התלות הביטחונית בתשתיות דיגיטליות מסחריות

מאי הר־שי[1]

המעבר מרכש ביטחוני לתלות מתמשכת אינו מבטל את הריבונות המדינתית, אך מציב לה גבולות חדשים, חלקם טכניים וחלקם מהותיים. עבור ישראל האתגר חד במיוחד. ככל שהיכולות המבצעיות והמודיעיניות נשענות על תשתיות שאינן בשליטת המדינה, גדלה חשיבותה של אסדרה מוקדמת והתייחסות משפטית לתלות המתמשכת. המטרה אינה עצמאות טכנולוגית מלאה, אלא ניהול מודע ומבוקר של התלות

מבוא

בספטמבר 2025, בשעה שכוחות צה"ל נלחמים וחטופים ישראלים עדיין שבויים ברצועת עזה, הודיעה חברת מייקרוסופט על החלטתה להשבית מערך שירותים שסיפקה ליחידה 8200. ההחלטה התקבלה לאחר בדיקת טענות שעלו בעיתון הגארדיאן הבריטי (The Guardian), ולפיהן שירותי הענן והבינה המלאכותית של החברה שימשו לאחסון ולעיבוד מידע שהופק ממעקב אחר שיחות טלפון של פלסטינים בעזה ובגדה המערבית.[2] בהודעתה הרשמית הדגישה החברה שגם לקוחות מדינתיים כפופים לתנאי השימוש המסחריים, והוסיפה כי ההשבתה באה בעקבות הפרתם.[3]

פרשת מייקרוסופט אינה רק אירוע נקודתי ביחסי חברה מסחרית ומדינה בעת מלחמה, אלא ביטוי לשינוי מוסדי רחב יותר בעידן הבינה המלאכותית. ההנחה בעת רכש ביטחוני היא שמרגע מכירת הטכנולוגיה השליטה בשאלה מתי ואיך להפעיל אותה עוברת במלואה למדינה. לדוגמה אם מדינה רכשה מטוס קרב מחברה מסחרית, ייתכן שהאחרונה תוסיף להעניק שירותי תחזוקה נקודתיים, אך אין בידיה להשפיע באילו תנאים אפשר לצאת לתקיפה במדינת אויב. בעידן הבינה המלאכותית התמונה שונה. התשתיות נשארות מסחריות גם לאחר הרכישה, למדינה הרוכשת אין שליטה מלאה עליהן ולחברות המפעילות נותרת שליטה מתמשכת בתנאי ההפעלה, ובכלל זה היכולת להפסיק את הפעלתן מרחוק או לצמצם את הכיסוי הגיאוגרפי, בהתאם לתנאי השימוש שהן קובעות. רכש ביטחוני מסוג זה יוצר אפוא תלות מתמשכת של המדינה בספק.[4]

חברות הטכנולוגיה הגלובליות - הביג־טק (Big Tech) - פועלות מעבר לגבולותיה של מדינה אחת, ויחסיהן עם מדינות מתנהלים לעיתים כיחסים בין שחקנים בעלי כוח דומה.[5] כוחן הרב בעידן הנוכחי אינו נובע רק מהמוצרים הספציפיים שהן מוכרות, אלא מהעובדה שהן שולטות בחלק מסביבת הפעולה והתשתיות שהמדינה פועלת בהן, גם במישור הצבאי.[6] בהקשר זה המונח "ריבונות

---

1 עו"ד מאי הר־שי היא עמיתת מחקר במרכז הנשיא מאיר שמגר למשפט דיגיטלי וחדשנות, עמיתה במרכז צבי מיתר ללימודי משפט מתקדמים ודוקטורנטית בפקולטה למשפטים ע"ש בוכמן באוניברסיטת תל אביב. מחקרה מתמקד ברגולציה של בינה מלאכותית.

2 Harry Davies & Yuval Abraham, *'A million calls an hour': Israel relying on Microsoft cloud for expansive surveillance of Palestinians*, The Guardian, Aug. 6, 2025, https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.

3 Brad Smith, *Update on Ongoing Microsoft Review*, Microsoft On the Issues, Sept. 25, 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/; Microsoft, *Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza*, Microsoft On the Issues, May 15, 2025, updated Aug. 15, 2025, https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/; Harry Davies & Yuval Abraham, Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians, The Guardian (Sept. 25, 2025), https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.

4 על תלות גוברת של גופי ביטחון בספקי ענן מסחריים ראו למשל, Vera Bergengruen, *Ukraine's "Secret Weapon" Against Russia Is Clearview AI*, Time, 2023, https://time.com/6334176/ukraine-clearview-ai-russia/; Mahmoud Javadi, *Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare: Insights from Ukraine, Israel and Taiwan*, 47 Cont. Sec. Policy 469 (2026), https://doi.org/10.1080/13523260.2025.2593247.

5 על השינוי במעמדן של חברות הטכנולוגיה ראו Hannah Bloch-Wehba, *How Tech Took Over* , Texas A&M University School of Law Legal Studies Research Paper, 2026, http://dx.doi.org/10.2139/ssrn.6378220; Udi Sommer, Eviatar Matania & Nir Hassid, *The Rise of Companies in the Cyber Era and the Pursuant Shift in National Security*, 75 Pol. Sci. 140, 143 (2023); Eviatar Matania & Udi Sommer, *Tech Titans, Cyber Commons and the War in Ukraine: An Incipient Shift in International Relations*, 39 Int'l Rel. 586, 590 (2025); Wil van der Aalst, Oliver Hinz & Christof Weinhardt, Big Digital Platforms, 61 Bus. & Info. Sys. Eng'g 645 (2019).

6 Andrea Coveri, Claudio Cozza & Dario Guarascio, *Blurring Boundaries: An Analysis of the Digital Platforms–Military Nexus*, Rev. Pol. Econ., Sept. 3, 2024, https://doi.org/10.1080/09538259.2024.2395832; Andrea Coveri, Claudio Cozza & Dario Guarascio, *Big Tech and the US Digital-Military-Industrial Complex*, 60 Intereconomics 81 (2025), https://doi.org/10.2478/ie-2025-0017; Mark A. Lemley, Matthew Wansley & David McGowan, *Cooping Disruption*, Cardozo Legal Stud. Res. Paper No. 2024-24, Stan. L. & Econ. Olin Working Paper No. 589, at 37-38, Feb. 1, 2024, https://ssrn.com/abstract=4713845; Fernando van der Vlist, Anne Helmond & Fabian Ferrari, *Big AI: Cloud Infrastructure Dependence and the Industrialisation of Artificial Intelligence*, 11 Big Data & Soc'y, at 3 (2024), https://doi.org/10.1177/20539517241232630; Swati Srivastava & Justin Bullock, *AI, Global Governance, and Digital Sovereignty* 2, 7, 10 (arXiv:2410.17481, Oct. 2024); Daniel Mügge, *EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?*, 31 J. Eur. Pub. Pol'y 2200, 2201 (2024).

