ארנון הראל

רח' הגבעה 36 arnonh@bezeqint.net נייד: 052-868-0800 טל': 077-4405441
גבעת עדה 37808 29 אוקטובר, 2006 פקס: 077-4405442

מה כה מיוחד בטכנולוגיה הביומטרית?

כך שזה מעורר את השאלות של זהות, פרטיות, חופש ודמוקרטיה, וכך שזה מעצים את הבעיתיות שבמימוש כל שיטת זיהוי אחרת שאינה ביומטרית

1. מבוא

בישראל קיים מרשם אוכלוסין וכל אזרח מזוהה בו ע"י מספר זהות והוא נושא תעודת זהות עפ"י חוק. במרבית הארצות המוגדרות כמתקדמות, או העולם "המערבי", אין לאזרחים תעודת זהות ואין מספר זהות כמשמעותו בישראל. תעודות זהות, לעומת זאת, נהוגות במרבית הארצות שנהוג לכנותן "העולם השלישי". הדרכונים מהווים ומוכרים בכל העולם כמסמכי זהוי בינלאומיים, ככל שהמדובר בתיעוד מסע.

הנושא של השימוש בטכנולוגיה הביומטרית, על הסיכויים והסיכונים שהיא טומנת בחובה, כמעט ולא נדון עד כה בציבור הרחב בארץ. בשנים האחרונות, ובמיוחד לאחר ארועי 11 לספטמבר בארה"ב, מתקיימים ברבות מארצות אירופה ובארה"ב ובקנדה, דיונים וויכוחים אודות הצורך בהנפקת תעוד מזהה מאובטח, הן לאזרחים והן לנוסעים העוברים ממדינה למדינה, לצורך התמודדות עם איומים כנגד הבטחון הלאומי והאישי. בארה"ב ובחלק ממדינות אירופה כבר הוחל לאחרונה, עפ"י חוקים תקנות ותקנים שנחקקו לצורך זה, בהנפקת דרכונים וויזות הכוללים טכנולוגיות ביומטריות.

בכל הדיונים הללו אודות הנפקת תעודות הזהות והדרכונים משתלב, כחלק בלתי נפרד, השימוש בטכנולוגיות ביומטריות כאמצעי לזיהוי האדם נושא התעודה ולאימות הקשר שלו עם התעודה. באותם דיונים מועלות, לצד הצורך הבסיסי ליכולת זיהוי אמינה של כל אדם, שאלות אתיות וחוקתיות רחבות, כגון:

- מהי זהות והאם יש לאדם זהות אחת ויחידה
- האם מוצדק ליצור זהות פורמאלית על בסיס לאומי, כגון תעודת זהות, או על בסיס גלובאלי, כגון דרכון בינלאומי
- האם מוצדק להקים בסיס נתונים מרכזי (מרשם אוכלוסין), אלו פרטים ישמרו בבסיס הנתונים המרכזי ואלו פרטים ירשמו בתעודה עצמה

לשאלות אלה יש משמעויות אתיות וחוקתיות רחבות, החל בזכות לפרטיות, חופש וזכויות הפרט, כבוד האדם, הזכות לבטחון אישי וכלה במהות הדמוקרטיה. לשאלות אלה גם יש השלכות מערכתיות וטכניות אודות הדרך שבה מוקמות אותן מערכות ומנגנונים שנועדו לזיהוי אדם. אולם חשוב לזכור כי שאלות אלה אינן ייחודיות לביומטריה אלא לעצם ההשקה של מערכת זיהוי כלשהי, גם כשהיא כלל אינה כוללת ביומטריה.

בישראל הועלה לאחרונה הצורך בשילוב טכנולוגיות ביומטריות בתעודת הזהות החדשה וגם בדרכון הלאומי החדש שבתכנון. באופן נפרד ובלתי תלוי גם הוגשה ביולי 2004 מטעם הממשלה וביוזמת המשרד לבטחון פנים, הצעת חוק שבאה להסדיר את סמכויות משטרת ישראל ליטול מחשוד, מנאשם או ממורשע, אמצעי זיהוי ביומטריים ולאגור אותם במאגר נתוני זיהוי שינוהל על ידה[1]. כך שבישראל נושא השימוש בביומטריה עומד לדיון בפני עצמו ואילו בארצות אחרות הוא משולב בשאלה הרחבה של עצם הנפקת התעוד המזהה.

הדיון כאן אינו בשאלה של היתרונות או החסרונות של עצם הזהוי הודאי והבטוח של האדם לצרכים שונים באמצעות אמצעי זהוי כלשהו, אלא בשאלה מה המיוחד בביומטריה לעומת כל שיטות הזיהוי האחרות.

בביומטריה יש שילוב אינהרנטי של תכונות שהופך אותה למיוחדת מול יתר אמצעי הזיהוי שאינם ביומטריים, מקנה לה יתרונות מול האמצעים האחרים, אך גם בו-זמנית מעצים את הסיכונים לפרטיות, פגיעה בחופש וזכויות הפרט ובדמוקרטיה.

מאמר זה עוסק באותם תחומים שלאחר שמפנים אליהם את תשומת הלב לראשונה הם הופכים להיות בחזקת מובנים מאליהם. מטרת המאמר היא, איפה, להגדיל את המודעות לנושא ולהוסיף מימדים וקריטריונים לשאלות הנוגעות להקמת מערכות ביומטריות על בסיס מקומי, לאומי ובין-לאומי ולמנגנוני ההגנה הנדרשים לשמירה והגנה עליהן.

מאמר זה לא נועד לעצור את הקידמה ואת היכולת לעשות שימושים חיוביים בביומטריה, אלא להתריע גם על הסיכונים הכרוכים בטכנולוגיה ולקרוא לאחריות ולזהירות בשימוש בה, כך שכל מערכת מבוססת ביומטריה תכיל בתוכה מלכתחילה את האמצעים הנאותים להגנה, בקרה ושליטה, שלא יעשה בה שימוש לרעה.

2. רקע כללי

פריטי מידע אישי מסוימים נחשבים כמידע רגיש בחלקים שונים של העולם ובתרבויות שונות. הביומטריה כשלעצמה לכאורה אינה מהווה מידע רגיש כי היא אינה מכילה פרטים רגישים אודות האדם אליו היא משויכת. הפרטים הנוספים של אותו אדם, שמתווספים לצד הביומטריה, הם אלו שרגישים. חשוב להחריג מכך את אותם סוגי ביומטריה שבהם מתוך הטביעה הביומטרית עצמה ניתן להפיק מידע אודות האדם, כגון מינו, גילו ומצב בריאותו (והדבר ידון בהמשך).

