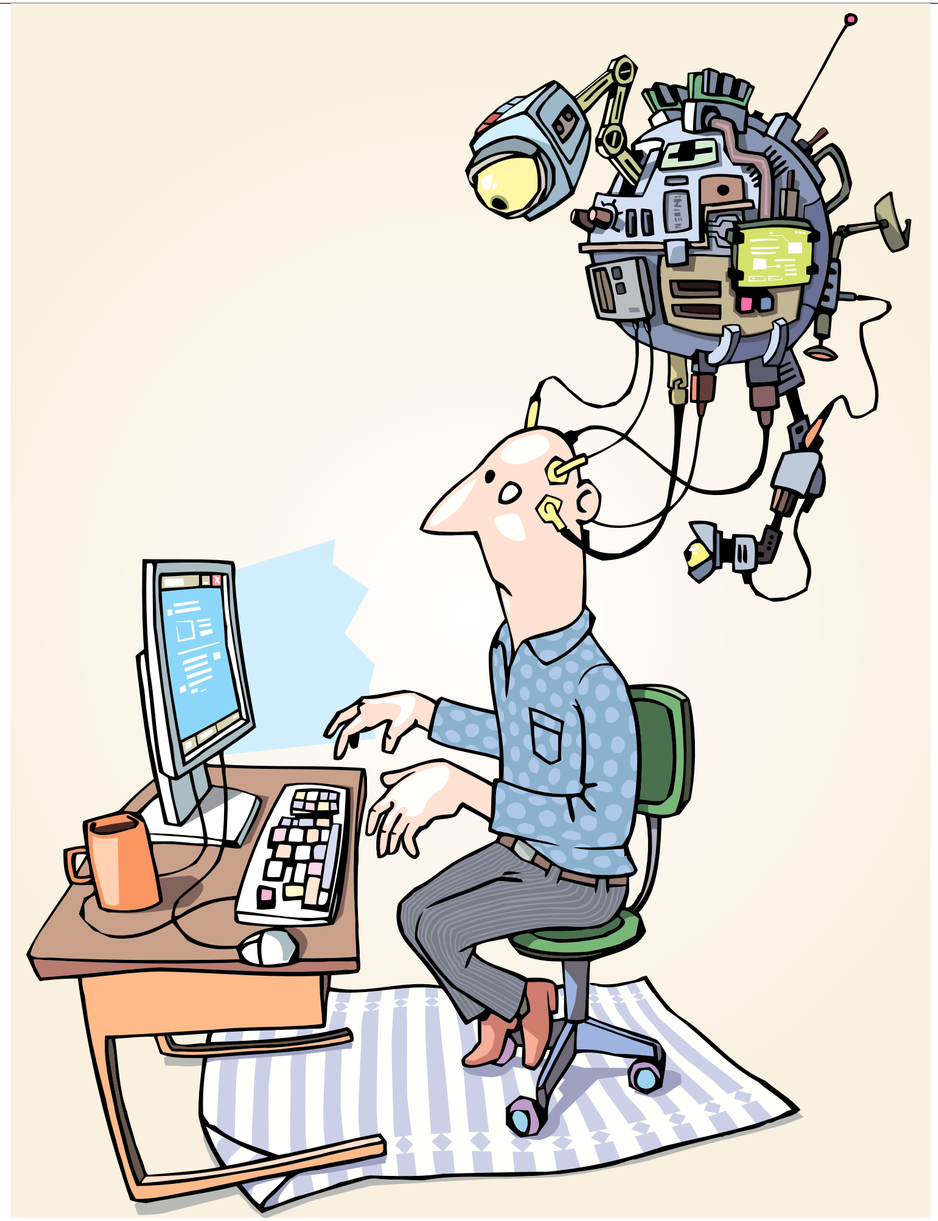
האתגר - לשמור על פרטיות המידע

גל חסר תקדים של רגולציית אבטחת סייבר סוחף את ארה"ב, במטרה להילחם באירועי סייבר. מה כדאי ללמוד מהאמריקאים ואיך ניתן לאזן בין ההגנה על מרחב הסייבר מפני סיכונים קיברנטיים לבין שמירת זכויות יסוד ופרטיות המידע?

