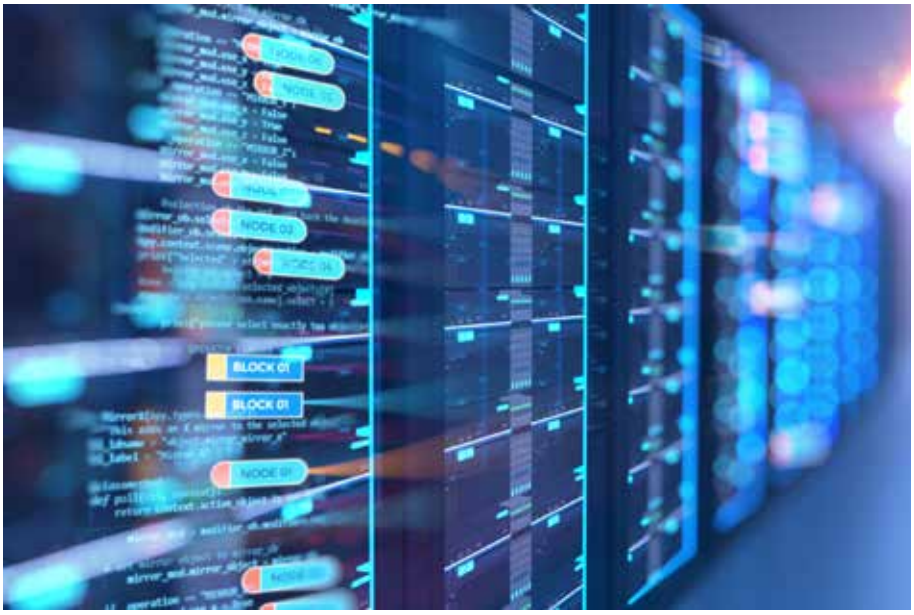
המדינה כסוכן כפול –
ביטחון לאומי מול פרטיות בראי תפקיד המדינה במרחב הסייבר בארצות־הברית

עידו סיון־סביליה

כיצד מַבנות החקיקה והרגולציה בארצות־הברית את מערכת היחסים בין ביטחון לאומי לפרטיות בעידן הדיגיטלי? כדי לענות על שאלה זו יצר המחבר מאגר מידע המכיל את כל החוקים הפדרליים וההנחיות הרגולטוריות הרלוונטיות (סך הכול 86 מופעים) שפורסמו בין השנים 1967 ל־2016. כל מופע של מדיניות סווג על פי מידת הסתירה או ההלימה שהוא מייצג בין ביטחון לאומי לפרטיות. הממצאים מלמדים על תמורות בעדיפות של ביטחון לאומי על פני פרטיות לאורך שלוש תקופות שונות, לפני ואחרי העידן הדיגיטלי, ועל פערים משמעותיים בקידום ביטחון לאומי ופרטיות במגזר העסקי־אזרחי. את הממצאים הללו ניתן להסביר באמצעות שלושה גורמים: הראשון – תפקידן המשתנה של קבוצות עסקיות בקידום ביטחון לאומי ופרטיות במרחב הסייבר, הכולל ניתוק האינטרסים החופפים בין המגזר העסקי לחברה האזרחית; השני – יחסי כוחות א־סימטריים לטובת הרשות המבצעת לעומת הקונגרס; השלישי – השפעתם המכרעת של סוכנויות ביטחון ומונופולים של טכנולוגיה המעכבים קידום מדיניות להגנת סייבר לשם חיזוק הביטחון הלאומי והפרטיות גם יחד. מחקר זה מתחקה באופן אמפירי אחר תפקידה הכפול והפרדוקסלי של המדינה בתחום הסייבר: מחד גיסא, המדינה משקיעה מאמצים רבים בקידום הגנת סייבר, שמירה על הפרטיות והגנה על הביטחון הלאומי. מאידך גיסא, המדינה מנצלת את מרחב הסייבר לצורכי איסוף מידע תוך פגיעה בפרטיות, על מנת להשיג מטרות "נעלות" יותר של ביטחון לאומי.

מילות מפתח: ביטחון לאומי, פרטיות, הגנת סייבר, רגולציה, ניהול סיכונים



iStock

מבוא

שאלת המחקר של מאמר זה מתמקדת באופן שבו הממשל הפדרלי בארצות־הברית מבנה את מערכת היחסים בין ביטחון לאומי לפרטיות בעידן הדיגיטלי. מחד גיסא, הטכנולוגיה מאפשרת למדינה לבצע מעקב המוני ומעמיקה את הקונפליקט בין ביטחון לאומי לפרטיות. מאידך גיסא, הטכנולוגיה מספקת תשתית שדרכה ניתן לקדם בו־זמנית ביטחון לאומי ופרטיות, דרך חיזוק הגנת הסייבר של מערכות הממשל הפדרלי ומערכות רגישות ממגזר הפיננסים והבריאות, המכילות מידע אישי למכביר. המאמר מוצא כי ביטחון לאומי ופרטיות מתנגשים ומשלימים זה את זה ובכך מאפשרים לחשוף את תפקידה הכפול של המדינה, שבעידן הדיגיטלי מקדמת את הגנת הפרטיות ופוגעת בה כאחת. סקירת ספרות בנושא מלמדת כי מאמצי המדינה לקידום הגנת הפרטיות במרחב הסייבר ומידת ריסון הכוח של הרשות המבצעת בעידן הדיגיטלי טרם נחקרו באופן אמפירי מעמיק. מחקר זה שואף למלא חלק מחלל זה ושואל מתי יש הלימה או סתירה בין שתי המטרות הללו לאורך זמן. מטרת המאמר היא להבהיר כיצד שתי מטרות משלימות ומנוגדות מתייחסות זו לזו לאורך זמן בהליכי מדיניות ציבורית במדינה דמוקרטית.

מבחינה מתודולוגית המאמר מתחקה אחר חקיקה פדרלית, הוראות נשיאותיות, הנחיות מסוכנויות מדינתיות, אסטרטגיות מדיניות ופסיקות בית משפט חשובות בזירת המדיניות הפדרלית בארצות־הברית בין השנים 1967 ל־2016 (86 מופעים), ומסווג

מופעי מדיניות אלו על פי מידת ההלימה או הסתירה בין ביטחון לאומי לפרטיות. בהמשך יוסברו ההגדרות של ביטחון לאומי ופרטיות שהמאמר מאמץ, וכן הדרך המתודולוגית למדידת ההלימה או הסתירה בין השניים. למען הבהירות יצוין כי מאמר זה בוחן הן את מאמצי המדינה בנושא הגנת הסייבר והפרטיות כגורמים חשובים בקידום הביטחון הלאומי, והן את איסוף המידע על חשבון הפרטיות, המבוצע למען הגברת הביטחון הלאומי. הממצאים מצביעים על שינוי מדיניות ושימת דגש רב יותר על הביטחון הלאומי על חשבון הפרטיות, החל מאמצע שנות התשעים. מדיניות זו נצפתה בכל אחת מרשויות הממשל הפדרלי: הרשות המבצעת, אשר הוגבלה באופן ניכר על ידי הקונגרס בשנות השבעים, מאפשרת מאמצע שנות התשעים מעקב מדינתי על חשבון פרטיות באמצעות החלטות בתי משפט מעוררות מחלוקת שהתקבלו בדלתיים סגורות, ועל ידי התערבות בארכיטקטורה של מוצרים טכנולוגיים על מנת לאפשר מעקב מדינתי מתמיד, עם איזונים ובלמים שאינם אפקטיביים במידה מספקת.[1] הרשות המחוקקת שינתה את תפקידה מגורם מאזן המנסה לפשר בין ביטחון לאומי לפרטיות במהלך שנות השבעים והשמונים, לגורם שמעביר חוקים המעודדים איסוף מידע על ידי המדינה וללא יכולת אכיפה משמעותיות על המגזר העסקי, הנשען גם הוא על איסוף כזה. הרשות השופטת, שבשנות השבעים והשמונים הובילו פסיקותיה לחוקים חשובים שעודדו הגנה על הפרטיות, אינה מצליחה מאז להשפיע באופן מהותי על סדר היום בנושא.

באופן מפתיע, הספרות בנושא הליכי המדיניות והרגולציה המתעצבים סביב הגנת הסייבר והפרטיות מצד אחד ואיסוף מידע למטרות ביטחון לאומי מנגד היא מצומצמת לרוב, ואינה כוללת התחקות אחר קבלת ההחלטות בנושא. חוקרים אחדים מתייחסים לסתירה הזו בתפקיד המדינה, כאשר המחקרים בתחום מספקים הסברים מוגבלים על הגורמים למגמת מדיניות זו.[2] חוקרים אחרים עוסקים רק בתפקיד אחד של המדינה: בתחום הגנת המידע[3] או הגנת סייבר והביטחון הלאומי,[4] אך מספקים הסברים צרים עבור תקופת זמן קצרה של קבלת החלטות בנושא. מחקר זה, לעומת זאת, מביא בחשבון ביטחון לאומי ופרטיות כחלקים חשובים מתוך השלם, ועוקב אחר תהליכי המדיניות המעצבים את הסתירה וההלימה ביניהם במשך כחמישה עשורים. נוסף על כך, הוא תורם להבנה של תפקיד המדינה בעידן הדיגיטלי ומספק מסגרת אנליטית שדרכה ניתן להבין את עושר התקנות והחוקים שמבנים את מערכת היחסים בין ביטחון לאומי לפרטיות עבור החברה. על אף הטענות החוזרות ונשנות על נסיגתה של המדינה בעידן הניאו־ליברלי, אנו עדים להתערבות מדינתית משמעותית בעיצובה ובהסדרתה של מערכת יחסים חשובה זו.