בד"כ כשמציגים את הביומטריה לקהל הרחב מזכירים את שתי השיטות "המסורתיות" לזיהוי אדם - באמצעות מה שיש לי, כגון תעוד מזהה, ובאמצעות מה שאני יודע, כגון סיסמה. ואז גם מציינים ששיטות אלה סובלות מחסרונות מהותיים שכן את האמצעי שיש לי ניתן לגנוב, להעתיק, לאבד, לזייף וכד' וגם את מה שאני יודע ניתן לשכוח, להעתיק ולזייף... ואז מציגים את הגישה הטכנולוגית המתקדמת והמנצחת של הביומטריה ואומרים ששיטה זו היא בחזקת "מי שאני", ללא מתווכים של אמצעי או מידע, ואותי (את האצבע שלי, את העין שלי...) קשה לאבד, לגנוב ולשכפל. אולם הצגה זו של הביומטריה הנה חד-ממדית ומכוונת לאותם מצבים שבהם מצד אחד אני מעוניין להזדהות ובעקבות זאת לקבל פריביליגיה כלשהי - להכנס לאתר מבוקר, להכנס לחשבון הבנק שלי, ומצד שני - למנוע זאת מאחרים המתחזים להיות אני.

מה שצורת הצגה זו אינה חושפת הוא שישנם מצבים רבים, בחיי היום-יום, בהם הפרט דוקא אינו מעוניין להזדהות ומעדיף להשאר אנונימי; וכי ישנם גורמים רבים, בפועל ובפוטנציה, שדוקא כן מעוניינים לזהות אותו ובעקבות זאת: לאסוף עליו מידע שאינו מעוניין שיאסף, למנוע ממנו פריבילגיות, להפלות אותו, להפליל אותו, לפגוע בפרטיותו, בבטחונו האישי וברכושו ולחשוף אותו לפרסום שלא ביקש. ואז חוסר האפשרות להפטר מהאצבע או העין או הפרצוף היא דוקא חסרון ואילו היכולת להשמיד או להחליף את התעוד המזהה או לשכוח את הסיסמה מהווים דוקא יתרון.

הביומטריה מהווה אם כן את המפתח של הפרט לעולם שלם של שייכות, זכויות והטבות, אבל בו-זמנית מהווה גם את המפתח של צדדי ג' למיניהם להזיק לו או לפגוע בו. וההבדל המהותי בין שני השימושים באותו מפתח הוא מידת השליטה של הפרט בהם - בצד האחד שליטה מלאה: ברצותו מזדהה או לא; ובצד האחר - חוסר שליטה מוחלט. כאשר אני מוסר את הטביעה הביומטרית שלי לגורם כלשהו, אפילו אם זה נעשה מרצוני החופשי ולמטרות מוצדקות, אני מאבד את השליטה בה ושוב איני יכול להבטיח שלא יעשה בה שימוש לרעה.

מן הראוי לציין כאן שאותם גורמים ורשויות המופקדים על הסדר הציבורי, בטחון הציבור ובטחון המדינה, עושים שימוש שיטתי ויום-יומי ביכולת הזיהוי של הפרט, ובהמשך לכך באיסוף מידע ומודיעין אודותיו, חקירתו וניתוחו, לשם השגת אותן מטרות ומשימות שעליהן הם מופקדים. אין חולק על כך שאלה הן מטרות ראויות אך הן נמצאות במתח מתמיד ומחייבות איזון הולם בין זכויות הפרט והבטחון האישי לבין אלו של הציבור והמדינה.

בעבר הלא רחוק נהננו מהעובדה שהזכרון האנושי ויכולות עיבוד המידע היו מוגבלים ואנו כפרטים יכולנו להטמע בהמון. ההתקדמות הטכנולוגית שהושגה (ועוד תושג) מאפשרת יכולות אגירה, אחזור, שילוב והצלבה, חקירה ואימות אדירות, שלא היו קיימות בעבר. בנית וניהול מאגרי מידע אודות אנשים הפכו להיות עסק כלכלי עצום ומשימה שלטונית ראשונה במעלה, וכיוון ש-"מידע הוא כוח" - הם גם מהווים מקור עצום של כוח ומוקד של אינטרסים הן לגורמים העסקיים והן לגורמי הממשל.

על פי העקרון האומר שמה שעלול לקרות אכן יקרה, והמשכו הפסימי של אותו עקרון, האומר שזה גם יקרה בנסיבות הקטסטרופאליות ביותר - יש לצפות ברמת ודאות גבוהה שאכן יעשה בטביעות הביומטריות שימוש לרעה וזה רק עניין של זמן ונסיבות כדי שהקטסטרופה אכן תתרחש. מדינה אחת משתלטת על רעותה, יחסים בין מדינות הופכים כיוון, שלטון מתחלף, חוקים משתנים, פקידי ממשל ואנשי שמירת החוק טועים, מתרשלים ומבצעים מעשי פשע ושחיתות, הנהלת החברה המסחרית מתחלפת ומשנה מדיניות, ומה שנעשה פעם בתום לב ומתוך כוונה טובה וחוקית יכול להפוך כיוון, ללא כל שליטה של הפרט והציבור.

3. הנחות יסוד:

א. טביעה ביומטרית היא מידע <u>אישי</u>

הטביעה הביומטרית היא אישית קודם כל משום שהיא ייחודית לאותו אדם ורק לו. היא גם מהווה מידע אישי כשהיא משויכת למידע אישי אחר כגון שם, תאריך לידה וכו', או שהיא מספקת קשר ישיר או עקיף למידע זה אודות אותו אדם, שזהו בד"כ המקרה במערכות יישומיות קונקרטיות. זה גם עולה במישרין מההגדרות המצויות בהנחיה (Directive) של האיחוד האירופאי[2] המהווה אבן יסוד מוכרת ובינ"ל לדיון בשאלות של פרטיות ואבטחת מידע.

ב. טביעה ביומטרית אינה מוגדרת (כיום) כמידע אישי שהוא רגיש

1) עפ"י ההגדרה החוקית - טביעה ביומטרית אינה מהווה מידע אישי רגיש כשלעצמה. למידע אישי רגיש אין הגדרה גלובאלית מחייבת אחת אך ההגדרה המקובלת בעולם אודות מידע אישי רגיש הנה, באופן כללי, נתונים אודות מוצאו הגזעי או האתני, דעותיו הפוליטיות, אמונתו הדתית, חברותו באיגודים מקצועיים, מצב בריאותו הפיזית והנפשית, חיי המין שלו ועבירות פליליות אותן ביצע או נחשד בביצוען[3]. חוק הגנת הפרטיות בישראל מוסיף על כך נתונים אודות אישיותו של אדם (כגון הערכות על תכונותיו האישיות), צנעת אישיותו, מצבו הכלכלי והכשרתו המקצועית; ואינו מתייחס למוצאו הגזעי או האתני וחברותו באיגודים מקצועיים[4]. מידע אודות מעמדו האישי של האדם (מידע דמוגרפי, כולל מספר זיהוי) בד"כ אינו נחשב למידע אישי רגיש.

2) שלא כמו מספר זהות (או מספר הביטוח הלאומי SSN בארה"ב, SIN בקנדה), שהוא כשלעצמו אמור לכאורה להיות חסר משמעות כלשהי (בפועל - הוא אינו חסר משמעות), סוגי ביומטריה מסוימים יכולים לספק מתוך הטביעה הביומטרית הגולמית נתונים אישיים נוספים אודות האדם, כגון: אודות מינו, גילו המשוער, מוצאו האתני, צבע עורו, קשרי המשפחה שלו, מצב בריאותו וההיסטוריה הרפואית שלו, בהריון, צורך אלכוהול או סמים ועוד.

