

פרטיות ובחירות

לקראת בחירות 2026

רחל ארידור הרשקוביץ | תהילה שוורץ אלטשולר

מרץ 2026

הצעה
לסדר
64



המכון הישראלי
לדמוקרטיה



המכון הישראלי
לדמוקרטיה

פרטיות ובחירות: לקראת בחירות 2026

רחל ארידור הרשקוביץ |
תהילה שוורץ אלטשולר

הצעה לסדר 64
מרץ 2026

The Algorithmic Campaign: Voter Privacy and the 2026 Israeli Elections

Rachel Aridor Hershkovitz | Tehilla Schwartz Altshuler

עריכת הטקסט: לילך צ'לנוב

עיצוב הסדרה והעטיפה: סטודיו Alfabees

ביצוע גרפי: נדב שטכמן פולישוק

הדפסה: גרפוס פרינט, ירושלים

מסת"ב 2-526-519-965-978

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר), 2026

נדפס בישראל, תשפ"ו/2026

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

המכון הישראלי לדמוקרטיה

רח' פינסקר 4, ת"ד 4702, ירושלים 9104602

טל': 02-5300888

אתר האינטרנט: www.idi.org.il

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

המכון הישראלי לדמוקרטיה

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

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

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

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

תוכן העניינים

7	תקציר
---	-------

8	מבוא
---	------

חלק ראשון
תעמולה דיגיטלית באמצעות מידע אישי

11	פרק 1. שימושים במידע אישי בתעמולת בחירות
42	פרק 2. פרטיות ובחירות בישראל: המצב המשפטי והמצב למעשה

חלק שני
תיקון 13 והשפעתו על השימוש במידע אישי על בעלי זכות הצבעה
במהלך תעמולת בחירות

55	מבוא
56	פרק 3. מידע אישי, מידע בעל רגישות מיוחדת ומאגר מידע לפי חוק הגנת הפרטיות
67	פרק 4. בעלי תפקידים וחובותיהם
71	פרק 5. החובות העיקריות המוטלות על מפלגות ועל מפעילי יישומוני בחירות

פרק 6. הגבלות ואיסורים על עיבוד המידע האישי במאגר מידע 85

פרק 7. כיבוד זכויות נושא המידע 106

פרק 8. פיקוח ואכיפה מצד הרשות להגנת הפרטיות,
בשגרה ובתקופת בחירות 113

חלק שלישי

המלצות לקראת הבחירות לכנסת ה-26

מבוא 131

פרק 9. המלצות לרשות להגנת הפרטיות 132

פרק 10. המלצות ליו"ר ועדת הבחירות המרכזית 141

פרק 11. שאלון בחינה עצמית למפלגות ומי שפועלים מטעמן,
לעמידה בדרישות חוק הגנת הפרטיות בעיבוד מידע על בוחרים 149

סיכום 156

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 מתרחש 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, מתוך טשטוש הגבולות בין מידע שנמסר בודיעין 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 מהותית את אופי ההשפעה הפוליטית על ציבור הבוחרים. עקב כך הם גם יוצרים סיכונים ממשיים לזכות לפרטיות, לאוטונומיה של הבוחרים, לחשאיות הבחירות ולטוהר הבחירות.

על רקע הבחירות הקרבות 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 ארגז כלים יישומיים להתמודדות עם האתגרים האלה, ובהם עקרונות פעולה והכוונה רגולטוריים לגורמי הפיקוח הרלוונטיים, ובראשם יו"ר ועדת הבחירות המרכזית והרשות להגנת הפרטיות, לצד שאלון בדיקה עצמית וניהול סיכונים פרטיות למפלגות ולגורמים המפעילים יישומוני בחירות. כלים אלו נועדו לסייע בזיהוי מוקדם של אתגרים הנובעים משימוש במידע אישי ובטכנולוגיות מתקדמות, ולשפר את היכולת להבטיח שימוש ראוי במידע במסגרת תעמולת בחירות, כדי להגן על פרטיות הבוחרים ועל תקינות ההליך הדמוקרטי.

מבוא

תעמולות בחירות נשענה מאז ומתמיד על מידע אישי על 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 שלו לנשיאות בשנת 2008.² בקמפיין הבחירות לנשיאות ארצות הברית בשנת 2016 הופצו ברשתות חברתיות מסרי תעמולה אישיים לתמיכה בדונלד טראמפ, על בסיס מידע אישי שנאסף עליהם בפיסיסבוק, ועיבדה, ללא הסכמתם, 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. על פי ממצאי ניתוח זה התמקד קמפיין הבחירות של טראמפ בכ-6.3 מיליון מצביעים בשבע מדינות מתנדדות, ולהם הוצגו מסרי בחירות בפרסומות בשידורי הזרמת מידע (סטרימינג), בדיוור ישיר ובהודעות טקסט. כך הצליח קמפיין הבחירות למשוך את תשומת ליבם של בוחרים מתלבטים במדינות מפתח בהשקעת משאבים כספיים מועטה יחסית.⁴

בגרמניה, בבחירות בשנת 2021, עשו כל המפלגות שימוש במיקוד מדויק (מיקרו-טירגוט) פוליטי בפיסיסבוק כדי לשכנע מצביעים. תלונות ששימוש כזה הוא הפרת האיסור הקבוע ב-GDPR (התקנות האירופיות בעניין הגנת מידע) על שימוש

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

Ed Pilkington & Amanda Michel, *Obama's Team of Tech Gurus to Unleash "Holy Grail" of Digital Campaigning*, THE GUARDIAN (May 14, 2012)

Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018); Joe Westby, *'The Great Hack': Cambridge Analytica is just the Tip of the Iceberg*, AMNESTY INTERNATIONAL (Jul. 24, 2019)

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

במידע על דעה פוליטית,⁵ הוגשו לנציבות הגנת המידע בגרמניה. ואולם, במערכת הבחירות הפדרליות בשנת 2025 המשיכו המפלגות לעשות שימוש בטקטיקה זו, אך השתמשו לשם כך במידע אישי שאינו דעה פוליטית, כמו מידע על להקות אהובות, כדי להעריך את נטייתם הפוליטית של הבוחרים.⁶

להתפתחות הטכנולוגית המאפשרת תעמולה ממוקדת אישית המבוססת על מידע אישי ועיבודו באמצעות בינה מלאכותית ("תעמולה חישובית") יתרונות רבים, אך היא מעלה גם חששות לא מעטים, ובראשם היכולת להשפיע על דעות פוליטיות, ובעיקר על העדפות והתנהגויות של הבוחרים, כגון על ידי יצירת מניפולציה שתביא לדיכוי הצבעה של ציבור מסוים. יכולות אלו מעניקות למועמדים ולמפלגות יתרון על פני הבוחרים ומאיימות על תקינות הליך הבחירות ועל עקרון ההוגנות בבחירות.⁷ משום כך, השאלות מהו סוג המידע האישי שמותר לעשות בו שימוש במסגרת תעמולת בחירות, מהו ההיקף המותר, ומהם השימושים המותרים למניפולציה על בוחרים במסגרת זו, עומדות היום בלב הדיון במדינות דמוקרטיות רבות.⁸

במערכות הבחירות האחרונות בישראל כשלו הניסיונות להתמודד בזמן אמת, במהלך מערכת הבחירות עצמה, עם התכר שבין דיני הפרטיות לדיני הבחירות, כפי שהוא בא לידי ביטוי בשימושים במידע אישי, בעיקר באמצעות יישומי בחירות, וההשלכות האפשריות של שימושים אלו על הגנה על זכות הבוחרים לפרטיות ועל עקרון טוהר הבחירות והוגנות הבחירות. אולם, טכנולוגיות תעמולה

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

noyb, *Snap Election Faster than German DPAs: Microtargeting Continues to Influence Voters* (Feb. 21, 2025)

Stephan Lewandowsky & Peter Pomerantsev, *Technology and Democracy: a Paradox Wrapped in a Contradiction inside an Irony*, MEMORY, MIND & MEDIA 1:e5 (2022)

Judit Bayer, *Double Harm to Voters: Data-Driven Micro-Targeting and Democratic Public Discourse*, 9(1) INTERNET POLICY REVIEW (2020); Cristina Blasi Casagran & Mathias Vermeulen, *Reflections on the Murky Legal Practices of Political Micro-Targeting from a GDPR Perspective*, 11(4) INTERNATIONAL DATA PRIVACY 348–359 (2021)

ממוקדת אישית המבוססות על מידע, לרבות מידע אישי, וגם הכללים המשפטיים המאסדרים שימוש במידע אישי, השתנו דרמטית מאז מערכת הבחירות הקודמת בשנת 2022.

ראשית, כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות באוגוסט 2025⁹, צפויה להשפיע על השימוש שיעשה במידע אישי על אודות בעלי זכות ההצבעה בישראל במערכות הבחירות הבאות. תיקון 13 והמהלכים הנלווים לו מביאים עימם שינוי עמוק בתפיסת ההגנה על מידע אישי בישראל, ומציבים סטנדרטים חדשים של אחריות, פיקוח וממשל נתונים.

שנית, היכולות הטכנולוגיות לנתח מידע אישי, להסיק היסקים מבוססי מכונה, למיקוד מדויק ולהשפעה פוליטית השתכללו מאוד בשנים האחרונות, בעיקר על רקע ההתפתחויות המואצות בתחום הבינה המלאכותית.

שלישית, החששות מפני דליפות מידע, מתקפות סייבר ושימושים עוינים בנתונים גרישים נעשו נוכחים ומוחשיים במיוחד בימינו, והמלחמה מ־7 באוקטובר, וגם התפתחות טכנולוגיות בתחום הסייבר, מחדדות את פגיעותן של מערכות מידע.

מטרתו העיקרית של המחקר הזה היא להבהיר את התפר המחודש שבין דיני הפרטיות לדיני הבחירות. במחקר ארבעה חלקים: בחלק הראשון נעסוק בתעמולה חישובית ובמאפייניה בעיקר בהיבט המעבר לתעמולה מבוססת בינה מלאכותית, וכן ביישומי הבחירות, שהם היום המכשיר המרכזי לניהול בחירות, ובפוטנציאל הטכנולוגי שהתווסף בשנים האחרונות בשל פיתוח יישומים המבוססים על 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, הרלוונטיים לשימוש במידע אישי במסגרת תעמולת בחירות; ובחלק הרביעי נציע המלצות ליישום ולשינוי, ונציג שאלון בחינה עצמית למפלגות ולמנהלי יישומים הקשורים לבחירות לעמידה בדרישות החוק, וכן המלצות לרשות להגנת הפרטיות וליו"ר ועדת הבחירות המרכזית.

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 1

שימושים במידע אישי בתעמולת בחירות

1.1. מבוא

"תעמולה חישובית" היא שימוש בכלים דיגיטליים להפצת מסרים פוליטיים. מפלגות ומועמדים בקמפיין בחירות אוספים ומרכזים נתונים דיגיטליים אישיים מזוהים על בוחרים בהיקף רחב, מתוך ייחוס ערך אסטרטגי לעצם צבירתם. הם מנתחים את הנתונים בשיטות חישוביות ובכלים מתחום חקר ההתנהגות, ותוצרי הניתוח משמשים אותם ליצירה ולהפצה של מסרים פוליטיים המותאמים אישית לבוחרים בקנה מידה רחב.¹⁰

The European Commission, *Study on the Impact of New Technologies on Free and Fair Elections* (Sep. 2021); 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)

יצירת הפרופילים האישיים משפיעה הן על הבוחרים נושאי המידע, הן על החברה הדמוקרטית, בעיקר בשל חוסר ההגינות האניהרנטי העולה מהחידרה למכמני נפשו של אדם בעזרת שימוש בטכנולוגיה והתאמת המסרים ל"מקומות הרכים" שבהם הוא עשוי להיות רגיש יותר להשפעה. העובדה שרוב המידע נאסף ומעובד ללא ידיעת הבוחרים ו"מחוץ לרדאר" התודעה שלהם, מאיימת על חופש הבחירה שלהם ויוצרת "מלכודת" העלולה לפגוע באוטונומיה שלהם בעוצמה ובאיכות שלא ידענו כמותן בעבר.¹¹ יש הטוענים כי בשנים האחרונות מצויות מפלגות בכל העולם הדמוקרטי ב"מרוץ חימוש של נתונים", שבו הן נשענות על ספקים מסחריים רבי עוצמה, בעוד שהרגולציה והאכיפה נותרות חלקיות, ולעיתים עמומות. מצב זה פוגע בשקיפות, יוצר פערי כוח ניכרים, ומערער את אמון הציבור בטוהר הליך הבחירות.¹² על כן, הגדרת גבולות הלגיטימיות של תעמולת הבחירות באמצעות תעמולה חישובית ואסדרתה חשובות מאוד, והתכפר שבין דיני הפרטיות – איסוף סוגים שונים של מידע; הגדרת הרמה והעומק של הפרופילים שמפלגות ומועמדים יכולים לבנות ולאגור; מיקוד מדויק של השפעה (מיקרו־טירגוט) על בוחרים – לבין דיני הבחירות, הוא קריטי.¹³

קמפיינים פוליטיים מבוססים על שתי שאלות יסוד: האחת – האם מדובר בבוחר שבכוונתו לצאת ולהשתתף בהצבעה? והאחרת – האם אותו בוחר יצביע למפלגה שלה מיועד הקמפיין? קמפיין דיגיטלי מבוסס נתונים נועד לפלח את הבוחרים לאחת מחמש קטגוריות: (א) מי שיוצאים להצביע ויצביעו למפלגה המועדפת; (ב) מי שיוצאים להצביע ויצביעו למפלגה אחרת; (ג) מי שאינם יוצאים להצביע אבל תומכים במפלגה המועדפת; (ד) מי שאינם יוצאים להצביע אבל תומכים במפלגות אחרות; (ה) מי שמתלבטים לאיזו מפלגה להצביע; ולמצוא את הבוחרים שניתן להניע אותם לפעולה הרצויה. הפילוח נעשה באמצעות סוגים

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, בעמ' 16-19.

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

1.2. מרכיבי קמפיינים של תעמולה חישובית

קמפיינים מבוססי נתונים (Data-Driven Campaigning, DDC), או קמפיינים של תעמולה חישובית,¹⁵ מבוססים על שני מאפיינים מרכזיים: האחד הוא מיקוד (טירגוט), כלומר קביעה "מה" (איזה מסר) יישלח ל"מי" (לאילו בוחרים) ו"מתי" (באיזה שלב של הקמפיין); והשני הוא בדיקה אמפירית (testing), כלומר מדידה שיטתית של יעילות המסרים השונים והשוואתם זה לזה, כדי להפיק תובנות המכוונות את המשך פעילות המיקוד.¹⁶ כדאי להדגיש שאין מדובר רק במאפיינים טכנולוגיים, אלא גם במאפיינים תפקודיים. אכן, ארגונים פוליטיים אוספים נתונים אישיים בהיקף נרחב על בוחרים ויוצרים מהם מאגרי נתונים גדולים ומפורטים, ונתונים אלו מנותחים באמצעות כלים סטטיסטיים ומודלים אלגוריתמיים המאפשרים הפצה של מסרים מותאמים אישית בקנה מידה המוני.¹⁷ אולם, בה בעת תוצאות הניתוחים האלה והמלצות המערכות הטכנולוגיות נהפכות לגורמים מכריעים בקבלת ההחלטות של ניהול הקמפיין, עד כדי כך שהן עשויות לקבוע את כיווני הפעולה הטקטיים והאסטרטגיים, לעיתים באופן אוטומטי

14 שם.

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); Hendrik Mildebrath, *The Arrival of E-voting and Campaign Technologies in Europe: Promise, Perils and Preparedness* (EPRS | European Parliamentary Research Service, May 2024)

Jessica Baldwin-Philippi, *The Myths of Data-Driven Campaigning*, 16 34(4) POLITICAL COMMUNICATION, 627–633 (2017)

Elizabeth F. Judge & Michael Pal, *Voter Privacy and Big-Data Elections*, 58(1) OSGOOD HALL LAW JOURNAL 1–55 (2021)

ודטרמיניסטי וללא דיון אנושי שוטף. המערכת הארגונית של הקמפיין פועלת כך שהקצאת המשאבים, בחירת קהלי היעד ועיצוב המסרים נקבעים בעיקר על בסיס הנתונים והמודלים האלגוריתמיים, ולא על פי שיקול דעת אנושי.

בקמפיין תעמולה חשובית שלושה שלבים: (א) איסוף המידע על הבוחרים; (ב) ניתוח ועיבוד שלו; (ג) התאמת המסרים ומיקוד קהלי היעד שלהם (טירגוט).

השלב הראשון הוא איסוף נתונים על בוחרים. נתונים אלו צריכים להיות בהיקף וברמת פירוט המאפשרים מיקוד אישי מדויק. כלומר, מדובר בכריית מידע על בוחרים ועיבודו למידע ממין. הנתונים כוללים פרטים אישיים (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 אלו יכולים להגיע מארבעה סוגי מקורות עיקריים:

(1) רשומות ציבוריות, כגון פנקסי בוחרים

רשומות ציבוריות הן בראש ובראשונה פנקס הבוחרים, אך יכולות להיות רחבות ממנו 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 למיניהם, 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 כדי לקבל שירות ציבורי מסוים, פוגע באמון הציבור ויוצר ערבוב בין משאבי המדינה לבין פעילות מפלגתית. לפי ממצאי הדוח, טשטוש הגבולות בין הממשלה לבין מפלגת השלטון, נוסף על השליטה המוסדית של הממשלה בגופים ציבוריים, תרמו לכך שהפיקוח של הרשויות על השימוש במידע הזה לא

היה אפקטיבי. 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 להטב מידע זה לשימוש פוליטי מעניקה יתרון חשוב למפלגת השלטון.¹⁸

רשומות ציבוריות שבידי המדינה עשויות לכלול גם מידע סטטיסטי ומידע ממרשם 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 הזה יש ערך גם במסגרת תעמולה חישובית.¹⁹

(2) מאגרי מידע מסחריים של חברות פרטיות

מאגרי מידע מסחריים של חברות פרטיות עשויים לכלול מידע שנאסף מהמשתמשים עצמם או מגופים שהעניקו להם שירותים. החל בהיסטוריית קניות בסופרמרקט שמקורה בחברות מרכולים או בהיסטוריית אשראי המגיעה מחברת האשראי, דרך "שביל פירורי הלחם הדיגיטליים" – פעילות דיגיטלית, כמו שימוש ביישומונים סלולריים, היסטוריית גלישה ונתוני מיקום, וכלה בשימוש במוצרים דיגיטליים לבישים, כגון שעונים חכמים ומכשירים אחרים המקושרים לרשת האינטרנט באמצעות מכשירי ה-GPS בטלפונים שלהם, Bluetooth ורשתות WiFi, והכול בזמן אמת וברמות דיוק גבוהות.²⁰

18 Human Rights Watch, *Trapped in a Web: The Exploitation of Personal Data in Hungary's 2022 Elections* (2022)

19 Lucas Georges, Gabriel Charpentier & Pierre Lison, *Re-identification of De-identified Documents with Autoregressive Infilling* (May 2025)

20 פרסומאי שעבד עם מפלגת הליכוד טען בריאיון לאחר הבחירות במרץ 2020, שבליכוד ידעו היכן המצביעים נמצאים ברמת דיוק של 15 מטרים, 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 "יידענו לעקוב אחרי הטלפון של כל אחד, זה היה בדאטה שלנו, האם הוא הלך לאזור הקלפי או נשאר בבית" העין השביעית (7.3.2020).

מידע על גולשים אינו מושג רק באמצעות מעקב ישיר אחריהם, אלא גם באמצעות ניתוח של מאגרי מידע גדולים כדי לאתר אנשים העשויים להיות בעלי מאפיינים דומים לאנשים שיש עליהם מידע אישי בעקבות מעקב ישיר אחריהם. הטכניקה של "אפיון דומים" (Look-alike Modelling) מאפשרת למשווקים "לשפוט" 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 שהזנו על קבוצת המקור, מזהה דפוסים במאפיינים האלה, ולאחר מכן מחפש בבסיס המשתמשים הקיים בפלטפורמה משתמשים בעלי 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 "Look-alike Audiences", ובפלטפורמת הפרסומות של גוגל "Similar Audiences". עם זאת, גם חברות עצמאיות המפתחות יישומי בחירות ייעודיות עושות שימוש באלגוריתמים דומים.²¹ בדרך זו מנהל הקמפיין הפוליטי יכול להגדיל ביעילות את קהל היעד למסרי התעמולה שלו.²² נוסף על כך, יישומי בחירות למיניהם 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 על מידע על בוחרים מבחירות קודמות שלא נמחקו.**

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](#).

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)

(4) **מידע הנאסף מהאינטרנט**, לרבות אפשרויות מיקוד המוצעות על ידי רשתות חברתיות וכוללות פרטי 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 במאגרים של ספקים חיצוניים.²³

השלב השני בקמפיין תעמולה חשבונית הוא ניתוח הנתונים ויצירת "פרופיל" לכל בוחר. יש שיטות שונות לניתוח נתונים לשם יצירת פרופיל באמצעות תוכנות ניתוח, למטרות של חיזוי, מדרוג (רייטינג) וניקוד (סקורינג). שיטות 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 כדי להצטרף לרשת חברתית או לקבלת שירותים אחרים, לבין פרדיגמת המיקוד שלהן.²⁴

השלב השלישי בתעמולה חשבונית הוא יישום תוצאות הניתוח כדי ליצור תקשורת פוליטית מותאמת אישית. תקשורת זו כוללת (1) עיצוב של מסרים מותאמים אישית, ו-(2) הפצה מותאמת אישית לבוחרים. אחד הכלים המרכזיים בשלב הזה הוא פרסום ממוקד (micro-targeted advertising) ברשתות

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 247 (2024)

24 Rachel Kraus, *How Well Does "Microtargeted Psychographic Advertising" Work Anyway?* MASHABLE (Mar. 24, 2018)

חברתיות, באמצעות מערכות התאמה אוטומטיות של פלטפורמות; שימוש בפלטפורמות הזרמת מידע (סטרימינג) דיגיטליות; או הפצה מתואמת לא אותנטית ברשתות חברתיות של תכנים, כגון פוסטים, ציורים, סרטונים והודעות טקסט, שנועדו להיות מופצים מחדש ברשת באופן ויראלי ולתת לגולשים תחושה כוזבת שהגיעו אליהם באופן אורגני. נקודות ההשקה עם מושא הקמפיין יכולות לנוע מטלוויזיה מסורתית חכמה ועד פרסום מותאם אישית במשקפיים חכמים, כדי להתאים תכנים לאנשים מסוימים ולפלטפורמות ספציפיות; לקבוע מועד ההפצה מדויק, למשל סמוך להתרחשותם של אירועים, ואת מיקומה הגאוגרפי, למשל כאשר מושא הקמפיין נמצא במקום מסוים; וליצור "קריאייטיב דינמי", כלומר לתפור מסרים המתפתחים לאורך זמן ומתאימים את עצמם בכל פעם מחדש למושא המסר. מאפיין מרכזי של שלב זה הוא אופיו המחזורי והניסויי – הצלחת המסרים נמדדת 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) כדי להעריך את הסיכוי שבוחר מסוים יגיב למסר מסוים או שהמסר יניע אותו לפעולה מסוימת. מיקוד מדויק (טירגוט) ברשתות חברתיות, למשל, מבוסס על עיבוד המידע ואיתור קשרים עם המשתמשים על פי 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 "טירגוט פסיכוגרפי".²⁶

Katherine Haenschen, *The Conditional Effects of Microtargeted Facebook Advertisements on Voter Turnout*, 45(4) POLITICAL BEHAVIOR 1661–1681 (2023); 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)

שאלת האפקטיביות של מיקוד אישי מדויק (מיקר-טירגוט) המבוסס על מאפייני ניתוח פסיכוגרפי הייתה מושא לכמה מחקרים, וחלקם הראו אפקטיביות בינונית בלבד.²⁷ כך גם טענו מפעילי חברת "קיימברידג' אנליטיקה" לאחר שהתגלה השימוש שעשו בפלטפורמה של פייסבוק בבחירות 2016 בארצות הברית.²⁸ בסעיף הבא נראה כיצד משתנות עמדות אלו לנוכח ההתפתחות בתחום מערכות מבוססות בינה מלאכותית מתקדמות יותר.

עוד נעיר כי חלק מהקשר 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 את מתלבטת?) ומעבירים מסרים פוליטיים מותאמים.²⁹ המיוחד ב־Canvassing בעולם של תעמולה חשובית הוא שמתנדבים או עובדי מפלגה נשענים על אפליקציות ייעודיות המציגות להם שכבות מידע על הבוחרים, מאפשרות להם להזין נתונים ומסנכרנות את הנתונים האלה עם מאגרי המידע המרכזיים של המפלגה. כלומר, מדובר במפגש פיזי-אנושי, המוזן, מנותב ומעובד דרך תשתיות נתונים דיגיטליות.³⁰

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)

28 Emma Woollacott, *Cambridge Analytica Did Not Influence Brexit Referendum*, FORBES (8.10.2020)

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 (Higher Grounds Labs, Spring 2025)

1.3. מתעמולה מבוססת נתונים לתעמולה מבוססת

בינה מלאכותית

העשור האחרון התאפיין בהתבססותה של תעמולת בחירות על איסוף וניתוח שיטתי של מידע אישי על בוחרים. כפי שתואר לעיל, מודל התעמולה החישובית (ה־Data-Driven Campaigning) נשען על איסוף מידע בהיקף נרחב על אזרחים, ניתוחו באמצעים סטטיסטיים ואלגוריתמיים, ושימוש בתובנות המתקבלות מהניתוח לשם התאמת מסרים פוליטיים והפצתם לקהלי יעד שונים. אולם, ההתפתחות בתחום הטכנולוגיות למימוש מהלכי תעמולה חישובית בארבע השנים האחרונות הייתה דרמטית, ולכן נוצר שוני מהותי בין הטכנולוגיות המשמשות היום לבין מה שהיה מקובל במסעות תעמולה פוליטיים בעבר, ובכלל זה במערכת הבחירות האחרונה בישראל.

התעמולה החישובית בעשור וחצי האחרונים התמקדה בעיקר באיסוף מידע על בוחרים ובהתאמת מסרים פוליטיים לקבוצות יעד מסוימות, ואילו טכנולוגיות בינה מלאכותית מאפשרות אוטומציה של תהליך ההשפעה הפוליטית כולו. מערכות בינה מלאכותית מסוגלות לייצר מסרים פוליטיים מותאמים אישית, לנתח תגובות רגשיות של בוחרים, לעשות ניסויים בזמן אמת ולשפר כל הזמן את האפקטיביות של הקמפיין. בה בעת הן מאפשרות הסקת מידע חדש על בוחרים מתוך עקבות דיגיטליים זמינים, גם כאשר המידע הזה לא נמסר במפורש.

בחלק זה נסקור את אבני הבניין הטכנולוגיות האלה ואת השלכותיהן. נדגיש כי עניינו הוא בעיקר בהיבטים הנוגעים לשימושי דאטה, לפרטיות וליצירת "מלכודות אוטונומיה" המאיימות על פרטיות הבוחרים.

1.3.1. שינוי אופי הפגיעה בפרטיות בעידן הבינה המלאכותית

בליבת הדיון בפרטיות בעידן הדיגיטלי עומדות הפעולות של איסוף מידע אישי, שמירתו, עיבודו, חשיפתו או דליפתו.³¹ אולם אתגרי הפרטיות הכרוכים במפגש עם מערכות מבוססות בינה מלאכותית קיימים בכמה מישורים נוספים. חלקם מוכרים יחסית מן הספרות, כגון האפשרות שמודלים "יספגו" מידע אישי מתוך מאגרי נתונים ויפרסמו אותו שוב פרסום לא מורשה; או האפשרות שמשמשים יזינו למערכות מידע רגיש בלי להבין שהוא נשמר, מעובד או משמש לשיפור המודל.³²

ואולם, מאמרים עדכניים מראים שמוקד הסיכון הוא יכולתן של מערכות להסיק מידע חדש על אדם מתוך נתונים קיימים. במובן זה, הבינה המלאכותית משנה את אופי הפגיעה בפרטיות מדיון בדבר הגישה לנתון אישי קיים, לעבר 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 אם דפוסים אלו 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 ותכונות

Grace Billiris, Assif Gill & Madhushi Bandara, *Privacy in the Age of AI: A Taxonomy of Data Privacy Risks* (Australasian Conference on Information Systems 2025, UniSC & AAIS) 31

Yifan Yao, Jinhao Duan, Kaidi Xu, Yuanfang Cai, Zhibo Sun & Yue 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) 32

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) 33

אישיות. במצבים האלה 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 גם מייצרת מידע עליהם. זהו שינוי עמוק באופייה של הפגיעה בפרטיות – מעבר ממידע גלוי למידע מוסק.³⁴

היבט מטרדי במיוחד הוא שקשה מאוד לזהות, לתעד ולפקח על היסקים ישירים ועקיפים כאלה. אחר איסוף נתונים או אחר שמירתם במאגרי מידע אפשר לעקוב, ואילו תהליך ההיסק מתרחש בתוך המערכת עצמה ואינו מותיר בהכרח עקבות ברורים. מבחינה זו, דיני הפרטיות הקיימים, הבנויים במידה רבה סביב שליטה במידע אישי קיים, נותנים מענה חלקי בלבד למצבים שבהם המידע הרגיש לא נאסף אלא נוצר מתוך נתונים שגורתיים, חלקם מידע אישי וחלקם אף עשוי להיות מידע בלבד ששולעצמו אינו מביא לזיהויו של אדם. הם אינם נותנים מענה גם לתרחישים שבהם המידע שתהליך ההיסק מבוסס עליו 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 מסוים אחד, אלא באיסוף, חיבור וניתוח של פיסות מידע מפוזרות ממקורות ציבוריים שונים כדי להרכיב פרופיל אישי מלא. אומנם המידע על האדם כבר נמצא ברשת, אך הוא מפוזר במקטעים, ורק באמצעות מערכות בינה מלאכותית אפשר לאתר, לאחד ולעבד אותו באופן אוטומטי. המערכת מאתרת מאפיינים מדויקים על אדם באמצעות חיפוש וניתוח רחבים של מידע ציבורי, לרבות באמצעות מערכות "חיפוש" מבוססות סוכנים או ניתוח עמוק של צ'טבוטים שאומנו לכך.³⁶ מידע שנאסף מכמה מקורות עשוי לאפשר לענות על שאלות הנראות שוליות, כמו מה שמו של חתול המחמד של

34 Niloofer Miresghallah & Tianshi Li, *Position: Privacy is Not Just Memorization!* (Oct. 2, 2025)

35 שם.

36 OpenAI, *Introducing Deep Research* (Feb. 2025)

אדם מסוים – אך שאלות כאלה עשויות לשמש בהמשך לשחזור סיסמאות, להשתלטות על חשבונות או ליצירת 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 ונתון, אלא ביכולת לחבר את העקבות הדיגיטליים לפרופיל אישי מדויק ומזוהה.³⁷

התפתחות נוספת בעלת משמעות היא מה שאפשר לכוונת "דמוקרטיזציה של יכולות מעקב". בעבר דרשו האיסוף, הסיתת והניתוח של היקפים גדולים של מידע פתוח ברשת משאבים טכנולוגיים גבוהים, מומחיות מקצועית וגישה לכלי מודיעין או דאטה מתקדמים, ואילו כיום מערכות בינה מלאכותית וסוכנים מורידים דרמטית את חסמי הכניסה לכך. היכולת לאסוף מידע ממקורות גלויים, לנתח אותו ולהסיק ממנו מסקנות נעשית זמינה גם לגורמים חסרי ידע טכני מוקדם. במובן זה בינה מלאכותית לא רק מעצימה יכולות מעקב קיימות, היא גם מפזרת אותן ומרחיבה את מספר הגורמים המסוגלים להפעילן.³⁸

בהקשר של תעמולה חישובית, המשמעות היא שהפגיעה בפרטיות אינה עוד תוצר בלעדי של מאגרי מידע מפלגתיים גדולים או של פלטפורמות טכנולוגיות

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

Zheyuan Liu, Guangyao Dou, Mengzhao Jia, Zhaoxuan Tan, Qingkai Zeng, Yongle Yuan & Meng Jiang, *Protecting Privacy in Multimodal Large Language Models with LLMU-Bench*, In PROCEEDINGS OF THE 2025 CONFERENCE OF THE NORTH AMERICAN CHAPTER OF THE ASSOCIATION FOR COMPUTATIONAL LINGUISTICS 4105–4135 (2025). מנגד כדאי לציין שיש המזהירים מפני התפיסה השגויה, ולפיה זמינותם של הכלים האלה מייצרת שוויון, הואיל ובפועל רק גורמים בעלי תשתיות הפצה, גישה לנתונים ויכולת להגיע לקהלים גדולים יכולים לממש את היתרון האלקטורלי. 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)

ענק. ככל שכלים מבוססי סוכנים הופכים נגישים יותר, גם יכולת המעקב, האיגום והאפיון (פרופיילינג) מתפשטת לגורמים קטנים יותר: קמפיינים מקומיים, פעילים ומתנדבים; חברות בינוניות וקטנות, וגם גורמים זרים. אם כן, השינוי אינו רק טכנולוגי אלא גם מבני: הוא משנה את מאזן הכוחות בין מי שאוספים מידע על בוחרים לבין הבוחרים עצמם.

1.3.2. יצירת תוכן פוליטי מבוסס מכונה

בינה מלאכותית יוצרת (Generative Artificial Intelligence) מאפשרת יצירת תוכן חדש – כגון טקסט, תמונות, קוד, מוזיקה וסרטוני וידאו – באמצעות אלגוריתמים מתקדמים של למידה חישובית. טכנולוגיה זו 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 היקפים אדירים של טקסטים כדי להבין ולהפיק שפה טבעית. המודלים פועלים בעיקר באמצעות ארכיטקטורת Transformer שמאפשרת להם לנתח הקשרים רחבים ולהגיב תגובות קוהרנטיות ורלוונטיות. דוגמאות למודלים מרכזיים כאלה הן Claude של Anthropic, Gemini של Google, ו-GPT של OpenAI.⁴⁰ מודלים אלו הם הבסיס למערכות צ'אט, למנועי חיפוש, לעוזרים אישיים, לכלים לכתיבה, לתרגום ולסיכום טקסטים, ההולכים ותופסים מקום מרכזי בחיי היום-יום ובמגוון מקצועות, תחומים ושימושים – מכתובת תכנים שיווקיים, סיכומי ישיבות ועזרה משפטית, ועד יצירת תמונות, הפקת מוזיקה, סימולציות, עיצוב גרפי, עריכת וידאו ויצירת דמויות דיגיטליות.