דיגיטלית" מתאר את יכולתה של מדינה לשלוט בתשתיות, בטכנולוגיות ובנתונים שהיא נסמכת עליהם ולפעול בהם עצמאית, והמונח "תלות דיגיטלית" מתאר מצב שבו יכולות לאומיות חיוניות מותנות בתשתיות שבבעלות פרטית, ולעיתים זרה.[7] השאלות שמעוררת תלות כזו הן דיפלומטיות ואסטרטגיות, לא פחות משהן משפטיות. הן נוגעות לכללי המשחק בזירה שבה פועלים שחקנים פרטיים חוצי מדינות, ולאופן שבו מדינה מנהלת את יחסיה עם תאגיד שכוחו התשתיתי עולה לעיתים על שלה. הדיון במאמר זה מתמקד ברובד המשפטי, בדגש על הדין הרלוונטי לרכש ביטחוני, שבו התלות מקבלת צורה מוחשית בחוזים ובמסמכי מדיניות.

מרכש ביטחוני מסורתי לתלות מתמשכת בעידן הענן והבינה המלאכותית

מקדמת דנא נשענו מערכות ביטחון על תעשייה פרטית ועל ספקים אזרחיים, החל מיַצרני נשק ותשתיות תקשורת וכלה במומחי תוכנה ומערכות מידע. גם המעבר של טכנולוגיות מן העולם הצבאי אל העולם האזרחי אינה תופעה חדשה. במהלך המאה ה־20 התפתחו יחסי גומלין הדוקים בין חדשנות צבאית לחדשנות אזרחית. לעיתים פותחה הטכנולוגיה במערכת הביטחון ולאחר מכן עברה לשוק האזרחי; במקרים אחרים טכנולוגיה שפותחה למטרות מסחריות אומצה בידי הצבא והותאמה לצרכיו.[8]

במבט ראשון, אפשר לראות את השימוש הצבאי בענן ובבינה מלאכותית כהמשך טבעי של מגמה מוכרת. המדינה מזהה יכולת אזרחית מתקדמת, רוכשת אותה, מתאימה אותה לצרכיה ומטמיעה אותה במערכת הביטחון. במובן זה, מדובר לכאורה בהתפתחות של הרכש הביטחוני, שלב נוסף בהסתמכות הגוברת של מערכות ביטחון בטכנולוגיות שמקורן בשוק האזרחי. עם זאת, מבט כזה מחמיץ את השינוי המוסדי העמוק המתרחש בעידן זה. כאשר המדינה רוכשת כלי נשק או מערכות מודיעין המותקנות במערכותיה הפנימיות, השליטה בשאלה מתי ואיך תופעל הטכנולוגיה עוברת לידיה, לפחות לאחר הרכישה. לעומת זאת, כאשר יכולת מודיעינית נשענת על ענן מסחרי או על תשתית או מודל בינה מלאכותית המתעדכנים ומופעלים מרחוק, הממשק בין המדינה לספק אינו מסתיים ברגע הרכישה, והספק ממשיך להחזיק ביכולת לשלוט בתנאי ההפעלה הלכה למעשה.[9]

השליטה הזו שמורה לשיקול דעתן של החברות ומתאפשרת, בין היתר, באמצעות מסמכי המדיניות שלהן. לצד ההסכם המסחרי, חברות ענן ובינה מלאכותית קובעות מדיניות שימוש מקובלת, מדיניות בטיחות, כללי שימוש במערכות בינה מלאכותית, מנגנוני ניטור ואכיפה.[10] מסמכי המדיניות השונים משאירים בידי החברות מנעד כלים רחב שנתונים להן, משך כל זמן השימוש בטכנולוגיה או התשתית, במקרה של שימוש אסור.[11] למשל בתנאים מסוימים שקובעות החברות, הן משאירות לעצמן את האפשרות להשבית או להגביל את השירות. הכלים יכולים להיות טכניים, כמו עדכון של מודל, שינוי בממשק הגישה, שינוי בהרשאות או התאמה של מדיניות אבטחה; כלים אחרים עשויים להיות תנאים חוזיים הכוללים התניות מסחריות או תפעוליות, למשל דרישה לקיום תהליך בדיקה נוסף, הגבלת סוגי שימוש מסוימים והערמת קשיים בהעברת מידע לספק חלופי.[12] כל צעד כזה עשוי להיראות טכני או חסר חשיבות כשהוא נבחן בפני עצמו, אך כאשר השירות משמש כחלק מסביבת פעולה ביטחונית - הוא יכול להשפיע על היכולת לשמר רציפות מבצעית ובכך לסכל פעילות מבצעית או מודיעינית חיונית להצלת חיי אדם.

פרשת מייקרוסופט ממחישה זאת היטב. בהודעת החברה ממאי 2025, שעודכנה באוגוסט אותה שנה, תיארה את יחסיה עם משרד

---

7 המונח "ריבונות" בהקשר של ריבונות דיגיטלית נתפס כצורה של עצמאות, שליטה ואוטונומיה על תשתיות דיגיטליות, טכנולוגיות ונתונים. בשונה מריבונות במובנה המסורתי, שעניינה סמכות משפטית בלעדית בתוך טריטוריה, ריבונות דיגיטלית מתארת יכולת מעשית: לקבוע כללים לסביבה הדיגיטלית, להבטיח גישה רציפה לתשתיות ולנתונים חיוניים, ולפעול בהם בלא תלות ברצונו של גורם חיצוני. הספרות מדגישה שהמונח משמש שחקנים שונים במשמעויות שונות, ושהוא מתאר לרוב שאיפה יותר מאשר מצב קיים. להרחבה, ראו למשל, Toupin Sophie & Couture Stephane, *The to Referring When Mean 'Sovereignty' of Notion the Does What Digital?*, New Media & Soc'y 2305 (2019), https://doi.org/10.1177/1461444819865984.

8 על התפתחות המעבר מ־Spin-off ל־Spin-on ועל אימוץ טכנולוגיות אזרחיות לצרכים צבאיים ראו John A. Alic et al., Beyond Spinoff: Military and Commercial Technologies in a Changing World (Harv. Bus. Sch. Press 1992); David C. Mowery & Timothy Simcoe, *Is the Internet a U.S. Invention? An Economic and Technological History of Computer Networking*, 31 Res. Pol'y 1369, 1370–1372 (2002); Jay Stowsky, *Secrets to Shield or Share? New Dilemmas for Military R&D Policy in the Digital Age*, 33 Res. Pol'y 257, 265–268 (2004).

9 על תלות המדינה בחברות מסחריות לצורך רכיבי מערכת מרכזיים של בינה מלאכותית צבאית, לרבות נתונים, כוח מחשוב, תשתיות ועדכונים שוטפים, ראו: Jeppe T. Jacobsen & Tobias Liebetrau, *Infrastructuring Public-Private Relations: Big Tech, the Ukraine War and Implications to Security Governance*, 32 European Journal of International Relations 183 (2026), https://doi.org/10.1177/13540661251370265; Rupert Barrett-Taylor & Matthew Ford, *Eroding Sovereignty in the Age of "War as a Service"*, Opinio Juris, Nov. 3, 2025, https://opiniojuris.org/2025/11/03/eroding-sovereignty-in-the-age-of-war-as-a-service/.

10 Elena Chachko, *National Security by Platform*, 25 Stan. Tech. L. Rev. 55, 70 (2021).

11 May Har-Shai, The *Commercial Veto over Military AI* (unpublished manuscript).

12 בחירות עיצוב טכנולוגיות, ובכללן קוד, ברירות מחדל וארכיטקטורת הרשאות, הן אינן תוצר טכני בלבד, אלא עשויות לגלם ערכים ולשקף הכרעות נורמטיביות. ראו למשל, Mary Flanagan, Daniel C. Howe & Helen Nissenbaum, *Embodying Values in Technology: Theory and Practice*, in Information Technology and Moral Philosophy 322 (Jeroen van den Hoven & John Weckert eds., 2008).

