תפקידן ואחריותן של ממשלות בהגנה על קניין רוחני דיגיטלי

רון שחר

ההתפתחות המהירה של מרחב הסייבר הובילה להתגברות האיום של גניבת קניין רוחני בכלל וסודות מסחריים דיגיטליים פרטיים ומסחריים בפרט. המדובר בגניבה המתרחשת בדרך קיברנטית ונובעת ממניעים פליליים. לסוג זה של פשעי סייבר יכולה להיות השפעה קריטית על המערכת המקרו־כלכלית הבין־לאומית, לרבות פוטנציאל לאובדן של הכנסות עתק ממסים ולצניחה בתמ"ג. מרבית המדינות ניסחו דוקטרינה אסטרטגית להגנת סייבר במטרה להגן על התשתיות הקריטיות הפיזיות שלהן כנגד לוחמת סייבר פוליטית. לעומת זאת, למרביתן אין עדיין דוקטרינה, חקיקה ואמצעים מתאימים להגנה על קניין רוחני דיגיטלי כנגד פשעי סייבר הנעשים ממניעים פליליים. הגישה המיושנת של ענישה על פשעי סייבר לאחר התרחשותם אינה רלוונטית, שכן מרחב הסייבר מקשה בכל מקרה על זיהוי גניבת הקניין הרוחני בזמן אמת.

מאמר זה בוחן האם ההשלכות המקרו־כלכליות של המגמות הגוברות והולכות של גניבה במרחב הסייבר יביאו להגדרת הקניין הרוחני הדיגיטלי, הפרטי והמסחרי, כתשתית קריטית, כזו הזקוקה להגנה ממשלתית פרואקטיבית.

מילות מפתח: קניין רוחני דיגיטלי, גניבת סייבר, תשתית קריטית, אחריות ממשלתית, פשעי סייבר, CNE, הגנה פרואקטיבית, דוקטרינות הגנת סייבר, השלכות מקרו־כלכליות.

רון שחר הינו יועץ אסטרטגי בתחום הסייבר. שירת בצה"ל כראש מדור תכנון סייבר־אסטרטגי וכעוזר לראש מחלקת הגנת הסייבר של צה"ל.

מבוא

"התשתית הדיגיטלית שלנו – הרשתות והמחשבים שאנו תלויים בהם מדי יום ביומו – תקבל מעתה ואילך את היחס הראוי לה ותהפוך לנכס לאומי אסטרטגי".[1]

"אנו מתכוונים להגן בצורה אגרסיבית על הקניין הרוחני שלנו. הנכס הגדול ביותר שלנו הוא החדשנות, כושר ההמצאה והיצירתיות של העם האמריקאי. הגנה כזו חיונית לשגשוגנו, ומגמה זו רק תלך ותתחזק במאה הנוכחית". [2]

נשיא ארצות הברית, ברק אובמה

קניין רוחני פרטי ומסחרי בכלל וסודות מסחריים בפרט נתפסים כיום כמרכיב חשוב בכלכלת המדינה המודרנית. במקביל, מרחב הסייבר מתפתח במהירות והופך מקור להזדמנויות מרתקות, ולצד זאת מקור לאיומים, המתבטאים בלוחמת סייבר ובפשעי סייבר.[3] חלק מאיומי הסייבר שמאחוריהם מסתתר מניע פלילי מכוונים ישירות לגניבת קניין רוחני פרטי או מסחרי. גניבה כזו עלולה לגרום לאובדן ניכר של הכנסות ממסים, וכתוצאה מכך להקטנת תקבולי המדינה ולירידה בתוצר המקומי הגולמי של מדינה, וכן להשפיע משמעותית על המערכות המקרו־כלכליות הבין־לאומיות.[4] מרבית המדינות ניסחו דוקטרינות להגנה אסטרטגית על מרחב הסייבר וחוקים להגנה על תשתיות קריטיות פיזיות מפני מתקפות סייבר שמקורן ביריבות פוליטית. לעומת זאת, אותן מדינות נוטות להתעלם מהצורך להגן על קניין רוחני דיגיטלי במרחב הסייבר מפני התקפות בעלות כוונות פליליות.

מאמר זה בוחן את השאלה מדוע ממשלות צריכות להתייחס לכלל הקניין הרוחני שלהן – המסחרי והפרטי כאחד – וספציפית לסודות מסחריים דיגיטליים, כאל תשתית לאומית קריטית שראויה להגנה פרואקטיבית הולמת מצדן. המאמר גם יבחן האם ההשלכות המקרו־כלכליות של גניבת קניין רוחני דיגיטלי פרטי ומסחרי יכולות לסייע להגדיר קניין רוחני זה כתשתית קריטית הראויה להגנה לאומית מפני גניבת סייבר. המאמר אינו מתיימר להציג אמצעים ספציפיים להגנה כזאת, וגם אינו מציע שהגנה ממשלתית על קניין רוחני פרטי צריכה להיות שוות ערך להגנת סייבר על תשתיות קריטיות לאומיות; כל שהוא מבקש להציע היא מסגרת כללית להשגת איזון טוב יותר בין ההגנה על תשתיות קריטיות לאומיות ובין ההגנה על הקניין הרוחני במרחב הסייבר.

תשתיות פיזיות קריטיות – הגדרה והיקף

מתקפות סייבר הן פריצות של האקרים, בעיקר מחוץ לרשת, במטרה להשיג שליטה מסוימת או מלאה על הרשת.[5] שליטה כזו משמשת לשתי מטרות: תקיפת רשתות מחשבים (CNA), או ניצול (Exploitation) של רשתות מחשבים (CNE).[6]

מתקפות סייבר מבקשות לחדור לרשתות מחשבים מסיבות פוליטיות או פליליות, או ממניעים של ביטחון לאומי.[7] סוכנויות ממשלתיות, חברות בשוק הפרטי או יחידים יכולים להיות בעלי מניעים למעורבות בגניבת סייבר או בהשגת קניין רוחני דיגיטלי.