הממצאים שיוצגו בהמשך קוראים תיגר על ההנחה שמתקפות הטרור ב־11 בספטמבר 2001 היו הסיבה העיקרית להעדפת הביטחון הלאומי על פני הפרטיות בארצות־

הברית. למרות שלאחר המתקפות הצהיר משרד המשפטים האמריקאי על שינוי באסטרטגיית המדיניות שלו – ממזעור נזקי פשיעה למניעה כוללת דרך מעקב ואיסוף מידע שיטתי,[5] ניכרת נטייה לדגש רב יותר על הביטחון הלאומי על חשבון הפרטיות כבר בשנות התשעים. המלחמה בטרור אומנם עודדה מגמה זו, אך היו גורמים נוספים כגון אינטרסים עסקיים, יחסי הכוחות בין הרשות המבצעת מול המחוקקת והשפעתם הגוברת של סוכנויות מודיעין ומונופולים של טכנולוגיה על פרטיות האזרחים החל מאמצע שנות התשעים, שתרמו לחוסר איזון זה.

המאמר מחולק לארבעה חלקים. החלק הראשון מספק מסגרת מושגית להבנת מערכת היחסים בין ביטחון לאומי ופרטיות דרך המִשׂגה של פרטיות, ביטחון ומעקב. בהמשך מובאת סקירת הספרות התיאורטית על המדינה כמנהלת סיכונים המַבנה את מערכת היחסים בין ביטחון לאומי לפרטיות, כולל פירוט המתודולוגיה למדידת מערכת היחסים הזו לאורך זמן. החלק השלישי כולל את הממצאים ודן בשני תפקידיה השונים של המדינה – ניצול מרחב הסייבר עבור קידום הביטחון הלאומי על חשבון הפרטיות וההגנה על מרחב הסייבר. בכך מקדמת המדינה את הגנת הפרטיות והביטחון הלאומי גם יחד. החלק הרביעי מסכם תוך דיון על הממצאים והמלצות להמשך.

הגדרת מושגי יסוד

ביטחון, פרטיות ומעקב הם מושגי יסוד להבניית הניתוח והדיון במאמר. אפשר להבין מושגים אלו באופנים שונים, ומטרת חלק זה היא להבהיר את הגדרות שהמאמר מאמץ עבור המדידה, בהמשך.

ראשית – המושג 'פרטיות'. בניגוד גמור לאופן הבלתי מספק שבו פרטיות מקודמת בשדה המדיניות הציבורית בארצות־הברית,[6] כלומר באופן מגזרי בלבד ודרך מודלים של רגולציה עצמית עם אכיפה חלקית, פרטיות כזכות מופיעה עוד בתיקון הרביעי לחוקה האמריקאית ונכתבה עליה ספרות ענפה. קבוצת הגדרות אחת ממשיגה פרטיות דרך החשיבות של המיקום פיזי המאפשר את השגתה, כלומר פרטיות היא פונקציה של מקום, ועל פי הגדרה זו אדם זכאי לפרטיות מלאה בביתו. קבוצת הגדרות אחרת מגדירה פרטיות כמידת השליטה של מושאי המידע על המידע האישי שלהם. יש הסבורים כי פרטיות עוסקת בחופש הגוף והמחשבה, ולאו דווקא במקומו הפיזי של היחיד או במידע האישי על אודותיו. בייגרייב מנסה להסדיר את בליל ההגדרות לעיל ומבנה את המשגת הפרטיות סביב ארבע קבוצות מרכזיות. הראשונה עוסקת באי־התערבות ומדברת על כך שפרטיות היא היכולת לכבד את רצונו של היחיד שלא להיחשף (הראשונים שהגדירו זאת כך היו וורן וברנדיס ב־1890).[7] הקבוצה השנייה עוסקת במידת השליטה של מושאי המידע על המידע האישי שלהם.[8] לקבוצה השלישית שייכים אלו הממשיגים פרטיות דרך אופן הגישה אל היחיד, וטוענים כי פרטיות נוגעת

לאינטימיות הגוף ולחופש המחשבה. גביסון מגדירה את אופני הגישה הללו דרך שלושה ממדים – סודיות המידע האישי, בידוד בהתאם לרצונו של אדם ואנונימיות.[9] קבוצה זו דוגלת בהמשגה רחבה של המושג המכלילה גם בריאות נפשית, אוטונומיות, צמיחה, יצירתיות והיכולת של יחידים ליצור יחסים משמעותיים. ללא פרטיות, על פי הגדרה זו, היחידים אינם שולטים ביכולת ההצגה העצמית שלהם, או באופן שבו הם מנהלים מערכות יחסים חברתיות. קבוצת ההגדרות הרביעית עוסקת בהמשגה של פרטיות דרך מידע אינטימי. אינס טוענת כי פרטיות היא היכולת לשלוט על קבלת החלטות אינטימית ברמת היחיד.[10] למטרות מאמר זה נבחרה התמקדות בקבוצת ההגדרות השנייה, הממשיגה פרטיות דרך שליטה על המידע האישי. עם זאת, לפרטיות כמושג יש מסגרת רחבה יותר כאשר ההגדרות לעיל אינן בלתי תלויות. למען הפשטות תעלה בהמשך טענה שהפרת הפרטיות היא איסוף מידע אישי שאינו חוקי או שקוף, והיא אינה מחייבת הוכחת נזק למושא המידע.

המושג 'ביטחון' חמקמק ורחב לא פחות. בניגוד לפרטיות, ביטחון נתפס באופן מסורתי כמטרת מדיניות דומיננטית אשר לאורה מתעצבים שדה המדיניות הציבורית, דעת הקהל, יחסי כוחות ותקציבים ציבוריים.[11] הפילוסוף הפוליטי תומאס הובס ראה בביטחון את המטרה העליונה של הריבון. ולדרון מרחיב הגדרה זו מעבר לביטחון פיזי. הוא טוען כי ביטחון מאפשר ודאות, שחרור מפחדים ושקט נפשי עבור היחידים. לטענתו, ביטחון הוא התשתית שדרכה יחידים יכולים ליהנות מזכויות אחרות.[12] הפילוסוף הפוליטי ג'ון לוק היה ככל הנראה הראשון שהגדיר את המתח בין ביטחון לחירות. הבטחת חירויות, לטענתו, אינה מספיקה ללא הביטחון שיאפשר ליהנות מהן. אך אם הביטחון עצמו פוגע בחירות, מתערער הרציונל לקדמו מלכתחילה. ולדרון ממשיך ומבדיל בין שני סוגים של ביטחון – ביטחון ברמת היחיד, שאותו הוא מגדיר כביטחון של זכויות אדם המושג על ידי התערבות מדינתית לרוב. יחידים, במקרה זה, מבינים כי על מנת להבטיח מבנים מדינתיים וחברתיים שישמרו על ביטחונם, עליהם "לשלם מס" כלשהו. ביטחון זה הוא מעבר לביטחון פיזי ונוגע בביטחון תרבותי וחברתי, וביכולתו של היחיד לחיות את חייו על פי רצונו. לעומת זאת, ביטחון ברמת הקבוצה מתייחס לביטחון המדינה, מוסדותיה והפיזור של ביטחון באוכלוסייה. סוג זה של ביטחון מעמיד בפני היחיד שאלות באשר לאילוצים שהוא מוכן לשאת עבור הביטחון הקולקטיבי. היחיד עלול לשאת במחיר שאינו בהכרח מבטיח שיפור בביטחונו האישי, אלא תורם לביטחונם של אחרים באוכלוסייה. מאמר זה מאמץ את הגדרת הביטחון ברמת הקבוצה, כאשר ההבחנה הזו בין ביטחון אישי לקבוצתי שימושית עבורו והיא תידון שוב בסיכום.

לאחר העיסוק בשני מושגי היסוד 'ביטחון' ו'פרטיות' יידון המושג 'מעקב', שהוא למעשה אחת הדרכים השגורות להגברת הביטחון הלאומי על חשבון הפרטיות.

התפיסה הרווחת קושרת בין מעקב למודרניות ומשתמשת במושג להסברת בעיות פרטיות בעידן הדיגיטלי.[13] מעקב אינו מתקשר בהכרח למידע אישי במרחב הפרטי, אלא לאיסוף מידע שיטתי ולניתוח התנהגויות של יחידים לצורך חיזוי פעולותיהם. בעידן הטכנולוגי הפך המעקב לכלי בידי מדינות ושחקנים פרטיים, המשמש למְשמוּעַ אזרחים ולהבניית צורות חדשות של ממשליוּת. הצידוקים לשימוש במעקב כוללים ביטחון אישי וקולקטיבי וביטחון מפני טרור ואי־סדר ציבורי. השפעות המעקב על אזרחים אינן נוגעות רק לפרטיותם, אלא גם להזדמנויות הנקרות בפני היחיד ולסגנון החיים שהוא בוחר לאמץ. כשמדובר במעקב, פרטיות נראית לפתע כמושג מוגבל שאינו מתאר כהלכה את איסוף המידע השיטתי בחיים המודרניים. המשׂגה של פרטיות התאימה לעידן שבו החברה עברה מנייר למאגרי מידע ממוחשבים, אך היא אינה מתאימה לעידן שבו קיימות מערכות האוגרות מידע על כל הפעילות היום־יומיות שלנו. המושג 'מעקב' יובא במאמר זה על מנת לתאר את ההפרה השיטתית של פרטיות על ידי מוסדות מדינתיים וחברות פרטיות, ללא הסכמה מצד מושאי המעקב.

סקירת ספרות ומתודולוגיה

מערכת היחסים הסבוכה בין ביטחון לפרטיות היא נגזרת של ספרות תיאורטית רחבה יותר בנושאי ביטחון וחירות בחברות מערביות.[14] ההבחנה בין ביטחון אישי וקולקטיבי חושפת חלק מהמורכבות. בעוד ביטחון קולקטיבי הוא התשתית שדרכה יחידים נהנים מחירות, האגרסיביות שנוקטות מערכות מדיניות נגד איומי ביטחון קולקטיביים היא אנטי־תזה לחירות, ועומדת בסתירה לביטחון. על כן ביטחון ופרטיות אינם בלתי תלויים זה בזה, ולשניהם יש ערך חברתי וקולקטיבי בחברה.[15] עם התרחבות מרחב הסייבר והתלות של חברות מודרניות במרחב הדיגיטלי, התעצם אתגר השמירה על פרטיות וביטחון. איומים מסורתיים מתחום הביטחון הפיזי התאימו עצמם לסביבה החדשה. פשיעת סייבר, חברות פריצה מסחריות וריגול מדינתי תרמו כולם לחוסר הביטחון במרחב החדש. באותה נשימה, ממשלות וחברות מסחריות מנצלות יכולות טכנולוגיות על מנת לאסוף מידע ולבצע מעקב, וכן לקדם ביטחון, יעילות ואינטרסים מסחריים על חשבון הפרטיות. מאמר זה מתחקה אחר המטרות המתנגשות והמשלימות הללו ומנסה להבין את תפקידה הכפול של המדינה כמקדמת ביטחון לאומי ופרטיות דרך הגנת הסייבר והמידע מצד אחד, אך בה בעת היא אוספת מידע למטרות ביטחון לאומי על חשבון הפרטיות.