הביטחון כקשר מסחרי רגיל הכפוף לתנאי השירות, למדיניות השימוש המקובל ולקוד ההתנהגות של שירותי הבינה המלאכותית הארגוניים. החברה ציינה כי מסמכים אלה אוסרים, בין היתר, שימוש בשירותי הענן והבינה המלאכותית שלה באופן הפוגע ביחידים או בארגונים או בניגוד לדין. בהודעה מאוחרת יותר מספטמבר 2025 מסרה כי בעקבות בדיקה שערכה מצאה ראיות התומכות בחלקים מדיווחי הגארדיאן, ולפיהן שירותי הענן והבינה המלאכותית של החברה שימשו לאחסון ולעיבוד מידע שהופק ממעקב אחר שיחות טלפון של פלסטינים בעזה ובגדה המערבית, וכי החליטה להפסיק ולהשבית מנויים ושירותים מסוימים, ובהם שירותי אחסון בענן ושירותי בינה מלאכותית.[13]

פרשת מייקרוסופט אינה מקרה בודד, ופרשות נוספות, שונות ממנה באופיין, התעוררו בזירות אחרות. במלחמה בין רוסיה ואוקראינה (2022–היום) הפך סטארלינק (Starlink), שירות האינטרנט הלווייני של ספייס־אקס (SpaceX), לרכיב חיוני בתקשורת הצבאית והאזרחית האוקראינית; בהמשך התעוררה מחלוקת על גבולות השימוש בשירות לצרכים התקפיים, ובפרט על השאלה אם ספק פרטי רשאי לאפשר שימוש בתשתית מסחרית גם לפעולה צבאית שהוא מבקש להימנע ממנה.[14] בארצות הברית התעוררה שאלה דומה מזווית אחרת, כאשר חברת אנת'רופיק (Anthropic), המפתחת את מודל הבינה המלאכותית קלוד (Claude), הסתייגה מהסרת מגבלות בטיחות על שימושים צבאיים ומודיעיניים במודל שלה.[15]

שלוש הדוגמאות מבהירות שאין מדובר בסוג אחד של שליטה מתמשכת או באתגר ישראלי בלבד. מייקרוסופט אכפה מדיניות שימוש כלפי לקוח מדינתי קיים; ספייס־אקס סירבה לאפשר שימוש מדינתי התקפי בתשתית שבבעלותה; ואנת'רופיק עמדה על מגבלות בטיחות שקבעה למודל שלה, גם עבור לקוח שהוא מדינה.[16] לכל אחת מן העמדות נדרש מענה משפטי ומדיני אחר, אך משמעותן המשותפת היא ששליטה או עצמאות פעולה שבעבר הייתה מסורה למדינה בלבד, תחת מגבלות הדין המקומי והבין־לאומי, מצויה עתה גם בידי מי שמחזיק בתשתית, במודל או בתנאי הגישה אליהם.

הדין החל כיום על רכש ביטחוני, הן בישראל הן במקומות אחרים בעולם, ממשיך להניח כי עם חתימת החוזה עוברת השליטה בטכנולוגיה לידי המדינה.[17] הנחה זו ניכרת, בין היתר, בשתי משפחות ההסדרים המרכזיות בתחום - דיני המכרזים ודיני הייצוא הביטחוני. הראשונים, המסדירים את הדרך שבה המדינה רוכשת, עוסקים בעיקר בשלב כריתת העסקה - בבחירת הספק ובתנאי ההתקשרות.[18] דיני הפיקוח על הייצוא הביטחוני, המסדירים את העברת הטכנולוגיה מן הכיוון המגביל, קובעים מה מותר למכור, למי ובאילו תנאים, ואף הם מניחים כי משאושרה העסקה השימוש בטכנולוגיה נתון בידי הרוכש.[19] שתי משפחות הדינים גם יחד אינן מתייחסות לשליטה המתמשכת של החברות בתנאי הפעלת המערכת לאחר ההתקשרות.[20] התוצאה היא שהמסמכים המעצבים בפועל את תנאי ההפעלה אינם רק החוזה שנכרת בעקבות המכרז, אלא בעיקר מסמכי המדיניות של החברות.

---

13 ראו הודעת מייקרוסופט, לעיל ה"ש 2; Microsoft, Summary of 2025 External Investigation and Follow Up.

14 על השימוש בסטארלינק באוקראינה ראו Amritha Jayanti, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose*, 9 Belfer Center for Science and International Affairs (2023); Kaushik Ray & William Selvamurthy, *Starlink's Role in Ukraine*, 17 Journal of Defence Studies 25 (2023); Josh Pennington & Sean Lyngaas, *Starlink in Use on 'All Front Lines,' Ukraine Spy Chief Says, but Wasn't Active 'for Time' over Crimea*, CNN, Sept. 10, 2023, https://www.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html.

15 על המחלוקת בין Anthropic לבין הפנטגון ראו Brianna Rosen, Expert Comment: The Pentagon-Anthropic Dispute Reflects Governance Failures - with Consequences That Extend Well beyond Washington, University of Oxford, Mar. 6, 2026, https://www.ox.ac.uk/news/2026-03-06-expert-comment-pentagon-anthropic-dispute-reflects-governance-failures-consequences; Amrith Ramkumar, Trump Administration Shuns Anthropic, Embraces OpenAI in Clash Over Guardrails, The Wall Street Journal, Feb. 27, 2026, https://www.wsj.com/tech/ai/trump-will-end-government-use-of-anthropics-ai-models-ff3550d9; Anthropic, Statement on the Comments from Secretary of War Pete Hegseth, Anthropic, Feb. 27, 2026, https://www.anthropic.com/news/statement-comments-secretary-war.

16 הסיבון שחברות יגבילו את הגישה הישראלית מוכר גם במסמכי מדיניות רשמיים. התכנית הלאומית להאצת בינה מלאכותית, בעמ' 78, מציינת, בהפניה מפורשת למלחמת חרבות ברזל, סיכון ממשי שחברות "ישקלו לשלול או לצמצם את הגישה הישראלית למודלי היסוד", ומציעה לזהות ולצמצם תלות במודלים חיצוניים בתחומים קריטיים כדי להבטיח רציפות תפקודית. ראו המטה הלאומי לבינה מלאכותית, "התכנית הלאומית להאצת בינה מלאכותית וביסוס מובילות גלובלית ביוזמי פעולה (אוגוסט, 2026): https://govextra.gov.il/livedai/en/home/?utm_source=go.gov.il&utm_medium=referral

17 לדיון מורחב בנושא מידת ההתאמה של הרגולציה הקיימת להעברת טכנולוגיות בעידן הבינה המלאכותית ראו Har-Shai, The Commercial Veto over Military AI, לעיל ה"ש 9.

18 ראו למשל דפנה ברק-ארז **משפט מינהלי** כרך ג 24-25 (2013).

19 חוק הפיקוח על יצוא ביטחוני, התשס"ז-2007. תכליתו המוצהרת של החוק, המנוסחת בסעיף 1, היא הסדרת הפיקוח על יצוא ציוד ביטחוני מטעמי ביטחון לאומי ויחסי חוץ; על תכלית החוק והרקע לחקיקתו ראו למשל הילה גולדשמיד "סייבר התקפי – בין יצוא בטחוני לייבוא אביפתי" פורום עיוני משפט (תגוביות משפט) מו (20.1.2022).