Adam Zewe, *Generative AI Explained*, MIT News (Nov. 9, 2023) 39

Stefan Feuerriegel, Jochen Hartmann, Christian Janiesch & Patrick Zschech, *Generative AI. BUSINESS & INFORMATION SYSTEMS ENGINEERING* (2023) 40

ככל שהמחקר והמסחור בתחום מתקדמים, כך גוברת חדירתם של כלים גנרטיביים לתוך תהליכים עסקיים, ממשלתיים וחינוכיים. היתרונות הבולטים של בינה מלאכותית יוצרת הם אוטומציה של משימות שגרתיות, שיפור חוויית לקוח וחווית עובד, הגדלת קצב היצירה והתפוקה, והנגשת כלים מתקדמים לאנשים שאין להם הכשרה טכנית.⁴¹ תכונות אלו הופכות את הבינה המלאכותית היוצרת לטכנולוגיה בעלת פוטנציאל גדול גם בתחום הקמפיינים הפוליטיים.

בינה מלאכותית מולטי־מודלית (Multimodal Artificial Intelligence) היא כינוי למערכות בינה מלאכותית המסוגלות לעבד ולשלב מידע ממקורות שונים זה מזה, טקסט, תמונה, שמע, וידאו ונתונים מבניים, לשם יצירת הבנה רחבה, אינטואיטיבית ומקיפה של סיטואציה או שאלה,⁴² וליצור מהם תוכן המשלב בין מגוון ערוצי מדיה. מערכות AI מסורתיות התמקדו לרוב בסוג מידע אחד בלבד, ואילו הבינה המולטי־מודלית מאפשרת לאחד את כל ערוצי המידע, באופן הדומה יותר לאופן שבו בני אדם תופסים את העולם: באמצעות קריאת שפה כתובה, חוש הראייה ויכולת דיבור.

יישומי הבינה המלאכותית המולטי־מודלית הם, בין השאר, מערכות חיפוש מידע משולבות, תרגום קונטקסטואלי (כגון שלטים בתצלום), אבחון רפואי משולב טקסט וסריקות,⁴³ ניתוח רגשות בשיחות, וכן ממשקים אינטראקטיביים, דוגמת מערכות ניהול שיחה המזהות גם טון דיבור וגם הבעות פנים.⁴⁴ אם בעידן

MIT Technology Review Insights, *Humans at the Heart of Generative AI*, MIT TECHNOLOGY REVIEW (2023) 41

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) 42

Adam Zewe, *Making AI Models More Trustworthy in High-Stakes Settings*, MIT News (May 1, 2025) 43

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) 44

התעמולה החישובית מבוססת הנתונים התמקדו קמפיינים פוליטיים בעיקר בהתאמת מסרים קיימים לקהלי יעד שונים (מיקרו־טירגוט), הטכנולוגיות הגנרטיביות מאפשרות שלב נוסף – **ייצור אוטומטי של מסרים פוליטיים מותאמים אישית**. במקום לבחור מבין מספר מצומצם של מסרים שונתבו מראש, מערכות בינה מלאכותית מסוגלות לייצר אין־סוף טקסטים, תמונות, סרטונים, קטעי קול ודמויות דיגיטליות בעלי ארבעה מאפיינים חשובים:

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

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

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

(4) הם אמניים ברמה כזאת שבני אדם מתקשים לזהות שהם יצירת מכוונה, ונראים "אנושיים" לא פחות מתכנים שיצרו בני אדם.⁴⁶

התפתחות זו משנה את מבנה הקמפיינים הפוליטיים במהותו. ראשית, היא מאפשרת מעבר מהתאמה של מסרים קיימים לייצור אוטומטי ומהיר של מסרים מותאמים אישית. שנית, היא מפחיתה מאוד את עלויות הפקת התעמולה הפוליטית. אם בעבר יצירת קמפיין דרשה צוותי קריאייטיב, הפקת

45 חלק מעניין זה נובע גם מכך שכיום פלטפורמות צ'טבוטים מבוססי מודלים גדולים של שפה אינן מגבילות את יכולות המיקוד והטירגוט, כפי שמחויבות לעשות פלטפורמות המדיה החברתיות, למשל. ראו Almog Simchon, Matthew Edwards & Stephan Lewandowsky, *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3 PNAS Nexus 1–5 (2024)

Angus R. Williams, Liam Burke-Moore, Ryan Sze-Yin Chan, Florence E. Enock, Federico Nanni, Ivesha 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)
Josh A. Goldstein, Jason Chao, Shelby Grossman, Alex Stamos & Michael Tomz, *How Persuasive is AI-generated Propaganda?*, 3(2) PNAS Nexus 34 (2024)
Yoshua Bengio, INTERNATIONAL AI SAFETY REPORT 50–57 (2nd edition, Feb. 2026)

וידאו וכתובת תכנים בהיקף רחב, היום אפשר לייצר גרסאות רבות של מסרים פוליטיים באמצעים אוטומטיים ובעלות נמוכה למדי. שילוב זה בין אוטומציה להזלת עלויות מאפשר להפעיל קמפיינים פוליטיים מדויקים ומותאמים אישית למספר רב של בוחרים ספציפיים ובהיקפים גדולים בהרבה מבעבר.

נדגיש כי ענייננו במסמך זה אינו בעצם יצירת התכנים בידי מכונות, כלומר ביכולת ההבחנה בין תוכן אותנטי לבין תוכן שהוא יציר מכונה, או בשימוש בבינה גנרטיבית לשם הפצת דיסאינפורמציה. אנו גם לא עוסקות בצעדי מדיניות והגנה בהקשר הזה, ובהם סימון תכנים יצירי מכונה, מערכות זיהוי מתמשכות של פעילות מתואמת לא אותנטית ברשתות חברתיות, חיזוק מנגנוני אימות זהות ומקור (provenance) של תוכן, פיתוח כלים לסימון תוכן חשוד עבור משתמשים וכיוצא באלו.⁴⁷ לצד זאת, יש לתת את הדעת לכך שהשימוש בכלי בינה מלאכותית כגון ChatGPT ו-Gemini עשוי להוביל לחשיפת מידע אישי על הבוחרים, לרבות מידע בעל רגישות מיוחדת, משום ששיתוף מידע אישי עם כלים אלו עלול להוביל לפגיעה בפרטיות.⁴⁸

1.3.3. מחשוב חישתי וניתוח רגשות בוחרים

מחשוב חישתי (Affective Computing) הוא תחום מתפתח בבינה מלאכותית, שמטרתו ליצור מערכות המסוגלות לזהות רגשות אנושיים לפרש ולדמות אותם, ואף להשפיע עליהם. תחום זה, שהציגה בפעם הראשונה החוקרת רזלינד פיקרד

47 בהקשר הזה, ראו שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 39-53, וכן בעת האחרונה החלטת יו"ר ועדת הבחירות לכנסת ה-26 בעניין חב"כ 12/26 מפלגת "בנט 2026" ואח' נ' הליכוד – תנועה לאומית ליברלית (29.1.2026), ובעניין חב"כ 15/26 מפלגת "בנט 2026" ואח' נ' הליכוד – תנועה לאומית ליברלית (12.2.2026).

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 (Jun. 6, 2024).

(Picard) בשנות ה-90 של המאה ה-20⁴⁹, 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; ניטור סימפטומים של דיכאון, חרדה ומצבים פסיכולוגיים אחרים, המבוסס על טון דיבור או על שפת גוף ומתן סיוע "פסיכולוגי" "טיפולי" מותאם; שיפור חוויית משתמש וחוויית לקוח על ידי תגובה מותאמת רגשית בזמן אמת; עיבוד של רגשות הקהל בזמן צפייה ביצירות מדיה למיניהן, התאמת מחיקה למצב רוח וכתובת שירה או סיפורת בעלות גוון רגשי מותאם אישית.

מערכות אלו אינן מסתפקות בעיבוד קוגניטיבי אלא שואפות לדמות התנהגות רגשית, ובכך הן חוצות את הגבול שבין כלי ניתוח לאובייקט של קשר. כך, לדוגמה, אם מערכות NLP סטנדרטיות מזהות תבניות תחביריות או מילים טעונות, מערכות מחשוב חישתי מזהות שהטון העדין או ההבעה הנלווית מרמזים על אירוניה, על עצב או על חרדה, ומתאימות לו את תגובתן. כך נוצרות אפשרויות לשינוי התנהגות אנושית לא רק על סמך ניתוח מידע, אלא גם על

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

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

הבנה וניהול של מחוות גוף פיזיות ותגובות רגשיות.⁵¹ המערכות האלה מעוצבות במכוון ליצירת קשר רגשי עם המשתמשים, ולכן עלולות לעודד תלות או אשליה של אינטימיות.⁵² אחת הדוגמאות הבולטות היא שימוש גובר בצ'טבוטים רגשיים המלווים אנשים בשיחות יום-יומיות, 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 ולפרש רמזים רגשיים, כגון טון דיבור, הבעות פנים, תנועות גוף, פניות לשוניות ומאפיינים גופניים והתנהגותיים אחרים, ולהגיב להם ברזולוציה 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, הן ליצירת מנגנוני השפעה שאינם שקופים למשתמש. כאשר מערכת מזהה מצב רגשי ומגיבה לו בזמן אמת, נוצר קשר שאינו סימטרי: המשתמש עשוי לפרש את התגובה כתקשורת אותנטית, אך 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 יחסי הגומלין בין אדם למערכת דיגיטלית, מרחיבים את מרחב הפגיעות הרגשית, ומאפשרים השפעה על עמדות ועל התנהגויות בדרכים שאינן מבוססות רק על מידע או טיעון אלא גם על ניהול מצבים רגשיים.

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

Rhiannon Williams, *The AI Relationship Revolution is Already Here*, 128(2) MIT TECHNOLOGY REVIEW 20–27 (2025) 52

Kate Darling, *It's No Wonder People Are Getting Emotionally Attached to Chatbots*, WIRED (Jan. 8, 2024) 53

Ayşe A. Bozdağ, *The AI-Mediated Intimacy Economy: A Paradigm Shift in Digital Interactions*, 40(4) AI & SOCIETY 2285–2306 (2024) 54

לתוך מערך זה נוסף גם הסיכון המתפתח הנוגע ליחסים בין אנשים למכונות. דוח סיכוני הבינה המלאכותית של יהושע בנג'יו מציין תופעות כגון הטיית אוטומציה (Automation Bias) – מצב שבו אנשים מפתחים אמון יתר במערכת ומפסיקים להפעיל שיקול דעת עצמאי גם אם היא שוגגת; 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 של ממש 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 עשוי להחריף מחלוקות חברתיות ולתרום לבעיות נפשיות, כגון בדידות והתמכרות.⁵⁶ לכן נטען שמחקר עתידי נדרש לבחון כיצד אפשר להסדיר את השימוש במודלים גנרטיביים כדי למנוע ניצול לרעה שלהם, למשל בקידום רכישה כפייתית ובפרקטיקות שיווק מניפולטיביות.⁵⁷

התפתחויות אלו חשובות במיוחד לאפקטיביות של התקשורת ושל ההשפעה הפוליטית.⁵⁸ תעמולה חישובית בעידן הנתונים התמקדה בעיקר בזיהוי דפוסי התנהגות של בוחרים – מי יוצא להצביע ומי לא, ואילו הטכנולוגיות האלה 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 כדי שיעורר תחושות תקווה, פחד, הזדהות או כעס,

55 Bengio, לעיל ה"ש 46.

56 Sandra Matz, et al., *The Potential of Generative AI for Personalized Persuasion at Scale*, 14(4692) SCIENTIFIC REPORTS (2024)

57 Timothy Aylsworth, *Autonomy and Manipulation: Refining the Argument against Persuasive Advertising*, 175(4) JOURNAL OF BUSINESS ETHICS 689–699 (2022)

58 Hause Lin et al., *Persuading Voters Using Human-Artificial Intelligence Dialogues*, 648 NATURE 394–401 (2025)

על פי מאפייני הנמען ותגובותיו. ההשפעה הפוליטית של יצירת תכנים מותאמים אישית ומבוססים על מחשוב חישתי עשויה לשקף גם מציאות פרשנית אחרת עבור מושאי מידע שונים, שאינה עולה בהכרח לכדי דיסאינפורמציה, אבל משפיעה על עמדות ורעיונות.⁵⁹ התאמה כזאת עשויה לגרום לאנשים לפתח עמדות חיוביות יותר כלפי מועמדים או כלפי סוגיות משהיו מפתחים בלעדיה. כאשר היכולות האלה פועלות בתוך סביבות מידע מקוונות שכבר נוטות ליצור "מעורות הדדיות" ולחזק הטיות אישיות, כלומר מגבירות את החשיפה בעיקר לתכנים התואמים את תפיסות העולם הקיימות של המשתמש, הן עלולות להעמיק עוד יותר את ההסתגרות של אנשים בעולמות מידע אישיים ומבודדים שחסרה בהם מציאות משותפת עם אחרים.⁶⁰

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

1.3.4. סוכני בינה מלאכותית וקמפיינים אוטונומיים

סוכן בינה מלאכותית (AI agent) הוא מערכת בינה מלאכותית בעלת התנהגות מכוונת מטרה, המסוגלת לקבל החלטות אוטונומית, להסתגל לסביבה משתנה ולעשות פעולות המשנות את המציאות. מערכות אלו מסוגלות לעשות סדרת

59 Simchon et al., לעיל ה"ש 45.

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

61 Simchon et al., לעיל ה"ש 45.

62 Simon & Altay, לעיל ה"ש 38.

63 שם.

פעולות לשם השגת מטרות מוגדרות, בין משימות חד־פעמיות, בין 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 בעצמו ולומד מניסיון. לעיתים הוא גם משתף פעולה עם סוכנים אחרים או עם בני אדם כדי למלא משימות מורכבות בדרך מיטבית.⁶⁴

סוכני בינה מלאכותית שונים מהותית ממודלי שפה גנרטיביים פשוטים דוגמת ChatGPT הפועל כתוכנת צ'ט סטטית. בעוד שצ'טבוטים רגילים מייצרים תגובה טקסטואלית לבקשה אנושית, סוכנים פועלים כישויות עצמאיות, הם מקבלים מטרה כללית, בונים תוכנית פעולה, מיישמים שלבים בתוכנית 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 היום של המשתמש, ללא התערבות אנושית שוטפת.⁶⁵

השימוש בסוכני בינה מלאכותית הופך נפוץ יותר במגוון תחומים: חברות כמו OpenAI, Anthropic ו־Google DeepMind, וכן ענקיות כמו LinkedIn ו־Stripe מפתחות ומשלבות סוכנים במערכות שירות, סיוע אישי, ניתוח מידע וייעול תהליכים. המטרה העיקרית היא לאפשר למערכות לפעול בעצמן, להפחית את העומס על עובדים אנושיים ולייעל תהליכים עסקיים, מתוך שמירה על רמה מינימלית של פיקוח והתערבות מצד המשתמשים.

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 לתכלל סוגי מידע שונים ולפעול ברציפות להשגת מטרות מורכבות ורב־תחומיות.

Will Douglas Heaven, *OpenAI Launches Operator, an Agent that Can Use a Computer for You*, MIT TECHNOLOGY REVIEW (Jan. 23, 2025)

Rhiannon Williams, *OpenAI's New Agent Can Compile Detailed Reports on Practically any Topic*, MIT TECHNOLOGY REVIEW (Feb. 3, 2025)

בהקשר הזה מתחדדת ההבחנה בין סוכן בינה מלאכותית (AI Agent) לבין המושג הרחב יותר של בינה מלאכותית אייג'נטית – "סוכנות בינתית" (Agentic AI).⁶⁶ סוכן בינה מלאכותית הוא כלי ממוקד משימה, הפועל לרוב בתוך מסגרת פעולה מוגדרת ומונחה על ידי קלט אנושי ראשוני, ואילו סוכנות בינתית 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 יצירתי, בלמידה מתמשכת, וביכולת לקבוע ולשנות את מטרותיה בהתאם לשינויים בסביבה או ביעדים.⁶⁷

כאשר סוכנים רבים פועלים יחד במערכת 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 ובתיאום, בעלי זהות מתמשכת וזיכרון, המסוגלים לתקשר ביניהם, להתאים את התנהגותם בזמן אמת ולחדור לקהילות מקוונות בעזרת חיקוי התנהגות אנושית.

בהקשר הפוליטי, מערכות מסוג זה עשויות לשנות שינוי מהותי את אופן הפעלתם של קמפיינים להשפעה על דעת הקהל. אם בעבר התבססו קמפיינים להשפעה על דעת הקהל הפוליטית על צוותים אנושיים או על רשתות בוטים פשוטות, היום שילוב של סוכני בינה מלאכותית מאפשר הפעלה אוטונומית ומתמשכת של מערכות השפעה. סוכנים כאלה יכולים ליצור מסרים ולהפיץ אותם, לנתח תגובות של משתמשים, לעשות ניסויים בזמן אמת ולשפר כל הזמן את האפקטיביות של הקמפיין.

Sahin Ahmed, *AI Agents vs. Agentic AI: What's the Difference and Why it Matters*, MEDIUM (17.6.2025) 66

67 שם.

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) 68

מחקרים עדכניים מצביעים על כמה יכולות עיקריות המאפיינות מערכות "נחיל" כאלה.⁶⁹ ראשית, הן מאפשרות תיאום דינמי בזמן אמת: אלפי פרסונות דיגיטליות יכולות לפעול בעת ובעונה אחת ולתאם ביניהן מסרים ונרטיבים על פי תגובות הציבור. שנית, הן מסוגלות למפות רשתות חברתיות ולחדור לקהילות באמצעות למידה של השפה, הסגנון והקודים התרבותיים שלהן. שלישית, הן מסוגלות לחקות התנהגות אנושית חיקוי משכנע – בעזרת שימוש בשפה טבעית, בדמויות דיגיטליות (אווטארים) ובדפוסי פעילות מגוונים – וכך הן מצליחות להערים על מערכות לזיהוי בוטים. רביעית, הן מבצעות אופטימיזציה מתמשכת של המסרים באמצעות ניתוח נתוני מעורבות של משתמשים וניסויי A/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 למילוי אופטימלי של המשימה שניתנה להן.⁷⁰ נחילי סוכנים שתכליתם ליצור שינוי בדעת הקהל או בדעתם של בוחרים ספציפיים עלולים ליצור ריבוי קולות מזויפים לשם יצירת אשליה של קונצנזוס ציבורי; הם עלולים ליצור סוגי מציאות שונים לאנשים שונים כדי להעמיק את הקיטוב החברתי, להציף את המרחב הציבורי בתוכן מזויף או עוין, או "להרעיל" את תשתית המידע של רשת האינטרנט כדי להשפיע על נגישות למידע של צ'טבוטים או של מאגרי המידע שמודלים של בינה מלאכותית מתאמנים עליהם, וכיוצא באלה. לא כחות מכך הם עלולים ליצור קמפיינים של הטרדה ממוקדת נגד עיתונאים, פוליטיקאים או פעילים אזרחיים, וכן מתקפות סייבר מסוג hack and leak, הכוללות הפצת מידע אישי.⁷¹

כך או כך, התפתחות זו מסמנת מעבר נוסף בתעמולה החישובית – מעבר מקמפיינים פוליטיים המתוכננים ומנוהלים בעיקר על ידי בני אדם, גם אם

69 שם.

70 Bengio, לעיל ה"ש 46.

71 Schroeder, לעיל ה"ש 68.

בנקודת הקצה של הפעלת הקמפיין נמצאת, למשל, רשת בוטים, לקמפיינים שבהם חלקים גדולים מתהליך ההשפעה נעשים מקצה לקצה ובאופן אוטונומי בידי מערכות בינה מלאכותית. במודל הזה, סוכנים דיגיטליים יכולים לבצע חלקים גדולים משרשרת ההשפעה – מיצירת מסרים, דרך התאמתם לקהלים שונים, ועד ניתוח תגובות הציבור ושיפור מתמיד של האסטרטגיה. כך משתנים במהותם ההיקף, המהירות ויכולת ההתאמה של קמפיינים פוליטיים להשפעה על דעת הקהל, והתעמולה החשובית מתקרבת למצב של אוטומציה של "מעגל השכנוע".

1.3.5. סיכום: אוטומציה של השפעה פוליטית בקנה מידה רחב

ההתפתחויות שתוארו לעיל מצביעות על שינוי מצטבר במבנה התעמולה החשובית ועל תהליך של סגירת "מעגל השכנוע". נתונים על משתמשים נאספים או מוסקים מתוך פעילותם הדיגיטלית; מערכות בינה מלאכותית מנתחות את הנתונים האלה ומייצרות פרופילים אישיים; על בסיס פרופילים אלו נוצר תוכן פוליטי מותאם אישית; והתגובות של המשתמשים למסרים האלה מוזנות חזרה למערכת לשם שיפור מתמשך של האסטרטגיה. כך נוצר תהליך דינמי של אופטימיזציה בזמן אמת, שבו המסרים עצמם, דרכי הפצתם והקבוצות שאליהן הם מכוונים משתנים כל הזמן על פי תגובות הציבור.

המאפיין הראשון של התפתחות זו הוא האוטומציה. אם המודל הקלסי של קמפיינים מבוססי נתונים נשען על איסוף מידע על בוחרים ועל התאמת מסרים לקבוצות יעד שונות, מתוך הפעלת שיקול דעת אנושי בכל אחד משלבי השרשרת, 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, לעשות ניסויים רבים בזמנית ולהפעיל מערכות השפעה אוטונומיות לאורך זמן, וכל זאת בלי צורך בהשקעת המשאבים שנדרשה בעבר לכוח אדם, למומחיות ולתשתיות טכנולוגיות. הפחתת העלויות הדרמטית מאפשרת להפעיל קמפיינים פוליטיים

בהיקפים גדולים בהרבה מבעבר, ולהפיץ מסרים מותאמים ליחידים.⁷² החידוש בהיבט הזה אינו בהבדל בין מסר מותאם למסר לא מותאם, שהוא אינו הבדל דרמטי ברמת הפרט ואינו מוביל לשינוי מידי 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 אוטומטית ומשולב במערכות הפצה קיימות, עלול להיות לו משמעות אלקטורלית. שינוי של אלפים ספורים מתוך מאה אלף בוחרים הנחשפים לקמפיין עשוי להיות מכריע בבחירות צמודות – תרחיש ראלי במדינות דמוקרטיות רבות. כלומר, הסיכון לדמוקרטיה אינו נובע מעצם המניפולציה, אלא מהאוטומציה, מהזמינות, מהמהירות, מהיקף המסרים ומהתחכום של התאמתם לאדם מסוים.⁷³

התוצאה היא שינוי עמוק בתעמולה החשובית, 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 הזה, התעמולה החשובית בעידן הבינה המלאכותית אינה רק שיפור של הכלים הקיימים, אלא שלב חדש בהתפתחותם של קמפיינים פוליטיים דיגיטליים.

1.4. יישומני בחירות

יישומני ניהול בחירות הם יישומנים המפותחים בהזמנת המפלגות, ומטרתם לייצר מעורבות של בוחרים ולסייע למפלגות ולמתמודדים לנהל את מערכת

72 Almog Simchon, Matthew Edward & Stephan Lewandowsky, *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3 PNAS Nexus 1–5 (2024); Sandra Matzet et al., *The Potential of Generative AI for Personalized Persuasion at Scale*, 14(4692) SCIENTIFIC REPORTS (2024)

73 שם, Matzet, et al.

הבחירות. ליישומי ניהול בחירות שימוש כפול: האחד – איסוף מידע על בוחרים; והאחר – הפעלת המתנדבים והמטה. יישומים אלו כוללים היקף עצום של מידע פרטי,⁷⁴ וייחודם בכך שיש בהם קשר מזהה בין אדם לבין עמדותיו הפוליטיות. מאגר המידע שעליו מבוסס היישומון בנוי בשכבות.

שכבת הבסיס היא מידע מפנקס הבוחרים (המכונה "מידע פנקס"), שנמסר ממשד 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 מגיל 18 ומעלה, 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 ולרשתות חברתיות אחרות, קשרי משפחה ושפת הדיבור. עוד נמצאים בשכבה זו פרטי מידע מעובד הנרכשים מסוחר מידע (data brokers), שעיסוקם העיקרי הוא עיבוד מידע אישי לשם מכירתו או העמדתו לשימוש צדדים שלישיים.

בשכבה השלישית נמצא מידע בדבר הזיהוי הפוליטי של הבוחרים: מידת התמיכה במפלגה ואם כוונתו של הבוחר נושא המידע להצביע ביום הבחירות. למעשה זו שכבת המידע החשובה ביותר לשימוש אפקטיבי ביישומון, משום שהיא תשמש כדי להכין את תוכנית הפעולה המותאמת אישית בנוגע לכל בוחר

74 תהילה שוורץ אלטשולר ורחל ארידור הרשקוביץ "חווה דעת בנושא יישומי הבחירות" אחר המכון הישראלי לדמוקרטיה (פברואר 2020). בקביעה שמדובר במאגר מידע תומכת גם קביעתה של הרשות להגנת הפרטיות, ראו ס' 4 להנחיות הרשות להגנת הפרטיות "אחריות המפלגות לקיום הוראות חוק הגנת הפרטיות בשימוש באפליקציות ובספקים חיצוניים לצורך ניהול מערכת בחירות" (11.2.2020).

75 ס' 39(א) לחוק הבחירות לכנסת [נוסח משולב], תשכ"ט-1969 (להלן: חוק הבחירות).

ובוחרת. האם המפלגה תפנה אליהם ביום הבחירות? באיזה שלב של היום? מי יפנה ובאילו טכניקות?

את פרטי המידע בשתי השכבות שמעבר לשכבת הבסיס מזינים משתמשים שהורידו את היישומון מחנות היישומים או מאתר אינטרנט לגיוס תומכים.⁷⁶ פעילי המפלגה שהתקינו את היישומון מזינים את פרטיהם, וכן ממלאים פרטים על אנשים אחרים. בין היתר מתבקש מי שהתקין את היישומון להזין לתוכו מידע על חבריו ועל קרוביו, ברמות שונות של פירוט. דליפת המידע מהיישומון "אלקטור" בעת ששימש את קמפיין הליכוד בבחירות מרץ 2020, חשפה בין השאר כי במידע נכללו גם תיאורים פרטניים של אנשים, וכן של הדרך שבה יש לשכנע אותם, כגון "אביו פעיל ליכוד מוכר", או "לחיץ כמו בקבוק קטשופ".⁷⁷

משימושים ביישומונים בעבר עולה שהמערכת מחלקת את האנשים שבמאגר המידע לארבע קבוצות, על פי מידת תמיכתם במועמד או ברשימה שהיישומון פועל לבחירתו: תומכים, תומכים פוטנציאליים, לא ידוע או לא תומך.⁷⁸ מיון האזרחים שפרטיהם נמצאים במאגר המידע לפי מידת תמיכתם משפיע על ההתמקדות במסרים ועל הטיפול מצד עובדי הקמפיין.⁷⁹ נתוני זמן האמת ביום הבחירות מוצגים גם כן בחלוקה לארבע קבוצות אלו.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

76 ראו, למשל, **אתר מפלגת הליכוד**.

77 עומר כביר "מכונת קישוש הקולות של הליכוד בפעולה: 'חשוב ללחוץ עליו ולפנות אליו מניפולטיבית'" **כלכליסט** (17.2.2020).

78 ראו בסרטון "**מערכת לניהול בחירות – אלקטור**".

79 שם.

80 שם.

למפלגה – מי מבעלי זכות ההצבעה לפי פנקס הבוחרים בחר לממש את זכותו הדמוקרטית ולהצביע בבחירות, ומי טרם עשה זאת.⁸¹

מאגר המידע שבשישומון מתעדכן כל העת. כך, באמצעות היישומון, אפשר לשפר את פרופיל האישיות של בעל זכות הבחירה ולמטב את המסרים המותאמים אישית אליו ואת פלטפורמת העברתם לשם השגת המטרה המבוקשת על ידי המפלגה. נוסף על כך, היישומון מאפשר לשלוח לבוחרים מסרים שנייעו אותם לפעולה – להתנדב בקמפיין הבחירות, וכך הוא מאפשר 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. בכך טמונה סכנה עצומה, לא רק למניפולציות על הבוחרים וליצירת מלכודות אוטונומיה ביום הבחירות עצמו.⁸³ בקיומם של מאגרי מידע רגישים כל כך טמון הסיכון שבמידע האגור בהם ייעשה שימוש עתידי, מורשה ושאינו מורשה,⁸⁴ כתנאי

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 הבחור ליום העוקב" העין השביעית (18.2.2020); שחר סמוחה "המצביע האוטומטי: 'הציבור לא מבין את עומק המניפולציה שעושים עליו' שומרים (29.9.2022).

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

מוקדם לקבלה לעבודה, לקבלת שירות מהמדינה, לאינטראקציה חברתית ועוד.⁸⁵

אחד מהיישומים שנעשה בהם שימוש בקמפיינים פוליטיים בכמה מדינות, כמו צרפת ובריטניה, ואף בפרלמנט 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 הכלים האלה נשענים על מסד נתונים מרכזי, ייחודי לכל לקוח של המערכת, המאחד מידע מכמה מקורות, 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 המידע הזה הפלטפורמה יוצרת פרופילים של בוחרים. כן מפעילה הפלטפורמה מערכת ניתוח 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 של פעילות. כך מאפשרת פלטפורמת NationBuilder למפלגות להפעיל קמפיינים מדויקים ומבוססי נתונים.⁸⁷

חבילת הכלים שפלטפורמת NationaBuilder מספקת משתנה לפי בחירתו של הלקוח והמחיר שהוא מוכן לשלם.⁸⁸ כך, הלקוח יכול לבחור אם ברצונו להצליב בין חשבונות ברשתות חברתיות לבין כתובות הדוא"ל של אנשים שזוהו כתומכים בו במסד הנתונים, להוסיף נתונים ממקורות נוספים, וכן לעשות שימוש במודלים

85 להרחבה ראו, למשל, שורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 54; בן דוד, לעיל ה"ש 83.

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 NationBuilder, *Understanding social capital*

88 NationBuilder, *Win your campaign with the leading all-in-one platform*

ניבויים ובניתוחים מותאמים אישית. כן יכול הלקוח לבחור לשלב גם חיבור לתהליכי פרסום שמספקים Amazon Advertising ו-Google Ads; לקבל הצעות לשיתוף פעולה עם שותפים, כגון חברות ייעוץ; או לקבל גישה ללוחות מחוונים וגישה לשירותי ניתוח של צדדים שלישיים.⁸⁹ הפלטפורמה עושה שימוש בכלי בינה מלאכותית לשם התאמת מסרי תעמולה מותאמים לבוחרים על פי תחומי העניין שלהם והיסטוריית הקשר שלהם עם המפלגה, וכן מספקת למפלגה מידע שניתן לפילוח ומיון בזמן אמת, כדי לקבל החלטות בנוגע לאסטרטגיית התעמולה הנכונה על בסיס מידע מלא.⁹⁰

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 סוג אחד הוא יישומונים ייעודיים לפעילי שטח, המאפשרים גישה למידע על בוחרים, הזנת נתונים בזמן אמת לאחר שיחות פנים אל פנים עם בוחרים, וסנכרון עם מאגרי מידע מרכזיים של המפלגה. ביישומונים האלה נעשו גם שימושים בשירותי ניתוח ובתשתיות של חברות חיצוניות, ובהן Microsoft Visual Studio App, ובהן ברכיבי תוכנה של Google (Firebase Crashlytics). סוג שני הוא יישומונים לניהול מדיה חברתיות, ובכללם ניתוח הלך רוח (סנטימנט) וזיהוי ישויות ואפיון מבוסס נתונים (פרופילינג). ביישומונים האלה נעשו שימושים גם בשירותי מעקב אחר מיקום ובזיהוי משתמשים בעזרת נתוני WIFI. באחד מהיישומונים 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 האלה אינה מספקת פירוט בדבר היקף השיתוף והכיוון שלו – כלומר אם נתונים הנאספים לשם פנייה ישירה לבוחרים (Canvassing), הכוללים מידע על דעה פוליטית, נגשים ל-Experian לצרכים שמעבר לפעילות המפלגתית עצמה.

89 NationBuilder, *Find an app or integration*

90 NationBuilder, *World-class Software for Political Parties, Optimized for Europe*

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

פרק 2

פרטיות ובחירות

בישראל: המצב המשפטי והמצב למעשה

דיני תעמולת הבחירות בישראל אינם עוסקים בשאלה אם יש סוגים של מידע אישי שאסור להשתמש בהם במסעות תעמולה, או אם יש טכניקות שרמת ההשפעה והמניפולציה שהן יכולות ליצור גדולה כל כך עד שיש לאסור אותן. בהקשר הזה, של פרטיות ובחירות, קיים אפוא חלל חוקי ואכיפתו.

הזכות החוקתית לפרטיות, המעוגנת בסעיף 7 לחוק-יסוד: כבוד האדם וחירותו, היא לפי הניסוח בחוק היסוד והפרשנות שניתנה לו בפסיקה, זכות בעלת ממד אינדיבידואלי, והיא עוסקת בעיקר במניעת כניסה למרחב הפרטי ובשליטתו של הפרט במידע האישי שלו. לכן במצב המשפטי במדינת ישראל, כמו שהוא בא לידי ביטוי בפסיקה בעניין יישומי הבחירות,⁹² אין התייחסות חוקתית לאיום שמציב השימוש בטכניקות איסוף של מידע אישי ועיבודו כדי לבצע מניפולציה על בוחרים על האינטרס הציבורי הקולקטיבי בקיום הליך דמוקרטי תקין, הוגן וטהור.

איסוף מידע אישי על בוחרים פוטנציאליים לשם העברת מסרי תעמולת בחירות בפלטפורמות דיגיטליות החל לצבור תאוצה בבחירות לכנסת ה-21 באפריל 2019. בבחירות אלו עשתה מפלגת הליכוד שימוש בתוכנת המסרים המיידים של פייסבוק באמצעות בוט שהופעל בדף הפייסבוק של ראש הממשלה בנימין נתניהו, וניהל שיחות אישיות לכאורה עם מצביעים פוטנציאליים, ובמהלכן אסף ועיבד מידע אישי עליהם מהמידע הזמין בפייסבוק ומהמידע שנמסר על ידם בשיחה. הבוט מיפה את המצביעים שהוא שוחח עימם על פי מידת תמיכתם במפלגת הליכוד, המריץ תומכים לסייע בהפצת תעמולה וגיוס תומכים, והמשיך בניסיונות שכנוע של מי שהוגדרו מתלבטים. פייסבוק מצאה שהשימוש בבוט מפר את כללי השימוש בפלטפורמה, ובהם האיסור על שידול, ודרשה לחדול מהשימוש בו.⁹³ לטענת מי שעמד בראש קמפיין הדיגיטל של הליכוד באותה

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: 'אוסף מידע'" N12 (18.8.2019).