ג. ביומטריה הנה אמצעי שמאפשר קישור למידע אישי רגיש

1) טביעה ביומטרית מאפשרת את הקישור בין אדם למידע אחר ונוסף אודותיו, כולל גם כמובן מידע רגיש. כל דיון בהקשר של כמה ואיזה פרטים אישיים האדם מוכן למסור לגורם כלשהו, או אלו פרטים נאגרים אודותיו במאגר מידע כלשהו, אינו רלוונטי דוקא לטכנולוגיה הביומטרית כי הטביעה הביומטרית כשלעצמה הנה אינדכס בלבד ואינה מכילה (למעט במקרים מסוימים) מידע שהוא בעל משמעות כלשהי. המידע המשוייך לחתימה הביומטרית הוא בד"כ זה שנמצא במחלוקת.

תכונה זו של הביומטריה אינה שונה מכל אמצעי זיהוי אחר, כגון מספר זהות.

2) מידת הרגישות של המידע הביומטרי אמורה להיות ביחס ישיר לרגישות של פריטי המידע המשוייכים לאותו אדם במאגר המידע. אולם הביומטריה הנה רגישה במיוחד כיוון שהיא מאפשרת באמצעותה את השיוך והקישור של מידע אחר ונוסף לאותו אדם, שהושג ממקורות אחרים ומאוחסן בבסיסי נתונים אחרים, גם אם לכאורה היא נלקחה ונאגרה מלכתחילה למטרות מוגדרות וחוקיות ושוייכה לפריטי מידע מוגבלים חוקיים ונאותים.

תכונה זו של הביומטריה אינה שונה מכל אמצעי זיהוי אחר, כגון מספר זהות.

3) הטביעה הביומטרית, כמו כל אמצעי זיהוי אחר, מאפשרת בקלות שימוש המוגדר כשימוש משני במידע. עצם היותה של הביומטריה בבחינת "מפתח" של גישה למידע נוסף אודות הפרט, מפריך את הכלל שבכל מידע שנמסר יעשה שימוש אך ורק למטרה שלשמה הוא נמסר (או "עקרון צמידות המטרה" שבחוק הגנת הפרטיות הישראלי[5]). לא ניתן להפעיל כלל זה על הביומטריה ולחליפין - לא ניתן להבטיח באופן מושלם שהוא אכן יקויים.

תכונה זו של הביומטריה גם היא אינה שונה מכל אמצעי זיהוי אחר, כגון מספר זהות.

ד. ביומטריה הנה גורם שמאפשר אבחנה או אפליה

רשימה כלשהי המבוססת על ביומטריה יכולה לשמש לצורך אבחנה או אפליה בין אלה שנמצאים ברשימה לבין אלה שלא, אפילו כשאינה מקושרת למזהה אחר כלשהו כגון מס' זהות או שם. כך למשל, ביישום המתאים, איני יכול להעביר למישהו אחר כרטיס שרכשתי לארוע ספורט באצטדיון אם מסרתי בעת הרכישה את הביומטריה שלי, אפילו מבלי שהזדהתי.

גם תכונה זו של הביומטריה אינה שונה מכל רשימה על פי אמצעי זיהוי אחר, כגון מספר זהות.

4. התכונות המיוחדות לטכנולוגיות הביומטריות

א. החתימה הביומטרית מועברת מהפרט לרשות

בכל שיטות הזיהוי האחרות הרשות היא המזהה, מגדירה ומעניקה לפרט (וברצונה גם שוללת) את האינדכס המזהה, כגון מספר תעודת זהות, מספר דרכון וכד'. בזיהוי ביומטרי החתימה הביומטרית מועברת, מרצון או בכפיה, בכיוון ההפוך - מהפרט אל הרשות. תכונה זו מהווה הבדל משמעותי ביחסים בין הפרט והרשות.

ב. היחודיות (Uniqueness) של הטביעה הביומטרית

ההנחה המונחת ביסודה של כל טכנולוגיה ביומטרית היא שלכל אדם יש טביעה ביומטרית שהיא ייחודית לו בלבד ואינה חוזרת על עצמה כלל. אחד הכיוונים העיקריים במאמצי הפיתוח של הטכנולוגיות הביומטריות לסוגיהן הנו המאמץ המתמשך להגדיל את הבידול ויכולת האבחנה שבין טביעה ביומטרית אחת לאחרת. אחד הפרמטרים בהם נעשה שימוש רווח להשוואת טכנולוגיות או להוכיח את עליונותה של טכנולוגיה אחת מול אחרת היא גודל בסיס הנתונים התיאורטי שבו לא תחזור טביעה ביומטרית על עצמה. יהיה זה הוגן לומר, כנקודת מוצא, שקיימות כיום טכנולוגיות ביומטריות שניתן באמצעותן לבדל בין טביעה אחת לאחרת מול בסיס נתונים שמכיל תיאורטית את כל האוכלוסיה האנושית על פני כדור הארץ לדורותיה - עד לשחר ההיסטוריה האנושית. יותר ויותר טכנולוגיות טוענות שהן כבר מגיעות ל-"הישג" זה או שהן עומדות להגיע אליו. יותר מכך - היה ונמצאה בבסיס הנתונים טביעה ביומטרית שהיא זהה לחלוטין לטביעה אחרת אך שיכת לכאורה לאדם אחר - המערכת אמורה עקרונית להתריע על חשש לשכפול או לזיוף. ולראיה - אחד היישומים הביומטריים הרווחים הנו זיהוי ומניעה של הרשמה כפולה, שבו נעשה שימוש אפילו לא בזהות מלאה אלא "רק" בדרגת דמיון מסוימת בין שתי טביעות ביומטריות, שדיה כדי להפיק התרעה על חשש להרשמה כפולה.

תכונה זו של הביומטריה מקנה מימד חדש למושג "ייחודיות" (Uniqueness) ומעניקה לה אבסולוטיות ועוצמה יתרה מול כל שיטות הזיהוי האחרות, הן במימדים הגלובליים שלה והן גם על ציר הזמן וההיסטוריה.

כל שיטה אחרת של הענקת מזהה ייחודי, כגון מספר כלשהו או שם, כאמצעי לזיהוי אדם, הנה מקומית ומוגבלת לאותה רשות או ארגון שהם הבעלים של המערכת והשיטה. כך למשל מספרי עובד במקומות עבודה שונים ומס' ת.ז. או דרכונים לאומיים של מדינות שונות. תכונת המקומיות של שיטות אלה פרושה

שהמזהה שנבחר הנו ייחודי (אם בכלל) אך ורק בתוך גבולות המערכת המקומית שבה הוא קיים. לכן מזהה זה יכול, תיאורטית ומעשית, לחזור על עצמו ולהצביע על אדם אחר בכל מערכת מקומית אחרת.

