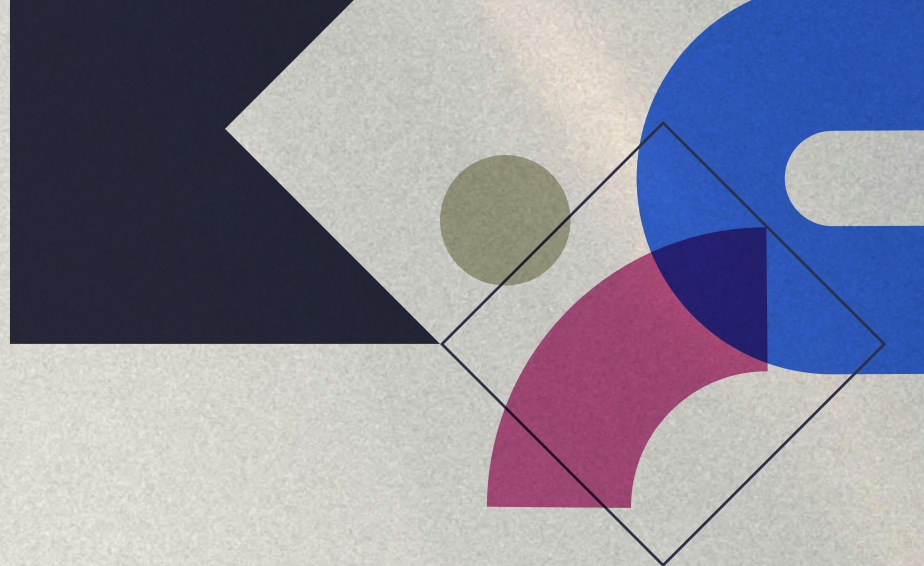




בינה מלאכותית בסקטור הפיננסי

דוח סופי



דצמבר 2025





תוכן עניינים

4	פתח דבר
7	תקציר מנהלים
21	חלק א' - רקע, התפתחויות ומגמות רגולטוריות
22	א. כניסתה של הבינה המלאכותית לחיינו
27	ב. רגולציה של בינה מלאכותית בארגונים בינלאומיים ובמדינות מפותחות
30	ג. העיסוק הממשלתי בישראל בבינה מלאכותית
32	ד. יישומי בינה מלאכותית בסקטור הפיננסי
34	ה. תועלות ואתגרים הנובעים משימוש בבינה מלאכותית
38	ו. הבינה המלאכותית ברגולציה פיננסית בעולם
41	ז. פעילות בינה מלאכותית בסקטור הפיננסי בישראל
42	ח. הצוות הבין-משרדי לבינה מלאכותית בסקטור הפיננסי
42	1. הרקע להקמת הצוות
43	2. עבודת הצוות
44	3. דוח הביניים
45	חלק ב' - גישה כללית, עקרונות מנחים לטיפול, והגדרת בינה מלאכותית בסקטור הפיננסי
46	א. הגישה הכללית – עידוד חדשנות והתמודדות עם סיכונים
47	ב. עקרונות מנחים לטיפול בבינה מלאכותית בסקטור הפיננסי
50	ג. הגדרת בינה מלאכותית
55	חלק ג' - סוגיות רוחב
57	"קופסה שחורה" והסברתיות
63	מעורבות אנושית
68	יידוע וגילוי
76	הזכות לפרטיות והגנה על מידע אישי
103	הטיה ואפליה
111	אחריות
120	ממשל בינה מלאכותית
130	"מחברים את הדברים" - ראייה כוללת ומבוססת סיכונים
135	יציבות פיננסית
139	תחרות
148	סיכונים תפעוליים ובהם סיכוני סייבר, סיכוני צד שלישי, הונאה ודיסאינפורמציה ("מידע כזב")



תוכן עניינים

157	חלק ד' – תחומים ספציפיים שנבחנו על-ידי הצוות
158	ייעוץ השקעות וניהול תיקים
176	אשראי במערכת הבנקאית
184	חיתום ביטוח
189	חלק ה' – פעולות נוספות לקידום רגולציה פיננסית בתחום הבינה המלאכותית
199	נספחים
200	נספח א' – כתב מינוי
202	נספח ב' – קול קורא
205	נספח ג' – רשימת הגורמים שהופיעו בפני הצוות
206	נספח ד' – ריכוז הערות הציבור לדוח הביניים
23	תיבה 1: בינה מלאכותית – מילון מונחים
74	תיבה 2: מהי אוריינות של בינה מלאכותית? וכיצד נוכל להשיגה במגזר הפיננסי?
138	תיבה 3: מהו Flash Crash כתוצאה מפעילות אלגוריתמית במסחר?
155	תיבה 4: עבירות במסחר בניירות ערך באמצעות בינה מלאכותית

פתח דבר

ההתפתחויות האחרונות בטכנולוגיות בינה מלאכותית מעוררות עניין חסר תקדים, על רקע הפוטנציאל שלהן לחולל מהפכה בחיינו. במיוחד היכולות החדשות של בינה מלאכותית יוצרת (Generative AI) ומודלי שפה גדולים (Large Language Models), כפי שנחשפו לציבור הרחב מסוף שנת 2022 והתחזיות בדבר הבינה המלאכותית הכללית (General Purpose AI), הובילו להכרה בהשפעה יוצאת הדופן שעשויה להיות לבינה מלאכותית כבר בעתיד הקרוב. השימוש ביישומי בינה מלאכותית התרחב, המחקר וההשקעות בתחום הבינה המלאכותית גדלו מאוד, וכך גם הניסיונות המעשיים להטמיע בינה מלאכותית בפעילויות עסקיות רבות ומגוונות. השיח ביחס לפוטנציאל ולסיכונים הנובעים מההתקדמות בתחום הבינה המלאכותית והאסדרה המתאימה נמצא כעת בראש סדר היום העולמי.

בעולמות הפיננסיים השימוש בבינה מלאכותית אינו חדש, אולם ההתפתחויות הטכנולוגיות מעוררות ציפייה כי בינה מלאכותית, במובנה הרחב והמתקדם, תשולב עם הזמן באופן משמעותי יותר במגוון שימושים אפשריים. כך למשל, יישומים של בינה מלאכותית עשויים לשמש בפעולות ליבה בתהליכי קבלת ההחלטות בתחומי האשראי, הביטוח וההשקעה, בממשקי עבודה מול לקוחות ומשקיעים (כגון בירור צרכי הלקוח, התאמת מוצרים, וטיפול בבקשות), ובייעול תהליכים פנימיים כגון ניהול סיכונים ומניעת הונאות.

ככל שההבטחה הגלומה בהתקדמות הבינה מלאכותית אכן תתממש, היא עשויה להניב יתרונות רבים מאוד לציבור הרחב, ובהם שיפור ניכר באיכות המוצרים והשירותים הפיננסיים, הוזלת עלויות, הגברת תחרות והנגשת השירותים. בד בבד מעוררת כניסתה של הבינה המלאכותית אתגרים וסיכונים שונים, בהם אתגרים חדשים וייחודיים כגון האתגר בהבנת אופן פעולת מערכות בינה מלאכותית ותוצריהן, ואתגרים קיימים העשויים להשתנות ולהתעצם עם שילובן של מערכות אלה, כגון סיכוני אפליה או מניפולציה.

הצוות הבין-משרדי לבחינת השימוש בבינה מלאכותית בסקטור הפיננסי הוקם על מנת להתמודד באופן ראשוני עם הפוטנציאל והאתגרים האמורים. בצוות חברו יחד נציגי משרדי המשפטים והאוצר, הפיקוח על הבנקים, רשות שוק ההון, ביטוח וחיסכון, רשות ניירות ערך ורשות התחרות, לעבודה משותפת, על בסיס תפישה כי נדרש מאמץ מיוחד ומערכתי לצורך לימוד התופעה והיערכות אליה.

עבודת הצוות באה בהמשך לעיסוק הממשלתי בנושא בינה מלאכותית בישראל. עיסוק זה כלל בין היתר את החלטת ממשלה 212 משנת 2021 והחלטת ממשלה 173 משנת 2023, אשר עסקו בגיבוש תכנית לאומית בנוגע לבינה מלאכותית; מסמך מדיניות של משרד החדשנות, המדע והטכנולוגיה ומשרד המשפטים משנת 2023, אשר הציג אסטרטגיה רגולטורית לעיסוק בבינה מלאכותית; דוח של משרד המשפטים וקבוצת חוקרים מאוניברסיטת תל-אביב, אשר עסק ביישומי בינה מלאכותית בסקטור הפיננסי. בפרט אפשר לראות בעבודת הצוות המשך ישיר להמלצות שנכללו במסמך המדיניות הממשלתי, ולפיהן הרגולציה בתחום הבינה המלאכותית תיעשה על בסיס ענפי (להבדיל מרגולציה רוחבית), תעמוד בהלימה לרגולציה הנוהגת במדינות מובילות בעולם, ותהא גמישה ורכה על מנת לאפשר את התקדמות הטכנולוגיה. עבודת הצוות בנוגע לענף הפיננסיים מיישמת תפישה זו.

עבודת הצוות כללה למידה של הטכנולוגיה שבבסיס יישומי בינה מלאכותית, הבנת היישומים של הטכנולוגיה בתחום הפיננסי, ניתוח של ההיבטים המשפטיים והרגולטורים של בינה מלאכותית, שיתוף ידע רגולטורי, פרסום קול קורא ומפגשים עם גורמים רבים מהתעשייה, האקדמיה, הממשל, כמו גם רגולטורים וארגונים זרים העוסקים בקביעת מדיניות בתחום.

הגישה הכללית שהנחתה את הצוות דוגלת בעידוד פעילות בינה מלאכותית בסקטור הפיננסי, לצד קביעת רגולציה מותאמת מקום בו הדבר נדרש. אמנם כניסתה של הבינה המלאכותית לשימוש צפויה להציב אתגרים מורכבים, ולמעשה דוח זה עוסק ברובו בדרכי ההתמודדות עם אתגרים אלה. אולם זאת מתוך גישה כי ניתן ויש לתת לאתגרים אלה מענה הולם על מנת לעודד חדשנות במגזר הפיננסי. האסדרה בתחום הפיננסי, לצד התאמות שיעשו בה במשך הזמן, מאפשרים לדעתנו לנקוט בגישה המעודדת חדשנות ושילוב של הטכנולוגיה, תוך שמירת יעדי הפיקוח הפיננסי ובהם הגנת הציבור והמערכת בכללותה.

עמדה כללית נוספת הבאה לידי ביטוי בדוח, ועולה בקנה אחד עם מסמך המדיניות הממשלתי, היא כי בשלב זה רצוי לנקוט בכלי אסדרה רכים וגמישים ביחס לבינה מלאכותית. כל עיסוק רגולטורי בנושא הבינה המלאכותית בסקטור הפיננסי בעת הנוכחית מגלם מתח בין כוחות מנוגדים: הרצון לעודד חדשנות ולממש את הפוטנציאל שיש בטכנולוגיה להשפיע על הפעילות הפיננסית למול החשש מסיכונים גלומים באימוצה; הצורך באסדרה למול

השינויים הטכנולוגיים המהירים המקשים על עיצוב רגולציה מותאמת; העניין הרב שיש ביישומי בינה מלאכותית, למול קצב האימוץ ההדרגתי שלה בסקטור הפיננסי, בעולם ובישראל.

מבט השוואתי מלמד כי ברוב המדינות לא נקבעה רגולציה ייעודית העוסקת בבינה מלאכותית בסקטור הפיננסי, והן ממשיכות בבחינת הנושא תוך יישום והבהרת הרגולציה הקיימת. רושם זה עלול להטעות, הואיל וישנן מדינות, ובראשן מדינות האיחוד האירופאי, בהן אומצה אסדרה רוחבית בנוגע לבינה מלאכותית, אשר תחול גם ביחס לפעילות פיננסית. כמו-כן, במדינות רבות רגולטורים פיננסיים מבצעים בחינה של הנושא וכן פרסמו עמדות בנוגע לתחולת הדין הקיים על בינה מלאכותית.

בהתאם לכך, גם המלצות הצוות עוסקות בניתוח הסוגיות המרכזיות בתחום הפיננסי בכלל וכן בשימושים ספציפיים, בקביעת קווי מדיניות ובהצגת פעולות נדרשות להמשך, להבדיל מניסוח של המלצות לאסדרה קשיחה כבר עתה.

בהינתן קצב ההתפתחות של הטכנולוגיה והעיסוק הנרחב בה, יהיה מקום להמשיך ולעדכן באופן שוטף את התפישה והכלים הרגולטוריים. כך למשל נוכח הצוות כיצד מסמכי מדיניות ומחקרים שנכתבו בנושא בינה מלאכותית לפני זמן לא רב, הפכו פחות רלוונטיים עם ההתפתחויות המהירות של מודלי שפה ובינה מלאכותית כללית. כמו כן, יש להניח כי הרגולטורים יצברו ידע בנושא עם התקדמות היכולות והשימושים בפועל. יש לראות אם כן בדוח זה נקודת פתיחה בלבד לעיסוק בנושא.

מה כולל הדוח?

חלק א' של הדוח פורש את הרקע להקמת הצוות וכן רקע, התפתחויות ומגמות רגולטוריות הנוגעות לבינה מלאכותית בכלל, ולסקטור הפיננסי בפרט. בין היתר יוצגו בקצרה העיסוק הממשלתי עד כה בנושא בינה מלאכותית, ויזמות רגולטוריות במדינות שונות ברחבי העולם, תוך התמקדות בסקטור הפיננסי.

בחלק ב' של הדוח יפורטו הגישה הכללית והעקרונות שלדעת הצוות צריכים להנחות בהתמודדות עם אתגרי הבינה המלאכותית בסקטור הפיננסי. עקרונות אלה כוללים לדוגמה התבססות על אסדרה מבוססת סיכונים, ניטרליות טכנולוגית, ושאפה לאחידות אסדרתית ביחס לשירותים וסיכונים דומים, ועוד. בנוסף לכך נדון בחלק זה בהגדרת בינה מלאכותית, על חשיבותה ומורכבותה.

בחלק ג' של הדוח יפורטו בהרחבה סוגיות רוחביות המתעוררות כתוצאה משימוש ביישומי בינה מלאכותית והמלצות הצוות בקשר עם אותן סוגיות. בין היתר נעסוק בחלק זה בסוגיות הנובעות ממאפיינים ייחודיים של בינה מלאכותית – כגון סוגיית "הקופסה השחורה" והסברתיות וסוגיית המעורבות האנושית; בסוגיות המעוררות שאלות ביחס לדין הכללי החל על גופים מפוקחים בתחום הפיננסי – בהיבטי אפליה ופרטיות; ובמישורים של ממשל בינה מלאכותית וניהול סיכונים במסגרתם נציג כלים להתמודדות משולבת עם כלל האתגרים האמורים. בהמשך לכך נדון בסוגיות הנוגעות לשוק בכללותו, קרי באתגרים המתעצמים לנוכח כניסתה של הבינה המלאכותית בהיבטי תחרות, יציבות פיננסית, וסיכוני הונאה, סייבר ודיסאינפורמציה. בנוגע לכל אחת מהסוגיות נציג את השאלות המתעוררות כתוצאה מכניסתה של בינה מלאכותית לתמונה, העיסוק בהן בחו"ל, חלופות אפשריות לטיפול, והמלצות.

חלק ד' של הדוח יעסוק בשלושה תחומי פעילות ספציפיים שהוגדרו לבחינת הצוות: ייעוץ השקעות וניהול תיקים, אשראי וחיתום ביטוח. לגבי תחומים אלה מציג כל אחד מהרגולטורים הפיננסיים את האופן בו הוא רואה שימושים אפשריים ליישומי בינה מלאכותית בתחום שתחת פיקוחו, מהי המסגרת הרגולטורית הרלוונטית, סוגיות לטיפול, והמלצות ראשוניות.

בחלק ה' של הדוח יוצגו פעולות נוספות לטיפול בבינה מלאכותית במסגרת רגולציה פיננסית. נעסוק למשל בהמלצות בנוגע לכלים לעידוד כניסה של הטכנולוגיה וליצירת ודאות רגולטורית, ובשימוש בבינה מלאכותית על-ידי הרגולטורים עצמם.

הדוח כולל המלצות רבות בתחומים השונים, כבסיס לבחינה ומתוך הבנה שההמלצות יאומצו בהתאם להתפתחות הטכנולוגיה ואופן הטמעתה, ובהתאם למאפייני הגופים והמוצרים הפיננסיים המפוקחים על ידי כל אחד מהרגולטורים. הצוות מבקש להודות לחברי ועדת ההיגוי, על זיהוי הצורך, ההכוונה המקצועית והתמיכה בעבודת הצוות:

עו"ד מאיר לוין, לשעבר המשנה ליועצת המשפטית לממשלה (ייעוץ וחקיקה – משפט כלכלי); מר עמית גל, ראש רשות שוק ההון, ביטוח וחיסכון; עו"ד ספי זינגר, יו"ר רשות ניירות ערך (וגב' ענת גואטה, לשעבר יו"ר רשות ניירות ערך); מר דני אחיאשווילי, המפקח על הבנקים (ומר יאיר אבידן, לשעבר המפקח על הבנקים); עו"ד מיכל כהן, הממונה על התחרות; עו"ד אסי מסינג, לשעבר יועמ"ש משרד האוצר.



הצוות מבקש להודות לשותפות ולשותפים אשר לקחו חלק בכתיבת הדוח ועל תרומתם לעבודת הצוות ולדוח: עו"ד אוראל שריקי בן-צבי ועו"ד ירון חפר מייעוץ וחקיקה (כלכלי); עו"ד לירון מאוטנר-לוגסי ועו"ד שירה גרטנברג מייעוץ וחקיקה (ציבורי-חוקתי) בין היתר על כתיבת הפרק בנושא פרטיות, ועו"ד אריאל אלקיים ועו"ד ענבל קליין על תרומתן לפרק זה; גב' יעל רגב מרשות שוק ההון, ביטוח וחיסכון; גב' דנה גרטי מהפיקוח על הבנקים, בנק ישראל.

עוד מבקש הצוות להודות למי שנטלו חלק פעיל ותרמו רבות לישיבות הצוות ועל תרומתם המשמעותית לדוח: עו"ד רוני טלמור ועו"ד יאירה פרנקל מייעוץ וחקיקה (כלכלי); עו"ד יערה למברגר מייעוץ וחקיקה (אזרחי); עו"ד טובי האריס ועו"ד זהר בוצר מרשות התחרות; עו"ד קרן קורן בנדלק ועו"ד אור שטרנברג מרשות ניירות ערך; מר סער קרביץ, עו"ד יעל צוקרמן בלאו ועו"ד אביתר תורג'מן מרשות שוק ההון, ביטוח וחיסכון; מר אדי אזולאי, מר אליעזר שיינפלד, עו"ד חן פליישר, ד"ר אנה ברודסקי ועו"ד רונן ניסים מבנק ישראל.

הצוות מבקש להודות גם למי שסייע בעבודת הצוות והעיר הערות טובות ומועילות לדוח: עו"ד ד"ר יובל רויטמן, עו"ד לירון נעים, עו"ד ישראל מדין, עו"ד עידית מועלם, וגב' הדו סופר מייעוץ וחקיקה (כלכלי), ועו"ד חמוטל דרקסלר; סדריק (יהודה) צבע מייעוץ וחקיקה (משפט בין-לאומי); עו"ד הילה דבידוביץ, ועו"ד ליאת לנדאו מייעוץ וחקיקה (אזרחי); לעו"ד איל זנדברג ועו"ד ליאת בן-מאיר מייעוץ וחקיקה (ציבורי-חוקתי); גב' ענבל פולק, מר אלחנן הרמור, גב' אורלי בלום ועו"ד יעל וייס מרשות ניירות ערך; מר דודי בבלי, ד"ר איתמר כספי מבנק ישראל; גב' רעות פנחס, ומר בוריס קליימן מרשות שוק ההון, ביטוח וחיסכון; לעו"ד ראובן אידלמן ועו"ד ניר גרסון מרשות הגנת הפרטיות; עו"ד יוסף גדליהו ממשרד החדשנות, המדע והטכנולוגיה; לד"ר זיו קציר, מרשות החדשנות; ולעו"ד שובל גפני.

הצוות גם מבקש להודות לפרופ' אסף חמדני, פרופ' קובי קסטיאל, פרופ' דן עמירם וד"ר ארי אחיעז מאוניברסיטת תל אביב על הדוח האקדמי שהיווה התשתית להקמת הצוות ועל הייעוץ המקצועי והסיוע במהלך כתיבת הדוח.

כמו כן, הצוות מבקש להודות לגורמים הרבים, מהתעשייה, האקדמיה, החברה האזרחית, וגופי הרגולציה, מהארץ ומהעולם, אשר הופיעו בפני הצוות והגיבו לקול הקורא שפורסם על תרומה משמעותית וחשובה שסייעה לצוות להיכנס לעובי הקורה ולגבש את המלצותיו.

על החתום, חברי הצוות:

- עו"ד אמיר וסרמן • רשות ניירות ערך • ראש הצוות (במשותף)
- עו"ד שרית פלבר • משרד המשפטים, ייעוץ וחקיקה (כלכלי) • ראשת הצוות (במשותף)
- עו"ד תום גולדריין • רשות ניירות ערך • מרכז הצוות
- גב' אילנית מדמוני • בנק ישראל (הפיקוח על הבנקים)
- עו"ד דוד קופל • משרד האוצר
- גב' אביבה וייס • רשות שוק ההון, ביטוח וחיסכון
- עו"ד איל שפירא • רשות התחרות

תקציר מנהלים

א. תועלות, סיכונים ותמונת מצב בנוגע לבניה מלאכותית בסקטור הפיננסי

ההתפתחויות המהירות בטכנולוגיית בינה מלאכותית הרחיבו והאיצו את העיסוק ברגולציה אפשרית בעניינה. לצד הערכות כי השימוש בבינה מלאכותית צפוי לגרום מהפכה של ממש בתחומי חיים רבים, לרבות בתחום הפיננסיים, אשר צפויים להיות לה יתרונות משמעותיים, גברו גם החששות מפני כניסתה של הטכנולוגיה החדשה.

תועלות פוטנציאליות עיקריות כתוצאה משילובה של בינה מלאכותית לסקטור הפיננסי עשויות להיות יעול הפעילות והפחתת עלויות, שיפור איכות המוצרים והשירותים, קידום הכלה ונגישות פיננסית, ושיפור בהיבטי ציות.

האתגרים העיקריים מכניסתה של בינה מלאכותית לסקטור הפיננסי כוללים אתגרים רוחביים, שאינם ייחודיים לסקטור הפיננסי בלבד, כגון בעיה של "קופסה שחורה" והסברתיות, הצורך במעורבות אנושית, מתן גילוי אפקטיבי על הפעילות, הגנה על פרטיות המידע, ומניעת אפליה והטיות בפעילות המערכת. בנוסף לכך ישנם אתגרים ייחודיים לסקטור הפיננסי כגון סיכוני יציבות פיננסית, סיכוני סייבר, הונאה ודיסאינפורמציה, וסיכון לפגיעה בתחרות בתחום.

העיסוק ברגולציה על בינה מלאכותית מעמיד לפני קובעי המדיניות מספר שאלות מפתח הנוגעות בין היתר לעיתוי הנכון להשית רגולציה שתחול על טכנולוגיה של בינה מלאכותית, לאופי ולעוצמת הרגולציה, ולבחירה אם רגולציה בנדון צריכה להשתלב ברגולציה קיימת בתחומי חיים שונים או שנדרשת רגולציה ייעודית.

בעולם מתפתחות גישות שונות ביחס להיבטים אלה – החל מהאיחוד האירופאי בו לאחרונה החלה להיכנס לתוקף חקיקה מקיפה שתסדיר את הפיתוח, ההפעלה והשימוש בבינה מלאכותית (ה-EU AI Act), ועד מדינות כמו ארה"ב ובריטניה, בהן לא נקבעה חקיקה רוחבית ומחייבת, אלא אומצה גישה רכה יותר, המבכרת עידוד של הפעילות תוך מתן גמישות לרגולטורים בתחומי פעילות שונים לפעול בהתאם לסמכויות הקיימות שלהם.

בישראל, הגישה שהוצגה במסמך המדיניות הממשלתי, היא כי האסדרה של תחום הבינה המלאכותית תיעשה באופן ענפי (להבדיל מרגולציה רוחבית שתשתרע על טכנולוגיית בינה מלאכותית באשר היא), תוך אימוץ רגולציה רכה והדרגתית בשלב זה, מקום בו היא נדרשת.

תמונת המצב הכללית לגבי אימוץ יישומי בינה מלאכותית בסקטור הפיננסי בישראל, תואמת ממצאים ממדינות אחרות בעולם, לפיהם הטכנולוגיה מעוררת עניין רב, אולם קצב האימוץ הוא איטי ומבוזר. ואולם, הערכת השחקנים בתחום היא כי בינה מלאכותית תתפוס תפקיד הולך וגדל בפעילויות הפיננסיות, והיא מקבלת ביטוי בהשקעת תשומות הולכות וגדלות בבחינת יישומים אפשריים והטמעתם.

בעבודתו ובהמלצותיו הביא הצוות בחשבון את המדיניות הממשלתית הכללית בנוגע לרגולציה על בינה מלאכותית, את קצב האימוץ של הטכנולוגיה בסקטור הפיננסי בשלב זה, את הצורך במדיניות זהירה שלא תייצר חסמים, ואת העובדה שבעולם אין לרוב רגולציה קשיחה וספציפית שנקבעה ביחס לבינה מלאכותית בסקטור הפיננסי. לנוכח אלה הצוות התמקד בניתוח הסוגיות המרכזיות, בקביעת קווי מדיניות ובהצגת פעולות נדרשות להמשך, להבדיל מניסוח של המלצות לאסדרה קשיחה כבר עתה. יהיה מקום להמשיך ולעדכן באופן שוטף את התפישה האמורה והכלים הרגולטוריים בהתאם להתפתחויות. דוח זה מהווה אם כן נקודת פתיחה בלבד לעיסוק בנושא.

ב. עקרונות מנחים לטיפול בבינה מלאכותית בסקטור הפיננסי

הגישה הכללית המוצעת על-ידי הצוות היא עידוד החדשנות לשם מימוש התועלות הגלומות בבינה מלאכותית, תוך התמודדות עם הסיכונים. מבלי לגרוע מהחששות הרבים שהוצגו בעולם ביחס להשלכותיה של טכנולוגיית הבינה המלאכותית, הצוות סבור כי בסקטור הפיננסי אפשר לתת מענה הולם לסיכונים אלה, בהינתן שהתחום נמצא תחת פיקוח הדוק באופן יחסי. זאת ועוד, הצוות בדעה כי שילובה של בינה מלאכותית בתחום הפיננסי הוא כמעט בלתי נמנע, וכי יכולות להיות לכך פוטנציאל גדול לשפר את השירותים הפיננסיים לצרכן, להוזיל אותם, ולהגביר את התחרות בתחום.

בדוח מפורטים תשעה עקרונות מנחים באשר לאופי ולאופן האסדרה הרצוי של בינה מלאכותית בסקטור הפיננסי:

- אסדרה גמישה ואדפטיבית
- התאמת האסדרה למקובל בעולם

- **עידוד חדשנות ושילוב הטכנולוגיה**, בין השאר באמצעות הסרת חסמים המפריעים להתפתחות השוק
- עידוד השימוש בכלים רגולטוריים המאפשרים **התנסות ולמידה**
- נקיטת **אסדרה רק מקום בו מתקיימות נסיבות המצדיקות זאת** (להבדיל מברירת מחדל לפיה שימוש בבינה מלאכותית בהכרח מחייב שינוי אסדרתי)
- אימוץ גישה של **אסדרה מבוססת סיכונים**
- התחשבות ב**שיקולים צרכניים וחברתיים** באסדרה של הפעילות
- חתירה ל**אחידות אסדרתית** ביחס לשירותים וסיכונים דומים
- **ניטרליות טכנולוגית** – אסדרה הנגזרת מאופי הפעילות ללא תלות בטכנולוגיה אלא אם כן זו מצדיקה התמודדות מיוחדת

ג. הגדרת בינה מלאכותית

עצם הגדרתה של בינה מלאכותית הוא סוגיה מורכבת, ואפשר לראות בעולם קשת של ניסיונות להגדיר מהי בינה מלאכותית. בענייננו תכליתה של ההגדרה היא רגולטורית, נועדה לצרכים של אסדרה ופיקוח, ועל כן יש לה חשיבות מעשית.

בישראל לא נקבעה הגדרה מחייבת בדין לבינה מלאכותית. הדוח כולל ניתוח של הקשיים המרכזיים בקביעת הגדרה לבינה מלאכותית, בחינה של דוגמאות להגדרות שניתנו בעולם, ודיון בסוגיות שונות בנוגע להגדרה: האם יש מקום להתייחס בהגדרה לטכנולוגיות מסוימות? האם יש מקום להתייחס למטרות השימוש או לתוצרי הפעולה של הבינה המלאכותית? האם וכיצד ניתן להבחין בין מערכות בינה מלאכותית ובין מערכות ממוחשבות "רגילות"?

ההגדרה המוצעת על-ידי הצוות לבינה מלאכותית בסקטור הפיננסי מבוססת בין היתר על הגדרות ה-OECD והאיחוד האירופאי, בהתאמות המתבקשות לפעילות בסקטור זה:

"מערכת בינה מלאכותית" – מערכת מבוססת מחשב, הפועלת בדרגות שונות של אוטונומיה, במטרה להפיק תוצרים כגון תוכן, תחזיות, המלצות או החלטות, אשר עשויה להיות לה השפעה על משקיעים, לקוחות, או על פעילותו של הגוף המפוקח.

לצד הגדרה בסיסית זו, ניתן יהיה לקבוע הגדרות נוספות באופן מודולרי, על מנת לתת מענה לקשיים של תחולת יתר ותחולת חסר. כך אפשר יהיה לקבוע הגדרה שתכלול רכיב מהותיות, הגדרה של בינה מלאכותית שמתאפיינת בלמידת מכונה, והגדרה של מערכת בינה מלאכותית יוצרת או בינה מלאכותית כללית.

בהקשר זה, מוצע כי בהתאם להנחיות הרגולטור, גוף פיננסי יוכל להחליט כי מערכת מבוססת מחשב אינה מהווה, על פי מהותה, מערכת בינה מלאכותית. שיקול דעת זה יוכל לאפשר התמודדות עם מצבים בהם ניכר שהמערכת המדוברת אינה מערכת בינה מלאכותית, אף שההגדרה עשויה לחול עליה מבחינה פורמלית.

ד. סוגיות הנוגעות לשילוב מערכות בינה מלאכותית בגופים פיננסיים

כניסתה של הבינה המלאכותית מעוררת אתגרים הנובעים בין היתר ממאפיינים ייחודיים של הטכנולוגיה, כגון סוגיית הקופסה השחורה, מכך שיישומי הטכנולוגיה עוד בראשיתם ובשללות הטכנולוגיה היא מוגבלת, ומכך שהמרחב האסדרתי הקיים מתמקד בשיקול דעת אנושי ואינו מותאם לקבלת החלטות אלגוריתמית. במסגרת בחינת סוגיות אלה כולל הדוח גבולות גזרה מוצעים לגבי הפעילות וכלים שמטרתם להבטיח שימוש בטוח ואחראי במערכות בינה מלאכותית בפיננסיים. ההכוונה בחלק זה של הדוח מיועדת הן לגופים מפוקחים המבקשים להפעיל מערכות בינה מלאכותית הן לרגולטורים העתידים לפקח על פעילות זו.

"קופסה שחורה" והסברתיות

המונח "**הסברתיות**" מתייחס ליכולת לספק הסבר, היגיון או הצדקה לתוצר (פלט) אליו הגיעה מערכת הבינה המלאכותית. ההתמקדות בצורך "להסביר" את פעילותה ותוצריה של מערכת הבינה המלאכותית נובע מכך שמערכות אלה, במובן המתקדם, מאופיינות כ"**קופסה שחורה**". כלומר, בכך שבין השאר, בשל מורכבותן, היקף הנתונים שבבסיסן, והאופן שבו נערכים הקשרים בין הנתונים, לא ניתן להתחקות אחר האופן בו התקבלו תוצרי המערכת. הדוח מבחין בין **הסברתיות כללית**, המתייחסת ליכולת להבין את מאפייני המערכת ואופן פעולתה באופן

כללי (הסברתיות מסוג זה מכונה לעיתים במסמכים בינלאומיים גם כשקיפות), לבין **הסברתיות פרטנית** המתייחסת ליכולת לספק הסבר ביחס לאופן שבו התקבלה החלטה ספציפית.

יש הצדקות שונות לדרישה רגולטורית להסברתיות – כללית ופרטנית – כלפי גורמים שונים: הגוף הפיננסי עצמו, הרגולטור, הצרכן והציבור. הסברתיות משרתת אינטרסים רגולטוריים, צרכניים וחברתיים. כך לדוגמה, הסברתיות לגבי האופן בו מערכת בינה מלאכותית קיבלה החלטה בנוגע למתן אשראי לאדם, תאפשר למוסד הפיננסי העושה שימוש במערכת להפעיל בקרה עליה, תאפשר לרגולטור לוודא כי הגוף המפוקח עומד בדרישות הדיון, תאפשר לצרכן להבין מדוע התקבלה החלטה מסוימת בעניינו ולהשיג עליה במידת הצורך, ותאפשר גם ביקורת ציבורית על המערכת. עם זאת, דרישת הסברתיות עלולה להיתקל בקשיים הנובעים, בין השאר, ממידת בשלותה של הטכנולוגיה או מהחובה להגן על סודות מסחריים. דרישת הסברתיות גורפת, כלומר חובת הסברתיות פרטנית ביחס לכל החלטה והחלטה (או אף יכולת הסברתיות פרטנית), עלולה למנוע כניסתה של טכנולוגיית בינה מלאכותית מתקדמת.

לאחרונה, החלו מודלים גדולים במיוחד להציע מעין הסבר או רשימת מקורות עיקריים בתהליך קבלת ההחלטות שלהם, במטרה לספק למשתמשים יכולת להבין (אף אם לא באופן מלא) את התהליך שהתחולל במערכת בעת ייצור הפלט אותו קיבלו. יש בכך כדי לסייע בהבנת תהליך קבלת ההחלטות של המודל.

להלן עיקרי המלצות הצוות לגבי חובת הסברתיות:

- **אין להחיל חובת הסברתיות פרטנית בכל מקרה שבו מעורבת מערכת בינה מלאכותית.** שיקולים בקביעה כי תחול חובה כאמור הם קיומה של חובת הנמקה בדיון, מידת חשיבות ההחלטה עבור הפרט או המוסד הפיננסי (החלטות בסיכון גבוה), ומידת המעורבות של הבינה המלאכותית בקבלת ההחלטה.
- **חובת הסברתיות (כללית ופרטנית) צריכה להישקל ביחס למערכות בסיכון גבוה.** בהקשר זה יש לבחון את טיב ההחלטה ולהתמקד בהחלטות שמרעות עם הלקוח שכן ככלל אלה המקרים בהם לקוח יבקש ללמוד על ההחלטה או להשיג עליה (לדוגמה, דחיית בקשת אשראי להבדיל מקבלת בקשת אשראי). ככל שמערכת הבינה המלאכותית אינה מספקת רכיב מהותי בתהליך יצירת המלצה או ההחלטה, הרי שלא תידרש הסברתיות ביחס לאופן פעילותה.
- **גם מקום בו צריכה לחול על פניו דרישת הסברתיות פרטנית, יש מקום להכיר בחלופות "מפצות" לכך – כגון בקרה הדוקה של תוצאות המערכת או חלופות שירות המוצגות ללקוח חלף מערכת הבינה המלאכותית. בהינתן חלופות מפצות הולמות, לא תידרש הסברתיות פרטנית.**
- **במקרים מסוימים, ניתן להסתפק בהסברתיות פרטנית חלקית.** התפתחויות הטכנולוגיות בתחום מבקשות להשיג הסברתיות פרטנית (גם אם לא מלאה). הסבר חלקי זה עשוי להיות בעל ערך במקרים רבים להבנת ההיגיון או הרכיבים שהובילו לתוצר. מכאן, שהרגולטורים יוכלו לערוך התאמות ביכולות ההסברתיות הנדרשות בהתאם לנסיבות, ולהסתפק לעתים גם בהסברתיות פרטנית חלקית.
- **חובת הסברתיות פרטנית לא תידרש מקום בו הטכנולוגיה היא רק גורם מסייע לקבלת החלטה.**
- **יש חשיבות של גוף הפיננסי המפעיל מערכת בינה מלאכותית תהיה הבנה לגבי אופן פעילותה, מגבלותיה וכדומה.**

מעורבות אנושית

אחד הפתרונות הנפוצים המוצעים על מנת להתמודד עם האתגרים הגלומים בפעילות של בינה מלאכותית הוא מעורבות ופיקוח אנושי על קבלת החלטות אלגוריתמיות. מעורבות אנושית נתפשת כאמצעי אפשרי להתמודד עם תקלות וכשלים אפשריים של מערכת אלגוריתמית, בעיקר בשלב הנוכחי בו יש ספק לגבי יכולותיה לקבל החלטות מדויקות, תקינות ובטוחות. הצדקה מרכזית נוספת לדרישת המעורבות האנושית היא החשש מפני אובדן האוטונומיה של הפרט אשר "מאבד" שליטה על החלטות שמתקבלות לגביו, בין השאר, בשל חוסר היכולת לתקשר או להבין את הגורם שקיבל את ההחלטה וכן חוסר היכולת של המערכת לבחון מאפיינים בתוך הקשר כולל, ולשם כך יש מקום לקבוע חובה לספק חלופה הכוללת מעורבות אנושית במקרים מסוימים. לבסוף יש טענה לפיה פעילות של מערכות בינה מלאכותית בתחומים בהם נדרש רישיון מקצועי כגון ייעוץ השקעות או ייעוץ פנסיוני, עלולה להפר את הדיון ודרישות הרישיון ללא מעורבות אנושית, וכי בלעדיה לא ניתן יהיה לקיים תכליות כגון חובת נאמנות כלפי הפרט או הבטחת כשירות מסוימת.

לצד הצדקות אלה יש גם ביקורת על דרישת המעורבות האנושית. ביקורת אחת היא כי אין ודאות שמעורבות אנושית

אכן משפרת את תוצאות המערכת. ביקורת נוספת נוגעת לאי ודאות לגבי חלוקת האחריות בין האדם לבין מערכת קבלת ההחלטות. לבסוף עולה חשש כי דרישת מעורבות אנושית תבטל או תצמצם את היתרונות שיש בשילוב מערכות אוטומטיות.

להלן עיקרי המלצות הצוות לגבי דרישת מעורבות אנושית:

- מעורבות אנושית יכולה להתקיים בזמן אמת או בדיעבד (למשל, באמצעות בחינת השגה). **מעורבות אנושית "בזמן אמת" תידרש רק בהחלטות מהותיות לפרט אשר הסיכון בהן גבוה, בתנאי שהטכנולוגיה משמעותית בקבלת ההחלטה, ובהיעדר חלופות מפתות.** זאת, כדי להימנע מדרישה גורפת שיש בצידה עלויות וחסמים. השיקולים שהוצגו לעיל בנוגע להסברתיות – החלטות חיוביות לעומת החלטות שליליות, מערכות תומכות החלטה לעומת מערכות מקבלות החלטה – נכונים גם לשאלת המעורבות האנושית. ביחס להחלטות אחרות, ניתן לשקול שהמעורבות האנושית תידרש בשלבי השגה או בחינה, למשל. המלצה זו רלוונטית גם בהקשרים של בינה מלאכותית יוצרת, למשל, כאשר ישנן אינטראקציות משמעותיות עם שירות לקוחות.
- **דרישת המעורבות האנושית תישקל בהתחשב במערכת הדרישות הרגולטוריות הנוספות החלות על המערכת.** גם החלטות בסיכון גבוה עשויות שלא לחייב מעורבות אנושית מקום בו קיימות חלופות מפתות הולמות.
- **במערכות בינה מלאכותית התומכות בקבלת החלטות אנושית (להבדיל ממערכות המקבלות החלטות באופן עצמאי ואוטומטי), ניתן לצמצם את דרישות המעורבות האנושית על החלטות ספציפיות ולהתמקד בבקרה על פעילות המערכת ותוצאותיה,** זאת נוכח העובדה שממילא גורם אנושי מקבל את ההחלטה.
- **אין להטיל חובה גורפת של העמדת פעילות אנושית לצד פעילות הנעשית בידי מערכות בינה מלאכותית.** יחד עם זאת, ככל שישנה אפשרות לקבל החלטה או שירות אנושיים, יש להביא זאת לידיעת הלקוח על מנת שיבחר האם הוא מעוניין בחלופה אנושית או אלגוריתמית.
- **יש מקום לדרישה של בקרה אנושית על פעילות המערכת בכללותה.** דרישה כזו נועדה להבטיח את תקינות המערכת בהיבטים כגון תאימות ההחלטות לדין ולרגולציה, היעדר שגיאות והטיות וכדומה. אין הכוונה שהבקרה הרציפה חייבת להיות אנושית בכל שלב, אלא שנדרשת גם מעורבות אנושית.
- **החובה להכניס לשימוש מערכות שמאפשרות בקרה ומעורבות אנושית מוטלת על הגוף הפיננסי המפוקח.**

יידוע וגילוי

אחת החובות הרגולטוריות הנדונות ביחס לשילוב מערכות בינה מלאכותית בשירותים ובמוצרים שונים היא דרישת יידוע על עצם השימוש במערכת בינה מלאכותית. כלומר יידוע כי בשירות או במוצר מסוים נעשה שימוש במערכת שניתן לאפיין כמערכת בינה מלאכותית. דרישת היידוע עשויה להקנות לצרכן אפשרות בחירה באשר לאופן שבו הוא מעוניין לצרוך את השירות שלו, עשויה ללמד את הרגולטור על סוג והיקף השימושים וכדומה.

מלבד יידוע על עצם השימוש במערכת בינה מלאכותית, עשויות להיות דרישות גילוי רגולטוריות החלות לגבי מוצרים ושירותים פיננסיים, בעניינן עולה שאלה אם נדרש מידע נוסף הנוגע למערכות בינה מלאכותית. בהקשר זה עשויות החובות הרגולטוריות לנוע על פני משרע רחב של אפשרויות, הן ביחס לתכני הגילוי (למשל, תכנים כלליים או ספציפיים; תכנים המיועדים לשקף בעיקר סיכונים ואזהרות או תכנים המיועדים לשקף גם יתרונות; וכדומה) הן ביחס למתכונת הגילוי (למשל, גילוי במסגרת הסכם עם הלקוח, גילוי על בסיס תקופתי, גילוי סטנדרטי או בולט; וכדומה).

פן שלישי של דרישות הגילוי הוא צמצום הסיכון לפרסומים מטעים סביב נושא הבינה המלאכותית. טכנולוגיות חדשות ומורכבות עשויות להוות כר פורה לפרסומים המאדירים את הגופים העושים בהן שימוש, ככלי שיווקי. חובות גילוי יכולות לצמצם סיכון זה ולחייב את הגופים בפרסום אמת.

בעולמות הפיננסיים, דרישות גילוי הן אחת הטכניקות הרגולטוריות השכיחות ביותר, וניתן למצוא אותן למעשה ביחס לכל שירות או מוצר המוצע ללקוח. אין זה מפתיע כי גם ברוב המוחלט של מסמכי הרגולציה והאתיקה המובילים בעולם בהקשרי בינה מלאכותית מוצע לעגן דרישות גילוי, שקיפות או הסברתיות. הצוות הבחין בהקשר זה בין שלושה היבטי גילוי: דרישת יידוע בסיסית בדבר עצם השימוש במערכת בינה מלאכותית (למשל יידוע בשירות לקוחות של בנק כי האינטראקציה בצ'אט-בוט אינה עם גורם אנושי אלא עם מערכת בינה מלאכותית); דרישות גילוי למשקיע או ללקוח העוסקות במאפייני פעילותה של מערכת הבינה המלאכותית (למשל, היקף מעורבותה של הבינה

המלאכותית בהחלטת אשראי, מגבלותיה של המערכת, קיומן של חלופות שירות, וכדומה); והתמודדות עם גילוי שיווקי מטעה בנושא בינה מלאכותית.

להלן עיקרי המלצות הצוות לגבי דרישות יידוע וגילוי:

- יש מקום לדרישת יידוע בדבר עצם השימוש במערכת בינה מלאכותית ביתר שאת בשלב ראשוני של כניסת הטכנולוגיה. דרישת היידוע בשלב זה נדרשת לא רק בגלל שיעילותה של הטכנולוגיה טרם התבררה, אלא גם משום שניתנים עדיין שירותים שלא באמצעות מערכות בינה מלאכותית וללקוחות יש לפיכך אפשרות בחירה. על היידוע להיעשות בשפה ניטרלית וברורה אשר לא תיצר העדפה לשירות אחד על משנהו ללא בסיס. דרישת היידוע מקבלת משנה תוקף מקום בו לקוח עשוי לטעות ולחשוב שהוא באינטראקציה עם אדם, כאשר בפועל האינטראקציה מבוצעת מול מערכת בינה מלאכותית. עם זאת, אין מקום לדרישת יידוע כאשר השימוש במערכת בינה מלאכותית ברור. יהיה מקום לבחון את הדרישה בחלופ השלב הראשוני של כניסת הטכנולוגיה.
- חובות גילוי בדבר מאפייני מערכת הבינה המלאכותית והשלכותיה צריכות להשתלב בדרישות הגילוי הקיימות לגבי השירות או המוצר המוצעים ללקוח. בהקשר זה, יש מקום לשקול חובות גילוי כאשר מערכת הבינה המלאכותית היא בעלת השפעה מהותית על השירות או המוצר, ובהתאמה, חובות הגילוי צריכות לעסוק במאפיינים הייחודיים הנובעים מטכנולוגיית הבינה המלאכותית. בדוח מוצגת דוגמה לחובות גילוי כאמור לגבי ניהול תיקים אלגוריתמי, העוסקות במהות השירות ומאפייניו הייחודיים, הסיכונים האפשריים הנובעים ממנו, והמתודולוגיה של המערכת.
- הגבלת פרסומים שיווקיים מטעים – ככל שתתפתח תופעה של פרסומים שיווקיים מטעים בנושא בינה מלאכותית (AI Washing), יש להתמודד איתם באמצעות סל הכלים הרגולטורי הקיים, הכולל עמדות והוראות בדבר הגילוי הניתן על-ידי גופים מפוקחים, פעולות אכיפה, ופעולות של חינוך פיננסי ללקוחות ולמשקיעים.

הזכות לפרטיות והגנה על מידע אישי

טכנולוגיות בינה מלאכותית מתבססות על איסוף ועיבוד מידע בצורה נרחבת, ובכלל זה על מידע אישי, כלומר מידע שנוגע לאדם מזהה או שניתן לזהותו. המידע הוא "הדלק" או "החמצן" המניע את מערכות הבינה המלאכותית, הוא המשאב העיקרי וההכרחי לפיתוחן ולפעילותן. לפיכך, פיתוח מערכות בינה מלאכותית והשימוש בהן, כרוך בניסיון להתבסס על מידע מקיף, מגוון ורחב ככל הניתן, בין אם מתוך שאיפה לייצר תוצרים ברמת דיוק גבוהה, ובין אם בשל הרצון לפתח מוצרים חדשניים שלא מסתמכים בהכרח על מידע "סטנדרטי". בנוסף לכך, תוצרי מערכות הבינה המלאכותית – התחזיות, ההמלצות ואף ההחלטות – מכוונים במקרים רבים כלפי בני אדם, ומשמשים אמצעי לחזות את התנהגותם, לזהות דפוסי פעולה אנושיים, תכונות אופי, מצב נפשי או פיזי ועוד. התוצרים מגלמים אם כן תובנות פרטניות ואישיות לגבי בני אדם, לעתים רגישות ביותר, על היבטים פרטיים שונים בחייו. מאפיינים אלה של מערכות הבינה המלאכותית מעוררים אתגרים ומתחים לא מבוטלים בקשר להגנה על הזכות לפרטיות ועל מידע אישי, לכל אורכו של מחזור החיים של מערכות אלו, ובכלל זאת לגבי יישומן של דרישות יסוד בדיני הגנת הפרטיות כמו עקרון צמידות המטרה או עקרון מזעור המידע.

הדוח כולל סקירה של ההסדרים הרלוונטיים בדיני הגנת הפרטיות בישראל, דיון והתמקדות במספר אתגרים מרכזיים תוך יישום על דוגמאות מעולם הפיננסים, בחינה משווה הסוגיות בעולם, ובפרט בראי הרגולציה של האיחוד האירופי העוסקת בעיבוד מידע אישי (ה-GDPR), והמלצות לגבי כל אתגר.

להלן עיקרי האתגרים והמלצות הצוות בנושא פרטיות והגנת מידע אישי:

- הבחנה בין מידע אישי למידע אנונימי – דיני הגנת הפרטיות חלים על מידע אישי, כלומר מידע שנוגע לאדם מזהה או לאדם הניתן לזהויו במאמץ סביר. השאלה אם ניתן לזהות אדם על בסיס נתונים מסוימים, ובכלל זה גם נתונים שהוסרו מהם רכיבים מזהים ברורים, הופכת מורכבת יותר עם עלייתן והתפתחותן של מערכות הבינה המלאכותית, המביאות לשדרוג יכולת הזיהוי מחדש של מידע לא מזהה. בכך סיכונים לא מבוטלים לפרטיות ולהגנת מידע אישי.

מוצע בין היתר לבחון הכוונה של הגורמים המפוקחים לבצע הערכת סיכונים ביחס לסיכון לזיהוי חוזר של מידע אישי וכן לנקוט אמצעים של אבטחת מידע גם על מידע "מותמם". עוד מוצע כי רגולטורים פיננסיים, בהתייעצות עם הרשות להגנת הפרטיות, יבחנו שיטות מקובלות ומתקדמות להתממת מידע אישי ככלי

להפחתת סיכון לזיהוי מחדש.

- הסכמה מדעת לעיבוד מידע במערכות בינה מלאכותית** – חוק הגנת הפרטיות קובע כי לא ניתן לפגוע בפרטיותו של אדם, אלא בהסכמתו או מכוח הסמכה בחוק, וכי על ההסכמה להיות "הסכמה מדעת". כבר כיום הסביבה הדיגיטלית מקשה על האפשרות להעניק הסכמה אמיתית ו"מדעת" לעיבוד מידע אישי ולמטרות העיבוד. יישום דרישת ההסכמה מדעת כתנאי לעיבוד מידע אישי הכרוך בפגיעה בפרטיות לצורך פיתוח, אימון ושימוש במידע במערכות בינה מלאכותית מציב אתגר משמעותי נוסף, נוכח פעילותן של מערכות אלו ככלל כ"קופסה שחורה", והקושי להציג לפרט מהן מטרות השימוש במידע האישי שלו, אילו פעולות ייעשו במידע, ובאיזה מידע אודותיו ייעשה שימוש לצורך אותן מטרות. זאת ועוד, ההסכמה "כובלת" את הגורם המעבד את המידע ביחס לשימושים המותרים, ולעתים אלה אינם ידועים בעת מתן ההסכמה. סוגיה נוספת שמתעוררת נוגעת לשימוש במידע אישי שנאסף במסגרת התקשרויות קודמות למתן שירות, שהסתיימו, ולא כללו הסכמה לפעולות עיבוד מידע לשם פיתוח או אימון של מערכות בינה מלאכותית (בעיית המלאי).

רוב המלצות הצוות בהקשר זה עוסקות באמצעים לחיזוק ההסכמה מדעת במקרים של שימוש במידע אישי במערכות בינה מלאכותית, ככל שהפעילות היא בסיכון גבוה, שמטרות השימוש בה מורכבות יותר או חורגות מציפיותו הסבירה של נושא המידע. **לצד המלצות אלה, מוצע לקבוע בסיסים חוקיים נוספים לעיבוד מידע אישי לצרכי פיתוח ואימון מערכות בינה מלאכותית**, באופן שיאפשר את התפתחות הטכנולוגיה מחד, אך ייתן מענה והגנות לנושאי המידע מאידך. באשר לנתוני עבר ("בעיית המלאי"), מוצע להבהיר כי הצורך בקבלת הסכמה מחודשת יהיה תלוי באופי ההסכמה שניתנה, בתכליתה, ובפעילות שמוצע לבצע, ואין להסיק כי עצם השימוש במערכות בינה מלאכותית מחייב בהכרח קבלת הסכמה חדשה מכל לקוח.
- מידע אישי מוסק (inferred personal data) בתוצרי מערכות בינה מלאכותית** – מערכות בינה מלאכותית מרחיבות באופן משמעותי את היכולת להסיק מידע חדש על נושאי מידע, ומכוונות, בין היתר, לאתר דפוסי פעולה או קורלציות בלתי צפויים או כאלה שלא היו נגישים קודם לכן לעין האנושית. יכולות המחשוב והעיבוד שהשתפרו לצד זמינות נתוני ענק ופיתוח טכנולוגיות הבינה המלאכותית משפרות דרמטית את היכולת להגיע לתובנות רגישות ועשירות על בני אדם ובין היתר בנוגע להיבטים אישיותיים והתנהגותיים, מוצא אתני, העדפה מינית ודעות, כמו גם תחזיות על התנהגותם בעתיד. יכולות אלו מציבות אתגר נוסף בהגנה על הזכות לפרטיות פרטיות, בשאלה האם יש לסווג את תוצרי הבינה המלאכותית כ"מידע אישי" והאם נדרש להחיל ביחס למידע מסוג זה חובות או זכויות ייעודיות נוספות או שיש התאמות שנכון לערוך במסגרת יישום החוק בנושא.

הנחת הדוח היא כי תוצרי מערכות בינה מלאכותית הנוגעים או מכוונים לאדם ספציפי הם מידע אישי על פי הדין הקיים, הזוכה להגנת דיני הגנת הפרטיות. בדוח מוצע לאמץ כלל בדבר היסק סביר בעניינו של אדם, אשר יחול ביחס להחלטות בסיכון גבוה, אשר ישען על אמות מידה של מקובלות (Acceptability), רלבנטיות (Relevance) ואמינות (Reliability).
- יישום עקרון צמידות המטרה** – עקרון יסודי זה בדיני הגנת הפרטיות קובע כי ניתן לאסוף מידע אישי ולהשתמש בו למטרה לשמה נאסף או נמסר בלבד. השאלות ביחס ליישום עקרון זה במערכות בינה מלאכותית נוגעות – בדומה לקשיים שתוארו לגבי דרישת ההסכמה – בין היתר לקושי כי מטרת עיבוד המידע תהיה ברורה, מפורטת ומפורשת, ולקושי ביחס לשימוש ב"מלאי" קיים של מידע שנאסף למטרות אחרות. קושי נוסף נוגע לקציר מידע המופיע באינטרנט (scraping) לצרכי פיתוח ואימון מערכות בינה מלאכותית, באופן שעשוי לחרוג מגדר ההסכמה או הציפיות הסבירות של המשתמשים ולהיעשות בניגוד לעקרון צמידות המטרה.

בהמלצות הוצע כי בשלב פיתוח מערכות, מידת הפירוט של מטרות עיבוד המידע האישי והשימושים בו תהיה בהלימה להערכת הסיכונים הנשקפים מן המערכת. על תוכן ההסבר האמור להיות מפורט ובהיר יותר ככל שמטרות השימוש במידע האישי מורכבות יותר או חורגות מציפיותו הסבירה של הלקוח. בשלב השימוש במערכות, ההנחה היא שהקושי לפרט בבירור את מטרות השימוש במידע פוחת ממילא. עוד הוצע לבחון הקלות ביישום עקרון צמידות המטרה לשם פיתוח מערכות בינה מלאכותית בכפוף למגבלות ואמצעי בקרה, הנוגעים בין היתר להגנת מידע אישי; ולבחון את האפשרות לקבוע הוראות המסדירות את התנאים והנסיבות שבהם ניתן לאסוף מידע בדרך של קציר מידע מהאינטרנט (scraping) באופן שאינו מפר את הוראות חוק הגנת הפרטיות וכל דין אחר.
- עקרון מזעור המידע** – עקרון ליבה בדיני הגנת הפרטיות, לפיו יש לאסוף רק את המידע שרלוונטי והכרחי למטרת העיבוד ויש איסור לאסוף ולעבד מידע עודף, כלומר מידע שחורג מהדרוש למימוש המטרה המקורית.

קיים מתח מובנה בין עקרון מזעור המידע ובין פיתוח מערכות בינה מלאכותית המתבססות על מידע בהיקפים גדולים ככל הניתן.

ההמלצות מבקשות לבחון כיצד ליישם את עקרון מזעור המידע ביחס למערכות בינה מלאכותית. למשל, באמצעות דגש על מזעור פרסונליות המידע, בעוד שמידע אחר לא יהיה חייב במזעור באותו האופן, או באמצעות נקיטת אמצעים ארגוניים וטכנולוגיים שיאפשרו ניקוי ומחיקה של נתונים שאינם נחוצים עוד. עוד מוצע לבחון הגבלות מראש על שימוש בסוגי מידע מסוימים לצורך פיתוח מערכות בינה מלאכותית בתחומים מסוימים (למשל הגבלה על שימוש בתמונות פנים). ואף מוצע ליצור הפרדה בין המידע שנאסף ונעשה בו שימוש, לשמור אותו בנפרד, ולקבוע תקופות שמירה, הרשאות גישה וכדו', בהתאם לצרכים המשתנים של כל שלב.

בנוסף להמלצות ביחס לאתגרים האמורים, **מוצע לשקול הכוונה של גורמים מפקחים לאמץ כלים ארגוניים לניהול וצמצום הסיכונים לפרטיות הכרוכים בפיתוח מערכות בינה מלאכותית כמו תסקיר השפעה על פרטיות, יישום והטמעת תפיסות עיצוב לפרטיות (Privacy by Design), וזאת בנוסף למינוי ממונה על הגנת הפרטיות.**

הטיה ואפליה

אתגר מרכזי ביחס למערכות מבוססות בינה מלאכותית הוא הסיכון לאפליה (Discrimination) ולהטיות (Biases). אמנם קבלת החלטה על ידי אלגוריתם ולא על ידי גורם אנושי עשויה למתן את הנטייה האנושית להטיות בלתי מודעות או מכוונות, אולם מערכות בינה מלאכותית חשופות אף הן לסיכון להטיות או לאפליה מטעמים שונים: שימוש במאגרי מידע שאינם מייצגים מספיק, או שהמידע בהם משקף הטיית ואפליה קיימות בחברה, וכן אלגוריתמים העלולים לעשות שימוש בנתוני השתייכות מפלים (דוגמת לאום, מגדר, גזע ועוד) או בנתוני "פרוקסי" שיש להם קורלציה עם נתונים מפלים. היקף פעילותן הרחב של מערכות בינה מלאכותית מגביר את הסיכון להתרחשות תופעות אלה בקנה מידה רחב, בהשוואה להחלטה אנושית פרטנית.

הדוח סוקר את הדין החל בעניין איסור אפליה בישראל וכן את העיסוק באפליה אפשרית של מערכות בינה מלאכותית ברגולציה העוסקת בפעילות פיננסית בחו"ל. החשש להטיות ולאפליה עשוי להתעורר לדוגמה בנוגע למתן אשראי או לתמחור של פוליסות ביטוח, ורגולטורים בחו"ל פרסמו גילויי דעת המבהירים כי יש להבטיח הוגנות והעדר אפליה בעת שימוש במערכות בינה מלאכותית.

להלן עיקרי המלצות הצוות בנושא אפליה:

- **דיני איסור האפליה הקיימים מוסיפים לחול גם כאשר נעשה שימוש במערכות בינה מלאכותית. הפעולות וההחלטות של גופים כפופים לאיסור האפליה ללא קשר לטכנולוגיה שבה הם עושים שימוש, ועל כן מובן כי כך הדבר גם כאשר נעשה שימוש במערכות בינה מלאכותית.**
- השימוש במערכות בינה מלאכותית עלול ליצור סיכונים לפגיעה בשוויון בין היתר בשל החשש שהפגיעה תהיה נסתרת, לא מודעת או קשה לאיתור. **מוצע כי הרגולטורים הפיננסיים ישקלו פעולות להכוונת הגורמים המפקחים במסגרת הסמכויות הנתונות להם.** סוגיות מרכזיות בהקשר זה הן בקרה ונקיטת אמצעים לזיהוי ומניעת הטיית לכל אורך חיי המערכת, ובפרט ביחס לתוצאות שאליהן מגיעה המערכת.
- **עריכת בקרה ונקיטת אמצעים לכל אורך חיי המערכת, בין היתר בהיבטים המרכזיים הבאים – על מאגרי הנתונים המשמשים לאימון, תיקוף ובחינת המערכות, להיות מאגרים מייצגים ומגוונים; יש לבחון את פעילות המערכת באופן שוטף, גם בשלב ההטמעה והיישום; ויש לבחון את תוצאות המערכת כדי לוודא שלא ניתן בפועל יחס מפלה לאוכלוסיות שונות בעלות נתונים דומים.**
- **בקרה תוצאתית – מוצע לנקוט בכלים של בקרה תוצאתית, בין השאר, לצורך בחינת טענות לאפליה (או להיעדרה).** כלים אלה יכולים לסייע בידי הגורם המפוקח והרגולטור בזיהוי אפליה במערכות אשר על פניו פעולתן עשויה להיראות נייטרלית וללא שימוש בנתונים מפלים. אין בכך כדי להחליף את השימוש בכלי בקרה אחרים אלא להוסיף.

אחריות

האסדרה המשפטית מבוססת על פי רוב על אחריות של גורם אנושי למילוי חובות ובוחנת את התנהלותו ושיקול דעתו במקרה של טענות להפרה. בעידן הבינה המלאכותית תפקידו של הגורם האנושי מצטמצם ולעיתים אף אינו מוגדר, ולכן מתערער המבנה המשפטי המוכר של הטלת אחריות, אשר הושתת היסטורית על הימצאותו של אדם

או תאגיד במוקד ההתרחשות, אשר ככלל נושא באחריות למעשיו. סוגיית האחריות מתחדדת גם לנוכח המאפיינים האוטונומיים והאוטונומיים של המערכות, וכן מפני שלעתים מדובר בשילוב של מספר מערכות וגורמים המובילים לתוצר שהציבור עושה בו שימוש. כך למשל, עולות שאלות מהו סטנדרט ההתנהגות המצופה ממערכת בינה מלאכותית; האם ניתן לייחס ידיעה או אמונה למערכת מחשב; וכדומה.

יכולות להיות גישות שונות לגבי אופן חלוקת האחריות בין הגורמים השונים המעורבים בפעילות של מערכות בינה מלאכותית. בעיקר מדובר במפתח המערכת (provider), מפעיל המערכת (deployer), ומשתמש הקצה (end user). בדוח נערך ניתוח של השיקולים להטלת אחריות על הגורמים המעורבים בפיתוח ושימוש בבינה מלאכותית וכן סקירה השוואתית של גישות בחו"ל בנושא האחריות על מערכות בינה מלאכותית.

להלן עיקרי המלצות הצוות בנושא אחריות:

- **שימור עיקרון האחריות של הגוף המפוקח** – אין מקום לסטות מהעיקרון המקובל ברגולציה הפיננסית, לפיו האחריות על פי דין מוטלת על הגוף המפוקח. במסגרת החוזית באמצעותה מסדיר הגוף המפוקח את פעילותו מול גורמים חיצוניים, יכול הגוף המפוקח לקבוע כי יהיה זכאי לשיפוי מהגורמים החיצוניים במקרה בו נגרם נזק (למשל כתוצאה מכשל במערכות מחשב שרכש מגורם חיצוני), אולם האחריות לפי דין וכלפי הלקוחות נותרת אצלו.
- **מוצע לראות בהתקשרות של גוף פיננסי עם צד שלישי לגבי מערכות בינה מלאכותית כמיקור חוץ, וליישם את ההוראות העוסקות בכך.** מיקור חוץ על ידי גופים פיננסיים הוא פרקטיקה מקובלת ומוסדרת, אשר נקבע לגביה כי היא אינה גורעת מאחריות הגופים הפיננסיים לקיום החובות הרגולטוריות החלות עליהם לפי מכלול הדינים וההוראות.
- **הרגולציה הפיננסית מטילה בנסיבות מסוימות אחריות ספציפית על אורגנים ובעלי תפקידים בגוף הפיננסי,** כאשר ככלל האחריות הכוללת לפעולותיו של הגוף המפוקח מוטלת על הדירקטוריון שלו. בהתאם לגישה שהוצגה לעיל, ולהמלצות האסדרה בחו"ל, **מוצע שלא לסטות מכללי אחריות אלה גם בנוגע למערכות בינה מלאכותית** – הן בקשר עם הטמעת מערכות בגוף הפיננסי, הן בקשר עם אופן השימוש בהן ועריכת ניהול סיכונים מתאימים. אין בכך לגרוע מהאפשרות כי בנוסף יחולו חובות ואחריות מיוחדים בהתאם להוראות מממשל בינה מלאכותית שייקבעו (ראו בהמשך).
- **לנוכח ההתפתחות שחלה בעולם בנוגע לחובות המוטלות על מפתחי מערכות בינה מלאכותית (providers), יהיה מקום לשקול בעתיד התייחסות לרגולציה החלה על המפתח כשיקול או כתנאי עתידי ביחס להפעלת מערכת בינה מלאכותית.**
- **איסור הגבלת אחריות כלפי הלקוח** – מוצע, ככלל, לאסור על גוף פיננסי להסיר או להגביל את אחריותו לגבי שירותים הניתנים ללקוח באמצעות מערכות בינה מלאכותית. אין באמור כדי להסיר אחריות מהלקוח מקום בו הנסיבות מצדיקות זאת, למשל מקום בו הלקוח נטל במודע סיכון השקעה שהתממש במהלך שירות שניתן לו בהתבסס על מערכת בינה מלאכותית או מקום בו נעשה שימוש לרעה במערכת באופן מודע או שימוש החורג ממתחם הסבירות על ידי הלקוח. כמו-כן, אין באמור כדי למנוע הבהרות של הגוף המפוקח בדבר מגבלות סבירות של מערכת בינה מלאכותית.

ממשל בינה מלאכותית

המונח ממשל בינה מלאכותית (AI Governance) משמש לתיאור מסגרת לצמצום האתגרים והפחתת הסיכונים הכרוכים בשימוש בבינה מלאכותית. תפקידם של כללי ממשל בינה מלאכותית ליצור מנגנוני ניהול ובקרה ראויים בתאגיד בתחום הבינה המלאכותית, תוך הסדרת אופן קבלת ההחלטות, ניהול הסיכונים, הבקרה והפיקוח על הפעלת מערכות בינה מלאכותית בארגונים. כללי ממשל המושתתים על עקרונות ראויים, מהווים אמצעי לניהול סיכונים התאגיד ומסייעים לשמור על חוסנו ויציבותו. הם נועדו "לתרגם" את הסיכונים והאתגרים הכרוכים בשימוש במערכות בינה מלאכותית לכדי שיטות, תהליכים ואמצעים פרקטיים ששיגו שימוש אחראי והוגן במערכות בינה מלאכותית.

הדוח פורש שורה של נושאים ואמצעים למסגרת של ממשל בינה מלאכותית בגופים פיננסיים, בהתבסס על הפרקטיקות המתפתחות בנושא זה בעולם. האמצעים מוצגים כארגז כלים עבור הרגולטורים והגופים המפוקחים, ואפשר לעשות בהם שימוש בהתאם לשיקולים ונסיבות שונים, לדוגמה אופי השירות הניתן באמצעות מערכות בינה מלאכותית, מהותיות, פוטנציאל הפגיעה בפרט, וכדומה. החלה כאמור צריך שתיעשה כמובן לאחר בחינת הסדרי

הממשל הקיימים והצורך באמצעים אלה (כולם, חלקם או שילובם). האמצעים המפורטים אינם מהווים רשימה ממצה, ובטרם יוחלט אחרת על ידי הרגולטורים הפיננסיים הם אינם מחייבים.

ארגז הכלים בנושא ממשל בינה מלאכותית מוצג לפי הקטגוריות הבאות:

נהלים, מסמכי מדיניות, תהליכים ופרקטיקות – העוסקים בכל מחזור החיים של מערכות הבינה המלאכותית; **תהליכי קבלת החלטות ואחריות** – לרבות אחריות הדירקטוריון וההנהלה הבכירה להיבטי אימוץ, פיקוח, ניטור ושימוש במערכות בינה מלאכותית; **ניטור, פיקוח, תיקוף** – בטרם תחילת השימוש במערכת הבינה המלאכותית, וכן באופן שוטף לאחר תחילת פעילותה; **חירום והפסקת פעילות** – אמצעים לעצירת פעילות המערכת וגיווי למערכת; **שימוש במיקור חוץ וספקי צד שלישי**.

תחום משיק לממשל הבינה המלאכותית הוא **ממשל נתונים (Data Governance)**. תחום זה מקבל משמעות יתרה בכל הקשור למערכות בינה מלאכותית, אשר פעולתן ותוצריהן תלוי במידה רבה במידע והנתונים המזינים אותן. בדומה להמלצות בנוגע לממשל בינה מלאכותית, הדוח כולל התייחסות לכלים אפשריים במישורים של **מקורות המידע והשימוש במידע**.

גישה מבוססת סיכונים

הטיפול בסיכונים הנובעים ממערכות בינה מלאכותית צריך להיעשות בראייה כוללת. הדבר נובע מכך שהסיכונים השונים עשויים להיות קשורים זה בזה, ובדומה לכך, גם אמצעי ההתמודדות עם הסיכונים עשויים להיות קשורים זה בזה. העיקרון של אסדרה מבוססת סיכונים מופיע כחוט השני במסמכי מדיניות בעולם ובישראל העוסקים בבינה מלאכותית, ויתרונותיו ברורים: הגברת אפקטיביות הרגולציה ויעילות בהקצאת משאבים על-ידי הרגולטורים והגופים המפוקחים לנוכח ההתמקדות בסיכונים המהותיים; גמישות בהתאמת הרגולציה לסיכונים המשתנים העולים מהפעילות על פני זמן ובמקרים ספציפיים; ועידוד פעילות עסקית וחדשנות בהנחה שרגולציה מבוססת סיכונים לא תכביד יתר על המידה על הגופים המפוקחים.

דוגמה בולטת לאסדרת בינה מלאכותית בהתאם לגישה מבוססת סיכונים היא ה-EU AI Act. במסגרת חקיקה זו אופיינו 4 קטגוריות סיכון למערכות בינה מלאכותית, וכפועל יוצא מכך נגזרים המגבלות והכללים החלים לגביהן.

להלן עיקרי המלצות הצוות בנושא גישה מבוססת סיכונים:

- כאמור, התפישה הכללית היא כי העיסוק במערכות בינה מלאכותית צריך להיות בגישה מבוססת סיכונים.
- מדרג סיכונים הוא כלי שימושי בסיווג רמת הסיכון של מערכות בינה מלאכותית בסקטור הפיננסי וקביעת אמצעים מותאמים להתמודדות עם הסיכון. ניתן לדוגמה למיין מערכות של בינה מלאכותית על בסיס **מדרג סיכונים הכולל שתי רמות סיכון – נמוכה-בינונית וגבוהה**.
- **סיווג הסיכון בגופים פיננסיים צריך להיעשות על בסיס כפול:** ראשית, רמת הסיכון **ללקוחות, למשקיעים או לציבור**, ושנית, רמת הסיכון **לגוף הפיננסי עצמו**. סיווג הסיכון צריך שיעשה בראש ובראשונה בידי הגופים המפוקחים. אין בכך למנוע כי בעתיד יבקש רגולטור פיננסי להכתיב כי מערכות מסוימות יסווגו בסיכון גבוה, או ידרוש מגוף מפוקח לשנות את רמת הסיווג, ובהתאמה את האמצעים הנדרשים לגבי מערכת מסוימת.
- **האמצעים שיינקטו ביחס למערכת בינה מלאכותית יהיו מותאמים לרמת הסיכון שלה**. כך למשל ביחס למערכות ברמת סיכון גבוהה אפשר להשית דרישות ממשל משמעותיות יותר על מנת להתמודד עם הסיכון הגלום בהן, בעוד שביחס למערכות המגלמות רמת סיכון נמוכה יותר, אפשר להסתפק בדרישות מצומצמות יותר.
- **הדוח כולל המחשה כיצד הטיפול בסוגיות השונות העולות בהפעלת מערכות בינה מלאכותית בסקטור הפיננסי יכול להיעשות על בסיס סיווג הסיכון**.

ה. סוגיות הנוגעות להשפעת שימושי בינה מלאכותית על השוק הפיננסי בכללותו

לכניסתה של הבינה המלאכותית לסקטור הפיננסי עשויות להיות השלכות גם בראיית השוק בכללותו. השפעות הבינה המלאכותית בהקשר זה אינן נוגעות רק לגופים שיבקשו להפעיל מערכות בינה מלאכותית, אלא למערכת הפיננסית בכללותה, והן נוגעות להיבטי יציבות פיננסית, מבנה שוק ותחרות, וסיכונים תפעוליים לרבות סיכוני דיסאינפורמציה. ההכוונה בחלק זה של הדוח מיועדת בעיקר לרגולטורים וליתר קובעי המדיניות העוסקים באסדרה של הסקטור הפיננסי.

יציבות פיננסית

ההתמודדות עם סיכוני יציבות פיננסית היא אינטרס פיקוחי ממדרגה ראשונה, לשם הגנת כספי הציבור, שמירה על תקינות פעילותה של המערכת הפיננסית, ומניעת משברים פיננסיים העלולים לפגוע במשק בכללותו. ההכרה בחשיבותם של סיכוני יציבות פיננסית גברה בעקבות המשבר הפיננסי העולמי של שנת 2008, אשר המחיש את הצורך לבחון את המערכת הפיננסית באופן רחב, להבדיל מבחינה של רכיבים או מוסדות ספציפיים בתוכה, ולעמוד על מגמות וסיכונים העלולים להשפיע באופן מהותי לשלילה על פעילותה. בעקבות המשבר התרחבו במדינות העולם העיסוק והבקורות בנוגע לסיכונים מערכתיים, וכך גם בישראל, בה הוקמה הוועדה ליציבות פיננסית, במטרה לתמוך ביציבותה של המערכת הפיננסית ובפעילותה הסדירה.

הסיכונים ליציבות פיננסית בעקבות כניסתה של הבינה המלאכותית מיוחסים בדרך כלל למישורים העיקריים הבאים המתוארים בדוח:

עדריות (herding) ותנודתיות – השימוש באותם מודלים של בינה מלאכותית על-ידי מספר גדול של שחקנים במערכת הפיננסית עלול להוביל להתנהגות עדרית, קרי פעולה נרחבת של שחקנים רבים באופן דומה.

ריכוזיות ותלות בצדדים שלישיים – ריכוז פעילות פיננסית בידי מספר קטן של גורמים, המחזיקים במידע וביכולות הטכנולוגיות לשימושי בינה מלאכותית, מעורר חששות להתגברות הסיכון מהתרחשות של כשל תפעולי או אחר, ולתלות שצפויה להתפתח במספר קטן של חברות בתחום הבינה המלאכותית.

קישוריות (interconnectedness) והדבקה (contagion) – סיכונים אלה נוגעים לחשש כי זעזועים בגוף או בחלק מסוים של המערכת הפיננסית יתפשטו ובמהירות לגופים ולאזורים נוספים במערכת.

לסיכונים האמורים מצטרפים מאפיינים של מערכות בינה מלאכותית כמו מאפיין "הקופסה השחורה" המקשה על הבנת פעולת המערכת, ומגביר מטבע הדברים את הסיכון הגלום בה, או הסיכון של הסתמכות יתר על מערכות בינה מלאכותית והשימוש הפוטנציאלי הנרחב בהן בהשוואה למערכות רגילות. יש גם להביא בחשבון את העובדה שמערכות אלה יכולות לקבלת כמות גדולה של החלטות בזמן קצר – דבר העלול להאיץ משברים. בדוח מוצגות מספר דוגמאות למצבי קיצון וסיכונים אפשריים כתוצאה משימוש מוגבר בבינה מלאכותית במגזר הפיננסי.

אף שסיכוני יציבות פיננסית הועלו גם במדינות ובארגונים בחו"ל, נראה שמדינות בעולם מסתפקות לעת עתה במעקב ובחינה של השלכות כניסתה העתידית של בינה מלאכותית על יציבות פיננסית.

להלן עיקרי המלצות הצוות בנושא יציבות פיננסית:

לנוכח היקף האימוץ המוגבל של יישומי בינה מלאכותית והעדר צעדים קונקרטיים במדינות העולם, הצוות סבור כי בשלב זה יש מקום להמשך מעקב בסוגיה זו ובחינת הצורך בנקיטת פעולות בעתיד. פעולות אלה יכול שיקלו מיפוי של פעילויות הנתונות לסיכון משמעותי, בחינת המסגרות הקיימות להתמודדות של מוסדות פיננסיים עם סיכונים תפעוליים וסיכוני סייבר, וגיבוש אסטרטגיה לצמצום סיכונים מערכתיים הנובעים מהסתמכות על צדדים שלישיים שהם קריטיים לתפקודה של המערכת הפיננסית.

בישראל פועלת הוועדה ליציבות פיננסית, וגם במסגרתה ניתן יהיה להמשיך ולבחון את ההשלכות של שימושי בינה מלאכותית על עמידות המערכת, כמו גם את ההתמודדות עם סיכונים מערכתיים ליציבות הפיננסית.

תחרות

לבינה מלאכותית יש פוטנציאל להגביר את הפיריון בתחום הפיננסי, להניע חדשנות בקרב שחקנים קיימים וחדשים, ולאפשר יצירת מוצרים ושירותים שייטיבו עם הציבור.

לצד ההשלכות החיוביות שעשויות להיות לבינה מלאכותית, הדוח מנתח את הבעיות התחרותיות שעלולות להיווצר לאורך שרשרת האספקה של תחום הבינה המלאכותית, הכוללת את ספקי הידע והתשומות לפיתוח מודלים של בינה מלאכותית, את השחקנים הפעילים בפיתוח ועיצוב המודלים, ואת המשתמשים העסקיים שמטמיעים את המערכות בתהליכי עבודה, במוצרים ובשירותים.

החששות התחרותיים המרכזיים נוגעים הן לתחום פיתוח המודלים של בינה מלאכותית, הן לשחקנים שיוכלו לעשות שימוש במודלים אלה. בתחום פיתוח המודלים של בינה מלאכותית עולים בין היתר חששות בנוגע לחסמים בגישה לתשומות הנדרשות, חשש מחיזוק המעמד הדומיננטי של חברות הטכנולוגיה הגדולות באמצעות מודלים של בינה מלאכותית וחשש מהתפתחות שווקים בעלי דינמיקה של "המנצח לוקח הכל" או "המנצח לוקח הרוב". לגבי השחקנים

הפיננסיים שיעשו שימוש במודלים, עולים חששות הנובעים גם מכך שהסקטור הפיננסי מתאפיין בריכוזיות ובחסימי מעבר כבר כיום, ועל כן יתרונות קיימים לגודל ולהיקף עלולים להתעצם.

להלן עיקרי המלצות הצוות בנושא תחרות:

- **המשך תחולה של דיני התחרות גם מקום בו פרקטיקות אנטי תחרותיות מתבצעות באמצעות מודלים של בינה מלאכותית או כתוצאה מהפעלתם.** לשם המחשה, מניעת גישה של מתחרים לתשומות מרכזיות שנדרשות לפיתוח מודלים של בינה מלאכותית על-ידי בעל מונפוליון, עלולה להוות הפרה של חוק התחרות הכלכלית, התשמ"ח-1988.
- **רשות התחרות תשקול במסגרת בחינת מיזוגים המובאים לשולחנה גם חששות להיווצרות כוח שוק או חסמי תחרות באמצעות בינה מלאכותית.** למשל, מיזוגים היוצרים כוח שוק על בסיס יתרון במידע על לקוחות שיש לגופים המבקשים להתמזג.
- **הרחבת הגישה הניתנת לגורמים פיננסיים למידע אגרגטיבי ואנונימי.** על מנת לפתח מודלים של בינה מלאכותית, נדרשת גישה למידע רב על פני זמן, ועל כן מוצע לאפשר גישה כאמור, למשל ביחס למאגר נתוני אשראי או ביחס לנתונים שניתן להנגיש מכוח רפורמת הבנקאות הפתוחה. בנק ישראל מסתייג מהמלצה זו.
- **מוצע לבחון כיצד אפשר למנוע מבעוד מועד את התפתחותו של כוח שוק בתחום מתן שירותי בינה מלאכותית.** אפשרויות שניתן לשקול בהקשר זה הן לקבוע הוראה רגולטורית לפיה נותן שירותי בינה מלאכותית אחד לא יעניק שירות לשחקנים שמחזיקים במצטבר מעל נתח שוק מסוים בשוק ספציפי, או חובה ששחקנים בשוק מסוים או בעלי מאפיינים מסוימים, יידרשו לעבוד עם יותר מנותן שירותי בינה מלאכותית אחד.

סיכונים תפעוליים ובהם סיכוני סייבר, סיכוני צד שלישי, הונאה ודיסאינפורמציה ("מידע כזב")

ההתפתחות והזמינות של כלי הבינה המלאכותית תורמות לגידול בסיכונים התפעוליים המאיימים על גופים פיננסיים, ובהם סיכוני סייבר, סיכוני צד שלישי, סיכוני הונאה ודיסאינפורמציה (מידע כזב). כלים של בינה מלאכותית עשויים להיות זולים יותר, נגישים יותר ואפקטיביים יותר עבור תוקפים המבקשים לפגוע במערכת הפיננסית או בציבור. מתוך הסיכונים התפעוליים העלולים להתממש כתוצאה מכניסתה של בינה מלאכותית לסקטור הפיננסי, ראה הצוות לנכון לייחד מקום מיוחד **לסיכוני דיסאינפורמציה** המעוררים חששות רבים, ועל כן בחן באופן מפורט יותר את השלכותיהם על הסקטור הפיננסי.

מניפולציה ושיבוש שיטתי של מידע, המכונים פעמים רבות גם "דיסאינפורמציה" או "ידיעות כזב", הינם תופעה רווחת בעידן הדיגיטלי, שמטרתה להשפיע על תוכן המופץ ברשת או אמצעים דיגיטליים אחרים, וכפועל יוצא גם על ההחלטות המתקבלות על בסיס אותו מידע.

סיכון הדיסאינפורמציה נתפש כאחד הסיכונים המשמעותיים בהתפתחותה של הבינה המלאכותית. ביחס לתחום הפיננסי הוא עלול להיות רלוונטי במיוחד הואיל והחלטות הציבור הרחב לגבי פעילותו הפיננסית, כמו גם המסחר בשווקים ופעילותם של גופים פיננסיים גדולים, מבוססים על קבלת מידע מהימן בהיקפים גדולים ובתדירות גבוהה ועל אמון הציבור בגופים ובמערכת הפיננסית. משכך, תחומי פעילות אלה (כמו גם תחומי פעילות אחרים המושתתים על קליטה ועיבוד של מידע רב) רגישים במיוחד לתופעת הדיסאינפורמציה, והתממשות סיכון הדיסאינפורמציה בהיקף נרחב עלולה לגרום לא רק נזק לכספי משקיעים ולקוחות, אלא גם לפגוע ביציבות המערכתית.

הדוח מציג אזורי בהם נדרשת תשומת לב רגולטורית מיוחדת בנדון: פעילויות פיננסיות בהן עשויות להתקבל החלטות מהירות על-ידי הציבור הרחב; פעילויות פיננסיות המתאפיינות בתמחור רציף על בסיס מידע; מוסדות פיננסיים החשופים לסיכוני הדבקה (contagion) וקישוריות (inter-connectedness); גופים פיננסיים העושים שימוש במערכות בינה מלאכותית לצורך פעולות פיננסיות מהירות; ושימוש בבינה מלאכותית על מנת לעקוף מנגנוני אבטחה.

להלן עיקרי המלצות הצוות בנושא סיכונים תפעוליים ובהם סיכוני סייבר, סיכוני צד שלישי, הונאה ודיסאינפורמציה:

מוצע לערוך מיפוי של הפעילויות שיש להן חשיפה מיוחדת לסיכון דיסאינפורמציה ולבדוק אם הכלים הקיימים להתמודדות עם סיכון זה מספקים או שיש מקום לשכללם. בין הכלים הרגולטוריים שמוצע לבחון בהקשר זה לשם מיפוי הסיכונים והתמודדות עימם:

- **הנחיית גופים מפוקחים להעריך את סיכון הדיסאינפורמציה, כחלק מסיכוני סייבר, ונאותות הכלים והבקורות**

הקיימים אצלם להתמודדות עם סיכון זה.

- **קביעת מנגנונים או בחינת מנגנונים קיימים להתמודדות עם סיכונים דיסאינפורמציה בגופים הרלוונטיים,** כגון הוראות ונהלים העוסקים בסיכונים סיבר בקרב גופים מפוקחים, או מנגנון מנתק הזרם ביחס לפעילות המסחר בבורסה.
- **הגברת מודעות הציבור לסיכונים דיסאינפורמציה,** באמצעות פרסום הסברים, אזהרות, ופעולות נוספות של חינוך פיננסי.
- **היערכות מוקדמת אצל הרגולטורים הפיננסיים עצמם להתמודדות עם אירועי דיסאינפורמציה** (בדומה להיערכות מוקדמת להתנהלות בשעת חירום).
- **הוספת תרחישים של התממשות סיכונים דיסאינפורמציה לנהלי התמודדות עם סיכונים סיבר והיערכות לשעת חירום וכן לתרגולים המתבצעים על-ידי הרגולטורים הפיננסיים והמערכת הפיננסית ביחס להתנהלות בשעת חירום.**
- **שכלול יכולות החקירה של אירועי דיסאינפורמציה כתוצאה מפעילות בינה מלאכותית.** בפרט יש חשיבות לכך ביחס לפעילות מסחר בניירות ערך שעשויה להיות רגישה במיוחד לאירועים אלה. בהקשר זה, יש מקום להמשיך בקידום הצעות חוק הנמצאות על המדוכה שנועדו לסייע באכיפה של עבירות לפי חוק העונשין וחוק המחשבים בתחום ניירות הערך.
- **בחינת קביעת סמכויות בדין הכללי להסרת תכנים כוזבים ופנייה לגורם המוסמך בהקשרים הללו.**

ו. תחומי פעילות פיננסיים שנבחנו על-ידי הצוות באופן ספציפי

הצוות בחן שלושה תחומי פעילות ספציפיים – ייעוץ השקעות וניהול תיקים; אשראי במערכת הבנקאית; חיתום ביטוח. לגבי תחומים אלה מציג כל אחד מהרגולטורים הפיננסיים את האופן בו הוא רואה שימושים אפשריים ליישומי בינה מלאכותית בתחום שתחת פיקוחו, מהי המסגרת הרגולטורית הרלוונטית, סוגיות לטיפול, והמלצות ראשוניות.

ייעוץ השקעות וניהול תיקים

לבינה מלאכותית עשויים להיות שימושים רבים ומגוונים בפעילויות של ייעוץ השקעות וניהול תיקים. שימושים אלה, הנסקרים בדוח, יכולים להשתרע למעשה על כלל הפעולות המקצועיות הנוגעות למתן הייעוץ או לניהול כספי הלקוח, וכן על פעילויות עסקיות נוספות של בעלי הרישיון כגון שיווק וקשר עם לקוחות או מנגנוני ציוד לדיון. רשות ניירות ערך נדרשה בשנים האחרונות לטפל בפעילות ייעוץ השקעות וניהול תיקים הנעשית בעזרת אלגוריתמים. במסגרת הוראת שירותים תוך שימוש באמצעים טכנולוגיים קבעה הרשות כיצד ניתן לשלב בינה מלאכותית בשלושת שלבי השירות – בירור צרכים והתקשרות בהסכם; קביעת מדיניות ההשקעה ורמת הסיכון של הלקוח; ומתן השירות השוטף. ההוראה מטפלת בין השאר בסוגיות של מיומנות, בקורות, אחריות, הסבר ללקוח, ומעורבות אנושית. הדוח כולל סקירה של הוראה זו ושל דין השוואתי רלוונטי, וכן ניתוח היתרונות והסיכונים בשילוב של בינה מלאכותית בפעילות של ייעוץ השקעות וניהול תיקים. יתרונות מרכזיים הם הרחבת והנגשת השירותים למספר גדול הרבה יותר של לקוחות; החיסכון הצפוי בעלויות מתן השירותים; והפוטנציאל לשיפור השירותים עצמם והתהליכים הנלווים להם אצל נותני השירותים. סיכונים מרכזיים הם אי עמידה בחובות אמון וזהירות והתממשות ניגודי עניינים פוטנציאליים; סיכונים משחקיות (Gamification); חשש לפגיעה באיכות השירות; וחשש לריכוזיות ותלות במספר קטן של מערכות. **להלן עיקרי המלצות הצוות בנושא ייעוץ השקעות וניהול תיקים:**

- **עידוד אקטיבי של הטמעת טכנולוגיית בינה מלאכותית בקרב בעלי רישיון ייעוץ השקעות וניהול תיקים במטרה להגדיל את מספר הלקוחות המקבלים שירותים אלה.** זאת בין היתר באמצעות פעולה פרטנית מול שחקנים קיימים ופוטנציאליים, פרסום מדריך המעודד ומסביר כיצד לבצע את השירות, ונקיטת אמצעים נוספים לקידום ודאות רגולטורית וחדשנות.
- **עדכון הוראת שירותים מקוונים.** מוצע לשקול הוספת פרק להוראה שיעסוק בטכנולוגיית בינה מלאכותית עכשווית, להבהיר עוד מהם תפקידם של בעל הרישיון הממונה (האחראי למתן השירותים הטכנולוגיים), לשקול התייחסות למערכות בינה מלאכותית שאינן מופעלות בממשקים עם הלקוח, ולשקול התייחסות לשימוש בצ'אט-בוטים.

- **בחינת פעילות של צ'אט-בוטים בייעוץ השקעות וניהול תיקים והרגולציה שצריכה לחול בעניינה.** בדוח מוסברים האתגרים הרגולטוריים הנובעים מפעילות זו, גם על רקע ההתפתחות של מודלים גדולים של שפה (Large Language Models).
- **הבהרת הדין ביחס למערכות כלליות של בינה מלאכותית,** כלומר ביחס למערכות העשויות לשמש לצרכים שונים, אך גם לייעוץ השקעות וניהול תיקים.
- **קידום מחקר לבחינת התנהלות לקוחות מול מערכות ממוחשבות.** מחקר בנוגע להתנהלות לקוחות המשתמשים במערכות בינה מלאכותית וקבלת החלטות אוטומטית נדרש לשם פיתוח השוק, הבנת ההשפעה של הטכנולוגיה על התנהגות המשקיעים, והערכת הרגולציה הקיימת והנדרשת לגבי הפעילות.
- **הסדרת תחום שירותי המסחר (ברוקראז').** בהינתן הקשר ההדוק בין פעילות ברוקראז' ובין פעילות של ייעוץ השקעות וניהול תיקים, והשימושים הנרחבים שיכולים להיות לבינה מלאכותית בפעילות ברוקראז', יש מקום להסדיר מקטע זה של הפעילות בניירות ערך, כדי שניתן יהיה לקדם את הפעילות ולהסדיר אותה באופן מלא ועקבי.

אשראי במערכת הבנקאית

יישומים של בינה מלאכותית יכולים לשמש בתחום האשראי בקשת רחבה של נושאים כגון איתור צרכי הלקוח, חיתום אשראי, דירוג אשראי וניהול האשראי באופן שוטף. ההנחה היא כי השימוש בבינה מלאכותית הוא אבולוציה מתבקשת של המודלים הסטטיסטיים הקיימים כיום בתחום האשראי.

בדוח מתואר תחום האשראי והאסדרה החולשת עליו, השימושים האפשריים של בינה מלאכותית בתחום זה בשוק הישראלי, ישימותה של הרגולציה הקיימת בנוגע אליהם, והסוגיות המתעוררות בנדון.

להלן עיקרי המלצות הצוות בנושא אשראי במערכת הבנקאית:

- **שימוש באסדרה הקיימת לניהול סיכונים והגנות צרכניות** – מוצע לדבוק באסדרה הקיימת מקום בו היא מתאימה לטיפול גם באתגרי הבינה המלאכותית, לצד הבהרות שיעניקו ודאות לשוק בהיבטים כגון הסברתיות, אפליה וכדומה. בפרט מוצע לדבוק בגישת ניהול הסיכונים המקובלת בפיקוח בתחום. ההוראות הקיימות בדבר הגנות צרכניות, ניהול סיכונים וניהול מודלים מספקות מעטפת אסדרתית מספקת, אם כי ייתכן שיידרשו הבהרות מצד המאסדר ביחס לגורמים מגבירי ומפחיתי סיכון והכלים להתמודד עימם, כפי שמפורט בפרק ניהול הסיכונים בדוח.
- **סיכוני אפליה והדרה** – בהמשך לאתגרים שנדונו בנוגע לאפליה, ישנן הוראות ספציפיות בנדון בתחום האשראי, למשל בכל הנוגע לנתונים שניתן ואסור לשקול לצורך קביעת דירוג אשראי. מוצע לשקול הבהרה, כי שימושי בינה מלאכותית אינם משנים מן הדין הקיים, ועל המוסדות הפיננסיים להבטיח, בטרם השימוש בכלי בינה מלאכותית, כי בידיהם הכלים להקפיד על האסדרה בתחום – כגון אי שימוש במשתני פרוקסי לנתונים שאסור לשקול לפי חוק נתוני אשראי.
- **חשש מ"דחיפת" אשראי** – אחד החששות המתוארים בדוח הוא שימוש בטכנולוגיה לשם שיווק אגרסיבי של אשראי ללקוח. בהקשר זה מוצע לשקול גילוי בדבר שימוש בבינה מלאכותית לצורך זה, אשר יוכל לשמש הן את הלקוח הן את הרגולטור.

חיתום ביטוח

חיתום הוא התהליך שבו חברת הביטוח מעריכה את הסיכון של כיסוי ביטוחי מסוים. גורמים מרכזיים בתהליך זה הם בחינת מאפייני הלקוח, מאפייני הכיסוי הביטוח שהוא רוכש, תמחור הפרמיה ומאפייני ביטוח המשנה. תהליך החיתום נועד לוודא שהפרמיה תהלוּם את הסיכון הביטוחי, והוא נעשה תוך שימוש במודלים אקטואריים המבוססים על כלים סטטיסטיים ואלגוריתמים, כך שטכנולוגיה בינה מלאכותית עשויה להיות שימושית בענייננו.

בדוח מתואר תהליך חיתום הביטוח, הנחלק לבניית מודל החיתום הכללי ולחיתום הלקוח או העסקה הפרטניים, ושימושים פוטנציאליים של בינה מלאכותית במסגרתו. הסוגיות המתעוררות לגבי תהליך זה נדונו גם באופן רחבי בדוח, והן כוללות סיכונים קופסה שחורה והעדר הסברתיות, פרטיות, אפליה, סיכונים מודל, וסיכונים מערכות מידע וסייבר. הכלים להתמודד עם אתגרים אלה כוללים תהליכי ניהול סיכונים המהווים חלק בלתי נפרד מעבודתן של חברות הביטוח, כמו גם כלים נוספים שנדונו בדוח כגון ממשל בינה מלאכותית, יידוע וגילוי.

להלן עיקרי המלצות הצוות בנושא חיתום ביטוח:

- **שימוש באסדרה הקיימת לניהול סיכונים והגנות צרכניות** – ככלל האסדרה הקיימת היא ניטרלית מבחינה טכנולוגית, ועל כן חברת ביטוח הבוחרת לאמץ בינה מלאכותית צריכה לפתח וליישם את הטכנולוגיה בהתאם לאסדרה הקיימת.
- **עדכון האסדרה מקום בו הטכנולוגיה מחייבת התייחסות מיוחדת** – תחומים עיקריים בהם נדרשת בחינה בדבר עדכון האסדרה הם ניהול סיכונים מודל, הסברתיות, יידוע וגילוי (למשל יידוע על השימוש בבינה מלאכותית כאמצעי קשר עם הלקוח בצ'אט בוט). בנוסף לכך, יש לבחון את דרכי הפיקוח והבקרה על חברות הביטוח והכלים העומדים לרשותו של הרגולטור – למשל, האם כלי הפיקוח לבדיקת כניסה של מוצר ביטוחי חדש, הם מספקים לבחינה של החלטות אשר התקבלו במערכת בינה מלאכותית.

ז. פעולות נוספות לקידום רגולציה פיננסית בתחום הבינה המלאכותית

הפרק האחרון בדוח אינו נוגע לסוגיה מסוימת בפעילות של בינה מלאכותית (הסברתיות, אפליה, וכן הלאה) או לסוג מסוים של פעילויות (ייעוץ השקעות, אשראי וכדומה), אלא לפעולות תשתיות הנדרשות בצד הרגולטורי כדי להפוך את הרגולציה הפיננסית בתחום הבינה המלאכותית למתקדמת ואפקטיבית. ההמלצות הכלליות בפרק זה נחלקות לשלושה מישורים: עידוד חדשנות; קידום ודאות רגולטורית והתאמות בדין; וקידום הפעילות הפיקוחית.

להלן עיקרי המלצות הצוות בהיבטים אלה:

עידוד חדשנות

- עדכון הצעת החוק הממשלתית שעניינה "ארגז חול רגולטורי" בסקטור הפיננסי, המניחה אסדרה ייעודית ואחודה עבור כלל הרגולטורים הפיננסיים להקמת סביבת ניסוי, והרחבתה לשם הגברת האפקטיביות הפוטנציאלית שלה.
- לצד קידום הצעת החוק האמורה, מוצע להקים "ארגזי חול" עצמאיים על ידי כל רגולטור פיננסי בתחום אחריותו, וליזום תיקוני חקיקה בדינים הפיננסיים הרלוונטיים כדי לאפשר זאת מקום בו הדין הקיים אינו מתיר זאת.
- הקמת מוקדי חדשנות על-ידי הרגולטורים הפיננסיים והקדשת משאבים ומיקוד פעילות בתקופה הקרובה ביישומי בינה מלאכותית.
- בחינת פתרונות לבעיית הנגישות למידע, בפרט של גופים קטנים או חדשים, כגון הקמה ופתיחה של מאגרי מידע כבסיס לפעילות בינה מלאכותית.

קידום ודאות רגולטורית והתאמות בדין

- הגברת הוודאות הרגולטורית בתחום הבינה המלאכותית באמצעות כלים כגון מסמכי מדיניות, מענה לפניות מקדמיות, עמדות פרשניות, שאלות ותשובות, פרסום מדריכים ואזהרות.
- יש לשאוף לכך שהאסדרה בחוק ובתקנות תשקף את העיקרון של ניטרליות טכנולוגית ותתיר גמישות לפעול באמצעים טכנולוגיים שונים. כמו-כן, ומבלי לגרוע מסמכויות קיימות של הרגולטורים הפיננסיים, מוצע לשקול הקניית סמכויות רגולטוריות לתת הוראות נדרשות על רקע שינויים בטכנולוגיה, להעניק פטורים, ולקבוע הוראות שעה וסעיפי שקיעה (sunset provisions), לשם התאמת הדין לפעילות והגברת הוודאות המשפטית, מקום בו הדבר נדרש.

קידום הפעילות הפיקוחית

- קידום פעילות פיקוחית המבוססת על טכנולוגיית בינה מלאכותית (Suptech), באמצעות בחינתה כחלק מהאסטרטגיה הכוללת של הרגולטור בנושא מערכות מידע ורתימתן לצרכי פיקוח ואכיפה.
- הפניית משאבים ממשלתיים, מחוץ למסגרות התקציב הרגילות, כדי לקדם פעילות פיקוחית מבוססת בינה מלאכותית.
- בחינת עדכון סמכויות קבלת מידע לצרכים של ניתוח, פיקוח ואכיפה.
- התמודדות באופן סדור ומרוכז עם סוגיות רוחב הקשורות בשימוש בבינה מלאכותית על-ידי המדינה / על ידי רשויות ציבוריות ועיצוב מתכונת טיפול אחידה.
- רתימת משאבים של הרגולטורים הפיננסיים, עידוד התיאום ביניהם, והמשך עבודה משותפת בנושא.

חלק א'

רקע, התפתחויות ומגמות רגולטוריות



א. כניסתה של הבינה המלאכותית לחיינו

נדמה כי הבינה המלאכותית פרצה לחיינו רק בעת האחרונה, אולם למעשה העיסוק בשיוך יכולות אנושיות למכונות, ובכלל זאת אינטליגנציה אנושית, החל כבר בשנות החמישים של המאה העשרים.¹ הביטוי "בינה מלאכותית" (Artificial Intelligence או בקצרה AI) נטבע ככל הנראה לראשונה בידי קבוצת חוקרים אמריקאים במסגרת הצעה לעבודת מחקר בקולג' של דארטמות' בשנת 1955.² כבר אז הניחו החוקרים שכל צורה של למידה או ביטוי של אינטליגנציה אנושית ניתנים לתיאור מדויק באופן שיאפשר למכונה לחקותו.³

בחלוף הזמן, חלה התקדמות משמעותית בתחום הבינה המלאכותית ובפרט במחקר האקדמי שלה, בעיקר כתוצאה מהתפתחות כוח המחשוב לצד גידול חד בזמינות מידע ונתונים והיכולת לעבדם בעלויות נמוכות מבעבר.⁴ בשנות התשעים של המאה ה-20 החל להתפתח בצורה משמעותית תחום למידת המכונה (machine-learning),⁵ המהווה ענף של בינה מלאכותית, ובעשור הראשון של המאה ה-21 החל לקבל הכרה תחום הלמידה העמוקה (deep-learning),⁶ המהווה בתורו מקרה פרטי של למידת מכונה.

לאחרונה אנו עדים להתפתחות משמעותית נוספת בעולמות הבינה המלאכותית בדמות הבינה המלאכותית היוצרת (Generative Artificial Intelligence), טכנולוגיה המאפשרת יצירה של תוכן חדש, לרבות טקסט, תמונה, תחזיות ועוד. ההבדל העיקרי בין בינה מלאכותית יוצרת לבין בינה מלאכותית מסורתית (או "רגילה", קרי כזו שאינה יוצרת), טמון בכך שהראשונה, כפי שמרמז שמה, מסוגלת לייצר תוכן מקורי, ובמקרים רבים קשה לזהות אם תוכן זה נוצר בידי מערכת מחשב או אדם בשר-ודם. זאת בעוד שבינה מלאכותית מסורתית נועדה בעיקר לזיהוי תבניות, סיווג וניבוי תחזיות על סמך מידע קיים. הבינה המלאכותית היוצרת מבוססת על מודל שפה גדול (Large Language Models או LLM), ובפרט עיבוד שפה טבעית (Natural Language Processing או NLP).

קו פרשת המים שסימל את פריצת הבינה המלאכותית בראיית הציבור הרחב, היה השקתו של Chat GPT על-ידי חברת OpenAI. אפליקציה זו גייסה לא פחות ממאה מיליון משתמשים במהלך החודשים נובמבר-דצמבר בשנת 2022, ועמדה לתקופה קצרה בראש הדירוג כאפליקציה שהשיגה את מספר המשתמשים בזמן הקצר ביותר.⁷ מספר ענקיות טכנולוגיה הציגו מאז חידושים ופיתוחים בתחום הבינה המלאכותית, ובפרט הבינה המלאכותית היוצרת, ונדמה שמדובר במהפכה של ממש. הערכות של גורמים העוסקים בנושא הן כי שימוש בכלי בינה מלאכותית בארגונים ישפר את תפוקת עובדים בכ-40% בעשור הקרוב.⁸ לפי חברת הייעוץ האסטרטגי McKinsey & Company, בינה מלאכותית יוצרת לבדה עשויה להוסיף לכלכלה העולמית כ-3.5 טריליון דולר בממוצע לשנה במקרי הבוחן שנבדקו (לשם ההשוואה, סכום זה גבוה יותר מהתמ"ג השנתי של בריטניה).⁹

1 Artificial Intelligence in The Financial Sector – Open Innovation and Ethical Commitment, Everis (2021). https://www.nttdata.com/global/en/-/media/nttdataglobal/1_files/services/data-and-intelligence/artificial_intelligence_in_the_financial_sector.pdf?rev=704e0e643b6b4f3bbd1ef22b04cdcd3e

2 A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, John McCarthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon (August 31, 1955), http://jmc.stanford.edu/articles/dartmouth.html?force_isolation=true; יש המתגרים קביעה זו בציינם שהנושא נחקר עוד קודם לכן, גם אם לא תוך שימוש במונח "בינה מלאכותית", ראו למשל <https://sites.harvard.edu/sitn/2017/08/28/history-artificial-intelligence/>.

3 שם, בעמוד 1. "The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves."

4 OECD (2021), Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, <https://doi.org/10.1787/98e761e7-en>.

5 תחום למידת המכונה מתמקד בפיתוח אלגוריתמים ומודלים המאפשרים למערכות מבוססות מחשב "ללמוד" ממידע שהוכנס להן כקלט, ובהתבסס על הקלט לייצר תוכן, הערכות, המלצות או החלטות באופן עצמאי.

6 תחום הלמידה העמוקה מתמקד בפיתוח אלגוריתמים ומודלים בניסיון לחקות פעולות של מוח אנושי באמצעות רשתות עצביות מלאכותיות (artificial neural networks) לעיבוד מידע באמצעות שכבות.

7 לשם ההשוואה, פייסבוק (כיום Meta) הגיעה למאה מיליון משתמשים רשומים כעבור ארבע וחצי שנים ממועד השקתה, יוטיוב הגיעה למאה מיליון משתמשים תוך ארבע שנים ממועד השקתה ואינסטגרם עשתה כן תוך שנתיים וחצי ממועד השקתה. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/?force_isolation=true; <https://www.forbes.com/sites/siladityaray/2023/07/10/with-100-million-users-in-five-days-threads-is-the-fastest-growing-app-in-history/?sh=269b58e649ab>;

8 <https://mitsloan.mit.edu/ideas-made-to-matter/how-generative-ai-can-boost-highly-skilled-workers-productivity>

9 <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights>.

ככל שטכנולוגיית הבינה המלאכותית מתפתחת, ניתן לראות את כניסתה ההדרגתית לתחומי חיים רבים ומגוונים. כך למשל, מערכות בינה מלאכותית מייצעות בבחירת סרטים או סדרות בהתאם להעדפות ההיסטוריות של הצופה, מסייעות ברכישת מוצרים ברשת האינטרנט, קובעות לאיזה תוכן ולאילו פרסומות ייחשפו הגולשים ברשתות חברתיות, מבצעות ניתוח של הדמיות רפואיות, משולבות בכלי רכב אוטונומיים ועוד. כניסתן של מערכות בינה מלאכותית יכולה, לפחות ברמה הפוטנציאלית, להציע את האנושות לעבר השגת יעדים שטרם נראו כמותם: מכונות אוטונומיות יוכלו להפחית את מספר תאונות הדרכים ועומסי התנועה; מכשור רפואי יוכל לסייע באיתור ואבחון מחלות בשלבים מוקדמים יותר ואף לסייע בפיתוח תרופות; מערכות מסחריות יוכלו לשפר תהליכים עסקיים, שרשראות אספקה, להגביר אפקטיביות של עובדים ולסייע במשימות שנעשו עד כה על ידי בני אנוש בלבד; וכן הלאה. לצד היתרונות, כניסתן של מערכות בינה מלאכותית, ובפרט בינה מלאכותית יוצרת, מעוררת חששות רבים, כגון אובדן משמעותי של משרות – בין היתר בעולמות הייצור, התפעול, הייעוץ, התחבורה, שירות הלקוחות, הרפואה ועוד; פגיעה בפרטיות – שהרי מערכות בינה מלאכותית מבוססות על מידע עתק שנאסף ממאגרי מידע שונים, והצלבתם עלולה להביא לחשיפת מידע על המשתמשים; שימוש לרעה בטכנולוגיה – כמו למשל מעקב אחר אזרחים על ידי ממשלות, יצירת כלי נשק אוטונומיים, פשיעה, אפליה ועוד.

על מנת שניתן יהיה להנות מהיתרונות הגלומים בבינה מלאכותית, יש להבטיח אם כן שהשימוש בה ייעשה באופן אחראי, הוגן וראוי. זאת, בין היתר, באמצעות רגולציה מאפשרת ותומכת בחדשנות מחד, אשר פועלת להפחתת הסיכונים הכרוכים בשימוש בבינה מלאכותית מאידך.

בתקופה שחלפה מאז פרסום דוח הביניים אפשר היה לראות את המשך המגמה של השקעות ניכרות בתחום הבינה המלאכותית, פיתוח יכולות מתקדמות יותר, והטמעת מערכות בינה מלאכותית בפעילויות עסקיות מגוונות. על ההתפתחויות בתחום ניתן למנות שיפור של יכולות ההסבר (reasoning) והניתוח של מודלים; פיתוח סוכני בינה מלאכותית (AI Agents), קרי מערכות או ישויות אוטונומיות הפועלות בסביבה מסוימת, מעבדות נתונים, מקבלות החלטות באופן עצמאי ומבצעות פעולות בהתאם למטרות שהוגדרו להן¹⁰; ופיתוח מודלים של בינה מלאכותית גם מחוץ לארה"ב, ובפרט מודל DeepSeek שהושק בסין ומופעל באמצעות כוח מחשוב נמוך משמעותית מזה שהיה מקובל קודם לכן.

תיבה 1: בינה מלאכותית – מילון מונחים

בינה מלאכותית (Artificial Intelligence): תחום במדעי המחשב העוסק בפיתוח מערכות ממוחשבות המסוגלות לבצע משימות המדמות יכולות קוגניטיביות אנושיות כגון למידה, זיהוי דפוסים, יצירת תחזיות או פתרון בעיות וקבלת החלטות.

למידת מכונה (Machine Learning): תת-תחום מרכזי של בינה מלאכותית המתמקדת ביכולתן של מערכות מחשב "ללמוד" ללא תכנות מפורש. זאת על ידי פיתוח מודלים סטטיסטיים המאפשרים למערכות ממוחשבות לבצע משימות מורכבות ללא תכנות מפורש של כל תרחיש אפשרי, באמצעות חשיפה לכמויות גדולות של נתונים (זיהוי דפוסים, יצירת תחזיות ועוד). יישומי למידת מכונה הם מגוונים וכוללים, בין השאר:

- **סיוע או קבלת החלטה ספציפית** – למשל, האם לאשר או לדחות בקשה של לקוח לאשראי לנוכח סיכויי החזיר את ההלוואה או האם לאפשר עסקה או פעולה פיננסית לאחר שנבחנו חששות להונאה.
- **סיוע בביצוע משימות מתמשכות ורחבות** – למשל, לצורך מערכות נהיגה אוטונומיות או צ'אט-בוטים.

למידה עמוקה (Deep Learning): תת-תחום מתקדם של למידת מכונה. היא מתבססת על רשתות עצביות מלאכותיות רב-שכבתיות, המחקות את מבנה המוח האנושי. שיטה זו מאפשרת למערכות

ללמוד ייצוגים מופשטים של נתונים, לזהות תבניות מורכבות, ולבצע משימות כמו זיהוי תמונות, עיבוד שפה טבעית, ותרגום אוטומטי ברמה גבוהה במיוחד. למידה עמוקה הובילה לפריצות דרך משמעותיות בתחומים רבים של בינה מלאכותית, ומהווה את הבסיס למערכות ה-AI המתקדמות ביותר כיום.

אלגוריתמים: ליבת למידת המכונה. אלגוריתמים מהווים סדרת הוראות שהמחשב מבצע כדי לפתור בעיה או להשלים משימה שהוגדרה לו. בניגוד לגישה המסורתית בה פעולת האלגוריתמים תוכננה והוגדרה מראש, בלמידת מכונה, האלגוריתמים מתוכננים ללמוד מדוגמאות, לנתח נתונים, לזהות דפוסים ולהשתמש במידע שנלמד כדי לייצר תובנות או תחזיות.

נתוני עתק (Big Data): מסדי נתונים מגוונים, מובנים ובלתי מובנים, שמצטברים מהר בהיקפים גדולים שלא ניתן לעבד בכלים מסורתיים כדוגמת מחשב אישי וגיליונות אקסל. איסוף נתוני עתק המתבצעת באופן מהיר וממקורות מידע מגוונים כגון נתונים הקיימים בארגון, איסוף מן האינטרנט, "טביעות רגל" דיגיטליות וכדומה. ארגונים וחברות מנתחים נתוני עתק כדי להפיק מהם ערך – ללמוד כיצד ניתן לייצל את עבודתם, לשפר הצעות ללקוחות ועוד.

מה בין AI, ML ומודלי חיזוי אחרים: שימוש במודלים לצרכי חיזוי אינו דבר חדש אלא פרקטיקה ותיקה בעולם המחקר וניתוח נתונים. שיטות סטטיסטיות וכלים מתמטיים, כגון רגרסיה ליניארית, שימשו ועודן משמשות לזיהוי קשרים בין משתנים ולייצור תחזיות. רגרסיה ליניארית, למשל, מאפשרת לבחון קשרים קורלטיביים או סיבתיים בין משתנים ומסייעת בבניית מודלים ליצירת תחזיות. ואולם, התפתחויות טכנולוגיות משמעותיות, ובראשן גידול עצום בזמינות נתונים דיגיטליים (נתוני עתק) ועלייה דרמטית בכוח מחשוב, הובילו לפריצת דרך בתחום למידת המכונה, ובעיקר אפשרו ניתוח של מסדי נתונים בהיקפים חסרי תקדים ויצירת הקשרים יותר מורכבים ומהירים בין משתנים. הדבר הוביל להתפתחות מודלים מתוחכמים יותר ולשילובם במגוון רחב של תחומים.

תפקיד הגורם האנושי: במודלים מסורתיים, מומחה אנושי מגדיר מראש את הקשר בין משתני הקלט (input) למשתנה היעד (target variable – המשתנה שאותו מבקשים לחזות) – כלומר עד כמה נתונים מסוימים קשורים למשתנה היעד. במודלי למידת מכונה, לעומת זאת, למערכת מוזנים משתני הקלט ומשתנה היעד ואז באמצעות אלגוריתמים סטטיסטיים מתקדמים המערכת לומדת "עצמאית" את הקשרים בין משתני הקלט למשתנה היעד ויוצרת מודל חיזוי.

גמישות והסתגלות: מודלי למידת מכונה מאופיינים בגמישות רבה יותר בזיהוי קשרים מורכבים שלגורם אנושי היה קושי לזהות באופן ידני. בנוסף מודלי למידת מכונה, כשמן כן הם – לומדים. מודלי למידת מכונה מסוגלים להשתפר באופן דינמי בעקבות חשיפה למידע חדש – הם מסוגלים לעדכן את תהליך יצירת התחזיות ומבנה המודל עצמו, לרבות הוספת משתנים חדשים, עדכון המשקולות של משתנים קיימים, זיהוי והסרת משתנים שאינם רלוונטיים עוד וכדומה. עם זאת, מודלי למידת מכונה מתאפיינים לרוב כ"קופסאות שחורות" – מנגנון קבלת ההחלטות שלהם מורכב ולעתים קשה להבנה עבור בני אדם. מגבלה זו עלולה להקשות על השימוש בהם בהקשרים מסוימים, שבהם נדרשת שקיפות בתהליך קבלת ההחלטות.

למידה מופקחת, שאינה מופקחת, ולמידת חיזוק supervised, unsupervised and reinforcement (learning):

- **למידה מופקחת** – שיטת למידת מכונה בה ממדלים אמפירית את היחס בין נתוני קלט למשתנה היעד. בתהליך למידה מופקח, למודל מוזנים נתונים "מתויגים" (labelled) – כלומר נתוני קלט כבר מתויגים לפי הקשר שלהם למשתנה היעד. למשל – אם מעוניינים לאמן מודל לחזות הונאה, מסד הנתונים יכול להיות נתוני קלט, כגון מאפייני עסקאות (מיקום, שעה, סכום וכו') שהתבררו בדיעבד ככשרות לצד עסקאות שהתבררו כהונאה והמודל יחלץ מתוכם את המשקל שיש לתת לכל משתנה בניסיון לסווג בצורה אופטימלית עסקה מסוימת כהונאה. לאחר מכן ניתן יהיה להזין למודל נתוני קלט חדשים והמודל יתייג אותם או יחזה באמצעותם את הסיכוי להונאה על בסיס מה שלמד. למידה מופקחת נפוצה בזיהוי הונאות, זיהוי דואר זבל, ניהול סיכונים ודירוג אשראי.

- **למידה שאינה מפוקחת** – למודל מסוג זה מוזנים נתונים לא מתויגים והמודל מתוכנת למצוא בהם, בעזרת שיטות סטטיסטיות, דפוסים בלי פיקוח אנושי ולקבץ קבוצות נתונים הדומים זה לזה בתוך כל קבוצה ושונים זה מזה בין הקבוצות. בדוגמא של מקרי ההונאה, למשל, המקרים שהתבררו כעסקאות או פעולות הונאה לא יהיו מתויגים ככאלה אלא רק יוזנו פרטי העסקאות. טכניקה זו משמשת, בין השאר, לזיהוי אנומליות במסדי נתונים – שבשלב מאוחר יותר יכולות לעזור בזיהוי הונאות או תופעות חריגות אחרות.
- **למידת חיזוק** – שיטה בבינה מלאכותית שבה סוכן (כמו תוכנה או רובוט) לומד לפעול בסביבה מסוימת כדי למקסם תגמול. הסוכן מבצע פעולות רבות, מקבל משוב בצורת תגמול (חיובי או שלילי), ולומד לבד עם הזמן אילו פעולות מובילות לתוצאות הטובות ביותר. למשל, סוכן המשחק משחק שחמט לומד אילו אסטרטגיות ומהלכים מובילים לניצחונות רבים יותר, בדיוק כפי ששחקן שחמט משפר את משחקו עם הניסיון. שיטה זו מאפשרת לסוכן ללמוד ולהשתפר באופן עצמאי, ללא תכנות מפורש של כל אסטרטגיה אפשרית. למידת חיזוק משמשת במגוון תחומים כמו משחקים, רובוטיקה וניווט אוטונומי.

שלבים בפיתוח מודל למידת מכונה מפוקחת:

1. בחירת האלגוריתם

בחירת סוג האלגוריתם בהתאם לסוג השימוש שעבורו פותח המודל. שיקולים רלבנטיים הם כמות הנתונים, סוג ההקשרים, הצורך בקבלת הסבר וכדומה.

2. אימון

לאלגוריתם מוזנים נתונים שעל בסיסם מפתח האלגוריתם מודל חיזוי

3. תיקוף המודל

למודל שפותח מוזנים נתונים – שונים מאלו שהוזנו לצורך האימון – על מנת לתקף את המודל. זאת, באמצעות בחינת התוצאות שמתקבלות מהזנת המידע החדש. שלב התיקוף מסייע להעריך את מהימנות המודל.

4. התאמת המודל ובדיקתו

בשלב הבא המודלים מותאמים (tuned) ונבחנים. בין השאר, בוחנים שהמודל לא לוקה ב"התאמת יתר", קרי, שהמודל מותאם בעיקר לנתונים שעליהם אומן ולכן אינו יעיל בביצוע תחזיות מדויקות ביחס לנתונים אחרים. בחינת המודל (validation) נעשית באמצעות הזנת נתונים חדשים לגמרי למודל. בשלב זה ניתן להפעיל את המודל כמודל "צל" – המודל פועל לצד המערכות המסורתיות ונערכת השוואה בין תוצאות המערכות ולערוך התאמות במודל, לתכנן את מדיניות ניהול הסיכונים ועוד.

בינה מלאכותית כללית (Artificial General Intelligence, AGI): ככלל, פיתוח מערכות בינה מלאכותית נעשה לצורך ביצוע משימה מסוימת ומובחנת. בינה מלאכותית כללית מתייחסת למערכות בינה מלאכותית אשר מסוגלות לבצע טווח רחב של משימות ופעולות, מבלי שתוכנתו לבצע משימות או פעולות מסוימות. כלומר, מערכת אשר כבר דומה יותר להתנהגות האנושית – המערכת היא אוטונומית ו"לומדת" את ביצוע המשימה מהסביבה בלי צורך בפיקוח אנושי. כלומר – בעתיד ייתכן שלא יהיה צורך בעיצוב מודל ייחודי ליעוץ השקעות אלא מערכת כללית תוכל ללמוד את המשימה ולבצע אותה.

בינה מלאכותית יוצרת (Generative AI): סוג של למידת מכונה אשר מסוגל לייצר תוכן במדיות שונות: כתיבה, תמונות, מוסיקה ועוד. בינה מלאכותית יוצרת היא תוצר של אלגוריתם המתאמן על כמויות עצומות של נתונים לא מעובדים – דפי אינטרנט, ספרים, תמונות, סרטים, קטעי קול וכדומה, ולומד דפוסים שמאפשרים למודל לייצר תכנים מתאימים בהתאם לשאלות או הוראות שמספקים לו. הבינה המלאכותית היוצרת היא אחת הטכנולוגיות המרכזיות שתורמות לפעולות דיסאינפורמציה. באמצעות טכנולוגיה זו ניתן לייצר, למשל, תמונות וסרטוני deep-fake אשר איכותן מקשה לבדל אותן מתמונות אמיתיות. ישנן טכניקות של למידת מכונה אשר מסוגלות לזהות האם תוצר מסוים הוא אמיתי או מזויף ("פייק"), וזאת גם באמצעות אימון, אך ככל שהבינה המלאכותית היוצרת מתקדמת ומתפתחת, גובר הקושי לזהות תכנים שאינם אמיתיים.

עיבוד שפה טבעית (Natural Language Processing): ענף בתחום הבינה המלאכותית העוסק בעיבוד טקסט כתוב ומדובר תוך הבנת המשמעות העולה מן הדברים. האלגוריתם תר אחר דפוסים באופן שבו טקסט בנוי וכיצד שימוש במילים ובמבנה של הטקסט יוצרים משמעות מסוימות וכך מסייעים ביצירת תוכן עצמאי שמשמש, למשל, בצ'טבוטים וכדומה. חזית הטכנולוגיה בתחום זה כיום היא מודלי שפה גדולים (Large Language Models, LLMs).

תאימות (Alignment): אחד האתגרים בפיתוח מערכות בינה מלאכותית הוא אתגר התאימות, קרי, הצורך לוודא שהמערכת האוטונומית תפעל בהתאם ליעדים שהוגדרו לה ולסט ערכים אנושיים מוגדר מראש. דוגמה נפוצה היא, למשל, כיצד להביא לכך שבינה מלאכותית יוצרת לא תספק מידע עצמאי בהקשרים פסולים מבחינה ערכית – כגון איך לפגוע במישהו או שתעשה שימוש בשפה לא ראויה ועוד.



ב. רגולציה של בינה מלאכותית בארגונים בינלאומיים ובמדינות מפותחות

עם התקדמות הטכנולוגיה וההכרה בקרב מקבלי ההחלטות בעולם בדבר פוטנציאל ההשפעה רחב-ההיקף של בינה מלאכותית על מרבית תחומי החיים, החלו רגולטורים, גופי ממשל וארגונים בינלאומיים לעסוק ביצירת מסגרות רגולטריות לפיקוח על תחום הבינה המלאכותית.

כך למשל, **האיחוד האירופי** החל לעסוק בהיבטים הרגולטוריים של בינה מלאכותית עוד בשנת 2018,¹¹ ולאחרונה הציג את המסגרת הרגולטורית המקיפה ביותר עד כה, ה-EU Artificial Intelligence Act (להלן: "EU AI Act").¹² חקיקה זו צפויה להיכנס לתוקף באופן הדרגתי החל מהמחצית השנייה של שנת 2024 ובאופן מלא עד שנת 2027 בכל המדינות החברות באיחוד האירופי. המדובר במסגרת רגולטורית החותרת לקבוע חקיקה הרמונית בכל הנוגע לפיתוח, הפעלה ושימוש בבינה מלאכותית בעקבות דחיות במועד יישומה בתחומי האיחוד האירופי. החקיקה החדשה מטילה חובות על מפתחי המערכות (כותבי הקוד) ועל מפעילי המערכות,¹³ בין היתר בהתאם לרמת הסיכון הנשקפת מיישומי הבינה המלאכותית בהם נעשה שימוש. נוסח ראשון של החקיקה הוצג בשנת 2021 והחקיקה אושרה ופורסמה באופן סופי ומחייב אך לאחרונה (יולי 2024). בתהליך החקיקה נערכו בהצעה שינויים לא מעטים, חלקם נבעו מההתקדמות הטכנולוגית הרבה שחלה מאז הוצגה לראשונה.

