חוק הסייבר: פרק הרגולציה – תמונת מצב עכשווית

ביום 6 במרץ 2018, ערך מרכז המחקר להגנת הסייבר שבאוניברסיטה העברית בשיתוף עם מערך הסייבר הלאומי שבמשרד ראש הממשלה כנס בנוגע לפרק הרגולציה בתזכיר חוק הסייבר המתהווה.

עו"ד [עמית אשכנזי](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/amit_ashkenazi_0.pdf), היועץ המשפטי של מערך הסייבר הלאומי, הציג את תהליכי קביעת המדיניות בתחום הגנת הסייבר בישראל, בדגש על הציר הרגולטורי. משנת 2015, ניכרת מגמת האחדה ברגולציית הסייבר, אשר נתבססה קודם לכן בעיקרה על רגולציה מגזרית: מערך הסייבר הלאומי מהווה גוף מנחה של הדיסציפלינה, וקיימת "רשת אסדרה", במסגרתה מונה נציג מקצועי של מערך הסייבר במשרדי ממשלה עם סמכויות אסדרה. עו"ד אשכנזי הדגיש כי "הגנת סייבר" פירושה פעולות לצורך שמירה על תפקודן התקין של מערכות מחשב, המידע בהן, והתקשורת הארגונית – ללא עיסוק בתוכן. הקפדה על טיפול במידע שאינו תוכן במסגרת גוף נפרד וייעודי שאינו עוסק באכיפת חוק, מאפשרת שמירה על זכויות יסוד וצמצום הפגיעה הפוטנציאלית בפרטיות.

עו"ד אשכנזי הציג את מתווה תזכיר חוק הסייבר, שטרם פורסם. לפי התזכיר, מערך הסייבר ישמש המנחה הלאומי בתחום הגנת הסייבר. מערך הסייבר ממפה וימשיך למפות את הסביבה בה נדרשת הגנת סייבר, ויפתח תורת הגנה בסייבר. ברמה המגזרית, הרגולטורים השונים יידרשו להתאים את הוראותיהם לתורת ההגנה, אלא אם ישנם שיקולים מקצועיים אחרים המכתיבים תוצאה שונה. במסגרת המיפוי, יזוהו גופים בעלי סיכון גבוה, ועליהם יופעל פיקוח במישרין על-ידי מערך הסייבר – אם במתווה של השלמת סמכויות מול הרשות המאסדרת המגזרית, ואם על דרך של הנחייה זמנית במקרה של סיכון גבוה נקודתי.

[רפאל פרנקו](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/rpl_prnqv.pdf), ר' אגף בכיר אסדרה והכשרה במערך הסייבר הלאומי, הדגיש כי בהתמודדות עם איומי סייבר, מדינת ישראל מפעילה כלים אחרים לצד רגולציה, דוגמת בניית תשתיות הגנה מבצעיות, בהתאם לאיום, לסיכון ולכשל השוק.

[יובל שגב](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/yuval_segev.pdf), ר' תחום מתודולוגיה במערך הסייבר הלאומי, הציג את [מפת הדרכים של מרכז המתודולוגיה](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/mtsgt_mrkz_mtvdvlvgyh_-_mpt_hdrkym_2018_002.pdf). ותיאר את תוכנית העבודה לשנת 2018 ביחס להטמעת, הרחבת והנגשת מסמך תורת ההגנה בסייבר, המשמש כתקן הגנת הסייבר הישראלי. בין השאר, הזכיר מר שגב את המאמץ למפות את תאימות תורת ההגנה אל מול תקנים קיימים, על מנת להקל על הגורמים המטמיעים אותו המצויים ממילא בסביבה היפר-רגולטורית ורוויות תקנים; פיתוח עזרים השונים לגורמים בתוך הארגון, הנדרשים להדגשים המתאימים להם ביחס לתורת ההגנה; וכן, ניסוח הרחבות ומסמכי best practice נקודתיים.

הפאנל 'פערי ידע בסייבר ואתגרים במשק הישראלי' נערך בהנחייתו של מר ישי ורטהיימר (שותף, KPMG), בהשתתפות מומחים מהתעשייה והממשלה. [יעקב דולמיצקי](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/yqb_dvlmtsqy.pdf), מנהל יחידת ההגנה על מידע וסייבר בתעשייה במשרד להגנת הסביבה, תיאר את התאמת תורת ההגנה בסייבר לאיומים הקונקרטיים בהם מטפל משרדו. [יוליה כץ](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/yvlyh_kts.pdf) התייחסה לאופן בו מטופלים ארגוני תמ"ק (תשתית מדינה קריטית) על-ידי מערך הסייבר. בארגונים אלה, שיש אינטרס לאומי בהמשך תפקודם, המדינה לא משאירה את הגנת הסייבר לארגון עצמו, ומחילה עליהם רגולציה נוקשה יותר, לצד תהליכי ליווי והנחייה צמודים.

