



נובמבר 2009

## תיעוד ומאגר מידע ביומטרי – הצורך והמשמעויות

הצעת החוק "הכללת אמצעי זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע" כורכת תיעוד לאומי מתקדם, הכולל גם אלמנטים של זיהוי ביומטרי, יחד עם הקמתו של מאגר מידע ביומטרי של כלל תושבי המדינה. המדובר במאגר מידע נרחב, מרכזי, שיכיל את כל המידע הביומטרי (טביעות אצבעות ומתאר פנים ביומטרי) שיירכש מכלל תושבי המדינה ("המאגר הביומטרי").

הנקודות להלן מסכמות, בקיצור רב, עמדה מקצועית בנושא. עמדה זו, יש לציין, בהבדלים מינוריים, משותפת לכל המומחים בישראל (וגם מומחים מובילים בעולם) בתחומי אבטחת המידע, הפרטיות ותחומים משיקים (למעט, כמובן, אלה המועסקים ע"י מקדמי החוק).

### 1. תיעוד ממשלתי משופר הוא הכרחי, תיעוד ביומטרי (ללא מאגר מרכזי) הוא רצוי

שיפור התיעוד הממשלתי כדי שיהיה עמיד בפני זיוף הוא כורח מציאות, במיוחד בהתייחס למצב התיעוד כיום. זיהוי חזק בתיעוד ממשלתי כזה הוא רצוי, וראוי להכליל שימוש בפרמטרים ביומטריים לזיהוי, באותם מסמכי זיהוי רשמיים שכיום כוללים תמונה.

יש לשים לב כי שימוש בביומטריה איננו פתרון קסם לכל הבעיות, ויש בו כשלים פוטנציאליים רבים. יישום תיעוד ביומטרי חייב להיעשות בזהירות, תוך שימת לב לכשלים אלה.

לעיתים קרובות מקובל להתייחס לאלמנט הדיוק הטכנולוגי – False Accept או False Reject וכיוצא בזה. אך זהו איננו האלמנט הרגיש ביותר ובוודאי לא היחיד. נקודות קריטיות ליישום הן –

א. תהליך ההרכשה. על תהליך זה נשענת אמינות המערכת כולה. אם בנקודה זו מתבצעת הונאה של המערכת ביחס לזהות האדם שמסר את הנתונים, הרי ששום טכנולוגיה לא תתקן תקלה זו בהמשך.

ב. נקודת הבחינה. הדרך בה מופקים האלמנטים הביומטריים שנבדקים מול הנתונים השמורים היא קריטית. למרות הדיוק העקרוני בטכנולוגיות, שהוא גבוה יחסית, קל מאד להונות מערכות בדיקה ביומטריות מסוימות, לעיתים באמצעים ביתיים פשוטים. ארכיטקטורת מערכות הבדיקה צריכה להיות כזו שתמנע או לפחות תצמצם את האפשרות להתקפות כאלה, שאם לא כן אין ערך למערך הביומטרי – ולמעשה, יש בו נזק גדול.

### 2. אין תלות בין תיעוד ביומטרי לבין מאגר מידע ביומטרי. ניתן לבצע תיעוד ביומטרי אמין ומאומת ללא מאגר מרכזי. הזיקה שנוצרה בתקשורת ובציבור בין השניים היא מופרכת.

מערך תיעוד ביומטרי יכול וצריך להיבנות כך שהמידע הביומטרי אינו נשמר במאגר מרכזי כלשהו, ולמעשה נמחק ממחשבי הממשל מייד בסיום שלב ההרכשה.

מערך כזה אינו ממעיט כלל מיכולת הזיהוי, ולא מיכולת המערכת להתמודד עם איומים כגון הפקת תעודה כפולה וכדומה.



