מדריך לאימוץ טכנולוגיות חדשות על ידי רשויות השלטון בישראל

תהילה שוורץ אלטשולר | גדי פרל

יולי 2024

הצעה לסדר 55

המכון הישראלי לדמוקרטיה

המכון הישראלי
לדמוקרטיה

מדריך לאימוץ טכנולוגיות חדשות על ידי רשויות השלטון בישראל

תהילה שוורץ אלטשולר | גדי פרל

הצעה לסדר 55
יולי 2024

A Guide for the Adoption of New Technologies by Local Government in Israel

Tehilla Shwartz Altshuler | Gadi Perl

עריכת הטקסט: גלית שמאע
עיצוב הסדרה והעטיפה: סטודיו Alfabees
ביצוע גרפי: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים

מסת"ב 978-965-519-457-9

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים:
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

תוכן העניינים

תקציר

הצעה לסדר זו עוסקת בכשלים ובקשיים בהטמעת טכנולוגיות מתקדמות וחדשניות על ידי רשויות השלטון ומציעה מודל בקרה שנועד לסייע לגורמי הרכש והליווי למזער את הסיכונים והכשלים שאנחנו עומדים עליהם.

המסמך עוסק בארבעה מקרי בוחן, שהתרחשו בישראל, בארצות הברית ובהולנד בשנים האחרונות: (א) מערכת לדירוג מורים שהייתה בשימוש בארצות הברית; (ב) רוגלת "פגסוס" בשימוש משטרת ישראל שאפשרה חדירה, העתקה והאזנת סתר לטלפונים של חשודים; (ג) מערכת בינה מלאכותית להכללה של חשודים בהברחת סמים בנמל תעופה בן־גוריון לצורך חיפוש על גופם; (ד) הטמעת מערכות לזיהוי פנים בהולנד. מתוך דיון במקרי הבוחן אנו מצביעים על כשלים חוזרים בהליכי הטמעה אלו. הכשלים כוללים, בין השאר, היעדר דיון רוחבי ותהליכי היוועצות טרם הכנסת הטכנולוגיה לשימוש, חסר בכתיבה ובפרסום של נהלים מסודרים לרכישה ולהפעלה של הטכנולוגיות, ולבסוף גם היעדר מעקב, תיעדוף ותיקוף לאחר יישום הטכנולוגיה, ואף הסתרת הכשלים אחרי שהתגלו בעיות. במסמך אנו מפרטים את הנזק התדמיתי שנגרם למשרדי הממשלה בעקבות הכשלים הנידונים.

אנו מייחסים את הכשלים הללו, בין השאר, לקושי של משרדי הממשלה והרשויות השונות לזהות כי מדובר בטכנולוגיות "משבשות" שעלולות להפר את מערכת היחסים ואת איזון הכוחות בין השלטון לבין האזרחים, וכי אין מדובר בכלים טכנולוגיים משופרים גרידא. קושי זה הביא את משרדי הממשלה שלא להבחין בקשיים שהתעוררו במהלך הדרך ולהיעדר הקפדה על תהליכי הטמעה, שהיו מקובלים בעבר.

כפתרון, אנו מציעים מודל תלת־שלבי לפיקוח על תהליכי הרכש וההטמעה של טכנולוגיות מתקדמות ברשויות:

(**1**) **בזמן הליך הרכש**: מילוי "שאלון סיכון ושיבוש" וכינוס "פורום הערכת השפעות" במקרה של חשש מטכנולוגיה משבשת.

(2) **טרם הטמעת הטכנולוגיה**: בדיקת התאמת נהלים, ציפיות מול ביצועים, איכות התוצר ובניית מעטפת ארגונית.

(3) **במועד מוגדר מראש לאחר כניסת הטכנולוגיה לשימוש**: וידוא שהציפיות מתממשות ושלא מתגלות תקלות או השפעות לא צפויות.

המודל המוצע מבקש ליצור הליכי בקרה ושקיפות שימנעו הטמעה לא מיטבית של טכנולוגיות ויגבירו את האמון הציבורי הן בטכנולוגיה והן בגורמים המפעילים אותה. זאת, באמצעות שילוב של הערכת השפעות, ניהול סיכונים, תיעוד קפדני והתייחסות למעגל החיים של מערכות טכנולוגיות.

מבוא

רשויות השלטון ומשרדי הממשלה בישראל ובעולם, ובכללם גם רשויות אכיפת חוק, שואפים תמיד לשיפור היכולות והאמצעים העומדים לרשותם באמצעות רכישת טכנולוגיות חדשות והטמעתן. כך למשל, משטרת ישראל מרחיבה את יכולותיה הטכנולוגיות כמענה לשינויים בעולם הפשיעה,[1] ומשרד הפנים מאפשר קבלת שירותים מרחוק בהסתמך על הזדהות מקוונת.[2]

הטמעת טכנולוגיות חדשניות מלווה בציפייה לשיפור עבודת הרשויות וייעולה, לטיוב השירות שניתן לאזרחים ולחיסכון תקציבי. אולם בצד הפוטנציאל המבטיח, תהליכים אלה מלווים בסיכונים. כפי שעולה ממחקרים ומניסיון העבר, קיים חשש כי בעקבות כשלים שונים – החל בחיסכון תקציבי בעת בחירת הטכנולוגיות, עובר באפיון לקוי שלהן וכלה בהטמעה לא ראויה – תהליכי טרנספורמציה דיגיטלית והטמעת טכנולוגיות מיכון עלולים להביא עימם דווקא ירידה באיכות, הרעה בשירות וחמור מזה – פגיעה בזכויות האזרח.

כדי לתת מענה לחששות בדבר כשלים בהטמעת טכנולוגיות, התפתחו בשנות התשעים ובראשית שנות האלפיים – בחסות המטרייה המחקרית של "New Public Management" (להלן: NPM)[3] – מתודולוגיות ושיטות פעולה שנועדו

1 דוגמה לחשיבות אימוץ טכנולוגיה מתקדמת במשטרה עולה מדבריו של המפכ"ל לשעבר רוני אלשיך בדיון בכנסת:

> הדבר השני שחשוב לומר אותו, העיקרון של רצף טכנולוגי לאורך המשטרה ולא רק לפנק יחידות ארציות, אלא בעצם לייצר מצב שכל המשטרה מחוברת לטכנולוגיה, מלמעלה עד למטה, ונהנית מהרצף הטכנולוגי שהוא מקבילה לרצף המודיעיני. הוא מכפיל כוח עצום והוא מאפשר לנו לטפל בדברים שבעבר לא ניתן היה לטפל, כי הקשב של היחידות הארציות לא יכול להיות באירועים שננים ברחוב, אבל הטכנולוגיה יכולה להיות שם ולאפשר לתחנה לקבל העצמה. עשינו קפיצת מדרגה משמעותית בתחום הזה.

מתוך פרוטוקול ישיבת ועדה של הכנסת ה־20 "טכנולוגיות מתקדמות בשירות משטרת ישראל" (5.2.2028).

2 החלטה 2960 של הממשלה ה־34 "אישור המדיניות הלאומית להזדהות בטוחה" (6.8.2017).

3 Jan-erik Lane, New Public Management: An Introduction (2002)

להבטיח כי שדרוג יכולות הממשלה ייעשה מתוך שמירה על עקרונות דוגמת שקיפות, זכויות אזרח וביקורת ציבורית. לפיכך הוגדרו עקרונות מסוג זה ביסוד תוכניות, כגון "ממשל זמין"[4] או "ישראל דיגיטלית";[5] נקבעו הליכים הדורשים היוועצות בין־משרדית, שיתוף הציבור וועדות מקצועיות; ואף נוסדו גופים מתווכים בעלי מומחיות בתחום הטכנולוגי. רשות החדשנות פועלת לפי עקרונות אלו כיום,[6] ולאחרונה אף פורסם מסמך מדיניות משותף למשרד המדע ולמשרד המשפטים הקורא להקפדה על עקרונות אלו בעת הטמעת טכנולוגיות חדשות בכלל וטכנולוגיות המבוססות על בינה מלאכותית בפרט.[7]

בהצעה לסדר זו נעמוד על התופעה של כשלים בהטמעת טכנולוגיות חדשות בקרב רשויות ציבוריות ונציע ארגז כלים אשר נכון לאמץ בשלב תהליכי ההטמעה. נתמקד בטכנולוגיות מתפרצות, כלומר כאלה שנמצאות בשלבי התהוות ובעיקר בטכנולוגיות שנועדו להעניק לרשות שלטונית יכולת חדשה שלא הייתה בידיה,[8] או כאלה שביכולתן להפר את איזון הכוחות הקיימים בין האזרח לבין השלטון.

בהצעה זו נבחן שלושה מקרים שהסתיימו בכישלון תהליכי הטרנספורמציה הדיגיטלית ומקרה רביעי המשמש דוגמה להצלחה. נבהיר תחילה כי בדיקת שלושת מקרי הכישלון **לא חשפה** מעשי שחיתות או שיקולים זרים, **ולא העלתה** כי נעשה שקלול מודע של אמצעים פוגעניים או מטרות לא לגיטימיות בעת

4 על הפרויקט אפשר ללמוד ממסמכי מבקר המדינה. ראו מבקר המדינה **דוח שנתי 59ב לשנת 2008 ולחשבונות שנת הכספים 2007** (2009).

5 החלטה 1046 של הממשלה ה־33, "המיזם הלאומי 'ישראל דיגיטלית': גיבוש מדיניות לאומית לשימוש בטכנולוגיות מידע ותקשורת כחלק מאסטרטגיה חברתית כלכלית" (15.12.2013).

6 "ישראל חייבת לפתח גישת רגולציה מאפשרת, שתביא להטמעת חדשנות במגזרים הציבוריים והפרטיים בשוק המקומי לטובת הפריון בכלל ענפי המשק מחד, ויצירת 'ארגזי חול' אשר יקנו יתרון תחרותי להיי־טק המקומי מאידך", מתוך רשות החדשנות, **דבר יו"ר הרשות והמנכ"ל לדוח שנת 2022** (2023).

7 משרד החדשנות, המדע והטכנולוגיה ומשרד המשפטים "עקרונות מדיניות, רגולציה ואתיקה בתחום הבינה המלאכותית 2023" (דצמבר 2023).

8 לפירוט על הטכנולוגיות ראו **להלן**, פרק שני.

בחירת הטכנולוגיות, פיתוחן והטמעתן. הכשל העיקרי שעלה הוא שהגורמים האחראים לאימוץ טכנולוגיה חדשה התייחסו אליה רק כאל שיפור של מערכות קיימות, ולא היו מודעים לאופנים מרחיקי הלכת שבהם משנה הטכנולוגיה את היכולת הקיימת או מערערת את סדרי הכוחות הקיימים. תופעה זו הובילה לאי־הפעלתן של מערכות בקרה נדרשות, ובראשן הערכת סיכונים לפגיעה בזכויות והטמעת תקני בקרה מקצועיים. לתפיסתנו, כשל חוזר ונשנה זה ניתן למניעה, הן באמצעות זיהוי מראש של טכנולוגיות שעלולות לגרום לשיבוש חברתי, כלכלי או משפטי גם אם יופעלו באופן תקין, והן באמצעות איתור טכנולוגיות שהפעלתן באופן לא תקין תביא עימה מגוון סיכונים.

שלושת מקרי הבוחן שהסתיימו בכישלון אירעו בשנתיים האחרונות בארץ ובארצות הברית. במסגרתם הוטמעו טכנולוגיות מתקדמות שהקנו לרשויות שלטוניות יכולות שלא היו בידיהן קודם לכן או טכנולוגיות שהעבירו למכונות את שיקול הדעת שהיה נתון עד אז בידי פקידים.[9]

מקרי הבוחן נבדלים זה מזה בטכנולוגיות שהוכנסו לשימוש, במדינות שבהן התרחשו, בתחומי המשפט (אכיפת חוק, דיני עבודה וכדומה) ובקשיים שהתגלו בשלבים השונים. עם זאת, כפי שנראה, לכולם מכנה משותף: כניסתן של הטכנולוגיות נעשתה באופן חפוז, ללא הליך בדיקה סדור לבחינת ההשלכות של השימוש בהן וללא הערכת סיכונים, אגב הסתפקות בבחינה מקצועית על ידי גורמים משפטיים שלא היו בקיאים ביכולות הטכנולוגיות, ללא דיון ציבורי וללא פיקוח פרלמנטרי.

בעקבות זאת, במקום התועלות הצפויות, נפגעו זכויות אדם בסיסיות: בארצות הברית אירעו פיטורים שלא כדין, ובישראל – חריגה מהוראות חוק האזנת סתר, פגיעה לא מידתית בצדדים שלישיים, משבר אמון קשה כלפי רשויות השלטון וכן אפליה נגד קבוצה מוחלשת.

9 המונח "בינה מלאכותית" הוא שם אב לכמה טכנולוגיות ומתודות סטטיסטיות, הכוללות גם למידת מכונה. במאמר זה לא נוכל לעסוק באבחנות השונות. להסבר על אודות הטכנולוגיה ראו Uday Kamath & John Liu, Explainable Artificial Intelligence : An Introduction to Interpretable Machine Learning (2021)

חשוב להדגיש כי מחקר זה אינו מתמקד רק בטכנולוגיות המבוססות על בינה מלאכותית, העומדות לאחרונה במוקד שיח העוסק באתגרים הרגולטוריים שהן מציבות. בהגדירנו מהי טכנולוגיה חדשה או מתפרצת אנו מתמקדים בשאלה אילו יכולות חדשות ושינוי דפוסי פעולה קיימים היא מעניקה לרשות המדינתית המטמיעה אותה.

להלן פירוט מבנה ההצעה לסדר: בפרק הראשון נסקור תאוריות קיימות בנוגע להטמעת טכנולוגיות על ידי גופים ציבוריים בעולם, ונבחן כיצד השיח הקיים עוסק בפוטנציאל של טכנולוגיות אלו לשפר את פעילות הגופים הממשלתיים. בפרק השני, נסקור שלושה מקרי בוחן שהסתיימו בכישלון ומקרה בוחן רביעי שהסתיים בהצלחה, ונתמקד בסיבות שהובילו לשילוב הטכנולוגיות בפעילות הגורמים הממשלתיים, בדרכי האישור לקראת השימוש בהן ובכשלים שאירעו הלכה למעשה. בפרק השלישי נציע הסבר אפשרי לכישלונן של המערכות מנקודת המבט של טכנולוגיות משבשות. בפרק הרביעי נרחיב על אודות מקורות ההשראה למודל שיאפשר פיקוח ומניעת הכשלים. בפרק החמישי והאחרון נתאר מנגנון תלת־שלבי שאנו מציעים לפיקוח על השימוש שעושים גופים ציבוריים בטכנולוגיות מורכבות ומערערות: השלב הראשון, בתחילת תהליך הרכש; השלב השני, בעת הכניסה הראשונית לשימוש והשלב השלישי, במועד שייקבע אחרי שהטכנולוגיה תיכנס לשגרת שימוש.

פרק 1

תהליך אימוץ טכנולוגיות חדשות "מן הדור הראשון" על ידי רשויות השלטון והפיקוח עליו

טכנולוגיות שנחשבות כיום בסיסיות ומובנות מאליהן, כגון אתרי אינטרנט ממשלתיים ומתן שירותי תשלום מקוונים במקום הגעה לאתרים פיזיים, נכנסו לשימוש בסוף שנות התשעים ובראשית שנות האלפיים. הן היו חדשניות מאוד בזמנן, וכניסתן הייתה בגדר מהפיכה בשירותי הממשלה. יעילותן ויתרונותיהן, בעיקר בהיבט החיסכון הכספי, היו ברורים: (א) חיסכון ניכר במשאבים ובכוח אדם ושיפור זמינותו של השירות הציבורי מעבר לשעות פעילות מצומצמות; (ב) ביטול הצורך בהעסקת מרכזנים ומוקדי קבלת קהל ובמקומם בניית אתרי אינטרנט ממשלתיים. יתר על כן, נטען כי הדבר ישפר אף את המנגנונים הדמוקרטיים בשלוש דרכים עיקריות: (א) הפחתת העלויות של הפצת המידע הקלה את זמינותו של המידע ואת הנגשתו עבור האזרחים ונתפסה כבעלת פוטנציאל להגברת השקיפות השלטונית ולקידום תקשורת מהירה בין הממשלה לבין האזרחים;[10] (ב) מחשוב של מערכות הממשל נתפס כאמצעי שביכולתו לאפשר להגביר את הפיקוח על משרדי הממשלה, אשר יהיו זמינים לבדיקה בכל עת;[11] (ג) טכנולוגיות מידע נתפסו ככאלה שיגבירו מעורבות ציבורית במעשי השלטון, ובכך יגבירו את רמת הלגיטימציה הדמוקרטית.[12]

כבר בעת כניסתן של טכנולוגיות אלה ניטש ויכוח אקדמי ורגולטורי בנושא החשש כי הן לא ישפרו את השירות בפועל, לא יביאו לחיסכון כספים ואף יגרמו לפגיעה בזכויות אזרח, בעקבות מגוון כשלים. נטען כי לצד התועלות, התקציביות

10 כרמית הבר **ממשל פתוח מקוון בישראל: הזדמנויות ואתגרים** (המכון הישראלי לדמוקרטיה, 2012).

11 תהילה שוורץ אלטשולר **מדיניות ממשל פתוח בישראל בעידן הדיגיטלי** (מחקר מדיניות 91, המכון הישראלי לדמוקרטיה 2012).

12 Arianna Bove, *Politics without Romance? The Pursuit of Consent in Democracy*, 46 HIST. EUR. IDEAS (2020)

והדמוקרטיות, קיימים חששות תהליכיים ומהותיים. ברמה התהליכית מדובר למשל בחשש מהתמקדות יתר ביעילות כלכלית על חשבון שיפור איכות השירות שניתן לאזרחים;[13] בחשש מכניסה מהירה מדי ולא איכותית של הטכנולוגיה; ובפגיעה באיכות השירות בזמן תהליך הדיגיטציה.[14] ברמה המהותית עלה החשש שדיגיטציה וריחוק של הפקידים מהעבודה שעשו בעבר יפגעו באחריותיותם כלפי החלטותיהם,[15] לנוכח הסתמכות יתר על המערכות ו"האשמת המכונה"; חשש מפני בורות דיגיטלית וחוסר הבנה של הפקידים בנושא דרך הפעולה של מערכות טכנולוגית ואופן הפעלתן.[16] חשש נוסף שהועלה היה הפגיעה בהליך הדמוקרטי עצמו[17] בעקבות כניסת טכנולוגיות שיבטלו את תהליך השיג ושיח הדמוקרטי ויעמידו בפני האזרחים מציאות מוגמרת שקובעת "המכונה".

לפיכך נטען כי יש לפתח ארגז כלים רגולטורי ומערכות בקרה, שתכליתם תהיה להבטיח כי הליכי דיגיטציה, מיכון והטמעת טכנולוגיות חדשניות, אכן יביאו לשיפור השירות לאזרח ולטיוב מערכת היחסים בין הממשלה לבין האזרחים.[18] בפרק זה נסקור את התפתחות הכלים הרגולטוריים ומערכות הבקרה אשר יועדו לתת מענה לחששות מפני כניסת טכנולוגיות חדשות, כבסיס לדיון בשאלה מדוע כשלו מערכות בקרה אלה בשלושת מקרי הבוחן, שנעסוק בהם בפרק הבא.

אחד המקורות התאורטיים העיקריים לדיון בכלים הרגולטוריים ובמנגנוני הבקרה הנדרשים במנהל הציבורי באופן כללי הוא ספרם המכונן של ג'יימס ביוקנן וגורדון טולוק שעוסק ב"תאוריית הבחירה הציבורית".[19] ביוקנן מונה

13 Vincent Homburg, *E-government and NPM: A Perfect Marriage?* 60 ACM International Conference Proceeding Series (2004)

14 Ryan Calo & Danielle Keats Citron, *The Automated Adminstrative State: A Crisis of Legitimacy*, 70 Emory Law J. (2021)

15 Homburg, **לעיל** ה"ש 13; Calo & Citron, **לעיל** ה"ש 14.

16 **שם**.

17 Bove, **לעיל** ה"ש 12.

18 שוורץ אלטשולר, **לעיל** ה"ש 11.

19 James M. Buchanan, *The Calculus of Consent : Logical Foundations of Constitutional Democracy*, The Calculus of Consent (1965)

כמה כשלים בתהליך קבלת ההחלטות השלטוני. הראשון הוא היעדר בקיאות ומודעות של הציבור הרחב לגבי תהליכי קבלת ההחלטות, מצב שמאיין את יכולתו לפעול נגד החלטות המזיקות לו. השני הוא כוח יתר של קבוצות לחץ ואינטרסים, המביאות תוצאות מיטיבות עבור עצמן על חשבון כלל הציבור. השלישי הוא נטייתם הטבעית של פוליטיקאים לשאת ולתת ברוח "תן וקח" במטרה להגיע לתוצאה כוללת מיטיבה, גם אם במהלך הדרך הם מתפשרים על עקרונות, פשרה שבסופה מזיקה לציבור. הרביעי הוא אינטרסים פרטיים ורצון לקידום אישי וכלכלי של פקידי ציבור המשפיעים על קבלת החלטותיהם.

לדעתנו, כשלים אלו מתרחשים בתהליכי קבלת ההחלטות לגבי שינויים טכנולוגיים ובעת תהליכי הקליטה וההטמעה של הטכנולוגיות החדשניות. כשלים נוספים עשויים להיות: היעדר בקיאותם של מקבלי ההחלטות בטכנולוגיות ובמשמעותן (ראו להלן); ושאיפה לחיסכון כספי בלי לבחון נזקים לא כספיים שעשויים להתרחש.

החששות והכשלים הפוטנציאליים שהתעוררו על רקע הדיון בתאוריית הבחירה הציבורית בהקשר של כניסת טכנולוגיות חדשניות נדונו במסגרת שיח נרחב יותר, שעסק בקשיים של בניית מערכת ניהול מודרנית, גדולה ומורכבת יותר מזו שהייתה בעבר. הפקידות הציבורית שהייתה בנויה כמערכת היררכית נתונה, נדרשה כעת לספק שירותים ממשלתיים מתוחכמים ומורכבים הרבה יותר מאלה שסיפקה בעבר.

אין זה מפתיע אפוא שתאוריית NPM,[20] שעסקה בבניית שירות ציבורי מודרני גדול ומורכב יותר, הביאה חוקרים רבים לעסוק בנושא במטרה לפתור את הכשלים הפוטנציאליים בהטמעת שינויים טכנולוגיים. הם עשו זאת באמצעות מיפוי ההליכים השונים המרכיבים יחדיו את תהליך הדיגיטציה, יצירת דגשים בתהליך

20 Lane, **לעיל** ה"ש 3. לעניין התפתחות התאוריה ראו Janet V. Denhardt & Robert B. Denhardt, The New Public Service: Serving, Not Steering (2016). ניסיונות לשיפור איכותו של השירות הציבורי ניתן למצוא כבר במחקר מוקדם, ראו Woodrow Wilson, *The Study of Administration*, 56 Polit. Sci. Q. (1941)

והנחלת עקרונות מרכזיים שישמשו בסיס לתהליך כולו.[21] חלק מן הפרסומים עסקו במיפוי הליך הדיגיטציה וסייעו להגדיר את הקשיים בכל שלב ושלב. כך למשל מיפתה קארן ליין את הליך הדיגיטציה של משרדי ממשלה וחילקה אותו לארבעה שלבים,[22] לפי סדר החשיבות ועומק הליך המחשוב שמתבצע בהם.[23] אלה ארבעת השלבים: (א) יצירת "נראות מקוונת" למשרדי הממשלה, בעיקר באמצעות הקמת אתר אינטרנט והנגשת מידע; (ב) מתן אפשרות לבצע פעולות מקוונות שקודם לכן דרשו הגעה פיזית; (ג) דיגיטציה מלאה של תהליכים שקודם לכן דרשו מילוי טפסים ידניים או פעולות אנלוגיות; (ד) אוטומטיזציה ומיכון של תהליכים שלטוניים, כגון החלפת תהליכי עדכון ידניים בשאיבת מידע אוטומטית מתוך מאגרים.

ראיין קאלו עסק גם הוא בעקרונות הנדרשים בתהליך הדיגיטציה השלטונית, במטרה לוודא שהפתרונות שייבחרו יהיו לא רק יעילים, אלא גם ישמרו על זכויות אזרח ויעצימו הליכים דמוקרטיים.[24] קאלו הגדיר שלושה עקרונות עיקריים: (א) הליך אימוץ הטכנולוגיה ייעשה בשקיפות מול האזרחים, וההגבלות וההזדמנויות יהיו ברורים ככל האפשר; (ב) פעולה רוחבית ועידוד שיתוף פעולה בין־משרדי, כדי לחלוק מידע, להעשיר את הליך קבלת ההחלטות ולוודא אחידות בין המשרדים; (ג) הטמעת תהליכי בקרת איכות בתהליך כדי לוודא שטובת הציבור לא תוקרב לטובת אינטרסים צרים של מהירות או רווח אישי וכן גיבוש תהליכי תקינה שתוודא איכות ניתנת למדידה.

