

בשנה האחרונה, עלתה לכותרות חברת NSO אשר מייצרת ומוכרת כלי סייבר התקפיים, ובפרט מוצר הדגל שלה - פגסוס. פגסוס היא רוגלת סייבר המאפשרת גישה למחשבים ולמכשירים אישיים במטרה לאסוף מידע, בין היתר לצרכי מניעת פשיעה, ריגול או מעקב. בנוסף, לתעשיית הסייבר ההתקפי חשיבות עצומה לכלכלת ישראל ולתדמיתה ככוח משמעותי בזירת הטכנולוגיה. מהם היתרונות והחסרונות של כלי סייבר התקפיים? האם זה רע הכרחי במאבק בטרור ובפשיעה חמורה, או שמא הם מקעקעים את שלטון החוק? כיצד ניתן לפקח ולהתמודד בצורה טובה יותר עם האתגרים בתחום זה? ד"ר טל מימרן ועו"ד עדן פרבר עונים על השאלות הקריטיות.

סייבר התקפי והזכות לפרטיות מה זה סייבר התקפי?

כלי סייבר התקפיים מאפשרים למשתמש בהם להיכנס מרחוק ובאופן סמוי למכשיר, לשאוב את תכולתו, לרבות מידע האגור בו ובאפליקציות הנמצאות עליו. ישנה חשיבות רבה לכלי סייבר התקפיים, דוגמת פגסוס, במאבק בטרור, בפשיעה חמורה ובאתגרים של רשויות החוק. ועדיין, כלי סייבר התקפיים מקצרים הליכי חקירה באופן משמעותי, ומכאן הפיתוי לעשות שימוש לרעה, או פשוט שימוש החורג במעט מהנחוץ, הוא רב מאוד.

ישנו קושי לפקח על ייצור, שיווק או שימוש בכלי סייבר התקפיים בשל האופי הייחודי של התעשייה - קוד, או אלגוריתם, יכולים להיות משוכפלים ולפעול ברחבי העולם בו זמנית, להבדיל מכלי נשק קלאסיים שמוגבלים למיקום פיזי אחד. כמו כן, עובד ממורמר יכול לנסות ולמכור מוצר בשוק השחור, וניתן להעתיק קוד, או לפתח תוכנות נגזרות שיכולות להביא לפגיעה

זדונית. בישראל, הרגולטור העיקרי אשר מפקח על שוק הסייבר ההתקפי (ובפרט רגולות) הוא משרד הביטחון, אשר אחראי על מתן רישיון שיווק וייצוא של מוצרים אלה, אך יכולתו לפקח מוגבלת מכובעו הכפול (מפקח ולקוח פוטנציאלי) ובשל תופעות דוגמת הדלת המסתובבת (מעבר של בכירים ברגולטור לתעשייה, ולהיפך).

הזכות לפרטיות בעידן הדיגיטלי

הזכות לפרטיות היא זכות אדם יסודית, ובישראל היא מעוגנת ברמה החוקתית בחוק יסוד: כבוד האדם וחירותו. הזכות לפרטיות היא בסיס חשוב לשימור על כבוד האדם, האוטונומיה שלו, רווחתו האישית (גופנית ומנטלית) ובשל היותה נחוצה לשם מימוש שאר זכויות האדם שלו. כמו כן, כמו כן, זכות אדם, גם הזכות לפרטיות היא יחסית ומוגבלת - מכוח אינטרסים חשובים דוגמת ביטחון הציבור, בריאות הציבור או הגנה על חירות אחרים. מכוח זכות זו, יש להגן מפני התערבות שרירותית או בלתי חוקית בפרטיות,

"הזכות לפרטיות היא בסיס חשוב לשימור על כבוד האדם, האוטונומיה שלו, רווחתו האישית (גופנית ומנטלית) ובשל היותה נחוצה לשם מימוש שאר זכויות האדם שלו"

לרבות חדירה לרשות יחיד ללא ידיעתו, הגבלות על חיפושים על אדם ובכליו וכן שמירה על סוד שיחו של אדם, כולל בכתביו או ברשומותיו. בעידן הדיגיטלי, הזכות לפרטיות נמצאת בסיכון מתמיד, וחשיבותה רק מתגברת.

כלי סייבר התקפי וזכויות אדם - הילכו יחדיו?

