מדינת ישראל
משרד המשפטים

אגף תכנון, מדיניות ואסטרטגיה

ירושלים: כ"ג סיוון תשע"ה
10 יוני 2015
מספרנו: 024-99-2015-001314

לכבוד: עו"ד אמי פלמור, המנהלת הכללית
עו"ד אלון בכר, ראש רמו"ט
אלדד קנטי, סמנכ"ל תכנון, מדיניות ואסטרטגיה

הנדון: <u>בחינת רמו"ט לאן ? - סיכום בחינה והמלצות למדיניות</u>

1. כללי

א. במסגרת דיון להצגת ואישור תכניות העבודה ליחידת הרשות למשפט, טכנולוגיה ומידע (להלן: רמו"ט) לשנת 2015 שהתקיים בתאריך 26/2/2015, מינתה המנהלת הכללית את הח"מ, כתוצאה מצורך שעלה בדיון, לבחון את ייעוד יחידת רמו"ט ומשימותיה בהתאמה לעת הנוכחית ולאתגרי העתיד.

ב. **<u>מטרת מסמך זה היא להציג את תוצאות הבחינה והמלצותיה.</u>**

ג. מסמך זה נכתב לאחר מפגשים עם בעלי תפקידים רלוונטיים לנושא במשרד המשפטים ומחוצה לו, קריאת מקורות כתובים, עריכת טיוטות והצגתם לבעלי תפקידים ולראש רמו"ט.

ד. מודגש כי ברמו"ט נמצאים עובדים מקצועיים ומסורים הפועלים מתוך שליחות ציבורית ומחויבות עמוקה להגנה על האינטרס הציבורי.

2. רקע

א. קיימים שינויים משמעותיים ומרחיקי לכת במרחב הסייבר ובין השאר במרחב הפעילות של רמו"ט. הנושא נמצא על סדר יומה של הממשלה ומתקיימים תהליכי העצמה של כלל הגורמים המטפלים בנושאים השונים. מסמך זה עוסק רק בנושאים שבאחריות משרד המשפטים (על הגופים והתפתחותם – ראה נספח א').

ב. רמו"ט משמשת כרשות משפטית לטכנולוגיות מידע והגנה על הפרטיות במשרד המשפטים. היחידה מאגדת תחתיה את הפעילויות של רשם מאגרי המידע לפי חוק הגנת הפרטיות, התשמ"א – 1981, רשם הגורמים המאשרים לפי חוק חתימה אלקטרונית, התשס"א – 2001 ורשם שירות נתוני אשראי ושירותי מידע על עוסקים לפי חוק שירותי נתוני אשראי, התשס"ב – 2002. ראש הרשות אחראי על ניהול וההפעלה של מערך הרישום, הפיקוח והאכיפה המנהלית שבסמכות הרשמים הנ"ל ומרכז את מכלול הפעילות (עפ"י החלטת ממשלה מס' 4660 מיום 19/1/2006).

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

ג. רמו"ט מהווה נדבך נוסף בהיערכות המדינתית לטיפול באיומי הסייבר ובבניית מערכי ההגנה והבקרה על הגנת המידע ועל שימוש במידע אישי במדינת ישראל (על המונח 'סייבר' – ראה נספח ב').

ד. משימה נוספת של רמו"ט היא להביא לכך שבכל הגורמים הרלוונטיים יפעלו לניהול מידע שברשותם באופן תקין בהתאם לחוק הגנת הפרטיות ולתקנותיו, כך שתישמר הזכות של כל אזרח לפרטיות במידע אודותיו.

ה. בימים אלו נכנסת לתוקף רפורמה רחבה במשטר הפרטיות במידע באיחוד האירופי ואנו נמצאים בשלבים האחרונים של תהליכי חקיקתה. להתפתחות זו השפעה בלתי מבוטלת על יכולתה של מדינת ישראל לעמוד בסטנדרטים בינלאומיים של הגנת פרטיות המידע (על הגנת הפרטיות בעולם – ראה נספח ג').

3. הנחות יסוד

א. מרחב הסייבר מתפתח בקצב מוגבר ובהתאמה גם השפעתו על כלל תחומי החיים.

ב. התפתחות מרחב הסייבר יוצרת פערים משפטיים-טכנולוגיים הולכים וגדלים (קצב התפתחות הטכנולוגיה גבוה לעין שיעור מקצב התפתחות החקיקה והמענה המשפטי בנושאי טכנולוגיה).

ג. בגלל עליית סיכון וזמינות טכנולוגית, קיימת מגמה של התחזקות והתעצמות של הגופים העוסקים בסייבר. עיקר העשייה וההערכות הינה במרחבים הביטחוניים, בהם ניתן מענה רחב לאיומים על התשתיות הביטחוניות ועל התשתיות הלאומיות הקריטיות.

ד. ההגנה על הזכות לפרטיות מקבלת משנה תוקף בעידן הטכנולוגי של היום, אשר בו מרבית הפעילויות של האדם הן מקוונות ולפיכך גם יותר גלויות (ככל שהטכנולוגיה מתפתחת, ישנו כרסום גובר בפרטיות הציבור במערכות מידע וביכולת שלו לשמור עליה בכוחות עצמו).

ה. ככל שמתחזקת המגמה של העשייה הביטחונית בתחום, עולה הצורך במעורבות משרד המשפטים בכלל ובגוף משפטי שיתמקד ויעסוק בהגנת הפרטיות והמידע האישי של הציבור, למול אותם גופים ביטחוניים.

4. הנחות עבודה

א. ההישענות הגוברת של מערכות כלכליות, תקשורתיות ואחרות על תקשורת מתווכת מחשב (CMC – Computer Mediated Communication) מעלה את הצורך והחשיבות לפיקוח רגולטורי מוגבר ובדגש על עבירות מידע אישי.

ב. חוק הגנת הפרטיות נדרש לעדכונים עיתיים תדירים התואמים את התפתחות מרחב הסייבר ואת הקשיים לשמור על פרטיות האזרח. כיום ניתן לומר שקצב החקיקה אינו משביע רצון ואינו תואם את קצב התפתחות הטכנולוגיה.

ג. הקמת מוסדות ורשויות נוספות בתחום (ראה נספח א') מחייב חיזוק ממשקי עבודה והגדרת יחסי גומלין בין הגופים העוסקים בתחום לבין משרד המשפטים, וזאת לשם שמירה על האינטרס הציבורי בהיבטים של פרטיות ומידע אישי.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

ד. משרד המשפטים נדרש להיות נוכח בכל צמתי קבלת ההחלטות בתחום הסייבר ולקיים ראייה הוליסטית רחבה וקביעת מדיניות בכל הקשור להגנה על הפרטיות במערכות מידע.

ה. בכדי לשמור על רלוונטיות, נדרש להיות משפטן בעל הבנה ויכולות טכנולוגיות עמוקות אשר יוכל לסייע בהכרעה משפטית המבוססת על הבנה טכנולוגית.

ו. חברה טכנולוגית מתקדמת כחברה הישראלית נזקקת למענה רגולטורי משפטי כולל, מיומן ודינמי ההולם את תמונת המצב הטכנולוגית והעסקית.

ז. ניתן לחלק את המשימות המוטלות על רמו"ט בתחום ההגנה על המידע האישי באופן הבא:

1) רובד ממשלתי:

- ליווי פרויקטים טכנולוגיים ממשלתיים רחבים לצורך וידוא עמידת הפרויקט בדרישות הגנת המידע האישי.
- ליווי פרויקטים ביטחוניים משמעותיים לצורך וידוא שמירה על פרטיות הציבור, תוך מתן מענה לצרכים ביטחוניים.
- ליווי פרויקטים אזרחיים-ביטחוניים לשמירה על תשתיות קריטיות ווידוא שמירה על פרטיות הציבור תוך מתן מענה לצרכים ביטחוניים.