20 על סיום תפקידם של דיני המכרזים בשלב כריתת החוזה, שממנו ואילך חלים על ההתקשרות דיני החוזים המינהליים, ראו ברק-ארז, לעיל ה"ש 15, בעמ' 155; ראו גם יצחק זמיר **הסמכות המינהלית** כרך א 310 (מהדורה שנייה מורחבת, 2010), המבחין במפורש בין השלב הטרום-חוזי, שבו הגוף הציבורי כפוף בעיקר לכללי המשפט הציבורי, לבין שלב ביצוע החוזה, שבו הוא כפוף בעיקר לכללי המשפט הפרטי.

מסמכי המדיניות כמשילות פרטית

מסמכי המדיניות של החברות מנוסחים בידי החברות וחלים על כלל לקוחותיהן, ובכללם גופי צבא וביטחון. בספרות המשפטית מקובל לכנות אסדרה מסוג זה משילות פרטית (ordering private) - יצירת כללים, פרשנותם ואכיפתם בידי גורם פרטי, מכוח ההסכמה החוזית והשליטה בטכנולוגיה, ולא מכוח הסמכה שלטונית.[21] חלק מן המסמכים מחייבים משפטית כחלק מן ההתקשרות; אחרים, כמו עקרונות לבינה מלאכותית אחראית או מסגרות בטיחות, אינם מנוסחים כחוזה אך מכוונים בפועל את התנהגות הלקוחות, משום שהחברה שולטת בגישה לשירות ובידיה לאכוף אותם באמצעים טכניים וחוזיים.

כאשר תנאי שימוש אוסרים סוג של מעקב, מגבילים שימושי בינה מלאכותית או מאפשרים השעיית שירות, הם מתפקדים כשכבה נורמטיבית נוספת המעצבת את מרחב הפעולה הביטחוני.[22] במובן זה, תנאי השימוש אינם רק מנגנון ציות פנימי של החברה, אלא גם כזה הקובע מי רשאי להשתמש בשירות, לאילו מטרות, באילו תנאים ומה יקרה כאשר החברה סבורה שהשימוש חורג מן המותר.[23] אצל לקוח מסחרי רגיל אפשר להבין זאת בעיקר כעניין חוזי; אצל גוף ביטחוני המשמעות משתנה. אותם תנאים עשויים לקבוע בפועל אם פעולה מודיעינית תוכל להימשך, אם תידרש בחינה מחודשת, ואם תהיה לחברה אפשרות להפעיל סנקציה תשתיתית בעת משבר. בכך, אף שאינם חוק, הם משפיעים במישרין על יכולת הפעלת כוח מדינתי־צבאי.[24]

אפשר לטעון שלריסון הכוח המדינתי על־ידי החברות יש יתרונות וחסרונות.[25] מצד אחד, מסמכי המדיניות יכולים לשמש שכבת הגנה מפני שימוש לרעה בטכנולוגיות מעקב, בינה מלאכותית וענן. חברות גלובליות חשופות לביקורת ציבורית, לנורמות בין־לאומיות של זכויות אדם וללחצים מעובדים ומשקיעים, ובמקרים מסוימים עשויות לזהות סיכונים שהמדינה אינה רוצה או מסוגלת לבחון בזמן אמת. מצד אחר, אין זה מנגנון דמוקרטי רגיל. חברה פרטית אינה כפופה לאותם מנגנוני אחריותיות כמו מדינה, אינה מאזנת בהכרח בין כלל האינטרסים הציבוריים הרלוונטיים ועשויה לפעול מתוך שיקולי מוניטין, לחץ שוק, יחסי ציבור או חשש משפטי במדינות אחרות. היא גם עשויה להחיל מדיניות אחידה על מצבים שונים מאוד, בלי להבין לעומק את ההקשר הביטחוני המקומי.[26]

עם זאת, מסמכי המדיניות משתנים ומתעדכנים תדיר, החברות משאירות לעצמן מרחב פעולה ושיקול דעת רחב הן בפרשנות השימושים האסורים הן באופן האכיפה והפעלת הסנקציות.[27] כך, האיסור שהושבתה נשענה עליו בפרשת מייקרוסופט - מעקב המוני אחר אזרחים - מופיע בהצהרות הפומביות של החברה, אך לא אותר כלשונו בגרסאות הציבוריות של מסמכי המדיניות שהחברה הפנתה אליהם. אף מסמך אינו מגדיר מיהו "אזרח" לעניין האיסור, וההכרעה אם המידע שנאסף היה מידע על אזרחים נותרה בידי החברה לבדה.[28] הכרעות אלה, ועימן סמכויות ההשעיה, הסיום והגבלת הגישה, נתונות כולן בידי צד אחד. זוהי תמצית הבעייתיות של המשילות הפרטית בהקשר הביטחוני: השאלה אם שימוש מדינתי עומד בכללים החלים עליו מוכרעת על פי מסמכים שצד אחד ניסח, מפרש ורשאי לשנות, בלא הליך שבו המדינה יכולה להשיג על ההכרעה.[29]

---

21 להרחבה על משילות פרטית ראו למשל Niva Elkin-Koren & Karni A. Chagal-Feferkorn, *Lex AI: Revisiting Private Ordering by Design*, 36 Berkeley Tech. L.J. 915, 916–917 (2021); Niva Elkin-Koren, *What Contracts Cannot Do: The Limits of Private Ordering in Facilitating a Creative Commons*, 74 Fordham L. Rev. 375, 376 (2005); Luca Belli & Jamila Venturini, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation*, 5 (Internet Pol'y Rev. 1, 4–5 2016).

22 הכוונה היא לשכבה נורמטיבית נוספת מעבר לדינים המוברים המסדירים מרחב זה, הדין המקומי והמשפט הבינלאומי, ובראשם דיני השימוש בכוח (law of force), המבחינים בין שימוש מותר לאסור בכוח, ודיני הלחימה (law of armed conflict), המסדירים את ההתנהלות בלחימה עצמה. ראו למשל David Kennedy, Of War and Law 39 (Princeton Univ. Press 2006).

23 על תפקיד מסמכי המדיניות בהסדרה פרטית באופן כללי ראו, למשל: Belli & Venturini, לעיל ה"ש 19.

24 על תנאי שימוש ומדיניות שימוש תאגידית בגורם המגביל שימושים צבאיים ומודיעיניים ראו Rosen, לעיל ה"ש 18; Carly Page & Ingrid Lunden, *Anthropic, OpenAI, and the New Rules of Defence AI*, Resilience Media, Mar. 3, 2026, https://resiliencemedia.co/anthropic-openai-and-the-new-rules-of-defence-ai/.

25 ניתן לטעון שגם לעצם החיכוך בין הגופים יש ערך בפני עצמו. ראו להרחבה: Niva Elkin-Koren & Maayan Perel, *Democratic Friction in Speech Governance by AI*, in Handbook of Critical Studies of Artificial Intelligence 643, 643–55 (Simon Lindgren ed., Edward Elgar 2023), https://doi.org/10.4337/9781803928562.00066.

26 Har-Shai, Governing Military Access to Commercial AI (unpublished manuscript).

27 ראו דיון מורחב בנושא ב- Har-Shai, Governing Military Access to Commercial AI, לעיל ה"ש 26; טענה דומה עולה גם בהקשרי הסרת נתונים ע"י פלטפורמות, ראו מאמרה של Chachko, לעיל ה"ש 9, בעמ' 91-90.

