרת מטרות השימוש הקבועה בסעיף 39(ג) לחוק הבחירות – לצורכי התמודדות המפלגה בבחירות לכנסת הנוכחית ולצורכי קשר עם ציבור הבוחרים?
- האם מטרות השימוש נרשמו במסמך מטרות המאגר?
- האם המטרות שפורטו במסמך המאגר מתאימות למטרות שבסעיף 39(ג) , מסוימות ומפורשות?
- האם המפלגה פירטה בפני הבוחרים נושאי המידע את מטרות השימוש במסגרת הודעה בעת פנייה לעיבוד מידע אישי לפי סעיף 11? (רחל: שאלנו את זה קודם. למה צריך שוב כאן?)

2. עקרון צמידות המטרה

- האם עיבוד המידע נעשה אך ורק לצורך המטרות שלשמן נמסר המידע על ידי נושא המידע או למטרות סעיף 39(ג) ובהיקף הנחוץ לשם כך?

[415] שאלה זו נמצאת כאן כי לעמדת הרשות לפרטיות נדרשת הסכמה, אבל כפי שהערנו למעלה זהו נושא שעדיין יש לגביו מחלוקת ואיננו מוסדר.

- האם למפלגה ו/או למפעיל יישומון הבחירות שליטה מלאה על השימושים הנעשים במידע האישי באמצעות היישומון על מנת להבטיח ציות לעקרון צמידות המטרה?
- האם המפלגה או מפעיל היישומון מאפשרים לכל אדם גישה למאגר המידע ביישומון?

שלב שלישי: ציות לחובות נוספות המוטלות על בעל השליטה ו/או המחזיק

1. חובת הודעה לרשות להגנת הפרטיות

- האם למפלגה מאגר מידע שבו מידע בעל רגישות מיוחדת על 100,000 נושאי מידע לפחות?
- אם התשובה חיובית, האם המפלגה מסרה על כך הודעה לרשות להגנת הפרטיות כנדרש לפי סעיף 8א(ב) לחוק הגנת הפרטיות?

2. חובת הודעה בפנייה בדיוור ישיר

- האם מבוצעת פנייה אישית לבוחר בהתבסס על השתייכותו לקבוצת אוכלוסיה שנקבעה על פי אפיונים של בני אדם ששמותיהם כלולים במאגר? (למשל, פנייה לכל מי שנקבע שהוא שייך לקבוצת המתלבטים או לקבוצת הבוחרים שהנושא המרכזי המעניין אותם הוא חינוך לגיל הרך).

אם כן,

- האם בצמוד לפנייה בדיוור ישיר ניתן לנמען מידע על זהותה ומענה של המפלגה, המקורות מהם קיבלה המפלגה את המידע האישי שעל פיו בוצעה הפניה, וזכותו של הנמען לבקש את מחיקת המידע האישי אודותיו מהמאגר?

3. חובת אבטחת מידע

- האם המפלגה עומדת בכל דרישות אבטחת המידע לפי חוק הגנת הפרטיות ותקנות אבטחת מידע?
- האם המפלגה בחנה את סיכוני אבטחת המידע הכרוכים בהתקשרות עם ספק יישומון או גורם חיצוני אחר לפני ההתקשרות?

האם בהסכם בין המפלגה לגורם החיצוני נקבעו במפורש ובשים לב לסיכוני אבטחת המידע הנושאים הבאים:

- המידע שהגורם החיצוני רשאי לעבד ולאלו מטרות
- המערכות אליהם רשאי הגורם החיצוני לגשת
- סוג העיבוד שהגורם החיצוני מוסמך לבצע
- משך ההתקשרות ואופן השבת המידע למפלגה בסיומה
- אופן יישום הוראות תקנות אבטחת מידע על ידי הגורם החיצוני
- חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע?
- חובתו של הגורם החיצוני לדווח לפחות אחת לשנה למפלגה על ביצוע חובותיו לפי ההסכם ולפי תקנות אבטחת מידע וכן להודיע לה על כל אירוע אבטחה.

4. חובת מינוי ממונה הגנת פרטיות

- האם מפעיל יישומון בחירות מינה ממונה הגנת פרטיות?

האם נערכה היוועצות לגבי אפיונה של מפלגה כגוף דו־מהותי כדי לבחון חובת מינוי ממונה הגנת פרטיות?

5. עיבוד מידע בהרשאה בלבד

- האם כל עיבודי המידע במאגר המידע מבוצעים בהרשאת המפלגה? למשל, אם אין למפלגה ו/או מפעיל יישומון הבחירות שליטה על מי מתקין את היישומון ומי מעבד מידע אישי המוצג בו, הרי שיתכן עיבוד מידע ללא הרשאה.

