

חוק המאגר הביומטרי: סיכונים והזדמנויות

עומר טנא*

בשנת 2009 אישרה הכנסת את חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009. על פי החוק, יונפקו לאזרחי ישראל תעודות זהות חכמות ודרכונים עם שבב אלקטרוני, הכוללים נתוני זיהוי ביומטריים שיישמרו במאגר מידע מרכזי. המאמר מסביר מהי מערכת ביומטרית ומהם הסיכונים והאתגרים שהיא מציבה לזכויות היסוד של האזרחים, ובעיקר הזכות לפרטיות. הוא סוקר את הוראות החוק במבט ביקורתי, המטיל ספק בנחיצות הקמתו של מאגר מידע ביומטרי לצורך קיום המטרות המוצהרות של החוק, ומתריע בפני הסכנות החמורות הנובעות ממאגר כזה. המאמר מפרט מדוע החוק יתקשה לעבור מעל המשוכה החוקתית שעשויים להציב בדרכו עותרים שונים; הן מבחינה פרוצדורלית, לנוכח חקיקתו כ"חוק על תנאי" המותנה באישורו של שר; והן מבחינה מהותית, מאחר שנחקק לתכלית לא ברורה תוך יישומו של אמצעי לא מידתי להשגתה. המאמר מפרט גם את המנגנונים הטכנולוגיים, הארגוניים והמשפטיים שהחוק מעמיד לצורך הגנה על פרטיות האזרחים ואבטחת המידע האישי שלהם. הטענה היא, כי חרף הבעייתיות של החוק בכללותו, קיימים בו כמה מנגנונים, המכונים כיום Privacy by Design, שראוי היה ליישם גם ביזמות חקיקה נוספות העלולות להשפיע על פרטיות המידע האישי של אזרחי ישראל.

א. מבוא. ב. מערכת ביומטרית מהי. ג. עיקרי החוק; 1. הגדרות; 2. נטילת אמצעי זיהוי; 3. המאגר הביומטרי; 4. הרשות; 5. העברות מידע. ד. הפגיעה בפרטיות; 1 זיהוי; 2. חפצון; 3 זחילת פונקציות; 4. סכנת אבטחה; מידע עודף; מעקב; עיקרי החוק. ה. המבחן החוקתי;

* סגן דקאן, בית הספר למשפטים ע"ש שטריקס, המסלול האקדמי המכללה למינהל. ברצוני להודות לפרופ' מיכאל בירנהק ולעו"ד רועי פלד על הערותיהם המועילות וכן לקרן המחקר הבית ספרית על סיועה לכתיבת מאמר זה. כמו כן, תודה לארנון הראל, מומחה למערכות מידע ביומטריות, על סיועו להבנת ההיבטים הטכנולוגיים של החוק. תודה מיוחדת להילה קנטרוביץ על סיוע מחקר מקיף ומעמיק.

1. פגיעה בחוק או על פי חוק; 2. תכלית ראויה "הקמת המאגר";
3. מידתיות: עלייתו ונפילתו של "המאגר המעומעם". 1. מנגנונים להבטחת הפרטיות: הזדמנויות; 1. מנגנונים טכנולוגיים; 2. מנגנונים ארגוניים; מנגנונים משפטיים. 2. לסיכום.

א. מבוא

ביום 7 בדצמבר 2009 אישרה הכנסת בקריאה שנייה ושלישית את חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009 (להלן: "החוק"). על פי החוק, יונפקו לאזרחי ישראל תעודות זהות חכמות ודרכונים בעלי שבב אלקטרוני שיחליפו בשנים הבאות את התעודות הנוכחיות. מדובר בתעודות איכותיות שיקשה לזייפן ולהעתיקן, והן יאפשרו אימות זהות מחזיקיהן באמצעות מידע ביומטרי הכולל תמונה של תווי הפנים ותמונות שתי טביעות של האצבעות המורות. המידע הביומטרי יישמר לא רק על גבי התעודות עצמן, אלא גם במאגר מידע מרכזי, שאליו תוענק גישה מוגבלת לעובדי משרד הפנים, אבל גם למשטרה ולשירותי הביטחון, וזאת למטרות של ביטחון לאומי ואכיפת חוק. החוק התקבל בכנסת לאחר הליך חקיקה מזורז, שבמסגרתו התכנסה עשר פעמים בתוך פחות מחודש ועדת כנסת מיוחדת המשותפת לוועדת המדע והטכנולוגיה ולוועדת הפנים בראשותו של ח"כ מאיר שטרית (להלן: "הוועדה המשותפת").¹ ח"כ שטרית כיהן בכנסת הקודמת כשר הפנים והיה מי שיזם בעצמו את הצעת החוק.² התקנות³ שהותקנו לצורך יישום החוק והצו⁴ שהכניסו לתוקף (באופן חלקי) אושרו בכנסת ביום 2 יוני 2011.⁵ החוק והמאגר הביומטרי המוקם מכוחו יוצרים סכנות

- 1 אהוד קינן וניב ליליאן "ועדת החוק הביומטרי: איפה חברי הוועדה?" Ynet 21.7.2009 www.ynet.co.il/articles/0,7340,L-3749497,00.html (נבדק לאחרונה ב-5.12.2012); שאול אמסטרדמסקי "שר הפנים מקדם את פרויקט הדרכון הביומטרי" כלכליסט 18.6.2008 www.calcalist.co.il/local/articles/0,7340,L-3082424,00.html (נבדק לאחרונה ב-5.12.2012). לתיאור מפורט של הליכי החקיקה שהוביל השר (לאחר מכן ח"כ) מאיר שטרית ראו עומר שרביט "תמונה מטרידה של הכנסת" ארץ אחרת 64 (2012).
- 2 תקנות הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי במסמכי זיהוי ובמאגר מידע, התשע"א-2011 (להלן: "התקנות").
- 3 צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי במסמכי זיהוי ובמאגר מידע (תקופת מבחן), התשע"א-2011 (להלן: "הצו").
- 4 פרוטוקול ישיבה מס' 1 של ישיבת הוועדה המשותפת של ועדת המדע והטכנולוגיה, ועדת החוקה, חוק ומשפט וועדת הפנים והגנת הסביבה לפי חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, הכנסת ה-18 (2.6.2011). יצוין כי

כבודות לזכות החוקתית של אזרחי ישראל לפרטיות, ועולה חשש לשימושים שניוניים במידע הביומטרי שלא למטרה המוצהרת שלשמה הוקם המאגר. בנוסף, נוצר תמריץ עז לארגוני פשיעה וטרור ולרשויות ביטחון של מדינות אחרות לנסות לפרוץ למאגר ולדלות מתוכו מידע שלנוכח אופיו לעולם לא יהיה אפשר להחליפו. זאת ועוד: הוראות התחולה של החוק יצרו מצב ייחודי שבמסגרתו החוק אינו בתוקף, למעט לגבי אזרחים הבוחרים להתנדב להנפקת התעודות הביומטריות. מנגנון כזה, המותיר שיקול דעת חקיקתי בידיו של שר בממשלה (בייחוד כשמדובר בשר שממונה על המנגנון הביורוקרטי והתקציבים המתחייבים על פי החוק), חדש בזירת החקיקה הישראלית ומשקף מעין "מיקור חוץ" של סמכויות הכנסת. יצוין כי ביום 23 יולי 2012 דחה בג"ץ את עתירתם של פרופ' קרין נהון ואחרים נגד חוקתיותו של החוק, בהתבסס על הנימוק כי העתירה מוקדמת לנוכח אי-כניסתו של החוק לתוקף עד תום תקופת ניסיון בת שנתיים.⁶ השופטים ציינו כי "בתום תקופת המבחן ממילא על פי החוק יש לבחון את נחיצות קיומו של המאגר".

במאמר זה אסביר מהי מערכת ביומטרית ומהם הסיכונים והאתגרים שהיא מציבה לזכויות היסוד של האזרחים, ובעיקר הזכות לפרטיות. אסקור את הוראות החוק במבט ביקורתי, המטיל ספק בנחיצות הקמתו של מאגר מידע ביומטרי לצורך קיום המטרות המוצהרות של החוק, ואתריע בפני הסכנות החמורות הנובעות ממאגר כזה. אפרט מדוע החוק יתקשה לעבור מעל המשוכה החוקתית שעשויים להציב בדרכו עותרים שונים; הן מבחינה פרוצדורלית, לנוכח חקיקתו כ"חוק על תנאי" במותנה באישורו של שר; והן מבחינה מהותית, מאחר שנחקק לתכלית לא ברורה ויישם אמצעי לא מידתי להשגתה. לבסוף, אפרט את המנגנונים הטכנולוגיים, הארגוניים והמשפטיים שהחוק מעמיד לצורך הגנה על פרטיות האזרחים ואבטחת המידע האישי שלהם.⁷ אטען כי חרף הבעייתיות בחוק

התקנות נדונו בוועדה המשותפת שלושה ימים בלבד לאחר פרסומן להערות הציבור. ראו בעניין זה את דבריו של יהושע שופמן (יו"ר המועצה להגנת הפרטיות) בדיון בוועדה בכנסת: "התקנות לא פורסמו לעיון הציבור קודם לכן, לכן לא היתה הזדמנות לגופים, למשל כמו המועצה להגנת הפרטיות וגופים אחרים, להעיר הערות ולכן אנחנו נאלצים להעיר אותן עכשיו. חבל, הייתי שמח אילו לפני האישור הסופי תינתן הזדמנות להעביר הערות בכתב, יותר מפורטות". שם, בעמ' 6-7. שופמן ממשיך ואומר: "אם דיברנו בתחילת הישיבה על כך שקיבלנו את הטיוטה לפני שלושה ימים, כאן את הסעיף שאולי הוא הכי משמעותי אנחנו שמענו רק היום, אפילו לא ראינו, אז אני לא יכול להתייחס לנוסח שהוקרא, שאני באמת לא ראיתי. וחבל". שם, בעמ' 131-132.

6 בג"ץ 1516/12 נהון נ' הכנסת (פורסם בנבו, 23.7.2012).

7 הציניקנים יטענו כי ההתייחסות הרבה בחוק לפרטיות (המילה פרטיות מוזכרת בחוק 24 פעמים), נובעת מניסיונה של הממשלה להכניס מראית עין של מידתיות לחוק שעיקרו פגיעה בזכות חוקתית, וזאת במטרה "לחסנו" מפני ביקורת שיפוטית בבג"ץ.

בכללותו, קיימים בו כמה מנגנונים, המכונים כיום Privacy by Design, שראוי היה ליישם גם ביזמות חקיקה נוספות העלולות להשפיע על פרטיות המידע האישי של האזרחים, כגון הרשומה הרפואית הלאומית⁸ ומאגר המידע של הרשות למדידה והערכה בחינוך (ראמ"ה)⁹.

ב. מערכת ביומטרית מהי

השימוש באמצעים ביומטריים, כלומר במאפיינים פיזיים או התנהגותיים ייחודיים של אדם, לצורך זיהוי או אימות זהות אינו חדש. טביעות אצבע וחתומות דיו משמשות לצרכים אלה זה מאות בשנים.¹⁰ עם זאת, ההתפתחויות הטכנולוגיות שחלו בעשורים האחרונים הביאו לפריסה רחבה של מערכות ביומטריות הן במגזר הציבורי והן במגזר הפרטי.¹¹ במאמר זה אעסוק ביישומים ביומטריים במגזר הציבורי בלבד. מערכות אלה רוכשות דגימות ביומטריות מבני אדם, מפיקות מהן נתונים ביומטריים, משוות בין הנתונים לבין נתונים הנאגרים במאגר, ומחליטות אם הושג זיהוי או אימות זהות.¹² בין היתר, מערכות אלה משתמשות במאפיינים פיזיים כגון טביעת אצבע, גאומטריית יד, תווי פנים, סריקת קשתית

- 8 יובל יועז "בעקבות האח הגדול: האגודה לזכויות האזרח מודאגת מצמיחה בכמות הפגיעות בפרטיותו של האדם הקטן" *The Marker* 6.12.2007 technation.themarker.com/internet-6.12.2007 technologies/1.1755508 (נבדק לאחרונה ב-5.12.2012).
- 9 הצעת חוק ראמ"ה: מדידה, הערכה ואיסוף מידע, פורטל השירותים והמידע הממשלתי, www.shituf.gov.il/discussion/184 (נבדק לאחרונה ב-5.12.2012). ראו גם גלית בינט "ללא ידיעתנו וללא הסכמתנו" *ארץ אחרת* 64 (2012).
- 10 LAWRENCE O'GORMAN, FINGERPRINT VERIFICATION IN BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY (Anil K. Jain, Ruud Bolle & Sharath Pankanti eds., 1999).
- 11 בשנים האחרונות נפוצה פריסה רחבה של מערכות ביומטריות במגזר הפרטי, כולל במקומות עבודה. ראו למשל שי ניב "צומת ספרים לא תפטר עובדת שסירבה למסור טביעת אצבע" *גלובס* 15.7.2010 bit.ly/g68Aqc; (נבדק לאחרונה 5.12.2012) או בחברות המספקות שירות לקוחות (ראו למשל יישום ביומטרית קול לצורך זיהוי לקוחות בבנקים: Penny Crossman, *Citi: Testing Voice Biometrics to Improve Security, Bank Systems & Technology* (15 October 2010), available at www.banktech.com/risk-management/227900022 (נבדק לאחרונה ב-5.12.2012); ראו בהקשר זה גם Lisa J. McGuire, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441 (2000).
- 12 על פעולתה של מערכת ביומטרית ראו Anil K. Jain & Arun Ross, *Introduction to Biometrics*, in *HANDBOOK OF BIOMETRICS* 3-6 (Anil K. Jain, Patrick J. Flynn & Arun Ross eds., Springer, USA, 2008) (להלן: *HANDBOOK OF BIOMETRICS*).

או רשתית העין, מערכת הוורידים על היד, או אף ריחות גוף; וכן במאפיינים התנהגותיים כגון קול, צורת החתימה, אופן ההקלדה על מחשב או צורת הליכה.¹³ מאפיינים ביומטריים נחשבים בעיני מדענים מתאימים למערכות זיהוי אם הם עומדים באמות מידה אחדות ובהן אוניברסליות (האם לכל בני האדם מאפיין כזה), ייחודיות (עד כמה ייחודי המאפיין לכל אדם באופן שיאפשר את זיהויו), קביעות (האם המאפיין משתנה לאורך חיי האדם), קלות איסוף (עד כמה המאפיין קל לדגימה ולמדידה), איכות ביצוע (מה מידת הדיוק ומהירות הזיהוי של המאפיין על ידי המערכת), הכרה (עד כמה בני אדם יסכימו לקבל את השימוש במאפיין למטרות זיהוי) ואי-עקיפה (עד כמה קשה לעקוף את המערכת או להביסה).¹⁴ מאפיינים ביומטריים שונים זוכים לציונים משתנים על פי אמות מידה אלה; טביעת אצבע או סריקת קשתית, למשל, נחשבות לביומטריות "חזקות" יותר מחתימה או צורת הליכה. כמו כן, פריסה רחבה של מערכת ביומטרית (למשל בשדה תעופה) מחייבת מהירות ויעילות של תהליך עיבוד הנתונים ולכן תביא להעדפה של מאפיין ביומטרי מסוים על פני מאפיין אחר.

קיימת הבחנה חשובה בין מערכות ביומטריות המשמשות לזיהוי (identification) לבין כאלה המשמשות לצורך אימות זהות (authentication or verification). מערכת זיהוי מבצעת השוואה בין נתון ביומטרי אחד לבין נתונים רבים (אחד מול רבים) כדי לזהות אדם שאינו טוען לזהות כלשהי.¹⁵ טלו למשל את הזיהוי שמעבדה לזיהוי פלילי מנסה לייצר באמצעות טביעת אצבע שנמצאה בזירת פשע. החוקרים משווים באמצעות המערכת הטכנולוגית את הנתון הביומטרי אל מול מאגר הנתונים שברשותם ומפיקים תוצאה שיכולה להיות "זיהוי" או "היעדר זיהוי".¹⁶ תוצאה של "זיהוי" מחייבת עמידה ברף דיוק סטטיסטי מסוים.¹⁷ כמו כן, מערכות הזיהוי נועדו למנוע שימוש בריבוי זהויות על ידי אדם אחד. כך, למשל, המערכת תתריע מפני ניסיון של אדם להנפיק תעודת זהות כפולה: היא תאתר את נתוניו הביומטריים במערכת עם התייצבותו לצורך ההנפקה השנייה המיועדת למטרה לא חוקית.

13 ש.ם.

14 ש.ם, בעמ' 15–19. אמות מידה אלה מכונות לפעמים "שבעה יסודות הביומטריה". ראו גם Working Party on Information Security and Privacy *Biometric-Based Technologies*, ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD) (Paris, 2004).

15 לעיל ה"ש 12, בעמ' 9–14.

16 דוגמה נוספת היא ניסיון לזהות גופה בזירת פשע, פיגוע או אסון טבע. לפני כשנתיים פסק בית הדין האירופי לזכויות אדם כי מאגר מידע שהחזיקה משטרת בריטניה ובו דגימות דנ"א של עצורים, כולל כאלה שזוכו במשפטם, מפר את זכות היסוד לפרטיות המעוגנת באמנה האירופית לזכויות אדם (European Convention on Human Rights); S and Marper v. The United Kingdom, 30562/04 [2008] ECHR 1581 (4 December 2008).

17 ש.ם.

מערכת אימות זהות, לעומת זאת, משווה בין נתונים ביומטריים שנדגמו במועד הבדיקה אל מול תבנית דיגיטלית (template) הקיימת במאגר או על גבי שבב או תעודה חכמה, במה שמכונה זיהוי של אחד מול אחד.¹⁸ מערכת אימות זהות מונעת שימוש בזהות מסוימת על ידי יותר מבן אדם אחד. כך, למשל, אם ראובן מנסה להשתמש בכרטיס הגישה האישי של חברו לעבודה שמעון, הוא ינסה להזדהות בפני המערכת כשמעון, אלא שזו תספק לטענתו תשובה "שלילית" ותחסום בפניו את הגישה לאגף או למערכת המוגנים.

פעולתה של מערכת ביומטרית מתחלקת לשלבים אחדים, ובהם: ההרכשה הראשונית, האגירה, רכישת הדוגמה וההתאמה.¹⁹ בשלב ההרכשה הראשונית נאסף לראשונה מידע ביומטרי מאדם; מהמידע מפיקה המערכת תבנית דיגיטלית, המתמצתת את מאפייניו הביומטריים הייחודיים של אותו אדם באמצעות נוסחה מתמטית ייעודית לתבנית, ושומרת את התבנית במאגר תוך קישור אל זהותו; בפעם הבאה שאותו אדם יציג את עצמו בפני המערכת, תשווה המערכת דגימה ביומטרית שתילקח ממנו באותו מועד אל מול התבנית השמורה במאגר ותיישם אלגוריתם לחיפוש מידת ההתאמה. ההחלטה של המערכת על קיום או אי-קיום התאמה מבוססת על רף סטטיסטי. זאת, מאחר שלעולם אין זהות של 100% בין שתי דגימות ביומטריות הנלקחות מאדם אחד בזמנים שונים: הבדלים דקים קיימים הן בתנאים של נטילת הדגימה (למשל, הזווית שבה נשענת כף היד על הסורק; או התאורה בחדר) והן במאפיינים הביומטריים של אותו אדם (תווי הפנים, למשל, משתנים עם הזמן). המשמעות היא, כי כל מערכת ביומטרית מציבה בעיות של שגיאות קבלה (false accept) ושגיאות דחייה (false reject), שאת שכיחותן ניתן לווסת באמצעות קביעת הגובה של רף ההתאמה.²⁰ קביעתו של רף התאמה סטטיסטי גבוה הופכת את המערכת למאובטחת יותר, אך מגדילה את הסיכון לחסימת גישה בפני מי שאין הצדקה עניינית לחסמו; אולם קביעתו של רף התאמה סטטיסטי נמוך הופכת את המערכת לחשופה ליותר טעויות מסוג של שגיאות קבלה, המאפשרת מעבר למי שאינו מוסמך לעבור. לכן אחד השיקולים בקביעת רף ההתאמה הסטטיסטי נוגע למידת האבטחה הנדרשת בהתאם לסוג הפעילות. כך, למשל, יישומה של מערכת ביומטרית שמטרתה קידום ביטחון תעופה מחייב קביעה של רף התאמה סטטיסטי גבוה, שכן המערכת אינה יכולה לסבול שגיאות קבלה; לעומת זאת, מערכת המוצבת בכניסה לספרייה של מוסד אקדמי יכולה להיות מכויילת לרף התאמה סטטיסטי נמוך יותר.

18 לעיל ה"ש 12, בעמ' 10–11.