21 לגבי מאפייני "New Public Management" מומלץ לפנות לתיאור המצב הקיים אצל Gerhard Hammerschmid et al., *A Shift in Paradigm? Collaborative Public Administration in the Context of National Digitalization Strategies*, Governance 1–5 (2023)

22 Karen Layne & Jungwoo Lee, *Developing Fully Functional E-government: A Four-Stage Model*, 18 Gov. Inf. Q. (2001)

23 מיפוי דומה ניתן למצוא גם אצל Oreste Signore, Franco Chesi, & Maurizio Pallotti, *E-Government : Challenges and Opportunities*, 1 Telematica (2005)

24 Calo & Citron, **לעיל** ה"ש 14.

גם גארי מרצ׳נט[25] סבר כי הואיל ואימוץ טכנולוגיות מתקיים בתנאי אי־ודאות, הן לגבי מורכבות התוכנה והן לגבי דרכי התפתחותה ויישומה, קיומו של דיון רוחבי, המשלב בתוכו גורמים מדיסציפלינות שונות ומנקודות מבט שונות, מהותי לשם הצלחת התהליך. יתר על כן, במקום אחר טענו גארי מרצ׳נט וונדל וולאך כי איתור השחקנים הרלוונטיים והבאתם לשיח פורה, הם הכרחיים,[26] בייחוד כשמדובר ברכש טכנולוגי, על רקע רמת האוריינות הדיגיטלית המשתנה בין השותפים. לעיתים, גורמים מומחים בהליכי רכש או אנשי בקרה משפטית, על אף מומחיותם המרשימה בתחומיהם המקצועיים, אינם בקיאים בטכנולוגיות האמורות, ולפיכך הם נסמכים על הסבריהם של אנשי טכנולוגיה ומחשוב הזמינים להם במסגרת עבודתם. ההתגברות על "פערי שפה" בין דיסציפלינות חשובה מאוד וניתנת להשגה רק באמצעות שולחנות משותפים רב־תחומיים.

אכן, עקרונות דומים לאלה שסקרנו כאן יושמו בהליכי דיגיטציה והטמעת טכנולוגיות חדשניות במדינות השונות, דוגמת פרויקט "ממשל זמין" בישראל[27] ו־e–government באירופה.[28] באיחוד האירופי הוקמו רשויות מרכזיות שעסקו בבקרת איכות, בכתיבת כללים ובבקרה על התקדמות תוכניות דיגיטציה.[29] כך למשל הוקמה באירופה רשות אבטחה שתפקידה היה לוודא אחידות בכללים בכל הנוגע להגבלות גישה ולאבטחת מידע וסייבר. הודגש הצורך בהיוועצות בין־

25 Gary E. Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 Vand. L. Rev. 1861 (2020)

26 Wendell Wallach & Gary Marchant, *Toward the Agile and Comprehensive International Governance of AI and Robotics*, 107 Proc. IEEE (2019)

27 כך למשל, במסגרת ממשל זמין בישראל, ראו דנה צימרין "ממשל זמין בישראל: תמונת מצב" **מקושרים: פוליטיקה וטכנולוגיה בישראל**, 101–136 (2011).

28 לסקירה על הגופים שהוקמו, על היחסים הפוליטיים בין הארגונים ועל היישום של מתודולוגיית הממשל באירופה, ראו סקירה כוללת בספר: Paul G. Nixon, Vassiliki N. Koutrakou, & Rajash Rawal, Understanding E–government in Europe: Issues and Challenges (2010)

29 כך למשל ראו במערכת הממשל האלקטרוני של האיחוד האירופי European Commission, *eGovernment and Digital Public Services*

משרדית,[30] ונוסדו שולחנות עגולים שעסקו ביצירת שיח משותף ושיתוף מידע בין גופים שונים, בהנחה שפעולות דומות נעשו על ידי המשרדים השונים, גם אם בזירות שונות.

גופים שהוקמו לצורך הטמעת טכנולוגיות התקיימו בישראל לאורך שנים, למשל בדמות מערכת שבעבר נקראה "תשתית הממשלה לעידן האינטרנט" (תהיל"ה), אשר הייתה חלק מיחידת ממשל זמין (וברבות הזמן הפכה לישראל דיגיטלית), והייתה אמונה על הפצת מידע ממשלתי באינטרנט ועל אבטחת שירותים דיגיטליים למוסדות הממשלה; וכן בחקיקה המחייבת הנגשת אתרי ממשלה לאנשים עם מוגבלויות בהתאם לחוק שוויון זכויות לאנשים עם מוגבלויות.[31]

אנו רואים אפוא כי במהלך הטמעתן של טכנולוגיות חדשניות בראשית שנות האלפיים התפתחו כמה מנגנוני בקרה, כגון שקיפות כלפי הציבור ותהליכי בקרת איכות פנים־ממשלתיים, שנועדו להבטיח עמידה ביעדי יעילות בד בבד עם שמירה על זכויות אדם. מנגנוני בקרה אלה היו אמורים להמשיך לשמש את המגזר הציבורי גם ב"דור השני" של רכישת טכנולוגיות, בעשורים השני והשלישי של המאה העשרים ואחת, ובייחוד בעת הטמעת מתקדמות יותר מאשר דיגיטציה, כגון טכנולוגיות אוטומציה ובינה מלאכותית.[32]

מאז החלטת ממשלה 212,[33] כלל משרדי הממשלה, בהובלת רשות החדשנות ובסיוע משרד המשפטים, עוסקים בבניית נהלים ובהתאמה לשילוב יכולות

30 Hammerschmid et al., **לעיל** ה"ש 21.

31 פרק ה, חוק שוויון זכויות לאנשים עם מוגבלויות, התשנ"ח–1998.

32 על הזרות של מערכות בינה מלאכותית, למשל בהקשר של מודולי שפה, ראו Emily M. Bender et al., *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?* FAccT 2021: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (2021)

33 החלטה 212 של הממשלה ה־36 "תכנית לקידום חדשנות, עידוד צמיחת ענף ההייטק וחיזוק המובילות הטכנולוגית והמדעית" (1.8.2021).

בינה מלאכותית במגזר הפרטי ובמגזר הציבורי.[34] משרד התחבורה אף ביצע שינוי חקיקתי כדי לאפשר כניסת כלי רכב אוטונומיים.[35] הליכים אלו מבוצעים באמצעות שיח רגולטורי ער, הכולל ימי עיון[36] והתייעצויות עם מומחים. משרדי הממשלה, ובראש ובראשונה משרד המשפטים,[37] משרד התחבורה[38] ומשרד הבריאות[39] מפרסמים מידע בדבר השינויים הרגולטוריים הנדרשים. עם זאת בפרק הבא נראה כי קיימים פערים בין העקרונות לבין יישומם בפועל.

34 **לעיל** ה"ש 7.

35 חוק לתיקון פקודת התעבורה (מס' 130), התשפ"ב–2022.

36 למשל משרד התחבורה והבטיחות בדרכים "יום עיון השלכות עידן הרכב האוטומטי על שימושי הקרקע והתכנון העירוני" (16.10.2018).

37 **לעיל** ה"ש 7.

38 משרד התחבורה והבטיחות בדרכים "התחבורה חכמה, פעילות ותחומי המיקוד של משרד התחבורה והבטיחות בדרכים בתחום התחבורה החכמה" (23.09.2019).

39 משרד המדע והטכנולוגיה "מדיניות רגולציה ואתיקה בתחום הבינה המלאכותית בישראל" (30.10.2022).

פרק 2

שלושה מקרי בוחן של כשלים באימוץ טכנולוגיות חדשות "מן הדור השני" ומקרה בוחן של הצלחה

בפרק זה נציג ארבעה מקרי בוחן: שלושה מהם מלמדים על כשלים בעת הכנסת טכנולוגיות חדשניות, שהעניקו לרשויות שלטוניות יכולות שלא היו בידיהן קודם לכן. מקרה הבוחן הרביעי מלמד על הצלחה בתחום זה.

מקרי הבוחן נבדלים זה מזה בטכנולוגיות שבהן מדובר: במקרה הראשון מדובר באלגוריתם לדירוג תפקוד מורים, שדרך פעולתו הוסתרה; במקרה השני מדובר ברוגלת מעקב שייחודה בכך שהעניקה לרשות אכיפת חוק יכולות מהותיות שלא היו בידיה בעבר; במקרה השלישי מדובר בשימוש בבינה מלאכותית שאופן פעולתה לא היה ידוע לגורמי האכיפה שהפעילו אותה. במקרה הרביעי מדובר בזיהוי פנים מבוסס בינה מלאכותית. מקרים אלה נבחרו דווקא בשל השונות ביניהם, כדי להמחיש שאין מדובר בקושי הנובע מטכנולוגיה ספציפית.

במהלך הפרק נראה שאף שמדובר בטכנולוגיות שונות, בנסיבות שונות ובמשטרים שונים – בשלושת מקרי הבוחן הראשונים רצף האירועים דומה: הטכנולוגיה הוטמעה ללא שקיפות ציבורית, ללא שיתוף פעולה בין־משרדי וללא אמות מידה (סטנדרטים) ברורות למדידה ולהערכה של הצלחה.

מאפיין משותף נוסף של שלושת המקרים הוא היעדר תיעוד גלוי של פעולות הרכש של הטכנולוגיות. בעקבות זאת קיים מיעוט מקורות שניתן להסתמך עליהם לצורך ניתוח הליך ההטמעה. מדובר במאפיין חשוב שיש לעמוד עליו כבר עתה. כפי שניתן יהיה לראות בהמשך, אין בידי יצרן הטכנולוגיה מסמכים המתעדים את דרך פעולתה, ולא נוצרה או נדרשה מערכת תקנים מסודרת ושקופה למדידת הצלחתה. המידע על אודות הטכנולוגיה מתגלה רק בהתקיים עתירה לביקורת שיפוטית או באמצעות ביקורת ציבורית בדיעבד שמקורה בתקשורת, ולכן גם היקף הגילוי מצומצם להקשרים ספציפיים.

נתאר להלן את נסיבות הטמעת הטכנולוגיה לגבי כל אחד ממקרי הבוחן, בהתייחס לתחום המשפטי שהופעלה בו (פלילי, אזרחי או מנהלי), לאמצעים החדשים שהעמידה בידי השלטון ולהשלכות השימוש בה, ובכלל זה זכויות האדם של מושאי השימוש בטכנולוגיה. נדון בדרך שבה נכנסה הטכנולוגיה לשימוש ונתמקד בשאלות הנוגעות לגורם המוסדי שהטמיע אותה, לגורם שפיתח אותה ולמידע הקיים על אודות דיונים שהתקיימו בתהליך ונבחן אילו גורמי ממשל השתתפו בהם.

א. מקרה בוחן ראשון: מערכת לדירוג של איכות מורים בארצות הברית

בשנת 2017 נדונה בארצות הברית עתירה בנושא מערכת טכנולוגית לדירוג של איכות מורים. ארגון המורים של מחוז יוסטון דרש לבטל פיטורים של מורים בטענה שהמערכת לבדה היא שקבעה כי הישגיהם נמוכים.[40] עיקר המידע הקיים בנוגע למקרה הבוחן מקורו בעתירה זו ובהחלטה בעניינה, אך מתווסף לו מידע שהתפרסם במאמרים העוסקים בביקורת על מערכות מדידה כאלה שראו אור זמן קצר לפני העתירה ואף אחריה.[41]

בהתאם לעתירה, בשנת 2010 החל מחוז יוסטון בטקסס בהליך מדידה של איכות המורים בבתי הספר הציבוריים, בהתבסס על שלושה קריטריונים: (א) איכות ההוראה (instructional practice), כולל חוויית התלמידים מדרך ההוראה;[42]

40 Houston Federation of Teachers, Local 2415 v. Houston Independent School District, 251 F. Supp. 3d 1168 (S.D. Tex. 2017)

41 Audrey Amrein-Beardsley & Tray Geiger, *Methodological Concerns about the Education Value-added Assessment System (EVAAS): Validity, Reliability, and Bias*, 10 Sage Open 2158244020922224 (2020)

42 Roseanne Elizabeth Ansell et al., *Leading Transformational Experiences for K-8 Teachers: How to Build Capacity to Implement*

(ב) התנהלות המורה ואיכותה בהתאם לציפיות המקצועיות ממנו (professional expectations);[43] (ג) שיפור רמת ביצועי התלמידים (student performance).

נרחיב לגבי הקריטריון השלישי הרלוונטי לענייננו. לכאורה מדובר במדד פשוט, המכונה "value added model",[44] ובוחן את הישגיהם של התלמידים בבחינות לפני שנת ההוראה הנמדדת ואחריה. ככל שהשיפור גבוה יותר, כך ציוניו של המורה צריכים לעלות. עם זאת, בפועל קשה להסתמך על מדד זה להערכה פשוטה של איכות ההוראה, לאור קיומם של משתנים חיצוניים רבים שעלולים להשפיע על הצלחת התלמידים שהם מחוץ לשליטתו של המורה. כך למשל, כיתה המאופיינת בשיעורי הצלחה גבוהים ממילא תראה שיפור נמוך, גם אם מדובר במורה איכותי, וכיתה ששיעורי הצלחתה נמוכים ונמצאת באזור מצוקה שבו קשה לשמר הישגים, לא תראה שיפור, גם אם המורה השקיע מאמץ רב בתלמידים. לפיכך, חיפשו רשויות הפיקוח על המורים מדידה של הצלחת התלמידים, שתמתן את השפעת המשתנים החיצוניים ותשמש כלי אמין למדידה.

בשנים 2011–2015 רכשו רשויות מחוז יוסטון תוכנה של חברת SAS[45] המכונה "Educational Value–Added Assessment System" — EVAAS, והסתמכו על המודל האלגוריתמי של המוצר כדי לקבל החלטות על אודות איכות ההוראה, שממנה נגזרו החלטות בנוגע להעסקת מורים. המודל התיימר לבצע מדידה איכותית של הצלחת התלמידים למול דרכי חישוב פשוטות יותר, כך שלאחר בחינת שיפור נומינלי בהישגי התלמידים, הושוו הישגי המורים לאחרים דומים להם באותו המחוז, ורק לאחר מכן דירג האלגוריתם את המורים באופן סטטיסטי

Innovative Practices, Redesigning Teaching, Leadership, Indig. Educ. 21st Century 196–218 (2020)

43 Professional Expectations of Student Teachers: Highland Local School District

44 Douglas N. Harris, William K. Ingle, & Stacey A. Rutledge, *How Teacher Evaluation Methods Matter for Accountability: A Comparative Analysis of Teacher Effectiveness Ratings by Principals and Teacher Value-added Measures*, 51 Am. Educ. Res. J. 73–112 (2014)

45 על החברה והמוצר ראו פרסום **באתר חברת SAS**.

כך שהם התחלקו לכמה קבוצות איכות: החל באלה שלא שיפרו את הישגי תלמידיהם וכלה באלה שהביאו לשיפור ניכר בהישגי התלמידים. חשוב לציין כי דרך פעולתו המדויקת של האלגוריתם נשמרה כסוד מקצועי, לא פורסמה למורים, ובמהלך העתירה לא הוגשו לגביה תצהירים לבית המשפט.

על פי העתירה, עם כניסת המוצר לשימוש השתנתה גם מדיניות הרשויות. עד אז ראו הרשויות במדידת איכות ההוראה כלי תומך מדיניות שלא נועד למקרים פרטניים. עם הטמעת המוצר נמסר שיישקל המשך העסקתם של 15% ממקבלי ההערכה הנמוכה, ועל פי טענות ארגון המורים, פעל המחוז בשנים לאחר מכן לפיטורי המורים שהישגיהם היו נמוכים. כלומר, אף שלתוכנה לא הוענקו סמכויות החלטה, ולכאורה פלט התוכנה לא אמור היה לשמש מקור הסתמכות בלעדי לקבלת החלטה, הרי שהלכה למעשה שימשו תוצריה מקור הסתמכות בלעדי להחלטת ועדת החינוך המחוזית לסיים העסקת מורים.

עתירת ארגון המורים ביקשה לבטל את המדיניות החדשה. נטען כי פיטורי המורים בוצעו על סמך האלגוריתם בלבד וללא שיקולים נוספים. בכך הופרה הזכות להליך הוגן של מורים אלה, הן ברמה הפרוצדורלית, משום שלא ניתן להם מידע מספיק שיאפשר להם לערער על החלטת הפיטורים, הן ברמה המהותית, משום שהאלגוריתם שהסתמכו עליו לא היה שקוף לעיני הציבור. עוד טענו כי ההחלטה להסתמך עליו לא עמדה בקריטריונים הנדרשים כדי להוות החלטה מנהלית מוצדקת.

בית המשפט נדרש אפוא לשאלה אם מדיניות מעשית של פיטורים, המסתמכים ישירות על תוצר שסיפקה תוכנה המבוססת על אלגוריתם שאינו שקוף, פוגעת בזכות המהותית להליך הוגן (substantive due process),[46] והשיב על כך בחיוב. מאחר שהמדינה לא סיפקה הסבר ממוקד כיצד חישבה את מקומו של המורה המסוים, ולא אפשרה לו לבחון אם חלה טעות בחישוב, ולפיכך ממילא נבצר ממנו לערער עליה – נמנע הליך הערעור המוגן במסגרת הזכות להליך הוגן.

46 Mark A. Paige & Audrey Amrein-Beardsley, *"Houston, We Have a Lawsuit": A Cautionary Tale for the Implementation of Value-Added Models for High-Stakes Employment Decisions*, 49 Educ. Res. 350-359 (2020)

אולם, בית המשפט קבע כי טענת העותרים שלפיה עצם השימוש בתוכנה שמפיקה תוצר שאינו בר הנמקה ושדרך החישוב בו אינה מפורסמת, מפר את הזכות להליך הוגן, ביוצרו רף שרירותי שאינו מכוון התנהגות. בית המשפט קבע שדי שנקבעה מדיניות, המבוססת על נתונים – גם אם היא נוטה לטעויות או לחוסר הוגנות – כדי להראות שאין מדובר בשרירותיות. כמו כן קבע כי היעדר הפרסום של דרך החישוב, כשלעצמו, אינו יכול להעיד על שרירותיות. בית המשפט גם דחה את טענת העותרים כי הבחירה במודל הספציפי של תוכנת EVAAS איננה סבירה משום שמודל זה לקוי, וקבע כי משמעות הסבירות בבחירה בטכנולוגיה כזאת או אחרת היא שדי בסיכוי סביר שהיא טובה למדידה כדי להצדיק את הבחירה להשתמש בה. בית המשפט אמר כך:

> אכן הצדדים חלוקים בשאלה אם אלגוריתמי EVAAS תוקפו, והתובעים מציעים כמה דרכים אחרות שבהן נכשל EVAAS. גם אם נקבל את הביקורות של התובעים כפי שהן, התקן החוקתי הגמיש של רציונליות מאפשר לממשלות להשתמש בכלים גסים שיכולים להניב להן תוצאות רווח שולי בלבד. הבקשה של HISD לפסיקת דין מקוצר בתביעה כי התקיים תהליך מהותי מתקבלת.[47]

קביעה זאת היא, לדעתנו, תמוהה שכן הוצגו בפני בית המשפט עמדות מומחים שנתמכו במחקרים, ולפיהן האלגוריתם שנבחר לצורך המדידה לא היה מיטבי וכי הסטטיסטיקה העומדת ביסודו היא "כלי קהה".[48]

במקרה בוחן זה מערכת אלגוריתמית לא שקופה החליפה מערכות מסורתיות למדידה ולהערכה. בעקבות אילוצים משפטיים של סודיות מסחרית, רשויות המנהל לא יישמו דרישות לשקיפות ולהסברתיות והטמיעו מערכת שדרך

47 "It is certainly disputed here whether EVAAS algorithms have been validated, and plaintiffs offer up numerous other ways in which EVAAS falls short. Even accepting plaintiffs' criticisms at face value, the loose constitutional standard of rationality allows governments to use blunt tools which may produce only marginal results. HISD's motion for summary judgment on this substantive due process claim is granted". ראו **לעיל**, ה"ש 40.

48 **שם**.

פעולתה עכורה ושהפיקה תוצר שהוביל, בהמשך, לפיטוריהם של מורים, בלי שניתנה להם האפשרות להתמודד עם הטענות נגדם. הביקורת השיפוטית, בתורה, מנעה את המשך השימוש בטכנולוגיה, אך לא בשל טעמים מהותיים הנוגעים לתהליך הבחירה וההטמעה של המוצר, אלא משום שהוא יצר הפרה דה־פקטו של החובה הפרוצדורלית לשימוע, שכן עובד שאינו יודע מדוע פוטר ממילא אינו יכול לערער על פיטוריו.

אנו רואים אפוא שהביקורת השיפוטית לא יצרה גוף דרישות וסטנדרטים צופי פני עתיד שעל הרשות לאמץ בבואה לבחור בכלי טכנולוגי כזה או אחר. לפיכך, לפי הלוגיקה של פסק הדין, ייתכן שלו הייתה המערכת מספקת הסבר לגבי דרך פעולתה או משקפת אותו כך שניתן היה לערער על תוצאותיה, היא הייתה נחשבת קבילה גם אם לא הייתה מדויקת או יעילה. בפועל, בית המשפט נתן את הסכמתו לפעולה לא סבירה, ללא אחריות מצידה של הרשות לכלים שבהם היא משתמשת. קשה לפיכך, לקבל את האמירה שהממשלה יכולה להשתמש בטכנולוגיה בלי לוודא שהיא מקצועית, מדויקת, מתוקפת אמפירית ובלי אמות מידה לבחינה.

ב. מקרה בוחן שני: שימוש משטרת ישראל במערכת "פגסוס"

בינואר 2022 פרסם העיתונאי תומר גנון בעיתון כלכליסט כמה כתבות תחקיר שעלה מהן כי משטרת ישראל הפעילה רוגלה לצורך ביצוע האזנות סתר בטלפונים סלולריים של אזרחים ישראלים. כל זאת ללא צווי בית משפט וללא ידיעת החשודים.[49] בהתאם לתחקיר, מערכת בשם "פגסוס",[50] שפותחה על ידי

49 תומר גנון "חברת NSO בשירות משטרת ישראל: פריצות לטלפון של אזרחים ללא פיקוח או בקרה" **כלכליסט** (18.1.2022).

50 או מערכת זהה אך מנוונת בחלק ממאפייניה שכונתה בפי משטרת ישראל "סייפן". ראו על אודות הכינוי המשטרתי שניתן לתוכנת פגסוס מבית NSO, משרד המשפטים **דין וחשבון הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים** (2022) (להלן: דוח מררי), עמ' 2.

חברת הסייבר הישראלית NSO, נכנסה לשימוש במשטרת ישראל באופן לא מבוקר. חשוב לציין שעד אז שימשה המערכת גופי מודיעין בלבד בישראל ולא הופעלה כנגד אזרחים ישראלים.

נוזקות מעקב הן תוכנות מחשב אשר מנצלות חולשות במכשירי טלפון ניידים של משתמשים מזוהים מראש, אינן מחייבות מעורבות מצד חברות הטלפוניה, מאפשרות מעקב אחר מגוון סוגי מידע, מעניקות למפעיליהן גישה מלאה למכשיר הטלפון הנייד של הנעקב וכמעט שאינן מותירות עקבות פורנזיים אחר פעילותן. הן מאפשרות למפעיליהן לשאוב מהמכשיר תמונות, הודעות טקסט, קובצי וידאו ואודיו, כולל שיחות קוליות, סיסמאות ליישומונים אחרים המותקנים על גבי המכשיר ונתונים אחרים הנקלטים באמצעות חיישני המכשיר, כגון מיקום גיאוגרפי ומידע קולי וחזותי באמצעות מיקרופון ומצלמת המכשיר.[51]

לשימוש בנוזקות מעקב עשויים להיות יתרונות והצדקות, שכן הוא עשוי לסייע לרשויות הביון ואכיפת החוק במאמצי הלוחמה בטרור ובפשיעה.