6. זכויות נושאי המידע

- האם יש מנגנון למתן מענה ולטיפול בבקשות עיון, תיקון או מחיקה והגבלת העברה במקרה של דיוור ישיר?

שלב חמישי: הערכת סיכונים להליך הדמוקרטי

1. שקיפות ומניפולציה סמויה

- האם הבוחר יודע או יכול לדעת שהוא נחשף לתוכן פוליטי מותאם אישית?
- האם סביר שהבוחר יבין מהו המידע האישי או האיפיון בגינו נשלחה לו תעמולה פוליטית מותאמת אישית?
- האם נעשה שימוש במידע אישי או במידע מוסק לשם זיהוי חולשות, מגבלות או מאפיינים רגשיים של הבוחר?
- האם מסרי התעמולה מנוסחים באופן העלול לנצל חולשות, מגבלות, מצוקות נפשיות או חוסר ידע של הבוחר?
- מהו היקף הבוחרים החשופים לתעמולה מותאמת אישית והאם נעשה שימוש בכלי בינה מלאכותית להגדלת ההפצה ולהגבר מלאכותית של מסרי תעמולה באופן המגדיל את עוצמת המניפולציה?

2. חשאיות הבחירות

- האם מוזן בזמן אמת ביום ההצבעה מהקלפיות מידע בדבר בוחרים המממשים את זכות ההצבעה שלהם, וכתוצאה מבוצעת פנייה אישית לבוחרים שטרם מימשו את זכות ההצבעה?
- האם הבוחרים הסכימו לשימוש במידע אישי אודות מימוש או אי מימוש זכות ההצבעה שלהם?[416]

שלב שישי: אימוץ והטמעה של אמצעים לבקרה על הסיכונים לפרטיות ולטוהר הבחירות ולצמצומם

האם ננקטו אמצעים ארגוניים או טכנולוגיים –

[416] בהקשר לשתי השאלות האלה נעיר כי ההכרעה בשאלה האם מדובר בפגיעה בחשאיות הבחירות, תלויה ועומדת בפני יו"ר ועדת המרכזית ואין לגביה החלטה בפסיקת עבר, וכן גם ההכרעה בשאלה האם המעבר מתיעוד ידני של רשימות הבוחרים לתיעוד באמצעות אפליקציות בזמן אמת יוצר פגיעה בטוהר הבחירות.

- להבטחת קבלת הסכמה תקפה של הבוחרים נושאי המידע לאיסוף המידע האישי אודותיהם ולשימוש בו?
- לבחינת חוקיות המידע האישי שבמאגר המידע ולמניעת שימוש במידע לא חוקי, למשל ממערכות בחירות קודמות, מידע הפנקס ממערכות הבחירות הקודמות או חוקיות המידע שנרכש מסוחרי מידע?
- למניעת עיבוד שלא למטרה לשמה נמסר המידע או שנקבעה על ידי המפלגה במסמך הגדרות המאגר ובהתאם לסעיף 39(ג) בחוק הבחירות?
- למניעת עיבוד ללא הרשאה?
- למתן מענה למימוש זכויות נושאי המידע?
- להבטחת השקיפות כלפי הבוחר מבחינת המידע האישי בו נעשה שימוש, שימוש בטכנולוגיות בינה מלאכותית ואותנטיות המסר?
- למניעת ניצול לרעה של מידע בעל רגישות מיוחדת אודות חולשות, מוגבלויות או מצוקות נפשיות של הבוחרים נושאי המידע?

סיכום

תעמולה פוליטית נשענה מאז ומתמיד על מידע אודות בוחרים. אולם, ההתפתחויות הטכנולוגיות, בעיקר בתחום הבינה המלאכותית, חוללו שינוי עומק באופן איסוף מידע אישי והשימוש בו בתעמולת בחירות. המדובר באיסוף מסיבי של נתונים, ניתוחם באמצעים חישוביים והפצת מסרים מותאמים אישית לבוחרים, לעיתים מבלי שהם מודעים לכך. מערכות בינה מלאכותית יכולות להסיק מידע חדש על בוחרים מתוך נתונים זמינים, ולאחד מידעים ממקורות שונים לכדי פרופיל אישי מקיף. מצב זה מעורר חשש לפגיעה בזכות בוחרים לפרטיות וגם לזכותם לבחור באופן אוטונומי וחופשי.