הארגון לשיתוף פעולה ופיתוח כלכלי (OECD) החל לעסוק בהיבטי בינה מלאכותית בשנת 2019, אז פרסם נייר מדיניות העוסק בשימוש בבינה מלאכותית במגזר הציבורי.¹⁴ היה זה מסמך העקרונות הכלליים הראשון שגובש על ידי ארגון בינלאומי מוביל, ובמסגרתו נקבעו עקרונות בתחום השימוש האחראי של בינה מלאכותית (Responsible AI) תחת תפיסה של "האדם במרכז" (Human-Centric Approach). על בסיס עקרונות אלה נקבעו מספר ערכים שיש לפעול לפיהם, ובהם: תרומה של הבינה המלאכותית לפיתוח בר קיימא ורווחה חברתית; כיבוד ערכים השמים את האדם במרכז וערך ההגיונות; השימוש במערכות בינה מלאכותית ואופן פעולתן צריכים להיות שקופים; מערכות בינה מלאכותית צריכות להיות עמידות ובטוחות; נדרשת אחריות לתוצאות של הבינה המלאכותית. בנוסף, במסגרת מסמך זה הוצעו כלי מדיניות שנועדו לקדם עקרון של שימוש בבינה מלאכותית באופן מהימן ואתי (Trustworthy AI). לאחר מכן פרסם הארגון סדרת ניירות מדיניות העוסקים בבינה מלאכותית בחברה,¹⁵ פיננסיים (להלן: "דוח ה-OECD משנת 2021" ו-"דוח ה-OECD משנת 2023", בהתאמה),¹⁶ תחרות,¹⁷ סביבה וקיימות,¹⁸ תעסוקה,¹⁹ ניהול סיכונים,²⁰ טכנולוגיה²¹ ועוד. הגישה הכללית המשותפת לכלל הפרסומים היא השמירה על זכויות אדם תחת התפיסה

- European Commission, High-Level Expert Group on Artificial Intelligence – Draft Ethics Guidelines for Trustworthy AI 11
(December 2019) – <https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai>
- Regulation (EU) 2024/168 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules 12
on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858,
(EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence
Act), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Deployers, ראו בהרחבה סוגיית האחריות (בחלק ג' – סוגיות רוחב להלן). 13
- Berryhill, J., et al. (2019), "Hello, World: Artificial intelligence and its use in the public sector", OECD Working Papers on 14
Public Governance, No. 36, OECD Publishing, Paris, <https://doi.org/10.1787/726fd39d-en>
- OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, <https://doi.org/10.1787/eedfee77-en> 15
- OECD (2023), "Generative artificial intelligence in finance", OECD Artificial Intelligence Papers, No. 9, וגם, 16
ראו ה"ש 4 לעיל, <https://doi.org/10.1787/ac7149cc-en>
- OECD (2017), Algorithms and Collusion: Competition Policy in the Digital Age, https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/05/algorithms-and-collusion-competition-policy-in-the-digital-age_02371a73/258dcb14-en.pdf 17
- OECD (2022), Measuring the environmental impacts of artificial intelligence compute and applications: The AI footprint 18
| en | OECD, <https://www.oecd.org/publications/measuring-the-environmental-impacts-of-artificial-intelligence-compute-and-applications-7babf571-en.htm>
- OECD (2023), OECD Employment Outlook 2023 : Artificial Intelligence and the Labour Market | OECD iLibrary, <https://www.oecd-ilibrary.org/sites/08785bba-en/index.html?itemId=/content/publication/08785bba-en> 19
- OECD (2023), Common guideposts to promote interoperability in AI risk management | OECD Artificial Intelligence 20
Papers | OECD iLibrary, https://www.oecd.org/en/publications/common-guideposts-to-promote-interoperability-in-ai-risk-management_ba602d18-en.html ; OECD (2023), Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI | en | OECD, <https://www.oecd.org/sti/advancing-accountability-in-ai-2448f04b-en.htm>
- OECD (2023), AI language models: Technological, socio-economic and policy considerations | en | OECD, <https://www.oecd.org/sti/advancing-accountability-in-ai-2448f04b-en.htm> 21



של האדם במרכז, לצד קידום חדשנות באופן אתי ומבוקר. להמלצות ה-OECD חשיבות מיוחדת, היות שהן נתפשות כרף בינלאומי המשקף מדיניות מוסכמת גם בקרב מדינות הנוקטות גישות שונות באשר לבניה מלאכותית.²² ארגונים בינלאומיים נוספים כגון **ארגון המדינות המתועשות (G7) ופורום נציגי 20 הכלכלות הגדולות (G20)** פרסמו אף הם הצהרות ומסמכי מדיניות בנושא תהליכים ושימוש בכלי בינה מלאכותית.²³

בתקופה שחלפה מאז פרסום דוח הביניים, נכנסו חלק מהוראות ה-EU AI Act לתוקף, ובכלל זאת הרגולציה החלה על מערכות בסיכון גבוה, הכוללת גם מערכות העוסקות בדירוג וזכאות לאשראי וניהול סיכונים ותמחור בתחום ביטוחי חיים ובריאות. ההוראות שנקבעו ביחס למערכות בינה מלאכותית כלליות (General Purpose AI – GPAI) נכנסו לתוקף באוגוסט 2025. בחודש יולי 2025 פרסמה הנציבות האירופית שלושה מסמכים מרכזיים בנושא בינה מלאכותית כללית: (1) מדריך למפתחי מודלים מבוססי בינה מלאכותית כללית באשר להיקף חובותיהם בהתאם ל-2 (EU AI Act);²⁴ קוד וולונטארי למפתחי מודלים מבוססי בינה מלאכותית כללית שפותח על ידי מומחי תעשייה ומספק מידע פרקטי בנוגע לשקיפות, זכויות יוצרים, אבטחה וכו';²⁵ ו- (3) טופס המחייב מפתחי מודלים מבוססי בינה מלאכותית כללית למסור מידע באשר למסדי הנתונים והמידע שעליהם מבוססות מערכות הבינה המלאכותית ומהם הן שואבות את המידע לפעולתן.²⁶

בארצות הברית פרסם הממשל הפדראלי בשנת 2020 מדריך לרגולציה ליישומי בינה מלאכותית לכל משרדי ומחלקות הממשל.²⁷ בשנת 2022 פרסם הממשל הפדראלי קווים מנחים ל"מגילת זכויות" בכל הנוגע לשימוש בבינה מלאכותית, בה מתוארים אמצעי הבטיחות שיש לנקוט לשם הגנה על הציבור האמריקאי וזכויותיו.²⁸ בשלהי שנת 2023 פרסם צו נשיאותי בנוגע לשימוש ופיתוח בטוח ואמין בבינה מלאכותית (להלן: "הצו הנשיאותי").²⁹ במקביל החלו מדינות בארצות הברית לחוקק חוקים מקומיים בנושאי בינה מלאכותית ויישומיהם בתחומי חיים רבים. הממשל האמריקאי, בניגוד לגישת האיחוד האירופי, אינו נוקט בגישה של חקיקה רוחבית בתחום הבינה המלאכותית, אלא מבקש להעניק לרגולטורים ולרשויות הרלוונטיות את הסמכות לפעול בתחומם, תחת העקרונות שפורסמו במגילת הזכויות ובצו הנשיאותי, לצד שימוש בכלי רגולציה רכים (דוגמת תקינה, מעורבות ברגולציה עצמית של השחקנים המרכזיים בתחום וכו').

בתקופה שחלפה מאז פרסום דוח הביניים, ולאחר עליית ממשל טרמפ, בוטל הצו הנשיאותי שפורסם בתקופת ממשל ביידן, ובמקומו פורסם צו נשיאותי חדש, המשקף גישה המבכרת הפחתת רגולציה ועידוד חדשנות תוך הסרת חסמים ומגבלות קיימים.³⁰ בהמשך לצו זה פורסמה בחודש יולי 2025 "תכנית הפעולה האמריקאית" בנושא בינה מלאכותית, שעניינה טיפול בתחום תחת נדבכים של חדשנות, תשתיות, דיפלומטיה בינלאומית ואבטחה.³¹ בארה"ב לא חוקק כאמור חוק בינה מלאכותית מקיף ברמה הפדראלית, אולם היו כמה מדינות, כגון קולוראדו, טקסס ויוטה, אשר פרסמו חוקי בינה מלאכותית מדינתיים. חוקים אלה עוסקים בהיבטים שונים כגון שקיפות, מניעת אפליה,

oecd.org/publications/ai-language-models-13d38f92-en.htm

22 ראו ה"ש 32 להלן, בעמוד 36.

23 G20, AI Principles (June 2019), https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf?force_isolation=true; G7, "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems On the basis of the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI systems, the Hiroshima Process International Code of Conduct for Organizations (October 2023)", https://ec.europa.eu/newsroom/dae/redirection/document/99644?force_isolation=true; G7, Leaders' Statement on the Hiroshima AI Process, <https://www.mofa.go.jp/files/100573466.pdf>

24 https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act?force_isolation=true

25 https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai?force_isolation=true

26 <https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act>

27 The White House, Guidance for Regulation of Artificial Intelligence Applications (November 2020), https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf?force_isolation=true

28 The White House, Blueprint for an AI Bill Of Rights: Making Automated Systems Work for the American People (October 2022), <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>

29 The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 2023), <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>

30 Removing Barriers to American Leadership in Artificial Intelligence – The White House <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>

31 תכנית הפעולה האמריקאית, בעמ' 1.

<https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

פרטיות ושימוש במידע.

בבריטניה פרסמה הממשלה אסטרטגיה לאומית בנושא בינה מלאכותית,³² ואף הקימה יחידה תחת משרד המדע, החדשנות והטכנולוגיה שתפקח על האימוץ של בינה מלאכותית בהתאם לאסטרטגיה שנקבעה.³³ הגישה הבריטית מבכרת את ערכי החדשנות והמובילות העולמית בתחום הבינה המלאכותית, זאת באמצעות השקעות ארוכות טווח בטכנולוגיה וקידום הטמעת הטכנולוגיה ברמה המדינתית, לצד שמירה על זכויות אדם ושימוש ראוי בטכנולוגיה. גם בבריטניה, בדומה לגישה הממשל האמריקאי, אין כוונה לקבוע חקיקה רוחבית אלא אסדרה סקטוריאלית באופן שיאפשר גמישות לרגולטורים ולרשויות הרלוונטיות לפעול בתחומי אחריותם בהתאם לעקרונות שנקבעו.

קיים אמנם דמיון בין הגישות שתוארו לעיל בכל הנוגע לצורך בניהול סיכונים בינה מלאכותית, הימנעות מפגיעה בזכויות אדם ושימוש אחראי וראוי בטכנולוגיה, אולם הדרכים להשגת יעדים אלה נבדלות בין הגישות השונות, ודומה כי יש פער תפיסתי באשר למקומה של רגולציה קשיחה ומחייבת לטפל בסיכונים אלה.

העיסוק בבינה מלאכותית מעמיד לפני קובעי המדיניות בעולם כולו מספר שאלות מפתח. כך לדוגמה, שאלות יסוד נוגעות לעיתוי הנכון להשית רגולציה שתחול על טכנולוגיה של בינה מלאכותית (האם יש מקום להמתין להתפתחות נוספת בטכנולוגיה או לקבוע כללים כבר עתה); **לאופי ולעוצמת הרגולציה** כאמור; לקביעה אם רגולציה בנושא בינה מלאכותית צריכה **להשתלב ברגולציה הקיימת** בתחומי חיים שונים או **לקבוע רגולציה ייעודית אשר תחול באופן רוחבי**. לשאלה האחרונה יש השלכות גם מבחינת המבנה הרגולטורי. בספרד, לדוגמה, בחרו להקים רשות עצמאית לבינה מלאכותית, שתפקידה לרכז את הפיקוח, היעוץ המקצועי, והמודעות הציבורית בהיבטי בינה מלאכותית, זאת עוד בטרם כניסת החקיקה האירופית לתוקף.³⁴

32 HM Government, National AI Strategy (September 2021), https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf?force_isolation=true

33 Office of Artificial Intelligence https://www.gov.uk/government/organisations/office-for-artificial-intelligence?force_isolation=true

34 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-20639

ג. העיסוק הממשלתי בישראל בבניה מלאכותית

בישראל החל בשנים האחרונות עיסוק ממשלתי בתחום הבניה המלאכותית. בחודש אוגוסט 2021 קיבלה ממשלת ישראל את החלטה מספר 212 שכותרתה "תכנית לקידום חדשנות, עידוד צמיחת ענף ההייטק וחיזוק המובילות הטכנולוגית והמדעית" (להלן: **"החלטת הממשלה"**), במסגרתה הונחה משרד החדשנות, המדע והטכנולוגיה לגבש תכנית לאומית שתעסוק בפנים הרבים המחייבים התייחסות, ובהם רגולציה, מדיניות מידע ואיסוף נתונים, אתיקה, שיתוף פעולה בין לאומי, והטמעת מערכות במגזר הציבורי.³⁵ החלטת הממשלה התבססה, בין היתר, על יוזמות ממשלתיות או ציבוריות אחרות בנושא.³⁶ בחודש פברואר 2023 אישרה הממשלה את החלטה מספר 173 שכותרתה "חיזוק המובילות הטכנולוגית של ישראל", ובה תכנית לאומית לבניה מלאכותית הכוללת האצת המחקר הבסיסי והיישומי בתחום, פיתוח תשתיות והטמעת יישומי בניה מלאכותי במגזר הציבורי, ותקצוב של השקעה בסך של עד 500 מיליון שקלים בנושא.³⁷

בחודש דצמבר 2023 פרסם משרד החדשנות, המדע והטכנולוגיה, בשיתוף מחלקת יעוץ וחקיקה (משפט כלכלי) במשרד המשפטים, מסמך מדיניות מקיף שעניינו "עקרונות מדיניות, רגולציה ואתיקה בתחום הבניה המלאכותית" (להלן: **"מסמך המדיניות"**).³⁸

במסמך המדיניות גובשו מספר עקרונות מוצעים למדיניות רגולציה. הנחת המוצא ביחס לעקרונות אלה היא כי יש חשיבות רבה לאימוץ מדיניות רגולציה ממשלתית אחידה וקוהרנטית, ועליה להתבסס, בין היתר, על רכיבים אלה:

- **רגולציה ענפית** – הרגולציה בתחום הבניה המלאכותית תיעשה בענף בו היא נדרשת ובהובלת הרגולטורים האמונים, זאת להבדיל מרגולציה רוחבית המשתרעת על פני כל תחום הבניה המלאכותית בענפים השונים. התפישה בבסיס עיקרון זה היא כי ענפים שונים מחייבים התייחסות שונה לרגולציה בתחום, מטעמים שונים (רמת סיכון השימוש בבניה מלאכותית, הפגיעה הפוטנציאלית בזכויות הפרט, פגיעה באינטרס ציבורי, וכו').
- **רגולציה בלתי-אחידה מבוססת סיכונים** – הרגולציה לא תחול באופן אחיד על יישומים שהסיכונים הכרוכים בהפעלתם שונים אחד מהשני. לשם כך, על הרגולציה להיות מותאמת לסיכונים הנשקפים מהשימוש ביישום הספציפי ותוצר של ניהול סיכונים שבוצע על ידי הרגולטור הרלוונטי. לשם המחשה, סיכון הנשקף משימוש ביישום ניווט מבוסס בניה מלאכותית אינו דומה במדרג הסיכונים לסיכון הנשקף משימוש ביישום המעבד הדמייה ומייצר דיאגנוזה רפואית באופן אוטומטי.
- **התאמה לכללים הנהוגים בעולם** – הרגולציה שתקבע תעמוד בהלימה לרגולציה הנוהגת במדינות מובילות בתחום הבניה המלאכותית ולעקרונות שאומצו על ידי ארגונים בינלאומיים מובילים, זאת במטרה להימנע מהצבת חסמים רגולטוריים הן ביחס לחברות ישראליות אשר יבקשו להפעיל יישומי בניה מלאכותית גם בחוץ לארץ והן ביחס לחברות זרות אשר יבקשו להפעיל יישומי בניה מלאכותית בארץ. נוסף על כך, מוצע שגורמי הממשלה והרגולטורים הרלוונטיים יהיו מעורבים באופן אקטיבי בפורומים בינלאומיים המגבשים רגולציה בתחום הבניה המלאכותית.
- **רגולציה "רכה"** – הוצע לקבוע רגולציה גמישה, שתאפשר את התקדמות הטכנולוגיה מבלי להידרש לעדכוני חקיקה באופן תדיר בהתאם להתפתחות הטכנולוגית. לצורך כך, הוצע להשתמש בקביעת עקרונות, תקינה, המלצות רגולטוריות לאימוץ וולונטרי ורגולציה עצמית.
- **פיתוח הרגולציה באופן מודולרי, תוך הסתייעות בנסיינות רגולטורית, ושמירה על ניטרליות טכנולוגית** – על מנת לוודא הכנסה בטוחה של יישומי בניה מלאכותית לשימוש הציבורי, והיכרות מעמיקה של הרגולטור את הטכנולוגיה וכיווני התפתחותה, מוצע לעשות שימוש בארגזי-חול רגולטוריים (regulatory sandboxes)

35 https://www.gov.il/he/departments/policies/dec212_2021.

36 בין היתר, המיזם הלאומי למערכות נבונות בטוחות להעצמת הביטחון הלאומי והחוסן המדעי-טכנולוגי: אסטרטגיה לאומית לישראל, ד"ח מיוחד לראש הממשלה (2020); פורום תלם, ועדת בניה מלאכותית ומדע הנתונים (2020).

37 https://www.gov.il/he/pages/dec173-2023?fireglass_rsn=true#fireglass_params&tabid=a1d3443a368e2634&start_with_session_counter=3&application_server_address=isagovil-2-me-west1.prod.fire.glass

38 עקרונות מדיניות, רגולציה ואתיקה בתחום הבניה המלאכותית, משרד המשפטים (יעוץ וחקיקה) ומשרד החדשנות, המדע והטכנולוגיה, דצמבר 2023. https://www.gov.il/he/pages/ai_23?fireglass_rsn=true#fireglass_params&tabid=a549eeda40bf1466&start_with_session_counter=3&application_server_address=isagovil-2-me-west1.prod.fire.glass

ובפיילוטם בשיתוף הרגולטורים.³⁹

- **שיתוף בעלי-עניין בקביעת הרגולציה** – הרגולציה בתחום הבינה המלאכותית תפותח ותקודם בשיתוף בעלי העניין ובעלי הידע בתחום, ובכלל זאת גורמים מהתעשייה, האקדמיה, וארגוני חברה אזרחית.
 - **הקמת פורום רגולטורים ופורום לשיתוף הציבור** – הוצע למסד פורום מקצועי, שיכלול נציגים מהרגולטורים הרלוונטיים, לצד מומחי טכנולוגיה, מדיניות ומשפט, על מנת לדון בסוגיות משותפות, לאמץ רגולציה אחידה וקוהרנטית, ולקדם את התיאום הממשלתי בטיפול בנושא. כן הוצע למסד פורום אשר יכלול את נציגי הרגולטורים וקובעי המדיניות, לצד נציגי תעשייה, אקדמיה, החברה האזרחית והציבור הרחב, זאת על מנת לעמוד על התחומים העיקריים שאליהם נדרשים הרגולטורים וקובעי המדיניות, בין היתר לביצוע התאמות נדרשות, החסרת חסמים, וגיבוש מענה בסוגיות שונות.
 - **סקר שימושים** – הרגולטורים וגורמי הממשלה הרלוונטיים ימפו ויסקרו את השימושים ביישומי בינה מלאכותית הנעשים בענפים עליהם הם אמונים, על מנת לוודא שקביעת הרגולציה תתקבל על בסיס מצע עובדתי מספק והבנה של הרגולטורים אודות השימושים הקונקרטיים, העכשוויים והעתידיים, ולא בחלל ריק.
 - **הנגשת מידע וכלים לשימוש אחראי בבינה מלאכותית, ובכלל זה כלי לניהול סיכונים** – הומלץ לשקול פיתוח ואימוץ של כלי אחיד לניהול סיכונים ביחס לשימוש בבינה מלאכותית, שייצור שפה משותפת בין גורמי הממשלה לבין הרגולטורים, ובין גורמי הממשלה והרגולטורים לבין הציבור הרחב. שימוש בשפה אחידה תגביר את הוודאות המשפטית, תסייע לציבור, ולשוק הפרטי בפרט, להעריך את הסיכונים הכרוכים בשימוש ביישומי בינה מלאכותית, ותסייע לרגולטורים לבחון היישומים עצמם ואת הסיכונים הכרוכים בשימוש בהם.
- בהמשך להחלטת הממשלה ועובר לפרסום מסמך המדיניות, במהלך חודש יולי בשנת 2022 הושקה התכנית הלאומית לבינה מלאכותית. מדובר בתכנית ארוכת טווח שמטרתה לסייע בפיתוח והטמעה של בינה מלאכותית במגזר הציבורי ובמשק הישראלי באמצעות קידום מחקר, הון אנושי ותשתיות להבטחת המובילות הטכנולוגית של מדינת ישראל.⁴⁰
- כחלק מהמאמץ הממשלתי לאסדר שימוש בבינה מלאכותית במגזרים ספציפיים, קודם בשנים האחרונות הטיפול בהיבטים רגולטוריים בתחום כלי רכב עצמאיים (אוטונומיים), פרטיות (עליהם נעמוד בחלק ג' להלן), בריאות,⁴¹ ועוד. בתקופה שחלפה מאז פרסום דוח הביניים, קיבלה ממשלת ישראל החלטה על הקמת מטה לאומי לבינה מלאכותית תחת משרד ראש הממשלה (החלטת ממשלה מס' 3375 מיום 21 בספטמבר 2025). תפקידיו של המטה הלאומי לבינה מלאכותית, בין היתר, להוביל גיבוש ויישום אסטרטגיה לאומית בתחום הבינה המלאכותית, לרבות ביחס לתשתיות מחקר; גיבוש תוכנית לאומית להאצת הבינה המלאכותית במשק במטרה לחזק את מעמדה העולמי של ישראל בתחום; גיבוש מדיניות, ליווי וייעוץ מקצועי למשרדי הממשלה ביחס להיבטים רגולטוריים הנוגעים לבינה מלאכותית לטובת הסרת חסמים והרחבת יכולות הפיתוח, היישום והשימוש בבינה מלאכותית במשק, ועוד.⁴²

39 ארגז חול רגולטורי הוא כלי מדיניות המאפשר לרגולטורים לייצר "סביבת ניסוי" רגולטורית. במסגרת זו, הרגולטור מבצע התאמות ברגולציה הקיימת כדי לאפשר למפוקחים להכניס טכנולוגיה חדשה באופן מבוקר, מצומצם ולזמן מוגבל. בנוסף, הסנדבוקס מסייע לרגולטורים להתמודד עם פערי המידע והמומחיות בינם לבין השוק ועם קצב ההתפתחות המהיר של הטכנולוגיה, שכן רגולציה זמנית, מדודה וגמישה מאפשרת תהליך למידה "תוך כדי תנועה" ומקנה כלים להסרה מבוקרת וזהירה של חסמים ממוקדים. המפוקחים מצדם מרוויחים מההזדמנות לפעול בסביבה "ידידותית", ובלי לשאת בנטל רגולטורי שלא חיוני לפעילותם (מסמך המדיניות, בעמ' 100).

40 <https://aiisrael.org.il/>

41 משרד הבריאות, עקרונות מנחים לפיתוח טכנולוגיות מבוססות למידת מכונה (אפריל 2023) <https://www.gov.il/he/pages/digital-medical-technology-gmlp-1>

42 החלטת ממשלה מספר 3375 מיום 21.9.25 <https://www.gov.il/he/pages/dec3375-2025>

ד. יישומי בינה מלאכותית בסקטור הפיננסי

הבינה המלאכותית עשתה את צעדיה הראשונים במגזר הפיננסי בתחילת שנות השמונים של המאה העשרים, אז נוסדה קרן גידור המתמחה בהשקעה כמותית (quantitative investing), גישה המבוססת על מודלים מתמטיים מתקדמים לקביעת נקודה אופטימלית לביצוע עסקה רווחית.⁴³ באותה השנה נוצרה גם מערכת לתכנון פיננסי מבוססת בינה מלאכותית לבעלי שגר גבוה.⁴⁴ באותה תקופה ניתן היה למצוא פיתוחים מבוססי בינה מלאכותית גם בעולמות המס, המסחר בבורסה, התכנון הפיננסי ודירוג אשראי.⁴⁵ בשנות התשעים חלה התקדמות באפליקציות לזיהוי הונאות והלבנת הון.⁴⁶ בשנת 1998 יצרה רשות ניירות ערך האמריקאית (SEC) מסגרת רגולטורית חדשה שמטרתה להקטין חסמים לכניסתן של מערכות מסחר חדשות לשוקי ההון ולעודד תחרות וחדשנות.⁴⁷ בפועל, הרגולציה החדשה אפשרה את כניסתן של מערכות מסחר בתדירות גבוהה (high frequency trading או HFT) ומערכות מסחר אלגוריתמיות (algorithmic trading), אשר באופן הדרגתי תפסו מקום מרכזי יותר ויותר במסחר הבורסאי בארה"ב. כיום ההערכות הן כי כמחצית מנפח המסחר בארצות הברית וכשליש מנפח המסחר באירופה מבוצע על ידי מערכות HFT או מסחר אלגוריתמי.⁴⁸

זה תקופה שגופים פיננסיים בעולם עושים שימוש ביישומים מבוססי בינה מלאכותית בפעילויות מגוונות שלהם, למשל: **בביטוח** (ישוב תביעות, חיתום ביטוח); **בבנקאות ובאשראי** (חיתום אשראי, דירוג אשראי); **בייעוץ פיננסי** (ייעוץ השקעות, ייעוץ פנסיוני); **ובניהול תיקים ומסחר בניירות ערך** (מסחר אלגוריתמי, מסחר בתדירות גבוהה, ניתוח כדאיות ביצוע עסקה, ניהול נזילות). כמו כן, גופים פיננסיים עושים שימוש בכלים מבוססי בינה מלאכותית גם לטובת פעילויות תומכות או נלוות לפעילויות הליבה של הגוף הפיננסי, למשל זיהוי הונאות פיננסיות (AML/CFT), שיווק ומכירות, שירות לקוחות, ניהול סיכונים וציות, סייבר, ועוד. דברים אלה נכונים, אם כי במידה פחותה כפי הנראה, גם למערכת הפיננסית בישראל, בה ניתן לזהות שימוש הולך וגובר ביישומי בינה מלאכותית בקרב חברות במגזר הפיננסי (להרחבה אודות פעילות בינה מלאכותית בסקטור הפיננסי בישראל, ראו פרק פעילות בינה מלאכותית בסקטור הפיננסי בישראל להלן).

על אף השיח הער וההתלהבות הרבה האופפים את תחום הבינה המלאכותית בכלל ואת יישומי הבינה המלאכותית בקרב גופים פיננסיים בפרט, מעטים הם המקרים בהם יישומי בינה מלאכותית מתקדמים מבצעים את פעילות הליבה של הגוף הפיננסי מקצה-לקצה, באופן אוטומטי וללא כל מעורבות אנושית. אמנם קיימים לא מעט יישומי בינה מלאכותית במגזר הפיננסי, אך אלו משמשים בעיקר ככלים תומכי-החלטה (המסייעים לקבלת החלטות של אדם בשר-ודם) בעוד אחרים מבצעים פעולות בצורה אוטומטית אך במקטעים מסוימים בלבד בשרשרת הערך של המוצר או השירות הפיננסי, לרוב ללא אינטראקציה ישירה עם הלקוח של הגוף הפיננסי.⁴⁹ לשם המחשה, גופים פיננסיים המעניקים אשראי ללקוחותיהם מסתייעים ביישומים מבוססי בינה מלאכותית לצורך חיתום ההלוואה ותנאיה, אולם ההחלטה הסופית בדבר מתן האשראי ותנאיו תיקבע על ידי נציגים אנושיים של הגוף הפיננסי, אשר גם יהיו בקשר עם הלקוח. דוגמה נוספת: יועצי השקעות המסתייעים ביישומים מבוססי בינה מלאכותית לצורך קביעת תמהיל השקעה עבור לקוחותיהם, בהתאם לתיאבון הסיכון והעדפותיהם הפרטניות של הלקוחות, אך ההחלטה הסופית אודות חלוקת תיק ההשקעות נותרת בשיקול דעתו של היועץ האנושי. ניתן להניח כי בעתיד, עם שיפור הטכנולוגיה וצמצום המגבלות והאתגרים עמם היא מתמודדת, נראה ירידה במידת המעורבות האנושית במתן השירותים הפיננסיים באופן שירחיב את מידת האוטומציה של יישומי הבינה המלאכותית למקטעים נוספים בקשת השירותים שתסופק על ידי הגופים הפיננסיים.

43 Artificial intelligence in finance – Bonnie G. Buchanan, PhD, FRSA, The Alan Turing Institute (April 2019), <https://doi.org/10.5281/zenodo.2612537>.

44 שם.

45 שם; וגם Everis (ה"ש 1) בעמוד 15.

46 שם, בעמוד 5.

47 Regulation of Exchanges and Alternative Trading Systems (1998). <https://www.sec.gov/rules-regulations/1998/12/regulation-exchanges-alternative-trading-systems>.

48 <https://www.nasdaq.com/glossary/h/high-frequency-trading>; Zaharudin KZ, Young MR, Hsu WH (2022) High-frequency trading: definition, implications, and controversies. J Econ Surv 36(1):75–107.

49 דוח ה-OECD משנת 2023, בעמוד 10.



ממחקרים שפורסמו עולה כי כיום השימוש העיקרי ביישומי בינה מלאכותית נוגע בעיקר לייעול ושיפור תפוקה בעולמות התפעול במסגרת מוקד עורפי (back-office) ובעולמות הציות וניהול סיכונים במסגרת ה-middle-office.⁵⁰ מסקר שערכה חברת הייעוץ מקינזי במוסדות פיננסיים בינלאומיים, עולה כי השימוש העיקרי ביישומי בינה מלאכותית נועד למיטוב (אופטימיזציה) של שירותי תפעול (כגון שירות לקוחות, משרד אחורי וכד'), נתון אשר חוזר על עצמו ארבע שנים ברציפות.⁵¹

דוגמה לשימוש נפוץ ביישומי בינה מלאכותית בקרב גופים פיננסיים היא בתחום שירות הלקוחות. כך, גופים פיננסיים רבים הטמיעו (או נמצאים בתהליכי הטמעה) של צ'אט-בוט (chatbot), יישום מבוסס בינה מלאכותית שמספק מענה אוטומטי, ברמות תחכום שונות, לפניות שירות מצד לקוחות, ומסוגל לספק מענה המדמה מענה של בן-אנוש. צ'אט-בוטים מתקדמים עושים שימוש במודלי שפה גדולים (LLM) ועיבוד שפה טבעית (NLP), וקיימים מקרים בהם קשה להבדיל בין מענה אוטומטי באמצעות בינה מלאכותית לבין מענה של אדם בשר ודם. במקרים מסוימים (וכתלות ברמת התחכום של הצ'אט-בוט), מסוגל הצ'אט-בוט לספק מענה מלא לפניות שירות מצד לקוחות, כאשר הלקוח כלל לא ידע שנעזר בכלי בינה מלאכותית להבדיל מבן אנוש. על-פי הערכות המשרד להגנת הצרכן הפיננסי בארצות הברית (CFPB), בשנת 2022 כ-37% מהאוכלוסייה האמריקאית נעזרה בצ'אט-בוט בפניית לקבלת שירות מהבנק, ומספר זה צפוי לגדול באופן משמעותי.⁵² אחת המוטיבציות העיקריות לאימוץ צ'אט-בוטים במערכת הפיננסית היא חיסכון בעלויות – על פי ההערכה אימוץ יישומי בינה מלאכותית למערכי שירות לקוחות עשוי להניב חיסכון של כ-8 מיליארד דולר למערכת הבנקאית בארצות הברית לבדה.⁵³

כפי שצוין לעיל, נראה שהאימוץ של יישומי בינה מלאכותית מתקדמים בקרב גופים פיננסיים (בעיקר גופים פיננסיים "מסורתיים"), בוודאי יישומים המאפשרים מיכון (אוטומציה) מלאה של פעילות הליבה של הגוף הפיננסי ללא מעורבות אנושית כלשהי, נעשה באופן איטי ומבוקר. כך, לדוגמה, מסקר שערכה רשות ניירות ערך האירופית, השימוש הנוכחי בכלי בינה מלאכותית בחברות המספקות שירותי ייעוץ השקעות רובוטיים (robo-advising) וחברות לדירוג אשראי מוגבל, ונעשה בהם שימוש, אם בכלל, בחלקים מסוימים מקשת השירותים שמספק הגוף הפיננסי (להבדיל מאוטומציה מלאה של השירות כולו) (להלן: "דוח ESMA משנת 2023").⁵⁴ לא בכדי, יועצי השקעות באיחוד האירופי ציינו כי עד כה לא נדרשו לשינויים מהותיים בפרקטיקות ההשקעה שלהם כתוצאה משימוש בכלי בינה מלאכותית.⁵⁵ ניתן למנות לא מעט סיבות לאימוץ האיטי והמבוקר של יישומי בינה מלאכותית במגזר הפיננסי, ובכלל זאת: סביבה רגולטורית הדוקה; התפתחות של סיכונים חדשים (שלא היו מוכרים בעבר) לצד התעצמות סיכונים קיימים (למשל, סיכונים מתחום פרטיות המידע וסודיות המידע, סיכוני סייבר, איכות המידע והחשש מהטיות ואפליה, ציות, היעדר הסברתיות לאופן עבודת הטכנולוגיה ותוצריה, וכדומה); היעדר הון אנושי בעל כשירות ומומחיות מספקים; שימוש בתשתיות מיושנות (legacy systems) והקושי להתאימן לסוג זה של טכנולוגיה, ועוד.

סיכומו של דבר, ישנם שימושים פוטנציאליים רבים מאוד לבינה מלאכותית בסקטור הפיננסי, והתפתחויות הטכנולוגיה הובילו לעניין רב בקרב גופים פיננסיים. בד בבד, היישומים עד כה הם בעיקר של טכנולוגיות בינה מלאכותית מדורות קודמים, וביחס לבינה מלאכותית מתקדמת יותר היישומים בפועל מוגבלים בשלב זה ונוגעים פחות לפעילויות ליבה מול לקוחות. תמונת מצב זו נכונה כפי הנראה לסקטור הפיננסי במדינות המערב וכן לישראל.

50 שם.

51 McKinsey & Company, The state of AI in 2022—and a half decade in review (December 2022), <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review>

52 CFPB, Chatbots in consumer finance (June 2023), <https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/#note>

53 שם.

54 ESMA, Artificial Intelligence in EU Securities Market (February 2023), https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf, בעמוד 9, 16; וגם: דוח OECD משנת 2023, בעמוד 4.

55 דוח ESMA משנת 2023, בעמוד 6.

ה. תועלות ואתגרים הנובעים משימוש בבינה מלאכותית

ההתקדמות הטכנולוגית בתחום הבינה המלאכותית בכלל ולמידת מכונה בפרט, מגלמת בחובה יתרונות משמעותיים במגוון רחב של תחומים, ואפשר כי בעתיד חלק ניכר מהפעולות היום-יומיות יבוצעו או ייתמכו על-ידי טכנולוגיית בינה מלאכותית. ואולם, לצד היתרונות הרבים, מתעוררים גם אתגרים משמעותיים הנובעים מהחדשנות הטכנולוגית שמציבה הבינה המלאכותית.

נעמוד ראשית על התועלות הפוטנציאליות העיקריות מכניסתה של בינה מלאכותית לסקטור הפיננסי:

- 1. ייעול הפעילות והפחתת עלויות** – שילוב של מערכות בינה מלאכותית במערכי תפעול בגופים פיננסיים ואוטומציה של פעולות המחייבות משאבים רבים, בעיקר הון אנושי, צפוי להוביל להתייעלות ולהפחתת עלויות. כך לדוגמה, שירות לקוחות שמבוצע על ידי צ'אט-בוט, צפוי להוביל לצמצום מערכי שירות הלקוחות האנושיים וניתוב של משאבים לביצוע פעולות אחרות. ההערכות הן ששימוש ביישומי בינה מלאכותית לפעולות תפעוליות יגדל באופן משמעותי בשנים הקרובות. הפחתת הוצאות הגופים הפיננסיים עשויה להתגלגל ללקוחות ולמשקיעים שיהנו משירותים ומוצרים זולים יותר.
- 2. שיפור איכות המוצרים והשירותים** – בינה מלאכותית עשויה לשפר את איכות המוצרים והשירותים המוצעים בסקטור הפיננסי, באמצעות שיפור של תהליכי קבלת ההחלטות, התאמה טובה יותר של המוצרים והשירותים לצרכי הלקוחות והמשקיעים, והרחבת הפעילות הפיננסית. לשם המחשה: פעילות של מתן אשראי תוכל להשתפר בעזרת בינה מלאכותית אשר תביא בחשבון נתונים רבים, לרבות מידע לא "מסורתי", אשר כיום אינו נלקח בחשבון בעת מתן אשראי ותקבל החלטות אשראי מדויקות יותר; היא תוכל להיעשות באופן מותאם יותר לצרכי הלקוחות, למשל בעצם הצעת האשראי לגורמים הזקוקים לה, ובתנאי האשראי; והיא תוכל להיות רחבה יותר, כך שינתן אשראי לקשת רחבה יותר של לוויים, לדוגמה לעסקים קטנים ובינוניים (SMEs).
- 3. שיפור בהכלה ובנגישות פיננסית** – אוכלוסיות שכיום מודרות מהמגזר הפיננסי יוכלו להסתייע בהתפתחות הטכנולוגית שתיווצר כתוצאה מאימוץ יישומי בינה מלאכותית במגזר הפיננסי על מנת לשפר את נגישותן לכלים פיננסיים, ובכלל זאת אשראי, ביטוח ויכולות חיסכון והשקעה. לשם המחשה: פעילות של ניהול תיקי השקעות, המוגבלת לעתים קרובות ללקוחות בעלי הון רב יחסית, תוכל להיעשות בעלויות נמוכות יותר ועל כן ניתן יהיה להפנות אותה לציבור רחב יותר של לקוחות.
- 4. שיפור בהיבטי ציות** – מערכות מבוססות בינה מלאכותית עשויות לסייע לגופים פיננסיים לשפר את יכולות הציות שלהם בזמן אמת. בכוחן של מערכות הבינה המלאכותית לעבד כמויות מידע אדירות במהירות רבה ולהתריע על חשדות או פעולות חריגות בסמוך למועד התרחשותן. כלים אלו יכולים לסייע גם בידי רגולטורים פיננסיים לזהות עבירות ופעולות חריגות בזמן אמת, באופן שסייע לאכיפה והרתעה ראויות ובכך לשמור על המשקיעים ועל הוגנות השוק. כמו כן, מערכות מבוססות בינה מלאכותית עשויות לסייע באיתור וזיהוי תבניות פעולה פליליות בזמן אמת ולסייע במניעת פעולות אלה.

נעמוד עתה על האתגרים הנובעים משימוש בבינה מלאכותית. הרשימה מטה כוללת שני חלקים:

בחלק הראשון יפורטו **אתגרים כלליים הנובעים משימוש במערכות בינה מלאכותית** ושאינם ייחודיים דווקא למגזר הפיננסי. אתגרים אלה נסקרים בהרחבה במסמך המדיניות. בחלק השני יפורטו **אתגרים ייחודיים למגזר הפיננסי**, או כאלה שהתממשותם עלולה להביא לפגיעה קשה ומשמעותית יותר ביחס למגזרים אחרים, נוכח מידת ההשפעה והסיכון הנלווים לפעילות פיננסית. יובהר, כי אין מדובר ברשימה סגורה של אתגרים וסיכונים.⁵⁶

אתגרים כלליים הנובעים משימוש במערכות בינה מלאכותית:

- 1. "קופסה שחורה" והסברתיות** – אופן קבלת ההחלטות של מערכות בינה מלאכותית מתואר לעתים קרובות כ"קופסה שחורה" (black box) במובן זה שלא ניתן להתחקות אחריו. כלומר, לא ניתן לדעת איך ומדוע התקבלה ההחלטה כפי שהתקבלה. הסיבה לכך נעוצה במורכבות האלגוריתמים העומדים בבסיס מערכות הבינה המלאכותית ובכמות המידע שעל בסיסו מתקבלות ההחלטות. יש הטוענים כי מתקיים שקלול תמורות (trade-off) בין מידת ההסברתיות ובין ביצועי המערכת, כלומר יש יחס הפוך בין מידת ההסברתיות ובין דיוק ביצועי

56 להרחבה בעניין סוגיות ואתגרים המתעוררים בקשר עם בינה מלאכותית, ראו מסמך המדיניות, בעמוד 46.

המערכת.⁵⁷ בעיית "הקופסה השחורה" מאפיינת מערכות בינה מלאכותית מתקדמות, בהשוואה למערכות מדורות קודמים, בהן היה ברור כיצד האלגוריתם פועל וכיצד התקבלו תוצריו. בעיית הקופסה השחורה עלולה לגרום בעיות נוספות כגון קושי לתת אמון במערכת, קושי לזהות טעויות ולתקן, קשיים אתיים הנוגעים לאי מתן הסבר לגורם שהחלטה התקבלה בעניינו, ועוד.

2. **מעורבות אנושית** – נשאלת השאלה באיזו מידה (אם בכלל) נדרשת מעורבות אנושית במעמד קבלת ההחלטות על ידי מערכות הבינה המלאכותית. מאפיין מרכזי של מערכות בינה מלאכותית מתקדמות הוא יכולתן לפעול ללא מעורבות אנושית, כאשר מידת המעורבות האנושית ניתנת לסיווג באופן הבא: (1) מעורבות אנושית לא קיימת כלל, ותהליך קבלת ההחלטות כולו מתבצע על ידי מערכות הבינה המלאכותית ללא מעורבות אנושית; (2) מעורבות אנושית קיימת במידה מסוימת, כך שתהליך קבלת ההחלטות מתבצע על ידי מערכות הבינה המלאכותית, אך גורם אנושי רשאי להתערב (במידה כזו או אחרת) בהחלטה המתקבלת על ידי המערכת. המעורבות יכולה להיעשות במספר שלבים של פעילות המערכת, בין מראש, בזמן אמת או בדיעבד; ו- (3) מעורבות אנושית קיימת באופן מלא, כך שמערכת הבינה המלאכותית היא בבחינת "גורם ממליץ" או כלי מסייע בקבלת החלטה על ידי בן-אנוש, אשר לו מסור שיקול הדעת הבלעדי בקבלת ההחלטה הסופית.

3. **יידוע וגילוי** – אתגר השקיפות והגילוי נוגע לכמה רבדים בפעילותן של מערכות בינה מלאכותית. שאלה אחת היא האם ובאיזו מידה יש ליידע אדם שבן-שיחו או מי שקיבל החלטה בעניינו אינו בן-אנוש אלא מערכת בינה מלאכותית. שאלה שנייה היא היקף הגילוי הנדרש אודות אופן הפעולה של מערכות בינה מלאכותית. כך למשל, האם נדרש גילוי מיוחד אודות קבלת החלטות, שעה שזו נעשתה על-ידי מערכת בינה מלאכותית. שאלה שלישית נוגעת לפרסומים שיווקיים אודות מערכות בינה מלאכותית והצורך כי אלה לא יטעו את הציבור. העיסוק בסוגיית הידוע והגילוי קשור במידה רבה לסוגיית ההסבריות, שכן יידוע וגילוי אודות השימוש ביישומי בינה מלאכותית יכולים להיכלל כחלק מחובת ההסבריות (שהיא, במהותה, סוג מסוים של שקיפות ביחס לליבת המערכת והנתונים המזינים אותה).

4. **פרטיות** – טכנולוגיית הבינה המלאכותית מתבססת על איסוף ועיבוד מידע בצורה נרחבת, ובכלל זה מידע אישי, כלומר מידע שנוגע לאדם מזהה או שניתן לזהותו. פיתוח הטכנולוגיה מהווה גורם מאיץ ומגביר משמעותי למוטיבציה להשגת נתוני עתק, שמירתם ושימוש מגוון בהם. כמו כן, תוצרי מערכות הבינה המלאכותית עלולים לגלם תובנות פרטניות ואישיות לגבי אדם, לעתים רגישות ואינטימיות ביותר. יתרה מכך, מערכות בינה מלאכותית מבצעות עיבוד על נתוני עתק באמצעות פעולות חישוב יעילות ואיכותיות, אשר בכוחן לאתר, בין השאר, קשרים ויחסי גומלין לא צפויים בין נתונים שונים ולמקסם את התוצרים והתובנות שניתן להפיק מהם. סוגיות אלה ואחרות מעוררות אתגרים ומתחים לא מבוססים בקשר להגנה על הזכות לפרטיות והגנה על מידע אישי, לכל אורך מחזור החיים של מערכות הבינה המלאכותית.

5. **אפליה והטיות** – בינה מלאכותית מבוססת על מידע ועל כן עולה חשש שהנתונים עליהם מתבססות המערכות יהיו מוטעים, במודע ושלא במודע. חשש נוסף הוא כי מערכות בינה מלאכותית יעשו שימוש אסור בקריטריונים שבכוחם לאפיין אוכלוסיות מסוימות, באופן שיוביל לתוצאות מוטות או לאפליה אסורה מצד המערכות ואף עלול להחריף אפליה קיימת. קיומה של אפליה או היעדרה תלוי במידה רבה בייצוגיות וברלוונטיות של הנתונים המזינים את המערכת ושעל בסיסם תקבל המערכת החלטה. מכאן, שסוגיית אמינות, איכות, דיוק וזמינות הנתונים שעל בסיסם מתקבלות החלטות על ידי המערכת היא מכרעת.

6. **אמינות, עמידות, אבטחה ובטיחות** – על מנת להנות מהתועלות הקשורות לשימוש בבינה מלאכותית, יש חשיבות רבה לוודא את תפקודן התקין, הבטוח והמהימן של המערכות, אשר נשענות על טכנולוגיה ומידע החשופים לטעויות ותקלות טכניות. על-פי מסמך המדיניות, ניתן לחלק את הכשלים שעלולים להתעורר בהקשר זה לכשלים פנימיים המשפיעים על אמינות המערכת (המביאים לחוסר דיוק וביצועים ירודים) ולכשלים חיצוניים המשפיעים על עמידות המערכת ושיבוש פעילותה על ידי ניצול נקודות תורפה שלה. ההתייחסות לכשלים הפנימיים מתמקדת לרוב בכשלים הקשורים לאיכות המידע שעל בסיסו מקבלת המערכת החלטות, תיקוף המידע וביצוע בדיקות ביצועים למערכות. ההתייחסות לכשלים החיצוניים נחלקת לעמידותה ואבטחתה של המערכת, המתמקדת לרוב באיומים הנובעים מהתערבות חיצונית שתגרום נזק או בניצול לרעה של המערכות, ובכלל זאת סיכוני סייבר. ההתייחסות לבטיחות המערכת נוגעת לכשלים פנימיים וחיצוניים, אשר עלולים לגרום

לפגיעה משמעותית בזכויות הפרט או באינטרסים ציבוריים, ובפרט בבטיחות המשתמשים המושפעים מהן.⁵⁸

7. **אחריות** – סוגיה עקרונית המתעוררת בעת שימוש במערכות בינה מלאכותית נוגעת לשאלת הגורם אשר יישא באחריות האזרחית או הפלילית ביחס לתוצאה מפלה או כשל של המערכת. כן עולה השאלה אם אותו מושא האחריות (יהא אשר יהא) יכול לבצע פעולות או להטמיע תהליכים אשר עשויים להוציא אותו ידי חובתו או לצמצם את מידת אחריותו. זאת ועוד, סוגיית האחריות מתעוררת גם בכל הנוגע למיקור חוץ והעברה של פעילויות עסקיות לביצוע של גורמים חיצוניים לארגון.

נוסף על האתגרים שפורטו לעיל, קיימים אתגרים וסוגיות ייחודיים למגזר הפיננסי:

א. **סיכוני יציבות פיננסית** – השימוש במערכות בינה מלאכותית עלול להגביר סיכונים ליציבות המערכת הפיננסית.⁵⁹ בין היתר שימוש במערכות בינה מלאכותית או מודלים דומים על ידי מספר גדול של גופים פיננסיים עלול לייצר קישוריות-גומלין (interconnectedness) בין הגופים הפיננסיים העושים שימוש באותן מערכות, באופן שעלול להוביל לפעולה נרחבת זהה (one-way markets). בעתות לחץ על השווקים, הדבר מגביר את החשש מסיכון נזילות ויציבות של המערכת.⁶⁰ בדומה לכך, מערכות בינה מלאכותית עלולות להגביר התנהגות "עדרית" ותנודתיות בשוק. סיכון נוסף ליציבות הפיננסית נובע מהישענות על צדדים שלישיים, המספקים את מערכות הבינה המלאכותית, באופן שייצור תלות בהם.

דוגמה לסיכון יציבותי ניתן למצוא בעולמות המסחר בשוק ההון. במאי 2010 התרחש בארצות הברית האירוע שזכה לכינוי Flash Crash of 2010, במהלכו איבדו מדדים מובילים בבורסת ניו-יורק עשרות אחוזים מערכם בתוך דקות ספורות של מסחר. כך נמחקו טריליוני דולרים בשווי בתוך דקות ונוצר משבר נזילות בבורסה. האירוע היכה גלים בארצות הברית ובעולם כולו, ונחקר על ידי שני רגולטורים פיננסיים בארצות-הברית. בין היתר נמצא כי אינטראקציה בין מערכות מסחר אוטומטיות ואסטרטגיות מסחר אלגוריתמיות עלולה להביא במהירות לפגיעה קשה בנזילות ניירות ערך ולפעילות בלתי סדירה של השוק.⁶¹ במיוחד בעתות לחץ על השווקים, ביצוע עסקאות דומות על ידי מספר רב של שחקני שוק עלול להביא לעלייה או ירידה דרסטית של מכשירים פיננסיים בשוק, להגביר את התנודתיות ובמקרים מסוימים אף להביא לכדי כשל יציבותי. באופן דומה, כשל באלגוריתם או בבסיסי מידע בהם עושים שימוש מספר נותני אשראי מרכזיים, עלול להוביל למתן אשראי ללווים אשר אינם בעלי יכולת פירעון, דבר שבתורו עלול לייצר פגיעה יציבותית ומשבר פיננסי. ודוק, אין הכרח שהכשל יימצא במערכות בינה מלאכותית אוטומטיות ואוטונומיות לחלוטין, שכן גם כאשר המערכות הן בבחינת כלים תומכי החלטה וההסתמכות על המלצות המערכות גבוהה, עלול להיגרם משבר אשראי ופגיעה יציבותית במשק.

ב. **סיכוני סייבר, הונאה ודיסאינפורמציה** – בינה מלאכותית עלולה לשמש בדרכים שונות לפגיעה בציבור המשקיעים והלקוחות, בגופים פיננסיים, ובמערכת הפיננסית בכללותה, באמצעות הפצת דיסאינפורמציה וביצוע הונאות פיננסיות. אין מדובר בתופעה חדשה, ואולם זמינותם ותפוצתם של כלי בינה מלאכותית מקלים על יצירתה, מגבירים את היקפה ואת התאמתה לנמענים, ולכן גם את האפקטיביות שלה בהשגת מטרות הגורם המשבש.⁶² סיכון הדיסאינפורמציה בפרט נתפש כיום כאחד הסיכונים המשמעותיים בהתפתחותה של הבינה המלאכותית, והוא רלוונטי לסקטור הפיננסי, בו מתקבלות החלטות מהירות על בסיס מידע. דוגמה אחת לסיכון זה הוא הדיפ-פייק (Deepfake), תוכן אשר נחזה להיות אמיתי, על ידי שילוב של תמונות, סרטונים, קולות ותוכן קיימים. תופעת הדיפ-פייק התרחבה מאוד בשנים האחרונות.⁶³ מומחים בפשיעה פיננסית מגדירים את התופעה כאחד מהסיכונים הגדולים ביותר עמו יתמודד המגזר הפיננסי.⁶⁴

58 מסמך המדיניות, בעמוד 65.

59 Danielsson, Jon and Uthemann, Andreas, On the use of artificial intelligence in financial regulations and the impact on financial stability * (June 05, 2024). <https://ssrn.com/abstract=4604628>.

60 דוח ה-OECD משנת 2023, בעמוד 23.

61 Findings Regarding the Market Events of May 6, 2010 – Report of the Staff of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (September 2010), <https://www.sec.gov/files/marketevents-report.pdf>.

62 רועי גולדשמידט "בינה מלאכותית יוצרת: הזדמנויות, סיכונים ורגולציה" מרכז המחקר והמידע של הכנסת, עמ' 2-3 (יוני 2023), https://fs.knesset.gov.il/globaldocs/MMM/11189446-7fc1-ed11-8159-005056aa4246/2_11189446-7fc1-ed11-8159-005056aa4246_11_20161.pdf?fireglass_rsn=true#fireglass_params&tabid=ae6f8e7252902d0a&start_with_session_counter=4&application_server_address=isagovil-2-me-west1.prod.fire.glass.

63 <https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/>.

64 שם.



בנוסף, קיים חשש שפרקטיקות אסורות יהפכו למורכבות וקשות יותר לגילוי כתוצאה מהשימוש במערכות בינה מלאכותית. כך, למשל, עבירת הספופינג (spoofing) – מצב שבו מוזרמות למערכת הבורסה פקודות קניה ומכירה שאין כוונה שיתממשו כדי להשפיע על המחירים. עבירה זו אמנם אינה חדשה, אך היא עלולה להתעצם ולהפוך מורכבת לגילוי והוכחה, במיוחד במצבים בהם קיימת אינטראקציה בין מערכות בינה מלאכותית שונות, גם אם לא תוכננו כך במקור.⁶⁵

ג. **סיכון לתחרות** – הסיכון לפגיעה בתחרות אינו ייחודי רק למגזר הפיננסי, אך הוא עלול להתעצם ולהתגבר במגזר זה, לנוכח כניסתה של טכנולוגיית הבינה המלאכותית ולנוכח ריכוזיות המערכת הפיננסית. כך למשל, במצב בו קיים שוק ריכוזי עם מספר מצומצם של ספקי מערכות בינה מלאכותית לסקטור הפיננסי, מתגבר הסיכון לפגיעה בתחרות (בנוסף לסיכונים היציבות שהוזכרו לעיל). הדברים דומים גם כאשר דנים בצד השני של אותו המטבע – מאגרי המידע העומדים בבסיס מערכות הבינה המלאכותית. ריכוז של מידע נרחב אצל מספר מצומצם של ספקים עלול להביא לפגיעה בתחרות, ביחוד כלפי ספקים שאין להם נגישות רחבה למידע או שאינם בעלי משאבים מספקים, וליצירת חסמי כניסה שאינם קיימים בהכרח במערכות הפיננסיות ה"מסורתיות". זאת ועוד, האינטראקציה בין מערכות הבינה המלאכותית השונות עלולה להביא לתיאום מחירים או ניצול מעמד מונופוליסטי לרעה, פעולות אסורות על פי דיני התחרות.⁶⁶

ד. **מחיר טעות גבוה (high cost of error)** – קיימים תחומי פעילות בהם לטעות של מערכת הבינה המלאכותית עלולה להיות השפעה קשה על הפרט, למשל מגזר הבריאות בו פענוח לא נכון של בדיקה קריטית או אבחנה שגויה של מחלה עלול להוביל לתוצאה בלתי הפיכה. ניתן לומר שגם במגזר הפיננסי טעות של מערכת בינה מלאכותית עלולה להיות בעלת השפעה שלילית ברמה גבוהה – למשל, הפסד חסכוניות כתוצאה מטעות של מנהל תיקים אלגוריתמי, דחיית בקשת הלוואה כתוצאה מהטיה או אפליה, דחיית חיתום ביטוחי כתוצאה מהיעדר בסיס נתונים מספק וכו'.

ה. **אמון במערכת הפיננסית** – המערכת הפיננסית מבוססת על אמון הציבור. אמון זה הכרחי לפעילות בכל תחומי הפיננסים. כך למשל, הציבור עושה שימוש באמצעי התשלום על בסיס ההנחה שהם יכובדו במלוא ערכם, מפקיד כספו בבנקים או בגופים מוסדיים על בסיס ההנחה שהם ישמרו וידאגו לכספים אלה; ומשקיע בניירות ערך על בסיס ההנחה של תקינות המסחר ופעילות החברות שהנפיקו את ניירות הערך. היעדר אמון הציבור במערכת הפיננסית, בשונה מאשר במערכות אחרות בתחומי חיים שונים, משמעותו כי המערכת כלל לא תתקיים, על כל השלכות הדבר על מרקם החיים המוכר לנו.



65 דוח ה-OECD משנת 2021, בעמוד 28.

66 Gal, Michal and Rubinfeld, Daniel L., Algorithms, AI and Mergers (June 5, 2023). Antitrust Law Journal (2023), NYU Law and Economics Research Paper No. 23-36, <https://ssrn.com/abstract=4469586>

ו. הבינה המלאכותית ברגולציה פיננסית בעולם

העיסוק הכללי בבינה מלאכותית, והשימושים הרבים האפשריים שלה בתחום הפיננסי, הובילו רגולטורים פיננסיים ברחבי העולם לעסוק בנושא בשנים האחרונות, וביתר שאת מאז פריצתה של הבינה המלאכותית היוצרת.

ארגון ה-OECD פרסם בשנת 2021 דוח מקיף בנוגע לבינה מלאכותית, למידת מכונה ונתוני עתק בסקטור הפיננסי. הדוח סוקר את האתגרים, התועלות וההשלכות של השימוש בטכנולוגיית הבינה המלאכותית בסקטור הפיננסי ומציע דרכי התמודדות אסדרתיות לקובעי מדיניות ולרגולטורים.⁶⁷ בהמשך לכך פרסם ה-OECD בשנת 2023 סקירה בנוגע לשימושי בינה מלאכותית יוצרת בסקטור הפיננסי. הנייר מתאר את ההתקדמות בתחומי הבינה המלאכותית היוצרת והטמעתה (האיטית) בארגונים פיננסיים, מנתח את הסיכונים הפוטנציאליים הגלומים בשימוש בטכנולוגיה באופן נרחב, וממליץ על צעדים שעל קובעי מדיניות ורגולטורים לנקוט בהקשר זה.⁶⁸ בדומה לכך, **קרן המטבע הבינלאומית** פרסמה דוח העוסק בהזדמנויות של שימוש בבינה מלאכותית ולמידת מכונה במגזר הפיננסי והאתגרים הייחודיים לה,⁶⁹ ולאחר מכן דוח הסוקר את האתגרים שבשימוש בינה מלאכותית יוצרת בעולמות הפיננסיים.⁷⁰ **הבנק הבינלאומי לסליקה** (BIS), הארגון הבינלאומי של הבנקים המרכזיים) פרסם נייר המתמקד בנתוני עתק ולמידת מכונה בבנקים מרכזיים,⁷¹ נייר נוסף המתמקד בהיבטי עקרונות ממשל בינה מלאכותית ומעורבות אנושית,⁷² ומספר ניירות נוספים, ובכלל זאת יחד פרק בדוח הכלכלי של שנת 2024 להשלכות הבינה המלאכותית על בנקים מרכזיים.⁷³ **IOSCO**, **הארגון הבינלאומי של רשויות ניירות ערך**, פרסם דוח אודות השימוש בבינה מלאכותית ולמידת מכונה על ידי מתווכים פיננסיים ומנהלי השקעות, הסוקר את הסיכונים הכרוכים בטכנולוגיה ומציע מדריך לקובעי מדיניות ורגולטורים בנושאי ממשל בינה מלאכותית ופיקוח; פיתוח אלגוריתמים וניטור; איכות בסיסי הנתונים והטיות; שקיפות והסברתיות; מיקור חוץ; ושיקולים אתיים (להלן: "**דוח IOSCO משנת 2021**").⁷⁴ גם רשות ניירות ערך האירופית (ESMA) פרסמה מאמר בנושא שימוש בבינה מלאכותית בשוק המניות האירופי, היישומים שבשימוש וקצב האימוץ (האיטי).⁷⁵

בארה"ב התייחסו רגולטורים פיננסיים לסוגיות שונות בעולמות הבינה המלאכותית: כך, למשל, רשות ניירות ערך האמריקאית (SEC) הציעה לתקן את הוראותיה בכל הנוגע לניגודי עניינים הנוצרים תוך שימוש בניתוח של מידע צופה עתיד על ידי יועצי השקעות וברוקר-דילרים (ובכלל זאת שימוש בבינה מלאכותית)(להלן: "**הצעת ה-SEC משנת 2023**")⁷⁶; המשרד להגנת הצרכן הפיננסי (CFPB), רגולטור העוסק בעיקר בהיבטים צרכניים בשדות הבנקאות והאשראי, פרסם מספר התייחסויות בנושא בינה מלאכותית, ובין היתר בעניין שימוש ביישומי בינה מלאכותית ככלי לשירות לקוחות,⁷⁷ וחוזר בנושא שימוש בהסברתיות בדחיית מתן אשראי תוך שימוש ביישומי בינה מלאכותית מורכבים (להלן: "**חוזר ה-CFPB משנת 2023**")⁷⁸; והרשות הפדראלית לצרכנות (FTC) פרסמה מספר התייחסויות,

67 דוח ה-OECD משנת 2021.

68 דוח ה-OECD משנת 2023.

69 IMF, Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance (October 2021), <https://www.imf.org/en/publications/departamental-papers-policy-papers/issues/2021/10/21/powering-the-digital-economy-opportunities-and-risks-of-artificial-intelligence-in-finance-494717>

70 IMF, Generative Artificial Intelligence in Finance: Risk Considerations (August 2023), <https://www.imf.org/en/publications/fintech-notes/issues/2023/08/18/generative-artificial-intelligence-in-finance-risk-considerations-537570>

71 BIS, BIS Working Papers No 930 – Big data and machine learning in central banking (March 2021), https://www.bis.org/publ/work930.htm?force_isolation=true

72 FSI, FSI Insights on policy implementation No 35 – Humans keeping AI in check – emerging regulatory expectations in the financial sector (August 2021), https://www.bis.org/fsi/publ/insights35.htm?force_isolation=true

73 BIS Annual Economic Report 2024, <https://www.bis.org/publ/arpdf/ar2024e.pdf>

74 International Organization of Securities Commissions (IOSCO), The use of artificial intelligence and machine learning by market intermediaries and asset managers – Final report (September 2021), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf?force_isolation=true

75 דוח ESMA משנת 2023.

76 SEC, Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers (July 2023), <https://www.sec.gov/rules-regulations/2023/07/s7-12-23>

77 ראו ה"ש 45 לעיל.

78 CFPB, Consumer Financial Protection Circular 2023-03 (September 2023), https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/?force_isolation=true

בהן בנושא מאמצי אכיפה כנגד מערכות אוטומטיות המייצרות אפליה והטיות (כהצהרה משותפת ביחד עם רגולטורים נוספים),⁷⁹ ואישור שימוש באמצעי אכיפה כנגד מוצרים ושירותים העושים שימוש בבינה מלאכותית.⁸⁰

בבריטניה פרסמו רשות הפיקוח הפיננסית (FCA) והבנק המרכזי מספר התייחסויות בנושא בינה מלאכותית, בהן נייר להערות הציבור בנוגע לשימוש בכלי בינה מלאכותית במגזר הפיננסי,⁸¹ וסקר שימושים של יישומים מבוססי למידת מכונה בשירותים הפיננסיים בבריטניה.⁸² הניירות אמנם לא כוללים המלצות, אך הם משקפים במידה רבה את גישת הממשלה הבריטית שתוארה לעיל – הסמכת הרגולטורים הסקטוריאליים לקבוע את המדיניות והרגולציה בתחומם.

רגולטורים פיננסיים במדינות מפותחות נוספות דוגמת **סינגפור**,⁸³ **הונג קונג**,⁸⁴ **הולנד**,⁸⁵ **קנדה** (אונטריו)⁸⁶ ועוד, פרסמו דוחות בנוגע לשימוש במערכות בינה מלאכותית בסקטור הפיננסי, רובם עוסקים בעקרונות הכלליים שעל גופים פיננסיים לקחת בחשבון בבואם לפתח או לאמץ מערכות בינה מלאכותית.

בתקופה שחלפה מאז פרסום דוח הביניים להערות הציבור, חלו מטבע הדברים התפתחויות רגולטריות שונות. כך למשל, בחודש דצמבר 2024 פרסם משרד האוצר האמריקאי דוח העוסק בבינה מלאכותית בשירותים הפיננסיים.⁸⁷ דוח זה כלל המלצות בעיקר לגופי ממשל ורגולטורים פיננסיים ובהן המשך שיתוף פעולה בינלאומי לקידום סטנדרטים עקביים ומשמעותיים בגין השימוש בבינה מלאכותית בסקטור הפיננסי; קידום שיח עם התעשייה לגבי פערי רגולציה קיימים שעלולים לגרום נזק ללקוחות הפיננסיים; שיפור מסגרות ניהול הסיכונים הקיימות ולעבוד בשיתוף פעולה עם רגולטורים אחרים על מנת להבהיר את הציפיות הפיקוחיות בסקטור; בחינת התאמת יישומי הבינה המלאכותית על-ידי הגופים המפוקחים לדרישות הרגולציה לפני תחילת השימוש בהם וביצוע בחינה תקופתית באשר לאופן ציות המערכות. בחודש יוני 2025 החליטה רשות ניירות ערך האמריקאית (SEC) לחזור בה מההצעה שפרסמה בשנת 2023, אשר ביקשה להתמודד עם ניגודי עניינים בקשר עם ניתוח מידע תחזיתי (Predictive Data Analytics)

79 FTC, Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems (April 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf?force_isolation=true

80 FTC, Resolution Directing Use Of Compulsory Process in a Non-Public Investigation of Products and Services that Use or Are Produced Using Artificial Intelligence or that Purport to Detect the Use of Artificial Intelligence (November 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/232%203087%20AI%20Omnibus%20Resolution.pdf?force_isolation=true

81 Bank of England & FCA, DP5/22 – Artificial Intelligence and Machine Learning: Discussion Paper 5/22 (October 2022), https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence?force_isolation=true

82 Bank of England & FCA, Machine Learning in UK Financial Services (October 2022), <https://www.bankofengland.co.uk/report/2022/machine-learning-in-uk-financial-services>

83 MAS, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector (February 2019), https://www.mas.gov.sg/-/media/mas/news-and-publications/monographs-and-information-papers/feat-principles-updated-7-feb-19.pdf?force_isolation=true

84 HKMA, High-level Principles on Artificial Intelligence (November 2019), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf?force_isolation=true. הרגולטור הבנקאי בהונג-קונג פרסם מדריך למגזר הבנקאי על שימוש ביישומי בינה מלאכותית. בסקר שימושים שערך מצא כי בנקים רבים אימצו או מתכננים לאמץ יישומי בינה מלאכותית, בין היתר בשירות לקוחות, שיווק, ביצוע תהליכים פנימיים ותפעוליים, ניהול סיכונים, סייבר, ועוד. בדומה לנייר הסינגפורי, גם הרגולטור בהונג-קונג קבע מספר עקרונות כלליים אשר על בנקים לקחת אותם בחשבון בעיצוב, אימוץ ושימוש ביישומי בינה מלאכותית וניתוח נתוני עתק. בין העקרונות ניתן למצוא אחריות של הדיקטוריון והנהלה הבכירה על פלטי המערכות, שימוש בנתונים באיכות גבוהה, דרישת הסברתיות מספקת, ביצוע תיקוף קפדני ליישומי הבינה המלאכותית, קביעת נהלים ופיקוח מספק על ספקי יישומי בינה מלאכותית בהם נעשה שימוש, הטמעת פתרונות סייבר מתאימים, ועוד.

85 DNB, General principles for the use of Artificial Intelligence in the financial sector (July 2019), https://www.dnb.nl/media/voffsrc/general-principles-for-the-use-of-artificial-intelligence-in-the-financial-sector.pdf?force_isolation=true. הבנק המרכזי בהולנד פרסם מספר עקרונות כלליים לשימוש ביישומי בינה מלאכותית בסקטור הפיננסי. העקרונות מחולקים לשישה תחומים עיקריים, והם: יציבות; אחריות; הוגנות; אתיות; כישורים; ו-שקיפות.

86 OSC & EY, Artificial Intelligence in Capital Markets: Exploring Use Cases in Ontario (2023), https://www.osc.ca/sites/default/files/2024-11/pub_20231010_artificial-intelligence-in-capital-markets.pdf. הנייר של רגולטור ניירות הערך בפרובינציית אונטריו בקנדה סוקר את היתרונות והאתגרים הצפויים כתוצאה משימוש ביישומי בינה מלאכותית, מציג מקרי בוחן של השימושים כאמור בגופים פיננסיים תחת פיקוחו וממפה את הסיכונים הכרוכים בשימושים העיקריים. התמונה העולה מן הדוח מגלה שהאימוץ של יישומי בינה מלאכותית באונטריו, קנדה, עולה בהדרגה ונמצא כעת בשלב ביניים. בנוסף, נמצא כי כללי הממשל הקיימים אינם מספקים מענה טוב דיו לאתגרים שמזמנים יישומי הבינה המלאכותית, וכי יש לפתח ולאמץ כללי ממשל אשר שמים דגש על שימוש אחראי והסברתיות של יישומי הבינה המלאכותית, לצד התייחסות במסגרות ניהול הסיכונים של הגופים הפיננסיים.

87 הקול הקורא – <https://home.treasury.gov/system/files/136/Treasury-AI-RFI-financial-sector-2024.pdf>; הדוח הסופי – <https://home.treasury.gov/news/press-releases/jy2760>

בעבודת ברוקר-דילר ויועצי השקעות. הצעה זו עוררה ביקורת, וכאמור ה-SEC הודיעה כי אינה מתכוונת לפרסם רגולציה חדשה על בסיסה.⁸⁸

בבריטניה נמשכה המדיניות לפיה יש להסתמך על הרגולציה הקיימת, תוך מתן גמישות לרגולטורים בתחומי הסמכות שלהם, ולהימנע מחקיקה רוחבית לתחום הבינה המלאכותית. גישה זו קיבלה ביטוי בתכנית האסטרטגית החמש-שנתית של ה-FCA לשנים 2025 – 2030⁸⁹ הרגולטורים הפיננסיים הבריטיים (FCA ו-PRA) פרסמו סקר שימושים נוסף אודות השימוש בבינה מלאכותית במגזר הפיננסי,⁹⁰ בו נמצא שכ-75% מהחברות הפיננסיות עושות שימוש בבינה מלאכותית, בעוד כ-10% נוספות מתכוונות להכניס מערכות בינה מלאכותית לשימוש בשלוש השנים הקרובות. נתונים אלה גבוהים משמעותית מאלו שנמצאו בסקר השימושים הקודם. יחד עם זאת, אימוץ פתרונות מבוססי בינה מלאכותית אוטונומיים ואוטומטיים לחלוטין עדיין נעשה בקצב איטי ומבוקר: רק ב-2% ממקרי המבחן שנסקרו בסקר השימושים נמצא כי מערכות הבינה המלאכותית מקבלות החלטות באופן מלא ומבצעות פעולות אוטונומיות לחלוטין.⁹¹

כמהלך משלים למאמצי ה-FCA לתמוך באימוץ מערכות בינה מלאכותית בסקטור הפיננסי, הוקם לאחרונה ארגון-חול רגולטורי ייעודי לבינה המלאכותית, אשר מיועד לחברות אשר נמצאות בשלבים ראשונים של זיהוי ואימוץ פתרונות מבוססי מערכות בינה מלאכותית.⁹² בנוסף, הוקמה מעבדת בינה מלאכותית ב-FCA, שמטרתה לאפשר לרגולטור להבין לעומק את האתגרים וההזדמנויות הכרוכים בשימוש במערכות בינה מלאכותית בסקטור הפיננסי ואיך אלו משפיעים על לקוחות ועל השוק בכללותו, ובכך לנקוט בגישה רגולטורית פרקטית ושיתופית.⁹³ במקביל, ה-FCA פרסם כי הוא מפתח קוד ייעודי (statutory code of practice) לחברות המפתחות ומטמיעות מערכות בינה מלאכותית במגזר הפיננסי.⁹⁴

התמונה הכללית העולה היא כי בעולם אין לרוב רגולציה ספציפית שנקבעה ביחס לבינה מלאכותית בסקטור הפיננסי, ורוב הרגולטורים מסתפקים במעקב, בבחינת הנושא, ובהנחיות שעניינן תחולת ויישום של הרגולציה הקיימת גם ביחס לפעילות בבינה מלאכותית. יש לסייג עם זאת כי בחלק מהמדינות, ובראשן מדינות האיחוד האירופאי, נקבעה חקיקה רוחבית בנוגע לבינה מלאכותית אשר תחול ככלל גם ביחס לסקטור הפיננסי. עוד יש לסייג, כי הרגולציה הפיננסית עוקבת באופן טבעי אחר ההתפתחויות בשוק. הואיל והאימוץ של בינה מלאכותית בסקטור הפיננסי הנו מוגבל בשלב זה, אין זה מפתיע כי לרוב לא נקבעה גם רגולציה ייעודית לשם טיפול בנושא. ככל שאימוץ הטכנולוגיה יהפוך נרחב ומשמעותי יותר, כך עשויה גם הרגולציה הפיננסית להשתנות בהתאם.

⁸⁸ <https://www.sec.gov/rules-regulations/2025/06/s7-12-23>

⁸⁹ https://www.fca.org.uk/publications/business-plans/annual-work-programme-2025-26?force_isolation=true

⁹⁰ מדובר בעדכון לסקר השימושים שבוצע בשנת 2022, ראו ה"ש 74.

⁹¹ https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024?force_isolation=true

⁹² https://www.fca.org.uk/news/press-releases/fca-allows-firms-experiment-ai-alongside-nvidia?force_isolation=true#:~:text=In%20April%202025%2C%20the%20FCA,by%20relying%20on%20existing%20frameworks

⁹³ <https://www.fca.org.uk/firms/innovation/ai-lab>

⁹⁴ <https://www.ftadviser.com/content/dbb2992c-591b-4c65-96b7-302635242a17>

ז. פעילות בינה מלאכותית בסקטור הפיננסי בישראל

בדומה לנעשה בעולם, גם בישראל החלו גופים פיננסיים לעשות שימוש ביישומים מבוססי בינה מלאכותית, במגוון פעילויות. כך למשל, בתחום הבנקאות, זה שנים לא מעטות בנקים עושים שימוש במערכות בינה מלאכותית לשם חיתום ודירוג אשראי ללווים. כמו כן, גופים העוסקים בניהול תיקים ומסחר בניירות ערך עושים שימוש במערכות בינה מלאכותית עבור פעילותם במסחר אלגוריתמי, במסחר בתדירות גבוהה, בניתוח תחזיות עסקיות וכלכליות, וכדומה.

על אף שהשימוש ביישומי בינה מלאכותית אצל גופים פיננסיים בישראל אינו חדש, ובדומה למגמה המסתמנת בעולם, השינוי הצפוי הוא בהיקף השימוש וביכולות של טכנולוגיית הבינה המלאכותית. ואמנם, התפתחותן של מערכות בינה מלאכותית מן הדור המתקדם יותר, הכולל בינה מלאכותית יוצרת, מעוררת עניין רב בסקטור הפיננסי בישראל וניכר כי נבחנים יישומים אפשריים לטכנולוגיה. בד בבד, **התרשמות הצוות היא כי לעת עתה קצב האימוץ של מערכות בינה מלאכותית עודנו איטי**. סיבות מרכזיות לקצב האימוץ הן קיומן של מערכות קיימות (legacy systems) וההשקעה הנדרשת בהחלפתן, מידת המהימנות של מערכות הבינה המלאכותית, וסיכונים שמעוררת הטמעת מערכות בינה מלאכותית, למשל בהיבטי ציות ומוניטין. עוד התרשם הצוות כי מסתמן פער שעשוי להתהוות בהיקף השימוש בבינה מלאכותית בין גופים פיננסיים גדולים ו"מסורתיים" ובין גופים קטנים וחדשים. נראה כי אצל האחרונים יש נכונות ומאמץ גדול יותר לעשות שימוש בבינה מלאכותית, בין היתר כדי להשיג יתרון תחרותי בדרך זו. נראה אם כן, כי יש עוד מרחק בטרם ניתן יהיה לראות יישומי בינה מלאכותית מתקדמים אשר מבצעים את פעילויות הליבה של הגוף הפיננסי מקצה-לקצה, באופן אוטומטי ואוטונומי, תוך יצירת אינטראקציה עם לקוח הקצה וללא כל מעורבות אנושית. מרבית הפעילויות המבוצעות כיום על ידי מערכות בינה מלאכותית בסקטור הפיננסי בישראל מסייעות לגורם אנושי לבצע משימות מורכבות או לקבל החלטות על סמך מידע רב, או שהן תפעוליות באופיין (back-office) המסייעות ביעול תהליכים, זיהוי הונאות פיננסיות, ניהול סיכונים, שיווק ומכירות וכיוצא באלו.

מסקר שימושים שערכה רשות שוק ההון, ביטוח וחיסכון בשנת 2022 ביחס לשימוש ביישומי בינה מלאכותית של גופים מוסדיים המייצגים מגוון שירותים פיננסיים בתחום הביטוח וחיסכון ארוך הטווח, נמצא, בין היתר, כי יישומי בינה מלאכותית נמצאים בשימוש ראשוני במספר גופים ויישומים נוספים נמצאים בפיתוח, כך שצפויה מגמת עליה בשימוש ביישומים אלה. תחומי השימוש ביישומי בינה מלאכותית מגוונים והם כוללים ניתוח התנהגות מבוטחים, יישוב תביעות, שירות לקוחות וייעול התפעול.

מסקר שימושים שנערך על ידי רשות ניירות ערך ביחס לשימוש ביישומי בינה מלאכותית בענף קרנות הנאמנות בשנת 2024, עלתה תמונה דומה. כמחצית ממנהלי הקרנות העידו כי הם עושים שימוש במערכות בינה מלאכותית, אלא שהשימוש כאמור נעשה באופן מוגבל ומצומצם, בעיקר בתחומי האנליזה והמחקר, מסחר וקבלת החלטות השקעה. ניתן גם לראות שבקרנות גידור בנאמנות, להן חופש פעולה רחב יותר, ובקרנות גמישות, השימוש מעט נרחב יותר ביחס לקרנות נאמנות בעלות אופי השקעה אחר.

יש לציון, כי באופן כללי קשה לעמוד בצורה מדויקת על קצב אימוץ יישומי בינה מלאכותית מתקדמים והיקפם בסקטור הפיננסי. גם סקרים בנושא אימוץ בינה מלאכותית הם מוגבלים מטבעם, לנוכח אי-אחידות באופן בו מגדירים הגופים פעילות של בינה מלאכותית, ולנוכח השימושים הרבים האפשריים.

תמונת המצב הכללית לגבי הסקטור הפיננסי בישראל, תואמת ממצאים ממדינות אחרות בעולם, לפיהם קצב האימוץ של בינה מלאכותית בסקטור זה הוא איטי ומבוזר. ואולם, הערכת השחקנים בתחום היא כי בינה מלאכותית תתפוס תפקיד הולך וגדל בפעילויות הפיננסיות, והערכה זו אף מקבלת ביטוי בהשקעת תשומות הולכות וגדלות בבחינת יישומים אפשריים והטמעתם.



ח. הצוות הבין-משרדי לבניה מלאכותית בסקטור הפיננסי

1. הרקע להקמת הצוות

בחודש דצמבר 2020 פרסמה המחלקה הכלכלית ביעוץ וחקיקה במשרד המשפטים קול קורא לעריכת מחקר וסקירה של שימושים נפוצים בבניה מלאכותית ונתוני עתק במגזר הפיננסי וסקירה השוואתית של התמודדות רגולטוריות עם שימושים אלו. צוות בינתחומי מאוניברסיטת תל-אביב, בראשות פרופ' אסף חמדני ופרופ' קובי קסטיאל (מהפקולטה למשפטים) ופרופ' דן עמירם וד"ר ארי אחיעז (מהפקולטה לניהול), נבחר להוביל את המחקר. הצוות ערך מיפוי של השימושים הנפוצים בבניה מלאכותית במגזר הפיננסי, הציג את הסוגיות העקרוניות המתעוררות עקב שימוש בכלי בינה מלאכותית בכלל (וסוגיות הייחודיות למגזר הפיננסי בפרט), סקר היבטים רגולטוריים ומשפטיים של שימוש בבניה מלאכותית במגזר הפיננסי ובחן מגמות עולמיות באסדרה של בינה מלאכותית תוך התייחסות להיבטים הקשורים באופן ספציפי למגזר הפיננסי (להלן: **"דוח אונ' תל-אביב"**).⁹⁵ דוח אונ' תל-אביב פורסם בחודש אוגוסט 2022, ועל המלצותיו העיקריות ניתן למנות את אלה:

- א. יש לשמר את מעמדה של ישראל כמוקד חדשנות, תוך איזון עם אינטרסים מוגנים בתחום הפיננסי, דוגמת הגנת הצרכן ושמירה על יציבות המערכת הפיננסית.
- ב. יש להתאים את האסדרה העתידית בתחום הבינה המלאכותית, ובסקטור הפיננסי בפרט, לסטנדרטים בינלאומיים שייקבעו, זאת בכדי למנוע חסמי כניסה לשחקנים זרים לשוק הישראלי ולעודד כניסת שחקנים חדשים (זרים ומקומיים) וטכנולוגיות חדשות לשוק הישראלי.
- ג. יש להימנע, בשלב זה, מקביעת כללים אחידים לכלל השימושים ביישומי בינה מלאכותית רק מעצם היותם מבוססים על טכנולוגיה דומה, ויש להבחין בין שימושים שונים שעלולים להביא עמם גם סיכונים שונים. יחד עם זאת, ייתכנו סוגיות בעלות מאפיינים דומים בשימושים שונים, ולכן יש צורך בתיאום האסדרה בענפי המשפט ובין גורמי הפיקוח הרלוונטיים, וכן ביישום מדיניות ממשלתית ברורה. החוקרים המליצו להפקיד את התיאום כאמור, של כל יישומי הבינה המלאכותית בתחומים השונים, בידי גורם ממשלתי אחד בעל מומחיות בתחום.
- ד. יש לעודד, לפחות בשלב זה בו קיים חוסר ודאות רגולטורי באשר לשימוש ביישומי בינה מלאכותית, פיתוח מודלים של רגולציה עצמית המבוססים על עקרונות ויעדים מקובלים. כמו כן, מומלץ לאמץ מודלים של ארגז חול רגולטורי (regulatory sandbox) שיש בכוחו לסייע הן בזירוז כניסת טכנולוגיות חדשות לשוק, והן בהבנת גורמי הפיקוח הרלוונטיים את הטכנולוגיה העומדת בבסיס השירותים או המוצרים החדשים ובכך אף לפתח מומחיות בנושא (דבר שבתורו יכול לסייע בהמשך ביצירה ועיצוב של אסדרה מתאימה).
- ה. יש לבצע תיאום בין גורמי הפיקוח הפיננסיים בכל הנוגע לפיקוח על משטרי הרישוי וכללי האחריות, לרבות קביעת הסדרים אחידים. עוד הוצע לבחון את חסמי הכניסה לשוק הישראלי וההשפעות הטכנולוגיות עליהם, ולבצע התאמה של הליכי הרישוי בתחומים השונים. באופן דומה, נוכח העובדה שקיימים מספר מפקחים פיננסיים בשוק הישראלי, דבר שעלול לייצר חוסר ודאות רגולטורית ואף ארביטראז' רגולטורי, מומלץ להתמקד בהאחדה של דרישות גורמי הפיקוח ביחס לסוגיות בעלות מאפיינים טכנולוגיים דומים, הן בפן המשפטי והן בפן הפיקוחי.
- ו. מבין שלל התחומים שנסקרו, הומלץ למקד את מאמצי פיתוח הרגולציה הפיננסית בתחומים הבאים: (א) ייעוץ – ייעוץ השקעות, ייעוץ פנסיוני; (ב) אשראי.

בהמשך לעבודה זו, על רקע ההתפתחויות המהירות בטכנולוגיית הבינה המלאכותית, ובהתאם להמלצות המסתמנות של מסמך המדיניות לבחון רגולציה ענפית, בחודש דצמבר 2022 הוקם הצוות לבחינת ההשפעות של מערכות אלגוריתמיות ובינה מלאכותית במגזר הפיננסי (להלן: "הצוות").

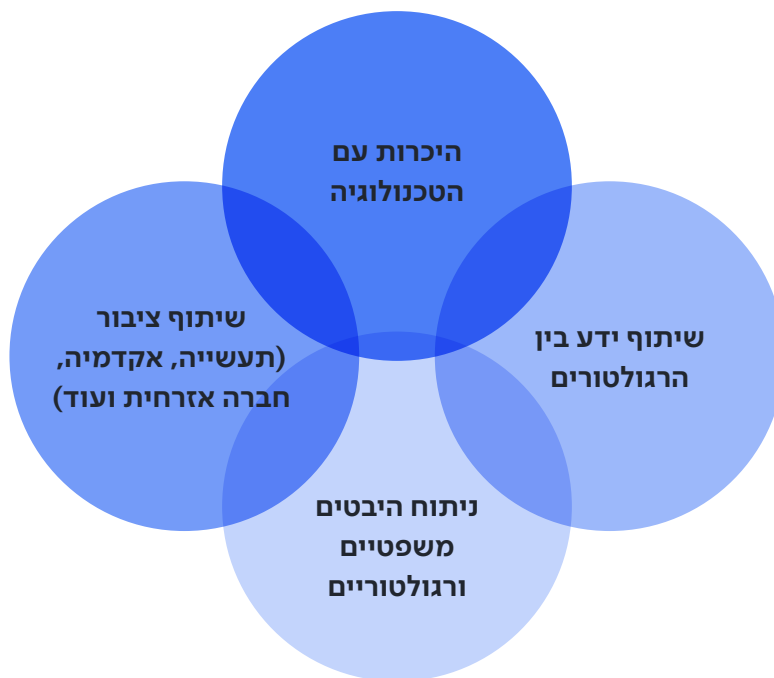
הצוות, אשר מורכב מנציגי משרדי האוצר והמשפטים (יעוץ וחקיקה, המחלקה הכלכלית), רשות התחרות, רשות ניירות ערך, בנק ישראל (הפיקוח על הבנקים) ורשות שוק ההון, ביטוח וחסכון, הונחה לבחון את ההשלכות

⁹⁵ אחיעז, חמדני, עמירם, קסטיאל, בינה מלאכותית במגזר הפיננסי: שימושים נפוצים, אתגרים וסקירה השוואתית של התמודדות רגולטוריות (דוח מחלקה הכלכלית ביעוץ וחקיקה במשרד המשפטים (יולי 2022). https://www.gov.il/BlobFolder/news/ai_report/he/AI_report.pdf?fireglass_rsn=true

הרגולטריות והמשפטיות שיש ליישומי בינה מלאכותית על פעילויות ושירותים פיננסיים, ולגבש המלצות בעניינם. נקבע כי על ההמלצות, לעסוק, בין השאר, בצורך באסדרה ובאופן עיצוב האסדרה הראויה, בהבהרות המשפטיות הנדרשות ביחס לדין הקיים, ובחסמים שנדרש להסירם. הצוות הונחה להתמקד בפרט בשימושי בינה מלאכותית הקשורים לחיתום אשראי וביטוח; לניהול תיקי השקעות ולפעולות ייעוץ; והמודלים בבסיס האלגוריתמים שבשימוש.

2. עבודת הצוות

במהלך עבודתו קיים הצוות עשרות מפגשים בהם למד לעומק את היישומים האפשריים של בינה מלאכותית בסקטור הפיננסי, ניתח את הסוגיות העיקריות העולות בקשר לפעילות זו, בחן את הרגולציה המתהווה בעולם, ודן בהמלצות אפשריות ביחס לפעילות זו בישראל.



במסגרת עבודתו פעל הצוות בכמה מישורים, ובכלל זאת:

- א. **היכרות עם הטכנולוגיה שבבסיס יישומי בינה מלאכותית** – הצוות נפגש עם גורמים בכירים מעולמות הטכנולוגיה, מהארץ ומחו"ל, כדי להבין את היסודות עליהם מושתתת טכנולוגיית הבינה המלאכותית.
- ב. **שיתוף ידע רגולטורי** – חברי הצוות שיתפו בפעולות הרגולטריות והמחקריות שבוצעו על-ידי כל אחד מהגופים החברים בו בקשר עם בינה מלאכותית.
- ג. **ניתוח היבטים המשפטיים והרגולטוריים של בינה מלאכותית** – הצוות עסק רבות בלימוד היבטים אלה ואף נפגש עם מומחי תוכן מהאקדמיה והשוק הפרטי, במטרה להבין לעומק את הסוגיות המשפטיות המרכזיות המתעוררות בעקבות שימוש ביישומי בינה מלאכותית.
- ד. **פרסום קול קורא ומפגשים עם גורמים שונים מהתעשייה, האקדמיה, חברה אזרחית, גורמי ממשל ורגולטורים זרים** – בחודש אפריל 2023 פרסם הצוות קול קורא, במסגרתו התבקש הציבור הרחב ובעלי עניין להביע את עמדותיהם והתייחסותם לסוגיות שונות, ובהן: שימושים נוכחיים ועתידיים בבינה מלאכותית במגזר הפיננסי; חסמים (טכנולוגיים, עסקיים, משפטיים) העומדים בפני גופים פיננסיים אחרים הקשורים לפיתוח, התנסות ושימוש בכלי בינה מלאכותית; התועלות שעשויות לנבוע והאתגרים והסיכונים הכרוכים בשילוב כלי בינה מלאכותית בגופים פיננסיים; שימוש בכלים להתמודדות עם האתגרים והסיכונים שבשימוש

בבינה מלאכותית במגזר הפיננסי; מדיניות ואסדרה ראויות בתחום הבינה המלאכותית במגזר הפיננסי ועוד.⁹⁶ לקול הקורא התקבלו התייחסויות מצד 17 גופי תעשייה (לרבות חברות יעוץ, איגוד מקצועי ומשרד עורכי דין בינלאומי), חברה אזרחית ואקדמיה. ההתייחסויות נגעו למספר תחומים הרלוונטיים לבינה מלאכותית, ובכלל זאת ביטוח, אשראי, אפליה, הלבנת הון, זיהוי מעילות, הונאות ואנומליות בשוק ההון, חסיון מידע ופרטיות, הון אנושי, שימוש אחראי בבינה מלאכותית (responsible AI) והסברתיות, תחרות, אבחנה בין סיכונים הכרוכים בשימוש בבינה מלאכותית, המתווה הרגולטורי הראוי וכו'. בנוסף לכך נפגש הצוות עם בעלי עניין שונים בתחום הבינה המלאכותית, לרבות גורמים אשר הגישו את התייחסותם לקול הקורא וגורמים נוספים מסקטורים שונים אשר הצוות ביקש את עמדתם בנושא. כך, לדוגמה, נפגש הצוות עם גורמי תעשייה מתחום הבנקאות, הביטוח, המסחר האלגוריתמי, הטכנולוגיה (לרבות ענקיות טכנולוגיה), הלבנת הון, המשפט; גורמי אקדמיה (מקומיים ובינלאומיים) מתחומי המשפטים, מדיניות ציבורית ומדעי המחשב; גורמי ממשל ומאסדרים מקומיים וזרים (רשות הפרטיות בישראל, OECD, האיחוד האירופי, ESMA, מאסדרים בארה"ב, אנגליה, סינגפור); וגורמי חברה אזרחית. המפגשים עסקו בקשת רחבה של נושאים וסייעו מאוד לצוות בהיבטים רבים, לרבות בהבנה של יישומי בינה מלאכותית בהם נעשה שימוש בשוק כבר כיום והצפי לעתיד. בנוסף קיים הצוות סדנאות שעסקו בהתמודדות עם טכנולוגיה חדשנית "משבשת" ואפשרויות ההתמודדות עם טכנולוגיה כזו ויישומיה.

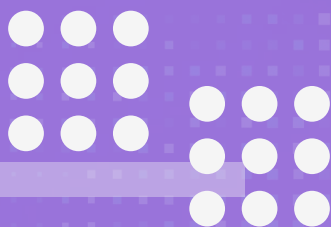
3. דוח הביניים

דוח הביניים פורסם להערות הציבור באוקטובר 2024, ובעקבותיו נערכה עבודה נוספת של הצוות שכללה מפגשים עם מגוון גורמים, ימי עיון, ודיונים בהערות הציבור לקראת הגשת הדוח וההמלצות סופיים. לדוח הביניים התקבלו 24 מסמכי הערות ציבור. טבלה מסכמת של הערות אלה מופיעה בנספח ד' לדוח.

⁹⁶ https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic/al_lobby/al_lobby-637f62a916518/Artificial_intelligence_team_financial_sector.pdf?fireglass_rsn=true#fireglass_params&tabid=a315d0774bfe64f2&start_with_session_counter=3&application_server_address=isagovil-2-me-west1.prod.fire.glass

חלק ב'

גישה כללית,
עקרונות מנחים
לטיפול, והגדרת בינה
מלאכותית בסקטור
הפיננסי



א. הגישה הכללית – עידוד חדשנות והתמודדות עם סיכונים

ככל שהתבהרו יכולותיה של טכנולוגיית הבינה המלאכותית וקצב התפתחותה והשתכללותה המהיר, התגבר השיח בעולם באשר לפוטנציאל התרומה של הטכנולוגיה, לסיכונים הגלומים בה ולתגובה הרגולטורית ההולמת התפתחויות אלה. הגישה האסדרתית המתאימה ביחס לטכנולוגיה נגזרת בעיקר מזיהוי סיכונים פוטנציאליים הנובעים מהטכנולוגיה והערכת חומרתם ומנגד הערכת פוטנציאל התרומה של השימוש בטכנולוגיות אלה.

מבלי לגרוע מהחששות הרבים שהוצגו בעולם ביחס להשלכותיה של טכנולוגיית הבינה המלאכותית, הצוות סבור כי בהתייחס לפעילות של בינה מלאכותית בסקטור הפיננסי ישנם שיקולים בגינם יש מקום לעודד פעילות זו:

ראשית, התחום הפיננסי נמצא תחת פיקוח הדוק באופן יחסי, החולש על מגוון פעולות של הגופים המפוקחים, ועל כן ניתן לתת מענה לסיכונים העולים מפעילות של בינה מלאכותית במסגרת פעולות אסדרה ופיקוח. שנית, בראיית ההתפתחויות הטכנולוגיות והרגולטוריות בעולם, דומה כי שילובה של טכנולוגיית בינה מלאכותית באופן נרחב בתחום הפיננסי הוא עניין של זמן, או במילים אחרות השאלה היא מתי תשולב הטכנולוגיה ובאיזה אופן, ולא האם תשולב, ועל כן נדמה שניסיון להתעלם מטכנולוגיית הבינה המלאכותית (או לצמצם את השימוש בה) אינו הפתרון הנכון בנסיבות. שלישית, לטכנולוגיה של בינה מלאכותית יש פוטנציאל גדול לשפר את השירותים הפיננסיים לצרכן, להוזיל אותם, וכן להגביר את התחרות בתחום. לבינה מלאכותית גם עשויים להיות יישומים רבים בסקטור הפיננסי, ועל כן תוצריה עשויים להיות מועילים מאוד בשורה ארוכה של היבטים בפעילות המתקיימת כיום ובפעילויות עתידיות.

אין באמור כדי להתעלם משיח הסיכונים הכללי ביחס לבינה מלאכותית שגם אם אינו ייחודי לפעילות בסקטור הפיננסי דווקא, בוודאי עלול לחלחל ולהתממש בתחום זה. בנסיבות אלה, נראה כי יש מקום להתמודד עם כניסת הבינה המלאכותית לתחום הפיננסי ולהיערך לשינויים שהיא צפויה לחולל תוך עידוד היבטי חדשנות שיש בהם להיטיב עם הצרכן לצד אימוץ אחראי של הטכנולוגיה, קביעת "כללי משחק" נאותים וניהול הסיכונים הכרוכים בכך.

לאור האמור, הגישה שהנחתה את הצוות והתוותה את ההמלצות שבדוח דוגלת בעידוד פעילות בינה מלאכותית בסקטור הפיננסי, לצד קביעת רגולציה מותאמת מקום בו הדבר נדרש – בין לשם שילוב הטכנולוגיה ובין לשם התמודדות עם הסיכונים הכרוכים בפעילות זו. הסיכונים והאתגרים הגלומים בשילוב של בינה מלאכותית בפעילות פיננסית הם משמעותיים, אולם עמדת הצוות היא שמדובר בסיכונים שניתן להתמודד איתם.

תפישה זו מתיישבת עם הגישה הממשלתית הכוללת המתגבשת ביחס לבינה מלאכותית, והעקרונות המוצעים להלן משתלבים בה (להרחבה ראו מסמך המדיניות והדיון בפרק פעילות בינה מלאכותית בסקטור הפיננסי בישראל לעיל).

ב. עקרונות מנחים לטיפול בבינה מלאכותית בסקטור הפיננסי



1. אסדרה גמישה ואדפטיבית

אחד האתגרים בעיצוב אסדרה בתחום הטכנולוגיה בכלל והבינה המלאכותית בפרט הוא התקדמות הטכנולוגיה תוך כדי קביעת האסדרה ואחריה. דומה שהדברים נכונים ביתר שאת בתחום הבינה המלאכותית שמדי יום חושף עוד יכולות שיהיו רלוונטיות גם לתחום הפיננסי. זאת, במקביל לכך שאף היכולות הקיימות טרם שולבו או מוצו ממגוון סיבות. כאמור, זהו אתגר שמאפיין התפתחויות טכנולוגיות בכלל, שלגביהן הרגולטור נדרש לאזן בין שיקולים שונים כדי להחליט מהו העיתוי הנכון לקבוע אסדרה, ובראשם הרצון לא לחסום את הטכנולוגיה אל מול הצורך (והחובה) להגן על האינטרס הציבורי. אף שאין זה אתגר חדש, דומה כי בתחום הבינה המלאכותית מדובר באתגר משמעותי מהרגיל.

נוכח האמור, **גישת הצוות היא שיש לעשות שימוש, ככל הניתן, בכלי אסדרה גמישים שניתן לעדכןם עם התפתחות הטכנולוגיה**, ולא פחות חשוב מכך, לאחר שלרגולטור הייתה הזדמנות ללמוד את הטכנולוגיה, השפעתה על התחום שבפיקוחו, הנעשה בעולם וכדומה. כלים אלה יכולים לכלול הוראות מנהל, תקנות (בהוראת שעה), סטנדרטים וכדומה. יהיה מקום גם לנקוט באסדרה "רכה" המותירה שיקול דעת מסוים בידי הגוף המפוקח, כגון כלי רגולציה עצמית. בהקשר זה יש חשיבות גם לקשר עם הגופים הטכנולוגיים והגופים המפוקחים כדי ללמוד על מידת האימוץ של יישומי בינה מלאכותית והאמצעים הפנימיים שהם נוקטים ביחס לשילוב בינה מלאכותית בפעילותם וניהול הסיכונים הנובע מכך.

ייתכנו כמובן חריגים להמלצה זו. למשל, מקום בו האסדרה הקיימת בחקיקה יוצרת מגבלה או חסם שנכון להתמודד עמו באמצעות תיקון החקיקה עצמה. חריג נוסף יכול להיות קשור למקרה שבו יתגלה סיכון מיוחד או שלא ניתן לתת מענה לאינטרס הציבורי בפיתוח הפעילות או באסדרתה בלי תיקון חקיקה מתאים.

אם כן, עמדת הצוות כי בשלב זה יש לאמץ ארגז כלים רגולטורי שיכלול כלי אסדרה אדפטיביים ורכים וככלל אין מקום בשלב זה לאמץ כלים חקיקתיים נוקשים לצורך קביעת אסדרה בתחום הפיננסי.

2. התאמת האסדרה למקובל בעולם

לצד הרצון לשמור על עצמאות האסדרה בישראל, הצוות רואה חשיבות באימוץ אסדרה שמשתלבת עם הרגולציה המקובלת בשווקים מפותחים בעולם. ראשית, הפוטנציאל והסיכונים הגלומים בבינה מלאכותית אינם ייחודיים לישראל, ועל כן ניתן להיעזר בכללים או בסטנדרטים שיתפתחו בעולם בהקשר זה, ואפשר אף יהיה להישען על רגולציה זרה שתתפתח, כגון רגולציה על ספקי טכנולוגיה בינלאומיים או על מוצרים ושירותים פיננסיים מבוססי בינה מלאכותית. שנית, קביעת סטנדרטים ייחודיים בישראל עלולה לפגוע ביכולת של גופים פיננסיים לקלוט שירותים ומוצרים שלא יותאמו במיוחד לרגולציה הישראלית. כך למשל, דרישות שיצרכו היערכות טכנולוגית שלא תידרש ביחס לשווקים גדולים אחרים, עלולה להדיר ספקיות טכנולוגיה מלפעול בישראל ולהוביל לכך שלא ניתן יהיה לשלב את אותם מוצרים ושירותים והציבור הישראלי יצא נפסד מכך. לבסוף, "שחקנים" טכנולוגיים ופיננסיים הפועלים בישראל מכוונים את פעילותם גם לשווקים בינלאומיים. לגופים אלה יהיה קושי להתאים את מוצריהם גם לרגולציה ייחודית ישראלית וגם לרגולציה הנהוגה בשווקים אחרים והדבר עלול לפגוע בשחקנים אלה אך גם בגופים הפיננסיים שיתקשו לשלב מוצרים מתקדמים בפעילותם. גם מטעם זה, אם כן, יש לוודא שהרגולציה שתאומץ בישראל תתאם את הנעשה בעולם ולא תייצר חסמים מיותרים למעבר מוצרים ושירותים בין ישראל למדינות אחרות.

גם אם ישנן יוזמות וכיווני אסדרה מסתמנים בעולם, בשלב זה אין סטנדרט רגולטורי עולמי הנוגע לבינה מלאכותית בכלל, ולבינה מלאכותית בסקטור הפיננסי בפרט. לפיכך, ההמלצות בדוח כוללות מבט לעולם ושאפה לדמיון לאסדרה המתפתחת במדינות המפותחות, אך אינן מאמצות סטנדרט זר ספציפי.

3. עידוד חדשנות ושילוב הטכנולוגיה

אתגר נוסף שמלווה את העיסוק בנושא הוא חוסר בהירות מסוים באשר למידת שילובה של הטכנולוגיה במגזר הפיננסי בישראל. התרשמות הצוות ממפגשים שהתקיימו עם שחקנים בשוק וסקירות שערכו הגופים החברים בצוות הייתה כי אף שהטכנולוגיה מעוררת עניין רב בקרב גופים פיננסיים, שילובה בתוך גופים אלה נמצא בשלבים ראשוניים ובכל מקרה השילוב אינו אחיד בקרב הגופים והשימושים השונים. מהמפגשים עלה, כי הגופים הפיננסיים ה"מסורתיים" בוחנים אפשרויות לשילוב הטכנולוגיה בפעילותם אך הם אינם ממהרים לעשות כן או שהאימוץ נעשה בצעדים זהירים ומדודים. כמו כן, נראה כי יש בישראל פעילות טכנולוגית ענפה המיועדת לתחום הפיננסי, אך פניהן של החברות העוסקות בכך הם בעיקר לחו"ל. התרשמות הצוות היא כי אי-שילובה של הטכנולוגיה בקרב גופים פיננסיים מושפע גם מחוסר ודאות רגולטורית מסוים, אך נראה שהסיבה המרכזית לכך אינה נעוצה באסדרה, אלא בעיקר בתשומות הכרוכות בשינוי מערכות קיימות ובהיותה של הטכנולוגיה חדשה יחסית וההתפתחויות המהירות שלה המצריכות בניית "אמון". מצב דברים זה, אשר כפי הנראה אינו ייחודי לישראל, מאפשר היערכות מסודרת לקראת הטמעת הטכנולוגיה בגופים פיננסיים בישראל.

הצוות רואה חשיבות בהטמעת שימושי בינה מלאכותית היכן שיש לה פוטנציאל חיובי למשק ולצרכן. לכן מעבר לשאלות של היערכות להטמעתה של הטכנולוגיה, ההמלצות נוגעות גם לאופן שבו ניתן לעודד את כניסת הטכנולוגיה לפעילות הפיננסית בישראל ולקדם את התחרות בתחום (בין השאר, באמצעות הסרת חסמים, יצירת הזדמנויות, וידוא שאין מגבלות לא נחוצות המפריעות להתפתחות השוק או עלויות רגולטוריות עודפות וכדומה), וזאת מעבר להמלצות הנוגעות לאופן שבו יש לאסדר פעילות קיימת או צפויה.

4. התנסות ולמידה

בהמשך לאמור בפסקה הקודמת ביחס לאימוץ הטכנולוגיה באופן מדוד וזהיר, גישת הצוות היא לעודד שימוש בכלים רגולטוריים המאפשרים התנסות בשימוש בטכנולוגיה – בהיקפים מוגבלים – תוך יצירת ודאות רגולטורית (גם אם זמנית) לשחקנים הרלוונטיים. באופן הזה, גם הגוף הפיננסי אבל גם הרגולטור, יוכלו להכיר ולקבל נתונים אמיתיים על אופן תפקוד הטכנולוגיה באופן שיאפשר בהמשך קביעת אסדרה "חכמה" ומבוססת נתונים. לפני מספר שנים הוכנה הצעת חוק ל"התנסות רגולטורית" בסקטור הפיננסי (הצעת חוק הסנדבוקס), אולם נראה כי זו אינה מספיקה, ורצוי לשקול שינויים בה, כמו גם בכלים משפטיים ורגולטוריים נוספים לעידוד התנסות ולמידה, חלקם כבר קיימים במסגרת סמכויותיהם של הרגולטורים הפיננסיים (עמדות פרשניות, פניות מקדמיות וכדומה).⁹⁷ מתוך הניסיון שנצבר בגופים החברים בצוות עלה גם שהמלצות בתחום זה אינן צריכות להסתפק ביצירת סביבה רגולטורית שמאפשרת התנסות, אלא יש להתייחס גם למעטפת שניתנת לגופים שמבקשים להתנסות עם הטכנולוגיה, לרבות ליווי טכנולוגי ועסקי, מתן תמריצים עסקיים וכדומה. גישה זו עשויה גם לסייע בכניסתם לשוק של שחקנים קטנים

97 להרחבה ראו חלק ה' – פעולות נוספות לקידום רגולציה פיננסית בתחום הבינה המלאכותית להלן.

ובינוניים שנזקקים לסיוע או להקלות כדי להתמודד בסביבה העסקית והפיננסית בישראל.

5. נסיבות המצדיקות שינויים אסדרתיים

שאלה משמעותית שהתעוררה בדיוני הצוות ובמפגשים שנערכו עם השוק הפרטי וחוקרים בתחום נגעה לצורך בבחינת האסדרה או הכללים הקיימים אך בשל שילובה של הבינה המלאכותית בפעילות קיימת. זאת, בפרט אם כבר עתה נעשה שימוש בכלים סטטיסטיים או אוטומטיים מסוימים. במילים אחרות – האם אותה פעילות צריכה להיות מוסדרת באופן שונה רק משום שהיא מבוצעת בעזרת או באמצעות בינה מלאכותית. **גישת הצוות בהקשר זה היא שיש לבחון את השלכות השימוש בבינה מלאכותית על השירות והצרכן, ובהתאם לכך לקבוע האם אכן נדרש שינוי באסדרה הקיימת.** כלומר, אין אנו מניחים שעצם השימוש בבינה מלאכותית במסגרת מתן שירותים פיננסיים מחייב שינוי אסדרתי. כך לדוגמה, מקום בו הדין הקיים אינו כולל חובת הנמקה, יש לבחון האם יש לייצר חובת הסברתיות כלפי הלקוח וזאת אך בשל המעבר לשימוש בכלי בינה מלאכותית.

6. גישה מבוססת סיכונים

בדומה למסמך המדיניות, ובדומה למדיניות הנוהגת כיום בקרב רגולטורים פיננסיים, **המלצות הצוות אף הן נוקטות בגישה של אסדרה מבוססת סיכון.** כלומר, הצורך בשינוי הרגולציה והיקפה תלוי בסיכון הכרוך בפעילות או בשירות הספציפי הרלוונטי, תוך שקילת הכלים הקיימים להתמודדות עם הסיכון והשפעת הבינה המלאכותית על הסיכון. ברי, כי במסגרת זו נדרש לבחון את הסיכון הספציפי ביחס לכל מוסד פיננסי ולכל סוג פעילות פיננסית וכן לשקול את הסיכון אל מול התועלת הפוטנציאלית הנובעת מהטעמת הטכנולוגיה. לעניין זה, ראו פרק ראייה כוללת ומבוססת סיכונים להלן.

7. התחשבות בשיקולים צרכניים וחברתיים

מעבר לסיכונים למוסדות הפיננסיים, **בינה מלאכותית עלולה להדגיש או לייצר סיכונים צרכניים וחברתיים.** בדומה לגישות המתהוות במסמכי אסדרה בעולם, הבוחנים את סיכוני הבינה המלאכותית ביחס לאזרחים וכוללים בתוך כך סיכונים צרכניים וחברתיים, יש מקום לעשות כן גם בישראל. כך, למשל, ב-EU AI Act, תחום האשראי הצרכני מוגדר כתחום בסיכון גבוה לנוכח השלכותיו על יכולתו של הפרט להתקדם כלכלית. סיכונים נוספים עלולים לנבוע משימוש בטכניקות למידת מכונה לומדות, המקשות על הבנת תוצרי המערכת ולבחון היבטי אפליה.

8. אחידות

הדוח והמלצותיו מקיפים מגוון של שירותים פיננסיים ומתייחסים לגופים פיננסיים שונים – חלקם מעוררים שאלות דומות אף אם השירות אינו דומה (למשל, חשיבות שירות הלקוחות לצרכן) וחלקם מעוררים שאלות דומות בשל דמיון מסוים בין השירותים הפיננסיים (למשל, בתחום הייעוץ). **גישתו הכללית של הצוות היא שיש לחתור לאחידות אסדרתית ביחס לשירותים וסיכונים דומים,** גם אם ייתכנו הבדלים מסוימים הנובעים מהמוצרים הפיננסיים המאוסדרים. הרגולציה על פעילות פיננסית מסוימת צריכה להיגזר ממאפייניה של אותה הפעילות והסיכונים הגלומים בה ולא צריכה להיות מושפעת מזהות הגוף המאסדר את אותה הפעילות. במילים אחרות, **פעילויות דומות וסיכונים דומים צריכים לקבל טיפול אסדרתי דומה כדי למנוע ארביטראז' רגולטורי. לכן יש חשיבות גם בפיתוח שפה רגולטורית אחידה,** למשל, לצורך הגדרת הסיכון הנובע מהטכנולוגיה או לצורך קביעת המענה הרגולטורי.

בנוסף, הנחת העבודה של הצוות היא שהטכנולוגיה תמשיך עוד להתפתח ולייצר הזדמנויות ואתגרים שיצריכו המשך הסתכלות רוחבית על התחום, ולכן יש חשיבות בהמשך השיח והתיאום שהחל בעבודת הצוות.

9. ניטרליות טכנולוגית

הצוות מכיר בכך ששירותים פיננסיים שנבחנו במסגרת עבודת הצוות יכולים להתבצע באמצעים שונים – באמצעות טכנולוגיה חדשנית, באופן מסורתי, באמצעות מודלים שונים של בינה מלאכותית וכדומה. **אופן ביצוע השירות הפיננסי או הבחירה בטכנולוגיה זו או אחרת אינם אמורים להכתיב בכל מקרה אסדרה שונה, אלא יש לבחון את השלכות הטכנולוגיה על השירות הפיננסי ולתת מענה להזדמנות או לאתגר הנובעים ממנה.** כך, למשל, פעילות של ניהול תיקים מסורתי כרוכה בסיכונים הכרוכים בהעברת כספי המשקיעים לידי גורם אחר המוסמך לקבל החלטות השקעה בהן לפי שיקול דעתו. כאשר הפעילות נעשית תוך שימוש בבינה מלאכותית, נותרת המסגרת הכללית שהייתה רלוונטית גם לפעילות של ניהול תיקים מסורתי, ובהתאם לעיקרון הניטרליות הטכנולוגית יש לזהות את השינויים הנובעים מהטכנולוגיה ולהתמודד עימם. באופן זה, האסדרה לא תקנה יתרון לטכנולוגיה מסוימת על פני אחרת אם אין הצדקה לכך ובכך תאפשר לשוק להתפתח ולמוצרים שונים להתחרות זה בזה במסגרת תנאים דומים.

ג. הגדרת בינה מלאכותית

עצם הגדרתה של בינה מלאכותית הוא סוגיה מורכבת. אפשר לראות בעולם קשת של ניסיונות להגדיר מהי בינה מלאכותית. ההבדלים בין ההגדרות השונות נובעים בין היתר מההקשר בו הוצעו ההגדרות ומהמועד בו הוצעו. כך למשל ניתן למצוא הגדרות תאורטיות יותר באופיין, המבקשות לעמוד על ההבדל העקרוני בין בינה אנושית ובין בינה מלאכותית, לצד הגדרות פרקטיות יותר, שנועדו לאפיין מהי בינה מלאכותית לצורך קביעת מדיניות או הדין שיחולו על מערכות בינה מלאכותית. הגדרות אלה נדרשות להיות מדויקות יותר מטבע הדברים. הבדלים בהגדרות נובעים כפי שצוין גם מהמועד בו הוצעו, ולנוכח התקדמות הטכנולוגיה והשימושים בה אפשר לראות לאחרונה הגדרות המתייחסות גם ספציפית לבינה מלאכותית מתקדמת יותר, מסוג בינה מלאכותית יוצרת (Generative AI), בינה מלאכותית כללית (Artificial General Intelligence) ומודלי בסיס. לעיתים ניתן לראות גם הגדרות נפרדות למערכות מסוגים שונים.

הגדרת בינה מלאכותית היא בעלת חשיבות בענייננו לא רק לשם תיאור התופעה בה אנו עוסקים בדוח זה, וניתוח הפוטנציאל, הסיכונים וההתמודדות הרגולטורית הקיימת והנדרשת, אלא גם משום שתכליתה של ההגדרה היא רגולטורית. ההגדרה שנבקש להציע לצרכי רגולציה פיננסית נועדה לסייע לרגולטורים בהיבטי אסדרה ופיקוח. כך למשל רגולטורים עשויים להסתייע בהגדרה המוצעת לשם קביעת הוראות המטילות חובות על גופים מפוקחים העושים שימוש בבינה מלאכותית. המשמעות היא כי חרף הקושי הגלום בהגדרת בינה מלאכותית, מדובר בהגדרה בעלת השלכות מעשיות, וככזו עליה להעניק בהירות וודאות משפטית מספקת באשר לתחולתה.

מהם הקשיים המרכזיים בקביעת הגדרה לבינה מלאכותית?

קושי ראשון הוא זיהוי הגדרה שתקיף טכנולוגיות קיימות ועתידיות. הגדרות לבינה מלאכותית מבקשות בדרך כלל להקיף טכנולוגיות שונות, קיימות ועתידיות. תכלית זו ברורה על רקע ההתקדמות הטכנולוגית, והגיוון שעשוי להיות בטכנולוגיות של בינה מלאכותית, אולם היא מקשה על קביעת הגדרה מדויקת. קושי זה הנו משמעותי כאשר תכלית ההגדרה היא רגולטורית.

קושי נוסף נעוץ בכך שבינה מלאכותית יכולה לשמש בהקשרים מגוונים מאוד. כפי שפורט בפתח הדברים, לבינה מלאכותית עשויים להיות שימושים רבים בכל תחומי החיים, וכך גם בתחום הפיננסי. בין היתר עשויה בינה מלאכותית למלא תפקיד בהיבטי ציות להוראות הדין, בשירות לקוחות, או בפעולות הליבה בתחומי הפיננסים כגון חיתום אשראי או ייעוץ השקעות ללקוחות. מערכות הבינה המלאכותית עשויות לשמש ככלי תומך החלטה או ככלי מקבל החלטה.

שני הקשיים האמורים משקפים מתח כללי ביחס להגדרת בינה מלאכותית לצרכי רגולציה פיננסית, בין השאיפה להשיג גמישות וניטרליות טכנולוגית (לסוגים שונים של בינה מלאכותית) על רקע האופי הדינמי של הטכנולוגיה והצורך לתת מענה רגולטורי לשינויים, ובין השאיפה להשיג ודאות משפטית לשם תחולה ברורה של הרגולציה והתאמה שלה לפעילות. מתח כללי נוסף הוא בין הגדרה רחבה מדי, העלולה להוביל לתחולת יתר של הרגולציה, ובין הגדרה מצומצמת מדי אשר עלולה להוביל לתחולת חסר שלה.

קושי שלישי בנוגע להגדרת בינה מלאכותית, אשר עלה גם בשיח שקיים הצוות עם גורמים מפוקחים, נוגע להבחנה בין שימושים מבוססי-מחשב סטנדרטיים ומתוחכמים. כך למשל אפשר לטעון, כי אפליקציות הנתפשות כיום כבסיסיות ושגרתיות, כגון תוכנת אקסל, מבצעות פעולות שבעבר נעשו באופן אנושי או מסייעות בקבלת החלטות על בסיס חישוב סטטיסטי, ועל כן הגדרת בינה מלאכותית צריכה להצטמצם לשימושים מבוססי-מחשב מתוחכמים, הכוללים רכיב של למידת מכונה. מאידך הגדרות בולטות לבינה מלאכותית בעולם אינן כוללות רכיב זה, והן מבקשות להקיף גם מערכות בינה מלאכותית שאינן כוללות למידת מכונה, מבלי לכלול כמובן אפליקציות בסיסיות ושגרתיות. יש להניח כי הדבר נובע מכך שגם מערכות שאינן כוללות רכיב של למידת מכונה עשויות להיות משמעותיות מאוד. נציין כבר עתה כי אכן יש שונות בהגדרות בינה מלאכותית בהקשר זה ונידרש לכך בהמשך.

קושי רביעי הנו בשאלה אם להישען על הגדרה בינלאומית לבינה מלאכותית. יש יתרון בבחירת הגדרה דומה להגדרה מקובלת בחו"ל, באופן שיקל על שימושים בטכנולוגיה הכפופה כבר לסטנדרטים שנקבעו בחו"ל. יחד עם זאת, בשלב זה אין הגדרה מוסכמת אחת לבינה מלאכותית, כל שכן אין הגדרה שכזו ביחס לתחום הפיננסיים.

ההתמודדות עם אתגרים אלה במסמכים רגולטוריים שונים אינה אחידה. לעיתים, כאמור, ניתן לראות מספר הגדרות

המשמשות באותו מסמך – לדוגמה הגדרה בסיסית של בינה מלאכותית והגדרה נוספת של בינה מלאכותית כללית (General Purpose AI). בדומה לכך, לצד ההגדרות יכולים להיות רכיבים נוספים, כמו מידת הסיכון של השימוש במערכת בינה מלאכותית, או מידת המהותיות של המערכת, אשר ישפיעו על תחולת הרגולציה ועל תכניה. קביעת מספר רבדים של הגדרות יכולה להיות שימושית, אך היא יוצרת שפע אפשרויות המגביר את המורכבות הקיימת גם כך.

דוגמאות להגדרות של בינה מלאכותית

עד כה לא נקבעה בישראל הגדרה מחייבת בדין לבינה מלאכותית. במסמך המדיניות מצוין כי לצורך הדוח "תחום הבינה המלאכותית הוא שם כולל להתפתחות בתחום טכנולוגיות המידע, התקשורת ומדעי הנתונים, המאפשרת קבלת החלטות, ייצור תחזיות, או ביצוע פעולות על ידי מחשב ברמת עצמאות גבוהה, באופן המדמה או מסוגל להחליף בינה אנושית". עוד מצוין שם כי קביעת הגדרה פורמאלית לבינה מלאכותית היא משימה שאינה פשוטה. בפרט מוזכר הקושי להציג הגדרה שכזו לצרכי רגולציה, באופן שמצד אחד יכלול את כלל מערכות המחשוב עליהן רצוי שהרגולציה תחול, ומצד שני יחריג מערכות פשוטות ויומיומיות שאינן מעוררות כל סיכון.⁹⁸

בין ההגדרות הרבות בעולם, נקודת מוצא טובה לדיון יכולה להיות הגדרת ה-OECD:⁹⁹

"AI system: An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

הגדרה נוספת בעלת חשיבות, שתהא גם בעלת תוקף מחייב, היא זו שנקבעה ב-EU AI Act:¹⁰⁰

"AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

בניגוד לגרסה מוקדמת יותר של ההגדרה, אשר כללה נספח ובו טכניקות וגישות של בינה מלאכותית, הגדרה זו כללית ודומה יותר (במכוון) להגדרת ה-OECD. בד בבד, ב-EU AI Act יש הגדרה נוספת ונפרדת לבינה מלאכותית של General purpose AI model.¹⁰¹ ההגדרה המקורית בהצעת החוק של האיחוד האירופאי נכתבה לפני פריצת הדרך של מודלי השפה, ועדכון זה נועד להתמודד עמה. לצד ההגדרה הנוספת נקבעו גם הוראות רגולטוריות נפרדות.

בדומה לכך מוגדרת בינה מלאכותית בצו הנשיאותי באופן הבא:¹⁰²

"The term 'artificial intelligence' or 'AI' has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine-

98 מסמך המדיניות, בעמ' 18.

99 OECD (2024), "Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, <https://doi.org/10.1787/623da898-en>

ב-OECD בשנת 2019.

100 EU AI Act, Article 3(1), ה"ש 11 לעיל.

101 'general-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development and prototyping activities before they are placed on the market. EU AI Act, Article 3(63).

102 הצו הנשיאותי. בצו הנשיאותי הופיעו הגדרות רלוונטיות נוספות כגון AI System, generative AI ו-machine learning, כך שהיו בו דוגמאות לשכבות של הגדרות העוסקות בבינה מלאכותית.

and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.”

הגדרות נוספות שכדאי לעיין בהן פורסמו בסינגפור ובקנדה.¹⁰³ המכנה המשותף לכל ההגדרות האמורות הוא הימנעות מהתייחסות לטכנולוגיה ספציפית; האפשרות כי מערכות הבינה המלאכותית יפעלו בדרגות שונות של אוטונומיה ואוטומטיות; והתייחסות לשימוש, יכולות ותוצרי מערכת מגוונים הנוגעים לתכנים כגון תחזיות, המלצות או החלטות ייצור תוכן. חשוב לציין כי מכיוון שהגדרות אלה הן כלליות ביחס לבינה מלאכותית, הן עשויות לחול גם בהקשרים פיננסיים שבהם עוסק דוח זה.

במישור של רגולציה פיננסית, אפשר לציין את התייחסות הבנק המרכזי באנגליה ורשות הפיקוח הפיננסית (FCA) באופן כללי למונח “בינה מלאכותית” כסימולציה של בינה אנושית בידי מכונות, לרבות השימוש במערכות מחשב המסוגלות לבצע משימות שמשקפות למידה, קבלת החלטות, פתרון בעיות, ומשימות נוספות שחייבו בעבר בינה אנושית. למידת מכונה מצוינת כקטגוריה אחת של בינה מלאכותית.¹⁰⁴ התייחסות כללית זו עוקפת את הצורך בניסוח מדויק של הגדרת בינה מלאכותית, אך אין היא משמשת עדיין להחלת רגולציה, אלא למסמך לדיון.

רשות ניירות הערך האמריקאית (SEC) הציעה הגדרה פורמאלית במסגרת כללים שפרסמה להערות הציבור בנוגע לניגודי עניינים פוטנציאליים של ברוקרים ויועצי השקעות. ההגדרה מכוונת להקיף גם פעילות של בינה מלאכותית:¹⁰⁵ “Covered Technology means an analytical, technological, or computational function, algorithm, model, correlation matrix, or similar method or process that optimizes for, predicts, guides, forecasts, or directs investment-related behaviors or outcomes.”

סוגיות עיקריות שבחן הצוות בנוגע להגדרה אפשרית של בינה מלאכותית:

(1) האם יש מקום להתייחס בהגדרה לטכנולוגיה מסוימת, או להזכיר במסגרתה מספר טכנולוגיות לדוגמה?

לנוכח קצב ההתקדמות בטכנולוגיות של בינה מלאכותית, רצוי לדעת הצוות שההגדרה תקיף טכנולוגיות וטכניקות שונות שעשויות להתפתח לאורך זמן. גישה זו ניכרת גם בהגדרות בעולם. כך למשל, ניתן לראות כי בהגדרה המקורית של האיחוד האירופאי נכלל המונח “software” ורשימת טכנולוגיות שהופיעה בנספח, בעוד שבהגדרה הנוכחית

103 ההגדרה שהוצעה במסמך מדיניות בסינגפור משנת 2020:

“AI refers to a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and, depending on the AI model, produce an output or decision (such as a prediction, recommendation, and/or classification). AI technologies rely on AI algorithms to generate models. The most appropriate model(s) is/are selected and deployed in a production system.”

