ל' ניסן תשפ"ה

28 אפריל 2025

טיוטת הנחיית הרשות להגנת הפרטיות:

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

מבוא

1. לטכנולוגיית הבינה המלאכותית יתרונות רבים ופוטנציאל כמעט בלתי מוגבל. עם זאת, השימוש בה טומן בחובו גם אתגרים וסיכונים משמעותיים לחברה האנושית הדורשים מענה מצד המערכת הרגולטורית.[1]

2. מסמך מקיף בנושא "עקרונות מדיניות, רגולציה ואתיקה בתחום הבינה המלאכותית" שפרסמו משרד החדשנות, המדע והטכנולוגיה ומשרד המשפטים בדצמבר 2023 (להלן: "**מסמך המדיניות הממשלתי**"), אשר חלקיו הנוגעים לפרטיות נכתבו בשיתוף פעולה עם הרשות להגנת הפרטיות, פירט את הסוגיות והאתגרים השונים המתעוררים בקשר לפיתוח יישומי בינה מלאכותית ולשימוש בהם, מנה את מערכות הדינים הרלבנטיות, סקר הצעות רגולציה המגובשות בעולם,[2] והמליץ על המדיניות הרצויה לאסדרת הנושא בידי הרגולטורים השונים בישראל, כל אחד בתחומו.[3]

3. הנחיה זו מיועדת להציג את פרשנות הרשות להגנת הפרטיות להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**" או "**החוק**") והתקנות שמכוחו, לצורך הפעלת הסמכויות המסורות לה על פי דין בנוגע למאגרי מידע בהם נעשה שימוש בטכנולוגיית בינה מלאכותית, לרבות לצורך ביצוע סמכויות הפיקוח, הבירור המינהלי, האכיפה והטלת הסנקציות אשר הוקנו לרשות בחוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024 (להלן: "**תיקון 13 לחוק הגנת הפרטיות**"), שאושר בכנסת וייכנס לתוקפו באוגוסט 2025. זאת, בשים לב להתפתחות הטכנולוגיה ולסיכונים שפורטו במסמך המדיניות הממשלתי, בפרסומים מקצועיים ובמסמכי יסוד אחרים בעולם, בתחום רגולציית הגנת המידע האישי והבינה המלאכותית, לרבות המלצות ארגון ה-OECD בנושא בינה מלאכותית.[4]

---

[1] לרבות הסיכונים הנובעים משימוש לרעה בטכנולוגיית Deepfake. להרחבה ראו עמדת הרשות להגנת הפרטיות בנושא "פרטיות ואבטחת מידע בשימוש בטכנולוגיות Deepfake (זיוף עמוק)" (2022).

[2] בפרק הזמן שחלף מאז פרסום מסמך המדיניות הממשלתי, הושלמה חקיקתו של חוק הבינה המלאכותית האירופי - EU AI ACT, וכן נחתמה אמנת מועצת אירופה, שהיא האמנה הבינלאומית הראשונה בתחום - The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, עליה חתמה גם מדינת ישראל.

[3] "עקרונות מדיניות, רגולציה ואתיקה בתחום הבינה המלאכותית" (דצמבר 2023), פורסם על ידי משרד החדשנות, המדע והטכנולוגיה יחד עם מחלקת ייעוץ וחקיקה (משפט כלכלי). הרשות להגנת הפרטיות היתה שותפה מרכזית בכתיבת המסמך, בכל הנוגע לחלקים הנוגעים לזכות לפרטיות בתחום הבינה המלאכותית, והאמצעים להבטיח את ההגנה עליה במערכות בינה מלאכותית. המסמך זמין כאן.

[4] OECD Council Recommendation on Artificial Intelligence (amended 3 May 2024).

ההנחיה

4. **הגדרה**

לצורך הנחייה זו:

"**מערכת בינה מלאכותית**": מערכת ממוכנת אשר מסיקה מהקלט המוזן לה כיצד להפיק תחזיות, תוכן, המלצות או החלטות שיכולות להשפיע על הפרט או פעילותו של בעל השליטה או המחזיק במאגר, הפועלת ברמות משתנות של עצמאות והסתגלות.[5]

5. **תחולת חוק הגנת הפרטיות על מערכות בינה מלאכותית**

5.1. הוראות חוק הגנת הפרטיות חלות על מודל בינה מלאכותית המאחסן או מעבד **בפועל** מידע אישי, הן בשלב הלימוד והן בשלב היישום, אם בכוונת מכוון ואם בשל רשלנות או טעות.[6]

5.2. אין חולק כי מידע אישי אשר נוצר תוך שימוש במערכות בינה מלאכותית, לרבות באמצעות היסקים או הערכות, הוא מידע שחלות עליו הוראות חוק הגנת הפרטיות. בדוח הביניים של הצוות הבינמשרדי בנושא בינה מלאכותית בסקטור הפיננסי תוארו הדברים כך: "מערכות בינה מלאכותית מרחיבות באופן משמעותי את היכולת להסיק מידע חדש על נושאי מידע, באמצעות הפעלת המודלים שלהן על מידע אישי. מערכות אלו לומדות ומעבדות נתוני עתק, ומכוונות למצוא דפוסי פעולה או קורלציות בלתי צפויות, או כאלו שלא היו נגישות קודם לכן לעין האנושית. באמצעות המודלים האמורים, משמשות המערכות לזיהוי, סיווג, תחזית או הערכה לגבי אדם מסוים. זאת, גם אם המידע עליו לא נכלל בנתוני העתק הגולמיים ואף אם הוא לא מסר את המידע אודותיו בעצמו".[7] עוד נאמר בדוח כי "אין בעינינו ספק כי תוצרי מערכות הבינה המלאכותית – תחזיות, היסקים, הערכות, סיווגים שנעשים לגבי אדם ספציפי הם מידע אישי הזוכה להגנת דיני הגנת הפרטיות".[8]

---

[5] השוו להגדרה העדכנית בעקרונות ארגון ה-OECD ממאי 2024 (לעיל ה"ש 4):
"An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

[6] CNIL :AI: ensuring GDPR compliance (2022):
"Furthermore, learned AI models are also likely to contain personal data:
by construction, as is the case for certain specific algorithms that may contain fractions of training data (e.g. SVM or some clustering algorithms); **by accident,** as described in the section "Safeguarding against the risks involved with AI models."

[7] עמ' 85 לדוח הביניים של הצוות הבינמשרדי בנושא "בינה מלאכותית בסקטור הפיננסי" (נובמבר 2024), שפורסם להערות הציבור (להלן: **דוח בינה מלאכותית בסקטור הפיננסי**).

