הנחיות EDPB – זיהוי פנים למטרות אכיפת החוק

מאת עו"ד ליאור גולדוסר, מתמחה במכון בהנחיית עו"ד רבקי דב"ש

רקע

המועצה האירופית להגנת מידע אישי, פרסמה בחודש מאי 2022 טיוטת הנחיות להערות הציבור בעניין שימוש בטכנולוגיות זיהוי פנים בהקשרים של אכיפת החוק. המסמך מיועד למחוקקים, לקובעי מדיניות ולעובדי הציבור המפעילים מערכות זיהוי פנים באיחוד האירופי, במטרה לייצר עקרונות זהים בהטמעת השימוש בטכנולוגיות אלו על ידי גורמי אכיפת החוק.

טכנולוגיות זיהוי פנים מבוססות על תהליך עיבוד מידע ביומטרי, ובתוך כך כוללות הליך עיבוד של נתונים אישיים. הצורך בקביעת הנחיות הנוגעות באופן ספציפי לתחום אכיפת החוק נובע מהשימוש הגובר בכלי הטכנולוגי בקרב רשויות אכיפת החוק, וההכרה בעובדה כי בעוד שמדובר בכלי המקנה לרשויות יתרון משמעותי בהתמודדות עם האתגרים הניצבים בפניהן, השימוש בו טומן בחובו פוטנציאל לפגיעה מהותית בזכויות יסוד ולפגיעה בערכים חברתיים ודמוקרטיים.

מערכות לזיהוי ביומטרי, הנן מערכות הקובעות התאמה או אי התאמה, כהכרעה סטטיסטית. כלומר, האלגוריתם שנקבע ככזה המאתר האם תווי פנים של פלוני זהים לאלו המצויים במאגר או בתמונה בודדת, קובע את המענה לשאלה כהכרעה ביחס לרמת הדיוק שנתבקשה. ככל שרמת הדיוק תהיה גבוהה יותר, אחוז האנשים שהמערכת תקבע כי אין התאמה בין האדם לתמונה על אף זהות האדם לתמונה – תגדל. מכאן, כי ככל שהמערכות עוסקות במספרים גדולים יותר, וככל שההשלכות על האנשים גדולות יותר (כדוגמת פתיחת הליך פלילי על בסיס זיהוי ביומטרי), הנזק לאזרח הבודד וכן לציבור המסתכן בחשיפה לפתיחת הליכי שווא, גדל. החשש מתעצם עוד יותר לאור העובדה כי ישנן הטיות במערכות ביומטריות הנוגעות לגזע ואף למגדר.[1] לכל אלו יש להתייחס עת מבקשים לעגן את השימוש במערכת אוטומטית לזיהוי פנים, במיוחד על ידי רשויות אכיפת החוק.

לאור השיח המתעורר בישראל בבקשה להטמיע שימוש במצלמות ביומטריות על ידי המשטרה, סברנו כי יש חשיבות בהבאת עיקרי הדברים גם בעברית.

המשרד לבטחון פנים מבקש לעגן בחוק היתר שימוש במצלמות מיוחדות, לרבות ביומטרית, כפי שעולה מהצעת חוק לתיקון פקודת המשטרה [נוסח חדש] (תיקון מס')(מערכות צילום מיוחדות), התשפ"א-2021,

[1] כך נמצא, בין היתר, במחקר של המכון הלאומי לסטנדרטים וטכנולוגיה בארה"ב (NIST) מחודש דצמבר 2021

אשר עברה אישור של ועדת שרים לענייני חקיקה, אולם נוסח סופי טרם פורסם.[2] כמו כן בחודש יוני 2022 פורסם כי המשטרה ביקשה מהיועצת המשפטית לממשלה לעשות שימוש במצלמות ביומטרית אגב מצעד הגאווה. הבקשה נדחתה אולם היא מעידה על יכולות של המשטרה בתחום זה, ועל הכוונה לעשות שימוש ביכולות טכנולוגיות אלו.

מסמך זה מציג את העקרונות המרכזיים בטיוטת הנחיות אלו, ואת העקרונות שמחברות המסמך ממליצות לאמץ ולהטמיע בעת שימוש במערכות ביומטריות גם בישראל.

