

בינה מלאכותית אחראית

מסע בעקבות חוק הבינה
המלאכותית האירופאי (AIA)

מהדורה ראשונה | יולי 2023

כתב: גלעד ירון



קצת על עצמי ומה כל זה?

שלום.

כבר למעלה מ-30 שנה אני מתגלגל בעולם ניהול מערכות המידע, תכנון פתרונות וייעוץ בתחום הגנת הסייבר והגנת הפרטיות.

לאחר שנדבקתי בוורוס הפרטיות (זה די מסוכן!) התחלתי לעסוק בנושא באופן די אינטנסיבי.

עבדתי עם כולם - מנכ"לים, יועצים משפטיים, מנהלי סיכונים, מנהלי מחשוב ואבטחת מידע, בניסיון לסייע להם להתמודד עם החוקים הסבוכים האלה, הסטנדרטים הארוכים ודרישות הלקוחות שלא נגמרות לעולם.

אני מנסה לעזור להם להבין מה רוצים מהם, לתרגם את זה לשפה אנושית ולתוכניות עבודה פרקטיות, כך שהם יוכלו לעמוד בדרישות מבלי לפגוע במשימותיהם העסקיות.

עם פריצתו (מחדש) של עולם האינטליגנציה המלאכותית והמודעות ההולכת וגוברת לסיכונים הכרוכים בנושא זה, התחלתי לעסוק גם בנושא זה שיש לו קווי דמיון רבים לאופן הניתוח, החשיבה וההערכות לנושאים האחרים בהם אני עוסק.

על מנת לקדם את התפיסה ההוליסטית של הגנת המידע, תוך דגש על הצד המעשי של השילוב בין כל התחומים הללו, הקמתי את חברת Data Protection Matters.

עם פרוץ ה-GDPR, ב-2017, פרסמתי מידי יום פרשנות לפסוק אחד מן ה-GDPR. 99 פסוקים סך הכול.

עתה בצעתי פרויקט דומה עבור חוק הבינה המלאכותית האירופאי.

עם סיום הפרויקט הרי לפניכם חוברת המסכמת את כל הפוסטים.

שימו לב – כרגיל, זוהי פרשנות חופשית שלי לטקסט ואינה מחייבת בשום צורה. השימוש בכתוב הוא על אחריותכם בלבד.

אתם מוזמנים לעקוב:

הפרופיל שלי ב-LinkedIn: <https://www.linkedin.com/in/giladyaron/>

דף הבית של החברה:

www.data-protection-matters.com

קבוצה ב-LinkedIn הדנה בבינה מלאכותית אחראית:

<https://www.linkedin.com/groups/9383372/>



גלעד ירון

Gilad@GiladYaron.com

052-6755514



מבוא

ברוכים הבאים לחוברת זו, שמטרתה להנגיש את חוק הבינה המלאכותית האירופאי (AIA) בשפה עברית פשוטה לכל מי שמתעניין בנושא.

AIA היא הצעת חוק פורצת דרך שהועלתה על ידי הנציבות האירופית. במטרה להסדיר את היצירה והיישום של מערכות בינה מלאכותית (AI) באיחוד האירופי.

זוהי תקנת הבינה המלאכותית המקיפה הראשונה בעולם.

היא מגדירה מסגרת לממשל בינה מלאכותית, תוך התייחסות לקשת רחבה של נושאים.

אלה כוללים, בין היתר, את הבטיחות של מערכות בינה מלאכותית, שמירה על זכויות יסוד ושקיפות החלטות שמתקבלות על ידי בינה מלאכותית.

החוק מתייחס למגוון רחב של יישומי בינה מלאכותית, מטכנולוגיית זיהוי פנים ועד כלי רכב בנהיגה עצמית כמו גם לרכיבי AI המהווים חלק ממערכת אחרות.

ה-AIA מרחיב את תחום השיפוט שלו למערכות בינה מלאכותית שפותחו ומשמשות מחוץ לאיחוד האירופי, במידה שהן משמשות לאיסוף או עיבוד נתונים של אזרחי האיחוד האירופי. כאן אנו רואים קווי דמיון לחוק פורץ דרך אחר של האיחוד – GDPR.

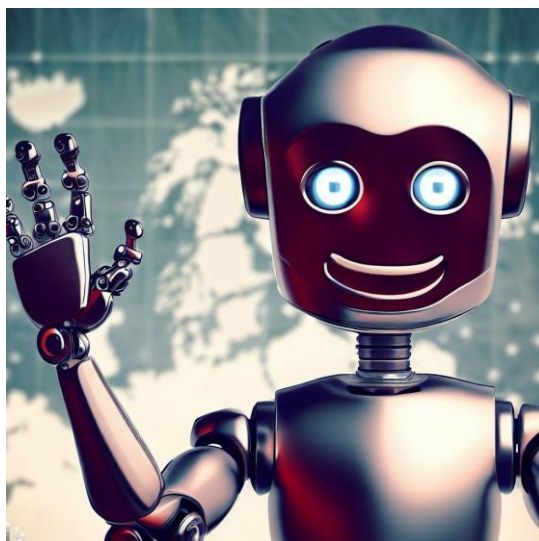
הרגולציה מספקת דרגות שונות של פיקוח ואכיפה, בהתאם לסיכון הקשור למערכת בינה מלאכותית מסוימת. אסטרטגיה זו שואפת להגיע לאיזון בין הבטחת הבטיחות והאבטחה של המערכות וטיפול חדשנות.

ה-AIA עשוי להשפיע באופן משמעותי על הפיתוח והיישום של מערכות בינה מלאכותית באיחוד האירופי ובעולם כולו.

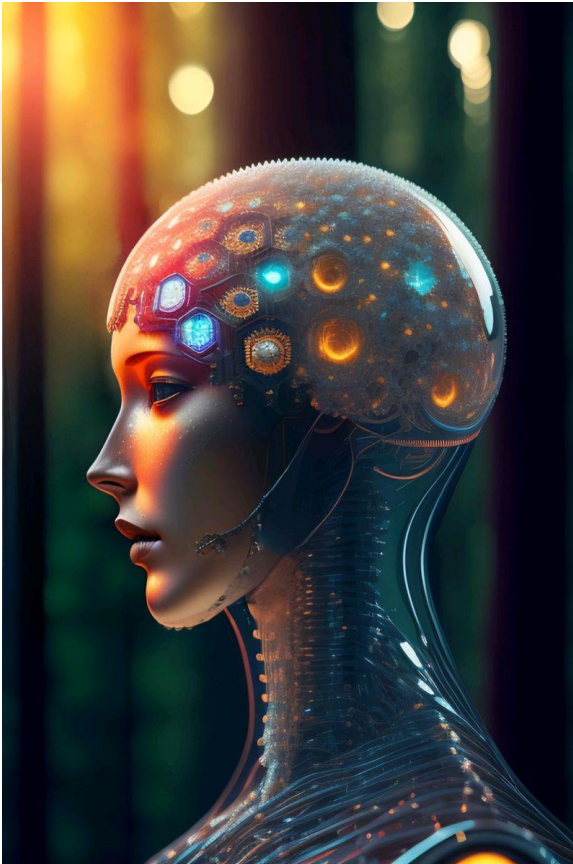
הרגולציה יכולה למלא תפקיד מרכזי בהבטחה כי מערכות בינה מלאכותית יפותחו ויעשה בהן שימוש באחריות, וזאת מבלי לפגוע בחדשנות העשויה לתרום רבות לעולמנו ולנו, היושבים בו.

להלן כמה מהיתרונות שתקנת ה-AIA מציעה:

- ✓ **בטיחות ואבטחה של מערכות** – החוק משלב מספר הוראות שמטרתן למנוע שימוש לרעה במערכות AI למטרות מזיקות, כגון הפצת דיסאינפורמציה או אפליה.
- ✓ **הגנה על זכויות יסוד** – החוק נועד לשמור על זכויות היסוד של יחידים, לרבות הזכות לפרטיות ואי-אפליה.
- ✓ **קידום שקיפות ואחריות** – החוק מחייב שמערכות בינה מלאכותית פועלות בצורה שקופה ואחריות, המאפשרת לאנשים להבין כיצד הנתונים שלהם מנוצלים וכיצד מתקבלות החלטות.



פרק 1 – יוצאים לדרך



אנחנו יוצאים למסע, צעד צעד, בנבכי חוק הבינה המלאכותית האירופי אשר ממשמש ובא. חוק זה אמור לעשות סדר במהפכת ה-AI שתשנה את חיינו. נפתח את המסע בחלק הראשון של היצירה שכולל את הפסוקים 1-4. חלק זה עוסק בתחולת התקנה:

תקנה זו קובעת כללים מותאמים להוצאה לשוק, הפעלה ושימוש במערכות בינה מלאכותית ('מערכות AI' באיחוד).

התקנה קובעת איסור מוחלט על פיתוח ושימוש בפרקטיקות מסוימות של בינה מלאכותית.

היא מציגה דרישות ספציפיות למערכות בינה מלאכותית בסיכון גבוה ומגדירה חובות למפעילי מערכות כאלה.

בנוסף היא מגדירה כללי שקיפות מותאמים עבור מערכות בינה מלאכותיות המיועדות לקיים אינטראקציה עם אנשים טבעיים, מערכות זיהוי רגשות ומערכות סיווג ביומטריות, ומערכות בינה מלאכותית המשמשות להפקה או מניפולציה של תוכן תמונה, אודיו או וידאו; ולבסוף היא קובעת כללים בנושא ניטור ופיקוח על השוק.

