

היבטים משפטיים של שימוש בבינה
מלאכותית – כלים פרקטיים וכללי
אצבע בניהול סיכונים והסדרת
השימוש ב- AI בארגון

GOLDFARB
GROSS
SELIGMAN

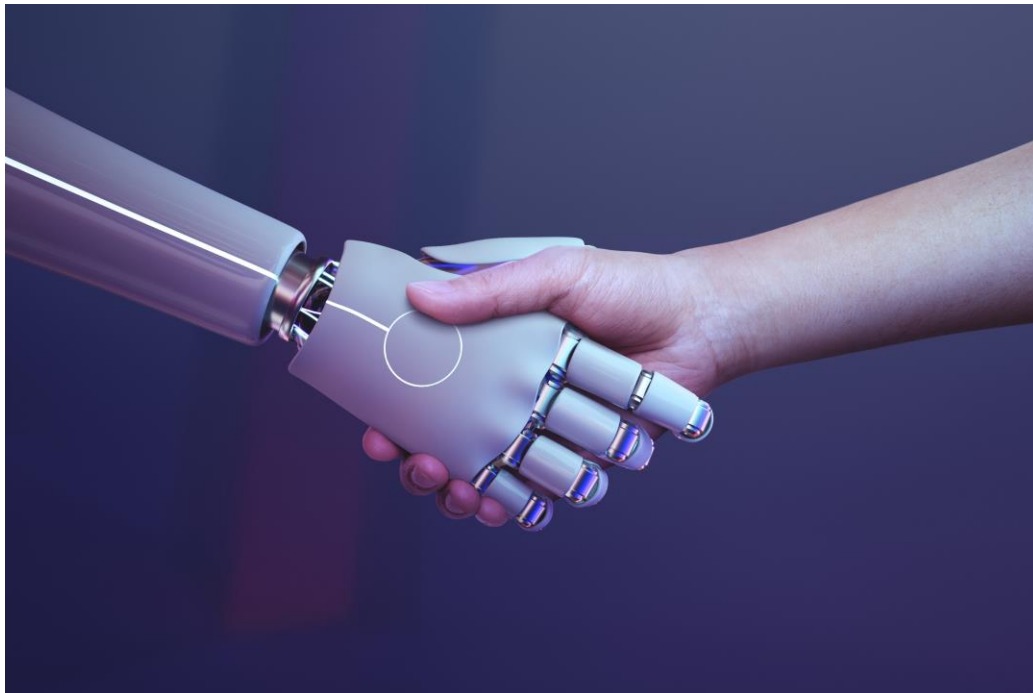
הרצאה בפני כנס המבקרים הפנימיים

עו"ד סער פלינר, שותף, ראש תחום ליטיגצית קניין רוחני,
רישום זכויות ודיני בידור

29 פברואר, 2024

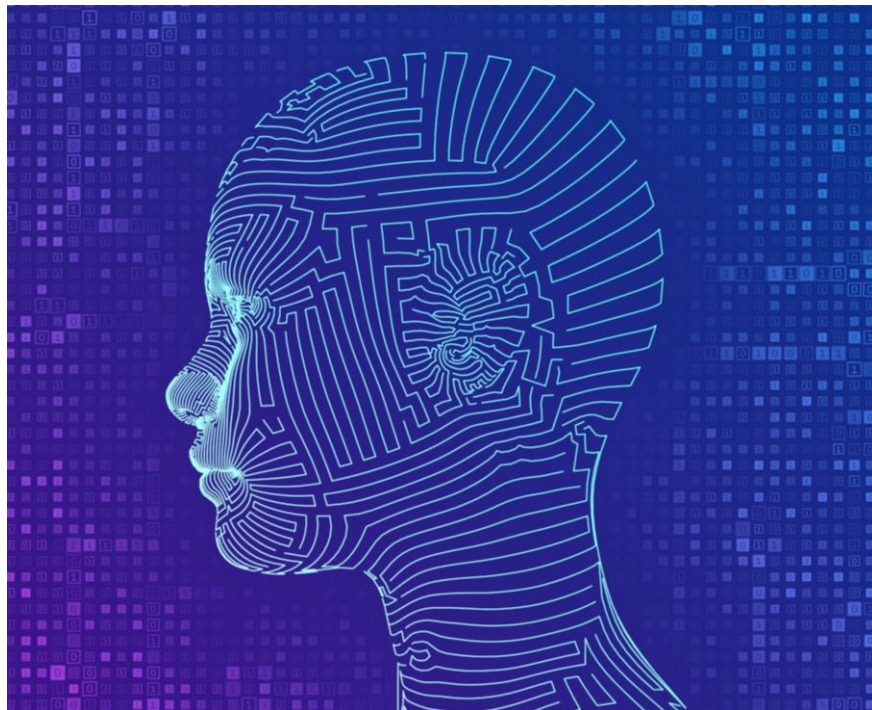
בינה מלאכותית

טכנולוגיה פורצת דרך



סטיבן הוקינג: "הצלחה ביצירת בינה מלאכותית אפקטיבית יכולה להיות האירוע הגדול ביותר בהיסטוריה של הציוויליזציה שלנו. או הגרוע מכל. אנחנו פשוט לא יודעים. לכן, אנחנו לא יכולים לדעת אם נעזר לאין ערוך על ידי AI או שנהרס על ידי זה".

בינה מלאכותית



המבחן המקובל ביותר לבינה מלאכותית הוטבע בשנת 1950 על ידי אלן טיורינג, וידוע בשם "מבחן טיורינג":

מכונה תחשב לתבונית, אם יינתן לאדם היושב בחדר סגור, לנהל שיחה באמצעות ממשק מחשב עם שתי ישויות שנמצאות בחדר השני, כאשר אחת מהן תהיה מכונה והשנייה אנושית, והמשוחח לא יוכל לזהות מי משתי הישויות היא מכונה או אדם.

The background is a dark purple gradient with a central light purple glow. It features a series of fine, parallel lines that create a sense of depth and movement, resembling a light tunnel or a data stream. Scattered throughout are small, bright purple particles, giving it a cosmic or digital feel.

