

מידע ביומטרי בישראל

מתי עצרתם לחשוב מה המשמעות של העובדה שהטלפון הנייד או המחשב האישי שלנו נפתחים עם טביעת אצבע, ולפעמים עם זיהוי פנים? או שהעוזר האישי החכם שלכם מתעורר לחיים כאשר הוא מזהה את תווי הקול הייחודיים שלכם? כיום, המידע הביומטרי שלנו משמש אותנו במרחבים רבים, אך אנו לא נוטים לייחס חשיבות מיוחדת לתופעה זו. אולם, כמה אנחנו יודעים על המאגרים בהם נשמר המידע הביומטרי שלנו? האם ברור לנו לאילו מטרות משמש המידע הביומטרי שלנו? וכיצד מגנה המדינה על מידע אישי רגיש כל כך מפני דליפות, תקיפות או ניצול לרעה? עו"ד עדן פרבר וד"ר טל מימרן עונים על השאלות.

אסדרת המידע הביומטרי הינו סוגית ההסכמה מדעת והזכות לפרטיות. אחת מן הסכנות הגדולות הכרוכות בניהול מאגר ביומטרי היא האפשרות שיחדרו

נדירה או יוצאת דופן: על פי מערך הסייבר הלאומי והלשכה המרכזית לסטטיסטיקה, בשנת 2021, אחד מתוך כל חמישה עסקים (18%) בישראל חווה תקיפת סייבר.

החשש איננו רק מדליפת המידע הקיים, אלא ישנן סכנות נוספות אותן יש להביא בחשבון. זאת, מאחר ומדובר במידע עם חשיבות אדירה, בעל ערך כלכלי רב, אשר שחקנים שונים, דוגמת חברות פרטיות, יכולים לנצל בקלות. מידע ביומטרי רב גם נשמר במאגרים של גופי ביטחון, ועל כן יש סכנה מוגברת לדליפה או גניבת מידע על ידי מדינות אויב. על כן, ישנה חשיבות רבה כי תהיה הגנה מרבית ומיטבית על המידע של אזרחים, והיא אף מוגברת לאור העובדה שאזרחים לרוב מחויבים למסור את המידע הזה למדינה על פי חוק.

(2) מניעת שימוש לרעה והסכמה מדעת
נושא נוסף בעל חשיבות רבה לתפקיד

א. מבוא למידע ביומטרי - מה מייעל ומה מסכן

מידע ביומטרי הינו אוסף נתונים אישיים המבוססים על המאפיינים הפיזיולוגיים הייחודיים של אדם, אשר מאפשרים למשתמש בהם זיהוי ודאי של אותו האדם. מידע ביומטרי יכול לכלול תווי הפנים, טביעת אצבע, זיהוי רשתית או קשתית העין, תווי הקול או אפילו כתמי דם ודנ"א. נכון לשנת 2021, לפחות 96 מדינות, בהן ארצות הברית, ה-UK, פורטוגל, אירלנד ואחרות, מנהלות מאגרים ביומטריים עצומים, לצורך ניהול מסמכי זיהוי, דרכונים, מאגרים פליליים ועוד. לצד יתרונות חשובים שיש במידע ביומטרי - בהם יעילות, דיוק, מניעת זיוף, ועוד - קמה חובה לאסוף ולשמור את המידע הזה באופן תקין ומאובטח. קיימים סיכונים ממשיים בניהול מאגרי מידע ביומטריים, ונתייחס כאן רק לשני חששות מרכזיים: דליפה או תקיפת סייבר, ושימוש שלא למטרות שהוגדרו מראש או אף ניצול מידע לרעה. לצד זאת, כפי שנראה בהמשך, לפעמים מידע ביומטרי הופך ליקר ביותר - למשל במצבי אסון קיצוניים.

