מבט על, גיליון 912, 2 באפריל 2017

חוק ביטחון הסייבר החדש בסין: מאפיינים והשלכות

דורון אלה, ישראל כנר

ב-1 ביוני 2017 יכנס לתוקף חוק ביטחון הסייבר החדש של סין. על פי הצהרותיה הרשמיות, חוק זה מיועד לשמור על ביטחונה הלאומי של סין ועל יציבותה החברתית, באמצעות פיקוח הדוק על תכנים וטכנולוגיות אינטרנט. לחוק פוטנציאל השפעה על כל גוף עסקי, סיני או זר, הפועל בסין בתחומי האינטרנט וטכנולוגיות מידע. לאחר פרסום החוק עלו חששות במערב, כי עם כניסתו לתוקף, יותנה המשך פעילותן של חברות זרות בסין במסירת מידע וטכנולוגיות לידי הרשויות הסיניות, או בהטמעת "דלתות-אחוריות" במוצריהן. חשש נוסף הוא כי חברות זרות יאלצו לפנות את מקומן לטובת חברות ממשלתיות מקומיות, המפתחות מוצרים המותאמים מבחינה רגולטורית לשוק הסיני.

רקע לחוק

חוק ביטחון הסייבר החדש מצטרף לחוק ה-NGOs וחוק הלוחמה בטרור, שנחקקו בשנה החולפת ומטרתם להגביל ולרסן את פעילותם של ארגונים ופרטים בתוך סין גופא. החוק הוא חלק ממגמת חקיקה מתהדקת, החותרת לקדם את שליטת הממשלה הסינית בממשק הטכנולוגי-אינטרנטי, וכך לצמצם את הסכנה האפשרית ליציבות המשטר כתוצאה משיח-אינטרנט חופשי. דוגמה לכך היא האמנה לריסון עצמי של תעשיית האינטרנט הסיני מ-2002, אשר העבירה את האחריות החוקית על מניעת הפצתם של תכנים לא מורשים לספקי התוכן עצמם, וכך הפכה אותם לסוכני צנזורה מטעם השלטון. החקיקה הסינית בשנת 2016 בנושאי סייבר, ארגונים בינלאומיים לא-ממשלתיים וטרור, מצביעה על חשש הולך וגובר של המפלגה הקומוניסטית הסינית מחדירה של השפעות זרות, הכוללות רעיונות מערביים-ליברלים או דתיים-אסלאמיים והשראה של תנועות היפרדות לאומיות. אחד הכלים המשמשים את המפלגה לשליטה בתכנים המופצים באינטרנט הוא "חומת האש הגדולה של סין", אשר בין היתר אחראית לחסימת הגישה לשירותי אינטרנט מערביים אסורים, כגון גוגל ופייסבוק. חוק הסייבר הוא צעד נוסף בהידוק שליטת המפלגה על המידע וביצור חוסנה השלטוני.

עיקרי החוק

חוק ביטחון הסייבר הסיני, שהוא בעל פוטנציאל השפעה על המערב בכלל ועל ישראל בפרט, נועד להגן על ביטחונה הלאומי של סין ועל שלטון המפלגה הקומוניסטית. החוק מחייב (סעיף 12) את משתמשי הרשת להימנע מפעילות המסכנת את הביטחון, הכבוד והאינטרס הלאומי הסיני; אוסר על קריאת תיגר על המפלגה הקומוניסטית ועל ניסיונות להפיל את המערכת הסוציאליסטית, לקדם טרור ובדלנות דתית או להפיץ מידע כוזב, שעלול לפגוע בכלכלה או בסדר החברתי. כבר בסעיף זה אנו רואים ניסיון לעצב שימוש ברשת, באופן ההולם את צרכיה ויעדיה של המפלגה. החוק קורא לעם לקחת חלק פעיל באכיפתו, ולפיכך דורש (סעיף 14) מכל אדם או ארגון, המזהים פעילות חתרנית ברשת, לדווח מיד למשרדי הממשלה המטפלים בכך.

בחוק מספר סעיפים אשר מעלים חששות ספציפיים עבור חברות מערביות. ראשית קורא החוק לאיסוף מידע אזרחי ושמירתו בתוך גבולות סין בלבד. סעיף 37 קובע, כי כל מידע אישי שנאסף בסין על ידי חברות העוסקות בתשתיות מידע חיוניות חייב להישמר על שרתים בסין (ואם הכרחי לשמרו על שרתים מחוץ לסין, ישנו פרוטוקול מיוחד לכך). בסעיף 24 נכתב כי חברות המעניקות שירותים דוגמת שמות

מאת: **דורון אלה, ישראל כנר**
המכון למחקרי ביטחון לאומי

דומיין, הפצת מידע אונליין, שירותי הודעות וכו', חייבות לדרוש מהלקוח את פרטיו האמתיים ולמנוע ממנו שירות אם סירב למסרם.

