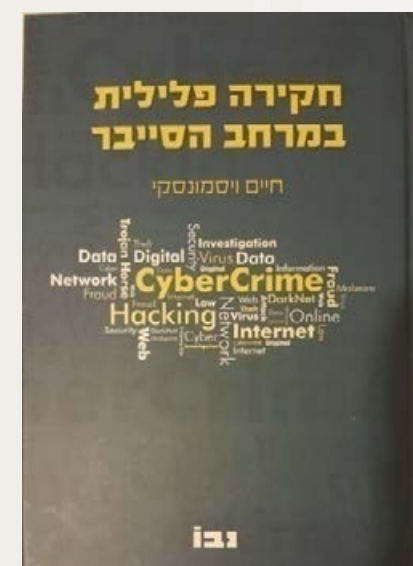


חיים ויסמונסקי "חקירה פלילית במרחב הסייבר"

חיים ויסמונסקי "חקירה פלילית במרחב הסייבר", הוצאת נבו, התשע"ו - 2015, 415 עמ'.

אוקינוסים של דיו נכתבו על השלכות רשת האינטרנט על חיינו, ובמקביל, על השינויים הצפויים וההכרחיים בעולם המשפט. המחקר שלפנינו מצומצם יותר ועוסק בשאלה ברורה וממוקדת, כיצד ניתן לאסוף ראיות קבילות ומהימנות במרחב הסייבר? ראיות אמינות, שניתן יהיה להגישן ולהסתמך עליהן במשפט הפלילי - הדורש כידוע הוכחה מעבר לספק סביר.

התיזה המרכזית של המחבר פשוטה. לטענתו, בדרך המקובלת כיום של איסוף הראיות במשפט פלילי שולטים שני עקרונות, הטריטוריאלי, והפיזי. על פי העיקרון הטריטוריאלי קיים מעין 'קיר ברזל' בתחומי המדינה. סמכותה היא רק עד הגבול ומתפוגגת לחלוטין מאחוריו. העיקרון הפיזי גורס שראיות הן 'חפצים' תופסי נפח ומשקל, ולבית המשפט יש להביא כמובן את הראיה הטובה ביותר שהיא בדרך כלל אחת ולא ניתנת לשכפול - 'הסכין המדממת', 'המסמך המזוייף', וכו'. אם מנסים אנו להשליך מעקרונות אלו הטריטוריאלי והפיזי על העולם הדיגיטלי, עומדים אנו בפני מכשול בלתי עביר. פעמים רבות מדי הראיות 'נמצאות' על גבי שרתים במדינות רחוקות מישראל, וגם אם יש משהו בידינו, מדובר בהעתק של העתק של חומר שאיננו כאן. ממילא תמיד יהיה מי שיגיד שהחומר



מזוייף ויתבע את 'המקור'. נציין כי בתחילת עבירות המחשב היו סניגורים רבים שתבעו כי המחשב המקורי יובא לבית המשפט, ואם היו כמה כאלה בשרשרת, דרשו את כולם, ועוד כהנה וכהנה.

אלא שהפגיעה לדעת ויסמונסקי איננה רק ברשות האוספת ראיות אלא גם בנאשמים ובציבור. כך למשל, לצורך גילוי ראיות, כמעט תמיד מחרימה המשטרה מחשבים וציוד אחר הנחוץ מאוד לנאשמים ולעיתים לצדדים שלישיים. הפגיעה בהם היא מעל ומעבר לנדרש לצורך הראיה הספציפית. לעתים לצורך תמונה במחשב או בטלפון הסלולרי מבקשת אותו המשטרה לזמן לא מוגבל. המחקר הראה שברוב צווי החיפוש שמבקשת המשטרה, מבוקשת חדירה לכל המחשבים ולכל המדיה הקיימת בחצרים שבהם נעשה החיפוש. הנזק הכלכלי ועוגמת הנפש הנגרמים ברורים, אך במסגרת הקיימת אין אפשרות אחרת.

כנגד כך מציע המחקר מודל חדשני שהוא קורא לו 'המודל הפרסונלי'. חידושו של מודל זה הוא התמקדותו באנשים נשואי העבירות (או החשדות) ולא בראיה עצמה. קרי, איננו מתמקדים בסכין המדממת אלא ביחס של סכין זו לבעליה. לענייננו, במקרה וחשוד כלשהו נמצא בישראל, הרי כל ראיה דיגיטלית הקשורה אליו תיחשב כרלוונטית ומותרת להשגה. אפילו אם מדובר בדוא"ל ו/או קובץ מחשב הנמצא על שרת שאיננו בישראל. הרחבת הסמכות פועלת גם לטובת הנאשם. באותה צורה, לא נאפשר למשטרה לחפש בכל מחשב/מדיה אלא אם כן ניתן יהיה להראות קשר ישיר בין החומר לבין החשוד.