תכונת המקומיות של כל השיטות האחרות גם אומרת שבאין קשר (Link) והעברת מידע בין כל שתי מערכות מקומיות - מערכת אחת לעולם לא תדע על קיומו של אותו פרט אצל המערכת האחרת ולכן גם לא תוכל לזהות אותו כאותו פרט שמזוהה במערכת האחרת. דבר זה מעצים את החשיבות והמשמעויות הנובעות, לטוב ולרע, של שיתוף מידע בין מערכות שונות ושיתוף מידע בין רשויות שונות. המימדים הגלובליים של ייחודיות הטביעה הביומטרית מאפשרים גישור וקישור בין מערכות ומאגרי מידע מקומיים שלא נועדו מלכתחילה להיות מגושרים ומקושרים.

ישנה דוגמא, שמוזכרת לעיתים קרובות, אודות השימוש בטכנולוגיה ביומטרית וללא הזדהות מפורשת כאמצעי לשמירת האנונימיות של הפציינט במעבדות לבדיקות AIDS. באותה דוגמא בדיוק גם ניתן דוקא להפר את האנונימיות המובטחת, היה והרשויות יתחבו את ידן הארוכה אל בסיסי הנתונים של אותן מעבדות, תחת העילה המוצדקת לכאורה של שמירה על בריאות הציבור.

המגמה הגוברת והולכת בעולם לסטנדרטיזציה של המזהים הביומטריים מעודדת גלובליזציה, חופש תנועה ופעילות כלכלית וחברתית, אך באותה עת היא גם מגבירה את האיום בפוטנציה, ואת המוטיבציה בפועל, להשתלט על מאגרי מידע ביומטריים שנועדו מלכתחילה להיות מקומיים ולמטרות מצומצמות באופיין. מגמה זו גם מגבירה את היכולת לזהות אדם ולעקוב אחריו בכל העולם. אין מפלט לגולים ונרדפים פוליטיים, אי אפשר לותר על אזרחות או להסתיר אותה. בשיטות המשפטיות הנהוגות במדינות רבות, כולל בישראל, אין אפשרות חוקית לגרש אדם מהארץ כאשר זהותו וארץ מוצאו אינם ידועים בודאות - זיהוי ביומטרי על בסיס גלובלי ימנע אפשרות מפלט כזו, לטוב ולרע.

תכונה נוספת של ייחודיות הטביעה הביומטרית היא שהיא מייצרת זהות אחת ויחידה למטרות רבות (Multi-purpose identity credential) בעוד שאנשים בד"כ מעדיפים שיהיו להם מספר זהויות שונות למטרות שונות, כגון Nicknames באינטרנט. דבר זה מתקשר לשאלה האתית/פילוסופית מהי זהות והאם לאדם יש בכלל זהות אחת ויחידה. מרבית האנשים מעדיפים בד"כ לשמור על מידה של הבדל בין זהויותיהם השונות מול הפעילויות והתפקידים החברתיים השונים שלהם: האם המעביד (בסביבת העבודה) או מנהל הבנק (בסביבה הפיננסית) אמור לדעת שאני גם הומוסכסואל (בסביבת ההעדפה המינית שלי) ובעל דעות סוציאליסטיות (סביבה פוליטית) או אמונה בודהיסטית (סביבה דתית)? אין זה סביר שלצרכי פעילות מסוימת אדם יגיש את אצבע יד ימין שלו ולצרכי פעילות אחרת יגיש את אצבע יד שמאל.

ג. חודרנות

יהיו רבים שיאמרו שכל סוג של איסוף מידע שהוא אישי למאגר מידע מהווה מידה של חודרנות לתחום הפרטי והאינטימי של הפרט. הטכנולוגיות הביומטריות, בנוסף לרמה מופשטת זו של חודרנות, שונות ומיוחדות בכך שיש בשימוש בהן רמה עמוקה בהרבה של חודרנות, עד לרמה הפיסית של חודרנות לגוף האדם. ניתן לייחס לטכנולוגיות הביומטריות השונות מידה שונה של חודרנות: החל בחודרנות במשמעות של צילום איבר כלשהו בגוף האדם שנעשה מרחוק וללא מגע, כמו בצילום פנים; עבור לצילום ממרחק קצר, כמו

במקרה של קשתית העין; עבור לצילום, או רכישת נתונים מסוג אחר כגון אולטרסאונד, שנעשה מתוך מגע פיסי של האיבר עם אביזר כלשהו, כמו בטכנולוגיות של טביעת אצבע וגאומטרית כף-יד, וכלה בלקיחת דגימה פיזית מגוף האדם - שערה, דגימת רוק ודגימת ריקמה חיה. בנוסף לכך יש מידה שונה של חודרנות כאשר תהליך ההרכשה של הטכנולוגיה הוא פסיבי, כמו למשל בצילום רגיל, או אקטיבי שבו מעורבת הארה אקטיבית מסוג כלשהו (הארה בתדר הנראה הרגיל, בתדר אינפרא אדום וכד'). אין ספק שלמידת החודרנות המתלווה לטכנולוגיה יש השפעה על מידת הרגישות שיש ליחס לשימוש בה.

ד. אי יכולת העברה לאחר

בשיטת זיהוי ביומטרית לא ניתן להעניק את אותה "חתימה" ביומטרית לאדם חדש שנולד, לאחר שאותה חתימה "היתה בשימושו" של אדם שהלך לעולמו, או להעביר אותה לאדם אחר, קרוב משפחה וכד', כפי שניתן לעשות עם סיסמת הגישה או כרטיס הזיהוי. כך למשל יש לתת את הדעת לאותם מקרים בהם אדם שעשה שימוש בבקרת גישה ביומטרית למשאבים שונים, בעיקר ממוחשבים, הלך לעולמו ויורשיו וקרובי משפחתו לא יכולים לגשת אפילו לרשימת אנשי הקשר שלו שבמחשב כדי להזמינם ללוויתו, שלא לדבר על גישה לתכתובת הדוא"ל המקוונת, לחשבונות כספיים ונכסים מוחשיים אחרים כגון כספת.

ה. לא לכל אדם יש טביעה ביומטרית (פרקטית)

ברמה הפרקטית לא כל בני האדם יכולים למסור טביעה ביומטרית מסוג מסוים, כגון טביעות אצבע לשחקני כדור-סל, קשתית העין לאנשים עם מחלות עיניים, זיהוי פנים לנשים רעולות פנים וכד'. יש לתת את הדעת לאותו חלק באוכלוסיה שאינו יכול לספק (Failure to enrol) את הטביעה הביומטרית התקנית שנקבעה ע"י הרשות או בחוק. גם יש לתת את הדעת למתקנים התיקניים להרכשת הטביעה הביומטרית כך שיהיו מתאימים לנכים ומוגבלים כך שלא יסבלו מהעדר ההטבות השמורות לאלה שנרשמו בהצלחה וגם לא יועמדו כל פעם מחדש במצב מביך בכל עמדת בקרה.

