מודלים רגולטוריים לניהול סיכוני סייבר בממשל הפדרלי בארצות הברית

מחקר השוואתי על אודות גישות סיכון שונות תחת שדה רגולטורי משותף

מאת

עידו סיון־סבִיליה*

במאמר זה נשאלת השאלה: כיצד ומדוע מתפתחות גישות שונות לניהול סיכונים על ידי המדינה? המאמר מתחקה אחר החוקים, הרגולציות וההסדרים הפרטיים (N=42) שהתמסדו בנוגע להגנת הסייבר בארצות הברית – משנת 1996 ועד לשנת 2018 – ומזהה גישות רגולטוריות שונות לניהול סיכוני סייבר על פני המגזר העסקי: (1) סיכונים ל"תשתיות קריטיות": מנוהלים על ידי מודלים של רגולציה־משותפת, בעלי מבני ממשל שיתופיים וחלוקת סמכויות לניהול סיכונים ואכיפה בין המגזר הפרטי לציבורי; (2) סיכונים למגזרי הבריאות והפיננסים: מנוהלים על ידי מודלים של רגולציה־מדינתית מסורתית של פיקוד, שליטה ואכיפה דרך חוקים וסוכנויות מדינתיות האחראים על הערכה וניהול הסיכונים; (3) סיכונים ליתר מגזרי המשק: מנוהלים על ידי מודלים של רגולציה־עצמית, דרך שיתופי פעולה בין מגזרים שונים וכוללים אימוץ וולונטרי של סטנדרטים, הנאכפים באופן חלקי על ידי סוכנויות מדינתיות.

השונות בגישות המדינה לסיכוני סייבר על פני מגזרי המשק מוסברת על ידי שלושה גורמים: (1) חשיבות מומחיותו של המגזר הפרטי בעיצוב הרגולציה לניהול סיכוני סייבר; (2) התרבות המוסדית ונורמות ההסדרה השונות הנהוגות בכל מגזר; (3) השפעתם של אינטרסים פרטיים על הליך קבלת ההחלטות,

---

* עידו סיון־סבִיליה נמצא בפוסט־דוקטורט באוניברסיטת Cornell-Tech בניו יורק, ארה"ב. עידו חוקר את החיבור שבין מדיניות ציבורית למדעי המחשב באופן השוואתי על פני מגזרים ומדיניות, ובאופן ספציפי בתחומי הגנת הסייבר והפרטיות. סיים דוקטורט במדיניות ציבורית באוניברסיטה העברית, תואר שני כעמית Fulbright באוניברסיטת מינסוטה תוך התמחות בקונגרס בווישינגטון, ותואר ראשון במדעי המחשב מהטכניון. בעל רקע טכנולוגי נרחב מחיל האוויר, משרד ראש הממשלה, והמגזר הפרטי. פרסם מאמרים אקדמאים בכתבי עת מובילים בעולם יחד עם מאמרי דעה בכלי תקשורת בישראל ובארצות הברית. מוזמן כדובר להרצאות בנושא המפגש של טכנולוגיה עם מדיניות ציבורית בארץ ובעולם.

המאפשר לשחקנים בתעשייה מנדט רגולטורי בנוגע לאופן שבו ינוהלו סיכוני סייבר במגזר העסקי.

המאמר מחבר בין ספרות מחקרית על אודות מודלים רגולטוריים לספרות העוסקת ברגולציה של סיכונים, ומקדם את ההבנה בדבר השיקולים הפוליטיים בעיצוב רגולציה לניהול סיכונים טכנולוגיים עבור החברה.

מבוא. א. סקירת ספרות: רגולציה לניהול סיכוני סייבר; 1. מודלים של רגולציה לניהול סיכונים; 2. הסברים לכינון רגולציה לניהול סיכונים. **ב. מסגרת אנליטית ומתודולוגיה. ג. התפתחות בזמן של המשטר הרגולטורי הפדרלי לצמצום סיכוני סייבר**; 1. רגולציה־משותפת: תשתיות קריטיות; (א) בניית משטר (מקור הסמכות והמבנה); (ב) הערכת סיכונים; (ג) צעדים לצמצום סיכונים ואכיפתם; 2. רגולציה־מדינתית: ספקי שירותי בריאות ופיננסים; (א) ספקי שירותי בריאות; (1) בניית משטר (מקור הסמכות והמבנה); (2) הערכת סיכונים; (3) צעדים לצמצום סיכונים ואכיפתם; (ב) ספקי שירותים פיננסיים; (1) בניית משטר (מקור הסמכות והמבנה); (2) הערכת סיכונים; (3) צעדים לצמצום סיכונים ואכיפתם; 3. רגולציה־עצמית: יתר המגזרים במשק; (א) בניית המשטר (מקור הסמכות והמבנה); (ב) הערכת סיכונים; (ג) צעדים לצמצום סיכונים ואכיפתם. **ד. דיון השוואתי. סיכום.**

מבוא

גיבוש רגולציה ומדיניות ציבורית לצמצום סיכונים הינו נושא הנחקר רבות על ידי מדעני מדינה, כלכלנים, סוציולוגים ומשפטנים.[1] גישת ניהול סיכונים לרגולציה מגדירה את מטרת הרגולציה כמזעור סיכונים עבור הציבור הרחב. ניתוח סיכונים מחייב הסתמכות על ידע לצורך הערכה והתמודדות עם הסיכון, ולעיתים, כמו בשדה הסייבר, יש אי־ודאות בנוגע לחומרת הסיכון וההסתברות להתממשותו. המורכבות הכרוכה בהערכת סיכונים והתמודדות עימם מצריכה הטלת תפקידי אסדרה הן על שחקנים מדינתיים והן

1 למשל, ראו עבודה של הכלכלן דיוויד מוס (David Moss): David Moss, *When all Else Fails: Government as the Ultimate Risk Manager* (2002); עבודתו של הסוציולוג ארטווין רן (Ortwin Renn): Ortwin Renn, *Risk Governance: Coping with Uncertainty in a Complex World* (2008); עבודתה של המשפטנית ג׳וליה בלאק: Julia Black, "The Role of Risk in the Regulatory Process", In: *The Oxford Handbook of Regulation* (Robert Baldwin, Martin Cave & Martin Lodge eds., 2010), pp. 302–348; עבודתו של מדען המדינה דיוויד ווגל: David Vogel, *The Politics of Precaution: Regulating Health, Safety, and Environmental Risks in Europe and the United States* (2012).

על שחקנים פרטיים, כדי לייצר רגולציה גמישה, הנשענת על מומחיות מספקת ומסוגלת להתמודד עם קצב מהיר של התפתחות טכנולוגית.[2]

עם זאת, תפקידה הספציפי של המדינה במבנים הללו נחקר בעיקר בהקשר של אסטרטגיות הסיכון שאותן המדינה בוחרת לאמץ,[3] ועל פי מידת הזהירות המונעת שבה פועלת המדינה מול סיכונים הכרוכים באי־ודאות.[4] מאמר זה עוסק ברובד נוסף בתפקיד המדינה ומספק מבט מעמיק על התפקיד המשתנה של המדינה במבני הממשל שנוצרו עבור ניהול סיכונים בתחום הסייבר בארצות הברית. על ידי התחקות השוואתית אחר מודלים מגזריים של רגולציית סיכונים שהתפתחו בין השנים 1996 ל־2018, מאמר זה ישאל כיצד ניתן להסביר את השונות בין גישות הסיכון של הממשל הפדרלי בארצות הברית על פני המגזרים במשק.

רגולציה של סיכוני סייבר נמצאת בליבת העיסוק של קובעי המדיניות הפדרלית בארצות הברית בשני העשורים האחרונים. העובדה שמרחב הסייבר מתרחב באופן עקבי[5] וממלא תפקיד חשוב עבור מגזרים רבים בתעשייה,[6] יחד עם ההתחדשות המתמדת של מרחב האיומים על זמינות המידע, מהימנותו ואמינותו,[7] הפכו את מרחב הסייבר לאתגר

---

2 על הקושי בהתמודדות עם קצב ההתפתחות הטכנולוגית, יחד עם התלות המסועפת בין שחקנים שונים וחוסר התאמה של מודלים רגולטוריים מסורתיים לניהול סיכוני טכנולוגיה מתפתחת ראו: G. Merchant, K. Abbott & B. Allenby, *Innovative Governance Models for Emerging Technologies* (2013).

3 דיוויס מוס (2002), בסקירתו ההיסטורית על אסטרטגיות הסיכון של המדינה, סוקר שיטות למניעה, הסטה, פיזור וצמצום נזקים כתוצאה של סיכונים. לעיל, הערה 1.

4 ויכוח נרחב בספרות התקיים בין דיוויד ווגל לג׳ונתן ויינר (Jonathan Weiner). בעוד ווגל טוען בעבודתו כי יש שוני מובהק במגמת ניהול הסיכונים בין האיחוד האירופי לארצות הברית, ויינר סבור כי לא ניתן להבחין בשונות מובהקת על פני כלל המגזרים, וטוען כי השונות נמצאת בין תחומים ולא בין מדינות. ראו: Jonathan Wiener, "The Politics of Precaution, and the Reality", 7 *Regulation & Governance* (2013) 258.

5 על פי הערכות, מחצית מאוכלוסיית העולם משתמשת ברשת האינטרנט. ראו: Simon Kemp, Digital in 2017 – Global Overview, 24 January 27 [https://wearesocial.com/special-reports/digital-in-2017-global-overview] (נצפה לאחרונה באוגוסט 2018). בנוסף, חברת גרטנר (Gartner) מעריכה כי עד שנת 2020, 20.4 מיליארד התקנים יחוברו לרשת האינטרנט. ראו: Gartner Press Release, Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, up 31 Percent from 2016, 7 February 2017 [https://www.gartner.com/newsroom/id/3598917] (נצפה לאחרונה באוגוסט 2018).

6 חברת הייעוץ מקאנזי (McKenzie) סוקרת את ההתפתחויות הללו על פני המגזרים השונים. ראו: Jacques Bughin, Laura LaBerge, and Anette Mellbye, The Case for Digital Reinvention, February 2017 [https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-case-for-digital-reinvention] (נצפה לאחרונה באוגוסט 2018).

7 לסקירה מקיפה של סיכונים במרחב הדיגיטלי ראו: OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document (2015).

רגולטורי שמושקעים בו משאבים רבים בהצלחה מוגבלת. כמות אירועי הפגיעה במערכות נמצאת בעלייה מתמדת, פושעים נושאים רווחים הולכים וגדלים מניצול המרחב לפשיעה וקניין רוחני נגנב בו על בסיס קבוע.[8]

את אתגרי הרגולטורים בצמצום סיכונים לחברה ניתן לייחס לאופיים של סיכוני הסייבר, המוגדרים בספרות המחקרית סיכונים ״מערכתיים״ (Systemic Risks).[9] סיכונים כאלו כוללים מידה רבה של אי־ודאות ומורכבות ביחסי הגומלין בין שחקנים המשפיעים על התעצמות הסיכון ומושפעים ממנה. אי־הוודאות באה לידי ביטוי בחוסר היכולת ליצור מודלים הסתברותיים להערכת הסיכוי להתממשות הסיכון ולהערכת חומרתו של הנזק. בניגוד לסיכונים המוגדרים סיכונים ״פשוטים״, המוסברים על ידי מודלים של סיבה ותוצאה (למשל תאונות דרכים), סיכונים ״מערכתיים״ אינם ניתן להפשטה על ידי מודל הסתברותי ויש אי־ודאות באשר למועד הופעתם. נוסף על כך, נזק עקב פגיעה במערכות במרחב הסייבר יכול להיות תוצאה של גורמים מגוונים: מטעות אנוש, דרך הגדרת מערכות שאיננה תואמת את איום הייחוס, ועד לפגיעות בתשתית התוכנה או החומרה שטרם הופץ עבורה תיקון. קשה להעריך מראש את השלכותיה של פגיעת סייבר ולכמת את רמת ההגנה הראויה המבטיחה את צמצום הסיכונים במרחב.[10]

הרובד השני של מורכבות הסיכונים בא לידי ביטוי בהיווצרותה של רשת סבוכה של יחסי גומלין ותלות הדדית בין שחקנים, החושפים זה את זה לסיכונים במרחב. פגיעה במערכת אחת עשויה להשפיע על מערכות נוספות המקושרות אליה במישרין או בעקיפין. חוליה אחת המספקת שירותים למגזרים רבים במשק עשויה להיות נקודת תורפה וליצור סיכון למסה קריטית של שחקנים במרחב.[11]

הספרות העוסקת בסיכונים ״מערכתיים״, כגון סיכוני סייבר, ממליצה על שילוב מספר רב ככל האפשר של שחקנים מהמגזר הפרטי והמדינתי, עם הסדרים מוסדיים ביניהם, זאת בכוונה להגדיל ככל האפשר את הוודאות בנוגע לחומרת הסיכון והסיכוי

---

8 על פי ההערכות של החטיבה הלאומית בארצות הברית למחקרי אסיה ב־2017, נזקי פשיעת סייבר מוערכים במאות מיליארדי דולרים עד כה. ראו: The Commission on the Theft of American Intellectual Property, “Update to the IP Commission Report: The Theft of American Intellectual Property – Reassessments of the Challenge and United States Policy”, 2017 [http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf] (נצפה לאחרונה באוגוסט 2018).

9 לעקרונות בניהול סיכונים מערכתיים ראו: Marjolein B.A. van Asselt & Ortwin Renn, “Risk Governance”, 14 *Journal of Risk Research* (2011) 431.

10 לקושי בכימות הגנת מידע ראו: Herley Cormac, Unfalsifiability of Security Claims (2016) [https://www.microsoft.com/en-us/research/wp-content/uploads/2015/09/unfalsifiabilityOfSecurityClaims.pdf] (נצפה לאחרונה באוגוסט 2018).

11 שתי דוגמאות לכך הן אירועי ה־ShellShock מספטמבר 2014, אשר פגעו באופן רוחבי במערכות יוניקס (Unix), ואירועי ה־HeartBleed מאפריל 2014, אשר פגעו באופן רוחבי בשרתים התומכים בתעבורה מאובטחת בפרוטוקול Https.

להתממשותו.[12] מאמר זה, לעומת זאת, מזהה יתרון מרכזי דווקא למדינה לעומת שחקנים אחרים בכל הקשור לקבלת אחריות על הערכת רגולציה לצמצום סיכונים, ניהולה ואכיפתה, וכן בהקמת מבני הממשל עבור ניהול סיכונים אלו. על ידי התחקות השוואתית אחר משטרי הסיכון המדינתיים לניהול סיכוני סייבר, הכוללים חקיקה פדרלית, תקנות משנה, הוראות נשיאותיות, מנגנוני שיתוף פעולה פרטיים־ציבוריים והנחיות מדיניות בין השנים 1996 ל־2018, המאמר מוצא כי מדיניות הגנת הסייבר בארצות הברית כוללת עשרות סוכנויות ושלושה מודלים רגולטוריים מרכזיים, אשר בכולם ניכרת השפעה הולכת וגוברת של המדינה.

הפרק הראשון במאמר מחולק לשני תתי־פרקים של סקירת ספרות מחקרית רלוונטית. בתת-הפרק הראשון נסקרת ספרות מחקרית העוסקת בטיפולוגיה של משטרי סיכון רגולטוריים (Risk Regulatory Regimes) יחד עם ספרות העוסקת בטיפולוגיה של מודלים שונים לחלוקת אחריות רגולטורית בין המדינה למגזר הפרטי. שילוב טיפולוגיות אלו מאפשר את בניית המסגרת האנליטית לניתוח מסמכי מדיניות בפרק השני. בתת-הפרק השני נסקרת הספרות המחקרית על אודות ההסברים להתעצבות רגולציה לניהול סיכונים על פני תחומי סיכון שונים. מספרות זו נובעות ההשערות הנבדקות במחקר.

בפרק השני מציע המאמר מסגרת אנליטית לניתוח, המשלבת כאמור בין שתי הטיפולוגיות שנסקרו. המסגרת האנליטית המוצעת בוחנת את מתן הסמכות, כינון ההסדרים המוסדיים וחלוקת האחריות בנוגע להערכת סיכונים, לרבות צעדים לצמצומם וניטור הרגולציה בתחום ואכיפתה. על פי מסגרת זו מבוצע ניתוח של 42 מסמכי מדיניות בין השנים 1996 ל־2018.