2) רובד אזרחי:

- הגנה מפני גניבת מידע אישי על אזרחים.
- הגנה בפני סחר במידע אישי של אזרחים.

5. עיקרי ההמלצה

א. מומלץ למקד את ייעודה של רמו"ט ולהגדיר אותה כ**רשות הגנת מידע אישי** במשרד המשפטים ולשנות בהתאם את שמה.

ב. במסגרת זו מומלץ למקד את היחידה בעיסוק בתחומים משפטיים-טכנולוגיים בהם יש לה יתרון יחסי מעצם היותה יחידה במשרד המשפטים. מיקוד זה משמעותו 'יחידת עילית' של מומחים בתחומי הטכנולוגיה והמשפט בעלי הבנה ייחודית של התחום ואשר ממוקדים בהגנה על זכותו הבסיסית של הפרט לפרטיות על פי החוק.

ג. מהעבודה עולה כי באין סמכויות מנהליות משמעותיות ויכולת חוקית להטיל סנקציות מנהליות משמעותיות אשר תייצרנה השפעה תודעתית בשוק, ניתן ברמו"ט דגש יתר לתחום האכיפה הפלילית. לאור התפתחות 'מגרש המשחקים' ו'השחקנים' החדשים בתחום, מומלץ שהיחידה תסיט משאבים מעיסוק זה לטובת קביעת מדיניות אכיפה (רישום, פיקוח ואכיפה מנהלית) בהקשרי הגנה על מידע אישי. יחידה זו תידרש לראייה רחבה ומשפיעה על כלל הגופים העוסקים בתחום שלהן נגיעה למערכות מידע. עליה לייצר הבנה והכרה בקרב כלל הגופים (הממשלתיים והאחרים), כי מטרתה המרכזית היא הגנה על פרטיות הציבור במערכות מידע.

ד. ישנה חשיבות לסמכויות האכיפה הפלילית, אך בעידן של מיעוט משאבים וריבוי משימות, מומלץ כי יחידה זו תפעיל סמכויות אלה במקרים מיוחדים בלבד ועל פי קריטריונים ברורים.

ה. לשם כך מומלץ כי היחידה תתמקד בעיסוק בסוגיות הבאות:

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

1) לשמש רשות מנהלית לביצוע התפקידים הנדרשים לפי חוק הגנת הפרטיות (רישום, פיקוח, בירור, אכיפה המותאמת למהות הנושא).
2) לשמש גורם מנחה, יוזם ומלווה בקביעת רגולציה בתחום הגנת מידע אישי.
3) לוודא מתן מענה הולם להיבטי הגנת מידע אישי במרחב הסייבר.
4) לשמש גוף מחקר וידע (זיהוי מגמות) בהיבטי הגנת מידע אישי.
5) לשמש גוף מנחה ומסביר לנושא הגנת מידע אישי באמצעות חינוך, הדרכה, הטמעה והסברה למול המרחב האזרחי, ארגונים וחברות ומשרדי ממשלה (לרבות מערכת הביטחון).
6) לשמש גוף המרכז את פניות הציבור בסוגיות של הגנה על מידע אישי.
7) לשמש גוף מנחה ומבקר לגופי הממשלה בהיבטי הגנה על מידע אישי.
8) להמליץ לשר על תיקוני חקיקה נדרשים בתחום, ככל שהם מצויים בתחומי סמכותו, ועל הצעות להחלטות ממשלה בתחום הגנת מידע אישי.

ו. מומלץ לחדש את פעילות 'המועצה להגנת הפרטיות' אשר תפקידה המרכזי הוא לייעץ לשרת המשפטים בנושאי חקיקה הקשורים להגנת הפרטיות. מומלץ להגדיר מחדש את תפקידה וסמכויותיה ולרענן את הרכבה כך שיינתן מקום לגופים המובילים בנושא מעולם האקדמיה, מהמגזר העסקי ועוד (ראה סעיף 10א בחוק הגנת הפרטיות, תיקון מס'4, תשנ"ו – 1996).

ז. קידום חקיקה רלוונטית - החקיקה הקיימת אינה עדכנית ואינה מתאימה למציאות הטכנולוגית המתפתחת. לכן מומלץ לתקן ולהתאים בהקדם את חוק הגנת הפרטיות למציאות העכשווית המתהווה בתחום. היעדר הסמכויות המפורטות בו פוגעים באפקטיביות היחידה.

ח. במסגרת תהליך המיקוד של היחידה, מומלץ להגיע להסכמה ברורה עם מחלקת ייעוץ וחקיקה על תהליכי העבודה המשותפים. מודל העבודה המשותפת צריך להיות על בסיס העיקרון של מיצוי היתרון היחסי של כל אחד מהגופים. המפתח להצלחה יכול להיות רק ע"י שילוב של התוכן המקצועי והגדרת מדיניות אכיפה (ע"י רשות הגנת מידע אישי) עם הידע בניסוח ותיקון חוקים והגדרת מדיניות ייעוץ וחקיקה (ע"י מחלקת ייעוץ וחקיקה).

ט. מומלץ להסדיר את יחסי הגומלין וממשקי עבודה למול גופים חיצוניים למשרד המשפטים הפועלים במרחב הסייבר (המטה הקיברנטי הלאומי ורשות הסייבר הלאומית במשרד ראש הממשלה, זרוע הסייבר בצה"ל, הרשות הממלכתית לאבטחת מידע בשב"כ, יחידת הסייבר המשטרתית ועוד). נכון יהיה ליצור מצב בו נציגי הרשות להגנת מידע אישי ישתתפו וישתלבו בכל אחד מצמתי קבלת ההחלטות בנושא הסייבר לצורך מימוש אחריותה.

י. רשם שירות נתוני אשראי ושירותי מידע על עוסקים לפי חוק שירותי נתוני אשראי (התשס"ב – 2002) – מומלץ לבחון מחדש מיהו הגורם המתאים להוביל רישום זה, במסגרת הסדרת כלל שוק האשראי.

יא. רשם הגורמים המאשרים לפי חוק חתימה אלקטרונית (התשס"א – 2001) – חתימה אלקטרונית הינה נדבך מתחום ההזדהות המכוונת. מומלץ לבחון העברת רישום זה ליחידת הממונה על יישומים ביומטריים במשרד ראש הממשלה.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

יב. מומלץ כי ביחידת רמו"ט תגובש תכנית אסטרטגית ליישום השינויים הנדרשים בנושאי התוכן וזאת בכדי להביא לידי ביטוי את קידום הגנת המידע האישי. מומלץ כי התכנית תתייחס לשני הרבדים המרכזיים של עבודת הרשות כיום: הרובד הממשלתי והרובד האזרחי ותתעדף את המשאבים והאמצעים העומדים לרשותה בצורה האפקטיבית ביותר לקידום הגנת מידע אישי ברבדים אלה. כמו כן, מומלץ כי הרשות תבצע בחינה אסטרטגית של מגמות טכנולוגיות אשר להן עלולה להיות השפעה על תחומי עבודתה של הרשות כגון: Internet Of Things, Big Data, שימוש באלגוריתמים אוטומטיים במתן שירותים, Self-Driving Cars, מחשוב לביש וכיוצ"ב.

יג. מומלץ כי משרד המשפטים יקיים תהליכי חשיבה ולמידה רוחבית בהקשרי הסייבר, לשם קידום וחידוד מעורבותו והשפעתו בתחום המתפתח וגיבוש אסטרטגיה משרדית אחידה המתכללת סוגיות חקיקה, אכיפה, מדיניות ורגולציה. בשל כך, מומלץ להקים ועדת היגוי משרדית לתחום הסייבר. מומלץ כי ועדה זו תנוהל ע"י ראש רמו"ט. מומלץ כי בוועדה זו ישתתפו הנציגים הרלוונטיים ממחלקת ייעוץ וחקיקה (כולל בינ"ל) ומפרקליטות המדינה, הממונה המשרדי על הגנת המידע וגופים נוספים כפי שיידרש.