תקנה זו חלה על:

- ספקים המוציאים לשוק מערכות בינה מלאכותית באיחוד, בין אם הם מבוססים באיחוד או במדינה שלישית;
 - משתמשים במערכות בינה מלאכותיות הממוקמות בתוך האיחוד;
 - ספקים ומשתמשים של מערכות בינה מלאכותיות הממוקמות במדינה שלישית, אשר התפוקה המיוצרת על ידי המערכת משמשת באיחוד;
- בחלק זה עשרות הגדרות של מושגים שונים. אנו נתייחס רק לעצם העניין. אומרים AI יש בעוולם. מה זה AI: 'מערכת בינה מלאכותית' (מערכת AI) היא תוכנה שפותחה עם אחת או יותר מהטכניקות הבאות ויכולה, עבור קבוצה נתונה של יעדים מוגדרים על ידי אדם, לייצר פלטים כגון תוכן, תחזיות, המלצות או החלטות המשפיעות על הסביבה שאיתן הם מתקשרים. זה כולל:
- למידת מכונה (machine learning) לרבות מפקחת ולא מפקחת, תוך שימוש במגוון רחב של שיטות כולל למידה עמוקה;
 - גישות מבוססות לוגיקה וידע, לרבות ייצוג ידע, תכנות אינדוקטיבי (לוגי), בסיסי ידע, מנועי הסקה, חשיבה (סמלית) ומערכות מומחה;
 - גישות סטטיסטיות, אומדן בייסיאני, שיטות חיפוש ואופטימיזציה.

פרק 2 - כשהבינה עושה מה שאסור



המסע שלנו היום ייקח אותנו לעיר האסורה.
ונשמרתם מאד לנפשתיכם.

כרגיל - קצת סיכום מהספר וקצת הערות משלי
(בסוגרים). זו אחריותכם המלאה מה תעשו עם
התובנות האלה ובכלל עם הסיכום שלי. רק
המסמך עצמו הוא המסמך עצמו (אל תגידו שלא
אמרת).

הפסוק שלנו להיום (שמספרו 5) מתאר שיטות
בינה מלאכותיות שאסורות בתכלית האסור בשל
הפגיעה הפוטנציאלית שלהן ביחידים או בחברה.

שימו לב, שהמושג "AI" בספרנו הוא סופר רחב.
הוא לא מתחיל ולא נגמר ב ChatGPT.

חלק מסוגי המערכות עליהן מדובר כאן קימות כבר
מקדמת דנא.

והזוכים המאושרים הם/הן:

1. מערכות המשתמשות בהשפעה תת-הכרתית
כדי לעוות מהותית את התנהגותו של אדם, ולגרום
לנזק פיזי או פסיכולוגי. (ככה כתוב במקור...
מישהו אמר קמברידג' אנליטיקה?).

2. מערכות בינה מלאכותית המנצלות פגיעות של קבוצות ספציפיות בשל גילן, מוגבלות פיזית או נפשית, כדי לעוות
מהותית את התנהגותן, ולגרום לנזק פיזי או פסיכולוגי. (ספאם כשירות?)

3. רשויות ציבוריות אינן יכולות להשתמש במערכות AI כדי להעריך או לסווג את מהימנותם של אנשים על סמך
התנהגותם החברתית או מאפיינים אישיים או אישיותיים ידועים או חזויים. (מבחני מיון במכון כזה או אחר?)

4. ניתן לעשות שימוש במערכות זיהוי ביומטריות מרחוק 'בזמן אמת' במרחבים נגישים לציבור עבור אכיפת החוק
רק בנסיבות ספציפיות, כגון חיפוש ממוקד אחר קורבנות פוטנציאליים ספציפיים לפשע, מניעת פשע ספציפי, איום
ממשי ומידי על החיים או על הבטיחות הפיזית, או גילוי, לוקליזציה, זיהוי או העמדתו לדין של מבצע או חשוד
בעבירה פלילית חמורה. (מישהו מביט עלינו כאן מעין הנץ?)

5. כל שימוש אינדיבידואלי במערכות 'זיהוי ביומטריות מרחוק' 'בזמן אמת' למטרות אכיפת חוק חייב להיות כפוף
לאישור מוקדם שניתן על ידי רשות שיפוטית או על ידי רשות מנהלית עצמאית של המדינה החברתית. (אהה)

האיסורים הללו נועדו להגן על הזכויות והחירויות שלנו מול טכנולוגיות AI מתקדמות.

פרק 3 - בינה מלאכותית במשקל חריג



חוק הבינה המלאכותית האירופאי נוקט בגישה מבוססת סיכונים.

רמת הפיקוח והבקרה הרגולטורית היא פרופורציונלית לרמת הסיכון הקשורה למערכת.

החוק מגדיר ארבע רמות של סיכון: מערכות ששומר נפשו ירחק מהן; כאלה שהסיכון שבשימוש בהן גבוה - עליהן נדבר היום; וכאלה בסיכון נמוך ומינימלי.

אז כפי שצינתי בספוילר, היום נדבר על מערכות שניתן להקים ולנהל, אבל הן מה זה מסוכנות (למהדרין - ראו פסוקים 6-7 ונספח III).

התקנה מסמיכה את הנציבות להוסיף מערכות בינה מלאכותית לרשימת הסיכון הגבוה אם הן מיועדות לשמש עבור אחד מהתחומים הבאים והן מהוות סיכון לפגיעה בבריאות ובבטיחות, או סיכון לפגיעה בזכויות יסוד.

הנספח נספח כדי לאפשר שינוי והרחבה שלו תוך כדי תנועה. אז הנה זה בא. מערכות מסוג זה נחשבות מסוכנות

- 1 זיהוי ביומטרי: מערכות בינה מלאכותית המשמשות לזיהוי ביומטרי של אנשים בזמן אמת ולאחר האיסוף.
- 2 ניהול תשתית קריטית: מערכות בינה מלאכותית המשמשות כרכיבי בטיחות בניהול ותפעול תשתיות קריטיות כמו תעבורת כבישים, מים, גז, חימום ואספקת חשמל.
- 3 חינוך והכשרה מקצועית: מערכות בינה מלאכותית המשמשות לקבלה למוסדות חינוך והכשרה מקצועית ולהערכת תלמידים ונבחנים.
- 4 ניהול תעסוקה ועובדים: מערכות בינה מלאכותית המשמשות לגיוס או מיון, קבלת החלטות לגבי קידום וסיום יחסים חוזיים הקשורים לעבודה, הקצאת משימות, ניטור והערכת ביצועים והתנהגות.
- 5 גישה לשירותים פרטיים וציבוריים חיוניים: מערכות בינה מלאכותיות המשמשות רשויות ציבוריות להערכת זכאות להטבות ושירותים של סיוע ציבורי, להערכת כושר האשראי ולשלוח שירותי תגובה ראשונה לשעת חירום.
- 6 אכיפת חוק: מערכות בינה מלאכותית המשמשות את רשויות אכיפת החוק להערכת סיכונים פרטניות, זיהוי מצבים רגשיים, זיהוי זיופים עמוקים, הערכת מהימנות הראיות, חיזוי עבירות פליליות, יצירת פרופילים וניתוח פשיעה.
- 7 ניהול הגירה, מקלט ובקרת גבולות: מערכות בינה מלאכותיות המשמשות רשויות ציבוריות מוסמכות להערכת סיכונים, אימות האותנטיות של מסמכי הנסיעה, וסיוע בבחינת בקשות למקלט, אשרה ואישורי שהייה.
- 8 ניהול משפט ותהליכים דמוקרטיים: מערכות בינה מלאכותית המשמשות לסייע לרשות שיפוטית בחקירה ופרשנות של עובדות ומשפט, ובהחלת החוק על מערכת עובדות קונקרטיה.

פרק 4 - נא לחזק את יסודות המבנה!



אחד מעקרונות היסוד של החוק הינו הגישה מבוססת הסיכונים. המשמעות היא כי רמת הפיקוח והבקרה הרגולטורית היא פרופורציונלית לרמת הסיכון הקשורה למערכת בינה מלאכותית מסוימת.

היום נדבר על הבקרות שהתקנה דורשת ליישם במערכות בסיכון גבוה, כפי שהן באות לידי ביטוי בפסוקים 8 עד 15 בתקנה.

מערכות AI בסיכון גבוה חייבות לעמוד בדרישות שנקבעו להלן. דרישות אלו נועדו להבטיח את הבטיחות והיעילות שלהן. יש להקים מערכת ניהול סיכונים לתוכנות בינה מלאכותית בסיכון גבוה. (הערה שלי: כשמשמשים במושג "מערכת" בהקשר זה, הכוונה לתהליכי ניהול, לא למערכת ברזלים ועננים). מערכת זו צריכה לפעול לאורך כל מחזור החיים של ה-AI מתוך עדכון שיטתי קבוע.

בין היתר צריכה מערכת זו לכלול זיהוי וניתוח של סיכונים ידועים וצפויים, הערכה של סיכונים קיימים וסיכונים העלולים להתעורר בהתבסס על בחינה וניטור לאחר יציאה לשוק, ואימוץ אמצעים מתאימים לניהול סיכונים.

✓ יש לוודא כי מערכות בינה מלאכותית בסיכון גבוה המשתמשות בטכניקות הכרוכות באימון של מודלים עם נתונים רבים, יסתמכו על מערכי נתונים איכותיים, לאחר אימות ובדיקה. מערכי נתונים אלה חייבים לעמוד בקריטריונים מסוימים של איכות ולהיות כפופים לנוהלי ממשל וניהול נתונים מתאימים. פרקטיקות אלו כוללות בחירות עיצוב, איסוף נתונים, פעולות עיבוד הכנת נתונים, גיבוש הנחות רלוונטיות, הערכה מוקדמת של זמינות מערכי הנתונים, כמותם והתאמתם, בחינת הטיות אפשריות וזיהוי כל פערים או חסרונות אפשריים בנתונים.

✓ יש ליצור תיעוד טכני עבור מערכות בינה מלאכותית בסיכון גבוה לפני פריסת המערכת ולעדכנו באורח שוטף. תיעוד זה אמור להוכיח שמערכת הבינה המלאכותית עומדת בדרישות ולספק לרשויות הרלוונטיות את כל המידע הדרוש כדי להעריך את תאימותן לדרישות.