בינה מלאכותית
מאפיינים עיקריים

בינה מלאכותית (יוצרת – generative)

תחום הבינה המלאכותית הג'נרטיבית מושך אליו שחקנים גדולים כמו מיקרוסופט, גוגל, Open AI המציעים לקהל הרחב אפשרויות שימוש חדשניות שלא היו קיימות עד היום.

מכונות חדשות כגון:

DALL-E, Midjourney , GitHub – Copilot , Stable Diffusion ,CHATGPT ,DreamUp

מאפשרות יצירת תוכן כתוב, ציורים, קבצי קול ויצירות מוסיקליות, שורות קוד, קליפים, ויצירות המחקות בני אדם (deep fake) כשהתפתחות של הטכנולוגיה מהירה מאוד ומציבה בפני המשפטנים שאלות חדשניות שטרם נדונו.

בינה מלאכותית (יוצרת – generative)

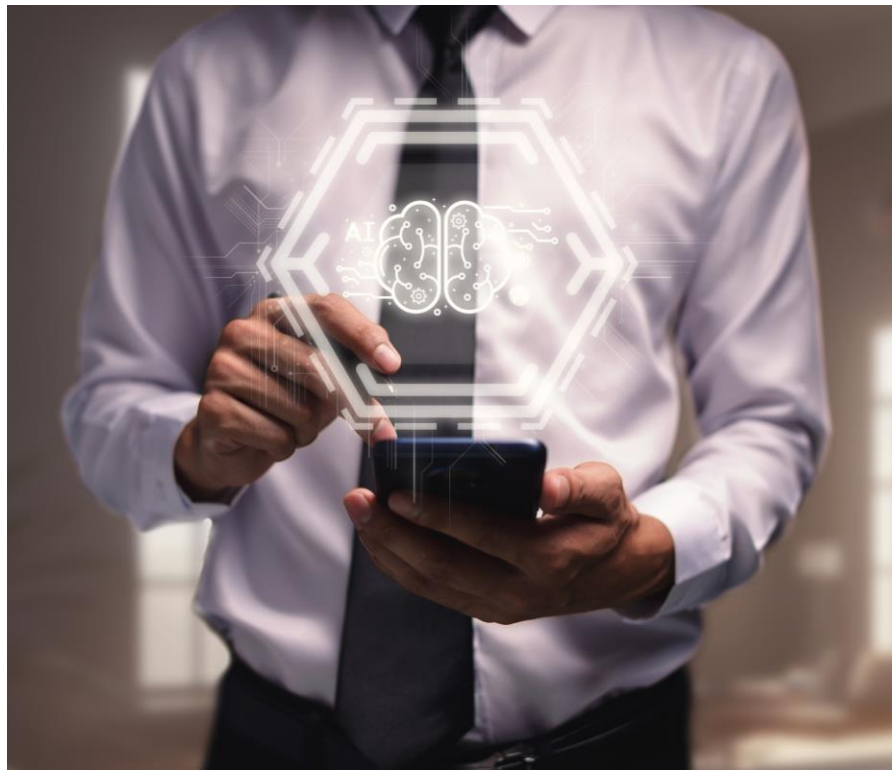
בקרוב הן גוגל והן מיקרוסופט יטמיעו כלי AI באופן מובנה ב- 365 וב- Google Docs וב- Gmail וגם במסגרת ה- BRAD (ChatGPT של גוגל).
הדאטה הנסרקת לתוך ה"מכונות" הינה רובה ככולה מידע הקיים באינטרנט ומשכך, ככל הנראה מוגנת כזכויות יוצרים.
לכן – כשאנחנו רוצים לברר את חוקיות השימוש המסחרי ביכולות ה- AI עלינו לבחון, ראשית, את הכלי בו נעשה שימוש, את חוקיות שלב ההזנה של המידע הנעשה על ידי החברות המחזיקות בבעלות במכונת ה- AI ואת שלב השימוש ב"מכונה" ותוצריה, על ידי האירגון ובהמשך - על קהל הלקוחות שלה.

