

מתווה להצעת חוק:

הגנה על זכויות משתמשים במרחב הדיגיטלי

ד"ר בר פרג'ון-מזרחי



מתווה להצעת חוק:

הגנה על זכויות משתמשים במרחב הדיגיטלי

ד"ר בר פרג'ון-מזרחי

מתווה להצעת חוק: הגנה על זכויות משתמשים במרחב הדיגיטלי

נייר מדיניות 3.2026
ד"ר בר פרג'ון-מזרחי

תשרי התשפ"ו | ספטמבר 2026

Protecting User Rights in the Digital Environment: A Risk-Based Legislative Framework

Dr. Bar Fargon-Mizrahi

All Rights Reserved

Copyrights © Tachlith Institute

נדפס בישראל תשרי התשפ"ו | ספטמבר 2026

כל הזכויות שמורות

© תכלית – המכון למדיניות ישראלית (ע"ר) תשפ"א-2021

תכלית – המכון למדיניות ישראלית (ע"ר)

אחד העם 35 תל אביב 6578403

טל. 03-6587445

דוא"ל. info@tachlith.org.il

אתר המכון. tachlith.org.il

עריכה לשונית: עודד רענן

עיצוב ועריכה גרפית: רויטל (ג'בקה) קלאוס

ISBN 978-965-93171-6-5

תכלית - המכון למדיניות ישראלית (ע"ר) הוא מכון מחקר מוכון מדיניות המבקש להביא לשינוי המציאות בישראל באמצעות מחקר יישומי, הכוונה וסיוע למערכי קבלת ההחלטות הפוליטיים והבירוקרטים לשם יישום מדיניות מושכלת ואפקטיבית, המחזקת את מהותה של ישראל כמדינה יהודית ודמוקרטית, ברוח מגילת העצמאות.

לצורך מימוש יעדיו, מפעיל המכון מארג של שלושה כלים, אשר שילובם מקנה ערך מוסף ייחודי בתחום המדיניות בישראל. מחקר עומק מוכון מדיניות, המתקיים בשיתוף פעולה עם אקדמאים מובילים ואנשי פרקטיקה מובילים מהארץ ומהעולם; פעילות תשתיתית שתכליתה תרגום והנגשה של המדיניות המופקת בידי המכון ישירות למקבלי ההחלטות הרלוונטיים ליישומה, וכן הטמעת מערך תמיכה היקפי המבקש לייצר שותפות שיח, על בסיס התוכן, עם מגזרים נוספים בישראל, כגון ארגוני חברה אזרחית, התקשורת, המגזר הפרטי והציבור הכללי הרחב.

ד"ר בר פרג'ון-מזרחי היא מרצה וחוקרת בתחום המשפט והטכנולוגיה. היא משמשת סגנית ראש בית הספר למשפטים במרכז האקדמי פרס, עמיתת מחקר במעבדה למשפט, מדעי המידע ואתיקה דיגיטלית ובמרכז ז'אן מונה לממשל דיגיטלי באוניברסיטת בר-אילן, וחוקרת ב"תכלית" – המכון למדיניות ישראלית.

מחקריה עוסקים בהסדרת המרחב הדיגיטלי, פרטיות והגנת מידע, זכויות משתמשים, צרכנות דיגיטלית ובינה מלאכותית, תוך התמקדות בפיתוח מודלים רגולטוריים להתמודדות עם אתגרי העידן הדיגיטלי. מחקריה משלבים בין ניתוח משפטי-נורמטיבי למחקר אמפירי, ומתמקדים בפיתוח כלים שיסייעו למשתמשים לקבל החלטות מושכלות יותר ביחס לשימוש במידע אישי ולסיכונים הכרוכים בשירותים דיגיטליים. מאמרים פרי עטה התפרסמו בכתבי עת אקדמיים בישראל ובעולם, ובהם מחקרי משפט Cardozo Villanova Law Review ו-Arts & Entertainment Law Journal.

לצד פעילותה האקדמית, ד"ר פרג'ון-מזרחי עוסקת בקידום מדיניות ציבורית ובהצעות חקיקה בתחומי הפרטיות, הממשל הדיגיטלי וזכויות משתמשים, במטרה להתאים את המסגרת הרגולטורית לאתגרים שמציבות טכנולוגיות מתקדמות ושירותים מקוונים.

חלקים מנייר מדיניות זה, אשר נכתב על ידי ד"ר בר פרג'ון-מזרחי, לקוחים ממאמרה "חוק וסדר: הצעה לאסדרה אחודה להגנה על זכויות משתמשים במרחב הדיגיטלי", אשר התפרסם בכרך לה (3) של כתב העת "מחקרי משפט" בשנת 2025.

תודות

נייר מדיניות זה הוא תוצר של תהליך מחקר, חשיבה וכתובה שנעשה בליווי ובסיוע של אנשים רבים, אשר תרומתם המקצועית הייתה משמעותית לגיבוש.

ברצוני להודות לד"ר אלעד גיל, ראש חטיבת המחקר בתכלית – המכון למדיניות ישראלית, לד"ר טל מימרן, עמית בכיר במכון תכלית, ולד"ר גלעד וינר, מנהל התוכניות הראשי בתכלית, על הליווי המקצועי לאורך העבודה, על ההערות המעמיקות, הדיונים המפרים והנכונות המתמדת להקדיש מזמנם ומניסיונם לטובת גיבוש ושיפור של נייר מדיניות זה.

תודה מיוחדת לעו"ד אריאל ענבי־כהן על הובלת תהליך העבודה ועל התכלול המקצועי של כלל שלבי הכתיבה והעריכה; לרויטל קלאוס על עיצוב המסמך; לעודד רענן על העריכה הלשונית המדויקת והקפדנית, ועל מעורבותו הרבה בתהליך גיבוש המסמך, אשר תרמה באופן משמעותי לבהירותו, לדיוקו ולאיכותו; ולאלרעי גולד על הסיוע המקצועי והמסור בעריכת ההערות והמקורות.

בעשור האחרון הפכו השירותים הדיגיטליים לתשתית חיונית המשפיעה כמעט על כל היבט בחיינו, החל בקבלת שירותים ממשלתיים, עבור למסחר, בריאות וחינוך וכלה בהשתתפות במרחב הציבורי והחברתי. לצד היתרונות הברורים שבשימוש במערכות אלו, הגידול בהיקף איסוף המידע ועיבודו יוצר מציאות שבה תהליכים טכנולוגיים מתקדמים משפיעים על זכויות הציבור ועל יחסי הכוחות בין המדינה, החברות והמשתמשים. מציאות זו מחייבת מסגרת רגולטורית עדכנית וברורה.

בתחום הגנת המידע נשענת ישראל כיום על חוק הגנת הפרטיות, שנחקק בשנת 1981 ואינו בנוי עוד להתמודד עם האופן שבו מידע נאסף, מנותח ומשמש לקבלת החלטות אוטומטיות בשירותים דיגיטליים.¹ בעקבות לחץ פנימי ובינלאומי, החל משרד המשפטים, עוד בשנת 2022, לנסות לגשר על הפערים בחקיקה באמצעות מספר הצעות לתיקון חוק הגנת הפרטיות,² ובאוגוסט 2025 נכנס לתוקפו תיקון מס' 13 לחוק.³ אולם, תיקון זה מספק מענה חלקי בלבד מפני הסיכונים בתחום הגנת מידע ומותיר את המשתמשים חשופים לניצול מידע אישי, לחוזים דרקוניים ולתנאי שימוש הפוגעים בזכויותיהם, ללא יכולת ממשית להתגונן. גם שאר ההצעות שהועלו וטרם אושרו אינן מציעות פתרונות מספקים.

ישראל הוכרה על-ידי האיחוד האירופי כמדינה שניתן להעביר מידע אישי לתחומה, על בסיס ההנחה שקיימת בה הגנה משפטית מספקת על פרטיות. אולם בפועל, האסדרה המקומית של תחום זה אינה אחידה ואינה נותנת מענה מלא לאופן שבו מידע אישי נאסף, מעובד ומנוצל במרחב הדיגיטלי. פער זה יוצר שלוש בעיות מרכזיות.

הבעיה הראשונה היא **כלכלית-מדינתית** ונובעת מכשל רגולטורי מבני: היעדר דרישות מקומיות המחייבות התאמה מוקדמת לעקרונות רגולציה בינלאומית מחייבת (ובראשם GDPR, AIA ו-DSA). כפועל יוצא, חברות טכנולוגיה בישראל מפתחות מוצרים בהתאם לסטנדרט המקומי, שאינו תואם את דרישות שווקי היעד המרכזיים. מצב זה שוחק את כושר התחרות והיצוא של המשק; יוצר תמריצים להסטת פעילות, השקעות ורישום תאגידי אל מחוץ לישראל; ומגביר חיכוך רגולטורי מול שותפות הסחר, עד כדי פגיעה במעמדה של ישראל כשותפה רגולטורית אמינה ויצירת סיכון עתידי למעמד קשרי הסחר עם האיחוד האירופי. מעבר לכך, היעדר סטנדרטים מחייבים להגנת מידע ואבטחתו מגביר את החשיפה של ישראל לדליפות ולתקיפות סייבר; מאפשר ניצול עוין של מידע אישי; מערער את אמון הציבור במוסדות המדינה; ומחליש את הריבונות הדיגיטלית והחוסן הלאומי.

1 חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות").
 2 הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022, ה"ח הממשלה 1496; תזכיר חוק הגנת הפרטיות (הגדרות וצמצום חובת הרישום), התש"ף-2020; הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח-2018, ה"ח הממשלה 1206.
 3 חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, ס"ח 1430.

הבעיה השנייה היא **חברתית**: בהיעדר חובות שקיפות על תהליכי תיוג (פרופיילינג), פלטפורמות דיגיטליות משפיעות על עיצוב התודעה הציבורית באופן שאינו מווסת. אלגוריתמים מסוגלים לזהות העדפות פוליטיות, לאמוד פרופיל רגשי ולהתאים תכנים להגברת מעורבות, גם אם הדבר מגביר את הקיטוב החברתי או מוביל לחשיפה לדיסאינפורמציה. בישראל נרשמו בשנים האחרונות מקרים שבהם קבוצות סגורות ברשתות חברתיות הפיצו מידע שגוי שהשפיע על דיון ציבורי בענייני בריאות וביטחון. במדינה בה השימוש ברשת גבוה במיוחד, היעדר הרגולציה על פרסום פוליטי מבוסס נתונים, אלגוריתמי המלצה ודיווח שקוף, עלול ליצור קיטוב ולהעמיק שסעים חברתיים-פוליטיים.

הבעיה השלישית והמרכזית ביותר היא **הפגיעה הישירה בפרט**: המשתמש הבודד הוא החוליה החלשה במערכת הדיגיטלית, ונושא בפועל במחיר כשלי האסדרה. יחסי הכוחות האיסימטריים בינו לבין תאגידי הטכנולוגיה מובילים לפגיעות שיטתיות בזכויות יסוד, לרבות פרטיות, אוטונומיה, שקיפות והליך הוגן. שירותים דיגיטליים אינם מספקים מידע ברור על היקף איסוף הנתונים על המשתמש ומטרותיו. תנאי שימוש ומדיניות פרטיות מורכבים מקשים על הבנה אמיתית והפכים את ההסכמה לפורמלית בלבד. המשתמשים חסרים כלים מעשיים לשליטה במידע שנאסף על אודותיהם ואין להם כמעט כל יכולת לערער, להגביל את השימוש בו, או לממש את זכויותיהם. התופעה נפוצה בתחומים שונים: החלטות סיכון פיננסיות לא שקופות; שימוש במידע רפואי למטרות מסחריות ללא הסכמה מודעת; הונאות מקוונות נפוצות; ועוד. נתונים מאיגוד האינטרנט הישראלי מלמדים על היקף הפגיעות ועל תחושת חוסר שליטה נרחבת בציבור הישראלי, בין היתר על רקע עלייה מתמשכת בפניות לקו הסיוע לאינטרנט בטוח, המשקפת ריבוי מקרים של הונאות, פגיעות ברשת וסיכוני סייבר.⁴

השילוב של שלוש הבעיות יחד מצביע על פער אסדרה עמוק בישראל. היעדר מסגרת חקיקה מאוחדת יוצר חוסר עקביות ברגולציה, באופן המחליש את יכולתה של המדינה לשמר את ההכרה מטעם האיחוד האירופי כמדינה המעניקה רמת הגנה נאותה למידע אישי, פוגע באיכות המרחב הציבורי ומשאיר את הפרט חשוף לפגיעה בזכויות בסיסיות.

נייר מדיניות זה מציע מתווה לחקיקה מאסדרת, המבוסס על קריטריון מאחד: הגנה על זכויות המשתמשים במרחב הדיגיטלי. המתווה יכלול עקרונות של שקיפות, הגבלת שימוש, אחריותיות וזכויות מהותיות למשתמש, ויישומו יאפשר לישראל ליישר קו עם הסטנדרטים הנהוגים במדינות מובילות ולחזק את ההגנה על הציבור בעידן הדיגיטלי.

⁴ "2024 Internet Safety Report by ISOC-IL: Significant Increase in Social Media Account Hijacking and Cyber Threats" Israel Internet Association (8.3.2025)

המתווה המוצע אינו נוסח חוק מלא, אלא מהווה תשתית מבנית להאצת קידומה של חקיקה מסגרתית ותקנות נלוות. הוא כולל שלושה רכיבים משלימים:

« עיגון זכויות משתמשים ומעטפת ההגנה עליה;

« כלי רגולטורי פרקטי מסוג גילוי נאות מבוסס סיכון;

« מערך אסדרה מתכלל בעל מומחיות וסמכויות אכיפה.

המתווה המוצע צריך להישען על שלושה עקרונות תכנוניים מרכזיים:

« **ניטרליות טכנולוגית וגמישות:** ניסוח במונחים רחבים, המתארים פעולות וסיכונים (איסוף, עיבוד, שיתוף, מעקב, פרופילינג, החלטות אוטומטיות), לצד הסמכה מפורשת לעדכון תקנות והוראות שעה בנושאים דחופים.

« **העברת מרכז הכובד מהסכמה פורמלית של המשתמש לחובות מהותיות של ספקי השירותים:** הסכמה מדעת נשמרת כמושג יסודי, אך אינה משמשת "כתב ויתור" על אחריות. לצידה, נקבעות חובות שאינן "תלויות קליק", כגון צמידות מטרה מחוזקת, שקיפות אפקטיבית, הגבלת מעקב, בקורות אבטחת מידע וניהול סיכונים.

« **איזון בין חדשנות להגנה על זכויות:** הטמעת מדרג רגולטורי מבוסס סיכון, שמצמצם הרתעה ומפחית עומס על שירותים בסיכון נמוך, תוך החמרה על שירותים בסיכון גבוה או כאלה הנוגעים בקטינים, במידע רגיש או בהחלטות אוטומטיות משמעותיות.

לב ההצעה הוא כלי גילוי נאות מבוסס סיכון, שיוצג בכל אתר ואפליקציה לצד הסכמי השימוש. הכלי הרגולטורי מורכב משלושה חלקים: (א) שאלון גילוי נאות אחיד שממלא קצין ציות של ספק השירות; (ב) מדד כמותי להגנת מידע אודות המשתמשים, המופק על-ידי גורם בלתי-תלוי מטעם הרשות האמונה על אכיפת המתווה המוצע ומוצג בארבע קטגוריות קבועות; ו-(ג) מנגנון לאיתור סתירות בין ההצהרות לבין ההסכמים והמדיניות בפועל, המשמש לתיעדוף ביקורות ואכיפה. כלי זה מתמודד עם שתי בעיות יסודיות: הוא מקל על משתמשים להבין סיכונים בצורה יעילה ואחידה, והוא מייצר לרגולטור תשתית בקרה ישימה שאינה תלויה בהכרעות פרטניות אינסופיות.

המלצות היישום מציעות מסלול הטמעה מדורג:

« בשלב ראשון, קידום חוק מסגרת קצר ועקרוני והפעלת פיילוט לשאלון ולמדד בשירותים גדולים ובתחומים רגישים.

« בשלב שני, הרחבה לכלל השירותים עם התאמות לעסקים קטנים ובינוניים.

« בשלב שלישי, ייצוב המודל באמצעות תקנות מתעדכנות ומערך אסדרה ייעודי או גוף מתכלל עצמאי, בעל סמכויות פיקוח, עיצומים, צווים מתקנים ומנגנוני תרופה אזרחיים (כולל פיצוי ללא הוכחת נזק והרחבת התאמה של תובענות ייצוגיות בתחום מידע דיגיטלי).

כך נבנית מסגרת הוליסטית שמגינה על זכויות משתמשים, מייצרת ודאות לשוק ושומרת על יכולת התאמה לשינויים טכנולוגיים עתידיים.

על רקע זה, נייר המדיניות בנוי באופן מדורג – מהצגת הבעיה, דרך מיפוי הסיכונים והכשלים הקיימים ועד לגיבוש מתווה אסדרה והמלצות יישומיות. **פרק 1** מציג את הבעיה המרכזית הניצבת כיום בפני הסדרתם של שירותים דיגיטליים בישראל, תוך תיאור הרקע להתפתחויות הטכנולוגיות והרגולטוריות בארץ ובעולם, זיהוי כשל המדיניות הקיים והגדרת מטרתה של החקיקה המוצעת. **פרק 2** ממפה את הסיכונים והפגיעות הנובעים מהשימוש הגובר בשירותים דיגיטליים, ברמות שונות – מהשלכות מדיניותיות וכלכליות, דרך פגיעות במרקם החברתי והדמוקרטי, ועד לפגיעות ישירות בזכויות הפרט, בדגש על פרטיות, אוטונומיה, חופש הביטוי וזכויות צרכניות וחוזיות, לצד המחשה באמצעות נתונים ומקורות רשמיים. **פרק 3** בוחן את מסגרות ההגנה הקיימות בישראל, לרבות הרגולציה, סמכויותיהן של רשויות הפיקוח, הכשלים המבניים והמעשיים בהסדרה וניסיונות עבר להתמודד עם הבעיה. **פרק 4** מציג סקירה השוואתית של מסגרות אסדרה בעולם, הכוללת גישות עקרוניות, כלים רגולטוריים ומנגנוני פיקוח ואכיפה במדינות נבחרות, ומפיק לקחים רלוונטיים לישראל.