(1) חשש מתקיפת סייבר והצורך ברמת אבטחה מספקת

מאגרים ביומטריים מחזיקים כמות עצומה של מידע אישי ורגיש, ועל כן, הסכנה הכרוכה בדליפת חומר או אף תקיפת סייבר גדלה. איננו זרים בישראל להשלכות מרחיקות הלכת של תקיפות סייבר על מאגרי מידע, כפי שקרה ביחס למתקפה על חברת הביטוח שירביט, על רקע ההתמודדות עם התפשטות מגפת הקורונה. נדגיש כי לא מדובר בתופעה

"יש חשיבות רבה לכך שמדינות תנהלנה את המאגרים הביומטריים באחריותה עם רמת אבטחה מספקת, בכדי למנוע סכנות באמצעות חשיפה לא מורשית למידע אישי וביומטרי, ובשביל להגן בצורה טובה יותר על זכויות הפרט"

למאגר, או ישתמשו במידע השמור בו באופן שונה מהמטרה למענה נלקח המידע. למשל, בארצות הברית נרשמה מגמה של שימוש לרעה במידע ביומטרי שנאסף במערכות זיהוי לוחיות רישוי (אשר





חשוב לציין כי הדאגות שהועלו בדו"ח זה אינן ראשוניות, אלא מדובר בסוגיות חוזרות בדיווחיו של הממונה, שאף הועלו בעבר על ידי מבקר המדינה.

כך, העלה הממונה בעיות מהותיות הנוגעות לניהול מידע ביומטרי בישראל, ובפרט העברת תמונות לגופים ממלכתיים אחרים ושלא על פי חוק, אי היערכות לפקיעת הוראת השעה המסדירה את הניהול של המאגרים הביומטריים בישראל, פגם בכיול מערכת ההשוואה הביומטרית ועוד. פערים אלו מעידים על בעיות עם אופן הניהול התקין של מאגר ביומטרי עצום ורגיש, מה שחושף את אזרחי ישראל לפגיעה אפשרית בזכותם החוקתית לפרטיות. דאגה מיוחדת הועלה מן הדו"ח נוגעת לרמת האבטחה של מאגרי מידע ביומטרי בישראל.

מעבר לחששותיו של הממונה על היישומים הביומטריים, ראוי לציין גם את הביקורת המקיפה שביצע מבקר המדינה בשנת 2020 בנושא ניהול מאגרים ביומטריים בישראל ושימוש במידע הנאגר בהם. בין היתר, ציין מבקר המדינה כי נדרשת אסדרת המאגרים הביומטריים הממשלתיים בחקיקה וכן לוודא את עמידת המאגרים הביומטריים בעקרונות המדיניות הלאומית ליישומים

לניהול המעבר בין ישראל לשטחי הרשות הפלסטינית ("בזל"); מערכת מעו"ז לזיהוי עובדים זרים; המאגר הביומטרי של מתגייסים לצה"ל התומך בבדיקת זהות לחללים, נפגעים ונעדרים; מערכת ביומטרית של משטרת ישראל; מערכת "התייצבומט" של שירות התעסוקה; וכן מערכת ביומטרית למטרות בקרת כניסה למתקנים, משרדים, מערכות מחשב וכן למערכות נוכחות עובדים. בנוסף, מופעלות מערכות ביומטריות עסקיות בשווקים שונים - למשל במכוני כושר, אפליקציות של קופות חולים, אפליקציות של בנקים ועוד.

השימוש במידע ביומטרי בישראל מוסדר במסמך הנחיות למדיניות לאומית אינטגרטיבית ליישומים ביומטריים משנת 2016, אשר הוכן על ידי היחידה להזדהות ויישומים ביומטריים במערך הסייבר הלאומי. מסמך המדיניות מונה שורה של עקרונות, בהם הגנת הפרטיות ושמירה על כבוד האדם, שמירת קיום התכלית שלשמה ניטלה המידע, וצמצום סיכוני אבטחת מידע. עקרונות אלו ועוד אמורים להנחות את הרשויות ואת הגופים הפרטיים אשר אוספים ושומרים מידע ביומטרי בכל הקשור לניהול המאגרים.

על מנת להתמודד עם הסכנות הכרוכות בהחזקת מאגרים ביומטריים, פועל הממונה על היישומים הביומטריים, רועי פרידמן, בכדי לפקח ולטייב את אופן הניהול של המאגרים ההולכים והגדלים בישראל. בדיווחו של הממונה על היישומים הביומטריים, משנת 2022, עולות מספר בעיות הנוגעות לאופן ניהול המידע, ובפרט לסוגיית האבטחה של המאגרים.