Singapore Model Artificial Intelligence Governance Framework (2020), Sections 2.14–2.15 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>

וההגדרה בהצעת החוק הקנדית משנת 2022:

“artificial intelligence system means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a generic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions. (système d’intelligence artificielle)”

.Canada Bill C-27 (June 16, 2022), Part 3. <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>

104 ראו ה"ש 74 לעיל:

“What is AI?”

2.10 While there is no consensus on a single definition, it is generally accepted that AI is the simulation of human intelligence by machines, including the use of computer systems, which have the ability to perform tasks that demonstrate learning, decision-making, problem solving, and other tasks which previously required human intelligence. Machine learning is a sub-branch of AI. AI, a branch of computer science, is complex and evolving in terms of its precise definition. It is broadly seen as part of a spectrum of computational and mathematical methodologies that include innovative data analytics and data modelling techniques.

2.11 The Bank and FCA previously defined AI in non-legal terms as ‘the theory and development of computer systems able to perform tasks which previously required human intelligence’. The term AI system refers to the set of integrated computational elements and microservices that input, output, process, and store data and information. Therefore, one AI system may include multiple AI algorithms, models, and datasets.”

<https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence>

105 הצעה זו נמצאת עדיין בבחינה על-ידי ה-SEC. הצעת ה-SEC משנת 2023, ראו ה"ש 69 לעיל.

המונח המשמש הוא "machine based system" והנספח, אשר כלל טכניקות ספציפיות, נמחק.

על כן מוצע שלא להתייחס בהגדרה לטכנולוגיה מסוימת של בינה מלאכותית. במסמכי רגולציה כגון הוראות או חוזרים יש לרוב גם דברי הסבר בהם אפשר יהיה להרחיב לגבי טכנולוגיות וטכניקות שונות לשם המחשה.

בבחינת המינוחים האפשריים, נבחנו שאלות כגון האם רצוי לכלול בהגדרה מינוח של "מחשב" או "מכונה" (דבר שהנו מקובל ברוב ההגדרות, אם כי הגדרת ה- SEC שהוזכרה לעיל רחבה יותר וכוללת "מתודה או תהליך" – method or process); או האם רצוי להוסיף דוגמאות או מלל לשם המחשת המערכות עליהן תחול ההגדרה – כך למשל בהגדרות בעולם ניתן למצוא מינוחים כגון "אלגוריתם", "מודל", "למידת מכונה", לרוב לא כרכיב מחייב בהגדרה, אלא לשם המחשה.

יצוין, כי הואיל ועבודת הצוות לא כיוונה להכנת חקיקה בנושא, העיסוק במינוחים לא עלה כדי נסחות מדויקת, אלא נעשה בעיקר לשם זיהוי הרכיבים העיקריים הנחוצים בהגדרה, במטרה לסייע לרגולטורים ולגופים הפיננסיים שיידרשו לשאלה זו (עד שתהיה הגדרה סטנדרטית מקובלת בעולם, ככל שתהיה).

(2) האם יש מקום להתייחס למטרות השימוש או לתוצרי הפעולה של הבינה המלאכותית?

כאמור לעיל, מטרות השימוש במערכות בינה מלאכותית ותוצרי הפעולה שלהן יכולים להיות מגוונים – החל מכלי ניטור שנועדו לשימושים פנימיים בלבד כמו זיהוי חריגים במסגרת בדיקת ציות להוראות הלבנת הון או פעילויות, ועד מיכון פעולות אשר בעבר נעשו באופן ידני דוגמת פעילויות back-office או אדמיניסטרטיביות כמו סליקה, מכלים תומכי החלטה בפעילויות פיננסיות שונות ועד כלים המקבלים החלטות ופועלים באופן עצמאי מול לקוחות הגופים הפיננסיים.

סוגיה אחת שבחן הצוות היא האם רצוי להגביל את ההגדרה רק לשימושים הנוגעים לפעילות מול לקוחות. הואיל והסיכונים הגלומים במערכות בינה מלאכותית עשויים להיות גם בקשר עם מערכות פנימיות, לדעת הצוות אין מקום להגבלה כאמור, שכן יתכן שהאסדרה תבקש לטפל גם בסיכונים כאמור אם הם מהותיים לפעילות הגוף המפוקח. כלומר, גם אם הסיכונים אינם נוגעים ישירות ללקוחות אך נוגעים לגוף המפוקח.

סוגיה שניה שבחן הצוות היא האם יש מקום להתייחס במסגרת ההגדרה לתוצרי המערכת כגון ניבוי, המלצות, יצירת תוכן או קבלת החלטות עצמאית או ככלי מסייע (בדומה למשל להגדרת האיחוד האירופאי). בהינתן שהתייחסות כאמור מקובלת בהגדרות בעולם, משקפת את הטכנולוגיה גם באמצעות יכולות ותוצרים מרכזיים של מערכות בינה מלאכותית, ואינה ממצה, הצוות סבור כי רצוי לכלול אותה גם בהגדרה.

סוגיה שלישית שנבחנה היא האם רצוי להתייחס במסגרת ההגדרה באופן ספציפי יותר לעולמות הפיננסיים – למשל, לקבלת החלטות של גופים מפוקחים בעניינם של לקוחות או משקיעים. לדעת הצוות התייחסות כאמור רצויה לשם אפיון הפעילות בה עוסקות המלצות הצוות, כל עוד אין היא מגבילה אותה לפעילות מול לקוחות בלבד והיא אכן מהותית בראייה פיקוחית. יש להניח כי רגולטורים עשויים בעתיד להתייחס לשימושים ספציפיים אף יותר, כגון התייחסות למערכת בינה מלאכותית העוסקת בהחלטות אשראי.

(3) האם וכיצד ניתן להבחין בין מערכות בינה מלאכותית ובין מערכות ממוחשבות "רגילות"?

סוגיה זו ממחישה את המורכבות בנוגע להגדרת בינה מלאכותית, ויש לה חשיבות רבה בקביעת תחולת ההגדרה והרגולציה שתהיה מבוססת עליה. נראה כי בהגדרות מרכזיות בעולם, כפי שהובאו לעיל, ההתמודדות עם סוגיה זו היא כפולה: מן הצד האחד, באמצעות קביעה כי מדובר ב"מערכת מבוססת מכונה" (machine-based system), אשר מדגישה את ההתבססות על מערכת ממוחשבת ולא על פעולה אנושית, וכך מצמצמת את תחולת ההגדרה. מן הצד האחר, באמצעות קביעה כי המערכת יכולה להתאפיין ברמות שונות של אוטונומיה ואינה חייבת להיות בעלת מאפיין של למידת מכונה וכן באמצעות תיאור יכולותיה או תוצריה. קביעות אלה מרחיבות את תחולת ההגדרה.

בהעדר פתרונות אחרים, אנו מציעים להיצמד לרכיבים אלה הקיימים בהגדרות בחו"ל. ניתן להעריך כי ביחס למערכות בינה מלאכותית רבות לא תקום כלל שאלה באשר לתחולת ההגדרה, וכי ביחס למערכות אחרות יוכל להתקיים שיח בין הגורמים המפוקחים והרגולטורים באשר לתחולה, וכך לפתור בעיות פוטנציאליות של עמימות.

עוד מוצע, כי בהתאם להנחיות הרגולטור, גוף פיננסי יוכל להחליט כי מערכת מבוססת מחשב אינה מהווה, על פי מהותה, מערכת בינה מלאכותית. שיקול דעת זה יוכל לאפשר התמודדות עם מצבים בהם ניכר שהמערכת המדוברת אינה מערכת בינה מלאכותית, אף שההגדרה עשויה לחול עליה מבחינה פורמלית.

מענה מסוים לקשיים שהוצגו לעיל יכול להיות באמצעות קביעתן של מספר הגדרות באופן מודולרי. קביעה שכזו יכולה לסייע בהתאמת הרגולציה לפעילות של בינה מלאכותית. הצוות מוצא לפיכך יתרון בהצעה של

הגדרה בסיסית, ולצידה הגדרות נוספות, כגון אלה:

- **הגדרה שתכלול גם רכיב מהותיות**, ותחול לפיכך על מערכות בינה מלאכותית בעלות השלכות מהותיות על פעילות הגוף המפוקח (ביחס לגוף עצמו וביחס ללקוחותיו). על בסיס זה אפשר יהיה לדוגמה לקבוע כי הרגולציה, כולה או חלקה, תחול רק על מערכות מהותיות.
 - **הגדרה של מערכת בינה מלאכותית שמתאפיינת בלמידת מכונה**. ביחס למערכת מסוג זה עולות ביתר שאת שאלות של הסברתיות וניהול סיכונים, כך שעשוי להיות יתרון בהצגת הגדרה נפרדת ממנה תיגזר רגולציה ייעודית.
 - **הגדרה של מערכת בינה מלאכותית יוצרת או בינה מלאכותית כללית**. גם ביחס למערכת מסוג זה עשויות לעלות ביתר שאת שאלות, הנובעות ממאגרי המידע העצומים בהם נעשה שימוש, מהתוכן המגוון שניתן ליצור באמצעות מערכות אלה, או מהשימושים המגוונים שעשויים להיעשות במערכת.
- במסגרת הערות הציבור לדוח הביניים התקבלו התייחסויות הנוגעות למעשה לקשיים שהוצגו לעיל, ובפרט לחשש כי הגדרת בינה מלאכותית תהיה רחבה מדי ותכלול גם מערכות שיכולותיהן ותפקידיהן אינם מצדיקים טיפול רגולטורי מיוחד. בהקשר זה הוצע בין היתר לצמצם את ההגדרה או למקד אותה בסיכונים הנוגעים ללקוחות הגופים הפיננסיים. הצוות סבור כי חרף הקשיים האמורים, ובהעדר פתרונות "קלים" בסוגיית ההגדרה, יש ערך בנקיטת הגדרה דומה להגדרות המקובלות בעולם, כפי שפורטו לעיל. ביחס להיבט הסיכונים (אשר יכולים להיות גם בנוגע לגוף הפיננסי עצמו ולא רק בנוגע ללקוחותיו) סבור הצוות, כי ניתן מענה באמצעות רכיב המהותיות שהוצע להגדרה, וכן באמצעות גישה מבוססת סיכונים המתוארת בדוח זה. בד בבד, לנוכח הערות הציבור, נערך תיקון לפיו בהתאם להנחיות הרגולטור, גוף פיננסי יוכל להחליט כי מערכת מבוססת מחשב אינה מהווה, על פי מהותה, מערכת בינה מלאכותית. שיקול דעת זה יוכל לאפשר התמודדות עם מצבים בהם ניכר שהמערכת המדוברת אינה מערכת בינה מלאכותית, אף שההגדרה עשויה לחול עליה מבחינה פורמלית.



הגדרה מוצעת

להלן הגדרה בסיסית המוצעת על-ידי הצוות למערכת בינה מלאכותית בסקטור הפיננסי:

"מערכת בינה מלאכותית" – מערכת מבוססת מחשב, הפועלת בדרגות שונות של אוטונומיה, במטרה להפיק תוצרים כגון תוכן, תחזיות, המלצות או החלטות, אשר עשויה להיות לה השפעה על משקיעים, לקוחות, או על פעילותו של הגוף המפוקח.

התמקדות רגולטורית במערכות בינה מלאכותית מהותיות יכולה להיעשות על-ידי הוספת רכיב של מהותיות להגדרה:

"... אשר עשויה להיות לה השפעה מהותית על משקיעים, לקוחות, או על פעילותו של הגוף המפוקח".

כמו-כן, בהתאם להנחיות הרגולטור, גוף פיננסי יוכל להחליט כי מערכת מבוססת מחשב אינה מהווה, על פי מהותה, מערכת בינה מלאכותית.



חלק ג'

סוגיות רחב





אתגרים בבינה מלאכותית וכלי אסדרה

כפי שתואר בפרק המבוא, הגישה הכללית שהותוותה במסמך הממשלתי בנושא בינה מלאכותית היא של "חדשנות אחראית". גישה זו גם ליוותה את כתיבת דוח זה, ומשמעותה היא שכדי לעודד להפיק תועלות משימושי בינה מלאכותית במגזר הפיננסי (ובכלל) יש גם לתת מענה לאתגרים ששימושים אלה מעוררים. בפרקים הבאים נדון באתגרים המרכזיים הנובעים משילוב הבינה המלאכותית בתחום הפיננסי וכן בכלים שעומדים לרשות הרגולטור כדי להתמודד עם אתגרים אלה. על אף החלוקה שנעשתה בחלק זה לסוגיות שונות, נכון להסתכל עליהן בראייה כוללת, שכן השימוש בכלי אסדרתי מסוים עשוי להשליך על הצורך בכלים אסדרתיים אחרים.

בחלק זה יפורטו בהרחבה סוגיות רוחביות המתעוררות כתוצאה משימוש ביישומי בינה מלאכותית והמלצות הצוות בקשר עם אותן סוגיות. בין היתר נעסוק בחלק זה בסוגיות הנובעות ממאפיינים ייחודיים של בינה מלאכותית – כגון סוגיית "הקופסה השחורה" והסברתיות וסוגיית המעורבות האנושית; בסוגיות המעוררות שאלות ביחס לדין הכללי החל על גופים מפוקחים בתחום הפיננסי – בהיבטי אפליה ופרטיות; ובמישורים של ממשל בינה מלאכותית וניהול סיכונים במסגרתם נציג כלים להתמודדות משולבת עם כלל האתגרים האמורים. בהמשך לכך נדון בסוגיות הנוגעות לשוק בכללותו, קרי באתגרים המתעצמים לנוכח כניסתה של הבינה המלאכותית בהיבטי תחרות, יציבות פיננסית, וסיכוני הונאה, סייבר ודיסאינפורמציה. בנוגע לכל אחת מהסוגיות נציג את השאלות המתעוררות כתוצאה מכניסתה של בינה מלאכותית לתמונה, העיסוק בהן בחו"ל, חלופות אפשריות לטיפול, והמלצות.



“קופסה שחורה” והסברתיות

המונח “הסברתיות” מתייחס ליכולת לספק הסבר, היגיון או הצדקה לתוצר (פלט) אליו הגיעה מערכת הבינה המלאכותית. ההתמקדות בצורך “להסביר” את פעילותה ותוצריה של מערכת בינה מלאכותית נובעת מכך שמערכות אלה, במובן המתקדם, מאופיינות כ”קופסה שחורה”. משמעות הדברים היא, שבשל מורכבותן או היקף הנתונים שבבסיסן, והאופן שבו נערכים הקשרים בין הנתונים, לא ניתן להתחקות אחר האופן בו התקבלו תוצרי המערכת.

בשיח הרגולטורי אין הגדרה למונח הסברתיות והוא משמש לעיתים להביע רעיונות דומים אך שונים מבחינה טכנולוגית ורגולטורית. בין השאר, ניתן להבחין בין הסבר על אופן פעילות המערכת במנותק מהחלטה ספציפית שהתקבלה, קרי, הנתונים שעמדו לרשותה, האלגוריתמיקה שבבסיסה וכדומה, לבין הסבר בדיעבד ביחס להחלטה ספציפית שהתקבלה. כפי שיפורט, ישנו דיון נרחב בשאלת המשמעות הטכנית של הדרישה האסדרתית להסברתיות וכיצד הדרישה האסדרתית מתורגמת ברמה הטכנית. בהיעדר בהירות ביחס לדרישה האסדרתית – מפתחי מערכות עשויים לפרשה באופן שונה כך שהדין ייושם באופן שונה. בענייננו, ולשם הבהירות, בנייר זה נבחין בין **הסברתיות כללית**, המתייחסת למאפייני המערכת ואופן פעולתה (מסמכים בינלאומיים מתייחסים להיבטים אלה לעיתים כשקיפות) לבין **הסברתיות פרטנית** המתייחסת להסבר ביחס לאופן שבו התקבלה החלטה ספציפית.

כפי שיפורט להלן, ישנן הצדקות שונות לקביעה רגולטורית להסברתיות – כללית ופרטנית – שכן הסברתיות משרתת, בין השאר, אינטרסים רגולטוריים, צרכניים וחברתיים. עם זאת, דרישת הסברתיות עלולה להיתקל בקשיים הנובעים, בין השאר, ממידת בשלותה של הטכנולוגיה או מהחובה להגן על סודות מסחריים. לפיכך, בכל המלצה הנוגעת לדרישת הסברתיות יש להתחשב בשיקולים אלו ובהשפעתם על הגוף המפוקח, על ציבור הצרכנים (המשקיעים או הלקוחות בעולמות הפיננסיים), על הרגולטור וכן על החדשנות.

מאז פרסום דוח הביניים חלו מספר התפתחויות בתחום ההסברתיות. מודלים גדולים במיוחד מציעים מעין הסבר או רשימת מקורות עיקריים בתהליך קבלת ההחלטות שלהם, במטרה לספק למשתמשים יכולת להבין (אף אם לא באופן מלא) את התהליך שהתחולל במערכת בעת ייצור הפלט אותו קיבלו.¹⁰⁶ גם אם אין מדובר בהסברתיות פרטנית מלאה, יש בכך לסייע בהבנת תהליך קבלת ההחלטות של המודל.

דרישת ההסברתיות

כאמור לעיל, מערכות בינה מלאכותית מתקדמות עשויות להוות “קופסה שחורה” או להתאפיין בהיעדר שקיפות ועכירות (opacity). משמעות הדבר היא שיש קושי לגורם אנושי להבין את אופן פעילות המערכת ומדוע המערכת הגיעה להחלטה מסוימת. מצב דברים זה הוביל לעיסוק טכנולוגי נרחב באופן שבו ניתן לפתח מערכות הניתנות להסברה (explainable AI) וכן לעיסוק רגולטורי ביחס למאפייני מערכת שניתן להכניס לשימוש בתחומים מאוסדרים ואחרים, לרבות שילוב דרישות ברוח זה במסמכי אסדרה או בהצעות אסדרה של בינה מלאכותית בכלל ובתחום הפיננסי בפרט, כפי שיפורט להלן.

הסברתיות בבינה מלאכותית:

General Data Protection Regulation (להלן: “GDPR”) – רגולציית האיחוד האירופי העוסקת, בין היתר, בעיבוד אוטומטי של מידע אישי. רגולציה זו קובעת הגנות שונות במקרים בהם החלטות בעניינו של אדם מתקבלות בהתבסס על עיבוד מידע אוטומטי בלבד, הגנות אלה גוזרות בתורן חובות למפעילי המערכת.¹⁰⁷ בין השאר, קובעת הרגולציה, כי ביחס להחלטות מסוימות נדרש לספק לפרט “הסבר משמעותי ביחס להיגיון שמנחה את המערכת מקבלת ההחלטה”.¹⁰⁸ בנוסף, במקרים מסוימים נדרש ממפעילי המערכת להקפיד על כך שלפרט תעמוד האפשרות להתנגד או להשיג על ההחלטה בעניינו. סעיפים אלו עוררו דיון אקדמי בשאלה אם ה-GDPR קובע זכות להסבר ומה

shan Bilal, David Ebert, Beiyu Lin, LLMs for Explainable AI: A Comprehensive Survey (31 March 2025), at 106 <https://arxiv.org/html/2504.00125v1>

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <http://data.europa.eu/eli/reg/2016/679/oj>.

GDPR, Articles 13(2)(f), Article 14(2)(g), and Article 15(1)(h). 108



היקפה.¹⁰⁹ יש הטוענים כי משמעות הסעיפים היא שנדרש לספק הסבר לפרט ברמה כזו שתאפשר לו להתמודד עם ההחלטה אך לא לחשוף סודות מסחריים בדבר אופן פעולת המערכת ויש הטוענים כי נדרש לספק לפרט מידע על ההחלטה בעניינו בהתאם למגבלות הטכנולוגיות. כך או כך, נראה שה-GDPR מכיר בחשיבות הצורך לספק הסבר לפרט בדבר החלטה אוטומטית בעניינו.

EU AI Act – החקיקה האירופית עוסקת בחובת השקיפות של מערכות בינה מלאכותית בסיכון גבוה (כאשר תחת סיכון גבוה נכללות גם החלטות בנושאים פיננסיים כגון דירוג אשראי וביטוחי חיים ובריאות).¹¹⁰ לפי החובה בסעיף זה, על מפעיל המערכת (הגורם שמעמיד את המערכת לשימוש) להפעיל מערכות שעוצבו ותוכננו כך שיאפשרו למפעיל המערכת להבין את אופן פעולת המערכת, לרבות הבנה של יכולותיה ומגבלותיה (למשל, אם ישנם מצבים בהם נדרש פיקוח אנושי על פעולת המערכת). הסעיף גם מחייב שלמערכת יהיה מעין "מדריך הפעלה" שיכלול מידע על תפקוד המערכת ונסיבות שעשויות להשפיע עליה ולהגביר את הסיכונים ממנה, לרבות בשל פעולות של מפעיל המערכת. במילים אחרות, דרישת השקיפות צריכה להבטיח שמפעיל המערכת יוכל לעשות שימוש מושכל ובטוח במערכת וכן כזה שעומד בדרישות הרגולציה החלות עליו. לבסוף, למפעיל המערכת צריכה להיות דרך לפרש את תוצאות המערכת.¹¹¹ במונחים שהתוונו לעיל, החוק קובע בעיקר דרישת הסברתיות כללית (עם זאת, לצדו של חוק זה ישנו גם ה-GDPR שנזכר לעיל, אשר רומז גם לדרישת הסברתיות פרטנית במקרים מסוימים).

כמו-כן, החקיקה מתייחסת לכך שככל שמערכת בינה מלאכותית מעורבת בהחלטות מהסוג שתואר לעיל הרי שלפרט יש זכות לקבל הסבר על אופן מעורבותה של מערכת הבינה המלאכותית בקבלת ההחלטה.¹¹² בנוסף לכך ישנה דרישת שקיפות בדבר מערכות בינה מלאכותית שנועדו להיות באינטראקציה עם משתמש הקצה. נתייחס לחובה זו בפרק העוסק בידוע וגילוי להלן.¹¹³

הצורך בהסברתיות עומד גם במוקד של מסמכי אסדרה נוספים. ה-OECD מונה את עקרון השקיפות כאחד העקרונות המנחים לפיתוח מערכות בינה מלאכותית.¹¹⁴ הסעיף מצוין שהשקיפות נועדה לשרת כמה מטרות, לרבות מתן אפשרות לגורם המושפע מפעולת הבינה המלאכותית להבין את תוצריה. לצד זאת, מודגש כי יש ליישם עקרון זה בהתאם להקשר של פעילות מערכת הבינה המלאכותית וכן בהתאם להתפתחות הטכנולוגית.

הסברתיות בסקטור הפיננסי

גם במסמכי אסדרה הנוגעים לסקטור הפיננסי ישנה התייחסות לסוגיית ההסברתיות מקום שבו החלטה בעניינו של צרכן התקבלה באמצעות מערכת אוטומטית.

כך, הדירקטיבה האירופאית בתחום הסכמי אשראי הצרכני קובעת הוראות ספציפיות ביחס למצבים בהם החלטת ותמחור אשראי נעשית באמצעות מערכות אוטומטיות. הדירקטיבה כוללת חובת גילוי ביחס למעורבות בינה מלאכותית בקבלת ההחלטה וכן מקנה זכות לצרכן לבקש מהגוף הפיננסי שנותן אשראי הסבר ביחס לקביעות בעניינו. על הסבר זה לכלול מידע בדבר ההיגיון שמנחה את המערכת, ובפרט כיצד ההיגיון של המערכת יושם בעניינו של צרכן ספציפי (כלומר, הן חובת הסברתיות כללית והן חובת הסברתיות פרטנית).¹¹⁵

בארצות הברית, קיימת בחקיקה חובת הנמקה כללית ביחס להחלטות אשראי מסוימות, ובעיקר כאלה המרעות עם הלקוח, וזאת ככלי למניעת אפליה וכן לצורך הכוונת התנהגות.¹¹⁶ בשנת 2023, ובעקבות השימוש ההולך וגובר באלגוריתמים מתוחכמים בקבלת החלטות אשראי, פרסמה ה"רשות להגנת הצרכן בפיננסיים" חוזר שבמסגרתו הובהר שחובת ההנמקה חלה גם מקום בו החלטת האשראי התקבלה באמצעות שימוש באלגוריתמים. יתרה מכך,

109 ראו, בין השאר, Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a right to explanation of automated decision-making does not exist in the general data protection regulation." International data privacy law 7, no. 2 (2017): 76-99.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi

110 ראו ה"ש 11 לעיל. ה-EU AI Act נוקט במינוח "transparency" (שקיפות) ולכן נקטנו בו בתיאור לעיל.

111 יצוין כי סעיף שעסק מפורשות בצורך שתהיה יכולת לספק הסבר לפרט, נחקק בהליך החקיקה בפרלמנט.

112 EU AI Act, Article 86

113 EU AI Act, Article 50

114 OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

115 ראו, למשל, סעיף 56 לדירקטיבה – <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L2225>

116 U.S.C. 1691(d)(2); 12 CFR 1002.9(a)(2)(i) 15



הובהר כי על ההנמקה להיות ספציפית ביחס לנסיבות של הלקוח ואין למסור לו מידע כללי: ¹¹⁷

"A creditor will not be in compliance with the law by disclosing reasons that are overly broad, vague, or otherwise fail to inform the applicant of the specific and principal reason(s) for an adverse action."

חובת הסברתיות – דיון והמלצות

כעולה מן המפורט לעיל, ישנה הסכמה רחבה יחסית בדבר הצורך בהסברתיות, אך נראה כי הדרישה הרגולטורית להסברתיות משתנה בהיקפה, בהגדרתה, וכך ביחס לגורמים שכלפיהם יש למלא דרישה זו:

באשר להיקף החובה, ניתן להבחין בין חובה כללית (הדומה לחובת שקיפות באשר לאופן פעולת המערכת) לבין חובה פרטנית (הדומה יותר לחובת הנמקה). חובת ההסברתיות הכללית עניינה בעיקר במתן מידע מפורט על אופן פעולת מערכת בינה מלאכותית, ההיגיון שבבסיסה, הנתונים בה נעשים שימוש ואף השיקולים המשמשים בקבלת החלטות. מדובר איפוא בהסבר כללי שאינו נותן מידע מפורט בשאלת ההיגיון וההצדקה לפלט שהפיקה המערכת בעניין ספציפי אלא מתייחס בעיקר לאופן פעולת המערכת ותהליך קבלת ההחלטה. לעומת זאת, חובת הסברתיות פרטנית בדרך כלל מתמקדת בהסבר שניתן בדיעבד (ex-post) ביחס להחלטה ספציפית כאשר המידע אינו רק תהליכי אלא מספק את ההיגיון להחלטה המסוימת, ויש בו כדי להסביר מדוע זו ההחלטה.

באשר לגורמים שכלפיהם חלה החובה, הרי שזו יכולה להיות כלפי הגוף הפיננסי המפוקח שעושה שימוש במערכת, כלפי הרגולטור וכלפי הציבור. כלפי כל אחד מהגורמים הללו ישנה הצדקה שונה להחיל חובת הסבר ושקיפות. להלן תיאור ההצדקות ביחס לכל אחד מהגורמים:

הסברתיות כללית על אופן פעילות המערכת כלפי הציבור, תאפשר להעמיד את המערכת ואופן פעילותה לביקורת ציבורית. כלומר, ארגוני חברה אזרחית, אקדמיה וכדומה, יוכלו לבחון את מאפייני המערכת ולחוות דעתם ביחס לעמידתה בחובות שונות, האם היא מגלה הטיות, מקבלת החלטות שרירותיות וכדומה.	הציבור
מתייחס להיקף המידע שיש למסור לרגולטור. ההצדקה להחלת חובת הסברתיות כלפי הרגולטור היא לצרכי פיקוח, אכיפה ולמידה. כלומר, על מנת שהרגולטור יוכל להבטיח שהמערכת שבשימוש הגוף המפוקח אכן עומדת בחובות החוקיות והרגולטוריות וכן על מנת לתקף את עבודת המערכת. היקף חובת ההסברתיות ייגזר מהצדקות אלה. ככלל, מדובר בהסברתיות כללית.	הרגולטור
מתייחס למידת הידע שיש לגוף הפיננסי המפוקח על אופן פעולת המערכת והחלטותיה. חובת הסברתיות פנימית נובעת, בין השאר, מכך שנדרש שהגוף הפיננסי יאמץ לשימוש מערכת שנבדקה על ידו, שמתאימה לצרכיו ושהוא מפעיל אותה בהתאם ליכולותיה ומגבלותיה. דרישה כזו מאפשרת לגוף הפיננסי להפעיל בקרה על המערכת ולבדוק שהיא פועלת וממשיכה לפעול בהתאם לצרכיו ולחובות החלים עליו. זאת גם כאשר המערכת היא גורם מסייע בקבלת החלטות.	הגוף הפיננסי
מושא קבלת ההחלטה זקוק, ככלל, לחובת הסברתיות פרטנית. ללא הסבר פרטני, ללקוח אין דרך לבסס השגה כלפי ההחלטה בעניינו. קבלת הסבר מאפשרת לצרכן לשנות את התנהגותו באופן שישנה החלטות עתידיות בעניינו. כך למשל – אם הלקוח יידע שאיחור בתשלומי חשבונות חשמל השפיע על מחיר האשראי שקיבל, הוא יוכל לעשות שימוש במידע כדי לשנות את התנהגותו.	הצרכן

117 חוזר ה-CFPB משנת 2023, ראו ה"ש 71 לעיל.



לצד הצדקות אלה יש להביא בחשבון שיקולים נוספים:

מגבלות הטכנולוגיה: כאשר דנים בשאלה אם יש להחיל חובת הסברתיות ובמיוחד פרטנית, לעמדת הצוות, יש להתחשב גם במגבלות הטכנולוגיות. נכון לכתובת דוח זה, ישנן מערכות אלגוריתמיות שהן אכן קופסה שחורה ויש קושי להסביר מדוע הן הגיעו לתוצר מסוים. עם זאת, מערכות אלה עשויות להיות דווקא מדויקות יותר לנוכח גודל המודל או מורכבותו. במקרים אלה דרישת הסברתיות פרטנית משמעותה, הלכה למעשה, איסור שימוש במערכת – דבר אשר עלול להוביל לשימוש במערכות מדויקות פחות וכן להאט חדשנות, שכן לא ניתן יהיה לאמץ מערכות כאלה. כפי שיפורט, אחד האתגרים הרגולטוריים הוא להגדיר היטב את דרישת ההסברתיות לכל אחד מהגורמים המפורטים לעיל. למשל, האם די בהסברתיות כללית לגבי אופן פעילות המערכת; האם אפשר להסתפק במידע חלקי על אופן קבלת ההחלטה ביחס לפרט – לדוגמא, אילו רכיבים היוו גורם מרכזי בקבלת ההחלטה, להבדיל ממתן הסבר מדויק על ההחלטה שיכלול גם את המשקל שניתן לרכיבים אלה.

מהותיות הרכיב הטכנולוגי: יש להתחשב גם בתפקיד הטכנולוגיה במערך הכולל של הדברים. כך, למשל, במידה והטכנולוגיה היא כלי מסייע ובסופו של דבר יש אדם שמסוגל לנמק את החלטתו באופן ברור – ייתכן שלא נדרשת חובת הסברתיות מלאה.

מגבלות משפטיות וחזיונות: עוד יש להביא בחשבון שפעמים רבות הסברתיות של המערכת עלולה להיתקל בקשיים משום שדרישה זו עלולה להביא לחשיפת סודות מסחריים.

מהות ההחלטה: כאמור לעיל, באיחוד האירופאי, חובה זו חלה רק על החלטות של מערכת המוגדרות סיכון גבוה, ובארצות הברית חובת ההנמקה חלה בהקשרים פיננסיים מסוימים ביחס להחלטות המשנות לרעה את מצבו של הלקוח. כלומר, אם בקשת הלקוח התקבלה, למשל, ייתכן שאין צורך לחייב בחובת הסברתיות פרטנית.

הערות הציבור לפרק זה כללו התייחסות הן לתיאור סוגיית ההסברתיות הן להמלצות עצמן.

ההערות ביחס לסוגיה הכללית התייחסו בין השאר לכך שהאבחנה בין "הסברתיות כללית" ו"הסברתיות פרטנית" אינה חדה מספיק, וכן כי לא ברורה דיה העמדה ביחס לדרישה הרגולטורית. בשל הערות אלה נערכו שינויים בחלק הכללי שמטרתם להבהיר נקודות אלה.

בכל הנוגע להמלצות, היו שהעירו כי לא נדרשת הסברתיות בכל מצב ויש למקד דרישה זו בסוגי מערכות או סוגי החלטות (מערכות בסיכון גבוה, מערכות לצורך מניעת הונאות, וכדומה). הערה נוספת היתה כי יש לחדד את ההמלצה לפיה אין צורך בהסברתיות מקום בו הטכנולוגיה היא רק גורם מסייע. בין היתר הוער כי יש להבטיח שהגורם האנושי המלווה את עבודת המערכת מבין היטב את מאפייניה וחולשותיה. עוד הוער, כי החשיבות בדרישת ההסברתיות היא גם בתיקוף תוצאות המערכת ויש לתת לכך משקל גם בהמלצות. לבסוף, הוער כי ההתפתחויות בטכנולוגיה מאפשרות להבין היבטים מסוימים באופן קבלת ההחלטה של המערכת ויש לבחון אם אין בכך כדי לרכך את קשיי ההסברתיות המתוארים בפרק.

התרשמות הצוות היא שעיקר ההערות נוגעות להבהרות שונות שהתבקשו ולא לשורש ההמלצות. בהמשך להערות אכן נערכו מספר הבהרות. כך למשל, הובהר שלא נדרשת הסברתיות פרטנית ביחס לכל שימוש או החלטה, ויש לייחד דרישה זו להחלטות מהותיות. עוד יש לציין בהמשך להערות, כי לעתים קרובות קיימת מוטיבציה של הגוף המפוקח עצמו בהסברתיות, ועל רקע זה אפשר לראות התפתחויות טכנולוגיות שנועדו לשפר את רמת ההסברתיות במערכות בינה מלאכותית. ההמלצות כוללות עדכון גם לעניין זה, ביחס לאפשרות לספק הסברתיות פרטנית חלקית.



המלצות בנושא "קופסה שחורה" והסברתיות

בהמשך לשיקולים שהוצגו לעיל להלן המלצות ביחס להטלת חובת הסברתיות או שקיפות:

1. חובת הסברתיות פרטנית תידרש בהתאמה לדין הקיים:

אין לקבוע בכל מקרה חובת הסברתיות רק בשל העובדה שהגוף המפוקח עושה שימוש במערכת בינה מלאכותית. כלומר, יש לבחון האם כבר במצב המשפטי הקיים ישנה חובת הסבר (וכלפי מי) – אם ישנה חובה כזו, אז עצם כניסתה של מערכת בינה מלאכותית אינה אמורה לשנות חובה זו, ואף לא את היקפה בהכרח. כמו כן, ייתכן שיש מקום לבחון חיוניות של חובות הנמקה קיימות וחלופות במקומן בהנחה שאלה עשויות להוות חסם מפני שילוב בינה מלאכותית.

במידה שאין כיום חובה כזו בדין, יש לבחון האם סוג המערכת או טיב ההחלטה מחייבים החלת חובה חדשה (בהתאם לשיקולים שימנו להלן).

2. חובת הסברתיות כללית ופרטנית ביחס להחלטות מהותיות בסיכון גבוה:

דרישות הסברתיות שיחולו כלפי הרגולטור והצרכן צריכות להישקל ביחס למערכות בסיכון גבוה. יש לבחון את טיב ההחלטה ולהתמקד בהחלטות מהותיות וכאלה שמרעות עם הלקוח שכן ככלל אלה המקרים בהם לקוח יבקש להשיג על ההחלטה או ללמוד ממנה ולשם כך נדרש לו הסבר בדבר ההחלטה בעניינו. בהקשר זה יודגש, כי ככל שמערכת הבינה המלאכותית אינה מספקת רכיב מהותי בתהליך יצירת ההמלצה או ההחלטה, ועוסקת למשל בביצוע משימות רקע כמו סידור מידע, הרי שגם אז לא תידרש הסברתיות ביחס לאופן פעילותה (בדומה לחקיקת האיחוד האירופי).

3. חלופות "מפצות" להסברתיות פרטנית - יש לבחון האם ישנן חלופות להסברתיות שיתנו מענה הולם להצדקות שנמנו לעיל:

לדוגמה, ניתן לבחון האם די להעמיד דרישת הסברתיות כללית לצד גורמים מפצים אחרים להתמודדות עם הקושי של היעדר הסבר סדור, כגון מעורבות אנושית, בקרה הדוקה של תוצאות המערכת או בקרה תהליכית. כלים אלה עשויים להיות מספקים לעתים גם ביחס למערכות בסיכון גבוה.

הצבת חלופות שירות – מקום בו הרגולטור סבר שניתן לוותר על דרישת הסברתיות בשל חלופת שירות אנושית: כך שהצרכן יוכל לבחור אם לצרוך שירות מבוסס בינה מלאכותית או שירות אנושי, יש לוודא כי חלופה זו לא תהיה נחותה מהחלופה האלגוריתמית ותינתן בתנאים דומים, כדי לא לייצר העדפה עקיפה לשירות האלגוריתמי הנעדר יכולת הסבר פרטנית.

הסתפקות בהסברתיות פרטנית חלקית – כאמור יש התפתחויות טכנולוגיות בתחום הבינה המלאכותית המבקשות להשיג הסברתיות פרטנית, אף אם זו לא תהיה מלאה. כך למשל, עשויה להיות מערכת בינה מלאכותית שתספק הסבר בדבר המשקולות שנתנה לרכיבים שונים בתהליך קבלת ההחלטות – אך לא תסביר מדוע. אף להסבר חלקי זה עשויה להיות ערך במקרים רבים, למשל לבדיקת טעויות בנתונים או להבנת הנתונים הדומיננטיים שהובילו לתוצר. מכאן שהגופים המפוקחים והרגולטורים יוכלו לערוך התאמות ביכולות ההסברתיות הנדרשות בהתאם לנסיבות, ולהסתפק לעתים גם בהסברתיות פרטנית חלקית.

4. אין הכרח בחובת הסברתיות פרטנית מקום בו הטכנולוגיה היא רק גורם מסייע בקבלת החלטה

יש להבחין בין מצב שבו הטכנולוגיה היא גורם מסייע לקבלת ההחלטה לבין מצב בו הטכנולוגיה היא הגורם מקבל ההחלטה (גם אם היא מתווכת על ידי גורם אנושי). אם מערכת הבינה המלאכותית היא גורם מסייע ובסופו של דבר אדם מקבל את ההחלטה – ומסוגל לנמק אותה – נראה שיש להקל בדרישת ההסברתיות. מנגד, אם האדם רק "מתווך" את ההחלטה, יש להבטיח שהצרכן והרגולטור יקבלו הסבר מקיף מספיק להחלטה.



5. חובת הסברתיות פנימית (בתוך הגוף הפיננסי): נראה כי יש חשיבות שלגוף הפיננסי המפעיל מערכת בינה מלאכותית תהיה הבנה לגבי אופן פעילותה, מגבלותיה וכדומה באופן דומה לנדרש באיחוד האירופאי. הדברים אמורים בעיקר בחובת הסברתיות כללית, ויש לשקול חובת הסברתיות פרטנית לפי השיקולים שנמנו לעיל – לפי מידת הסיכון בהחלטות, חלופות מפצות להסברתיות, ומרכזיות הטכנולוגיה בקבלת ההחלטה.

6. חובת הסברתיות כללית כלפי הציבור: חובה זו עשויה לשרת צורך חברתי חשוב, אך יש לאזן אותה עם שיקולים אחרים כגון חשיפה של סודות מסחריים, שיקולי תחרות וכדומה. יש חשיבות לעודד חברות וגופים פיננסיים לחשוף היבטים מסוימים במערכות שהם מעמידים לגופים פיננסיים אך נראה כי יש קושי לחייבן לעשות כן.



מעורבות אנושית

אחד הפתרונות הרגולטורים הנפוצים המוצעים על מנת להתמודד עם הסיכונים האתגרים הגלומים בפעילות של בינה מלאכותית הוא מעורבות ופיקוח אנושי על קבלת החלטות אלגוריתמיות (שיכולנו לצורך דוח זה כמעורבות אנושית).

דרישת המעורבות האנושית נתפסת ככלי אסדרתי יעיל שנועד להתמודד עם תקלות וכשלים אפשריים של מערכת אלגוריתמית. המעורבות האנושית נועדה להוות כלי שמאזן בין הרצון לשלב מערכות בינה מלאכותית בתחומים שונים לבין החששות שמערכות אלה עדיין אינן בשלות מספיק כדי להתגבר על כשלים שונים שעלולים לפגוע או לסכן את הפרט או החברה.

הצדקה מרכזית אם כן לדרישת המעורבות האנושית היא שהאדם נתפס כמונע יעיל של כשלי מערכת אלגוריתמית, לפחות בשלב הנוכחי בו עדיין יש ספק לגבי יכולותיה לקבל החלטות מדויקות, שעומדות בכללי הדיון וכדומה. התקלות והכשלים הנדונים בהקשר זה יכולים להיות קשורים בתוצאות מוטות של המערכת, הפצת מידע שגוי, תוצאות שגויות של המערכת בשל תקלות תפקודיות וכדומה. ככל שלהחלטה השלכות משמעותיות על הפרט, כך גוברת חשיבות דרישת המעורבות והפיקוח האנושי.

הצדקה נוספת הנשמעת בהקשר של דרישת הפיקוח האנושי היא החשש מפני אובדן האוטונומיה של הפרט, אשר מבסס במקרים מסוימים חובה לערב גורם אנושי בתהליך, בין השאר לנוכח הקושי להסביר את החלטות המערכות הללו במקרים מסוימים והחשש שמצב זה יפגע ביכולתו של הפרט להבין את ההחלטה בעניינו, וכי החלטה של גורם שאינו אנושי בעניינו עלולה להוביל לתחושת אובדן שליטה של הפרט בגורלו. מעורבות אנושית – בין בקבלת ההחלטה עצמה ובין באמצעות בקרה אנושית – עשויה לתת מענה מסוים לחששות אלה. בהקשר זה מוצגת גם הצדקה לפיה יש ערך בכך שבעניינו של הפרט יופעל גם שיקול דעת אנושי שמסוגל להכיל מורכבות שמודל אלגוריתמי אינו מסוגל לשקלל.

לבסוף, ישנה גם הצדקה חוקית לדרישת המעורבות האנושית. מערכות אלגוריתמיות מעורבות בקבלת החלטות גם בתחומים שבהם נדרש רשיון מקצועי, כגון ייעוץ השקעות, ייעוץ פנסיוני, עריכת דין וכדומה. היעדר מעורבות אנושית בקבלת החלטות בתחומים אלה עלול להיתפס כהפרה של הדיון ודרישת הרשיון. להצדקה זו יש פן פורמלי אך גם פן מהותי. המצדדים בה טוענים כי בבסיס הדרישה לרישיון עומדות תכליות כגון הבטחת חובת נאמנות של בעל המקצוע כלפי הפרט או הבטחת כשירות מסוימת ולכן יש לשמר את מעורבותם של בעלי רישיון אלה.

לצד הצדקות אלה ישנה גם ביקורת על הדרישה הזו, או לכל הפחות, על הדרישה להחילה באופן גורף.

ביקורת מרכזית כלפי דרישה זו נוגעת לכך שאין ודאות שמעורבות אנושית אכן משפרת את תוצאות המערכת. אחת הסיבות לכך היא נטיית בני האדם שלא לסטות מהמלצות המערכת, כך שאם אכן יש כשל במערכת אין הכרח שהמעורבות האנושית היא זו שתפתור את הכשל. בנוסף, אם הדרישות הרגולטוריות מתמקדות בהחלטות אוטומטיות לחלוטין, הרי שניתן לעקוף אותן באמצעות מעורבות אנושית מצומצמת שאינה מגשימה באמת את התכליות שתוארו לעיל.¹¹⁸ ביקורת מסוג זה גורסת שבבסיס הדרישה מובלעת הנחה ששיקול הדעת האנושי עדיף על זה האלגוריתמי, אף שגם בני אדם מפלים, מוטים, טועים וכדומה. בהקשר זה, המבקרים טוענים כי ראוי שהרגולטור יתמקד בקביעת אמות מידה למניעת הטיות בהחלטות אלגוריתמיות מאשר להעביר את שיקול הדעת לגורם אנושי, שכאמור, עשוי להסתמך על המלצת המערכת או להפלות בעצמו.¹¹⁹

ביקורת נוספת נוגעת לאי ודאות לגבי חלוקת האחריות בין האדם לבין מערכת קבלת ההחלטות. דרישת מעורבות אנושית בלי כללים מוגדרים עלולה לטשטש את קווי האחריות בין הגורם האנושי לבין האלגוריתם. כך למשל, האם אדם ייטה להתערב בהחלטות המערכת גם כשלא ברור אם אירע כשל רק כדי להימנע מנשיאה באחריות? לחלופין האם אדם יימנע מהתערבות בשל חוסר הבנה של המערכת או מחשש לשאת באחריות?

לבסוף ישנה טענה כי דרישה זו מבטלת או מצמצמת את היתרונות שבשילוב מערכות אוטומטיות בארגון. ארגונים משקיעים במערכות אלה כדי ליעל את עבודת הארגון ולהתגבר על חסרונות "אנושיים" כגון מגבלות שעות עבודה,

Green, Ben, The Flaws of Policies Requiring Human Oversight of Government Algorithms (April 26, 2022). Computer Law & Security Review, Volume 45, 2022, <https://ssrn.com/abstract=3921216>.

<https://www.ecgi.global/blog/regulating-%E2%80%99Chumans-loop%E2%80%99D>



שיקול דעת לקוי, ובעיקר כדי לעשות שימוש ביכולות המחשוב המוגברות של מערכות שאמורות להוביל להחלטות מדויקות יותר עבור הארגון. הותרת הגורם האנושי בתמונה עלולה לצמצם יתרונות אלה.

דרישת המעורבות והפיקוח האנושי יכולה לחול לגבי שלבים שונים במחזור חיי האלגוריתם:



שלושת השלבים הראשונים המוצגים בתרשים עוסקים בתהליך ובתנאים לשילוב מערכת בינה מלאכותית: עצם קבלת ההחלטה לעשות שימוש במערכת כזו בפעילות של המוסד הפיננסי, התאמת המערכת או עיצובה לצרכי הגוף הפיננסי, ולבסוף הצורך בגיבוי אנושי במקרה של כשל טכני של המערכת. שלבים אלה לא יידונו בחלק זה אלא בפרקים שיעסקו בראייה כוללת ומבוססת סיכונים ובממשל בינה מלאכותית שכן המיקוד לגביהם הוא בפן התהליכי. בחלק זה נתמקד במעורבות האנושית בתהליך קבלת ההחלטות של המערכת, שם בדרך כלל דרישת המעורבות האנושית נועדה למטרות פיקוח על תפקוד המערכת – מבחינת תוכן ההחלטות או המידע שהיא מספקת והתאימות לדרישות רגולטוריות ומשפטיות שחלות על הגוף הפיננסי.



דרישת המעורבות האנושית במסמכי אסדרה בעולם

הדרישה למעורבות אנושית חוזרת על עצמה, בהיקפים שונים, במסמכי אסדרה בולטים בתחום.

- ה-EU AI Act קובע כמה חובות בהקשרי המעורבות והפיקוח האנושי, בעיקר עבור מערכות בסיכון גבוה, הכוללות מערכות שנועדו לקבל החלטות פיננסיות מסוימות.¹²⁰ החקיקה קובעת כי יש לפתח ולעצב **מערכות בסיכון גבוה, באופן שיאפשר לגורם אנושי לפקח על פעולתן בזמן אמת**, זאת על מנת למזער, ככל הניתן, את הסיכונים האפשריים הנובעים מהמערכת, לרבות סיכונים שלא נובעים מהשימוש "המתוכנן" של המערכת אלא מחבלה או תקלה. עוד נקבע בחקיקה האירופית, כי יש להתאים את רמת הפיקוח האנושי למידת הסיכון של המערכת, מידת האוטונומיה וההקשר שבו נעשה בה שימוש. החקיקה ממשיכה וקובעת שורת תנאים שיש לקיים כדי לעמוד בתנאי הסעיף, ובין השאר: (1) על הגורם האנושי להיות מסוגל לזהות אנומליות ותקלות בתפקוד המערכת; (2) מודעות של הגורם האנושי בדבר הנטייה להסתמך על המערכת; (3) יכולת לפרש את החלטות המערכת; (4) לאפשר לאדם את היכולת הטכנית לעקוף או להתעלם מהחלטת המערכת; (5) להתערב בפעילות המערכת ולהפסיק את עבודתה. החקיקה גם מתייחסת לדרישות ולכישורים הנדרשים מהגורם האנושי המפקח.¹²¹
 - **GDPR** – מעניקה לפרט זכות לדרוש שלא תתקבל בעניינו החלטה המבוססת על מערכת אוטומטית בלבד וזאת ביחס להחלטות שהן בעלות השלכות משפטיות משמעותיות ואחרות על הפרט (בכפוף לחריגים).¹²² בהמשך להוראות אלה, באירופה גם הדירקטיבה בענייני הסכמי אשראי צרכני חוזרת על החובה לאפשר התערבות אנושית בהחלטות אשראי לבקשת הצרכן.¹²³
 - **בקנדה** הצעת החקיקה לאסדרת בינה מלאכותית קובעת חובה לערוך הערכת סיכונים למערכות וביחס למערכות עם השלכות משמעותיות על הפרט (high-impact) ישנה חובת פיקוח אנושי וניטור של המערכת. בדומה לאיחוד האירופאי, הדרישה היא שפיתוח ועיצוב המערכת יאפשרו לגורמים אנושיים לפקח על פעילותה, לרבות היכולת לפרש את פעילותה. בנוסף, ישנה חובה לאפשר לעקוב אחר פעילות המערכת, ותוצאות פעילותה.¹²⁴
 - **בארצות הברית** הצו הנשיאותי (שבוטל בינתיים) התייחס למקרים בהם נדרשת מעורבות אנושית. בין השאר, הצו הנשיאותי קבע כי במקרים מסוימים, כגון שילוב מערכות בינה מלאכותית בהחלטות ממשלתיות שמשפיעות על זכויות מסוימות, יש לאפשר בחינה של ההחלטה בידי גורם אנושי לבקשת הפרט. עוד הורה הצו לרשויות לקבוע את המקרים שבהם יש לאפשר לפרט לקבל שירות ותמיכה מגורם אנושי.¹²⁵
- ההתייחסות למעורבות אנושית באה לידי ביטוי גם במסמכי מדיניות בתחום הפיננסי. במסמך המדיניות של הבנק המרכזי של **אנגליה** נדונה החשיבות של המעורבות האנושית הן בשלבי הפיתוח והן בשלבי הפעלת המערכת. ביחס לשלב הפעלת המערכת הדוח מתייחס לכך שמעורבות אנושית היא אמצעי יעיל להתמודד עם תוצאות בעייתיות של המערכת שכן לגורם האנושי יש ידע רלוונטי שלא בהכרח יבוא לידי ביטוי במודל קבלת ההחלטות (כגון, הקשר קבלת ההחלטה, הבנת הטיות מובנות במידע וכו'). כמו כן, גורם אנושי יכול לזהות דפוס או החלטות ספציפיות בעייתיות ולהעביר אותן לבחינה מחדש.¹²⁶
- בנייר התייעצות של ה-CFPB בעניין הערכת נכסים לצורך מתן משכנתאות והערכת בטוחות, נדונו מגבלות המודלים האוטומטיים לביצוע משימה כזו לעומת מעריך אנושי ולכן מוצע שם פיקוח אנושי על תוצאות המודל.¹²⁷ בנוסף, בנייר מדיניות אחר בעניין שימוש בצ'אט-בוטים במגזר הפיננסי, נדונו חסרונות הכלי האוטומטי לעומת שירות לקוחות אנושי וגם שם מוצע לשקול לאפשר מעבר לנותן שירות אנושי במקרים מסוימים.¹²⁸
- בדוח ה-OECD משנת 2023, אחד מכלי המדיניות המוצעים כדי להגביר את השליטה והאחריותיות כלפי מערכות בינה מלאכותית הוא פיקוח אנושי לאורך מחזור חיי המערכת. הדגש בדוח הוא שהפיקוח האנושי לא ייפסק בשלב פיתוח ועיצוב המערכת וימשיך גם לשלב הפעלת המערכת, בין השאר, באמצעות פיקוח על תוצאות ו"התנהגות"

120 EU AI Act, Article 14.

121 שם.

122 GDPR, Article 22.

123 ראו לעיל ה"ש 98.

124 <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>

125 ראו ה"ש 25.

126 ראו ה"ש 74.

127 <https://www.consumerfinance.gov/rules-policy/rules-under-development/quality-control-standards-for-automated-valuation-models/>

128 ראו ה"ש 45.

המודל בזמן אמת.¹²⁹

לבסוף, יצוין כי בדוח ESMA משנת 2023 עלה כי מרבית החברות העוסקות בתחום הביעו עמדה כי בשלב זה השימוש היעיל ביותר במערכות אלגוריתמיות יושג באמצעות שילוב של החלטה אלגוריתמית והחלטה אנושית.¹³⁰

במסגרת הערות הציבור לדוח הביניים היו מעירים שטענו כי מעורבות אנושית אינה עדיפה על בינה מלאכותית, ועל כן דרישה למעורבות אנושית לא בהכרח תיטיב עם הלקוחות והיא אף צפויה לפגוע ביעילות מערכת הבינה המלאכותית. מנגד, היו מעירים שלא טענו לבעייתיות בעצם קיומה של דרישה למעורבות אנושית, אך סברו כי ההמלצות בהקשר זה צריכות להיות קונקרטיות יותר, ולהציג קריטריונים למקרים בהם תידרש מעורבות אנושית לצד קריטריונים למקרים בהם לא תידרש מעורבות אנושית. באופן ספציפי נטען כי ההמלצה לפיה מעורבות אנושית נחוצה יותר ביחס להחלטות "שליליות" ללקוח אינה נכונה שכן גם החלטות "חיוביות" לכאורה (למשל, החלטה לאשר בקשה להלוואה) עלולות לפגוע בלקוחות, וממילא בעל רישיון נדרש לבחון גם החלטות חיוביות. הערה נוספת היתה כי לא בהכרח ניתן יהיה לדרוש מהגוף הפיננסי מעורבות אנושית, שכן זו תהיה תלויה בהסכם המסחרי בינו ובין מפתח המערכת.

אמות המידה בשאלה מתי מעורבות אנושית תידרש הן אכן תלויות נסיבות. הקו המוצג בדוח זה הוא הצבת דרישות רגולטוריות, ובהן דרישת מעורבות אנושית, כאשר מדובר בפעילות בסיכון גבוה ואין אמצעים אחרים הננקטים להפחיתו. כך למשל, יש להתחשב בהשפעה הפוטנציאלית של פעילות המערכת על הלקוח או על הגוף הפיננסי, האם תוצרי המערכת הם החלטות או נוגעים יותר למסירת מידע וקיום תקשורת עם הפרט, וכדומה. הבהרות בעניין זה נעשו בהמלצות הפרק. בין היתר התקבלה ההערה לפיה גם החלטות "חיוביות" לכאורה עלולות לפגוע בלקוחות, ועל כן הדגש הוא על מהותיות ההחלטה עבור הלקוח והסיכון לפגיעה בו. עוד בהתייחס להערות הציבור, הובהר בדוח הקשר בין דרישת מעורבות אנושית ודרישת בקרה אנושית: בקרה אנושית על פעילות המערכת ותוצאותיה היא כלי מתבקש ונדרש, אך אין הוא מהווה מענה בכל מקרה לדרישה למעורבות אנושית. הערה שלא התקבלה היתה כי מעורבות אנושית אינה תלויה בגוף הפיננסי אלא במפתח המערכת, שכן האחריות על הכנסת המערכת ותוצריה מוטלת בסופו של יום על הגוף הפיננסי (ראו גם בפרק העוסק באחריות).

סוגיה נוספת שעלתה במסגרת הערות הציבור היא קריאה לחייב גופים פיננסיים להעמיד חלופת פעילות עם מעורבות אנושית לצד מערכות בינה מלאכותית. לפי גישה זו, גוף פיננסי העוסק למשל במתן אשראי ללקוחות, יהיה חייב להעמיד מערך אשראי אנושי לצד מערכות בינה מלאכותית שיקבלו החלטות אשראי. הצוות סבור כי אין מקום לקבוע דרישה רוחבית שכזו, שכן היא תלויה בשאלות כגון מידת חיוניות השירות, קשיים שעשויים להיות בקבלת השירות ממערכות בינה מלאכותית (בדומה לקשיים שיש לאוכלוסיות מסוימות בקבלת שירותים דיגיטליים ולא פיזיים), והאפשרות לקבלו מגופים פיננסיים אחרים. לשם המחשה, עשוי להיות גוף פיננסי שיבקש לעסוק בניהול תיקי השקעות רק באמצעות מערכת בינה מלאכותית, ואף למצב את עצמו תחרותית כגוף הפועל כך. כיוון שניהול תיקי השקעות הוא פעילות וולונטרית של לקוחות, ויש חלופות למכביר המאפשרות קבלת שירות אנושי, נראה כי אין מקום לקבוע חובה כפי שהוצע. ובאופן כללי, סוגיה זו עשויה לעלות בהמשך הדרך כאשר פעילות בינה מלאכותית תהפוך משמעותית יותר, ואין מקום להקדים ולקבוע חובה גורפת של העמדת חלופה עם מעורבות אנושית. בד בבד, יש מקום לאפשר השגה לגורם אנושי, ובדומה לכך הרגולטורים עשויים לחייב חלופת מענה אנושי לפניות של לקוחות. בעתיד עשויות להידרש חלופות אנושיות גם למערכות בנושאים מסוימים.

129 דוח OECD משנת 2023.

130 דוח ESMA משנת 2023.



המלצות בנושא מעורבות אנושית

א. מעורבות אנושית בהחלטות משמעותיות: בעוד שמעורבות אנושית עשויה להיות כלי אסדרתי יעיל, המשרת תכליות שונות, החלת דרישת מעורבות אנושית באופן גורף עשויה לייצר עלויות וחסמים לשילוב הטכנולוגיה ואף לפגוע ביתרונות הבינה המלאכותית עבור הצרכן. לפיכך, וכפי שפורט ביחס לכלים אחרים ובדומה למסמכי אסדרה בעולם, לעמדת הצוות איזון ראוי הוא אימוץ דרישה זו ביחס להחלטות בעלות השלכות משמעותיות עבור הפרט (המקבילות לסיכון גבוה), בהיעדר חלופות מפצות כמפורט להלן. בהקשר זה יוכלו הרגולטורים לקבוע קריטריונים או להבנות את שיקול הדעת לצורך הגדרת ההחלטה ככזו, על בסיס מהותיות ההחלטה עבור הפרט והסיכון הגלום בטעות בה (בהקשר זה ראו הפרק ראייה כוללת ומבוססת סיכונים וכן פרק היידוע והגילוי).

ב. נקודת הזמן למעורבות אנושית: מעורבות אנושית בנוגע להחלטה ספציפית יכולה להתבצע בשתי נקודות זמן מרכזיות: בעת קבלת ההחלטה או לאחר קבלתה באמצעות השגה של הלקוח. החיסרון המרכזי של מעורבות אנושית מוקדמת, בעת קבלת ההחלטה, נוגע לשיקולי היעילות שנדונו לעיל. החיסרון המרכזי של מעורבות מאוחרת, בעקבות השגה של הלקוח, נעוץ בכך שהיא מחייבת את הפרט לפעול כדי להפעיל את המעורבות האנושית, ומבוססת על הנחה לפיה יהיו לפרט המודעות והיכולות להשיג על החלטה שהתקבלה בעניינו. גם בהקשר זה מומלץ לאמץ את ההבחנה שבהמלצה הראשונה, **קרי, מעורבות בזמן אמת תידרש רק ביחס להחלטות מהותיות עבור הפרט אשר הסיכון הגלום בהן גבוה, בהיעדר חלופות מפצות כמפורט להלן.**

ג. חלופות מפצות: יש לבחון את דרישת המעורבות האנושית בתוך מערכת הדרישות הרגולטוריות הנוספות החלות על המערכת. כך, אם ישנה מערכת עם יכולת הסברתיות, כנראה שאין הכרח לדרוש מעורבות אנושית בעת קבלת ההחלטה וניתן להסתפק בהשגה או בקרה אנושית על ההחלטות. משמעות הדבר היא כי **גם החלטות בסיכון גבוה עשויות שלא לחייב מעורבות אנושית אם קיימות חלופות מפצות הולמות.**

ד. אבחנה בין מערכות תומכות החלטה לבין מערכות המקבלות החלטות: אם ממילא גורם אנושי מקבל את ההחלטה בסופו של דבר, הרי שיש לצמצם את דרישת המעורבות האנושית רק להיבטי בקרה ופיקוח כלליים על תפקוד המערכת. מכאן שבמערכות תומכות החלטה, בהן אין פעילות אוטומטית מלאה, אפשר לצמצם את דרישות המעורבות האנושית על החלטות ספציפיות ולהתמקד בבקרה על פעילות המערכת ותוצאותיה.

ה. חלופה של פעילות אנושית ו-Opt Out: הצוות אינו סבור כי יש מקום להטיל חובה גורפת של העמדת פעילות אנושית לצד פעילות הנעשית בידי מערכות בינה מלאכותית. הצורך בהטלת חובה כאמור תלוי בנסיבות שונות, ובהן מידת חיוניות השירות, קשיים שעשויים להיות לציבור כולו לקבל את השירות ממערכות בינה מלאכותית, והאפשרות לקבלו מגופים פיננסיים אחרים. בד בבד, ככל שישנה אפשרות לקבל החלטה או שירות אנושיים, יש להביא זאת לידיעת הלקוח על מנת שיבחר האם הוא מעוניין בחלופה אנושית או אלגוריתמית, על כלל מאפייניה (ראו פרק יידוע וגילוי). יודגש, כי אם צרכן בחר בחלופה אלגוריתמית – אין למנוע ממנו אפשרות השגה לגורם אנושי כמפורט לעיל.

ו. בין מעורבות אנושית לבקרה על פעילות המערכת: הצוות סבור כי יש חשיבות רבה לבקרה על פעילות המערכת ותוצאותיה. בקרה כזו, בניגוד לדרישת מעורבות אנושית בכל החלטה פרטנית, נראית מתבקשת ביתר שאת בשלב הנוכחי בו מצויה הטכנולוגיה, בפרט אם מדובר במערכת חדשה שאין ניסיון רב בהפעלתה. בקרה על פעילות המערכת ותוצאותיה היא חיונית במניעת תקלות או שגיאות במערכת וכן בטיפול בתקלה אם תתרחש. **מוצע לאמץ את דרישה של בקרה אנושית על פעילות המערכת, להבדיל מבקרה על כל החלטה שלה.** יובהר, כי הבקרה הרציפה לא חייבת להיות אנושית בכל שלב ושלב, אך נדרשת גם בקרה אנושית.

ז. עיצוב המערכת: לנוכח ההמלצות לקיומה של בקרה אנושית בזמן אמת ובדיעבד, נראה כי על גופים פיננסיים לאמץ מערכות המאפשרות בקרה אנושית בהתאם להמלצות שלעיל. **החובה לאפשר בקרה ומעורבות אנושית מוטלת על הגוף הפיננסי המכניס את מערכת הבינה המלאכותית לפעילות.**

יידוע וגילוי

אחת החובות הרגולטוריות הנדונות ביחס לשילוב מערכות בינה מלאכותית בשירותים ובמוצרים שונים היא **דרישת יידוע על עצם השימוש במערכת בינה מלאכותית**. כלומר יידוע לציבור, לרגולטורים ובעלי עניין נוספים כי בשירות או במוצר מסוים נעשה שימוש במערכת שניתן לאפיין כמערכת בינה מלאכותית.

מלבד יידוע על עצם השימוש במערכת בינה מלאכותית, עשויות להיות **דרישות גילוי למשקיע או ללקוח שעניינן מאפייני מערכת הבינה המלאכותית, השלכותיה, והאופן בו היא משתלבת בשירות או המוצר**. דרישות גילוי אלה עשויות לנוע על פני משרע רחב של אפשרויות, הן ביחס לתכני הגילוי (למשל, תכנים כלליים או ספציפיים; תכנים המיועדים לשקף בעיקר סיכונים ואזהרות או תכנים המיועדים לשקף גם יתרונות; וכדומה) הן ביחס למתכונת הגילוי (למשל, גילוי במסגרת הסכם עם הלקוח, גילוי על בסיס תקופתי, גילוי סטנדרטי או בולט; וכדומה). דרישות הגילוי קשורות בקשר הדוק לסוגיית ההסברתיות שנדונה לעיל.

פן נוסף של דרישות הגילוי הוא **צמצום הסיכון לפרסומים מטעים סביב נושא הבינה המלאכותית**. טכנולוגיות חדשות ומורכבות עשויות להוות כר פורה לפרסומים המאדירים את הגופים העושים בהן שימוש, ככלי שיווקי. חובות גילוי יכולות לצמצם סיכון זה ולחייב את הגופים בפרסום אמת.

נציין כבר עתה כי בהקשרי בינה מלאכותית יוצרת (Generative AI) לדרישת הגילוי חשיבות מוגברת לנוכח האתגרים הייחודיים שטכנולוגיה זו מזמנת, למשל, ביחס לאמינות המידע, מקורותיו וכדומה. מסמכי אסדרה, כגון החקיקה האירופאית, כבר מייחדים לטכנולוגיה זו דרישות רגולטוריות מובחנות גם בהקשרי הגילוי.

תכליות חובות הגילוי

חובות יידוע או גילוי מוכרות בהקשרים רגולטוריים שונים כאשר תכליתן לאפשר לציבור לקבל החלטות מושכלות. כך מצטמצמים פערי המידע בין הצרכן לנותן השירות, ובפני הציבור נפרש כלל המידע הרלוונטי לקבלת החלטה תוך שקילת כלל השיקולים הרלוונטיים – בין אם מדובר בהחלטה בדבר השקעה בחברה ציבורית שחבה בחובות גילוי ובין אם מדובר בהחלטה לצרוך סוג מזון מסוים בהתאם למידע התזונתי שיש לכלול על האריזה.¹³¹

הנחה זו מתקשרת גם לתפישה שלפיה חובות גילוי הן חלק חשוב מהאוטונומיה של הפרט לשלוט בקבלת ההחלטות בענייניו. מעבר לכך, חובות גילוי ויידוע נתפשות גם כדרישות שמסייעות לקיים ביקורת ציבורית, לעודד תחרות וכדומה.

בעולמות הפיננסיים, דרישות גילוי הן אחת הטכניקות הרגולטוריות השכיחות ביותר, וניתן למצוא אותן למעשה ביחס לכל שירות או מוצר המוצע ללקוח.¹³² כך למשל בישראל אפשר למצוא חובות גילוי מקיפות ללקוח במסגרת פעילות בנקאית,¹³³ במסגרת פעילות ייעוץ השקעות או ייעוץ פנסיוני,¹³⁴ או במסגרת של השקעה עקיפה או ישירה בניירות ערך.¹³⁵

חובות הגילוי מכוח הוראות אלה והוראות רבות נוספות נועדו לאפשר לציבור בין היתר לדעת מהו מצבו הכספי, להשוות בין חלופות השקעה וחיסכון שונות, ללמוד על הגוף המציע לו את השירות או המוצר ועל אופיים של אלה, לדעת מהן העמלות או דמי הניהול הנגבים ממנו להבין את הסיכון הכרוך בשירות מסוים או מגבלותיו, וכיוצא באלה. כפי שהוסבר לעיל, דרישות גילוי אלה משרתות תכליות יסוד של קבלת החלטות מושכלות, צמצום פערי מידע וכו'

131 Weil, David, Archon Fung, Mary Graham, and Elena Fagotto. "The effectiveness of regulatory disclosure policies." *Journal of Policy Analysis and Management: The Journal of the Association for Public Policy Analysis and Management* 25, no. 1 (2006): 155-181.

132 Enriques, Luca and Gilotta, Sergio, Disclosure and Financial Market Regulation (April 11, 2014). Chapter in *The Oxford Handbook on Financial Regulation*, edited by Eilís Ferran, Niamh Moloney, and Jennifer Payne, (Oxford University Press), European Corporate Governance Institute (ECGI) – Law Working Paper No. 252/2014, Oxford Legal Studies Research Paper No. 68/2014, <https://ssrn.com/abstract=2423768>.

133 ראו למשל סעיף 5 לחוק הבנקאות (שירות ללקוח), התשמ"א-1981, וכללי הבנקאות (שירות ללקוח) (גילוי נאות ומסירת מסמכים), התשנ"ב-1992.
134 ראו למשל סעיף 21 לחוק הפיקוח על שירותים פיננסיים (ייעוץ, שיווק ומערכת סליקה פנסיוניים), התשס"ה-2005; סעיפים 14 ו-16 לחוק הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, התשנ"ה-1995, ותקנות הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות (דוחות), התשע"ב-2012.

135 ראו למשל סעיפים 16, 17 ו-36 לחוק ניירות ערך, והתקנות מכוחם; סעיפים 26, 72 ו-73 לחוק השקעות משותפות בנאמנות, התשנ"ד-1994, והתקנות מכוחם.

הקיימים בין הציבור ובין הגופים הפיננסיים, הרתעת בעלי כוח בגופים הפיננסיים מניצול לרעה של כוחם, עידוד תחרות בין גופים ומוצרים פיננסיים וביסוס אמון הציבור במערכת הפיננסית. לעתים משרתות דרישות הגילוי יעדים נוספים כגון יעילות השוק ותמחור רציף של הנכסים הנסחרים בו.¹³⁶

ההנחות וההצדקות הללו משמשות גם בשיח ביחס להחלת חובה זו בהקשרי מערכות בינה מלאכותית. בהקשר זה ישנו גם דגש על כך שעצם הגילוי והיכולת לקיים ביקורת ציבורית על שירותים ומוצרים שמשלבים טכנולוגיה זו מגבירים את בטיחותן, אמינותן ואמון הציבור בהן. כפי שיידון להלן, הגשמת תכליות אלה קשורה בהיקף חובת הגילוי ביחס לפעילות המערכת.

ראשית, שילובה של הטכנולוגיה במוצרים ובמוסדות פיננסיים נמצא בראשיתו. יעילותה של הטכנולוגיה והסיכונים שהיא מזמנת עוד טרם התבררו לחלוטין. במצב דברים זה, יש ערך ליידע את הציבור בדבר השינוי באופן מתן השירותים כדי שתעמוד בפניו הבחירה איזה שירות לצרוך (ככל שישנה חלופה כזו). ייתכן שיהיה מקום לבחון היקף דרישה זו לאחר שהטכנולוגיה תשתרש בתחום השירותים הפיננסיים.

שנית, דרישת הגילוי עשויה לדחוף לשיפור הטכנולוגיה עם פגיעה מוגבלת ביעילות. הדרישה של לקוח לעבור לשירות לקוחות או לגורם אנושי במקום להמשיך באינטראקציה עם בינה מלאכותית, בעקבות הגילוי, תושפע מאיכות שירות הלקוחות שיציע המוסד הפיננסי. במובן זה ניתן לצפות כי דווקא חובת גילוי והרצון לשמר את היעילות תדחוף את המוסדות הפיננסיים לשפר את מוצריהם באופן שיפחית את המקרים בהם לקוחות יירתעו מפני השימוש בבינה מלאכותית.

לבסוף, לדרישת הגילוי יש גם יתרונות עבור הרגולטור. כאמור לעיל, שילוב הטכנולוגיה במוצרים ובמוסדות פיננסיים נמצאת בראשיתה. לעיתים אין מגבלה רגולטורית על עצם שילוב הטכנולוגיה. מכאן שהידיעה בדבר המעבר לשימוש בטכנולוגיה זו בתחום הפיננסי עשויה להיחשף רק בדיעבד לרגולטור. דרישת גילוי בסיסית תאפשר לרגולטור לקבל תמונת מצב עדכנית ביחס לשילוב הטכנולוגיה במוסדות הפיננסיים וכן ללמוד על השפעת הטכנולוגיה על המוסד הפיננסי (למשל, ללמוד על עלייה בתלונות על שירות הלקוחות).

כפי שיידון להלן, הגשמת תכליות אלה קשורה בהיקף ובמתכונת חובת הגילוי ביחס לפעילות המערכת.

דרישות הגילוי במסמכי אסדרה בעולם העוסקים בבינה מלאכותית

הרוב המוחלט של מסמכי הרגולציה והאתיקה המובילים בעולם בהקשרי בינה מלאכותית מציע לעגן דרישות גילוי, שקיפות או הסברתיות, ובכך מציבים דרישות אלו כאחד מעמודי התווך של רגולציית בינה מלאכותית.

- אחד מעקרונות ה-OECD ביחס לשימוש אחראי ביישומי בינה מלאכותית הוא **שקיפות** (והסברתיות בדיבר אחד). תכליות השקיפות, בהתאם לעקרונות אלה, הן לטפח הבנה כללית של מערכות בינה מלאכותית; ליידע שחקנים רלוונטיים שונים באשר לממשקים שלהם עם מערכות בינה מלאכותית ולאפשר לאלה המושפעים מתוצרי המערכת הבנה יותר עמוקה של המערכת ויכולת להתמודד או לערער על החלטותיה.¹³⁷
- **EU AI Act** – חקיקה זו מונה את עקרון השקיפות כעקרון כללי שחל על כלל מערכות הבינה המלאכותית במנותק משאלת הסיכון הטבוע בהן. החקיקה אמנם קובעת רגולציה לפי גישה מבוססת סיכונים, אך עקרון השקיפות יחול על כלל המערכות. כחלק מחובה זו קיימת חובת יידוע על כך שאינטראקציה עם מערכת המערכת בינה מלאכותית, אך זאת גם באופן המאפשר לפרט להבין ולהתמודד עם תוצרי המערכת. מעבר לחובה הכללית הזו, החקיקה מתייחסת לדרישות יידוע ספציפיות בהתאם לסוג המערכת. כך, למשל, חלה חובת יידוע כאשר מידע מסוים נוצר באמצעות בינה מלאכותית יוצרת, ויש לפרסם את דוח הערכת הסיכונים שנערך ביחס למערכות בסיכון גבוה. חובת השקיפות, במקרה האירופאי, משתרעת גם לחובה לרשום מערכות מסוימות במאגר מידע ייעודי למערכות בסיכון גבוה.¹³⁸
- **ארצות הברית** – הצו הנשיאותי ממוען, בין השאר, לרגולטורים ולסוכנויות הפדרליות ביחס לשימוש של גופים מפוקחים במערכות בינה מלאכותית ושימוש של הסוכנויות עצמן במערכות אלה. בין השאר, מומלץ לרגולטורים

¹³⁶ ראו בפסיקת בית המשפט העליון לגבי תכליות הגילוי בהקשרים פיננסיים שונים: ע"א 5320/90 א.צ. ברנוביץ נכסים והשכרה בע"מ נ' רשות ניירות ערך, פ"ד מו(2) 818 (1992); ע"א 5893/91 טפחות – בנק למשכנתאות לישראל בע"מ נ' צבאח, פ"ד מח(2) 573 (1994).

¹³⁷ OECD, Transparency and Explainability (Principle 1.3), <https://oecd.ai/en/dashboards/ai-principles/P7>

¹³⁸ EU AI Act, Article 50

לעשות שימוש בסמכויותיהם כדי לקבוע חובות שקיפות לגופים המפוקחים. בהקשר זה, מבהיר הצו כי דרישות אלה נועדו להגן על צרכנים מפני מקרים של הונאה, פגיעה בפרטיות או ביציבות פיננסית. כמו כן, הצו מדגיש את חשיבות השקיפות ביחס לשימוש של סוכנויות פדרליות בבינה מלאכותית לצרכיהן.¹³⁹ זאת ועוד, ב"מגילת הזכויות" שפרסם הבית הלבן, שקיפות נמנתה כאחד מהעקרונות המנחים לאסדרת השימוש בבינה מלאכותית.¹⁴⁰

• חובת הגילוי קשורה גם בהיבטי מידע אישי. ה-GDPR כוללת חובה לגלות לפרט כי נעשה שימוש במידע שנאסף בעניינו במסגרת מערכת עיבוד מידע אוטומטי ולצורך קבלת החלטות באמצעות מערכת כזו או (ובהמשך גם מעניקות לו את הזכות להתנגד לכך).

סקירה קצרה זו ממחישה כי דרישת הגילוי השתרשה כדרישה עצמאית במסמכים רגולטוריים מובילים העוסקים באסדרת שימושי בינה מלאכותית. עם זאת, היקף דרישת הגילוי אינו בהכרח אחיד ועשוי להשתנות בהתאם לסוג הטכנולוגיה שבה נעשה שימוש, מידת הסיכון של המערכת, סוג המשתמש וכדומה.

דיון במישורי הגילוי השונים

כאמור בפתח הדברים, אפשר לחלק את הדיון בדרישות גילוי בסקטור הפיננסי לשלושה מישורים: המישור הראשון עניינו דרישת היידוע הבסיסית בדבר עצם השימוש במערכת בינה מלאכותית. המישור השני עניינו במתכונת חובת הגילוי ותכניה בדבר מאפייני מערכת הבינה המלאכותית והחלטותיה. המישור השלישי הנו התמודדות עם גילוי שיווקי מטעה בנושא בינה מלאכותית.

א. דרישת היידוע הבסיסית בדבר עצם השימוש במערכת בינה מלאכותית

דרישת הגילוי הבסיסית עשויה להסתכם בכך שיהיה גלוי וברור שהאינטראקציה עם שירות לקוחות של בנק, למשל, אינה עם גורם אנושי אלא עם מערכת צ'אט-בוט המתבססת על בינה מלאכותית או שבקבלת ההחלטה בעניינו של גורם מסוים הייתה מעורבת מערכת בינה מלאכותית. כלומר, דרישת היידוע תשתרע על עצם השימוש בבינה מלאכותית. גילוי זה יכול להניע את הציבור לפעולה במובן זה שהוא יוכל לבחור לצרוך שירות מנותן שירות פיננסי אחר, או לבקש, ככל שהדבר ניתן, לעבור למערכת ללא בינה מלאכותית או לאינטראקציה עם אדם אנושי (ככל שהמוסד הפיננסי מספק שירות חליפי). יתרה מכך, ניתן גם לטעון שדרישת יידוע "בסיסית" עשויה לשרת תכליות רחבות יותר, כגון ביקורת ציבורית על מוצרים ושירותים, שכן הידיעה על השימוש במערכת בינה מלאכותית יכולה להניע תגובה ואף דרישה לקבלת מידע יותר על פעילות המערכת שבשימוש.

החיסרון המרכזי בהחלת דרישת יידוע גורפת הוא הפגיעה האפשרית ביעילות שלשמה מלכתחילה הוחלט לשלב בינה מלאכותית בפעילות המוסד הפיננסי. מודלים ג'נרטיביים, למשל, נועדו לתת לצרכן "חוויית משתמש" כמעט אנושית. באופן זה מוסד פיננסי יכול להעניק שירות יותר מהיר ולחסוך עלויות בגין שירות לקוחות. עם זאת, החלת חובת גילוי עלולה להרתיע צרכנים ולהניע אותם לבקש לעבור לשירות לקוחות אנושי בלי קשר לאיכות המענה שניתן לקבל מהמערכת וכך לפגוע ביעילות שהמוסד הפיננסי ביקש להשיג. חסרון אפשרי נוסף בדרישת היידוע "הבסיסית" הוא החשש שהרגולטור יסתפק בדרישת יידוע בסיסית וימנע מקביעת דרישות יידוע נרחבות יותר כאשר הדבר יתאפשר ואף יידרש לשם הגשמת תכליות נוספות שחלקן נמנו לעיל, כגון ביקורת על המערכת וכדומה. לבסוף, דרישת היידוע עלולה להתפרש כאיתות שלילי מטעם הגוף הפיננסי המאותת לפרט שכדאי לו להימנע מצריכת שירות כזה.

ב. חובות גילוי בדבר מאפייני מערכת הבינה המלאכותית והשלכותיה

מעבר לדרישת היידוע הבסיסית, ישנן, כמתואר לעיל, דרישות גילוי רבות בתחומי הפיננסיים, והשאלה העולה היא האם וכיצד לשלב בתוכן חובות גילוי העוסקות במאפייני פעולתה של מערכת הבינה המלאכותית.

שאלה זו מתעוררת ביחס לפירוט שאמור להרחיב את מנעד המידע עבור הצרכן הפיננסי ביחס למערכת ולכלול בו גם מידע על המערכת עצמה ומאפייניה.

כך למשל, ביחס להיקף הגילוי – האם יש לפרט על מגבלות המערכת או לחלופין על יתרונותיה או האם יש לפרט אם מדובר בשירות ניסיוני. וביחס למתכונת הגילוי – האם יש למסור את הגילוי בפרסומים של המוצר או השירות, בהסכם עם הלקוח, וכדומה, ואיזו מידה של בולטות, אם בכלל, יש לדרוש ביחס אליו.

139 ראו ה"ש 25 לעיל.

140 ראו ה"ש 24 לעיל, שם עקרון הגילוי מעוגן כחובת "notice".



להמחשת הצורך בגילוי בדבר מאפייני מערכת בינה מלאכותית והשלכותיה, אפשר לקחת כדוגמא מערכת המספקת אנליזות על ניירות ערך, קרי פעילות של ייעוץ השקעות בנוגע לכדאיות ההשקעה בניירות ערך שונים. נניח כי מערכת בינה מלאכותית כאמור מבצעת ניתוח של ניירות הערך על בסיס נתונים שונים, ובהם דיווחי התאגידים שהנפיקו את ניירות הערך, אך היא מתבססת רק על נתוני הדוחות הכספיים של התאגידים ואינה מביאה בחשבון דיווחים אחרים. במסגרת הגילוי אודות מערכת כאמור יהיה מקום להסביר כי זהו בסיס המידע של המערכת וכן את השלכות הדבר על ביצועיה. כך לדוגמא, מערכת כאמור צפויה להציג ניתוח בדבר כדאיות ההשקעה בתאגיד בלי להביא בחשבון דיווח שנמסר על-ידו לאחר פרסום הדוחות הכספיים בנוגע להתפתחות מהותית בעסקיו. לגילוי זה על מגבלות המערכת עשויה להיות חשיבות עבור לקוח העושה בה שימוש.

ג. התמודדות עם גילוי שיווקי מטעה בנושא בינה מלאכותית

גילוי שיווקי מטעה בנושא בינה מלאכותית, אשר מכונה גם בשם AI Washing, זוכה לאחרונה לתשומת לב רגולטורית גוברת בעולם. הכוונה בביטוי זה היא למצגים לפיהם מוצרים או שירותים נהנים מפעילותן של מערכות בינה מלאכותית, כאשר בפועל מערכות אלה כלל אינן בשימוש או שהשימוש בהן שולי ויתרונותיהן מוגבלים. כך למשל רשות ניירות ערך האמריקאית (SEC) נקטה הליכים כנגד מנהלי השקעות שהצהירו באופן כוזב ומטעה אודות השימוש שלהם במערכות בינה מלאכותית,¹⁴¹ והצעת ה-SEC משנת 2023 מבקשת להתמודד גם עם סיכון זה.¹⁴² גם רשות הגנת הסחר האמריקאית (FTC) פרסמה אזהרות מפני הפרזות והבטחות לא מבוססות בשיווק מוצרים המבוססים לכאורה על פעילות מערכות של בינה מלאכותית.¹⁴³

גילוי שיווקי מטעה מסוג זה אינו ייחודי לפעילות של בינה מלאכותית, וניתן היה למצוא אותו גם בעבר ביחס לתופעות שיצרו עניין בקרב הציבור הרחב, שעה שזה אינו יכול באופן מעשי לעמוד על מהימנות הפרסומים, מפאת מורכבות הטכנולוגיה והעדר ידע מספק.

חובות הגילוי בדינים הפיננסיים כוללות פן שלילי שעניינו איסור על מסירת מידע מטעה לציבור. גופים פיננסיים אינם מחויבים רק למסור מידע מלא אודות פעילותם אלא גם להימנע ממסירת מידע מטעה.¹⁴⁴ ההתמודדות עם פרסומים לא מדויקים בהיבטים שונים נעשית באמצעות פיקוח ואכיפה על דרישות הגילוי והפרסום החלות על הגופים המפוקחים, והיא תוכל להיות דומה ביחס לפרסום מטעה הנוגע לפעילות של בינה מלאכותית.¹⁴⁵

מלבד האיסור על מידע מטעה, דרישות גילוי להסבר על מהות השימוש בבינה מלאכותית, ובמקרים בהם ניתן לעשות כן – גם על איכות המערכת (למשל בדרך של מסירת מידע על תוצאות הפעילות בה), יוכלו לסייע במניעת מצגים "ורודים" שאינם מדייקים למציאות.

במסגרת הערות הציבור לדוח הביניים עלתה טענה לפיה יש לחייב יידוע וגילוי רק במקרים בהם יש למשתמש במערכת אינטראקציה ישירה עם הבינה המלאכותית, וכי דרישות בהקשר זה עלולות לפגוע בחוויית המשתמש, להעמיס במידע שספק אם לקוחות יעשו בו שימוש, ולהרתיע מפני שימוש במערכת. הצוות סבור כי אין מקום לקבל טענות אלה. ראשית, יידוע וגילוי עשויים להיות חשובים ללקוח או למשקיע גם אם אין לו אינטראקציה ישירה עם המערכת, אך יש לה השפעה מהותית עליו. כך למשל, כאשר מנהל תיקים משתמש במערכת בינה מלאכותית לצורך קבלת החלטות השקעה עבור הלקוח, אין ללקוח עצמו אינטראקציה ישירה עם המערכת, אולם השימוש בה עשוי בהחלט להשפיע עליו (כמו גם על החלטתו לקבל את השירותים ממנהל תיקים זה). שנית, בדומה לדרישות גילוי קיימות, המהוות כאמור כלי רגולטורי שכיח מאוד בתחום הפיננסיים, צריך וניתן לעצב את דרישות הגילוי באופן שיתרום ללקוח או למשקיע. בדוח נוספה דוגמא להמחשת הצורך בגילוי כאמור.

הערה אחרת היתה כי מקום בו מיידעים את הלקוח על מערכת בינה מלאכותית, יש להציע לו אפשרות לשימוש במוצר חלופי ללא בינה מלאכותית. בהקשר זה נטען גם כי הזכות להחלטה אנושית הוצעה כבר בספרות העוסקת בנושא, וכי היא תקדם עקרונות של הגינות וצדק. הערות אלה חורגות מנושא היידוע ועוסקות למעשה בשאלת המעורבות האנושית, לרבות שאלת הצורך בהעמדת חלופה של מעורבות אנושית, ולכן הן נדונו בפרק הקודם העוסק בכך.

¹⁴¹ <https://www.sec.gov/newsroom/press-releases/2024-36>

¹⁴² ראו ה"ש 69 לעיל.

¹⁴³ FTC Division of Advertising Practices "Keep your AI claims in check" (February 27, 2023)

¹⁴⁴ ראו למשל סעיף 44 לחוק ניירות ערך, התשכ"ח-1968, וסעיף 73 לחוק השקעות משותפות בנאמנות, התשנ"ד-1994, האוסרים על הכללת "פרט מטעה" במסמכי גילוי שונים.

¹⁴⁵ ראו הסדרי אכיפה בהם התקשרה ה-SEC בחודש מרץ 2024 עם שתי חברות ייעוץ השקעות בגין מצגים מטעים בדבר השימוש שהן עשו כביכול בבינה מלאכותית, <https://www.sec.gov/news/press-release/2024-36>



הערות נוספות היו כי הדוח אינו מבהיר די הצורך מהן דרישות הגילוי שיחולו בכל מקרה ומקרה, ואינו מציג לדוגמא את הגילוי הנדרש במצב בו מופעלות מערכות במודל ניסיוני, או לדוגמא דרישות גילוי ומנגנונים ספציפיים למניעת תופעת ה-AI Washing שנדונה בדוח. ואולם, בהינתן שהדוח עוסק בפעילויות פיננסיות מגוונות, לגביהן קיימות כבר דרישות גילוי רבות במסגרת הדינים השונים, אין מקום או אפשרות מעשית להתייחס בפירוט לדרישות כאמור. כפי שצוין בהמלצות הצוות, חובות הגילוי בדבר מאפייני מערכות בינה מלאכותית והשלכותיה צריכות להשתלב בדרישות הגילוי הקיימות לגבי השירות או המוצר המוצעים ללקוח, ולעסוק במאפיינים הייחודיים הנובעים מטכנולוגיית הבינה המלאכותית. בהתאם להמלצה עקרונית זו יוכלו הרגולטורים הפיננסיים לעצב את דרישות הגילוי הספציפיות בכל תחום ותחום כאשר הדבר יידרש.



המלצות בנושא יידוע וגילוי

1. דרישת יידוע בדבר עצם השימוש במערכת בינה מלאכותית -

לדרישת יידוע בסיסית בדבר עצם השימוש במערכת בינה מלאכותית יש ערך ציבורי וצרכני העולה על החסרונות שנמנו לעיל.¹⁴⁶ דגשים ליישום הדרישה:

- נראה כי יש מקום לדרישה זו ביתר שאת בשלב ראשוני של כניסת הטכנולוגיה, בפרט כאשר ישנה במקביל פעילות פיננסית שלא באמצעות בינה מלאכותית;
- כאשר יש השפעה מהותית לטכנולוגיה על השירות או המוצר המוצע ללקוח, בפרט אם זו קיימת בהשוואה לשירות או המוצר המוצעים במקביל שלא באמצעות בינה מלאכותית;
- יש להקפיד כי הודעת היידוע תינתן בשפה ניטרלית וברורה – אשר לא תייצר העדפה לשירות אחד על משנהו ללא בסיס.
- דרישת היידוע יכולה להיות רלבנטית מקום בו לקוח עשוי לטעות ולחשוב שהוא באינטראקציה עם אדם. לצד האמור, אין הכרח לדרישת יידוע מקום בו ברור כי נעשה שימוש בבינה מלאכותית.

2. חובות גילוי בדבר מערכות בינה מלאכותית -

הצוות סבור כי חובות גילוי בדבר מאפייני מערכת הבינה המלאכותית והשלכותיה צריכות להשתלב בדרישות הגילוי הקיימות לגבי השירות או המוצר המוצעים ללקוח. בהתאמה, חובות הגילוי צריכות לעסוק במאפיינים הייחודיים הנובעים מטכנולוגיית הבינה המלאכותית:

בדומה להמלצה בנושא זה בפרק "קופסה שחורה" והסבריות, יש מקום לחובות גילוי מוגברות בדבר מאפייני מערכת הבינה המלאכותית, כאשר יש למערכת זו השלכות מהותיות על פעילות המוסד והצרכנים. הגילוי בהקשר זה צריך להתמקד במאפיינים הייחודיים של הפעילות הנובעים מהטכנולוגיה (בהשוואה למצב בו הפעילות הייתה נעשית ללא מערכת של בינה מלאכותית). לשם המחשה, בפעילות של ניהול תיקי השקעות הנעשית בעזרת מערכת בינה מלאכותית יש להתמקד במהות השירות ובמאפייניו הייחודיים, בסיכונים האפשריים הנובעים ממנו, במתודולוגיה של המערכת המשמשת לקביעת מדיניות השקעה או לקבלת החלטות ההשקעה.¹⁴⁷

מתכונת הגילוי – נדרש כי הגילוי יעשה בטרם רכישת הנכס הפיננסי או ההתקשרות בשירות הפיננסי המשלב בינה מלאכותית. יש לחתור לכך שהגילוי יינתן בשפה בהירה, תמציתית, פשוטה ומובנת ככל הניתן ללקוח. הוראות גילוי ספציפיות יעוצבו על-ידי הרגולטורים בהתאם לאופי הפעילות והדרישות החלות לגביה.

3. הגבלת פרסומים שיווקיים מטעים -

ככל שתתפתח תופעה של פרסומים שיווקיים מטעים בנושא בינה מלאכותית (AI Washing) יהיה מקום להתמודד איתה באמצעות סל הכלים הרגולטורי הקיים, הכולל עמדות והוראות בדבר הגילוי הניתן על-ידי גופים מפוקחים, פעולות אכיפה לטיפול בהפרת הדין מקום בו ניתן גילוי מטעה למשקיעים או ללקוחות, ופעולות של חינוך פיננסי כגון התראות והסברים לציבור בנוגע לפעילויות פיננסיות המוצעות להם תוך הדגשת שימושי בינה מלאכותית.

¹⁴⁶ זו גם הגישה המוצגת במסמך המדיניות.

¹⁴⁷ ראו רשות ניירות ערך, הוראה לבעלי רישיון בקשר למתן שירותים תוך שימוש באמצעים טכנולוגיים (2016), סעיפים 10, 11, 12, 17 ו-20 להוראה. בדברי ההסבר של ההוראה הובהר כי דרישה זו אינה כוללת חשיפת סודות מסחריים, ומטרתה היא להעניק הסבר עקרוני, המתמקד לדוגמה בכך שהאלגוריתם מעבד את המידע לנוכח תשובות הלקוח ועל כן יש חשיבות במענה יסודי לשאלות, או לדוגמה בסוגי הנכסים עליהם עשוי האלגוריתם להמליץ. ראו עוד על הוראה זו בפרק ייעוץ השקעות וניהול תיקים להלן.



תיבה 2: מהי אוריינות של בינה מלאכותית? וכיצד נוכל להשיגה במגזר הפיננסי?

בעולם הטכנולוגי והדיגיטלי בו אנו חיים, "אוריינות" אינה מתמצה ביכולת לקרוא, לכתוב ולהשתמש בשפה אלא כוללת סט כישורים רחב יותר המאפשר להשתמש ביישומי טכנולוגיה מתקדמים, ובכלל כן היכולת לנתח, להבין, להגיב ולבקר את היישום הרלוונטי.

ההגדרה המקובלת בספרות האקדמית לאוריינות בתחום הבינה המלאכותית מתייחסת ליכולתו של אדם להבין את מנגנון הפעולה של בינה מלאכותית, להעריך אותה באופן ביקורתי, לקיים עימה אינטראקציה, ולעשות בה שימוש יעיל לצרכיו באינטרנט, בבית ובמקום העבודה.¹⁴⁸

על אף שהשימוש ביישומי בינה מלאכותית הולך וגובר, מחקרים מצביעים על כך שיכולת ההתמצאות של הציבור הרחב בטכנולוגיה של הבינה המלאכותית הינה במקרים רבים מוגבלת. מרבית האוכלוסייה אינה מבינה את אופן הפעולה של מערכות בינה מלאכותית והטכנולוגיה הניצבת מאחוריהן ואף אינה ערה להשלכות של הסוגיות האתיות והסיכונים הכרוכים בבינה מלאכותית.¹⁴⁹ מצב דברים זה נכון ככל הנראה גם לישראל. כך למשל, במסגרת דיון שהתקיים באחרונה בכנסת בוועדת המשנה של ועדת המדע והטכנולוגיה לענייני בינה מלאכותית, ציינה נציגת בנק ישראל ביחס לכישורים שצפויים להידרש בשוק העבודה כי רמת המוכנות של המשק הישראלי לאימוץ בינה מלאכותית אינה גבוהה דיה, ויו"ר הוועדה קראה לנקיטת צעדים להגברת המוכנות.¹⁵⁰

רגולטורים וקובעי מדיניות בעולם כבר עוסקים באוריינות בבינה מלאכותית ("AI Literacy"). דוגמה בולטת לכך היא חקיקת האיחוד האירופאי (EU AI Act) במסגרתה יוחדה הוראה לנושא.¹⁵¹ מטרת האסדרה בהקשר זה היא כי חברות שיוצרות ומשתמשות במערכות בינה מלאכותית – ללא תלות במידת הסיכון הכרוכה בהן – יוודא שעובדיהן וכל מי שמתפעל או משתמש במערכות הללו עבורן או מטעמן הינם בעלי יכולת הבנה והתמצאות הולמים, ובכלל כן לעניין היכולת הטכנית, הניסיון וההכשרה. ואכן, **היבט אחד** של אוריינות בתחום הבינה המלאכותית מטרתו לוודא כי גופים עסקיים היוצרים או משתמשים ביישומי בינה מלאכותית הינם בעלי כישורים מתאימים לכך.

היבט שני נוגע לאוריינות בינה מלאכותית בקרב עובדי המגזר הציבורי – הן קבוצת העובדים שעיסוקה קשור בבינה מלאכותית הן הקבוצה הרחבה יותר שתעשה שימוש בבינה מלאכותית במסגרת עבודתה. שתי הקבוצות האמורות נזקקות לכישורי בינה מלאכותית, ובפרט ליכולת לעשות שימוש אפקטיבי ביישומי בינה מלאכותית וכן להכיר ולהתמודד עם הסיכונים הנובעים מהם. ראו בהקשר זה את המלצת הצוות בנדון בחלק ה' – פעולות נוספות לקידום רגולציה פיננסית בתחום הבינה המלאכותית להלן.

היבט שלישי הוא קידום אוריינות בקרב הציבור הרחב. בארה"ב, למשל, הוגשה בחודש דצמבר 2023 הצעת חוק AI Literacy Act אשר נועדה לתקן את חוק האוריינות הדיגיטלית בארה"ב במטרה להדגיש את החשיבות של אוריינות בינה מלאכותית עבור הציבור הרחב (ולא רק ביחס ליצרנים או משתמשים).¹⁵²

Duri Long and Brian Magerko. 2020. What is AI Literacy? Competencies and Design Considerations. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–16. <https://doi.org/10.1145/3313831.3376727>

Cary Funk, Alec Tyson, Brian Kennedy, How Americans view emerging uses of artificial intelligence, including programs to generate text or art (February 22, 2023) <https://pewrsr.ch/3xP4NdO>

150 דיון בוועדת המשנה של ועדת המדע והטכנולוגיה לענייני בינה מלאכותית מיום 15 במאי 2024 – https://main.knesset.gov.il/news/pressreleases/pages/press15052024c.aspx?fireglass_rsn=true#fireglass_params&ta_bid=a4894da853688af8&start_with_session_counter=3&application_server_address=isagovil-2-me-west1.prod.fireglass.

151 EU AI Act, article 4

152 H.R.6791 – Artificial Intelligence Literacy Act of 2023, <https://www.congress.gov/bill/118th-congress/house-bill/6791>



האם יש חשיבות מיוחדת לאוריינות בינה מלאכותית של הציבור הרחב בפעילותו הפיננסית?

עיקר הספרות האקדמית בתחום עוסק באוריינות בינה מלאכותית בשוק העבודה ובמערכת החינוך באופן רחבי ולא סקטוריאלי. ואולם בהינתן חשיבותם של השירותים הפיננסיים לאזרח, והשימוש הגובר הצפוי ביישומי בינה מלאכותית בעולם הפיננסי, בין היתר, באינטראקציה מול לקוחות ובקבלת החלטות פיננסיות עבור הלקוח, צפויה להיות חשיבות רבה לאוריינות בתחום זה.

חינוך פיננסי מהווה זה מכבר אחד האתגרים הגדולים של מדינות בקידום מצבם הכספי של האזרחים, עידוד הפעילות בשוק ההון, וצמצום הסיכונים הנובעים מפעילות פיננסית לא מושכלת לרבות סיכוני הונאה. בישראל ננקטו מהלכים שונים לקידום חינוך פיננסי בקרב הציבור הרחב. כך למשל, התקבלה בשנת 2011 החלטת ממשלה בעניין הגברת החינוך הפיננסי בישראל ואף הוחלט לעגן בחוק את הקמתה של קרן ממשלתית שמטרתה לקדם את החינוך הפיננסי בישראל, אם כי זו טרם הוקמה.¹⁵³ כל הרגולטורים הפיננסיים בישראל משקיעים משאבים בחינוך פיננסי בתחומי פעילותם.

אוריינות בינה מלאכותית בתחום הפיננסי צפויה להצטרף לאתגר זה ולהוות חלק מהידע והכישורים הנדרשים במסגרת חינוך פיננסי של הציבור. ככלל, מדובר בכמה היבטים חדשים בהם תידרש למידה והבנה, כגון ההיבטים הבאים:

הבנת הרעיון ואופן הפעולה של בינה מלאכותית; רכישת כלים לשימוש ולאינטראקציה יעילה עם בינה מלאכותית; היכולת להבחין בין הפוטנציאל של AI ובין המציאות (מה בינה מלאכותית יכולה/אינה יכולה לעשות); יכולת הערכה וביקורת ביחס לתוצאה ולסיכונים הכרוכים בשימוש בבינה מלאכותית; ושימוש אחראי בבינה מלאכותית ויכולת לשקול שיקולים אתיים במסגרת זאת.

¹⁵³ החלטה מספר חכ/243 של ועדת השרים לענייני חברה וכלכלה (קבינט חברתי-כלכלי) מיום 28.11.2011, https://www.gov.il/he/pages/2011_28.11.2011
des3926?fireglass_rsn=true#fireglass_params&tabid=af5424f9d7e12c08&start_with_session_counter=3&application_server_address=isagovil-2-me-west1.prod.fire.glass



הזכות לפרטיות והגנה על מידע אישי

טכנולוגיות בינה מלאכותית מתבססות על איסוף ועיבוד מידע בצורה נרחבת, ובכלל זה על צריכת מידע אישי, כלומר מידע שנוגע לאדם מזהה או שניתן לזהותו. פיתוח טכנולוגיות אלו, שהשימוש הפוטנציאלי בהן נפרס על הקשרים מגוונים בכל תחומי החיים, מהווה גורם מאיץ ומגביר משמעותי ביותר למוטיבציה להשגת נתוני עתק, שמירתם ושימוש מגוון בהם. המידע הוא "הדלק"¹⁵⁴ או "החמצן" המניע את מערכות הבינה המלאכותית, הוא המשאב העיקרי וההכרחי לפיתוח ולפעילותו. לפיכך, פיתוח מערכות בינה מלאכותית והשימוש בהן, כרוך בניסיון להתבסס על מידע מקיף, מגוון ורחב ככל הניתן, בין אם מתוך שאיפה לייצר תוכן, תחזיות, או המלצות ברמת דיוק גבוהה, ובין אם בשל הרצון לפתח מוצרים חדשניים שלא מסתמכים בהכרח על מידע "סטנדרטי" שאפשר לצפות שישמש כתבחין להפקת תחזית מסוימת.¹⁵⁵

זאת ועוד, תוצרי מערכות ויישומי הבינה המלאכותית: התחזיות, ההמלצות ואף ההחלטות, מכוונות במקרים רבים כלפי בני אדם, ומשמשים אמצעי לחזות את התנהגותם, לזהות דפוסי פעולה אנושיים, תכונות אופי, מצב נפשי או פיזי ועוד. התוצרים מגלמים תובנות פרטניות ואישיות לגבי אדם, לעתים רגישות ואינטימיות ביותר, על היבטים פרטיים שונים בחייו.

מערכות הבינה המלאכותית מבצעות עיבוד על נתוני עתק באמצעות פעולות חישוב יעילות ואיכותיות, ומאפשרות על כן ניתוח כמויות עצומות של מידע העולה על יכולות הבינה האנושית. עיבוד המידע המבוצע על ידן נועד לאתר בין השאר קשרים ויחסי גומלין **לא צפויים** בין נתונים שונים ולמקסם את התוצרים והתובנות שניתן להפיק מהם. מכאן נובע, כי מעבר לרמה הגבוהה של הדיוק והרגישות של ניתוח ההתנהגות האנושית כאמור, למצער בשלב פיתוח מערכות הבינה המלאכותית, התוצרים והתחזיות שהן יפיקו אינם בהכרח צפויים, ידועים או מוגדרים מראש.

מאפיינים אלה של מערכות הבינה המלאכותית, מטבע הדברים, מעוררים אתגרים ומתחים לא מבוטלים בקשר להגנה על הזכות לפרטיות ועל מידע אישי, לכל אורכו של מחזור החיים של מערכות אלו – איסוף מידע לצורך פיתוח המערכת ("אימון" האלגוריתם), ועיבוד מידע בשלב יישום המערכת והשימוש בה לשם השגת מטרותיה ולשם המשך פיתוחה ודיוקה.

כך למשל, עקרון יסודי וחשוב בדיני הגנת הפרטיות, עקרון צמידות המטרה, קובע כי אין להשתמש במידע אישי אלא למטרה לשמה נאסף. ואולם כאמור בשלבי פיתוח מערכות הבינה המלאכותית (ואולי אף במהלך השימוש בהן) אין בהכרח ידיעה לגבי מהות התוצר שיופק מהן. קושי זה בא לידי ביטוי גם בשאלת טיב ההסכמה של אדם לעיבוד מידע לגביו למטרות מתחום זה, בהינתן הקושי לפרט מראש על מטרות המערכת ותוצריה ועל סוגי המידע שבהם ייעשה שימוש לצורך אותן מטרות.

מכאן עולה מתח נוסף, לעניין העמידה בדרישה הבסיסית בדיני הגנת הפרטיות שלא לעבד מידע מעבר לנדרש למימוש המטרה, בהתאם לעקרון מזעור המידע (data minimisation). על כך ציין פרופ' מיכאל בירנהק כי "כאשר מפעילי המערכת מבקשים ממנה לאתר דפוסים והקשרים שהעין האנושית לא מזהה, **קשה לומר יותר מאשר 'אנחנו מבקשים מידע כדי ללמוד על הלא נודע'**. בלי לדעת מהי בדיוק המטרה, אי אפשר לבחון האם המידע שנאסף מספיק, או חורג מהדרוש".¹⁵⁶

אתגרים אלה ואחרים שנעמוד עליהם בפרק זה, במפגש שבין המאפיינים המובנים של מערכות בינה מלאכותית לבין כללים ועקרונות יסוד בדיני הגנת הפרטיות הם במידה רבה רוחביים, ומשותפים לתחומי תוכן ומגזרים שונים, מעבר למגזר הפיננסי. עם זאת, בהמשך להמלצה במסמך המדיניות להסדיר פיתוח ושימוש בבינה מלאכותית על בסיס ענפי, בשלב זה ועם הקמתו של הצוות הבין-משרדי לבחינת השימוש בבינה מלאכותית בסקטור הפיננסי, סברנו שנכון לערוך את הניתוח המשפטי בסוגיה מרכזית ורוחבית זו כבר עתה ובכך לייצר תמונה מלאה בכל הנוגע לפיתוח

* פרק זה נכתב על ידי ע"ד לירון מאוטנר-לוגסי ועו"ד שירה גרטנברג מיינעץ וחקיקה (ציבורי-חוקתי).

154 עמיר כהנא ותהילה שוורץ אלטשולר **אדם, מכונה, מדינה: לקראת אסדרה של בינה מלאכותית** 53 (המכון הישראלי לדמוקרטיה, 2023).

155 למאפיין זה ישנן משמעויות גם מבחינת הסיכון להפליה על ידי מערכות אלו, שעשויות לעשות שימוש בנתוני "פרוקסי" שאינם מפלים כשלעצמם, אולם יש להם קורלציה משמעותית עם משתנים מפלים. ראו בהרחבה פרק הטיה ואפליה.

156 מיכאל בירנהק "פרטיות ובינה מלאכותית" משפט חברה ותרבות ח 139-175 (2025), בעמ' 163. https://law.tau.ac.il/sites/law.tau.ac.il/files/media_server/law_heb/Law_Society_Culture/books/AI/6Michael%20Birnhack.pdf (להלן: **בירנהק "פרטיות ובינה מלאכותית"**).

ושימוש בבינה מלאכותית במגזר הפיננסי וכן להניח את התשתית המשפטית גם עבור תחומי תוכן ומגזרים אחרים.

בהקשר של שימושים פיננסיים במערכות בינה מלאכותית, נקדים ונציין כי בחוק הגנת הפרטיות בנוסחו לאחר תיקון 12 לחוק, מסווג מידע על נתוני שכר של אדם ועל פעילותו הפיננסית כמידע בעל רגישות מיוחדת.¹⁵⁷ כך גם מידע שחלה עליו סודיות שנקבעה בדין מוגדר בחוק כמידע בעל רגישות מיוחדת.¹⁵⁸ מסיווג זה נגזרות משמעויות שונות לפי חוק הגנת הפרטיות, המשקפות הגנה מוגברת על מידע מסוג זה, נוכח רגישותו, ובין היתר הוא בא לידי ביטוי בהוראות לגבי חובת הודעה לרשות להגנת הפרטיות על מאגרי מידע גדולים בהם מידע מצוי על רגישות מיוחדת וחובת מינוי ממונה על הגנת הפרטיות, החלה על מי שמעבד מידע שכזה בהיקף ניכר, העיצומים הכספיים המוטלים בגין הפרות החוק, הדרישות בתחום אבטחת המידע ועוד.

בפרק זה נעמוד על אתגרים מרכזיים במפגש בין ההגנה על הזכות לפרטיות ועל מידע אישי בישראל לבין מאפייני מערכות הבינה המלאכותית, בשלבים השונים של חיי המערכת. חלק מן האתגרים היו קיימים עוד קודם לעלייתן של טכנולוגיות הבינה המלאכותית, ורק מועצמים על ידם, וחלקם נובעים מן המאפיינים המיוחדים של טכנולוגיות אלו. במסגרת זאת יוצעו גם המלצות להמשך בחינה של הנושא, באופן כללי ובהתייחס בפרט למגזר הפיננסי.

כפי שמפורט בהרחבה בדוח זה, השימוש בבינה מלאכותית (AI) מעורר שאלות חברתיות ואתיות. בעולם מתפתחות גישות שונות להתמודד עם שימושים פוגעניים ותרמישי קיצון הנוגעים לבינה מלאכותית ובכלל זה מניפולציה קוגניטיבית לרבות ניצול חולשות, הטיות, שימושים פולשניים המאיימים על האוטונומיה ובכבוד האדם ועוד.¹⁵⁹

אחת הדרכים להתמודד עם הסיכונים שנמנו לעיל היא להפעיל מנגנונים משפטיים קיימים, ובשלב זה הדברים עלולים להתנתק לעקרונות מדיני הפרטיות כגון עקרונות הסכמה מדעת, בחינת היסק סביר וסוגיית החריגה מציפייה סבירה של נושא המידע. זאת הן בשל היעדרה של מסגרת רגולטורית אחרת והן מאחר שכלים אלו מבוססים על איסוף, ניתוח ועיבוד של מידע אישי בהיקפים חסרי תקדים, ומאחר שיש להם קשר הדוק באיבוד השליטה של אדם ביחס לשימוש שיעשה במידע שלו.

לעמדת הצוות, דיני הגנת הפרטיות לא יכולים או אמורים לתת מענה לכל האתגרים הנובעים מעיבוד מידע אישי לשם פיתוח מערכות בינה מלאכותית ובעת השימוש בהן. על כן, הצוות סבור כי לצד ההתמודדות עם אתגרים אלה בתחום הפיננסי באמצעות הרגולציה הפיננסית, יש מקום לבחון מחדש את הצורך ביצירת מסגרות משפטיות שיתמודדו עמם באופן רוחבי וייעודי עם האתגרים האמורים, לצד דיני הגנת הפרטיות ותוך השלמתם או דיוקם ככל שיעלה בכך הצורך. מענה כזה יאפשר להתאים את המענה המשפטי והרגולטורי לאתגרים באופן אפקטיבי וממוקד.

סקירת עיקרי ההסדרים הרלוונטיים בדיני הגנת הפרטיות בישראל

הזכות לפרטיות הוכרה כזכות יסוד בעלת מעמד חוקתי ועוגנה בסעיף 7 לחוק יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו". חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") קובע עוולות ועבירות הקשורות בפגיעה בפרטיות של אדם והוראות המסדירות עיבוד מידע אישי במאגרי מידע.

דיני הגנת הפרטיות או הגנת המידע האישי ("Data Protection") בישראל, כמו בעולם, נוגעים **למידע אישי** שעובר עיבוד. על פי ההגדרה העדכנית בחוק הגנת הפרטיות, "מידע אישי" הוא "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזוהה כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי".

עקרונות הגנת המידע לא חלים על מידע אנונימי – מידע שלא נוגע לאדם מזוהה או ניתן לזיהוי או מידע אשר לאחר שבוצעו בו פעולות מסוימות לא ניתן יותר לזהות את האדם באמצעותו.

מן ההבחנה בין מידע אישי למידע שהוא לא מידע אישי, נגזרת תחולת הוראות חוק הגנת הפרטיות ותקנותיו (וגם הוראות ה-GDPR – הרגולציה של האיחוד האירופי העוסקת בעיבוד מידע אישי), ובין היתר ההסדרים הנוגעים למצבים שבהם ניתן לעבד מידע אישי, המגבלות והעקרונות החלים על עיבוד כאמור, וזכויות **נושא המידע**, היינו: הפרט שהמידע האישי נוגע אליו או שאפשר לזהותו באמצעות המידע האישי.

157 פרט (10) להגדרת מידע בעל רגישות מיוחדת.

158 פרט (11) להגדרת מידע בעל רגישות מיוחדת.

159 Chapter III, ה"ש 11 לעיל.

במסגרת תיקון 13 לחוק,¹⁶⁰ נקבעו ועודכנו הגדרות מהותיות בחוק – "מידע אישי", "בעל שליטה במאגר מידע", "עיבוד"¹⁶¹ והוגדרו גם סוגי מידע אישי בעלי "רגישות מיוחדת", בהרמוניזציה לסטנדרטים בינלאומיים של הגנה על מידע אישי, ובפרט ל-GDPR. לצד עדכונים אלו, נוסף לחוק פרק ייעודי של עבירות פליליות במאגרי מידע, עוגנו והורחבו סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות והוקנתה לה סמכות להטיל עיצומים כספיים וסנקציות מנהליות נוספות בגין הפרות החוק וכן בגין אי עמידה בדרישות אבטחת המידע המעוגנות בסעיף 17 לחוק ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, שהותקנו מכוחו (להלן: "**תקנות אבטחת מידע**") ובגין הפרת תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), תשפ"ג-2023 (להלן: "**תקנות הגישור**"). עוד נקבעה חובת מינוי ממונה על הגנת הפרטיות בגופים רבים ובהם בנקים וחברות ביטוח.¹⁶²

תקנות אבטחת מידע, שנכנסו לתוקף במהלך שנת 2018, מהוות נדבך חשוב נוסף בדיני הגנת מידע אישי בישראל. "אבטחת מידע" מוגדרת בחוק הגנת הפרטיות כ"הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד, ללא רשות כדין".¹⁶³ התקנות קובעות הסדר מקיף ומפורט לעניין ההגנה על מאגרי מידע, ולגבי סדרי הניהול וכללי האבטחה במאגרי מידע והן חלות על מאגרי מידע של גופים ציבוריים ופרטיים כאחד. התקנות מגדירות מהי רמת האבטחה החלה על כל מאגר מידע, ומטרתן להחיל חובות קונקרטיות בתחום אבטחת המידע בארגונים במטרה להגן על פרטיות המידע במאגר ועל זכויות נושאי המידע מפני שימוש לרעה במידע אודותיהם, הן על ידי גורמים מחוץ לארגון והן על ידי עובדי הארגון.

האחריות לאבטחת המידע שבמאגר המידע נקבעה בסעיף 17(א) לחוק, לפיו "בעל שליטה במאגר מידע ומחזיק במאגר מידע", כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע". בנוסף, בסעיף 17 לחוק זה נקבעה חובת מינוי ממונה אבטחת מידע בגופים שונים ובהם בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.¹⁶⁴ גם ממונה אבטחת המידע נושא אחריות אישית לאבטחת המידע שבמאגר.

ע"פ החוק, לצד ההסדרים בדיון הישראלי, במסגרת הניתוח שיובא להלן, נתייחס באופן ממוקד גם להסדרים הקבועים ב-GDPR (שחלקם הוזכרו גם בפרקים נוספים בדוח זה). ה-GDPR מהווה נקודת ייחוס ומקור השראה מרכזי לרגולציה בתחום הפרטיות והגנת מידע אישי, כסטנדרט בינלאומי, ולאור מעמד התאימות (Adequacy) של ישראל לסטנדרט זה, אשר אושר בינואר 2024. בנוסף, לצד תיקון 13 לחוק הגנת הפרטיות שנכנס לתוקפו באוגוסט 2025, משרד המשפטים מתכוון לקדם תיקון נוסף לחוק, הכולל שורה של הסדרים מהותיים חדשים, המיועדים בין השאר להביא להרמוניזציה עם ההסדרים הקבועים ב-GDPR וברגולציית מידע אישי מתקדמת בעולם. זאת, כחלק מהשלמת התהליך שהחל למעשה בחקיקת תקנות הגישור, אשר חלות החל מינואר 2025 גם על מידע אישי על ישראלים, המצוי באותו מאגר מידע יחד עם מידע שהתקבל מהאזור הכלכלי האירופי, ונמשך בחקיקת תיקון 13.¹⁶⁵

פרטיות והגנת מידע אישי במערכות בינה מלאכותית – אתגרים והמלצות

כאמור בפתח הדברים, המפגש בין הפיתוח והשימוש במערכות בינה מלאכותית לבין דיני הגנת הפרטיות והמידע האישי מעורר אתגרים ומתחים רבים, הנובעים מהמאפיינים של מערכות אלו, הן בשלב הפיתוח והאימון והן בשלבי הפעלת המערכת, דיוקה, ותוצרי פעולתה. אתגרים אלה אינם ייחודיים לשימוש במערכות בינה מלאכותית במגזר הפיננסי, אולם יש להתייחס במסגרת הבחינה לרגישותו של המידע הפיננסי, לחובות הסודיות החלות עליו, וכן לחובות תום הלב או ההגינות החלות במערכות יחסים בין נותני שירותים במגזר זה לצרכנים, הרלוונטיות למשל בעת בחינת דרישת ההסכמה ויישומם של כללים אחרים, כמפורט להלן.

160 ס"ח תשפ"ד מס' 3287 מיום 14.8.2024 עמ' 1430.

161 בעל שליטה במאגר מידע הוגדר "מי שקובע, לברור או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר מידע"; "עיבוד", "שימוש" הוגדרו "כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו, או מתן גישה אליו (סעיף 3 לחוק הגנת הפרטיות).

162 סעיף 17ב(א)(4) לחוק.

163 סעיף 3 לחוק. "שלמות המידע" מוגדרת בסעיף כ"זאות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששוננו, נמסרו או הושמדו ללא רשות כדין". ראו גם סעיף 5(f) ל-GDPR וכן סעיף 32.

164 סעיף 17ב(א)(3) לחוק. וראו גם סעיף 17ב(א)(1), ולפיו חייבים במינוי ממונה אבטחת מידע גם בעל שליטה במאגר החייב ברישום או בהודעה לפי סעיף 8 לחוק, או מחזיק בחמישה מאגרי מידע כאמור. חובת מינוי ממונה אבטחת מידע קיימת גם בהסדרים פרטניים בחקיקה, ראו למשל סעיף 29א(ג) לחוק מרשם האוכלוסין.

165 כאמור, בהחלטת נציבות האיחוד האירופי מינואר 2024 אושרר מעמד התאימות (Adequacy) של ישראל בתחום הגנת הפרטיות, **כאן**. אחד הצעדים המשמעותיים שננקטו כדי להביא לאשרור ההכרה בישראל כמדינה בעלת מעמד תאימות, היה חקיקתן של תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023. תקנות אלו נועדו להבטיח את שימור מעמד התאימות שנבחן אותה עת, באמצעות קביעת חובות נוספות על גופים ישראלים שמקבלים מידע מאירופה. במהלך הליך אישור התקנות בכנסת, החליטה ועדת החוקה כי התקנות יחולו גם על מידע "ישראלי" המצוי באותו מאגר מידע יחד עם מידע שהתקבל מהאזור הכלכלי האירופי, על כל המשתמע מכך מבחינת החובות המהותיות הקבועות בתקנות אלו.



כעמדה עקרונית נציין כי הדין בנושא הגנת הפרטיות והמידע האישי בישראל הוא דין קיים, ניטרלי טכנולוגית, והוא חל, ככלל, על גופים ציבוריים ופרטיים כאחד.¹⁶⁶ נקודת המוצא לענייננו היא כי דיני הגנת הפרטיות חלים גם כאשר השימוש במידע הוא במערכות בינה מלאכותית,¹⁶⁷ לרבות ההתייחסות למידע פיננסי וההסדרים הפרטניים החלים עליו.

לצד זאת, אין חולק כי כניסתן של מערכות הבינה המלאכותית מציפה אתגרים ומתחים לגבי יישום דיני הגנת הפרטיות, ואכן בדוחות שונים של ארגונים בינלאומיים ומדינות שבחנו היבטים של הבינה המלאכותית עולה סוגיית הפרטיות כמעט בכלום.¹⁶⁸ מחקרים עדכניים מראים כי גם בקרב הציבור הרחב, נושא הפרטיות וההגנה על המידע הוא סוגיה מרכזית לצורך מתן אמון במערכות בינה מלאכותית.¹⁶⁹

בשלב בו אנו נמצאים, בו הטכנולוגיה של מערכות בינה מלאכותית ממשיכה להתפתח והשימושים האפשריים, התועלות והסיכונים הנשקפים מהם עוד נלמדים במקביל, וכך גם מתפתחת ההתמודדות בעולם עם סיכונים אלה, נציע בפרק זה להתמקד במספר אתגרים מרכזיים, שאינם ייחודיים לישראל ומתעוררים גם בעולם. נציע המלצות וכיווני חשיבה לאתגרים אלה, שמבטאים ניסיון לאזן באופן זהיר בין השיקולים הרלוונטיים בשים לב לכיווני אסדרה מסתמנים בעולם.

א. אתגר ההבחנה בין מידע אישי למידע אנונימי

כאמור, דיני הגנת הפרטיות חלים על מידע אישי, כלומר מידע שנוגע לאדם מזוהה או לאדם הניתן לזיהוי במאמץ סביר, במישרין או בעקיפין. אם לא ניתן לזהות את האדם אליו המידע נוגע – המידע נחשב למידע אנונימי, לא מזוהה – ודיני הגנת הפרטיות לא חלים עליו.

אם כן, סיווג מידע כמידע אישי הוא זה ש"פותח את הדלת" לתחולת דיני הגנת הפרטיות, בין היתר בעניין המצבים שבהם ניתן לעבד באופן חוקי מידע אישי, הוראות הנוגעות לעיבוד המידע וזכויות נושאי המידע.

כיצד בוחנים אם המידע ניתן לזיהוי? חוק הגנת הפרטיות קובע כי מידע אישי הוא נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי במאמץ סביר, במישרין או בעקיפין. עוד קודם להגדרה החדשה של מידע אישי בחקיקת תיקון 13 לחוק, פורש המבחן בפסיקת בית המשפט העליון בעניין **גוטסמן**, שם נקבע כי דרישת הזיהוי מתקיימת מקום שבו אדם סביר יכול לקשור בין מידע לבין אדם ספציפי, וכי גם מידע שמוצג בצורה אנונימית לכאורה עלול לבסס קשר לאדם ספציפי אם ניתן לקשור בין המידע לאדם באמצעים אחרים, בדרך של "הנדסה חוזרת".¹⁷⁰ בעקבות עדכון הגדרת מידע אישי בחוק, יש ליישם פסיקה זו בראי המבחן שנקבע בחוק עצמו, כמפורט לעיל. מבחן זה הולם גם את התפיסה המקובלת ברגולציה בעולם, ובכלל זאת את הגדרת מידע אישי בסעיף 4(1) ל-GDPR. בהערות המבוא ל-GDPR (recitals) צוין כי השאלה האם ניתן לזהות אדם במאמץ סביר תיבחן בהתבסס על שיקולים אובייקטיביים, ובהם עלויות והזמן הנדרש לזיהוי, בהתחשב בטכנולוגיות הזמינות בזמן העיבוד, וההתפתחויות הטכנולוגיות.¹⁷¹

הפיכת מידע אישי למידע אנונימי, המכונה גם "התממה" או "אנונימיזציה" נעשית באמצעות הסרת מרכיבים מזיהוי מהמידע האישי, בדרכים שונות המפחיתות את הסיכון לזיהוי או לחשיפה של מידע מזוהה, כגון: הַצְרָפָה (אגרגציה, צירוף נתונים), הפחתת הדיוק של נתונים באמצעות שימוש בטווח במקום בערך ייחודי, השמטת פרטים, הרעשה (הוספה או הפחתה של ערך לנתונים) וכדומה.

166 על גופים ציבוריים חלים במסגרת חוק הגנת הפרטיות הסדרים פרטניים נוספים (ראו למשל ביחס לחובת רישום מאגרי מידע, סעיף 8 לחוק). זאת, בנוסף לכללי המשפט המינהלי והמשפט החוקתי המחייבים אותם.