28 האיסור מופיע בהודעות החברה, ראו Microsoft, Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza, Microsoft On the Issues (May 15, 2025, updated Aug. 15, 2025); Brad Smith, Update on Ongoing Microsoft Review, Microsoft On the Issues (Sept. 25, 2025). להרחבה על אודות המחקר שבחן את האיסור בלשונו בגרסאות הציבוריות של מסמכי המדיניות, על היעדר הגדרה ל"אזרח" ועל כך שהבדיקה נסמכה על נתוני העסק של החברה בלבד, ללא גישה לתוכן הלקוחות, ראו May Har-Shai, Governing Military Access to Commercial AI, לעיל ה"ש 26.

29 Har-Shai, Governing Military Access to Commercial AI, לעיל ה"ש 26.

מקרה המבחן של ישראל

ישראל נהנית מקרבה אסטרטגית וטכנולוגית לארצות הברית ומנוכחות עמוקה של חברות טכנולוגיה בין־לאומיות בשוק המקומי, אך אינה שולטת במרכזי הכוח התאגידיים של חברות הענן הגדולות.[30] ההחלטות הקריטיות, למשל בנוגע לתנאי שימוש, מדיניות זכויות אדם, סיכוני מוניטין, תגובות ללחץ ציבורי או שינויים במדיניות גלובלית, מתקבלות מחוץ לישראל. לעיתים הן מתקבלות לפי דין זר, על בסיס ייעוץ משפטי זר ובהתחשב בשיקולים פוליטיים וציבוריים שאינם חופפים את תפיסת הביטחון הישראלית.[31]

עבור מעצמה טכנולוגית כמו ארצות הברית, הדיון בתלות בביג־טק מתנהל במגרש מורכב אך פנימי יותר. רבות מחברות הענן והבינה המלאכותית המרכזיות הן בבעלות אמריקנית, והדין, הכלכלה ושיקולי הביטחון האמריקניים משפיעים על סביבת פעולתן. גם שם היחסים בין המדינה לחברות אינם פשוטים, אך לממשל מנופי השפעה משמעותיים דרך רכש פדרלי, רגולציה, חקיקה, ביקורת קונגרס, תמריצים, ולעיתים אף יכולת להפעיל סמכויות ביטחון לאומי כלפי חברות מקומיות, כמו במקרה של אנת'רופיק.[32]

בין שני הקצוות האלה ניצבות מדינות אירופה. כוחן הרגולטורי רב, אך תלותן בספקיות הענן האמריקניות דומה, והדיון הציבורי שם עוסק במה שמכונה "מתג כיבוי" (kill switch) אמריקני, כלומר בחשש שוושינגטון תורה לספקיות להשבית שירותים שממשלות ומוסדות באירופה נשענים עליהם. החשש התחדד לאחר שב־2025 נותקו, על רקע סנקציות אמריקניות, חשבונות מייקרוסופט של בעלי תפקידים בבית הדין הפלילי הבין־לאומי, ובהם התובע הראשי. בתגובה התחייבה החברה כלפי ממשלות אירופה והנציבות האירופית, בין היתר בתנייה חוזית שלפיה תתנגד בערכאות לצו שיורה לה להשבית שירותי ענן באירופה, ואולם גם מענה זה הוא התחייבות של החברה.[33]

לישראל אין את מנופי ההשפעה הפנימיים של ארצות הברית או את המשקל הרגולטורי של האיחוד האירופי, ולכן ניהול הממשק מול החברות תלוי אצלה, יותר מבשתי הזירות האלה, בעיצוב ההתקשרות. בניהול ממשק זה יש לה ולחברות הפרטיות אינטרסים שונים. מעבר להטמעת יכולות צבאיות מתקדמות המפותחות כיום בשוק הפרטי, למדינה עניין ברציפות מבצעית, בעצמאות שיקול הדעת הביטחוני ובהימנעות ממצב שבו גורם פרטי זר מחזיק למעשה ביכולת להטיל וטו על פעולה מודיעינית או מבצעית. לחברות הפרטיות לעומת זאת, עניין בהגנה על מוניטין, בצמצום חשיפה משפטית בכמה תחומי שיפוט, בעמידה במחויבויות שלקחה על עצמה בתחום זכויות האדם ובהתמודדות עם לחצים מצד עובדים, משקיעים וציבור. אינטרסים אלה אינם בהכרח מנוגדים, אך אינם חופפים ולרוב מתנגשים דווקא במצבי הקצה שהשאלה המשפטית מתחדדת בהם.

מעבר לכך, מדובר גם ביחסי כוח. עמדת המדינה אינה נשענת על זכות משפטית מופשטת בלבד, אלא על מנופי לחץ מעשיים, ובראשם קיומן של חלופות. כאשר אין למדינה חלופה ממשית לספק מסוים, מנגנונים פרוצדורליים אינם יכולים לפצות על היעדר מנוף לחץ מבני - וזו אחת הסיבות שהאסדרה צריכה לכלול גם יתירות ולא הליך בלבד. עם זאת, אין להסיק מעובדה זו שעל ישראל לשאוף לעצמאות טכנולוגית מלאה. קשה להניח שמדינה קטנה תוכל לשחזר עצמאית את מכלול תשתיות הענן, מרכזי הנתונים, מודלי הבסיס וכוח המחשוב שבידי החברות הגדולות, וספק אם הדבר אף רצוי. לטעמי, אין לזהות ריבונות דיגיטלית בעידן הענן עם אוטרקיה טכנולוגית, אלא ביכולת לנהל את התלות באופן מודע ומבוקר.[34]

---

30 עמית אשכנזי "שוברת שוק: זירת הסחר הבינלאומי והשפעתה על הביטחון בסייבר" **הזירה** (29.2.2024), https://www.arenajournal.org.il/single-post/ashkenazi-trade-arena-cybersecurity

31 על התלות של מדינות בתשתיות הנשלטות בידי חברות גלובליות ראו Freddy Dezeure et al., *Digital Sovereignty Is Impossible Without Big Tech*, 48 Atlantisch Perspectief 30 (2024), https://www.jstor.org/stable/48761751; Ala Ali Almahameed et al., *Sovereignty, Surveillance, and the Cloud: Geopolitical and Ethical Issues of Global Cloud Computing*, in Ethical and Social Impacts of Information and Communication Technology 109, 81 (Ignacio Alvarez, Mario Arias-Oliva, Adrian Horia Dediu & Nuno Silva eds., 2026). כן ראו Coveri , לעיל ה"ש 4, בעמ' 82, 88; ; Henry Farrell & Abraham Newman, *Underground Empire: How America Weaponized the World* Economy (2023).

32 ראו בדוגמה לעניין זה את הכרעת בית המשפט הפדרלי לערעורים במחוז קולומביה בעתירות שהגישה אנת'רופיק במסגרת הסכסוך המתוקשר בינה לבין הפנטגון. בית המשפט דחה את עתירות החברה ואישר בדעת רוב את החלטת משרד ההגנה האמריקאי (משרד המלחמה כיום), להכריז על קלוד, מודל השפה של אנת'רופיק, כסיכון לשרשרת האספקה מכוח ה-Federal Acquisition Supply Chain Security Act (41 U.S.C. § 4713). ראו Anthropic PBC v. U.S. Dep't of War, No. 26-1049 (D.C. Cir. Sept. 25, 2026)).