בפרק השלישי מבוצע ניתוח אמפירי של מסמכי מדיניות על בסיס המסגרת האנליטית המוצעת. מן הניתוח מתקבלים שלושה מודלים לרגולציית סיכונים: (1) סיכוני סייבר בתשתיות קריטיות: מנוהלים על ידי מודלים של רגולציה־משותפת, שבהם המדינה מתווה את בניית היכולת המוסדית ומסגרות המדיניות ומבצעת ניטור ואכיפה של הסטנדרטים המעוצבים יחד עם המגזר הפרטי; (2) סיכוני סייבר עבור ספקי שירותי בריאות ופיננסים: מבוצעים דרך רגולציה־מדינתית מסורתית, שבה סוכנויות מדינתיות מרחיבות את דריסת הרגל בהתוויית הסטנדרטים, הניטור והאכיפה של המגזר הפרטי; (3) סיכוני סייבר עבור מגזרים ש״אינם קריטיים״[13] ומייצגים את ה״כלכלה הדיגיטלית״:

---

12 Gary Marchant & Brad Allenby, “Soft law: New Tools for Governing Emerging Technologies”, 73 *Bulletin of the Atomic Scientists* (2017) 108.

13 מקורה של הגדרה זו במסמך הנחיות מ־2011 של משרד המסחר בארצות הברית (Department of Commerce), העוסק בהמלצות להנחיית מגזרים שאינם מוגדרים ״תשתיות קריטיות״ ומייצגים את מרבית הפעילות ב״כלכלה הדיגיטלית״ (The Digital Economy). ראו כאן: The Department of Commerce Internet Policy Task Force, “Cybersecurity, Innovation, and the Internet Economy”, 2011 [https://www.nist.gov/

מנוהלים על ידי מודלים של רגולציה־עצמית, שבה המגזר הפרטי קובע באופן כמעט בלעדי את הסדרי הפעולה והמדינה עוסקת באופן חלקי בניטור ואכיפה.

הפרק הרביעי דן בממצאים ומציע הסברים לשונות המתוארת לעיל על ידי שלוש השערות. **ההשערה הראשונה** מספקת הסבר פונקציונלי ומתייחסת למומחיות הנדרשת בניהול סיכוני סייבר בכל מגזר. בתחום התשתיות הקריטיות, המנוהל ברובו על ידי המגזר הפרטי, המדינה נשענת על מומחיותם של שחקנים פרטיים בתחום ובונה מודלים לרגולציה משותפת בהתאם. לעומת זאת, שאר המגזרים אינם דרושים מומחיות ייחודית, וביכולותיה של המדינה ליצור עבורם אסדרה מתאימה באופן אוטונומי.

ההשערה השנייה עוסקת בהסדרים המוסדיים השונים המסדירים את המגזרים במשק. ההשערה מייחסת את השונות המתקבלת לנורמות ההסדרה הנהוגות בכל המגזר ולשונות בלגיטימיות של המדינה להתערב במשק על פני מגזרים שונים.

ההשערה השלישית עוסקת בהשפעתם של אינטרסים פרטיים בהקשר שלאורו התפתח כל משטר רגולטורי. בעוד סיכוני סייבר בתשתיות קריטיות נתפסים על ידי מקבלי ההחלטות כסיכונים לביטחון הלאומי הדורשים התערבות מדינתית מדוקדקת, סיכונים למגזרי הבריאות והפיננסים, וכן למגזר העסקי בכללותו, נתפסו בראש ובראשונה כסיכונים לפרטיות הצרכנים.

על אף ההקשרים השונים, השפעתם של אינטרסים פרטיים ניכרת באופן ההתערבות המדינתית שהתעצבה ומסבירה את השונות בין המודלים השונים. בעוד ההשערה הראשונה מסבירה שונות ברגולציית סיכונים דרך רציונליות בחישוב הסיכון והצורך במומחיות, שתי ההשערות האחרות אינן פונקציונליות ומשייכות את הבניית הרגולציה לפוליטיקה של צמיחת המשטר. על כן, הבנת האופן שבו מתפתח תפקיד המדינה בניהול סיכוני סייבר עשויה לתרום להבנה של ניהול סיכונים דרך מדיניות ציבורית בתחומים נוספים.

הפרק החמישי במאמר מסכם את עיקרי התובנות ומציע דגשים להתבוננות עתידית בכינון מדיניות ציבורית עבור סיכונים טכנולוגיים.

מפת הדרכים של המאמר היא כלהלן: הפרק הבא יעסוק כאמור בסקירת ספרות על אודות רגולציה לניהול סיכוני סייבר, הפרק השני מספק את המסגרת האנליטית והמתודולוגיה, הפרק השלישי מתחקה אחר התפתחות בזמן של המשטר הרגולטורי הפדרלי לצמצום סיכוני סייבר, הפרק הרביעי מבצע דיון השוואתי והפרק החמישי מסכם.

---

sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf] (נצפה לאחרונה באוגוסט 2018).

א. סקירת ספרות: רגולציה לניהול סיכוני סייבר

הספרות המחקרית עוסקת באופן מצומצם ברגולציה ומדיניות ציבורית לניהול סיכוני סייבר במגזר הפרטי, ועל כן מאמר זה נשען על מחקרים מתחומים משיקים. בחלק הראשון של סקירת הספרות, שממנה נובעת המסגרת האנליטית לניתוח, מחבר המאמר בין ספרות העוסקת בכינון מודלים שונים של רגולציה – רגולציה־משותפת, רגולציה־מדינתית ורגולציה־עצמית – ובין ספרות העוסקת בניתוח המורכבות שבניהול סיכונים דרך ממשל ומדיניות ציבורית. בחלק השני של סקירת הספרות, שממנה נובעות השערות המחקר, נשען המאמר על הסברים ממחקרים העוסקים ברגולציה לניהול סיכונים מתחומים אחרים ובוחן תובנות מן הספרות על מדיניות ציבורית בתחום הסייבר.

1. מודלים של רגולציה לניהול סיכונים

מבני רגולציה שונים מוגדרים בספרות על פי חלוקת האחריות בין המגזר הפרטי לציבורי. הספרות עוסקת בספקטרום שבין רגולציה מדינתית נוקשה של פיקוד ושליטה, ללא מעורבות המגזר הפרטי, לבין רגולציה־עצמית מלאה, שבה התוויית הסטנדרטים, הניטור והאכיפה מבוצעים על ידי המגזר הפרטי.[14] בין שני קצוות אלו מוגדר המבנה של רגולציה־משותפת, הכולל סימביוזה של שני המבנים הקיצוניים ויוצר חלוקת אחריות בין המגזר הפרטי למדינה בהקשרים של קביעת הנורמות, הניטור והאכיפה.

זרם נרחב של חוקרים מצביע על מעבר מרגולציה מדינתית נוקשה של פיקוד ושליטה, עם הפרדה ברורה בין המדינה המפקחת למגזר הפרטי המפוקח, לרגולציה הנשענת על שחקנים פרטיים.[15] לאטזר ואחרים (Latzer et al.) עוסקים בחשיבותם של שחקנים פרטיים בכינון הסדרים רגולטוריים ומסבירים זאת נורמטיבית, מתוך שיקולים של העצמת הידע הרגולטורי ומתן גמישות למפוקחים.[16] בהיעדר משאבים וידע להעריך סיכונים מורכבים, למפותם ולנהלם, המדינה מצאילה סמכויות למגזר הפרטי בנושאים החוצים את כלל המגזרים במשק. עידן זה מכונה עידן ה״ממשליות החדשה״ (New

---

14 למחקר המסתמך על הספקטרום הנ״ל סביב מודלים שונים של רגולציה ראו: Avshalom Ginosar, “Co-Regulation: From Lip-Service to a Genuine Collaboration – The Case of Regulating Broadcast Advertising in Israel”, 3 *Journal of Information Policy* (2013) 104.

15 לסקירה רחבה על המעבר להסתמכות על שחקנים פרטיים ברגולציה ראו: Levi-Faur, David, “Regulatory Theory: Foundations and Applications”, *Handbook on the Politics of Regulation* (David Levi-Faur ed. 2011) pp. 3-22.

16 ראו: Michael Latzer, Natascha Just, Florian Saurwein & Peter Slominski, “Regulation Remixed: Institutional Change Through Self- and Co-Regulation in the Mediamatics Sector”, 50 *Communications and Strategies* (2004) 2127.

Governance), שבו המוקד עובר מן המדינה, כמקדמת הבלעדית של האינטרס הציבורי, אל יחסי הגומלין בין שחקנים פרטיים למדינה, הפועלים יחדיו לקידום מטרות ציבוריות.

באופן מסורתי, מודלים של רגולציה משולבת התפתחו באזורים שבהם נדרשת מומחיות הנמצאת בעיקרה אצל המגזר הפרטי. עקב כך, כדי להבטיח שימוש בידע נרחב בהליך גיבושה של המדיניות הציבורית, תוך ביצוע מהיר וגמיש של משימות רגולטוריות על ידי המפוקחים, צומחים הסדרים שיתופיים. אלו נתפסים על ידי התעשייה כשלב אחד לפני השתת הנחיות מחייבות על ידי המדינה.

סאנדן ואחרים (Senden et al.) מנתחים את יחסי הגומלין בין המדינה לשחקנים פרטיים בעידן ה״ממשליות החדשה״ ומגדירים מודל של רגולציה-משותפת ככזה הכולל מעורבות של המדינה בשלבים שונים של ההליך הרגולטורי, אך מעוצב בשיתוף פעולה מלא בין המגזרים. המדינה עדיין נהנית ממנדט בלעדי על ניטור ואכיפת הרגולציה.[17] למשל, רגולציה־עצמית כפויה (Enforced Self-Regulation) היא מודל רגולטורי המשקף האצלת סמכויות רגולטוריות של קביעת נורמות אל המגזר הפרטי, אך אמצעי האכיפה – הרתעה וענישה – מבוצעים על ידי המדינה בלבד.

גינוסר (2013) מרחיב את הניתוח של יחסי הגומלין בין המדינה לתעשייה וטוען כי כל מודל רגולטורי הוא מקרה פרטי של רגולציה־משולבת, כאשר רגולציה־עצמית ורגולציה מדינתית הן שני קצוות של מודלים של רגולציה־משולבת.[18] הוא מציע טיפולוגיה להבנת השונות בהסדרי רגולציה על פי הסמכות, המבנה וחלוקת האחריות הרגולטורית בין המדינה לתעשייה. סמכות יכולה להתקבל מתוקף חקיקה ראשית המחלקת סמכויות בין המדינה לתעשייה, או על ידי אימוץ וולונטרי בלבד של הסדרים. מבנים מוסדיים יכולים להיות מופרדים, משותפים או עצמאיים ואינם תלויים במקבלי ההחלטות או הגופים המפוקחים. חלוקת האחריות בין התעשייה למדינה מתפלגת על פני התוויית סטנדרטים, ניטור ואכיפה.

לדברי גינוסר, רגולציה־משולבת מאופיינת באוטונומיה ועצמאות של המוסדות הרגולטוריים, שקיפות בנוגע לתהליך קבלת ההחלטות ואכיפה ועניש על ידי גורמים מקצועיים. בפועל, רגולציה־עצמית עשויה להיתקל בהתנגדויות מצד רגולטורים העשויים לאבד מכוחם ולהיתפס כרגולציה שמיטיבה עם התעשייה ולא עם החברה, בעוד רגולציה־משולבת עשויה להיות מסורבלת למימוש ולאפשר מקום מצומצם למומחיות מהמגזר הפרטי במקרה של דומיננטיות מדינתית על הליך קבלת ההחלטות.[19]

---

17 L.A.J Senden, E. Kica, M. Hiemstra & K. Klimger, "Mapping Self- and Co-regulation Approaches in the EU Context", *Explorative Study for the European Commission DG Connect* (2015).

18 Ginosar (לעיל, הערה 14).

19 ראו עוד על המגבלות של שני המודלים: Tony Prosser, "Self-regulation, Co-regulation and the Audio-Visual Media Services Directive", 31 *Journal of Consumer Policy* 99 (2008).

את היתרונות והחסרונות של כל מודל רגולטורי, כמו גם סיבות אפשריות למכשולים או תמריצים לכינונו, יש לשקלל עם מגוון המשימות הרגולטוריות הכרוכות בניהול סיכונים עבור החברה. ספרות זו, העוסקת בהסדרה של סיכונים (Risk-Governance), מנתחת את המורכבות שבצעדי הערכה, ניהול ואכיפה עבור צמצום סיכונים.[20] בפרט, סיכוני סייבר מוגדרים בספרות הזו כסיכונים מערכתיים (Systemic Risks).[21] מושג זה הפך פופולרי לאחר ניתוח המשבר הכלכלי מ־2008. לפי הניתוח כאמור, אחד הגורמים המרכזיים למשבר היה התנהגותו של כל שחקן בנפרד למקסום רווחיו, באופן שהכשיל את המערכת כולה.[22]

סיכונים מערכתיים הם אפוא סיכונים שבעת התממשותם עשויים לגרום לקריסה מערכתית, ולא רק לפגיעה בשחקנים בודדים. סיכונים אלו הם לרוב בלתי צפויים, והסיכוי להתממשותם עולה עם הזמן. מקבלי החלטות אינם ערים לאופן שבו ההסתברות לסיכון עולה, וזאת כתוצאה של הערכת סיכון המבוצעת באופן חסוי ומבודד משאר השחקנים במרחב. על כן, חוקרים רבים ממליצים על האצלת סמכויות לניהול סיכונים למספר רב ככל האפשר של שחקנים, תוך שימת דגש בחשיבות התיאום ביניהם. כמו כן, ספרות זו מדגישה את החשיבות שבהבנת דפוסי הפעולה הנפרדים של הערכת הסיכון, הצעדים לצמצום הסיכון ואכיפתם.

2. הסברים לכינון רגולציה לניהול סיכונים

עד כה נסקרה ספרות המסייעת בבניית המסגרת האנליטית לניתוח מדיניות ציבורית לצמצום סיכונים במרחב הסייבר. מסגרת כזו צריכה לכלול הן מאפיינים של מודלים רגולטוריים שונים והן מאפיינים של דפוסי פעולה לניהול סיכונים. עם זאת, יש ספרות מחקרית ענפה המסבירה את היווצרותם של משטרי סיכון רגולטוריים בתחומים נוספים,

---

20 עבודות בנושא מורכבות הערכה וניהול סיכונים עוסקות לרוב בהמלצות נורמטיביות על עקרונות לניהול סיכונים מיטבי. ראו: Ortwin Renn, "Emerging Risks: Methodology, Classificaiton and Policy Implications", 4 *Journal of Risk Analysis and Crisis Response* (2014) 3. p. 114; Igor Linkov, Elke Anklam, Zachary A. Collier, Daniel DiMase & Ortwin Renn, "Risk-based Standarnds: Integrating Top-Down and Bottom-up Approaches", 34 *Environment Systems and Decisions* (2014) 134.

21 ראו ניתוח סיכוני סייבר כסיכונים מערכתיים: World Economic Forum, Understanding Systematic Cybersecurity Risks, *Global Agenda Council on Risk & Resilience* (2016).

22 על פי אחד הניתוחים, משקיעים סירבו להלוות כסף זמין לבנקים מתוך מקסום האינטרס האישי שלהם, אך קריסה של בנק אחד הכשילה את המערכת כולה. ראו כאן: Andy Hindmoor, Systemic Risk was the real culprit in the 2008 financial crisis and with banks continuing to borrow huge amount, the dangers are still there, 2013 [blogs.lse.ac.uk/politicsandpolicy/systemic-risk-was-the-real-culprit-in-the-2008-financial-crisis-and-with-banks-continuing-to-borrow-huge-amounts-the-dangers-are-still-there/] (נצפה לאחרונה באוגוסט 2018).

וממנה ניתן לנסח השערות לבחינה במהלך המחקר. הספרות העוסקת בגישות שונות של המדינה לרגולציית סיכונים מתבססת על מחקר השוואתי בין מדינות או על פני נושאי סיכון שונים. אלאמנו (Alemano) (2016) סוקר את ההתפתחות והפריחה של אימוץ רגולציה לצמצום סיכונים על פני תחומים ומדינות ומגדיר רגולציית סיכונים כאסדרה הקובעת אילו סיכונים אפשר לקבל ומהם הצעדים לצמצום הסיכונים שלא ניתן לקבלם.[23] המונח ״סיכון״ משמש הן כמושא הרגולציה והן כהצדקה לכינון רגולציה מלכתחילה.

מחקר השוואתי בין מדינות מוצא כי שונות בגישת המדינה לסיכונים היא תוצאה של השפעת אינטרסים פרטיים על הליך המדיניות הציבורית, כמו גם תרבויות ממשל שונות ולחץ ציבורי משתנה בעת משבר או חשיפה לסיכון.[24] חוקרים אחרים שמו דגש בתפקידה המתרחב של המדינה באסדרת סיכונים עבור החברה. בעוד הדעה הרווחת בספרות היא כי המדינה אינה מחזיקה במומחיות הנדרשת להסדיר סיכונים מורכבים כחומרים מסוכנים, ג׳וסטו־חנני ודיין (2014) מזהים עלייה בהתווייתנורמות מדינתיות

---

23 ראו: Alberto Alemano, “Risk and Regulaiton”, *Routledge Handbook of Risk Studies* (Adam Burgess, Alberto Alemano & Jens Zinn eds., 2016) 191, pp. 191–203.