השימוש בכלי סייבר התקפיים מעורר חששות רבים, ובפרט: (א) היקף הכוח המتركז בידי ממשלות; (ב) אופן השימוש בכלי וההצדקות לכך; ו-(ג) איזון השימוש באמצעי כה קיצוני אל מול הצורך להגן על זכויות אדם, ובפרט הזכות לפרטיות, חופש הביטוי והזכות לקניין רוחני.

"יש קושי להגביל את השימוש בתוכנות ריגול באמצעות החקיקה הקיימת, והמיושנת, אשר לא עומדת בקצב ההתפתחויות הטכנולוגיות"

לעניין היקף הכוח, יש קושי להגביל את השימוש בתוכנות ריגול באמצעות החקיקה הקיימת, והמיושנת, אשר לא עומדת בקצב ההתפתחויות הטכנולוגיות.



את הייצוא, מכירה והעברה של טכנולוגיות אלו – ובפרט פגסוס – עד ליצירת הסדר חוקי מתאים. גם ברמה המדינית, נוצרו תגובות נגד – למשל הכללה של NSO ב"רשימה השחורה" של מחלקת המסחר האמריקנית. לבסוף, חברות טכנולוגיה

הרוגלה. ועדיין, בשנים האחרונות ישנם דיווחים הולכים וגוברים לגבי שימוש לרעה בתוכנת פגסוס, ברחבי העולם. בין היתר, נטען כי הרוגלה שימשה לצרכי מעקב אחר מגיני זכויות אדם, עיתונאים, עורכי דין, פוליטיקאים ועוד (בין היתר, פורסמו

ביחס לאופן השימוש, ישנה חשיבות להגדרה של איזונים ובלמים בפני שימוש ללא רסן – למשל באמצעות צו שיפוט. אך, כפי שנראה ביחס לפרשת פגסוס – סייפן בישראל, נראה כי גם אמצעי זה אינו מספק לעיתים. כמובן, חשש מרכזי

השימוש בכלי סייבר התקפיים מעורר חששות רבים

איזון השימוש
באמצעי הקיצוני
לבין ההגנה על
זכויות אדם

אופן
השימוש
בכלי
וההצדקות
לכך

היקף הכח
אצל
הממשלות

מובילות בעולם תובעות את NSO בשל שימוש לרעה ופריצה למערכות שלהן, כמו וואטסאפ ואפל.

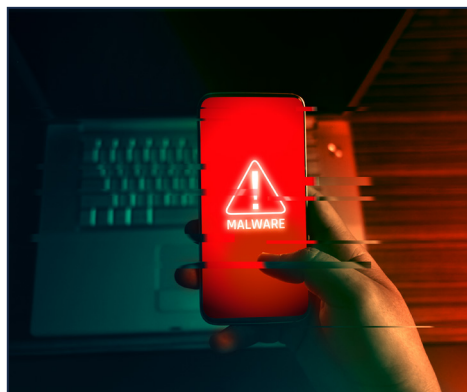
זליגה למרחב הישראלי – פרשת סייפן ומשטרת ישראל

לפני כשנה, תחקיר של תומר גנון מכלכליסט חשף לכאורה כי משטרת ישראל עשתה שימוש במערכת פגסוס, לעיתים אף ללא אישור צו שיפוט. בעקבות התחקיר, והביקורת הציבורית שקמה בעקבותיו, הוקמה ועדה ממשלטתית בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי), עו"ד עמית מררי.

לאחר שהצוות השלים את עבודתו, פורסם רשמית דו"ח מררי וחשף גילויים משמעותיים לגבי הפרשה. ראשית, הסתבר כי משטרת ישראל לא השתמשה בפגסוס, אלא ברוגלה מותאמת ייחודית עבורה (גם של NSO) בשם סייפן. שנית, מסקנות הדו"ח מתחו ביקורת על המשטרה וציינו כי ההכנסה של מערכת האזנות רחבת היקף נעשתה בלי שהובנה לאשורה על ידי מקבלי ההחלטות. על רקע זה, פסק הדו"ח כי הטענות לגבי השימוש במערכת פגסוס ללא צו שיפוט פגעו בליבת שלטון החוק במדינה דמוקרטית, וכי שימוש לא ראוי בתוכנה מהווה פגיעה חמורה במרחב הפרטיות הנתון לכל אדם.