ממשלות אחראיות לספק הגנה וביטחון לאזרחים ולנכסים הלאומיים שלהן,[8] אולם הדָרגה שבה אחריות זו מתממשת משתנה בין מדינות בהתאם למשטר הנהוג בהן. על פי ג'יימס לואיס (Lewis) וקתרינה טימלין (Timlin) מהמכון ללימודים אסטרטגיים בין־לאומיים בוושינגטון די. סי., ככל שהאינטרנט הופך לתשתית גלובלית מודרנית לעסקי סחר בין־לאומיים ולפעילות ממשלתית, כך אבטחת הסייבר הופכת לעניין לאומי ובין־לאומי גם יחד.[9] ד"ר קריסטין לורד (Lord) וטרוויס שארפ (Sharp) מציינים כי מספרן של מתקפות הסייבר שנובעות ממניעים פליליים ופוליטיים גדל במהירות. הערכתם היא כי מדי חודש מתרחשות 1.8 מיליארד מתקפות סייבר, בדרגות חומרה שונות של תחכום, נגד הקונגרס של ארצות הברית וסוכנויות פדרליות אמריקאיות בלבד.[10] אריק סטרנר (Sterner) ממשרד ההגנה של ארצות הברית גורס שמספר מתקפות הסייבר גדול הרבה יותר מכך, במיוחד אם כוללים בהן גם מתקפות בין־לאומיות על ממשלות זרות ומגזרים פרטיים.[11] פרופ' אריק טלבוט ג'נסן (Talbot Jensen) מעריך כי אלפי חברות בכל העולם נמצאות תחת מתקפה בכל רגע נתון, וכי הקניין הרוחני שלהן, ובמיוחד סודותיהן המסחריים, נפגעים כתוצאה מכך.[12] למעשה, רק אם הממשלה וסוכנויותיה הרלוונטיות מיידעות את החברות המסחריות והפרטיות בנוגע למתקפה, הן מודעות לה. במקרים אחרים, חברות אינן מודעות כלל לכך שהן מותקפות, וכשהן מגלות זאת, כבר מאוחר מדי לטפל באיום, שכן נתוני החברה והקניין הרוחני שלה כבר נגנבו.[13]

מכל מתקפות הסייבר האפשריות, מתקפות ניצול (CNE), שבמגזר הפרטי באות לידי ביטוי בעיקר כגניבת קניין רוחני, הן המטרידות ביותר. על פי מרטין ליביקי, מתקפות CNE מעוררות דאגה רבה, בעיקר משום שהן מתמקדות בגניבת נתונים וסודות דיגיטליים ועושות זאת "מתחת למכ"ם" של הבעלים, מבלי שהן נחשפות ובשיטות שקשה לזהות.[14] לכן, גניבת קניין רוחני ומתקפות ניצול הן האיום הגדול ביותר על שמירה וניהול של קניין רוחני פרטי או מסחרי, דוגמת סודות מסחריים.

הגידול המהיר במתקפות סייבר בזירה הבין־לאומית, והאיום שהן מטילות על מערך האבטחה הגלובלית ועל מערכות כלכליות בכלל, הפכו למצב קבוע ומתמשך של פשעי סייבר ולוחמת סייבר. מתקפות סייבר אלו נעשות מצד אחד על ידי יחידות צבאיות מיומנות הפועלות מסיבות פוליטיות, ומצד שני על ידי פושעים מומחים המונעים מכוח אינטרסים מסחריים ופליליים.[15] התפתחות מתקפות הסייבר הביאה ממשלות בכל רחבי העולם להקים סוכנויות ייעודיות להגנת סייבר

ולגבש דוקטרינות בתחום זה, וזאת כדי להתמודד בדרך אפקטיבית עם האיומים החדשים ההולכים ומתרחבים במרחב הסייבר. כך, למשל, "סוכנות פיקוד הסייבר" (Cyber Command Agency) בארצות הברית מופקדת על התמודדות עם כל סוגי האיומים על תשתיות סייבר – קריטיות וצבאיות – המגיעים ממקורות פוליטיים. גופי ממשל אחרים, כמו ה־FBI, עוסקים באיומי סייבר שמקורם בפלילים.[16] מצב זה הוא תוצאה של ההסתמכות הגוברת של העולם המודרני על מערכות מידע מרושתות, ששולטות בתשתיות הקריטיות ובמערכות התקשורת והפכו חיוניות לאורח החיים הנוכחי.[17]

האחריות הגוברת של ממשלות במרבית המדינות המערביות על תחום הסייבר מתבטאת בעיקר בהגנה על תשתיות ואינטרסים בין־לאומיים, תוך התעלמות מהצורך להגן גם על קניין רוחני, מסחרי ופרטי. צרפת[18] וגרמניה[19] רואות באיומי הסייבר על תשתיות לאומיות קריטיות איום אסטרטגי, שזכה לעדיפות בדוקטרינת ההגנה שלהן. בבריטניה, הדגש מושם בעיקר על נכסים ממשלתיים, פעילויות, ארגונים לאומיים ותשתיות קריטיות, כמו המערכת הפיננסית.[20] בישראל, המשטרה היא האחראית על טיפול בפשעי סייבר, בעוד שמטה הסייבר הלאומי במשרד ראש הממשלה אחראי על הגנה התשתיות הקריטיות של המדינה, ואף זוכה למשאבים ולתשומת לב ממשלתית רבים יותר.[21]

הדגש הדומה ששמות ממשלות מערביות על הגנת תשתיות לאומיות מפני התקפות סייבר שונות מצביע על הסכמה רחבה בדבר הצורך לתת עדיפות להגנה פיזית על תשתיות לאומיות קריטיות במרחב הסייבר. הסכמה זו קיבלה דחיפה נוכח מספר מתקפות סייבר נגד תשתיות לאומיות קריטיות שזכו לחשיפה רבה בשנים האחרונות והעלו את המודעות לסוג זה של מתקפות. מתקפת הסייבר הגדולה על אסטוניה בשנת 2007,[22] ומתקפת "סטקסנט" על תוכנית הגרעין של איראן בשנת 2010[23] גרמו למרבית המדינות לתת עדיפות, במסגרת דוקטרינות ההגנה שלהן, להגנה ממשלתית פיזית על תשתיות קריטיות.