Israel Internet Association (ISOC-IL)

איגוד האינטרנט הישראלי ע"ר

### 3. אין צורך במאגר מידע ביומטרי בכדי להתמודד עם הבעיות המוצגות בדברי ההסבר להצעת החוק, ככל שמדובר בצורך אזרחי.

- א. זיהוי ניתן לבצע זיהוי מלא מול מסמכי זיהוי המכילים מידע ביומטרי, ללא כל צורך במאגר מרכזי.
  - ב. זיוף. תעודה אלקטרונית מאומתת קשה ביותר לזיוף, ותעודה כזו המכילה אלמנטים ביומטריים קשה לזיוף באותה מידה. המאגר המוצע לא ישפר עמידות זאת כלל.
  - ג. תיעוד כפול / הרכשה כפולה. קיימים שני סוגי מקרים שונים החולקים מושג זה. הוצאה במרמה של מספר תעודות זהות לאותו אדם, תוך הודעה על אובדן / גניבה / השחתה וכו', ושימוש או סחר בהן, הוא המקרה הנפוץ. מערך תעודות אלקטרוניות מאומתות יכול באופן פשוט להיות חסין לאפשרות קיומה של יותר מתעודה אחת תקפה למספר זהות אחד. (הנקודה המשמעותית היא כי בישראל קיים מספר זהות לכל אזרח, בניגוד לחלק מהמדינות המוזכרות בדברי ההסבר להצעה). הרכשה כפולה במשמעות של אדם המשיג לעצמו מספר זהויות ע"י השגת כמה מספרי זהות, היא תופעה שיכולה להתקיים רק בנקודות של קליטת מהגרים (אם נתעלם מהאפשרות לעשות זאת בבתי חולים ליולדות). תופעה זו היא ככל הידוע שולית מאד ואין עליה סטטיסטיקה ידועה. ניתן לצמצם תופעה זו באמצעות תהליכים מוקפדים. מאגר מידע יכול היה לצמצם אותה במידה מסוימת, אך אפילו אם נניח שתופעה זו גדולה מספיק כדי לדרוש טיפול בדרך זו, המאגר שנדרש ומספק לצורך כך הוא מסוג אחר ומצומצם באופן קיצוני יחסית למאגר המוצע.
  - ד. גניבת זהות. היותו של מסמך זיהוי בעל פרמטרים ביומטריים מקשה ביותר על גניבת זהות. מאגר מרכזי איננו מסייע בכך כהוא זה. יצוין, אגב, כי בעיית גניבת הזהות היא תיאורטית, ואיננה בעיה משמעותית כיום במדינת ישראל, בניגוד למדינות אחרות שהוזכרו בדברי ההסבר ובדיונים השונים.
- אפילו לשימוש המשטרה בזיהוי פלילי לא יצלח מאגר כזה, עפ"י עדותו של איש המז"פ בפני הועדה בדיונים על הצעת החוק.
- בסיכום, הנימוק שנוותר להקמת המאגר המרכזי הוא רצונם של גופי הביטחון במאגר מידע נוח לשימוש על כל תושבי המדינה. היתר הם נימוקים שאינם תקפים טכנולוגית.

### 4. הנזק הפוטנציאלי מהקמת מאגר ביומטרי מרכזי הוא גדול מאד.

- א. פוטנציאל הדליפה. עם כל ההבטחות התיאורטיות בהצ"ח, ההיסטוריה הישראלית עגומה בנושא שמירה על מאגרי מידע, בייחוד ממשלתיים. הסיכוי שמאגר ממשלתי שנגיש לכל כך הרבה בעלי תפקיד (כל שוטר!) לא ידלוף, חלקית או במלואו, נראה זעיר.
- ב. נזק הדליפה אינו הפיך. נדרשת "תקלה" אחת, כשל אחד, בלבד – כדי שהמידע הביומטרי של תושבי המדינה ייחשף. יידרשו 80-90 שנה ל"תיקון" נזק זה.
- ג. גניבת זהות. בהיותו של מאגר מידע ביומטרי, כולו או חלק קטן ממנו, בידי גורם בעל כוונות כאלה, יהיה ניתן לבצע גניבת זהות בקלות יחסית (בתנאים מסוימים). יוצא שמה שבא החוק למנוע, הוא מכניס בדלת האחורית.
- ד. הפללה. בהיותו של מאגר מידע ביומטרי, כולו או חלק קטן ממנו, בידי גורם בעל כוונות כאלה, תוכל להתבצע הפללה של כל אדם (ע"י שימוש באלמנטים הביומטריים שלו הנמצאים במאגר), שקשה מאד, אם ניתן בכלל, להפריכה.