[8] עמ' 87 לדוח בינה מלאכותית בסקטור הפיננסי. ראו לעניין זה גם הגדרת "מידע אישי" בתיקון 13 לחוק הגנת הפרטיות, כדלקמן: "מידע אישי" - "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן

5.3. יש לוודא קיומו של **בסיס חוקי המאפשר עיבוד מידע אישי המהווה פגיעה בפרטיות בכל אחד משלבי מחזור החיים של המערכת, ובכלל זה אימון המודל או השימוש בו בפועל.**

5.4. כאשר עיבוד מידע אישי המהווה פגיעה בפרטיות מבוצע בידי רשות מרשויות המדינה הוא טעון **הסמכה בחוק**.[9] במקרים אלה, ובנסיבות נוספות עליהם הצביעה הפסיקה במסגרת יחסי עבודה,[10] על פעולת עיבוד המידע **לקיים גם את דרישת המידתיות**.

5.5. הצורך בזיהוי בסיס משפטי לעיבוד מידע אישי המהווה פגיעה בפרטיות הוא **חשוב במיוחד לאור הסיכון הגבוה לפרטיות ולנוכח חוסר הוודאות בעניין המטרות העתידיות של עיבוד המידע וההשלכות שתהיינה לו על נושאי המידע,** המאפיינים באופן מובהק שימוש מערכות בינה מלאכותית.

5.6. כאשר **שימוש במידע אישי במערכת בינה מלאכותית הוא בעל פוטנציאל לסיכון גבוה לפרטיות**[11] אזי בהתאם להוראת סעיף 20(ב) לחוק,[12] הנטל על המשתמש במערכת כזו, אשר יבקש לטעון לקיומה של הגנת תום לב, או לקיומו של עניין לציבור הפוטרים אותו מאחריות לפגיעה בפרטיות לפי סעיף 18 לחוק – יהיה גבוה יותר.

6. <u>קבלת הסכמה ומימוש חובת היידוע והשקיפות</u>

6.1. סעיף 3 לחוק קובע כי ההסכמה הנדרשת כדי לאפשר פגיעה בפרטיותו של אדם,[13] כולל כזו הכרוכה בשימוש במידע אישי אודותיו, צריכה להיות "**מדעת**". משמעותה של "הסכמה מדעת" (informed consent) היא כי **"בידי האדם שנתונה לו זכות לפרטיות (מושא המידע) היה המידע הדרוש לו באורח סביר כדי להחליט אם להסכים למסירת המידע ולשימושים שיעשו בו, ובכלל זה להעברתו לצדדים שלישיים"**.[14] סעיף 11 לחוק קובע כי פניה לאדם לשם קבלת מידע על אודותיו תלווה בהודעה הכוללת את המטרה לשמה מבוקש המידע, למי יימסר ולאיזו מטרה, והאם חלה חובה חוקית למוסרו. בנוסף על חובת

לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי."

[9] ראו למשל רע"א 2558/16 **פלונית נ' קצין התגמולים – משרד הביטחון** (נבו 5.11.2017), פסקאות 36-44 לפסק הדין.

[10] ע"ע (ארצי) 90-08 **טלי איסקוב ענבר נ' מדינת ישראל - הממונה על חוק עבודת נשים** (נבו 8.2.2011).

[11] למשל בשל **מאפייני הארגון**; בשל **סוג המידע המעובד במערכת בינה מלאכותית ורגישותו**, כגון סוגי המידע המפורטים בפרט 1 לתוספת הראשונה לתקנות אבטחת המידע או בהגדרת "מידע בעל רגישות מיוחדת" בתיקון מס' 13 לחוק הגנת הפרטיות או מידע על אוכלוסיות מיוחדות כדוגמת קטינים; בשל **היקף המידע המעובד** (בשים לב לקריטריונים המפורטים בסעיף 17ב1(ב) שנוסף לחוק בתיקון 13) **או מספר מורשי הגישה** אליו. בכל הנוגע לסיכוני הפרטיות שבמודל שפה גדול (LLM), ראו למשל את מסקנות צוות המשימה של ה- European Data Protection Board (EPDB), בעניין השימוש במודל ChatGPT, בעמ' 6-9 לדוח הצוות. הדוח זמין כאן. ראו גם "גילוי דעת מקדים בעניין שימוש בבינה מלאכותית בעבודת עורך הדין" מטעם ועדת האתיקה של לשכת עורכי הדין (החלטה את/60/24), ובפרט בעמ' 3–5 לגילוי הדעת, אשר זמין כאן. לא בכדי בתיקון 13 לחוק הגנת הפרטיות, אשר מגדיר בין היתר מהו "מידע בעל רגישות מיוחדת", נכללה בהגדרה זו גם קטגוריה שעניינה "מידע אישי שהוא הערכת אישיות ... **שנערכה באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים**..." (סעיף 8 להגדרה).

[12] סעיף 20(ב) לחוק הגנת הפרטיות קובע כך: "חזקה על הנאשם או הנתבע שעשה את הפגיעה בפרטיות **שלא בתום לב** אם הוא פגע ביודעין **במידה גדולה משהיתה נחוצה באופן סביר לצורך הענינים שניתנה להם הגנה** בסעיף 18(2)".

[13] "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו" – סעיף 1 לחוק הגנת הפרטיות.

[14] מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 100 (התשע"א), שצוטט גם בת"א (ירושלים) 3213-09 **פלונית נ' פלוני** (נבו 11.10.2011).

הידוע המוטלת מכוח סעיף 11 לחוק בעת **פניה** לאדם לקבלת מידע, מוטלת חובת יידוע דומה ואף רחבה יותר גם ביחס למידע שהגיע לבעל השליטה במאגר **באופן עקיף** מן האזור הכלכלי האירופי.[15]

6.2. תוכן והיקף היידוע והגילוי הדרושים לביסוס הסכמה **מדעת** ולקיום חובת היידוע הקבועה בסעיף 11 לחוק,[16] לרבות לעניין עיבוד מידע באמצעות מערכות בינה מלאכותית, הוצגו בפירוט ובהרחבה בעמדה שפרסמה הרשות להגנת הפרטיות בעניין "חובת יידוע במסגרת איסוף ושימוש במידע אישי".[17] בתמצית, כתנאי לקבלת הסכמה בת תוקף, יש להציג בפני נותן ההסכמה **מהי המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה, והאם חלה על נושא המידע חובה חוקית למסור את המידע**, כנדרש בסעיף 11 לחוק[18]. בנוסף, יש להציג בפני נושא המידע גם את הסיכונים העשויים לנבוע מעיבוד המידע: **הן סיכונים לפרטיות והן סיכונים או השלכות שליליות אחרות** העלולות להיגרם לו כתוצאה מעיבוד המידע או השגת מטרתו.[19]

6.3. בהקשר של פיתוח ושימוש במערכות בינה מלאכותית, מקבלת חובת היידוע והחובה לקבל הסכמה מדעת חשיבות יתרה. מבלי לגרוע מכלליות האמור, עמדת הרשות היא כי קיום דרישת סעיף 11 לחוק **בטרם איסוף מידע אישי מאדם למערכת בינה מלאכותית או הסתמכות על הסכמה כבסיס לעיבוד מידע באמצעותה, נדרשות לפיכך לקיים בין השאר תנאים אלה**:

6.3.1. לנוכח מאפייני מערכות בינה מלאכותית העשויים להקשות על נושא המידע להבין איזה מידע נאסף עליו על-ידי המערכות, איזה שימוש נעשה בו, איזה מידע עוּבַּד יחד עם המידע על אודותיו ולאילו מטרות, ההסבר לנושא המידע על מטרת איסוף המידע ועל השימוש בו **צריך לכלול גם תיאור של אופן פעולת המערכת** ביחס לעיבוד מידע אישי, ברמת הפירוט הנדרשת לגיבוש ההסכמה ובשים לב למגבלות טכנולוגיות.[20] בין היתר, עמדת הרשות היא כי העובדה שהגורם המקיים עם נושא המידע אינטראקציה הכוללת מסירת מידע **אינו בן אנוש, אלא מערכת אוטומטית מבוססת בינה**

---

[15] תקנה 6 לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023 (להלן: "**תקנות מידע מהאזור הכלכלי האירופי**"). החל מיום 1.1.25, חובה זו חלה גם על מידע המוחזק באותו מאגר יחד עם מידע שהועבר לישראל מהאזור הכלכלי האירופי.

[16] ביחס למידע שהגיע מהאזור הכלכלי האירופי או מידע שמצוי במאגר בו יש מידע אירופי כאמור – גם לפי סעיף 6 לתקנות מידע מהאזור הכלכלי האירופי.

[17] עמדת הרשות להגנת הפרטיות בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (2022) (להלן: "**מסמך חובת היידוע**"). המסמך זמין כאן. לעניין היחס בין קיום חובת היידוע לבין הסכמה תקפה לפי חוק הגנת הפרטיות ראו גם טיוטת גילוי הדעת של הרשות בנושא "הסכמה בדיני הגנת הפרטיות", שפורסמה להערות הציבור (פברואר 2025). גילוי הדעת זמין כאן.

[18] בתיקון מס' 13 לחוק הורחב תוכן ההודעה לפי סעיף 11 ונקבע כי יש למסור גם פרטים אודות תוצאת אי ההסכמה למסירת המידע, פרטים על בעל השליטה במאגר ועל קיומן של זכות העיון והתיקון המוקנות לנושאי המידע.

[19] ראו סעיפים 11–12 למסמך חובת היידוע; ולהשוואה ראו גם סעיף 13(ב)(3) לחוק זכויות החולה, התשנ"ו-1996.

[20] סעיף 24 למסמך חובת היידוע. להרחבה ולהדגמה של דרכים מוצעות ליישום חובת היידוע ראו סעיפים 4.3 ו-6.2.3(ד) למסמך המדיניות הממשלתי.

מלאכותית ("בוט") – גם היא רכיב חשוב בגיבוש הסכמה מדעת ויש ליידע את נושא המידע לגביה, ככל שעשויה להיות לעובדה זו השפעה מהותית על מתן ההסכמה.[21]

6.3.2. יש ליידע את נושא המידע אודות **פרטי וסוגי המידע** בהם עשויות המערכות להשתמש במסגרת השימוש במידע הנוגע אליו, **והמקור של פרטי מידע אלו.**[22]

6.3.3. ההסבר לנושא המידע צריך להתייחס **לכל אחת ממטרות השימוש** במידע והסיכונים האפשריים הכרוכים בה, לרבות אימון האלגוריתם.

6.3.4. ככל שמטרות השימוש מורכבות יותר, או חורגות מציפייתו הסבירה של נושא המידע או מן המטרה העיקרית לשמה התקשר עם בעל השליטה במאגר, לרבות מערכות בינה מלאכותית כללית – כך נדרש כי תוכן ההסבר הנוגע אליהן **יהיה מפורט ובהיר יותר, וכי האינדיקציה לרצונו ולמודעותו** של נושא המידע למטרת העיבוד ולהשלכותיו **תהיה מפורשת יותר**, כגון בהסכמה נפרדת במתכונת של Opt-in.[23]

6.3.5. **גם כריית מידע אישי מרשת האינטרנט (scraping) לצורך עיבודו במערכת בינה מלאכותית, לרבות למטרת אימון האלגוריתם, כרוכה בפגיעה אסורה בפרטיות, אם לא ניתנה לכך הסכמה מדעת של נושא המידע.**[24] עמדת הרשות היא שגם כאשר אדם מפרסם באופן יזום מידע אודותיו באינטרנט, למשל ברשתות חברתיות, ניתן לייחס לו הסכמה מדעת לכריית המידע ולשימוש בו למטרות כלליות נוספות, **רק** אם תנאי השימוש של האתר לא מייחדים במפורש או במשתמע[25] את השימוש במידע למטרה ספציפית אחרת[26], וגם זאת רק אם נושא המידע בחר שלא להגביל את סוג המשתמשים המורשים להיחשף למידע (כגון חברים בלבד ברשת חברתית). בנוסף, מובן שעל מידע שפורסם באינטרנט חלים גם העקרונות המפורטים בסעיף 6.3.4 לעיל. לפיכך, **גם כאשר אדם מפרסם מידע אודות עצמו ברשת חברתית - לא ניתן יהיה בדרך כלל להסיק מעצם הפרסום הסכמה מדעת לעיבוד המידע אודותיו לצורך**

---

[21] ראו סעיף 5.7 למסמך המדיניות הממשלתי במסגרתו הובאה עמדת הרשות להגנת הפרטיות לגבי רכיבי חובת היידוע. ראו גם סעיף 1 בעמ' 69 לדוח בינה מלאכותית בסקטור הפיננסי.

[22] סעיף 24 למסמך חובת היידוע.

[23] ראו גם סעיף 1 בעמ' 90 לדוח בינה מלאכותית בסקטור הפיננסי. עוד ראו סעיפים 8–9 להנחיית הרשות להגנת הפרטיות מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר". על הסכמה במתכונת של Opt-in בהקשר לזכות החוקתית לפרטיות, ראו פסיקת בית המשפט העליון בעע"מ 1386/07 **עיריית חדרה נ' שנרום** (נבו 16.7.2012), פסקאות 14 ו-17 לפסק הדין.

[24] להרחבה בעניין תחולת חוקי הגנת הפרטיות על כריית מידע מן הרשת, השלכותיה וחובות הרשתות החברתיות ומפעילי אתרים להגנה על מידע מפני כריית מידע (scraping) ראו: "Concluding joint statement on data scraping and the protection of privacy", שפורסמה באוקטובר 2024 בידי קבוצת רשויות הגנת מידע אישי מרחבי העולם. ראו גם סעיף 4 בעמ' 90 לדוח בינה מלאכותית בסקטור הפיננסי.