19 Jain & Ross, לעיל ה"ש 12.

20 שם, בעמ' 6–12.

חוק המאגר הביומטרי: סיכונים והזדמנויות

כאמור, התבנית הדיגיטלית של המידע הביומטרי יכולה להישמר בנקודת הקצה, למשל על גבי שבב המוטבע בכרטיס חכם,²¹ או במאגר מידע מרכזי. ככלל, מערכת זיהוי מחייבת אגירה של המידע במאגר מרכזי, כדי לאפשר התאמה של דגימה ביומטרית אל מול כלל הנתונים במאגר (אחד מול רבים), ואילו מערכת אימות זהות מאפשרת אגירה מבוזרת, למשל על גבי כרטיס חכם המוצג בעת הדרישה לאמת את זהותו של נושא הכרטיס (אחד מול אחד).²² כפי שיפורט להלן, מאגר מרכזי של נתונים ביומטריים מעורר בעיות קשות של פרטיות, שלרוב אינן מתעוררות במערכות מבוזרות; ובכלל זה סכנות אבטחה, "זחילת פונקציות" (function creep), מעקב (surveillance) וכריית מידע (data mining).²³

ג. עיקרי החוק

לאחר שעמדנו על מאפייניה של מערכת ביומטרית, נפרט את יסודותיה של המערכת המוקמת מכוח החוק. כפי שנראה, מדובר במערכת ביומטרית האוגרת נתונים גולמיים במאגר מידע מרכזי ומאפשרת הן תהליך של אימות זהות (אחד מול אחד) והן תהליך של זיהוי (אחד מול רבים).

1. הגדרות

סעיף 2 לחוק עוסק בהגדרת מונחים בסיסיים, החשובים להבנת אופייה של המערכת הביומטרית. המונח "אמצעי זיהוי ביומטריים" מוגדר בחוק כ"תמונת תווי הפנים ותמונות שתי טביעות האצבעות המוררות של אדם, שניתן להפיק מהן נתוני זיהוי ביומטריים". אלה

21 כרטיס חכם הוא כרטיס פלסטי שבו מוטבע מנגנון זיכרון ממוחשב, שיכול לאגור כמויות גדולות של מידע, ולעתים אף מעבד זעיר. זאת, תוך שמירה על רמת אבטחה גבוהה. הכרטיס יכול לשמש לאימות זהות, לזיהוי, לאחסון מידע או לעיבודו. היתרון העיקרי של מערכת זיהוי המבוססת על כרטיסים חכמים ללא מאגר מרכזי, הוא כי המידע מבוזר ואינו ניתן לפריצה במקום מסוים.

22 מערכת אימות זהות באה להשיב על השאלה "האם זה מי שהוא טוען שהוא"; היא מאפשרת לאמת לצורך כך את הטענה שמציג אדם ("אני עומר טנא") אל מול מידע המוטבע על גבי הכרטיס עצמו. זאת, בניגוד למערכת זיהוי, הבאה להשיב על השאלה "מי זה?" ומחייבת השוואת הפרטים של אדם אל מול אוסף פרטים המוחזק במאגר. Nalini Ratha, Jonathan Connell & Ruud Bolle, *Enhancing Security and Privacy in Biometrics-Based Authentication Systems*, 40 IBM SYSTEMS JOURNAL 614 (2001)

23 לדיון מקיף בזכות לפרטיות על היבטיה השונים, כולל פרטיות במידע אישי, הן כלפי השלטון והן כלפי המגזר הפרטי, ראו ספרו מאיר העיניים של מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** (2010).

הם אפוא הנתונים הביומטריים שיידגמו על ידי המערכת ויישמרו במאגר. המונח "נתוני זיהוי ביומטריים" מוגדר כ"נתונים ביומטריים שהופקו מאמצעי זיהוי ביומטריים, וניתן לעשות בהם שימוש לצורך זיהוי או אימות זהותו של אדם באופן ממוחשב או ממוחשב בחלקו". אלו הן התבניות הדיגיטליות המתמצות את אמצעי הזיהוי לכלל נוסחה מתמטית לצורך זיהוי או אימות זהות של אדם אל מול המאגר.

2. נטילת אמצעי זיהוי

פרק ג' לחוק, כולל סעיפים 3 עד 9, עוסק בנטילת אמצעי הזיהוי הביומטריים והפקת נתוני הזיהוי באמצעותם. סעיף 3(ד) לחוק קובע כי מסירת אמצעי זיהוי ביומטריים לצורך הנפקת מסמך זיהוי היא חובה. לצורך אבטחת המידע הנאסף בשלב זה, נקבע בסעיף 3(ב) לחוק כי אמצעי הזיהוי ונתוני הזיהוי יוצפנו באופן אוטומטי מיד לאחר הנטילה וההפקה, כך שלא יהיו ניתנים לפענוח, קריאה או שימוש על ידי מי שאינו מוסמך לכך. המידע הביומטרי הנאסף מן האזרחים מועבר למאגר המידע הביומטרי ול"מרכז הנפקה" המוקם על פי סעיף 4 לחוק לשם הנפקת התעודות המזהות. סעיף 6 לחוק מסמיך עובדי ציבור שונים, ובכלל זה שוטרים ועובדי משרד הפנים, ליטול מאדם דגימה ביומטרית לצורך אימות זהותו; מהדגימה מופקת תבנית, וזאת תשווה לנתונים הביומטריים הכלולים במסמך הזיהוי של אותו אדם (אחד מול אחד). כך, למשל, יוכל שוטר תנועה שעוצר רכב לדרוש מבעל הרכב להזדהות באמצעות הצגת תעודת זהות והשוואת טביעת האצבע שלו לזאת המקושרת אל התעודה. סעיף 6(ה) לחוק קובע, כי "אדם חייב לאפשר למי שמוסמך לכך [...] ליטול ממנו אמצעי זיהוי ביומטריים לפי סעיף זה; סירב אדם לנטילת אמצעי זיהוי ביומטריים כאמור, יראו אותו כמי שלא הזדהה". אם תהליך אימות זהות של אדם נכשל, או אם אדם כלל אינו נושא עמו תעודה, מוסמך שוטר ליטול ממנו דגימה ביומטרית, להפיק ממנה תבנית ולהעבירה לרשות לניהול המאגר הביומטרי לצורך זיהוי של אותו אדם (אחד מול רבים).

3. המאגר הביומטרי

פרק ד' לחוק, כולל סעיפים 10 ו-11, עוסק בהקמת המאגר הביומטרי וניהולו. מאגר המידע הביומטרי מוקם במשרד הפנים, והוא אוגר לא רק את נתוני הזיהוי הביומטרי, אלא אף את אמצעי הזיהוי הביומטרי, כלומר את המידע הביומטרי הגולמי של האזרחים. סעיף 10(א) לחוק קובע, כי "המאגר הביומטרי יישמר באופן מוצפן, בנפרד מכל מידע אחר ולא יכלול פרטי רישום של התושב כמשמעותם בחוק המרשם [חוק מרשם האוכלוסין, התשכ"ה – 1965] או כל פרט מזהה אחר". הפרדת המאגר הביומטרי משאר מערכות המידע של משרד הפנים, והמדינה בכלל, נועד ליצור "חומה סינית" בין המידע הביומטרי לבין מידע אחר ולמנוע שימוש במידע הביומטרי כמפתח ליצירת פרופיל מקיף.

4. הרשות

פרק ד' לחוק מוסיף ומקים את הרשות לניהול המאגר הביומטרי במשרד הפנים, שתהא אחראית "לניהול המאגר הביומטרי ובכלל זה להפקת נתוני זיהוי ביומטריים מאמצעי זיהוי ביומטריים שהועברו אליה, לעיבודם, להעברת מידע מהמאגר הביומטרי וכן לאבטחת המאגר, לאחזקתו ולטיפול השוטף בו".²⁴ הרשות תוקם על ידי שר הפנים אשר ימנה באישור הממשלה גם את ראש הרשות. ראש הרשות וכל עובדיה יהיו עובדי מדינה שעברו בדיקות התאמה ביטחוניות, ולא ימלאו כל תפקיד אחר מלבד תפקידם ברשות.

5. העברות מידע

פרק ה' לחוק, הכולל את סעיפים 12 עד 22, עוסק בהעברת מידע מהמאגר הביומטרי וגישה אליו. סעיף 12 לחוק מוציא את העברות המידע מהמאגר מתחום התחולה של פרק ד' לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות"), המתיר בתנאים מסוימים להעביר מידע אישי בין גופים ציבוריים. סעיף 12 לחוק קובע כי "העברת מידע מהמאגר הביומטרי וגישה אליו מותרות בהתאם להוראות לפי חוק זה בלבד". סעיף 17 לחוק מאפשר לבית משפט שלום להתיר העברת מידע מהמאגר הביומטרי למשטרה לצורך חקירת עברות או לצורך אימות או בירור זהותו של אדם, לרבות גופה, שזהותו אינה ידועה או מוטלת בספק, ולצורך איתור נעדרים או שבויים. סעיף 18 לחוק מתיר העברת מידע מהמאגר למשטרה, אף בלא צו של שופט, אם הדבר דרוש לצורך חקירת חשד בדבר גניבת זהות או זיוף פרטים בתעודה מקורית. ההוראה המגבילה העברות מידע לרשויות הביטחון מעורפלת הרבה יותר, ומאפשרת העברות לרשויות הביטחון "לצורך מימוש ייעודן ותפקידיהן [...] על פי הכללים שייקבעו".²⁵

ד. הפגיעה בפרטיות

מערכות ביומטריות מעוררות בעיות אתיות שונות. חשוב להבין כי בעיות אלה אינן נובעות מהטכנולוגיה הביומטרית עצמה, אלא מאופן יישומה והשימושים שנעשים במידע המיוצר באמצעותה.²⁶ חלק מהבעיות האתיות הקשורות למערכות ביומטריות מתעורר לנוכח שילובן במערכות טכנולוגיות מתקדמות נוספות; כגון מעקב באמצעות מצלמות טלוויזיה

24 ס' 11 לחוק.

25 שם, ס' 21.

26 כפי שיפורט להלן, מערכות ביומטריות יכולות לשמש גם כאמצעי להגנה על פרטיות ואבטחת מידע. ראו להלן ה"ש 45-46 והטקסט הנלווה.

במעגל סגור (CCTV); תיוג אלקטרוני באמצעות גלי רדיו (RFID); וכמובן העברות מידע באינטרנט.²⁷ מטרות המדיניות, החשובות כשלעצמן, כגון ביטחון לאומי ואכיפת חוק, יעילות כלכלית או בריאות הציבור מקודמות באמצעות היישום של מערכות ביומטריות. החשש הוא כי קידום המטרות יפגע באופן לא מידתי בעקרונות יסוד כגון הזכות לפרטיות, הזכות לאוטונומיה אישית וזכות האדם על גופו. במאמר זה אתמקד בסכנות הנובעות מיישומן של מערכות ביומטריות לזכות האדם הבסיסית לפרטיות.²⁸ הזכות לפרטיות היא מזכויות האדם הבסיסיות בישראל ובמדינות המערב.²⁹ היא מעצבת את יחסי הכוחות בין האזרח לשלטון, בין היחיד לגופים עסקיים גדולים, ובין אדם

- 27 ראו למשל רשות למשפט, טכנולוגיה ומידע מצלמות מעקב: הדין החל ואופן השימוש www.justice.gov.il/NR/rdonlyres/AFA7C4A5-8481-4FC1-A939-B844F0170111 (2010) Article 29 Data Protection Working Party; (5.12.2012) (נבדק לאחרונה ב־5.12.2012) /23249/cctv.pdf Opinion 3/2012 on developments in biometric technologies, WP 193, 16–18 (2012) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (6.12.2012) (נבדק לאחרונה ב־6.12.2012)
- 28 הזכות לפרטיות קשה להגדרה מדויקת. לניסיונות שונים להגדירה ראו Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Alan F. Westin, *Privacy and Freedom*, WASH. & LEE L. REV. (1967); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); Ken Gormley, *One Hundred Years of Privacy*, 1992 Wis. L. REV. 1335 (1992). הניסיון להגדיר את הזכות לפרטיות חורג ממסגרתו של מאמר זה. לדין בפרטיות בהקשר הביומטרי ראו Article 29 Data Protection Working Party, Working Document on Biometrics, 12168/02/EN, WP 80, 1 August 2003, available at ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf. (נבדק לאחרונה ב־5.12.2012).
- 29 בישראל: ס' 7 לחוק-יסוד: כבוד האדם וחירותו; רע"א 4447/07 מור נ' ברק אי.טי.סי. החברה לשרותי בזק בינלאומיים בע"מ (פורסם בנבו, 25.3.2010); בג"ץ 6650/04 פלוני נ' בית הדין הרבני האזורי בנתניה (פורסם בנבו, 14.5.2006). באירופה: Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, 213 U.N.T.S. 221; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (נבדק לאחרונה ב־5.12.2012) (להלן: "דירקטיבת 95/46"). בארצות-הברית הזכות אינה מעוגנת במפורש בחוקה, אבל היא מוגנת בפסיקה, בין היתר כנגזרת של הוראות חוקתיות שונות, ראו למשל Griswold v. Connecticut, 381 U.S. 479 (1965). ראו גם Katz v. United States, 389 U.S. 347 (1967); וכמובן פסק הדין הידוע התולה את זכות האישה להפלות בזכות חוקתית לפרטיות: Roe v. Wade, 410 U.S. 113 (1973). להשוואת הגישה האמריקנית לגישה האירופית ראו James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

לחברו. היא מהווה תנאי מקדמי להתפתחותה של חברה חופשית ודמוקרטית: ללא פרטיות אין חופש ביטוי, חופש דת או חירות תנועה. לא בכדי נוהגים שלטונות טוטליטריים רבים להתמקד בפגיעה בזכותם של אזרחיהם לפרטיות, באמצעות הפעלתן של משטרות חשאיות, מעקבים, ציתותים והאזנות.³⁰ כפי שציין מישל פוקו בספרו "לפקח ולהעניש: הולדת בית-הסוהר", "למבט יש כוח ממשטר".³¹ אזרחים שחשים כי הם נמצאים תחת מעקב חוששים לנקוט עמדות מעוררות מחלוקת ונוטים לקונפורמיזם ולפאסיביות פוליטית. פגיעה בפרטיות היא פגיעה בכבוד האדם וחירותו.³²

בשנים האחרונות נמצאת הזכות לפרטיות במגננה. יש הטוענים, כי ירדה קרנה כערך חברתי.³³ דור חדש של טכנולוגיות מאיים עליה ובתהליך של סיפוח זוחל נוגס ממנה פלח ועוד פלח.³⁴ ניתוח התנהגותי באינטרנט מאפשר לדעת מה אנחנו מחפשים והיכן אנחנו גולשים;³⁵ הטלפון הסלולרי מדווח היכן אנחנו נמצאים;³⁶ יישומי פייסבוק או אייפון

30 ראו למשל הסרט הגרמני "חיים של אחרים" (Das Leben der Anderen) (גרמניה, 2006), המתעד את החיים תחת עינה הפקוחה ואוזנה הכרויה של המשטרה החשאית של מזרח גרמניה, השטאזי. ראו גם דוח ארגון Privacy International על מצב הפרטיות בסין: People's Republic of China 22.10.2012, available at www.privacyinternational.org/reports/china/i-legal-framework.

31 MICHEL FOUCAULT, DISCIPLINE & PUNISH THE BIRTH OF THE PRISON (Alan Sheridan trans., 1995).

32 Whitman, לעיל ה"ש 29; ראו גם עומר טנא "הזכות לפרטיות בעקבות חוק יסוד כבוד האדם: מהפך מושגי, חוקתי ורגולטורי" **קרית המשפט** ח 39 (תשס"ט).

33 Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, GUARDIAN, 11 January 2010, available at www.guardian.co.uk/technology/2010/jan/11/facebook-privacy (נבדק לאחרונה ב-5.12.2012). אבל ראו מחקרים אמפיריים המוכיחים כי הפרטיות חשובה מאוד גם לבני הדור הצעיר החולקים מידע אישי ברשתות חברתיות באינטרנט: Chris Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*, 14 April 2010, available at www.papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864; Mary Madden & Aaron Smith, *Reputation Management Online: How People Monitor and Maintain their Identity through Search and Social Media*, Pew Internet & American Life Project, 26 May 2010, available at www.pewinternet.org/Reports/2010/Reputation-Management.aspx (נבדק לאחרונה ב-5.12.2012).

34 Omer Tene, *Privacy: The New Generations*, 1 INTERNATIONAL DATA PRIVACY LAW REV. 1434 (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1710688 (2010) (נבדק לאחרונה ב-5.12.2012).

35 Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1434 (2008); Article 29 Working Party, Opinion 2/2010 on Online Behavioral Advertising, WP 171, (2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/>

משגרים את המידע הזה לכל עבר;³⁷ שבכי RFID מזהים אותנו, את מכוניותינו ואת מוצרינו;³⁸ מצלמות אבטחה מועצמות בתכנות זיהוי פנים צופות אלינו מכל פינה;³⁹ רשת החשמל הופכת חכמה ומדווחת לחברת החשמל מתי אנחנו שותים קפה ומתי שכחנו להתקלח;⁴⁰ בדיקות גנטיות מזהות נטיות רפואיות שלנו;⁴¹ ומידע ביומטרי מזהה אותנו באופן חד-חד-ערכי שאינו ניתן להכחשה.

למערכות ביומטריות עשויה להיות השפעה חיובית על הזכות לפרטיות. הן מאפשרות זיהוי או אימות זהות של אדם תוך שימוש בשיעור מינימלי של מידע אישי עליו. הן

2010/wp171_en.pdf; *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, December 2010, available at www.ftc.gov/os/2010/12/101201privacyreport.pdf (נבדק לאחרונה 5.12.2012).

Jorg Hladjk, *Location Based Services: European Data Protection Rules for Mobile*, 36 Center for Democracy & Commerce, Privacy & Security Law Report (2009) Technology Policy Post, *The Dawn of the Location-Enabled Web*, 6 July 2009, available at www.cdt.org/policy/dawn-location-enabled-web (נבדק לאחרונה ב-5.12.2012).

Mobile Web Application Best Practices, W3C Recommendation, 14 December 2010, 37 available at www.w3.org/TR/mwabp (נבדק לאחרונה ב-5.12.2012).

Article 29 Data Protection Working Party, Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175, (2010) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf (נבדק לאחרונה ב-6.12.2012); Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, WP 105, (2005) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf (נבדק לאחרונה ב-6.12.2012).

Ting Shan, Shaokang Chen, Conrad Sanderson & Brian Lovell, *Towards Robust Face Recognition for Intelligent-CCTV based Surveillance using One Gallery Image*, IEEE CONFERENCE ON ADVANCED VIDEO AND SIGNAL BASED SURVEILLANCE 470, 470-475 (2007); Bridget Mallon, "Every Breath You Take, Every Move You Make, I'll Be Watching You": *The Use of Face Recognition Technology*, 48 VILL. L. REV. 955 (2003).

Elias Leake Quinn & Adam Reed, *Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act*, 81 U. COLO. L. REV. 833 (2010).

Berrie R. Goldman, *Pharmacogenomics: Privacy in the Era of Personalized Medicine*, 41 NW. J. TECH. & IP 83 (2005); Jennifer A. Gniady, *Regulating Direct to Consumer Genetic Testing*, 76 FORD. L. REV. 2429 (2008).¹⁶ לעיל ה"ש 16.

מתגברות את אבטחת המידע האישי מפני סכנה של פריצה או גנבת זהות.⁴² הן מאפשרות לאבטח מידע תוך שימוש במידע ביומטרי כמפתח הצפנה (Biometric Encryption).⁴³ לעומת זאת, עלולות להיות למערכות ביומטריות השלכות שליליות – ולעתים אף קשות – על הזכות לפרטיות. בעמודים הבאים אסקור סיכונים שמציבות מערכות ביומטריות לפרטיות.

1. זיהוי

מערכות ביומטריות מאפשרות לזהות אדם; אדרבה, זאת מטרתן העיקרית. בטקסונומיה (מיון) שערך לפגיעות שונות בזכות לפרטיות, הסביר פרופ' דניאל סולוב (Solove) כי זיהוי מהווה הלבשה של "מטען מידע" על אדם, קישור בין זהותו לבין פרטים אישיים על אודותיו.⁴⁴ מידע ביומטרי יכול לשמש כמפתח המקשר בין סוגים שונים של מידע על אודות אדם הנאגרים במערכת – כגורם מרכזי ליצירת פרופיל מידע מקיף על אדם. במובן זה, אין המידע הביומטרי שונה ממספר זיהוי קבוע, כגון מספר תעודת זהות בישראל או מספר ביטוח לאומי בארצות-הברית. אלא שבניגוד למספרי זהות שונים, מידע ביומטרי אינו ניתן להחלפה לעולם: אדם אינו יכול להחליף מרצונו החופשי את תויו פניו או את טביעת אצבעותיו, כך שדליפת מידע כזה עלולה להעמידו בפני חשש מתמיד של שימוש לרעה בפרטיו האישיים או אף "גנבת זהותו".⁴⁵ זיהוי מגדיל את כוחה של המדינה על

Anil K. Jain, Arun Ross & Sharath Pankanti, *Biometrics: a Tool for Information Security*, 1 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 125–143 (2006); פרופ' חיים זנדברג מסביר כי אפשר ליישם מערכת זיהוי ביומטרית לצורך ייעול של שיטת מרשם המקרקעין; Haim Sandberg, *Real Estate E-conveyancing: Vision and Risks*, 19 INF. & COMM. TECH. L. 101 (2010).