ו. פגיעה בבסיס נתונים ביומטרי

המשמעות של פגיעה בבסיס נתונים ביומטרי הנה דרמטית מעבר לכל פגיעה בבסיס נתונים אחר. פגיעה בבסיס נתונים כלשהו יכולה להיות מסוגים שונים ולהתרחש בתסריטים שונים: אסון טבע, תקלה טכנית, שיבוש של אינדכסים, מחיקה/שינוי של רשומות או שדות ברשומות, הגעת בסיס הנתונים כולו או חלקו לידיים לא מורשות ועוד. כל אלה יכולים להתרחש במקרה, מתוך רשלנות או מתוך כוונת זדון. המיוחד שבבסיס נתונים ביומטרי הוא שפעם שנפגע - סוגי נזק מסוימים אי אפשר לשקם בדרכים המקובלות. בסיס נתונים המבוסס על סיסמאות שנפגע - ניתן לבחור סיסמה אחרת. בסיס נתונים ביומטרי שהשתבש - יש קושי גדול לשחזר אותו. גם אין לנו מספיק אצבעות או פרצופים להחלפה ובמקרה של מידע ביומטרי שהגיע לידיים הלא נכונות שוב אי אפשר להחזיר את הגלגל לאחור ולתקן את הנזק. נזק מסוג זה הוא מוחלט, סופי ולאורך זמן בלתי מוגבל.

ז. מסירת מידע ביומטרי אינה ניתנת לביטול

טביעה ביומטרית, פעם שנמסרה, אינה ניתנת להתחרטות ולביטול במשמעותם הרגילה. כל אמצעי זיהוי אחר שהונפק ושוייך לאדם ניתן לביטול ואפילו להתעלמות. אדם יכול להשמיד תעודת זהות שניתנה לו או

לשכוח סיסמה שנמסרה לו. אדם לא יכול להתכחש לטביעה הביומטרית שלו. מסירת טביעה ביומטרית, לכל צורך שהוא, הנה לכל החיים.

התעשיה הביומטרית ככלל מתאמצת להוכיח שהמזהים הביומטריים אינם מתיישנים (Do not Age) ואינם משתנים לאורך השנים וכי טביעה ביומטרית שנלקחה במועד מסוים או בגיל מסוים הנה תקפה לתקופה ארוכה. קיימים הבדלים בנושא זה בין הטכנולוגיות השונות ויש כאלה שטוענות לאורך חיים בלתי מוגבל ואחרות שדורשות רענון של הטביעה הביומטרית אחת לתקופה.

גם המושג "לכל החיים" מקבל כאן משמעות אחרת כי הוא יכול להיות תקף גם לאחר המות (למשל - השימוש במזהים ביומטריים לצורך זיהוי חללים במקרים של אסון המוני). ניתן רק לדמיין אלו אפשרויות היו נפתחות עבורנו לו היה למשל בידנו מאגר המידע הביומטרי של אבותנו, ומה זה היה עושה לחקר ההיסטוריה, האנטרופולוגיה, הארכיאולוגיה, המחקר על התפשטותן ותפוצתן של מחלות מגפות ושינויים גנטיים.

מאגר מידע ביומטרי יכול לקשר, באופן שהוא בלתי ניתן לשינוי וערעור, את הקשר שבין ילד להוריו ומשפחתו, ולכל השושלת המשפחתית לדורותיה, המוצא האתני והמעמד החברתי/דתי/לאומי. איזו עוצמה וכלים זה יכול לתת למשטרים חברתיים המבוססים על בידול לפי מעמדות חברתיים, אפליה על רקע גזעי, דתי וכד'. איזו מגבלה עצומה זה יכול להטיל על הניידות החברתית, על שוויון ההזדמנויות, על היכולת להמיר את דתך, לשנות את אמונותיך ואת קבוצת השתייכותך. כמה חוקים חברתיים אנו מכירים שעושים שימוש בזהותו של האב/אם והסב/סבתא? מה היה קורה אם בימי השלטון הנאצי שעלה, אגב, לשלטון באמצעים דמוקרטיים, היה קיים מרשם אוכלוסין מבוסס ביומטריה בכל המדינות שנדרסו ע"י המגף הנאצי?

ח. טעות מערכת ובטחון במערכת

ספקי הטכנולוגיות הביומטריות השונות מתחרים בינהם ומתהדרים בדרגת דיוק גבוהה והולכת. למעשה זו השאלה העיקרית כמעט שנשאלת ונבחנת במודלים שונים של מבדקים, תחרויות ספקים ותקנים בינלאומיים. כתוצאה מכך נבנית והולכת מידה רבה של אמון בביצועי המערכת, עד כדי אמון עיוור. המשפט "המערכת אינה טועה" הוא וריאציה על המשפט המוכר "המחשב אינו טועה". ובכל זאת, בכל טכנולוגיה ביומטרית שהיא יש שעור כלשהו של טעויות מסוגים שונים ושנגרמות מסיבות שונות, כולל אותם מקרים בהם אנשים אינם יכולים להזדהות כלל בטכנולוגיה מסוימת, באופן זמני או קבוע. כיצד אנו מתגוננים, מבחינה תפעולית (Operational) ומבחינה חברתית, מפני טעויות מערכת והנזק שהן עלולות לגרום, אפילו אם המדובר במקרים בודדים יחסית? האם הנהלים והפרוצדורות להתמודדות עם חשש לטעות, או טענה לטעות, הנם מספקים? ועל מי מוטל נטל ההוכחה? מה היכולת של אדם להגן על עצמו מפני טעות זיהוי ביומטרית הנחשבת לכל כך אמינה ובטוחה, ולהוכיח שזו טעות? דוקא העוצמה של הטכנולוגיה היא המסוכנת כל כך משום שהיא נותנת תחושה מוגזמת של אמינות סופית ומוחלטת. וכיצד זה עלול להשפיע על כבוד האדם, האפשרות של השפלתו או גרימה למבוכתו בפרהסיה, חירותו וזכותו למניעת אפליה על בסיס שאינו רלוונטי?

בגלל תכונה זו של הטכנולוגיה (בין היתר), שהיא סטטיסטית באופיה, המפתחים של מערכות ביומטריות יישומיות חייבים גם לקחת בחשבון את יתירות (Redundancy) המערכת ואפשרויות המעקף שלה

(Bypass) במקרה של כשלון מערכת מסיבה כלשהיא. מקרה פשוט יחסית הוא המקרה שאדם אינו יכול לגשת למכונית היוקרה שלו בגלל שריטה באצבע. מקרה מורכב יותר הוא כאשר בקרת הגישה לאספקה ממוכנת של תרופות של מרשם קבוע הנה מבוססת ביומטריה.

לחלק מהטכנולוגיות הביומטריות גם אין "גבוי אנושי" זמין למקרה של חשש או טענה לטעות. יש הבדל בהתמודדות עם טעות בטכנולוגיה של זיהוי פנים לבין התמודדות עם טעות בזהוי בטכנולוגיה של קשתית העין. כל בני האדם נולדו עם היכולת המובנית לזהות פרצוף אנושי בדרגת דיוק גבוהה יחסית אך לצורך ההשוואה בין שתי טביעות אצבע או שתי קשתיות עין קיימים מומחים מעטים בלבד ונדרשות לכך מעבדות וציוד מיוחד, שלא לדבר על השוואת טביעות DNA. ומי הם האנשים שאנו מעמידים בחזית של ההתמודדות עם מקרים כאלה, מה הסמכויות שאנו מעניקים להם לעקוף את החלטת המערכת ומה רמת ההכשרה והמיומנות שלהם?