העת, הצ'טבוט תרם תרומה של ממש 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 שיש גם חלל חוקתי בשאלה אם עצם היציאה להצביע הוא מידע אישי החוסה תחת הזכות לפרטיות. אף שאין מחלוקת שעמדתו הפוליטית של אדם ותוכן ההצבעה מאחורי הפרגוד שבקלפי הם מידע אישי רגיש, בכל הנוגע לשאלה אם המידע על עצם היציאה להצביע הוא מידע פרטי – אין קביעה ברורה. בעתירה בעניין **עדאלה**,⁹⁵ נטען כי סימון דיגיטלי של המצביעים, והבנה בזמן אמת מי לא יצא להצביע, עלולים להביא לחשש מפני פגיעה במעמדו המקצועי, החברתי או האישי של אדם, עקב חשיפה ציבורית שהוא נמנע מלממש את חובתו האזרחית להצביע. נוסף על כך, מהימנותו של פלוני מלהצביע בבחירות אפשר להסיק גם על עמדותיו הפוליטיות. למשל, אי-הצבעה יכולה ללמד על חוסר אמון במוסדות השלטון. ניתן גם להפעיל עליו לחץ מבוסס מיקום, למשל, אם ידוע שאדם הוא סטודנט ונמצא על יד מוסד הלימודים והרחק ממקום הקלפי, אפשר לעודד אותו לצאת להצביע בקלפי נגישה ולזייף את העובדה שאינו בעל מוגבלות (שכן הכללים הקיימים אינם דורשים להציג תעודה כלשהי על מוגבלות בקלפי). בכיוון ההפוך ייתכן מצב שבו הודעות שקריות מגיעות במכוון אל בוחרים ספציפיים, כמו למשל הודעה המיועדת 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 הבחורים

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

95 ה"ש 7/22 **עדאלה המרכז המשפטי לזכויות המיעוט הערבי בישראל ואחרים נ' הליכוד ואחרים** (26.8.2019).

שהצביעו איננה, לכאורה, חסויה בפני סיעות הכנסת ששלחו נציגים לוועדת הקלפי.⁹⁶

בבחירות לכנסת ה-22, שהתקיימו בספטמבר 2019, המשיך הליכוד לעשות שימוש בבוט שהופעל מדף הפייסבוק של ראש הממשלה בנימין נתניהו ודימה שיחה במסגרת. משתמשים שזוהו כתומכי ליכוד התבקשו באמצעות הבוט לטלפן לאנשים אחרים, 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.⁹⁷ עוד נחשף בתקשורת כי מאגר מידע עצום שמטרתו לקטלג את בעלי זכות הבחירה בישראל לפי האוריינטציה הפוליטית שלהם דלף לרשת האינטרנט.⁹⁸

במערכת הבחירות לכנסת ה-23 (מרץ 2020) 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 הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: תקנות אבטחת מידע). בעתירה נטען שהמידע המועלה ליישומון גלוי לכל אדם, ללא כל פיקוח ובקרה, ושהופצו סיסמאות כניסה ליישומון ברשתות החברתיות ובקבוצות ווטסאפ. עוד נטען בעתירה כי הופצו סרטונים מטעם

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

97 איתמר ב"ז "סממנים של מדינת מעקב" העין השביעית (9.9.2019).

98 עמית, לעיל ה"ש 84.

תנועת הליכוד, ובהם נקראו תומכי המפלגה להוריד את יישומון אלקטור. בסרטון פורסם מספר טלפון, וכל המעוניין היה יכול לשלוח מסרון למספר הטלפון ולקבל בתגובה קישורית וסיסמה להתקנת היישומון ולהפעלתו. מרגע זה קיבל המתקין גישה לכל מידע הפנקס ולמידע המטויב שצורף לו, ולמעשה היה יכול לחפש מידע על כל אחד מבעלי זכות הבחירה בישראל, בלא 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 לדיון, שטיוב המידע על 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 הוא הפרה של חשאיות הבחירות ואסור על פי חוק.⁹⁹ כן נטען כי השימוש ביישומון ללא הגבלות הרשאה עלול להביא לפגיעה בביטחון המדינה ולאפשר לגורמי ביון זרים לחשוף סיפורי כיסוי של סוכני ביון ישראלים בחו"ל.¹⁰⁰ הבקשה שהוגשה הייתה למתן צו מניעה, מכוח סעיף 17ב בחוק הבחירות (דרכי תעמולה), התשי"ט-1959 (להלן: חוק דרכי תעמולה), להפסקת שימוש המפלגות ביישומון.

יו"ר ועדת הבחירות המרכזית לכנסת ה-23, השופט ניל הנדל, הצביע על היעדר התאמה בין חוק דרכי תעמולה, שנחקק בשנת 1959, לשימוש שנעשה בטכנולוגיה לצורכי תעמולת בחירות, וגם למעמדה של הזכות לפרטיות, שמאז חקיקת חוק-יסוד: כבוד האדם וחירותו בשנת 1992, היא זכות יסוד חוקתית. לשיטתו, היעדר התאמה זה מחייב בחינה נורמטיבית מעמיקה של ההסדרים הקבועים בחוק דרכי תעמולה, ולכן הצהיר כי בתום הבחירות יפעל להקמת ועדה לבחינת הנושא, והיא תעסוק ב"מכלול הסוגיות המתעוררות בנקודות המפגש

99 חב"כ 14/23 בן מאיר ואח' נ' הליכוד - תנועה לאומית ליברלית ואח' (18.2.2020), פסקה 1 להחלטה.

100 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).

שבין פרטיות וטכנולוגיה בדיני הבחירות".¹⁰¹ עם זאת, לנוכח הפרשנות שהעניק בית המשפט העליון לסעיף 17 בחוק דרכי תעמולה,¹⁰² סבר השופט הנדל שידיו כבולות ואין בידו להוציא את צו המניעה המבוקש. חוק הגנת הפרטיות אינו מבין החוקים המנויים במפורש בסעיף 17 בחוק 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 שר הפנים.¹⁰³ 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.¹⁰⁴ השופטים קבעו כי הדרך להתמודד עם הסוגיה של אבטחת המידע ביישומי הבחירות היא באמצעות הגשת תביעה אזרחית, והדרך לערער על החלטותיה של הרשות להגנת הפרטיות היא בבית משפט לעניינים מינהליים. עם זאת קבע השופט שטיין כי מדובר בסוגיה מטרידה, ולנוכח חשיבותן הציבורית של הטענות שהעלו העותרים הוא בחר שלא להשית עליהם הוצאות משפט.¹⁰⁵ 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.¹⁰⁶

לאחר הדיון בעתירה האמורה ולפני מתן ההחלטה בה, בפברואר 2020, אירע אירוע אבטחת המידע במערכות המידע של יישומן הבחירות של חברת אלקטור,

101 תב"כ 23/14 בן מאיר ואח' נ' הליכוד ואח' (18.2.2020).

102 דנג"ץ 1525/15 ח"כ ד"ר אחמד טיבי נ' מפלגת ישראל ביתנו ואח' (נבו 23.8.2017).

103 תב"כ 13/23 בן מאיר ואח' נ' הליכוד ואח', ועדת הבחירות המרכזית לכנסת ה-23 (18.2.2020).

104 בג"ץ 1311/20 בן מאיר ואח' נ' הליכוד - תנועה לאומית ליברלית ואח' (נבו 25.2.2020).

105 אורי ברקוביץ' "בג"ץ דחה על הסף את העתירה נגד אפליקציית המרצ הבוחרים אלקטור" גלובס 25.2.2020; איתמר ב"ז "בג"ץ דחה את העתירה נגד הליכוד ו'אלקטור' העין השביעית 25.2.2020.

106 בן דוד, לעיל ה"ש 83.

שבמסגרתו התאפשרה גישה למערכות המידע של החברה, ולרשת האינטרנט דלף קובץ ובו 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 נוספות של מידע אישי, ולעיתים רגיש, כגון מספר טלפון, כתובת דוא"ל, מצב רפואי, דעה פוליטית ומידת תמיכה במפלגה. המידע אף פורסם ברשת האפלה (dark web).¹⁰⁷ כשבוע אחרי חשיפת פרצת המידע הראשונה נודע על שני כשלי אבטחה נוספים במערכת היישומון אלקטור שהובילו לחשיפת כל מאגרי המידע שהעלו המפלגות שעשו באותה העת שימוש ביישומון – הליכוד וישראל ביתנו, לרבות מידע הפנקס, וכן נחשף קוד המקור של היישומון עצמו.¹⁰⁸

אירוע זה שווה ערך, למעשה, לדליפת מרשם האוכלוסין, והוא אירוע סייבר חמור ביותר. הרשות להגנת הפרטיות פתחה בחקירת האירוע ימים ספורים לאחר חשיפתו. בחקירת האירוע נמצא שמערכת אלקטור אפשרה לייצא את המידע שבמערכת על ידי הפקת דוחות לפי בקשת כל משתמש. לכל משתמש ביישומון ניתנה הרשאה ל-50 שאילתות חיפוש, כלומר כל פעיל מפלגה שהתקין את היישומון הורשה להצליב 50 הצלבות בין אנשי הקשר שלו לבין הבוחרים המופיעים בפנקס הבוחרים, ולהזין עליהם מידע נוסף שהיה בידו.¹⁰⁹ עם הורדת היישומון הוצגה למשתמש הודעה ולפיה ביכולתו להזין אך ורק פרטי מידע

¹⁰⁷ עומר כביר "פרצת האבטחה באפליקציה של הליכוד: הפרטים האישיים של כל הבוחרים נחשפו" **כלכליסט** (9.2.2020); קביעת הפרה ישראל ביתנו, לעיל ה"ש 84; קביעת הפרה הליכוד, שם; קביעת הפרה אלקטור, שם.

¹⁰⁸ 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. התביעות הוגשו עוד לפני שהרשות להגנת הפרטיות סיימה את חקירתה בנושא, אולם שתייהן 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).

¹⁰⁹ מחלקת האכיפה, הרשות להגנת הפרטיות, קביעת הפרה של חוק הגנת הפרטיות, התשמ"א-1981 (27.1.2021) (סימוכין 008-2021-00000695; 008-2021-00000712). (008-2021-00000695; 008-2021-00000712).

על אנשים שנתנו את הסכמתם לכך. בשטח, הפעילים לא יישומו את דרישת ההסכמה כנדרש.¹¹⁰

ביונאר 2021 פרסמה הרשות את ממצאי חקירתה, ונקבע שהליכוד, ישראל ביתנו וחברת אלקטור הפרו את הוראות חוק הגנת הפרטיות ואת תקנות אבטחת מידע. ואולם, הרשות להגנת הפרטיות הצהירה שבכוונתה להטיל קנס מינהלי רק על חברת אלקטור.¹¹¹ החלטת הרשות ניתנה כ-11 חודשים אחרי אירוע דלף המידע, ובהיעדר סמכות להטיל קנסות בגין מרבית ההפרות שנמצאו הוטל בסופו של דבר קנס אך ורק על חברת אלקטור.¹¹²

בבחירות לכנסת ה-24 בשנת 2021 עשה הליכוד שימוש ביישומון שכונה בתחילה "ליכוד נט", ומאוחר יותר הוחלף שמו ל"ניצחון 22", שפותח בחברת אלקטור ושימש למטרה דומה.¹¹³ מקורב לחברת אלקטור טען באותה העת כי במערכת שנעשה בה שימוש בעבר נעשו שינויים ניכרים ושמהמערכת המעודכנת לא דלף מידע. לפי המידע שמסר, המשתמשים ביישומון החדש אינם נחשפים למספר ת"ז של כלל הבוחרים שפרטיהם מופיעים במאגר המידע שביישומון על בסיס מידע הפנקס. נוסף על כך, גם כתובת המגורים הנגישה לכלל הציבור כוללת רק את שם הרחוב ולא את מספר הבית. כן, המשתמש ביישומון אינו יכול לאתר מידע אישי על אנשים אחרים באמצעות היישומון. באפשרותו להתקשר למספר טלפון של בוחר אחר דרך היישומון רק אם הוא הוסיף את מספר הטלפון הזה. עוד נמסר כי כל מפלגה יכולה להוסיף ליישומון שכבות מידע וקטיגוריות כרצונה.¹¹⁴

110 ענת ציגלמן "האפליקציה שמכריעה את הבחירות וכל האמצעים כשרים. כמעט" שומרים (18.3.2021).

111 קביעת הפרה ישראל ביתנו, לעיל ה"ש 84; קביעת הפרה הליכוד, שם; קביעת הפרה אלקטור, שם.

112 מחלקת האכיפה, הרשות להגנת הפרטיות, קביעת הפרה של חוק הגנת הפרטיות, לעיל ה"ש 109.

113 שוקי טאוסיג "קמפיין בהסוואה?" העין השביעית (18.9.2022).

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

כבר בפתח שנת הבחירות לכנסת ה-26, בינואר 2026, הגיע לפתחה של ועדת הבחירות המרכזית נושא הקשור בשימוש ביישומוני בחירות, והוגשה עתירה הטוענת כי הפרקטיקה של תיעוד מצביעים שעושים חברי ועדת הקלפי והמשקיפים בקלפיות והכנסת המידע לתוך יישומוני הבחירות המפלגתיים, היא פגיעה בחשאיות הבחירות ובזכות הבחור לפרטיות. לפי סעיף 79 לחוק הבחירות, משקיף ראשי להוסיף בפרוטוקול ועדת הקלפי את הערותיו העובדתיות הנוגעות לפעולות הוועדה ולבדוק את תא ההצבעה מעת לעת כדי לוודא שיש מספר פתקים מספיק לרשימה שהוא מייצג או לכל רשימה אחרת.¹¹⁵ 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 לשם זיהוי הבוחרים בקלפי. ואולם החוק אינו מסמך את חברי ועדת הקלפי או את המשקיפים להשתמש בפרטים האישיים האלה ולהעבירם בחזרה אל מרכזי המפלגות.

סעיף 45 לתקנות הבחירות קובע כי ביום הבחירות, כאשר מצביע נמצא בקלפי ובעת ספירת הקולות, אין לשוחח במכשיר טלפון נייד או במכשיר קשר בחדר שבו פועלת ועדת קלפי, אלא לשם ניהול ההצבעה בקלפי או במקרי חירום. אפשר לפרש כלל זה כאוסר על כל שימוש במכשיר טלפון נייד שאינו לשם ניהול ההצבעה. נוסף על כך, אם נציגי המפלגות ממלאים במקום הקלפי תפקיד ציבורי על פי דין – חברי ועדת הקלפי או משקיפים, מכוח עקרון החוקיות אסור להם לעשות פעולות שהם לא הוסמכו במפורש בדין לעשותן.

נעיר כי כבר במכתב שהגשנו בשנת 2020 ליו"ר ועדת הבחירות לכנסת ה-23 בעניין דומה, סברנו כי אין לאפשר לחברי ועדות קלפי ולמשקיפים להשתמש באפליקציות כדי להעביר פרטי בוחרים בזמן אמת ל"מוח מרכזי" ולאגמם עם מאגרים מרכזיים, הן בשל היעדר סמכות, הן בשל הפגיעה בפרטיות הבוחרים ובחשאיות הבחירות. סברנו גם כי ליו"ר ועדת הבחירות הסמכות ליתן החלטות והוראות בעניינים האלה, הן לנוכח פרשנות נצרכת למילוי החלל שבין האסדרה

115 ועדת הבחירות המרכזית לכנסת ה-21 מטה ההדרכה חדריק ונוהלי עבודה למזכיר ולבעלי תפקידים בוועדות הקלפי 2 (2019).

לטכנולוגיה ולמניעת ניצולו לרעה, הן בשל פרשנות סעיף 17 לחוק התעמולה וסעיף 118 לחוק הבחירות.¹¹⁶

בחוות דעת שהוגשה לוועדת הבחירות המרכזית לכנסת ה-26 בהליך הנוכחי הסבירו מומחי פרטיות כי המידע על הצבעתו של פלוני בקלפי מגיע לחברי ועדת הקלפי ומשקיפים כחלק מתפקידם לפקח ולשמור על טוהר הבחירות. תיעוד עצם ההגעה להצביע מוגדר "חומר רגיש" בתוספת הראשונה לכללי הבחירות לכנסת (עיון בחומר בחירות) תשע"ח-2018, הוא אמור להיות מתועד רק בעותקים קשיחים ולא דיגיטליים, ולפי סעיף 79 לחוק הבחירות, חובה להשמידו לאחר תום המועד להגשת ערעורי בחירות. לפיכך, תיעוד עצם ההצבעה ביישומי בחירות מפלגתיים חורג מסמכותם לפי דין של המשקיפים וחברי ועדת הקלפי, הוא פוגע בפרטיות הבוחרים ובעקרון חשאיות הבחירות, ויוצר אפקט מצנן על ההצבעה או אי-הצבעה, הפוגם באמון הציבור בטוהר הבחירות.¹¹⁷ נכון לכתיבת שורות אלו העתירה עודה תלויה ועומדת.

לסיכום, מנגנוני ההגנה על השימוש האסור במידע פרטי על אזרחי ישראל לשם השפעה על הבחירות – אינם מספקים. מצד אחד, השימוש במידע מפנקס הבוחרים באמצעות יישומי בחירות אינו מוסדר בחוקי הבחירות, ובעתירות שהוגשו בנושא בבג"ץ ולוועדת הבחירות המרכזית לא התקיים דיון מהותי. העתירה נדחתה בבג"ץ בנימוק שהוא אינו הערכאה המתאימה,¹¹⁸ ובוועדת הבחירות המרכזית שאין ליו"ר הוועדה סמכות להכריע בנושא אלא נדרש

116 תהילה שוורץ אלטשולר ורחל ארידור הרשקוביץ מכתב ליו"ר ועדת הבחירות המרכזית לכנסת ה-23 בעניין שימוש באפליקציות לניהול מאגר בוחרים כדוגמת "אלקטור" כפי שעולה מחב"כ 14/23 בן מאיר ואח' נ' הליכוד תנועה לאומית וליברלית ואח', אתר המכון הישראלי לדמוקרטיה (13.2.2020).

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

118 בג"ץ 1311/20 בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח' (נבו) 25.2.2020.

שינוי חקיקתי.¹¹⁹ אולם שינוי כזה טרם נעשה, אך שהשימושים במידע אישי על בוחרים אינם פוגעים רק בפרטיות, אלא בעיקר עשויים לפגוע בעקרון חשאיות הבחירות,¹²⁰ ולסכן את טוהר ההליך הדמוקרטי ואת מימושה המלא של הזכות לבחירות שוות והוגנות,¹²¹ נושא שאין מחלוקת שהוא נמצא בתחום סמכותו הטבעית של יו"ר ועדת הבחירות המרכזית.¹²²

בנסיבות אלו יש חשיבות רבה לתחולתם של חוק הגנת הפרטיות ושל תקנות אבטחת מידע על שימוש במידע אישי לצורך תעמולת בחירות ולכלים שהם מעניקים לרשות להגנת הפרטיות לשם אסדרת השימוש הזה. 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.¹²³

אכן, לקראת הבחירות לכנסת ה-23 ולכנסת ה-24 פרסמה הרשות להגנת הפרטיות כמה מסמכים חשובים הנוגעים לתחולת הוראות חוק הגנת הפרטיות

119 תב"כ 14/23 בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח' (נבו 18.2.2020).

120 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).

121 כך, למשל, נטען שבמערכת הבחירות לנשיאות ארצות הברית בשנת 2016 שלח המועמד טראמפ מסרים אישיים בטכניקת מיקוד מדויק (מיקרו-טרגרטינג), לכ-3.5 מיליון בוחרים אפרו-אמריקאים, שעיבוד המידע האישי עליהם מצא שהם נוטים שלא להצביע. המסרים כללו מודעות בדבר יחסה הקלוקל של המועמדת היריבה, הילרי קלינטון, לאפרו-אמריקאים. מטרת שליחת המסרים הייתה לעודד את הבוחרים האלה 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).

122 בג"ץ 1311/20 בן מאיר ואח' נ' הליכוד – תנועה לאומית ליברלית ואח' (נבו 25.2.2020).

123 ראו קביעת הפרה ישראל ביתנו, לעיל ה"ש 84, ס' 9.1, 10.2; קביעת הפרה הליכוד, שם, ס' 9.5, בעמ' 4.

על השימוש שעושות המפלגות או גורמים מטעמן במידע אישי, לרבות מידע מפנקס הבוחרים וביישומונים לניהול מערכת בחירות.¹²⁴

הרשות הדגישה שעל המידע שנמסר למפלגות במסגרת מידע הפנקס, וגם על המידע שמפלגות אוספות בקמפיין בחירות, חלות הוראות חוק הגנת הפרטיות, לצד חוק הבחירות. המפלגות הן הנושאות באחריות בהיותן "בעלות מאגר". ספקי השירות החיצוניים שהמפלגה מתקשרת עימם לשם עיבוד המידע באמצעות יישומון, או בדרך אחרת, או לשם אחסון בלבד, נושאים באחריות לפי חוק הגנת הפרטיות בהיותם "מחזיקים".¹²⁵ בין ההוראות המחייבות בחוק הגנת הפרטיות מנתה הרשות את הוראות תקנות אבטחת מידע ביחס למאגר מידע ברמת אבטחה גבוהה או בינונית,¹²⁶ וכן את עקרון צמידות המטרה ואיסור שימוש במידע שלא למטרה לשמה הוקם המאגר. על בסיס שילוב ההוראות האלה 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.¹²⁷

יתרה מזו, לעמדת הרשות אין לעשות שימוש בפנקס הבוחרים ממערכות בחירות קודמות או ממערכות בחירות לרשויות מקומיות, ויש לבער את כל

- 124 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 הפרטיות לקראת הבחירות לכנסת ה־24: מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר ואחריות המפלגות על אפליקציות וספקים חיצוניים (7.1.2021). (להלן: דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24).
- 125 דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בס' 7-10, 24-25.
- 126 דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בס' 17.4.
- 127 הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 124, ס' 8-10; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה־24, שם, בס' 11-12, 17.1.

עותקי המידע שמקורם במידע הפנקס, בין שהם בידי המפלגה בין בידי ספקיות שעימן היא התקשרה, וכן כל נגזרת של מאגרי המידע האלה, בתום הבחירות.¹²⁸

כן 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 פרטים ביישומונים או במאגרי המידע של המפלגה, במיוחד היעדר אינדיקציות בדבר תמיכתם או אי־תמיכתם במפלגה כזאת 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 על אודותיו אינו חוקי. ולפיכך, בעת התקשרות עם צד שלישי לשם רכישת מידע אישי על בוחרים יש לוודא את חוקיות מקורות המידע.¹²⁹

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, משום שמדובר בפניה לאדם המתבססת על אפיון אישי, ולפורמט בו נעשית הפניה, לרבות מדיה, הודעות SMS, רשתות חברתיות או באפליקציות מסרים מיידיים, לתוכן הפניה או למהותה אין חשיבות. יתרה מזו, בניגוד לחוק דואר זבל,¹³⁰ הוראות חוק הגנת הפרטיות בנושא דיוור ישיר חלות גם על תעמולה פוליטית. במסגרת זו עומדת לבוחר הזכות שפרטיו יימחקו ממאגר מידע ששימש לדיוור הישיר.¹³¹

128 דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24, שם, בס' 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.

129 הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 124, ס' 17-18; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24, לעיל ה"ש 124, בס' 17.2.

130 ס' 30 לחוק התקשורת, התשס"ח-2008 (להלן: חוק דואר זבל).

131 הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 124, ס' 13-16; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24, לעיל ה"ש 124, בס' 17.6.

למרות הבהרותיה של הרשות להגנת הפרטיות, בדוח מבקר המדינה מ־12 ביולי 2022 נמצא ששש מהסיעות והמפלגות ביצעו טיוב של הנתונים מהמידע פנקס בעזרת חברות מסחריות, בלי לבדוק את מידת חוקיות המידע שרכשו מהחברות לצורכי הטיוב ובלי לוודא שנושאי המידע נתנו את הסכמתם לאיסוף, להעברה ולעיבוד המידע האישי על אודותיהם.¹³² נוסף על כך, התפרסם בתקשורת כי חלק מן המפלגות עשו שימוש במידע שברשותן בדבר השאלה מי יצאו להצביע בבחירות האחרונות ומי לא, אף שמדובר במידע שלפי הדין ולפי התחייבויותיהן שנחתמו על ידן כתנאי לקבלת המידע, היה עליהן למחוק אותו בתום מערכת הבחירות הקודמת.¹³³

עד חקיקת 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 במהותו עם חקיקת תיקון 13 לחוק הגנת הפרטיות, שבו נעסוק בהמשך, אולם החוסר המהותי בהסדרים בחוק הגנת הפרטיות, וגם ההסדר להקפאת סמכויות הפיקוח והאכיפה של הרשות בתקופת בחירות,¹³⁴ עדיין יוצרים קושי באכיפה הנדרשת בזמן אמת לשם מזעור הפגיעה בפרטיות.

132 מבקר המדינה, פרסום דוחות מימון המפלגות – יולי 2022.

133 שוקי טאוסיג "תיעוד מכנס מתנדבי הליכוד: נביא לכם טלפונים של כל מי שלא הצביע למפלגה" העין השביעית (22.7.2022).

134 ראו פרק ד'5 לחוק הגנת הפרטיות, לעיל ה"ש 9.

חלק שני

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

מבוא

תיקון 13 הוא אבן דרך בהתפתחות הגנת הפרטיות במדינת ישראל, והוא כולל תיקונים חשובים ונחוצים לחוק הגנת הפרטיות. בתיקון נוסף גם הסדר מיוחד לאכיפת הוראות חוק הגנת הפרטיות בתקופת בחירות. לכלל השינויים האלה השפעה

ישירה על השימוש במידע אישי על אודות בעלי זכות הבחירה בישראל בתקופת בחירות; סמכויות הרשות להגנת הפרטיות; וגם על הפעולות שאפשר לנקוט – הן באמצעות רשויות השלטון, הן באמצעות אכיפה פרטית – כדי לשפר את ההגנה על הזכות לפרטיות מפני פגיעה בה מצד 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 שעושים מפלגות ומפעילי יישומי בחירות במידע אישי על אודות הבוחרים. בהמשך נעמוד על הגדרות בעלי התפקידים הרלוונטיים לעיבוד מידע אישי לפי תיקון 13, על החובות העיקריות המוטלות עליהם והאחריות שהם נושאים בה, ונבחן את יישומן של הוראות אלו על מפלגות ועל מפעילי יישומי בחירות. כן נעמוד על ההגבלות והאיסורים שהוספו לחוק הגנת הפרטיות בתיקון 13 על עיבוד מידע אישי במאגר מידע והחלתן על השימוש שעושות מפלגות ומפעילי יישומים 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 המנגנון הזה על הרשות להגנת הפרטיות, על ציבור הבוחרים, ועל ועדת הבחירות המרכזית.

פרק 3

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 התנאים לתחולת חוק הגנת הפרטיות. רק אם הנתון עונה להגדרת מידע אישי והוא נאסף באוסף העונה להגדרת מאגר מידע, יחולו הוראות חוק הגנת הפרטיות.

אם המידע האישי שבמאגר המידע נכנס לגדר אחת מהקטגוריות שהוגדרו בחוק "מידע בעל רגישות מיוחדת", מדובר במידע אישי מיוחד ששימוש לא מורשה או לא חוקי בו טומן בחובו סכנה גדולה יותר לזכות לפרטיות, ועל כן מוטלות דרישות מחמירות יותר על השימוש בו, שמירתו והעברתו.

3.1. הגדרת "מידע אישי"

תיקון 13 הרחיב את ההגדרה של המונח "מידע", שהוא 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;¹³⁵

להגדרה זו משמעות כפולה. ראשית, ההגדרה היא רחבה, וכוללת גם נתון הנוגע ל"מצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי" של אדם. כלומר, מרבית המידע שבידי מפלגה, הן מידע שמקורו במידע הפנקס (שם, מספר זהות וכתובת מגורים), הן מידע מטויב שהוסיפו פעילי מפלגה ומשתמשי יישומוני הבחירות למיניהם (למשל, מידע המתאר את נכותו של אדם, או את הסטטוס החברתי או התרבותי שלו), נחשב מידע אישי.

נוסף על כך, מדובר במידע של אדם מזהה או של מי ש"ניתן לזהותו במאמץ סביר". כלומר, גם אם מדובר במידע מותמם, יש להביא בחשבון את האפשרות שעיבוד המידע המותמם והצלבתו עם נתונים אחרים עשוי להביא לזיהוי, במישורין או בעקיפין, של אדם מסוים. עם זאת, ככל שהדברים אמורים במידע הנוגע לבחירות,¹³⁶ המידע איננו מותמם אלא ההיפך – יש חשיבות להיותו מידע מזהה, ולכן הוא מועבר באמצעות פנקס הבוחרים ונבנות על גביו שכבות נוספות של מידע מזהה.

3.2. מידע בעל רגישות מיוחדת

ההגדרה שמידע אישי הוא "מידע בעל רגישות מיוחדת", אינה משפיעה על תחולת חוק הגנת הפרטיות, אלא על החובות המוטלות על מי שמבקש לעבד מידע הנכלל בקטיגוריות האלה. למשל, מי שבבעלותו מאגר מידע שבו מידע בעל רגישות מיוחדת על 100,000 נושאי מידע ויותר, חייב להודיע על כך לרשות להגנת הפרטיות.¹³⁷ כן, חלות עליו דרישות אבטחת מידע מחמירות יותר,¹³⁸ ואם

136 ראו גם את התכלית למסירת מידע פנקס הבוחרים, המופיעה בס' 39(ג) לחוק הבחירות, לעיל ה"ש 75.

137 ס' 8א(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

138 תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: תקנות אבטחת מידע). במהלך הדיונים בחיקון 13 הובהר שייעשו התאמות בתקנות אבטחת מידע כדי להבטיח את התאמתן לחיקון 13 בכל הקשור להגדרת מידע בעל רגישות מיוחדת. ראו פרוטוקול 210 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (26.12.2023).

הוא או מי שמעבד בעבורו את המידע במאגר המידע מפר הוראה מהוראות חוק הגנת הפרטיות, הוא עשוי לשאת בסכום עיצום גבוה יותר מזה שהיה מוטל עליו אם במאגר המידע לא היה מידע בעל רגישות מיוחדת.¹³⁹

תיקון 13 יצר שינוי חשוב בהגדרת קטיגוריות המידע האישי הנחשבות "מידע בעל רגישות מיוחדת", משום שהוא הוסיף סוגי מידע בעל רגישות מיוחדת שלא נכללו בחוק קודם לכן ועשויות להיות רלוונטיות ביחס למידע האישי שבשליטת מפלגה או שמוסק על ידה. להלן נסקור את סוגי המידע האלה.

3.2.1. מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישותו ועל נטייתו המינית¹⁴⁰

מדובר בפרטי מידע המעידים בבירור, ולא בעקיפין או על דרך ההיסק, על צנעת אישותו של אדם, נטייתו המינית וצנעת חיי המשפחה שלו. התיבה "חיי המשפחה שלו" כוללת את כל סוגי המידע וההתנהגויות שאינם נכללים בהגדרות "צנעת אישותו" ו"נטייה מינית", אך קשורים לצנעת הפרט. למשל, התנהלות בין בני זוג, יחסים בין הורים לילדיהם, שיטות חינוך במשפחה, אלימות כלכלית, החלטות הנוגעות להרחבת המשפחה או לעתיד התא הזוגי.¹⁴¹

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 בדבר פנייה של בני זוג לטיפול זוגי או לגישור לפני גירושין, או על שיטות חינוך במשפחה ייחשבו מידע בעל רגישות מיוחדת בקטגוריה זו.

¹³⁹ פרוטוקול 203 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (18.12.2023), בעמ' 3.

¹⁴⁰ ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

¹⁴¹ ראו פרוטוקול 203, לעיל ה"ש 139, בעמ' 12-13; פרוטוקול 210, לעיל ה"ש 138, בעמ' 3-7.

3.2.2. מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי כהגדרתו בחוק זכויות החולה, התשנ"ו-1996¹⁴²

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 היא איננה מוגבלת רק למידע הנוצר או נאסף בנסיבות של יחסי מטפל-מטופל.¹⁴³ כלומר, כל מידע על מצב בריאותו של אדם, על מחלה ספציפית שלו, נכותו, או הימצאותו בטיפול פוריות ייחשב ללא ספק מידע על מצב בריאותו. מדדים בריאותיים של אדם, כפי שנאספים על ידי יישומני כושר למיניהם, או שעונים חכמים, ייחשבו גם הם מידע בעל רגישות מיוחדת.¹⁴⁴ מנגד, הערתו של פעיל מפלגה, שאינו איש מקצוע, שאדם הוא "לחיץ כמו קטשופ" לא תיחשב בהכרח מידע על מצב בריאותו, אך הדבר יהיה תלוי בנסיבות.

3.2.3. מידע אישי שהוא מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב¹⁴⁵

"מזהה ביומטרי" הוא "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".¹⁴⁶ אולם, לא כל מזהה ביומטרי הוא מידע בעל רגישות מיוחדת, שכן לנוכח טכנולוגיות מתקדמות הקיימות כבר, מאגרי תצלומים וסרטונים באיכות רגילה עשויים להכיל מזהים ביומטריים.¹⁴⁷

142 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

143 ראו הגדרת "מידע רפואי" בס' 2 לחוק זכויות החולה, תשנ"ו-1996 (להלן: חוק זכויות החולה) – "מידע המתייחס באופן ישיר למצב בריאותו הגופני או הנפשי של מטופל או לטיפול הרפואי בו".

144 פרוטוקול 203, לעיל ה"ש 139, בעמ' 17-19.

145 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

146 ס' 3 לחוק הגנת הפרטיות, שם.

147 פרוטוקול 203, לעיל ה"ש 139, בעמ' 23.