[25] כך לדוגמא, אם אדם מפרסם מידע באתר שיש לו מטרה מוגדרת כגון אתר היכרויות, עמדת הרשות היא שניתן לייחס לו הסכמה לשימוש במידע רק למטרה המוגדרת כאמור, וזאת גם אם תנאי השימוש באתר לא אוסרים במפורש מטרה אחרת.

[26] כריית מידע אישי מרשת חברתית או מאתר אינטרנט לצורך עיבודו במערכת בינה מלאכותית בניגוד לתנאי השימוש וללא הסכמת נושא המידע גם מפרה לכאורה את האיסור על עיבוד מידע ממאגר ללא הרשאת בעל השליטה במאגר, שנוסף בסעיף 8(ג) לחוק הגנת הפרטיות במסגרת תיקון 13, ועלולה להגיע גם כדי עבירה פלילית לפי סעיף 23נה לחוק, בנוסחו לאחר כניסתו לתוקף של תיקון 13.

אימון או שימוש במידע במערכות מורכבות לגביהן קיים חוסר ודאות גדול בדבר התכליות להן ישמשו וההשלכות והסיכונים הכרוכים בהן[27] – זאת מפני שלא ניתן לייחס לנושאי המידע ידיעה כללית או ציפייה לשימוש במערכות אלו ללא הסבר. **בדומה, לא ניתן יהיה להסיק מפרסום כאמור כי אדם הסכים שהמידע אודותיו ישמש לאימון או למערכת בינה מלאכותית היוצרת סיכון גבוה במיוחד לפרטיות.** כך לדוגמה, אי אפשר יהיה להשתמש בשם ובתמונה שפרסם אדם ברשת חברתית כדי לאמן אלגוריתם של זיהוי פנים אוטומטי או במטרה ליצור מאגר שכזה.[28] קל וחומר שלא ניתן להשתמש למטרת מערכת בינה מלאכותית במידע על אדם שפורסם עליו ברשת בידי אדם אחר. בהמשך לכך גם לא ניתן להסיק מפרסום כאמור את הסכמתו של אדם לקבלת החלטה בעניינו על ידי צד שלישי על בסיס מידע אישי זה, שאיתורו התאפשר באמצעות מידע אישי אחר שמסר נושא המידע לאותו צד שלישי (כגון פרטי הזיהוי שלו).

7. <u>אחריותיות</u>

7.1. **מהי אחריותיות**

7.1.1. בתחום הגנת המידע האישי עיקרון האחריותיות קובע בין השאר את אחריות הארגון לקיום הוראות הדין הנוגעות לשימוש במידע, ואת חובתו לנקוט בשיטות עבודה פנימיות שיישמו את אחריותו ויאפשרו לו להציג ולהוכיח אותה.

7.1.2. אחריותיות מקובלת זה מכבר כדרך התנהלות ראויה בהגנה על מידע אישי, אשר מסייעת לארגון לוודא כי הוא מקיים את ההוראות המהותיות של הדין, מצמצמת את חשיפתו לסיכונים משפטיים ותפעוליים, ותורמת לביסוס האמון בו בעיני לקוחות, שותפים עסקיים, רגולטורים וצדדים שלישיים נוספים.[29]

7.1.3. **חשיבות מיוחדת נודעת ליישום פרקטיקות של אחריותיות בפיתוח ובשימוש בטכנולוגיות בינה מלאכותית**, בשל הפוטנציאל הרב לסיכון לפרטיות, ובמיוחד בשל הקושי המובנה לזהות מבעוד מועד את הסיכונים העתידיים העשויים לנבוע מן

---

[27] למשל מודל בינה מלאכותית כללית - '**general-purpose AI model**'. להשוואה ראו ההגדרה בסעיף 3(63) לחוק הבינה המלאכותית האירופי:
" '**general-purpose AI model**' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;"

[28] ראו לעניין זה את הנחיית ה-EDPB – "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", בסעיף 76 להנחיה, הזמינה כאן.

[29] להרחבה ראו: OECD Privacy Guidelines Implementation Guidance: Foreword and Chapter on Accountability (2023). זמין כאן.

השימוש בטכנולוגיות אלה וההשלכות שיהיו להן בהיבטי פרטיות והגנת מידע אישי. כמו כן, המאפיין האוטונומי של מערכות אלה, המאפשר את פעולתן ללא מעורבות אנושית, מעורר מורכבויות ביישום המבנה המקובל של הטלת אחריות משפטית על אדם הנמצא במוקד ההתרחשות המזיקה. כפי שנאמר במסמך המדיניות הממשלתית, "ככל שהמעורבות האנושית בהחלטה או בפעולה מצטמצמת ורחוקה יותר, אתגר זה מתחדד ומתעוררות שאלות בנוגע לנשיאה באחריות בגין טעויות שנגרמו אגב השימוש במערכות....המונח אחריותיות מתייחס ככלל לצורך בכך שיהיו גורמים מתאימים שיוודאו כי המערכת מפותחת ופועלת בהתאם לתפקיד שהוגדר לה ולסביבה הרגולטורית הרלבנטית".[30]

7.1.4. האחריותיות כעיקרון כללי בתחום עיבוד המידע, ודרישות קונקרטיות הנגזרות ממנו, הפכו לעקרון יסוד ולחובות בנות אכיפה בחקיקת הגנת מידע אישי מתקדמת בעולם, כולל ב-GDPR האירופית.[31] היבטים מסוימים של אחריותיות באים לידי ביטוי גם בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: **תקנות אבטחת המידע**).[32]

7.1.5. בתחום הגנת המידע האישי, הפרקטיקות המרכזיות המקובלות מתחום האחריותיות כוללות ממשל תאגידי, מינוי ממונה על הגנת הפרטיות בארגון, ביצוע מוקדם של תסקיר השפעה על הפרטיות, וקיום עקרון העיצוב לפרטיות (Privacy by Design).

מינוי ממונה על הגנת הפרטיות

7.1.6. בתוך כך, מינוי ממונה על הגנת הפרטיות (DPO) שיתכלל את הטיפול בכלל היבטי הפרטיות בעיבוד מידע אישי בארגון, הוא פרקטיקה מקובלת שאת חשיבותה ויתרונותיה לארגון ולזכות לפרטיות גם יחד – פירטה הרשות בהרחבה במסמך מקיף שפרסמה בנושא.[33] כמו כן, במסגרת תיקון 13 לחוק הגנת הפרטיות נקבעה חובה רחבה למינוי ממונה על הגנת הפרטיות בכלל הגופים הציבוריים במשק ובשורה ארוכה של גופים במגזר הפרטי, בהתאם לתנאים המנויים בסעיף 17ב1 לחוק, אשר נוסף בתיקון 13, ובין השאר בגוף שהוא בעל שליטה או מחזיק במאגר מידע שעיסוקו

[30] סעיף 4.6 למדיניות הממשלתית; ראו גם מסמך המדיניות של ה-OECD בנושא: Advancing Accountability In Ai Governing And Managing Risks Throughout The Lifecycle For Trustworthy AI (2023). זמין כאן. עוד ראו: OECD AI, Data Governance and Privacy: Synergies and Areas of International Co-operation (2024). זמין כאן.

