

השימוש בבינה מלאכותית צובר תאוצה בשנים האחרונות, וניכר שאנו רק בתחילתה של מהפכה טכנולוגית בעלת משמעות רבה על חיינו. בצד היתרונות הרבים של תופעה זו, ישנן גם סכנות לא מעטות, ובמיוחד במובן של פגיעה בזכויות אדם על ידי תאגידים ללא אחריותיות דמוקרטית. אם כן, מהי בדיוק בינה מלאכותית? באילו שדות היא מיושמת, ואילו אתגרים מתעוררים בשל הפניה אליה? וכיצד יכולה מדינת ישראל לשמר עליונות טכנולוגית ולעודד חדשנות, תוך שמירה על עקרונות כגון שוויון, ושקיפות, ביחס לטכנולוגיה שרוב הנסתר על הגלוי לגביה? ד"ר אלעד גיל וד"ר טל מימרן עונים על השאלות הקריטיות.

בינה מלאכותית מהי?

בינה המלאכותית היא למעשה הכלי המאפשר "למידת מכונה" או "למידה חישובית", ברמה גבוהה של אוטומציה שלא דורשת התערבות אנושית. התהליך של למידת מכונה הוא תהליך של עיבוד נתונים ולמידה דרך הקשר – לדוגמה, שימוש במאגר מידע של תמונות פנים, אשר מלמד את הבינה המלאכותית לזהות דמות או לשחזר מבנה של פנים אנושיות על פי בקשה. היישום של הבינה המלאכותית הוא מגוון מאוד, והולך ומתגבר עם כל יום שעובר, ותופעה זו משפיעה על תחומי ידע רבים (שפה, תרבות ועוד).

המשך, לסכם טקסטים ארוכים בשניות בודדות, לאתגר הנחות יסוד לא נכונות ואפילו להודות בטעויות ולסרב לבקשות לא מתאימות. הקפיצה ביכולות של בינה מלאכותית הופכת אותה לכלי עזר בעל

"הקפיצה ביכולות של בינה מלאכותית הופכת אותה לכלי עזר בעל חשיבות הולכת וגוברת, אך כמו כל זינוק טכנולוגי – לצד היתרונות, ישנם גם צדדים מסוכנים יותר אשר יש להביאם בחשבון."

חשיבות הולכת וגוברת, אך כמו כל זינוק טכנולוגי – לצד היתרונות, ישנם גם צדדים מסוכנים יותר אשר יש להביאם בחשבון.

מורכבות נוספת נובעת מפערים אידאולוגיים ברמה הבינלאומית, אשר

תוכנות רבות משתמשות בכלים של בינה מלאכותית כיום. תוכנה אשר הפכה לפופולרית במיוחד, ומייצגת של מהפכת הבינה המלאכותית בעיני השוק הרחב, היא ChatGPT. כלי זה מסוגל לענות על שאלות כמעט בכל תחום ושאלות

מביאים לפערים ברמת הנכונות לפקח על פיתוח ויישום של בינה מלאכותית, גם במחיר של פגיעה בזכויות אדם. כך, בעוד במדינות דוגמת סין נעשה שימוש במכשירים הפועלים באמצעות בינה מלאכותית ובוחנים את מצב הרוח של קטינים, או את רמת הריכוז שלהם בכיתה, נראה כי העולם המערבי מתחיל להתעורר לגבי הסכנות האפשריות ובהתאם יש הקוראים להצבת מגבלות על השימוש בבינה מלאכותית.

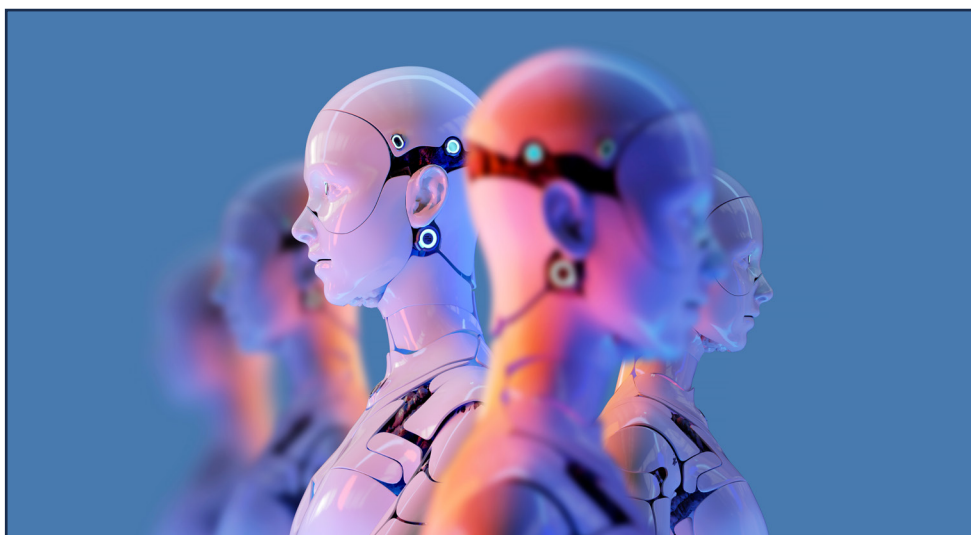
יישומים של בינה מלאכותית - כלי אומנותי או כלי נשק?