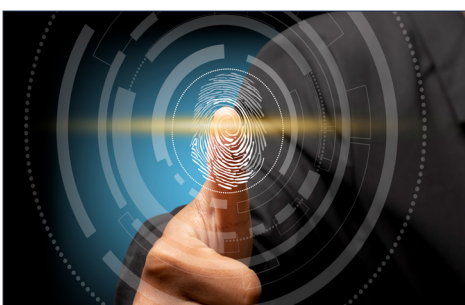
בעלות יכולת לשמור גם תמונות תווי פנים המהווים חלק מן המידע הביומטרי של הנוסעים) כלפי אוכלוסיות מוחלשות, למשל מהגרים. כתוצאה מכך, ערים מסוימות בארצות הברית אימצו חוקי "sanctuary" אשר מגבילים את היכולת של עובדי הציבור בהם לשתף פעולה עם גורמי הגירה פדרליים, במטרה לסייע למהגרים הנמצאים בגבולותיה. אולם, המחקר מראה כי גוף אכיפת ההגירה (ICE) מסוגל לעקוף חוקים אלו תוך שימוש במערכות פרטיות ובפרט מערכות זיהוי לוחיות רישוי (בהליך משפטי שהתנהל בקליפורניה - התגלה כי רשויות ההגירה השתמשו במנועי חיפוש של תכנות זיהוי לוחיות רישוי אלפי פעמים בחודש). במונחים של דיני פרטיות, הפעולה נעשית תוך הפרה של חובת ההסכמה מדעת של בעל המידע למסירה שלו - אם בכלל ניתנה הסכמה לאגור את המידע מלכתחילה.

בנוסף לחשש של חדירה למאגר ישנה דאגה כי המידע שנאגר ישמש למטרות שנושא המידע לא נתן את הסכמתו להן. כאשר אדם מנפיק דרכון ביומטרי, לדוגמה, הוא אינו מבטא הסכמה לאפשרות של העברת המידע שלו לרשויות אחרות. העברתו ללא רשות ומבלי שתהיה אסדרה חוקית להעברת המידע פוגעת, בין היתר, בפרטיותו של האדם ובאוטונומיה שלו.

לסיכום, יש חשיבות רבה לכך שמדינות תנהלנה את המאגרים הביומטריים באחריותה עם רמת אבטחה מספקת, בכדי למנוע סכנות באמצעות חשיפה לא מורשית למידע אישי וביומטרי, ובשביל להגן בצורה טובה יותר על זכויות הפרט. בפרט, יש להבטיח כי המידע משמש למטרות שמוסר המידע הסכים להן ומודע לגביהן.

ב. מה קורה בישראל?

גם מדינת ישראל אוספת מידע ביומטרי מאת אזרחיה במגוון תחומים, במרחב הציבורי והפרטי, על ידי מספר רשויות. על פי הרשות להגנת הפרטיות, השימושים הננקטים במידע ביומטרי במרחב הציבורי בישראל כוללים: תעודות זהות ביומטריות; מעבר הגבול בנתב"ג; מערכת



רגיש בצה"ל, ובפרט אי עמידה בתקנות אבטחת מידע, כשלים בהגנה הפיזית והלוגית על המערכות בנושאי הזדהות, הרשאות, בקרת גישה, ופיקוח על ביצוע פעולות לא מורשות. כאמור, מדובר במידע עם חשיבות אדירה אשר שחקנים שונים יכולים לנצל בקלות, ובהקשר הצבאי – אויבי מדינת ישראל יכולים לנצל אותו לרעה. הסיכונים אשר הצביע

"המידע הביומטרי הנשמר בצה"ל היווה כלי קריטי בתהליך זיהוי החללים בנסיבות הקשות של הטבח"

עליהם מבקר המדינה - בהם גניבת זהות, חשיפת מידע ביטחוני ומודיעיני וחשיפת מידע אישי רגיש - מהווים לא רק סיכונים תיאורטיים אלא סיכונים ממשיים.

ביקורת שנייה של מבקר המדינה הפכה לרלוונטית במיוחד במציאות האכזרית שבה מצא את עצמה מדינת ישראל ביום שבת הנורא של השביעי באוקטובר. המידע הביומטרי הנשמר בצה"ל היווה כלי קריטי בתהליך זיהוי החללים בנסיבות הקשות של הטבח. אולם, בדו"ח מבקר המדינה משנת 2022, צוין כי לא הוסדר השימוש במרכז איסוף נתוני חללים של הרבנות הצבאית בהתרחש אסון רב נפגעים מעורב של אזרחים וחילים. כמו כן, צוין כי אף שצה"ל מחזיק במאגר ובו מאות אלפי רשומות של אזרחים וחילים הכולל אמצעי זיהוי ייחודיים, לא הושלמה הבחינה של אפשרות השימוש במאגר אמצעי הזיהוי המוחזקים בצה"ל לצורך זיהוי חללים בהתרחש אירוע שכזה.