6. סיכום

א. ניתוח מרחבי הסייבר בישראל מצביע על חלוקה של שלוש קבוצות: ארגוני הביטחון, תשתיות לאומיות ומשאבים קריטיים ושאר משתמשי מרחב הסייבר האזרחיים.

ב. שתי הקבוצות הראשונות מכילות גופים אזרחיים מובהקים ואין להמעיט בנזקים הלאומיים היכולים להיגרם כתוצאה מתקיפה מאורגנת על גורמים אלו. בגופים אלו מושקעים משאבים רבים הפועלים להגנתם, אך עלולים לעשות זאת תוך הפרת פרטיותו של הציבור.

ג. הקבוצה האחרונה היא למעשה הקבוצה הפגיעה ביותר לתקיפה של מי שיעדיפו לפעול מול יכולות הגנה פחותות. לתובנה זו משמעות רבה בהקשר לפיתוח הצורך בהגנה אפקטיבית על המידע האישי ואשר רמו"ט (רשות הגנת מידע אישי) צריכה להיות שותפה מרכזית בקיומה.

ד. בעידן בו אחסון המידע הוא נגיש ונוח, כמויות המידע הן עצומות וישנה יכולת פשוטה לעבד את המידע ולנתחו, כולנו יכולים להיות מושאים ליצירת פרופילים עד כדי הפיכתנו ל'חברה שקופה' בה כל אחד (או כל גוף מסחרי) יכול לדעת פרטים רבים על השני, והחיץ בין 'הפרטי' ובין 'הציבורי' נשחק עד כדי הריסתו לחלוטין. הסכנה בחברה כזו היא ברורה ואין צורך להכביר עליה מילים.

ה. הטכנולוגיה שמתפתחת בקצב מסחרר טומנת בחובה סכנות רבות לפרטיות ולאפשרות המשך קיומנו כחברה אנושית מתפקדת. באמצעות הטכנולוגיה, אזרחים רבים יכולים להגיע למידע פרטי על אודות אזרחים רבים אחרים וההרגשה היא של איבוד שליטה על המידע האישי. הגבולות חייבים להישמר והגורמים המתאימים חייבים לעמוד על המשמר כדי למנוע מצב בו לא ניתן יהיה לחזור לאחור.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

ו. מדינת ישראל כמעצמת סייבר עתידה ועלולה לטשטש את הגבולות בין מרחב אזרחי ובין מרחב ביטחוני ויש לפיכך להגדיר בצורה ברורה את הכלים הנכונים כדי לשמור את האיזונים הנכונים. במישור זה לרמו"ט (רשות הגנת מידע אישי) תפקיד קריטי וחיוני לשמירה על הפרטיות של האזרחים ועל עיצוב היכולת של הגופים הרלוונטיים לעשות שימוש במידע פרטי של הציבור ושל האזרח. לתפקיד זה גם פן תדמיתי-תקשורתי (כלפי פנים וכלפי חוץ) והוא מקבל משנה תוקף בעת בה מדינות העולם בוחנות את מעשינו בפריזמה של שמירה על חירויות האזרח.

ז. במרחב הסייבר פועלים גופים רבים, אך גם שחקנים קטנים באופן יחסי עלולים להשפיע באופן משמעותי על הביטחון הלאומי של מדינות.

ח. עבודה זו תיקפה את הצורך בגוף רגולטורי משמעותי בתחום הגנת מידע אישי. גוף אשר תפקודו ימצה את יתרונותיו היחסיים אל מול גופים אחרים. גוף אשר ישיל מעליו משקלות ותהליכים שלגופים אחרים יש בהם יתרונות יחסיים על פניו. גוף אשר יתמקם בצמתי קבלת ההחלטות בתחום הסייבר בנושאים שיש להן השלכות להגנת הפרטיות במערכות המידע.

ט. **רק שילוב ומימוש של כלל ההמלצות, ייצר מענה הוליסטי וערכי לנושא הגנת הפרטיות במערכות המידע.** מימוש כלל ההמלצות יחזקו את מעמדו ומיקומו של משרד המשפטים במארג הטיפול בהגנת המידע האישי בכלל, ובמרחב הסייבר בפרט.

"You can't have 100 percent security and then also have 100 percent privacy and zero inconvenience. You know, we're going to have to make some choices as a society."

Barak Obama, the New York Times, June 7, 2013.

בכבוד רב,

עוז שנהב
מנהל תחום בכיר תכנון אסטרטגי
אגף תכנון, מדיניות ואסטרטגיה
משרד המשפטים

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

מדינת ישראל
משרד המשפטים

נספח א' – גופים העוסקים בסייבר

רקע

האיומים במרחב הסייבר הופכים משמעותיים לביטחון הלאומי, לתפקוד התקין של המדינה והארגונים שבה, לסדר הציבורי ולפעילות המשק, ומצויים בעלייה מתמדת. כתוצאה מהיקף האיומים וחומרתם, עלול להיגרם נזק לרציפות במתן שירותים חיוניים, לחיי אדם, לפעילות המשק ולאינטרסים לאומיים חיוניים אחרים.

המענה המדינתי הנוכחי בתחום הגנת הסייבר אינו שלם ואף אינו מספק. הסנכרון בין כלל המאמצים והיכולות המדינתיות חסר, ויש צורך להעמיק את השותפות המתחייבת בין המגזר הביטחוני לבין המגזר האזרחי לצורך הגנה אפקטיבית.

לפיכך, נדרשת היערכות מדינתית כוללת שתוביל להעלאת רמת הגנת הסייבר ולהגדרת אחריות להגנת הסייבר ברמה הלאומית, זאת לצד שמירתו של הסייבר כמרחב פתוח המאפשר זרימה חופשית של ידע, הון ושירותים, מחולל חדשנות ותורם לרווחה חברתית, תוך שמירה על זכויות יסוד, ובהן הזכות לפרטיות וחופש הביטוי.

לאור זאת, החליטה ממשלת ישראל על 'קידום היכולת הלאומית במרחב הקיברנטי' (החלטת ממשלה מס' 3611 מיום 7/8/2011). במסגרת החלטה זו הוחלט:

א. להקים מטה קיברנטי לאומי במשרד ראש הממשלה (או בשמו המעודכן 'מטה הסייבר הלאומי').

ב. להסדיר את האחריות לטיפול בתחום הקיברנטי.

ג. לקדם את יכולת ההגנה על המרחב הקיברנטי בישראל ולקדם מחקר ופיתוח בתחום הקיברנטי.

מטה הסייבר הלאומי

ייעוד (החלטת ממשלה מס' 3611 מיום 7/8/2011):

גוף מטה לראש הממשלה, לממשלה ולוועדותיה, אשר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הקיברנטי, בכפוף לכל דין והחלטות ממשלה.

תפקידי המטה (החלטת ממשלה מס' 3611 מיום 7/8/2011):

א. לייעץ לראש הממשלה, לממשלה ולוועדותיה בנושא הקיברנטי. בענייני חוץ וביטחון הייעוץ לממשלה, לוועדותיה ולהרכבי שרים ייעשה באמצעות המטה לביטחון לאומי.

ב. לרכז את עבודת המטה של הממשלה וועדותיה בתחום הקיברנטי, להכין את דיוניהם ולעקוב אחר ביצוע החלטותיהם. בענייני חוץ וביטחון, הריכוז של עבודת המטה, הכנת הדיונים והמעקב אחר ביצוע ההחלטות, ייעשו באמצעות המטה לביטחון לאומי.