24 רוטשטיין, בוראז והובר (Rothstein, Borraz, Huber) חקרו צמצום סיכונים על ידי רגולציה ומדיניות ציבורית בבריטניה, צרפת וגרמניה. הם מצאו כי גישת הסיכונים פופולרית בבריטניה אך מקובלת פחות בצרפת וגרמניה, וסיפקו לכך הסברים מוסדיים: בעוד בבריטניה יש נטייה להליך קבלת החלטות המזכיר ניהול חברה עסקית, עם דרישות גבוהות לשקיפות ואחריות, בצרפת התרבות היא תרבות טכנוקרטית ומסורבלת של פקידים, ואילו בגרמניה קבלת ההחלטות מבוזרת על פני גורמים רבים. בבריטניה השיקול המרכזי הוא התמודדות יעילה עם סיכונים ומשברים לחברה. לאחר משברים קשים שמה המדינה דגש באופן שבו ניתן לצפות משברים ולמנוע אותם מבעוד מועד. נוסף על כך, יש תרבות של רציונליות כלכלית בפעילות הממשלה, וגישת סיכונים מאפשרת לשיקולים רציונליים להוביל את תהליך קבלת ההחלטות. בצרפת, האליטה של הפקידים בממשל ששה לאמץ גישת סיכונים דרך רגולציה כדי לשמר ולהבטיח את כוחה בתהליך קבלת ההחלטות. ואכן, צרפת מאמצת גישת סיכון בכמה נושאים חברתיים מרכזיים – בטיחות מזון, תרופות, איכות סביבה, בטיחות בעבודה ומניעת מחלות. האימוץ המוגבל מוסבר על ידי החוקרים כתוצאה של תרבות של שוויון, שעלולה להיפגע מאימוץ גישת ניהול סיכונים, המתעדפת סיכון אחד על פני האחר, ונוסף על כך עלולה לייצר שקיפות ברמה כזו שתפגע בסמכותם של הנמנים עם אליטת מקבלי ההחלטות להחליט על המדיניות הנבחרת על פי האינטרסים שלהם. בגרמניה, אימוץ של רגולציה לצמצום סיכונים מתרחש במספר מצומצם של תחומים. הסיבות לכך הן המערכת הפדרלית המבוזרת בגרמניה, המקשה אימוץ מתודה אחת לניהול סיכונים ויוצרת חיכוכים בין רמות הממשל השונות. נוסף על כך, התרבות הקורפורטיסטית בגרמניה, שרגילה למצוא פשרות דרך משא ומתן, מתקשה לקבל תרבות של ניהול סיכונים היוצרת מערכת העדפות ברורה ואינה נותנת מקום ליחסי אמון ופשרות בין הצדדים. ראו Henry Rothstein, Oliver Borraz & Michael Huber, “Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe”, 7 *Regulation & Governance* (2013) 215.

לניהול סיכונים באיחוד האירופי ובארצות הברית.[25] לכאורה, מקומם של שחקנים פרטיים הוא מרכזי בגלל אי־הוודאות הכרוכה בסיכוני ננו־טכנולוגיה במקרה הזה, והעיסוק בנושאים טכניים, אשר נמצא בלב ההסדרה של נושאים אלו. אף על פי כן, החוקרות מוצאות עלייה בתפקידה של המדינה ברגולציה לצמצום סיכונים בנושאים הללו, אך אינן מסבירות מהיכן היא נובעת.

אחד הוויכוחים המרכזיים בספרות בין חוקרים העוסקים במחקר השוואתי לרגולציית סיכונים נסב על קיומם של הבדלים בגישות לסיכון בין ארצות הברית לאיחוד האירופי. התפיסה הרווחת היא כי החל משנות התשעים, האיחוד האירופי נוטה להחמיר יותר מארצות הברית באימוץ טכנולוגיות היוצרות אי־ודאות בנוגע לסיכונים הנובעים מהן.[26] הדוגלים בתפיסה זו משייכים אותה למרכיבים שונים במערכות הרגולטוריות האמריקאית והאירופאית – כגון ההישענות על חישובי עלות־תועלת והיעדרם של יחסי אמון במערכות רגולטוריות ממוסדות בין התעשייה לקובעי המדיניות. כמו כן, תפקידם של משברים והתממשותם של סיכונים, אשר יצרו לחץ ציבורי באירופה, משפיעים על השוני בין המדינות. חוקרים אלו טוענים כי המערכת האמריקאית מגיבה ומחכה להתממשותם של סיכונים לפני שהיא מחליטה להסדירם, בעוד האירופאים נוקטים את עקרון הזהירות המונעת (Precautionary Principle) בבואם לצמצם סיכונים עבור החברה. בפועל, לעומת זאת, זרם חוקרים אחר טוען כי יש קווי דמיון רבים בין ארצות הברית לאירופה, ללא שונות מובהקת ביניהם על פני כלל התחומים המוסדרים.[27]

ווגל (Vogel) (2003), מחד גיסא, מוצא שלוש סיבות מרכזיות להבדלים בין ארצות הברית לאיחוד האירופאי בנושאי רגולציה של סביבה וצרכנות.[28] לטענתו, שורה של משברים וכישלונות בהסדרת סיכונים בנושאי סביבה ובטיחות מזון באירופה דחקו במקבלי ההחלטות לפעול בנושא. כמו כן, תמיכה רחבה של אזרחי האיחוד ברגולציה נוקשה יותר כלפי סיכונים, ויכולותיו הרגולטוריות המתחזקות של האיחוד האירופי במטרה להסדיר את השוק המאוחד, הן שגרמו, במישרין ובעקיפין, לשינוי התבנית הרגולטורית בין ארצות הברית לאיחוד האירופי. בארצות הברית לעומת זאת, המבנה

---

25 ג׳וסטו־חנני ודיין (2014) מבצעות השוואה בין אימוץ רגולציה לסיכונים מחומרים כימיים בארצות הברית ובאיחוד האירופי ומזהות עלייה בתפקידה של המדינה, אף על פי שבאופן מסורתי, בנושאי ננו־טכנולוגיה, מסגרות המדיניות מוכתבות על ידי ארגונים בין־לאומיים כגון ה־OECD, עם השפעה גדולה מצד שחקנים פרטיים ואימוץ מודלים של רגולציה־עצמית. ראו: Ronit Justo-Hanani& Tamar Dayan, "The Role of the State in Regulatory Policy for nanomaterials risk: Analyzing the expansion of state centric rulemaking in the EU and US chemical policies", 43 *Research Policy* (2014) 169.

26 Vogel (לעיל, הערה 1).

27 Wiener (לעיל, הערה 4).

28 ראו: David Vogel, "The Hare and the Tortoise Revisited: The New Politics of Consumer and Environmental Regulation in Europe", 33 *British Journal of Political Science* (2003) 4557.

הפדרלי וחלוקת הסמכויות מקשה על רגולציה משמעותית לעבור החל משנות התשעים. היעדר משברים, יחד עם השפעתם החזקה של אינטרסים פרטיים על הרגולציה, יצרו סטגנציה במערכת האמריקאית וגרמו לכך שמדיניות ציבורית לצמצום סיכונים איננה מתעדכנת ומתחדשת עם התפתחות הידע על אודותיהם.

מאידך גיסא, המרכז הבין־לאומי לניהול סיכונים (International Risk Governance Council) פרסם ב־2017 סקירה על מערכות רגולציה לצמצום סיכונים באירופה וארצות הברית בנושאי בטיחות מזון, תחבורה, חומרים כימיים ותרופות.[29] המסקנה הראשית של מחקרם היא כי בניגוד לדעה הרווחת, הרגולציה לצמצום סיכונים באיחוד האירופי איננה מחמירה יותר מזו המקבילה בארצות הברית. בפועל אין מגמה ברורה; בנושאים מסוימים ארצות הברית מחמירה יותר, ובנושאים אחרים האיחוד האירופי מציב דרישות נוקשות יותר. המחקר איננו עוסק בסיבות להיווצרות תבניות רגולטוריות שונות בין שתי הישויות על פני הנושאים השונים.

נוסף על ההשוואה בין מדינות יש עיסוק נרחב גם בשונות הרגולטורית בין נושאי סיכון שונים. הוד, רוטשטיין ובולדווין (Hood, Rothstein, Baldwin) ביצעו ניתוח מקיף על פני תשעה נושאי סיכון שונים ומצאו כי הסברים המבוססים על אינטרסים פרטיים מסבירים בצורה הטובה ביותר שונות בין משטרי סיכון שונים באותה מדינה.[30] עם זאת, לקבוצות אינטרס יהיה קשה יותר להשפיע ולשנות מדיניות בתחומים שבהם נוצרו הסדרים מוסדיים משמעותיים.

התפתחות בגישות המדינה לנושאי סיכון שונים לאורך זמן משתקפת גם במחקרו של מוס (Moss), המזהה אסטרטגיות מדינתיות שונות לצמצום סיכונים מסוף המאה התשע עשרה ועד תחילת המאה העשרים ואחת.[31] המחקר מראה כי התערבות מדינתית בסיכונים הנובעים מהמגזר הפרטי איננה חדשה, אפילו במדינה כארצות הברית, אשר תרבותית והיסטורית איננה נוהגת להתערב באופן גס במשק. בשלבים שונים בהיסטוריה התערבה המדינה על פי הצרכים הבוערים של אותה תקופה בשלל תחומי החיים לאחר המהפכה התעשייתית – מקידום הפעילות העסקית במשק ומיגור סיכונים כלכליים, דרך דאגה לבטיחות העובדים ועד למיגור סיכונים עבור הצרכנים.

לאורך ההיסטוריה מבחין מוס בשתי צורות עיקריות של צמצום סיכונים: הקצאתם מחדש – דרך הסטת סיכונים ופיזורם או צמצומם – על ידי מניעה פרו־אקטיבית או מזעור נזקים לאחר התממשות הסיכון. מחקרו של מוס שופך אור על אסטרטגיות הסיכון השונות הניתנות ליישום, אך איננו מסביר מדוע מתעצבת רגולציה לצמצום סיכונים באופן הנבחר.

---

29 International Risk Governance Council (IRGC), Transatlantic Patterns of Risk Regulation: Implications for International Trade and Cooperation (2017).

30 Christopher Hood, Henry Rothstein & Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (2001).

31 Moss (לעיל, הערה 1).

מניתוח רגולציית סיכונים בתחומים אחרים אפשר אפוא לצפות כי מבנים רגולטוריים יושפעו מחד גיסא מאינטרסים פרטיים ומאידך גיסא מהסדרים מוסדיים, שעשויים להקשות על שינוי. נוסף על כך, יחסי אמון בין התעשייה למדינה חשובים להבנת המודלים שהתפתחו, ואני מצפה למצוא תפקיד מתרחב של המדינה לאורך זמן, בראי המחקרים שעסקו בניתוח דומה. כמו כן, אני מצפה למצוא שונות בין כלי המדיניות ובין אסטרטגיות הסיכון הננקטות בכל משטר רגולטורי. מחקר זה אף מספק רובד נוסף לספרות הבוחנת שונות בין מדינות או בין נושאים, ומספק הבנה של תבניות ניהול הסיכונים של המדינה בנושא אחד, סיכוני סייבר, על פני מגזרי המשק השונים.

אומנם הספרות המחקרית בנושאי מדיניות ציבורית בתחום הסייבר איננה מאמצת הסתכלות על רגולציה ככלי להערכת סיכונים וצמצומם, אך יש תובנות שניתן ללמוד מהמחקרים שנעשו בתחום זה. הספרות מתמקדת לרוב במגזרים מסוימים ואיננה מנתחת באופן שיטתי את הנעשה בכלל המגזרים במשק. חוקרים מתמקדים באסטרטגיות הנשיאותיות להסדרת מרחב הסייבר,[32] אחרים חוקרים את האופן שבו התפתחה רגולציית חובת דיווח (Notification Breach),[33] הגנת תשתיות קריטיות[34] או האתגרים הרגולטוריים שבשיתוף מידע.[35] חוקרים נוספים התמקדו בתפיסות הסיכון השונות של קובעי המדיניות,[36] בהתפתחות ההיסטורית של התעצבות אתגר הסייבר במחלקת ההגנה האמריקאית[37] ובטכניקות הרגולטוריות להגנת מידע מגזרית.[38] על סמך ספרות זו, אני מצפה למצוא השפעה של אינטרסים פרטיים ורגולציה משתנה בין מגזרים לניהול סיכוני סייבר, המשתקפת בכל אחד מהמחקרים הללו.

---

32 David W. Opderbeck, "Cybersecurity and Executive Power", 89 *Washington University Law Review* (2012) 795.

33 David Thaw, "Data Breach (Regulatory) Effects", University of Pittsburgh Legal Studies Research Paper No. 2015-2013 (2015).

34 ראו: Zachary Collier, Igor Linkov, Daniel DiMase, Steve Walters, Mark Tehranipoor & James Lambert, "Cybersecurity Standards: Managing Risk and Creating Resilience", *IEEE Computer Society* (2014) 70.

35 ראו: Johannes M. Bauer & Michel J.G. van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options", 33 *Telecommunications Policy* (2009) 706.

36 Kevin Quikley, Calvin Burns & Kristen Stallard, "'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection", 32 *Government Information Quarterly* (2015) 108.

37 Michael Warner, "Notes on the Evolution of Computer Security Policy in the US Government 1965-2003", *IEEE Annals of the History of Computing* (2015).

38 Abraham Newman & David Bach, "Privacy and Regulation in the Digital Age", *E-Life after the Dot.Com Bust* (Harry Bouwman, Brigitte Preissl, and Charles Steinfield – eds. 2004) 249; David Thaw, "The Efficacy of Cybersecurity Regulation", 30 *Ga. St. U. L. Rev.* (2014) 287.

הסקירה מלמדת על הפער בספרות המחקרית העוסקת במדיניות ציבורית בתחום הסייבר. הספרות אינה מסבירה כיצד התפתחו גישות שונות לסיכון על פני המגזרים השונים. אף על פי כן, הספרות מסייעת בבניית מסגרת אנליטית לניתוח של גישת המדינה לניהול סיכוני סייבר ומספקת הסברים נורמטיביים למעורבות נרחבת של המגזר הפרטי. כמו כן, מהנעשה בתחומים אחרים ניתן לצפות להשפעתם של אינטרסים פרטיים והסדרים מוסדיים על תהליכי קבלת ההחלטות בכל מגזר. מאמר זה שואף לבחון את ההסברים הללו ולהתחקות אחר הסיבות לגישות הסיכון השונות של המדינה על פני המשק.

ב. מסגרת אנליטית ומתודולוגיה

מחקר זה מתמודד עם מספר אתגרים מתודולוגיים. אתגרים אלו כוללים התמודדות עם כמות גדולה של מסמכי מדיניות והסדרי שוק בשלושת העשורים האחרונים, קביעת קריטריונים למדידת גישתה של המדינה לסיכון בכל אחד מהמגזרים והסקת מסקנות על הסיבות לגישות השונות של המדינה. אסביר להלן כיצד התמודדתי עם כל אחד מהאתגרים הללו.

ראשית, כדי להכיל ולהבין את גישתם של מקבלי ההחלטות ואת המבנים המתעצבים לניהול סיכוני סייבר בארצות הברית בשני העשורים האחרונים, המאמר משלב את הטיפולוגיה המוצעת בספרם של כריסטופר הוד, הנרי רוטשטיין ורוברט בולדויין (2001),[39] יחד עם הטיפולוגיה של גינוסר (2013), ובונה מסגרת אנליטית לניתוח מודלים רגולטוריים לניהול סיכונים על ידי המדינה.

על פי הטיפולוגיה של הוד, רוטשטיין ובולדויין, משטר סיכון רגולטורי (Risk Regulatory Regime) כולל את כלל החוקים, התקנות, הנחיות המדיניות וההסדרים המתעצבים לניהול סיכון מסוים על ידי המדינה. גישה זו היא כוללנית ורחבה, וכוללת לא רק שחקנים רשמיים של המדינה, אלא גם שחקנים פרטיים ועמותות ללא מטרות רווח העוסקים בנושאים הבאים: (1) איסוף מידע להערכת הסיכון; (2) נקיטת צעדים לצמצומו; (3) ניטור ואכיפה של צעדים אלו. אסביר להלן את החלוקה הזו לשלוש הקטגוריות.