Ann Cavoukian & Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security, and Privacy*, White Paper, March 2007, available at www.ipc.on.ca/images/Resources/PrivacybyDesign%20Book-ch7.pdf (נבדק לאחרונה ב-5.12.2012); Paul de Hert & Annemarie Sprokkereef, *The Use of Privacy Enhancing Aspects of Biometrics* (Tilburg University; TILT – Tilburg Institute for Law, Technology, and Society), January 2009, available at arno.uvt.nl/show.cgi?fid=93109 (נבדק לאחרונה ב-5.12.2012).

Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006). הטקסונומיה היא ניסיונו של פרופ' סולוב להתמודד עם קשיי ההגדרה של הזכות לפרטיות באמצעות פירוט וקטלוג הפגיעות השונות בזכות.

גנבת זהות, שבמסגרתה נעשה שימוש בפרטיו האישיים של אדם לצורך רכישות בכרטיס אשראי, פתיחת חשבונות בנק ונטילת הלוואות, הלבנת הון, ואף קבלת טיפול רפואי, מהווה אחד הפשעים הנפוצים והמזיקים ביותר בארצות-הברית. ראו למשל *The President's Identity*

חשבון היחיד ומאפשר לה, במקרים הגרועים, להפלות קבוצות אוכלוסין לרעה או אף לייחדן לטיפול אכזרי ואלים.⁴⁶ זיהוי גם מאיין את זכותם של יחידים לאנונימיות או פסבדונימיות, ובכלל זה לביטוי אנונימי, שחשיבותו הוכרה בפסיקה של בית המשפט העליון בישראל ובארצות-הברית.⁴⁷ יובהר, כי כפי שציין בית המשפט העליון בפסק דין מור ובעניינים אחרים, הזכות לאנונימיות אינה זכות מוחלטת, לעתים היא תיסוג מפני זכויות אחרות כגון זכותו של אדם לשם טוב⁴⁸ או זכות קניין של אדם אחר.⁴⁹ אלא שפרק זה אינו עוסק באיזון הרצוי שבין הזכות לפרטיות לבין זכויות אחרות, אלא אך באפיון הפגיעה בפרטיות הטמונה במערכת זיהוי ביומטרית.

זאת ועוד: אם בעבר יכולנו לשוטט במקום העבודה או להיכנס למקומות בילוי ציבוריים מבלי שתנועותינו יתועדו, הרי בקרוב ישחקו מערכות ביומטריות את מעטה האנונימיות וינציחו באופן דיגיטלי כל פתיחת דלת במשרד או תנועה שלנו ברחובות עיר. אמן הגרפיטי הבריטי Banksy אמר בהקשר זה, כי "בעתיד ייהנה כל אדם מ-15 דקות של אנונימיות".⁵⁰

2. "חפצון" הגוף

ככל שגדל היקף השימוש בביומטריה למטרות זיהוי, מצטמצמת זהותו של אדם לאוסף של נתונים ביומטריים; גופו נתפס כחפץ שמידותיו נמדדות, נאגרות ומשמשות את רשויות השלטון למטרות שאינן תמיד נהירות לו. חשבו למשל על תחושתו של אדם בכניסה לתחום השיפוט של ארצות-הברית, בעמדת ביקורת הגבולות בשדה התעופה ג'יי-אף-קיי בניו-יורק,

- Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007, available at www.idtheft.gov/reports/StrategicPlan.pdf (נבדק לאחרונה ב-5.12.2012).
- Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37 (2002); וראו גם ספרו של העיתונאי אדווין בלק, המתאר את השימוש שעשתה גרמניה הנאצית במאגרי מידע מבית היוצר של איי-בי-אם לצורך זיהוי ואיסוף היהודים במדינות אירופה הכבושות לצורך שיגורם למחנות ריכוז והשמדה: EDWIN BLACK, *IBM and the HOLOCAUST* (2001).
- עניין מור, לעיל ה"ש 29; מיכאל בירנהק "חשיפת גולשים אנונימיים ברשת" חוקים ב 51 (2010); (1995) 514 U.S. 334 *McIntyre v. Ohio Elections Commission*.
- עניין מור, לעיל ה"ש 29.
- ע"א 9183/09 *The Football Association Premier League Limited נ' פלוני* (פורסם בנבו, 13.5.2012).
- ראו את פסלו של האמן באתר www.flickr.com/photos/fstutzman/246517721 (נבדק לאחרונה ב-5.12.2012).

בעת שקצין ההגירה נוטל את סריקת אצבעותיו ואת צילום הפנים שלו.⁵¹ למה משמש מידע זה שנלקח ממנו? מה ייעשה בו? למי יועבר? עד מתי יישמר? כיצד "סיווג" אותו קצין ההגירה? האם שויך לקבוצה ב"סיכון גבוה"? שאלות אלה ואחרות עלולות להטרידו במסגרת תהליך הזיהוי בשדה התעופה. מדובר בפגיעה בכבוד האדם המהווה גם פגיעה בפרטיותו.⁵² זאת ועוד: תהליך הדגימה הביומטרי כולל איסוף מידע מגופו של אדם, להבדיל ממידע על האדם, ומכאן שהוא עלול להיתפס כחודרני ואף משפיל.⁵³ נטילת טביעות אצבעות, למשל, היא תהליך הנחזה מבחינה חברתית להיות חלק מהיחס המוענק לעבריינים,⁵⁴ והיא עשויה לעורר חוסר נוחות גם כאשר היא מבוצעת בהקשר חברתי שונה – כגון בנמל התעופה בכניסה לארצות הברית. תפיסתו של הגוף כחפץ, כאובייקט, מהווה כשלעצמה פגיעה בפרטיות שעליה התריעה פרופ' רות גביון במאמר משנת 1980.⁵⁵ פרופ' גביון ציינה כי ה"חפצון" ("החפצה"), היינו האובייקטיביזציה, של גוף האדם גורם לכך שאדם מאבד את השליטה בכל מיני היבטים חשובים של חייו. הוא הופך ל"מספר", לפרופיל, שכל פקיד יכול בהקשת כפתור לקבלו. זוהי פגיעה בכבוד, פגיעה בשליטה של אדם בגורלו, באוטונומיה שלו. אכן, כבר במאה ה-18 הזהיר הפילוסוף הגרמני עמנואל קאנט מפני הפיכתו של אדם לאובייקט ושימוש בו כאמצעי להבדיל מתכלית בפני עצמו.⁵⁶

51 בעקבות ניסיונות פיגוע אחדים בטיסות בין-לאומיות לארצות הברית, החליטו רשויות הביטחון האמריקניות להציב ברוב נמלי התעופה הגדולים "סורקי גוף" ממוכנים המספקים תמונה של גופו העירום של אדם על מנת לזהות חומרי נפץ המוסתרים מתחת לבגדיו. פריסתם הרחבה של סורקי הגוף עוררה גל גדול של מחאה בקרב ארגוני זכויות ואזרחים מודאגים, שמחו על הפגיעה הקשה בפרטיות ו"הפשטתם" הווירטואלית של הנוסעים. ראו Jessica Rettig, "TSA Balances Privacy and Security with Body Scanners, Pat Downs", US NEWS & WORLD REP., 24 Nov. 2010, available at bit.ly/f0mUXo (5.12.2012).

52 על הקשר בין כבוד האדם לבין הזכות לפרטיות ראו Omer Tene, *Privacy in Europe and the United States: I Know It When I See It*, CDT Blog, 27 June 2011, available at www.cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it. (נבדק לאחרונה ב-5.12.2012).

53 חגי אפרתי "לסמן אנשים" **ארץ אחרת** 72 (2012).

54 ראו דיון מקיף בפסק דינו של בית הלורדים: *Wainwright v. Home Office*, [2003] UKHL 53.

55 רות גביון "הזכות לפרטיות ולכבוד" **בלי הבדל... זכויות האדם בישראל אוסף מאמרים לזכרו של חמן שלח ז"ל** 61, 67–68 (1988); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980).

56 זוהי כמובן נגזרת של הצו הקטגורי של קאנט: עמנואל קאנט **ביקורת התבונה הטהורה** 7581 (שמואל הוגו ברגמן ונתן רוטנשארף תרגמו, 1993).

לחששות עקרוניים אלה נלווה הסיכון המוחשי, כי קבוצות אוכלוסין מסוימות יופלו לרעה עקב הקושי האובייקטיבי לדגום את נתוניהם הביומטריים. כך, למשל, עלולים קטועי ידיים (או שחקני כדורסל, שהעור על קצות אצבעותיהם נשחק) להיתקל בקשיים בפני מערכת הדוגמת טביעות אצבע; או בעלי קטרקט מול מערכת סריקת קשתית.⁵⁷ נשים מוסלמיות למשל עלולות להימנע מלשתף פעולה עם מערכת הדורשת צילום פנים, מטעמי דת. בני אדם אלה עלולים לסבול מסטיגמה שלילית עקב אי-התאמת גופם לאמות המידה המוכתרות על ידי המערכת הביומטרית. השלכותיה של הסטיגמה כוללות עיכוב לחקירה, עמידה בטורים ארוכים, או הפליה.

3. זחילת פונקציות

אחד החששות הכבדים הנקשרים תדירות למאגרי מידע בכלל ולמערכות ביומטריות בפרט, הוא החשש מפני "זחילת פונקציות" (function creep) שתוביל לשימושים שניוניים או לא צפויים במידע או להעברות מידע בין גופים שונים או מדינות שונות.⁵⁸ כך, למשל, עשוי מאגר טביעות אצבע שנאסף למטרות הנפקה מסודרת של תעודות זהות לשמש את המשטרה ורשויות הביטחון לצורכי אכיפת חוק;⁵⁹ באופן דומה ומטריד אף יותר, עשוי מאגר תמונות הפנים הביומטרי להשתלב עם מידע שנאסף באמצעות הרשת ההולכת ונפרשת של מצלמות אבטחה במרחבים ציבוריים; וזאת, לצורך מעקב מתמיד אחר מיקומם של אזרחים. זמינותם של נתוני הזיהוי הביומטרי כ"מפתח" שאליו אפשר לקשור פרטי מידע שונים על אדם, הופכת אותם לשימושיים במיוחד למטרות שונות מאלה שלשמן נאספו. ככל שהמידע הביומטרי נגיש ליותר רשויות שלטון או גופים עסקיים, וככל שהמערכות מתוכננות לתפעוליות בינית (interoperability), גובר החשש מפני שימושים שניוניים במידע. כך, למשל, הפך מספר תעודת הזהות בישראל לנתון מפתח המשמש רשויות ציבוריות וגופים עסקיים לצורך קטלוג מידע מתחומים שונים ובהיקף נרחב על אזרחים. לא בכדי, נפתחת כיום כל שיחה עם מרכז שירות לקוחות של עסקים שונים בשאלה "מה מספר תעודת הזהות?" ואכן, כפי שאראה בהמשך, במקרה של המאגר

57 ראו תקנה 8 לתקנות, המנסה להתמודד עם קושי זה באמצעות קביעתם של הסדרים ל"נטילת אמצעים ביומטריים מקשישים או בעלי מוגבלות".

58 ראו ה"ש 29. ס' 6(1)(B) של דירקטיבת 95/46 קובע: "[personal data must be] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". זהו "עקרון צמידות המטרה" החל גם בישראל מכוח סעיף 2(9) וס' 8(ב) לחוק הגנת הפרטיות. ראו מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" משפט וממשל יא 9 (2007).

59 ראו למשל ס' 17 ו-21 לחוק.

הביומטרי ניכרת זחילת הפונקציות כבר במסגרת לשון החוק עצמו; ⁶⁰ אדרבה, יש שיטענו כי השימושים השניוניים במידע הביומטרי הם המטרה האמתית העומדת בבסיס חקיקתו של החוק (או למצער, הקמתו של המאגר המרכזי), ה-*raison d'être* שלו.⁶¹ מאגרי מידע ממשלתיים בישראל לא הצטיינו עד כה במבחן "זחילת הפונקציות". כך, למשל, הקים חוק איסור הלבנת הון, התש"ס-2000 (להלן: "חוק איסור הלבנת הון") מאגר מידע מקיף ורגיש למטרות מוגבלות, שעיקרן איסור הלבנת הון ומימון טרור. עם זאת, במהלך השנים התארכה מאוד רשימת "עברות המקור" הכפופות לחוק, באמצעות תיקונים חוזרים ונשנים של התוספת הראשונה שלו.⁶² כמו כן, הותקנו בשנת 2006 תקנות איסור הלבנת הון (כללים לשימוש במידע שהועבר למשטרת ישראל ולשירות הביטחון הכללי לשם חקירת עבירות נוספות ולהעברתן לרשות אחרת), התשס"ו-2006, המסמיכות את המשטרה והשב"כ להשתמש במאגר לשם חקירת שורה ארוכה של עברות שאינן מנויות בחוק כ"עברות מקור", וכן להעביר מידע מהמאגר לידיהם של גורמי חקירה חיצוניים רבים. יש לציין עוד, כי למרות רגישותו הרבה של המידע במאגר הרשות לאיסור הלבנת הון ואמצעי האבטחה הקפדניים הנהוגים ברשות, דלף לאחרונה מידע רגיש מהמאגר והגיע לידיהן של רשויות ביטחון במדינה שלה יחסים רגילים עם ישראל. האדם שהמידע על אודותיו דלף הועמד לפיכך בסכנה ברורה ומוחשית.⁶³

4. סכנת אבטחה

כל מומחה אבטחת מידע יעיד כי הדרך היעילה ביותר לאבטח מאגר מידע היא לא להחזיקו כלל. מאגרי מידע חשופים לכשלים ולפרצות אבטחה, להדלפה על ידי עובדים רשלנים או מושחתים, לפריצה על ידי האקרים או גופי מודיעין, או לשינוי מידע או אבדנו עקב תקלות מערכת או אסון טבע.⁶⁴ החשש לפרצות אבטחה במערכות ביומטריות כבד ביותר, שכן

60 ש.ם.
61 ראו למשל אלי ביהם "אל תיתנו את האצבע למאגר" **ארץ אחרת** 64 (2012).
62 התוספת הראשונה לחוק איסור הלבנת הון, המפרטת את עברות המקור, תוקנה במסגרת תיקון 2 (2003), 4 (2005), 6 (2006) ו-7 (2007) לחוק וכן בצווים משנת 2002 ו-2010 ובהוראת שעה משנת 2004.
63 צבי לביא "דו"ח: ליקויי אבטחה גרמו לדליפת מידע על נבזלין" **Ynet** 30.3.2008
64 פרצת אבטחה מהווה פגיעה בפרטיות, מכוח סעיף 17 לחוק הגנת הפרטיות. ראו גם תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986.

הנזק העלול להיגרם הוא בלתי-הפיך.⁶⁵ מידע ביומטרי אינו ניתן להחלפה, ודליפתו עלולה להציב אדם בפני חשש מתמיד מפני ניצול המידע לרעה או גנבת זהותו. סיכון האבטחה הכרוך במערכת הביומטרית חמור במיוחד אם המערכת מחזיקה במידע במאגר מרכזי; והוא חמור עוד יותר אם המידע שמוחזק במאגר הוא המידע הביומטרי הגולמי להבדיל מתבנית דיגיטלית שלו, וזאת עקב הקושי הגלום באחזור מידע גולמי מהתבנית הדיגיטלית שלו. במקרים אלה, עלולה פרצת אבטחה לאפשר למי שהשיג שלא כדין את המידע להשתמש בו לצורך התחזות; חתימה דיגיטלית על הודעות או עסקאות; או אף הפללה של האדם שהמידע שלו דלף (למשל באמצעות השארת העתק של טביעת אצבעותיו בזירת פשע). ככל שהמידע המזהה נחשב אמין יותר – ונתונים ביומטריים נחשבים אמינים במיוחד – כך יקשה על אדם להתנער מעקבות המידע שהשאיר או ש"הושארו" בשמו. הוא עלול אפוא להיות קרבן להתחזות ולהיאלץ להיאבק על חפותו כנגד כל הסיכויים וללא יכולת לשנות את נתוני הזיהוי שלו כדי למנוע הישנות התופעה בעתיד.⁶⁶ לחלופין, יפגעו אירועי אבטחה כאלה באמינות הראיות מסוג זה המוגשות לבתי המשפט.⁶⁷

יש הטוענים כי אפשר להתגבר על הבעיה של דליפות מידע או פריצות למאגר באמצעות אמצעי אבטחה הולמים. עם זאת, לאחרונה עורר אתר הדלפות המידע ויקיליקס (WikiLeaks), שערורייה ציבורית בין-לאומית בחשפו מאות אלפי מסמכים צבאיים, דיפלומטיים ועסקיים, לרבות מסמכים שסווגו כ"סודי ביותר" על ידי כוחות הביטחון של ארצות-הברית. שערורייה זו מוכיחה עד כמה קשה להתבסס כיום על אמצעי אבטחה "הרמטיים" במאגרי מידע ממוחשבים.⁶⁸ במקרה זה הודלפו המסמכים הרגישים, שגילויים גרם נזק לביטחון המעצמה האמריקנית וליחסי החוץ שלה, בידי חייל מודיעין אמריקני בדרגת טוראי.⁶⁹ בין המסמכים שהודלפו נחשפו גם מסמכים המעידים על העניין הרב בקרב

65 Andy Adler, *Biometric System Security*, HANDBOOK OF BIOMETRICS, בתוך Handbook of Biometrics, לעיל ה"ש 12, בעמ' 380–402.

66 ראו עומר טנא "זיהוי ביומטרי: חוק האח הענק הוא הסייט הקפקאי הבא" *The Marker* 17.6.2008 www.themarker.com/law/1.485953 (נבדק לאחרונה ב-5.12.2012)

67 התוצאות של מידע שגוי הנשמר במאגרי מידע רשמיים עלולות להיות הרוות אסון. טלו למשל את המקרה של התובע בת"א (שלום ב"ש) 8051/00 טזנו נ' משרד הבריאות מחזו דרום (פורסם בנבו, 1.6.2000), שתויג בטעות כ"חולה נפש" ואיבד בעקבות כך את מקום עבודתו ובהמשך גם את זכאותו למשכנתה.

68 Scott Shane & Andrew Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, NY TIMES, 28 Nov. 2010, available at www.nytimes.com/2010/11/29/world/29cables.html (נבדק לאחרונה ב-5.12.2012).

69 Nick Allen, *Bradley Manning: The Prime Suspect of Giving Files to WikiLeaks*, THE TELEGRAPH, 28 Nov 2010, available at bit.ly/fid0jH (נבדק לאחרונה ב-5.12.2012).

אנשי משרד החוץ האמריקני, ובראשם שרת החוץ הילרי קלינטון, באיסוף מידע ביומטרי של דיפלומטים זרים.⁷⁰ נקל לשער מה רב העניין שיעורר מאגר מידע המכיל מידע ביומטרי של כל אזרחי ישראל בקרב ארגוני פשע וטרור ורשויות ביטחון של מדינות עוינות יותר או פחות.