עו"ד ירון סובול, עו"ד שני וינדר



סיכוני אבטחה

בשנתיים האחרונות חברות ענק חוו אסונות סייבר. ניתן למנות, בין היתר, את המתקפה הידועה על רשת טרגט (Target) במס־גרתה האקרים פרצו למערכות של החברה וגנבו עשרות מיליוני רשומות דיגיטליות של לקוחות החברה, לרבות פרטי כרטיסי אשראי ומידע אישי נוסף. כמו כן, המתקפה האחרונה על סוני "זכתה" לכותרות רבות. מתקפה זו כללה הפצתו בפומבי של מידע פנים־אסטרטגי, לרבות אימיילים וסרטים מסחריים. המתקפה על סוני בלטה במיוחד לאור התערבות הממשל האמריקאי בדרגים הגבוהים ביותר לאחר המתקפה - לרבות הנשיא אובמה עצמו - אשר איים על מדינת צפון־קוריאה, שנחשדה כמי שעמדה מאחורי מתקפת הסייבר.

בתקיפה על Anthem, חברת ביטוח הבריאות השנייה בגודלה בארצות־הברית, נפרצו נתונים של כ־80 מיליון מבוטחים. מתקפה זו לא כללה כנראה זליגת רשומות רפואיות או פרטים פיננסיים, אלא מספרי ביטוח לאומי, כתובות, נתוני השתכרות ומידע אישי אחר. ועדיין, התקפת הסייבר על חברה המחזיקה רשומות רפואיות הכוללות מידע אישי רגיש ביותר ממחישה את הסכנה הטמונה בכך. למשל, למידע כזה יש ערך רב בשוק האפור ובנוסף מידע כזה אינו "ניתן לביטול" מרגע שנחשף, בניגוד, לדוגמא, למספרי כרטיסי אשראי שנפרצו והניתנים לביטול. מתקפות אלו ואחרות ממחישות באופן מי־טבי את הרגישות של כל חברה באשר היא למתקפות סייבר. במאמר זה נתמקד בנקודות המשמשך שבין אבטחת הסייבר לבין היכטי פרטיות של המידע הרב הנצבר עלינו במאגרי המידע של גופים שונים - Big Data ("ביג דאטה").

הנתונים המתקבלים מאותם "דברים" מאפשרות ניצול לרעה של המידע האישי ואף יוצרות סיכונים לביטחון אישי. בין היתר, האקרים עשויים לנצל פרצות אבטחה לצורך גישה בלתי־מורשית ולגרום בכך לסיכון פיזי של חיי אדם. למשל, באמצעות השתלטות על "דברים" כמו מכוניות במישור האזרחי או על מפעלים ומתקני תשתיות לאומיות במישור הלאומי־מדינתי. שנית, קיימת דאגה ממשית מפני יצירת התנהגויות מפלות, ניצול המידע לרעה ושי־מוש בו למטרות אחרות מהמטרה המקורית ושאר סיכוני פרטיות. זאת, באמצעות איסוף ישיר של מידע אישי - כמו מיקום גיאוגרפי, מידע פיננסי ואף מידע רפואי - באמצעות ה"דברים".

ה"ביג דאטה" מאפשר גם להסיק, באופן עקיף, מידע אישי רגיש על בני אדם, כמו הרגלים ותבניות התנהגות, תכונות אישיות והעדפות ויצירת "פרופי־לים". גופים שונים - לרבות חברות המחזיקות במידע "ביג דאטה" באופן חוקי לכאורה, או צדדים שלישיים שקיבלו את המידע - עשויים לקבל החלטות בנוגע לאותם אנשים עליהם נאסף המידע בהסתמך על אותם נתונים. למשל, בנקים יקבלו החלטות בתחומי מידע אישי - כמו מיקום גיאוגרפי, מידע פיננסי ואף האשראי, מעסיקים יקבלו החלטות בעניין העסו־קה של עובדים, או עובדים פוטנציאליים, וחברות ביטוח תקבלנה החלטות בנושאי ביטוח. מדובר בא־סימטריה מובנית בין חברות וגופים אחרים התנהגות, תכונות אישיות והעדפות ויצירת "פרופי־לים". גופים שונים - לרבות חברות המחזיקות במידע "ביג דאטה" באופן חוקי לכאורה, או צדדים שלישיים שקיבלו את המידע - עשויים לקבל החלטות בנוגע לאותם אנשים עליהם נאסף המידע בהסתמך על סיכוני פרטיות. זאת, באמצעות איסוף ישיר של מידע אישי - כמו מיקום גיאוגרפי, מידע פיננסי ואף מידע רפואי - באמצעות ה"דברים".