באופן מפתיע, התפקיד הכפול של המדינה כמנהלת סיכונים עבור החברה בעידן הדיגיטלי אינו נחקר כמעט בספרות המדיניות הציבורית. חסרה המשגה והבנה של תהליכי קבלת ההחלטות סביב שתי מטרות חשובות אלו. דייברט ורוהוזינסקי[16] מתייחסים לסתירה הזו ומפרידים בין סיכונים ל'ביטחונו של מרחב הסייבר', המטופלים

על ידי סטנדרטים והגנה על שלמות ואמינות המידע, לבין סיכונים הנשקפים מ'שימוש במרחב הסייבר' לקידום מטרות אחרות. הם מתארים כיצד מדינות נוטות לבצע דיכוי פוליטי ולפגוע בפרטיות ובביטחון המידע של יחידים על מנת להבטיח יציבות ושמירה על הסדר החברתי הקיים, ומציעים הבחנה חשובה באשר לסתירה בתפקידיה השונים של המדינה בעידן הדיגיטלי. עם זאת, הבחנה זו אינה מספקת הבנה לגבי מקור הסתירה הזו בהליכי המדיניות וההסדרה סביב הנושאים הללו. מנדז ומנדז[17] מספקים הסברים קונקרטיים יותר על הליכי המדיניות מאחורי הקונפליקט בתפקיד המדינה. הם מביאים בחשבון חוקים ורגולציות אשר מקדמים את הפרטיות ובה בעת מאיימים עליה, וטוענים שבשני התפקידים הללו יש ריכוז כוח מדינתי. בהסברם הם מדגישים את האיום המסחרי על ארצות־הברית מצד חוקי הפרטיות האירופיים, ורואים בכך את התמריץ לשינוי המדיניות המתירנית בנושאי פרטיות להתכנסות ואכיפה על ידי סוכנות פדרלית מרכזית בדמות ועדת הסחר הפדרלית (FTC). בהמשך הם מנסים להסביר פגיעה בפרטיות למטרות ביטחון לאומי דרך העיסוק באיומים חדשים בדמות המלחמה בטרור, אשר הובילו לפתרונות הפוגעים בפרטיות ללא פיקוח מצד הקונגרס. אומנם יש כאן עיסוק חשוב בסתירה סביב תפקידה של המדינה, אך הדבר נעשה דרך מחקר אמפירי מצומצם. אין התייחסות לשינויים בזירה הפדרלית לאורך זמן, ואין הם בוחנים מדיניות הגנת סייבר כמקדמת פרטיות וביטחון לאומי יחדיו. נקודת המבט המצומצמת הזו מונעת מהמחברים להביא בחשבון שגורמים אחרים מלבד מתקפות ה־11 בספטמבר 2001 הובילו לפגיעה בפרטיות, והם גם אינם עוסקים במקומם של אינטרסים עסקיים במרחב הדיגיטלי. אם מתקפות הטרור של 2001 הן אכן הגורם המרכזי להפרת האיזון בין ביטחון לאומי לפרטיות, מדוע אנו רואים דומיננטיות של ביטחון לאומי על פני פרטיות כבר באמצע שנות התשעים? מה היה התפקיד של הרשויות הפדרליות השונות בכינון מדיניות בנושא?

מלבד החוקרים הללו, העוסקים בשני תפקידי המדינה כשומרת ומגינה על הפרטיות והביטחון מחד גיסא ואוספת מידע להגברת הביטחון הלאומי מאידך גיסא, יש ספרות לא מעטה העוסקת בהיבט אחד של תפקיד המדינה בעידן הדיגיטלי, ולא במערכת היחסים הכוללת. אלו העוסקים בפרטיות ובהגנת מידע מסבירים את חוסר הפרטיות דרך האופן שבו נתפסת פרטיות כערך אישי ולא ציבורי בקרב מקבלי ההחלטות, או כתוצאה מהיעדר יכולות מוסדיות לקידום פרטיות ברמה הפדרלית.[18] בעוד המחקרים הללו מעשירים את הידוע על הליכי המדיניות, הם אינם מעודכנים ומתמקדים בשנות השבעים והשמונים בלבד. מה שחוקרים אלו ראו כהגנת מידע בלתי מספקת מובן היום כ'תור הזהב' של הגנת הפרטיות בארצות־הברית, שאחריו הגיעו הפרות פרטיות רציניות על ידי המדינה והמגזר הפרטי. מחקר מאוחר יותר של ניומן ובאך מנתח את התמריצים לכינון רגולציה עצמית בנושאי הגנת מידע בארצות־הברית.[19] הטענה העולה

ממחקר זה היא העובדה שהיעדר איומים משמעותיים ועלויות רגולציה גבוהות יצרו שיתופי פעולה תדירים בתעשייה, על מנת להימנע מרגולציה מדינתית. בעוד ניומן ובאך מאירים את עינינו בנוגע לגישת השוק האמריקאית, איננו מבינים מדוע גישה זו אומצה מלכתחילה בנושאי פרטיות. החוקרים אינם מתייחסים להשלכות הקשות על הפרטיות שהיו למודל הרגולציה העצמית של חברות מסחריות, אשר הוביל למסחור במידע אישי שאנו עדים לו כיום. לבסוף, חוקרים העוסקים בהיבט הגנת הסייבר כדרך לקידום הפרטיות אינם מקדמים את ההבנה על הליכי המדיניות בנושא. עציוני[20] מסביר את ההשלכות הנובעות מחוסר הרצון של שחקנים פרטיים לקבל על עצמם מחויבות רגולטורית. הילר וראסל[21] מסבירים באופן מעומעם את מודל הרגולציה העצמית דרך התרבות הרגולטורית האמריקאית, שבאופן מסורתי נוטה לטובתם של עסקים. לעומתם, מחקרם החשוב של במברגר ומוליגן שמנסה ללמוד את השדה מעבר להנחיות הרגולטוריות מגלה שבאופן מעשי, הגמישות והוואקום הרגולטורי סביב הגנת המידע מייצרים שיח עשיר והגנת מידע על ידי קציני פרטיות בשטח (Data Protection Officers), מעבר לנדרש על ידי המדינה.[22] עם זאת, מושא המחקר של מאמר זה הוא המדינה, והגישה המחקרית המוצעת היא לנסות להבין כיצד המדינה, כישות בפני עצמה, מבנה את מערכת היחסים בין ביטחון לאומי לפרטיות. אומנם ייתכן שחברות מסוימות מנצלות את הגמישות הרגולטורית להנחיות מחייבות יותר, אולם אחרות משתמשות בגמישות זו כדי להשקיע את המינימום בהגנת המידע ובפרטיות לקוחותיהן. על כן, בחינה של הרגולציה וההנחיות המדינתיות היא הבסיס להבנת תפקידה של המדינה במרחב.

סקירת הספרות מלמדת כי חסרים מחקרים המתייחסים לתפקידה הכפול של המדינה בעידן הדיגיטלי לאורך זמן. חסרה התייחסות לביטחון לאומי ולפרטיות כאל שני חלקים המרכיבים את השלם, אשר מתייחסים זה לזה בסתירה ובהלימה בו־זמנית. על כן, לצורך התחקות אחר מערכת היחסים בין הביטחון הלאומי לפרטיות ברמה הפדרלית בארצות־הברית, מאמר זה מתבסס על מאגר מידע מקורי המכיל 86 'מופעי מדיניות', המוגדרים ככלל מסמכי החקיקה והרגולציה הרלוונטיים בין השנים 1967 ל־2016 – חקיקה ראשית, חקיקת משנה, הוראות נשיאותיות, פסיקות בית משפט חשובות, החלטות של המועצה לביטחון לאומי ומסמכי אסטרטגיה. כל מופע מדיניות כזה מתייחס לאיסוף מידע על ידי המדינה למטרות ביטחון לאומי על חשבון הפרטיות; להגבלות מטעמי הגנת הפרטיות על האופן שבו המדינה יכולה לאסוף מידע לצורכי ביטחון לאומי; לדרכים אפשריות לקידום הגנת המידע והסייבר, שיקדמו הן את הביטחון הלאומי והן את הפרטיות בעידן הדיגיטלי. על כן, הגישה המתודולוגית של מאמר זה היא רחבה ועוסקת בנושאי ביטחון לאומי, אכיפת חוק והגנת סייבר, המגדירים יחדיו את האופן שבו המדינה מבנה את מערכת היחסים בין הביטחון

הלאומי לפרטיות בעידן הדיגיטלי. גישה זו מאפשרת הבנה נרחבת באשר לדינמיקה בין הביטחון הלאומי לפרטיות ולתפקידה הכפול המדינה. נקודת הפתיחה לבחינת האירועים נבחרה להיות החלטת בית המשפט העליון מ־1967 (Katz vs. The United States), אשר העניקה לראשונה הגנה חוקתית עבור הזכות לפרטיות.[23] החלטה זו יצרה תגובת שרשרת של כינון מדיניות בנושאי ביטחון לאומי ופרטיות, אשר עיצבה את הזירה הרגולטורית כפי שאנו מכירים אותה עד היום.

