

## פרטיות מותאמת אישית

### תגובה על מאמרם של ליאור סטרכילביץ' ואריאל פורת

מאת

מיכאל בירנהק\*

#### תקציר

לעיבודו של מידע אישי בהיקפים נרחבים ובשיטות ניתוח של נתוני-עתק (big data) יש יתרונות רבים. מאמרת-גובה זה מבקש לטעון כי ההסתמכות על נתוני-עתק חייבת להיעשות תוך מודעות והתייחסות מעמיקה לסוגיית הפרטיות. המאמר בוחן את הצעתם של סטרכילביץ' ופורת לשימוש במידע אישי לשם עיצובם של כללי בררת-מחדל במשפט, ומצביע על קוצר-היד שלה בהיבטי הפרטיות. הצעתם נסמכת בהכרח על עיבוד מידע בהיקף נרחב, על יצירת פרופילים של אזרחים, ועל שימוש בהם הן באופן כללי לשם עיצוב הכלל המשפטי והן ביישומו של הכלל. למרות יתרונותיה של ההצעה במישור היעילות, יש בה הנחה לא-משכנעת כי הפרטיות מתנגשת בהכרח באינטרסים של יעילות וחדשנות, וכי ידה על התחונה; יש בה המעטה לא-מוצדקת של הזכות לפרטיות; היא מתמקדת רק בשלב איסוף המידע, תוך הזנחת השלבים של עיבוד המידע והשימוש בו; יש בה ערוב מסוים של הקשרים ציבוריים וצרכניים; ויש קשיים בפרטי הצעתם עצמה בהיבט של הפרטיות.

המאמר טוען כי אין בהכרח התנגשות בין פרטיות לבין אינטרסים של יעילות וחדשנות, וכי ניתן לשלב ביניהם. חלף התפיסה הרוזה של הפרטיות במידע המשתקפת בדבריהם של סטרכילביץ' ופורת, אצביע על תפיסת הפרטיות כשליטה, שמשמעה הוא הכוח והזכות המשפטיים של אדם לקבוע מה יעלה בגורל המידע האישי על-אודותיו. עם זאת, המאמר מצביע על הקשרים מסוימים שבהם יש יתרון לגישתם של סטרכילביץ' ופורת – למשל, בקשר לקביעת גורלם של זכרונות דיגיטליים, דהיינו, מידע דיגיטלי שנשאר אחרי מותו של אדם. בנושא זה, כפי שהמאמר מסביר, יש להצעתם בדבר קביעת כללי בררת-מחדל מותאמים אישית יתרון לעומת הגישות הקיימות, המבקשות לקבוע בררת-מחדל מסוימת כללית.

\* פרופסור מן המניין, סגן דקן למחקר, הפקולטה למשפטים, אוניברסיטת תל אביב. הדיון בחלק ג של מאמרת-גובה זה מבוסס על מחקר בנושא זכרונות דיגיטליים שנערך בשיתוף עם טל מורס, בסיוע מענק של הקרן הלאומית למדעים (ISF 257/18).

## מבוא

א. על התאמה אישית ועל פרטיות

1. מידע קטן ומידע גדול

2. עיבודי מידע

3. מדינה ואזרחיה; תאגיד ולקוחותיו

ב. פרטיות לפי סטרכילביץ' ופורת

ג. פרטיות – תפיסה מהותית

1. פרטיות כשליטה

2. פרטיות ועיצוב כללי בררת־מחדל

3. מקרה־מבחן: זכרונות דיגיטליים

סיכום

## מבוא

מידע הוא סם החיים של שווקים. לכן, כדי שהשווקים יהיו יעילים יותר, יש לאפשר למידע לזרום בחופשיות בשוק ולהגיע למקבלי החלטות בארגונים ובמדינה. זו הנחת־המוצא של הגישה הכלכלית של המשפט למידע.<sup>1</sup> ליאור סטרכילביץ' ואריאל פורת מבקשים להיעזר בטכנולוגיות של נתוני־עֵתֶק (big data) כדי לשכלל עוד יותר את השימוש במידע, כך שהוא יוכל להוות בסיס לקבלת החלטות מותאמות אישית ולעיצוב כללים משפטיים של בררת־מחדל.<sup>2</sup> טכנולוגיות אלה מאפשרות לאסוף מידע בהיקף ניכר ממקורות ומסוגים שונים, לעבד אותו ולהשתמש בו על־אתר.<sup>3</sup>

עיבוד של מידע אישי על בני־אדם<sup>4</sup> לשם עיצוב כללים משפטיים מעורר מייד שאלות של פרטיות. סטרכילביץ' ופורת (להלן: המחברים) מזכירים במאמרם את הפרטיות כביקורת

1 גישה זו רואה במידע אמצעי לשיפור תפקודו של השוק. ענף אחר של הניתוח הכלכלי עוסק במצב שבו המידע הוא המשאב שנסחר בשוק, וכדי לאפשר את המסחר במידע, המשפט מסייע באמצעות יצירת זכויות קניין רוחני במידע.

2 ראו ליאור סטרכילביץ' ואריאל פורת "פרסונליזציה של כללי בררת־מחדל וחובות גילוי באמצעות נתוני־עֵתֶק (Big Data)" בחוברת זו, וכן את מאמרם המקורי: Ariel Porat & Lior Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 *MICH. L. REV.* 1417 (2014).

3 תיאור זה משקף את שלושת המאפיינים המרכזיים של נתוני־עֵתֶק, המכונים "שלושת ה־Vים": כמות (volume), מגוון (variety) ומהירות השימוש (velocity). להגרורות המקובלות ראו, למשל, ARVIND SATHI, *BIG DATA ANALYTICS: DISRUPTIVE TECHNOLOGIES FOR CHANGING THE GAME* (2012) 4. אפשר לתאר זאת גם כ"שלושת ה־Mים": Mix, Mine, Match, כלומר, לערכב מידע ממקורות שונים, לכרות מידע (כלומר, להפיק מידע חדש, נוסף על המידע הקיים) ולאחר מתאמים מעניינים.

4 אני משתמש במונח "מידע אישי" כמוכנו בדִין האיחוד האירופי: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference

אפשרית – אחת מבין כמה – על הצעתם, אך ממהרים להדוף אותה. איני כופר בתועלת האפשרית של כללים מותאמים אישית, אולם הסתמכות על נתוני-עתק חייבת להיעשות תוך מודעות והתייחסות מעמיקה לסוגיית הפרטיות. בהתאם, מאמרת-גובה זה מבקש להתעכב על היבטי הפרטיות ולהעמיק את הביקורת בנושא זה. אני מבקש להצביע באופן רחב יותר על החשיבות של שילוב שיח הפרטיות בשלושה הקשרים: ראשית, במקרה הנוכחי, של עיצוב כללים משפטיים בהתבסס על מידע אישי, כהצעת המחברים במאמרם;<sup>5</sup> שנית, בהקשר של שימוש בטכנולוגיות של נתוני-עתק באופן כללי; ושלישית, במסגרת הניתוח הכלכלי של המשפט, שנוטה למעט מערכה של הפרטיות, ולעיתים אף להתייחס אליה כאל מטרד שניתן לוותר עליו בקלות רבה בתמורה ליתר יעילות.<sup>6</sup>

המחשה של הפער בין גישת הניתוח הכלכלי לפרטיות לבין הגישה המקובלת בשיח הפרטיות אפשר למצוא במסגור של מקרה מוכר בשיח הפרטיות בשנים האחרונות, שנזכר גם במאמר מושא הביקורת הנוכחית, והוא סיפור של נערה שרכשה מוצרים ברשת הקמעונאית האמריקנית Target. כך הדברים מתוארים אצל סטרכילביץ' ופורת:

"חוקרי המידע של רשת Target גילו כי נשים המתחילות לפתע לרכוש מולטי-ויטמינים רוכשות חודשים מספר לאחר-מכן טיטולים ומוצרים אחרים לתינוקות. כך הם גילו את הקשר בין רכישת מולטי-ויטמינים לבין היות הרוכשת בהיריון. רשת Target אף הבינה כי הזמן לרכוש לקוחות למוצרי תינוקות הוא לפני הולדת התינוק. כך מצאו עצמן נשים בהיריון – וכנראה גם כאלה שאינן בהיריון – מקבלות עלוני פרסום וקידום מכירות למוצרי תינוקות 'דק' משום שרכשו קודם לכן מולטי-ויטמינים."<sup>7</sup>

תיאור זה מציג את הפרסום המותאם אישית לנשים בהיריון כשימוש עסקי נבון ומוצלח בטכנולוגיות של נתוני-עתק. אולם בספרות המחקרית בתחום הפרטיות הדגש (שמקורו

"...to an identifier such as a name, an identification number..." (14) 'ס' 14) Regulation 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 movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 (להלן: GDPR). הגדרה זו מדגישה את אופי הזיהוי של המידע, ולא את תוכנו. ההנחה המגולמת בהגדרה זו היא שכל מידע מזהה עשוי להיות חשוב, גם אם במבט ראשון הוא נראה טריוויאלי, כגון הרגלי הרכישה במרכול.

5 להצעתם של המחברים במאמרם יש השלכות נוספות, כגון קיבוע והסללה של בני-אדם לדפוסים מוכתבים וכן חפצון של בני-אדם. הגם שלסוגיות אלה יש ממשק עם הפרטיות, לא אתעכב עליהן כאן. לדיון ראו, למשל, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 252 (2012). בהקשר הנוכחי ראו את מאמרו של צחי קרן-פז "סיפור חייו או סיפורו של חייב? על בעיית ההסללה הנובעת מאימוץ כללים אישיים" בחוברת זו.

6 היחס העיוני-משהו של הניתוח הכלכלי לפרטיות נמצא אצל פונור, אם כי בהקשר טרום-דיגיטלי. ראו Richard A. Posner, An Economic Theory of Privacy, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 333 (Ferdinand David Schoeman ed., 1984).

7 סטרכילביץ' ופורת, לעיל ה"ש 2, ליד ה"ש 63-64.

בכתבה של ה-*NEW YORK TIMES*) הוא בסיפורה של נערה שקיבלה לביתה קופונים מהרשת; אביה – שראה את הקופונים למוצרים לנשים בהיריון – זעם, עד שהתברר לו כי בתו אכן הרה. חוקר הפרטיות פרנק פסקואלה (Pasquale) מתאר זאת בתמציתיות: “A major retailer like Target can ‘know’ a customer is pregnant before even other family members do, simply by crunching the numbers on a sufficiently large data set of purchases and doing pattern recognition”<sup>8</sup>. הדגש כאן אינו ביעילות של הפעולה המידעית של הרשת, אלא בכך שהחנות ידעה על ההיריון לפני קרובי-המשפחה. קרופורד (Crawford) ושולץ (Schultz) קובעים כי במקרה זה מדובר בחשיפה לא-מורשית של מידע, ומציינים כי הגם שיש להניח כי הלקוחות הבינו שהרשת אוספת מידע על הרגלי הרכישה שלהם, ספק אם הם הניחו שהמידע משמש ליצירת פרופיל אישי, שיהווה בסיס למשלוח פרסומות.<sup>9</sup> הפתרון של Target, דרך אגב, לא היה לחדול מהשימוש בנתוני-העתק, אלא להסוותו: על הפרסומות למוצרים הקשורים להיריון מוסף “רעש” של פרסומות אחרות, אשר יוצר רושם של מקריות ולכן מצמצם את תחושת המעקב.<sup>10</sup>

מהו, אם כן, מקומה של הזכות לפרטיות בניתוח הכלכלי? מה מקומה בהקשר של שימוש בנתוני-עתק בכלל, ומה מקומה בהקשר של שימוש בהם ככלי לעיצוב כללים משפטיים מותאמים אישית בפרט? זה נושא התגובה, וזה מהלך הטיעון: בפרק א אפתח במיפוי דרוש של היבטי הפרטיות שמתעוררים אגב יישום של התאמה אישית במשפט. אעיר על היקפי המידע, על זהות הצדדים ועל סוגים של עיבודי מידע. בפרק ב אבחן את עמדתם של סטרכילביץ' ופורת כלפי פרטיות. כאמור, הם מציגים אותה כביקורת אפשרית, ומתשובתם עליה, כמו-גם מהערות נוספות לאורך מאמרם, ניתן לחלץ את תפיסתם לגבי פרטיות. מן הדברים עולה תפיסה רזה למדי של פרטיות, שמתמקדת בעיקר בשלב של איסוף המידע, ללא הבחנה בין הגורמים השונים שאוספים את המידע ומעבדים אותו. בפרק ג אציע תפיסה עבה יותר של פרטיות – פרטיות כשליטה, שהיא נגזרת של כבוד האדם. בתפיסה כזו יש חשיבות רבה לכל השלבים במחזור החיים של המידע, ויש חשיבות להקשר שבו מדובר – ציבורי או פרטי. אראה כיצד עמדה זו יכולה דווקא לשלב את ההצעה להתאמה אישית של כללי בררת-מחדל עם תפיסת הפרטיות. אציע מקרה-מבחן שמראה כיצד ניתן לגייס את נתוני-העתק לטובת עיצוב כללים משפטיים, וכיצד אפשר לעשות זאת תוך שמירה והגנה על הפרטיות, ולא תוך ויתור עליה. מקרה-המבחן הוא של זכרונות דיגיטליים – מידע אישי שנשאר אחרי מותו של גולש ברשת. לבסוף אסכם.