ג. להמליץ לראש הממשלה ולממשלה על מדיניות קיברנטית לאומית, להנחות את הגורמים הרלבנטיים אודות המדיניות עליה הוחלט על ידי הממשלה ו/או ראש הממשלה, ליישם את המדיניות ולבקר את יישומה.

ד. לפרסם, ככל שהדבר יידרש, לכלל הגופים הרלבנטיים, הנחיות מדיניות משלימות הנגזרות מהחלטות הממשלה וועדותיה בתחום הקיברנטי.

ה. לקבוע ולתקף מדי שנה את איום הייחוס הלאומי להגנה על המרחב הקיברנטי.

ו. לקדם מחקר ופיתוח בתחום הקיברנטי באמצעות הגופים המקצועיים.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

ז. לפעול לעידוד התעשייה הקיברנטית בישראל.

ח. לגבש תפיסה לאומית לטיפול במצב חירום במרחב הקיברנטי.

ט. לערוך תרגילים לאומיים ובינלאומיים לשיפור המוכנות של מדינת ישראל בתחום הקיברנטי.

י. לרכז את תמונת המודיעין בנושא הביטחון הקיברנטי מכלל גורמי קהילת המודיעין.

יא. לרכז את תמונת המצב הלאומית בנושא הביטחון הקיברנטי, מכלל הגופים העוסקים בתחום.

יב. לקדם ולהעלות את המודעות הציבורית לאיומים ולדרכי ההתמודדות עמם במרחב הקיברנטי.

יג. לגבש ולפרסם אזהרות ומידע לציבור בנוגע לאיומים הקיימים במרחב הקיברנטי, וכן כללים להתנהגות מונעת.

יד. לקדם בניית תכניות לאומיות לחינוך ולשימוש נבון במרחב הקיברנטי.

טו. לקדם שיתופי פעולה מול גורמים מקבילים בחו"ל בנושא הקיברנטי.

טז. לקדם את התיאום ושיתוף הפעולה בין הגופים הממשלתיים, הביטחוניים, האקדמיים, התעשייתיים, העסקיים והאחרים, הרלבנטיים לתחום הקיברנטי.

יז. לקדם חקיקה ותקינה בתחום הקיברנטי.

יח. להוות גורם מסדיר בתחומי הביטחון הקיברנטי.

יט. לבצע כל תפקיד אחר בתחום הקיברנטי שיקבע ראש הממשלה, בכפוף לכל דין ולהחלטות ממשלה.

<u>התשתית התפיסתית והחוקתית להקמת רשות לאומית להגנה בסייבר</u>

בתחילת ינואר 2015 הציג המטה הקיברנטי הלאומי, בישיבת הממשלה, שתי הצעות לקידום הרגולציה בתחום הסייבר: 'קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר' (החלטת ממשלה מס' 2443 מיום 15/2/2015), ו'קידום ההיערכות הלאומית להגנת הסייבר' (החלטת ממשלה מס' 2444 מיום 15/2/2015). בהצעות אלה הוצע להסדיר את תחום הסייבר בכללותו ולרכז את סמכויות האכיפה והאסדרה בו.

הצעות המטה הגיעו בעקבות העלייה באיומי הסייבר והפיכתם למשמעותיים ביותר לביטחון הלאומי, לתפקוד התקין של המדינה והארגונים בה, לסדר הציבורי ולפעילות המשק. בחודשים שלפני הגשת ההצעות, ניסח המטה הקיברנטי הלאומי תכנית לאומית להיערכות להגנה במרחב הסייבר.

בהצעה מגדיר המטה את המונח "הגנת סייבר" כ"מכלול הפעולות למניעה, נטרול, לחקירה ולהתמודדות עם איומי סייבר ואירועי סייבר, ולצמצם השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם". ניתן לראות, כי הגדרה זו הינה רחבה ועשויה לכלול אף מוצרים ושירותים בתחום תקיפת הסייבר, <u>ולמעשה מדובר באסדרה כוללת של כלל שוק הסייבר בישראל</u>.

על פי ההצעה תוקם, בהחלטת ממשלה, רשות לאומית להגנת הסייבר, <u>מעין רשות מבצעת</u>, שתפקידיה העיקריים הינם: לנהל, להפעיל ולבצע את כלל מאמצי הגנת הסייבר האופרטיביים, ביניהם לטפל באיומי סייבר בזמן אמת, גיבוש תמונת מצב שוטפת, ריכוז מחקר ומודיעין, ועוד; להפעיל מרכז לסיוע והתמודדות עם איומי סייבר, ה- CERT הלאומי, עבור כלל המשק, אשר יהווה גם נקודת ממשק בין גופי הביטחון לבין הגורמים במשק ובמסגרתו תרכז ותשתף מידע רלוונטי עם כלל הגורמים במשק; לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות <u>בנייה, פיקוח ויישום של הצעת האסדרה</u>.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

כמו כן, קובעת הצעת ההיערכות הלאומית, כי על המטה להקים, תשתית טכנולוגית לאומית ל: גילוי, זיהוי, התרעה ושיתוף מידע, לצורך גילוי וזיהוי של תקיפות סייבר על מדינת ישראל, אשר תופעל על ידי הרשות תוך מתן דגש לזכויות יסוד ובכלל זה היקף המידע שייאסף, היכולת לעשות בו שימוש, שמירתו ומסירתו.

הצעת ההיערכות הלאומית מציעה, כי על המטה, הלשכה המשפטית במשרד רוה"מ ומשרד המשפטים, להכין תזכיר חוק הגנת הסייבר, במסגרתה ייבחן, בין היתר, הצורך בתיקוני חקיקה נדרשים.

בעוד, כי הצעת ההיערכות הלאומית מסדירה, במאקרו, את סמכויות הגופים האחראים על הגנת הסייבר בישראל, הצעת האסדרה לעומת זאת, מסדירה במיקרו את האופן שבו תוסדר הגנת הסייבר.

תכלית הצעת האסדרה, בהתאם לדברי ההסבר שלה, הינה לתת "מענה למצב הקיים בו כל אדם יכול להציג ולהגדיר את עצמו כמומחה להגנת הסייבר או למכור מוצר המוצג כמוצר להגנת סייבר או להציע שירותים המוצגים כשירותי הגנת סייבר..." וכן לתת "מענה לכך שלמעט תחומים כגון תשתיות קריטיות ומגזרים וארגונים ספציפיים, רוב המשק פועל בתחום הגנת הסייבר באופן לא מוסדר ולא מחייב". לצורך כך, מציעה האסדרה לעשות שימוש בסטנדרטים מקצועיים הקיימים בעולם ואשר אומצו בישראל זה מכבר, וכן בחקיקה פרטנית בהתאם למגזר ו/או ענף ספציפי.

הרגולציה כאמור, עתידה לחול על כל הארגונים, חברות, נותני שירותים וספקים בתחום הגנת הסייבר בישראל ועל מוצרים ושירותים המיובאים לישראל או ניתנים בה.

בכל הנוגע למשרדי הממשלה, מציעה האסדרה, כי כל משרדי הממשלה יחויבו לעמוד בתקני אבטחת מידע ארגוניים, ימנו מומחה הגנת סייבר במשרד הממשלתי שתפקידו יהיה לגבש מדיניות הגנת סייבר אשר תהא גמישה לאיומים הקיימים, לתכנן תכנית תקציבית, לבנות תכנית עבודה ליישום התוכנית ולערוך ביקורת על אופן יישום התוכנית. כמו כן, יהא על משרדי הממשלה למנות "אחראי על הגנת הסייבר ביחידת מערכות המידע".

