

לשכת הייעוץ המשפטי

טלפון: 02-5428150

פקס: 02-5898762

ה' בתשרי, התשפ"ה

07 אוקטובר 2024

מספרנו: 88682624

מסמך הנחיה - עקרונות ואתיקה של פיתוח ושימוש במערכות בינה מלאכותית

1. כללי

- 1.1 עם התפתחות הטכנולוגיה, הבינה המלאכותית התקדמה באופן משמעותי ויכולותיה רבות ובעלות משמעויות קריטיות. שימוש אחראי בבינה מלאכותית הוא אמצעי לעידוד צמיחה, התפתחות וקידום המשטרה בתחום החדשנות. ליכולות אלה יתרונות ופוטנציאל קידום עצום לחברה ולמערכת אכיפת החוק, אולם יש בכך גם סיכונים משמעותיים לזכויות אדם, למערכת שלטון החוק ולמשטר הדמוקרטי.
- 1.2 לאור כך, השימוש במערכות בינה מלאכותית מחייב גילוי אחריות ביחס לשימוש בהן ובהשפעותיהן. הדבר משמעותי במיוחד עבור מערכות לאכיפת חוק, שכן אלו פועלות בהתאם לסמכויות המוקנות להן ע"פ דין ובהתאם מוסמכות לפגוע בזכויות אדם לשם ביצוע פעולות לאכיפת חוק.
- 1.3 מטרת מסמך זה להבהיר את הסכנות והאתגרים בהפעלתן של מערכות בינה מלאכותית במסגרת פעילות המשטרה ולתאר את עקרונות המסגרת האתית להפעלתן של מערכות אלו בשירות המשטרה. כמו כן, לצד מסמך זה ולשם השלמת בחינתן הפרקטית ואישורן של הפעלת מערכות בינה מלאכותית בשירות המשטרה יש לעקוב אחר פרוטוקול ניהול הסיכונים המצורף כנספח א' למסמך זה.

2. הגדרות

- 2.1 **בינה מלאכותית** - שם כולל להתפתחות בתחום טכנולוגיות המידע, התקשורת ומדעי הנתונים, המאפשרת קבלת החלטות, ייצור תחזיות, או ביצוע פעולות על ידי מחשב ברמת עצמאות גבוהה, באופן המדמה או מסוגל להחליף בינה אנושית.
- 2.2 **מערכת מבוססת בינה מלאכותית** - מערכת ממוכנת שיכולה, בהתאם למטרות מוגדרות בידי אדם, להפיק תחזיות, המלצות, או החלטות המשפיעות על סביבות פיזיות או וירטואליות, ומתוכננת לפעול ברמת עצמאות משתנה.

- 2.3. **כלי לניהול סיכונים** – כלי או פרוטוקול לניתוח רמת הסיכון הנשקפת מפיתוח ושימוש במערכות בינה מלאכותית ובאמצעותו ניתן להגדיר את רמת הסיכון הגלומה במערכת: סיכון "בלתי מקובל" ולכן אסור באופן גורף; "סיכון גבוה" ולכן מצריך בחינה מראש וכפוף לשורה של דרישות מפורטות; "סיכון מוגבל" ולכן מחייב מגבלות ודרישות בהיקף מצומצם יחסית.
- 2.4. **מחזור החיים של מערכת בינה מלאכותית** - שלבי יזום המערכת, עיצובה, פיתוח ותכנות (ארכיטקטורה), בחינת הסיכונים, עריכת ניסויים, הפעלתה בפועל, ועד לשלבי פיקוח ובקרה והסקת מסקנות לטיוב פעולת המערכת.