167 יצוין כי הרשות להגנת הפרטיות פרסמה טיוטת הנחייה לעניין תחולת חוק הגנת הפרטיות על מערכות בינה מלאכותית (2025) – https://www.gov.il/he/pages/ai_reg

168 מיכאל בירנהק "פרטיות ובינה מלאכותית" משפט חברה ותרבות ח (2025), עמ' 142 ה"ש 17 במאמר.

169 ראו למשל מחקר רחב היקף שערכה אוניברסיטת קווינסלנד באוסטרליה בשנת 2023 בקרב 17,000 משתתפים מ-17 מדינות, אשר דירגו את נושא הפרטיות במידע ואבטחתו כנושא ראשון במעלה לשם פיתוח מערכות המימנות של בינה מלאכותית. עמ' 42 לדוח ממציא הסקר, אשר זמין כאן.

170 ע"א 1697/11 א. גוטסמן **אדריכלות בע"מ נ' ורדי**, פס' 18, 21-22 (23.1.2013). ברע"א 7828/17 **הסתדרות מדיצינית הדסה נ' פלוני**, פס' 14 (9.1.2018). נקבע כי "במקרה כזה, בו הציבור שנחשף למידע הרפואי אינו יכול לקשור בין המידע המוצג לבין אדם ספציפי, פרטיותו של אותו אדם אינה נפגעת, שכן ללא האפשרות להצביע על זהות המטופל, איש לא חודר למרחב האישי שלו. המידע הרפואי נותר תלוש מהקשר ובלתי-קונקרטי, ומשכך הצגתו אינה מפירה את החיסיון הרפואי או את זכותו של המטופל לפרטיות". וראו גם פסק דינו של בית המשפט המחוזי בעת"ם (מינהליים ת"א) 28857-06-17 **עמותת חברות הסיעוד נ' משרד הביטחון**, פס' 16.4 לפסק דינה של כב' השופטת אגמון-גונן (1.7.2019) (להלן: "עניין עמותת חברות הסיעוד").

עוד ראו בהקשר זה עמדת היועץ המשפטי לממשלה שהוגשה בת"צ 22141-03-15 **גרינברג נ' סלקום ישראל בע"מ**, פס' 40, 46 (יוער כי באותו מקרה אושר הסדר פשרה מתוקן שהגישו הצדדים, חרף התנגדות היועץ המשפטי לממשלה, אולם בית המשפט לא הכריע בשאלה האם באותו מקרה היה ניתן לזהות את המנויים באמצעות המידע (סעיפים 79.4-79.5 לפסק הדין מיום 5.3.2020).

171 GDPR, recital 26

"פסאודו-אנונימיזציה" (תכונה להלן: **קידוד**), כוללת הפרדה בין הנתונים המזהים לנתונים לא מזהים, באמצעות מפתח שנשמר בצורה נפרדת, וכפוף לאמצעים טכניים וארגוניים המגבילים את הגישה למפתח (במקום הפרטים המזהים הנתונים משויכים לקוד מסוים, כך שנשמר מתאם בין המאפיינים). שיטה זו מפחיתה את הסיכון לחשיפה של מידע אישי, אך לא מאיינת את האפשרות להביא לזיהוי האדם, ולכן לא הופכת את המידע לאנונימי ולא מוציאות אותו מתחולת דיני הגנת הפרטיות.

פעולות התממה שונות מביאות לרמת שונות של סיכון לזהות מחדש את המידע עם אדם ספציפי. כך למשל, על פי ה-GDPR, מידע שעבר קידוד (פסאודו-אנונימיזציה) עדיין נחשב למידע אישי, שכן עדיין ניתן לייחסו לאדם מזהה (באמצעות המפתח המאפשר התאמה בין המאפיינים האישיים לאלה שלא).¹⁷² אנונימיזציה מלאה היא זו שאינה מאפשרת עוד זיהוי מחדש של נושא המידע.

חוק הגנת הפרטיות לא מתייחס במישור להתממה כאמצעי להפחית את הסיכון לפגיעה בפרטיות (למעט התייחסות מסוימת בתקנות הגישור, שחלות גם על מידע של ישראלים אם הוא נמצא במאגר מידע שהתקבל מהאזור הכלכלי האירופי).¹⁷³ אולם ניתן למצוא ביטוי לאפשרות זו בחקיקה המסדירה שימוש במידע אישי לצרכי מחקר, כך, בהתייחס למידע רפואי, סעיף 20(א)(7) לחוק זכויות החולה, התשנ"ו-1996 מתיר מסירת מידע רפואי, בלא הסכמת המטופל, למטרות מחקר **ובלבד שלא נחשפו פרטים מזהים של המטופל**.¹⁷⁴ סעיף 23(1) לחוק מידע גנטי, התשס"א-2000 קובע כי ניתן למסור מידע גנטי למטרות מחקר שאושר בדין, הוראה או פרסום בביטאון מדעי אם המידע הגנטי מועבר **"בלא כל פרט מזהה"**. גם אם הנבדק נותן הסכמה בכתב למסירת המידע, הפרסום לא יכלול חשיפת כל פרט מזהה שלו אלא אם הוא נתן לכך הסכמתו המפורשת, מראש ובכתב.¹⁷⁵

בהתייחס לתחום הפיננסי, **חוק נתוני אשראי, התשע"ו-2016** נועד בין היתר ליצור בסיס מידע לא מזהה שישמש את בנק ישראל לשם ביצוע תפקידיו¹⁷⁶ וכולל הסדר מפורט לעניין השימושים במידע הלא מזהה, אבטחת המידע, וכן איסור על ביצוע כל פעולה לאיתור זהות של לקוח על בסיס מידע לא מזהה שמקורו במאגר שהוקם בחוק.¹⁷⁷ גם **חוק שירות מידע פיננסי, התשפ"ב-2021** קובע כי נותן שירות מידע פיננסי רשאי לעשות שימוש במידע פיננסי שאסף או קיבל גם למטרות סטטיסטיות הקשורות למתן שירות מידע פיננסי לכלל לקוחותיו, ובלבד שניתנה לכך הסכמה מפורשת ובכתב על ידי הלקוח, ושהמידע שיוצג ללקוחות **יהיה מידע סטטיסטי מצרפי שהוא מידע לא מזהה**.¹⁷⁸

בעולם הדיגיטלי, טכנולוגיות הבינה המלאכותית וכלים של סטטיסטיקה חישובית מגבירים את יכולת הזיהוי מחדש או הזיהוי החוזר (Re-identification) של מידע שהוא לכאורה אנונימי או מידע שעבר על פניו התממה מלאה. כלים אלה מאפשרים קישור בין מידע לא מזהה לפרטים רלוונטיים שמאפשרים זיהוי, על בסיס שימוש בנתוני עתק. תהליך הזיהוי מחדש מבוסס בדרך כלל על קורלציות סטטיסטיות בין מידע לא מזהה לבין מידע אישי זמין לגבי אותו אדם.

אתגר הזיהוי מחדש אמנם אינו ייחודי לטכנולוגיות הבינה המלאכותית ולמעשה היה קיים בהתייחס לכלים שאוספים נתוני עתק ממקורות שונים, מנתחים אותם ועורכים הצלבות ביניהם.¹⁷⁹ עם זאת, עלייתן והתפתחותן של מערכות

172 שם.

173 תקנה 3(ג) לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי (תשפ"ג-2023) להלן: "תקנות הגישור"), הקובעת את חובתו של בעל שליטה במאגר מידע למחוק מידע לבקשת נושא המידע במקרים מסוימים. מקום שנושא המידע ביקש מחיקה כאמור בתקנה, ולא התקיימו החריגים המנויים בתקנה 3(ב) – על בעל השליטה למחוק את המידע שבשליטתו או לבצע פעולות המבטיחות שלא יתאפשר, באמצעים סבירים, לזהות את נושא המידע. כך גם בתקנה 4 המסדירה את חובותיו של בעל שליטה במאגר להבטיח כי במאגר לא מוחזק מידע שאינו נחוץ עוד למטרה לשמה נאסף או הוחזק, או למטרה אחרת לשמה מותר להחזיקו ולמחוק את המידע הלא נחוץ. צוין כי החובה כאמור לא תחול אם בוצעו לגבי המידע האמור פעולות המבטיחות שלא יתאפשר באמצעים סבירים לזהות את נושא המידע (תקנה 4(ג)).

174 וראו גם סעיף 20(ב) לחוק זה, המורה באופן כללי כי מסירת המידע הרפואי לפי סעיף 20(א), המסדיר עוד מקרים בהם נמסר מידע רפואי אף ללא הסכמת המטופל, לא תיעשה אלא במידה הנדרשת לצורך העניין ותוך הימנעות מרבית מחשיפת זהותו של המטופל.

175 סעיף 23(2) לחוק מידע גנטי.

176 סעיף 1(א)(4) לחוק נתוני אשראי. חוק נתוני אשראי מגדיר בסעיף 2 מידע מזהה "מידע הכולל פרט מזהה של לקוח, או מידע שפרטים מזהים של לקוח הופרדו ממנו אך ניתן במאמץ סביר לזהות את הלקוח שאליה מתייחס המידע". "מידע לא מזהה" מוגדר כמידע על לקוח שאינו מידע מזהה.

177 ראו סעיפים 16(ב)(3)-(4) לחוק זה המסדירים את מטרות מאגר המידע הלא מזהה; סעיפים 44-45 המסדירים את השימוש במידע לא מזהה ומתן הגישה אליו (והנתנים לכך). כן ראו סעיף 58(ב) לגבי איסור זיהוי חוזר של מידע לא מזהה וההסדר לגבי אבטחת המידע במאגר, המורה בין היתר כי בנק ישראל יאסוף ישמור ויאסוף את המידע בדרך שתבטיח כי המידע הלא מזהה נשמר ונמסר ככזה (סעיף 60(א)(4)), וראו גם סעיפים 60(ב)-(ג).

178 סעיף 25(ד)(2) לחוק שירות מידע פיננסי, וסעיף 27(ד) לחוק זה. עוד ראו ההסדר הנוגע למחקר על ידי הלשכה המרכזית לסטטיסטיקה, בסעיף 17(ב) לפקודת הסטטיסטיקה [נוסח חדש], התשל"ב-1972 קובע כי מידע אישי שנאסף מהסוגים המפורטים בסעיף "לא יפורסמו באופן שאפשר לזהות למי הן נוגעות".

179 ראו עת"מ (מינהליים ת"א) 17-06-28857 עמותת חברות הסינום נ' משרד הביטחון (1.7.2019): בעידן של מידע עתק או נתוני עתק, קיים חשש כי חשיפת נתונים "תמימים" לכאורה כגון מיקום, תביא בסופו של יום לפגיעה בליבת הפרטיות". ראו גם עומר טנא "הסתכל בקנקן וראה מה יש בו:

הבינה המלאכותית מביאות לשדרוג נוסף של היכולת לבצע זיהוי מחדש של מידע אנונימי.¹⁸⁰ מערכות בינה מלאכותית מאפשרות לאתר דפוסים לא צפויים על בסיס ניתוח נתוני העתק, ובדרך זו יכולת הזיהוי החוזר של פרטים לא מזוהים מתעצמת ומתרחבת.¹⁸¹ לכך יש להוסיף את המוטיבציה ההולכת וגדלה בעת פיתוח טכנולוגיות של בינה מלאכותית להרחיב את בסיס המידע האישי לצורך אימון של המערכות ופיתוח האלגוריתמים והפיכתם למדויקים ומשוכללים ככל הניתן. ככל שרמת ההתממה וההכללה של הנתונים גבוהה יותר, הדבר עלול להפחית את יעילות השימוש במידע. לאתגר ההתממה בעת הנוכחית התייחסה, באופן כללי, גם רשות הסחר האמריקאית, ה-FTC (Federal Trade Commission), בגילוי דעת מחדש יולי 2022 לגבי שימוש ושיתוף לא חוקיים במידע אישי רגיש. בין היתר צוין שם כי טענות שמידע הוא "אנונימי" או עבר התממה עלולות להטעות צרכנים, שכן מחקר מקיף מראה שמידע מותמם יכול לעבור לעתים קרובות זיהוי חוזר.¹⁸²

גם באנגליה פרסמה נציבות הגנת המידע, ה-ICO (Information Commissioner's Officer) טיוטה של מדריך בנושא התממה, התממה חלקית וטכנולוגיות מגבירות פרטיות (PET) שבו הוצעו קווים מנחים להערכת הסיכון לזיהוי מחדש, בהתחשב בשיקולים שונים: רגישות המידע שמבקשים להתמים, נסיבות החשיפה של המידע, היקף החשיפה (למשל אם מדובר בהנגשתו לציבור או בהעברתו לגורם מוגדר), האם קיים מידע נוסף שיכול לאפשר זיהוי וזמינות, השימוש במידע לאחר ההתממה וכן הטכנולוגיות הזמינות לזיהוי חוזר והתפתחות. עוד צוין כי ההערכה לגבי סיכון הזיהוי מחדש צריכה להיבחן באופן תקופתי, בהתאם לטכנולוגיות הזמינות או למידע הציבורי הנגיש בתחומים מסוימים.¹⁸³

בצרפת, נציבות הגנת המידע וחירויות דיגיטליות (CNIL) פרסמה מדריך על אנונימיזציה של מידע אישי ובו בין היתר תיאור ופירוט של שיטות התממה שונות, והתוויה של בניית הליך התממה.¹⁸⁴ במדריך זה הוצעו שלושה קריטריונים שעמידה בהם משמעה שהמידע אכן מותמם: אינדיווידואליזציה, קורלציה והיסק. אינדיווידואליזציה משמעה כי לא יהיה אפשרי לבדוד אדם באופן פרטני מבסיס הנתונים. קורלציה דורשת כי לא יהיה ניתן לקשר מידע לאדם באמצעות קישור לנתונים אחרים שכוללים את אותו מידע, לצד מידע מזהה עליו (למשל מאגר של כתובות לא יוכל להיחשב אנונימי אם קיים מאגר כלשהו שמכיל את הכתובות עם נתונים אחרים המאפשרים זיהוי של הפרטים שגרים בכתובות). לפי דרישת ההיסק, לא ניתן יהיה להסיק ממידע מותמם מידע חדש על אדם (כך למשל, אם תוצאות סקר מפורסמות בחתכים ברזולוציה גבוהה מאוד, באופן המאפשר לגלות מידע על אנשים פרטניים באמצעותו, למשל נתוני התחסנות לפי בניין).

מקום שאין עמידה בשלושת הקריטריונים האמורים, לפי המדריך הצרפתי, בעל שליטה במידע שמעוניין להשתמש במידע מותמם צריך להוכיח, באמצעות הערכה מעמיקה של הסיכונים לזיהוי חוזר, שהסיכון לזיהוי חוזר באמצעים

נתוני תקשורת ומידע אישי במאה העשרים ואחת" **רשת משפטית: משפט וטכנולוגיות מידע** 287, 301 (ניבה אלקין קורן ומיכאל בירנהק עורכים, 2011).

180 ראו גם ההתייחסות בפרק הפרטיות במסמך המדיניות, עמ' 79-80.

181 Karl Manheim & Lyric Kaplan, Artificial intelligence: Risks to Privacy & Democracy, 21 Yale J.L. & Tech. 106, 127-129 (2019); Yves-Alexandre de Montjoye, et al., Unique in the shopping mall: On the Reidentifiability of Credit Card Metadata, 347 Sci. 536 (2015). בירנהק "פרטיות ובינה מלאכותית", בעמ' 21; אבנר לוי "הפרטיות בעידן הטכנולוגיות המתפרצות" **טכנולוגיות מתפרצות: אתגרים בדין הישראלי** 215, 222-223 (ליאור זמר, דב גרינבאום ואביב גאון עורכים, 2022): "למעשה, מתקיים כיום מרוץ חימוש בין טכנולוגיות אנונימיזציה לעיבוד נתונים המאפשר שיום מחדש וההנחה היא שכל טכנולוגיות נתוני עתק ובינה מלאכותית יתקדמו, תהפוך אנונימיזציה (השומרת עדיין על שימושיות כלשהי של המידע) – לבלתי אפשרית". עוד ראו מחקר שנערך לבקשת מרכז המחקר של הפרלמנט האירופי לגבי השפעת ההסדרים ב-GDPR על בינה מלאכותית, Giovanni Sartor, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence" 36-37 (2020) (להלן: **מחקר הפרלמנט האירופי**).

ראו גם גילוי דעת מקדים של הוועדה המייעצת לוועדת האתיקה הארצית של לשכת עורכי הדין בעניין שימוש בבינה מלאכותית בעבודת עורכי הדין (7.5.2024). בקישור **כאן**. בגילוי הדעת צוין בין היתר כי על עורך הדין להימנע מהזנת מידע סודי כלשהו של לקוח ולהפעיל שיקול דעת פרטני על מנת למנוע חשיפה של מידע אישי של הלקוח שאינו מצוי בידעית הרבים. לעניין זה צוין "יש לזכור כי עקומת הלמידה של מערכות אלו היא מהירה ומתוחכמת מאין כמוה. משכך יש לחשוש מצב עתידי בו גם השמטת פרטים מזהים, תוך הותרת מקבץ "פרטים שוליים" בטקסט המעובד על ידי פלטפורמת בינה מלאכותית, יוצלב בידי הפלטפורמה ויעובד בצורות שונות תוך גילוי זהות הלקוח ו/או סודותיו" (ראו סעיפים 14-15 לגילוי הדעת).

182 <https://www.presidency.ucsb.edu/documents/white-house-press-release-location-health-and-other-sensitive-information-ftc-committed>. ראו גם התייחסותה העדכנית של ה-FTC מחדש יולי 2024 לטכניקת "hashing" (כאחת השיטות להתממה חלקית) לפיה מידע שעבר את התהליך עדיין לא נחשב לאנונימי ולא ניתן להציגו ככזה, נוכח היכולת לזהותו עם אדם ספציפי מחדש: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous#ftn_10.

183 מיום 16.6.23 ICO – Privacy-enhancing technologies (PETs). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies> יתכן ובמסמך יערכו שינויים לאור כניסתו הצפויה לתוקף של (DUA) Act 2025 (Data Use and Access).

184 ראו (19.5.2020) CNIL "Anonymization of Personal Data" (זמין **כאן**).

סבירים הוא זעיר. גם ההנחיות בצרפת מתייחסות לכך שפעולות ההתממה והערכת הסיכון לזיהוי חוזר צריכות להתבסס על **בקרה תקופתית** נוכח התפתחותן של שיטות ההתממה, לצד השיטות לביצוע זיהוי חוזר. על הבקרה האמורה להתחשב הן באמצעים הטכנולוגיים הזמינים, והן במקורות מידע אחרים שיכולים לאפשר זיהוי של מידע שהיה אנונימי.

נוסף לאלה יש לציין את הדו"ח שפרסם ה-OECD בנושא **טכנולוגיות מגבירות פרטיות**, אשר מתאר את ההתפתחויות האחרונות בתחום ואת סוגי הטכנולוגיות המרכזיות הקיימות היום לצד הערכה של האפקטיביות שלהן.¹⁸⁵ טכנולוגיות מגבירות פרטיות (PETs – Privacy Enhancing Technologies) הוא מונח גג שמתייחס לטכנולוגיות דיגיטליות, גישות וכלים שנועדו להגן על סודיות המידע, ובמקרים מסוימים גם על האוטנטיות שלו והגישה אליו, במטרה להגן על פרטיות נושאי המידע לצד אינטרסים מסחריים של בעלי שליטה במידע (ולכן המונח PETs רחב יותר מהתממה). בדו"ח צוין כי טכנולוגיות אלו, באופן טיפוסי אינן עומדות לבדן, ויש לראות בהן כלים לצד צעדים ארגוניים ומשפטיים אחרים לשם הגנה על פרטיות ומידע אישי.¹⁸⁶

הרשות להגנת הפרטיות פרסמה גם היא בשנת 2025 מדריך לטכנולוגיות מגבירות פרטיות (PETs – Privacy Enhancing Technologies), בו סקרה בהרחבה סוגים שונים של טכנולוגיות קיימות ושיטות בתחום זה, תוך התייחסות ליתרונות ולחסרונות של כל אחת מן הטכנולוגיות.¹⁸⁷

על רקע האמור, דומה שהחלוקה בין מידע אישי, שעליו חלים דיני הגנת הפרטיות, לבין מידע לא מזוהה, שאינו כפוף להם, נעשית פחות מובחנת במסגרת השימוש במערכות בינה מלאכותית, ועלולה להביא לסיכונים לא מבוטלים לפרטיות ולהגנת מידע אישי בעקבות זיהוי חוזר של מידע לא מזוהה לכאורה. כך גם פעולת ההתממה של מידע אישי כפתרון אפשרי המתיר את השימוש במידע, בפרט לצורך פיתוח ואימון של מערכות בינה מלאכותית, היא לא פתרון "בינארי" המבטיח הגנה מוחלטת על מידע אישי ועל פרטיותם של נושאי המידע. בצד האמור, ברי כי לפעולת ההתממה יתרונות משמעותיים בהגנה על הפרטיות של נושאי המידע, במיוחד מקום שהמידע לא נאסף בהסכמתם. היא מאפשרת לצמצם את הפגיעה בפרטיות כתוצאה משימוש במידע תוך שימור התועלות בעיבוד מידע – בין היתר לשיפור איכות החיים, מחקרה, לקידום חדשנות וכו'.

תוצאה שלפיה אין משמעות לפעולות התממה נוכח הסיכון ההולך וגובר במציאות הטכנולוגית הנוכחית לזיהוי חוזר של המידע היא תוצאה לא רצויה שעלולה לתמרץ גופים שלא להשקיע משאבים בשיטות התממה. כמו כן, ניתן לומר שלצד ההתפתחות הטכנולוגית ביכולת הזיהוי החוזר, עם התמריצים הנכונים, יכולה להיות גם התפתחות של טכנולוגיות מגבירות פרטיות ושיטות התממה חדשות שיכולות לצמצם את הסיכון לזיהוי חוזר.

לפיכך יש לעודד פיתוח שיטות התממה מידע כדי לשפר את יכולת ההתמודדות שלהן עם הסיכון לזיהוי חוזר וכן לעודד מפתחי ומשתמשי מערכות בינה מלאכותית המבקשים להתבסס על מידע מותמם להשתמש בשיטות התממה שנחשבות מקובלות ומתקדמות, להפחתת הסיכון של זיהוי חוזר.

במסגרת הערות הציבור לדוח הביניים עלה חשש מפני עלויות ויצירת חסם בהתפתחות הטכנולוגיה אם תינקט גישה מחמירה ביחס להתממה. טענה נוספת בהקשר זה היתה כי ספק אם לגופים המפוקחים עצמם, להבדיל ממפתחי מערכות הבינה המלאכותית, יש כלים מתאימים לבחון את יעילות ההתממה. בהמשך לכך, הוער על-ידי גורם אחד כי יש מקום להבהיר את הציפיות הרגולטוריות בעניין אמות מידה להתממה, באופן מתואם עם הרשות להגנת הפרטיות, תוך התייחסות לכלים נוספים מלבד התממה. מנגד, גורם אחר המליץ להסתפק בהכוונת הגופים הפיננסיים להיות ערים לסיכון ולנהלו. עוד הוצע להבהיר כי דרישת ההתממה חלה רק במקרים של שיתוף מידע עם צד שלישי ולא במקרים של שימוש פנימי, וכן כי אין מקום להטיל חובות מרובות על מידע מותמם המשמש לאימון של מודלים.

ההתלבטות העולה מהערות אלה נוגעת לסוגיה שעלתה גם בהקשרים אחרים, והיא מידת המעורבות הרגולטורית הנדרשת בהיבטים שונים של בינה מלאכותית, כאשר היו מעירים שצידדו במעורבות רגולטורית (לשם הגנה חזקה יותר על אינטרסים מוגנים או לשם הגברת הוודאות הרגולטורית) והיו מעירים שקראו להימנע ממעורבות רגולטורית (לשם מניעת הגבלות שלא לצורך והותרת שיקול דעת רב יותר בידי הגופים המפוקחים). הצוות בדעה כי לנוכח חשיבות ההתממה כאמצעי להגנת הפרטיות, ההמלצות שהוצעו בהקשר זה הן מאוזנות ויכולות לסייע לאפקטיביות

185 OECD, "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351 p. 14–26 (2023) (זמין כאן).

186 ראו שם, בעמ' 13.

187 הרשות להגנת פרטיות "מדריך לטכנולוגיות מגבירות פרטיות" (2025). https://www.gov.il/he/pages/guide_enhancing_technologies.



ההתממה ולהגברת הוודאות הרגולטורית. כמו כן, בעקבות ההערות הובהר כי בכל הנוגע לטיב ההסכמה הנדרשת או ליכולת להוכיח בדיעבד את קיומן של אחת מההגנות לפי סעיף 18 לחוק, למשל לצורך עיבוד מידע אישי לצורך פיתוח מודל, יש לתת משקל לשימוש בשיטות התממה מקובלות ומתקדמות, יחד עם נקיטת אמצעים נוספים למניעת סיכון של זיהוי חוזר וזליגת מידע אישי. זאת לצד בחינה של נסיבות נוספות כמו מטרת עיבוד המידע, רמת רגישות המידע, ציפייתו הסבירה של נושא המידע לגבי מה יעשה במידע שלו ועוד.



המלצות בנוגע לאתגר ההבחנה בין מידע אישי למידע אנונימי:

1. מוצע כי הרגולטורים הפיננסיים, בהתייעצות עם הרשות להגנת הפרטיות, ישקלו להכווין את הגורמים המפוקחים לבצע הערכת סיכונים ביחס לסיכון לזיהוי חוזר של מידע אישי¹⁸⁸ בטרם השימוש במידע מותמם, לכל אורך חיי המערכת המבוססת בינה מלאכותית – למשל באמצעות הנחיות, גילויי דעת והבהרות פרשניות. ככל שמקור המידע לאימון המערכת או לשימוש בה הוא בגוף הפיננסי, האחריות על הערכת הסיכון לזיהוי חוזר חלה על הגוף הפיננסי המפוקח. תהליך זה צריך לערב תחומי ידע שונים ובכלל זה התחום המשפטי ותחום אבטחת המידע.

א. ניתן לקבוע קריטריונים או להבנות את שיקול הדעת בביצוע הערכת הסיכון ובין היתר: סוג המידע שמבקשים להתמים ורגישותו, היקף המידע הנדרש ומה הרזולוציה הנדרשת עבור כל שדה מידע, נסיבות החשיפה של המידע (היקף וסוג הגורמים הנגישים למידע, השימוש המיועד בו לאחר ההתממה), עלותו ומורכבותו של הזיהוי החוזר, מידת הסיכון לזיהוי חוזר בהינתן מאגרי מידע זמינים לציבור, מאפייני שיטת ההתממה הספציפית והמענה שהיא נותנת לסיכון של זיהוי חוזר ושיטות ההתממה הזמינות.¹⁸⁹

ב. שימוש בכלים ארגוניים וחוזיים לצד כלים טכנולוגיים על מנת להתמודד עם הסיכון של זיהוי מחדש, כגון הגבלת הרשאות וטכנולוגיות נוספות מגבירות פרטיות. ככל שמידע מותמם מועבר לצדדים שלישיים – לכלול התחייבות הסכמית שלא לעשות במידע שימוש לשם זיהוי חוזר, לצד אמצעים לפקח על הפרות של התחייבות זו.¹⁹⁰

ג. עקב התפתחויות טכנולוגיות ואחרות הן של יכולות ההתממה, והן של יכולות הזיהוי החוזר (בין היתר על רקע הרחבת מאגרי המידע הנוצרים והמפורסמים לציבור והיכולת להצליבם עם מידע קיים נוסף), יש להתייחס **לבקרה תקופתית** על שיטות ההתממה הזמינות ולהעריך בהתאם את הכלים להפחתת הסיכון לזיהוי מחדש.¹⁹¹

ד. מוצע לשקול לכלול בהערכת הסיכונים תכנית פעולה למקרה של חשיפת המידע, קרי: זיהוי מחדש. תכנית זו יכולה לכלול למשל את האמצעים שבהם יעודכנו הנפגעים על חשיפת המידע ואיזה סיוע יוצע להם.¹⁹²

2. על רקע הקושי לבצע התממה "מוחלטת" ולאור העובדה שהמידע שמוחזק במערכת הפיננסית הוא מידע בעל רגישות מיוחדת, מוצע להכווין גורמים מפוקחים לנקוט אמצעים של אבטחת מידע גם על מידע מותמם.

188 ראו הצעה ברוח הדברים גם אצל דן חי "פרטיות וטכנולוגיה בישראל" **טכנולוגיות מתפרצות: אתגרים בדיון הישראלי** 241, 277 (ליאור זמר, דב גרינבאום ואביב גאון, עורכים, 2022). ראו גם עומר טנא "הסתכל בקנקן וראה מה יש בו: נתוני תקשורת ומידע אישי במאה העשרים ואחת" רשת משפטית: משפט וטכנולוגיות מידע 287, 301 (ניבה אלקין קורן ומיכאל בירנהק עורכים, 2011), בעמ' 319.

189 ראו טיוטת מדיניות של ה-ICO בנושא זה, Draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies guidance, 13-14 (October 2021). קישור זמין כאן.

190 Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for 21 (October 2012). Businesses and Policymakers 21 (2012). זמין כאן.

ראו גם שרון בר-זיו וטל ז'רסקי "פרטיות במשבר זהות: אסטרטגיות הסדרה בעידן ההתממה" **משפט חברה ותרבות** ב' 125, 141 (מיכאל בירנהק עורך, 2019) (להלן: "בר-זיו וז'רסקי").

191 שם, בעמ' 142. ראו גם טיוטת המדיניות של ה-ICO, Draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies guidance 13-14 (October 2021), <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2023/12/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/>. ראו גם המדריך של CNIL, Anonymization of Personal Data (19.5.2020), <https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles>.

192 בר-זיו וז'רסקי, "פרטיות במשבר זהות: אסטרטגיות הסדרה בעידן ההתממה" **משפט חברה ותרבות** ב' 125, 141 (מיכאל בירנהק עורך, 2019), בעמ' 142. ראו גם בסעיף 34 ל-GDPR.

3. בבואם של הרגולטורים לבחון שימוש בשיטת התממה פרטנית ככלי להפחתת סיכון לזיהוי מחדש על ידי גורמים מפקחים, מוצע לבחון את השיטות בהשוואה לאלו המקובלות בשווקים מפותחים בעולם, ובפרט בתחום הפיננסי. מומלץ להתייעץ עם הרשות להגנת הפרטיות, באשר לשיטות הנחשבות מקובלות ומתקדמות והמענה שהן יכולות לתת מפני הסיכון לזיהוי מחדש. כאמור, הרשות להגנת הפרטיות פרסמה מדריך לטכנולוגיות מגבירות פרטיות PETs שיכול לסייע בידי הרגולטורים הפיננסיים וציבור המפקחים.¹⁹³

4. בכל הנוגע לטיב ההסכמה הנדרשת או ליכולת להוכיח בדיעבד את קיומן של אחת מההגנות לפי סעיף 18 לחוק, למשל לצורך עיבוד מידע אישי לצורך פיתוח מודל, יש לתת משקל לשימוש בשיטות התממה מקובלות ומתקדמות, יחד עם נקיטת אמצעים נוספים למניעת סיכון של זיהוי חוזר וזליגת מידע אישי. זאת לצד בחינה של נסיבות נוספות כמו מטרת עיבוד המידע, רמת רגישות המידע, ציפיותו הסבירה של נושא המידע לגבי מה יעשה במידע שלו ועוד.¹⁹⁴

ב. אתגר ההסכמה מדעת לעיבוד מידע במערכות מבוססות בינה מלאכותית

חוק הגנת הפרטיות קובע כי לא ניתן לפגוע בפרטיותו של אדם, אלא בהסכמתו או מכוח הסכמה בחוק.¹⁹⁵ כפועל יוצא מהאמור, בישראל רוב עיבוד המידע האישי שכתוב בפגיעה בפרטיות, שלא על-ידי רשויות ציבוריות, מתבסס על הסכמה של נושא המידע, או בהסתמך על ההגנות הקבועות בסעיף 18 לחוק.¹⁹⁶ ההסכמה צריכה להיות "הסכמה מדעת"¹⁹⁷ ובכלל זאת, היא צריכה להינתן ביחס לכל הפעולות שהגורם האוסף את המידע מבקש לעשות במידע, ובין היתר לשימושים שיעשו במידע והעברתו לצדדים שלישיים.¹⁹⁸ בהמשך לכך, בהתאם לעקרון צמידות המטרה, לא ניתן לעשות שימוש במידע אישי בניגוד למטרה לשמה נמסר המידע, אלא בהסכמת נושא המידע.

הסכמתו של אדם נתפסת כאמצעי שמסיר את הפסול מפגיעה בפרטיותו, באופן המבטא את התפיסה של "פרטיות כשליטה" – הפרטיות כביטוי לאוטונומיה של האדם להחליט איזה מידע ייחשף לגביו, למי, מתי ואיך, אם בכלל. תפיסה זו מדגישה לא רק את החלטת האדם בקשר למידע אודותיו, אלא שיש בידיו את האפשרות להחליט ולבחור מה יעשה באותו מידע.¹⁹⁹ לפיכך, כאשר מתקיימת הסכמה מדעת של נושא המידע, וכל עוד הפעולות המבוצעות במידע תואמות את ההסכמה, אין מדובר בפגיעה אסורה בפרטיות.

ביטוי מעשי הנוגע לדרישת ההסכמה מדעת נמצא בסעיף 11 לחוק, הקובע חובת יידוע של אדם בעת פניה לקבל מידע אישי על אודותיו. חובה זו נועדה להבטיח את יכולת נושאי המידע לשלוט במידע לגביהם, ועל השימושים

193 לעניין זה נציין גם את ההסדר בסעיף 2ט17 לחוק הגנת הפרטיות, שנוסף בתיקון 13 האחרון, המעגן את מנגנון הפניה המקדמית לרשות להגנת הפרטיות בעניין עמידת מאגר המידע בדרישות החוק או ההוראות לפיו.

194 למען הסר ספק, מובהר שלפי הדין הקיים, ביצוע התממה שאיננה מבטיחה שאין אפשרות לזיהוי הלקוח במאמץ סביר, במישרין או בעקיפין – לא מוציאה את הנתונים מגדר "מידע אישי".

195 ראו סעיף 1 לחוק הקובע: "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו", וסעיף 35 (סעיף שמירת הדינים).

196 ביחס לרשויות ציבוריות, עיבוד מידע אישי לא יכול להסתמך על ההגנות הקבועות בסעיף 18 לחוק כמקור סמכות למדיניות הכרוכה בפגיעה בפרטיות, ראו פסק הדין ברע"א 2558/16 פלונית נ' קצין התגמולים משרד הביטחון, פס' 59 (5.11.2017).

נקודת המוצא ברגולציה של האיחוד האירופי, ה-GDPR בעניין זה היא שונה, ולפיה כל עיבוד מידע אישי טעון עילה חוקית מבוססת, מבין העילות המנויות ב-GDPR, המכונות "בסיסי עיבוד" (סעיף 6 ל-GDPR). שניים מבסיסי העיבוד מבוססים על הסכמת נושא המידע – האחד על הסכמת נושא המידע לעיבוד מידע למטרה ספציפית, והשני כאשר העיבוד חיוני לביצוע הסכם שנושא המידע הוא צד לו.

197 סעיף 3 לחוק הגנת הפרטיות מגדיר הסכמה כ"הסכמה מדעת, במפורש או מכללא". המילה "מדעת" נוספה לדרישת ההסכמה שבחוק בתיקון משנת 2007. התיקון נועד להבטיח כי ההסכמה הניתנת לפגיעה בפרטיות, תהיה הסכמה מודעת, היינו: שבידי האדם המסכים לפגיעה יהיה מידע, "הדרוש לו, באורח סביר, כדי להחליט האם להסכים או לא, והמידע יימסר לו בצורה מובנת" (דברי ההסבר להצעת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ו-2005, ה"ח הממשלה 230).

במסגרת התיקון הנוסף לחוק הגנת הפרטיות שמשרד המשפטים שוקל לקדם יש כוונה לחזק בין היתר את הדרישות שיאפשרו התבססות על הסכמת האדם כבסיס חוקי לעיבוד מידע אודותיו, לצד הוספה של בסיסים חוקיים נוספים לעיבוד המידע.

198 מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה 100 (להלן: "בירנהק מרחב פרטי"); ראו גם ת"א (מחוזי ו-ם) 3213/09 פלונית נ' פלוני, פס' 58 לפסק דינה של כב' השופטת כנפי שטייניץ (11.10.2011). בערעור על פסק הדין אישר בית המשפט העליון את מסקנת בית המשפט המחוזי לפיה לא התקיימה הסכמה לפגיעה בפרטיות באותו מקרה, ראו ע"א 8954/11 פלוני נ' פלונית, פס' 160 לפסק דינו של כב' השופט סולברג (22.5.2014) (להלן: עניין פלונית).

199 מיכאל בירנהק פרטיות חוקתית 89-90 (2023). ראו גם ת"צ 21-04-25669 אביב נ' Facebook (9.7.2025), פסקה 61 להחלטה. עוד ראו טיוטת גילוי הדעת של הרשות להגנת הפרטיות בנושא הסכמה בדיני הגנת הפרטיות (2025). <https://www.gov.il/he/pages/consent2025>.

הנעשים בו.²⁰⁰ בנוסף, בחלק מהמקרים קיימים הסדרים חוקיים או רגולטוריים נוספים בנוגע לאופן יישום חובת היידוע בהקשר ספציפי או על ידי גורמים ספציפיים (כמו בנקים).²⁰¹

נוכח מרכזיותה של ההסכמה כאמור, יש לבחון את מערכת היחסים שבה היא ניתנת. חלק מההסכמות, "חשודות מטבען" נוכח יחסי הכוחות והנסיבות שבהן ניתנת ההסכמה, והדבר יכול להשפיע על ההסתמכות על ההסכמה ככזו שמרפאת את הפגיעה בפרטיות. הסכמות "חשודות" יכולות להיות כאלו הניתנות במערכת יחסים בין צדדים המצויים בפערי כוחות ברורים,²⁰² או כאשר ההסכמה היא תנאי לקבלת שירות חיוני, ובפרט כאשר אין קשר בין המידע או השימוש המיועד למידע לבין השירות החיוני. במקרים אלה, אל מול האפשרות להסכים לפגיעה בפרטיות אין אלטרנטיבה של ממש,²⁰³ ולכן יש קושי להסיק שההסכמה משקפת בחירה אמיתית של האדם וביטוי לשליטתו על המידע אודותיו.²⁰⁴

סוגיה אחרונה זו נדונה גם **בהקשר הפיננסי** בבקשת היועץ המשפטי לממשלה לבטל ולשנות תנאים מקפחים בהסכם התנאים הכלליים לפתיחת חשבון עובר ושב של בנק לאומי. בית הדין לחוזים אחידים פסק כי התנאי שנכלל בהסכם לפתיחת חשבון, שכלל ויתור גורף על חובת הסודיות הבנקאית כלפי חברות הקשורות לתאגיד הבנקאי הוא תנאי מקפח בחוזה אחיד, בין היתר נוכח הכריכה בין ההסכמה האמורה לבין פתיחת החשבון ונוכח העדר האפשרות ללקוח לתת אישור פרטני להעברת מידע למטרה מסוימת לצורך קבלת שירות מסוים, וכך נקבע:²⁰⁵

"שיקול נוסף שהזכיר הבנק בהקשר זה נעוץ בצורך להעביר מידע הנדרש, למשל, לחברות כרטיסי אשראי או בהעברת מידע המתבצעת בין הבנק לבין חברות ליסינג או העברת מידע לשם חיקור לקוח לקביעת מסגרת אשראי. בכל המקרים הללו העברת המידע נועדה לקדם אינטרס של הלקוח. על-כן הלקוח יוכל לתת אישור ספציפי להעברת מידע למטרה מסוימת לגוף זה או אחר. בכך אין להכשיר הסכמה כוללת וגורפת להעברת המידע מראש.

...אולם, כאן הבנק מתנה את פתיחת החשבון בויתור מראש על חובת הסודיות כלפי החברות הקשורות לתאגיד הבנקאי. התנאה כזאת אינה הוגנת ומקפחת את הלקוחות. אם הלקוח יזקק לאשראי או לכל שירות אחר מחברות הקשורות לתאגיד הבנקאי, ואם מצבו הכספי של הלקוח רלוונטי למתן השירות המבוקש, כי אז יוכלו נותני אותם שירותים להתנות את מתן השירותים בויתור על סודיות הבנקאית. בכך לא יהיה כל דופי. אלא שבמקרה שלפנינו נדרש וויתור גורף ומראש על הסודיות הבנקאית, כתנאי לפתיחת חשבון. התנאה כזו אינה נדרשת, ויש בה משום התנאה על חובה שהבנק חב על-פי הדין ללקוחו, מה שמקים חזקת קיפוח על-פי סעיף 4(6) לחוק החוזים האחידים."

יועץ, מעבר למצבים שבהם כאמור ההסכמה "חשודה מטבעה", ומעלה ספק אם היא משקפת את רצונו החופשי

200 לפי הסעיף, פניה לאדם לקבל מידע או עיבודו במאגר מידע צריכה להיות מלווה בהודעה שתכלול את הפרטים הבאים: אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, ומהי תוצאת אי ההסכמה; את המטרה לשמה מבוקש המידע; שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עמו; למי יימסר המידע ומטרות המסירה; וכן קיומן של זכות עיון במידע אישי והזכות לבקש תיקונו (לפי סעיפים 13 ו-14 לחוק, בהתאמה).

201 או למשל סעיף 33 לחוק נתוני אשראי שקובע חובת יידוע של לקוח (מראש ובאופן מפורש) מקום שבו נותן אשראי מתכוון לבקש מלשכת אשראי לקבל חיווי אשראי וכן על כך שלשם קבלת החיווי כאמור, לשכת האשראי תגיש לבנק ישראל בקשה לקבלת נתוני האשראי לגביו הכלולים במאגר. ראו התייחסות בעמדת הרשות להגנת הפרטיות "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (18.7.2022) (המסמך זמין כאן).

202 למשל: המדינה מול אזרח, תאגיד גדול מול צרכן בודד, מעסיק מול עובד. בירנהק "מרחב פרטי", מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה עמ' 253 (2010), בעמ' 253. ראו גם עמדת היועץ המשפטי לממשלה שהוגשה בת"צ 22141-03-15 גרינברג נ' סלקום ישראל בע"מ (5.3.2020), פס' 54-58. ראו בג"ץ 8298/22 הסיגוריה הציבורית נ' היועצת המשפטית לממשלה (31.8.2025), פסקה 42 לפסק הדין, כמו גם בג"ץ 70206-12-14 האח הקטן בע"מ נ' הכנסת (5.10.2025), פסקה 8 לפסק הדין.

203 ראו גם להלן הערת המבוא ל-GDPR ביחס להסכמה הניתנת מרצון חופשי.

204 כך למשל בעבר, הותנתה קבלת דמי אבטלה ברישום באמצעות מסירת טביעת אצבע. האגודה לזכויות האזרח פנתה וביקשה לאפשר אפיקים חלופיים ובהמשך לפנייה זו הובהר כי הלשכה תאפשר למי שחפץ בכך להמשיך ולהתייצב לפני פקיד. ראו פירוש אצל מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה 100 (2010), בעמ' 104-105, 253-254.

ההסכמה הנדרשת לעיבוד מידע אישי על פי ה-GDPR היא הסכמה חופשית, ספציפית ומדעת, שמהווה אינדיקציה חד משמעית לרצונו של נושא המידע ושניתנת בהצהרה או בפעולה ברורה להסכים לעיבוד מידע אישי לגביו (ראו ההגדרה בסעיף 4(11) ל-GDPR). על מנת להבטיח שההסכמה ניתנת מרצון חופשי, היא לא יכולה לשמש בסיס חוקי לעיבוד מידע על פי ה-GDPR במקרים שבהם: קיים חוסר איוון ברור בין נושא המידע ובין בעל השליטה (ובפרט כאשר בעל השליטה הוא רשות ציבורית); כאשר לא מתאפשרת הסכמה לפעולות עיבוד שונות במידע האישי, למרות שניתן להפרידן; או כאשר ביצוע החוזה ובכלל זאת מתן שירות, תלוי בהסכמה לעיבוד המידע למרות שהיא אינה חיונית לביצועו (Recital 32)

205 ע"ש (י-ם) 195/97 היועץ המשפטי לממשלה נ' בנק לאומי, פס' 281-282 (2004). בערעור שהוגש על פסק הדין (ע"א 6916/04) עניין זה לא נדון.



של נושא המידע, הסביבה הדיגיטלית מגלה, באופן כללי, אתגרים נוספים בהתבססות על הסכמה כמקור חוקי לעיבוד מידע אישי, בשל הספק האם הסכמתו של נושא המידע היא אמנם **מדעת**. זו האחרונה מתאפיינת בעיבוד מידע בהיקף נרחב, ובפעולות עיבוד מורכבות ומשוכללות, באופן המעלה ספק אם לנושאי המידע יש את הידע או הכישורים להבין את הפרטים הנמסרים להם על עיבוד המידע ואת הסיכונים שכרוכים בו.

ההודעה הנלווית לפנייה לנושאי המידע בסביבה הדיגיטלית על מנת לקבל את הסכמתם לעיבוד המידע ולמטרות העיבוד מיתרגמת לרוב ל"מדיניות פרטיות" – טופס ממוחשב אשר **מקשה על האפשרות להעניק הסכמה אמיתית ו"מדעת", למצער באופן מספק. בעת שימוש יומיומי רגיל באתרים וביישומונים, אדם נדרש לבחון ולהסכים למסמכי מדיניות רבים וארוכים, המתעדכנים לעתים קרובות, ושנוקטים, בדרך כלל שפה משפטית ולא נגישה. הכרה בהקשה על התיבה "אני מסכים" על ידי הפרט בנסיבות אלו ככזו המבטאת הסכמה מדעת, מעוררת אפוא קושי, באופן המציב אתגר משמעותי להגשמת התכלית היסודית של דרישת ההסכמה ומנגנון היידוע הנלווה לה, של מימוש השליטה של נושא המידע במידע אודותיו והשימוש שנעשה בו.**²⁰⁶

בכל הנוגע לאתגר ההסכמה מדעת בהקשר של מערכות בינה מלאכותית באופן פרטני – כפי שתואר בהרחבה בפרק "קופסה שחורה" והסברתיות, אחד המאפיינים המייחדים חלק ממערכות הבינה המלאכותית הוא פעילותן ככלל "קופסה שחורה", כלומר, באופן שלא מאפשר להתחקות אחר האופן בו התקבלו תוצרי המערכת. באותו פרק נערכת הבחנה בין הסברתיות **כללית**, המתייחסת למאפייני המערכת ואופן פעולתה (המכונה לעיתים גם שקיפות), לבין הסברתיות **פרטנית** המתייחסת להסבר ביחס לאופן שבו התקבלה החלטה ספציפית.

המאפיין האמור של מערכות בינה מלאכותית משפיע גם על יישום דרישת ההסכמה כתנאי לעיבוד מידע אישי הכרוך בפגיעה בפרטיות. על הקשיים שעליהם עמדנו בהסתמכות על הסכמה לעיבוד מידע בסביבה הדיגיטלית, מועמס אפוא אתגר משמעותי נוסף שעניינו במגבלה הקשורה ביכולת להציג לפרט מהן מטרות השימוש במידע האישי שלו, אילו פעולות יעשו במידע ובאיזה מידע אודותיו יעשה שימוש לצורך אותן מטרות.

נראה כי קושי זה יכול להיות יותר משמעותי דווקא בהתייחס לפניה לקבלת מידע שאינה לצורך שימוש במערכת בינה מלאכותית קיימת לשם קבלת החלטה פרטנית, שאז למצער קיימת אפשרות להציג לנושא המידע באופן ברור ומפורט את מטרות שימוש המידע, באילו נתונים ייעשה שימוש, ומהן הפעולות שייעשו בהם.

להבדיל, בפנייה לקבלת מידע אישי לצורך פיתוח מערכות בינה מלאכותית, או אימון שלהן, נראה שדווקא הנדבכים של ההסברתיות ה**כללית** הם הרלוונטיים, ובעיקר כאמור מידע על אופן פעולת מערכת הבינה המלאכותית ומטרותיה (אשר בשלב זה הן לא בהכרח ידועות או ברורות למפתח או לגוף שבכוונתו להשתמש במערכת), ההיגיון שבבסיסה, הנתונים בהם יעשה שימוש והשיקולים המשמשים בקבלת החלטות. לכך יש להוסיף, כי מדובר בטכנולוגיה חדשה שההבנה של הציבור לגביה, ובמיוחד לגבי פוטנציאל השימושים השונים בה, עשויה להיות מוגבלת.

זאת ועוד, ההסכמה "קובלת" את אוסף המידע ביחס לשימושים המותרים במידע האישי בעוד שלעיתים מטרות השימוש ותוצרי המערכת – אינם בהכרח ידועים. לכן, למצער כאשר הפנייה לנושאי המידע לקבלת מידע אודותיהם נעשית לצורך **פיתוח** מערכות בינה מלאכותית, קיים קושי לפרט מעבר לרמה כללית יחסית, מהם השימושים שתעשה המערכת במידע.²⁰⁷

במסגרת עמדה שפורסמה מטעם הרשות להגנת הפרטיות בנושא חובת היידוע במסגרת איסוף ושימוש במידע אישי, ציינה הרשות בהתייחס לעיבוד באמצעות מערכות בינה מלאכותית כי על הפנייה לפי סעיף 11 לחוק הגנת הפרטיות לפרט על פעולת המערכות האמורות, ככל שהדבר רלוונטי לגיבוש ההסכמה, וככל שפירוט זה אפשרי מבחינה משפטית, טכנולוגית ומסחרית (אבחנה שגם נדונה בפרק העוסק ב"קופסה שחורה" והסברתיות). עוד המליצה הרשות כי יוסבר לנושא המידע על פרטי המידע שבהם עשויות המערכות להשתמש בנוגע אליו, והמקור של פרטי מידע אלו.²⁰⁸ בהמשך לדברים אלו צוין כי "אין באמור במסמך זה בכדי לומר כי חובת היידוע מחייבת לחשוף את כלל הפרטים והנתונים הנוגעים לאיסוף ולשימוש במידע אישי. יתכנו מצבים בהם חשיפה שכזו תהיה בלתי אפשרית או מנוגדת לתכליות חוקיות או לאינטרסים לגיטימיים אחרים. **במצבים שכאלו על הגורם המבקש לאזן**

206 ראו בהרחבה מיכאל בירנהק "פרטיות ובינה מלאכותית", בעמ' 160-159. בירנהק מביא במאמרו דוגמאות למחקרים אמפיריים שמצאו שמדיניות הפרטיות הלכה למעשה לא משיגה את מטרותיה ליידע את נושא המידע באופן מספק, כי משתמשים רבים בטוחים שהכותרת "מדיניות פרטיות" משקפת הגנה על פרטיותם באתר בו הם גולשים, ולא היא; כי המדיניות הנפוצה נועדה לנצל קשיים קוגניטיביים של המשתמשים; וכי קריאת מסמכי מדיניות הפרטיות באתרים שונים תיארך בממוצע 201 שעות בשנה.

207 שם, בעמ' 18. וראו הדוגמאות המובאות שם על דוגמאות למדיניות פרטיות הכוללות התייחסות כללית ביותר לשימושי בינה מלאכותית.

208 ראו עמדת הרשות להגנת הפרטיות, חובת יידוע במסגרת איסוף ושימוש במידע אישי" (18.7.2022), בסעיף 24/ https://www.gov.il/he/pages/duty_to_notify

בין האינטרסים השונים. עליו לבחון כיצד הוא מספק לנושא המידע את הנתונים המרכזיים הנוגעים לאיסוף המידע והשימוש בו (כגון נתונים שבלעדיהם אין לנושא המידע אפשרות להעניק הסכמה מדעת לאיסוף), תוך הימנעות מחשיפת נתונים אותם אין באפשרותו לחשוף.

סוגיה נוספת שעולה אף היא בשלב השימוש במידע אישי לצורך פיתוח או אימון מערכות בינה מלאכותית נוגעת לשימוש בנתוני עבר, קרי בנתונים בנוגע ללקוחות קיימים או לקוחות קודמים, להחלטות שניתנו לגביהם במסגרת התקשרות למתן שירות שהסתיימה, או שלא כללה בשעתו הסכמה לפעולות עיבוד מידע לשם מטרות אימון או פיתוח יישומי בינה מלאכותית ("בעיית המלאי").

בעוד הדין הישראלי מתבסס על דרישת ההסכמה (או ההסמכה) כאשר יש פגיעה בפרטיות, ה-GDPR אוסר על כל פעולת עיבוד מידע אישי ללא בסיס עיבוד חוקי אך כולל בסיסי עיבוד נוספים. כך, לצד הסכמת נושא המידע לעיבוד המבוקש, ה-GDPR קובע בסיסי עיבוד נוספים המאפשרים עיבוד של מידע אישי באופן כללי, למעט לגבי "קטגוריות מיוחדות של מידע אישי" (שהן ככלל מקבילות להגדרה של "מידע בעל רגישות מיוחדת" בדין הישראלי) אותן אסור לעבד, אלא אם מתקיימת אחת מן הנסיבות המצמצמות המנויות ב-GDPR.²⁰⁹ לצד בסיסי העיבוד הנוספים, ה-GDPR קובע חובות נוספות החלות על בעל שליטה ומחזיק במאגר מידע וכן מעניק זכויות משמעותיות לנושאי מידע. נושא זה של הרחבת בסיסי העיבוד, לצד הטלת חובות וזכויות נוספות, בדומה ל-GDPR, נכלל במסגרת עבודת משרד המשפטים בגיבוש תיקון נוסף לחוק הגנת הפרטיות וזאת גם במנותק משאלת השימוש במערכות בינה מלאכותית. בנוסף, נוכח הקשיים והאתגרים שפורטו בהסתמכות על "הסכמה מדעת" כאשר עסקינן במערכות בינה מלאכותית, נדרשת מחשבה על בסיסים חוקיים נוספים לעיבוד מידע אישי לצרכי פיתוח ואימון מערכות בינה מלאכותית, שיאפשרו את התפתחות הטכנולוגיה מחד, אך יכללו מענה והגנות לנושאי המידע מאידך. בהקשר זה עלתה שאלה האם נכון יהיה להסתפק בבסיסי העיבוד הנוספים הקיימים ב-GDPR לצורך פיתוח מערכות בינה מלאכותית, שכן שימוש בבסיסי עיבוד אלה מורכב ומעורר שאלות אף בעולם.²¹⁰ לפיכך, הצוות ביקש לקבל את הערות הציבור לעניין זה ולעניין האם יש מקום לייצר בהקשר של בינה מלאכותית בסיס עיבוד ייעודי, לצד איזונים והגנות ייעודיות.

במסגרת הערות הציבור לדוח הביניים, הערות רבות התייחסו להבחנה בין הדין הישראלי לבין ה-GDPR בכל הנוגע לכך שבדין הישראלי הצורך בהסכמה או הסמכה רלוונטי רק למצב שבו יש פגיעה בפרטיות (ולא ביחס לכל עיבוד מידע) מחד, ומאידך, שבסיסי העיבוד ב-GDPR רבים יותר מאשר אלה שבדין הישראלי. עוד נטען באופן ספציפי בנוגע לאימון מודלים של בינה מלאכותית, כי דרישת ההסכמה אינה מתאימה, אינה נדרשת על פי הדין, וכי קביעת עקרון של חזרה מהסכמה הקיים ב-GDPR ללא בסיסי המידע האחרים הקיימים בו, תקשה מאוד על פיתוח ואימון מערכות בינה מלאכותית. בהמשך להערות ולשאלה בנושא זה שהפנה הצוות להערות הציבור, נוספה המלצה להרחיב את בסיסי העיבוד בדין הישראלי.

בנוגע להמלצות שביקשו לחזק את ההסכמה מדעת בדרישות ייחודיות שיחולו לגבי מערכות בינה מלאכותית, כגון ברירת מחדל של הסכמה במתכונת opt in, דרישה להסכמה מפורשת ובולטת, או מנגנון של הסכמה מדורגת, נטען כי אלה מוסיפות נדבכים לא מחויבים ומכבידים. רוב המעירים גרסו כי אין מקום לכללים ייחודיים בדבר הסכמה מדעת עבור שימוש בטכנולוגיות בינה מלאכותית. מנגד, היו מעירים שסברו כי השימוש במערכות בינה מלאכותית מעלה שאלות משמעותיות בנוגע ליכולת של נושאי מידע להבין ולהסכים לעיבוד מידע באופן מודע ומושכל וסברו שיש מקום לחזק את מנגנון ההסכמה מדעת. הצוות סבור כי לא נכון לומר בצורה גורפת כי שימוש בבינה מלאכותית זהה לשימוש בכל טכנולוגיה אחרת אלא שיש למערכות בינה מלאכותית מאפיינים מיוחדים שיכולים להצדיק התייחסות משפטית או אחרת מותאמת. עם זאת, המלצות הדוח לקחו בחשבון את ההערות שהתקבלו במטרה למקד את הנסיבות בהן אכן נדרשת הסכמה מדעת כאשר השימוש בבינה מלאכותית פוגע בפרטיות.

אחת השאלות שעלתה מצד מעירים לדוח הביניים היא יכולת השימוש של גופים פיננסיים בנתוני עבר שנמצאים

209 סעיפים 6 ו-9 ל-GDPR.

210 ראו למשל (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111). כך למשל בעניין OPEN AI התעוררה השאלה בדבר ההסתמכות על בסיס העיבוד שעניינו אינטרס לגיטימי של בעל השליטה, בין היתר נוכח ההוראות הנוספות ב-GDPR לגבי בסיסי העיבוד המותרים בקטגוריות מיוחדות של מידע (לפי סעיף 9(2) ל-GDPR) וכן על רקע השימוש בכריית מידע מאתרי אינטרנט (web scraping). ראו דוח ראשוני שפרסם ה-EDPB בנושא עמידת הטכנולוגיה ChatGPT בהוראות ה- (https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf) (23.5.2024). EDPB "Report of the work undertaken by the ChatGPT Taskforce". וכן חוות הדעת העדכנית של ה-EDPB מיום 17 במרץ 2024 (https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf).



בידיהם, במסגרת פעילות במערכות בינה מלאכותית. הדבר תלוי בין השאר בהיקף ההסכמה שניתנה לגוף הפיננסי בנוגע לאותו מידע. עמדתם היתה כי אין להסיק שעצם השימוש במערכת בינה מלאכותית מחייב בהכרח קבלת הסכמה מחדש מכל לקוח. לשם המחשה – אם חברת אשראי עשתה שימוש במידע על לקוחותיה במסגרת מודל חיתום אשראי, על בסיס הסכמת הלקוחות, לא בהכרח תתחייב קבלת הסכמה מחדש מהלקוחות לשם שימוש במערכת בינה מלאכותית לאותו צורך ממש. דרישה כאמור אינה מתחייבת מהדיון, אלא תלויה כאמור באופי ההסכמה שניתנה ובפעילות שמוצע לבצע. הצוות בחן את ההערה וערך שינויים בהמלצות הדוח בהיבט זה.



המלצות בנוגע לאתגר ההסכמה מדעת:

1. ככל שהפעילות שמוצע לבצע במערכות בינה מלאכותית היא בסיכון גבוה, שמטרות השימוש בה מורכבות יותר (פחות קלות להבנה מבחינת תוצאת עיבוד המידע או השלכותיה) או חורגות מציפייתו הסבירה של נושא המידע, כך יש מקום לנקוט במתכונת הסכמה מפורשת יותר כגון ברירת מחדל להסכמה במתכונת opt in או הסכמה שתתבקש באופן בולט.

אפשרות נוספת היא נקיטה במנגנוני "הסכמה מדורגת", כאמצעי מאזן לקושי למסור פירוט במסגרת חובת היידוע בשלב איסוף המידע ושיכול לשפר את אופן הלכוחות ביחס למסירת המידע, כגון:²¹¹

א. כאשר המטרה של עיבוד המידע באמצעות בינה מלאכותית אינה ידועה וכללית יותר בשלב האיסוף, לציון זאת במפורש.

ב. כאשר הדבר אפשרי, לנקוב במטרות פרטניות או שימושים פרטניים אפשריים של המערכת שנמצאת בפיתוח, באופן שיאפשר לנושא המידע לסמן מטרות/שימושים שהוא מסכים כי המידע האישי שלו יעובד עבורם.

2. התניית מתן שירות פיננסי במתן הסכמה לעיבוד מידע אישי לצורך פיתוח, אימון והפעלה של מערכת הבינה המלאכותית תהיה אפשרית, ובלבד שהפיתוח, האימון וההפעלה הוא של המערכת המשמשת למתן אותו שירות. ואולם, כאשר מדובר **בשירותים פיננסיים בסיסיים**, התניה כאמור תתאפשר רק כאשר היא נדרשת לצורך מתן השירות לנושא המידע באופן ספציפי.²¹²

3. ביחס לנתוני עבר ("בעיית המלאי"): הצורך בקבלת הסכמה מחודשת לשם שימוש במערכות בינה מלאכותית תלוי באופי ההסכמה שניתנה ובפעילות שמוצע לבצע, ואין להסיק כי עצם השימוש במערכת בינה מלאכותית מחייב בהכרח קבלת הסכמה מחדש מכל לקוח. ככל שהשימוש בבינה מלאכותית הוא לצורך אותה תכלית לשמה נמסר המידע מלכתחילה (למשל – כחלק ממתן השירות הפיננסי שהלקוח צורך) אזי לא תידרש הסכמה מחודשת אך בשל השימוש במערכות בינה מלאכותית לצורך אותה תכלית. עם זאת, ככל שהשימוש במערכות בינה מלאכותית נעשה תוך חריגה מהתכלית המקורית (למשל כאשר ניתנה הסכמה לעיבוד מידע לצורך מתן שירות פיננסי מסוים ונעשה בו שימוש לצורך אימון מודל כללי (general AI) או לצורך מתן שירות שונה מזה שהלקוח ביקש לצורך) הרי שתידרש הסכמה נפרדת לתכלית זו. גם כאשר השימוש במידע נעשה לאותה מטרה, אך אופן השימוש חורג מהותית מהצפיות הסבירות של הלקוח (לדוגמה שימוש בתמונה מתעודת הזהות של הלקוח לשם אימון אלגוריתם זיהוי פנים אוטומטי למטרות מניעת הונאות כלפי הבנק) – גם אז תידרש הסכמה נפרדת מהלקוח.

במקרה שנדרשת הסכמה מחודשת לצורך שימוש במידע על לקוחות קודמים או לקוחות קיימים שלא נתנו הסכמה לשימוש במידע לגביהם לצרכי פיתוח ואימון מערכות בינה מלאכותית –

(1) התממת המידע בכפוף להוראות הרגולטורים הפיננסיים בדבר הערכת הסיכון לזיהוי חוזר יכולה להוות פתרון אפשרי לרצון להשתמש במידע מחד, ולקושי ביצירת קשר לקבלת הסכמה מחודשת מהלקוחות, מאידך. היעדר דרישה להסכמה מחודשת תתאפשר במקרה שלא קיים סיכון סביר לזיהוי מחדש של המידע, בהתאם לקריטריונים ולשיקולים שתוארו מעלה (בצירוף נקיטת בקורות ארגוניות ומשפטיות מפצות כמו התחייבות משפטית של מקבלי המידע שלא לערוך זיהוי חוזר וכדו').

(2) מוצע לשקול כי הרגולטורים הפיננסיים, יחד עם הרשות להגנת הפרטיות, יבהירו את רף מתכונת הידוע או ההסכמה בנסיבות בהן בוצעו הליכי התממה מקובלות ומתקדמות לצד אמצעים נוספים אך עדיין יש סיכון לזיהוי חוזר הנמצא ברף הנמוך. כך למשל, בהתקיים התנאים האמורים, ניתן יהיה לשקול

211 ראו הצעתו של בירנהק "פרטיות ובינה מלאכותית", בעמ' 174, כמקובל בתחום המחקר הרפואי. עוד ראו Brent Daniel & Luciano Floridi, The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, 22 Sci. & Eng. Ethics 303, 312 (2016).

212 ראו בהקשר זה את הדיון שנערך לעיל בפרק המעורבות האנושית, ממנו עולה כי עשויות להיות בעתיד פעילויות לגביהן תתחייב העמדת חלופה אנושית. דרישה כאמור עשויה להשליך מטבע הדברים גם על דרישת הסכמה למסור המידע לצורך פיתוח ואימון מערכות בינה מלאכותית. אך כאמור, הצוות אינו סבור כי בעת הנוכחית יש מקום להטיל חובה גורפת של העמדת פעילות אנושית לצד פעילות הנעשית בידי מערכות בינה מלאכותית.



להסתפק בקבלת הסכמה לעיבוד המידע במתכונת של opt-out ובתנאים שייקבעו.

4. מוצע כי הרגולטורים הפיננסיים ישקלו לקבוע הוראות בדבר מתן זכות ללקוחות, נושאי המידע, לחזור בהם מהסכמה לעיבוד מידע אישי לשם פיתוח ואימון מערכת בינה מלאכותית, בנסיבות המתאימות, גם מעבר לאפשרות החזרה מהסכמה המוקנית להם לפי הדין הקיים. זכות זו היא חלק מהזכויות המוקנות היום לנושאי מידע ב-GDPR, ומשמעותה כי לא ניתן להמשיך לעבד את המידע האישי לצורך מטרות אלו בהסתמך על הסכמת נושא המידע שחזר בו מהסכמתו (חזרה מהסכמה אינה פוגעת בחוקיות פעולות עיבוד שבוצעו לפני ההודעה על החזרה מהסכמה). עוד לפי ה-GDPR, היידוע בדבר זכות החזרה מההסכמה צריך להיעשות טרם מתן ההסכמה ומימוש הזכות צריך להיות נגיש באותו אופן כמו מתן ההסכמה. יובהר כי אין הכוונה להטיל חובה לאימון מחודש של המודל ללא פרטי המידע על אודות נושא המידע שביקש לחזור בו מההסכמה אלא מגריעה של המידע על אודות אותו נושא מידע מבסיס הנתונים המשמש לאימון המודל כך שלא יעשה בו שימוש מאותו מועד והלאה.

5. בדומה להסדרים הקבועים ב-GDPR לפיהם תנאי לעיבוד מידע אישי, הוא קיומו של בסיס עיבוד מבין אלה המנויים ברגולציה, וזו כוללת בסיסים נוספים מעבר להסכמת נושא המידע, מוצע לקבוע בסיסים חוקיים נוספים לעיבוד מידע אישי לצרכי פיתוח ואימון מערכות בינה מלאכותית, שיאפשרו את התפתחות הטכנולוגיה מחד, אך יכללו מענה והגנות לנושאי המידע מאידך. מוצע לעשות כן בחקיקה, תוך בחינה האם נכון לייצר בהקשר של פיתוח מערכות בינה מלאכותית בסיס עיבוד ייעודי, לצד איזונים והגנות ייעודיות.²¹³

ג. אתגר התוצרים של מערכות בינה מלאכותית - מידע אישי מוסק (Inferred personal data):

מערכות בינה מלאכותית מרחיבות באופן משמעותי את היכולת להסיק מידע חדש על נושאי מידע, באמצעות הפעלת המודלים שלהן על מידע אישי. מערכות אלו לומדות ומעבדות נתוני עתק, ומכוונות למצוא דפוסי פעולה או קורלציות בלתי צפויות, או כאלו שלא היו נגישות קודם לכן לעין האנושית. באמצעות המודלים האמורים, משמשות המערכות לזיהוי, סיווג, תחזית או הערכה לגבי אדם מסוים. זאת, גם אם המידע עליו לא נכלל בנתוני העתק הגולמיים ואף אם הוא לא מסר את המידע אודותיו בעצמו.²¹⁴ כלומר, גם אם אדם בוחר שלא לשתף מידע אישי לשם לימוד מכונה, אחרים מסרו מידע, והמידע שלהם משמש לצורך הלימוד של הדפוס הכללי, שיאפשר בהמשך להגיע לתובנות פרטניות ורגישות לעתים ביחס לאותו אדם (בפרט כשמדובר בשירותים כגון אשראי או ביטוח), ללא צורך בגישה למידע אישי אודותיו (או על בסיס מידע אישי בסיסי ביותר).²¹⁵

מאפייני הלימוד ועיבוד נתוני העתק המבוצע על ידי מערכות הבינה המלאכותית, מביאים לשיפור ניכר באיכות, בדיוק ובפירוט של המידע המוסק וכן את היכולת להסיק מידע מנתונים שלא נראים רלוונטיים כלל למסקנה או להערכה. עם פיתוחן של מערכות הבינה המלאכותית, יכולת ההיסק האמורה משתדרגת כל העת וניתן באמצעותה להגיע למידע בעל רגישות מיוחדת על האדם מנתונים "רחוקים" יחסית, כך שגם אם לאדם יש שליטה על המידע אודותיו, הוא לא יכול לשלוט על האופן בו המידע יוערך והתובנות שיתגלו לגביו, לא כל שכן לצפות את פוטנציאל השימושים במידע מסוים לגביו.²¹⁶ כך למשל היסקים על נטייה מינית מניתוח מאפיינים חיצוניים של הפנים, היסק על מצבו הנפשי של אדם ומאפיינים אישיותיים בהתבסס על דפוסי השימוש שלו במכשיר טלפון חכם או על בסיס היסטוריית עסקאות.²¹⁷

213 סעיף 7(3) ל-GDPR. זכות החזרה מההסכמה היא חלק ממערך הזכויות לנושאי מידע שצפוי להיכלל בתיקון הנוסף שמקדם משרד המשפטים לחוק הגנת הפרטיות, והיא מעוגנת היום בהקשרים צרכניים שונים; ראו לעניין זה עמדת היועץ המשפטי לממשלה בת"צ 15-03-22141 גרינברג נ' סלקום ישראל בע"מ (5.3.2020), פס"כ 61. ע"א 8954/11 פלוני נ' פלונית, פס"כ 160 לפסק דינו של כב' השופט סולברג (22.5.2014).

214 כך למשל במודלים שנותנים המלצות: על בסיס ניתוח רכישת ספרים או הרגלי צפייה, הבינה המלאכותית מזהה דפוסי קריאה וצפייה, וכאשר היא מזהה אדם שהמידע עליו לא נכלל בנתונים הגולמיים אולם מתאפיין בדפוס דומה היא משערת שהוא יתעניין במוצרים דומים. בירנהק "פרטיות ובינה מלאכותית", בעמ' 156-157.

215 בירנהק מכנה אתגר זה "אתגר הקבוצה", ראו שם, בעמ' 22-23.

216 Alicia Solow-Niederman, "Information Privacy and the Inference Economy", 117 Nw. U. L. Rev. 357 (2022).

217 Wang, Y. & Kosinski M. "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images", Journal of Personality & Soc. Psychology 114(2), 246 (2018); Stachl, Clemens, et al. "Predicting Personality from Patterns of Behavior Collected with Smartphones", Proceedings of the National Academy of Sciences of the United States of America 117, no. 30 (2020); Ramon Y. Farrokhnia R.A, et al. Explainable AI for Psychological Profiling from Behavioral Data: An Application to Big Five Personality Predictions from Financial Transaction Records, Information 12 (2021).

אם כן, יכולות המחשוב והעיבוד שהשתפרו לצד זמינות נתוני ענק ופיתוח טכנולוגיות הבינה המלאכותית משפרות דרמטית את היכולת למצוא קורלציות והקשרים המאפשרים להגיע לתובנות רגישות ועשירות על בני אדם ובין היתר בנוגע להיבטים אישיותיים והתנהגותיים, מוצא אתני, העדפה מינית ודעות, כמו גם תחזיות על התנהגותם בעתיד. לתובנות אלו פוטנציאל לשימוש מסחרי רחב ומגוון, כגון שירותים מותאמים אישית (ראו למשל בפרק אשראי במערכת הבנקאית ביחס לשיווק אשראי), מיקוד התנהגותי לצרכי פרסום ושיווק ועוד. הן גם יכולות לשמש כלי לקבלת החלטות בעלות פוטנציאל משמעותי לגבי אדם. בהקשרים פיננסיים כלים אלו יכולים לבוא לידי ביטוי במסגרת תמחור ביטוחים מסוגים שונים, הערכת סיכון במתן אשראי או זיהוי חריגות בשימוש בכרטיס אשראי לשם התראה על הונאה, המלצות לניהול תיק השקעות מותאם אישית וכדומה.

על המורכבות שמעוררות מערכות הבינה המלאכותית מבחינת פוטנציאל השימושים הלא צפויים והקושי לעתים לעמוד על מטרות הפיתוח שלהן בכל הנוגע ליישום חובת היידוע וקבלת הסכמה לשימוש במידע אישי עמדנו לעיל. החלק הנוכחי יוקדש לאתגר נוסף בהגנה על הזכות לפרטיות ועל מידע אישי שמציבות יכולות אלו, ועניינו בשאלה כיצד לסווג את **תוצרי** הבינה המלאכותית הנוגעים לאדם מזוהה או ניתן לזיהוי, האם יש לסווג גם את תוצרי האלגוריתמים הנוגעים לאדם כ"מידע אישי" והאם נדרש להחיל ביחס למידע מסוג זה חובות או זכויות ייעודיות נוספות או שיש התאמות שנון לערוך במסגרת יישום החוק בנושא.²¹⁸

בישראל, הגדרת "מידע אישי" החדשה בחוק הגנת הפרטיות, כ"נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי" משמיעה כי גם נתון שהוא היסק או תחזית לגבי אדם הוא נתון הנוגע לאדם כאמור ולכן נחשב ל"מידע אישי", המוגן על פי חוק הגנת הפרטיות. לשם המחשה, התרשמותו של גורם מטפל מאדם והערכתו את דפוסי ההתנהגות שלו, או הערכה רפואית של מצבו של אדם – גם אם הן נתונות לפרשנות סובייקטיבית של מומחים שונים ואפילו לא היו מדויקות או מתבררות כשגויות – הן מידע אישי בנוגע לאותו אדם, שעליו חלים דיני הגנת הפרטיות. כלומר אין דרישה שהמידע יתאר בצורה מדויקת את האדם המזוהה או הניתן לזיהוי, על מנת לפרוס עליו את הגנת החוק, כי אם די בכך שמדובר בנתון הנוגע לאותו אדם.

זאת ועוד, בחוק הגנת הפרטיות כנוסחו לאחר תיקון 12, קובע כי מידע אישי שהוא "הערכת אישיות שנערכה מטעם גורם מקצועי שכדרך עיסוק מחווה דעתו על אישיותו של אדם או שנערכה באמצעי שמועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים" ייחשב ל"מידע בעל רגישות מיוחדת".²¹⁹ הגדרה זו נועדה לסווג כמידע רגיש במיוחד את תוצריהן של אמצעים טכנולוגיים, ובהם גם יישומי בינה מלאכותית, המיועדים להפיק הערכות או תחזיות לגבי מאפייני האישיות המהותיים המפורטים, סיווג שיש לו משמעות בין היתר להוראות לגבי חובת ההודעה לרשות להגנת הפרטיות על מאגרי מידע, חובת מינוי ממונה על הגנת הפרטיות, עיצומים המוטלים בגין הפרות החוק, דרישות בתחום אבטחת המידע ועוד.

רגולציית המידע האירופית ב-GDPR כוללת גם היא התייחסות מיוחדת לנושא זה, במסגרת ההוראות הנוגעות ל"פרופילינג", המוגדר כך:²²⁰ "כל צורה של עיבוד אוטומטי (ולא פעולה שמבוססת רק על עיבוד אוטומטי) של מידע אישי המורכבת משימוש במידע אישי כדי להעריך היבטים אישיים מסוימים לגבי אדם, ובמיוחד לנתח או לחזות היבטים הנוגעים לביצועיו של אותו אדם בעבודה, מצבו הכלכלי, בריאותו, העדפותיו האישיות, תחומי עניין, אמינות, התנהגות, מיקום או תנועות".

הדגש בהגדרה הוא על מטרת העיבוד האוטומטי. כך עיבוד אוטומטי שנועד לסווג אנשים לפי מאפיינים כמו גיל, גובה ומגדר – אינו בהכרח נכנס להגדרת הפרופילינג – למשל אם הוא משמש לניתוח סטטיסטי בלבד. אם העיבוד

218 ניתן להמחיש את השאלה בדוגמה מהעולם האנלוגי, במקרה שדנון בבית הדין האירופי לצדק (ECJ) על פי הדירקטיבה של האיחוד האירופי לעיבוד מידע אישי שקדמה ל-GDPR, בעניין **נובאק** (Case C-434/16 Nowak v. Data Protection Commissioner (2017), זמין כאן). באותו מקרה נבחן בבחינות ראיות חשבון טען שהערות הבוחן על המבחן שבו נבחן באות בגדר מידע אישי ולכן הוא זכאי לבקש גישה אליה וכן לתקן אותן כי הן לא מדויקות. ה-ECJ קבע כי ההערות על הבחינה הן גם מידע אישי, שכן גם התרשמות סובייקטיבית כמו הערכה או דעה, יכולה להיות מידע הנוגע לאדם מזוהה או ניתן לזיהוי. עוד נקבע כי כפועל יוצא, כדי להשתמש בהערכת הבוחן לצרכים אחרים מחוץ להליך הבחינה או כדי להעבירם לצד שלישי, צריך לקבל את הסכמת הנבחן, וכן כי יש לאחסן גם את הערכת הבוחן באופן מאובטח מפני גישה לא מורשית אליה. בית הדין הכיר בכך שגם זכויות של נושאי מידע כמו זכות העיון, זכות התיקון וזכות המחיקה, חלות גם על הערכת הבוחן אולם קבע שהזכות לבקש תיקון היא בהתאם למטרה לשמה המידע נאסף. לכן זכות התיקון לא כוללת זכות לתקן תשובות במבחן או את הערות הבדוק (אלא אם הם תועדו באופן לא נכון).

219 פסקה (8) להגדרת "מידע בעל רגישות מיוחדת" בסעיף 3 לחוק הגנת הפרטיות. ראו גם הנחיית הרשות להגנת הפרטיות 2/2012 "תחולת הוראות חוק הגנת הפרטיות על הליכי מיון לקבלה לעבודה ופעילות מכוני מיון" (2012) (זמינה כאן). בהנחיה (המבוססת על ההגדרה הקודמת בחוק הגנת הפרטיות ל"מידע") נקבע כי ככלל מכוני מיון צריכים למסור למועמדים לעבודה את חוות הדעת שנערכה לגביהם, כפי שנמסרה למעסיק שהזמין את המבחנים, לרבות תוצאות המבחנים.

220 סעיף 4(4) ל-GDPR.



האוטומטי נועד לתחזיות או מסקנות לגבי אדם ספציפי, אז הוא בא בגדרי ההגדרה.²²¹

בדברי המבוא ל-GDPR צוין כי פרופיילינג נתון לכללי הרגולציה בעניין עיבוד מידע אישי, כגון עקרונות עיבוד המידע והדרישה לעיבוד מידע לפי אחד מבסיסי העיבוד.²²² זוהי גם הנחיית הוועדה המקצועית של רשויות הגנת הפרטיות במדינות האיחוד האירופי (EDPB).²²³

זאת ועוד מעבר לתחולת הוראות בסיסי העיבוד ועקרונות העיבוד, ה-GDPR כוללת התייחסות קונקרטית לזכויות נושא המידע כאשר מתבצע פרופיילינג, ובין היתר חובת שקיפות, זכות עיון וזכות תיקון החלות גם על תוצרי הפרופיל ולא רק על נתוני הקלט וזכות להתנגד לפרופיילינג, ובפרט לפרופיילינג למטרות שיווק.

משמעות הדברים היא, למשל, כי מקום שעיבוד המידע האישי מבוסס על הסכמת לקוח כי המידע בעניינו ישמש לצורך דירוג אשראי, הרי שגם התוצר של העיבוד האלגוריתמי שלפיו נקבע דירוג אשראי מסוים הוא מידע אישי – אשר המשך עיבודו טעון בסיס עיבוד חוקי. לפיכך, כדי להשתמש בדירוג לצרכים אחרים (למשל לצורך אימון למודל כללי, או לצורך פיתוח אלגוריתמים שיספקו שירותים אחרים – תידרש הסכמה של נושא המידע גם לשימוש הזה, או בסיס עיבוד אחר).

גם חוק הגנת הפרטיות הצרכני בקליפורניה ה-CCPA (California Consumer Privacy Act) משנת 2018 כולל בהגדרת מידע אישי בין היתר היסקים המבוססים על סוגי המידע האישי נוספים הנמנים בחוק, שנעודו לייצר פרופיל על הצרכן בהיבטים שונים, כדלקמן:²²⁴

"Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."²²⁵

כמפורט לעיל, עולם הבינה המלאכותית משנה (וישנה) לבל היכר את היכולות ותוצאות ההיסקים והתחזיות על בני אדם. התחזיות יהפכו מפורטות, מדויקות ועמוקות יותר, ויוכלו להתבסס גם על מידע לא שגרתי או אופייני על מנת להגיע למאפיינים מהותיים ולמידע רגיש על אדם, לעתים גם מידע שלא בהכרח ידוע לו עצמו (למשל דפוסים התנהגותיים ונפשיים, ניתוח חוזקן של מערכות יחסים מסוימות וכו'). בהקשר זה, מעבר ליצירת המידע האישי החדש ויכולת ההיסק כשלעצמה, מתעורר היבט נוסף של פגיעה בפרטיות כפגיעה בשליטה של אנשים לגבי האופן שבו המידע אודותיהם משמש להסקת מסקנות לגביהם, או על האופן שבו המידע מוערך.²²⁶

במסגרת דוח הביניים ביקש הצוות את עמדות הציבור בשאלה האם נדרש להחיל ביחס למידע אישי מוסק חובות או זכויות ייעודיות נוספות או שיש התאמות שנכון לערוך במסגרת יישום החוק בנושא. כן התבקשו התייחסויות בשאלה אם יש מקום לקבוע, במסגרת שימוש בכלי בינה מלאכותית במערכות יחסים שמתאפיינות בחובות תום לב והגינות מוגברות (כמו במתן שירותים פיננסיים) כי לאדם תהיה זכות להיסק סביר בעניינו.²²⁷ קרי כזה שעומד באמות מידה של **Acceptability, Reliability** ו-**Reliability**:

Acceptability – המידע באינפוט עבור ההיסק צריך להיות כזה שמקובל לגבי פרטים – למשל איסור על התחשבות בקריטריון מוגן כמו נטייה מינית (וראו בהקשר זה גם המלצות בפרק העוסק בהטיה ואפליה).²²⁸

Relevance – המידע המוסק צריך להיות רלוונטי להחלטה ומקובל באותו הקשר. למשל, אין מקום כי יישום שנועד להפיק הערכה למטרה של מתן הלוואה יסיק מידע על מוצא אתני.

Reliability – המידע עליו מבוסס המודל, כולל המידע שעליו הוא התאמן צריך להיות אמין ומדויק מבחינה סטטיסטית (ראו גם המלצה 4 בפרק העוסק בהטיה ואפליה, בין היתר).

ההערות שהתקבלו בהקשר זה נעו בין שני קצוות. לפי גישה אחת שהוצגה על-ידי שני גורמים, יכולה להיות רגישות מיוחדת במידע מוסק בהיבטים רגישים, כגון מאפייני אישיות או מצב נפשי. רגישות זו, לצד פוטנציאל פגיעה

Article 29 Data Protection Working Party "Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679" (זמין כאן) (להלן: "פרשנות ה-EDPB בנושא פרופיילינג").²²¹

GDPR, recital 72; פרשנות ה-EDPB בנושא פרופיילינג.²²²

שם.²²³

Section 1798.140 (o)(1)(K).²²⁴

ראו גם הנחיית הבינה המלאכותית של ה-ICO המתייחסת במפורש לשימוש במערכות בינה מלאכותית לצורך ביצוע היסקים (קישור כאן).²²⁵

בירנהק "פרטיות ובינה מלאכותית", בעמ' 156 וההפניות שם.²²⁶

Sandra Wachter & Brent Mittelstadt, "A Right to Reasonable Inference: Re-thinking Data Protection Law in the Age of Big Data and AI", Colum. Bus. L. Rev. 494 (2019).²²⁷

עניין אחרון זה נובע במישור מהדין הקיים בנושא שוויון והפליה בישראל, ראו פרק הטיה ואפליה.²²⁸

בפרטיות הנובע מכך שנושאי המידע אינם שולטים או מודעים לתובנות המופקות לגביהם, מצדיקים טיפול מיוחד. אחד הגורמים הציע לנקוט בדרישה לקבל הסכמה מפורשת מנושאי המידע לצרכי הסקת מידע ושימוש בו, לחייב באמות המידה שצוינו לעיל (מקובלות, רלבנטיות, אמינות), ולנקוט אמצעים נוספים כגון הרחבת יידוע נושאי המידע והבחנה ברגולציה הפיננסית בין מידע גולמי ומוסק. גורם נוסף ציין כי מרכיבי ההיסק הסביר צריכים להיכלל במסגרת תהליך הערכת הסיכונים ביחס למערכות בינה מלאכותית, תוך וידוא שהעיבוד והתוצאה עומדים בשלוש אמות המידה האמורות.

גורם אחר שהעיר לעניין זה הציע להתייחס ל- Recital 71 של ה-GDPR העוסק בזכות שלא להיות כפוף להחלטות המתקבלות באופן בלעדי על-ידי מערכות אוטומטיות, לרבות פרופילינג, שעשויות להיות להן השלכות משמעותיות עליו, כגון דחיית בקשת אשראי. יובהר כי ה-Recital מתייחס לסעיף 22 ל-GDPR העוסק בזכות של אדם שלא להיות כפוף להחלטות כאמור, לצד חריגים הקבועים בו, אשר אין לו מקביל בדין הישראלי.

לפי הגישה האחרת, שהובעה על-ידי גורם אחד, מידע מוסק אכן כלול בהגדרת "מידע אישי", אולם אין לגזור מכך כי נדרשים הסדרים מיוחדים לגביו, ואין מקום להסדרים כאלה הייחודיים למערכת הפיננסית בלבד. עוד צוין, כי "יבוא" של הסדרים מהדין הזר בהיבטי פרטיות צריך להיעשות במסגרת חקיקה ראשית ולא בדרך של אסדרה מגזרית על הגופים הפיננסיים.

לאחר בחינת הערות הציבור וחשיבה נוספת בנושא, מוצע כי היסק של מידע אישי בידי גופים פיננסיים ידרש להיות סביר, קרי מבוסס על אמות מידה של מקובלות, רלבנטיות ואמינות. המלצה כזו, אף אם אינה נגזרת באופן מלא מדיני הגנת הפרטיות דווקא מתיישבת עם יתר המלצות הדוח בנוגע להתמודדות עם הסיכונים הגלומים במערכות בינה מלאכותית, ועם ההגנות הנדרשות למשקיעים וללקוחות שמערכות בינה מלאכותית פועלות בעניינים ובהינתן מערכות היחסים המיוחדות שיש בין גופים פיננסיים ללקוחותיהם. מוצע כי הרגולטורים הפיננסיים יבחנו את הצורך בפירוט ובהנחיה כיצד ליישם כלל זה בנוגע לאופן פעולתם של הגופים המפוקחים במערכות בינה מלאכותית המבצעות היסקים רגישים.



המלצות בנוגע לאתגר המידע האישי המוסק:

1. מידע אישי מוסק נכלל בהגדרת "מידע אישי" - הבסיס למענה לסוגיית המידע האישי מצוי בדין הקיים, המגדיר "מידע אישי" באופן רחב ככל "נתון הנוגע לאדם מזהה או לאדם הניתן לזיהוי". המוסק כי תוצרי מערכות הבינה המלאכותית – תחזיות, היסקים, הערכות, סיווגים שנעשים לגבי אדם ספציפי הם **מידע אישי** הזוכה להגנת דיני הגנת הפרטיות. זאת, בנוסף להוראת החוק המפורשת המתייחסת להערכת אישיות שנערכה **באמצעי שמיועד לביצוע הערכה** של מאפייני אישיות מהותיים, כמידע בעל **רגישות מיוחדת**.

2. היסק סביר – מוצע לאמץ כלל בדבר היסק סביר בעניינו של אדם, אשר יחול ביחס להחלטות בסיכון גבוה. היסק סביר נשען על אמות מידה של מקובלות (Acceptability), רלבנטיות (Relevance) ואמינות (Reliability). מוצע כי הרגולטורים הפיננסיים יבחנו את הצורך בפירוט ובהנחיה כיצד ליישם כלל זה בנוגע לאופן פעולתם של הגופים המפוקחים במערכות בינה מלאכותית המבצעות היסקים רגישים.

ד. אתגרים ביישום עקרון צמידות המטרה

כלל בסיסי ויסודי בדיני הפרטיות והגנה על מידע אישי, בישראל ובעולם, הוא כלל צמידות המטרה, לפיו ניתן לאסוף מידע אישי ולהשתמש בו למטרה לשמה נאסף או נמסר בלבד.²²⁹ הכלל מעוגן בסעיף 2(9) לחוק הגנת הפרטיות, הקובע כי שימוש בידעה על ענייניו הפרטיים של אדם שלא למטרה שלשמה נמסרה מהווה פגיעה בפרטיות (המהווה עוולה אזרחית ועבירה פלילית),²³⁰ וכן בפרק ב לחוק העוסק במאגרי מידע, בסעיף 8(ב), לפיו "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין". בגין הפרת הוראות אלו ניתן להטיל עיצומים כספיים על בעל שליטה במאגר מידע או מחזיק בו²³¹ וכן להורות, בצו שיפוטי הניתן לבקשת ראש הרשות להגנת הפרטיות, על הפסקת פעולות עיבוד המידע המפרות הוראות אלו או עלולות להביא להפרתן.

עקרון צמידות המטרה בא לידי ביטוי גם בהסדרים פרטניים המסדירים העברות מידע אישי לגורמים שונים. כך למשל ההסדר בסעיף 29א לחוק מרשם האוכלוסין, התשכ"ה-1965 המסמך את רשות האוכלוסין להעביר מידע לגופים שנדרשים לאמת פרטי זיהוי של אדם עם פרטי הרישום במרשם, ובהם בנקים. הסעיף כולל עיגון נוסף לעקרון צמידות המטרה לפיו תנאי להעברת המידע הוא התחייבות של הגוף המקבל את המידע כי ישתמש בו למטרה לשמה נמסר בלבד.²³² כך גם סעיף 25 לחוק שירות מידע פיננסי קובע כי נותן שירות מידע פיננסי יכול לאסוף ולקבל מידע פיננסי, ולעשות בו שימוש למטרות שפורטו בחוק בלבד.²³³

בעניין **איי. די. איי חברה לביטוח**, שבו נדרשו בית המשפט המחוזי ובהמשך גם בית המשפט העליון, ליישום עקרון צמידות המטרה, נדון מקרה בו חברת ביטוח שהועבר אליה צו עיקול של נכסי חייב בהוצאה לפועל, לצורך תפיסת כספים של אותו חייב המצויים בחזקתה, המשיכה לשמור את המידע גם לאחר שההליך שחייב את שמירת צו העיקול הסתיים. כאשר אותו חייב ביקש לרכוש ביטוח מחברת הביטוח – הוא סורב, על בסיס אותו מידע לגבי צו העיקול.²³⁴

בית המשפט המחוזי קבע כי עקרון צמידות המטרה באותו עניין אוסר על חברת הביטוח להשתמש במידע על עיקולים שמגיע אליה על מנת להקל על גביית חוב של נושים, לצורך סיווג לקוחות או לקוחות פוטנציאליים. בערעור שהוגש על פסק הדין, אישר בית המשפט העליון קביעות אלו.²³⁵

עקרון צמידות המטרה מוכר גם כאחד העקרונות הבסיסיים לעיבוד מידע (**GDPR ב-purposes limitation**), המורה כי מידע אישי ייאסף למטרה ספציפית, מפורשת ולגיטימית ולא יעובד באופן שאינו תואם לאותן מטרות.²³⁶ ההסדר ב-GDPR קובע כי עיבוד למטרות ארכוב לטובת האינטרס הציבורי, לטובת מחקר מדעי או היסטורי או לטובת מטרות סטטיסטיות ייחשב למטרה תואמת למטרה המקורית, תחת ערובות מסוימות, על מנת למנוע שימוש לרעה.²³⁷

229 ראו סעיף 2(9) לחוק הגנת הפרטיות, שקובע כי שימוש בידעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה לשמה נמסרה היא פגיעה בפרטיות המהווה עוולה אזרחית ועבירה פלילית שהעונש המרבי בצדה הוא 5 שנים (סעיפים 4-5 לחוק); סעיף 8(ב) קובע כי לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין. ב-GDPR עקרון צמידות המטרה עוגן כאחד מעקרונות העיבוד המנויים בסעיף 5. סעיף 1(5)(b) קובע כי מידע אישי צריך להיאסף למטרות ספציפיות, מפורשות ולגיטימיות ולא ניתן לעבד מידע באופן שלא תואם את אותן מטרות.

230 ליישום עקרון זה בפסיקה ראו למשל ע"א 439/88 **רשם מאגרי מידע נ' ונטורה**, פ"ד מח(3) 817, 808 (1994); ע"ע (ארכי) 8/90 **איסקוב ענבר – מדינת ישראל – הממונה על חוק עבודת נשים**, פס"כ 26(ד), 41 (8.2.2011).

231 מחזיק במאגר מידע מוגדר בחוק כגורם חיצוני לבעל השליטה במאגר המידע, המעבד בעבורו מידע (וראו גם הגדרת processor בסעיף 4(8) ל-GDPR).

232 סעיף 29א(א) לחוק מרשם האוכלוסין, וראו גם סעיפים 29א(ד)-(ו).

233 עוד קובע חוק שירות מידע פיננסי כי נותן שירות מידע פיננסי רשאי לעשות שימוש במידע פיננסי שאסף או קיבל גם למטרות סטטיסטיות הקשורות למתן שירות מידע פיננסי לכלל לקוחותיו, ובלבד שניתנה לכך הסכמה מפורשת ובכתב על ידי הלקוח, ושהמידע שיוצג ללקוחות יהיה **מידע סטטיסטי מצרפי שהוא מידע לא מזוהה** (ראו סעיף 25(2)(ד) לחוק זה). ראו גם סעיפים 25 ו-58(א) לחוק נתוני אשראי; סעיפים 52 ו-136 לחוק חדלות פירעון ושקידום כלכלי, התשע"ח-2018.

234 ההליך הגיע לבתי המשפט בעקבות תלונה שהוגשה לרשות להגנת הפרטיות, ובהמשך לטיפול בה הוצאה הנחיית הרשות להגנת הפרטיות 1/2011 "איסור שימוש במידע בדבר הטלת עיקול אצל צד שלישי" מחודש ספטמבר 2011 (קישור כאן). בהנחיה צוין כי ניתן להכשיר את הפגיעה בפרטיות הנובעת משימוש במידע אודות הטלת העיקול באמצעות קבלת הסכמתם המוקדמת והמודעת של החייבים, בהתאם לסעיף 1 לחוק. משמעות הדבר כי שימוש כזה יהיה אפשרי הלכה למעשה רק במקרים שבהם החייב לקוח של הצד השלישי (וראו עמדת הרשות ביחס לנסיבות שבהן תניה כזו בחוזה אחיד של נותן שירות תיחשב לתנאי מקפח, סעיפים 3.1.6-3.1.7 להנחיה זו). בנוסף, ההנחיה קובעת כי צד שלישי שקיבל החלטה הנוגעת ללקוח בהתבסס על מידע אודות עיקול שהוטל עליו, להודיע במפורש ללקוח – וזאת על מנת לאן את הנזק העלול להיגרם לאדם שעל נכסיו הוטל עיקול מתוך טעות או טענת שווא (סעיף 3.1.9).

235 עת"מ (מינהליים ת"א) 24867-02-11 **איי.די.איי חברה לביטוח בע"מ נ' רשם מאגרי המידע, הרשות למשפט טכנולוגיה ומידע במשרד המשפטים**, עמ' 22-26 (5.8.2012). לערעור בבית המשפט העליון – עמ"מ 7043/12 **איי.די.איי חברה לביטוח בע"מ נ' משרד המשפטים, הרשות למשפט טכנולוגיה ומידע – רשם מאגרי מידע** (15.1.2014) (להלן: "ערעור איי די איי").

236 סעיף 1(5)(b) ל-GDPR.

237 ראו סעיף 1(89) ל-GDPR הדורשת בין היתר נקיטת אמצעים טכניים וארגוניים למימוש עקרון המינימליזציה כגון התממה חלקית, אם המטרות

ההנחה בסעיף זה ב-GDPR היא כי שימוש במידע למטרות סטטיסטיות נמצא בהלימה למטרה המקורית כאמור, ולכן ככלל יהיה קביל בכפוף לערובות נוספות כאמור.²³⁸ עם זאת, כאשר מדובר במידע המסווג כרגיש על פי ה-GDPR העיבוד למטרות סטטיסטיות מותר אם הוא חיוני להגשמתו, ואם הוא מתבסס על חוק של האיחוד או של מדינה חברה, שיהיה מידתי ביחס לתכלית העיבוד, שיכבד את מהות הזכות להגנת מידע אישי, ושיכלול הגנות לזכויות ולאינטרסים של נושאי המידע.²³⁹ דברי המבוא ל-GDPR מפרטים ומבהירים לגבי עיבוד תואם למטרות סטטיסטיות לצורך עקרון זה, ולפיהם עניין בכל פעולה של איסוף ועיבוד מידע אישי הנדרשת לסקרים סטטיסטיים (בדומה ללמ"ס) או להפקת תוצאות סטטיסטיות. תוצאות אלו יכולות לשמש למטרות שונות, כמו מחקר מדעי. לפי דברי המבוא, המטרה הסטטיסטית משמעה כי התוצאה של העיבוד הסטטיסטי היא לא מידע אישי אלא מידע מצרפי נצבר, וכי המידע האישי שנאסף או התוצאה לא משמשים לתמוך באמצעים או החלטות הנוגעות לאדם ספציפי.²⁴⁰

נוכח האמור, נראה כי מטרה סטטיסטית שתחשב למטרה תואמת לצורך עקרון צמידות המטרה על פי ה-GDPR אינה יכולה לשאת על כתפיה פרשנות לפיה שימוש במידע אישי לצורך פיתוח כלים ואלגוריתמים של בינה מלאכותית באים גם הם בגדר "מטרות סטטיסטיות", ככל שאלה נועדו לתמוך באמצעים או בקבלת החלטות הקשורים באדם ספציפי. למיטב הבנתנו, חלק ניכר מהמערכות הן כאלו. על כל פנים, חריג כאמור לעקרון צמידות המטרה לא קיים בדין הישראלי נכון להיום.

יישום עקרון צמידות המטרה בהקשר של עיבוד מידע אישי לצרכי פיתוח במערכות מבוססות בינה מלאכותית היא סוגיית מפתח משום שבניית הביג דאטה לרוב מערבת שילוב של נתונים שנאספו בנפרד למטרות שונות ועיבוד אותו מידע לצורך נושאים שלא ניתן היה להעלות על הדעת בזמן איסוף המידע. כלומר, מערכות אלו מבקשות לא פעם להתבסס ואף להשתמש בנתונים שלא שימשו באופן מסורתי למטרות מסוימות על בסיס גילוי קורלציות לא צפויות בין הנתונים כאמור.

בהקשר זה מוצע להתמקד בשלושה אתגרים ליישום עקרון צמידות המטרה: הראשון, עניינו בעמידה בדרישה כי מטרת עיבוד המידע תהיה ברורה, מפורטת ומפורשת, על מנת להבטיח עמידה בעקרון זה. כפי שצוין בפרק ההסכמה לעיל, לעתים בשלב פיתוח כלי הבינה המלאכותית – מטרות השימוש ותוצרי המערכת אינם ידועים למפתח או לגוף שבכוונתו להשתמש במערכת, וקיים קושי לפרט מעבר לרמה כוללת יחסית, מהם השימושים שתעשה המערכת במידע. אתגר שני נוגע לסוגיית "המלאי", קרי מצב שבו מבוקש לערוך שימוש במידע שנאסף על לקוחות למטרה מסוימת לצרכי פיתוח כלי בינה מלאכותית. בפרק ההסכמה התייחסנו למענה אפשרי לסוגיות המתעוררות אגב כך, בדרך של התממה או פניה מחודשת ללקוחות, בהתאם למתווה שפורט לעיל. שלישית, ובהמשך למוטיבציה ההולכת וגדלה להרחבת בסיס הנתונים שעליהן מתבססות מערכות הבינה המלאכותית, גופים שונים מבצעים קציר מידע מהאינטרנט (scraping) לצרכי פיתוח במערכות בינה מלאכותית (למשל, תמונות או מידע אחר מרשתות חברתיות). מידע זה מפורסם לכאורה באתרים פומביים אולם נטילת המידע מאותן פלטפורמות ושימוש בו לצורך פיתוח מערכות בינה מלאכותית בשירותים פיננסיים (ובכלל) עשויה לחרוג מגדר ההסכמה או הציפיות הסבירות של המשתמשים עת פרסמו מידע באותן פלטפורמות, ומנוגדת לעקרון צמידות המטרה.²⁴¹

במסגרת הערות הציבור לדוח הביניים הציע אחד הגורמים המעירים לנקוט בפתרונות הבאים לסוגיית צמידות המטרה: התאמת רמת הפירוט הנדרשת לגבי מטרת עיבוד המידע להערכת הסיכונים מהמערכת (ככל שהשימוש נרחב יותר או חורג מציפיותיו הסבירות של הלקוח, ידרש פירוט נרחב ובהיר יותר של המטרות); התאמה של מטרות חדשות למטרות הקיימות על בסיס הערכת הסיכונים מהמערכת; ותיקון החקיקה כך שתאפשר שימוש מוגבל בנתונים לצורכי פיתוח מערכות בינה מלאכותית בכפוף לבקורות.

גורם אחר טען כי התפישה שהשתרשה בדין הישראלי לפיה אסור להשתמש במידע לאף מטרה נוספת מבלי לקבל הסכמה מבעל המידע, אינה הכרחית או דומה ל-GDPR שעוסק רק בהגבלת מטרה ולא בצמידותה. על כן הוצע לבחון את ההרחבה של עקרון צמידות המטרה בהתאם לפרשנות תכליתית של סעיף 2(9) לחוק הגנת הפרטיות וההגנות בסעיף 18 לחוק זה.

גורם שלישי חזר על טענתו שהופיעה גם בעניינים אחרים, לפיה סוגיית צמידות המטרה אינה ייחודית למוסדות

האלו יכולות להיות מוגשמות באופן זה. כאשר ניתן להגשים מטרות סטטיסטיות בעיבוד שלא מאפשר או לא עוד מאפשר את הזיהוי של נושא המידע, יש להגשימן באופן זה. ראו גם הערת המבוא ל-GDPR, Recital 156.

GDPR, recital 50 238

סעיף 9(j) ל-GDPR 239

GDPR, recital 162 240

241 ראו בירנהק "פרטיות ובינה מלאכותית", בעמ' 164-165.

פיננסיים או למערכות בינה מלאכותית, ואין להטיל לגביה הוראות מיוחדות. עוד ציין אותו גורם כי שימוש במידע לצרכי אימון מערכות בינה מלאכותית מצוי בגדר הציפיה הסבירה של הלקוח ולכן אין הצדקה לדרוש לגביו הסכמה נוספת.

ההמלצות בנוגע לאתגר עקרון צמידות המטרה נותרו ביסודן כפי שהיו בדוח הביניים. בהמשך להערות הציבור ולשינויים שנערכו בהמלצות הנוגעות לבעיית המלאי באתגר ההסכמה, נערך שינוי גם בהמלצה הנוגעת לשימוש במידע אישי לצורך פיתוח מערכות בינה מלאכותית כך שחודד שזו חלה רק ביחס לפיתוח מודל שאינו למטרה המקורית לשמה נמסר המידע. כך לדוגמא, ככל שמטרת השימוש במידע היתה בין היתר שיפור פעילות חיתום האשראי של גוף פיננסי, הרי שביצוע פעילות זו גם במסגרת של מערכת בינה מלאכותית תיכלל בגדר אותה מטרה ולא תהווה פגיעה בפרטיות המצריכה הסכמה מחודשת.

אחת ההמלצות עסקה בסוגיה של קציר מידע מהאינטרנט (scraping). לאחר פרסום דוח הביניים, פרסמה הרשות להגנת הפרטיות טיוטת הנחיה בעניין תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית,²⁴² בה נכתב כי כריית מידע אישי מרשת האינטרנט לצורך עיבודו במערכת בינה מלאכותית, לרבות למטרת אימון האלגוריתם, כרוכה בפגיעה אסורה בפרטיות, אם לא ניתנה לכך הסכמה מדעת של נושא המידע. הצוות הותיר את ההמלצה לפיה הרגולטורים הפיננסיים, יחד עם משרד המשפטים, יבחנו את האפשרות לקבוע הוראות המסדירות את התנאים והנסיבות שבהם ניתן לאסוף מידע בדרך של קציר מידע מהאינטרנט (scraping) באופן שאינו מפר את הוראות חוק הגנת הפרטיות וכל דין אחר.

242 טיוטת הנחיית הרשות להגנת הפרטיות: תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית (2025), שפורסמה להערות הציבור (https://www.gov.il/he/pages/ai_reg).



המלצות בנוגע לאתגר עקרון צמידות המטרה:

1. מוצע כי מידת הפירוט הנדרשת ביחס למטרת עיבוד המידע האישי והשימוש בו לצורך **פיתוח** מערכות בינה מלאכותית תהיה הולמת להערכת הסיכונים הנשקפים מן המערכת שהגוף הפיננסי מבקש לפתח. ככל שמטרות השימוש במידע האישי מורכבות יותר, או חורגות מציפיותו הסבירה של הלקוח או מן השירות לשמו התקשר עם נותן השירות הפיננסי, כך נדרש כי תוכן ההסבר הנוגע אליהן יהיה **מפורט ובהיר יותר**. בהקשר זה ראו לעיל ההצעה לגבי מנגנון הסכמה מדורגת כדרך לגשר על הפער ביכולת לפרט על מטרת העיבוד בשלב הפיתוח, מקום שבו עיבוד המידע נסמך על הסכמה. יחד עם זאת יוער כי לעמדתנו, נוכח האתגרים שמעוררות מערכות הבינה המלאכותית ביחס לשליטת האדם על המידע אודותיו וליישום העקרונות הבסיסיים החלים על עיבוד מידע, אין מקום לראות בפיתוח מערכות בינה מלאכותית שאינן למטרה לשמה נאסף המידע (כדוגמת פיתוח מודל AI כללי או פיתוח מודל לצורך שירות אחר מהשירות אותו ביקש הלקוח לצורך) כשימוש תואם למטרה אחרת לשמה נאסף המידע, כגון לצורך מתן השירות הפיננסי, וממילא כאמור עקרון צמידות המטרה לא כולל נכון להיום היתר לעבד מידע אישי למטרות תואמות.²⁴³

2. בצד האמור, מקום שהשימוש במידע האישי הוא לצורך **שימוש** במערכת בינה מלאכותית שכבר הופעלה, או מקום שבו השימוש המבוקש הוא לצורך **אימון** מערכת קיימת, על מטרות השימוש להיות מפורטות ובהירות. ההנחה היא כי בשלב זה, הקושי הראשוני בפירוט והסבר על מטרות עיבוד המידע האישי המאפיין את שלב פיתוח המערכת, מתקיים במידה פחותה.

3. מוצע לשקול חקיקה שתאפשר הקלות ביישום עקרון צמידות המטרה למטרות פיתוח מערכות בינה מלאכותית, על בסיס נתונים שנאספו למטרות אחרות, בכפוף למגבלות ואמצעי בקרה. ב-EU AI Act נקבע הסדר כזה, בכפוף בין היתר לתנאים הבאים: השימוש במידע יכול להיות רק לשם מערכת בינה מלאכותית **שנועדה להגן על אינטרסים ציבוריים חיוניים** כמו חקירת ומניעת עבירות פליליות, בטיחות ובריאות הציבור, הגנת הסביבה; **המידע האישי נדרש ואי אפשר להשתמש במידע שעבר התממה**; מידע המעובד בארגז החול **לא יועבר או יהיה נגיש לצדדים אחרים, ולא ישמש ולא ישפיע על החלטות שיתקבלו לגבי נושאי המידע**; המידע יישמר בסביבה מאובטחת, נפרדת ומבוקרת שהגישה אליה מוקנית למורשים בלבד; תיעוד מלא של פעולות עיבוד מידע אישי; כללים לגבי מחיקת המידע וכמה זמן ניתן לשמור אותו.²⁴⁴

4. מוצע כי הרגולטורים הפיננסיים, יחד עם משרד המשפטים, יבחנו את האפשרות לקבוע הוראות המסדירות את התנאים והנסיבות שבהם ניתן לאסוף מידע בדרך של קציר מידע מהאינטרנט (scraping) באופן שאינו מפר את הוראות חוק הגנת הפרטיות וכל דין אחר, לצרכי פיתוח כלי בינה מלאכותית על ידי או בשימוש הגופים הפיננסיים (למשל, תמונות או מידע אחר מרשתות חברתיות). מידע זה מפורסם לכאורה באתרים פומביים אך עולה שאלה אם נטילת המידע מאותן פלטפורמות ושימוש בו²⁴⁵ לצורך פיתוח ואימון מערכות בינה מלאכותית בשירותים פיננסיים או לצורך קבלת החלטה ספציפית בעניינו של אדם במסגרת קבלת השירות הפיננסי, עלולים לחרוג מגדר ההסכמה או הציפיות הסבירות של המשתמשים עת פרסמו מידע באותן פלטפורמות ולהיעשות בניגוד לעקרון צמידות המטרה.

²⁴³ לשם המחשה, שימוש במידע שניתן לצורך מתן שירות פיננסי בידי הגוף המפוקח יכול להיות גם לצורך אימון מערכות הבינה המלאכותית שישמשו אותו במתן השירותים. זאת בדומה לשימוש שהיה אותו הגוף עושה במידע לשיפור מערכות, לניהול סיכונים, וכדומה, ללא מערכת בינה מלאכותית. מנגד, ככל שמדובר לדוגמה במכירת המידע לגורם אחר לשם פיתוח מערכת בינה מלאכותית שלו לצרכים אחרים, לא מתקיים כמובן עיקרון צמידות המטרה.

²⁴⁴ סעיפים 53-55 ל-EU AI Act.

²⁴⁵ ראו לעניין זה סעיפים 104-106 בחוות הדעת של ה-European Data Protection Board (EDPB) – Opinion 28/2024 on certain data-protection aspects related to the processing of personal data in the context of AI models המציעה לנקוט אמצעים שונים במסגרת ההתמודדות עם הסיכון ששימוש ב-web scraping יוצר – הגבלת איסוף ומקורות למשל לגבי מידע אישי שיכול ליצור סיכון לאנשים או קבוצות ספציפיות (קורבנות פוטנציאליים לפגיעה, אפליה או אלימות), החרגת קטגוריות מידע (למשל רגישותם), כיבוד התנגדויות של אתרים אשר בוחרים להשתמש במנגנונים טכנולוגיים למניעת כריית מידע מאתרים ויצירת רשימת "opt out" המאפשרת לנושאי מידע להתנגד לאיסוף המידע עליהם מאתרים מסוימים.

ה. אתגרים ביישום עקרון מזעור המידע במערכות מבוססות בינה מלאכותית

עקרון ליבה נוסף החל על עיבוד מידע אישי הוא עקרון מזעור המידע (Data Minimisation) או הגבלה על שימוש במידע עודף. לפי עקרון זה, יש לאסוף רק את המידע שרלוונטי והכרחי למטרת העיבוד ויש איסור לאסוף ולעבד מידע עודף, כלומר מידע שחורג מהדרוש למימוש המטרה המקורית.²⁴⁶

מידע עודף יכול להיווצר בשלב איסוף המידע הראשוני וגם להפוך לכזה במהלך שמירתו לאורך זמן, בעקבות, למשל, השלמת המטרה, איסוף מידע נוסף וכו', וכך גם חובת מזעור המידע העודף – חלה הן בשלב האיסוף הראשוני והן לאורך תקופת שמירתו של המידע במאגר.²⁴⁷ איסוף ושימוש במידע אישי כאשר הוא לא נחוץ למטרה לשמה נמסר, או למטרות המאגר, מפרים את עקרון צמידות המטרה כמפורט לעיל, והם גם יוצרים סיכונים אבטחה מיותרים, שעלולים להוות הפרה של חובת אבטחת המידע.²⁴⁸ ככל שהמידע האישי השמור במאגר רב יותר, כך הסיכון לפגיעה בפרטיות כתוצאה מזליגה וחשיפה של המידע – גדול יותר.²⁴⁹

עקרון מזעור המידע בא לידי ביטוי בין היתר בתקנה 2(ג) לתקנות אבטחת מידע, המחייבת בעל מאגר מידע אישי לבחון אחת לשנה אם הוא מחזיק במאגר מידע עודף שאינו דרוש עוד למטרות המאגר.²⁵⁰ בנוסף, תקנה 6 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 העוסקת בהליך העברות מידע בין גופים ציבוריים לפי פרק ד' לחוק, מחייבת את הגוף מקבל המידע להפריד מידע עם קבלתו את הנתונים שהם מידע עודף ולמחוק אותו מיד.²⁵¹

בהקשר הפיננסי ראו גם ההסדר בסעיף 27 לחוק שירות מידע פיננסי, שקובע הוראות המגבילות את משך תקופת ההחזקה של נתון שירות במידע פיננסי שאסף או שהועבר לו.²⁵² עוד נקבע בחוק זה שעל נתון שירות חובה למחוק את המידע הפיננסי בתום תקופה שנקבעה בחוק.²⁵³ גם חוק נתוני אשראי קובע כי לשכת אשראי שקיבלה נתוני אשראי תחזיק בהם "לתקופה המזערית הנדרשת" לשם מתן שירות נתוני אשראי או שירות המתבסס על נתוני אשראי וקובע תקרה לתקופת החזקת הנתונים.²⁵⁴

עקרון מזעור המידע הוא גם אחד מעקרונות עיבוד המידע הקבועים גם ב-GDPR.²⁵⁵ בהערות המבוא ל-GDPR צוין כי משמעותו של עקרון זה היא כי נדרש להבטיח שהתקופה שבה מידע אישי מאוחסן מוגבלת למינימום האפשרי (strict minimum), וכי על מנת להבטיח זאת, על בעל השליטה לקבוע פרקי זמן שבהם מידע אישי נמחק או לקיים בקרה תקופתית על המידע המאוחסן. עוד נקבע כי מעקרון זה נובע כי יש לעבד מידע אישי רק אם מטרת העיבוד לא יכולה להיות מושגת בצורה סבירה באמצעים אחרים.²⁵⁶

קיים מתח מובנה בין יישום עקרון מזעור המידע, המבקש להגביל את איסוף המידע והשימוש בו רק מקום שהוא רלוונטי והכרחי להגשמת המטרה לשמה המידע נאסף, לבין פיתוח מערכות מבוססות בינה מלאכותית, המתבססות על מידע בהיקפים גדולים ככל הניתן, ממנו הן יכולות ללמוד על היסודות בלתי צפויים – ולהתאמן ולשכלל את התובנות שלהן. כאמור, בשלב פיתוח המודל – לא בהכרח ניתן לדעת מהן התובנות והתועלות שהמערכת תפיק מהמידע ואיזה קשרים יימצאו מועילים לניבוי או להשגת מטרות העיבוד. זאת ועוד, בשל חוסר הבהירות שיכולה

246 ראו פסק הדין בעמ"ס 7043/12 אי.די.איי חברה לביטוח בע"מ נ' משרד המשפטים, הרשות למשפט טכנולוגיה ומידע – רשם מאגרי מידע (15.1.2014), בו התייחס בית המשפט העליון גם לסוגיית שמירת המידע העודף והשימוש בו. בעניין זה נקבע כי "אין לעשות שימוש במידע שהגיע לגוף כגון חברת ביטוח או בנק בעניין פלוני לצרכים שמחוץ לשימוש המקורי המותר, ויש להסירו מזכרונם המוסדי לכל צורך למעט המקורי".

247 ראו מסמך מדיניות בנושא צמצום מידע של הרשות להגנת הפרטיות, טיוטה שפורסמה להערות הציבור במרץ 2021 (כאן). ביטוי לעקרון צמצום המידע כבר בשלב איסוף המידע הראשוני ניתן לראות בחוק מס' להפחתת גודש התנועה באזור גוש דן, התשפ"ב-2021, שבו נקבע כי צילום רכב במצלמות לא יהיה ניתן לצפייה ולא יישמר אלא באופן שלא יאפשר את זהויה הנוסעים ברכב המצולם או עוברי דרך אחרים (סעיף 28(א) לחוק).

248 סעיף 17 לחוק הגנת הפרטיות.

249 מסמך מדיניות בנושא צמצום מידע של הרשות להגנת הפרטיות, טיוטה שפורסמה להערות הציבור במרץ 2021 https://www.gov.il/BlobFolder/rfp/data_minimization_public_hearing/he/data_minimization_public_hearing.pdf.

250 לעיצום שנקבע על הפרת הוראה זו במסגרת תיקון מס' 13 לחוק הגנת הפרטיות, ראו פרט (3) לתוספת השלישית.

251 סעיף 23(ה) לחוק הגנת הפרטיות. עוד ראו תקנה 4 לתקנות הגישור המחייבת בעל מאגר מידע להפעיל מנגנון ארגוני, טכנולוגי או אחר, שמטרתו להבטיח כי במאגר לא מוחזק מידע שאינו נחוץ עוד למטרה שלשמה נאסף או הוחזק או למטרה אחרת שלשמה מותר להחזיקו לפי כל דין, ולמחוק מידע שנמצא לא נחוץ כאמור מוקדם ככל הניתן בנסיבות העניין. החל מחודש ינואר 2025 התקנות חלות גם על מידע על ישראלים המצוי במאגר מידע בישראל אשר מצוי בו מידע שהועבר מאירופה.

252 סעיף 27(א)(1) לחוק זה. ראו גם סעיף 27(א)(2) הקובע כי השר רשאי לקצר את התקופות.

253 סעיף 27(ב) לחוק שירות מידע פיננסי, מלבד מקרה של שמירת מידע לצורך הליך משפטי או הליך ביקורת פנימית או פיקוח לפי דין, המוסדר בסעיף 27(ג), לרבות התנאים השונים החלים על שמירת המידע לצרכים אלה.

254 סעיף 49(א) לחוק נתוני אשראי.

255 סעיף 1(5)(c) ל-GDPR.

256 GDPR, recital 39.

להתקיים כמפורט לעיל ביחס לשימושים המיועדים למערכת בינה מלאכותית, קיים קושי בסיווג מידע עודף ככזה. בנוסף, יישום דרישת מחיקת המידע האישי יכול לעורר קושי במישור המעשי מקום שבו האלגוריתם ממילא מבוסס עליו, לצד פגיעה אפשרית ביכולת להתחקות אחר האופן בו נוצר המודל, ולערוך בקרה על התוצאות אליהן מגיע האלגוריתם.

במסגרת הערות הציבור לדוח הביניים הוצגה התייחסות שהדגישה אף היא את הבעייתיות הנובעת מהקושי לצפות מראש מהו המידע שעשוי להיות רלבנטי. הגורם שהעיר בעניין הציע בין היתר לשקול פיתוח של מדדי מזעור, להוסיף התייחסות לקושי למזעור מידע בלתי מובנה, ולהוסיף מנגנונים שיאפשרו סטיה מעקרון המזעור כשיש הצדקה לכך. הואיל והמלצות הדוח כוללות כבר מספר אפשרויות בנוגע ליישום עקרון המזעור המידע, שכל אחת מהן תצריך מחשבה ופיתוח, לא נוספו החלופות האמורות אשר הוצגו באופן כללי בהערה. המלצה נוספת שעלתה במסגרת הערות הציבור ואומצה היא יצירת הפרדה בין המידע שנאסף בהתאם לשלבים השונים של מחזור החיים של המערכת ושמירה של המידע בנפרד, כאשר תקופות השמירה, הרשאות הגישה וכדומה יקבעו בהתאם לצורך של כל שלב.



המלצות בנוגע לעקרון מזעור המידע:

1. מוצע לשקול יישום דרישת מזעור המידע בדגש על הפרסונליות של המידע – כלומר שהיכולת לבצע קישור בין המידע לבין אנשים שהמידע הוא לגביהם תהיה נמוכה ככל האפשר – וזאת לעומת הדגש על מזעור כמות המידע שנאסף (שהיא קריטית למודלים). ראו לעיל בפרק על התממת מידע וכן להלן על טכנולוגיות מגבירות פרטיות (PETs).
2. נקיטת אמצעים ארגוניים וטכנולוגיים לבדיקה ותייעוד של הנתונים הנדרשים לפיתוח מערכת הבינה המלאכותית לאורך תהליך הפיתוח, וביצוע ניקוי ומחיקה של נתונים שניתן לומר שאינם רלוונטיים כבר בשלב זה.
3. מוצע כי גופים פיננסיים ישקלו, בשים לב לעלויות ולתועלת שכרוכה בדבר, אם במקרים המתאימים נכון ליצור הפרדה בין המידע שנאסף ונעשה בו שימוש, בהתאם לשלבים השונים של מחזור החיים של המערכת (פיתוח ואימון, יישום ושימוש, תחזוקה ושיפור המודל), לשמור אותו בנפרד, ולקבוע תקופות שמירה, הרשאות גישה וכדומה, בהתאם לצרכים המשתנים של כל שלב.
4. מוצע לבחון הגבלות מראש על שימושים בסוגי מידע מסוימים לצורך פיתוח מערכות בינה מלאכותית בתחומים מסוימים (למשל הגבלה על שימוש בתמונות פנים).



המלצות כלליות נוספות

נוכח האתגרים השונים שעליהם עמדנו, ניכר כי פיתוח כלי בינה מלאכותית מביאים לאתגרים משמעותיים ומגוונים בהגנה על פרטיות הלקוחות והמידע האישי שלהם. על רקע האמור, ובפרט מקום בו הערכת הסיכונים של פיתוח מערכת בינה מלאכותית מסוג מסוים מביאה למסקנה כי יש לסווג כמערכת בסיכון גבוה, מוצע כי הרגולטורים הפיננסיים ישקלו להכווין את הגורמים המפוקחים, באמצעות הנחיות, גילויי דעת או המלצות בדבר best practices לאמץ כלים ארגוניים שיתנו מענה לסיכונים הפרטיות שיש בכלים אלה ובהם:

1. תסקיר השפעה על פרטיות (Privacy Impact Assessment): תהליך מתודולוגי שנועד לסייע לארגון באיתור, הערכה וניהול של סיכונים לפרטיות בפרויקטים או פעילות עסקיות וארגוניות אחרות הכוללות עיבוד של מידע אישי. אין כיום חובה כזו בדין הישראלי, אולם מוצע להמליץ לאמץ כלי זה ככלי לניהול והערכת הסיכון בשימוש בכלי בינה מלאכותית המייצרים תחזיות והערכות לגבי אנשים לצורך קבלת שירותים פיננסיים.²⁵⁷ מוצע להנחות לבצע את התסקיר בשלבים מוקדמים של הנעת פרויקט הכרוך באיסוף או עיבוד מידע אישי, במקביל לתהליך והתכנון של המערכת – ולפני תחילת פעולות העיבוד.²⁵⁸
2. יישום והטמעת תפיסות עיצוב לפרטיות (Privacy by Design) ו- "פרטיות כברירת מחדל" (Privacy by Default) (יכולנו להלן ביחד – עיצוב לפרטיות) – תפיסת העיצוב לפרטיות מיועדת לשרת את התכליות (העסקיות או האחרות) של הארגון, בד בבד עם מזעור הסיכונים לפרטיות והשקעת משאבים באמצעי ההגנה המתאימים אל מול הסיכונים שזוהו בתהליך עיבוד המידע האישי בארגון, בין במסגרת תסקיר השפעה על הפרטיות או בדרך אחרת. לפי תפיסה זו, החל משלב התכנון המוקדם ולאורך כל

²⁵⁷ ראו סעיף 35(א)(3) ל-GDPR.

²⁵⁸ ראו מדריך עזר מתודולוגי לעריכת תסקיר השפעה על פרטיות שפרסמה הרשות להגנת הפרטיות, (עודכן ב-7 בדצמבר 2025), זמין ב[כאן](#).