בינה מלאכותית (יוצרת – generative) - תוצרים

תמונת מחווה ל"נערה עם עגיל פנינה" שנוצרה
ב-Midjourney מופיעה כתוצאה ראשונה
בחיפוש "Vermeer" בגוגל



בינה מלאכותית (יוצרת – generative)



בחודש דצמבר 2022 חוות דעת של מחלקת ייעוץ וחקיקה במשרד המשפטים, לפיה שימוש בתכנים מוגנים בזכויות יוצרים לצורך אימון מערכות בינה מלאכותית חוסה תחת הסדרי השימושים המותרים בדיני זכויות היוצרים, ומשכך אינו מהווה הפרה של חוק זכות יוצרים. יושם לב כי חוות הדעת מתייחסת לתהליך האימון של מודל הבינה המלאכותית, אך לא לתוצרים שהוא מפיק.

מדובר בחוות דעת ייחודית בעולם המפורסמת על ידי גוף ממשלתי בנושא שהינו, לכאורה, נתון להסדרת השוק הפרטי.

האם המדובר ב"צדיק" היחידי ב"מערב הפרוע" של עולם ה-AI?

בינה מלאכותית - סיכונים אפשריים ובחינתם

כאמור, מערכת AI לא יכולה ליצור תוצרים לרבות אמנות, קוד מחשב, מוסיקה וטקסטים יש מאין. תוצרי התוכנה מבוססים על הזנה וסריקה של כמויות אדירות של מידע לרבות יצירות (טקסט, תמונה, שורות קוד) של יוצרים רבים בהם היא משתמשת כדי ליצור יצירות חדשות מבוססות בינה מלאכותית.

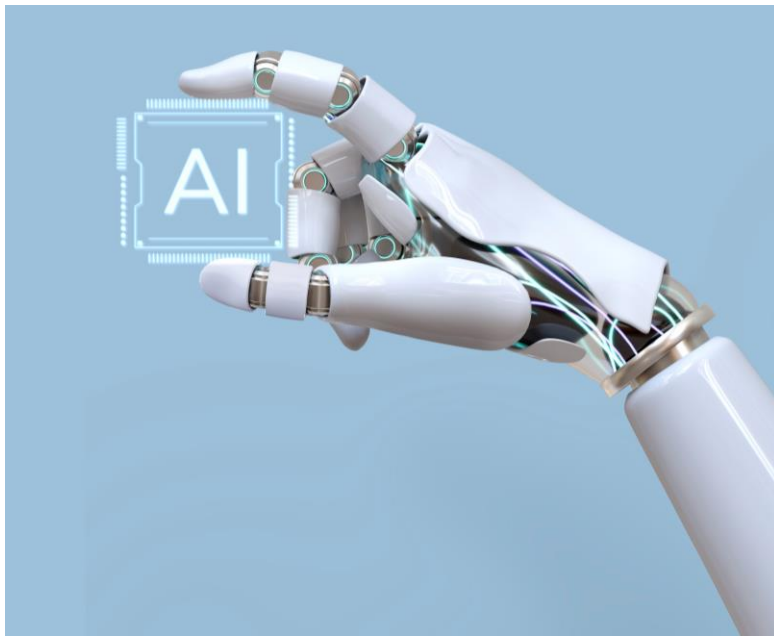
לכן, יש להניח, כי חוקי הקניין הרוחני יחולו על כל תוצרי מכשירי הבינה המלאכותית. חברה העושה שימוש במהלך עסקיה ב"מכונות" AI אשר מפותחות על ידי צד שלישי (בין אם כמוצר "מדף" ובין אם כפיתוח המותאם ספציפית לצרכי הארגון), נדרשת להכיר את הסיכונים המשפטיים הפוטנציאליים הקיימים עקב שימוש בתוכנת AI על ידי עובדי הארגון וכחלק ממוצריה.