נעיר כי המודל נראה מבטיח אך המחקר לא ירד לרזולציה מספקת שתסביר אותו לפרטיו. לא לגמרי ברור כיצד התיאוריה תתורגם לשפת המעשה. המחבר מציע כי החוק והמעשה יתייחסו פחות להיבט הטריטוריאלי והפיזי של הראיה, ויותר לשיקולים ממוקדים. למשל, בחירת פעולות איסוף ראיות פוגעניות פחות, הטלת חובת תיעוד על רשויות האכיפה, אישור שימוש בהעתקים ועוד. אבל

המחקר מציע מודל חדשני שהוא קורא לו 'המודל הפרסונלי'. חידושו של מודל זה הוא התמקדותו באנשים נשואי העבירות (או החשדות) ולא בראיה עצמה

למרות זאת, ההסברים אינם מפורטים דיים כדי שניתן יהיה להשתמש בהם כבר כעת. מבחינה זאת, יש מקום נרחב להעמקה.

למרות שהספר מתמקד באיסוף ראיות דיגיטליות, הוא מכיל רבות מעבר לכך. פרק נרחב עוסק בחלופות לאכיפה הפלילית. הכוונה היא למנגנונים חברתיים, כלכליים וטכניים שאינם קורים למנגנוני אכיפת החוק. מנגנון הביוש (shaming) לדוגמה ידוע ואפקטיבי מאוד, אם כי סכנותיו ברורות. פתרונות טכנולוגיים פתרו ופותרים בעיות בצורה עדיפה מהפללה. למשל, כיום כמעט ונפתרה בעיית ה-spam על ידי מנגנוני ניטור שלא מאפשרים ל-spam להגיע לתיבת הדואר האלקטרוני. ייתכן (אך לא בהכרח) שחלק מאותן נזקות הקיימות כיום ייבלמו בעתיד בצורה דומה. בכל מקרה, המחבר מגיע למסקנה ההגיונית שגם אם הטכנולוגיה תהיה נפלאה, תמיד נצטרך כנראה גם את שוט האכיפה הפלילית.

בעייתיות אחת בספר עולה מייד לעיני הקורא. למעשה, היא משותפת לכל ספר/מחקר שעוסק במשפט האינטרנט וקשורה לעובדה שהטכנולוגיה מתקדמת פלאים. עוד טרם יוצא הספר לדפוס כבר יש התפתחויות חדשות. גם בספר שלפנינו יש דוגמאות לכך. כתיבתו הסתיימה לערך בשנת 2014 והוא יצא לאור בשלהי 2015. ממילא הוא עוסק בעבירות האינטרנט שהיו

נפוצות אז אך מתייחס פחות לעבירות המטרידות כיום. אלו קשורות לתוכנות הכופר למיניהן (כִּפְרָה בעברית תקנית ובאנגלית Ransomware). תוכנות אלו (נוֹזְקוֹת) מצפינות את החומר במחשב המותקף ושולחות את המפתח לשחרורו רק אחרי תשלום הכופר (בדרך כלל באמצעות ביטקוין). ניצנים של תוכנות מעין אלו היו כבר בתחילת שנות התשעים. אולם רק לאחרונה עקב התחזקות כח המחשוב שאיפשר הצפנות מתוחכמות, והשימוש בביטקוין שאיפשר אנונימיות, הפכו אלו לשכיחות ומציקות. נראה שיהיה צורך בחקיקה ייחודית לעבירות אלו, ויפה שעה אחת קודם.

המחבר מגיע למסקנה ההגיונית שגם אם הטכנולוגיה תהיה נפלאה, תמיד נצטרך כנראה גם את שוט האכיפה הפלילית

כך גם אין התייחסות מספקת בספר לטלפונים החכמים (smartphones). כיום קשה לנו לחשוב על חיינו בלעדיהם, אבל הטלפון החכם הראשון (הדור הראשון של האיפון) יצא לאור באמצע שנת 2007. כיום (ראשית שנת 2017) קשה לדמיין את חיינו בלעדיו למרות שפחות מעשר שנים עברו. רוב הציבור משתמש במכשיר הנייד פי כמה מאשר במחשב האישי. הדור הצעיר משתמש יותר בתוכנות מסרים מיידיים למיניהן מאשר בדואר אלקטרוני. סביר להניח שחיפושי ראיות יתמקדו יותר במכשירים הניידים מאשר במחשבים, ולמרות שהנושאים קרובים, הם אינם זהים.

הספר מבוסס על עבודת הדוקטורט של המחבר, ד"ר חיים ויסמונסקי המשמש כיום מנהל מחלקת הסייבר בפרקליטות המדינה ועוסק בכך בפועל. יתרונו של המחבר הוא בשילוב התיאוריה עם המציאות וניסיונו המעשי נראה בבירור בספר.

מומלץ לכל מי שמתעניין בצד הפלילי של דיני האינטרנט, ובעיקר לאלה שעוסקים בכך בפועל.