ספק אם המדינה תגלה נחישות רבה יותר באבטחת מידע פרטי של אזרחיה מאשר בהגנה על מידע ביטחוני רגיש, המודלף ומופץ לעתים לעיתונות בארץ ובעולם.⁷¹ הישגי העבר של המדינה בתחום זה אינם מעוררים הערכה: אין הרבה מדינות בעולם שמאגר המידע הרגיש של מרשם האוכלוסין שלהן ניתן להורדה באתרי שיתוף קבצים ברשת, כמו מרשם האוכלוסין של מדינת ישראל.⁷² זאת, בעקבות פרצת אבטחה שמקורה לא נודע (המשטרה סגרה את תיק החקירה לנוכח "ריבוי חשודים").⁷³ מבקר המדינה קבע בעניין זה,

- Robert Booth & Julian Borger, *US diplomats spied on UN leadership*, THE GUARDIAN, 28.11.2010, available at www.guardian.co.uk/world/2010/nov/28/us-embassy-cables-spying-un (נבדק לאחרונה ב-5.12.2012): "A classified directive which appears to blur the line between diplomacy and spying was issued to US diplomats under Hillary Clinton's name in July 2009, demanding forensic technical details about the communications systems used by top UN officials, including passwords and personal encryption keys used in private and commercial networks for official communications. It called for detailed biometric information 'on key UN officials, to include undersecretaries, heads of specialised agencies and their chief advisers, top SYG [secretary general] aides, heads of peace operations and political field missions, including force commanders' [...] A parallel intelligence directive sent to diplomats in the Democratic Republic of the Congo, Uganda, Rwanda and Burundi said biometric data included DNA, fingerprints and iris scans"
- 70 אין צורך להזכיר, כמובן, את פרשת ההדלפה של סודות הגרעין של ישראל בידי מרדכי וענונו. ראו גם לאחרונה תפ"ח (מחוזי ת"א) 17959-01-10 **מדינת ישראל נ' קם** (פורסם בנבו, 30.10.2011); ורד לוביץ' "חיילת-מרגלת: גנבה אלפי מסמכים 'סופר-מסווגים'" **Ynet** 8.4.2010 www.ynet.co.il/articles/0,7340,L-3871970,00.html (נבדק לאחרונה ב-5.12.2012).
- 71 ניב ליליאן ואהוד קינן "מעקב: המידע האישי של אזרחי ישראל מופץ ברשת" **Ynet** 11.10.2007 www.ynet.co.il/articles/0,7340,L-3459002,00.html (נבדק לאחרונה ב-5.12.2012); אור הירשאווגה ובר בן ארי "הרשות למשפט וטכנולוגיה: מרשם האוכלוסין שדלף מנוצל לצורך גביית חובות" **The Marker** 22.9.2009 it.themarker.com/tmit/article/8197 (נבדק לאחרונה ב-5.12.2012).
- 72 היונתן ליס "המשטרה לא הצליחה לאתר את מדליפי מרשם האוכלוסין" **הארץ** 4.5.2009 www.haaretz.co.il/hasite/spages/1082874.html (נבדק לאחרונה ב-5.12.2012).

כי "יש לראות בחומרה את כישלונה של רשות האוכלוסין בהגנת פרטיותם של אזרחי המדינה".⁷⁴

משה בסול, שכיהן כראש היחידה לאבטחת מידע במשרד ראש הממשלה, הבהיר מה צפוי למאגר הביומטרי, בכותבו: "שלא יהיה ספק – גם המאגר הביומטרי יפרץ מתישהו; כולו או חלקו. זה יכול להיות מבצע מתוחכם שייקח שנים להבין מי, מתי ואיך זה נעשה, אבל זה יכול להיות גם כתוצאה מסתם טעות שולית של חוסר תשומת לב. צריך לזכור שבכל מערכת דיגיטלית מעורבים גורמים רבים בהם: ספקי ציוד של חומרה תוכנה ותקשורת, מתכנתים, יועצים ואנשי תחזוקה. המידע מועבר על קווי תקשורת, מאוחסן על גבי מדיות דיגיטליות ומגיע למשתמשים שונים. יש נקודות כשל רבות שאחת מהן תפרץ לבסוף. זה יקרה מכשל ברמה האנושית, באבטחה הדיגיטלית, דרך קווי התקשורת, יועץ או איש תחזוקה שלא נבדקו כראוי, או משהו שעוד לא הספקנו לחשוב עליו."⁷⁵ אם זוהי עמדתו של הדרג המקצועי האמון על אבטחת המאגר, נקל להבין מדוע מעורר החוק חששות רבים בקרב הציבור.

כפי שציינתי לעיל, אבטחת מידע היא משימה סיוזיפית הכוללת מרוץ חימוש בלתי פוסק בין מומחי הגנה למומחי התקפה.⁷⁶ לא רק מדינת ישראל, אלא גם שורה ארוכה ומכובדת של גופים עסקיים גדולים ורשויות ציבוריות, נחשפו בשנים האחרונות בקוצר ידם למנוע את התופעה. פרשת "ההאקר הסעודי" שפרץ ב-2012 לעשרות אתרי אינטרנט ישראלים וחשף באינטרנט את פרטי כרטיסי האשראי של אלפי לקוחותיהם, אינה אלא קצהו של קרחון, שהיקפו העולמי אדיר.⁷⁷ כך, למשל, בשנת 2007 דלפו רשומות מפורטות של מידע פיננסי על 25 מיליון אזרחי בריטניה בעקבות אבדן דיסקים ממוחשבים בידי רשויות המס

74 דו"ח מבקר המדינה לשנת 2008, דו"ח שנתי 59 בשנת 2008 ולחשבונות שנת הכספים 2007 (הדו"ח המלא), עמ' 860. וראו גם אהוד קינן "המבקר: כישלון חמור בהגנה על פרטיות האזרחים" *Ynet* 6.5.2009 www.ynet.co.il/articles/0,7340,L-3710407,00.html (נבדק לאחרונה ב-5.12.2012).

75 משה בסול "המאגר הביומטרי: אי אפשר לעצור את הקדמה" *The Marker* 4.5.2011 it.themarker.com/tmit/article/15219 (נבדק לאחרונה ב-5.12.2012) (לצורך שלמות התמונה יצוין כי בסול עדיין תומך בהקמת המאגר הביומטרי, שכן "צריך לזכור כי לקדמה זו יש גם תג מחיר שאל לנו להתעלם ממנו או להדחיקו. צריך להסתכל על תג המחיר בעיניים פקוחות, ולקבל החלטה שהקדמה והיתרונות שהיא מעניקה אכן מצדיקים את המחיר").

76 ראו STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984).

77 אופיר פרימט ואור הירשאוגה "פריצת כרטיסי האשראי: האקר סעודי פירסם 15,000 כרטיסים ישראלים" *The Marker* 3.1.2012 www.themarker.com/hitech/1.1607776 (נבדק לאחרונה ב-5.12.2012).

של המדינה (HM Revenue and Customs (HMRC));⁷⁸ בשנת 2009 איבדה ממשלת ארצות-הברית מידע אישי על 76 מיליון חיילים משוחררים; ואילו חברת Card Systems המשתמשת כמסלקת כרטיסי אשראי של חברת מאסטרקארד הודתה ב-2005 כי פורצים השיגו את פרטי כרטיסי האשראי של יותר מ-40 מיליון לקוחות.⁷⁹ בעקבות ריבוי הפריצות ודליפות המידע מהמאגרים, שטף ראשית את ארצות-הברית ולאחר מכן את אירופה גל של חקיקה המחייב גופים עסקיים ושלטוניים למסור הודעה על כשל אבטחת מידע לרגולטורים או לנפגעים מהדליפה.⁸⁰

5. מידע עודף

איסוף דגימות של מידע ביומטרי עלול להיות מלווה באיסוף מידע נוסף הנגזר מהמידע הביומטרי עצמו. כך, למשל, טביעות אצבע עשויות להעיד על תופעות כגון תסמונת דאון;⁸¹ סריקת קשתית – לחשוף שימוש באלכוהול או סמים;⁸² וצילום פנים – לגלות פרטים על גזעו של אדם, מינו, דתו, תרבותו ומצבו הנפשי. מידע עודף זה עלול לשמש לשימושים שניוניים במידע, כגון יצירת פרופילים או הפליה לרעה של האדם שמסר את המידע. השילוב בין איסוף מקיף של מידע המוחזק במאגרים שונים בחזקת המדינה⁸³ לבין

- Patrick Wintour, *Lost in the Post – 25 Million at Risk After Data Discs Go Missing*, THE GUARDIAN, 21.11.2007, available at www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.economy3 (נבדק לאחרונה ב-5.12.2012). 78
- Ki Mae Heussner, *10 of the Top Data Breaches of the Decade*, ABC News, 14.6.2010, available at abcn.ws/grB78J (נבדק לאחרונה ב-5.12.2012). לרשימה ממצה של הודעות על כשל אבטחת מידע ראו המאגר המעודכן של ארגון הזכויות: Privacy Rights Clearinghouse. *A Chronology of Data Breaches* www.privacyrights.org/data-breach (נבדק לאחרונה ב-5.12.2012). 79
- Cal. Civ. Code § 1798.29, .82, .84 בקליפורניה: 2003 נחקק מסוג זה נחקק ב-2003 בקליפורניה: Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007). 80
- Thomas Fogle, *Using Dermatoglyphics from Down Syndrome and Class Populations to Study the Genetics of a Complex Trait*, in TESTED STUDIES FOR LABORATORY TEACHING 129 (C.A. Goldman ed., 1990). 81
- Courtney Ostaff, *Retinal Scans Do More Than Let You In The Door*, PHYSORG.COM, August 2005, available at www.physorg.com/news6134.html (נבדק לאחרונה ב-5.12.2012). 82
- A האקונומיסט דיווח לאחרונה כי היקף המידע הדיגיטלי גדל פי עשרה בכל חמש שנים; *Special Report on Managing Information: Data, Data Everywhere*, THE ECONOMIST 25.2.2010. 83

היכולת ההולכת וגדלה של כריית מידע, מעמיק את הסכנה לשימושים שניוניים כאלה, ועמה את הפגיעה בפרטיות האזרחים.⁸⁴

6. מעקב

נתונים ביומטריים שונים משאירים שובל של מידע שבאמצעותו אפשר להתחקות אחר התנהגותו של אדם ללא ידיעתו.⁸⁵ כך, למשל, נוהגים חוקרי משטרה לעקוב אחרי חשודים באמצעות טביעות אצבע שהשאירו אחריהם. עם התפשטות השימוש במצלמות אבטחה, בני אדם מותירים אחריהם שובל של מידע המאפשר לעקוב אחרי תנועותיהם ברחובות עיר או במקומות ציבוריים אחרים. לאחרונה התברר כי המדינה מתכוונת לפרוס מצלמות אבטחה (CCTV) במרחב הציבורי במסגרת פרויקט "עיר ללא אלימות" למאבק בפשיעה.⁸⁶ השילוב בין מצלמות אבטחה בפריסה רחבה האוגרות מידע בפורמט דיגיטלי לבין יכולות חיפוש ומעקב באמצעות מאגר תמונות בתקן ביומטרי, מעורר חששות ליצירת "פנאופטיקון" מודרני,⁸⁷ שבו הופך האזרח ל"נקודת ציון ניידת" על מפה המוחזקת בידי המדינה.⁸⁸ כפי שהוסבר לעיל, עלול חשש זה להתרגם לצנזורה עצמית של ביטוי, התנהגות ואף מחשבות על מנת להתאימן לתפיסה המקובלת על ידי בעל הכוח הצופה באזרח.⁸⁹

- Ira Rubinstein, Ronald Lee & Paul Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008) 84
- סעיף 2 לחוק הגנת הפרטיות קובע: "פגיעה בפרטיות היא אחת מאלה (1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרידה אחרת". 85
- "המשרד לביטחון פנים ירכוש מצלמות אבטחה עירוניות בעשרות מיליוני שקלים" The Marker 29.5.2011 it.themarker.com/tmit/article/15532 (נבדק לאחרונה ב־5.12.2012): "במסגרת מכרז חדש שפרסם המשרד לביטחון פנים, ירכשו מצלמות, חיישנים ויוקמו מוקדי שליטה ובקרה בערים המשתתפות בתוכנית 'עיר ללא אלימות'". 86
- Foucault, לעיל ה"ש 31. הפנאופטיקון, מודל של בית כלא שבו האסיר נתון למעקב תמידי, הוצג במקור על ידי הפילוסוף הבריטי בן המאה ה־18 ג'רמי בנת'הם. JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., 1995) 87
- ראו למשל Ting Shan, *Reliable Face Recognition for Intelligent CCTV*, RNSA SECURITY TECHNOLOGY CONFERENCE CANBERRA, AUSTRALIA 356–364 (2006), available at www.nicta.com.au/___data/assets/pdf_file/0009/14949/Reliable_Face_Recognition_for_Intelligent_CCTV.pdf (נבדק לאחרונה ב־5.12.2012). 88
- ראו לעיל ה"ש 29–32 והטקסט הנלווה. 89

ה. המבחן החוקתי

ראינו אפוא כי הקמתה של מערכת ביומטרית המכילה מידע על כלל אוכלוסיית ישראל עלולה לפגוע, בכוח ובפועל, בזכות החוקתית לפרטיות.⁹⁰ חוק הפוגע בזכות חוקתית המעוגנת בחוק יסוד נדרש לעמוד במבחניה של פסקת ההגבלה, המכשירה את הפגיעה רק אם זאת נעשתה בחוק או על פי חוק, לתכלית ראויה ההולמת את ערכיה של מדינת ישראל כמדינה יהודית ודמוקרטית ובמידה שאינה עולה על הנדרש.⁹¹ בדרך כלל מתמקדת הבדיקה החוקתית בשאלת המידתיות; לנוכח ניסוחו של סעיף המטרה בחוק, שעליו אעמוד להלן, מתעורר במקרה זה ספק לא מבוטל בדבר עמידתו של החוק במבחן "התכלית הראויה". לפני שאערוך את הניתוח החוקתי המהותי, אדון בסוגיה חוקתית-מנהלית המתעוררת עקב הוראת התחולה הייחודית של החוק, ההופכת אותו למעין "חוק על תנאי".⁹²

1. "פגיעה בחוק או על פי חוק"

בסעיף 41 לחוק, שכותרתו "תחולה הדרגתית ותקופת מבחן", נאמר כי השר יקבע "תקופת מבחן של שנתיים שבמהלכה יחולו ההוראות לפי חוק זה על תושבים שייתנו את הסכמתם לכך בכתב, במטרה לבחון בתקופה זו את אופן היישום של הוראות לפי חוק זה על תושבים אלה, את נחיצות קיומו של מאגר ביומטרי ומטרותיו, את המידע שיש לשמור במאגר ואת אופן השימוש בו".⁹³ אם כן, כניסתו של החוק לתוקף תלויה בקביעתו של השר ומכך שמדובר ב"חוק על תנאי".⁹⁴ באופן מפתיע, מי שמוסמך לקבוע כי התנאי התקיים וכי החוק

90 ראו לעיל פרק ד.

91 ע"א 6821/93 בנק המזרחי נ' מגדל כפר שיתופי, פ"ד מט(4) 221, פס' 70, 90–93 לפסק דינו של הנשיא ברק (1995); בג"ץ 1715/97 לשכת מנהלי ההשקעות בישראל נ' שר האוצר, פ"ד נא(4) 367, פס' 18–17 לפסק דינו של הנשיא ברק (1997).

92 מאמר זה עוסק בעיקרו בהיבטים של משפט וטכנולוגיה. לפיכך, לא ארחיב את הדיון על ההיבטים המנהליים הנדונים בתת-פרק זה אלא רק אציג את הבעיה המתעוררת.

93 אבנר פינצ'וק טוען כי אין זה המקרה היחיד שבמסגרתו המדינה מקדמת מיום העלול לפגוע בפרטיות כ"פיילוט" ולאחר מכן מנסה "להלבינו" בחקיקה. ראו אבנר פינצ'וק "כשפקידי הממשלה עוברים על החוק" ארץ אחרת 64, 48 (2012). הכותב מתייחס אל הרשומה הרפואית הלאומית במשרד הבריאות; פרויקט מצלמות האבטחה "עיר ללא אלימות" של המשרד לביטחון פנים.

94 העובדה כי החוק עדיין איננו בתוקף אלא רק בתקופת ניסיון היוותה בסיס לקביעת בית המשפט העליון, כי העתירה שהוגשה כנגד חוקתיות החוק מוקדמת. ראו עניין נהון, לעיל ה"ש 6.

יוחל על כלל אזרחי המדינה איננה הכנסת, אלא שר הפנים (החייב להתייעץ לשם כך עם ועדות השרים והח"כים המוקמות מכוח החוק). כמו כן, מוסמך שר הפנים לקבוע כי תקופת התנאי תוארך במשך שנתיים נוספות, וכי ההסדר ייכנס לתוקף רק באופן הדרגתי ובתנאים שפשרם לא הוברר במסגרת לשון החוק. סעיף 41(6) לחוק, במעין סוף פסוק המאיין באבחה חדה אחת את אלפי המילים שהופיעו לפני כן, קובע כי אם "לא הוצא צו [המרחיב את תחולת החוק על כל האוכלוסייה] בתוך ארבע שנים מיום תחילתו של צו כאמור בפסקה (1), יימחק המאגר הביומטרי".

מקורן של הוראות אלה בפשרה פוליטית שהושגה לנוכח המחלוקת הציבורית העזה שניטשה סביב הקמת המאגר במקביל לדיונים בכנסת על הצעת החוק.⁹⁵ באחדים מהדיונים בוועדה המשותפת נכח רק חבר כנסת אחד, הוא יו"ר הוועדה ומי שיזם את החוק במושב הקודם של הכנסת בעת שכיהן כשר הפנים, ח"כ מאיר שטרית.⁹⁶ לעומת זאת, בציבור התנהל דיון ער (יחסית לנושאים מסוג זה) בעד ונגד החוק, בהשתתפות מומחים מהאקדמיה, מהתעשייה ומרשויות הביטחון, כולל משפטנים, מומחי הצפנה ומומחי ביומטריה.⁹⁷ לקראת העברתה של הצעת החוק לקריאה שנייה ושלישית, הגיעה המחלוקת למסדרונות הכנסת, כאשר חברי כנסת אחדים במפלגת השלטון (הליכוד) ובראשם השר מיכאל איתן, ניסו לבלום את רכבת החקיקה השועטת בראשותו של "הקטר" ח"כ שטרית,

95 אטילה שומפלבי ואהוד קינן "פשרה: המאגר הביומטרי יידחה בשנתיים" Ynet 17.11.2009 www.ynet.co.il/articles/0,7340,L-3806715,00.html (נבדק לאחרונה ב-5.12.2012).

96 אהוד קינן וניב ליליאן "ועדת החוק הביומטרי: איפה חברי הוועדה?" Ynet 21.7.2009 www.ynet.co.il/articles/0,7340,L-3749497,00.html (נבדק לאחרונה ב-5.12.2012): "ועדת המדע של הכנסת אישרה בימים האחרונים, פה אחד, כמה סעיפים בחוק המאגר הביומטרי לקריאה שנייה ושלישית. אין זה בגלל שיש תמימות דעים בנוגע לסעיפי החוק, אלא מאחר ששטרית הוא חבר הוועדה היחיד שמצביע"; ארז רונן ואהוד קינן "המלצה: שטרית יטפל בחוק המאגר הביומטרי" Ynet 15.6.2009 www.ynet.co.il/articles/0,7340,L-3731697,00.html (נבדק לאחרונה ב-5.12.2012): "ועדת הפנים של הכנסת המליצה היום לוועדת החוק להעביר את הטיפול בחוק הביומטרי לוועדה משותפת של הפנים והמדע. אם תקום, יעמוד בראש הוועדה מי שיזם את החוק – שר הפנים לשעבר מאיר שטרית. המתנגדים: אם הוועדה תקום, היא תהיה חותמת גומי בלבד".

97 ראו למשל את אתר מטה המאבק במאגר הביומטרי: no2bio.org/home, וכן את מכתבה של נציבת הגנת הפרטיות של אונטריו, אן קאווקיאן, אליי: "החוק הביומטרי – מדרון חלקלק למדינת משטרה" Ynet 10.8.2009 www.ynet.co.il/articles/0,7340,L-3759781,00.html (נבדק לאחרונה ב-5.12.2012); וראו תקציר של יום עיון שנערך בנושא במרכז הבינתחומי בהרצלייה: אור הירשאוגה "לא בכדי רוב המדינות לא מחזיקות במאגר" The Marker 12.8.2009 it.themarker.com/tmit/article/7711 (נבדק לאחרונה ב-5.12.2012).