להלן נציע מספר דגשים, לעריכת פעולות ביקורת פנים אירגוניות אפשריות, בעת הערכת או בדיקת פעילות AI של חברה.

בינה מלאכותית (יוצרת – generative)



בינה מלאכותית - סיכונים אפשריים ובחינתם



1. הבנת הכלי בו נעשה שימוש

האם השימוש לצרכים פנימיים בלבד של
האירגון (מחקר, איסוף מידע, פיתוח)

סיכון נמוך יחסית

או

כחלק ממוצר של החברה
(שורות קוד שיוטמעו במוצר)

בינה מלאכותית - סיכונים אפשריים ובחינתם

2. תנאי השימוש

בחינת והבנת תנאי השימוש וההגבלות החלות על ידי הבעלים של כלי ה AI בו משתמשים;
בחינת תנאי הרישיון, בעלות בקניין רוחני, הגבלת אחריות, שיפוי ומשמעות ממשקי אינטגרציה עם מערכות אחרות בארגון;
האם מדובר, למשל, ברישיון קוד פתוח
בדיקה האם יש להתאים את ההסכמים עם הלקוחות – הערכת הסיכון;
יש לבדוק בידי מי הבעלות בתוכן הנוצר מהשימוש בכלי ה AI הספציפי;
האם יש לכך השפעה או שעשויה להיות השפעה בעת גיוס השקעות או רכישה אפשרית;

בינה מלאכותית - סיכונים אפשריים ובחינתם

השימוש – המשך

יש להכיר את הכלי בו יעשה השימוש ולהבין אם המדובר בשימוש פנימי או שמשולב עם מוצרי החברה, האם תנאי הרישיון דורשים עדכון של הסכמי הלקוחות, כתבי ויתור, הגבלות שונות.

הבנת היקף החשיפה והשימוש כדי לספק מצגי אמת בעת עריכת בדיקות נאותות לפני השקעה או מיזוג ורכישה (M&A).

הערכה על ידי מומחה קניין רוחני של מעמדם המשפטי של תוצרי ה"מכונה" – האם לארגון חשיפה של הפרת זכויות צד שלישי או, לחלופין, האם ניתן להגן על התוצר ולמנוע העתקתו על ידי מתחרים.

מה המידע שאותו מזינים עובדי החברה ל"מכונה" והאם מדובר במידע/תוכן השייך לצד שלישי ויש לקבל רשותו לשם עשיית השימוש?

בינה מלאכותית - סיכונים אפשריים ובחינתם

השימוש – המשך

האם נעשה שימוש בכלי לכתובת קוד – שימוש בכלי קוד פתוח של צד שלישי ישפיע על סוג הרישיון הנדרש להטמעה במוצר.

מומלץ לאתר את סוג הרישיון וכן לסרוק את רכיבי המקור שנמצאים בקוד החדש שנוצר כדי לסמן את החלקים שבהם קיים סיכון להפרת הסכם הרישיון הרלוונטי.

בעת הצורך ליצר הפרדה מובנית בין תוצרי ה AI לבין תוצרי החברה כדי להפחית סיכון להפרת רישיון קוד פתוח שתפגע בנושות ברישיונות השימוש של הארגון.

בינה מלאכותית - סיכונים אפשריים ובחינתם

3. השפעות נוספות

האם החברה תושפע מהכלי אם פעולתו תשובש או תצומצם (תביעות, רגולציה וכו).
כאן יש לבחון את ההשפעה שתהיה לנ"ל על הארגון. (ראו סקירת תובענות ייצוגיות להלן).