מעבר לכך, בחסות מלחמת חרבות ברזל, הממשלה מקדמת הוראות שעה לפיה תהיה הקלה בדרישות מנגנון העברת המידע הביומטרי לטובת זיהוי חללים, חטופים ונעדרים. לפי התזכיר, הרשות לניהול המאגר הביומטרי תספיק למטרה נתונים ביומטריים לאימות או בירור זהותו של אדם, חי או מת, בהקשר של המלחמה. מדובר בשינוי משמעותי שכן קודם לכן המידע הביומטרי עצמו לא הוצא מהמאגר, אלא הרשות ביצעה

"מקרה מבחן אשר לצערנו קיבל חשיבות מיוחדת בתקופה האחרונה, הוא זה שעוסק בשימוש במידע ביומטרי בשעת חירום להגן בצורה טובה יותר על זכויות הפרט"

מורכב מטביעות אצבע וכפות ידיים, צילומי שיניים וכתמי דם לזיהוי דנ"א. מידע מסוג זה הפך לקריטי אחרי השבעה באוקטובר, בשל הצורך לזהות חללים רבים – לאחר שאלו עברו התעללות קשה המקשה על זיהויים. חשוב ללמוד מהאסון שהתדפק על דלתנו על מנת לראות כיצד ניתן להגיב בעתיד בצורה טובה יותר במקרי אסון.

למעשה, כבר בשנת 2022, מבקר המדינה פרסם דו"ח בנושא המידע הביומטרי

"מידע מסוג זה הפך לקריטי אחרי השבעה באוקטובר, בשל הצורך לזהות חללים רבים – לאחר שאלו עברו התעללות קשה המקשה על זיהויים"

בצה"ל ובו ציין מספר חששות מרכזיים. החשש הראשון, על פי דו"ח מבקר המדינה, הוא כי ישנם פערים בניהול מידע

ביומטריים ובקווים המנחים ליישומה. כפי שניתן לראות, מבקר המדינה מחזק את החששות שמופיעים בדיווחיו של הממונה על יישומים ביומטריים. בעוד כמות המידע שיש במאגרים הביומטריים רק גדל מאז שפורסמו מסקנות מבקר המדינה, קשה לומר שרמת ההגנה עליו השתפרה במקביל.

נראה כי החששות אשר הועלו על ידי הממונה על היישומים הביומטריים, כמו גם מבקר המדינה, טרם קיבלו מענה מוסדי, או חקיקתי. בשנה האחרונה, קודמו מספר מהלכים חקיקתיים, בהם הארכת תוקף הוראת השעה המסדירה את נושא שמירת תמונות פנים וטביעות אצבע במאגר הביומטרי של משרד הפנים, ותזכיר חוק המרחיב את הגישה של עובדי מדינה ואחרים למידע ביומטרי לצורך שיפור הליך הנפקת מסמכי זיהוי. יוזמות חקיקה אלו באו ליתן מענה לנושאים חשובים בתחום הביומטרי בישראל, אולם הם לא נתנו את הדעת על הסיכונים המרכזיים שיש בנטילת מידע ביומטרי, וכן לא הציעו מענה לחשש אשר מועלה שוב ושוב על ידי הגורמים האחראיים של היעדר רמת אבטחה מספקת.

(1) חשיבותו של מידע ביומטרי בעתות חירום - אסון רב נפגעים

מקרה מבחן אשר לצערנו קיבל חשיבות מיוחדת בתקופה האחרונה, הוא זה שעוסק בשימוש במידע ביומטרי בשעת חירום. בצה"ל נשמר מידע ביומטרי אשר



קרדיט: לשכת העיתונות הממשלתית, צלם - Kobi Gideon

על אבטחת המידע והגנה על הפרטיות בזמני שגרה. על מדינת ישראל לעשות שימוש במידע הביומטרי שנשמר על ידי צה"ל בעתות אסון, ולחזק את שיתוף

"מדינת ישראל צריכה להכריע כיצד היא מבקשת לנהל מידע ביומטרי של אזרחיה, ומהם האיזונים הנכונים בין צרכי ביטחון ממשיים לבין זכויות הפרט"

פעולה בין גורמי ביטחון, רפואה והצלה. יצירת נוהל סדור יוכל להיות משמעותי במאמצי זיהוי עתידיים, ובתקווה יגביר את הוודאות בתקופה שזו כל כך חסרה בה ויכול לסייע בהחזרת אמון הציבור בשלטון.