על בסיס ממצאים אלה, **פרק 5** מחדד את המעבר מן הסיכונים שזוהו אל הפער הרגולטורי הקיים ואת הצורך בחקיקה אחודה. בהמשך לכך, **פרק 6** מציג את המלצות המדיניות המרכזיות, ובמרכזן מתווה לאסדרה אחודה לשירותים דיגיטליים בישראל, ואילו **פרק 7** מפרט את ההמלצות האופרטיביות ליישום המתווה, לרבות שלבי הטמעה, כלים רגולטוריים ומנגנוני אכיפה. לבסוף, **פרק 8** מסכם את עיקרי הנייר, את הפתרון המוצע ואת ההשלכות הצפויות של יישומו.

מתווה להצעת חוק: הגנה על זכויות משתמשים במרחב הדיגיטלי

העברת מוקד האחריות מהמשתמש אל ספקי השירות
באמצעות רגולציה מבוססת סיכון, שקיפות ואכיפה.

עקרונות החוק



רגולציה מבוססת סיכון והיקף שימוש

מדרג חובות בהתאם לרמת
הסיכון ולהיקף השימוש בשירות



חובות מהותיות על ספקי השירות

האחריות אינה מבוססת עוד
רק על הסכמת המשתמש



חוק מסגרת אחיד

אסדרה אחידה לכלל
השירותים הדיגיטליים

כלי שקיפות והגנה



מדד הגנה על זכויות משתמשים

ציון אחיד המאפשר השוואה
בין שירותים דיגיטליים



שאלון גילוי נאות אחיד

דיווח אחיד ושקוף של ספקי
השירות בהתאם לתבנית
רגולטורית



זכויות משתמש

מחיקה, עיון, נידוד, תיקון, הסבר
אנושי והגנות מיוחדות לקטינים
ולאנשים עם מוגבלויות

פיקוח, אכיפה ותרופות



תרופות למשתמש

פיצוי ללא הוכחת נזק
ותובענות ייצוגיות



כלי אכיפה מדורגים

האחריות אינה מבוססת עוד
רק על הסכמת המשתמש



רשות ייעודית

גוף פיקוח עצמאי בעל
סמכויות פיקוח ואכיפה

19	פרק א הצגת הבעיה: פגיעות רב־שכבתיות בהיעדר אסדרה דיגיטלית
27	פרק ב סיכוני המידע בשירותים הדיגיטליים
41	פרק ג האסדרה הקיימת בישראל להתמודדות עם סיכונים בתחום שירותי המידע
51	פרק ד מגמות אסדרה בתחום שירותי המידע הדיגיטלי - מבט השוואתי
57	פרק ה סיכום ביניים: מן הסיכונים אל הפער הרגולטורי והצורך בחקיקה אחודה
61	פרק ו המלצות מדיניות: מתווה אסדרה אחודה להגנה על משתמשים בעידן הדיגיטלי
71	פרק ז המלצות אופרטיביות ליישום המתווה
77	פרק ח סוף דבר

פרק א |
הצגת הבעיה: פגיעות רב־שכבתיות
בהיעדר אסדרה דיגיטלית

השירותים הדיגיטליים הפכו בעשור האחרון לתשתית מרכזית של החיים הכלכליים, החברתיים והאזרחיים. פלטפורמות מקוונות, מערכות מבוססות מידע וכלי בינה מלאכותית משפיעים כיום על האופן שבו פרטים מתקשרים, צורכים מידע, מקבלים החלטות ומממשים זכויות. לצד תרומתם המשמעותית, שירותים אלה יוצרים גם סיכונים רחבי היקף, אשר רגולציה מדינתית מיושנת ומפוצלת בישראל מתקשה להתמודד עמם באופן אפקטיבי.

היעדר אסדרה עדכנית של המרחב הדיגיטלי אינו מוביל רק לפגיעות נקודתיות בפרטיות המשתמשים, אלא מייצר כשל מבני בעל השלכות מצטברות בשלושה רבדים מרכזיים: ברמת המדינה – באמצעות פגיעה בתחרותיות, בקשרי סחר ובחוסן הדיגיטלי; ברמת החברה והדמוקרטיה – באמצעות השפעה על השיח הציבורי, הקיטוב החברתי ואמון הציבור במדינה ובמוסדותיה; וברמת הפרט – באמצעות פגיעות מתמשכות בזכויות יסוד, ובהן הזכות לפרטיות, לאוטונומיה, לשקיפות ולהליך הוגן.

מבין שלושת הרבדים הללו, הפגיעה בזכויות המשתמשים היא הביטוי הישיר והמידי ביותר של כשלי האסדרה, והיא גם הרובד המצוי במוקד נייר מדיניות זה. יחסי הכוחות האי־סימטריים בין משתמשים לבין תאגידי טכנולוגיה, לצד הסתמכות גוברת על עיבוד מידע ומנגנונים אוטומטיים, מקשים על משתמשים להבין כיצד מידע אישי נאסף ומעובד ומצמצמים את יכולתם לממש שליטה אפקטיבית במידע שלהם ובזכויותיהם.

להלן יוצגו שלושת רבדי הפגיעה המרכזיים, המשמשים בסיס להצדקת הצורך במסגרת אסדרה ייעודית ומקיפה למרחב הדיגיטלי.

1. פגיעות ברמת המדינה

היעדר אסדרה עדכנית ומקיפה של שירותים דיגיטליים חושף את מדינת ישראל לנזקים כלכליים, מדיניים וביטחוניים. בראש ובראשונה, רגולציית פרטיות שאינה עומדת בסטנדרטים בינלאומיים עלולה לפגוע בקשרי הסחר של ישראל וביכולתה להשתלב בשווקים גלובליים ובפרויקטים חוצי-גבולות. כך, האיחוד האירופי מתנה העברת מידע אישי למדינות שלישיות בקיומה של "רמה נאותה" (Adequacy) של הגנת מידע, והיחלשות מעמדה של ישראל בהקשר זה עלולה להקשות על חברות ישראליות לפעול בשוק האירופי ולפגוע בתחרותיות המשק.⁵

European Commission, *Report from the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC*, COM (2024) 7 final (Jan. 15, 2024); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General

בהיעדר דרישות מקומיות המחייבות עמידה מראש בעקרונות מרכזיים של רגולציה בינלאומית מחייבת, ובראשם תקנות הגנת המידע של האיחוד האירופי (להלן: GDPR);⁶ חוק השירותים הדיגיטליים של האיחוד (להלן: DSA)⁷ וחוק הבינה המלאכותית שלו (להלן: AIA);⁸ חלק מחברות הטכנולוגיה הפועלות בישראל מפתחות שירותים ומוצרים בהתאם לסטנדרט רגולטורי מקומי, שאינו תואם את הדרישות של שוקי היעד המרכזיים שלהן. במצב זה, ובהיעדר תמריץ רגולטורי מוקדם להתאמה, עלויות הציות לרגולציה זרה נדחות לשלב ההתרחבות הבינלאומית, שבו הן גבוהות במיוחד ולעיתים אף חוסמות את עצם הכניסה לשוק.

מצב זה אינו נובע בהכרח ממודעות לקויה של החברות לדרישות הדין הזר, אלא מכשל תמריצים שמקורו במדיניות: בהיעדר חובה או עידוד רגולטורי להתאמה מוקדמת, לחברות יש תמריץ רציונלי לדחות השקעות בציות עד לשלב שבו הכניסה לשוק הזר נעשית קונקרטית. דחייה זו מייצרת עלויות מעבר גבוהות ופוגעת ביכולת התחרות. כך, חברות ישראליות בתחום הבריאות הדיגיטלית נדרשות לבצע בדיעבד הליכי DPIA (Data Protection Impact Assessment) מקיפים ויקרים כתנאי בסיסי להטמעת שירותיהן באירופה; חברות בתחום הפרסום המקוון נאלצות לשנות מנגנוני איסוף ושימוש במידע בשל פרקטיקות שאינן מקובלות באיחוד האירופי; וסטרטאפים בתחום הבינה המלאכותית אינם יכולים לשווק מוצרים מסוימים באיחוד, משום שהמודלים לא פותחו מלכתחילה בהתאם לדרישות השקיפות וסיווג הסיכונים הקבועות ב-AIA.

ליקויים אלו אינם פוגעים רק בחברות בודדות, אלא מתורגמים לחסמי כניסה ועיכובים בפעילות בשווקים בינלאומיים. כפועל יוצא, הם מצמצמים את כושר התחרות של המשק הישראלי בכללותו. כאשר ההתאמה לדרישות רגולטוריות נעשית רק בשלב מאוחר, היא כרוכה בעלויות גבוהות, בעיכוב חדירה לשוק ואף בווייתור על הזדמנויות עסקיות, ובכך מחלישה את היקף היצוא הדיגיטלי. בנוסף, מצב זה יוצר תמריץ להעברת פעילות, השקעות ורישום תאגידי מחוץ לישראל, למדינות שבהן קיימת ודאות רגולטורית מוקדמת והתאמה לסטנדרטים בינלאומיים כבר בשלב הפיתוח. במקביל, הוא מגביר חיכוך

1 (Data Protection Regulation), 2016 O.J. (L 119) 6
Commission Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1,17 (להלן: GDPR).
7 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (DSA) (להלן: DSA).
8 European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (AIA) (להלן: AIA) (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

רגולטורי בין ישראל לשותפות הסחר המרכזיות שלה, ועלול לפגוע במעמדה כשותפה רגולטורית אמינה ואף לסכן את המשך ההכרה בה כמדינה בעלת רמת הגנה נאותה על מידע אישי בבחינות עתידיות של האיחוד האירופי.

מעבר לכך, היעדר סטנדרטים מחייבים בתחום הגנת המידע ואבטחתו יוצר סיכונים לביטחון הלאומי ולריבונות הדיגיטלית. דליפת מידע ממאגרים רגישים, מתקפות סייבר והיעדר פיקוח אפקטיבי על עיבוד מידע אישי, עלולים לשמש גורמים עוינים לצרכים מגוונים: איסוף מודיעין; השפעה ממוקדת על עמדות והתנהגות של משתמשים, לרבות באמצעות התאמת מסרים או הפצת דיסאינפורמציה; פגיעה בתשתיות חיוניות או ניצול מידע אישי לצרכים ביטחוניים וכלכליים; וכן כדי לערער את אמון הציבור במוסדות המדינה.⁹ אירועי סייבר חמורים שאירעו בישראל בשנים האחרונות ממחישים את פגיעותן של תשתיות דיגיטליות ואת הצורך במדיניות הגנת מידע איתנה כנדבך של חוסן לאומי.¹⁰

2. פגיעות ברמת החברה והדמוקרטיה

לשירותים הדיגיטליים השפעה עמוקה על המרחב הציבורי, השיח החברתי והתפקוד הדמוקרטי. אלגוריתמים של פלטפורמות מקוונות וכלי בינה מלאכותית מעצבים את החשיפה למידע, את סדר היום הציבורי ואת האופן שבו אזרחים מגבשים עמדות.¹¹ התאמה אישית של תכנים על בסיס פרופילים דיגיטליים עלולה לצמצם חשיפה לדעות מגוונות, להעמיק קיטוב חברתי ולפגוע ביכולת לקיים שיח ציבורי פתוח.¹² מחקרים בינלאומיים מצביעים על כך שמדינות ללא אסדרה מודרנית של פעילות פלטפורמות חוות שחיקה באמון הציבור במוסדות השלטון ועלייה בהשפעתם של תכנים קיצוניים.¹³

בנוסף, השימוש במידע אישי לצורך הפצת תכנים ממוקדים, לרבות מידע כוזב ותעמולה פוליטית, יוצר סיכונים ממשיים לתהליכי קבלת החלטות דמוקרטיות. בהיעדר חובות שקיפות, אחריות ופיקוח, פלטפורמות פרטיות מחזיקות בכוח משמעותי להסיר תכנים, להשעות חשבונות או לעצב את השיח הציבורי בהתאם לאינטרסים כלכליים, לעיתים ללא

9 באוקטובר 2025 דווח באתר הרשמי של מערך הסייבר הלאומי כי זוהתה "מגמה של גל מתקפות סייבר כלפי חברות המספקות שירותי מחשוב לחברות רבות במשק. יותר מעשר חברות פרטיות במשק היו נתונות לרמה כל־שהי של מתקפה, רובן נתקפו דרך חיבורם לחברות שירותים דיגיטליים לגופים עסקיים המהוות חוליה בשרשראות האספקה". ראו: "גל מתקפות סייבר איראניות על חברות וגופים חיוניים בישראל בשבועות האחרונים" **מערך הסייבר הלאומי** (22.10.2025).

10 דו"ח של מערכת הסייבר הלאומי מצביע על עלייה של 24% באירועי סייבר בשנת 2024. ראו: מערך הסייבר הלאומי דו"ח **סיכום שנה 2024** (2025).

11 "Cambridge Analytica, LLC, In the Matter of," Cases and Proceedings, Federal Trade Commission (18.12.2019).

Katharine Kemp, *Concealed Data Practices and Competition Law: Why Privacy Matters* 12

16 EUR. COMPETITION J.628, 648-652 (2020).

13 הרשות להגנת הפרטיות דו"ח **פעילות** (2023).

הליך הוגן או הנמקה.¹⁴

מצב זה מעורר שאלות יסוד בדבר חופש הביטוי, שוויון והשתתפות אזרחית, ומדגיש את הצורך לראות במרחב הדיגיטלי מרחב אזרחי בעל חשיבות חוקתית, ולא רק זירה מסחרית. בישראל, שבה שיעור השימוש ברשתות גבוה במיוחד,¹⁵ השלכות אלו משמעותיות אף יותר. היעדר מגבלות על פרקטיקות פרסום פוליטי מבוסס נתונים, חוסר שקיפות לגבי מנגנוני המלצה והיעדר חובות דיווח, מפחיתים את היכולת לנהל מרחב ציבורי הוגן ושוויוני.

3. פגיעות ברמת הפרט – זכויות משתמשים (מוקד נייר המדיניות)

על אף חשיבותן של הפגיעות ברמת המדינה והחברה, עיקר הבעיה מצוי ברמת הפרט. יחסי הכוחות האסימטריים בין משתמשים לבין תאגידי טכנולוגיה, הפועלים על בסיס מודלים כלכליים מבוססי מידע, מובילים לפגיעות שיטתיות בזכויות יסוד, ובראשן הזכות לפרטיות, לאוטונומיה, לשקיפות ולהליך הוגן.¹⁶ לפיכך, המשתמש הבודד הוא הגורם החלש ביותר במערכת היחסים הזו, והוא נושא בפועל במחירם של כשלי האסדרה.

פגיעות אלה אינן תיאורטיות, אלא מהוות חלק אינהרנטי מהשימוש היומיומי בשירותים דיגיטליים. רבים מהם אינם מספקים כיום מידע ברור על היקף איסוף הנתונים שהם מבצעים, על מטרות עיבוד המידע או על השימוש המשני שנעשה בו. המשתמשים מתבקשים לאשר תנאי שימוש ומדיניות פרטיות ארוכים ומורכבים, שקשה להבין מהם כיצד מידע אישי על אודות המשתמשים נאסף ומעובד בפועל. כתוצאה מכך, מרבית המשתמשים אינם מבינים מה קורה לנתונים שלהם, ולרובם חסרים הכלים המעשיים לממש שליטה אמיתית במידע, כולל היכולת לערער, להגביל שימוש או לממש את זכויותיהם באופן אפקטיבי.¹⁷ במציאות זו, ההסכמה הופכת לעיתים לפורמלית בלבד, והגנות משפטיות קיימות אינן מצליחות לאזן את פערי הכוחות בפועל.¹⁸

¹⁴ Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WIS L. REV 861, 882 (2014).

¹⁵ "תדירות השימוש באינטרנט בישראל ומדינות העולם בשנת 2025: נתונים וניתוח השוואתי" **איגוד האינטרנט הישראלי** (3.1.2026).

¹⁶ Sofia Graffanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INT'L. PROP. MED. ENT. L. J 803, 810 (2017); Daniel Susser et al., *Technology, autonomy, and manipulation*, 8 INTERNET POL. REV. 1, 8, 9 (2019); Yaniv Roznai & Nadiv Mordechai, *Access to justice 2.0: Access to legislation and beyond*, 3 THEORY PRACT. LEGIS. 333, 348-353 (2015), Australian Competition & Consumer Commission, *Digital Platforms Inquiry: Final Report* (2019), (להלן: ACCC), Uri Benoliel & Samuel I. Becher, *The Duty to Read the Unreadable*, 60 B. C. L. REV. 2255, 2270 (2019).

¹⁷ Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARVARD LAW REVIEW 1880, 1880-1883 (2013); Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARVARD JOURNAL OF LAW & TECHNOLOGY 551, 553-556 (2023).

תופעה זו ניכרת במגוון תחומים: משתמשים בשירותים פיננסיים נתקלים בהחלטות סיכון המבוססות על פרופילינג שאינו שקוף; שירותי אשראי דיגיטליים מפעילים מודלים שאינם מאפשרים ערעור בפני גורם אנושי; מידע רפואי ורגיש נאסף לעיתים למטרות טיפוליות, אך נעשה בו שימוש נוסף לצרכים מחקרניים ומסחריים ללא הסכמה מודעת; ועוד.