רגולציית אבטחת סייבר

אך גם החוקים והתקנות הקיימים בישראל הנו־געים לאבטחת סייבר ולפרטיות עדיין יחסית "בחי־תוליהם" ולגבי סוגיות רבות יש "ואקום" חקיקתי. לכן, ראוי ללמוד על ההתפתחויות בתחום מעבר לים. גל חסר תקדים של רגולציית אבטחת סייבר "סוחף" את ארצות הברית בשנים האחרונות. ועדיין, החקיקה האמריקאית בתחום אבטחת הסייבר אינה קוהרנטית ומעודכנת דיה כדי להילחם באופן מיטבי באירועי סייבר בסקטור הפרטי ובגזרה הלאומית. משכך, בינואר 2015 נשיא ארה"ב, ברק אובמה, יזם מספר הצעות חקיקה חשובות, שמטרתן להסדיר באופן קוהרנטי את תחומי אבטחת הסייבר והפר־טיות. נסקור להלן את המרכזיות והמעניינות שבהן:

ראשית, חקיקת שיתוף מידע.

מטרת הצעת החקיקה לתמרץ את הסקטור הפר־טי לשתף מידע מסוג אינדיקטורים על הפרות סייבר עם הסקטור הציבורי - הממשל האמריקאי. לשם כך, ההצעה מספקת חסינות מפני חבות משפטית - אזרחית ופלילית - לאותם גופים ששיתפו וולונ־טרית מידע כאמור. אין זו הפעם הראשונה שהצעת חקיקה כזו הוגשה למחוקק האמריקאי. הצעות חקיקה קודמות דומות נכשלו בשל התנגדות רבה, שנבעה מהחשש להפרות של פרטיות ושל זכויות אדם אחרות כתוצאה מגילוי מידע לממשל. ההצעה מחייבת גופים המגלים, או מקבלים מידע כאמור, לנקוט אמצעים סבירים כדי למזער את האפשרות שיהיה ניתן לזהות באמצעות מידע זה פרטים שאינם רלוונטיים לצורך התמודדות עם איום הסייבר.

יוער בעניין זה, כי גם עצם קיומו וגילויו של מטא־דאטה, כלומר המידע על המידע עצמו, מעלה חששות לגבי הגנת הפרטיות. חקיקת שיתוף מידע חקיקה אמריקאית העוסקת בחופש המידע. חששות מפני הפרות אפשריות של דיני ההגבלים העסקיים הן מכשול נוסף לשיתוף פעולה פורה בין חברות מתחרות המשתפות מידע זו עם זו.

שנית, הצעת חוק פדרלית של "ידוע על הפ־רות מידע (Personal Data Notification & Protection Act).

כיום יש במרבית ממדינות ארה"ב חקיקה מדינ־תית המחייבת דיווח לנפגעים על הפרות של מידע פרטי רגיש (PII). כך, פרטים רבים קיבלו הודעות על כך שהמידע האישי שלהם נפרץ. למרות קיומה של הפיפה מסויימת בדרישות בין החקיקה המדי־נתית, הדרישות אינן זהות בין המדינות. כיום אין חקיקה פדרלית אחידה בתחום היידוע על זליגות מידע, אלא חקיקה שחלה על סקטורים מסוימים בלבד, בעיקר הבריאות, הפיננסים והאזרחי־פדרלי. החקיקה המוצעת קובעת סטנדרט פדרלי אחיד שיחול על כל מדינות ארה"ב ובכך יוצרת הרמוניזציה בתחום. הצעת החוק קובעת כי גוף המשתמש, ניגש, מעביר, מאחסן או אוסף מידע אישי רגיש על יותר מ־10,000 פרטים - חייב להודיע לפרטים שנפגעו מהפרת המידע על כל גישה בלתי מורשית למידע שלהם. על ההודעה לנפגעים להינתן תוך 30 ימים מיום הגילוי על הפרת הסייבר. עם זאת, הצעת החוק קובעת חריג, לפיו אין דרישה להודיע כאשר אותו גוף ביצע הערכת סיכונים והגיע למסקנה לפיה לא קיים סיכון סביר שהגישה הבלתי מורשית גרמה או עלולה לגרום לנזק לאותם פרטים. כך, למשל, אם המידע הוצפן באופן שאינו ניתן לפיענוח. אותו גוף יידרש לדווח לרשות הממונה (ה־FTC) על תוצאות הערכת הסיכונים ועל החלטתם שלא ליידע פרטים על ההפרה.