- 
- 8 Frank Pasquale, *Redescribing Health Privacy: The Importance of Information Policy*, 14 Hous. J. Health L. & Pol'y 95, 109 (2014).
- 9 Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 BOSTON COLLEGE L. REV. 93, 95–96 (2014).
- 10 Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 67 (2013).

## א. על התאמה אישית ועל פרטיות

סטרכילביץ' ופורת מבקשים לגייס את הטכנולוגיות של נתוני-עתק ככלים שיסייעו בעיצוב כללים משפטיים, ובאופן ספציפי, לשם התאמה אישית של כללי בררת-מחדל, כלומר, של הכללים שיחולו על מי שמתמש בהם כל עוד הוא לא הגדיר כללים ספציפיים שיחולו לגביו. לפי הצעתם, עיבודי מידע – על בסיס מידע שנאסף משלל הקשרי חיים של צרכנים ואזרחים – יכתיבו מהו כלל בררת-המחדל שיחול על כל אדם בנפרד, בהקשרים חוזרים וכנראה גם בהקשרים שלטוניים. עצם הרעיון של התאמה אישית אינו חדש, והוא מוכר לנו מחיי היומיום, עוד מלפני שהבשילו טכנולוגיות של נתוני-עתק. עיקר החידוש במאמרם הוא השימוש בעיבודי מידע בשלב מוקדם יותר וכללי יותר לשם עיצוב הכללים המשפטיים עצמם. ראוי לכן להבחין בין מצבים שונים לפי היקפי המידע, לפי סוגים שונים של עיבודי מידע ולפי זהות הצדדים. הבחנות אלה יסייעו בזיקוקם של היבטי הפרטיות.

### 1. מידע קטן ומידע גדול<sup>11</sup>

בסביבה הלא-דיגיטלית אנו מכירים את התופעה של הפליית מחירים: צרכנים שונים עשויים לשלם מחירים שונים בגין אותו שירות. מוכר שמכיר את לקוחותיו עשוי לתת הנחה ללקוח נאמן, ואילו מלקוחות חד-פעמיים הוא עשוי לדרוש מחיר מלא. יחסי המוכר ולקוחותיו הם קשר של אדם אחד עם אדם אחר, וממילא אינם עניין של נתוני-עתק, אולם הפליית המחירים הפשוטה הזו מבוססת על מאפיין של הלקוח שידוע למוכר. מצב זה מעורר היבטי פרטיות, אך אלה מעטים, ומוסדרים בדרך-כלל בפן הנזיקי – למשל, אם המוכר יספר לאחרים נתון על "ענייניו הפרטיים של אדם", כגון מצבו הבריאותי, הכלכלי או האישי, תקום ללקוח עילת תביעה לפי החוק.<sup>12</sup>

בסביבה הדיגיטלית אנו עוברים ממידע קטן למידע גדול, עד לנתוני-עתק, שמשמש בסיס להפליית מחירים או ליצירת תנאים שונים בעסקה לכל לקוח בנפרד. למשל, במקרים רבים שני נוסעים באותה טיסה, שיושבים זה בצד זה באותה מחלקה, משלמים מחיר שונה. השוני נעוץ במאפיינים מסוימים של הלקוחות שזוהו על-ידי המוכר – מועד רכישת הכרטיס, נסיעות קודמות, מידת הגמישות של הלקוחות במועדי הטיסה ועוד. כאן האינטראקציה היא בין שחקן אחד (חברת התעופה) לבין לקוחות רבים, והיא מבוססת על מאפיינים של הלקוחות שהחברה אספה ועיבדה לאורך זמן. באופן דומה, פרסומות שמותאמות אישית לכל גולשת

11 במקום אחר הבחנתי בין מצבים שונים, וכן בין דינים שחלים עליהם, לפי היקף המידע. ראו Michael Birnhack, *S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm*, in *BIG DATA AND PRIVACY: MAKING ENDS MEET 7* (Future of Privacy Forum & Center for Internet & Society, Stanford Law School, 2013).

12 ראו ס' 2 לחוק הגנת הפרטיות, התשמ"א-1981, המונה מצבים שונים של פגיעה בפרטיות. כך, לפי ס' 9(2), שמגלם את "עקרון צמידות המטרה", אין להשתמש במידע על ענייניו הפרטיים של אדם למטרה שונה מזו שלשמה הוא נמסר. המונח "ענייניו הפרטיים של אדם" זכה בפרשנויות שונות בפסיקה. ראו, למשל, רע"א 6902/06 צדיק נ' הוצאת עיתון הארץ בע"מ, פ"ד סג(1) 52, 58-59 (2008). ראו גם ס' 11(2) לחוק הגנת הפרטיות, שעניינו פרסום מידע על צנעת חייו האישיים של אדם.

ברשת לפי היסטוריית הגלישה שלה ומידע אחר שנצבר על-אודות המשתמשים בכלל; מערכות של המלצות, כגון המלצות של אמזון על רכישת ספרים, בהתבסס על רכישות-עבר שלנו ושל לקוחות ש"דומים" לנו; או הצעות להשלמה אוטומטית של שאילתות חיפוש במנועי חיפוש (Autocomplete) – הם מצבים מוכרים של התאמה אישית שמבוססים על איסוף מידע על הלקוח המסוים ועל השוואת המידע הפרטני לדפוסי התנהגות כלליים. שימוש בשירותים דיגיטליים במלואם (שאינן להם מרכיב מחוץ למרשתת), כגון רשתות חברתיות, כרוך באיסוף מידע בהיקף עצום על תוכן הפעילות ונתוני הפעילות (מי יצר קשר עם מי, לכמה זמן, מהיכן ועוד). מפעילות השירותים מסבירות כי המידע נאסף, בין היתר, כדי לאפשר התאמה אישית.<sup>13</sup> במצב של נתוני-עתק נוספים לתמונה מרכיבים של גודל, היקף וכן חיזוי העתיד על-סמך העבר, ובכלל זה ניבוי התנהגותו של אדם יחיד. יצירת פרופיל צרכני מעוררת שאלות רבות על היכולת לבנא את התנהגות הלקוחות בעתיד על-סמך התנהגותם בעבר ועל-סמך התנהגותם של אחרים, וכן שאלות של פרטיות בקשר לאיסוף המידע ולעיבודו ובקשר לעצם יצירת הפרופיל. סוגיה זו זכתה בדיון ער בשיח הפרטיות בעשור הראשון של המאה הנוכחית.<sup>14</sup> הנושא מוסדר כיום בדיני הפרטיות, לפחות בדין האירופי, בדין הישראלי ובדיניהן של עשרות מדינות נוספות בעולם.<sup>15</sup> ההסדרה הטיפוסית היא בדרך של כללים המכונים באופן כולל Fair Information Practices או בקיצור – FIPs. כללים אלה עוסקים בהודעה ללקוח על איסוף המידע והשימושים בו,

13 כך, למשל, מסבירה פייסבוק את מדיניות הפרטיות שלה:

“To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide); how you use and interact with our Products; and the people, places, or things you’re connected to and interested in on and off our Products.”

זמין בכתובת <https://www.facebook.com/policy.php>. מדיניות הפרטיות המפורטת שם מונה את סוגי השימושים הרבים שהרשת עושה במידע, ומביניהם ההתאמה האישית מופיעה ראשונה. בין שלל המטרות הנוספות נזכרת גם המטרה של התאמה אישית של פרסומות. זהו, כמובן, ליבו של המודל העסקי של הרשת הזו.

14 ראו, למשל, Jason Millar, *Core Privacy: A Problem for Predictive Data Mining*, in LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 103 (Ian Kerr, Valerie Steeves & Carole Lucock eds., 2009). לדין תיאורטי מן העת האחרונה ראו מיקי זר “אנשים שקראו מאמר זה התעניינו גם ב...”: על הקשר בין פרטיות לפרופילינג” משפט, חברה ותרבות ב 69 (מיכאל בירנהק עורך, 2019).

15 להתפשטותם של דיני הגנת הפרטיות בעולם ראו Graham Greenleaf & Bertil Cottier, *Data Privacy Laws and Bills: Growth in Africa, GDPR Influence*, 152 PRIVACY L. & BUS. INT’L REP. 11 (2018). בארצות-הברית ההסדרה הפדרלית היא רק בהקשרים מסוימים שבהם יש חקיקה ספציפית, לפי תוכן המידע שבו מדובר – למשל, מידע רפואי או מידע פיננסי. אין שם חקיקה ייעודית בקשר למידע על טיסות, למשל, ולכן הדין הפדרלי אינו מסדיר מידע כזה. במישור שבין המדינה לאזרחיה חל התיקון הרביעי לחוקה, שעניינו חיפוש ותפיסה של מידע בהקשרים של אכיפת חוק.

בצורך בקבלת הסכמה מדעת, במגבלות שונות בנוגע לאיסוף מידע מסוגים שונים (שעיקרון מרכזי בהן הוא עקרון צמידות המטרה, כלומר, שהשימוש במידע צריך להיות צמוד למטרה הראשונית שהודעה לאדם), במגבלות החלות על השימושים האפשריים במידע, בחובות נוספות שמוטלות על מעבדי המידע (כגון חובת סודיות ואבטחת מידע, ולפי הדין העדכני באיחוד האירופי – גם חובות ארגוניות שונות), וכן בזכויות שונות של מושאי המידע (data subjects), כגון זכות הגישה למידע על-אודותיהם והזכות לדרוש את תיקונם.<sup>16</sup> הדין האירופי להגנת מידע אישי, שנכנס לתוקף במאי 2018 (ה-GDPR), מגדיר במפורש את פעולת הפרופילינג,<sup>17</sup> וקובע חובה ליידע את מושא המידע בדבר פעולה של פרופילינג וקבלת החלטות על בסיסה, ובכלל זה להעביר לו מידע על הלוגיקה של קבלת ההחלטות,<sup>18</sup> וכן להעניק לו זכות גישה לפרופיל<sup>19</sup> וזכות להתנגד לעיבוד מידע במצבים מסוימים,<sup>20</sup> כאשר מתקבלת החלטה שיש לה השלכה משפטית על מושא המידע.<sup>21</sup> הדין הישראלי הנוכחי חסר בכל ההיבטים האלה.