על פי נתוני איגוד האינטרנט הישראלי לשנת 2025, פגיעות דיגיטליות הן תופעה נפוצה בציבור הישראלי. כך, לדוגמה, כ-42% מהישראלים דיווחו שמהלכה כי נפלו קורבן להונאות מקוונות או לניסיונות פישניג, לרבות הודעות דוא"ל או SMS המתחזות לגורם מוכר במטרה לקבל פרטים אישיים. בנוסף, 21% מהציבור גילו תוכנה זדונית מותקנת באחד ממכשיריהם, 7% חוו חדירה לא מורשית לחשבונות דוא"ל או רשתות חברתיות ו-6.1% דיווחו על גניבת זהות או התחזות ברשת. מעבר לפגיעות בפועל, 64% מהציבור חשים כי אין להם שליטה ממשית על המידע האישי שלהם במרחב המקוון.¹⁹ המשותף לכלל הדוגמאות ההלו הוא שניתן היה לצמצם אותן באמצעות מנגנוני פיקוח, שקיפות וציות שהחוק הישראלי אינו מספק כיום.

משום כך, נייר מדיניות זה מתמקד בראש ובראשונה בפגיעות ברמת הפרט ובצורך לגבש מענה רגולטורי שיציב את זכויות המשתמש במרכז. ההתמקדות בזכויות המשתמשים נובעת מתוך הבנה כי עיקר הפגיעות המדינתיות והחברתיות נגזרות במידה רבה מהאופן שבו מטופלות זכויות המשתמשים היחידים.

הפרק הבא יעמיק בזיהוי הסיכונים הדיגיטליים המרכזיים הפוגעים בפרט ובמיפויים, כבסיס לפיתוח מסגרת הגנה ייעודית וממוקדת סיכון.

¹⁹ "מדידת אוריינות סייבר והתנהגות של הציבור הישראלי מול פגיעות מקוונות ופשיעת סייבר: ידע, התנהגות ומסוגלות" **איגוד האינטרנט הישראלי** (25.3.2025); "תחושות ועמדות הציבור הישראלי ביחס לפגיעה בפרטיות" **איגוד האינטרנט הישראלי** (18.1.2022).

פרק ב | סיכוני המידע בשירותים הדיגיטליים

בשנים האחרונות חלה עלייה בשימוש בשירותים דיגיטליים בישראל. סקר שביצע איגוד האינטרנט הישראלי בשנת 2025 מצא כי 98% מהישראלים משתמשים באופן תדיר (יומיומי או מספר פעמים בשבוע) ברשתות חברתיות או בפלטפורמות תוכן, 99% מבצעים שימוש באופן תדיר באפליקציות מסרים ו-70% נעזרים בשירותי בינה מלאכותית.²⁰

למרות החדירה של הטכנולוגיות החדשניות הללו למרבית היבטי החיים בישראל בעשורים האחרונים, החוקים אשר אמורים להסדיר את התחום נחקקו לפני עידן טכנולוגיית המידע. כתוצאה, התפתחות ההגנה המשפטית המוענקת למשתמשים אינה עומדת בקצב השימוש הגובר וההאצה בפיתוחים הטכנולוגיים.²¹ כפועל יוצא, נוצרת פגיעה קשה בזכויות המשתמשים, הנובעת מהסיכונים השונים שקיימים בעת השימוש בשירותים דיגיטליים.

ניתן לחלק סיכונים אלה לארבעה סוגים:

1. סיכונים מסוג היעדר הסכמה מדעת לתנאי השימוש ומדיניות הפרטיות.
2. סיכונים מסוג הגנת מידע.
3. סיכונים מסוג אבטחת מידע.
4. סיכונים מתחום הגנת הצרכן בסביבה הדיגיטלית.

הגנת הצרכן		אבטחת מידע	הגנת מידע		היעדר הסכמה מדעת	
הגבלת פעולות משפטיות	שליטה מוגבלת בתנאי החוזה		פרופילינג	עיבוד מידע	קריאות מוגבלות	הסכמה לא ספציפית לשירות שניתן
חובת בורות ברירת דין	סעיף הסרת תוכן		העברת מידע לצדדים שלישיים	מעקב מתמיד	ז'רגון משפטי מורכב	הגדרת מטרה רחבה
ברירת מקום שיפוט	סיום חד צדדי של ההתקשרות		חוסר יכולת למחוק מידע		הסכמים ארוכים	חוסר שקיפות
הגבלת אחריות	סעיף שינוי חד צדדי				קושי לנווט דו-משמעות	חוסר יכולת להתנות על סעיפים ספציפיים

²⁰ "תדירות השימוש באינטרנט בישראל" איגוד האינטרנט הישראלי, לעיל ה"ש 15.
²¹ חוק הגנת הצרכן, התשמ"א-1981 (להלן: "חוק הגנת הצרכן"); חוק הגנת הפרטיות; חוק החוזים האחדים, התשמ"ג-1982 (להלן: "חוק החוזים האחדים").

1. סיכונים מסוג היעדר הסכמה מדעת לתנאי השימוש ומדיניות הפרטיות

מכוח סעיף 1 לחוק הגנת הפרטיות,²² הסכמה היא הכלי המרכזי של משתמשים להגן על עצמם מפני הפרות אפשריות של זכויותיהם. אך בפועל, ההסכמה הפכה מכלי הגנה לכלי שמכשיר את הפגיעה. במילים פשוטות: כתנאי להתחלת השימוש בשירות או במוצר הדיגיטליים, המשתמשים נדרשים לקרוא מסמכים משפטיים ארוכים, להבין שפה מורכבת, להעריך סיכונים טכנולוגיים – ולעשות כל זאת בפרק זמן קצר. בפועל, רובם מאשרים הסכמות "בעיוורון", מבלי לדעת למה נתנו יד.

כך, תוך שימוש במנגנון משפטי תקין-לכאורה, עלול להתרחש ויתור לא-מודע על זכויות המשתמשים בעידן הדיגיטלי. דפוס זה חמור במיוחד בעידן של שירותים מבוססי דאטה ובינה מלאכותית, שדורשים כמות גדולה של מידע אישי.²³ כאשר משתמש מאשר גישה למידע (גם אם מבלי להבין זאת), הוא למעשה "מזין" את אותם כלים במידע פרטי, ללא שליטה או שקיפות.

הבעיה חריפה במיוחד בקרב אוכלוסיות פגיעות: קטינים, אנשים עם מוגבלויות ודור הגיל השלישי מתקשים במיוחד להתמודד עם הדרישות לקריאה, להבנה ולהסקת מסקנות משפטיות. עבורם, הדרישה להסכמה מדעת הופכת כמעט ריקה מתוכן, ודורשת פתרונות מותאמים. לכן, מדיניות ציבורית חייבת להגדיר מהי הסכמה אפקטיבית, לא רק פורמלית, ולשאוף ליצור כלים שמפשטים את המידע, ממחישים את הסיכון ומצמצמים את ההסתמכות על הסכמה כצידוק בלעדי לעיבוד מידע רגיש.

את הסיכון הכללי של הענקת הסכמה שלא מדעת מצד המשתמשים, ניתן לסווג לשני סוגים עיקריים:

(1) הסכמה כללית לשירות הניתן. למשתמשים אין באמת אפשרות להעניק הסכמה ספציפית לשירות, זאת בשל הסיכונים המשניים הבאים:

- הגדרת מטרה רחבה לשימוש במידע: הגדרת המטרה כה רחבה וכללית, שהיא מאפשרת לספקי השירות לעשות שימוש במידע האישי כמעט לכל פעולה, על סמך הגדרה עמומה, ואינה מאפשרת למשתמשים להבין באופן מלא מהי התכלית של העברת המידע.²⁴ כך, לעיתים מטרות איסוף המידע מנוסחות באופן כללי ועמום, כגון "שיפור חווית השירות" או "שימור קשרי לקוחות". זאת, מבלי שניתן להבין מהו

22 ס' 1 לחוק הגנת הפרטיות.

23 Daniel Nunan & Baskin Yenicioglu, *Informed, uninformed and participative consent in social media research*, 55 INT'L J. MKT. RSCH. 791 (2013).

24 ACCC, לעיל ה"ש 16.

הצורך הקונקרטי של השירות הספציפי באיסוף המידע האישי, לאילו שימושים מעשיים הוא נועד, או כיצד הוא קשור לפונקציונליות המוצעת למשתמש.

- חוסר שקיפות מצד ספקי השירות ביחס למידע שנאסף: ההסכמים אינם מספקים למשתמשים מידע מלא והכרחי בנוגע לשימוש הנעשה במידע האישי שלהם, ולכן אינם מאפשרים להם לגבש הסכמה מדעת ולהבין את משמעות העברת המידע והשלכותיה. כך, לדוגמה, האפליקציות אינן מציינות בפני המשתמשים אילו סוגי נתונים הן עשויות לעבד, מהן מטרות העיבוד, מהם הסיכונים הגלומים בעצם העברת המידע, לאיזה צדדים מועבר המידע האישי ועוד.

- חוסר יכולת להתנות על סעיפים מסוימים בתנאי השימוש ובמדיניות הפרטיות: ההסכמים של האפליקציות הדיגיטליות הם בגדר חוזה אחיד שהמשתמש יכול רק לקבלו – או לוותר על כניסה לשירות. למעשה, אין למשתמש אפשרות לנהל משא ומתן על תנאי ההסכם.²⁵ גם במקרים בהם ניתן לנהל את הרשאות הגישה למידע, למשל בשירותים המופעלים באיחוד האירופי, ייתכן כי אי-הסכמה לתנאים מסוימים תמנע את מתן השירות המבוקש, מה שהופך את ניהול ההרשאות לפעולה לא-מעשית.²⁶

כך, גם כאשר מוצגים למשתמש מנגנונים לניהול העדפות פרטיות, הם עשויים להיות מעוצבים באופן שאינו מאפשר בחירה חופשית ומשמעותית. בפרט, קיימים מקרים שבהם הגישה לשירות מותנית במתן הסכמה גורפת לכלל ההעדפות, תוך שלילת האפשרות להשתמש בשירות בהיקף מצומצם יותר של עיבוד מידע. תצורה זו מהווה דוגמה לדפוסי ממשק מטעים (dark patterns), אשר פוגעים בעקרון ההסכמה מדעת ומרוקנים מתוכן את זכות הבחירה של המשתמש.

(2) קריאות מוגבלת של תנאי השימוש ומדיניות הפרטיות. תנאי השימוש ומדיניות הפרטיות כתובים בשפה משפטית מורכבת,²⁷ מנוסחים בצורה דו-משמעית,²⁸

Hans-W. Micklitz, *Reforming European unfair terms legislation in consumer contracts*, 4 Eu. 25
REV. CONTRACT L. 347 (2010).

Sanchari Das et al., *Privacy Preserving Policy Framework: User-Aware and User-Driven*, in 26
TPRC47: THE 47TH RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY (2019).

Omri Ben-Shahar & Adam Chilton, *Simplification of privacy disclosures: An experimental test*, 45 27
J. LEG. STUD. 5 (2016); ACCC, Roznai and Mordechai, 405 בעמ' 16, לעיל ה"ש 16.

Joel Reidenberg et al., *Trustworthy Privacy Indicators: Grades, Labels, Certifications, and 28*
Dashboards, 96 WASH. U. L. REV. 1409 (2019); Robert H. Sloan & Richard Warner, *Beyond Notice*
and Choice: Privacy, Norms, and Consent, 14 J. HIGH TECH. L. 370 (2014); Mark MacCarthy, *New*
Directions in Privacy: Disclosure, Unfairness and Externalities, 6 I/S A .J. LAW POLICY INF. SOC. 425
(2010).

משתרעים על פני עמודים רבים,²⁹ וכוללים קישורים להסכמים של חברות אחרות.³⁰ כמו כן, גם היבטים טיפוגרפיים אינם מאורגנים (למשל, גודל גופן קטן, גובה קו דחוס, אורך קו מקוצר ועוד).³¹ כלל עניינים אלו מקשים על קריאת ההסכמים והופכים אותה לכמעט בלתי-אפשרית.

2. סיכונים מסוג הגנת מידע

קבוצת סיכונים זו כוללת את כל אותם סיכונים אשר עשויים להביא לפגיעה במידע עצמו, לאחר שנמסר לשירות, בשל השימושים השונים שנעשים בו, אחסונו, המעקב אחריו והעברתו. זאת, לצד ההשלכות השונות שעשויות להיות לפעולות אלו על המשתמשים שמסרו את המידע הראשוני.³² קבוצה זו תכלול את חמשת הסיכונים כדלקמן:

(1) עיבוד מידע למטרות לא-רצויות ובלתי-צפויות:

עיבוד מידע כולל את כל סוגי הפעולות שנעשו במידע הראשוני שניתן על-ידי המשתמש, לרבות אחסון, צבירה, שמירה, איחוד, פיצול, הצלבה ועוד. שירותים רבים, בשל הרצון להשיא רווחים ולקדם את האינטרסים של החברות, מעבדים את המידע באופן שעלול לסכן את המשתמש והמידע שמסר. זאת, בשתי דרכים עיקריות:

- הפיכת נתונים טכניים למידע משמעותי: כאשר המשתמשים מספקים מידע לשירות, הם חושפים פרטים שנראים להם טכניים ולכן אינם חוששים ממסירתם. אולם, התפתחויות טכנולוגיות שיפרו את היכולת לאיין אנונימיות של נתונים ולהסיק מסקנות מהצטברות של נתונים שאינם אישיים. באופן זה, מידע שנחשב טכני עשוי לחשוף מידע אישי על המשתמשים, לרבות הרגלי צריכה, העדפה פוליטית ואף נטייה מינית.³³
- צבירה של מידע ממספר מקורות ושילובו: מפעילי השירות משתמשים בשיטות מתקדמות לאיסוף מידע, אשר מאפשרות להם לצבור נתונים אישיים ממקורות רבים. בדרך זו, השירות יכול ללמוד מידע אישי חדש על אודות המשתמש שהאחרון לא חשף כחלק מההתקשרות בין הצדדים, לבנות עליו פרופיל בהתאם למידע ולסווג אותו.³⁴

Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 41 S.A.J. L. 29 (2008). POL'Y INF. Soc. 543

30 ACCC, לעיל ה"ש 16, בעמ' 406.

31 שם.

32 סיכונים אלו לקוחים מטיפולוגיית סיכונים אותה פיתחה כותבת נייר המדיניות במאמר קודם. להרחבה ראו: Bar Fargon Mizrahi, *Risky Fine Print: A Novel Typology of Ethical Risks in Mobile App User Agreements*, 66(3) VILL. L. REV. 483 (2021).

33 שרון בר-זיו וטל ז'רסקי "פרטיות במשבר זהות: אסטרטגיות הסדרה בעידן ההתממה" **משפט, חברה ותרבות** ב, 125 (2019).

34 René Arnold, Annette Hillebrand & Martin Waldburger, *Informed Consent in Theorie und Praxis*, 39

(2) שימוש בפרופיל דיגיטלי של המשתמש למטרות לא-רצויות:

הפרופיל שיוצר השירות על המשתמש מושפע מהרגלי הצריכה הקבועים שלו, תחביביו ותכונותיו האישיות. בהתאם למאפיינים אלו, אשר מבטאים את עברו של המשתמש, יושפעו ההנחות העתידיות לגביו. על בסיס פרופיל זה, במהלך השימוש בשירות הוא יקבל פרסומת ממוקדת, סל קניות מותאם אישית, כתבות ספציפיות וכדומה. באופן זה, בחירות העבר של המשתמש משפיעות גם על אפשרויותיו והזדמנויותיו העתידיות ומקשות על חשיפתו לבחירות נוספות ועל השתייכותו לקבוצות אחרות.³⁵

בנוסף, ספקי שירות שונים עלולים להפלות בין המשתמשים על בסיס הפרופיל שלהם ולגרום להם לנזק.³⁶ ניתן גם לבצע מניפולציה מקוונת על בסיס פרופיל:³⁷ קמפיינים פוליטיים, לדוגמה, משתמשים בטקטיקה זו כדי למקד פרסומים באופן ספציפי עבור בוחרים מתלבטים.³⁸

לבסוף, יש צדדים שלישיים שאוספים מידע ומגבשים פרופילים על המשתמשים ועושים בהם שימוש, ולא במידע המקורי שהמשתמש נתן.³⁹ בדרך זו, הקשר בין המידע הראשוני שסיפק המשתמש לפרופיל שנוצר על-ידי הצד השלישי אינו מדויק ועשוי להוביל להנחות מוטעות על אודות המשתמש.⁴⁰

כך, עשויים להיווצר הבדלים במחירים המוצגים לצרכנים שונים עבור אותו מוצר או שירות מקוון, בין היתר על בסיס דפוסי גלישה והתנהגות קודמת. לדוגמה, צרכן שאינו נוהג להשוות מחירים או לבצע חיפושים חוזרים, עשוי להיתקל בתג מחיר גבוה יותר מצרכן הנוהג להשוות בין הצעות שונות, אך שמדובר באותו מוצר ובאותם תנאי רכישה. באופן דומה, בשירותי תיירות ותעופה, משתמש בעל דפוסי שימוש קבועים או תדירים

DATENSCHUTZ UND DATENSICHERHEIT - DuD, 730 (2015); Kemp 631-633, בעמ' 12, לעיל ה"ש 14.
 Omer Tene & Jules Polonetsky, Big Data for All: *Privacy and User Control in the Age of Analytics*, 11 NORTHWEST. J. TECH. INT'L. PROP. 5 (2012); Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2012); Sofia Graffanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INT'L. PROP. MED. ENT. L. J. 803 (2016).
 Martin E. Abrams & Lynn A. Goldstein, *Applying Ethics When Using Data beyond Individuals' Understanding*, in THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 270-282 (2018).
 Daniel Susser et al., *Technology, autonomy, and manipulation*, 8 INTERNET POLY REV. 1, 8-9 (2019).
 Rubinstein, לעיל ה"ש 14. 38
 Neumann Nico et al., *How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies* 38(6) MKTG. SCIENCE 918 (2019); Joel Reidenberg et al., *Ambiguity in privacy policies and the impact of regulation*, 45 J. LEG. STUD. S163-S190 (2016).
 Omar Hasan et al., *A discussion of privacy challenges in user profiling with big data techniques: The EEXCESS use case*, in PROCEEDINGS - 2013 IEEE INTERNATIONAL CONGRESS ON BIG DATA, BigData 25-30 (2013). 40

עשוי לקבל הצעת מחיר שונה מזו המוצגת למשתמש המבצע חיפוש חד-פעמי לאותו יעד ובאותם מועדים.