על פי ברוס ברקוביץ (Berkowitz), תשתיות קריטיות ונכסי מפתח הם מרכיבים חיוניים בכל מדינה: אם יותקפו דרך מרחב הסייבר, תימצא המדינה הנתונה למתקפה במצב קיצוני של פגיעות.[24] לדבריו, ההתפתחות הטכנולוגית והתלות הגוברת של תהליכים צבאיים וממשלתיים במרחב הסייבר הביאו לכך שההגדרה של תשתיות קריטיות הלכה והתרחבה. ברקוביץ גם סבור כי העובדה שקניין רוחני דיגיטלי ומערכות מידע הם כה חיוניים לממשלות, לחברה האזרחית ולצבאות המודרניים, עשויה להפוך אותם למטרות מרכזיות בעת מלחמה.[25] המסקנה היא שיֵש מקום לעדכן את ההגדרה של המושג "תשתית קריטית", כך שתכלול את מרכיבי הליבה הדיגיטליים.[26]

לוחמת סייבר, והאיום הישיר שהיא מטילה על היציבות ואורח החיים של מדינות שונות, הביאו את הקהילה הבין־לאומית לגבש דוקטרינות לאומיות להגנת סייבר. דוקטרינות אסטרטגיות אלו מבקשות להתמודד עם האיום הפוליטי באמצעות הגנה פיזית על התשתיות הקריטיות, אולם אינן נותנות מענה מספק לאיומים של גניבה פלילית של קניין רוחני ומתקפות ניצול על נכסים מסחריים ופרטיים. מצב זה מעלה את השאלה האם ההשלכות המקרו־כלכליות של העלייה בהיקף גניבות הסייבר צריכות להניע ממשלות לראות בקניין רוחני דיגיטלי, הן פרטי והן מסחרי, חלק מהתשתית הקריטית שראוי להגן עליה פרואקטיבית מפני גניבת סייבר, פוליטית ופלילית גם יחד.

קניין רוחני דיגיטלי, מסחרי ופרטי, כתשתית לאומית קריטית

למרות השוני בהגדרה הפורמאלית של קניין רוחני במדינות שונות, יש הסכמה על שלושה קריטריונים החייבים להתקיים כדי שקניין רוחני ייחשב כסוד מסחרי מבחינה משפטית: ראשית, על שמירת הנתונים כסוד להעניק יתרון תחרותי; שנית, חובה שהנתונים אכן יישמרו כסוד: קריטריון הסודיות הוא מוחלט ומחייב שלא ניתן יהיה לקחת או לחלץ את הסוד בקלות מהמוצר הזמין בשוק; שלישית, על הנתונים השמורים להיות מוגנים באמצעות מנגנון הגנת סודיות סביר[27] (לרבות טכנולוגיות הגנת סייבר), שמרחיק מהם פולשים. ישנם בתי משפט שמכירים גם בקריטריון רביעי של חבות, ותובעים שהמידע הסודי יימצא בשימוש מתמיד בעסקי החברה.

כפי שצוין קודם לכן, פעמים רבות חברות אינן יודעות שהנתונים שלהן נגנבו דרך מרחב הסייבר, וכאשר הן מגלות זאת, הן נמנעות לא פעם מלדווח על האובדן מתוך חשש לנזק מסחרי פוטנציאלי לִשמן.[28] גניבת סייבר של קניין רוחני מסחרי או פרטי יכולה להיות ממניעים פוליטיים, שמכוּונים "ריגול כלכלי" (ביוזמת מדינה),[29] או ממניעים פליליים שחותרים להשיג יתרון בשוק המסחרי, המכונים "ריגול תעשייתי".[30] ההשלכות הפוטנציאליות המקרו־כלכליות של גניבה כזו על החברה ממנה נגנב הקניין הרוחני הן עצומות והרסניות, ללא תלות במניע או במטרה המקוריים. חברות שהקניין הרוחני נגנב מהן מסתמכות על שיטות שונות כדי לאמוד את הנזק הכספי הנובע מכך. חלקן מבססות את ההערכות שלהן על העלויות בפועל של פיתוח הנתונים הסודיים שנגנבו, ואילו אחרות מחשבות את אובדן ההכנסה העתידי שנגרם להן בגין הגניבה.[31]

מלבד הנזק שנגרם לחברה מסוימת מגניבת הקניין הרוחני שלה, השאלה המתעוררת היא האם גניבת סודות מסחריים מסוימים יכולה להביא לפגיעה מקרו־כלכלית בחוסן (resilience) של מדינה. גניבת סייבר של קניין רוחני דיגיטלי פוגעת ביכולת של המגזר הפיננסי המקומי לייצר הכנסות ומשרות חדשות או

