

"אני מצטער דיב, אני חושש שאני לא יכול לעשות זאת" / עו"ד עדי מרכוס*

בסרט הקלאסי "2001: אודיסאה בחלל" (1968), טוענת בינה מלאכותית בשם האל כי "אף מחשב מסוג זה מעולם לא עשה טעות או סילף מידע. אנחנו תחת כל הגדרה – חסינים ולא יכולים לטעות", כמה דקות לפני שהיא מתחילה להביא למותם של האסטרונאוטים. ב"שליחות קטלנית" (1984), הבינה המלאכותית סקיינט מנהלת מלחמת חורמה נגד שארית האנושות בניסיון לחסל אותם. אולם, מה אם הייתה בידינו הדרך להבטיח שסקיינט לא תיוולד לעולם או שהאל לא תוצב לעולם על ספינת חלל? הרגולציה החדשה של האיחוד האירופי לעניין בינה מלאכותית לאו דווקא תציל את האנושות (ונודה, שאם כן אז זה יהיה סרט מדע בדיוני משעמם במיוחד), אולם היא שואפת, לפחות בבסיסה, לאפשר לעסקים לזהות בינה מלאכותית "מסוכנת" ולהגביל את יכולתה להתפתח ולנוע בשוק ללא פיקוח.

הרגולציה, אשר טיוטה שלה פורסמה עוד במאי 2024¹, ואשר נכנסה לתוקף לבסוף ב-01 אוגוסט, 2024, שואפת ליצור גבולות אתיים ושקיפות בנושא השימוש בבינה מלאכותית ולהחיל את הגבולות כאמור בצורה אחידה בכל העולם, כפי שרגולציות הפרטיות של האיחוד (GDPR) השפיעה על כלל העולם. כך, הרגולציה מוחלת לא רק על כל עסק בתחום הבינה המלאכותית באיחוד אלא גם על כל עסק בעולם, המשווק או מפעיל את מוצריו הכוללים בינה מלאכותית, ברחבי האיחוד.

הרגולציה נוקטת גישת "הערכת סיכונים" המסווגת את מערכות הבינה המלאכותית ל-4 דרגות סיכון: בלתי סביר, גבוה, מוגבל ומינימלי. במסגרת הסיווג כאמור, מערכות המאפשרות למפעיל לנצל בינה מלאכותית למטרות שאינן אתיות, למשל, מסווגות כסיכון בלתי סביר. כך, למשל, מערכות שבנויות כדי לנצל חולשות של אנשים כתוצאה מגיל או מגבלה פיזית, מערכות שמנצלות מידע ביומטרי לצורך קיטלוג לפי דת, גזע או מין או מערכות שאוספות תמונות מהאינטרנט או ממצלמות אבטחה למאגר שישמש לזיהוי פנים. פעולות אלה, המהוות רשימה סגורה, אסורות וחברה העומדת מאחורי מערכת כזו חשופה לקנסות של עד 35 מיליון יורו או 7% מרווחי החברה השנתיים, הגדול מביניהם.

לעומת זאת, סיווג בסיכון גבוה אינו מונע שימוש אך דורש רישום במאגר האיחוד האירופאי והצבת חסמים, מערכות ניהול סיכונים ופיקוח אנושי, שנועדו לפקח על המערכת ולוודא שלא תצא מכלל שליטה או תממש את הסיכון. במערכות בסיכון מוגבל ההגבלות והדרישות פחותות בהרבה ומרבית הדרישות נוגעות לשקיפות וגילוי נאות. במערכות בסיכון מינימלי, אשר נתפסות כמערכות בינה מלאכותית כלליות יותר המסוגלות למספר גדול של מטרות, החוק מתיר אותן לרוב ללא התייחסות ומשאיר אותן לחסות תחת חקיקה מקומית או אירופאית אחרת.