(3) מעקב מתמיד אחר משתמשים בשירותים דיגיטליים:

בעידן המודרני מתרחש מעקב תמידי אחר כל פעולותינו, בעיקר על-ידי גופי מסחריים אשר מנסים להכווין את צעדיהם בהתאם להעדפות המשתמשים.⁴¹ המעקב מתבצע גם כחלק מהגלישה בשירות וגם כאשר איננו משתמשים בשירות במסגרת קבצי Cookies (עוגיות).⁴² המעקב פוגע הן בחירותינו לנוע בצורה חופשית, הן בפרטיותנו והן באוטונומיה שלנו, כי עצם הידיעה על אודות המעקב גורמת לנו לנהוג אחרת ממה שהיינו פועלים אילולא התקיים.⁴³

באופן הזה, משתמשים עשויים להיחשף לתכנים פרסומיים מותאמים בעקבות פעילות שאינה כוללת בהכרח חיפוש יזום או פעולה מקוונת גלויה. לדוגמה, לאחר שיחה טלפונית העוסקת בנושא מסוים, עשויות להופיע על גבי מכשיר הטלפון של המשתמש פרסומות או קישורים לרכישת מוצרים או שירותים הקשורים לאותו נושא, אף מבלי שבוצעה פנייה יזומה לאתר או חיפוש מקוון רלוונטי.

(4) העברות המידע של המשתמשים לצדדים שלישיים:

לעיתים תכופות מעבירים ספקי השירות את המידע שהתקבל על אודות המשתמשים לצדדים שלישיים, לרבות שותפים עסקיים, חברות אם וחברות בת, בתמורה ושלא בתמורה. פעולה זאת פוגעת ביכולת המשתמש להבין את אופן השימוש במידע האישי שלו, לצפות אותו ולשלוט בו – היכן הוא נמצא, למי הוא מועבר ואם הוא מאובטח כראוי.⁴⁴

לדוגמה, משתמשת שהתקינה אפליקציה למעקב אחר מחזור והעניקה הסכמה לעיבוד מידע במסגרת השימוש בשירות, לא התקשרה עם חברות חיצוניות לניתוח נתונים. עם זאת, נמצא כי האפליקציה העבירה מידע אישי על אודותיה, לרבות פרטים

⁴¹ Jose Pagliery, "Super Cookies" Track You, Even in Privacy Mode, CNN BUSINESS (9.1.2015), 41
⁴² Jaspreet Bhatia, *Ambiguity in Privacy Policies and Perceived Privacy Risk* (PhD Thesis. Carnegie Mellon University, 2019); Loos Marco, et al. *Regulation of Digital Content Contracts in the Optional Instrument of Contract Law*, 19 THE. EUR. REV. PRIVATE L. 729 (2011); ACCC בעמ' 387.

⁴³ Daniel J. Solove, *I've Got Nothing to Hide and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007). בית המשפט העליון הכיר באפקט המצנן הזה בהקשר של הכלי של השב"כ (בתקופת הקורונה) בבג"ץ 6732/20 **האגודה לזכויות האזרח נ' הכנסת**, פס' 5 לפסק דינה של השופטת ברוך (נבו 1.3.2021), שקבעה כי עצם האפשרות של השימוש באיכוני השב"כ לצורך איתור חולי קורונה ואנשים עמם באו במגע, יוצרת תחושת מעקב ואפקט של "משטור" ולכך השלכות על הפרט.
⁴⁴ ACCC, לעיל ה"ש 16.

מזהים, לחברת ניתוח נתונים חיצונית (Mixpanel), עמה לא היה לה כל קשר ישיר, ולעיתים גם ללא מודעות להיקף ההעברה.⁴⁵

(5) חוסר יכולת של המשתמש למחוק את המידע שנאסף עליו מהשירות:

כיום, אין בישראל סעיף בחוק שמחייב את ספק השירות למחוק את המידע של המשתמש. עניין זה בעייתי מאחר שלמשתמש אין אפשרות למחוק את ההיסטוריה של השימוש שלו בשירות, היסטוריה שאיננה בהכרח רלוונטית אליו עוד וגם איננה בהכרח נכונה עוד, והוא אף עשוי להתבייש בה. זאת, בניגוד למדינות רבות בעולם, בהן יש לאדם זכות לעדכן או למחוק מידע אישי שנאסף עליו (מכוח "הזכות להישכח").⁴⁶ בנוסף, גם במקומות שבהם מחיקת המידע נדרשת על-פי חוק, קיימים ספקי שירות שמערימים קשיים משמעותיים על ביצוע המחיקה (למשל, היא אורכת זמן רב ונדרשת פרוצדורה מורכבת להשלמתה).⁴⁷

דוגמה לכך היא עובד שהתבקש להוריד למכשיר שלו אפליקציה ייעודית לצורך השתתפות בפעילות ארגונית חד-פעמית, ואשר מבקש למחוק את האפליקציה ואת המידע האישי שמסר במסגרתה לאחר סיום האירוע. עובד זה עלול לגלות כי אין אפשרות מעשית למחיקת המידע או להסרתו ממערכות האפליקציה, חרף היעדר צורך מתמשך במידע שלו לצורך מתן השירות (שכאמור, הוא כבר אינו מעוניין להשתמש בו).

3. סיכוני אבטחת מידע

סיכונים בתחום אבטחת המידע נובעים הן מפריצות למאגרי מידע, כלומר גישה בלתי-מורשית למידע אישי, והן מכשלים בהגנה על מידע, כגון הרשאות גישה רחבות מדי, היעדר הצפנה מספקת או ניהול לקוי של נתונים. סיכונים אלה עשויים להתממש לא רק באפליקציה עצמה, אלא גם אצל צדדים שלישיים, כגון ספקי שירות, חברות ניתוח נתונים או שותפים עסקיים, המעבדים את המידע במסגרת השירות.⁴⁸

הסביבה הדיגיטלית מבוססת על מספר לא-מבוטל של ספקי שירות. בעיית אבטחה – אפילו

⁴⁵ "בניגוד להצהרתה: אפליקציית המעקב אחר מחזור סטארדאסט מעבירה מידע לצד שלישי" **כלכליסט** (28.6.2022).

⁴⁶ טל מימרן וליאור ויינשטיין, **הזכות להישכח**, נייר מדיניות (מכון תכלית, דצמבר 2023).

⁴⁷ Hana Habib et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, The Fifteenth Symposium on Usable Privacy and Security. Santa Clara, CA, USA 395 (2019).

⁴⁸ תהילה שוורץ אלטשולר, "הקדמה", בתוך: **פרטיות בעידן של שינוי** 11-13 (המכון הישראלי לדמוקרטיה, 2012).

אם היא קיימת רק אצל גורם אחד בשרשרת השחקנים – מגבירה את הפוטנציאל להעברת מידע אישי לצדדים שלישיים, ללא הסכמה וללא ידיעה.⁴⁹ סקר שערכה הסוכנות לעסקים קטנים ובינוניים בשנת 2024 העלה כי 6% מכלל העסקים נחשפו באותה שנה למתקפות סייבר, וכי 1.6% מכלל העסקים חוו מתקפה שגרמה לנזק משמעותי לארגון.⁵⁰ בתקופות רגישות, כמו מערכות בחירות, מלחמות או מצבי חירום ביטחוניים, שכיחות המתקפות אף עולה בצורה משמעותית.⁵¹ נתונים אלה ממחישים עד כמה סביבת המידע בישראל פגיעה, גם כאשר מדובר במשתמשים פרטיים הנתפסים כ"בלתי מעניינים".

סיכון נוסף הינו **סחר במידע האישי** של המשתמשים על-ידי חברות או גופים שמוכרים מידע לצדדים שלישיים.⁵² חשש מרכזי נוסף הינו גניבת זהותו של המשתמש בדרכים שונות, לרבות גניבת פרטי כרטיס אשראי, שימוש בשם האדם לביצוע עבירה פלילית ועוד.⁵³

החשש לליקויי אבטחת מידע בישראל אינו תיאורטי – כבר קיימות עדויות לחומרתן של ההשלכות האפשרויות של תקיפות סייבר על מאגרים הכוללים מידע אישי, כפי שקרה בזמן מלחמת "חרבות ברזל" בקריה האקדמית אונו. באותו מקרה, קבוצת האקרים בשם Malek-Team הדליפה מידע שכלל, בין היתר, רשומות עם פרטים אישיים של מאות סטודנטים, צילומי וידאו של שיעורים, מאגרי מידע, מסמכים פיננסיים ועוד.⁵⁴

החשש איננו רק מדליפת המידע הקיים, אלא מפני סכנות נוספות כגון זינף, התחזות ועוד.⁵⁵ מידע אישי הוא בעל חשיבות אדירה להגנה על פרטיות. יש לזכור כי חשיבותה של הזכות לפרטיות נובעת, בין היתר, מהעובדה שהיא בסיס חשוב להגנה על כבוד האדם⁵⁶ והאוטונומיה שלו,⁵⁷ ומהווה דרישה בסיסית לרווחתו של אדם ולמימוש שאר החירויות שלו.⁵⁸ בנוסף, כמצוין לעיל, בעידן הנוכחי למידע אישי יש ערך כלכלי רב אשר שחקנים שונים, דוגמת חברות פרטיות, יכולים לנצל בקלות.

49 מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 169 (2010).
 50 הסוכנות לעסקים קטנים ובינוניים במשרד הכלכלה דו"ח סייבר בעסקים קטנים ובינוניים (2024).
 51 ראו: מערך הסייבר **סיכום שנה 2023** (2024).
 52 Amir Fux, *Terrorism and Privacy - A Proposal for Rethinking the Tools for Coping with Terrorism Online*, in: TEHILLA SCHWARTZ .A., *PRIVACY IN AN ERA OF CHANGE*, THE ISRAELI DEMOCRACY INSTITUTE 242-243 (2012).
 53 Kemp, לעיל ה"ש 12.
 54 יובל מן "בצל המלחמה: האקרים פרצו לקריה האקדמית אונו" **Ynet** (10.10.2023).
 55 ר' למשל: Identity Management Institute, *Biometric Authentication Benefits and Risks* (14.5.2024),
 56 Beizaras and Levickas v. Lithuania, App. No. 41288/15 Eur. Ct. H.R. 117 (2020).
 57 Reklos and Davourlis v. Greece, App. No. 1234/05 Eur. Ct. H.R. 38 (2009).
 58 ראו לדוגמה: UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8.5.1988), 11 **חוקתית**, 83 (2023).
 59 **פרטיות**

4. סיכונים מתחום הגנת הצרכן בסביבה הדיגיטלית

בנוסף לסיכונים אשר עוסקים במידע של המשתמש, בהגנה עליו ובאבטחתו, קיימים סיכונים שנובעים מפערי הכוחות בין המשתמשים לספקי השירות. תנאי השירות ומדיניות הפרטיות נחשבים חוזים אחידים דיגיטליים, אשר המשתמשים אינם יכולים לנהל משא ומתן לגבי תנאיהם. ספקי השירות מודעים לכך ובמסגרת התנאים מוסיפים סעיפים שיש בהם כדי לפגוע בזכויות הצרכניות של המשתמשים ובאפשרותם לפנות לערכאות משפטיות. סיכונים אלו ניתן לחלק לשני סיכונים משניים, כדלקמן:

(1) שליטה מוגבלת של המשתמשים בתנאי החוזה ובמידע על אודותיהם המוזן בשירות: סיכון משני זה מורכב מהסיכונים הבאים:

- סעיף להסרת תוכן: ספקי השירות קובעים במסגרת ההסכמים עמם כי שמורה להם הזכות להסיר את התוכן שיצרו המשתמשים על-פי שיקול דעתם ומבלי ליידע את המשתמשים מראש או לקבל את הסכמתם.⁵⁹

לדוגמה, משתמש עשוי לפרסם ברשת חברתית תוכן הכולל הבעת עמדה פוליטית, ולאחר זמן קצר לגלות כי התוכן הוסר על-ידי ספק השירות, מבלי שנמסר לו נימוק קונקרטי להסרה. בפנייתו לשירות עשוי המשתמש להיווכח כי תנאי השימוש מקנים לספק שיקול דעת רחב ובלתי-מוגבל להסרת תוכן, בכל עת וללא חובת הנמקה או זכות השגה אפקטיבית.

- סיום ההתקשרות החוזית באופן חד-צדדי: סעיף זה מעניק למפעילי השירות את הזכות להשעות את החוזה עם המשתמש או להפסיק אותו.⁶⁰ הסעיף הופך להיות בעייתי כאשר סיום ההתקשרות יכול להיעשות מכל סיבה שהיא, בלי הסבר מצד ספק השירות וללא מתן התראה מראש.

לדוגמה, משתמש ותיק בפלטפורמה חברתית, אשר עשה בה שימוש במשך שנים וצבר במסגרתה תכנים אישיים, קשרים ומידע רב, עלול לגלות כי חשבונו הוסר או הושעה באופן חד-צדדי, ללא התראה מוקדמת. במצב כזה, נמנעת ממנו הגישה לכלל המידע האישי שצבר במהלך השנים, בלא שניתנה לו אפשרות מוקדמת להשגה, לשימור המידע או לניודו.

Marco Lippi et al., *Automated detection of unfair clauses in online consumer contracts*, 302 59 in *FRONTIERS IN ARTIFICIAL INTELLIGENCE AND APPLICATIONS* 145-154 (2017); Marco Lippi et al., *CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service*, 27 *ARTIF. INT'L. L.* 117 (2019).

Lippi et al., לעיל ה"ש 59, בעמ' 125. 60

- סעיף שינוי חד-צדדי: באמצעות סעיף זה, ספקי שירות רבים יכולים לעדכן את תנאי ההסכם הראשוני לעיתים תכופות. כמו כן, הם מניחים את האחריות להתעדכן מעת לעת בשינויים שהם מבצעים לפתחם של המשתמשים, ומצפים מהם להיות מודעים לשינויים שנעשו.⁶¹

לדוגמה, משתמש בשירות מסרים מיידיים עשוי לקבל הודעה שלפיה המשך השימוש בשירות מותנה באישור מדיניות פרטיות ותנאי שימוש מעודכנים. גם כאשר השינויים כוללים הרחבה של אופן עיבוד המידע או שינוי מהותי בתנאי ההתקשרות, למשתמש לא ניתנת אפשרות ממשית להתנגד לשינויים או לבחור חלופה, וההסכמה הופכת בפועל לתנאי כפוי להמשך קבלת השירות.

- סעיף הגבלת אחריות: ספקי שירות רבים מסירים מעצמם כל אחריות לגבי המידע של המשתמשים, להעברתו לצדדים שלישיים, לאבטחתו, להגנתו ולפגיעות שעשויות להיגרם למידע כתוצאה מהשירות. ספקי השירות מציינים במסגרת תנאי השימוש שהם אינם אחראים למידע המשתמש אשר מוזן באתר, ובכך בעצם מכשירים בצורה חוקית הסרת אחריות כללית.⁶²

לדוגמה, משתמש באפליקציית משחקים בתשלום עלול לגלות כי פרטי כרטיס האשראי שהוזנו במסגרת השימוש בשירות נוצלו לרעה לביצוע עסקאות נוספות ללא הרשאה. עם פנייתו לספק השירות, נמסר לו כי בהתאם לתנאי השימוש האחריות לנזקי אבטחת מידע או לשימוש בלתי-מורשה בפרטי התשלום אינה מוטלת על הספק, וכי עליו להפנות את הטיפול בנושא לגורם חיצוני, כגון חברת האשראי.

- (2) הגבלת פעולות משפטיות של משתמשים:** ספקי שירות עשויים לכלול בהסכמים שלהם הוראות אשר מגבילות את אפשרותם של המשתמשים לקיים הליך משפטי, ובכך מצמצמים את יכולתם לממש את הזכויות המוקנות להם בחוק.⁶³ הוראות אלה כוללות חובת בורות, סעיף ברירת דין וסעיף ברירת מקום שיפוט.

לדוגמה, משתמש שרכש כרטיסים לאירוע באמצעות אפליקציה דיגיטלית עלול לגלות במועד האירוע כי הכרטיסים שסופקו לו אינם תקפים או אינם קיימים בפועל. בבואו לפנות לערכאות לשם מימוש זכויותיו, הוא עלול לגלות כי תנאי השימוש של השירות מחייבים ניהול הליכים משפטיים במדינה זרה ועל-פי דין זר, באופן המקשה באופן מהותי על מימוש זכות הגישה לערכאות.

Loos, M., & Luzak, J. *Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers*, 39(1) J. CONSUMER POL'Y, 63, 86-88 (2016).

62 שם, בעמ' 79-81.

63 להגדרת תנאי מקפח בהקשרים אלו ראו ס' 3 לחוק החוזים האחדים.

הצגת הסיכונים המרכזיים הנובעים מהשימוש הגובר במידע אישי במרחב הדיגיטלי מעלה תמונה מורכבת, המחייבת תשומת לב רגולטורית מוגברת. הפרקים הבאים יבחנו כיצד מתמודדות מערכות אסדרה עם סיכונים אלו. פרק 3 יסקור את ההגנות הרגולטוריות שנקבעו בשנים האחרונות בישראל, ופרק 4 יסקור את המודלים המרכזיים שהתפתחו בעולם. בחינה זו תאפשר לעמוד על הפערים בין היקף הסיכונים לבין טיב ההגנות הקיימות, ולבחון אם המענה הרגולטורי שניתן כיום אכן תואם את מורכבות האתגרים שתוארו.