המעקב באמצעות נוזקות המוחדרות למחשב האישי של המשתמש או, ברוב המקרים, למכשיר הטלפון הנייד שלו הפך לתעשייה גלובלית משגשגת בשווי מוערך של 12 מיליארד דולר, שפועלות בה חברות רבות, מרביתן לא מוכרות לציבור.[52] תעשייה זו התפתחה במסגרת ניצול היתרונות הרבים הטמונים

51 Hendrik Milderbrath, *Europe's PegasusGate*, European Parliamentary Research Service 3 (PE 729.397, July 2022); Marcin Rojszczak, *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses*, 29 European J. of Crime, Criminal Law & Criminal Justice 290, 300 (2021); Otavvio Marzocchi & Martina Mazzini, *Pegasus and Surveillance Spyware*, Policy Department for Citizens' Rights and Constitutional Affairs (2022); Directorate-General for Internal Policies, Policy Department A, The Impact of Teleworking and Digital Work on Workers and Society: Analysing its Economic, Social, and Environmental Effects (2022)

52 קבוצת ניתוח האיומים של גוגל איתרה במאי 2022 כשלושים ספקי נוזקות מעקב למכירה שמוצריהם תקפו מכשירי טלפון ניידים, שמותקנת עליהם מערכת הפעלה אנדרואיד, ראו Lily Hay Newman, *Spyware Vendors Target Android With Zero-Day*

בשימוש הנרחב במכשיר הטלפון הנייד. באמצעות החדרת נוזקת מעקב הופך המכשיר הנייד לא רק לחלון לעולם עבור המשתמש בו, אלא גם חלון נוח ביותר לחייו הפרטיים של המשתמש.[53] לעומת יירוט נתוני תקשורת מחברת הטלפוניה, המאפשר איסוף נתונים דוגמת מספר הטלפון שיצאה ממנו השיחה, יעד

Exploits, Wired (May 19, 2022). עם החברות הידועות בתחום נמנות חברת NSO הישראלית, שהחזיקה במשך שנים בבכורה בשוק, אך בשנים האחרונות ספגה מכה קשה וירדה מגדולתה; Paragon הישראלית, שמפתחת ומשווקת נוזקת מעקב שאינה מיועדת להשיג שליטה מלאה מרחוק במכשיר טלפון נייד אלא בפריצה לתוכנות מסרים מיידים מוצפנות, ולפי הפרסומים מוכרת את מוצריה לממשל האמריקני; Cytrox מהונגריה, אשר מפתחת ומשווקת את נוזקת המעקב Predator שהוחדרה למכשירי טלפון ניידים מבוססי אנדרואיד במצרים, בארמניה, ביוון, במדגסקר, בחוף השנהב, בסרביה, בספרד ובאינדונזיה; Hacking Team מאיטליה, שפיתחה ושיווקה את נוזקת המעקב Remote Control System, שלפי הדיווחים שימשה למעקב אחר פעילים למען זכויות אדם ועיתונאים ממדינות שונות; Memento Labs, שפיתחה על בסיס הטכנולוגיה של Hacking Team את הנוזקות Krait ו־RCS X המאפשרות חדירה למכשיר הטלפון הנייד של יעד המעקב, ללא כל פעולה מצידו, ומעניקות למפעיליהן גישה למגוון הסיסמאות של יעד המעקב, למכלול חיישני המכשיר החכם ולכלל המידע המאוחסן בו; RCS Lab, גם היא מאיטליה, שמפתחת ומשווקת את נוזקת המעקב Hermit, שלפי הדיווחים שימשה את ממשלת קזחסטאן, את רשויות אכיפת החוק באיטליה, ולדיכוי המיעוט הכורדי בצפון מזרח סוריה. ראו Ronen Farrow, *How Democracies Spy on their Citizens*, The New Yorker (April 18, 2022). ביולי 2023 הודיעה מחלקת המסחר האמריקני על הוספתה של החברה לרשימה השחורה של החברות שאין לסחור עימן, ראו Jarrett Renshaw, David Shepardson & Karen Freifeld, *U.S. Adds Two European Surveillance Firms to Export Control list*, Reuters (July 18, 2023). בשנת 2015 סבלה חברת Hacking Team ממתקפת סייבר שהובילה לחשיפת השימוש שנעשה בנוזקת המעקב שבפיתוחה על ידי משטרים דיקטטוריים בסודן, בערב הסעודית ובמצרים. באופן הפוגע שלא כדין בזכויות אדם. החשיפה הובילה למפלת החברה שהצטיירה כמי שמאפשרת משטרים המדכאים את אזרחיהם. בשנת 2016 אף ביטלה רשות הייצוא האיטלקית את רישיון הייצוא שניתן לחברה ומנעה ממנה למכור את טכנולוגיית המעקב שלה ללקוחות זרים. אולם בשנת 2019 נרכשה החברה על ידי איש היי־טק ויזם איטלקי, אשר השתמש בקניינה הרוחני לפיתוח נוזקות מעקב מתוחכמות על ידי החברה שבבעלותו, Memento Labs. ראו בעניין זה Patrick Howell O'Neill, *The Fall and Rise of a Spyware Empire*, MIT Tech. Rev. (Nov. 29, 2019); Tera Seals, *Sophisticated Hermit Mobile Spyware Heralds Wave of Government Surveillance,* Dark Reading (Sep. 21, 2022); Fred Guterl, *Special Report: When Spyware Turns Phones into Weapons,* Committee to Protect Journalists (Oct. 12, 2022)

53 Ron Deibert, *Protecting Society from Surveillance Spyware*, XXXVIII (2) Issues in Science and Technology (Winter 2022)

השיחה, מיקום המכשיר, תא השטח שהתבצעה ממנו השיחה או נשלחה הודעת טקסט והיסטוריית הגלישה באינטרנט, נוזקות מעקב הן פולשניות הרבה יותר: הן מנצלות חולשות במכשירי טלפון ניידים של משתמשים מזוהים מראש; אינן מחייבות מעורבות מצד חברות הטלפוניה וניתן להתקינן מרחוק ובאופן חשאי, במה שמכונה "Zero Click Attack"; מאפשרות מעקב אחר מגוון סוגי מידע; מעניקות למפעיליהן גישה מלאה למכשיר הטלפון הנייד של הנעקב ללא מגבלת גבולות גיאוגרפיים, כולל גישה למסרונים, לתמונות, לתכתובת דוא"ל, לקובצי וידאו, לרשימת אנשי קשר ולכלל חיישני המכשיר, לרבות הפעלה מרחוק של מיקרופון המכשיר והמצלמה שלו; ומאפשרות גישה למידע המצוי ביישומונים מוצפנים, כגון תוכנת המסרים המיידיים "Signal". והכול כמעט בלי להותיר עקבות פורנזיים לפעילותן.[54]

יש להודות כי איסוף מידע אישי אינו חדש או ייחודי. חברות מסחריות רבות נשענות כיום על איסוף מידע אישי, על עיבודו ועל הפקת תובנות על בסיסו בנוגע לחייו האישיים של המשתמש, קשריו החברתיים, תחביביו ומיקומו הגיאוגרפי, לשם "דחיפת" פרסומות ותכנים מותאמים אישית. ואולם, קיים הבדל מהותי בין פעילות החברות המסחריות לאיסוף המידע לבין המעקב המבוצע על ידי נוזקות: האחרונות פועלות בחשאיות, ללא ידיעת משתמש הקצה וכאמור כמעט בלי להותיר עקבות פורנזיים, עובדה המקשה את איתורן גם בדיעבד. משום כך, הן ניצבות בצד הקיצוני והחודרני ביותר בסולם הפגיעה בפרטיות. מדובר בחדירה המערערת את שליטתו של המשתמש במידע האישי על אודותיו, אגב פגיעה בסודיות ובאנונימיות, המובילה גם לפגיעה בזכויות נוספות, דוגמת הזכות לחופש ביטוי ואף הזכות לחיים.[55]

54 Audrey Travere, *The Rise and Fall of NSO Group*, Forbidden Stories (July 19, 2021); Phineas Rueckert, *The Pegasus Project*, Forbidden Stories (July 18, 2021); Hendrik Milderbrath, *Europe's PegasusGate*, European Parliamentary Research Service 3 (PE 729.397, July 2022); Marcin Rojszczak, *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses*, 29 European J. of Crime, Criminal Law & Criminal Justice 290, 300 (2021); Marzocchi & Mazzini Guterl, **לעיל** ה"ש 51; **לעיל** ה"ש 52.

55 Deibert, **לעיל** ה"ש 53.

ידוע זה מכבר המעקב שעושים ממשלות וארגוני פשיעה אחר עיתונאים מחשש פן אלו יפרסמו תחקירים על שחיתויות ועל פעולות לא חוקיות שלהם. אולם, השימוש בנוזקות למעקב אחר טלפונים ניידים מבטא עליית מדרגה ניכרת ביכולות המעקב, במידת החודרנות והפגיעה בפרטיות שהוא גורם, ומכאן גם בהשלכותיו החמורות. היכולת לגבש תמונה מפורטת ומדויקת של חייו האישיים של יעד המעקב, לרבות קשריו החברתיים והמקצועיים, דעותיו ומחשבותיו, באמצעות איסוף המידע האישי הרגיש באופן קבוע וחודרני, יוצרת אקלים של פחד, פרנויה וצנזורה עצמית, ומהווה איום קיומי על עתיד העיתונות וחופש הביטוי.[56] מקורות חוששים להעביר מידע לעיתונאים, ועיתונאים חוששים מביצוע תחקירים מסוכנים מחשש לשלומם ולשלום מקורותיהם, משפחותיהם וחבריהם. העיתונאים חשים חסרי אונים מפני שאין בנמצא כלים, כגון תוכנת אנטי־וירוס, כדי למנוע את ההדבקה בנוזקה או כדי להסירה. אפילו שימוש בתוכנות מסרים מוצפנות אינו מהווה ערובה לביטחון.[57]

בשלב הראשון הכחישו גורמים במשטרת ישראל את השימוש שעשתה המשטרה במערכת, אך לבסוף התברר שהמערכת אכן נכנסה לשימוש לצורכי האזנות סתר שביצעה המשטרה.[58] בהמשך לכך ובעקבות פרסומים אלה הקפיא היועץ המשפטי לממשלה דאז, ד״ר אביחי מנדלבליט, את השימוש במערכת ומינה צוות לבדיקת החשדות, בראשות עו״ד עמית מררי, המשנה ליועץ המשפטי לממשלה לענייני משפט פלילי (להלן: צוות מררי או הצוות).[59]

מדובר באירוע הרה גורל מבחינת הפעלת יכולות חדירה סמויות מרחוק של גורמי אכיפה נגד חשודים בעבירות פליליות, שאינן נוגעות לביטחון המדינה. עד אז התבצעו האזנות סתר לטלפונים ניידים באמצעות מרכזיות של ספקיות

56 **שם**; Ronen Farrow, *How Democracies Spy on their Citizens*, The New Yorker (April 18, 2022)

57 Guterl, **לעיל** ה"ש 52.

58 עומר כביר "מה באמת אומרת משטרת ישראל כשהיא מכחישה את תחקיר כלכליסט" **כלכליסט** (20.1.2022).

59 דוח מררי (**לעיל** ה"ש 50).

התקשורת השונות בלבד, ולא היו בידי המשטרה יכולות ליירט שיחות אודיו או וידאו שבוצעו באמצעות תוכנות, כגון ווטסאפ או סקייפ.[60]

צוות מררי עסק בשני היבטים הנוגעים לדיוננו: האחד הוא חוקיות הפעלת המערכת, שתעוגן בנהלים להפעלתה; והאחר הוא היעדר קיומו של הליך סדור טרם רכישת התוכנה והטמעתה במשטרת ישראל, שאמור היה לבחון מהן ההשלכות של הפעלת הטכנולוגיה.

מדוח הצוות ומתמלילי ועדת החוקה, חוק ומשפט של הכנסת שעסקה בנושא, עולה כי כמה כשלים התקיימו בעת ובעונה אחת:

(**1**) המערכת הטכנולוגית נכנסה לשימוש בהליך פנים־משטרתי, לא שקוף, והעברת המידע לגבי יכולותיה נעשתה באופן לוקה בחסר. לפיכך ניתן ייעוץ משפטי חלקי בלבד בנושא.

(**2**) כניסת הרוגלה לשימוש נעשתה ללא היוועצות בין־משרדית רוחבית, וגורמי מקצוע שהיו יכולים להתריע לא שולבו בתהליך.

(**3**) ההליך הפנים־משטרתי אף הוא נעשה באופן כושל שכן כניסת הרוגלה נעשתה ללא נהלים ברורים בשלבים המקדמיים, ללא התאמות שנדרשו מהייעוץ המשפטי וללא תיעוד מספק. עובדה זו הקשתה את בדיקת איכות פעולתה.

רצף הכשלים הוביל לעצירת השימוש בתוכנה, על אף המשמעויות הקשות הכרוכות בהגבלת כוחה של המשטרה לפענח פשעים, ולמשבר אמון קשה שנוצר בין הדרג הפוליטי לבין הדרג הביצועי במשטרה ובמשרד המשפטים.

דוח הוועדה קבע כי השימוש בטכנולוגיה נעשה במסגרת חוק האזנת סתר ואינו חורג מן ההסמכה בו, ומציין כי התקבלו צווים שיפוטיים להאזנת סתר.[61] עם

60 להסבר על יכולת זו ראו **אחר רשות התקשורת הפדרלית בארצות הברית**.

61 דוח מררי (**לעיל** ה"ש 50), עמ' 2 (בתקציר): "הבדיקה העלתה כי אין כל אינדיקציה לכך שמשטרת ישראל הדביקה באמצעות מערכת בסוס שבידיה [...] ללא צו שיפוטי".

זאת, הצוות העיר כי היעדר נהלים ברורים בהפעלת המערכת הביא לך שאגב פעולתה "שאבה" המערכת מהטלפון מידע שקיים בו (המכונה "data at rest"), מתוך חריגה מצו האזנת סתר אשר מאפשר יירוט שיחות בלבד (המכונה מידע "חי" או "data in transit"). כניסתה של המערכת לשימוש בוצעה ללא תיעוד מספיק, ובעיקר ללא ניוון היכולות העודפות, אלה שהלכה למעשה חורגות מסמכות לפי חוק האזנת סדר, אף שהיועצים המשפטיים של המשטרה, שליוו חלק מתהליך הרכש, דרשו את ניוונן. הדוח מציין כך:

> לא ידוע לצוות הבדיקה באיזה שלב הוחלט להפעיל את המערכת ועל ידי מי, על אף שלא בוצעו כלל הניוונים הטכנולוגיים הנדרשים על מנת שהמערכת לא תאפשר לאסוף מידע אגור טרם התקנת הכלי, וכן סוגי מידע מסוימים שאינם מועברים בתקשורת בין מחשבים (כגון אנשי קשר, יומן ופתקים). אולם ידוע כי דה פקטו, עם תחילת השימוש במערכת, לערך בתחילת שנת 2016 וכן לאורך תקופת פעילותה עד היום, המערכת הופעלה ללא ניוון טכנולוגי של היקף היכולות הפוטנציאליות האמורות לעיל, אשר אינן בסמכות משטרת ישראל להאזנת סתר לפי החוק.[62]

עם זאת, הצוות העיר כי מידע זה נשאר בידי גורמי המודיעין שהפעילו את התוכנה, וכי בבדיקה מדגמית שערכו עלה שהמידע לא הגיע לתיקי החקירה. ואולם, התברר לאחר מכן, כפי שעלה בתגובות לבית המשפט, כי ייתכן שבניגוד להצהרות המשטרה, נעשה שימוש במידע השאוב לצורכי חקירה, והדבר הוביל לביטול כתבי אישום.[63] בדיוני ועדת החוקה, חוק ומשפט בכנסת בעניין השימוש בתוכנה, עלה חשד כי הבדיקה המדגמית שבוצעה במסגרת פעילות הצוות לא הייתה מקיפה דייה, וגורמים בפרקליטות ביצעו לאחר מכן בחינה מחודשת של כלל התיקים שנעשה בהם שימוש בתוכנה.[64]

62 **שם**, עמ' 55.

63 אברהם בלוך ואלון חכמון "בשל האזנת סתר פסולה – הפרקליטות משכה ראיות בתיק רצח" **מעריב** (5.6.2023).

64 מתוך דברי ד"ר חיים ויסמונסקי, מנהל מחלקת הסייבר בפרקליטות המדינה בדיוני ועדת חוק חוקה ומשפט, פרוטוקול 97 (12.6.2023), עמ' 17, אשר דיווח על אודות הנחיה שהוציא פרקליט המדינה.

אם כן, בעקבות היעדר ההליך הסדור לא התקיים דיון משפטי, בשיתוף הייעוץ המשפטי לממשלה העוסק בעניינים אלה ופרקליטות המדינה האחראית לפיקוח המשפטי, בנושא פועלה של המשטרה להתאמת המערכת החדשה למסגרת החוקית הקיימת. כך לא היה עיסוק באנומליה המשפטית: הצורך בשני צווים שיפוטיים, האחד מכוח סעיף 23א׳ לפקודת סדר הדין הפלילי,[65] חתום בידי שופט שלום לחדירה לחומר מחשב השאוב במכשיר; והאחר צו ליירוט השיחות מכוח חוק האזנת סתר, חתום בידי נשיא בית המשפט המחוזי או סגנו.[66] כמה משפטנים בכירים, כגון פרופ׳ בעז סנג׳רו, סברו שייתכן שהפעלתה של המערכת נגדה את הוראות החוק,[67] ועתירה בעניין אף הוגשה בנושא על ידי האגודה לזכויות האזרח ועל ידי פרופ׳ מיכאל בירנהק.[68] ההוראות לנוון את המערכת כדי שתוכל לעמוד בדרישות הייעוץ המשפטי לא יושמו בפועל, והמערכת נכנסה לפעילות כשהיא מסוגלת לבצע פעילויות החורגות בהרבה מאלה שמותר לבצע על פי חוק. כל זאת בהתאם לפרשנות של היועצים המשפטיים מתוך המשטרה שליוו את תהליך הרכש, וללא שאלה פנו למומחי תוכן בנושא ממשרד המשפטים או מרשויות אחרות בעלות ניסיון.[69] כמו כן עלה כי הליך כתיבת הנהלים בוצע רק לאחר חודשים רבים שבמהלכם הופעלה התוכנה במסגרת ניסיון הרצה (להלן: ״פיילוט״) בתוך גופי הסייבר המשטרתיים, ללא נוהל מסודר.

ממצא נוסף וחשוב של הצוות, לדעתנו, היה היעדר ניהול של דיון רוחבי בנושא קליטת המערכת והיעדר בחינת ההשלכות של השימוש בכלי מורכב זה, שעד

65 ס׳ 23א, פקודת סדר הדין הפלילי (מעצר וחיפוש) (נוסח חדש), התשכ"ט–1969, שהתווסף בתיקון שהוכנס בשנת 2005.

66 ס׳ 6(א), חוק האזנת סתר, התשל"ח–1979.

67 בועז סנג׳רו "פרשת פגסוס: כישלון רוחבי" **ישראל היום** (30.1.2022).

68 בג"ץ 6604/23 **האגודה לזכויות האזרח בישראל נ׳ מפכ"ל משטרת ישראל**, לעתירה ולתקציר על אודותיה ראו בפוסט של האגודה לזכויות האזרח בנושא "פגסוס והמשטרה: על השימוש לרעה ברוגלה המסוכנת" האגודה לזכויות האזרח בישראל (2022).

69 דוח מררי (**לעיל** ה"ש 50), עמ׳ 55–57.

אז היה כאמור בשימוש גורמי ביון וסיכול בלבד,[70] ומעבר לשאלה הצרה של התאמת המערכת לסמכויות מכוח חוק האזנת סתר.[71]

בין השאר, צוין שהייעוץ המשפטי הפנים־משטרתי, שאחראי ללוות את תהליכי הרכש, ופרקליטות המדינה, שאחראית על פיקוח משפטי של מוסד החקירה המשטרתית, הן במחלקת הסייבר והן באמצעות פרקליטויות המחוזות, לא היו מודעים ליכולותיה המלאות של המערכת שנרכשה בכל הנוגע לשאיבת מידע ממכשירים, וסברו כי היא מאפשרת יירוט שיחות "חיות" בלבד, הגם שידעו שמידע אגור כלשהו נקלט על ידי המערכת.[72] הדוח מתאר זאת במילים האלה:

> במבט לאחור, הצוות סבור כי המשמעות הדרמטית של הכנסת מערכת בעלת יכולות טכנולוגיות פוטנציאליות רחבות היקף המהווה נקודת מפנה מבחינת עולם האזנות הסתר לתקשורת בין מחשבים לא הובנה לאשורה על ידי הגורמים הבכירים במשטרה. לאורך השנים לא יוחסה מלוא המשמעות המתבקשת להיקף היכולות הפוטנציאליות של המערכת ולעצם הכנסת חומרים אסורים אל מערכות המשטרה ומשמעות החריגה מסמכות, אף אם לא ייעשה בהם שימוש בפועל.[73]

בהמשך, נקבע בדוח כי לא נמצאו מסמכים המעידים על כך שהייעוץ המשפטי לממשלה, בייחוד מחלקת ייעוץ וחקיקה שאמונה על ראייה רוחבית של השפעות תוכנה על יכולותיה של המדינה, היו מודעים לשימוש בתוכנה ונתנו את דעתם בנושא:[74]

70 David D. Kirkpatrick & Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client,* The New York Times (Aug. 31, 2018)

71 דוח מררי (**לעיל** ה"ש 50), פרק 8 "בחינת הליכי האישור ביחס למערכות האזנת לתקשורת בין מחשבים המותקנות על מכשיר קצה", עמ' 53.

72 **שם**, עמ' 45.

73 **שם**, עמ' 53.

74 **שם**, פרק 8.

> מבירור הצוות, על אף מערכת היחסים ההדוקה וההתייעצויות השוטפות של משטרת ישראל עם מחלקת הסייבר בפרקליטות ועם הייעוץ המשפטי לממשלה, לא נמצא מסמך או גורם שאיתו שוחח צוות הבדיקה (במשטרה או במשרד המשפטים), אשר מהם עולה כי הועבר לידי משרד המשפטים מידע בדרך זו או אחרת בדבר כלל מאפייני המערכת, ובאופן ספציפי מידע ביחס ליכולות הטכנולוגיות של המערכת אשר חורגות מהסמכות לפי חוק האזנת סתר.[75]

הדיון הרוחבי הוא עניין חשוב בשל הצורך הן במומחיות והן בצורך בראייה ביקורתית בנוגע להליכי מחשבה שיכולים להתפתח במסגרת משרד מסוים. היעדרו – היה כנראה שורש הכשל.

עניין נוסף שראוי לציין הוא היעדר הפומביות סביב כניסתה של הטכנולוגיה לשימוש המשטרה. ככלל, גם לאחר גילוי הפרשה, אופן השימוש במערכת לא פורסם לציבור, מתוך רצון להגן על שיטות הפעולה של המשטרה ולמנוע את חשיפתן. גם בתי המשפט לא נחשפו לפרטי הפעלת התוכנה, מכוח חיסיון "שיטות פעולה" המוכר בדין הישראלי.[76] נעיר כי חלק מחוסר היכולת לנהל דיון מושכל בשאלת ההשלכות של השימוש בטכנולוגיה, טמון בהיעדר השקיפות המופרז. מעבר לשיטות הפעולה עצמן, לא מסרה המשטרה נתוני עומק בדבר השימוש שעשתה בטכנולוגיה בפילוחים שונים.[77] לאור הסערה הציבורית שהתעוררה בעקבות הפרסומים, התקיימו דיונים פומביים וחסויים בוועדת החוקה, חוק ומשפט של הכנסת. בחלקו הפומבי של הדיון בוועדה עלה כי נעשו יותר מאלף

75 **שם**, עמ' 57.

76 ס' 74, חוק סדר הדין הפלילי (נוסח משולב), התשמ"ב–1982. חיסיון זה קיים גם בדין המינהלי. למאמר המבקר את השימוש בחיסיון זה, ראו למשל, אלעד כהנא "הזכות לדיון לא הוגן: עלייתם של דיונים חסויים, נפילתן של עתירות לגילוי ראיה" **מעשי משפט** ט 159 (2018).

77 תהילה אלטשולר־שורץ ועמיר כהנא "דיון בדו"ח האזנות סתר 2021, לאור מסקנות דו"ח וועדת מררי" (המכון הישראלי לדמוקרטיה, 12.3.2023).

ניסיונות הדבקה באמצעות הרוגלה, ללא ציון מספר התיקים הפליליים שבהם נעשה השימוש וללא ציון מידת ההצלחה.[78]

השימוש בתוכנה הוקפא, והוועדה המליצה על הקמת ועדת בדיקה ממשלתית לשימוש בה. ממשלת ישראל אימצה את ההחלטה ביום 27 באוגוסט 2023.[79] השופט בדימוס יעקב דרורי מונה לעמוד בראש הוועדה, והיא יושבת על המדוכה בימים אלה.[80]

מקרה הבוחן הזה עסק במערכת טכנולוגית שנתפסה בעיני מי שביקש להשתמש בה ולהטמיע אותה, ככלי שייתן מענה יעיל לאכיפת חוק באמצעות האזנות הסתר בעולם של תעבורת נתונים על גבי האינטרנט. בפועל, דובר בהכנסת טכנולוגיה שחיזקה עד מאוד את יכולות הריגול של משטרת ישראל, ונתפסה בעיני הציבור ובעיני מומחי משפט כחציית קו אדום ללא הסמכה בחוק.

ג. מקרה בוחן שלישי: מערכת הכללה מבוססת בינה מלאכותית לעיכוב נכנסים לארץ בשדה התעופה

כתבה שהתפרסמה בעיתון כלכליסט בנובמבר 2022 חשפה שמשטרת ישראל מפעילה בנמל התעופה בכניסה לישראל, מערכת מבוססת בינה מלאכותית, אשר באמצעות מערכת כללים מורכבת (מכלילה), מסמנת אוטומטית חשודים

78 מתוך דברי עו"ד אלעזר כהנא, היועץ המשפטי של משטרת ישראל בדיוני ועדת חוק חוקה ומשפט, פרוטוקול 47 (13.3.2023), עמ' 17.

79 תומר גנון "ועדת החוקה לממשלה: 'הקימו ועדת חקירה בראשות שופט לפרשת הרוגלות'" **כלכליסט** (13.6.2023).

80 כתב מינוי לוועדת הבדיקה הממשלתית לבדיקת רכש, מעקב ואיסוף מידע בכלים קיברנטיים אחר אזרחים ונושאי משרה, המבוצעים על ידי גורמי האכיפה (14.9.2023).

פוטנציאליים וממליצה לשוטרי המתחם לחפש בכליהם.[81] מדובר במערכת שעד אז לא פורסמה פעולתה לציבור, ודרכי פעולתה היו עלומות. המידע על אודות המערכת התגלה בעקיפין במהלך דיון בבית משפט שעסק בהארכת מעצר חשוד שבכליו נעשה חיפוש, ולאחר מכן בסדרת עתירות לגילוי ראיה שפרסומן הותר רק לאחרונה. מן הכתבה ומן המידע שהותר לפרסום,[82] עלה כי עם חזרתו ארצה של אזרח ישראלי התריעה המערכת על חשוד פוטנציאלי, ובעקבות זאת חיפשו השוטרים בכליו ומצאו בהם "סם מסיבות" מסוג קטמין. נגד האזרח הוגש כתב אישום בגין ייבוא סמים מסוכנים לישראל.[83]

משטרת ישראל הודתה כי המערכת, המבוססת על אלגוריתם של בינה מלאכותית, היא הסיבה שהביאה לחיפוש בכליו של הנאשם, ומדברי השוטרים בדיוני בית המשפט עלה כי הם פעלו ללא שיקול דעת עצמאי אלא על פי הוראות המערכת.[84] עם זאת, בכל שלבי הדיון סירבה המשטרה לאפשר לסנגוריו של החשוד גישה למידע על דרך הפעולה של המערכת, בטענה כי עלולות להיחשף שיטות מודיעיניות משטרתיות, וממילא אין זה רלוונטי לעצם העובדה שנמצאו סמים בכליו של הנאשם.