מחזור החיים של איסוף המידע והשימוש בו, ובשים לב לחלופות הטכנולוגיות המקובלות, יעוצבו מערכות המידע ויוטמעו בארגון אמצעים נוספים לשם אופטימיזציה של ההגנה על פרטיות נושאי המידע ושמירה על זכויותיהם לפי דיני הגנת הפרטיות.

אופן יישום עקרון העיצוב לפרטיות בכל מקרה לגופו תלוי בנסיבות הקונקרטיות של פעולת עיבוד המידע ושל הארגון, וכן במצב התפתחות הטכנולוגיה בזמן הנתון. מבלי לגרוע מכלליות האמור, עיצוב לפרטיות ניתן ליישם בין השאר בדרך של צמצום איסוף המידע ועיבודו למינימום ההכרחי, התממת המידע האישי או פסאודו-אנונימיזציה, שימוש במידע סינתטי במקום מידע אישי, טכניקות פרטיות יחסית (Differential Privacy), הצפנה, צמצום הרשאות גישה, קביעת נהלי עבודה, שיפור השקיפות כלפי נושאי המידע לרבות במתכונת מתן ההסכמה, ושורה ארוכה של טכנולוגיות מגבירות פרטיות (Privacy Enhancing Technologies) אחרות.²⁵⁹

נוכח המלצות אלו באות בנוסף לחובת מינוי **ממונה על הגנת הפרטיות** כפי שנקבעה במסגרת תיקון 13 לחוק הגנת הפרטיות. החוק מטיל חובת מינוי ממונה על הגנת הפרטיות על ארגונים רבים ובהם, ארגון שבו עיסוקו העיקרי של בעל שליטה במאגר מידע או מחזיק בו כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר. לעניין זה החוק מונה במפורש דוגמאות לגופים שבאים בגדרי חלופה זו, ובהם גם **גופים פיננסיים** (תאגיד בנקאי כהגדרתו בחוק הבנקאות (שירות ללקוח), התשמ"א-1981 ומבטח כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ"א-1981).²⁶⁰ תפקידו של הממונה על הגנת הפרטיות הוא לפעול להבטחת קיום הוראות חוק הגנת הפרטיות על ידי הגוף הפיננסי ולקידום השמירה על הפרטיות ואבטחת המידע במאגרי המידע.²⁶¹

259 OECD, "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351 (2023). https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html

260 להרחבה בנוגע לטכנולוגיות מגבירות פרטיות ראו מדריך מקיף שפרסמה הרשות להגנת הפרטיות בנושא, לעיל. כן, סעיף 17ב(א)(4) לחוק.

261 ראו פירוט תפקידיו בסעיף 17ב לחוק. להרחבה ראו טיוטת גילוי דעת שפרסמה הרשות להגנת הפרטיות בנושא מינוי ממונה על הגנת הפרטיות בארגון לפי דרישות תיקון 13 לחוק (https://www.gov.il/he/pages/dpo25_1).



הטיה ואפליה

אתגר מרכזי שמתעורר ביחס לשימוש במערכות מבוססות בינה מלאכותית הוא הסיכון לאפליה (Discrimination) ולהטיות (Biases). למרות שקבלת החלטה על ידי אלגוריתם ולא על ידי גורם אנושי עשויה למתן את הנטייה האנושית להטיות בלתי מודעות או מכוונות – מערכות בינה מלאכותית חשופות אף הן לסיכון להטיות או לאפליה מטעמים שונים שיפורטו להלן. היקף פעילותן הרחב מגביר את הסיכון להתרחשות תופעות אלה בקנה מידה רחב, בהשוואה להחלטה אנושית פרטנית.

אחד הטעמים הבולטים שעלולים לגרום להטיות ולאפליה על ידי מערכות בינה מלאכותית נוגע **למאגרי המידע** שעליהם מתאמנת המערכת. כאשר המערכת מתאמנת על מאגרי מידע שאינם מייצגים מספיק, כלומר אינם כוללים מידע מייצג ביחס לכל האוכלוסיות הרלוונטיות לפעילות המערכת – המערכת עלולה להפיק תוצרים מוטעים או מפלים. להמחשה, בתחום הרפואה, מערכת בינה מלאכותית אשר תאמן ביחס לנתונים הנוגעים לגברים בלבד – עלולה להיות מיושמת באופן לא מיטבי ומוטה ביחס למקרים רפואיים של נשים.²⁶² בנוסף לייצוג חסר, הנתונים שעליהם מתאמנות מערכות בינה מלאכותית עלולים לשקף הטיות ואפליה **קיימות** בחברה. למשל, ככל שקיימת הטיה כלפי חתך אוכלוסייה מסוים בקבלה למשרות מסוימות או בקבלת אשראי – מערכת בינה מלאכותית הנשענת על נתונים מוטעים אלה עלולה לשחזר ולהנציח את התוצאות המפלות.²⁶³

טעמים נוספים שעלולים לגרום להטיות ולאפליה נוגעים לאופן שבו מעוצב האלגוריתם **ולאופן בחירת המשתנים** המשמשים את המודל לקבלת החלטה. במסגרת זו, גם אם מאגר המידע שעליו מבוסס האלגוריתם הוא מאגר מייצג – מודלי בינה מלאכותית עלולים להוביל לאפליה אסורה בשל התייחסות לנתוני השתייכות קבוצתית "מוגנים", דוגמת לאום, מגדר, גזע, מין ועוד. בהקשר זה, אחד האתגרים המוכרים בנוגע לעיצוב מערכות בינה מלאכותית, הוא שלא תמיד ניתן לחסום לחלוטין את המערכת מהתחשבות בנתוני השתייכות קבוצתית מפלים. זאת כיוון שמערכות בינה מלאכותית עשויות לעשות שימוש בנתוני "פרוקסי" – נתונים שאינם מפלים כשלעצמם (כגון מוסד השכלה גבוהה, מיקוד, היסטוריית גלישה וכו'), שיש להם קורלציה משמעותית עם משתנים מפלים (כגון גזע, לאום וכו'). להמחשה, אחד המחקרים הבולטים בנושא, מצא כי מערכות מבוססות בינה מלאכותית ששימשו לצורך איתור מועמדים לתוכניות טיפול ייעודית בארה"ב, התחשבו בנתון בדבר היקף ההוצאות הרפואיות של המטופלים, שאינו מפלה כשלעצמו – אך כתוצאה מכך, איתרו שלא במתכוון פחות מטופלים שחורים בהשוואה לגברים לבנים.²⁶⁴

לצד הטעמים האמורים שמעוררים סיכון להטיות ולאפליה, חשש מרכזי שמתעורר ביחס לאפליה על ידי מערכות בינה מלאכותית הוא שחזור והגברה של הטיה או אפליה על ידי המערכת, בשל "Feedback Loop". החשש הוא שאם מערכת בינה מלאכותית תפיק מסקנות מוטות, או תוביל להשלכות מוטות ומפלות בפועל – המערכת תוסיף ותלמד את אותן תוצאות מוטות, ובכך תחזק את ההטיות שלה לאורך זמן.²⁶⁵

בהקשר של הסקטור הפיננסי, החשש להטיות ולאפליה על ידי מערכות בינה מלאכותית עשוי להתעורר ביחס לתחומי פעילות שונים. אחד התחומים הבולטים, שגם זכה לעיסוק ניכר באסדרה העולמית, הוא **מתן אשראי**. אמנם, מודלים המשמשים לצורך הערכת הסיכון במסגרת מתן אשראי מאפשרים ביצוע של הערכות מדויקות ויעילות יותר, ולכן עשויים להרחיב את הנגישות לאשראי לאוכלוסיות שונות עקב חיזויים מדויקים יותר המבוססים על מידע עשיר יותר,²⁶⁶ ובכך להפחית את הסיכון לאפליה והטיות במסגרת החלטה אנושית פרטנית. ואולם, שימוש במודלים מעורר גם סיכון להטיות או אפליה, למשל בשל אימונם על מאגרי מידע הכוללים מידע חסר או מוטה כלפי אוכלוסיות מסוימות או בשל שימוש של המערכת בנתוני פרוקסי.²⁶⁷

Isabel Straw, The Automation of Bias in Medical Artificial Intelligence (AI): Decoding the Past to Create a Better Future, 110 262 ARTIFICIAL INTELLIGENCE MED. 101965, 101966 (2019).

Michael A. Griffith, AI Lending and ECOA: Avoiding Accidental Discrimination, 27 N.C. Banking Inst. 349 (2023), <https://scholarship.law.unc.edu/ncbi/vol27/iss1/16>.

Ziad Obermeyer et al., Dissecting racial bias in an algorithm used to manage the health of populations, Science, 366, 447– 264 453 (2019), <https://www.science.org/doi/10.1126/science.aax2342>.

Emilio Ferrara, The Butterfly Effect in Artificial Intelligence Systems: Implications for AI Bias and Fairness, Machine Learning 265 with Applications, Volume 15, 2024, https://doi.org/10.48550/arXiv.2307.05842?force_isolation=true.

266 בהקשר זה יצוין שאחת ממטרותיו המוצהרות של חוק נתוני אשראי, שמכוחו החל לפעול מאגר נתוני אשראי בבנק ישראל, היא הרחבת הנגישות לאשראי וצמצום האפליה במתן אשראי.

267 לדוגמה, הסתמכות המערכת על נתון כגון השכלה גבוהה, שאינו מהווה קריטריון זהותי מוגן כשלעצמו – עשויה להוביל בפועל לאפליה תוצאתית

טענות לאפליה על ידי מערכות בינה מלאכותית במתן אשראי עלו בשנים האחרונות בהקשרים שונים בארה"ב. למשל, בשנת 2019, עלתה טענה ברשתות החברתיות לאפליה על ידי אפליקציית האשראי של חברת Apple, שהופעלה בשיתוף בנק גולדמן זקס, שכן זו קבעה מסגרות אשראי נמוכות יותר לנשים בהשוואה לגברים. ה-DFS (The New York State Department of Financial Services), הרגולטור של השירותים הפיננסיים והביטוח במדינת ניו יורק, בחן את הטענות ומצא כי לא הייתה אפליה על בסיס מגדר.²⁶⁸ במקרה אחר, בפרסום משנת 2020 מטעם ארגון בשם "student borrower protection center" תוארו פערים משמעותיים בעמלות ובריביות של הלוואות סטודנטים, שביקשו מועמדים בעלי נתונים זהים – וזאת על רקע מוסד ההשכלה הגבוהה שבו הם למדו, שמצוי בקורלציה לקטגוריה גזעית.²⁶⁹

הסיכון להטיות או אפליה עשוי להתעורר בהקשרים פיננסיים נוספים. בתחום הביטוח למשל, בכל הנוגע לתמחור פוליסת ביטוח, שימוש בבינה מלאכותית אמנם מאפשר לדייק את תמחור הסיכון ביחס לכל מבוטח ומבוטח – אך במקביל, קיים סיכון להתייחסות של המערכת למאפיינים זהותיים מוגנים, כגון לאום או גזע, באופן מפלה.²⁷⁰ גם בתחום ההשקעות, מערכת המבוססת על נתונים שאינם מייצגים, עלולה להפיק תוצאות מוטות או לא מיטביות עבור פלחי אוכלוסייה מסוימים.²⁷¹

הדין בעניין אפליה בישראל

החובה לנהוג בשוויון חלה על גופים ציבוריים או דו-מהותיים במסגרת המשפט המינהלי.²⁷² לצד זאת, בכל הנוגע לגופים פרטיים, חוק איסור הפליה במוצרים, בשירותים ובכניסה למקומות בידור ולמקומות ציבוריים, התשס"א-2000 (להלן: "**חוק איסור הפליה**"), קובע איסור רוחבי על אפליה בעת הספקת מוצר או שירות ציבורי, או הפעלת מקום ציבורי. כך, לפי סעיף 3(א) לחוק:

3(א). מי שעיסוקו בהספקת מוצר או שירות ציבורי או בהפעלת מקום ציבורי, לא יפלה בהספקת המוצר או השירות הציבורי, במתן הכניסה למקום הציבורי או במתן שירות במקום הציבורי, מחמת גזע, דת או קבוצה דתית, לאום, ארץ מוצא, מין, נטיה מינית, השקפה, השתייכות מפלגתית, גיל, מעמד אישי, הורות או לבישת מדי כוחות הביטחון וההצלה או ענידת סמליהם".

סעיף זה קובע איסור אפליה מחמת רשימה של עילות אפליה המנויות בסעיף, הנוגעות לקבוצות שלגביהן קיימת היסטוריה של קיפוח ואפליה.²⁷³ לצד עילות אלה, בסעיף 3(א1) לחוק נקבע איסור הפליה גם מחמת מקום מגורים. חוק איסור הפליה הוא חוק רוחבי, אך הובהר במסגרתו במפורש כי הוא חל גם על שירותים פיננסיים שונים. כך, "שירות ציבורי" מוגדר בסעיף 2 לחוק (סעיף ההגדרות) גם כ"שירותים פיננסיים", ואלה מוגדרים באותו סעיף כ"שירותי בנקאות, מתן אשראי וביטוח".

לצד האיסור על אפליה מחמת העילות המפורטות בחוק איסור הפליה, במסגרת סעיף 3(ד) לחוק נקבעו סייגים

במתן אשראי כלפי קבוצות אוכלוסייה מסוימות. לניתוח הטעמים לאפליה בהקשר זה ראו: רות פלאטו-שנער ומעיין פרל "חיתום אשראי צרכני על סמך עיבוד מידע אלגוריתמי – היש סיבה לחשוש מאפליה אסורה?" **עיוני משפט** 553 (2022).

268 New York State Department of Financial Services **Report on Apple Card Investigation** March 2021, https://www.dfs.ny.gov/system/files/documents/2021/03/rpt_202103_apple_card_investigation.pdf

269 Student Borrower Protection Center, **Educational Redlining** (February 5, 2020), <https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf>.

270 לשם המחשה, בתחקיר מטעם "Pro Publica", משנת 2017, נמצא כי תושבים בשכונות מיעוטים במדינות שונות בארה"ב, שילמו פרמיית ביטוח רכב גבוהה יותר מאשר באזורים אחרים – insurance-premiums-white-areas-same-risk. <https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk> Center for Data Ethics and Innovation שכותרתו, "Review into bias in algorithmic decision-making", בעמוד 56 https://assets.publishing.service.gov.uk/media/60142096d3bf7f70ba377b20/Review_into_bias_in_algorithmic_decision-making.pdf

271 למשל, מודלים המבוססים על היסטוריית ההשקעה של הלקוח, עשויים להביא לתוצאות פחות טובות ביחס ללקוחות צעירים שלגביהם אין די מידע. ראו דוח IOSCO משנת 2021, בעמ' 10-11, ובפרט בהערות שוליים 9.

272 יצחק זמיר, הסמכות המינהלית, כך ה – עילות הביקורת המשפטית, עמ' 3970 (2020). בהקשר זה, ביחס לתאגידים בנקאיים, לא אחת הובעה העמדה כי התאגידים הבנקאיים הם גופים דו-מהותיים, וככאלה חבים הם בחובות מן המשפט הציבורי, לרבות הגינות, סבירות, שיוון וכללי הצדק הטבעי (ע"א 1691/11 בנק לאומי למשכנתאות בע"מ נ' צוברי, פסקה ב לחוות דעתו של המשנה לנשיאה א' רובינשטיין (15.12.2015), וראו גם רע"א 9065/23 ס.ע. טופ השקעות בע"מ נ' בנק מרכנתי דיסקונט בע"מ, פסקה 33 וההפניות שם (3.1.2024).

273 ראו דברי ההסבר לסעיף 3 בהצעת חוק איסור הפליה, ה"ח 2871 (15 במאי 2000).

לאיסור האפליה. בין היתר, בסעיף 3(ד)(1) לחוק איסור הפליה נקבע כי אין רואים אפליה "כאשר הדבר מתחייב מאופיו או ממהותו של המוצר, השירות הציבורי או המקום הציבורי". כלומר, הבחנה על בסיס העילות המנויות בסעיף 3 לא תהווה אפליה כאשר יש **טעם ענייני ממשי** לעשות כן והדבר מתחייב מאופיו או ממהותו של המוצר.

בהקשר של שירותים פיננסיים, כגון מתן אשראי או חיתום ביטוח, השאלה מהי הבחנה מותרת החוסה תחת סייג זה היא שאלה מרכזית, שנדונה מעת לעת בפסיקת בתי המשפט.²⁷⁴ ברקע לכך, בהקשרים פיננסיים שונים התייחסות למאפייניו האישיים של הלקוח (למשל, גילו) עשויה להיות הכרחית לצורך מתן שירות מותאם באופן אישי, למשל, לצורך הערכת סיכון אשראי של לקוח מסוים או לצורך קביעת פרמיית ביטוח – ועל כן עשויה שלא להיחשב לאפליה אסורה. יודגש כי דוח זה לא מכוון להביע עמדה פרשנית ביחס לסוגיה מהו הגבול בין הבחנה מותרת לבין אפליה אסורה. מדובר בשאלה רוחבית, שאינה נוגעת רק לשילוב מערכות בינה מלאכותית, וגבולותיה עודם מתעצבים בכל מקרה לגופו בפסיקת בתי המשפט.²⁷⁵ יחד עם זאת, יש לציין ששאלה זו עשויה לעורר אתגר מיוחד ביחס למערכות בינה מלאכותית, שכן למערכות אלה עלול להיות קושי לתת הסבר מנומק לבחירת המערכת לעשות שימוש בקריטריון זה או אחר.

אתגר נוסף המתעורר בנוגע ליישום חוק איסור הפליה ביחס למערכות בינה מלאכותית נוגע לשאלה כיצד תיבחן אפליה מחמת אחת העילות המנויות בחוק. בעוד חוק איסור הפליה מונה רשימת מאפיינים זהותיים שחל איסור להפלות על יסודם – בהקשר של מערכות בינה מלאכותית, עשוי להתעורר קושי לזהות **מה הקריטריון המסוים שבו נעשה שימוש** לצורך קבלת ההחלטה, בשל אופן הפעילות המורכב של המערכות, השימוש במשתני "פרוקסי", או בשל תופעת "הקופסה שחורה". דרכי הפעולה של מערכות בינה מלאכותית עלולות להקשות על זיהוי שימוש בקריטריון אסור, הן על ידי לקוחות שיבקשו לבחון האם הופלו, הן על ידי גופים פיננסיים המבקשים לעמוד בהוראות הדין בתחום האפליה, והן על ידי הרגולטורים בהליכי הפיקוח שלהם.

לצד חוק איסור הפליה, שחל באופן רוחבי, גם בהסדרי חקיקה פרטניים בהקשרים פיננסיים שונים נקבעו הסדרים פרטניים הנוגעים לאיסור אפליה. כך למשל:

בחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998, נקבעו בסימן ח' הוראות לעניין אפליה מחמת מוגבלות ביחס לחוזה ביטוח, למשל בכל הנוגע לסירוב לבטח אדם עם מוגבלות, לרבות מתן יחס שונה באופן קיצוני שבעקבותיו לא נכרת חוזה ביטוח.²⁷⁶ בהקשר זה, בסעיף 19(א) לחוק נקבע סייג, לפיו מתן יחס שונה בחוזה ביטוח לא יהווה אפליה "אם הוא מבוסס על נתונים אקטואריים, נתונים סטטיסטיים, מידע רפואי, או מידע אחר, שהם אמינים ורלוונטיים להערכת הסיכון הביטוחי המסוים, ומתן יחס זה סביר בנסיבות העניין".²⁷⁷

גם **בחוק נתוני אשראי**, אחת המטרות לשיתוף נתוני אשראי, שעוגנה במסגרת סעיף 1 לחוק, היא צמצום האפליה במתן אשראי וצמצום הפערים הכלכליים. למעשה, אחת מתפיסות היסוד הניצבות בבסיס החוק היא כי שיתוף בנתוני אשראי מאפשר לצמצם את השימוש במאפיינים מפלים, שכן הם מאבדים מחשיבותם ככל שקיים לגבי הלקוח מידע אישי רב יותר.²⁷⁸ בנוסף, ביחס לפעילות לשכות האשראי, סעיף 51 לחוק קובע כי "לשכת אשראי לא תביא בחשבון נתונים בדבר מינו, גילו, נטייתו המינית, גזעו, דתו, ארץ מוצאו, לאומיותו, מקום מגוריו ומצבו המשפחתי או הבריאותי של לקוח, לעניין המודל הסטטיסטי שלה הדרוש לה למתן שירותים המתבססים על נתוני אשראי וחיוויי אשראי, לעניין מתן חיוויי אשראי על לקוח ולעניין דירוג אשראי שלו".

274 ראו למשל בג"ץ 4948/03 אלחנתי נ' שר האוצר (2008); ע"ע (ארצי) 26328-09-14 הראל חברה לביטוח בע"מ נ' אשבל (3.12.2019) וכן תצ (מרכז) 8214-05-14 מירב נ' אי.די.איי. חברה לביטוח בע"מ (23.8.2018).

275 למשל, בתחום הביטוח, ראו ע"א 7308/19 טמיר נ' בנק הפועלים בע"מ (20.10.2022) (להלן – עניין טמיר). בין היתר, ראו הערת השופט י' עמית בפסקה 9 לגבי התחשבות בקריטריון גיל בגביית פרמיית ביטוח, והערת השופט ע' גרוסקופף (במיעוט בפסק הדין) בפסקה 32, בנוגע להבחנה תיאורטית בתמחור פוליסות ביטוח חיים בין קבוצות אוכלוסייה שונות על בסיס מוצא למשל.

276 להרחבה על אודות ההסדר, ראו נציבות שוויון זכויות לאנשים עם מוגבלות "איסור אפליית אדם עם מוגבלות בחוזה ביטוח מידע לציבור" (2.8.2018) https://www.gov.il/he/pages/nondiscrimination_in_insurance.

277 יצוין כי חוק שוויון זכויות לאנשים עם מוגבלות קובע חובת הנמקה ייחודית בהקשר זה, בדבר הסיבות להחלטה. כך, בסעיף 19(ז) נקבע כי אם "החליט מבטח ליתן למבוטח יחס שונה או סירב מבטח לבטח אדם, ימסור לו המבטח הודעה מנומקת בכתב עם תמצית בסיס הנתונים, אם המבטח התבסס עליהם במתן ההחלטה, וכן תמצית המידע שעליהם התבסס...".

278 בדברי ההסבר להצעת החוק נכתב כי "בהעדר מידע לגבי יחידים, נוטים נותני אשראי להשתמש בנתונים סטטיסטיים המבוססים על מאפייני אוכלוסייה, כגון מין, דת וגזע. שיתוף בנתוני אשראי מאפשר לצמצם את השימוש במאפיינים אלה, שכן הם מאבדים מחשיבותם ככל שקיים לגבי הלקוח מידע אישי רב יותר. כמו כן, איסוף מידע לגבי יחידים יאפשר לקובעי המדיניות לבחון, באמצעות השוואת תנאי האשראי שמקבלים פלחים שונים באוכלוסייה, האם מתקיימת בפועל אפליית אשראי, וכן לערוך בקרה על רמות הסיכון של הלוחים השונים. בלא איסוף מידע שיטתי על חובות משקי בית, לא ניתן לאמוד מהו היקף האשראי שמקבלות קבוצות שונות באוכלוסייה".

לבסוף יצוין, כי במסגרת **סעיף 2(א) לחוק הבנקאות (שירות ללקוח), התשמ"א-1981**, נאסר על תאגידים בנקאיים לסרב "סירוב בלתי סביר" למתן שירותים שונים, כגון פתיחת חשבון עובר ושב בתנאים מסוימים, או מכירת שיקים בנקאיים.²⁷⁹ הגם שהחוק אינו נוקט במונח איסור הפליה, האיסור לסרב סירוב "בלתי סביר" עשוי להוות אף הוא חלק מהמסגרת לדיון במקרים מסוימים.²⁸⁰

אפליה במבט השוואתי

בהקשר הבינלאומי, נושא האפליה וההטיות על ידי מערכות בינה מלאכותית זכה להתייחסות הן במסגרות האסדרה הכלליות הן באופן פרטני בהקשר הפיננסי.

ראשית, במסגרת ה-EU AI Act, נושא ההטיות זכה להתייחסות בעיקר במסגרת הסעיף העוסק **בנתונים וממשל נתונים**, אשר נוגע למערכות בינה מלאכותית המסווגות על פי החוק כמערכות בסיכון גבוה.²⁸¹ במסגרת זו, נקבע כי מאגרי נתונים לאימון, תיקוף ובדיקה של מערכות בינה מלאכותית בסיכון גבוה יהיו כפופים לפרקטיקות של ממשל בינה מלאכותית וממשל נתונים. פרקטיקות אלה יכללו הן בחינה של הטיות אפשריות, שעשויות, בין היתר, להשפיע באופן שלילי על זכויות יסוד או להוביל לאפליה אסורה על פי חוקי האיחוד האירופאי, במיוחד כאשר פלט הנתונים משפיע על קלט עבור פעולות עתידיות (כלומר, Feedback loop); והן נקיטת אמצעים מתאימים לאיתור, מניעה וצמצום של הטיות אפשריות שזוהו.

לצד זאת, בכל הנוגע ל**מאגרי הנתונים** לאימון, אימות ובדיקה – ה-EU AI Act קובע, בין היתר, כי אלה צריכים להיות רלוונטיים, מייצגים באופן מספק (representative), וככל האפשר – גם חפים מטעויות ושלמים ביחס למטרה המיועדת.²⁸² עוד נקבע כי המאגרים צריכים להיות בעלי מאפיינים סטטיסטיים ראויים ביחס לקבוצה או לאדם שביחס אליהם המערכת בסיכון גבוה צפויה להיות בשימוש.²⁸³ כמו כן, ה-EU AI Act קובע הוראות בדבר הנתונים שבהם ניתן לעשות שימוש לצורך גילוי ותיקון הטיות במערכת, לרבות נתונים אישיים במידה שהדבר הכרחי לחלוטין.²⁸⁴

נושא **ההטיות** זכה להתייחסות גם בסעיף העוסק בדיוק, חוסן ואבטחת סייבר,²⁸⁵ שם נקבע כי ככלל, מערכות בינה מלאכותית בסיכון גבוה יתוכננו ויפותחו באופן שיגיעו לרמה מתאימה של דיוק, חוסן, ואבטחת סייבר, וכי הן יפעלו באופן עקבי בתחומים אלה לאורך כל מחזור החיים שלהן.

למרות שה-EU AI Act הוא חוק כללי, בנוגע למערכות המשמשות להערכת **דירוג אשראי** או **זכאות לאשראי**, המסווגות על פי החוק האירופאי כמערכות בסיכון גבוה – הוסבר בדברי המבוא לחוק במפורש כי אלה עלולות להביא לאפליה בין אנשים או קבוצות, ולהנציח דפוסים היסטוריים של אפליה, דוגמת אפליה על בסיס מוצע גזעי או אתני, מגדר, מוגבלויות, גיל או נטייה מינית, וכן עלולות ליצור שונות של תוצאות מפלות (discriminatory impacts).²⁸⁶

בהקשר הפיננסי, בדוח ה-OECD משנת 2021 זכה נושא ההטיות והאפליה להתייחסות מקיפה. במסגרת הדוח נקבע כי ייתכן שקובעי המדיניות יצטרכו לחדד את מאגר הכלים הקיים שלהם להתגוננות מפני סיכונים הנובעים, או מחריפים, מהשימוש בבינה מלאכותית, במספר תחומים. בכלל זאת, בתחום האפליה וההטיות הומלץ כך:²⁸⁷

279 ראו בהקשר זה, ברק מדינה "איסור הפליה במגזר הפרטי מנקודת מבט של תיאוריה כלכלית" עלי משפט ג (תשס"ג).

280 ראו למשל טענת המשיבים בעניין טמיר, וכן הדיון בת"א (ת"א) 29979-08-14 רינסנס בית ספר בע"מ נ' בנק מסד בע"מ, פס' 35 לפסק הדין (2.8.2017).

281 EU AI Act, Article 10 – Data and data governance.

282 סעיף 10.3. כמו כן, בסעיף 67 לדברי המבוא לחוק הוסברה החשיבות של מאגרי נתונים: High-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it **does not become a source of discrimination prohibited by Union law**. High-quality data sets for training, validation and testing require the implementation of appropriate data governance and management practices. Data sets for training, validation and testing, including the labels, should be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose of the system.

283 EU AI Act, בסעיף 10.3.

284 EU AI Act, בסעיף 10.5.

285 EU AI Act, בסעיף 15.

286 ראו פס' 58 לדברי ההסבר: "AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of **discriminatory impacts**."

287 דוח ה-OECD משנת 2021, בעמ' 59-60.



"Promote practices that will help overcome risk of unintended bias and discrimination.

In addition to efforts around data quality, safeguards could be put in place to provide assurance about the robustness of the model when it comes to avoiding potential biases. Appropriate sense checking of model results against baseline datasets and other tests based on whether protected classes can be inferred from other attributes in the data are two examples of best practices to mitigate risks of discrimination. The validation of the appropriateness of variables used by the model could reduce a source of potential biases."

בדוח IOSCO משנת 2021, אחד הצעדים שעליהם הומלץ בתחום האפליה הוא כי הרגולטורים ישקלו לדרוש מחברות לקיים **מנגנוני בקרה** מתאימים, כדי להבטיח שהנתונים שעליהם מסתמכות המערכות הם באיכות מספיקה כדי למזער הטיית, ורחבים מספיק לצורך יישום מבוסס של המערכות. עוד הומלץ לגופים הפיננסיים לוודא כי הן מאגרי הנתונים והן התפוקות של המערכות – מנותחים ביחס לסיכונים אפליה. כמו כן, על חברות להיות בעלות תהליכי בקרה מתאימים, לצורך זיהוי והסרת הטיית לא מוצדקות ממאגרי הנתונים. עוד הומלץ לשקול קיום קורסי הכשרה פרטניים לגורמים הרלוונטיים (data scientists, and/or other relevant staff) על מנת להעלות מודעות לפוטנציאל ההטיית.²⁸⁸

בארצות הברית, התשתית החוקית בתחום האפליה בסקטור הפיננסי רחבה, וישנם חוקים העוסקים באיסור אפליה בתחומים פיננסיים באופן פרטני. במסגרת זו, ה-FTC (Federal Trade Commission) פרסם גילוי דעת תחת הכותרת "Aiming for truth, fairness, and equity in your company's use of AI",²⁸⁹ שבו הובהר כי חוקים קיימים הנוגעים בין היתר לשוויון ומניעת אפליה – הנם משמעותיים גם עבור מפתחי ומשתמשי בינה מלאכותית. בהקשר זה, גילוי הדעת מתייחס להוראות החוקים הבאים, שיש להם חשיבות עבור מפתחים ומשתמשים במערכות בינה מלאכותית: סעיף 5 ל-FTC Act (חוק נציבות הסחר הפדרלית) האוסר על שיטות מטעות או לא הוגנות; חוק דיווח אשראי הוגן (Fair Credit Reporting Act) FCRA; וכן ההסדר המעוגן בחוק שוויון הזדמנויות באשראי, ה-ECOA (Equal Credit Opportunity Act), מכוחו לא ניתן להשתמש באלגוריתם מוטא, שגורם לאפליה באשראי על בסיס קטגוריות כגון גזע, צבע, דת וכו'.²⁹⁰

לצד סקירת החוקים שעשויים לחול במקרה של אפליה על ידי מערכות בינה מלאכותית בסקטור הפיננסי, גילוי הדעת כולל המלצות שונות ביחס להימנעות מהטיית או תוצאות לא הוגנות אחרות. כך למשל, בכל הנוגע לנתונים, הומלץ לחשוב על שיטות לשיפור מערכי נתונים, וכן הומלץ להגביל את השימוש במודלים במקרים המתאימים. בנוסף, הומלץ להיזהר מתוצאות מפלות, תוך בחינת האלגוריתמים הן לפני השימוש בהם והן באופן עיתי לאחר מכן, כדי לוודא שהם אינם מפלים על בסיס קריטריונים מוגנים. בנוסף, הומלץ לקדם שקיפות ועצמאות, למשל תוך פרסום תוצאות של ביקורות בלתי תלויות, או פתיחת הנתונים או הקוד לבחינה חיצונית.

בגילוי דעת נוסף מטעם ה-FTC, שכותרתו "Using Artificial Intelligence and Algorithms",²⁹¹ הובהר בין היתר כי לשם בחינת אפליה בלתי חוקית, נבחנים על ידי ה-FTC הנתונים המוזנים למודל (inputs), לרבות באמצעות פרוקסי, וכן התוצאות שאליהן הוביל המודל. במסגרת זו, נבחן האם המודל הוביל לתוצאות מפלות בפועל, והאם למודל שנחזה כניטרלי יש השלכות מפלות על קבוצות מוגנות. ככל שיאותרו תוצאות מפלות, נבחנת ההצדקה של הגופים הפיננסיים לעשות שימוש במודל זה, והאם אלטרנטיבה מפלה פחות הייתה מגיעה לאותן תוצאות.

יצוין כי הדגש שהושם על בחינת **התוצאות** שאליהן הגיעה מערכת הבינה המלאכותית, בהקשר של הדין הפיננסי בארה"ב (כמו גם בדוח ה-OECD משנת 2021 כאמור) – מהווה מענה מסוים לאתגר שפורט לעיל בנוגע לקושי לזהות שימוש קונקרטי במאפיינים זהותיים מוגנים על ידי מערכות בינה מלאכותית, בשל אופן פעילותן המורכב של מערכות אלה (בשל השימוש במשתני "פרוקסי" או תופעת "הקופסה שחורה"). בהתאם לדוקטרינות כגון אפליה

288 דוח IOSCO משנת 2021.

289 <https://privacysecurityacademy.com/wp-content/uploads/2021/04/Aiming-for-truth-fairness-and-equity-in-your-companys-use-of-AI.pdf>

290 ה-Equal Credit Opportunity Act (ECOA), שנחקק בשנת 1974, מונה רשימה של פעולות שיהיו אפליה ביחס לעסקאות אשראי, על בסיס גזע, צבע, דת, מוצא לאומי, מין, מצב משפחתי, גיל, והעובדה שהכנסתו של המבקש נובעת מתכנית סיוע ציבורית. לצד זאת, החוק מונה שורה של פעולות שלא יהיו אפליה, דוגמת בדיקה של מצב משפחתי או גיל, אם הבירור נוגע להיבטים נדרשים שונים המפורטים בחוק, ולא על מנת להפלות.

291 Andrew Smith, Director, FTC Bureau of Consumer Protection, Using Artificial Intelligence and Algorithms (April 8, 2020).



עקיפה או אפליה תוצאתית,²⁹² אשר פותחו באופן נרחב בהקשרים שונים במשפט האמריקאי (Disparate impact לעומת Disparate treatment), ואף יושמו בהקשרים שונים במשפט הישראלי –²⁹³ הבחינה מתמקדת בשאלה האם במבחן התוצאה ישנה הפליה אסורה כלפי קבוצות מוגנות.²⁹⁴

עוד בארה"ב, בתחום האשראי, המשרד להגנת הצרכן הפיננסי (CFPB) פרסם חוזר המחייב גופים מפקחים להסביר ללקוחות את הסיבות המדויקות להחלטות שליליות נגדם בהתאם ל-ECOA, ללא תלות בטכנולוגיה שבה נעשה שימוש. בכלל זאת הובהר כי לא ניתן שימוש במודלים אלגוריתמיים מורכבים (למשל, הכוללים קופסה שחורה), ככל שהם לא מאפשרים למסור במדויק את הסיבות לשלילת אשראי או פעולות שליליות אחרות.²⁹⁵

לצד הבהרות אלה, ה-CFPB פרסמה מסמך הבהרה משותף יחד עם סוכנויות פדרליות אחרות לגבי מאמצי אכיפה ביחס לאפליה או הטיות במערכות אוטומטיות, בו הובהר כי הסמכויות המשפטיות הקיימות – חלות גם ביחס למערכות אלה.²⁹⁶

גם **באנגליה**, פורסמו מספר דוחות ומדריכים הנוגעים בין היתר לאפליה והטיות על ידי מערכות בינה מלאכותית. כך, ה-ICO, לשכת נציבות המידע (Information Commissioner's Office) פרסמה מדריך מוגש, שעודכן לאחרונה בחודש מרץ 2023, הכולל מידע נרחב הנוגע לאתגרים ולדרישות החוק בנוגע למערכות בינה מלאכותית, ובכלל זאת בהיבטי הטיות ואפליה.²⁹⁷ קודם לכן, בחודש ספטמבר 2021, פרסם המשרד לדיגיטל, תרבות, מדיה וספורט באנגליה, דוח תחת הכותרת "Data: A new direction", העוסק באופן נרחב בין היתר **בהוגנות** של מערכות בינה מלאכותית, בשלושה מעגלים – אפליה של ממש, הטיות, והוגנות למשל במישור התהליכי ובהיבט יכולת הפרט להבין או לאתגר החלטות המתקבלות בעניינם.²⁹⁸

כלי התמודדות עם אפליה

בעוד שניתן להתרשם כי חלק מהמלצות הגופים הבינלאומיים השונים שהובאו לעיל מתוות מסגרות עקרוניות לבחינה וניטור של מערכות בינה מלאכותית כדי להתמודד עם חששות להטיות ואפליה, גופים וגורמים שונים מנסים להתוות פרקטיקות מומלצות להתמודדות עם אתגר זה, שיוכלו לשרת בין היתר מפתחים ומטמיעים של מערכות בינה מלאכותית.

כך למשל, המכון הלאומי לתקנים ולטכנולוגיה בארה"ב, NIST (National Institute of Standards and Technology), פרסם מסגרת חברתית-טכנית ראשונית בנושא הטיות בבינה מלאכותית, הכוללת המשגה יסודית, מיפוי האתגרים המרכזיים, וכיוונים מרכזיים להנחיות עתידיות. המסמך מתאר את האתגרים בתחום האפליה בשלושה תחומי ליבה, ומציע קווים מנחים להתמודדות עמים: מאגרי מידע; בדיקה, הערכה תיקוף ואימות (test and evaluation, validation, and verification (TEVV); וגורמים אנושיים (הטיות חבריות והיסטוריות; גישה של האדם במרכז, ומעורבות אנושית).²⁹⁹ כפי שנראה להלן, NIST פרסם מספר מדריכים נוספים בהקשרים דומים.

292 ראו בהקשר זה Talia B. Gillis, The Input Fallacy, 106 Minn. L. Rev. 1175 (2022), https://scholarship.law.columbia.edu/faculty_scholarship/3312. גיליס מדגימה כיצד בחינה של אפליה בתוצאה, יכולה לסייע הן בבחינה של אפליה כ"השפעה מפלה", והן בבחינה האם מאפיין מוגן שימש כקריטריון, כאשר לא ניתן לענות על שאלה זו ישירות – "Considering whether 'similarly situated' borrowers were treated differently provides the second-best way of analyzing whether a protected characteristic was used as a criterion when this question cannot otherwise be answered directly". וראו גם המחשה לגבי האופן שבו ניתן לערוך בחינה תוצאתית בתחום האשראי בעמוד 1245-1246.

293 על ההבחנה בין אפליה עקיפה ואפליה ישירה, ראו טליה שטיינר שוכרים אי שוויון – התמודדות עם אפליית ערבים בשוק העבודה הישראלי מחקר מדיניות 97, המכון הישראלי לדמוקרטיה (2013), <https://www.idi.org.il/media/3434/pp97.pdf>; וכן ראו ע"א 7308/19 טמיר נ' בנק הפועלים בע"מ, בפסקה 12 לפסק דינו של השופט עמית וההפניות שם (להלן: "עניין טמיר").

294 בהקשר זה, יצוין כי חוק איסור הפליה מונה מספר תרחישים, בהתקיימם מועבר נטל ההוכחה לנתבע, שנדרש להוכיח כי הוא לא פעל בניגוד לסעיף 3 במסגרת הליכים אחרניים. כך, למשל, במקרה שבו הנתבע סירב לספק מוצר או שירות ציבורי לאדם הנמנה על קבוצה חשודה, ולא סירב באופן נסיבות למי שלא נמנה על קבוצה כזו – יהא עליו להוכיח כי לא הפר את הוראות סעיף 3.

295 Consumer Financial Protection Circular 2022-03 <https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms>, וכן ראו Consumer Financial Protection Circular 2023-03, לגבי השימוש בטפסים שמספקת ה-CFPB בהקשר זה.

296 ראו ה"ש 72 לעיל.

297 <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>

298 Data: a new direction – government response to consultation, <https://www.gov.uk/government/consultations/data-a-new-direction>

299 NIST Special Publication 1270 Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, <https://www.nist.gov/publications/towards-standard-identifying-and-managing-bias-artificial-intelligence>

דוגמה נוספת ניתן למצוא בסינגפור, שם פורסם ה-“AI Verify” – מסגרת עקרונות וארגז כלים טכני (Toolkit) לבדיקות מערכות בינה מלאכותית, המאפשרת לארגונים לבחון באופן עצמאי את הביצועים של מערכות בינה מלאכותית, כדי לוודא שהן עומדות בעקרונות בינלאומיים מוכרים ובכלל זאת הגינות והימנעות מאפליה.³⁰⁰ ארגז הכלים הוא חבילת תוכנה הניתנת להורדה, שניתן ליישם ולהפיק באמצעותה דוחות בדיקה למערכות בינה מלאכותית.

בעולם מתפתחים כלי בקרה (כלי Audit) – לרבות באמצעות טכנולוגיות בינה מלאכותית – שמטרתם לבחון באופן שיטתי ועקבי האם מערכות בינה מלאכותית לוקות בהטיות או באפליה. כלים טכנולוגיים יכולים אפוא לסייע לתהליכי הבקרה של מפתחים או גופים פיננסיים המטמיעים מערכות אלה, וכן לרגולטורים עצמם במסגרת הליכי הפיקוח.

ריכוז נגיש של כלים ומדדים שונים בהקשר זה, מצוי באתר האינטרנט של ה-OECD. הארגון פרסם **קטלוג**, הכולל כלים ומדדים שונים, שנועדו לסייע לשחקנים השונים לפתח ולהטמיע מערכות בינה מלאכותית אמינות. במסגרת הקטלוג מרוכזים כלים שונים ומגוונים להתמודדות עם האתגרים הנוגעים למערכות בינה מלאכותית – החל מכלים טכניים, דוגמת קודים ותוכנות, בין היתר לצורך זיהוי הטיות ועוד, דרך כלים פרוצדוראליים, דוגמת הנחיות או כלי ניהול סיכונים, וכלה בכלים חינוכיים דוגמת תוכניות הדרכה וחומרים חינוכיים.³⁰¹

במסגרת הערות הציבור לדוח הביניים הובעה גישה אחת המדגישה את אתגר ההבחנה בין נתונים שניתן לעשות בהם שימוש לגיטימי ובין נתונים המהווים אפליה אסורה, וכפועל יוצא מכך את הצורך בקיום בקרה ושקיפות כפי שהוצע בדוח. עוד צוין, כי פיתוח ההלכה הפסוקה בעניין זה בבתי המשפט צפוי להיעשות בקצב איטי מזה של התפתחות הבינה המלאכותית, ועל כן על הרגולטור לקחת תפקיד מרכזי בהובלת הדיון הציבורי בנדון. הצוות מסכים עם גישה זו, והדבר בא לידי ביטוי בהמלצותיו בדבר בקרה ונקיטת אמצעים לכל אורך חיי המערכת וכן בנוגע לנקיטת פעולות רגולטוריות להכוונת הגורמים המפוקחים.

גישה שונה שהוצגה במסגרת הערות הציבור היתה כי הסיכונים בנושא הטיה ואפליה אינם ייחודיים למערכת הפיננסית, ועל כן לא נדרשת רגולציה נוספת מזו הקיימת. לפי גישה זו, כיוון שהדוח אינו קובע באופן ברור את היקף הבקורות ונחיצותן, התוצאה עלולה להיות עלויות משמעותיות וקושי בהטמעת מערכות בינה מלאכותית. בהקשר זה סבור הצוות, כי הדוח מפרט את הבעיות הייחודיות לבינה מלאכותית בהקשר של הטיה ואפליה, כגון הישענות גדולה יותר על מאגרי מידע לא מייצגים, אופן עיצוב האלגוריתם, ושימוש בנתוני “פרוקסי” שאינם מפלים כשלעצמם אך עלולים להיות בעלי קורלציה למשתנים מפלים. על כן, יש הצדקה לנקוט אמצעים נוספים כפי שהוצע בדוח הביניים. זאת כמובן כאשר עולה צורך בכך, ובהתאם גם לדין הקיים. הערה נוספת עסקה בכך שהדין עצמו אינו בהיר לעתים – לדוגמה בהבהרת הגבול שבין הבחנה מותרת ואפליה אסורה בהקשר של ביטוח רכב. נקודה זו נכונה לדעת הצוות, ניתן לה ביטוי בדוח, ואכן יהיה מקום לשקול לעסוק עוד גם במישור בסיסי זה, לשם הבהרת הדין.

בהמשך לשאלה שהעלה הצוות בדוח הביניים, בדבר יעילות והיתכנות הטמעת דוקטרינה של אפליה עקיפה או אפליה תוצאתית, התקבלו תגובות בדבר הערך שעשוי להיות לדוקטרינה זו הן לגופים הפיננסיים הן ללקוחותיהם. לנוכח השלכות הרוחב של אימוץ דוקטרינה כאמור, מעבר לתחום הפיננסי, הדוח אינו מתייחס לכך ישירות אך נכללה בו התייחסות לבקרה תוצאתית כמענה לקשיים שעשויים להתגלע בזיהוי שימוש פסול בקריטריון מוגן (למשל בשל השימוש במשתני “פרוקסי”, או בשל סוגיית “הקופסה השחורה”).

³⁰⁰ <https://aiverifyfoundation.sg> וכן ראו הסבר באתר ה-OECD, “Singapore’s A.I. Verify builds trust through transparency”, <https://oecd.ai/en/wonk/singapore-ai-verify>.

³⁰¹ OECD, Catalogue of Tools & Metrics for Trustworthy AI, <https://oecd.ai/en/>.



המלצות בנושא אפליה

1. תחולת דיני האפליה – הדין בנושא אפליה בישראל הוא דין קיים ובכל הנוגע לגופים פרטיים עקרון השוויון ואיסור האפליה מוסדרים בעיקר בחוק איסור הפליה, הכולל התייחסות מפורשת לשירותים פיננסיים כשירותים ציבוריים (בנקאות, מתן אשראי וביטוח) ובדינים ספציפיים נוספים, כמפורט לעיל. **הפעולות וההחלטות של גופים כפופים לאיסור האפליה ללא קשר לטכנולוגיה שבה הם עושים שימוש ועל כן מובן כי כך הדבר גם כאשר נעשה שימוש במערכות בינה מלאכותית.**

2. נקיטת פעולות להכוונת הגורמים המפוקחים – השימוש במערכות הבינה המלאכותית עלול ליצור סיכונים לפגיעה בשוויון בין היתר בשל החשש שהפגיעה תהיה נסתרת, לא מודעת או קשה לאיתור. כך למשל, כמפורט לעיל, דרכי הפעולה של מערכות בינה מלאכותית עלולות להקשות על זיהוי מצב שבו מי למעשה נעשה שימוש פסול בקריטריון מוגן, למשל בשל השימוש במשתני "פרוקסי", או בשל סוגיית "הקופסה שחורה". על כן נדרשת זהירות מיוחדת ובקרה ביחס להיבטים אלה בעת השימוש בבינה מלאכותית.

על רקע זה, ובדומה לנעשה בחו"ל, מוצע כי הרגולטורים הפיננסיים ישקלו **פעולות להכוונת הגורמים המפוקחים** ולהטלת חובות מתאימות במסגרת הסמכויות הנתונות להם – למשל באמצעות הנחיות, גילויי דעת והבהרות (לרבות בעקבות בירורים שנערכו לגבי פניות ציבור, פסיקה והנחיות שניתנו בעניינים אלה). זאת ככלל וביתר שאת ביחס לפעולות פיננסיות משמעותיות עבור הפרט כגון דירוג אשראי וחיתום ביטוח מסוגים מסוימים. זאת על מנת לצמצם את הסיכון לאפליה (ישירה או עקיפה, מכוונת או לא מודעת), לעודד יצירת סביבה בטוחה, הוגנת ואחראית בעת הכנסת מערכות בינה מלאכותית ולהגביר את הוודאות הרגולטורית. סוגיות מרכזיות שמוצע לעסוק בהן במסגרת זו, הן **בקרה ונקיטת אמצעים** לזיהוי ומניעת הטיות לכל אורך חיי המערכת (ראו המלצה בהמשך), ובפרט ביחס **לתוצאות** שאליהן מגיעה המערכת.

3. בקרה ונקיטת אמצעים לכל אורך חיי המערכת – נוכח הנטייה של מערכות בינה מלאכותית לאפליה והטיות, נדרשת בקרה מוגברת, מתועדת ושקופה לכל אורך חיי המערכת, לרבות בשלבי ההטמעה והיישום, במטרה להתמודד עם הסיכון להטיות ולאפליה. מומלץ להנחות ולתת הוראות למפוקחים לפעול בכל הנוגע להיבטים המרכזיים שלהלן, לערוך בקרה, לתעד את ממצאיה ולפעול לתיקון של פגמים שנתגלו:

א. **מאגרי נתונים** – יש לדאוג לכך שמאגרי המידע המשמשים לאימון, תיקוף ובחינת המערכות, יהיו מאגרים מייצגים ומגוונים, שאינם מוטים, וכי הם יכללו מידע רלוונטי על האוכלוסיות שלגביהן המערכות תקבל החלטות.

ב. **אופן פעילות המערכת** – יש לבחון את פעילות המערכות באופן שוטף, גם בשלב ההטמעה והיישום, על מנת להימנע מהסתמכות של המערכות על קריטריונים מוגנים שעשויים להוביל לאפליה, לרבות באמצעות פרוקסי.

ג. **תוצאות המערכת** – בחינת הטיות ואפליה בתוצאות המודל, למשל תוך בחינה האם ניתן בפועל יחס מפלה לאוכלוסיות שונות בעלות נתונים דומים.

4. בקרה תוצאתית – בהמשך להמלצה הקודמת, מאחר שמערכות בינה מלאכותית נעדרות לעיתים הסברתיות פרטנית, או שעולה חשש לגביהן כי לא יזוהה שימוש במשתני "פרוקסי", מוצע לנקוט בכלים של בקרה תוצאתית, בין השאר, לצורך בחינת טענות לאפליה (או להיעדרה). כלים אלה יכולים לסייע בידי הגורם המפוקח והרגולטור בזיהוי אפליה במערכות אשר על פניו פעולתן עשויה להיראות נייטרלית וללא שימוש בנתונים מפלים. אין בכך כדי להחליף את השימוש בכלי בקרה אחרים כפי שצוין לעיל, למשל בנוגע לייצוגיות מאגר המידע או להנחיית המערכת להימנע משימוש בנתונים מפלים, אלא לבוא בנוסף להם.

5. הסברתיות – הסברתיות, ובעיקר הסברתיות פרטנית ביחס להחלטה ספציפית, היא אחד הכלים האפשריים להתמודדות עם הסיכון לאפליה. כך, הסברתיות יכולה לאפשר לוודא כי המערכת לא התבססה על קריטריון זהותי מוגן באופן מפלה, וכן לאפשר בקרה חיצונית על ידי הציבור, הצרכנים או הרגולטור ביחס לפעילות המערכת (וראו הפרק העוסק ב"קופסה שחורה" והסברתיות).



אחריות

סוגיית האחריות היא אחת הסוגיות המדוברות בהקשר של מערכות בינה מלאכותית. הסוגיה אינה מתמצה בשאלה על מי תוטל האחריות המשפטית אם נגרם נזק למשתמש (liability), אלא נוגעת גם לשאלה הכללית יותר, מיהו הגורם האחראי (responsible/accountable) על מערכת בינה מלאכותית. במילים אחרות, הדיון בסוגיית האחריות אינו מתמקד רק בשאלות מתחומי המשפט האזרחי או הפלילי, אלא גם בשאלה על מי ראוי ויש להטיל אחריות בהקשרים הרגולטוריים.

יצוין כבר עתה, כי בפרק זה לא נתמקד בתחולת דיני הנזיקין הכלליים בהקשרי בינה מלאכותית, אלא נבקש למקד את הדיון באחריות לעמוד בחובות רגולטוריות המוטלות על מערכות בינה מלאכותית ככאלה, ובחובות הרגולטוריות הכלליות מתחום הפיננסיים (בפרק אחר נעסוק בשאלת האחריות לאפליה). הצידוק להפרדה זו נובע, בין היתר, מכך שדיני הנזיקין והדין הפלילי חולשים על מגוון תחומי פעילויות בהקשרי בינה מלאכותית ומביאים בחשבון שיקולים רחבים יותר מאשר אלה הנוגעים לתחום הפיננסי. הצורך בעדכון ופרשנות דינים אלה בוודאי יידון על ידי המחוקק וקובעי המדיניות בהקשרים רחבים יותר של אסדרת בינה מלאכותית והוא יחול בהתאם גם על התחום הפיננסי, וממילא חורג מגבולות דוח זה.

סוגיית האחריות מתחדדת בהקשרי מערכות בינה מלאכותית בראש ובראשונה בשל היעדר גורם אנושי בעל שיקול דעת, או צמצום מקומו, בתהליך קבלת ההחלטות. האסדרה המשפטית הנפוצה מבוססת על פי רוב על אחריות של גורם אנושי למילוי חובות ובוחנת את התנהלותו ושיקול דעתו במקרה של טענות להפרה. בעידן הבינה המלאכותית תפקידו של הגורם האנושי מצטמצם ולעיתים אף אינו מוגדר. בהיעדר מעורבות אנושית לאורך שרשרת קבלת ההחלטות, כולה או חלקה, מתערער המבנה המשפטי המוכר של הטלת אחריות, אשר הושתת, היסטורית, על הימצאותו של אדם או תאגיד במוקד ההתרחשות, אשר ככלל נושא באחריות למעשיו.³⁰²

סוגיית האחריות מתחדדת גם לנוכח המאפיינים האוטונומיים והאוטונומיים של המערכות, וכן מפני שלעיתים מדובר בשילוב של מספר מערכות וגורמים המובילים לתוצר שהציבור עושה בו שימוש. כך למשל, עולות שאלות מהו סטנדרט ההתנהגות המצופה ממערכת בינה מלאכותית; האם ניתן לייחס ידיעה או אמונה למערכת מחשב; וכדומה. הדברים באים לידי ביטוי גם בהקשרים הפיננסיים. כך, למשל, בסעיף 2 לחוק הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, תשנ"ה-1995, נקבע כי רק אדם בעל רישיון מתאים רשאי לעסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקים, ובסעיפים 11 ו-20 נקבעו חובות האמון והזהירות (בהתאמה) באשר לבעלי רישיון, וגם שם נדרשות תכונות אנושיות כגון ביצוע פעולות "באמונה ובשקידה" או מבחן "בעל הרישיון הסביר". באופן דומה, גם בחוק הפיקוח על שירותים פיננסיים (ייעוץ, שיווק ומערכת סליקה פנסיוניים), תשס"ה-2005 (להלן: "חוק הייעוץ הפנסיוני") נקבעה הוראה דומה ביחס לעיסוק בייעוץ פנסיוני, וכך גם באשר לחובות האמון והזהירות (סעיפים 15 ו-16 לחוק הייעוץ הפנסיוני).

גישות אפשריות לקביעת אחריות

חרף ההסכמה בנוגע לצורך בהגדרת תחומי האחריות של הגורמים הרלוונטיים שלהם מעורבות ב"מחזור החיים" של מערכות הבינה המלאכותית, קיימות גישות שונות לגבי אופן חלוקת האחריות בין הגורמים השונים. נציג בקצרה מספר אפשרויות מרכזיות לשחקנים עליהם ניתן להטיל אחריות וההצדקות לכך:

מפתח האלגוריתם (provider) – הכוונה היא למפתח המערכת, מי שאחראי על כתיבת הקוד או האלגוריתם. מערכות בינה מלאכותית מתאפיינות במורכבות טכנולוגית רבה. הגורם שפיתח את המערכת הוא בעל הידע הרב ביותר לגבי אופן פעולתה, מנגנון קבלת ההחלטות שהוטמע בה ונקודות התורפה שלה, ולכן ניתן לראות בו הגורם היעיל ביותר ללקיחת אחריות על פעילות המערכת. כמו כן, מפתח המערכת הוא בעל יכולת לצפות את הסיכונים העיקריים אשר עלולים להיגרם כתוצאה משימוש במערכת ולקבוע מראש מנגנונים אשר יפחיתו או ימנעו את התממשותם.

מנגד, ניתן למנות מקרים בהם זיקתו של המפתח למערכת פוחתת, ולכן הטלת אחריות על המפתח מעוררת קשיים.

302 מסמך המדיניות, בעמ' 62.

לדוגמה, ככל שהמערכת אוטונומית יותר ובעלת יכולות למידה עצמית, פוחתת יכולתו של המפתח לצפות את התקיימות הסיכונים הכרוכים בשימוש בה. למשל, מערכת בינה מלאכותית מבוססת למידת מכונה המיועדת למסחר בבורסה עלולה לאמץ טכניקות של מסחר בלתי חוקיות, וזאת מבלי שלמפתח הייתה אפשרות ממשית לחזות זאת. בדומה לכך, ככל שהמערכת כללית יותר ביישומיה, כך קשה יותר למפתח לצפות את הסיכונים הנובעים מיישום מסוים זה או אחר, לרבות במצב בו נעשו במערכת התאמות לצורך שימוש ספציפי. זאת ועוד, קיימת אפשרות שמפתחי המערכת אינם יכולים לטפל בתוכן בעייתי המוזן למערכת. פעילותן של מערכות בינה מלאכותית מבוססת במידה רבה על בסיס הנתונים שעליו המערכת מתאמנת, ובהקשר זה ישנה חשיבות לייצוגיות, איכות ומהימנות הנתונים. כאשר למפתח אין שליטה על בסיס הנתונים המזינים את המערכת (למשל, בשל הזנת נתונים נוספת על ידי המשתמש), קיים קושי בהטלת האחריות עליו, לנוכח יכולתו המוגבלת לצפות, למנוע או להפחית את הנזקים, משום שהוא כבר אינו הגורם היעיל ביותר לשליטה על המערכת.

מפעיל המערכת (deployer) – הכוונה היא לגוף העושה שימוש בבינה מלאכותית במסגרת עסקיו, בין לצרכיו הפנימיים של התאגיד ובין לצורך מתן שירות ללקוחותיו. הגוף העסקי אינו בהכרח גורם פסיבי המנגיש את השימוש במערכת מבוססת בינה מלאכותית, אלא הוא שהחליט לעשות שימוש בבינה מלאכותית, בחר במערכת עצמה, החליט על אופי השימוש בה, ולעיתים קרובות אף ערך (או ביקש שיערכו) בה שינויים לצרכיו. כאשר גוף עסקי בוחר להפעיל מערכת מבוססת בינה מלאכותית לשם ביצוע פעולות וקבלת החלטות, לרבות תמיכה בקבלת החלטות (ובפרט כאשר בתהליך ההטמעה בתאגיד בוצעו שינויים במערכת), ניתן לומר שמפעיל המערכת הוא בבחינת הגורם היעיל בשליטה על המערכת, וכן בעל היכולת הטובה ביותר לצפות את הנזקים ולפעול למניעת או הפחתת ההסתברות להתרחשותם. זאת ועוד, הטלת אחריות על מפעילי המערכות עשויה לתמרץ שחקנים אלו להבטיח הטמעה, שימוש ופיקוח נאותים, לרבות בהיבטי בדיקות נאותות למערכות, ניטור ופיקוח, ממשל תאגידי ראוי וכדומה.

יחד עם זאת, במקרים בהם מפעילי המערכות עושים שימוש במערכות בינה מלאכותית מבלי לבצע בהן כל שינוי, כל שכן שינוי מהותי, ובפרט שהמערכות לא ניזונות מבסיסי נתונים השייכים לאותם גופים עסקיים, ניתן לטעון כי במקרים אלו מפעילי המערכת אינם הגורם היעיל ביותר למניעת הנזק. גם הם עשויים לטעון כי אינם יכולים להיות אחראים לפעולות של המפתחים או המשתמשים.

משתמש הקצה (end user) – ניתן לחשוב על נסיבות בהן ניתן לייחס למשתמש הקצה אחריות לנזק שאירע לו, במיוחד במקרים בהם יש ללקוח הקצה "אשם תורם" בגרימת הנזק שנגרם לו או במקרים של פעילות חסרת אחריות במערכת, ביצוע פעולות בחוסר תום לב, הסתרה או אי גילוי מידע חיוני וכו'.³⁰³ יתרה מזאת, ניתן לחשוב על דוקטרינה משפטית הגורסת כי בעצם ידיעת הסיכונים הכרוכים בשימוש במערכות בינה מלאכותית, לוקח על עצמו משתמש הקצה גם את הסיכון וההשלכות הפוטנציאליות, לטובה או לרעה, בבחינת יזהר המשתמש (בהקבלה לדוקטרינת "יזהר הקונה").

גישה זו אינה נטולת קשיים, משום שיכולתו של לקוח הקצה להכיר את מלוא סיכוני המערכת, לשאול את מפתחיה שאלות, להבין את מורכבותה הטכנולוגית ובמקרה הצורך לבצע בה בדיקות היא מוגבלת מאוד עד בלתי אפשרית או בלתי ישימה, מה גם שבמרבית המקרים ללקוח הקצה לא תהיה נגישות לבסיס הנתונים המזין את המערכת. אימוץ דוקטרינה המטילה אחריות על משתמש הקצה עלולה להיות גורם מעכב בכניסת טכנולוגיות חדשות לשוק ולמנוע חדשנות בתחומי חיים רבים. בנוסף, אימוץ גישה המטילה את האחריות על משתמש הקצה, עלול להוביל להכנסה לשוק של מערכות בינה מלאכותית באופן לא אחראי, לא ראוי ולא הוגן, כאשר דווקא מי שפיתח או הטמיע את המערכות הללו בשוק אינו נדרש לתת דין וחשבון על כך.

גורם אנושי "הקרוב ביותר למוקד ההתרחשות" – אפשרות נוספת היא הטלת אחריות על גורם אנושי כפונקציה של מידת מעורבותו בתהליך קבלת ההחלטות, באופן המשתנה ממקרה למקרה. יחד עם זאת, בהטלת אחריות על הגורם האנושי שקיבל את ההחלטה בפועל או "הקרוב ביותר" למוקד ההתרחשות, קיימים קשיים בלתי מבוטלים. ראשית, בחינת זהות הגורם האנושי "הקרוב ביותר למוקד ההתרחשות" עשויה להיות מורכבת, ואי-קביעה מראש עלולה ליצור חוסר ודאות. שנית, גם בהנחה שניתן יהיה לקבוע מיהו גורם זה, תעלה השאלה בדבר יכולתו לבקר את המלצות המערכת, לסרב לקבל את המלצותיה או להתערב באופן כזה או אחר באופן בפעילותה. אפשרות זו גם לא פותרת מצבים בהם מערכות מבוססות בינה מלאכותית מקבלות החלטות באופן אוטומטי ואוטונומי, ללא מעורבות אנושית כלל. בנוסף, אפשרות זו יוצרת אי ודאות משמעותית ביחס לגורם האחראי ועלולה לייצר "אפקט מצנן" מפני שילוב המערכת בפעילות הגוף הפיננסי.

303 דוח אונ' תל-אביב, עמ' 104-103.



ישות משפטית נפרדת – חלופה נוספת היא הכרה במערכת מבוססת בינה מלאכותית כישות בפני עצמה, במנותק מהגורם אשר פיתח או הטמיע אותה. אפשרות זו מצריכה לעשות שימוש בקונסטרוקציה משפטית שעלולה לעורר קשיים לוגיים ופרקטיים וכן היא נעדרת כל ביסוס נכון לעת הנוכחית.³⁰⁴ ניסיונות מן העולם להכיר במערכות בינה מלאכותית כישויות נפרדות לצורך הטלת אחריות נזיקית עלו עד כה בתוהו.³⁰⁵

גורמים נוספים אשר ניתן להטיל עליהם את האחריות למערכות בינה מלאכותית הם גורמים אחרים המעורבים בשלבים שונים בפעילותן של מערכות בינה מלאכותית. כך, למשל, ניתן להטיל אחריות על היבואן של המערכת (importer) או המפיץ שלה (distributor) אם לא ביצעו את הבדיקות המצופות מהם בטרם הכנסת המערכת לשוק או הפצתה למשתמשי המערכות, וכן על צדדים שלישיים שהייתה להם נגיעה או מעורבות במערכות. אפשרות נוספת היא לאמץ גישה המסירה אחריות מכל אחד מהשחקנים המעורבים במערכות בינה מלאכותית. בשלב זה, ולאור האמור בהמשך חלק זה, אין צורך לדון לעומק בכל אחת מאפשרויות אלה.

אחריות למערכות בינה מלאכותית – סקירה בינלאומית

גישת **האיחוד האירופאי**,³⁰⁶ כפי שבאה לידי ביטוי ב-EU AI Act, היא משטר אחריות עיקרי שיחול על מפתחי מערכות מבוססות בינה מלאכותית וזאת כאשר מדובר במערכות המוגדרות כמערכות בעלות סיכון גבוה (High-Risk AI Systems). החוק נוקט בלשון provider אך הגדרתו של גורם זה עוסקת בעיקר במי שמפתח מערכות בינה מלאכותית.³⁰⁷ כך, למשל, בסעיף 8(2) a המתייחס לדרישות החלות על מערכות בינה מלאכותית בסיכון גבוה (ההדגשה אינה במקור):

"Where a product contains an artificial intelligence system, to which the requirements of this Regulation as well as requirements of the Union harmonisation legislation listed in Annex II, Section A apply, **providers shall be responsible for ensuring that their product is fully compliant with all applicable requirements required under the Union harmonisation legislation.**"

חובות מקיפות מוטלת על מפתחים של מערכות בינה מלאכותית כללית (General purpose AI) (סעיף 52C ו-52D לחקיקה האירופאית).

החוק האירופאי מבחין בין חובות שיחולו על שחקנים שלהם מעורבות במערכות בינה מלאכותית בטרם יציאתן לשוק, לבין חובות שיחולו על שחקנים לאחר שהמערכות נפרשו בשוק.

סעיף 16 לחוק האירופאי מפרט את החובות החלות על מפתחים של מערכות בינה מלאכותית בסיכון גבוה, בין היתר לאחר שכבר נעשה בהן שימוש בשוק. הן כוללות בין היתר חובות לוודא עמידה בחוקים ובדרישות הרלוונטיים, לבצע בקרת איכות למערכת, לשמור תיעוד מסודר, לבצע הערכת התאמה (conformity assessment), לבצע רישום של המערכת במרשם ייעודי, ועוד.

לצד הגישה הבסיסית לפיה האחריות למערכות מבוססות בינה מלאכותית מוטלת על המפתחים, בהתקיים נסיבות מסוימות גורמים נוספים שלהם מעורבות במערכות בינה מלאכותית (מפיצים, יבואנים, מפעילים וצדדים שלישיים) עשויים למצוא עצמם בבחינת מפתחי המערכות. זאת בין היתר אם ביצעו שינויים מהותיים במערכות הבינה המלאכותית (סעיף 28 לחקיקה האירופאית). בנוסף לכך, סעיף 29 לחקיקה האירופאית קובע חובות שונות המוטלות באופן ספציפי על מפעילי המערכות (deployers). אלה בין היתר חובות לעניין מעורבות אנושית, ממשל תאגידי, הנתונים המזינים את המערכת (כאשר למפעילי המערכות שליטה על נתונים אלה) וכדומה. ראוי להדגיש כי חלוקת האחריות המתוארת לעיל מתייחסת בעיקר לאחריות לחובות הרגולטוריות הנובעות מהצעת החקיקה הספציפית

³⁰⁴ מסמך המדיניות, עמ' 65-66.

³⁰⁵ https://www.washingtonpost.com/travel/2024/02/18/air-canada-airline-chatbot-ruling/?force_isolation=true

³⁰⁶ בפרק זה נתייחס להגדרת האחריות ביחס למילוי חובות רגולטוריות הכלולות ב-EU AI Act בהקשרים נזיקיים. האיחוד האירופאי מקדם דירקטיבה נפרדת שנועדה לעשות הרמוניזציה לדינים החלים במדינות האיחוד – <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>.

³⁰⁷ הגדרת provider ב-EU AI Act: 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge;



והיא אינה מתייחסת לדיני הנזיקין הכלליים (אם כי נעשית עבודה גם בהקשרים אלה, למשל, קידום דירקטיבה בנושא אחריות נזיקית בהקשרי בינה מלאכותית ועדכון הדינים בהקשרים של אחריות למוצרים פגומים).

בארה"ב לא נקבעה כאמור חקיקה רוחבית בתחום הבינה המלאכותית ונכון למועד כתיבת שורות אלה, גם לא חוקקו חוקים פדראליים העונים על סוגיית האחריות. יחד עם זאת, בכל הנוגע לרגולציה מדינתית בארה"ב, יש הצעות בנוגע להטלת האחריות על השחקנים השונים. ראו למשל במדינת קליפורניה, הצעת חוק AB No. 331 – Automated Decision Tools ("ADT") אשר במסגרתה מוצע להחיל דרישות הן ביחס למפעילי המערכות (deployers) והן ביחס למפתחי המערכות (developers) ב-ADT.

רשות הסחר האמריקאית (FTC) פרסמה באפריל 2021 גילוי דעת הכולל קווים מנחים להערכה של שימוש במערכות בינה מלאכותית לפי המסגרת החקיקתית הקיימת, קרי החובות המוטלות על גופים עסקיים כיום ימשיכו לחול גם תוך מתן השירותים בעזרת מערכות מבוססות בינה מלאכותית.³⁰⁸

בנוסף, בשנת 2023 פרסמה קבוצת רגולטורים בארה"ב הכוללת את ה-FTC הצהרה משותפת בה הודגש כי סמכויות האכיפה של רגולטורים אלו חלות על "מערכות אוטומטיות" אשר כוללות גם מערכות בינה מלאכותית, וכי הרגולציה הנוכחית תחול על אותן מערכות באותה מידה שהיא חלה על מערכות אחרות. יצוין כי ההחלטה המשותפת של הרגולטורים נוגעת לפיקוח הן על הפיתוח הן על השימוש של מערכות אוטומטיות וקידום חדשנות אחראית (responsible innovation), וכי על פי ההצהרה, בכוונת הגופים החתומים להפעיל את סמכויותיהם כדי להגן על זכויות הפרט בין שהפרות ייגרמו כתוצאה משימוש באמצעים מסורתיים ובין כתוצאה של טכנולוגיות מתקדמות.³⁰⁹ בנייר מדיניות של ממשלת בריטניה שנוגע לשימוש בבינה מלאכותית יוצרת על ידי גורמי ממשל, נקבע כי האחריות לכל תוצר של מערכת מבוססת בינה מלאכותית תוטל על הארגון שבחר להטמיעה:

"Ultimately, responsibility for any output or decision made or supported by an AI system always rests with the public organisation. Where generative AI is bought commercially, ensure that vendors understand their responsibilities and liabilities, put the required risk mitigations in place and share all relevant information."³¹⁰

אחריות במגזר הפיננסי בישראל

נקודת המוצא ברגולציה בסקטור הפיננסי בישראל היא שכלל, האחריות מוטלת על הגוף הפיננסי המפוקח בהתאם לרגולציה שחלה עליו. זאת בין שהשירות הניתן על ידו פותח על ידו במישרין ובין שהוא נעזר במיקור חוץ או בצד ג' לצורך מתן השירות. ההוראות הרגולטוריות בהקשר זה מתמקדות בניהול הסיכונים של הגופים הפיננסיים, וקובעות הוראות בדבר האחריות המשפטית, הנובעת בין היתר ממערכת היחסים ומהחובות שחב הגוף הפיננסי ללקוחותיו (חובות אלה כוללות גם חובת זהירות, חובת אמון מוגברת וכדומה). גישה זו באה לידי ביטוי גם בפסיקת בתי המשפט. כך למשל, בתי המשפט חזרו והדגישו את כוחו הרב של הגוף הפיננסי אל מול הלקוח, ואת האמון שנותן הלקוח והסתמכותו על עצתו של בנק. יש לציין עם זאת כי האחריות המוטלת על גוף פיננסי כלפי הלקוח אינה מוחלטת וחד צדדית, ובעניינים מסוימים מוטלות על לקוח חובות כלפי הגוף הפיננסי אשר עלולות להשליך על חובות הגוף הפיננסי כלפי הלקוח.³¹¹

הוראות הנוגעות לאחריות הגופים הפיננסיים ניתן למצוא אצל כל הרגולטורים הפיננסיים. לשם המחשה:

רשות ניירות ערך – במסגרת ההוראה לבעלי רישיון בקשר למתן שירותים תוך שימוש באמצעים טכנולוגיים נקבע כי בעל רישיון ליעוץ השקעות, לשיווק השקעות או לניהול תיקים יישא באחריות כלפי הלקוח לנזק שנגרם ללקוח עקב

308 ראו ה"ש 266 לעיל. כך למשל, חוק FTC חל גם על חברות המפיקות דוחות צרכניים, ובכלל כך למשל, חברות המפיקות דוחות לצורך דירוג אשראי עבור הלוואות. בגילוי הדעת שפורסם הובהר כי חוק FTC יחול גם כאשר הדוח הופק באמצעות בינה מלאכותית. דוגמה נוספת היא שחוק ה-FTC אוסר על הפליט מבקשי אשראי (החוק חל בהקשרים קמעונאיים, חברות פיננסיות וחברות אשראי שאינן מפוקחות על ידי רשות אחרת). גילוי הדעת קובע כי כאשר השימוש באלגוריתם מביא לתוצאה מפלה, הדבר יהווה הפרה של החוק.

309 ראו ה"ש 72 לעיל.

310 HM Government "Generative AI framework for HM Government V.1", <https://www.gov.uk/government/publications/generative-ai-framework-for-hmg>.

311 כך למשל, בפסיקה הוכרו חובות של לקוח כלפי הבנק, וכן במספר מקרים אי-עמידת לקוח בחובותיו הוכרה כעילה להפחתת אחריות הגוף הפיננסי. כמו כן, במסגרת דיני הביטוח למשל מקובל כי חלה על מבטח חובת זהירות לנהוג באותו האופן אלמלא היה מבטח כתנאי לתחולת הביטוח, וכן חלה חובת גילוי רחבה כלפי המבטח; ירון אליאס, דיני ביטוח (מהדורה שניה, 2009), עמ' 331 ואילך ועמוד 449 ואילך.



שימוש באמצעים טכנולוגיים לשם מתן שירותיו ללקוח. הוראה זו נוגעת הן לשלב ההצטרפות וההתקשרות בהסכם, בירור הצרכים של הלקוח, קביעת מדיניות ההשקעה ואסטרטגיית ההשקעה ובמתן השירות השוטף. בהקשר זה נקבע במסגרת ההוראה, כי ביצוע התהליך באופן טכנולוגי הוא בבחינת סיכון שעל נותן השירות הפיננסי לשאת בו, עליו לשאת באחריות לכל נזק שייגרם כתוצאה מכך, והוא יהיה מנוע משלוח את הלקוח לתבוע את נזקו מצד ג' המעורב באספקת השירות.³¹²

רשות שוק ההון, ביטוח וחיסכון – בדברי ההסבר לסעיף 2 בחוזר הרשות בעניין "מיקור חוץ בגופים מוסדיים", אשר חל על חברות ביטוח וקופות גמל, נקבע כי "בהוראות הדין החלות על גוף מוסדי מוגדרות, בין היתר, החובות והאחריות החלות עליו ועל נושאי משרה בו. הוראה זו מבקשת להבהיר כי אין בהעברת פעילות לנותן שירות באמצעות מיקור חוץ כדי לאפשר העברה או האצלה של החובות והאחריות כאמור החלות עליו ועל נושאי משרה בו לפי הוראות הדין". הוראה זו מוצאת את ביטוייה גם בהוראות נוספות בחוזר, בסעיפים 6(ב)(2)(ג), 6(ב)(2)(ו) ו-8, המבקשות להבהיר ולהבטיח כי הגוף המוסדי ימשיך לשאת בחובות ובאחריות לגבי כל פעילות שהועברה לנותן שירות כמיקור חוץ ויפעל להבטיח כי נותן השירות יעמוד בדרישות החלות על הגוף המוסדי.³¹³

הפיקוח על הבנקים – בנוהל בנקאי תקין מס' A359 שכותרתו "מיקור חוץ" נקבע בסעיף 6 שהוצאת פעילות למיקור חוץ אינה גורעת מאחריות התאגיד הבנקאי לקיום מכלול הדינים וההוראות החלים עליו. ההוראה כוללת שורה של חובות על תאגיד בנקאי בתחום הממשל תאגידי.³¹⁴

אם כן, בהקשרים שונים באסדרה הפיננסית, הכלל הוא כי החובות הנוגעות לשירות או למוצר הפיננסי הניתן לציבור מוטלות על הגוף הפיננסי המפוקח, ובהתאמה גם האחריות בנוגע לאותו שירות או מוצר חלה עליו. בהמשך לחלופות שהוצגו לעיל, מדובר בחלופת האחריות על מפעיל המערכת (deployer). כאשר הגוף המפוקח מסתייע בגורם או במערכת חיצוניים, אין בכך כדי להסיר ממנו אחריות כלפי הלקוחות לפי דין. במסגרת החוזית באמצעותה מסדיר הגוף המפוקח את פעילותו מול גורמים חיצוניים, יכול הגוף המפוקח לקבוע כי יהיה זכאי לשיפוי מהגורמים החיצוניים במקרה בו נגרם נזק (למשל כתוצאה מכשל במערכות מחשב שרכש מגורם חיצוני), אולם האחריות לפי דין וכלפי הלקוחות נותרת אצלו.

אחריות בסקטור הפיננסי – סקירה בינלאומית

כמפורט במבוא, ארגונים בינלאומיים העוסקים בגיבוש אסדרה בתחומים כלכליים-פיננסיים, פרסמו בשנים האחרונות דוחות הנוגעים לבינה מלאכותית. דוחות אלה כללו גם התייחסות לשאלת האחריות.

בדוח ה-OECD משנת 2021 נקבע כי האחריות מוטלת על כתפי הדירקטוריון והנהלות הגופים הפיננסיים:

"Ultimate responsibility, oversight and accountability over AI-based systems lies by definition with Executive and board level of management of the financial services provider, who have to establish an organization-wide approach to model risk management, and ensure that the level of model risk is within their tolerance".³¹⁵

דברים דומים נקבעו בדוח ה-OECD משנת 2023:

"In alignment with their fiduciary duties, financial service providers have the legal responsibility to act

³¹² הוראה לבעלי רישיון בקשר למתן שירותים תוך שימוש באמצעים טכנולוגיים, הוראה לפי סעיף 28(ב) לחוק הסדרת העיסוק ביועץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, התשנ"ה – 1995; כך למשל גם בנוגע לחברי הבורסה לניירות ערך: בפרק 1 לחלק הראשון לתקנון הבורסה קבועות חובות חברי בורסה שאינם בנקים (חש"בים) ביחס לקבלת שירותי מיקור חוץ במסגרת ניהול טכנולוגיות המידע. סעיף 24(ח) לחלק הראשון לתקנון הבורסה קובע כי "קבלת שירותי מיקור חוץ על ידי החש"ב אינה גורעת מחובת החש"ב לקיים את כל ההוראות על פי התקנון ו/או הוראות כל דין, וכן אינה גורעת מאחריות החש"ב לכך שהשירותים הניתנים לו באמצעות מיקור חוץ, עומדים בתנאים הקבועים על פי התקנון".

³¹³ חוזר מיום 3.6.2018, תוקן ביום 31.12.2018.

³¹⁴ כגון: בסעיף 10 לנב"ת נקבע כי "הדירקטוריון נושא באחריות הכוללת למיקור החוץ ועליו לוודא כי הוצאת פעילות למיקור חוץ אינה גורעת מקיום חובותיו ומאחריותו של התאגיד הבנקאי לעמוד בכל הוראת דין לרבות הוראות המפקח על הבנקים ובפרט: (א) אחריותו כלפי לקוחותיו, ולרבות שקיפות וגילוי נאות, מתן תמיכה טלפונית לשאלות ובידורים וטיפול בתלונות; (ב) אחריותו לוודא כי לא תיפגע יכולתו של המפקח על הבנקים לקבל מידע ולהפעיל את סמכויותיו וחובות ביקורת פנימית. בנוסף, על התאגיד הבנקאי מוטל לקיים בדיקת נאותות לנותן השירות במיקור חוץ, וכן נקבעו הוראות ספציפיות לגבי אופן ההתקשרות עם נותן השירות באמצעות חוזה מיקור חוץ. בהוראה נקבעו גם חובות לעניין ניהול סיכונים וחובות דיווח למפקח על הבנקים.

³¹⁵ דוח ה-OECD משנת 2021, בעמ' 50.



in the best interest of the clients, which also means protecting them from risks of deceptive outputs, misinformation or other risks to financial consumers related to GenAI tools in particular.”³¹⁶

ובהמשך מצוין כך, בהקשר של מערכות מבוססות בינה מלאכותית שאינן בהכרח בינה מלאכותית יוצרת:

“Similar to any type of model, the use of AI-based models by financial market participants would need to comply with their existing model governance frameworks and oversight arrangements. This includes clear lines of responsibility for the development and overseeing of AI-based systems throughout their lifecycle, from development to deployment, and explicit designation of accountability for any adverse outcome produced by the model.”³¹⁷

בדוח IOSCO משנת 2021, מוצעת שורה של צעדים שעל רשויות וקובעי מדיניות לאמץ בהקשרי אימוץ של בינה מלאכותית. הצעד המוצע הראשון מתייחס להטלת אחריות על נושאי משרה מכהנים במתווכים פיננסיים ובמנהלי נכסים העושים שימוש במערכות מבוססות בינה מלאכותית, שהם מושא הדוח.

“Measure 1: Regulators should consider requiring firms to have designated senior management responsible for the oversight of the development, testing, deployment, monitoring and controls of AI and ML. This includes a documented internal governance framework, with clear lines of accountability.”³¹⁸

המלצות דומות ניתן למצוא גם בדוחות של רגולטורים פיננסיים מדינתיים. כך, לדוגמה, בדוח משותף שהוציאו הרגולטורים הפיננסיים האנגליים:

“The supervisory authorities’ existing rules and guidance, in particular, those implementing the SM&CR, emphasise senior management accountability and responsibility and are relevant to the use of AI. Currently, technology systems are the responsibility of the SMF24 (Chief Operations function ...). [...] PRA-authorized SM&CR banking and insurance firms and FCA-authorized enhanced scope SM&CR firms must ensure that one or more of their SMF managers have overall responsibility for each of the activities, business areas, and management functions of the firm. That means any use of AI in relation to an activity, business area, or management function of firm would fall within the scope of a SMF manager’s responsibilities. For banks, the General Organisational Requirements (part 2.1) states that ‘firms must have robust governance arrangements, which include a clear organisational structure with well defined, transparent, and consistent lines of responsibility and effective control and safeguard arrangements for information processing systems’.”³¹⁹

גם הרגולטור הסינגפורי התייחס להטלת אחריות על הגוף הפיננסי אשר עושה שימוש במערכות מבוססות בינה מלאכותית, ללא רלוונטיות לשאלה אם המערכת פותחה על ידי הגוף הפיננסי או באמצעות ספק חיצוני:

“It is important that there is clear responsibility for and ownership of AIDA-driven decisions within an AIDA firm, with appropriate internal approving authorities for the use of AIDA. Such accountability applies to all uses of AIDA, whether internally developed or externally sourced.”³²⁰

316 דוח ה-OECD משנת 2023, בעמ' 10.

317 דוח ה-OECD משנת 2023, בעמ' 24.

318 דוח IOSCO משנת 2021, בעמ' 17.

319 ראו ה"ש 74 לעיל בעמ' 39.

320 ראו ה"ש 76 לעיל, בעמ' 10.



המלצות בנושא אחריות

כאמור לעיל, המלצות חלק זה יתייחסו לשאלת האחריות ביחס לחובות הרגולטוריות החלות על הגופים הפיננסיים במקרים בהם הגופים נעזרים או עושים שימוש במערכות בינה מלאכותית. בשלב זה, אין בדין חובות ייחודיות או אסדרה ביחס לפיתוח והטמעת מערכות בינה מלאכותית (בדומה ל-EU AI Act) אך ככל שייקבעו חובות כאלה ייתכן שיהיה מקום לדון מחדש בהמלצות אלה לנוכח אופי החובות שיוטלו בהקשרי פיתוח ושימוש במערכות בינה מלאכותית.

במסגרת הערות הציבור לדוח הביניים הובעה מצד אחד תמיכה בגישה שהוצגה בו ומצד שני היו שטענו כי הדוח אינו מספק מענה חד-משמעי לשאלת האחריות המשפטית במקרה של נזק שנגרם כתוצאה משימוש, וכי יש לוודא כי אין סטייה ממשטרי האחריות המקובלים בעולם. כאמור, עמדתו העקרונית של הצוות, כפי שהובעה בדוח הביניים, היא שאין מקום לסטות מהמצב הקיים, קרי הטלת האחריות ביחס לחובות הרגולטוריות על הגופים הפיננסיים המפוקחים. זו הגישה המקובלת בישראל בסקטור הפיננסי, והצוות אינו רואה מקום לסטות ממנה כאשר תהליכים שונים נעשים באמצעות מערכות בינה מלאכותית. הדברים נכונים, בין היתר, למיקור חוץ ולשימוש במערכות שפותחו על ידי צדדים שלישיים, להסדרים החוזיים שבין הגופים הפיננסיים וספקיהם, וכדומה. להבנת הצוות, זו הגישה המקובלת גם בחו"ל. הצעות נוספות שעלו במסגרת הערות הציבור, כגון הצגת קריטריונים נוספים להטלת אחריות, הגדרת חובות הזהירות והפיקוח של כל צד המעורב בתהליך הפיתוח והשימוש במערכת, או טיפול במצבים בהם ספקים חיצוניים סטו מהוראות הגוף המפוקח, אינן נחוצות לדעת הצוות בשלב זה, שכן לא ניתן להתייחס לנסיבות שיכולות להיווצר בכל התקשרות בין מפתח ומפעיל של מערכת, וממילא תחת משטר האחריות הקיים יכולות לעלות גם כיום סוגיות דומות במערכות היחסים שבין הגופים המפוקחים וצדדים שלישיים שהם נעזרים בהן.

הערה נוספת התייחסה להמלצה לאסור על הגבלת אחריות, לגביה נטען כי היא תטיל אחריות רחבה מדי על גופים פיננסיים. בהקשר זה יש להבהיר כי איסור הגבלת האחריות מהווה המשך ישיר לעקרון האחריות של הגופים המפוקחים והוא קיים כיום בהקשרים אחרים של פעילותם. ראו למשל סעיף 13(ה) לחוק הייעוץ, הקובע כי תניית פטור בהסכם, הפוטרת בעל רישיון מאחריות המוטלת עליו לפי חוק זה או לפי דין אחר, בעניין אופן מילוי תפקידו או המסוייגת את אחריותו – בטלה.

אין באמור כדי למנוע הבהרות של הגוף המפוקח בדבר מגבלות סבירות של מערכת בינה מלאכותית. כך למשל, ביחס למערכת בינה מלאכותית המבצעת אנליזות של חברות הנסחרות בבורסה, ניתן להבהיר ללקוח כי מערכת זו אינה מביאה בחשבון מידע מסוים, בדומה למגבלה דומה שניתן היה להציג לגבי שירות שלא בעזרת מערכת הבינה המלאכותית.

כמו כן, אין באמור כדי לפגוע בקביעת הסדרים פרטניים בין הגוף הפיננסי לבין צדדים שלישיים הקשורים למערכות הבינה המלאכותית (ספקים, מפתחים וכו'), ובלבד שלא תוגבל אחריותו של הגוף הפיננסי במערכת היחסים שבינו לבין הלקוח.

לאור האמור ובמטרה להשיג עקביות עם מתכונת הטלת האחריות ברגולציה הקיימת, אלה המלצות הצוות:



המלצות בנושא אחריות

1. שימור עיקרון האחריות של הגוף המפוקח

הגישה המקובלת בישראל בסקטור הפיננסי היא החלת החובות הרגולטוריות על הגופים הפיננסיים המפוקחים על ידי הרגולטורים השונים – וזאת בין שהשירות ניתן על ידי הגוף הפיננסי עצמו ובין שהוא ניתן באמצעות מיקור חוץ או בהתבסס עליו. כפועל יוצא מכך, גם האחריות על פי דין מוטלת על הגוף המפוקח. איננו מוצאים מקום לסטות מעיקרון זה, הן מבחינה ערכית והן מבחינה פרקטית. **הכנסת מערכות מבוססות בינה מלאכותית לגופים פיננסיים אינה צריכה לגרוע מחובות ומאחריות הגופים הפיננסיים לעמוד בכללי הרגולציה וחובותיהם כלפי הלקוחות, שהן המפתח להגנה על אינטרס הציבור וראוי שלציבור תהיה כתובת ברורה לפנות אליה.** יתרה מכך, הרציונל העומד בבסיס הטלת האחריות על הגופים הפיננסיים נותר זהה גם עם הכנסת מערכות מבוססות בינה מלאכותית, שכן לא ניתן לצפות מלקוח קצה אשר נגרם לו נזק כתוצאה מהתנהלותו מול גוף פיננסי, שיידרש לחפש גורם חיצוני על מנת לתבוע ממנו את נזקיו. לקוח הקצה נמצא בחיסרון מבחינת הידע והנגישות ביחס לגוף הפיננסי, שנדרש לעמוד בדרישות רגולטוריות שונות, לרבות בהיבטים טכניים, קבלת החלטות, ממשל בינה מלאכותית וכו'. לבסוף, הגוף הפיננסי הוא עדיין הגורם המונע היעיל ביותר שכן תחום העיסוק הוא עדיין בחובות רגולטוריות הנוגעות לגופים הפיננסיים.

2. מיקור חוץ

השימוש במיקור חוץ על ידי גופים פיננסיים הינו פרקטיקה מקובלת ומוסדרת (למשל, קניית תוכנות מסוימות במקום לפתח אותן בתוך הבנק). למיקור חוץ יכולות להיות תועלות רבות בביצוע הפעילות הפיננסית, ולמעשה הוא בגדר הכרח עבור מרבית הגופים הפיננסיים. בהוראות השונות שנקבעו על-ידי הרגולטורים הפיננסיים הובהר כי מיקור חוץ הנו אפשרי ביחס לפעילויות רבות, ובד בבד נקבע שהוצאת פעילות למיקור חוץ אינה גורעת מאחריות הגופים הפיננסיים לקיום החובות הרגולטוריות החלות עליהם לפי מכלול הדינים וההוראות. **לעניין זה, מוצע לראות בהתקשרות של גוף פיננסי עם צד שלישי לגבי מערכות מבוססות בינה מלאכותית כמיקור חוץ, והמלצתנו היא כי אין לסטות מההוראות שנקבעו בהקשר זה שלא בהכרח לעניין בינה מלאכותית.**

3. שימור כללי האחריות בגופים הפיננסיים עצמם

הרגולציה הפיננסית מטילה בנסיבות מסוימות אחריות ספציפית על אורגנים ובעלי תפקידים בגוף הפיננסי, כאשר ככלל האחריות הכוללת לפעולותיו של הגוף המפוקח מוטלת על הדירקטוריון שלו. בהתאם לגישה שהוצגה לעיל, ולהמלצות האסדרה בחו"ל, מוצע שלא לסטות מכללי אחריות אלה גם בנוגע למערכות בינה מלאכותית – הן בקשר עם הטמעת מערכות בגוף הפיננסי, הן בקשר עם אופן השימוש בהן ועריכת ניהול סיכונים מתאימים. אין בכך לגרוע מהאפשרות כי בנוסף לכך יחולו חובות ואחריות מיוחדים בקשר עם בינה מלאכותית (בכך נעסוק בפרק ממשל בינה מלאכותית להלן).

4. אחריות המפתח כשיקול או כתנאי עתידי ביחס להפעלת מערכות בינה מלאכותית

כפי שתואר לעיל, בעולם מתפתחת רגולציה שתחול על מערכות בינה מלאכותית. הדוגמה המובהקת לרגולציה שכזו היא ה-EU AI Act, המטיל אחריות על מפתחי מערכות בינה מלאכותית לעמוד ברגולציה שנקבעה בחקיקה זו. לאחריות, ולחובות שיחולו מכוח רגולציה כאמור, עשויות להיות חשיבות גם בראיית הפיקוח הפיננסי.

לאור האמור יהיה מקום לשקול בעתיד התייחסות לרגולציה החלה על המפתח (ובכלל זה האחריות החלה עליו מכוח אותה רגולציה), כשיקול או כתנאי עתידי ביחס להפעלת מערכת בינה מלאכותית. לשם המחשה, ניתן יהיה לקבוע כי רק מערכות מבוססות בינה מלאכותית הכפופות לרגולציה מקובלת בחו"ל והוכחת עמידה בה, יותרו לשימוש גם בשוק הישראלי. לחלופין, ניתן יהיה לקבוע כי הטמעה של מערכות בינה מלאכותית הכפופות לרגולציה כאמור, תהווה שיקול בעת בחינת האחריות המוטלת על הגופים המפוקחים בישראל במקרה בו נגרם נזק כתוצאה מהשימוש במערכות אלה.

5. איסור הגבלת אחריות כלפי הלקוח

מוצע לאסור על גוף פיננסי להסיר או להגביל את אחריותו לגבי שירותים הניתנים ללקוח באמצעות מערכות בינה מלאכותית. כך למשל, אין בפרסום תניית-פטור (disclaimer) בקשר עם שירותים הניתנים באמצעות מערכות בינה מלאכותית כדי להסיר או להגביל אחריות של הגוף הפיננסי כלפי לקוחותיו. אין באמור כדי להסיר אחריות מהלקוח מקום בו הנסיבות מצדיקות זאת, למשל מקום בו הלקוח נטל במודע סיכון השקעה שהתממש במהלך שירות שניתן לו בהתבסס על מערכת בינה מלאכותית, או מקום בו נעשה שימוש לרעה במערכת באופן מודע או שימוש החורג ממתחם הסבירות על ידי הלקוח. כמו-כן, אין באמור כדי למנוע הבהרות של הגוף המפוקח בדבר מגבלות סבירות של מערכת בינה מלאכותית.

6. קביעת הוראות ממשל בינה מלאכותית

כפי שצוין בפתח פרק זה, נושא האחריות קשור גם להיבטי ממשל בינה מלאכותית, שכן אלה נועדו לקבוע באופן מפורט, בין היתר, הסדרים למימוש אחריותו של הגוף הפיננסי. ראו עוד בהקשר זה בפרק ממשל בינה מלאכותית.



ממשל בינה מלאכותית

להבדיל מהאתגרים שתוארו עד כה, ניתן לתאר את ממשל הבינה המלאכותית (AI Governance) כמסגרת לצמצום האתגרים והפחתת הסיכונים הכרוכים בשימוש בבינה מלאכותית. תפקידו של ממשל הבינה המלאכותית ליצור מנגנוני ניהול ובקרה ראויים בתאגיד, ואלה אמורים להכתיב ולהסדיר את אופן קבלת ההחלטות, ניהול הסיכונים, הבקרה והפיקוח על הפעלת מערכות בינה מלאכותית בארגונים. כללי ממשל המושתתים על עקרונות ראויים, מהווים אמצעי לניהול סיכונים התאגיד ומסייעים לשמור על חוסנו ויציבותו (לאו דווקא הפיננסית) של הארגון. במילים אחרות, ממשל בינה מלאכותית אמור "לתרגם" את הסיכונים והאתגרים הכרוכים בשימוש במערכות בינה מלאכותית לכדי שיטות, תהליכים ואמצעים פרקטיים ליישום כך שניתן יהיה לעשות שימוש אחראי והוגן במערכות בינה מלאכותית, בנתונים המזינים אותן ובפלטי המערכות.

אין כיום בנמצא הגדרה מקובלת לממשל בינה מלאכותית, אם כי קיימת כתיבה אקדמית בנושא, אשר מתרחבת עם הצמיחה בעיסוק הכללי בבינה המלאכותית. יחד עם זאת, ניתן לומר שמרבית הניסיונות להגדיר ממשל בינה מלאכותית עוסקים בצורך בשימוש נרחב בכלים, פרקטיקות, תהליכים, מדיניות וסטנדרטים לצורך פיתוח אחראי וראוי של מערכות ויישומי בינה מלאכותית, וניהולם.³²¹ ממשל בינה מלאכותית מקיף יתייחס לשלבים שונים במחזור החיים של מערכות הבינה המלאכותית, החל משלב ההחלטה על שימוש בבינה מלאכותית, פיתוח האלגוריתם, הטמעת המערכת בארגון, השימוש במערכת, תפעולה ובקרתה, איסוף המידע והנתונים המזינים את המערכת וכדומה.

לא בכדי, ארגונים בינלאומיים עמדו על חשיבות הימצאותם של כללי ממשל בגופים וארגונים העושים שימוש במערכות בינה מלאכותית. כך, למשל, סימן 6 ב-EU AI Act עוסק כולו בכללי הממשל של בינה מלאכותית באיחוד האירופי. כך, בין היתר, הוחלט להקים את משרד הבינה המלאכותית האירופי (European AI office); להקים מועצה אירופית לבינה מלאכותית (European Artificial Intelligence Board) שתפקידה ליעץ לנציבות האירופית בתחומים שהוגדרו תחת סמכותו; להקים פורום מיעץ (Advisory Forum) שתפקידו לספק מומחיות טכנית; להקים פאנל מדעי של מומחים עצמאיים (Scientific Panel of Independent Experts) שתפקידו ליעץ לנציבות האירופית בתחומי ההטמעה, האכיפה, היציבות, הפיתוח, המעקב וכו'; נקבעו מנגנוני שיתוף פעולה בין הרשויות הרלוונטיות, להקים מאגר מידע שיקלוול נתונים בדבר מערכות בינה מלאכותית בסיכון גבוה, וכדומה.

גם ה-OECD, ביחד עם ארגון ה-G7, עמדו על חשיבותם של החלט כללי ממשל בינה מלאכותית:

"The 'responsible' use of generative AI technologies was also viewed as the most "important" priority for policy, followed by governance and by addressing disinformation."³²²

בפסגת הירושמה (אשר עסקה בהתמודדות העולמית בסיכונים הכרוכים בינה מלאכותית, ובמיוחד בבינה מלאכותית יוצרת), ארגון ה-G7 קרא בין היתר לכל בעלי העניין והנוגעים בדבר לפתח ולהטמיע כללי ממשל בבינה מלאכותית: "Develop, implement and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems."³²³

בבריטניה פרסמה הממשלה אסטרטגיה בתחום הבינה המלאכותית. עקרונות ממשל תקין וראוי קיבלו ביטוי בדוח זה, והממשלה הבריטית עמדה על חשיבותם:

Mäntymäki, M., Minkinen, M., Birkstedt, T. et al. Defining organizational AI governance. *AI Ethics* 2, 603–609 (2022). ³²¹ <https://doi.org/10.1007/s43681-022-00143-x>

OECD (2023), G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on ³²² Generative AI, OECD Publishing, Paris, <https://doi.org/10.1787/bf3c0c60-en>

Hiroshima Process International Guiding Principles for All AI Actors, [https://www.soumu.go.jp/hiroshimaaiprocess/pdf/](https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03_en.pdf?force_isolation=true) ³²³ document03_en.pdf?force_isolation=true



"Governance measures should be in place to ensure effective oversight of the supply and use of AI systems, with clear lines of accountability established across the AI life cycle. AI life cycle actors should take steps to consider, incorporate and adhere to the principles and introduce measures necessary for the effective implementation of the principles at all stages of the AI life cycle. Regulators will need to look for ways to ensure that clear expectations for regulatory compliance and good practice are placed on appropriate actors in the AI supply chain, and may need to encourage the use of governance procedures that reliably ensure these expectations are met."³²⁴

בארה"ב, הבית הלבן פרסם את מגילת הזכויות בקשר עם בינה מלאכותית, המתייחסת לחשיבות של כללי ממשל אצל גופים העושים שימוש בכלי בינה מלאכותית וכן אצל גופים המפתחים כלים אלו:

"Entities responsible for the development or use of automated systems should lay out clear governance structures and procedures. This includes clearly-stated governance procedures before deploying the system, as well as responsibility of specific individuals or entities to oversee ongoing assessment and mitigation."³²⁵

נוסף על כך, התכנית למגילת זכויות בקשר עם בינה מלאכותית כוללת התייחסות גם לצורך בבחינת המערכות טרם השימוש בהן, זיהוי הסיכונים הכרוכים בשימוש במערכות בינה מלאכותית וצמצומם, ניטור שוטף של פעילות המערכות, פיקוח ועוד. הגם שהתכנית למגילת הזכויות בקשר עם בינה מלאכותית אינה מתמקדת בסקטור הפיננסי, נדמה שעקרונותיה יחולו על כלל הסקטורים ותחומי החיים בהן תפעלנה מערכות בינה מלאכותית.

ממשל בינה מלאכותית בסקטור הפיננסי

ה-EU AI Act מתייחס לממשל בינה מלאכותית באופן ספציפי בגופים פיננסיים. ראו, לדוגמה, בסעיף 80 בדברי המבוא:

Union legislation on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems.

מעבר לכך, ה-EU AI Act קובע הוראות בדבר הפעלת מערכות לבקרת איכות של המערכת,³²⁶ שמירת תיעוד,³²⁷ ביצוע ניטור של המערכת מראש ובדיעבד (לאחר פעילותה בשוק),³²⁸ וכדומה.

זאת ועוד, בסעיף 17 ל-EU AI Act, נקבע ביחס לספקים (providers) של מערכות בינה מלאכותית שהם מוסדות פיננסיים, כי ככל שהם יעמדו בהסדרי ממשל פנימיים בהתאם לחקיקה פיננסית של האיחוד, יראו אותם כעומדים בדרישות מסויימות בנוגע לקיום מערכות בקרת איכות. הוראה דומה נקבעה גם בסעיף 26(6) לחקיקה האירופאית בנוגע ל-deployers שהם מוסדות פיננסיים, בנוגע לנקיטת אמצעים טכניים וארגוניים כדי להבטיח עמידה בדרישות המלוות את המערכת.

בדוח IOSCO משנת 2021, אשר, כאמור, מתמקד בנושא יישומי בינה מלאכותית ולמידת מכונה על ידי מתווכים פיננסיים ומנהלי נכסים, תחומי הממשל והפיקוח (כמו גם מספר תחומים אחרים) זהו כתחומים שיש לתת עליהם דגש בעקבות השימוש ההולך וגובר במערכות בינה מלאכותית בפעולות פיננסיות. כל האמצעים שהוצעו על ידי IOSCO כמענה לסיכון זה, מתייחסים (באופן כזה או אחר) לעקרונות ממשל בבינה מלאכותית. הדוח מתייחס לצורך שגופים פיננסיים יעדכנו את עקרונות הממשל שלהם לעידן הבינה המלאכותית. למעשה, IOSCO קורא לרגולטורים

³²⁴ A pro-innovation approach to AI regulation (August 2023), <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#executive-summary>

³²⁵ ראו ה"ש 24 לעיל.

³²⁶ סעיף 17(3) ל-EU AI Act.

³²⁷ למשל סעיפים 18 ו-19 ל-EU AI Act.

³²⁸ למשל סעיף 72 ל-EU AI Act.



המדינתיים לחייב גופים פיננסיים מפוקחים לפעול בין היתר בהתאם להנחיות הבאות, שגם אם הן אינן בליבת הממשל "המקובל", מצופה שעמידה בעקרונות אלה תונחל לגופים באמצעות כללי ממשל מתאימים:³²⁹

(1) אחריות ההנהלה: למנות גורם מטעם ההנהלה הבכירה שיהיה אחראי על הפיקוח, הפיתוח, הבחינה, השימוש והניטור של יישומי בינה מלאכותית. אמצעי זה כולל גם קיומו של ממשל תאגידי מתועד. על הגורם מטעם ההנהלה הבכירה להיות בעל ידע וכישורים טכנולוגיים.

(2) בחינה מקדימה ופיקוח: לבצע בדיקות של האלגוריתם ותיקוף של תוצאות מערכות הבינה המלאכותית ובטרם שימוש עסקי בהן. לאחר תחילת השימוש במערכות בינה מלאכותית, יש לחייב את הגופים המפוקחים לבצע ניטור שוטף של המערכות, בשים לב שהאלגוריתם עשוי להשתנות עם הזמן כתוצאה מיכולות הלמידה העצמית והאוטונומיה של האלגוריתם.

(3) כישורים ומומחיות: להעסיק אנשי מקצוע עם כישורים, ידע, מומחיות וניסיון בפיתוח, בדיקה, הפעלה ניטור ופיקוח של מערכות בינה מלאכותית. כמו כן, פונקציות הציות וניהול הסיכונים צריכות להיות בעלות כישורים מספקים כדי לבחון יישומי בינה מלאכותית שפותחו על ידי צדדים שלישיים ושהגוף הפיננסי מבקש לעשות בהן שימוש.

(4) הסדרת יחסים עם צדדים שלישיים: הסכמים ייעודיים עם צדדים שלישיים המספקים לארגון מערכות בינה מלאכותית.

(5) איכות נתונים: להפעיל אמצעי שליטה ובקרה ביחס למסדי הנתונים שבבסיס מערכות הבינה המלאכותית, כדי לוודא שהמידע והנתונים באיכות וייצוגיות מספקת.

(6) שקיפות: חובות גילוי כלפי לקוחות על שימוש באלגוריתמים.

גם ה-OECD התמקד בנושא הממשל בדוח הארגון בנושא בינה מלאכותית בפיננסיים. בדוח נדונה החשיבות של כללי ממשל בייחוד בהחלטות מהותיות שיש להן השפעה רבה על הפרט (למשל בתחום האשראי או ניהול תיקי השקעות), והוסבר שההשפעה על הצרכנים צריכה לקבל ביטוי בעקרונות הממשל:³³⁰

"Solid governance arrangements and clear accountability mechanisms are fundamentally important as AI models are deployed in high-value decision-making use-cases (e.g. in determining who gets access to credit or how investment portfolio allocation is decided) [...] Internal governance frameworks could include minimum standards or best practice guidelines and approaches for the implementation of such guidelines [...] Importantly, intended outcomes for consumers would need to be incorporated in any governance framework, together with an assessment of whether and how such outcomes are reached using AI technologies."

דברים דומים ברוח זו נכתבו גם בדוח ה-OECD משנת 2023 באשר לבינה מלאכותית יוצרת:³³¹

Strengthen model governance and promote accountability mechanisms: Currently applicable frameworks for model governance in finance may need to be enhanced or adjusted to address incremental risks emerging from advances in AI. Solid governance arrangements and clear accountability mechanisms are fundamental in AI models deployed in high-value use-cases (e.g. in determining access to credit or investment advice).

דוח ה-OECD משנת 2021 מתייחס גם לסוגיות נוספות בתחום הממשל, דוגמת הניטור והפיקוח על מערכות בינה מלאכותית, מיקור חוץ וספקים חיצוניים, בחינה ותיקוף של המערכות ותוצאותיהן ועוד.

הרגולטורים הפיננסיים הבריטיים FCA ו-PRA התייחסו בדוח מפורט לעקרונות השימוש בבינה מלאכותית בגופים פיננסיים, ונתנו משקל רב לחשיבותם של כללי ממשל לשם אימוץ הטכנולוגיה באופן בטוח ואחראי. בתוך כך, התייחסו

329 דוח IOSCO משנת 2021.

330 דוח ה-OECD משנת 2021, בעמ' 49.

331 דוח ה-OECD משנת 2023, בעמ' 30.



הרגולטורים הפיננסיים האנגליים לסוגיות רבות הקשורות בממשל תאגידי ראוי, ובכלל זאת: מבנה תאגידי, שקיפות ועקביות בכל הנוגע לאחריות, מנגנוני ניהול סיכונים, מבנה הדירקטוריון, ביקורת פנימית, וכדומה.³³²

ממשל תאגידי

תחת המינוח הרחב של "ממשל בינה מלאכותית" ניתן לכלול גם כללי ממשל תאגידי. אלה מתייחסים למערכת של חוקים, כללים, פרקטיקות, תהליכים ובקורות, אשר על פיה נשלטים ומנוהלים ארגונים. מוקד מרכזי בכללי ממשל תאגידי הוא התנהלות הדירקטוריון וועדותיו, אך הם עוסקים ברכיבים נוספים בארגון, וכן ביחס בין החברה לבין בעלי מניות ובעלי עניין (Stakeholders) נוספים. כללי ממשל תאגידי ראויים צריכים לקחת בחשבון אינטרסים בעלי העניין בארגון, דוגמת בעלי המניות, ההנהלה הבכירה, העובדים, הלקוחות, הספקים, הרגולטורים, הקהילה, וכו'. התפיסה היא שממשל תאגידי תקין וראוי מהווה תשתית לפעילות ראויה ואחראית של הארגון, החל מהדירקטוריון, דרך ההנהלה הבכירה ועד העובדים הזוטרים.

אחד האמצעים להתמודד עם האתגרים הגלומים במערכות בינה מלאכותית כחלק מממשל בינה מלאכותית הוא אימוץ ויישום של כללי ממשל תאגידי, לרבות התאמתם והבהרתם לעידן הבינה המלאכותית.³³³ עד כה לא מוכרים כללי ממשל תאגידי ייחודיים ומקובלים לפעילות של בינה מלאכותית בקרב גופים פיננסיים, והם עושים שימוש בכללי הממשל התאגידי הקיימים. גישה זו מובנת על רקע התפיסה לפיה יש להתייחס לחידושים טכנולוגיים באופן ניטרלי ולא נדרש להתייחס לכל טכנולוגיה באופן שונה מקודמתה, וכן על רקע היקף השימוש המוגבל במערכות בינה מלאכותית.³³⁴

ואולם גישה זו צפויה להשתנות ככל שהיקף השימוש במערכות בינה מלאכותית יתרחב, ובהינתן סיכונים ואתגרים ייחודיים (או החרפתם של סיכונים קיימים) הכרוכים במערכות בינה מלאכותית, שלא התקיימו ביחס לחידושים טכנולוגיים קודמים או לא קיבלו בהכרח ביטוי בכללי הממשל התאגידי הקיימים. על סיכונים אלה אפשר למנות סיכונים לגופים עצמם וכן לציבור הצרכנים הנובעים מהמידע ונתונים שבבסיס המערכת (למשל, חוסר ייצוגיות של בסיס הנתונים או שימוש בנתונים לא עדכניים, שעלולים להוביל להטיות או להחרף הטיות קיימות, מידע לא נכון שעל בסיסו תוצאות המערכת תהיינה שגויות וכו'), סיכונים הכרוכים במערכות עצמן (למשל, שינוי אוטונומי של האלגוריתם בעקבות למידה עצמית שעלול להוביל לשינוי מהותי בפעילות המערכת ולפעולה של המערכת באופן שלא תוכננה במקור, הצורך בתחזוקה תדירה של המערכת נוכח אופייה, היעדר כלי בחינה ובקרה אפקטיביים); היעדר מעורבות אנושית בכל שלבי קבלת ההחלטה, וכדומה.³³⁵

הוראות ממשל תאגידי קיימות כבר כיום אצל כל אחד מהרגולטורים הפיננסיים, בין בחוק ובין ברגולציה שקבעו הרגולטורים. כך למשל, חוק ניירות ערך, התשכ"ח-1968 (להלן: "חוק ניירות ערך") מגדיר את כללי הממשל התאגידי הנדרשים מבורסה וממסלקה, ופרק ד'1 בחוק הסדרת העיסוק (ראו להלן) עוסק גם הוא בממשל תאגידי, וקובע הוראות מפורשות לגבי מנהלי תיקים, יועצי ומשווקי השקעות. בהוראה לבעלי רישיון למתן שירותים תוך שימוש באמצעים טכנולוגיים נקבעו גם הוראות העוסקות בממשל תאגידי, כגון רכישת ידע, מיומנות והבנה ביחס לאמצעי הטכנולוגי; עריכת בקורות, איתור כשלים ומניעתם שיבטיחו את נאותות השימוש באמצעי הטכנולוגי; מעורבות הדירקטוריון באישור האמצעי הטכנולוגי והשימוש בו; מינוי בעל רישיון ממונה; שמירת תיעוד וכדומה.³³⁶

נוהל בנקאי תקין מספר 310 שכותרתו "ניהול סיכונים" עוסק, בין היתר, בכללי ממשל תאגידי הנדרשים מתאגיד בנקאי על ידי הפיקוח על הבנקים. בהתאם לנוהל בנקאי תקין זה, ממשל תאגידי הוא אחד האמצעים המרכזיים

³³² ראו ה"ש 74 לעיל.

³³³ פעילות הפיקוח על הבנקים בתחום ממשל תאגידי במערכת הבנקאית, 14.5.2018 https://boi.org.il/media/0zaj2atu/%D7%AA%D7%90%D7%92%D7%99%D7%93%D7%91%D7%94-%D7%A2%D7%9C-%D7%9E%D7%9E%D7%A9%D7%9C-%D7%AA%D7%90%D7%92%D7%99%D7%93%D7%99.pdf?force_isolation=true

³³⁴ IOSCO משנת 2021, בעמ' 9.

³³⁵ NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0).

³³⁶ ראו ה"ש 387 להלן.



בניהול הסיכונים של תאגיד בנקאי, והוא מורכב משלושה "קווי הגנה":³³⁷

(1) הנהלות קו העסקים (הנהלת היחידות העסקיות) – אלה נושאות באחריות לזיהוי, להערכה, למדידה, לניטור, להפחתה ולדיווח על הסיכונים המובנים במוצרים, בפעילויות, בתהליכים ובמערכות הנתונים לאחריות, וכן לניהול סביבת בקרה נאותה בהקשר של ניהול סיכונים;

(2) פונקציית ניהול סיכונים בלתי תלויה – תפקידה להשלים, כקו הגנה שני, את פעילויות ניהול הסיכונים של קו העסקים. פונקציה זו תהיה אחראית לתכנון, לתחזוקה ולפיתוח השוטף של מסגרת העבודה לניהול הסיכונים בתאגיד הבנקאי. תפקיד מרכזי של הפונקציה הוא לאתגר את נאותות התשומות של קווי העסקים לניהול הסיכון, למדידת הסיכון ולמערכות הדיווח של התאגיד הבנקאי ונאותות התפוקות המתקבלות. פונקציות ציות, מעקב ובקרה אחרות, דוגמת קצין הציות ואיסור הלבנת הון, החשבונאי הראשי והבקרה על דיווח כספי מהוות אף הן חלק מקו ההגנה השני;

(3) ביקורת פנימית – מבצעת סקירה בלתי תלויה ואיתגור של הבקורות, התהליכים והמערכות לניהול הסיכונים בתאגיד הבנקאי. תפקידה מפורטים בנוהל בנקאי תקין מספר 307.

לצד הוראה זו, הוראות נוהל בנקאי זה העוסקות בממשל תאגידי, עוסקות בין היתר, בפיקוח ובבקרה, בניהול סיכונים, בציות ובתרבות ארגונית. עקרונות הממשל התאגידי באים לידי ביטוי בעיקר בתפקודם התקין של האורגנים בתאגיד, כאשר דגש מיוחד ניתן לתפקודם של: הדירקטוריון, רואה החשבון המבקר, הביקורת הפנימית, מנהל הסיכונים, היועץ המשפטי, קצין הציות והחשבונאי הראשי.³³⁸

כפי שעולה מהסקירה לעיל, כללי ממשל תאגידי מהווים חלק מרכזי מניהול הסיכונים של תאגידים במגזר הפיננסי, והם זוכים להתייחסות משמעותית במסגרת האסדרה הפיננסית. הצוות סבור כי כלי ממשל תאגידי עשויים להוות לבנת יסוד גם בהתמודדות של תאגידים פיננסיים גם עם הסוגיות והאתגרים שמתעוררים כתוצאה משילוב מערכות בינה מלאכותית.

במסגרת הערות הציבור לדוח הביניים עלו הערות לפיהן יש לקבוע תהליך מובנה ביחס לשימושי בינה מלאכותית או נוהל רישוי מוסדר. על אף שיש טעם בהערות אלה, וקביעתו של תהליך בגוף מפקח השוקל אימוץ מערכות בינה מלאכותית היא מתבקשת, הצוות סבר כי קשה להכתיב בדוח דרישה לתהליך או לנוהל ספציפיים בנושא שימושי בינה מלאכותית. הסיבה לכך היא ששימושי הבינה המלאכותית עשויים להיות מגוונים מאוד, ולכן הגדרת תהליכים מחייבים עלולה ליצור כפילות עם תהליכים קיימים (למשל תהליך רישוי של פעילות פיננסית, אשר תבוצע כעת גם תוך הסתייעות במערכות בינה מלאכותית). יתכן עם זאת כי רגולטורים פיננסיים יחליטו לעשות כן ביחס לתחומי פעילות מסוימים או אף באופן כללי יותר.

עניין נוסף שעלה מהערות הציבור, ומקורו ככל הנראה באי הבנה של המלצות דוח הביניים, הוא הטענה שדרישות ספציפיות עשויות להיות מכבידות מדי. ואולם בדוח הביניים הובהר כי אמצעי ממשל הבינה המלאכותית שהוצגו במסגרתו הם ארגז כלים שאפשר להיעזר בו, ולבחור מתוכו את האמצעים המתאימים בנסיבות העניין. הבהרה לעניין זה הוספה גם לדוח הסופי. לשם המחשה, במסגרת תהליכי קבלת החלטות ואחריות הוצג מנגנון אפשרי של אישור דירקטוריון למערכת בינה מלאכותית. אין להסיק מכך המלצה שכל מערכת בינה מלאכותית תחייב אישור של דירקטוריון החברה. הצורך באישור דירקטוריון החברה או גורמים אחרים בחברה תלוי בנסיבות העניין, בהתאם לניהול הסיכונים של הגוף הפיננסי, מהותיות המוצר או השירות, ובהתאם למדיניות הדירקטוריון.

337 סעיף 4 לנוהל בנקאי תקין מספר 310.

338 פעילות הפיקוח על הבנקים בתחום ממשל תאגידי במערכת הבנקאית https://boi.org.il/media/0zaj2atu/%D7%AA%D7%99%D7%91%D7%94-%D7%A2%D7%9C-%D7%9E%D7%9E%D7%A9%D7%9C-%D7%AA%D7%90%D7%92%D7%99%D7%93%D7%99.pdf?force_isolation=true.



המלצות בנושא ממשל בינה מלאכותית

להלן יפורטו מספר אמצעים שיוכלו לשרת את השחקנים בסקטור הפיננסי בבואם לקבוע מנגנוני ממשל ראויים בגופים פיננסיים אשר יפעילו מערכות בינה מלאכותית. הרשימה שלהלן אינה מחייבת, עד לקביעה אחרת מצד הרגולטורים הפיננסיים, והיא גם אינה רשימה ממצה. מטרתה היא להוות ארגז כלים לרגולטורים ולגופים המפוקחים בבואם לקבוע את ההסדרים הראויים.

האמצעים המפורטים להלן נוסחו באופן אופרטיבי ומציגים קשת רחבה של אפשרויות לכללי ממשל המבוססים על הפרקטיקות המתפתחות בעולם. ניתן להחיל אותם, במלואם או בחלקם, בהתאם לשיקולים ונסיבות שונים, לדוגמה אופי השירות הניתן באמצעות מערכות בינה מלאכותית, מהותיותו, פוטנציאל הפגיעה בפרט, וכדומה. החלה כאמור צריך שתיעשה כמובן לאחר בחינת הסדרי הממשל הקיימים והצורך באמצעים אלה. אף אם לא ייקבעו דרישות כאלה, רשימת האמצעים יכולה לשמש גופים פיננסיים השוקלים קביעת כללי ממשל מותאמים למערכות בינה מלאכותית באופן וולונטרי.

קביעת מסמכי מדיניות, תהליכים, נהלים (לרבות נהלים טכניים) ופרקטיקות (לרבות self-practices) שיסייעו במיפוי, מדידה וניהול הסיכונים הכרוכים בשימוש מערכות הבינה המלאכותית. על מסמכי המדיניות, התהליכים, הנהלים והפרקטיקות להיות מתועדים וגלויים. מסמכי המדיניות, התהליכים, הנהלים והפרקטיקות צריכים להתכתב ולחול לצד כללי ממשל תאגידי קיימים, שאינם עוסקים בהכרח בבינה מלאכותית.

מסמכי המדיניות, התהליכים, הנהלים והפרקטיקות יעודכנו בהתאם להתפתחות הטכנולוגיה, היקף ומהותיות השימוש במערכות בינה מלאכותית על ידי הגופים הפיננסיים ויש להבטיח כי הם מובנים ושקופים לכל הגורמים הרלוונטיים בארגון.

על מסמכי המדיניות, התהליכים, הנהלים והפרקטיקות להתייחס לכל מחזור החיים של מערכות הבינה המלאכותית, לרבות לבחינת המערכות טרם השימוש בהן, השימוש במערכות, הניטור והפיקוח של המערכות, וכן לאופן הפעולה כאשר נמצאים פגמים במערכות ובתוצאותיהן.

עובדי הגוף הפיננסי המעורבים בפעילות מערכות הבינה המלאכותית או בתוצאותיהן יעברו הדרכות וסדנאות להקניית ידע מספק על מנת שיוכלו לבצע את תפקידם באופן מספק.

במסגרת הניטור והפיקוח השוטפים של המערכות, יש להביא בחשבון התייחסויות לפעולת המערכת שהתקבלו משלל גורמים הקשורים לפעילותן של מערכות הבינה המלאכותית (לדוגמה, משתמשי המערכת), ולא רק מהגורמים אשר פיתחו את המערכות או הגורמים שהיו אמונים על הטמעת המערכות בגוף הפיננסי.

נהלים, מסמכי מדיניות, תהליכים, ופרקטיקות

אימוץ מערכות הבינה המלאכותית ואופן השימוש בהן יאושרו על ידי דירקטוריון הגוף הפיננסי, כחלק מתפיסת ניהול הסיכונים ותיאבון הסיכון של הגוף הפיננסי. הגורם האחראי (accountable) לפעילות הגוף הפיננסי, לרבות בהיבטי אימוץ, פיקוח, ניטור ושימוש של מערכות בינה מלאכותית יהיה דירקטוריון הגוף הפיננסי וההנהלה הבכירה. על הגוף הפיננסי, באמצעות מי מאורגניו, לרכוש ידע, הבנה ומיומנות ביחס למערכות הבינה המלאכותית בטרם יחל את השימוש בהן ולאורך כל תקופת השימוש בהן. מינוי ממונה בינה מלאכותית, אשר תפקידו להכיר ולהבין את המתודולוגיה שבבסיס מערכות הבינה המלאכותית בהן נעשה שימוש בגוף הפיננסי. על הממונה להיות בעל הידע, הכישורים והניסיון על מנת לקבל החלטות ביחס למערכות הבינה המלאכותית, לספק הסברים על דרכי פעולתן ולבצע בדיקות, ניטור, פיקוח ותיקוף של מערכות קיימות או חדשות.³³⁹ ממונה הבינה המלאכותית כאמור יכול להיות גם ממונה קיים (למשל, ממונה טכנולוגיה ראשי, ממונה סיכונים ראשי וכדומה) שיבצע את התפקיד במקביל לתפקידיו האחרים.	תהליכי קבלת החלטות ואחריות
קביעת תהליכים לבחינה ותיקוף של מערכות בינה מלאכותית, חדשות או קיימות. הניטור והפיקוח צריכים להיעשות בטרם תחילת השימוש במערכת הבינה המלאכותית, לרבות תיקוף שתוצאות המערכת תקינות טרם השימוש במערכת, וכן באופן שוטף באמצעות כלי ביקורת מתאימים, לרבות בחינה תוצאתית וביקורת שוטפת על האלגוריתמים עצמם. על הגוף הפיננסי לקיים בדיקה תקופתית של תוצאות מערכות הבינה המלאכותית על מנת לבחון את תקינות התוצאות בדיעבד (בידי הגוף או בידי גורם חיצוני). למען הסר ספק, בחינה זו אינה מיועדת להחליף את הבחינה השוטפת של המערכות או את הבחינה טרם תחילת השימוש במערכות.	ניטור, פיקוח, תיקוף

339 מינוי פונקציה של ממונה בינה מלאכותית מתכתב עם הוראות שונות באסדרה הפיננסית שעוסקות במינוי בעלי תפקידים שיהיה אמונים על תחומי פעילות או סוגיות שעמם מתמודד התאגיד. כך, למשל, ראו החובה למנות מנהל סיכונים ראשי בגופים מוסדיים (ראו סקירה בנושא "ניהול סיכונים בגופים מוסדיים – סקירה רוחבית במבט השוואתי" – https://www.gov.il/BlobFolder/generalpage/information-entities-corporate-governance/he/nihul-siconim_em31082016.pdf?force_isolation=true ובתאגידים בנקאיים <https://www.boi.org.il/media/lajbthth/200944.pdf>), כמו גם מינוי בעל רישיון ממונה בגופים פיננסיים המספקים שירותי ניהול תיקים, ייעוץ ושיווק השקעות [הוראה לבעלי רישיון בקשר למתן שירותים תוך שימוש באמצעים טכנולוגיים, הוראה לפי סעיף 28 (ב) לחוק הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, התשנ"ה – 1995]. ממונה הבינה המלאכותית יהיה כפוף להנהלת הגוף הפיננסי וידווח להנהלה ולדירקטוריון. זאת ועוד, מינוי כאמור מתכתב גם עם חובת מינוי קצין ציות ראשי, בהתאם להוראות הפיקוח על הבנקים https://www.boi.org.il/media/1xdf0b3e/308.pdf?force_isolation=true אשר גם הוא כפוף לדירקטוריון התאגיד הבנקאי, ועם חובת קביעת תכניות אכיפה אפקטיביות בהתאם לחוק החברות וחוק ניירות ערך (בהקשר זה ראו תיקון מס' 16 לחוק החברות, ותיקון מס' 47 לחוק ניירות ערך. בהקשר דומה, ראו חובת גופים פדראליים בארצות הברית למנות ממונה בינה מלאכותית – https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf?force_isolation=true of-Artificial-Intelligence.pdf?force_isolation=true) זאת בהמשך לצו הנשיאותי בנושא. ההוראה, אשר יצאה גם היא מטעם הממשל האמריקאי, קובעת את תפקידיו וסמכויותיו של ממונה הבינה המלאכותית, היקף אחריותו, ואת מעמדו בהיררכיה הארגונית.