חבר מפלגת האופוזיציה (קדימה).⁹⁸ במסגרת הפשרה, שאושרה על ידי ראש הממשלה בנימיין נתניהו, הוסכם על הקמתו של מאגר "פיילוט", אשר ההצטרפות אליו רצונית, לתקופת ניסיון של שנתיים.⁹⁹

אם וכאשר יידון הנושא בבג"ץ, מעניין יהיה לראות את עמדתו של בית המשפט העליון בסוגיות החוקתיות המתעוררת לנוכח דבר החקיקה "על תנאי".¹⁰⁰ זאת, בעיקר נוכח העובדה שההחלטה שיש לקבל לאחר תקופת התנאי בת השנתיים: האם התנאי התקיים (כך שהחוק ייכנס לתוקף) אם לאו (שאז יבוטל המאגר), מופקדת בידי של השר הממונה על המנגנון הביורוקרטי המיישם את החוק. ודוק: אין מדובר בסמכות של שר לקבוע את מועד כניסתו של חוק, אלא בסמכות מהותית להחליט אם החוק ייכנס לתוקף ובאיזה היקף.¹⁰¹ סמכות כזאת לא הופקדה בידי שר באף דבר חקיקה אחר.¹⁰²

98 שמוליק שלח ואדריאן פילוט "הלחץ עבד: ההצבעה על חוק המאגר הביומטרי נדחתה בשבוע" גלובס 16.11.2009 www.globes.co.il/news/article.aspx?did=1000514292 (נבדק לאחרונה ב-5.12.2012): "השר מיכאל איתן אמר בתגובה: 'אני מקווה שהדחייה תוביל לבחינה מחודשת של המהלכים להקמת המאגר הביומטרי השנוי במחלוקת. זו הוכחה שדעת הקהל יכולה להשפיע ואני מקווה כי דחייה זו תאפשר לאזרחי ישראל להנות מתועודות זהות ודרכונים חכמים ללא הסיכונים שבהקמת מאגר ביומטרי'. יו"ר הכנסת ראובן ריבלין הביע ביקורת ביחס לאופן שבו קודמה הצעת החוק, ואמר כי 'הדיונים בהצעה לא מוצו בהתחשב בסוגיות המורכבות וכבדות המשקל שכרוכות בה ובהשלכותיה על זכויות הפרט וצנעת חייו'. לדברי ריבלין, ניתן היה לקיים את הדיונים בוועדה באופן מעמיק ויסודי יותר, תוך מתן שימוע רחב להתנגדויות ולהסתייגויות מההלך. ריבלין אמר כי 'הדיון בוועדות הכנסת אינו מספתיים, ואין לשוות לו רושם כזה אפילו למראית עין'; ראו גם אהוד קינן "השר איתן: לעצור את המאגר הביומטרי" Ynet 18.7.2009 www.ynet.co.il/articles/0,7340,L-3748374,00.html (נבדק לאחרונה ב-5.12.2012): "השר מיכאל איתן יוצא נגד החוק שיחייב את אזרחי ישראל לתת טביעות אצבע למאגר שתקים המדינה: 'הליך החקיקה אינו ראוי, צריך לעצור את ההירה אל המאגר'".

99 יהונתן לייס "מסתמן: ועדת השרים תידחה את הדיון על הקמת מאגר ביומטרי בשנתיים" הארץ news.walla.co.il/?w=/1609329.17.11 (נבדק לאחרונה ב-5.12.2012). ראו הוראות הצו, ובפרט סעיף 3(ב) הקובע כי "בטרם ביצוע אימות או נטילה [של אמצעים או נתונים ביומטריים], ימסור עובד רשות האוכלוסין לתושב טופס הסכמה, הערוך לפי הנוסח שבתוספת, עליו יחתום התושב ובו יביע הסכמתו המפורשת לנטילת אמצעי זיהוי ביומטריים, הכללת האמצעים או הנתונים הביומטריים של התושב במאגר הביומטרי, ושימוש בהם לפי הוראות החוק וצו זה (להלן – טופס הסכמה)".

100 כאמור לעיל, בעניין נהון לא דן בג"ץ לגופן בטענות העותרים, אלא דחה את העתירה כמוקדמת.

101 ס' 41(5) ו-41(6) לחוק.

102 ראו גם עומר טנא "ההליך המוזר של החוק הביומטרי: בפעם הראשונה הכנסת מאצילה סמכויות חקיקה לשר הפנים" The Marker 9.6.2011 www.themarker.com/law/1.653266 (נבדק לאחרונה ב-5.12.2012).

לדעתי, הקניית הסמכות לשר לקבוע אם יחול החוק, ואם כן – באיזה היקף, פוגעת בכלל ההסדרים הראשוניים הנובע מעקרון הפרדת הרשויות.¹⁰³ כפי שהבהיר הנשיא ברק בפרשת ועדת המעקב העליונה, עקרון הפרדת הרשויות מחייב ביזור של סמכויות: "המחוקק יחוקק; המבצע יבצע; השופט ישפוט". במקרה זה, לא זאת בלבד שסמכויות מעין-חקיקתיות מוענקות לשר, אלא שהדבר נעשה בהקשר של חוק בעל השפעה מהותית על זכויות אדם, המציב לכל הדעות סיכונים משמעותיים לפרטיות אזרחי ישראל ולביטחונם.¹⁰⁴ עקרונות המשפט החוקתי והמנהלי מחייבים כי החלטות מסוג זה תהיינה שמוורות לרשות המחוקקת. לדברי הנשיא אהרן ברק, "מעליונותה של הכנסת מתבקש שההכרעות החשובות והעקרוניות למהות המשטר ייעשו על-ידי הכנסת ולא על-ידי הרשויות האחרות. זאת סמכות המיוחדת לכנסת. סמכות זו – חובה בצדה. על הכנסת להגשים סמכות זו בעצמה, ואין היא יכולה [...] להעביר סמכות זו לזולתה".¹⁰⁵

זאת ועוד: עקרון חוקיות המנהל מחייב כי משניתנה לרשות מנהלית בחקיקה הסמכות לקבוע הסדרים משניים, לא תהא ההסמכה רחבה ובלתי-מוגבלת, אלא כזאת הקובעת גם עקרונות הפעלה ואמות מידה מנחות להפעלת שיקול הדעת. ככל שההסמכה רחבה וגורפת, כך גדל פוטנציאל הפגיעה בזכויות האדם, ועקרון שלטון החוק מתקיים רק במובנו הפורמלי.¹⁰⁶ עולה מכך כי סעיף 41 לחוק, המקנה לרשות המבצעת שיקול דעת נרחב בדבר תחולתו של הסדר ראשוני, חייב היה לפרט היטב את אמות המידה והשיקולים שהשר חייב

103 ראו דפנה ברק ארז **משפט מנהלי** א 99–98 (2010); כמו כן ראו בג"ץ 11163/03 **ועדת המעקב העליונה לענייני הערבים בישראל נ' ראש ממשלת ישראל**, 48 פס' 28 לפסק דינו של השופט חשין (פורסם בנבו, 27.2.2006) (להלן: פרשת **ועדת המעקב העליונה**): "הכנסת היא המוסמכת לקבוע, בחוקים, 'הסדרים ראשוניים' – הסדרים הקובעים את הנורמות העיקריות ואת אמות-המידה להפעלתן – בעוד אשר הממשלה מוסמכת, על דרך העיקרון, לקבוע – בתקנות למיניהן ובמעשים – 'הסדרים משניים' בלבד. ובלשון אחר: אין הממשלה ובנותיה מוסמכות לקבוע 'הסדרים ראשוניים' אלא על-פי המחוקק, מכוחו של חוק הכנסת".

104 בעניין הסמכות שהוענקה לשר הביטחון להעניק פטורים מחובת השירות בצה"ל, קבע בית המשפט העליון בבג"ץ 3267/97 **רובינשטיין נ' שר הביטחון**, פ"ד נב(5) 481, פס' 35, 39 לפסק דינו של הנשיא ברק (1998): "דחיית שירות לתלמידי ישיבה [...] צריכה להתקבל במסגרת הכרעה לאומית אשר הכנסת צריכה לקבל באשר לעמדתה של מדינת ישראל בסוגיה החברתית השנוי במחלוקת. [...] שיקול דעתו של שר הביטחון צריך להיות מופעל בסוגיות הפרטניות, במסגרת ההכרעה העקרונית שנתקבלה על ידי הכנסת. עליה להכריע בשאלה כדין. כך פועלת שיטת משפט הנאמנה להפרדת הרשויות".

105 אהרן ברק "הפרלמנט ובית-המשפט העליון – מבט לעתיד" **הפרקליט** מה 5, 7 (2000).

106 ברק ארז, לעיל ה"ש 103, בעמ' 98.

לשקול בטרם הכרעתו בדבר תחולת החוק. זאת, גם על מנת לאפשר להעמידם למבחן משפטי בבוא היום ובמידת הצורך.¹⁰⁷

בנוסף, בהתחשב בכך שעלויות יישומו של החוק עלולות להיות אדירות,¹⁰⁸ יהיה ודאי מי שיביע ספק לגבי ההיגיון הכלכלי שבבסיס אישורו של פרויקט לאומי חשוב בדרך של חוק "על תנאי". לדעתי, מהלך חקיקתי כזה תמוה, בעיקר לנוכח העובדה שאחד הנימוקים העיקריים להקמתו של המאגר הביומטרי במסגרת הקיימת (כמאגר של מידע ביומטרי גולמי ולא רק של תבניות) היה חוסר היעילות הכלכלית של החלופות. המדינה החליטה לדחות את האפשרות להקים מאגר של תבניות, שנזקו הפוטנציאלי לפרטיות ואבטחת המידע נמוך בהרבה מזה של המאגר הקיים, עקב החשש להיקשר עם ספק מסוים המספק את שירות ההפקה של התבניות הביומטריות מהמידע הגולמי. אלא שכעת מתברר כי ההשקעה האדירה בתשתיות הנדרשות ליישומו של החוק עלולה ממילא לרדת לטמיון אם לבסוף יוחלט שלא "להפעילו".

יצוין כי תכניתה של ממשלת אוסטרליה להנפיק בסוף שנות ה-80 של המאה הקודמת תעודות זהות ביומטריות לכלל האוכלוסייה, קרסה בעקבות כשלים טכניים במבנה החוק המסמיך, שכניסתו לתוקף הייתה תלויה בהתקנת תקנות שלעולם לא הותקנו.¹⁰⁹ עם זאת,

107 על אף האמור לעיל, בתי המשפט אישרו בעבר הסדרים ראשוניים שנקבעו על ידי מחוקק המושג. לניתוח נרחב בדבר התייחסות הפסיקה לאורך השנים לכלל ההסדרים הראשוניים ראו שם, בעמ' 138–135. עמידה דווקנית על חלוקת התפקידים בין הרשויות השונות נועדה להבטיח את הפיקוח של הכנסת על הרשות המבצעת ולהביא הסדרים ראשוניים לדיון ציבורי. יצוין כי לא פעם, עצם ההכרח להביא סוגיה להכרעה בכנסת גרם לכך שבמשך שנים לא נקבעה עמדה בנושא. ראו למשל נושא הפטור משירות צבאי לבני ישיבות. אמנון רובינשטיין וברק מדינה *עקרונות יסוד המשפט החוקתי של מדינת ישראל*, 163, 170 (2005); ראו גם בג"ץ 5100/94 *הועד הציבורי נגד עינויים בישראל נ' ממשלת ישראל*, פ"ד נג(4) 817 (1999) והדיון הציבורי שהתעורר בעקבותיו.

108 הערכות בדבר עלותו של הסדר דומה בבריטניה נעו בין 4.5 לבין 12 מיליארד ליש"ט (בין 7 לבין 19 מיליארד דולר). London School of Economics, *The Department of Information Systems, The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 11–12, 27.6.2005, available at is2.lse.ac.uk/idcard/identityreport.pdf (נבדק לאחרונה ב-5.12.2012). עם כניסתה של ממשלת השמרנים ב-2009, בוטלה התוכנית ליישום חוק המאגר הביומטרי באנגליה. David Meyer, *ID Cards, National Identity*. Register Scrapped, ZDNET UK, 12.5.2010, available at bit.ly/aCiesY (5.12.2012).

109 Graham Greenleaf, *Lessons from the Australia Card – Deux ex Machina?*, 3(6) COMP. L. & SEC. REP. 6, 6 (1988). "[T]he crucial clauses of the Bill [...] were all defined to commence operation 'on or after the first relevant day'. This 'first relevant day' was defined (cl 32) such that it could only be declared by regulations, and the

יובהר כי, לדעתי, גם ללא פגמים פרוצדורליים אלה, דינם של חלק מעיקרי החוק להיפסל לנוכח אי-עמידתם במבחנים המהותיים של פסקת ההגבלה. אפנה לדיון במבחנים אלה כעת.

2. תכלית ראויה: "הקמת מאגר"

פסקת ההגבלה קובעת כי אפשר לפגוע בזכות חוקתית אך ורק לשם הגשמת מטרות שיש בהן הצדקה מבחינה ערכית לפגיעה באותה זכות. "חקיקה הפוגעת בזכויות אדם תקיים את הדרישה בעניין 'תכלית ראויה', אם תכליתה של אותה חקיקה מעניקה צידוק מספיק לאותה פגיעה בזכויות אדם".¹¹⁰ כדי לברר אם החוק בא לשרת תכלית ראויה, יש להתחקות ראשית אחר מטרותיו. המטרה המוצהרת שעמדה בבסיס חקיקתו של החוק היא "להתמודד עם הבעיות החמורות שמולן ניצבת מדינת ישראל בשנים האחרונות בתחום מסמכי הזיהוי המנופקים בידי משרד הפנים, ובין השאר זיוף תעודות זהות, דרכון ותעודת מעבר [...] ניפוק תיעוד כפול לאותו אדם, ו'גניבת זהות' של אדם בידי אדם אחר תוך שימוש בתיעוד הרשום על שם האדם שממנו נגנבה הזהות... מטרת החוק המוצע לקבוע הסדרים אשר יאפשרו אימות זהות וזיהוי של תושבי ישראל תוך שימוש באמצעים ביומטריים ובנתונים ביומטריים שיופקו מהם, שייכללו במסמכי הזיהוי ובמאגר ביומטרי מרכזי, באופן שיקשה מאוד על זיוף התיעוד, ניפוק תיעוד כפול לאותו אדם ושימוש בזהות גנובה".¹¹¹

דא עקא, שאיסוף נתונים ביומטריים כלל אינו תורם למיגור התופעה של מניעת זיוף התעודות; לכל היותר הוא עשוי לסייע בשלב אימות זהותו של אדם הנושא את התעודה (האותנטית או המזויפת). במילים אחרות, אפשר היה ליצור תעודה חדשה שתהיה קשה מאוד לזיוף גם ללא מידע ביומטרי; ואפשר היה ליצור תעודת זהות הנושאת מידע ביומטרי

Government did not have the necessary majority in the Senate to prevent the Opposition parties disallowing any regulations which were made. The Opposition vowed that no 'first relevant day' would ever occur and that the Bill was 'stone dead'. In effect, if the Bill was passed, obtaining a Card would really be voluntary because no adverse consequences would attach to failure to hold one. The Government was hoist on its own petard"

110 בג"ץ 1661/05 המועצה האזורית חוף עזה נ' כנסת ישראל, פ"ד נט(2) 481, 548 (2005).

111 הצעת חוק הכללת אמצעי זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשס"ט-2009 (להלן: "הצעת החוק").

שתהיה קלה (יחסית) לזיוף.¹¹² זאת ועוד: גם אם היינו מקבלים את הצורך בהטענת מידע ביומטרי על התעודה למטרת שיפור איכותה, אין בכך כדי להסביר את הקמתו של מאגר ביומטרי מרכזי כדוגמת זה המוקם בסעיף 10 ואילך לחוק. אם כן, מדוע מוקם המאגר הביומטרי, ומהם המנגנונים שהוכנסו לחוק על מנת להבטיח את פרטיותם של האזרחים ואבטחת המידע שלהם?

סעיף 1 לחוק מגדיר באופן מפורש את מטרותיו. סעיפי מטרה אינם שכיחים בחקיקה הישראלית, ואפשר לשער שהשימוש בסעיף מטרה בחוק זה דווקא מעיד על הצורך שראה המחוקק להסביר את חשיבות הפרויקט הלאומי רחב ההיקף המושק באמצעותו. אולי גם צפה המחוקק את ההתמודדות עם תקיפת חוקתיותו של החוק בבג"ץ. סעיף 1(1) לחוק מבאר כי מטרת החוק לקבוע "הסדרים אשר יאפשרו זיהוי ואימות זהות של תושבי ישראל באמצעות הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים בתעודת הזהות ובמסמך נסיעה, באופן שימנע זיוף ושימוש בזהות אחרת". כפי שציינתי לעיל, המידע הביומטרי המוטמע בתעודה אינו מהווה ערובה נדרשת או מספיקה לאי-זיופה, אף שאין ספק כי הוא עשוי למנוע "שימוש בזהות אחרת". זאת, מאחר שאם ראובן יבקש להשתמש בתעודתו של שמעון, תתריע מערכת המבוססת על אימות זהות כי הצהרתו של ראובן שקרית.

סעיף 1(2) לחוק מציין כי מטרה נוספת של החוק היא "הקמת מאגר מידע ביומטרי שיכלול אמצעי זיהוי ביומטריים שניתלו לצורך שילובם במסמכי זיהוי כאמור בפסקה (1), וכן נתוני זיהוי ביומטריים שהופקו מהם, וקביעת השימושים המותרים במאגר כאמור לרבות בידי משטרת ישראל ורשויות הביטחון". מעניין כי המחוקק בחר לתאר את המאגר הביומטרי כמטרה בפני עצמה ולא כאמצעי להשגתה של מטרה אחרת, כגון מניעת הרכשה כפולה של תעודות זהות. לדעתי, ספק אם "הקמת מאגר מידע ביומטרי" מהווה "תכלית ראויה" המצדיקה כשלעצמה פגיעה בזכות יסוד חוקתית בהתאם לפסקת ההגבלה שבסעיף 8 לחוק-יסוד: כבוד האדם וחירותו (להלן: "חוק-היסוד"). צאו וראו: אילו מטרת החוק הייתה מצומצמת למטרה הנקובה בסעיף 1(1), כלומר לקביעת הסדרים שיאפשרו זיהוי ואימות זהות של תושבי ישראל באמצעות אמצעי זיהוי ביומטריים, אזי נראה היה שאין צורך בהקמתו של מאגר מידע ביומטרי, שכן אפשר להשיג את התוצאה המבוקשת גם ללא מאגר מרכזי. ולחלופין, אם מטרת החוק היא "הקמת מאגר מידע ביומטרי", ספק אם מדובר במטרה ראויה המצדיקה פגיעה בזכות יסוד חוקתית.

הייתכן כי המטרה המרכזית (האמתית) של החוק היא דווקא זאת המוצנעת בסיפה לסעיף 1(2), קרי: "קביעת השימושים המותרים במאגר כאמור לרבות בידי משטרת ישראל ורשויות הביטחון"? לדעתי, אילו המטרות הביטחוניות-משטרתיות עמדו בראש מעייניו

112 ראו עמדת מבקר המדינה בדו"ח לשנת 2008, לעיל ה"ש 74; וכן ביהם, לעיל ה"ש 161.

של המחוקק, היה עליו להציג זאת כך במפורש. אדרבה, גישה זאת מתחייבת גם מפרשנות מילולית-לשונית של הסעיף. היעלה על הדעת שמטרתו העיקרית של החוק הוצנעה בדחילו ורחימו בסיפה של סעיף 1(2), תוך שימוש בוי"ו החיבור וב"לרבות" ("וקביעת השימושים המותרים במאגר כאמור לרבות בידי משטרת ישראל ורשויות הביטחון"), בעוד שהמטרה המפורטת ברישה של אותו סעיף ("הקמת מאגר מידע ביומטרי שיכלול אמצעי זיהוי ביומטריים") אינה אלא מטרה משנית? מבנה לשוני-תחבירי כזה, בבחינת זנב (הסיפה) המקשקש בכלב (הרישה), מעורר תמיהה.

אין ספק כי מטרת ביטחוניות-משטרתיות חשובות ולגיטימיות במסגרת משטר דמוקרטי, תואמות את אופייה של מדינת ישראל כמדינה יהודית ודמוקרטית, ואף זוכות למשקל מיוחד בהחלטותיו של בית המשפט העליון הרואה בה "דמוקרטיה מתגוננת".¹¹³ כך, למשל, קובע הנשיא ברק, כי "התגוננותה של הדמוקרטיה אינה שוללת ממנה את אופייה הדמוקרטי. ההתגוננות, היא השומרת על אופייה הדמוקרטי. זאת, בשל האיזון הראוי שנמצא בין ביטחון לכבוד האדם וחירותו".¹¹⁴ ואולם, ככל שמדובר במאגר הביומטרי, כלל לא ברור מהן אותן מטרת ביטחוניות-משטרתיות, מה היקפן, מה גבולותיהן, ומדוע בדיוק זקוקות רשויות הביטחון למידע? ראשית, ספק רב אם המשטרה תוכל להשתמש במאגר סריקות האצבע לצורך פענוח פשעים, שכן התאמה לטביעות אצבע שנותרו בזירה מחייבת שימוש בטכניקה שונה (גלילת כל עשר האצבעות) להבדיל מתמונת שתי טביעות האצבעות המורות הנרכשת בסביבה סטרילית.¹¹⁵ שנית, חזקה שאילו המשטרה ושיירות הביטחון היו מבקשים להקים מאגר מידע לאומי של טביעות אצבע ותמונות פנים של כל אזרח, כולל מי שמעולם לא נחשד בביצוע עברה או בפעילות החותרת תחת ביטחון המדינה, הייתה בקשתם מסורבת על ידי המחוקק או למצער נפסלת על ידי

113 ע"ב 1/65 ירדור נ' יושב-ראש ועדת הבחירות המרכזית לכנסת השישית, פ"ד יט (3) 363, פס' 6 לפסק דינו של השופט זוסמן (1965).