סטרקטורלי 'ופורת מתמקדים באיסוף מידע, בעיבודו וביצירת פרופיל על בני-אדם לשם עיצוב הכללים המשפטיים עצמם. עיקר עניינם הוא בכללי בררת-מחדל, אשר מציעים אפשרות אחת, שתחול כל עוד האדם לא ישנה אותה. דוגמה שנדונה במאמר היא דיני הירושה, שקובעים בררת-מחדל ומסדירים את סדר הירושה ואת חלקו של כל יורש, אולם באמצעות כתיבת צוואה ניתן לשנות את בררת-המחדל. איסוף מידע ועיבודו לשם עיצוב הכללים מעוררים מייד כמה סוגיות של פרטיות: עצם איסוף המידע, השימוש בו, יצירת הפרופיל על בסיסו והשימוש בפרופיל למטרה של עיצוב הכללים. הבעיה מחריפה כאשר המידע נאסף אגב שירות אחד, ספציפי, וכעת הוא משמש למטרה נוספת, כללית, של עיצוב כלל משפטי. נוסף על כך, העמדת אדם מסוים אל מול דפוס כללי, בוודאי כמה שהמחברים מכנים התאמה אישית עדינה, מחייבת יצירת פרופיל של אותו אדם, ולפעולה זו יש השפעה משפטית מיידית עליו.

16 בישראל ראו פרק ב לחוק הגנת הפרטיות וכן את תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, ק"ת התשע"ז 1022 (להלן: תקנות אבטחת מידע). באשר לאיחוד האירופי, הרגולציה שנכנסה שם לתוקף במאי 2018 – ה-GDPR – קובעת את הכללים שיש לפעול לפיהם.

17 ס' 4(4) ל-GDPR, לעיל ה"ש 4, מגדיר:

“profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

18 ס' 13(2)(f) ל-GDPR, וכך גם כאשר המידע נאסף לא ממושג המידע עצמו – ס' 14(2)(g) ל-GDPR.

19 ס' 15(1)(h) ל-GDPR.

20 ס' 21 ל-GDPR.

21 ס' 22 ל-GDPR.

## 2. עיבודי מידע

סטרכילביץ' ופורת מזכירים סוגים שונים של כללי בררת-מחדל: כללים של רוב וכללים של מיעוט, אבל גם אלה לדידם גסים מדי, והם מתארים מצבים שבהם העלות של שינוי הכללים גבוהה מדי. לטענתם, כללי בררת-מחדל מותאמים אישית יכולים לסייע בעניין זה. התאמה אישית גסה תתבסס על נתון מרכזי אחד (למשל, גיל, מגדר או משקל, אם לשפוט לפי הרוגמאות שהם מביאים), ואילו התאמה אישית עדינה יותר תביא בחשבון שלל נתונים. ראוי להבחין כאן בין שני אופנים שונים של עיבודי מידע – הבחנה שהיא רלוונטית לניתוח של דיני הפרטיות. אופן אחד של עיבוד מידע הוא כאשר נתוני-עתק משמשים לזיהוי דפוסי התנהגות כלליים, ואז לכל אדם מותאם הדפוס המתאים לו ביותר מבין אותם דפוסים. זהו הליך דו-שלבי: תחילה, איסוף מידע כללי לשם איתור דפוסי התנהגות, ולאחר-מכן איסוף מידע על אדם מסוים ומציאת הדפוס המתאים לו ביותר.

עיקר הביקורת שעלתה בספרות בקשר לאופן זה של עיבוד מידע בדרך של איתור דפוסים כללים אינה נוגעת בהיבטי הפרטיות, אלא ביכולת לזהות את הדפוסים הנכונים בצורה מדויקת. חסידי השימוש בנתוני-עתק למטרה זו נוטים להתייחס לממצאיהם כאילו הם משקפים את המציאות. תפיסה זו מגולמת לעיתים בביטוי  $N=ALL$ , כלומר, שאין מדובר בהסקת מסקנות על-סמך מודגם, אלא בתיאור כלל האוכלוסייה, ולכן לממצאים יש תוקף מוחלט. אכן, נראה שגם המחברים במאמרם מניחים כי עיבוד של נתוני-עתק יכול להוביל לגילוי אמת אובייקטיבית. אולם המבקרים מצביעים על שורה של כשלים בהנחות בדבר כוחו של העיבוד של נתוני-עתק, במיוחד בקשר לאמונה הכמעט-דתית בכוחם של נתוני-עתק לשקף את המציאות האובייקטיבית.<sup>22</sup> מיריי הילדברנדט (Hildebrandt) מצביעה על היבטים של האישיות שאינם ניתנים לכימות ולמחשוב, ומכנה זאת incomputability.<sup>23</sup> דנה בויד (boyd) וקייט קרופורד (Crawford) הצביעו גם הן על צורך בזהירות בהסקת מסקנות מנתוני-עתק, הן מן הטעם שהעלתה הילדברנדט והן מטעמים נוספים, ביניהם החשיבות של שמירה על ההקשר של המידע, היבטים אתיים והיבטים חלוקתיים.<sup>24</sup> ביקורת חשובה נוספת נמתחה על ההיגיון שמנחה את ההסתמכות על נתוני-עתק בעיצוב מדיניות, ששונה מהתפיסה המערבית הרווחת של המשפט, מהבסיס הערכי-הנורמטיבי שלו ומצורת ההתפתחות של המשפט.<sup>25</sup> כך או כך, אין כאן שאלה ישירה של פרטיות, ולכן שאיר אותה בצד.

לגבי השלב הראשון, איסוף מידע על "שפני-ניסיון", כפי שהמחברים מציעים,<sup>26</sup> יכול לסייע, אם הוא נעשה כשורה, באיתור דפוסים כלליים ובגיבוש כללי בררת-המחדל לפיהם.

22 ראו, למשל, MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW 166 (2015); Caryn Devins, Teppo Felin, Stuart Kauffman & Roger Koppl, *The Law and Big Data*, 27 CORNELL J.L. & PUB. POL'Y 357, 371–79 (2017)

23 Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQ. L. 83, 91 (2019)

24 danah boyd & Kate Crawford, *Critical Questions for Big Data*, 15 INFO. COMM. & Soc'y 662 (2012)

25 ראו Devins et al., לעיל ה"ש 22.

26 סטרכילביץ' ופורת, לעיל ה"ש 2, תת-פרק 3.



איסוף מידע כזה ייעשה, לפי הצעתם של המחברים במאמרם, בהסכמה מלאה של המשתתפים, ומשום כך הפגיעה בפרטיות של אותם שפני-ניסיון תצטמצם עד כדי איונה המלא (אם כי ייתכנו היבטים אתיים אחרים במצב כזה). דיני הפרטיות חלים כאן, אולם מאחר שיש מפגש ישיר בין אוספי המידע לבין אותם שפני-ניסיון, ניתן ליידע אותם, להסביר להם היטב את מטרת השימוש במידע, ולקבל את הסכמתם, שצריכה להיות מדעת ומרצון חופשי. כן מוטל על הגורם האוסף את המידע לא לחרוג מההסכמה שניתנה, ולעמוד בשאר הכללים שיש ברין. אם המידע נאסף ממשתמשים שלא הסכימו להיות שפני-ניסיון, אזי מתעוררות שאלות של פרטיות: איסוף המידע מחייב עמידה מלאה בכללים השונים שיש ברין, שנזכרו לעיל, בדבר הודעה, הסכמה וכן הלאה. ניסיון אחד להימלט מדרישות החוק הוא להתמים את המידע, כלומר, ליצור אנונימיזציה שלו. ההנחה היא שמידע שאינו מזהה בני-אדם אינו פוגע בפרטיותם. אולם התממה אינה פותרת את הקשיים. ראשית, מדעני המחשב כופרים ביכולת לבצע התממה מלאה.<sup>27</sup> מבחינתם, השאלה אינה אם אפשר לבצע הנדסה חוזרת ולחשוף זהות, אלא רק כמה זמן ומשאבים צריך להשקיע לשם כך. שנית, נטילת מידע שנאסף למטרה אחת, בדרך-כלל מתן שירות כלשהו, ועיבודו למטרה אחרת – גם אם היא ראויה וגם אם העיבוד נעשה באופן אנונימי – מחייבים הסכמה לעצם ביצועה של ההתממה. סוגיה זו טרם הוכרעה במפורש ברין האירופי או הישראלי, אולם יש לה כבר הדים בפסיקה, ויש דיון בה בספרות.<sup>28</sup>

השלב השני הוא כאשר הכללים כבר גובשו וכעת הם מופעלים – צרכן חדש יאופיין לפי אחד הדפוסים שזוהו בשלב הראשון, ומרגע שהוא יסוג לפי דפוס מסוים, יופעל כלפיו דפוס זה. במידה רבה אין זו פרקטיקה חדשה. מפרסמים נהגו כך גם בעבר, על-ידי סיווג אוכלוסיית הצרכנים הפוטנציאליים לקבוצות שונות והתאמת אסטרטגיות פרסום שונות לכל קבוצה.<sup>29</sup> אולם כיום זיהוי הקבוצות ודפוסי ההתנהגות שלהן מבוסס יותר על נתונים, ופחות על הערכות גרידא. לכן בשלב שני זה עשויים להתעורר קשיים של פרטיות, שכן

27 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 U.C.L.A. L. Rev. 1701 (2010)

28 במהלך דיון בתביעת נזיקין בגין רשלנות רפואית ביקש עד מומחה להציג מסמכים רפואיים מותממים של מטופל אחר. הצד שכנגד ביקש לפסול את הגשת המסמך המותמם בטענה שזו פגיעה בפרטיותו של המטופל האחר. בבית-המשפט העליון קבעה השופטת וילנר, כדנה יחידה, כי ניתן להגיש את המסמך שבו הושחרו פרטי המטופל האחר, אולם היא התייחסה גם לשלב המקדים, של איסוף המידע, ולצורך לבחון אותו. ראו רע"א 7828/17 הסתדרות מדיצינית הרסה נ' פלוני (פורסם בנוב, 9.1.2018). במקום אחר, בהקשר של עיבוד נתוני-עתק רפואיים, הסברתי מדוע יש חובה לקבל הסכמה מדעת גם לעצם ההתממה ולשימושים במידע מותמם. ראו Michael Birnhack, *A Process-Based Approach to Informational Privacy and the Case of Big Medical Data*, 20 THEORETICAL INQ. L. 257 (2019). עוד על התממה ופרטיות

29 ראו שרון ברזיו וטל ז'רסקי "פרטיות במשבר זהות: אסטרטגיות הסדרה בעידן ההתממה" משפט, חברה ותרבות ב 125 (מיכאל בירנהק עורך, 2019).  
לדיון בפילוחים בקרב חברות לניתוחי שוק ראו מיכאל בירנהק מרחב פרטי – הזכות לפרטיות בין משפט לטכנולוגיה 173 (2010).

סיווג הלקוח לדפוס מסוים מצריך איסוף מידע אישי ממנו. הזכות לפרטיות אמורה לתת בידי הלקוח כוח להתנגד לסיווג, וכך להיחלץ מהצבת המקבעת של השלב הראשון בתהליך. אופן אחר של עיבוד מידע הוא כאשר אין זיהוי מוקדם של דפוסי פעולה, אלא התאמה אישית מלאה לכל אדם ואדם – לדוגמה, התאמה של כרית-אוויר למשקלו של הנוסע המסוים. במקרים אלה אין צורך באיתור דפוס כללי (אלא רק בהבנה הכללית שלמשקל הנוסע, בדוגמה שלעיל, יש משמעות לגבי פעולתה של כרית-האוויר), וההתאמה האישית נעשית רק על-סמך מאפייני האדם ברגע נתון ומסוים אחד.<sup>30</sup> מכאן שאין צורך באיסוף מידע ובעיבודו בטכנולוגיות של נתוני-עתק עד להשגת אלגוריתם, אלא רק באיסוף מידע על האדם המסוים. קשיי הפרטיות שמתעוררים כאן מתלכדים עם אלה שהזכרתי בקשר לשלב השני של אופן העיבוד הראשון, ואשוב לכך בהמשך.