זאת ועוד, הצעת האסדרה מציעה להקים יחידה להגנת הסייבר בממשלה אשר תהא כפופה לממונה על התקשוב הממשלתי ובהנחיה מקצועית של הרשות הלאומית להגנת סייבר. מטרת היחידה הינה להכוון ולהנחות מקצועית את משרדי הממשלה בתחום הגנת הסייבר. כמו כן, מציעה האסדרה להקים מרכז שליטה ובקרה ממשלתי למול איומי סייבר, ה-SOC הממשלתי, במסגרת ה- CERT הלאומי, אשר יעסוק בגיבוש תמונת מצב ממשלתית שוטפת ומתן מענה באירועי סייבר.

רשות לאומית להגנה בסייבר

ייעוד (החלטת ממשלה מס' 2444 מיום 15/2/2015)

א. לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, בתפיסה מערכתית, לטובת מענה הגנתי שלם ורציף למול תקיפות סייבר, ובכלל זה טיפול באיומי סייבר ובאירועי סייבר בזמן אמת, גיבוש תמונת מצב שוטפת, ריכוז ומחקר מודיעין, ועבודה עם גופים מיוחדים.

ב. להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר (להלן ה- CERT הלאומי) עבור כלל המשק, ובכלל זה לפעול לשיפור החוסן ההגנתי בסייבר, לסייע בטיפול באיומי סייבר ואירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק ולהוות נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

ג. לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים וגופים במשק, הנחיית המשק בתחום הגנת הסייבר, אסדרת שוק שירותי הגנת הסייבר, רישוי, תקינה, עריכת תרגילים ואימונים, מתן תמריצים וכלים נדרשים נוספים.

ד. לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר.

ה. לבצע כל תפקיד אחר שיקבע ראש הממשלה בהתאם לייעוד הרשות.

החלטת ממשלה זו מסכמת עבודת מטה מקיפה, שהצביעה על הצורך בגוף אופרטיבי ייעודי שיוביל את פעילות הגנת הסייבר בישראל בהסתכלות ארוכת טווח מול האיומים הגוברים והמתפתחים.
סוכם כי רשות הסייבר הלאומית תפעל לצד המטה הקיברנטי הלאומי, אשר ימשיך בהובלת המדיניות הלאומית, בבניין כוח טכנולוגי פורץ דרך ובחיזוקה של מדינת ישראל כמובילה עולמית בתחום הסייבר. הרשות והמטה יהוו מערך סייבר לאומי אחוד במשרד ראש הממשלה.

<u>יחידת הסייבר המשטרתית</u>

במשטרת ישראל זיהו כי בשנים האחרונות מסתמנת עלייה בפשיעה הטכנולוגית במרחב הסייבר בעולם ובישראל. זירת העבירה הקלאסית משתנה בעקבות הפשיעה הטכנולוגית ומשטרת ישראל נערכה בהתאם לכך.

<u>ייעוד</u>

יחידת הסייבר הארצית הוקמה בלהב 433 במטרה להוביל את המאמץ הלאומי בלחימה בתופעות פשיעה במרחב הקיברנטי. היחידה אמונה על חקירת עבירות מחשב איכותיות ומתוחכמות במיוחד המצריכות מומחיות ואמצעים מתוחכמים, עבירות הנוגעות לתשתיות לאומיות ומוסדות פיננסים, פעילות עבריינית המסתייעת באמצעים מתוחכמים, יצור והפצת נגיף מחשב, סחיטה במרחב הקיברנטי ועוד.

<u>תפקידים</u>

א. ניהול חקירות בתחומי הייעוד של היחידה

ב. טיפול בפשיעת סייבר המלווה בפגיעה כלכלית

ג. טיפול בפגיעת סייבר בתשתיות חיוניות/מוסדות פיננסיים

ד. חשיפת תופעות פשיעה במרחב הקיברנטי לרבות פדופיליה

ה. פעילות יזומה בנוגע לתרחישי איום מקוונים

ו. סיוע ושיתוף פעולה בינלאומי בתחום הסייבר

<u>עקרונות פעולה</u>

הקמת היחידה בלהב 433, כחלק ממארג היחידות הארציות, תוך הקצאת משאבים משמעותיים להצטיידות טכנולוגית, מובילה לקפיצת מדרגה ביכולות המשטרה לטיפול בחקירות בעולם הסייבר. בעוד יחידות הסייבר המחוזיות עוסקות בעיקר במענה תגובתי לחקירות בעולם הסייבר, היחידה הארצית מפנה את עיקר משאביה לחשיפת אותן עברות המשפיעות על בטחון אזרחי ישראל במרחב

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

הקיברנטי. היחידה עתידה להוות את חוד החנית בלחימה בפשיעה המקוונת במדינת ישראל. עקרונות הפעולה במסגרת זו:

חשיפה - על זרוע זו מוטלת המשימה לחשוף תופעות פשיעה ברשת על ידי איסוף מידע מודיעיני וראייתי והעברתו אל זרוע החקירות. בידי הזרוע אמצעים טכנולוגיים מתקדמים ויכולות גבוהות אשר מסייעים בקביעת תמונת המצב של תופעת פשיעה והעברת המידע הנדרש לפתיחה בחקירה.

חקירה – תפקיד זרוע החקירות לגבש את החומר לכלל ראיות משפטיות. אנשי הזרוע הינם חוקרי מחשב מיומנים ובעלי תארים והכשרות רלוונטיים בתחום. תפקיד חוקר הסייבר נחלק ליכולות חוקר מן השורה וליכולות מיצוי ראיות מחומר מחשב.

שיתוף פעולה - היחידה מושתתת על שיתוף פעולה עם גורמים בתעשייה, ארגוני אכיפה בארץ ובעולם, אקדמיה וארגונים לא ממשלתיים ברחבי העולם.

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

נספח ב' – הגדרת המונח 'סייבר'

מתוך המאמר: 'התהוות המדינה במרחב המקוון: השוואה תיאורטית והיסטורית', עמית שיניאק

את המושג "מרחב מקוון" (Cyberspace) הגה וביאר הסופר ויליאם גיבסון במסגרת רומן בדיוני ידוע שפורסם ב 1984 בשם Neuromancer. העובדה שמקורו של המושג הוא בז'אנר הספרות הבדיונית, היא אולי אחת הסיבות לריבוי הפרשנויות למושג זה, ולקושי הקיים בקרב חוקרים, בירוקרטים ומדינאים לפרש אותו כבעל משמעות יישימה ובת השוואה למרחבים "פיזיים" כגון המרחב הימי. ביטוי מרכזי למחלוקת באשר לשאלה האם יש להשוות את המרחב המקוון למרחבים פיזיים, הוא בהבדלים שבין שתי קבוצות של ההגדרות המקובלות למושג ה"מרחב המקוון": <u>ההגדרה הטכנית</u>, שנתגבשה על בסיס הפיתוח הטכנולוגי של האינטרנט בקרב מומחי מחשבים ומשפטנים המתמחים בטכנולוגיה; <u>וההגדרה החברתית מרחבית</u>, שנתגבשה לראשונה על ידי גיבסון ופותחה על ידי שורה של סופרי מדע בדיוני.

גיבסון, שהגה את המושג "מרחב מקוון" בראשית ימי המחשב הביתי והתקשורת מתווכת המחשב, ועוד בטרם פיתוחה של האינטרנט והתבססותם של יישומים כגון "הרשת העולמית הרחבה" (WWW), מבסס את ההגדרה החברתית מרחבית באמצעות תיאור את המרחב המקוון כביטוי גראפי של מטריקס (Matrix) מתמטי, המייצר חוויה סובייקטיבית חזותית ומקיפה, בקרב משתמשי מחשב שונים במדינות שונות. ההתייחסות של גיבסון למרחב המקוון, הוא כתופעה המאתגרת את כל המרכז החושי (Sensorium) של המוח, כפי שעולה מ"ההגדרה הספרותית" למושג "מרחב מקוון".