שנית, חברות מחויבות לסייע לגופים ממשלתיים-מפלגתיים העוסקים בביטחון לאומי וציבורי. כך, בסעיף 28 נכתב כי "מפעילי רשת" (network operators) יגישו סיוע טכני לגופי ביטחון ציבורי הזקוקים לכך. הלשון העמומה של החוק כאן, במיוחד "סיוע טכני", מעלה חשש שחברות יהיו מחויבות על-פי חוק בחשיפות מידע על לקוחותיהן, ללא יכולת משפטית לסרב. בסעיף 49 נכתב כי על מפעילי רשת לשתף פעולה גם עם מחלקות הממשלה בכל האמור לבדיקות ופיקוח שגרתיות. סעיף 50 מוסיף כי לרשויות ממשלתיות הזכות לבקש מחברות למחוק מידע, אם לדעתן הוא מסכן או נוגד את החוק.

כל המפר את החוק צפוי לקנס כספי, עד גובה של מיליון יואן (144 אלף דולר). אולם, סעיף 75 מפרט מעט על אופי הענישה בכל האמור לחברות זרות. על-פי סעיף זה, כאשר מוסדות, ארגונים או פרטים זרים עוסקים בפעילות סייבר לא חוקית, המסכנת את תשתיות המידע החיוניות של סין ואת ביטחונה הלאומי, יהיו המשרדים הממשלתיים הרלוונטיים רשאים להקפיא את נכסיהם ולנקוט בכל אמצעי ענישה נדרשים. גם כאן, הניסוח המרחיב של החוק, במיוחד "כל אמצעי ענישה נדרשים", מפקיד את עתידן של חברות, המבקשות לפעול בשוק הסיני לשיקול דעתן של רשויות השלטון השונות בסין.

השלכות לישראל

חקיקה זו מצביעה על מודעות הממשל הסיני לפוטנציאל הכלכלי והשלטוני המתרחב של יישומי רשת, אשר באמצעותם אפשרי לצבור עוצמה כלכלית בסין גופא ובחו"ל ולהשפיע פוליטית, ועל כוונתה לחזק את אמצעי הפיקוח והבקרה על אזרחיה ועל זרים הפועלים בשטחי סין בתחום זה כדי לבצר את היציבות השלטונית. מכיוון שעבור הממשל, הסתמכות על טכנולוגיות זרות מהווה איום פוטנציאלי על הביטחון הלאומי, היא מבקשת לשדרג את יכולותיה בתחום שירותי האינטרנט והסייבר אל מול מתחרותיה מהמערב. החקיקה החדשה מתווה קו פעולה לחברות הסיניות, אשר יצטרכו לשפר את הטכנולוגיה שבידיהן לצרכי הממשל ודרישותיו.

סין רואה בישראל מקור לחדשנות וידע טכנולוגי, גורם שסייע להעמקת יחסי הסחר בין שתי המדינות בשנים האחרונות. עם זאת, חוק ביטחון הסייבר החדש עלול להקשות על המשך ההתפתחות החיובי של יחסים אלו.

כל חברת טכנולוגיה ישראלית העוסקת בתחום הרשתות החברתיות או המידע תפוקח על ידי הרשויות הסיניות ותאלץ לפעול תחת מגבלות רבות יותר מאשר טרם כניסת החוק לתוקף. חברות ישראליות המעוניינות לפעול בסין צריכות לקחת בחשבון כי הממשל הסיני יוכל לדרוש את העברת קוד המקור שלהן לבחינתו (ראה המקרה של אפל). דרישה זו מאפשרת "דלת האחורית" לממשל לשים את ידו על קודי מקור של חברות מערביות ולהשתמש בו לצרכיו, כמו גם להעתקת הקוד על-ידי חברות סיניות המקושרות לממשל. כמו כן, הממשל יוכל לדרוש את המידע שאספו על לקוחותיהם הסינים – דרישה היכולה ליצור בעיה אתית-מוסרית אם מידע זה ישמש נגד אזרחים. לכן, נכון יהיה אם משרדי הממשלה הרלוונטיים בישראל יעבדו יחדיו על מנת להעלות את המודעות לחוק ביטחון הסייבר הסיני החדש בקרב חברות ישראליות הפועלות כיום בסין או המעוניינות להתחיל פעילות בה. ובנוסף, על אף שחברות ישראליות הפועלות במדינות זרות מחויבות לפעול תחת הרגולציה המקומית, יש מקום לבחון את האפשרות לספק יעוץ משפטי מיוחד לחברות הפועלות בסין לנוכח האתגרים הייחודיים שעמם יהיה עליהן להתמודד.