[31] Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 5(2).

[32] למשל בסעיפים 2, 5, 16 ו-19 לתקנות אבטחת מידע.

[33] להרחבה ראו מסמך ההמלצות של הרשות להגנת הפרטיות "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו" (2022). המסמך זמין כאן.

העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר[34] - תנאים שקיימת סבירות גבוהה שיתקיימו לפחות כתוצאה מאימון של מודלים של בינה מלאכותית. בעידן הבינה המלאכותית, סבורה הרשות שמינויו של ממונה הגנת פרטיות ארגוני מקבל משנה חשיבות ותוקף, והופך לרכיב משמעותי במתן מענה הולם לקפיצת המדרגה בסיכוני הפרטיות הנובעים מעיבוד המידע האישי בארגון. למעשה, במקרים רבים **ממונה הגנת הפרטיות עשוי להיות גם הגורם המתאים והמיומן ביותר ליטול על עצמו את המשימה לתכלל גם את הטיפול בסוגיות הנובעות משימוש במערכות בינה מלאכותית בארגון**, לפחות כל עוד לא מונה בארגון בעל תפקיד ייעודי; הגם שהסיכונים והאתגרים הנובעים מפיתוח של מערכות בינה מלאכותית ומן השימוש בהן, חורגים מעבר לזכות לפרטיות ולהגנת המידע האישי, הרי שהידע והניסיון של ממוני הגנת הפרטיות מקנים להם בדרך כלל מידה לא מבוטלת של הבנה ומיומנות שלא מצויה אצל גורמים אחרים בארגון.

7.2. **תסקיר השפעה על פרטיות**

7.3. תסקיר השפעה על פרטיות (Privacy Impact Assessment או Data Protection Impact Assessment) הוא רכיב מרכזי בתפיסת האחריותיות. תסקיר הוא תהליך מתודולוגי המנתח באופן מקיף ושיטתי את השפעת עיבוד המידע על הפרטיות של מי שהמידע על אודותיו נאסף או מוחזק, מזהה את מכלול הסיכונים לפרטיות, בוחן חלופות ומציע את הדרך לצמצם את אותם סיכונים למינימום.[35]

7.4. התסקיר נועד לשמש ארגונים לזיהוי וצמצום הסיכון לפרטיות במהלך הקמה וניהול של פרויקטים חדשים בעלי השפעה על הפרטיות, במיוחד מערכות טכנולוגיות ופרויקטים הכרוכים באיסוף ובעיבוד של מידע אישי. השימוש בתסקיר מסייע בזיהוי סיכונים לפרטיות והפרות של הוראות החוק או התקנות בשלב מוקדם, ובכך מקל על ההתמודדות עימם בצורה פשוטה ויעילה יותר, ומצמצם את החשיפה של הארגון לסיכונים משפטיים ותפעוליים.

7.5. הדין בישראל לא כולל אמנם חובה לעריכת תסקיר השפעה על הפרטיות בטרם עיבוד מידע אישי.[36] אולם, **עמדתה של הרשות היא שעריכתו של תסקיר השפעה על הפרטיות, או הליך מתודולוגי דומה, בטרם שימוש במערכות בינה מלאכותית לעיבוד מידע אישי**, ודאי

---

[34] סעיף 17ב1(א)(4) לחוק.

[35] להרחבה ראו מדריך עזר מתודולוגי לעריכת תסקיר השפעה על הפרטיות (2022), שפרסמה הרשות להגנת הפרטיות, זמין כאן.

[36] יצוין, עריכת התסקיר הפכה זה מכבר לחובה החלה על כל ארגון הכפוף ל-GDPR בנסיבות המפורטות בסעיף 35(1) ל-GDPR, וכן נדרשת בחקיקת הגנת מידע אישי במדינות רבות נוספות בעולם. ככזו, היא חלה כבר היום ביחס לארגונים ישראליים הפועלים במדינות זרות בהן מוטלת חובה זו, וכפופים לרגולציה הנוהגת בהן.

במערכות בינה מלאכותית בסיכון גבוה,[37] היא הדרך המיטבית המומלצת **לארגונים לוודא ולהוכיח כי השימוש במערכות אלו עומד בדרישות דיני הגנת הפרטיות:** [38]

7.5.1. **עבור רשויות ציבוריות ובעלי מאגרים אחרים הכפופים לדרישת המידתיות** (כגון בעת עיבוד מידע אישי במסגרת יחסי עבודה או עיבוד המסתמך על הגנות סעיף 18), עמדת הרשות היא כי **תסקיר הוא הכלי המיטבי והמומלץ** לוודא ולהוכיח כי קיים קשר רציונלי בין הפגיעה בפרטיות בשימוש בבינה מלאכותית לבין השגת המטרה, כי לא קיימת חלופה שפגיעתה בפרטיות פחותה, וכי התועלת הצפויה מן השימוש במערכת עולה על הפגיעה הצפויה בפרטיותם של נושאי המידע;

7.5.2. עריכת תסקיר תסייע בין היתר בתיאור אופן פעולת המערכת, הסיכונים וההשלכות הנובעים ממנה על זכויות נושאי המידע, כנדרש כדי **לעמוד בחובת היידוע הקבועה בסעיף 11 לחוק והנדרשת גם לביסוס הסכמה מדעת של נושאי המידע**, בהתאם למפורט בסעיף 6 לעיל;

7.5.3. **עבור כלל בעלי המאגרים במשק**, עריכת תסקיר תאפשר לגבש תיאור מספק ומדויק של פעולות האיסוף והשימוש במידע, של מטרות השימוש במידע ושל הסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עמם – **הנדרשים כיום לקיום החובה להכין מסמך הגדרות מאגר**, לפי תקנה 2(א) לתקנות אבטחת המידע, כמו גם **לקיום החובה השנתית לבדוק האם קיים במאגר מידע עודף, רב מן הנדרש למטרות המאגר**, המתחייבת לפי תקנה 2(ג).

