



רגולציה תקדימית על טכנולוגיות בינה מלאכותית: אושר חוק ה-AI של האיחוד האירופי

לקוחות יקרים,

היום, 13 במרץ 2024, נחקק חוק ה-AI של האיחוד האירופי,¹ הקובע מסגרת משפטית אחידה לפיתוח ולאספקה של מערכות בינה מלאכותית ולשימוש בהן במדינות האיחוד. מטרתו של החוק היא לקדם טכנולוגיות בינה מלאכותית אמינות, תוך הבטחת רמת הגנה גבוהה על הבריאות, על הבטיחות ועל זכויות האדם והפחתת הסיכון מפני השפעות מזיקות אפשריות. דרישות החוק יחולו ביחס לכל טכנולוגיית AI המשוקת או מופעלת באיחוד האירופי, ללא קשר למקום הימצאות הספק של המערכת או המשתמש בה. בצד החובות המשמעותיות שנקבעו בה, החקיקה מקנה גם סמכות הטלת קנסות חסרת תקדים.

החוק נוקט גישה מבוססת סיכון, המבקשת להתאים את הדרישות שיוטלו ביחס לכל טכנולוגיה לעוצמת הסיכון שהיא עלולה ליצור. לשם כך, החוק מבחין בין טכנולוגיות שהשימוש בהן אסור לחלוטין, טכנולוגיות מסוכנות במיוחד וטכנולוגיות בינה מלאכותית לשימוש כללי (כדוגמת Chat-GPT) וכן מחיל חובת שקיפות ביחס לשימושים מסוימים בטכנולוגיות בינה מלאכותית.

להלן עיקרי הוראות החוק:

שימושים אסורים בבינה מלאכותית

החוק אוסר על שיווק של שימוש במערכות המאפשרות את השימושים הבאים:

1. השפעה על התודעה - טכניקות תת-הכרתיות, מניפולטיביות או מטעות בכוונה, הפוגעות ביכולתו של האדם לקבל החלטה מושכלת או עלולות לגרום לו או לאחרים לנזק משמעותי.
2. ניצול אנשים פגיעים או קבוצות מוחלשות - טכניקות המנצלות נקודות תורפה עקב גיל, מוגבלות או מצב חברתי-כלכלי, והמעוותות באופן מהותי את התנהגות האדם או עשויות לגרום לו או לאחרים לנזק משמעותי.
3. סיווג ביומטרי - סיווג אנשים על סמך נתוניהם הביומטריים כדי ללמוד או להסיק נתונים על גזע, דעות פוליטיות, חברות באיגודים מקצועיים, אמונה דתית או פילוסופית, חיי מין או נטייה מינית.
4. דירוג חברתי - טכניקות להערכה או לסיווג של אנשים בהתבסס על התנהגותם החברתית או על

¹ Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts

תכונותיהם הידועות או המוסקות, באופן המביא ליחס שלילי או כזה שאינו מוצדק ומידתי ביחס להתנהגותם החברתית ולחומרתה.

5. זיהוי ביומטרי - טכניקות לזיהוי ביומטרי בזמן אמת במרחב הציבורי לצורך אכיפת החוק. זאת, למעט כשהדבר נחוץ לזיהוי קורבנות חטיפה, סחר בבני אדם וניצול מיני, חיפוש נעדרים, מניעת איום ממשי ומידי לביטחון, או איתור וזיהוי חשודים בעבירות פליליות, ככל שהשימוש נעשה באופן מידתי ולאחר קבלת הרשאה מגורם מוסמך.
6. ניבוי היתכנות לביצוע עבירה - טכניקות להערכה או ניבוי של הסיכון שאדם מסוים יבצע עבירה פלילית, בהתבסס על הפרופיל שלו, תכונות אישיות ומאפייניו.
7. יצירת מאגרים לזיהוי פנים - טכניקות ליצירה או הרחבה של מאגרים לזיהוי פנים באמצעות איסוף מידע לא ממוקד מהאינטרנט או מצילומי טלוויזיה במעגל סגור.
8. זיהוי רגשות במקום העבודה או בלימודים - טכניקות להסקת רגשות בתחומי מקום העבודה ובמוסדות חינוך, למעט מסיבות רפואיות או בטיחותיות.