התייחסות של גיבסון לאינטרנט כאל מרחב (Space), נובעת מהחזון שלו על אודות היקף ההשפעה של רשתות מחשבים על בני האדם המשתמשים בהן, עד לכדי התחושה הקיימת בקרב ציבורים רבים היום של מרחב חדש ושל מציאות מדומה. ההגדרה זו "המרחבית" עושה שימוש במטפורות גיאוגרפיות וחברתיות כדי לתאר את האינטרנט כמרחב המכיל בתוכו את כלל האפשרויות הגלומות באינטראקציה האנושית: רגש, אמונה, יחסי שיתוף פעולה, מלחמה, טרור וכדומה. בעיניו, המשתתפים אינם "מִתקשרים", כפי שמתארים שיחה בטלפון, או "צופים" באופן פאסיבי, כפי שמתארים צפייה בטלוויזיה. מי שעושה שימוש באינטרנט מקיים על פי הגדרה או גישה זו וכפי שרווח בהתייחסות הציבורית בימינו, אינטראקציה דומה לזו שבין בני אדם למרחב פיזי. לכן המשתמש "גולש", "נמצא ב..", "נכנס" או "יוצא" מבחינה מטאפורית מהמרחב המקוון. ההגדרה המרחבית היא זו המאפשרת להשוות את האינטראקציה החברתית במרחב המקוון, מבחינה מדינית וביטחונית למרחבים פיסיים אחרים.

לעומת ההגדרה המרחבית של גיבסון, ההגדרה המקובלת בחלק גדול מהספרות המחקרית, המשפטית מסמכי מדיניות וחקיקה, מתאפיינת בתיאור "טכני" של האינטרנט ומסתמכת על מונחים מקצועיים של מומחי מחשבים, המתמקדים בתיאור ההמצאה הטכנולוגית ולא במשמעויות הגלומות בה.

ההגדרה הטכנית מבצעת הקבלה בין התיאור הטכני של המושג "אינטרנט", כיישום של תקשורת מתווכת מחשב, העושה שימוש בטכנולוגיות מידע ומבחינה מעשית מתקיימת במסגרת רשת המחשבים העולמית הרווחת היום (WWW), מצד אחד, לבין המונח "מרחב מקוון", הנתפס ככינוי או כמטפורה בלבד לאינטראקציה המתקיימת ברשת מחשבים, מצד שני. ההקבלה, מתבססת על דרך הפעולה של תקשורת המתווכת באמצעות מחשב (CMC), המתייחסת בדרך כלל לתקשורת בין "יחידות מארחות" (Hosts). יחידות אלו, מוגדרות כחומרת מחשבים המחוברת לאינטרנט, בעוד שכל נקודת קצה (Node) נספרת כיחידה נוספת בפריסת הרשת. חדשנותה של האינטרנט נובעת מהיותה רשת תקשורת המחברת

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

רשתות מחשב פנימיות (Intranet) שכבר היו קיימות, באמצעות יישום של פיתוח טכנולוגי המאפשר העברת מידע אלקטרוני יעילה ומבוזרת המכונה "מערך מיתוג מנות", המאפשרת יַתִּירוּת לאחר תקיפה ופגיעה חלקית.

בין אלו המפרשים את האינטרנט כהתפתחות טכנולוגית תקשורתית, קיימים אלו הסוברים כי היא אינה יכולה להביא לשינוי משמעותי מעבר להשפעות המוכרות של אמצעי התקשורת המודרניים. הסתירות הקיימות בין חקיקה ותוכניות מדיניות המסתמכות על תפיסה טכנית את האינטרנט, לבין התפיסה הציבורית המרחבית את המרחב המקוון, הן אחת מבעיות היסוד המקשות על קידום מדיניות מקובלת ודינים בינלאומיים אחידים.

לעומת זאת, בשנים האחרונות מעידות הגדרות למרחב המקוון במסמכים רשמיים עדכניים, על הכרה במהותו הטכנית של המרחב המקוון, אך גם על הצורך לפעול למולו כאל מרחב בעל השלכות חברתיות פוליטיות וביטחוניות מורכבות. כך למשל החלטת ממשלת ישראל 3611 על "קידום היכולת הלאומית במרחב הקיברנטי" מאוגוסט 2011 מגדירה את "המרחב הקיברנטי" כ"מתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה".

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

האיחוד האירופי – הליך הרגולציה

שאלת מעמדה של רמו"ט כרשות עצמאית ואפקטיבית להגנת מידע אישי מקבלת בימים אלה משנה דחיפות לאור כניסתה של רפורמה במשטר הפרטיות במידע באיחוד האירופי לשלב האחרון של הליכי חקיקתה. כפי שיפורט להלן, להתפתחות זו השפעה בלתי מבוטלת על יכולתה של רמו"ט להבטיח שישראל תוסיף לעמוד בסטנדרטים בינלאומיים של הגנת פרטיות במידע, במסגרת משאביה הקיימים.

ביום 15.6.2015 הושגה במועצת האיחוד האירופי הסכמה כללית על הנוסח שלה לטיוטת רגולציית הגנת המידע (General Data Protection Regulation), ובכך הוסר המכשול המשמעותי האחרון בדרך להשלמת הכנתה של הרגולציה להצבעה הסופית שעתידה להתקיים לגביה בסוף 2015. עם קבלת הרגולציה החדשה וכניסתה לתוקף, ייכון באיחוד האירופי משטר פרטיות שיהיה מהודק ואחיד בהרבה בהשוואה להיום: בעוד שדירקטיבת הגנת המידע מ-1995 (Directive 95/46/EC) שאותה היא מחליפה, העמידה רק מתווה עקרוני שעל יסודו נחקקו ויושמו בכל מדינה חברה הסדרי פרטיות מקומיים, שביניהם פערים רבים, לרגולציה תהיה תחולה ישירה ומיידית בכל 28 המדינות החברות (ללא אימוץ בחקיקה פנימית), והיא מטילה עליהן חובות מוגברות המותאמות לאתגרים החדשים של עידן המידע.

לישראל עניין מיוחד בהחמרת הדרישות האירופיות, מאחר שהסטנדרט האירופי לא רק נחשב למוביל בתחום הגנת הפרטיות במידע אישי בעולם, אלא שישראל נהנית ממעמד של מדינה שלישית שמקיימת אותו מאז הכיר בה האיחוד האירופי ב-2011 כבעלת "רמת הגנה נאותה" בנושא ("Adequacy"), ובכך התיר להעביר אליה מידע ללא מגבלות ביורוקרטיות. מדובר בסטטוס לא שכיח, שמקנה למשק הישראלי יתרון תחרותי בניהול עסקים בינלאומיים ומיזמים הכרוכים בעיבוד מידע אישי ממוחשב מאירופה; אלא שאת מעמדה זה עלולה המדינה לאבד אם הגנת הפרטיות בה תתחיל לפגר, היות שהרגולציה קובעת כעת במפורש שהנציבות האירופית תהיה מוסמכת לבטל החלטות שקיבלה מכוח הדירקטיבה, בדבר הכרה במדינה שלישית כבעלת "רמת הגנה נאותה".

כדי לשמור על מעמד ישראל בתחום זה באירופה, חשוב לשים לב שמתווה הרגולציה נוקב בעצמאות ובתפקוד האפקטיבי של הרשות הלאומית להגנת מידע אישי (Supervisory Authority) כקריטריוני מפתח בהערכת קיומה של "רמת הגנה נאותה" במדינה שלישית. למעשה, הרגולציה החדשה מקדישה פרק שלם לחיזוק מעמדה של הרשות הלאומית להגנת מידע אישי (Supervisory Authority), ובפרט לדרישה שתובטח לרשות עצמאות מוחלטת בהפעלת סמכויותיה - כולל תקציב שנתי נפרד, מינוי בכירים בידי הפרלמנט או הממשלה וסגל עובדים שממונה על ידיהם והכפוף ישירות לניהולם – וכן לדרישה שיועמדו לרשותה המשאבים האנושיים, הכלכליים והטכניים הנחוצים לביצוע יעיל של סמכויות הרשות, כפי שהורחבו ברגולציה.