✓ מערכות בסיכון גבוה חייבות להיות בעלות יכולות הקלטת אירועים (רישום לוג) התואמות לסטנדרטים מוכרים. יכולות רישום אלו אמורות להבטיח מעקב אחר תפקוד מערכת הבינה המלאכותית לאורך מחזור החיים שלה ולהקל על ניטור לאחר יציאתה לשוק.

✓ מערכות בינה מלאכותיות בסיכון גבוה חייבות להיות מתוכננות ומפותחות בצורה שתבטיח שהפעולה שלהן שקופה מספיק כדי לאפשר למשתמשים לפרש את הפלט של המערכת ולהשתמש בה כראוי. יש לצרף למערכות הוראות שימוש הכוללות מידע תמציתי, מלא, נכון וברור רלוונטי, נגיש ומובן למשתמשים.

✓ מערכות בינה מלאכותיות בסיכון גבוה חייבות להיות מתוכננות ומפותחות בצורה כזו שניתן יהיה לפקח עליהן ביעילות על ידי בני אנוש במהלך התקופה שבה הן נמצאות בשימוש. פיקוח אנושי זה נועד למנוע או למזער את הסיכונים לבריאות, לבטיחות או לזכויות יסוד שעלולים להופיע כאשר נעשה בהן שימוש.

✓ מערכות בינה מלאכותית בסיכון גבוה חייבות להיות מתוכננות ומפותחות כך שהן ישיגו רמה מתאימה של דיוק, חוסן ואבטחת סייבר, ויתפקדו באופן עקבי בהיבטים אלו לאורך מחזור החיים שלהן.

✓ המערכות צריכות להיות עמידות בפני שגיאות, תקלות או חוסר עקביות ונגד ניסיונות של צדדים שלישיים לא מורשים לשנות את השימוש או הביצועים שלהן.

פרק 5 – השחקנים במחזה



במחזה הזה של הבינה המלאכותית מספר שחקנים: יצרני המערכות, המפיצים שלהן ובסוף המשתמשים בהן. אנו מסכמים היום את הפסוקים 16 עד 29 של היצירה. הנחיות לספקי בינה מלאכותית בסיכון גבוה:

◊ הספקים נדרשים להקים מערכת ניהול איכות, לבצע הערכה של ההתאמה לדרישות, לנקוט פעולות מתקנות אם המערכת אינה עומדת בדרישות, להודיע לרשויות המוסמכות על כל אי התאמה ופעולות מתקנות שננקטו ולהציג את התאימות של מערכת הבינה המלאכותית בסיכון גבוה על פי דרישה.

- ◊ עליהם להקים מערכת ניהול איכות המבטיחה עמידה בתקנה זו. המערכת צריכה לכלול אסטרטגיות לעמידה ברגולציה, נהלי עיצוב ופיתוח, מערכות ניהול נתונים, מערכות ניהול סיכונים, מערכות ניטור לאחר יציאה לשוק, נהלי דיווח על אירועים, נהלי תקשורת, מערכות ניהול רישומים, ניהול משאבים ומסגרת אחריות.
- ◊ עליהם להכין תיעוד טכני הכולל תיאור כללי של המערכת, מרכיביה ותהליך הפיתוח; מידע על הניטור, התפקוד והבקרה; מערכת ניהול הסיכונים; התקנים המיושמים; הצהרת התאימות של האיחוד האירופי ומערכת הערכת הביצועים לאחר השוק.
- ◊ הם נדרשים להבטיח שהמערכות שלהם יעברו את תהליך הערכת ההתאמה הרלוונטי לפני יציאתן לשוק או כניסתן לשירות. לאחר שהוכחה תאימות, על הספקים לערוך הצהרת התאמה של האיחוד האירופי. (על תהליך זה נרחיב בפרקים הבאים).

מפצי מערכות בינה מלאכותית בסיכון גבוה נדרשים:

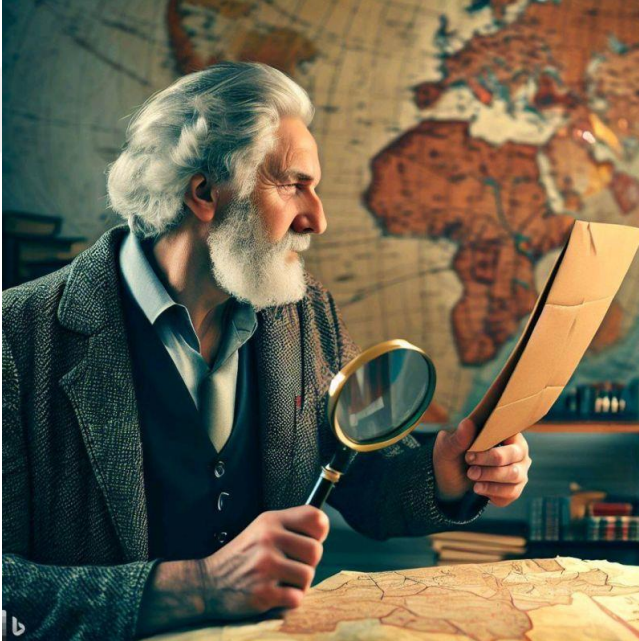
- ◊ לוודא שלמערכות בינה מלאכותית בסיכון גבוה יש את הסימון והתיעוד הנדרשים לתאימות CE לפני שהן זמינות בשוק. אם מערכת אינה תואמת את הדרישות, אין להפיץ אותה עד שתהפוך להיות תואמת.
- ◊ על המפיצים לוודא שתנאי האחסון או ההובלה אינם מסכנים את תאימות המערכת. אם נמצא שמערכת אינה עומדת בדרישות, על המפיצים לנקוט בפעולות מתקנות או לוודא שהספק או היבואן יעשו זאת.
- ◊ עליהם לספק את כל המידע והתיעוד הדרושים להדגמת התאמה של מערכת לפי בקשה מרשות מוסמכת לאומית.
- ◊ כל מפיק, יבואן, משתמש או צד שלישי אחר ייחשבו כספק אם הם מוציאים לשוק מערכת בינה מלאכותית בסיכון גבוה תחת שמם או הסימן המסחרי שלהם, ישנו את המטרה המיועדת של המערכת או יבצעו שינוי מהותי במערכת. במקרים אלו, הספק המקורי אינו נחשב עוד כספק.

משתמשים במערכות בינה מלאכותית בסיכון גבוה נדרשים:

- ◊ להשתמש במערכות בהתאם להוראות המצורפות ולוודא שנתוני הקלט רלוונטיים אם יש להם שליטה עליהם.
- ◊ עליהם לפקח על פעולת המערכת ולהודיע לספק או למפיץ אם הם סבורים שהמערכת מהווה סיכון או אם הם מזהים אירוע חמור או תקלה כלשהי.
- ◊ על המשתמשים לשמור את היומנים שנוצרו אוטומטית על ידי המערכת למשך תקופה מתאימה.
- ◊ עליהם להשתמש במידע המסופק לפי סעיף 13 כדי לעמוד בחובתם לבצע הערכת השפעה על הגנת מידע, במידת הצורך.

להזכירכם, סעיף 13 מציינ כי מערכות בסיכון גבוה חייבות להיות מתוכננות לשקיפות, לספק הוראות שימוש מקיפות ולספק מידע מפורט על הספק, מטרת המערכת, מאפייני הביצועים, מגבלות, סיכונים ידועים, מפרטי נתוני קלט, שינויים שנקבעו מראש, אמצעי פיקוח אנושי, משך החיים הצפוי וכן מידע על תחזוקה ועדכוני תוכנה.

פרק 6 - מי מעריך אתכם?



האיחוד האירופי הגדיר מוסדות שנקראים גוף מודיע (Notified Body). אלה ארגונים המוקמים על ידי מדינה חברה באיחוד על מנת להעריך את התאמתם של מוצרים מסוימים, לפני יציאתם לשוק האירופי, ולדרישות הטכניות הרלוונטיות.

ברשותכם, אנחנו נכנה גופים אלה "גופי הערכה". (אם למישהו יש תרגום יותר טוב - שיקום).

היום נסכם את הפסוקים 40-51 של ה-AIA המדברים על גופי הערכה ספציפיים לעולם הבינה המלאכותית.

תשתו הרבה מים. אנחנו יוצאים לדרך.

כל מדינה באיחוד אחראית על הקמת רשות הערכה מרכזית האחראית על קביעה וביצוע נהלים להערכה, ייעוד ואסמכה של גופי הערכת התאמה ולמעקב אחריהם.

על רשויות אלה להיות מאורגנת ומופעלת באופן המונע ניגודי עניינים ומבטיח אובייקטיביות וחוסר משוא פנים של פעילותן.

גופי הערכה אחראים לאמת את התאימות של מערכות בינה מלאכותית בסיכון גבוה.

כדי להיות מוכרים, על גופי הערכה להגיש בקשה לרשות האסמכה של המדינה שבה הם ממוקמים.

הבקשה חייבת להיות מלווה בתיאור פעילויות הערכת ההתאמה, מודול או המודולים של הערכת ההתאמה, וטכנולוגיות הבינה המלאכותית בהן גוף הערכת ההתאמה מעוניין לעסוק.

גופי הערכה אינם יכולים להיות תלויים בספק AI בסיכון גבוה שיש לו אינטרסים כלכליים במערכת הנבחנת כמו גם בכל מתחרה או ספק של מערכת כזו.

הנציבות תקצה מספר זיהוי לגופים מוכרים ותפרסם לציבור את רשימת הגופים והפעילויות אנתן הם זכאים לבחון.