האם יש חשש להפרת זכויות יוצרים כחלק מפעילות הכלי?

האם יש חשש מתביעות צדדים שלישיים? (האם שימוש פנימי או שמשולב במוצר של החברה)

4. פרטיות

בדיקת המידע המוזן ל"מכונה" והפעלת נוהל ברור בקשר עם מידע/תוכן סודי/מוגן/אישי;

בדיקת נוהלי הפרטיות של כלי ה AI והתאמתם לדרישות כגון GDPR

בדיקת סיכוני "זליגת" מידע למתחרים ולצדדים שלישיים – אי שמירה על "סוד מסחרי".

בינה מלאכותית - סיכונים אפשריים ובחינתם

השפעות נוספות

אחריות – הערכת סיכונים (הפרת קניין רוחני, סודיות, פרטיות) והתאמה לדרישות רגולטוריות של המחוקק.

סודות מסחריים – ניהול תהליכי ההזנה של הפרומפט, המידע המוזן, מניעת זליגת מידע, שימוש במידע מוגן של צד שלישי.

הכנה לאירוע קטסטרופה – קריסה של מערכת ה AI.

התקדמות חקיקה

קיימת חשיבות קריטית במעקב אחרי התקדמות קבועה בחקיקת חוקים ותקנות שונים המטילים חובות על חברות המפתחות כלי AI ועל משתמשים בכלים כאלה. חשוב מאוד לחברות להתעדכן בחקיקה זו כדי להבטיח עמידה בתנאים רגולטורים בכל מדינה ומדינה כדי להימנע מקנסות, אכיפה ומניעת התקשרויות עסקיות.

בינה מלאכותית (יוצרת – generative)

נביא מספר דוגמאות המעידות על הבלבול וחוסר הבהירות המשפטיים שנוצרו ונוצרים כמעט מדי יום ועל היותה של חוות הדעת של משרד המשפטים שנויה במחלוקת:

לאחרונה הוגשה בארה"ב תביעה ייצוגית נגד ספקי מערכות AI על-ידי מספר אמנים, הטוענים, בין היתר, כי **אימון המודלים באמצעות מאגרי תמונות השייכות להם, ללא הסכמתם, מהווה הפרה של זכויותיהם.**

חברת המוסיקה Universal (אשר נוקטת בגישה הפוכה לזו של משרד המשפטים) פונה לאחרונה לשירותי מוסיקה בסטרימינג כגון Spotify ו-Apple music ודורשת כי **לא יאפשרו לחברות בינה מלאכותית גישה ליצירות מוגנות לצורך לימוד ואימון בסיס המידע שלהן.**

גטי אימאג' (חברת רישיונות התמונות) תבעה את חברת Stable Diffusion ("הילד הרע" של עולם ה AI) על גניבה של 12 מיליון תמונות ממאגריה **לצורך אימון האפליקציה.** חברה אחרת בתחום "שאטרסטוק" התחילה לשלם ליוצרים הרשומים אצלה עבור מתן רישיון שימוש בתמונותיהם שמאגריה, לחברות בינה מלאכותית.

קיימות ראיות למסמכים מועתקים, ויצירות תוכן הכוללות מידע שקרי שהומצא לחלוטין על ידי התוכנה.

לא ניתן להגן על יצירת מכונה ב"זכויות יוצרים" Artificial Intelligence – an original work of Art?

- The US Copyright Office says an AI can't copyright its art
- "Courts have been consistent in finding that non-human expression is ineligible for copyright protection
- A recent Entrance to Paradise
- Steven Thaler and/or Creativity Machine



בינה מלאכותית (יוצרת – generative) - תוצרים

יש לשים לב שלא ברור כיום אם אלה יכולים לקבל הגנה נפרדת ועצמאית כיצירה חדשה, או אולי מהווים יצירה נגזרת כיוון, שלמשל, משרד זכויות היוצרים בארה"ב סירב זה מכבר להעניק זכויות יוצרים ליצירה שנוצרה באמצעות בינה מלאכותית מכיוון שחוק זכות יוצרים בארה"ב דורש קיומו של יוצר אנושי לצורך קבלת הגנה על זכויות יוצרים.

עוד נדגיש כי קיימות מערכות חוקים נוספות כגון חוקי הגנת הפרטיות או חוק הגנת הצרכן, אשר גם לאורן יש לבחון את הסיכון שבשימוש בכלי ה AI ואף בתוצרים. כך, למשל, בכל הקשור בשימוש בתמונות של אנשים בשר ודם לצרכים מסחריים (ידוענים, או תוכנות deep-fake וסרטי פרסומת וכד') או בפרסומים שעלולים להוות הטעיית צרכנים בפרסום. גם הם חלים באופן מלא על תוצרי תוכנת הבינה המלאכותית ויש לבדוק ולוודא שאינם מפרים את החוקים הרלוונטיים.

בינה מלאכותית (יוצרת – generative) - תוצרים

חשוב לזכור: מערכת AI לא יכולה ליצור תוצרים לרבות אמנות, קוד מחשב, מוסיקה וטקסטים יש מאין. תוצרי התוכנה מבוססים על סריקה של כמויות אדירות של מידע לרבות יצירות (טקסט, תמונה, שורות קוד) של יוצרים רבים בהם היא משתמשת כדי ליצור יצירות אמנות חדשות מבוססות בינה מלאכותית. לכן, חוקי הקניין הרוחני יחולו על כל תוצרי מכשירי הבינה המלאכותית. בהתאם, נבחן תוצרים אלה כדי לקבוע אם הינם מותרים לשימוש (על פי קריטריונים משפטיים) או מפרים. אם, לאחר בחינת התוצר, יעלה כי מדובר בתוצר מפר כיוון שנראה כהעתק של תמונה מקורית; או נשמע כמו לחן מקורי; או שמועתק משורות קוד שנלקחו ללא רשות; או מהווה העתקה של מאמר ואף העתקה של סימן מסחר, לוגו או עיצוב של מוצר מסוים – כל אלה יחשבו כעותק מפר של יצירה ופגיעה בבעל הזכויות, ועלולים להוות בסיס לפתיחה בהליכים משפטיים כנגד כל מי שעושה שימוש כלשהו בתוצרי המכונה (בין אם הוא המשתמש הסופי ובין אם הוא קבלן ביצוע כגון משרד פרסום, סטודיו לעיצוב, חברה הבונה אתרי אינטרנט ועוד) לרבות צווי מניעה ותשלום פיצוי כספי.

בינה מלאכותית (יוצרת – generative) - תוצרים



בינה מלאכותית (יוצרת – generative)



בינה מלאכותית (יוצרת – generative)

המלצות לעקרונות בסיסיים בניהול והסדרת סיכוני השימוש בכלי AI באופן מסחרי

או במסגרת הארגון

מומלץ לצור נוהל שימוש ברור ומסודר אשר יופץ בין העובדים.



רצוי שהנהל ייקח בחשבון את צרכי הארגון, המשתמשים בכלי ה AI, התוצרים, הלקוחות והסיכון הקיים בשימוש בכלים אלה ומומלץ כי יקבע גורם אחראי בחברה, בין אם ה CISO (Chief Information Security Officer) או ה CAISO (Chief Artificial Intelligence Security Officer) שירכז את הפיקוח על השימוש באפליקציות כלפי פנים החברה וכלפי בעלי המקצוע (עורכי דין) האמונים על מתן הנחיות מקצועיות.

בינה מלאכותית (יוצרת – generative)

המלצות לעקרונות בסיסיים בניהול והסדרת סיכוני השימוש בכלי AI באופן מסחרי או במסגרת הארגון

חלק מהשאלות שעל ה CAISO לשאול הינן, למשל:

מי משתמש בטכנולוגיית ה AI אצלי בארגון ולאיזו מטרה? האם מדובר גם בעובדים שאינם בעלי אוריינטציה טכנולוגית?

כיצד אוכל להגן על מידע בזמן שעובדים עושים שימוש במערכות AI ג'נרטיביות?

מה היא הדרך הנכונה לניהול סיכונים הקיים בעת שימוש בכלי AI?