33 Charles Pahud de Mortanges, *Avoiding the Kill Switch: Europe's Digital Sovereignty Dilemma* (ORBi, Univ. of Liège, 2026), https://orbi.uliege.be/handle/2268/347210; לחשיפתן של מערכות ההגנה האירופיות לסיכון זה ראו למשל Future of Technology Institute, *Cloud Defence: An Exposed European Flank* (2026), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cdn.prod.website-files.com/6a61d19f83fdca4fd1dd7efb/6a732bbe698401458f882b6e_CLOUD_REPORT.pdf; להתחייבויות מייקרוסופט כלפי ממשלות אירופה ראו Brad Smith, *Microsoft Announces New European Digital Commitments, Microsoft On the Issues* (Apr. 30, 2025), https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/.

34 התכנית הלאומית להאצת בינה מלאכותית, לעיל ה"ש 14, בעמ' 57, מתארת מודל ביניים שבו מדינות אינן מסתמכות עוד באופן מלא על השוק הגלובלי, אך גם אינן שואפות לאוטרקיה מלאה.

כיוונים ראשוניים לאסדרה

התקשרויות ביטחוניות עם ספקי ענן ובינה מלאכותית צריכות לכלול הסדרים ברורים יותר מאלה המקובלים בהתקשרות מסחרית או ממשלתית רגילה. ראשית, בכל הנוגע להפסקת שירות ולשינוי תנאים, על ההתקשרות לקבוע מראש אם וכיצד רשאי הספק לצמצם או להשבית את השירות, ובכלל זה חובת הודעה מוקדמת, פרק זמן להיערכות והליך מוסכם, במקום להותיר את ההשבתה לשיקול דעתו החד־צדדי של הספק. שנית, בכל הנוגע להעברת מידע, לאפשרויות גיבוי ולמעבר בין ספקים, על ההתקשרות לצמצם את התלות בספק יחיד ואת עלות המעבר ממנו, שכן הקושי להעביר מידע לתשתית חלופית הוא מקור לשליטה מתמשכת. שלישית, נדרש סיווג מראש של שימושים רגישים, כדי שהצדדים יידעו אילו שימושים כרוכים בחשיבות מבצעית או מודיעינית מיוחדת לפני שיתעורר משבר. כאשר מדובר בשירות בעל חשיבות מבצעית או מודיעינית, אין די בתנאי שירות כלליים שנוסחו עבור לקוחות מסחריים רגילים; נדרשים מנגנוני התראה, בירור וערעור המתאימים לחשיבות התשתית ולרגישות השימוש.

מאחר שמסמכי המדיניות משתנים תדיר ומותירים לחברות שיקול דעת רחב, פוחתת הוודאות שהמדינה יכולה להסתמך עליה בתכנון פעולתה. אי הוודאות הזו היא לב האתגר, ולכן עיצוב מנגנונים פרוצדורליים מתאימים יפחית את השרירותיות של שני הצדדים - את הסיכון שחברה תשבית שירות קריטי ללא הליך מתאים, ואת הסיכון שמדינה תנצל את מנוף ההתקשרות כדי לעקוף מגבלות משפטיות וציבוריות. מנגנונים כאלה אינם צריכים להכריע מראש במחלוקת המהותית בין המדינה לחברה. תפקידם צנוע יותר אך חשוב - לקבוע מהו ההליך שבו מתקבלת החלטה כאשר מתעורר חשד לשימוש אסור בשירות בעל חשיבות ביטחונית. בהקשר זה, ההליך חשוב לא פחות מהתוצאה מכיוון שהוא יכול להבחין בין מצבים שבהם נדרשת השעיה מיידית בשל חשש חמור וקרוב, ובין מצבים שאפשר לברר בהם את הטענות בלי לפגוע ברציפות השירות באחת. ככל שמנגנון קבלת ההחלטה ייקבע מראש על ידי שני הצדדים, תתגבר הוודאות וההחלטה לא תיוותר לשיקול דעתו המלא והיחיד של הספק.

הליך כזה נשען על כמה רכיבים המשלימים זה את זה. למשל יש לקבוע מראש ערוץ בירור מוסכם לחשדות שעולות אצל החברות על שימוש אסור של גורמי קשר מוסמכים בין הצבא לחברות הפרטיות.[35] נוסף על כך, יש לקבוע לוחות זמנים קצרים לתגובה של המדינה על החשדות הללו ולתת אפשרות להציג מידע מסווג או רגיש במסגרת חשאית. לבירור של החברות יתלווה מדרג של תגובות אפשריות ומוסכמות, שכן לא כל חשד מחייב השעיה מלאה, ולעיתים אפשר להסתפק בהגבלה חלקית, בחסימת שימוש מסוים, בדרישת תיקון או במעבר הדרגתי לתשתית חלופית. לצד אלה נדרש מנגנון תיעוד וביקורת של החברות, המאפשר לבחון בדיעבד אם ההחלטה התקבלה על בסיס מידע מספיק, בהליך הוגן ובאופן מידתי ביחס לסיכון.

כיוון נוסף הוא הכרה בשירותי ענן וכוח מחשוב מסוימים כתשתית קריטית לביטחון הלאומי.[36] הכרה כזו אינה צריכה לחול על כל שירות דיגיטלי, אלא רק על אלה שהפסקתם עלולה לפגוע ממשית ביכולת מודיעינית או מבצעית חיונית. על השירותים הללו יש להחיל דרישות מיוחדות של ניהול סיכונים, גיבוי, המשכיות, אבטחת מידע ובחינת חלופות.[37] עם זאת, המפתח הוא מדרגיות. אם כל טכנולוגיה תוגדר כתשתית ביטחונית קריטית - ההסדרה תהפוך רחבה מדי ובלתי ישימה. סיווג מוקדם יאפשר להצדיק מנגנונים חזקים יותר בלי להעמיס על כלל השוק. הסדרה כזו אינה שואלת אפוא אם הענן המסחרי מסוכן או חיוני, אלא מתמקדת בשאלות קונקרטיות יותר כמו איזה שימוש נעשה בו, באיזו שכבה של המערכת, ומה תהיה משמעות הגבלת השירות בעת משבר?

המשותף לכיוונים האלה הוא ההכרה שבעידן הענן והבינה המלאכותית אין די בהתמקדות בטכנולוגיה ובעסקת הרכש, ויש להוסיף עליהן התייחסות גם לממשק המתמשך שבו נחלקת השליטה בין המדינה לספק, ובתוך כך למסמכי המדיניות. הכיוונים והצעות ההסדרה לא נועדו להכריע במחלוקת בין השניים, אלא ליצור מסלול מוסדי שבו כוחה הציבורי של המדינה וכוחו התשתיתי של הספק מופעלים באופן שקוף, מדורג וביקורתי יותר.

---

35 התוכנית הלאומית להאצת בינה מלאכותית וביסוס מובילות גלובלית שפורסמה באוגוסט 2026 מכירה בחשיבות שיתוף הפעולה עם חברות הביג טק ואף מציעה מענה מוגבל ליצירתו בדמות "שגרירות תאגידית". לפי התכנית, רעיון השגרירות התאגידית נועד ליצור קשר עמוק ומחייב בין חברות הביג טק והאקוסיסטם הישראלי. עם זאת, פתרון זה מוגבן בעיקר בהקשרי חדשנות, ולא עוסק, לפחות באופן מוצהר, בשאלת התלות הביטחונית בחברות אלו. ראו התכנית הלאומית להאצת בינה מלאכותית, לעיל ה"ש 14.