פרק ג | האסדרה הקיימת בישראל להתמודדות עם סיכונים בתחום שירותי המידע

נוכח היקפם וחומרתם של הסיכונים המרכזיים הכרוכים בשימוש הגובר במידע אישי ובשירותים מקוונים, אם מדינת ישראל מבקשת להגן על אזרחיה מפניהם – עליה לייצר מנגנוני אסדרה מתאימים. ואכן, הדין הישראלי מנסה לגבש מענה לסיכונים השונים באמצעות מספר מסגרות חקיקתיות העוסקות בהיבטים של הגנת מידע ופרטיות ואבטחת מידע, וכן בהיבטים צרכניים וחוזיים של התקשרויות דיגיטליות. פרק זה מציג את ההגנות המרכזיות שנקבעו בחקיקה הקיימת בישראל, ואת האופן שבו הן מבקשות להתמודד עם הסיכונים שתוארו לעיל.

1. החקיקה הקיימת בהיבטים של הגנת מידע, אבטחת מידע ופרטיות

הזכות לפרטיות מעוגנת במשפט הישראלי כזכות יסוד⁶⁴, וחוק הגנת הפרטיות מהווה את התשתית המרכזית להסדרת השימוש במידע אישי.⁶⁵ החוק מגדיר מהי פגיעה בפרטיות⁶⁶ ומעגן עקרונות יסוד כגון דרישת ההסכמה,⁶⁷ חובת היידוע⁶⁸ וצמידות המטרה.⁶⁹ כמו כן, החוק מסדיר את החזקת המידע במאגרי מידע, מגדיר קטגוריות של מידע רגיש וקובע חובות החלות על בעלי השליטה במאגרים והמחזיקים בהם.⁷⁰

לצד החוק, תקנות אבטחת מידע שנכנסו לתוקף בשנת 2018 קובעות סטנדרטים מפורטים ומדורגים לאבטחת מידע אישי המצוי במאגרי מידע.⁷¹ התקנות מסדירות, בין היתר, את אופן ניהול המאגר, מיפוי מערכות המידע וביצוע סקרי סיכונים, ומפרטות את החובות החלות על בעלי המאגרים בהתאם לרמת הסיכון. בנוסף, הן מרחיבות את סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות, אשר פועלת באמצעות ביקורות יזומות, פיקוח מגזרי ופרסום הנחיות מקצועיות.

באמצעות מסגרת זו מבקש הדין הישראלי להתמודד עם סיכונים הנוגעים לאבטחת מידע, לשמירה על שלמותו ולמניעת גישה בלתי-מורשית אליו. במקביל, חוק הגנת הפרטיות כולל מנגנונים כלליים להסדרת השימוש במידע, אשר יושמו לאורך השנים גם בהקשרים דיגיטליים, בין היתר באמצעות פרשנות שיפוטית והנחיות רגולטוריות.⁷²

64 ס' 7 לחוק יסוד: כבוד האדם וחירותו, התשנ"ב-1992, ס"ח 150.

65 חוק הגנת הפרטיות.

66 ס' 1 ו-2 לחוק הגנת הפרטיות.

67 ס' 3 לחוק הגנת הפרטיות.

68 ס' 11 לחוק הגנת הפרטיות.

69 ס' 8(ב) וס' 9(2) לחוק הגנת הפרטיות.

70 פרק ב' לחוק הגנת הפרטיות; תיקון מס' 13 לחוק הגנת הפרטיות יוצר הגדרות חדשות לבעל שליטה במאגר ומחזיק במאגר. "בעל שליטה" בהתאם לס' 2(3) לתיקון הוא מי שקובע את מטרות עיבוד המידע שבמאגר המידע; "מחזיק" בהתאם לס' 2(5) לתיקון הינו גורם חיצוני לבעל השליטה במאגר המידע המעבד בעבורו מידע.

71 תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

72 ראו לדוגמה: "מדיניות הרשות להגנת הפרטיות בנוגע לקבלת דיווח אירוע אבטחה חמור" (משרד המשפטים, הרשות להגנת הפרטיות 2018.1.5); עת"מ 28857-06-17 עמותת חברת הסייעוד נ' משרד הביטחון

2. החקיקה הקיימת בהיבטים של הגנות צרכניות וחוזיות בהתקשרויות דיגיטליות

ההגנה על משתמשים בהתקשרויות מקוונות נשענת גם על דיני הצרכנות והחוזים. חוק הגנת הצרכן מסדיר את יחסי ספק-צרכן וקובע איסורים על הטעיה וניצול פערי כוחות, ⁷³ חובות גילוי ביחס לפרטים מהותיים בעסקה ⁷⁴ ודרישות בסיסיות של הוגנות וקריאות. ⁷⁵ הוראות אלה חלות גם על התקשרויות המתבצעות בסביבה דיגיטלית, ובכלל זה עסקאות מכר מרחוק. ⁷⁶

לצד זאת, חוק החוזים האחידים מוסיף שכבת הגנה ביחס לתנאי שימוש ומדיניות פרטיות, בהיותם חוזים אחידים דיגיטליים. ⁷⁷ החוק מגדיר מהם תנאים מקפחים ומקנה לבית המשפט סמכות לבטל או לשנות אותם, לרבות תנאים העוסקים בשינוי חד-צדדי של ההסכם, הגבלת אחריות, קביעת מנגנוני יישוב סכסוכים וברירת מקום שיפוט. ⁷⁸

באמצעות חקיקה זו מבקש הדין הישראלי להתמודד עם הסיכונים הנובעים מפערי כוחות, מחוסר שקיפות ומהיעדר משא ומתן בהתקשרויות מקוונות.

לצד החקיקה, פועל מערך רגולטורי שמבטיח את יישום ההגנות על צרכנים גם במרחב הדיגיטלי. הרשות להגנת הצרכן ולסחר הוגן אוכפת את חוק הגנת הצרכן וחוק הסחר ההוגן, חוקרת הפרות, מטילה עיצומים כספיים, מנפיקה הנחיות ומטפלת בתלונות צרכנים, לרבות בעסקאות מקוונות ובמכר מרחוק. פעילותה מבקשת להבטיח גילוי נאות, שקיפות והימנעות מהטעיה וחייבים בלתי-מורשים. לצידה, רשות התחרות מגינה על הצרכן ברמה המערכתית באמצעות פיקוח על כוחות שוק ואיתור מצבים שבהם פלטפורמות דיגיטליות או ספקים דומיננטיים עלולים לפגוע בתחרות החופשית.

כאמור, הסיכונים המרכזיים הנובעים משירותים מקוונים זכו להתייחסות בחקיקה הישראלית הקיימת, הן בתחום הגנת המידע והפרטיות והן בתחום הצרכנות והחוזים. עם זאת, ההסדרים הקיימים אינם מספקים מענה שלם ומעודכן לאופן שבו סיכונים אלה מתממשים בפועל בסביבה הדיגיטלית. חלק ניכר מהחקיקה הרלוונטית נחקק בשנות ה-80

(נבו 1.7.2019); רע"א (ת"א) 29227-02-15 **אוקסמן נ' סוברי** (נבו 1.6.2015); ת"פ (י-ם) 52026-06-15 **מדינת ישראל נ' כהן ואח'** (נבו 25.05.2018); ע"א (ת"א) 44711-11-14 **סביר נ' בר נוי** (נבו 22.6.2015).

73 ס' 2 לחוק הגנת הצרכן.

74 ס' 4 לחוק הגנת הצרכן.

75 ס' 4א' לחוק הגנת הצרכן.

76 ס' 14ג' לחוק הגנת הצרכן.

77 ביתיה גוטל "חוזים אחידים: הצדקה להתערבות, המצב הקיים וחוזי מכר מרחוק כמקרה בוחן" חוות דעת הרשות להגנת הצרכן וסחר הוגן, 15-18 (2018).

78 ס' 2-4 לחוק החוזים האחידים.

של המאה הקודמת ואינו מבוסס על תפיסה ייעודית של שירותים דיגיטליים, פלטפורמות מבוססות מידע ומודלים כלכליים הנשענים על איסוף מידע אישי ועיבודו.

בתחום הגנת המידע והפרטיות, הדגש בדין הישראלי מושם בעיקר על היבטים של אבטחת מידע ועל חובות פורמליות הנוגעות לניהול מאגרי מידע. לעומתם, סיכונים הנובעים מאופן עיבוד המידע, משימושים משניים, מפרופילינג וממעקב מתמשך אחר משתמשים, זוכים לאסדרה כללית בלבד או מוסדרים בעקיפין. היעדר התייחסות מפורשת לפרקטיקות אלו מגביל את יכולת המשתמשים להבין את היקף השימוש במידע על אודותיהם ולממש שליטה אפקטיבית בו.

גם התחום הצרכני-חוזי אינו מותאם למאפייניהם הייחודיים של חוזים אחידים דיגיטליים, אף שהדין הישראלי כולל מנגנונים חשובים של חובת גילוי, איסור הטעיה והתמודדות עם תנאים מקפחים. חוזים אלה מעוצבים לעיתים באופן המקשה על קריאה והבנה, כוללים שינויים חד-צדדיים תכופים ומאופיינים בריבוי הסכמות קצרות בזמן – במיוחד בשירותים המוצגים כ"חינמיים", שבהם המידע האישי משמש בפועל כאמצעי תשלום. מאפיינים אלה מגבירים את הסיכון לאי-מודעות של המשתמשים לתנאי ההתקשרות ולמשמעויותיהם.

בנוסף, מנגנוני הפיקוח והאכיפה הקיימים מתקשים להתמודד עם היקף ההתקשרויות הדיגיטליות ומהירותן. במרבית המקרים, פגיעות הנובעות מתנאי שימוש, מעיבוד מידע או משילוב בין השניים אינן מגיעות לבירור משפטי, בין היתר בשל העלות הגבוהה של ההליך ביחס לנזק האישי שנגרם לכל משתמש. כתוצאה מכך, ההגנות הקבועות בדין מופעלות באופן מוגבל בלבד, והפער בין האסדרה הפורמלית לבין רמת ההגנה בפועל הולך ומתרחב.

3. יוזמות חקיקה בישראל בתחום השירותים הדיגיטליים ותיקון מס' 13

בשנים האחרונות, על רקע האתגרים שתוארו לעיל, החל משרד המשפטים לקדם שורה של תיקונים לחוק הגנת הפרטיות במטרה לצמצם את הפערים הקיימים בדין הישראלי ולהתאים את ההסדרים הקיימים לעידן הדיגיטלי. תיקונים אלה ביקשו, בין היתר, לחזק את מנגנוני הפיקוח והאכיפה, לעדכן הגדרות מיושנות ולהרחיב את ההגנה על משתמשים מפני סיכונים הנוגעים לעיבוד מידע אישי ולהגנת מידע.

עם זאת, ההתפתחות נעשתה לאורך השנים באופן הדרגתי ומקוטע, באמצעות תזכירים והצעות חוק נפרדות, אשר לא תמיד גובשו במסגרת תפיסה רגולטורית אחידה וקוהרנטית. כפועל יוצא, דיני הגנת הפרטיות בישראל המשיכו להתפתח באופן חלקי, תוך פיצול בין תיקונים מוסדיים, תיקוני הגדרות והסדרים נקודתיים נוספים.

הרפורמה המרכזית ביותר בשנים האחרונות בעיצוב דיני הפרטיות בישראל הוא תיקון מס' 13 לחוק הגנת הפרטיות, אולם דרכו לחקיקה הייתה ארוכה ורצופת קשיים, עיכובים ושינויים. בחודש מרץ 2018 אישרה הכנסת בקריאה ראשונה את הצעת חוק הגנת הפרטיות (תיקון מספר 13),⁷⁹ שעיקרה הרחבת סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות. בהמשך, ב-23 ביולי 2020 פרסם משרד המשפטים את תזכיר חוק הגנת הפרטיות (הגדרות וצמצום חובת רישום),⁸⁰ אשר ביקש לעדכן את הגדרות החוק ולהתאימן, בין היתר, לעקרונות תקנות ה-GDPR, לצד צמצום חובת רישום מאגרי מידע למאגרים בעלי סיכון גבוה לפגיעה בפרטיות ובהגנת מידע. התזכיר מבוסס ברובו על תזכיר חוק שהוצע בשנת 2012 ולא התגבש לכדי חוק.⁸¹

לאחר מכן, ביום 7 בנובמבר 2021, אישרה ועדת השרים לענייני חקיקה את הצעת חוק הגנת הפרטיות (תיקון מס' 14),⁸² אשר נועדה לרכז חלק מן ההסדרים שנכללו בתיקון מס' 13 ובתזכיר משנת 2020 במסגרת רפורמה רחבה יותר בדיני הגנת הפרטיות. עם זאת, הצעת תיקון מס' 14 לא הבשילה לכדי חקיקה עצמאית, וחלק מהוראותיה שולבו בהמשך במסגרת הליכי החקיקה של תיקון מס' 13, שאושר לבסוף באוגוסט 2025 בקריאה שנייה ושלישית.⁸³

מטרתו של תיקון מס' 13 היא להתאים את החקיקה לעידן הדיגיטלי ברוח תקנות ה-GDPR, להקנות למשתמשים זכויות נוספות ביחס למידע ואף להרחיב את סמכויות הפיקוח והאכיפה של הרשות האמונה על התחום, קרי הרשות להגנת הפרטיות. התיקון מעדכן את ההגדרות הקיימות בחוק הגנת הפרטיות לעידן המודרני, מרחיב את תחולתן של קטגוריות מידע רגיש ומגביל את עיבוד המידע למטרות שנקבעו כדין.⁸⁴

בנוסף, תיקון מס' 13 מצמצם את חובת הרישום של מאגרי מידע כך שתחול בעיקר על מאגרים בעלי היקף פעילות רחב או כאלה הכרוכים בסיכון מוגבר לפגיעה בפרטיות, ובכלל זה מאגרים הכוללים העברת מידע לצדדים שלישיים. מאגרים אחרים, לרבות כאלה הכוללים מידע רגיש, עשויים להיות כפופים לחובת הודעה לרשות במקום חובת רישום.⁸⁵

לצד זאת, התיקון מעניק לרשות להגנת הפרטיות סמכויות פיקוח ואכיפה מוגברות, לרבות

79 הצעת חוק הגנת הפרטיות (תיקון מס' 13).
80 תזכיר חוק הגנת הפרטיות (תיקון הגדרות וצמצום חובת הרישום).
81 תזכיר חוק הגנת הפרטיות (תיקון צמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב-2012.
82 הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022, ה"ח הממשלה 1496.
83 חוק הגנת הפרטיות (תיקון מס' 13).
84 שם, בס' 1 ו-4.
85 שם, בס' 4.

האפשרות להטיל קנסות מנהליים,⁸⁶ ומחייב גופים מסוימים למנות ממונה הגנת פרטיות.⁸⁷ הוא אף קובע סנקציות חדשות, בהן פיצויים עונשיים ללא הוכחת נזק,⁸⁸ וכולל פרק ייעודי חדש של עבירות פליליות במאגרי מידע, למשל בגין עיבוד מידע אישי ללא רשות.⁸⁹ לבסוף, התיקון קובע הליך פנייה מקדמית לרשות, למתן חוות דעת מטעמה בעניין עמידה בתקנות.⁹⁰

לצד חקיקתו של תיקון מס' 13 נעשו ניסיונות משפטיים נוספים לרפורמות בתחום הפרטיות: באפריל 2023 אישרה ועדת החוקה, חוק ומשפט תקנות אשר קובעות הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי.⁹¹ התקנות מטילות שלוש חובות נוספות על בעל מאגר מידע ביחס למידע הנמצא במאגר אשר כפוף לתקנות: (1) מחיקת המידע של נושא המידע לפי בקשתו או במקרה של מידע עודף שאינו נדרש עוד; (2) יצירת מנגנונים שיוודאו כי המידע שקיים במאגר שלם, נכון, ברור ומעודכן; ו-(3) חובת יידוע נושא המידע על זהות בעל המאגר, דרכי ההתקשרות עמו, המטרה שלשמה נאסף המידע, סוג המידע שהועבר, זכויותיו והעברת מידע לצדדים שלישיים.

בנוסף, הונחו על שולחן הכנסת ה-25 עוד מספר הצעות חוק פרטיות בתחום הפרטיות וההגנה על מידע אשר חקיקתן לא הושלמה:

- ההצעה הראשונה, הגנת הפרטיות (תיקון – חיזוק הזכות לפרטיות וההגנה עליה),⁹² עוסקת בהרחבת הפיקוח והאכיפה להבטחת קיום הוראות החוק ומבצעת תיקונים מהותיים בהצעת החוק (תיקון מספר 14).
- ההצעה השנייה, הגנת הפרטיות (תיקון – מחיקה ממאגרי מידע),⁹³ נועדה לעגן בחקיקה את זכותו של אדם לדרוש את מחיקת המידע על אודותיו ממאגר מידע.
- ההצעה השלישית, הצעת חוק הגנת הפרטיות (תיקון – איסור פרסום הקלטה של אדם), מוסיפה להגדרה של פגיעה בפרטיות גם מעשה של פרסום הקלטה של אדם ברבים וקובעת שמעשה זה יהווה עוולה אזרחית ועבירה פלילית, בכפוף לחריגים והגנות הקבועים בדין, לרבות במקרים של עניין ציבורי או פרסום מותר לפי חוק.⁹⁴

86 שם בס' 33 והתוספת השלישית.

87 שם, בס' 18.

88 שם, בס' 13.

89 שם, בפרק ד'.

90 שם, בס' 24.

91 תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023.

92 הצעת חוק הגנת הפרטיות (תיקון – חיזוק הזכות לפרטיות וההגנה עליה), התשפ"ג-2022, פ/8/25.

93 הצעת חוק הגנת הפרטיות (תיקון – מחיקה ממאגרי מידע), התשפ"ג-2022, פ/549/25.

94 הצעת חוק הגנת הפרטיות (תיקון – איסור פרסום הקלטה של אדם), התשפ"ג-2023, פ/1343/25.