לפתח חידושים,[32] וצפויה לגרום להפסדים בהכנסות ממסים, שיקטינו את תקבולי המדינה ואת התמ"ג שלה.[33] כתוצאה מכך, גניבת סייבר של קניין רוחני פרטי או מסחרי, בקנה מידה גדול ורחב היקף, יכולה להיות מתורגמת להפסד מקרו־כלכלי משמעותי, שיסתכם במיליארדים וישתקף בצניחה בתוצר הלאומי הגולמי.[34] גניבת סייבר משוכללת ומתוכננת היטב של סודות מסחריים דיגיטליים (ללא קשר למניע שמאחוריה) עלולה אפילו לגרור פשיטת רגל פתאומית של מדינה כתוצאה מאיבוד הכנסות עתק בעקבות אובדן תקבולים והכנסות ממיסוי החברות המחזיקות בבעלות על הקניין הרוחני שנגנב דרך מרחב הסייבר. ניתוח כלכלי שנערך על ידי גורם אמריקאי רשמי מעריך כי ההפסדים שנגרמו כתוצאה מגניבת סודות מסחריים בסייבר בארצות הברית בלבד, נעים בין שני מיליארד דולר ל־400 מיליארד דולר ויותר מדי שנה.[35]

המוטיבציה הראשונית לגניבת הסייבר אינה רלוונטית במיוחד כאשר שוקלים גישות שונות של הגנת סייבר. זאת, מכיוון שאין קשר בין מטרותיה של מתקפת הסייבר מצד אחד ובין השלכותיה המקרו־כלכליות ההרסניות ושיטות המניעה המקיפות (מבחינה טכנולוגית ודוקטרינרית) של הגנת הסייבר מצד שני. יחד עם זאת, ההשפעה הכלכלית שיש לגניבת סייבר על החוסן הלאומי היא בכל מקרה משמעותית.

קצב החדשנות, המחקר והפיתוח במגזר הפרטי והמסחרי במאה הנוכחית האיץ את צמיחת הסודות המסחריים ואת מספר הפטנטים שנרשמים בארצות הברית ב־40.6 אחוזים, עובדה הממחישה יותר מכל את התפקיד רב העוצמה שממלאים סודות מסחריים בכלכלה הגלובלית.[36] על פי נתוני הארגון האמריקאי של מנכ"לים בענף ההייטק (Technet), יותר משישה מיליון מקומות עבודה ושליש מהכלכלה האמריקאית (שהיקפה 15 טריליון דולר) מבוססים על חדשנות, ולכן על סודות מסחריים וקניין רוחני.[37] גנרל קית' אלכסנדר, לשעבר ראש סוכנות הביטחון הלאומי ופיקוד הסייבר של ארצות הברית, העריך שההפסדים לתמ"ג האמריקאי בעקבות גניבת סודות מסחריים במרחב הסייבר עומדים על כ־205 מיליארד דולר לשנה, וכינה זאת "העברת ההון הגדולה בהיסטוריה".[38] דוגמה בולטת לכך היא גניבת התוכניות של מטוס הקרב החמקן F–35 מחברת "לוקהיד מרטין" ב־2007, לכאורה על ידי חברה סינית שפיתחה אז מטוס קרב דומה (J–20).[39] המניעים מאחורי גניבת סייבר זאת היו אמנם פוליטיים, אך הייתה לה השפעה כלכלית רבה.

אחת הדרכים להבין את ערכם המקרו־כלכלי של סודות מסחריים, ובהתאם לכך את הפוטנציאל לאובדן ההכנסות למדינה מגניבתם, היא באמצעות סקירת ההשקעות שמשקיע המגזר הפרטי והמסחרי במחקר ופיתוח. אמנם, ישנם סודות מסחריים רבים וחשובים שאינם קשורים למחקר ופיתוח (כמו, למשל, נתוני מכירות, רשימות לקוחות, אסטרטגיות שיווק וכדומה), אולם תחום המחקר והפיתוח מייצג

השקעה בטכנולוגיות החדשות ביותר, ברעיונות ובהמצאות, שכולם הם מרכיבים חיוניים בסודות מסחריים רבים.[40] ההשקעות במו"פ בארצות הברית מהוות 2.7 אחוזים מהתמ"ג, ומסתכמות בכ־447 מיליארד דולר לשנה. השקעות במו"פ בגרמניה מהוות 2.9 אחוזים מהתמ"ג, בסין – שני אחוזים מהתמ"ג, בבריטניה – 1.8 אחוזים וברוסיה – 1.5 אחוזים.[41] כל השקעה במו"פ מייצרת גרסאות נוספות של סודות מסחריים חדשים (דולר אחד של השקעת מו"פ יצר עד 69 דולר של סודות מסחריים חדשים במהלך העשור האחרון), כך שערכם הכלכלי של סודות מסחריים גדול אפילו יותר מאשר ההשקעה הבסיסית במו"פ.[42]

במציאות שבה מרבית הנכסים בעלי הערך, וכן התשתיות, הם דיגיטליים, בלתי מוחשיים וקלים להעברה ברשת, גניבת סייבר של קניין רוחני מקבלת חשיבות קריטית נוספת.[43] בדוח משנת 2001, שהקיף 14 סוכנויות ביון אמריקאיות, הוערך כי גניבת סייבר עתידה להפוך ל"איום מתגבר ומתמשך",[44] וראש קהילת המודיעין האמריקאי דירג אותה כאיום קונקרטי משמעותי יותר אפילו מאיום הטרור.[45] על פי דוח של מכון Ponemon, יש עלייה בהיקף גניבת קניין רוחני במרחב הסייבר, כאשר חלק מהחברות חוות מעל 72 מתקפות סייבר בשבוע.[46]