7.6. ממשל תאגידי אף הוא רכיב מרכזי בתפיסת האחריותיות. מדובר ביצירת מחויבות כלל ארגונית לציות לחוק ולקידום ההגנה על הפרטיות בהובלת הדרג הבכיר של הנהלת החברה וחבר הדירקטורים שלה; חלוקת משימות ותפקידים; וכינון מנגנוני פיקוח ובקרה פנימיים נאותים. כמפורט בהנחיית הרשות להגנת הפרטיות מס' 1/2024, על דירקטוריון חברה שעיבוד מידע אישי מצוי בליבת הפעילות שלה, או שפעילותה יוצרת סיכון גבוה לפרטיות, מוטלת חובה לפקח על ציות החברה להוראות החוק ותקנות אבטחת המידע, ונדרשת מעורבת משמעותית של הדירקטוריון בביצוע דרישות מרכזיות לפי תקנות אלו.[39] עוד נקבע בהנחיה, כי ביחס לחברות אלו באחריות הדירקטוריון לוודא גיבוש, אימוץ ויישום של מדיניות בדבר אופן ביצוע דרישות החוק והתקנות בחברה; כי על המדיניות להתייחס בין היתר לאופן השימוש במידע אישי בחברה **וניהולו בנושאים מהותיים**; ועליה להגדיר תהליכי פיקוח, בקרה, וציות אפקטיביים. לנוכח הסיכון הרב לפרטיות ולזכויות

[37] להשוואה: סעיף 27 לחוק הבינה המלאכותית האירופי מחייב משתמשים במערכות בינה מלאכותית בסיכון גבוה לערוך "Fundamental Rights Impact Assessments".
[38] ראו גם סעיף 1 בעמ' 9 לדוח בינה מלאכותית בסקטור הפיננסי.
[39] להרחבה ראו "הנחיית הרשות להגנת הפרטיות מס' 1/2024: תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)" הזמינה כאן.

יסוד אחרות הגלום בשימוש במידע אישי במערכות בינה מלאכותית, יש לראות בו נושא מהותי ביחס לניהול המידע האישי בחברה לעניין זה.

8. **<u>דיוק המידע האישי וזכויות נושא המידע</u>**

8.1. סעיף 14(א) לחוק הגנת הפרטיות מקנה לאדם שמצא כי המידע שעליו אינו נכון, שלם, ברור או מעודכן, זכות לפנות לבעל השליטה במאגר המידע בבקשה לתקן את המידע או למוחקו. כאמצעי למימוש הזכות לדרוש את תיקון המידע, מקנה סעיף 13(א) לחוק לכל אדם (יחיד) זכות לעיין במידע שעליו, המוחזק בכל מאגר מידע. **הרשות מבהירה כי במערכות בינה מלאכותית הזכות לבקש תיקון מידע שגוי עשויה בנסיבות מסוימות ובהתאם להקשר להתייחס גם לתיקון האלגוריתם שהפיק מידע כאמור**, ככל שאין דרך אחרת למנוע מן האלגוריתם לשוב ולהפיק מידע שגוי.[40]

8.2. בנוסף על זכותו של נושא המידע **לבקש** תיקון מידע, הרי שביחס למידע שהגיע מן האזור הכלכלי האירופי או מידע אחר הכלול באותו מאגר מידע יחד עמו – מטילה תקנה 5(א) לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023 (להלן: "**תקנות מידע מהאזור הכלכלי האירופי**") על בעל השליטה במאגר **חובה להפעיל באופן יזום מנגנון שמטרתו להבטיח כי המידע שבמאגר המידע נכון, שלם, ברור ומעודכן**.[41] בכל הנוגע לפיתוח ולהפעלה של מודלים מבוססי בינה מלאכותית, משמעות חובה זו היא בין השאר להפעיל מנגנונים למניעת "מתקפות שמטרתן לגרום למערכת **ללמוד** את הדבר הלא-נכון (Learn the wrong thing); ומתקפות שמטרתן לגרום למערכת **לעשות** את הדבר הלא-נכון (Do the wrong thing)",[42] וזאת בין השאר באמצעות הקפדה על איכות המידע המשמש לאימון המערכת, הרלבנטיות שלו למטרתה, קיום הסברתיות של האלגוריתם, ביצוע בקרות איכות קפדניות ועוד.[43]

8.3. לאור החשיבות המיוחדת של הדיוק והאמינות של המידע המעובד ומופק במערכות בינה מלאכותית, **בכוונת הרשות לשים דגש על האכיפה של סעיפים 13 ו-14 לחוק הגנת הפרטיות ושל תקנה 5 לתקנות מידע מהאזור הכלכלי האירופי ביחס למערכות בינה מלאכותית**.

---

[40] ראו לעניין זה את הנחיית רשות הגנת המידע בבריטניה (ICO) בנושא בינה מלאכותית והגנת מידע, בדגש על הפרק העוסק בהבטחת זכויות נושאי המידע במערכות בינה מלאכותית, זמין כאן. ראו גם את הנחיית נציב הפרטיות הפדרלי של קנדה – Principles for responsible, trustworthy and privacy-protective generative AI technologies – בסעיף 6 להנחיה, הזמינה כאן.

[41] בהתאם לתקנה 9(2) לתקנות מידע מהאזור הכלכלי האירופי, החל מיום 1.1.2025 חלה חובה זו גם ביחס למידע שמקורו ישראלי, אם הוא מצוי במאגר שמצוי בו גם מידע שהתקבל מהאזור הכלכלי האירופי.

[42] ראו סעיף 4.5.2 למסמך המדיניות הממשלתי.

[43] להרחבה על דרכים להבטיח אמינות, עמידות ובטיחות של מערכות בינה מלאכותית, ראו סעיף 5.5 למסמך המדיניות הממשלתי.

9. <u>אבטחת מידע</u>

9.1. הסיכונים המיוחדים הכרוכים בשימוש במערכות בינה מלאכותית, מחייבים לנקוט זהירות יתרה ולהקפיד על הדגשים שלהלן לצורך קיום חובת אבטחת המידע הקבועה בסעיף 17 לחוק ובתקנות אבטחת המידע. זאת הן לעניין ארגונים שמערכות הליבה הפנימיות שלהם מבוססות בעצמן על בינה מלאכותית, והן לעניין ארגונים אחרים אשר עובדיהם עושים שימוש באפליקציות ובטכנולוגיות חיצוניות מבוססות בינה מלאכותית, כדוגמת ChatGPT, מערכות בינה מלאכותית יוצרת אחרות, ומערכות בינה מלאכותית בכלל.

9.2. על רבים ממאגרי המידע שמערכות המאגר שלהם מבוססות בינה מלאכותית, יחולו רמות אבטחת המידע הבינונית או הגבוהה **בשל סוג והיקף המידע המוחזק או מעובד בהם בפועל** (וכן בשים לב לזהות בעל השליטה במאגר ולמספר מורשי הגישה אליו), בהתאם למפורט בתוספת הראשונה או השנייה לתקנות אבטחת המידע.

9.3. מבלי לגרוע מהאמור בסעיף 9.2, בכוונת הרשות לבחון, מכוח סמכותה לפי תקנה 20(א)(1) לתקנות אבטחת המידע, האם ישנם טעמים המצדיקים החלה של רמת אבטחה גבוהה על מאגרי מידע מסוימים, בשל העובדה שמערכותיהם מבוססות בינה מלאכותית בסיכון גבוה.

