

היבטים בהגנה על הפרטיות במאגרי מידע

תקציר

רקע כללי

הזכות לפרטיות היא זכות יסוד ואחת מזכויות האדם החשובות בישראל. הזכות עוגנה בחוק יסוד: כבוד האדם וחירותו, הקובע כי כל אדם זכאי לפרטיות ולצנעת חייו, ובהסדרים בכמה חוקים אחרים. חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק) קובע את הכללים להגנה על פרטיותו של אדם. בדומה לזכויות יסוד אחרות, הזכות לפרטיות אינה מוחלטת וכשהיא מתנגשת עם זכויות אחרות או עם אינטרסים ציבוריים אחרים, נדרש איזון בין הזכויות.

בעשורים האחרונים הפך המידע למשאב מרכזי ורב ערך, לרבות ערך כלכלי. גם הנורמות החברתיות המשתנות מרגילות את הציבור למסור מידע אישי, וזה נאגר במאגרי מידע, ברשתות החברתיות ובמאגרים ממשלתיים, הכוללים מידע רב ורגיש הנוגע לכל היבטי חייהם של בני האדם. לפיכך, לצד תועלתה העצומה של ההתפתחות הטכנולוגית לאדם ולחברה, עלולה להיפגע הזכות לפרטיות.

על פי חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, הגוף המופקד על אסדרתם של מאגרי מידע הוא רשם מאגרי המידע (להלן גם - הרשם), העומד בראש הרשות להגנת הפרטיות שבמשרד המשפטים (להלן - הרשות). הרשות הוקמה בינואר 2006, בתור "רשות משפטית לטכנולוגיות מידע והגנת הפרטיות" ושמה הנוכחי ניתן לה בספטמבר 2017, תוך העברת הדגש לתפקידה בתחום זה.

במאי 2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע), הקובעות דרישות בתחום אבטחת המידע, וחלות על בעלים, מנהלים ומחזיקים של מאגרי מידע. במאי 2018 נכנסה לתוקפה גם "האסדרה הכללית להגנה על מידע"¹ של האיחוד האירופי.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

פעולות הביקורת

בחדשים מרץ עד אוגוסט 2018 בדק משרד מבקר המדינה היבטים בסוגיית ההגנה על הפרטיות במאגרי מידע בישראל. הבדיקה נעשתה ברשות להגנת הפרטיות, במשרד החינוך ובמשרד הבריאות, ובדיקות השלמה נעשו במחלקת ייעוץ וחקיקה במשרד המשפטים, במערך הסייבר הלאומי וברשות התקשוב הממשלתי במשרד ראש הממשלה, בשתי קופות חולים ובשני בתי חולים ממשלתיים. בעבר עשה מבקר המדינה כמה ביקורות בתחום אבטחת מידע ופרטיות².

הליקויים העיקריים

הרשות להגנת הפרטיות

צוות שהוקם במשרד המשפטים לשם בחינת החקיקה בתחום מאגרי המידע הגיש בינואר 2007 דוח על תיקוני חקיקה נחוצים בתחום זה. אף שמשרד המשפטים החל במהלך השנים בתהליכים ליישום המלצותיו של צוות ההסדרה רובן לא יושמו עד מועד סיום הביקורת.

בפברואר 2018 פורסמה הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח-2018, שמטרתה להרחיב את סמכויות האכיפה של הרשם, לאחר שתהליך חקיקה קודם בנושא שארך כשש שנים לא הסתיים. בשל מחלוקות שלא יושבו בין משרד המשפטים והרשות להגנת הפרטיות ובין מערך הסייבר הלאומי במשרד ראש הממשלה, הצעת החוק לא קודמה. כל עוד לא תוקן החוק, לא קיימת סנקציה יעילה, בין השאר, בגין הפרה של חובת אבטחת המידע, והדבר פוגע ביכולת ההרתעה של הרשות.

על אף החשיבות שהרשות מייחסת למעורבותה בסוגיות הגנת הפרטיות במאגרי מידע העולות במגזר הציבורי, פעילותה בנושא חלקית. הרשות אינה מעורבת בפרויקטים ממשלתיים בנושא בצורה אפקטיבית, ודיונים רבים בכנסת נערכים ללא השתתפות הרשות.

מכלל הגופים הציבוריים, ארבעה בלבד המקבילים מידע דרך קבע מגוף ציבורי אחר, מדווחים לרשם מאגרי המידע כקבוע בחוק, והרשות אינה מבצעת מעקב או אכיפה יזומה על גופים שאינם מעבירים דיווחים כחוק.

2 מבקר המדינה, **דוח שנתי 2013** (2013), "רישום מאגרי מידע בישראל", עמ' 1147 - 1163; מבקר המדינה, **דוח שנתי 2012** (2012), "אבטחת מידע והגנת הפרטיות ברשויות המקומיות", עמ' 1513 - 1537; מבקר המדינה, **דוחות על הביקורת בשלטון המקומי** (2017), "אבטחת מידע והגנת הפרטיות ברשויות מקומיות - מעקב מורחב", עמ' 201 - 245; מבקר המדינה, **דוח שנתי 2018** (2018), "הגנת הפרטיות - אבטחת מידע ואיכותו במאגרי מידע ממשלתיים", עמ' 193 - 196.