הנאשם מצידו טען כי המערכת החשידה אותו באמצעות שימוש בפרמטרים אסורים, כגון נטייתו המינית, ולפיכך שמורה לו הזכות לדרוש מידע כיצד קבעה המערכת שדווקא הוא ייבחר לחיפוש. במהלך הדיון בבית המשפט העידו קציני משטרה כי אינם יודעים כיצד המערכת פועלת ומהם מקורות המידע שתרמו להליך הלמידה של המכונה.

81 תומר גנון "ללא מגע יד אדם: האלגוריתם שיעצור אתכם בכניסה לנתב"ג" **כלכליסט** (10.11.2022).

82 תחילה הוטל צו איסור פרסום על הפרשה. לאחר מכן הותרו כמה החלטות לפרסום. ראו ע"פ 8660/22 **מדינת ישראל נ' עומר ברגר** (12.11.2023). החלטה זו מתירה את פרסום החלטת בית המשפט העליון מיום 21.9.2023.

83 נוסף על החומרים שהותרו לפרסום, פרטים חשובים על הפרשה מובאים גם בדיוני ועדת חוק חוקה ומשפט פרוטוקול 89 (21.5.2023).

84 יש לציין כי גרסת השוטרים בפני בית המשפט לא תואמת את אמירתו של גלעד בהט מהייעוץ המשפטי של משטרת ישראל, ולפיהם המערכת משמרת את שיקול הדעת של השוטר (**שם**, עמ' 12). אם כי ייתכן שהשוטרים בחרו להתנער משיקול דעתם.

בהליך לגילוי ראיה שהוגש לבית המשפט סירבו נציגי המדינה לפרט לפי אילו קריטריונים מסננת המערכת את החשודים. המדינה הסכימה להודות שנעשה שימוש בנתונים דמוגרפיים, שאותם לא פירטה, וכן במידע שהצטבר מתפיסות עבר של מבריחי סמים בנתב"ג. הם הדגישו שהקריטריונים המשמשים ללמידת המכונה אינם כוללים אבחנות האסורות על פי דין.

בית המשפט הכריע כי על המשטרה להעביר לידי סנגוריו של החשוד מידע על דרך פעולתה של המערכת,[85] ודרישה זו הובילה לביטול כתב האישום על ידי התביעה.

בערעור בבית המשפט העליון[86] על ההחלטה בנוגע לגילוי הראיה, התקיים בפעם הראשונה, גם אם בדלתיים סגורות, דיון בשימוש במערכת בינה מלאכותית – הן בקשר לחשש מהטיות כנגד אוכלוסיות מוגנות, הן בנוגע ליעילות המערכת ודיוקה.

ראשית, בנוגע לחשש מפני הטיות כלפי אוכלוסיות מוגנות, תהו שופטי ערכאת הערעור אם הנתונים הדמוגרפיים שבהם משתמשת המשטרה עלולים להפלות אוכלוסיות מוגנות. בכך התייחסו למה שמכונה במחקר העוסק בבינה מלאכותית "proxy bias" (הטיה מוסווית מתווך).[87] במקרים כאלה, אומנם נתונים אסורים לשימוש, כגון דת, גזע, נטייה מינית ומין, אינם חלק ממאגר המידע של המערכת, אך נתונים אחרים מביאים הלכה למעשה לאותן הטיות כאילו הנתונים האסורים היו שם. לדוגמה, גם בהיעדר נתונים על אודות צבע עורו או מוצאו של אדם, בארצות הברית נתוני המיקוד (Zip Code), ובישראל מקום המגורים – יכולים להביא את המערכת להסיק לגביהם במדויק. מערכת

85 צ"א 24474-01-22 **ברגר נ' מדינת ישראל** (11.9.2022).

86 ע"פ 8660/22 **מדינת ישראל נ' עומר ברגר** (21.9.2023).

87 להסבר על הטיות אלו ואחרות שעלולות להיווצר בפלטים המופקים על ידי מערכות מבוססות בינה מלאכותית, ראו עמיר כהנא ותהילה שורץ אלטשולר **אדם, מכונה, מדינה: לקראת אסדרה של בינה מלאכותית** (המכון הישראלי לדמוקרטיה, 2023).

שחשופה לכך שאנשים שמתגוררים באזור מיקוד מסוים נעצרו לחיפוש, תסיק שהיא צריכה להמשיך לעצור אנשים מאותו אזור, וכך תמשיך להפלות אנשים כהי עור. בישראל, ניתן להגדיר שמבצעים חיפוש לאנשים מקלנסווה, ללא ציון העובדה שהם ערבים, וברור כי התוצאה תהיה זהה.[88]

משטרת ישראל התנגדה לטענת האפליה, אך הסכימה לפרט בדבר פעולת המערכת במעמד צד אחד. בית המשפט השתכנע מטיעוניה של המשטרה וקיבל את ערעורה על ביטול כתב האישום, שנבע מהדרישה לגילוי הראיה.

שנית, בנוגע ליעילותה של המערכת העלתה המשטרה שני טיעונים. מחד גיסא, בא כוח המדינה טען כי מדובר במערכת ממליצה בלבד, וכי שיקול הדעת הסופי נמצא בידי השוטר בשטח, ולכן לדבריו לא עברה המערכת את התיקוף הנדרש המחייב מערכות מקבלות החלטה. מאידך גיסא טען כי מדובר במערכת שאין לחשוף את פעילותה, משום שהיא ממלאת תפקיד חיוני במניעת הברחות של סמים למדינת ישראל. אומנם אין מדובר בסתירה גמורה בין שני הטיעונים, שכן מערכת יכולה להיות יעילה "מניסיון חיים" ללא תיקוף מדעי, אך הדבר מעיד על כך שלא נוהל הליך עומק לבדיקת איכות המערכת ויעילותה – לא לפני הטמעתה וגם לא במהלך שנות הפעלתה. לו היו מתקיימים הליכים של תיקוף סטטיסטי או של היזון חוזר מהפעלת המערכת, הייתה יכולה המשטרה לענות על שאלות בית המשפט ולא להסתתר מאחורי טיעוני אי־רצון לחשוף שיטות פעולה.

לסיכום, מדובר במקרה בוחן שבו הוטמעה טכנולוגיה מבוססת בינה מלאכותית, כחלק מאמצעי החקירה הפליליים, בתהליך חסר, לא שקוף ובאופן שהעלה

88 לשאלת הצד שמוטל עליו נטל ההוכחה לקיומה של אפליה: בדין הנהוג במשפט הפדרלי בארצות הברית, למשל, מרגע שיש בידי תובע ראשית ראיה בדבר קיומה של אפליה, מתקיים היפוך נטלים. ממועד זה, במקום שנטל ההוכחה יהיה על התובע, על הצד הנתבע, המואשם באפליה, להוכיח כי לא פעל באופן מפלה. במקרה שלנו, מאחר שמדובר בהליך גילוי ראיה לפי הדין הפלילי – לא התבצע היפוך נטלים זה, וגם ראשית הראיה, שהוצגה בדיון אצל השופט דרויאן, לא הובילה את השופטים לדרוש מהמשטרה הוכחה כי התוכנה שברשותה איננה מפלה, והסתפקו בדיון במעמד צד אחד.

חשדות לפעולה באופן מפלה. נוסף על כך לא נערכו הליכי תיקוף ובדיקה במהלך השנים לגבי הפעלת המערכת.

הליך הכניסה של המערכת לשימוש בוצע ללא שקיפות ציבורית, מאחר שהמערכת נתפסה בעיני המשטרה כחלק מן השיטות ומן האמצעים הייחודיים המשמשים אותה וראויים להישאר חסויים. לא קדמו לכך דיון ציבורי או דיון פנימי ברשות המבצעת או בכנסת.

יתר על כן, הכנסת המערכת לשימוש מבצעי נעשתה ללא הליך הטמעה פנים־משטרתי. בין אם נכתבו נהלים סדורים (אין בידינו לדעת לאור הסודיות) ובין אם לאו, מדובר במערכת, שעל פי הודאת המשטרה היא "קופסה שחורה" והופעלה על ידי שוטרים שלא היו בקיאים בדרך פעולתה. הפעלתה בוצעה ללא בקרה וללא הדרכת השוטרים המשתמשים בה בנוגע ל"יחסי אדם ומכונה". התנהלות זו הביאה את השוטרים להודות כי מילאו הוראות על פי המלצות התוכנה ללא הפעלת שיקול דעת מצידם.

ההליכים המשפטיים חשפו גם הם הטמעה של טכנולוגיה ללא סטנדרטים ברורים, והדגישו גם את סירוב המשטרה לחשוף את מאגר המידע ששימש להליך למידת המכונה, הגם שעלה חשש שהמערכת פועלת באופן מפלה.

יש לציין כי הואיל ובפני בית המשפט הוצג הליך של גילוי ראיה, הוא נדרש רק לשאלה הצרה אם יש במידע שגילויו התבקש כדי לסייע בזיכוי הנאשם. משהכריע בית המשפט בסוגיה זו, לא היה עוד בסמכותו לקבוע מסמרות בעניין חוקיות המערכת. כל עוד לא היה בידי בית המשפט מידע ישיר כי מדובר במערכת שפעלה שלא לפי דין, הרי שגם אם עלו פגמים, לא היה צידוק משפטי להתערבותו בעניין חוקיות השימוש בה. הפגמים שעלו בפני בית המשפט לא הגיעו לרף המשפטי של פסילה, אף שהוצגו בפניו.

עניין זה מלמד גם על המגבלות המובנות של ביקורת שיפוטית בפיקוח על אימוץ מערכות טכנולוגיות. לבית המשפט אין יכולת לטפל בכשלים מבניים,

לקבוע כללים עתידיים או להעניק סעד שאינו מוגבל למקרה שלפניו.[89] כמו כן אין בידיו המומחיות הנדרשת להתמודד עם סוגיה חדשה וסבוכה, כגון זו הנוגעת לסכנות של הטיה ואפליה באמצעות מידע פרוקסי במאגר הנתונים שמשמש לאימון מכונה.

לאחרונה, בעקבות עתירה שהגישה האגודה לזכויות האזרח בדבר חוקיות השימוש במערכת ההכללה על ידי משטרת ישראל, מדינת ישראל השיבה כי השימוש במערכת הופסק כבר לפני שנתיים מסיבות מבצעיות.[90] תשובה זו נמסרה במסגרת טענת המדינה כי המחלוקת הפכה תאורטית והתייתרה. תשובת המדינה שניתנה בקצרה מעלה מספר תהיות. לא ברור מתשובת המדינה מהן הסיבות המבצעיות להפסקת השימוש; לא ברור אם השימוש במערכת הופסק לצמיתות או רק באופן זמני לצורך בחינה ותיקוף. כמו כן, לא ברור מדוע לאורך ניהול ההליך הפלילי שתואר לעיל המשטרה לא עדכנה כי המערכת איננה עוד בשימוש. התנהלות זו רק מגבירה את החשש בנוגע לקשיים שתוארו לעיל אגב כניסתה של המערכת לשימוש, ואף מעלה חשש כי קיימות מערכות נוספות כאלה, שהשימוש בהן טרם התגלה.

ד. מקרה בוחן רביעי: אימוץ טכנולוגיות זיהוי פנים על ידי המשטרה בהולנד

מטרת מקרה בוחן זה היא להמחיש את הפער בין אימוץ והטמעה של טכנולוגיות ללא תהליך חשיבה רוחבי וללא שקיפות לבין תהליך שהתבצע לאחר בקרה תהליכית, דיון ציבורי ובחינה משפטית.

89 יואב דוחן **ביקורת שיפוטית על שיקול דעת מנהלי** כרך א (2022), פרק 2.3 יתרונות וחסרונות של ביקורת שיפוטית.

90 בג"ץ 4271/24 **האגודה לזכויות האזרח נ' משטרת ישראל ואח'** – במסגרת תגובה מקדמית מטעם המשיבים מיום 15 באוגוסט 2024 (טרם פורסם).

טכנולוגיות זיהוי פנים מבוססות בינה מלאכותית, מסוגלות לזהות אם תמונת פנים הנגלית מתוך תמונה או סרטון, תואמת למאגר תמונות שהוזן למערכת קודם לכן. בחינת ההתאמה נעשית באמצעות המרת תמונת הפנים לרצף של פיקסלים ובדיקת התאמה ביניהם, בזמן אמת או בדיעבד. אמצעי זה יכול לשמש הן לאימות בכניסה לאתרים מאובטחים,[91] הן לצורכי זיהוי חשודים בתוך קהל או במהלך חקירה משטרתית והן לצורכי ביטחון אחרים.[92]

החששות העיקריים שמתעוררים בנושא אימוץ טכנולוגיות של זיהוי פנים נוגעים לפגיעה בזכות לפרטיות ובזכויות אדם אחרות, כגון הזכות להפגין והזכות לביטוי, בעקבות קיומן של מערכות זיהוי ביומטרי על ידי מערכות האכיפה שיוכלו לעקוב אחרי האזרחים בכל עת. משפטנים וארגוני זכויות אדם הביעו חשש שעל אף ההצהרות כי טכנולוגיה זו תוכל לסייע במאבק בטרור ובפדופיליה, הלכה למעשה היא תנוצל למעקב אחר המונים.[93] כמו כן עלו חששות מכשלים תפקודיים וטכניים, דוגמת זיהוי שגוי הנובע משימוש לא מקצועי בטכנולוגיה[94] או מהטיות הנובעות מתקלות ביצירת מאגר התמונות ואלגוריתם הזיהוי, שעלולות, בתורן, לפגוע בזכויות מיעוטים שהתוכנה תזהה

91 למשל כדי לאכוף איסור על כניסת אוהדים שהתפרעו בעבר למשחקי ספורט המוניים, בלי לבדוק את זהותו של כל נכנס ונכנס, ראו Andrew Cohen, *Facial Recognition in Sports: The Biometrics Technology Shaping Ticketing, Payments, Security, More,* SBG (Feb. 16, 2023)

92 כדוגמה לביקורת על הרגולציה של מערכות אלו, ובכלל זה הדגמת שימושים, ראו Elias Wright, *The Future of Facial Recognition is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media Ent. LJ 611 (2018). ראו גם חוות הדעת של המכון הישראלי לדמוקרטיה בנושא הצעת התיקון "חוק המצלמות", תהילה שוורץ אלטשולר "תזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (מערכות צילום מיוחדות), התשפ"ג–2023" (19.2.2023).

93 Mark Andrejevic & Neil Selwyn, *Facial Recognition Technology in Schools: Critical Questions and Concerns*, 45 Learn. Media Technol. 115–128 (2020)

94 **שם**. כמו כן בעניין זה ניתן לקרוא את עדותו של מנהל מעבדה במכון התקנים בעניין סטנדרטים ותקנים לזיהוי פנים: *Facial Recognition Technology (FRT)* (Feb. 6, 2020)

באופן מוטעה. דוח מכון התקנים האמריקני שהתפרסם בשנת 2018 [95] אף אישש טענות אלה, ואירועים של זיהוי שגוי של אנשים ומעצר שווא בעקבות זאת, יצרו שיח ציבורי ספקני בנוגע ליישומה של הטכנולוגיה לזיהוי פנים, ואף גרמו לשיח לעומתי בנוגע לכניסת טכנולוגיות מבוססות בינה מלאכותית במגוון תחומים[96] ובכללם במערכת המשפט.[97]

משטרת הולנד החלה להשתמש בטכנולוגיות זיהוי פנים בשנת 2016, לצורך איתור חשודים בתצלומי אבטחה, במסגרת ניסיונות לפענוח פשעים. מתוך הכרה בסכנות הפוטנציאליות שטומנת בחובה הטכנולוגיה היא הוכנסה לשימוש באופן מבוקר ואגב הטלת מגבלות משמעותיות. מפעילי הטכנולוגיה היו מודעים לסכנות הכרוכות בשימוש בה, הן בהיבט של סטנדרט היעילות והדיוק שלה שלא היו בהירים באותה עת והן בהיבט החשש מפני הטיות כלפי קבוצות מיעוט. לכן, נקבע כי זיהוי פנים על ידי המערכת לא יוכל לשמש ראיה בלי ששני מומחים יאשרו את הזיהוי, כל אחד בנפרד.[98]

השימוש בטכנולוגיה הוגבל בנהלים לצורך זיהוי רטרוספקטיבי של חשודים על גבי סרטוני אבטחה ומצלמות גוף של שוטרים,[99] ולא לזיהוי "חי" של אנשים בשטחים ציבוריים. שר המשטרה ההולנדי התבטא פומבית לגבי החלטה זו וקבע כי שימוש בזמן אמת אינו הולם את ערכיה של החברה ההולנדית.[100]

95 *NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding,* NIST (July 13, 2021)

96 Robert D. Atkinson et al., A policymaker's guide to the "techlash": what it is and why it's a Threat to growth and progress (2019)

97 Rebecca Crootof *"Cyborg Justice" and the Risk of Technological–Legal Lock-in*, 119 Columbia Law Rev. (2019)

98 Eva Krikken "But they do it too": The Dutch National Police and Real-Time Facial Recognition Technology (Master's thesis, Utrecht University, 2022)

99 שם.

100 Written observations by the Ministry of Justice and Security and the Ministry of Defence: on the draft-Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

בדיון המקדמי בנושא הטמעת הטכנולוגיה בעבודת המשטרה השתתפו גם רשויות אחרות מחוץ למשטרת הולנד. רשות הגנת הפרטיות ההולנדית התבטאה בנושא, וקיימים דוחות רבים, ובהם של ה־World Economic Forum שעקבו אחר היישום.[101] התקיים שימוע ציבורי בנושא, שבמסגרתו חיוו את דעתם מומחים ואנשי אקדמיה.[102] הולנד פעלה בשקיפות מול מדינות אחרות, והלקחים שהיא הפיקה מכניסת הטכנולוגיה אליה, סייעו בהגדרת המדיניות הכלל־אירופית, במסגרת החוק לרגולציה של בינה מלאכותית באיחוד.[103]

חשוב להדגיש: הליך קליטת הטכנולוגיה בהולנד לא היה חף מטעויות. אומנם במשטרה נבנה מאגר תמונות להשוואה אשר היה של חשודים אזרחי הולנד בלבד, אך בד בבד בנתה משטרת הגבולות מאגרי תמונות של מהגרים ונכנסים לגבולות המדינה, אף שלא היה מדובר בחשודים, אלא בתיירים ובמבקשי מקלט.[104] כמו כן, נעשו ניסיונות לקבל היתר להשתמש בטכנולוגיה אף לזיהויים בזמן אמת, גם אם בכפוף למגבלות משפטיות.[105] עם זאת, הדבר התבצע בשקיפות ותוך כדי דיון ציבורי. בניגוד לאירועים שהוזכרו לעיל לגבי ישראל בנושא מערכת ההכללה בנתב"ג, בהולנד לא נעשה ניסיון עיקש כל כך להימנע מחשיפת היכולות של התוכנה כלפי הציבור.

העובדה שנושא זיהוי הפנים הפך לסוגיה ציבורית מוכרת, השפיעה על הפיקוח הציבורי בעת הרחבת הטכנולוגית גם למגזר הפרטי. כך, כאשר רשת

101 Sebastien Louradour & Lofred Madzou, *A Policy Framework for Responsible Limits on Facial Recognition, Use Case: Law Enforcement Investigations*, World Economic Forum (2021)

102 **שם**.

103 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data – Publications Office of the EU

104 *Millions of Passport Photos of Innocent Foreigners in Police Face Database*, NL Times (Feb. 4, 2023)

105 **לעיל** ה"ש 99.

סופרמרקטים הולנדית הודיעה ללקוחותיה על שימוש בטכנולוגיה זו כדי לאתר גנבים ומי שהורחקו מהמקום, הרשות ההולנדית להגנת פרטיות פנתה אל הרשת והפנתה אותה לאיסורים החלים בנושא.[106]

המקרה ההולנדי מלמד כיצד מודעות להשפעות של טכנולוגיה תוספתית מסוימת, הקפדה על תהליכים של בחינת חוקיות, היוועצות רוחבית עם רשויות אחרות וכן פעולה בשקיפות כלפי הציבור, אפשרו לרגולטורים בהולנד להיות מודעים להשלכות התוכנה על זכויות אזרח. בזכות זאת הוכנסה הטכנולוגיה בשלבים, בזהירות ותוך כדי בדיקת השפעותיה לאורך זמן.

הטכנולוגיה נכנסה לשימוש לאחר היוועצות בין כמה גופים בממשלה, שבמסגרתה תרם כל גוף ממומחיותו, וכולם פעלו יחד למען שילוב נכון של הטכנולוגיה. ניתן לראות כיצד הוגדרו והוטמעו ערכים בתוך הליך קליטת התוכנה, ואלה עזרו לשמור על הרגולטורים מלחרוג בכל השלבים השונים. נוצרו כללים אתיים עקרוניים, סטנדרטים שנועדו להגן על זכויות הפרט וכן חובות פרוצדורליות בנוגע לאימוץ הטכנולוגיה – שביקשו כולם לוודא כי הטכנולוגיה מנותבת בהתאם לנורמות שנקבעו מראש.

קיים הבדל ניכר בין הליך קליטת הטכנולוגיה בהולנד לבין ההליך במדינות שונות בארצות הברית. בארצות הברית ביצעה המשטרה מעצרים על סמך זיהויים אוטומטיים, ללא מעורבות וביקורת אנושית, והביאה בכך למעצר שווא של חשודים, בעיקר כהי עור, שהתוכנה שהשתמשו בה נטתה לזהות דמיון בינם לבין חשודים בעקבות הטיות במאגר הנתונים ובאלגוריתם המזהה.[107] קליטת טכנולוגיה ללא מעורבות וביקורת אנושית התרחשה גם בשימושים נוספים של בינה מלאכותית בהקשר של ההליך הפלילי, בעיקר בכל הקשור

106 *Dutch DPA Issues Formal Warning to a Supermarket for its Use of Facial Recognition Technology,* European Data Protection Board (2021)

107 T. J. Benedict, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 Wash. Lee L. Rev. 849 (2022)

לאלגוריתמים המיועדים לחיזוי פשיעה. אלו נכנסו לשימוש ראשוני בארצות הברית בשותפות בין חברות טכנולוגיה לבין גופי משטרה במדינות שונות, כגון משטרת לוס אנג׳לס.[108] בדיעבד, התברר שהמידע ששימש לאימון מערכות אלה הגיע בעיקר מדוחות עבר של שוטרים, ולכן היה מוטה בעקבות שיטות הפעולה האופייניות של המשטרה. הדבר הביא לאכיפה בררנית ומפלה באמצעות האלגוריתם, שחיפש פשיעה במקומות שבהם ניתנו דוחות ולשיטור יתר כלפי אוכלוסיות מסוימות. סוגי עבירות שלא היו מתועדים במאגר המידע, כגון עבירות צווארון לבן ואלימות במשפחה, זכו להתעלמות מצד המערכות, עובדה שהגבילה את האמון בה.[109] מחקרי המשך הראו יעילות מוגבלת של המערכות, והדיון הציבורי והמשפטי הביא להפסקת השימוש בהן כמה מדינות בארצות הברית ואף אסר על שימוש בהן.[110]

רצף ההתרחשויות בארצות הברית ובמדינות אחרות בנושא כניסת הטכנולוגיות פגע קשות באמון הציבור הן בכוונות הרשויות והן בטכנולוגיה שהתכוונו להכניס לשימוש. התפיסות האוהדות שלהן זכתה עד אז הטכנולוגיה פינו את מקומן לחשדנות גבוהה, באופן שאף עורר חשש מפני פגיעה בהתקדמות טכנולוגית.[111]

108 Ali Winston, *Palantir has Secretly been using New Orleans to Test its Predictive Policing Technology*, 27 The Verge (2018)

109 Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. Online 15 (2019)

110 ראו למשל, איסור שנכנס לתוקף בסנטה קרוז בארצות הברית בשנת 2020.

111 Atkinson et al., **לעיל** ה"ש 96.

ה. סיכום ביניים: הטמעת טכנולוגיות ללא אמצעי בקרה

מתוך שלושת מקרי הבוחן הראשונים, על אף השונות ביניהם, אנו למדים על שלושה כשלים חוזרים בעת אימוץ מערכות טכנולוגיות על ידי רשויות שלטון. כשלים אלה מהותיים, והימנעות מהם הייתה יכולה למנוע חלק לפחות מן התוצאות השליליות, הן בצמצום הנזק שהסבה הטכנולוגיה ושהביא את בתי המשפט להוציא פסקי דין המבטלים את האפשרות להשתמש בה בדיעבד, והן במניעת משברי באמון מול הרשויות שהטמיעו את הטכנולוגיה. להלן סיכום שלושת הכשלים:

1. היעדר דיון רוחבי והליכי היוועצות טרם הכנסת טכנולוגיות לשימוש

כפי שהראינו בפרק הקודם, אחד העקרונות העשויים להפחית את החשש מפני כשלים ברכישת טכנולוגיות חדשות ובהטמעתן הוא דיון רוחבי בין־משרדי המערב גם מומחים, ועוסק בניהול סיכונים[112] ובהערכת השפעות קצרות וארוכות טווח. מטרות הדיון הרוחבי הן לנתב את שיח הרכש וההטמעה של טכנולוגיות לסוגיות חברתיות רחבות ומהותיות, לעמוד על השלכות השימוש בטכנולוגיות על זכויות אדם וכן להתגבר על "פערי שפה" בין דיסציפלינות שונות: משפט, טכנולוגיה, אכיפת חוק, רכש ועוד. הדיון יכול לסייע בזיהוי מוקדם של בעיות שעלולות להתגלות מאוחר מדי. עם זאת, במקרי הבוחן ניתן למצוא מידע דל בלבד המתעד הליכי היוועצות וחשיבה כאלה.