גוף פיננסי יפעיל אמצעי שליטה ובקרה מתאימים לניהול מערכות הבינה המלאכותית. כחלק מאמצעי השליטה והבקרה, הגוף הפיננסי צריך להיות בעל יכולת לעצור את פעילות מערכת הבינה המלאכותית, אם ימצא בה כשל מהותי המחייב עצירה מיידית של פעילות המערכת. אמצעי זה, בבחינת Kill Switch, צריך להיות מוסדר כחלק מנהלי הגוף הפיננסי, לרבות המקרים בהם יופעל והפונקציות בארגון להם הסמכות להפעיל מנגנון זה. מנגנון ה-Kill Switch צריך להיבחן אף הוא אחת לתקופה על מנת לוודא את פעילותו גם בשעת כשל של המערכת ובתסריטי חירום שונים. ניתן להקביל מנגנון זה לניתוק זרם בבורסה לניירות ערך, כפי שנקבע בתקנון הבורסה לניירות ערך.³⁴⁰ הגוף הפיננסי צריך להחזיק גיבוי מתאים למערכות הבינה המלאכותית, למקרה שבו תידרש הפעלת ה-Kill Switch או למקרה כשל במערכות הבינה המלאכותית שלא יאפשר נגישות למערכות.	חירום והפסקת פעילות
על הגופים הפיננסיים לדאוג לקיומם של מסמכי מדיניות, תהליכים, נהלים הקשורים לסיכונים הנובעים משימוש במערכות בינה מלאכותית המסופקים על ידי צדדים שלישיים לגוף הפיננסי או שהשירות ניתן באמצעות מיקור חוץ. בין היתר, מסמכי המדיניות, התהליכים והנהלים צריכים להתייחס למנגנוני המשכיות עסקית, טיפול בכשלי מערכת או מידע וכדומה. מידע ונתונים המתקבלים על ידי צדדים שלישיים או במיקור חוץ צריכים לעבור תיקוף שהם יצוגיים, לא מפלים ולא מייצרים הטיות. בחינה כאמור צריכה להיעשות לפני השימוש בנתונים, ולאחר השימוש באופן שוטף על מנת לוודא את הרלוונטיות והעדכניות שלהם.	שימוש במיקור חוץ וספקי צד שלישי

340 לצורך הדוגמה בלבד, ראו מנגנון מנתק הזרם המופיע במדריך המסחר בבורסה לניירות ערך בתל אביב, הנחיות על פי החלק השלישי לתקנון.



ממשל נתונים

סוגיה מרכזית הנקשרת לעיתים קרובות עם תחום ממשל הבינה המלאכותית היא ממשל נתונים (Data Governance). תחום זה מקבל משמעות יתרה בכל הקשור למערכות בינה מלאכותית, אשר פעולתן ותוצריהן תלוי במידה רבה במידע והנתונים המזינים אותן. הביטוי המקובל בהקשר זה, garbage in, garbage out, ממחיש בצורה ציורית את המשמעות של מידע ונתונים באיכות נמוכה המוכנסים למערכות בינה מלאכותית והתוצר המופק מכך. סעיף 10 ב-EU AI Act עוסק באופן ממוקד בנושא הנתונים (Data) וממשל הנתונים. הסעיף מתייחס למערכות בסיכון גבוה ודן בדרישות החלות על מידע ונתונים בשלבי האימון, התיקוף והבחינה של מערכות הבינה המלאכותית, ובכלל זאת כללי ממשל הנתונים צריכים להתייחס להליך איסוף המידע ומקורו, רלוונטיות וייצוגיות המידע, אמצעים לאיתור, מניעה וצמצום אפליה והטיות, פערי מידע מבחינת נתונים וכדומה.

בהמלצות דוח ה-OECD משנת 2021 ניתן למצוא גם כן התייחסות לנושא ממשל הנתונים ועל המדיניות המוצעת שעל קובעי המדיניות לנהוג בהקשר זה:³⁴¹

"Policy makers could consider the introduction of specific requirements or best practices for data management in AI-based techniques. These could touch upon data quality, adequacy of the dataset used depending on the intended use of the AI model, and safeguards that provide assurance about the robustness of the model when it comes to avoiding potential biases. Appropriate sense checking of model results against baseline datasets and other tests based on whether protected classes can be inferred from other attributes in the data are two examples of best practices to mitigate risks of discrimination. The validation of the appropriateness of variables used by the model could reduce a source of potential biases. Tools could be developed and used to monitor and correct for conceptual drifts."

בהמלצות דוח ה-OECD משנת 2023 מקבל נושא ממשל הנתונים משנה חשיבות ומוצג כסוגיה קריטית:

"Strengthen data governance practices by model developers and deployers: The importance of data is undisputed when it comes to the training of GenAI models and their usage by financial market participants. Best practices for data management and governance practices may be considered to ensure data quality, data adequacy depending on the intended use, data privacy when financial consumer data is fed into the model, and data authenticity and appropriate source attribution/copyrighting when applicable. This could include increased transparency, model documentation and reporting about the data used to train the model and any other data introduced into the model, including their location, origin and source attribution for copyrighted data used [...] This would need to include any data inputted in the model through prompts or otherwise, and the output of the model itself, given feedback loops for its self-training."³⁴²

341 דוח ה-OECD משנת 2021, בעמ' 56.

342 דוח ה-OECD משנת 2023, בעמ' 28.



המלצות בנושא ממשל נתונים

להלן יפורטו מספר אמצעים שיוכלו לשרת את הרגולטורים הפיננסיים בבואם לקבוע מהם כללי ממשל נתונים ראויים בגופים פיננסיים בקשר להפעלת מערכות בינה מלאכותית. הרשימה שלהלן אינה רשימה ממצה ומהווה ארגז כלים לרגולטורים בבואם לקבוע את ההסדרים הראויים:

קביעת מסמכי מדיניות, תהליכים, נהלים (לרבות נהלים טכניים) ופרקטיקות בכל הנוגע לבחינת מקורות המידע והנתונים, וכן ביצוע בדיקות נאותות בקשר לייצוגיות ונכונות הנתונים, האופן בו הושגו ורגישותם, ככל שאלה מתקבלים או נרכשים מגורמים חיצוניים לגוף הפיננסי. בכל הנוגע להסתמכות על צדדים שלישיים חיוניים לפעילות הגוף הפיננסי, לרבות בקשר עם מידע ונתונים, ראו לעיל. יש לשקול מינוי ממונה מידע ונתונים, במקביל למינוי ממונה בינה מלאכותית או בכפוף לו.	מקורות המידע
קביעת מסמכי מדיניות, תהליכים, נהלים (לרבות נהלים טכניים) ופרקטיקות (לרבות self-practices) ספציפיים לממשל נתונים. מסמכים אלו צריכים להתייחס, בין היתר, לשימוש במידע ונתונים רגישים ו/או שעלולים לייצר סיכון מיוחד. במסגרת זו, מסמכי מדיניות, תהליכים, נהלים ופרקטיקות צריכים לתת ביטוי לסוגיות של אימון המודלים, אפליה והטיות, ייצוגיות ותיקוף, פרטיות, רלוונטיות והקשר מקורי של הנתונים.	השימוש במידע



“מחברים את הדברים” – ראייה כוללת ומבוססת סיכונים

הטיפול בסיכונים הנובעים ממערכות בינה מלאכותית צריך להיעשות בראייה כוללת. הדבר נובע מכך שהסיכונים השונים עשויים להיות קשורים זה בזה, ובדומה לכך, גם אמצעי ההתמודדות עם הסיכונים עשויים להיות קשורים זה בזה. לשם המחשה: סיכון של “קופסה שחורה” והעדר הסברתיות של מערכת בינה מלאכותית המסייעת בקבלת החלטות לגבי התקשרות בפוליסות ביטוח עלול להגביר סיכון של אפליה במתן הביטוח (בין היתר בהינתן הקושי לזהות את האפליה) או להגביר סיכון של הטלת אחריות לפעולת המערכת (בין היתר בהינתן הקושי להסביר ולהתאים את המערכת, על-ידי מפתח המערכת או מפעיל המערכת). גם אמצעי ההתמודדות עם מערכת כאמור יכולים להיות מגוונים וקשורים זה בזה. כך למשל, דרישה של מעורבות אנושית עשויה לצמצם את הסיכון הנובע מהמערכת, וכך גם דרישות של יידוע וגילוי בדבר המערכת. בראייה כוללת של המערכת ניתן אם כן לזהות באופן אפקטיבי יותר את הסיכונים ולהתאים את אמצעי ההתמודדות להתמודד עימם.

ההתמודדות עם מערכות בינה מלאכותית צריך שתיעשה גם על בסיס גישה מבוססת סיכונים. העיקרון של אסדרה מבוססת סיכונים מופיע כחוט השני במסמכי מדיניות בעולם וב ישראל העוסקים בבינה מלאכותית, ויתרונותיו ברורים: הגברת אפקטיביות הרגולציה ויעילות בהקצאת משאבים על-ידי הרגולטורים והגופים המפוקחים לנוכח ההתמקדות בסיכונים המהותיים; גמישות בהתאמת הרגולציה לסיכונים המשתנים העולים מהפעילות על פני זמן ובמקרים ספציפיים; ועידוד פעילות עסקית וחדשנות בהנחה שרגולציה מבוססת סיכונים לא תכביד יתר על המידה על הגופים המפוקחים.

מהי המשמעות המעשית של אסדרה מבוססת סיכונים?

דוגמה בולטת לאסדרת בינה מלאכותית בהתאם לגישה מבוססת סיכונים היא ה-EU AI Act. במסגרת חקיקה זו אפיינו 4 קטגוריות סיכון למערכות בינה מלאכותית, וכפועל יוצא מכך נגזרים המגבלות והכללים החלים לגביהן:

סיכון שאין לקבלו (unacceptable risk) – החוק מונה רשימה של פרקטיקות אסורות בתחום הבינה המלאכותית. מערכות ברמת סיכון זו כוללות, בין השאר, מערכות העושות שימוש בטכניקות מניפולטיביות כדי להטות התנהגות ולפגוע בקבלת החלטות מושכלת, ויצורות נזק משמעותי; מערכות המנצלות חולשות הקשורות בגיל, במוגבלות או בנסיבות סוציו-אקונומיות, כדי להטות התנהגות ויצורות נזק משמעותי; מערכות המבצעות דירוג חברתי (social scoring) וגוררות התנהלות שלילית ביחס לאנשים או קבוצות שהוערכו או סווגו באמצעותן; ומערכות המשמשות להסקת רגשות במקומות עבודה או במוסדות חינוך, למעט לצרכים רפואיים או בטיחותיים; מערכות הבונות מאגרי מידע לזיהוי פנים באמצעות איסוף לא מבוקר של נתונים מהאינטרנט או מצלמות אבטחה וכן מערכות ביומטריות מסוימות.³⁴³ ככלל, **מערכות בינה מלאכותית ברמת סיכון שאין לקבלו נאסרו לשימוש, למעט חריגים ספציפיים.**

סיכון גבוה (high risk) – החוק מונה כללים לסיווג מערכות ברמת סיכון גבוהה, ושורה של מערכות כאלה מופיעות בתוספות לחוק. בין היתר מדובר במערכות העוסקות בזיהוי ביומטרי שאינו אסור; מערכות המשמשות כרכיבי בטיחות בתשתיות חיוניות; מערכות המשפיעות על קבלה למוסדות לימוד ובהערכת תלמידים; מערכות המשמשות בהיבטי תעסוקה; מערכות המשפיעות על נגישות לשירותים חיוניים (ציבוריים ופרטיים) – לרבות מערכות המשמשות לדירוג אשראי, או להערכת סיכונים במסגרת תמחור פוליסות חיים או בריאות; מערכות בתחום אכיפת החוק בהקשרים מסוימים; ועוד. בנוסף לכך, מערכות נחשבות ברמת סיכון גבוהה, אם הן מייננות אנשים (profile individuals), קרי עוסקות בניתוח אוטומטי של מידע אישי כדי להעריך היבטים בחיי אדם, כגון ביצועים בעבודה, מצב כלכלי או בריאות, העדפות, התנהגות, וכדומה. יצוין בהקשר זה, כי רמת הסיכון נבחנת גם לפי מידת המעורבות של המערכת בקבלת החלטה בהקשרים אלה. כך למשל, מערכת שמשמשת רק בהיבט פרודורלי זניח, גם אם באחד התחומים המנויים לעיל, אינה בהכרח מערכת בסיכון גבוה לפי החקיקה.³⁴⁴ **מערכות בינה מלאכותית ברמת סיכון גבוהה כפופות לפיקוח בהתאם לחוק, ומושתות לגביהן בין היתר דרישות ניהול סיכונים לכל אורך חיי המערכת, דרישות ממשל נתונים, תיעוד, שקיפות, מעורבות אנושית, רישום במאגר ייעודי ועוד.** רוב הדרישות מושתות על מפתחי המערכות (providers) אך יש גם דרישות ביחס לגורמים המפעילים אותן (deployers).

מערכות המגלמות סיכון שקיפות (transparency risk) – מערכות מסוימות – לרבות כאלה שיכולות להיות במקביל ברמת סיכון גבוהה אך לא בהכרח – נדרשות לעמוד בחובות שקיפות. **המדובר במערכות המיועדות להיות**

³⁴³ EU AI Act, בסעיף 5.
³⁴⁴ EU AI Act, בסעיף 6(3).



באינטראקציה ישירה עם בני אדם, ולכן הושתו עליהן דרישות שקיפות כגון יידוע המשתמשים כי הם נמצאים באינטראקציה כאמור אלא אם כן הדבר ברור מהנסיבות; תיוג תכנים שנוצרו או שונו באמצעות בינה מלאכותית וכוללים deep fake ככאלה; וסימון תוכן שנוצר על-ידי בינה מלאכותית ככזה (למעט חריגים).

סיכון מינימלי או העדר סיכון כלל (minimal or no risk) – מערכות ברמת סיכון נמוכה מאוד זו, כגון מערכות במשחקי וידאו או מערכות לסינון תכנים (spam filters), אינן כפופות לרגולציה.

בנוסף לרמות הסיכון האמורות, נקבעו גם דרישות אסדרתיות ביחס לקטגוריה חדשה של **בינה מלאכותית כללית (General Purpose AI)**.³⁴⁵ מפתחים של מערכות אלה נדרשים בין השאר לתיעוד, הנחיות שימוש, מדיניות ציות לדירקטיבת זכויות יוצרים, ופרסום הסבר אודות התוכן המשמש באימון המודל. אם המערכת מוגדרת כבעלת סיכון מערכתי (למשל, כפועל יוצא של כוח המחשוב) חלות דרישות נוספות כגון חובת דיווח והתמודדות מתאימה עם סיכוני סייבר.



כאמור, גישה מבוססת סיכונים אינה ייחודית לאיחוד האירופאי וניתן למצוא אותה במסמכי אסדרה או מדיניות של מדינות נוספות – באופן כללי ביחס לבינה מלאכותית וגם ביחס לשימושים ספציפיים.³⁴⁶ הייחודיות של החקיקה האירופאית בשלב זה היא בכך שהיא מאפיינת את השימושים והמערכות שנכללות בכל קטגוריית סיכון.

מדרג סיכונים עשוי להיות שימושי בסיווג רמת הסיכון של מערכות בינה מלאכותית בסקטור הפיננסי וקביעת אמצעים מותאמים להתמודדות עם הסיכון. ניתן לדוגמה למיין מערכות של בינה מלאכותית על בסיס **מדרג סיכונים הכולל שתי רמות סיכון – נמוכה-בינונית וגבוהה.**

סיווג הסיכון בגופים פיננסיים צריך להיעשות על בסיס כפול: ראשית, רמת הסיכון **ללקוחות או למשקיעים**, ושנית, רמת הסיכון **לגוף הפיננסי** עצמו. כך למשל, מערכת בינה מלאכותית שיש לה השפעה מהותית על הלקוח או על המשקיע, כגון מערכת המסייעת בקבלת החלטות אשראי, עשויה לסכן לקוחות, בכך שתגביל את נגישותם לאשראי או תייקר את האשראי שהם מקבלים. לעומת זאת, מערכת בינה מלאכותית הבודקת תהליכי ציות בתחום הלבנת הון, לא תפגע בהכרח ישירות בלקוחות הגוף הפיננסי, אולם אם תיכשל היא עלולה לפגוע בגוף הפיננסי (באופן שיגרור סנקציות, פגיעה במוניטין, וכדומה). בתוך כך יש להעריך גם את מידת המעורבות של המערכת בקבלת

³⁴⁵ מונח זה מתייחס למערכות בינה מלאכותית שניתן לעשות בהן שימוש במגוון הקשרים ולאמן אותן למגוון שימושים וזאת בניגוד למערכות שפותחו עבור שימוש מסוים. ראו EU AI Act, בסעיף 50.

³⁴⁶ ראו ה"ש 301 לעיל, בסעיפים 1.2, 3.2.2.

ההחלטה או ביצוע המשימה וזאת בדומה להחרגה של מערכות עם מעורבות שולית בתהליך בחקיקה האירופאית. שיקול נוסף בסיווג הסיכון הוא הרגולציה שתחול על המערכת והגורמים הרלוונטיים לפעילותה – לדוגמה רגולציה שתחול על מפתח המערכת, שיש בה כדי להשפיע על סיווג הסיכון הגלום במערכת.

האמצעים שיינקטו ביחס למערכת בינה מלאכותית יהיו מותאמים לרמת הסיכון שלה. כך למשל ביחס למערכות ברמת סיכון גבוהה אפשר להשית דרישות ממשל בינה מלאכותית משמעותיות יותר על מנת להתמודד עם הסיכון הגלום בהן, בעוד שביחס למערכות המגלמות רמת סיכון נמוכה יותר אפשר להסתפק בדרישות מצומצמות. זאת בנוסף לדרישות מחייבות החלות על הפעילות הרלוונטית מכוח הדין וההוראות הרגולטוריות הנוגעות לאותה פעילות.

ראו לשם המחשה יישום של כלים המפורטים בדוח זה בהתאם למדרג רמות סיכון כאמור. אין מדובר ברשימה סגורה או ממצה, אלא במתווה לסיווג לרמות סיכון שונות, שעל בסיסו ניתן יהיה לאפיין את רמת הסיכון של המערכת, ולהתאים את הדרישות הרגולטוריות ביחס אליהן (למשל, בהיבטי הסברתיות, מעורבות אנושית ועוד). כפי שהוסבר לעיל, בביצוע התאמה זו, יש להביא בחשבון כי אמצעי התמודדות מסוים עשוי לשמש למספר תכליות, וההשפעה של אמצעי ההתמודדות השונים צריכה להיבחן באופן כולל.

הדוגמאות הקונקרטיות המוצגות לצד כל רמת סיכון הן לצורך המחשה בלבד, ותידרש בחינה ספציפית של המערכת בה נעשה שימוש.

רמת הסיכון	סיכון נמוך – בינוני	סיכון גבוה
דוגמאות וסוגיות לבחינה	מערכות בינה מלאכותית המשמשות למטלות back-office מסוימות, כגון מערכות המבצעות פעולות שגרתיות של טיפול בנתונים בתהליכי עבודה שונים, מערכות המסייעות בהגנת הגופים הפיננסיים (למשל זיהוי ומחיקה של דואר זבל), או צ'אט-בוטים המשמשים לפעולות פשוטות שאינן כרוכות בקבלת החלטות משמעותיות עבור לקוחות (למשל מסירת מידע כללי על הגוף הפיננסי).	מערכות בינה מלאכותית העוסקות בין היתר בניתוח מידע אישי של לקוחות ומשפיעות על השירות הניתן להם. כך לדוגמה, מערכת המשמשת לניתוח פרופיל הסיכון של לקוחות, ובהתאם בונה עבורם תיק השקעות מנוהל. או לדוגמה, מערכת המשמשת לזיהוי סיכונים הונאה שתוצאתה עשויה להיות מניעת גישה של לקוחות לפעילות בנקאית. או לדוגמה, מערכת המשמשת לתמחור פוליסות ביטוח חיים בהתבסס על מידע אישי של הלקוחות.
"קופסה שחורה" והסברתיות	הסברתיות כללית ופרטנית. הסברתיות כללית – לגבי אופן פעולת האלגוריתם, להבדיל מהסבר ספציפי כיצד התקבלה החלטה מסוימת. הסברתיות פרטנית – על הגוף המפוקח להכיר את פעילות האלגוריתם, גישה למסמכי ההפעלה וכדומה.	מעבר להסברתיות פרטנית וכלפי הרגולטור, לגוף המפוקח צריכה להיות היכולת להסביר לצרכן את ההחלטה הספציפית שהתקבלה לגביו. בעניין זה תידרש הסברתיות פרטנית, אלא אם כן מתקיימים אמצעי התמודדות המפצים על העדרה.
מעורבות אנושית	בקרה אנושית על פעילות המערכת (במובחן מבקרה על כל החלטה שלה). בקרה בדיעבד על החלטות המערכת, בהיקף המותאם לסיכון נמוך.	בקרה אנושית על פעילות המערכת. בקרה בזמן אמת ובדיעבד על החלטות המערכת בהיקף המותאם לסיכון גבוה.

רמת הסיכון	סיכון נמוך - בינוני	סיכון גבוה
מניעת אפליה	בקרה ונקיטת אמצעים למניעת אפליה בהיבטים ממוקדים של פעילות המערכת (הצטרפות לקוחות בדוגמה שהובאה לעיל) ובהיבטים ממוקדים לאורך חיי המערכת	בקרה ונקיטת אמצעים למניעת אפליה לכל אורך חיי המערכת, בפרט בהיבטים הבאים: מאגרי נתונים אופן פעילות המערכת תוצאות המערכת
אחריות	אחריות הגוף המפוקח איסור הגבלת אחריות כלפי הלקוח	אחריות הגוף המפוקח איסור הגבלת אחריות כלפי הלקוח אחריות המפתח כשיקול או כתנאי עתידי ביחס להפעלת המערכת ו/או כפיפות לרגולציה מקובלת זרה
גילוי ויידוע	דרישת יידוע בדבר עצם השימוש במערכת בינה מלאכותית אלא אם כן הדבר עולה בבירור מהנסיבות. גילוי – ככל שנדרש בהתאם לנסיבות (אם למשל מדובר במערכת לצרכים פנימיים שאינה משפיעה על הפעילות מול הלקוחות, אין צורך ביידוע או בגילוי)	דרישת יידוע בדבר עצם השימוש במערכת בינה מלאכותית חובות גילוי פרטניות בדבר המערכת, ומאפיינים ייחודיים הנובעים מהטכנולוגיה גילוי בשפה בהירה, תמציתית וניטראלית הגבלת פרסומים שיווקיים מטעים
ממשל בינה מלאכותית	מסגרת מוגבלת של אמצעי ממשל בינה מלאכותית כגון: פעילות בהתאם למסמכי מדיניות ונהלים פנימיים של הגוף המפוקח הנוגעים למערכות מידע. פעילות בהתאם למסמכי מדיניות ונהלים פנימיים של הגוף המפוקח הנוגעים למיקור חוץ. ככל שמדובר במערכות הכרוכות בסיכון רב יותר, נדרשות גם בקורות לפני הכנסת המערכת ובמהלך פעילותה; רכישת ידע, הבנה ומיומנות מעמיקים יותר ביחס למערכת; גיבוי למערכת ויכולת להחליף אותה במקרה של כשל מהותי. אחריות מלאכותית כגון: מסגרת משמעותית של אמצעי ממשל בינה מלאכותית כגון: מינוי ממונה בינה מלאכותית. אישור מערכת הבינה המלאכותית על-ידי דירקטוריון הגוף המפוקח. בקורות הדוקות לפני הכנסת המערכת ובמהלך פעילותה. רכישת ידע, הבנה ומיומנות מעמיקים ביחס למערכת. גיבוי למערכת ויכולת להחליף אותה במקרה של כשל מהותי. הקפדה ביחס למיקור החוץ המשמש בהפעלת המערכת, בין היתר ביחס לתלות במיקור החוץ והמידע בו נעשה שימוש.	מסגרת מוגבלת של אמצעי ממשל בינה מלאכותית כגון: פעילות בהתאם למסמכי מדיניות ונהלים פנימיים של הגוף המפוקח הנוגעים למערכות מידע. פעילות בהתאם למסמכי מדיניות ונהלים פנימיים של הגוף המפוקח הנוגעים למיקור חוץ. ככל שמדובר במערכות הכרוכות בסיכון רב יותר, נדרשות גם בקורות לפני הכנסת המערכת ובמהלך פעילותה; רכישת ידע, הבנה ומיומנות מעמיקים יותר ביחס למערכת; גיבוי למערכת ויכולת להחליף אותה במקרה של כשל מהותי. אחריות מלאכותית כגון: מסגרת משמעותית של אמצעי ממשל בינה מלאכותית כגון: מינוי ממונה בינה מלאכותית. אישור מערכת הבינה המלאכותית על-ידי דירקטוריון הגוף המפוקח. בקורות הדוקות לפני הכנסת המערכת ובמהלך פעילותה. רכישת ידע, הבנה ומיומנות מעמיקים ביחס למערכת. גיבוי למערכת ויכולת להחליף אותה במקרה של כשל מהותי. הקפדה ביחס למיקור החוץ המשמש בהפעלת המערכת, בין היתר ביחס לתלות במיקור החוץ והמידע בו נעשה שימוש.

במסגרת הערות הציבור לדוח הביניים התקבלו התייחסויות הנוגעות בין היתר לחשיבות ניהול הסיכונים וקביעת רמת הסיכון. היו מעירים שטענו בהקשר זה כי הואיל ומדובר בסיכון חדש ומתפתח, יש חשיבות רבה ליצירת מומחיות בעניינו, אך נכון בשלב זה להשאיר דרגות חופש ארגוניות כיצד ליישם זאת. מעירים אחרים סברו, לעומת זאת, כי על הרגולטור להגדיר תהליך ניהול סיכונים ברור וכן רשימת סיכונים ברורה. בהקשר זה, ובהתייחס גם לכלי ממשל הבינה המלאכותית שהוצעו בדוח, היו מעירים שסברו כי נכון לדוגמא להציב דרישות קשיחות לעניין גורם אחראי בארגון להיבט סיכוני בינה מלאכותית.

הצוות ביקש בין היתר את התייחסות הציבור לסיווג שהוצע בדוח הביניים, לקטגוריות של סיכון נמוך, בינוני וגבוה. אחת ההערות בהקשר זה היתה כי עדיף למקד את הרגולציה ביישומים בעלי פוטנציאל סיכון גבוה. הערה אחרת היתה כי הגדרת רמות הסיכון שהוצעה בדוח אינה ברורה דיה ונעדרת קריטריונים כמותיים ואיכותיים, וכי יש לקבוע קריטריונים כאמור, כגון רמת ההשפעה האפשרית על הפרט או כמות ואופי הנתונים האישיים המעובדים במערכת. הערות אלה נוגעות למעשה למידת הפירוט והקשיחות של המלצות הדוח ביחס לגישה מבוססת סיכונים. בהינתן שמדובר בשלב ראשוני עדיין של אימוץ מערכות בינה מלאכותית, במגוון הגדול של מערכות בינה מלאכותית אפשריות, ובהתחשב בכך שיש במקרים רבים מסגרות קיימות ברגולציה הפיננסית העוסקות בניהול סיכונים, הצוות סבור כי קביעת מסגרת קשיחה ופרטנית במסגרת המלצות הדוח לא תהא נכונה, אם כי אפשר שבעתיד יהיה לה מקום.

ביחס לחלוקה לקטגוריות סיכון, נערך שינוי בדוח, והחלוקה המוצעת כעת היא לסיכון נמוך-בינוני ולסיכון גבוה. שינוי זה נועד להקל על היישום, ונעשה גם בהתחשב בכך שהחלוקה לשלוש דרגות סיכון – נמוך, בינוני ונמוך – אינה מקבילה לחלוקה בחקיקת האיחוד האירופאי. בחקיקה זו שתי רמות הסיכון הגבוהות אופיינו כמפורט לעיל, כ"סיכון שאין לקבלו" וכ"סיכון גבוה". על פניו, קטגוריית הסיכון שאין לקבלו, עוסקת בפרקטיקות שהמחוקק האירופאי קבע כי יהיו לא חוקיות, ולכן הצוות לא ראה מקום לייחד לה קטגוריית סיכון עצמאית. כמו-כן, הסיכונים הנוספים שאופיינו בחקיקת האיחוד האירופאי – סיכון שקיפות וסיכון של בינה מלאכותית כללית – יכולים להתבטא לדעת הצוות בעוצמות סיכון שונות. על כן לא אומצה גם בדוח הסופי חלוקת הסיכונים שננקטה על-ידי האיחוד האירופאי. הצוות סבור כי הגמישות שהוענקה ביחס לטיפול ברמות הסיכון השונות, תומכת אף היא בחלוקה פשוטה יותר, לשתי דרגות סיכון, שכן ביחס לכל מערכת אפשר יהיה לנקוט באמצעים ההולמים להתמודדות עם הסיכונים הגלומים בה. בד בבד יובהר, כי לא התקבלה ההערה לפיה מערכות שאינן ברמת סיכון גבוהה צריכות שלא להיות מטופלות במסגרת דוח זה והרגולציה הפיננסית בכלל. דוח זה עוסק גם במערכות ברמות סיכון אלה אך מציע להתאים את הטיפול לרמת הסיכון.

במענה לשאלה שהוצגה על-ידי הצוות אם סיווג הסיכונים צריך להיעשות בידי הגופים המפוקחים או הרגולטור, התקבלו התייחסויות מנוגדות. אחד הגורמים המעירים טען כי הגופים המפוקחים הם הגורם היעיל ביותר לקביעת רמת הסיכון, בעוד שהיו גורמים אחרים שקראו לרגולציה הדוקה יותר בנושא זה, שתספק הכוונה ברורה יותר ביחס לסיווג הסיכונים. הצוות בדעה, כי בשלב זה של הטמעת הטכנולוגיה ולנוכח השימושים האפשריים הרחבים שלה, סיווג רמת הסיכון של מערכות בינה מלאכותית צריך שיעשה בראש ובראשונה בידי הגופים המפוקחים. בד בבד, הרגולטור הפיננסי יוכל לקבוע בעתיד כללים ספציפיים, לפיהם למשל מערכות בעלות פונקציות מסוימות או בתחומים מסוימים הן ברמת סיכון גבוהה. המלצה בעניין זה נוספה לדוח.

הערה שלא התקבלה על-ידי הצוות היתה כי יש לייחד את הדוח למערכות בינה מלאכותית שאינן מיועדות לפעילויות פנימיות בגופים הפיננסיים. על בסיס גישה מבוססת סיכונים כפי שהוצגה לעיל, יש לבחון לא רק את רמת הסיכון ללקוחות או למשקיעים אלא גם לגוף הפיננסי עצמו. על כן אין מקום לעסוק רק במערכות המיועדות לצרכים חיצוניים, ובפרט לאינטראקציה עם לקוחות, אלא גם מערכות בינה מלאכותית לצרכים פנימיים עשויות להיות רלבנטיות ודוח זה עוסק אף בעניינו.

יציבות פיננסית

ההתמודדות עם סיכוני יציבות פיננסית היא אינטרס פיקוחי ממדרגה ראשונה, לשם הגנת כספי הציבור, שמירה על תקינות פעילותה של המערכת הפיננסית, ומניעת משברים פיננסיים העלולים לפגוע במשק בכללותו. ההכרה בחשיבותם של סיכוני יציבות פיננסית גברה בעקבות המשבר הפיננסי העולמי של שנת 2008, אשר המחיש את הצורך לבחון את המערכת הפיננסית באופן רחב, להבדיל מבחינה של רכיבים או מוסדות ספציפיים בתוכה, ולעמוד על מגמות וסיכונים העלולים להשפיע באופן מהותי לשלילה על פעילותה. בעקבות המשבר התרחבו במדינות העולם העיסוק והבקורות בנוגע לסיכונים מערכתיים, וכך גם בישראל, בה הוקמה הוועדה ליציבות פיננסית, במטרה לתמוך ביציבותה של המערכת הפיננסית ובפעילותה הסדירה. הוועדה הוקמה בשנת 2018 לפי חוק בנק ישראל, והיא פועלת באמצעות תיאום, שיתוף פעולה ושיתוף מידע, בין כלל הגורמים הרלוונטיים לנושא היציבות הפיננסית – בנק ישראל, משרד האוצר והרגולטורים הפיננסיים.³⁴⁷

האם כניסתה של בינה מלאכותית לסקטור הפיננסי עלולה להביא עימה סיכוני יציבות פיננסית? התשובה העקרונית לכך היא חיובית; הסיכונים ליציבות פיננסית מיוחסים בדרך כלל למישורים העיקריים הבאים:

עדריות (herding) ותנודתיות – השימוש באותם מודלים של בינה מלאכותית על-ידי מספר גדול של שחקנים במערכת הפיננסית עלול להוביל להתנהגות עדרית, קרי פעולה נרחבת של שחקנים רבים באופן דומה. הדבר עלול להגביר סיכונים, בעיקר בעתות משבר. כך לדוגמה, ירידות בשוקי ניירות הערך עלולות להוביל למכירות גדולות המבוצעות בו-זמנית, ובאופן זה להעצים את הירידות ואת תנודתיות השוק.³⁴⁸ יש לציון, כי גם ללא התממשות הסיכון בעתות משבר, שימוש באותם מודלים ומידע לקבלת החלטות עלולים לפגוע בגיוון הדעות וההחלטות הקיים במערכת. יו"ר רשות ניירות הערך האמריקאית, פרופ' גארי גנסלר, הזהיר בהקשר זה מפני התכנסות ואי גיוון ("monocultures") אשר המערכת הפיננסית צפויה לחוות אם לא תינקט התערבות מהירה ביחס לשימוש בבינה מלאכותית.³⁴⁹ חשש נוסף הוא כי מערכות בינה מלאכותית המאומנות על מידע שנוגע לפעילות שגרתית, יובילו בעת התרחשות אירועים לא שגרתיים בשוק, לקבלת החלטות לא נכונה באופן שיגדיל את הסיכון למשבר.

ריכוזיות ותלות בצדדים שלישיים – ריכוז פעילות פיננסית בידי מספר קטן של גורמים, המחזיקים במידע וביכולות הטכנולוגיות לשימושי בינה מלאכותית, מעורר חששות לא רק במישור התחרותי אלא גם במישור היציבות הפיננסית. ריכוזיות עלולה להגביר את הסיכון מהתרחשות של כשל תפעולי או אחר, לנוכח השפעתו המסתברת על היקפי כספים גדולים יותר ועל גורמים רבים יותר. סיכון הריכוזיות בתחום הבינה המלאכותית בפיננסיים קשור באופן הדוק לתלות שצפויה להתפתח במספר קטן של חברות בתחום הבינה המלאכותית. ככל שיישומי בינה מלאכותית יסופקו או יהיו תלויים במערכות של מספר קטן של גורמים, הפעלתן התקינה של אותן מערכות תהא תלויה למעשה באותם צדדים שלישיים. סיכון זה מטריד רגולטורים פיננסיים גם מפני שאותם צדדים שלישיים לרוב אינם כפופים לרגולציה הפיננסית, אלא נמצאים מחוץ לטווח הפיקוח הישיר שלה.

קישוריות (interconnectedness) והדבקה (contagion) – סיכונים אלה נוגעים לחשש כי זעזעים בגוף או בחלק מסוים של המערכת הפיננסית יתפשטו ובמהירות לגופים ולאזורים נוספים במערכת. קישוריות והדבקה נובעות מקשרים ישירים ועקיפים בין מוסדות ושוקים פיננסיים, ומהמהירות והאופן הלא צפוי לעתים בהם קורלציה או תלות בין גורמים שונים במערכת באות לידי ביטוי. בהקשר של בינה מלאכותית, קישוריות והדבקה עלולות להיווצר בין היתר בדוגמאות שצוינו לעיל, שעה שתנועת השוק מוכתבת מהחלטות המתקבלות באופן נרחב על-ידי מערכות בינה מלאכותית, או כאשר ספקים חיצוניים של מערכות בינה מלאכותית נותנים שירות למגוון גורמים, ופגיעה בפעילותם התקינה משליכה על תקינות עבודתם של שחקנים פיננסיים רבים.

סיכונים תפעוליים וסיכוני סייבר – ככל שהתועלת משימושי בינה מלאכותית תגדל והטכנולוגיה תוטמע בתהליכים פנימיים רבים במערכת הפיננסית, כך עלולים להתגבר הסיכונים התפעוליים וסיכוני הסייבר הקשורים בטכנולוגיה. השפעתם של סיכונים אלה על היציבות הפיננסית קשורה מטבע הדברים גם במישורים האחרים שצוינו לעיל.

³⁴⁷ להרחבה ראו חוק בנק ישראל (תיקון מס' 7), התשע"ט-2018 אשר אושר ביום 26.11.2018 והצעת החוק מיום 25.1.2017.

³⁴⁸ דוח ה-OECD משנת 2021, בעמ' 8.

³⁴⁹ ראודבריו של פרופ' גנסלר מיום 17.7.2023 – <https://www.sec.gov/news/speech/gensler-isaac-newton-ai-remarks-07-17-2023> וכן דבריו בראיון מיום 15.10.2023: <https://www.ft.com/content/8227636f-e819-443a-aeba-c8237f0ec1ac>.



לסיכונים האמורים מצטרפים מאפיינים של מערכות בינה מלאכותית אשר נדונו בדוח זה. כך למשל, מאפיין של "קופסה שחורה" המקשה על הבנת פעולת המערכת, מגביר מטבע הדברים את הסיכון הגלום בה, הואיל וקשה יותר לקיים בקורות לגביה, בהשוואה למערכת רגילה. בדומה לכך, סיכון של **הסתמכות יתר** על מערכות בינה מלאכותית וצדדים שלישיים, והשימוש הפוטנציאלי הנרחב במערכות בינה מלאכותית בהשוואה למערכות רגילות, עלול להגביר סיכון יציבותי.³⁵⁰

להלן דוגמאות למצבי קיצון וסיכונים אפשריים כתוצאה משימוש מוגבר בבינה מלאכותית במגזר הפיננסי:

1. מכירות נכסים פיננסיים המזרזות "תגובת שרשרת" – מצב שבו מספר גופים פיננסיים מובילים משתמשים באותו מודל לביצוע מכירות אוטומטיות בו-זמנית בהיקף משמעותי, ואלה מזרזות בתורן נפילת שערי נכסים פיננסיים.
2. תמחור יתר בשוק ההון – אחידות באסטרטגיות ההשקעה על ידי גופים פיננסיים מעלה חשש כי נכסים פיננסיים מסוימים או דומים יטופחו על ידי כלי בינה מלאכותית. כתוצאה מכך עלולים להיווצר ביקוש ותמחור יתר לנכסים פיננסיים, באופן שאינו מותאם לערכם הריאלי אשר עלול לרדת באופן מהיר.
3. תקיפת סייבר – ניצול חולשות במערכות בינה מלאכותית המשמשות גורמים רבים במערכת, ויכולתם של התוקפים להשפיע על שחקנים רבים הפועלים באותו האופן או באמצעות אותן המערכות.
4. שגיאות מודל והסתמכות יתר של גופים פיננסיים – במצב בו גופים רבים מאמנים את המודלים שלהם על אותם מסדי נתונים, עולה חשש לחשיפה לאותן הטיות וחולשות המגולמות במסדי הנתונים הללו. בנסיבות קיצון עלול להיגרם כשל מערכתי אם מסדי הנתונים יכילו שגיאות או לא יהיו עדכניים.
5. החרפת מגמות פרו מחזוריות (procyclicality) – לצד החשש משימוש של גופים פיננסיים במודלים זהים או דומים, קיים בנוסף חשש שמודלים אחרים בעלי יכולות למידה יזהו מגמה שנוצרה לכאורה על ידי מודלים אחרים, ילמדו מהם ויבצעו פעולות דומות, וזאת באופן מופרז יחסית לבסיס הנתונים.
6. אפשר להעלות על הדעת דרכים שונות להתמודד עם סיכונים אלה, כגון דרישות הנוגעות להתקשרות עם ספקי מערכות בינה מלאכותית כדי לנטר ולצמצם את הסיכונים הנובעים מתלות אפשרית בהם. בד בבד, מדובר עדיין בסיכון עתידי ועל כן נראה שמדינות בעולם מסתפקות לעת עתה במעקב ובחינה של השלכות כניסתה העתידית של בינה מלאכותית על יציבות פיננסית.³⁵¹

European Central Bank, Financial Stability Review (May 2024), https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02_58c3ce5246.en.html 350

ראו למשל התייחסויות רשות הפיקוח היציבותי (PRA) והוועדה ליציבות פיננסית (FPC) בבריטניה בנושא: 351

The Bank and the PRA's response to DSIT/HMT: update on our approach to AI (April 22, 2024), section 12, at <https://www.bankofengland.co.uk/prudential-regulation/letter/2024/artificial-intelligence-and-machine-learning-letter>; Financial Policy Summary and Record of the Financial Policy Committee meeting on 21 November (December 6, 2023), sections 89– 94 at <https://www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2023/fpc-summary-and-record-december-2023.pdf>



המלצות בנושא יציבות פיננסית

כפי שצוין בפתח הדברים, בישראל פועלת הוועדה ליציבות פיננסית, במסגרתה ניתן יהיה להמשיך ולבחון את ההשלכות של כניסת בינה מלאכותית לסקטור הפיננסי על עמידות המערכת, כמו גם את ההתמודדות עם סיכונים מערכתיים ליציבות הפיננסית.

בשלב זה, לנוכח היקף האימוץ המוגבל של יישומי בינה מלאכותית והעדר צעדים קונקרטיים במדינות העולם, הצוות סבור כי יש מקום להמשך מעקב ובחינת הצורך בנקיטת פעולות בעתיד. פעולות אלה יכול שיכללו מיפוי של פעילויות הנתונות לסיכון משמעותי, בחינת המסגרות הקיימות להתמודדות של מוסדות פיננסיים עם סיכונים תפעוליים וסיכוני סייבר, וגיבוש אסטרטגיה לצמצום סיכונים מערכתיים הנובעים מהסתמכות על צדדים שלישיים שהם קריטיים לתפקודה של המערכת הפיננסית.



תיבה 3: מהו Flash Crash כתוצאה מפעילות אלגוריתמית במסחר?

השנה היא 2029. פאניקה פורצת בשוקי ההון בעולם כתוצאה ממכירה המונית של נכסים פיננסיים על ידי מערכות מסחר אלגוריתמיות אשר גורמת ל-"Flash Crash" הנובע משימוש בלתי מבוקר של בנקים, בתי השקעות וקרנות במודלים זהים של בינה מלאכותית. המודלים מנחים לבצע פעולות מכירה באותה העת, והמכירות ההמוניות מובילות לתגובת שרשרת בלתי נשלטת, לצניחה בשווקים ולמשבר אשראי רחב היקף. שוויים של חלק מהנכסים הפיננסיים מתאושש באותו היום, אך הנזקים הכלכליים נאמדים בטריליוני דולרים.

תרחיש בדיוני? לא ממש. יו"ר ה-SEC הקודם, פרופ' גארי גנסלר, התריע כי השימוש ההולך וגובר במערכות בינה מלאכותית יגרום קרוב לוודאי למפולת בשווקים הפיננסיים בנקודה מסוימת במהלך העשור הקרוב.³⁵²

אם תרחיש כאמור יתממש, לא תהיה זו הפעם הראשונה שבה מסחר אלגוריתמי גורם למפולת בשווקים הפיננסיים. האירוע, המכונה Flash Crash of 2010, אירע ב-6 במאי 2010 כאשר בתוך דקות ספורות מדד הדאו ג'ונס קרס בכ-900 נקודות אשר היוו כ-9% מהמדד ומספר דקות לאחר מכן "תיקן" המדד חלק ארי מהירידות.

באותו היום המסחר בשוק הנגזרים בארה"ב התאפיין בסנטימנט שלילי, בתנודתיות בלתי רגילה ובנזילות מעטה. חקירת האירוע הצביעה על הוצאה לפועל של תכנית מכירות של חוזים עתידיים בהיקף גדול מאוד באמצעות מסחר אלגוריתמי. כפי שעולה מדוח של הרגולטורים הפיננסיים בארה"ב, מסחר אלגוריתמי במהירות גבוהה (High Frequency Trading) האיץ את האפקט והעצים את הירידות. משבר הנזילות שהחל בשוק הנגזרים, השפיע גם על המסחר במניות, כאשר מנגנונים מובנים אוטומטיים הקיימים במערכות מסחר אוטומטיות המשמשות ספקי נזילות בשוק המניות, הביאו לעצירת המסחר באופן זמני. אחת ממסקנות הדוח הייתה שהמפולת אירעה בשל האינטראקציה בין המנגנונים המובנים האוטומטיים במערכות המסחר לבין האסטרטגיות של מערכות מסחר אלגוריתמיות.³⁵³

החשש מפני נפילות בשווקים בשל פעילות אלגוריתמית קיים אם כן ביתר שאת מאז שנת 2010. עם החדירה הצפויה של טכנולוגיית בינה מלאכותית לשווקים הפיננסיים, גובר החשש שריכוזיות ספקי המודלים ומערכות בינה מלאכותית מחד ושימוש הגובר בהם מאידך יגבירו את ההסתברות להישנות אירועים אלה.

פרופ' גארי גנסלר טען כי הפתרון לחשש צריך להימצא במסגרת ניהול סיכונים. בעוד המודלים הקיימים לניהול סיכונים בוחנים את הסיכון ברמת התאגיד, יש לאמץ שיטה שתאפשר לבחון את הסיכון ברמת המאקרו. לדבריו, על רגולטורים לאתר במהירות כלים לניהול סיכונים הקשורים בשימוש המוגבר בבינה מלאכותית במגזר הפיננסי על מנת להפחית את הסיכונים ליציבות הפיננסית.³⁵⁴

352 ראו Gensler, G. and L. Bailey (2020), "Deep Learning and Financial Stability", SSRN Electronic Journal, <http://dx.doi.org/10.2139/ssrn.3723132>; בהקשר זה ראו גם Financial Stability Board (2017), Artificial intelligence and machine learning in financial services Market developments and financial stability implications, <https://www.fsb.org/uploads/P011117.pdf>
353 ראו SEC and CFTC, Findings Regarding The Market Events Of May 6, 2010 (September 30, 2010), at <https://www.sec.gov/files/marketevents-report.pdf>; "מסחר בתדירות גבוהה – השפעותיו של שוק ההון והשפעות רגולציה עליו" דורון גרינברג, גיתית גור גרשגורן, רשות ניירות ערך (אוקטובר 2015), https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic//mechkar.pdf
354 ראו דבריו של פרופ' גנסלר, ה"ש 326 לעיל, וכן סקירת הבנק האירופאי המרכזי (ECB) מחודש מאי 2024, ה"ש 327 לעיל.

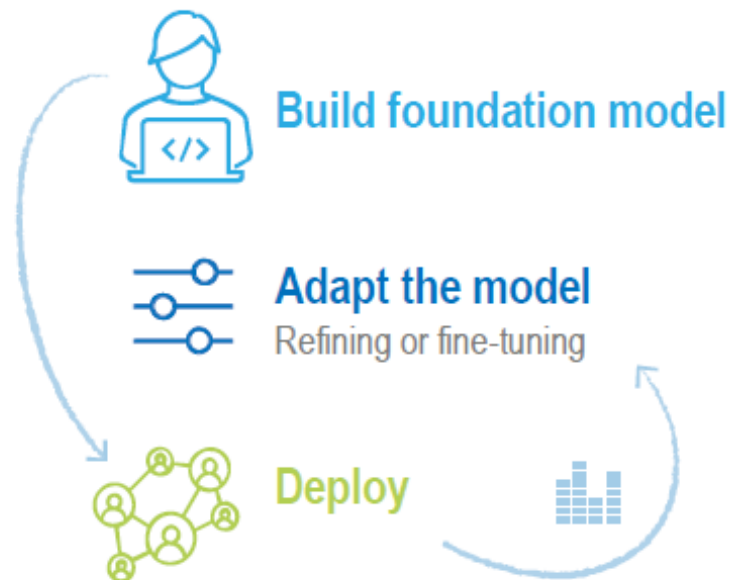


תחרות

לבינה מלאכותית יש פוטנציאל להגביר את הפיריון בתחום הפיננסי, להניע חדשנות ולקדם יצירת מוצרים ושירותים חדשים שייטיבו עם הציבור. לנוכח חשיבותה הצפויה של בינה מלאכותית בשנים הקרובות, שאלת התחרות בתחום זה הופכת אף היא משמעותית מאוד. לצורך פיתוח הטכנולוגיה, הטמעתה בשווקים והשגת התועלות מהטכנולוגיה על ידי הצרכנים, נדרשת תחרות אפקטיבית ודינמית בתחום שירותי הבינה המלאכותית.³⁵⁵

שלבים בפיתוח מודלים של בחינה מלאכותית

על מנת לנתח תחרותית את תחום הבינה המלאכותית, נדרשת ראשית הבנה של השלבים המרכזיים בפיתוח מודל בינה מלאכותית והתשומות הנדרשות לכך. במסמך שפרסמה ועדת התחרות של ארגון ה-OECD בשנת 2024, מתוארים השלבים הנדרשים לפיתוח מודל בינה מלאכותית באופן שלהלן:³⁵⁶

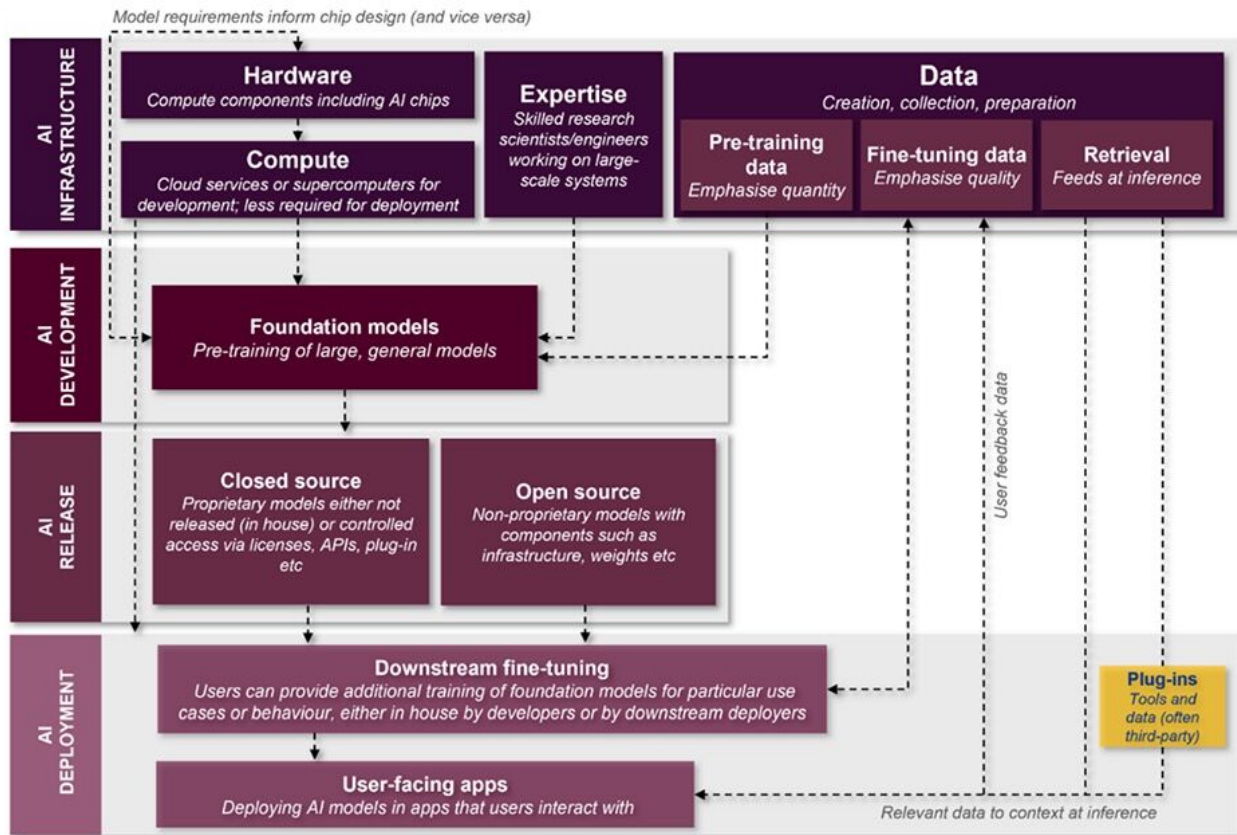


OECD (2024), "Artificial intelligence, data and competition", OECD Artificial Intelligence Papers, No. 18, OECD Publishing, 355
Paris, <https://doi.org/10.1787/e7e88884-en>, בעמ' 17 (להלן בפרק זה: "דוח ועדת התחרות של ארגון ה-OECD").

356 דוח ועדת התחרות של ארגון ה-OECD, בעמוד 15.



בשנת 2024, רשות התחרות הבריטית (CMA) הציגה באופן ויזואלי את פירוט התשומות הנדרשות עבור כל שלב משלבי הפיתוח של מודל בינה מלאכותית, באופן הבא:³⁵⁷



כפי שניתן לראות, שלבי הפיתוח העיקריים הם:

א. **יצירת התשתית לפיתוח המודל** – לצורך כך נדרשת גישה לשלוש תשומות עיקריות:

- **ראשית**, יכולת מחשובית. מודלים של בינה מלאכותית משתמשים במספר רב של חישובים מתמטיים על מנת לפתח את המודל ולייצר את הפלט שלו.³⁵⁸ העלות להשגת היכולת המחשובית לפיתוח מודל משתנה בהתאם לגודל של המודל ולכמות המידע הנחוצה לפיתוח שלו, אך בכל מקרה מדובר בעלות משמעותית. האפשרויות העיקריות להשגת יכולת מחשובית הן בניית חדר מידע עצמאי; שימוש במחשב-על (supercomputer) זמין לציבור; או דרך אחת מספקיות שירותי הענן.

- **שנית**, גישה למומחיות, ידע ויכולות פיתוח – לצורך כך נדרש כוח אדם מיומן.

- **שלישית**, גישה למידע. את המידע צריך לייצר, לאסוף ולהכין לשימוש. כפי שיפורט להלן, המידע הנדרש הוא הן מידע פומבי הן מידע קנייני.

ב. **פיתוח המודל היסודי** – בשלב זה בעצם מתפתח ה"ידע" של המודל. השלב מתבצע באמצעות מידע לצורך "אימון מוקדם" של המודל והדגש הוא על כמות רבה של מידע, ולא על איכות המידע. לכן, בדרך כלל בשלב זה נעשה שימוש במידע פומבי ופחות במידע קנייני.

ג. **שחרור המודל לשוק** –

- **מודלים של קוד פתוח** – אלו מודלים פתוחים לשימוש הציבור, ללא עלות, בכפוף לתנאי הרישיון שלהם. במקרים רבים, מודלים של קוד פתוח מאפשרים שימוש במודל יסודי ומאפשרים למשתמש לבצע כוונן של

CMA AI strategic update (29 April 2024), <https://www.gov.uk/government/publications/cma-ai-strategic-update/cma-ai-strategic-update> (להלן בפרק זה: "דוח רשות התחרות הבריטית משנת 2024").³⁵⁷

UK Competition and Markets Authority (CMA), AI Foundation Models Initial Report (18 September 2023)³⁵⁸ (להלן בפרק זה: "דוח רשות התחרות הבריטית משנת 2023"), בעמוד 12.



המודל לצרכים הנדרשים שלו.

- **מודלים של קוד סגור** – אלו מודלים שמפותחים על ידי חברות ספציפיות, מיועדים לצרכיהן ואינם פתוחים לציבור. לעיתים החברות משלבות את המודלים הללו במוצרים קיימים שלהן, לפעמים הן מייצרות באמצעותם שירותים או מוצרים חדשים ולפעמים הן משווקות את מודל הבינה המלאכותית עצמו כשירות לצדדים שלישיים שישלבו אותו בתוך העסק שלהן.

ד. **הטמעה ושימוש במודל** –

- **כוונון המודל** – בשלב זה מתבצע תהליך של כונון מודל שעבר אימון מוקדם לצורך משימה או פעולה ספציפית. כעת הדגש הוא על איכות המידע ופחות על כמות המידע ובמקרים רבים נעשה שימוש במידע קנייני ולא במידע פומבי.
- **אפליקציות למשתמשים** – זהו השלב שבו המשתמשים מבצעים שימוש במודל. ככלל, מודל של בינה מלאכותית ממשיך להתפתח ולהשתפר גם במהלך השימוש בו. עצם השימוש במודל מייצר מידע נוסף שבאמצעותו ניתן לחזור ולבצע את שלב כונון המודל ולשפר את הביצועים של המודל. השימוש במודלים של בינה מלאכותית נחלק ככלל לשימוש במודלים של קוד פתוח ושימוש במודלים של קוד סגור.³⁵⁹

מאפייני התחרות של תחום הבינה המלאכותית

כפי שיפורט להלן, מרבית החששות התחרותיים בתחום פיתוח המודלים של בינה מלאכותית נוגעים לחסמים בגישה לתשומות הנדרשות, חשש מחיזוק המעמד הדומיננטי של חברות הטכנולוגיה הגדולות באמצעות מודלים של בינה מלאכותית וחשש מהתפתחות שווקים בעלי דינמיקה של "המנצח לוקח הכל" או "המנצח לוקח הרוב".³⁶⁰

א. **יתרונות לשחקנים הפועלים ראשונים בתחום**

בתחום הבינה המלאכותית עשויים להיות יתרונות לשחקנים הפועלים ראשונים בשוק. יחד עם זאת, כיוון שמדובר בתחום שבו הדינמיקה התחרותית עדיין מתפתחת, לא ניתן לענות בשלב זה על השאלה עד כמה היתרונות הללו יהיו משמעותיים לאורך זמן.

- **אפקט רשת ו"לולאות משוב" (feedback loops)** – ככל שבמודל מסוים משתמשים יותר לקוחות, כך מצטבר יותר ידע שמזין את המודל ומאפשר שיפור מתמיד שלו. כאשר המודל הולך ומשתפר ישנו תמריץ לעוד ועוד לקוחות להשתמש בו. כאשר מתחרה נכנס לשוק בשלב ראשוני ומגייס לקוחות, יש לו אפשרות לפתח מודל איכותי, לשפר את המודל על פי צרכי הלקוחות ולגרום לכך שלקוחות ייטו לפנות לאותו מתחרה בשל היתרון הראשוני.³⁶¹ באופן זה, עלול להיווצר חסם עבור שחקנים שמגיעים בשלב מאוחר יותר ומעוניינים להיכנס לשוק.

- **שימוש במודלים לא מושלמים** – בשלב הראשוני של כניסת הטכנולוגיה לשוק, המשתמשים עדיין סבלניים לטעויות או חוסרים במודלים. לאחר שימוש נוסף של משתמשים במודל, שיאפשר איסוף נתונים ואימון נוסף של המודל, יושלמו החוסרים והטעויות הללו. אולם, ככל שהטכנולוגיה מתפתחת, המשתמשים יהיו פחות ופחות סבלניים למודלים שאינם מושלמים ויעדיפו לעשות שימוש במודלים הוותיקים. חברה חדשה שתצא להיכנס לשוק תהיה חייבת להיכנס עם מודל שפועל ללא טעויות וחוסרים.³⁶²

- **עלויות כניסה** – עלויות הכניסה בשלב מוקדם של פיתוח התעשייה צפויות להיות נמוכות יותר מעלויות הכניסה בשלב מאוחר יותר. למשל, עלויות מחשוב או עלויות של מידע, ככל הנראה יעלו ככל שחברות נוספות ייכנסו לשוק וייצרו ביקוש רב לאותן תשומות.³⁶³

- **הכרה במוטג ונאמנות לקוחות** – לחברות שנכנסות ראשונות יש יכולת לרכוש נאמנות של הלקוחות ולמצב את עצמן כחברות המובילות של השוק.³⁶⁴

כאמור לעיל, כיוון שתחום הבינה המלאכותית נמצא עדיין בשלבים ראשוניים, התפתחות הדינמיקה התחרותית

359 שם, בעמ' 14.

360 דוח ועדת התחרות של ארגון ה-OECD, בעמ' 27.

361 שם, בעמ' 28.

362 דוח רשות התחרות הבריטית משנת 2023, בעמ' 48.

363 שם.

364 שם.



בתחום זה אינה ברורה דיה. ייתכן שלשחקנים שייכנסו ראשונים לשווקים יהיו גם חסרונות. למשל, ייתכן שהמודלים הראשונים יהיו פחות מדויקים או פחות יעילים ממודלים שיתפתחו בשלבים מאוחרים יותר, לאחר למידת תובנות מהמודלים הראשונים. ייתכן גם שמודלים יסודיים שייבנו במודל פתוח, יאפשרו לשחקנים שייכנסו בשלב מאוחר להדביק את הפער באופן מהיר ואולי אף באופן מותאם ונכון יותר משחקנים שנכנסו בשלב מוקדם, וזאת אף מבלי להשקיע השקעות בפיתוח מודל יסודי.

ב. יתרונות לשחקנים גדולים

- **יתרונות לגודל** – עלויות הפיתוח הראשוניות של מודל הן גבוהות. היכולת לעשות שימוש בתוכנות, באלגוריתמים, במידע, בטכניקות אימון מודלים ועוד, במספר רב של מודלים ועבור מספר רב של לקוחות, מאפשר לחברות גדולות לנצל יתרונות לגודל ולפתח מספר מודלים בעלות נמוכה יותר.³⁶⁵
- שימוש בבסיס לקוחות קיים – ככל שלחברה יש לקוחות רבים יותר, כך ניתן לנצל באופן משמעותי יותר את אפקט הרשת ואת "לולאות המשוב" ולשפר את המודל באופן מתמיד.³⁶⁶
- **יתרונות להיקף** – חברות שפעילות בשווקים רבים יכולות לעשות שימוש במודל אחד, בשיטות הפיתוח, באלגוריתמים או בתשומות גם לשווקים אחרים וכך להשיג יתרונות להיקף. למשל, מידע עשוי לתת לחברות יתרונות להיקף, אם איסוף מידע משוק אחד מאפשר לפתח מודל בינה מלאכותית טוב יותר בשווקים אחרים.³⁶⁷
- **חברות הטכנולוגיה הגדולות** – אחד האתגרים המרכזיים בתחום הבינה המלאכותית הוא שחברות הטכנולוגיה הגדולות, שהינן בעלות כוח שוק בשווקים טכנולוגיים רבים, עלולות לפתח את התחום ואת השווקים שמושפעים ממנו באופן שעלול לפגוע בתחרות אפקטיבית. חלק מחברות הטכנולוגיה הללו הן בעלות כוח רב בתשומות הנדרשות לצורך פיתוח מודלים של בינה מלאכותית ויש להן יכולת השפעה משמעותית על היכולת של מפתחי מודלים מבוססים בינה מלאכותית לחדור לשווקים. נוסף על כך, העובדה שלאותן חברות יש כוח משמעותי בשוקי טכנולוגיה קיימים, אשר יכולים להיות מאוימים תחרותית על ידי מודלים של בינה מלאכותית, נותנת להם תמריץ לפעול להגבלת התחרות בתחום הבינה המלאכותית.³⁶⁸

ג. חסמי מעבר

מודלים של בינה מלאכותית יכולים ללמוד את העדפות ויכולות המשתמש באופן שמקשה על מעבר בין מתחרים. למשל, אם המודל יכול ללמוד את ההעדפות של הצרכן הפיננסי, תהיה עלות לאותו צרכן לעבור למתחרה אחר, כיוון שייקח זמן עד שהמודל החדש ילמד גם הוא את אותן ההעדפות של הצרכן.

חששות תחרותיים בתחום הבינה המלאכותית

לאור כל האמור, החששות התחרותיים המרכזיים שעולים בהקשר לתחום הבינה המלאכותית הם:

- היעדר גישה לתשומות** (כוח מחשובי, מידע, מומחיות) – חברות שמחזיקות בתשומות העיקריות לפיתוח מודלים של בינה מלאכותית עלולות למנוע גישה אליהם על מנת לבצר את מעמדן התחרותי.
- צמצום מרחב הבחירה של לקוחות בשוק** – קיים חשש כי חברות הטכנולוגיה הגדולות יצמצמו את מרחב הבחירה של השחקנים בשירותי בינה מלאכותית. למשל, ביחס לבחירה הראשונית של אופן ההטמעה של מודל הבינה המלאכותית, ליכולת המעבר בין מודלים או בין ספקים שונים לאורך זמן ועוד.
- ביצור מעמד דומיננטי** – שותפויות בין שחקני מפתח בתחום יכולות לחזק את מעמדן של חברות בעלות כוח שוק לאורך שרשרת האספקה.³⁶⁹
- 'המנצח לוקח הכל'** – קיים חשש, לפיו שווקים מבוססי בינה מלאכותית, יפתחו דינמיקה של 'המנצח לוקח הכל'. השאלה אם השווקים יתפתחו לכיוון זה תלויה בשאלות משנה: עד כמה מדובר בשווקים המתאפיינים ביתרונות לגודל בהיבט המידע; עד כמה יש צורך בשירות מותאם אישית לכל לקוח מצד נותן השירות; ועד כמה מדובר

365 שם, בעמ' 49.

366 שם.

367 דוח ועדת התחרות של ארגון ה-OECD, בעמ' 27.

368 דוח רשות התחרות הבריטית משנת 2024, בעמ' 12.

369 שם, בעמ' 13.



בשווקים שבהם יש אפקט רשת.

ה. **נקיטת פרקטיקות אנטי תחרותיות על ידי המודלים** – למשל, מודל בינה מלאכותית שתוכנת על מנת להשיא רווחים עבור החברה, עשוי לנקוט בפעולות של דחיקת מתחרים, ניצול לקוחות, או אפליית לקוחות שעלולים להוות פרקטיקות אנטי תחרותיות. יתרה מכך, מודלים של בינה מלאכותית עשויים, באופן אוטומטי וללא התערבות אדם, להבין וליישם פרקטיקות של תיאום בין מתחרים, עד כדי קרטלים של ממש.

ו. **יצירת התאמה על ידי שימוש של מתחרים באותו מודל של בינה מלאכותית** – כאשר מתחרים מבצעים שימוש במודל אחד של בינה מלאכותית, לשם קבלת החלטות עסקיות של כל אחד מהם בנפרד, קיימת סכנה כי קבלת ההחלטות של כל המתחרים תתקבל באופן זהה ויווצר חשש מהתאמה בין השחקנים, ללא ביצוע תיאום מפורש ביניהם.

תחרות ובינה מלאכותית בסקטור הפיננסי בישראל

א. מקומם של השחקנים הפיננסיים בישראל בתחום הבינה המלאכותית

ארגון ה-OECD מחלק את שרשרת האספקה של תחום הבינה המלאכותית לשלוש קבוצות עיקריות: קבוצה ראשונה היא ספקי הידע והתשומות לפיתוח מודלים של AI (מידע, בניית קוד, שבבים, חוות שרתים ועוד). קבוצה שנייה היא השחקנים הפעילים בפיתוח ועיצוב המודלים. הקבוצה השלישית היא המשתמשים העסקיים של המודלים שמטמיעים אותם בתהליכי העבודה שלהם, במוצרים שלהם ובשירותים שלהם.³⁷⁰

הגופים הפיננסיים בישראל הם, ככלל, רוכשי התשומה של מודלים של בינה מלאכותית. יחד עם זאת, לאור העובדה שגופים פיננסיים בישראל מחזיקים במידע רב על לקוחות, ייתכן שיהיו גופים פיננסיים שגם יפתחו מודלים בעצמם או גופים שיפתחו מודלים בשיתוף פעולה עם שחקנים אחרים בתחום הטכנולוגיה שיספקו את התשומות הנוספות הדרושות לפיתוח המודל.³⁷¹

השחקנים הפיננסיים בישראל צפויים גם לשלב מודלים של בינה מלאכותית בתוך השירותים הקיימים שהם מציעים ללקוחות. קיימת אפשרות שמודלים של בינה מלאכותית יאפשרו להם להציע שירותים פיננסיים חדשים, וקיימת אף אפשרות שבאמצעות שיתופי פעולה, אותם גופים פיננסיים יהפכו לנותני שירותים של שירותי בינה מלאכותית לגופים פיננסיים אחרים בישראל.

ב. מאפיינים תחרותיים של שוק הפיננסיים בישראל

על אף צעדים רגולטוריים שונים שננקטו בשנים האחרונות שנועדו להגביר את התחרות בתחום הפיננסי ולאפשר כניסה של שחקנים חדשים לתחום, יש בסקטור הפיננסי בישראל תחומים שונים המאופיינים בריכוזיות גבוהה, בין היתר בשל חסמי כניסה וחסמי מעבר גבוהים. כך, בתחום הבנקאות, חמש הקבוצות הבנקאיות הגדולות מחזיקות בכ-98% מהנכסים. התחום מתאפיין בחסמי כניסה ומעבר גבוהים וברמת תחרות נמוכה, במסגרתה הבנקים ממעטים להתחרות באופן אגרסיבי על לקוחות של בנקים אחרים ולהציע מוצרים "פריקים" ללקוחות שאינם מנהלים אצלם חשבון. כתוצאה מכך, מרבית הצרכנים רוכשים את סל השירותים הבנקאי מהבנק בו הם מנהלים את חשבון העו"ש שלהם, מבלי לערוך תיחור של ממש לבנקים או שחקנים חוץ-בנקאיים אחרים. יוצא אפוא, כי למערכת הבנקאית מאפיינים המאפשרים היווצרות של שיווי משקל מתואם, כאשר לשחקנים השונים יש תמריץ לשמר מאפיינים אלה, כך שלכל בנק קיים כוח שוק כלפי לקוחותיו.

תחום הביטוח באופן כללי מתאפיין ברמת תחרות גבוהה יותר, אם כי גם בתחומי ביטוח מסוימים יש רמת ריכוזיות גבוהה, למשל, ביטוחי בריאות, ביטוחי חיים ותחומים נישתיים נוספים. בצד זאת, מידת התחרות שרואים הצרכנים היא ככל הנראה פחותה, שכן קיימות בעיות מבניות חמורות בכל הנוגע לפעילותם ותמריציהם של סוכני ביטוח. בעיות אלה מביאות לכך שהתחרות בין חברות הביטוח היא לרוב על הסוכנים ותחרות זאת אינה מתגלגלת לטובת ציבור המבוטחים.

ככלל, שירותים פיננסיים מתאפיינים ביתרונות ברורים לגודל, כאשר ישנה חשיבות משמעותית להתאמת השירות באופן אישי ללקוח ולמאפייניו הפרטניים.

370 דוח ועדת התחרות של ארגון ה-OECD.

371 שם.



ג. חששות תחרותיים מהטמעת מודלים של בינה מלאכותית בתחום הפיננסיים בישראל

נוכח האמור, קיים חשש מהתפתחותו של כוח שוק בתחום מתן שירותי בינה מלאכותית למגזר הפיננסי בישראל ומכך שהשימוש של גופים פיננסיים בישראל בבינה מלאכותית יגביר את הריכוזיות הקיימת בתחום הפיננסיים עצמו, כפי שיפורט להלן:

1. **חשש מהתפתחותו של כוח שוק בתחום נותני שירותי בינה מלאכותית אל מול גופים פיננסיים בישראל** – כתוצאה מהיתרונות לגודל, מאפקט הרשת ומהחשיבות למוניטין הקיימים בתחום מתן שירותי בינה מלאכותית ועל רקע האפשרות ששוקי הבינה המלאכותית בתחומים שונים יתפתחו לעבר שווקי 'המנצח לוקח הכל' (או הרוב) קיים חשש ליצירתו והתעצמותו של כוח שוק על ידי נותני שירותי בינה מלאכותית, למשל חברות טכנולוגיה גדולות, אל מול הגופים הפיננסיים בישראל.
2. **היעדר גישה למידע** – כאמור לעיל, היעדר גישה לתשומות הוא אחד החששות התחרותיים המשמעותיים ביותר. השחקנים הקיימים בתחום הפיננסיים הם בעלי גישה למידע קנייני רב שנצבר אצלם במהלך שנות פעילותם בתחום וממשיך להצבר ולהתעדכן באופן רציף. באמצעות המידע הזה, ניתן לפתח מודלים של בינה מלאכותית, להתאים אותם לצרכים שונים של כל גוף פיננסי, ולהתאים את המודל לצרכים הקבועים והמשתנים של כל לקוח ולקוח. אמנם, לצורך פיתוח מודל בינה מלאכותית נדרשות תשומות נוספות, כמו יכולות מחשוביות ומומחיות אך הגופים הפיננסיים הקיימים יכולים להתגבר על כך באמצעות שיתופי פעולה עם חברות טכנולוגיה לצורך פיתוח מודלים שימשו את ורק אותן. שחקנים פיננסיים חדשים שאינם מחזיקים במידע בהיקפים דומים, עלולים לעמוד בפני חסמי כניסה משמעותיים, בשל חוסר היכולת לפתח ולאמן מודל על סמך מידע קיים.
3. **הגופים הפיננסיים הקיימים הם שחקנים גדולים שצפויים להיות הראשונים בשוק** – כפי שתואר לעיל, עלולים להיות יתרונות תחרותיים לשחקנים שנכנסים ראשונים לתחום הבינה המלאכותית. העובדה שהגופים הפיננסיים הקיימים יטמיעו ראשונים מודלים של בינה מלאכותית עשויה להעניק להם יתרונות בשוק, כמו יצירת אפקט רשת, חיזוק הנאמנות המותגית, או עלויות כניסה נמוכות, שלשחקנים חדשים יהיה קשה לגשר עליהם בשלב מאוחר יותר.
4. **יתרונות לגודל ולהיקף** – כפי שתואר לעיל, תחום הבינה המלאכותית מאופיין ביתרונות לגודל, ביתרונות להיקף וביכולת לבצע שימוש בבסיס לקוחות קיים על מנת לשפר את היכולות של המודל. העובדה שהגופים הפיננסיים הקיימים הם גופים גדולים, בעלי איתנות כלכלית גבוהה וחלקם פעילים במספר רב של שווקים, מאפשרת להם לפתח מודל ולעשות בו שימוש במספר רב של שירותים פיננסיים ואף לעשות שימוש בבסיס הלקוחות הקיים על מנת לשפר את המודל באופן יעיל ומהיר. כל אלה, עשויים להעלות את חסמי הכניסה או ההתרחבות של שחקנים אחרים בתחום.
5. **פרקטיקות אנטי תחרותיות** – כאמור לעיל, מודלים של בינה מלאכותית עשויים במישרין או בעקיפין לנקוט בפרקטיקות של העדפה עצמית, אפליית לקוחות או קשירה בין שירותים. ככל שהשירות והתמחור שניתן לכל לקוח הוא אישי וככל שמידע על כל לקוח הוא משמעותי יותר לאופן התמחור, כך יש אפשרות רבה יותר להפלות בין לקוחות, לקשור בין שירותים או לבצע העדפה עצמית. לכן, בתחום הפיננסיים, אשר מאופיין במתן שירות אישי לכל לקוח על בסיס מידע אישי ובכך שהגופים הפיננסיים הקיימים מחזיקים מידע רב על לקוחותיהם, קיים חשש לפיו מודלים של בינה מלאכותית ינצלו זאת ויבצעו אפליה בין לקוחות באופן שעלול לפגוע בהתפתחות התחרות בתחום. כמו כן, מודלים של בינה מלאכותית עשויים לאפשר לגופים הפיננסיים הגדולים לבצע קשירה בין מוצרים באופן טוב יותר – המודלים יזהו את העדפות הלקוחות, את הרצונות שלהם ואת אופן הפעולה שלהם וייצרו קשירה בין מוצרים שתשיא את רווחי הגוף הפיננסי.³⁷² חלק מהפרקטיקות האמורות יכולות להביא לעיתים לתרומה לצרכן, אך בנסיבות מסוימות עלולות גם לגרום לפגיעה בתחרות ובציבור. חשש נוסף הוא מצב בו גופים פיננסיים בעלי מידע שנדרש לצורך פיתוח מודלים של בינה מלאכותית, יגבילו או יפגעו בגישה לאותו מידע ויסרבו באופן בלתי סביר לספק אותו למתחריהם.³⁷³
6. **חשש מתיאום והתאמה בשוק** – החשש נובע משימוש של גופים פיננסיים רבים באותו מודל. ככל שגופים פיננסיים שונים יעשו שימוש באותו מודל לשם קבלת החלטות עסקיות, למשל קבלת החלטות השקעה, קבלת החלטות על מתן ותמחור אשראי ועוד, קיים חשש להיווצרות תיאום או התאמה ביניהם. ככל שמדובר בשוק

372 שם, בעמ' 45.

373 שם.

פיננסי שבו קיימת ריכוזיות גבוהה יותר בין השחקנים הקיימים בשוק, כך החשש הוא משמעותי יותר. יצוין, כי חשש זה עשוי להשפיע הן על ההיבט היציבותי והן על ההיבט התחרותי.

במסגרת הערות הציבור לדוח הביניים נטען בין היתר כי יש להיזהר מתחולה שגויה של דיני התחרות. בהקשר זה נטען כי הגישה לפיה הסקטור הפיננסי מאופיין בריכוזיות גבוהה אינה נכונה בהכרח עבור כלל הענפים, כי לבינה מלאכותית יכולים להיות יתרונות תחרותיים רבים, וכי החשש התחרותי צריך להתמקד בכוחן של חברות הטכנולוגיה. הצוות סבור כי בדוח זה אין מקום לדון בפירוט במידת התחרות בסקטור הפיננסי, אולם ודאי שנקודת המוצא היא כי פעילויות מסוימות בסקטור זה סובלות מריכוזיות. הדוח מרחיב על יתרונות פוטנציאליים של הבינה המלאכותית (כך נפתח גם פרק זה), ואף מתייחס לכוחן של חברות הטכנולוגיה הגדולות, אך אין בכך כדי להסיר את הצורך בבחינה ובהמלצות לגבי פעילויות הגופים המפוקחים המקומיים.

הערות נוספות קראו להבחין בין מישורי התחרות השונים – יוצרי הכלים של הבינה המלאכותית שצפויים לכלול בעיקר חברות זרות; שווקים ליצירת אפליקציות שצפויים להיות גם הם בינלאומיים בעיקרם; ושירותי השימוש באפליקציות שמאופיין בתחרות מקומית. חלוקה זו מקובלת על הצוות, ופורטה גם בדוח, בהתבסס על הניתוח שערך ה-OECD בנושא. בהמשך לכך, הוצע לבחון עניינים ספציפיים כגון הסכמי בלעדיות או עדיפות בשימוש בכלי בינה מלאכותית, או כללי שיתוף במידע. בהינתן קצב אימוץ הטכנולוגיה כפי שתואר בדוח, נראה שנקיטה בצעדים קונקרטיים בעניינים אלה תהא מוקדמת, אך אפשר שתידרש בעתיד.

הערות נוספות נגעו מחד לחששות של תיאום מידע (למשל תיאום במחירים או מנגד תיאום פעולות מסחר) ומאידך לצורך בשיתוף מידע של הגופים הפיננסיים המסורתיים עם גופים חדשים כדי שאלה יוכלו להתחרות. הצוות מסכים לחשיבותם של היבטים אלה, כפי שבא לידי ביטוי בהמלצה הראשונה בפרק הקובעת את העיקרון של תחולת דיני התחרות גם ביחס לפעילות של בינה מלאכותית, ובהמלצה השלישית העוסקת בגישה למידע אגרגטיבי ואנונימי כדי לאפשר את התנאים להתפתחותה של תחרות.



המלצות בנושא תחרות

נוכח ניתוח השוק והחששות התחרותיים שהוצגו לעיל, יוצגו להלן התייחסויות והמלצות במטרה לצמצם את החששות התחרותיים.

(1) תחולת דיני התחרות גם ביחס לפעילות של בינה מלאכותית -

ראשית, חשוב להדגיש שדיני התחרות ימשיכו לחול גם מקום בו הפרקטיקות האנטי תחרותיות יתבצעו באמצעות מודלים של בינה מלאכותית או כתוצאה מהפעלתם של מודלים כאמור. לדוגמה: הסדר כובל שישתכלל באמצעות בינה מלאכותית יהווה הפרה של הוראות סעיף 2 לחוק התחרות הכלכלית, התשמ"ח-1988 (להלן: "חוק התחרות"), כאשר המפרים עשויים להיות הן המשתמשים במודל והן מפתח המודל. דוגמה נוספת היא מקרה שבו בעל מונופולין ימנע גישה של מתחרים לתשומות מרכזיות שנדרשות לפיתוח מודלים של בינה מלאכותית, כמו מידע. מקרה כזה עלול להוות הפרה של סעיפים 29 ו-29א לחוק התחרות. הדבר נכון גם במקרה של מניעת גישה למודלים בנסיבות מסוימות. כך גם, מקום בו בעל מונופולין יבצע קשירה בין שירותים פיננסיים או אפליה בין לקוחות, עלולים המעשים להוות הפרה של סעיף 29א לחוק התחרות, אף אם הפעולה בוצעה באמצעות מודלים של בינה מלאכותית ובאופן לא מכוון.

(2) בחינת חששות להיווצרות כוח שוק או חסמים לתחרות במסגרת בחינת מיזוגים -

שנית, במסגרת בחינת מיזוגים המונחים על שולחן הממונה על התחרות, הרשות תשקול, בין היתר, חששות להיווצרות של כוח שוק או חסמים לתחרות בהקשרים המתוארים לעיל, כמו גם חששות ליצירת יכולת לבצע פרקטיקות כאמור שעלולות לפגוע בתחרות,³⁷⁴ כל זאת באמצעות שימוש, בין היתר, במודלים של בינה מלאכותית.

(3) גישה למידע אגרגטיבי ואנונימי -

שלישית, על מנת לאפשר את התנאים להתפתחותה של תחרות בתחום מתן שירותי בינה מלאכותית במגזר הפיננסי בישראל, ועל רקע החששות המוצגים לעיל, מוצע לאפשר לגורמים פיננסיים גישה למידע אגרגטיבי ואנונימי מתוך מאגר הנתונים הנמצא אצל בנק ישראל במאגר נתוני אשראי, כמו גם שימוש באמצעים ובתשתית הקיימים מכוח בנקאות פתוחה כדי להרחיב את המידע הנגיש לשחקנים הפיננסיים השונים, באופן שיאפשר לאותם גורמים לפתח מודלים של בינה מלאכותית באמצעות שימוש באותו מידע. נכון להיום, בנקאות פתוחה מאפשרת ללקוחות הבנקים, חברות כרטיסי האשראי וגופים נוספים לשתף צדדים שלישיים במידע הפיננסי שלהם. כך, שחקנים פיננסיים, יכולים לגשת לחשבון הבנק של הלקוח, בהסכמתו, ולהציע לו שירותים בנקאיים מותאמים לצרכיו. ואולם, על מנת לפתח מודלים של בינה מלאכותית, נדרשת גישה למידע רב על פני זמן ואין די בנתונים על לקוח בודד או בנתונים שנאספו על פי הסכמה פרטנית של לקוחות. בנק ישראל מסתייג מהמלצה זו.

(4) בחינת דרכים למניעת התפתחות כוח שוק -

רביעית, מוצע לא להסתפק בטיפול בחסמי הכניסה וחסמי המעבר לתחום מתן שירותי בינה מלאכותית לסקטור הפיננסי בישראל, במיזוגים בעייתיים ובהפרות חוק התחרות, אלא למנוע, מבעוד מועד, את התפתחותו של כוח שוק בתחום זה. כוח שוק של נותן שירותי בינה מלאכותית יכול להוביל הן להפעלת כוח שוק כלפי הגופים הפיננסיים, הן לסיכויים גבוהים יותר לקיומה של התאמה או תיאום בין השחקנים השונים בשוק כתוצאה משימוש באותו מודל, הן לכוח מיקוח של אותו גורם מול הגופים הפיננסיים

374 דוגמה לכך היא התנגדותה של הרשות בתחילת שנת 2024 למיזוג בין חברת כרטיסי האשראי הישראלית לבין חברת הביטוח הראל. במסגרת הבחינה נמצא שהמיזוג מעלה חשש סביר לפגיעה משמעותית בתחרות בתחום ביטוחי בריאות פרט, בו הראל היא חברה מובילה. נמצא כי אם יאושר המיזוג, קיים חשש שהחברה הממוזגת תוכל לדחוק את מתחרותיה מהשוק או לפגוע בכושרן התחרותי וביכולתן לרסן את כוח השוק שלה. החשש התמקד בפגיעה בתחרות שתעשה באמצעות שימוש במידע של ישראל כרטיס בנוסף למידע של הראל כדי לקבוע מחיר מותאם אישית ללקוחות (בין היתר, על סמך נכונות הלקוח לשלם) ובכך לגרוף יותר רווח מבסיס לקוחות נתון, באופן שיאפשר להראל למשוך אליה סוכני ביטוח. ראו התנגדות הממונה על התחרות למיזוג בין הראל השקעות בביטוח ושירותים פיננסיים בע"מ לבין ישראל כרטיס בע"מ, 2024, <https://www.gov.il/he/pages/cases2023-008372>



והמאסדרים והן לחשש יציבותי, בין היתר כתוצאה מהתלות בגורם אחד משמעותי. ניתן לחשוב על דרכים שונות למניעת התפתחותו של אותו כוח שוק. למשל, ניתן לקבוע הוראה רגולטורית לפיה נותן שירות בינה מלאכותית אחד, לא יעניק שירות לשחקנים שמחזיקים במצטבר מעל נתח שוק מסוים בשוק ספציפי בישראל. או למשל, לקבוע חובה לשחקנים פיננסיים בשוק מסוים או בעלי מאפיינים מסוימים, לעבוד עם יותר מנותן שירותי בינה מלאכותית אחד. מטבע הדברים, לכל הוראה יתרונות וחסרונות ומומלץ לבחון אותה בהתאם לנסיבות השוק ואופן פעילות המפוקחים.



סיכונים תפעוליים ובהם סיכוני סייבר, סיכוני צד שלישי, הונאה ודיסאינפורמציה ("מידע כזב")

סיכונים תפעוליים (operational risks) כוללים קשת רחבה של פגמים פוטנציאליים העלולים לגרום נזק לפעילותו של ארגון, כפועל יוצא של כשלים פנימיים או אירועים חיצוניים.³⁷⁵ ניהול סיכונים תפעוליים אפקטיבי נדרש מכל מוסד פיננסי והוא כולל זיהוי, הערכה, בקרה והתמודדות עם סיכונים אלה באמצעות מגוון כלים ותהליכים.

ההתפתחות והזמינות של כלי הבינה המלאכותית תורמות לגידול בסיכונים התפעוליים המאיימים על גופים פיננסיים, ובהם סיכוני סייבר, סיכוני צד שלישי, סיכוני הונאה ומידע כוזב (דיסאינפורמציה). החדשנות הטכנולוגית ממניחה את מחסום הכניסה לתוקפים ומייצרת טכניקות חדשות להפצה ואוטומציה של התקפות מקוונות. הכלים הגנרטיביים מעצימים עוד את פוטנציאל הסיכונים. הם מאפשרים לתוקפים לפתח ולהפעיל תוכנות זדוניות יעילות בעלות נמוכה ומרחיבים את היקף התוקפים והאיומים. התלות של מערכות בינה מלאכותית במאגרי נתונים ובצדדים שלישיים מגדילה את האתגרים הקיימים ומצריכה התמודדות גם במישור של גורמים חיצוניים לגופים הפיננסיים, השותפים בשרשרת הפיתוח והאספקה של מערכות הבינה המלאכותית.

איומי סייבר -

כלי בינה מלאכותית עלולים לסייע לתוקפים, בין היתר בהיבטים הבאים:

- **דיסאינפורמציה (מידע כזב):** טכנולוגיית בינה מלאכותית משמשת ליצירת תוכן מגוון העשוי להיחזות כאותנטי, ולשמש כך גורמים המבקשים לפגוע במערכת הפיננסית, בגופים ספציפיים או במשקיעים ובלקוחות. ראו בהרחבה על סיכון זה והשלכותיו בהמשך פרק זה.
- **קוד מחשב זדוני:** בינה מלאכותית יוצרת נמצאה שימושית בפיתוח קודים. תוקפים פוטנציאליים עשויים לפתח לפיכך קוד זדוני חדש או גרסה חדשה של תוכנה זדונית קיימת מהר יותר, ובאופן שיהיה קשה יותר לזהותו.
- **איתור חולשות במערכת:** תוקפים יכולים להשתמש בכלים מתקדמים מבוססי בינה מלאכותית כדי לזהות נקודות תורפה וחולשות במערכת הגנת הסייבר של הנתקף.

תקיפות סייבר עלולות לפגוע במערכות של גופים פיננסיים בין היתר בדרכים הבאות: "הרעלת" נתונים – פגיעה והשחתה של הנתונים המשמשים ללימוד המערכות ושל המודל כדי להטות אלגוריתם להשיג תוצאה רצויה; דליפת נתונים – באמצעות שאילתות באופן שהאלגוריתם של המודל "מתבלבל" וחושף מידע שאינו אמור להציג במתן התשובה; חשיפה של המודלים – למשל באמצעות שאילתות חוזרות והסקת המודל מתוצאותיהן; והטיית תוצאות המודל – הזנת קלט כדי להשיג תוצאה רצויה.

סיכוני צד שלישי -

בין שמוסד פיננסי מחליט לפתח פתרון בינה מלאכותית באופן עצמאי ובין שהוא מבקש לרכוש אותו דרך ספק, דרישות המשאבים של מערכות בינה מלאכותיות יגדילו בדרך כלל את התלות שלו בתשתיות מחשוב ונתונים של צד שלישי. לכן מוסדות פיננסיים חייבים להעריך ולנהל את הסיכונים של שרשרת אספקה מורחבת, לרבות סיכונים פוטנציאליים למאגרי נתונים ולעיבוד נתונים של מגוון רחב של ספקים, מתווכים וספקי תשתית.

צדדים שלישיים הקשורים לנתונים ולטיפול בהם יכולים לחשוף את המוסדות לסיכונים פיננסיים, משפטיים וסיכוני סייבר. במידה רבה, ההישענות על צדדים שלישיים יוצרת צורך אצל הגופים הפיננסיים לבחון כיצד להתמודד עם סיכונים שהועלו בדוח זה, ביחס לפעילות המתקיימת עבורם אצל גורמים חיצוניים. צורך זה קיים כבר כיום ביחס לפעילויות הנעשות אצל גופים פיננסיים תוך התבססות על צדדים שלישיים או אף במיקור חוץ, כגון שמירת גיבוי נתונים בענן, אולם ככל ששימושי בינה מלאכותית יהפכו שכיחים יותר, כך יתגבר הצורך להתמודד עם התלות בצדדים שלישיים, גם ביחס לפעילויות שאינן טכניות במהותן.

³⁷⁵ ראו לדוגמה הגדרת "סיכון תפעולי" בהוראת ניהול בנקאי תקין 350 של הפיקוח על הבנקים כ"סיכון להפסד כתוצאה מאי נאותות או מכשל של תהליכים פנימיים, אנשים ומערכות או כתוצאה מאירועים חיצוניים. הגדרה זו כוללת סיכון משפטי, אך אינה כוללת סיכון אסטרטגי וסיכון תדמיתי (reputational)" (בסעיף 5 להוראה).



סיכוני הונאה -

כלי בינה מלאכותית עלולים לשמש למטרות הונאה בדרכים שונות. כך למשל, הם עלולים לאפשר לנוכחים להתחזות לעובדים ולקוחות של מוסדות פיננסיים, ביתר קלות בהשוואה לעבר, באמצעות חיקוי של קול, תמונה, וידאו וגורמים התנהגותיים נוספים שמוסדות פיננסיים משתמשים בהם כדי לאמת את זהות הלקוח. שימושים אפשריים נוספים למטרות הונאה הם פיצוח סיסמאות בעזרת כלי בינה מלאכותית כדי להשיג גישה לחשבונות של לקוחות, או זיהוי פרטי מידע אישי של לקוחות ברשת או במאגרי מידע על מנת להשיג גישה כאמור.³⁷⁶

על אף שהמסגרת הרגולטורית הקיימת בהקשר של סיכונים תפעוליים אינה מתייחסת במפורש לבינה מלאכותית, העקרונות הכלולים בה יכולים לסייע באימוץ בטוח ואחראי של הטכנולוגיה. יחד עם זאת, יתכן כי בתהליך הלמידה וההערכה של הטכנולוגיה, יידרשו תיקונים והבהרות לרגולציה הקיימת, ככל שיזוהו פערים.

דיסאינפורמציה ("מידע כזב") -

מבין הסיכונים התפעוליים ראה הצוות לנכון ליחד מקום מיוחד לסיכוני דיסאינפורמציה המעוררים חששות רבים, ולבחון באופן מפורט יותר את השלכותיהם על הסקטור הפיננסי.

מניפולציה ושיבוש שיטתי של מידע, המכונים פעמים רבות גם "דיסאינפורמציה" או "ידיעות כזב", הינם תופעה רווחת בעידן הדיגיטלי, שמטרתה להשפיע על תוכן המופץ ברשת או אמצעים דיגיטליים אחרים, וכפועל יוצא גם על ההחלטות המתקבלות על בסיס אותו מידע. אף טרם הופעתה של טכנולוגיית הבינה המלאכותית, פעלו בעלי אינטרס שונים להפצת דיסאינפורמציה באמצעות יצירה של ידיעות שקריות והפצתן על-ידי ישויות פיקטיביות מרובות הנשלטות על-ידי מעט גורמים, ערבוב מכוון של מסמכים אמיתיים ופיקטיביים והכוונה של עיתונאים ואנשי ציבור אל אותו מידע משובש.³⁷⁷

תופעת הדיסאינפורמציה אינה חדשה אם כן, ואולם זמינותם ותפוצתם של כלי בינה מלאכותית מקלים על יצירתה, מגבירים את היקפה ואת התאמתה לנמענים, ולכן גם את האפקטיביות שלה בהשגת מטרות הגורם המשבש.³⁷⁸ יישומי בינה מלאכותית יוצרת (Generative AI) מאפשרים ליצור באמצעות שאילתה קצרה, תוכן חדש – טקסטים, תמונות, סרטונים, מוזיקה ועוד, ובכך מקלים על יצירת תוכן סינתטי, פיקטיבי שקשה ולעיתים כמעט בלתי-אפשרי להבדיל בינו לבין תוכן אותנטי. כלי בינה מלאכותית נוספים יוצרים אפשרויות הפצה חדשות של תוכן כזה.³⁷⁹

סיכון הדיסאינפורמציה נתפש כאחד הסיכונים המשמעותיים בהתפתחותה של הבינה המלאכותית. בסקר הסיכונים שערך ארגון ה- World Economic Forum לשנת 2023–2024 דורג סיכון זה במקום גבוה במיוחד,³⁸⁰ ויש כבר המחשות מן העבר ומן ההווה להתממשותו בקשר עם מערכות בחירות במדינות דמוקרטיות, ובקשר עם עימותים פוליטיים או בין-מדינתיים.³⁸¹ בפרט זיופים עמוקים (Deepfakes), המהווים נדבך מרכזי בסיכון הדיסאינפורמציה תוך שימוש בטכנולוגיית הבינה המלאכותית, הוגדרו על ידי מומחי פשיעה כלכלית כאחד הסיכונים הגדולים עמם יתמודד המגזר הפיננסי בשנים הקרובות.³⁸² המונח Deepfake משמש לתיאור תכני בינה מלאכותית היוצרת מניפולציה של תמונה, קול או וידאו, בין היתר לשם זיוף של תמונת המציאות, לרבות חיקוי התנהלות או דברים של אדם, אשר לא התרחשו במציאות. יש דוגמאות רבות לזיופים אלה, אשר בשל השימוש בבינה מלאכותית, הולכים ומשתכללים, ונהיים קשים ביותר לזיהוי. במקביל, הפקתם הפכה זמינה, קלה וזולה בהינתן טכנולוגיית הבינה

376 כפי שיפורט להלן, סיכוני הונאה עלולים להתממש גם באמצעות דיסאינפורמציה, אולם אין חפיפה בין הדברים. עשויים להיות כאמור ניסיונות הונאה בעזרת בינה מלאכותית שאינם בדרך של דיסאינפורמציה, ועשויות להיות פעולות דיסאינפורמציה שאינן למטרות הונאה (אלא למשל לשם פגיעה במערכות על-ידי גורמים עוינים למדינה).

377 רועי גולדשמידט "השימוש בבינה מלאכותית ליצירה והפצה של חדשות כזב" מרכז המחקר והמידע של הכנסת, בעמ' 2 (21.12.2023).

378 ראו ה"ש 55 לעיל.

379 ראו ה"ש 354 לעיל.

380 World Economic Forum, Global Risks Report 2023 (January 10, 2024), <https://www.weforum.org/publications/global-risks-report-2024/in-full/>; יש לציין כי דירוג גבוה זה נבע בין היתר מהחששות להתממשות סיכוני דיסאינפורמציה במהלך מערכות בחירות חשובות העתידות להתקיים, בין היתר בארה"ב ובבריטניה.

381 לדיון בדוגמאות אחרונות לתופעה זו: Hanna Murphy "The rising threat to democracy of AI-powered disinformation" Financial Times (January 11, 2024), <https://www.ft.com/content/16f23c01-fa51-408e-acf5-0d30a5a1ebf2>; Tate Ryan-Mosley "How Generative AI is boosting the spread of disinformation and propaganda" MIT Technology Review (October 4, 2023), <https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/>.

382 <https://www.bloomberg.com/news/articles/2023-08-21/money-scams-deepfakes-ai-will-drive-10-trillion-in-financial-fraud-and-crime>.



המלאכותית.³⁸³ לא מן הנמנע שהתכנים יופקו מחוץ לגבולות הארץ על ידי גורמים עברייניים או עוינים.

באיזו מידה רלוונטי סיכון הדיסאינפורמציה לתחום הפיננסיים וכיצד ניתן להתמודד עימו?

החלטות הציבור הרחב לגבי פעילותו הפיננסית, כמו גם המסחר בשווקים ופעילותם של גופים פיננסיים גדולים, מבוססים על קבלת מידע מהימן בהיקפים גדולים ובתדירות גבוהה ועל אמון הציבור בגופים ובמערכת הפיננסית. משכך, תחומי פעילות אלה (כמו גם תחומי פעילות אחרים המושתתים על קליטה ועיבוד של מידע רב) רגישים במיוחד לתופעת הדיסאינפורמציה, והתממשות סיכון הדיסאינפורמציה בהיקף נרחב עלולה לגרום לא רק נזק לכספי משקיעים ולקוחות, אלא גם לפגוע ביציבות המערכתית.

ואכן, בשנים האחרונות ניתן היה לראות דוגמאות לשימוש בבינה מלאכותית לשם יצירת דיסאינפורמציה המשתיה נזק בתחום הפיננסי. דוגמה ידועה היא פרסום מזויף ברשת החברתית X (לשעבר טוויטר) בשנת 2013, לפיו התרחש פיצוץ בבית הלבן, ובעטיו צנחו מדדי המסחר בבורסה בארה"ב. בעקבות הפרסום, התבצעה מכירת ענק של ניירות ערך על-ידי יישומי מסחר אלגוריתמי ואבדו השקעות בשווי מיליארדי דולרים.³⁸⁴ בדומה לכך, בחודש מאי 2023 שותפו ברשת החברתית X תמונות מזויפות של עשן מיתמר בקרבת הפנטגון. בדקות שלאחר התפשטות המידע ברשתות החברתיות (ובמקרים מסוימים אף באמצעי תקשורת מסורתיים) ועד להבנה כי מדובר במידע כוזב, חווה שוק המניות האמריקאי ירידות בולטות.³⁸⁵

יש לשים לב לכך שדיסאינפורמציה אינה בהכרח הפצת מידע כוזב ושקרי, וניתן לראות מקרים בהם נעשה ניסיון להציג מידע אמיתי באופן שמערכות בינה מלאכותית יסווגו אותו באופן שונה מכפי שניתן היה לצפות. דוגמה לכך היא הימנעותם של תאגידים הנסחרים בבורסה משימוש במילים הנתפסות כבעלות הקשר שלילי על-ידי מערכות בינה מלאכותית למסחר אלגוריתמי המבוססת על ניתוח שפה, כדי לשפר את הערכת מצבם בעיני השוק והסוחרים.³⁸⁶

כאמור, סיכון הדיסאינפורמציה אינו נובע מבינה מלאכותית בלבד. כאמור, ההתקדמות בבינה מלאכותית הגבירה מאוד את היכולת לייצר בקלות יחסית תוכן שקרי, וברמה המקשה מאוד על זיהוי התוכן כשקרי. ואולם, עוצמת סיכון הדיסאינפורמציה נגזרת ממגמות נוספות, כגון מידת השימוש ברשתות חברתיות והיכולת להעביר בהן תוכן שקרי, מידת ההישענות של הציבור הרחב על פלטפורמות אלה, מידת זליגת המידע למערכות אחרות כמו כלי התקשורת המסורתיים, והאמון שנותן הציבור בתכנים אלה. מכאן שגם ההתמודדות עם סיכון הדיסאינפורמציה עשויה להיות במישורים שונים, כגון חיוב הרשתות החברתיות לפקח על התכנים המפורסמים במסגרתם; סמכות להסרת תכנים; חובה לציין מהו מקור המידע במקרים מסוימים וכדומה.

התמודדות עם סיכון הדיסאינפורמציה בתחום הפיננסי

כפי שצוין לעיל, חלק מההתמודדות עם סיכונים דיסאינפורמציה מטופל במסגרת אסטרטגיית ההתמודדות של הרגולטורים הפיננסיים עם **סיכוני סייבר**. כך למשל, לפי חוזר רשות שוק ההון בעניין,³⁸⁷ "סיכון סייבר" מוגדר כסיכון הכולל גם שימוש לא מורשה בזהות (או התחזות), כאשר "אירוע סייבר" מוגדר גם כמקרה של תקיפת מערכות או אמצעי טכנולוגי אחר ששייכים לגוף מוסדי העלולה לפגוע, בין היתר, בשלמות המידע של הגוף המוסדי. סיכונים אלו כרוכים, במידה כזו או אחרת, בפעולת דיסאינפורמציה מצד התוקף המכוונת לפגוע בגוף המוסדי – התחזות ללקוח או ספק במערכות הגוף המוסדי או שיבוש המידע הקיים במערכותיו באמצעות כלי סייבר ואגב כך שיבוש פעילותו. בהתאם לכך, בחוזר נקבעו מנגנונים שונים להתמודדות עם סיכונים אלו, לרבות קביעת נהלים לניהול משתמשים והרשאות, ויישום נתיב בקרה וניטור של פעולות ושאליות המתבצעות במערכות המנהלות מידע רגיש על לקוחות

383 דוגמאות ל-Deepfakes שנערכו באמצעות בינה מלאכותית כוללות הקלטות או צילומים לכאורה של מנהיגים ואנשים ידועים אחרים תוך זיוף התוכן. ראו הרחבה בהקשר זה: Meredith Somers "Deepfakes, explained" MIT (July 21, 2020), <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>; Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Europol (13 March 2024), <https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes>.

384 Peter Foster, 'Bogus' AP Tweet about Explosion at the White House Wipes Billions Off US Markets, The Telegraph (23.04.2013), <https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html>.

385 https://edition.cnn.com/2023/05/22/tech/twitter-fake-image-pentagon-explosion/index.html?force_isolation=true.

386 דוח אונ' תל-אביב, בעמ' 21-22.

387 חוזר גופים מוסדיים 2016-9-14: ניהול סיכונים סייבר בגופים מוסדיים, רשות שוק ההון, ביטוח וחסכון (31.8.2016).

וכן במערכות שרמת החשיפה שלהן לביצוע פעילות בלתי מורשה הינה גבוהה, במטרה לאפשר זיהוי של פעילות בלתי מורשה אשר עלולה להתבצע באמצעות התחזות. עוד לפי החוזר האמור, גופים מוסדיים נדרשים להגדיר תכנית היערכות וניהול אירועי סייבר, כגון גישה לא מורשית לנכסי הגוף, זליגת מידע, התחזות, והונאה, וכן לבצע מבחני חדירה תקופתיים הכוללים בדיקות הנדסה חברתית, התחזות ופשיג. יוער כי עקרונות ומנגנונים דומים להתמודדות עם דיסאינפורמציה בקשר לסיכוני סייבר, מוצאים ביטוי גם בנוהל בנקאי תקין של המפקח על הבנקים בעניין ניהול הגנת סייבר.³⁸⁸ נקודה נוספת שיש לשים לב אליה בהקשר זה, היא כי בינה מלאכותית עשויה לשמש גם בעולמות הגנת הסייבר, שם נפתחה קשת חדשה של אפשרויות טכנולוגיות. בינה מלאכותית מאפשרת יכולות הגנה מתקדמות יותר, כגון איתור קשרים, חיבור אוסף פעולות לכדי רצף אחד, ייצור תוכנות בטוחות יותר, זיהוי מדויק ומהיר של חריגות בתהליכים ועוד, אשר ראוי לבחון שילובם כחלק מהמנגנונים האמורים.

מכאן שגם הטיפול בסיכוני דיסאינפורמציה עשוי להיעשות, לפחות בחלקו, במסגרות קיימות שנועדו לטפל בסיכוני סייבר לסוגיהם, או באמצעות אסדרה נפרדת.³⁸⁹ ואולם, גם בתחום הסייבר בינה מלאכותית משנה את כללי המשחק. כך, בינה מלאכותית עשויה להגביר ולהחמיר את תהליכי התקיפה, להתמקד בחולשות המערכת במהירות גדולה יותר ובאמצעותן לשבש מידע באופן סיסטמתי, לדמות התנהגות אנושית ולהתחזות ליעדים בצורה שנראית אמינה יותר מהיום. למעשה, בינה מלאכותית מביאה לגידול בקצב הופעת האיומים ובמהירות הנדרשת לטפל בהם, ובכלל זה התמודדות מול עלייה בקצב התקיפה, ושינוי ביכולות התקיפה בדרך של אוטומציה.³⁹⁰

יכולות הבינה מלאכותית והתפתחותה המואצת מצריכות אם כן חשיבה נוספת לגבי חוזקת המנגנונים הקיימים לשם התמודדות עם מתקפות סייבר. זאת ועוד, הטיפול בסיכוני סייבר מתמקד באופן מסורתי בתקיפה אפשרית של הגופים הפיננסיים, ופחות בסיכונים הנובעים מהפצת דיסאינפורמציה בשוק, העלולה להשפיע באופן עקיף על הפעילות הפיננסית, וגם מסיבה זו יש לבחון את מנגנוני ההתמודדות הקיימים. בבסיס טכנולוגיית הבינה המלאכותית נמצא מידע בהיקף גדול מאוד, ופגיעה בו (דוגמת הפצת דיסאינפורמציה בשוק או פעולה מכוונת אשר תשפיע על מהימנות המידע), בהכרח תשפיע על תוצרי המערכת.

מבין סיכוני הדיסאינפורמציה האפשריים לגבי פעילויות פיננסיות, סבור הצוות כי נדרשת תשומת לב רגולטורית מיוחדת ביחס לעניינים הבאים:

- **פעילויות פיננסיות בהן עשויות להתקבל החלטות מהירות על-ידי הציבור הרחב.** פעילויות אלה יתאפיינו ביכולת משיכת או הסטת כספים מהירה, ובכך שהן נעשות לעתים קרובות ללא תיווך פיננסי של גורם מקצוע (אשר עשוי "לצנן" פעולה מהירה או לא מבוססת). על פעילויות אלה נמנות לדוגמה השקעה בניירות ערך או בקרנות נאמנות (שאינה מיועצת) והפקדת כספים בפיקדונות או בחשבונות עובר ושב או חשבונות תשלום. סיכון זה גובר ככל שפעילות הציבור מתבססת על מידע ממקורות לא מבוססים, כגון מידע ברשתות החברתיות או אתרי אינטרנט לא מהימנים. בהקשר זה עלולה בינה מלאכותית לשמש להטיית פעילות לאפיקי השקעה המשרתים באופן מכוון שחקנים מסוימים בשוק או כדי לגרום נזק באופן מכוון למשקיעים ולמערכת הפיננסית.³⁹¹
- **פעילויות פיננסיות המתאפיינות בתמחור רציף על בסיס מידע.** הדוגמה המובהקת לכך היא פעילות הבורסה, שם מתקיים מסחר רציף בניירות ערך על בסיס מידע המתפרסם על-ידי התאגידים הנסחרים. דיסאינפורמציה בדבר תאגיד מסוים או בדבר אירוע חיצוני בעל השלכות מקרו-כלכליות לכאורה, עלולה להשפיע על התנהגות המשקיעים ושערי ניירות הערך (וראו להמחשה הדוגמאות של פרסום תמונות הכזב בבית הלבן ובפנטגון שהוזכרו לעיל). דוגמה נוספת היא פעילות בזירות סוחר הנעשית אף היא על בסיס תמחור שיש לו רגישות רבה יחסית למידע.
- **מוסדות פיננסיים החשופים לסיכוני הדבקה (contagion) וקישוריות (inter-connectedness).** המשבר

388 ניהול בנקאי תקין [3] (9/21): ניהול הגנת סייבר, המפקח על הבנקים (30.09.2021).

389 ראו, למשל, את חקיקת ה-Digital Services Act באיחוד האירופאי אשר נועדה להתמודד עם הפצת דיסאינפורמציה בפלטפורמות שונות, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

390 ראו דברי ראש מערך הסייבר בכנס נקסטק: "בינה מלאכותית משנה את כללי המשחק בסייבר", אתר מערך הסייבר הלאומי (24.11.2019), https://www.gov.il/he/pages/nextec2019?fireglass_rsn=true#fireglass_params&tabid=aab55ae619fd94f7&start_with_session_counter=9&application_server_address=isagovil-2-me-west1.prod.fire.glass

391 דוח אונ' תל-אביב, בעמ' 22.



הפיננסי העולמי בשנים 2007–2009 חשף את הסיכונים הנובעים למוסדות פיננסיים ולמערכת הפיננסית בכללותה כתוצאה מקשרים ישירים ועקיפים בין גופים שונים. בנוסף לכך, אפשר היה לראות במשבר זה את הסיכון הנובע מאי-וודאות במידע בנוגע למוסדות פיננסיים. כך למשל, נפילתו של בנק ההשקעות ליהמן ברדרס אשר התרחשה תוך זמן קצר לאחר שמוסדות פיננסיים אחרים סירבו להמשיך ולפעול מולו בהעדר מידע מלא ויכולת להעריך את הסיכונים הגלומים בפעילותו. דיסאינפורמציה עלולה להגביר סיכונים של הדבקה וקישוריות, שכן הם נוגעים למידע הקיים בידי מוסדות פיננסיים על אודות מוסדות ונכסים אחרים.

כמו-כן, הסתמכות של גופים פיננסיים על מערכות בינה מלאכותית זהות אשר עושות שימוש באלגוריתמים דומים ושואבות מידע (מוטעה) דומה, עלולה להביא לאפקט שרשרת שיפגע בשוק כולו. כאמור, מדובר בתופעה שעלולה להתרחש גם בשל טעויות אנושיות, ללא קשר לשימוש בבינה מלאכותית, ואולם המהירות המאפיינת מנגנונים אוטומטיים הפועלים על בסיס מידע חיצוני יוצרת סיכון מוגבר להתרחשות התופעה וכן מעצימה את השלכותיה בשל הקושי לקטוע את שרשרת האירועים בזמן. בהקשר זה, שימוש נרחב של סוחרים במודלים זהים או דומים מבוססי בינה מלאכותית, עלולה להביא לתופעה של "לולאת משב" – הדהוד המידע השגוי או המטעה בין הסוחרים, וכפועל יוצא לתנודתיות קיצונית בשווקים ואף להתרסקותם (Flash Crash).³⁹²

- **גופים פיננסיים העושים שימוש במערכות בינה מלאכותית לצורך פעולות פיננסיות מהירות.** בדומה לסיכון הראשון שתואר לעיל, שעניינו פעולות פיננסיות המתבצעות על-ידי הציבור הרחב, עשוי להתקיים סיכון דומה לגבי גופים פיננסיים העושים שימוש במערכות בינה מלאכותית. כך לדוגמה, גופים פיננסיים העושים שימוש במערכות אלגוריתמיות במסחר בניירות ערך או מנהלי תיקי השקעות המפעילים מערכת בינה מלאכותית לצורך קבלת החלטות השקעה עבור לקוחותיהם. מהירות ואוטומטיות הפעולה וההתבססות על מידע חיצוני בקבלת ההחלטות הם גורמים התורמים להגברת הסיכון כמתואר לעיל.
- **שימוש בבינה מלאכותית על מנת לעקוף מנגנוני אבטחה.** כך לדוגמה בינה מלאכותית עלולה לסייע בהתחזות לשם פריצה לחשבונות של לקוחות, לשם עקיפה של כללי הלבנת הון המבוססים בין היתר על הזדהות, או לשם עקיפת כללי פיקוח פיננסי מסוגים אחרים. פעולות התחזות באמצעות בינה מלאכותית יכולות להיות מופנות הן כלפי הציבור הרחב, לשם ביצוע הונאות, הן כלפי הגופים הפיננסיים.³⁹³ בהקשר זה בינה מלאכותית מגבירה סיכוני סייבר.

בהינתן שתופעת הדיסאינפורמציה אינה חדשה, התמודדו עימה רגולטורים פיננסיים גם בעבר באמצעות כלים שונים.

כך לדוגמה, בנוגע למסחר בניירות ערך בבורסה, קיימים כלים שנועדו להתמודד עם בעיות של השפעת מידע שטרם דווח או מידע לא אמין הגורר "חרושת שמועות" ושינויים חדים במחירי ניירות הערך. כלי אחד הינו הוראת הפסקת מסחר זמנית אשר יכולה להינתן על-ידי רשות ניירות ערך מכוח סמכותה לפי חוק ניירות ערך, או על-ידי הבורסה עצמה מכוח תקנון הבורסה. המקרים שבעטיים אפשר כי המסחר ייפסק הינם חריגה מהותית מחובת הדיווח על-ידי החברה, פרסום מידע שגוי לגבי השער של נייר ערך או קבוצת ניירות ערך, פרסום בדרך כלשהי של מידע מהותי המתייחסת לחברה לרבות לבעל השליטה בה או לניירות הערך שלה, התרחשות אירוע מקרו-כלכלי מהותי שיכול להשפיע על המסחר בקבוצה של ניירות ערך וכדומה.³⁹⁴ כלי נוסף הינו "מנתק זרם" העוצר את המסחר בניירות הערך לתקופה קצובה, במהלכה יכול השוק לבחון את המידע הרלוונטי ותגובת המחירים ביחס אליו.³⁹⁵ מישור התמודדות נוסף הוא בפן האכיפתי, במסגרתו כבר כיום ניתן להעמיד לדין בגין עבירות במסחר בניירות ערך, לרבות עבירות הנעשות תוך שימוש בטכנולוגיית בינה מלאכותית. הקושי בהקשר זה נוגע בעיקר לסמכויות החקירה אשר אינן נותנות מענה מספק להתמודדות עם עבירות מחשב. הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשפ"ג-2023, אשר מבקשת להסדיר את דיני החיפוש והתפישה של רשויות האכיפה בהליכים פליליים, יכולה להשלים את החסר.

392 דוח אונ'תל-אביב, בעמ' 82–83. וראו גם: Ghiath Shabsigh and El Bachir Boukherouaa Generative Artificial Intelligence in Finance: Risk Considerations (International Monetary Fund Fintech Notes (August 2023), <https://www.imf.org/en/publications/fintech-notes/issues/2023/08/18/generative-artificial-intelligence-in-finance-risk-considerations-537570>.

393 ראו על חקירת משטרה בהונג קונג בחשד כי עובד גוף פיננסי נפל קורבן להונאה במסגרתה העביר סכום של 25 מיליון דולר, וזאת לאחר שהצטרף לשיחת ועידה בוידאו, בה השתתפו לכאורה חבריו לעבודה, אך דמויותיהם היו זיופי deepfake. Heather Chen and Kathleen Magramo "Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'" CNN (February 4, 2024), <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>.

394 סעיף 338 לחוק ניירות ערך והחלק הרביעי לתקנון הבורסה.

395 הנחיות על פי החלק השלישי לתקנון הבורסה.

כלי נוסף להתמודדות עם מידע לא אמין הוא פרסום אזהרות והבהרות בידי רגולטורים ומוסדות פיננסיים. כך לדוגמה, פרסום אזהרות של מוסדות פיננסיים ללקוחותיהם (כגון אזהרות של חברות כרטיסי אשראי בנוגע לשימוש לרעה בפרטים אישיים של לקוחות) או פרסום הבהרות של רגולטורים בנוגע למצב השווקים או מידע הנוגע להם.³⁹⁶

בפרק הזמן שחלף מאז פרסום דוח הביניים התפשטה בעולם ובישראל תופעת ההונאות הפיננסיות באמצעות התחזות קולית וחזותית בעזרת כלי בינה מלאכותית. בין היתר ניתן היה לראות ניסיונות פנייה ללקוחות המערכת הבנקאית תוך זיוף זהות הפונה (אשר הוצג כבנק, כחברת כרטיסי אשראי או כגורם שלטוני) ופרסומים ברשתות החברתיות של סרטונים מזויפים של דמויות ידועות ברשתות החברתיות על מנת להניע השקעה בניירות ערך. הרגולטורים הפיננסיים פרסמו אזהרות וצעדי התגוננות מוצעים מפני פעילות עבריינית זו.

במסגרת הערות הציבור לדוח הביניים צוין כי היה מקום להרחיב עוד לגבי סיכוני סייבר, וכן כי יש מקום ליזום שינוי חקיקתי לגבי תהליכי הכר את הלקוח, שכן אלה חשופים בפרט להונאות באמצעות זיופים עמוקים (Deepfakes). הצוות מסכים כי יש חשיבות רבה לסיכוני סייבר בכלל לנוכח ההתפתחויות בבינה מלאכותית, וכן מכיר בכך שהם רלבנטיים לגבי תהליכי הכר את הלקוח, אך לא סבר שנדרש תיקון בעניין זה בדוח כיוון שניתן ביטוי לעוצמת סיכוני הסייבר בפרק זה, ותהליכי הכר את הלקוח אף הוזכרו ספציפית בדוח כאזור בו נדרשת תשומת לב רגולטורית מיוחדת.

396 ראו למשל אזהרת ארגון FINRA האמריקאי מפני הונאות משקיעים באמצעות בינה מלאכותית: FINRA "Artificial Intelligence (AI) and Investment Fraud" (January 25, 2024), <https://www.finra.org/investors/insights/artificial-intelligence-and-investment-fraud>.



המלצות בנושא סיכונים תפעוליים ובהם סיכוני סייבר, סיכוני צד שלישי, הונאה ודיסאינפורמציה

המלצת הצוות לרגולטורים הפיננסיים היא לערוך מיפוי של הפעילויות שיש להן חשיפה מיוחדת לסיכון דיסאינפורמציה ולבדוק אם הכלים הקיימים להתמודדות עם סיכון זה מספקים או שיש מקום לשכללם. בין הכלים הרגולטוריים שמוצע לבחון בהקשר זה לשם מיפוי הסיכונים והתמודדות עימם:

- הנחיית גופים מפוקחים להעריך את סיכון הדיסאינפורמציה, כחלק מסיכוני סייבר, ונאותות הכלים והבקורות הקיימים אצלם להתמודדות עם סיכון זה.
- הנחיית גופים מפוקחים לקבוע נהלים לשם ביצוע פעילות מניעתית להתמודדות עם אירועי דיסאינפורמציה, כחלק מסיכוני סייבר, לרבות באמצעות ניטור מוקדם ככל הניתן, וכן קביעת דרכי ההתנהלות בעת התממשות אירועים כאמור (כחלק מהיערכות מוקדמת להתמודדות עם אירועי סייבר ו/או להתנהלות בשעת חירום).
- קביעת מנגנונים או בחינת מנגנונים קיימים להתמודדות עם סיכוני דיסאינפורמציה בגופים הרלוונטיים, כגון הוראות ונהלים העוסקים בסיכוני סייבר בקרב גופים מפוקחים, או מנגנון מנתק הזרם שהוזכר לעיל ביחס לפעילות המסחר בבורסה.
- הגברת מודעות הציבור לסיכוני דיסאינפורמציה, באמצעות פרסום הסברים, אזהרות, ופעולות נוספות של חינוך פיננסי.
- היערכות מוקדמת אצל הרגולטורים הפיננסיים עצמם להתמודדות עם אירועי דיסאינפורמציה (בדומה להיערכות מוקדמת להתנהלות בשעת חירום). לדוגמה, ניטור מוקדם של התפשטות דיסאינפורמציה (למשל, פעילות לא שגרתית ברשתות החברתיות), קביעת נהלים ותהליכי עבודה שעניינם פרסום הבהרות בתקשורת על-ידי רגולטורים, דרישת פרסום מידע על-ידי גופים מפוקחים כתגובה למידע כזב, וכדומה.
- הוספת תרחישים של התממשות סיכוני דיסאינפורמציה לנהלי התמודדות עם נהלי סייבר ו/או לנהלי היערכות לשעת חירום וכן לתרגולים המתבצעים על-ידי הרגולטורים הפיננסיים והמערכת הפיננסית ביחס להתנהלות בשעת חירום.
- שכלול יכולות החקירה של אירועי דיסאינפורמציה כתוצאה מפעילות בינה מלאכותית. בפרט יש חשיבות לכך ביחס לפעילות מסחר בניירות ערך שעשויה להיות רגישה במיוחד לאירועים אלה. בהקשר זה, יש מקום להמשיך בקידום הצעות חוק הנמצאות על המדוכה שנועדו לסייע באכיפה של עבירות לפי חוק העונשין וחוק המחשבים בתחום ניירות הערך.
- בחינת קביעת סמכויות בדין הכללי להסרת תכנים כוזבים ופנייה לגורם המוסמך בהקשרים הללו.



תיבה 4: עבירות במסחר בניירות ערך באמצעות בינה מלאכותית

האם אפשר לבצע עבירות במסחר בניירות ערך תוך שימוש במערכות בינה מלאכותית? והאם ניתן לאכוף עבירות אלה בישראל כיום?

פעילות המסחר בניירות ערך בבורסה היא מורכבת מאוד – הבורסה מאפשרת למספר לא מוגבל של שחקנים לפעול בו-זמנית באמצעות הגשת פקודות מכירה וקנייה של ניירות ערך; המסחר מתבצע בשורה ארוכה של ניירות ערך, על בסיס המידע שמתפרסם על-ידי החברות; התמחור נעשה באופן רציף ופומבי בהתאם לעסקאות בניירות הערך המתבצעות כל העת; ופעילות הסליקה, קרי העברת ניירות הערך כנגד התמורה הכספית, מתבצעת בסמוך לאחר ביצוע העסקאות.