ככל שקניין רוחני הופך לגורם דומיננטי ומכריע בכלכלה המודרנית (כפי שניתן להבין מהסטטיסטיקות שהובאו לעיל), כל גניבה שלו או נזק שייגרם לו יביאו להפסדים כספיים כבדים למדינה לה הוא שייך. לפיכך, כלכלות לאומיות ימצאו עצמן בסיכון כלכלי עצום, אם יקרה דבר מה לקניין הרוחני הדיגיטלי הפרטי או המסחרי שלהן. דוח של הקונגרס האמריקאי בנושא הריגול התעשייתי ציין בהקשר זה כי גניבת קניין רוחני מחברות פרטיות ומסחריות עלולה להשפיע על היכולת של המגזר הפרטי לייצר הכנסות ומקומות עבודה, לעודד חדשנות ולהניח את התשתית הכלכלית לצמיחה עתידית ולביטחון לאומי.[47] ואכן, החשיבות הגוברת של קניין רוחני דיגיטלי לכלכלה המודרנית מצד אחד, והנזק ההרסני הפוטנציאלי לכלכלה של אותה מדינה במקרה של גניבתו מצד שני, הופכים את האיום של גניבת קניין רוחני במרחב הסייבר למסוכן ביותר לחוסנה הכלכלי של המדינה. זאת ועוד, העלייה במספר מתקפות הסייבר שמתמקדות בגניבת קניין רוחני דיגיטלי, וההפסדים המקרו־כלכליים הכבדים הנובעים מכך, מכניסים את הקניין הרוחני הדיגיטלי המסחרי והפרטי לתוך ההגדרה של תשתיות לאומיות קריטיות שראויות להגנה על ידי המדינה. הדבר מחייב ממשלות ליישם את אמצעי הזהירות הנדרשים ולהפעיל גישת הגנה פרואקטיבית נגד מתקפות סייבר על התשתית הקריטית של קניין רוחני פרטי או מסחרי.

הגנה על קניין רוחני פרטי ומסחרי מפני גניבת סייבר היא קריטית לרווחיות החברה ולצמיחתה,[48] אולם יש להתייחס אליה גם כאל גורם בעל חשיבות לאומית. הסיבה לכך היא שקניין רוחני מסחרי משפיע על הכלכלה הלאומית באמצעות

הכנסות ממסים, הכנסות בלתי ישירות אחרות והתמ"ג, ולפיכך כל גניבה של קניין רוחני מסחרי בקנה מידה גדול במרחב הסייבר עלולה לפגוע בחוסן הכלכלי של המדינה ואף לגרום לתגובת שרשרת העלולה להיות חמורה פי כמה מכל מתקפת סייבר על תשתית קריטית בודדת. לכן, על ממשלות ליטול אחריות, ולו מסוימת, על הגנת קניין רוחני מסחרי ופרטי, ולאמץ גישה מעורבת ופרואקטיבית להגנתם. מהלך כזה עלול לעורר דילמה, שכן לצד החשיבות של קניין רוחני לחוסנה של המדינה מבחינה מקרו־כלכלית, הוא גם ישות הנמצאת בבעלות פרטית, ואינו שייך לממשלת אותה מדינה.

מודלים של זכויות יוצרים במדינות שונות

לאחר שאִפיַנו את הבעיה והצבענו על המצב שבו ממשלות נמנעות מקבלת אחריות על הגנת קניין רוחני פרטי ומסחרי מפני מתקפות סייבר, נפנה להגדיר מודלים קיימים של זכויות יוצרים במדינות שונות ולהמליץ על פתרון שיתבסס עליהם. למרות שזכויות יוצרים הן רק סוג אחד של קניין רוחני, חלק מהמרכיבים בשיטות ההגנה עליהן עשויים להיות רלוונטיים גם להגדרת האחריות הממשלתית להגנה אופטימלית על קניין רוחני דיגיטלי פרטי ומסחרי באופן כללי, ועל סודות מסחריים באופן ספציפי.

המודל האנגלי־אמריקאי נועד להבטיח את טובת הציבור ורווחתו באמצעות הפעלת תמריצים כלכליים עבור בעלי הזכויות – דבר שמעודד יצירת מוצרים חדשים.[49] לפי מודל זה, הגנה ממשלתית פרואקטיבית על קניין רוחני דיגיטלי תעודד ישויות מסחריות ואנשים פרטיים להמשיך לייצר סודות מסחריים חדשים. לעומת זאת יש מי שטוען כי אין כל עדות אמפירית לכך שהגנה חזקה על קניין רוחני מגדילה את היקפו.[50] זוהי טענה שעשויה להיות נכונה כאשר מדובר בזכויות יוצרים בתחום האמנות והמדעים; לעומת זאת, סודות מסחריים מושפעים יותר מתמריצים כלכליים, שכן אלה משמשים גורם חשוב בצמיחתה הכלכלית של מדינה. הגנת סייבר פרואקטיבית של המדינה על סודות מסחריים תמשוך ממציאים חדשים הודות לתמריצים הכלכליים שהיא מעניקה. בדרך זו, הגנת סייבר ממשלתית על קניין רוחני דיגיטלי יוצרת רווח כפול: מניעת נזקים מקרו־כלכליים בקנה מידה לאומי כתוצאה מגניבת סייבר של קניין רוחני מסחרי, ועידוד צמיחה של קניין רוחני מסחרי חדש. שני יתרונות תוצאתיים אלה משקפים, כאמור, את המודל האנגלי־אמריקאי, שתורם לציבור בזכות העידוד שהוא נותן להמצאות נוספות ובזכות חיזוק החוסן הכלכלי הלאומי.

המודל הצרפתי לזכויות קניין משלים את המודל האנגלי־אמריקאי ומנסח את תפקידה של הממשלה בשמירה על הקניין הרוחני בידי בעליו. על פי המודל צרפתי, ובהתבסס על זכויות היוצרים, לא ניתן לנתק בין היצירה ליוצרה, שמחזיק

בזכויות הקניין על עבודתו.[51] היבט זה של המודל הצרפתי מטיל על הממשלה אחריות להבטיח שהקניין הרוחני הדיגיטלי יישאר מוגן כנכס של היוצר, ומונע הפקעת נכסים מסוג זה מבעליהם. במילים אחרות, המודל הצרפתי מבטיח שהגנה ממשלתית על קניין רוחני דיגיטלי פרטי ומסחרי לא תוביל להלאמה של קניין רוחני המצוי בבעלות פרטית וגם לא תביא להתערבות ממשלתית מוגזמת במגזר הפרטי. מודל זה מסייע לקביעת המידה הראויה והמאוזנת של הגנת סייבר ממשלתית על קניין רוחני פרטי ומסחרי. כמו כן, יש בו כדי לסייע להשגת מצב כלכלי לאומי איתן יותר, שיגביל כל חדירה מוגזמת מצד הממשלה למגזר הפרטי.