לפיכך, כמו ב-GDPR¹⁴⁸, בתיקון 13 נקבע כי רק מזהה ביומטרי שאכן משמש, או מיועד לשמש, לזיהוי אדם או לאימות זהותו, ייחשב מידע בעל רגישות מיוחדת.¹⁴⁹ על פי הגדרה זו סביר שתמונת סלפי, למשל, שמשתמש ביישומון בחירות צילם והעלה למאגר המידע, לא תיחשב מידע בעל רגישות מיוחדת. לעומת זאת, תצלום של תעודת זיהוי, רישיון נהיגה או דרכון ביומטרי שיעלה משתמש למאגר המידע ביישומון הבחירות עשוי להיחשב מידע בעל רגישות מיוחדת.

3.2.4. מידע אישי על מוצאו של אדם¹⁵⁰

מידע על מוצאו של אדם הוא מידע על מוצאו הגזעי או האתני של אדם.¹⁵¹ קטגוריה זו אינה כוללת מידע על השתייכות לאומית או 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 ייחשב מידע בעל רגישות מיוחדת. למשל, ציון העובדה שאדם הוא אשכנזי, ספרדי, תימני, אתיופי או רוסי, הנאמר בהקשר העדתי-תרבותי ייחשב מידע על מוצאו, ולכן מידע בעל רגישות מיוחדת. כמו כן, ציון העובדה שאדם מחזיק באזרחות גרמנית לא ייחשב מידע על מוצאו של אדם, ולעומת זאת, ציון היותו "יקה" נכלל בקטגוריה זו של מידע בעל רגישות מיוחדת.¹⁵²

3.2.5. מידע אישי על אודות עברו הפלילי של אדם¹⁵³

קטגוריה זו עוסקת בעברו הפלילי של אדם במובן הרחב, שכן היא אינה מוגבלת רק למידע מהמרשם הפלילי או למידע פלילי שיש צורך לפנות למשטרה לשם

148 ס' 9(1) ל-GDPR, לעיל ה"ש 5.

149 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

150 שם.

151 ס' 9(1) ל-GDPR, לעיל ה"ש 5.

152 פרוטוקול 210, לעיל ה"ש 138, בעמ' 39-42.

153 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

קבלתו. משום כך, בהחלט ייתכן שציון במאגר מידע שבשליטת מפלגה שפלוני יושב בכלא או שהוא עבריין מורשע ייחשב מידע הנכלל בקטגוריה זו.¹⁵⁴

3.2.6. מידע אישי על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם או השקפת עולמו¹⁵⁵

קטגוריה זו עוסקת בדעות פוליטיות ובאמונות דתיות ופילוסופיות,¹⁵⁶ ואינה מצומצמת רק להזדהות מפלגתית. הקביעה אם מידע הוא פוליטי תיעשה בהתאם לשאלה אם הוא מחזיק בעמדה ידועה בנושא השנוי במחלוקת פוליטית. השקפת עולמו של אדם בקטגוריה זו היא מידע המלמד עניין מהותי על אופיו של אדם, והיא אינה כוללת, למשל, העדפה שלו לצבע מסוים.

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

נציין בהקשר הזה 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 הליכוד, 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

154 אם מדובר במידע שגוי, ייתכן שיהיה מדובר גם במידע שהוא בבחינת לשון הרע לפי חוק איסור לשון הרע, תשכ"ה-1965.

155 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

156 ראו ס' 9(1) ל-GDPR, לעיל ה"ש 5.

תיאורו כ'תומך' או 'לא תומך'".¹⁵⁷ ואולם, בקביעת ההפרה דחתה, בצדק, הרשות להגנת הפרטיות את הטענות האלה והבהירה כי כדי להיחשב מידע רגיש "אין חובה שמידע, כגון דעותיו הפוליטיות של אדם, יהיה אמין באופן מוחלט, אלא די שניתן יהיה לייחס לו אמינות ברמה סבירה ואף פחות מכך".¹⁵⁸

3.2.7. 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 בלימודים¹⁵⁹

קטגוריה זו של מידע בעל רגישות מיוחדת נועדה לתת מענה למאפייני האישיות שאינם נכללים בקטגוריות האחרות. ואולם, אין הכוונה לכל מאפיין אישיות, אלא רק למאפיינים 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, ולפיה הכוונה היא לקווי אופי מהותיים, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים.¹⁶⁰

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 ייחשבו מידע בעל רגישות מיוחדת לפי קטגוריה זו. גם סיווגים של מאפייני אישיות מהותיים שעשתה מערכת בינה מלאכותית עשויים להיכלל בקטגוריה זו. לעומת זאת, חיווי דעה שמשתמש מזין על אדם אחר ביישומון לא תיחשב "הערכת אישיות".

157 קביעת הפרה הליכוד, לעיל ה"ש 84, ס' 9.8, בעמ' 5.

158 שם, ס' 10.7, בעמ' 11.

159 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

160 פרוטוקול 210, לעיל ה"ש 138, בעמ' 27-39; פרוטוקול 223, מישיבת ועדת החוקה, חוק ומשפט, הכנסת ה-25 (9.1.2024), בעמ' 3-7.

3.2.8. 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)¹⁶¹

בתיקון 13 הובהר שנתוני תעבורה ומיקום ייחשבו בעלי רגישות מיוחדת רק אם יש בהם כדי ללמד על מידע רגיש אחר,¹⁶² או שנוצרו על ידי ספק מורשה, כהגדרת מונחים אלו בחוק נתוני תקשורת.¹⁶³ לכן, ארגונים שאינם חברת תקשורת, למשל, חברה המוכרת תוכנה לבתי עסק ומנהלת תקשורת עם לקוחותיה, אינם נחשבים "ספק מורשה".¹⁶⁴

על פי הגדרה 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 לבילי שבת עשוי ללמד על אמונתו הדתית או על השקפת עולמו, ועל כן ייכלל בקטגוריה זו.

3.2.9. מידע אישי על נתוני שכר של אדם ועל פעילותו הפיננסית¹⁶⁵

קטגוריה זו מצומצמת רק למידע על נתוני שכר ופעילות פיננסית, שנאסף או מופק בידי גורמים, מוסדיים ושאינם מוסדיים, מהשוק הפיננסי. לדוגמה, מוסד

161 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

162 פרוטוקול 203, לעיל ה"ש 139, בעמ' 42, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

163 ס' 1 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007 (להלן: חוק נתוני תקשורת).

164 פרוטוקול 210, לעיל ה"ש 138, בעמ' 8-16.

165 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

אקדמי המעניק זכאות למלגה על בסיס מצבו הפיננסי של אדם, או עסקים המספקים שירות לניהול יעיל וכלכלי של משק הבית.¹⁶⁶

לפיכך, אם מאגר מידע של מפלגה או יישומון בחירות כולל מידע על אודות נתוני שכר של בעל זכות בחירה או על פעילותו הפיננסית, הוא ייכנס לקטגוריה הזאת. מנגד, אמירות כלליות שלפיהן פלוני "מרוויח כמו בהיי־טק", עונד שעון רולקס, "טחון", בונה ארמון או רוכש מכוניות פאר, לא ייכללו בקטגוריה הזאת.

3.3. מאגר מידע

העובדה שמפלגה מחזיקה בנתונים הנכללים בהגדרה "מידע אישי"¹⁶⁷, אינה מספיקה כשלעצמה לשם החלת הוראות חוק הגנת הפרטיות על עיבוד המידע, אלא על המידע להיות מאוגד ב"מאגר מידע".¹⁶⁸ תיקון 13 דייק וצמצם במידה מסוימת את ההגדרה "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;¹⁶⁹

166 פרוטוקול 210, לעיל ה"ש 138, בעמ' 44-49.

167 ראו לעיל דיון בהגדרת "מידע אישי", ס' 3.1.

168 לביקורת על הותרת המונח "מאגר מידע" כתנאי לתחולת הוראות חוק הגנת הפרטיות, ראו רחל ארידור הרשקוביץ **תיקון 13 לחוק הגנת הפרטיות: משמעות התיקון, השלכותיו וחסרונותיו** (הצעה לסדר 62, המכון הישראלי לדמוקרטיה 2026).

169 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

לפי הגדרה זו, אוסף פרטי מידע לשימוש אישי בלבד לא ייחשב מאגר מידע. נוסף על כך, אוסף הכולל רק שם, מען ודרכי תקשורת על 100,000 נושאי מידע או פחות, שאי אפשר להפיק ממנו נתונים שייחשבו "מידע אישי", ושלבעליו אין אוסף אחר הכולל פרטי מידע על אותם נושאי מידע, יוחרג מהגדרת מידע אישי.

עם תחילת תקופת הבחירות כל מפלגה מקבלת לידיה את מידע הפנקס, הכולל את מספרי הזהות של כל אחד מבעלי זכות הבחירה בישראל, והיקפו עולה כמובן על 100,000 איש. לכן, כל מפלגה מחזיקה במאגר מידע. גם אם מפלגה תפצל את מידע הפנקס לאוספים נפרדים, ובכל אחד מהם רק שם, מען ודרכי תקשורת על 100,000 בעלי זכות בחירה לכל היותר, היא תתקשה להימלט מהגדרת "מאגר מידע", משום שהחריג להגדרת "מאגר מידע" מחייב שלא יהיה אצל בעל האוסף או אצל תאגיד שבשליטתו אוסף נוסף הכולל פרטי מידע אישי אחרים על אותם נושאי מידע. סביר שבידי מפלגה יש פרטי מידע נוספים על בעלי זכות הבחירה בישראל, כגון מידת תמיכתם במפלגה או אם הם צריכים סיוע בהגעה לקלפי ביום הבחירות.

אשר למפעיל יישומון בחירות, לכאורה אם יחזיק אך ורק באוספי מידע הכוללים רק שם, מען ודרכי תקשורת על עד 100,000 בעלי זכות בחירה, הוא עשוי להימלט מהגדרת "מאגר מידע". אולם, מהמידע שפורסם בציבור על יישומון אלקטרוני נראה שהחזקת אוספי מידע דלים שכאלה אינה סבירה, שכן מפעיל יישומון הבחירות לא יוכל לסייע באמצעותם במיקוד ובהמרצת תעמולת הבחירות למפלגה השוכרת את שירותיו. זאת ועוד, גם אם מפלגה אחת מסתפקת במאגר מידע קטן, אם מפעיל יישומון הבחירות מספק שירותים למפלגות נוספות הוא 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 ב"מאגרי מידע".

3.4. עיבוד ושימוש במידע

"עיבוד" מידע ו"שימוש" במידע הם מונחים חלופיים המתארים רשימה רחבה ופתוחה של פעולות, כמו המונח "עיבוד" (processing) ב-GDPR.¹⁷⁰ "עיבוד" ו"שימוש" משמעם כל פעולה המבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו.¹⁷¹ בשל רוחב ההגדרה נקודת המוצא היא שכל פעולה הנעשית במידע אישי תיחשב "שימוש" או "עיבוד".

3.5. סיכום

כל מפלגה ורשימת מועמדים מקבלת לידיה עם תחילת תקופת הבחירות את מידע הפנקס, ובו שם, מען ומספר זהות של כל בעלי זכות הבחירה בישראל. על בסיס מידע הפנקס מוסיפה המפלגה שכבות נתונים נוספות. מאחר שמידע אישי מוגדר בהרחבה, מידע הפנקס ושכבות הנתונים הנוספות נכללים בהגדרה "מידע אישי". יתרה מזו, לעיתים קרובות אף מדובר ב"מידע 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 יישומי בחירות הוא "מאגר מידע" כהגדרתו בחוק, והפעולות שעושים המפלגות ומפעילי יישומי בחירות במידע אישי ובמידע בעל רגישות מיוחדת שבמאגרי המידע הן "עיבוד" או "שימוש".

170 ראו ס' 4(2) ל-GDPR, לעיל ה"ש 5.

171 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

פרק 4

בעלי תפקידים וחובותיהם

4.1. בעלי תפקידים רלוונטיים

עיבוד נתונים שהם מידע אישי ב"מאגר מידע" מקים חבות. כדי להבין מה נכלל באותה חבות, יש להבין את סוג התפקידים שממלאות מפלגות, רשימות מועמדים ומפעילי יישומי בחירות לפי החוק.

4.1.1. 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 הייתה שהמפלגה היא הבעלים אך ורק של המידע המטויב, שהוא חלק קטן ממידע הפנקס,¹⁷² והיא מחזיקה בזכות שימוש מוגבלת במידע הפנקס.¹⁷³ הרשות להגנת הפרטיות קבעה שאף שהמדינה היא בעלת מאגר מרשם האוכלוסין, שממנו נגזר מידע הפנקס שנמסר למפלגות, מרגע מסירת מידע הפנקס למפלגה, נוצר מאגר מידע חדש שהמפלגה, ולא המדינה, היא המחליטה אם וכיצד להשתמש בו לקידום מטרותיה הפוליטיות. העובדה שהשימוש במידע הפנקס מוגבל לפי חוק הבחירות, אינה גורעת מאחריות המפלגה בהיותה בעלת המאגר.¹⁷⁴

172 ראו, למשל, קביעת הפרה ישראל ביתנו, לעיל ה"ש 84, ס' 9.1.

173 שם, ס' 9.6, בעמ' 4.

174 ראו קביעת הפרה הליכוד, לעיל ה"ש 84, ס' 10.4-10.6.

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".¹⁷⁵ בעל השליטה במאגר המידע קובע רק את מטרות העיבוד, ואת האמצעים לעיבוד המידע קובע על פי רוב מי שמעבד בפועל את המידע ונקרא ה"מחזיק".¹⁷⁶

על פי הגדרה זו, אף שמפלגות מקבלות את מידע הפנקס מכוח חוק הבחירות,¹⁷⁷ המגביל את השימושים לצורכי התמודדות בבחירות וקשר עם ציבור הבוחרים,¹⁷⁸ כלומר, קובע מסגרת מטרות חוקית לשימוש במידע פנקס, בתוך מסגרת זו כל מפלגה יכולה לקבוע כרצונה את מטרות השימוש. לכן, המפלגה היא בעלת השליטה במאגר המידע, בין שמדובר רק במאגר מידע אחד הכולל את מידע הפנקס והמידע המטויב המוסף על ידה, בין בשני מאגרי מידע נפרדים, האחד כולל רק את מידע הפנקס, והשני – מידע מטויב וחלקים ממידע הפנקס. לחלופין, המפלגות הן הגוף שהוסמך בחיקוק (חוק הבחירות) לעבד מידע במאגר מידע, וגם משום כך הן עונות להגדרה "בעל שליטה במאגר מידע".¹⁷⁹

4.1.2 "מחזיק"

בהחלטה בדבר ההפירה בפרשת אלקטור קבעה הרשות להגנת הפרטיות שאלקטור היא "מחזיק", ושאין בעובדה שמאגר המידע היה בידי אלקטור תקופה קצרה ולא דרך קבע, כדי לשנות את הקביעה הזאת, משום שבתקופה זו חברת אלקטור הייתה רשאית לעשות פעולות עיבוד מידע במאגר על פי

175 ס' 2 לחוק הגנת הפרטיות, לעיל ה"ש 9.

176 ראו הדיון בטקסט הנלווה לה"ש 180-183 להלן.

177 ס' 39(ב) לחוק הבחירות לכנסת, לעיל ה"ש 75.

178 ס' 39(ג) לחוק הבחירות לכנסת, שם.

179 כך גם בהפירה הרשות להגנת הפרטיות בהנחיות שפרסמה לאחרונה. ראו הרשות להגנת הפרטיות, [הנחיות למפלגות לקראת הבחירות לכנסת ה-26](#): דרישות חוק הגנת הפרטיות, מגבלות השימוש בפנקס הבוחרים ואחריות המפלגות על אפליקציות וספקים חיצוניים, בעמ' 4.

דרישת המפלגה.¹⁸⁰ קביעה זו נותרת בעינה גם לפי ההגדרה המעודכנת למונח "מחזיק" בתיקון 13. גם לאחר תיקון 13 חוק הגנת הפרטיות מבחין בין בעל שליטה במאגר מידע לבין מי ש"מחזיק בו", שלפי ההגדרה הוא גורם חיצוני לבעל השליטה במאגר המידע, המבצע במידע שבמאגר המידע פעולות עיבוד על פי המטרות שקובע בעל השליטה. אולם, אופן העיבוד עצמו והאמצעים שבעזרתם יעובד המידע נתונים לשיקול דעתו ולהחלטתו של המחזיק.¹⁸¹ למשל, משרד עורכי דין הוא בעל השליטה במידע האישי על עובדיו. אולם, אם הוא מעביר לחברה המספקת שירותי ניהול שכר מידע אישי על עובדיו, החברה המספקת את שירותי ניהול השכר היא ה"מחזיק" במאגר המידע. לעומת זאת, חשב השכר העובד במשרד עורכי דין לא ייחשב מחזיק, שכן הוא אינו גורם חיצוני לבעל השליטה (משרד עורכי הדין). נוסף על כך, לפי הגדרת "מחזיק" שתוקנה בתיקון 13, אין צורך בהחזקת עותק פיזי של מאגר המידע כדי להיחשב מחזיק,¹⁸² ולא נדרשת הוכחת התקשרות בין בעל השליטה למחזיק.¹⁸³

לפיכך, כל גורם חיצוני למפלגה, כלומר כל מי שאינו עובד המפלגה שהמפלגה העבירה לו את מאגר המידע לשם עיבודו בעבורה ייחשב "מחזיק". פרק הזמן של עיבוד המידע, אופן ההתקשרות בין המפלגה לגורם הזה, והשאלה מי קובע את אמצעי העיבוד – אינם רלוונטיים לכך שמדובר ב"מחזיק".¹⁸⁴

180 ראו, למשל, קביעת הפרה ישראל ביתנו, לעיל ה"ש 84, ס' 10.3, 10.5 ו-10.11, בעמ' 13; קביעת הפרה הליכוד, שם, ס' 10.4 בעמ' 10; קביעת הפרה אלקטור, שם, ס' 9.4 ו-10.5, בעמ' 4 ו-11.

181 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

182 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' 423-424.

183 זאת בניגוד לדרישת ההתקשרות שהופיעה בהגדרת "מחזיק" בהצעת החוק הממשלתית, שם, ס' 2(1):

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

184 כך גם בהחירה הרשות להגנת הפרטיות בהנחיות שפרסמה לאחרונה. ראו הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 4.

4.1.3. 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".¹⁸⁵

הואיל ומפלגה או מפעיל יישומון בחירות אינם "גוף ציבורי" כהגדרתו בסעיף 23 לחוק הגנת הפרטיות ובצו 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 5

החובות העיקריות המוטלות על מפלגות ועל מפעילי יישומוני בחירות

חוק הגנת הפרטיות מטיל על בעל שליטה במאגר מידע ועל מחזיק כמה חובות, ואותן נסקור להלן.

5.1. חובת רישום מאגר מידע

תיקון 13 צמצם מאוד 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; וכן על 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 מעל 10,000 בני אדם.¹⁸⁶

חובת רישום מוטלת רק על בעל שליטה במאגר מידע, ועל כן אינה רלוונטית למפעיל יישומון בחירות. אשר לחבותה של מפלגה בהיותה בעלת השליטה במאגר המידע, ברישום מאגר מידע נדרשת בחינה מעמיקה. על מפלגה לעבד את המידע במאגר המידע בהתאם לסעיף 39(ג) לחוק הבחירות, שלפיו היא מתחייבת שהשימוש שתעשה במידע הפנקס, לרבות העברתו לאחר, יוגבל רק

186 ס' 8א(א)(1) לחוק הגנת הפרטיות, ש.ס.

"לצורכי התמודדותה בבחירות ולצורכי קשר עם ציבור הבוחרים". כלומר, מטרתו העיקרית של איסוף המידע לא יכולה להיות מסירתו לאחר כדרך עיסוק או בתמורה. העברת המידע מהמפלגה למפעיל יישומן בחירות, היא במסגרת יחסי בעל שליטה ומחזיק ואינה נחשבת מסירה כדרך עיסוק או בתמורה. יתרה מזו, 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) 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". הגדרתו של "דיוור ישיר" בחוק היא "פנייה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר המידע".¹⁸⁷ לפיכך, וכפי שהבהירה הרשות להגנת הפרטיות בהבהרות שפרסמה לפני הבחירות לכנסת ה-23 וה-24,¹⁸⁸ מסרי תעמולה חישובית המותאמים אישית למאפייניו של בוחר עשויים להיחשב דיוור ישיר. אולם חובת הרישום חלה רק אם מטרתו העיקרית של מאגר המידע היא "שירותי דיוור ישיר". אלו מוגדרים "מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא".¹⁸⁹ מפלגה עושה דיוור ישיר בעצמה או באמצעות מפעיל יישומן בחירות, אך היא אינה מספקת שירותי דיוור ישיר לאחרים. משום כך, נראה לנו שלא חלה עליה חובת הרישום מטעם זה.

אשר לשאלה אם חלה על מפלגה חובת רישום בהיותה גוף ציבורי, מפלגה אינה "גוף ציבורי" כהגדרתו בפסקה (1) להגדרת גוף ציבורי שבסעיף 23 לחוק הגנת הפרטיות.¹⁹⁰ אולם מפלגה נחשבת גוף דו-מהותי, שכן פעולותיה עשויות להיות

187 הגדרת "דיוור ישיר" בס' 3 לחוק הגנת הפרטיות, שם.

188 הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 124, בס' 13-16; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24, לעיל ה"ש 124, בס' 17.6.

189 ס' 3 לחוק הגנת הפרטיות, לעיל ה"ש 9.

190 ס' 23(1) לחוק הגנת הפרטיות, שם: "משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין".

בחלקן בעלות אופי פרטי ובחלקן בעלות אופי שלטוני ציבורי. כך, לצד עקרונות מהמשפט הפרטי החלים על ענייניה ופעולותיה של המפלגה, עשויים לחול עליה גם כללים וחובות מכוח המשפט הציבורי.¹⁹¹

בית המשפט העליון הכיר בכך שפעולותיה של מפלגה בכל הקשור לענייניה הפרטיים, לרבות הפעולות שהמפלגה נוקטת לקידום ערכים ועקרונות התואמים את צו מצפונם ואמונותיהם של חבריה, הן אמצעי חשוב למימושן של זכויות יסוד של חבריה ותומכיה, בעיקר חופש ההתאגדות הפוליטי, חופש הביטוי והזכות לבחור ולהיבחר. מדובר, לפיכך, בנושאים פרטיים, שבהם המפלגה צריכה ליהנות מחופש פעולה יחסי בהיותה גוף פרטי.¹⁹²

עם זאת, בפרשת ערוץ 14 קבע בית המשפט העליון שהחלטתה 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, ובראשם החובה לנהוג בשוויון ולכבד את חופש העיתונות. סיקור אירוע הבחירות המרכזי במטה המפלגה משקף מפגש בין חופש הביטוי, חופש העיתונות וזכות הציבור לדעת, ולכן חסימת כניסתו של כלי תקשורת מסוים אחד בלבד לאירוע בעל גוון ציבורי ניכר היא פגיעה ב"גרעין הקשה" של חופש העיתונות. 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, והיא אינה פוגעת פגיעה של ממש בחופש הפעולה או בחופש הביטוי של המפלגה. לעומת זאת, החלטה של מפלגה לקיים ראיונות יזומים או למסור מידע רק לערוץ תקשורת מסוים, באופן המבטא את תמיכתה של המפלגה בערוץ תקשורת זה ובלי לזמן את כל ערוצי התקשורת או מרביתם למשרדיה, היא בעלת מאפיינים פרטיים הגוברים על המאפיינים הציבוריים.¹⁹³

191 בג"ץ 7232/22 ערוץ יהודי ישראלי בע"מ נ' מרצ – השמאל של ישראל בראשות זהבה גלאון ואח' (31.10.2022), ס' 19 לפסק דינה של השופט ברק ארז (לעיל פרשת ערוץ 14).

192 שם, ס' 20 לפסק דינה של השופט ברק ארז.

193 שם, ס' 22–24 לפסק דינה של השופט ברק ארז.

עם זאת, אין בפסיקה או בחקיקה קביעות מהותיות קשיחות בשאלה 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.¹⁹⁴

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

אשר לתכלית הטלת חובת הרישום על גופים ציבוריים, במהלך הדיונים בנושא בתיקון 13 הסבירה ועדת החוקה כי המדינה אוספת בכפייה מידע אישי רב על אזרחיה, ועל כן, כחלק מעקרון חופש המידע, עליה לספק לאזרח מידע מדויק על המידע שהיא מחזיקה על אודותיו ולאפשר לו לממש את זכויותיו ביחס למידע הזה.¹⁹⁵

אשר 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.¹⁹⁶ 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 של המידע הזה, לא ברור שמתקיימת תכלית הטלת חובת הרישום על גופים ציבוריים, שכן אין מדובר במידע הנאסף בכפייה מהאזרחים. זאת ועוד, עיבוד המידע האישי אינו מבטא בהכרח מאפיינים ציבוריים בולטים.

194 שם, ס' 25, 27 לפסק דינה של השופט ברק ארז.

195 פרוטוקול 210, לעיל ה"ש 138, בעמ' 107-108, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

196 ס' 26(ה), 40(א) לחוק הבחירות, לעיל ה"ש 75.

כמו כן, תחולת חובת הרישום הוגבלת 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,¹⁹⁷ מוחרגים במפורש מתחולת חובת הרישום.¹⁹⁸ החרגה זו עשויה ללמד דווקא על רצונו של המחוקק להימנע מהרחבת יתר של חובת הרישום.

לפיכך, מכלול נסיבות אלו, העובדה שלבד מהמידע המופיע במידע הפנקס, המידע האישי שבמאגר המידע שבידי המפלגה לא נאסף על ידה בכפייה, הימנעותו של המחוקק מהרחבת חובת הרישום גם על גופים ששר המשפטים יכריז שהם גופים ציבוריים, בשילוב העובדה שחובת הרישום אינה מספקת הגנה מהותית לזכות לפרטיות,¹⁹⁹ תומכות לדעתנו באי־החלת חובת הרישום על מפלגות.

5.2. 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 הנמסרת לרשות לכלול את פרטי בעל השליטה ואת דרכי ההתקשרות עימו, מידע על זהותו של הממונה על הגנת הפרטיות בארגון ודרכי ההתקשרות עימו, והעתק ממסמך הגדרות המאגר. המדובר במסמך הנדרש מבעל השליטה לפי תקנות אבטחת מידע. על בעל שליטה לפרט במסמך הגדרות המאגר כמה נושאים, כגון מטרות השימוש במאגר המידע, סוגי המידע

197 ס' 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".

198 ס' 8א(1)(ב) לחוק הגנת הפרטיות, שם.

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

שבמאגר, אם מבוצע עיבוד מידע באמצעות גורם אחר, מהם סיכוני האבטחה למאגר וכיצד הוא מתמודד עימם. כן עליו לשמור את המסמך אצלו ולעדכנו בכל שנה לפחות.²⁰⁰ בעל השליטה נדרש להעביר את מסמך מטרות המאגר לעיונה של הרשות להגנת הפרטיות כחלק מחובת ההודעה, כדי לספק לה את המידע הנחוץ להערכת חוקיותו של מאגר המידע ולפעולות הפיקוח והאכיפה המינהלית הנדרשות ביחס אליו. על בעל השליטה במאגר המידע לעדכן את הרשות בדבר שינוי באחד מהפרטים האלה או על שינוי במסמך הגדרות המאגר.²⁰¹

מאחר שמידע הפנקס כולל מידע אישי על כל בעלי זכות הבחירה בישראל, כלומר על יותר מ-100,000 איש, 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 בהיותן בעלות שליטה.

5.3. חובת אבטחת מידע וחובת מינוי ממונה אבטחת

מידע

חובת אבטחת מידע המוטלת על בעל שליטה ומחזיק כדי להגן על מידע אישי שברשותם מפני גישה, שימוש או חשיפה בלתי מורשים, אינה חדשה. בפרשת **אלקטור** כפרו מפלגת הליכוד וחברת אלקטור בקביעה שהפרו חובה זו. מפלגת הליכוד טענה ש"לא קיימת מערכת שהיא חסינה לאירועי אבטחה וכי העולם הרשתי אינו חסין מפני אירועים של אבטחת מידע".²⁰² אלקטור מצידה טענה שמאחר שאין אפשרות לחסינות מלאה מאירועי אבטחה בעולם התוכנה, "המדד הנכון לבחינת רמת האבטחה [...] הינו המהירות שבה מאותרת פרצת אבטחה

200 חקנה 2(א)(1) לתקנות אבטחת מידע, לעיל ה"ש 138; פרוטוקול 223, לעיל ה"ש 160, בעמ' 77.

201 ראו ס' 8א(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

202 קביעת הפרה הליכוד, לעיל ה"ש 84, ס' 9.14, בעמ' 6.

ומנוטרלת".²⁰³ 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".²⁰⁴ עוד קבעה הרשות שמפלגה, בהיותה בעלת שליטה במאגר מידע, נושאת באחריות גם להתנהלותו של המחזיק, דהיינו אלקטור, בכל הקשור לעיבוד מידע במאגר מידע, ואינה יכולה להסתפק בהצהרות המחזיק שהוא עומד בהוראות החוק והתקנות. כן אין בעובדה שאלקטור הייתה בפיקוח הרשות להגנת הפרטיות בעבר, בשנת 2018, כדי להעניק אישור מספק לרמת אבטחת המידע הנוכחית של מערכותיה. לפי הרשות להגנת הפרטיות, כדי לעמוד בחובות אבטחת המידע המוטלות על בעל מאגר מידע, לרבות אלו הקבועות בתקנות אבטחת מידע, על בעל מאגר מוטלת 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.²⁰⁵ עוד הבהירה הרשות שרמת האבטחה המינימלית שחלה על מאגר מידע המבוסס על מידע הפנקס היא רמת האבטחה הבינונית לפי תקנות אבטחת המידע.²⁰⁶

תיקון 13 הוסיף לחובת אבטחת מידע כמה הבהרות, ובהן ביטול סעיף 17 לחוק הגנת הפרטיות שחייב מחזיק של כמה מאגרי מידע של בעלים שונים לעקוב אחר מורשי הגישה למאגר. בנימוק שהנושא מוסדר בתקנות אבטחת מידע.²⁰⁷

203 קביעת הפרה אלקטור, שם, ס' 9.7.4, בעמ' 6.

204 קביעת הפרה הליכוד, שם, ס' 10.10, בעמ' 13; קביעת הפרה אלקטור, שם, ס' 10.8 בעמ' 13.

205 ראו, למשל, קביעת הפרה ישראל ביתנו, שם, ס' 10.12, בעמ' 13; קביעת הפרה הליכוד, שם, ס' 10.9, בעמ' 12.

206 הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 4.

207 פרוטוקול 233 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (21.1.2024), בעמ' 46-45.

נוסף על כך, 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.²⁰⁸

בהיותה בעלת שליטה במאגר מידע מפלגה אחראית לאבטחת המידע שבמאגר המידע שבשליטתה, ומפעיל יישומון בחירות בהיותו מחזיק אחראי לאבטחת המידע שבמאגרי המידע שבחזקתו.²⁰⁹ כמו כן, 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 יכול ללמוד מידע בעל רגישות מיוחדת על 100,000 איש לפחות.²¹⁰

מפעיל יישומון בחירות המחזיק בחמישה מאגרי מידע החייבים בהודעה לרשות להגנת הפרטיות,²¹¹ בין שמאגרים אלו הם של אותה המפלגה או של מפלגות שונות, חייב במינוי ממונה אבטחת מידע.

5.4. חובת מינוי ממונה הגנת פרטיות

חובת מינוי ממונה הגנת פרטיות היא חובה חדשה שהוספה בתיקון 13, והיא חלה על בעל שליטה במאגר מידע ועל מחזיק, בהתקיים אחד מהתנאים הקבועים בחוק.²¹²

208 ראו ס' 17 לחוק הגנת הפרטיות, לעיל ה"ש 9; פרוטוקול 249 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (6.2.2024), בעמ' 117-118; פרוטוקול 336 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (4.6.2024), בעמ' 37-39.

209 על פי הוראת ס' 17(א) לחוק הגנת הפרטיות, לעיל ה"ש 9.

210 לפי ס' 8א(ב)(1), (3) לחוק הגנת הפרטיות, שם. ראו הדיון בס' 5.2 לעיל.

211 לפי ס' 8א(ב)(1), (3) לחוק הגנת הפרטיות, שם. ראו הדיון בס' 5.2 לעיל.

212 ס' 17ב(א)(1), (2) לחוק הגנת הפרטיות, שם.

(1) בעל שליטה, שהוא גוף ציבורי כהגדרתו בסעיף 23 לחוק הגנת הפרטיות (למשל, רשות מקומית או משרד ממשלתי), למעט גוף ביטחוני כהגדרתו בסעיף 223 לחוק 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 היא חלה גם על גופים ששר המשפטים יקבע בצו שהם גופים ציבוריים.²¹³ עובדה זו עשויה להיות רלוונטית בבחינה אם ניתן להטיל את חובת מינוי ממונה הגנת הפרטיות על מפלגה על בסיס היותה גוף 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.

(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".²¹⁴

החוק מספק דוגמאות לבעלי שליטה או למחזיקים, למשל ספק מורשה של שירותי טלקומוניקציה, ספק שירות חיפוש מקוון ומי שפעולות שנכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, 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; הפעלת יישומון מעקב אחר מיקום פיזי או אחר נתוני בריאות; שימוש במכשירי "אינטרנט של דברים" (IoT), כגון כלי רכב חשמליים; מאגר תצלומים של מצלמות מעקב וספקי אינטרנט.²¹⁵ לעומת זאת,

213 ס' 23(2) לחוק הגנת הפרטיות, שם.

214 ס' 117(א3) לחוק הגנת הפרטיות, שם.

215 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), בס' 9.8.

עסק קטן המנטר רק את עובדיו ניטור פנימי ולא שוטף עשוי שלא להיות חייב במינוי ממונה הגנת פרטיות.

(5) בעל שליטה או מחזיק "שעיסוקו העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר".