ראשית, איסוף מידע להערכת סיכון כולל את כלל ההנחיות המורות על ניתוח איומים פנימי וחיצוני אשר מסייעות להעריך את הסתברות איום הנשקף וחומרתו. צעדים כאלו כוללים הנחיות לארגונים לביצוע סקירת סיכונים תקופתית או הנחיה על הקמה של מרכזי שיתוף מידע להערכת איומים חיצוניים. שנית, צעדים מדינתיים תחת הקטגוריה של נקיטת צעדים לצמצום הסיכון כוללים הנחיות לניהול הסיכון בפועל. צעדים אלו

---

39 Hood, Rothstein & Baldwin (לעיל, הערה 30).

יכולים לכלול הנחיה על נקיטת אמצעי התגוננות מתאימים למניעת הסיכון, הסטה של סיכון על ידי העברת האחריות לסיכון מגוף אחד לגוף אחר (כמו למשל במקרה של הסדרי ביטוח) או הנחיות לפעילות בעת התממשות הסיכון לצורך צמצום הנזק ככל שניתן (כמו למשל מתן סיוע מדינתי במקרה שהסיכון אכן התממש). לבסוף, צעדים לניטור ואכיפה כוללים את הפעולות שהמדינה נוקטת להבטחת ציות של המפוקחים לפעולות של הערכת סיכונים וניהולם. צעדים אלו יכולים לכלול ביקורות תקופתיות ואמצעי ענישה והרתעה. טיפולוגיה זו לניתוח הצעדים לניהול סיכונים על ידי המדינה מוצגת בנספח 1, ומהווה חלק אחד של המסגרת האנליטית בה עושה שימוש מאמר זה.

שלוש הקטגוריות לעיל, עבור ניהול סיכונים דרך רגולציה, מיושמות על ידי המדינה על בסיס מודלים רגולטוריים שונים. על מנת לנתח את המודלים הללו נבחנות הפעולות המדינתיות לניהול סיכוני סייבר על בסיס הטיפולוגיה של גינוסר (2013) לניתוח מודלים של מבנים רגולטוריים.[40] גינוסר (2013) מתייחס במאמרו לשלושה היבטים – סמכות, מבני הממשל וחלוקת האחריות הרגולטורית בין המגזר הפרטי למדינה – כדי לקבוע אם מודלים רגולטוריים הינם משותפים, מדינתיים או עצמיים.

ראשית, הסמכות הרגולטורית בכל משטר נמדדת על סמך מקור הסמכות של החוקים והתקנות העוסקים בסיכוני סייבר או בחינת החקיקה המעניקה למדינה, לתעשייה או לארגונים ללא מטרות רווח סמכות לפעול בהקשר של סיכוני סייבר. שנית, מבני הממשל המתעצבים בכל משטר נמדדים מתוך ניתוח הטקסטים של החוקים והתקנות ויחסי הגומלין המשתקפים מהם בין המפקחים למפוקחים כמו גם בין סוכנויות מדינתיות שונות. לבסוף, חלוקת האחריות הרגולטורית במודל של גינוסר מתחלקת כאן (על פי נספח 1) לחלוקת אחריות בנושאים הבאים: (א) הערכת הסיכון – הנמדדת על ידי הצעדים להבנת אופי הסיכון והסתברותו. בהקשר של סיכוני סייבר, הערכה כזו כוללת הן הערכה פנימית של כל ארגון בנוגע לעמידות תשתיותיו הדיגיטליות והן הערכה חיצונית של האיומים הנשקפים במרחב, המבוצעת על ידי שיתוף מידע בין שחקנים שונים; (ב) צעדים לצמצום סיכונים – הכוללים בניית יכולות לשיפור הערכת הסיכונים והפיקוח עליהם, בניית מומחיות וצבירת ידע בנושאי חומרת הסיכון והסתברותו, עיצוב צעדי בקרה למניעת הסיכון וצעדים להתאוששות מנזק לאחר שסיכון התממש; (ג) לבסוף, נבחנות פעולות ניטור ואכיפה של רגולציה לצמצום סיכונים בידי הרגולטור על ידי בחינת צעדים של בקרה, הרתעה וענישה.

על בסיס המסגרת האנליטית הזו, המשלבת טיפולוגיה להבנת האופן שבו המדינה מנהלת סיכונים עם טיפולוגיה למודלים רגולטוריים שונים עבור חלוקת האחריות בין המדינה לתעשייה, מזהה המחקר שלושה מודלים רגולטוריים לניהול סיכוני סייבר עבור מגזרי המשק בארצות הברית. על בסיס ניתוח 42 מסמכי מדיניות פדרליים העוסקים בהגנת סייבר משנת 1996 עד שנת 2018, המחקר מזהה כי פעולות המדינה נחלקות

40 Ginosar (לעיל, הערה 14).

לפעולות בשלושה מגזרים: (1) התשתיות הקריטיות; (2) בריאות ופיננסים; (3) יתר הכלכלה הדיגיטלית.

עבור כל מגזר, המחקר מתחקה אחר מסמכי המדיניות הרלוונטיים ומפלח את פעולות המדינה על פי קטגוריות של הערכת סיכונים, צמצום סיכונים וניטור ההנחיות המדינתיות ואכיפתן. עבור כל הנחיה מדינתית נבחנת חלוקת האחריות בין המגזר הפרטי למדינה על פי המודל של גינוסר. נוסף על כך, מקור הסמכות ואופי המבנה הרגולטורי המתעצב סביב כל מגזר מנותחים על סמך מקור הסמכות של הסוכנויות המדינתיות הפועלות בתחום ויחסי הגומלין בין המפקחים למפוקחים, כפי שהם משתקפים במסמכי המדיניות.

לבסוף, נוסף על הגדרת מודלים רגולטוריים שונים לניהול סיכוני סייבר והתחקות אחריהם, המתודולוגיה הנבחרת גם מבקשת להסביר את ההקשר הפוליטי והמוסדי שלהם. הסברים אלו התבססו על ההקשר והזמן שבהם התרחש כל מופע מדיניות ממאגר הנתונים, המקום שניתן לשחקנים פרטיים על ידי קובעי מדיניות וההסתמכות על מומחיותם של שחקנים אלו בהליכי קבלת ההחלטות, ונורמות ההסדרה של כל מגזר, כפי שהן משתקפות בספרות המחקרית.

אם כן, הפרק הבא מבצע ניתוח של מבני הממשל הפדרליים בארצות הברית לניהול סיכוני סייבר על פני התחומים הבאים: (1) תשתיות קריטיות; (2) מגזרי הבריאות והפיננסים; (3) יתר המגזרים במשק. כל ניתוח כזה מתחקה אחר ההיבטים הבאים: (א) האופן הכרונולוגי שבו נבנה המשטר הרגולטורי, המדגיש את מקור הסמכות והמבנה המתקבלים; (ב) ההנחיות להערכת סיכוני סייבר במגזר המפוקח; (ג) ההנחיות לניהול סיכונים וצמצומם בד בבד עם הצעדים לאכיפתם.

ג. התפתחות בזמן של המשטר הרגולטורי הפדרלי לצמצום סיכוני סייבר

סביבת סיכוני הסייבר התפתחה באופן ניכר ב־20 השנים האחרונות ודחקה מקבלי החלטות לעבור מניהול סיכונים עבור רשתות פדרליות בלבד למתן הנחיות רגולטוריות גם עבור המגזר הפרטי. עוד בשנות השישים הזהירו קובעי מדיניות כי מידע במערכות מחשב נתון לסכנות של גנבה וגישה בלתי מורשית, באופן שמסכן את פרטיות האזרחים והביטחון הלאומי.[41] בשנות השמונים, עם התפתחות טכנולוגיות קישוריות מתקדמות

41 Michael Warner, "Cybersecurity: A Pre-history", 27 *Intelligence and National Security* (2012) 781, p. 783.

והגברת נוכחותם של מחשבים ביתיים, הפך המרחב הדיגיטלי לסביבה שעליה נשענים ארגונים רבים ולתשתית של אספקת שירותים לחברה כולה.[42]

ממרחב שהיה ברובו צבאי ובשימוש מדינתי הפך המרחב לכזה המשמש את התעשייה והצרכנים. עקב כך, אינטרסים פרטיים, ולא רק מדינתיים, תפסו מקום מרכזי בזירת קבלת ההחלטות. קובעי מדיניות החלו לעצב רגולציה עבור מגזרי הבריאות והפיננסים, וב־1998 התעצבה תפיסת סיכון חדשה, שעל פיה הגנה על ״תשתיות קריטיות״ היא אינטרס חיוני במסגרת התלות הגוברת של המדינה במרחב הדיגיטלי. על ידי חקיקה ראשית והוראות נשיאותיות התפתחו מבנים מוסדיים חדשים ומשותפים למפעילי תשתיות קריטיות פרטיים ולמדינה. עסקים פרטיים שעסקו בפעילות שלא הוגדרה קריטית לתפקודה או ביטחונה של המדינה, או לחלופין עסקו בעיבוד מידע שאיננו נתפס כאינטימי ואישי, עמדו בפני המלצות וולונטריות בלבד להסדרת סיכוני הסייבר שנבעו מפעילותם.

כיום, משטרי הרגולציה לצמצום סיכוני הסייבר במגזר הפרטי בארצות הברית מעוצבים סביב תשתיות קריטיות, ספקי בריאות ופיננסים, ומגזרים ש״אינם קריטיים״, אשר מייצגים את כלל הכלכלה הדיגיטלית. שלושת המגזרים הללו מוסדרים על ידי מגוון כלים ואסטרטגיות מדיניות, תוך גישה נפרדת לתפקידה של המדינה בצמצום סיכוני הסייבר בכל מגזר. עם זאת, בכל המודלים הרגולטוריים ניתן להבחין בנוכחות גוברת של המדינה לאורך זמן, הבאה לידי ביטוי בכלי המדיניות, הסוכנויות המעורבות וסמכויות האכיפה המתרחבות.

1. רגולציה־משותפת: תשתיות קריטיות

רגולציה לצמצום סיכוני סייבר בתשתיות קריטיות פועלת דרך מודל של רגולציה־משותפת בין המדינה למגזר העסקי. מודל זה בא לידי ביטוי בסמכויות המשותפות שסיפקו החוקים וההוראות הנשיאותיות ובהקמתם של מבני ממשל משותפים ועצמאיים, המשקפים שותפות בין המדינה לתעשייה בגיבוש מדיניות לניהול סיכונים ויישומה. נוסף על כך משתקפת בו חלוקת האחריות לניהול סיכונים בין המדינה (אשר מתווה את החוקים והנורמות לאכיפה) לבין תעשייה וארגונים ללא מטרת רווח שאחראים על מימוש הצעדים להסדרה, תוך רמות שונות של ניטור ואכיפה על ידי המדינה וארגוני מגזר שלישי על פני מגזרי התשתיות השונים.

מסמכי המדיניות המתארים את המשטר משקפים גישה של התמודדות עם סיכוני סייבר כמשימה משותפת, שבה הממשל הפדרלי פועל בשיתוף פעולה עם בעלי תשתיות קריטיות במגזר הפרטי והציבורי על מנת להעריך את הסיכונים הנשקפים וכדי להחליט

---

42 Dunn Cavelty, *Myriam, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (2008) pp. 6–12.

יחדיו על הצעדים לצמצומם. בעוד עיקר האחריות להגנה מפני נזקי סייבר והתאוששות מהם מוטלת על מפעילי התשתיות הפרטיים, המדינה רשאית להתערב במגזרים שבהם המפעילים כושלים לספק הגנה ראויה. עם הזמן, המדינה מרחיבה את הכפופים להגדרת המגזרים ה״קריטיים״ ומגבירה את מעורבותה בהם.[43]

(א) בניית משטר (מקור הסמכות והמבנה)

המשטר הרגולטורי התפתח בשני העשורים האחרונים תוך התעצבות מארג המבנים המוסדיים המדינתיים המסדירים תחום זה. ראשיתו של המשטר, ב־1996, עם החלטת הנשיא דאז, ביל קלינטון (Bill Clinton), להקים את ועדת מארש (Marsh Commission) לבחינת ההגנה על תשתיות המדינה בעידן הדיגיטלי.[44] הוועדה הדגישה בהמלצותיה את האיום והפגיעות של תשתיות המדינה לסיכוני סייבר, אגב קריאה לאימוץ מודלים של שיתוף אחריות רגולטורית בין המדינה לתעשייה. הוועדה המליצה על חליפת מדיניות המאתגרת את החשיבה הקונבנציונלית על רגולציה מדינתית ויחסי הגומלין בין המדינה למגזר הפרטי.[45]

דוח הוועדה מגדיר את תפקיד המדינה כמסייעת לשיפור הערכת הסיכונים, תוך שיתוף ידע רלוונטי והצעות ליישום הגנה ראויה מפני האיומים. כדוגמה מביאה הוועדה את הנעשה בתחום התקשורת והאנרגיה ומבקשת לאמץ מודלים קיימים של שיתוף מידע והתוויית סטנדרטים כאחריות משותפת של המדינה והתעשייה. הוועדה גם ממליצה על הקמת גופי תיאום בכל מגזר ״קריטי״; גופים אלו יכילו שחקנים פרטיים ומדינתיים ליישום המדיניות המוצעת.

לאחר כחצי שנה מפרסום מסקנות הוועדה, ב־1998, הורה הנשיא קלינטון על האצלת האחריות להגנה על תשתיות קריטיות לכל מחלקה רלוונטית בממשל על פי תחום שיפוטה,[46] לצד הקמת מרכז המאגד את מאמצי ההגנה בכל המגזרים תחת הרשות הפדרלית לחקירות (Federal Bureau of Investigation – FBI). הקמת המרכז בוצעה בתיאום עם סוכנויות המודיעין, כדי לספק מידע עדכני על איומים למפעילי התשתיות הקריטיות. כמו כן, בכל משרד ממשלתי הוסמכו האחראים ליצירת שיתופי פעולה עם המגזר הפרטי בהערכה וצמצום סיכונים.

---

43 למשל במגזרי הכימיקלים והאנרגיה. ראו: Eldar Haber & Tal Zarsky, “Cybersecurity for Infrastructure: A Critical Analysis”, 44 *Florida State University Law Review* (2017) 515, pp. 534–536.

44 Executive Order No. 13010, “Critical Infrastructure Protection”, 1996.

45 ראו דוח הוועדה: The President’s Commission on Critical Infrastructure Protection, “Critical Foundations: Protecting America’s Infrastructures”, 1997 [https://fas.org/sgp/library/pccip.pdf] (נצפה לאחרונה באוגוסט 2018).

46 The White House, Presidential Decision Directive/NSC 63, Washington, May 22, 1998.

מן העבר האחר, בכל מגזר תעשייתי הוגדרו הישויות הרלוונטיות לעבודה מול הממשלה. המדינה סיפקה מומחיות וידע מודיעיני, ושחקנים מהמגזר הפרטי והמדינתי הסכימו על הסטנדרטים לאימוץ. ההוראה הנשיאותית הדגישה את הצורך בהתערבות מינימלית ושמירה על התרבות הרגולטורית האמריקאית של אי־התערבות בהחלטות עסקיות. ההוראה חידדה את הצורך למצוא חלופות לרגולציה מסורתית של פיקוד ושליטה ולהיעזר בתמריצים על מנת למנוע א־סימטריה במידע בין המגזרים השונים.

בשנת 2000 הוציא הבית הלבן את אסטרטגיית הסייבר הראשונה שלו והרחיב את סמכות הרשות המבצעת להנחות תשתיות קריטיות.[47] עם זאת, האסטרטגיה איננה מחייבת את המגזר הפרטי להנחיות נוקשות ומציינת כי לנשיא ולקונגרס אין סמכות בלעדית להורות על פתרונות מנדטוריים למגזר הפרטי בנושאים הדורשים מומחיות, כגון תשתיות קריטיות. ב־2001 העביר הנשיא בוש (Bush) הוראה נשיאותית מספר 13231 שנועדה להגדיל את שיתוף הפעולה בין משרדי הממשלה בנושאי תשתיות קריטיות ומינה יועץ ומתאם להגנת תשתיות קריטיות.[48]

ב־2002, לאחר המלצות שהתקבלו מהוועדה שעסקה בביטחון הלאומי בארצות הברית במאה העשרים ואחת,[49] וכמה ניסיונות חקיקה שלא צלחו בקונגרס, הוקמה המחלקה לביטחון המולדת (The Department of Homeland Security). המחלקה ריכזה לתוכה מגוון סוכנויות ממשלתיות ויצרה חטיבה ייעודית להגנה על תשתיות קריטיות, האחראית על הערכה וצמצום של סיכונים, בהם גם סיכוני סייבר. הוראה נשיאותית מ־2003 (Homeland Security Presidential Directive #7) עדכנה את ההחלטה הנשיאותית מ־1998 (PPD-63) ויצרה תוכניות מגזריות לכל מפעילי התשתיות.[50]

ההוראה קבעה כי המחלקה לביטחון המולדת היא רגולטור־על המפקח על כל משרד פדרלי בעל סמכויות להגנה על תשתיות קריטיות. סוכנויות מדינתיות נתבקשו לדווח באופן קבוע על סטטוס שיתוף הפעולה עם המגזר הפרטי. תשתית המדיניות עודכנה ב־2006, 2009 ו־2013 דרך התוכנית הלאומית להגנה על תשתיות (National Infrastructure Protection Plan), וכללה הנחיות מגזריות דרך גופי התיאום המגזריים שהוקמו (Sector Coordinating Councils).[51] ב־2013 פרסם הנשיא אובמה החלטה

---

47 The White House, National Plan for Information Systems Protection, January 2000.

48 Executive Order No. 13231, "Critical Infrastructure Protection in the Information Age", October 16, 2001.

49 ראו המלצות הוועדה: James Thomason, The US Commission on National Security/21st Century, 2000 [http://www.dtic.mil/dtic/tr/fulltext/u2/a387277.pdf] (נצפה לאחרונה באוגוסט 2018).