הבעיה היא כמובן שמערכות הבינה המלאכותית, מעצם הגדרתם, הן מערכות לומדות ומתפתחות. קיימת סבירות גבוהה שהרשימה הסגורה שמציגה הרגולציה לעניין מערכות בסיכון בלתי סביר תהא לוקה בחסר באופן משמעותי עוד מספר שנים כשהתפתחות טכנולוגית תאפשר ותציף בעיות אתיות מהותיות שהחוק אינו צופה. בנוסף, גם ההגדרה של מערכות בסיכון גבוה היא אמורפית ומקשה על חברות בסיווג נכון של המערכות המופעלות על ידם, מעבר לכך שלא תמיד ניתן לצפות מלכתחילה את הסיווג של המערכת המפותחת. כך יכולה חברה למצוא עצמה מפתחת מערכת בינה מלאכותית ומשקיעה כספים ומשאבים ניכרים, רק כדי לגלות בסוף הדרך שהמערכת שפותחה נופלת נחשבת בסיכון בלתי סביר (ולו רק בגלל שיכולה לבצע אילו מן הדברים המנויים ברגולציה, אפילו אם הוא משני למטרות המערכת) ועל כן לא יכולה לפעול או נדרשת להשקיע עוד כספים ומשאבים בהוספת חסמים והליכי בדיקה בשל הסיווג כמערכת סיכון גבוה.

החוק לא נועד לחול במלואו באופן מיידי ונותן לוח זמנים, הפרוס על פני 5-6 שנים, לתחולת החוק בשלבים. כך, למשל, דרישות השקיפות מיועדות ליישום בשנה הראשונה אולם דרישות אופרטיביות של פיקוח אנושי במערכות סיכון גבוה נדרשות ליישום רק תוך שנתיים ויותר. ועדיין, המדובר בלוח זמנים נוקשה ובהגדרות מסובכות ורגישות, המחייבות כל חברה בתחום לבצע במיידית בדיקה משפטית וטכנית מדוקדקת של הערכת סיכונים ותכנון עתידי על מנת לוודא עמידה בדרישות בבוא העת וחשוב שהדבר ייעשה בשיתוף עורכי דין בעלי הבנה של התחום הטכנולוגי ושל הרגולציה החדשה.

* עו"ד עדי מרכוס הינה עורכת דין במשרד אפיק ושות' (www.afiklaw.com) המתמקדת במשפט מסחרי ודיני חברות, זכויות יוצרים, דיני תקשורת ואומנים ועסקאות בינלאומיות. עו"ד מרכוס הינה הפקולטה למשפטים ובעלת תואר שני בתקשורת באוניברסיטת תל אביב ותואר שני במנהל עסקים בינלאומי מאוניברסיטת בר אילן. היא התמחתה במשרד המשפטים אצל המשנה ליועץ המשפטי לממשלה בתחום הדין האזרחי וזכויות היוצרים, לאחר מכן עבדה כ-18 חודש במשרד שלמה כהן בתחום הקניין הרוחני, כ-11 שנה במחלקה המשפטית בגוף התקשורת "רשת נגה בע"מ" (ערוץ 2 של הטלוויזיה), כאשר תפקידה האחרון בטרם מיוזג החברה עם ערוץ 10, כראש תחום במחלקה המשפטית ולאחר כן, טרם הצטרפותה למשרד, כיועצת המשפטית הפנימית של קנלר ייצוג אמנים, בכל נושא היעוץ המשפטי של אמנים ואנשי תרבות, בין בישראל ובין במישור הבינלאומי. אין בסקירה כללית זו משום ייעוץ משפטי כלשהו ומומלץ להיוועץ בעורך דין המתמחה בתחום זה בטרם קבלת כל החלטה בנושאים המתוארים בסקירה זו. לפרטים נוספים: 03-6093609, או באמצעות הדואר האלקטרוני: afiklaw@afiklaw.com.

¹ <https://he.afiklaw.com/articles/a391>

I'm sorry Dave, I'm afraid I can't do that/Adi Marcus, Adv.*

In the classic film "2001: A Space Odyssey" (1968), Hal9000, the artificial intelligence system contends: "No 9000 computer has ever made a mistake or distorted information. We are all, by any practical definition of the words, foolproof and incapable of error", just before it goes on to systematically kill the astronauts. In "Terminator" (1984), the artificial intelligence Skynet wages a war of attrition against the remainder of humanity in an attempt to eliminate them. What if we had a way to ensure that Skynet would never be born or HAL would never be placed on a spaceship? The new European Union regulation regarding artificial intelligence will not necessarily save humanity (and we admit, if it did so, it would make for a particularly boring science fiction movie), but it aims, at least at its core, to allow businesses to identify "dangerous" AI and limit its ability to develop and move freely in the market without Supervision.