החוק מספק כמה דוגמאות לבעל שליטה או למחזיק העונים לתיאור הזה, כמו תאגיד בנקאי, חברת ביטוח, בית חולים וקופת חולים.²¹⁶ בטיוטת גילוי דעת של הרשות לפרטיות הובהר שהכוונה היא לגופים שעבוד המידע בעל הרגישות המיוחדת בהיקף ניכר הוא חלק מרכזי בהגשמת המטרות הארגוניות או העסקיות שלהם, או חלק אינהרנטי מפעילות הליבה של הארגון, אך אם אינו חיוני להגשמתה. עם זאת, אם עיבוד המידע בעל הרגישות המיוחדת בהיקף ניכר נעשה "רק לצורך ביצוע מטרות עזר משניות כגון העסקת עובדים, אם אינן בעלות זיקה ישירה למטרות המרכזיות של הארגון", אין מדובר בארגון שזהו עיסוקו העיקרי.²¹⁷

החוק מונה גם רשימה פתוחה של קריטריונים שלפיהם אפשר לקבוע אם 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 הגאוגרפי של פעולת העיבוד.²¹⁸ הרשות להגנת הפרטיות הבהירה בטיוטת גילוי הדעת שאין הכרח שכל הקריטריונים יתקיימו במצטבר כדי להכיר בכך שעיבוד המידע עולה כדי עיבוד מידע בהיקף ניכר.²¹⁹

216 ס' 117(א)(4) לחוק הגנת הפרטיות, לעיל ה"ש 9: פרוטוקול 336, לעיל ה"ש 208, בעמ' 6-15; פרוטוקול 351 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (23.6.2024), בעמ' 36-54.

217 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 215, בס' 9.6. פרשנות זו עולה בקנה אחד גם עם הפרשנות האירופית בנושא. ראו Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017).

218 ס' 117(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

219 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 215, בס' 9.10.

הוראות החוק עוסקות גם בכישורים הנדרשים לשם מינוי ממונה הגנת פרטיות ובהגדרת תפקידיו, מתוך התפיסה שמילוי 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.²²⁰ ממונה נדרש להחזיק בידע בדיני הגנת הפרטיות בישראל, לצד הבנה הולמת בטכנולוגיה ובאבטחת מידע, וכן להכיר את תחומי הפעילות של הגוף שבו הוא משמש ממונה. הכול בהתאם לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו באותו הארגון. הרשות להגנת הפרטיות הוסיפה כי נכון לדרוש גם ניסיון ממש, וכן הכשרה בסיסית בתחום.²²¹

החוק קובע כי יש לספק לממונה את התנאים והמשאבים הדרושים למילוי נאות של תפקידו ולוודא שהוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות.²²² כדי לוודא שניתן קשב ראוי להערותיו של הממונה, עליו לדווח ישירות למנכ"ל בעל השליטה או המחזיק, או לעובד הכפוף לו ישירות. הרשות להגנת הפרטיות קבעה שהחוק מחייב את הארגון להיוועץ בממונה על הגנת הפרטיות, כלומר, שיש להתייחס לדעתו בכובד ראש, ואם מוחלט לנהוג שלא לפי חוות דעתו – יש לנמק את הסיבות לכך.²²³

החוק גם אוסר על הממונה למלא תפקיד נוסף בארגון או להיות כפוף לנושא משרה בארגון, אם מילוי התפקידים האלה עלול להעמידו בחשש לניגוד עניינים.²²⁴ 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

220 ס' 217(א) לחוק הגנת הפרטיות, לעיל ה"ש 9; פרוטוקול 336, לעיל ה"ש 208, בעמ' 23-26.

221 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 215, בס' 12.2.

222 ס' 217(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

223 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 215, בס' 15.1.

224 ס' 117(ג)(3) לחוק הגנת הפרטיות, לעיל ה"ש 9.

בהכרח תפקידים היוצרים ניגוד עניינים כזה. נוסף על כך, הרשות מציעה לקבוע כלל אצבע, שלפיו תפקידים בכירים, כגון מנהל שיווק, מנהלת לקוחות, מנהל כספים, מנהלת מערכות מידע או מנהל טכנולוגיות ראשי הם תפקידים היוצרים ניגוד עניינים מול תפקיד הממונה.²²⁵

לצד התנאים הקבועים בחוק הגנת הפרטיות למינוי ממונה הגנת הפרטיות המליצה הרשות להגנת הפרטיות בטיטת גילוי הדעת למנות ממונה כזה בארגון גם אם התנאים למינוי אינם מתקיימים, משום שמינוי צפוי לשפר את הגנת הפרטיות והציות לחוק בארגון.²²⁶

כאמור, מפלגה אינה גוף ציבורי או סוחר מידע, וכן אינה אוספת מידע אישי לשם מתן שירותי דיוור ישיר, אף שהיא בהחלט שולחת מסרי דיוור ישיר.²²⁷ עם זאת, יש לבחון אם היותה של מפלגה גוף דו־מהותי עשוי להקים חובת מינוי ממונה הגנת פרטיות במקרה הזה. אומנם, התבחינים להטלת חובת מינוי ממונה הגנת הפרטיות על גוף ציבורי או סוחר מידע נקבעו בוועדת החוקה במהלך הדיונים על תיקון 13, על בסיס 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.²²⁸ עיבוד מידע אישי בעל רגישות מיוחדת, בהיקפים שמעבדות

225 גילוי הדעת בנוגע למינוי ממונה הגנת פרטיות, לעיל ה"ש 215, בס' 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 Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01 (Apr. 5, 2017).

226 שם, בס' 9.12.

227 ראו הדיון בטקסט הנלווה לה"ש 187-189.

228 פרוטוקול 336, לעיל ה"ש 208, בעמ' 16.

מפלגות מעורר חשש, לא תאורטי,²²⁹ לפגיעה בפרטיות העלולה להוביל, אף שהנושא טרם הוכרע, לפגיעה בחשאיות הבחירות ובהגיונותם ובזכות לבחור. משום כך, מדובר בפעולה העשויה להיחשב לבעלת מאפיינים ציבוריים מובהקים המצדיקים את החלת חובת מינוי ממונה הגנת פרטיות על מפלגה במסגרת החלתה על גופים ציבוריים ועל בסיס היותה גוף 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. עם זאת, כאמור, החלת חובות על מפלגה בהיותה גוף דו־מהותי צריכה להיבחן בכל מקרה ומקרה.²³⁰

לצד השאלה אם חובת מינוי ממונה הגנת פרטיות עשויה לחול על מפלגה בשל היותה גוף דו־מהותי יש לבחון גם את התנאים הנוספים להטלתה. אומנם עיסוקה העיקרי של המפלגה אינו כולל פעולות עיבוד מידע ואינו כרוך בפעולות עיבוד מידע, שלנוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם. אולם התנאי האחרון הקבוע בחוק למינוי ממונה הגנת פרטיות עשוי להיות רלוונטי למפלגה בהיותה בעלת שליטה. 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 שעיסוד זה יהיה חלק מרכזי בהגשמת המטרות הארגוניות שלה. עיבוד מידע שהוא אינהרנטי לפעילות בעל השליטה ייחשב חלק מרכזי בהגשמת המטרות הארגוניות או העסקיות שלה גם אם אינו חיוני להגשמתן. לפיכך, בבחינת נסיבות עיבוד המידע האישי בידי מפלגות בשנים האחרונות, בהחלט ייתכן שאפשר לומר שהוא נעשה חלק אינהרנטי בפעולות שמפלגה נוקטת לשם התמודדות בבחירות לכנסת ולשם תקשורת עם ציבור הבוחרים, אף שאין מדובר בפעולה שאי אפשר בלעדיה, שכן מפלגה יכולה להתמודד בבחירות וליצור קשר עם ציבור הבוחרים אף מבלי לעבד מידע אישי בעל רגישות מיוחדת בהיקף ניכר על אודותיהם.²³¹ בהנחות הרשות

229 הזכות לפרטיות כבר הופרה במערכות בחירות בעבר, כפי שמוכיחה פרשת אלקטור. ראו הדיון בטקסט הנלווה לה"ש 107-112.

230 פרשת ערוץ 14, לעיל ה"ש 191, ס' 25, 27 לפסק דינה של השופט ברק ארז.

231 החלופה הקבועה בס' 117(א)(4) לחוק הגנת הפרטיות, לעיל ה"ש 9.

להגנת הפרטיות שפורסמו לקראת הבחירות לכנסת ה-26 ציינה הרשות שחובת מינוי ממונה הגנת פרטיות לפי תנאי זה תחול על רבות מהמפלגות, שכן הן מעבדות מידע אישי בעל רגישות מיוחדת בהיקף ניכר.²³²

אשר למפעיל יישומון בחירות, לעמדת הרשות להגנת הפרטיות, כאשר בעל השליטה חב בחובת מינוי ממונה הגנת פרטיות חובה זו תחול גם על המחזיק.²³³ כלומר, מפעיל יישומון יחוב במינוי ממונה הגנת פרטיות אם ייקבע שמפלגה חייבת במינוי ממונה הגנת פרטיות מכורח היותה גוף דו־מהותי ועל בסיס סעיף 17ב(א)(1) המטיל חובת מינוי על גוף ציבורי או על מחזיק במאגר מידע שבשליטת גוף ציבורי או סעיף 17ב(א)(4) המטיל חובת מינוי כאשר מעובד מידע אישי בעל רגישות מיוחדת בהיקף ניכר כחלק מעיסוקו העיקרי.²³⁴ אפשרות נוספת לחיובו של מפעיל יישומון במינוי ממונה הגנת פרטיות מבוססת על העובדה שמפעיל יישומון בחירות מעבד את מידע הפנקס ומידע מטיוב, לרבות מידע בעל רגישות מיוחדת, המוסף לו. עיבוד מידע זה נעשה בהיקף ניכר, שכן מדובר במאגרי מידע הכוללים את כל בעלי זכות הבחירה בישראל. יתרה מזו, עיבוד המידע כאמור הוא חלק מרכזי בהגשמת מטרותיו העסקיות של מפעיל יישומון בחירות, שהרי זו ליבת השירות שהוא מספק למפלגה. משום כך, סביר שמפעיל יישומון בחירות יחוב בחובה למנות ממונה הגנת פרטיות לפי החלופה הקבועה בסעיף 17ב(א)(4) לחוק הגנת הפרטיות.

232 הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 7.

233 שם.

234 שם.

פרק 6

הגבלות ואיסורים על עיבוד המידע האישי שבמאגר המידע

6.1. הסכמה מדעת

סעיף 1 לחוק הגנת הפרטיות קובע שכל הפוגע בפרטיותו של אדם באחת מהדרכים המנויות בסעיף 2 לחוק, ובהן שימוש בידעה על ענייניו הפרטיים של אדם שלא למטרה שלשמה נמסרה (סעיף 2(9)), בילוש או התחקות אחרי אדם העלולים להטרידו (סעיף 2(1)), בלי שהוסמך לעשות זאת בדין, נדרש להוכיח שהפגיעה בפרטיות נעשתה בהסכמת נושא המידע.²³⁵

דרישת ההסכמה חוזרת גם בסעיף 11(1) לחוק, העוסק בחובת ההודעה לנושא המידע ומחייב שבעת פנייה לאדם לקבלת מידע אישי על אודותיו לשם עיבודו במאגר מידע, על הפונה לציין גם אם חלה על האדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן מה עשויה להיות תוצאת אי-ההסכמה.²³⁶ כן נכללת דרישת ההסכמה בעקיפין בסעיף 8(ב) לחוק הגנת הפרטיות העוסק בעקרון צמידות המטרה ומחייב שעיבוד מידע אישי יעשה אך ורק על פי מטרת המאגר שנקבעה כדין, שכן בהיעדר הסמכה בדין שימוש במידע למטרה מסוימת יכול להיעשות רק מכוחה של הסכמת נושא המידע. סעיף 8(ד)(1) עוסק בדרישת ההסכמה על דרך השלילה. הוא אוסר על עיבוד מידע אישי במאגר מידע אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד

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

236 שם, וכן ראו הדיון בס' 5.1.

להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע". כך חל האיסור גם על עיבוד מידע אישי שנאסף אגב פגיעה בפרטיות ללא הסכמה תקפה ובהיעדר הסמכה בדין.²³⁷

על פי סעיף 3 בחוק הגנת הפרטיות, "הסכמה" תקפה היא הסכמה המתקבלת מדעת, מרצון חופשי, במפורש או מכללא (במשתמע).

6.1.1. "מדעת"

הדרישה שההסכמה תהיה מדעת נועדה להבטיח שלנושא המידע הייתה בחירה אמיתית ואוטונומית. הסכמה מדעת נדרשת בין שההסכמה ניתנת במפורש, בין שהיא ניתנת מכללא. כדי לעמוד בדרישה שההסכמה תהא מדעת יש להבטיח שהאדם מודע לזכותו לסרב לבקשה לספק מידע אישי על אודותיו לאחר שנתיין לו כל המידע הנחוץ לו, באורח סביר ומובן, לשם החלטה אם לספק מידע אישי על אודותיו או לסרב לה. במסגרת זו נדרש לספק לאדם נתונים על איסוף המידע ועל השימוש בו, לרבות מטרות איסוף המידע וזהות הגורמים שאליהם עשוי המידע האישי להיות מועבר. לעמדת הרשות, די בציון סוג הגורמים שאליהם יועבר מידע אישי על פי השיוך המקצועי שלהם, אך אין להסתפק בזיהוי כללי שאין בו כדי ללמד על השימוש שיעשה אותו הגורם במידע האישי שיקבל. למשל, אפשר 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, כדי שנושא המידע יוכל להבין איזה מידע אישי נאסף על בסיס הסכמתו ולאילו שימושים. בהקשר הזה הבהירה הרשות שפירוט חלקי של המידע שבעל השליטה נדרש לספק, כגון פירוט חלקי של מטרות איסוף המידע, זהות הגורמים שהמידע יועבר אליהם או סוגי המידע האישי הנאספים, ושימוש בביטויים כגון "וכיו"ב" או "בין היתר", אינו מספק. נוסף על כך, יש להקפיד שתוכן המידע המסופק לאדם בעת בקשה לקבל את הסכמתו לאיסוף מידע אישי על אודותיו יוצג בבירור, נגיש, פשוט ומובן. הסכמה שניתנה בלי שהייתה לאדם אפשרות סבירה להבין את משמעותה ואת השלכותיה לא

237 גילוי דעת בנושא הסכמה, לעיל ה"ש 235, בעמ' 2.

תיחשב הסכמה תקפה. כך, למשל, אתר אינטרנט שמדיניות הפרטיות ומסמך תנאי השימוש שלו אינם נגישים באופן סביר למשתמשים, או שהאמור בהם מוצג באופן מסורבל, ארוך וקשה להבנה עשוי להיחשב מי שלא סיפק את המידע הדרוש לשם קבלת הסכמה מדעת לפגיעה בפרטיות.²³⁸

זאת ועוד, פרטי המידע שיש לפרט בהודעה לנושא המידע לפי סעיף 11 אינם מספיקים בהכרח לשם עמידה בדרישת ההסכמה מדעת. אם יש פערי כוחות מהותיים בין הצדדים, ומדובר בפעולה העשויה לפגוע קשה בזכות לפרטיות, או בנסיבות מורכבות אחרות, כגון שימוש בטכנולוגיה חדשה שהשלכותיה אינן ברורות, חובת ההסכמה מדעת מחייבת פירוט רחב יותר של מידע מהפירוט הנדרש במסגרת חובת ההודעה שבסעיף 11 לחוק. על מבקש המידע בנסיבות כאמור לפרט באופן ברור ופשוט את הנתונים המהותיים הרלוונטיים לנושא המידע לשם קבלת החלטה אם להסכים לעיבוד מידע אישי על אודותיו.²³⁹

עוד הבהירה הרשות, שכאשר מבקש המידע הוא ספק שירות והמידע האישי המבוקש הוא למטרות השונות במהותן מתכלית העסקה העיקרית או מידע בעל רגישות מיוחדת שסביר שאינו תואם את ציפיית הלקוח, יש להציג את המידע ואת המטרות האלה בהבלטה ובנפרד ככל הניתן מרכיבי ההתקשרות לצורך מתן השירות. למשל, אם חברה המשווקת מזון בריאות אוספת ממשתמשים הנרשמים לאתר שלה נתוני מיקום ומסלולי תנועה, מדובר במידע שמרבית המשתמשים אינם מצפים שייאסף מהם במסגרת מתן שירות לרכישת מזון. משום כך על החברה להדגיש ולהציג בבירור את עובדת איסוף נתוני המיקום ומסלולי התנועה בתנאי השימוש שלה, בעמוד הבית הראשי, או בהודעה קופצת בעת הרישום לאתר, כדי לבסס את הדרישה שההסכמה היא מדעת. כמו כן, לעמדת הרשות, במתן שירות המיועד לאוכלוסייה בעלת מאפיינים ייחודיים, כגון אנשים עם מוגבלויות, יש לתת לכך את הדעת באופן הצגת המידע לשם ביסוס דרישת ההסכמה מדעת. למשל, יישומון המכוון לאוכלוסייה של ליקוי

238 שם, בעמ' 3-5.

239 שם, בעמ' 7.

ראייה יש להציג את המידע באמצעים ויזואליים או קוליים נגישים העשויים לסייע בהבנת משמעות ההסכמה.²⁴⁰

הסכמה מדעת יכולה להינתן באופן אקטיבי ומפורש (opt-in) של נושא המידע, למשל סימון במשבצת המתירה שימוש במידע. אך גם הסכמה פסיבית (opt-out), כלומר הימנעות של נושא המידע מסימון במשבצת האוסרת על שימוש במידע אישי שאינו הכרחי למתן השירות, בתנאי שההסכם מבהיר שאי-הסימון מבטא קבלה של כל תנאי ברירת המחדל בהסכם, עשויה להיחשב הסכמת מדעת. עם זאת, הסכמה אקטיבית מלמדת על מודעות גבוהה יותר לרכיבי ההסכמה, ועל כן בנסיבות מסוימות תידרש הסכמה מסוג זה כדי לקיים את דרישת ההסכמה מדעת. נסיבות אלו כוללות מקרים שבהם עיבוד המידע הוא למטרות אפיון (פרופילינג) שאינו קשור ישירות בתכלית העסקה, ובעיקר אם מדובר בנסיבות שבהן יש פערי כוחות בין הצדדים, העיבוד מבוצע בהקשר של שירותי דיוור ישיר, אינו נחוץ למתן השירות, או מבוקש למטרות השונות מהותית ממטרות ההסכם שבעניין ניתנה הסכמה כללית ומפורשת.

6.1.2. "מרצון חופשי"

הדרישה שההסכמה תינתן מרצון חופשי נועדה להבטיח שלנושא המידע תהיה בחירה אמיתית אם להסכים לעיבוד המידע האישי על אודותיו או לסרב לה. היותה של ההסכמה "מדעת" אינה מלמדת בהכרח שהיא עומדת גם בדרישה שהיא תינתן מרצון חופשי. בגילוי הדעת בנושא הסכמה הבהירה הרשות ששימוש בכלים עיצוביים ובטקטיקות אפלות (dark patterns) שמטרתן להקשות על נושא המידע להבין את משמעות הסכמתו ולהשפיע השפעה פסולה על החלטתו, עלול ללמד שההסכמה אינה מבטאת את רצונו החופשי של נושא המידע ואינה הסכמה מדעת. לדוגמה, בקשה לאיסוף נתוני מיקום הקופצת בקביעות במהלך משחק רשת לילדים ומקפיאה את המשחק, אינה מאפשרת למשתמש לבטל אותה, וגם לא מציעה לו גישה למידע בנוגע למטרות

השימוש במידע הזה, אלא ביציאה מהמשחק, תיחשב בקשה הפוגעת בחופשיות ההסכמה.²⁴¹

נוסף על כך, לעמדת הרשות, ייתכנו נסיבות שבהן יש 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 מוטלת חובה 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.²⁴²

6.1.3. במפורש או מכללא

חוק הגנת הפרטיות מכיר הן בהסכמה הניתנת במפורש, כלומר הסכמה מובהקת וחד-משמעית בכתב או בעל פה לפגיעה בפרטיות בהקשר שבו התבקשה ההסכמה. במסגרת זו הסכמה מפורשת מוכרת בחתימה על חוזה, סימון אקטיבי במשבצת האישור במסמך תנאי השימוש, אמירה בעל פה, ובמקרים מסוימים גם מחווה גופנית, כגון הנהון בתגובה לשאלה מפורשת.²⁴³

אולם, על פי חוק הגנת הפרטיות גם הסכמה מכללא היא הסכמה תקפה. הכוונה להסכמה משתמעת הנלמדת מהנסיבות, מההקשר ומדרכי ההתנהגות של נושא המידע, על בסיס הפרשנות הסבירה והמקובלת של ההתנהגות. למשל, פעילות פומבית של אדם במפלגה פוליטית היא הסכמה מכללא לחשיפת דעתו הפוליטית. גם השתתפות בתהלוכה במרחב הציבורי היא הסכמה מכללא לפרסום תמונתו של האדם בדיווח חדשותי בדבר קיום התהלוכה. גם בהקשרים דיגיטליים מכירה הרשות להגנת הפרטיות בנסיבות שבהן הסכמה מכללא תקפה. למשל, המשך

241 שם, בעמ' 9-8.

242 שם, בעמ' 10-9.

243 שם, בעמ' 12.

גלילה באתר אינטרנט, לאחר שהוצג בפני המשתמש המידע הנדרש לשם קבלת הסכמתו מדעת לאיסוף מידע על אודותיו עם כניסתו לאתר היא הסכמה מכללא לאיסוף המידע, ובלבד שיש קשר סביר בין מטרות איסוף המידע ועיבודו לבין מאפייני השירות.²⁴⁴

עם זאת, לעמדת הרשות, כפי שהיא 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 בפרטיות, ויש להוכיח הסכמה מפורשת. כן אין בעובדה שאדם הסכים לגילוי מידע אישי מסוים לגורמים מסוימים כדי לתמוך בקיומה של הסכמתו מכללא לגילוי אותו המידע לגורמים אחרים. נוסף על כך, שתיקתו של אדם או היעדר מחאה מצידו לעיבוד מידע על אודותיו ייחשבו הסכמה מכללא לעיבוד המידע רק בנסיבות שבהן אפשר ללמוד שנושא המידע התכוון באמת להסכים לעיבוד המידע, ובלבד שגם אפשר להוכיח שהוא היה מודע לכל המידע הנדרש לשם הוכחת הסכמה מדעת.²⁴⁵

זאת ועוד, נקיטת פעולות לחיזוק הליך קבלת ההסכמה, כגון העדפת הסכמה מפורשת על פני הסכמה מכללא, העדפת הסכמה אקטיבית על הסכמה פסיבית ושימוש בכלים טכנולוגיים ועיצוביים לפישוט ולהנגשת דרישת ההסכמה והמידע הנחוץ לשם קבלתה, אף שאינן נדרשות לפי החוק, תסייע בהוכחת תקפותה של ההסכמה.²⁴⁶

6.1.4 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 שופט בית המשפט העליון סולברג בעניין פלוני, שלפיה ככל שהפגיעה בפרטיות חמורה יותר כך ייטה בית המשפט

244 שם, בעמ' 12.

245 שם בעמ' 14-15.

246 שם, בעמ' 10.

להימנע מלאכוף את הסכמתו של נושא המידע לפגיעה בפרטיותו ויעדיף את סעד הפיצויים.²⁴⁷ אולם, לנוכח היעדר עיגון בחוק לזכות החזרה מהסכמה הבהירה הרשות להגנת הפרטיות שאם נושא המידע מבקש לחזור בו מהסכמה שנתן כדין לעיבוד מידע אישי על אודותיו על בעל השליטה לשקול להיענות בחיוב להסכמה, במיוחד אם 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 שנעשה קודם לה, ולא בהכרח תוביל למחיקת המידע האישי שכבר נאסף.

עוד המליצה הרשות, שבמקרים שבהם התנהגותו של נושא המידע עשויה ללמד שהוא מבקש לחזור בו מהסכמתו, או שההסכמה שנתן מלכתחילה הייתה נקודתית או לזמן מוגבל, יפנה בעל השליטה מיזמתו לנושא המידע כדי לבחון אם 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 על אודותיו באמצעות היישומון נמשך ולבחון אם הוא עדיין מסכים לכך.²⁴⁸

המידע שמפלגה ומפעיל יישומון בחירות מעבדים הוא מידע בעל רגישות מיוחדת בהיקף נרחב. זאת ועוד, כחלק מעיבוד המידע נעשה גם איפיון (פרופילינג) של הבוחרים, מתוך כוונה להתאים להם מסרי תעמולה מותאמים אישית ולשלוח אותם בדיוור ישיר. לפיכך, על מפלגה ומפעיל יישומון בחירות לקבל את הסכמת הבוחרים, נושאי המידע, לעיבוד המידע על אודותיהם. הרשות אף הבהירה שעל המפלגה האחריות להבהיר לכל הפעילים והמשתמשים ביישומון מטעמה שעליהם לקבל את הסכמתו של כל תומך פוטנציאלי לאיסוף המידע

247 ע"א 8954/11 פלוני נ' פלונית (נבו 20.4.2014).

248 גילוי דעת בנושא הסכמה, לעיל ה"ש 235, בעמ' 15-16.

אודותיו ושימוש בו, אלא אם המידע לא נמסר ישירות ממנו.²⁴⁹ 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 עליהם, השימוש שיעשה בו, מטרותיו וסוגי הגורמים שאליהם עשוי המידע להיות מועבר. המידע צריך להיות מוצג בבירור, ולהיות נגיש, פשוט ומובן. מאחר שעיבוד המידע הוא למטרות אפיון, עדיף שההסכמה תתקבל באמצעות פעולה אקטיבית מצד הבוחרים נושאי המידע (opt-in). כן נדרשים המפלגה ומפעיל יישומון הבחירות להוכיח שההסכמה ניתנת מרצונו החופשי של הבוחר נושא המידע, ושימוש בכלים עיצוביים ובטקטיקות אפלות שמטרתן להקשות על הבנת משמעות ההסכמה, למשל, טענה שהבוחר חייב לתת את הסכמתו לעיבוד המידע האישי באופן הפוגע בפרטיותו כדי לממש את זכותו לבחור, יפגע בתקפותה של ההסכמה ובהיותה הסכמה מרצון חופשי. כן מוצע למפלגה ולמפעיל יישומון בחירות להעדיף קבלת הסכמה מפורשת ולא מכללא, משום שבמקרים שבהם המידע האישי הנאסף משמש להסקת דעתו הפוליטית של הבוחר ולנקיטת תעמולת בחירות מותאמת מדובר בפגיעה חמורה בזכות הפרטיות. ככל שהפגיעה בזכות לפרטיות חמורה יותר פוחת הסיכוי שההסכמה מכללא תיחשב הסכמה תקפה. ולבסוף, לנוכח חומרת הפגיעה בפרטיות מוצע שהמפלגה ומפעיל יישומון הבחירות יעמידו לרשות הבוחרים נושאי המידע מנגנון לחזרה מההסכמה, על פי המלצת הרשות בנושא.

6.2. צמידות המטרה

עקרון צמידות המטרה הוא עקרון יסוד בדיני הגנת הפרטיות עוד לפני תיקון 13, והוא מחייב שעיבוד מידע ייעשה אך ורק למטרה שלשמה נאסף המידע. בסעיף 2(9) לחוק הגנת הפרטיות, עוד לפני התיקון, נקבע ששימוש בדיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסר, הוא

²⁴⁹ הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 6-7.

פגיעה בפרטיות שתותר רק בהסכמת נושא המידע.²⁵⁰ סעיף 11 מחייב לפרט את המטרה שלשמה מבוקש המידע בכל פנייה לקבלת מידע אישי.

סעיף 8(ב) לחוק הגנת הפרטיות, שתוקן בתיקון 13, הוא נדבך נוסף בעקרון צמידות המטרה. סעיף זה קובע כי "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין".²⁵¹ כלומר, עיבוד מידע חייב להיעשות על פי מטרת המאגר המפורטת במסמך מטרות המאגר, ומטרה זו צריכה להיות חוקית, מסוימת ומפורשת.²⁵² נעיר כי חוק הגנת הפרטיות אינו מבהיר על מי מוטלת החובה לפעול בהתאם לעקרון צמידות המטרה לפי סעיפים אלו – בעל שליטה, מחזיק או שניהם.²⁵³

לפי סעיפים אלו, 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 אך ורק למטרות שנקבעו. נוסף על כך, מטרות עיבוד המידע צריכות להיכלל הן במסמך מטרות המאגר, הן בכל פנייה לאדם לשם קבלת מידע אישי. על מפעיל יישומון בחירות להבטיח שעיבוד המידע שהוא מעבד הוא אך ורק למטרות שהגדירה המפלגה בהיותה בעל שליטה במסמך מטרות המאגר, בפנייה לאדם לשם קבלת מידע אישי ממנו, ובמטרות שלשמן נמסרה ידיעה על ענייניו הפרטיים של אדם.

בבחינת הפרת עקרון צמידות המטרה יש לתת את הדעת לכך שאין לעשות שימוש במידע אישי אם האדם שעליו נאסף המידע לא נתן הסכמה תקפה,

250 ס' 1, (9)2 ו-8(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

251 ס' 8(ב) לחוק הגנת הפרטיות, שם.

252 ס' 23(א) לחוק הגנת הפרטיות, שם.

253 לביקורת על כך ראו רחל ארידור הרשקוביץ **תיקון 13 לחוק הגנת הפרטיות: משמעות התיקון, השלכותיו וחטרונותיו** (הצעה לסדר 62, המכון הישראלי לדמוקרטיה 2026).

מדעת ומרצון חופשי, למטרת השימוש או לגורמים שלהם יועבר המידע.²⁵⁴ עיבוד מידע אישי בנסיבות כאמור עלול להביא להפרת עקרון צמידות המטרה. למשל, כאשר מידע על עמדתו הפוליטית של אדם מעודכן ביישומן בחירות על ידי בן משפחה או עמית לעבודה על בסיס שיחה שקיימו, בלי שמעדכן המידע ביקש את הסכמתו של האדם להזנת המידע הזה ביישומן בחירות, שכן סביר שהמידע נמסר בשיחה אישית, לא למטרה של עדכון ביישומן בחירות ולא לעיבוד מידע לשם יצירת אפיון (פרופיילינג) והתאמת מסרי תעמולה מותאמים אישית. משום כך, לא מתקיימים היסודות "מדעת", "מרצון חופשי" וההסכמה המפורשת הנדרשים כדי להכיר בתקפות ההסכמה.²⁵⁵ לעומת זאת, כאשר אדם מעדכן ביישומן בחירות ששכנו אינו תומך במפלגה מסוימת על סמך שלט תמיכה במפלגה אחרת שהציב השכן במרפסת ביתו הגלויה לרחוב ולציבור בכללותו, אפשר לומר שאין בכך פגיעה בעקרון צמידות המטרה, שכן אפשר להסיק על הסכמתו של השכן לשימוש במידע על עמדתו הפוליטית למטרות תעמולת בחירות. השכן יתקשה לטעון שהביע את עמדתו הפוליטית בפני שכנו בלבד ולא ציפה שייעשה בה שימוש למטרות אחרות, כגון עדכון מפלגה כלשהי בעמדותיו.

עקרון צמידות המטרה מופר גם כאשר אדם מעדכן ביישומן 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. משום שבהיעדר הבהרה ברורה שייעשה שימוש במידע האישי בכל מערכת בחירות עתידית, השימוש במידע במערכת הבחירות שאחרי מערכת הבחירות שבמהלכה התקבלה ההסכמה תקפה לעיבוד המידע, הוא שימוש למטרה אחרת מהמטרה שלשמה נתן הבוחר ההסכמה מדעת. יתרה מזו, נראה שלפי עמדת הרשות להגנת הפרטיות, בגילוי הדעת בנוגע להסכמה חלוף השנים אף מצדיק פנייה מחודשת לנושא המידע

254 ראו, למשל, קביעת הפרה ישראל ביתנו, לעיל ה"ש 84, ס' 10.3, בעמ' 9; קביעת הפרה הליכוד, שם, ס' 10.7 בעמ' 11.

255 ראו הדיון בטקסט הנלווה לה"ש 235-248 לעיל.

לשם בחינה אם הסכמתו לשימוש במידע האישי על אודותיו לצורכי תעמולת הבחירות עומדת בעינה.²⁵⁶

נוסף על כך, למפעיל יישומון בחירות חייבת להיות שליטה מלאה בשימושים הנעשים ביישומון, כדי לממש את עקרון צמידות המטרה. למשל, אם כל המעוניין יכול לשלוח מסרון למספר טלפון ולקבל בתגובה קישורית להתקנת היישומון, וכך לקבל גישה לכל המידע (מידע פנקס ושכבות מידע נוספות) ולחפש במאגר מידע על כל מי שנמצאים בו, ללא קשר למטרת המאגר שהתוותה המפלגה על פי המסגרת המותרת לה בחוק הבחירות, מדובר בהפרת עקרון צמידות המטרה. אין מדובר בחשש בעלמא, אלא באירועים שקרו במערכות בחירות קודמות.²⁵⁷

6.3. מידתיות עיבוד המידע

הדרישה שפגיעה בפרטיות תעמוד בדרישת המידתיות מקורה בעיגונה של הזכות לפרטיות כזכות יסוד חוקתית בחוק־יסוד: כבוד האדם וחירותו.²⁵⁸ משום כך, עיבוד מידע בידי גוף שחלים עליו עקרונות המשפט הציבורי חייב להיעשות בהתאם לדרישת המידתיות. כן נקבע בפסיקה שדרישת המידתיות חלה גם על פגיעה במסגרת יחסי עבודה.²⁵⁹

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, משום שחזקת תום הלב תחול רק אם הפגיעה נעשתה על פי עקרון המידתיות והנחיצות.

256 ראו הדיון בטקסט הנלווה לה"ש 248 לעיל.

257 שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 70–106.

258 ס' 7 לחוק־יסוד: כבוד האדם וחירותו.

259 בג"ץ 8298/22 הסניגוריה הציבורית נ' היועצת המשפטית לממשלה (נבו 31.8.2025).

בפועל, כדי לעמוד בדרישת המידתיות יש להוכיח התאמה בין סוג המידע המעובד והיקפו לאינטרס הציבורי שהוא מטרת העיבוד, ולהראות שעיבוד המידע האישי נחוץ להשגת המטרה, שהוא האמצעי שפגיעתו בזכות הפרטיות פחותה, ושבאיזון בין הפגיעה בזכות הפרטיות לבין התועלת מהשגת האינטרס הציבורי שבבסיס מטרת העיבוד האחרונה גוברת.²⁶⁰

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

אף שההכרעה בנושא תתקבל בכל מקרה לגופו,²⁶¹ לדעתנו עיבוד המידע האישי על ידי מפלגה, לנוכח סוג המידע – מידע בעל רגישות מיוחדת – והיקפו הרחב, הוא בעל מאפיינים ציבוריים מובהקים, שכן קמפיינים פוליטיים מבוססי נתונים ובינה מלאכותית מאפשרים איסוף, ניתוח והיסק של מידע על בוחרים בהיקפים ובנומק שלא היו אפשריים בעבר, וכן יצירה והפצה של מסרים פוליטיים מותאמים אישית בקנה מידה רחב. יכולות אלו מעוררות חשש הולך וגובר לפגיעה בפרטיות הבוחרים, להגדלת פערי הכוח בין מפלגות לאזרחים, ולפגיעה בזכות לבחור בחירה חופשית ואוטונומית, ועקב כך פגיעה בהגונות הבחירות, בחשאיות הבחירות ובטוהר הבחירות. לפיכך, לדעתנו, לשם מזעור סיכון כאמור יש לחייב את המפלגה לעבד מידע אישי על אודות בוחרים על פי עקרון המידתיות.