50 The Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

51 The Department of Homeland Security, National Infrastructure Protection Plan 2006, 2009, 2013.

נשיאותית (Presidential Policy Directive #21) אשר הגדירה 16 מגזרים כתשתית קריטית להגנה.[52] ההוראה מעדכנת את ההחלטה הנשיאותית מ־2003 ומבהירה את תפקידי שיתוף המידע של המדינה להערכת האיומים ואת מפת הסיכונים.[53]

מבני הרגולציה לניהול סיכונים לתשתיות קריטיות התעצבו מאז ההוראה הנשיאותית מ־1998, אשר יצרה מנגנוני שותפות הכוללים נציגים מן התעשייה והמשרד הממשלתי הרלוונטי בכל מגזר; אלה הורחבו מאוחר יותר ליצירת מנגנוני תיאום בכל מגזר תעשייתי (Sector Coordinating Councils (SCCs)) ובכל סוכנות ממשלתית העוסקת בתשתיות קריטיות במגזר מסוים (Government Coordinating Councils (GCCs)). המטרה הייתה להרחיב את הנציגות של התעשייה והשחקנים המדינתיים ולמסד הליך קבלת ההחלטות שיתופי.[54]

מנגנוני התיאום המגזריים (SCCs) מאפשרים לשחקנים שונים בתעשייה תחת אותו מגזר ללמוד זה מזה ולתאם אסטרטגיות ופעולות לצמצום הסיכון. מנגנוני התיאום הממשלתיים (GCCs) מאפשרים תיאום בין סוכנויות ובין מגזרים באופן עצמאי מהממשל הפדרלי. מנגנוני התיאום משתפים פעולה ביניהם דרך הסדר מוסדי ייעודי במחלקה לביטחון המולדת (Critical Infrastructure Partnership Advisory Council – CIPAC).

(ב) הערכת סיכונים

הערכת סיכונים לתשתיות קריטיות, המתחלקת בין הערכת איומי סייבר במרחב להערכת סיכוני סייבר הנובעים מתוך פעולות הארגון, מבוצעת על ידי המדינה והתעשייה יחדיו. ההוראה הנשיאותית מ־1998 הרחיבה את תפקידם של הארגונים המדינתיים לתיאום בין המגזרים (National Coordinating Councils)[55] והפכה אותם למרכזי שיתוף וניתוח מידע (Information Sharing and Analysis Centers – ISACs). בכל מגזר הוקם ארגון ייעודי לשיתוף מידע בין השחקנים השונים. בה בעת הקימה הרשות הפדרלית לחקירות (FBI) תוכנית ליצירת ממשק עם התעשייה לשיתוף מידע עם המדינה.

---

52 The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013.

53 The Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

54 John Moteff, "Critical Infrastructures: Background, Policy, and Implementation", *Congressional Research Service* (2015).

55 Executive Order No. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions", April 5, 1984 שהוקמו ב־1984 על ידי.

נוסף על כך, ב־2002 החריגה המחלקה לביטחון המולדת מידע המשותף בין ארגונים מתוך כוונה להקל את שיתופו.[56] הקלות אלו כוללות פטור מחשיפת המידע לציבור על אף חוקי חופש המידע או מניעה מהסתמכות על מידע זה בתביעות אזרחיות. כיום, ארגוני ה־ISAC לשיתוף מידע דומיננטיים בכלל המגזרים הקריטיים ומספקים שירותי תגובה לאירועים ומידע על המתרחש בתמורה לדמי חברות. 20 ארגוני ה־ISACs מנוהלים דרך המועצה הלאומית לארגוני שיתוף מידע (National Council of ISACs) ומבטאים מודלים עסקיים שונים סביב פיתוחו של כל ארגון לשיתוף ידע.[57] פרט לשיתוף מידע פנים־מגזרי, המחלקה לביטחון המולדת מנהלת תוכנית מרכזית לשיתוף מידע (The Cyber Information Sharing and Collaboration Program), אשר מספקת מידע מדינתי בנוגע לאיומי סייבר ומשתמשת במומחיות פרטית וממשלתית כדי להגיב לאירועים שמתרחשים.

עם זאת, יש מחלוקות בין המדינה למגזר הפרטי באשר למידת המעורבות של כל מגזר בהליכי שיתוף המידע. בעוד המגזר הפרטי מעוניין במידע מודיעיני על איומים ספציפיים, המדינה נוטה שלא לשתף מידע מודיעיני מתוך כוונה להגן על מקורות האיסוף או לצורך מיצוי חקירה המתנהלת בנוגע לאיומים מסוימים. מנגד, התעשייה אינה ששה לשתף מידע על איומים וסיכוני סייבר בתוך ארגונים, על מנת שלא לפגוע במוניטין הארגון וכדי לשמור על החיסיון של מפת איומי הסייבר הפנימית. המגזר הפרטי חושש כי מידע כזה ישמש את הרגולטור או הלקוחות כדי לבוא בדרישות אל החברה.[58] התעשייה מפקפקת לעיתים באפקטיביות של שיתוף מידע מצד המדינה, ונציגים ממגזרים שונים טוענים כי מידע מדינתי מעולם לא עזר למנוע מתקפה כנגד ארגונים פרטיים, מאחר ששיתוף כזה אינו מתרחש באופן מהיר מספיק.[59]

הערכת סיכונים לאיומים מתוך פעולת הארגון מבוצעת על ידי התעשייה עצמה בפיקוח המדינה ועל בסיס סטנדרטים שמספק המוסד הלאומי לסטנדרטים וטכנולוגיה

---

56 The Homeland Security Act of 2002, 6 U.S.C $124 (a) (2002).

57 אחד המודלים המוצלחים הוא בתחום הפיננסי, שבו בנקים גדולים ובעלי משאבים מגנים על בנקים קטנים על ידי שיתוף מידע. יש ארגונים שצמחו מתוך התעשייה, בעוד אחרים ניצלו מבנים קיימים ויצקו לתוכם תוכן רגולטורי של הגנה על תשתיות קריטיות, כמו במגזרי החשמל והתקשורת. לעיתים ארגונים אלו מקבלים מימון התחלתי מהמדינה, או לחלופין תומכים בעצמם על ידי מימון מהמגזר הפרטי.

58 The Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

59 לתפיסת התעשייה בנושא ראו: Commission on Enhancing National Cyber Security, "Meeting Minutes: Security challenges in the Digital Economy", *University of California Berkley*, June 21st, 2016 (www.nist.gov/sites/default/files/june_21_2016_ucb_meeting_minutes.pdf) (נצפה לאחרונה באוגוסט 2018).

(National Institute of Standards and Technology – NIST), אגב מתן שיקול דעת לתעשייה ולרגולטור המגזרי בנוגע ליישום הספציפי.

(ג) צעדים לצמצום סיכונים ואכיפתם

התוויית הסטנדרטים לצמצום סיכונים נחלקת בין המגזר הפרטי למדינה. בעוד המדינה מספקת את תשתית המדיניות תוך ניטור ואכיפה ברמה משתנה על פני המגזרים, התעשייה נהנית לרוב משיקול לדעת עבור אופן יישומה של מדיניות לצמצום סיכונים.

הסדרה של סטנדרטים בתשתיות קריטיות מבוססת על הוראה נשיאותית מס׳ 13636, אשר דורשת מהמוסד הלאומי לסטנדרטים וטכנולוגיה (NIST) להוביל את פיתוחה של תשתית הנחיה לכלל המגזרים הקריטיים.[60] המחלקה לביטחון המולדת הופקדה על יצירת התמריצים לתעשייה ליישום ההנחיות.

ההוראה מרחיבה את תוכניות שיתוף המידע למגזרים נוספים ויוצרת תהליכים לזיהוי מגזרים קריטיים. מרבית הסוכנויות המדינתיות האחריות על המגזרים השונים (Sector Specific Agencies) פרסמו הוראות ליישומה של תשתית המדיניות של המוסד הלאומי לסטנדרטים וטכנולוגיה (NIST). מפעילים פרטיים של תשתיות קריטיות מבצעים הערכות סיכונים ומאמצים צעדים לצמצומם באופן מחייב או וולונטרי, כתלות במגזר שממנו הם באים. כך למשל, מפעלי אנרגיה גרעינית חייבים לעמוד בדרישות סף לביצוע הערכות סיכונים ונקיטת צעדים לצמצומם, והם כפופים לאכיפה מהמועצה הפדרלית לרגולציה של אנרגיה גרעינית (Nuclear Regulatory Commission). במגזר החשמל, איגוד תשתיות החשמל הצפון־אמריקאי (North American Reliability Corporation) מפרסם ואוכף דרישות מחייבות. לעומתם, במגזר התקשורת ומערכות המידע או במגזר הנפט והגז, פעילויות להערכה וצמצום של הסיכונים אינן מחייבות, אך המדינה מתמרצת ומעודדת את יישומן. במגזרי הפיננסים והאנרגיה, המדינה מנטרת ואוכפת רגולציה לצמצום סיכונים דרך ארגוני רגולציה־עצמית מסורתיים (FINRA ו־NERC), שהוסמכו בעבר על ידי הקונגרס ופועלים כעת כמתווכים בין שחקנים פרטיים ובין המדינה ביישום הרגולציה, ניטורה ואכיפתה.

2. רגולציה־מדינתית: ספקי שירותי בריאות ופיננסים

סיכוני סייבר לספקי שירותי בריאות ופיננסים מנוהלים על ידי המדינה דרך מבני פיקוד ושליטה מסורתיים. הסמכות של סוכנויות פדרליות לפעול בנושא נובעת מחקיקה ראשית, ומשימות רגולטוריות של הערכה, ניהול, ואכיפה של רגולציה לצמצום סיכונים מוטלות כולן על המדינה, עם הפרדה ברורה בין שחקנים מדינתיים כרגולטורים ובין

60 Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity", February 12, 2013.

שחקנים פרטיים כנמעני רגולציה. עם זאת, התעשייה נהנית משיקול דעת בעיצוב הסטנדרטים לצמצום סיכוני סייבר בעת הליך החקיקה ומחופש לבחור את אופן המימוש של המסגרת הרגולטורית המוצעת. הן מנגנוני הערכת סיכון בכל ארגון והן הצעדים הנבחרים לצמצום הסיכון הינם מחייבים ומעוצבים בחלקם הארי על ידי המדינה. המדינה גם אוכפת עמידה בתנאים ובהסדרים שחוקקו דרך מספר הולך וגדל של חוקים, סוכנויות וסמכויות אכיפה.

(א) ספקי שירותי בריאות

(1) בניית משטר (מקור הסמכות והמבנה)

המאמצים הרגולטוריים של המשטר ממוקדים בסיכונים למידע אישי המוחזק על ידי ספקי שירותי בריאות. קובעי המדיניות נדרשו לתת מענה לגנבת זהות לצורך קבלת שירות רפואי, מרשמי תרופות והגשת תביעות ביטוח. לשם המחשה, בשנת 2014 היו חצי מיליון אזרחים נתונים לגנבת מידע רפואי. שלא כמו הונאות כרטיסי אשראי, קורבנות גנבת זהות בקרב ספקי שירותי בריאות שילמו בממוצע 13,500 דולר כדי לתחקר ולפתור את מקרי הגנבה.[61]

החל משנות התשעים לכדו העלייה בשימוש במרחב הדיגיטלי והתופעה של גנבת מידע אישי מארגונים את תשומת הלב של קובעי המדיניות. אף על פי שהמדינה נמנעה לרוב מלהטיל רגולציה פדרלית להגנת מידע בארגונים, ב־1996 חלה ההחרגה הראשונה, עם כינון רגולציה על ספקי שירותי בריאות דרך חקיקה ראשית. הקונגרס העביר את ה־Health Insurance Probability and Accountability Act (HIPAA), היוצר סטנדרט אחיד לאבטחת מידע והגנה על נתונים רפואיים.[62] החוק חל על כל ספק שירות אשר מעבד או מאחסן מידע רפואי ונאכף על ידי המשרד לזכויות אזרחיות (Office of Civil Rights) תחת המחלקה לשירותי בריאות (Health and Human Services) בממשל הפדרלי.

המגזר הפרטי השפיע רבות על הליך קבלת ההחלטות. השפעה זו באה לידי ביטוי בדרישה של הקונגרס להתייעץ עם קבוצת ארגונים מהתעשייה לפני כינונן של תקנות מחייבות על בסיס החקיקה. לאחר שבע שנים של סבבי התייעצות ותיקונים רבים הופצו תקנות ממשלתיות בהתאם. ב־2009, לאחר לחץ מצד ארגוני חברה אזרחית לשמירה על הפרטיות, הכניס הקונגרס תיקונים ל־HIPAA על מנת לחזק את סמכויות האכיפה, להגדיל את סוגי הארגונים הכפופים לרגולציה וליצור לראשונה חובת דיווח על נזקי

61 Stephen Redhead, “Anthem Data Breach: How Safe Is Health Information Under HIPAA?”, *CRS Insights* (2015).

62 The Health Insurance and Portability and Accountability Act, Public Law 104–191 (August 21, 1996).

סייבר ודלף מידע בארגון.[63] כל פריצה למאגר מידע המכיל מידע אישי על יותר מ־500 לקוחות צריכה להיות מדווחת לסוכנות הממשלתית תוך 60 יום. במקרה של גנבת מידע שאינו מוצפן חלה חובת דיווח כלפי הציבור. החקיקה החדשה יצרה גם קריטריונים לכינונה של חקירה ממשלתית, במקרה הצורך.

(2) הערכת סיכונים

הערכת סיכונים לנזקי סייבר כתוצאה של איומים בתוך הארגון הינה פרקטיקה מחייבת מתוקפן של הנחיות מדיניות שאוכף המשרד לזכויות אזרחיות במשרד הבריאות. כל ארגון נדרש לתוכנית ניהול סיכונים עבור המידע הנמצא ברשותו. נוסף על כך, ספקי שירותי בריאות עובדים דרך ארגונים ייעודים לשיתוף מידע על מנת ללמוד האחד מהשני על איומי סייבר בסביבתם. ארגון ה־Health Information Trust Alliance – HiTrust הוא הארגון שהמדינה מכירה בו לשיתוף וניתוח של איומי סייבר בסביבת ספקי הבריאות. השירות שמספק הארגון כולל כינון של תוכניות לניהול, ציות לרגולציה ויצירת מתודולוגיה להערכת סיכונים לכל ארגון.

(3) צעדים לצמצום סיכונים ואכיפתם

החקיקה הפדרלית מ־1996 הייתה הפעם הראשונה שבה סטנדרטים להגנת מידע במגזר הפרטי חוקקו ברמה הפדרלית בארצות הברית. קובעי המדיניות שאפו ליצור אחידות בבקרה של ארגונים על המידע המוחזק, כדי לוודא כי הוא איננו חשוף לגישה לא מורשית. הסטנדרטים כללו ניתוח סיכונים בשגרה, הערכתם, וניהולם, יחד עם צעדים להתמודדות עם נזקי סייבר, שכללו חובת דיווח. ארגונים חויבו לוודא כי הערכה וניהול של סיכונים הינם תהליך מתמשך המתעדכן תדיר. דרישות נוספות, כגון הצפנה, אינן מחייבות ונתונות לשיקול הדעת של ארגונים.[64] ב־2009 הרחיב התיקון לחוק את סמכויות המדינה אל ארגונים נוספים המנהלים קשר עסקי עם ארגוני הבריאות המפוקחים. ספקי השירות הפכו חשופים לסנקציות פליליות ואזרחיות במקרה של אי־עמידה בתנאֵי הרגולציה.

החקיקה הפדרלית אפשרה לשחקנים פרטיים שיקול דעת בביצוע הערכות סיכון וצעדים לצמצום סיכונים ויצרה מדרג להנחיות על פי כמות המידע שמחזיק הארגון המפוקח. לאחר כינון החקיקה נדרשה המחלקה לשירותי בריאות הציבור לפרסם סטנדרטים לאומיים. בתהליך שנמשך כשבע שנים וכלל כ־2,300 התייחסויות שונות לעיצוב החקיקה הותקנו התקנות המחייבות, שכללו פירוט מדוקדק של שלב היישום.

---

63 Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §201 (2009).

64 להרחבה, ראו הערה 62 לעיל.