רשויות הגנת פרטיות בעולם

באחרונה ניכרת תכונה רבה באירופה ובארגונים בינלאומיים לשיתוף פעולה כלכלי, דוגמת איפא"ק ו-OECD, לקראת השלמת חקיקתה של הרגולציה האירופית וההכרה בצורך להיערך לכך בהתאם ובמועד. כיוון שהרגולציה החדשה סובבת כולה על עקרון ההרמוניזציה - קרי, השלטת סטנדרטים גבוהים ואחידים של הגנת הפרטיות במידע אישי באירופה – נודעת בהסדר החדש חשיבות מיוחדת

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

לרשויות הלאומיות להגנת מידע, שתפקידיהן כוללים אכיפה יעילה ומתואמת, פירוש ועיצוב אחידים של הדין המתפתח, שיתוף פעולה ותיאום שוטף מול רשויות הגנת מידע אחרות. כפי שמדגיש דוח של ה-OECD ממרץ 2015 בכותרת "אמון בכלכלה הדיגיטלית", בעידן המידע הגלובלי יש לסטנדרטים האירופיים החדשים ולשאר מאמצי הסדרה בין-מדינתיים, השפעה עצומה גם על מי שאינם חברים רשמיים באותן מסגרות, אך מעוניינים להמשיך לקיים עם חבריהן קשרי מסחר, תקשורת ועוד.

שורה של מחקרים, פרסומים ודוחות רשמיים הוקדשו בעת האחרונה להערכת מוכנותן של רשויות לאומיות להגנת מידע בעולם ליישום הרפורמה האירופית. מפרסומים אלה עולה קריאה להעניק תקצוב מוגבר לרשויות הלאומיות להגנת מידע, ולהבטיח שאלה יקבלו אמצעים מספיקים לתפקודן התקין.

כך, דוח סוכנות זכויות היסוד של האיחוד האירופי (FRA) קבע שמחסור במשאבים פיננסיים ואנושיים מתאימים מהווה אתגר משמעותי ליעילות שיטת הרשויות הלאומיות, ומעמיד בסכנה את ההגנה על זכויות היסוד של נושאי מידע. מחקר השוואתי אחר שנערך באירופה מצא שלהיעדר משאבים מספיקים יש השפעה שלילית על איכות וכמות עבודתן של רשויות לאומיות להגנת מידע, ובפרט נרשמה יכולת מוגבלת לפקח ולהטיל סנקציות על הפרות פרטיות במידע היכן שלא ניתנה לרשות הקצאה מספקת. בד בבד, ה-IAPP, גוף מחקר עצמאי שמפרסם סקירת רוחב שנתית בנושא, מדווח מאז 2011 על מגמה נמשכת של עלייה במצבת העובדים ובתקציבי רשויות להגנת מידע.

מטבע הדברים, רשויות להגנת מידע בעולם נבדלות זו מזו בגודל, בהיקף הסמכויות ובמבנה הארגוני, ותקציביהן נעים על טווח רחב ומגוון. יש מדינות המקצות לרשות תקציב עצמאי מתקציב המדינה (למשל, איטליה, צרפת, הולנד, אסטוניה) או מתקציב משרד המשפטים (שוודיה, דנמרק, לטביה), באחרות נתמכת הרשות בהכנסות מגביית אגרות וקנסות שמטילה הרשות עצמה (בריטניה, ספרד, לוקסמבורג, מלטה), ויש הנהנות מתוספת תקציב שמזרים אליהן האיחוד האירופי (צ'כיה, הונגריה ועוד). בנוסף, העובדה שמתווה הרגולציה האירופית מחייב כל מדינה חברה לדאוג שתפעל בה רשות "ראשית" להגנת מידע (Lead Supervisory Authority), היא ביטוי לתופעה הנפוצה של מדינות שבהן פועלת יותר מרשות אחת, בין בשל חלוקה פנימית למחוזות פדרליים שלכל אחד רשות משלו (קנדה, בלגיה, גרמניה) ובין בשל אסדרה נפרדת של המגזר הפרטי והפרטי (שוודיה, קפריסין).

מכל אלה עולה שיש קושי לבצע השוואה מהימנה ומושכלת בין רשויות מקבילות בעולם. בד בבד, ברור שכדי שרשות להגנת מידע אישי תוכל לממש את ייעודה, היא זקוקה לכמות בסיסית של עובדים שמתחתיה לא תוכל לעשות כן, לאו דווקא כתלות בגודל המדינה. לדוגמה יש צורך בפעילות נרחבת של הסברה, חינוך והדרכה המחייבת תקנים נפרדים. כמו כן, היקף הפעילות הבינ"ל הוא נגזרת של הפעילות במרחב הגלובלי (ייצוג והשתתפות בוועדות בינלאומיות, שיתופי פעולה בין-מדינתיים ועוד) ולאו דווקא של גודלה היחסי של המדינה. גם פרויקטים מדינתיים רחבי היקף (כגון המאגר הביומטרי ופרויקט המסלקה הפנסיונית) מחייבים כמות מסוימת של עובדים, ולגודל המדינה אין בהכרח השפעה. דברים אלה כוחם יפה גם לעניין התקציב; הרשות נדרשת למינימום מסוים של משאבים תקציביים, כדי למלא את ייעודה, גם ללא תלות בגודל המדינה. לדוג', פעילות של הסברה כללית איכותית, תצריך מינימום מסוים של משאבים, גם אם הקהל, באופן היפותטי הוא מיליון איש או לחילופין 5 מיליון איש. כמובן, שככל שהקהל הרלוונטי גדול יותר, ידרשו משאבים גבוהים יותר כדי להגיע לכולם ובתפוצה רחבה.

בבריטניה, לדוגמה, הרשות להגנת הפרטיות (ICO) העסיקה בשנת 2004 208 עובדים, בשנת 2007 המספר עלה ל– 262 ובשנת 2014 378 עובדים (עלייה של כ–82% במספר העובדים משנת 2004 לשנת 2014 ושל כ – 44% משנת 2007).

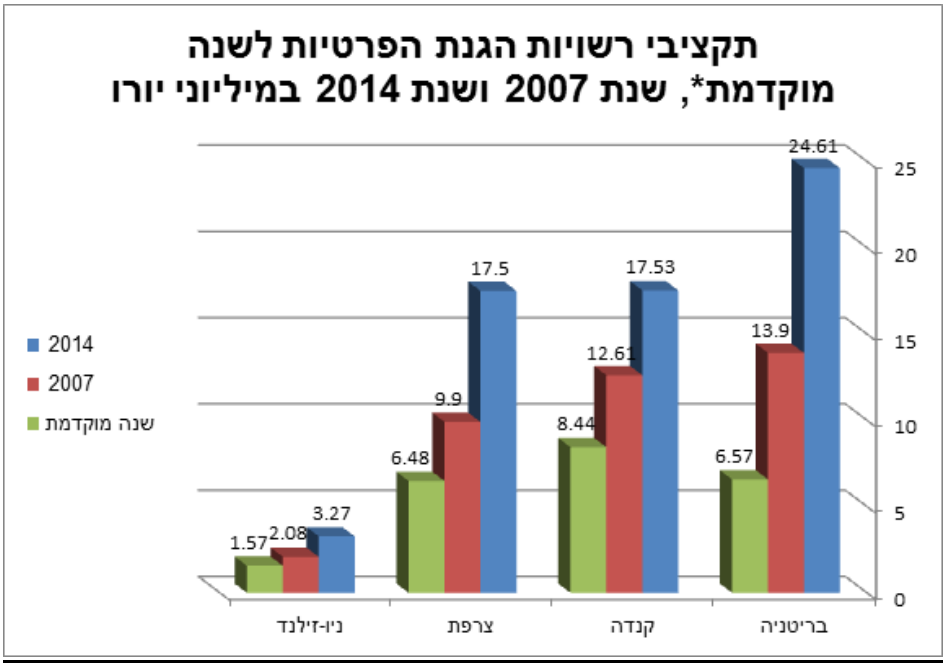
רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

דוגמה נוספת היא קנדה, בה מספר העובדים בשנת 2004 היה 100 עובדים, בשנת 2007 107 עובדים ובשנת 2014 מספר העובדים עמד על 192 (עלייה של כ – 92% במספר העובדים משנת 2004 ושל כ - 79% משנת 2007).