המסגרת המשפטית באיחוד האירופי

המסגרת המשפטית שעל בסיסה יש לבחון את ההיבטים המשפטיים של זיהוי פנים למטרות אכיפת החוק מורכבת משני מסמכי חקיקה של האיחוד האירופי – צ'רטר זכויות היסוד (The EU Charter of Fundamental Rights) ואמנת זכויות האדם (European Convention on Human Rights). השניים כוללים הגנה על הזכות לפרטיות ועל הזכות לאבטחת מידע ונתונים אישיים, ובתוך כך איסוף וניתוח צילומי וידיאו של פרטים בהם נכלל צילום פניהם, אשר נחשב למידע ביומטרי. תהליך עיבוד מידע ביומטרי, המאפשר לזהות אדם, ולאתר את מיקומו בזמן מסוים, מאפשר ללמוד אודות חייו האישיים של אותו אדם ועל כן כרוך ישירות בזכות לפרטיות.

עוד מודגש כי הפגיעה בזכויות אינה תלוית תוצאה – קרי, אין קשר לשאלה האם ישנה התאמה בין המידע הביומטרי שנאסף לאדם מסוים, או לשאלה האם התבנית הביומטרית נמחקה לאחר שלא נמצאה התאמה – על פי התפיסה האירופית, כל עוד נעשה הליך עיבוד ביומטרי, מתקיימת פגיעה בזכויות.[3]

בנוסף לאלו מציינת המועצה את האפקט המצנן של מערכת למעקב המוני אחר אוכלוסייה רחבה. גם במקום בו לא נעשה שימוש קונקרטי נגד אדם זה או אחר, החשש למעקב תמידי אחר אדם עשוי להניע ביצוע פעולות גם אם הן בתחום ההתנהגות החוקית, אך שנויים במחלוקת נורמטיבית בחברות מסוימות.

---

[2] על אף שהוחלט על פיזור הכנסת והליכה לבחירות, יש להניח כי הצעת החוק, או הצעה דומה לה, יקודמו גם בממשלה ובכנסת הבאה.

[3] נציין כי בתקנות הגנת הפרטיות (אבטחת מידע), התשס"ז-2017 קיומו של מידע ביומטרי במאגר מידע, מעלה את הרגישות שבו לרמה בינונית. כמו כן בהצעת חוק הגנת הפרטיות (תיקון מספר 14), התשפ"ב-2022, מוצע להתייחס למידע ביומטרי כ"בעל רגישות מיוחדת". מכאן כי גם בישראל, מידע זה נחשב בעל רגישות מיוחדת, אם כי לא ברור מאימתי מתגבש החשש לפגיעה בזכויות, במיוחד לאור החלטת בית המשפט העליון לאחרונה בעניין המאגר הביומטרי (בג"ץ 1946/17 **ארד ואח' נ' ממשלת ישראל ואח'** (12/7/2022)) אשר קבע כי קיום המאגר כשלעצמו, אינו מעלה חשש לפגיעה בזכויות כל עוד לא התממש בו החשש בשל דלף מידע או תרחיש אחר.

<u>פגיעה בזכויות היסוד והחירויות הקבועות בצ'רטר זכויות היסוד ואמנת זכויות האדם של האיחוד</u>

סעיף 52 לצ'רטר זכויות היסוד של האיחוד האירופי קובע תנאים לפגיעה בזכויות יסוד:

1. כל מגבלה על זכויות יסוד חייבת להיות בעלת בסיס חוקי ספציפי ("provided for by law") – על החקיקה המגבילה את זכויות היסוד ואת חירויות האדם להיות למטרה ראויה, מפורשת וברורה על מנת לאפשר לאזרחים להבין מהם התנאים והנסיבות בהם רשות מוסמכת לנקוט באמצעים של איסוף נתונים ומעקב. על החקיקה לכלול את היקף שיקול הדעת הניתן לרשות ציבורית ואופן הפעלתה, על מנת להבטיח לאזרחים את ההגנה המינימלית לה הם זכאים מכוח היותם חלק מחברה דמוקרטית.

2. על חקיקה הפוגעת בזכויות יסוד לעמוד במבחן הנחיצות והמידתיות, ובתוך כך להיות בעלת מטרה לגיטימית, קרי – לשרת מטרות כלליות שהוגדרו על-ידי האיחוד האירופי, או להגן על זכויות וחירויות של קבוצת פרטים. ההנחיות מציינות כי במקרה של זיהוי פנים למטרת אכיפת החוק, מדובר במטרה ברורה של צדק, ביטחון ומניעת פשע. עם זאת, בקביעת המטרות יש לאבחן בין סוג השימושים וקהל היעד השונה – לא דומה ניסיון לאתר אסיר שברח ממשמורת, לניסיון לבסס התנהלות קודמת של עד, שאינו חשוד בדבר, בהליך משפטי.