לסיכום, גישת המודל האנגלי־אמריקאי מסייעת לדרבן ממשלות לקבל על עצמן אחריות להגנה על קניין רוחני דיגיטלי פרטי ומסחרי, מתוך הבנה שההשלכות המקרו־כלכליות הלאומיות של נטילת אחריות כזאת ישרתו את טובת הציבור. מרכיבים במודל הצרפתי מבטיחים שחדירה ממשלתית למגזר הפרטי במסגרת ההגנה על הקניין הרוחני לא תפקיע את הבעלות על קניין זה מידי בעליו. הסינתזה המשפטית בין המודל האנגלי־אמריקאי והמודל הצרפתי יוצרת אחריות ממשלתית פרואקטיבית מאוזנת, מבלי שייחָצה הקו הדק המפריד בין המגזר הפרטי למגזר הציבורי.

האחריות והתפקיד הפרואקטיבי של הממשלה

לאור העקרונות והמודלים שהוצגו לעיל, נתמקד בשני מרכיבי ביצוע מרכזיים הנובעים מהאחריות הממשלתית הכוללת להגנה על קניין רוחני דיגיטלי, שכאמור, נועדה להשיג הגנה פרואקטיבית על קניין זה, כולל צדדיו הפרטיים והמסחריים. המרכיב הראשון הוא חקיקה של חוקי הגנת סייבר ייעודיים, שיספקו הגנה על קניין רוחני דיגיטלי פרטי וציבורי מכל הסוגים. בחלק מהמדינות קיים חוק מקיף ואחיד בנושא זה, ואילו מדינות אחרות מסתמכות על מערך של חוקים שונים, שבצירופם יחד משיגים הגנה משפטית מלאה על הקניין הרוחני. לדוגמה, בארצות הברית חוקקו שני חוקים בעניין סודות מסחריים, האחד בעל אוריינטציה אזרחית והשני בעל אוריינטציה פלילית: הראשון הוא חוק Uniform Trade Secrets Act (UTSA) משנת 1979, שמספק הגדרה רשמית וקריטריונים לסודות מסחריים ומגדיר מהי גניבה שלהם ומהו הסעד ההולם בעקבות גניבה כזו (כגון מתן צו מניעה, פיצוי כלכלי, תשלום שכר טרחת עורך דין וכיוצא באלה).[52] החוק השני נחקק ב־1996 ונקרא Economic Espionage Act (EEA), ובעקבותיו הפכו גניבה של סודות מסחריים וריגול כלכלי לפשעים פדרליים שעונשיהם נקבעו בהתאם.[53] שני החוקים מתמקדים בתוצאה ובהשלכות של גניבת סודות מסחריים דיגיטליים, אך אינם מנסים למנוע מראש ובזמן אמת את מעשה הגניבה עצמו.

חקיקת חוקי סייבר ייעודיים עשויה להרתיע במידה מסוימת תוקף סייבר פוטנציאלי, אולם אין בה כשלעצמה די כאמצעי מונע, מכיוון שמרחב הסייבר מספק לתוקפים אנונימיות יחסית, לרבות סיכון נמוך לזיהוי וקושי בהטלת האשמה על תוקפים ספציפיים.[54] לאור זאת, המרכיב השני של האחריות הממשלתית להגנה פרואקטיבית על קניין רוחני דיגיטלי הוא עיצוב דוקטרינת הגנת סייבר מקיפה, שמכירה ברמת האחריות האסטרטגית של הממשלה ובתעדוף הנובע ממנה לגבי הגנה על קניין רוחני דיגיטלי פרטי ומסחרי. דוקטרינות הגנת סייבר לאומיות כאלו לא יהיו הצהרתיות בלבד, אלא יגלמו בתוכן את העדיפות הלאומית במונחים של הקצאת משאבים (תקציבים, כוח אדם, יישום פתרונות טכנולוגיים ייעודיים וכיוצא באלה), כדי להגן על נכסים דיגיטליים חיוניים. לדוגמה, נשיא צרפת, פרנסואה הולנד, פרסם בשנת 2013 דוקטרינת הגנת סייבר לאומית כללית שמתייחסת לאיום גניבת סייבר. הדוקטרינה הצרפתית מדגישה את החשיבות שיש להגנה על נכסיה הטכנולוגיים והמדעיים של צרפת ולמניעת גניבה של ידע ומידע צרפתיים בעלי אופי פרטי וציבורי כאחד.[55] דוגמה טובה נוספת אפשר למצוא בדוקטרינת אסטרטגיית הסייבר של בריטניה, שמדגישה את החשיבות שיש להגנה על הקניין הרוחני הדיגיטלי של המדינה, לצד הגנה על תשתיות קריטיות צבאיות ולאומיות אחרות.[56] הדוח *Digital Britain* משרטט את חזון הדיגיטליזציה של בריטניה ומדגיש את החשיבות של הגנת סייבר כחלק מחזון אסטרטגי לאומי.[57]