השימוש הגובר בבינה מלאכותית משפיע באופן עמוק על חיינו, ביחס לניתוח וניהול מידע, ואף משפיע על הליכי קבלת החלטות באופן שיכול להוביל לפגיעה בזכויות אדם. חסרון מרכזי של בינה מלאכותית הוא העדר היכולת של כלי זה להסביר את עצמו, מה שמקשה על קידום ודאות ושקיפות, וזאת לצד העובדה שגם מערכת מתקדמת כל כך יכולה לבצע טעויות. למעשה, ככל שדורשים יותר הסברים מבינה מלאכותית, כך, ככלל, יורדות היעילות שלה ורמת הדיוק שלה.

ישנן מספר זירות מרכזיות בהן אנו רואים התפתחויות בתחום. במסמך הנוכחי, נבקש להתמקד בשתי דוגמאות מייצגות – שדה האומנות ושדה הקרב.

השדה האומנותי

פריצת דרך משמעותית הושגה בתחום היצירה, לאחר שמספר חברות חשפו לציבור כלים של בינה מלאכותית אשר



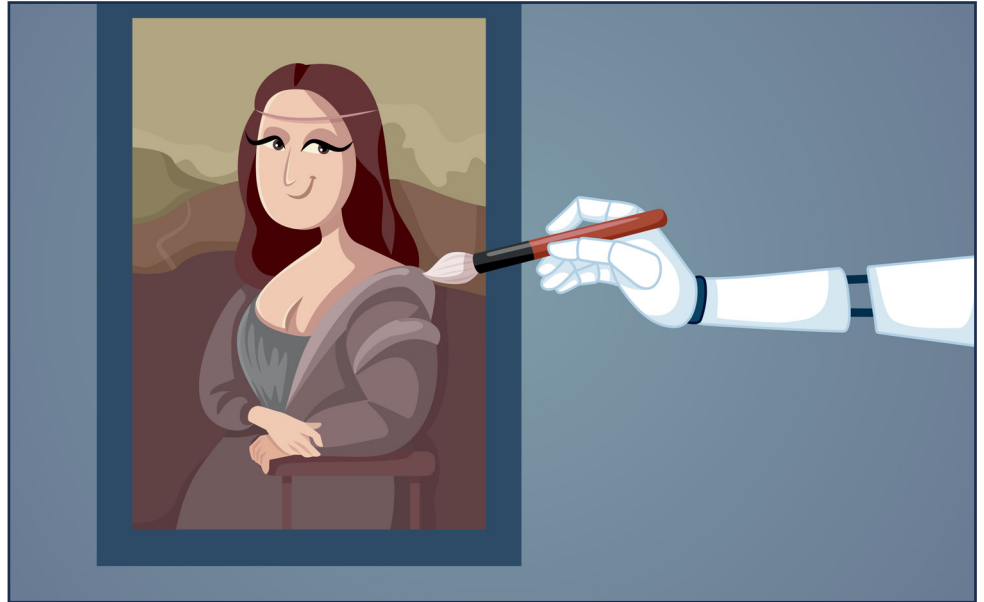
להתנסות בשימוש בכלים המבוססים בינה מלאכותית נגד ישראל.

לבסוף, מדינת ישראל מחויבת לבחון נשקים חדשים, כמו גם אמצעי לחימה, אשר היא מכניסה לשימוש. לא ברור האם בוצע הליך בחינה מראש, או פיקוח בדיעבד, ביחס לכלי כה מרחיק לכת. למעשה, ישנם קולות הקוראים לאיסור מוחלט על שימוש בבינה מלאכותית ליישום צבאי, עד להגדרה של נורמות בתחום. מכאן, בחירתה של ישראל לצאת לאור, בדיוק כאשר מתגבר השיח הבינלאומי לגבי הגבלות, מעוררת תמיהה.