במקרי הבוחן הישראליים, הייעוץ המשפטי הפנימי הוא זה שבמקרה הטוב ליווה את התהליך, אך אין זה ברור שהתאים ביכולותיו למשימה.[113] בהיעדר שיתוף של

112 על הליך ניהול סיכונים ראו Marjolein Brigit Agnes, Van Asselt, & Ortwin Renn, *Risk Governance*, 14 J. Risk Res. 431–449 (2011). מדיניות לניהול סיכונים קיימת במשרד ממשלת ישראל. כך למשל, במשרד התקשוב, קיימת הנחיה בעניין ניהול סיכונים, ראו הנחיה 1.3.01 עקרונות לניהול סיכוני תקשוב במשרדי הממשלה (2.7.2024).

113 זאת, בלי להיכנס לעובי הקורה של הטענה ולפיה המידע העובדתי שהועמד בפני הייעוץ המשפטי לא היה מלא.

משרדים שונים ומומחים, התנהל בין גורמי המקצוע הטכנולוגיים לבין הגורמים המשפטיים המלווים "שיח של חירשים", שבמסגרתו יכולות הטכנולוגיה לא היו מובנות לגורמי הפיקוח, ופערי ההבנה יצרו כשלים. כשל זה בולט במיוחד בעניין פגסוס. דוח ועדת מררי מציין במפורש כי הגורמים (המעטים) שאישרו את השימוש בטכנולוגיה לא הבינו אותה לעומקה.[114] הבנה מעמיקה של דרך הפעולה של הרוגלה, הייתה מובילה לתובנה שהיא אינה רק אוספת מידע בתנועה ומיירטת אותו, אלא גם אוספת מידע אגור. לו תובנה זו הייתה עולה לדיון, הדבר היה משפיע על הליך ההטמעה ומונע את הכשלים בהמשך, למשל מה לעשות עם המידע האגור שנאסף.

2. היעדר נהלים מסודרים לרכישת טכנולוגיות מתקדמות ולהפעלתן

בשלושת מקרי הבוחן שסקרנו לא נעשה הליך סדור לקליטת הטכנולוגיה, וממילא במסגרת רכישת התוכנה לא פורסמו נהלים לגבי השימוש בה: החל בהגדרת מקרים שבהם אין להשתמש בה או מאפיינים טכנולוגיים של המוצרים שנכון לנוון; עובר בשרשרת אחריות ודרישה לקבלת אישורים במקרים פרטניים של שימוש; וכלה במעקב אחר יעילות הטכנולוגיה.

הדבר גרר פגמים בהליך אפיון המוצרים, בהליכי הרכישה וההטמעה ובבניית ממשקים חסרים, אף שהיו בנמצא פתרונות ישימים ופשוטים. כך למשל, עלה כי בפועל מערכת ההכללה בנתב"ג הופעלה ללא שיקול דעת של השוטרים בנמל התעופה, אף שמדובר במערכת שמתכנניה ראו בה מערכת ממליצה ומסייעת בלבד.[115] מצב שבו תוכנה ממליצה הופכת לתוכנה מחליטה, המחליפה שיקול דעת אנושי, מבטא כשל מוכר שנגרם מאפיון לא נכון של המערכת ומהדרכה לא נכונה כיצד להשתמש בה.[116] מדובר בכשל שניתן להתגבר עליו בפשטות

114 ראו דוח מררי (**לעיל** ה"ש 50), עמ' 4.

115 על מעמד המערכת כפי שהוצגה בוועדת הכנסת אל מול עדויות השוטרים לעניין דרך פעולתם על פי המלצות המערכת בנתב"ג, ראו **לעיל** ה"ש 78.

116 Rebecca Crootof et al., *Humans in the Loop*, 76 Vand. L. Rev. 429 (2023)

יחסית בעת בניית הממשק.[117] תהליך כזה היה מונע הפעלה של המערכת באופן שרירותי יותר מזה שמתכנניה סברו שיש להפעיל.

יתרה מזו, היעדר נהלים ומעטפת משפטית מתאימה, ובכלל זאת טיעונים המגינים על השימוש בטכנולוגיה – חשף את הרשויות לתביעות מצד אזרחים שנפגעו ממנה.

3. היעדר מעקב, שקיפות, תיעוד ותיקוף לאחר יישום טכנולוגיה, והסתרת היכולות לאחר פרסום

משלושת מקרי הבוחן עולה שלא הוכנו, וממילא לא בוצעו, תהליכי בדיקה ותיקוף וכן "מחקרי פעולה" בנושא הפעלת הטכנולוגיות שנכנסו לשימוש, במטרה לעמוד על טיב ההפעלה. כך, למשל, לא נבדק אם המשתמשים האנושיים רואים בתוצר של מכונה המלצה או החלטה סופית; לא נבחנה מידת הדיוק של ההחלטות; ולא נמדדה מידת היעילות של הטכנולוגיה במילוי המשימה שלשמה הוטמעה. יתרה מזאת, גם לאחר חשיפת השימוש המדינתי בטכנולוגיה, בעקבות תקיפתה על ידי אזרחים שנפגעו ממנה או חשיפתה בעיתונות, ניתן לראות מגמה של ניסיונות להסתיר את דרכי פעולתה אגב שימוש בטיעונים שונים: החל בקניין רוחני ורצון להגן על בית התוכנה שממנו נרכשה הטכנולוגיה וכלה ברצונה של המשטרה לשמור על חסיון שיטות פעולתה.[118] דומה שחלק מן ההסתרה לא שירת טיעונים אלה, אלא ניסה לחפות על היעדר התיעוד והתיקוף של השימוש בטכנולוגיה.

להסתרת היכולות ולהיעדר שקיפות יש גם ביטוי חיצוני שלילי משום שכלל הציבור לא מודע למתרחש, וגם כאשר מתפרסמות סוגיות עקרוניות הן לא זוכות לעניין רב בשל מורכבותן. כך קרה במקרה האמריקני וכן בעניין מערכת ההכללה בישראל. עם זאת, השימוש במערכת פגסוס זכה לפרסום על רקע

117 **שם.**

118 לעניין חלק מהפרטים, ראו תומר גנון "האלגוריתם שיעצור אתכם בנחיתה בנתב"ג", **כלכליסט** (10.11.2022).

ההקשר הפוליטי והחשש שנעשה שימוש בטכנולוגיה בחקירות ראש הממשלה נתניהו.[119] מערכת ההכללה עד כה לא עוררה עניין דומה.

בראייה לאחור קשה להבין כיצד ייתכן שנרכשו ונקלטו הטכנולוגיות שתיארנו במקרי הבוחן, ללא הליכי בקרה, אף שמדובר ברשויות שעובדיהן אמורים להיות בעלי מקצוע וניסיון. לכאורה אמור היה להיות ברור לרשויות במחוז יוסטון כי מורה מפוטר זכאי לקבל את המידע הדרוש לו כדי לערער על פיטוריו. מפתיע גם שאיש במשטרת ישראל לא חשש שחדירה מרוחקת לטלפון נייד עלולה להיתפס כקו אדום ציבורי ומשפטי. הכשלים הללו מתבלטים על רקע ההשוואה למקרה הבוחן הרביעי, שבו הולנד לא כשלה באף לא אחד מן הליקויים המתוארים.

הקושי בבקרה ובפיקוח על הטמעת טכנולוגיות חדשות – מוכר.[120] קושי זה, מקובל להניח, נובע מכמה סיבות: היעדר מומחה משרדי, רשויות או מומחים בתוך השלטון שתפקידם להתמודד עם טכנולוגיות חדשות; היעדר חקיקה מתאימה ועדכנית; תגובה איטית של המוסדות לאתגרים טכנולוגיים וקושי להדביק את קצב ההתפתחות; התעצמותן של חברות פרטיות המשפיעות על תהליכי רכש ובחירות טכנולוגיות; קיומן של בעיות שהופכות מורכבות יותר בהשוואה לעבר – בין מן הבחינה המעשית־טכנולוגית ובין מן הבחינה המשפטית – באופן שמקשה לספק פתרון מתאים, על רקע הזמן הדוחק והמשאבים המוגבלים שעומדים לרשות מוסדות השלטון.

עם זאת, קשה לייחס את הכשלים שעליהם הצבענו רק לתרבות פוליטית וארגונית ספציפית או לרמת מומחיות חסרה, משום שמדובר במגוון מדינות

119 הדיון הציבורי התעורר בייחוד סביב הכוונה לבחון תיקים קיימים, אגב הדגשת תיקי ראש הממשלה. ראו, למשל, יהונתן ליס וחן מענית "הממשלה אישרה את הקמת הוועדה לבדיקת פרשת פגסוס, תבדוק תיקים מתנהלים" **הארץ** (27.8.2023).

120 דוגמאות לכישלונות של מערכות התבטאו בהטיות גזעניות של מערכות מבוססות בינה מלאכותית, והצעות לתיקון שעלו אחריהן. ראו למשל: Julia Angwin et al., *Machine Bias,* Pro Publica (May 23, 2016); Sina Fazelpour & David Danks, *Algorithmic Bias: Senses, Sources, Solutions*, 16 Philos. Compass (2021); וכן Wallach & Marchant, **לעיל** ה"ש 26.

ורשויות. גם אין לנמק זאת בסוג הטכנולוגיות שהוטמעו, משום שמדובר בכשלים דומים של טכנולוגיות שונות. ניתן עוד לטעון כי חלק מן הכשלים היו נמנעים לו הרשויות האמונות על התפר שבין השלטון לבין טכנולוגיות חדשות, כגון רשות התקשוב הממשלתי, ישראל דיגיטלית או הרשות להגנת הפרטיות, היו ממלאות תפקיד בולט ופעיל יותר.[121] ייתכן שכל אחד מן ההסברים האלה הוא נכון, וכולם יחד תורמים למארג הכשלים. ואולם, אין בנימוקים שהצגנו כדי להסביר את הכשלים בנושאי כתיבת הנהלים והשקיפות שהיו נחלת גם רשויות בעלות ידע טכנולוגי וניסיון עשיר בהסדרה באמצעות נהלים.

ההסברים גם חלשים יותר כאשר מדובר בטכנולוגיות שהמדינה רוכשת מחברות מסחריות או מפתחת בעצמה לצורך הפעלה ככלי שלטוני, לעומת מצב שבו המדינה נדרשת, כרגולטור, רק לפקח על יישומן של טכנולוגיות בשוק הפרטי. בתהליכי רכש וייצור למדינה יש, או אמורה להיות, גישה למידע ולכלים שיאפשרו לה להתגבר לפחות על בעיית האוריינות הדיגיטלית. במקרה הבוחן של מערכת ההכללה בנתב"ג, לקחה המשטרה חלק נכבד בפיתוח הטכנולוגיה, ולכן אמורה הייתה להיות בקיאה בדרך פעולתה של המערכת וברמת מורכבותה. לפיכך, קשה להניח שבמקרה זה מדובר בכשל הנובע מחוסר מידע. גם במקרים שבהם רכשה המדינה טכנולוגיה מספקים פרטיים ולא ביצעה את הליך הפיתוח בעצמה, הרי שבמסגרת הליך הרכישה היו בידיה אפשרויות לבחון מידע טרם קבלת ההחלטה על הרכש.

יתרה מזאת, דווקא כאשר מדובר ברכש ממשלתי, החשש שיצרניות הטכנולוגיה המפתחות נוזקות מעקב ישליכו על המדינה את האחריות ויטילו עליה את האשמה בעת שימוש לרעה בתוכנה הוא מוחשי יותר מזה שקיים במקרי רכש של המגזר הפרטי. מצד אחד, לטענת החברות הן מוכרות רישיונות שימוש לנוזקות המעקב לרשויות אכיפת מדינתיות בלבד ולמטרות לגיטימיות הקשורות בהגנה על הביטחון הלאומי ומניעת טרור, ואין ביכולתן לדעת מהו השימוש

121 דוגמה לטענות בדבר נזקים שנגרמו בעקבות פעולה לא מקצועית של רגולטור ניתן למצוא, למשל, אצל ע"א 6313/19 **רשות ניירות ערך נ' רותם שמואל** שבמסגרתו הפך בית המשפט העליון החלטה של השופטת רות רונן במחוזי, שבה הטילה אחריות על רשות ניירות הערך בטענה שבגין התרשלותה נגרמו נזקים למשקיעים בחברת "יוטרייד".

שעושים הלקוחות בפועל בנוזקת המעקב או לפקח עליו.[122] מצד אחר, רשויות מדינה הרוכשות טכנולוגיה נוטות להעביר את האחריות אל ה"מכונה" או אל "המערכת", בייחוד במקרים של טעויות. כך נוצר מצב של ריק מבחינת האחריות.

בפרק הבא נציג את היעדר הזיהוי של הטכנולוגיות החדשות כמשבשות, כזווית התבוננות נוספת בכישלונות שתוארו בפרק זה.

122 ראו, למשל, תגובת חברת הסייבר האיטלקית RCS Lab: Apple and Android *Phones Hacked by Italian Spyware, Says Google,* Reuters (June 23, 2022); וכן תגובת NSO הישראלית Ronen Farrow, *How Democracies Spy on their Citizens*, The New Yorker (April 18, 2022)

פרק 3

קושי בזיהוי טכנולוגיות משבשות

אנו סבורים כי מקור אפשרי לכשלים שהתגלו במקרי הבוחן שתוארו בפרק הקודם הוא קושי לזהות טכנולוגיות חדשות כטכנולוגיות משבשות (disruptive technologies) והתייחסות מוטעית אליהן כתוספת רכש רגילה המיועדת לייעול תפקודה הרגיל של הרשות, במקום להתייחס אליהן כאל כלים המשנים את כללי המשחק. מדובר בפער תפיסתי עקרוני שבעקבותיו המערכת אינה מכיילת את עצמה ואינה מפעילה את שיקול הדעת והכלים הרגולטוריים המתאימים כדי הביא את מירב התועלת החברתית והכלכלית וכדי להתמודד עם השפעות חיצוניות שליליות של הטכנולוגיה החדשה.

המונח "טכנולוגיה משבשת" הוטבע על ידי באוור וקריסטנסן[123] כדי לתאר המצאות החותרות תחת מבנה שווקים קיים או קו מוצרים קיים ומחליפות אותם במבנה חדש. ברמה התחרותית, היא יכולה לשבש את מבנה השוק הקיים עם כניסתם של מתחרים חדשים או עלייתם של יצרנים מסוימים על חשבון אחרים.[124] שיבוש נוסף הוא ביצירת שחקנים חדשים, כגון מתווכי תוכן שבאו לעולם עם כניסת הרשתות החברתיות.[125] לעיתים, השיבוש מתרחש גם ברמה החברתית,[126] עם שינוי פערי הכוחות בין קבוצות שונות בחברה, כמו היכולת

123 Joseph L. Bower & M. Clayton M. Christensen, *Disruptive Technologies: Catching the Wave,* 73/1 Harvard Business Review, 43, 43–53 (January–February, 1995)

124 Yu Dan & Hang Chang Chieh, *A Reflective Review of Disruptive Innovation Theory*, 12 (4) International Journal of Management Reviews, 402–414 (2008)

125 Tarleton Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media (2018)

126 Carla Millar et al., *Disruption: Technology, Innovation and Society*, 129 (4) Technological Forecasting and Social Change, 254 (2018)

ליצור קהילות חדשות וכוח צרכני באמצעות שיתוף מידע מהיר המתאפשר באמצעות הרשתות החברתיות.

הגדרה זו מאפשרת להבין תופעות וישנות כאחת. למשל, באמצע המאה ה־20 "מודל טי" של מכונית פורד נחשב לטכנולוגיה משבשת, לאור יכולת הייצור ההמונית שהורידה את מחיר הרכב והפכה אותו בר השגה למשפחות מעמד הביניים.[127] יכולת ניהול שיחה על גבי רשת האינטרנט, מאפיינת את הטכנולוגיה המשבשת של תחילת המאה ה־21.[128] טכנולוגיות שהתפתחו בעקבות כניסתה של בינה מלאכותית, כגון כלי רכבי אוטונומיים, בינה מלאכותית יוצרת[129] ואחרות, הן טכנולוגיות משבשות של העשור השלישי של המאה ה־21.

טכנולוגיה משבשת מביאה עימה לעיתים קרובות צורך ברגולציה חדשה או מותאמת כדי לאפשר את הטמעתה או פיקוח עליה.[130] חוקרים נדרשים לעסוק במתח שנוצר בעקבות הצורך לנהל סיכונים רגולטוריים בנושא הטכנולוגיות המשבשות:[131] מחד גיסא, מיתון הסיכונים הפוטנציאליים לכלכלה, לחברה, למשטר ולפרטים בתוכם; ומאידך גיסא, פעילות בתנאי אי־ודאות וחשש מפני דיכוי התפתחות טכנולוגית על היתרונות שהיא מביאה.

כאשר טכנולוגיה משבשת אינה נתפסת ככזאת בשרשרת הפיתוח והיישום שלה, או כאשר שחקנים אינם תופסים את הטמעתה כשיבוש, נוצר פער תפיסתי ומושגי

127 Lindsay Brooke, Ford model T: The Car That Put the World on Wheels (2008)

128 Gregory S. Yovanof & George N Hazapis, *Disruptive Technologies, Services, or Business Models?* 45 Wirel. Pers. Commun., 569–583 (2008)

129 Yogesh K. Dwivedi et al., *Opinion Paper: "So What if ChatGPT Wrote It?": Multidisciplinary Perspectives on Opportunities, Challenges and Implications of Generative Conversational AI for Research, Practice and Policy*, 71 Int. J. Inf. Manage. 102642 (2023)

130 Mathias Klang, Disruptive Technology: Effects of Technology Regulation on Democracy (2006)

131 Marta Katarzyna Kołacz, Alberto Quintavalla, & Orlin Yalnazov, *Who Should Regulate Disruptive Technology?* (May 6, 2019)

המשפיע על ההיערכות לכניסתה לשימוש. השחקנים אינם מפעילים כלי בקרה שהיה מצופה מהם להפעיל בנסיבות העניין, אינם מתקינים כללים חדשים, אינם יוצרים בלמים ואיזונים ואינם שוקלים שיקולי רוחב שהיה מצופה מהם לשקול, לו הייתה הטכנולוגיה נתפסת כמשבשת.[132] אי־ראיית טכנולוגיה כמשבשת גורמת למרחבי עיוורון לגבי הבנת הסיטואציה שבה נדרש דיון.[133]

נקודת הזמן שבה מתגלה כי טכנולוגיה משבשת, מתרחשת מטבע הדברים רק בעת שהיא מתחילה להביא לשינויים ניכרים. המשמעות היא שבשלבים שקדמו לכך – שלבי האפיון, הפיתוח וההטמעה הראשונית – קשה לזהות אם אכן מדובר בטכנולוגיה שתשבש בסופו של דבר את המבנה הקיים או שמא תוביל לשינוי קל בלבד. לעיתים גם חולף זמן בין ההבטחה השיווקית והציפייה כי הטכנולוגיה תגרום לשיבוש לבין מימושו בפועל, כפי שקיים למשל לגבי שוקי הרכב האוטונומי ולגבי משקפי מציאות רבודה, שההבטחות הגלומות לגביהם טרם התממשו אף שברי כי אם ימומשו ייווצר שיבוש.

שחרור גרסת הבטא של פלטפורמת הבינה המלאכותית היוצרת "ChatGPT" על ידי חברת "OpenAI" הפתיע את העולם, כאשר אומצה על ידי יותר ממאה מיליון משתמשים במשך זמן קצר.[134] השיבוש שעושה הטכנולוגיה כה משמעותי עד שרגולטורים בכל העולם עסוקים בניסיון למנוע ניצול לרעה של הטכנולוגיה החל בהפרת זכויות יוצרים ופגיעה בפרטיות,[135] עובר בסוגיות מקרו, כגון השפעתה

132 Barrie Sander, *Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law*, 32 Eur. J. Int. Law 159 (2021). סנדר מתייחס הן לכישלונן של המערכות להביא בחשבון את השלכות המידע הכוזב ברשתות החברתיות, והן להיעדר תגובת המערכת בעקבות אי־ההבנה של הרכיב המשבש במדיה החברתית.

133 תהילה שוורץ אלטשולר "'הטכנולוגיה תבלום': אינסוף טכנולוגיה כפול כמעט אפס חיילים שווה כמעט אפס תגובה" **דה מרקר** (7.11.2023).

134 Gohil Shivbhadrasinh, *ChatGPT Statistics & Facts to Know in* 2024, Meetanshi (Jun 13, 2024)

135 על האסדרה של בינה מלאכותית ראו כהנא ושוורץ אלטשולר, **אדם, מכונה, מדינה (לעיל** ה"ש 87).

על שוקי התעסוקה ועל דרכי הוראה והשכלה,[136] וכלה בחשש מפני הפצת מידע כוזב והשפעה על יכולת בירור המציאות במשטרים דמוקרטיים.[137]

במרחב אבטחת הסייבר הקושי לנבא איזו טכנולוגיה תהפוך משבשת גדול אף יותר.[138] מייקל היידן, מי שעמד בראש הסוכנות לביטחון לאומי של ארצות הברית (NSA) וגם בראש סוכנות הביון המרכזית (CIA), כתב בנושא ש"קיימות מעט תופעות חברתיות כה חשובות ומדוברות שיש לגביהן הבנה כה מועטה".[139] היידן הדגיש שהוא אינו מתייחס לטכנולוגיה ספציפית או לרמה הטקטית של הפעלת כלי כזה או אחר, אלא לחוסר במסגרת תפיסתית שמאפשרת להבין את ההשלכות של השימוש בכלים ובטכנולוגיות ולדון בהן.[140]

על רקע זה, ניתן להבין מדוע הטכנולוגיות שנסקרו במקרי הבוחן – מדידת הערכת מורים, רוגלות לחדירה מרחוק לטלפונים חכמים ומערכת הכללת חשודים בכניסה לארץ – לא נתפסו כטכנולוגיות משבשות בעיני מי שעסקו ברכישתן ובהטמעתן. המערכת למדידת מורים, נתפסה ככלי שהתווסף לאמצעי מדידת הערכת הוראה שהיו כבר לפניו. הלכה למעשה הייתה זו הפעם הראשונה שה"מחשב פיטר אדם", כלומר שאדם פוטר מעבודתו כתוצאה מחישוב כלשהו, לכאורה אובייקטיבי, שאותו לא יכול היה להבין ולא הוסבר לו. אין זה מפתיע

136 Ali Zarifhonarvar, *Economics of ChatGPT: A Labor Market View on the Occupational Impact of Artificial Intelligence*, 3 (2) Journal of Electronic Business & Digital Economics, 100–116 (2024)

137 Yue Huang & Lichao Sun, *Harnessing the Power of ChatGPT in Fake News: An in-depth Exploration in Generation, Detection and Explanation*, arXiv Prepr. arXiv 2310.05046 (2023)

138 Samuel Mbonu, *Cybersecurity Innovations and Disruptions: What to Know before Adopting New Technologies*, Forbes Technology Council (December 19, 2022)

139 Michael V. Hayden, *The Future of Things Cyber*, 5 Strateg. Stud. Q. 3–7 (2011). התרגום לעברית מתוך כהנא ושורץ אלטשולר, **אדם, מכונה, מדינה** (**לעיל** ה"ש 87).

140 **שם**.

אפוא שמורכבותו של האלגוריתם בבסיס המערכת או העובדה שהוא אינו ניתן להבנה על ידי המורים מושאי המלצותיו לא עלו למודעות הגורמים האחראים.

גם מערכת פגסוס נתפסה בעיני המשטרה כאמצעי משלים אשר יאפשר האזנת סתר לשיחות VoIP[141] ונרכשה במסגרת הצטיידות משטרתית כוללת כדי לטפל במורכבות הטכנולוגית של עולם הפשיעה.[142] ההנחה כי מדובר בתוספת המשכית ליכולות קיימות הייתה רווחת והתבטאה בתשובות שסיפקה המשטרה לתקשורת בשאילתות השונות.[143] אולם, לא בכדי כונו נוזקות מעקב אמצעי "שובר שוויון" (game–changer), כלומר אמצעי המביא לשינוי פרדיגמה של ממש מבחינת הגישה לתקשורת פרטית, ומשלב רמת פולשנות שאין שנייה לה עם מאפיינים שהופכים כל אמצעי אבטחה משפטי או טכני לחסר משמעות.[144] כאמור, בניגוד ליירוט נתוני תקשורת מחברת הטלפוניה, המאפשר איסוף נתונים דוגמת מספר הטלפון שממנו יצאה השיחה, יעד השיחה, מיקום המכשיר, תא השטח שממנו התבצעה השיחה או נשלחה הודעת טקסט והיסטוריית הגלישה באינטרנט, נוזקת המעקב מאפשרת לגבש תמונה מפורטת ומדויקת לגבי חייו האישיים של יעד המעקב, לרבות קשריו החברתיים והמקצועיים, דעותיו ומחשבותיו.[145] גורמי הרכש במשטרה לא הבחינו כי לראשונה מוענקת לגוף אכיפה פלילית, להבדיל מרשויות מודיעין, יכולת חדירה מרחוק – שמעולם לא הייתה ברשותו קודם לכן – לשאוב את כלל הפעילות הדיגיטלית של בעל

141 קיצור של Voice Over Internet Protocol, כלומר שיחות על גבי המרשתת שמתווכות על ידי אפליקציה, בניגוד לשיחות המנותבות באמצעות מרכזייה טלפונית.