9.4. מודלים של בינה מלאכותית מאפשרים הסקת נתונים חדשים על בסיס מאגרי מידע נרחבים אשר שימשו לאימון המערכת.[44] לפיכך, ניהול מאגרי מידע מבוססי בינה מלאכותית כרוך בסיכוני אבטחת מידע ייחודיים, כגון "**מתקפות הסקה**" המיועדות לחלץ שרידי מידע אישי ניתן לזיהוי שנותרו באלגוריתם, או להסיק ולהפיק מחדש מידע אישי אשר שימש לאימון המודל אך לא היה אמור להישאר במערכת בשלב התפעולי שלה. כמו גם התקפות אשר נועדו לעקוף בקרות מפצות המצויות במאגר מתוך שאיפה להתגבר על אלו.[45]

9.5. לסיכונים הנובעים ממתקפות אלה,[46] יש להתייחס ולתת מענה קונקרטי בעת יישום תקנות אבטחת המידע, בין השאר –

---

[44] מיכאל בירנהק תיאר זאת כך: "בינה מלאכותית מאתרת דפוסים שיצרה על בסיס ניתוח המידע שלמדה ומשתמשת בהם. הדפוסים כלליים, ולאחר שנוצרו, ניתן להשוות אליהם נתונים של אדם מסוים. לשם כך דרוש מידע נוסף על אותו אדם. התוצאה תהיה מסקנה לגבי האדם: זיהוי, סיווג, הערכה, או תחזית לעתיד. הפלט המוסק אינו בהכרח מידע שנמסר על ידי האדם במפורש או תוך כדי התנהגותו, וגם אינו חוות דעת על האדם. המידע מוסק מתוך המידע על האדם המסוים, תוך השוואה למידע שנאסף על אנשים רבים אחרים (מיכאל בירנהק "פרטיות ובינה מלאכותית" (מיועד לפרסום **במשפט חברה ותרבות** ח (2025)). טיוטת המאמר זמינה כאן.

[45] להרחבה ראו סעיף 4.5.2 למדיניות הממשלתית, וכן הצהרת מדינות ה-G7 ביחס לבינה מלאכותית יוצרת: https://www.priv.gc.ca/en/opc-news/speeches/2023/s-d_20230621_g7.

[46] כגון: "**membership inference** attacks, **model evasion** attacks or even a **model inversion**"; ראו פרסום של רשות הגנת הפרטיות הצרפתית (CNIL): AI: ensuring GDPR compliance.

9.5.1. בתיאור הסיכונים ואופן ההתמודדות עמם במסמך הגדרות המאגר, שהכנתו נדרשת לפי תקנה 2(א) לתקנות, תוך התייחסות מפורשת להשלכות השימוש במערכות בינה מלאכותית;

9.5.2. בסקר הסיכונים ובמבדקי החדירות אותם יש לערוך לפי תקנה 5 לתקנות;

9.5.3. בניטור ומעקב שוטף אחר מתקפות הסקה על מאגרי הארגון, ובדיווח מיידי לרשות להגנת הפרטיות על מתקפות הגורמות לאירוע אבטחה חמור, כנדרש לפי תקנה 11(ד)(1) לתקנות.[47]

9.6. כדי למזער סיכונים אלה, יש לתת דגש מיוחד גם לעקרון צמצום המידע הבא לידי ביטוי בתקנה 2(ג) לתקנות אבטחת המידע, המחייבת כל בעל מאגר מידע אישי לבחון אחת לשנה אם הוא מחזיק במאגר מידע עודף, שאינו דרוש עוד למטרות המאגר.[48]

9.7. גם התפוצה הגוברת במהירות של אפליקציות ושירותים חיצוניים מבוססי בינה מלאכותית יוצרת – ChatGPT, DALL-E, Midjourney, Copilot ואחרים – משנה באורח דרמטי את תמונת איומי אבטחת המידע. בין הסיכונים המרכזיים ניתן למנות דליפה של מידע אישי שנכלל בשאילתה שהוזנה לשירות החיצוני, שימוש במידע לצרכים החורגים ממטרת המאגר המקורי (לרבות למטרת אימון האפליקציה), או חשיפתו בפני צדדים שלישיים בלתי מורשים (כגון משתמשים אחרים של האפליקציה מחוץ לארגון). התועלת העצומה לארגון, שיפור וייעול תהליכי העבודה, הנגישות הגבוהה וקלות השימוש - הופכים את אפליקציות הבינה היוצרת לרכיב מרכזי במחזור החיים של עיבוד המידע האישי בארגון. זאת, הן בהתקשרויות של הארגון עם ספקים חיצוניים לצורך עיבוד מידע (מחזיקים), והן בהסתייעות של עובדים במערכות חיצוניות אלה, אף שלא במסגרת התקשרות רשמית של הארגון. שינוי זה מחייב את בעלי השליטה במאגרים להיערכות הולמת ולקביעת מדיניות ארגונית ייעודית שתיתן מענה לסיכוני האבטחה הנובעים מכך.[49] על המדיניות הייעודית ונהלי אבטחת המידע להסתייעות במערכות חיצוניות של בינה מלאכותית יוצרת להתייחס בין השאר לסוגיות הבאות:

9.7.1. בחינת הסיכונים הנובעים מהסתייעות בשירות בינה מלאכותית יוצרת בדרך של חשיפת מידע אישי המהווה פגיעה אסורה בפרטיות או הפרה של חובת הסודיות[50]; קביעה מי ממורשי הגישה בארגון רשאי להסתייע בשירות חיצוני כאמור ומיהו הדרג

---

[47] ראו: הרשות להגנת הפרטיות, דיווח על אירוע אבטחה חמור.
[48] ראו טיוטת מסמך מדיניות בנושא צמצום מידע (Data Minimization) שפרסמה הרשות להגנת הפרטיות, אשר מפרט בהרחבה את חשיבות העיקרון בהגנה על הזכות לפרטיות ומצביע על המקורות בו הוא מחויב לפי דין. המסמך זמין כאן.
[49] להרחבה ראו: A CISOs Guide: Generative AI and ChatGPT Enterprise Risks.
[50] ראו למשל "גילוי דעת מקדים בעניין שימוש בבינה מלאכותית בעבודת עורך הדין" מטעם ועדת האתיקה של לשכת עורכי הדין, לעיל ה"ש 11.

המאשר; מהי מטרת השימוש; ואילו סוגי מידע אישי ניתן לחשוף בעת ההסתייעות בשירות.

9.7.2. בחינת סיכוני האבטחה הכרוכים בהתקשרות עם האפליקציה החיצונית ואופן קיום שאר הוראות תקנה 15 לתקנות אבטחת מידע ביחס לשימוש הארגוני באפליקציה – בין השאר בהתחשב במשך שמירת המידע הכלול בשאילתות המוזנות לאפליקציה והיכולת למנוע שימוש בו למטרת אימון האלגוריתם שלה, או לכל מטרה אחרת החורגת ממטרת המאגר המקורי;

9.7.3. הגדרת אפליקציות חיצוניות המותרות לשימוש בידי עובדי הארגון, או אסורות עליהם;

9.7.4. כללים בדבר חובת הארגון והעובדים לעשות שימוש באפליקציה באופן שיצמצם ככל הניתן את סיכוני האבטחה והפרטיות, לרבות סירוב לשימוש במידע הכלול בשאילתה לאימון האלגוריתם או למטרות אחרות החורגות מתכלית השאילתה, וצמצום למינימום של משך שמירת השאילתה באפליקציה.