36 תשתיות קריטיות או חיוניות (Critical Infrastructures) הן תשתיות ששיבוש תפקודן עלול להוביל לנזקים כלכליים, חברתיים וסביבתיים משמעותיים, ולעיתים אף להסב פגיעות בנפש. למותר לציין כי הגדרה זו של תשתיות חיוניות אינה ממצה, שכן בנסיבות שונות ניתן להגדיר תשתיות חיוניות באופן שונה, בתלות, בין היתר, בתפיסה תרבותית. להרחבה ראו למשל, Massimo Ficco et al., *Simulation platform for cyber-security & vulnerability analysis of critical infrastructures*, 22 J. Computational Sci. 179, 179–86 (2017); אלדר הבר וטל ז'רסקי "דרכי ההגנה על תשתיות חיוניות במרחב הסייבר בישראל" **משפט וממשל** יח 99 (2017).

37 על הצורך להגן על תשתיות ענן וכוח מחשוב כעל תשתיות קריטיות ועל פגיעותן בעת עימות, ראו Jacobsen & Liebetrau, לעיל ה"ש 28, בעמ' 183-208; Aziz Z. Huq, *The Geopolitics of Digital Regulation*, 92 University of Chicago Law Review 833 (2025), https://chicagounbound.uchicago.edu/uclrev/vol92/iss3/4/.

הכיוונים האלה אף משתלבים בתוכנית הלאומית להאצת בינה מלאכותית מאוגוסט 2026, שהכירה בסיכון של צמצום הגישה הישראלית לתשתיות ולמודלים. התוכנית מציעה מענה בשכבת התשתית, ובכלל זה ענן ריבוני לרציפות בעת משבר, הרחבה ניכרת של כוח המחשוב הלאומי וצמצום התלות במודלים חיצוניים בתחומים קריטיים. ההצעות שלהלן משלימות מענה זה בשכבה נוספת - מאחר שחלק ניכר מן היכולות יוסיף להישען על תשתיות מסחריות גם לאחר יישום התכנית, נדרש לצד בנייתן של חלופות לאומיות גם עיצוב משפטי של הממשק המתמשך מול הספק.[38]

סיכום

המעבר מרכש ביטחוני לתלות מתמשכת אינו מבטל את הריבונות המדינתית, אך מציב לה גבולות חדשים, חלקם טכניים וחלקם מהותיים. המדינה ממשיכה לאשר פעולות צבאיות עצמאית, להפעיל סמכויות ולאסוף מודיעין, אך עושה זאת בסביבה שבה גורם פרטי עשוי להחזיק בשליטה מעשית על תנאי הגישה לתשתית החיונית לפעולה. שליטה זו מופעלת, בין היתר, באמצעות מסמכי המדיניות של החברות, המשמשים שכבה נורמטיבית נוספת המגבילה את מרחב הפעולה הביטחוני.

עבור ישראל - מדינה קטנה בעלת צרכים מודיעיניים וביטחוניים רחבים - האתגר חד במיוחד. היא אינה יכולה להרשות לעצמה להתעלם מן היכולות שמציעות חברות הענן והבינה המלאכותית הגלובליות, אך גם אינה יכולה להתייחס אליהן כאל ספקי רכש רגילים בלבד. ככל שהיכולות המבצעיות והמודיעיניות נשענות על תשתיות שאינן בשליטת המדינה, גדלה חשיבותה של אסדרה מוקדמת והתייחסות משפטית לתלות המתמשכת. המטרה אינה עצמאות טכנולוגית מלאה, שספק אם היא בת־השגה או רצויה, אלא ניהול מודע ומבוקר של התלות. ניהול כזה מתחיל בהכרה במעמדם של מסמכי המדיניות ברכש הביטחוני. משאלה הפכו מנספח מסחרי להסכם לגורם המעצב את תנאי ההפעלה של יכולות חיוניות - נדרשת להם גם התייחסות משפטית, כסוגיה מרכזית ולא כעניין טכני.

רשימת מקורות

מקורות בעברית

1. הוראת תכ"ם 16.12.1 "פרויקט נימבוס – הנחיות כלליות בנוגע לרכש שירותי ענן ציבורי" (2024)
2. תקנות חובת המכרזים, התשנ"ג-1993
3. חוק הפיקוח על יצוא ביטחוני, התשס"ז-2007
4. עמית אשכנזי "שוברת שוק: זירת הסחר הבינלאומי והשפעתה על הביטחון בסייבר" הזירה (29.2.2024) https://www.arenajournal.org.il/single-post/ashkenazi-trade-arena-cybersecurity
5. דפנה ברק-ארז **משפט מינהלי** כרך ג (2013).
6. הילה גולדשמיד "סייבר התקפי – בין יצוא בטחוני לייבוא אביפתי" **פורום עיוני משפט** (תגוביות משפט) מו (20.1.2022) https://www.taulawreview.sites.tau.ac.il/tguvit-goldschmid
7. המטה הלאומי לבינה מלאכותית, "התכנית הלאומית להאצת בינה מלאכותית וביסוס מובילות גלובלית ביווני פעולה (אוגוסט, 2026): https://govextra.gov.il/livedai/en/home/?utm_source=go.gov.il&utm_medium=referral.
8. אלדר הבר וטל ז'רסקי "דרכי ההגנה על תשתיות חיוניות במרחב הסייבר בישראל" **משפט וממשל** יח 99 (2017)
9. יצחק זמיר **הסמכות המינהלית** כרך א (מהדורה שנייה מורחבת, 2010).
10. שלמה טייטלבאום "נחתמו החוזים: פרויקט נימבוס הממשלתי יעסיק כ-3,000 עובדים" **כלכליסט** (24.5.2021)
11. יוסי מלמן "מעל או מתחת לאדמה: מכרז 'הענן הממשלתי' הוכרע, אך הקרב נמשך" **הארץ** (25.1.2022)

פסיקה

12. Anthropic PBC v. U.S. Dep't of War, No. 26-1049 (D.C. Cir. Sept. 25, 2026)

38 התכנית הלאומית להאצת בינה מלאכותית, לעיל ה"ש 14, בעמ' 57, 69 ו-72.

ספרים

13. John A. Alic et al., Beyond Spinoff: Military and Commercial Technologies in a Changing World (1992)
14. Henry Farrell & Abraham Newman, Underground Empire: How America Weaponized the World Economy (2023)
15. David Kennedy, Of War and Law (2006)