אכן, תיקון 13 לחוק הגנת הפרטיות הרחיב את ארגז הכלים הקיים בידי הרשות להגנת הפרטיות, ובידי אזרחים, על מנת להתמודד עם פגיעות אלו. עם זאת, מדובר בכלים מוגבלים. ראשית, כלי הפיקוח והאכיפה של הרשות להגנת הפרטיות מוגבלים בתקופת בחירות, נוכח ההסדר המחייב אישור יו״ר ועדת הבחירות.[417] אומנם, הרשות יכולה להפעיל את סמכויותיה בתום תקופת הבחירות, אולם במקרים רבים נדרשת התמודדות מיידית ומהירה להפסקת הפרה. חקירה ואכיפה מינהלית של חשד להפרה שבועות או חודשים לאחר התרחשותה, הם פעמים רבות בעלי נפקות מעשית נמוכה ואף עשויים להיחשב בעיני מפלגה כ״הפרה יעילה״ – מחיר שכדאי לה לשלם על מנת להבטיח תעמולת בחירות מוצלחת יותר מבחינתה.

שנית, בהיעדר תיקון של הדין המהותי בחוק הגנת הפרטיות, רשימת הזכויות שיש בידי האזרח הבוחר, וכלי האכיפה הפרטית העומדים לרשותו, מצומצמים. דבקותו של חוק הגנת הפרטיות במנגנון הסכמה מדעת בלבד כתנאי להתרת פגיעה בפרטיות, הופך את ההסכמה לבעלת משמעות מעשית נמוכה ואת דרישת ההסכמה לקשה לאכיפה.

וועדת הבחירות המרכזית לכנסת נמנעה עד כה מהכריע בנושאים הקשורים בשימושים במידע אישי במסגרת תעמולת בחירות, בסכנות שבשימושים אלו לזכות הבוחר לפרטיות, ובהשלכותיהם על רצונות החופשי של הבוחר, האוטונומיה שלו וזכותו לבחור. זאת, בנימוק שאין היא מוסמכת לדון בנושאים הקשורים בחוק הגנת הפרטיות לפי חוק הבחירות (דרכי תעמולה). אולם, הימנעות ועדת הבחירות המרכזית לדון בנושאים אלו היוותה בפועל הכרעה שמשמעותה התרת כלל השימושים במידע אישי הנעשים במסגרת תעמולת בחירות ושיש בהם כדי לסכן את הזכות לפרטיות. זאת, נוכח הצורך לקבל החלטות מיידיות בפרקי זמן קצרים לשם מניעת פגיעה בפרטיות או מזעורה.

לדעתנו, יש בחקיקתו של תיקון 13 כדי לשנות את תפיסת הסמכות של ועדת הבחירות המרכזית לדון בסוגיות הנוגעות לתפר שבין חוק הגנת הפרטיות וחוקי הבחירות. תיקון 13 הסמיך את יו״ר ועדת הבחירות המרכזית להכריע האם לאפשר לרשות להגנת הפרטיות להפעיל חלק מסמכויותיה בתקופת בחירות. זאת, על בסיס בחינת מידתיות הפגיעה ביכולתה של המפלגה להתמודד בבחירות או לנהל את הקשר עם ציבור הבוחרים, לעומת הסיכון לפגיעה בפרטיות ובאינטרס הציבורי העומד בבסיס הפעלת הסמכות. כלומר, המחוקק הכיר בסמכותו של יו״ר ועדת הבחירות המרכזית לעסוק בנושאים הקשורים בהגנה על הזכות לפרטיות, בנסיבות בהן נדרשת הכרעה מהירה וכאשר יש חשש שהמתנה להליך פיקוח ואכיפה מצד הרשות להגנת הפרטיות תוביל לפגיעה משמעותית בזכות הבוחרים לפרטיות, שלא ניתן יהיה למנוע, למזער או לתקן בדיעבד.

[417] פרק ד׳5 לחוק הגנת הפרטיות, לעיל ה״ש 9.

גם ללא הרחבת הסמכות, אנו סבורות שקיימים בידי יו"ר ועדת הבחירות המרכזית כלים להתמודדות עם הסכנות הנלוות לעיבוד עמוק ורחב היקף של מידע אישי למטרות תעמולת בחירות. על ועדת הבחירות המרכזית לעשות שימוש בכלים אלו וליצור גבולות מותר ואסור בעיבוד מידע אישי אודות בוחרים. לדעתנו, על ועדת הבחירות המרכזית להבהיר כי יש לפרש את סעיף 119(א)(3) לחוק הבחירות כאוסר על הפרעה לבחירות המבוססת על פעולות דיגיטליות מותאמות אישית והעלולות לגרום לאדם סביר להימנע מלהצביע. כן נציע שוועדת הבחירות המרכזית תבהיר שמעשים של מניפולציה רגשית על בוחרים, המבוססים על עיבוד מידע בעל רגישות מיוחדת אודות הבוחרים באופן המפר את הוראות חוק הגנת הפרטיות, מהווים עבירה של שחיתות ואיום לפי סעיף 122(6) לחוק הבחירות.