שני מרכיבים מוצעים אלה – חוקים ודוקטרינות אסטרטגיות – גם הם אינם מספיקים כדי לפתור את בעיית גניבת הקניין הרוחני הדיגיטלי, ועדיין יש צורך בגישה ממשלתית פרואקטיבית כדי למנוע גניבת סייבר כזאת. על פי פרופ׳ לורנס לסיג (Lessig), האחריות הפרואקטיבית של הממשלה להגנה על נכסים פרטיים ומסחריים יכולה להתבצע ללא הסכמת הבעלים או ידיעתם,[58] אם כי סוג כזה של פעילות ממשלתית פירושה הפרה של זכויות אדם, ובמיוחד של זכות האדם לפרטיות. גלן גרינוולד (Greenwald) מצידו סבור כי המעורבות הממשלתית הגוברת במרחב הסייבר לא רק שתפגע בפרטיות הציבור, אלא תעשה מעט מאוד לשיפור אבטחת הסייבר.[59]

הפתרון הנכון צריך להיות פתרון מאוזן: על הממשלה להפעיל הגנה פרואקטיבית על קניין רוחני דיגיטלי פרטי ומסחרי, ובמקביל לדאוג להגבלה מרבית של כל אפשרות להפרת פרטיות במה שנוגע לנתונים ונכסים שאינם עונים על ההגדרה של קניין רוחני. במקום להסתפק בהגנה על רשתות צבאיות בלבד כדי למנוע חדירה עוינת, על הממשלות לפרוס את אמצעי הגנת הסייבר שלהן בכל המרחב הדיגיטלי האזרחי/ציבורי, ובכך להגן על רשתות ציבוריות וציבוריות־אזרחיות משותפות, וכן על נתבי ומתגי תעבורה לאומיים, כדוגמת ספקיות אינטרנט.

הפתרון האופטימלי להגנה על קניין רוחני פרטי ומסחרי צריך להיות באמצעות חקיקת חוקים הולמים וגיבוש דוקטרינות הגנת סייבר אסטרטגיות לאומיות, שביחד יניחו את היסודות שיעניקו לממשלות את הכלים והלגיטימיות הנכונים להגן בצורה פרואקטיבית על נכסים דיגיטליים חיוניים, פרטיים ואזרחיים. בנוסף להגנת סייבר ממשלתית, על חברות מסחריות ופרטיות להשקיע מאמצים ולעשות שימוש במשאבים ובהשקעות שבידיהן כדי למנוע ולאתר כל פרצה בתוך הרשתות שלהן וכל ניסיון לגניבת סייבר מתוכן.

מסקנות

> "החוק החדש לריגול כלכלי יסייע לנו לפצח עבירות כגון פירטיות תוכנה והפרת זכויות יוצרים, שעולות למשק האמריקאי מיליארדי דולרים באובדן הכנסות, ובכך יחזק את הביטחון הלאומי שלנו".[60]
>
> נשיא ארצות הברית, ביל קלינטון

הרבה השתנה מאז השמיע נשיא ארצות הברית את דבריו אלה על התקווה לעצור מעשי פירטיות והפרת זכויות יוצרים של סודות מסחריים וסוגים אחרים של קניין רוחני. מרחב הסייבר התפתח במהירות בעשרים השנים האחרונות, כשהוא מצמיח איומים אסטרטגיים חדשים, כמו גניבה של קניין רוחני דיגיטלי פרטי ומסחרי. במקביל, הקניין הרוחני הדיגיטלי הפרטי והמסחרי בכלל, וסודות מסחריים בפרט, הפכו לגורמים קריטיים ודומיננטיים בכלכלה בת־זמננו.

הגישה המיושנת של הטלת עונשים לאחר מעשה ועל בסיס התוצאות כמעט שאינה רלוונטית כיום, נוכח הקושי לאתר גניבות במרחב הסייבר בזמן אמת והיכולת הבו־זמנית להטיל את האחריות למניע הזדוני על כל אדם, ארגון או מדינה. המסקנה הנובעת מכך היא שממשלות בכל רחבי העולם צריכות לשנות את תפקידן ואחריותן בתחום ההגנה מפני גניבות במרחב הסייבר ולעבור לגישה פרואקטיבית שתתבסס על דוקטרינות, חקיקה ותקנות. עליהן ליטול על עצמן אחריות מסוימת להגנה על קניין רוחני דיגיטלי מסחרי ופרטי, וזאת בשל הפוטנציאל לכשל כלכלי עמוק במקרה של גניבות כאלו, וההשלכות שלהן על המערכות המקרו־כלכליות. ההפסדים המקרו־כלכליים הצפויים מגניבות במרחב הסייבר מגבירים את החשיבות של הגנה על הקניין הרוחני הפרטי והמסחרי של המדינה בכל תחומיו של מרחב זה. לפיכך, עליה להתייחס אל ההגנה על הקניין הרוחני בצורה דומה להתייחסותה להגנה על תשתיות קריטיות פיזיות וצבאיות. המודל האנגלי־אמריקאי יוכל להביא לכך שההגנה הממשלתית על הקניין הרוחני תכיל תמריצים כלכליים ליצירת קניין רוחני חדש; המודל הצרפתי יכול לעזור בניסוח זכותו האינדיבידואלית של היוצר לשמור ברשותו את הקניין הרוחני שפיתח.

הערות

1 President Barack Obama, "Remarks on Securing Our Nation's Cyber Infrastructure," Office of the Press Secretary, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

2 President Barack Obama, "Remarks by the President at the Export-Import Bank's Annual Conference," Office of the Press Secretary, March 11, 2010, http://www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference

3 מרחב הסייבר הוא מדיום וירטואלי המורכב מצבר של התקנים ממוחשבים ומרושתים המחוברים לעולם שבחוץ (האינטרנט למשל). ראו: Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009).

4 Pamela Passman, Sanjay Subramanian, George Prokop, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats* (Washington, DC: The Center for Responsible Enterprise and Trade, 2013), p. 8.

5 Libicki, *Cyber Deterrence and Cyberwar*.

6 המושג CNA (Computer Network Attack) מתייחס למתקפה על הרשת והתהליכים העסקיים בה באמצעות שיבוש, מניעת שירות או הרס של מידע המאוחסן בה. המושג CNE (Computer Network Exploitation) מתייחס לגניבת נתונים מהרשת. ראו: US Department of Defense, *Dictionary of Military and Associated Terms* (Joint Education and Doctrine Division, 2014).