מאמרים בכתבי עת ובספרים

16. Ala Ali Almahameed et al., *Sovereignty, Surveillance, and the Cloud*: Geopolitical and Ethical Issues of Global Cloud Computing, in Ethical and Social Impacts of Information and Communication Technology 109 (Ignacio Alvarez et al. eds., 2026)
17. Luca Belli & Jamila Venturini, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation*, 5 (Internet Pol'y Rev. 1 (2016
18. (Hannah Bloch-Wehba, *How Tech Took Over* (Tex. A&M Univ. Sch. of L. Legal Stud. Rsch. Paper, 2026
19. (Elena Chachko, *National Security by Platform*, 25 Stan. Tech. L. Rev. 55 (2021
20. Stephane Couture & Sophie Toupin, *What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?*, 21 New Media & Soc'y 2305 (2019)
21. Andrea Coveri, Claudio Cozza & Dario Guarascio, *Big Tech and the US Digital-Military-Industrial Complex*, 60 Intereconomics 81 (2025)
22. Andrea Coveri, Claudio Cozza & Dario Guarascio, *Blurring Boundaries: An Analysis of the Digital Platforms–Military Nexus*, Rev. Pol. Econ. (2024)
23. Freddy Dezeure et al., *Digital Sovereignty Is Impossible Without Big Tech*, 48 Atlantisch Perspectief 30 ((2024
24. Niva Elkin-Koren, *What Contracts Cannot Do: The Limits of Private Ordering in Facilitating a Creative Commons*, 74 Fordham L. Rev. 375 (2005)
25. Niva Elkin-Koren & Karni A. Chagal-Feferkorn, *Lex AI: Revisiting Private Ordering by Design*, 36 (Berkeley Tech. L.J. 915 (2021
26. Niva Elkin-Koren & Maayan Perel, *Democratic Friction in Speech Governance by AI*, in Handbook of Critical Studies of Artificial Intelligence 643 (Simon Lindgren ed., 2023)
27. Massimo Ficco et al., *Simulation Platform for Cyber-Security & Vulnerability Analysis of Critical Infrastructures*, 22 J. Computational Sci. 179 (2017)
28. Mary Flanagan, Daniel C. Howe & Helen Nissenbaum, *Embodying Values in Technology: Theory and Practice*, in Information Technology and Moral Philosophy 322 (Jeroen van den Hoven & John Weckert eds., 2008)
29. May Har-Shai, *The Commercial Veto over Military AI* (unpublished manuscript)
30. May Har-Shai, *Governing Military Access to Commercial AI* (unpublished manuscript)
31. Aziz Z. Huq, *The Geopolitics of Digital Regulation*, 92 U. Chi. L. Rev. 833 (2025)
32. Jeppe T. Jacobsen & Tobias Liebetrau, *Infrastructuring Public-Private Relations: Big Tech, the Ukraine War and Implications to Security Governance*, 32 Eur. J. Int'l Rel. 183 (2026)
33. Mahmoud Javadi, *Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare: Insights from Ukraine, Israel and Taiwan*, 47 Contemp. Sec. Pol'y 469 (2026)
34. Amritha Jayanti, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose* (Belfer Ctr. for Sci. & Int'l Affs., 2023)
35. Mark A. Lemley, Matthew Wansley & David McGowan, *Coopting Disruption* (Cardozo Legal Stud. Rsch.

Paper No. 2024-24, Stan. L. & Econ. Olin Working Paper No. 589, 2024)
.36 Eviatar Matania & Udi Sommer, *Tech Titans, Cyber Commons and the War in Ukraine: An Incipient Shift in International Relations*, 39 Int'l Rel. 586 (2025)
.37 David C. Mowery & Timothy Simcoe, *Is the Internet a U.S. Invention? An Economic and Technological History of Computer Networking*, 31 Res. Pol'y 1369 (2002)
.38 Daniel Mügge, *EU AI Sovereignty*: *For Whom, to What End, and to Whose Benefit?*, 31 J. Eur. Pub. Pol'y 2200 (2024)
.39 Charles Pahud de Mortanges, Avoiding the Kill Switch: Europe's Digital Sovereignty Dilemma (ORBi, Univ. of Liège, 2026), https://orbi.uliege.be/handle/2268/347210
.40 Kaushik Ray & William Selvamurthy, *Starlink's Role in Ukraine*, 17 J. Def. Stud. 25 (2023)
.41 Udi Sommer, Eviatar Matania & Nir Hassid, *The Rise of Companies in the Cyber Era* and the Pursuant Shift in National Security, 75 Pol. Sci. 140 (2023)
.42 Swati Srivastava & Justin Bullock, *AI, Global Governance, and Digital Sovereignty* (arXiv:2410.17481, (2024
.43 Jay Stowsky, *Secrets to Shield or Share*? *New Dilemmas for Military R&D Policy in the Digital Age*, 33 Res. Pol'y 257 (2004)
.44 Wil van der Aalst, Oliver Hinz & Christof Weinhardt, *Big Digital Platforms*, 61 Bus. & Info. Sys. Eng'g 645 (2019)
.45 Fernando van der Vlist, Anne Helmond & Fabian Ferrari, *Big AI: Cloud Infrastructure Dependence and the Industrialisation of Artificial Intelligence*, 11 Big Data & Soc'y (2024)

מקורות אינטרנטיים

.46 Anthropic, *Statement on the Comments from Secretary of War Pete Hegseth*, Anthropic (Feb. 27, 2026), https://www.anthropic.com/news/statement-comments-secretary-war
.47 Rupert Barrett-Taylor & Matthew Ford, *Eroding Sovereignty in the Age of* "War as a Service", Opinio Juris /(Nov. 3, 2025), https://opiniojuris.org/2025/11/03/eroding-sovereignty-in-the-age-of-war-as-a-service
.48 Vera Bergengruen, *Ukraine's "Secret Weapon" Against Russia Is Clearview AI*, Time (2023), https://time. /com/6334176/ukraine-clearview-ai-russia
.49 Harry Davies & Yuval Abraham, 'A Million Calls an Hour': *Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians*, The Guardian (Aug. 6, 2025), https://www.theguardian.com/ world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud
.50 Harry Davies & Yuval Abraham, Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance ofPalestinians,TheGuardian(Sept.25,2025),https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians
.51 Future of Technology Institute, *Cloud Defence: An Exposed European Flank* (2026), https://cdn.prod. website-files.com/6a61d19f83fdca4fd1dd7efb/6a732bbe698401458f882b6e_CLOUD_REPORT.pdf
.52 Microsoft, *Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza*, Microsoft On the Issues (May 15, 2025, updated Aug. 15, 2025), https://blogs.microsoft.com/on-the- /issues/2025/05/15/statement-technology-israel-gaza
.53 Microsoft, *Summary of 2025 External Investigation and Follow Up* (June 2026)
.54 Carly Page & Ingrid Lunden, *Anthropic, OpenAI, and the New Rules of Defence AI*, Resilience Media /(Mar. 3, 2026), https://resiliencemedia.co/anthropic-openai-and-the-new-rules-of-defence-ai
.55 Josh Pennington & Sean Lyngaas, *Starlink in Use on 'All Front Lines,' Ukraine Spy Chief Says*, but Wasn't

Active 'for Time' over Crimea, CNN (Sept. 10, 2023), https://www.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html

56. Amrith Ramkumar, *Trump Administration Shuns Anthropic, Embraces OpenAI in Clash Over Guardrails*, Wall St. J. (Feb. 27, 2026), https://www.wsj.com/tech/ai/trump-will-end-government-use-of-anthropics-ai-models-ff3550d9

57. Brianna Rosen, Expert Comment: *The Pentagon-Anthropic Dispute Reflects Governance Failures – with Consequences That Extend Well beyond Washington*, Univ. of Oxford (Mar. 6, 2026), https://www.ox.ac.uk/news/2026-03-06-expert-comment-pentagon-anthropic-dispute-reflects-governance-failures-consequences

58. Brad Smith, *Microsoft Announces New European Digital Commitments, Microsoft On the Issues* (Apr. 30, /2025), https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments

59. Brad Smith, *Update on Ongoing Microsoft Review*, Microsoft On the Issues (Sept. 25, 2025), https://blogs. /microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review