לצד ועדת הבחירות המרכזית, על הרשות להגנת הפרטיות לפעול כבר עתה בשני מישורים מקבילים. האחד, לעשות שימוש בשלל סמכויות האכיפה והפיקוח הנתונות בידה טרם הכניסה לתקופת בחירות, על מנת לוודא שמפלגות מצייתות להוראות חוק הגנת הפרטיות. השני, לחדד בפני המפלגות את מהות דרישת ההסכמה מדעת ביחס לכלל עיבודי המידע האישי הנעשים על ידן במסגרת תעמולת בחירות; כיצד עליהן לציית לעקרון צמידות המטרה, לרבות בכל הקשור להתרת גישה למידע אודות הבוחרים לכל משתמש ביישומון הבחירות; וחשיבות אבטחת המידע ומשמעות דרישות אבטחת המידע ביחס לעיבוד המידע המבוצע על ידן, לרבות בכל הקשור לקביעת ומורשה גישה למידע ולאופן אימות זהותם. כן נציע כי הרשות להגנת הפרטיות תפרסם את עמדתה בכל הקשור לנושאים מהותיים שאין לגביהם הכרעה ובכלל אלה החובות החלות על מפלגה כגוף דו־מהותי, ופרשנות הרשות לגבי גירוד מידע אישי והסקת מידע אישי באמצעות בינה מלאכותית, בהקשרי בחירות.

לקראת מערכת הבחירות לכנסת ה־26, האתגר הניצב בפני גורמי האכיפה והפיקוח הוא כיצד להתאים את כללי המשחק הדמוקרטים למציאות שבה מידע אישי, בינה מלאכותית וכלי השפעה מתקדמים מאפשרים עיצוב שיטתי, מתמשך ולרוב בלתי נראה, של רצון הבוחר. זוהי שאלה עקרונית חוקתית: איזה סוג של השפעה פוליטית ניתן להתיר במסגרת משטר דמוקרטי, מבלי שעקרון הבחירות החופשיות יהפוך לפארסה. בהיעדר היערכות מוקדמת והבהרות נורמטיביות מצד ועדת הבחירות המרכזית והרשות להגנת הפרטיות, קיים חשש שיתרונות טכנולוגיים יהפכו ליתרונות פוליטיים בלתי הוגנים, ושהאיזון בין חופש הביטוי הפוליטי, לבין הגנה על פרטיות הבוחרים וחירות הבחירה שלהם, יופר.

נדמה שאפשר לחזור בעניין זה לדברי בית המשפט בעניין שרון, עוד משנות ה־70 של המאה הקודמת:

> **חובה להקפיד על כך, שהבחירות תהיינה חופשיות וטהורות מכל רבב של כפיה, השפעה לא הגונה ושחיתות, וכי יהיה ברור שהאזרח הבוחר, כשמימש את זכותו להצביע ומיצה את רצונו הפוליטי בפתק הבוחר, עשה כן כבן חורין ועל פי שיקול דעתו החופשי... חופש הבחירה משמעו לא רק החופש הפיסי – להטיל לקלפי את פתק ההצבעה, אלא גם, ובעיקר, החופש הגמור לעבור כבן חורין את תהליך ההצבעה מהבחינה הנפשית והשכלית. לכן, כל מעשה, שיש בו כדי לצמצם או לבטל, בין במישרין ובין בעקיפין, את חירות חשיבתו של הבוחר ויכולתו לתת ביטוי אמיתי לתכנית הפעולה הרצויה בעיניו ולהשקפת עולמו, על שיקול דעתו העצמי... פוגע בעיקרון הבסיסי של טוהר הבחירה ואי־תלותה.**[418]

[418] ע"פ 83/71 **שרון נ' מדינת ישראל**, פ"ד ל"ח (2) 757 בעמ' 765 (1984).

ד"ר רחל ארידור 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.

ד"ר תהילה שוורץ אלטשולר היא עמיתה בכירה וראשת התוכנית "דמוקרטיה בעידן המידע" במכון הישראלי לדמוקרטיה. תחומי עיסוקה משלבים טכנולוגיה, משפט, מדיניות ואתיקה ומתמקדים באסדרת בינה מלאכותית, רגולציה על תקשורת ורשתות חברתיות והגנה על זכויות אדם במרחבים טכנולוגיים. היא חברה בוועד המנהל של האוניברסיטה הפתוחה וכותבת טור בנושאי רגולציה וטכנולוגיה במגזין "דה מרקר".

המכון הישראלי
לדמוקרטיה

www.idi.org.il