פרטי הפעולה של המנגנון הטכנולוגי לעיצוב כללים משפטיים על בסיס נתוני-עתק חשובים עדי-מאוד. למשל, בדיון בביקורת אפשרית על חשש מהתנהגות אסטרטגית, המחברים מציינים כי "צרכנים לא באמת ירוויחו מכך שהם יעמידו פנים שהם משהו אחר. מאפיינים מסוימים של צרכנים עשויים להועיל להם בעסקאות מסוימות אך להזיק להם בעסקאות אחרות".<sup>31</sup> כלומר, נראה שהמחברים סבורים כי יהיה מנגנון טכנולוגי כללי אחד שירכז את כל המידע ויצור פרופיל אחד ואחוד שיהיה נגיש לכל המוכרים באשר הם, ואולי גם למדינה. לקיומו של מאגר מרכזי כזה יש השלכות ניכרות בהקשר של פרטיות לעומת אוסף של מאגרים מבוזרים, ובמיוחד בהיבט של אבטחת מידע. נוסף על כך, אם המדינה היא מנהלת המאגר, מתעוררות שאלות חוקתיות כבדות-משקל של הסמכה, תכליות ומידתיות.<sup>32</sup>

### 3. מדינה ואזרחיה; תאגיד ולקוחותיו

כאמור, המחברים מציעים שכללי בררת-המחדל יותאמו באופן אישי לצרכן/אזרח על-סמך איסוף מידע ועיבודו בטכנולוגיות של נתוני-עתק. הם מביאים דוגמאות מהקשרים ציבוריים ומהקשרים פרטיים גם-יחד. אני סבור שהיה ראוי להפריד בין שני סוגי הדוגמאות, שכן היחסים שבין המדינה לאזרחיה שונים מהיחסים שבין מוכר לצרכן. בהקשר הראשון, של יחסי המדינה ואזרחיה, נתעקש לא רק על יעילות, אלא גם על שורה של ערכים חוקתיים. בהתאם, מסגרת הבדיקה של שימוש מדינתי במידע, ובכלל זה בנתוני-עתק, היא זו שקבועה בחוק-יסוד: כבוד האדם וחירותו, שמגן באופן כללי על הפרטיות (סעיף 7 (א) קובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"), ומתווה בפסקת ההגבלה כיצד ניתן בכל-זאת לפגוע בה במקרים המתאימים.

30 דיון בדוגמה זו נמצא במאמרם המקורי של המחברים: Porat & Strahilevitz, לעיל ה"ש 2, בעמ' 1433-1434.

31 סטרכילביץ' ופורת, לעיל ה"ש 2, בפסקה האחרונה בתת-פרק 2ג.

32 ראו לעניין זה את הביקורת על המאגר הביומטרי שהוקם לפי חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009, ואת הדיון אצל קרין נהון 'קול פרטי: הפוליטיקה של המאגר הביומטרי' משפט, חברה ותרבות ב 271 (מיכאל בירנהק עורך, 2019). לצורך בהסמכה מפורשת בחוק לצורך פגיעה בפרטיות ראו, למשל, רע"א 2558/16 פלונית נ' קצין התגמולים – משרד הביטחון (פורסם בנבו, 5.11.2017).

בהקשר השני, של יחסים בין תאגיד ללקוחותיו, נשאף ליצור תנאים מיטביים לתפקודו של השוק. למדינה יש תפקיד גם בהקשר הצרכני – לסייע לצדדים לקיים עסקאות שרצויות להם – אולם היא אינה מעורבת באופן ישיר בעסקאות כאלה. היא קובעת את כללי המשחק, תומכת בהם, ואמורה לאכוף אותם במידת הצורך, אבל בדרך-כלל אין היא משחקת בעצמה. כללי משחק אלה כוללים הסדרה מפורטת של השימושים במידע אישי, כפי שתואר קודם, לכל אורך מחזור החיים של המידע.

היבט של הפרטיות הקושי הוא, כאמור, שכדי לגבש כללי בררת-מחדל מותאמים אישית יש צורך באיסוף אינטנסיבי של מידע, והדיון העלה שעיקר הקושי הוא בשלב של איסוף המידע הפרטני מלקוחות שאינם שפני-ניסיון שהסכימו לכך, וכן באיסוף המידע מלקוחות ומאזרחים לשם סיווגם לדפוס המתאים.

### ב. פרטיות לפי סטרכילביץ' ופורת

ראינו שעיבוד מידע באמצעות נתוני-עתק למטרה של איתור דפוסים כלליים, ואז התאמה של אדם לדפוסים כאלה, מעוררים שאלות של פרטיות במידע, ובמדינות שבהן המשפט מסדיר את איסוף המידע ועיבודו יש כללים שונים שיש לעמוד בהם. המחברים לא התעכבו על כללים אלה, ואיני בא בטרוניה על כך – אין זה מוקד הדיון שלהם. הקושי אינו בהתייחסות לדיון, אלא בלב תפיסתם בנוגע לפרטיות. הם דנים בפרטיות רק לקראת סוף מאמרם, כאחת הביקורות האפשריות על הצעתם לכללי בררת-מחדל מותאמים אישית, ומשום כך הדיון שם קצר. המחברים אינם מציגים את תפיסתם לגבי מהותה של הפרטיות (וגם על כך איני בא בטרוניה), אולם לאורך המאמר יש רמזים אחדים שניתן לחלץ מהם את עמדתם בקשר לפרטיות. את חלקם כבר ציינתי. התמונה העולה היא שתפיסתם בנוגע לפרטיות רזה מאוד, ובוודאי רזה מההגנה המשפטית הקיימת בדיון.

ראשית, הדיון הישיר של המחברים בסוגיית הפרטיות מציג אותה, במידה רבה, כמטרד שניתן להתגבר עליו בקלות. ההתגברות היא בדרך של ויתור על הפרטיות. המחברים מזכירים התנגשויות אחרות בין הפרטיות לבין ביטחון, מניעת הפליה וחדשנות, ומשתמע שהם סבורים כי אינטרסים חשובים אלה גוברים על הפרטיות. את המתח בין פרטיות לבין התאמה אישית, שאותה הם מציגים כמקדמת יעילות, הם מתארים באופן דומה. במילים אחרות, הם סבורים כי בתחרות שבין הזכות לפרטיות לבין אינטרס היעילות, היעילות צריכה לגבור, אפריורית.<sup>33</sup>

אכן, לעיתים יש התנגשויות בין הפרטיות לבין אינטרסים ציבוריים חשובים, ואוסיף – גם בין הפרטיות לבין זכויות-יסוד אחרות, כחופש הביטוי, ולעיתים קרובות הזכויות או האינטרסים היריבים גוברים על הפרטיות.<sup>34</sup> אולם זו יכולה להיות לכל-היותר מסקנה של דיון,

33 בן-שחר ופורת נקטו עמדה דומה בקשר להתאמה אישית של דיני הנזיקין. ראו Omri Ben-Shahar & Ariel Porat, *Personalizing Negligence Law*, 91 N.Y.U. L. Rev. 627, 687–88 (2016).

34 בהקשר הישראלי ראו, למשל, את האיזון בין פרטיות לבין צרכי אכיפת חוק בקשר לשימוש של רשויות חקירה בנתוני תקשורת. בג"ץ 3809/08 האגודה לזכויות האזרח בישראל נ' משטרת ישראל (פורסם בנבו, 28.5.2012).

ולא נקודת המוצא. המסקנה אמורה לבוא רק אחרי בדיקה פרטנית של הזכויות והאינטרסים האחרים, ובשפה החוקתית המשפטית הישראלית – רק אחרי שנערך איזון אינטרסים ("איזון אנכי" מול אינטרסים ו"איזון אופקי" מול זכויות שוות-מעמד) במסגרת פסקת ההגבלה.<sup>35</sup> נוסף על כך, עמדה זו, שמבטלת מראש את הפרטיות, שוללת אפשרות אחרת: שאין התנגשות של ממש בין פרטיות לבין יעילות וחדשנות.<sup>36</sup> יש שלל דרכים שבהן ניתן דווקא לשלב פרטיות עם חדשנות. בשפה הכלכלית נאמר שיש ביקוש ניכר לפרטיות. ספקי שירותים שידעו להגן על הפרטיות יוכלו להתהדר בכך,<sup>37</sup> ובדרך זו ליצור שוק של פרטיות. שוק כזה יממש את העדפותיהם של הצרכנים ובו-בזמן יאפשר פעילות עסקית, וכך תגדל הרווחה המצרפית ותושג יעילות. נוסף על כך, שירותים שאין בצידם הגנה מספקת של פרטיות עלולים להתיע משתמשים רבים, כך שדווקא העדר פרטיות עלול לפגוע בחדשנות וביעילות. למשל, בעקבות פרשת פייסבוק וקיימברידג' אנליטיקה, שנחשפה באביב 2018, גברה ההבנה בקרב משתמשיה של אותה רשת חברתית בנוגע לאיסוף המידע, ורבים מהם שינו את התנהגותם שם.<sup>38</sup> כמוכן, לעיתים יש התנגשויות של ממש בין הפרטיות לבין אינטרסים אחרים, אלא שאז, כאמור, יש מקום לאיזון פרטני, ולא לביטול מוקדם של הפרטיות.

שנית, נראה שאת עיקר הקושי בהיבט של הפרטיות המחברים מזהים בשלב הראשוני של איסוף המידע או גילויו. הדבר עולה ממקורות המידע שהם מציינים ומדוגמאות שונות במאמרם. כך, למשל, הם מביאים דוגמה לתניה בדבר מקום הספקת הנכס שעניינה בצרכן שמרותק לכיסא-גלגלים המבקש לרכוש טלוויזיה.<sup>39</sup> המחברים מצביעים על כך שהצרכן נדרש לחשוף מידע על מוגבלותו כדי להביא לידי כך שכלל בררת-המחלל המותאם אישית יקבע כי מקום ההספקה של המוצר יהיה בביתו, ולא בחנות. שלב איסוף המידע חשוב, כמוכן, אולם הוא רק שלב אחד, ראשון, בשרשרת המידע. ההתמקדות בשלב זה בלבד מרדדת את הפרטיות לסודיות, וממעיתה מערכה של הפרטיות בשאר שלביו של מחזור החיים של המידע האישי. כך, אחרי שלב האיסוף של המידע מגיע שלב עיבוד המידע. הבנה מהותית של הזכות לפרטיות תדרוש שתכלית העיבוד תהיה ראויה, ושמעבר המידע יפעל בשקיפות בקשר לצורת העיבוד ובאחריותות בקשר לכל פעולותיו. הבנה מהותית של הפרטיות תעמוד

35 גם בדין האירופי נדרש איזון. לפי ס' 8 של ה"European Convention on Human Rights", כדי להצדיק פגיעה בפרטיות, נדרשות הסמכה בחוק, תכלית ראויה ומידתיות של האמצעי אל מול התכלית הראויה.

36 לביקורת על ההנגדה בין חדשנות לפרטיות, במיוחד בהקשר של טכנולוגיות של נתוני-עתק, ראו Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).

37 למשל, במחקר אמפירי שנערך בישראל נמצא כי אתרי מרשתת רבים – יותר מ-50% מהאתרים שנדגמו – התפארו בהגנת המידע שהם מספקים, הגם שאין חובה בחוק לפרט זאת. ראו Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. & TECH. L. REV. 337, 368 (2011).

38 ראו, למשל, Julie Beck, *People Are Changing the Way They Use Social Media*, THE ATLANTIC (June 7, 2018), <https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/>.

39 סטרכילביץ' ופורת, לעיל ה"ש 2, אחרי ה"ש 24 (הצגת הדוגמה) וחלק ב(א) (דיון בגילוי המוגבלות הפיזית).

על זכותם של מושאי המידע לעיין במידע על-אודותיהם, לתקנו, להגביל את השימושים בו, להורות על הפסקת השימוש במידע שלהם ואף על מחיקתו, ועוד. מובן שמתעוררות פה שאלות רבות בדבר יישום הכללים, אולם כאשר אנו עוצרים אחרי שלב איסוף המידע, שאלות אלה אינן נשאלות כלל.