כל מופע מדיניות במאגר המידע סווג בהתאם, על פי שלוש קטגוריות שונות הבונות את מערכת היחסים בין ביטחון לאומי לפרטיות, כפי שמראה הטבלה הבאה:

טבלה 1: סיווג אירועי מדיניות על פי מערכת היחסים הרעיונית בין ביטחון לאומי לפרטיות

		פרטיות	
		+	−
ביטחון לאומי	+	**הלימה בין הביטחון הלאומי לפרטיות (33 מופעים):** רגולציה ומדיניות העוסקת בהגנת הסייבר והמידע, אשר מחזקת את הביטחון הלאומי ואת הפרטיות בו־זמנית (למשל: התוויית תקנים להגנה על מערכות הבריאות, הפיננסים והממשל).	**ביטחון לאומי על חשבון הפרטיות (31 מופעים):** מדיניות ביטחון לאומי ואכיפת חוק ברובה, שמקדמת איסוף מידע ומחלישה תשתיות טכנולוגיות למטרות ביטחון לאומי על חשבון פרטיות (למשל: 'חוק הפטריוט' מ־2001 המתיר איסוף מידע נרחב לצורכי ביטחון לאומי, על חשבון הפרטיות.
	−	**פשרה בין הביטחון הלאומי לפרטיות (21 אירועים):** מופעי מדיניות המגבילים איסוף מידע על ידי המדינה לצורכי ביטחון לאומי (למשל: חוק מ־1978 המייצר מנגנוני איזונים ובלמים לאיסוף מידע של סוכנויות מודיעין).	

הקטגוריה **הראשונה** של האירועים כוללת מופעי מדיניות בין השנים 1984–2016 שמחזקים בו־זמנית ביטחון לאומי ופרטיות בעידן הדיגיטלי, דרך הגנת הסייבר והמידע (33 אירועים). אלו בעיקר חוקים ורגולציות המקדמים את הגנת הסייבר והמידע במערכות הממשל, הבריאות והפיננסים. הקטגוריה **השנייה** של מופעי המדיניות כוללת אירועים מן השנים 1976–2015 שמרחיבים את היכולות של מדינה לאסוף מידע למטרות ביטחון לאומי על חשבון הפרטיות (31 אירועים). אלו בעיקר הנחיות וחוקים המסייעים לסוכנויות הביטחון והמודיעין לנצל את מרחב הסייבר לצרכים ביטחוניים אחרים. הקטגוריה **השלישית** כוללת מופעי מדיניות מן השנים 1967–2016 שמגבילים

את המדינה ומייצגים פשרה בין ביטחון לאומי לפרטיות (21 אירועים). אלו בעיקר אירועים משנות השבעים והשמונים, אשר הגבילו את האופן שבו סוכנויות ביטחון לאומי ומודיעין יכולות לנצל את מרחב הסייבר. אף על פי שכאמור בספרות, מופעי מדיניות אלו אינם נמצאים על אותו ציר או מישור, כל קטגוריה כזאת חשובה להבנת מערכת היחסים הכוללת בין ביטחון לפרטיות בעידן הדיגיטלי, שבו המדינה היא גם הפתרון לחיזוק ההסדרה בנושא הגנת סייבר ופרטיות, אך גם הבעיה – בהיותה איום מתמיד על הפרטיות לצורך חיזוק הביטחון הלאומי.

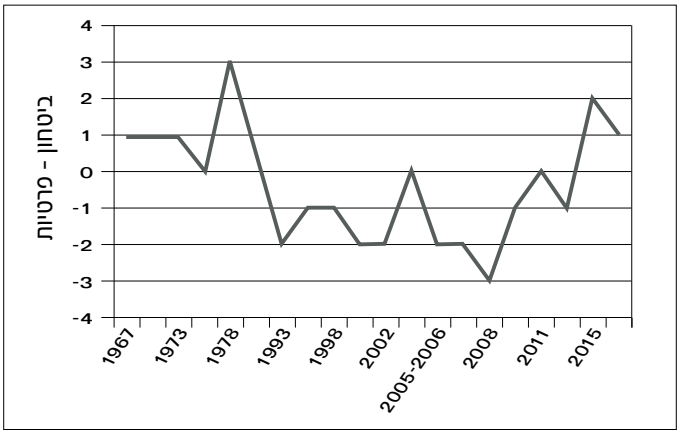
ממצאים

התפקיד הראשון של המדינה: ביטחון לאומי ≠ פרטיות

המדינה מנצלת את מרחב הסייבר לאיסוף מידע לצורכי ביטחון לאומי על חשבון הפרטיות

התרשים שלהלן מתאר את השינוי שעברה מערכת היחסים בין הביטחון הלאומי לפרטיות, כפי שהיא מובנית על ידי המדינה לפני ואחרי העידן הדיגיטלי. החל מאמצע שנות התשעים אפשר לזהות בזירה הפדרלית מגמה ברורה של העדפת הביטחון הלאומי על פני הפרטיות. על ידי ספירה של מופעי המדיניות בכל שנה מציג התרשים את ההפרש הכמותי בין מופעי מדיניות המגבילים איסוף מידע על ידי סוכנויות המודיעין והביטחון לשם שמירה על הפרטיות, לבין מופעי המדיניות המעודדים איסוף מידע לצורכי ביטחון לאומי על חשבון הפרטיות. הגבלה של איסוף מידע כוללת ניסוח הסדרים וחוקים חדשים המייצרים אחריותיות, חובת דיווח ואמות מידה מגבילות, שבהן יש להתחשב כאשר נאסף מידע לצורכי ביטחון לאומי. עידוד איסוף המידע כולל הפחתה וריכוך של ההגבלות הללו, או דרישה לשינויים טכנולוגיים כגון צמצום הצפנה עבור איסוף מידע על ידי סוכנויות המודיעין. המגבלה המרכזית של תרשים זה היא העובדה שהוא מתאר שינוי מגמה כמותי בלבד, ואינו מתייחס למשמעויות של כל רגולציה או חוק שנבחן. עם זאת, הסתכלות כזאת ממעוף הציפור על כמויות הרגולציה המשתנות יכולה ללמד על שינוי מגמה. בשנות השבעים והשמונים התאפיינה הזירה הפדרלית במופעי מדיניות רבים יותר שיצרו פשרה בין ביטחון לאומי לפרטיות (הקו הכחול מעל ציר ה־X), אולם החל מאמצע שנות התשעים הקו נמצא ברובו מתחת לציר ה־X ומייצג העדפה כמותית של ביטחון לאומי על חשבון הפרטיות.

על מנת לתאר את הנעשה ולהסביר מה עומד מאחורי המגמה המסתמנת בתרשים החל מאמצע שנות התשעים, יש לבחון את תפקוד הרשויות הפדרליות והקבוצות העסקיות הרלוונטיות. ראשית, **הרשות המבצעת** – החל מאמצע שנות התשעים היא הסירה את החסמים לאיסוף מידע והשתמשה בהצלחה בכוחה הפוליטי לניצול מרחב הסייבר לצרכיה: במהלך שנות השישים והשבעים, לאחר שנחשפו פרשיות ריגול רחבות



תרשים מס׳ 1: (מדיניות המקדמת פרטיות) – (מדיניות המקדמת ביטחון), בכל שנה לאורך זמן (1967–2016)

היקף של אזרחים אמריקאים לצרכים פוליטיים, בהוראת נשיאים שונים ובהובלת ה־FBI נחלש מעמדה של הרשות המבצעת מבחינת הלגיטימציה הציבורית לפגוע בפרטיות למען ביטחון לאומי. הקונגרס מינה ועדות בדיקה כגון ועדת צ׳רץ׳ (Church Committee), שבסופו של הליך התחקור המליצו על מגבלות משמעותיות על איסוף מידע כדי להגביר את הפרטיות. המלצות אלו הפכו להצעות חוק ולכינונם של חוקים בשנות השבעים והשמונים, שהגבילו במידה רבה את דרכי איסוף המידע. אפילו הרשות המבצעת עצמה, באמצעות הוראות נשיאותיות של הנשיאים קרטר ופורד מסוף שנות השבעים, הורתה על הגבלת איסוף מידע מטעמי פרטיות. לעומת זאת, החל מאמצע שנות התשעים השתנתה הלגיטימציה לאיסוף מידע – המחאה הציבורית בנושא הגנת הפרטיות נמוגה, והמלחמה בטרור הלכה ותפסה מקום מרכזי ויצרה בסיס להצדקת הפגיעה בפרטיות לצורכי ביטחון לאומי. הרשות המבצעת הסירה חסמים חוקתיים והפכה מנגנוני פיקוח על איסוף מידע ללא רלוונטיים. מגמה זו החלה כבר בשנת 1981 בהוראה נשיאותית שנויה במחלוקת של הנשיא רייגן (Executive Order #12333), אשר הורה על איסוף מידע מחוץ לגבולות ארצות־הברית, כולל על אזרחים אמריקאים, ללא פיקוח משמעותי. אומנם הוראה זו נגעה בנעשה מחוץ לגבולות ארצות־הברית, אך היו לה השפעות רחבות היקף על פרטיות האזרחים האמריקאים בעידן האינטרנט הגלובלי, שנסק בשנות התשעים. העידן הדיגיטלי טשטש את הגבולות הריבוניים, כאשר חברות כמו גוגל ויאהו מאחסנות מידע אישי היכן שמשתלם להן מבחינה כלכלית לעשות כן, ללא זיקה למדינות הריבון של לקוחותיהן. כך למשל מידע על אזרחי ארצות־הברית עשוי להיות מאוחסן באסיה או באירופה, ובכך להיות כפוף לאיסוף על פי הוראה זו. על כן, מתירנותה של ההוראה הנשיאותית העניקה לסוכנות לביטחון לאומי לגיטימציה

ליצירת תוכניות מעקב על פני רשת האינטרנט ולאיסוף מידע על אזרחים אמריקאים רבים. הלכה למעשה, הוראה זו מאפשרת איסוף מידע ללא פיקוח מצד הקונגרס או הרשות השופטת, ואינה דורשת את הסכמתה של החברה המסחרית שאספה את המידע. איסוף זה כולל לא רק את כותרי המידע אלא גם את התוכן עצמו, ללא צורך מצד סוכנויות המודיעין להציג ראיות שבגינן יש לבצע איסוף מידע.[24] נוסף על כך, הנחיות התובע הכללי מהשנים 1983, 1989 ו־2002 הרחיבו את המנדט של המדינה לאיסוף מידע, ללא שיח או הליך מדיניות מוסדר הכולל את האיזונים והבלמים הרלוונטיים. אחד השיאים של העדפת ביטחון לאומי על פני פרטיות הוא התמסדותן של תוכניות מעקב ביוזמת הנשיא ג'ורג' בוש הבן, בין השנים 2001 ו־2007. הנשיא החליט על דעת עצמו לאשר ולהוציא לפועל תוכניות מעקב על אזרחי ארצות־הברית, הסותרות את חוקי הפרטיות הקיימים. תוכניות אלו פעלו במשך שנים באופן חשאי, הוצאו לפועל על ידי סוכנויות המודיעין ונעצרו חלקית רק לאחר חשיפות ה'ניו יורק טיימס' מ־2005.[25] הממשל האמריקאי גם הרחיב לאורך השנים את השימוש בכלי מדיניות ייחודיים המכונים National Security Letters, אשר נועדו לאסוף מידע מחברות אזרחיות במקרי חירום. כלים אלו הפכו לשגרתיים כמעט במאמצי האיסוף המדינתיים, וחרגו מכוונות המחוקק שמיסד את השימוש בכלי חירום אלו לראשונה בהקשרים של מידע פיננסי (דרך ה־Financial Privacy Act מ־1978).