ט. טכנולוגיות שמשאירות עקבות

חלק מהטכנולוגיות הביומטריות משאירות עקבות במקומות ובתרחישים שונים, שניתן באמצעותן לעקוב אחר התנהלותו (Whereabouts) של אדם מבלי ידיעתו ומבלי שתהיה לו כל שליטה על כך. השימוש בטביעת אצבע שנמצאה במקום הפשע לצורך החשדתו ולביסוס הרשעתו של אדם הנו שימוש ותיק ומוכר בזירה הפלילית. אך יש לקחת בחשבון שגם ניתן להחשיד ואף להפליל אדם שהוא חף מפשע על ידי השתלת טביעת האצבע שלו, שהועתקה ללא ידיעתו מכוס המשקה שלו, בזירה של רצח. ובאופן דומה גם ניתן לעשות שימוש בטכנולוגיה של DNA.

הטכנולוגיה של זיהוי פנים מאפשרת ביצוע סריקה נסתרת על תנועותיו של אדם או על נוכחותו במקום מסויים ובמועד מסויים. העולם בו אנו חיים הולך ונעשה רווי יותר ויותר במצלמות וידאו המותקנות באופן גלוי או נסתר. גם הטכנולוגיה של זיהוי דובר (Speaker recognition) הנה מהסוג שמשאירה עקבות וגם אחד מהכיוונים של מאמצי הפיתוח המתקדמים המתבצעים כיום הוא לאפשר דגימה של קשתית העין מרחוק.

שימוש נרחב בטכנולוגיות ביומטריות שמשאירות עקבות עלול להוות תמריץ לפגיעה גורפת בזכות לפרטיות ובזכות לאי-הפללה עצמית (Self incrimination) והוא מרוקן מתוכן את העיקרון של "הסכמה מודעת".

י. דגימה ביומטרית גולמית מול החתימה הדיגיטאלית שלה

כל הטכנולוגיות הביומטריות רוכשות טביעה ביומטרית גולמית מסוימת (Image/Raw) וממירות אותה, לצורך פעולת ההשוואה הביומטרית, לתבנית דיגיטלית כלשהי (Template). טכנולוגיות ביומטריות מסוימות, ולעיתים הדבר תלוי באופן היישום של מערכות ביומטריות קונקרטיות, מאפשרות את שמירת הטביעה הביומטרית בגרסת התבנית הדיגיטלית שלה בלבד, ללא צורך בשמירת הטביעה הגולמית, וגם ללא יכולת של שחזור לאחור של הטביעה הגולמית מתוך התבנית שנשמרה. מובן מאליו שטכנולוגיה, או מערכת, המבוססת על תבניות דיגיטליות בלבד הנה רגישה פחות ממערכת השומרת בבסיס הנתונים את הטביעה הגולמית כפי שנרכשה במקור. וככל שהתבנית הנה יותר ייחודית לאותו יישום (פחות סטנדרטית) כך גם פוחתת הרגישות שמה יעשה בה שימוש שאינו ראוי. יצויין שעקרונית ניתן להצפין, הן את הטביעה הגולמית

והן את התבנית הדיגיטלית שלה (כמו כל מערכת זיהוי שאינה ביומטרית), ובכך לספק מנגנון של הגנה מפני השימוש הבלתי ראוי בהן.

5. סוגי טכנולוגיות ביומטריות ומידת רגישותן

לא כל הטכנולוגיות הביומטריות עשויות ממקשה אחת ויש לטכנולוגיות שונות, ולעיתים גם לאופן היישום הקונקרטי של המערכות המבוססות עליהן, תכונות תפעוליות שונות המקנות להן מידה שונה של רגישות בהיבטים שנדונו כאן. התכונות התפעוליות הללו כוללות את הפרמטרים שלהלן:

- טכנולוגיה/מערכת הפועלת (או מאפשרת לפעול) באופן גלוי וביודעין, או באופן סמוי ושלא ביודעין
- טכנולוגיה/מערכת הפועלת עם או בלי שיתוף פעולה אקטיבי ומרצון של הנבדק
- מערכת השומרת את הטביעה הביומטרית הגולמית, או את רק הייצוג הדיגיטאלי שלה
- מערכת מחליטה או מערכת ממליצה
- האם יש לטכנולוגיה או אין לה גבוי אנושי זמין
- אורך החיים של הטביעה
- האם הטכנולוגיה/המערכת היא כזו שמשאירה עקבות או לא
- מתבצעת בזמן אמיתי או בדיעבד ב-Offline
- מידת החודרנות (המעשית וזו הנתפסת) של אופן הרכשת הטביעה הביומטרית
- האם הטביעה הביומטרית היא "שקופה", או מכילה נתונים נוספים אודות האדם ממנו נלקחה.

להלן מספר אבחנות בתחום זה:

א. אימות זיהוי וסריקה

נהוג לחלק את מודי הפעולה של המערכות הביומטריות לשלושה סוגים עיקריים:

1) מוד <u>אימות</u> (Verification) - מוד בקרה שבו האדם מבקש לקבל פריבילגיה כלשהי בגלל מי שהוא טוען שהינו והמערכת הביומטרית מאשרת או שוללת את הזהות הנטענת. בעגה המקצועית מוד זה מכונה השוואה של "אחד לאחד" (1:1) כיוון שמהערכת שולפת מבסיס הנתונים רק את הטביעה הביומטרית המסוימת של אותו אדם, שמאותרת בבסיס הנתונים לפי אמצעי זיהוי אחר, למשל - מספר הזהות או השם הנטען, ומשווה אותה לטביעה הטריה הנרכשת במעמד תהליך הבקרה. מוד זה הוא המוד השכיח במערכות ביומטריות שנועדו למכן, לזרז ולהבטיח את השלמות (Integrity) של תהליך בקרה, בעיקר ביישומים אזרחיים של בקרת גישה (Civil Access Control). הפעולה במוד אימות מתבצעת תמיד בזמן אמיתי, ביודעין, תוך שיתוף פעולה אקטיבי מצד הנבדק ומרצון, ובכך היא מזכירה את שיטות הזיהוי המסורתיות לפי מה שיש לי או לפי מה שאני יודע. לכן גם מוד זה הנו הרגיש פחות והמסוכן פחות מיתר מודי העבודה, בהקשר של אפשרות השימוש הבלתי ראוי.