התקדמות נחוצה, אך בלתי-מספקת

חרף התקדימים החשובים שקבעו תיקון מס' 13 והתקנות שהותקנו מכוחו, הם מספקים מענה חלקי בלבד לסיכונים בתחום הגנת המידע. לצידם, ההצעות החדשות שהוצגו לעיל משקפות ניסיון להתמודד עם פערים נוספים, אך כל עוד לא התקבלו, אין בהן כדי להעניק מענה משפטי מחייב. מכל מקום, גם בהינתן מכלול ההסדרים הקיימים והמוצעים, תחומים מרכזיים ובהם פרופילינג ומעקב מתמיד אחר משתמשים, אינם מוסדרים באופן מלא. אך גם אם יתקבלו כל התיקונים הללו, זכויות מהותיות למשתמשים, ובהן הזכות לניוד מידע, הזכות לחזרה מהסכמה והזכות לערער על החלטה משמעותית שהתקבלה באמצעים אוטומטיים, עדיין יהיו זקוקות לאסדרה.

לבסוף, גם שיטת החקיקה עצמה יוצרת קשיים: מתכונת של "טלאי על טלאי" – עבודה בשלבים, כאשר כל שלב מבצע תיקון אחר בחוק – עלולה לייצר חוסר אחידות במונחים השונים ולהפנות לסעיפי חוק שאינם תקפים עוד. בנוסף, ביצוע מספר רב של תיקונים בחוק הגנת הפרטיות יקשה על המעקב אחר התיקונים שהוכנסו והבנה מה חודש בחקיקה, ועלול לבלבל משתמשים אשר ירצו לממש את זכויותיהם.⁹⁵

ראוי לציין כי לצד תיקוני החקיקה הממשלתיים, בשנת 2019 פורסמה גם הצעה מטעם המכון הישראלי לדמוקרטיה לרפורמה כוללת בדיני הגנת הפרטיות בישראל, תחת הכותרת "הצעת חוק הגנת הפרטיות, התשע"ט-2019".⁹⁶ מטרת ההצעה הייתה לעדכן מן היסוד את ההסדרים הקיימים ולהתאימם למציאות הדיגיטלית ולטכנולוגיות עיבוד מידע מתקדמות, תוך התבססות על עקרונות רגולטוריים המקובלים בעולם, ובראשם תקנות ה-GDPR.

ההצעה כוללת שורה של חידושים משמעותיים בתחום הגנת המידע, ובהם הרחבת זכויות נושאי מידע; הכרה בזכות להישכח ובזכות לניוד מידע; קביעת זכות לקבלת הסבר ביחס להחלטות המבוססות על עיבוד אוטומטי; חיזוק חובותיהם של בעלי שליטה ומעבדי מידע; הרחבת תחולתו האקסטרטוריאלית של החוק; וכן חיזוק סמכויותיה של הרשות להגנת הפרטיות. בנוסף, ההצעה מבקשת לעדכן את מושגי היסוד של הדין הישראלי, ובהם הגדרת "מידע אישי", "עיבוד" ו"הסכמה", ולהתאים אותם לעידן הדיגיטלי.

עם זאת, על אף חשיבותה והיקפה הרחב, ההצעה של המכון הישראלי לדמוקרטיה ממוקדת בעיקר בדיני פרטיות והגנת מידע, ואינה מספקת מענה כולל למכלול הסיכונים

⁹⁵ יניב רוזנאי ונדיב מרדכי "על נגישותה של החקיקה" **משפט וממשל** יט 429, 461-473 (2018).
⁹⁶ רחל ארידור הרשקוביץ ותהילה שוורץ-אלטשולר, **הצעת חוק הגנת הפרטיות, התשע"ט-2019** (המכון הישראלי לדמוקרטיה, יוני 2019).

שמייצרים שירותים דיגיטליים במציאות הטכנולוגית העכשווית. כך, למשל, היא איננה מתמודדת באופן מספק עם סוגיות רחבות הנוגעות לעיצוב כוחן של פלטפורמות דיגיטליות, להשפעות חברתיות ודמוקרטיות של אלגוריתמים ומנגנוני המלצה, לפרקטיקות מסחריות מבוססות מניפולציה התנהגותית, או לחובות שקיפות ואחריות רחבות ביחס למערכות בינה מלאכותית ושירותים דיגיטליים מורכבים. במובן זה, גם ההצעות המתקדמות ביותר בתחום הפרטיות, כמו זו שמביא המכון הישראלי לדמוקרטיה, אינן מייצרות כיום מסגרת אסדרה כוללת למרחב הדיגיטלי.

משכך, על אף החשיבות הרבה של תיקון מס' 13 ושל ההצעות לרפורמה בדיני הגנת הפרטיות, מעצם היותם ממוקדים בדיני פרטיות והגנת מידע בלבד, הם אינם מספקים מענה כולל לאתגרים שמציב המרחב הדיגיטלי בימינו. מסגרת אסדרה המבקשת להגן באופן אפקטיבי על זכויות משתמשים בעידן הדיגיטלי, בדומה לחקיקות אחרות בעולם, צריכה להיות מקיפה ולאגד בתוכה גם היבטים צרכניים וחוזיים, בנוסף להיבטים של פרטיות.

פרק ד | מגמות אסדרה בתחום שירותי המידע הדיגיטלי – מבט השוואתי

בעשור האחרון נרשמה בעולם התקדמות משמעותית בהתמודדות עם סיכונים הכרוכים בשימוש בשירותים דיגיטליים. עם זאת, חרף הצעדים שננקטו, הפער בין הטכנולוגיה למשפט ממשיך לגדול: הטכנולוגיה מתפתחת ומתפשטת בקצב מהיר, בעוד שהמשפט מתקשה להדביק את קצב השינויים ולהעניק מענה מלא ועדכני לסיכונים הנובעים ממנה.

בישראל, הפער הזה מופיע ביתר שאת. ישראל היא מדינה מתקדמת מבחינה טכנולוגית, אבל החקיקה בה נותרה מאחור בהשוואה לתהליכים המקודמים במדינות רבות בעולם. בטרם נפנה לגיבוש פתרונות, נבחן את ההסדרים הקיימים בעולם להתמודדות עם הבעיה.

חקיקה מרכזית בהקשר זה היא ה-GDPR⁹⁷, שנועדה לחזק את ההגנה על הפרטיות במאגרי מידע ולאפשר לנושאי המידע שליטה מרבית על המידע האישי שנאסף, נשמר ונצבר עליהם. היא נחשבת לחקיקה המתקדמת והמקיפה ביותר בעולם בתחומי הגנה על פרטיות ומידע, אשר קובעת כללים אחידים להגנה על מידע של משתמשים באיחוד האירופי וגם מחוצה לו (תחולה טריטוריאלית ואקסטרטוריאלית).⁹⁸

שתי חקיקות נוספות באיחוד האירופי שראויות לציון הן חוק השירותים הדיגיטליים (Digital Services Act – DSA)⁹⁹, וחוק השווקים הדיגיטליים (Digital Markets Act – DMA)¹⁰⁰. ה-DMA נועד לצמצם את פערי הכוחות בין המשתמשים לפלטפורמות המקוונות באיחוד האירופי על-ידי הסדרת הפעילות של האחרונות. כחלק מהאסדרה, מוטלות חובות על ספקי שירותים מקוונים בצורה מדורגת, בהתאם לסוג השירות ותוך חלוקה לארבעה סוגים של ספקי שירותים: (1) ספקים של שירותי תיווך; (2) ספקים של שירותי אירוח; (3) פלטפורמות אינטרנטיות ופלטפורמות אינטרנטיות גדולות מאוד; ו-(4) מנועי חיפוש גדולים מאוד (יותר מ-45 מיליון משתמשים באירופה). עמידה בחובות מעניקה חסינות משפטית לכל אחד מספקי השירותים בנוגע לפעילות חוקית המתבצעת על-גבי הפלטפורמה שלהם. בנוסף, החקיקה מטפלת בתוכן בלתי-חוקי ויוצרת אחידות רגולטורית.

מטרת ה-DMA היא להתמודד עם בעיית הריכוזיות הגבוהה בתחום השירותים הדיגיטליים; להבטיח את קיומו של שוק דיגיטלי שוויוני והוגן; להגן על זכויות ואינטרסים של משתמשים עסקיים; ולמנוע את תלותם העמוקה של האחרונים בפלטפורמות מסחריות דומיננטיות

⁹⁷ GDPR, לעיל ה"ש 6.

⁹⁸ Chris Jay Hoofnagle et al., The European Union general data protection regulation: what it is and what it means, 28 INF. COMMUN. TECH. L. 65, 77-78 (2019); Tal Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV. 995, 1005-1009 (2016).

⁹⁹ DSA, לעיל ה"ש 7.

¹⁰⁰ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

להפצת מוצריהם או שירותיהם.¹⁰¹

כמו כן, ראוי לציין את המאמץ הרגולטורי המקיף הראשון בעולם להסדרת בינה מלאכותית – חוק הבינה המלאכותית של האיחוד האירופי (Artificial Intelligence Act - AIA), אשר אושר במרץ 2024.¹⁰² החוק מסדיר בצורה רוחבית את הטיפול בטכנולוגיות של בינה מלאכותית באמצעות יצירתה של תפיסת ניהול סיכונים, הקובעת כי ככל שהטכנולוגיה מסוכנת יותר, כך נכון להחיל עליה יותר חובות רגולטוריות. בנוסף, החוק מקים מוסדות פיקוח על התחום, הן ברמה המדינתית והן ברמת האיחוד האירופי.¹⁰³

חקיקה נוספת בתחום, שמקורה בארצות הברית, היא החוק להגנת פרטיות הצרכן בקליפורניה (The California Consumer Privacy Act – CCPA),¹⁰⁴ שנחקק בשנת 2018 ונכנס לתוקף בשנת 2020. החוק הורחב ותוקן במסגרת חוק זכויות הפרטיות של קליפורניה (The California Privacy Rights Act – CPRA),¹⁰⁵ שנחקק בשנת 2020 ונכנס לתוקף בשנת 2023. שתי חקיקות אלה מרחיבות את פריזמת ההגנה לא רק להיבטי פרטיות ומידע, אלא גם לעולמות צרכניים, תוך חיזוק זכויות המשתמשים והגברת החובות המוטלות על גופים המעבדים מידע אישי.

ה-CCPA כולל שורה של כללים והגבלות החלים על שימוש במידע אישי של תושבי קליפורניה. הוא מעניק למשתמשים זכויות בקשר לנתונים שלהם, לרבות הזכות ליידוע; הזכות לסיום התקשרות; הזכות למחיקת מידע אישי; והזכות לקבל שירות ותמחור שווה מעסק, גם אם המשתמשים בוחרים לממש את זכויות הפרטיות שמוקנות להם בהתאם לחוק.

ה-CPRA מתקן חלקים מרכזיים ב-CCPA ומעניק זכויות נוספות לצרכנים, לרבות הזכות לתקן מידע לא מדויק ולהימנע משימוש בטכנולוגיית קבלת החלטות אוטומטיות. כמו כן, הוא מטיל חובות נוספות על עסקים לגבי התכנים שיש לכלול בהודעות הפרטיות וכיצד יש לספק אותם למשתמש. בנוסף, הוא מורה על הקמת רשות פרטיות חדשה.

101 להרחבה ביחס ל-DMA וה-DMA: ד"ר אסף וינר ועדן אילי, "מודל ה-Digital Markets Act לרגולציה של תחרות והגנת צרכן בשירותים מקוונים – סקירה מתעדכנת" (מחלקת רגולציה ומדיניות, **איגוד האינטרנט הישראלי**, 01.11.2022); ד"ר אסף וינר ועדן אילי, "מודל ה-Digital Services Act לרגולציה של שירותים מקוונים – סקירה מתעדכנת" (מחלקת רגולציה ומדיניות, **איגוד האינטרנט הישראלי**, 20.2.2023).

102 AIA, לעיל ה"ש 8.

103 להסבר מקיף על ההצעה ר': טל מימרן, "הצעת הרגולציה של האיחוד האירופי בתחום הבינה המלאכותית", *חוות דעת* (מכון תכלית, יולי 2023).

104 Cal. Civ. Code §§1798.100-1798.199, 1798.105 (West 2020) (להלן: CCPA).

105 S. 746, 2021 Leg., Reg. Sess. (Cal. 2021) (להלן: CPRA).

כלל החקיקות שהוצגו מלמדות על שינוי תפיסתי בעולם המערבי ביחס להגנה על משתמשים בשירותים דיגיטליים. הן משקפות את ההכרה בחשיבות הרבה של התחום ובמגוון הדרכים שבהן ניתן לפגוע בזכויות המשתמשים בעידן הדיגיטלי, ועל כן מעניקות לנושאים אלה משקל רגולטורי משמעותי באמצעות חקיקה ייעודית ואחודה.

מעבר להיבט המבני, קרי, הצורך בדבר חקיקה אחוד ומגובש להסדרת שירותי מידע דיגיטליים, גם מבחינת התוכן, חקיקות שנחקקו בשנים האחרונות במדינות שונות בעולם מטפלות במגוון רחב של סיכונים המחייבים התייחסות גם מצד המחוקק הישראלי. סיכונים אלה כוללים, בין היתר, פרופילינג, מעקב מתמיד, העברת מידע לצדדים שלישיים, ניווד ומחיקת מידע, טיפול בתוכן בלתי חוקי והזכות לערער על החלטות אוטומטיות. עם זאת, בחינה השוואתית של החקיקות מלמדת כי כל אחת מהן מתמקדת במערך סיכונים מסוים, בהתאם למטרותיה ולהיקף תחולתה. כפי שניתן לראות בטבלה שלהלן, אף שמדובר בחקיקות מתקדמות ובעלות חשיבות רבה, אף אחת מהן אינה מספקת מענה כולל לכלל הסיכונים העומדים בפני משתמשים בשירותים דיגיטליים. פער זה עומד בבסיס המתווה המוצע במסמך זה, המבקש לאחד תחת חוק מסגרת אחד את מכלול מנגנוני ההגנה הנדרשים להתמודדות עם כלל הסיכונים המרכזיים במרחב הדיגיטלי.

הטבלה שלהלן מסכמת את אופן הטיפול של החקיקות השונות, בישראל ובעולם, בסיכונים המרכזיים שנסקרו בחלק זה.

טבלה מס' 1: סיכונים דיגיטליים והאופן בו החקיקה מטפלת בהם

חוק החוזים האחידים	חוק הגנת הצרכן	חוק הגנת הפרטיות (לאחר תיקון מס' 13)	AIA	UCTD	CPRA	CCPA	DMA	DSA	GDPR	
		✓	✓		✓	✓			✓	צמידות מטרה
		✗	✓		✓	✓	✗	✓	✓	שקיפות מוגברת
									✓	חזרה מהסכמה
							✓		✓	ניוד מידע
	✓		✓		✓	✗	✗	✓	✗	קריאות מוגבלת
		✗	✗		✓		✗		✓	עיבוד מידע
			✗		✓					פרופיילינג
			✓						✓	ערעור על החלטות אוטומטיות
		✗			✗	✗			✗	מעקב מתמיד
		✓			✓	✓	✓		✗	העברת מידע לצדדים שלישיים
					✓	✓			✓	מחיקת מידע
		✗					✓	✓		טיפול בתוכן בלתי חוקי
		✗	✓							אבטחת מידע
								✓		סעיף הסרת תוכן
✓										סיום התקשרות
✓				✓						שינוי חד צדדי של תנאי החוזה
✓								✓		סעיף חובת בורות
										סעיף ברירת דין
✓										ברירת מקום שיפוט
✓			✗		✓					הגבלת אחריות

פרק ה | סיכום ביניים: מן הסיכונים אל הפער הרגולטורי והצורך בחקיקה אחודה

מיפוי הסיכונים שנערך בפרקים הקודמים מלמד כי הפגיעות הנלוות לצריכת שירותים דיגיטליים אינן נקודתיות, אלא הינן תופעה מבנית החוצה תחומי משפט שונים ומתממשת במקביל בהיבטים של הגנת מידע, יחסי ספק-צרכן, הוגנות חוזית ונגישות. פגיעות אלו מתעצמות לנוכח יחסי כוחות א־סימטריים והיקף התקשרויות נרחב, המקשים על המשתמש הבודד להבין את תנאי ההתקשרות, לשלוט בעיבוד מידע על אודותיו ולממש את זכויותיו באופן אפקטיבי.¹⁰⁶

הבחינה של המסגרות הקיימות בישראל מצביעה על כך שהדין כולל רכיבים משמעותיים של הגנה. חוק הגנת הפרטיות ותקנות אבטחת מידע מציבים תשתית להסדרת מאגרי מידע, לאבטחתם ולחובות יידוע כלליות. דיני הצרכנות והחוזים האחידים מספקים כלים להתמודדות עם הטעיה, פערי כוחות ותנאים מקפחים.

עם זאת, ההגנות הללו מפוזרות בין מסגרות נורמטיביות נפרדות, שאינן יוצרות תפיסה רגולטורית כוללת של השירות הדיגיטלי כמערכת התקשרות אחת המבוססת על מידע. במצב זה, שאלות הנוגעות לאיסוף מידע, עיבודו והשימושים המסחריים והחברתיים הנעשים בו מוסדרות לעיתים במנותק זו מזו, באופן המקשה על מימוש זכויות ועל אכיפה אפקטיבית.

בהקשר זה, מתחדדת ההבחנה בין **הגנות טכניות**, המתמקדות באבטחת מידע ובמניעת גישה בלתי-מורשית, לבין **הגנות מהותיות**, העוסקות בלגיטימיות של עיבוד המידע, בהיקף השימוש בו ובהשלכותיו על זכויות המשתמש. בעוד שהמשפט הישראלי פיתח בשנים האחרונות מנגנונים משמעותיים בתחום ההגנה הטכנית, הסדרתם של ההיבטים המהותיים נותרה חלקית ומקוטעת, אף שדווקא הם מצויים בליבת הפגיעה בזכויות הפרט בעידן הדיגיטלי.