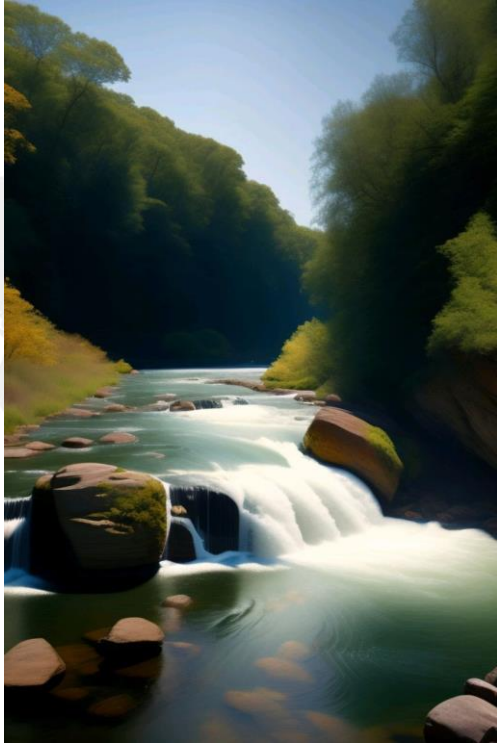
אם רשות ההערכה חושדת שגוף מסוים אינו עומד עוד בדרישות או בהתחייבויותיו, עליה לחקור את הנושא. בהתאם, הרשות יכולה להגביל, להשעות או לבטל את אישור הגוף.

הנציבות תחקור מקרים בהם יש סיבות לפקפק באם גוף אסמכה עומד בדרישות. אם ימצא שגוף כזה אינו עומד עוד בדרישות, היא תבקש מהמדינה הרלוונטית לנקוט באמצעים לתיקון הליקויים.

הנציבות תבטיח תיאום ושיתוף פעולה בין גופי האסמכה הפעילים בהליכי הערכת ההתאמה של מערכות בינה מלאכותית.

גופי הערכת התאמה שהוקמו על פי חוק של מדינה שלישית יכולים להיות מוסמכים לבצע את הפעילויות לפי תקנה 20 אם האיחוד יכרות הסכם עם גופים אלה.

פרק 7 - בין שיטת השימו לבין ההסמכה



בפרק הקודם דיברנו על גופי הערכת ההתאמה ותפקידם. היום נעסוק בדרך הארוכה והמפותלת הנדרשת על מנת לאשר מערכות בינה מלאכותית בסיכון גבוה.

אנו צולחים את הנהר המתפרס בין פסוקים 40 ל-50 של היצירה. חגורות הצלה הן ציוד חובה!

אם מערכת בסיכון גבוה עומדת בתקנים הרלוונטיים המוסכמים ברחבי האיחוד האירופי (מה שנקרא Harmonized Standards) ניתן להתייחס אליה כעומדת בתקנה זו.

אם אין תקנים מותאמים, או אם אלו הקיימים אינם מספיקים, הנציבות האירופית יכולה ליצור מפרטים חדשים. אם הספקים אינם פועלים לפי המפרטים הללו,

עליהם להסביר מדוע אינם עושים זאת ולהראות שהם משתמשים בפתרונות חלופיים המספקים מענה לפחות באותה רמה.

מערכות המוסמכות לדרישות הגנת הסייבר בהתאם לתקנה 2019/881 של הפרלמנט האירופי, והבקורות המיישמות הן בהלימה עם דרישות תקנה זו, יחשבו כעומדות בדרישות אבטחת הסייבר הכלולות בתקנה זו.

על למנת להעריך את רמת העמידה בדרישות ניתן לבצע בקרה פנימית ו/או תהליך הערכת ההתאמה תוך מעורבות של גוף הערכה מוסמך. מערכות בינה מלאכותית בסיכון גבוה יעברו הליך הערכת התאמה חדש בכל פעם שהן עוברות שינוי מהותי, ללא קשר לשאלה אם המערכת שהשתנתה מיועדת להפצה נוספת או ממשיכה לשמש את המשתמש הנוכחי.

תעודות הסמכה אשר יופקו על ידי הגופים המוסכמים יהיו תקפות לפרק זמן שלא יעלה על חמש שנים.

כאשר גוף הערכה ימצא שמערכת בינה מלאכותית אינה עומדת עוד בדרישות, הוא ישעה או יבטל את התעודה שהונפקה או יטיל עליה מגבלות מסוימות, בהתחשב בעקרון המידתיות. גוף הערכה יכול להטיל על הגוף המבוקר לתקן את הליקויים בפרק זמן סביר שחוגדר על ידו. המדינות החברות יבטיחו קיומו של הליך ערעור על החלטות של גוף הערכה.

גופי הערכה חייבים ליידע את הרשות המרכזית על החלטותיהם. יש לשתף מידע בין גופי הערכה השונים. במקרים חריגים, רשות לפיקוח שוק יכולה לאפשר שימוש במערכת בינה מלאכותית בסיכון גבוה במדינה חברה לזמן מוגבל בזמן שהליכי הערכת ההתאמה הדרושים מבוצעים.

על הספקים להכין הצהרה כתובה עבור כל מערכת AI המציינת שהיא עומדת בכללים הדרושים. עליהם לשמור הצהרה זו למשך 10 שנים לאחר יציאת המערכת לשוק ולמסור עותק לרשויות הלאומיות הרלוונטיות אם יתבקשו.

יש לסמן מערכת בינה מלאכותית בסיכון גבוה בסימן CE באופן גלוי, קריא וקבוע. אם זה לא אפשרי, ניתן לשים סימון זה על האריזה או על התיעוד הנלווה.

ספקים צריכים לשמור מסמכים מסוימים, כמו התיעוד הטכני והצהרת התאימות של האיחוד האירופי, למשך 10 שנים לאחר יציאת מערכת הבינה המלאכותית לשוק.

לפני שניתן להוציא לשוק מערכת AI בסיכון גבוה, על הספק או נציגו לרשום את המערכת במסד הנתונים של האיחוד האירופי. (בוקר טוב עולם, האם רישום מאגרי מידע חוזר לבמה? כאילו, למה???)

ספקים צריכים לוודא שמערכות בינה מלאכותית המיועדות לאינטראקציה עם אנשים, מיוצרות באופן שמאפשר להם לדעת שהם מדברים עם מערכת מסוג זה ולא עם בן אנוש משתמשים במערכות בינה מלאכותית היוצרות או משנות תוכן באופן שגורם לו להיראות אמיתי (Deep Fake) צריכים לציין באופן ברור כי התוכן נוצר או שונה באופן מלאכותי.

פרק 8 – רואים רחוק רואים שקוף

היום יש לנו יום קל - אנחנו סוקרים פסוק אחד ודי, ומספרו באירופה 52. מסיימים את הפסוק ומתפזרים לאוהלים למנוחת צהרים.

פסוק זה דן בחובות שקיפות עבור מערכות בינה מלאכותית.

על הספקים להבטיח שמערכות המיועדות לקיים אינטראקציה עם בני אנוש יתוכננו ויפותחו באופן שאלו יקבלו הודעה על כך שהם מקיימים אינטראקציה עם מערכת בינה מלאכותית, אלא אם כן הדבר ברור מהנסיבות ומהקשר השימוש.

יש לחשוף בפני משתמשים במערכת אשר מזהות רגשות או מערכת סיווג ביומטרית את פעולת המערכת.

מערכת בינה מלאכותית המייצרת או מבצעת מניפולציות של תוכן תמונה, אודיו או וידאו הדומה במידה ניכרת לאנשים קיימים, חפצים, מקומות, ישויות או אירועים אחרים, הנראים כאותנטיים ("Deep Fake") יחשפו בבירור את העובדה כי התוכן נוצר או נעשתה בו מניפולציה מלאכותית.

חובות השקיפות שצוינו לעיל לא יחולו על מערכות בינה מלאכותית אשר השימוש בהן מותר על פי חוק לאיתור, מניעה, חקירה והעמדה לדין של עבירות פליליות או שהוא הכרחי למימוש הזכות לחופש הביטוי והזכות לחופש האומנויות והמדעים המובטחת באמנת זכויות היסוד של האיחוד האירופי, ובכפוף להגנת הזכויות והחירויות של צדדים שלישיים.



פרק 9 – אל תשימו את הראש בחול

היום נבקר בפסוקים 53 ו 54 של היצירה.

פסוקים אלה עוסקים במה שמכונה "ארגז חול רגולטורי".

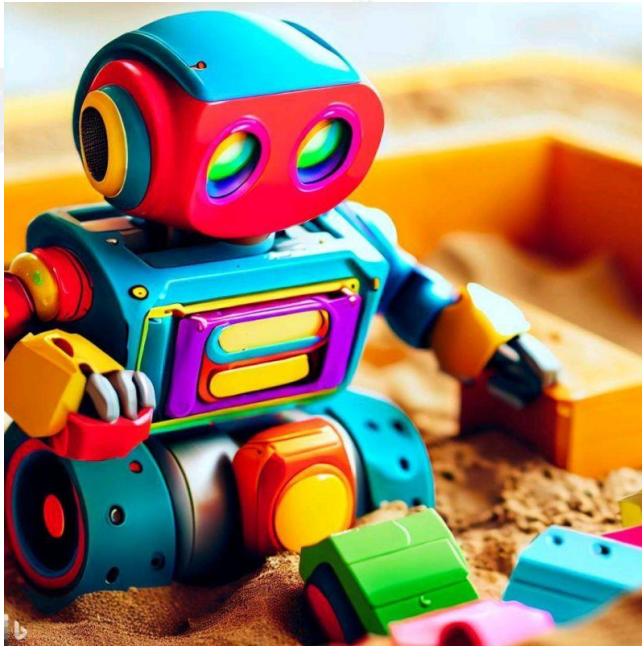
הרעיון בארגז חול שכזה הינו לספק סביבה מבוקרת המאפשרת את הפיתוח, הבדיקה והתיקוף של מערכות AI חדשניות לזמן מוגבל לפני יציאתן לשוק.

ארגזים כאלו יוקמו תחת פיקוח ישיר והנחיה של הרשויות המוסמכות במטרה להבטיח עמידה בדרישות תקנה זו, או חקיקה רלוונטית אחרת של האיחוד והמדינות החברות. ארגזי החול הרגולטוריים לא ישפיעו על סמכויות הפיקוח והתיקון של הרשויות המוסמכות.