שלישית, מקורות המידע שהמחברים מציינים מגוונים, וכוללים את "האפשרות לעקוב אחר התנהגויות של פרטים במרשתת, לאסוף מידע ממאגרי מידע שונים ולעשות שימושים בטכנולוגיות לעיבוד נתוני-עתק".<sup>40</sup> כל אחד מהמקורות האלה מעורר קשיים משלו. כך, מעקב אחר התנהגות ברשת מניח שוויון הזדמנויות ושוויון שימושים, אלא שיש פערים דיגיטליים רבים ומתועדים בין משתמשים. הפערים הבולטים הם לכלליים, אבל יש גם פערים של שפה, אוריינות טכנולוגית, מגבלות פיזיות שונות ועוד. איתור דפוסי פעילות מבלי להתחשב בשונות שבין בני-האדם המשתמשים – במיוחד כאשר הפעולה נועדה לאתר את השונות הזו בדיוק – יהיה חלקי, וככל שהוא יהווה בסיס למדיניות, המדיניות עלולה להיות מעוותת. הגנת הפרטיות עשויה לצמצם עיוותים אלה. מעניין שבכתיבה קודמת דן סטרכילביץ' בהרחבה בפן החלוקתי של דיני הפרטיות ושל נתוני-עתק.<sup>41</sup>

לגבי מאגרי המידע השונים, המחברים אינם מבחינים כאמור בין מאגרים ציבוריים-שלטוניים לבין מאגרים פרטיים, ובהתייחסותם גלומה הנחה שהמאגרים נגישים לכל ושמנהליהם יסכימו למסור את המידע למטרה של יצירת הפרופיל האחד. אולם עקרון צמידות המטרה הוא עקרון-יסודי בגנת הפרטיות, ולפיו מידע שנמסר למטרה אחת אינו יכול לשמש למטרה אחרת.<sup>42</sup> עיקרון זה משקף את העמדה של פרטיות כשליטה – שארחיב עליה בהמשך – שלפיה מושא המידע הוא שיחליט מה יעלה בגורל המידע שלו. ההנחה של איחוד או הצלבה של מאגרים שונים מבטלת כלאחר-יד את העיקרון הזה ואת מה שביסודו. רביעית, כפי שכבר הערתי, המחברים אינם מבחינים בין שני הסוגים הבסיסיים של הצד האחד של הפרטיות. פרטיות היא זכות הקשרית או זכות יחס, כלומר, יש לה משמעות רק אל מול אחרים. אין משמעות לפרטיות של אדם שנקלע לאי בודד, אלא אולי בינו לבין אלוהיו, כאדם וחיה בגן-עדן. פרטיות של אזרח מול המדינה שונה מפרטיותו של אותו אזרח בכובעו כצרכן מול תאגיד שמבקש לאסוף מידע. מערכת היחסים הראשונה מבוססת על הרעיון של אזרחות, של המדינה ככלי חברתי לחיים משותפים וכמימוש של אידיאולוגיה לאומית. זו מערכת יחסים שמכתיבה עקרונות ידועים במשפט המנהלי – למשל, שהמדינה היא נאמן הציבור. משום כך אנחנו זהירים בכוחה של המדינה, מגבילים אותה בחובה לציית לזכות חוקתית לפרטיות, ודורשים ממנה לעמוד בתנאים נוקשים בשעה שהיא מבקשת לפגוע בכל-זאת בזכות לפרטיות. מול התאגידים, לעומת זאת, ההחלטה אם למסור מידע אישי

40 שם, ליד ה"ש 115.

41 Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. (2013) 2021–33, 2010.

42 לעיקרון זה יש ביטוי מפורש בדין הישראלי. ראו ס' 2(9) לחוק הגנת הפרטיות ואת פרשנותו בעניין עת"ם (מנהליים ת"א) 24867-02-11 איי. די. איי חברה לביטוח בע"מ נ' רשם מאגרי המידע (פורסם בנבו, 5.8.2012). בדין האירופי ראו ס' 5(1)(b) ל-GDPR.

היא של האדם. נקודת המוצא היא שמדובר ביחסים שוקיים. מאחר שביחסים אלה יש פערי כוחות ידועים וכשלים מוכרים, המשפט מסייע לצרכנים להגן על פרטיותם. חמישית, וגם על כך הערתי, נראה שהמחברים מניחים כי יהיה פרופיל אחד אחר לכל צרכן. התוצאה היא שיווצר פרופיל צרכני שלא יהיה אפשר להתחמק ממנו: הוא יסווג את האדם לדרפוס מסוים, ואז אותו אדם לא יקבל הצעות אחרות מחוץ למתחם שאליו סווג. הסיווג נהפך כך לקיבוע, והתהליך נהפך להסללה, שמקשה ניעות חברתית וכלכלית. אלה בעיות כלליות של פרופילים, שמתיימרים לשקף את האדם אבל בפועל מגבילים את התנהגותו. אולם הגנת הפרטיות שמופקדת בידי צרכנים אמורה לתת להם כלי מסוים להגביל את יצירתו של פרופיל כזה, ומחזירה אותם לתמונה – לא ככלי-משחק, אלא כבני-אדם אוטונומיים. מעבר לכך, במאגר מרכזי יש סכנות ידועות של שימוש לרעה, שימוש חורג (למטרות שלא לשמן נאסף המידע), פגיעה בסודיות וכשלים באבטחת מידע. יש לכך פתרונות טכנולוגיים אפשריים, כגון קיום מאגרים נפרדים ומבוזרים, אשר לכל-היותר נשלף מהם מידע ברזומנית לפי שאילתה פרטנית ומתועדת, אבל המידע עצמו מתפוגג בתום השימוש. אולם כל עוד יש מאגר אחד, החשש ממשי וניכר.

שישית, המחברים מציעים דרך מעניינת לזהות את מי שפרטיותו יקרה לו – על-ידי שימוש במודל המוצע עצמו, קרי, על-ידי איסוף מידע על התנהגותם של המשתמשים ומאפייניהם. למשל, "אם הפרופיל של לקוח מעיד כי חשוב לו מאוד לשמור על פרטיותו באשר לדרך גלישתו במרשתת... אזי אין לאסוף מידע על-אודותיו, אלא אם כן הוא הביע רצון אחר באופן ברור ומפורש".<sup>43</sup> במילים אחרות, הם מציעים שהפרסונליזציה תופעל כדי לזהות את מי שאינו מעוניין בה. אלא שכאן המודל נקלע לסחרור מסוים. ראשית, לשיטתם, יש לאסוף מידע על המשתמש רק כדי להגיע למסקנה שאין לו עניין בכך. שנית, וזו ביקורת חשובה יותר, המחברים מבקשים להסיק את ההעדפה של פרטיות מתוך ההתנהגות. בעגה הכלכלית, הם מבקשים לזהות את ההעדפות הגלויות של צרכנים (revealed preferences), ומציינים כי להעדפות גלויות יש יתרון על תשובות שמתקבלות בסקרי צרכנים.<sup>44</sup> אלא שבתחום הפרטיות התנהגות היא סימן רעוע להעדפת פרטיות. פער כזה בין העדפת פרטיות לבין התנהגות בקשר למידע אישי זוהה בספרות זה כבר, וכונה "פרדוקס הפרטיות".<sup>45</sup> זהו הפער שבין העדפה לבין התנהגות: גולשים רבים מביעים עניין בהגנה על פרטיותם אבל מתנהגים באופן שנחזה כאחר, כלומר, מפרסמים מידע אישי רב ברשת.

בספרות ובמחקר הוצעו הסברים שונים לפער הזה, שאושרו במחקרים אמפיריים. בחלק מהמקרים מדובר בהחלטה מודעת של המשתמש לוותר על פרטיותו בתמורה לערך שהוא מקבל כתוצאה מכך. אם משתמשת ברשת חברתית מבינה שפרסום תמונה שלה פוגע בפרטיותה במידת-מה מול חבריה ברשת ומול הרשת עצמה, ועושה כן בכל-זאת משום ההון התרבותי שהיא נהנית ממנו בפעילות זו, אזי אין כאן פער. אולם ההתנהגות בדוגמה זו

43 סטרכילביץ' ופורת, לעיל ה"ש 2, בפסקה האחרונה של תת-פרק 8.

44 שם, אחרי ה"ש 57.

45 לדיון ראשון ראו Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007).

אינה מעידה על המעטה בערך הפרטיות בכלל, אלא על פשרה מודעת בהקשר מסוים.<sup>46</sup> אין להסיק מכך ויתור גורף. במקרים אחרים מדובר בפערי ידע ומידע: משתמשים אינם מבינים תמיד מה המשמעות של פרסום המידע ברשת. הם אינם יודעים מי עשוי לראות את המידע מעבר למעגל ה"חברים" המיידי (התשובה היא שהכל עשויים לראות את המידע, ובכלל זה חברות ביטוח, מעסיקים, המדינה ואחרים), ובעיקר הם אינם מבינים את איסוף המידע בהקשר התאגידי, כלומר, על-ידי הרשת עצמה.<sup>47</sup> לבסוף, יש שורה של הטיות קוגניטיביות שמגבילות את היכולת להבין את הפעולות של איסוף המידע ולהתנהג בצורה נבונה בעניין.<sup>48</sup>

\* \* \*

העולה מן האמור הוא שהמחברים מניחים מראש שהפרטיות היא אינטרס צר שמתמקד באיסוף מידע בלבד, תוך התבססות על התנהגות נחזית שאינה משקפת בהכרח העדפות־אמת, ושהאינטרס הצר הזה ניגף בקלות מול אינטרסים אחרים, בלי קשר לשאלה אם הצד הניצב ממול הוא המדינה או תאגיד. במקום גישה זו, יש לבחון את הזכות לפרטיות ביסודיות. לאחר־מכן יהיה אפשר לבחון שוב את המפגש של הפרטיות עם האינטרס של השאת יעילות בדרך של עיצוב כללי בררת־מחדל בהתאמה אישית.

## ג. פרטיות – תפיסה מהותית

### 1. פרטיות כשליטה

מול התפיסה הרזה של פרטיות שהמחברים מניחים כמאמרם ראוי להציב תפיסה רחבה יותר של הזכות לפרטיות במידע, שהיא גם הדרך שבה הפרטיות מוכנת כיום ברוב מדינות העולם. יש להקדים ולומר כי ארצות־הברית חריגה מעט בנוף הזה, והגנת הפרטיות שהדין הפדרלי מציע בנוגע למידע אישי צרה מזו שבאיחוד האירופי, אם כי גם בכך מתרחשים לאחורונה שינויים משמעותיים, בעקבות חוק הגנת פרטיות מקיף שהתקבל בקליפורניה והצעות לחקיקה פדרלית שתלויות ועומדות בקונגרס נכון למועד כתיבתן של שורות אלה.<sup>49</sup>

Jay P. Kesan., Carol M. Hayes & Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267 (2016) 46

נמצא שמשמשי הרשתות החברתיות מוטרידים מההקשר החברתי הרבה יותר מאשר מההקשר התאגידי. ראו Alyson Leigh Young & Anabel Quan-Haase, *Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited*, 16 INFO. COMM. & Soc'y 479 (2013). 47

Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, in DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363 (Alessandro Acquisti et al. eds., 2007). 48

לשוני העקרוני בתפיסת הפרטיות בין הדין האירופי לדין האמריקני ראו James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004). לחוק החדש בקליפורניה, שנכנס לתוקף בראשית 2020, ראו California Consumer Privacy Act (CCPA) of 2018. 49

בספרות הוצעו הצדקות אין-ספור לזכות לפרטיות, עד כדי כך שיש חוקרים שהרימו ידיים או פנו לאפיקים תיאוריים והציעו מתווה לזיהוי פגיעה בפרטיות.<sup>50</sup> במקום אחר קיבצתי את ההצדקות העיקריות והצעתי לארגן אותן בסדרה של מעגלים קונצנטריים, לפי הקשרי התייחסות שונים: מעגל האדם, מעגל הקשרים הבין-אישיים, מעגל הקהילה ומעגל המדינה.<sup>51</sup> הפרטיות חשובה ומוצדקת בכל אחד מההקשרים האלה. ההצדקות מדגישות את תפיסת האדם, את הצורך הפסיכולוגי והאינטלקטואלי של האדם במרחב פרטי נטול מעקב מנטר וממשמע, את הצורך שלו בהצגת העצמי באופן קוהרנטי, את הצורך שלו בטיפוח קשרים אינטימיים וקשרים מקצועיים, את חשיבותה של הפרטיות לכינון החברה ולתפקודה (ובכך יש הדגשה חשובה שהפרטיות אינה רק זכות ליברלית שמדמה אנשים נפרדים ופרודים זה מזה, אלא זכות שיש לה ערך חברתי ראשון במעלה)<sup>52</sup> ואת חשיבותה של הפרטיות לזוהתה של המדינה כמדינה דמוקרטית-ליברלית.