מנגד, ההתפתחות הרגולטורית בזירה הבינלאומית, ובפרט באיחוד האירופי, משקפת תפיסה אינטגרטיבית רחבה יותר של הגנה על משתמשים במרחב הדיגיטלי. מסגרות אלו אינן מסתפקות בהידוק אבטחת המידע, אלא מבקשות להסדיר באופן כולל את יחסי הגומלין בין משתמשים לספקי שירותים באמצעות חובות שקיפות, אחריותיות, זכויות שליטה במידע ומנגנוני פיקוח ואכיפה ייעודיים. ההשוואה הבינלאומית מדגישה כי הפער הקיים בישראל אינו רק תוכני, אלא מבני, וכי תיקונים נקודתיים בדברי חקיקה שונים מתקשים לספק מענה שלם לסיכונים חוצי התחומים שנוצרו במרחב הדיגיטלי.

OECD, The Intersection between Competition and Data Privacy, OECD Roundtables on 106 Competition Policy Papers No. 310 (7.6.2024),

מכאן נגזר הצורך באסדרה אחודה של זכויות משתמשים בשירותים דיגיטליים. חקיקה ייעודית מקיפה אחת תבטיח אחידות על פני כלל שלבי ההתקשרות, תבסס מערך הגנה קוהרנטי על זכויות אדם במרחב הדיגיטלי, ותתרום ליציבות ולוודאות משפטית באמצעות עקרונות ניטרליים מבחינה טכנולוגית, אשר ניתנים ליישום לאורך זמן.¹⁰⁷ בנוסף, ריכוז הזכויות והחובות תחת מסגרת אחת צפוי לצמצם את פערי הכוחות בין משתמשים לספקי שירותים, להקל על הפיקוח והאכיפה ולהפחית את הנטל המוטל כיום על משתמשים לנווט בין מסגרות חקיקה מפוצלות.¹⁰⁸

על יסוד מסקנות ביניים אלה, הפרק הבא עובר מן התיאור וההשוואה אל הדיון האופרטיבי. הפרק יציג את העקרונות והמאפיינים המרכזיים של חקיקה אחודה להגנה על משתמשים בשירותים דיגיטליים, כבסיס לגיבוש המלצות מדיניות קונקרטיות.

¹⁰⁷ להרחבה ביחס להצדקות לחקיקה אחודה, ראו: בר פרג'ון-מזרחי, "חוק וסדר: הצעה לאסדרה אחודה להגנה על זכויות משתמשים במרחב הדיגיטלי" **מחקרי משפט** לה (3) 1, 43-29 (2025) (להלן: פרג'ון-מזרחי "חוק וסדר").

¹⁰⁸ שם, בעמ' 34-39.

פרק ו | המלצות מדיניות: מתווה אסדרה אחודה להגנה על משתמשים בעידן הדיגיטלי

לאחר הצגת הצורך באסדרה אחודה של השירותים הדיגיטליים בישראל, הן במישור התוכני והן במישור המבני, פרק זה מציע מתווה אסדרה אפשרי. המתווה אינו נוסח הצעת חוק, אלא תשתית שיטתית לקידום הדיון החקיקתי: מיפוי הנושאים העיקריים שיש להסדיר; הצעת הסדרים אפשריים; והצגת מנגנוני יישום, פיקוח ואכיפה שיוכלו להפוך את האסדרה לאפקטיבית במציאות דיגיטלית משתנה.

בשלב זה מתמקדת ההצעה במערכת היחסים שבין משתמשים לבין פלטפורמות וספקי שירותים דיגיטליים, מתוך הנחת מוצא בדבר פערי הכוחות המובנים בין הצדדים ופגיעותם המוגברת של משתמשים במרחב הדיגיטלי. בהתאם, ההסדרים המוצעים אינם ממצים בשלב זה את המישור שבין משתמשים למדינה, או את המישור שבין משתמשים למשתמשים אחרים. מישורים אלו מצדיקים התייחסות משלימה בהמשך, אולם ניתן יהיה להסדירם על בסיס המתווה המוצע כאן.

1. עקרונות עיצוב ההסדר: גמישות, ניטרליות טכנולוגית ואיזון בין חדשנות לזכויות

חקיקה אחודה בתחום השירותים הדיגיטליים נדרשת כדי להתמודד עם אתגר היסוד: חקיקה ראשית אשר אינה מצליחה להדביק את קצב ההתפתחות הטכנולוגית. לכן, המתווה המוצע נשען על שלושה עקרונות מבניים, שמטרתם להבטיח יציבות רגולטורית, ישימות מעשית ורלוונטיות לאורך זמן.

העיקרון הראשון הוא **גמישות חקיקתית**. כדי למנוע מצב שבו החוק מתיישן במהירות או הופך למסורבל לעדכון, מוצע לעגן בחקיקה מונחים רחבים ורלוונטיים לכל סוגי הטכנולוגיות והשירותים, תוך התמקדות בפעולות ובסיכונים ולא בטכנולוגיה מסוימת. כך, למשל, מושגים כגון "הסכמה מדעת", "עיבוד מידע", "שיתוף מידע" או "פרופילינג" יוגדרו באופן שיחול גם על שירותים קיימים וגם על תצורות עתידיות. במקביל, מוצע לשלב בחוק מנגנון מוסדר של תקנות והוראות שעה, שיאפשרו התאמות נקודתיות ומהירות במצבים שבהם נדרשת תגובה רגולטורית מיידית.¹⁰⁹ סמכות זו צריכה להיות בידי גורם רגולטורי ייעודי, שיפעל בתוך מסגרת עקרונות החוק ויהיה מחויב לעדכון תקופתי בהתאם להתפתחויות.

העיקרון השני הוא **ניטרליות טכנולוגית**. המתווה אינו מבקש "לרדוף" אחרי טכנולוגיות

109 על היתרונות בשימוש בהוראות שעה כמנגנון דינמי להסדרת תחומים דינמיים, ר': איתי בר סימן טוב וגאיה הררי-הייט "שעתן היפה של הוראות-השעה?" **עיוני משפט** מא 539, 566-567, 590 (2019); Sofia Ranchordás, *Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation*, 55 JURIMETRICS 201, 219 (2015).

מתחלפות, אלא להקים מסגרת נורמטיבית קבועה להגנה על זכויות משתמשים בכל שירות מידע דיגיטלי. במובן זה, אין חשיבות מכרעת לשאלה איזו טכנולוגיה תתפתח בעתיד; העיקר הוא שהחקיקה תגן באופן עקבי על אוטונומיית המשתמש, פרטיות המידע שלו, השוויון שלו וחירויותיו, ותציב גבולות ברורים לפרקטיקות מסחריות ומידעיות הפוגעות בזכויות אלו.¹¹⁰

העיקרון השלישי הוא **איזון בין חדשנות וקידמה לבין שיקולים אתיים, חברתיים וסביבתיים**. ישראל תלויה באופן משמעותי במגזר הטכנולוגי שלה כמנוע צמיחה וכנכס אסטרטגי.¹¹¹ לפיכך, חקיקה בתחום השירותים הדיגיטליים אינה יכולה להתעלם מהחשש מפני רגולציה מרתיעה. עם זאת, חדשנות שאינה מלווה בהגנות נאותות על זכויות משתמשים עלולה להוביל לפגיעות מערכתיות, לאובדן אמון ציבורי ולנזקים חברתיים ארוכי-טווח, ובכלל זה פגיעה באוכלוסיות פגיעות והעמקת אי-השוויון. מכאן שהמתווה המוצע מאמץ גישה מבוססת סיכון: התאמת היקף החובות וחומרת הפיקוח למידת הסיכון שנוצר מהשירות, תוך הבחנה בין שירותים שונים והימנעות מהטלת חובה אחידה המייצרת עודף רגולטורי.¹¹²

במסגרת זו, מוצע גם להכיר בכך שמנגנון ההסכמה המסורתי, המבוסס על אישור מצד המשתמש לתנאי השימוש ולמדיניות הפרטיות של השירות, אינו יכול לשמש עוד עמוד השדרה של ההגנה על זכויות במרחב הדיגיטלי. ההסכמה הפורמלית אינה מבטיחה קריאה או הבנה, ולעיתים אף יוצרת אשליית הגנה.¹¹³ לכן, שינוי מוקד האסדרה הוא מרכיב מרכזי במתווה: מעבר מהטלת אחריות על המשתמשים אל הטלת חובות מהותיות על ספקי השירות, בצירוף שקיפות אפקטיבית, מנגנוני ביקורת ואכיפה, וכלים המאפשרים לרגולטור להעריך סיכון ולפעול בהתאם לו.

2. עקרונות שלב ראשון: זכויות המשתמשים ומעטפת ההגנה

נקודת המוצא של המתווה היא שהקריטריון המאחד של האסדרה צריך להיות הגנה על זכויות המשתמשים במרחב הדיגיטלי. בהקשר זה, הזכות המתפתחת והיסודית של העידן היא זכות הגישה לאינטרנט. אין מדובר רק בגישה פיזית לתשתית תקשורת, אלא

¹¹⁰ להרחבה ביחס לאימוץ עקרונות אתיים אשר שמים את זכויות האדם במרכז ביחס לתחומי הטכנולוגיה, ראו "מדיניות רגולציה ואתיקה בתחום הבינה המלאכותית בישראל", 109-102 (מסמך מדיניות של שרת החדשנות, המדע והטכנולוגיה 30.10.2022).

¹¹¹ הסקטור הטכנולוגי מהווה מנוע צמיחה מרכזי של המשק הישראלי. כך, למשל, בשנת 2023, ההייטק היה אחראי לכ-53% מכלל היצוא התעשייתי של ישראל ותרם כ-19.7% מהתוצר הלאומי. ראו: רשות החדשנות **דוח שנתי מצב ההייטק הישראלי 2024** (2024).

¹¹² כך למשל, בדומה לחקיקת ה-DPA, ניתן לקבוע כי תכנים מסוימים נחשבים בלתי-חוקיים ולמנוע מראש את פרסומם בפלטפורמות.

¹¹³ ראו, פרג'ון-מזרחי "חוק וסדר", לעיל ה"ש 107, בעמ' 20.

גם בגישה מהותית: גישה לשירותים דיגיטליים בסביבה שבה זכויות האדם של המשתמש אינן נשחקות כחלק בלתי-נמנע מהשימוש, המאוזנת עם הצורך לאפשר פעילות כלכלית, חדשנות ותחרות בשוק הדיגיטלי, ובשים לב למגבלות כוחה של ישראל כשחקן רגולטורי בזירה גלובלית.

פגיעה עקבית באוטונומיה, בפרטיות, בשוויון ובזכויות צרכניות וחוזיות בעת השימוש עלולה לפגוע בפועל בזכות הגישה עצמה, שכן היא הופכת את השתתפותו של הפרט במרחב הדיגיטלי לתלויה בהסכמה לתנאים הפוגעים באופן מהותי בזכויותיו. בהקשר זה, מטרת האסדרה אינה למנוע סיכונים באופן מוחלט, אלא לצמצם פגיעות בזכויות לרמה מידתית והוגנת, באופן המאזן בין הגנה על המשתמש לבין היתכנות פעילותם של ספקי השירות.

בהתאם, מוצע לעגן במתווה ארבע חטיבות של זכויות ולגזור מכל אחת מהן מעטפת הגנה המשלבת בין זכויות פעולה למשתמש, חובות מהותיות לספק השירות ומנגנוני בקרה.

2.1 אוטונומיה והסכמה מדעת

אוטונומיה במרחב הדיגיטלי אינה מסתכמת בחופש ללחוץ "אני מאשר/ת". היא דורשת שליטה אמיתית של המשתמש בהקשרים שבהם נעשה שימוש במידע הנאסף עליו ובהחלטות הנגזרות ממנו. לכן מוצע להגדיר בחוק "הסכמה מדעת" כהסכמה ספציפית, חופשית, מודעת וחד-משמעית; לעגן זכות חזרה מהסכמה; לחזק את עקרון צמידות המטרה, באופן שיאסור מטרות עמומות ומופשטות של איסוף מידע; ולהרחיב את חובת השקיפות של ספק השירות כך שתכלול, בין היתר, סוגי מידע, מקורות איסוף, מטרות שימוש והעברה, משכי אחסון, אפשרויות עיבוד ומנגנוני מימוש זכויות. לצד זאת, מוצע לעגן זכות נידוד מידע ככלי המחזק תחרות ומקטין תלות של המשתמש בפלטפורמה ספציפית, וכן להבטיח קריאות ונגישות של הסכמים והודעות באמצעות דרישות צורניות ומהותיות וניסוח בהיר במספר שפות מרכזיות בישראל.

עם זאת, יש להדגיש כי הנגשה אינה מספיקה: רבים מהמשתמשים אינם קוראים הסכמים גם כשהם נגישים, ולעיתים אינם משנים את החלטתם גם לאחר קריאה. מכאן נובעת ההצדקה להסטת ההסכמה ממרכז הכובד של ההגנה, והשלמתה בכלים רגולטוריים נוספים.¹¹⁴

114 להרחבה שם, בעמ' 45.

2.2 פרטיות מידע והגנת מידע

הזכות לפרטיות במרחב הדיגיטלי מחייבת התייחסות מפורשת לפרטיות מידע: הזכות להגן על מידע אישי מפני עיבוד שאינו כדון, מעקב, העברה לצדדים שלישיים ופעולות נוספות החורגות ממטרת האיסוף, תוך דרישות אבטחה אפקטיביות. לפיכך, מוצע להסדיר באופן רחב מהו "עיבוד מידע": להגדיר בסיסים משפטיים לעיבוד, לחייב שקיפות, להחמיר ביחס למידע רגיש ולהטיל חובות ביקורת תקופתיות על היקפי עיבוד וסיכונים. בנוסף, מוצע להסדיר סוגיות של מידע מזוהה לעומת מידע הניתן לזיהוי, אנונימיזציה ומבחן סבירות, וכן צבירה והצלבת מידע כמוקד סיכון הדורש הסכמה מפורשת והודעה ברורה.

במקביל, מוצע להסדיר באופן קונקרטי מהו "מעקב מקוון": להגבילו למטרה צרה ומידתית, לחייב יידוע בדבר מעקב גם מחוץ לשימוש הישיר בשירות, ולהעניק אפשרויות ניהול והימנעות ככל שהן אינן פוגעות בליבת השירות. ביחס להעברת מידע לצדדים שלישיים, מוצע לחייב יידוע והסכמה, פירוט זהותם של הצדדים השלישיים ומטרותיהם, והגדרה רחבה של "שיתוף" מידע. לבסוף, מוצע לעגן ולהרחיב זכויות לעיון, תיקון ומחיקה, ובפרט זכות למחיקה במצבים שבהם הסתיימה ההתקשרות או שהמידע אינו נחוץ עוד או שעובד שלא כדון, לצד חובת הקמה של מנגנונים נגישים וברורים למימוש זכויות.¹¹⁵

2.3 שוויון, אי-אפליה והגנה על אוכלוסיות פגיעות

במרחב הדיגיטלי, שוויון נפגע לא רק בזמן מתן שירותים אלא לעיתים כבר בשלב יצירת פרופיל משתמש, בקטגוריזציה ובהפעלת כלים אוטומטיים. לכן, מוצע לתרגם את עקרון השוויון לכלל קונקרטי של איסור הפליה בשל מימוש זכויות לפי החוק; להסדיר "פרופיילינג" באופן רחב; ולהעניק זכות להסבר אנושי וזכות ערעור ביחס להחלטות משמעותיות שנעשו באמצעים אוטומטיים, בצירוף דרישות להפחתת הטיות ומעורבות אנושית נאותה.

בתוך כך, מוצע לייחד הגנה מוגברת לקטינים ולאנשים עם מוגבלויות. ביחס לקטינים, ההצעה כוללת הגבלות על איסוף ושימוש במידע, דרישות שקיפות מותאמות גיל, מגבלות על העברת מידע לצדדים שלישיים, והסדר מדורג של הסכמה הורית בהתאם לרגישות המידע, לצד יחידה ייעודית וחינוכית בתחום. ביחס לנגישות, מוצע לאמץ סטנדרטים של הנגשה לאתרים, אפליקציות והסכמים, תוך אפשרות לפטורים מסוימים לעסקים קטנים בהתאם ליכולת טכנולוגית ותקציבית.¹¹⁶

115 שם, בעמ' 49-50.

116 שם, בעמ' 54-56.

2.4 זכויות צרכניות וחוזיות בשירותים דיגיטליים

מאחר שתנאי שימוש ומדיניות פרטיות הם בפועל חוזים דיגיטליים אחידים, מוצע להגביל מראש אפשרות לשילוב תנאים מקפחים: לתחם הסרת תוכן ולהגדיר קריטריונים, להסדיר סיום התקשרות, להגביל שינוי חד-צדדי של תנאים (ובייחוד תנאים בתחום המידע), לצמצם תניות הגבלת אחריות בנושאים מהותיים, ולהבטיח נגישות לערכאות באמצעות איסור בורות כפויה והגבלות על ברירת דין ומקום שיפוט, תוך התאמה לפערים ביחסי הכוחות ולשוק המקומי.

בנוסף, מוצע לקבוע מנגנוני תרופה אפקטיביים: פיצוי ללא הוכחת נזק והרחבת האפשרות לתובענות ייצוגיות בעילות מידעיות דיגיטליות, כדרך ליצירת הרתעה והשלמת אכיפה ציבורית.¹¹⁷ יובהר כי מנגנונים אלה נועדו להשלים את ההסדר הקיים בדין ולהרחיב אותו. הדבר נכון במיוחד בכל האמור בהצעת חוק תובענות ייצוגיות (תיקון מס' 16), אשר מתמקדת בעיקר בפגיעות פרטיות הנובעות מדליפות מידע וניהול מאגרי מידע בניגוד לחוק, אך אינה נותנת מענה כולל להפרות מידעיות וחוזיות רחבות המאפיינות את פעילותם השוטפת של שירותים דיגיטליים.¹¹⁸

3. שלב שני: שיטת פעולה רגולטורית – כלי גילוי נאות מבוסס סיכון

לאחר בניית מעטפת הזכויות, השלב השני מציע כלי פעולה רגולטורי שנועד להפוך את ההגנה על זכויות לשימה ואפקטיבית, תוך התאמתה לשוק הישראלי. נקודת המוצא היא כפולה: מצד אחד, השוק בישראל קטן יחסית במפת השירותים הדיגיטליים, והטלת חובות מחמירות מדי עלולה להוביל להרתעה רגולטורית; מצד שני, מודל המבוסס על הסכמות פורמליות אינו מגן בפועל על משתמשים.