260 להרחבה ראו אהרון ברק, מידתיות במשפט: הפגיעה בזכות החוקתית הגבולותיה (נבו 2010); ולעניין המבחן האחרון למידתיות במובנה הצר, ע"א 8954/11 פלוני נ' פלונית (נבו 2014.4.24) ס' 118–136 לפסק דינו של השופט סולברג.

261 פרשת ערוץ 14, לעיל ה"ש 191, ס' 25, 27 לפסק דינה של השופט ברק ארז.

6.4. 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, שנוסח בתיקון 13, אוסר על בעל שליטה לעבד מידע אישי במאגר מידע, או להתיר לאחר לעשות כן בעבורו, אם המידע הכלול במאגר המידע "נוצר, התקבל, נצבר 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, ובהם עקרון צמידות המטרה; סעיף 11 המטיל חובה לתת הודעה בעת פנייה לאדם לשם קבלת מידע אישי ממנו; וסעיף 23 המאסר מסירת מידע אישי על ידי גוף ציבורי.²⁶²

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

(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.²⁶³

(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.²⁶⁴

262 ס' 1 ו-2 לחוק הגנת הפרטיות, לעיל ה"ש 9.

263 פרוטוקול 223, לעיל ה"ש 160, בעמ' 39-58; פרוטוקול 233, לעיל ה"ש 207, בעמ' 17-21.

264 פרוטוקול 223, לעיל ה"ש 160, בעמ' 39-41.

הוראה זו, וגם ההגנה הצמודה אליה, אינן מעניקות תשובה בהירה בדבר מעמדו של מידע שהגיע למאגר מידע באמצעות "גירוד" מידע אישי (data scraping) ממקורות גלויים – למשל אתרי אינטרנט או רשתות חברתיות. בנסיבות אלו אין גורם מזהה המוסר 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 מסוחר מידע המגרדים מידע הקיים ברשת האינטרנט לשם יצירת מסרים מותאמים אישית לצרכים מסחריים, ובמקרה הזה גם פוליטיים.

חוסר בהירות זה מתגבר הואיל ובדיונים בוועדת החוקה נקבע שהגנת "תקנת השוק" חלה גם כאשר נעשה 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, שהפגיעה היא קלת ערך.²⁶⁵

לעומת זאת, בטיטות הנחיית הרשות להגנת הפרטיות בנושא בינה מלאכותית עמדה הרשות על כך שכאשר מערכות מבוססות בינה מלאכותית מגרדות מידע – אפילו מידע שנושא המידע פרסם על עצמו ברשת חברתית, ובוודאי מידע הזמין ברשת האינטרנט – אי אפשר להסיק הסכמה מדעת לעיבוד המידע רק מעצם הימצאות המידע באופן זמין ופתוח ברשת האינטרנט (כלומר שהגישה אליו אינה מוגבלת רק למי שיש בידו סיסמה או לקבוצת חברים מסוימת). הרשות סברה כי אי אפשר להניח שלנושא המידע הייתה ציפייה סבירה שייעשה שימוש במידע עליו באמצעות מערכות בינה מלאכותית ושהוא היה מודע לסכנות הטמונות בהם. לכן הציעה הרשות לחייב בעלי שליטה המאפשרים שיתוף מידע אישי ברשת האינטרנט לנקוט אמצעים נאותים למניעת פעולות אסורות של

265 שם, בעמ' 56-58, ראו דבריו של ח"כ רוטמן בעמ' 57: "לקחת אותו מאחר. הוא מסר. בשנייה שהוא פרסם משהו בפומבי, בצורה שניתן לעשות עליו data scraping, הוא נמסר על ידי המחזיק בו לציבור. זה מה שהוא עשה. אז הוא נמסר, אתה אספת".

גירוד מידע.²⁶⁶ משמעות הנחייה זו היא שמידע שנאסף בדרך של גירוד מידע באינטרנט בלי לקבל את הסכמתו מדעת של נושא המידע, עשוי להיחשב שימוש במידע שלא למטרה לשמה נמסר, כלומר פגיעה בפרטיות לפי סעיף 2(9) לחוק הנעשית ללא הסכמה מדעת של נושא המידע. עיבוד מידע ממאגר מידע הכולל מידע שנאסף בדרך גירוד כזאת יהיה, לפיכך, הפרה של האיסור הקבוע בסעיף 8(ד) לחוק הגנת הפרטיות. אומנם, הנחיה זו זכתה לביקורת לא מעטה, ובזמן כתיבת המחקר הזה היא טרם פורסמה בגרסתה הסופית. קבלתה כלשונה משמעה ביטול ההכרה בהסכמה מכללא והחמרת דרישת ההסכמה שתהפוך 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. כל זאת לצד מתן סמכות עוצמתית לרשות להגנת הפרטיות, שלא הייתה בכוונת המחוקק לתת לה, ובלי בחינה מעמיקה של השלכותיה. ודוק, נושא גירוד המידע הוצג כמה פעמים בדיוני ועדת החוקה שעסקו בתיקון 13, ומעולם לא הוסכם שם על הפרשנות המוצגת בטיטות ההנחיה.²⁶⁷ בהנחיות שפרסמה הרשות לקראת הבחירות לכנסת ה-26 הבהירה הרשות כי "כל הוראות חוק הגנת הפרטיות חלות גם על איסוף ועיבוד של מידע אישי באמצעות מערכות בינה מלאכותית על ידי מפלגות או עבון במסגרת מערכת הבחירות, כולל מידע אישי שנוצר בדרך של היסק או הערכה", והפנתה להרחבה בנושא לטיטות הנחייתה בנוגע לבינה מלאכותית.²⁶⁸ עם זאת, היא הבהירה שכאשר נאסף מידע על מידת תמיכתו של אדם במפלגה לפי פרסומיו

266 ס' 6.3.4 ו-10 בטיטות הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית (28.4.2025). לביקורת על הנחיה זו, ראו רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר "טיטות הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית – חוות דעת" **אחר המכון הישראלי לדמוקרטיה** (3.8.2025).

267 פרוטוקול 233, לעיל ה"ש 207; פרוטוקול 298 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (26.3.2024); פרוטוקול 210, לעיל ה"ש 138. לביקורת על הנחיה זו ראו, למשל, ארידור הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 266.

268 הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 6.

הפומביים בפרופיל הפתוח שלו ברשת חברתית, ניתן להסיק על הסכמתו מכללא לעיבוד המידע על ידי המפלגה.²⁶⁹ הבהרה זו מרמזת דווקא שניתן להסיק הסכמה מכללא לגירוד כאמור של מידע מרשתות חברתיות באמצעות טכנולוגיות בינה מלאכותית.

עקב חוסר הבהירות באשר לתחולת האיסור הקבוע בסעיף 8(ד), האכיפה בגין הפרתו היא דו־שלבית. בשלב הראשון, אם ראש הרשות להגנת הפרטיות סבור שבעל השליטה במידע מפר את האיסור הזה, עליו לתת לו להשמיע את טענותיו, ולאחר מכן בסמכותו להודיע לו שעליו להפסיק את ההפרה.²⁷⁰ לבעל השליטה במאגר המידע אפשרות לערער על הוראת ראש הרשות לבית משפט השלום.²⁷¹

בשלב השני, אם בעל השליטה אינו מגיש ערעור או שערעורו נדחה, והוא אינו מקיים את הוראת ראש הרשות, בסמכות ראש הרשות להטיל עליו עיצום כספי.²⁷² קודם להטלת העיצום, על ראש הרשות למסור לבעל השליטה הודעה על כוונת חיוב, שלאחריה לבעל השליטה במאגר המידע האפשרות לטעון את טענותיו בפני ראש הרשות.²⁷³ גם לאחר הודעה על כוונת חיוב, או אמצעי אכיפה אחר, שמורה לבעל השליטה האפשרות להגיש ערעור לבית משפט השלום.²⁷⁴

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 אם **מידע שבמאגר המידע שבשליטתה נחשב מידע ש"נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה או להוראות כל דין אחר המסדיר**

269 ש.ס.

270 ס' 23(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9.

271 ס' 23(ו) לחוק הגנת הפרטיות, ש.ס.

272 ס' 23(ה)(1) (ג) לחוק הגנת הפרטיות, ש.ס.

273 ס' 23כז, 23כח לחוק הגנת הפרטיות, ש.ס.

274 ס' 23מה לחוק הגנת הפרטיות, ש.ס.

עיבוד מידע. הואיל ומפלגות מחזיקות בכמה סוגי מידע, נחלק אותם לכמה קבוצות:

(1) מידע פנקס ממערכת בחירות קודמת

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".²⁷⁵ "כתב ההתחייבות" שעל מפלגה או סיעה לחתום עליו כדי 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 ההתמודדות בבחירות הקרובות לכנסת ולצורכי קשר עם ציבור הבוחרים של הסיעה או המפלגה האמורה ולא לכל צורך אחר".²⁷⁶

הרשות להגנת הפרטיות הבהירה במסמכיה לקראת הבחירות לכנסת ה-24 וה-25 כי "אין לעשות שימוש בפנקסי עבר, פנקסים מהבחירות לרשויות המקומיות וכד'".²⁷⁷ הרשות חזרה על העמדה שמידע הפנקס הניתן למפלגה הוא **ביקדון זמני למערכת בחירות ספציפית** גם בקביעות ההפירה שפרסמה בפרשת **אלקטור**, ושם 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".²⁷⁸ גם בהנחייתה לקראת הבחירות

275 ס' 39(ג) לחוק הבחירות, לעיל ה"ש 75.

276 תקנה 6א(ג) לתקנות הבחירות לכנסת, תשל"ג-1973 (להלן: "תקנות הבחירות"), ס' א בנוסח כתב התחייבות שבחוספת לתקנות, בטופס 1.

277 דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24, לעיל ה"ש 124, בס' 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.

278 קביעת הפרה הליכוד, לעיל ה"ש 84, ס' 10.3, בעמ' 8.

לכנסת ה-26 חזרה הרשות והבהירה שיש לבער את כל עותקי פנקס הבוחרים הנמצאים אצל המפלגה ולוודא שכך נעשה גם אצל כל המחזיקים.²⁷⁹

ייתכן 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, בניגוד לעמדת הרשות בנושא. אולם, כך או כך, בכל הקשור לשימוש לצורכי התמודדות בבחירות כתב ההתחייבות שסעיף 39(ג) לחוק הבחירות מפנה אליו קובע במפורש שהשימוש מוגבל למערכת בחירות ספציפית.

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 הכולל את מידע הפנקס ממערכות בחירות קודמות, כולל למעשה מידע שנוצר בניגוד לחוק הבחירות, ולכן אסור לעבד אותו לפי סעיף 8(ד).

(2) מידע שנאסף במערכת בחירות קודמת

כאשר אדם מעדכן ביישומון הבחירות של מפלגתו כי הוא תומך במפלגה מסוימת, הוא עושה זאת מתוך ידיעה והבנה שמטרת עיבוד המידע על אודותיו הוא הצלחתה של המפלגה בבחירות הקרובות. לפיכך, שימוש שמפלגה עושה במידע כאמור במערכת הבחירות הבאה, בלי לקבל לשם כך את הסכמתו המפורשת, מדעת ומרצון חופשי של הבוחר,²⁸⁰ עשוי להפר את עקרון צמידות המטרה.

279 הרשות להגנת הפרטיות "הנחיות למפלגות לקראת הבחירות לכנסת ה-26", לעיל ה"ש 179, בעמ' 8.

280 ראו הדיון בטקסט הנלווה לה"ש 235-248 לעיל.

(3) מידע שנאסף ללא הסכמת נושא המידע או מבלי לתת לו הודעה

כפי שכבר הובהר לעיל, איסוף מידע אישי ישירות מאדם, במסגרת פנייה אליו, מחייב את בעל השליטה להודיע על כך לנושא המידע ולפרט בהודעה פרטים למיניהם, ובהם את 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 יישומי בחירות.** מהמידע שפורסם על יישומן הבחירות אלקטור²⁸¹ נלמד שלעיתים מידע אישי על אודות בוחר נאסף ללא ידיעתו, למשל מידע שמזין בן משפחה, שכן או חבר, שהתקין את היישומן במכשירו האישי. עדכון מידע בעל רגישות מיוחדת, כמו דעה פוליטית, או מידע אישי אחר המשמש להסקת דעתו הפוליטית של הבוחר ללא ידיעתו או ללא הסכמתו לעיבוד המידע על ידי מפעיל יישומן בחירות או מפלגה לצורכי תעמולת בחירות מותאמת אישית עשוי להיחשב פגיעה בעקרון צמידות המטרה, "בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת", שהן 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.²⁸² הרשות להגנת הפרטיות אף ציינה במכתבי קביעת ההפירה בפרשת **אלקטור** שאין לעשות שימוש במידע אישי אם האדם שעליו נאסף המידע לא הסכים לכך מדעת ומרצון חופשי, לאחר שהוסברו לו מטרות השימוש ולמי יימסר המידע.²⁸³ אולם, מהמידע שפורסם בציבור לא נמצא שמפלגות שעשו שימוש ביישומי בחירות או מפעילי יישומן בחירות ביקשו את הסכמתם של בעלי זכות בחירה, למשל, לתיוגם כתומכים במפלגה, מתנגדים לה או מתלבטים.²⁸⁴

281 ראו סמוחה, לעיל ה"ש 114.

282 ראו הדיון בטקסט הנלווה לה"ש 235-248 לעיל.

283 ראו, למשל, קביעת הפרה ישראל ביתנו, לעיל ה"ש 84, ס' 10.3, בעמ' 9; קביעת הפרה הליכוד, שם, ס' 10.7, בעמ' 11.

284 שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 70.

(ב) גירוד מידע מאתרי אינטרנט ומרשתות חברתיות. לנוכח עמדת הרשות במסמכי ההבהרה לקראת הבחירות לכנסות ה־23 וה־24, ובטיוטת הנחיות הרשות להגנת הפרטיות בנוגע לבינה מלאכותית, בהחלט ייתכן שגם פרקטיקה זו יתישב איסוף מידע אישי המחייב את קבלת הסכמתו התקפה של נושא המידע. אם איסוף המידע האישי הוא מאתר אינטרנט שאינו 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, יהיה אפשר לטעון שהמשתמשים לא נתנו את הסכמתם לגירוד המידע.²⁸⁵ עם זאת, לדעתנו, פרשנות שכזאת אינה רצויה, ונכון לכתובת שורות אלו אף אין הכרעה ברורה בעניין זה בחוק או בפסיקה.²⁸⁶ יתרה מזו, בהנחיות לקראת הבחירות לכנסת ה־26 ציינה הרשות שפרסום תמיכה מפורשת של אדם במפלגה מסוימת בפרופיל פתוח ברשת חברתיות הוא הסכמה מכללא לשימוש במידע זה על ידי מפלגה.²⁸⁷

לטעמנו, מפלגות לא יוכלו ליהנות מהגנת תקנת השוק בהקשרים שנידונו למעלה. מפלגה תתקשה לטעון שלא ידעה שעליה 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 להודיע לנושאי המידע על הכוונה לאסוף עליהם מידע אישי מאדם או לציית לעקרון צמידות המטרה. שכן הרשות להגנת הפרטיות הבהירה נושאים אלו במפורש בהנחיות שפרסמה בעת האחרונה לקראת הבחירות לכנסת ה־26,²⁸⁸ וכן לנוכח קביעת ההפרה של הרשות להגנת הפרטיות בעניין אלקטור שפורסמה בציבור.²⁸⁹ נוסף על כך, אשר להגנה המבוססת על קלות הערך שבפגיעה בפרטיות, נראה כי זה

285 ראו הדיון בטקסט הנלווה לה"ש 266–269 לעיל.

286 ראו הטקסט הנלווה לה"ש 267 לעיל.

287 הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה־26, לעיל ה"ש 179, בעמ' 6.

288 שם.

289 קביעת הפרה ישראל ביתנו, לעיל ה"ש 84; קביעת הפרה הליכוד, שם; קביעת הפרה אלקטור, שם.

אינו המצב בכל הקשור לעיבוד מידע אישי על ידי מפלגה, הנעשה בהיקפים נרחבים ביותר וביחס למידע אישי בעל רגישות מיוחדת.

6.5. איסור עיבוד מידע במאגר מידע ללא הרשאה

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

לא יעבד אדם מידע אישי ממאגר מידע ללא הרשאה מאת בעל השליטה במאגר המידע או בחריגה מהרשאה כאמור.²⁹⁰

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.²⁹¹ עם זאת, תיקון 13 לא סיפק פרשנות ברורה למהות ההרשאה הנדרשת.²⁹²

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

על מפעיל יישומון בחירות, בהיותו מחזיק של מאגר מידע שבשליטת מפלגה, לעבד את המידע במאגר המידע אך ורק במסגרת, בהיקף ובאופן שהתירה לו המפלגה.

290 ס' 8(ג) לחוק הגנת הפרטיות, לעיל ה"ש 9.

291 פרוטוקול 223, לעיל ה"ש 160.

292 ס' 29 ל-GDPR, לעיל ה"ש 5.

פרק 7

כבוד זכויות

נושא המידע

לפי חוק הגנת הפרטיות, לנושא המידע, כלומר לאדם שמידע אישי על אודותיו מועבד על ידי בעל שליטה או מחזיק, זכות לעיין במידע האישי על אודותיו ולבקש תיקון של המידע האישי או מחיקתו אם הוא אינו מדויק, שלם או נכון. כשפונים אליו לשם איסוף מידע, יש לו גם זכות לקבל הודעה על הכוונה לאסוף מידע אישי על אודותיו ועל מטרת איסוף ועיבוד המידע הזה,²⁹³

וכן זכות לקבל פרטי מידע מסוימים בצירוף להודעת דיוור ישיר, וכן לדרוש את מחיקת המידע האישי או להגביל את העברתו לצדדים שלישיים.²⁹⁴ תיקון 13 לא הרחיב מאוד את זכויות נושא המידע, למעט הרחבה מסוימת של זכות נושא המידע לקבל הודעה. כמו כן נוספו שני כלים חשובים לרשות נושא המידע – פיצויים לדוגמה וביטול מגבלת ההתיישנות. לכלים אלו עשויה להיות השפעה גם על מפלגה ועל מפעיל יישומון בחירות.

7.1. חובת הודעה לנושא המידע

חובת הודעה לנושא המידע קבועה בסעיף 11 לחוק הגנת הפרטיות, והיא חלה בנסיבות שבהן פונים לאדם כדי לאסוף מידע אישי על אודותיו לשם עיבודו במאגר מידע, בין שהמידע נאסף מכוח הסכמת נושא המידע בין מכוח סמכות בדיון. הרשות להגנת הפרטיות אף הבהירה שחובת היידוע תחול גם אם הפנייה לאדם לקבלת מידע אישי על אודותיו נעשית בעקבות פנייתו של האדם עצמו לקבלת שירות מסוים. לעומת זאת, חובת היידוע לא חלה על השימוש במידע או העברתו. כלומר, היא אינה מחייבת צדדים שלישיים שמידע אישי מועבר אליהם מתוקף הסכמת נושא המידע, או בעת העברת מידע בין גופים ציבוריים.²⁹⁵

²⁹³ ס' 13, 14 ו-11 לחוק הגנת הפרטיות, לעיל ה"ש 9.

²⁹⁴ ס' 17 לחוק הגנת הפרטיות, שם.

²⁹⁵ הרשות להגנת הפרטיות, חובת יידוע במסגרת איסוף ושימוש במידע אישי, נוסח מעודכן בעקבות תיקון 13 (18 ביולי 2022), בס' 4, 5, 25.

כלומר, אם המידע האישי על 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 יאסף בהסכמת נושאי המידע.²⁹⁶

אומנם, הרשות להגנת הפרטיות הבהירה בהנחייתה בנושא כי נדרש יידוע של נושא המידע כאשר המידע נאסף באמצעות מערכות קבלת החלטות המבוססות על בינה מלאכותית. כלומר, אם המידע נאסף באמצעות גירוד מידע מרשת האינטרנט, או באמצעות שאיבה של פרטים על אנשי קשר ממכשיר טלפון נייד של אדם שהתקין את יישומון הבחירות, באמצעות טכנולוגיית בינה מלאכותית – נדרשת הודעה.²⁹⁷ אולם, בהנחייתה לקראת הבחירות לכנסת ה-26 הרשות מבהירה שחוק הגנת הפרטיות חל גם על מידע המעובד באמצעות בינה מלאכותית, אך מציינת שהודעה לפי סעיף 11 לחוק הגנת הפרטיות נדרשת רק אם המידע נמסר על ידי האדם עצמו.²⁹⁸

אשר 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 על אודותיו, את פרטי הקשר של בעל השליטה במידע, וכן מידע על זכויותיו של נושא המידע לעיין במידע האישי על אודותיו ולבקש את תיקונו.²⁹⁹

אין בחוק הבחנה בין בעל השליטה במאגר המידע לבין המחזיק. אולם בהנחייתה לקראת הבחירות לכנסת ה-26 הבהירה הרשות כי המפלגה היא שנושאת

296 לעניין זה ראו גם את הטקסט הנלווה לה"ש 129 לעיל.

297 עם זאת, נושא חוקיות גירוד מידע מרשת האינטרנט באמצעות בינה מלאכותית אינו ברור לאשורו. ראו הדיון בטקסט הנלווה לה"ש 266-269 לעיל.

298 הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 6-7.

299 ס' 17 לחוק הגנת הפרטיות, לעיל ה"ש 9.

באחריות למתן הודעה לפי סעיף 300.11 לפיכך, על מפלגה או מפעיל יישומון בחירות הפונים לאדם לשם איסוף מידע אישי, להודיע לו הודעה שבה יצוין:

- אם 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 אם הוא יסרב למסור את המידע האישי על אודותיו. הרשות להגנת הפרטיות הבהירה דרישה זו באמצעות דוגמה. אם רשות מקומית מבקשת לספק לתושביה שירותים ציבוריים מקוונים, ולשם כך היא מבקשת מהם לספק לה מידע אישי, עליה להבהיר שאדם שאינו מעוניין למסור את המידע יוכל לקבל אותם פנים אל פנים במשרדי הרשות. כמו כן, אם סירוב למסור מידע עשוי להשפיע על זכויות נושא המידע, יש לפרט זאת.³⁰¹

- המטרה לשמה מבוקש המידע.

- שמה של המפלגה ודרכי ההתקשרות עימה.

- למי יימסר המידע ומטרות המסירה.

- זכויותיו של נושא המידע לעיין במידע המעובד על אודותיו ולדרוש את תיקונו על פי סעיפים 13 ו-14 לחוק הגנת הפרטיות.

7.2. הודעה בעת פנייה בדיוור ישיר

כל פנייה בדיוור ישיר חייבת לכלול ציון שמדובר בדיוור ישיר, ואת זהותו ומענו של בעל השליטה, פירוט המקורות שמהם קיבל בעל השליטה את המידע האישי,

300 הרשות להגנת הפרטיות, הנחיות למפלגות לקראת הבחירות לכנסת ה-26, לעיל ה"ש 179, בעמ' 6.

301 הרשות להגנת הפרטיות, חובת יידוע, לעיל ה"ש 285, ס' 14-15.

וכן הודעה על זכותו של מקבל הפנייה בדיוור ישיר להימחק מהמאגר, בצירוף המען שאליו יש לפנות כדי לממש את זכות המחיקה הזאת.³⁰²

מסרי תעמולה חישובית המותאמים אישית למאפייניו של בוחר או בוחרת עשויים להיחשב דיוור ישיר, כפי שקבעה גם הרשות להגנת הפרטיות.³⁰³ החובה אינה מוטלת במפורש על בעל שליטה או על מחזיק, ולפיכך הן מפלגה והן מפעיל יישומון בחירות חבים בה. כן עליהם לתת את הדעת לכך שההודעה צריכה לכלול גם את פירוט מקורות המידע.

7.3. 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 על אודותיו. כן הוא רשאי לדרוש מבעל השליטה במאגר מידע שבו נמצא המידע שעל פיו נעשתה פנייה בדיוור ישיר שלא למסור את המידע האישי עליו לאדם, לסוג בני אדם או לאנשים מסוימים, לפרק זמן מוגבל או קבוע. דרישות אלו צריכות להימסר בכתב ולבעל השליטה, ואין לו שיקול דעת אם להיענות להן. על בעל השליטה לפעול לפי הדרישה 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 על פי דרישתו.³⁰⁴

302 ס' 17(א) לחוק הגנת הפרטיות, לעיל ה"ש 9.

303 הנחיות הרשות לעניין שימוש במידע מפנקס הבוחרים, לעיל ה"ש 124, ס' 13-16; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת ה-24, שם, בס' 17.6. כן ראו הטקסט הנלווה לה"ש 188-189.

304 ס' 17(ב), (ג), (ד), (ה) לחוק הגנת הפרטיות, לעיל ה"ש 9.

זכות המחיקה חלה על בעל שליטה במאגר מידע המשמש לדיוור ישיר, והזכות להגביל את מסירת המידע חלה על בעל שליטה במאגר מידע שבו נמצא המידע שעל פיו נעשתה הפנייה בדיוור ישיר. בהנחה שתעמולה חישובית מותאמת אישית היא דיוור ישיר, הוראות אלו מחייבות מפלגה בהיותה בעלת שליטה במאגר המשמש לדיוור ישיר, או שבו נמצא המידע שלפיו נעשתה הפנייה בדיוור ישיר. על המפלגה להיענות לבקשת מחיקה או לבקשה להימנע ממסירת המידע האישי לצדדים שלישיים בהתאם לבקשה, למשל, אם בוחר מבקש למנוע העברת מידע על אודותיו לספק יישומון בחירות או לספק טכנולוגיה המשמשת להפצת מסרים מותאמים אישית.

7.4. פיצויים לדוגמה

סעד הפיצויים לדוגמה מתבסס על מודל דומה בחוק הגנת הצרכן,³⁰⁵ ומטרתו ליצור מנגנון הרתעתי ביחס להפרת הוראות החוק, שהוא חלופה למנגנון התביעות הייצוגיות ששימש בשנים האחרונות לעיתים להגשת תביעות סרק.³⁰⁶ התיקון קובע פיצויים מוסכמים בסכום מירבי של 10,000 ש"ח לטובת נושא המידע בגין הפרת החובות האלה על ידי בעל השליטה או מחזיק;³⁰⁷

• **חובת הודעה לנושא המידע.** מחזיק או בעל שליטה הפונים לאדם לקבלת מידע אישי לשם עיבודו בלי למסור הודעה כנדרש לפי בסעיף 11 לחוק הגנת הפרטיות,

³⁰⁵ פרוטוקול 310 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (8.4.2024), בעמ' 57, דברי יועמ"ש ועדת החוקה, עו"ד מנחמי; ס' 31 לחוק הגנת הצרכן, חשמ"א-1981; פרוטוקול 359 של ועדת החוקה, הכנסת ה-25 (30.6.2024), בעמ' 4-5.

³⁰⁶ פרוטוקול 320 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (16.5.2024), בעמ' 118, דברי יו"ר ועדת החוקה, ח"כ רוטמן; נטע סרוסי "אלפי תביעות נגד עסקים: הכירו את שיטת מצליח של עורכי הדין" **גלובס** (11.4.2024).

³⁰⁷ ס' 15א לחוק הגנת הפרטיות, לעיל ה"ש 9. להלן יפורטו רק סעיפי ההפרות הרלוונטיים למפלגה ו/או למפעיל יישומון בחירות.

בתנאי שנושא המידע פנה לבעל השליטה בדרישה לקבל הודעה כאמור ובקשתו לא נענתה בחלוף 30 ימים.³⁰⁸

• **זכות עיון.** בעל שליטה במאגר מידע שלא כיבד את זכות העיון של נושא המידע.³⁰⁹

• **זכות תיקון.** בעל שליטה במאגר מידע שהסכים לבקשת תיקון שהגיש נושא המידע, אך לא פעל לפיה, או לא הודיע על השינויים שיש לעשות בעקבותיה לכל מי שקיבל ממנו את המידע, במסגרת הזמן הקבועה בחוק הגנת הפרטיות.³¹⁰

• **הודעה בדבר סירוב לבקשת תיקון.** בעל שליטה במאגר מידע שסירב לבקשת תיקון, אך לא הודיע על כך לנושא המידע שביקש את התיקון במסגרת הזמנים הקבועה בחוק הגנת הפרטיות.³¹¹

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 בעניין אותן ההפרות.³¹²

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, להבדיל מפעולות חקירה ואכיפה מצד הרשות להגנת הפרטיות המוגבלות בקיומן ובהיקפן במהלך תקופת בחירות לפי פרק ד'5.³¹³

308 ס' 15א(א)(2) לחוק הגנת הפרטיות, שם.

309 ס' 15א(א)(3) לחוק הגנת הפרטיות, שם.

310 ס' 15א(א)(4) לחוק הגנת הפרטיות, שם.

311 ס' 15א(א)(5) לחוק הגנת הפרטיות, שם.

312 ס' 15א(ב) לחוק הגנת הפרטיות, שם.

313 ס' 23נח לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 317-334.

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

- מפלגה ו/או מפעיל יישומון בחירות שאספו מידע אישי באמצעות פנייה לאדם בלי למסור לו הודעה כנדרש לפי סעיף 11, ובלי להיענות לדרישתו לקבל הודעה כאמור בתוך 30 יום מדרישתו.

- מפלגה שלא כיבדה את זכותו של האדם לעיון במידע.

- מפלגה שהסכימה לבקשת תיקון שהגיש לה אדם שפרטיו נמצאים במאגר המידע שלה, אך לא תיקנה את התיקון, או לא הודיעה על כך לצדדים שלישיים שאליהם העבירה את המידע.

- מפלגה שסירבה לבקשת תיקון שהגיש לה אדם שפרטיו נמצאים במאגר המידע שלה, אך לא הודיעה על כך למבקש על פי הנדרש בחוק.

7.5. תקופת התיישנות

תקופת ההתיישנות של תביעה אזרחית בגין פגיעה בפרטיות הייתה לאורך שנים קצרה בהרבה מתקופת ההתיישנות הנהוגה ביחס לתביעות נזיקיות רגילות,³¹⁴ ועמדה על שנתיים בלבד.³¹⁵ בתיקון 13 הוחלט להשוות את תקופת ההתיישנות לשבע שנים, כמקובל בתביעות אזרחיות.³¹⁶

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

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

315 ס' 26 לחוק הגנת הפרטיות, לעיל ה"ש 9.

316 ס' 34 לתיקון 13, שם, המבטל את ס' 26 לחוק הגנת הפרטיות לפני תיקון 13.

פרק 8

פיקוח ואכיפה מצד הרשות להגנת הפרטיות, בשגרה 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 כן התקבל לכך אישור של יושב ראש ועדת הבחירות המרכזית, אך הגבלת סמכויות האכיפה

והפיקוח של הרשות בתקופת הבחירות אין פירושה 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.

8.1. 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,³¹⁷ ביחס למאגר מידע שמפלגה³¹⁸ היא בעלת השליטה בו.³¹⁹ הסדר זה מונע מראש הרשות, מפקח

³¹⁷ "תקופת בחירות לכנסת" היא "תקופה שתחילתה ביום הקובע, כהגדרתו בחוק מימון מפלגות, התשל"ג-1973, וסיומה ביום פרסום תוצאות הבחירות לפי ס' 11 לחוק-יסוד: הכנסת". ראו ס' 23 לחוק הגנת הפרטיות, לעיל ה"ש 9.

³¹⁸ "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 ס' 23 לחוק הגנת הפרטיות, שם.

³¹⁹ ההסדר חל גם במהלך תקופת בחירות לרשויות מקומיות, ביחס למאגר מידע שמועמד בבחירות לרשות המקומית הוא בעל השליטה בו. ס' 23 לחוק הגנת הפרטיות, שם.

או חוקר, להפעיל סמכויות מסוימות בתקופת בחירות כאשר מדובר בהפרות הנוגעות למאגר מידע שמפלגה היא בעלת השליטה בו, ושמפלגה או מחזיק מטעמה ביצעו. מועד ההפרה אינו משנה, וגם אם ההפרה שהמפלגה נחשדת בה אירעה לפני תחילת תקופת הבחירות, מרגע שהחלה תקופת הבחירות לא תוכל הרשות להפעיל את אחת מהסמכויות המפורטות להלן בלי אישור יו"ר ועדת הבחירות המרכזית.³²⁰

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, לשם ניגוח פוליטי של מפלגה מסוימת או מפלגות מסוימות.³²¹

נעיר כי אנו סבורות שמדובר בהסדר בעייתי, המעניק הגנה לזכות להיבחר, כלומר למפלגות ולפועלים מטעמן, אך אינו מגן מספיק על הבוחרים ועל זכותם לבחור בלי שיופעלו עליהם מניפולציות מבוססות מידע אישי. ההסדר אינו עוסק במקרים שבהם עלולה להיות פגיעה חמורה בזכות לפרטיות ונדרשת פעולה דחופה לשם עצירת הפגיעה בזמן אמת, וכך עלול להיווצר מצב שבו ההגנה על הזכות לפרטיות היא בבחינת "מעט מדי ומאוחר מדי", והשהיית הבירור והחקירה עלולה לפגוע ביכולת הרשות להגנת הפרטיות להפעיל כלי אכיפה בדיעבד. הגנת המפלגות באמצעות הסדר זה צורמת עוד לנוכח היעדר הכלים שיש בידי אזור ואזרחית מן השורה שמפלגה פוגעת בזכותם לפרטיות במהלך תקופת בחירות. אזרחים אינם יכולים 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.³²²

320 פרטוקול 313 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (16.4.2024), בעמ' 13.

321 שם, בעמ' 5-6, דברי יו"ר ועדת החוקה, ח"כ רוטמן; הצעת החוק הממשלתית, לעיל ה"ש 182, דברי ההסבר בעמ' 441.

322 חב"כ 13/23 בן מאיר ואח' נ' הליכוד ואח', ועדת הבחירות המרכזית לכנסת ה-23 (18.2.2020), וכן הדיון בטקסט הנלווה לה"ש 102-106 לעיל.