142 על התפיסה של שיחות אלו כמקור לעבירות פליליות, ראו ערן גבאי "10% מתנועת השיחות הבינלאומיות – לא חוקיות" **הארץ** (3.3.2003).

143 "המשטרה רוכשת כלים טכנולוגיים מחברות חיצוניות, גם בתחום התקשורת והסייבר. החברות החיצוניות אינן חשופות למידע מודיעיני או לתוצרי המידע החקירתי. הפעלת הכלי הטכנולוגי לצורך משטרתי נעשית על ידי גורמי המקצוע של משטרת ישראל ולא על ידי עובדי החברות החיצוניות", מתוך לירון לוי "המפכ"ל על השימוש בכלי הריגול של NSO: 'לא מופעל על אזרחים תמימים'" **ynet** (18.1.2022).

144 *European Data Protection Supervisor*, Preliminary Remarks on Modern Spyware, 2, 4–5 (Feb. 15, 2022)

145 Deibert, **לעיל** ה"ש 53.

הטלפון, כלומר לפלוש למרחב חייו האישיים. רק כעבור זמן רב ניתן היה לראות ניצנים ראשונים של הבנה כי ייתכן שמדובר בשינוי מהותי שהיה צריך לתת עליו את הדעת.[146]

דווקא המאפיין המשבש במערך יחסי הכוחות שנוצר עם השימוש בתוכנה שבלחיצת כפתור אפשרה גישה לכל מכשיר טלפון בעולם – זה שהביא לידי המשטרה יכולות שמעולם לא היו ברשותה – הוא זה שנעלם מעיניהם של אלה שהטמיעו את התוכנה והשתמשו בה. משהתגלה, הציבור הזדעזע מכך שעוצמה חזקה כל כך הועברה לידי גופי אכיפה פליליים, ולא רק לאלו העוסקים בביטחון המדינה. לא היה זה בעיני רבים עניין של סמכות תאורטית בחוק, אלא כלי עוצמתי מדי שבעיני רבים אסור היה לו להגיע לידיהן של רשויות אכיפה העוסקות בעניינים פליליים בלבד.

מן ההתייחסויות שהציג בא כוח המדינה בפני בית המשפט בנוגע למערכת ההכללה עולה שהמערכת נתפסה כאמצעי לייעול החיפוש בכליהם של המוני הנכנסים לארץ. מי שהיו מעורבים ברכש ובשימוש במערכת לא נתנו את דעתם לכך שמדובר בהעברת שיקול דעת לידי מכונה שמפעיליה אינם יודעים או מבינים מדוע החליטה כפי שהחליטה. נכונותה של המדינה להסתכן בניהול הליכים בערכאות גבוהות ממחישה את חוסר המודעות לסכנות הפוטנציאליות של הטכנולוגיה.

מאחר שהתוכנות לא נתפסו כמשבשות אלא כחלק משגרת רכישת תוכנות, ניתן להבין מדוע לא יושמו לקחי הרכש הטכנולוגי. יתרה מכך, הפקידים בארצות הברית וגם בישראל, ככל הנראה, הסתנוורו מיכולותיהן המיוחדות של הטכנולוגיות ולא הבינו את משמעויותיו העמוקות של המתרחש. נראה בדיעבד שרצונם של אנשי משרד החינוך בטקסס לשפר את ביצועי מערכת החינוך ורצונם של אנשי המשטרה לתת מענה אכיפתי יעיל יותר לבעיית פשיעה גואה – גברו על שיקולים אחרים.

146 ראו לעיל על התפתחות הגרסה שמסרה המדינה, החל בפרסומים ראשוניים וכלה בזו שנאמרה בוועדת חוק חוקה ומשפט, כמפורט לעיל בעמ' 34.

נדגיש פעם נוספת: אין מדובר בשיבוש טכנולוגי וביכולת מסוימת שמוענקת למשתמש מסוים, אלא מדובר בשיבוש חברתי, משטרי ותפיסתי. קשה להתגבר על הקושי לזהות טכנולוגיה משבשת משתי סיבות עיקריות: ראשית, אין תמיד הלימה בין עוצמת השיבוש של טכנולוגיה לבין המחיר שנדרשות הרשויות לשלם תמורתה או להיקף הטמעתה בקרב רשויות שלטון. רשויות השלטון מבצעות רכישות רבות ותדירות, שמטרת רובן לשפר מערכות קיימות. קשה להבחין מתי יש בכוחה של רכישה, שאיננה בהכרח יקרה או מתקדמת במיוחד, להיחשב טכנולוגיה משנה סדרי עולם. שנית, נקודת הזיהוי של טכנולוגיה כמשבשת היא מורכבת, משום שלא תמיד ניתן להעריך שמדובר בשיבוש כבר בשלב הפיתוח, ולעיתים אפילו לאחר הטמעת התוכנה חולף זמן עד שמתגלה השיבוש. מציאות זו מחייבת את הגורמים המעורבים ברכישה ובהטמעה של התוכנה לנהל הליך של חיזוי, שהוא מטיבו מסובך. אתגר נוסף טמון בשאלה באיזה סוג של שיבוש מדובר, טכנולוגי, מוצרי, משפטי או ערכי, חוסר ודאות המשפיע על השאלה איזה גורם יוכל לזהות טכנולוגיה כמשבשת: מפתחים, משתמשים, מומחים, משפטנים ועוד.

בפרק הבא נמליץ על מודל לאימוץ טכנולוגיות מתקדמות, שתכליתו להקל על רשויות שלטוניות להתמודד עם מגוון הכשלים שתיארנו עד כה.

פרק 4

מודל מוצע לפיקוח על רכש והטמעה של טכנולוגיות חדשות: עקרונות ומקורות השראה

א. מבוא: תפיסת המודל

בפרק זה נציע מודל שתכליתו לסייע לרשויות השלטון לצמצם כשלים בתהליכי רכש והטמעה של טכנולוגיות מתקדמות לשימוש מדינתי. המודל מסתמך הן על מגוון הכשלים שזיהינו ונוגעים לצורך בחשיבה רוחבית ורב־תחומית; ביצירת נהלים ותהליכי הטמעה; בשקיפות ומעקב אחר שימוש בטכנולוגיות, והן על אלה הנוגעים לקושי לזהות טכנולוגיות משבשות.

הצעתנו מבוססת על התפיסה שלפיה יש לפעול למיתון החשש מכשלים בעת הטמעת טכנולוגיה בשלושה היבטים:

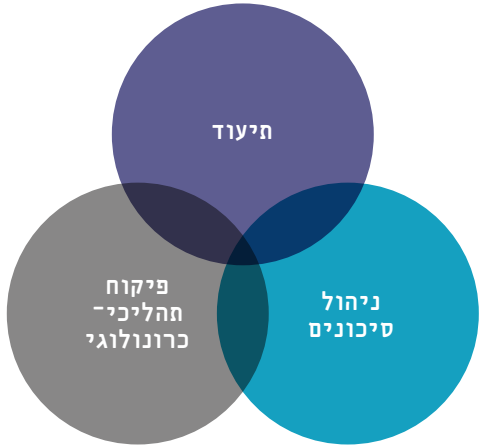
(**1**) הטמעת תהליכי שקיפות ותיעוד מפורטים.

(**2**) יצירת הליך להערכת השפעות, לניהול סיכונים ולזיהוי מאפייני שיבוש.

(**3**) גיבוש תפיסה תהליכית־כרונולוגית המתייחסת למעגל החיים של מערכות טכנולוגיות.

נתמקד תחילה בפירוט שלושת ההיבטים הללו (ראו להלן תרשים 1) ובהמשך נפרט את מקורות ההשראה של המודל המוצע.

תרשים 1
פעולות למיתון החשש מכשלים



1. תיעוד

מורכבותן של מערכות טכנולוגיות בכלל ושל מערכות בינה מלאכותית בפרט, מערימה קשיים מיוחדים על קובעי המדיניות ועל הרגולטורים בבואם לנסח כללי אחריות ולזהות את השרשרת הסיבתית שעלולה להוביל לפגיעה בזכויות מוגנות בעקבות שימוש שעושות רשויות השלטון בטכנולוגיות. מוסכמה היא שהבסיס לכל בחינה עובדתית הוא משילות נתונים ותיעוד קפדני של הליכי עבודה, מקורות מידע, תיוגים, מודלים, תהליכי עיצוב קוד, הערכת סיכונים ובסיסי נתונים.[147] הבניה נכונה של הליך התיעוד ודרכו תאפשר לתחקר בדיעבד כשלים ותופעות שלא נצפו מראש וגם לעמוד בדרישות המנהליות.[148] לעומת זאת,

147 ראו למשל ס' 10(2) להצעת תקנות הבינה המלאכותית האירופיות, **לעיל** ה"ש 103.

148 בתקנות הכלליות בדבר הגנת מידע (GDPR), למשל, יש חובת תיעוד מפורשת (ס' 30), אך גם משתמעת. החובה המשתמעת מקיפה יותר: בעל מאגר מידע (controller) נדרש להיות מסוגל לספק הוכחות לכך שכל מושאי המידע שבמאגר הביעו את הסכמתם לעיבוד המידע.

הסתמכות על תיעוד חלקי של מסמכי הערכת סיכונים, ללא שאר המסמכים הנדרשים, משולה להישענות על משענת קנה רצוץ.

אנו סבורים כי תיעוד הוא כלי להתמודדות עם אי־ודאות. לפיכך אנו מציעים לקבוע משטר תיעוד איכותי, שסנקציות בצידו, שיאפשר לתחקר בדיעבד נזקים שלא נחזו.[149] יש לקבוע תקנים אחידים של תיעוד כדי לאפשר פיקוח אחיד, יעיל, שיטתי וחוצה רשויות שלטון. אכן, תיעוד אינו חזות הכול אבל באמצעותו ניתן יהיה לזהות, ולו בדיעבד, שגיאות מתודולוגיות וטעויות שהביאו לאפיון ולפיתוח שגויים או להטמעה לקויה.

חובת התיעוד צריכה לעסוק בתקינות הליכי איסוף הנתונים ואימונם או המתודולוגיה הסטטיסטית. אך היא יכולה להתגלם גם בדרישה לדיווח על אירועים מפתיעים או תוצאות הערכה מדאיגות במהלך אימון מערכות; או בדיווח מדעי, כלומר הצגת תיעוד לקהילה המדעית כדי לעודד מחקר מדעי נוסף בנושא.

אין ספק שאת הבקרה צריכים לעשות בראש ובראשונה גורמים פנימיים המעורבים בתהליך האפיון והפיתוח, שיש להם הבנה עמוקה וגישה למכלול הנתונים והמודלים. חברות טכנולוגיה שונות מציעות דוגמאות לטופסי תיעוד כאלה.[150]

2. ניהול סיכונים כפול

תסקירי השפעה ומתודולוגיות לניהול סיכונים הפכו למקובלים בתחומים, כגון הגנת הסביבה, דיני חברות, פיננסים וזכויות אדם. כאשר מדובר במערכות טכנולוגיות מורכבות ומתקדמות, נדרשת התבוננות כפולה: תחילה יש להעריך את פוטנציאל המסוכנות של המערכת כפי שתוכננה; אחר כך יש להעריך את

149 Jessica Morley et al., *Ethics as a Service: A Pragmatic Operationalisation of AI Ethics* 31, 239 Minds and Machines (June 19, 2021)

150 תבניות כאלה מכונות "model cards". ראו למשל את אלו שמציעה חברת גוגל: The value of a shared understanding of AI models

רמת הקשר בין המשימה לבין התוצאה (alignment), כלומר את האפשרות של המערכת לממש פוטנציאל מסוכנות מחוץ לתפקיד שייעדו לה מתכנניה.

היערכות למצב שבו תפעל המכונה כשורה וגם למצב שבו לא תפעל כשורה

הערכה כפולה זו לשני המצבים תהיה הבסיס לקבלת ההחלטות, וכדי שיהיה אפשר להוציאה לפועל יש לפעול בשני מישורים: (א) לנסח כללי משילות ובטיחות, כגון כללים לאימון מכונה אחראי (האם לאמן מודל חדש שניכרים בו סימנים מוקדמים של סיכון, ואם כן – כיצד?) וכללים ליישום אחראי (האם, מתי וכיצד ליישם מודלים שעלולים להיות מסוכנים?); (ב) לקבוע אילו רמות של שקיפות ותיעוד נדרשות במקרה של מודלים שעלול להיות בהם סיכון קיצוני, ואילו בקרות ומערכות אבטחת מידע חזקות יש ליישם בעניינם.

ניהול סיכונים הן למגזר הפרטי והן למגזר הממשלתי

תפיסת ניהול הסיכונים שאנו מציעים משלבת בין שני סוגי ניהול סיכונים: (א) ניהול סיכונים של הפעילות העסקית במגזר הפרטי; (ב) ניהול סיכונים ממשלתי, כפי שמתבטא למשל בהחלטות הנוגעות להפעלת סמכות רגולטורית לפי חוק.[151] הליך ניהול הסיכונים מאפשר למבצע אותו להבחין בין שני סוגי סיכונים: (א) סיכונים מובנים בפעילות באופן כללי או ייחודי; (ב) סיכונים לנזקים משניים בעקבות הפעילות המבוצעת. בהתאם יכול יוזם התהליך להעריך את העלות הכרוכה בפעולותיו ולהחליט, האם וכיצד יש לפעול: האם להכיל את הסיכונים, לצמצם אותם או להימנע מפעילות.

תהליך ניהול סיכונים (או כפי שהוא מכונה גם ניתוח השפעות של סיכונים) בתחום הרגולציה מבקש להבנות את פעילות ניהול הסיכונים של רשויות ממשלה בפעולות רגולטוריות, מתוך כוונה להפוך תהליך זה למוסדר, ולאפשר לשלב בו שחקנים שונים – כגון משרדי ממשלה, גורמים מן המגזר הפרטי וכן

151 משרד ראש הממשלה **מדריך לניהול סיכונים ברגולציה ובמדיניות ציבורית** (גיא מור עורך, יוני 2018, גרסה 1).

ארגוני מגזר שלישי – בתוך הליך ניהול הסיכונים. ניתוח השפעת הסיכונים (risk impact analysis) של רגולציה הוא תהליך להערכת ההשלכות והסיכונים הפוטנציאליים[152] הכרוכים ביישום רגולציה חדשה או בשינוי רגולציה קיימת. המטרה היא להבין כיצד רגולציה עשויה להשפיע על בעלי עניין שונים, על תעשיות ועל הכלכלה בכללותה, ולזהות השלכות אפשריות בלתי מכוונות.[153]

שבעה היבטים עיקריים בניתוח השפעת הסיכונים:

(**1**) **זיהוי בעלי עניין:** קביעה מי יושפע מהרגולציה, כולל עסקים, צרכנים, סוכנויות ממשלתיות והציבור הרחב.

(**2**) **הערכת עלויות ותועלות:** ניתוח העלויות והתועלות הפיננסיות והלא פיננסיות הפוטנציאליות של הרגולציה עבור בעלי עניין שונים.

(**3**) **הערכת ציות:** בחינת ההיתכנות של ציות לרגולציה וזיהוי אתגרים או חסמים פוטנציאליים לציות.

(**4**) **ניתוח השפעה על השוק:** בחינת האופן שבו הרגולציה עשויה להשפיע על דינמיקת השוק, על תחרות, על חדשנות ועל התנהגות צרכנים.

(**5**) **התחשבות בהשלכות לא מכוונות:** זיהוי השפעות שליליות או לא מכוונות פוטנציאליות של הרגולציה, כגון אובדן משרות, ירידה בהשקעות ועיוותים בשוק.

(**6**) **השוואת חלופות:** הערכת שינויים או גישות רגולטוריות כדי למזער סיכונים וכדי להשיג את מרב התועלות.

(**7**) **ניטור וסקירה:** הקמת תהליך לניטור ולבחינה מתמשכים של השפעת הרגולציה כדי להבטיח שהיא נותרת יעילה, מועילה ורלוונטית לאורך זמן.

152 השיח בעניין בדיקת השפעת פעולה רגולטורית מתנהל בערבוביה עם שיח ניהול סיכונים. שיח בדיקת השפעות חייב לכלול בתוכו רכיב של ניהול הסיכון, כלומר בדיקת עלות מול תועלת וכן בדיקת אמצעיים חלופיים למזעור הסכנה.

153 OECD, Recommendation of the Council on Regulatory Policy and Governance (2012)

ניתוח השפעת הסיכונים מסייע לקובעי מדיניות ולרגולטורים לקבל החלטות מושכלות באמצעות גישה מובנית. ניתן להשתמש במידע זה כדי לשפר את הרגולציה, לפתח אסטרטגיות להפחתת הסיכוניסולהבהיר לבעלי העניין את ההיגיון העומד מאחורי ההחלטות הרגולטוריות.[154]

גם במאמר של ון אסלט ורן בנושא ממשל ניהול הסיכונים (risk governance)[155] מציעים הכותבים למסד את הנושא של שיתוף שחקנים, כך שכל מי שיכול להיות מושפע ממהלך כלשהו יהיה חלק מהליך ניהול הסיכונים, הן מטעמים תועלתניים – הגברת מועילות וריבוי דעות, צמצום חיכוכים והגדלת לגיטימציה ציבורית – והן מטעמים דמוקרטיים. הרעיון של ריבוי הדעות בהליך ניהול סיכונים דומה מאוד ללוגיקה שהזכרנו לעיל בנוגע לאימוץ טכנולוגיות, ולפיה שילוב אנשים מדיסציפלינות שונות, ממשרדים שונים וכן עירוב גורמי ממשל ומגזר פרטי – תורמים לגיוון עמדות ומשפרים את ההליך.

3. מעקב תהליכי־כרונולוגי

המודל המוצע כולל תהליך של שלושה שלבים כרונולוגיים היוצרים פיקוח מתמשך, להבדיל מפיקוח חד־פעמי: (א) פיקוח בזמן הליך הרכש של הטכנולוגיה; (ב) פיקוח טרם יישום הטכנולוגיה; (ג) פיקוח במועד נקוב לאחר כניסתה לשימוש. הואיל ועקרונות שונים של פיקוח כגון הוגנות, שקיפות, אחריותיות וניהול סיכונים, מתבטאים בכל אחד מרכיבי מעגל החיים של מערכות טכנולוגיות, כדי ליצור פיקוח אפקטיבי יש להביא בחשבון רכיבים אלו. היעדר התייחסות לרכיבי מעגל החיים עלול ליצור מצב של אסדרת יתר של רכיבים מסוימים והתעלמות מרכיבים אחרים, ומכאן לצמצום האפקטיביות של הפיקוח. למשל, ההתייחסות הרחבה בספרות המשפטית למאגרי נתונים ולהשלכות אפשריות של הפגמים בהם על המוצר הסופי באה במידה רבה על חשבון התייחסות להשלכות הבחירה במודלים שונים או לקשיים שעלולים להתעורר לאחר יישום המודל.

154 **שם**. ראו גם מדריך לניהול סיכונים (**לעיל** ה"ש 145).

155 Van Asselt & Renn, **לעיל** ה"ש 112.

לעומת זאת, תפיסה אינטגרטיבית מביאה בחשבון את מכלול רכיבי מעגל החיים ונדרשת גם לקשרי הגומלין ביניהם. למשל: תכלית המערכת ומסגור הבעיה צריכים להשפיע על בחירת המודל (האם לבחור במודל שיש בו עכירות רבה יותר באשר לדרכים שבהן הוא מקבל החלטות או שלא לאפשר זאת); תוצאות הערכה בשלב בניית המודל מזינות תהליכים להערכת סיכונים, והם בתורם מחייבים קבלת החלטות הנוגעות לאימון המודל, לפרישתו או לאבטחתו; תכלית המודל משפיעה על הבחירה בממשקי המשתמש (האם מערכת המעניקה ייעוץ רפואי אמורה להציג את האפשרות שהיא טועה? האם נכון לספר למשתמש שהוא מתקשר עם מערכת מלאכותית ולא אנושית?).

לפירוק מעגל החיים לחלקים יתרון נוסף: אם כבר בשלב ראשוני, למשל בשלב איסוף המידע, מוערך שיש פגמים, אפשר לטפל בהם כבר אז; ואם מתעוררות הערכות מדאיגות בעניין אימון של מודל אפשר להשהות אותו או להימנע מיישומו המלא.

נמחיש זאת באמצעות שלוש דוגמאות:

דוגמה ראשונה, אם במאגר הנתונים מתגלות הטיות, אפשר להידרש לשאלות כמו הטיית ייצוג (אם למשל מדובר במאגר העוסק במערכת החינוך, אפשר לשאול אם המידע מגיע רק ממוסד חינוכי אחד; באיזה אופן אפשר להשליך ממאגר הנתונים המסוים הזה על כלל האוכלוסייה; האם יש ייצוג יתר לקבוצות אוכלוסייה קטנות) או הטיית מדידה (האם המדידה תופסת את מה שנכון לחפש? ואם מדובר בחיזוי מחלה, האם המודל מודד רק את מי שאובחנו בעבר במחלה זו?). תשובות על שאלות אלו עלולה להעיד על בעיות הטיה במאגר. בתהליך בניית המודל אפשר לדבר על הטיות שנוצרות בעקבות בחירת המודל (למשל, האם בשל תהליכים של דחיסת נתונים, כדי שהמודל יעבוד מהר יותר, נפגעו קבוצות קטנות כבר בשלב האימון?), ואילו לאחר יישום המודל ייתכנו הטיות הנובעות מכך שהמודל אומן בהקשר מסוים (למשל, סיכון לחזרתיות בפשיעה) לצורך הקשר אחר (למשל, קביעת גזר דין).

דוגמה שנייה, נוגעת לשקיפות ולהסברתיות. אין דומה הסברתיות שתכליתה להבהיר כיצד נאסף מידע (מי אסף את הנתונים? מהי התפלגותם? וכיוצא בזה)

להסברתיות שעניינה נימוק החלטה (למשל, אלה המילים שבעקבותיהן נמחק ציוץ פוגעני ברשת חברתית).

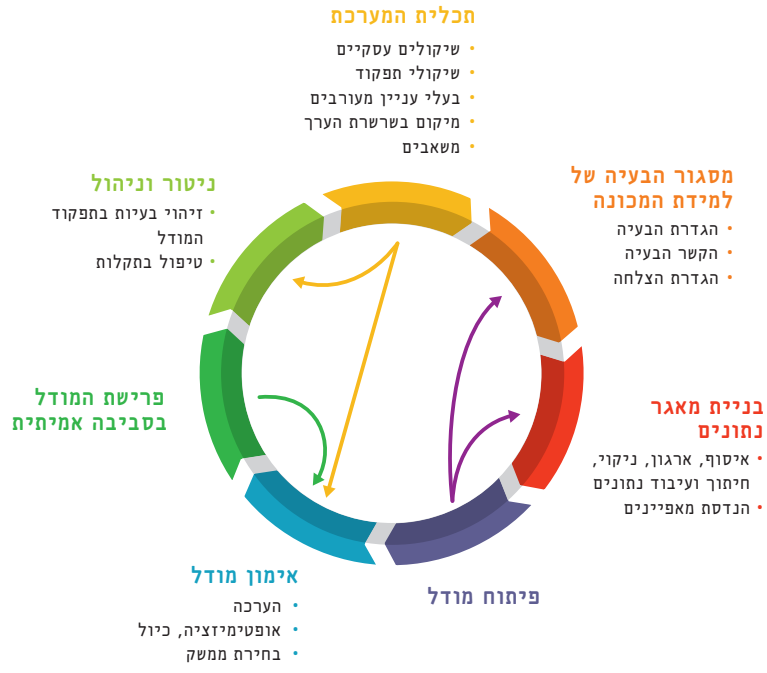
דוגמה שלישית נוגעת להערכת סיכונים. הערכת הסיכונים בבחירה ראשונית של מודל צריכה להסתמך על סבבי אימון קודמים או על בנייה של מודל ניסיוני, אך הערכת סיכונים לאחר סבב אימון ראשוני שמתגלה בו בעיית תאימות בין משימה לבין תוצאה צריכה להוביל להתאמה מחודשת של הנתונים, של הארכיטקטורה ושל משימות האימון, ולעורר את השאלה אם נכון לאמן מודל קטן יותר או חלש יותר, ובוודאי לא להמשיך לאמן מודל בהיקף שתוכנן מלכתחילה.

חלק חשוב בהבנת מעגל החיים של מערכות לומדות נוגע לצורך לנטר אותן לאחר שיושמו בפועל (post deployment) בעולם האמיתי (למשל הבניה של המערכת בתוך מוצר או בתוך ממשק). הסיבה לכך היא שמערכת לומדת, להבדיל ממוצרים אחרים (תרופות למשל), יכולה מעצם טיבה להשתנות גם לאחר יישומה בעקבות המשוב שהיא מקבלת מן המשתמשים.[156] חשוב אפוא לשאול לקראת היישום מה עלול להשתבש? האם המודל בטוח ליישום? ואילו מנגנוני בטיחות נחוצים כדי ליישמו בבטחה? ואם נדרש יישום בהיקף קטן תחילה – מי יקבל התראה במקרה של תקלה? לאחר היישום – יש לבחון למשל באיזו מערכת בקרה לבחור; אם יש ניטור שתכליתו לאתר התנהגויות לא צפויות, בעיקר בסביבות יישום מורכבות (למשל, האם משתמשים מצאו יישומים חדשים או אסטרטגיות הנדסיות חדשות על בסיס המודל?), יש לדווח על אירועים כאלה; אם נדרשים עדכונים למודל לאחר יישומו ואם הם משמעותיים במידה שמחייבת הערכה מחודשת של השלבים שלהם (למשל, תיוג מחדש של הנתונים, אימון מחדש של המודל ובדיקה מחודשת שלו).