שנית, **הרשות המחוקקת** הייתה גם היא שחקנית חשובה בשינוי המגמה של העדפת הביטחון הלאומי על פני הפרטיות, החל מאמצע שנות התשעים. בשנות השבעים והשמונים היה הקונגרס פעיל מאוד בהגבלת איסוף מידע על אזרחי ארצות־הברית לצורכי ביטחון לאומי. עיקר הפעילות התבצעה דרך ועדות מיוחדות שמונו בנושא (ועדת צ'רץ' וועדת פייק [Pike]) וחקיקה חשובה שבאה בעקבות המלצותיהן (חוק הפיקוח על איסוף מודיעין זר FISA 1978, חוק הפרטיות בתקשורת אלקטרונית 1986 ECPA). עם זאת, החל מאמצע שנות התשעים נעשה הקונגרס גורם מעודד והעביר חקיקה המרככת הגבלות שהוטלו בשנים קודמות. רק ב־2015, לראשונה מזה שלושה עשורים, העביר הקונגרס את חוק החירות (USA Freedom Act) אשר מגביל איסוף מידע למטרות ביטחון לאומי. במהלך עשרים השנים האחרונות, נושאי הדגל בתחום הפרטיות בקונגרס נחלשו והיו כפופים למקבלי ההחלטות בנושאי ביטחון ומודיעין. הקונגרס הפך את עורו, ממקדם פשרה בין ביטחון לפרטיות לכזה המגבה את הממשל בתמיכתו באיסוף מידע על חשבון הפרטיות. למשל, החל מאמצע שנות התשעים אפשר הקונגרס חקיקה אגרסיבית מאוד בנושאי מעקב, ונתן אור ירוק לפרקטיקות זמניות שהפכו עד מהרה לקבועות. חקיקת חוק הפטריוט (Patriot Act) אחרי מתקפות הטרור ב־11 בספטמבר 2001 היא אולי הבולטת ביותר בנושא. גם התיקונים ל־FISA מ־2007 ומ־2008 מצביעים על מגמה של היחלשות ההגבלות על איסוף מידע והעדפת הביטחון

הלאומי על פני הפרטיות. מגמה זו באה לידי ביטוי בין היתר בטשטוש הגבולות בין איסוף מידע למטרות ביטחון לאומי לבין איסוף מידע לטובת מיגור פשיעה. בעוד איסוף מידע לצורכי חקירת פשיעה מנוהל תוך פיקוח הדוק ודורש נימוקים לכך שאיסוף המידע יסייע בחקירה המתנהלת, איסוף מידע לצורכי ביטחון לאומי אינו נתון להגבלות כאלה ומבוצע באופן חופשי יותר. החל משנות האלפיים טושטשו גבולות אלו על ידי חקיקת חוק הפטריוט והובילו לפגיעה בפרטיות לצורך קידום מטרות של ביטחון לאומי. איסוף מידע בשם צורכי ביטחון לאומי למטרות אכיפת חוק מאפשר מעקב אחר אזרחים אמריקאים ללא איזונים ובלמים מתאימים.

לבסוף, גם **הרשות השופטת** ממלאת תפקיד בהעדפת הביטחון הלאומי על פני הפרטיות בארצות־הברית החל משנות התשעים. לאורך שנות השבעים והשמונים סללו בתי המשפט באמצעות הכרעות דין חשובות את הדרך למספר חוקים, אשר קידמו את הפרטיות או פגעו בה. שתי דוגמאות מרכזיות לכך הן הפסיקה התקדימית מ־1967 (Katz vs. The United States 389 U.S. 347), אשר קבעה כי הזכות לפרטיות נובעת מהתיקון הרביעי לחוקה ותקפה עבור כל אדם, ללא קשר למיקומו הפיזי. פסיקה תקדימית זו היוותה את הבסיס לחוק הגנת הפרטיות הראשון שהיה תקף בעת איסוף מידע לצורכי מיגור פשיעה וחוקק ב־1968 (The Omnibus Safe Streets and Crime Control Act). פסיקה מ־1976 (United States vs. Miller 425 U.S. 435) פגעה בפרטיות והולידה חקיקה נגדית לריסון הפגיעה. הפסיקה קבעה כי אדם אינו זכאי להגנת פרטיות מצד ספקי צד שלישי, אם מסר להם מידע מרצונו. בתגובה חוקק הקונגרס ב־1986 את חוק הפרטיות בתקשורת אלקטרונית (ECPA) לחיזוק הגנת הפרטיות בטכנולוגיה מתקדמת. בשנות התשעים והאלפיים, לעומת זאת, נעשה תפקידו של בית המשפט שולי יותר. דרך מספר מקרים הטילה הרשות השופטת הגבלות על איסוף מידע בעזרת פרקטיקות השמורות למצבי חירום כמו National Security Letters השמורות למצבי חירום. הגבלות אלו היו ספורות, ורוב הזמן בית המשפט לא השכיל להגביל את הפרות הפרטיות ואת איסוף המידע האינטנסיבי של המדינה בימים של ראשית המלחמה בטרור. נהפוך הוא, באמצעות בתי משפט ייעודיים לאישור צווי איסוף מידע – Foreign Intelligence Surveillance Courts (FISC) – הרשות השופטת אף תרמה למאמצי המעקב של המדינה. השופטים בדיונים אלו, שהיו חסרי הבנה טכנולוגית נדרשת של הסוגיות שעמדו לפתחם, אישרו בקשות חריגות ומעוררות מחלוקת לאיסוף מידע מצד הסוכנות לביטחון לאומי. אישורי הבקשות הללו פתחו פתח רציני לסוכנויות המודיעין להרחיב את מאמצי המעקב שלהם. באופן גורף ובמבט רחב על ארבעת העשורים האחרונים, אפשר לומר שגם הרשות השופטת עברה מפסיקות חשובות שהשפיעו על חקיקה מקדמת פרטיות בשנות השבעים והשמונים, לפסיקות שוליות או לפסיקות המעודדות מעקב וקידום ביטחון לאומי על חשבון הפרטיות.

מעבר לפועלן של רשויות הממשל השונות בהבניית מערכת היחסים בין הביטחון הלאומי לפרטיות, גם לאינטרסים של קבוצות עסקיות מתחום תקשורת הנתונים הייתה השפעה מכרעת על שינוי המגמה. בשנות השבעים והשמונים נתפסה הגנת הפרטיות על ידי חברות אלו כיתרון מסחרי בשוק מתפתח. שדלנים (לוביסטים) של קבוצות אלו עשו יד אחת עם נציגי חברה אזרחית להעברת חקיקה שתגביל מעקב ותגן על פרטיות הלקוחות. דוגמאות לחוקים בנושא הגנת פרטיות שהועברו בתמיכת קבוצות אלו הן 1978 Financial Privacy act ו־1986 ECPA. החל מאמצע שנות התשעים התפוגגה שותפות האינטרסים בין החברה האזרחית לשדלנים עסקיים. נקודת המפנה הייתה ב־1994, עת חוקק הקונגרס בהובלה ובלחץ מצד ה־FBI את ה־Communications Assistance for Law Enforcement Act (CALEA). חוק זה דרש מחברות מסחריות לאפשר לגורמי אכיפת החוק לאסוף מידע מתשתיות התקשורת שלהם, על ידי שינוי ממשקי העבודה באופן שיאפשר למדינה גישה לכל נתוני התקשורת של אזרחי ארצות־הברית. המחוקק סיפק פיצוי נדיב לבעלי העסקים, והם מצידם התיישרו עם דרישות המדינה לאיסוף מידע. היחסים הקרובים הללו בין גורמי הביטחון וסוכנויות המודיעין לבין בעלי עסקים בארצות־הברית נמשכו ביתר שאת לאורך שנות התשעים והאלפיים. רוב שיתופי הפעולה הללו אינם גלויים. מה שכן ידוע הוא הכמות הנכבדת של שיתופי פעולה סביב שימוש ב־National Security Letters לאיסוף מידע, והמנדט שקיבלו ספקיות האינטרנט באמצעות חוק הפטריוט לעקוב אחר לקוחותיהן על בסיס הצדקה מינימלית בלבד.

באחרונה, אחרי חשיפות אדוארד סנודן, נראה שינוי מגמה נוסף. האינטרסים של חברות מסחריות וארגוני חברה אזרחית סביב הפרטיות שבים ומתלכדים. כדוגמאות ניתן להזכיר את סירובה של חברת אפל לפצח את הצפנת הטלפון הנייד של המחבל מפיגועי סן ברנרדינו בקליפורניה, ואת ההתנגדות של חברת מיקרוסופט לדרישת גורמי אכיפת החוק לחשוף מידע על לקוחותיה הנמצא על שרתים באירלנד, מחוץ לתחום השיפוט של ארצות־הברית. בשני האירועים הללו גברו שיקולי הפרטיות על רצון המדינה לאסוף מידע בשם הגברת הביטחון הלאומי. ב־2013 נעשה ניסיון להעביר חוק נוסף לאיסוף מידע מרשתות תקשורת בשם CALEA II, על שם החוק הראשון בנושא מ־1994, אך הוא נתקל בהתנגדות עזה של תעשיית התקשורת. הפרטיות חזרה להיות יתרון עסקי ותחרותי של חברות מסחריות, ודרך להגיע לליבם של הצרכנים.