בעיניי, המשותף לכל ההצדקות ולכל ההקשרים הוא ציר מארגן אחד – הבנת הפרטיות כשליטה. רעיון זה הוצע על-ידי אלן וסטין (Westin) עוד לפני חמישים שנה.<sup>53</sup> דניאל סולוב (Solove) הציע לדבר על פרטיות כמופעה השונים כעל משפחה, תוך שימוש במושג הוויטגנשטייני "דמיון משפחתי".<sup>54</sup> ברוח זו אני סבור כי "פרטיות כשליטה" הוא "שם המשפחה" שמתאים כאן. בתמצית, הפרטיות כשליטה היא הכוח והזכות המשפטיים של אדם לקבוע מה יעלה בגורל המידע האישי על-אודותיו.<sup>55</sup> במוכן הזה הפרטיות כשליטה היא נגזרת ישירה של כבוד האדם.<sup>56</sup> ליסה אוסטין (Austin) מציעה להרחיב את ההבנה

50 זו גישתה של הלן ניסנבאום, למשל, שמציעה גישה של "פרטיות הקשרית" – contextual integrity – המבקשת לסייע לנו באיתור המצבים שבהם יש פגיעה בפרטיות. לשיטתה, מצבים אלה הם כאשר יש שינוי בכללי זרימת המידע בהקשר חברתי נתון. ראו, HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2010) Helen Nissenbaum, *Contextual Integrity Up and Down the* *Data Food Chain*, 20 THEORETICAL INQ. L. 221 (2019). בגישתה זו אין הסבר מספק של "הקשר" או התייחסות למצבים של קריסת הקשרים, ובעיקר חסר בו מימד נורמטיבי שיסביר מדוע שינוי בכללי זרימת המידע הוא פגיעה בפרטיות. לביקורת זו ראו, Michael Birnhack, *A Quest for A Theory of Privacy: Context and Control: Review of Helen Nissenbaum's Privacy in Context*, 51 JURIMETRICS 447 (2011).

51 בירנהק, לעיל ה"ש 29, בעמ' 115-125.

52 להדגשת הערך החברתי של הפרטיות ראו את מאמרה פורץ-הדרך של Priscilla M. Regan, *Privacy as a Common Good in the Digital World*, 5 INFO. COMM. & SOC'Y 382 (2002). לגישה עכשווית ראו ARI EZRA WALDMAN, *PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE* (2018).

53 ALAN WESTIN, *PRIVACY AND FREEDOM* 7 (1967).

54 DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* 40 (2008).

55 ראו בירנהק, לעיל ה"ש 29, בעמ' 89.

56 לדיון ראו שם, בעמ' 115-117. לגזירה של הפרטיות מכבוד האדם ראו גם את פסק-דינו של בית-המשפט העליון בהודו שקרא את הזכות לפרטיות בתוך החוקה ההודית אף שהזכות אינה מנויה שם במפורש: Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC



של פרטיות כשליטה, ולומר שהפרטיות היא האפשרות לבחור בחירות משמעותיות בקשר לפרטיות.<sup>57</sup> כך או כך, הפרטיות כשליטה אינה הצדקה כשלעצמה. היא מסקנה של דיון תיאורטי, והיא ציר שמשותף לשורה של הצדקות: יש ביניהן הצדקות שרואות בפרטיות זכות בפני עצמה, ויש ביניהן הצדקות מכשירניות שלפיהן הפרטיות היא אמצעי למניעת עוולות אחרות. למשל, פעמים רבות הפרטיות מאפשרת לאדם לא לחשוף מידע מסוים כאשר יש לו חשש שהדבר יוביל, למשל, להפליה שלו בקבלה למקום עבודה.<sup>58</sup>

תפיסה אחרת היא של הפרטיות כגישה. לפי תפיסה זו, משמעותה של הפרטיות היא הגבלת גישה אל האדם.<sup>59</sup> אולם הפרטיות כשליטה והפרטיות כגישה אינן יריבות. למעשה, הן שני הצדדים של אותה מטבע: פרטיות כשליטה מתחילה מהאדם ובוחרת את יכולתו להפיץ מידע, ואילו פרטיות כגישה בוחרת את הדברים מן הצד האחר – הגישה של האחרים אל האדם. העיקר, כפי שהצביע ארווין אלטמן (Altman), הוא בממשק שבין האדם לבין אחרים – חבריו, סביבתו בכלל, תאגידים והמדינה.<sup>60</sup>

במישור שבין אדם לתאגיד התרגום המשפטי של ההצדקות השונות ושל תפיסת הפרטיות כשליטה ותפיסת הפרטיות כגישה דומה, ומתמצה בעקרונות הגנת המידע שנזכרו לעיל – ה-FIPs. כללים אלה התגבשו בעשורים האחרונים בעולם, וכיום הם הדין המחייב במדינות רבות, וביניהן גם ישראל, אם כי יש צורך בעדכון דחוף של הכללים.<sup>61</sup> לכללים אלה יש חסרונות רבים, וראוי לנסות לחזקם ולתקנם. למשל, לדרישת ההודעה יש חיסרון ידוע: איש כמעט אינו קורא את הודעות הפרטיות. הן ארוכות, מייגעות, מבלבלות וכתובות לרוב בשפה משפטית שאינה נגישה לרוב המשתמשים, וככאלה הן אינן משיגות את המטרה של יידוע של ממש.<sup>62</sup> אולם אלה סוגיות לדיון אחר. כאן אני מבקש לקרוא את הכללים האלה באור הטוב ביותר שלהם.

- 
- 57 Lisa M. Austin, *Re-reading Westin*, 20 THEORETICAL INQ. L. 53 (2019)
- 58 זו, דרך אגב, תוצאה מצערת במובן החברתי, למשל, כאשר אישה לסבית מסתירה את העדפתה המינית בעת קבלה לעבודה מחשש שהיא תופלה עקב כך לרעה, וזאת אף שבחוק שוויון ההזדמנויות בעבודה, התשמ"ח-1988, יש לה הגנה ישירה מפני הפליה. כמובן, העדפה מינית אינה רלוונטית כלל לשאלת התאמתה של מועמדת לעבודה, כך שהנושא אינו אמור לעלות מלכתחילה בריאיון כזה.
- 59 הניסוח הברור ביותר של תפיסה זו נמצא אצל רות גביוון. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980). גביוון פורטת את הפרטיות כגישה לשלושה מצבים של פרטיות: סודיות, אנונימיות ויחידות (solitude).
- 60 Irwin Altman, *Privacy: A Conceptual Analysis*, 8 ENV'T & BEHAV. 7 (1976). לניסוח משפטי עדכני של גישה זו ראו Kirsty Hughes, *A Behavioural Understanding of Privacy and Its Implications for Privacy Law*, 75 MOD. L. REV. 806 (2012).
- 61 ראו מבקר המדינה "היבטים בהגנה על הפרטיות במאגרי מידע" דוח שנתי 2019, 3, 27-39 (2019).
- 62 ראו, למשל, ממצאי מחקר אמפירי נמשך אצל Joseph Turow, Michael Hennessy & Nora Draper, *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015*, 62 J. BROADCASTING & ELECTRONIC MEDIA 461 (2018).

אני סבור כי הדרך המשכנעת ביותר להבין את הכללים האלה היא כניסיון של המשפט לעקוב אחר שלבים שונים במחזור החיים של המידע, תוך יצירת נקודות מפגש שונות בין מושא המידע לבין המידע על-אודותיו.<sup>63</sup> נקודת המפגש הראשונה היא זו של איסוף המידע, אולם לאחריה יש שלבים חשובים נוספים של עיבוד המידע, העברתו הלאה, ולבסוף מחיקתו. בנקודה הראשונה יש למושא המידע אפשרות לקבל החלטה אם להסכים לאיסוף. במהלך עיבוד המידע מוטלות חובות שונות על המעבד, שמטרתן להבטיח כי ההסכמה שניתנה בנקודה הראשונה נשמרת. עקרון צמידות המטרה פועל כאן, וכך גם חובות של שקיפות. למושא המידע יש זכות לעיין במידע שנאסף על-אודותיו, ובכך יש לו אמצעי בקרה מסוים. האכיפה בדיעבד – אכיפה פרטית בדרך של תביעות רגילות או תביעות ייצוגיות, ואכיפה ציבורית של הרשות המוסמכת – אמורה גם היא ליצור נקודת בקרה. לבסוף, הזכות להישכח, כפי שהיא מכונה, מאפשרת למושא המידע להביא את השימוש במידע על-אודותיו לקיצו. במישור הציבורי, כפי שנזכר, כאשר המדינה מבקשת לאסוף מידע ולעבדו, עליה לעמוד בביקורת חוקתית, שבישראל מגולמת בפסקת ההגבלה. כדי לברר אם איסוף מידע הוא מירתי, בתי-משפט עשויים לפנות לעקרונות הגנת המידע – ה-FIPs – ולאמצע להקשר החוקתי. כך המשפט יוצר נקודות מפגש בין מושא המידע לבין המידע על-אודותיו, ומקנה לו מידה מסוימת של שליטה במידע ובעצמו.

כעת, לאחר שהצטיידנו בהבנה עבה יותר של הפרטיות, ניתן לשוב לסוגיה של שימוש בנתוני-עתק לשם עיצוב כללים משפטיים.

## 2. פרטיות ועיצוב כללי בררת-מחדל

ראינו את התפיסה המהותית של הזכות לפרטיות כשליטה של האדם במידע על-אודותיו, וזאת כנגזרת של כבוד האדם וסך של הצדקות שונות. כיצד הבנה זו של הפרטיות משפיעה על הסוגיה של עיצוב כללים משפטיים, ובמקרה הנוכחי – על עיצובם של כללי בררת-מחדל? ראשית, אין מקום להתחיל את הדיון בקביעה כי באיזון שבין היעילות לבין הפרטיות יש לוותר על הפרטיות. הפרטיות היא זכות-יסוד אשר מוגנת ומעוגנת הן במישור החוקתי והן בחקיקה רגילה. יש לה הצדקות משכנעות, ויש לה ביקוש ניכר בקרב הציבור, גם אם ההתנהגות נחזית לעיתים כאחרת. במקום זאת יש לבחון את הפעולות לגופן, כדי לדייק מהי הפגיעה בפרטיות הגלומה באיסוף מידע לצורך עיבודו בטכנולוגיות של נתוני-עתק לשם גיבוש כללים משפטיים. רק לאחר-מכן יהיה אפשר לגשת למלאכת האיזון.