מערכות בינה מלאכותית מסוכנות במיוחד

מערכת בינה מלאכותית תיחשב כמערכת מסוכנת במיוחד אם היא נכללת באחת מהקטגוריות הבאות :

1. מוסדרת במסגרת תקני ההרמוניזציה של האיחוד האירופי - מערכת שמיועדת לשמש כרכיב בטיחות של מוצר או שהמערכת היא בעצמה מוצר, שהעיסוק בו מוסדר באמצעות תקנים של האיחוד האירופי.
 2. טכנולוגיה ביומטרית - מערכות ביומטריות לזיהוי מרחוק, מערכות לסיווג ביומטרי על פי הסקה של תכונות ומאפיינים, או מערכות לזיהוי רגשות.
 3. תשתיות קריטיות - מערכות המיועדות לשמש כרכיבי בטיחות בניהול ובתפעול של תשתיות קריטיות, תחבורה, אספקת מים, גז, חימום וחשמל.
 4. השכלה והכשרה מקצועית - מערכות לקביעת קבלה למוסדות חינוך והכשרה מקצועית, להערכת הישגי למידה ורמת לימודים, או לזיהוי התנהגות אסורה של תלמידים במבחנים.
 5. תעסוקה וניהול עובדים - מערכות לגיוס או בחירה של עובדים או לקבלת החלטות המשפיעות על קידום וסיום של יחסי העבודה, הקצאת משימות והערכת ביצועים.
 6. זכאות לשירותים חיוניים - מערכות לבדיקת זכאות לשירותים חיוניים ולהטבות, לרבות שירותי בריאות, קביעת דירוג אשראי ותמחור ביטוחי בריאות וחיים.
 7. אכיפת החוק - מערכות להערכת סיכון שאדם יבצע עבירה או יהפוך לקורבן עבירה, לביצוע פולגרף או כלים דומים, להערכת מהימנות ראיות וליצירת פרופיל של אדם לצורך טיפול בעבירות פליליות.
 8. הגירה, מקלט וביקורת גבולות - מערכות להערכת סיכון של מהגר, לבחינת בקשות מקלט ואשרות ולאיתור וזיהוי של אנשים בביקורת גבולות (למעט לצורך אימות מסמכי נסיעה).
 9. הליכים משפטיים ודמוקרטיים - מערכות שנועדו לסייע לרשות שיפוטית או למנגנון יישוב סכסוכים חלופי לחקור, לפרש את הדין ולהחילו על מערכת עובדתית נתונה, או מערכות שנועדו להשפיע על תוצאות בחירות או משאלי עם (למעט כלים לארגון, ייעול ובנייה של קמפיינים פוליטיים).
- ספק רשאי לטעון בפני הרשויות המוסמכות כי על אף שהמערכת שהוא מציע נכללת באחת מהקטגוריות

הללו, היא אינה מסוכנת במיוחד, משום שאינה יוצרת סיכון משמעותי לבריאות, לבטיחות או לזכויות יסוד, ובכלל זה אינה משפיעה באופן מהותי על הליכי קבלת החלטות ביחס לאנשים. למשל, אם המערכת נועדה לבצע משימה פרוצדורלית צרה, כשהמערכת נועדה אך ורק לשיפור תוצאה של פעולה אנושית, או כשהמערכת נועדה לזהות דפוסי קבלת החלטות שהתקבלו ולא להחליף או להשפיע על הערכה אנושית, יהיו אלה טיעונים רלוונטיים כי יש להחריג את המערכת מתחולת המגבלות על מערכות מסוכנות במיוחד.

ספקים של מערכות מסוכנות במיוחד יהיו אחראים לעמידת מערכותיהם בדרישות הבאות, כאשר גורמים נוספים בשרשרת האספקה (כגון יבואנים, מפיצים וספקים של מערכים נלווים) יידרשו לוודא, ברמות אחריות שונות, כי דרישות אלה מתקיימות:

1. מערכת ניהול סיכונים - על הספק לקיים תהליך מתמשך ומתעדכן לאורך חיי המערכת לזיהוי ולניתוח של סיכונים ידועים וצפויים שהיא עלולה לייצר לבריאות, לבטיחות ולזכויות יסוד. הערכה זו תיעשה הן בהתאם למטרה המיועדת של המערכת והן במצב של שימוש לרעה שניתן לצפותו באופן סביר. המערכת תגדיר אמצעים לביטול או הפחתת הסיכונים. במסגרת חובה זו, הספק יידרש להפעיל מערכת לניטור של ביצועי המערכת לאחר שיווקה, שתאסוף, תתעד ותנתח מידע רלוונטי שמגיע ממטמיעי המערכת או ממקורות אחרים ביחס לביצועי המערכת ותבחן את המשך עמידתה בדרישות החוק. בנוסף, הספק מחויב בדיווח על אירועים חמורים שהתרחשו בעקבות הפעלת המערכת (כגון מוות, נזקים חמורים, גגיעה בזכויות ושיבוש תשתיות) לרשויות הרלוונטיות.
2. איכות המידע וטיפול בנתונים - המערכת תפותח על בסיס אימון מודלים הכוללים מערכי נתונים איכותיים. בכלל זה, ייבחרו מערכי נתונים רלוונטיים ומייצגים ביחס למטרת המערכת, והמתחשבים במאפיינים ייחודיים לסביבה שבה המערכת מיועדת לשימוש. בנוסף, ייערכו פעולות הכנה לעיבוד המידע (כגון ניקוי ועדכון), ייבחנו הטיות אפשריות במידע וינקטו אמצעים לזיהוי ולצמצום ההטיות.
3. תיעוד טכני - תיעוד של מאפייני המערכת, שיאפשר להוכיח את עמידתה בדרישות החוק. התיעוד יכלול, בין השאר, תיאור של מרכיבי המערכת ותהליך התכנון והפיתוח שלה, הבדיקות שנעשו ואמצעי האבטחה שהוטמעו בה, מידע על יכולות ומגבלות המערכת והסיכונים האפשריים שבהפעלתה, תיאור השינויים שבוצעו בה ותיאור תוכנית הפיקוח על פעילותה של המערכת לאחר שיווקה ואספקתה.
4. שמירת לוגים - המערכת תכלול אפשרות לתיעוד אוטומטי של אירועים לאורך חיי המערכת, בין היתר ביחס למצבים היוצרים סיכון או לשינויים מהותיים שהתרחשו בה לאחר הפצתה ושלא נחזו מראש, ואשר משפיעים על עמידתה בדרישות החוק. דרישות תיעוד מחמירות יחולו ביחס למערכות לזיהוי ביומטרי מרחוק.
5. שקיפות ומסירת מידע למטמיעי המערכת - המערכת תתוכנן ותפותח באופן שיאפשר למשתמשים לפרש את הפלט שנוצר על ידה ולהשתמש בו כראוי. המערכת תלווה בהוראות שימוש שיכללו, בין השאר, פרטי קשר עם הספק או נציגו המורשה, פירוט על המאפיינים, היכולות והמגבלות של המערכת, שינויים צפויים במערכת ואמצעי הפיקוח האנושיים שיופעלו עליה.
6. פיקוח אנושי - המערכת תתוכנן ותפותח כך שבני אדם יוכלו לפקח על פעילותה במטרה למנוע או למזער סיכונים לבריאות, לבטיחות ולזכויות יסוד כתוצאה משימוש בה. המערכת תכלול הן אמצעים שהוטמעו במערכת לפני שיווקה, והן ממשקים שיאפשרו פיקוח על ידי המשתמש עצמו. על המערכת להימסר למשתמש במצב שבו קיים גורם אנושי שיכול להבין כראוי את היכולות והמגבלות של המערכת, לפרש נכונה את הפלט שנוצר על ידה, להתערב בפעולות המערכת ולעצור את פעולתה.

דרישות מחמירות יחולו ביחס לקבלת החלטות המתבססת על מערכות זיהוי ביומטרי מרחוק, באופן שיחייב, למעט בנסיבות מוגדרות, אימות אנושי.

7. דיוק, עמידות ואבטחת סייבר - ינקטו אמצעים טכניים וארגוניים כדי להבטיח שהמערכת תהיה עמידה ככל האפשר מפני שגיאות, תקלות או פעולות לא עקביות, וכן כדי למנוע פגיעה בעמידותה או ניסיונות של גורמים בלתי מורשים להשפיע על תפקודה.

דרישות נוספות המוטלות על ספקי מערכות מסוכנות במיוחד כוללות שמירת התיעוד הטכני ומסמכים נוספים למשך 10 שנים מיום שיווק המערכת באיחוד ומסירתם לרגולטורים לפי הצורך, סימון המערכת בתו הסימון והתקינה האירופי, רישום המערכת במאגר ייעודי של האיחוד ומינוי נציג מורשה באיחוד לספקים הממוקמים מחוצה לו. כמו כן, הספק יידרש לקיים הליך הערכת תאימות בהתאם לדרישות החוק, כשביחס למערכות ביומטריות מסוימות, ההערכה תידרש להתבצע בידי גוף בדיקה חיצוני.