טכנולוגיית בינה מלאכותית עלולה לשמש גורמים בביצוע עבירות במסחר. כך לדוגמה, פרסום מידע שקרי שנוצר באמצעות בינה מלאכותית על מנת שייחזה כאמין, עלול להשפיע על שערי ניירות ערך ולאפשר לגורם האחראי לפרסום להנות מתנודת השערים. הוא עשוי למשל לממש מניוניה של חברה במחיר גבוה, לאחר ששער המניה הגיב בחיוב למידע שקרי אודות התפתחות לטובה בעסקי החברה. פעילות זו עלולה לפגוע לא רק במשקיעים ספציפיים אלא גם בערך הכללי של הגינות המסחר בבורסה ואמון הציבור בו.

סעיף 54 לחוק ניירות ערך אוסר על ביצוע תרמית בניירות ערך. הסעיף כולל שני סוגי התנהגות אסורה: הנעה בתרמית לרכוש או למכור ניירות ערך; והשפעה בדרכי תרמית על שערי ניירות ערך.

עבירת ההנעה אוסרת על יצירת מצג שווא בדרך של הצגת פרטים כוזבים או העלמת עובדות מהותיות, במטרה להניע משקיעים לבצע פעולות בניירות ערך. עבירת התרמית במסחר אוסרת על פגיעה במנגנון התמחור של ניירות הערך הנסחרים בבורסה. לא אחת מתקיימים שני סוגי ההתנהגות יחד. כך לדוגמה, אדם המפרסם מידע כוזב עשוי להניע בכך משקיעים לרכוש או למכור ניירות ערך (תוך הפרת האיסור הראשון), וכן להשפיע באופן זה על שער ניירות הערך באופן תרמיתי (תוך הפרת האיסור השני).

בתי המשפט עמדו על כך שעבירת התרמית עשויה לכלול פעילויות מגוונות ומשתנות. כך למשל, קבע בית המשפט העליון ביחס לעבירת התרמית במסחר כי "החיים עשירים מכל דמיון. אין זה ראוי לקבוע מראש 'רשימה סגורה' של מצבים האסורים על פי הוראות סעיף 54(א)(2) לחוק ניירות ערך. יש להימנע מהגדרות כוללניות, שעם ניסוחן נמצא מיד המקרה הנוסף שאינו נכנס לתחומן אך שההתנהגות על פיו אסורה אף היא. בתחום חי ותוסס זה של המסחר בשוק ניירות הערך, עדיפה גישה אינדוקטיבית, הנעה ממקרה למקרה, ועל בסיס נסיון החיים המצטבר מרחיבה ומשכללת את תפיסותיה העקרוניות".³⁹⁷

ואכן, עבירות תרמית שעניינן דיסאינפורמציה כבר נדונו והוכרעו בעבר. בפרשת **פודים** הורשע נאשם, שהפיץ הודעות כוזבות בלוח הודעות באתר אינטרנט, תחת שמות בדויים שונים, בתרמית בניירות ערך; בפרשת **דהאן** הורשעו חמישה נאשמים שרכשו מניות דלות סחירות, ולאחר מכן פרסמו פרסומים כוזבים בפורומים ובתגובות באתרי השקעות, במטרה להעלות את שעריהן ולמכור אותן ברווח; ובפרשת **הולצמן** הורשע נאשם בכך שפרסם בפורומים ייעודיים למשקיעים מסמך שנחזה להיות כתבה אינטרנטית של עיתון גלובס, שכלל מידע חיובי על ניירות ערך שהיו ברשותו, במטרה להניע משקיעים לרכוש אותם.³⁹⁸

בדומה לכך, גם בארה"ב טופלו אירועי תרמית בניירות ערך, כגון פרשת **Burns** שעסקה בהעלאת דיווח כוזב לאתר דיווחי החברות של רשות ניירות הערך האמריקאית, בעקבותיו זינק השער ומומשו אופציות ברווח; או פרשת **Craig** בה פורסמו ציורים שקריים בחשבונות טוויטר מזויפים, כביכול של פירמות ניירות ערך, במטרה להשפיע על השער ולגרוף רווחים.³⁹⁹

397 ע"פ 5052/95 ואקנין נ' מדינת ישראל, פ"ד נ(2) 642, בסעיף 29 לפסק הדין.

398 ע"פ (ת"א) 70571/01 מדינת ישראל נ' פודים טל (נבו, 23.3.2002); ת"פ (ת"א) 6952/06 מדינת ישראל נ' אבי דהאן (22.22.2010); ת"פ (ת"א) 31515-05-16 מדינת ישראל נ' שרון הולצמן (11.12.2016).

399 <https://www.sec.gov/litigation/litreleases/lr-24557>; <https://www.sec.gov/litigation/litreleases/lr-24481>



עבירת התרמית תחול אם כן גם על פעולות שנעשו באמצעות בינה מלאכותית. האתגר בהקשר זה הוא בפן החקירתי. זאת בהינתן שעבירות אלה יכולות להיעשות בפלטפורמות אינטרנטיות שונות, שמופיעים בהן תכנים בהיקפים עצומים, וכן משום שהעבירות יכולות להיעשות מרחוק, כולל ממחשבים מחוץ לישראל. כפי שפורט בפרק העוסק בדיסאינפורמציה באמצעות בינה מלאכותית, קושי נוסף נוגע ל"איכות" הזיוף, קלות ההפקה שלו, וזיהוי מקורו.

בהקשר זה יש חשיבות רבה בעדכון סמכויות החקירה לגבי חומרי מחשב לשם אכיפה אפקטיבית בעתיד. בימים אלה מקודמת הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשפ"ג-2023. הצעה זו מכילה, בין היתר, סמכויות חיפוש וחדירה לחומרי מחשב שאינן קיימות כיום, אשר נועדו לאפשר לגופי החקירה להתמודד עם פשיעה מורכבת תוך מתן מענה להתפתחויות טכנולוגיות. כך למשל, הצעת החוק מסדירה את הסמכות לבצע חיפוש סמוי מרחוק בחומרי מחשב, כאשר סמכות זו חיונית על מנת להתמודד עם המהירות והתחכום של העבירות המבוצעות באמצעים טכנולוגיים מתוחכמים לרבות בינה מלאכותית. לאור האמור לעיל, יש חשיבות במתן סמכויות אלה על מנת לאפשר אכיפה אפקטיבית בתחום עבירות ניירות הערך.

חלק ד'

תחומים ספציפיים שנבחנו על-ידי הצוות



פרק זה עוסק בשלושה תחומי פעילות ספציפיים שהוגדרו לבחינת הצוות: ייעוץ השקעות וניהול תיקים, אשראי וחיתום ביטוח. לגבי תחומים אלה מציג כל אחד מהרגולטורים הפיננסיים את האופן בו הוא רואה שימושים אפשריים ליישומי בינה מלאכותית בתחום שתחת פיקוחו, מהי המסגרת הרגולטורית הרלוונטית, סוגיות לטיפול, והמלצות ראשוניות.

ייעוץ השקעות וניהול תיקים

שימושים אפשריים של בינה מלאכותית בפעילות ייעוץ השקעות וניהול תיקים

לבינה מלאכותית עשויים להיות שימושים רבים ומגוונים בפעילויות של ייעוץ השקעות וניהול תיקים. שימושים אלה יכולים להשתרע למעשה על כלל הפעולות המקצועיות הנוגעות למתן הייעוץ או לניהול כספי הלקוח. כך למשל, בינה מלאכותית יכולה לשמש בתהליך בירור צרכי הלקוח, בין היתר בדרך של שאלונים מקוונים וניתוח התשובות הניתנות במסגרתם; היא יכולה לשמש בבנייה ובהצגה של מסלולי השקעה או המלצות השקעה המותאמות ללקוח; והיא יכולה לשמש אף בניהול כספי הלקוח עצמם שעה שמדובר בפעילות של ניהול תיקי השקעות. בהקשר זה עשויה בינה מלאכותית ליטול חלק בפעולות הליבה של בחירת ההשקעות ואף ביצוען.

מעבר לפעילויות אלה, עשויים להיות לבינה מלאכותית שימושים בהיבטים עסקיים נוספים של בעלי הרישיון כגון פעילות שיווק וקשר עם לקוחות (למשל איתור לקוחות פוטנציאליים והצעת שירותים רלוונטיים), או מנגנוני ציות לדין (למשל עמידה בדרישות מתחום איסור הלבנת הון או ניהול סיכונים).

בדומה לפעילויות פיננסיות אחרות, עוצמת השימוש בבינה מלאכותית עשויה להשתנות ממקרה למקרה, ובהתאמה גם מידת המעורבות האנושית. כך למשל, שימוש באלגוריתמים בבחירת השקעות יכול להיעשות כמנגנון תומך החלטה של מנהל תיקים, או ככלי מרכזי לקבלת החלטות ההשקעה.

פרק זה עוסק הן בשימושים ותיקים ופשוטים יותר של מערכות בינה מלאכותית וקבלת החלטות אוטומטית, כגון אלגוריתמים המשמשים בשירות לקוחות אשר תוצריהם נקבעו מראש, הן בשימושים חדשים ומתוחכמים, כגון אלגוריתמים המשמשים בבירור צרכי לקוחות המבוססים על למידת מכונה ומודלים של שפה (LLM). האתגר הרגולטורי, כפי שניתן יהיה להתרשם מהמשך הפרק, נובע מהטיפול בשימושים השונים לסוגיהם – פשוטים ומורכבים – ומהמעבר שמתרחש בימים אלה בין מערכות טכנולוגיות מדורות שונים. הדור החדש של מערכות טכנולוגיות צפוי להרחיב מאוד את השימושים האפשריים, לפתור מחד בעיות שעלו בקשר עם מערכות קבלת החלטות אוטומטיות פשוטות, ומאידך לעורר בעיות חדשות שיש לתת להן מענה רגולטורי.

להלן פירוט שימושים אפשריים של בינה מלאכותית בפעילויות של ייעוץ השקעות וניהול תיקי השקעות בהתבסס על סקירות ודוגמאות מחו"ל:⁴⁰⁰

400 ראו דוח אונ'תל-אביב, בעמ' 17–19; הצעת ה-SEC משנת 2023, בעמ' 21–15; דוח ה-OECD משנת 2023, בעמ' 13–18; דוח IOSCO משנת 2021, בעמ' 6–8; Blake Schmidt and Amanda Albright, AI Is Coming to Wealth Management. Here's What That Means, Bloomberg Markets (April 21, 2023), <https://www.wealthmanagement.com/technology/ai-coming-wealth-management-here-s-what-means>.

שימושים אפשריים בטכנולוגיות בינה מלאכותית בפעילות של ייעוץ השקעות וניהול תיקי השקעות יכולים להיות לכל אורך שרשרת הפעילות. כך למשל:	
פרסום ושיווק הפעילות	איתור לקוחות פוטנציאליים, יצירת עניין בקרב לקוחות, פרסונליזציה של השיווק, והגעה לקהל לקוחות גדול יותר.
תהליך הצטרפות לקוח לשירות (onboarding)	הכנסת לקוחות חדשים למערכות נותני השירותים, הכרת השירותים האפשריים השונים ללקוחות, תוך וידוא עמידה בהוראות הדין לרבות הוראות KYC (Know Your Customer), וחתימה על ההסכם למתן השירותים.
זיהוי לקוח מרחוק	סיוע במעבר מזיהוי "פנים אל פנים" לזיהוי מרחוק באמצעות מערכות זיהוי פנים וסממני זיהוי נוספים.
תהליך בירור צרכי לקוח	ביצוע התהליך העומד בבסיס פעילות ייעוץ השקעות וניהול תיקי השקעות – בירור עם הלקוח של מטרות ההשקעה, מצבו הכספי, העדפותיו, ושאר הנסיבות הצריכות לעניין, לשם התאמת הפעילות לצרכיו ולהנחיותיו. בינה מלאכותית מאפשרת בין היתר איסוף, הכללה ועיבוד של מידע רב נוסף אודות הלקוח, כמו היסטוריית רכישות והתנהלות כספית שלו. לכן בירור הצרכים יכול להתבצע גם באמצעות איסוף נתונים ולא רק באמצעות מענה אקטיבי של הלקוח לשאלות.
ניתוח ובחירת השקעות	סריקה וניתוח של אפשרויות השקעה רבות ובחירה מתוכן, וכן של אופן הביצוע המיטבי של פעולות נלוות (המרת מטבע, בחירת ברוקר).
המלצות השקעה	המלצה על תיק השקעה המותאם לצרכי הלקוח, על בסיס שקלול הנתונים שעלו בתהליך בירור הצרכים (היקף השקעה, מטרות ההשקעה, פרופיל סיכון, וכדומה) והיצע ההשקעות האפשריות.
החלטות השקעה	בפעילות ניהול תיקים מתקבלות החלטות ההשקעה עצמן על-ידי מנהל התיקים, בהתאם למדיניות השקעה שנקבע מראש. מערכות בינה מלאכותית יכולות לשמש ככלי תומך החלטה או מקבל החלטה, וכן לבצע את הפעולות. בפרט יכולות מערכות אלה לבצע איזון מחדש של תיק הלקוח באופן אוטומטי, לתת ללקוח התראות בדבר תיק ההשקעות, להגיב למצבי שוק חדשים, ועוד.
תיעוד, הנמקה, עדכונים ודיווחים ללקוחות	הדין החל על שירותי ייעוץ השקעות וניהול תיקים מחייב תיעוד של פעולות ייעוץ והשקעה, דין ודברים בין הלקוח ונותן השירות, הנמקות לפעולות המתבצעות על-ידי נותן השירות, הסכמה מצד הלקוח לפעולות מסוימות (כגון ביצוע עסקה הכרוכה בסיכון מיוחד), ודיווחים ללקוחות. מעבר לעמידה בדרישות הדין, מערכות בינה מלאכותית יכולות לשמש לביצוע פניות נוספות ללקוח, עדכון על מצבו מעבר לדרישות הדין, מתן סקירות על השקעותיו, וכדומה.
תמיכה טכנית ושירות לקוחות	אוטומציה ומתן מענה מהיר לפניות לקוחות, בפרט כאשר מדובר בפניות שגרתיות; סיוע בהתאמת התמיכה ללקוח, באמצעות בדיקת פרטי הלקוח, פניות קודמות שלו, מצב החשבון שלו; סיוע למענה אנושי באמצעות הצגת המשאבים והמידע הנחוץ באופן מהיר לשם פתרון בעיות של לקוחות; סיוע בהפניית הלקוח לגורם הרלוונטי תוך חיסכון בזמן לנותן השירות וללקוח; ועוד.
מנגנוני ציות וניהול סיכונים	בין היתר מערכות העוסקות באיתור הונאות, זיהוי פעילויות חריגות בפעילות, עמידה בדרישות הדין, בקרות הלבנת הון, וכיוצא באלה.

המסגרת החוקית הכללית

חוק הסדרת העיסוק ביעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, התשנ"ה-1995 (להלן: **"חוק הסדרת העיסוק"**) קובע משטר של אסדרה ופיקוח לשלושת סוגי השירותים האמורים. בבסיסו של משטר זה ניצבת חובת רישיון המוטלת על המבקש לעסוק בפעילות, ובהמשך לכך קבועה שורה של חובות נוספות החלות על בעל הרישיון לשם הגנת הלקוחות, כגון חובות אמון וזהירות, חובה לערוך הסכם בכתב, וחובה להתאים את השירות לצורכי הלקוח לאחר בירור צרכיו.⁴⁰¹

חוק הסדרת העיסוק, קבצי התקנות והוראות הרשות שנקבעו מכוחו, יוצרים מעטפת אסדרה משמעותית. תכליות מרכזיות של אסדרה זו הן הבטחת רמת השירות שיקבל ציבור המשקיעים, הן מבחינת איכות השירות הן מבחינת מהימנותו; הסדרת דרכי הפעולה של בעלי הרישיון ומערכת היחסים שבין בעלי הרישיון והלקוחות במטרה לצמצם, בין היתר, סיכונים פוטנציאליים ללקוחות, כגון כאלה הנובעים מניגודי עניינים אפשריים; פתיחת אפשרויות להשאת תשואה על כספי המשקיעים והתאמת מתכונת ואופי ההשקעה של כל משקיע לצרכיו; והרחבת השתתפות ציבור המשקיעים בשוק ההון כחלק מהאינטרס הכלכלי של המדינה בפעילות בשוק ההון.⁴⁰²

ההבחנה היסודית בין פעילויות של ייעוץ השקעות וניהול תיקי השקעות נעוצה בכך שבפעילות של ייעוץ השקעות ניתנת על-ידי היועץ המלצת השקעה ללקוח, אשר יכול להחליט אם הוא מעוניין לפעול על פיה, בעוד שבפעילות של ניהול תיקי השקעות יש למנהל התיקים שיקול דעת בדבר ביצוע פעולות השקעה בניירות ערך ובנכסים פיננסיים המוחזקים בחשבון על שם הלקוח, באמצעות יפוי כוח לפעול בחשבון, בהתאם למדיניות ההשקעה שהוסכמה מראש עם הלקוח. לאור האמור, לגבי פעילות של ניהול תיקי השקעות מטיל הדין חובות נוספות הנוגעות בין היתר לאופן ההחזקה והניהול הנפרד של נכסי הלקוח, ואיסור שימוש בנכסי הלקוח אלא לצורך ביצוע עסקאות עבורו ובהתאם להסכם עמו.⁴⁰³

בהתאם להבחנה זו, פעילות של ייעוץ השקעות מוגדרת בחוק כ"מתן ייעוץ לאחרים בנוגע לכדאיות של השקעה, החזקה, קניה או מכירה של ניירות ערך או של נכסים פיננסיים". פעילות של ניהול תיקי השקעות מוגדרת בחוק כ"ביצוע עסקאות, לפי שיקול דעת, לחשבונם של אחרים".⁴⁰⁴

העיסוק הרגולטורי עד כה

הרגולציה הענפה החלה על ייעוץ השקעות וניהול תיקים התפתחה במשך עשרות שנים, אך לא הייתה בה התייחסות קונקרטית לפעילות של בינה מלאכותית. הוראות הדין, שנכתבו בבסיסן בשנות התשעים, ראו לנגד עיניהן פעילות אנושית הכוללת מפגש בנוכחות פיזית בין בעל רישיון ולקוח, בירור ועדכון צרכים הנעשים במסגרת שיחה פנים אל פנים או טלפונית, ומתן המלצות השקעה וניהול תיקים באופן מסורתי. בשנים האחרונות קידמה רשות ניירות ערך התאמות בדין כדי לאפשר מתן שירותים של ייעוץ השקעות וניהול תיקי השקעות באמצעים טכנולוגיים מתקדמים וכדי להתמודד עם התמורות המשמעותיות החלות באופן צריכת השירותים הפיננסיים על-ידי הציבור לנוכח ההתפתחות הטכנולוגית.⁴⁰⁵ בין היתר קבעה רשות ניירות ערך את ההוראה לבעלי רישיון למתן שירותים תוך שימוש באמצעים טכנולוגיים, העוסקת גם בפעילות של בינה מלאכותית, אשר נרחב בעניינה בהמשך.

(1) פעילות של ניהול תיקים ממוחשב ללא פיקוח

העיסוק המשמעותי לראשונה של רשות ניירות ערך בבינה מלאכותית בהקשר של פעילויות ייעוץ השקעות וניהול תיקי השקעות התרחש על רקע תופעה בעייתית: לנוכח סביבת הריבית הנמוכה והנגישות הרבה ללקוחות באמצעות פנייה באינטרנט ובדרכים נוספות, החלה להתגבר בשנת 2014 ואילך התופעה של הצעת השקעות לא מפוקחות לציבור. על הצעות אלה, שהתרחשו באפיקים שונים של פעילויות פיננסיות, נמנתה גם קטגוריה של ניהול תיקים ממוחשב אשר כונה לרוב "מסחר רובוטי" או "אלגוריתמי". במסגרת זו פנו גופים לא מפוקחים לציבור והציעו לו להשקיע את כספו באמצעות אלגוריתמים. במצגים שניתנו על-ידי אותם גופים למשקיעים הם התיימרו לבצע את

401 סעיפים 11–21 לחוק הסדרת העיסוק.

402 ראו למשל הצעת חוק הסדרת העיסוק ביעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, תשנ"ה-1995, ה"ח 2320, עמ' 92; בג"ץ 1715/97 לשכת מנהלי ההשקעות נ' שר האוצר, פ"ד נא(4) 367 (1997), בעמ' 391; ת"צ 15–12–47119 אפרימוב נ' יו אס ג'י קפיטל בע"מ ואח' (24 ביוני 2019), בסעיפים 26–27 (להלן: "עניין אפרימוב").

403 סעיפים 22–24 לחוק הסדרת העיסוק.

404 סעיף 1 לחוק הסדרת העיסוק. פעילות של "שיווק השקעות", שלא נעסוק בה בדוח זה, מוגדרת אף היא בסעיף 1 לחוק כ"מתן ייעוץ לאחרים בנוגע לכדאיות של השקעה, החזקה, קניה או מכירה של ניירות ערך או של נכסים פיננסיים, כשלנותן הייעוץ יש זיקה לנכס פיננסי".

405 ראו למשל הצעת חוק לעידוד פעילות בשוק ההון (תיקוני חקיקה), התשפ"ד-2024 (26 ביוני 2024), בעניין ייעוץ השקעות כללי.

ההשקעה באופן שהנו מתוחכם, בטוח, ונושא תשואות יוצאות דופן.

פעילותה של רשות ניירות ערך בנוגע להשקעות לא מפקחות כללה בין היתר פרסום של אזהרות לציבור וחינוך פיננסי, זיהוי פעילויות לא מפקחות שהיוו הפרה של החוק, פניה לגורמים בדרישה לחדול מפעילות מפרה, פעולות אכיפה, וחקיקה להסדרת תחומים לא מפקחים. בהקשר של פעילות "מסחר רובוטי"/"אלגוריתמי", פעלה הרשות בשנים 2015 ו-2016 נגד שורה של מיזמים שביצעו פעילות זו ללא פיקוח.⁴⁰⁶

אחת הטענות שעלתה מצד המיזמים, ונדחתה על-ידי רשות ניירות ערך, הייתה כי הם אינם כפופים לדין, שכן שיקול הדעת וביצוע העסקאות הנם של מחשב. רשות ניירות ערך גרסה לעומת זאת כי העובדה שהחלטות ההשקעה מתקבלות על-ידי תוכנת מחשב אינה גורעת מכך שהעסקאות מבוצעות לפי שיקול דעת נותן השירות באמצעות תוכנת המחשב וללא הפעלת שיקול דעת על-ידי הלקוח, ולפיכך הפעילות טעונה רישיון וכפופה ליתר הדרישות הקבועות בחוק הסדרת העיסוק בנוגע לניהול תיקים. טענה אחרת שהעלו מיזמים באותה העת הייתה כי אין מדובר בפעילות של ניהול תיקים אלא בפעילות של זירת סוחר, אשר האסדרה בעניינה טרם נכנסה לתוקף בזמנו. בהקשר זה פרסמה הרשות עמדה משפטית המבהירה מתי ובאילו תנאים ייחשב שימוש בתוכנת מסחר אלגוריתמי בזירת סוחר כשירות של מתן פלטפורמה למסחר עצמאי של לקוחות הזירה, ולא כפעילות של ניהול תיקים או ייעוץ השקעות.⁴⁰⁷ עמדתה של רשות ניירות ערך בדבר תחולתו של חוק הסדרת העיסוק גם על פעילות של ניהול תיקים ממוחשב התקבלה בבתי המשפט בהליכים פליליים ואזרחיים שנוהלו נגד מיזמים לא מפקחים. כך למשל קבע בית המשפט בעניין יו אס ג'י קפיטל ביחס לסוגיית הפעלת שיקול הדעת בידי מחשב:⁴⁰⁸

"ואכן שאלת הפעלת "שיקול-דעת" בביצוע החלטות השקעה היא מורכבת יותר כאשר מדובר בעסקאות המבוצעות מחשב. ביצוע עסקאות באמצעות אלגוריתם הוא חידוש טכנולוגי של השנים האחרונות. ניהול התיקים ה"קלאסי" נעשה על-ידי הפקדת כספי הלקוח בידי אחר המפעיל שיקול-דעת ומקבל באופן עצמאי את החלטות היכן ובאיזה אופן להשקיע את הכספים. חוק הייעוץ שנחקק בשנת 1995, ראה לנגד עיניו את המסחר המסורתי שהתקיים באופן בלתי-אמצעי על-ידי סוחרים אנושיים. במועד בו חוקק החוק, לא ניתן היה לצפות את כלל ההתפתחויות הטכנולוגיות שחלו בשנים האחרונות, המאפשרות פתרונות טכנולוגיים גם בתחום השירות הפיננסי.

...

אני סבורה כי שיקול-הדעת ביחס לבחירה בין עסקאות שונות חייב בהכרח להיות אצל גורם אנושי כלשהו – הלקוח שלו שייך הכסף או החברה באמצעותה הוא משקיע אותו ושסיפקה לו את התוכנה המקבלת את החלטות ההשקעה. לכן, אם שיקול-הדעת אינו של הלקוח, הרי שהוא בהכרח בידי החברה ולהפך. כל קביעה אחרת תיצור "ואקום", ותוביל למצב בו לכאורה שיקול-הדעת אינו של אף גורם אנושי – ואין משום כך כל גורם שנושא בכך באחריות.

אינני מקבלת גם את הטענה לפיה השימוש בביטוי "שיקול-דעת" מחייב התערבות אנושית לפני כל החלטה קונקרטית. ראשית, גם כאשר מדובר בתוכנת מחשב, תוכנה זו תוכנה על-ידי גורם אנושי כלשהו, שהוא ש"הנחה" אותה בדרך קבלת החלטות על-ידיה. האלגוריתם הממוחשב "מקבל" את החלטת ההשקעה על-סמך בחינה וניתוח של נתונים המוזנים אליו. אולם גם אם החלטת ההשקעה הקונקרטית נעשית באופן אוטומטי ולכאורה "ללא מגע יד-אדם", הרי בפועל החלטה מתקבלת בהתאם לתהליך קבלת החלטות שעוצב מראש ובהסתמך על פרמטרים שנקבעו מראש. יתרה מזאת – כפי שהובהר לעיל, הבחירה באלגוריתם שיקבל את החלטות, אף היא החלטה אנושית, שלצורך קבלתה

406 ראו רשות ניירות ערך "אזהרה לציבור בדבר ניהול השקעות ממוחשב ("מסחר רובוטי", "אלגו טריידינג" וכו') (2.8.2015). המקרה הידוע ביותר מתוך מיזמים אלה היה של חברת יוטריויד אשר גייסה כספים ממאות משקיעים לאחר שהציעה להם שירותי מסחר ממוחשב המתבסס על תוכנה הכוללת אלגוריתם לבחירת השקעות, אשר התמקדו במסחר בחוזי הפרשים על מגוון נכסי בסיס. רשות ניירות ערך עצרה את פעילות החברה, אשר נעשתה ללא פיקוח, ופתחה חקירה פלילית בעניינה. ההליך הסתיים בהרשעתו של הבעלים ומנכ"ל החברה בין היתר בגין מצגי כזב כלפי הלקוח, גניבת כספים, ניהול תיקי השקעות ללא רישיון, ושיבוש מהלכי משפט. ראו גם ת"פ 60588-12-18 מדינת ישראל נ' טלמור ואח' (13.9.2022) (להלן: "עניין טלמור").

407 רשות ניירות ערך "עמדת סגל משפטית: הצעת שירותי מסחר באמצעות אלגוריתם בזירת סוחר" (14.9.2016). הרגולציה החלה על זירת סוחר מגבילה אותן מביצוע פעילות של ייעוץ השקעות וניהול תיקי השקעות, ועל כן עלה הצורך להבהיר איזה שימוש הן יכולות לעשות בתוכנות מסחר אלגוריתמי מבלי להפר מגבלות אלה. ראו תקנה 10(א) ו-10(ג) לתקנות ניירות ערך (זירות סוחר לחשבון העצמי), התשע"ה-2014, והתנאים שנקבעו בעמדה האמורה.

408 עניין אפרימוב, בסעיפים 30 ו-33 לפסק הדין. וראו גם עניין טלמור בסעיפים 320-323, 328-332 לפסק הדין.

נדרשת הפעלה של "שיקול-דעת". לכן, השאלה איננה האם הופעל שיקול-דעת או לא, אלא האם יש לייחס את שיקול-הדעת ללקוח או לחברה."

תופעת המיזמים הלא מפוקחים המציעים פעילות של ניהול תיקים ממוחשב דעה בשנת 2016, וכמה לקחים עולים ממנה לגבי בינה מלאכותית:

לקח אחד הוא חשיבות ההקפדה על עיקרון של "ניטרליות טכנולוגית", שמשמעו בין היתר כי אין מקום לאפשר מעקף של הוראות הדין רק משום שפעילות מסוימת הטעונה פיקוח נעשית בטכנולוגיה שונה. אמנם לעתים קרובות יהיה מקום לבצע התאמות בהוראות הדין לשם קידום חדשנות טכנולוגית והתמודדות עימה, אך התפישה הכללית היא שהאינטרסים הנוגעים לשמירת עניינו של הציבור צריכים להישמר ללא קשר לטכנולוגיה באמצעותה נעשית הפעילות נושא הרגולציה. לעקרון זה חשיבות נוספת, שכן עיצוב הרגולציה בהתאם לטכנולוגיה הקיימת ברגע נתון עלולה לעודד יצירת מעקפים טכנולוגיים ובכך גם להקנות לחברות מסוימות, שמבצעות אותה פעילות, יתרון רק בשל הבדלים טכנולוגיים שאינם משפיעים על הפעילות.

לקח נוסף נוגע לפוטנציאל השימוש לרעה בטכנולוגיה חדשה לצרכים של שיווק ו"מיתוג", כאשר בפועל אין מאחורי פרסומים אלה ממש. לקח זה רלוונטי לא רק לפעילות שאינה מפוקחת אלא גם לפעילות מפוקחת, ועולה ממנו הצורך להבהיר ללקוח באופן מהימן מהי הטכנולוגיה בה נעשה שימוש, על יתרונותיה וחסרונותיה.⁴⁰⁹

(2) הוראת שירותים מקוונים

לצד הטיפול בתופעת ההשקעות הלא מפוקחות, התגברה ברשות ניירות ערך ההכרה כי יש לערוך התאמות והבהרות בהוראות הדין על מנת לקדם את השימוש באמצעים טכנולוגיים במתן שירותי ייעוץ השקעות וניהול תיקי השקעות. רשות ניירות ערך סברה כי לשימוש באמצעים טכנולוגיים עשויים להיות יתרונות רבים כגון שכלול, שיפור והוזלה של השירותים, וכן הנגשתם לציבור רחב יותר של לקוחות, לרבות כאלה שביכולתם להשקיע סכומי כסף קטנים יחסית ועל כן בעלי רישיון מעדיפים שלא להעניק להם שירותים משיקולי כדאיות כלכלית. התאמות והבהרות אלה מצאו ביטוי ב"הוראה לבעלי רישיון בקשר למתן שירותים תוך שימוש באמצעים טכנולוגיים" שפרסמה רשות ניירות ערך בשנת 2016 (להלן: "הוראת שירותים מקוונים", ובפרק זה גם "ההוראה").⁴¹⁰

ההוראה אמנם אינה מתייחסת מפורשות לבינה מלאכותית, אך הלשון הכללית הננקטת בה מאפשרת את החלתה גם במקרים מסוימים של שימוש בטכנולוגיה זו. ההוראה עוסקת למעשה בשני נושאים קשורים: הנושא האחד הוא תהליכים שמקיימים בעלי רישיון ללא מעורבות אנושית. לשם המחשה, בירור צרכים של לקוחות יכול להיעשות באמצעות שאלון מקוון, להבדיל מבירור הצרכים המסורתי שנעשה עם הלקוח בדרך של שיחה. בהקשר זה עולות שאלות הקשורות במעבר לפעילות דיגיטלית. לדוגמה, האם הלקוח מבין עד תום את משמעויות הדברים שהוא נשאל לגביהם בשאלון המקוון. או לדוגמה, האם לקוח עלול לבצע עסקה באופן פזיז על בסיס המלצה הניתנת לו מבלי לשקול היטב את משמעותה. הנושא השני בו עוסקת ההוראה הוא שימוש של בעלי רישיון ביישומים אלגוריתמים בהיבטים שונים בפעילות. בהקשר זה עולות שאלות הקשורות באופן ישיר בבינה מלאכותית. לדוגמה, מהי מידת האחראיות של בעל רישיון העושה שימוש באלגוריתם לשם קבלת החלטות השקעה עבור הלקוח, או לדוגמה, האם נדרשת מבעל הרישיון מעורבות אנושית במצבים מסוימים. לאור האמור אפשר לראות בהוראה ניסיון חלוצי ברגולציה הפיננסית בישראל, עוד בשנת 2016, להתמודד עם מקצת הסוגיות בהן עוסק דוח זה.

ההוראה עוסקת בשלושת השלבים העיקריים בתהליך מתן שירותים של ייעוץ השקעות וניהול תיקי השקעות.⁴¹¹ נקודת המוצא בהוראה היא כי יש להתיר ביצועם של שלבים אלה באמצעים טכנולוגיים מתקדמים תוך התמודדות עם הסוגיות שביצוע כאמור מעורר. שלושת השלבים המתוארים בהוראה הם אלה:

1. **בירור הצרכים וההתקשרות בהסכם** – ביצוע התהליך באופן מקוון, ללא מפגש פנים אל פנים וללא אינטראקציה מלאה בין גורם אנושי שהוא בעל רישיון ובין הלקוח.

409 ראו לעניין זה תת-הפרק העוסק בהתמודדות עם גילוי שיווקי מטעה בנושא בינה מלאכותית בפרק ידוע וגילוי לעיל.

410 רשות ניירות ערך, הוראה לבעלי רישיון למתן שירותים תוך שימוש באמצעים טכנולוגיים (23.8.2016). לנוסח מעודכן של ההוראה ראו https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic/al_lobby/al_lobby-6283705a39f5d/horaa7822.pdf.

411 בנוסף לכך עוסקת הוראת שירותים מקוונים בשני שירותים אשר בשל אופיים הם ניתנים באופן מקוון: שירות ייעוץ למסחר עצמאי (אשר נקרא בעבר שירות איתותים) במסגרתו משוגרות המלצות השקעה באופן שוטף ללקוחות, ושירותי מסחר חברתי בהם יכול לקוח לצפות בעסקאות המבוצעות על-ידי אדם אחר בפלטפורמת מסחר חברתי או לעקוב באופן אוטומטי בניהול כספיו אחר תיק ההשקעות של אותו אדם. בשני סוגי השירותים האמורים יכול להיעשות שימוש בבינה מלאכותית אך ההוראה אינה עוסקת דווקא באפשרות זו אלא מסדירה היבטים אחרים הנוגעים לשירותים אלה.

2. **קביעת מדיניות ההשקעה ורמת הסיכון של הלקוח** – עיבוד הנתונים שהתקבלו מהלקוח, לשם קביעת רמת סיכון ומדיניות השקעה, באמצעות יישום אלגוריתמי.

3. **מתן השירות השוטף** – הפקת המלצות השקעה ומסירתן ללקוח (שעה שמדובר ביעוץ השקעות), וקבלת החלטות השקעה (שעה שמדובר בניהול תיקי השקעות), תוך שימוש ביישום אלגוריתמי, וכן קיום הקשר השוטף עם הלקוח באופן מקוון לרבות עדכון צרכי לקוח מעת לעת.

ההוראה בנויה באופן מודולרי, כך שבעל רישיון יכול לעשות שימוש באמצעים טכנולוגיים בשלב אחד או יותר מהשלבים האמורים בשירות הניתן על-ידו. כך למשל, עשוי להיות בעל רישיון שיבחר לבצע את שלב ההתקשרות ובירור הצרכים באופן מסורתי במפגש פנים אל פנים עם הלקוח, בעוד שאת שני השלבים הבאים יבחר לבצע באמצעים טכנולוגיים. כמו-כן, אופי השימוש בבינה מלאכותית עשוי להשתנות ממקרה למקרה, ויכולים אלה להיות שימושים בסיסיים או מתוחכמים. "מתן שירותים תוך שימוש באמצעי טכנולוגי" הוגדר באופן כללי כ"מתן שירותים באופן מקוון, או שימוש באלגוריתם לצורך קבלת החלטות, ללא אינטראקציה עם גורם אנושי" בכל אחד מהשלבים האמורים.⁴¹²

ההוראה נוקטת גישה מבוססת עקרונות (Principle Based) המציגה שורה של חובות, אך מותירה שיקול דעת לבעל הרישיון באשר לאופן יישומן. בד בבד מדובר בדרישות שהן בגדר חובה לשם שימוש באמצעים טכנולוגיים על-ידי בעלי הרישיון, ולא בהמלצות בלבד.

להלן הסוגיות העיקריות שההוראה מטפלת בהן והדרישות שהיא מציבה בנוגע להן:

מיומנות – ההוראה קובעת כי מכוח חובות האמון והזהירות החלות על בעל רישיון הוא רשאי לעשות שימוש באמצעי טכנולוגי רק לאחר שרכש מיומנות והבנה ביחס אליו, ומצא כי ניתן לפעול בעזרתו באופן שלא יפגע בלקוחותיו או בחובותיו על פי החוק.⁴¹³ בדברי ההסבר להוראה מצוין, כי דרישת המיומנות רלוונטית כבר בעת קבלת ההחלטה של בעל רישיון לעשות שימוש באמצעי טכנולוגי, לרכוש או לפתח אותו, וכי היא הופכת משמעותית במיוחד בשלבים השני והשלישי של מתן ההחלטות, בהם נעשה השימוש האמצעי הטכנולוגי גם לצורך קבלת החלטות.

בעלי רישיון ייעוץ השקעות או ניהול תיקי השקעות עשויים להיות תאגידים או יחידים. כאשר מדובר בתאגיד, חלה חובה כי ימנה יחיד בעל רישיון להיות ממונה על מתן השירותים כאמור (להלן: "**בעל רישיון ממונה**"). מעבר להיבטי הבקרה והאחריות הגלומים בדרישה זו, נקבע באופן ספציפי כי לגבי קביעת מדיניות השקעה ורמת סיכון ומתן שירותים ללקוח (השלבים השני והשלישי), יכיר ויבין בעל הרישיון הממונה את המתודולוגיה שבבסיס האלגוריתם באופן שיאפשר לו לקבל החלטה מושכלת בדבר השימוש בו וההסברים שיש לתת בדבר אופן פעולתו ללקוח, וכן לבחון אם הוא פועל כמצופה.⁴¹⁴

בקורות – החובה לקיים בקורות אשר יבטיחו את נאותות השימוש באמצעי הטכנולוגי, לרבות איתור כשלים אפשריים בו ומניעתם, מוצגת אף היא כחלק מחובות האמון והזהירות של בעל הרישיון. מעבר לחובה כללית זו, מזכירה ההוראה באופן ספציפי את הצורך בנקיטת כל האמצעים הנדרשים בהיבטים של אבטחת מידע, הגנת הפרטיות, הבטחת זיהוי הלקוח, וזיהוי כשלים בתהליך בירור הצרכים.⁴¹⁵ לצד בעל הרישיון הממונה שהוזכר לעיל, נדרש גם דירקטוריון התאגיד לאשר את האמצעי הטכנולוגי ואת השימוש בו.⁴¹⁶

אחריות – ההוראה מדגישה כי שימוש באמצעי טכנולוגי אינו גורע מאחריות בעל הרישיון. האחריות באה לידי ביטוי בדרישת המיומנות שתוארה לעיל, אך גם בהוראות מפורשות לפיהן בעל האחריות יישא באחריות כלפי לקוח לנזק שנגרם לו עקב השימוש באמצעי טכנולוגי.⁴¹⁷ הוראה זו שוללת אפשרות מבעל הרישיון לטעון כלפי לקוח כי צד שלישי אחראי לנזקים שנגרמו לו, וכך מבטיחה "כתובת" ברורה ללקוח.⁴¹⁸ בנוסף לכך נדרש בעל הרישיון לוודא כי הכיסוי הביטוחי שלו יכלול אחריות של המבטח לשימוש בעל הרישיון באמצעי הטכנולוגי.⁴¹⁹

412 סעיף 1 להוראת שירותים מקוונים.

413 סעיף 2.1 להוראה.

414 סעיפים 15 – 16, 19 להוראה. בדברי ההסבר להוראה מצוין כי כל בעלי הרישיון המעורבים במתן השירות נדרשים להכיר ולהבין את המתודולוגיה ברמה המותאמת לשלב במתן השירות בו הם מעורבים, אם כי זו אינה נדרשת להיות רמת ההבנה המוגברת של בעל הרישיון הממונה.

415 סעיפים 2.3, 14 להוראה.

416 סעיף 6 להוראה.

417 סעיף 4 להוראה.

418 בעל הרישיון יכול לקבוע באופן חוזי הסדרי אחריות מול צד שלישי המספק לו מערכת טכנולוגית, וכך להשיג שיפוי במקרה של נזק, אך אין בהסדרים כאמור כדי להשפיע על מידת אחריותו הישירה כלפי הלקוח.

419 סעיף 5 להוראה.

הסבר ללקוח – דגש מיוחד בהוראה הנו במישור ההסברים ללקוח, וזאת על רקע המעבר מצריכת שירותים באופן מסורתי לצריכת שירותים באמצעים טכנולוגיים. החובה לתת הסבר ללקוח, באופן בהיר, נועדה גם למנוע מצגי שווא למטרות שיווקיות, בדבר יכולות טכנולוגיות. ההוראה כוללת דרישות לתת הסברים ללקוח לפני תחילת השירות, לרבות הכללת התייחסות לעניין בהסכם עם הלקוח, ובכל אחד משלבי מתן השירותים. גם בהקשר זה מדובר בחובה כללית, וההוראה מבארת כי ההסברים צריכים לעסוק במהות השירות ובמאפייניו הייחודיים, בסיכונים האפשריים הנובעים ממנו, במתודולוגיה של האמצעי הטכנולוגי המשמש לקביעת מדיניות השקעה או לקבלת החלטות ההשקעה.⁴²⁰ הובהר כי דרישה זו אינה כוללת חשיפת סודות מסחריים, ומטרתה היא להעניק הסבר עקרוני, המתמקד לדוגמה בכך שהאלגוריתם מעבד את המידע לנוכח תשובות הלקוח ועל כן יש חשיבות במענה יסודי לשאלות, או לדוגמה בסוגי הנכסים עליהם עשוי האלגוריתם להמליץ.⁴²¹

מעורבות אנושית – ההוראה כוללת התייחסות למצבים בהם תידרש מעורבות של גורם אנושי. כך למשל נדרשת מעורבות אנושית בכל מצב בו לקוח מבקש מענה של גורם אנושי, או במצב בו לקוח מבקש לסטות ממדיניות השקעה שונה מזו שנקבעה לו על-ידי האמצעי הטכנולוגי.⁴²² על בעל הרישיון לספק ללקוח, באופן ובהיקף זמן סבירים, בשעות שיקבעו מראש, תמיכה של גורם אנושי, הן בפן הטכני הן בפן המקצועי.⁴²³

השלכות רוחב של השימוש באלגוריתם – ככלל, ההוראה אינה עוסקת בהשלכות רוחב שעשויות להיות כתוצאה ממעבר הציבור לצורך שירותים מקוונים הניתנים תוך שימוש באמצעים טכנולוגיים, לרבות אלגוריתמים. לכך יש חריג אחד בהוראה, המביא בחשבון סיכון לפיו ניהול תיקים ייערך באופן זהה למספר רב של לקוחות תוך שימוש ביישום אלגוריתמי. הדבר יכול להוביל לכך שפעילות ניהול התיקים תהפוך דומה במהותה לפעילות של ניהול קרן נאמנות, שהיא השקעה משותפת של ציבור המשקיעים המנוהלת בידי מנהל הקרן. בפעילות של קרן נאמנות מופקדים הכספים בחשבון נאמנות של הקרן והם מושקעים באותו האופן (pool אחד) בהתאם למדיניות ההשקעה של אותה הקרן.

החשש שעלה בהקשר זה הוא כי פעילות כאמור תוביל לעקיפת מגבלות שנקבעו ברפורמת בכר, במסגרתה חויבו הבנקים למכור את קרנות הנאמנות שהיו בבעלותם, בעוד שהותר להם להמשיך ולהחזיק בפעילות של ניהול תיקי השקעות. כיוון שניהול תיקים באמצעות יישום אלגוריתמי עשוי להפוך את הפעילות משירות אישי באופיו למוצר מדף השקול לקרנות נאמנות, נקבע בהוראה כי ניהול תיקים כאמור בידי תאגיד הקשור לתאגיד בנקאי, יכלול אך ורק יחידות של קרנות נאמנות, פיקדונות ומזומנים.⁴²⁴

יישום ההוראה ושימושי בינה מלאכותית בייעוץ השקעות וניהול תיקים בישראל

מאז נקבעה הוראת שירותים מקוונים נעשה בה שימוש על-ידי הגופים המפוקחים. ההוראה נמצאה שימושית בעיקר ביחס לשני השלבים הראשונים שתוארו לעיל – שלב בירור הצרכים וההתקשרות בהסכם ושלב קביעת מדיניות ההשקעה ורמת הסיכון של הלקוח. בין היתר, גורמים מפוקחים נעזרים בשאלונים מקוונים וצ'אט-בוטים לשם ביצוע תהליך הצטרפות הלקוחות והכנסתם למערכת הגוף המפוקח (תהליך ה-onboarding).

השימוש בשלב השלישי של מתן השירות השוטף הוא מוגבל לעת עתה. בהקשר זה גורמים מפוקחים נעזרים ביישומים אלגוריתמיים בעיקר ככלי תומך החלטה, תוך שימור המעורבות האנושית. לעומת זאת, המקרים בהם בעלי רישיון מבצעים את פעילות הליבה של הפקת המלצות השקעה ומסירתן ללקוח (שעה שמדובר בייעוץ השקעות) וקבלת החלטות השקעה (שעה שמדובר בניהול תיקי השקעה), באופן בלעדי באמצעות יישומי בינה מלאכותית, הם נדירים. הרושם הוא כי הן בעלי הרישיון והן הלקוחות מוצאים ערך באינטראקציה אישית ולא נוטים לוותר עליה באופן מלא. עבור בעלי הרישיון מדובר באמצעי ללמוד עוד על הלקוח, ליצור מערכת יחסים ואמון עימו, ולבדוק מהם צרכי ההשקעה להם ניתן לתת מענה. גם עבור הלקוחות מענה ממוחשב מלא עלול להיראות חסר ולא אינטראקציה אישית עשוי להיות ערך מוסף בנוחות ובאמון שהיא מעניקה. יש להניח אם כן כי שיקולי מומחיות, עלות, ונטיית בעלי הרישיון והלקוחות לשמר אינטראקציה אישית, הם המובילים לאימוץ מודלים היברידיים בשלב זה.

ניתן לסכם אם כן, כי עד כה עיקר השימוש בישראל בבינה מלאכותית וקבלת החלטות אוטומטית בפעילויות ייעוץ

420 סעיפים 10, 11, 12 ו-20 להוראה.

421 דברי ההסבר להוראה.

422 סעיפים 3, 18 להוראה.

423 סעיף 3 להוראה.

424 סעיף 21 להוראה ודברי ההסבר להוראה.

השקעות היה בביצוע בירור הצרכים וקביעת מדיניות ההשקעה ורמת הסיכון של הלקוח. ישנם גם בעלי רישיון העושים שימוש בבינה מלאכותית ביחס לעצם מתן המלצות השקעה או ניהול תיקי השקעות אך מקרים אלה אינם שכיחים לעת עתה.⁴²⁵

היקף השימוש המוגבל בישראל עד כה תואם את האמור בסקירות לגבי המתרחש בעולם. בדוח ESMA משנת 2023, צוין כי אף שאפשרויות השימוש (use cases) בבינה מלאכותית הן רבות ומבטיחות הרי שהיקף היישום בפועל משתנה בין סקטורים ולא נראה עדיין שימוש נרחב בבינה מלאכותית בתהליכים עסקיים מרכזיים בתעשייה הפיננסית. באופן כללי, למרות שימוש גדל בבינה מלאכותית בתמיכה ובאופטימיזציה בחלק מהפעילויות, נראה שאין מדובר בשינוי מהיר וחזק (disruptive) בתהליכים העסקיים.⁴²⁶ ביחס ליעוץ השקעות ממוחשב צוין כי בפועל הוא מבוסס על אלגוריתמים פשוטים ומידע מוגבל, וביחס לניהול תיקים צוין כי נרשם עניין בקרב גורמים בתעשייה אך לא נראה שינוי משמעותי באופן ההשקעה.⁴²⁷ בדומה לכך, בדוח ה-OECD משנת 2023, צוין כי שימושים מתקדמים בבינה מלאכותית המשקפת אוטומציה מלאה נמצאים בשלבי פיתוח בלבד, אם בכלל, וקצב האימוץ של מערכות בינה מלאכותית הנו איטי. בין יתר הסיבות האפשריות שצוינו כתורמות לכך הן הסביבה הרגולטורית, האחריות המוטלת על גופים פיננסיים, הסיכונים השונים הגלומים במערכות אלה, כגון בקשר עם מידת הדיוק של התוצרים, פרטיות מידע, והמורכבות בהחלפת מערכות קיימות.⁴²⁸

רגולציה בנושא בינה מלאכותית ביעוץ השקעות וניהול תיקים בראי השוואתי

בדומה להוראת שירותים מקוונים בישראל, נקבעו במדינות נוספות בחו"ל הסדרים המבקשים להסדיר פעילות של יעוץ וניהול השקעות דיגיטלי. פעילות זו כונתה בשמות כגון digital advice, robo-advice או automated advice, והתאפיינה בכך שהפעולות נעשות באופן מקוון ובמעורבות אנושית מוגבלת, או אף ללא מעורבות אנושית כלל. מטרת הסדרים רגולטוריים אלה אינה רק הגנת ציבור המשקיעים שיקבל שירותים אלה, אלא גם הנגשת שירותים של יעוץ השקעות וניהול תיקים לציבור הרחב.

קווי המתאר של ההסדרים שנקבעו במדינות השונות דומים ביסודם. הם קובעים כי בהתאם לעיקרון של ניטרליות טכנולוגית ותכלית הגנת המשקיעים, חלות ככלל החובות הרגילות החלות על בעלי רישיון "רגילים". במסגרת ההסדרים מוסבר כיצד ליישם חובות אלה בעת ביצוע הפעילות באופן מקוון ואוטומטי, וכן מוצגות התאמות שונות הנדרשות בביצוע פעילות זו. אפשר לראות לדוגמה, הוראות הנוגעות לדרישות מיומנות והבנה בקשר עם האמצעים הטכנולוגיים, הוראות הנוגעות לבקורות על האמצעים הטכנולוגיים ותוצרי הפעילות, הוראות העוסקות בגילוי שיש לתת ללקוח על מאפייני הפעילות, הוראות הנוגעות לתיעוד הפעילות, הגנת מידע והמשכיות עסקית, והוראות העוסקות במיקור חוץ בעזרתו נעשית הפעילות.

גישה זו באה לידי ביטוי גם בפרסום של רשות ניירות הערך האירופאית (ESMA), לאחר פרסום דוח הביניים, בו הוסבר כי על מנת לעמוד בדרישות הדין הקיים (דירקטיבת MIFID II האירופאית), נדרשים גופים מפוקחים העושים שימוש בטכנולוגיות בינה מלאכותית, לפעול לטובת הלקוחות, למסור להם גילוי בדבר התפקיד שממלאות טכנולוגיות אלה בשירותים הניתנים להם, ולקבוע הסדרים ארגוניים הנוגעים לממשל, ניהול סיכונים, ידע ומיומנות העובדים.⁴²⁹

יש לציין, כי חלק מההסדרים הזרים מפורטים יותר, וחלקם אינם זהים בתחולתם בהשוואה להוראה הישראלית, אלא עוסקים בפעילויות נוספות כמו יעוץ לגבי פעילות פיננסיות נוספות או פעילות ברוקראז'. אולם כפי שניתן להתרשם, מדובר בסטנדרטים דומים לאלה שעוצבו בישראל.⁴³⁰ בד בבד עולה כי ההסדרים האמורים, בחו"ל ובישראל, נועדו לטפל בעיקר בתופעה של מעבר לשירותי יעוץ השקעות דיגיטלי ואוטומטי. הפריצה הטכנולוגית בפעילויות בינה מלאכותית לאחרונה מסמנת התקדמות אפשרית ליישומים מתוחכמים יותר, אשר האסדרה שפורסמה לא טיפלה

425 ראו למשל התשובה שניתנה בחודש אוקטובר 2022 על-ידי רשות ניירות ערך במענה לפניית חברה בעלת רישיון יעוץ השקעות להפיק אנליזות דיגיטליות על בסיס אלגוריתמים שפיתחה, בהתאם להוראת שירותים מקוונים:

<https://app.new.isa.gov.il/public/download/media/12766.json>.

426 דוח ESMA משנת 2023, בעמ' 3, 19.

פעילות NLP מוזכרת עם זאת ככזו ההופכת רווחת יותר מקום בו יש צורך בעיבוד כמויות גדולות של טקסט ואיתור מידע לא מובנה.

427 דוח ESMA משנת 2023, בעמ' 5–10.

428 דוח ה-OECD משנת 2023, בעמ' 10–12.

429 ראו ESMA, Public Statement On the Use of Artificial Intelligence (AI) in the provision of retail investment services (30 May 2024), https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdf.

430 להרחבה על הרגולציה החלה על Robo Advising בחו"ל ראו בדוח אונ' תל-אביב, בעמ' 24–27.

בהם.

במקביל להתקדמות הטכנולוגית האמורה, משתקף חשש גובר מצד רשות ניירות הערך האמריקאית (SEC) בנוגע לשירותים אוטומטיים (robo-advising) ובינה מלאכותית ביעוץ השקעות וניהול תיקים. חשש זה בא לידי ביטוי, בין היתר, בממצאי ביקורת שהעלו ליקויים בפעילותם של יועצי השקעות, לרבות בקשר עם תכניות ציט, ניהול תיקים באופן שיעלה בקנה אחד עם אינטרס הלקוח, ופרקטיקות שיווק;⁴³¹ בהתבטאויות של יו"ר ה- SEC בדבר הסיכונים הגלומים בבינה מלאכותית, בין היתר בהתייחס לפגיעה ביציבות פיננסית לקבלת החלטות דומה בהתבסס על אותו מודל;⁴³² ובפרסום הצעת ה- SEC משנת 2023 שעניינה ניגודי עניינים בקשר עם ניתוח מידע תחזיתי (Predictive Data Analytics) בעבודת ברוקר-דילר ויועצי השקעות.⁴³³

הצעת הכללים בעניין Predictive Data Analytics היתה מיועדת לחול על טכנולוגיות שונות הנכללות תחת המונח Covered Technology.⁴³⁴ על פי ההצעה ברוקרים, דילרים ויועצי השקעות יידרשו להעריך טכנולוגיות ניתוח מידע תחזיתי הנמצאות בשימוש על-ידם, לזהות, ולהעלים או לנטרל ניגודי עניינים העלולים להוביל לכך שאינטרס הגורם המפוקח יבוא על חשבון אינטרס הלקוחות. על הגורמים המפוקחים לאמץ וליישם מדיניות ומנגנונים לשם כך, וכן לתעד את הבקורות שיישמו. החשש הניצב מאחורי ההצעה הוא כי יישומי בינה מלאכותית מחמירים בעיות מסורתיות של ניגודי עניינים, כגון מתן ייעוץ או ניהול השקעות באופן מוטע על מנת להניב דמי ניהול או עמלות מסחר גבוהות יותר. זאת בין היתר מפני שזיהוי ניגודי העניינים והטיפול בהם עלולים להיות קשים יותר, והיקף הנזק מהטיה עלול להיות גדול יותר.⁴³⁵

ביקורת רבה נמתחה על הצעת כללים זו, ונטען כי ככל שתאושר במתכונת המוצעת או דומה, היא עשויה להקשות מאוד על השימוש ביישומי בינה מלאכותית. כך למשל עשוי להיות קושי בזיהוי מדויק של ניגודי עניינים וביצוע בקורות על תוצרי מערכות בינה מלאכותית, אשר יכולת ההסבריות שלהן מוגבלת. ההצעה משקפת גם דרישה להתמודד עם ניגודי עניינים באמצעות נטרול, להבדיל מאשר באמצעות אמצעים של גילוי נאות או צמצום ניגודי העניינים.⁴³⁶ בהמשך לחילופי הממשל בארה"ב, הודיעה ה- SEC בחודש יוני 2025 כי אינה מתכוונת לקדם עוד את ההצעה האמורה.⁴³⁷

יתרונות וסיכונים מרכזיים תוך שימוש בבינה מלאכותית ביעוץ השקעות וניהול תיקים

לאורך הדוח נסקרו יתרונות וסיכונים שונים של בינה מלאכותית בתחום הפיננסיים. בין היתר נדונו סיכונים הקשורים בפגיעה בפרטיות, התבססות על מידע לא אמין או חלקי, פגיעה ביכולת ההסבריות, וכן הלאה. נבקש להתמקד כעת ביתרונות וסיכונים מרכזיים שהנם מיוחדים יותר לפעילות של ייעוץ השקעות וניהול תיקים.

יתרונות מרכזיים

יתרונות מרכזיים בשילוב של בינה מלאכותית בפעילות של ייעוץ השקעות וניהול תיקים הם הרחבת השירותים למספר גדול הרבה יותר של לקוחות; החיסכון הצפוי בעלויות מתן השירותים; והפוטנציאל לשיפור השירותים עצמם והתהליכים הנלווים להם אצל נותני השירותים.

(1) הרחבת היקף הפעילות וציבור הלקוחות הנהנים משירותי ייעוץ השקעות וניהול תיקים

שירותים של ייעוץ השקעות וניהול תיקי השקעות יכולים לסייע מאוד לציבור הרחב בניהול כספיו. יועצי ההשקעות

431 SEC Risk Alert, Observations from Examinations of Advisers that Provide Electronic Investment Advice (November 9, 2021), <https://www.sec.gov/files/exams-eia-risk-alert.pdf>.

432 SEC Chair Gary Gansler "Remarks before the Financial Stability Oversight Council: 2023 Annual Report" (December 14, 2023), <https://www.sec.gov/news/speech/gansler-remarks-fsoc-121423>.

433 הצעת ה- SEC משנת 2023.

434 Covered technology means an analytical, technological, or computational function, algorithm, model, correlation matrix, or similar method or process that optimizes for, predicts, guides, forecasts, or directs investment-related behaviors or outcomes.

435 הצעת ה- SEC משנת 2023, בעמ' 33–6.

436 Daniel Michael, David Simon, Merin Cherian "Understanding SEC's Focus Amid Lack of Final AI Rules" Skadden Insights (February 23, 2024), <https://www.skadden.com/insights/publications/2024/02/understanding-sec-focus-amid-lack-of-final-ai-rules>; James Deekan "SEC Predictive Tech Ban Causes Confusion for Investment Advisers" Bloomberg Law (January 8, 2024), <https://news.bloomberglaw.com/us-law-week/sec-predictive-tech-ban-causes-confusion-for-investment-advisers>.

437 <https://www.sec.gov/rules-regulations/2025/06/s7-12-23>

מעניקים ייעוץ אובייקטיבי, לאחר בדיקה מעמיקה של מטרות ורמת הסיכון של המשקיעים. תפקידם להמליץ למשקיעים כיצד לבנות את תיק ההשקעות שלהם, וכן לסייע בבחירת השקעות ספציפיות. בדומה לכך, מנהלי תיקי השקעות מקבלים הרשאה לחשבונות ניירות ערך של הלקוחות, בונים עבורם תיקי השקעות, בהתאם למאפייני הסיכון ולהעדפות ההשקעה שהוגדרו מראש, ומבצעים את פעולות ההשקעה עבורם.

הרחבת מעגל הלקוחות אשר מקבלים שירותי ייעוץ או ניהול תיקים מבעל רישיון מפוקח היא אינטרס מובהק של הציבור והמדינה היות וציבור שאינו מבין בתחום ואינו מלווה בשירות תיווך פיננסי, ישאר על פי רוב מחוץ למעגל המשקיעים או יפנה לגורמים שאינם מפוקחים – פעולה העשויה להוביל לאובדן כספי, לרבות בשל תרמית או הונאה. על אף האמור, בשנים האחרונות ניכרת ירידה מתמשכת במספר בעלי הרישיון בישראל, כמו גם ירידה במספר הלקוחות הנהנים משירותים של ייעוץ השקעות וניהול תיקים.⁴³⁸ סיבות עיקריות לירידה זו הן העלויות הכרוכות במתן השירותים וכפועל יוצא מכך העדפה של בעלי רישיון להעניק אותם רק ללקוחות בעלי היקף השקעה מינימלי גבוה, וכן פנייה של הציבור לערוצים שאינם מפוקחים (בין שפעילותם חוקית ובין שאינה חוקית). הטמעת מערכות בינה מלאכותית עשויה להפוך מגמה זו ולסייע בהנגשת השירותים לציבור רחב יותר.

(2) חיסכון בעלויות

מעבר אפשרי לאוטומטיזציה והפחתת ההסתמכות על הון אנושי בשלבים שונים של מתן השירות, כמו גם בפעילויות נלוות כגון back-office או ציות, צפוי להפחית את עלויות הפעילות. חיסכון כאמור עשוי להוביל להתגשמות היתרון הקודם שהוזכר, קרי הרחבת שירותי ייעוץ ההשקעות וניהול התיקים לציבור רחב יותר של לקוחות, וכן להתגלגל להפחתת עלות השירותים ללקוחות.

(3) שיפור איכות השירות

היישומים הרבים האפשריים לבינה מלאכותית בתחום ייעוץ ההשקעות וניהול התיקים תוארו לעיל. איכות השירות עשויה להשתפר בין היתר בממדים של זמינות המענה ללקוח, היקף המענה ללקוח, והתאמה טובה יותר של השירות לצרכיו. יש לציין עם זאת כי בעוד שלפחות לגבי חלק מהשימושים שפורטו לעיל, כניסתה של בינה מלאכותית צפויה לשפר את המצב הקיים, הרי שביחס לליבת שירותי ייעוץ ההשקעות וניהול התיקים – קרי בירור הצרכים, התאמת הפעילות לצרכי הלקוח, ומתן המלצות ההשקעה או קבלת החלטות ההשקעה – קיימת מחלוקת בשאלה אם שירות לא אנושי יהיה טוב מהקיים. כך למשל, בכתיבה העוסקת בשירותי ייעוץ השקעות אוטומטיים (robo-advising) הועלו ספקות לגבי איכות השירות, ובפרט היכולת של מערכות ממוחשבות להבין את מצבו של הלקוח בהקשר רחב.⁴³⁹ אף בהנחה שמערכות בינה מלאכותית מתוחכמות יוכלו לשפר בהיבטים מסוימים את מצב הדברים, בדוח זה מוצגות בעיות אחרות שעשויות להתממש, כמו בעיות הסברתיות, ניגודי עניינים, וכדומה, אשר יפגעו באיכות השירות.

סיכונים מרכזיים

(1) אי עמידה בחובות אמון וזהירות והתממשות ניגודי עניינים פוטנציאליים

ביקורת מרכזית שהושמעה בחו"ל ביחס לפעילות של robo-advising נוגעת ליכולתן של מערכות ממוחשבות לעמוד בחובות האמון וזהירות הקבועות ביחס לפעילות של בעלי רישיון ייעוץ השקעות וניהול תיקים. ביחס לחובת הזהירות נטען, בין היתר, כי מילוי שאלונים באופן דיגיטלי עלול להחמיץ מידע רלוונטי אודות הלקוח, כי נחוצה ראייה אנושית כדי להבין סיטואציות מסוימות הנוגעות לצרכי הלקוח, וכי הפעילות האוטומטית עלולה להיות יעילה אך פשטנית.⁴⁴⁰ מערכות בינה מלאכותית על בסיס טכנולוגיית LLM או טכנולוגיות מתקדמות אחרות צפויות להיות מתוחכמות יותר וכך לשפר את הבנת צרכי הלקוח והתאמת השירות לצרכיו, אולם לפחות בשלב הביניים הנוכחי הן סובלות מבעיות אחרות, כגון תשובות גנריות שאינן מותאמות דיון, תשובות לא מאוזנות המשקפות מידע חלקי או לא מהימן ואף "הזיות" (hallucinations), קרי תוכן לא נכון.⁴⁴¹

⁴³⁸ ראו הנתונים להלן בפרק זה.

⁴³⁹ ראו דוח אונ' תל-אביב, בעמ' 20 והאסמכתאות המוזכרות שם, וכן בהמשך פרק זה.

⁴⁴⁰ שם, בעמ' 19-21 והאסמכתאות המוזכרות שם; Itamar Caspi, Sarit S. Felber, Talia B. Gillis, Generative AI and the Future of Financial Advice Regulation, Proceedings of the 38th International Conference on Machine Learning, PMLR 139, 2021, <https://blog.genlaw.org/CameraReady/19.pdf>.

⁴⁴¹ שם, בסעיף 4. מנגד אפשר לטעון כי גם ייעוץ בידי בני אדם אינו נטול בעיות ואף הוא עלול לסבול מהטיות, ניגודי עניינים או אי הבאה בחשבון של מידע רלוונטי. טענה זו עולה כמובן גם בהקשרים אחרים של המעבר מפעילות אנושית לבינה מלאכותית.

ביחס לחובת האמונים נטען כי מערכות בינה מלאכותית עלולות להביא בחשבון שיקולים זרים תוך העדפת ענייניו של נותן השירות על פני טובת הלקוח. יתרה מכך, לנוכח מאפייני הפעילות של המערכות, והקושי להסביר את עבודתן, התממשות של ניגודי עניינים כאמור עלולה להיות קשה יותר לניטור ולטיפול בהשוואה ליעוץ השקעות או ניהול תיקים אנושי. חשש זה מהתממשות ניגודי עניינים עומד כפי שפורט לעיל בבסיס הצעת הכללים של ה-SEC להחמרת הרגולציה על מערכות בינה מלאכותית בתחומים האמורים.⁴⁴²

טכנולוגיה של בינה מלאכותית יוצרת עשויה אף היא לאתגר את חובות האמון והזהירות של בעלי רישיון, כיוון שהיא מקשה על יצירת גבולות פעולה ברורים. כך למשל, בפעילות ניהול תיקים שתתבסס על אלגוריתם לומד ומגיב, או בתקשורת של צ'אט-בוט של בעל רישיון מול לקוח, שכוללת יצירת תכנים ואינה מוגבלת לקבוצה מוגדרת של תכנים.

(2) סיכוני משחקיות (Gamification)

תופעת המשחקיות (Gamification) בפעילות פיננסית התרחבה בשנים האחרונות בשוקי ההון בעולם. המדובר בשימוש בכלים טכנולוגיים במטרה להפוך את הפעילות הפיננסית בה עוסקים הלקוחות לדמויות משחק. אפליקציות ידידותיות בטלפון הנייד, ממשקי לקוח נוחים, עיצוב המזמין ביצוע פעולות והשקעות, "דחיפת" מידע והצעות (push notifications), "תגמול" סמלי או מעשי (rewarding) בגין ביצוע פעולות, הם אמצעים להשגת אותה משחקיות. כלים אלה מכוונים בעיקר לציבור משקיעים לא מתוחכם (משקיעי retail), בפרט משקיעים צעירים.⁴⁴³

תופעת המשחקיות התעצמה לא רק בשל שינויים טכנולוגיים אלא גם על רקע מאפיינים אחרים שהגדילו את השתתפות הציבור בהשקעה עצמאית בניירות ערך, כגון היכולת לסחור בסכומים קטנים וללא עמלות בפלטפורמות מסחר. היא מאפיינת בעיקר פעילות של מסחר בניירות ערך, אך רלוונטית גם לפעילויות קשורות כמו ייעוץ השקעות. בארה"ב לדוגמה הפכו פלטפורמות מסחר כגון Robinhood פופולריות מאוד בקרב משקיעים.

אמנם אפשר למצוא נקודות חיוביות במשחקיות בתחום הפיננסיים, ובהן יצירת עניין בקרב הציבור הרחב, הנגשת פעילות ההשקעה, והשתלבות בחינוך פיננסי. ואולם מנגד הועלו חששות כבדים מצד רגולטורים וגורמים נוספים לגבי משחקיות, ובין היתר: חשש לניצול חולשות אנושיות לצורך ביצוע פעולות מיותרות או שגויות; הסטת המשקיעים מהתנהגות רציונלית באופן כללי או הסטתם לעבר ביצוע פעולות מסוימות, כגון רכישת מניות מסוימות; ועידוד פעילות עדרית כגון רכישת מניות לאחר שמחיריהן עלו בשיעור משמעותי. פרשת GameStop בה התרחש מסחר רחב היקף וספקולטיבי, שהוביל לנסיקה וצניחה בשער מניית החברה, המחשה את הסיכונים הגלומים בהשקעה שאינה מבוססת על שיקולים כלכליים, הן למשקיעים עצמם הן לתקינות השוק בכללותו, וכן בעידוד לא מבוקר של פעילות השקעה בפלטפורמות מסחר וברשתות חברתיות.⁴⁴⁴

בהינתן היקף התופעה בארה"ב, ננקטו בעניינה גם פעולות רגולטוריות. ה-SEC פרסמה בשנת 2021 בקשה לקבל מידע והתייחסות לפרקטיקות בתקשורת דיגיטלית (Digital Engagement Practices) של ברוקר-דילר ויועצי השקעות עם לקוחות.⁴⁴⁵ פרקטיקות אלה כוללות תמריצי התנהגות, פעילות שיווק פרסונלית ודיפרנציאלית, מאפיינים משחקיים בפעילות, ורכיבים נוספים שנועדו לעודד פעילות של לקוחות. בהמשך לכך, פורסמה ההצעת ה-SEC משנת 2023 שתוארה לעיל, שעניינה ניגודי עניינים בקשר עם ניתוח מידע תחזיתי (Predictive Data Analytics) בעבודת ברוקר-דילר ויועצי השקעות, אם כי הצעה זו נזנחה כאמור.

442 ראו דוח אונ' תל-אביב, בעמ' 21-23 והאסמכתאות המוזכרות שם;

Nicole G. Iannarone, Computer as Confidant: Digital Investment Advice and the Fiduciary Standard, 93 Chi.-Kent L. Rev., 141 (2018). <https://scholarship.kentlaw.iit.edu/cklawreview/vol93/iss1/5>; Sophia Duffy and Steve Parrish, You Say Fiduciary, I Say Binary: A Review and Recommendation of Robo-Advisors and the Fiduciary and Best Interest Standards, 17 Hastings Bus. L.J. 3, https://repository.uclawsf.edu/hastings_business_law_journal/vol17/iss1/3 (2021).
James Fallow Tierney, Investment Games, 72 Duke Law Journal 353-446 (2022), <https://scholarship.law.duke.edu/dlj/vol72/iss2/2>; Nolan Schloneger "A Case for Regulating Gamified Investing" 56 Ind. L. Rev. 175 (2022), <https://doi.org/10.18060/27147>.

444 ראו עוד על פרשת GameStop:

Game Stopped? Who Wins and Loses When Short Sellers, Social Media, and Retail Investors Collide: Hearing Before the H. Comm. on Fin. Servs., 117th Cong. (2021), <https://www.govinfo.gov/content/pkg/CHRG-117hrg44837/pdf/CHRG-117hrg44837.pdf>; Jill E. Fisch "GameStop and the Reemergence of the Retail Investor" 102 B.U.L. Rev. 1799 (2022), https://scholarship.law.upenn.edu/faculty_scholarship/2817/.

Request for Information and Comments on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools and Methods, and Regulatory Considerations and Potential Approaches; Information and Comments on Investment Adviser Use of Technology To Develop and Provide Investment Advice, Securities Exchange Act Release No. 92766 (August 27, 2021), 86 Fed Reg. 49067 (Sept. 1, 2021), available at <https://www.federalregister.gov/d/2021-18901>

ככל שפעילות של בינה מלאכותית הופכת משמעותית ומתוחכמת יותר, כך היא עשויה לשמש להגברת המשחקיות בפעילות פיננסיות, על הסיכונים הגלומים בה. בין היתר, אלגוריתמים יכולים להתאים את פעילות ייעוץ ההשקעות ופלטפורמות המסחר להעדפות (ולחולשות) של כל לקוח ולקוח, לנתח לעומק את התנהגות הלקוחות ולהניע אותם בהתאם לפעילות השקעה, ולהציע באופן מהיר תגובות ייעוץ או הצעות מסחר לפעולות של הלקוחות. לאלה מתווספים קשיים של הסברתיות ופוטנציאל ניגודי עניינים שתוארו לעיל.

(3) פגיעה באיכות השירות

כאמור לעיל, החשש מפני פגיעה באיכות השירות הניתן ללקוחות נדון בעולם אגב התרחבות הפעילות של ייעוץ השקעות אוטומטי (robo-advising). סימני השאלה בדבר איכות השירות ממשיכים לרחף גם ביחס לפעילות מתוחכמת יותר של בינה מלאכותית.

ביחס לייעוץ השקעות אוטומטי עלו חששות כי בירור צרכי הלקוח יהיה פשטני, כי מצבו של הלקוח לא יובן באופן מלא, כי המלצות ההשקעה יהיו גנריות ופחות מותאמות לצרכי הלקוח, ובסופו של יום הנגישות מרחוק והחיסכון בעלויות יבואו על חשבון איכות הייעוץ.

קפיצת היכולות שהתרחשה לאחרונה במערכות בינה מלאכותית נושאת עימה הבטחה לשיפור ניכר בהשוואה לפעילות של ייעוץ השקעות אוטומטי שנעשה עד כה. היכולות המשופרות של הבנת שפה ומתן מענה כמו-אנושי, יכולות חזקות יותר לניתוח מידע ולהצגת חלופות מגוונות, ויכולות משופרות להשיג פרסונליזציה הנחוצה בבירור צרכי לקוח ובהתאמת השירות ללקוח – כל אלה צפויות לשפר את השירות הדיגיטלי שהיה אפשרי עד כה. בד בבד, לפחות בשלב הנוכחי בו מצויה הטכנולוגיה, נראה כי התבססות על מודלים כלליים של LLM עדיין עלולה להשיג תוצאות מעורבות, בדמות מידע חלקי, לא מאוזן, המלצות גנריות ולא עדכניות או מבוקרות. פיתוח של מערכות בינה מלאכותית ייעודיות צפוי להוביל לשיפור בתוצרים, ורבים מאמינים כי הדבר אכן צפוי להתרחש בעתיד הקרוב, בתחומי חיים רבים כמו גם בתחום הפיננסיים אך בתקופת הביניים עד השקעה ואופטימיזציה של מערכות כאלה קיים סיכון לפגיעה באיכות השירות.

(4) ריכוזיות ותלות במספר קטן של מערכות

סיכון ייחודי אחרון שראינו מקום לציין לגבי פעילות בינה מלאכותית בייעוץ השקעות וניהול תיקים נובע מכך שמספר קטן של מערכות טכנולוגיות עשוי לשמש בעתיד בעלי רישיון רבים ולקוחות רבים מאוד. החששות העולים בהקשר זה הם לפגיעה בגיוון ההשקעות וקורלציה בתיקי ההשקעות של לקוחות רבים; לכך שתקלה או טעות במערכות תהיה בעלת השפעה רוחבית על השוק כולו; ולתלות שתיווצר במספר קטן של גורמים, לרבות תלות במיקור חוץ של מספר יצרנים דומיננטיים.⁴⁴⁶ בכל הקשור לפעילות ייעוץ השקעות וניהול תיקים בישראל, סיכון זה נראה רחוק מהתממשות, אולם יש להביאו בחשבון ככל שדפוסי הפעילות ישתנו.

יתרונות וסיכונים מיוחדים לפעילות בינה מלאכותית בייעוץ השקעות וניהול תיקים	
הרחבת היקף הפעילות וציבור הלקוחות הנהנים משירותי ייעוץ השקעות וניהול תיקים	אי עמידה בחובות אמון וזהירות והתממשות ניגודי עניינים פוטנציאליים
חיסכון בעלויות	סיכוני משחקיות (Gamification)
שיפור איכות השירות	פגיעה באיכות השירות
	ריכוזיות ותלות במספר קטן של מערכות

המלצות בנושא ייעוץ השקעות וניהול תיקים

המעבר לייעוץ השקעות וניהול תיקי השקעות אוטומטי החל לתפוש תאוצה בעולם לפני כעשור. בישראל מדובר עד כה על פי רוב במעבר חלקי, לשירות שאינו ממוחשב במלואו, אלא נשען עדיין על פעילות אנושית בהיבטי הליבה של

446 ראו דוח אונ' תל-אביב, בעמ' 23–24; דוח ה-OECD משנת 2023, בעמ' 24–25. ראו עוד על סיכונים אלה בפרקים העוסקים ביציבות פיננסית ובתחרות.

הפקת ההמלצות (בשירות ייעוץ) או קבלת החלטות ההשקעה (בשירות ניהול תיקים). ההתפתחויות הטכנולוגיות האחרונות בתחום הבינה המלאכותית צפויות להאיץ מעבר זה, הן בפן של מספר הגופים והלקוחות הן בפן של היקף הפעילות האוטומטית.

למעבר זה לאוטומציה עשויות להיות השלכות משמעותיות. מצד אחד, הוא עשוי לגלם יתרונות משמעותיים כגון הנגשת השירותים לציבור רחב יותר, ייעול התהליכים, והפחתת עלויות עבור המשקיעים ובעלי הרישיון כאחד. מצד שני, מעבר לא מוצלח עלול להוביל להתממשות סיכונים, כגון אי-הבנת השירות על-ידי הלקוחות, מתן המלצות וקבלת החלטות שאינן מותאמות ללקוחות (למשל לפרופיל הסיכון שלהם), וסיכונים טכנולוגיים ותפעוליים הקשורים בהפעלת המערכות.

(1) עידוד יישומי בינה מלאכותית לשם הרחבת פעילות של ייעוץ השקעות וניהול תיקים

נתוני השנים האחרונות מצביעים על ירידה בהיקף הפעילות המפוקחת של ייעוץ השקעות וניהול תיקים. בתחום ייעוץ ההשקעות בא הדבר לידי ביטוי בירידה במספר בעלי רישיון ייעוץ השקעות, במספר הלקוחות להם ניתן ייעוץ, ובסכומי כסף גבוהים הנדרשים לשם קבלת ייעוץ השקעות.⁴⁴⁷ – כך למשל, מספר היועצים הפעילים בבנקים ירד מ-1,513 בשנת 2020 ל-1,200 בסוף שנת 2023, מספר החשבונות המיועצים ירד מ-453 אלף בשנת 2018 ל-323 אלף בסוף שנת 2023, וממוצע שווי חשבון מיועץ עלה מ-656 אלף שקלים בשנת 2018 ליותר ממיליון שקלים בשנת 2023. בתחום ניהול התיקים בא הדבר לידי ביטוי בסטגנציה במספר חברות ניהול התיקים, במספר הלקוחות ובשווי הנכסים המנוהלים. כך למשל, מספר החברות המנהלות עמד על 124 ו-130 בשנים 2018 ו-2023, בהתאמה; מספר הלקוחות עמד על כ-83 וכ-85.5 אלף בשנים 2018 ו-2023, בהתאמה; ושווי הנכסים המנוהלים עמד על כ-271 וכ-324 מיליארד שקלים בשנים 2018 ו-2023, בהתאמה.⁴⁴⁸

חולשת נתוני הפעילות האמורים בולטת על רקע העובדה כי בחמש השנים האמורות גדל היקף הפעילות הכלכלית והיקף חסכוניות הציבור במשק. הסיבות לירידה האמורה בפעילות ייעוץ השקעות וניהול תיקים יכולות להיות מגוונות, אולם מובן כי יש לירידה זו בהיקף הפעילות השלכות שליליות על נגישות הציבור לשירותים פיננסיים מקצועיים ועל איכות ניהול חסכוניות הציבור. כפי שצוין לעיל, הרחבת מעגל הלקוחות היא אינטרס מובהק של הציבור והמדינה.

טכנולוגיית בינה מלאכותית יכולה להוביל לשינוי מגמה בהיקף שירותים אלה לרווחת הציבור. האוטומציה בשורה של פעולות צפויה לחסוך בעלויות הגופים המפוקחים ולהקל על הציבור להצטרף לשירותים. בבינה מלאכותית גלום גם פוטנציאל של ניתוח צרכים אישיים של משקיעים והתאמת ההמלצות או ניהול ההשקעות לצרכים אלה. כך יוכל הציבור, לרבות אוכלוסיות שאינן נהנות כיום משירותי ייעוץ השקעות או ניהול תיקי השקעות, לזכות בשירותים מקצועיים נגישים וזולים, על פני חלופות בעייתיות כגון ניהול עצמאי לא מקצועי, פנייה לאפיקים לא מפוקחים, או הסתמכות על ייעוץ כללי שאינו מותאם לצרכי הלקוח.

לנוכח המגמה האמורה והפוטנציאל הגלום בטכנולוגיית בינה מלאכותית, מוצע לפעול באופן אקטיבי על מנת לקדם הטמעה של הטכנולוגיה בקרב בעלי רישיון. בסקירת הרגולציה לא זוהה חסם ברור המונע פעילות כאמור וניתן לייחס את הפעילות המעטה בתחום גם למגבלות טכנולוגיות או עסקיות, אולם הניסיון מלמד כי צעדים אקטיביים בשיתוף השחקנים הפיננסיים יכולים לעודד פעילות חדשה. מעבר לדרכים המנויות בדוח זה לקידום ודאות רגולטורית וחדשנות (להלן בחלק ה' – פעולות נוספות לקידום רגולציה פיננסית בתחום הבינה המלאכותית), מוצע לפעול באופן פרטני מול שחקנים קיימים ופוטנציאליים, וכן לשקול פרסום מדריך המסביר באופן ידידותי מהם השירותים האפשריים וכיצד ניתן לעמוד בהוראות הדין. ראו לשם השוואה מדריך שפורסם לעניין פעילות robo-advising באוסטרליה, וכולל טיפים והסברים כיצד לעמוד בדרישות הדין. מידע מסוג זה יכול לסייע הן למפוקחים הן למי שמעוניין לפתח מערכות עבורם.⁴⁴⁹

⁴⁴⁷ רשות ניירות ערך, פעילות מערכי הייעוץ בבנקים 2023, https://www.new.isa.gov.il/images/Fittings/isa-be/asset_library_pic/al_lobby/al_lobby-6283705a39f5d/Consulting2023.pdf

⁴⁴⁸ רשות ניירות ערך, פעילות חברות בעלות רישיון לניהול תיקי השקעות, נתונים ליום 31.12.2022, https://www.new.isa.gov.il/images/Fittings/isa-be/asset_library_pic/al_lobby/al_lobby-637b90c7be39b/NihulTikim2023.pdf

⁴⁴⁹ ASIC, Regulatory Guide 255 – Providing digital financial product advice to retail clients (August 2016), <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-255-providing-digital-financial-product-advice-to-retail-clients>

(2) עדכון הוראת שירותים מקוונים

הוראת שירותים מקוונים מציגה תשתית לביצוע פעילות בבינה מלאכותית תוך שמירת האינטרס הציבורי, והיא עולה בקנה אחד עם הסדרים חוקיים בחו"ל. יחד עם זאת, בהינתן שההוראה נקבעה בשנת 2016, לפני ההתפתחויות האחרונות בבינה מלאכותית, מוצע לבחון עדכון שלה, הן בפן הטכני הן בפן המהותי.

בפן הטכני, רצוי לשקול עדכון של התייחסויות ומינוחים, כך שיתכתבו עם רגולציה עכשווית בנושא הבינה המלאכותית. כך למשל, ההוראה אינה מתייחסת כיום מפורשות לבינה מלאכותית ואינה כוללת מינוחים מקובלים כגון "הסבריות", "בינה מלאכותית יוצרת" וכדומה. בהקשר זה מוצע לשקול הוספת פרק ספציפי להוראה שיעסוק ביישומי בינה מלאכותית.⁴⁵⁰

בפן המהותי, מוצע להבהיר עוד מהם תפקידיו של הגורם האחראי אצל בעל הרישיון למתן השירותים הטכנולוגיים ("בעל הרישיון הממונה").⁴⁵¹ מנגנון זה אומץ גם בחו"ל ויש לו חשיבות רבה בעמידת בעל הרישיון בהוראות הדין. כך למשל, מוצע להבהיר מהם תפקידיו של בעל הרישיון הממונה בבדיקת תוצרי המערכת.

בנוסף יש לשקול התייחסות רגולטורית, במסגרת ההוראה או במקום אחר, לפעילות בינה מלאכותית שאינה קשורה בממשקים עם הלקוח. כמפורט בדוח זה, בינה מלאכותית צפויה למלא תפקיד בשורה של פעילויות נוספות אצל הגופים המפוקחים. מענה רגולטורי בהקשר זה יכול להינתן בהוראה ייעודית או בעמדה פרשנית, המסבירה את יישום החובות הקבועות בדין ביחס למערכות בינה מלאכותית.

עניינים נוספים שיש לבחון התייחסות פרטנית אליהם במסגרת עדכון ההוראה הוא השימוש בצ'אט-בוטים בקשר עם הלקוח (ראו להלן), והיבטי ניגודי עניינים הנמצאים במוקד העיסוק הרגולטורי בארה"ב.

(3) בחינת פעילות של צ'אט-בוטים והרגולציה שצריכה לחול בעניינה

הפיתוח שהעלה את קרנה של הבינה המלאכותית לאחרונה הוא מודלים מבוססי שפה (Large Language Models) (LLM). מודלים אלה הם סוג אחד של בינה מלאכותית יוצרת (GenAI), אשר התוכן שנוצר על-ידיה הוא שפה/טקסט. הם מסוגלים ליצור באופן מיידי תוכן חדש, תוך שיח ומענה עם האדם הפועל מולם.⁴⁵² יכולותיהם של מודלים אלה, ובהם ChatGPT אשר היה המודל הראשון שהושק לשימוש ציבורי רחב, עוררו השתאות ממספר סיבות ובהן ההתמודדות עם מגוון רחב מאוד של נושאים; קליטה ומיקוד יוצאי דופן במהות הפנייה; יכולת מענה גבוהה כפי שבאה לידי ביטוי באיכות השפה; גיוון בסוגי המענים האפשריים – באורך, בסגנון, וכדומה; ומיידיות התגובה.

השימוש בצ'אט-בוטים קדם לפיתוח מודלים מסוג LLM של בינה מלאכותית. צ'אט-בוט הוא הכינוי לכל אפליקציה המקיימת דיאלוג עם אדם בשפה טבעית, והוא יכול להתבסס גם על מודלים פשוטים יותר. כך למשל, ישנם rule-based chatbots, המבצעים התאמה בין שאלה של לקוח ובין תגובה הלקוחה מתוך פורטפוליו של תגובות אפשריות. צ'אט-בוט מסוג זה אינו יוצר תשובה חדשה.⁴⁵³ בתחומי חיים רבים לרבות המגזר הפיננסי, רווח השימוש בצ'אט-בוטים בעיקר בפעולות של תמיכה בלקוחות או פעולות בשירות עצמי.⁴⁵⁴

ההתפתחות שחלה במודלים של LLM, והממשקים הנוחים של ChatGPT ואפליקציות דומות שהושקו בעקבותיו, מגדילים את השימושויות של צ'אט-בוטים. הם צפויים להיכנס לפיכך לפעולות נוספות של נותני שירותים, ובהן פעולות המצויות בליבת השירות של ייעוץ השקעות וניהול תיקים – ביור צרכי הלקוח והתאמת השירות לצרכיו. מעבר להרחבת השימושים בצ'אט-בוטים, היכולות המשופרות של צ'אט-בוטים בהתבסס על טכנולוגיית בינה מלאכותית צפויות להוביל להשפעה גדולה יותר על הלקוחות. כך למשל, צ'אט-בוטים עשויים להיות אקטיביים יותר (להבדיל מתגובתיים), ללמוד את פניות הלקוח, להתאים את התגובה לפניותיו, להפגין רגשות לכאורה, ליצור קשר ולהגביר אמון.

התרחבות השימוש בצ'אט-בוטים מעוררת גם אתגרים רגולטוריים. כך למשל, פרסם המשרד להגנת הצרכן הפיננסי בארצות הברית (CFPB) דוח בשנת 2023, על צ'אט-בוטים בצרכנות פיננסית. בדוח הוסבר כי השימוש בצ'אט-

450 כיום כוללת ההוראה פרקים המתייחסים ספציפית לשירותי מסחר חברתי ואיתותים. בינה מלאכותית יכולה לשמש במגוון פעילויות בייעוץ השקעות וניהול תיקים, ולנוכח חשיבותה הצפויה בשנים הקרובות מוצע לשקול להקדיש לה התייחסות מפורטת יותר.

451 סעיף 7 להוראת שירותים מקוונים.

452 ראו דוח ה-OECD משנת 2023, בעמ' 8-9, 12-13, וכן בפרק יישומי בינה מלאכותית בסקטור הפיננסי לעיל.

453 ראו על סוגי צ'אט-בוטים אצל Eleni Adamopoulou, Lefteris Moussiades "Chatbots: History, technology, and applications" Machine Learning with Applications 2 (2020) 100006, <https://www.sciencedirect.com/science/article/pii/S2666827020300062>.

454 ראו דוח אונ' תל-אביב, בעמ' 28-30.

בוטים הולך וגדל: עשרת הבנקים הגדולים בארה"ב השיקו צ'אט-בוטים כחלק משירות הלקוחות שלהם; כ- 37% מאוכלוסיית ארה"ב קיימה פעילות בצ'אט-בוט מול בנק בשנת 2022 ושיעור זה צפוי לגדול; ויש מגמת מעבר מצ'אט-בוטים פשוטים לצ'אט-בוטים מתוחכמים יותר המבוססים על טכנולוגיות כגון LLM. הדוח מתאר תלונות שהתקבלו ב- CFPB מלקוחות שפעלו מול צ'אט-בוטים, ומעלות בין היתר את הנושאים הבאים: יכולת מוגבלת של הצ'אט-בוטים לפתור בעיות מורכבות; הגבלת נגישות הלקוחות למעורבות אנושית מהירה; מגבלות טכניות ובעיות הגנת מידע שנגזרות מהן; ואי-עמידה בדרישות הדין.⁴⁵⁵

בישראל הרגולציה החלה על ייעוץ השקעות וניהול תיקים, לרבות הוראת שירותים מקוונים, אינה עוסקת באופן ספציפי בצ'אט-בוטים, כל שכן צ'אט-בוטים המבוססים על טכנולוגיות עכשוויות ומתקדמות של בינה מלאכותית. מוצע לבחון פעילות זו, לעקוב אחר התפתחות הדין ההשוואתי, ובמידת הצורך לעדכן בעתיד את הרגולציה בישראל.⁴⁵⁶ עדכון כאמור יכול שיעשה באמצעות עדכון הוראת שירותים מקוונים כאמור לעיל או הבהרות ביחס לחובות זהירות ואמון בעת הפעלת צ'אט-בוט. כללי הרגולציה בהקשר זה צפויים לעסוק בסוגיות שנדונו בדוח זה, כגון הסבריות, מהימנות, פרטיות המידע, וכן לעסוק במאפיינים ייחודיים יותר לצ'אט-בוטים שעוסקים בייעוץ השקעות וניהול תיקים, כגון אימון האלגוריתמים בנושאים אלה ובקרה על תכניהם, הפעלתם בנושאים רגישים כמו טיפול במחלוקות בין נותן השירות ולקוחות, וזמינות של מענה אנושי לצד הצ'אט-בוטים.

(4) הבהרת הדין ביחס למערכות כלליות של בינה מלאכותית

כניסתן של מערכות בינה מלאכותית כלליות, המספקות מענה בכל נושא שהוא, כגון ChatGpt, Claude, וכדומה, מעוררות שאלות באשר לאיכות התוכן ולתחולת הדין. בקשר עם איכות התוכן עולה השאלה עד כמה המענה לשאלות בנושאי השקעה הוא טוב ומועיל ללקוח. בקשר עם תחולת הדין עולה השאלה האם חוק הסדרת העיסוק חל על מערכות מסוג זה כאשר הן מספקות לאדם המשתמש בהן ייעוץ השקעות.

בנוגע לאיכות התוכן יש דעות שונות. מחד יש הסבורים כי המלצות השקעה המוצגות על-ידי בינה מלאכותית הן גנריות, לא מעמיקות ולעתים אף לא מעודכנות. מאידך יש הסבורים כי מערכות בינה מלאכותית יכולות לספק כלי ניתוח לא רעים שאפשר לשפרם עוד.⁴⁵⁷ מכל מקום, דעות אלה נוגעות למערכות שהושקו בזמן האחרון, ויש להניח כי תוצרי המערכות ישתכללו וישתפרו עם הזמן.

בנוגע לתחולת הדין, מאפיינים שעשויים להיות רלוונטיים הם מגוון הנושאים המטופלים על-ידי מערכת הבינה המלאכותית, קיומה של תמורה בגין השימוש במערכת, וזהות הגורם המגיש אותה.

יצוין, כי לפני מספר שנים עלתה שאלה קשורה בנוגע לפעילות של ניהול תיקים אלגוריתמי, שעה שזירות סוחר טענו כי הן מנגישות ללקוח "תוכנת מדף" המאפשרת לאותו אדם לסחור באמצעות התוכנה, וכי פעילות זו פטורה מתחולת הדין. על זירות סוחר נאסר בדין לתת ייעוץ השקעות ללקוחות או לבצע עבורו עסקאות לפי שיקול דעת (קרי פעילות של ניהול תיקים).⁴⁵⁸ כפועל יוצא מכך הציגה רשות ניירות ערך תנאים בהתקיימם לא תראה הרשות באפשרות של הפעלת תוכנת מסחר על-ידי לקוח, במסגרת פעילותו בזירה, כפעילות של ייעוץ השקעות או ניהול תיקים, ובהם איסור שיווק של תוכנות מסחר אלגוריתמי או שידול לקוחות לבצע מסחר בהן על-ידי הזירה; איסור קשר בין הזירה ובין יצרן או מתכנת תוכנת המסחר; העדר שליטה על הפעלת תוכנת המסחר האלגוריתמי.⁴⁵⁹ גישה דומה הובעה על-ידי בית המשפט, ולפיה הנגשת התוכנה ללקוח על-ידי גורם מקומי אינה פעולה טכנית אלא נופלת בתחולת הדין.⁴⁶⁰

בעניין איכות המענה, מוצע לשקול פרסומים במסגרת חינוך פיננסי, המסבירים לציבור את המגבלות של מערכות בינה מלאכותית כללית והחלופה המתבקשת של שירות פיננסי ברישיון.

בעניין תחולת הדין, מוצע לשקול פרסום הבהרה לגבי הנגשה אסורה של מערכות בינה מלאכותית כלליות.

455 ראו ה"ש 45 לעיל.

456 ראו לעניין זה בדוח אונ' תל-אביב מסגרות רגולטוריות חלות על צ'אט-בוטים, וכן מסגרות בהקשרים אחרים: World Economic Forum, "Chatbots RESET – A Framework for Governing Responsible Use of Conversational AI in Healthcare" (December 2020), <https://www.weforum.org/publications/chatbots-reset-a-framework-for-governing-responsible-use-of-conversational-ai-in-healthcare/>.

457 ראו לדוגמה Dowling, Michael M. and Lucey, Brian M., ChatGPT for (Finance) Research: The Bananarama Conjecture (January 2023), <https://ssrn.com/abstract=4322651>; Kim, Alex G. and Muhn, Maximilian and Nikolaev, Valeri V., Financial Statement Analysis with Large Language Models (May 20, 2024). Chicago Booth Research Paper, Fama-Miller Working Paper, <https://arxiv.org/abs/2407.17866>.

458 תקנות 10(א) ו-10(ג) לתקנות ניירות ערך (זירות סוחר לחשבוננו העצמי), התשע"ה-2014.

459 רשות ניירות ערך, עמדת סגל משפטית: הצעת שירותי מסחר באמצעות אלגוריתם בזירת סוחר (14 בספטמבר 2016).

460 ראו סעיף 34 בעניין אפרימוב, וכן ההתייחסות לעמדת הרשות בסעיפים 50–52 לפסק הדין.

(5) מחקר על התנהלות לקוחות מול מערכות ממוחשבות

לשם קביעת רגולציה מיטבית על פעילות בינה מלאכותית וקבלת החלטות אוטומטית, יש חשיבות בהבנה מעמיקה של התנהגות המשתמשים. כך למשל: האם משקיעים מעדיפים לפעול מול מערכות אוטומטיות או לחלופין – מעדיפים שלא לפעול מולן, ומהן הסיבות לכך?; כיצד משקיעים מגיבים למידע והמלצות הניתנים להם על-ידי מערכות אוטומטיות?; האם משקיעים מושפעים יותר על המידה ממידע והמלצות של מערכות אוטומטיות וניתן להצביע על דפוסי התנהלות שונים שלהם בהשוואה לדפוסי ההתנהלות של לקוחות ביעוץ השקעות וניהול תיקים מסורתי?; מהו המשקל שמייחסים משקיעים, אם בכלל, לאזהרות הנמסרות להם במערכות אוטומטיות; ועוד.⁴⁶¹

סוגיות אלה וסוגיות נוספות מציגות שאלות מחקר מעניינות, וניתן לראות כי העיסוק בהן בעולם אכן גדל. התשובה לשאלות אלה, התלויה בין היתר בקצב אימוץ הטכנולוגיה בקרב הציבור, עשויה להשתנות על פני מדינות, תרבויות, תקופות זמן שונות, חתכי גיל ומאפיינים נוספים.

בישראל חסר מחקר בסוגיות אלה ויש מקום לקדמו. בראייה רגולטורית יש חשיבות בביצוע מחקרים בנושא הן לשם פיתוח השוק הן לשם הבנת ההשפעה של הטכנולוגיה על התנהגות המשקיעים. הדבר יסייע בהערכת הרגולציה הקיימת והנדרשת לגבי הפעילות. מחקר כאמור יכול להתבצע על-ידי הרגולטורים עצמם וכן במסגרות משותפות לרגולטורים, לאקדמיה ולגופים הפיננסיים. קיימות גם מסגרות אפשריות לעידוד מחקרים מצד הרגולטורים, כגון מימון כספי לביצוע מחקרים, סיוע בנגישות למידע רלוונטי, או פרסום קולות קוראים לעידוד מחקרים בנושא.

(6) הסדרת תחום שירותי המסחר (ברוקראז')

הצוות הונחה לעסוק באופן ספציפי בטכנולוגיית בינה מלאכותית בפעילויות של ייעוץ השקעות וניהול תיקי השקעות. בעיסוק הרגולטורי בעולם בולט הקשר בין פעילויות אלה ובין פעילות של שירותי מסחר (ברוקראז'). שירותי מסחר כוללים פלטפורמות מסחר המאפשרות לציבור לבצע באמצעותן מסחר בניירות ערך בבורסה וברוקרים ודילרים המבצעים פעולות מסחר בניירות ערך בבורסה עבור לקוחות. תחום שירותי המסחר עבר בשנים האחרונות שינויים משמעותיים, עם השקתן של פלטפורמות דיגיטליות המאפשרות לציבור הרחב לבצע בקלות עסקאות בניירות ערך ועם כניסתו של ציבור רחב לפעילות ישירה במסחר בניירות ערך, בפרט במהלך תקופת מגפת הקורונה.

לנוכח התפתחויות אלה, מעורר תחום שירותי המסחר סוגיות רגולטוריות כבדות משקל. כך לדוגמה, בארה"ב עסקו רבות בשנים האחרונות בסיכונים הנובעים מתופעת המשחקיות (gamification) שתוארה לעיל של פעילות המסחר, עידוד השקעה בקרב משקיעים מהציבור הרחב (משקיעי retail) ללא הבנת הסיכונים הגלומים בה, ניגודי עניינים בפעילות הפלטפורמות, ופגיעה בתקינות המסחר.

כפי שהוסבר לעיל, טכנולוגיית בינה מלאכותית יכולה להעצים סיכונים אלה. כך למשל, היא עשויה להגביר את יכולת ההשפעה על אופן הפעולה של משקיעים בפלטפורמות מסחר דיגיטליות (באמצעות הצעת שירותים ללקוחות, הנעתם לבצע פעולות, וכדומה). או למשל, היא עלולה להגביר את הסיכון לפעילות עדרית של משקיעים הסוחרים בניירות ערך בפלטפורמות אלה.

בישראל תחום שירותי המסחר אינו מפוקח על-ידי רשות ניירות ערך באופן ישיר. הפיקוח הוא עקיף וחלקי, בעיקר באמצעות הפיקוח של הבורסה על חברי הבורסה שאינם בנקים, דרכם נעשה מסחר בבורסה בהתאם להוראות הקבועות בתקנון הבורסה.⁴⁶² פער פיקוחי זה הנו חריג בהשוואה עולמית והוצע זה מכבר להשלימו.⁴⁶³ הצורך לעשות כן נבע מסיבות שונות ובהן הגנת ציבור המשקיעים, הרחבת פעילות הציבור במסחר בניירות ערך, כניסה של שחקנים

461 ראו אצל Caspi, Felber, Gillis, ה"ש 415 לעיל; Belanche, Daniel, Luis V. Casalo and Carlos Flavián "Artificial Intelligence in FinTech: understanding robo-advisors adoption among customers" Industrial Management & Data Systems 119.7 (2019) 1411, https://www.researchgate.net/publication/344743097_Artificial_Intelligence_in_FinTech_understanding_robo-advisors_adoption_among_customers#read; World Bank, Facundo Abrahá, Sergio L. Schmukler and Tessada, Jose "Robo-Advisors: Investing through Machines" Research & Policy Briefs no. 21 (2019), <https://documents1.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisors-Investing-through-Machines.pdf>

462 הבורסה מפקחת על כל חברי הבורסה בהיבטים של עמידה וציות לכללי מסחר. חברי בורסה שהם תאגידים בנקאיים מפוקחים גם על-ידי המפקח על הבנקים בבנק ישראל.

463 בשנת 2010 נעשה ניסיון ראשון לאסדרת תחום הברוקראז' בישראל, בדומה לאסדרה במדינות העולם המערבי. בשנת 2020 פורסם תזכיר חוק ניירות ערך (הסדרת פעילות ברוקר דילר), התשפ"א-2020, אך הוא לא קודם מעבר לכך. ראו גם רשות ניירות ערך ורשות התחרות "תחרות בשוק הברוקראז' הקמעונאי" (אוגוסט 2019), בעמ' 27–29, בדבר החשיבות של קידום האסדרה האמורה, https://www.gov.il/BlobFolder/reports/marketresearch-brokeragefinal/he/marketresearch_%D7%AA%D7%97%D7%A8%D7%95%D7%AA%20%D7%91%D7%A9%D7%95%D7%A7%20%D7%94%D7%91%D7%A8%D7%95%D7%A7%D7%A8%D7%90%D7%96%20.%D7%94%D7%A7%D7%9E%D7%A2%D7%95%D7%A0%D7%90%D7%99%200819.pdf

חדשים לתחום ועידוד התחרות והחדשנות, והבטחה כי הגופים הפועלים בתחום עומדים בסטנדרטים מקובלים של פיקוח.

שיקולים אלה חורגים ממסגרת הדיון בדוח זה. בהקשר של בינה מלאכותית, בולט כפי שצוין לעיל הקשר בין התחומים, והצורך להסדיר גם את תחום שירותי המסחר כדי למנוע פער רגולטורי. לשם המחשה: קיים סיכון כי ייעוץ השקעות תוך שימוש בבינה מלאכותית יוביל להתממשות ניגודי עניינים, תוך הטיית לקוחות לבצע פעולות באופן המגדיל את עמלות המסחר. אפשר לטפל בסיכון זה באמצעות האסדרה החלה על ייעוץ השקעות. ואולם סיכון דומה קיים גם ביחס לפלטפורמות מסחר, באופן שפעילות הפלטפורמות תוך שימוש בבינה מלאכותית תוביל להתממשות ניגודי עניינים, תוך הטיית לקוחות לבצע פעולות באופן המגדיל את עמלות המסחר. אסדרה להתמודדות עם סיכון זה צריכה להיות בשני המישורים.

לאור האמור, יש חשיבות בהשלמת מקטע הפיקוח האמור, על מנת שניתן יהיה לטפל באופן דומה ביישומי בינה מלאכותית הנוגעים לפעילות בניירות ערך.

במסגרת הערות הציבור לדוח הביניים התקבלו התייחסויות ספורות בנוגע למגמות ולסיכונים שתוארו לעיל. הצוות סבר שאין בהן כדי לשנות את האמור בדוח, לרבות ההמלצות בנוגע לתחום פעילות זה.



סיכום ההמלצות בנוגע לפעילות ייעוץ השקעות וניהול תיקים:

1. עידוד אקטיבי של הטמעת טכנולוגיית בינה מלאכותית בקרב בעלי רישיון ייעוץ השקעות וניהול תיקים במטרה להגדיל את מספר הלקוחות המקבלים שירותים אלה. זאת בין היתר באמצעות פעולה פרטנית מול שחקנים קיימים ופוטנציאליים, פרסום מדריך המעודד ומסביר כיצד לבצע את השירות, ונקיטת אמצעים נוספים לקידום ודאות רגולטורית וחדשנות.
2. עדכון הוראת שירותים מקוונים. מוצע לשקול הוספת פרק להוראה שיעסוק בטכנולוגיית בינה מלאכותית עכשווית, להבהיר עוד מהם תפקידם של בעל הרישיון הממונה (האחראי למתן השירותים הטכנולוגיים), לשקול התייחסות למערכות בינה מלאכותית שאינן מופעלות בממשקים עם הלקוח, ולשקול התייחסות לשימוש בצ'אט-בוטים.
3. בחינת פעילות של צ'אט-בוטים בייעוץ השקעות וניהול תיקים והרגולציה שצריכה לחול בעניינה.
4. הבהרת הדין ביחס למערכות כלליות של בינה מלאכותית.
5. קידום מחקר לבחינת התנהלות לקוחות מול מערכות ממוחשבות. עריכת מחקר בנוגע להתנהלות לקוחות המשתמשים במערכות בינה מלאכותית וקבלת החלטות אוטומטית נדרש לשם פיתוח השוק, הבנת ההשפעה של הטכנולוגיה על התנהגות המשקיעים, והערכת הרגולציה הקיימת והנדרשת לגבי הפעילות.
6. הסדרת תחום שירותי המסחר (ברוקראז'). בהינתן הקשר ההדוק בין פעילות ברוקראז' ובין פעילות של ייעוץ השקעות וניהול תיקים, והשימושים הנרחבים שיכולים להיות לבינה מלאכותית בפעילות ברוקראז', יש מקום להסדיר מקטע זה של הפעילות בניירות ערך, כדי שניתן יהיה לקדם את הפעילות ולהסדיר אותה באופן מלא ועקבי.

אשראי במערכת הבנקאית

אחד התחומים בו ישנו פוטנציאל ליישומים משמעותיים של בינה מלאכותית בסקטור הפיננסי הוא תחום האשראי. היישומים של בינה מלאכותית בתחום זה נעים על קשת רחבה של נושאים – איתור צרכים של הלקוח, חיתום אשראי, דירוג אשראי וניהול האשראי באופן שוטף. הנחת המוצא היא כי השימוש בבינה מלאכותית הוא אבולוציה מתבקשת של המודלים הסטטיסטיים הקיימים היום בתחום האשראי.

בפרק זה נתאר בכלליות את תחום האשראי במערכת הבנקאית והאסדרה החולשת עליו, את השימושים האפשריים לשימושי בינה מלאכותית בתחום האשראי במערכת הבנקאית בישראל, נדון בשימושה של הרגולציה הקיימת על שימושים אלה, נעריך מגמות בתחום זה ולבסוף נדון בסוגיות העולות מיישומים אלה וההמלצות לגביהן.

רקע – אשראי

לאשראי חלק חשוב ביצירת תנאים לצמיחה במשק, בין השאר, משום שהאשראי מגדיל את היכולת להקים עסקים חדשים, להרחיב ולהשקיע בעסקים קיימים. כיום נוטל הציבור הרחב הלוואות ממגוון גופים פיננסיים ובהם הבנקים, גופים מוסדיים וחברות כרטיסי אשראי.

ישנן מספר חלוקות המקובלות בעולמות האשראי:

• סוג המלווה:

מקובל להבחין בין אשראי בנקאי לאשראי חוץ בנקאי, דבר המשפיע על סוג המלווה:

אשראי בנקאי – אשראי שניתן ע"י גורם בנקאי (בנקים וחברות כרטיסי אשראי) וכפוף להוראות של המפקח על הבנקים בעניין הכללים והמגבלות על מתן אשראי, הפיקוח והמעקב הנדרשים במהלך חיי ההלוואה וכן הטיפול במקרים בהם הלווה מתקשה לעמוד בהתחייבויותיו.

אשראי חוץ בנקאי – אשראי שניתן ע"י גופים אשר מפוקחים ע"י רשות שוק ההון, ביטוח וחסכון.

• סוג הלווה:

ישנה גם הבחנה בין אשראי צרכני לבין אשראי עסקי, דבר המשפיע על סוג הלווה:

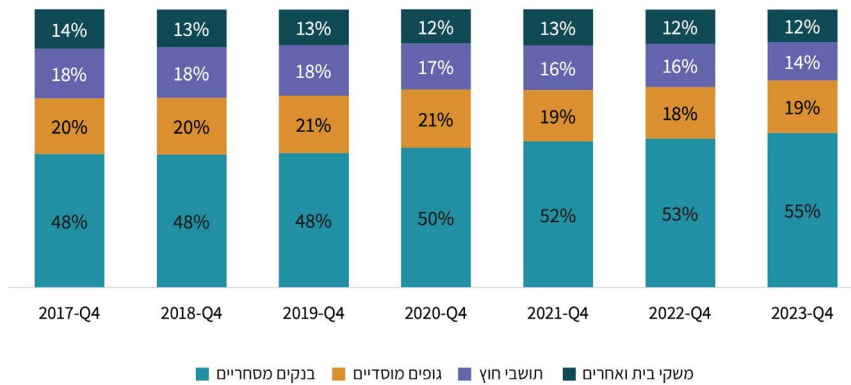
אשראי צרכני – הכוונה למתן אשראי ללקוחות פרטיים. אשראי צרכני מאופיין בהלוואות בסכומים נמוכים יחסית לאנשים פרטיים לטובת צריכה פרטית. האשראי הצרכני נשלט כמעט כולו ע"י הבנקים וחברות כרטיסי האשראי, למרות שבשנים האחרונות קמו אלטרנטיבות בדמות פלטפורמות להלוואות כסף ישירות מאנשים אחרים (P2P) וגופים חוץ בנקאיים שמעמידים אשראי צרכני. עד סוף העשור הראשון של המאה ה-21, נשלט גם האשראי העסקי בידי המערכת הבנקאית, אך בעקבות מהלכים שונים בשווקים הפיננסיים, ניתן לראות פיזור באשראי העסקי בין המערכת הבנקאית לגופים המוסדיים.

אשראי עסקי – מתן אשראי ללקוחות עסקיים לטובת הקמת או פיתוח עסק קיים או חדש. במקרים אלה הלווה הוא במקרים רבים העסק עצמו ולא אדם פרטי.



מערכת הבנקאות הגדילה במהלך שנת 2023 את משקלה בסך המימון למגזר העסקי על חשבון תושבי חוץ

התפלגות החוב של המגזר העסקי, לפי מלווים במערכת הפיננסית, אחוזים | 2023 עד 2017



(1) החברות החוץ-בנקאיות שנכללות בחישוב החל משנת 2019 הינן: אופל בלאנס השקעות בע"מ, אורשי ג.ש. בע"מ, אס.אר. אקורד בע"מ, בול מסחר והשקעות בע"מ, ברקת קפיטל בע"מ, גיבוי אחזקות בע"מ, גמא ניהול וסליקה בע"מ, גמלא - הראל נדל"ן למגורים בע"מ, יונט קרדיט שירותים פיננסיים בע"מ, מיכמן בס"ד בע"מ, מכלול מימון בע"מ, מ.ל.ר. פרויקטים ומסחר בע"מ, מניף - שירותים פיננסיים בע"מ, קבוצת אחים נאוי בע"מ, ערך פיננסים כהלכה בע"מ, פסגות קבוצה, קבוצת פינסולה בע"מ, א.ג. שוהם ביזנס בע"מ, יעקב פיננסים והשקעות בע"מ.
(2) חברות כרטיסי האשראי מעניקות אשראי עסקי בהיקפים מזעריים (פחות מ-0.5% מסך האשראי מסוג זה, ולכן לא צורפו לאיור זה).

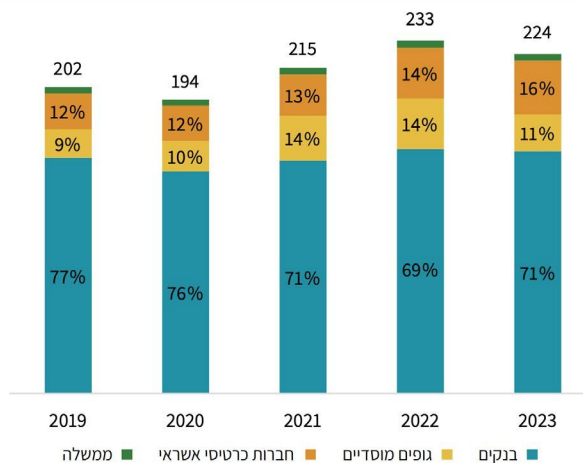
המקור: דיווחים לבנק ישראל, הבורסה לני"ע ועיבודי הפיקוח על הבנקים.

• מטרות האשראי/ההלוואה

אבחנה אחרונה היא בין מטרות האשראי / ההלוואה. כך לדוגמה ניתן למצוא אשראי לדיור אשר ניתן לאחר הליך חיתום ייעודי ולאחר שהגורם המלווה בחן את כושר ההחזר של הלווה ואת שווי הבטוחה, שכן אשראי מסוג זה במרבית המקרים מגובה בשעבוד הנכס הנרכש לטובת הגוף המלווה וניתן לתקופה ארוכה; אשראי לרכב אשר גם הוא מגובה בביטחונות כדוגמת שיעבוד הרכב הנרכש לטובת הגוף המלווה, גם אשראי זה ניתן לתקופה ארוכה, אך בד"כ קצרה מזו של האשראי לדיור. לעומתם אשראי לזמן קצוב או אשראי מתחדש, כדוגמת מסגרת אשראי בחשבון העו"ש או מסגרת כרטיסי אשראי, בדרך כלל איננו מגובה בביטחונות ומתקבל לאחר הליך חיתום הבוחן את כושר ההחזר של הלווה. אשראי זה אינו לזמן קצר ומתחדש מעת לעת. הבחנות אלו בין סוגי האשראי השונים משפיעות, בין היתר על התנאים למתן אשראי: סכום ההלוואה, גובה הריבית ותקופת ההחזר.

ביתר החוב שאינו לדיור של משקי הבית חל צמצום, בעיקר בגופים המוסדיים, בעוד שבקרב חברות כרטיסי האשראי חל גידול קל

התפלגות יתרות החוב שאינו לדיור¹ של משקי הבית לפי מקורות, דצמבר 2019 עד דצמבר 2023 | אחוזים | מיליארדי ש"ח



(1) יתרת החוב בבנקים כוללת גם את האשראי שניתן במסגרת הלוואה לכל מטרה בביטחון דירת מגורים ואשראי שהינו באחריות או בערבות הבנקים. לא כולל אשראי מתושבי חוץ, עקב היעדר נתונים. בחישוב זה לא נכלל האשראי שניתן על ידי מקורות חוץ-בנקאיים שאינם מוסדיים או חברות כרטיסי אשראי.

המקור: דוחות כספיים לציבור, דיווחים לפיקוח על הבנקים ועיבודי הפיקוח על הבנקים.

הרגולציה בנושא מתן אשראי

תחום האשראי כפוף לרגולציה נרחבת הקבועה בחיקוקים וכן בהוראות המאסדר, ובעניינו – הוראות ניהול בנקאי תקין הקובעות ומגדירות את הסטנדרטים בתחום ניהול הסיכונים וההגנות הצרכניות.

הרגולציה מסדירה בין השאר את חובות המוסדות הפיננסיים בהתנהלות נאותה כלפי הלקוח, כגון חובות נאמנות וזהירות כלפי הלקוח, איסור הטעיה חובות גילוי כלפי הלקוח וכן באסדרה של תחום דירוג האשראי, לרבות הנתונים שניתן או אסור להביא בחשבון לצורך קביעת הדירוג.

ניהול סיכונים אשראי

ניהול סיכונים נאות מבוסס על שלושה קווי הגנה: קווי עסקים, פונקציית ניהול סיכונים בלתי תלויה וביקורת פנימית. בכל אחת מההוראות של הפיקוח על הבנקים בנושא ניהול סיכון אשראי ישנה התייחסות לממשל התאגידי, תיאבון הסיכון, מסגרת ניהול הסיכונים, מדידת הסיכון, ניטור והערכתו.

סיכון אשראי הוא הסיכון שלווה, או צד נגדי של מלווה, לא יעמוד בהתחייבויותיו ולא יפרע את חובותיו כפי שנקבע בהסכם, וכתוצאה מכך למלווה יגרם הפסד. המלווים מנסים להעריך את הסיכון הכרוך בכל חוב, לפי נתוני הלווה והשוק. הערכת הסיכון מאפשרת להם לקבל החלטות שונות, כמו האם לאשר חוב מסוים או לסרב לו, להגדיר את התנאים במהלך חיי האשראי (covenants) שיכולים להביא לעצירת האשראי (call) וכן את שאר התנאים המגדירים אותו: תקופת פירעון, גובה הריבית, תצורת ההחזר וכו'. הערכה של סיכון אשראי כרוכה באומדן של ההסתברות לכשל של צד נגדי (PD) והן של החשיפה או ההשלכה הפיננסית על הארגון של אירוע הכשל (LGD). מלווים רבים משתמשים במודלים של סיכונים אשראי כדי לדרג את הסיכון של לקוחות קיימים ולקוחות פוטנציאליים. ניהול סיכונים אשראי נעשה הן לפני מתן האשראי ללקוח, כאשר בוחנים את טיבו, והן במהלך חיי האשראי (התנהגות הלווה).

המאסדר מגדיר בהוראותיו באופן ספציפי את שיטות העבודה לניהול סיכון אשראי. כך, הוראות הפיקוח על הבנקים מתייחסות לתחומים הבאים: יצירת סביבת סיכון נאותה (קביעת תיאבון סיכון ומדיניות אשראי), הגדרת תהליך אישור האשראי, קביעת תהליכים נאותים ועדכניים לתפעול אשראי, מדידה, מעקב ופיקוח והבטחת בקורות הולמות על סיכון האשראי, וכן תהליכים לניהול חובות בעייתיים והסדרת חובות בקשיים.

מחיר האשראי או גובה הריבית הם תשובה לשאלה עד כמה "מסוכן" למלווה להלוות ללווה כסף, או במילים אחרות, מה הסיכוי שכספי המלווה יוחזרו במלואם ובמועד שנקבע. המלווה נמצא בחוסר ודאות מסוים לגבי היכולת של הלווה להחזיר את ההלוואה, והריבית (מעבר לריבית השוק) מהווה מנגנון פיצוי על הסיכון שהוא לוקח. שיעורי הריבית, תלויים בגורמים שונים, בהתאם לסוג ההלוואה ולמאפיינים האישיים של הלווה.

• **מאפייני הלווה:** מאפייני הלווה נועדו להעריך את הסיכון של הלווה הספציפי – האם הוא צפוי לעמוד בהתחייבות ולהחזיר את ההלוואה. הדרך המקובלת בשוק האשראי להעריך אם לווה מסוים יחזיר הלוואה מבוססת על ההתנהגות של אותו לווה במקרים דומים בעבר – אם ישנן עדויות לכך שלקוח מקפיד לשלם כל התחייבות בזמן במשך תקופה ארוכה, סביר מאוד להניח שהוא ימשיך להחזיר הלוואות באותו אופן והדבר ישפיע על תנאי ההלוואה. יצוין, כי מתן אשראי כפוף לחוק איסור הפליה (כמפורט בפרק הטיה ואפליה לעיל) ועל כן ישנם גם מאפיינים שאסור להביא בחשבון בעת ההחלטה על מתן אשראי ותנאיו.

• **משך ההלוואה:** הלוואה לטווח ארוך תהיה "יקרה" יותר, לנוכח הסיכון שמשוה ישתבש עם הזמן.

• **בטוחות:** אם יש נכס המשמש כבטוחה להלוואה, מחיר ההלוואה צפוי להיות זול יותר כי במקרה שללווה לא יהיה כסף לשלם, ניתן יהיה לממש את הנכס ובכסף שיתקבל לפרוע את ההלוואה.

הגנות צרכניות

החקיקה וההוראות הפיקוח על הבנקים מטילים על הגופים המפוקחים חובת גילוי ושקיפות ללקוח על תנאי האשראי. כמו כן, ישנה דרישה מהגוף המפוקח, כי תהיה התאמה בין מאפייני האשראי המוצע ללקוח לבין מטרת האשראי ויכולותיו הפיננסיות של הלווה לעמוד בהתחייבויותיו. זאת ועוד, כדי לוודא התנהלות הוגנת של הגופים המפוקחים בשיווק אשראי צרכני, נכנסה לתוקף הוראה ספציפית בנושא שיווק אשראי צרכני במרץ 2024. בהוראה זו מודגש כי התנהגות שאינה עולה בקנה אחד עם כללי ההוראה מהווה אף היא סיכון מסוים למוסד הפיננסי.

ההוראה קובעת חמישה עקרונות צרכניים עיקריים שתכליתם להבטיח התנהלות הוגנת מצד התאגידים בנקאיים:

• **חובה לנהל שיחות שיווק בהגינות:** ההוראה אוסרת על שיווק אגרסיבי ועל הפעלת לחץ על לקוחות לקבל החלטה להתקשר בעסקת אשראי.

• **חובה להתאים את שירות האשראי לצרכי ויכולות הלקוח** – על הגופים המפוקחים חלה החובה לתת שירותי

אשראי באופן אחראי למניעת מינוף יתר של משקי בית. חובה נוספת היא לוודא התאמה בין מאפייני האשראי המוצע ללקוח לבין מטרת האשראי וצרכי הלווה. בהתאם לכך, חל איסור על גופים מפוקחים ליזום ולשווק שירות אשראי מבלי לברר את צרכי הלקוח.

- **חובת תמחור הוגן** – ההוראה מחייבת את הגופים המפוקחים לתמחר אשראי צרכני באופן הוגן, בין היתר, בעקביות עם רמת הסיכון של הלווה ומאפייניו. בהתאם להוראות הפיקוח על הבנקים, רמת הסיכון של כל לקוח נקבעת באופן עצמאי על ידי הגופים המפוקחים, באמצעות מודלים שהם פיתחו. לצורך הערכת הסיכון של הלקוח רשאי הבנק להשתמש לא רק בתבחינים הקבועים במודל, אלא גם "במידע רך" על הלקוח, כמו מידע שטרם בא לידי ביטוי בנתונים כמותיים בדבר הרעה צפויה במצב הכלכלי של הלקוח. ההוראה דורשת לקבוע במסמכי מדיניות האשראי הצרכני קווים מנחים לתמחור הוגן ועל בסיס זה נדרשו הגופים המפוקחים לגבש וליישם מתודולוגיה לתמחור תואם סיכון. יצוין, כי המתאם בין רמת הסיכון לבין שיעור הריבית צריך שיתקיים גם ברמת הלקוח הבודד ולא רק ברמת תיק האשראי הכולל של הבנק.
- **חובות גילוי מוגברות** – ההוראה מוסיפה חובות גילוי מעבר לאלה שקבועות בחקיקה הרלבנטית (אשראי הוגן, חוק הבנקאות (שירות ללקוח)) ובכללי הגילוי הנאות הרגילים שחלים על הגופים המפוקחים. בין השאר, נקבעו כללי גילוי של מידע רלבנטי בתהליך שיחות השיווק – גילוי מטרת השיחה, פרטי ההלוואה המוצעת וכדומה.
- **צמצום תדירות הפניות היזומות והסרת שמות מרשימות השיווק.**

הוראה נוספת עוסקת ב**ניהול סיכוני מודל** – בחודש אוגוסט 2024 פרסם הפיקוח על הבנקים הוראת ניהול בנקאי תקין 369 בנושא ניהול סיכוני מודלים, במטרה לחזק את אופן ניהול סיכונים אלו במערכת הבנקאית, האמור בהוראה זו חל גם על מודלים הכוללים שימוש או התבססות על בינה מלאכותית. ההוראה מבוססת על אסדרה של הרגולטורים האמריקאים (ה-OCC וה-FED) הנחשבת למובילה בתחום. ההוראה מתארת את ההיבטים העיקריים של ניהול אפקטיבי של סיכוני מודלים. פיתוח, יישום ושימוש הולמים במודלים, כמו גם תיקוף קפדני של מודלים מהווים מרכיבים חיוניים בניהול סיכוני מודלים. ניהול סיכוני מודלים כולל גם מנגנוני ממשל תאגידי ובקרה, כגון פיקוח מצד הדירקטוריון וההנהלה הבכירה, מדיניות ונהלים, בקורות וציות וכן מבנה ארגוני מתאים ומערך תמריצים (incentives) נאות. תאגיד בנקאי נדרש לנהל את סיכוני מודלי בינה מלאכותית על בסיס הדרישות בהוראה זו, תוך מתן דגש להיבטים של: מהימנות והוגנות המודלים בהיבטי הטיה או אפליה; אחריותיות (accountability) שמותאמת למודלי בינה מלאכותית בשים לב למידה ולאופן שבו מתקיימת מעורבות אנושית; עיצוב הבקורות במנגנוני קבלת ההחלטות על בסיס מודלים אלו; שקיפות (transparency), בדגש על יכולת הסבר לתוצאות המושגות, תיעוד מקיף לרכיבי השונים של המודל, וגילוי נאות כך שלא ייגרעו זכויות של המושפעים מהמודל לקבל מידע, לערער על התוצאות וכדומה.