ההסדרים החדשים יצרו סמכויות אכיפה נרחבות למדינה. החקיקה קבעה לראשונה קנסות פליליים ואזרחיים לאי־עמידה בתנאֵי הגנת מידע. קנסות אזרחיים נעים בין 100 ל־25,000 דולר. ענישה פלילית ככלל יכולה להגיע ל־50,000 דולר ושנת מאסר, והיא מגיעה אף ל־250,000 דולר במקרים שבהם הפשיעה מבוצעת מתוך כוונה למכור מידע או להשתמש בו להשגת יתרון מסחרי או גרימת נזק. ב־2009, עם תיקון החוק, סמכויות האכיפה אף התרחבו. החקיקה מגדילה את הענישה האזרחית ומחזקת את סמכויות האכיפה של המשרד לזכויות אזרחיות תחת משרד הבריאות. ארגון או אזרח יכולים גם הם להגיש תלונה לרגולטור במקרה שהם עדים לאי־עמידה בתנאי הרגולציה.

החקיקה מ־2009 מתייחסת גם לניטור על ידי הרגולטור ודורשת מהסוכנות הממשלתית לבצע ניטור תקופתי כדי לוודא שנמענֵי הרגולציה עומדים בתנאי החקיקה. תוכנית הניטור צריכה לעמוד בקריטריונים מוגדרים המזהים את ההליך, הבקרות והמדיניות של נמענֵי הרגולציה בנושאי שמירה על אבטחת המידע, הפרטיות וחובת הדיווח במקרה של נזקי סייבר. משרד הבריאות מחויב להגיש לקונגרס דוח שנתי,[65] המסכם את כמות התלונות שהתקבלו וסוגיהן, פעילויות האכיפה והניטור וצעדים לשיפור הציות להנחיות הרגולטוריות.

(ב) ספקי שירותים פיננסיים

(1) בניית משטר (מקור הסמכות והמבנה)

ספקי שירותים פיננסיים, כגון בנקים, נותני הלוואות, מספקי משכנתאות, יועצי השקעות וגובי חוב, נתונים לסיכוני סייבר העלולים להוביל לגנבה של כספים, קניין רוחני ומידע אישי. הגנת סייבר נתפסת על ידי קובעי המדיניות כמרכזית לבניית אמון בהליכי אספקת שירותים פיננסיים. יש ספקים, כגון בנקים מרכזיים, שהוגדרו על ידי המדינה ״תשתית קריטית״,[66] ולעומתם ספקים אחרים מונחים על ידי חקיקה ראשית ייעודית ותקנות משנה להגנת מידע, שאותן מפרסמות סוכנויות מדינתיות אחדות בעלות סמכות רגולטורית מסורתית בתחום הפיננסים.

המשטר הרגולטורי מורכב מכמה חוקים פדרליים שיצרו את התשתית להגנה על מידע אישי פיננסי. החקיקה על שם גרהאם, ליץ׳ ובלילי (The Gramm-Leach-Bliley Act

---

65 דוגמה לדוח כזה ראו: The Office of the National Coordinator for Health Information Technology (ONC), Report to Congress, 2016 [https://dashboard.healthit.gov/report-to-congress/2016-report-congress-examining-hitech-era-future-health-information-technology.php] (נצפה לאחרונה באוגוסט 2018).

66 הוראה נשיאותית PPD-21 מ־2013 הגדירה את מגזר הפיננסים כמגזר קריטי בו נותני שירותים מסוימים כפופים להנחיות משרד האוצר בשמירה והגנה על מערכות המידע שלהם הכוללות שיתוף מידע והתוויית סטנדרטים משותפת של התעשייה והמדינה. לעיל, הערה 52.

(GLBA)) מ־1999,[67] ועל שם סארבאנס ואוקסלי (Sarbanes-Oxley Act (SOX)) מ־2002,[68] כמו גם החקיקה לרפורמה בוול סטריט והגנת הצרכן על שם דוד ופרנק (The Dodd-Frank Wall Street Reform and Consumer Protection Act) מ־2010, שתוקננה לאחר המשבר הכלכלי של 2008, כוללות צעדים לצמצום סיכוני סייבר במגזר הפיננסי.[69] נוסף על כך יש מגוון סוכנויות מדינתיות אשר הוסמכו בחקיקה ייעודית לעסוק בהנחיית צמצום בסיכוני סייבר למגזר זה.

הרגולציה פועלת באמצעות מכניזמים רגולטוריים מסורתיים של פיקוד ושליטה במבנה מסועף דרך סוכנויות רבות. מושא הרגולציה הוא לרוב השירות הפיננסי אשר ממנו נגזרות החברות המפוקחות. על כן, סוכנויות שונות מטפלות בשירותים פיננסיים שונים, כניהול חשבונות בנק, מסחר בניירות ערך וביטוח. ניתן לחלק את המשטר הרגולטורי לשלוש קבוצות של סוכנויות – רגולטורים של בנקים פדרליים, של מסחר בניירות ערך ושל הגנת הצרכן. לכל קבוצה יש סטנדרטים שונים להערכת סיכוני סייבר וניהולם.

רגולטורים של בנקים פדרליים מחייבים להחיל סטנדרטים להבטחת יציבותם וביטחונם של המוסדות הפדרליים העוסקים בהפקדות כספים כדי להגן על יציבות המערכת הבנקאית בכללותה. סטנדרטים אלו כוללים הנחיות לאבטחת מידע על מנת למנוע דלף מידע או גנבה של מידע עסקי. המשרד לבקרת המטבע (The Office of the Comptroller of the Currency) הוא הרגולטור המרכזי בתחום זה ומתוקף תפקידו עוסק גם בסיכוני סייבר. נוסף על כך, הבנק המרכזי (Federal Reserve) הוא הרגולטור של מגוון מוסדות פיננסיים, כבנקים במדינות ארצות הברית השונות, סניפים אמריקאיים של בנקים זרים, פעילות בין־לאומית של בנקים אמריקאיים, חברות המנהלות בנק וכן מחזיקי ניירות ערך ונותני הלוואות. החברות שבאחריות הבנק המרכזי הן חברות שהמועצה ליציבות פיננסית (The Financial Stability Oversight Council) הגדירה אותן כבעלות חשיבות ליציבות המערכת הפיננסית. רגולטור נוסף הוא ה־Federal Deposit Insurance Corporation, המשמש כרגולטור לבנקים המבוטחים ברמה הפדרלית אך אינם חלק מהמערכת הפדרלית.

קבוצה נוספת של רגולטורים במשטר הם העוסקים ברגולציה על סחר בניירות ערך – הרשות לניירות ערך (Securities Exchange Commission (SEC)) והרשות לסחר בסחורות וחוזים עתידיים (Commodity Futures Trading Commission (CFTC)). הנחיותיהן כוללות דיווח שנתי למשקיעים על סיכוני סייבר שהתממשו בארגונים והנזקים שנגרמו. באופן ספציפי, SEC מפקחת על סחר בניירות ערך, ברוקרים, יועצי השקעות וקרנות

67 Gramm-Leach-Bliley Act, Public Law 106-102 (November 12, 1999).

68 Sarbanes-Oxley Act of 2002, Public Law 107-204 (July 30, 2002).

69 Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111–203 (July 21, 2010).

נאמנות. הרשות אחראית על השקיפות בחברות הנסחרות בבורסה ומטילה סנקציות במקרה של הונאה או אספקת מידע שאיננו מדויק.

קבוצת הרגולטורים השלישית במגזר הפיננסי כוללת סוכנויות להגנת הצרכן. הרשות להגנת הצרכן (Consumer Financial Protection Bureau (CFPB)) נהנית מסמכויות חקיקה, ניטור ואכיפה על ספקי שירותים ומוצרים פיננסיים. הסוכנות מוסמכת להתקין תקנות אשר עוסקות בהגנת סייבר וכוללות הנחיות למניעת גנבת זהות הנובעות מה־Fair and Accurate Credit Transactions Act,[70] ובהתאם, הנחיות להגנת מידע הנובעות מחקיקת GLBA.[71]

הסוכנות, מתוקף החקיקה מ־2010 שייסדה אותה, מוסמכת להתקין תקנות אשר מגדירות שגרות מסוימות כלא חוקיות כתוצאה של פגיעה בפרטיות והגנת המידע של צרכנים פיננסיים. ב־2016 השלימה הסוכנות פעולת אכיפה ראשונה בהתבסס על סמכות זו.[72] לאחרונה חברה הסוכנות לרגולטורים של הבנקים הפדרליים והוציאה כלי להערכת סיכוני סייבר.

סוכנות חשובה נוספת להגנת הצרכן הפיננסי היא הסוכנות הפדרלית למסחר (The Federal Trade Commission (FTC)). הסוכנות הוקמה ב־1914 כדי להגן על צרכנים מפני סחר לא הוגן מצד חברות, ועל בסיס סמכות זו היא מבצעת פעולות ניטור ואכיפה נגד שגרות של הגנת סייבר לקויה ופגיעה בפרטיות הצרכנים. הסוכנות אוכפת את הדרישות להגנת המידע הנובעות מחקיקת GLBA ומטפלת במוסדות פיננסיים אשר מוגדרים באופן רחב ככאלו העוסקים במסחר ואינם כפופים להנחיות מרגולטורים פדרליים אחרים.[73]

עד כה ביצעה הסוכנות אכיפה ביותר מ־50 מקרים נגד חברות שהואשמו במסחר לא הוגן כתוצאה של היעדר הגנה על מידע אישי של לקוחותיהן.[74] חברות פרטיות התלוננו

---

70 The Fair and Accurate Credit Transactions Act of 2003, Public Law 108–159, December 4, 2003.

71 Gramm-Leach-Bliley Act, Public Law 106-102 (November 12, 1999).

72 עוד על פעולת האכיפה הראשונה של הרשות להגנת הצרכן ראו: Paul Weiss, Rifkind, Wharton & Garrison LLP, "The CFPB Enters the Cybersecurity Arena With Its First Enforcement Action", 2016 [https://www.paulweiss.com/media/3377203/4mar16cyberalert.pdf] (נצפה לאחרונה באוגוסט 2018).

73 Congressional Research Service, "Financial Services and Cybersecurity: The Federal Role", 2016 [https://www.everycrsreport.com/files/20160323_R44429_983f4a1ffab71b2e8a2f025e2e6cd39d65d6f61f.pdf] (נצפה לאחרונה באוגוסט 2018).

74 The Federal Trade Commission, Data Security Update: 2017, 2017 [https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf] (נצפה לאחרונה באוגוסט 2018).

שהקריטריונים לאכיפה אינם ברורים דיים, והסוכנות סיפקה לאחרונה הנחיות שנועדו להבהיר מתי שגרה ארגונית עשויה להוביל לפעולת אכיפה מצד הסוכנות.

רגולטור נוסף בתחום הגנת הצרכן הוא האיגוד הלאומי לסחר באמצעות אשראי (The National Credit Union Administration), העוסק באסדרה של הגנת מידע באיגודי אשראי הפועלים ברמה הפדרלית. האיגודים הללו הם ארגונים שיתופיים של אזרחים אשר מקבלים הפקדות מחברים שונים ועובדים דרך חשבונות משותפים לאספקת אשראי ודיבידנדים לחברים.

(2) הערכת סיכונים

הן הערכת הסיכונים והן הצעדים לצמצומם נובעים מתוקף אותן חקיקות והנחיות המתייחסות לשני האלמנטים יחדיו. האסדרה כוללת לרוב התייחסות להערכת סיכונים בד בבד עם צעדים מחייבים עבור מניעת נזקי סייבר והתאוששות מהם. צעדים אלו יפורטו בהרחבה בחלק הבא. עם זאת, תחום הערכת הסיכונים מפני איומים חיצוניים במגזר הפיננסי התפתח והתרחב אל מעבר לתחום של שירותים פיננסיים קריטיים, וכעת מאפשר גישה למידע על איומים עבור ארגונים פיננסיים נוספים. המרכז לשיתוף וניתוח של איומי סייבר במגזר הפיננסי (Financial Sector Information Sharing and Analysis Center (FS-ISAC)) הוא איגוד חברות המספק גישה למידע על איומים במרחב לכל חברה פיננסית החבֵרה בארגון ונתפס היום כאחד המודלים המוצלחים לשיתוף מידע בהקשר של סיכוני סייבר.

(3) צעדים לצמצום סיכונים ואכיפתם

סעיף 501 בחקיקת GLBA מחייב מוסדות פיננסיים להגן כראוי על מידע אישי פיננסי של לקוחותיהם אגב יצירת תוכנית להתמודדות עם סיכונים של גנבת מידע.[75] החקיקה מאפשרת לארגונים גמישות ושיקול דעת בבחירת הכלים והתצורה ליישום הגנת מידע, אך מחייבת ארגונים לנסח תוכנית כתובה לניהול סיכונים. כמה סוכנויות מוסמכות ליצור ולאכוף תקנות בהתאם לחקיקה זו: הסוכנויות האחראיות על הבנקים הפדרליים וניירות הערך (The Federal Banking and Securities Agencies), הסוכנות הפדרלית למסחר (FTC) ורגולטורים של חברות ביטוח הפועלים ברמת המדינות בארצות הברית. נוסף על כך, איסור לשיתוף מידע אישי עם צד שלישי נבדק ונאכף על ידי הרשות הפדרלית להגנת הצרכן (CFPB).

החל משנת 2000 הוציאה הרשות לניירות ערך שלוש תקנות העוסקות במישרין בצמצום סיכוני סייבר. התקנה הראשונה, Regulation SCI, מחייבת ארגונים האוכפים רגולציה עצמית במגזר הפיננסי, כגון הרשות הרגולטורית למגזר הפיננסי (Financial

---

75 Gramm-Leach-Bliley Act, 15 U.S.C $6801 (1999).

(Industry Regulatory Authority (FINRA), ליישם הגנה על מערכות המידע שלהם.[76] תקנה נוספת, Regulation S-P, מיישמת את הדרישות לפרטיות המידע מהחקיקה הפדרלית (GLBA) ומחייבת חברות השקעות ומשקיעים רשומים להגן על המידע האישי של לקוחותיהם.[77] התקנה השלישית, Regulation S-ID, דורשת מחברות להגן מפני גנבת זהות.[78]

המשרד ברשות לניירות ערך העוסק באכיפת הרגולציה (Office of Compliance Inspections and Examinations) מתריע בפני כלל החברות הכפופות על הדגשים בהליכי הניטור ובקרה התקופתיים; ב־2015 פרסם המשרד הנחיות להגנת הסייבר שהתקבלו מבדיקה של כ־100 נמעני רגולציה. סמכויות האכיפה של הרשות באו לידי ביטוי ב־2016, כאשר חברת השקעות נאלצה לשלם מיליון דולר בעקבות אי־יישומן הנחיות להגנת מידע על אף התחייבותה.[79]

CFTC הוא רגולטור נוסף במגזר ניירות הערך, וחברות שונות כפופות אליו. תחת החקיקה משנת 2000 – The Commodity Futures Modernization Act – הרשות מוסמכת להתקין תקנות ולאכוף את הגנת הפרטיות של לקוחות פיננסיים על סמך חקיקה פדרלית (GLBA).[80] הרשות פרסמה כמה צעדים מחייבים לצמצום סיכונים, הכוללים חובת דיווח, כינון תוכנית לניהול סיכונים לאבטחת המידע, התאוששות מנזק וצעדי מניעה. נוסף על כך, סחר בניירות ערך מוסדר גם על ידי ארגונים ללא מטרות רווח האוכפים הסדרי רגולציה־עצמית של המפוקחים. ארגונים אלו כוללים את FINRA ואת ה־National Futures Association, הפועלים כמתווכים בין הרגולטור למפוקחים ביישום ההנחיות הנדרשות.[81]

ניטור של רגולציה לצמצום סיכונים בארגונים פיננסיים מבוצע גם על ידי המועצה לבחינת מוסדות פיננסיים (Federal Financial Institution Examination Council), אשר הוקמה ב־1978 כדי ליצור אחידות באופן שבו מוסדות פיננסיים מבוקרים על ידי הרגולטור. המועצה עוסקת באופן שבו הרגולטורים האחראים על פעילות הבנקים

---

76 Regulation Systems Compliance and Integrity, 17 CFR Parts 240,242,249 (February 3, 2015).

77 Regulation S-P: Privacy and Consumer Financial Information and Safeguarding Personal Information, 17 CFR Part (2000) 248.

78 Identity Theft Red Flags Rules, 17 CFR 248 (2013).

79 Jonathan Stempel, "Morgan Stanley Pays $1 million Sec five over Stolen Customer Data", 2016 [https://www.reuters.com/article/us-morgan-stanley-sec-idUSKCN0YU27J] (נצפה לאחרונה באוגוסט 2018).

80 The Commodity Futures Modernization Act, Public Law 106-554, December 21, 2000.

81 FINRA הינה ארגון שהוסמך על ידי הקונגרס להגן על נמעני הרגולציה של הרשות לניירות ערך דרך ניסוח ואכיפה של סטנדרטים. הארגון נוצר ממיזוג של איגוד החברות לסחר בניירות ערך והבורסה בניו יורק. NFA הינו ארגון זהה שהוקם עבור נמעני הרגולציה של CFTC.