ד. סיכום

אזרחי מדינת ישראל נותנים את האמון שלהם במדינה בעת מסירת המידע האישי שלהם לשם שמירה במאגרים אלו. על כן, ראוי לייחס חשיבות רבה לשמירה על מידע זה בכל הרבדים: שמירה פיזית ולוגית, מפני תקיפות ודליפות, ושמירה מהותית ומשפטית, מפני שימוש שלא למטרות קבועות מראש או אף ניצול לרעה. בפרט, כאשר מדובר במידע הרגיש ביותר, אשר נשמר בצה"ל ומשמש למטרה קשה וקדושה במיוחד, חשוב להבטיח את ההגנה המספקת על המידע ואת השימוש התקין בו, במיוחד בתקופה פגיעה כמו שלאחר אסון. אל לנו להקל ראש בחשיבות השמירה והשימוש הנכון במידע הביומטרי - זו הזהות האישית שלנו, וחובה על מי שנוטל את המידע הזה לשמור עליו, ובכך גם עלינו.

כיצד היא מבקשת לנהל מידע ביומטרי של אזרחיה, ומהם האיזונים הנכונים בין צרכי ביטחון ממשיים (למשל, לצורך הפעלת מערכת איתור החשודים בנתב"ג), לבין זכויות הפרט של אזרחי ישראל (ובמיוחד, פרטיות, חופש התנועה, אוטונומיה וכבוד האדם). על מדיניות זו להתגבש אגב ניהול דיון ציבורי פתוח ושקוף בנושא, כזה אשר יאפשר להביא לידי ביטוי את הגישות השונות בחברה המגוונת הישראלית, ואשר תאפשר גם לאקדמיה ולחברה האזרחית לתרום מהמומחיות שלהן על מנת לטייב את המשטר הקיים.

בפרט, בצה"ל מוחזק מידע רגיש ביותר - וככל שחשוב לשמור על המידע, גם חשוב, בעת הצורך, לדעת איך להשתמש בו. אל מול החשיבות של השימוש בו, יש תמיד לשקול גם את החובה לשמור עליו מפני ניצול או מתקפה, ולא לוותר על אמצעי אבטחה הגבוהים ביותר, כפי שמוצע בתזכיר החוק. בעקבות האסון של השביעי באוקטובר ומלחמת חרבות ברזל, ביום שאחרי המלחמה וכחלק מתהליך הפקת לקחים, חשוב להתייחס גם להיבטים של ניהול ושימוש במידע ביומטרי בצה"ל, ובפרט אבטחת מידע, ריכוך מנגנוני העברת המידע, והשימוש בנתונים ביומטריים במקרה של אסון רב נפגעים מעורב אזרחים וחיילים.

נרצה להדגיש כי חשוב להגדיר הליך יעיל אשר יאפשר שימוש נחוץ במידע ביומטרי בשעות אסון רב נפגעים, תוך חיזוק ההגנה



את הבדיקה בעצמה דרך הצלבת המידע שמסרה לה המשטרה ועדכנה את המשטרה בתוצאות. לשינוי זה יכולות להיות השלכות מרחיקות לכת על רמת האבטחה של המידע הביומטרי של כלל אזרחי ישראל, ולהגביר את הפוטנציאל לדליפות ברמה הלאומית.

ג. איך מתקדמים מכאן?

ככלל, מדינת ישראל, שהיא אחת מן המדינות המתקדמות ביותר מבחינה טכנולוגית ברחבי העולם, צריכה להכריע



ד"ר טל מימרן

ראש תוכנית "אמנה חברתית לעידן הדיגיטלי" במכון תכלית, חוקר ומרצה בתחומי המשפט הבינלאומי והסייבר.



עו"ד עדן פרבר

עורכת דין וחוקרת בתוכנית "האמנה החברתית לעידן הדיגיטלי" במכון תכלית.