2) מוד זיהוי (Identification) - מוד פעולה שבו שום זהות אינה נטענת (Claimed) מלכתחילה וגם אם נטענת - אין מתחשבים בה. המערכת הביומטרית רוכשת טביעה ביומטרית טריה במקום הארוע, מריצה אותה להשוואה מול כל הרשומות שקיימות בבסיס הנתונים ומחזירה תשובה של זיהוי, או מועמדים לזיהוי (עם רמות הסתברות), או שאין זיהוי. בעגה המקצועית מוד זה מכונה השוואה של אחד לרבים (1:M) כיוון שהמערכת מבצעת ריצת השוואה של רשומה ביומטרית אחת מול כל אלה שבמאגר. מוד זה הנו המוד העיקרי ביישומים של זיהוי פלילי (Forensic Identification) וכן גם ביישומים של זיהוי נעדרים או כאלה שהם חסרי יכולת להזדהות. מוד פעולה זה משמש גם, לעיתים, בתהליך ההרשמה הראשונית לאותן המערכות שפועלות בשגרה במוד אימות, כשהמטרה שם היא לאתר נסיונות להרשמה כפולה. הפעולה במוד זיהוי יכולה להתבצע בזמן אמיתי או בדיעבד ב--Off line, ביודעין, בשיתוף פעולה מרצון וגם בכפיה, אך גם שלא ביודעין וללא שיתוף פעולה, באותן טכנולוגיות שמשאירות עקבות. בנוסף לכך - המענה של המערכת יכול להיות לא חד-משמעי ומחייב מעורבות והחלטה אנושית, לעיתים של מומחה בלבד. לפיכך מוד פעולה זה הנו רגיש מאד בהקשר של אפשרות השימוש הבלתי ראוי.

3) מוד סריקה (Surveillance) - מוד פעולה שבו מערכת ביומטרית מחפשת ברצף, בקרב כל האנשים המופיעים בגזרת העבודה שלה, מופע של אדם שהיא מזהה כמצוי ברשימת המעקב שלה ומנפקת למפעיל המערכת התרעה על זיהוי או מועמדים לזיהוי. מוד זה מכונה בעגה המקצועית השוואה של "רבים למעטים" (Many to Few) כאשר המערכת מבצעת ברצף השוואה של רשומות ביומטריות רבות מאד, של הקהל העובר בגזרת אמצעי ההרכשה, מול רשימה קטנה יחסית של רשומות שבמעקב, בבסיס הנתונים. סוג זה של מערכות משמש בעיקר ליישומי בטחון, סיכול ומודיעין, אך יכול גם לשמש לצרכים "אזרחיים" של קבלת התרעה מוקדמת על בואו של אורח חשוב או פתיחת הדלת מבעוד מועד למורשים. הפעולה במוד סריקה יכולה להתבצע בזמן אמיתי או בדיעבד ב- Off-line, ביודעין או שלא ביודעין, בהסכמה או בלעדיה, עם או בלי שיתוף פעולה, והיא גם מתבצעת לאורך זמן, מול אוכלוסיות נרחבות ובמקומות פומביים, בתוכן אוכלוסיות שהגיעו לגזרת הפעולה לשם תכלית כלשהי וכאלה שנקלעו לשם באקראי, ללא כל אבחנה. לפיכך זהו מוד העבודה הרגיש והמסוכן ביותר, יחסית לאחרים, בהקשר של אפשרות השימוש הלא ראוי במערכת.

ב. תמצית התכונות התפעוליות של הטכנולוגיות הביומטריות הנפוצות

להלן רשימה לא ממצה של תכונות תפעוליות של הטכנולוגיות הנפוצות, לפי סדר יורד של הרגישות הפוטנציאלית שלהן לאפשרות של שימוש בלתי ראוי. ברשימה הממוינת שלהלן מקופלת הנחת יסוד שכל הטכנולוגיות הנמנות כאן כבר הגיעו, או יגיעו עם הזמן, לבשלות טכנולוגית בפרמטרים של דיוק והגודל הפרקטי של בסיסי הנתונים מולן הן פועלות:

1) טכנולוגיה של זיהוי פנים - מאפשרת את כל שלושת מודי הפעולה של אימות, זיהוי וסריקה. משאירה עקבות ויכולה להתבצע בזמן אמיתי, קרוב לזמן אמיתי ובדיעבד (ע"י הקלטת וידאו או שמירת התמונות שנרכשו בבסיס הנתונים, בצרוף חתימת זמן ומקום). יכולה להיות גלויה אך גם יכולה להיות מוסלקת וסמויה, עם או בלי שיתוף פעולה מרצון. הטביעה מתיישנת (Aged) עם הזמן בתדירות של

מספר שנים (אך לא מאבדת לגמרי את יכולת ההשוואה), יש לטכנולוגיה גיבוי אנושי פשוט וזמין. בנוסף, הטביעה הגולמית של זיהו פנים מכילה בתוכה פרטים נוספים אודות האדם - כגון מוצא אתני, צבע עור, גיל משוער, מין ועוד. הטכנולוגיה אינה נחשבת כחודרנית ויצויין גם שבגרסתה הטרום-ביומטרית (השוואה אנושית של הנבדק מול תמונתו) היא מקובלת בציבור, מזה דורות, כאמצעי העיקרי לזיהוי אדם.

2) טכנולוגיה של DNA - פועלת במוד זיהוי בלבד, כיום בדיעבד וב-Off-Line אך בזמני תגובה שמתקצרים והולכים, מחייבת גבוי והחלטה אנושיים של מומחה ובתנאי מעבדה, כוללת מידה רבה או מעטה של חודרנות (לפי טכניקת ההרכשה), יכולה להתבצע ביודעין בהסכמה ובשיתוף פעולה וגם באופן סמוי, ללא שיתוף פעולה וללא ידיעה והסכמה. הטביעה הגולמית אינה מתיישנת ומכילה את המידה הרבה ביותר של נתונים נוספים אודות הפרט, כולל היסטוריה של מחלות ומצב בריאותי, קשר (או שלילתו) לקרובי משפחה, מוצא אתני ועוד, כולל גם נתונים שכיום עדיין לא מובנים דים וכנראה יתבררו יותר בעתיד.

3) טכנולוגיה של טביעת אצבע (וכף-יד) - פועלת במוד אימות ובמוד זיהוי, בזמן אמיתי, קרוב לזמן אמיתי ובדיעבד. יכולה להתבצע ביודעין בהסכמה ובשיתוף פעולה וגם באופן סמוי, ללא שיתוף פעולה וללא ידיעה וללא הסכמה. משאירה עקבות, הגבוי האנושי שלה מתבצע ע"י מומחה ובתנאי מעבדה. אינה נחשבת לחודרנית אך מחייבת מגע פיזי עם אביזר ההרכשה וכוללת הארה של האצבע בתחומי תדר שונים, הטביעה הגולמית מתיישנת כעבור שנים וכמעט ואינה כוללת נתונים נוספים אודות הפרט ממנו נלקחה.

4) טכנולוגיה של קשתית עין - פועלת בעיקר במוד זיהוי (אך אפשרית גם באימות). פועלת בזמן אמיתי, מחייבת שיתוף פעולה ביודעין ע"י הנבדק ולא אפשרית בכפיה ישירה. הטביעה הגולמית אינה מתיישנת וכמעט ואינה כוללת נתונים נוספים אודות הפרט ממנו נלקחה (למעט אודות מחלות עיניים). אינה נחשבת לחודרנית למרות שהמימוש הפרקטי שלה כולל הארה של העין באור אינפרא אדום. ברמה הפרקטית אין לה גבוי אנושי. מתקיים כיום מאמץ פיתוח לאפשר בטכנולוגיה שימוש מרחוק.