שלישית, הצעת חוק בעניין הגנה על פרטיות הס־טודנטים (Student Digital Privacy Act). הצעה זו נועדה להבטיח שמידע שנאסף במסגרות חינוכיות ישמש למטרות חינוכיות בלבד וכן למנוע מחברות למכור מידע על סטודנטים לצדדים שלישיים, או להשתמש במידע זה למטרות מפלות. עם זאת, החוק מאפשר לשתף מידע אודות סטודנטים למטרות מחקר ולמטרה של שיפור החינוך. מדובר בהצעת חקיקה נוספת שהיא סקטוריאלית בלבד, כלומר היא מגנה על הפרטיות של סקטור ספציפי - הסטודנטים.

רביעית, הצעת חוק בעניין הגנה על פרטיותם של צרכנים (Consumer Privacy Bill of Rights).

מדובר בניסיון להעביר חקיקה קוהרנטית בתחום הפרטיות (להבדיל מחקיקה סקטוריאלית), אך סיכויי ההצעה לעבור הם נמוכים יחסית. מטרת ההצעה היא ליצור סטנדרט אחיד לייצור ולעיבוד מידע עבור בנקים וחברות אחרות. הזכויות העיקריות עליהן ההצעה באה להגן הן הזכות להחליט אילו סוגי מידע אישי נאספים על צרכנים, הזכות לדעת ולשלוט כיצד משתמשים במידע האישי וכן הזכות שהמידע יאוחסן באופן בטוח ומאובטח.

כאמור לעיל, מעקב אחר עלילותיו של "חוק האח הגדול" (ראה מסגרת) בשנים הספורות שחלפו מאז נחקק, מלמד כי מרגע שנחינה לגופי החקירה האפ־שרות לאסוף מידע חל סחף מטריד בכמות המידע האישי שנאסף על ידם, פעמים מעצם היכולת ההנר־שאה לאסוף ובמנותק מהרעיון המרכזי שמאחורי חקיקתו - איזון ראוי בין צרכי אכיפה ושמירה על אינטרסים ציבוריים חשובים מחד גיסא, וצמצום פגיעה אפשרית בפרטיות, מאידך גיסא.

ארגונים שעיסוקם בזכויות האזרח טוענים שגופי חקירה מתמהמהים במסירת דיווחים על היקפי החדירה שלהם לפרטיות, שצווים רבים למסירת מידע אישי הוצאו לצורך חקירות עבירות קלות של "פגיעה בסדר הציבורי או החברתי" ושכמחצית מהבקשות לקבלת מידע לא עברו מבחן שיפוטי. הסכנה הטמונה בחוקים דוגמת חוק "האח הגדול" היא שגופים ממשלתיים נוספים, שעיסוקם המרכזי אינו חקירות ואכיפה, יבקשו לעשות שימוש בכלים שמקנה חוק כאמור ולו בגלל הזמינות והאפשרות.

למנוע פגיעה בזכויות יסוד

החשש הוא שככל שמקבל הגישה למידע אינו מתמחה בחקירות ואכיפה ויכולתו לבור את המוץ מהתבן פחותה כך איסוף המידע יהיה גורף יותר. לדוגמא, לאחרונה משרד המשפטים ביקש להרחיב את רשימת הגופים המורשים לקבל מידע במסגרת חוק נתוני תקשורת ולכלול בה רשויות שעיסוקן המ־רכזי אינו חקירות ואכיפה - המשרד להגנת הסביבה, רשות העתיקות ורשות הטבע והגנים.

לסיכום, החששות מפני הפרות אפשריות של זכויות אדם עומדות הן בפני המחוקק והרגולטור האמריקאי והן בפני חברי הישראלי. הלקח שנלמד מ"חוק האח הגדול" מלמד שהחיעדר חסמים ומג־בלות ראויים שמאזנים בין רצון המדינה לדעת לבין זכויות הפרט, רשויות המדינה נוטות לפלוש למת־חם בפרטיות ולאגור מידע אף כשאין צורך מהותי למהלך זה. על פניו, ללא מערכת בלמים ואיזונים מתאימה יהיה בידי הרשות הלאומית לסייבר כוח רב ויכולות להתממשק לביג דאטה ולמידע הרב האגור שם (ראה מסגרת).