התפקיד השני של המדינה: הלימה בין ביטחון לאומי לפרטיות

המדינה מקדמת את הגנת הסייבר ואת השמירה על הפרטיות, ותוך כך מחזקת את הביטחון הלאומי

במקביל למאמצי המדינה לנצל את מרחב הסייבר לאיסוף מידע לצורכי ביטחון לאומי תוך פגיעה בפרטיות, נעשתה גם פעילות חקיקה ורגולציה ענפה לקידום משותף של הביטחון הלאומי והפרטיות באמצעות חיזוק הגנת הסייבר. עם זאת, פעילות זו מצומצמת ברובה ומקודמת באופן חלקי בלבד, בעקבות הדומיננטיות של אינטרסים עסקיים בשדה מדיניות זה. מנקודת מבט רחבה על פעילות זו לאורך שלושת העשורים האחרונים אפשר להבחין בשלושה רכיבים מרכזיים: ראשית, מאמצי ההגנה על הביטחון הלאומי והפרטיות על ידי חיזוק הגנת הסייבר ממוקדים במגזרים מסוימים מאוד בחברה. כחלק מהשקפת העולם המסורתית האמריקאית של אי־התערבות רגולטורית במגזר העסקי, חברות מסחריות ושירותי תקשורת כפופים להנחיות וולונטריות בלבד, שאינן מחזקות במידה מספקת את הביטחון הלאומי ואת הפרטיות. נוסף על כך, גישת הממשל כלפי כלכלת האינטרנט הייתה מלכתחילה גישה לא־מתערבת, שאפשרה איסוף מידע אישי לצרכים עסקיים. כך נוצרו התנאים המוסדיים למסחור המסיבי במידע אישי שאנו רואים כיום, שנעשה על ידי מונופולים של מידע כמו גוגל ופייסבוק, ולפגיעה אנושה בפרטיות הצרכנים על ידי חברות מסחריות. לבסוף, ישנן דוגמאות לרגולציה שתפקידה לחזק את הגנת הסייבר, אשר כוללת פגיעה בפרטיות. חוק שיתוף המידע בסייבר (CISA) משלהי 2015 מתיר איסוף מידע ללא צו בית משפט, תוך מתן תמריצים של פטור מאחריות על מנת לרכז מידע בדבר איומי סייבר במגזר העסקי, ולייצר תגובה הגנתית מבעוד מועד.

חלק זה מחולק בהמשך לשני חלקים המסבירים בנפרד הן את השמירה המוגבלת על פרטיות וביטחון לאומי דרך הגנה על מערכות המידע, והן את הסתירה הפנימית הקיימת בין הגנת הסייבר לפרטיות בתפקיד זה של המדינה.

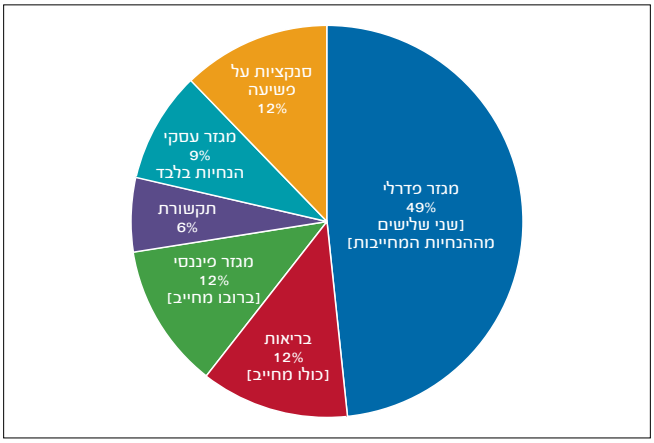
שמירה על הביטחון הלאומי והפרטיות באופן מגזרי ומצומצם

הצורך בהגנה על מערכות ממוחשבות ומידע דיגיטלי הפך לנושא מרכזי מבחינת קובעי מדיניות פדרליים בארצות־הברית באמצע שנות השמונים.[26] אף על פי כן ולמרות הצמיחה העצומה של שוק כלכלת האינטרנט, תוך הגברת התלות של החברה במרחב סייבר יציב ומתפקד, המדינה מקדמת ביטחון לאומי ופרטיות באופן מגזרי שאינו מספק ואינו חורג מתחומי הבריאות, הפיננסים והרשתות הפדרליות. בעוד מרבית המחויבויות הרגולטוריות שמטילה המדינה נוגעות למגזרים הנתפסים כחיוניים לתפקוד המדינה, שאר התעשיות, שהן חלק הארי במרחב הסייבר, מטופלות דרך רגולציה עצמית ומדיניות שאינה מקשה יתר על המידה עם התעשייה. תרשים מס' 2

מתאר את אוזלת היד של מאמצי הממשלה הפדרלית לקידום החוסן במרחב הסייבר, ועל כן ביטחון לאומי ופרטיות יחדיו, באופן חוצה מגזרים. כמחצית ממאמצי המדינה מרוכזים בהגנה על הרשתות הפדרליות. בעוד הממשלה מיטיבה להגן על עצמה, היא משאירה את התעשייה והחברות המסחריות לפרקטיקות הגנה וולונטריות בלבד.[27]

בעלי עסקים השכילו לפעול נגד הכללתם ברגולציית הגנת מידע מחייבת בשלב מוקדם מאוד. חוק הפרטיות מ־1974 (The 1974 Privacy Act) חוקק על ידי הקונגרס מתוך הבנת החשיבות של שמירה על מידע אישי הנמצא ברשות המדינה. במהלך הדיונים שקדמו לחקיקה טענו חברות מסחריות שאין כל עדות ממשית לפגיעה בפרטיותם של אזרחים מצד עסקים פרטיים. הנחת העבודה שלהם הייתה כי הם קורסים תחת הנטל הרגולטורי גם כך, והחוק המוצע אינו נחוץ ומגביר נטל זה שלא לצורך.[28] האסטרטגיה שלהם הייתה לדחוק בחברות מסחריות לאמץ רגולציה עצמית, ובכך להפחית את הנטל והלחץ של בעלי עסקים מפני רגולציה ממשלתית. נוסף על כך התנגד המגזר העסקי להקמת סוכנות פדרלית שתאכוף את השמירה על פרטיות האזרחים. למעשה, הצעת חוק של הסנאט שכללה הקמה של סוכנות כזו נגנזה. לבסוף, החוק שעבר ב־1974 כלל את הגנת הפרטיות המינימלית שעליה דובר באותה תקופה. מגמה זו נמשכה גם באמצע שנות התשעים, כאשר הממשל הפדרלי הגיב לצמיחה של כלכלת האינטרנט על ידי כינון רגולציה להגנת הפרטיות והסייבר – ועל כן, להגנת הביטחון הלאומי – בענפים נבחרים בלבד של המגזר העסקי (בריאות, פיננסים וכדומה), כאשר הוא מותיר את רוב המגזר ללא רגולציה מחייבת. ב־1997 פרסמו הנשיא דאז ביל קלינטון וסגנו אל גור מתווה למסחר בעידן הדיגיטלי (The Framework for Global Electronic Commerce), שבו הם תיארו את המרחב האינטרנטי כחיוני לצמיחה כלכלית, ובשל כך אין להטיל עליו מגבלות רגולטוריות שיקשו על פיתוח הכלכלה. המסמך קרא לאימוץ מודלים של רגולציה עצמית והשאיר את תהליך קבלת ההחלטות בנושאי הגנת הפרטיות לפתחן של חברות מסחריות. מאז מתווה זה, חברות מסחריות הן המחליטות הבלעדיות על רמת הפרטיות שתהיה ללקוחותיהן, וכך נבנתה באין מפריע הפרקטיקה של מסחור במידע אישי למטרות רווח.

במהלך השנים הונחו על שולחן הקונגרס עשרות הצעות חוק להגברת הפיקוח והשמירה על פרטיות האזרחים הנתונים לחסדיהן של חברות מסחריות. מתוכן הצליחו לעבור חוקים ספורים בתחום הבריאות והפיננסים. מידע אישי על בריאותם של אזרחים נתפס כרגיש והוא מוגן על פי חוק מ־1996 (Health Insurance Portability and Accountability Act – HIPAA). הייתה זו למעשה הפעם הראשונה שהגנת מידע עוגנה בחוק. המגזר הפרטי התנגד בנחרצות וחשש מעלויות ומרגולציה שאינה מתאימה לשטח. לאחר שבע שנים הפך החוק בשנת 2003 לרגולציה מחייבת. בתחום הפיננסים חוקק ב־1999 חוק (The Gramm-Leach-Bliley Act) שמגן על מערכות פיננסיות ועל



תרשים מס' 2: מופעי מדיניות פדרליים בנושאי פרטיות והגנת סייבר [1974 – 2016]

פרטיות האזרחים. זאת ועוד, ב־2002, לאחר קריסת החברות אנרון ו־WorldCom חוקק חוק (The Sarbanes-Oxley Act SOX) אשר מחדד את הבקרה על חברות מסחריות באופן הכולל בין היתר פרקטיקות הגנה על מידע. ב־2010, אחרי כשני עשורים של עיסוק במגזרים מסוימים בלבד, החלה מחלקת המסחר האמריקאית לעסוק בנעשה בתחומי הגנת הסייבר והפרטיות במגזר הפרטי בכללותו. אך במקום לשנות את המגמה הוולונטרית של רגולציה מחייבת הנאכפת במלואה, נכתבו שני מסמכי מדיניות המורים על יישום אסטרטגיות הגנת מידע ופרטיות באופן שאינו מחייב יישום על ידי חברות פרטיות. המסמך הראשון מדבר על אימוץ סטנדרטים פדרליים שנחקקו כבר ב־1974 ומחייבים את הרשויות הפדרליות, ועל החלתם גם על המגזר הפרטי. המסמך קורא גם להקמת סוכנות פדרלית להגנת הפרטיות במסגרת מחלקת המסחר. במובן מסוים, מסמכי המדיניות נועדו לתקן ולהעלות מחדש את ההצעות שנפלו בשנות השבעים, אך הם עושים זאת באופן שאינו מחייב הגנה ושמירה על פרטיות מצד המגזר העסקי. המסמך השני מגדיר מגזר חדש – Internet and Information Innovation Sector (I3S) – אשר מכיל המלצות טכניות להתמודדות עם איומי סייבר ופרטיות עבור חברות. עם זאת, אף על פי שמסמכי המדיניות הללו מציעים פתרונות נחוצים, רמות ההגנה והשמירה על פרטיות הלקוחות של חברות מסחריות ממשיכות להיות נתונות לשיקול הדעת של החברות עצמן, וכפופות רק לעקרונות של 'מסחר הוגן' אשר נאכפים בדיעבד על ידי ועדת הסחר הפדרלית (FTC).