כל סיכון משמעותי לבריאות ובטיחות ולזכויות יסוד שיוזחה במהלך הפיתוח והבדיקה של מערכות כאלה ידרוש תיקון מיידי, או, לחילופין, השעיית תהליך הפיתוח והבדיקה עד לביצוע תיקון כזה.

המשתתפים בארגז החול יישארו אחראים לכל נזק שייגרם לצדדים שלישיים כתוצאה מהניסוי. התירוץ "אבל זה עבד לי בחממה" לא יתפוס.

הרשויות יתאמו את פעילותן וישתפו פעולה במסגרת מועצת הבינה המלאכותית האירופית.



בארגז החול הרגולטורי יעובדו נתונים אישיים שנאספו כדין למטרות פיתוח ובדיקה של מערכות AI חדשניות בכפוף לתנאים הבאים:

- (א) המערכות יפותחו לשמירה על אינטרס ציבורי משמעותי באחד או יותר מהתחומים הבאים:
 - מניעה, חקירה, איתור או העמדה לדין בגין עבירות פליליות או ביצוע עונשים פליליים;
 - בטיחות ובריאות הציבור, לרבות מניעת מחלות, בקרה וטיפול;
 - רמה גבוהה של הגנה ושיפור איכות הסביבה;

(ב) הנתונים המעובדים נחוצים לצורך עמידה באחת או יותר מהדרישות הנזכרות בתקנות אלה, כאשר לא ניתן למלא אותן ביעילות על ידי עיבוד נתונים אנונימיים, סינתטיים או אחרים שאינם אישיים;

(ג) ישנם מנגנוני ניטור יעילים המאפשרים לזהות סיכונים גבוהים לזכויות היסוד של נושאי המידע בארגז החול וכן מנגנון תגובה המאפשר להפחית את הסיכון באופן מיידי, ובמידת הצורך, להפסיק את העיבוד;

(ד) כל הנתונים האישיים שיעובדו ימצאו בסביבת עיבוד נתונים נפרדת מבחינה תפקודית, מבודדת ומוגנת בשליטת המשתתפים אשר רק לאנשים מורשים תהיה גישה אליה;

(ה) הנתונים האישיים שיעובדו לא יתוקשרו "מחוץ לארגז" ולצדדים שלישיים לא תהיה כל יכולת לגשת אליהן;

(ו) כל עיבוד של נתונים אישיים בהקשר של ארגז החול לא יוביל לצעדים או להחלטות המשפיעות על נושאי המידע;

(ז) כל מידע אישי שיעובד בארגז החול ימחק לאחר שההשתתפות בו הסתיימה או שהנתונים האישיים הגיעו לסוף תקופת שמירתם;

(ח) יומני העיבוד של נתונים אישיים ישמרו בתקופת ההשתתפות בארגז החול ושנה אחת לאחר סיומו;

(ט) תיאור מלא ומפורט של התהליך והרציונל מאחורי ההדרכה, הבדיקה והתיקוף של מערכת הבינה המלאכותית ישמר יחד עם תוצאות הבדיקה;

(י) סיכום קצר של פרויקט הבינה המלאכותית שפותח בארגז החול, מטרותיו והתוצאות הצפויות יפורסמו באתר האינטרנט של הרשויות המוסמכות.

פרק 10 – מועצת גדולי הבינה



היום נדבר קצת על ממשל הבינה המלאכותית של הממלכה האירופית.

אנחנו סוקרים את הפסוקים 56 עד 58.

לכבוד החגיגה שלנו תוקם 'מועצה אירופאית לבינה מלאכותית'.

המועצה תספק ייעוץ וסיוע לנציבות על מנת:

(א) לתרום לשיתוף פעולה יעיל בין רשויות הפיקוח הלאומיות והנציבות האירופית בכל הנוגע לעניינים המכוסים בתקנה;

(ב) לתאם ולתרום להנחיה ולניתוח של הנציבות ורשויות הפיקוח הלאומיות וכן רשויות מוסמכות אחרות בנושאים המתעוררים ברחבי השוק הפנימי בהתייחס לעניינינו;

(ג) לסייע לרשויות הפיקוח הלאומיות ולנציבות בהבטחת יישום עקבי של תקנה זו.

המועצה תורכב מרשויות הפיקוח הלאומיות. רשויות לאומיות אחרות עשויות להיות מוזמנות לפגישות, כאשר הנושאים הנדונים רלוונטיים עבורן.

המועצה תקבע תקנון ברוב רגיל של חבריה. המועצה רשאית להקים תת-קבוצות בהתאם לצורך לחינת שאלות ספציפיות.

בראש הוועדה עומדת הנציבות האירופאית אשר תכנס את הישיבות ותכין את סדר היום.

המועצה רשאית להזמין מומחים ומשקיפים חיצוניים להשתתף בישיבותיה.

משימות המועצה כוללות:

(א) איסוף ושיתוף ידע ושיטות עבודה מומלצות בין המדינות החברות;

(ב) תרומה לפרקטיקות אדמיניסטרטיביות אחידות במדינות החברות, לרבות לתפקודן של ארגזי חול רגולטוריים עליהם דיברנו בפרק הקודם;

(ג) פרסום חוות דעת, המלצות ופרסומים בנושאים הקשורים ליישום תקנה זו, בפרט:

• על מפרטים טכניים או תקנים קיימים בנוגע לדרישות המפורטות בתקנה;

• על השימוש בתקנים מותאמים או מפרטים משותפים;

• הכנת מסמכים מנחים, לרבות ההנחיות בדבר קביעת קנסות מנהליים.

פרק 11 – כולם ביחד וכל אחד לחוד



הסיפור שלנו היום נסוב מסביב לתפקידן של כל אחת מהמדינות החברות (BFF) בממלכת הבינה האירופאית.

בואו נבקר בפסוק 59. שלום פסוק. מישהו בבית?

כל אחת מן המדינות החברות תמנה רשויות לאומיות מוסמכות במטרה להבטיח את יישומה תקנה זו.

רשויות אלה יקפידו לשמור על אובייקטיביות וחוסר משוא פנים בפעילותן ומשימותיהן.

כל מדינה תמנה רשות פיקוח לאומית שתהיה אחראית על הערכת התאימות ולפיקוח על השוק.

המדינות החברות יבטיחו שלרשויות המוסמכות יסופקו משאבים כספיים ואנושיים נאותים למילוי משימותיהן.

בפרט יש לוודא כי יהיה להם כוח אדם זמין ומקצועי

האנשים המופלאים הללו נדרשים לכישורים ומומחיות הכוללת הבנה מעמיקה של טכנולוגיות בינה מלאכותית, מערכות מידע, זכויות יסוד, סיכונים בריאות ובטיחות וידע מקיף בנושא תקנים רלוונטיים ובעולם המשפטי.

(היכן ישנם עוד אנשים עם כל הכישורים האלה יחדיו? לאירופאים פתרונים).

המדינות החברות ידווחו לנציבות על בסיס שנתי על מצב המשאבים הכספיים והאנושיים שלהן כולל הערכה של נאותותם.

הנציבות תעשה הכול כדי לשתף ידע וניסיון בין הרשויות המוסמכות הלאומיות.

הרשויות הלאומיות המוסמכות רשאיות לספק הנחיות וייעוץ לגבי יישום תקנה זו, לרבות לספקים בקנה מידה קטן.

במידת העניין וההקשר, הרשויות יתייעצו עם הקולגות שלהן ברשויות מקבילות, לפי העניין.

משפט אחרון מעניין מאוד.

עד כמה הגנת המידע (יענו פרטיות) קשורה לבינה מלאכותית אחראית?

תראו מי מולךךךך.

כאשר מוסדות, סוכנויות וגופים שונים של האיחוד עוסקים באותן סוגיות הקשורות לתקנה זו, המפקח האירופי להגנת המידע ישמש כרשות המוסמכת לפיקוח עליהם.

פרק 12 – תרשום תרשום!

אנו מבקרים היום בפסוק 60.

דָּזָה-וּ! מאיפה זה מוכר לנו? אה... רישום מאגרי מידע. לא אמרנו שזה עולם הולך ונעלם?
האירופאים אוהבים לטייל בנופי בראשית.

אז ככה.

הנציבות, בשיתוף המדינות החברות, תקים ותתחזק מסד נתונים המכיל מידע לגבי מערכות בינה מלאכותית
בסיכון גבוה.

הנתונים יוכנסו למסד הנתונים על ידי הספקים.

המידע שירשם יהיה נגיש לציבור.

מסד הנתונים יכיל נתונים אישיים רק במידה הנדרשת בהתאם לתקנה זו.

מידע זה יכלול את השמות ופרטי ההתקשרות של אנשים טבעיים שאחראים על רישום המערכת ובעלי הסמכות
החוקית לייצג את הספק.

הנציבות תהיה אחראית על מסד הנתונים הזה. כמו כן, היא תבטיח לספקים תמיכה טכנית ואדמיניסטרטיבית
נאותה.



פרק 13 – ניטור גדול לבינה



אנו מבקרים היום בפסוקים 61 ו-62 העוסקים בניטור ובקרה של מערכות בינה מלאכותית בסיכון גבוה לאחר יציאתן לשוק.

פסוק 61 דורש מהספקים להקים ולתעד מערכת ניטור לאחר היציאה לשוק בהתאם לאופי טכנולוגיות הבינה המלאכותית ולסיכונים של מערכת הבינה המלאכותית בסיכון גבוה.

התיעוד של מערכת זה יהיה חלק מהתיעוד הטכני הנדרש.

על מערכת זו לאסוף, לתעד ולנתח באופן פעיל ושיטתי נתונים רלוונטיים אשר יסופקו על ידי משתמשים או שיאספו באמצעות מקורות אחרים בנושא הביצועים של מערכות בסיכון גבוה לאורך כל חייהן, ויאפשרו לספק להעריך את התאימות המתמשכת של מערכות AI עם הדרישות המפורטות ב-AIA.