Israel Internet Association (ISOC-IL)

איגוד האינטרנט הישראלי ע"ר

- ה. מעקב וזיהוי אזרחי ישראל. בהיותו של מאגר מידע ביומטרי בידי גורם המעוניין לזהות מיהו אזרח ישראלי, לצורך פגיעה / חטיפה או לכל צורך אחר, תספיק מצלמה פשוטה כדי לאתר תושבי ישראל בנמל תעופה, במלון, ברחוב או בכל מקום אחר.
- ו. פגיעה קשה בפרטיות. מאגר מידע ביומטרי מאפשר למי שהמידע בידו, אם גורם שהמידע דלף לידי וואם השלטון עצמו, לעקוב אחרי תנועותיו של כל אזרח באשר הוא. נראה שאין צורך להרחיב על הפגיעה בפרטיות ובביטחון האישי הנגזרות מכך.
- ז. פוטנציאל האגירה. אם תכנון המערכת הוא כזה שכל שוטר מוסמך ליטול נתוני ביומטריה מאדם ולהעבירם לבדיקה, הרי שתיווצר עבורו היכולת הטכנית לשמור את הנתונים (לצורך העברתם). אמנם הצעת החוק קובעת שהנתונים "יימחקו מייד לאחר הבדיקה", אבל זוהי פרצה שקוראת לגנב, וחובה עלינו להניח כי גופים שונים יבחרו "לשכוח" למחוק את הנתונים.
- ח. Mission Creep. מעת שנוצר המאגר, שינויים בחוק ובתקנות יכולים ליצור "סיפוח זוחל" לגבי השימוש בו. אין מכאן דרך חזרה, ולא קיימת אפילו הגנה ע"י חוק יסוד, רוב מיוחס או דבר דומה.

## 5. לא קיים מאגר מידע כזה באף מדינה דמוקרטית.

בניגוד למה שטוענים תומכי ההצעה חוזר וטעון, לא הוקם באף מדינה דמוקרטית מאגר מידע ביומטרי של כלל תושביה. ואין זאת משום שלא מצאו זאת חשוב – הרשויות במדינות רבות שקלו אפשרות זאת, בדרך כלל מתוך דחיפה של גופי הביטחון השונים. בשום מדינה דמוקרטית לא ניתן אור ירוק לביצוע מאגר זה – וזאת לאור נזקיו הפוטנציאליים העצומים, שהם ללא כל פרופורציה לתועלתו השולית.

## 6. הצעות ה"פשרה" השונות אינן משנות את הבעיה באופן מהותי

במהלך הדיונים הועלו כמה הצעות "פשרה", כדוגמת פיצול המאגר לשני חלקים וכדומה. הצעות אלה משנות טכנית את המבנה הצפוי של המאגר ואת מודל האיום, אך אינן פותרות מהותית את הבעיות העקרוניות המוצגות כאן. הבעיה המהותית נשארת בעינה: מאגר של המידע הביומטרי של כל תושבי המדינה, הניתן לאחזור (בתהליך כזה או אחר).

## 7. עלויות. הקמת רשות חדשה; מערך אבטחה; מערך תקשורת; גיבוי משפטי; מדובר בעלות עצומה.

לא התקיים כל דיון בעלויות הנגזרות מהקמת המאגר. הקמת רשות ממשלתית חדשה (אם גם בתוך משרד הפנים), בניית מערך אבטחה (פיסית ומידע), מערך תקשורת שיאפשר אינטראקציות המוגדרות בהצ"ח, מתן הגיבוי המשפטי – כל אלה, חזקה עליהם שעלותם גבוהה מאד. לא הוצג כל מידע על עלויות אלה או על דרכי המימון שלהן.

בסיכום: תיעוד מתקדם ואף ביומטרי הוא צורך חיוני וחשוב. לעומת זאת, מאגר מידע ביומטרי הוא תוספת מיותרת ומזיקה. מהצד האחד אין בו צורך כדי לפתור את הבעיות המוצגות בדברי ההסבר להצ"ח, ומהעבר השני נזקו הפוטנציאלי אדיר.

הסרת הסרח העודף הזה, במלואו, מהצעת החוק, חיונית.