שנית, ראוי לזהות את השחקנים המעורבים כאן. כאשר מדובר במדינה, עליה להסביר מדוע היעילות בעיצוב הכללים ראויה. מאמרם של סטרכילביץ' ופורת מספק הסבר מפורט לעניין זה, אבל יש להתמודד עם הביקורות על עיבוד הנתונים ותקפותו. על המדינה להסביר מדוע איסוף המידע ועיבודו הוא האמצעי המתאים ביותר למטרה, שפגיעתו היא

63 ראו באופן כללי Michael Birnhack & Niv Ahituv, *Privacy Implications of Emerging and Future Technologies* (PRACTIS report, 2013), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2364396](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2364396). גישה זו מצמידה כללים משפטיים לשלבים השונים בתהליך העיבוד של המידע. ליישום בהקשר של נתוני-עתק ומחקר רפואי ראו Birnhack, לעיל ה"ש

הפחותה ביותר. כאן יש לבחון חלופות: לעיתים ניתן לפעול בדרך של ניסוי וטעייה;<sup>64</sup> לעיתים אפשר לערוך מחקר אקדמי מתאים כדי להבין מה הכלל העדיף; ההצעה להשתמש ב"שפני-ניסיון", שהעלו המחברים, עשויה גם היא לפגוע פחות בפרטיות מאשר עיבוד מידע על כלל האוכלוסייה הרלוונטית.

כאשר מדובר בתאגיד פרטי המבקש לגבש כלל פנימי להתנהלותו מול לקוחותיו בדרך של בררות-מחדל מותאמות אישית, ככל שגיבוש כלל כזה כרוך באיסוף מידע אישי ובעיבודו, על התאגיד לעמוד בעקרונות הגנת המידע. משמעות הדבר היא, בין היתר, שעל התאגיד ליידיע את לקוחותיו שהוא אוסף מידע למטרה זו, לבקש מראש את הסכמתם לכך, לא לחרוג מההסכמה, לשמור על סודיות המידע, להקפיד על אבטחתו ועוד.

שלישית, ובהמשך לנקודה הקודמת, יש להבחין בשלבים השונים של חיי המידע. אין לעצור את הדיון בשלב איסוף המידע. שלב זה חשוב, ויש להבהיר בו לאזרחים/צרכנים כי המידע שנאסף על-אודותיהם יישמש, בין היתר, לעיצוב הכללים בדרך האמורה, ולקבל את הסכמתם לכך, גם אם המשך עיבוד המידע ייעשה באופן אנונימי (לכאורה). אבל הדיון אינו מסתיים שם. יש צורך בפירוט ניכר, והפירוט מורכב ומאתגר: יש ליצור מנגנוני שקיפות לבדיקת השימוש במידע;<sup>65</sup> יש לאפשר גישה אל המידע ותיקון שלו במידת הצורך; יש ליצור מנגנוני בקרה; יש להגן על סודיות המידע ועל אבטחת המידע; כאשר ניתנה הסכמה לשימוש במידע במקום אחד אבל לא במקום אחר, אסור להצליב בין המאגרים. לכל זה יש עלות, ואין להלין על כך – לשמירה על זכויות יש עלות, ויש להביאה בחשבון בעת ההחלטה אם לבחור בדרך של עיצוב כללים משפטיים על בסיס נתוני-עתק.

הדור המעודכן של עקרונות הגנת המידע, כפי שהוא מגולם במיוחד ב-GDPR האירופי, מחזק את העקרונות הקודמים, ומוסיף עליהם כללים ארגוניים וטכנולוגיים, תוך הבנה שאלה יכולים לחזק את הגנת הפרטיות לא פחות מאשר כללים משפטיים ישירים. כך, בארגונים יש חובה למנות ממונה הגנת פרטיות במצבים מסוימים. כמו-כן, לפני יישום של מערכת חדשה יש לבצע תהליך של תסקיר הגנת פרטיות, ובמקרה של דליפת מידע יש להודיע על כך לרשות, ולעיתים גם למושאי המידע עצמם.<sup>66</sup> עיקרון נוסף הוא החובה לבצע תהליך של הנדסת פרטיות (Privacy by Design) בעת עיצוב הטכנולוגיה או המערכת. חובה משפטית זו עמומה-משהו, וקשייה בצידה, אולם כאן היא יכולה להועיל בצמצום הפגיעה בפרטיות. מערכות כאלה יודעות, למשל, לזהות מאפיין רלוונטי של המשתמש ולהתאים את עצמן מבלי לאסוף מידע מוקדם ומבלי לשמור את המידע – למשל, הדוגמה שהביאו המחברים

64 על-פי דרך זו לעיצוב כללים משפטיים, המחוקק יחוקק כלל, יבחן אותו, ואם יתברר שטעה, יתקן אותו. לדרך כזו יש כמובן עלויות, שכן עד שנוזהה את הטעות – ככל שיש כזו – יחלוף זמן וייגרמו נזקים. אולם לעיתים אין מנוס מכך. גישה זו מתאימה כאשר התחום המוסדר חדש וקשה להעריך כיצד יפתח, וכאשר יש עניין לתת מרחב פעולה חופשי, לפחות כל עוד הנזקים הצפויים אינם גבוהים מהתועלת הצפויה.

65 דרישה לשקיפות נתקלת לעיתים קרובות בהתנגדות של מעבדי המידע, בטענה שהאלגוריתמים הם בחזקת סוד מסחרי. השגת שקיפות לגבי מקורות איסוף המידע, צורת העיבוד ובעיקר צורת הפעולה של האלגוריתמים שמבוססים על ניתוח המידע היא משימה מורכבת מאוד. לדיון ראו Tal Z. Zarsky, *Transparent Predictions*, 2013 U. Ill. L. Rev. 1503.

66 חובה זו קיימת כיום גם בדין הישראלי לפי תקנות אבטחת מידע, לעיל ה"ש 16.

של כרית-אוויר שמופעלת לפי משקלו של האדם.<sup>67</sup> כך גם לגבי איסוף מידע נקודתי כדי לברר את העדפתו של אדם בקשר לכלל בררת-המחדל. למשל, בדוגמה של הצרכן המבקש לבחור בכלל בררת-מחדל שונה מזה של הרוב בשל רגישות כלשהי שהוא מעדיף לא לפרט רבים, אין צורך לשאול אותו אם הוא סובל מנכות, אלא אפשר פשוט לשאול אותו אם הוא מעדיף לקבל את המוצר בביתו במקום בחנות.

אולם נראה שבמקרים רבים אין כלל צורך בבררות-מחדל. כאשר אנו רוכשים שירותים או מוצרים באמצעות הרשת, אפשר לעצב ממשק פשוט שמציג לצרכן שאלות פשוטות לגבי העדפותיו באותה עסקה: אם הוא מבקש לקבל את המוצר בביתו, בחנות או במקום אחר; אם הוא מעוניין באפשרות החזרה פשוטה של המוצר, בתוספת תשלום, או שהוא מוותר על הזכות הזו; וכן הלאה. ממשקים כאלה קיימים ונמצאים בשימוש נרחב בשורה של שירותים מקוונים. למשל, בעת רכישת כרטיס טיסה ניתן לבחור שירותים נוספים, בין בתשלום ובין לא בתשלום; בעת רכישה ברשת אפשר לבחור בין אפשרויות משלוח שונות; ועוד. כשם שבמסעדה לקוח יכול לבחור את התפריט שמתאים לו לפי רצונו, כך ניתן לבחור מתוך אפשרויות, וכאשר יש אפשרות לממשק פשוט, אין צורך בבררת-מחדל. במילים אחרות, במצבים צרכניים רבים נראה שאין עוד צורך בכללי בררת-מחדל מוכתבים מראש. כך גם בהקשרים שלטוניים. המחברים מביאים דוגמה של שינוי שם משפחה בעקבות נישואים ואת האפשרות של שימוש בהתאמה אישית עדינה לשם כך.<sup>68</sup> לא ברור לי מדוע יש צורך בכך בכלל: הדרך הנכונה בעיניי היא שבעת רישום הנישואים יתבקשו הנישואים לציין איזה שם הם מבקשים לשאת, מבלי להציע להם בררת-מחדל כלשהי מראש.

### 3. מקרה-מבחן: זכרונות דיגיטליים

הביקורת על ההצעה של סטרכילביץ' ופורת שהצגתי כאן מהצד של הפרטיות אינה פוסלת את הצעתם לשימוש בטכנולוגיות של נתוני-עתק לשם גיבוש כללי בררת-מחדל, אבל מבקשת שפעולה כזו תיעשה באופן שיעלה בקנה אחד עם הפרטיות, והדבר אפשרי, כפי שהצעתי בחלק הקודם.

אני מבקש להצביע על מקרה-מבחן, חשוב כשלעצמו, שמראה כיצד הצעתם יכולה להתממש תוך שמירה על הפרטיות. זהו המקרה של זכרונות דיגיטליים. ככל שחיינו מקבלים ביטוי דיגיטלי, עוד ועוד מידע נוצר, נצבר ונשמר במחשבים ובחשבונות מקוונים שונים, כגון חשבונות דואר אלקטרוני ורשתות חברתיות. במותם של המשתמשים מתעוררות שאלות מורכבות – משפטיות, חברתיות, טכנולוגיות וכמובן רגשיות – בדבר הגישה למידע, הבעלות בו ועוד.<sup>69</sup> כאן אסתפק בהצבעה על האפשרויות שיש בגישה של עיצוב כללי בררת-מחדל לפי נתוני-עתק.

67 ראו לעיל ה"ש 30.

68 סטרכילביץ' ופורת, לעיל ה"ש 2, תת-פרק ג7.

69 להרחבה ראו מיכאל בירנהק וטל מורס זיכרונות דיגיטליים: גורלם של תוכן ומידע אישיים אחרי המוות (איגוד האינטרנט הישראלי, 2018) - [www.isoc.org.il/files/docs/digital-memories-for-comments-04-2018.pdf](http://www.isoc.org.il/files/docs/digital-memories-for-comments-04-2018.pdf)

הדיון הוא במידע אישי, ולא במידע שהוא עצמו קניין (כגון מטבע דיגיטלי או צילום שמוגן בזכות יוצרים) או במידע על קניין (כגון מידע על חשבון בנק מקוון). משום כך המסגרת המתאימה אינה של דיני הקניין והירושה, ויש חסר מסוים בדין המצוי. דיני הפרטיות אינם מתאימים במלואם להסדרת הגישה אל מידע דיגיטלי של אדם שמת, משום שההגנה על פרטיותם של המתים מוטלת בספק: לפי החוק הישראלי ניכר שאין מקום להגנה על פרטיותם של המתים במידע שנצבר על-אודותיהם בימי חייהם, ואילו בפסיקה יש הערות שונות, הגם שהן נעדרות בעיניי הצדקה וביסוס מספיקים.<sup>70</sup>

בחלל הזה פועלים תאגידי המידע, שהם כיום הגופים שקובעים את הכללים, ויש שוני בין ספקי השירותים השונים. חלקם, למשל, קובעים כי עם מות המשתמש יפקע חשבוננו (למשל, חשבון הדוא"ל של יאהו ואתרי היכרות מרכזיים). אחרים ממליצים לבני המשפחה לנסות לגשת לקבצים של המשתמשים המנוחים (למשל, שירותי האחסון בענן דרופבוקס). שניים מתאגידי המידע הגלובליים, גוגל ופייסבוק, מציעים כלים מקוונים למשתמשים שמאפשרים להם לתת הנחיות פרטניות בקשר לגורל החשבונות שלהם לאחר מותם. יש שם אפשרויות שונות, אולם מחקר אמפירי מצא כי ההיכרות של המשתמשים עם השירותים מצומצמת, והשימוש בפועל מצומצם עוד יותר.<sup>71</sup> מובן שיש חסמים שונים שמגבילים את השימוש בכלים אלה. במציאות כזו – שבה יש צורך לקבוע למי תהיה גישה למידע של משתמש מנוח ויש כלים טכנולוגיים שמציעים פתרונות אבל רק מעטים משתמשים בהם – ניתן לעצב כללי בררת-מחדל.