גילויים לגבי מעקב אחר פעילי זכויות אדם פלסטיניים, נציגי חברה אזרחית בקזחסטן, גורמי אופוזיציה בפולין, סגל דיפלומטי באוגנדה, פעילי זכויות אדם בבחריין וירדן, עיתונאים באל-סלוודור ואף נציגי או"ם). אחת הדוגמאות הבולטות ביותר, הייתה ההאשמה לפיה פגסוס שימשה בכדי לעקוב אחר פעילי זכויות אדם בסעודיה, וסייעה במימוש המזימה להוציא להורג ללא משפט את

הוא שהכלים הללו יקדמו מטרות שאינן הכרחיות – דוגמת מיגור טרור או פשיעה חמורה – אלא בשם אינטרסים מסחריים או פוליטיים. לבסוף, באשר לזכויות האדם, היכולת של כלי סייבר התקפי לאסוף מידע מתחת לרדאר מגבירה את האתגר, ובנוסף ישנו קושי להגביל את הפגיעה רק למישור אחד (למשל, פרטיות) מבלי שהדבר ישליך על מישורים נוספים (לדוגמה, הגנה על סודות מסחריים).



העיתונאי ג'מאל חשוקג'י (באירוע מטלטל ואכזרי במיוחד, בשטחה של שגרירות סעודיה בטורקיה).

על רקע זה, קראו מומחים בינלאומיים רבים לזכויות אדם, ובפרט נציבות זכויות האדם של האו"ם, כי תיאסר המכירה של רוגלות עד שתגובש רגולציה מספקת. גם מועצת אירופה, בין היתר, קראה לעצור

מקרה מבחן – NSO העסק מסתבך – פרשת פגסוס

כמצוין לעיל, חברת NSO היא חברה ישראלית אשר מוכרת כלי סייבר התקפיים. לפי דו"ח שקיפות שפרסמה החברה ביוני 2021, התוכנות שחברת NSO מייצרת ומשווקת סייעו למניעת פיגועי ירי והתאבדות, להציל ילדים חטופים, לאתר אנשים שניצלו מאסונות טבע ועוד. באשר להיקף הפעילות של החברה, מדובר בסדר גודל של כ-60 לקוחות בכ-40 מדינות ברחבי העולם, מתוכם 38% גורמי אכיפת חוק, 51% סוכני מודיעין ו-11% גורמים צבאיים.

לטענת החברה, מכוח מחויבותה לעקרונות זכויות אדם, היא בוחנת את המהימנות של הלקוחות הפוטנציאליים שלה ואף מפקחת עליהם לאחר מכירת

אדם. אמנם, בשלב הזה מדובר במסמכים המעידים על הדין הרצוי (lex ferenda) ולא הדין המצוי (lex lata), אך חשוב לציין כי הוא אומץ על ידי חברות טכנולוגיה גדולות: גוגל, אפל, ומייקרוסופט. בהתאם, הוא כבר זכה להשפעה על המציאות. למעשה, גם חברת NSO קיבלה על עצמה לפעול בהתאם לקווים המנחים של מסמך זה.

לטוב ולרע, ולרע יותר

אין ספק, השילוב של טכנולוגיות מתקדמות מסייע לאכיפת החוק, מייעל עשיית צדק, ויכול לתרום גם לביטחון הציבור וגם לשלטון החוק. באותה הנשימה, כגודל הפוטנציאל כך גם גודל הסיכון, ובפרט זה של ניצול לרעה. האם עלינו להעניק חשיבות רבה יותר להצלחות ולהשפעה החיובית של פגסוס, למשל שהרוגלה סייעה להגן על חיי אדם בעת אסונות טבע, או למעצרו של סוחר הסמים