3. **אתגרים וסיכונים בהפעלת מערכות בינה מלאכותית** – לצד היתרונות המשמעותיים למערכות

אכיפת החוק בשימוש בבינה מלאכותית גלומים גם סיכונים ביחס לזכויות הפרט ושמירה על שלטון החוק והדמוקרטיה כגון:

- 3.1. **אפליה** - חשש לאפליה ביחס לאוכלוסיות בשל הטיות המבוססות על מאגרי מידע לא ייצוגיים או כאלו המשקפים הטיה קיימת.
- 3.2. **אוטונומיה** - חוסר מעורבות אנושית מספקת במערכת עלולה להביא לקבלת החלטות שגויות, שרירותיות או בררניות וכן מעלה סוגיות מוסריות של אחריותיות כלפי הפעלת המערכת.
- 3.3. **העדר הסברתיות** - חשש להתבססות על יכולות חישוביות היוצרות תחזיות וקבלת החלטות שלעיתים לא ניתן לחלץ מתוך המערכת על מנת להסביר את פעולותיה (black box).
- 3.4. **העדר שקיפות** - חשש שאנשים לא יהיו מודעים לכך שלמערכות בינה מלאכותית יש תפקיד משמעותי "מאחורי הקלעים" בקבלת ההחלטות בעניינם, שהם משוחחים עם מערכות ולא עם אנשים (למשל במערכות צ'אט-בוט) או שהם נחשפים לתכנים שנוצרו על ידן (ובכך להיחשף ל-deep fake או fake news).
- 3.5. **אמינות, עמידות, אבטחה ובטיחות** - חשיפה לטעויות ותקלות טכניות, או למניפולציות מכוונות.
- 3.6. סוגיות של **הפרת הפרטיות והגנת המידע** שכן מערכות בינה מלאכותית מבוססות על מאגרי נתוני עתק (big data).

4. **עקרונות האתיקה** - עקרונות האתיקה של פיתוח ושימוש משטרתי במערכות בינה מלאכותית הן:

- 4.1. **שמירה על עקרון שלטון החוק** – שימוש אחראי במערכות בינה מלאכותית בהתאם להוראות כל דין.
- 4.2. **כיבוד זכויות יסוד ואינטרסים ציבוריים** – פיתוח ושימוש בבינה מלאכותית תוך כיבוד זכויות יסוד ואינטרסים ציבוריים ובפרט תוך שמירה על כבוד האדם ועל הזכות לפרטיות.
- 4.3. **שוויון ומניעת אפליה פסולה** – שימוש במערכות בינה מלאכותית תוך עידוד ושמירה על עיקרון השוויון ומניעת אפליה פסולה ביחס לקבוצות או יחידים.

- 4.4. שימוש לתכלית ראויה באמצעות פיתוח כלים מתקדמים ויעילים לאכיפת החוק לשם ביצוע תפקידיה וחובותיה של המשטרה על פי דין, ובהתאם לסעיפים 3-5 לפקודת המשטרה.
- 4.5. **שקיפות והסברתיות** – יידוע מי שבא במגע עם בינה מלאכותית או מושפע מפעילותה על כך, וכן צורך במתן הסבר להחלטתה או לאופן שבו פעלה, במידת האפשר.
- 4.6. **אמינות, עמידות, אבטחה ובטיחות** – יש לוודא כי מערכות בינה מלאכותית תהיינה אמינות, מאובטחות ובטיחותיות לאורך כל "מחזור חייהן", כך שבתנאי שימוש רגילים, שימוש צפוי או שימוש שגוי או תנאים מסוכנים אחרים, הן יפעלו כראוי ולא יהוו סיכון בטיחותי בלתי סביר.
- 4.7. **אחריותיות** – מפתחי בינה מלאכותית, מפעיליה או המשתמשים בה יגלו אחריות לתפקודה התקין, ולקיום העקרונות האתיים האחרים בפעילותם, בין היתר בשים לב לתפיסות מקובלות של ניהול סיכונים ולאפשרויות הטכנולוגיות הזמינות.