בארצות הברית מבקרים את נמעני הרגולציה. המועצה הוסיפה לבחינות הציות שלה גם בדיקה של אופן השמירה על הגנת הסייבר בארגונים, הנסמכת על הוראות שהוציא הבנק המרכזי הפדרלי (Federal Reserve) לשמירה על הגנת המידע. הנחיה נוספת כוללת חובת דיווח במקרה של גנבת מידע לרשויות אכיפת החוק והרגולטור הרלוונטי, על פי סוג הבנק. כמו כן יש מקרים שבהם יש לדווח ללקוחות עצמם.

סמכויות האכיפה מתחלקות גם הן בין הסוכנויות השונות. סעיף 404 בחקיקת SOX מ־2002 מסמיך את הרשות לניירות ערך (SEC) להיות הרגולטור של סיכוני סייבר בחברות ציבוריות.[82] חברות אלו מוגדרות כחברות החייבות בדיווחים בעקבות עיסוקים בסחר בניירות ערך ואגרות חוב. בהקשר של סיכוני סייבר, החקיקה מחייבת דיווח שנתי מצד ארגונים להערכת אמצעי הבקרה שלהם לצמצום סיכונים. חקיקה זו עברה לאחר הקריסה של חברות Enron ו־WorldCom, אשר פגעה קשות באמון של משקיעים בחברות אמריקאיות.

חקיקה משמעותית נוספת אשר הסמיכה את הרשות הפדרלית להגנת הצרכן לאכוף רגולציה לצמצום סיכוני סייבר במגזר הפיננסי היא ה־Dodd-Frank מ־2010. החוק הורה על הקמת הרשות להגנת הצרכן והסמיך אותה לבדוק חברות ולקנוס אותן עקב יישום לקוי של אמצעי אבטחת מידע שהן מחויבות להם על סמך חקיקת GLBA.

יחד עם המודלים הקשיחים לרגולציה מדינתית מסורתית, יש גם הסדרי רגולציה עצמית עבור ארגונים העוסקים בסליקת כרטיסי אשראי. הסטנדרט להגנת מידע של תעשיית כרטיסי האשראי (Payment Card Industry Data Security Standard (PCI-DSS)), שעוצב על ידי החברות המרכזיות בשוק האשראי – American Express, Discover, JCB International, MasterCard, VISA – מכיל הנחיות להגנת המידע ואבטחתו במערכות לסליקת תשלומים בארגונים. ההסדר עוצב ב־2006 ומתעדכן מאז תדיר. בנקים אשר מספקים כרטיסי אשראי, חנויות מסחר המקבלות תשלומי לקוחות דרך כרטיסי אשראי ועסקים העובדים מול חברות האשראי, כפופים כולם להתקשרות חוזית המחייבת אותם לעמוד בסטנדרטים של הגנת מידע. ההסדרים עודכנו ב־2015 וכוללים מספר עולה של בקרות להגנת מידע, אשר בכל מקרה אינן מחליפות הנחיות מדינתיות רשמיות. הערכה של עמידה בתנאי הרגולציה מבוצעת על ידי בודקים מוסמכים שעברו הכשרה מתאימה ואכיפתם נעשית על סמך חוזים.[83]

3. רגולציה־עצמית: יתר המגזרים במשק

יתר המגזרים במשק פועלים על פי מודלים של רגולציה־עצמית, שבה למדינה יש תפקיד במתן מידע על איומים במרחב, פרסום הנחיות וולונטריות, כולל המלצות לצמצום סיכוני סייבר, ואכיפה במקרים של הונאה וסחר לא הוגן כתוצאה של היעדר הגנה מפני

---

82 Sarbanes-Oxley Act of 2002, 15 U.S.C $7262 (2002).

83 כמו למשל חוזים בין חברות האשראי לבנקים המספקים כרטיסי אשראי או בין בנקים לספקי שירותים העובדים עם כרטיסי אשראי.

סיכוני סייבר. ארגונים קובעים בעצמם סטנדרטים להערכה וצמצום של סיכונים ופועלים מתוקף החשש שללא אסדרה עצמית מתאימה, המדינה עלולה להשית רגולציה מחייבת או לחלופין לאכוף הגנת סייבר לקויה לטעמם דרך רשויות ה־FTC או ה־SEC. בשל כך נשען המשטר על מודלים של רגולציה־עצמית, אך גם בו תפקיד המדינה הולך ומתעצם בפעילויות אכיפה והתערבות גוברת מצד סוכנויות מדינתיות.

(א) בניית המשטר (מקור הסמכות והמבנה)

מסוף שנות התשעים, שבמהלכן החלה הכלכלה האמריקאית להתבסס על שירותים דיגיטליים, קידם הממשל מדיניות של אי־התערבות, בהנחה שכך תקודם צמיחתם של ארגונים המתבססים על עיבוד מידע באופן דיגיטלי. דרך תשתית המדיניות למסחר דיגיטלי מ־1997 (The Global Electronic Commerce Framework), הדגיש הנשיא דאז קלינטון את החשיבות שבאימוץ מודלים של רגולציה עצמית, ולא מדינתית, על פני ארגונים פרטיים.[84]

מאז הלכה כלכלה זו והתעצמה כתוצאה של גורמים מספר: הפרטות במשק שהובילו לכך שמידע אישי רב יוחזק בידי ארגונים פרטיים, טכנולוגיות מתפתחות של איסוף נתונים וניתוחם, אשר עודדו ארגונים לצבור מידע, והתקדמות ביכולות הקישוריות, שאפשרה לחברות לפנות לקהל רחב ולהשיג כוח והשפעה על הליך קבלת ההחלטות. ארגונים החלו לבסס את המודל העסקי שלהם על ניתוח מידע אישי, התאמת פרסומת ממוקדות ולכידת תשומת הלב של לקוחותיהם על סמך ניתוחים מתקדמים וחסויים של תחומי העניין וההעדפות האישיות של הצרכנים. הכוח המונופוליסטי שצברו כמה חברות במשק מקשה כיום על רגולטורים להטיל הנחיות מחייבות להגנה על מידע אישי וצמצום סיכוני סייבר במגזרים רבים. נוסף על כך, כשלי השוק בתחום הסייבר, היוצרים היעדר השקעה של ארגונים בצעדים לצמצום סיכונים, מערערים על אפקטיביות הרגולציה העצמית.[85]

הקונגרס נכשל באופן עקבי בהעברת חקיקה להגנת מידע שתגביל את יכולתן של חברות פרטיות לאסוף ולעבד מידע אישי ותרחיב את דרישות ההגנה מהן. על כן, הרגולציה המחייבת הינה מגזרית וללא רגולטור מרכזי. פעולות האכיפה של ה־FTC תקפות למצבים שנתפסים כ״סחר לא הוגן״ ומגבילות את זרוע האכיפה לצמצום סיכוני סייבר במגזרי המשק שאינם כפופים לרגולציה מחייבת.

ב־2011 עסקו קובעי המדיניות הפדרליים בכלל המגזרים בכלכלה הדיגיטלית, אך המשרד למסחר פרסם מסמך ובו הנחיות וולונטריות בלבד לניהול סיכוני סייבר במגזרים אלו.[86] ההנחיות כוללות תמריצים לארגונים להתמודדות עם איומי סייבר, צעדים

---

84 The White House, The Framework for Global Electronic Commerce (1997).

85 Nathan Alexander Sales, "Regulation Cyber-security", 107 *Northwestern University Law Review* (2013) 4.

86 ראו מסמך הנחיות מ־2011 של משרד המסחר בארצות הברית (לעיל, הערה 13).

להעלאת מודעות לסיכונים אלו ופעולות לקידום מחקר ושיתופי פעולה בין־לאומיים. מטרת ההנחיות הייתה ליצור שיתופי פעולה אשר יהפכו לסטנדרטים לאימוץ בכלל המגזרים.

המסמך כולל שתי המלצות מרכזיות: (1) יצירת גישה מדינתית אחידה למיגור סיכוני סייבר דרך נורמות משותפות, התוויית סטנדרטים וקידום אוטומציה בנושאי הגנת מידע; (2) מתן תמריצים להתמודדות עם סיכוני סייבר דרך כינון חוק פדרלי לחובת דיווח על נזקי סייבר, עידוד שיתוף מידע וקידום שוק ביטוח לנזקי סייבר העשויים לצמצם את הצורך ברגולציה מחייבת.

(ב) הערכת סיכונים

הערכת איומים במרחב הסייבר מבוצעת על ידי כמה יוזמות במגזר הפרטי. יוזמה ראשונה, Threat Exchange, מאפשרת ממשק בין מערכות שונות לשיתוף איומי סייבר ומונה כ־350 חברות.[87] המידע המשותף כולל אתרים זדוניים וכתובות אינטרנטיות של מקורות פוגעניים. מטרת השיתוף היא למנוע התפשטות נזק במרחב הסייבר על ידי התראה בזמן אמת לחברות רבות ונקיטת צעדים פרו־אקטיביים למניעה.

יוזמה נוספת היא ה־Cyber Threat Alliance, אשר יוצרת שיתוף פעולה בין ספקי מוצרים להגנת סייבר דרך מנגנונים אוטומטיים של שיתוף מידע, ובכך מאפשרת לכלל החברות להתמודד עם איומים שנצפו בכל אחת מהמערכות המותקנות אצל לקוחותיהן.[88] ב־2015 ניסתה המדינה לשפר את מנגנוני הערכת האיומים במגזר הפרטי דרך כינון החוק לשיתוף מידע בסייבר (The Cyber Information Sharing Act). החקיקה יצרה תשתית לשיתוף וולונטרי של מידע על אודות איומים ואמצעי ההגנה של ארגונים, תוך מתן תמריצים לחברות מסחריות דרך מנגנונים של פטור מאחריות לנזק כתוצאה של המידע המשותף. נוסף על כך, ב־2015 הורה הנשיא אובמה למחלקה לביטחון המולדת, באמצעות הוראה נשיאותית 13691, ליצור מנגנונים לשיתוף מידע עבור כלל המגזרים, ולא רק עבור מגזרים המוגדרים ״קריטיים״, מתוך הצורך לשיפור בהערכת הסיכונים הנשקפים למגזרים אלו מאיומים חיצוניים.[89]

---

87 עוד על המיזם, ראו: Facebook for Developers, ThreatExchange Documentation, 2018 (developers.facebook.com/programs/threatexchange) (לאחרונה באוגוסט 2018).

88 אחד מסיפורי ההצלחה הבולטים של מיזם שיתוף זה היה ה־Crypto Wall 3 Campaign, שבו חברות חברו יחדיו כדי להתמודד עם התקפת כופרה והגיעו לכ־870 פיסות מידע המזהות חד־חד ערכית את הנוזקה, מתוכן 165 פיסות מידע שהיו חדשות עבור הרשויות המדיניות. יחדיו הגיעו התעשייה והמדינה לכ־1,000 מזהים חזקים של הנוזקה ואילצו את התוקפים לפתח גרסה חדשה. ראו: Commission on Enhancing National Cyber Security, "Meeting Minutes: Security challenges in the Digital Economy", *University of California Berkley*, June 21st, 2016 [https://www.nist.gov/sites/default/files/june_21_2016_ucb_meeting_minutes.pdf] (נצפה לאחרונה באוגוסט 2018).

89 Executive Order No. 13691, "Promoting Private-sector Cybersecurity Information Sharing", February 13, 2015.

הערכת סיכונים פנימית לארגונים מבוצעת, בין היתר, על ידי שותפות עם קהילות המחקר דרך תוכניות לאיתור פרצות במערכות (Bug Bounty Programs), המאפשרות חדירה באופן חוקי למערכות על מנת לזהות מקומות הדורשים תיקון.[90] נוסף על כך, יש מקרים שבהם חברות מפתחות תשתיות חומרה או תוכנה הנמצאות בשימוש נרחב על ידי מסה קריטית של שחקנים במרחב. במקרים כאלו המדינה מתערבת על ידי בדיקה ודיווח לחברות על חולשות אפשריות במוצריהן. התערבות כזו נעשית על ידי החטיבה לביטחון מידע בסוכנות לביטחון לאומי בארצות הברית (The Information Assurance Directorate at the National Security Agency). כך למשל, החטיבה פנתה בעבר לחברת גוגל והזהירה מפני פרצות אפשריות במערכת ההפעלה אנדרואיד.[91]

(ג) צעדים לצמצום סיכונים ואכיפתם

המדינה יצרה את התשתית של ארגון הסטנדרטים הלאומי, NIST, לניהול סיכוני סייבר בתשתיות קריטיות, שאומצה באופן וולונטרי על ידי ארגונים פרטיים.[92] תשתיות סטנדרטים נוספות הנמצאות בשימוש במשק כוללות את ה־UL Cybersecurity Framework, ISACA, ו־Fast Identity Online Alliance. חברות פרטיות בוחרות אילו סטנדרטים לאמץ ולעיתים יוצרות בעצמן דרישות סף לצמצום סיכוני סייבר מאיומים חיצוניים ופנימיים לארגון.

אכיפה מבוצעת באופן חלקי על ידי ה־FTC, CFPB, וה־SEC. סוכנות ה־FTC עורכת גם סדנאות להדרכה והנחיה של ארגונים. ב־2018 פרסמה הרשות לניירות ערך (SEC) הנחיות על מידת השקיפות הנדרשת מחברות ציבוריות כלפי המשקיעים והציבור בכל הנוגע להתמודדותן עם סיכוני סייבר.[93] שקיפות זו כולל חובת דיווח בזמן סביר. אף על פי שהמסמך איננו מחייב, הוא מבהיר מהו המינימום הנדרש כי להימנע מפעולות אכיפה ועניש של הרשות. בעוד הרשות לניירות ערך מספקת באופן מסורתי הנחיות מחייבות עבור המגזר הפיננסי, היא השלימה לאחרונה באופן תקדימי פעולת אכיפה נגד חברת יאהו, שאיננה מספקת שירותים פיננסיים, וקנסה אותה ב־35 מיליון דולר.[94]

---

90 למשל, חברת פייסבוק אימצה תוכניות כאלו לשיפורה של הערכת הסיכונים הפנימית של הארגון ותיקנה לדבריה כ־2,400 בעיות אבטחה במערכותיה בתשלום של 4.3 מיליון דולר לחוקרים (לעיל, הערה 88).

91 שם.

92 על פי מחקר של חברת גרטנר, כ־30% מהחברות הפרטיות אימצו את תשתיות המדיניות להגנה של NIST. ראו: National Institute of Standards and Technology, Cybersecurity "Rosetta Stone" Celebrates Two Years of Success, 2016 [https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success] (נצפה לאחרונה באוגוסט 2018).

93 Commission Statement and Guidance on Public Company Cybersecurity Disclosers, 17 CFR Parts 229 and 249, February 26, 2018.

94 עוד על פעולת האכיפה של הרשות לניירות ערך מול חברת יאהו ראו: Zaid Shoorbajee, SEC Fines Yahoo Remnant Altaba $35 million for Failing to Disclose Breach, 2018

ד. דיון השוואתי

מבט השוואתי על משטרי הרגולציה שהתפתחו סביב המגזרים השונים מלמד על השונות המגזרית שבכינון רגולציה לצמצום סיכוני סייבר. טבלה מס׳ 1 מסכמת את עיקריהם של שלושת המודלים הרגולטוריים על סמך המסגרת האנליטית של המאמר, כפי שהוסברה בפרק השני.

טבלה מס׳ 1: מודלים רגולטוריים לניהול סיכוני סייבר בזירה הפדרלית בארצות הברית [1996–2018]

		<u>רגולציה-משותפת</u> [תשתיות קריטיות]	**<u>רגולציה-מדינתית</u>** [ספקי בריאות ופיננסים]	**<u>רגולציה-עצמית</u>** [מגזרים שאינם קריטיים]
מקור סמכות המשטר		חוקים פדרליים והוראות נשיאותיות.	חוקים פדרליים ייעודיים וחקיקה להסמכת הסוכנויות הרלוונטיות.	-
מבנה		המחלקה לביטחון המולדת כרגולטור-על האחראי על מודלים שיתופיים בין התעשייה למשרד הממשלתי הרלוונטי תוך שימוש במתווכים רגולטוריים ללא מטרות רווח לניטור ואכיפה.	סוכנויות מדינתיות המפקחות ממעל על נמעני הרגולציה.	מבני איגוד ושיתוף בין שחקנים פרטיים מתוך התעשייה.

[www.cyberscoop.com/yahoo-altaba-35-million-sec-fine/] (נצפה לאחרונה באוגוסט 2018).