עוד מדגישות ההנחיות את העקרונות הבאים:

1. כאשר מתערבים ומגבילים זכויות יסוד, היקף שיקול הדעת של המחוקק עשוי להיות מוגבל. על אמצעי החקיקה להלום את מטרותיה. מטרה בעלת עניין כללי, כשלעצמה, אינה מצדיקה הגבלה של זכות יסוד.

2. בהתאם לפסיקתו של בית הדין האירופי לצדק, הגבלות על אבטחת מידע אישי (Protection of personal data) יחולו רק במקרים של הכרח מהותי. בנוסף, יש להבדיל ולמקד את האוכלוסייה הנפגעת בהתאם למטרת לשמה נעשית הפגיעה. אם הפגיעה נעשית באופן כוללני ובאוכלוסייה רחבה יש בכך כדי להעצים את הפגיעה.

3. כל חקיקה צריכה לקבוע כללים ברורים ומפורשים המסדירים את היקף ותחולת האמצעי העומד במרכז החקיקה. על החקיקה לקבוע מפורשות הגנות אפקטיביות לאלו אשר כתוצאה מהשימוש באמצעי המידע האישי שלהם עלול להיפגע ולאפשר להם להתגונן מפני שימוש לרעה וגישה או שימוש שאינם

כחוק. הצורך בהגנות מסוג זה גובר כאשר המידע נתון לתהליך עיבוד אוטומטי וכאשר קיים סיכון ממשי לגישה שאינה כחוק לנתונים שנאספו.

4. על החקיקה להיות מותאמת לסיטואציה הספציפית ונסיבותיה, למשל אופי המידע הנאסף, כמות המידע, וגודל הסיכון לגישה בלתי חוקית.

5. בהתאם להנחיות, על החקיקה לקבוע מפורשות תנאים מהותיים ופרוצדורליים וקריטריונים אובייקטיביים למגבלות הסמכות של הרשות בעלת הגישה לנתונים. ביחס למטרות של מניעה, גילוי או העמדה לדין פלילי, העבירות המיוחסות לאדם צריכות להיות חמורות דיין על-מנת להצדיק את היקף וחומרת הפגיעה בזכויות.

6. יש לראות בחומרה עיבוד נתונים באופן שיטתי ללא ידיעת נושאי המידע. יש להניח כי עיבוד שכזה ייתפס על-ידי הציבור כמעקב מתמיד, ועלול לגרום לאפקט צינון בהתנהגות האזרחים.

<u>המסגרת המשפטית הרלוונטית לפגיעה בזכויות לשם אכיפת החוק – LED (Law Enforcement Directive)</u>

הדירקטיבה האירופית[4] בנושא Law Enforcement Directive (LED), קובעת את המסגרת האירופאית להגנה על אדם בכל הנוגע לעיבוד מידע אישי על ידי רשויות אכיפה פלילית. הדירקטיבה מגדירה מידע ביומטרי (סעיף 3(13) לדירקטיבה), וקובעת את התנאים בהם ניתן לעבד מידע ביומטרי. (סעיף 10).

סעיף 10 ל-LED קובע כי עיבוד קטגוריות מיוחדות של מידע אישי כדוגמת מוצא, דעות פוליטיות והשתייכות דתית, וכן עיבוד נתונים גנטיים וביומטריים יהיו מותרים רק כאשר עיבוד המידע **נחוץ לחלוטין** (strictly necessary) ויעשו בכפוף להגנות על זכויות הפרט. מכאן כי רמת ההוכחה הנדרשת ממי שמבקש לעגן בחקיקה שימוש באמצעים ביומטריים, חייבת להיות גבוהה ביחס לחשיבות אמצעים אלו להשגת המטרות הלגיטימיות אותן הוא מבקש לקדם. עיבוד נתונים מיוחדים אלו למטרות אכיפת החוק מותר רק בהתקיים אחד התנאים הבאים:

1. העיבוד מורשה על פי חוק של האיחוד האירופי או מדינה החברה בו;

2. עיבוד המידע מתבצע על מנת להגן על האינטרסים החיוניים של נושא המידע או של אדם אחר (שאינו תאגיד);

3. עיבוד המידע מתבצע ביחס לנתונים אשר פורסמו באופן גלוי על ידי נושא המידע. בהקשר זה ההנחיות מדגישות מפורשות כי תצלום לכשעצמו אינו נחשב כנתון ביומטרי. לכן, אין בפרסום צילום כדי לאפשר משיכת נתונים ביומטריים על-ידי אמצעים טכנולוגיים. הנחיות המועצה מבהירות כי בכדי שדרישות הסעיף יתקיימו, נדרש שנושא המידע יפרסם את התבנית הביומטרית באופן פומבי ונגיש. אם התבנית הביומטרית פורסמה על-ידי צד שלישי, לא מתמלאות דרישות הסעיף.