9.7.5. הדרכת העובדים בעניין סיכוני האבטחה המיוחדים לשימוש במערכות בינה מלאכותית יוצרת.

10. <u>כריית מידע</u>

בעלי שליטה במאגרי מידע המאפשרים שיתוף מידע אישי ברשת האינטרנט (למשל ברשתות חברתיות, בשירותי מכירות או היכרויות) נדרשים לנקוט באמצעים נאותים כדי למנוע כריית מידע (scraping) אסורה מאתרי האינטרנט שהם מנהלים.[51] חובה זו, נובעת לכל הפחות מתקנות 9 ו-14 לתקנות אבטחת המידע,[52] וביצועה של כרייה אסורה של מידע אישי מן המאגר, **היא בבחינת "אירוע אבטחה חמור" – עליו חייב בעל המאגר לדווח באופן מיידי לרשות להגנת הפרטיות**, כנדרש בתקנה 11(ד) לתקנות אבטחת המידע. החובה לנקוט אמצעים למניעת כרייה אסורה מקבלת משנה תוקף לנוכח הצורך הגובר והולך של מפתחי מערכות בינה מלאכותית לעשות שימוש במידע אישי כבסיס למטרת אימון המודלים, וההשלכות המשמעותיות הצפויות על זכויותיהם של נושאי המידע.[53]

[51] למשל משום שאינה עומדת בתנאים המפורטים בסעיף 6.3.5 לעיל.
[52] תקנה 9 קובעת חובה לנקוט אמצעים מקובלים בנסיבות העניין כדי לוודא כי הגישה למאגר נעשית רק בידי בעל הרשאה המורשה לכך. תקנה 14 קובעת איסור לחבר את מערכות המאגר לרשת האינטרנט בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית.
[53] להרחבה, כולל פירוט של אמצעים נאותים לצמצום כרייה בלתי חוקית, ראו ההצהרה המשותפת בעניין כריית מידע (scraping) שפורסמה בשנת 2024 בידי קבוצת רשויות הגנת מידע אישי מרחבי העולם, לעיל ה"ש 24.

11. <u>חובת רישום מאגרי מידע מבוססי טכנולוגיות בינה מלאכותית וחובת הודעה על ניהולם</u>

11.1. סעיף 8(ג) לחוק הגנת הפרטיות קובע שורה של נסיבות בהן חלה על בעל השליטה במאגר מידע חובה לרשום את המאגר בפנקס בטרם תחילת פעילותו. בהתאם לסעיף 8(א) אסור לנהל או להחזיק מאגר שלא נרשם כנדרש. לאחר כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות, תוטל חובת הרישום על מאגרים שמטרתם העיקרית איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, ועל מאגרי מידע שבעלי השליטה בהם הם גופים ציבוריים. כמו כן, על ניהולם של מאגרים הכוללים מידע בעל רגישות מיוחדת על 100 אלף נושאי מידע ומעלה, תוטל חובת הודעה לרשות, כולל מסירת העתק ממסמך הגדרות המאגר.[54]

11.2. כאמור בסעיף 10(א)(1) לחוק, בהחלטתה האם לאשר את רישום המאגר, נדרשת הרשות לבחון האם "המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין"; כמו כן, בהתאם לסעיף 10(ו) לחוק, מוסמך ראש הרשות לבטל רישום מאגר או להתלות את תוקפו אם "הפר מחזיק או בעל של מאגר מידע הוראות של חוק זה או התקנות לפיו, או לא מילא אחר דרישה שהפנה אליו הרשם".

11.3. כלומר, במסגרת תהליך הרישום רשאית הרשות לבדוק, בין היתר, **אם עצם איסוף המידע או צבירתו** במערכת הבינה המלאכותית, מפרים הוראות דין, ואם השימוש במידע **מפר את הוראות חוק הגנת הפרטיות או פוגע בפרטיות נושאי המידע** באופן בלתי חוקי, לרבות כאשר מאגר המידע **משמש רשות ציבורית**, ואיסוף המידע אליו או עיבוד המידע בו פוגעים בפרטיות ללא הסמכה מפורשת בחוק או במידה העולה על הנדרש.

11.4. כמו כן, סמכותו של ראש הרשות לפי סעיף 10(א)(1) לחוק לסרב לרשום מאגר גם "אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן", נועדה בין היתר למנוע ניצול של עיבוד ממוחשב של מידע אישי למטרות לא חוקיות.[55]

11.5. היכולות מעוררות ההשתאות של מערכות מבוססות בינה מלאכותית כיום, שאחריתן מי ישורנה, מעצימות בקצב אקספוננציאלי את הסיכון הצפוי לביטחונו, שלומו ורווחתו של הציבור אם מאגרי מידע ינוצלו, באמצעות מערכות בינה מלאכותית, לפעולות בלתי חוקיות. אולם, כיוון שהסמכות בסעיף 10(א)(1) עשויה להתנגש באינטרסים מוגנים אחרים של בעלי השליטה במאגרים, סבורה הרשות שיש להפעיל אותה בזהירות ותוך

---

[54] סעיף 8א לחוק הגנת הפרטיות, כנוסחו לאחר כניסתו לתוקף של תיקון 13.

[55] ביטוי מובהק נוסף לתכלית רחבה זו של חוק הגנת הפרטיות, מודגם בתקנה 1 לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001: "לא יעביר אדם מידע ולא יאפשר העברה של מידע ממאגר מידע בישראל אל מחוץ לגבולותיה, אלא אם כן דין המדינה שאליה מועבר המידע, מבטיח רמת הגנה על מידע שאינה פחותה, בשינויים המחויבים, מרמת ההגנה על מידע הקבועה בדין הישראלי, ובכלל זה קובע עקרונות אלה:
(1) מידע ייאסף ויעובד **באופן חוקי והוגן**".

ריסון, רק במקרים של אי חוקיות מובהקת הכרוכה בסיכון גבוה לביטחונו, שלומו או רווחתו של הציבור.

11.6. כנדרש בסעיף 9(ב) לחוק, **יש לציין בבקשת הרישום מהי המטרה הברורה והמדויקת של המערכת,** ולוודא כי המטרה וסוגי המידע המפורטים בבקשה מתאימים לשלב הרלבנטי – אימון או יישום. זאת, בין השאר כדי לוודא כי ייאסף ויעובד רק המידע המינימאלי הדרוש למימוש המטרה שהוגדרה למערכת מראש. בשינויים המחויבים, יפים הדברים גם לתיאור מטרות השימוש במסגרת מסמך הגדרות המאגר, כנדרש לפי תקנה 2(א)(2) לתקנות אבטחת המידע.