תהליך העמדת אשראי

בחלק זה נסקור את השלבים השונים בתהליך העמדת אשראי ולאחר מכן נסקור כיצד הבינה המלאכותית עשויה להשתלב בכל אחד מהשלבים הללו.

• איתור צרכים

הצורך באשראי יכול להתעורר בצד הלקוח, שפונה לגוף המלווה ומבקש הלוואה, ע"י פניה יזומה של הגוף הפיננסי ללווה בהצעה לקבלת הלוואה או באמצעות צד ג' שעוזר ללקוח להתנהל פיננסית ומציע לו לקחת אשראי. פעילות איתור הצרכים מהווה חלק מרכזי בהבנת הלקוח וביצירת חווית משתמש מותאמת אישית. הבנקאות הפתוחה מאפשרת שיתוף במידע הפיננסי, שעל בסיס המידע הנצבר ניתן לאתר צרכים של לקוחות.⁴⁶⁴ דרך מידע המגיע ממערכות פיננסיות פתוחות יכול הגוף המלווה או צד ג' לנתח את פעולות הלקוחות ולזהות את הצרכים שלהם בצורה יעילה יותר ולהציע מוצרים ושירותים מותאמים אישית. לדוגמה: לקוח שרוכש כרטיס טיסה באמצעות כרטיס אשראי, הגוף המלווה או צד ג' מאתרים את הצורך במימון טיול זה ומציעים ללקוח אשראי לצורך זה.

• חיתום האשראי

בשלב זה המלווה יאסוף מידע על מבקש האשראי, כדי להעריך את כושר ההחזר של מבקש האשראי. לצורך כך

464 חוק שירות מידע פיננסי, התשפ"ב-2021.

יבחן את היסטוריית האשראי שלו, יקבל את דירוג מבקש האשראי שמתקבל מלשכות האשראי, יאסוף מידע פיננסי רלוונטי על מבקש האשראי, לרבות באמצעות הבנקאות הפתוחה. בהתבסס על המידע שנאסף, המלווה ינתח את סיכון האשראי של המבקש. ניתוח זה מסייע למלווה להעריך את ההסתברות לכך שהמבקש לא יעמוד בהתחייבויותיו ויתקשה להחזיר את האשראי כפי שהוסכם. הערכת הסיכון של המבקש שמתקבלת בשלב זה, מאפשרת למלווה לקבל החלטה האם לאשר או לדחות את בקשת האשראי. במקרים בהם החליט המלווה לאשר את הבקשה מתקבלת גם החלטה באשר לתנאי ההלוואה, לדוגמה, גובה הריבית, סכום ההלוואה המאושר ותקופת ההחזר.

• הצעת האשראי על ידי המלווה

המלווה חוזר למבקש האשראי ומציע הצעה הכוללת את התנאים והמגבלות של האשראי. במקרים בהם המלווה מחליט שלא להעמיד את האשראי לאור הערכת הסיכונים שביצע, עליו ליידע את מבקש האשראי.

• שלב קבלת ההצעה על ידי מבקש האשראי

כאשר הלווה מסכים להצעת המלווה הוא חותם על הסכם ומתחייב לעמוד בתנאים כפי שהוגדרו.

• העברת הכסף

לאחר שההצעה התקבלה, המלווה יעביר את הכספים ללווה בין בתשלום חד פעמי בין במתן מסגרת אשראי, בהתאם לסוג האשראי שניתן.

• ניטור וניהול

במהלך חיי ההלוואה, הלווה אחראי להחזר האשראי על פי תנאי ההסכם, בדרך כלל זה כרוך בביצוע תשלומים של הקרן והריבית במועדים קבועים. לאורך כל תקופת האשראי, המלווה עוקב אחר מצב האשראי של הלווה ואחר ביצוע ההחזרים, פעולות אלו מסייעות למלווה לנהל את סיכון האשראי ולנקוט בפעולות מול הלווה אם האחרון לא עומד בהתחייבויותיו. בנוסף למעקב הפרטני של כל הלוואה, המלווה נדרש לביצוע בקורות וניטור שוטף של תיק האשראי שלו ולדווח להנהלה הבכירה ולדירקטוריון מדי תקופה (וזאת בהתאם לנהלי הגוף המלווה ולהנחיות הרגולטור). בנוסף, ישנה סדרה של הוראות המנחות את המלווים לגבי איתור, סיווג וגילוי של חובות בקשיים, כלומר חובות אשר הלווה מתקשה לעמוד בהחזר התשלומים שנקבע בהסכם. כללים אלו מסדירים הן את הגילוי ללקוח והן את הגילוי בדוחות הכספיים של המלווה וכן את האופן בו מצופה מהלווה לפעול כדי למצות את הליך הגבייה.

• סגירה ודיווח

לאחר החזר האשראי במלואו, חשבון ההלוואה אצל המלווה נסגר, והמלווה מדווח ללשכת האשראי על היסטוריית ההחזרים החיובית של הלווה, מה שיכול לסייע בשיפור ניקוד האשראי של הלווה.

שימושי בינה מלאכותית בתהליך העמדת אשראי

השימושים האפשריים בבינה מלאכותית לאורך השלבים השונים מהעמדת האשראי ועד פירעונו הסופי הם מגוונים ומצויים הן בצד התפעולי (back-office) והן בממשק מול הלקוחות. לשימושים אלו יש את היכולת להגביר את היעילות התפעולית של הבנקים, לשפר את ניהול הסיכונים וכן שירות הלקוחות:

איתור צרכי לקוח – איתור הצרכים מתבצע על בסיס מידע רחב ואישי של הלקוח (מידע המגיע מהנתונים הקיימים אצל הגוף הפיננסי או נאסף על ידי הגוף הפיננסי באמצעות בנקאות פתוחה). אנו מעריכים שבשימוש זה נראה התקדמות בזמן הקרוב. בינה מלאכותית יכולה להשתלב בתהליך איתור הצרכים שכן היא משמשת לניתוח מקיף של נתונים פיננסיים והתנהלות כלכלית של הלקוחות, כולל זיהוי תבניות ושימוש במודלים חכמים לזיהוי צרכים. באמצעות זיהוי אוטומטי של אופני ההתנהגות והסיכונים, בינה מלאכותית יכולה להציע המלצות אוטומטיות והתאמת ההצעה הפיננסית לצרכי הלקוח.

בנושא אשראי צרכני קיים מתח מובנה בין הרצון לפרסונליזציה, כלומר התאמת המוצר הספציפי ללקוח הקצה, לבין החשש מהדרה משוק האשראי. שימוש בכלי בינה מלאכותית עשויים אמנם לשפר מאוד את היכולות של המלווים לזהות בזמן אמת את הצורך של לווה ספציפי ולהציע לו אשראי מותאם אישית, אך באותה מידה הוא עשוי לגרום להדרה של אוכלוסיות מסוימות, לדוגמה אוכלוסיות שהן פחות דיגיטליות וכך היעדר המידע "הדיגיטלי" בעניין עלול לפעול לרעתן (למשל, לקוחות שעיקר הפעילות שלהם במזומן או שאינם משתפים מידע במסגרת הבנקאות הפתוחה).

חיתום אשראי – הליך חיתום מחייב שימוש במידע רב. ליכולות הניתוח של הבינה המלאכותית הפוטנציאל לסייע לנתח כמויות גדולות יותר של נתונים, לרבות מידע אישי והיסטורית אשראי, ובכך לסייע ביצירת תמונה מקיפה

ומדויקת של יכולת החזר הלוואה של הלקוח בצורה יעילה ואוטומטית. בעולם גם ידועים שימושי בינה מלאכותית לצורך הערכת בטוחות בהליך החיתום. דבר זה משתלב עם הוראות הפיקוח על הבנקים בנושא דירוג אשראי וטיוטת ההוראה בנושא ניהול סיכונים מודל הקובעים סטנדרט שלפיו על התאגיד הבנקאי לזהות את הסיכונים הגלומים במודל לאורך חיי האשראי.

חרף הפוטנציאל של הבינה המלאכותית בשלב זה, אנו מעריכים כי התאגידים הבנקאיים לא יעשו שימוש בבינה מלאכותית בטווח הקרוב לצורך הליכי חיתום אוטומטיים ואוטונומיים, זאת מכמה סיבות: תיאבון הסיכון של התאגידים הבנקאיים; הדרישות הרגולטוריות; הניסיון הקיים של התאגידים הבנקאיים בשימוש במודלים סטטיסטיים כמו גם הדומיננטיות שלהם בשוק האשראי הצרכני; רמת הכלה פיננסית גבוהה בארץ; וחקיקת חוק מאגר נתוני אשראי.

ממצא דומה עולה גם מדוח שפורסמה לאחרונה ועדת באזל ממנו עולה כי הבנקים משתמשים בבינה מלאכותית בזהירות בשלב זה, ונעשה שימוש במודלי בינה מלאכותית לצורך השוואה או ביסוס החלטות אנושיות (ולא לצורך העברת תהליכים וקבלת החלטות למסלולים אוטומטיים ואוטונומיים). בין היתר מוסבר, כי אחד הגורמים לכך הוא אי ודאות רגולטורית ומשפטית ביחס לציפיות לגבי אחריותיות, אתיקה, פרטיות נתונים, הוגנות, שקיפות והסבריות, זאת בפרט ביחס לשימושים עם השלכות צרכניות.

הצעת אשראי ע"י המלווה – בעתיד נראה כי ניתן יהיה לשלב בינה מלאכותית גם בשלב זה על-ידי פיתוח חוויות משתמש משופרות באמצעות יישומי מחשב, צ'אט-בוטים ועוזרים וירטואליים. אנו מעריכים כי בעת הזו לא יעשה שימוש בכלים אלו ישירות מול הלקוחות בין השאר, לנוכח אתגרים מתחום האחריות, הגילוי, ההגנה על המידע והאתיקה אשר נדונו בפרקים הקודמים. יחד עם זאת, סביר כי בשלב הראשון יתרבו הפיתוחים של כלי עזר פנימיים שמטרתם לעזור לעובדי התאגיד הפיננסי לנווט במערכות הפנימיות ולהגיב לשאלות הקשורות לנושאים שונים בהם גם נושאים פנים ארגוניים. באשר למודלים של בינה מלאכותית יוצרת, השימוש של הבנקים מוגבל במיוחד עבור שירותים מול לקוחות ובפעילות המוגדרת על ידם כפעילות בסיכון גבוה. עם זאת חלק מהבנקים בוחנים או מבצעים פיילוטם של יישומים באופן פנימי כדי לשפר את היעילות התפעולית.⁴⁶⁵

ניטור התנהגות הלווה ואיתור מוקדם של כשלי אשראי – דיוק ועקביות גדולים יותר בעיבוד בהשוואה למעקב ידני או מבוסס חוקים יכול לסייע בזיהוי חריגות ובניטור פעולות חריגות אשר יסייעו באיתור טיפולוגיות של פעולות החשודות כהלבנת הון ומימון טרור. בנוסף, יכולות מתקדמות מאפשרות לחברות טכנולוגיות להציע שירותים של ניתוח התנהגות פיננסית של לקוחות בטרם נקלעו לקשיים פיננסיים ולהציע פתרונות שיכולים לסייע בשלבים מוקדמים דבר אשר יכול לסייע גם בשיקום מהיר של הלווה.

סוגיות הנובעות משימוש בבינה מלאכותית

הסוגיות שנדונו בדוח זה ביחס לשימושי בינה מלאכותית בתחום הפיננסי באופן כללי רלוונטיות ברובן המוחלט גם לשימושים בתחום האשראי. כך, למשל, ככל שייעשה שימוש בבינה מלאכותית יוצרת לצורך תקשורת עם לקוחות, תתעורר שאלת הגילוי ביחס לכך לשימוש במערכת זו. ככל שייעשה שימוש במערכות שהן "קופסה שחורה" לצורך חיתום אשראי או ניטור, תתעורר שאלת ההסבריות. מעבר לסוגיות הכלליות שנדונו לגבי בינה מלאכותית בפרקים הקודמים, ישנן גם סוגיות ממוקדות העולות משימוש בבינה מלאכותית לאורך חיי האשראי. חלקן קשורות לסוגיות שנדונו בפרקים קודמים בדוח אך נודעת להן חשיבות נוספת כאשר מדובר באשראי – הן לנוכח חשיבותו של שירות זה, הן לנוכח הרגולציה הייחודית בתחום.⁴⁶⁶

- **הדרה מתחום האשראי** – כאמור, שימוש בבינה מלאכותית לצורך הערכת סיכון של אי פירעון הלוואה עשויה לשפר את דיוק התחזיות בעניין זה. יש לכך יתרונות ברורים: הערכת סיכון מדויקת תסייע בניהול הסיכונים של הבנק. כמו כן, יש בכך לסייע בעמידה בחובה הרגולטורית להתאים את ההלוואה לצרכיו ויכולותיו של הלקוח. לצד זאת, פרסונליזציה עלולה גם להביא להדרה משוק האשראי בשל דחיית בקשת הלוואות או ייקורן. במקרים כאלה עלול להתעורר חשש לאפליית מחירים בכלל וכלפי אוכלוסיות בעלי מאפיינים מוגנים בפרט.⁴⁶⁷
- **אפליה** – גם אם הרגולציה מסדירה את סוג המידע שבו ניתן לעשות שימוש לצורך דירוג אשראי או חיתום הלווה, למערכות בינה מלאכותית ישנה יכולת הסקה ממשנתנים שאינם ישירים ("פרוקסי") והדבר עלול להשליך

⁴⁶⁵ Digitalization of finance, Basel Committee on Banking Supervision, May 2024, בעמ' 8.

⁴⁶⁶ בהקשר זה, ראו EU AI Act וההתייחסות לאשראי כאל תחום בסיכון גבוה המצדיק כללים רחבים יותר.

⁴⁶⁷ דוח אונ' תל-אביב, בעמ' 19.

על החלטות במתן האשראי או אי מתן האשראי, הן במחיר והן בטיפול בלווה לאורך חיי הלוואה (ראו פירוט בפרק הטיה ואפליה לעיל).

- **חשש מפני דחיפת אשראי** – בינה מלאכותית עשויה לשפר ולייעל את פעילות הגופים הבנקאים ובכלל זה לאתר צרכי אשראי אצל לקוחות בצורה מהירה ומדויקת יותר, לחסוך בכוח אדם לצורך שיווק הלוואות וכדומה. לצד היתרונות הגלומים בכך, ישנו גם חשש שהדבר יוביל לשיווק אגרסיבי יותר של אשראי לציבור בכלל ולציבור בעל מאפיינים רגישים בפרט.

- **חשש ליציבות המערכת הפיננסית** – בין השאר, עולה חשש לסיכוני "הידבקות מערכתית" שעלולה להתרחש מקום בו ישנו שימוש של מספר גופים מרכזיים באותו אלגוריתם או אלגוריתמים דומים, למשל, לבניית מודל לסיכוני אשראי ובמקרה של תקלה או טעות ההשפעה על המערכת הפיננסית עלולה לערער את יציבות המערכת (ראו פירוט בפרק יציבות פיננסית לעיל).

במסגרת הערות הציבור לדוח הביניים לא התקבלו התייחסויות ספציפיות לפרק זה, למעט הערה לפיה החששות הנוגעים לדחיפת אשראי אינם ייחודיים לבינה מלאכותית. מטרת הצוות בהקשר זה היתה לשקף סיכונים הצפויים להתעצם באופן מיוחד לנוכח שימוש בבינה מלאכותית, ולכן לא נערך תיקון בהקשר זה.



המלצות בנוגע לאשראי במערכת הבנקאית

- **כללי:** כאמור לעיל, הסוגיות הכלליות שנדונו בדוח זה נוגעות גם לתחום האשראי ומכאן שההמלצות הכלליות בפרקים הקודמים רלוונטיים גם לתחום האשראי לרבות בתחום האפליה. בפרט יש להתייחס להמלצות בדבר התאמת הכלים הרגולטורים לסיכונים הייחודיים לכל שימוש ושימוש בבינה מלאכותית (ראו פרק ראייה כוללת ומבוססת סיכונים לעיל).

- **שימוש באסדרה הקיימת לניהול סיכונים והגנות צרכניות:** בדומה לאמור בפרק העקרונות המנחים לטיפול בבינה מלאכותית בסקטור הפיננסי, אנו סבורים כי ככל שניתן לעשות שימוש באסדרה הקיימת כדי להתמודד עם אתגרי הבינה המלאכותית יש לדבוק בכך כדי לא לייצר רגולציה ייחודית ומגבילה, וכדי לא לעכב את הפיתוח של הבינה המלאכותית ואת אימוצה על ידי הגופים הפיננסיים. יחד עם זאת, אנו ערים לסוגיות המתעוררות אגב שימוש בטכנולוגיה החדשה ולצורך להבהיר את תחולת הדין הקיים על הגופים הפיננסיים בהקשרי בינה מלאכותית כדי לספק ודאות לשוק בהיבטים שנמנו לעיל (ראו האמור לעיל בדבר אי-ודאות רגולטורית כחסם אפשרי מפני שילוב בינה מלאכותית בפעילות הגופים הפיננסיים).

כאמור לעיל, תחום האשראי מבוסס במידה רבה על ניהול סיכונים שמבוצע על ידי המוסד הפיננסי, בכפוף להוראות המאסדר בעניין זה.

ראשית, אנו סבורים כי יש להמשיך בגישת ניהול הסיכונים גם כאשר ישנה מעורבות של בינה מלאכותית בכל אחד משלבי מתן האשראי והפיקוח עליו. **הגופים הפיננסיים, בבואם לאמץ יישומים של בינה מלאכותית, נדרשים ליישם עקרונות של ניהול סיכונים והגנה על הלקוח, בהתאמה להיקף השימוש שלהם ביישומי בינה מלאכותית ולרמת הסיכון שיישומים אלו משיתים.**

שנית, באשר להסדרים הפרטניים החלים על ניהול סיכונים – ניתוח הרגולציה הקיימת מעלה כי זו מתאימה ברובה ליישומי בינה מלאכותית המיושמים כבר היום וגם לאלו המתוכננים לעתיד הקרוב. ההוראות הקיימות בדבר הגנות צרכניות, ניהול סיכונים וניהול מודלים, לא יוצרות חסמים לשילוב בינה מלאכותית בתחום מחד, ומעניקות מעטפת אסדרתית מספקת ככל שיעשה שימוש בכלים אלה. כך, למשל, החובה לשיווק הוגן תחול בין שאדם יפנה ללקוח ובין שיעשה שימוש בבינה מלאכותית יוצרת לאותה מטרה. החובה לתמחור הוגן ומתאים רלוונטית גם למקרה שבו יעשה שימוש בבינה מלאכותית בתהליך הערכת הסיכונים של הלווה. עם זאת, ייתכן ויידרשו הבהרות מצד המאסדר ביחס לגורמים מגבירי ומפחיתי סיכון והכלים להתמודד עמם, כפי שמפורט בפרק ראייה כוללת ומבוססת סיכונים לעיל.

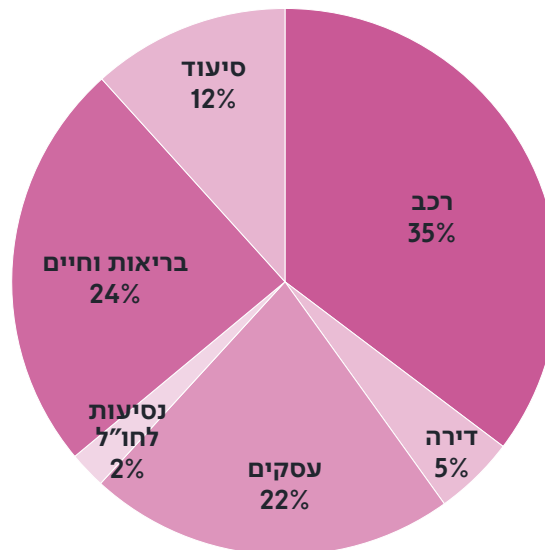
- **ממשל בינה מלאכותית:** כאמור, כבר היום קיימים כללי ממשל בינה מלאכותית, ובכל זאת כללי ממשל תאגידי המתייחסים, בין השאר, לתפקידי הדירקטוריון וההנהלה הבכירה בכל הקשור ליישום טכנולוגיות חדשות ופיתוח מערכות ומודלים. כללים אלה רלוונטיים במרביתם גם למציאות בה נעשה שימוש בבינה מלאכותית. לצד כלים אלה, לא מן הנמנע שיהיה צורך לפתח כלי ממשל לבינה מלאכותית בכלל בהתאם לנדון בפרק ממשל בינה מלאכותית.
- **ממשל נתונים:** כאמור בתת-הפרק העוסק בממשל נתונים, כניסת הבינה המלאכותית לשימוש נרחב מגבירה את התלות בנתונים ולפיכך עלולה לעורר שאלות נוספות באשר להגנה על הנתונים, בחינת מסדי הנתונים בהם נעשה שימוש, שימוש בנתונים חדשניים/אלטרנטיביים לצורך קביעת סיכוני אשראי וכדומה. בהקשר זה נראה כי נדרשת השלמה של המעטפת של הכללים הקיימים על מנת לספק הגנה לציבור על פרטיות הנתונים ולהבטיח כי נעשה שימוש בנתונים רלוונטיים ולא נעשה שימוש בנתונים שעשויים להוביל להדרה או אפליה. הוראות דומות פורסמו ע"י רגולטורים כדוגמת ה-BIS בשנים האחרונות.
- **סיכוני אפליה והדרה – הבהרות לדין הקיים:** האתגרים בתחום האפליה נדונו בהרחבה לעיל בפרק הטיה ואפליה. כמפורט שם, איסור אפליה חל על שירותים פיננסיים מכוח הדין הכללי אך ישנן גם הוראות ספציפיות בתחום, למשל, בכל הנוגע לנתונים שניתן ואסור לשקול לצורך קביעת דירוג אשראי. גם במקרה זה נראה כי יש לשקול הבהרה, כי שימושי בינה מלאכותית אינם משנים מן הדין הקיים ועל המוסדות הפיננסיים להבטיח, בטרם השימוש בכלי בינה מלאכותית, כי יש בידיהם את הכלים להקפיד על האסדרה בתחום – כגון אי שימוש במשתני פרוקסי לנתונים שאסור לשקול לפי חוק נתוני אשראי. בהקשר זה, יש חשיבות גם לשימוש בכלים הנוגעים למעורבות אנושית והסברות שיש עשויים לסייע למוסד הפיננסי להבטיח שהחלטה בנושא אשראי לא הובילה לאפליה.
- **חשש מ"דחיפת אשראי":** הבקרה והגילוי ביחס לשימושי או אינטראקציה עם בינה מלאכותית נדונו בפרק יידוע וגילוי. אך נראה כי כלים אלה עשויים להיות רלוונטיים באופן ספציפי גם לחשש מדחיפת אשראי. מאחר שמדובר בטכנולוגיה חדשנית יחסית, שאין לדעת איך תשפיע על ציבור הצרכנים ועל אופן האינטראקציה עמם, נראה כי יש לשקול שאם נעשה שימוש בבינה מלאכותית בפעולת אינטראקציה שנועדה לשווק אשראי ללקוח, יהיה גילוי בדבר נתון זה. הגילוי גם יאפשר לרגולטור לבחון אם השימוש בבינה מלאכותית הוביל לפרקטיקות המאתגרות את הדין בעניין זה.



חיתום ביטוח

חיתום ביטוח הוא אחד מהיישומים הפוטנציאליים של בינה מלאכותית בתחום הפיננסי. חיתום הוא התהליך שבו חברת הביטוח מעריכה את הסיכון של כיסוי ביטוחי מסוים. הגורמים המרכזיים בהליך החיתום הם בחינת מאפייני הלקוח, מאפייני הכיסוי הביטוחי אותו הוא רוכש, תמחור הפרמיה ומאפייני ביטוח המשנה לאותו כיסוי ביטוחי. תהליך החיתום עצמו כולל פעולה של בחינת הצורך בנקיטה בצעדים כדי שהאיזון בין כל הגורמים לעיל יתקיים כך שהפרמיה תהלו את הסיכון הביטוחי תוך שימוש במודלים אקטואריים, סטטיסטיים ואלגוריתמים. מוצרי הביטוח או הפוליסות מתחלקים לסוגים שונים ולכל אחד מאפיינים משלו וגורמי סיכון משלו. למשל, ביטוח בריאות מכסה סיכונים של מחלות קשות וניתוחים יקרים, ביטוח דירה מכסה נזקים למבנה ולרכוש בתוכו. כתוצאה מכך, לכל מוצר יש מודל חיתום משלו. להלן חלוקה של נתח השוק למוצרי ביטוח בשנת 2023:

סוגי ביטוח על פי נתח שוק



הליך החיתום יכול להיות מחולק לשני תהליכים נפרדים, בניית מודל החיתום הכללי וחיתום הלקוח או העסקה הפרטניים. בינה מלאכותית עשויה להשתלב בכל אחד מן החלקים הללו. להלן תיאור קצר של תהליכי החיתום ומקומות בהם בינה מלאכותית עשויה להשתלב. נדגיש כי לא מדובר בהמלצות או בסקירה של מצב קיים, אלא בסקירה של אפשרויות, חלקן תאורטיות, לפיתוח מערכות בינה מלאכותית.

בניית מודל חיתום כללי וקביעת תנאי החיתום עבור המוצר הביטוחי, כולל זיהוי ואומדן של הסיכונים הנובעים מהכיסויים הביטוחיים המוצעים במוצר. התהליך יכול לכלול זיהוי של קבוצות סיכון על פי גורמי הסיכון השונים דוגמת סוג הרכב או שנת ייצור הרכב בביטוח רכב, או היסטוריה רפואית בביטוח מחלות קשות. חיתום הוא תהליך מורכב בשל ריבוי סוגי המוצרים הביטוחיים. כל סיכון ביטוחי דורש התייחסות ייחודית, גם בהתאם לזמינות המידע או יחוד גורמי הסיכון בו. נוסף לזיהוי הסיכונים, בניית מודל וקביעת תנאי החיתום כוללת גם הערכה של הסיכוי להתממשות הסיכון ואומדן של העלות העולה לבוע מכך. הערכה ואומדן אלה יכולים להיות מבוססים על מאגר נתונים שיש בידי חברת הביטוח וכן על נתונים ממקורות אחרים. כלי בינה מלאכותית, כמו למשל למידת מכונה (ML), עשויים להשתלב בפעולות של ניתוח נתונים אקטואריים ותמחור בזכות יכולות ניתוח עמוק של נתונים רבי-היקף ממגוון מקורות, תוך מציאת קשרים סטטיסטיים ומגמות קיימות אשר יסייעו בזיהוי של סיכונים ואומדן של סיכויי ההתממשות שלהם והיקפם. כלי בינה מלאכותית נוסף העשוי להתאים לשלב זה ולסייע בבניית מאגרי מידע מגוונים הוא כלי עיבוד שפה טבעית (NLP). התבססות על מגוון רחב של נתונים ויכולת לעבר נתונים רבים עשויה להגביר יכולות של איתור וזיהוי של קורלציות בין מגוון רחב של משתנים, מה שעשוי להגדיל את היכולת של חברת הביטוח ליצור קבוצות סיכון קטנות וייחודיות יותר, ולהגדיל את הדיוק של התאמת מחיר ותנאים לפרופיל הספציפי ולצרכים האישיים של כל לקוח. נוסף לכך, שילוב אלגוריתמים מתקדמים של בינה מלאכותית, אשר יזהו ויבחרו את

הפרמטרים המרכזיים לאיסוף המידע, כמו למשל המידע שהלקוח צריך לספק, עשויים לשפר רלוונטיות ויעילות של תהליך החיתום.

חיתום הלקוח או חיתום עסקה הוא התהליך בו בוחנים מאפיינים של לקוח או עסקת ביטוח פוטנציאלית באמצעות מודל החיתום שפותח בשלב הראשון. חיתום הלקוח כולל התייחסות למאפייני הלקוח באופן פרטני, בחינת התאמתו ושיוכו לקבוצות הסיכון והחלטה בנוגע לעסקת הביטוח ולתנאיה. שלב זה דורש מהלקוח הפוטנציאלי למסור מידע רלוונטי ומהימן לסוג הכיסוי הביטוחי, למשל מאפייני מיגון הרכב בביטוח רכב ומאפייני הבניין בביטוח דירה. שילוב בינה מלאכותית בשלב זה עשוי להתבצע דרך ממשק חכם, כגון צ'אטבוט אינטראקטיבי, אשר ינהל את התקשורת הראשונית עם הלקוח ויאסוף מידע ראשוני. נוסף לכך, גם כאן כלי עיבוד שפה טבעית (NLP) יכול לסייע בעיבוד הנתונים המתקבלים מהלקוח. שילוב כלי בינה מלאכותית בחיתום הלקוח עשוי להביא לאיסוף נתונים מרוכז ממקורות מידע שונים, לרבות מקורות מידע אלטרנטיביים כמו התנהלות באינטרנט ולייעל את תהליך חיתום הלקוח. נוסף לכך, בינה מלאכותית עשויה לשמש ככלי עזר בתהליך קבלת ההחלטות אשר יתרונותיו ביכולת התאמה לנתונים ודיוק, וכן כמו כל מודל ממוחשב, בהפעלת משקלות זהות למדדים באופן עקבי בכל תהליך, בלי הטיות אנושיות בשיקול הדעת.

רשות שוק ההון סקרה במחצית השנייה של 2022 את תהליך אימוץ הבינה המלאכותית על-ידי גופים מוסדיים. בסקר השתתפו 20 גופים מוסדיים המייצגים מגוון של שירותים פיננסיים בתחום הביטוח והחיסכון לטווח ארוך וכן רמות שונות של היקף נכסים מנוהלים. נמצא כי מתוך 20 הגופים שהשתתפו בסקר, עשרה כבר עושים שימוש מסוים במודלים של בינה מלאכותית במערכותיהם בתהליכים העסקיים השונים שלהם. נוסף לכך, נמצא כי כלי בינה מלאכותית נוספים נמצאים בפיתוח באותם גופים שכבר עושים שימוש במודלים של בינה מלאכותית וכן במספר גופים שטרם החלו שימוש. ממצאי הסקר מצביעים על שילוב של כלים שונים של בינה מלאכותית בכל שלבי החיתום הביטוחי. הממצאים מעלים כי חברות ביטוח שונות שילבו מודלים של בינה מלאכותית בשלבים שונים של החיתום, וכי המערכות משמשות לבקרה ולתמיכה בקבלת החלטות. ניתן למצוא שימוש בבינה מלאכותית בבזטים לשירות לקוחות, מערכות לניתוח התנהגות מבטחים ובמערכות לתמחור, ניתוח נתונים אקטואריים וביצוע תהליכי הערכת סיכונים לעסקה בודדת. ממצאי סקר השימושים מצביעים על ההשפעה המשמעותית העשויה להיות לבינה מלאכותית על תחום החיתום עם התקדמות הפיתוחים הטכנולוגיים.

סוגיות וסיכונים

שילוב של בינה מלאכותית בהליך חיתום ביטוח עשוי להביא למספר יתרונות, בהם הגדלת ההתאמה של המוצר ללקוח הן בפן הכיסוי הביטוחי והן בפן המחיר; הגברת יכולת זיהוי והערכת הסיכון מצד חברת הביטוח כולל יכולת איתור הונאות, וברמת השוק להגביר נגישות למוצרי ביטוח. נוסף ליתרונות, הטמעת בינה מלאכותית בהליכי חיתום ביטוח מעלה מספר סוגיות, בתוכן סיכונים המאפיינים כבר כיום את הליך החיתום, ועשויים להיות מוגברים בעקבות השימוש בכלי בינה מלאכותית. כלי בינה מלאכותית מתאפיינים בעיבוד כמויות גדולות של מידע, מהירות עיבוד גבוהה ומתן תוצאות מהיר, הסברתיות נמוכה והתבססות על מערכות מידע. מאפיינים אלה משפיעים על הגברה של סיכונים מסוימים בשל שימוש במערכות מבוססות בינה מלאכותית. הסיכונים והסוגיות הכרוכים בשימוש בבינה מלאכותית נדונו בהרחבה בדוח זה. נציג את עיקריהם כאן בקצרה בהקשר של הליך חיתום ביטוח:

פרטיות – השלב הראשון בתהליך החיתום הוא, כאמור, איסוף מידע לצורך יצירת תמונת סיכונים של הלקוח המסוים המבקש לרכוש ביטוח. שילוב בינה מלאכותית בהליך זה עשוי לאפשר איסוף של מידע מפורט יותר, לרבות מידע שאינו בהכרח רלוונטי להערכת הסיכון, וממקורות מידע מגוונים יותר מאשר תהליכים הנערכים באמצעים אחרים. כלומר, כמות המידע הפרטי הנאסף עלולה לגדול משמעותית, בהיקף וכן במגוון, דבר אשר מגדיל את הסיכון לפגיעה בפרטיות, במקרה בו המידע לא יהיה מוגן כראוי.

אפליה – תהליך החיתום במהותו הוא תהליך שמטרתו להבחין בין לקוחות פוטנציאליים שונים על בסיס מאפיינים ייחודיים להם, כגון שווי הרכוש שלהם או מצבם הבריאותי, ועל בסיס מאפיינים אלה להתאים להם את המוצר הביטוחי. מערכות בינה מלאכותית עשויות לסייע בהעלאת רמת הדיוק של תהליך החיתום, בין השאר, על-ידי מציאת קשרים סטטיסטיים בין מאפיינים שהקשר הישיר בינם לבין הסיכון הביטוחי לא היה ידוע. היכולת לאתר קשרים סטטיסטיים שהסבר להם לא תמיד ידוע, עלולה להביא ליצירת קשרים סטטיסטיים בין מאפיינים שלא ניתן או אין הצדקה בהכרח להשתמש בהם בשל חשש לאפליה, ועל בסיס קשר סטטיסטי זה ליצור אפליה.

קופסה שחורה והעדר הסברתיות – אחד היתרונות המרכזיים של בינה מלאכותית הוא היכולת לאתר קשרים סטטיסטיים אשר נראים אקראיים לעין האנושית ואינם מבוססים על קשר ישיר או קשר סיבתי הבהיר אפילו לאנשי

המקצוע בתחום. העדר היכולת להסביר את הקשר בין הנתונים שהוכנסו אל המערכת לבין התוצאות שהיא מציגה עלול לעורר מספר אתגרים בהקשר של הליך החיתום הביטוחי. כפי שנדון מוקדם יותר בדוח זה, היעדר הסברות עשוי להקשות על המבטח בבחינת סבירות תוצאות מודל הבינה המלאכותית ובתיקוף התוצאות, וכן עשויה להקשות על נימוק של החלטה בעניין עסקה מסוימת. הדבר יכול לעורר קושי, למשל אם מדובר בעסקה מהותית למבטח או עסקה בה עלתה שאלה מצד הלקוח. בנוסף, עשוי להידרש הסבר כללי על תוצאות המודל או הסבר פרטני לתוצאה מסוימת על-ידי הרגולטור, על-ידי הציבור או על ידי בית המשפט.

סיכון מודל – מודלים התומכים בקבלת החלטות הם כלי אשר נעשה בו שימוש רב בעולם הפיננסים. הליך חיתום ביטוחי נשען על מודל כמותי-סטטיסטי אשר מספק אומדן להתממשות סיכונים ולעלות הכלכלית במקרה של התממשותם. כאמור, שימוש במודל חיתום ביטוח מורכב משני שלבים. שלב ראשון בו נבנה המודל ועובר בחינת אמינות ותיקוף. בשלב זה נערך שימוש במידע המורכב בדרך כלל מנתוני עבר על התממשות הסיכונים ועל התרחשותם של מקרי ביטוח. קיימים מוצרי ביטוח מסוימים בהם כמות מקרי העבר אינה מספיקה כדי לבסס מסקנה סטטיסטית ואז המודל יכול להתבסס גם על מחקרים מדעיים האומדים את הסיכוי להתממשותו של סיכון מסוים ואת ההשפעה הצפויה שלו, למשל בסיכון רעידת אדמה. שלב שני בשימוש במודל הוא שלב בחינת עסקת ביטוח מסוימת, בשלב זה המודל מקבל מידע על פרטי העסקה ומעבד את המידע אל מול הסיכונים המכוסים בביטוח. תוצאות המודל בשלב הזה משמשות את המבטח בקבלת החלטה אם להתקשר בעסקת הביטוח ועל תנאי העסקה. בין סיכונים המודל המוגברים במודלים של בינה מלאכותית ניתן למנות את סיכון הטעות בשל ההסברות הנמוכה, וסיכונים הקשורים בטיוב הנתונים הנקלטים במודל בשל ריבוי המקורות ומגוון הנתונים הנקלטים.

סיכונים מערכות מידע וסייבר, וסיכונים שרשרת אספקה הם סיכונים מהותיים נוספים המאפיינים שימוש בבינה מלאכותית. מערכות בינה מלאכותית הן למעשה מערכות מחשוב המקושרות למערכות מחשוב אחרות, ומתבססות על כח החישוב, העברת המידע ועוד הנובעות מכך, ובמקביל חשופות לסיכונים האופייניים למערכות מידע ולסייבר. נוסף על כך, פיתוח מערכות בינה מלאכותית נעשה במקרים רבים בשילוב של ספקים חיצוניים, למשל מומחים לתחום המספקים את שירותי פיתוח, או ספקים חיצוניים המתמחים באיסוף מידע והרחבת בסיס הנתונים המשמש את מודל הבינה המלאכותית, ובכך השימוש בבינה מלאכותית יוצר חשיפה גם לסיכונים שרשרת אספקה.

טכנולוגיית בינה מלאכותית נמצאת בשלבי פיתוח ואימוץ ראשוניים בשווקים הפיננסיים והשימוש בה צפוי להמשיך ולהתרחב. שילוב בינה מלאכותית בפעילות הקיימת משמעה כי לצד המאפיינים המשותפים למערכות בינה מלאכותית, יהיו לכל מערכת מאפיינים ייחודיים הקשורים בתהליך העסקי בו היא משולבת. כלומר, ניהול הסיכונים והתמודדות עם הסוגיות שמעלה הבינה המלאכותית יבוצע בעיקרו במסגרות הקיימות לניהול הסיכונים של התהליכים העסקיים הקיימים בגופים הפיננסיים, תוך יצירת התאמה ועדכון לסיכונים המוגברים והסוגיות העולות משימוש בבינה מלאכותית.

כלים להתמודדות עם הסוגיות והסיכונים

דוח זה סוקר בהרחבה כלים להתמודדות עם הסוגיות והסיכונים הנובעים משימוש בבינה מלאכותית. נציג כאן דיון ממוקד בהקשר של הליך חיתום ביטוח.

תהליכי ניהול סיכונים משמעותיים ואיכותיים מהווים חלק בלתי נפרד מניהול התקין של חברת ביטוח ותומכים בניהול זהיר ומושכל של הפעילות הפיננסית והעסקית, באופן שיבטיח בהסתברות גבוהה את השגת מטרותיה ואת יכולתה לקיים את התחייבויותיה לאורך זמן. מסגרת ניהול הסיכונים מקיפה את כל הפעילויות והתהליכים המתקיימים בחברת הביטוח, ולפיכך כניסה של כלי בינה מלאכותית לתהליכים שונים, כמו הליך החיתום הביטוחי, תיערך באופן מובנה בתוך מסגרת ניהול הסיכונים. מסגרת ניהול הסיכונים מתייחסת למעשה לכל הסיכונים והסוגיות העולות מאימוץ טכנולוגיית בינה מלאכותית ומהשילוב שלה בתהליכי העבודה של חברת הביטוח, וכלי ניהול הסיכונים מספקים יכולות של פיתוח מענה לסיכונים והסוגיות, עריכת תוכניות הפחתה לסיכונים במקומות המתאימים לכך, ואימוץ כלי מעקב ובקרה.

ממשל תאגידי, קביעת אחריות ומעורבות אנושית הם כלים להסדרה של אופן ההתנהלות של היחידות העסקיות ובעלי התפקידים השונים בחברת ביטוח. באמצעות כלים אלה ניתן לטפל בסוגיות ובסיכונים שונים. למשל, סוגיית הקופסה השחורה והיעדר הסברות, וכן סוגיית האפליה יכולים להיות מטופלים באמצעות מעורבות אנושית וכן קביעה של מדרג לקבלת החלטות בתוך הממשל התאגידי, כך שהשימוש במערכת בינה מלאכותית ובתוצאות והמידע אותן היא מספקת יהיו תוך הפעלת ביקורת ובחינה של שיקול דעת אנושי. שיקול דעת אנושי מסוגל להבחין

בתוצאות שאינן סבירות ביחס למצב עניינים מסוים, אשר עשוי שלא להשתקף באופן מלא בנתונים או במודל עליהם מבוססת המערכת. למשל, עסקה של חידוש ביטוח רכב למי שגרים באזור שנפגע במלחמה דורשת מחד התחשבות בסיכון הנובע מהלחימה ומאידך התחשבות במצב הכלכלי-חברתי של המבוטח תוך הפעלת שיקול דעת על ההשלכות החברתיות של חידוש או אי חידוש הביטוח. שיקול דעת אנושי עשוי להיות בעל הטיות משלו וכן מעורבות אנושית בהליכים ממוחשבים עשויה להאט אותם ולהפחית את היעילות בפיתוח ושילוב מערכות ממוחשבות בארגון, לפיכך עדכון כללי הממשל התאגידי וקביעת אחריות ומעורבות אנושית צריכים להיעשות בשים לב לתועלות ולעלויות שלהם.

הסברתיות היא מונח ייעודי למערכות בינה מלאכותית, כפי שכבר הוצג בדוח זה, והיא מתייחסת ליכולת להסביר את תוצריה של מערכת בינה מלאכותית באופן שיהיה מובן לבני אדם. הסברתיות היא יכולת טכנולוגית המפותחת במקביל או אגב פיתוח מערכת הבינה המלאכותית, והיא יכולה לסייע בטיפול במספר סוגיות וסיכונים. למשל, באמצעות הסברתיות ניתן לבחון האם מודל הבינה המלאכותית הביא בחשבון מאפיינים שלא נהוג להשתמש בהם בשל חשש לאפליה וכן ניתן לטפל בחלק מסיכונים המודל. הסברתיות יכולה גם לסייע לכלי הממשל התאגידי, כמו גם לכלי הגילוי, בכך שהיא תספק מידע על הגורמים שהביאו לתוצאה שהתקבלה ממערכת הבינה המלאכותית כך שניתן יהיה לקיים דיון מושכל בתוצאה. הסברתיות, כפי שנדון כבר בדוח, אינה הכלי היחיד לבקרה על מערכת בינה מלאכותית. כלי נוסף, למשל, הוא הפעלת מודלים סטטיסטיים מקבילים על אותם נתונים, וכן בחינת מקרי החלטה מסוימים באופן מדגמי על-ידי מומחה.

גילוי ויידוע הם כלים המשמשים לחשיפה של מידע על אופן פעילות גוף פיננסי, עליו חלה חובת הגילוי. שקיפות וחשיפה של מידע הם כלים המאפשרים הפעלת ביקורת חיצונית על הגוף הפיננסי, בין אם המידע נחשף לציבור הכללי או לרגולטור. תוצאות הליך חיתום הביטוח נמסרות ללקוח הפוטנציאלי והוא מקבל הצעה לביטוח הכוללת את תנאי הפוליסה והמחיר, או במקרים חריגים, סירוב לעסקה. האסדרה של שוק הביטוח, עליה נרחיב בהמשך, מכילה, בין היתר, הוראות על המידע אותו על חברת הביטוח למסור ללקוח בנוגע להליך החיתום הביטוחי וכן בחובות גילוי נוספות המאפשרות בראש ובראשונה לרגולטור, וגם לציבור, לבצע פיקוח ובקרה על הליך זה, ועל פעילות חברות הביטוח באופן כולל.

אסדרה קיימת

רשות שוק ההון, ביטוח וחיסכון מאסדרת ומפקחת על חברות הביטוח באמצעות מסגרת אסדרה הנוגעת לכלל תחומי והיבטי הפעילות שלהן. האסדרה מורכבת מחקיקה ראשית ומשנית, לרבות הוראות הממונה על שוק ההון, ביטוח וחיסכון (חוזרים). שילוב מערכות בינה מלאכותית בפעילות חברות הביטוח לא תגרע מחובותיהן, והטכנולוגיה החדשה תצטרך להיות מפותחת ומופעלת בהתאם למסגרת החוקית. סקירה של האסדרה הקיימת מעלה כי היא מכילה את מרבית הכלים להתמודדות עם הסוגיות והסיכונים שמעלה בינה מלאכותית, אך היא עושה זאת באופן כללי וממבט על, ויש לבחון אם השימוש בבינה מלאכותית מעורר סוגיות נקודתיות להן נדרשת התייחסות מיוחדת. נציג בקצרה את הנושאים בהם מטפלת האסדרה הקיימת, ולאחר מכן נציג המלצות לעדכון ההסדרה.

חברת ביטוח נדרשת לקיים מסגרת לניהול סיכונים כוללת ולזהות, לאמוד ולטפל בכל סוגי הסיכונים להם היא חשופה, לרבות התאמה ועדכון מסגרת ניהול הסיכונים כדי שתכלול גם סיכונים חדשים או מתפתחים. נוסף לקביעת מסגרת סיכונים כללית, קיימות הוראות ממוקדות לאופן הניהול של סוגי סיכון שונים בניהם סיכון מודל, סיכונים סייבר וטכנולוגיות מידע, וסיכונים מיקור חוץ.⁴⁶⁸

הוראות ממשל תאגידי כוללות קביעת אחריות על אורגנים של חברת הביטוח ובעלי תפקידים על תחומי פעילות שונים וכן מדרגים לקבלת החלטות המחייבים דיון אנושי. הוראות הממשל התאגידי שזורות באסדרה על פי סוגי הסיכונים השונים, וקיימת הוראה מרכזת בנוגע לדירקטוריון, כל זאת כדי להבטיח שהאחריות מוגדרת וברורה בכל תחומי הפעילות. נוסף לכך, קיימות הוראות גילוי ודיווח לרגולטור, לציבור הכללי וכן הוראות מסירת מידע ללקוח, הכוללות דיווחים על הפעילות השוטפת וכן דיווחים ממוקדים על אירועים מסוימים.⁴⁶⁹

נושאי אפליה ופרטיות מטופלים בהוראות הדין הכלליות החלות באופן רוחבי על כלל המשק, וזאת בנוסף לאסדרה

468 אסדרה עיקרית: ניהול סיכונים – פרק 10 לחלק 1 לשער 5 לחוזר המאוחד; מדידת התחייבויות – פרק 1 לחלק 2 לשער 5 לחוזר המאוחד; ניהול טכנולוגיות מידע בגופים מוסדיים – חוזר 4-9-2010 מיום 22.8.2010; ניהול סיכונים סייבר בגופים מוסדיים – חוזר 14-9-2016 מיום 31.8.2016; מיקור חוץ בגופים מוסדיים – פרק 6 לחלק 3 לשער 5 לחוזר המאוחד.

469 אסדרה עיקרית: דירקטוריון גוף מוסדי – פרק 2 לחלק 1 לשער 5 לחוזר המאוחד; גילוי ודיווח – חלק 4 לשער 5 לחוזר המאוחד.

החלה על חברות הביטוח באופן ממוקד. הסדרת ההגנה על הפרטיות מתבססת בעיקרה על חוק הגנת הפרטיות, התשמ"א-1981 והתקנות הנלוות אליו, אך רשות שוק ההון יצרה גם הסדרה משלימה עבור הגופים הפיננסיים שתחת פיקוחה. ההסדרה כוללת קביעת עקרונות סודיות בניהול המידע, נהלים לניהול סיכונים, והנחיות להצפנה ואחסון המידע, זאת בנוסף להוראות אבטחת המידע וסייבר שחלים על מאגרי המידע. ההסדרה של מניעת אפליה מורכבת מהוראות חוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998 וחוק אישור הפליה במוצרים, בשירותים ובכניסה למקומות בידור ולמקומות ציבוריים, התשס"א-2000, וכן מהוראות של הממונה על שוק ההון, ביטוח וחסכון. ההסדרה הקיימת קובעת מסגרת לאבחנה בין לקוחות באמצעות הליך החיתום וכוללת הגבלות על איסוף נתונים ובמקרים מסוימים אף מגבילה את השימוש במשתנים ספציפיים בקביעת החיתום. בנוסף, נקבעו תנאים אחידים ופוליסות סטנדרטיות לסוגים שונים של ביטוח, כגון רכב, בריאות וחסכון פנסיוני.



המלצות בנוגע לחיתום ביטוח

עקרונות מנחים בעבודת הרגולטורים הפיננסיים עוסקים בצורך להבטיח סביבה פיננסית יציבה ואמינה ויחד עם זאת סביבה בה טכנולוגיות ושיטות עבודה חדשות וחדשניות יכולות להתפתח, כל זאת לטובת צרכני השירותים הפיננסיים. יצירת אסדרה לטיפול בסיכונים והסוגיות העולים מבינה מלאכותית צריכה להתאים לעקרונות הללו. האסדרה הקיימת על חברות ביטוח מתאפיינת במיקוד לפי סיכונים והיא ניטרלית מבחינה טכנולוגית. כתוצאה מכך, חברת ביטוח הבוחרת לאמץ בינה מלאכותית, צריכה לפתח וליישם את טכנולוגיית הבינה המלאכותית בהתאם לאסדרה. עם זאת האסדרה הקיימת אינה ייעודית לטכנולוגיה החדשה, ויש לבחון צורך בעדכון שלה, ולוודא כי היא מספקת מענה אפקטיבי לסוגיות ולסיכונים המרכזיים באופן התואם את מאפייניה הייחודיים של הבינה המלאכותית. תחומים לגביהם נדרשת תשומת לב מיוחדת הם ניהול סיכונים מודל, הסברתיות וגילוי, למשל, גילוי על השימוש בבינה מלאכותית כאמצעי קשר עם הלקוח (צ'ט-בוט). נוסף לכך יש צורך לבחון את דרכי הפיקוח והבקרה על חברות הביטוח והכלים העומדים לרשותו של הרגולטור. למשל, מודל חיתום הביטוח עובר בקרה מסוימת אצל הרגולטור בעת כניסה של מוצר ביטוחי חדש, וכן מתקבל מידע על תוצאות המודל בעת טיפול בפניות ציבור. התגברות השימוש בבינה מלאכותית מעלה צורך לבחון את כלי הפיקוח העומדים לרשותו של הרגולטור ואת ההתאמה שלהם לבחינה של החלטות עסקיות ותהליכי עבודה שבוצעו באמצעות בינה מלאכותית.

חלק ה'

**פעולות נוספות
לקידום רגולציה
פיננסית בתחום
הבינה המלאכותית**



ההמלצות בחלק זה אינן נוגעות לסוגיה מסוימת בפעילות של בינה מלאכותית (הסברתיות, אפליה, וכן הלאה) או לסוג מסוים של פעילויות (ייעוץ השקעות, אשראי וכדומה), אלא לפעולות תשתיות הנדרשות בצד הרגולטורי כדי להפוך את הרגולציה הפיננסית בתחום הבינה המלאכותית למתקדמת ואפקטיבית. המלצות אלה נחלקות לשלושה מישורים: עידוד חדשנות; קידום ודאות רגולטורית והתאמות בדין; וקידום הפעילות הפיקוחית.

עידוד חדשנות

א. ארגזי חול רגולטוריים (Regulatory Sandboxes) ומוקדי חדשנות (Innovation Hubs)

טכנולוגיות חדשות שינו בשנים האחרונות את הפעילות הפיננסית במגוון תחומים. כך למשל, פעולות יומיומיות כגון ביצוע תשלומים או הפקדת שיקים עברו מביצוע ידני לביצוע מרחוק במחשב או בסלולר, ופעילות השקעה בניירות ערך הפכה נגישה יותר באמצעות פלטפורמות מסחר הנגישות לציבור הרחב. הפוטנציאל הגלום בטכנולוגיות חדשות הוביל רגולטורים פיננסיים ברחבי העולם לנסות ולקדם אימוץ טכנולוגי במגוון פעילויות, במטרה להרחיב פעילות פיננסית, ליעל ולהוזיל אותה, וכן במטרה להכניס מתחרים חדשים למערכת הפיננסית. מעורבות הרגולטורים באימוץ הטכנולוגיות יכולה גם לסייע להם בהבנתן ובהתמודדות עם הסיכונים הגלומים בהן. הרגולציה הפיננסית שואפת בהקשר זה לקדם בעזרת טכנולוגיות חדשות פיתוח שוק מבלי להתפשר על תכליות של הגנת הציבור ושמירת פעילותה התקינה ויציבותה של המערכת הפיננסית.⁴⁷⁰

בהינתן האימוץ המוגבל בשלב זה של טכנולוגיית בינה מלאכותית בסקטור הפיננסיים בישראל, יכול להיות משנה חשיבות ליישום שתי טכניקות רגולטוריות – הקמתם של 'ארגזי חול רגולטוריים' ויצירת מוקדי חדשנות.

המונח "ארגז חול רגולטורי" (Regulatory Sandbox) משמש לתיאור אסטרטגיה רגולטורית המעניקה למפתחים של טכנולוגיה פיננסית סביבת ניסוי גמישה ותחומה בזמן לפיתוח המוצר, תחת פיקוח רגולטורי נוח יחסית הכולל הפחתת נטלים ודרישות פיקוחיות. במקביל, סביבה זו מאפשרת לרגולטור לנטר אחר הסיכונים שמציבה הטכנולוגיה החדשה, לאמוד את טיב ומידת הרגולציה הנדרשת במקביל לשלבי פיתוח המוצר, ולהתאימה לידע הנרכש על הפעילות החדשה, וזאת מתוך הכרה כי פעמים רבות הרגולטור מתאפיין בפערי מידע ומומחיות בעולם הטכנולוגי ביחס לשוק.

מאז יישום מודל ארגז החול הרגולטורי לראשונה בשנת 2016 על-ידי הרשות הפיננסית הבריטית (FCA) הוא הפך נפוץ, ומשמש רגולטורים רבים ברחבי העולם לשם קידום חדשנות טכנולוגית, עידוד כניסת שחקנים חדשים לשוק והגברת התחרות, תוך שמירה על סביבת פעילות מפוקחת.⁴⁷¹

גם בישראל ננקטו צעדים לקידום כלי רגולטורי זה, אשר שיקפו הכרה בחשיבותו לקידום החדשנות בתחום הפיננסי. הצעד המרכזי היה הצעת החוק לעידוד פיתוח טכנולוגיה בתחום הפיננסי בישראל, התשפ"א–2021, אשר פורסמה בחודש ינואר 2021 (להלן בפרק זה: "הצעת החוק").⁴⁷² הצעת החוק ביקשה להקל ולקבוע הוראות המותאמות לפעילות חדשנית (בין שהיא כפופה לחובת רישוי לפי הדין ובין שאינה כפופה), כדי לנסות את המודל העסקי

470 ראו עוד על התמודדות הרגולציה הפיננסית עם אתגרי החדשנות:

Emilios Avgouleas "Regulating Financial Innovation" The Oxford Handbook on Financial Regulation (Eds. Niamh Moloney, Eilis Ferran and Jennifer Payne) (Oxford University Press, 2015), <https://ssrn.com/abstract=2458335>; OECD/KDI (2021), Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses, OECD Publishing, Paris, <https://doi.org/10.1787/8fa190b5-en>.

471 רות פלאטו-שנער "תפקיד המשפט בפיתוח ובעיצוב מערך אמצעי התשלום בישראל" משפט, חברה ותרבות: משפט, כלכלה ומוסדות בישראל, 361, 373–374 (2022); רות פלאטו-שנער "תרומתו של ארגז החול הרגולטורי לפיתוח יישומי בינה מלאכותית בתחום הפיננסי", עמ' 2 (עתיד להתפרסם בכתב העת משפט, חברה ותרבות: אלוטריה, בינה מלאכותית והמשפט, כרך ח, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4666710; דו"ח הצוות הבין-משרדי לרגולציה חכמה, בעמ' 129–130, https://www.gov.il/BlobFolder/reports/he/smart-regulation-team-recommendations-report.pdf?fireglass_rsn=true; Buckley, Ross P. and Arner, Douglas W. and Veidt, Robin and Zetzsche, Dirk Andreas, Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond (November 1, 2019). University of Luxembourg Law Working Paper No. 2019-010, European Banking Institute Working Paper Series 2019 – no. 53, UNSW Law Research Paper No. 19-72, University of Hong Kong Faculty of Law Research Paper No. 2019/100, Washington University Journal of Law and Policy, Vol. 61, 2020, <https://ssrn.com/abstract=3455872>.

472 הצעת חוק הממשלה לעידוד פיתוח טכנולוגיה בתחום הפיננסי בישראל, התשפ"א–2021 (מ/1390). הצעת החוק הוצגה בהמשך להחלטת ממשלה מס' 3411, שעניינה הקמת סביבת ניסוי לחברות טכנולוגיה פיננסיות, מחודש ינואר 2018, ולדוח של צוות בין-משרד אשר פרסם בחודש ינואר 2019 דוח לעניין מתווה להקמת סביבת ניסוי כאמור.

ולאפשר לבחון את אופן השפעת השירות או המוצר על צרכנים. הוצע כי מגבלות אלו ייקבעו למשך תקופת זמן של עד שנתיים, עם אפשרות להאריך בשנתיים נוספות בכפוף לנסיבות מסוימות. הואיל וחברות המשתתפות בתכנית עשויות להיות בעלות יתרון על פני חברות שאינן משתתפות בה, ועל מנת להגביר את השקיפות גם לטובת חברות השוקלות להגיש בקשה להשתתפות בתכנית, הוצע לקבוע חובת פרסום בנוגע להחלטות שונות שקיבלו הרגולטורים בעניין ההוראות שייקבעו לחברות המשתתפות. בדברי ההסבר להצעה צוין, כי פרסום ההחלטות חשוב גם על מנת להגן על ציבור הלקוחות או המשקיעים של המשתתפת, ונועד לאפשר להם לכלכל את צעדיהם בידיעה שמדובר בחברה הפועלת במסגרת של מסלול חדשני וקצר טווח.

עוד הוצע להקים ועדה סטטוטורית מיוחדת שתשמש כתובת אחת (one-stop-shop) לחברות המבקשות להשתתף בתכנית, ותכלול את הרגולטורים הפיננסיים וגורמים ממשלתיים נוספים. מתווה זה נועד לאפשר לרגולטורים השונים לתאם את אופן הטיפול בחברות המשתתפות בתוכנית, למנוע אי-התאמות בפיקוח וארביטראז' רגולטורי, ולהקל על מלאכת צבירת המומחיות בידי הרגולטורים באופן מערכתי.

מודל של "ארגז חול רגולטורי" יכול לסייע בהכנסה בטוחה של מערכות בינה מלאכותית לתחומי הפיננסיים, כחלק מסביבה רגולטורית לומדת, דינמית ותחומה בזמן. טכנולוגיות הבינה המלאכותית מתאפיינות בדינמיות ובהתקדמות מהירה, אשר מאתגרות את מידת התאמתה של החקיקה הפיננסית המסורתית בישראל לפעילות זו. על כן נדרשת גישה יעילה וגמישה לרגולציה שתאפשר למצות את פוטנציאל ההתפתחויות בתחום זה, ואף לעודד אותן, אך לעצב אותן באופן שלא פוגע בתכליות החקיקה הפיננסית.⁴⁷³ כך למשל, גורמים שיבקשו לעשות שימוש בטכנולוגיות בינה מלאכותית לשם סיוע בקבלת החלטות מתן אשראי ללקוחות או לשם בנייה והצגה של מסלולי השקעה ללקוח, יוכלו לעשות כן תחת סביבה רגולטורית מותאמת. גורמים אלו ייהנו מסביבה רגולטורית שתאפשר גמישות הנחוצה לפיתוח ולהרצה של הפעילות החדשה, וזאת במקביל לפיקוח הדוק שיאפשר הגנה על הציבור וקיום שאר התכליות הרגולטוריות של האסדרה, כמו גם שיפור היכרות הרגולטור עם מאפייני הפעילות החדשה.

המלצה זו עולה בקנה אחד עם המגמה העולמית, המצביעה על כך שהשימוש ב"ארגז חול רגולטורי" עשוי להפוך שכיח במיוחד בקרב רגולטורים בהקשרים של בינה מלאכותית.⁴⁷⁴ האיחוד האירופאי הדגיש את התפקיד שעשוי להיות לארגזי חול רגולטוריים בפיתוח טכנולוגיות בטוחות של בינה מלאכותית, ומדינות כגון בריטניה וסינגפור התייחסו לכך ספציפית בהקשר של תחום הפיננסיים.⁴⁷⁵ יש לסייג, עם זאת, ולציין כי קיימים סימני שאלה עד כמה טכניקה רגולטורית זו היא אפקטיבית. ביקורת משמעותית בהקשר זה היא כי עד כה טופל במסגרת ארגזי חול מספר קטן של מקרים, ולא ברור עד כמה אלה תרמו באופן מצרפי לחדשנות במערכת הפיננסית.⁴⁷⁶

בהקשר הישראלי עולה חשש כי הצעת החוק, ככל שתקודם, אינה מספקת לצורך קידום פעילות של בינה מלאכותית. הצעת החוק קובעת מנגנון העלול להיות מסורבל, שכן הוא מחייב פעולה באמצעות ועדה סטטוטורית. הרציונל למנגנון זה היה השגת כתובת אחת כאשר גוף מבקש לקבל התייחסויות ממספר רגולטורים פיננסיים, אולם טכנולוגיית בינה מלאכותית עשויה לשמש בפעילויות ליבה הנמצאות תחת פיקוח של רגולטור מסוים, כך שספק אם יש הכרח לעסוק בפניות שיהיו באמצעות ועדה סטטוטורית מיוחדת הכוללת את כל הרגולטורים וכן גורמים נוספים. בנוסף לכך, הצעת החוק הציגה מגבלות זמן משמעותיות לפעילות במסגרת סנדבוקס (שנתיים + שנתיים). הרציונל למגבלות אלה היה ההיתר לסטות זמנית מהוראות הדין, וההערכה כי ניתן יהיה לקבוע אסדרה קבועה בתקופה זו. ואולם בהינתן שמדובר בפעילות דינאמית ומתפתחת, ופרק הזמן הדרוש לקביעת אסדרה (בעיקר בדרך של חקיקה) הנו ארוך מאוד, מגבלות אלה צפויות לפגוע באפקטיביות ארגז החול הרגולטורי. קשיים אלה עלולים ליצור תמריץ שלילי עבור גופים, ובעיקר עבור גופים פיננסיים גדולים המעוניינים להשקיע משאבים גדולים בפעילות של בינה מלאכותית, לעשות כן.

מוצע לבחון שינויים בהצעת החוק, וכן לגבש תיקוני חקיקה בדינים הפיננסיים הרלוונטיים אשר יאפשרו הקמת "ארגזי חול" עצמאיים על ידי כל רגולטור פיננסי בתחום אחריותו, מקום בו הדבר אינו אפשרי לפי הדין הקיים.

473 ראו מסמך המדיניות, בעמ' 100.

474 Lawrence G. Baxter, Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures, 66 Duke Law Journal 567-604, <https://scholarship.law.duke.edu/dlj/vol66/iss3/5> (2016).

475 Attrey, A., M. Leshner and C. Lomax (2020), "The role of sandboxes in promoting flexibility and innovation in the digital age", OECD Going Digital Toolkit Note, No. 2, https://goingdigital.oecd.org/data/notes/No2_ToolkitNote_Sandboxes.pdf, בעמ' 30-32; פלאטו-שנער "תרומתו של ארגז החול הרגולטורי לפיתוח יישומי בינה מלאכותית בתחום הפיננסי", ה"ש 446 לעיל, בעמ' 13-16.

476 ראו Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond, ה"ש 446 לעיל.

מתן סמכות פרטנית כאמור מתיישבת עם הגישה הכללית שמוצע לאמץ בדוח זה, לפיה נדרשת גמישות רגולטורית מוגברת המאפשרת התאמה מהירה, בין היתר, של סביבות הניסוי למנעד מוצרי בינה מלאכותית רחב, בהינתן שמדובר בתחום טכנולוגי חדשני, לומד ומתפתח. היא נובעת גם מן ההכרה בכך שבינה מלאכותית עשויה לשמש בפעילויות ליבה פיננסיות, המפוקחות על-ידי רגולטור אחד, ועל כן אין הצדקה למנגנון הוועדה הסטטוטורית. יתרון נוסף בארגז חול עצמאי עשוי להיות בממד של ליווי מצד הרגולטור בשלבי פיתוח והשקת המוצר או השירות, גם אם לא ידרשו בסופו של יום התאמות רגולטוריות בעניינם. המלצת הצוות בנוגע לארגזי חול רגולטוריים עוסקת מטבע הדברים בטכנולוגיית בינה מלאכותית, אולם רצוי לשקול אותה גם ביחס לטכנולוגיות אחרות.

טכניקה רגולטורית נוספת, המשתייכת לקטגוריה של יוזמות רגולטוריות הפונות לגורמים מפוקחים קיימים ופוטנציאליים (יוזמות Outreach), והצוות ממליץ לקדמה, היא הקמת **מוקדי חדשנות**. בעוד ארגז חול רגולטורי משמש ליוזמות קונקרטיות, המבקשות הקלות זמניות ממשרר רגולטורי, מוקדי חדשנות יכולים לנקוט שורה של מהלכים כלליים ליצירת עניין ודיאלוג בין הרגולטור ובין גופים מפוקחים.

שתי הטכניקות יכולות לשמש יחדיו, ולמעשה ארגזי החול בבריטניה ובאוסטרליה צמחו מתוך מוקדי החדשנות שהוקמו שם על-ידי הרגולטורים הפיננסיים. מטרותיהן של שתי הטכניקות הן דומות למדי, וכוללות שידור מסר של פתיחות וגמישות מכיוון הרגולטור לעבר השוק; קידום חדשנות ותחרות אצל גופים פיננסיים; ורכישת ידע רגולטורי.⁴⁷⁷

יתרונות אפשריים של מוקד חדשנות נעוצים בפנייה לקבוצה רחבה יותר של גופים, וביכולת להעלות מודעות ולעורר עניין סביב נושא ספציפי, כגון יישומים של טכנולוגיית בינה מלאכותית (ואף בתחום מסוים, כגון חיתום אשראי או ביטוח). דרכים מקובלות לכך הן האקדמיות טכנולוגיים-רגולטוריים, תחרויות, כנסים, תכניות פיילוט, ושיח עם גורמים ספציפיים. בסינפפור, לדוגמה, אפשר לראות שלל פעילויות ביוזמת או בתמיכת המדינה לעידוד הכנסת טכנולוגיה בכלל, וטכנולוגיית בינה מלאכותית בפרט, לעולמות הפיננסיים.⁴⁷⁸

בישראל אפשר לציין כדוגמה את מרכז החדשנות הרגולטורי של רשות ניירות ערך אשר הוקם בשנת 2018 (Fintech Regulatory Innovation Hub). מטרתו של המרכז היא לסייע ולהעניק הכוונה שאינה פורמלית לחברות פינטק המעוניינות לפעול בישראל. מרכז החדשנות מסייע לגורמים המבקשים להתחיל לפעול בשוק המקומי להבין את המסגרת החוקית בישראל ולקבוע אם היא מתאימה לתחום פעילותן. מטרה נוספת של המרכז היא ללמוד ולהכיר טוב יותר את השחקנים השונים, צרכיהם, החסמים העומדים בפני חברות הטכנולוגיה המבקשות לפעול בישראל, ולהעמיק את המומחיות והידע ברשות בסוגיות טכנולוגיות ואחרות הנוגעות לפעילות החברות. החברות הפונות למרכז החדשנות נמצאות, בדרך כלל, בשלבי פעילות ראשוניים של מוצר (C2B (Business to Consumer ומעדיפות, בשלב הראשון, להכיר היטב את המסגרת החוקית הקיימת ולהתאים אליה את מתווה פעילותן, לעיתים אף קודם לקבלת חוות דעת משפטית.⁴⁷⁹

תכנית נוספת המופעלת על ידי רשות ניירות ערך ורשות החדשנות החל משנת 2020 היא תכנית הפיילוט, המאפשרת לחברות טכנולוגיה ישראליות בתחום הפיננסי, לערוך פיילוט עם לקוחות הקצה שלהן (רשות ניירות ערך, גוף פיננסי או הציבור הכללי). לחברות המשתתפות בתכנית מוצעת גישה למאגרי המידע של רשות ניירות ערך ולנתוני המסחר של הבורסה לניירות ערך, מימון בהיקף של 30%–50% מהוצאות הפיילוט וליווי רגולטורי של סגל רשות בכל הסוגיות הנוגעות אליו.

במהלך שנת 2022 הצטרף בנק ישראל לתכנית כמשקיף, סייע בהערכת הבקשות שהוגשו בתחומי פעילותו והעניק ליווי מקצועי לחברות שנבחרו. הליווי המקצועי המוענק על ידי רשות ניירות ערך ובנק ישראל מאפשר לחברות רמה גבוהה יותר של ודאות בשאלות העולות אגב הטמעת טכנולוגיות חדשות ועמידתן בהוראות הדין. עם זאת, הרשות אינה רשאית להעניק במסגרת התכנית פטורים או הקלות כלשהן מהוראות הדין. מאז הקמתה, פעלו במסגרת תכנית הפיילוט 15 חברות אשר נהנו מהיקף מימון כולל של כ-14.5 מיליון שקלים.

במסגרת הקמה או הרחבה של מוקדי חדשנות מוצע לבחון חיבור אפשרי לא רק בין הרגולטורים ובין שחקנים פיננסיים קיימים ופוטנציאליים, אלא גם עם האקדמיה וגורמים רלוונטיים מהחברה האזרחית. התפתחות טכנולוגיית הבינה

477 שם, בעמ' 60, 78–79.

478 ראו באתר הרשות הסינפפורית <https://www.mas.gov.sg/development/ai-in-finance>.

479 צוות הפינטק ברשות ניירות ערך המפעיל את מרכז החדשנות מורכב מנציגי כלל המחלקות במטרה להעניק מענה מהיר ואינטגרטיבי לחברות. במסגרת זאת הרשות אינה מעניקה סיוע כלכלי או הכוונה בנושאי חקיקה שאינם בתחום אחריותה וכי פעילות במרכז אינה תחליף לליעוץ הנדרש, משפטי או אחר. בתקופת פעילותו נפגש הצוות עם חברות רבות, ליווה אותן בהכרת המסגרת החוקית והפנה אותן לעתים לתוכניות הרלוונטיות לפעילותן או לגורמי ממשל אחרים הרלוונטיים לפעילותן.

המלאכותית בעולם מבטאת קשר חזק בין מחקר אקדמי ויזמות עסקית, ובמסגרת מוקד חדשנות יש לשלב צדדים אלה.⁴⁸⁰

המלצת הצוות אם כן היא להתבסס על הפעילות הקיימת ולהרחיב את השימוש בארגזי חול רגולטוריים ובמוקדי חדשנות, תוך הדגשת פעילות בינה מלאכותית כתחום מרכזי לקידום.

ב. בחינת פתרונות לבעיית הנגישות למידע

אימוץ טכנולוגיית בינה מלאכותית מחייב מאגרי מידע משמעותיים. גופים פיננסיים חדשים או קטנים עלולים להתקשות להשיג את היקף ומגוון הנתונים הנדרשים לצורך פיתוח או שימוש במודל בינה מלאכותית. בעיית המידע קיימת כבר כיום, למשל ביחס לפיתוח מודל מבוסס סטטיסטית לצורך חיתום הלוואות או ביטוח, והיא עשויה להתעצם עם כניסת טכנולוגיית בינה מלאכותית. פתרון אפשרי אחד הוא פתיחה של מאגרי מידע קיימים או הקמה ופתיחה של מאגרי מידע חדשים לשימוש על-ידי השחקנים הרלוונטיים. דוגמאות מהעולם לפיתוח מאגרי מידע לצרכי בינה מלאכותית משתרעות על מגוון שימושים – מזהוי בעיות בריאותיות ועד חיזוי שריפות יער.⁴⁸¹

הקמתם ופתיחתם של מאגרי מידע מתכתבת עם מדיניות של ממשל פתוח (open data) אשר קדמה לטכנולוגיית הבינה המלאכותית, במטרה לקדם ערכים כגון שקיפות שלטונית, מימוש זכות האזרח למידע, ועידוד צמיחה כלכלית.⁴⁸² בהקשר הפיננסי עשויה להיות חשיבות לפתיחת מאגרי מידע גם בהיבט התחרותי, על מנת שהמידע לא יעניק יתרון בלעדי לגופים פיננסיים גדולים. ראו לעניין זה את הניתוח לעיל בפרק התחרות, בו מוסבר מדוע היעדר גישה לתשומות מידע מהווה אחד החששות התחרותיים המשמעותיים ביותר מכניסתה של פעילות בינה מלאכותית, ומוצע לפעול בנדון.

האתגרים הכרוכים בהקמה ופתיחה של מאגרי מידע לצרכי בינה מלאכותית הם רבים. ניתן למנות עליהם אתגרי פרטיות ואבטחת מידע, איכות המידע, שילוב מידע ממקורות שונים, ובקורות על הגישה למידע, שמירתו, השימוש בו ומחיקתו. בהקשר הפיננסי, מאגרי מידע עשויים לכלול מידע אישי ולכן לגביהם המורכבות גדולה באופן מובהק בהשוואה למאגרי מידע שאינם כוללים מידע כאמור. האפשרות לנקוט צעדים לפתיחת מאגרי מידע שיהיו נגישים לשחקנים בשוק כפופה לחובות סודיות ולעקרונות וכללי הגנת מידע אישי במאגרי מידע הקבועים בדיון.

המלצת הצוות היא לבחון פתרונות לבעיית הנגישות למידע, בפרט של גופים קטנים או חדשים, ובכלל זה לבחון את האפשרות להקים או לפתוח מאגרי מידע כבסיס לפעילות בינה מלאכותית.

⁴⁸⁰ <https://fintech-israel.org/> חברה בנק ישראל, רשות ניירות ערך, רשות החדשנות, מערך הדיגיטל הלאומי, משרד הכלכלה ומשרד האוצר לקהילת Fintech IL – Innovation Community, המופעלת על ידי עמותת מרכז הפינטק הישראלי. חזון הקהילה הוא לקדם את החדשנות במגזר הפיננסי בישראל כדי להנגיש לציבור הרחב ולעולם העסקים הישראלי מגוון רחב של שירותים מתקדמים, איכותיים ותחרותיים ולממש את הפוטנציאל של תעשיית הפינטק כמקור לצמיחה כלכלית ולתעסוקת עובדים איכותיים וכענף ייצוא. מטרות הקהילה הן בין השאר לסייע למוסדות הפיננסיים לאמץ, לקדם ולנהל תהליכי חדשנות ולקדם ממשקי עבודה יעילים בין הרגולטורים הפיננסיים לתעשייה, וליזום שיתופי פעולה ושיתוף ידע בין השחקנים השונים. למידע נוסף ראו <https://fintech-il.org.il/>.

⁴⁸¹ Niklas Berglind, Ankit Fadia and Tom Isherwood "The potential value of AI – and how governments could look to capture it" McKinsey (July 25, 2022), <https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it>.

⁴⁸² תהילה שוורץ-אלטשולר "ממשל פתוח בישראל בעידן הדיגיטלי" המכון הישראלי לדמוקרטיה, מחקר מדיניות 91 (2012), https://www.idi.org.il/media/3512/pp_91.pdf; Anneke Zuiderwijk and Marijn Janssen "Open data policies, their implementation and impact: A framework for comparison" Government information quarterly 31, no. 1 (2014) 17–29.

קידום ודאות רגולטורית והתאמות בדיון

ג. כלים להגברת ודאות רגולטורית

לאורך הדוח מוצגות שאלות שונות שיתעוררו עם כניסתה של הבינה המלאכותית לפעילות הפיננסית. בד בבד, ההנחה היא כי בשלב זה אין עוד מקום לרגולציה ייעודית שתסדיר פעילות זו, ויש להתבסס בעיקר על הדיון הקיים. מהן אם כן הדרכים לתת מענה לשאלות האמורות? קיימים כלי עבודה שונים אשר הרגולטורים הפיננסיים עושים שימוש בהם כבר כיום, ועשויים לסייע בהתמודדות עם אי-בהירות רגולטורית, ואף למטרת קידום פעילות פיננסית מסוימת. מוצע לעשות שימוש גם בכלים אלה לאסדרת פעילות טכנולוגית בכלל, ובינה מלאכותית בפרט.

דרך אחת להגביר את הודאות המשפטית היא באמצעות פרסום **מסמכי מדיניות**. דוח זה למעשה עושה כן, ופורסם עקרונות מנחים, סוגיות רגולטוריות, וגישה מוצעת כיצד להתמודד עימן. בעתיד אפשר יהיה לשקול גיבוש מדיניות בתחומי פעילות ספציפיים יותר (לרבות אלה שלא נדונו בדוח זה) ולפרסמה, במטרה להבהיר עוד לגופים הפיננסיים מה מצופה מהם בבואם לפתח או לעשות שימוש בטכנולוגיה של בינה מלאכותית.

כלי רגולטורי הזמין כבר היום עבור הרגולטורים הפיננסיים, הינו **פנייה מקדמית**. פניה מקדמית היא פניה או בקשה קונקרטית של מבקש מסוים לקבל את עמדת הרגולטור בסוגיה הצופה פני עתיד. הפניה המקדמית היא בדרך כלל שאלה מורכבת בעלת היבטים חדשניים או רוחביים שאין לגביה תשובה מובנית או הנחיות מדויקות מטעם הרגולטור, והיא משמשת לעיתים מפוקחים המבקשים לקבל חוות דעתו של הרגולטור לגבי עסקה או פעילות מסוימת שהם עומדים לבצע או שכבר בוצעה.⁴⁸³

כלי רגולטורי נוסף הוא פרסום **עמדות פרשניות**, במסגרתן מציג הרגולטור עמדה מקצועית (למשל, משפטית או חשבונאית) המשקפת החלטות ועמדות בסוגיות הנוגעות ליישום הדינים עליהם הוא מפקח. העמדות נועדו לענות על שאלות או סוגיות שהתעוררו במקרים אשר הובאו בפני הרגולטור ולאור טיבם, הם עשויים להתעורר גם אצל מפוקחים אחרים הנתונים לסמכותו, כגון, פרשנות סעיפי חוק מסוימים ועוד. עוד מפרטות העמדות את השיקולים שהובילו את הרגולטור לאמץ העמדה המקצועית. כלי דומה הינו פרסום **שאלות תשובות (Q&A)** על-ידי הרגולטור.⁴⁸⁴ במסגרת זו מתפרסמות תשובות לשאלות קונקרטיות שנשאלו והן עשויות להיות רלוונטיות לגורמים נוספים.

כלי נוסף להגברת ודאות רגולטורית, שאינו מופנה לרוב לגופים המפוקחים אלא לציבור הרחב ולגופים שאינם מפוקחים, הוא **פרסום של מדריכים ואזהרות** הנוגעים לפעילות פיננסית. בחו"ל אפשר לראות לאחרונה פרסומים מסוג זה הנוגעים לפעילות של בינה מלאכותית. כך למשל, אזהרות הנוגעות לסיכונים הונאה הקשורים בבינה מלאכותית, צעדים שכדאי לנקוט לפני השקעה בחברות הטוענות כי הן מעורבות בפעילות של בינה מלאכותית, וכדומה.⁴⁸⁵

חלק גדול מעבודת הפיקוח של הרגולטורים הפיננסיים מתבצע באמצעות כלים אלו. בהתאמה, הם עשויים להיות לעזר גם לשם התמודדות עם פעילות פיננסית מבוססת בינה מלאכותית, אשר יוצרת אי-בהירות בדבר תחולת הדינים או אופן תחולתם על פעילות כזו או אחרת. שימוש בכלים אלו, הזמינים כבר עתה, מזמן אפשרות לפרש את הדינים ולהחילם באופן גמיש, יעיל ומשתנה בהתאם לצורך ולהתפתחות הטכנולוגית, במיוחד בשלב שבו התחום לא מוסדר מלכתחילה בדברי חקיקה. מעבר לכך, כלים אלו משמשים פעמים רבות כחלק מהמענה הניתן לסיכונים הכרוכים בפעילות פיננסית כזו או אחרת.

ד. הסמכה לקבוע הוראות מיוחדות הנוגעות לפעילות בינה מלאכותית

אתגר מרכזי במלאכת אסדרת פעילות טכנולוגית בכלל, ובינה מלאכותית בפרט, הוא הקצב המהיר והדינמיות המאפיינים את ההתפתחות הטכנולוגית. מאפיינים אלו מצריכים מהרגולטור קשב מתמשך ותגובתיות מוגברת על מנת להדביק את קצב ההתפתחות, ובתוך כך להתמודד עם הסיכונים המשתנים שהטכנולוגיה מציבה. לעיתים אף עולה צורך ברגולציה בשלב שבו עדיין אין ודאות בנוגע לשימושים וההשלכות של הטכנולוגיה החדשה, בייחוד כאשר מדובר בטכנולוגיית בינה מלאכותית הלומדת ומתפתחת במהרה, באופן המקשה להסדיר אותה באופן הרמטי מלכתחילה.

⁴⁸³ ראו למשל נוהל פניה מקדמית לרשות ניירות ערך (יוני, 2008). בתי המשפט הכירו בחשיבותו של כלי רגולטורי זה. ראו דבריו של בית המשפט על כך שמן הראוי שחברות ציבוריות בישראל יוכלו לפנות לקבלת עמדתה המקדמית של רשות ניירות ערך ולפעול בהסתמך עליה, באופן המאפשר להן לפעול בדינאמיות וביעילות. ת"צ (כלכלי ת"א) 2484-09-12 **הצלחה התנועה הצרכנית לקידום חברה כלכלית הוגנת נ' כהן**, עמ' 27 (פורסם בנבו, 22.04.2014).

⁴⁸⁴ ערוץ תקשורת של פרסום שאלות ותשובות קיים כבר עתה אצל מאסדרים פיננסיים שונים, כמו בנק ישראל, רשות שוק ההון, ביטוח וחיסכון ורשות ניירות ערך. ראו למשל, עמוד שאלות ותשובות באתר בנק ישראל, עמוד שאלות ותשובות בנושא ביטוח ועמוד נוסף בנושא שירות מידע פיננסי הרלוונטיות למקורות מידע שהם גופים מוסדיים באתר רשות שוק ההון, וכן עמוד שאלות ותשובות ועמדות סגל באתר רשות ניירות ערך.

⁴⁸⁵ ראו ה"ש 373 לעיל.

הנחת הבסיס היא כי רגולציה שנועדה להסדיר פיתוח ושימוש בבינה מלאכותית בתחום הפיננסי, תידרש להיות מקודמת ולהתפתח בשלבים ובאופן גמיש בהתאם להתפתחויות הטכנולוגיות. הליכי חקיקה ותקינה מסורבלים המקשים על עדכון הרגולציה שנקבעה, אינם מהווים כלי יעיל דיו להתמודדות עם האתגרים כאמור, ובשל כך עשויים להוות חסם משמעותי הבולם חדשנות ותחרות בשוק. לכן גם אין זה מעשי להישען באופן מוחלט על הליכי חקיקה.⁴⁸⁶ גם הכלים הרגולטוריים שהוצגו לעיל, הנשענים בעיקר על פרשנות הדין הקיים, מוגבלים במידת האפקטיביות שלהם. הרגולציה הפיננסית כוללת הוראות רבות הנקבעות על-ידי הרגולטורים עצמם, באופן המאפשר גמישות והתאמות לשינויים טכנולוגיים ולצרכים אחרים המתעוררים בשוק. בד בבד היא מושתתת גם על חקיקה ראשית ותקנות, אשר עריכת שינוי בהן היא מורכבת וממושכת כאמור הרבה יותר. רשות ניירות ערך בפרט סבורה כי מערכת הדינים בתחומי הפיקוח שלה היא מוטת חקיקה וקשיחה יתר על המידה, וכי יש להרחיב את סמכויות קביעת הכללים שלה, על מנת שתוכל לערוך התאמות ברגולציה תוך זמן סביר.⁴⁸⁷

יש לשקול תיקוני חקיקה מקום בו הדבר נדרש במטרה שהאסדרה הקבועה בחוק ובתקנות תשקף את העיקרון של ניטרליות טכנולוגית ותתיר גמישות לפעול באמצעים טכנולוגיים שונים. כמו-כן, ומבלי לגרוע מסמכויות קיימות של הרגולטורים הפיננסיים, מוצע לשקול **הקניית סמכות רגולטורית לתת הוראות נדרשות על רקע שינויים בטכנולוגיה** מקום בו הדבר נחוץ ובכפוף להוראות הדין. כך יושג הערך הכפול של מתן מענה לסיכונים הכרוכים בשימוש בבינה מלאכותית, לצד שימור יתרונותיה הפוטנציאליים, עידוד חדשנות, פיקוח אפקטיבי, פיתוח שוק, והסרת דרישות עודפות וחסמי כניסה.

גישה זו תומכת בעיקרון הניטרליות הטכנולוגית המקובל ברגולציה הפיננסית והוצג בפרק העקרונות המנחים לטיפול בבינה מלאכותית בסקטור הפיננסי לעיל. לפי עקרון זה, יש לקבוע את מסגרת האסדרה באופן שאינו תלוי או מותנה בטכנולוגיה מסוימת. אחת שפעילות חייבת להיעשות בהתאם לדינים הפיננסיים בשל אופייה והסיכונים הגלומים בה, הרי שאין בביצוע הפעילות באמצעות בינה מלאכותית כדי לגרוע מתחולת הדין והוא צריך לחול עליה, אך בהתאמות הנדרשות. הואיל ולא ניתן לבצע התאמות תכופות אלה במסגרת חקיקתית או פרשנית שמסורבל לעדכנה, מוצע כי הן יבוצעו באופן גמיש על-ידי הרגולטורים הפיננסיים באמצעות קביעת הוראות מאסדר מכוח סעיפי הסמכה בדיון המנוסחים בכפוף לעיקרון הניטרליות הטכנולוגית. חלק ניכר ברגולציה הפיננסית הקיימת נקבע כבר כיום באמצעות הוראות מאסדר, ועל כן ההמלצה האמורה נוגעת לדינים בהם נדרש הדבר.

כלים נוספים שיכולים לסייע בהשגת התכלית של גמישות ויכולת תגובה זו הם **סמכויות פטור** מהוראות רגולציה (המאפשרות גם מתן פטור בתנאים), **הוראות שעה וסעיפי שקיעה** (Sunset provisions). סמכויות אלה מאפשרות להתמודד עם צרכי שוק וצרכים רגולטוריים שלא נחזו מראש, וכן לקבוע רגולציה לתקופה מוגבלת מראש, על מנת לצמצם סיכונים או להגדיר תקופת ניסיון.

קידום הפעילות הפיקוחית

ה. שימוש בבינה מלאכותית לצרכים רגולטוריים (SupTech)

דוח זה עוסק בעיקרו ביישומים של בינה מלאכותית בפעילות פיננסית. יש מקום עם זאת להפנות את תשומת הלב גם לפוטנציאל הגדול שיש לבינה מלאכותית בפעילות פיקוחית.

רגולטורים פיננסיים עושים זה זמן רב שימוש באמצעים טכנולוגיים לצורך ביצוע משימותיהם. המונח Supervisory Technology, או בקצרה SupTech, משמש לתיאור פעילותם זו. מונח זה כולל שימוש בטכנולוגיות לצרכים מגוונים ובהם דיגיטציה של תהליכים רגולטוריים כגון דיווחים של גופים מפוקחים; איסוף של מידע פיקוחי וניתוח שלו לצרכים רגולטוריים; ופיתוח של כלי בקרה ואכיפה על פעילות מפוקחת.

כחלק מפעילות SupTech יכולה טכנולוגיית בינה מלאכותית לסייע מאוד לרגולטורים פיננסיים בעבודתם. ככל שהרגולציה והפעילות המפוקחת הינם מבוססי מידע רחב יותר, כך גדל האתגר הפיקוחי, והרגולטור הפיננסי נדרש בעצמו לעשות שימוש בטכנולוגיות מידע. בינה מלאכותית עשויה לסייע אם כן בניתוח מידע על השוק ועל גופים מפוקחים, בזיהוי פגמים בפעילות מפוקחת (לדוגמה דיווחים חסרים או מניפולציה במסחר), בזיהוי אנומליות או סיכונים בגופים מפוקחים (לדוגמה נתונים המשקפים גידול בסיכונים שונים של גופים מפוקחים) ובניתוח מגמות

486 ראו דו"ח הצוות הבין-משרדי לרגולציה חכמה, ה"ש 446 לעיל, בעמ' 99-100.

487 בתחומים שהפיקוח עליהם נמסר לרשות ניירות ערך בשנים האחרונות – שירותי מידע פיננסי ושירותי תשלום – אכן נקבעה מסגרת חקיקה כללית בעוד שיתר האסדרה נעשה בדרך של הוראות. רשות ניירות ערך הציעה להרחיב מודל זה, המקובל בפיקוח הפיננסי בישראל ובח"ל, לתחומים נוספים הנמצאים תחת פיקוחה. ראו בהקשר זה הצעה להרחבת תזכיר חוק ייעול אסדרה בניירות ערך (תיקוני חקיקה), התש"ף-2000, https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic/al_lobby/al_lobby-637f62a916518/RMP6122.pdf

ובעיות בשוק המפוקח בכללותו. בדומה למגוון השימושים האפשריים של גופים פיננסיים בבינה מלאכותית לפעילותם העסקית, כך גם רגולטורים פיננסיים עשויים למצוא מגוון שימושים אפשריים שונים בבינה מלאכותית לפעילותם, ולייצר באמצעותה ניתוחים, תחזיות או תכנים אחרים במסגרת פעילות הפיקוח.⁴⁸⁸ לפעילות SupTech בעזרת בינה מלאכותית יש גם ערך מוסף לימודי עבור הרגולטור, אשר יכול להכיר כך את הטכנולוגיה ויישומיה מקרוב, באופן שיסייע לו גם בפעילות הפיקוחית.

בעולם אפשר לראות כבר דוגמאות לשימושי בינה מלאכותית לצרכים פיקוחיים. בדוח של קרן המטבע הבינלאומית (IMF) צוינו בין היתר דוגמאות של שימוש בבינה מלאכותית לחיזוי כשלי אשראי (הבנק המרכזי של איטליה, Banca d'Italia), שימוש בבינה מלאכותית לניתוח גילוי בנושא היבטי ESG (הבנק המרכזי של ספרד, Banco de España), ושימוש בבינה מלאכותית לקריאת שאלוני מהימנות (fit and proper) וזיהוי בעיות בהם (הבנק המרכזי של אירופה, European Central Bank).⁴⁸⁹ דוגמאות נוספות הן שימוש בבינה מלאכותית לשם מסירת דיווחים ובדיקת ציות בעניינים (רשות הגנת הצרכן הפיננסית של בריטניה, FCA),⁴⁹⁰ שימוש בבינה מלאכותית לשם בדיקת פרוטוקולים של דירקטוריונים בגופים פיננסיים (הבנק המרכזי של תאילנד, Bank of Thailand),⁴⁹¹ ושימוש בבינה מלאכותית לזיהוי קרטלים במכרזים ציבוריים (רשות התחרות של ברזיל, CADE).⁴⁹² אלה רק מקצת הדוגמאות וקיימים כמובן שימושים פוטנציאליים רבים נוספים.

מלבד היתרונות הפוטנציאליים לשיפור יכולותיהם ויעילותם של הגופים המפקחים, בפתרונות טכנולוגיה לצרכי פיקוח (SupTech) גלום גם פוטנציאל לצמצם נטל רגולטורי על הגופים המפוקחים. כך למשל, מעבר לתהליכי דיווח דיגיטליים ומובנים עשוי להקל הן על המפקח הן על המפוקח, ולחסוך תשומות בשני הפנים.

לצד הפוטנציאל שיש בטכנולוגיית בינה מלאכותית לצרכי פיקוח, ישנם גם סיכונים ואתגרים בכך. חלקם אינם ייחודיים לבינה מלאכותית, אלא מאפיין הכנסת טכנולוגיה לשירות הציבורי בהקשרים נוספים. כך למשל מגבלות הקשורות במשאבים תקציביים ואנושיים. ואולם, ישנם גם סיכונים ואתגרים ספציפיים לבינה מלאכותית לצרכי SupTech. אתגר משמעותי אחד נוגע למידע, שהנו הבסיס ההכרחי לפעילות של בינה מלאכותית. היקף ואיכות המידע הנחוצים לשם אימון המערכת וכדי שתפעל באופן יעיל ומדויק לאחר מכן תלויים בבסיס מידע איכותי, גדול ועדכני, שלא בהכרח הנו בהישג ידו של הרגולטור. אתגר משמעותי נוסף נוגע להיבטים המשפטיים של השימוש במערכות בינה מלאכותית על-ידי רגולטורים, החל בשאלת השימוש במידע למטרה שלשמה הושג, עבור בשאלות הנוגעות לאחסון המידע והטיפול בו על-ידי גורמים חיצוניים, וכלה בשאלת השימוש בתוצרי המידע, למשל לצרכים ראייתיים בבתי המשפט. אתגר משמעותי שלישי נוגע לסוגיות ה"קופסה שחורה" וההסברתיות והמעורבות האנושית שנדונו בדוח זה ביחס לגופים המפוקחים. עבור רגולטורים (ולמעשה עבור רשויות שלטון באופן כללי) עלול להיות קושי מיוחד בכך שפעולות שלהם אינן מוסברות באופן מלא וכפועל יוצא מכך יש גם קושי בשקיפות ובקרה לגביהן.⁴⁹³

בישראל עושים הרגולטורים הפיננסיים שימוש נרחב בטכנולוגיות במסגרת תפקידי הפיקוח והאכיפה שלהם, אולם נכון למועד זה לא נעשה שימוש בטכנולוגיות מתקדמות של בינה מלאכותית ואפשרות זו נמצאת בשלבי בחינה. רשות ניירות ערך למשל החלה בשנת 2024 פרויקט לשילוב מודלים פיננסיים של למידת מכונה ועיבוד שפה טבעית כדי לאפשר ניתוח ותובנות מנתונים הנצברים במאגרי תוך חיסכון במשאבי פיקוח ואכיפה.

לשם קידום פעילות פיקוחית המבוססת על טכנולוגיית בינה מלאכותית, סבור הצוות כי יש מקום לפעול במישורים הבאים:

ראשית, בחינת אפשרות פעילות פיקוחית בהתבסס על טכנולוגיית בינה מלאכותית, כחלק מהאסטרטגיה הכוללת של הרגולטור בנושא מערכות מידע ורתימת הטכנולוגיה לצרכי פיקוח ואכיפה. בהקשר זה מוצע כי

488 ראו עוד על יתרונות של בינה מלאכותית לצרכים פיקוחיים – OECD Business and Finance Outlook 2021: AI in Business – OECD (2021), and Finance, OECD Publishing, Paris, <https://doi.org/10.1787/ba682899-en>, בפרק 5 (עמ' 121 והלאה).

489 IMF "Powering the Digital Economy – Opportunities and Risks of Artificial Intelligence in Finance" (October 2021), https://www.imf.org/-/media/Files/Publications/DP/2021/English/PDEORAIFEA.ashx?force_isolation=true, בעמ' 11; European Central Bank "SupTech: Thriving in the digital age" (15 November 2023), <https://rb.gy/ldey1i>.

490 ה-FCA נמצאת בעיצומו של פרויקט קודיפיקציה (digital regulatory reporting) של החוקים עליהם היא אמונה כדי שיהיו readable ויאפשרו לגופים המפוקחים למסור דיווחים ומידע לרגולטור באופן מהיר, השוואתי, מתואם וגם יאפשר בדיקת ציות תוך דקות. השלבים השני והשלישי (הנוכחי) של הפרויקט עסקו, בין היתר, בניתוח שפה טבעית. <https://www.fca.org.uk/innovation/regtech/digital-regulatory-reporting#section-project-overview>.

491 Financial Stability Institute "FSI Insights on Policy Implementation No 37 – SupTech tools for prudential supervision and their use during the pandemic" (December, 2021) 18, https://www.bis.org/fsi/publ/insights37.pdf?force_isolation=true.

492 OECD Business and Finance Outlook 2021, ה"ש 463 לעיל, בעמ' 129.

493 להרחבה לגבי אתגרים אלה וסיכונים ואתגרים נוספים בפעילות SupTech של רגולטורים פיננסיים, ראו שם בעמ' 135–140.

הרגולטורים יבחנו את הצרכים האפשריים לפעילות כאמור, תרומתה האפשרית של הפעילות ביחס למערכות קיימות, היתכנות הפעילות, וכו'. יש לציין, כי על אף הנטייה הטבעית להצטרף במהירות לעולמות הבינה המלאכותית, עשויים להיות לרגולטורים מגבלות ושיקולים מדוע לא לעשות כן, ועל כל רגולטור לבצע ניתוח עצמאי בנדון. כך למשל, עשויים להיות רגולטורים שיעדיפו להסתמך על מערכות קיימות ולהמתין להתפתחות נוספת בטכנולוגיה, שכן לעתים יש יתרון דווקא להצטרפות מאוחרת ("late mover advantage"). או למשל, עשויות להיות מגבלות תקציב וכוח אדם שיגבילו פעילות כאמור.⁴⁹⁴

שנית, מוצע לעדכן סמכויות של קבלת מידע לצרכים של למידה, ניתוח, פיקוח ואכיפה מקום בו הדבר נחוץ. לרגולטורים הפיננסיים ניתנו סמכויות שונות לדרוש מידע על מנת למלא את תפקידם. חלק מהסמכויות הקיימות הן כלליות וחלקן ספציפיות באופיין. כך למשל, הוראות המחייבות מסירת פרטים בנוגע לפעולה מסוימת של גוף מפוקח, לשם בדיקה אם אותה פעולה עומדת בדרישות הדין. רשות ניירות ערך סבורה כי על מנת להתמודד עם אתגר המידע, נחוצות לה הסמכות רחבות יותר, המאפשרות קבלת מידע שיטתי מכלל השחקנים הרלוונטיים בשוק. כך למשל, לגבי פעילות של סוחרים גדולים הפועלים באמצעות אלגוריתמים במסחר בבורסה. סמכויות דרישת מידע יכולות לסייע בפיקוח על פעילויות פיננסיות שונות וכן על פעילויות בהן נעשה שימוש בבינה מלאכותית. בד בבד, דרישות מידע עלולות ליצור נטל רגולטורי, ולכן יש לדאוג לכך שההסמכה לקבל מידע והפעלתה תוגבל לשימוש סביר ולא תשית נטל עודף על הגופים המפוקחים (כפי שצוין לעיל, שיפור במתכונת מסירת המידע יכולה להקל גם על הגופים המפוקחים).

שלישית, מוצע להפנות משאבים ממשלתיים, מחוץ למסגרות התקציב הרגילות, כדי לקדם פעילות פיקוחית מבוססת בינה מלאכותית. מצב דברים בו השוק הפרטי מתקדם לעבר שימוש בטכנולוגיות חדשות בעת שהמגזר הציבורי נותר מאחור הנו בעייתי, הן לנוכח חשיבות הפעילות של המגזר הציבורי (בענייננו הגנת ציבור המשקיעים והצרכנים הפיננסיים), הן משום שאי התקדמות של המגזר הציבורי תעכב בסופו של יום גם את התקדמות השוק הפרטי.

לבסוף, מוצע להתמודד באופן מרוכז עם סוגיות רוחב הקשורות בשימוש בבינה מלאכותית במגזר הציבורי / בקרב רשויות ציבוריות ולעצב מתכונת טיפול אחידה. השימוש בבינה מלאכותית במגזר הציבורי מעורר סוגיות שונות שהטיפול בהן עשוי להיות מורכב עבור כל רשות ציבורית באופן עצמאי. בהקשר זה, המכנה המשותף של הרגולטורים הפיננסיים אינו תחום הפיקוח שלהם אלא היותם רשויות ציבוריות שעשויות לעשות שימוש בבינה מלאכותית למטרות אכיפה ופיקוח, בדומה לרשויות ציבוריות אחרות. הצוות אינו הפורום המתאים בהכרח לעסוק בסוגיות אלה, ועל כן ראה לנכון להמליץ כי הגורמים הרלוונטיים בממשלה יגבשו הנחיות וכלי התמודדות מתאימים ואחידים לשימושים מסוג זה אשר ישרתו גם הרגולטורים בצוות זה. יצוין, כי בארה"ב, למשל, הצו הנשיאותי התייחס למגזר הציבורי בצורה רוחבית.⁴⁹⁵ היתרונות בדרך התמודדות זו הם חיסכון בזמן ומשאבים, לרבות משאבי ידע (אשר לא קיימים בהכרח אצל כל רשות שלטונית), כמו גם הגעה למתכונת טיפול אחידה וידועה בסוגיות דומות.

ו. רתימת משאבים של הרגולטורים הפיננסיים והמשך עבודה של צוות משותף בנושא

הצוות מצא יתרונות רבים בעבודה המשותפת בנושא בינה מלאכותית בסקטור הפיננסי. מדובר בנושא חדש ומורכב, המעורר שאלות משותפות רבות, ולכן הקמתו של צוות רחב הכולל את הגורמים הרלוונטיים הייתה הכרחית לשם עיסוק יסודי בסוגיה.

עם היתרונות שנבעו מהקמת הצוות הבין-משרדי אפשר למנות את שיתוף הידע הרגולטורי, במסגרתו נעשתה למידה הדדית מסודרת על הידע הקיים אצל כל גורם בנוגע לבינה מלאכותית; היכולת לקיים מפגשים רבים ומשמעתיים עם גורמים חיצוניים, כגון מומחים ורגולטורים זרים; הגישה והבמה שניתנה לגורמים רלוונטיים בשוק המעוניינים להציג את משנתם בנוגע לבינה מלאכותית; ליבון של סוגיות משותפות הקשורות בשימוש בטכנולוגיה של בינה מלאכותית כגון פרטיות, ממשל תאגידי והסברתיות, בהן יכל כל גורם להציג את עמדתו וכן טכניקות רגולטוריות המקובלות אצלו; ויצירתו של מוקד ידע. בהקשר האחרון, גישת הצוות הייתה לשתף בעבודת הצוות עובדים נוספים בארגונים השונים שנטלו בו חלק, הן כדי להנות מתרומתם לדיונים הן כדי להרחיב עוד את מעגל ההכרות עם תחום הבינה המלאכותית.

494 וראו גם פילוט הטמעת בינה מלאכותית במשרדי ממשלה: https://www.gov.il/he/pages/most_ai_government_agencies_open_call_winners?fireglass_rsn=true#fireglass_params&tabid=afc880ab5bd32cd6&start_with_session.counter=5&application_server_address=isagovil-1-me-west1.prod.fire.glass

495 הצו הנשיאותי.

בהתחשב בכך שעבודת הצוות נעשתה בשלב מוקדם של כניסת הבינה המלאכותית לתחומי הפיננסיים בישראל, ולנוכח ההתפתחויות הטכנולוגיות והרגולטוריות בעולם, המלצה מתבקשת של הצוות היא להמשיך ברתימת משאבים משותפת של משרדי המשפטים והאוצר והרגולטורים לנושא. המשך עבודה של צוות משותף צפוי לסייע מאוד בהתמודדות עם הנושא, ולייצר רציפות מקצועית בתקופה זו בה טכנולוגיית הבינה המלאכותית מתחילה להיות מיושמת בפועל בקרב הגופים הפיננסיים.

במסגרת הערות הציבור לדוח הביניים עלה הצורך בהשקעת משאבים רגולטוריים בנושא ובקידום אסדרת ארגזי החול הרגולטוריים. הצוות מסכים להערות אלה וסבור כי הן קיבלו ביטוי גם בדוח.

להלן סיכום הפעולות הנוספות לקידום רגולציה פיננסית בתחום הבינה המלאכותית:

עידוד חדשנות וביחית פתרונות לבעיית הנגישות למידע

1. עדכון הצעת החוק הממשלתית שעניינה "ארגזי חול רגולטורי" בסקטור הפיננסי, המניחה אסדרה ייעודית ואחודה עבור כלל הרגולטורים הפיננסיים להקמת סביבת ניסוי, והרחבתה לשם הגברת האפקטיביות הפוטנציאלית שלה.
2. לצד עדכון הצעת החוק האמורה, מוצע להקים "ארגזי חול" עצמאיים על ידי כל רגולטור פיננסי בתחום אחריות, וליזום תיקוני חקיקה בדינים הפיננסיים הרלוונטיים כדי לאפשר זאת מקום בו הדין הקיים אינו מתיר זאת.
3. הקמת מוקדי חדשנות על-ידי הרגולטורים הפיננסיים והקדשת משאבים ומיקוד פעילות בתקופה הקרובה ביישומי בינה מלאכותית, נוסף על הקיימים.
4. בחינת פתרונות לבעיית הנגישות למידע, בפרט של גופים קטנים או חדשים, ובכלל זה לבחון את האפשרות להקים או לפתוח מאגרי מידע כבסיס לפעילות בינה מלאכותית.

קידום ודאות רגולטורית והתאמות בדין

5. הגברת הוודאות הרגולטורית בתחום הבינה המלאכותית באמצעות כלים כגון מסמכי מדיניות, מענה לפניית מקדמיות, עמדות פרשניות, שאלות ותשובות, פרסום מדריכים ואזהרות.
6. יש לשאוף לכך שהאסדרה בחוק ובתקנות תשקף את העיקרון של ניטרליות טכנולוגית ותתיר גמישות לפעול באמצעים טכנולוגיים שונים. כמו-כן, ומבלי לגרוע מסמכויות קיימות של הרגולטורים הפיננסיים, מוצע לשקול הקניית סמכויות רגולטוריות לתת הוראות נדרשות על רקע שינויים בטכנולוגיה, להעניק פטורים, ולקבוע הוראות שעה וסעיפי שקיעה (sunset provisions), לשם התאמת הדין לפעילות והגברת הוודאות המשפטית, מקום בו הדבר נדרש.

קידום הפעילות הפיקוחית

7. קידום פעילות פיקוחית מבוססת על טכנולוגיית בינה מלאכותית (Suptech), באמצעות בחינתה כחלק מהאסטרטגיה הכוללת של הרגולטור בנושא מערכות מידע ורתימתן לצרכי פיקוח ואכיפה.
8. הפניית משאבים ממשלתיים, מחוץ למסגרות התקציב הרגילות, כדי לקדם פעילות פיקוחית מבוססת בינה מלאכותית.
9. בחינת עדכון סמכויות קבלת מידע לצרכים של ניתוח, פיקוח ואכיפה.
10. התמודדות באופן סדור ומרוכז עם סוגיות רחב הקשורות בשימוש בבינה מלאכותית במגזר הציבורי ועיצוב מתכונת טיפול אחידה.
11. רתימת משאבים של הרגולטורים הפיננסיים, עידוד התיאום ביניהם, והמשך עבודה משותפת בנושא.



נספח א' – כתב מינוי

22 בדצמבר 2022

כ"ח בכסלו תשפ"ג

לכבוד

עו"ד אמיר וסרמן, היועץ המשפטי, רשות ניירות ערך
עו"ד שרית פלבר, ממונה, ייעוץ וחקיקה (משפט כלכלי), משרד המשפטים
גב' יעל רגב, מנהלת מחלקת טכנולוגיות מידע וסייבר, רשות שוק ההון ביטוח וחסכון
עו"ד דוד קופל, המשנה ליועץ המשפטי (בפועל), משרד האוצר
גב' אילנית מדמוני, מנהלת יחידת החדשנות בטכנולוגיה פיננסית, הפיקוח על הבנקים, בנק ישראל
עו"ד טובי הריס, ראשת צוות פיננסים, מחלקת שווקים, רשות התחרות

מכובדי,

הנדון: צוות לבחינת ההשפעות של מערכות אלגוריתמיות ובינה מלאכותית במגזר הפיננסי

בשנים האחרונות התרחב השימוש בטכנולוגיות של בינה מלאכותית ומערכות אוטומטיות במגזר הפיננסי, והוא מקיף כיום מגוון של פעילויות. מערכות ממוחשבות מבוססות נתונים משמשות יותר ויותר לתהליכי חיזוי, מתן המלצות או קבלת החלטות אוטומטיות. בכך מערכות אלה מבצעות, או מסייעות לבצע, משימות שנעשו בעבר באופן אנושי תוך הפעלת שיקול דעת, כגון קיום ממשקים עם לקוחות וקבלת החלטות בנוגע לעצם מתן השירות ללקוח, אופי השירות ותנאיו. שימוש זה צפוי להמשיך ולהתרחב. כך גם פעילות של למידת מכונה, המהווה ענף מסוים בבינה מלאכותית, במסגרתו הביצוע הממוחשב של פעולות מתבסס על מידע וניסיון מצטברים.

השימוש בבינה מלאכותית ובתהליכים ממוחשבים המסייעים בקבלת החלטות במגזר הפיננסי עשוי לגלם תועלות רבות, ובהן הצעת מוצרים ושירותים טובים יותר ללקוחות, עידוד התחרות, חיסכון בעלויות, ושיפור הפעילות העסקית וניהול הסיכונים של הגופים הפיננסיים. מנגד הוא עלול להציב אתגרים רגולטוריים ומשפטיים לא מבוטלים, חלקם בעלי מאפיינים ייחודיים, בהיבטים כגון התמודדות עם חששות הנוגעים לפרטיות ואבטחת מידע, להטיות בקבלת החלטות, ולפגיעה בתחרות.

בחודש אוגוסט 2022 פרסמה המחלקה למשפט כלכלי בייעוץ וחקיקה דוח אקדמי בנושא "שימושי בינה מלאכותית במגזר הפיננסי". בהמשך לפרסום הדוח ולאחר התייעצויות שקיימו הוחלט להקים צוות משותף לבחינת השפעות השימוש בטכנולוגיית הבינה המלאכותית ותהליכי קבלת החלטות אוטומטיים, ומערכות דומות, במגזר הפיננסי.

בהמשך לכך, הוחלט למנותכם כחברים בצוות האמור.

הצוות יבחן את השלכות הרגולטוריות והמשפטיות שיש לטכנולוגיה על פעילויות ושירותים פיננסיים ויגבש המלצות בעניינה. ההמלצות יעסקו, בין השאר, בצורך באסדרה ובאופן עיצוב האסדרה הראויה, בהבהרות המשפטיות הנדרשות ביחס לדין הקיים, ובחסמים שנדרש להסירם.

בשלב ראשון הצוות יתמקד בשימושים הקשורים לחיתום אשראי וביטוח, ניהול תיקי השקעות ולפעולות ייעוץ, לרבות המודלים בבסיס האלגוריתמים שבשימוש. בהתאם להתקדמות עבודת הצוות, ממצאיו או התפתחויות אחרות – הח"מ יוכלו להנחות את הצוות לשנות או להוסיף נושאים.



סדרי עבודה

בראש הצוות יעמדו עו"ד אמיר וסרמן ועו"ד שרית פלבר. עו"ד תום גולדרייך ישמש כמרכז הצוות. חברי הצוות יקבעו את סדרי עבודתה, ויהיו רשאים להזמין לדיוניו גורמים נוספים ממשרדיהם בהתאם לצורך. הצוות יתייעץ וישמע גורמים רלבנטיים, לפי שיקול דעתו. כן יהיה רשאי הצוות להסתייע בגורמי ייעוץ חיצוניים, לרבות חברות ייעוץ ויועצים אקדמיים (ובכלל זה מחברי הדוח הנזכר מאוניברסיטת תל-אביב). הצוות יקיים ישיבת עדכון עם הח"מ אחת לחודשיים. הצוות מתבקש להגיש את המלצותיו לח"מ בתוך תשעה חודשים מתחילת עבודתו. אנו מודים לכם על נכונותכם ליטול חלק בצוות ומאחלים הצלחה ועבודה פורייה.

בברכה,

מר עמית גל
מ"מ הממונה על שוק ההון,
ביטוח וחסכון

גב' ענת גואטה
יו"ר רשות ניירות ערך

מר יאיר אבידן
המפקח על הבנקים, בנק ישראל

מר אסי מסינג
היועץ המשפטי, משרד האוצר

גב' מיכל כהן
הממונה על התחרות

מר מאיר לוין
המשנה ליועץ המשפטי לממשלה
(משפט כלכלי)



נספח ב' – קול קורא

קול קורא מטעם הצוות הבין-משרדי לבחינת השימוש בבינה מלאכותית ולמידת מכונה במגזר הפיננסי

בדצמבר 2022 החל את עבודתו הצוות הבין-משרדי לבחינת שימושי הבינה המלאכותית (לרבות למידת מכונה) במגזר הפיננסי. הצוות פונה לציבור לקבלת מידע על השימוש הקיים והצפוי בבינה מלאכותית במגזר הפיננסי ובמוסדות פיננסיים. בפרט מבקש הצוות ללמוד על אופי השימושים; התועלות והסיכונים הנובעים משימושים אלה; האתגרים הרגולטוריים, המשפטיים או האחרים שעומדים בפני מפתחים, חברות ומוסדות פיננסיים; וסוגי הפרקטיקות שאומצו להתמודדות עם האתגרים, החסמים והסיכונים הנובעים משימוש אלה.

מועד אחרון להגשת התייחסויות: 1 במאי 2023.

רקע

בשנים האחרונות אנו עדים למגמה הצוברת תאוצה, במסגרתה פעולות שבעבר הצריכו הפעלת שיקול דעת אנושי מתבצעות, בחלקן או במלואן, באמצעים טכנולוגיים תוך שימוש בבינה מלאכותית (Artificial Intelligence) ולמידת מכונה (Machine Learning). כך, אלגוריתמים בעלי רמות שונות של עצמאות שהוגדרה מראש, מסתמכים על סוגים שונים של מקורות מידע בהיקפי עתק, לצורך פיתוח היכולת לבצע מטלות "אנושיות" כגון לימוד, הנמקה, ניבוי תחזיות, גיבוש המלצות, קבלת החלטות ועוד. אמנם, שימושים במודלים סטטיסטיים ותהליכי אוטומציה מסוימים כבר בשימוש במערכת הפיננסית לא מעט שנים, אבל בשנים האחרונות ישנה הרחבה של סוגי השימושים, של מידת ההשפעה שלהם על תהליכי קבלת החלטות וביצוע פעולות, וכן הרחבה ניכרת במידת העצמאות של האלגוריתמים. ההערכה היא כי מגמות אלו ילכו ויגברו. הדבר מחייב היערכות משפטית ואסדרתית (רגולטורית) במטרה לתת מענה לאתגרים ולהזדמנויות, ולבחון האם וכיצד יחולו כללים, קיימים או חדשים, במציאות טכנולוגית משתנה. העיסוק בבינה מלאכותית גובר ככל שניתן להטמיע כלים של בינה מלאכותית ולמידת מכונה במוצרים ובשירותים שונים הנגישים לקהל הרחב. השיא, בוודאי במונחים של חשיפה לקהל הרחב, התרחש לאחרונה עם הופעתו של כלי ה-CHAT GPT (אשר פותח על ידי חברת OpenAI ועושה שימוש במקרה פרטי של בינה מלאכותית – Generative AI). כלי זה יצר עניין וסקרנות חוצי-גבולות ומגזרים, בעודו מסוגל לבצע פעולות ולספק מענה (גם אם חלקי) כמעט בכל תחומי החיים.

בינה מלאכותית במגזר הפיננסי

בשנים האחרונות התרחב השימוש בטכנולוגיות של בינה מלאכותית ולמידת מכונה בכלל ובמגזר הפיננסי בפרט, והוא מקיף כיום מגוון של פעילויות. כלים ויישומים שונים העושים שימוש בבינה מלאכותית מסייעים בידי גופים פיננסיים בניהול סיכונים וקבלת החלטות בדבר מתן המלצות השקעה בשוק ההון, ביצוע ניהול תיקים אוטומטי, חיתום לצורך התקשרות באשראי או ביטוח, מתן שירות לקוחות, הצגת הצעות ערך ללקוחות, יישוב תביעות ביטוח, ועוד.

השימוש בבינה מלאכותית ובלמידת מכונה עשוי לגלם תועלות רבות, ובהן הצעת מוצרים ושירותים טובים יותר ללקוחות, זיהוי הונאות, עידוד התחרות, חיסכון בעלויות, ושיפור הפעילות העסקית וניהול הסיכונים של הגופים הפיננסיים. מנגד, הוא עלול להציב אתגרים רגולטוריים ומשפטיים לא מבוטלים, חלקם בעלי מאפיינים ייחודיים, בהיבטים כגון התמודדות עם חששות הנוגעים לפרטיות ואבטחת מידע, להטיות בקבלת החלטות, להגנת הצרכן ולפגיעה בתחרות. כמו כן, ייתכן כי קיימים חסמים רגולטוריים ואחרים אשר מקשים על הפקת מירב התועלות הפוטנציאליות.

לאור השימוש ההולך וגובר בבינה מלאכותית ובלמידת מכונה במגזר הפיננסי, התפרסם בחודש יולי 2022 מטעם המחלקה למשפט כלכלי ביעוץ וחקיקה במשרד המשפטים דוח אקדמי בנושא "בינה מלאכותית במגזר הפיננסי: שימושים נפוצים, אתגרים וסקירה השוואתית של התמודדות רגולטורית" (להלן – הדוח) אשר נכתב על ידי צוות



חוקרים מאוניברסיטת תל אביב.⁴⁹⁶

כמו-כן, בשנים האחרונות מדינות רבות בעולם השקיעו משאבים בלימוד נושא השימוש בבינה מלאכותית ולמידת מכונה במגזר הפיננסי. כך, מבלי למצות, בארצות הברית, באיחוד האירופי, בגרמניה, בהולנד, באנגליה, בסינגפור, בהונג-קונג, בנוסף לגופים בינלאומיים, כתיבה אקדמית ועסקית וכו'.

הקמת הצוות ומטרותיו

בהמשך לפרסום הדוח וההמלצות העולות ממנו, הוחלט להקים צוות משותף לבחינת השפעות השימוש בטכנולוגיית הבינה המלאכותית ותהליכי קבלת החלטות אוטומטיים ומערכות דומות, במגזר הפיננסי. הצוות מורכב מנציגי משרדי האוצר והמשפטים (ייעוץ וחקיקה), רשות ניירות ערך, הפיקוח על הבנקים בבנק ישראל, רשות שוק ההון ורשות התחרות.

הצוות הונחה לבדוק לעומק את פוטנציאל הפעילות, התועלות, החסמים והסיכונים, ובין היתר לגבש תמונת מצב עדכנית של השימוש בבינה מלאכותית במגזר הפיננסי בישראל (לרבות השימוש בבינה מלאכותית "פשוטה", קרי תהליכים ממוחשבים המסייעים בקבלת החלטות); להעריך את ההשפעה של הבינה המלאכותית על פעילות ושירותים פיננסיים בישראל בהווה ובעתיד הקרוב; לגבש המלצות ביחס לצורך באסדרה ואופן עיצוב האסדרה הראויה (ככל שנדרשת), לרבות הסרת חסמים לפעילות רצויה; וכן לבחון הבהרות משפטיות (ככל שנדרשות) ביחס לדין הקיים זאת תוך שקילת שיקולי מדיניות ואינטרסים נוספים הקשורים במערכת הפיננסית.⁴⁹⁷

קול קורא

- הצוות פונה בזאת לציבור הרחב ולבעלי עניין להעביר מידע ועמדות ביחס לנושאי העיסוק של הצוות, ובכלל זאת:
1. השימושים הנוכחיים והצפויים בבינה מלאכותית בסקטור הפיננסי בישראל, לרבות מידע בדבר סוג המודלים בהם נעשה שימוש (מידת אוטונומיות, תהליך ההתעדכנות של המודלים וכדומה);
 2. החסמים העומדים בפני גופים פיננסיים ואחרים בפיתוח, התנסות ושימוש בבינה מלאכותית (הטכנולוגיים, העסקיים, הרגולטוריים או המשפטיים);
 3. התועלות משילוב טכנולוגיות אלה בעבודת גופים פיננסיים (הפחתת עלויות, שיפור ביצועים, דיוק, התאמה ללקוח והגדלת מגוון, שיפור השירות וההצעות ללקוחות, ניהול סיכונים וכדומה);
 4. האתגרים והסיכונים הכרוכים בשימוש בבינה מלאכותית (ובין היתר בהיבטי יציבות מערכתית, הסבריות (explainability ו/או interpretability) וקופסה שחורה, אחריות וחובות זהירות ואמון, הטיות ומניפולציות על המידע, פרטיות, תחרות, הגנת הצרכן, אבטחת מידע וכו').
 5. האמצעים הננקטים להתמודדות עם האתגרים האמורים ונוספים: כלי ניהול סיכונים, ביקורת אלגוריתמית (Algorithm Audit) כאמצעי להפחתת סיכונים, סיכוני סייבר, עמידה בכללים רגולטוריים ומשפטיים, כגון איסור אפליה וכדומה;
 6. המדיניות והאסדרה הראויות בתחום הבינה המלאכותית במגזר הפיננסי, לרבות בהיבטי פיקוח, אתיקה, רגולציה עצמית, נסיינות, סטנדרטים וכדומה;
 7. נושאים נוספים שעל הרגולטורים והממשלה להידרש אליהם בבואם לבחון את האסדרה של תחום זה.

בהינתן שאין הגדרה מוסכמת ומקובלת למונח "בינה מלאכותית", והיא כוללת בתוכה מגוון טכניקות, נבחר כי בקול קורא זה אנו מתייחסים לבינה מלאכותית במובנה הרחב, לרבות מערכות הכוללות מודלים מתקדמים המעבדים נתונים באופן אוטומטי (מלא או חלקי) לצורך ניפוק תחזיות, המלצות, החלטות וכדומה, וכן מערכות ליצירת תוכן עבור שחקנים בסקטור הפיננסי.

הצוות ישמח לקבל כל מידע רלוונטי, לרבות נתונים, מחקרים ומאמרים בנושא למטרות עבודתו.

⁴⁹⁶ https://www.gov.il/BlobFolder/news/ai_report/he/AI_report.pdf
⁴⁹⁷ <https://www.new.isa.gov.il/nav-index/supervised-publications/news1323>



הפנייה לצוות תעשה בכתב. הצוות יתייחס בכובד ראש לכלל הפניות שיגיעו אליו, ובמידת הצורך יצור קשר עם גורמים שייטלו חלק בהליך, לפי שיקול דעתו.

אנו מזמינים אתכם להשפיע ולקחת חלק בהליך חשוב זה!

נודה לקבלת התייחסותכם עד ליום 1 במאי 2023.

אנא שלחו התייחסותכם לידי עו"ד תום גולדרייך, מרכז הצוות, בכתובת דואר האלקטרוני: tomg@isa.gov.il.



נספח ג' - רשימת הגורמים שהופיעו בפני הצוות

Bloomberg
 European Securities and Markets Authority (ESMA)
 European Commission
 Financial Conduct Authority (FCA)
 Google
 Marie Briere, Dr.
 Mark Fagan, Prof.
 Microsoft
 Organization for Economic Co-operation and Development (OECD)

אורי אליאבייב
 אורי הכהן, ד"ר
 אורלי לובל, פרופ'
 אמפליפייר
 אריאל בן פורת
 בנק One Zero
 בנק דיסקונט
 בנק הפועלים
 בנק מזרחי
 דנה יפה
 הבנק הבינלאומי הראשון
 זיו כהן
 חופית וסרמן רוזן, ד"ר
 חיים רביה
 טליה גיליס, ד"ר
 יואב אבנשטיין
 ירון חזן
 מייקרוסופט ישראל מחקר ופיתוח
 מיכל גל, פרופ'
 ניר גרסון
 עמרי רחום טוויג, ד"ר
 עפרה עמיר, פרופ'
 קתרונה ליגת, פרופ'
 שוקו ביטוח



נספח ד' - ריכוז הערות הציבור לדוח הביניים



shaulski.com