החל מ־2013 ניכרת פעילות לא מבוטלת של סוכנויות רגולטוריות עצמאיות בשדה הגנת הסייבר והשמירה על הפרטיות. הסוכנות לטיפול במפעילי רשתות תקשורת – רשות התקשורת הפדרלית (FCC) פרסמה מסמך אסטרטגיה ובו המלצות יישום לשמירה על הגנת המערכות ופרטיות המשתמשים. זאת ועוד, ב־2015 קבע בית משפט לערעורים

בפילדלפיה כי לוועדת הסחר הפדרלית יש סמכות אכיפה כלפי חברות גם בנושאי הגנת סייבר, ולא רק במקרים של פגיעה בפרטיות (FTC vs. Wyndham Worldwide Corporation). פסיקה זו הייתה חשובה שכן קודם לכן סמכות האכיפה של ועדת הסחר התרכזה בפגיעות בפרטיות ונשענה על מה שנחשב מסחר הוגן. עתה מתבססת הוועדה על מעמד מוסדי חדש שהוענק לה על ידי בית המשפט. העלייה בהשפעתן של סוכנויות רגולטוריות נצפתה גם ב־2016, בעת שרשות התקשורת הפדרלית עברה מהמלצות למעשים ופרסמה חוק מחייב הדורש מספקיות אינטרנט (ISPs) להגן על המידע ועל פרטיות הלקוחות שלהם. החוק החדש דורש שקיפות מלאה לגבי האופן שבו ספקיות אינטרנט עושות שימוש במידע אישי. אך באחרונה, עם עלייתו של ממשל חדש בוושינגטון, מינה הנשיא הנבחר טראמפ פקיד ציבור חדש להובלת הרשות, Ajit Pai, אשר מיהר לבטל חוקים אלו.

לסיכום, בניסיונות המדינה לקדם שמירה על הפרטיות ועל הביטחון הלאומי יחדיו דרך הגברת הגנת הסייבר אנו למדים על פעילות מגזרית בלבד, ללא סוכנות אכיפה וריבון מרכזי אחד, תוך יצירת התנאים המאפשרים לחברות לסחור במידע אישי ולהעמיק את הפגיעה בפרטיות. רגולציה מחייבת של הגנת הסייבר אינה מאומצת מאחר שלפי התפיסה היא כרוכה בעלויות גבוהות עבור בעלי העסקים, בעוד רגולציה להגנת הפרטיות מאומצת באופן חלקי מאוד, כדי שלא תפגע ברווחים של אלו המבססים את המודל העסקי שלהם על מסחר במידע אישי.

שמירה על הגנת הסייבר ועל הזכות לפרטיות והסתירה ביניהן

מעבר ליכולת המצומצמת הבאה לידי ביטוי בקידום הגנת הפרטיות והביטחון הלאומי דרך החלת רגולציה מחייבת להגנה בסייבר, באופן פרדוקסלי המדינה מקדמת לעיתים הגנת סייבר תוך פגיעה בפרטיות. באחרונה הוטבע מושג חדש – Sigint Cyber-Security – המתאר שימוש באיסוף מידע על איומי סייבר לצורכי הגנת סייבר.[29] מושג זה אומנם חדש אך הפרקטיקה נמצאת בשימוש כבר שנים רבות מאוד, בעידוד המדינה, בעיקר מאז פיגועי ה־11 בספטמבר 2001.

כבר ב־1984 עלה החשש לפגיעה בפרטיות לצורכי הגנת מידע. דרך ה־National Security Directive #145 העניק הנשיא דאז רייגן לסוכנות לביטחון לאומי (NSA) את הסמכות להגן על כל מאגרי המידע הממשלתיים. החלטה זו – שהתקבלה כאשר פרקטיקות המעקב של גופי הביטחון האמריקאיים נחשפו ביתר שאת על ידי ועדת צ'רץ' מ־1976 – עוררה דאגה בקרב מחוקקים רבים, ובתגובה חוקק הקונגרס ב־1987 חוק המעניק לסוכנות האזרחית National Institute for Security Standards (NIST) את הסמכויות שניתנו ל־NSA. עם זאת, מעמדה המוסדי של NIST מול ה־NSA היה חלש. שתי הסוכנויות חתמו ב־1989 על מסמך הבנות שלפיו ה־NSA אינה מאבדת

מהסמכויות שניתנו לה על ידי הנשיא רייגן. המגמה נמשכה ב־2001 כאשר חוק הפטריוט אפשר לסוכנויות אכיפת החוק לעקוב אחר נתוני התקשורת של חשודים פוטנציאלים על מנת למגר פשיעת סייבר. החוק מאפשר לשופטים להטיל צו גורף על חשודים מכל מקום בארצות־הברית ולבצע איסוף נרחב של מידע, כולל מידע טכנולוגי, הנחוץ לאיתור ולמעקב אחר חשודים. המתח בין השמירה על הפרטיות להגנה על המידע בא לידי ביטוי גם באסטרטגיית הסייבר הנשיאותית שפורסמה ב־2008 – The Comprehensive National Cyber Security Initiative (CNCI). האסטרטגיה פורסמה כדי לוודא שרשתות פדרליות עמידות בפני מתקפות סייבר. הדרך לעשות זאת הייתה בין היתר על ידי עידוד איסוף מידע ושימוש ביכולות של שבירת הצפנה ופגיעה בפרטיות מצד סוכנויות המודיעין, לצורך הגנה על מידע פדרלי. ב־2015 חוקק חוק שיתוף המידע בסייבר (CISA), המאפשר איסוף מידע מהמגזר הפרטי באופן שאינו שקוף, לצורכי הגנת סייבר. חוק זה היווה עליית מדרגה בכל הקשור במתח בין הגנת הפרטיות להגנת סייבר. על פי החוק, חברות מסחריות אינן נושאות באחריות כלפי צד שלישי במקרה של מתקפת סייבר, אם בחרו מבעוד מועד לשתף מידע עם המדינה. יש כאן תמריץ משמעותי לאיסוף מידע מדינתי ללא צו בית משפט וללא הצדקה ברורה.[30]

סיכום

במהלך חמשת העשורים האחרונים מחזיקה ארצות־הברית בתפקיד כפול וסותר בכל הנוגע לקידום הביטחון הלאומי והגנת הפרטיות בראי המרחב הדיגיטלי. בתפקידה הראשון של המדינה – ניצול מרחב הסייבר לעידוד איסוף מידע לצורכי ביטחון לאומי על חשבון הפרטיות – כל הרשויות הפדרליות מעודדות מגמה של ביטחון לאומי על חשבון הפרטיות. החל מאמצע שנות התשעים מתקיימים יחסי כוחות א־סימטריים בין הרשות המבצעת למחוקקת, ושיתופי פעולה הדוקים בין המדינה לחברות מסחריות החולשות על מידע אישי רב. בתפקידה השני של המדינה – קידום הגנת הסייבר להגברת הביטחון הלאומי והפרטיות גם יחד – אנו עדים להתנגדות עזה של חברות מסחריות לקבל על עצמן רגולציה מחייבת לקידום הגנת הסייבר. המגמות הללו יצרו מרחב דיגיטלי שאינו רק מנוצל על ידי המדינה ופוגע בפרטיות, אלא גם אינו מוגן דיו מאיומים חיצוניים על הפרטיות. עם התפשטות התלות במערכות טכנולוגיות במגזרי המשק השונים נולד מרחב הסייבר, שהוא מרחב חדש לחלוטין שהמדינה צריכה למַשטֵר. ואולם במסגרת תרבות רגולטורית של ניו־ליברליזם ואי־התערבות מדינתית לכאורה, האינטרס הציבורי כפוף לכוחן של סוכנויות ביטחון וחברות מסחריות. בעוד ארצות־הברית פועלת רבות באופנים הפוגעים בפרטיות אזרחיה על מנת לקדם מטרות של ביטחון לאומי, היא אינה מצליחה לקדם רגולציה המגינה על המרחב עצמו, ולכן גם

על הפרטיות ועל הביטחון הלאומי יחדיו, באותו אופן שהיא שומרת על נכסי ציבור בתחומים אחרים.

אחרי כמה עשורים של מדיניות ציבורית המבנה את מערכת היחסים בין הביטחון הלאומי לפרטיות, מאמר זה מחדד את הדחיפות בשינוי השיח ובכיווני הפעולה סביב המדיניות הנוכחית. מסגור השיח בדבר מדיניות הסייבר – אשר מתייחס להגנת סייבר כאל מרכיב במערכות ולא מרכיב בביטחונם ובפרטיותם של יחידים – צריך להשתנות. כאשר ההגדרות המסורתיות של הגנת סייבר עוסקות בהגנה על מערכות מפני פצחנים ונותנות את המנדט לסוכנויות מודיעין וביטחון ולגופים עסקיים, נוצר שיח שמרחיב את יכולות המעקב, מגביל את ההצפנה ומאפשר התקנת 'דלתות אחוריות' ללא אחריותיות ראויה. פרקטיקות אלו גורמות פגיעה משמעותית בביטחונם ובפרטיותם של יחידים, ומציגות את התלות החברתית במרחב הסייבר כגורם המחליש את החברה.