הסדר ראוי יותר – במקום הצורך לפנות ליו"ר ועדת הבחירות – היה, למשל, מאפשר למפלגה להגיש ערעור לבית משפט השלום על הוראת ראש הרשות להפסקת הפרה, לפי סעיף 2323 לחוק הגנת הפרטיות, וכך מרגע הגשת הערעור ועד החלטת בית המשפט לא תידרש המפלגה להפסיק את ההפרה.³²³

כך או כך, הסמכויות שהפעלתן בתקופת בחירות דורשת מראש הרשות לפרטיות לקבל לשם כך אישור מראש מיושב ראש ועדת הבחירות המרכזית הן:³²⁴

(1) סמכות להיכנס למקום למטרות פיקוח על יישום הוראות לפי פרקים ב', ד' ו-ה' בחוק, ופיקוח על יישום הוראות שראש הרשות מוסמך להורות על הפסקתן לפי סעיף 2323, 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 101, כיבוד זכות העיון, התיקון והמחיקה והגבלת העברת מידע אישי בהקשר של דיוור ישיר לפי סעיפים 13, 14 ו-117 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 מתוך הפרת הוראות מסוימות בתקנות אבטחת מידע, יישום הוראות הקשורות לדיוור ישיר, או הוראות הקשורות במינוי ממונה הגנת פרטיות.³²⁵

(2) סמכות לפנות לבית משפט בבקשה לצו חיפוש ותפיסה או צו חדירה לחומר מחשב אם יש לו יסוד סביר להניח שהייתה הפרה של הוראות סעיף 2323.³²⁶

(3) סמכות לפנות לבית משפט לעניינים מינהליים לתת צו להפסקת פעולות עיבוד מידע הגורמות, או שיש חשש שיגרמו, להפרת עקרון צמידות המטרה

323 ס' 2323(ו) לחוק הגנת הפרטיות, לעיל ה"ש 9. ראו גם פרוטוקול 313, לעיל ה"ש 320, בעמ' 13-15 דברי ד"ר ארידור הרשקוביץ, דברי עו"ד אור-חוף.

324 ס' 2323(ב) לחוק הגנת הפרטיות, שם.

325 ס' 2323(א)(1) לחוק הגנת הפרטיות, שם.

326 ס' 2323(א)(2) לחוק הגנת הפרטיות, שם.

בסעיף 2(9), האיסור לעבד מידע שלא למטרה שנקבעה לו בדין לפי סעיף 8(ב), האיסור לעבד מידע ללא הרשאה לפי סעיף 8(ג), האיסור לעבד מידע שנוצר בניגוד לחוק לפי סעיף 8(ד) או חובת אבטחת מידע לפי סעיף 17.³²⁷

(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), ומסירת פרטים לא נכונים בכוונה להטעות באשר למסירת המידע האישי במסגרת הודעה לנושא המידע לפי סעיף 11.³²⁸

(5) סמכות לבקש מבית משפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב ולבצעו, אם יש לחוקר יסוד סביר לחשד שנעברה עבירה של פגיעה במזיד בעקרון צמידות המטרה, עבירה על הוראות פרק ב' או עבירה לפי פרק ד' 4.³²⁹

(6) סמכות למסור הודעה על כוונה להטיל עיצום כספי אם יש לו יסוד סביר להניח שמקבל ההודעה הפר הוראה מההוראות המנויות בסעיף 23 כזו 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 על אודותיו לאנשים מסוימים לפי סעיף 17(ד), אי-מתן הודעה לנושא מידע לפי סעיף 11, פנייה בדיוור ישיר בלי לספק פרטים הנדרשים לפי סעיף 17(א), או עיבוד מידע ממאגר למטרה שאינה כדין או עיבוד מידע שלא למטרה שנקבעה לפי סעיף 8(ב).³³⁰

327 ס' 23נט(א)(3) לחוק הגנת הפרטיות, שם.

328 ס' 23נט(א)(4), 23נד, 23נו לחוק הגנת הפרטיות, שם.

329 317 ס' 23נט(א)(5) לחוק הגנת הפרטיות, שם.

330 ס' 23נט(א)(6) לחוק הגנת הפרטיות, שם.

(7) סמכות למסור לאדם התראה מינהלית אם יש לו יסוד סביר להניח כי אותו אדם הפר אחת מההוראות המנויות בסעיף 23כז לחוק הגנת הפרטיות והתקיימו הנסיבות שקבע שר המשפטים.³³¹

(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 מההוראות סעיף 23כז לחוק הגנת הפרטיות והתקיימו הנסיבות שקבע שר המשפטים.³³²

לפני מתן אישור, על יושב ראש ועדת הבחירות המרכזית לתת למפלגה הזדמנות להשמיע את טענותיה, אלא אם כן מדובר בהפעלת סמכות לפי סעיפים (1)–(5) לעיל, וטעמי הדחיפות מצדיקים קבלת החלטה בלי 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 את טעמי הדחיפות שהצדיקו שלא לתת למפלגה לטעון את טענותיה.³³³ יושב ראש ועדת הבחירות המרכזית רשאי להתנות בתנאים את האישור להפעלת אחת מהסמכויות האלה.

המבחן שבו על יושב ראש ועדת הבחירות המרכזית להשתמש בהחלטה בדבר מתן היתר להפעיל את סמכות האכיפה, הוא מבחן מידתיות. כלומר, יו"ר ועדת הבחירות צריך להשתכנע שהפעלת הסמכות לא תפגע פגיעה מהותית 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.³³⁴ להלן, נבהיר את הסמכויות המוגבלות בתקופת בחירות, ולאחר מכן נעסוק בסמכויות שאינן מוגבלות.

331 ס' 23נט(א)(7) לחוק הגנת הפרטיות, שם.

332 ס' 23נט(א)(8) לחוק הגנת הפרטיות, שם.

333 ס' 23נט(ג) לחוק הגנת הפרטיות, שם.

334 ס' 23נט(ד) לחוק הגנת הפרטיות, שם.

8.2. סמכויות הרשות להגנת הפרטיות המוגבלות

בתקופת בחירות

8.2.1. סמכויות פיקוח, אכיפה ובירור מינהלי

מפקח מטעם הרשות להגנת הפרטיות מוסמך לעשות כל אחת מהפעולות המפורטות בסעיף 23 לחוק, ובכללן כניסה למקום או דרישה מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך או עותק מחומר מחשב,³³⁵ לשם פיקוח על הוראות החוק לפי פרקים ב', ד' וה'. הוראות אלו כוללות, בין השאר, הוראות בדבר חובת אבטחת מידע,³³⁶ חובת מינוי ממונה הגנת פרטיות,³³⁷ חובת מתן הודעה לרשות להגנת הפרטיות בדבר קיומו של מאגר מידע,³³⁸ חובת מתן הודעה לאדם בעת פנייה אליו לשם קבלת מידע לעיבודו,³³⁹ חובת צירוף הודעה לפנייה בדיוור ישרי,³⁴⁰ איסור עיבוד שלא למטרה שנקבעה למאגר,³⁴¹ או כיבוד זכויות נושא המידע לעיון, לתיקון, למחיקה ולהגבלת העברת מידע אישי בהקשר של דיוור ישרי.³⁴²

כן מוסמך מפקח מטעם הרשות לעשות כל אחת מהפעולות המפורטות בסעיף 23 לחוק לשם פיקוח על יישום ההוראות שבגין הפרתן רשאי ראש הרשות

335 ס' 23 לחוק הגנת הפרטיות, שם.

336 ס' 17 לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 202-211 לעיל.

337 ס' 11 לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 212-234 לעיל.

338 ס' 8א(ב)(1), (3) לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 200-201 לעיל.

339 ס' 11 לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 295-301 לעיל.

340 ס' 17 לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 302-303 לעיל.

341 ס' 8(ב) לחוק הגנת הפרטיות, שם.

342 ס' 13, 13א, 14 ו-17 לחוק הגנת הפרטיות, שם.

להגנת הפרטיות להורות על הפסקת ההפרה,³⁴³ כגון עקרון צמידות המטרה,³⁴⁴ איסור עיבוד מידע ללא הרשאה מבעל השליטה,³⁴⁵ או איסור עיבוד מידע לשם פגיעה בפרטיות.³⁴⁶ כמו כן, בסמכותו של המפקח להחליט לפתוח בהליך בירור מינהלי אם יש לו יסוד סביר להניח שהייתה הפרה של אחת מהוראות אלו,³⁴⁷ או אחת מהוראות החוק שבגין הפרתה ניתן להטיל עיצום כספי.³⁴⁸ במסגרת בירור מינהלי ראשי מפקח לפנות לבית משפט בבקשה לקבל צו חיפוש ותפיסה או צו חדירה לחומר מחשב ולבצעו בהתאם להוראות בית המשפט.³⁴⁹ כמו כן, במקרים שבהם לראש הרשות יסוד סביר לחשד שאפשר אף לפתוח בחקירה פלילית בגין המעשה או המחלל הנחקרים, בסמכותו להחליט אם לקיים בירור מינהלי או חקירה פלילית.³⁵⁰

נוסף על כך, במקרה של חשד לפגיעה במזיד בעקרון צמידות המטרה לפי סעיף 2(9), או עבירה אחרת לפי חוק הגנת הפרטיות, ראשי החוקר לחקור כל אדם הקשור לעבירה, לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא קשור לעבירה, או לבקש מבית המשפט צו חיפוש ותפיסה.³⁵¹

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.³⁵²

343 ס' 23 לחוק הגנת הפרטיות, שם, והדיון בטקסט הנלווה לה"ש 374-377 לעיל.

344 ס' 2(9) ו-8(ב) לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 250-257 לעיל.

345 ס' 8(ג) לחוק הגנת הפרטיות לפני תיקון 13, ה"ש 1 לעיל, וכן הדיון בטקסט הנלווה לה"ש 290-292 לעיל.

346 ס' 2 לחוק הגנת הפרטיות, לעיל ה"ש 9.

347 ס' 23 לחוק הגנת הפרטיות, שם.

348 ס' 23 לחוק הגנת הפרטיות, שם.

349 ס' 23ד, 23ט לחוק הגנת הפרטיות, שם.

350 ס' 23טז לחוק הגנת הפרטיות, שם.

351 ס' 23נא(א) לחוק הגנת הפרטיות, שם.

352 ס' 23נט(א)(1), (2), (4), (5) לחוק הגנת הפרטיות, שם.

8.2.2. 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 שבהם יש לראש הרשות להגנת הפרטיות חשד סביר שיש או עלולה להיות הפרה חמורה ולהפסיק אותה מיד. המקרים האלה הם:

- הפרת איסור על שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה (סעיף 2(9)).³⁵³

- הפרת איסור על עיבוד מידע אישי במאגר מידע שלא למטרת המאגר שנקבעה לו כדין (סעיף 8(ב)).³⁵⁴

- 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)).³⁵⁵

- הפרת חובת אבטחת מידע (סעיף 17).

- מסירת מידע אישי מגוף ציבורי שלא בהסכמת נושא המידע או פרסומו שלא בסמכות כדין (סעיף 23ב).

במקרים האלה יוכל ראש הרשות לפנות לבית המשפט לעניינים מינהליים בבקשה לתת צו לבעל השליטה במאגר המידע או למחזיק להפסיק את פעולות

353 ראו הדיון בטקסט הנלווה לה"ש 250–257 לעיל, לעניין הפרה אפשרית של עקרון צמידות המטרה על ידי מפלגה או מפעיל יישומון בחירות.

354 ש.ס.

355 ש.ס.

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 קיצוני.³⁵⁶ בית המשפט יבחן גם את מידת הפגיעה האפשרית של הצו המבוקש בזכות לחופש הביטוי. כן ייתן בית המשפט למפלגה או למפעיל יישומון הבחירות הזדמנות להציג את טענותיהם. צו שניתן במעמד צד אחד בלי שמפלגה או מפעיל היישומון התגוננו, יעמוד על 48 שעות, ומכל מקום לא יינתן צו מחיקה במעמד צד אחד.³⁵⁷ אומנם, בתקופת בחירות לא יכול ראש הרשות להפעיל את סמכותו זו לבקשת צו הפסקה אלא באישור יו"ר ועדת הבחירות המרכזית,³⁵⁸ אך חשוב להבין שאם ישתכנע יו"ר ועדת הבחירות המרכזית שיש להפעיל סמכות זו, ובית המשפט ישתכנע שהחשד שהייתה הפרה הוא סביר, וכי הסעד הוא מידתי, הסעד של הפסקת עיבוד המידע, או של מחיקת המאגר במקרה קיצוני, משמעותו שיתוק מלא של כלל הפעולות הנשענות על עיבוד המידע שבמאגר.

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

סעיף 23כז, 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.³⁵⁹

356 פרוטוקול 347 של ועדת החוקה, חוק ומשפט, הכנסת ה-25 (18.6.2024), בעמ' 31-32; פרוטוקול 351, לעיל ה"ש 216, בעמ' 16-17.

357 שם, בעמ' 38, 42; פרוטוקול 351, לעיל ה"ש 216, בעמ' 17, דברי יו"ר ועדת החוקה, ח"כ רוטמן.

358 ס' 23נט(א)(3) לחוק הגנת הפרטיות, לעיל ה"ש 9.

359 ס' 23כז לחוק הגנת הפרטיות, שם. להלן יפורטו רק הפרות העשויות להיות רלוונטיות למפלגה בהיותה בעלת שליטה ו/או למפעיל יישומון בחירות בהיותו מחזיק.

הסעיף המופר בחק הגנת הפרטיות	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 על אודותיו האגור במאגר המידע.	15,000 ש"ח
14(ב)	בעל שליטה	תיקון מידע אישי בעקבות מימוש זכות התיקון על ידי נושא המידע, בלי 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 בלי למסור לו הודעה כנדרש.	50 ש"ח לכל אדם שפנו אליו או דרשו ממנו מידע, 100 ש"ח לכל אדם אם הפנייה או הדרישה היא בדבר מידע בעל רגישות מיוחדת; או 30,000 ש"ח בהוראות ראש הרשות

הסעיף המופר בחוק הגנת הפרטיות	על מי יוטל העיצום	ההפרה	סכום העיצום
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 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
17ב(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

הסעיף המופר בחוק הגנת הפרטיות	על מי יוטל העיצום	ההפרה	סכום העיצום
117(ב), (ד)	בעל שליטה ומחזיק	לא נענה לדרישתו של אדם שמידע עליו יימחק ממאגר המשמש לדיוור ישיר.	15,000 ש"ח
117(ג), (ד)	בעל שליטה	לא נענה לדרישתו של אדם שמידע אישי על אודותיו שעל פיו נעשתה פנייה בדיוור ישיר לא יימסר לאדם, לסוג בני אדם או לאנשים מסוימים.	15,000 ש"ח
117(א)	בעל שליטה ומחזיק	פנייה לאדם בדיוור ישיר בלי לציין בפניו שמדובר בדיוור ישיר, לספק את זהותו ומענו של בעל השליטה, לפרט את המקורות שמהם קיבל בעל השליטה את המידע שבמאגר ולספק לנמען הפניה מידע בדבר זכותו להימחק מהמאגר.	50 ש"ח לכל אדם שפנו אליו או דרשו ממנו מידע; 100 ש"ח לכל אדם אם הפנייה או הדרישה היא בדבר מידע בעל רגישות מיוחדת; או 30,000 ש"ח בהוראות ראש הרשות
23(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.

הסעיף המופר בחוק הגנת הפרטיות	על מי יוטל העיצום	ההפרה	סכום העיצום
23(א) כה	בעל שליטה ומחזיק	אי-מילוי הוראת ראש הרשות להפסקת הפרה עקב הפרת עקרון צמידות המטרה שבסעיף 2(9) לחוק הגנת הפרטיות, או בגין עיבוד מידע אישי למטרה שמהווה פגיעה בפרטיות לפי סעיף 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
23(ב) כה	בעל שליטה	אי-מילוי הוראת ראש הרשות להפסקת הפרה עקב הפרת האיסור על עיבוד, או הרשאה לאחר לעבד, מידע במאגר מידע שנוצר, התקבל, נצבר או נאסף בניגוד לחוק הקבוע בסעיף 8(ד) 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
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 בנסיונות שבהן היה ניתן לקבוע כדין מטרה כאמור.	לפי פרט 1 בתוספת השלישית לחוק הגנת הפרטיות לאחר תיקון 13

הסעיף המופר בחוק הגנת הפרטיות	על מי יוטל העיצום	ההפרה	סכום העיצום
23(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. אם המחזיק אינו מפסיק את ההפרה ובעל השליטה אינו עושה את שנדרש ממנו על ידי ראש הרשות לשם הפסקת ההפרה, יראו בו מפר.	לפי המפורט 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.	על פי המפורט בתוספת הרביעית לחוק הגנת הפרטיות.

במקום להטיל עיצום כספי, ראש הרשות רשאי למסור לבעל שליטה או למחזיק התראה מינהלית, אם יש לו יסוד סביר להניח כי הופרה הוראה מההוראות המפורטות בטבלה שלעיל.³⁶⁰ מפר המקבל התראה מינהלית רשאי לפנות לראש הרשות להגנת הפרטיות בבקשה לבטל את ההתראה.³⁶¹ עם זאת, המשך ההפרה

360 ס' 23לז לחוק הגנת הפרטיות, לעיל ה"ש 9.

361 ס' 23לז לחוק הגנת הפרטיות, שם.

לאחר קבלת התראה ייחשב הפרה נמשכת שתוביל להטלת עיצום כספי. כמו כן, הפרה של אותו הסעיף במהלך שנתיים לאחר קבלת ההתראה המינהלית תיחשב הפרה חוזרת, שגם בגינה ניתן להטיל עיצום כספי.³⁶²

אפיק חלופי נוסף לעיצום כספי הוא כתב התחייבות והפקדת עירבון, אם התקיימו הנסיבות המתאימות לפי קביעת שר המשפטים.³⁶³ בכתב ההתחייבות נדרש המפר להתחייב להפסיק להפר את הוראת החוק הרלוונטית, ולהימנע מהפרה נוספת של אותה ההוראה לתקופה שתיקבע 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. נוסף על כתב ההתחייבות על המפר להפקיד עירבון בסכום העיצום הכספי שראש הרשות היה רשאי להטיל עליו.³⁶⁴

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.³⁶⁵ כן יש להביא בחשבון את חובת ראש הרשות להגנת הפרטיות לפרסם את דבר הטלת עיצום כספי באתר האינטרנט של הרשות להגנת הפרטיות.³⁶⁶

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

362 ס' 23 לחוק הגנת הפרטיות, שם.

363 ס' 23 לטלחוק הגנת הפרטיות, שם.

364 ס' 23 לחוק הגנת הפרטיות, שם.

365 ס' 23 לחוק הגנת הפרטיות, שם.

366 ס' 23 לחוק הגנת הפרטיות, שם.

כתב התחייבות ולהפקיד עירבון.³⁶⁷ כלומר הרשות להגנת הפרטיות לא תוכל להטיל על מפלגה או מפעיל יישומון בחירות סנקציות מינהליות במהלך תקופת בחירות.

8.2.4. האפיק הפילי

פעולות מסוימות של הפרת החוק עשויות לעלות כדי עבירה פלילית. למשל, הפרעה לראש הרשות, לחוקר או למפקח במילוי תפקידו;³⁶⁸ 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;³⁶⁹ עיבוד מידע ללא הרשאה מבעל השליטה בניגוד לסעיף 8(ג);³⁷⁰ ופנייה לאדם לקבלת מידע אישי לשם עיבודו, מתוך מסירת פרטים לא נכונים, בכוונה להטעות את אותו אדם באשר למסירת המידע האישי.³⁷¹ אומנם הרשות להגנת הפרטיות עשתה שימוש מצומצם יחסית בסמכויותיה הפליליות עד כה,³⁷² אולם בהחלט ייתכן שראשי מפלגה או מפעילי יישומון בחירות יהיו נתונים לחקירה פלילית, ואף להגשת כתב אישום, אם ימצא חשד סביר לעבירות פליליות כאמור. עם זאת, סמכויות אלו מוגבלות בעת תקופת בחירות.³⁷³

367 ס' 23נט(א)(6)–(8) לחוק הגנת הפרטיות, שם.

368 ס' 23נג לחוק הגנת הפרטיות, שם.

369 ס' 23נד לחוק הגנת הפרטיות, שם.

370 ס' 23נה לחוק הגנת הפרטיות, שם.

371 ס' 23נו לחוק הגנת הפרטיות, שם.

372 בשנת 2023 קיבלה הרשות להגנת הפרטיות 34 פניות המעלות חשד לעבירה פלילית, נפתחו עשרה תיקי חקירה פלילית בגין חשד לעבירות של סחר או שימוש במידע רגיש בניגוד לחוק, נמשכה חקירתם של חמישה תיקי חקירה משנת 2022 ושלושה 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), בעמ' 20–21.

373 ס' 23נט(א)(4), (5) לחוק הגנת הפרטיות, לעיל ה"ש 9.

8.3. סמכויות הרשות להגנת הפרטיות שאינן מגבולות בתקופת בחירות

8.3.1. 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 האלה:

• עקרון צמידות המטרה בסעיף 2(9) לחוק: שימוש בדיעה על ענייני הפרטיות של אדם במאגר מידע שלא למטרה לשמה נמסר. למשל, כאשר מפלגה או מפעיל יישומון בחירות עושים שימוש במערכת בחירות עכשווית במידע מטיוב שבוחר עדכן על עצמו במערכת בחירות קודמת בלי לקבל את הסכמתו התקפה לכך.³⁷⁴

• עיבוד מידע אישי במאגר מידע למטרה שהיא 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.³⁷⁵

• עיבוד, או מתן הרשאה לאחר לעבד, מידע במאגר מידע שנוצר, התקבל, נצבר או נאסף בניגוד לחוק מתוך 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.³⁷⁶

• עיבוד מידע בניגוד להוראות תקנות אבטחת מידע המנויות בחלק ב' לתוספת הרביעית לחוק הגנת הפרטיות.

374 ראו הדין בטקסט הנלווה לה"ש 256 לעיל.

375 שם.

376 שם.

- 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 נחשבים הפרה. אופן הפסקת ההפרה ופרק הזמן שבמהלכו 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 את עצמם מנועים מלעשות פעולות המבוססות על עיבוד מידע במאגר מידע. למשל, כאשר מאגר המידע ביישומון הבחירות מבוסס על מידע הפוקס 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 קבלת הוראה אחרת מבית המשפט.

אם המפלגה או מפעיל היישומון ממשיכים בהפרה למרות הוראתו של ראש הרשות להפסיק אותה, ראש הרשות רשאי להטיל עליהם עיצום כספי. אולם סמכות זו מוגבלת בתקופת הבחירות.³⁷⁷

377 ס' 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. תעמולה חישובית, דהיינו 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 אלו עשויות לפגוע בפרטיות הבוחרים, ליצור פערי כוח ניכרים 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, יש חשש שהשימוש בטכנולוגיות האלה יתרחב בלי שתתקיים בקרה מספקת על השלכותיו על פרטיות הבוחרים ועל תקינות ההליך הדמוקרטי.

על רקע זה מוצעות להלן המלצות מדיניות שמטרתן להבהיר את גבולות השימוש במידע אישי במסגרת קמפיינים פוליטיים, ולחזק את יכולת האכיפה והפיקוח של הרשות להגנת הפרטיות ושל ועדת הבחירות המרכזית. בפרק 11 יוצג שאלון בחינה עצמית למפלגות ולמי שפועלים מטעמן כדי לספק להם כלים מעשיים לעמידה בדרישות הדין.

פרק 9

המלצות לרשות להגנת הפרטיות

כל עוד לא החלה "תקופת בחירות" לכנסת,³⁷⁸ 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, כדי לשפר את הגנת הפרטיות של בעלי זכות הבחירה, כמפורט להלן:

(א) הרשות תפתח בהליכי פיקוח ובירור מינהלי לשם בחינת ציות המפלגה לחובת ההודעה לרשות,³⁷⁹ ותטיל עיצום כספי, התראה מינהלית או כתב התחייבות על מפלגות שהפרו את חובת ההודעה לרשות.³⁸⁰

(ב) הרשות תפתח בהליכי פיקוח ובירור מינהלי כדי לבחון אם עיבוד מידע נעשה על פי הוראות תקנות אבטחת מידע,³⁸¹ ובמקרים מתאימים גם תפנה לבית משפט לעניינים מינהליים בבקשה להוצאה צו להפסקת עיבוד המידע,³⁸² תורה למפלגה בהיותה בעלת השליטה ולכל מחזיק מטעמה להפסיק את ההפרה במקרים המתאימים,³⁸³ תטיל עיצום כספי, תמסור התראה מינהלית או תדרוש חתימה על כתב התחייבות עקב הפרת הוראות תקנות אבטחת מידע.³⁸⁴

³⁷⁸ "תקופת בחירות לכנסת" היא ה"תקופה שתחילתה ביום הקובע, כהגדרתו בחוק מימון מפלגות, החשל"ג-1973, וסיומה ביום פרסום חוצאות הבחירות לפי ס' 11 לחוק-יסוד: הכנסת". ראו ס' 23נח לחוק הגנת הפרטיות, לעיל ה"ש 9.

³⁷⁹ ס' 23 לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 200-201 לעיל.

³⁸⁰ ס' 23כז, ו-23לז לחוק הגנת הפרטיות, שם.

³⁸¹ ס' 23זי לחוק הגנת הפרטיות, שם.

³⁸² ס' 23 מט לחוק הגנת הפרטיות, שם.

³⁸³ ס' 23כח לחוק הגנת הפרטיות, שם.

³⁸⁴ ס' 23כז, ו-23לז לחוק הגנת הפרטיות, שם.

(ג) הרשות תפתח בהליכי פיקוח ובירור מינהלי לבחינת מינוי ממונה הגנת פרטיות וציות לדרישות כשירותו ומילוי תפקידיו.³⁸⁵ הפרת החובה למנות ממונה הגנת פרטיות בארגון, או אי-עמידה בדרישות כשירות המינוי ובתנאים למילוי תפקידו, מקימים לרשות להגנת הפרטיות את הסמכות להורות למפלגה בהיותה בעלת השליטה ולכל מחזיק מטעמה להפסיק את ההפרה.³⁸⁶ כן מוסמך ראש הרשות להגנת הפרטיות להטיל על מפלגה או על מחזיק מטעמה עיצום כספי, למסור לה התראה מינהלית או לדרוש את חתימתה על כתב התחייבות והפקדת עירבון עקב הפרת הוראות תקנות אבטחת מידע.³⁸⁷

נוסף על סמכויות האכיפה אנו מציעות כי לנוכח החידושים שבתיקון 13 וטענות מפלגות בעבר שאכיפת חוק הגנת הפרטיות היא חדשנית והן לא הבינו את השלכותיה,³⁸⁸ נכון כבר עכשיו, בטרם החלה תקופת 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 האלה:

(א) דרישת ההסכמה מדעת

חוק הגנת הפרטיות מתנה כל פגיעה בפרטיותו של אדם בקבלת הסכמתו התקפה, שמשמעה הסכמה מדעת, מרצון חופשי, במפורש או מכללא.³⁸⁹ לטעמנו, יש לחדד בפני המפלגות את המשמעות המעשית של דרישת ההסכמה התקפה, ובכלל זה את הצורך להציג בפני האדם שממנו מתבקש המידע האישי

385 ס' 23 לחוק הגנת הפרטיות, שם, וכן הדיון בטקסט הנלווה לה"ש 212–234 לעיל.

386 ס' 23כה לחוק הגנת הפרטיות, שם.

387 ס' 23כו, 23לו ו-23לט לחוק הגנת הפרטיות, שם.

388 ראו, למשל, קביעת הפרה ישראל ביתנו, לעיל ה"ש 84, ס' 9.3 בעמ' 4. טענה דומה העלתה גם הליכוד. ראו קביעת הפרה הליכוד, שם, ס' 9.17, בעמ' 6.

389 להרחבה ראו הטקסט הנלווה לה"ש 235–248 לעיל.

את המידע הנחוץ לו לשם קבלת החלטה אם 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. כדי לקבל הסכמה תקפה יש לתת בידי האדם מידע על כלל סוגי המידע המבוקשים, מטרות השימוש בהם וזהות סוגי הגורמים שאליהם הוא יועבר. המידע צריך להיות ברור ונגיש, כדי שלאדם תהיה אפשרות סבירה להבין את משמעותה של הסכמתו למסירת המידע והשלכותיה.³⁹⁰

לנוכח רגישות המידע הנאסף ועיבודו למטרות דיוור יש להבהיר למפלגות שההסכמה צריכה להינתן באופן אקטיבי על ידי נושא המידע, ואין להסתפק בהסכמה פסיבית (opt-out). נוסף על כך, על המפלגות להבין ששימוש בכלים עיצוביים ובטקטיקות אפלות (dark patterns) שמטרתן להקשות על נושא המידע להבין את משמעות הסכמתו ולהשפיע השפעה פסולה על החלטתו, עלול לפגוע ברכיב הרצון החופשי, ומכאן בתקפותה של ההסכמה. יתרה מזו, חומרת הפגיעה בזכות לפרטיות עקב עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר וההשלכות האפשריות של עיבוד כאמור על הזכות לבחור מצדיקים דרישה שההסכמה תיעשה 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 את הסכמתו התקפה, מדעת ומרצון חופשי של נושא המידע לפני הזנת הנתונים ליישומון. אין די בהצגת מסר עם התקנת היישומון, שלפיו באחריות המשתמש לקבל את הסכמת הבוחר 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 על בוחר, תופיע חלונית שבה יתבקש המשתמש לאשר שקיבל את הסכמתו התקפה של הבוחר, ותפרט בקצרה את

390 גילוי דעת בנושא הסכמה, לעיל ה"ש 229.

דרישות ההסכמה התקפה ואת ההשלכות האפשריות על משתמש המאשר בלי לקבל הסכמה בפועל.

(ב) הקפדה על עקרון צמידות המטרה

מטרות המאגר שהמפלגה קובעת חייבות לעמוד במסגרת המטרות החוקיות הקבועה בסעיף 39(ג) לחוק הבחירות, כלומר "לצורכי התמודדות בבחירות ולצורכי קשר עם ציבור הבוחרים".³⁹¹ עקרון צמידות המטרה הוא עיקרון יסודי דיני הגנת הפרטיות, והוא מחייב שעיבוד מידע אישי במאגר המידע ייעשה אך ורק למטרה שלשמה נמסר המידע ולמטרת המאגר שנקבע כדין.³⁹² אולם, במערכת הבחירות לכנסת ה-23 פורסם ברבים אופן תקנת היישומון אלקטור, ששימש את מפלגת הליכוד, ונעשו מאמצים נרחבים להגדיל את בסיס משתמשיה. בעקבות זאת, כל אדם, פעיל במפלגה ואף אזרח זר, שאינו מתגורר כלל בישראל, היה יכול להתקין את היישומון ולחפש בו פרטים על כל אזרח ישראלי בעל זכות בחירה. אפשרות זו היא שהובילה גם לאזהרתו של ראש המוסד לשעבר, תמיר פרדו, שהשימוש ביישומון אלקטור עלול להביא לפגיעה חמורה בביטחון המדינה.³⁹³ נוסף על כך, אפשרותו של כל אחד להתקין את היישומון ולהשתמש בו לצרכיו מונעת מהמפלגה (בעלת השליטה במאגר) וממפעילי היישומון (המחזיקים בו),³⁹⁴ לעמוד בדרישת קיום המטרה.

391 ראו הדיון בטקסט הנלווה לה"ש 275–279 לעיל.

392 ס' 2(9) 8(ב) לחוק הגנת הפרטיות, לעיל ה"ש 9. כן ראו הדיון בטקסט הנלווה לה"ש 250–257 לעיל.

393 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).

394 מחלקת האכיפה, הרשות להגנת הפרטיות, קביעת הפרה של חוק הגנת הפרטיות, לעיל ה"ש 109.

משום כך, לדעתנו, יש לחזור ולהבהיר למפלגות את משמעות עקרון צמידות המטרה, ואת אחריות 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. כמו כן יש לנקוט צעדי אכיפה מהירים ומיידיים אם יתקבל מידע על שיווק דומה של יישומון לניהול בחירות במהלך מערכת הבחירות לכנסת ה-26.

(ג) דרישת אבטחת המידע

לדעתנו, יש לחדד בקרב המפלגות את משמעותן של דרישות תקנות אבטחת המידע. במסגרת זו חשוב להבהיר את הדרישה שיוענקו הרשאות גישה רק במידה הנדרשת לצורך מילוי תפקידו של מקבל ההרשאה,³⁹⁵ 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,³⁹⁶ אימות הזהות של מורשה הגישה צריך להיעשות ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. למשל, תעודה המכילה חתימה אלקטרונית מאובטחת.³⁹⁷ 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 להחיל גם

395 תקנה 8(א) לתקנות אבטחת מידע, לעיל ה"ש 138.

396 מאגר מידע שחלה עליו רמת האבטחה הבינונית הוא, למשל, מאגר מידע המכיל מידע בעל רגישות מיוחדת. מאגר מידע שחלה עליו רמת האבטחה הגבוהה הוא מאגר שחלה עליו רמת האבטחה הבינונית, אך יש בו מידע על 100,000 איש ומעלה או שמספר בעלי ההרשאה בו עולה על 100. ראו התוספות הראשונה והשנייה לתקנות אבטחת מידע, לעיל ה"ש 111.

397 תקנה 9 לתקנות אבטחת מידע, לעיל ה"ש 138. כן ראו הרשות להגנת הפרטיות, המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע).

על כל פעיל מפלגה או מתנדב המקבל הרשאת גישה לעשות שימוש ביישומון מטעם המפלגה או לטובתה.

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 בהיותה בעלת השליטה לדון בתוצאות הסקר ולפעול לתיקון הליקויים בו.³⁹⁸ במסגרת סקר סיכונים נבחנות נקודות התרופה בתשתית הטכנולוגית כדי למזער את הסיכון לזליגת מידע ולתקיפות סייבר העלולות לשבש את קמפיין הבחירות, ובתוך כך גם לפגוע בזכות לפרטיות של הבוחרים.

(ד) עיצוב לפרטיות

הביטוי "עיצוב לפרטיות" מבטא את התפיסה שבמערכות 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.