מסיבה זו, מוצע כלי גילוי נאות של ספק השירות. הכלי מבוסס סיכון, יפעל במקביל להסכמים ולא במקומם, וישמש הן את המשתמשים והן את הרגולטור. הכלי כולל שלושה רכיבים משלימים:

הרכיב הראשון הוא שאלון גילוי נאות ממוקד סיכונים, שימלא על-ידי קצין הציות של ספק השירות ויכלול בעיקר שאלות סגורות. השאלון יכסה סיכונים מרכזיים למידע ולזכויות ויאפשר תיאור מובנה של מדיניות החברה באופן קצר, השוואתי וידידותי יותר למשתמש מהסכמים ארוכים. לצד זאת, השאלון יכלול הפניות לסעיפים הרלוונטיים בהסכמים, כך שמשמש המעוניין להעמיק יוכל לעשות כן באופן ממוקד.

117 שם, בעמ' 57-59.

118 הצעת חוק תובענות ייצוגיות (תיקון מס' 16), התשפ"ד-2024.

הרכיב השני הוא מדד כמותני להגנת מידע משתמש, המבוסס על השאלון. המדד נועד להתמודד עם מציאות שבה חלק ניכר מהמשתמשים לא יקראו טקסט, גם אם יונגש. המדד יפיק ציון בארבע קטגוריות – הודעה אפקטיבית, הגנה על מידע, אבטחת מידע והגנת הצרכן בסביבה הדיגיטלית – ויעניק לספק ציון משוקלל. הציון יופק על-ידי גורם בלתי-תלוי מטעם הרשות הרגולטורית ויוצג באתר ובאפליקציה, כדי ליצור איתות ברור למשתמשים בדבר רמת ההגנה על פרטיותם ואיכות ניהול המידע בשירות, והוא יהווה תמריץ מתמשך לשיפור מדיניות.

הרכיב השלישי הוא מנגנון לזיהוי סתירות אצל ספק השירות, שמטרתו להתמודד עם הפער בין הצהרות לפרקטיקה. המנגנון יאתר מקרים של אי-התאמה בין התשובות לשאלון לבין תנאי השימוש ומדיניות הפרטיות, ויעביר את הממצאים לרגולטור כסימני אזהרה לצורך מיקוד מאמצי אכיפה. אין מדובר בהכרעה אוטומטית על קיומה של הפרה פוטנציאלית, אלא בכלי תיעדוף ובקרה שמחזק את אפקטיביות האכיפה ומייצר תמריץ לשקיפות.

שלושת הרכיבים הללו מונחים על-ידי תפיסת יסוד מרכזית: **התאמת היקף החובות לרמת הסיכון**. דירוג הסיכון ייקבע על בסיס המדד הכמותני להגנת המידע של המשתמש ויופק על-ידי גורם בלתי-תלוי מטעם הרשות הרגולטורית. זאת, בהתאם לקריטריונים אחידים, שקופים ומבוססי סיכון, המשקפים בין היתר את מאפייני השירות, סוג המידע המעובד, היקף השימוש והחשיפה של המשתמשים. ככל שהשירות ידורג בסיכון נמוך יותר, כך ניתן יהיה להטיל עליו פחות חובות רגולטוריות; ככל שהסיכון גבוה, יוגברו דרישות הביקורת, הדיווח והפיקוח. בדרך זו נשמר איזון בין הגנה על זכויות לבין מניעת עומס רגולטורי אחיד, שאינו מבחין בין סוגי שירותים.¹¹⁹

4. שלב שלישי: מערך אסדרה ייעודי

הצלחת המתווה תלויה ביכולת פיקוח ואכיפה. כיום, קיימת בישראל תמונת מצב של ביזור רגולטורי עם חפיפות חלקיות: רשות לפרטיות והגנת מידע, רשות להגנת הצרכן, מערך הסייבר הלאומי וגופים נוספים, לצד צוותים בין-משרדיים אד-הוקיים. מודל זה יוצר קשיי תיאום, קיבעון נורמטיבי ולעיתים גם חוסר בהירות כלפי השוק.

מסיבה זו, מוצע להקים מערך אסדרה ייעודי שיהיה אמון על תחום השירותים הדיגיטליים כמכלול, תוך חלוקת סמכויות ותחומי חפיפה מוסדרים עם הרשויות הקיימות. המערך ירכז מומחיות, ייצור קוהרנטיות במדיניות ויאפשר אכיפה יעילה של מעטפת הזכויות,

119 ראו: פרג'ון-מזרחי "חוק וסדר", לעיל ה"ש 107, בעמ' 60-62.

כלי הגילוי הנאות והמדרג מבוסס הסיכון. תפקידיו יכללו פיקוח על שקיפות אפקטיבית ונגישות, קביעת ציונים במדד, ביצוע ביקורות ובירורים, פיתוח תשתית מחקר וידע, קידום סטנדרטיזציה, וכן הפעלתה של יחידת הגנה ייעודית לאוכלוסיות פגיעות ובפרט קטינים.

ביחס לסמכויות האכיפה, נייר זה מציע לאמץ תפיסה מרחיבה, בדומה למגמות שהתעצמו בשנים האחרונות בדין הישראלי (ובפרט לאחר הרחבת כלים מנהליים בתחום הפרטיות): עיצומים כספיים מדורגים, סמכויות חקירה וביקורת, צווים מתקנים וחובות דיווח. שילוב סמכויות זה נדרש כדי שההגנות לא יישארו הצהרתיות.¹²⁰

120 שם, בעמ' 63-65.

פרק ז | המלצות אופרטיביות ליישום המתווה

כדי להפוך את המתווה למסגרת ישימה, ההמלצות שלהלן מציעות מסלול הדרגתי המשלב חקיקה ראשית, תקנות, פיילוטים וכלי אכיפה, תוך שמירה על ניטרליות טכנולוגית, גמישות רגולטורית ואיזון בין חדשנות להגנה על זכויות.

1. קידום חקיקה מסגרתית קצרה ומבנית

מומלץ לקדם חקיקה ראשית שתשמש "חוק מסגרת" לשירותים דיגיטליים. החוק יגדיר זכויות ליבה, יטיל חובות מהותיות על ספקי שירות ויעגן מנגנון תקנות דינמי. חקיקה זו צריכה להימנע מתיאור טכנולוגיות מסוימות ולהתמקד בפעולות ובסיכונים: איסוף, עיבוד, מעקב, פרופילינג, שיתוף מידע, שינוי חד-צדדי של תנאים והגבלות גישה.

2. עיגון מפורש של זכויות משתמשים וזכויות פעולה

מומלץ שהחקיקה תכלול סט זכויות פעולה ברור למשתמש – קרי, זכויות הניתנות למימוש אקטיבי על-ידי המשתמש ביחס למידע האישי שלו ולהסכמי השימוש – אותן ניתן לממש בפועל: חזרה מהסכמה, נידוד מידע, עיון בו, תיקונו ומחיקתו, זכות להסבר אנושי ביחס להחלטות אוטומטיות משמעותיות והגנות ייחודיות לקטנים ולאנשים עם מוגבלויות. זכויות אלה צריכות להיות מלוות בדרישות פרוצדורליות לספק השירות, כך שהן לא יישארו הצהרות בלבד.¹²¹

3. שינוי מוקד האסדרה – מהסכמה פורמלית לחובות מהותיות

מומלץ להגדיר בחוק כי הסכמת המשתמש אינה מהווה "כרטיס פטור" מאחריות עבור הספק. במקביל לשימור מושג ה"הסכמה מדעת", יש לעגן סט חובות מהותיות שאינן תלויות הקלקה: צמידות מטרה מחוזקת, שקיפות אפקטיבית, הגבלת מעקב, בקורות פנימיות, סטנדרטים לאבטחה וניהול סיכונים. כך מתחזק הרציונל המרכזי של המתווה: הפחתת הנטל המוטל על המשתמשים בקבלת החלטות ובהבנת הסיכונים, והעברת האחריות אל ספקי השירות.¹²²

4. קביעת "גילוי נאות מבוסס סיכון" כחובה רגולטורית משלימה להסכמים

מומלץ לחייב כל ספק שירות להציג באתר ובאפליקציה שלו, באופן נגיש וידידותי, כלי גילוי נאות מבוסס סיכון לצד תנאי השימוש ומדיניות הפרטיות. הכלי חייב להיות מוצג

121 שם, בעמ' 53.
122 שם, בעמ' 60-65.

בהתאם לתבנית אחידה ולסט קריטריונים קבועים שייקבעו על-ידי הרשות הרגולטורית, כדי לאפשר השוואה בין שירותים ולהפוך את השקיפות לאפקטיבית, ולא רק פורמלית.

5. פיתוח שאלון גילוי נאות אחיד והטמעתו

מומלץ כי הרשות הרגולטורית תגבש שאלון גילוי נאות במתכונת סגורה (שאלון רב-ברירה), המתעדכן מעת לעת בתקנות. כל ספקי השירות יחויבו למלא שאלון בסיסי, ושירותים בעלי סיכון מוגבר או היקפי שימוש נרחבים ימלאו גם שאלון מורחב, בהתאם למדדים שייקבעו בתקנות.

6. הקמת מדד כמותי להגנה על מידע של משתמשים והצגתו בממשק השירות

מומלץ לקבוע כי ציון המדד יופק על-ידי גורם בלתי-תלוי מטעם הרשות הרגולטורית, ולא על-ידי ספק השירות, כדי לחזק את אמון הציבור ולצמצם תמריצים לאופטימיזציה הצהרתית. המדד צריך להיות מוצג בארבע קטגוריות קבועות, עם ציון משוקלל בסופו, ולהתעדכן אחת לשנה או בעת שינוי מדיניות משמעותי.

7. שילוב מנגנון לזיהוי סתירות כמכשיר תיעדוף אכיפה

מומלץ לאמץ מנגנון לאיתור מקרים של אי-התאמה בין הצהרות ספק השירות (השאלון) לבין ההסכמים והמדיניות בפועל. הכלי ישמש לתיעדוף ובקרה, ולא כהכרעה אוטומטית בדבר קיומה של הפרה. ממצאי הסתירות יוזנו למערכת פיקוח שתאפשר לרשות לזהות מוקדי סיכון ולכוון ביקורות.

8. גיבוש מדרג חובות מבוסס סיכון

מומלץ לקבוע בתקנות מדרג רגולטורי בהתאם לשני ממדים: (1) היקף השימוש – מספר משתמשים, היקף המידע, מספר מורשי גישה; ו-(2) רמת הסיכון – ציון במדד והקשרים רגישים כגון קטינים, מידע רגיש, החלטות אוטומטיות משמעותיות ועוד. ככל שהסיכון גבוה יותר, יוגברו חובות ביקורת, דיווח ואימות; ככל שהסיכון נמוך, תישמר הקלה יחסית כדי למנוע הרתעה רגולטורית.

9. הקמת מערך אסדרה ייעודי או רשות מתכללת בעלת סמכויות אפקטיביות

מומלץ להקים רשות ייעודית לשירותים דיגיטליים, או לכל הפחות גוף מתכלל עצמאי בעל סמכויות פיקוח ואכיפה, שיפעל בתיאום עם הרשויות הקיימות. לרשות ייעודית יתרון מרכזי: היא מחברת בין פרטיות, צרכנות, נגישות והיבטי אבטחת מידע תחת קריטריון מאחד של זכויות משתמשים.

10. קביעת סט כלי אכיפה מדורג, הכולל עיצומים, צווים מתקנים וביקורות חובה

מומלץ להעניק לרשות סמכויות להטיל עיצומים כספיים מדורגים, לדרוש תיקון ליקויים, לערוך ביקורות חובה תקופתיות לשירותים בעלי סיכון מוגבר, וכן לחקירה ולבירור. מנגנון האכיפה צריך לשלב בין ענישה להכוונה: תמריצים לשיפור מדיניות והפחתת סיכון, לצד סנקציות על אי-ציות.

11. יצירת מנגנוני תרופה אזרחיים אפקטיביים למשתמשים

מומלץ לעגן בחוק מנגנון פיצוי ללא הוכחת נזק בגין הפרת זכויות משתמשים מרכזיות, וכן להסדיר עילות מותאמות לתובענות ייצוגיות בתחום מידע דיגיטלי בהקשרי משתמש-פלטפורמה. רכיב זה משלים את האכיפה הציבורית ומייצר הרתעה.

12. יישום מדורג: פיילוט, הרחבה והסדרה מלאה

מומלץ ליישם את המתווה בשלושה שלבים עיקריים:

שלב ראשון: פיילוט לשאלון ולמדד בקרב שירותים גדולים ובינוניים, ובתחומים רגישים (קטינים, בריאות, פיננסים, השמה).

שלב שני: הרחבה לכלל השירותים, עם התאמות לעסקים קטנים ובינוניים.

שלב שלישי: ייצוב המסגרת באמצעות עדכון תקנות תקופתי ומנגנוני ידע ומחקר בתוך הרשות.

פרק ח | סוף דבר

נייר מדיניות זה מצביע על פער הולך ומעמיק בין האופן שבו שירותים דיגיטליים מעצבים כיום את חיי הפרט, החברה, הפוליטיקה והכלכלה, לבין המסגרת המשפטית הישראלית שנועדה להגן על המשתמשים במרחב זה. בעוד שהטכנולוגיה מתפתחת בקצב מואץ, חוצה תחומים ומטשטשת גבולות מסורתיים בין פרטיות, צרכנות, חוזים, נגישות ואבטחת מידע, המשפט הישראלי ממשיך לפעול באמצעות אסדרה מפוצלת, תגובתית ולעיתים אנכרוניסטית. פער זה אינו טכני בלבד, אלא מבני ונורמטיבי, והוא מוביל לפגיעה שיטתית בזכויות המשתמשים, להעמקת הפערים ביחסי הכוחות בינם לבין ספקי השירותים הדיגיטליים, ולהעמסת נטל רגולטורי בלתי-יעיל על כתפי הציבור ועל השוק.

השפעותיו של פער זה אינן מתמצות בפגיעה בפרטיות או באוטונומיה של המשתמשים. הן מקרינות גם על מעמדה של ישראל בזירה הבינלאומית כמדינה המחויבת להגנה על זכויות אדם בעידן הדיגיטלי, על יכולתה להשתלב במשטרים רגולטוריים מתקדמים ועל יחסי המסחר והאמון עם שווקים גלובליים. בעידן שבו מידע חוצה גבולות, ומדיניות ההגנת עליו הפכה לשיקול מרכזי בהתקשרויות בינלאומיות, היעדר מסגרת רגולטורית עדכנית, קוהרנטית ומובנת עלול להציב את ישראל בעמדת נחיתות, הן מבחינה ערכית והן מבחינה כלכלית.

כנגד מציאות זו, נייר מדיניות זה מציע שינוי תפיסתי ומבני: מעבר מאסדרה מקוטעת, המבוססת בעיקר על הסכמה פורמלית של משתמשים – לחקיקת מסגרת אחודה, שמעמידה במרכזה את ההגנה על זכויות המשתמשים במרחב הדיגיטלי. המתווה להצעת חוק הגנה על זכויות משתמשים במרחב הדיגיטלי, מבקש לאחד, לפשט ולהמשיג מחדש את ההגנות הקיימות, לסגור פערים מהותיים ולהתאים את הדין למציאות הטכנולוגית המשתנה. ריכוז ההסדרים תחת קורת גג אחת יאפשר לטפל באופן קוהרנטי בסיכונים חוצי-תחומים, להגביר את הוודאות המשפטית ולהפחית את הנטל המוטל כיום על משתמשים שנדרשים לנווט בין מקורות נורמטיביים שונים כדי להבין את זכויותיהם.

המתווה המוצע מדגיש כי הגנה אפקטיבית על זכויות משתמשים אינה יכולה להישען עוד על מודל של "קרא והסכם", אלא מחייבת להעביר את מרכז הכובד הרגולטורי אל ספקי השירותים עצמם. שילוב של זכויות מהותיות, כלי גילוי נאות מבוסס סיכון ומערך אסדרה מתכלל, מבקש ליצור איזון חדש: כזה שמצמצם את הפער ביחסי הכוחות, מייצר שקיפות מדידה וברורה ומאפשר פיקוח ואכיפה יעילים מבלי לפגוע בחדשנות הטכנולוגית. גישה זו מתיישבת עם מגמות רגולטוריות עולמיות ומאפשרת לישראל להשתלב בהן, תוך התאמה למאפייניה הייחודיים כשוק קטן אך מתקדם טכנולוגית.

יישום מוצלח של ההמלצות המוצעות צפוי להניב שורה של תועלות מצטברות. עבור המשתמשים, הוא עשוי להבטיח הגנה ממשית על זכויותיהם, להפחית את נטל האחריות המוטל עליהם ולאפשר קבלת החלטות מושכלת במרחב הדיגיטלי. עבור השוק, הוא עשוי

לייצר סטנדרטים ברורים, להפחית חיכוך רגולטורי ולעודד תחרות הוגנת, המבוססת גם על איכות ההגנה על המשתמשים. עבור הרגולטור והמדינה, הוא עשוי לשפר את יכולת האכיפה, לחזק את אמון הציבור ולבסס את מעמדה של ישראל כמדינה המשלבת קידמה טכנולוגית עם מחויבות עמוקה לזכויות אדם.

בסופו של דבר, השאלה העומדת בפני מקבלי ההחלטות איננה אם להסדיר את תחום השירותים הדיגיטליים, אלא כיצד לעשות זאת באופן שישקף את ערכי היסוד של החברה הישראלית בעידן דיגיטלי. נייר מדיניות זה מבקש להציע מענה כולל, ישיר וערכי לאתגר זה, וגם לפתוח פתח לדיון חקיקתי רחב שיציב את האדם, ולא רק את הטכנולוגיה, במרכז המרחב הדיגיטלי.