5) טכנולוגיה של גאומטרית כף-יד - פועלת במוד אימות בלבד, בזמן אמיתי, מחייבת שיתוף פעולה ביודעין ובהסכמה, אינה נחשבת לחודרנית אך מחייבת מגע פיזי עם אביזר ההרכשה וכוללת הארה של כף היד בתחום האור הנראה, מכילה מנגנון "למידה" שמפצה על שינויים לאורך הזמן, אין לה גבוי אנושי, שומרת רק את החתימה הדיגיטלית של הטביעה הגולמית ואינה ניתנת לשחזור. אינה כוללת נתונים נוספים אודות הפרט.

6. סיכום

משפחת הטכנולוגיות הביומטריות שונה מכל יתר השיטות המשמשות לזיהוי אדם. אמנם יש לה מספר תכונות במשותף עם טכנולוגיות ושיטות זיהוי אחרות אך גם יש לה מספר תכונות שייחודיות רק לה.

הביומטריה היא טכנולוגיה שהציבור הרחב אינו מכיר ומבין דיו. לא בכדי היא גורמת להתנגדות אינסטינקטיבית בשדרות רחבות של הציבור. הכרת הטכנולוגיה, על עוצמתה, יתרונותיה וחסרונותיה, תשנה את התפישה שלנו אודות שיטות ואמצעים לזיהוי אדם.

הרגישות והחשש האינסטיקטיביים של הציבור מפני הטכנולוגיות הביומטריות הביאו חלק ממקבלי ההחלטות ברשויות ממשל שונות לקצר את הדרך ולעקוף את התהליכים החוקתיים והדיון הציבורי הנדרש בנושא; וזאת על ידי הקמה של מערכות המבוססות על הרשמה וולונטרית, תוך יצירת הפיתוי שמי שמסכים להרשם למערכת יקבל בשל כך הטבות אלה או אחרות, כגון קיצור תורים וטיפול VIP. בכך משמשת הביומטריה כאמצעי המפלה בין אלה שמוכנים למסור את הטביעה הביומטרית לבין אלה שלא מוכנים, מבלי שהציבור מודע לסיכונים שהוא נוטל על עצמו. מה עוד שבחלק ניכר מהמקרים הללו זוהי חובתה הבסיסית של אותה רשות לתת לכלל הציבור את השירות הטוב ביותר וללא אפליה. בחלק מהמקרים הרשויות אפילו מורידות את רמת השירות לאלה שאינם רשומים במערכת, כאמצעי לחץ או סתם כדי להצדיק את קיומה של המערכת.

אותה טכנולוגיה יכולה לשמש בו-זמנית הן להגנה והן להפרה של הפרטיות, חופש וזכויות הפרט, כבוד האדם, הזכות לבטחון אישי והדמוקרטיה. לכל מאפיין בנפרד של הטכנולוגיות הביומטריות יש עוצמה משלו, עם היבטים חיוביים ושליליים. השילוב של המאפיינים הללו עוד מגביר בהרבה עוצמה זו, לטוב ולרע. מאגר מידע ביומטרי מהווה מידע רב-עוצמה. וככל שהוא רב עוצמה יותר כך גדל גם הפיתוי והסכוי שיעשה בו שימוש לא ראוי.

הייחודיות המוחלטת של הביומטריה מצד אחד וחוסר המודעות לסיכונים שהיא טומנת בחובה מצד שני, מקשים על היכולת להקים מערכות שהן פרופורציונאליות ומתאימות למטרתן בלבד. מבחינת רגישותן לאפשרות של שימוש לא ראוי - לא כל הטכנולוגיות הביומטריות נחנו באותן תכונות ואין להתייחס אליהן כאל מקשה אחת.

יש לאמץ, בהקשר של טעויות מערכת, את המונח "Graceful Degradation" בכל הקשור לתכנון והגדרת הדרישות במצבי הכשל הצפויים בכל מערכת ביומטרית יישומית, כולל גם את הנהלים והפרוצדורות שיש לפתח להדריך ולהטמיע בקרב המשתמשים שלה, מנהלי המערכת והמפקחים האנושיים שלה שבחזית.

הביומטריה מאפשרת לחצות בקלות גבולות של מדינות ומערכות משפטיות שונות. כבוד האדם וזכותו לחופש בטחון ופרטיות הנם זכויות בעלות אופי חוצה גבולות וגלובלי אך מדינות מסוימות מיישמות מערכות ביומטריות שמכוונות לקהל יעד שאינו האזרחים שלהן עצמן - מהגרים, עובדים זרים, מבקרים ואנשי עסקים, באופן שהוא שונה מיישומן מול אזרחיהן שלהן.

האם מקבלי ההחלטות מודעים לרמות הסיכון השונות הגלומות בטכנולוגיות הביומטריות השונות ובוחרים את הטכנולוגיה המתאימה לצורך מתוך איזון בין המטרות והסיכונים? האם המאמץ להגן על החברה במסגרת של המלחמה בטרור הבינ"ל ולסיכול סוגי פשיעה אחרים מצדיקים ונמצאים בפרופורציה עם הסיכונים להם נחשף הציבור בהקשר של פגיעה בפרטיות, פגיעה בחופש ובאוטונומיה האישית ובכבוד האדם ובדמוקרטיה? האם אין אנו סוללים את הדרך למדינה טוטליטרית (באמצעים דמוקרטיים)?

הביומטריה דומה במידה מסוימת לאנרגיה אטומית: יש בה הרבה תועלת אבל אם היא תפול ליידים הלא נכונות היא עלולה להיות הרסנית. האם יש לנו אמצעי שמירה נאותים? האם חוקקנו, עיצבנו ובנינו את מנגנוני ההגנה שנדרשים

כדי להגן מפני העברת מידע לא ראויה או מוצדקת בין מערכות ורשויות שונות? האם הקמנו מנגנוני אבטחה והשמדה עצמית במקרה של השתלטות עוינת או שכשפג תוקפה של העילה לשיתוף המידע מלכתחילה? האם מערכות ההגנה והאבטחה שאנו מקימים לטובת מאגרי מידע לאומיים ובינ"ל מתקרבים בעוצמתם לאלה שאנו מקימים מול איומים לאומיים ובינ"ל אחרים שהם בעלי עוצמה ופוטנציאל דומים?

ולסיום - תחומי האתיקה והחקיקה בנושא לוקים גם הם בחסר וחסרות לנו המשגות והגדרות שיתנו מענה הולם לרגישות הנודעת לשימוש בטכנולוגיות ביומטריות. נראה שיש לבחון את הכללת מידע ביומטרי, במסגרת החוק, כמידע אישי רגיש.

---

[1] רשומות, הצעת חוק הממשלה, סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף החשוד) (תיקון) (נטילת אמצעי זיהוי ומאגר נתוני זיהוי) התשס"ד-2004

[2] Directive 95/46/EC, Article 2 - Definitions, "For the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

[3] UK Data Protection Act 1998 Chapter 29, Means personal data consisting of information as to:
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

[4] חוק הגנת הפרטיות תשמ"א-1981 סעיף 7

[5] חוק הגנת הפרטיות תשמ"א-1981 סעיף 2 (9)