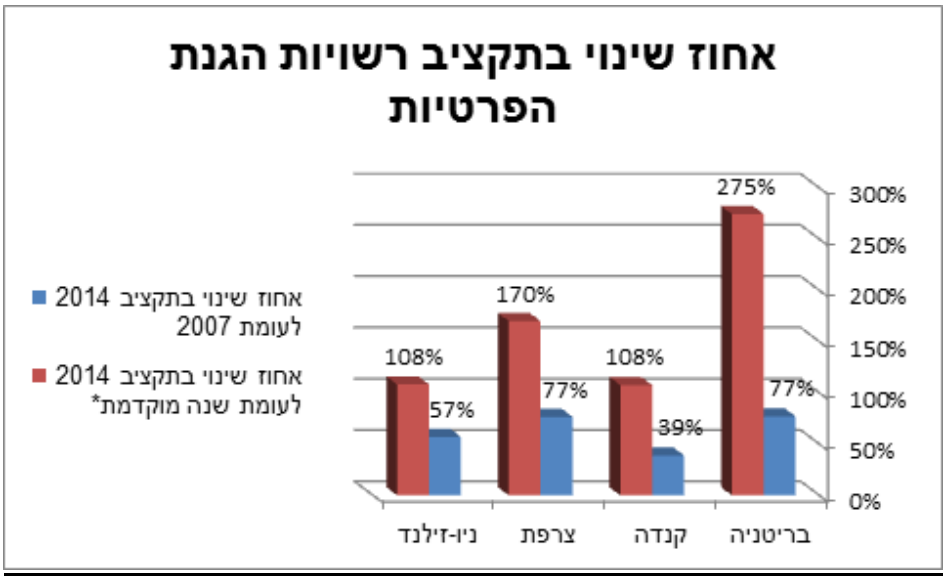
דוגמה שלישית היא צרפת, בה מספר העובדים בשנת 2003 היה 76, בשנת 2007 105 ובשנת 2014 178 (עלייה של כ - 134% משנת 2003 ושל כ – 70% משנת 2007).

במסגרת זו יצוין, כי בישראל מספר התקנים ברמו"ט כיום הוא 28. בשנת 2006 נכתב בעקבות החלטת הממשלה להקמת הרשות, 'מסמך ייזום' המפרט, בין היתר, את תפקידי הרשות ובמסמך זה נקבע כי נדרשים 28 תקנים. היינו, בשנת 2015 מספר התקנים ברשות הוא המספר עליו הומלץ במסמך הייזום, כמעט עשור לפני כן.

להלן שני גרפים לעניין התקציבים של ארבע רשויות הגנת הפרטיות:



רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494



*בריטניה – 2001, קנדה – 2004, צרפת – 2003 וניו זילנד – 2004 (הנתונים המוקדמים ביותר שנמצאו ברשת)

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

מקורות מידע

ראיונות אישיים

- עו"ד אלון בכר, ראש רמו"ט, משרד המשפטים
- עו"ד לימור שמרלינג-מגזניק, מנהלת מחלקת רישוי ופיקוח מנהלי, רמו"ט, משרד המשפטים
- עו"ד מילי בך, מנהלת מחלקת אכיפה וחקירות, רמו"ט, משרד המשפטים
- עו"ד אייל זנדברג, ראש אשכול, מח' חקיקה, ייעוץ וחקיקה, משרד המשפטים
- עו"ד ליאת בן-מאיר שלום, מנהלת תחום הגנת הפרטיות, מח' חקיקה, ייעוץ וחקיקה, משרד המשפטים
- עו"ד צילי נאה, רפרנטית, מח' חקיקה, ייעוץ וחקיקה, משרד המשפטים
- עו"ד ד"ר חיים ויסמונסקי, ראש תחום ידע, חקיקה, משפט וטכנולוגיה, פרקליטות המדינה, משרד המשפטים
- עו"ד יורם הכהן
- אלדד קנטי, סמנכ"ל תכנון, מדיניות ואסטרטגיה, משרד המשפטים
- רו"ח יוני רובין, מנהל אגף א' תקציבים, משרד המשפטים
- עו"ד ד"ר נמרוד קוזלובסקי
- עו"ד עמית אשכנזי, יועמ"ש מטה הסייבר הלאומי, משרד ראש הממשלה
- עו"ד ד"ר שלומית ווגמן, ראשת הרשות לאיסור הלבנת הון, משרד המשפטים
- עו"ד ריבקי דב"ש, ראשת היחידה הממשלתית לחופש המידע, משרד המשפטים
- רס"ן ד"ר עמית שיניאק

מקורות כתובים

- חוק הגנת הפרטיות, תשמ"א – 1981
- החלטת ממשלה מס' 4660 מיום 19/1/2006 – 'הקמת רשות משפטית לטכנולוגיות מידע והגנה על הפרטיות במשרד המשפטים'
- החלטת ממשלה מס' 3611 מיום 7/8/2011 – 'קידום היכולת הלאומית במרחב הקיברנטי'
- החלטת ממשלה מס' 2443 מיום 15/2/2015 – 'קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר'
- החלטת ממשלה מס' 2444 מיום 15/2/2015 – 'קידום ההיערכות הלאומית להגנת הסייבר'
- 'הרשות למשפט, טכנולוגיה ומידע בראי המציאות של 2015', עו"ד אלון בכר, 16/7/2015
- 'מערך התביעה ברשות לטכנולוגיות מידע ולהגנת הפרטיות - נייר עבודת מטה פנימי', משרד המשפטים, ינואר 2006
- 'הרשות המשפטית לטכנולוגיות מידע ולהגנת הפרטיות - מסמך ייזום', משרד המשפטים, 2/5/2006

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494

- מבנה ארגוני ותקני כוח אדם לרשות המשפטית לטכנולוגיות מידע והגנת הפרטיות, נציבות שירות המדינה, 2006
- הרשות למשפט, טכנולוגיה ומידע – הערכת מצב יחידתית לקראת תכנית עבודה 2015, 13/11/2014
- הרשות למשפט, טכנולוגיה ומידע – תכנית עבודה לשנת 2015, 26/2/2015
- 'המענה הלאומי להגנה אזרחית בסייבר: המלצות למקבלי החלטות – נייר עמדה', ד"ר גבי סיבוני
- 'שוברים את הכללים וכולם משחקים – על המפגש בין המרחב הקיברנטי לבין כללי המשפט הבינלאומי', אל"ם עו"ד שרון אפק
- 'התהוות המדינה במרחב הספר המקוון: השוואה תיאורטית והיסטורית', רס"ן ד"ר עמית שיניאק
- 'איך בונים הגנה קיברנטית לאומית', רמי אפרתי
- המטה הקיברנטי הלאומי: ייעוד, רקע, פעילות

רחוב ס'לאח א-דין 29, ת.ד. 49029 ירושלים 91490. טל: 02-6466494