נדרשת גם הסדרה חקיקתית מול דברי חקיקה קיימים, כמו חוק חופש המידע ודיני ההגבלים הע־סקיים, כך שתהיה "הרמוניה" מקסימלית של חוקים אלה ושל דיני ההגנה על מרחב הסייבר מפני הסי־כונים הקיברנטיים. לפיכך, וכדי להימנע מהסכנות הטבועות במתן כוח נרחב מדי לרשויות ההגנה על הסייבר, יש ליצור מערך כללי משחק מקיף, שיאזן כראוי בין הצורך בהגנת המרחב הקיברנטי לבין זכויות יסוד מוגנות ויהיה מורכב מחקיקה, תקינה ושומרי סף מתקדמים בתחום, אשר מצד אחד בעת הצורך יספקו סמכויות ו"שיניים" לרשויות ומצד שני יימנעו, בגלל הזמינות והיכולת, פגיעה בלתי מידתית בזכויות יסוד מוגנות.

עו"ד ירון סובול הינו שותף במשרד המבורגר עברון ושות', מנהל מחלקת הטכנולוגיה והסייבר; עו"ד שני וינדר הינה עורכת דין במחלקת הטכנולוגיה והסייבר במשרד המבורגר עברון ושות'

אין במאמר זה כדי להוות חוות דעת משפטית מכל סוג שהוא אלא הוא בבחינת הבעת דעה בלבד של כותבי המאמר. מומלץ לפנות ליישץ משפטי פרטני לכל מקרה ומקרה

להבטיח איזונים ובלמים

הקמת רשות לאומית להגנת הסייבר היא צעד מבורך, אך יש להבטיח שבידי הרשות לא יהיה כוח רב מידי ויכולת נרחבת לקבל גישה למאגרי הביג דאטה

עם ההכרה, כי סיכוני אבטחת הסייבר הם מהסיכונים המרכזיים המאיימים על גופים פרטיים ועל מדינות כאחד, אישרה ממשלת ישראל בחודש פברואר 2015 את הקמתה של רשות לאומית להגנת הסייבר - רשות ייעודית להגנת מרחב הסייבר הלאומי. רשות זו מיועדת להוות גוף אופרטיבי, שיפעל לצד מטה הסייבר הלאומי, שעוסק בהתוויית מדיניות ויישא באחריות הלאומית הכוללת להגנה על מערך הסייבר. במסגרת זו הממדט של רשות הסייבר הלאומית יהיה לנהל את פעולות ההגנה כדי לייצר פתרון כלל מערכתי נגד התקפות סייבר, לרבות טיפול באיומים ובאירועים בזמן אמת. כמו כן, באחריות הרשות החדשה יהיה להקים ולהפעיל את Cyber Event Readiness Team) CERT) ישראלי - מרכז לסיוע בהתמודדות עם איומי סייבר באמצעות מנגנוני בדיקה, חקירה, עדכון והתמודדות. הרשות צפויה ליצור מנגנונים של שיתוף מידע בזמן אמת עם הגופים הנפגעים ולסייע הן לרשויות ציבוריות והן לארגונים פרטיים בהתמודדות עם התקפות סייבר.

אכן, מדובר בצעד חיוני וחשוב. עם זאת, היקף סמכויותיה של ותפקידיה של הרשות עדיין אינו מתוחם ולא הוגדרו סייגים ומגבלות לשימוש בכוח הרב שצפוי להינתן לרשות. למשל, יש להבהיר מהו ה"מידע" הרלוונטי לשיתוף ומהם השימושים המותרים לרשויות במידע זה. כמו כן, יהיה צורך למסד מנגנוני בקרה ופיקוח על פעולתה, מנגנוני דיווח והסדרת הפעולות מול הגופים שעל-פי החלטת הממשלה אמורים להיות הנהנים מפעילותה - המגזר הציבורי והמגזר הפרטי. אחד החששות המהותיים הוא שמא מתן סמכויות נרחבות מדי לרשות זו תגרום לפגיעה בזכויות יסוד מוגנות, ובעיקר בזכות לפרטיות. כך למשל, ללא מערכת בלמים ואיזונים מתאימה, יהיה בידי הרשות הלאומית לסייבר כוח רב ויכולת נרחבת לקבל גישה למאגרי הביג דאטה.