החוק מחיל חובות נוספות על משתמשי המערכות מסוג זה, שנדרשים לנקוט אמצעים טכניים וארגוניים כדי לוודא שהשימוש נעשה בהתאם להוראות השימוש, למנות מפקחים אנושיים בעלי הכשרה מתאימה, להתריע לגורמים הרלוונטיים (ובכלל זה לרשויות המוסמכות) על חשד לסיכון משמעותי שעולה מהמערכת, לשמור לוגים שנוצרים במערכת, וליידע את הגורמים המושפעים מהמערכת (למשל, עובדים במקום העבודה).

חובות שקיפות

חובות שקיפות תחול ביחס למערכות המיועדות לשימושים הבאים:

1. מערכות המתקשרות עם בני אדם - ספק המערכת אחראי לתכנון ולפיתוח המערכת כך שאנשים ידעו שהם מתקשרים עם מערכת בינה מלאכותית, אלא אם הדבר ברור מנקודת מבטו של אדם סביר. החובה לא תחול ביחס למערכות הפועלות להתמודדות עם עבירות פליליות.
2. מערכות המייצרות תוכן סינתטי - ספק המערכת אחראי לוודא כי הפלט של מערכת המייצרת אודיו, תמונה, וידאו או טקסט יסומן באופן המזהה אותו כתוכן שנוצר באופן מלאכותי או עבר מניפולציה. החובה לא תחול ביחס למערכות המסייעות לעריכה סטנדרטית או אינן משנות באופן מהותי את הקלט שסופק על ידי המשתמש.
3. מערכות לזיהוי רגשות או מערכות סיווג ביומטריות - על מטמיע המערכת ליידע את האנשים שנחשפו למערכת בדבר השימוש בה. החובה לא תחול ביחס למערכות שמטרתן התמודדות עם עבירות פליליות.
4. מערכות המייצרות דיפ-פייק או מניפולציות בטקסט - על מטמיע המערכת לחשוף כי התוכן נוצר על ידי המערכת או עבר מניפולציה מלאכותית על ידה, למעט בהקשרי התמודדות עם עבירות פליליות. כשהשימוש נעשה כחלק מתוכנית אומנותית-יצירתית, היידוע ייעשה כך שלא תיפגע ההנאה מהיצירה.

מודל בינה מלאכותית למטרות כלליות (GPAI)

מודל למטרות כלליות הוא מודל המסוגל לבצע במיומנות מגוון רחב של משימות מובחנות, לרבות באמצעות אימון עם כמות מידע גדולה, ושניתן לשלבו במגוון מערכות או יישומים, כדוגמת Chat-GPT.

על כלל הספקים של מודלים אלה יחולו החובות לערוך תיעוד טכני מתעדכן של המודל ולספק מידע רלוונטי לספקי מערכות בינה מלאכותית שמבקשים לשלב את המודל במערכותיהם, וכן להעמיד לרשות הציבור סיכום מפורט של המידע ששימש לאימון המודל. כמו כן, ספק שהוקם מחוץ לאיחוד ושיבקש

להפוך את המודל לזמין ברחבי האיחוד, יידרש למנות נציג מורשה באיחוד. דרישות מופחתות יחולו על מודלים המונגשים לציבור תחת רישיון חופשי ופתוח (למעט מודלים בעלי סיכון מערכתי).

חובות נוספות יחולו ביחס למודלים הכוללים סיכון מערכתי. בקטגוריה זו יכללו מודלים שהם בעלי יכולות השפעה גבוהות, שייקבעו בהתבסס על כוח העיבוד המצטבר המשמש לאימון המודל, וכן מודלים שהנציבות קבעה שהם מייצרים סיכון דומה. ספקים אלה יוכלו לערער על הכללתם בקטגוריה בפני הנציבות.

ספקים של מודלים הכוללים סיכון מערכתי יחויבו לבצע הערכות סיכון בהתאם לפרוטוקולים מוכרים, להעריך סיכונים מערכתיים אפשריים ואת מקורותיהם ולנקוט אמצעים להפחתתם, לדווח לרשויות על תקריות חמורות שאירעו והאמצעים המתקנים האפשריים לטיפול בהן, ולהבטיח רמה נאותה של הגנת סייבר על המודל ועל התשתית הפיזית שלו.