156 מִנהל המזון והתרופות האמריקני (FDA) מתחיל בניסוח המלצות כאלו למערכות לומדות בתחום הרפואה, ראו רותי לוי "ה־FDA יקל על שיווק מערכות בינה מלאכותית: המשתנות לאחר שהן מאושרות לשימוש" **דה מרקר** (11.5.2023).

תרשים 2

מעגל החיים של פיתוח ויישום מערכת טכנולוגית



ב. מקורות ההשראה של המודל

המודל שאנו מציעים שואב השראה משלושה מקורות מרכזיים: (א) הליך ניהול סיכונים ברכש והפעלה של בינה מלאכותית שפרסמה ממשלת קנדה;[157] (ב) בחינת השפעות, ניהול סיכונים ובדיקת השלכות אתיות וחוקיות בנוגע לטכנולוגיות זיהוי

ביומטריות על ידי רגולטורים באירופה;[158] (ג) חובות הנוגעות למערכות המוגדרות "בסיכון גבוה" בחוק הבינה המלאכותית האירופי.[159] להלן הפירוט.

1. ההליך הקנדי

ההליך הקנדי לניהול הסיכונים בנושא הבינה המלאכותית (להלן: Algorithmic Impact Assesment — AIA) נוצר על ידי ממשלת קנדה במטרה להבטיח שימוש אחראי ואתי בבינה מלאכותית (במערכות אוטומטיות לקבלת החלטות), באמצעות עידוד מעורבות ציבורית, פיקוח והכשרה של עובדי מדינה ואימוץ אחראי של טכנולוגיות בינה מלאכותית. מועצת האוצר הקנדי מחייבת להשתמש בהליך ניהול הסיכונים בכל מקרה שיש בו כוונה לאמץ מערכת קבלת החלטות אוטומטית על ידי רשות ציבורית. ה־AIA הוא שאלון הערכת סיכונים. חישוב הסיכונים מתבצע לגבי היבטים שונים, כגון השפעה על זכויות, איכות נתונים ופרטי הפרויקט הספציפי. כמו כן, יש לבחון אמצעים חלופיים להפחתת הסיכון, כגון הליכי התייעצויות ופעולות נקודתיות למזעור סיכונים. תוצרי השאלון משמשים לקביעת רמת ההשפעה שעשויה להיות למערכת, החל ברמה 1 (השפעה מועטה) ועד רמה 4 (השפעה גבוהה מאוד). בהתאם לרמת ההשפעה יש להתאים אמצעים למזעור נזקים וליצירת מנגנוני ניטור של תחומים, כגון הטיה ושוויון, אינטרסים כלכליים וקיימות סביבתי – ובקרה עליהם.

המודל הקנדי משמש מקור השראה למודל שאנו מציעים בכל הקשור לבחינת השפעות כלל חברתיות שהן מעבר להשפעות ישירות. עם זאת, המודל הקנדי מוגבל לבחינת השפעות של בינה מלאכותית בלבד, והוא מתבצע במועד אחד בלבד. אנו מציעים מודל רחב יותר כפי שנפרט בהמשך.

158 בשיח הטכנולוגי הרגולטורי באירופה מכונה Biometric Identification Methods.

159 בשם המלא: Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts (להלן: חוק הבינה המלאכותית האירופי).

2. השיח האירופי

מקור ההשראה השני הוא השיח האירופי הער שהתנהל בשנים האחרונות על רקע התפתחות יכולות זיהוי ביומטריות, הן ברמת המדינות השונות והן בפרלמנט ובסוכנויות הכלל־אירופיות. שיח זה עסק בהשלכות האתיות הנובעות מן השימוש בטכנולוגיות אלו ובניהול הסיכונים הכרוך בשימוש בהן. האירופים סברו שזיהוי ביומטרי הוא אמצעי פוגעני על רקע העובדה שהוא מאפשר פגיעה נרחבת בזכויות האדם, ובכלל זאת איתור בנקל של בני אדם במרחב הציבורי.[160] דווקא משום כך התנהל דיון ציבורי ער ומעמיק שהתבסס על מסמכים רשמיים, דוגמת המסמך של הסוכנות האירופית לזכויות אדם בסיסיות (European Union Agency for Fundamental Rights — FRA).[161] מסמך זה בחן את השלכות השימוש בטכנולוגיות אלו בהקשר של אכיפת חוק, ופירט לגבי הזכות לכבוד, הזכות לחיים, הזכות לפרטיות, איסור אפליה, הזכות להליך הוגן, הגנה על מיעוטים והזכות להתאגד ולהפגין; כמו כן הוא עסק בחובות של מנהל תקין במשפט מנהלי.[162] המסמך מנתח בפירוט השלכות והמלצות מרכזיות הנוגעות להגדרה ברורה של ההיתר החוקי הנדרש, ובכלל זאת: קובע גבולות של נחיצות השימוש; מגדיר הוראות מתי יהיה השימוש מותר; ולבסוף מגדיר סטנדרטים לגבי איכות הפעולה של המערכות ומניעת תקלות.[163]

בד בבד בבריטניה, המרכז לחקר חדשנות ואתיקה במידע,[164] שהופעל באמצעות קבוצת חוקרים עצמאית בחסות ממשלת בריטניה, פרסם מסמך הבוחן את השלכות הטכנולוגיה. המסמך מפרט את יתרונותיה של הטכנולוגיה, הן בסיוע

160 להנחיות הסופיות ראו *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*

161 European Union Agency for Fundamental Rights (FRA), Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement: Helping to Make Fundamental Rights a Reality for Everyone in the European Union [FRA Focus] (2019)

162 **שם**.

163 **שם**.

164 שמו שונה מאז ל"מרכז לאימוץ אחראי של טכנולוגיות", ראו את **אתר היחידה**.

באכיפה ובפענוח פשיעה במישור הממשלתי, והן בזיהוי לצורך ייעול מתן שירותים במגזר הפרטי. המסמך עוסק גם בחששות מפני הטכנולוגיה, בדומה למפורט במסמך האירופי, אגב הדגשת ההשפעות האתיות, כגון סוגיות של הסכמה להיות מושא לשימוש בתוכנה;[165] וההשפעה של השימוש בה על ההתאגדות במרחב הציבורי.[166] נוסף על המלצות המסמך האירופי, הצוות הבריטי ממליץ על הגדלת המעורבות הציבורית בהטמעת התוכנה, וכן על אימוץ סטנדרטים ורגולציה עצמית, שיתווסף למארג החקיקה.

שני המסמכים הללו – האירופי והבריטי – השפיעו במידה רבה על השיח הציבורי בנושא, וגם על החלטת הפרלמנט האירופי לאסור באופן גורף שימוש בטכנולוגיות אלו במרחב הציבורי בזמן אמת, ולעגן זאת בחוק הבינה המלאכותית.[167]

ההשראה שאנו שואבים מן השיח האירופי נוגעת בעיקר לשיקולים שיש להתחשב בהם בשלב המתרחש טרם הטמעת הטכנולוגיה.

3. חוק הבינה המלאכותית שאושר באיחוד האירופי

מקור ההשראה השלישי הוא חוק הבינה המלאכותית שעבר לאחרונה באיחוד האירופי, המבוסס על רגולציה המותאמת לרמת הסיכון של מוצרים טכנולוגיים מבוססי בינה מלאכותית. מערכות שעלולות לפגוע באוטונומיה של הפרט או בזכויות בסיסיות אחרות, נמצאות ברף סיכון גבוה יותר לעומת כאלה שאינן משפיעות על זכויות אדם או על מעמדם המשפטי של אזרחים, ולכן התביעות הרגולטוריות ממפעיליהן – רחבות. החוק מבחין בין שני סוגים עיקריים של מערכות בינה מלאכותית בסיכון גבוה: מערכות שמשמשות רכיב בטיחות במוצר;

165 Centre for Data Ethics and Innovation, Facial Recognition Technologies, Snapshot Series, May 2020

166 שם.

167 EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk – Amnesty International

ומערכות שלפעולתן יש השלכות על זכויות יסוד מתוך רשימה מפורשת,[168] אם אלו מסכנות באופן ממשי את בריאותם, את בטיחותם או את זכויותיהם הבסיסיות של אנשים.[169]

רשימה זו מפורטת בתוספת השלישית לחוק, וכוללת כעשרים קטגוריות של מערכות בינה מלאכותית, כגון: מערכות זיהוי ביומטריות; מערכות שנועדו לבקרה ולבטיחות בתשתיות קריטיות; מערכות שמשמשות לקבלת מועמדים ללימודים או למתן ציונים; מערכות שמשמשות לגיוס עובדים ולהערכתם; מערכות דירוג אשראי; מערכות לקביעת זכאות לקבלת שירותים ציבוריים או לקבלת זכויות סוציאליות; מערכות לקביעת סדרי עדיפות בטיפול של שירותי חירום והצלה ציבוריים (טריאז'); מערכות בשימוש רשויות אכיפת החוק, ובהן מערכות לזיהוי דיפ־פייק, להערכת מצב נפשי, להערכת סיכון, לחיזוי מועדות לביצוע עבירות על בסיס פרופילים, לחיזוי פשיעה על בסיס פרופילים ולאנליטיקה קרימינולוגית; מערכות בשירות רשויות ההגירה והגבולות; מערכות בשירות מערכת המשפט, שנועדו לסייע במחקר, בפירוש עובדות וחוקים וביישום החוק במערך נסיבות מוגדר. אפשר להוסיף על כל אלו מערכות בינה מלאכותית המוגדרות בסיכון גבוה ובתנאי שרמת הסיכון הנשקפת מהן שקולה לזו של המערכות ברשימה או גבוהה מהן.

נוסח החוק מושתת על הדגם האירופי לבטיחות מוצרים והוא מטיל על המערכות הללו חובות בעניין נתונים, משילות נתונים (data governance; כלומר היכולת לדעת איזה מידע נמצא ברשותך ולשלוט בניהולו), תיעוד, יידוע, בקרה אנושית, חוסן ודיוק. עמידה בחובות אלו – מהן מהותיות ומהן מנהליות – נבחנת במסגרת בחינת תאימות (conformity assessment),[170] שמשמשת תנאי לשחרורן של מערכות אלו לשוק האירופי. אחרי שמערכות אלו משוחררות לשוק הן נתונות

168 ס' 6 להצעת חוק הבינה המלאכותית האירופי.

169 **שם**, ס' 6(2) להצעה המתוקנת. הנציבות תפרסם קווים מנחים המגדירים את הנסיבות שבהן פלט של מערכות בינה מלאכותית עלול להיות איום מסוג זה בתוך שישה חודשים מיום כניסת החוק לתוקף.

170 **שם**, ס' 49, e16, 19.

לפיקוחן של רשויות פיקוח לאומיות (market surveillance authorities), שתפקידן לבחון אם המערכות הללו עדיין פועלות בהתאם לחוק.[171]

לאורך כל מחזור החיים של מערכות בינה מלאכותית בסיכון גבוה יש להפעיל מערכת לניהול סיכונים. מערכת זו נועדה לזהות, לנתח ולהעריך סיכונים צפויים, ונוסף על כך לבחון מתווים צפויים של שימוש לרעה, להעריך סיכונים על בסיס נתונים ממערכות ניטור אחרות (post market),[172] ולאמץ אמצעים נאותים לניהול סיכונים בהתאם להוראות החוק.[173] בדיקות של מערכות בינה מלאכותית בסיכון גבוה ייערכו לפני הפצתן בשוק.[174]

החקיקה האירופית מדגישה במידה רבה את נושאי התיעוד ומשילות המידע והנתונים מתוך הבנה שמשילות נתונים אפקטיבית הכרחית לשמירה על איכות גבוהה של מידע, שהיא עצמה תנאי הכרחי לתפקודן של מערכות בינה מלאכותית.[175] יש להבטיח שנתוני אימון, תיקוף (validation) ובדיקה יהיו כפופים לפרקטיקות מתאימות של משילות נתונים, המביאות בחשבון היבטים מסוימים של עיצוב המערכת, איסוף מידע, פעולות הכנה של הנתונים, פערים בנתונים ואפשרות להטיות.[176] בסיסי נתונים בשימוש מערכות בינה מלאכותית יביאו בחשבון היבטים מיוחדים הנוגעים לאופן פעולתן של מערכות בינה מלאכותית בסיכון גבוה.[177]

יש להקפיד על תיעוד טכני של מערכות בינה מלאכותית בסיכון גבוה. על מלאכת התיעוד להתחיל בטרם שימושן בשוק, והתיעוד צריך להישאר מעודכן

171 **שם**, ס' 62–65.

172 **שם**, ס' 61.

173 **שם**, ס' 9(2).

174 **שם**, ס' 9(7).

175 **שם**, פס' 44 למבוא.

176 **שם**, ס' 10(2).

177 **שם**, ס' 10(4).

גם לאחר מכן.[178] התיעוד נועד לאפשר להדגים כי המערכת פועלת בהתאם להוראות החוק.[179] נוסף על התיעוד הטכני נדרשות המערכות לתעד גם את פעולתן השוטפת (log) לצורכי נעקבות.[180]

על מערכות בינה מלאכותית בסיכון גבוה חלה גם חובת שקיפות. יש לאפיין ולפתח מערכות שיהיו שקופות די הצורך כדי לאפשר למשתמשים בהן לפרש את הפלט שלהן ולהשתמש בו כראוי.[181] מנגנוני השקיפות יכללו בין השאר הנחיות רלוונטיות למשתמשים,[182] שמקצתן מוגדרות בתקנות.[183]

מערכות בסיכון גבוה יפותחו באופן שיאפשר פיקוח אנושי אפקטיבי לכל אורך מחזור החיים שלהן כדי למזער סיכונים לבריאות, לבטיחות או לזכויות יסוד עקב שימוש סביר במערכות אלו (לרבות שימוש צפוי לרעה) או כדי למנוע סיכונים כאלה.[184] כך תהיה למפקח האנושי האפשרות לעמוד על יכולותיהן ועל מגבלותיהן של המערכות המפוקחות, להיות מודע לנטייה להסתמך על תוצריהן (אפילו הסתמכות מופרזת), לפרש נכונה את המידע המתקבל מהן, להחליט בנסיבות מסוימות שלא להשתמש בו וכן להתערב במהלך פעולתן או לעצור אותה.[185]

אפיון ופיתוח של מערכות בינה מלאכותית בסיכון גבוה נדרשים לפי התקנות המוצעות כדי להבטיח שמערכות אלו יעמדו ברמה נאותה של דיוק, חוסן

178 שם ס' 11(1).

179 שם, ס' 11(2).

180 שם, ס' 12.

181 שם, ס' 13(1).

182 שם, ס' 13(2).

183 שם, ס' 13(3).

184 שם, ס' 14(1).

185 שם, ס' 14(4).

(robustness) ואבטחה.[186] בין השאר נקבע שמערכות בינה מלאכותית בסיכון גבוה שלמידת המכונה שלהן נמשכת גם לאחר שיווקן יפותחו באופן שיבטיח מיתון של משובים המגבירים הטיות קיימות במערכת.[187]

מהחובות החלות על מערכות בינה מלאכותית בסיכון גבוה נגזרות החובות החלות על ספקיהן.[188] ספקי המערכות נדרשים בין השאר להקים מערכת בקרת איכות שתבטיח ציות להוראות התקנות,[189] להקפיד על התיעוד הטכני של המערכות,[190] לשמור על התיעוד המתמשך (log) של פעולתן[191] ולהבטיח שטרם הפצתן יעברו בחינת תאימות.[192]

חובה מרכזית בתקנות המוצעות היא, כאמור, בחינת התאימות, אשר יכולה להיעשות בהסתמך על בקרות פנימיות של הספק[193] או בהסתמך על הערכה של גורם ביקורת חיצוני מוסמך (notified body).[194] בחינת התאימות נועדה לבדוק את הלימתן של מערכות בינה מלאכותית בסיכון גבוה להוראות החוק, וכוללת בחינה של מערכת בקרת האיכות,[195] של התיעוד הטכני,[196] של תהליכי העיצוב והפיתוח ושל אופן ניטורן של המערכות אחרי ששוחררו לשוק. גורמי הביקורת

186 **שם**, ס' 15(1).

187 **שם**, ס' 15(3).

188 **שם**, ס' 16–25.

189 **שם**, ס' 16, 17b.

190 **שם**, ס' 16(c). ס' 50 מורה כי על תיעוד זה להיות נגיש לרשויות המוסמכות הלאומיות לתקופה של עשר שנים מיום שחרורה של מערכת בינה המלאכותית בסיכון גבוה לשוק.

191 **שם**, ס' 16(d), 20.

192 **שם**, ס' 16(e), 49.

193 **שם**, ס' 43(1)(A). ראו גם ההוראות שבתוספת VI לתקנות.

194 **שם**, ס' 43(1)(B). ראו גם ההוראות שבתוספת VII לתקנות.

195 **שם**, ס' 16(b), 17. וכן ס' 2 בתוספת VI לתקנות; ס' 3 בתוספת VII לתקנות.

196 **שם**, ס' 16(c), 18. וכן ס' 3 בתוספת VI לתקנות; ס' 4 בתוספת VII לתקנות.

החיצוניים ינפיקו תעודה שתוקפה לא יעלה על חמש שנים, המעידה על הלימת המערכת לתקנות.[197]

לאחר יציאתן של מערכות בינה מלאכותית בסיכון גבוה לשוק נדרשים ספקיהן להקים מערכת ניטור מותאמת לשלב זה ולתעד את הקמתה. המערכת תאסוף ותנתח באופן שיטתי נתונים רלוונטיים על ביצועיהן מערכות הבינה המלאכותית כדי לאפשר לספקים לאמוד את הלימתן הרציפה להוראות החוק.[198] מערכת הניטור נדרשת לדווח לרשויות הפיקוח הלאומיות על השוק על כל תקרית חריגה במערכות אלו, שעלולה להיות בגדר הפרה של דינים אירופיים שנועדו להגן על זכויות אדם.[199]

נוסח החוק האירופי מחיל חובות לא רק על ספקי מערכות בינה מלאכותית בסיכון גבוה, אלא גם על מארג הגומלין בין כלל השחקנים ("אקוסיסטם"), ובכלל זה על יבואנים, על מפיצים[200] ואף על המשתמשים במערכות אלו. יבואני מערכות בינה מלאכותית בסיכון גבוה נדרשים להבטיח שהמערכות מתועדות כראוי ועברו בחינת תאימות,[201] ואם אין הלימה ביניהן ובין הוראות החוק, עליהם להימנע מייבואן.[202] כשספק, מפיץ או צד שלישי כלשהו מוציאים לשוק מערכת בינה מלאכותית בסיכון גבוה בשמם או בחסות סימן מסחרי שלהם, או כשהם משנים את תכליתה המקורית של מערכת בינה מלאכותית שכבר קיימת בשוק, או כשהם משנים באופן מהותית את המערכת עצמה, חלות עליהם החובות החלות על ספקי בינה מלאכותית בסיכון גבוה.[203]

197 שם, ס' 44.

198 שם, ס' 61.

199 שם, ס' 62(1).

200 שם, ס' 27.

201 שם, ס' 62(1).

202 שם, ס' 62(2).

203 שם, ס' 28.

משתמשים של מערכות בינה מלאכותית בסיכון גבוה – למשל משתמשים מוסדיים המעבדים מידע אישי של רבבות לקוחות ויותר – נדרשים בין השאר להשתמש במערכות אלו בהתאם לתיעוד ולהנחיות, כדי להבטיח שהמידע שמוזן במערכות הללו רלוונטי לתכלית שהן מיועדות לה; לתעד ולנטר את פעילותן; ולדווח לספק או למפיץ כשמתעורר חשש לסכנה של ממש.[204]

לענייננו, החוק האירופי מציע מערכת של "משילות טכנולוגית", הכוללת בעיקר ניהול סיכונים, תיעוד ושקיפות של מערכות שנתפסות כמערכות בסיכון גבוה. ההשראה שניתן ללמוד ממנה נוגעת הן לצורך לזהות ולאתר טכנולוגיות הנתפסות ככאלה שמייצגות סיכון, והן לדרך שבה ניתן לצמצם את הסיכון שהן טומנות בחובן, כך שאפשר יהיה ליהנות מיתרונותיהן ומן הקדמה שהן מביאות עימן.

204 **שם**, ס' 29.

פרק 5

מודל מוצע לפיקוח על רכש והטמעה של טכנולוגיות חדשות: הצעה למהלך ביצועי

בפרק זה נפרט את דרך היישום של המודל המוצע לפיקוח על רכש והטמעה של טכנולוגיות חדשות. כאמור בפרק הקודם, המודל מחולק לשלושה שלבים הנוגעים לתהליך הכנסת טכנולוגיה חדשה לשימוש: שלב הרכש, שלב ההכנסה ליישום ושלב פוסט־היישום. בכל אחד מן השלבים שיקולים שונים וצורך במעורבות של גורמים אחרים ושל תפוקות מסוגים אחרים. המשותף לכולם, כפי שנכתב לעיל, הוא הצורך במודעות וביצירת מסגרת תפיסתית להבנת העומק של הטכנולוגיה, וכן הצורך בתיעוד ובשקיפות. המודל המוצע מנסה לקשור בין הצרכים לבין תהליכים ובעלי עניין שצריכים להיות מעורבים בכל שלב.

תרשים 3
המודל המוצע

א. פיקוח בזמן הליך הרכש של הטכנולוגיה

1. מילוי "שאלון סיכון ושיבוש"

תכלית שאלון זה היא לסייע לגורמי המקצוע לבחון את הסיכון לגרימת שיבוש בעקבות יישום הטכנולוגיה. השאלון יתייחס בשאלותיו לנושאים האלה:

(**א**) **השינוי או החידוש שהטכנולוגיה מציעה:** האם הטכנולוגיה מעניקה לרשות המבקשת לרכוש אותה יכולת ביצועית שלא הייתה בידיה עד כה?

(**ב**) **שינוי זהותו או מעמדו של מקבל ההחלטות:** האם הטכנולוגיה משפיעה על מי שבידיו היה עד כה שיקול הדעת לביצוע משימות במרחב שבו מדובר? כלומר, גם אם מדובר בטכנולוגיה שאינה מחליפה את שיקול הדעת אלא רק ממליצה, הגורם המנהל את הליכי הרכש יצטרך לציין באילו רכיבים של שיקול הדעת מדובר.[205]

(**ג**) **השפעה חוקתית:** האם יש בכוחה של הטכנולוגיה להשפיע על זכויות אדם, ואם כן – באילו זכויות מדובר, מהי עוצמת הפגיעה הצפויה וכיצד היא משתנה בהשוואה למצב שהיה קודם לכן?

(**ד**) **שינוי ברמת השקיפות וההסברתיות של ההחלטה:**

(1) האם מדובר בטכנולוגיה שמאפשרת לספק הסבר לגבי החלטותיה או לתקף סטטיסטית את הפלט שהיא מפיקה?

(2) האם ניתן לספק הסבר לציבור או מסמך אחר המהווה תיקוף כלפיו או להגישו כתצהיר בפני ערכאה שיפוטית?

205 לעניין סמכויות ראו בג"ץ 2303/90 **פיליפוביץ נ' רשם החברות**, פ"ד מו(1) 410, 420 (1992). עם זאת, אנחנו לא עוסקים פה רק בשאלות הקשורות לסמכות בחוק להאצלה או להסתייעות ובהשלכות של שימוש של בינה מלאכותית כסוג של הפרטה – אלא גם בהקשר של טכנולוגיה משבשת חברתית בריחוק שנוצר בין המפעיל לבין ההחלטות שהוא מקבל ובחפיסה של הציבור את ההחלטה כשלו. לעניין זה ראו Alon Harel & Gadi Perl, *Can AI-Based Decisions be Genuinely Public? On the Limits of Using AI-Algorithms in Public Institutions*, Jus Cogens (2024) 1–18

(3) האם מדובר בהחלטה שאין חובה לקיימה? האם ניתן להבין מדוע התקבלה ובהתאם אף להשיג עליה במקרה הצורך?

(ה) זיהוי השפעה חברתית:

(1) מיהן האוכלוסיות שצפויות להיות מושפעות מן השימוש בטכנולוגיה?

(2) האם יש אוכלוסיות שיהיו חשופות יותר לפעילות התוכנה מאחרות – ואם כן, האם מדובר באוכלוסיות מוגנות?

(3) האם מדובר בסוגיות של רווחה או של אכיפה פלילית, או בסוגיות דומות שבעבר עלו בהקשר של מעמדות חברתיים וכלכליים?

(ו) איתור ניסיון קודם בשימוש בטכנולוגיה ולקחים ממנו:

(1) האם יש מידע המתעד שימוש בפועל בטכנולוגיה על ידי גורם שלטוני אחר בישראל או במדינה דמוקרטית אחרת?

(2) האם נוצר קשר עם מומחי תוכן או עם קבוצות בינלאומיות של רגולטורים כדי לבחון אם פעילות מהסוג המדובר מוכרת להם, ואם כן – מה ניסיונם בנושא?