114 בג"ץ 7052/03 עדאלה המרכז המשפטי לזכויות המיעוט הערבי נ' שר הפנים, פ"ד סא (2) 202, פס' 82 לפסק דינו של הנשיא ברק (2006).

115 ראו למשל דבריו של רפ"ק דוד אטיאס, ראש מעבדת השוואת טביעות אצבע במשטרת ישראל, במסגרת הדיון בוועדה: "לגבי מאגר טביעות אצבע. כמונחים הפליליים של מאגרי טביעות אצבע, אם אני לוקח רק את תמונות טביעות האצבע וגם את תבניות טביעות האצבע בלבד, ללא כל נתוני זיהוי אחרים, אי-אפשר לעשות איתם כלום. ממש לא ניתן לעשות עם זה כלום. אחרי הוועדה אני מוכן לתת את טביעת האצבע שלי למי שרוצה. ממש לא ניתן לעשות עם זה כלום". פרוטוקול ישיבה מס' 1 של וועדה משותפת – מדע ופנים, הכנסת ה-18, 55 (30.6.2009).

בג"ץ¹¹⁶ מדינות דמוקרטיות אינן נוהגות להתייחס לכל אזרחיהן כחשודים בביצוע עברות או פעולות טרור. גישה כזאת אינה ראויה, אינה מידתית ואינה הולמת את ערכיה של מדינת ישראל כמדינה יהודית ודמוקרטית, ולכן היא פסולה על פי כל אחד מהמבחנים של פסקת ההגבלה. כך, למשל, פסל בית הדין האירופי לזכויות אדם בשטרסבורג בעניין *Marper* את חוקיותו של מאגר דגימות דנ"א שהקימו רשויות הביטחון בבריטניה, וקבע כי אין בסיס להחזקת מידע מסוג זה על מי שהיו חשודים בעברות אך זוכו מכל אשמה.¹¹⁷ שלישיית, המטרות הביטחוניות-משטרתיות של הקמת המאגר הביומטרי לא הובהרו דיין גם במסגרת הדיון הציבורי הער שנסוב סביב חקיקת החוק. כך, למשל, הדגישה יועצת משפטית של המשרד לביטחון פנים באחד מדיוני הוועדה המשותפת, בתגובה לטענה שהמשטרה היא שחפצה בהקמת המאגר הביומטרי: "למה משטרת ישראל? זאת הנחה לא נכונה. דרישת המאגר היא מתוך זה שמשרד הפנים החליט שהדבר הזה נדרש לו. ככל שיהיה מאגר, בהחלט המשטרה תרצה להתחבר אליו אבל ההנחה שמשטרת ישראל דרשה את זה, היא לא הנחה נכונה."¹¹⁸ ובהמשך: "האפשרות של המשטרה להשתמש במאגר היא באחד משני מצבים מאוד קיצוניים. השימוש הראשון הוא במצבים בהם יש בפנינו אדם או גופה שנבקש לקבל רק את שמו של האדם. אותו אדם לא יכול להזדהות, אין לו תעודה, הוא לא רוצה להזדהות ואנחנו נבקש לדעת את השם שלו ולא נקבל שום מידע אחר מהמאגר."¹¹⁹ השימוש השני, היא ממשיכה, הוא במצבים שבהם "האיש מעביר את התעודה שלו מול המכשיר, רואים שאין התאמה בין האיש לבין טביעת האצבע לתעודה שלו."¹²⁰ האומנם התכוון המחוקק להקים מאגר ביומטרי של כלל אזרחי המדינה, המטיל צל כבד של סכנות אבטחה ופרטיות (שלא לדבר על עלויות כספיות), לצורך אחד מאותם "שני מצבים מאוד קיצוניים"?

אם כן, לא נותר לנו אלא לחזור למטרה העיקרית המפורטת ברישה לסעיף 1(2) לחוק ("הקמת מאגר מידע ביומטרי שיכלול אמצעי זיהוי ביומטריים"), שעליו נסמכת הסיפה

116 השוו חוק סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף ונטילת אמצעי זיהוי), התשנ"ו – 1996, המאפשר לשוטרי ליטול טביעת אצבע או דגימה ביולוגית ממי שחשוד, נאשם או הורשע בעברה המפורטת בתוספת לחוק.

117 עניין *S and Marper v. United Kingdom*, לעיל ה"ש 16.

118 דבריה של נצ"מ איילת אלישר, משנה ליועץ המשפטי, המשרד לביטחון פנים, פרוטוקול מס' 2 משיבה משותפת של ועדת המדע והטכנולוגיה וועדת הפנים והגנת הסביבה, הכנסת ה-18, 11 (7.7.2009); ראו גם דבריו של יורם אורן, יועץ של משרד הפנים, שם, בעמ' 19: "בפעם הקודמת דובר על היכולת של המשטרה להסתייע במידע כזה ולכלל הדעות היכולת היא יכולת מוגבלת, אם כי היא לא אפסית".

119 דבריה של נצ"מ אלישר, לעיל ה"ש 118, בעמ' 21.

120 שם.

הביטחוני-משטרית ("וקביעת השימושים המותרים במאגר כאמור לרבות בידי משטרת ישראל ורשויות הביטחון"). ההצגה של המאגר הביומטרי כמטרה בפני עצמה בסעיף 1(2) לחוק משקפת ניתור דיאלקטי שנחזה להיות צנוע, אך למעשה מהווה קפיצה נחשונית בין מערכת שתפקידה לאמת זהות ולמנוע שימוש בתעודות מזויפות (קרי: מטרתו המוצהרת המקורית של המחוקק) לבין מערכת שמטרתה זיהוי ומעקב. לכן, או שהקמת המאגר הביומטרי היא מטרה בפני עצמה, שאז החוק ככל הנראה אינו חוקתי ואינו עומד בפסקת ההגבלה; או שהקמת המאגר הביומטרי אינה מטרה עצמאית, שאז ספק אם ניתן להצדיקה לנוכח המטרה המוצהרת של החוק שאותה אפשר להשיג גם ללא מאגר מרכזי.

3. מידתיות: עלייתו ונפילתו של "המאגר המעומעם"

גם אם החוק עומד במבחן "התכלית הראויה" (ולא בטוח כלל ועיקר כי כך הוא), ספק אם הוא מקיים את מבחן המידתיות החוקתי. מבחן המידתיות מורכב משלושה מבחני משנה: מבחן הקשר הרציונלי בין מטרת החוק לבין האמצעים שנבחרו על ידו; מבחן האמצעי שפגיעתו פחותה; ומבחן התועלת מול הנזק (מבחן המידתיות במובן הצר).¹²¹

(א) מבחן הקשר הרציונלי

האם האמצעי שהחוק נקט, קרי: הקמת מאגר ביומטרי המחזיק במידע גולמי על כלל האוכלוסייה, אכן יהא בכוחו להגשים את המטרות הראויות שביסוד החוק? חשוב להבחין מבחינה מושגית בין מטרות החוק לבין מטרות המאגר. אמנם הקביעה בסעיף 1(2) לחוק כי מטרתו של החוק היא "הקמת מאגר מידע ביומטרי" מעמעמת לכאורה את ההבחנה; אולם אפשר (וראו) היה לקיים את מטרותיו הנוספות של החוק גם ללא הקמתו של מאגר מרכזי. נתעלם לרגע אפוא מהמטרה המעגלית, המגלמת כשל לוגי, שבסעיף 1(2) לחוק, ונתרכז במטרה הראשונית, המפורטת בסעיף 1(1) לחוק: קביעת הסדרים שיאפשרו זיהוי ואימות זהות של תושבי ישראל באופן שימנע זיוף ושימוש בזהות אחרת.

ראינו כי המאגר הביומטרי כלל אינו נחוץ לצורך "אימות זהות של תושבי ישראל [...] באופן שימנע זיוף". ודוק: המדינה יכולה הייתה למנוע זיופים באמצעות הנפקה של תעודות זהות חדשות שיהיו קשות מאוד לזיוף גם ללא מידע ביומטרי, קל וחומר שללא מאגר ביומטרי מרכזי. ואילו אימות זהות אפשר היה להשיג באמצעות הטבעת המידע

121 ראו למשל בג"ץ 6427/02 התנועה לאיכות השלטון נ' הכנסת, פס' 62–57 לפסק דינו של הנשיא ברק (פורסם בנבו, 11.5.2006); ראו גם דליה דורנר "מידתיות" בני סברה ספר ברנזון כרך שני 281 (אהרן ברק וחיים ברנזון עורכים, 2000).

הביומטרי על התעודות עצמן, מבלי לאגור אותו במאגר מרכזי. אדרבה, חקיקת החוק והתלייתו למשך תקופת מבחן ארוכה רק דוחה את הנפקתן של תעודות זהות חדשות ועמידות יותר, ומכשילה את קידום מטרתו הראשית (המוצהרת) של החוק. מבקר המדינה בדו"ח השנתי ל-2010 כותב מפורשות שמשרד הפנים פועל זה כ-15 שנים לקידום הנפקתה של תעודת זהות חכמה כדי להנהיג תעודה בעלת עמידות משופרת, וכי הטיפול בנושא זה נקלע ל"מצב בלתי נסבל" של העדר פתרון. לדברי המבקר, לשם מניעת זיוף תעודות זהות – התכלית המוצהרת של משרד הפנים שהוגדרה צורך לאומי חיוני, יש "[ל]נקוט לאלתר מהלכים להנפקתן של תעודות זהות חכמות לכלל האוכלוסייה עוד קודם שייכללו בהן אמצעי הזיהוי הביומטריים, ובכך יקשה את זיופן ויגביר את מהימנות השימוש בהן".¹²² בעניין זה יפים דבריו של השופט אור בפרשת תחנות הרדיו הפיראטיות: "מכל זווית שלא נתבונן על נוסח התיקון לחוק, מתבקשת המסקנה כי האמצעי שנקבע בו אינו מוביל להגשמת התכלית החקיקתית האמורה. אין מתאם אמתי כלשהו בין התכליות הנטענות על ידי המשיבים של התיקון לחוק לבין האמצעים שנקבעו בו לצורך הגשמת תכלית זו".¹²³ אם כן, מדוע מוקם המאגר הביומטרי? על פי דברי ההסבר להצעת החוק, המטרה העיקרית של המאגר היא "לאפשר עריכת השוואה ביומטרית בין האמצעים הביומטריים שניטלו מתושב והנתונים שהופקו מהם לבין אלה הכלולים במאגר [...] לשם מניעת הנפקת תיעוד כפול לאותו אדם". כלומר, המאגר נועד למנוע מאזרחים "הרכשה כפולה" של תעודת זהות או דרכון. כמו כן, מאפשר המאגר את זיהוי של אדם אשר אין בידו מסמך זיהוי או שהתעורר ספק לגבי זהותו לאחר בדיקה מול מסמך הזיהוי שהוא נושא; ומקל על זיהוי של נפגעים וחללים עקב פיגוע המוני או אסון טבע. בהמשך מפורטת מטרה נוספת, שדומה שוב כי הוצנעה מעט במסגרת דברי ההסבר הארוכים: "הקמת המאגר תאפשר גם להסתייע בו לצורך גילוי, חקירה או מניעה של עבירות מסוג פשע או עוון, לצורך זיהוי ותפיסה של עבריינים שעברו עבירות כאמור, ולצורך סיכול פיגועים והגנה מפני פגיעה בחיי אדם".

מניעה של הרכשה כפולה היא כמובן מטרה ראויה, והמאגר אכן מקדם מטרה זאת, אך כפי שאסביר בהמשך, ספק אם הקמתו לצורך זה עומדת במבחן האמצעי שפגיעתו פחותה ובמבחן התועלת מול הנזק.¹²⁴

122 משרד מבקר המדינה, דו"ח שנתי 61 לשנת 2010 ולחשבונות שנת הכספים 2009 (הדו"ח המלא), חלק שני 1165–1197, 1197 (2011).

123 בג"ץ 1030/99 אורון נ' יושב ראש הכנסת, פ"ד נו(3) 640, פס' 37 לפסק דינו של השופט אור (26.3.2002); וראו גם אהרן ברק מידתיות במשפט: הפגיעה בזכות החוקתית והגבלותיה 374–375 (2010).

124 ראו דיון להלן בפרק 3(ב).

לבסוף, חשוב להדגיש כי העברות המידע למשטרה ולרשויות הביטחון על פי סעיפים 17–18 ו־21–22 לחוק **חורגות מהמטרה הראשונית** שלשמה נחקק החוק. לכן יש לראות בהן את תחילתה של תופעת "זחילת הפונקציות" הפוגעת מעבר לנדרש בזכות היסוד החוקתית לפרטיות. כאמור לעיל, ספק אם המחוקק היה מכשיר חקיקתו של חוק שמטרתו העיקרית להקים מאגר טביעות אצבע של כל אזרחי המדינה למטרות אכיפת חוק. אם חוק מסוג זה אינו ראוי לעבור בשער הכניסה הראשי, לא ראוי לדעתי להכניסו באמצעות "הדלת האחורית", כשהוא מסתתר מאחורי טיעונים בדבר תעודות מזויפות או הרכשה כפולה. חלק מטיעונים אלה אינו רלוונטי להקמת המאגר הביומטרי, וחלקם האחר אינו מספיק כדי להצדיקו. הניסיון מלמד כי התופעה של זחילת פונקציות אינה זרה לתחום מאגרי המידע הממשלתיים הרגישים בישראל, ואילו כשמדובר במאגר הביומטרי החלה זחילת הפונקציות כבר במסגר לשון החוק עצמו.¹²⁵

(ב) מבחן האמצעי שפגיעתו פחותה

קיימים אמצעים חלופיים להתמודד עם בעיית ההנפקה הכפולה, כגון תשאול מי שמבקש להנפיק תעודה על ידי פקיד משרד הפנים בהתאם למידע שעליו המוחזק במרשם האוכלוסין או במאגרי מידע נוספים של המדינה. המדינה הייתה ערה להשגות אלה, וציינה בדבריה ההסבר כי גם לחלופות אלו יש לעתים מחיר של פגיעה בפרטיות, מאחר שהמשמעות עשויה להיות הצלבת נתונים עם מאגרי מידע חיצוניים; בדיקה מול פרטים אישיים הנמצאים במאגרי מרשם האוכלוסין בלבד, עלולה להביא לתוצאות שאינן חד־משמעיות (מאחר שתושבים עשויים לשכוח פרט מסוים הרשום לגביהם במרשם האוכלוסין, גם שלא בכוונת זדון). דא עקא, המאגר אינו פותר את הצורך לזהות את האזרחים כולל באמצעות בדיקה של פרטים אישיים בשלב ההרכשה הראשונה של התעודה הביומטרית; זאת, על מנת לוודא שמי שמתייצב במרכז ההנפקה ומוסר את נתוניו הביומטריים וטוען שהוא ראובן, הוא אכן ראובן ולא שמעון.¹²⁶ המאגר הביומטרי אפוא מקל על הנפקת התעודות בעיקר

¹²⁵ ראו דיון בחוק איסור הלבנת הון, לעיל ה"ש 62–66, והטקסט הנלווה.

¹²⁶ תק' 1 לתקנות קובעת הליך תשאול מפורט שעל כל אזרח לעבור בטרם תונפק בעבורו תעודה: "לאחר אימות הנתונים שבמסמך הזיהוי מול מרשם האוכלוסין, עובד רשות האוכלוסין ישאל את התושב סדרת שאלות מזהות המקיימות את התנאים הבאים (להלן – הליך תשאול): (1) מערכת ממוכנת בחרה בהן באופן אקראי, מתוך מאגר שאלות; (2) הן מבוססות על מידע הקיים במרשם האוכלוסין או על מידע שהתקבל מגוף ציבורי (...); (ג) אם נמצאה התאמה מספקת בין התשובות שנתן התושב לבין המידע המצוי במערכת המחשב, ייטול עובד רשות האוכלוסין אמצעי זיהוי ביומטריים מהתושב; (ד) במקרה שלא התקבלה התאמה מספקת כאמור, יועבר המשך הליך הבדיקה לידי בעל תפקיד נוסף שהוכשר לכך (להלן – פקיד קו

בשלבם מאוחרים יותר של הנפקת תעודות חלופיות למי שאיבד את תעודתו המקורית.¹²⁷ יש לזכור, כי יעילות זאת תישא תו מחיר כבד לפרטיות האזרחים, אולי כבד מנשוא אם חלילה ידלוף מידע מהמאגר.¹²⁸

אפשר היה לצמצם את הפגיעה בפרטיות באמצעות הקמתו של מאגר הכולל תבניות ביומטריות בלבד ("נתוני זיהוי ביומטרי" בלשון החוק) להבדיל מהמידע הביומטרי הגולמי ("אמצעי זיהוי"). מאגר תבניות כזה היה מציב סכנות פחותות בהרבה לפרטיות האזרחים ואבטחת המידע עליהם. זאת, מאחר שאין אפשרות לשחזר מידע גולמי (כלומר תמונת פנים או טביעת אצבע) מן התבניות, כך שאם הן נופלות לידי גורמים לא מורשים, אלה לא יוכלו להשתמש במידע לרעה.¹²⁹ גם אפשרות זאת נדחתה על ידי המדינה, שציינה בדברי ההסבר,

שני; (ה) פקיד קו שני ישאל סדרה נוספת של שאלות מזהות, ובכלל זה חזרה על שאלות שנשאלו למקרה של אי-התאמה מטעמים טכניים בלבד; (ו) ככל שלאחר סדרת השאלות הנוספת, לא התקבלה התאמה מספקת בין התשובות שנתן התושב לבין המידע המצוי במערכות המחשב, רשאי פקיד קו שני להפסיק את הליך הבדיקה ולדרוש מהתושב להביא מסמך או אמצעי זיהוי נוסף (...); (ז) לא יינטלו אמצעי זיהוי ביומטריים מתושב ולא יונפק מסמך זיהוי ביומטרי, אלא לאחר השלמת הליך וידוא ואימות זיהוי התושב.

127 תק' 4 לתקנות מבהירה: "תושב המבקש הנפקה חדשה של מסמך זיהוי, לאחר שהונפק לו בעבר מסמך זיהוי עם אמצעים או נתונים ביומטריים על פי תקנות אלה, יידרש לבצע הליך זיהוי מלא ונטילה נוספת של אמצעים ביומטריים, לפי הוראות תקנות אלה; ואולם לא יידרש הליך תשאול במקרה שבו קיים בידי התושב מסמך זיהוי ובו אמצעים או נתונים ביומטריים ונמצאה התאמה בין אמצעי הזיהוי הביומטריים שניטלו ממנו לבין האמצעים או הנתונים הביומטריים שבמסמך הזיהוי, אלא אם כן הורה ראש רשות האוכלוסין כי נדרש הליך תשאול" (ההדגשה שלי – ע.ט.).

128 בבג"ץ 8070/98 האגודה לזכויות האזרח בישראל נ' משרד הפנים, פ"ד נח (4) 842, פס' 9 לפסק דינה של השופטת דורנר (פורסם בנבו, 10.5.2004) דוחה השופטת דורנר (בדעת רוב) את עמדתו של השופט גרוניס, שלפיה יש בשיקולים של יעילות כלכלית כדי להצדיק את הפגיעה בפרטיותם של אזרחים (באותו מקרה באמצעות העברות מידע בין גופים ציבוריים). השופטת דורנר כותבת: "אף בהנחה – שאיני מקבלת – כי הפגיעה בפרטיות הנוצרת כתוצאה מהתחברות גוף פרטי, דרך קבע, למאגר מידע ממשלתי היא זניחה, הרי שאין בידי להסכים לגישת חברי, הפוטר פגיעות קלות בזכויות-אדם מתחולת פסקת ההגבלה. מושכלות ראשונים הם, כי ניתן לפגוע בזכויות-אדם, ובכללן הזכות לפרטיות, רק אם הפגיעה מקיימת את כל ארבעת היסודות המצטברים הקבועים בפסקת ההגבלה, לרבות היות הפגיעה בחוק או לפי חוק, מכוח הסמכה מפורשת בו. דרישת החוקיות היא איפוא דרישה עצמאית, המצטברת לשאר הדרישות – הלימת ערכי המדינה, תכלית ראויה, ומידתיות. בכך שהפגיעה היא קלה, אין כדי לשחרר מדרישת החוקיות".