אכיפה וקנסות

הפרת החוק עשויה להביא לקנסות מנהליים בהיקפים משמעותיים. שימושים אסורים בטכנולוגיות בינה מלאכותית מאפשרים הטלת קנס מנהלי של **עד 35 מיליון אירו או עד 7% מסך המחזור השנתי העולמי** של החברה בשנת הכספים הקודמת להפרה, הגבוה מבניהם. אי-עמידה בהוראות החוק ביחס למערכות מסוכנות במיוחד, ביחס למודלים למטרות כלליות או עקב הפרה של חובת השקיפות מאפשרים להטיל **קנס של עד 15 מיליון אירו או עד 3% מהמחזור השנתי העולמי** של החברה.

בנוסף, לנציבות האירופית ולרשויות הפיקוח תינתן הסמכות להורות על נקיטת פעולות מתאימות כדי להתאים את הטכנולוגיה להוראות החוק או להפחית את הסיכון שהמערכת או המודלים עלולים ליצור, ובכלל זה לעצור את שיווק המערכת או לחייב את החזרת המערכת לספק (recall).

תחילת החוק

תחולת הוראות החוק נקבעה באופן הדרגתי. השימושים האסורים בבינה מלאכותית ייכנסו לתוקף חצי שנה מיום פרסום החוק; מרבית החובות ביחס למערכות המסוכנות במיוחד ייכנסו לתוקף שנתיים מיום פרסום החוק; הוראות ביחס למודלים למטרות כלליות, וכן ההוראות לעניין העיצומים המנהליים, ייכנסו לתוקף שנה מיום פרסום החוק.

סיכום

חוק ה-AI של האיחוד האירופי מעצב סביבה רגולטורית ראשונה מסוגה לתכנון, פיתוח ושיווק של טכנולוגיות בינה מלאכותית ולשימוש בהן. החוק צפוי להשפיע על מפתחים וספקים של מערכות ומודלים של בינה מלאכותית, הן במהלך שלבי התכנון והפיתוח והן לאחר השיווק והאספקה, ובכלל זה ביחס לניהול הסיכונים הקיימים והאפשריים שהטכנולוגיה יוצרת, למודלים שמשמשים לאימון המערכות, לניטור פעולות המערכת לאחר הפעלתה ולשקיפות כלפי המפעילים והמושפעים מהטכנולוגיה. לחוק תהיה השפעה גם מעבר לגבולות מדינות האיחוד, לאור תחולתו על כל טכנולוגיית בינה מלאכותית המשווקת או המופעלת באיחוד, ללא קשר למיקום הספק, וכן בשל ההשפעה הצפויה של החוק על גיבוש רגולציה במדינות אחרות. השפעה זו תתעצב גם לאור אסדרה של סוגיות נוספות בבינה מלאכותית שאינן זוכות למענה במסגרת החוק, וביניהן החלת "נמלי מבטחים" להפחתת הנטל הרגולטורי והכרעה בשאלת האחריות ביחס לנזקים שנגרמו ממערכות AI על אף עמידת ספקיהן ומשתמשיהן בהוראות החוק. ההיערכות לעמידה בדרישות החוק מחייבת הכנה טכנולוגית, ארגונית ומשפטית נרחבת, שתתעצב בשנים

הקרובות לאור ההנחיות ופעולות האכיפה של הרגולטורים האירופיים.

מחלקת הסייבר וטכנולוגיות המידע במשרדנו עומדת לרשותכם ומציעה תהליכי מיפוי, ליווי, הכנה וציות להוראות החוק, ועומדת לרשותכם בכל שאלה בנושא זה.

עדכון זה נכתב על ידי אמיר איל

למידע נוסף ניתן לפנות אל:

03-6941320

adat@fbclawyers.com

עו"ד עמית דת

03-6941320

orachum@fbclawyers.com

עו"ד עמרי רחום-טוויג

.....
הכלול באגרת מידע זו הוא מידע כללי בלבד, הוא אינו חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו. כל הזכויות שמורות לפישר (FBC & Co.).
להירשם למייל זה או להסרה מרשימת התפוצה: news@fbclawyers.com