על פי הערכת Team8 CISO Village מאפריל 2023 **Generative AI and ChatGPT Enterprise Risks**

<https://team8.vc/wp-content/uploads/2023/04/Team8-Generative-AI-and-ChatGPT-Enterprise->

[Risks.pdf](#) (Risks.pdf) הסיכונים העיקריים יכולים להיות:

בינה מלאכותית (generative – יוצרת)

המלצות לעקרונות בסיסיים בניהול והסדרת סיכוני השימוש בכלי AI באופן מסחרי או במסגרת הארגון

השפעת השימוש ב AI על פעילות פנים אירגונית;
הצורך "לסמוך" על אמצעי בטחון של צדדים שלישיים;
סיכונים רגולטוריים ומשפטיים הקיימים;
סיכוני זליגת מידע (בחשיבות נמוכה בשלב הזה)

בינה מלאכותית (יוצרת – generative)

המלצות לעקרונות בסיסיים בניהול והסדרת סיכוני השימוש בכלי AI באופן מסחרי או במסגרת הארגון

הסיכונים האמורים יכולים להיות מנוהלים, באמצעות הטמעת הכלים, למשל:

זיהוי הסיכונים וההשפעה שלהם על הארגון (Team8 CISO Village מאפריל 2023 Generative AI and ChatGPT Enterprise Risks)

שימוש באפליקציה שאושרה על ידי החברה בלבד לאחר בחינת החלופות ואישור המתאימה ביותר לארגון;

שימוש רק באופן שאושר מראש (דהיינו – לא שימוש פרטי, על פי נוהל השימוש להלן וכו');;

התייחסות לשימוש בתוכן של לקוח – אבטחת מידע ופרטיות (בין אם תוכן שהגיע מהלקוח ובין אם תוכן שיוצר עבור הלקוח – למשל במשרד עורכי דין).

בינה מלאכותית (יוצרת – generative)

המשך -

למשל – אפשר לקבוע כי ניתן להעלות תמונות או תוכן או שורות קוד של לקוח בתנאים שמפורטים בנוהל:
קבלת אישורים נדרשים מדרג מנהל;
שמירה על נוהל סודיות של פרטי לקוח (פרטים מסוויים).

בינה מלאכותית (יוצרת – generative) הנחיות וכללי שימוש

הזנת הפקודות – "הפרומפט"

מומלץ להימנע ממתן פקודות טקסטואליות ("פרומפט") המתייחסות ספציפית לאלמנטים מוגנים בזכויות יוצרים (תמונות, סגנון אמנותי artistic style, דמויות מסרטים וכו'), אלמנטים המוגנים כסימני מסחר (למשל של מותגים בינלאומיים), או בתמונות התייחסות/תמונות עזר (reference images) מחוללי AI כמו Midjourney למשל מאפשרים למשתמש להעלות תמונות התייחסות בנוסף להנחיות תיאוריות שיכולות לעזור לכוון את המחולל לעבר פלט/תוצר רצוי; אין לכתוב בפרומפט רפרור ליצירות קיימות או להעלות תמונות כרפרור.

בינה מלאכותית (יוצרת – generative) הנחיות וכללי שימוש

בחינת התוצרים אותם מייצרת ה"מכונה"

באשר לתוצרים נמליץ להתייחס אליהם באותם כלים משפטיים מוכרים כפי שנעשה עד היום. השוואה של התוצר לתמונות קיימות לשם בחינת דימיון ליצירה קיימת, לרבות בכלי בדיקה כגון גורם אנושי (עדיף קבוצה של אנשים שונים בארגון), וכן באמצעות כלי חיפוש תמונות הפוך (כמו למשל reverse image search tools, Google Lens או Google Reverse Image)

בנוסף נמליץ לשמור את ה"פרומט" שהוא ההנחיות המשמשות ליצירת כל תוצר במחולל AI

ב- metadata או שם הקובץ של קובץ התמונה לעיון ובחינה מאוחרים יותר ובמיוחד לוודא שתנאי השימוש של מחולל ה-AI מאפשרים שימוש מסחרי בתוצרים;

DALL-E 2

<https://openai.com/dall-e-2/>

- Dall e mini-interpretation of Kermit the frog painted by Munch.



- An astronaut on a horse on the moon or a soup monster made of threads. DALL-E 2 neural network released



תודה על ההקשבה תהיו סקרנים,
תשאלו שאלות ותגידו בוקר טוב במעלית



<http://www.youtube.com/watch?v=lnzDjH1-9Ns>

(04:39)

GOLDFARB
GROSS
SELIGMAN



תודה רבה!

עו"ד סער פלינר

שותף, ראש תחום ליטיגצית קניין רוחני,

רישום זכויות ודיני בידור