129 על הקושי לשחזר מידע גולמי מתבניות ביומטריות ראו Andy Adler, *Biometric System Security*, בתוך HANDBOOK OF BIOMETRICS, לעיל ה"ש 12, בעמ' 380–401. לאחרונה הראו מדענים כי בנסיבות מסוימות אפשר בכל זאת לעשות כן. ראו Karl Kümmel & Claus Vielhauer, *Reverse-Engineer Methods on a Biometric Hash Algorithm for Dynamic*

כי לחלופה זאת חסרונות אחדים; כגון היעדר תקן אחיד לגבי מיצוי תבניות ביומטריות מהמידע הגולמי, כך שהתוצאות שונות מאלגוריתם לאלגוריתם ומספק לספק; ומכאן ששמירת תבניות בלבד, על פי הטיעון, תצמיח תלות של המדינה בספק יחיד "דבר שאינו נכון מקצועית וכלכלית". כמו כן, ציינה המדינה כי קיימת כיום היכולת "באמצעים מסוימים ובמצבים מסוימים" לשחזר את המידע הגולמי גם מתוך נתוני התבנית; וכי לגבי תווי הפנים, נדרש בכל מקרה לשמור את המידע המקורי כדי להציגו לבדיקה חזותית. האם די בנימוקים אלה כדי להצדיק פתרון מרחיק לכת כדוגמת הקמתו של המאגר הביומטרי? הנימוק הראשון, שלפיו המדינה חוששת מתלות בספק יחיד, כלכלי באופיו, ונראה כי ניתן לפתרו באמצעים חוזיים. הנימוק השני, שלפיו "באמצעים מסוימים ובמצבים מסוימים" אפשר יהיה לשחזר את המידע הגולמי באמצעות התבנית ודאי לא מצדיק אגירה של המידע הגולמי. ואילו הנימוק האחרון, שלפיו התמונה המקורית נדרשת לצורך בדיקה חזותית לא ממוכנת על ידי אדם, אינו מצדיק שימור של התמונה באיכות הביומטרית, אלא לכל היותר שימור של תמונת פנים באיכות פחותה, כפי שיוסבר להלן.¹³⁰

במסגרת הדיונים על חקיקת החוק, הציע פרופ' עדי שמיר, חתן פרס ישראל ומחשובי הקריפטולוגים (מומחי תורת ההצפנה) בעולם, ליישם מנגנון שיאפשר ליהנות ממטרתו העיקרית של החוק – מבלי לאפשר "זחילת פונקציות" ושימושים שניוניים או לא מורשים במידע.¹³¹ לדברי פרופ' שמיר, יש לעמעם את הקשר בין נתוניו הביומטריים של אדם לבין זהותו, למשל באמצעות חלוקת אזרחי המדינה לקבוצות אקראיות של 1000 איש בכל קבוצה והכנסת נתונייהם הביומטריים של כל 1000 אזרחים ל"סל" משותף אחד. אם ראובן,

Handwriting, Proceedings of the 12th ACM Workshop on Multimedia and Security (2010). בתכתובת עם ארנון הראל, מומחה למערכות מידע ביומטריות, נמסר לי כי "התשובה העקרונית והפרקטית לכך היא שכיום לא ניתן לשחזר את המידע הגולמי (במילים אחרות – התמונה) מהתבנית שבה היא נשמרה. זאת בהסתייגות מסוימת שלאחרונה, במסגרת מחקרים במספר מכוני מחקר ואוניברסיטאות, הצליחו לפתח אלגוריתמים מאד מורכבים שבעזרתם ניתן לשחזר באופן סינטטי מתוך התבנית את המידע הגולמי. אין ספק שכרגע הדבר אינו פרקטי ליישום אבל מי יודע – אולי בעתיד (הלא רחוק) זה יהיה פרקטי [...] כל הנאמר כאן נכון לטביעות אצבע. לגבי טכנולוגית זהו פנים הקביעה נכונה שבעתיים – לא ניתן לשחזר את המידע הגולמי מהתבנית בה הוא נשמר בגלל סוג המידע המשמש ליצירת התבנית שאינו נגזר מ'תמונה' אלא מ'תכונה' (למשל – המרחק בין שני האישונים)". ראו גם, Arnon Harel, *Biometrics, Identification and Practical Ethics, in Identity, Security and Democracy: the Wider Social and Ethical Implications, in NATO SCIENCE FOR PEACE AND SECURITY* .SERIES- E: HUMAN AND SOCIETAL DYNAMICS 69 (Emilio Mordini ed., 2009)

130 ראו להלן, ה"ש 150 והטקסט הנלווה.

131 ניב ליליאן "פרופ' שמיר מציע: מאגר טביעות אצבע מעומעם" Ynet 13.8.2009 www.ynet.co.il/articles/0,7340,L-3761566,00.html (נבדק לאחרונה ב-5.12.2012).

שכבר רכש תעודה, יתייצב בשנית במרכז ההנפקה, תזזה המערכת את הכפילות ותסרב לבקשתו; ואולם, אם טביעות האצבע של ראובן יימצאו בזירת פשע, תידרש המשטרה לבצע פעולות משלימות במסגרת החקירה על מנת לקשור בין הנתונים לבין זהותו, שכן בשלב הראשוני לכל היותר תדע שטביעת האצבע שייכת לאחד מתוך 1000 האזרחים שבקבוצה. פרופ' שמיר מראה, כי במידת הצורך תוכל המשטרה לזהות את החשוד, שכן באמצעות פעולות חקירה פשוטות המבוססות על מידע שקל להשיג (כגון מין החשוד או גילו המסוער) אפשר יהיה לצמצם, ברוב המקרים, את קבוצת החשודים לכדי קבוצה שניתן לתשאל אותה אישית. עם זאת, יניאו עלויות נוספות אלה את המשטרה מפני יציאה ל"מסע דיג" של חשודים בעקבות שימוש בנתונים ביומטריים. הצעתו של פרופ' שמיר חשובה במיוחד מבחינת היבטי אבטחת המידע, שכן אם ידלוף מידע מהמאגר, לא יוכלו הגורמים שהמידע נפל לידיהם להשתמש בו. זאת, מאחר שהמידע יישאר בלתי מזוהה. אף כי אפשר היה להשתמש בהצעתו של פרופ' שמיר במסגרת סמכותו של שר הפנים להתקין תקנות על פי סעיף 10(ד) לחוק, החליטה הממשלה שלא לאמץ את המלצותיו, ולהקים במקום זאת מאגר ביומטרי המאפשר זיהוי חד-חד-ערכי.¹³² הדיון באישור התקנות והצו בוועדה המשותפת, מעלה כי הסיבה העיקרית לדחייתה של הצעת שמיר, היא כי ההצעה עשויה הייתה לסכל שימוש במידע שבמאגר למטרות ביטחוניות-משטרתיות.¹³³ מכך עולה כי המדינה מעניקה למטרות אלה קדימות על פני המטרה העיקרית של המאגר, שלא הייתה נפגעת אילו הייתה מיושמת הצעת שמיר. פרופ' אלי ביהם, דיקן הפקולטה למדעי המחשב בטכניון, ומבכירי המומחים בהצפנה ובאבטחת מידע בארץ ובעולם, כתב בהקשר זה כי "העובדה ששיטת העמעום שהציע פרופ' שמיר, שמטרתה להפחית את דליפת הפרטיות

132 עודד ירון "השרים אמרו לא להצעת שמיר לחוק הביומטרי" **הארץ** 16.5.2011 www.haaretz.co.il/hasite/spages/1228081.html (נבדק לאחרונה ב-5.12.2012).

133 ראו בעניין זה את דבריו של דורון שקמוני, מומחה לאבטחת הוועדה, המופיעים בפרוטוקול מס' 1 משיבת הוועדה המשותפת של ועדת המדע והטכנולוגיה, ועדת החוקה, חוק ומשפט וועדת הפנים והגנת הסביבה לפי חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, הכנסת ה-18, 127 (2.6.2011): "דורון שקמוני: אני חושב שנחשפת מתוך הדברים האלה המטרה האמיתית של מרכיב המאגר שבחוק. היו"ר מאיר שטרית: ממש לא. דורון שקמוני: אני חושב. כבודו, זה מה שאני רוצה לומר. המטרה האמיתית, שהיא בעצם המטרה שמנצחת כל פתרון חלופי, היא המטרה שלא לשמה מראש נוצר החוק והיא טענות כאלה ואחרות, שחלקן מחזיקות מים וחלקן פחות, של המערכות של ביטחון פנים ומערכת הביטחון. אני חושב שזה חשוב שהנושא הזה צף מכיוון שאת הבעיה המקורית, שהיא בעיית ההרכשה הכפולה, שהיא בעיה שגודלה המספרי הוא גודל מאוד מאוד קטן, ניתן היה לפתור בשלל דרכים אחרות, שהיו יוצרות מאגר הרבה פחות מסוכן מהמאגר שאנחנו יוצרים היום, ועדיין לתת את כל המענה שדורש משרד הפנים, אבל מסתבר שזו איננה המטרה המרכזית שבעצם לשמה נבנה המאגר הזה".

מהמאגר הביומטרי, לא נבחרה לשימוש על ידי משרד הפנים בטענה המגוחכת שהיא פוגעת בפרטיות, מוכיחה שכוונת מקימי המאגר אינה מניעת זיופי זהות, אלא קידום מטרות זרות שאינן מוזכרות בחוק.¹³⁴

(ג) מבחן התועלת מול הנזק

ראינו כי התועלת העיקרית של המאגר הביומטרי היא מניעת התופעה של הרכשה כפולה של מסמכי זיהוי – כלומר הנפקת שתי תעודות אותנטיות (או יותר) לאותו אדם המופיע בכל פעם במרכז ההנפקה בנושא זהות שונה. דא עקא, במסגרת הליך החקיקה לא נמסרו כלל נתונים בדבר היקף התופעה של אזרחים הנושאים תעודות זהות כפולות או רבות. ודוק: אין קשר הכרחי בין מספר תעודות הזהות המזויפות, שהוערך על ידי מקדמי החוק במאות אלפים,¹³⁵ לבין מספר התעודות האותנטיות שהונפקו למי ששם לו למטרה להחזיק ביותר מתעודה אחת. לנוכח הסיכון הכבד לאבטחת המידע שבמאגר, לדחיית הפריסה של תעודות זהות חכמות בעקבות אימוצו, לעלויות הכספיות של יישומו וכמובן לפרטיות האזרחים, נראים יתרונותיו של המאגר צנועים לעומת הנזק הגלום בו. את התועלת העיקרית של החוק אפשר היה להשיג גם מבלי להקים מאגר ביומטרי מרכזי; ואילו גם התועלות הביטחוניות-משטרתיות השניוניות – שחוקתיותן מוטלת בספק – כגון זיהוי אדם שאינו נושא תעודה מזהה בהעדר אמצעי זיהוי אחר, נראות מוגבלות.

שיקולי עלות-תועלת אלה הובילו שתי דמוקרטיות מערביות חשובות, הולנד ובריטניה, לסגת מתכניותיהן להקים מאגר ביומטרי מרכזי לצורך תמיכה בהנפקת מסמכי זיהוי לכלל האוכלוסייה לאחר אימוצה של חקיקה בנושא.¹³⁶ בהולנד החליטה הממשלה להקפיא את הקמת המאגר הביומטרי ולאגור את המידע הנאסף רק עד למועד הנפקתם של מסמכי הזיהוי.¹³⁷ זאת, לנוכח ההיקף המדאיג של שגיאות קבלה ושגיאות דחייה שהתגלו

134 ביהם, לעיל ה"ש 61.

135 יש לציין כי ספק אם אכן קיימות בישראל מאות אלפי תעודות זהות מזויפות, כפי שנטען על ידי מקדמי החוק. יש להניח כי נתון זה כולל גם מקרים רבים של אזרחים שתעודותיהם אבדו או הושחתו והם ביקשו להנפיק בעבורם תעודה חדשה.

136 ראו במבי שלג ונעמה צפרוני "מדינות אירופה נסוגות מן המהלך הביומטרי" **ארץ אחרת** 64 (2012). בהולנד נכנס ב-28 יוני 2009 לתוקף חוק להקמת מאגר ביומטרי והטמעת הנתונים בתעודות זהות ודרכונים: Rijkswet van 11 juni 2009 tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie, 252, available at www.eerstekamer.nl/behandeling/20090623/publicatie_wet_2/f=vi6pcfrrua0a4.pdf (נבדק לאחרונה ב-5.12.2012).

137 בדואר אלקטרוני ממר Paul Breitbarth, האחראי על יחסים בין-לאומיים ברשות הגנת המידע ההולנדית, אליי (19.5.2011) נמסר לי כך: "The discussion on the necessity of the central

במערכת, והביקורת הקשה שהוטחה בה על ידי מומחי אבטחת מידע וארגוני זכויות אדם.¹³⁸ בבריטניה, לאחר דיון ציבורי סוער שהפך לאחד מנושאי המחלוקת העיקריים במערכת הבחירות,¹³⁹ ביטלה ממשלת השמרנים שזכתה בבחירות ב-2010 את החקיקה להקמת מאגר ביומטרי לאומי (National Identity Registry) והורתה להשמיד את כל המידע שהוחזק בו.¹⁴⁰ בסופו של דבר, התערער אמון הציבור בפרויקט נוכח אי-הבהירות בדבר מטרותיו האמתיות; אי-הבהירות המעיבה, כפי שהסברתי לעיל, גם על החוק הישראלי. כך מציין העיתון "האקונומיסט" כי ממשלת בריטניה לא הבהירה במידת הצורך את המטרה המדויקת של תעודות הזהות הביومترיות:

database only really took off this year, after several objections from within the civil rights movement and some test trials to object against the collection of fingerprints in the central database. After a renewed discussion in parliament, the Minister for Home Affairs has decided in April to suspend the build of the central database. He states in his letter to parliament that central storage remains the objective, but that the quality of fingerprinting is too low to enable true law enforcement activity. The number of so-called false positives would be too high...". The Dutch House of Representatives, *Security of Biometric Details in Passports*, 27.4.2011, available at www.houseofrepresentatives.nl/dossiers/security_biometric_details_passports.jsp (נבדק לאחרונה ב-5.12.2012). Centralized storage postponed MPs discussed the safety and reliability of fingerprint storage with a range of experts and researchers. A number of experts made some critical remarks on the reliability of the fingerprints and the storage of data. As a result, Mr Piet Hein Donner, the Dutch minister of the Interior, decided to postpone the centralized storage of finger prints"

Max Snijder, WRR Scientific Council for Government Policy Study, *Het Biometrisch Paspoort in Nederland: Crash of Zachte Landing* (The biometric passport in the Netherlands: crash or soft landing) (2010) *A.T.B. Bijleveld-Schouten, Briefaan* (Netherlands: crash or soft landing) (2010) *de Tweede Kamer over evaluatie van de invoering van de vingerafdrukken in de Nederlandse reisdocumenten* (Letter to the Dutch Lower House on the evaluation of the introduction of fingerprints in Dutch travel documents), 2010, Parliamentary documents II 2009-2010, 31 324 no. 23

Jennifer Morris, *Big Success or "Big Brother?"*: *Great Britain's National Identification Scheme Before the European Court of Human Rights*, 36 GA. J. INT'L & COMP. L. 443 (2008).

Identity Documents Act 2010 (c. 40); Alan Travis, *ID Cards Scheme to Be Scrapped Within 100 Days*, THE GUARDIAN (26.5.2010), available at www.guardian.co.uk/politics/2010/may/27/theresa-may-scrapping-id-cards (נבדק לאחרונה ב-5.12.2012): "Bill abolishing ID cards and national identity register will be first piece of legislation introduced to parliament by the new government, says Theresa May"

“Depending on the phases of the moon (or, more accurately, the headlines in that week's papers) they were meant to combat terrorism, keep tabs on immigrants, cut down on benefit fraud, nobble criminals and suppress identity theft”.¹⁴¹

לדברי האקונומיסט, חוסר הבהירות הזאת לא סייעה לקדם את הפרויקט אל מול ההתנגדות מצדם של כלכלנים וארגוני זכויות האדם. בארצות־הברית קיימים אמנם מאגרים ביומטריים מבוזרים (למשל, לתיירים שנדרשים למסור סריקה של כל טביעות אצבע וצילום פנים בנמל התעופה),¹⁴² אך מסיבות שונות, ובהן סיבות היסטוריות הנוגעות למתח בין המדינות לבין הממשל הפדרלי, אין בארצות־הברית מרשם אוכלוסין מרכזי ולא קיימות תעודות זהות לאומיות, להבדיל מרישיון נהיגה מדינתי או מספר ביטוח לאומי.¹⁴³ מדינות אחרות המחייבות את אזרחיהן לשאת תעודות זהות עם מידע ביומטרי המוחזק במאגר מרכזי הן בעלות היסטוריה לא דמוקרטית (כגון ספרד) או משטר דמוקרטי מוגבל בקנה מידה מערבי (כגון מקסיקו או הונג קונג).¹⁴⁴

ו. מנגנונים להבטחת הפרטיות: הזדמנויות

כנגד הסיכונים המגולמים בו, מציג החוק שורה של מנגנונים טכנולוגיים, ארגוניים ומשפטיים הבאים להבטיח את פרטיות המידע הביומטרי ואבטחתו, בהיקף שאינו קיים באף דבר חקיקה אחר בישראל. כיום נהוג לכנות מנגנונים אלה “תכנון לפרטיות” (Privacy)

141 *Scrapping ID cards: No ID Cards, Please, We're LibCons*, THE ECONOMIST, 27.5.2011, available at www.economist.com/blogs/newsbook/2010/05/scrapping_id_cards (נבדק לאחרונה ב־5.12.2012).

142 United States Visitor and Immigrant Status Indicator Technology (US-VISIT), Department of Homeland Security, 8 CFR 215 and 235, 73(245) Federal Register 77473–77491, 19.12.2008.

143 Neda Matar, *Are You Ready for a National ID Card? Perhaps We Don't Have to Choose Between Fear of Terrorism and Need for Privacy*, 17 EMORY INT'L L. REV. 287 (2003).

144 לסקירה מקיפה ראו הכנסת, מרכז המחקר והמידע **אמצעי זיהוי ביומטריים במסמכי זיהוי ומאגרי מידע ממשלתיים: סקירה משווה** (14.1.2009) www.knesset.gov.il/mmm/ (נבדק לאחרונה ב־5.12.2012); Statewatch Briefing, *ID Cards in the EU: Current State of Play* (2010), available at www.statewatch.org/analyses/no-107-national-ID-cards-questionnaire.pdf (נבדק לאחרונה ב־5.12.2012).

145. (by Design) הם הוכנסו לחוק בעקבות מעורבותם בהליך החקיקה של משרד המשפטים – ובעיקר של הרשות למשפט, טכנולוגיה ומידע (רמו"ט), שהעומד בראשה כיום, עו"ד יורם הכהן, חרת על דגלו את עקרון התכנון לפרטיות – וכן של ארגוני זכויות אדם, אנשי אקדמיה, מומחים לביומטריה, לאבטחת מידע ולהצפנה ועוד. הרעיון העומד בבסיס התפיסה של תכנון לפרטיות, הוא כי יש להטמיע את הגנת הפרטיות כבר בשלב תכנון המערכת, המוצר או השירות. זאת, להבדיל מגישה של תגובות, הממתינה להתמודד עם השלכות הפרטיות רק לאחר אירוע של נזק. כך הופכת ההגנה על הפרטיות לתחום עיסוקם לא רק של עורכי דין אלא גם של מהנדסים ומעצבי מערכות.¹⁴⁶ יש לקוות כי אחד היתרונות שיופקו בעקבות חקיקתו של החוק הוא הפצתם של מנגנוני תכנון לפרטיות גם לדברי חקיקה אחרים בעלי השלכה על הפרטיות. להלן אסקור מנגנונים אלה בקצרה.

1. מנגנונים טכנולוגיים

כדי לאבטח את המידע הביומטרי הגולמי ולהפרידו מהמידע הדמוגרפי והאחר המוחזק בידי המדינה, קובע החוק כי המידע יוצפן מיד לאחר איסופו וישמר באופן מוצפן ובנפרד מכל מידע אחר. סעיף 3(ב) לחוק קובע: "אמצעים ונתונים שניטלו והופקו [...] יוצפנו באופן אוטומטי מיד לאחר הנטילה וההפקה, כך שלא יהיו ניתנים לפענוח, קריאה או שימוש, אלא על ידי הרשות או מרכז הנפקה בהתאם להוראות לפי חוק זה". הוראה זאת יש לקרוא עם הוראת סעיף 10(א) לחוק, הקובעת כי "המאגר הביומטרי יישמר באופן מוצפן, בנפרד מכל מידע אחר ולא יכלול פרטי רישום של התושב כמשמעותם בחוק המרשם או כל פרט מזהה אחר". חריג להוראה זאת קיים בסעיף 10(ב), שלפיו "על אף האמור בסעיף קטן (א), יהיה ניתן לקשר בין אמצעים או נתונים ביומטריים שבמאגר הביומטרי, לבין מספר זהותו במרשם האוכלוסין של התושב שאליו הם מתייחסים, בדרך שתקבע בכללים ובכפוף לתקנות שיוקנו לפי סעיף (ד)".