		<u>רגולציה-משותפת</u> [תשתיות קריטיות]	**<u>רגולציה-מדינתית</u>** [ספקי בריאות ופיננסים]	**<u>רגולציה-עצמית</u>** [מגזרים שאינם קריטיים]
אחריות רגולטורית לצמצום סיכונים	**הערכת הסיכון**	מוסדות משולבים של המדינה והתעשייה לשיתוף מידע עבור הערכת איומים חיצוניים. תוכניות משותפות של המדינה והתעשייה להערכת סיכונים פנימיים.	מוסדות משולבים לשיתוף מידע להערכת איומים חיצוניים והנחיות מחייבות בחקיקה לאימוץ שגרות להערכת סיכונים פנימיים.	יוזמות פרטיות לשיתוף מידע עבור הערכת איומים חיצוניים, אימוץ וולונטרי של סטנדרטים שונים להערכת סיכונים מתוך הארגון והתערבות מדינתית במקרה של פיתוח תשתיות שירותים דיגיטליות נרחבות.
	צעדים לצמצום הסיכון	תשתית מדינתית מחייבת המיושמת על פי שיקול הדעת של התעשייה בעזרת מתווכים רגולטוריים פרטיים.	הנחיות מחייבות מתוקף חקיקה עם מקום לשיקול דעת עבור התעשייה ביישומן.	אימוץ וולונטרי של סטנדרטים מגופי תקינה שונים.
	ניטור ואכיפת הרגולציה	משתנים בהתאם למגזר הקריטי ומבוצעים על ידי מתווכים רגולטוריים וסוכנויות ממשלתיות.	ניטור קבוע ורחב על ידי סוכנויות מדינתיות ואכיפה הכוללת סנקציות אזרחיות ופליליות.	ניטור חלקי על ידי סוכנויות להגנת הצרכן ושוק ההון המבצעות גם את האכיפה על ידי ענישה אזרחית.

הספרות המחקרית על אודות רגולציה לניהול סיכונים מתחומים אחרים, שנסקרה בפרק הראשון של המאמר, מעידה על השפעתם של אינטרסים פרטיים והסדרים מוסדיים בכינון רגולציה לניהול סיכונים, יחד עם התערבות גוברת של המדינה בתחומים רבים. נוסף על כך, ספרות המנתחת את המורכבות שבניהול סיכונים בעידן המודרני מעידה על הצורך בהסתמכות על מספר רב של שחקנים לתיאום ופיתוח הידע הנדרש לניהול סיכונים.

הפסקאות הבאות בודקות את הממצאים העולים מן הספרות המחקרית, תוך בחינת שלוש השערות המחקר. הן מנסות להסביר את השונות במשטרים הרגולטוריים שיכולה לנבוע מהגורמים הבאים: (1) הצורך במומחיות ושיתוף שחקנים מהמגזר הפרטי לשיפורו של הליך ניהול הסיכונים על ידי המדינה; (2) השפעתם של הסדרים מוסדיים ונורמות מגזריות מקובלות על אופי הרגולציה בכל מגזר; (3) השפעתם של אינטרסים פרטיים על פני מגזרים שונים ובהקשר מדיניות שונה.

ראשית, אבדוק את הצורך במומחיות לניהול הסיכון וההישענות הפונקציונלית של המדינה על המגזר הפרטי. צורך זה משפיע באופן מובהק על כינון רגולציה סביב עולם התוכן המורכב של התשתיות הקריטיות; הוא גם מופיע בהסדרים להיוועצות והשפעה של המגזר הפרטי בכינון רגולציה בנושאי בריאות ופיננסים, ובהיעדר ההסדרים לניהול יתר המגזרים הנשענים על מומחיות בעולמות התוכן שלהם.

העיסוק בתשתיות קריטיות, שעוצב לראשונה בסוף שנות התשעים על ידי קובעי המדיניות, משקף התייחסות למומחיות המגזר הפרטי מן הרגע הראשון. דוח ועדת מארש מ־1996, קריאת הנשיא קלינטון מ־1998 לשילוב ידע מדינתי עם מומחיות עסקים פרטיים ואסטרטגיית הבית הלבן מ־2000, כולם מחדדים את הצורך במומחיות המגזר הפרטי ובכינון הסדרים רגולטוריים משותפים לשם כך. התפיסה הזו משתקפת במודלים לניהול סיכוני סייבר בתשתיות קריטיות על פני כלל המגזרים – הן במבנים המשותפים לכינון ההנחיות ויישומן והן במרכזי שיתוף הידע של המדינה, הנשענים על מומחיות פרטית לשיפור הערכת סיכונים. בנושאי אכיפה, שבהם אין למדינה צורך במומחיות מסוימת, יש פעילות של ארגונים להסדרת רגולציה עצמית, המתווכים בין המפקח למפוקחים ומאפשרים אכיפה המביאה בחשבון את צורכי המגזר הפרטי.

בנושאי בריאות ופיננסים עולה צורך מובהק פחות במומחיות המגזר הפרטי, אך על אף המבנה נוקשה, הרגולטור מאפשר לשחקנים פרטיים להשפיע על עיצובן של תקנות לניהול סיכונים במגזר הבריאות ומעודד גמישות ביישום ההנחיות במגזר הפיננסי. הסתייעות במומחיות המגזר הפרטי באה לידי ביטוי גם במרכזי שיתוף הידע הוולונטריים בשני התחומים. עם זאת, הצורך במומחיות לא הוביל ליצירת מבנים רגולטוריים משותפים. המומחיות הנדרשת במגזרים אלו היא בעיקר באופי השירות הפיננסי/הבריאותי שמספק כל ארגון מפוקח, והיא איננה נתפסת כמומחיות ייחודית עבור ניהול סיכוני סייבר המצריכה מודלים רגולטוריים שונים מהנהוג בעבר. עבור יתר המגזרים במשק, מומחיות המגזר הפרטי איננה נמצאת בליבת דיוני הרגולציה, אך מבני רגולציה־עצמית מאפשרים למפוקחים שיתופי פעולה עם קהילת חוקרים (דרך bug bounty programs) והישענות על מומחיות מבחוץ, כחלק מההסדרים העצמיים.

שנית, אבחן את השפעתם של הסדרים מוסדיים ונורמות מקובלות על כינון המודלים הרגולטוריים בכל מגזר. הסדרים שעוצבו לראשונה בהקשר של סיכוני סייבר, כגון התשתית המוסדית של אסדרת תשתיות קריטיות, נתנו משקל גדול למורכבות שבניהול

הסיכון ועוצבו על פיה. לעומת זאת, במגזרי הבריאות, הפיננסים ויתר הכלכלה־הדיגיטלית, ההסדרים והנורמות המקובלים מהעבר נתנו את הטון בכינון משטרים לניהול סיכוני סייבר והתפתחותם בהווה.

נורמות של רגולציה נוקשה בנושאי ביטחון לאומי ופיננסים באו לידי ביטוי במעורבות נרחבת של המדינה והשפעתה על קבלת ההחלטות של עסקים פרטיים. לעומת זאת, נורמות של היעדר רגולציה מחייבת כלפי המגזר הפרטי בנושאי הגנת מידע מסבירות את ההתמדה הרגולטורית בעיצובם של משטרי רגולציה־עצמית על אף הסיכונים המתפתחים בתחום הסייבר.

עבור תחום התשתיות קריטיות נוצר מלכתחילה מודל מוסדי משותף, המעניק סמכות למגזר הפרטי ולמדינה בכינון רגולציה. המבנה המוסדי התרחב מאוחר יותר וכלל הנחיה של רגולטור־על, המחלקה לביטחון המולדת, מול המשרדים השונים, אך שמר על שותפות באחריות רגולטורית כלפי סיכוני סייבר בין התעשייה למדינה. עם זאת, ההקשר של ביטחון לאומי, אשר נתפס ככזה שבו מוסדרות תשתיות המדינה להגנה מפני סיכוני סייבר, נתן לגיטימיות להתערבות מדינתית בקרב קובעי מדיניות ושחקנים פרטיים. הערכת סיכונים פנימית וחיצונית יוצאת לפועל בשיתוף פעולה עם המדינה, בעוד ניטור ואכיפה בחלק מהמגזרים מבוצעים דרך ארגונים להסדרת רגולציה־עצמית ללא מטרות רווח, אשר הוסמכו בעבר ונושאים תפקיד חשוב בהסדרים המוסדיים החדשים שנוצרו.

בתחומי הבריאות והפיננסים, הכפופים באופן מסורתי לרגולציה מדינתית נוקשה של פיקוד ושליטה, נשענת הרגולציה במובהק על המודלים שכבר קיימים בתחום. סמכויות האכיפה הנוקשות והניטור הנרחב נשמרים ומתרחבים גם כשהדבר נוגע לסיכוני הסייבר במגזרים אלה. החקיקות החדשות נוסחו בהתאם, אך עם זאת יש למידה ממודלים של תשתיות קריטיות ביצירת מרכזי שיתוף מידע להערכת איומים חיצוניים. המסורת הרגולטורית הנוקשה באה לידי ביטוי גם בהרחבה לאורך זמן של הארגונים הכפופים לרגולציה זו. סוכנויות קיימות מרחיבות את היריעה של הנחיותיהן ומוסיפות הנחיות לניהול סיכוני סייבר אצל המפוקחים המסורתיים שלהן.

עבור יתר המגזרים, היעדר הסדרים מוסדיים מאפשר לאינטרסים פרטיים לעצב את המשטר. היסטורית, החל מסוף שנות התשעים נקטה המדינה גישה של אי־התערבות בהגנה על מידע בקרב מגזרים שאינם קריטיים במשק. מסלול מדיניות זה לא השתנה מאז, על אף הסיכונים הגואים וכשלי השוק בתחום. לעיתים הסדרים מוסדיים ממגזרים אחרים מתרחבים וזולגים להסדרתם של כלל המגזרים במשק – כגון פעולות אכיפה מצד SEC ו־FTC – המעידים על התערבות מדינתית ההולכת וגדלה עם הזמן. עם זאת, התערבות זו עדיין איננה יוצרת רגולציה מדינתית משמעותית עבור מגזרים אלו.

שלישית, אבחן את השפעתם של אינטרסים פרטיים על פני הקשרי המדיניות השונים של ביטחון לאומי ופרטיות בהסדרת המגזרים השונים. הניתוח לאורך זמן מלמד כי אינטרסים פרטיים מצליחים להשפיע על כינון רגולציה ולעצבה הן בנושאי ביטחון

לאומי בהקשרי תשתיות קריטיות והן בנושאי פרטיות בהקשרי בריאות ופיננסים. בתחום התשתיות הקריטיות המדינה יוצרת מודלים משותפים שבהם לאינטרסים פרטיים יש משקל מכריע, בעוד בתחום הבריאות והפיננסים המדינה מחייבת היוועצות ויוצרת גמישות עבור המגזר הפרטי. הנעשה ביתר המגזרים מושפע גם הוא מאינטרסים פרטיים, ולמרות עשרות ניסיונות חקיקה בעבר, מגזרים אלו עדיין נתונים למודלים של רגולציה־עצמית.

בתחום התשתיות הקריטיות, הוראה נשיאותית מ־1998 מחדדת את הצורך למצוא חלופה לרגולציה של פיקוד ושליטה ולהתחשב באינטרסים של המגזר הפרטי, בעוד אסטרטגיית הבית הלבן משנת 2000 מבהירה כי למדינה אין סמכות למתן הנחיות נוקשות באופן שנוגד אינטרסים פרטיים. בתחום הבריאות והפיננסים, שחקנים פרטיים נהנים ממנדט לסייע למדינה לעצב תקנות בהתאם לדרישות הקונגרס וזוכים לגמישות ביישום ההוראות המחייבות.

אינטרסים פרטיים משפיעים גם במקומות המעטים שבהם אין מענה רגולטורי בתחומי הבריאות והפיננסים, כגון תחום השימוש בכרטיסי האשראי ומרכזי שיתוף מידע בנוגע לאיומים חיצוניים. בהיעדר הסדרה מוסדית, אינטרסים פרטיים מעצבים הסדרים־עצמיים בתחומים אלו. עבור יתר המגזרים, רגולציה־עצמית מקודמת על ידי שחקנים פרטיים כדי להימנע מרגולציה מדינתית. כוחן המונופוליסטי של חברות שירותים דיגיטליות יצר השפעה רבה על תהליכי קבלת ההחלטות ומונע מהקונגרס להעביר חקיקה מחייבת. נוסף על כך, כאשר הקונגרס מעביר חקיקה בנושאים הקשורים לכלל המגזרים, מוקמים מנגנונים וולונטריים הכוללים פטור מאחריות על מנת לתמרץ את המגזר הפרטי. יוצאים מן הכלל הם מקרים שבהם המגזר הפרטי עוסק בפיתוח תשתית רוחבית המשמשת מסה קריטית של משתמשים במרחב. במקרים אלה המדינה מתערבת ומסייעת למגזר הפרטי להעריך איומים פנימיים וחולשות אפשריות בתשתית שפותחה.

סיכום

התעצבות רגולציה לניהול סיכוני סייבר בממשל הפדרלי בארצות הברית בין השנים 1996 ל־2018 משקפת שונות רבה באשר לאופן שבו המדינה בוחרת לנהל סיכונים עבור החברה. דרך שלושה מודלים רגולטוריים של רגולציה־משותפת, רגולציה־מדינתית, ורגולציה־עצמית, הנבדלים זה מזה בסמכות, במבנה ובחלוקת האחריות בין המגזר הפרטי למדינה, מנהלת המדינה סיכוני סייבר במשק באופן שאינו עולה בקנה אחד עם ההסתברות למימוש הסיכון וחומרתו.

בעוד למומחיות יש השפעה על עיצובם של שלושת המשטרים הרגולטוריים, יחסי הגומלין בין אינטרסים פרטיים להסדרים מוסדיים הם המעצבים את האופן שבו סיכוני

סייבר מנוהלים עבור החברה. מאמר זה מחדד את החשיבות שבהבנת הפוליטיקה של ניהול הסיכונים של המדינה ומראה כיצד התבוננות רציונלית־פונקציונלית על התעצבות רגולציה ומדיניות ציבורית מסבירה רק חלק מהבחירות של קובעי המדיניות.

אסדרה של תחום התשתיות הקריטיות מעוצבת תוך מתן תפקיד רגולטורי חשוב לאינטרסים פרטיים, המשתקף הן בהסדרים המוסדיים המתעצבים והן ביכולות החקיקה, הניטור והאכיפה של המדינה. בתחומי הבריאות והפיננסים, שבהם התעצבו הסדרים מוסדיים טרם הצורך באסדרת סיכוני סייבר, הייתה לאינטרסים פרטיים השפעה מסוימת והם באו לידי ביטוי באזורים שהיו ממוסדים פחות על ידי רגולציה קודמת. עם זאת, הסדרים מוסדיים מסורתיים יצרו רגולציה נוקשה ומסועפת, באופן המטיל ספק באפקטיביות של מודלים אלו.

אסדרה של יתר מגזרי המשק נותנת, באופן היסטורי, מקום מרכזי להשפעת אינטרסים פרטיים. ההתלכדות בין הנורמות המוסדיות להשפעתם של אינטרסים פרטיים יוצרת קיפאון בעיצוב מדיניות ציבורית לניהול סיכוני סייבר ביתר המגזרים, על אף כשלי השוק ומפת האיומים המתעצמת. המדינה מצליחה להשפיע רק על ידי הרחבת הסדרים מוסדיים קיימים, במטלות רגולטוריות של ניטור ואכיפה ובאופן חלקי בלבד.

בחינת השערות המחקר מאששת את הספרות המחקרית על אודות רגולציית סיכונים מתחומים אחרים. מערכת היחסים שבין הנורמות הממוסדות להשפעתם של שחקנים פרטיים מנבאת את אופי הרגולציה המתפתח ומטילה ספק ביכולתה של המדינה להתמודד עם סיכונים מורכבים מטכנולוגיות מתפתחות. סיכונים אלו דורשים מענה רגולטורי גמיש, מהיר ורך, בהתאם לקצב המהיר של התפתחותן. לאור זאת, המאמר מחדד את הצורך בהבנה ויצירת מודלים רגולטוריים אדפטיביים, שאינם נשענים על גורמים היסטוריים המעכבים את התפתחותם, על מנת להתמודד בהצלחה עם סיכוני הסייבר עבור החברה.

נספח 1

מדידה של הערכה, ניהול ואכיפה של רגולציית סיכונים

	<u>הערכת סיכון</u>: כיצד נוצר הסיכון ועל ידי מי?		**<u>צעדים לצמצום הסיכון</u>**	**<u>ניטור ואכיפת הרגולציה</u>**
	איומים חיצוניים	איומים פנימיים	בניית יכולת להערכת סיכונים ופיקוח, בניית מומחיות, עיצוב נקודות בקרה למניעת הסיכון, התאוששות מנזק.	צעדי בקרה, הרתעה ועניישה מצד הרגולטור.
תשתיות קריטיות				
ספקי שירותי בריאות ופיננסים				
יתר מגזרי המשק				