אין, בשלב זה, פירוט כלשהו כיצד תראה תכנית ניטור זו, אך הכתוב מתחייב כי הנציבות האירופית תפרסם הוראות מפורטות אשר יקבעו תבנית לתוכנית הניטור שלאחר היציאה לשוק.

פסוק 62 מדבר על תוכנית ניטור אירועים.

ספקים של מערכות בינה מלאכותית בסיכון גבוה המוצבות בשוק האיחוד ידווחו על כל תקרית חמורה או כל תקלה במערכות אלו המהווה הפרה של חובות על פי דיני האיחוד שנועדו להגן על זכויות יסוד לרשויות פיקוח השוק של המדינות החברות שבהן אותו אירוע התרחש.

הודעה כזו תיעשה מיד לאחר שהספק יקבע קשר סיבתי בין מערכת הבינה המלאכותית לבין האירוע או התקלה או אם יהיה סביר להניח כי קיים קשר כזה.

בכל מקרה, יש להודיע לא יאוחר מ-15 ימים לאחר שנודע לספקים על אירוע חמור או תקלה.

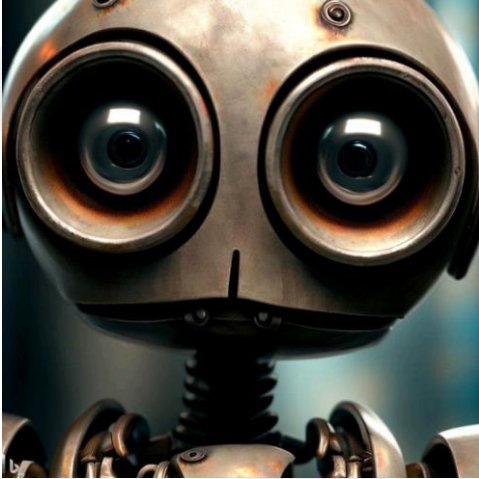
עם קבלת ההודעה הקשורה להפרת חובות על פי דיני האיחוד שנועדו להגן על זכויות יסוד, רשות פיקוח השוק תודיע על כך לרשויות הציבוריות הלאומיות וגופים רלוונטיים אחרים.

גם כאן ההנחיות כלליות לגמרי, תוך התחייבות כי הנציבות תפתח הנחיות ייעודיות כדי להקל על עמידה בהתחייבויות זו. הנחיה זו תינתן 12 חודשים לאחר כניסתה לתוקף של תקנה זו, לכל המאוחר.

עבור מערכות בינה מלאכותית בסיכון גבוה אשר מועלות לשוק או מופעלות על ידי ספקים שהם מוסדות אשראי ולמערכות AI בסיכון גבוה שהם רכיבי בטיחות של מכשירים, או שהם עצמם מכשירים, ההודעה על תקריות חמורות או תקלות תוגבל לאלו המהווים הפרה של חובות לפי דיני האיחוד אשר נועדו להגן על זכויות יסוד.

פרק 14 – כולם ביחד וכל אחד לחוד

היעד שלנו היום הוא טיפוס אתגרי למרומי הפסוקים 63 ו-64.



פסוק 63 מתייחס לתקנה (EU 2019/1020) של הפרלמנט האירופי. אז נתחיל את הסיור שלנו היום בפניית פרסה וסיכום של התקנה ההיא.

ובכן, תקנה 2019/1020 נועדה להבטיח שהמוצרים הזמינים בשוק תואמים לחקיקת ההרמוניה הרלוונטית של האיחוד, ושמוצרים שאינם עומדים בדרישות יתגלו ויוצאו מהשוק או שהצבתם בשוק תהיה אסורה.

התקנה קובעת כללים ונהלים לשיתוף פעולה בין רשויות פיקוח שוק, הנציבות וגופים רלוונטיים נוספים. היא כוללת הוראות לטיפול במוצרים המהווים סיכון חמור, מימון פעילות מעקב שוק ועונשים על אי ציות.

אפשר להסתובב, אנחנו חוזרים לפסוק שלנו.

הפסוק מכיר בתקנה האמורה וקובע כי כל התייחסות למוצר לפי תקנה זו תובן ככוללת את כל מערכות הבינה המלאכותית הנופלות בגדר תקנה זו.

רשות הפיקוח הלאומית תדווח לנציבות על בסיס קבוע על התוצאות של פעילויות פיקוח שוק רלוונטיות.

רשות הפיקוח הלאומית תדווח, ללא דיחוי, לנציבות ולרשויות התחרות הלאומיות הרלוונטיות על כל מידע שזוהה במהלך פעילויות פיקוח שוק שעשוי להיות בעל עניין פוטנציאלי להחלת דיני האיחוד על כללי תחרות.

לגבי מערכות בינה מלאכותית בסיכון גבוה הקשורות למוצרים אשר נופלים במסגרת של רגולטורים שונים, רשות פיקוח השוק למטרות תקנה זו תהיה הרגולטור הרלוונטי.

המדינות החברות יקלו על התיאום בין רשויות פיקוח השוק המוזכרות במסגרת תקנה זו לבין רשויות או גופים לאומיים רלוונטיים אחרים המפקחים העשויה להיות רלוונטית עבור מערכות בינה מלאכותית בסיכון גבוה.

יעלה ויבוא פסוק 64 העוסק בגישה למידע ותייעוד.

במידת הצורך, על מנת לאפשר הערכה של התאמת מערכת הבינה המלאכותית בסיכון גבוה לדרישות ועל פי בקשה מנומקת, תינתן לרשויות פיקוח השוק גישה לקוד המקור של מערכת הבינה המלאכותית.

לרשויות או גופים ציבוריים לאומיים המפקחים או אוכפים את החובות בהקשר לשימוש במערכות בינה מלאכותית בסיכון גבוה, תהיה הסמכות לבקש ולגשת לכל תיעוד שנוצר או נשמר לפי תקנה זו.

תוך 3 חודשים לאחר כניסתה לתוקף של תקנה זו, כל מדינה חברה תזהה את הרשויות הציבוריות או הגופים ותפרסם רשימה זמינה לציבור באתר האינטרנט של רשות הפיקוח הלאומית.

כאשר התיעוד לא יספיק כדי לוודא אם התרחשה הפרת חובות על פי דיני האיחוד שנועדה להגן על זכויות יסוד, הרשות רשאית להגיש בקשה מנומקת לרשות לפיקוח על השוק במטרה לארגן בדיקות של מערכת הבינה המלאכותית בסיכון גבוה באמצעים טכניים.

רשות פיקוח השוק תארגן את הבדיקה תוך מעורבות צמודה של הרשות הציבורית או הגוף המבקש תוך זמן סביר לאחר הבקשה.

כל מידע ותייעוד שהושגו על ידי הגופים שנזערו לעיל בהתאם להוראות סעיף זה יטופלו בהתאם לחובות הסודיות המפורטות בסעיף 70 (אליו עוד נגיע ביום מן הימים).

פרק 15 - איך מגרשים את הזאב הרע?



היום נבקר בפסוק 65 של היצירה העוסק בטיפול במערכות בינה מלאכותיות המהוות סיכון ברמה הלאומית.

כאשר לרשות פיקוח השוק של מדינה חברה סיבה טובה לחשוב כי מערכת בינה מלאכותית מהווה סיכון ברמה הלאומית, היא תבצע הערכה לגבי עמידתה בכל הדרישות המופיעות בתקנה זו.

כאשר מדובר בסיכונים לפגיעה בזכויות יסוד, תעדכן בכך רשות הפיקוח גם את הרשויות הציבוריות הלאומיות או הגופים הרלוונטיים.

כאשר רשות פיקוח השוק תמצא שמערכת אינה עומדת בדרישות הקבועות בתקנה זו, היא תדרוש מהמפעיל הרלוונטי לנקוט ללא דיחוי בכל פעולות התיקון המתאימות כדי לתקן את הליקוי.

אם רשות פיקוח השוק סבורה שאי-הציות אינו מוגבל לשטחה הלאומי, היא תודיע על כך לנציבות ולשאר המדינות החברות תוך פירוט הפעולות שהיא דרשה מהמפעיל לנקוט.

המפעיל יבטיח שכל הפעולות המתקנות המתאימות יינקטו תוך פרק זמן שיקבע.

אם המפעיל לא ינקוט בפעולה מתקנת בתוך התקופה האמורה, רשות פיקוח השוק תנקוט בכל האמצעים המתאימים כדי לאסור או להגביל את הצגת מערכת הבינה המלאכותית בשוק הלאומי שלה, או למשוך אותו מן השוק.

רשות זו תודיע לנציבות ולשאר המדינות החברות, ללא דיחוי, על אמצעים אלה.

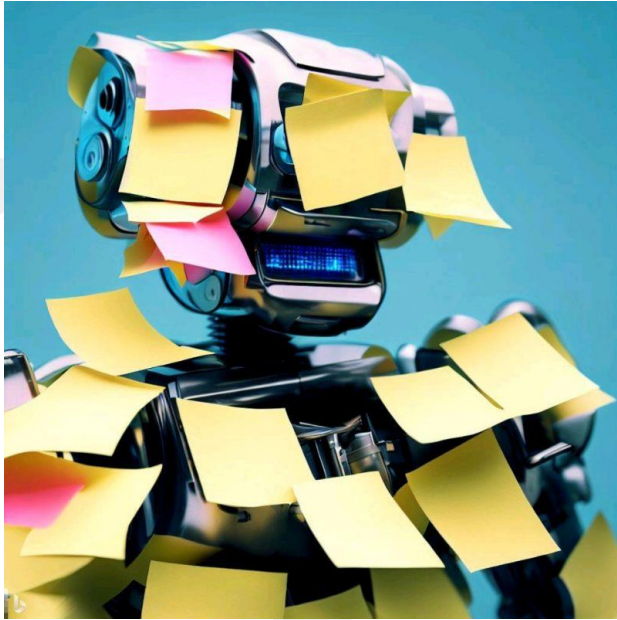
המידע יכלול את כל הפרטים הרלוונטיים, בפרט את הנתונים הדרושים לזיהוי מערכת הבינה המלאכותית שאינה תואמת, מקור המערכת, אופי אי ההתאמה והסיכון, טיב ומשך האמצעים הלאומיים שנקטו והטיעונים שהעלה המפעיל הרלוונטי.