סעיף 11(1) ל-LED קובע כי כלל, על מדינות החברות באיחוד לאסור מנגנון החלטות המתבסס על תהליך אוטומטי אשר יש לו השפעה משפטית על אדם. חריג לכך הוא אם הליך שכזה אושר בחקיקה של האיחוד

[4] דירקטיבה הוא מסמך של האיחוד האירופי, המחייב את המדינות להתאים את החקיקה במדינה לעקרונות ולכללים שהדירקטיבה קובעת

או מדינה החברה באיחוד אליה כפוף הגוף בו מתבצע ההליך, ושהחקיקה כוללת הגנות לנושא המידע, וזכות להתערבות אנושית בהליך. עם זאת, ביחס לקטגוריות המיוחדות המפורטות בסעיף 10, ובהם מידע ביומטרי, סעיף 11(2) מחמיר עוד יותר וקובע כי החלטות המבוססות על תהליך אוטומטי לא יתבססו על הקטגוריות המיוחדות אלא אם קיימים אמצעים מתאימים לשמירה על זכויותיו של נושא המידע, וישנם אינטרסים לגיטימיים לעשות כן.

סעיף 6 ל-LED מבחין בין קטגוריות שונות של נושאי המידע, על מנת שאלו ישמשו באופן שונה בהליך עיבוד המידע. כך למשל, לשאלה האם המידע הביומטרי המעובד נוגע לחשוד או לקורבן העבירה, יש השלכות שונות ביחס למבחן הנחיצות מידתיות.

<u>זכויות נושא המידע</u>

ההנחיות מציינות כי בעוד שהן ה-GDPR והן ה-LED מתייחסים להגנות וזכויות של נושא המידע, בשל אופי השימוש במערכת זיהוי פנים (המאפשרת עיבוד מידע אודות אדם ללא אינטראקציה עמו) על הרשות העושה שימוש במערכת זיהוי פנים לשקול כיצד היא ממלאת אחרי הוראות החקיקה ביחס לזכויות האדם לגביו נאסף או עובד המידע עוד בטרם השקת השימוש במערכת מסוג זה, ובפרט: מי הוא נושא המידע שנאסף, כיצד מיידעים אותו בדבר איסוף המידע וכיצד הוא יכולים לממש את זכויותיהם הקבועות בחוק.

ההנחיות קובעות כי על גוף האכיפה לאפשר לאדם נושא המידע את זכויותיו ולפעול באופן הבא:

1. **יידוע** – בהתאם לסעיף 13 ל-LED, יש לפרסם מידע נחוץ ואת זכויותיו של מי שנאסף אודותיו מידע באופן נגיש, תמציתי ומובן. ההנחיות מתייחסות הן לחובת יידוע כללי, והן לחובת יידוע פרטנית, במקרים מסוימים. בכל מקרה, על פי הוראות החקיקה באירופה, קבלת החלטה המתבצעת באופן **בלעדי** על עיבוד מידע ביומטרי, מחייב מתן הודעה על נושא המידע על העיבוד האמור. גם בחוק הישראלי יש לנו חובת יידוע על איסוף מידע (סעיף 11), אך היא מתייחסת רק לחובת היידוע הפרטנית, שבמקרים רבים אינה רלוונטית לרשויות אכיפה פלילית.

2. **זכות עיון** – לאדם יש את הזכות לקבל תשובה ביחס לשאלה האם עובד מידע אישי שלו. בישראל קיימת זכות עיון במאגרי מידע (סעיף 13), אולם רשויות הבטחון על פי החוק, ורשויות נוספות המנויות בסעיף קטן 13(ה), מוחרגות מחובה זו.

3. **זכות לתיקון** – בשל העובדה שטכנולוגיית זיהוי פנים אינה מספקת דיוק מוחלט, יש לאפשר בקשות לתיקונים, ובתוך כך תיקון הקטגוריות הקבועות ב-LED (כאשר למשל אדם סווג לקטגוריה של חשוד על בסיס התנהגותו בצילום וידיאו). זכות התיקון קיימת גם בחוק הישראלי, בסעיף 14 לחוק הגנת הפרטיות, אך פרשנותו ויותר מכך אופן יישומו אינו ברור, במיוחד בכל הקשור למידע המוחזק בידי רשויות אכיפה.