נציגי התעשייה בפאנל ציינו את האתגרים שבמורכבות העומס הרגולטורי המוטל על חברות, הנדרשות לתת מענה לרגולטור המגזרי ולמערך הסייבר, כמו גם לרגולציה זרה (HIPPA, GDPR), והתייחסו לקשיים בהעלאת המודעות להגנת סייבר בארגון. ישנם ארגונים בהם המנהלים אינם מודעים למחויבות שלהם לביטחון סייבר, וקיומה של רגולציה מחייבת עשויה לשמש כתמריץ לכך, ולהקצאת משאבים ארגוניים לקידום הנושא. הליווי המתודולוגי של מערך הסייבר את הארגונים הגדולים צויין לחיוב, כמערכת יחסים בין שותפים בעלי זהות אינטרסים בהגנת סייבר, ולא כמערכת יחסים של רגולטור וגורם מפוקח. הפאנל התייחס בנוסף למצבם של גופים עתירי רגולציה בסביבה חסרת רגולציה. שרשרת האספקה היא עקב האכילס של ארגונים אלה, בהיותה מורכבת מגופים קטנים יותר, שאינם נושאים בנטל הרגולטורי, אלא אם תקנים ודרישות מסוימות מעוגנים בהסכמים חוזיים. כמו כן, חברי הפאנל חזרו והדגישו את מצוקת כוח האדם ואת הצורך בהכשרה של מקצועות הסייבר, כמו גם בחינוך כללי יותר להעלאת המודעות בקרב הציבור לחשיבות הנושא.

הפאנל 'החוק המוצע ועקרונות הרגולציה' בחן את התזכיר המוצע בפרספקטיבה אקדמית. [פרופ' יואב](http://csrcl.huji.ac.il/people/yoav-dotan?ref_tid=3506) דותן התייחס להיבטים המיוחדים של רגולציה בזירת הסייבר: היתרון לריכוזיות ולשמירה על תקנים אחידים, וקיומם של מתווכים. להבדיל מרגולציה קלאסית, המעמידה את הממשלה מול הסובייקטים של הרגולציה, בעולם הסייבר נראה שישנם שחקנים רבים בעלי מעמד ביניים, גורמים פרטיים שמפאת גודלם ומעמדם בשוק יש בכוחם לבצע עבודה רגולטורית משמעותית – איזה שימוש יש לעשות במתווכים אלה? פרופ' [מרגית כהן](http://csrcl.huji.ac.il/sites/default/files/csrcl/files/margit_cohen.pdf) התייחסה למודל הרגולטורי המבוזר המוצע בתזכיר, במסגרתו מערך הסייבר מנחה את הרגולטורים המגזריים, והצביעה על דמיונו למודלים של enforced self-regulation. עו"ד יורם הכהן הצביע על כך ששאלת ההגנה על האזרחים הוצאה מהפתרון הרגולטורי – אך יש להתייחס גם אליה, למשל, באמצעות פיקוח על איכות ציוד התקשורת, או באמצעות חינוך, תוך שימת לב להיבטים של שמירה על זכויות אדם. עו"ד הכהן ציין את הצורך בפיקוח רגולטורי על משרדי הממשלה. בעוד שבהעדר ניגוד עניינים בסיסי, ישנה זהות אינטרסים בין מערך הסייבר לגופים המסחריים עליהם הוא מפקח, גופים ממשלתיים לא רואים לנגד עיניהם אינטרסים מסחריים בלבד, ויש לתת למערך הסייבר סמכויות לעבוד מול משרדי ממשלה. ד"ר [תהילה שוורץ אלטשולר](http://csrcl.huji.ac.il/people/tehilla-shwartz-altshuler?ref_tid=3507) התייחסה לכך שסייבר הוא לא חזות הכל, וכי חינוך למודעות לאיומי סייבר מהווה חלק מהקניית אוריינות דיגיטלית, הכוללת היבטים שאין עמם דבר וחצי דבר עם ביטחון. נוסח תזכיר החוק נעדר איזונים ובלמים המבטיחים הגנה ראויה על הפרטיות, וזאת כאשר ישנו חוסר במדיניות פרטיות חוצת ממשלה. המודל המולטי רגולטורי המוצע, עשוי להתגלות כבעייתי. יש רשויות שלהן יש ניסיון רע בשיתוף פעולה רגולטורי עם רשויות אחרות, ואפשר שמערך הסייבר, המשמש כרגולטור של רגולטורים, עשוי לסבול מכך. ד"ר אלטשולר התייחסה גם לכך שהתזכיר נמנע מלהתייחס לאיומי 'תקיפה תודעתית', דוגמת תופעת ה-fake news ומניפולציות אחרות על תוכן חברתי. פתרון המביא בחשבון היבטים של cognitive security, נדרש להתייחס לשאלות של זכויות אדם ולהתמודדות עם מתווכים גלובליים. פרופ' [דוד לוי פאור](http://csrcl.huji.ac.il/people/david-levi-faur) הצביע על תפקידו של המתווך הרגולטורי (rule intermediary), המצוי בתווך שבין המאסדר למאוסדר. המתווך הרגולטורי הוא בדרך כלל גוף פרטי המספק שירותי סרטיפיקציה וקרדיטציה.

.