בפרט, רשויות פיקוח השוק יצינו אם אי הציות נובע מכשל של מערכת הבינה המלאכותית לעמוד בדרישות החוק או בשל ליקויים בתקנים המותאמים או במפרטים המשותפים.

אם תוך שלושה חודשים מיום קבלת המידע האמור לא הועלתה התנגדות מצד מדינה חברה או מן הנציבות לגבי צעד זמני שנקט על ידי מדינה חברה, ייחשב אמצעי זה כמוצדק.

רשויות פיקוח השוק של כל המדינות החברות יודאו כי ינקטו, ללא דיחוי, הצעדים המתאימים לגבי המוצר הנוגע בדבר, כגון ביטול המוצר מהשוק שלהן.

פרק 16 - על פתקים ושאר ירקות



היעד שלנו היום הוא צליחת ים האדמיניסטרציה המתגלה בפנינו בפסוקים 66 עד 68 של היצירה.

בפרק הקודם אמרנו כי יתקיים תיאום בין המדינות השונות בנושא החלטות לגבי צעדים הננקטים בשל חוסר התאמה משמעותית העלולה להשפיע על כלל האיחוד.

לכל המדינות זכות להגות בהם יומם ולילה במשך שלושה חודשים.

אם במהלך תקופה זו מועלות התנגדויות על ידי מדינה חברה נגד צעד שננקט על ידי מדינה אחרת, או כאשר הנציבות חושבת כי הצעד מנוגד לדיני האיחוד, תקיים הנציבות התייעצות עם המדינה הרלוונטית והמפעיל או המפעילים ותעריך את הצעד שננקט.

על בסיס אותה הערכה תחליט הנציבות אם הצעד מוצדק או לא ותודיע על החלטתה למדינה הנוגעת בדבר.

אם יוחלט שזה לא זה, תבטל המדינה את הצעד בו נקטה.

אחרת, כל המדינות יישרו קו וקדימה צעד.

כאשר רשות פיקוח השוק של מדינה מוצאת כי למרות שהמערכת עומדת בתקנה, היא מהווה סיכון לבריאותם או בטיחותם של אנשים, או פגיעה בזכויות יסוד או אינטרסים ציבוריים, היא תדרוש מהמפעיל להבטיח שבטרם תצא לשוק הליקוי יתוקן

ואם לא? אז זהו שהמערכת תיעצר בעודה באיבה.

הספק או מפעילים רלוונטיים אחרים יוודאו שננקטת פעולות מתקנות לגבי כל המערכות הנוגעות בדבר בטרם יהיו זמינות לשוק ברחבי האיחוד, וזאת בתוך פרק הזמן שנקבע על ידי רשות פיקוח השוק של המדינה.

המדינה תודיע על כך מיד לנציבות ולשאר המדינות החברות. בפרט יצוין המידע הדרוש לזיהוי המערכת הרלוונטית, המקור ושרשרת האספקה שלה, אופי הסיכון ואופי ומשך האמצעים הלאומיים שננקטו.

הנציבות תכונס ללא דיחוי להתייעצות עם המדינות החברות והמפעיל הרלוונטי ותעריך את האמצעים הלאומיים שננקטו. על בסיס זה תחליט הנציבות אם הצעד מוצדק או לא, ובמידת הצורך, תציע אמצעים מתאימים.

כאשר רשות פיקוח השוק של מדינה חברה קובעת את אחד מהממצאים הבאים, היא תדרוש מהספק הרלוונטי לשים קץ לאי הציות הנוגע בדבר:

(תראו איפה הדגש - על הצמדת הפתקאות).

(א) סימון ההתאמה הוצמד למערכת ללא הצדקה;

(ב) סימון ההתאמה לא הוצמד למערכת;

(ג) הצהרת ההתאמה של האיחוד האירופי לא נערכה;

(ד) הצהרת התאימות הנדרשת לא נוסחה כהלכה;

(ה) מספר הזיהוי של הגוף המודיע, המעורב בהליך הערכת ההתאמה, אם רלוונטי, לא הוצמד למערכת;

כאשר אי ההתאמה הנזכרת נמשכת, המדינה הנוגעת בדבר תנקוט בכל האמצעים כדי להגביל או לאסור את הצגת מערכת הבינה המלאכותית בסיכון גבוה לשוק או תבטיח שהיא תוסר מהשוק, אם כבר הגיעה לשם.

פרק 17 – נא להתנהג בהתאם

היום נדבר על קודי התנהגות (Codes of conduct) בהתאם לפסוק 69 של היצירה.

רעיון קודי ההתנהגות מופיע כבר בגדפ"ר והנה הוא מציץ לנו גם כאן.

לא ראיתי את הנושא תופס יותר מידי תנופה בגדפרינו. אולי הפעם...

קודי התנהגות יפותחו במטרה לטפח את היישום מרצון של דרישות התקנות במערכות בינה מלאכותיות שאינן בסיכון גבוה.

הם יכתבו על בסיס מפרטים טכניים ופתרונות המהווים אמצעים מתאימים להבטחת עמידה בדרישות התקנות בהתאם למטרה המיועדת של המערכות.

קודים אלה יפרטו בין היתר דרישות הקשורות לקיימות סביבתית, נגישות לאנשים עם מוגבלות, השתתפות בעלי עניין בתכנון ובפיתוח של מערכות AI על בסיס יעדים ברורים ומדדי ביצוע מוגדרים אשר יוודאו השגת יעדים אלו.

קודי התנהגות יכולים להיערך על ידי ספקים בודדים של מערכות בינה מלאכותית או על ידי ארגונים המייצגים אותם או גם וגם.

הם יכולים לכסות מערכת AI אחת או יותר תוך התחשבות בקווי הדמיון של המטרה המיועדת של המערכות הרלוונטיות.

הנציבות והמועצה ייקחו בחשבון את האינטרסים והצרכים הספציפיים של הספקים והסטרטאפים בקנה מידה קטן כאשר הם מעודדים ומקלים על הכנת קודי התנהגות.



פרק 18 - שומרים על השומרים

היום נדבר על שמירת הסודיות של המידע בהתאם לפסוק 70.

אבל לא מדובר על שמירת הסודיות של מפתחי או משתמשי המערכות. מדובר על שומרי הסף.

רשויות לאומיות מוסמכות וגופי הסמכה המעורבים ביישום תקנה זו יכבדו את סודיות המידע והנתונים שהושגו תוך ביצוע משימותיהם ופעילויותיהם.

הן יגנו על זכויות קניין רוחני, מידע עסקי סודי או סודות מסחריים או משפטיים, לרבות קוד מקור, מידע שנאסף לצורך בדיקות, חקירות או ביקורת.

כך גם על אינטרסים של ביטחון ציבורי ולאומי והגנה על שלמותם ששל הליכים פליליים או מנהליים.

מידע סודי המועבר בין הרשויות הלאומיות המוסמכות לא ייחשף ללא התייעצות מוקדמת.

כאשר רשויות אכיפת החוק, ההגירה או המקלט הן ספקיות של מערכות בינה מלאכותית בסיכון גבוה, התייעוד הטכני יישאר ברשויות הרלוונטיות.

רשויות פיקוח השוק יוכלו, לפי בקשה, לגשת לתייעוד או לקבל עותק ממנו.

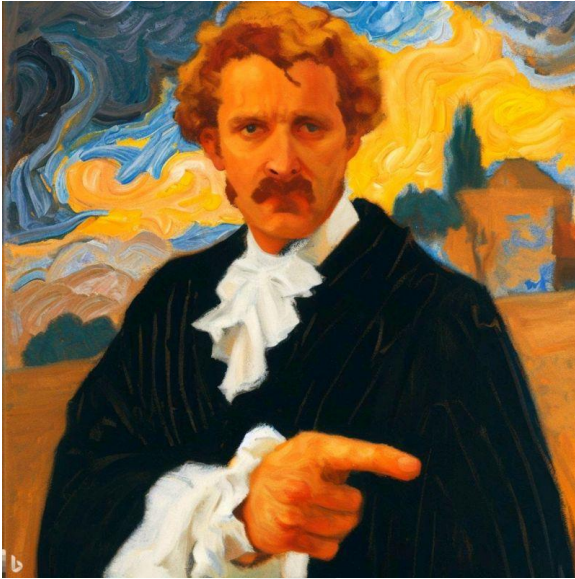
רק צוות של רשות פיקוח השוק המחזיק ברמת הסיווג הביטחוני המתאימה יורשה לגשת לתייעוד הזה או לכל עותק שלו.

האמור לא ישפיע על הזכויות והחובות של הנציבות, המדינות החברות והגופים המסמיכים בכל הנוגע לחילופי מידע והפצת אזהרות וגם לא על החובות של הצדדים הנוגעים בדבר למסור מידע לפי החוק הפלילי של המדינות החברות.

הנציבות והמדינות החברות רשאיות לשתף מידע סודי, במידת הצורך, עם רשויות רגולטוריות של מדינות שליטיות עמן סיכמו הסדרי סודיות דו-צדדיים או רב-צדדיים המבטיחים רמת סודיות נאותה.



פרק 19 – שכר ועונש



פסוק 71 מפרט כיצד יקבעו העונשים שיוטלו על מי שיפר את התקנות.

הפסוק מותיר חופש מסוים בידי המדינות החברות לקביעת הכללים בדבר העונשים אשר יוטלו על הפרות של תקנה זו אך קובע גבולות גזרה.

העונשים יהיו יעילים, מידתיים ומרתיעים. הם ייקחו בחשבון את האינטרסים של ספקים וסטרטאפים בקנה מידה קטן וכדאיותם הכלכלית.