The regulation, a draft of which was published back in May, 2024¹, and which finally entered into force on August 1, 2024, aims to create ethical and transparent limits on the use of AI and to apply the aforementioned limits in a uniform manner throughout the world, as the EU's privacy regulation (GDPR) affected the entire world. Thus, the regulation is applied not only to every business operating in the field of AI in the EU, but also to every business in the world, which markets or operates products which include AI, throughout the EU.

The regulation takes a "risk assessment" approach that classifies AI systems into 4 levels of risk: unreasonable, high, limited and minimal. Within this classification, systems that allow the operator to utilize AI for non-ethical purposes, for example, are classified as an unreasonable risk. Thus, for example, systems built to usurp people's weaknesses as a result of age or physical limitations, systems that use biometric information to catalog people under religion, race or gender, or systems that collect images from the Internet or from security cameras to create a database that will be used for facial recognition. These actions, which constitute a closed list, are prohibited and the company behind such a system may be subject to fines of up to EUR 35 million or 7% of the company's annual profits, whichever is greater. Classification as a high-risk does not prevent use, but requires recording in the EU's database and placement of barriers, risk management systems and human supervision, all designed to monitor the system and ensure that it does not get out of control or realize the inherent risk. In limited risk systems, the restrictions and requirements are considerably less strict, mainly requiring transparency and disclosure. Minimal Risk systems, seen as more general AI systems capable of a large number of purposes, are left without reference and subjects them to other local or European legislation.

The issue is, of course, that AI systems, by their definition, are learning and evolving systems. There is a high probability that the unreasonable risk closed list will be significantly lacking in a few years when technological development will allow and flood essential ethical issues that the law does not anticipate. In addition, the definition is essentially amorphous, in a manner that may make it difficult for companies to correctly classify the systems operated by them. Moreover, the classification of the developed system cannot always be expected from the beginning. A company may find itself developing an AI system and investing considerable funds and resources only to find out at the end of the road that the developed system is now defined as of unreasonable risk (if only because it can perform some of the things listed in the regulation, even if secondary to the real system goals) and therefore cannot operate or is required to invest more funds and resources in adding barriers and inspection procedures due to the classification as a high risk system.

The law is not intended to fully apply immediately and sets a schedule of 5-6 years for the application. e.g., the transparency requirements are implemented in the first year, but operative requirements of human supervision for high risk systems received a two or more years grace. Nevertheless, this is a rigid schedule and complicated and sensitive definitions, which require every company in the field to promptly carry out a careful legal and technical review of risk assessment and appropriate future planning, in order to ensure compliance with the requirements when the time comes and it is vital that this be done in cooperation with lawyers who understand the field of technology and the new regulation.

*Adi Marcus, Adv. is an attorney in the office of Afik & Co. (www.afiklaw.com) who focuses primarily on commercial and corporate law, copyrights, media law and international transactions. Advocate Marcus holds a major in law, an M.A in communication from Tel Aviv University and an international MBA from Bar Ilan University. She completed her internship at the Ministry of justice under the Deputy Attorney General focusing civil law and copyright law, then worked for about 18 months in the office of Shlomo Cohen in the field of intellectual property, about 11 years in the legal department of the communications network "Noga Network" (Channel 2 of TV), with her last position before the company merged with Channel 10, was head of department in the legal department and then, before joining the firm, as Kneller Artists Representation's internal legal advisor, representing in all matters of legal advice to artists and cultural figures, both in Israel and internationally. Nothing herein should be treated as a legal advice and all issues must be reviewed on a case-by-case basis. For additional details: +972-3-6093609 or at the e-mail: afiklaw@afiklaw.com.

¹ <https://he.afiklaw.com/articles/a391>