חובת החריצות הנאותה של מדינות

דיני זכויות האדם מחייבים את המדינה לפעול בחריצות נאותה כדי למנוע הפרה של זכויות אדם, גם על ידי שחקנים פרטיים, ואם אלו בוצעו – לחקור, להעמיד לדין ולהעניק סעד ביחס אליהם. בהתאם, מעבר לפיקוח ישיר של המדינה, חשוב לייצר מסגרת משפטית שתוודא כי המגזר הפרטי במדינה לא מפר התחייבויות בינלאומיות ובפרט בתחום זכויות האדם. חובת החריצות הנאותה אינה מוחלטת, אלא היא חלה באופן יחסי ליכולת המדינה לפעול באותו התחום. ככל שמדינה מתקדמת יותר בתחום מסוים, כך הרף שיידרש ממנה הוא גבוה יותר. בעקבות הדומיננטיות הרבה של ישראל בשוק הסייבר, כמו גם רמת הידע והמומחיות בתחום, נראה כי רף האחריות של המדינה הוא גבוה. מוקד החובה היא עצם הניסיון של המדינה להתמודד עם ההפרה, ולא

לעניין הטענות הקונקרטיות שעלו מן התחקיר, נתגלה כי מצד אחד משטרת ישראל לא הדביקה טכנולוגיית ריגול על טלפונים ללא צו שיפוטי (למעט ב-4 מקרים בהם הוועדה קבעה שמדובר בטעות בתום לב). אולם, מצד שני, הצוות מצא כי היכולות הטכנולוגיות של

"הפיתוי הרב לעשות שימוש בטכנולוגיות מעקב הוא משמעותי, במיוחד באקלים רגיש פוליטי וביטחוני. עובדה זו מעידה על חשיבותם של מנגנוני איזון, ברמה החוקית וגם ברמה המעשית"

מערכת סייפן הן בהחלט מעבר למותר לפי חוק, וכי נאסף מידע אישי מעבר לנדרש. לדוגמה, נתגלה כי סייפן מאפשר לקבל מידע "היסטורי" מהמכשיר, עוד מהתקופה שהרוגלה לא הותקנה עליו (לשם ההמחשה, אם ניתן אישור לקלוט מידע מאדם X החל מיום 1.1.23 כי יש חשש שביום זה האדם הצטרף לארגון פשיעה, התוכנה אספה מידע שהיה על המכשיר גם משנים קודמות – בטרם הצטרף האדם לארגון הפשיעה). בנוסף, בעוד החוק מתיר לאסוף מידע שהוא "תקשורת בין מחשבים", סייפן אפשרה לקלוט מידע נוסף כמו פרטי יומן, פתקים במכשיר ורשימת אפליקציות מותקנות. לבסוף, נתגלה כי חלק מן המידע שנאסף על ידי הרוגלה נשמר גם במערכות של חברת NSO (חברה פרטית ללא אחריות ציבורית, להבדיל ממשטרת ישראל). גילויים אלו מעוררים דאגה, במובן של האצלת סמכות שלטונית, ופגיעה בזכויות יסוד דוגמת פרטיות.

כפי שניתן לראות, הפיתוי הרב לעשות שימוש בטכנולוגיות מעקב הוא משמעותי, במיוחד באקלים רגיש פוליטי וביטחוני. עובדה זו מעידה על חשיבותם של מנגנוני איזון, ברמה החוקית וגם ברמה המעשית. בהתאם, נציע בהמשך אופן חיזוק מנגנוני פיקוח אפשריים.

דווקא התוצאה של המהלך. ככל שבוצעה הפרה, כלומר המדינה לא הצליחה למנוע אותה מראש, למדינה עדיין עומדת החובה לחקור ולהעמיד לדין את האחראים, ולנפק סעד לנפגעים.

באשר לאחריות תאגידים על זכויות אדם, ישנה מגמה גוברת הדורשת אחריות של תאגידים לגבי זכויות אדם המושפעות בשל פעולתם, מכוח יוזמות דוגמת עקרונות האו"ם בנוגע לתאגידים וזכויות



"השילוב של טכנולוגיות מתקדמות מסייע לאכיפת החוק, מייעל עשיית צדק, ויכול לתרום גם לביטחון הציבור וגם לשלטון החוק. באותה הנשימה, כגודל הפוטנציאל כך גם גודל הסיכון, ובפרט זה של ניצול לרעה"

עם ביקורות בינלאומיות. דרך אפשרית למימוש נתיב זה היא הקמת ועדת משנה, אם תחת ועדת חוקה או ועדת המדע והטכנולוגיה. אמנם, חברי הכנסת בישראל נמצאים תחת עומס עבודה משמעותי, אך מדובר כאן בסוגיה חוקית ומוסרית מן המעלה הראשונה, כזו שמשפיעה על יחסי החוץ של מדינת ישראל והכלכלה שלה, ומכאן כזו הראויה לזמנם.