רגולציה של בינה מלאכותית רגולציה בעולם

ברמה הבין-מדינתית, לא נעשתה התקדמות מספקת במובנים של הגדרת נורמות ברורות לפיתוח של בינה מלאכותית, ויישום שלה בתחומי חיים

הקרב, וזאת מזה מספר שנים. השימוש בבינה מלאכותית, כך נטען, מגביר יכולות הגנתיות (ובפרט הגנה על גבולות, או שימוש טוב יותר במערכות דוגמת כיפת ברזל), כמו גם התקפיות (פריצות דרך מודיעיניות, לצד איתור מטרות לתקיפה).



"ברמה הבין-מדינתית, לא נעשתה התקדמות מספקת במובנים של הגדרת נורמות ברורות לפיתוח של בינה מלאכותית, ויישום שלה בתחומי חיים שונים. ישנם כלים "רכים" לא מעטים המציעים סטנדרטים, אבל אין אמנות בינלאומיות או הכרזות מחייבות ברמה האוניברסלית"

אין ספק, חשיפה של יכולות מסוג אלו היא משמעותית במובנים של חיזוק ההרתעה של ישראל. ועדיין, בשלב הנוכחי בו אין בהירות לגבי הנורמות החלות על השימוש בבינה מלאכותית בשדה הקרב, בין היתר בגלל חילוקי דעות אידיאולוגיים בין-מדינתיים, נראה כי ההחלטה לרוץ קדימה ולפרסם נמהרת קמעא. בנוסף, הודאה בשימוש בכלי מסוים בשדה הקרב מתירה את הרסנים בפני יריבות של מדינת ישראל, דוגמת איראן אשר יש לה יכולות טכנולוגיות בלתי מבוטלות, ומזמינה אותן

חופש היצירה – ברמה כזו שמעלה שאלות לגבי חוקיות הפעולה מבחינת זכויות יוצרים. הרי, על מנת ליצור אומנות, בינה מלאכותית צריכה ללמוד מאומנות קיימת, ולהסתמך עליה בעת יצירה של חומרים חדשים. בהתאם, הגבול שבין השראה הופך להיות בלתי ברור עם כל יום שעובר, ועולות שאלות משמעותיות במובן של הפרת זכויות יוצרים.

למעשה, ישנם כבר הליכים משפטיים אשר הותנעו נגד מספר חברות (Stability AI, Midjourney ועוד), ביחס לפגיעה בזכויות היוצרים של אמנים שנעשה שימוש ביצירותיהם ללא אישור על מנת לאמן את הבינה המלאכותית. בדומה, הונעו הליכים משפטיים ביחס לכלי המעניין Copilot, אשר מאפשר לכתוב קוד מחשב (על בסיס לימודי של קודים קיימים, אך מבלי ליתן קרדיט למתכנתים המקוריים). יהיה מעניין לעקוב ולראות לאן הליכים מסוג אלו יובילו במובנים של הגבלות על פיתוח ושימוש בתחום.

בינה מלאכותית בשדה הקרב

בפברואר 2023, חשף מפקד מרכז הבינה המלאכותית ביחידה 8200 כי צה"ל עושה שימוש בבינה מלאכותית בשדה



שונים. ישנם כלים "רכים" לא מעטים המציעים סטנדרטים, אבל אין אמנות בינלאומיות או הכרזות מחייבות ברמה האוניברסלית.

ובכל זאת, ישנה התקדמות מסוימת בנושא. ארגון ה-OECD, לדוגמה, פרסם עקרונות לפיתוח בר-קיימא ושימוש בבינה מלאכותית תוך קידום הוגנות, שוויון, בטיחות, אחריותיות ובאופן רחב יותר הגנה על זכויות אדם. על בסיס עקרונות אלו, מעודד הארגון להשקיע במחקר ופיתוח של בינה מלאכותית, לעצב מדיניות מתאימה, לבצע הכנות בשווקים רלוונטיים ובכלל בעולם התעסוקה, ולקדם שיתוף פעולה בינלאומי.

בנוסף, ניתן לציין אימוץ צו נשיאותי בארצות הברית בנושא שימור הנהגה בתחום הבינה המלאכותית, הקמה של ועדה מייעצת בנושא בקנדה, והקמה של ועדה מיוחדת באיחוד האירופי לפיתוח, עיצוב ויישום של בינה מלאכותית על בסיס עקרונות דמוקרטיים ובמיוחד הגנה על זכויות אדם.