נציבי פרטיות ברחבי העולם אימצו את חובת העיצוב לפרטיות בעשור השני של המאה ה-21, בהיותה צעד יזום ומניעתי, ולא סעד שלאחר מעשה לאחר מחדל אבטחה או פגיעה בפרטיות. בשנת 2023 נכללה החובה בתקן בינלאומי להגנה על צרכנים.³⁹⁹ אומנם, החובה אינה מעוגנת בחוק הגנת הפרטיות בישראל, אולם הרשות להגנת הפרטיות ממליצה לבעלי שליטה ומחזיקים לאמצה ככלי חיוני במזעור סיכוני פרטיות ולשם בניית אמון.⁴⁰⁰

398 תקנה 5(ג) לתקנות אבטחת מידע, לעיל ה"ש 138.

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

400 הרשות להגנת הפרטיות "עיצוב לפרטיות (Privacy by Design)" (פורסם 4.8.2021, עדכון אחרון 10.7.2025).

הצעד הראשון בעיצוב לפרטיות הוא עריכת תסקיר השפעה על פרטיות (Privacy Impact Assessment), שבו יש לבחון בחינה מקיפה ושיטתית 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 על פי ממצאי התסקיר ומטרות העיבוד.⁴⁰¹

לדעתנו, יש להבהיר למפלגות את חשיבות העיצוב לפרטיות ויתרונותיו ולעודדן לאמצו, ולערוך תסקיר השפעה על הפרטיות כבר בתחילת קמפיין הבחירות, בעת התקשרות עם מחזיק, פיתוח יישומון בחירות או בחירת פלטפורמה להפצת מסרי תעמולה חישובית. מדובר בכלי שיתאים את טכנולוגיית עיבוד המידע למטרות העיבוד של המפלגה, ובכך יבטיח מזעור של הפגיעה בפרטיות במהלך קמפיין הבחירות, ויגביר את אמון הציבור במפלגות בכל הקשור לעיבוד מידע שהן עושות.

(ה) דיוור ישיר

יש להבהיר למפלגות שכל פנייה אישית לבוחר, בין פנייה של המפלגה עצמה, בין של גורם אחר מטעמה, המבוססת על השתייכותו לקבוצת אוכלוסין שנקבעה על פי אפיון אחד או יותר של בני האדם הכלולים במאגר, למשל, פנייה לבוחרים שנקבע שהם שייכים לקבוצת המתלבטים, היא דיוור ישיר לפי הגדרתו בחוק הגנת הפרטיות. לפיכך חלות על המפלגות החובות החלות בעת משלוח דיוור ישיר – החובה להודיע לנמען הפנייה שמדובר בדיוור ישיר, ובהודעה זו לציין את זהותו ומענו של בעל השליטה, ולפרט את המקורות שמהם קיבל בעל השליטה

⁴⁰¹ 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).

את המידע האישי, וכן להודיע לנמען על זכותו להימחק מהמאגר, בצירוף המען שאליו יש לפנות כדי לממש את הזכות הזאת.⁴⁰²

על המפלגות לכבד את זכותו של בוחר לבקש את מחיקתו ממאגר המידע המשמש לדיוור ישיר ולהגביל את העברת המידע האישי על אודותיו לצדדים שלישיים. במסגרת זו על המפלגות להבין שעליהן להחזיק במנגנון שיאפשר לבוחרים לממש את זכויותיהם אלו, וכן שאין להן שיקול דעת אם להיענות לבקשה. מרגע קבלת בקשה מבוחר להימחק ממאגר המידע או להגביל את העברת המידע על 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.⁴⁰³

(ו) כיבוד זכויות הבוחרים נושאי המידע

יש להבהיר למפלגה שעליה לכבד את זכויות הבוחרים נושאי המידע ליידוע בעת פנייה לאיסוף מידע אישי,⁴⁰⁴ לעיבוד המידע האישי עליהם רק בהסכמה תקפה שלהם,⁴⁰⁵ לדרוש עיון במידע על אודותיהם ולבקש את תיקונו,⁴⁰⁶ נוסף על הזכויות העומדות להם בדיוור ישיר.⁴⁰⁷ במסגרת זו יש להבהיר למפלגה מהן הפעולות שעליה לנקוט לשם כיבוד זכויות אלו, וכן שעליה לוודא שגם מפעיל יישומון בחירות יכבד את הזכויות האלה של נושא המידע.⁴⁰⁸ כן על מפלגה לתת

402 ס' 17(א) לחוק הגנת הפרטיות, לעיל ה"ש 9.

403 ס' 17(ב)-(ה) לחוק הגנת הפרטיות, שם.

404 ראו הדיון בטקסט הנלווה לה"ש 296-301 לעיל.

405 ראו הדיון בטקסט הנלווה לה"ש 235-248 לעיל.

406 ס' 13, 14 לחוק הגנת הפרטיות, לעיל ה"ש 9.

407 ראו הטקסט הנלווה לה"ש 302-304 לעיל.

408 ס' 13א, 14(ד) לחוק הגנת הפרטיות, לעיל ה"ש 9.

את הדעת לזכותו של בוחר נושא מידע שזכויותיו לא כובדו לפנות לבית משפט בבקשה לפיצויים לדוגמה ולהשפעת ביטול המגבלה על תקופת ההתיישנות על זכויות אלו.⁴⁰⁹

(ז) הבהרות בנושאים שאין בהם הכרעה: החובות החלות על מפלגה בהיותה גוף 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. לכן על הרשות לבחון ולהבהיר מהן החובות שעל מפלגה לציית להן לפי חוק הגנת הפרטיות מכורח היותה גוף דו־מהותי המבצע פעולות בעלות מאפיינים ציבוריים מובהקים. למשל, האם חלות על מפלגה חובת רישום והחובה למנות ממונה הגנת פרטיות ומידתיות בעיבוד המידע האישי מטעם זה?

נוסף על כך, יש מחלוקת ציבורית בנוגע לדין המחייב בנושא 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. 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 אם התקבלה הסכמה כאמור? האם מאגרי המידע שנוצרו בעבר על בסיס גירוד מידע אינם חוקיים? על הרשות לתת את דעתה בנושא בהנחיותיה, בשים לב למגבלות חוק הגנת הפרטיות הקיים, וכן להשלכות קביעותיה לא רק על המרחב הפוליטי אלא גם על המרחב העסקי הפרטי.

409 ס' 15א לחוק הגנת הפרטיות, שם, וכן הטקסט הנלווה לה"ש 305–316 לעיל.

פרק 10

המלצות ליו"ר ועדת הבחירות המרכזית

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

סוגיות הקשורות בתעמולה חישובית, לרבות עיבוד מידע אישי באמצעות בינה מלאכותית לצורכי תעמולת בחירות, הפצת מסרי תעמולת בחירות מותאמים אישית ושימוש ביישומוני בחירות, יהיו ללא ספק "תפוח האדמה הלוהט" בבחירות לכנסת ה-26. סוגיות אלו נשענות בעיקר על ההכרה בזכות לפרטיות כזכות חוקתית, וכן על עקרון חשאיות הבחירות, שנועד לשרת הן את האינטרס הפרטי של המצביעים לשמור על סודיות הצבעתם (שהוא אינטרס שאפשר לוותר עליו בהסכמה), הן את האינטרס הציבורי למנוע השפעה פסולה ולשמור על טוהר הבחירות.⁴¹⁰ לעומת הזכות לפרטיות ניצבת הזכות החוקתית להיבחר, שמכוחה יכולות מפלגות לעשות פעולות שונות למטרת הצלחה בבחירות.

סעיף 17 לחוק דרכי תעמולה מסמיק את יו"ר ועדת הבחירות להוציא צווי מניעה כדי למנוע עבירה על הוראות החוק, וכן על הוראות פרק י"א לחוק הבחירות לכנסת. רוב העתירות המוגשות ליו"ר ועדת הבחירות הן להוצאת צווי מניעה (תב"כ), ורוב החלטותיו בשנים האחרונות קשורות לעבירות על חוק דרכי תעמולה.⁴¹¹ בפרשת **שרלי הבדו** הגביל בית המשפט העליון במפורש את

410 בר"ס 3235/90 עמאש נ' מנהל הבחירות למועצה המקומית ג'סר אלזרקא (נבו) 1.3.2011.

411 להרחבה ראו דנה בלאנדר ועדת הבחירות המרכזית - מקצועית או פוליטית? 101-108 (מחקר מדיניות 175, המכון הישראלי לדמוקרטיה 2022).

סמכות יו"ר ועדת הבחירות המרכזית להוציא צווי מניעה, רק לעבירות על אחד מהחוקים המנויים בסעיף 17 לחוק דרכי תעמולה.⁴¹² חוקים אלו הם חוק התעמולה עצמו, וכן לעבירות המנויות בפרק י"א לחוק הבחירות לכנסת.

ברוח זו, במערכות הבחירות הקודמות בחרה ועדת הבחירות המרכזית למשוך את ידה מהסוגיות הנוגעות לשימושים במידע אישי ולהגנת 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 לנוכח 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 17 לחוק דרכי תעמולה. החלטתו אושרה גם על ידי בית המשפט העליון, שהביע אף הוא חוסר נוחות לנוכח הפגיעה האפשרית בזכות לפרטיות, אך החזיק בעמדה שלפיה אין בסמכותה של ועדת הבחירות המרכזית להכריע בנושא.⁴¹³

בפועל, חוסר ההכרעה מצד ועדת הבחירות המרכזית כמוהו כהכרעה. עיבוד מידע אישי לצורכי תעמולה חישובית באמצעות בינה מלאכותית ויישומי בחירות ימשיך ויגבר. בהקשר הזה נציע שתי דרכים. הדרך האחת היא לטעון כי תיקון 13 יצר סמכות משלימה עבור יו"ר ועדת הבחירות לדון בענייני פרטיות ובחירות. הדרך השנייה היא להרחיב את תחולת הפרשנות של סעיפים בפרק י"א לחוק הבחירות ולהתאימם לעידן הזה.

⁴¹² שוורץ אלטשולר ולוריא, לעיל ה"ש 1, בעמ' 76-79.

⁴¹³ 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 101-106 לעיל.

(ב) סמכות יו"ר ועדת הבחירות לנוכח 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 מהתיקון הוענקה ליו"ר ועדת הבחירות המרכזית סמכות להכריע אם 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.⁴¹⁴

במובן זה, בעת חקיקת ההסדר המיוחד להגבלת סמכויותיה של הרשות להגנת הפרטיות בתקופת בחירות,⁴¹⁵ הכיר המחוקק בסמכותו של יו"ר ועדת הבחירות המרכזית לעסוק בנושאים הקשורים בהגנה על הזכות לפרטיות. כן קבע המחוקק שיו"ר הוועדה הוא הגורם שביכולתו לגשר בין הזכות להיבחר, לרבות זכויותיה של מפלגה להתמודד בבחירות וליצור קשר עם הבוחרים לפי חוק דרכי תעמולה וחוק הבחירות, לבין זכות הבוחרים לפרטיות. לטעמנו ההסדר בתיקון 13 צריך להיות מתורגם להבנה שליו"ר ועדת הבחירות יש סמכות לדון בנושאים הקשורים בהגנת הפרטיות בתקופת הבחירות בנסיבות שבהן נדרשת הכרעה מהירה בתקופת הבחירות, וכאשר יש חשש שהמתנה להליך פיקוח ואכיפה מצד הרשות להגנת הפרטיות תוביל לפגיעה ניכרת בהיקפה ובחומרתה בזכות הבוחרים לפרטיות, שלא יהיה אפשר למנוע, למזער או לתקן בדיעבד. לכן מדובר בהסדר חדש, שניתן לקרוא אותו אל תוך סעיף 17 לחוק התעמולה.

נציין שעמדתנו זו הובעה גם בדיונים 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

414 ראו ס' 23נט(ד) לחוק הגנת הפרטיות, לעיל ה"ש 9.

415 ס' 23נח-23נט לחוק הגנת הפרטיות, שם.

של הרשות להגנת הפרטיות ולא בסמכויות של ועדת הבחירות. לכן אין לראות בכך הסדר שלילי ביחס לוועדת הבחירות.⁴¹⁶

סמכות ראש הרשות להגנת הפרטיות להוציא צו להפסקת עיבוד,⁴¹⁷ שהוספה בתיקון 13, אינה עומדת בסתירה להכרה בסמכותו של יו"ר ועדת הבחירות המרכזית לדון בנושאים הקשורים בחוק הגנת הפרטיות. סמכותו של ראש הרשות להגנת הפרטיות להוציא צו להפסקת עיבוד מידע אישי במאגר מידע אם יש לו חשד סביר שמבוצעת או עלולה להתבצע הפרה חמורה,⁴¹⁸ אינה מוגבלת בתקופת בחירות. המדובר בסמכות חשובה הנוגעת מענה מסוים לחששות העולים מעיבוד מידע אישי לצורכי תעמולת בחירות חישובית, באמצעות טכנולוגיות מבוססות בינה מלאכותית ויישומוני בחירות. במסגרת סמכות זו ראשי ראש הרשות להגנת הפרטיות להורות על הפסקה מיידית של עיבוד מידע אישי אם יש לו חשד סביר שמבוצעת או עלולה להתבצע הפרה חמורה של הוראות למיניהן, כגון עקרון צמידות המטרה, עיבוד בחריגה מהרשאה, הפרת חובת אבטחת המידע או הפרת האיסור על עיבוד מידע שנוצר, התקבל או נצבר בניגוד לדין.⁴¹⁹ אולם, כפי שטענו במהלך המחקר, לנוכח החשש שהוזכר גם בדיונים בוועדת החוקה בנוגע לתיקון 420¹³ מפני חולשתה של הרשות להגנת הפרטיות למול גורמי ממשל וגורמים מהמגזר הציבורי כיוון שעצמאותה מוסדרת רק בהחלטת ממשלה המופיעה בתוספת לחוק הגנת הפרטיות – אין די בסמכות הזאת.⁴²¹

בעידן הנוכחי יש חלון זמנים קצר ומצומצם ביותר למניעת פגיעה בפרטיות, שכן מרגע שניתנת הרשאת גישה למידע אישי לגורמים שונים או שמתגלה

416 פרוטוקול 313, לעיל ה"ש 320, בעמ' 4-8.

417 ס' 23 מט לחוק הגנת הפרטיות, לעיל ה"ש 9.

418 שם, וכן ראו הדיון בטקסט הנלווה לה"ש 353-358 לעיל.

419 ס' 23 מט לחוק הגנת הפרטיות, לעיל ה"ש 9, וכן ראו הדיון בטקסט הנלווה לה"ש 358-353 לעיל.

420 ראו, למשל, פרוטוקול 223, לעיל ה"ש 160, בעמ' 116.

421 החלטת ממשלה מס' 1890 עצמאות הרשות להגנת הפרטיות ותיקון החלטת ממשלה (2.10.2022); וכן החוספת הראשונה לחוק הגנת הפרטיות, לעיל ה"ש 9.

פרצת אבטחה, המידע עלול לזלוג בתוך זמן קצר, ואחר כך קשה מאוד לאתר את המידע ולמנוע שימוש בו בידי גורמים בלתי מוסמכים. יתרה מזו, ראש הרשות ממוקד בשיקולי פרטיות, ואילו ליו"ר ועדת הבחירות המרכזית ראייה רחבה יותר וסמכות לשקול את הפגיעה בזכות להיבחר לצד פגיעה אפשרית בזכות לבחור ובהגנות הבחירות, כפי שעולה למעשה מן ההסדרים שבתיקון 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 בסעיפים שבהם ניתן לתת צווי מניעה מכוח סעיף 17 לחוק התעמולה, פרשנות המתאימה למציאות הנוכחית.

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

סעיף 118 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". סעיף זה ממוקד בהפרה של עקרון צמידות המטרה מחוק הגנת הפרטיות,⁴²² וקובע שמדובר בעבירה פלילית. קביעה זו מתווספת להוראת סעיף 5 לחוק הגנת הפרטיות, שלפיה פגיעה במזיד בפרטיות לפי סעיף 2(9), כלומר הפרת עקרון צמידות המטרה עקב שימוש בידעה על ענייניו הפרטיים של אדם שלא למטרה לשמה הוא נמסר, היא עבירה שדינה מאסר חמש שנים.

עם זאת, סעיף 118א לחוק הבחירות נבדל מסעיף 5 לחוק הגנת הפרטיות מכמה בחינות, כמפורט להלן.

סעיף 118א לחוק הבחירות	סעיפים 5 ו-9 לחוק הגנת הפרטיות	
תחולה	רק מידע הפנקס.	ידיעה על ענייניו הפרטיים של אדם. כלומר כולל גם מידע הפנקס וגם מידע מטיוב.
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 ההבדלים האלה היא ששימוש במידע הפנקס שלא למטרה לשמה נמסר היא עבירה שהעונש בגינה קל יותר מהעונש בגין הפרה בזדון של עקרון צמידות המטרה ביחס למידע מטיוב או מידע הפנקס. כפי שפורט לעיל, חקירת העבירה החמורה יותר מחייבת את אישור יו"ר ועדת הבחירות המרכזית. אולם, דווקא בתקופת בחירות חקירת העבירה הקלה יותר אפשרית ואינה דורשת אישורים נוספים, אלא אם כן 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,⁴²³ שגם בגינה מוסמך יו"ר ועדת הבחירות להוציא צו מניעה לפי סעיף 17 לחוק תעמולה, שכן היא נופלת בגדר סעיף 126(6) לחוק הבחירות – "המפר הוראה מהוראות חוק זה שלא נזכרה בפרק זה".

עם זאת, בהקשר זה אנו מציעות להחיל את העבירה לפי סעיף 118א הן על מידע פנקס, הן על מידע מטויב, זאת מתוך ההבנה שהבחנה בין סוגי המידעים ויצירת משטר משפטי אחר 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 לנוכח הקושי המעשי והנטל הכלכלי והבירוקרטי שבהחלת משטרי פרטיות שונים זה מזה על שני סוגי מידע הנמצאים שניהם באותו מאגר מידע – מידע שהגיע מהאזור הכלכלי האירופי ומידע שהגיע מישראל – יש להחיל את הוראות התקנות על כל מידע המצוי במאגר מידע שיש בו מידע שהתקבל מהאזור הכלכלי האירופי.⁴²⁴ אכן, כאן מדובר בעבירות שהתנאים לתחולתם שונים ולא בשני משטרים משפטיים שונים, אך יש להביא בחשבון את הטענה שהפרדה בין סוגי מידע במאגר אחד קשה ליישום.

(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 העשויים לדכא הצבעה ולדכא בוחרים מלצאת ולהצביע, ראוי לדעתנו שוועדת הבחירות המרכזית תבדוק כי מניעת הצבעה איננה רק חסימה פיזית של הגישה לקלפי, אלא גם מניעה

⁴²³ להרחבה ראו הטקסט הנלווה לה"ש 276–279 לעיל.

⁴²⁴ תקנה 2(א) לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), תשפ"ג–2023; פרוטוקול 66 של ועדת החוקה, חוק ומשפט, הכנסת ה־25 (23.4.2023), בעמ' 20–27.

המבוססת על פעולות דיגיטליות מותאמות אישית לבוחר העלולות לגרום לאדם סביר להימנע מלהצביע. למשל, מסרים של שכנוע או מניפולציה, כמו מסר המבוסס על מידע אישי בנוגע למיקומו של המצביע ("אנחנו יודעים שאתה בדרך, אבל התור בקלפי שלך ארוך, לא להתקרב!"); או למצב בריאותו ("אנחנו יודעים שאת בקבוצת סיכון, ובקלפי יש אדם חולה מאוד שמשתעל כל הזמן").

(3) סעיף 122(6) לחוק הבחירות

סעיף 122(6) לחוק הבחירות קובע ש"המשדל אדם להצביע או להימנע מלהצביע, בכלל או בעד רשימת מועמדים מסוימת, 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 על הבוחרים באופן המפר את הוראות חוק הגנת הפרטיות. בתקופה הנוכחית מניפולציה רגשית המבוססת 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 פגיעה של ממש 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,⁴²⁵ את תחולתה ואת אופן יישומה המעשי על תעמולת בחירות המופצת על ידן באמצעות יישומון בחירות, או מותאמת אישית לבוחרים ומופצת בפלטפורמות דיגיטליות למיניהן, כגון הודעות SMS אישיות, מסרים בפלטפורמות הזרמת מידע (סטרימינג) או בהסכתים (פודקסט).

425 ס' 1א2 לחוק הבחירות (דרכי תעמולה), החשי"ט-1959.

פרק 11

שאלון בחינה עצמית למפלגות ולמי שפועלים מטעמן, לעמידה בדרישות חוק הגנת הפרטיות בעיבוד מידע על בוחרים

שאלון זה נועד לשמש כלי בחינה עצמית למפלגות ולמנהלי קמפיינים פוליטיים מטעמן, בהשראת תסקיר השפעה על פרטיות המקובל בדיני הגנת המידע בעולם. מטרתו של השאלון היא לסייע בזיהוי מוקדם של סיכונים פרטיות הנובעים משימוש במידע אישי ובכלים טכנולוגיים וחשובים מתקדמים במסגרת תעמולת בחירות, וכן לספק מסגרת בסיסית לבחינת עמידה בדרישות דיני הגנת הפרטיות.

שלב ראשון: מיפוי המידע וחוקיות השימוש בו

1. מידע או נתון

האם המידע בהם מותמם או שמדובר במידע מזוהה או ניתן לזיהוי ולכן הוא "מידע אישי"? ⁴²⁶

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, ⁴²⁶

- האם הבוחרים מקבלים הודעה כנדרש לפי סעיף 11 לחוק, הכוללת הסבר אם חלה עליהם חובה חוקית למסור את המידע והשלכות הסירוב למסור אותו, מטרת השימוש במידע, שמה של המפלגה ודרכי ההתקשרות עימה, הגורמים שלהם יימסר המידע, וזכויותיהם בדבר המידע שהם מוסרים?

⁴²⁶ עם זאת, נושא חוקיות גירוד מידע מרשת האינטרנט באמצעות בינה מלאכותית אינו ברור לאשורו. ראו הדיון בטקסט הנלווה לה"ש 266-269 לעיל.

- 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 אם להסכים או לסרב לעיבוד המידע האישי על אודותיהם?

- האם היישומון כולל מידע לבוחרים בדבר סוגי המידע הנאספים על אודותיהם, השימוש שיעשה בהם, המטרות וסוגי הגורמים שאליהם 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 על אודותיו במפורש?

- האם המפלגה ו/או מפעיל יישומון הבחירות מחזיקים במנגנון לחזרה מהסכמה?

אם מקור המידע הוא צדדים שלישיים המזינים את המידע באמצעות יישומון בחירות או טכנולוגיה אחרת:

- האם הצדדים השלישיים סיפקו לבוחרים הודעה הכוללת הסבר אם חלה עליהם חובה חוקית למסור את המידע והשלכות הסירוב למסור אותו, מטרת השימוש במידע, שמה של המפלגה ודרכי ההתקשרות עימה, הגורמים שלהם יימסר המידע, וזכויותיהם בדבר המידע שהם מוסרים?

- האם הסכמת הבוחרים היא הסכמה תקפה על פי התבחינים שפורטו לעיל?

אם מקור המידע הוא סוחרי מידע שמהם 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 על אודותיהם כלול במאגר הנרכש?

- אם המידע שנרכש מסוחרי מידע נאסף באמצעות גירוד מאתרי אינטרנט פתוחים, או באמצעות מערכות בינה מלאכותית, שגירדו מידע או הסיקו מידע אישי על בסיס מידע קיים:

• האם המפלגה וידאה שהבוחרים נושאי המידע נתנו הסכמה תקפה, על פי תבחינים שפורטו לעיל לגירוד המידע?⁴²⁷

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?

⁴²⁷ שאלה זו נמצאת כאן משום שלעמדת הרשות לפרטיות נדרשת הסכמה, אבל כפי שהערנו למעלה עדיין יש בו מחלוקת, והוא איננו מוסדר.

- האם מטרות השימוש נרשמו במסמך מטרות המאגר?
- האם המטרות שפורטו במסמך המאגר מתאימות למטרות שבסעיף 39(ג), והן מסוימות ומפורשות?
- האם המפלגה פירטה בפני הבוחרים נושאי המידע את מטרות השימוש בהודעה בעת פנייה לעיבוד מידע אישי לפי סעיף 11?

2. עקרון צמידות המטרה

- האם המידע עובד אך ורק למטרות שלשמן נמסר המידע על ידי נושא המידע או למטרות סעיף 39(ג) ובהיקף הנחוץ לשם כך?
- האם למפלגה ו/או למפעיל יישומון הבחירות שליטה מלאה בשימושים הנעשים במידע האישי באמצעות היישומון כדי 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 כן,

- האם המפלגה מסרה הודעה על כך לרשות להגנת הפרטיות כנדרש לפי סעיף 8א(ב) לחוק הגנת הפרטיות?

2. חובת הודעה בפנייה בדיוור ישיר

- האם נעשית פנייה אישית לבוחר על בסיס השתייכותו לקבוצת אוכלוסייה 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 לצד הפנייה בדיוור ישיר ניתן לנמנע מידע על זהותה ומענה של המפלגה, המקורות שמהם קיבלה המפלגה את המידע האישי שעל פיו נעשתה הפנייה, וזכותו של הנמען לבקש את מחיקת המידע האישי על אודותיו מהמאגר?

3. חובת אבטחת מידע

- האם המפלגה עומדת בכל דרישות אבטחת המידע לפי חוק הגנת הפרטיות ותקנות אבטחת מידע?

- האם המפלגה בחנה את סיכויי אבטחת המידע הכרוכים בהתקשרות עם ספק יישומון או עם גורם חיצוני אחר לפני ההתקשרות?

- האם בהסכם בין המפלגה לגורם החיצוני נקבעו במפורש ובשים לב לסיכויי אבטחת המידע הנושאים האלה:

- המידע שהגורם החיצוני רשאי לעבד ולאילו מטרות.
- המערכות שאליהם רשאי הגורם החיצוני לגשת.
- סוג העיבוד שהגורם החיצוני מוסמך לעבד.
- משך ההתקשרות ואופן השבת המידע למפלגה בסיומה.
- אופן יישום הוראות תקנות אבטחת מידע על ידי הגורם החיצוני.
- חובתו של הגורם החיצוני להחזיר את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע.
- חובתו של הגורם החיצוני לדווח לפחות אחת לשנה למפלגה על מילוי 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 בדבר היותה של מפלגה גוף דר־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 זהותם של מתקין היישומון ועל הרשאות הגישה הניתנות לו, ייתכן 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 רביעי: 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 האפיון שבגיננו 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 ולהגברה מלאכותית של מסרי תעמולה באופן המגדיל את עוצמת המניפולציה?

2. חשאיית הבחירות

- האם מוזן בזמן אמת, ביום ההצבעה, מידע מהקלפיות בדבר בוחרים המממשים את זכות ההצבעה שלהם, ובעקבותיו נעשית פנייה אישית לבוחרים שטרם מימשו את זכות ההצבעה?

- האם הבוחרים הסכימו לשימוש במידע אישי על אודות מימוש או אי-מימוש זכות ההצבעה שלהם?⁴²⁸

שלב חמישי: אימוץ והטמעה של אמצעים לבקרה על הסיכונים לפרטיות ולטוהר הבחירות ולצמצום

- האם ננקטו אמצעים ארגוניים או טכנולוגיים –

- להבטחת קבלת הסכמה תקפה של הבוחרים נושאי המידע לאיסוף המידע האישי על אודותיהם לשימוש 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 שלשמה נמסר המידע או שנקבעה על ידי המפלגה במסמך הגדרות המאגר ועל פי סעיף 39(ג) בחוק הבחירות?
- למניעת עיבוד ללא הרשאה?
- למתן מענה למימוש זכויות נושאי המידע?
- להבטחת השקיפות כלפי הבוחר מבחינת המידע האישי שבו נעשה שימוש, שימוש בטכנולוגיות בינה מלאכותית ואוטנטיות המסר?
- למניעת ניצול לרעה של מידע בעל רגישות מיוחדת על אודות חולשות, מוגבלויות או מצוקות נפשיות של הבוחרים נושאי המידע?

428 ההכרעה בשאלה אם מעשה זה הוא פגיעה בחשאיית הבחירות תלויה ועומדת בפני יו"ר ועדת הבחירות המרכזית ואין בה החלטה בפסיקת עבר, וכך גם ההכרעה בשאלה אם המעבר מתיעוד ידני של רשימות הבוחרים לתיעוד באפליקציות בזמן אמת יוצר פגיעה בטוהר הבחירות.

סיכום

תעמולה פוליטית נשענה מאז ומתמיד על מידע על בוחרים. אולם ההתפתחויות הטכנולוגיות, בעיקר בתחום הבינה המלאכותית, חוללו שינוי עמוק באופן איסוף מידע אישי ובדרכי השימוש בו בתעמולות בחירות. המדובר באיסוף מסיבי של נתונים, ניתוחם באמצעים חישוביים ובהפצת מסרים מותאמים אישית לבוחרים,

לעיתים בלי שהם מודעים לכך. מערכות בינה מלאכותית יכולות להסיק מידע חדש על בוחרים מתוך נתונים זמינים, ולאחד פרטי מידע מכמה מקורות לפרופיל אישי מקיף. מצב זה מעורר חשש לפגיעה בזכות בוחרים לפרטיות, וגם לזכותם לבחור בחירה אוטונומית וחופשית.

אכן, תיקון 13 לחוק הגנת הפרטיות הרחיב את ארגז הכלים שבידי הרשות להגנת הפרטיות, ובידי אזרחים, כדי להתמודד עם פגיעות אלו. עם זאת, מדובר בכלים מוגבלים. ראשית, לראש הרשות סמכות להורות על הפסקת הפרה, וסמכות זו אינה מוגבלת בתקופת בחירות. אולם, לנוכח חולשתה של הרשות מול המגזר הציבורי, לרבות מול גורמי ממשל, כלל לא ברור שראש הרשות יפעיל את סמכותו זו כבר בתקופת הבחירות הקרובה. נוסף על כך, כלי הפיקוח והאכיפה של הרשות להגנת הפרטיות מוגבלים בתקופת בחירות, לנוכח ההסדר המחייב את אישור יו"ר ועדת הבחירות.⁴²⁹ 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 לעיתים קרובות בעלי נפקות מעשית נמוכה, ואף עשויים להיחשב בעיני מפלגה "הפרה יעילה" – כלומר, מחיר שכדאי לה לשלם כדי להבטיח תעמולת בחירות מוצלחת יותר מבחינתה.

שנית, בהיעדר תיקון של הדין המהותי בחוק הגנת הפרטיות, רשימת הזכויות שיש בידי האזרחים הבוחרים, וכלי האכיפה הפרטית העומדים לרשותם, מצומצמים. מכיוון שחוק הגנת הפרטיות דבק במנגנון הסכמה מדעת בלבד כתנאי להתרת פגיעה בפרטיות, יש להסכמה משמעות מעשית מעטה ודרישת ההסכמה קשה לאכיפה.

ועדת הבחירות המרכזית לכנסת נמנעה עד כה מלהכריע בנושאים הקשורים בשימוש במידע אישי במסגרת תעמולת בחירות, בסכנות שבשימושים אלו לזכות הבוחר לפרטיות, ובהשלכותיהם על רצונם החופשי של הבוחר והבוחרת, האוטונומיה שלהם וזכותם לבחור. כל זאת, בנימוק שאין היא מוסמכת לדון בנושאים הקשורים בחוק הגנת הפרטיות לפי חוק דרכי תעמולה. אולם, הימנעות ועדת הבחירות המרכזית מלדון בנושאים אלו היוותה בפועל הכרעה שמשמעותה התרת כלל השימושים במידע אישי הנעשים במסגרת תעמולת בחירות ושיש בהם כדי לסכן את הזכות לפרטיות, לנוכח הצורך לקבל החלטות מיידיות בפרקי זמן קצרים לשם מניעת פגיעה בפרטיות או מזעורה.

לדעתנו, חקיקתו של תיקון 13 יכולה לשנות את תפיסת הסמכות של ועדת הבחירות המרכזית לדון בסוגיות הנוגעות לתכר שבין חוק הגנת הפרטיות לחוקי הבחירות. תיקון 13 הסמיך את יו"ר ועדת הבחירות המרכזית להכריע אם לאפשר לרשות להגנת הפרטיות להפעיל חלק מסמכויותיה בתקופת בחירות, 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 שבהן נדרשת הכרעה מהירה וכאשר יש חשש שהמתנה להליך פיקוח ואכיפה מצד הרשות להגנת הפרטיות תוביל לפגיעה של ממש בזכות הבוחרים לפרטיות, שלא יהיה אפשר למנוע, למזער או לתקן בדיעבד.

גם ללא הרחבת הסמכות, אנו סבורות שיש בידי יו"ר ועדת הבחירות המרכזית כלים להתמודד עם הסכנות הנלוות לעיבוד עמוק ורחב היקף של מידע אישי למטרות תעמולת בחירות. על ועדת הבחירות המרכזית לעשות שימוש בכלים אלו ולהגדיר את גבולות מותר ואסור בעיבוד מידע אישי על אודות בוחרים. לדעתנו, על ועדת הבחירות המרכזית להבהיר כי על פי סעיף 119(א)(3) לחוק הבחירות אסור להפריע לבחירות על בסיס פעולות דיגיטליות מותאמות אישית העלולות לגרום לאדם סביר להימנע מלהצביע. כן נציע שוועדת הבחירות המרכזית תבהיר שמעשים של מניפולציה רגשית על בוחרים, המבוססים על

עיבוד מידע בעל רגישות מיוחדת על אודות הבוחרים המפר את הוראות חוק הגנת הפרטיות, הם 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, כדי 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 על אודות הבוחרים לכל משתמש ביישומון הבחירות; וחשיבות אבטחת המידע ומשמעות דרישות אבטחת המידע ביחס לעיבוד המידע המבוצע על ידן, לרבות בכל הקשור לקביעת מורשי גישה למידע ולאופן אימות זהותם. כן נציע כי הרשות להגנת הפרטיות תפרסם את עמדתה בכל הקשור לנושאים מהותיים שאין בהם הכרעה, ובכללם החובות החלות על מפלגה בהיותה גוף דו־מהותי, ופרשנות הרשות בדבר 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 הדמוקרטיים 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 אפשר להתיר במסגרת משטר דמוקרטי, בלי שעקרון הבחירות החופשיות ירוקן מתוכן. בהיעדר היערכות מוקדמת והבהרות נורמטיביות מצד ועדת הבחירות המרכזית והרשות להגנת הפרטיות, עולה חשש שיתרונות טכנולוגיים ייהפכו 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, משנות ה־70 של המאה ה־20:

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.⁴³⁰

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'טלית.

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