המדינות החברות יודיעו לנציבות על כללים ועל אמצעים אלה ויעדכנו אותה, ללא דיחוי, על כל תיקון שישיפע עליהם.

ההפרות הבאות יהיו כפופות לקנסות מנהליים של עד 30,000,000 אירו או, אם העבריין הוא חברה, עד 6% מסך המחזור השנתי שלה ברחבי העולם לשנת הכספים הקודמת, לפי הגבוה מבניהם:

(א) אי ציות לאיסור של שיטות בינה מלאכותית שאין לעשות בהן שימוש;

(ב) אי עמידה של מערכת בינה מלאכותית בסיכון גבוה בדרישות התקנות.

אי-עמידתה של מערכת בינה מלאכותית בדרישות, מלבד אלו שהוזכרו לעיל, תהיה כפופה לקנסות מנהליים של עד 20,000,000 אירו או, אם העבריין הוא החברה, עד 4% מסך המחזור השנתי שלה ברחבי העולם לשנת הכספים הקודמת, הגבוה מבניהם.

אספקת מידע שגוי, חלקי או מטעה לגופי הסמכה ולרשויות לאומיות תהיה כפופה לקנסות מנהליים של עד 10,000,000 אירו או, אם העבריין הוא חברה, עד 2% מסך כל מחזור שנתי ברחבי העולם לשנת הכספים הקודמת, הגבוה מבניהם.

ההחלטה על גובה הקנס המנהלי תתקבל בכל מקרה לגופו, תוך שקלול כל הנסיבות הרלוונטיות ותשומת לב ראויה לנקודות הבאות:

(א) מהות, חומרתה ומשך ההפרה ושל תוצאותיה;

(ב) האם כבר הוטלו קנסות מנהליים על ידי רשויות פיקוח שוק אחרות על אותו מפעיל בגין אותה הפרה;

(ג) גודלו ונתח השוק של המפעיל המבצע את ההפרה.

כל מדינה חברה תקבע כללים האם ובאיזו מידה ניתן להטיל קנסות מנהליים על רשויות ציבוריות וגופים שהוקמה באותה מדינה חברה.

בהתאם למערכת המשפטית של המדינות החברות, ניתן להחיל את הכללים בדבר קנסות מנהליים באופן שהקנסות יוטלו על ידי בתי משפט לאומיים מוסמכים או גופים אחרים לפי העניין באותן מדינות חברות.

פרק 20 - שכר ועונש מלהפך

ממש בפרק הקודם דיברנו על קנסות ומכות אשר יוטלו על אנשים פרטיים וחברות אשר לא יצייתו לתקנות.

פסוק 72 מדבר על קנסות מנהליים שיוטלו על מוסדות, סוכנויות וגופים רשמיים של האיחוד.

מעניין מי הגוף האחראי על האכיפה: מי אם לא המפקח על הגנת המידע, ידידנו משכבר הימים המוכר מעולם הגנת הפרטיות בהתאם ל GDPR.

המפקח האירופי על הגנת המידע רשאי להטיל קנסות מנהליים על מוסדות, סוכנויות וגופים של האיחוד הנופלים בתחומה של תקנה זו.

ההחלטה האם להטיל קנס מנהלי ועל גובהו תתקבל בכל מקרה לגופו, תוך התחשבות בניסיונות הרלוונטיים למצב הספציפי, ובפרט בדברים הבאים:

- (א) מהותה, חומרתה ומשכה של ההפרה ותוצאותיה;
- (ב) שיתוף הפעולה עם המפקח האירופי להגנת המידע על מנת לתקן את ההפרה;
- (ג) הפרות קודמות דומות על ידי המוסד, הסוכנות או הגוף של האיחוד.

ההפרות הבאות יהיו כפופות לקנסות מנהליים של עד 500,000 אירו:

- (א) שימוש בשיטות הבינה המלאכותית אסורות;
- (ב) אי עמידה של מערכת הבינה המלאכותית בסיכון גבוה דרישות שנקבעו.

הפרות אחרות יהיו כפופות לקנסות מנהליים של עד 250,000 אירו.

לפני קבלת החלטות בהתאם לסעיף זה, המפקח האירופי על הגנת המידע ייתן למוסד, לסוכנות או לגוף הזדמנות להשמיע את דבריו בנוגע להפרה.

זכויות ההגנה של הצדדים הנוגעים בדבר ינובדו במלואן בתהליך.

הם יהיו זכאים לקבל גישה לתיק של מפקח הגנת המידע האירופי, בכפוף לאינטרס הגליטימי של יחידים או חברות בהגנה על הנתונים האישיים או הסודות העסקיים שלהם.



פרק 21 - מה נשתנה

פסוק 73 מדבר על הזכות לעדכן או לשנות את החוק.

כפי שהזכרנו בתחילת המסע, לפני שצוללים לעמקי החוק, יש לפתוח בשאלה: כשאנחנו אומרים אינטליגנציה מלאכותית, למה אנחנו מתכוונים?

לחוק ה-AIA האירופי (Artificial Intelligence Act) חמישה נספחים המספקים תשובות לשאלה זו והבהרות על הנוסח העיקרי של החוק. זה כולל:

- ☆ נספח I המגדיר את המונחים המשמשים ב-AIA.
- ☆ נספח II המפרט את יישומי AI בסיון גבוה הכפופים לדרישות המחמירות ביותר של AIA.
- ☆ נספח III המפרט את יישומי AI בסיון נמוך הפטורים מרוב הדרישות של AIA.
- ☆ נספח IV המספק הנחיות לגבי הערכת סיכונים של יישומי בינה מלאכותית.
- ☆ נספח V המספק הנחיות לגבי תאימות של יישומי בינה מלאכותית ל-AIA.

על מנת לוודא כי נספחים אלה נשארים מעודכנים, לנציבות האירופית מוקנית הסמכות לעדכן אותם באמצעות חקיקת משנה בהתאם לתנאים הבאים:

☆ הזכות תוענק לתקופה בלתי מוגבלת מכניסת התקנה לתוקף.

☆ כל שינוי ניתן לביטול בכל עת על ידי הפרלמנט האירופי או על ידי המועצה.

☆ החלטת ביטול תכנס לתוקף ביום שלאחר פרסומה בכתב העת הרשמי של האיחוד האירופי או בתאריך מאוחר יותר המצוין בו. היא לא תשפיע על תוקפן של חקיקות משנה שכבר תקפות.

☆ היא תכנס לתוקף רק אם הפרלמנט האירופי או המועצה לא הביעו התנגדות בתוך שלושה חודשים מיום פרסומה.

☆ ניתן להאריך תקופה זו בשלושה חודשים ביוזמת הפרלמנט האירופי או המועצה.



פרק 22 – סוף סוף ההתחלה



פסוקים 75 עד 82 של היצירה מתייחסים לתיקונים בחוקים קודמים של האיחוד האירופי ומרחיבים אותם כך שיתאימו לתקנה זו. ברשותכם נדלג על פסוקים אלה.

נשארו לנו שלושה פסוקים להשלמת הפרויקט - פסוקים 83 עד 85.

פסוק 83 מדבר על מערכות בינה מלאכותית שכבר יצאו לשוק או הוכנסו לשימוש.

תקנה זו לא תחול על מערכות בינה מלאכותית שהן רכיבים של מערכות ז'בקנה מידה גדול אשר הוצאו לשוק עד 12 חודשים לאחר תאריך יישום התקנה זו אלא אם כן יעברו שינוי משמעותי בתכנון או המטרה לשמה הן מיועדות.

פסוק 84 מדבר על סקירה ובקרה של התקנה.

הנציבות תעריך את הצורך בתיקון רשימת המערכות בסיכון גבוה הנזכרות בנספח III אחת לשנה לאחר כניסתה לתוקף של תקנה זו.

עד שלוש שנים לאחר תאריך היישום של תקנה זו וכל ארבע שנים לאחר מכן, תגיש הנציבות דוח על ההערכה והסקירה של תקנה זו לפרלמנט האירופי ולמועצה. הדוחות יפורסמו ברבים.

דוחות אלה יקדישו תשומת לב מיוחדת לדברים הבאים:

(א) מצב המשאבים הכספיים והאנושיים של הרשויות הלאומיות המוסמכות על מנת לבצע ביעילות את המשימות שהוטלו עליהן לפי תקנה זו;

(ב) מצב העונשים, ובמיוחד קנסות מנהליים, המוחלים על ידי מדינות חברות על הפרות של הוראות תקנה זו.

בתוך שלוש שנים לאחר תאריך החלת תקנה זו וכל ארבע שנים לאחר מכן, הנציבות תעריך את ההשפעה והיעילות של קודי התנהגות כדי לטפח את היישום של הדרישות המפורטות.

בביצוע ההערכות והביקורות אלה הנציבות תתחשב בעמדות ובמצאים של המועצה, של הפרלמנט האירופי ושל גופים או מקורות רלוונטיים אחרים.

הוועדה תגיש, במידת הצורך, הצעות מתאימות לתיקון תקנה זו, במיוחד בהתחשב בהתפתחויות טכנולוגיות ולאור ההתקדמות בעולם המידע.

הגענו לפסוק אחרון אחרון חביב 85 - כניסת תוקף ויישום.

תקנה זו תיכנס לתוקף ביום העשרים לאחר פרסומה בכתב העת הרשמי של האיחוד האירופי.

תקנה זו תחול החל מ-24 חודשים לאחר כניסתה לתוקף.

בינה מלאכותית אחראית

מסע בעקבות חוק הבינה
המלאכותית האירופאי (AIA)

מהדורה ראשונה | יולי 2023

הפרופיל שלי ב-LinkedIn:
<https://www.linkedin.com/in/giladyaron/>

דף הבית של החברה:

www.data-protection-matters.com

קבוצה ב-LinkedIn הדנה בבינה מלאכותית אחראית:

<https://www.linkedin.com/groups/9383372/>