7 Oona A. Hathaway and others, "The Law of Cyber-Attack," *California Law Review*, 100, no. 4 (2012), p. 827.

8 Gareth Evans, Mohamed Shanoun, *The Responsibility to Protect: Report for the International Commission on Intervention and State Sovereignty* (Ottawa: International Development Research Centre, 2001), p. 13.

9 James A. Lewis, Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, 2011), p. 3.

10 Kristin M. Lord, Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, DC: Center for a New American Security, 2011), p. 7.

11 Eric R. Sterner, "Deterrence in Cyberspace: Yes, No, Maybe?" in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, ed. Robert Butterworth (Arlington, VA: George C. Marshall Institute, 2011), pp. 28-35.

12 Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," *Texas Law Review*, 88 (2010), p. 1536.

13 Kim Zetter, "Report Details Hacks Targeting Google, Others," WIRED, February 3, 2010, http://www.wired.com/threatlevel/2010/02/apt-hacks/

14 Libicki, *Cyber Deterrence and Cyberwar*, p. 23.

15 Abraham R. Wagner, "Cybersecurity: From Experiment to Infrastructure," *Defense Dossier*, 4 (2012), p. 17.

16 Lewis and Timlin, *Cybersecurity and Cyberwarfare,* p. 22.

17 The White House, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (2011), p. 9.

18 Lewis, Timlin, *Cybersecurity and Cyberwarfare,* p. 11.

19 Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin, 2011).

20 UK Office of Cyber Security and UK Cyber Security Operations Centre, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (London, 2009), p. 9.

21 Israel's Prime Minister's Office, *Advancing National Cyber Space Capabilities – Decision Number 3611* (August 7, 2011).

22 Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, 56 (2011), p. 569.

23 Thomas M. Chen, "Stuxnet, the Real Start of Cyber Warfare?," *IEEE Network*, 24, no. 6 (2010), p. 3.

24 Bruce D. Berkowitz, "Warfare in the Information Age," In *Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla, David Ronfeldt (Santa Monica: RAND National Security Research Division, 1997), p. 181.

25 שם. עמ' 177, 181.

26 Myriam A. Dunn, "Securing the Information Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory," *International Relations and Security in the Digital Age* (ETH Zurich: Center for Security Studies, 2007), p. 11.

27 Robert G. Bone, "A New Look at Trade Secret Law: Doctrine in Search of Justification," *California Law Review*, 86 (1998), pp. 248-249.

28 Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

29 שם. עמ' 7.

30 שם. עמ' 8.

31 שם. עמ' 2.

32 שם. עמ' 3.

33 Passman, Subramanian, Prokop, *Economic Impact of Trade Secret Theft*, p. 8.

34 Shahar Argaman, Gabi Siboni, "Commercial and Industrial Cyber Espionage in Israel," *Military and Strategic Affairs*, 6 (2014), p. 51, http://media.wix.com/ugd/d48d94_a62f01468dc8448ebe635f8d962c410f.pdf

35 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets*, p. 4.

36 Passman, Subramanian, Prokop, *Economic Impact of Trade Secret Theft*, p. 7.

37 Dennis C. Blair, Jon M. Huntsman, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (The National Bureau of Asian Research, 2013), p. 23.

38 Carrie Lukas, "It's Time for The U.S. to Deal with Cyber-Espionage," *U.S. News and World Report*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy

39 Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China: Hearing on the Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology, Before the Oversight and Investigations Subcommittee of the Foreign

Affairs Committee of the U.S. House of Representatives (2011) (statement of Richard D. Fisher, Jr., Senior Fellow, International Assessment and Strategy Center), p. 5.

40 Passman, Subramanian, Prokop, *Economic Impact of Trade Secret Theft*, p. 8.

41 שם.

42 שם.

43 Blair and Huntsman, *The IP Commission Report*, p. 43.

44 Siobhan Gorman, "China Singled Out for Cyber Spying," *Wall Street Journal*, November 4, 2011, http://allthingsd.com/20111104/china-singled-out-for-cyberspying/

45 Argaman, Siboni, "Commercial and Industrial Cyber Espionage in Israel," p. 54.

46 Ponemon Institute, *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies* (Ponemon Institute, 2011).

47 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets*, p. 3.

48 שם. עמ' 2–A.

49 Neil Netanel, "Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation," *Rutgers Law Journal*, 24 (1993), p. 9.

50 Richard Watt, "An Empirical Analysis of the Economics of Copyright: How Valid are the Results of Studies in Developed Countries for Developing?" in *The Economics of Intellectual Property* (WIPO, 2006), p. 68.

51 Netanel, "Copyright Alienability Restrictions," p. 15.

52 Uniform Trade Secrets Act §§ 1-12 (amended 1985).

53 The Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (1996).

54 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets*, p. 1.

55 President of the French Republic's Office, *French White Paper: Defense and National Security* (2013), p. 102.

56 United Kingdom's Prime Minister's Office, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (2009), p. 9.

57 The United Kingdom's Department of Culture, Media and Sport & the Department for Business, Innovation and Skills, *Digital Britain: Final Report* (2009), pp. 189-207.

58 Lawrence Lessig, "The Law of the Horse: What Cyber Law might Teach," *Harvard Law Review*, 113 (1999), p. 5.

59 Glenn Greenwald, Ewen MacAskill, "Obama Orders US to Draw up Overseas Target List for Cyber-attacks," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

60 President Bill Clinton, "Statement on Signing the Economic Espionage Act of 1996," October 11, 1996, Weekly Compilation of Presidential Documents, 32, no. 41 (October 14, 1996), http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/html/WCPD-1996-10-14-Pg2040.htm.