מעיין פרל*

פרטיות, שליטה ופיקוח בעידן של נתוני עתק: חובת הנמקה על החלטות אלגוריתמיות

א. מבוא

אנו חיים בעידן שבו נתוני עתק (big data) מנבאים אותנו. כשירותו של פרט לקבל הלוואה, מידת התאמתו למשרה מסוימת או למסלול לימודים ורמת האמינות שלו בעיני הרשתות החברתיות נמדדים כיום על סמך ניבויים סטטיסטיים שהופקו משכלול וניתוח של נתוני מידע ממגוון מקורות עצום.[1] גופים פרטיים מקבלים החלטות שונות ואף גורליות בנוגע לפרט מושא המידע (data subject) על בסיס ניבויים אלה. האם הם כפופים לפיקוח ובקרה הולמים? במאמר זה אבקש להסביר את אתגר הפיקוח הכרוך בקבלת החלטות על סמך ניבויים אלגוריתמיים שאינם מובנים לפרט מושא ההחלטה, ואציע להתמודד עמו באמצעות הטלה של חובת הנמקה על גופים פרטיים, העולה בקנה אחד עם גישת הפרטיות כשליטה. אטען כי באמצעות כלים משפטיים אפשר ליצור תמריץ שיחייב מקבלי החלטות פרטיים להוביל לשיפור הטכנולוגי הדרוש כדי להפוך ניבויים סטטיסטיים למובנים, וכפועל יוצא – להכפיפם לפיקוח ראוי. הזכות למתן הסבר, שהוכרה לאחרונה במסגרת הרפורמה האירופית להגנה על מידע בעידן של נתוני עתק (The General Data Protection Regulation),[2] תשמש מודל השוואתי ליצירת מנגנון פיקוח ישראלי המבוסס על הרחבת התחולה של חובת ההנמקה הציבורית.

השימוש בניבויים סטטיסטיים בנוגע לפרט טומן בחובו פוטנציאל עצום מבחינת יעילות ודיוק, ובכפוף לעיצוב נכון – גם מבחינת קידום של ערכים דמוקרטיים כמו שוויון, צדק והוגנות.[3] טכנולוגיות של נתוני עתק מבוססות על ניתוח אוטומטי של מידע גולמי רב, מגוון

---

* מרצה מן המניין, המכללה האקדמית נתניה; חוקרת בכירה, המרכז לסייבר, משפט ומדיניות, אוניברסיטת חיפה; תודה מקרב לב לעורכי הכרך, לשופט החיצוני ובמיוחד לפרופ׳ מיכאל בירנהק על הערות מועילות ומאירות שסייעו בידי בכתיבת תוצר מוגמר זה.

1 מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 169 (2010); Elizabeth Dwoskin, *Facebook is rating the trustworthiness of its users on a scale from zero to 1,* The Washington Post (Aug. 21, 2018), https://wapo.st/2B3WayB.

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

3 בהקשר זה הראו מחקרים רבים כי בניגוד לאינטואיציה, אלגוריתמים אינם אובייקטיבים אלא סובלים מאותן הטיות קוגניטיביות ודעות קדומות שיש למתכנתים או צרובות במידע המזין אותם. ראו לעניין זה Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*,

ומעודכן.[4] טכנולוגיות אלו מסוגלות לשקול אין־סוף שיקולים רלוונטיים, ללא מגבלות של זמן או זיכרון אנושי, ובמובן זה הן מסוגלות לתפוס את מגוון רבדיה המורכבים של אישיות האדם. עיצוב מבוקר של טכנולוגיות של נתוני עתק, וכן פיקוח ראוי ומתמשך – הן בנוגע למהימנות המידע הגולמי שמזין את האלגוריתמים שבבסיס טכנולוגיות נתוני עתק והן בנוגע לאופן עיבודו וניתוחו[5] – יכולים לנטרל דעות קדומות או הטיות קוגניטיביות אחרות שמאפיינות את בני האדם, וכך למנוע אפליה ומשוא פנים.[6]

אולם, ללא עיצוב מבוקר של טכנולוגיות נתוני עתק, ובהיעדר פיקוח ראוי ומתמשך על המידע הגולמי שמזין אותן ועל האופן שבו הוא מעובד, ניבויים סטטיסטיים עלולים לשקף הערכות שגויות או מוטות בנוגע לפרט מושא המידע,[7] ולאלה יש השלכות משמעותיות על זכויות הפרט כגון חופש הביטוי,[8] הזכות לשוויון[9] והזכות להליך

Engin Bozdag, *Bias in algorithmic* ;14 ACM Transactions on Info. Sys. 330 (1996) Omer Tene & Jules ;*filtering and personalization*, 15 Ethics & Info. Tech. 209 (2013) Polonetsky, *Big Data for all: Privacy and user control in the age of analytics,* 11 Nw. Solon Barocas & Andrew D. Selbst*, Big Data's* ;J. Tech. & Intell Prop. 385 (2012) *Disparate Impact*, 104 Calif. L. Rev. 671 (2017); עם זאת, התפיסה המקובלת כיום היא שבאמצעות מנגנוני שקיפות אפשר לפחות לבחון באיזו מידה אלגוריתמים הם אובייקטיביים. ראו Gianclaudio Malgieri & Giovanni Comande, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation,* 7 International Joshua A Kroll et al., *Accountable Algorithms*, ;Data Privacy Law 243, 249 (2017) .165 U. Penn. L. Rev. 636, 639 (2016)

4 תכונות אלו מתייחסות ל־Volume, Variety, Velocity ו־Veracity ולכן זכו לכינוי "The 4 V's of Big Data".

5 כך, למשל, רצוי שלמידת מכונה (machine learning), שבאמצעותה מנגנונים אלגוריתמיים לומדים לנבא על סמך נתוני עבר, תתבצע על מאגרי מידע מסוימים, ידועים ומוגבלים, שאפשר לבדוק את מהימנותם. למידת מכונה לא מבוקרת (unsupervised learning) מצמצמת את היכולת להזים טעויות. ראו, באופן כללי, Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making*, 59 Communications of the ACM 56 (2016).

6 Tal Zarsky, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making,* 41 Sci. Tech. & Kate Crawford & Jason Shultz, *Big Data and Due Process:* ;Hum. Values 118 (2016) ;*Toward a Framework to Redress Predictive Privacy Harms,* 55 B.C. L. Rev. 93 (2014) Tal Zarsky, *Understanding Discrimination in the Scored Society*, 89 Wash. U. L. Rev. .1375 (2014)

7 J. Nathan Matias, *Bias and Noise: Daniel Kahneman on Errors in Decision-Making*, Medium, (Oct. 18, 2017), https://bit.ly/2oHrU6r.

8 Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement,* 19 Stan. Tech. L. Rev. 473, 488 (2016) (שם תיארנו את ההשלכות של אכיפה אוטומטית של זכויות יוצרים על חופש הביטוי).

9 ראו, למשל, Solon Barocas, *Data Mining and the Discourse on Discrimination*, https://bit.ly/2En165N.

הוגן.[10] פוטנציאל ההשפעה של טעויות אלה איננו צפוי משום שאין לדעת מראש מה תהיינה ההשלכות העתידיות של ניבוי סטטיסטי מסוים שנעשה לגבי הפרט מושא ההחלטה.[11] כך, ניבוי שגוי – שלפיו הסיכויים שהפרט יעמוד בהתחייבויות כלכליות הם מעטים – עשוי להוביל לשלילת כשירותו לקבל הלוואה, ובהמשך עלול להשפיע על אפשרויות הדיור והתעסוקה שלו ועל היבטים משמעותיים נוספים בחייו. נוסף על כך, גם היקפן וקצב התפשטותן של טעויות בהערכת הפרט על סמך טכנולוגיות של נתוני עתק, המשעתקות את עצמן במהירות רבה, עשוי להיות חסר תקדים. לפיכך, היכולת להזים טעויות הרות־גורל הגלומות בניבויים סטטיסטים שהופקו בנוגע אלינו באמצעות עיצוב טכנולוגי שקול ומנגנוני פיקוח הולמים, היא קריטית.

הצורך לפקח על אלגוריתמים הוכר זה מכבר בספרות האקדמית[12] אולם טרם נמצא לו פתרון טכנולוגי. טכנולוגיות של נתוני עתק הן מסובכות, דינמיות ובלתי־שקופות, מה שמקשה על מי שפיתח אותן להסביר את האופן שבו הן מעבדות מידע לשם הפקת ניבויים סטטיסטיים בנוגע לפרט מושא המידע. בד בבד, ברמה המשפטית, שאלת היכולת להסביר אלגוריתמים (algorithmic explainability) הולכת ותופסת מקום מרכזי בשיח האקדמי[13] וגם במשפט עצמו. כך במיוחד ה־GDPR, שנכנס לתוקף במאי 2018, הכיר בזכותו של מושא המידע לקבל הסבר על החלטות אוטומטיות שהתקבלו בנוגע אליו – אם כי בהקשרים מסוימים בלבד: כל עוד מושא המידע כפוף למנגנון אוטומטי לחלוטין (כלומר כזה שאינו כולל כל מעורבות אנושית) של קבלת החלטות, וככל שמדובר בהחלטה בעלת השלכה משפטית או השלכה בעלת חשיבות דומה על הפרט.[14] מאמר זה תומך באימוץ המנגנון האירופי

10 ראו Crawford & Schultz, לעיל ה"ש 6.

11 ומכאן החשיבות של פיקוח ובקרה על כל הערכה אוטומטית, תהא השלכתם הנוכחית אשר תהא. ראו חלק ה להלן.

12 Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 Ga. L. Rev. 1 (2005); Tarleton Gillespie, Wired Shut: Copyright And The Shape Of Digital Culture 240-42 (2007); Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1252 (2008); Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. Telecomm. & High Tech. L. 235, 235-36 (2011); Crawford & Schultz, לעיל ה"ש 6; Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, לעיל ה"ש 8; Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 Fla. L. Rev. 181 (2017); Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J.L. & Tech. 103, 114-15 (2018); Nicholas Diakopoulos, *We Need to Know the Algorithms the Government Uses to Make Important Decisions About Us*, The Conversation (May 23, 2016), https://goo.gl/SQhJNa.

13 שם; Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 18 (2017); Bryce Goodman & Seth Flaxman, Malgieri & Comand, לעיל ה"ש 3; *European Union regulations on algorithmic decision-making and a 'right to explanation'*, 38 AI Magazine 50 (2017).

14 ראו בחלק ו להלן.

בכפוף לשני שינויים עקרוניים: הראשון, שהזכות לקבל הסבר על החלטות שהתקבלו על סמך ניבויים סטטיסטיים – שאל מולה ניצבת חובת הנמקה אקטיבית – תחול ללא קשר לקיומה של מעורבות אנושית בתהליך קבלת ההחלטה; השינוי השני הוא שהזכות לקבל הסבר תחול על כל החלטה המתקבלת בנוגע לפרט, גם אם תוכן ההסבר והיקפו עשויים להשתנות בהתאם לאופי ההחלטה.

נקודת המוצא של המאמר היא שחוק הגנת הפרטיות, התשמ"א-1981 (להלן: חוק הגנת הפרטיות) הישראלי אינו נותן מענה מספק לאתגר הפיקוח הכרוך במנגנונים אלגוריתמיים לקבלת החלטות, משום שבקובעם את עקרון ההסכמה מדעת ואת עקרון צמידות המטרה, הסדריו מתמקדים בשלב שבו נאסף המידע.[15] הזכויות המוקנות למושא המידע – לעיין במידע שנאסף על אודותיו ולתקנו – חלות גם הן על מידע שנאסף במאגר מידע. ככל שמדובר באיסוף של מידע מסוים למטרה מסוימת על ידי גוף מסוים, כוחם של עקרונות אלו עומד; אולם במציאות איסוף מידע אישי נעשה בהיקף עצום ובאופן גורף, על ידי גופים רבים ושונים ולמטרות רבות ובלתי־צפויות. בעידן של נתוני עתק, ערכו האמתי של המידע טמון בשילובו, בהמשך הדרך, עם מקורות מידע שאינם ידועים בשלב של איסוף המידע.[16] משכך, תחולתם המהותית של הסדרי חוק הגנת הפרטיות צרה מכדי לאפשר לפרט לשלוט בהחלטות המשפיעות על חייו. במדינה דמוקרטית הדוגלת בזכויות אדם אין מקום לתוצאה כזו, החותרת תחת עקרונות בסיסיים של שלטון החוק וביקורת משפטית וציבורית.[17] כיצד יוכל הפרט לשפוט אם המידע שנאסף על אודותיו מתגלגל באופן חוקי? כיצד יוכל להעריך אם התחייבויות חוזיות בנוגע למידע על אודותיו אכן מתמלאות? כיצד ידע אם הגופים הפרטיים שמולו פועלים בדרך מקובלת ובתום לב? היכולת להבין כיצד מתגלגל המידע וכיצד הוא משמש לקבלת החלטות בנוגע לפרט הוא תנאי שבלעדיו לא תוכל להתקיים ביקורת אפקטיבית על מקבלי ההחלטות.

לפיכך, במאמר זה אטען כי הגיעה העת לעדכן את דיני הגנת הפרטיות בישראל ולהרחיב את תחולתם אל מעבר לשלב איסוף המידע, אל השלב שבו מתקבלות החלטות הנוגעות לפרט על בסיס הערכות מסובכות, דינמיות ובלתי־שקופות של טכנולוגיות נתוני עתק. לשם כך ראוי להשלים את מנגנון ההגנה מראש, הקבוע כיום בחוק הגנת הפרטיות, במנגנון הגנה בדיעבד דוגמת המנגנון האירופי, שיטיל חובת הנמקה על גופים פרטיים שמקבלים החלטות בנוגע לפרט על סמך ניתוח של נתוני עתק,[18] שתחולתו תהיה רחבה מתחולת המנגנון האירופי ותכלול את כל סוגי ההחלטות – משמעותיות וזניחות לכאורה כאחת. הכרה בזכות הפרט לקבל הסבר על ההיגיון שבבסיס החלטות המתקבלות לגביו על סמך טכנולוגיה של נתוני

15 ס' 1 ו־2(9) לחוק הגנת הפרטיות התשמ"א-1981, ס"ח 128.

16 Tene & Polonetsky, לעיל ה"ש 3, בעמ' 240; Crawford & Schultz, לעיל ה"ש 6, בעמ' 106; Cynthia Dwork & Deirdre Mulligan, *It's Not Privacy, and It's Not Fair*, 66 Stan. L. Rev. Online 35, 36-38 (2013).

17 Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, לעיל ה"ש 8 (שם הסברנו את חשיבותה של ביקורת ציבורית על החלטות המתקבלות באמצעות מנגנונים אלגוריתמיים לקבלת החלטות).

18 Tene & Polonetsky, לעיל ה"ש 3, בעמ' 271 (שם הם טענו שיש להקנות לכל אזרח – ולא רק למי שעומד למשפט – זכות להשיג על החלטות המתקבלות בנוגע אליו).

עתק, המבוססת על דוקטרינת ההנמקה שבמשפט הציבורי, תוכל לסייע לפרט להבין כיצד התקבלו ההחלטות הנוגעות אליו, ובהמשך – להשיג עליהן ולדרוש את תיקונן במקרה הצורך, תוך שהוא שולט באופן מלא ואפקטיבי בעצמו ובחייו.

מהלך הדיון: בחלק ב אתאר את פעילותם של מנגנונים לקבלת החלטות המבוססים על ניתוח של נתוני עתק, כדי להסביר את הקושי שכרוך בהכפפתם לפיקוח ובקרה. בחלק ג אפרט את החסמים המקשים על חשיפת ההיגיון שבבסיס הניבויים הסטטיסטים של טכנולוגיות נתוני עתק, ואטען שאפשר להתגבר עליהם באמצעות מהלך משפטי־טכנולוגי: קביעת חובה משפטית להסביר את ההיגיון שבבסיס הניבויים תיצור תמריץ שוקי לפיתוח אלגוריתמים שמעבדים מידע באופן שאפשר להסבירו. בחלק ד אראה כי גישת הפרטיות כשליטה יכולה לספק עוגן מושגי לפיתוח אמצעי לפיקוח על החלטות המתקבלות בנוגע לפרט על סמך ניתוח של נתוני עתק, אם כי לפי שעה ההסדרים שבחוק הגנת הפרטיות אינם מספיקים לכך מבחינה מהותית. בחלק ה אציע תשתית ראשונית לפיתוח מנגנון הגנה בדיעבד תחת דיני הגנת הפרטיות בישראל, דוגמת המנגנון שאומץ ב־GDPR, בהתבסס על דוקטרינת ההנמקה שבמשפט הציבורי כדי לאפשר לפרט מושא המידע לקבל הסבר על ההחלטות שהתקבלו לגביו על סמך ניתוח של נתוני עתק.

ב. קבלת החלטות על סמך הערכות אוטומטיות של טכנולוגיות מידע

אנו מצויים בעידן של נתוני עתק המזוהה לרוב באמצעות ארבעה מאפיינים: כמות המידע (Volume), מהירות השימוש במידע (Velocity), מידת הדיוק של המידע (Veracity) ומגוון המקורות שלו (Variety).[19] הודות לטכנולוגיות מחשוב מתקדמות דוגמת הענן, כמויות עצומות של מידע גולמי ניתנות כיום לאיסוף, לאחסון ולהפצה. אלגוריתמים משוכללים וטכנולוגיות של למידת מכונה (machine learning)[20] מאפשרים לחפש הקשרים רבים בין פרטי מידע שונים על אודות מושא המידע (data mining),[21] לעבד ולנתח נתוני עתק (data analytics) ולייצר כלי ניבוי בנוגע לפרט.[22] כך, למשל, טכנולוגיות מתקדמות לניתוח מידע מאפשרות לחברות ענק מסחריות (דוגמת eBay ואמזון) לנתח את המידע שהן אוספות מלקוחותיהן כדי ללמוד את העדפותיהם וליצור עבורם ממשק רכישה אידאלי.[23] טכנולוגיות של פרסום

19 Jules J. Berman, Principles of Big Data: Preparing, Sharing, and Analyzing Complex Information 1-2 (2013).

20 למידת מכונה מאפשרת לפתח אלגוריתמים שלומדים מתוך דוגמאות ולא בהכרח מתוך קובץ חוקים מוגדר וקבוע מראש.

21 ראו דיון בסוגיה של כריית המידע ובהשפעתה על הזכות לפרטיות Tal Zarsky, *Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion,* 5 Yale J.L. & Tech. 1 (2002).

22 Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 Texas L. Rev. 669, 687-89 (2010).

23 יאיר עמיחי־המבורגר ואורן פרז "אנונימיות ואינטראקטיביות באינטרנט: הזכות לפרטיות כמושג רב־ממדי" **פרטיות בעידן של שינוי 201, 204–205** (תהילה שוורץ אלטשולר עורכת, 2012).

דיגיטלי ממוקד לומדות מה הם תחומי העניין של הפרט כפי שהם משתקפים בפעילותו ברשת, ומעבדות את הנתונים כדי לחשוף אותו לפרסום ספציפי הרלוונטי עבורו.[24] רשויות האכיפה נעזרות גם הן בהערכות אוטומטיות כדי להביא להקצאה יעילה של משאבי אכיפה,[25] למשל על ידי שימוש באלגוריתמים להערכת מסוכנות פוטנציאלית על סמך ניתוח והצלבה של מידע על אודות פעילות עבריינית קודמת, מעורבות באירועי ירי והשתייכות לכנופיות.[26]

עם זאת, קבלת החלטות על סמך ניבויים סטטיסטיים המופקים באמצעות טכנולוגיות של נתוני עתק מציבה לפני הפרט מושא ההחלטה אתגר פיקוח רציני. ההיגיון שעליו ניבויים אלה מבוססים, ככל שהוא קיים, הוא מורכב מאוד;[27] מכל מקום, מי שמעצב את המערכות שמייצרות אותם, כמוסבר להלן,[28] אינו מחויב בהכרח לגלותו.[29] בשונה משכלול אנושי של מידע אישי על אודות הפרט, הפועל על סמך הקשרים לוגיים, צפויים ומוגבלים שאפשר לתרגם מילולית, שכלול של מידע אלגוריתמי הוא מורכב, דינמי, בלתי־צפוי ובלתי־שקוף. לפיכך, מושאי ההחלטות – מבקשי הלוואה שידורגו על ידי אחת מארבע לשכות אשראי מורשות כבעלי אשראי נמוך;[30] מועמדים לעבודה שידורגו כבעלי יצירתיות או כושר מנהיגות נמוכים[31] או נהגים שיתויגו כמסוכנים לצורך קביעת פרמיית הביטוח שלהם[32] – יתקשו להשיג על החלטות קונקרטיות המתקבלות בקשר אליהם ועלולות למנוע מהם הלוואה, תעסוקה או ביטחון כלכלי.

אמנם רמת הדיוק של ניבויים סטטיסטיים המבוססים על ניתוח נתוני עתק עשויה להיות גבוהה מאוד, אולם בכך אין כדי ליתר את נחיצותם של פיקוח ובקרה. אין זה חדש שהאלגוריתמים המבססים את טכנולוגיות נתוני העתק אינם מושלמים:[33] הם משעתקים את ההטיות הקוגניטיביות של מי שתכנת אותם, ולפיכך עשויים לקבל בקשר לפרט החלטות

24 Elspeth A. Brotherton, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 Emory L.J. 555, 558 (2012).

25 Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 Emory L.J. 259, 265-69 (2013).

26 Jeff Asher, *Inside the Algorithm That Tries to Predict Gun Violence in Chicago,* N.Y. Times (June 13, 2017), https://nyti.ms/2sqLTur.

27 Perel & Elkin-Koren, *Black Box Tinkering*, לעיל ה"ש 12, בעמ' 189–190 (שם טענו כי אחת הסיבות המרכזיות שבגינה קשה לבקר מנגנונים אלגוריתמיים לקבלת החלטות קשורה למורכבות האנליטית שלהם).

28 ראו את הדיון בחלק ג להלן.

29 Tal Zarsky, *Transparent Predictions*, 2013 Ill. L. Rev. 1503, 1512.

30 ס' 12–14 לחוק נתוני אשראי, התשע"ו–2016, ס"ח 2551.

31 Don Peck, *They're Watching You at Work*, Atlantic Monthly (Dec. 2013), https://bit.ly/2RLt2Do.

32 Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 8-10 (2014).

33 Friedman & Nissenbaum, *Bias in Computer Systems*, לעיל ה"ש 3, בעמ' 330–347; Brent Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 Big Data & Society 2 (2016).

מוטות, המבוססות על עמדות מפלות כלפי קבוצות מיעוט מסוימות.[34] תוצאות מוטות עשויות לנבוע גם מהטיות מובנות במידע שהוזן לאלגוריתם, ללא קשר לעמדות המתכנתים.[35] במקרים אחרים אלגוריתמים עלולים לקבל תוצאות שגויות פשוט בשל מידע שגוי שהוזן להם או בגלל שגיאות עיצוביות.[36] כך, למשל, התוכנה האוטומטית לסינון תכנים של YouTube, Content ID, חסמה סרטון אקדמי־לימודי בגין הפרת זכות יוצרים, אף על פי שהשימוש שנעשה במסגרת הסרטון שנחסם ביצירות מוגנות היה מותר בהיותו שימוש הוגן;[37] האלגוריתם של גוגל הציג מודעות דרושים יוקרתיות לגברים ולא נשים;[38] תיוג שגוי של נזירות קתוליות ומועמדים לרשויות מקומיות תחת הקטגוריה "טרוריסטים" הועבר לרשויות הפדרליות בארצות־הברית בלי ליידע את המתויגים ובלי לאפשר להם לתקן את המידע השגוי.[39] כל אלה משליכים על זכויותיו הבסיסיות של הפרט, לרבות חופש הביטוי,[40] הזכות לשוויון[41] והזכות להליך הוגן.[42]

ללא כלים המתאימים לבקר את ההיגיון המבסס הערכות אוטומטיות בנוגע לפרט אי־אפשר לעמוד על איכות הניבויים שלהן בנוגע לפרט מושא ההחלטה ולהשיג עליהם במקרה הצורך. כפי שאראה להלן, יש קושי ממשי לחשוף את ההיגיון המבסס מנגנונים אלגוריתמיים לקבלת החלטות; לדעתי קושי מחייב פיתוח של אמצעי בקרה המותאמים לעידן נתוני העתק שבו אנו חיים.

ג. החלטות המתקבלות על סמך ניתוח של נתוני עתק: כשל פיקוח

היכולת להפעיל אמצעי פיקוח ובקרה על החלטות המתקבלות בנוגע לפרט מותנית בראש ובראשונה ביכולת להבין את ההיגיון שבבסיס החלטות אלה. איך אפשר להשיג על החלטה שאופן קבלתה איננו ידוע?[43] הבעיה היא שפרט הכפוף להחלטות המתקבלות על סמך ניתוח

34 Julia Angwin, Jeff Larson & Surya Mattu Lauren Kirchner, *Machine Bias*, ProBulitca (May 23, 2016), https://goo.gl/KnNFVy (מחקר שהצביע על כך שהאלגוריתמים המשמשים את המשטרה למניעת פשע מוטים לרעת שחורים); Barocas & Selbst, *Big Data's Disparate Impact*, לעיל ה"ש 3, בעמ' 677.

35 Barocas & Selbst, שם, בעמ' 674.

36 Citron, *Technological Due Process*, לעיל ה"ש 12, בעמ' 1256.

37 Fred Von Lohmann, *YouTube's Content ID (C)ensorship Problem Illustrated*, EFF (Mar. 2, 2010) https://bit.ly/2FQ8TJp.

38 Julia Carpenter, *Google's Algorithm Shows Prestigious Job Ads to Men, but not to Wome*n, Independent (July 7, 2015), https://goo.gl/enNAAM.

39 David Gray & Danielle Citron, *The Right to Quantitative Privacy,* 98 Minn. L. Rev. 62, 81 (2013).

40 Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, לעיל ה"ש 8, בעמ' 488–492.

41 ראו, למשל, Barocas, *Data Mining and the Discourse on Discrimination*, לעיל ה"ש 9.

42 ראו, למשל, Crawford & Schultz, *Big Data and Due Process*, לעיל ה"ש 6.

43 Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, לעיל ה"ש 8, בעמ' 495.

של נתוני עתק, המעוניין להבין כיצד התקבלה החלטה בעניינו, ניצב לפני קושי ממשי לברר אילו נתוני מידע השפיעו על ההחלטה, באיזה אופן נשקלו ואיזו אמת־מידה הכריעה ביניהם.

ראשית, טכנולוגיות ניתוח של נתוני עתק הן מסובכות. האלגוריתמים שבבסיסן מבטאים למעשה סדרת צעדים שיש לבצע כדי לפתור בעיה מסוימת או להשיג תוצאה מסוימת,[44] ואלו נצרבים בתוך אוסף של נוסחאות מתמטיות מסובכות.[45] פרנק פסקואלה (Pasquale), אחד החוקרים הבולטים ביותר בתחום של Algorithmic Accountability, היטיב להגדיר את המנגנונים האלגוריתמיים לקבלת ההחלטות המנהלים את חיינו כ"קופסה שחורה" של נוסחאות וחישובים מתמטיים מורכבים.[46] כך, למשל, מנגנון פשוט המוטבע במד סוכר קובע את רמת הסוכר בדם בהתאם לנתוני אמת של הנבדק בלי לאסוף ולשמור נתונים על אודותיו. לעומת זאת, מד סוכר "חכם", הפועל על סמך טכנולוגיה משוכללת של אינטרנט־של־הדברים (Internet-of-Things), אוסף ומנטר נתוני מידע בנוגע לנבדק באופן מתמיד. כך, בצד אספקת מידע בזמן אמת על אודות רמת הסוכר, הוא משמש גם מכשיר ניבוי הממליץ לנבדק כיצד לנהוג, כלומר אם לאכול או להזריק אינסולין ובאיזה מינון.[47] שני המדדים – הפשוט והחכם – מספקים לנבדק הערכה אוטומטית שעל בסיסה הוא מחליט אם להזריק אינסולין או לא.[48] אולם, בעוד שההיגיון העומד מאחורי המדד הפשוט ברור ומובן (רמת הסוכר בדם ברגע הבדיקה חורגת מטווח רמות הסוכר הסבירות), ההיגיון העומד מאחורי המדד החכם מורכב בהרבה, ועשוי להילמד מאין־ספור נתונים בנוגע לפעילותו ולהרגליו של הנבדק, כולל נתונים שאינם קשורים ישירות אליו אלא למאפייני הקבוצה שאליה הוא משתייך.[49]

שנית, הערכות אוטומטיות המתקבלות על סמך ניתוח של נתוני עתק מבוססות על מנגנונים דינמיים המשתנים ללא הרף, מה שמקשה לעקוב אחר ההיגיון שבבסיסם.[50] למידת מכונה מאפשרת עדכון שוטף של אמצעי הניבוי האלגוריתמי בהתאם למידע עדכני המוזן

---

44 Nicholas Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, Nick Diakopoulos Musings on Media 12-14 (Feb. 2014), https://bit.ly/2E7QPJz.

45 Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. On Telecomm. & High Tech. L. 235, 246 (2011).

46 Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information 18 (2015).

47 ראו פרויקט "לבלב מלאכותי פתוח" (Open APS) שמספק מערכת טכנולוגית לניטור רמות הסוכר ולהזרמת אינסולין בזמן אמת https://openaps.org.

48 אף שיש אפשרות לתכנת את מדדי הסוכר החכמים כך שיוכלו לשמש לקבלת ההחלטה הסופית במקום הנבדק. ראו שם.

49 ראו Kamalika Chaudhuri & Daniel Hsu, *Sample Complexity Bounds for Differentially Private Learning*, 19 J. Machine Learning Research 155, 155-56 (2011); Cynthia Dwork & Aaron Ruth, *The Algorithmic Foundations of Differential Privacy* (2014) https://bit.ly/2cDVqo5.

50 Perel & Elkin-Koren, *Accountability in Algorithmic Enforcemen*, לעיל ה"ש 8, בעמ' 518–520.

אליו.[51] אלגוריתמים לומדים מסוגלים לזהות מגמות, קשרים ותבניות בין מידע ממקורות שונים ורחוקים[52] עד כדי עיצוב מחדש של הבעיות שהם נועדו לפתור או של המטרות שהם מבקשים להשיג.[53] לפיכך, שימוש בהנדסה חוזרת (reverse engineering) כדי ללמוד על מנגנון הניבוי אינו מועיל בהכרח.[54] לכאורה, ככל שידועים גם הקלט ששימש את מנגנון הניבוי וגם הפלט, נדמה שאפשר לפצח את מנגנון ההכרעה וליישמו על כל קלט אחר באותו הקשר כדי להעריך מה יהיה הפלט הצפוי. אולם, הבעיה היא שהקלט המזין את מנגנון הניבוי – כמו גם אופן עיבודו והמשקל שניתן לפרטיו השונים – כפוף לעדכון, ולכן החשיפה של מנגנון קבלת ההחלטות באמצעות הנדסה חוזרת היא רלוונטית, אם בכלל, למועד החשיפה בלבד, אך לא למועד שבו התקבלה ההחלטה או למועדים מאוחרים יותר. משכך, אלגוריתמים המבוססים על ניתוח של נתוני עתק אינם בהכרח נהירים אפילו למי שתכנת אותם, לא כל שכן לפרט בעל ידע טכנולוגי ממוצע הכפוף להכרעותיהם.

סיבה שלישית שבגינה יש קושי ממשי להבין כיצד מנגנונים אלגוריתמיים לקבלת החלטות פועלים נובעת מכך שמנגנונים אלה מטבעם אינם שקופים. הם מיישמים הוראות מתמטיות מורכבות ומסובכות שאינן נהירות לאדם הממוצע. אמנם מנגנונים אלגוריתמיים אמורים לכאורה לתרגם הוראות מילוליות ברורות ונהירות שנתנו קובעי המדיניות למתכנתים, אך כפי שהראו הלן ניסנבאום (Nissenbaum) ובתיה פרידמן (Friedman),[55] הבחירות ההנדסיות של המתכנתים עלולות לעוות הוראות אלו באופן שמקשה לגזור מהן את משמעותם הנורמטיבית של האלגוריתמים. כך, למשל, תוכנת סינון התכנים של YouTube שהוזכרה לעיל מאותתת לבעלי הזכויות ברגע שיש זהות מסוימת בין יצירה מוגנת בזכות יוצרים לבין סרטון שמבקשים להעלות לפלטפורמה, והם – בעלי הזכויות – מחליטים אם לאפשר את השימוש או לא.[56] דיני זכויות יוצרים קובעים מדד איכותי להפרת זכות יוצרים: "דמיון מהותי" ("substantial similarity")

---

51 Peter Flach, Machine Learning: The Art and Science of Algorithms that Make Sense of Data 3 (2012).

52 Bernhard Anrig et al., *The Role of Algorithms in Profiling*, *in* Profiling the European Citizen 65, 65 (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

53 Bamberger, *Technologies of Compliance*, לעיל ה"ש 22, בעמ' 676.

54 Nicholas Diakopoulos, *Algorithmic Accountability: Journalistic investigation of computational power structures*, 3 Digital Journalism 398, 410-12 (2015) (להלן: Diakopoulos, *Algorithmic Accountability: Journalistic investigation*). חשוב לציין כי להנדסה חוזרת ייתכנו חסמים משפטיים וחוזיים העשויים להניא חוקרים מלהשתמש בה כדי ללמוד על מנגנון קבלת ההחלטות האלגוריתמי. כך, למשל, ס' 2 לחוק המחשבים, התשנ"ה-1995, ס"ח 336 קובע כי שיבוש או הפרעה למחשב או לחומר מחשב הם עברה פלילית שדינה מאסר שלוש שנים. גם תנאי השימוש בפלטפורמות שונות עשויות לאסור על המשתמשים לבצע פעולות מחקריות בנתוני הפלטפורמה. ראו לעניין זה Perel & Elkin-Koren, *Black Box Tinkering*, לעיל ה"ש 12, בעמ' 34-35.

55 Helen Nissenbaum, ;3 Friedman & Nissenbaum, *Bias in Computer Systems*, לעיל ה"ש *From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?*, 26 Berkeley Tech. L.J. 1367 (2011).

56 *What is Content ID Claim*, YouTube, https://goo.gl/UdXRDU.

בין היצירה המקורית לשימוש המאוחר.[57] אולם, תרגומו האלגוריתמי של מדד איכותי זה מסנן לעתים גם תכנים שאינם מפרים את הזכויות ומכאן שלא ברור אם ועד כמה הוא אכן מיישם את המדד האיכותי להפרה (להבדיל מקביעה כמותית שלפיה נלקחו חלקים מהותיים וממשיים מהיצירה המוגנת).[58] אף שהסטנדרט המשפטי ידוע, חוסר הדיוק הכרוך ביישומו האלגוריתמי מעיד על סטייה מסוימת ממנו.

אכן, מלאכת התכנות עלולה להוביל לעיוותי משמעות הנובעים ממוגבלותה האובייקטיבית של שפת המחשב.[59] במיוחד, תרגום הוראות מילוליות לשפת מחשב עלול לדרוש התאמות ושינויים המושפעים משיקולים מקצועיים, כמו גם מעמדות סובייקטיביות ומערכים מוסריים של המתכנתים.[60] לפיכך, אין לזהות את מנגנון האלגוריתמי לקבלת ההחלטות עם ההוראות המילוליות שמכתיבות אותו כדי לחשוף את משמעותו. בהיעדר כלים טכנולוגיים מתאימים לניתוח של מנגנונים אלגוריתמיים לקבלת החלטות, משמעות זו פשוט נותרת באפלה.

רביעית, יש גם חסמים עסקיים או משפטיים המקשים על הפרט באופן כללי לחשוף כיצד מתקבלות החלטות שונות בקשר אליו. כך, למשל, חשיפת מנגנון לקבלת ההחלטות עשויה לסכל את יעילותו, מה שעלול להוביל לפגיעה כלכלית במי שפיתח אותו.[61] טיעון זה עמד בבסיס התנגדותן של חברות המיון וההשמה להנחיית הרשות להגנת הפרטיות במשרד המשפטים (בשמה הקודם – הרשות למשפט, טכנולוגיה ומידע), שביקשה לחייבן לספק למועמדים את חוות הדעת בדיוק כפי שנמסרה למעסיק שהזמין את המבדקים, לרבות תוצאות המבחנים שנכללו בה. בין היתר נטען:

> חשיפת הדוחות הפסיכולוגיים בפני המועמדים תוביל לכך שחוות הדעת של המכונים תהיינה מצומקות ו'עטופות' במונחים שהמועמדים לא ייפגעו מהם. חוות דעת כאלה תפגענה באופן ברור באיכות החלטותיהם של מנהלי משאבי אנוש ושל מנהלים אחרים ביחס לקבלתם או דחייתם של המועמדים וביחס לשיבוצם לתפקידים המתאימים להם. בסופו של דבר, מעסיקים רבים, כדי לחסוך מעצמם הוצאות ודיונים משפטיים ועקב שביעות רצון נמוכה מחוות הדעת, יפסיקו את קשריהם עם מכוני המיון ויפנו לשיטות מיון אחרות.[62]

משמעות הדברים היא שלמַפתח הטכנולוגיה יש תמריץ עסקי שלילי לפרסם פרטים הנוגעים למנגנון לקבלת ההחלטות שפיתח. למעשה, ככל שטכנולוגיה זו מפותחת על ידי גופים

57 ראו, למשל, ע"א 81/15 **גולדנברג נ' בנט**, פ"ד לו(2) 813 (1982).

58 Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, לעיל ה"ש 8, בעמ' 476 (שם הבאנו דוגמאות קונקרטיות שבהן הסירה תוכנת הסינון של YouTube תכנים שאינם מפרים זכויות יוצרים).

59 James Grimmelmann, *Regulation by Software*, 114 Yale L.J. 1719, 1728 (2005).

60 ראו Bamberger, לעיל ה"ש 22, בעמ' 1252–1253.

61 Diakopoulos, *Algorithmic Accountability: Journalistic investigation*, לעיל ה"ש 54, בעמ' 403.

62 עת"מ (מנהלי ת"א) 4749-04-12 **אדם מילוא בע"מ נ' רשם מאגרי המידע במשרד המשפטים**, פס' 185 (לא פורסם, 22.4.2013).

פרטיים, תמריץ עסקי זה מקבל גם גושפנקה משפטית מכוח דיני הגנת הסוד המסחרי[63] המגנים על בעלי הטכנולוגיה מפני חשיפתה.[64] משמע, שגם אם עומדים לרשות הפרט מושא ההחלטה הידע והמומחיות הדרושים לפענוח של מנגנון הניבוי, יש אפשרות ממשית שתוגבל גישתו למנגנון.

מן האמור עולה כי יש חסמים משמעותיים לחשיפת ההיגיון שבבסיס הערכות אלגוריתמיות המשמשות לקבלת החלטות בקשר לפרט מושא המידע – אולם אין זה אומר שהדבר איננו אפשרי. מתודולוגיות טכנולוגיות שונות עשויות לאפשר זאת כמו, למשל, שימוש עקבי ושיטתי בהנדסה חוזרת[65] או ניטור של התהליך האלגוריתמי לקבלת ההחלטות.[66] נוסף על כך, פיתוחים טכנולוגיים מתקדמים יכולים כיום לאפשר לעצב מראש אלגוריתמים שאפשר יהיה להסביר.[67] הטלה של חובת הנמקה משפטית על גופים פרטיים – שברגיל אמנם אינם כפופים לכללי המשפט הציבורי אך מקבלים החלטות המשפיעות על חיי הפרט על סמך ניבויים סטטיסטיים שמבוססים על ניתוח של נתוני עתק – תעודד את הטמעת הפיתוחים הטכנולוגיים הללו ותסייע לפתור את כשל הפיקוח הכרוך בשימוש במנגנוני אלגוריתמיים לקבלת החלטות. במיוחד, כפי שיודגם בהמשך, עיצוב של מנגנוני ניבוי שאפשר להסבירם יאפשר לפרט לקבל הסבר על אודות האופן שבו התקבל ניבוי מסוים הנוגע אליו, וכפועל יוצא – לשלוט ולפקח על האופן שבו מתקבלות החלטות הנוגע אליו על סמך המידע שלו.

בחלק הבא אבחן אם אפשר לעגן את החלתה של חובת הנמקה ציבורית על גופים פרטיים שיידרשו להסביר את האופן שבו ניבויים סטטיסטיים משמשים אותם לקבלת החלטות בנוגע לפרט מושא המידע תחת דיני הגנת המידע והפרטיות. תחילה אבדוק אם אפשר לזהות בזכות לפרטיות במידע אישי עוגן מושגי לפיקוח על החלטות שמתקבלות בנוגע לפרט על סמך ניתוח נתוני עתק בקשר אליו. בהמשך, לאחר שאראה שעוגן מושגי שכזה אכן מתקיים תחת גישת הפרטיות כשליטה, אראה שההסדרים הקיימים בחוק הגנת הפרטיות אינם מאפשרים פיקוח הולם מבחינה מהותית ולכן ראוי להוסיף עליהם את מנגנון ההנמקה המוצע.

63 ס׳ 5 לחוק עוולות מסחריות, התשנ״ט-1999, ס״ח 146.

64 למשל, ס׳ 2.7.6.2 להנחית רשם מאגרי המידע 2/2012 ״תחולת הוראות חוק הגנת הפרטיות על הליכי מיון לקבלה לעבודה ופעילות מכוני מיון״ (28.2.2012) https://goo.gl/WugkjH (להלן: הנחיית רמו״ט). סעיף זה מתיר למכונים לצמצם במידה מסוימת את ההיקף של זכות העיון המוקנית למועמד באמצעות קבלת הסכמה מוקדמת ומודעת שלו, אם הדבר מתחייב במישרין מאינטרס מנוגד, במיוחד האינטרס הנוגע ״לחשיפת סודות מסחריים של מכון המיון עקב חשיפת שיטות בדיקה שהן קניינו או פרי פיתוחו״.

65 Perel & Elkin-Koren, *Black Box Tinkering*, לעיל ה״ש 12 (שם הצענו ובחנו את השימוש הסיסטמתי בהנדסה לאחור כדי לחשוף את אופן הפעולה של תוכנות אוטומטיות המסננות תכנים שמפרים זכויות יוצרים).

66 Kroll et al., לעיל ה״ש 3.

67 Finale Doshi-Velez & Mason Kortz, *Accountability of AI under the Law*, https://goo.gl/FzB65Q.

ד. הזכות לפרטיות במידע אישי: עוגן מושגי ומהותי לפיקוח על החלטות המבוססות על ניתוח של נתוני עתק

1. הפרטיות כשליטה: עוגן מושגי לפיקוח על החלטות המבוססות על ניתוח של נתוני עתק

נהוג לגזור את לידתה הרשמית של הזכות המשפטית לפרטיות מתוך מאמרם המפורסם של וורן וברנדייס (Warren & Brandeis), שהגדירו אותה כזכות להיעזב במנוחה (the right to be let alone).[68] תחת הגדרה זו, שאומצה גם במשפט הישראלי,[69] הזכות לפרטיות מתמקדת באינטרס הפרט לשלוט במידע אישי על אודותיו ובאישיותו, כמו שהללו משתקפים למשל ביצירותיו, בכתביו ובתמונתו.[70] אפשר לומר שהגדרה היסטורית זו של הזכות לפרטיות מבוססת על אוטונומיית הפרט לשלוט בעצמו ובחייו ולהחליט מתי להיעזב לנפשו.[71] פגיעה בפרטיות של אדם ללא הסכמתו משמעה פגיעה באוטונומיה שלו,[72] וזאת בין שמדובר בגופו או בתצלום גופו[73] ובין שמדובר בענייניו הפרטיים[74] דוגמת שיחותיו,[75] שמו, כינויו, תמונתו

---

68 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). ניסיונות מאוחרים להגדרה של הזכות לפרטיות כוללים את זיהויה על דרך השלילה מתוך מצבים מוגדרים המהווים פגיעה בפרטיות; את הגדרת הפרטיות כהגבלת גישה אל הפרט; את ביסוסה על יכולת הפרט לשלוט בחייו ואת גזירתה מתוך ההקשר הספציפי שבו סוגיית פרטיות מתעוררת. **ראו** William L. Prosser, *Privacy (A Legal Analysis)*, 48 Cal. L. Rev. 383 (1960); Daniel Solove, *A Taxonomy of Privacy*, 154 U. Penn. L. Rev. 477 (2006); **רות גביזון** "הזכות לפרטיות ולכבוד" **זכויות אדם בישראל: קובץ מאמרים לזכרו של חמן שלח 61 (רות גביזון עורכת, 1989)**; Alan Westin, *The Origins of Modern Claims to Privacy*, *in* Philosophical Dimensions of Privacy: An Anthology 56 (Ferdinand David Schoeman ed., 1984); Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010).

69 **ע"א 1211/96 כהן נ' נשיונל קונסלטנטס, פ"ד נב(1) 481 (1998).**

70 **בירנהק מרחב פרטי**, לעיל ה"ש 1, בעמ' 58–59.

71 **שם**, בעמ' 59.

72 **ראו**, למשל, בג"ץ 2481/93 **דיין נ' וילק**, פ"ד מח(2) 456, 469–470 (1994) ("ביתו של אדם הוא מבצרו, ובגדריו הוא זכאי כי יניחו אותו לעצמו, לפיתוח האוטונומיה של הרצון הפרטי [...]"); ע"א 8483/02 **אלוניאל בע"מ נ' מקדונלד**, פ"ד נח(4) 314, פס' 33 לפסק דינו של השופט ריבלין (2004) ("עניינה של זכות הפרטיות הוא אפוא באינטרס האישי של האדם בפיתוח האוטונומיה שלו, במנוחת נפשו, בזכותו להיות עם עצמו ובזכותו לכבוד ולחירות").

73 ס' 2(1) לחוק הגנת הפרטיות (מגדיר "בילוש" או "התחקות" אחרי אדם כפגיעה בפרטיות), וס' 2(3) לחוק (מתייחס לצילום אדם כשהוא ברשות היחיד); ס' 2(4) לחוק (מתייחס לפרסום תצלומו של אדם ברבים בנסיבות שבהן הפרסום עלול לבזות את האדם או להשפילו).

74 ס' 2(7), (8), (9) ו־(11) לחוק הגנת הפרטיות.

75 ס' 2(2) לחוק הגנת הפרטיות קובע כי האזנה אסורה היא פגיעה בפרטיות; ס' 1 לחוק האזנת סתר, התשל"ט–1979, ס"ח 118, קובע כי האזנה לשיחה ללא הסכמת מי מבעלי השיחה היא עברה פלילית.

או קולו,[76] או בהחלטות אינטימיות שהוא מקבל.[77]

שליטה עצמאית היא המפתח למימוש האוטונומיה.[78] כדי שאדם יוכל להיות אחראי לגורלו, להחלטותיו ולעצמו, עליו לשלוט במידע על אודותיו, במיוחד בעידן המידע שבו אנו חיים.[79] זו היא מציאות דינמית של איסוף אוטומטי, בלתי־שקוף ובלתי־צפוי של מידע אישי על אודות הפרט, העלול לשמש שחקנים למיניהם – רשויות ציבוריות וגופים פרטיים – במסגרת מנגנוני קבלת ההחלטות שלהם. חברות נדל"ן, למשל, יכולות לקבוע את אסטרטגיות הפרסום והשיווק של הדירות שבבעלותן בהתאם למצבו הכלכלי היחסי של הפרט,[80] המגדר שלו או נטיותיו המיניות, כפי שאלו נלמדים אוטומטית מתוך ניתוח של עקבות פעילותו ברשתות החברתיות;[81] מעסיק עלול לדחות מועמד שטכנולוגיות של עיבוד נתוני עתק ייחסו לו תכונות אופי מסוימות (עצלנות, מרדנות וכדומה),[82] וחברות אשראי עלולות להוריד את מסגרת האשראי של לקוח שנובאה לו דרגת אמינות נמוכה על סמך עיבוד של נתוני מידע עדכניים בדבר האמינות הנמוכה של לקוחות אחרים שמבצעים רכישות במקומות זהים לאלו שבהם הלקוח רוכש.[83] בצד היעילות שבקבלת החלטות על סמך ניבויים שמבוססים על טכנולוגיות עיבוד של נתוני עתק, אל נשכח את פוטנציאל הטעות שגלום בהם.[84] הבעיה היא שמקבלי ההחלטות אינם מסבירים לפרט בדיעבד אילו נתוני מידע שימשו ליצירת הניבוי, כיצד הם שוכללו ומה היה הקריטריון שהכריע ביניהם.[85] משכך, יכולתו של הפרט להזים טעויות בניבוי – וכפועל יוצא לשלוט בהחלטות הנוגעות אליו – מוטלת בספק רב.

במציאות מורכבת זו, שליטה במידע משמעה שליטה בכל השלבים שבהם המידע האישי מתגלגל, החל ברגע איסופו ושמירתו, המשך בעיבודו וכלה בהחלטות שמתקבלות על בסיסו. ומה משמעותה של שליטה זו? שליטה זו חובקת כמה רבדים: בשלב איסוף

---

76 ס' 2(6) לחוק הגנת הפרטיות.

77 *Roe v. Wade*, 410 U.S. 113 (1973). בפרשה זו עיגן בית המשפט העליון של ארצות־הברית בזכות לפרטיות את זכותה האוטונומית של אשה לבצע הפלה.

78 מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 41 (2008).

79 שם, בעמ' 90.

80 ראו Crawford & Schultz, לעיל ה"ש 6.

81 Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 Stan. L. Rev. Online 81; Michael Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavio*r, 110 Proc. Nat'l Acad. Sci. 5802 (2013), https://goo.gl/CkCftY (שם נטען כי אפשר ללמוד, בהצלחה רבה, על תכונות אישיות של פרטים על סמך חיבובים בפייסבוק).

82 Jennifer Alsever, *How AI is Changing Your Job Hunt*, FORTUNE (May 19, 2017), https://goo.gl/nVASJR.

83 Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J.L. & Tech. 148, 150-51 (2016).

84 ראו לעיל ה"ש 39.

85 Hurly & Adebayo, לעיל ה"ש 83, בעמ' 151.

המידע, שליטה משמעה מתן הסכמה מדעת לאיסוף מידע שנעשה למטרות קונקרטיות;[86] בשלב עיבוד המידע, שליטה משמעה הגבלת הפצתו ושמירה על סודיותו כמו גם מתן זכות לעיין במידע ולתקן אותו;[87] בשלב קבלת החלטות על סמך המידע, שליטה ראוי שתתפרש כהבנת ההיגיון שבבסיס ההחלטה. אדם שאינו מבין כיצד המידע על אודותיו הוביל לקבלת החלטה מסוימת לגביו מאבד מיכולתו לשלוט בעצמו ובגורלו. כיצד יוכל אדם זה להשיג על ההחלטה ולדרוש את תיקונה במקרה הצורך, אם איננו מבין את ההיגיון שעומד מאחוריה?

אשר ל"פרטיות כשליטה" טען מיכאל בירנהק: "כאשר אנו מפקידים את השליטה בידי האדם עצמו, יש להפקיד בידיו גם כלים מעשיים לשלוט בעצמו".[88] לפיכך, גישת הפרטיות כשליטה מספקת עוגן מושגי ליצירת כלי בקרה שיאפשר לפרט מושא המידע לשלוט על החלטות המתקבלות בקשר אליו על סמך מידע אישי. עם זאת, כפי שאראה להלן, יש פער בין מובנה המושגי של הפרטיות כשליטה לבין תוכנה המהותי, כפי שזה משתקף בחוק הגנת הפרטיות בישראל. נוכח המעבר משימוש בנתוני מידע מסוימים, השמורים במאגר מידע מסוים, על אודות פרט מסוים, לשימוש גורף ומקיף בנתוני מידע מגוונים ומשתנים על אודות פרטים שונים, ממקורות רבים, כדי לשכלל ניבויים סטטיסטיים בקשר לפרט מושא ההחלטה – היכולת להסתמך על הסדרים אלה מוטלת בספק רב.

2. חוק הגנת הפרטיות אינו מספק עוגן מהותי לפיקוח על החלטות המבוססות על ניתוח של נתוני עתק

הזכות לפרטיות והגנתה תחת חוק הגנת הפרטיות הם כיום המכשיר עיקרי להגנה על מידע אישי, בהסדירם סוגיות ספציפיות בנוגע לאיסוף, לאחזקה ולשימוש במידע שבמאגרי מידע, וכן בהסדירם את ההעברה של מידע אישי בין גופים ציבוריים.[89] הסדרים אלה מבקשים לכאורה להפקיד בידי הפרט מושא המידע כלי לשליטה פעילה ביחידה האוטונומית שסביבו,[90] אף שבין תכליתם הנורמטיבית להצלחתם הפוזיטיבית יש עדיין מרחק רב.

איסוף, אחסון וניהול של נתוני מידע בנוגע לאישיותו של אדם, לצנעת אישיותו, למצבו הבריאותי, למצבו הכלכלי, להכשרתו המקצועית, לדעותיו או לאמונתו ב"מאגר מידע" שמוחזק בישראל כפופים להוראות פרק ב לחוק הגנת הפרטיות. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017,[91] שנכנסו לתוקפן במאי 2018, קובעות שלוש רמות של מאגרי מידע, שעליהן חלות רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים: רמת אבטחה בסיסית, רמת אבטחה בינונית ורמת אבטחה גבוהה. "מאגר מידע" מוגדר כ"אוסף

86 בירנהק **מרחב פרטי**, לעיל ה"ש 1, בעמ' 100; ס' 1 לחוק הגנת הפרטיות.

87 בירנהק, שם, בעמ' 232-235; ס' 13, 13א, 14 ו־16 לחוק הגנת הפרטיות.

88 בירנהק, שם, בעמ' 99.

89 ס' 7-17 ו־23 לחוק הגנת הפרטיות.

90 בירנהק, **מרחב פרטי**, לעיל ה"ש 1, בעמ' 91.

91 תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, ק"ת 7809 (להלן: תקנות אבטחת מידע).

של נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב", שאינו כולל אוסף פרטי שאיננו למטרות רווח.[92]

סעיף 11 לחוק מקים חובת יידוע שלפיה איסוף מידע במאגר מידע או שימוש בו מותנים ביידוע קודם של מושא המידע על אודות קיומה או היעדרה של חובה חוקית למסור את המידע, המטרה של מסירת המידע וייעודו של המידע הנאסף. בהתאם לעיקרון צמידות המטרה,[93] חובת היידוע נועדה להגן על מושא המידע מפני שימושים במידע שלא למטרה שלשמה נאסף. נוסף על כך, תקנות אבטחת המידע מפרטות אילו עניינים בעל מאגר מידע נדרש לפרט במסגרת מסמך מעודכן של הגדרות המאגר.[94] אלו כוללים גם פירוט של סוגי המידע הכלולים במאגר,[95] פרטים על העברה של מאגר המידע או שימוש בו מחוץ לגבולות ישראל,[96] פעולות לעיבוד מידע באמצעות מחזיק,[97] הסיכונים העיקריים של פגיעה באבטחת מידע ואופן ההתמודדות עמם,[98] וכן את השמות של מנהל מאגר המידע, מחזיק המאגר והממונה על אבטחת המידע בו אם מונה כזה.[99]

הבעיה היא שחובת היידוע מתגבשת כשיש "פניה לאדם לקבלת מידע", כלומר ברגע איסוף המידע.[100] בנקודת הזמן הראשונית הזו, הפוטנציאל הקונקרטי שגלום במידע שנאסף – מעבר להיותו חומר גלם כללי להפקת אפיון עתידי ביחס לסיכון או לסיכוי הטמון באדם – איננו ידוע.[101] פוטנציאל זה יתגלה רק בשלב מאוחר יותר, אם טכנולוגיות מתקדמות של כריית מידע יזהו את המידע הספציפי הזה כרלוונטי – בהינתן סך כל המידע האחר שנאסף – לזיהוי של תכונות או עניינים הקשורים במושא המידע.[102] אכן, פעולותינו במרחב הווירטואלי משאירות שובל של רסיסי מידע על אודותינו, ואלה יכולים להעיד על הרגלינו, העדפותינו ואורחות חיינו במגוון רב של הקשרים.[103] כך, למשל, חיבוב (like) בפייסבוק עשוי להצביע על עמדות פוליטיות, חיפוש של שיטת טיפול מסוימת במנוע החיפוש של גוגל עשוי ללמד על מצב בריאותי, רכישת פריטים באמזון עשויה ללמד על מעמד כלכלי ומענו של דואר

92 ס' 7 לחוק הגנת הפרטיות.

93 ראו ס' 2(9) ו־8(ב) לחוק הגנת הפרטיות.

94 תקנה 2(ב) לתקנות אבטחת מידע קובעת שבעל המאגר יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי באחד העניינים המפורטים בו, וכן יבחן את הצורך בעדכונו בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה אחת לשנה. כמו כן, תקנה 2(ג) לתקנות אבטחת מידע קובעת כי "בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר".

95 ס' 2(א)(3) לתקנות הגנת הפרטיות (אבטחת מידע).

96 שם, בס' 2(א)(4).

97 שם, בס' 2(א)(5).

98 שם, בס' 2(א)(6).

99 שם, בס' 2(א)(7).

100 ס' 11 לחוק הגנת הפרטיות.

101 Tene & Polonetsky, לעיל ה"ש 3, בעמ' 260.

102 Crawford & Schultz, לעיל ה"ש 6, בעמ' 106–107.

103 בירנהק **מרחב פרטי**, לעיל ה"ש 1, בעמ' 169.

אלקטרוני יכול להעיד על קשר חברתי מסוים.[104] רסיסי מידע אלו יכולים לשמש בהמשך לקבלת החלטות בקשר אלינו: האם להעסיק אותנו? האם לממן לנו הלוואה? האם להוזיל את פרמיית הביטוח שלנו? בעידן של נתוני עתק, היכולת של אוסף המידע לפרט למושא המידע מראש את רשימת השימושים האפשריים במידע על אודותיו היא מוגבלת מאוד. הדבר פשוט איננו צפוי.

על רקע זה, הגבלה של דרישת היידוע לרגע איסוף המידע עלולה לחתור תחת עקרון ההסכמה מדעת שנועד לאפשר לפרט לשלוט במידע על אודותיו. אם משמעותה האמתית של מסירת המידע יכולה להתברר רק בדיעבד,[105] אזי הסכמה מראש לאיסוף המידע איננה מאפשרת שליטה בגלגוליו השונים בדיעבד. לכאורה, אפשר לפרש את מועד התגבשותה של חובת היידוע בדרך אחרת, ולקבוע שבכל פעם שיעשה שימוש חוזר במידע תידרש הסכמה נוספת מצד מושא המידע. בהקשר זה יצוין כי תקנות אבטחת המידע קובעות שיש לעדכן את מסמך ההגדרות של מאגר המידע בכל עת שנעשה שינוי משמעותי באחד העניינים המפורטים בו; כן יש לבחון את הצורך בעדכונו בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה אחת לשנה.[106] כלומר, ככל שהשימושים הצפויים במידע שנאסף משתנים, בעל מאגר המידע נדרש לעדכן זאת במסמך הגדרות המאגר. גם בכך לא מתאפשרת שליטה מספקת בהחלטות שמקבלות על סמך ניתוח של נתוני עתק.

ראשית, כפי שטענו טנא ופולונטצקי (Tene & Polonetsky), למידע אינדיבידואלי העומד בפני עצמו אין בהכרח נפקות ממשית. החיבור בין פיסות המידע הרבות הוא שיוצר את התשתית הסטטיסטית להפקת הניבוי בנוגע לפרט. מכאן, שכדי שהפרט יוכל להסכים מדעת לשימוש נוסף במידע, עליו לדעת איזה משקל יינתן למידע זה במסגרת שכלול של כל פרטי המידע על אודותיו.[107] אולם, מי שקובע איזה משקל יינתן למידע הוא מי שמפתח את טכנולוגיות הניבוי – וזה איננו בהכרח בעל מאגר המידע או המחזיק בו, הכפופים לחובת היידוע. על פי רוב מדובר בחברות פרטיות שמנתחות מידע רב ומגוון הנאסף ממקורות שונים.[108] אמנם מסמך הגדרות המאגר אמור ליידע את מושא המידע אם המידע שנאסף על

---

104 עמיר פוקס "טרור ופרטיות: הצעה לחשיבה מחודשת על הכלים להתמודדות עם פעילות טרור באינטרנט" **המכון הישראלי לדמוקרטיה – פרטיות בעידן של שינוי** 231, 244 (תהילה שוורץ אלטשולר עורכת, 2012).

105 שם, בעמ' 107.

106 ס' 2(ב) לתקנות הגנת הפרטיות. כמו כן, ס' 2(ג) לתקנות קובע כי "בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר".

107 Tene & Polonetsky, לעיל ה"ש 3, בעמ' 261.

108 ראו, למשל, כיצד חברת הטכנולוגיה Palantir פיתחה טכנולוגיה תומכת אכיפה שרשויות רבות בארצות־הברית משתמשות בה. טכנולוגיה זו מבוססת על ניתוח נתונים המופיעים במאגרי מידע בנוגע לדוחות פשיעה ולוחיות זיהוי. ראו Mark Harris, *How Palantir Thiel's Secretive Data Company Pushed Into Policing*, Weird (Aug. 9, 2017), https://goo.gl/qncpqQ. אמנם כאשר הגוף מקבל ההחלטה הוא גוף ציבורי דוגמת רשות האכיפה, הרי הוא כפוף לכללי המשפט הציבורי ובכללם לחובת ההנמקה, ולכן הוא נדרש להסביר לפרט את ההחלטות שהוא מקבל בנוגע אליו. חרף זאת, כאשר הגוף שמעבד את המידע לשם הפקה של אמצעי ניבוי הוא גוף פרטי דוגמת פלנטיר, והמידע שהוא מעבד הוא מידע שנאסף על ידי אחרים והוא עצמו

אודותיו צפוי להיות מעובד על ידי גורם שלישי, שאינו מי שאסף את המידע מלכתחילה;[109] אולם יידוע כזה אינו שקול ליידוע הפרט על אופן השימוש במידע. כדי להחיל את חובת היידוע גם על צדדים אחרים בשרשרת השימוש במידע נדרשת פרשנות מרחיבה של בתי המשפט או של הרשות להגנת הפרטיות, פרשנות החורגת מלשונו המפורשת של חוק הגנת הפרטיות.[110] שנית, גם אם אפשר להרחיב את התחולה של חובת היידוע בנוגע לגורמים מאוחרים בשרשרת השימושים במידע, הדבר עלול להכביד יתר על המידה על אוספי המידע, הן מבחינה כלכלית והן מבחינה פרוצדורלית. מצב זה עלול ליצור תמריץ כלכלי שלילי לאיסוף מידע, תוך פגיעה ביתרונות הרבים הכרוכים בטכנולוגיות של נתוני עתק.[111]

מנגנון נוסף שנועד להגן על הפרט מפני שימושים פוגעניים במידע האישי שלו במסגרת פרק ב לחוק עוסק בזכות העיון.[112] ככלל, מושא המידע זכאי לעיין (בעצמו או באמצעות בא כוחו) במידע על אודותיו המוחזק במאגר מידע, אלא אם כן מדובר במידע הקשור למצבו הרפואי או הנפשי של הפרט ויש סיכון שגילויו יגרום לפרט נזק חמור (במקרה כזה יועבר המידע לרופא או לפסיכולוג מטעם מושא המידע).[113] זכות העיון אינה חלה על מאגרי מידע של רשויות ביטחון ואכיפת חוק.[114] אף שזכות העיון מתגבשת בנקודת זמן מאוחרת יותר – ובכך חורגת מרגע איסוף המידע, המתאפיין כאמור באי־ודאות לגבי השימושים האפשריים במידע – אין היא מבטיחה את שליטת הפרט בהחלטות שמתקבלות על סמך הצלבה וחיבור בין רסיסי מידע, שמקורם במאגרי מידע שונים ומגוונים. עיון במידע אישי המאוחסן במגוון רב של מאגרי מידע – גם אם הוא אפשרי מבחינה טכנולוגית (על ידי פיתוח אפליקציה שמנגישה לפרט את כל המידע שיש עליו במאגרי מידע, למשל) – איננו פותר את אתגר הפיקוח: ללא הסבר או הנמקה לגבי המשקל שניתן על אודות פרטי המידע

איננו כפוף לחובת היידוע שבחוק הגנת הפרטיות ואף לא לחובת ההנמקה שבמשפט הציבורי. ראו דיון בחלק ה להלן.

109 ס׳ 2(א)(5) לתקנות הגנת הפרטיות.

110 כך, למשל, בהנחיית רמו״ט, לעיל ה״ש 64, נקבע כי ״נקודת המוצא של הרשם היא כי כאשר מעביד מבצע את הליך גיוס העובדים בדרך של מיקור חוץ (outsourcing) באמצעות מכון המיון, ואפילו כאשר המעביד מעוניין כי משאבי האנוש שלו ינוהלו באופן מלא בחברת המיון – לא נוצרת מערכת יחסים נפרדת בין העובד לבין המכון, ובמונחי חוק הגנת הפרטיות, מכון המיון הוא מחזיק בלבד במידע״. אולם, מכוני המיון אכן עונים על ההגדרה של ״מחזיק מאגר מידע״ החלה על ״מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש״ (ס׳ 3 לחוק הגנת הפרטיות), שכן הם אוספים בעצמם מידע על המועמדים. לעומת זאת, מערכות אוטומטיות אחרות לניבוי עשויות לשכלל ניבויים על סמך מידע שאספו קודמיהם בלי לאסוף אותו בעצמם. במקרה כזה אי־אפשר לומר על הגופים שאוספים את הנתונים שהם עונים על ההגדרה של ״מחזיק, לענין מאגר מידע״. ראו גם Citron & Pasquale, *The Scored Society*, לעיל ה״ש 32, בעמ׳ 3–4.

111 Tene & Polonetsky, לעיל ה״ש 3, בעמ׳ 243–251 (שם הם מתארים את היתרונות של ניתוח נתוני עתק).

112 ס׳ 13 ו־13א לחוק הגנת הפרטיות.

113 שם, בס׳ 13(ג).

114 שם, בס׳ 13(ה).

ששוכללו והקריטריון שהכריע ביניהם, הפרט נותר חסר שליטה במידע שעל אודותיו. כאמור, עשויות להיות לכך השלכות הרות־גורל על זכויות אדם. כך, למשל, כאשר מצמצמים את מסגרת האשראי של הפרט על סמך שילוב מידע ממקורות מגוונים,[115] לרבות מידע על אודות המקומות שבהם הפרט מבצע את רכישותיו, המוצרים שהוא רוכש ופעילותו ברשתות חברתיות – עיון במאגרי המידע שעליהם התבססה ההחלטה לצמצם את מסגרת האשראי לא יועיל לו כדי לחשוף את הסיבה לצמצום פתאומי ובלתי־צפוי זה, ולכך יש כמובן השלכות ישירות על התנהלותו היום־יומית ועל אורחות חייו הבסיסיים.[116]

יתרה מזו, זכות העיון מופעלת כאמור כלפי בעלים או מחזיק של מאגר מידע ולא בהכרח כלפי גורמים מאוחרים יותר בשרשרת השימושים במידע, המדרגים את הפרט מושא המידע על סמך המידע שנאסף על אודותיו. אמנם רמו"ט, כשמה דאז (כיום – הרשות להגנת הפרטיות), הרחיבה בשנת 2012 את תחולתה של זכות העיון בהקשר הספציפי של שימוש במידע אישי על ידי מכוני מיון, וקבעה כי למועמד לעבודה תהיה זכות לעיון בתוצאות מבחני ההתאמה לעבודה;[117] אולם, בעקבות ההתנגדות שהביעו מכוני המיון למהלך זה[118] ריככה רמו"ט את דרישותיה הגורפות ופתחה צוהר ליישום סובייקטיבי וחלקי של הנחיותיה על ידי חברות ההשמה.[119] מכל מקום, אין בפרשנות מרחיבה כזו של זכות העיון כדי להבטיח את שליטתו של הפרט בהחלטות שמתקבלות לגביו על סמך דירוג שנשען על ניתוח של נתוני עתק. עיון בתוצאה, במיוחד כשמדובר בתוצאה סטטיסטית, איננו שקול להבנת ההיגיון שמאחוריה. כך, למשל, עיון בדירוג האשראי שייקבע לפרט עם כניסתו לתוקף של חוק נתוני אשראי, התשע"ו–2016, על ידי חברת אשראי פרטית, איננו שקול להבנת ההיגיון שבבסיס הדירוג. גם אם הדירוג יהיה שגוי, ללא הסבר על הקריטריון המכריע בתוצאה אין

115 Hurley & Adebayo, לעיל ה"ש 83, בעמ' 148.

116 שם.

117 לעניין זה קובעת הנחיית רמו"ט כי "למועמד הנבחן זכות לדעת מהו המידע על בסיסו התקבלה החלטת המעביד בהכרעה שקיבל לגביו, על מנת שיוכל להחליט כיצד להמשיך לפעול, ובמידה שירצה בכך, להעמידה למבחן משפטי, או לטעון כי התקבלה משיקולים זרים או מפלים. על מנת לאפשר מימושה של זכות זו, נדרש המועמד לקבל את המדע שנצבר אודותיו". לעיל ה"ש 64, בס' 2.7.2.

118 עניין **אדם מילוא**, לעיל ה"ש 62.

119 לפי ס' 2.7.5. להנחיית רמו"ט, מוטלת על המעביד חובה לאפשר לכל מועמד לעבודה "לקבל את חוות הדעת בדיוק כפי שנמסרה למעביד שהזמין את המבדקים"; אולם, נספח 1 להסכם הפשרה קובע את האפשרות להשמיט מחוות הדעת שתעמוד לעיון המועמד פרטים מסוימים דוגמת פרטים הנוגעים למעסיק הפוטנציאלי, מאפיינים ספציפיים של המשרה שבהקשרה נעשה האבחון ולניתוח מידת ההתאמה של תכונותיו ומאפייני אישיותו למשרה. על כך אפשר להוסיף כי יישום הנחיות קודמות של רמו"ט היה גם הוא מוגבל למדי: נועם שרביט "משרד המשפטים: נמחק מאגרי מידע של פילת בשל פגיעה בפרטיות המועמדים" **גלובס** 13.8.2008 https://goo.gl/xB7FWM (דיווח על ביטול רישומם של שני מאגרי מידע של פילת בשל הפרת זכות העיון); ראו גם חיים ביאור "מכוני מיון שקופים? אולי במאבק הבא" **גלובס** 14.3.2012 https://goo.gl/KMnPsc (לטענה כי יישום הנחיות רמו"ט איננו מבטיח שקיפות מספקת).

לפרט יכולת ממשית להשיג עליו ולשלוט על החלטות עתידיות (למשל, בנוגע לדיור או לתעסוקה) שיתקבלו לגביו על סמך דירוג זה.

גם הזכות לתיקון המידע שבסעיף 14 לחוק איננה מאפשרת לפרט שליטה מלאה בהחלטות המתקבלות על סמך ניתוח של נתוני עתק הואיל ותחולתה מוגבלת לתיקון או למחיקה של מידע "חלקי או שגוי". איזו תרופה תהיה לפרט שכל רסיס מידע שמסר הוא נכון כשלעצמו, אך החיבור בין רסיסי המידע מוציא אותו מהקשרו ויוצר החלטה שגויה לגביו?[120] הרי בפרשת **ביטון נ' סולטן** קבע בית המשפט העליון כי הוצאה מהקשר איננה עולה כדי פגיעה בפרטיות.[121] נחזור לדוגמת מכוני המיון וההשמה שהוזכרה לעיל. מועמד פוטנציאלי, המממש את זכותו לעיין בחוות הדעת של מכון המיון שאליו נשלח, עלול להיווכח שנתוני המידע על אודותיו נכונים – לרבות פרטיו האישיים, מצבו הכלכלי וניסיונו התעסוקתי – אך הניבוי שהתקבל על סמך השילוב ביניהם (למשל "התמדתו איננה בטוחה"[122]) איננו נכון. נניח כי ניבוי זה נבע מכך שלמידע על אודות מצבו המשפחתי של המועמד כהורה יחידני ניתן משקל מכריע במסגרת בחינת התאמתו למשרה. אף שמדובר באפליה אסורה,[123] למושא המידע אין דרך להשיג עליה אם לא יוסבר לו תחילה כי ניתן למצבו המשפחתי משקל מכריע במסגרת הערכת התמדתו. לכאורה, אפשר לטעון כי מאחר שהנטל להוכיח שלא מדובר באפליה רובץ על הנתבע,[124] יש למעביד תמריץ לוודא כי הניבוי שעליו הוא מסתמך איננו מפלה. אולם, בכך אין כדי להבטיח פיקוח מספק על החלטות המתקבלות על סמך שיקולים לא ענייניים. כל עוד המעביד אינו מחויב לנמק את החלטתו, אין כל ערובה שהמועמד יפנה לערכאות כדי להשיג על החלטה שאין הוא יודע כיצד התקבלה. משכך, זכות התיקון איננה מקנה לו יכולת לשלוט בהחלטה שלא להעסיקו, שהתקבלה על סמך ניתוח לא ענייני של פריטי המידע שלו.

חוק הגנת הפרטיות גם מבקש ליצור מנגנוני הגנה נגד הפצת מידע אישי על אודות הפרט, ואלה פורטו במסגרת תקנות אבטחת המידע שאוזכרו לעיל. החוק מגן מפני הפרת חובת הסודיות של מושא המידע,[125] במיוחד כשמדובר במידע השמור במאגר מידע. בנוגע לזה האחרון, סעיף 16 לחוק אוסר על כל מי שיש לו גישה כדין למאגר מידע לגלות את המידע שיש בו, אלא אם נעשה הגילוי לצורך עבודתו, לביצוע החוק או לביצוע של צו בית משפט. הבעיה היא שמנגנונים אוטומטיים לקבלת החלטות מבססים את החלטותיהם על הצלבה וחיבור בין פיסות מידע שחלקן נגישות לכול, דוגמת נתוני מידע פומביים המפורסמים ברשתות חברתיות או במאגרי מידע פומביים, ולכן חובת הסודיות איננה מבטיחה את שליטת הפרט בהחלטות שמתקבלות על סמך ניתוח של נתוני עתק. נוסף על כך, ככל שהמידע הוצלב על ידי חברות פרטיות העוסקות בהרכבה של מאגרי מידע אישיים המשמשים גופים

120 Ian Kerr & Jessica Earle, *Prediction, Preemption Presumption: How Big Data Threatens Big Picture Privacy*, 66 Stan. L. Rev. Online 65, 69 (2013).

121 רע"פ 9818/01 **ביטון נ' סולטן**, פ"ד נט(6) 554 (2005) (שם נקבע כי פרסום תמונה "תמימה" בהקשר פוגעני אינו עולה כדי פגיעה בפרטיות לפי ס' 2(4) ו־5 לחוק הגנת הפרטיות).

122 ראו דוח אבחון לדוגמה של מכון נועם https://bit.ly/2Gp7LxW.

123 ראו ס' 2(א)(1) לחוק שוויון ההזדמנויות בעבודה, התשמ"ח–1988, ס"ח 1240.

124 שם, בס' 9.

125 ראו ס' 2(7) ו־(8) לחוק הגנת הפרטיות.

ציבוריים,[126] דומה כי דרישת הסודיות לא תמנע את העברת המידע לגורמים הרלוונטיים, לפחות לא כשהוראות חוק מתנגשות מתירות לכאורה לגוף הציבורי לקבל מידע הדרוש לו לביצוע תפקידו. על כך יעידו פרשיות רכישה של נתוני תקשורת מחברות סלולר על ידי הלשכה המרכזית לסטטיסטיקה, במטרה לאסוף ולנתח מידע אישי על אזרחי המדינה כבסיס לקבלת החלטות על ידי המדינה.[127]

לבסוף, פרק ד לחוק מסדיר את אופן המסירה של מידע או של ידיעות על ענייניו הפרטיים של אדם שנאספו על־ידי גופים ציבוריים,[128] ובזאת בדיוק חולשתו: החלטות שבעבר התבססו על מידע רגיש שמקורו במאגרי מידע ציבוריים מתקבלות כיום על סמך ניתוח של נתוני עתק שמקורם במאגרי מידע פרטיים לחלוטין. כך, למשל, פרמיית הביטוח הרפואי של הפרט נקבעת כיום על סמך שקלול של נתוני מידע על אודות הרגלי הצריכה של הפרט, פעילותו ברשתות החברתיות, תכניות הטלוויזיה שבהן הוא צופה ורמת המשכל שלו,[129] ולא בהכרח על סמך מידע רפואי מסורתי על אודותיו המופיע במאגרי מידע ציבוריים. אולם, שלא כמו מידע רפואי שמסירתו כפופה להגבלות מחמירות הקבועות בחוק[130] ובתקנות,[131] העברה של נתוני המידע מידיים פרטיות אינה כפופה כאמור להגבלות אלה.

---

126 Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People"*, Colum. Bus. L. Rev. 950, 951-52, 990-99 (2009).

127 עומר כביר ואלירן מלכי "פגיעה חמורה בפרטיות: המדינה קונה את המידע שלכם מחברות הסלולר" **כלכליסט** 22.11.2015. www.calcalist.co.il/internet/articles/0,7340,L-3674012,00.html/ (פרשיות אלה עסקו בעסקאות שנרקמו בין הלשכה המרכזית לסטטיסטיקה לחברות סלולר, לרבות בזק, סלקום, פלאפון, גולן טלקום ו־HOT, שבהן רכשה הלשכה מידע מזהה על לקוחות שמשייך בין מספרי הטלפון שלהם למספרי תעודת הזהות שלהם. הלשכה טענה שהיא פועלת כדין מאחר שפקודת הסטטיסטיקה מסמיכה אותה לקבל מידע הדרוש לה לשם ביצוע תפקידה. הבעיה היא שהמידע שנרכש היה מידע אישי מזהה ולא מידע סטטיסטי, ולפיכך בעצם העברתו חברות הסלולר מפֵרות את חובת הסודיות המוטלת עליהן מכוח חוק הגנת הפרטיות).

128 העברת מידע בין גופים ציבוריים וההגבלות עליה מוסדרים – נוסף על ההסדר הכללי שבחוק הגנת הפרטיות ובתקנות שלפיו – גם בשורה של דברי חקיקה ספציפיים, הנוגעים לסוגי מידע או לגופים מסוימים, לדוגמה פרק ה לחוק מרשם האוכלוסין, התשכ"ה–1965, ס"ח 466; חלק י"ב לפקודת מס הכנסה [נוסח חדש], התשכ"א–1961, נ"ח 6; ס' 17–20 לפקודת הסטטיסטיקה [נוסח חדש], התשל"ב–1972, נ"ח 24; ס' 19–20 לחוק זכויות החולה, התשנ"ו–1996, ס"ח 1591.

129 Marshall Allen, *Health Insurers Are Vacuuming Up Details about You – And it Could Raise Your Rate*, NPR (July 17, 2018), https://n.pr/2Gs5Nga.

130 נוסף על הוראות פרק ד, החלות על מידע רפואי המוחזק במאגרי מידע ציבוריים, ראו גם ס' 13(ג) לחוק שלפיו "בעל המאגר רשאי שלא למסור למבקש מידע המתייחס למצבו הרפואי או הנפשי אם לדעתו עלול המידע לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו". כן ראו הוראות ס' 19–20 לחוק זכויות החולה.

131 תקנה 1(3)(ב) לתוספת הראשונה לתקנות אבטחת הפרטיות קובעת שעל מאגר מידע הכולל מידע רפואי תחול רמת אבטחה בינונית, וככל שיש במאגר כזה מידע על אודות מאה אלף אנשים ומעלה – תחול עליו רמת אבטחה גבוהה לפי האמור בתקנה 1(1) לתוספת השנייה

אכן, היכולת להשתמש במידע שאספו גופים פרטיים חיונית לא פחות מהשימוש במידע שאספו גופים ציבוריים לקבלת החלטות בנוגע לפרט. משכך, מכירת מידע אישי על ידי גופי ביניים נהפכה לעסק של ממש:[132] גוף הביניים אוסף מידע הנוגע למשתמשים; פיסות המידע מוצלבות ליצירת פרופיל באמצעות טכנולוגיות של נתוני עתק; הפרופיל נמכר לצדדים שלישיים כמו חברות פרסום המבצעות פרסום ממוקד.[133] מושאי המידע מוסרים מידע תמורת אינטראקטיביות – שירות שלכאורה ניתן חינם (אולם התשלום האמתי עבורו הוא במידע)[134] – והגדלה של היצע השירותים והמוצרים,[135] וגופי הביניים מוכרים מידע של משתמשים תמורת כסף.

כל עוד הסוגיה של מסירת מידע שנאסף על ידי גופים פרטיים איננה מוסדרת בחוק, יש חשש רציני שהמידע יועבר לשם קבלת החלטות מפוקפקות בנוגע לפרט. פרשת פייסבוק-קיימברידג׳ אנליטיקה ממחישה זאת היטב: איסוף של מידע פרטי מפייסבוק על ידי חברת קיימברידג׳ אנליטיקה אִפשר למועמדים רפובליקנים, בבחירות לנשיאות בשנת 2016, לנהל את אסטרטגיית התעמולה שלהם באופן אידאלי; יש הסבורים שאף הוביל הלכה למעשה לניצחונם בבחירות.[136] העברת מידע שמשקף לכאורה עמדות פוליטיות של משתמשים למעשה שימשה גורמים שלישיים כדי לעצב את תודעתם, בניגוד לרצונם החופשי.

לבסוף, הטלת הגבלות על העברה של מידע אישי – גם אם תורחב תחולתן למידע הנמצא בידיים פרטיות – אינה מספקת מענה הולם לפיקוח על החלטות שמתקבלות על סמך מידע זה. בדומה לקוצר ידם של עקרונות ההסכמה מדעת וצמידות המטרה בהקשר זה, פרק ד לחוק מתמקד גם הוא בשלב שבו המידע מועבר ואינו חל על השלב שבו המידע נתון לעיבוד לשם קבלת החלטות בנוגע לפרט מושא המידע. לכן, גם כשמתאפשר לפרט לשלוט במכירת המידע שלו לצדדים שלישיים – אם באמצעות פרשנות משפטית או רגולציה שמכירות בזכות כזו ואם באמצעות כוחות השוק שמאפשרים לו לשלם עבור שליטה כזו[137] – עדיין אין בכך כדי להקנות לו שליטה בהחלטות שמתקבלות על סמך המידע שהסכים למכור לצדדים שלישיים.

לתקנות האבטחה; ראו גם תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ״ו-1986, ק״ת 858.

132 Mark Hachman, *The Price of Free: how Apple, Facebook, Microsoft and Google sell you to advertisers*, PC World (Oct. 1, 2015), https://bit.ly/2hBxALN.

133 Candice L. Kline, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. Tol. L. Rev. 443, 447 (2008).

134 Jonathan Zittrain, *Meme patrol: "When Something Online is Free, You're Not the Customer, You're the Product"*, The Future of the Internet (Mar. 21, 2012), https://goo.gl/JK4B31.

135 עמיחי־המבורגר ופרז, לעיל ה״ש 23, בעמ׳ 207.

136 Jake Canter, *Cambridge Analytica bosses were secretly filmed boasting about how they helped Trump win the US election*, Business Insider (Mar. 20, 2018), https://read.bi/2EWcaCB.

137 ראו, למשל, את מודל Transactional Privacy שנועד ליצור מנגנון לתמחור המידע האישי, Christopher Rider et al., *For Sale: Your Data, By: You*, https://goo.gl/56nDhn.

מן האמור עולה כי גישת הפרטיות כשליטה יכולה לספק עוגן מושגי לפיתוח אמצעי לפיקוח על החלטות המתקבלות בנוגע לפרט על בסיס ניתוח של נתוני עתק, אולם ההסדרים שבחוק הגנת הפרטיות, במתכונתם הנוכחית, אינם מאפשרים זאת מבחינה מהותית. שליטת הפרט בהחלטות שמתקבלות על סמך המידע האישי שלו מותנית ביכולתו להבין את ההיגיון שבבסיס החלטות אלה, כדי שיוכל לערער עליהן ולדרוש את תיקונן במקרה הצורך.[138] בהמשך אציע להטיל חובה על גופים פרטיים, שמקבלים החלטות בנוגע לפרט על סמך ניתוח של נתוני עתק: החובה להסביר לפרט איזה מידע שימש לקבלת ההחלטה ומה היה הקריטריון המכריע.

ה. תשתית לפיתוח כלי משפטי להשגת שליטה על החלטות המתבססות על ניתוח של נתוני עתק

בחלק אחרון זה של המאמר איעזר בזכות למתן הסבר שהוכרה לאחרונה במסגרת ה־GDPR כדי ליצור תשתית ראשונית לפיתוח כלי משפטי, תחת המבנה המושגי של הזכות לפרטיות כשליטה, שבאמצעותו יוכל הפרט לשלוט בהחלטות המתקבלות בקשר אליו על סמך ניתוח של נתוני עתק. תשתית זו מבוססת על הרחבת תחולתה של חובת ההנמקה שבמשפט הציבורי גם להחלטות שגופים פרטיים מקבלים כאמור בנוגע לפרט.

1. העקרונות המנחים

חובת ההנמקה ממוקמת בסִפְרה הציבורית. היא נגזרת מחובת הנאמנות הציבורית: אין לו למְנהל הציבורי אלא מה שהציבור העניק לו ואין הוא רשאי להשתמש בסמכויותיו אלא לטובת הציבור.[139] חובת ההנמקה היא אבן יסוד בתורת המִנהל הציבורי.[140] היא מאפשרת לו להגשים את תכליתו – לשרת את הציבור בנאמנות.[141] מקורה הסטטוטורי של חובת ההנמקה נעוץ בחוק לתיקון סדרי המינהל (החלטות והנמקות), התשי"ט–1958[142] (להלן: "חוק ההנמקות"), המחיל חובת הנמקה על עובדי ציבור. עם זאת, דברי חקיקה נוספים מטילים חובות הנמקה בהקשרים ספציפיים יותר.[143] הטעמים לחובת ההנמקה מגוונים.[144] ראשית, חובת ההנמקה

138 Article 29 Data Protection Working Party 17/EN WP260, **בעמ' 19, 27 ו־35** (הנחיות ה־Working Party **בנוגע ל־**GDPR **ולזכות לקבל מידע שהוכרה במסגרתו**); Margot E. Kaminski, *The Right to Explanation, Explained,* 34 Berkeley Tech. L.J. (forthcoming, 2019), https://goo.gl/SrSZ9P.

139 **בג"ץ 142/70 שפירא נ' הועד המחוזי של לשכת עורכי הדין, ירושלים**, פ"ד כה(1) 325, 331 (1971).

140 **רע"א 8996/04 שכטר נ' נציגות הבית המשותף**, פ"ד נט(5) 17, פס' 20–21 לפסק דינו של השופט רובינשטיין (2004).

141 **בג"ץ 143/56 אחג'יג' נ' המפקח על התעבורה**, פ"ד יא 370, 371 (1957).

142 חוק לתיקון סדרי המינהל (החלטות והנמקות), התשי"ט–1958, ס"ח 264 (להלן: חוק ההנמקות).

143 ראו, למשל, **ס' 33(ו)** לחוק הנכים (תגמולים ושיקום) [נוסח משולב], התשי"ט–1959, ס"ח 295; **ס' 75(ג)** לחוק המקרקעין, התשכ"ט–1969, ס"ח 575; **ס' 40** לחוק בתי דין מינהליים, התשנ"ב–1992, ס"ח 1385.

144 יואב דותן "חובת ההנמקה של רשויות מינהל וגופים נבחרים" **מחקרי משפט** טו 5 (2002).

מאפשרת ביקורת על החלטות מנהל ותקיפה שלהן.[145] ההנמקה חיונית כדי לאפשר לאזרח הנוגע בדבר לערער עליה או לעתור נגדה לערכאות.[146] ההנמקה גם מסייעת לממונים על הרשות המנהלית לוודא שהיא מפעילה את סמכותה בהתאם למדיניות רשמית או להנחיות של הממונים.[147] שנית, חובת ההנמקה תורמת לאיכות ההחלטה ומשפרת את דרכי פעילותו של מקבל ההחלטה.[148] במיוחד, ההנמקה יוצרת מנגנון ביקורת עצמי לפני קבלת ההחלטה; ביקורת כזו מקטינה את החשש מפני החלטות שרירותיות או שגויות.[149] שלישית, לחובת ההנמקה יש ערך מרכזי בשמירה על אמון הציבור במנהל הציבורי.[150] לבסוף, היא משרתת גם את הצורך הרגשי של הפרט לקבל הסבר על החלטות מנהליות שמתקבלות בענייניו, וזאת ללא קשר לשאלה אם מדובר בהחלטה נכונה אם לאו.[151]

ככלל, גופים פרטיים אינם כפופים לכללי המנהל הציבורי; ההנחה היא שהם פועלים לפי כללי ההיצע והביקוש כדי לספק באופן תקין ויעיל את צורכי הציבור.[152] עם זאת, יש מקרים שבהם חובת הנאמנות הציבורית – וכפועל יוצא גם חובת ההנמקה – יזלגו לספֵרה הפרטית. במיוחד כך כשגוף פרטי ממלא תפקיד בעל אופי ציבורי (כמו חברת חשמל או חברה קדישא, למשל) ונחשב לגוף דו־מהותי הכפוף לדואליות נורמטיבית.[153] נוסף על כך, כשגוף פרטי ממלא תפקיד על פי דין, ראוי לחייבו בהנמקה מאחר שבהפעלת סמכותו גם הוא נחשב לרשות מנהלית.[154] לבסוף, אפשר להזרים ערכי יסוד מהמשפט הציבורי, לרבות חובת ההנמקה, אל תוך המשפט הפרטי, באמצעות דוקטרינות של משפט פרטי דוגמת עקרונות תום הלב ותקנת הציבור.[155]

האם עקרונות אלה מאפשרים להחיל את חובת ההנמקה הציבורית על גופים פרטיים שמקבלים החלטות בנוגע לפרט על סמך ניתוח של נתוני עתק? ככלל יודגש כי החלה של חובת הנמקה ציבורית על גופים פרטיים איננה חריגה בנוף המשפטי בישראל. כך, למשל,

145 שם, בעמ' 7.

146 יצחק זמיר **הסמכות המינהלית** כרך ב 1269 (מהדורה שנייה מורחבת, 2011).

147 שם.

148 דותן, לעיל ה"ש 144, בעמ' 7.

149 עע"מ 9135/03 **המועצה להשכלה גבוהה נ' הוצאת עיתון הארץ**, פ"ד ס(4) 217 (2006); בג"ץ 3734/14 **פלוני נ' ראש ממשלת ישראל** (פורסם בנבו, 17.11.2015); זמיר **הסמכות המינהלית** כרך ב, לעיל ה"ש 146, בעמ' 1269.

150 דותן, לעיל ה"ש 144, בעמ' 9.

151 שם.

152 יצחק זמיר **הסמכות המנהלית** כרך א 33 (מהדורה שנייה מורחבת, 2010).

153 שם, בעמ' 49, 524; ע"א 10419/03 **דור נ' רמת הדר – כפר שיתופי להתיישבות חקלאית בע"מ**, פ"ד ס(2) 277, 288 (2005).

154 ס' 2א לחוק ההנמקות קובע כי חובת ההנמקה חלה על "עובד ציבור". ס' 1 לחוק זה מגדיר כי "עובד ציבור" הוא "עובד־מדינה, עובד רשות מקומית וכן כל רשות שהוענקה לה סמכות על פי דין". יצחק זמיר מפרש הגדרה זו בהרחבה וקובע כי היא חלה גם על גוף פרטי שהוענקה לו סמכות על פי דין. ראו זמיר **הסמכות המינהלית** כרך ב, לעיל ה"ש 146, בעמ' 1274.

155 ע"א 294/91 **חברה קדישא גחש"א "קהילת ירושלים" נ' קסטנבאום**, פ"ד מו(2) 464, 532 (1992).

החוק לתיקון פקודת האגודות השיתופיות (מספר 8), התשע"א-2011 מחיל חובת הנמקה סטטוטורית על ועדות הקבלה של יישובים קהילתיים;[156] וחוק חוזה הביטוח, התשמ"א-1981 מחייב את חברת הביטוח לגבש עמדה ברורה בשאלת החבות,[157] וזו פורשה כחובה למסור למבוטח הודעה מנומקת בדבר הסיבות לדחיית התביעה.[158] יתרה מזו, דומה כי האיחוד האירופי סבר שלצורך מתן הסבר על החלטות שמתקבלות בנוגע לפרט על סמך מנגנונים אוטומטיים, אין צורך להבחין בין גופים פרטיים לגופים ציבוריים.[159] לדעתי, יש מקום לאמץ גישה כזו בדין הישראלי.

ראשית, קבלת החלטות על סמך ניבוי סטטיסטי שהפיקה רשות פרטית, הפועלת על פי סמכות שבדין,[160] כפופה לפי גישתו של זמיר להנמקה לפי חוק ההנמקות[161] ולעתים גם לפי החוק הספציפי שמסדיר את פעילותה.[162] שנית, ככל שמקבל ההחלטה כפוף לעקרונות ציבוריים בהיותו גוף דו־מהותי, ודאי שהדרישה להנמקה מתבקשת. כך, למשל, בכל הנוגע לפעילותה של אוניברסיטה כמעסיקה, נקבע כי יחולו עליה בהתאמה הנדרשת לעניין הכללים המחייבים את הרשות המנהלית, לרבות גילוי מסמכים ומתן זכות לנפגע מהחלטתה לעיין בהם.[163]

לגבי גופים פרטיים מובהקים – דוגמת חברות לפרסום ממוקד, המתאימות פרסום שיווקי, עסקי או תעסוקתי לפרופיל הדיגיטלי של המשתמש, או חברות דירוג המדרגות את

156 ס' 36(ג) לפקודת האגודות השיתופיות התשי"א-1951, ס"ח 225.

157 ס' 23 לחוק חוזה ביטוח, התשמ"א-1981, ס"ח 1005.

158 ראו, למשל, ת"א (שלום, ראשל"צ) 2225/04 **הורוביץ הפקות בע"מ נ' כלל חברה לביטוח בע"מ** (פורסם בנבו, 4.4.2006) ("ס' 23 לחוק חוזה הביטוח מחייב את חברת הביטוח להידרש לפניית המבוטח ולגבש עמדה ברורה בשאלת החבות. מקום בו החליטה חברת הביטוח לדחות את תביעת המבוטח – כולה או מקצתה – עליה לנמק את הדחייה בגלוי ובאופן מנומק. חובת ההנמקה נלמדת מס' 23 עצמו").

159 ראו, למשל, הערת פתיח 71 ל־GDPR, הקובעת כי פרט הכפוף להחלטות אוטומטיות, המתקבלות על סמך עיבוד של מידע אישי, זכאי לקבל הסבר אם ההחלטה תחול בנוגע להחלטות שמשפיעות עליו משמעותית, לרבות החלטות של חברות אשראי וחברות לאיתור וגיוס עובדים, שהן גופים פרטיים ("The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, *such as automatic refusal of an online credit application or e-recruiting practices* without any human intervention").

160 כגון חברה לדירוג אשראי, הקובעת את דירוג האשראי של אזרחי ישראל מכוח חוק הסדרת פעילות חברות דירוג האשראי; ראו לעיל ה"ש 33.

161 ראו את פרשנותו המרחיבה של זמיר **הסמכות המינהלית** כרך ב, לעיל ה"ש 146.

162 ראו תקנה 17 לתקנות הסדרת פעילות חברות דירוג האשראי, תשע"ה-2014, ק"ת 7465, המפרטת איזה מידע נלווה תפרסם חברת הדירוג בדו"ח הדירוג: מידע כללי, מידע ששימש בתהליך הדירוג ומידע שנוגע לשיטת ההערכה.

163 ע"ע (ארצי) 1185/04 **אוניברסיטת בר אילן נ' קיסר** (פורסם בנבו, 24.3.2005); ע"ע (ארצי) 371/05 **עוז נ' אוניברסיטת חיפה**, פס' 10–11 לפסק דינה של השופטת נילי ארד (פורסם בנבו, 19.12.2005).

איכות השירות שהפרט מציע – הדרישה להנמקה מוצדקת כאמצעי לפיקוח ובקרה (ראו לעיל הטעם הראשון לחובת ההנמקה). היא חיונית כדי לאפשר למושא המידע להזים טעויות בניבוי שהופק לגביו ולהשיג על החלטות שגויות שהתקבלו בנוגע אליו על בסיסו.[164] כמו כן, חובת הנמקה מאפשרת פיקוח רגולטורי מצד רשויות המנהל,[165] במיוחד הרשות להגנת הפרטיות המופקדת "על הגנת המידע האישי במאגרי מידע דיגיטליים ועל ביצורה של הזכות לפרטיות", תוך שהיא "מפעילה רגולציה, לרבות אכיפה מנהלית ופלילית, על כלל הגופים בישראל – פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי דיגיטלי".[166] כדי לממש את תכליתה ולוודא כי יש למושא המידע שליטה ממשית ואפקטיבית במידע על אודותיו, בכל שלבי התגלגלותו, לרבות בשלב שבו הוא משמש לקבלת החלטות בנוגע לפרט – על הרשות להגנת הפרטיות להבין כיצד המידע מתגלגל ובאיזה אופן הוא מעובד לשם הפקת ניבוי סטטיסטי בנוגע לפרט מושא ההחלטה.

חובת הנמקה ציבורית תחייב את מקבלי ההחלטות לאמץ מנגנוני ניבוי הניתנים להסבר אנושי, ואלו בהמשך יפעילו את לחצם על אנשי הטכנולוגיה להמשיך ולהשקיע בפיתוח מנגנונים כאלה. אכן, היכולת הטכנולוגית לפתח מנגנונים אלגוריתמיים לקבלת החלטות, המבוססים על היגיון הניתן להסבר אנושי, הולכת ומשתכללת.[167] כך, במיוחד, אנשי טכנולוגיה מסוגלים כבר היום להסביר החלטות מסוימות של אלגוריתמים ללא צורך בחשיפה של מנגנון ההחלטה עצמו, שכאמור עשוי להיות מוגן כסוד מסחרי.[168] עיצוב של מנגנוני ניבוי שאפשר להסביר יגביר את רמת הדיוק שלהם: מקבלי ההחלטות יהיו חייבים לדעת אילו פריטי מידע הובאו בחשבון ובאיזה אופן, וכפועל יוצא מכך יהיה קל יותר לזהות הזנה של מידע שגוי או מוטה, כמו גם הסתמכות על שיקולים לא ענייניים (ראו לעיל הטעם השני לחובת ההנמקה). מנגנוני ניבוי מדויקים הם כמובן גם יעילים ומבוקשים יותר, דבר שעולה בקנה אחד עם שאיפתם העסקית של גופים פרטיים להשיא את רווחיהם.

נוסף על כך, עיצוב של מנגנוני ניבוי באופן המתיישב עם חובת ההנמקה יגביר את אמון המשתמשים במגוון המוצרים והשירותים הטכנולוגיים שסביבם ויבטיח המשך צמיחה של כלכלת המידע (ראו לעיל הטעם השלישי לחובת ההנמקה). ככל שהציבור יבין שיש בידיו אפשרות ממשית לשלוט בהחלטות שמתקבלות בנוגע אליו על סמך ניתוח המידע האישי שלו, יש לשער כי יפחת החשש הגובר מפני שימוש בספקי שירותים ובטכנולוגיות אוספות

164 ראו לעיל ה"ש 39.

165 זמיר **הסמכות המנהלית** כרך א, לעיל ה"ש 152, בעמ' 49.

166 ראו אתר הרשות להגנת הפרטיות https://goo.gl/FPZwz8.

167 Doshi-Velez & Kortz, לעיל ה"ש 67, בעמ' 6.

168 Marco Tulio Ribeiro et al., *Why Should I Trust You?: Explaining the predictions of any classifier*, Cornell University Library (Aug. 9, 2016), https://goo.gl/cWk5iu; Tao Leiet al., *Rationalizing Neural Predictions*, Cornell University Library (Nov. 2, 2016), https://goo.gl/TcrtRB; Philip Adler et al., *Auditing Black-Box Models for Indirect Influence in Data Mining,* Springer Link (Oct. 25, 2017), https://goo.gl/KZNJ4w; Malgieri & Comand, לעיל ה"ש 3, בעמ' 249.

מידע.[169] לבסוף, ביסוס של חובת הנמקה בהקשר הנדון ללא ספק תשרת את הצורך הרגשי של הפרט לדעת שהוא נחשב, ושהחלטות המשפיעות על חייו אינן מתקבלות באופן שרירותי אלא על סמך היגיון ושקילה (ראו הטעם הרביעי לחובת ההנמקה).

2. תוכנה של חובת ההנמקה

חוק ההנמקות אינו מסביר איזו מידת פירוט דרושה לשם הנמקה,[170] אולם הפסיקה מראה שהדבר תלוי בנסיבות.[171] ההנמקה צריכה להעמיד את מושא ההחלטה במצב שבו הוא יוכל להעמידה לביקורת ולערעור.[172] לשם כך יש לפרט את הפרמטרים המרכזיים של קבלת ההחלטות כמו גם את הנתונים העובדתיים העיקריים שעליהם התבססה.[173] בכל מקרה, הרשות המנהלית אינה יכולה לעמוד בחובתה באמצעות הנמקה כללית וסתמית, תוך ציון "הכותרת" של טעמיה ובלא להתייחס לנסיבות המקרה.[174]

עקרונות אלה יכולים לשרת אותנו נאמנה בבואנו להרחיב את תחולתה של חובת ההנמקה הציבורית גם לגופים פרטיים המקבלים החלטות הנוגעות לפרט על בסיס ניתוח של נתוני עתק. כדי שמושא המידע יוכל לפקח על החלטות המתקבלות בקשר אליו על סמך מידע אישי שנוגע לו, עליו לקבל הסבר הולם על אודות הניבוי הסטטיסטי שביסס את ההחלטה – כזה שיאפשר לו להשיג עליה.[175] הסבר הולם יכלול את מקורות המידע ואת הסטטיסטיקות שבהם

---

169 ראו, למשל, את הקמפיין הציבורי להתנתקות מפייסבוק שהגיע בעקבות פרשת קיימברידג'־אנליטיקה. הקמפיין מעיד שכאשר הציבור חש שהוא מאבד שליטה במידע האישי שלו, הוא בוחר להימנע משימוש בטכנולוגיות שאוספות עליו מידע. מכאן אפשר להסיק כי תחושת השליטה במידע אישי היא חיונית עבור צרכנים של שירותים מקוונים המוסרים מידע אישי תמורת השירות שהם מקבלים. ראו, למשל, Andrew Griffin, *Delete Facebook Campaign Takes Off – But Actually Removing Your Data .Might Prove More Difficult than it Seems, Independent*, Independent (Mar. 21, 2018), https://ind.pn/2NxKLv3.

170 דותן, לעיל ה"ש 144, בעמ' 19–20.

171 ראו, באופן כללי, ע"א 668/89 **פאר נ' חברת בית פרישמן 38 בע"מ (בפירוק מרצון)**, פ"ד מד(4) 693, 697 (1990); ע"א 30/56 **בן חרוש נ' קצין התגמולים**, פ"ד י 931, 932 (1956) ("עניין שהעדויות בו מועטות, העובדות ברורות ושאלות התיק אינן מסובכות, אין מן ההכרח להרחיב עליו את הדיבור, וועדת ערעור יוצאת ידי חובתה בהסבירה קצרות שאין היא משוכנעת באמיתות גרסתו של המערער או של המשיב. אך לא כך הדבר כשעצם אי השכנוע טעון הנמקה"). במקרים שבהם ההחלטה כוללת רכיבים חסויים קבע בית המשפט כי נדרשת הנמקה מפורטת, הכוללת את כל החומרים הגלויים שאפשר לגלות לפונה. ראו עניין **פלוני נ' ראש ממשלת ישראל**, לעיל ה"ש 149; בג"ץ 9343/11 **פלוני נ' ועדת המאוימים** (פורסם בנבו, 7.3.2012).

172 בג"ץ 6728/06 **עמותת "אומץ" אזרחים למען מינהל תקין וצדק חברתי נ' ראש ממשלת ישראל**, פס' 17 לפסק דינה של השופטת נאור (פורסם בנבו, 30.11.2006).

173 דותן, לעיל ה"ש 144, בעמ' 37.

174 עניין **המועצה להשכלה גבוהה**, לעיל ה"ש 149, בעמ' 247 ("רשות ציבורית אינה רשאית להסתפק בסירוב לקוני לבקשה למסירת מידע ועליה לפרט את הטעמים לכך כדי לאפשר למבקש המידע לעמוד על טעמים אלה ולשקול את מהלכיו").

175 Kaminski, לעיל ה"ש 138, בעמ' 20.

נעשה שימוש, את הסיבה שבגללה הניבוי רלוונטי להחלטה ואת האופן שבו שימש לקבלת ההחלטה.[176] כפי שעולה מחוות הדעת של קבוצת המומחים האירופית להגנת מידע אישי, בנוגע לזכותו של הפרט לקבל הסבר על אודות החלטות אוטומטיות המתקבלות ביחס אליו תחת ה־GDPR, הנמקה הולמת אמורה לספק לפרט מושא ההחלטה הסבר ברור, משמעותי וממצה על אודות ההחלטה שהתקבלה בעניינו; כלומר אילו פרטי מידע הובאו בחשבון ואיזה קריטריון היה המכריע.[177] הנמקות מסורבלות, שמציפות את מושא ההחלטה במידע חסר תועלת; הנמקות מסובכות מעבר לדרוש או הנמקות המחייבות פרק זמן לא הגיוני כדי לקרוא אותן אינן מאפשרות לפרט לפעול על פיהן ומשכך אינן הולמות.[178] בעידן של ייצור מידע בלתי־מוגבל, שקיפות חסרת רסן מובילה לבעיה שעומרי בן שחר וקרל שניידר (Ben-Shahar & Shneider) כינו "too much information", המכרסמת בתכלית השקיפות ככלי מרכזי להגנה על אוטונומיית הפרט.[179] לפיכך, הנמקה יעילה צריכה להיות כזו שמשקפת את ההיגיון שבבסיס ההחלטה – ובו בזמן איננה מציפה את מושא ההחלטה במידע שאיננו חיוני להבנת היגיון זה. העובדה שההיגיון שמבסס את הניבויים הסטטיסטיים המשמשים לקבלת החלטות בנוגע לפרט מושא המידע הוא מורכב, אין משמעה שאי־אפשר לעצבו מראש באופן שיאפשר להסבירו.[180] גם אינפורמציה מורכבת ניתנת להנגשה.[181]

יודגש כי רצוי שלא לקבוע סטנדרט אחיד של הנמקה, שאיננו תואם לאופי הדינמי של הסביבה הטכנולוגית שאליה הוא מכוון. כך, למשל, ככל שהקריטריונים ששימשו לקבלת ההחלטה חסויים[182] או מוגנים תחת דיני הסוד המסחרי,[183] ייתכן שיהיה ראוי שלא לכוללם במסגרת ההנמקה. הרשות להגנת הפרטיות או בית המשפט יידרשו לבצע איזון הולם ועדכני

176 שם, בעמ' 22.

177 שם, בעמ' 27, "The controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision".

178 Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability*, 20 New Media & Soc. 973, 977 (2016); Jennifer Shkabatur, *Transparency With(out) Accountability, Open Government in the United States,* 31 Yale L. & Pol'y Rev. 79, 84 (2012).

179 Omri Ben-Shahar & Carl E. Shneider, *The Failure of Mandated Disclosure*, 159 U. Pa. L. Rev. 647, 647 (2011).

180 ראו עניין **רמת הדר**, לעיל ה"ש 153, בעמ' 287–288.

181 Randall Monroe, Thing Explainer: Complicated Stuff in Simple Words (2015).

182 ראו, למשל, בג"ץ 4458/03 **פלונים נ' ראש ממשלת ישראל** (פורסם בנבו, 22.6.2005); בג"ץ 6230/08 **פלונים נ' ראש ממשלת ישראל** (פורסם בנבו, 20.9.2010); בג"ץ 1907/05 **פלוני נ' ראש ממשלת ישראל** (פורסם בנבו, 2.2.2012) (בפרשות אלה נקבע כי הקריטריונים שלפיהם מתקבלות החלטות בוועדת המאוימים ובמנהלה הביטחונית לסיוע הם חסויים ולכן המדינה אינה מחויבת בחשיפתם).

183 הנחיית רמו"ט, לעיל ה"ש 64, בעניין מכוני המיון וההשמה ועדכונה לאחר הסכם הפשרה שהושג בין המכונים לרשם מאגרי המידע משאירה בידי המכונים שיקול דעת להשמיט פרטים מסוימים מחוות הדעת שתעמוד לעיון הנבחן, למשל מידע על סוג המבחנים ותוכנם (ס' 2.7.7.1.) או

בין זכות המשתמשים לפרטיות לבין אינטרסים ציבוריים מתנגשים דוגמת ביטחון הציבור, או זכויות מתחרות דוגמת זכותם הקניינית של מפתחי הטכנולוגיה.[184] מכל מקום, גם אם תותר אי־חשיפתו של מידע מסוים, אין בכך כדי לאיין את קיומה של הנמקה מפורטת, הכוללת את פרטי המידע הגלויים שאפשר לגלות למושא ההחלטה.[185] נוסף על כך, ככל שמדובר בהחלטה אוטומטית פשוטה יותר (כלומר כזו שאינה מבוססת על שקלול של פריטי מידע רבים ממקורות מידע שונים ומגוונים) – למשל שליחת דרישה אוטומטית לקביעת תור לבדיקה תקופתית אצל רופא השיניים – חובת ההנמקה שתוצמד אליה תהיה בסיסית ומצומצמת יותר. חרף זאת, מקבל ההחלטה לא יוכל לנמק את החלטתו באמצעות הפניה פורמלית לניבוי הסטטיסטי המסוים שנקבע לפרט ויהיה עליו להעניק הסבר מהותי לניבוי שעליו התבסס. כלומר, רופא השיניים יצטרך לפרט מתי היה הביקור האחרון של הנבדק במרפאה ומדוע הגיע המועד להיבדק שוב.

בכל הנוגע להיקף תחולתה של חובת ההנמקה המוצעת, המנגנון המוצע מסתייג מהמודל שב־GDPR בכמה בחינות. ראשית, תחת המנגנון האירופי, הזכות למתן הסבר צומחת עם פנייתו של הפרט מושא המידע לקבל הסבר על אודות ההחלטה,[186] ואילו המנגנון המוצע כאן תומך באימוץ של חובת הנמקה אקטיבית ולא של חובת הסבר פסיבית.[187] חוקרים הצביעו במגוון הקשרים כי בעלי זכויות אינם תמיד ממהרים לעמוד על זכויותיהם ולממשן,[188] אולם אם אחת המטרות המרכזיות של המנגנון המוצע היא לעודד את השוק הטכנולוגי לפתח

פרטים בנוגע למעביד החושפים בפועל סוד מסחרי שלו (ס' 2.7.7.7.7.). משמע, שטיב ההסבר עשוי להשתנות ממקרה למקרה.

184 עניין **רמת הדר**, לעיל ה"ש 153, בעמ' 287–288.

185 עניין **פלוני נ' ראש ממשלת ישראל**, לעיל ה"ש 149, בפס' כ.

186 הזכות לקבל הסבר תחת הערת פתיח 71 ל־GDPR מנוסחת כך: "The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention […] In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision".

187 אייל פלג **אתגר העוני של המשפט המנהלי** 621 (2013) (שם הוא מציע להטיל על פקידי רווחה חובה אקטיבית למתן הסבר אישי בנוגע לפרטים העניים שבטיפולם משום שאלה מוחלשים, פגיעים, חסרי ידע ופעמים רבות גם חסרי שפה מתאימה והשכלה).

188 ראו, למשל, Perel & Elkin-Koren, *Accountability in Algorithmic Enforcement*, לעיל ה"ש 8, בעמ' 524–525 (שם הצבענו על אחוזי השימוש הנמוכים בזכות הערעור הניתנת למשתמשים שתוכניהם הוסרו בגין טענה להפרת זכויות יוצרים); בירנהק **מרחב פרטי**, לעיל ה"ש 1, בעמ' 234–235 (שם הוא מדגיש את הבעייתיות במימוש זכות התיקון תחת חוק הגנת הפרטיות).

מערכות טכנולוגיות שאפשר להסביר את ההיגיון שבבסיסן, מוטב לאמץ חובה מפורשת שלא מותירה מרחב גדול מדי לעקיפתה.[189]

שנית, המנגנון המוצע תומך בחובת הנמקה של כל ההחלטות שמתקבלות בנוגע לפרט על סמך ניתוח של נתוני עתק: משמעותיות כזניחות לכאורה, כאלו הכרוכות במעורבות אנושית וכאלו שהן אוטומטיות לחלוטין. לעומת זאת, באיחוד האירופי אומצה גישה שונה. שם, במסגרת הזכות למתן הסבר תחת ה־GDPR, הוגבלה זכות זו להחלטות אוטומטיות לחלוטין ולכאלו שיש להן השלכות משפטיות או השלכות בעלות משמעות דומה על הפרט:

> The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.[190]

ביקורת נוקבת נמתחה על גישה זו.[191] ראשית, נטען כי כל שילוב של חותמת גומי בדמות בן אנוש עשוי לאפשר עקיפה של ההסדר האירופי.[192] ברי כי אם נאמץ הגבלה זו נוציא מגדר חובת ההנמקה החלטות רבות שנדונו במאמר זה (כגון החלטת מעביד אם לזמן מועמד לריאיון עבודה[193]) שיש בהן החלטה אנושית המבוססת על ניבוי סטטיסטי לפי מידע אישי. שנית, לדעתי קשה לקבוע מראש איזו נפקות תהיה להחלטה מסוימת, מאחר שזו תלויה הן בנסיבות המקרה הספציפיות והן במועד בחינתה. לא הרי שלילת רישיון אוטומטית בגין נסיעה באור אדום לנהג בעל היסטוריה של עברות תנועה כהרי מתן דירוג אשראי נמוך מאוד לזוג צעיר, ללא עבר פיננסי מפותח, המעוניין לרכוש בית מגורים; לא הרי השפעתה של שלילת הרישיון על פרט המתפרנס מנהיגה (נהג משאית, למשל) כהרי השפעת דירוג אשראי נמוך על אדם מבוגר, בעל בית, בעל היסטוריה פיננסית עשירה אך בעייתית.

מהאמור לעיל, אפשר לגזור כמה כללי אצבע מנחים לפיתוח מודל הנמקה תחת גישת הפרטיות כשליטה במידע אישי:

1. תוטל חובת ההנמקה אקטיבית על גופים פרטיים שמקבלים החלטות בנוגע לפרט על סמך ניתוח טכנולוגי של נתוני מידע על אודותיו; יש לקיימה בין שהפרט עמד על זכותו לקבל הסבר ובין שלא.

---

189 ראו בהקשר זה את הנימוקים שהועלו בנוגע לפרשנות הראויה לס׳ 22 ל־GDPR, הקובע כי לפרט "have the right not to be subject to a decision based solely on automated proceeding". מרגוט קמינסקי, למשל, מצדדת בפירוש של סעיף זה כמטיל איסור על קבלת החלטות אוטומטיות לחלוטין, וזאת כדי לחייב את מקבלי ההחלטות לוודא שהם עומדים באחד הפטורים המנויים ב־GDPR. Kaminski, לעיל ה״ש 138, בעמ׳ 4.

190 הערת פתיח 71 ל־GDPR; ראו גם ס׳ 22(1) ל־GDPR החוזר על הגבלות אלה.

191 Kaminski, לעיל ה״ש 138, בעמ׳ 5.

192 Malgieri & Comand, לעיל ה״ש 3, בעמ׳ 251.

193 Aarti Shahani, *Now Algorithms Are Deciding Whom to Hire, Based on Voice*, NPR (Mar. 23, 2015), https://n.pr/2S9dQ2X.

2. חובת ההנמקה תחול בנוגע לכל החלטה שמתקבלת בנוגע לפרט על סמך ניתוח טכנולוגי של נתוני מידע על אודותיו, אם כי במידה ובהיקף הדרושים באופן סביר, בנסיבות העניין, כדי לאפשר לפרט להשיג על ההחלטה שהתקבלה בעניינו.
3. תוכנה של חובת ההנמקה יכלול את פרטי המידע שנשקלו במסגרת קבלת ההחלטה כמו גם את אופן שקילתם ואת הקריטריון המכריע.

3. ביקורת אפשרית על אימוץ המודל המוצע ומענה לה

ההצעה להחיל עיקרון ציבורי על גופים פרטיים צפויה לעורר גם ביקורת. הקושי הראשון עלול להתעורר עקב כך שהטלה של חובת הנמקה אקטיבית על מקבלי החלטות פרטיים מתערבת באוטונומיה העסקית והתפקודית שלהם – לקבל החלטות באופן שמשרת את האינטרסים הכלכליים־פרטיים שלהם. גוף פרטי, יטען הטוען, אינו חייב דין וחשבון לציבור בדרך המקובלת בדמוקרטיה.[194] אולם, האוטונומיה העסקית הזו איננה מוחלטת: גם למשפט הפרטי יש כלים שמתערבים בחופש העסקי של הפרט כדי לקדם ערכים חשובים כמו עקרון תום בלב או תקנת הציבור.[195] נוסף על כך, התנהלות עסקית־פרטית איננה פועלת בריק רגולטורי והיא כפופה להגבלות ספציפיות של המשפט הפרטי. כך, מעסיק אינו יכול להפלות בין עובדיו או בין דורשי עבודה מהטעמים המנויים בחוק שוויון ההזדמנויות בעבודה;[196] יוצר של יצירה המוגנת בזכות יוצרים אינו יכול למנוע מהציבור למתוח ביקורת על יצירתו;[197] ואוסף מידע אינו יכול לפנות לפרט לשם קבלת מידע על אודותיו אלא לאחר שהפרט מסר לכך הסכמה מדעת.[198] חובת ההנמקה הנדונה במאמר זה היא אמנם חובה שמזוהה עם המשפט הציבורי, אולם החלתה על גופים פרטיים שמקבלים החלטות בנוגע לפרט, על סמך ניתוח מידע, נעשית באמצעות המשפט הפרטי – ותחת הבסיס המושגי של דיני הגנת הפרטיות בישראל. בעידן של נתוני עתק, תחת גישת הפרטיות כשליטה, האיסור על פגיעה בפרטיותו של אדם ראוי שיתפרש כאיסור על נטילת שליטתו של הפרט במידע על אודותיו בכל שלבי התגלגלותו, לרבות ברגע שהוא משמש לקבלת החלטות לגביו. מאחר שלפי שעה דיני הגנת הפרטיות אינם מאפשרים שליטה כזו, מוצע לעדכנם – אם כי באמצעות עדכון פנימי בחוק ולא בעדכון חיצוני לו. אמנם העדכון המוצע נשען על מנגנון ציבורי, אך זה מוזרם מתוך צינור פנימי למשפט הפרטי והוא הדין הישראלי העוסק בהגנת מידע.

ביקורת אפשרית נוספת על המנגנון המוצע עשויה לטעון כי השוק החופשי יביא לפתרון אופטימלי ללא צורך בהתערבות רגולטורית. חברה פרטית, שתחשוב שמתן הסבר ללקוחותיה על אודות ההיגיון שבסיס הניבויים הסטטיסטיים שמשמשים אותה לקבלת החלטות בנוגע לפרט יעניק לה יתרון כלכלי על פני מתחרותיה, תפעל בהתאם לכך; חברה שאיננה חושבת

194 זמיר **הסמכות המנהלית** כרך ב, לעיל ה"ש 146, בעמ' 521–522.

195 דנג"ץ 4191/97 **רקנט נ' בית־הדין הארצי לעבודה**, פ"ד נד(5) 330, 362 (2000); דפנה ברק־ארז "משפט ציבורי ומשפט פרטי: תחומי גבול והשפעות גומלין" **משפט וממשל** ה 110–113 (1999).

196 ס' 2 לחוק שוויון ההזדמנויות בעבודה.

197 ס' 19 לחוק זכות יוצרים, התשס"ח–2007, ס"ח 2119.

198 ס' 11 לחוק הגנת הפרטיות.

כך תימנע מלפעול כאמור. השוק יגיב בהתאם ותתקיים תחרות על מידת השקיפות של מקבלי ההחלטות הפרטיים: ככל שיש לקבלת הסבר חשיבות מבחינת הפרט, יגבר הביקוש לניבויים סטטיסטיים של חברות המספקות הסבר כזה, וכך יגיע השוק לשיווי משקל אופטימלי, ללא התערבות חיצונית. לדעתי אין לקבל טענה זו מאחר שהמציאות מראה שיש כשל שוק בכל הנוגע למתן הסבר על החלטות שמתקבלות על סמך ניתוח של נתוני עתק. אף על פי שלקבלת הסבר על ניבויים סטטיסטיים במידע אישי יש ערך חשוב להגשמה של אוטונומיית הפרט, עדיין יש ספקנות לגבי קיומו של היגיון בבסיסם של מנגנונים טכנולוגיים לומדים (interpretability).[199] כדי שחברות פרטיות שמקבלות החלטות בנוגע לפרט על סמך ניבויים סטטיסטיים יגבירו את הביקוש לניבויים שאפשר להסביר, צריך להיות להן תמריץ כלכלי מספק לדרוש זאת. במיוחד יש להצביע על הסיכון שהפרט יימנע מלהתקשר עמן אם לא יספקו לו הסבר על אודות החלטותיהן. ספק אם מדובר בסיכון ממשי נוכח פערי הכוחות התהומיים שבין הפרט מושא המידע לבין החברות הפרטיות שמקבלות את החלטות בנוגע אליו על סמך ניתוח של נתוני עתק. איזו אלטרנטיבה יש לגולש החשוף לפרסום ממוקד ברשת? אמנם הוא יכול לבחור שלא להיות חשוף כלל לפרסומות, אך ככל שהוא מעוניין בפרסום, אין לו אפשרות אמתית להשפיע על האלגוריתם שיחליט אילו פרסומות מתאימות לפרופיל הדיגיטלי שלו.

לבסוף, קושי נוסף ביישום המנגנון המוצע כרוך בעלויות שהוא עתיד להשית על מפתחי הטכנולוגיה.[200] לדעתי גם בכך אין כדי לגבור על התועלת שיצמיח המנגנון המוצע. לעתים הגנה הולמת על זכויות הפרט, במציאות טכנולוגית משתנה, כרוכה במחיר כלכלי. כך, למשל, יישום המנגנונים המוצעים בתיקון 5 לחוק זכות יוצרים בעניין חשיפת פרטי מעוול אנונימי[201] או צווי חסימה צפויים להטיל עלויות כלכליות על גופים פרטיים שאמורים ליישם אותם.[202] בדומה, גם היישום של פרקים ב ו־ד לחוק הגנת הפרטיות כרוכים בעלויות כלכליות, לרבות הצורך להגיש בקשות לרישום מאגרי מידע, בניית תשתית ליידוע משתמשים על אודות איסוף המידע ומטרתו ושמירה על אבטחת המידע וסודיותו. מכל מקום, אין לשכוח שתעמוד למפתחי הטכנולוגיה אפשרות לגלגל את הוצאות הפיתוח על החברות הפרטיות המתבססות על הניבויים שהם מפיקים, ואלו יוכלו להמשיך לגלגל את הוצאותיהן הלאה, על הציבור הרחב.[203]

199 Lisboa P. J.G., *Interpretability in Machine Learning – Principles and Practice, in* Fuzzy Logic and Applications 15-21 (Francesco Masulli et al. eds., 2013).

200 Doshi-Velez & Kortz, **לעיל ה"ש 67, בעמ' 10.**

201 **ראו, למשל, ע"א 9183/09 The Football Association Premier League Limited נ' פלוני, ס' 5 לפסק דינו של השופט הנדל (פורסם בנבו, 13.5.2012).**

202 **ראו מעיין פרל וניבה אלקין־קורן "השטן הוא בפרטים הטכנולוגיים: על הפרטת האכיפה בעקבות תיקון 5 לחוק זכות יוצרים, התשע"ח־2017" חוקים יג (צפוי להתפרסם ב־2019).**

203 **שם (שם הצגנו את טענתו של השופט ארנולד, שלפיה העלויות שיספגו ספקי גישה שיחסמו גישה לאתרים פיראטיים בהתאם לצו חסימה של בית המשפט יגולגלו בסופו של יום על ציבור המשתמשים).**

ו. סיכום

יותר ויותר החלטות שמשפיעות על הפרט מתקבלות כיום על סמך ניתוח טכנולוגי משוכלל של נתוני המידע על אודותיו. הבעיה היא שהניבויים הסטטיסטיים הללו מופקים על ידי אלגוריתמים מסובכים, דינמיים וסודיים. לפיכך, חוסר שקיפותם האינהרנטי מציב לפני מושא ההחלטה אתגר פיקוח רציני. מאמר זה הציע לפתח מנגנון פיקוח חדש תחת חוק הגנת הפרטיות, שיתבסס על חובת ההנמקה שבמשפט הציבורי ויישען על תובנות בנוגע למנגנון האירופי שאומץ לאחרונה בהקשר זה תחת הרגולציה האירופית להגנת מידע בעידן של נתוני עתק (GDPR). מנגנון זה מבוסס על כמה עקרונות: ראשית, על מקבלי החלטות פרטיים שמתבססים על ניתוח של נתוני מידע תוטל חובת ההנמקה אקטיבית. שנית, חובת ההנמקה תחול על כל החלטה שמתקבלת בנוגע לפרט על סמך ניתוח טכנולוגי של נתוני מידע על אודותיו, במידה ובהיקף הדרושים באופן סביר כדי לאפשר לו להשיג על ההחלטה שהתקבלה בעניינו. שלישית, ההנמקה תפרט את פרטי המידע שנשקלו במסגרת קבלת ההחלטה כמו גם את אופן שקילתם ואת הקריטריון המכריע. ברי כי אין מדובר בהסדר פיקוח ממצה על מנגנונים אלגוריתמיים לקבלת החלטות. כפי שטען פרנק פסקואלה, פיקוח איכותי על קבלת החלטות אוטומטיות תלוי בקיומם של רובדי בקרה מגוונים בהיקפם, הנתונים בידיהם של כמה גורמים: הפרט, הגופים המקבלים החלטות, צדדים שלישיים ורגולטורים.[204] כאשר פנינו לעולם שבו הגולם קם על יוצרו והמכונה שולטת באדם באמצעות המידע האישי שלו, הטלה של חובת הנמקה על מקבלי החלטות בנוגע לפרט היא אבן דרך משמעותית בדרך לשמירת שליטתנו העצמאית בחיינו.

204 Pasquale, The Black Box Society, **לעיל ה"ש 46, בעמ' 142.**