רגולציה בישראל

ישנה חשיבות עצומה בפיתוח מדיניות סדורה ביחס לאסדרה של טכנולוגיית בינה מלאכותית, בשלב מוקדם של טכנולוגיות חדשות, ובשלב מוקדם. המחשה טובה לסיכון שבמתן יד חופשית לחברות עצמן, ניתן לאתר בתחום הרשתות החברתיות.

"ישנה חשיבות עצומה בפיתוח מדיניות סדורה ביחס לאסדרה של טכנולוגיית בינה מלאכותית, בשלב מוקדם"

בעוד רשתות חברתיות תרמו במובן של מתן קול לאנשים רבים יותר, ברור היום כי הן גורמות לנזקים חברתיים לא מבוטלים (הסלמה של קיטוב וביטויי שנאה, השפעה על אירועים משמעותיים דוגמת בחירות או חוסר שקט חברתי, ואף פגיעה פסיכולוגית במשתמשים). בעוד המחוקק מתעורר בימים אלה לגבי החשיבות של הסדרת חשיבות הרשתות החברתיות, נראה כי נזק רב כבר נעשה.

למרבה השמחה, נראה כי הלקח נלמד וישנו דיון מעמיק כבר בשלב זה לגבי הצורך לאסדר את השימוש בבינה מלאכותית בישראל. בשנת 2022, פרסם משרד החדשנות, המדע והטכנולוגיה עקרונות מדיניות, רגולציה ואתיקה בתחום הבינה המלאכותית. המסמך מבקש להגדיר מדיניות בתחומי הבינה המלאכותית ללא אימוץ חקיקה רוחבית, אלא באמצעות רגולטורים סקטוריאליים בכל תחום וכלי רגולציה "רכים". בנוסף, אימץ המסמך עקרונות אתיים לשימוש בבינה מלאכותית, למשל: קידום צמיחה באופן בר-קיימא, שמירה על בטיחות בייצור ושימוש, חיזוק אמינות המערכת, כמו גם שקיפות לגביה והסברתיות ביחס לאופן קבלת ההחלטות שלה. בשלב הבא, ממשלת ישראל תקים מוקד ידע ותיאום ממשלתי בנושא.

והרגולטורי לאתגרי הבינה המלאכותית במגזרים השונים. העמדה לפיה אין צורך בקידום חקיקה כוללת, כפי שהוצגה על ידי משרד החדשנות, מבקשת לעודד יזמות ויצירתיות של השוק הפרטי. בעוד מטרות אלו הן בעלות חשיבות רבה, אין בכך בכדי להעניק מענה מספק לסיכונים הכרוכים בשימוש רחב ובלתי מוסדר בבינה מלאכותית. הסיבה לכך, היא כי בעוד מדובר בתפריט אקלקטי של הצעות וכלים, מסמך העקרונות מאפשר לרגולטורים שונים לפרש את ההמלצות בצורה שונה ולתעדף את האינטרסים הצרים של עולם התוכן עליו הם אמונים, תוך התעלמות מהשפעה אפשרית על מגזרים אחרים. חשש נוסף הוא, כי הסתפקות בכלי רגולציה רכים ומחויבות אתית בלבד, ביחס למערכות בינה מלאכותית אשר יש להן השפעה יסודית



מה כדאי לעשות הלאה?

מסמך העקרונות של משרד המדע והטכנולוגיה הוא התקדמות חשובה ביותר, אך יש מקום לחזק ולהדק את מדיניותה של ממשלת ישראל בנושא. בפרט, תכלית-המכון למדיניות ישראלית, ממליץ על שני צעדים עיקריים: (א) מיסוד של מאסדר לאומי אשר תפקידו יהיה להנחות ולייצר הרמוניה בין הרגולטורים המגזריים, ו-(ב) אימוץ של מתודולוגיה אחידה לבחינת המענה המשפטי

על זכויות אדם, תייצר גרעון דמוקרטי הנובע מהעדר אחריותיות מצד מפעילי בינה מלאכותית כלפי משתמשים. לשם ההשוואה, בטיטת חוק המוצעת בנושא בינה מלאכותית, מטעם האיחוד האירופי, הועדפה גישת אסדרה לפיה יש צורך בחקיקה אופקית נוקשה ביחס לבינה מלאכותית עם סיכון גבוה יותר, על פני רגולציה סקטוריאלית, תוך יצירת קוד התנהגות מחייב פחות כלפי בינה מלאכותית עם סיכון נמוך. גישה זו מבקשת