לסיכום, פרשת סייפן היוותה אירוע מוכן בישראל, בדומה לפרשת סנודן בארצות הברית, והיא הזדמנות לקדם הליכי פיקוח יעילים יותר, אשר יבטאו מחויבות של ישראל לשלטון החוק ויגבירו את האמון בתעשיית הסייבר הישראלית. למעשה, גם מעבר למישור המקומי, טוב יהיה אם מדינת ישראל תיקח חלק בשיח הבינלאומי בנושא, ותנסה להגדיר את סדר היום במקום לרדוף אחריו. השתתפות פעילה תאפשר השפעה על נורמות אשר ייווצרו

טכנולוגיים כולל סייבר התקפי. לפי מודל זה, יתבצע פיקוח בשני שלבים: (1) פיקוח בשלב הפיתוח, השיווק והמכירה; (2) פיקוח לאחר המכירה (מעת לעת).

"מדינות מעטות - בוודאי בהשוואה לכמות המדינות המשתמשות בסייבר התקפי - אכן מפעילות גופי פיקוח משמעותיים המתמחים ברוגלות סייבר"

ראשית, חשוב לפקח על הליך הפיתוח של רוגלות, בשלבים מוקדמים יותר משלב השיווק והמכירה, בהם עוד ניתן לבצע שינויים מהותיים בעלות כלכלית נמוכה יותר (אגב צמצום פגיעה כלכלית בחברה - *sunk costs*). מנגנון שכזה נדרש משפטית מכוח חובת החריצות הנאותה,

הגדול בעולם? או, שמא, הגילויים לגבי שימוש לרעה ברוגלה - בישראל ובעולם - מראים כי הנזק עולה על התועלת? קשה להכריע בשאלות מסוג אלו, במיוחד בשל ההשפעה ההדדית החזקה, ואף לפרקים הערבוב, בין אינטרסים מקומיים לבינלאומיים.

"מרחב הסייבר היה אמור להוביל לעצמאות רבה יותר של אנשים פרטיים, אבל בפועל - כפי שניתן לראות - הוא רק החריף את פערי הכוחות בין השלטון לאזרח הקטן, וחיזק את הראשון על חשבון האחרון"

ברמה המעשית, מתן כוח שלטוני משמעותי כל כך - בלחיצת כפתור - מזמין אצבע קלה על ההדק. מרחב הסייבר היה אמור להוביל לעצמאות רבה יותר של אנשים פרטיים, אבל בפועל - כפי שניתן לראות - הוא רק החריף את פערי הכוחות בין השלטון לאזרח הקטן, וחיזק את הראשון על חשבון האחרון. התפתחות זו מצריכה חשיבה מחודשת על האופן בו יש למנוע ניצול לרעה של מרחב זה, אשר הופך למשמעותי יותר עם כל יום שעובר. בפרט, ישנו צורך אמיתי להתאים את המסגרות הרגולטוריות להתפתחויות הטכנולוגיות, ולאפשרויות שהן מייצרות בעולם האמיתי.



כיום, מדינות מעטות - בוודאי בהשוואה לכמות המדינות המשתמשות בסייבר התקפי - אכן מפעילות גופי פיקוח משמעותיים המתמחים ברוגלות סייבר. דוגמאות בולטות לחיוב ניתן למצוא, למשל, בארצות הברית, גרמניה והולנד. סיבה מרכזית לכך היא האינטרסים הכלכליים הכבדים שמייצרת תעשייה זו, והרצון בביסוס ושימור הגמוניה טכנולוגית במישור הבינלאומי.

בעתיד, תגן על ענף בעל חשיבות עצומה מבחינה כלכלית, ותחזק את מעמדה הבינלאומי של ישראל.

ד"ר טל מימון
ראש תוכנית "אמנה חברתית לעידן הדיגיטלי" במכון תכלית, חוקר ומרצה בתחומי המשפט הבינלאומי והסייבר.



עו"ד עדן פרבר
עורכת דין ועוזרת מחקר בתוכנית "האמנה החברתית לעידן הדיגיטלי" במכון תכלית.



ובכל זאת, מה ניתן לעשות?

תכלית - המכון למדיניות ישראלית מציע מודל דו שלבי לפיקוח על השימוש בכלים