4. **זכות למחיקה** – בשל העובדה שטכנולוגית זיהוי פנים לרוב אוספת מידע אודות מספר רב של אנשים יש לשקול את התכלית לשמה נאסף המידע באמצעי טכנולוגי זה לפני השימוש במערכת מבוססת זיהוי פנים, באופן שיאפשר מחיקה של מידע בהתאם לסעיף 16 ל-LED (הדורש מחיקה ללא דיחוי כאשר מתקיימים התנאים הקבועים בחוק). כאשר יש מניעה חוקית מלמחוק את המידע, ההנחיה המוצעת היא לאפשר את המשך עיבוד המידע רק למטרות אשר בשמן נמנעה המחיקה, ולא למטרות נוספות. בישראל אין הוראה המחייבת מחיקה.

5. **הזכות להגבלות על המידע שנאסף** – כאשר נושא המידע טוען לחוסר דיוק במידע שנאסף אך הוא אינו יכול להוכיח טענתו, יש להגביל את השימוש במידע בהתאם לסעיף 16 ל-LED, ובמיוחד כאשר בשימוש בטכנולוגית זיהוי פנים נאספה כמות גדולה של חומרים אשר איכותם אינה אחידה וגובר החשש לאימות חיובי כוזב (FAR) או לחוסר זיהוי שגוי (FRR). הסיכון עבור נושא המידע גובר כאשר נתונים לא מדויקים משותפים עם רשויות החוק או צדדים שלישיים. במקרים בהם מתגלה חוסר דיוק כאמור, על בעל השליטה לתקן את המידע שאוחסן ואת המערכת בהתאם.

6. **הגבלות לגיטימיות על זכויותיו של אדם שנאסף מידע אודותיו** – הגבלות הנגזרות מעיבוד המידע הביומטרי, מותרות רק כאשר הן קבועות בחוק ולמטרות לגיטימיות, למשל הגנה על הביטחון הלאומי או ביטחון הציבור. כאשר השימוש בטכנולוגית זיהוי פנים הוא למטרת אכיפת החוק, ניתן להניח כי קיום חובת היידוע או מתן זכות עיון לחשוד בביצוע עבירה בעת ביצוע חקירה סמויה, למשל, עשויה לפגוע בעבודת רשות האכיפה ובהשגת מטרות אלו.

7. **מימוש זכויות באמצעות הרשות המפקחת** – כאשר קיימת הגבלה חוקית על מימוש זכויותיו של אדם אשר נאספו נתונים אודותיו, אותו אדם רשאי לפנות לרשות הרלוונטית האמונה על הגנת המידע האישי לשם בדיקת חוקיות עיבוד המידע אודותיו. בישראל הרשות הרלוונטית היא הרשות להגנת

הפרטיות, אולם מכיוון שאין התייחסות לעוגנים חוקים לעיבוד מידע, יש לשאול הכיצד תוכל הרשות לבצע אכיפה כנגד רשויות אכיפה פלילית שיעשו שימוש במידע ביומטרי.

<u>דרישות והגנות נוספות</u>

1. **הערכת השפעה על הגנת מידע אישי** – ההנחיות קובעות חובה לבצע הליך הערכת השפעה על הגנת מידע אישי (Data Protection Impact Assessment - DPIA) **לפני** שימוש בטכנולוגית זיהוי פנים, בשל הסיכון הגדול שמהוות לחירויות האישיות הקיימות לאדם. על ההליך לכלול לכל הפחות:
   1.1 תיאור של תהליך העיבוד המיועד;
   1.2 הערכה של נחיצות ומידתיות הפעולה;
   1.3 הערכת הסיכונים הקיימים לחירויות ולזכויות של נושאי המידע;
   1.4 אמצעי ההגנה המוקנים לנושאי המידע במקום של שימוש לא הוגן.

   בהערכה כאמור, יש לתת את הדעת על רמת הדיוק אליה המערכת מכוונת, תוך הבנה כי הגברת רמת הדיוק, צפויה לפגוע בציבור רחב יותר שלא בצדק, ובמיוחד באוכלוסיות מיעוט אשר בדרך כלל לגביהן אחוז הטעויות במערכת גדול יותר.

   המלצת ההנחיות היא כי תוצאות ההערכה יפורסמו לציבור, או לכל הפחות הממצאים העיקריים.

2. **התייעצות מוקדמת עם הרשות המפקחת** – בהתאם לסעיף 28 ל-LED, יש תנאים בהם על הרשות אשר עושה שימוש בטכנולוגית זיהוי הפנים להיוועץ עם הרשות המפקחת (בישראל הרשות להגנת הפרטיות) לפני עיבוד המידע. לדוגמה, כאשר עולה מה-DPIA כי כתוצאה משימוש בטכנולוגיות, מנגנונים או נהלים חדשים, קיים סיכון גבוה לזכויותיהם וחירותם של פרטים.