מילוי שאלון זה ייעשה על ידי היחידה המבקשת לרכוש את הטכנולוגיה יחד עם יחידת הרכש של הרשות המבקשת זאת. אל השאלון תצורף סקירת ספרות מחקרית טכנולוגית על אודות הטכנולוגיה או טכנולוגיות דומות לה ועל השפעתן.

השאלון יועבר אל אנשי הייעוץ המשפטי של הרשות אשר יקבעו אם קיים חשש המחייב את מימוש היחידה השנייה של הבדיקה – כינוס פורום השפעות. עותק של השאלון יועבר לגוף שייקבע במשרד המשפטים (למשל, לממונה על תחום הפרטיות והמידע אצל היועץ המשפטי לממשלה), כדי שגוף זה יוכל לבצע מעקב, גם אם בדיעבד, אם אין מדובר ברכש של טכנולוגיה משבשת.

חשוב להגדיר לוחות זמנים קשיחים וקצרים למענה על השאלון או לפעולות בירור אחרות. לצד הצורך בהליך בדיקה מקדמי שעניינו הפחתת סיכון וטיפולו, יש למנוע מצב שבו סרבול בירוקרטי, בעקבות עירוב יחידות ייעוץ משפטי אחרות או היגררות תהליכים יגרום לאי־עשייה או יפגע ביכולתם של משרדי הממשלה להצטייד בטכנולוגיות חדשות.

2. כינוס "פורום הערכת השפעות"

אם בעקבות מילוי השאלון יתעורר חשש שמדובר בטכנולוגיה משבשת או מסוכנת, יידרש הגורם המבצע את הרכש לכנס פורום הערכת השפעות. פורום זה יכלול מומחי תוכן חיצוניים בתחום הטכנולוגי הספציפי ומומחי משפט מתוך הרשות מבצעת הרכש, וכן ממשרד המשפטים; רשויות רגולטוריות רלוונטיות ככל שישנן; הרשות להגנת הפרטיות; רשות החדשנות; מערך הסייבר; ובמידת הרלוונטיות – גם רשות המאגר הביומטרי הלאומי. גופים אלה מחזיקים בידיהם הן ידע מקצועי ספציפי ויכולת להאיר סוגיות שייעוץ משפטי כללי או ייעוץ מקצועי כללי אינם מכירים לפרטים, והן ניסיון מעשי בהפעלת מקרים דומים בעבר. לפיכך גם אם מדובר בגוף מרובה משתתפים שכינוסו עלול להיות מסורבל, השתתפותם של גופים אלה עשויה לייעל את התהליך בטווח הארוך. הגופים יידרשו להתייצב לפורום ולספק תשובות במסגרת סד זמנים קצוב, במטרה שלא לעכב את הרכש מחד גיסא ולאפשר מתן מענה מקצועי מאידך גיסא.

בפני הפורום יוצגו השאלון המלא וכן מסמך מפורט על אודות יכולות הטכנולוגיה והדרך שבה מתכוונים להשתמש בה. חוות דעתה של הוועדה תובא בפני הגורם מבצע הרכש באותו שלב – ועדת המכרזים או בפני ועדת הרכש או בפני היועץ המשפטי של הרשות אם מדובר ברכש ללא ועדה. בפני הוועדה יוצגו תקנים בינלאומיים מקובלים הקשורים לתוכנה, כגון תקני NIST, CENCELEC ו־ISO.[206] בהיעדרם, תהיה התייחסות מפורשת למאפיין החדשני של התוכנה ולהיעדר מדדים חיצוניים קיימים לאיכות פעולתה.[207] כל אחד מחברי הפורום יהיה חופשי לדווח למשרד שאותו מייצג על אודות המידע שהתקבל בעת ההתכנסות.

206 לעניין מעמדה של התקינה, ראו כהנא ושורץ אלטשולר, **אדם, מכונה, מדינה (לעיל** ה"ש 87), עמ' 286. NIST, למשל, נמצאים בהליך בחינה של תקנים אלו. להתרשמות, ראו **אתר מכון התקנים האמריקני**.

207 לדוגמה בנושא ניסיונות תקינה של בינה מלאכותית ראו מסמכי ISO: ISO/IEC 23894:2023 Information Technology – Artificial Intelligence – Guidance on Risk Management; ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)

נבהיר כי אין כוונתנו להפקיע מידי מנהל הליך הרכש ברשות את הסמכות שנתונה לו בנוגע לרכישת מוצרים טכנולוגיים, ואין זה נכון בעינינו לאפשר לגוף חיצוני לרשות, גם אם מתוך הממשלה, שאינו נושא באחריות לפעילות ולא יישא בהכרח בהשלכות של אי־השימוש בתוכנה או שימוש שגוי בה, להתערב בהחלטה הסופית. ואולם, אנו סבורים כי ככל שיעלו הערות לגבי סיכונים פוטנציאליים או מגבלות של הטכנולוגיה הנדונה, הם ישמשו בסיס להליך ניהול סיכונים שתערוך הרשות בכתב.

נוסף על כך תחויב הרשות להתייחס להערות שיימסרו במהלך הדיון בפורום, ואם תחליט שלא לקבלן תצטרך לנמק זאת בכתב. כמו כן, תהיה חובה על הרשות מבצעת הרכש לנסח נהלים שיהיו חלק מתיק המכרז או להסביר כיצד נהלים והוראות הפעלה שהיא קובעת מתמודדים עם ההערות שעלו בשלבים הקודמים. הנהלים וההוראות יהיו חלק בלתי נפרד ממסמכי הרכישה של הטכנולוגיה וייקבעו לפי העניין כתנאים להפעלתה על ידי הרשות.

ב. פיקוח טרם יישום הטכנולוגיה

שלב זה יתבצע לאחר הליך הרכש, טרם כניסת הטכנולוגיה לשימוש רחב ביחידות היעד שלה. מדובר בהליך מבוקר שיכול להתבצע במסגרת פיילוט או במסגרת תקופת יישום ראשונית קצובה בזמן, בהתאם לנסיבות הטכנולוגיה ולמורכבות כניסתה לשימוש. מטרת שלב זה היא לבחון אם בהפעלה מדגמית מתבררות השלכות משבשות, תקלות או טעויות, בין בעקבות יכולות הטכנולוגיה כשלעצמה ובין בעקבות שרשרת הפעלתה בידי הרשות.

הבדיקה תכלול את הרכיבים האלה:

(א) התאמת הנהלים

(1) האם הנהלים שנכתבו בשלב הקודם מתאימים גם ליישום הטכנולוגיה?

(2) האם הנהלים הופצו בקרב המשתמשים והם זמינים לבדיקה?

(3) במקרה שהתגלו פערים, האם הנהלים אכן תוקפו או הותאמו?

בפרשת פגסוס עלה פער ניכר בין הצורך בנהלים, לבין כתיבתם בפועל, כך שאלה התעכבו לאורך זמן, גם אחרי שהמערכת התחילה להפיק תוצרים שהוטמעו בתיקי חקירה. חלק מהתקלות ביישום המערכת מנומק בפער זה. לכן יש לוודא כי הטמעת הטכנולוגיה מתבצעת מתוקף נהלים ברורים, וכי היחסים האלה פועלים בצורה טובה.

(ב) התאמה בין הציפייה לבין הביצוע

(1) האם הטכנולוגיה מתפקדת בהתאם לציפיות של גורמי הרכש?

(2) האם הטכנולוגיה עומדת בהסכמות שהתקבלו בין גוף הרכש לבין מי שמכר את המוצר?

(3) האם הטכנולוגיה מבצעת את המשימות בהתאם לקריטריונים שנקבעו בתהליך הרכש?

(4) האם יש תקלות, ואם כן – האם הן מתועדות? מה בוצע לצורך תיקון התקלות?

(ג) איכות התוצרים

(1) האם התוצרים עומדים בדרישות המשפטיות שנקבעו כבר בשלבים הקודמים?

(2) האם התוצרים נבחנו בערכאה מנהלית או משפטית, ואם כן – מה הייתה המסקנה?

(3) האם עלו פערים בנוגע לתוצרים, ואם כן – כיצד טופלו?

(ד) בניית מעטפת ארגונית בד בבד עם תחילת ההטמעה:

(1) האם יש שירות תיקוני תקלות ובאילו לוחות זמנים והאם נקבע הסכם תחזוקה?

(2) האם נתוני המערכת נשמרים בהתאם להנחיות שנקבעו בשלב הרכש, או בהתאם להוראות חוק אחרות – כגון אבטחת מידע, גיבוי ושמירה בשרתים?

(3) האם הוכשרו האנשים שאמורים להשתמש בטכנולוגיה והאם הם מודעים למגבלותיה?

(4) כיצד המעטפת הארגונית והמנהלית מתפקדת: האם התקלות מטופלות במהירות וביעילות, מהם הפערים וכיצד הם מטופלים?

מניסיון העבר, הצלחתה של מערכת טכנולוגית תלויה גם ביכולת לתחזק אותה. טכנולוגיה שאינה מתוחזקת, או שאופן הפעלתה אינו תואם את יכולותיה, כגון היעדר היכרות מספקת של משתמש הקצה עם מגבלות התוכנה, עלולה להביא לתפקוד כושל של הטכנולוגיה בעת מבחן.

תוצאות הבדיקה יועברו לצוות הבין־משרדי, במטרה לבחון באופן רוחבי את השלכות הטכנולוגיה על סוגיות הדורשות ראייה מערכתית, כגון השפעה על זכויות אדם ועל מערכת הכוחות בין המדינה לבין הציבור. הצוות יידרש לעדכן את הערכת הסיכונים שביצע בשלב המקדמי, ולבחון אם בהפעלת התוכנה התגלו סיכונים חדשים. הוא יצטרך להעניק פתרונות לסיכונים שאותם הוא מעלה, ולתעד את התהליך שבמסגרתו הוסכם כי הסיכונים שנלקחו מקובלים על המערכת המדינתית. קביעותיו והערותיו של הצוות יהיו חלק מתיק הרכש, ויעברו למנכ״ל המשרד לידיעתו.

מאחר שבשלב זה הסתיים הליך הרכש, והאחריות לשימוש בטכנולוגיה עברה מגורמי הרכש ליחידה הרוכשת, יש לוודא כי היחידה בתוך הרשות המשתמשת במוצר קיבלה את כל המידע המלווה את ההטמעה ועברה הכשרה מתאימה. לאור זאת, חתימתו של המנכ״ל תידרש לצורך מעבר לשלבי ההמשך, כדי לקשור בין מידע והבנה לבין אחריות.

ג. פיקוח לאחר כניסת הטכנולוגיה לשימוש

נקודת הבדיקה השלישית תתרחש בחלוף כשנה מאז הטמעת הטכנולוגיה (post deployment), או במועד אחר שייקבע בשלב השני. מטרת הבדיקה בשלב זה היא לוודא שהציפיות מהמערכת הטכנולוגית מתממשות, הן ברמת יכולותיה הן ברמת תהליך הפעלתה. מדובר בשלב של בקרה שלא חלו תקלות מהותיות במהלך ההטמעה. בנקודת בחינה זו, כבר מצופה מגורמי המקצוע להכיר את הטכנולוגיה ואת דרך פעולתה, ולכן יוכלו בקלות יחסית לוודא כי היא אכן עומדת בסטנדרטים שנקבעו מראש.

שלב זה הוא מורכב ומובנה פחות מהאחרים, מפני שבמהותו הוא עוסק בנעלם העומד במוקד העיסוק של מחקרי בינה מלאכותית: הקושי לשמור על איכות הפעולה של בינה מלאכותית לאורך זמן, ובכלל זה עדכון התוכנה, וידוא יחס בין הפעולה לבין התוצר (alignment)[208] ובקרת איכות.

חשיבות השלב השלישי טמונה בזיהוי תקלות והשלכות שנוצרו במהלך פעילותה של המערכת. ייתכן שהמערכת לא תשבש סדרים כל עוד היא מופעלת בהתאם לכללים, אך תסב נזקים של ממש אם אין הקפדה על הפעלתה בתוך המסגרת שנקבעה לה. כך למשל, תוכנה ממליצה שהלכה למעשה הופכת לתוכנה מחליטה, או מקרים שמתגלה בהם כי מפעילי המערכת משתמשים בה מחוץ ליישומים שהגדיר היצרן.

בשלב השלישי יש להטמיע הליך של בדיקה עיתית של התוכנה כדי שגורמי הבקרה יוודאו שהיא פועלת במסגרת המדדים שנקבעו במהלך הרכש, וכי השימוש בה נעשה בהתאם להמלצות הגורמים המשפטיים או גורמים רגולטוריים אחרים. ואולם, בשלב זה, הדבר כבר לא יהיה במסגרת הליך ההטמעה, אלא חלק מהליך הבקרה השוטף על פעילות הרשות השלטונית.

בשלב זה יש לוודא כי אכן נשמר מידע המתעד את פעולת המערכת, את התקלות שאירעו לאורך זמן הפעלתה וכן את הפעלת התוכנה על ידי המשרד. מידע זה חיוני לשם תחקור פעולת המערכת בדיעבד ולביצוע מחקרים מתקנים בהתאם לצורך. בפרשת פגסוס עלה היעדר קיומו של תיעוד על אודות הפעלת התוכנה כגורם שהשפיע לרעה על יכולתו של משרד המשפטים לתחקר את פעולתה, ובהתאם גם לאתר תקלות נקודתיות.

208 ראו כהנא ושוורץ אלטשולר, **אדם, מכונה, מדינה** (**לעיל** ה"ש 87).

ד. יתרונותיו וחסרונותיו של המודל

מטרתו העיקרית של המודל התלת־שלבי היא לוודא שהטכנולוגיה שהוכנסה לשימוש במסגרת רשות שלטונית, תמלא את ייעודה ולא תוביל לתוצאות לא רצויות. הצפת הסכנות באמצעות המודל תאפשר תממש מטרה זו, בין שבאמצעות הימנעות מרכש ובין שבאמצעות קביעת נהלים, בקרות והתאמות שיאפשרו את מזעור הסיכונים באופן יעיל. המודל מבקש לכפות על המערכות השלטוניות תהליך מובנה, כדי להוות משקל נגד לנטייה שעליה מלמדים מקרי הבוחן וניסיון החיים: לחרוג מן הכללים בכל הקשור לחדשנות ולרכישת טכנולוגיות, לשכוח מושכלות יסוד ולנהל תהליכי רכש ללא בקרה סדורה וחשיבה מתודולוגית.[209]

חובות ההיוועצות שהן חלק מן המודל יסייעו להידוק הקשר בין יחידות וגופי ממשל שהיעדר התקשורת ביניהם, כפי שראינו למשל בפרשת פגסוס, יצר שרשרת של כשלים. כך למשל, מצוין בדוח מררי כי הייעוץ המשפטי לממשלה לא היה מודע כלל להליך כניסת המערכת לשימוש,[210] ואילו היה מודע ייתכן שהיה משנה את הייעוץ המשפטי שניתן באותה העת.[211] הדוח גם מציין את קיומם של פערים בין הייעוץ המשפטי המשטרתי לבין מפעילי המערכת בתוך המשטרה.[212]

הליך הבדיקה התלת־שלבי שבמודל מותאם למערכות טכנולוגיות חדשות הדורשות בקרה גם לאחר יישומן, כגון מערכות מבוססות למידת מכונה. הוא מונע את תופעת ה"שגר ושכח" של רכש טכנולוגי ומבטיח תיקוף של הפעלתו.

209 ראו דוח מררי (**לעיל** ה"ש 50) וההערות לעניין התנהלות מערכת הביטחון אגב הסתמכות יתר על טכנולוגיה ללא בקרות, ללא הבנת מגבלות הטכנולוגיה וללא יישום לקחי עבר.

210 **שם**, עמ' 57.

211 **שם**, עמ' 58 וההמלצות שלאחר מכן.

212 **שם**, עמ' 63.

המודל מציע גם מסגרת תיעוד להליך הרכש, שיאפשר להתחקות לאחור על ההליך במקרה של תקלות, כדי שאפשר יהיה ללמוד ולמנוע טעויות דומות בעתיד. כפי שניתן היה לראות במקרי הבוחן, היעדר תיעוד ראוי מנע למידה מטעויות. יתרה מכך, כדי לתחקר בדיעבד את הכשלים היה צורך בבזבוז זמן שיפוטי או בהקמת ועדות בכירים שעלותן גבוהה, וגם הן נאלצו להסתמך על עדויות ועל זיכרון ולא על מידע מתועד ומסודר.

אנו סבורים כי מחויבות כלפי יישום המודל תוביל בטווח הארוך להרחבת הידע והאוריינות הטכנולוגית בקרב רשויות השלטון ובעיקר בקרב גורמי הרכש הממשלתיים. עניין זה כשלעצמו יוביל לצמצום טעויות עתידיות.

לתפיסתנו, פעולה בהתאם למודל תסייע לגשר על פערי המינוח הקיימים בין גורמים שונים הקשורים לרכש הטכנולוגי[213] הפנים־מדינתי, בעיקר בין הייעוץ המשפטי, גורמי הטכנולוגיה ואנשי הרכש. כמו כן היא תאפשר לגשר בצורה טובה יותר על פערי השיח בין גורמי המדינה לבין חברות פרטיות שמהן נרכשים מוצרים ותסייע לתאם ציפיות בין הגורמים. אכן, פערי אוריינות ומידע קיימים בכל הליך רכש טכנולוגי,[214] וכניסתה של טכנולוגיה משבשת עלולה להרחיב את פער האוריינות עוד יותר. חלק מן המעורבים בהליכי רכש טכנולוגי אינם בעלי אוריינות טכנולוגית מספקת, אינם מבינים כיצד מוצר טכנולוגי מבצע את

213 על אוריינות טכנולוגית, ובייחוד הערת דוח מררי בעניין זה, כגון הערות על היעדר הבנה, ראו **שם**, עמ' 41.

214 **שם**, ובייחוד הערת הצוות בעמ' 67:

> צורך באוריינות טכנולוגית: מחלקת ייעוץ וחקיקה במשרד המשפטים עוסקת באופן יומיומי בסוגיות טכנולוגיות. הצוות סבור כי נדרשת העמקה של הידע המשפטי הטכנולוגי בדבר מגמות והתפתחויות טכנולוגיות בעולם, בין היתר, בנוגע לאיסוף, שימוש ועיבוד מידע פרטי על אודות אדם על ידי גופי האכיפה. העמקה כאמור תאפשר לטייב את היכולת לאתר ולטפל בסוגיות משפטיות המתעוררות, תוך התייחסות מראש להתפתחויות צפויות, באופן שיצמצם ככל האפשר את הפער בין ההסדרה בדין לבין המציאות הטכנולוגית הקיימת באותה עת, כמו גם לזהות ולנתח מגמות ולהמליץ על תיקוני חקיקה בהתאם, במיוחד לאור מהירות התפתחות הטכנולוגיה מול קצב התקדמות החקיקה.

משימותיו, ולפיכך אינם יודעים לעמוד על בעיות פוטנציאליות שעלות להיגרם במהלך הפעלתו.

לצד יתרונות המודל יש לתת את הדעת גם לחסרונות פוטנציאליים ולוודא כי נעשה ניסיון להתמודד איתם. החשש העיקרי הוא מפני סרבול בירוקרטי, שעלול להיווצר בעקבות הדרישות לבדיקות בשלושה שלבים שונים ולמעורבות אישים וגופים במהלכם. מאמציה של המדינה להתחדש במהירות לטובת כלל האזרחים עלולים להיפגע בעקבות זאת. עם זאת, אנו סבורים כי חשש זה מובנה בכל הליך בקרה. בהנחה שתג המחיר הפוטנציאלי הוא עצירה בדיעבד של שימוש בטכנולוגיה שנרכשה בממון רב, מדובר בגידור סיכונים שיש בו תועלת ממשית. כך למשל, בפרשיית פגסוס, הובילו הפרסומים להוראה לעצור את השימוש ברוגלה, ובעקבות זאת טענו גורמי אכיפה כי הם מתקשים לתת מענה לאיומים, עובדה המובילה לפגיעה בביטחון הציבור. כמו כן, נזקים שיש להביא אותם בחשבון כוללים הן את מי שלא ידעו או שלא היו מסוגלים למצות את זכויותיהם והן את הנזקים שלא התגלו, וממילא לא תוקנו, באמצעות חשיפה עיתונאית או הליך משפטי. כל אלו מצדיקים את תג המחיר של עיכוב אפשרי בהליך קליטת התוכנה.

לשיטתנו, הקפדה על הטמעה מבוקרת ועל כתיבת כללים אומנם מאטה מעט את תהליך הכנסת המערכת, אך מביאה לתוצר סופי איכותי יותר. החשש מפני עיכוב תהליכי בעקבות הדרישה לשיתוף פעולה בין כמה גורמים תוך־משרדיים, כגון הרכש, הייעוץ המשפטי ומומחי הטכנולוגיה, קיים אך לא גבוה. הניסיון מלמד כי רשויות שלטוניות משתפות פעולה הן כדי ליצר ידע ארגוני, הן כדי לשמור על רלוונטיות מוסדית (כגון הרשות לפרטיות) והן כדי להימנע משערוריות בדיעבד (משרד המשפטים). לפיכך, מזעור הסכנה מפני פגיעה באמון הציבור, בזכויות אדם וביעילות מצדיק את ההשקעה בתהליך בקרה מוסדר.

סיכום

כוונותיהם הטובות של משרדי ממשלה פוגשות את קרקע המציאות, והליכי רכש שהחלו עם רצון של המשרדים לשפר את היכולות ולייעל את פעילות המשרד, הסתיימו, כפי שהראינו בכמה מקרי בוחן, בבלימה משפטית או בסערה ציבורית. התנהלות זו ערערה את אמון הציבור במערכות השלטון ומנעה את פריסתן של טכנולוגיות, שייתכן ולו השימוש בהן היה נעשה באופן אחר, מותאם, היו מוטמעות בהצלחה.

לשם הצלחת רכש ממשלתי – בייחוד בכל הקשור לטכנולוגיות מתקדמות וחדשניות – יש לקיים הליכים סדורים, היוועצות בין משרדים ושיתוף גורמים מומחים שיכולים להעשיר את השיח. הסיבה לכך היא שטכנולוגיות מורכבות יכולות לגרום לתוצאות לא צפויות, גם אם פעולתן תקינה, אך בעיקר אם מדובר בהפעלה לא תקינה בידי גורמים שאינם מיומנים או שאינם מבינים את השלכות פעולותיהם. המחקר וניסיון העבר מוכיחים שהדרך להימנע מכך היא באמצעות רכש מלווה בשיח מבוזר ושקוף.

במסמך זה ניסינו גם להאיר כשל מחשבתי שהביא לאי־זיהוין של הטכנולוגיות כמחדשות וכמשבשות. המסמך מציע מודל בדיקה שתכליתו לוודא כי בוצעו שלושה הליכים: (א) הליך הערכת השפעות במטרה לזהות פוטנציאל משבש של טכנולוגיה; (ב) הליך ניהול סיכונים המיועד למזער סיכונים באמצעות מגבלות ונהלים מתאימים; (ג) הליך פוסט־יישום במטרה לוודא כי המלצות שניתנו בתהליך הרכש מיושמות וכי לא מתגלות השפעות חדשות בעת השימוש, שלא נצפו מוקדם יותר.

לטעמנו, המודל המוצע יחסוך בהוצאות ציבור שנגרמות בעקבות רכש והטמעה לא נכונים של טכנולוגיות ויסייע במניעת הליכים משפטיים מורכבים. מבחינת רשויות השלטון הוא יאפשר גידור תקלות ומתן מענה כן ושקוף לציבור במקרה של תקלות. מדובר, לפיכך, בכלי חשוב לבניית אמון[215] בהטמעת טכנולוגיות חדשות.

215 Tammy Bahmanziari, J. Michael Pearson, & Leon Crosby, *Is Trust Important in Technology Adoption? A Policy Capturing Approach*, 43 J. Comput. Inf. Syst. 46–54 (2003)

כעבור כשלושים שנה מאז החלה המהפכה הטכנולוגית העצומה, יש לנסח תורות הפעלה לגבי יחסי הגומלין שלה עם רשויות השלטון. יש לעשות זאת באמצעות תהליכי רכש מובנים במטרה לצמצם פערי הבנה ולהימנע מהליכת שולל אחר הבטחות טכנולוגיות לא ראויות. הקפדה על הליכים מוכרים ודבקות בתאוריות שהוכחו כיעילות, תוך התאמתם למציאות החדשה, היא האמצעי היעיל ביותר לשמירה הן על איכות השירות הציבורי ויעילות השימוש בכספי ציבור, והן על זכויות האדם והאזרח שהם מושאי השימוש בטכנולוגיה.

ד"ר תהילה שוורץ אלטשולר היא עמיתה בכירה וראשת התוכנית "דמוקרטיה בעידן המידע" במכון הישראלי לדמוקרטיה. מומחית למשפט ומדיניות של טכנולוגיה ותקשורת, ובכלל זה פרטיות, אסדרת סייבר, רשתות חברתיות ושוק התקשורת. חברה במועצת הארכיונים העליונה ובארגוני חברה אזרחית העוסקים באתיקה עיתונאית ובזכויות דיגיטליות ובעלת טור בנושאי טכנולוגיה ורגולציה במגזין "דה מרקר".

עו"ד גדי פרל הוא תלמיד לתואר שלישי במשפטים באוניברסיטה העברית בירושלים; עמית מחקר במרכז מישאל חשין ללימודי משפט מתקדמים ומנהל המחקר של תוכנית משפטים במרכז פדרמן לחקר הסייבר באוניברסיטה.

המכון הישראלי לדמוקרטיה
www.idi.org.il

מסת"ב:
978-965-519-457-9