סעיף 10(ד) לחוק קובע כי שר הפנים "בהתייעצות עם שר המשפטים ובאישור ועדת הכנסת המשותפת, יקבע תקנות בדבר דרכי ניהול המאגר הביומטרי, שמירת המידע בו ואופן העברת המידע ממנו, ורשאי הוא לקבוע בדרך כאמור כי המאגר הביומטרי יורכב מתתי-מאגרים נפרדים, שיתנהלו במשרד הפנים או במשרד ממשלתי אחר, או שיתנהלו

145 Ann CAVOUKIAN, PRIVACY BY DESIGN... TAKE THE CHALLENGE (2009) וראו חומר רב באתר: www.privacybydesign.ca (נבדק לאחרונה ב-5.12.2012).

146 Seda Gürses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design, in Computers, Privacy & Data Protection in Conference and Computers, Privacy & Data Protection* (2011), available at www.dagstuhl.de/mat/Files/11/11061/11061.DiazClaudia.Paper.pdf (נבדק לאחרונה ב-5.12.2012).

בחלקם במשרד הפנים ובחלקם במשרד כאמור, והכל לשם הבטחת רמה גבוהה ככל שניתן של הגנה על המידע המצוי במאגר ואבטחתו". מטרתו של סעיף 10(ד) לחוק לאפשר מנגנון המכונה בשפת ההצפנה "חלוקת סוד", שלפיו מפוצל מידע ("סוד") בין שותפים אחדים, באופן שהמידע אינו ידוע לאף אחד מהם בנפרד ואפשר לגלותו רק באמצעות שיתוף פעולה של כל השותפים.¹⁴⁷ שוו בנפשכם תיבת אוצרות אשר נפתחת רק כאשר שני שומרים מכניסים כל אחד את המפתח הייחודי שלו למנעול שמוטבע בה. כך, למשל, עשוי היה חלק מהמידע הביומטרי להיות מוחזק בידי משרד הפנים וחלקו האחר בידי משרד המשפטים, כך שגם אם תתבצע פריצה לאחד המאגרים או יודלף ממנו מידע, לא יוכל הפורץ או המדליף ליהנות מגישה אל מידע מזהה מבלי לפרוץ גם אל המאגר האחר.¹⁴⁸ נוכח סעיף זה מצער היה להיווכח כי התקנות כפי שהותקנו לבסוף על ידי שר הפנים באישורה של הוועדה המשותפת לא כללו פיצול בין המאגרים.

במקומות אחדים בחוק הוכנסו הוראות האוסרות אגירה מקומית של מידע בתחנות ההרכשה או בעמדות האיסוף שבידי השוטרים. כך, למשל, קובע סעיף 3(ה) לחוק, בהקשר של נטילת אמצעי הזיהוי הביומטריים, כי "אמצעים ונתונים שניטלו והופקו לפי הוראות סעיף קטן (א) לא ייאגרו באופן ממוחשב, למעט במאגר הביומטרי, מעבר לנדרש לצורך העברתם לרשות ולמרכז הנפקה לפי הוראות סעיף קטן (ג), והם יימחקו באופן אוטומטי מכל מקום שבו נשמרו". כלומר, שוטר הנוטל מאדם דגימה ביומטרית לא יוכל לאגור את המידע במאגר "מקומי"; המידע יימחק באופן אוטומטי על ידי המערכת עם העברתו לתחנה הבאה. סעיף 4(ב) לחוק קובע, בהקשר של מרכז ההנפקה, כי "האמצעים והנתונים המוצפנים שהועברו למרכז הנפקה לפי הוראות סעיף 3(ג) לא ייאגרו באופן ממוחשב, מעבר לנדרש לצורך הנפקת מסמך זיהוי והם יימחקו באופן אוטומטי מיד לאחר הנפקתו". הוראות דומות אפשר למצוא גם בסעיפים 6(ו), 7(ב) ו-24(ב) לחוק. במסגרת זאת יש לציין גם את סעיף 25(ב) לחוק, הדורש כי "כל פעולה המבוצעת במאגר הביומטרי תתועד באופן שיאפשר פיקוח ובקרה על אופן ביצועה, על מועד ביצועה ועל מבצע הפעולה". תיעוד הגישות למערכת והפעולות המבוצעות באמצעותה חשוב לצורך אבטחת מידע, זיהוי פעולות חשודות והענשתם של עובדים החורגים מהנהלים.

במסגרת הפתרונות הטכנולוגיים לבעיות הפרטיות, אפשר למנות גם את השימוש בתמונת פנים באיכות פחותה לצורך זיהוי אנושי, לא ממוכן, על ידי פקיד משרד הפנים,

147 הביטוי הידוע ביותר של תיאוריה זאת הוא מאמרו של פרופ' עדי שמיר: *Adi Shamir, How to Share a Secret*, 22 COMMUNICATIONS OF THE ACM 612 (1979).

148 אפשר כמובן לחלק ברוח זאת את המידע בין יותר משני גורמים ולהקשות עוד על גישה לא מורשית אל כל המידע הנדרש.

חוק המאגר הביומטרי: סיכונים והזדמנויות

תוך מניעת שימושים והעברות מיותרים של התמונה המקורית באיכות הביומטרית.¹⁴⁹ המונח "תמונת פנים באיכות פחותה" מוגדר בסעיף 2 לחוק כ"תמונת תווי פניו של אדם המאפשרת זיהוי חזותי שלו והמעובדת כך שנתוני הזיהוי הביומטריים שיהיה ניתן להפיק ממנה לא יוכלו לשמש, באופן מעשי, לצורך זיהוי או אימות זהותו של אדם, באופן ממוחשב או ממוחשב בחלקו".

ראוי היה שמנגנונים טכנולוגיים של תכנון לפרטיות יאומצו גם במסגרת יזמות חקיקה ותכנון לאומי נוספות. כך, למשל, אפשר היה להנפיק כרטיס חכם לתחבורה ציבורית שאינו אוגר את כל המידע על תנועותיו של אדם ואינו מהווה תנאי לשימוש של אדם במערכת.¹⁵⁰ מידע הנאסף על ידי ראמ"ה יכול היה לעבור תהליך של "אנונימיזציה" ולהישמר כמידע סטטיסטי המשמש לצורך מחקר בלבד.¹⁵¹ הרשומה הרפואית הלאומית יכולה הייתה להיות מבוזרת, כך שרופא או אחות הנדרשים למידע היו מזמנים אותו מנקודות קצה שונות, בהתאם להרשאות הגישה המוקנות להם.¹⁵²

2. מנגנונים ארגוניים

עצם הקמתה של הרשות לניהול המאגר הביומטרי מהווה חידוש חקיקתי וצעד חשוב של תכנון לפרטיות. אפשר לתאר את המאגר הביומטרי מוחזק בידי אותם עובדים של משרד הפנים האמונים על שמירתו של מרשם האוכלוסין.¹⁵³ הרשות החדשה תהיה מופקדת על ניהול המאגר הביומטרי – העברת מידע ממנו, אבטחתו ותחזוקתו השוטפת. היא תורכב מעובדים שכולם עובדי מדינה, שאינם ממלאים תפקיד אחר מלבד עבודתם ברשות, ושעברו בדיקות התאמה ביטחוניות בהתאם לסעיף 15 לחוק שירות הביטחון הכללי, התש"ס–2002. סעיף 13(ג) לחוק קובע כי "קביעת מורשי הגישה למאגר הביומטרי [...] והתנאים וההגבלות שיחולו עליהם [...] תיעשה באופן שיצמצם ככל הניתן את מספר המורשים

149 ס' 27 לחוק.

150 ראו הנחיית רשם מאגרי מידע 1/2012 בעניין תחולת הוראת חוק הגנת הפרטיות על מאגרי מידע של מפעלי כרטיס חכם בתחבורה ציבורית: www.justice.gov.il/NR/rdonlyres/EA5A7893-2BF4-4CA8-82D4-91BABFF3DE5A/33915/12012.pdf (נבדק לאחרונה ב-5.12.2012).

151 בינט, לעיל ה"ש 9.

152 פינצ'וק, לעיל ה"ש 93.

153 דו"ח מבקר המדינה לשנת 2009 תיאר שורה של כשלים שהובילו לדליפת מאגר המידע של מרשם האוכלוסין של מדינת ישראל לאינטרנט וזמינותו להורדה על ידי גולשים החפצים בכך. יובל אזולאי "דו"ח מבקר המדינה 2009: משרד הפנים התרשל, והמידע האישי של האזרחים חופשי באינטרנט" **הארץ** 6.5.2009 www.haaretz.co.il/hasite/spages/1083483.html (נבדק לאחרונה ב-5.12.2012).

כאמור ואת היקף המידע הנגיש". הוראה זאת תואמת את עקרון צמצום המידע, שלפיו יש להגביל במידת האפשר את היקף המידע שנעשה בו שימוש במערכת ואת מספר מורשי הגישה לכל פריט.¹⁵⁴ חידוש חקיקתי חשוב הוא מינויו של "הממונה על הפרטיות במאגר הביומטרי". תפקיד הממונה על הפרטיות (CPO – Chief Privacy Officer) קנה לו אחיזה בקרב חברות מובילות ורשויות שלטון בארצות־הברית והוא החל להתפשט לאחרונה גם באירופה. מן הראוי לייבא את תפקיד ה־CPO לישראל, גם אם הדבר נעשה באמצעות חוק בעייתי זה המזיק לפרטיות.¹⁵⁵ הפקדתו של נושא משרה בדרג הנהלה גבוהה על הגנת הפרטיות בארגון, מבטיחה "כתובת" ומוקד לאחריות אישית ונחשבת צעד חשוב במסגרת ההטמעה של עקרונות האחריות בארגון, אם באמצעות כללי המשטר התאגידי (corporate governance) (במגזר הפרטי) ואם דרך כללי המנהל התקין (במגזר הציבורי). בעל תפקיד חשוב נוסף שקובע החוק הוא "הממונה על יישומים ביומטריים" במשרד ראש הממשלה, שתפקידו להמליץ על מדיניות כוללת בתחום הביומטריה, אבטחת המאגר והמידע המועבר ממנו, ולפקח על יישום הוראות החוק, התקנות, הכללים, ההנחיות והנהלים מכוחו.¹⁵⁶

ברי כי המנגנונים הארגוניים של התכנון לפרטיות שמציב החוק יכולים היו להשתלב במסגרת רשויות ציבוריות רבות נוספות. אמנם לא בכל עניין נדרשת הקמה של רשות ממשלתית מיוחדת; אך מינוי של ממונה על פרטיות נוהג כיום בחברות פרטיות רבות,

154 עקרון צמצום המידע הוא אחד העקרונות החשובים בדיני הפרטיות והגנת המידע, אם לא החשוב שבהם. הוא מעוגן בס' 6(1)(B) ו־6(1)(C) לדירקטיבת 95/46, לעיל ה"ש 29. ראו בהקשר זה דבריה של השופטת דורנר בבג"ץ 8070/98, לעיל ה"ש 128, פס' 9 לפסק דינה, שלפיהם דרישת צמצום המידע נובעת מעקרון המידתיות החוקתית. לאחרונה אימצה הרשות למשפט, טכנולוגיה ומידע טיוטת תקנות אבטחת מידע, שלפיהן: "על מנת להפחית את סיכוני אבטחת המידע למידע שבמאגר, יבחן בעל המאגר לפני הקמת מאגר המידע ולכל אורך פעילותו של מאגר המידע, כי המידע הנאסף והנשמר על ידו אינו מעבר לנדרש לצורך מימוש מטרות המאגר". ס' 2(ג) לנוסח מוצע לתקנות מכוח חוק הגנת הפרטיות, התשמ"א-1981, לעניין אבטחת מידע במאגרי מידע; ראו גם ס' 15(א) לטיוטת התקנות הקובע: "מידע המצוי במאגר מידע שכבר אין בו צורך לתפעולו השוטף של המאגר, יימחק אלא אם קיים צורך על פי דין לשומרו לצורכי גיבוי; גיבוי כאמור יישמר בנפרד באופן שיפחית את סיכוני אבטחת המידע לשימוש לא מורשה בו". bit.ly/dNrYy5 (נבדק לאחרונה ב־5.12.2012).

155 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011); International Association of Privacy Professionals, *A Call for Agility: The Next-Generation Privacy Professional*, WHITE PAPER (2010).

156 דא עקא כי לא מוגזם יהיה להניח ש"הממונה על יישומים ביומטריים" יהיה איש רשות ביטחון – בבחינת "החתול השומר על השמנת".

חוק המאגר הביומטרי: סיכונים והזדמנויות

ומסייע להטמיע ערכים של פרטיות והגנת מידע בעסק. מן הראוי היה כי לפחות רשויות ציבוריות המנהלות מאגרי מידע מקיפים ורגישים, כגון המוסד לביטוח לאומי, רשות המסים, משרד הבריאות, מרשם האוכלוסין ועוד – יחויבו למנות בעל תפקיד בכיר שיהיה ממונה על נושא זה ויישא באחריות לקידומו.

3. מנגנונים משפטיים

החוק עשיר בהוראות שתפקידן להטמיע עקרונות של פרטיות ואבטחת מידע במערכת הביומטרית, כולל ענישה בגין אי-שמירה על פרטיות המידע וסודיותו.¹⁵⁷ סעיף 29(ה) לחוק מטיל אחריות אישית כבדה על ראש הרשות לניהול המאגר הביומטרי: "ראש הרשות חייב לפקח ולעשות כל שניתן למניעת עברה לפי סעיף זה, בידי מי שיש לו הרשאת גישה [...] הפר את חובתו האמורה, דינו – מאסר שישה חודשים או הקנס הקבוע בסעיף 61(א)(4) לחוק העונשין"; מדובר בקנס בסכום נכבד של 226,000 ש"ח, שעלול להיות מוטל אישית על ראש הרשות.

כבר בשלב נטילת אמצעי הזיהוי הביומטריים, מורה החוק כי יש לבצע את הפעולות הנדרשות "בדרך ובמקום שיבטיחו שמירה על כבוד האדם ועל פרטיותו וימנעו פגיעה בהם במידה העולה על הנדרש".¹⁵⁸ כמו כן, מלבד הדרישות הפרוצדורליות השונות, חייב צו של בית משפט להעברת מידע מן המאגר, לעמוד במבחן מהותי שלפיו "אין בהעברת המידע כאמור כדי לפגוע במידה העולה על הנדרש בפרטיותו של אדם".¹⁵⁹

סעיפים 24–25 לחוק מוקדשים לשמירה על פרטיות המידע הביומטרי, סודיותו ואבטחתו. בין היתר, דורש סעיף 25 לחוק לשמור על המידע הביומטרי "בדרך שתבטיח הגנה מפני דליפת מידע מהמאגר או פריצה אליו, וכן מפני העברה, חשיפה, מחיקה, שימוש, שינוי או העתקה בלא רשות כדין [...] וכן שתבטיח הגנה על פרטיותם של התושבים שהאמצעים והנתונים כאמור מתייחסים אליהם, ותאפשר בקרה ופיקוח על אופן השימוש במאגר, לרבות שימוש החורג ממסגרת ההרשאה". כאמור, הדרך היעילה ביותר לשמור על המידע הביומטרי ולהבטיחו מפני דליפה, פריצה או גישה לא מורשית היא לא להחזיקו כלל, וודאי שלא להחזיקו בצורתו הגולמית.

החוק דורש גם דיווחים רבים של שר הפנים, שר הביטחון, השר לביטחון פנים, ראש הרשות, הממונה על הפרטיות ברשות ורשויות הביטחון, לממשלה, לכנסת ולרשם מאגרי

157 ס' 29 לחוק מונה שורה של עברות פליליות, שעונשן נע בין שנה לבין שבע שנות מאסר.

158 ס' 9(א) לחוק.

159 ס' 17 לחוק.

מידע.¹⁶⁰ החוק מקים ועדת שרים ליישומים ביומטריים, בראשות ראש הממשלה ובהשתתפותם של שר הפנים, שר המשפטים והשר לביטחון הפנים;¹⁶¹ "ועדת כנסת משותפת" לוועדת החוקה חוק ומשפט של הכנסת, לוועדת הפנים והגנת הסביבה של הכנסת ולוועדת המדע והטכנולוגיה של הכנסת;¹⁶² וכן "ועדת כנסת משותפת ליישומים ביומטריים", בראשותו של יושב ראש ועדת החוץ והביטחון של הכנסת, ובהשתתפותם של יושב ראש ועדת הכנסת המשותפת, חברי ועדת החוקה חוק ומשפט של הכנסת וחברי ועדת המשנה למודיעין ולשירותים חשאיים של ועדת החוץ והביטחון של הכנסת.¹⁶³ כמו כן, דורש החוק סמכויות שונות מכוח החוק יופעלו על ידי שר הפנים אך ורק בשיתוף עם ראש הממשלה, שר המשפטים, או ועדת הכנסת המשותפת.¹⁶⁴

מנגנונים משפטיים של תכנון לפרטיות ראוי היה לאמץ גם בדברי חקיקה אחרים היוצרים סיכון לפרטיות או לאבטחת מידע. כך, למשל, הטלת חובה על ארגונים לדווח לרגולטור או לציבור על אירוע של כשל אבטחת מידע, תבטיח כי דליפת מידע לא תישאר "אירוע פנימי"; כי במידת הצורך תוטל אחריות משפטית על גורם רשלין או מזיק; וכי לארגונים יהיה תמריץ חזק לאבטח מידע כנדרש כדי למנוע מלכתחילה את החובה למסור הודעה לא נעימה על כשל. כמו כן, הטלת קנסות, ובמקרים מתאימים גם אחריות אישית על נושאי משרה, עקב הפרות שונות של דיני הגנת הפרטיות, תסייע ליצור תמריץ מתאים אצל ארגונים להשקיע בהגנת הפרטיות כפי שנהוג להשקיע בתחומים אחרים של ציות לחוק.

ז. לסיכום

מערכות ביומטריות מציבות אתגרים קשים לפרטיות ואבטחת מידע. הן יוצרות בעיות של זיהוי, חפצון (או החפצה) של הגוף, זחילת פונקציות, סכנות אבטחה, איסוף מידע עודף ומעקב על ידי המדינה. בעיות אלה מחריפות ככל שמדובר במערכות האוגרות מידע במאגר מרכזי, ובעיקר כאשר המידע הנאגר הוא המידע הביומטרי הגולמי, להבדיל מתבניות שנגזרו ממנו. מדינת ישראל החליטה להפעיל מערכת ביומטרית מהסוג הבעייתי ביותר מבלי שהובהר הצורך בקיומה או שנסקלו בפתיחות מלאה חלופות המשרתות את המטרה הראשית המוצהרת של החקיקה: מניעת זיופים או הרכשה כפולה של תעודות זהות

160 ראו למשל ס' 5(ג), 17(1), 20, 33 ו-41 לחוק.

161 ס' 31 לחוק.

162 ס' 2 לחוק.

163 ס' 32 לחוק.

164 ראו למשל ס' 4(ג), 5(ב), 6(ב), 10(ד), 11(ב), 15, 24(ג), 26, 27(ג), 34, 35, 37, 40 ו-41.

חוק המאגר הביומטרי: סיכונים והזדמנויות

ודרכונים. יש להצר על כך כי פרויקט לאומי כה גדול וחשוב יצא לדרך לאחר דיונים בוועדה בכנסת, שבאחדים מהם השתתף לא יותר מחבר כנסת אחד – יושב ראש הוועדה, שיזם בעצמו את הצעת החוק. התוצאה הסופית היא חוק שתוקפו מותלה בהחלטה של שר הפנים ואשר צפוי לעמוד למבחן חוקתי בבג"ץ. במסגרת הליך כזה, מן הראוי שבג"ץ יקבע כי החוק אינו עומד בתנאיה של פסקת ההגבלה לפגיעה בזכות חוקתית מכוח חוק-יסוד: כבוד האדם וחירותו, לנוכח תכליתו המעורפלת ואי-המידתיות של האמצעים שהוא נוקט להשגתה. מאגר ביומטרי לאומי אינו נחוץ לצורך מניעת זיופים של מסמכי זיהוי, ומהווה פתרון גם ודרקוני לבעיה שהיקפה לא הובהר – הרכשה כפולה של תעודות אותנטיות. גם מדינות דמוקרטיות אחרות ששקלו הקמת מאגר כזה נסוגו בהן מכוונתן. לעומת קשיים אלה, יש לציין לטובה את מנגנוני התכנון הפרטיות שהוכנסו לחוק, ולקוות כי מנגנונים טכנולוגיים, ארגוניים ומשפטיים מסוג זה יאומצו גם בדברי חקיקה אחרים בעלי השלכה על הזכות לפרטיות.