3. **אבטחה בעיבוד המידע** - האופי הייחודי של הנתונים הביומטריים מחייב תשומת לב מיוחדת לאבטחת תהליך העיבוד ומניעת דליפת נתונים (סעיף 29 ל-LED). במקום בו מתבצע עיבוד אוטומטי של נתונים, ישנן חובות מוגדרות יותר כאמור בס"ק 29(2) ל-LED.

4. **עיצוב (הנדסה) לפרטיות** (Data Protection by Design and Default) - בהתאם לסעיף 20 ל-LED יש לשלב מתודות להנדסת פרטיות דוגמת פסאודונימיזציה או צמצום המידע הנאסף ונשמר, עוד לפני תחילת תהליך עיבוד המידע הביומטרי ולאורך כל התהליך.

5. **הליך תיעוד** – חקיקת ה-LED קובעת שיטות שונות המאפשרות לרשות המעבדת את המידע להבטיח את חוקיות התהליך ואבטחת המידע. על מנת להוכיח כי ההליך עמד בדרישות שבחוק, יש לשמר תיעוד ממוחשב (logging).

<u>סיכום של ה-EDPB</u>

לסיכום, מציינים מחברי טיוטת ההנחיות, כי הצורך של רשויות אכיפת החוק לעשות שימוש בטכנולוגיות חדשות כדי להגביר את יכולותיו בתחום מניעת הטרור וזיהוי פשעם חמורים נוספים, מובן.[5] עם זאת, חייבת להיות הקפדה וכללים ברורים על מנת להבטיח שימוש במערכות מסוג זה רק כאשר הדבר נחוץ ונעשה באופן מידתי, ולא להפוך אותם לטכנולוגיה השגרתית בה נעשה שימוש, וזאת לאור פוטנציאל הפגיעה שלה בזכויות אדם במיוחד ביחס למעקב המוני. יש חשיבות לקביעת הגבולות לשימוש במערכות מסוג זה. זיהוי ביומטרי מרחוק של אנשים במרחבים ציבוריים, מהווה סיכון משמעותי לחדירה לפרטיותם של אנשים, ואין לו מקום בחברה דמוקרטית לשיטתם. ה-EDPB מציין כי שימוש בזיהוי פנים לצורך זיהוי אתני, מגדרי, כמו גם נטייה פוליטית או מינית, וניסיון להסיק רגשות של אדם, אינם רצויים ויש לאסור אותם למעט חריגים מוצדקים מעטים.

בנוסף, המחברים סבורים כי הסתמכות על בסיס נתונים שמקורו באיסוף נתונים אישיים בקנה מידה המוני ובאופן חסר הבחנה, למשל על ידי "גרידת" תמונות הנגישות באינטרנט, לא עומדות בדרישות המחמירות של האיחוד לשימוש במידע זה.

[55] לתשומת הלב כי השימוש בביומטריה מוגדר רק לצרכים אלו, החריגים מאוד, ולא למנעד רחב של אכיפה פלילית כמוצע בישראל.

<u>אילו מהעקרונות המוצעים רצוי לאמץ בישראל</u>

מטיוטת ההנחיות עולים נושאים ועקרונות אשר מומלץ לשקול ולאמץ גם בישראל, במסגרת החקיקה המתגבשת ובפרקטיקה מיטבית ("Best practice"). עקרונות אלו יכולים להנחות המחוקקים כמו גם את רשויות האכיפה בעת שימוש במערכות זיהוי ביומטרי, ולסייע בחיזוק אמון בשמירה על זכויותיהם בעת שימוש במערכת:

1. **הליך הערכת מהימנות המערכת** – בהתחשב בעובדה שהמערכת מכוונת לדיוק סטטיסטי ולא מוחלט, מומלץ לשקול אימוץ פרקטיקה של הליך בחינת מהימנות מינימלית של המערכת, ובמסגרתו לאמוד את טווח הטעות בזיהוי של המערכת. לתוצאות בחינה זו יש השלכות בבחינת הסתמכות על המערכת לצורך ביצוע עיבוד אוטומטי, וכן השפעה על הפגיעה בזכויות וחירויות הפרט – שכן ככל שטווח הטעות גדול יותר, גדל הסיכוי לזיהוי שגוי. לאור ההטיות המובנות במערכות לזיהוי פנים, יש לבחון גם את מידת הדיוק של המערכת ביחס לאוכלוסיות שונות ובהם בעלי לאום, גזע ומגדר שונה. נדרש כי תוצאות הערכת המהימנות יפורסמו לציבור וכי הערכה כאמור תתבצע טרם אימוץ טכנולוגיה חדש ואחת לתקופה (מומלץ לא יותר מאחת לשלוש שנים), בהינתן שינויים והתפתחויות בתחום הטכנולוגי.