על פי ההדגמה האמפירית במאמר זה, הפעולות המדינתיות במרחב הסייבר הן מקור לדאגה. השיח צריך להשתנות כך שיושם דגש על ביטחונם של יחידים. המשמעות היא מתן בעלות מלאה למושאי המידע על המידע האישי שלהם, שימוש גורף בהצפנה ומיסוד מנגנוני פיקוח ואחריותיות לאיסוף מידע מדינתי באופן שירסן את כוחם של המדינה ושל מונופולים עסקיים. יש להביא בחשבון אינטרסים אזרחיים ולא רק ביטחוניים ומודיעיניים, ולוודא שהאינטרס הציבורי מקודם כראוי במרחב הסייבר.

שימוש בספרות של רגולציה ככלי לניהול סיכונים ולניתוח הממצאים במרחב הסייבר מאפשר להבחין בליקויים הנובעים מתפקיד המדינה כמנהלת סיכונים דו־משמעיים כאלה עבור החברה. בסקירת הספרות דן המאמר בשאלה המרכזית המעסיקה את החוקרים שמאמצים גישה הטוענת שתפקיד המדינה הוא לנהל סיכונים בחברה. האם פעולות מדינתיות של ניהול סיכונים הן תולדה של סיכונים חדשים העולים מהשטח, ועל כן יש לוודא שהאינטרס הציבורי מקודם לנוכח המצב החדש, או שמא המדינה למעשה דואגת בראש ובראשונה למוסדותיה, ופחות להשלכות הציבוריות של מדיניות ניהול הסיכונים שלה? הממצאים על הנעשה במרחב הסייבר מלמדים שהתשובה היא גם וגם. כאשר המדינה מנצלת את מרחב הסייבר למטרותיה, קיימת פגיעה משמעותית בפרטיות באופן שמבטיח את קידום מטרותיהן של סוכנויות הביטחון והמודיעין על חשבון האזרחים. כאשר המדינה מנסה לקדם את הגנת סייבר היא עושה זאת באופן שאינו מקדם את האינטרס הציבורי, ומעבר למגזרים שהוגדרו כרגישים, היא נתונה ללחצים מצד קבוצות עסקיות. ניהול סיכונים בשני משטרים חופפים למחצה – ביטחון לאומי ופרטיות – מאתגר את הספרות הקיימת בנושא ושופך אור על המורכבות של תפקיד המדינה כמנהלת סיכונים עבור החברה.

מגבלות המחקר הנוכחי נובעות בראש ובראשונה מנקודת המבט הרחבה ומההמשגה של מסגרת אנליטית חדשה לניתוח מדיניות ציבורית על פני חמישה עשורים. מפאת

התיאור הנרחב, המאמר אינו עוסק במנגנונים שמאחורי העדפות של ביטחון לאומי ופרטיות בכל זירת מדיניות, ואינו מנתח לעומק הליכי מדיניות ציבורית סביב מקרה מסוים. על כן, מחקר עתידי בנושא שיתמקד בזירת מדיניות מסוימת בתוך הטווח של מערכת היחסים בין ביטחון לאומי ופרטיות עשוי לאפשר הבנה מדוקדקת יותר של ניהול סיכונים על ידי המדינה במרחב מסוים.

הערות

1 האיזונים והבלמים של הרשות המבצעת כוללים אומנם בתי משפט ייעודים שהוקמו עבור דיון בבקשות מעקב של המדינה וועדות קונגרס שאליהן מחויבות רשויות המודיעין הפדרלי לדווח באופן מחזורי. עם זאת, על אף היכולת המוסדית שהוקמה זה מכבר, מסמכי המדליף אדוורד סנוודן משנת 2013, חשפו כיצד מנגנונים אלו הם לרוב חותמת גומי, ואינם מבצעים ניטור ובלימה אפקטיביים לתיאבון איסוף המידע של הממשל. הפרשנות המצומצמת והמוטה של הסוכנות לביטחון לאומי על התשתית הרגולטורית המפקחת עליה מדגימה זאת. לחוסר האפקטיביות בפיקוח על איסוף המידע ראו כ-3000 מקרים שבהם הודתה הסוכנות בטעותה, https://goo.gl/hFGmsj לחוסר היכולת לפקח על בקשות טכנולוגיות מורכבות מצד ה-NSA ראו עדותו של שופט, https://goo.gl/XEWHCZ

2 Frenando Mendez and Mario Mendez, "Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States"*, The Journal of Federalism*, Vol. 40, No. 4, 2009, pp. 617-645; Ronald Deibert and Rafael Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology*, Vol. 4, No. 1, 2010, pp. 15-32.

3 David Flahert, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, 1989, UNC Press; Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, 1995, UNC Press.

4 Amitai Etzioni, "Cybersecurity in the Private Sector", *Issues in Science and Technology*, Vol. 28, No. 1, 2011; Janine Hiller and Roberta Russel, "The challenge and imperative of private sector cybersecurity: An international comparison"*, Computer Law & Security Review*, Vol. 29, 2013, pp. 236-245.
Richard Harknett and James Stever, "The New Policy World of Cybersecurity"*, Public Administration Review*, 2011, pp. 455-460.

5 ראו הנחיות התובע הכללי מה-30 במאי 2002, המורות על שינוי באסטרטגיה הכוללת של ניטור ואיסוף מידע למניעת טרור אחרי מתקפות 11 בספטמבר, https://fas.org/irp/news/2002/05/ag053002.html

6 וזאת על אף הליכים מקבילים להגנת הפרטיות באירופה, שהחלו עוד בשנות השמונים ב-OECD, ושיאם בשנת 1995 עם כינון תקנות הגנת מידע מחייבות ונוקשות בכל המדינות החברות באיחוד.

7 Lee Bygrave, *Data Protection Law – Approaching its Rationale, Logic, and Limits*, 2002; Kluwer Law Intl; Samuel Warren Louis Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, 1890, pp. 193-220.

8 Alan Westin, *Privacy and Freedom,* 1967, New York: Atheneum; Charles Fried, "Privacy", *Yale Law Journal*, Vol. 77, 1968, pp. 475-93;
James Rachels, "Why Privacy is Important", *Philosophy & Public Affairs*, Vol. 4, No. 4, 1975, pp. 323-333; Kenneth Laudon, "Markets and Privacy"*,* Association for Computing

Machinery, *Communications of the ACM*, Vol. 39, No. 9, 1996; Lawrence Lessig, *Code and Other Laws of Cyberspace,* 1999, Basic Books.

9 Ruth Gavison, "Privacy and the Limits of Law", *Yale Law Journal*, Vol. 89, No. 3, 1980, pp. 421-471.

10 Julie Innes, *Privacy, Intimacy, and Isolation*, 1992, New York: Oxford University Press.

11 Emma Rothschild, "What is Security?" *Daedalus*, Vol. 24, No. 3, 1995, pp. 53-98, MIT Press.

12 Jeremy Waldron, "Safety and Security", *Nebraska Law Review*, Vol. 85, No. 2, 2006, pp. 454-507.

13 David Lyon, *Surveillance Society: Monitoring Everyday Life,* 2001, Open University Press; Priscilla Regan, "Response to Bennett: Also in defense of privacy", *Surveillance & Society*, Vol. 8, No. 4, 2011; Collin Bennett, "In Defense of Privacy: The Concept and the Regime", *Surveillance & Society*, Vol. 8, No. 4, 2011.

14 Ronald Dworkin, *Taking Rights Seriously*, Harvard University Press, 1977; Jeremy Waldron, "Security and Liberty: The Image of Balance", *Journal of Political Philosophy*, Vol. 11, No. 2, 2003, pp. 191-210; Lucia Zedner, "Too Much Security?", *The Journal of Sociology of Law*, Vol. 31, No. 3, 2003, pp. 155-184.

15 Simon Hallsworth and John Lea, "Reconstructing Leviathan: Emerging contours of the security state", *Theoretical Criminology*, Vol. 15, No. 2, 2011, pp. 141-157.

16 Ronald Deibert and Rafael Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", שם.

17 Fernando Mendez and Mario Mendez, "Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States", שם.

18 Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy,* שם.
David Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, 1989, UNC Press.

19 Abraham Newman and David Bach, "Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States", *Governance*, Vol 17, No. 3, 2004, pp. 387-413.

20 Amitai Etzioni, "Cybersecurity in the Private Sector", *Issues in Science and Technology,* שם.

21 Janine Hiller and Roberta Russel, "The challenge and imperative of private sector cybersecurity: An international comparison", שם.

22 Kenneth Bamberger and Deirdre Mulligan, "Privacy on the Books and on the Ground", *Stanford Law review*, Vol. 67, 2011, pp. 247-316.

23 בית המשפט העליון החליט כי ציתות טלפוני מפר את הזכות לפרטיות על פי התיקון הרביעי לחוקה האמריקאית, וקבע כי הזכות לפרטיות ניתנת לאנשים באשר הם, ללא קשר למקום הפיזי בו הם נמצאים.

24 ביולי 2014 פרסם ג'ון נייפלר נאי, עובד לשעבר במחלקת המדינה האמריקאית, טור דעה ב'וושינגטון פוסט', המחדד את הרלוונטיות של הוראה נשיאותית זו להפרת האיזונים בין ביטחון לאומי לפרטיות בארצות־הברית: John Napier Tye , "Meet Executive Order 12333: The Reagan Rule that Lets the NSA Spy on Americans", July 18 2014, https://wapo.st/2Ttlqti

25 ראו את ההדלפה ואת כתבת ה'ניו יורק טיימס' מ־2005 בנושא: James Risen and Eric Lichtblau, "Bush Let U.S. Spy on Callers Without Courts", nytimes.com, December 16, 2005, https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

26 Michael Warner, "Cyber Security: A Pre-history", *Intelligence and National Security,* Vol. 27, No. 5, 2012, pp. 781-799.

27 Abraham Newman and David Bach, "Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States", שם.

28 Priscilla Regan, *Legislating Privacy,* שם.

29 ראו עיסוק במושג זה במאמרו של דניס צ'או: Dennis Chow, "Using Signals Intelligence within Cyber Security", eforensicsmag.com, November 12, 2015, https://eforensicsmag.com/dennis-chow

30 ראו מאמרה של חוקרת הפרטיות ג'ניפר גראניק בנושא: Jennifer Granick, "OmniCISA Pits DHS Against the FCC and FTC on User Privacy", December 16, 2015, https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy