Technologic Papers

סייבר רגולציה

מאת עו"ד יהונתן קלינגר

הקדמה

מטה הסייבר הלאומי מקדם במקביל שני נסיונות אסדרה; הראשון הוא נסיון אסדרה למקצועות הסייבר, והשני הוא הפיקוח על ייצוא מוצרי סייבר. עכשיו, סייבר היא בסך הכל מילה שיווקית להגדרה של סט מקצועות בעולם אבטחת ותקיפת המידע, והרצון לרגולציית סייבר לא צריך לבוא ממקום שונה מהרגולציה הרגילה; ועדיין, הבחירה ברגולציה של מקצועות סייבר ושל ייצוא של מוצרי סייבר נראים בעייתיים בדיוק בגלל שהרגולציה היא על הפצה חופשית של ידע ומידע, ולא על הפעילות הזדונית בעצמה.

מהי הרגולציה?

אז נתחיל בהבנה של מהי הרגולצה, ומדוע המדינה רוצה להסדיר דברים שעד היום לא הוסדרו. מעטים הם המקצועות שדורשים הסדרה, ובדרך כלל מדובר במקצועות שיוצרים סכנה כחלק מהשימוש בהם: עריכת דין מוסדרת באמצעות חוק לשכת עורכי הדין כיוון שעורכי דין יכולים לייצר נזק פוטנציאלי רב לאחרים וכיוון שיש להשתמש בכחם בזהירות; כך גם אדריכלים, אופטומטריסטים, גנטיקאים, גננות, חשמלאים, טכנאי שיניים, מהנדסים, מורים, רופאים, עובדים סיעודיים, פיזיותרפטיסטים, קלינאי תקשורת, רוקחים, רופאי שיניים ותזונאים (הרשימה מכאן, אך אינה ממצה).

בתחום הבניה, לדוגמא, הקבלן הוא בר-רישוי, והעבודה עצמה אמורה להיות כפופה למספר חוקים, אבל בפועל קורה שלמרות מקרי מוות רבים באתרי בניה, ולמרות ליקויים רבים, אף לא מקבלן אחד נלקח הרשיון בגלל תקלות אלו. בפועל, מקצועות שצריכים רישוי נובעים מהסבר פשוט: השימוש בכלים שהמקצוע נותן הם מסוכנים לחברה, ויש להטיל עליה פיקוח שכן לא בהכרח ברור האם השוק יכול לסדר את עצמו.

עם כן, מה יש במקצועות הסייבר שדורש אסדרה שלא קיים במקצועות בעלי חשיבות לא פחותה כגון סנדלרים, טבחים, פועלי בניין או גננים? האם יש צורך ברגולציה כדי להמנע משימוש לרעה בכוחות הקסם של אנשי הסייבר, או שמטרת ההסדרה היא למנוע משרלטנים להכנס למקצוע ולמכור את מרכלתם תוך ניצול פערי ידע?

על הכנסת תחום אחר לגמרי, יועצי השקעות, דן בית המשפט העליון כשזה נכנס לראשונה לפיקוח (בג"ץ 1715/97 לשכת מנהלי השקעות נ' שר האוצר); עד לשנת 1995 יכל כל אדם לנהל תיקי השקעות עבור

אחרים, כלומר לקחת את הכספים שלהם ולנהל את המקומות בהם הכספים יושקעו. בשנת 1995 התקבל חוק הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, תשנ"ה-1995 שבעצם קבע כי מי שינהל תיקי השקעות עבור אחרים יהיה כפוף לרגולציה, בחינות עקרוניות, וכדומה. מספר רב של יועצי השקעות, שלא ממש רצו להיות כפופים לרגולציה, עתרו נגד החוק לבית המשפט העליון.

בית המשפט העליון קבע כי בהתחשב בעדינות המקצוע יש מקום לרגולציה, אבל הוראות המעבר, אלו שקבעו שמי שעסק במקצוע טרם החוק עדיין יצטרך לעבור בחינות, יפסלו. באותה הפסילה, פסק בית המשפט העליון כי "*נקודת החיתוך של הוראות המעבר (סעיף 48) בחוק תיקי השקעות לעניין חובת הבחינות, המבחינה בין מי שעסק בעבר לפחות שבע שנים בניהול תיקי השקעות לבין מי שעסק בעבר תקופה קצרה משבע שנים, אינה מידתית. אין היא מתחשבת דיה בנסיון החיים ובאינטרס ההסתמכות של העוסקים הישנים. אין היא מאזנת כראוי בין הנזק לפרט לבין התועלת לכלל. כמובן, בכל הוראות מעבר יש הכרח לקבוע נקודת חיתוך מבחינת הזמן. בכל קביעת זמן יש מן השרירות. מכאן לא נובע שכל הבחנה הקשורה בזמן היא שרירותית. אף שקו הגבול בין יום ולילה הוא שרירותי משהו, וקיים פרק זמן של דמדומים, כולנו נדע להבחין בין יום ולילה בלא שהבחנה זו תהא שרירותית.*"

אולם, יש כמה הבדלים קטנים בין הגבלת העיסוק המוצעת על ידי רשות הסייבר לבין חוק ניהול תיקי השקעות. ההבדל הראשון הוא שבמקרה השני מדובר בחוק, ואצלנו עדיין מדובר בחוזר (בהסדרת המקצוע) ובצו (בהסדרת הייצוא).

בתחום ההסדרה של ייצור ומכירה של מוצרים אנחנו מוכנים לחיות עם לא מעט הגבלות; אנחנו חיים עם הגבלה על מכירה של אלכוהול לקטינים, אנחנו חיים עם הדרישה של מכון התקנים לבדיקה של מוצרי חשמל (והמחיר של אותה דרישה); אנחנו מוכנים גם לחיות עם הסדרה של ייבוא של גבינות, ואפילו הגבלות של כשרות על מוצרים. לכן, השאלה מדוע מסדירים את נושא ייצוא הסייבר ומכירתו לא צריכה להיות זרה.

ואחרי שהבנו איך ומדוע מסדירים, נעבור לשאלה החשובה והיא האם ראוי להסדיר.

הסדרת המקצועות, בקצרה.

הסדרת מקצועות הסייבר מובאת במסמך הסבר ממשלתי. ההסדרה בעצם מייצרת מספר מקצועות (בדומה להצעה של IFIS מ-2012); המקצועות הם מיישם הגנת סייבר (סיסאדמין משודרג), מוסמך מבדקי חדירה, איש תחקור (פורנזיקה), מוסמך מתודולוגיה (חוקר שעוסק בכתיבת מדיניות) ומוסמך טכנולוגיות הגנת סייבר.

ההצעה מייצרת מערך של הסמכה לכל אחד מהתפקידים, שכולל גם את דרישות הקדם, הידע המקצועי, וקיומו של מרשם של העוסקים בתחום. כאשר, מי שאינו רשום במרשם ולא עבר הסמכה מסוג זה לא יוכל לספק שירותים לממשלה, וגם לא יוכל (ככל הנראה) לתת שירותים בתחום זה למגזר הפרטי.

לפי ההצעה, גורמים שאינם רשומים במרשם יוכלו לתת שירותים אך לא יכולים להשתמש בשם התואר שמוגדר בהצעת ההסדרה. כלומר, לא יהיה איסור על העיסוק אלא על הכינוי. *הדבר דומה למה שמתרחש בעולם אחר בו יש שרלטנים לא מעטים, והוא תחום ה"טיפול" האלטרנטיבי (כלומר זה שאינו מוכח מדעית). שם יש איסור על השימוש במילים "פסיכולוג" או "רופא" ולכן השימוש במונח "מטפל" ב"שיטת" גובר*. כך גם צפוי בעניין הסייבר; שכן לאחר שיוטל איסור על השימוש בשם "מוסמך מבדקי חדירה" יחלו מי שאינם מוסמכים להשתמש בתארים כגון "מיומן מבדקי חדירה", "חודר מיומן", "אחראי בדיקות חדירה" או דברים שמגיעים לידי דמיון רב, אך ללא זהות.

המדינה היא לא רגולטורית טובה.

יש לא מעט בעיות בהצעה להסדרה ופיקוח ממשלתי על השוק, ולא הסדרה ופיקוח של גוף וולונטרי שמורכב מפרקטיקאים; הבעיה הראשונה היא כמובן שהמגזר הממשלתי, מה לעשות, לא מכיר את הנושא טוב מספיק כמו הפרקטיקה. הממשלה מאמצת בדרך כלל טכנולוגיות מיושנות (1, 2); הממשלה מיישמת טכנולוגיות שקשורות לעולם תוכנה מאוד מסוים ומקודם על ידי בעלי אינטרס כלכלי (מיקרוסופט היא דוגמא קלאסית לטכנולוגיה שנכחדת מחוץ למשרדי הממשלה, ופורחת בממשלה, גם כאן). לכן, מבחני הסמכה ממשלתיים שיוכתבו על ידי עובדי מדינה שלא מכירים טכנולוגיות חיצוניות עשויים לצאת מאוד לא רלוונטיים ומאוד לא ענייניים.

גורמים אחרים שמסדירים (נניח, לשכת עורכי הדין או לשכת רואי החשבון) מבססים את בחינות הקבלה שלהם על פרקטיקאים בשוק: עורכי דין ורואי חשבון כותבים את הבחינות. במקרה שלנו, מדינת ישראל, גם אם תעסיק את מיטב המומחים, עדיין אינה מסוגלת לקבל על עצמה לנסח מבחנים בתחום הסייבר. ומדוע? אפילו כשהמדינה מארגנת "אליפות סייבר" במשרד החינוך, יש הונאות באליפות.

הרגולציה היא גרנולרית מדי.

מעבר לבעיה שלפיה הממשלה היא שמסדירה, וקובעת מהם הנושאים שצריכים לבוא לידי ההסמכה (גם אם הדבר מבוצע ביחד עם השוק הפרטי), הרי שיש בעיה נוספת; הבעיה הנוספת היא שאותה ממשלה מגדירה מקצועות שכן כפופות להסדרה וביחד עם אותה הגדרה יוצרים את המקצועות. באף מקצוע אחר שאני מכיר (ויכול להיות שאני טועה כאן), אין הבדל בין הסמכות בגרנולציה כזו. אין "עורך דין למקרקעין" ו"עורך דין למסים" אלא יש עורך דין. המדינה החליטה שכל עורך דין ידע שכבה בסיסית של החוק, וכאשר יחליט לבחור לעצמו לאחר מכן לעסוק רק בחלק מהתחומים, לא תהיה מניעה שהוא יעסוק בעוד תחומים.

כלומר, **המדינה החליטה שמרגע שעברת את ההסמכה כעורך דין, אם תחליט בבוקר לייצג נאשם בהליך פלילי ובערב לתת ייעוץ מס לחברות בינלאומיות, זה מותר.**

במקרה שלנו, לא יכול להיות חוקר על שבבוקר הוא חוקר פורנזי שמעצב ראיות ובערב עורך בדיקות חדירה. מי שרוצה לעשות את שני הדברים יצטרך לערוך שתי בחינות שונות, ולקבל הסמכה בשני מקצועות שונים. מדובר בהסמכת יתר.

ההסדרה חלה רק על עולם הסייבר, לצערנו.

כל מי שקרא קצת על ההיסטוריה של עולם אבטחת המידע (ונניח, לקרוא את הספר של קווין מיטניק Ghost in the Wires, היא התחלה טובה) מבין ש"סייבר" זו שיטת חשיבה; היא לא מוגבלת לטכנולוגיה או לידע מקצועי בתפעול של מכשירים או קוד כלשהוא, אלא דווקא חלק מאנשי האבטחה הטובים ביותר מעולם לא אחזו במקלדת. לדוגמא, האחים בדיר ואורן אברהם הם לא אנשי מחשוב מובהקים, ודווקא ההקשר שלהם כאנשים מה"תחום" הוא מתחייב. כך גם התחביב של מנעולנות, שנפוץ מאוד בקרב קהילת אבטחת המידע, הוא חלק מהידע שדרוש לצורך ארגז הכלים הכללי של האקרים.

כך גם הכלל של "הנדסה חברתית", מה לעשות, מוזכר במסמך ב"מוסמך מבדקי חדירה" כחלק משילוב (תחת הגדרת חלק מההסמכה "משולב טכנולוגי ואנושי"). אבל נושא ההנדסה החברתית, שבדרך כלל אינו דורש ידע טכנולוגי כלל אלא יכולות הטעיה שמבוססות על כשלים פסיכולוגיים, יכול לבוא ממישהו שכלל אינו מוסמך או מיומן בכלים טכנולוגיים.

עכשיו; אני לא אומר שצריך להוסיף מקצוע בשם "מוסמך הנדסה חברתית" אלא ההפך: שכל הנושא של לייצר תתי מקצועות בתוך נושא ההסדרה הזה מגוחך בערך כמו שיהיה בדל בין ההסמכה בחוק של "טבח אסייתי" ל"שף במסעדת יוקרה". בשני המקרים צריך להעביר לאנשים את העקרונות של בטיחות במזון, להכיר להם את הסיכונים בשימוש בסכין, אבל להגיד לשף כמו **ישראל אהרוני** שמרגע שהוסמך כשף אסייתי הוא יצטרך לעבור הסמכה שונה אם הוא ירצה לפתוח מסעדה צרפתית זה בערך כמו לייצר הבדל בין **מוסמך מבדקי חדירה** ל**מוסמך הנדסה חברתית**.

ההסדרה תייצר מאכערים, קורסים מיותרים, ועלויות כניסה לשוק.

ברגע שיש בחינות הסמכה, יש תמיד קורסים להכנה לאותן בחינות הסמכה. במקרים רבים (והבחינות של לשכת עורכי הדין הן רק דוגמא אחת) מדובר בהכשרה יקרה יחסית, עם קורס שמלמד אותך לעבור את הבחינה ולא מלמד אותך את המקצוע. גם כאן, כאשר יש בחינות סדורות סביר מאוד להניח שמה שיקרה הוא שגורמים יעשו הוא להכין קורסי הכנה, ככל הנראה על חשבון הפקדון הצבאי, שכל מה שהם יעשו הוא לכלכל תעשיה שלא באמת מכשירה את האנשים למקצוע, אלא רק לעבור את הבחינה.

לדוגמא, הרבה מאוד מערכות ההכנה לבחינות של מיקרוסופט הן לא יותר מאשר Brain Dumps. אני לא חושב לרגע שזה לא יהיה המצב בבחינות ההסמכה שלנו; במקום להתמקד בהסמכה שהיא מבוססת על תוצאות או על ידע מקצועי, הרי שהבחינה תהיה מבוססת על שפיכה של חומרים ושינון בעל פה, ולא תועיל במיוחד למקצוע .התוספת השניה לעניין תהיה ההכנסה של מאכערים לשוק (גיא רולניק כתב על זה דווקא בהקשר של הייצוע הבטחוני); כל מי שירצה לקדם טכנולוגיה מסוימת יכניס אותה לחומר הלימוד והבחינה בלי קשר לשאלה האם זו חלק מהפרקטיקה המקובלת.

ומכאן להסדרת הייצוא הבטחוני, בקצרה.

בניגוד להסדרת מקצועות הסייבר, בה מדינת ישראל השקיעה 20 עמודים בכתיבת מסמך מפורט, שאפשר להגיב אליו ולהעיר על תוכנו, הרי שבהסדרת הייצוא הבטחוני לא כך הדבר. נבין קודם כל את הדרך שבה המוצרים עוברים רגולציה, ואז משם נוכל גם להבין את הביקורת הרבה שנשמעת בחודש האחרון. חוק הפיקוח על ייצוא בטחוני הוא חוק שעיקרו היא הגבלה על מסחר בנשק. המטרה של החוק היא שכל מי שסוחר עם מדינות (גם ידידותיות) בנשק, מתווך בעסקאות כאלו, או קשור לעסקאות, יעבור תהליך של רגולציה, ירשם, יקבל את הבדיקות הנאותות.

אבל מה זה נשק? יש כלים שהם "דו שימושיים (dual use)" מדובר על כלים שיש להם גם שימוש אזרחי וגם שימוש צבאי; אבל בגלל דו-השימושיות הזו, צריך להגדיר אותם יותר לעומק. ובכן, כאן בא צו הפיקוח להסביר מהו נשק דו שימושי. אבל יש בעיה; צו הייצוא הבטחוני בנוי קצת עקום. במקום להכין רשימה של מה זה נשק דו שימושי, הצו קובע שמה שנכלל ברשימה שמפורסמת באתר של משרד הבטחון הוא נשק דו שימושי.

אם נכנס לאתר, נראה שהקישור בכלל מפנה לאתר מחו"ל, של הסדר בשם "הסדר וסנאאר"; ההסדר עצמו מכיל רשימה מאוד טכנית של מהן הטכנולוגיות הנתונות לפיקוח, וקובע כלל שטכנולוגיות מדף, טכנולוגיות שנמצאות בנחלת הכלל, או טכנולוגיות שמבוססות על פרסומים מדעיים קודמים, לא ממש יכללו בפיקוח. למרות זאת, כרגע החליט משרד הבטחון לשנות את ההסדר, ולהוסיף לא מעט מוצרים לרשימה .צו הפיקוח המוצע, ודברי ההסבר שמובאים לידו, הם לא ארוכים (שני עמודים כל אחד מהם), ופתאום מוסיפים להתייחסות לא מעט דברים שנראים לנו, כאנשים שעוסקים במקצוע, כלא ראויים להכלל תחת ההגדרה של "נשק".

הבעיה, אם כבר יש חוק נגד וירוסים.

התייחסות חברת סימטריה היא התחלה טובה להבין את ההסדרה עצמה והרעיונות מאחוריה, למרות שמסמך תגובה בן 40 עמודים להצעה בת שני עמודים היא קצת בעייתית. הדבר הבעייתי העיקרי בצו הוא

ההגדרה של "חולשה" וההגדרה של סחר בחולשות כסחר באמצעי נשק (כלומר, איסור פלילי על מכירת חולשות בלי רישוי של משרד הבטחון).

עכשיו, צריך לזכור שגם היום יש איסור פלילי על מכירה של וירוסים ותוכנות פריצה, למעט מכירה לרשויות מוסמכות (סעיף 6 לחוק המחשבים); כלומר, כבר היום אסור להפיץ תוכנות ריגול, וירוסים ודברים דומים וגם לפתח את התוכנות האלה אלא "כדין", כלומר לצורך שימוש על ידי רשויות שמורשות להשתמש בתוכנות. לכן, הוספת איסור ייצוא והגבלה על מכירה של תוכנות חדירה, גם לרשויות מבצעיות אחרות, אומר שיש עוד איסור מיותר, ושצריך לעבור תהליך של הסמכה ואימות שלא מתאים לעולם הסטארטאפ הקטן של ישראל.

הבעיה, אם פתאום צריך לעבור תהליכי אישור ארוכים.

אם מדובר על סטארטאפ ישראלי שמייצר מוצר תקיפה, או מוצר שמבוסס על חולשה שידועה רק לו, שמוכר את המוצר בעולם למשטרות כדי לעזור להן לפרוץ מכשירים של חשודים בטרור, או כדי להאזין לשיחות מוצפנות, אז נכון להיום אין לו הגבלה בחוק והוא יכול למכור את המוצר בצורה חופשית. לעומת זאת, מרגע שההסדרה הזו תתקבל, אז לפני שהוא בכלל מתחיל לשווק את המוצר הוא יצטרך ללכת לקבל אישורים רבים ממשרד הבטחון, ולהעזר באותם מאכערים ואנשי תעשיה.

זה אומר שכל תהליך של מכירת תוכנה, שיכול היה להיות קצר במיוחד, יהפוך להיות תהליך של שנים, מה שמעוות מעט את היכולת להשקיע באותו סטארטאפ.

אז מה אפשר לעשות?

הרצון של המדינה לפקח על התחום הוא לגיטימי ומקובל; אבל, לדעתי האישית, הרצון לייצר גרנולציה במקצוע במקום דרישות קדם תייצר יותר נזק מתועלת. הסדרה יעילה היתה דורשת באמת קבלת הסמכה בצורה דומה לחוקר פרטי (בדיקה של עבר פלילי, מבחני אתיקה בסיסיים, מבחני ידע ראשוניים) ולאחר מכן, כל מי שעבר את ההסמכה יקבל את הזכות להשתמש בכינוי "עוסק סייבר" או "מוסמך סייבר". כמו כן, **ביחד עם ההסמכה המדינה צריכה לתת פטור לחוקרי אבטחה מאחריות על בדיקות חדירה**. כלומר, לאפשר להם ארגז חול קטן שאומר "כל עוד לא עשיתם נזק, ניתן לכם גם סוכריה ביחד עם ההסמכה הזו."

בכל הנוגע לנושא הגבלות הייצוא, הרי שהרשימה שהמדינה בנתה בנויה לא טוב; היא עוברת ומגדירה טכנולוגיות רבות מדי כאסורות בייצוא, היא מטילה רגולציה כבדה ויקרה והיא מייצרת תמריצים לרמות ולעקוף את החוק הזה.