2. **הליך הערכת סיכונים לזכויות הפרט** – בשל אופיו של המידע הביומטרי, והסיכון שיש בשימוש במערכות אלו לזכויות פרטים, ובתוך כך הזכות לפרטיות, כבוד האדם, והזכות לשוויון. מומלץ לקבוע כפרקטיקה ראויה קיום הליך של הערכת הסיכונים לזכויות הפרט, עוד בטרם הטמעת השימוש במערכת. במסגרת הליך הערכת הסיכונים מומלץ לבחון ולמפות את הזכות שעלולה להיפגע, מהי חומרת הפגיעה, מי האוכלוסייה שעשויה להיפגע (האם מדובר בציבור בכללותו, או באוכלוסייה מצומצמת), ומהי ההסתברות לפגיעה. במסגרת הליך הערכת הסיכונים לזכויות יש להתייחס לשאלה האם השימוש במערכת נעשה למטרת אימות או למטרת זיהוי, שכן היקף הפגיעה בעת אימות ביומטרי נמוך מאשר זיהוי ביומטרי, שכן לרוב האימות נעשה בידיעת נושא המידע, וכן כולל שימוש במידע ביומטרי של אדם אחד (להבדיל מניסיון לזהות תמונה וכדומה באמצעות עיבוד מידע ביומטרי של קבוצת אנשים גדולה).

3. **עיצוב לפרטיות** – מומלץ לשקול לכלול הנחיה לפיה יש לפעול על מנת לשלב הנדסת פרטיות בעת השימוש במערכת, ולעשות שימוש באמצעים אשר יבטיחו כי איסוף הנתונים האישיים יהיה מצומצם ככל הניתן ביחס למטרת האיסוף, ביחס לכמות הנתונים, היקף העיבוד שלהם, תקופת האחסון שלהם

והגישה אליהם. עיצוב לפרטיות עוד בשלב תכנון הטכנולוגיה עשוי להיות כלי יעיל לצמצום הפגיעה בזכויות הפרט בעת השימוש במערכת.

4. **מועד תחילת ההליך הביומטרי** – כלל, מוצע לדון בשאלה מתי מתחיל תהליך עיבוד המידע הביומטרי, באופן אשר מכפיף את ההליך להוראות החוק. מההנחיות של המועצה האירופית ניתן ללמוד כי הן מכירות בכך שהפגיעה בזכויות היא משלב האיסוף של המידע, גם אם לא נעשה עיבוד ביומטרי וזאת בשל פוטנציאל הפגיעה. על מנת לחזק את אמון הציבור ולהבטיח שמירה על זכויות הפרט, ראוי להגדיר את נקודת הזמן בהליך בה נגדיר מאגר כמכיל מידע ביומטרי, ובכך כפוף להוראות החוק המיוחדות בנושא. נבהיר כי אין בדברים האמורים המלצה לאמץ את עמדת האיחוד האירופי בהקשר זה, ולקבוע כי יש לקבל את הסכמתו של נושא המידע לשימוש בתמונה שפורסמה על-ידו ברבים על מנת לעבד תבנית ביומטרית. עם זאת אנו רואים בעמדת האיחוד את החשיבות בהכרעה ברורה מתי מתחיל הליך העיבוד הביומטרי לגביו נדרשים לקבוע הסדרים מיוחדים.

5. **עיגון בחקיקה** – הדרישה של האיחוד האירופי כי שימוש במערכת ביומטרית על ידי רשויות האכיפה תהיה מעוגנת בחקיקה ספציפית ומפורטת, ראוי שתתקיים גם בישראל. פוטנציאל הפגיעה בזכויות אדם של השימוש במידע ביומטרי המאפשר מעקב והתחקות קבועים אחר כלל האוכלוסיה, מצדיק את החובה לעגן את השימוש ביכולות אלו בחקיקה. חקיקה כאמור תצטרך לתת את הדעת גם לנושאים הבאים:

5.1 קביעת מגבלות מיוחדות ביחס להיתר לעשות שימוש בזיהוי פנים (One to Many) לצורך זיהוי ביומטרי שנעשה ללא ידיעתו של אדם (להבדיל מאימות אשר ברוב המקרים נעשה בידיעתו);

5.2 קביעת בסיסי הנתונים מהם יאושר לעשות שימוש לצורך זיהוי ואימות ביומטרי;

5.3 הטלת חובה לבחון את מהימנות המערכת טרם הטמעתה ואחת לתקופה;

5.4 רמת השקיפות של מערכות מסוג זה במיוחד אל מול ניהול הליכים פליליים;

5.5 חובות מחיקה מהמאגר בחלוף תקופה;

5.6 זכויות נושא המידע.