את הדמיון באותה המידה שהוא מעורר חששות. יש לקוות כי היכולות הבלתי רגילות של כלי בינה מלאכותית ישמשו את האנושות, ויתמכו בהתפתחות שלה,

"מתודולוגיה סדורה נחוצה על מנת להגשים מדיניות רגולטורית ומשפטית הנשענת על רעיון מארגן אחיד, וזאת במקום ליצור איים מבודדים מבחינה משפטית ורגולטורית אשר לא יתקשרו האחד עם השני ואולי אף יביאו לקביעות סותרות"

וזאת למרות הסיכון הרב של ניצול לרעה של כלים אלו ואף גרירת האנושות למירוץ אל התחתית במובנים של הרס עצמי נטול בקרה (ככל שמדינות יתמקדו בעליונות טכנולוגית בכל מחיר). בעוד חשוב כי המחוקק הישראלי יעודד חדשנות ואינטרסים כלכליים, עליו לשמור על ערנות גם לגבי הסיכונים, ולמסד מנגנונים אשר יצמצמו פגיעה אפשרית במגזר אחד על חשבון אחר, בביטחון או בזכויות הפרט.



ד"ר אלעד גיל

הוא עמית בכיר וראש המחקר במכון תכלית, המכון למדיניות ישראלית.



ד"ר טל מימרן

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



"מאסדר על שכזה מהווה מודל ביניים רצוי בין החלופה של רגולציה רוחבית לבין החלופה של רגולציה מגזרית ומאפשר להנות מחלק ניכר מהיתרונות של כל מודל"

צעד חשוב נוסף, הוא הטמעת מתודולוגיית חשיבה אחידה להתמודדות עם הבעיות המשותפות הנוצרות עבור רגולטורים, יועצים משפטיים וגורמים אחרים אשר אמורים לפקח ולאסדר את השימוש בבינה מלאכותית. סיבה מרכזית לכך, היא כי לבינה מלאכותית צפויה השפעה משבשת (disruptive) על שווקים וחברות, אשר ראוי כי ייבחנו ויקבלו מענה באופן הרמוני. לדוגמה, מבנים תעסוקתיים יעברו שינוי דרמטי עם הופעתן של טכנולוגיות מתקדמות, אשר בתורן ייצרו סיכונים בטיחות חדשים, באופן שישפיע על תחומים רבים (המגזר הפיננסי, הרפואי, החינוכי ועוד). מתודולוגיה סדורה נחוצה על מנת להגשים מדיניות רגולטורית ומשפטית הנשענת על רעיון מארגן אחיד, וזאת במקום ליצור איים מבודדים מבחינה משפטית ורגולטורית אשר לא יתקשרו האחד עם השני ואולי אף יביאו לקביעות סותרות (בהתאם לאינטרסים השונים של כל מגזר).

לסיכום, עולם הבינה המלאכותית מצית

לקדם באופן מיטבי הגנה על זכויות אדם בהתאם לרמת הסיכון, להגביר את הוודאות המשפטית, לשפר את יעילות כלי האכיפה, וליצור סביבה המאפשרת פיתוח של מערכת בינה מלאכותית בטוחה למשתמשים.

אנו מציעים מודל ביניים בין זה שהוצע על ידי משרד החדשנות, לבין הגישה האירופית, וזאת באמצעות על הקמה של מאסדר לאומי אשר ימלא שתי פונקציות מרכזיות: (1) המאסדר יבטיח הרמוניזציה וחתירה משותפת של כלל המגזרים במשק להגשמת יעדי המדיניות הלאומית בתחום הבינה המלאכותית (בתור ה"רגולטור של הרגולטורים"); (2) המאסדר יפתח את המדיניות הרגולטורית וייעץ לממשלה על הצעדים הנדרשים להמשך פיתוחה וקידומה. אנו מציעים כי המאסדר הלאומי יהיה בעל סמכויות להנחות את הרשויות השונות לגבי אופן מימוש מדיניות הרגולציה לאומית, וביחס לאסדרה של סוגיות משפטיות פרשניות להתאמת הדין הקיים. בנוסף, ניתן לבסס מנגנון לפיו מי שרואה עצמו נפגע מהחלטות של רגולטורים מגזריים יוכל לפנות למאסדר הלאומי לבחינה מחדשת של ההחלטה. לתחשתנו, מאסדר על שכזה מהווה מודל ביניים רצוי בין החלופה של רגולציה רוחבית לבין החלופה של רגולציה מגזרית ומאפשר להנות מחלק ניכר מהיתרונות של כל מודל.