המדינה הייתה יכולה לחוקק כלל בררת-מחדל שיקבע כי כל עוד לא הורה המשתמש אחרת בחייו, לאיש לא תהיה גישה למידע על-אודותיו לאחר מותו. כלל בררת-מחדל הפוך שאפשר לחשוב עליו יקבע כי כל עוד לא הורה המשתמש אחרת בחייו, המידע שלו יהיה נגיש לאחרים לאחר מותו – למשל, ליורשיו או לבני משפחתו הגרעינית (ככל שאלה אינם יורשיו). היה אפשר לקבוע כללי בררת-מחדל מפורטים יותר, כך שלגבי סוגי מידע מסוימים יחול כלל הגישה ואילו לגבי סוגי מידע מסוימים יחול הכלל של העדר גישה. בארצות-הברית יש חוק-מודל שנוסח על-ידי ה-National Conference of Commissioners on Uniform State Laws והוצע למדינות השונות כנוסח אחיד.<sup>72</sup> בחוק-המודל יש מדרג שלפיו הנחיה שנתן משתמש באמצעות מערכת ניהול דיגיטלית (דוגמת אלה של גוגל ופייסבוק) תגבר על הנחיות אחרות; בהעדר הנחיה דיגיטלית יקבעו ההנחיות המופיעות בצוואה; ובהעדר הנחיות בצוואה יחולו כללי השימוש שקבע ספק השירות. חוק-המודל מציע כללי בררת-מחדל שמבחינים בין תוכן התקשורת המקוונת לבין נתוני התקשורת: התוכן יימסר לנציגו של המשתמש המנוח (כלומר, מנהל העיזבון) רק אם המשתמש הסכים בחייו למסירת החומר או אם בית-משפט יורה על כך; ואילו נתוני התקשורת – כלומר, רשומה של התקשורות,

70 לדיון בסוגיית פרטיותם של המתים ראו, למשל, ה"פ (שלום ת"א) 29490-05-12 עיזבון פלונית נ' פלדמן-קופלד (פורסם בנבו, 31.10.2012).

71 בירנהק ומורס, לעיל ה"ש 69. רק 18% מהמשתתפים במדגם השיבו כי הם מכירים את השירותים לניהול המידע לאחר המוות, ומתוכם רק כשליש השיבו שהם השתמשו בשירות.

72 Uniform Law Commission, Fiduciary Access to Digital Assets Act (2015).

הכוללת, לדוגמה, את הנמענים של הודעות הדוא"ל – יועברו לידי נציגו של המשתמש אלא אם כן התנגד לכך המשתמש בחייו.<sup>73</sup>

מחקר שנערך על בסיס מדגם מייצג של משתמשי מרשתת בישראל מצא כי למשתמשים ישראלים יש העדפות שונות: בקשר לרשתות חברתיות, למשל, 36% אינם מעוניינים שתהיה למישהו גישה לחשבונותיהם לאחר מותם, 45% מעוניינים שתהיה גישה כזו לכל התכנים, ו-19% מעוניינים לאפשר גישה רק לחלק מהתכנים.<sup>74</sup> משמעות הממצא היא שיש שונות גבוהה בהעדפות של הציבור הישראלי. בישראל אין לפי שעה הסדרה של הנושא. לפיכך, אם המדינה תקבע כלל בררת-מחדל של מתן גישה גורפת או לחלופין כלל בררת-מחדל של הגבלת גישה גורפת, או אפילו כלל בררת-מחדל מפורט יותר, בהכרח יסוכלו הרצון והציפיות של קבוצות גדולות של משתמשים בקשר לגורל המידע האישי שלהם לאחר מותם. ייתכן שזו בעיה זמנית, ושבחלוף הזמן ילמדו המשתמשים את האפשרויות, ומי שירצו ישנו את בררת-המחדל. אולם ניתן לשער שרק מעטים יעשו כן, בשל ה"דביקות" של כללי בררת-מחדל בכלל,<sup>75</sup> ובהקשר הזה גם בשל הרתיעה מעיסוק בסוגיית המוות.

לכן נראה שבמקרה הזה הפתרון של כללי בררת-מחדל מותאמים אישית עשוי להתאים. אם נצליח להתאים לכל משתמש את בררת-המחדל שמתאימה לה, לא יהיה צורך בכלל גורף שיחמיץ ויסכל ציפיות של קבוצות גדולות של משתמשים. הכלל המותאם אישית לא ייקבע על-ידי המדינה, אלא על-ידי ספקי השירות.

חשוב, למשל, על פייסבוק: יש לה קשר ישיר עם המשתמשים בשירותיה, ולכן יש לה אפשרות לבקש הסכמה מדעת של המשתמשים, ולאפשר להם לנהל את העדפות הפרטיות שלהם. פייסבוק עושה כן כל העת: היא אוספת מידע על המשתמשים ועל פעילותם, ומשתמשת בו כדי ללמוד את דפוסי ההתנהגות הכלליים והאישיים שלהם לצרכיה, שהם בעיקר התאמת פרסום למשתמשים. כידוע, יש פה קשיים רבים, אבל לצורך המחשת הפוטנציאל של גישתם של סטרכילביץ' ופורת, נניח שפייסבוק מצייתת להוראות הדין בקשר לאיסוף מידע ולעיבודו. לפייסבוק כבר יש מידע אישי רב על המשתמשים, ועל-כן אין צורך בפנייה לגורם שלטוני ואין צורך להצליב מידע ממקורות אחרים. כך, אם ההודעה וההסכמה של המשתמשים לתנאי השימוש תקפה, לא מתעוררת בעיה של עקרון צמידות המטרה.

יתרה מזו, לפייסבוק כבר יש נקודת התחלה טובה: היא יודעת מי ממשתמשיה הפעיל את השירות שהיא מציעה לניהול מידע לאחר המוות. באמצעות טכנולוגיות של נתוני-עתק ניתן ללמוד על מאפייניהם של המשתמשים האלה. באופן דומה ניתן ללמוד על מאפייניהם של משתמשים שלא בחרו להשתמש בשירות. מתוך ההתנהגות של המשתמשים ניתן ללמוד עוד על העדפות הפרטיות שלהם. לצורך הדיון אניח כי חברת טכנולוגיה כפייסבוק תוכל לפתח אלגוריתם שידע לזהות את ההעדפות של המשתמשים בקשר לניהול המידע שלהם. כאמור,

73 ש' ס' 7-8. גישה זו מניחה שתוכן התקשורת רגיש יותר מאשר נתוני התקשורת. הנחה זו קורסת בסביבה הדיגיטלית, שבה לעיתים נתוני השיחה מעידים על תוכנה – למשל, התקשורת לקליניקה להפלות או לרופא מומחה, שיחה של מקור לעיתונאי ועוד. להערות בעניין זה בהקשר הישראלי ראו עניין האגודה לזכויות האזרח בישראל, לעיל ה"ש 34, פס' 8 לפסק-דינה של הנשיאה (בדימ') ביניש.

74 בירנהק ומורס, לעיל ה"ש 69, בעמ' 76.

75 לעניין זה ראו סטרכילביץ' ופורת, לעיל ה"ש 2, ליד ה"ש 11.

פייסבוק יכולה בקלות לכלול בתנאי השימוש שלה התייחסות לשימוש זה במידע, ולאפשר למשתמשים לנהל את הבחירה הראשונה שלהם גם בהמשך, ובכלל זה לשנותה ולבטל את הסכמתם. לפיכך, על בסיס לימוד העדפותיהם, תוכל פייסבוק להתאים למשתמשים כללי בררת-מחדל שונים בקשר לגישה אל המידע שלהם לאחר מותם. כמובן, אפשר להרחיב כאן באפשרויות שונות, אולם לענייננו גישה כזו מאפשרת השאה של ההעדפות האמיתיות של המשתמשים (ולא להסתפק בהסקת מסקנות מתוך התנהגותם), וזאת ללא ערוב מאגרים, ללא עירוב המדינה, ותוך שמירה על כללי הפרטיות שפייסבוק ממילא מחויבת בהם. פתרון כזה מראה גם כיצד ניתן להשיג הן את היעילות שסטרכילביץ' ופורת מבקשים לקדם והן את שמירת הפרטיות.

## סיכום

בטכנולוגיות של נתוני-עתק יש הבטחה גדולה לפריצת מחסומים ישנים במחקר ובמדע ולקידום מודלים עסקיים יעילים יותר. נראה שהאפשרויות מרקיעות-שחקים. אולם ראוי לנקוט זהירות. לטכנולוגיות עצמן יש חסרונות שחשוב להכיר, דוגמת ההנחה בדבר האובייקטיביות של המידע המעובד. כאן התמקדתי בהשפעה אחת של טכנולוגיות של נתוני-עתק – ההשפעה על הפרטיות. סטרכילביץ' ופורת מניחים תפיסה רזה של פרטיות, וממהרים לוותר על הפרטיות לטובת מה שהם סבורים כי הוא יעיל ומועיל יותר. הסברתי מדוע תפיסה כזו מחמיצה את הבנת הפרטיות כנגזרת של ערך-היסוד של כבוד האדם. בתפיסת הפרטיות כשליטה, שנגזרת מהעיקרון של כבוד האדם, יש הבנה רחבה בהרבה. הבנה זו מקפידה על ההקשר – שלטוני או צרכני – ומתעקשת על כך שהגנת הפרטיות אינה פעולה חד-פעמית שמתמזה בעת מסירת המידע, אלא פעולה שנמשכת לכל אורך מחזור החיים של המידע. לפני שאנו אצים לאזן את היעילות מול הפרטיות, חשוב להבין את מהותה של הפרטיות, והאיזון צריך להיות בהתאם. סל הכלים המשפטי מאפשר פעולות רבות של עיבודי מידע, לרבות בטכנולוגיות של נתוני-עתק, תוך שמירה על הפרטיות. יש כאן אתגר לברר כיצד בדיוק לעשות זאת, והפרטים של כל מערכת טכנולוגית-חברתית הם נתונים מרכזיים במסגרת בירור זה. פעולה כזו מחייבת מאמץ, ויש לה עלויות, אולם זהו מחירה של זכות-יסוד.

ההתאמה האישית שסטרכילביץ' ופורת מבקשים לקדם היא התאמה שנעשית על-ידי נותן שירותים ועל-ידי המדינה בקשר לצרכנים ולאזרחים. הצרכן נהפך אצלם מסובייקט לאובייקט.<sup>76</sup> נקודת המוצא של הפרטיות כשליטה הפוכה: יש להתחיל את הדיון במושאי המידע. הסובייקטים נשארים – וצריכים להישאר – אדוני (או גברות) המידע. כל צרכן וכל אזרחית הם שיחליטו אם למסור מידע, איך, למי ולאילו מטרות, ובכלל זה אם להתיר שימוש במידע הפרטי שלהם לצורך גיבוש דפוסים כלליים ולצורך סיווגם-הם לדפוסים שכבר אותרו. הדין האירופי והדין הישראלי מנסים לסייע במימוש שליטתו של מושא המידע במידע האישי על-אודותיו, גם אם הם ניצבים בפני אתגרים של ממש. כאשר אנו זוכרים שהאדם הוא

76 להמשגה דומה בהקשר של הפרטיות, אך לא בקשר לרעיון ההתאמה האישית של כללים משפטיים, ראו Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as an Object*, 52 STAN. L. REV. 1373 (2000).

שצריך לשלוט במידע, מתבהרת גם החובה שמוטלת על מי שאוספים את המידע ומעבדים אותו. מעבר לציות לעקרונות הגנת המידע, גורמים אלה חבים חובת אמון למושאי המידע,<sup>77</sup> וראוי שהם יבטיחו שקיפות, יתנהגו באחריות וישמרו על הפרטיות.

---

77 ג'ק בלקין מציע להתייחס לתאגידי מידע כאל נאמני מידע, ולהטיל עליהם חובות מתאימות. Jack M. Balkin, *Information* בשינויים המתחייבים, רעיון זה מתאים גם למקרה הנוכחי. ראו Jack M. Balkin, *Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).