6. **זכות המחיקה –** כחלק מעיגון זכויות נושא המידע בחקיקה פרטנית, מומלץ לשקול לכלול עיגון מפורש של הזכות למחיקה (אשר כאמור לא קיימת כיום בדין הישראלי), בדומה לסעיף 16 ל-LED. הזכות למחיקה במסגרת סעיף זה מתייחסת למחיקה בשל עיבוד שלא על-פי חוק, ותחת חריגים מאפשרת לבעל השליטה שלא למחוק את המידע אלא לעבד אותו בכפוף להגבלות הקבועות בחוק.

7. **חובת יידוע** - בשל אופיין הייחודי של מערכות לזיהוי פנים, מומלץ לשקול לכלול חובת יידוע ביחס למערכות ביומטריות, אשר תהיה מורכבת משני נדבכים:

7.1 יידוע אודות פעולות איסוף ועיבוד המידע – יש ליידע את הציבור בכללותו אודות השימוש במערכת, וכן ליידע באופן פרטני את נושא המידע במקרה של איסוף מידע בעניינו. בשני המקרים, מומלץ לספק מידע אודות אופן איסוף המידע, מטרת האיסוף, ואופן השימוש במידע שנאסף, למשל, למי יכול המידע להיות מועבר, ובאילו נסיבות. היקף חובת היידוע יכול להיות מושפע מאופי השימוש במערכת הביומטרית (האם משמשת לצורכי זיהוי או לצורכי אימות), ואף להיות מסויג בנסיבות בהן קיים חשש כי יידוע מראש בדבר איסוף המידע יפגע משמעותית במאמצי אכיפת החוק, זאת בכפוף למנגנוני בקרה אשר ייקבעו בחקיקה.

7.2 מידע אודות המערכת הטכנולוגית – לאור היותה של המערכת מבוססת הכרעה סטטיסטית, ואשר מטבע הדברים הכרעות באמצעותה מתקבלות על בסיס אלגוריתם, מומלץ לכלול בחובת היידוע גם מתן אינפורמציה בדבר מאפייני המערכת כדוגמת בסיס הנתונים עליה מושתתת, מה מידת הדיוק שנקבעה בה וההטיות המצויות בה. חובת היידוע על נתונים אלו חשובה במיוחד במקום בו ננקט הליך פלילי נגד נושא המידע, לדוגמא בעת בקשת צו מעצר על בסיס ראיה ביומטרית, ראוי כי לסניגור ושופט יינתן מידע בדבר המערכת עצמה על מנת שיוכל להעריך את עוצמת הראיה.

סיכום

אופייה הייחודי של מערכת לזיהוי פנים באופן ביומטרי, הכוללת איסוף ועיבוד של מידע אישי ביחס לקבוצה גדולה של אנשים ומאפשרת גם את זיהויו של אדם במרחב הציבורי (וכפועל יוצא מעקב והתחקות אחרי פרטים) מקנה לרשויות האכיפה כוח משמעותי בעת ביצוע מלאכתן. לצד היתרונות הברורים, שימוש בטכנולוגית זיהוי פנים טומן בחובו גם פוטנציאל משמעותי לפגיעה בזכויות אדם ובערכים חברתיים אשר הינם חלק בלתי נפרד מחברה דמוקרטית.

ההסדר האירופי המוצע מהווה דוגמה לניסיון לבצע איזון בין ההכרה בצורך של רשויות האכיפה להצטייד בכלים טכנולוגיים שיסייעו להן בביצוע עבודתן, לבין שמירה על זכויות הפרטים בחברה דמוקרטית. הכללים הקבועים בהנחיות יכולים לשמש את המחוקק הישראלי, ואת רשויות האכיפה, בבואם להסדיר את השימוש בטכנולוגיית זיהוי פנים. הסדרת הפיקוח על השימוש בטכנולוגיה זו באמצעות דבר חקיקה פרטני הקובע כללי מסגרת לשימוש במערכות זיהוי פנים על ידי רשויות האכיפה, וכן על ידי גיבוש פרקטיקות מיטביות המתייחסים שניהם להיבטים ייחודיים שמעלה השימוש במערכת כאמור, נחוצה על מנת לצמצם את הפגיעה בזכויות ולתת את הכלים וההגנות הנדרשות ככל שיוחלט לעשות שימוש במערכות מסוג זה.