5. רגולציה פנים משטרתית להסדרת השימוש בבינה מלאכותית

- 5.1. בהתאם להחלטת ממשלת ישראל ביחס לחקיקה בנושא הבינה המלאכותית, הרגולציה תהיה ענפית ולא רוחבית. היינו, ההסדרה תהיה מותאמת לכל סקטור בהתאם למאפייניו הייחודיים.
- 5.2. בהתאם לכך, ההסדרה הפנים משטרתית תהיה מותאמת ככלל לסיכונים הנשקפים **מסוג הטכנולוגיה ומהשימוש הספציפי** שאותו היא נועדה להסדיר, ותהיה תוצר של ניהול סיכונים ביחס למערכת הקונקרטי. הרגולציה לא תחול באופן אחיד על טכנולוגיות ושימושים שרמת הסיכונים והחששות לגביהם שונה באופן ניכר.
- 5.3. יש לבצע את ניהול הסיכונים ובדיקות המערכת לכל אורך "מחזור החיים" של מערכות הבינה המלאכותית, החל משלב העיצוב והפיתוח ובאופן מתמשך גם בשלבי הפיקוח והבקרה לאחר הפעלה מוסדרת של המערכת.
- 5.4. העקרונות להדרכה והערכה של שימוש משטרתית במערכות בינה מלאכותית הן:
- 5.4.1. **חוקיות** (עיקרון הליבה) - מחד הבסיס החוקי והסמכות החוקית להפעלת המערכת ומאידך בחינה כי הפעלת המערכות והשימושים בהן אינם מתנגשים עם הוראות חוקיות אחרות ובראשן זכויות היסוד. יש לבחון את מטרת המערכת והצורך בה אל מול רמת הסיכון המוערכת (מידתיות).
- 5.4.2. **צמצום הנזק** - באמצעות ניהול הסיכונים, אבטחת מידע, דיוק וייעול המערכת, הטלת מגבלות רגולטוריות ובחינת אמצעים מקבילים שפגיעתם פחותה ככל הניתן.
- 5.4.3. **אוטונומיה אנושית** - בחינת מעורבות ופיקוח אנושי בכל אחד משלבי מחזור החיים של פיתוח ושימוש בתוצרים או מערכות של בינה מלאכותית וכן שמירה על פרטיות והסברתיות.
- 5.4.4. **הוגנות** - מערכות בינה מלאכותית עלולות לשקף ואף להגביר הטיות חברתיות קיימות, מה שעלול להוביל לשיטור לא הוגן או מפלה. נדרשת בחינה מתמדת של מקורות הנתונים ותוצאות המערכת לזיהוי וטיפול בהטיות.

- 5.5. **ניהול סיכונים** - לשם בחינת סוג הטכנולוגיה והשימוש הספציפי אותה נועדה מערכת בינה מלאכותית להסדיר, וכן לצורך עמידה בעקרונות ההדרכה וההערכה כאמור בסעיף 5.4 יש לבצע ניהול סיכונים בהתאם לפרוטוקול ניהול הסיכונים המצורף למסמך זה כנספח א'.
- 5.6. **שימוש בארגזי חול רגולטוריים (פיילוט)** – במידת האפשר יש להיעזר בשימוש ב"ארגזי חול" רגולטוריים, המאפשרים לבחון ולשפר מוצרים ושירותי בינה מלאכותית חדשניים בסביבה מבוקרת. השימוש בארגזי חול רגולטוריים מאפשר הזדמנות מחקר עבור טכנולוגיות חדשות, הבנת השלכותיהן וזיהוי בעיות פוטנציאליות לפני היישום בהקשרים אמיתיים של אכיפת חוק. יחד עם זאת, כאשר מבצעים בפיילוט שימוש במידע אישי או מפעילים את המערכת כלפי אזרחים יש לבצע את הליך ניהול הסיכונים ולקבל אישור משפטי מקדמי טרם ביצוע הפיילוט.
- 5.7. **זכויות יוצרים** – סוגיות של זכויות יוצרים רלוונטיות למערכות בינה מלאכותית יוצרת המשתמשת בנתונים חוץ משטרתיים. ככל שמתעוררת סוגיה בנושא זה יש לפעול ע"פ חו"ד משרד המשפטים בנושא זכויות יוצרים במערכות בינה מלאכותית באמצעות יועמ"ש.
- 5.8. **תיעוד, פיקוח ובקרה** – יש לתעד ולשמור בצורה מסודרת את המסמכים והפרוטוקולים לבחינת חוקיותה ואופן פעילותה של מערכת בינה מלאכותית במהלך מחזור החיים שלה לשם ביצוע פיקוח ובקרה על פעולותיה והכנסתה לשימוש וכן לצורך הליכי בקרה, בדיקה או תביעה חיצוניים.

בכבוד רב,



עו"ד מוריה בן משה, רפ"ק
יועמ"ש אגף הטכנולוגיה והתקשוב