הרשות אינה מעודכנת על העברות מידע בין גופים ציבוריים גם בקשר ל"מאגרי על" שהם, על פי הגדרתם, מאגרים בעלי מידע רגיש, שפגיעה בחשאיותם, באמינותם, בשלמותם ובזמינותם עלולה לגרום נזק רב מאוד לציבור ולמדינה בהיבטים מדיניים-ביטחוניים, כלכליים או אזרחיים.

קביעת הנחיות ופרסומן מייעלים את פעולת הרשות ותורמים לאחידות, לעקביות ולשוויון בהפעלת סמכויותיה. על אף החשיבות הרבה שהרשות מייחסת לפרסום הנחיות, בשנים 2008 - 2018 היא פרסמה 15 הנחיות בלבד בתחום הגנת הפרטיות³, ובשנים 2013 - 2016 לא פרסמה הנחיות כלל. גם בנושאים שהרשות זיהתה כי נכון יהיה לפרסם הנחיות לגביהם, בשל חשיבותם והרלבנטיות שלהם לציבור, היא לא עשתה כן לבסוף.

הרשות לא קבעה מדיניות אכיפה סדורה המתחשבת בשיקולים שקבע ראש הרשות, כגון מידת ההשפעה הרוחבית של פעולת האכיפה, אכיפה בנושא הייחודי לרשות, תיעודף הטיפול בגופים חזקים, ועוד.

בעשור האחרון פחתו פעולות האכיפה שהרשות נקטה בהן בהשוואה לתחילתו, ואף שבשלהי העשור חלה עלייה, עדיין מספרן קטן משהיה בשנים 2008 - 2009. זאת, על אף הגידול בהיקפו של שוק המידע האישי בישראל ועל אף שכוח האדם בתחום האכיפה ברשות גדל במשך השנים עד להכפלתו.

הגנה על פרטיות ילדים - משרד החינוך

החקיקה בתחום הגנת הפרטיות אינה תואמת את ההתפתחות הטכנולוגית של העשורים האחרונים, ואף אינה כוללת התייחסות מיוחדת לילדים. גם הניסיונות להסדרתה של ההגנה על פרטיות הילדים בחקיקה או בכללים לא צלחו. עבודת העדכון של חוזר מנכ"ל משרד החינוך בנושא העברת מידע בין מוסדות חינוך הנמשכת לפחות מספטמבר 2013 טרם הושלמה. הוראות החוזר עשויות להיות רלוונטיות לכ-1.7 מיליון תלמידים ויסייעו לבתי הספר למנוע את הפגיעה בפרטיותם של תלמידים במעבריהם בין מוסדות חינוך.

נכון למועד סיום הביקורת אין למשרד החינוך מדיניות אבטחת מידע וסייבר מאושרת.

הרשות הארצית להערכה ומדידה בחינוך פועלת למן הקמתה, מזה 12 שנים, בלי שנחקק חוק המסדיר את פעולתה, תפקידיה וסמכויותיה ובלי שנקבעו בחוק כללים לאיסוף, להחזקה ולשמירה של מידע רגיש ומזוהה, ולהעברתו ממאגריה לגורמים אחרים.

על אף הוראותיו המפורטות של חוזר המנכ"ל ממאי 2015 בעניין מצלמות במוסדות חינוך, הבקרה הנעשית כיום על ידי משרד החינוך אינה בודקת את

מילוי דרישות החוזר ואינה מספקת תמונה מלאה על אופן הטמעתן של הוראותיו.

משרד החינוך אינו עושה בדיקות מקדמיות כנדרש בתקנות אבטחת מידע ובהנחיית הרשם בנושא מיקור חוץ, לפני פרסום מכרזים לשירותי מיקור חוץ, הכוללים גישה למאגרי מידע או קבלת מידע ממאגרי מידע שבבעלות משרד החינוך; ומשהתקבלו הצעות במכרזים, לא נעשית בדיקה אם הספקים עומדים בדרישותיו של נספח אבטחת המידע שצורף למכרז. בהתקשרויות הפטורות ממכרז אין גורם מקצועי במשרד החינוך המנסח דרישת עמידה בחובות וסטנדרטים של אבטחת מידע. בתקופת ההתקשרות עם ספקים משרד החינוך לא עושה בקרה ופיקוח בתחום אבטחת מידע.

למשרד החינוך אין מיפוי של מאגרי המידע שלו או רשימת מצאי של מערכות המידע. הפעילות למיפוי מאגרי המידע נמצאת רק בראשית דרכה כחלק מהסמכה לתקן אבטחת מידע ארגוני ועתידה להסתיים ביוני 2019; במשרד החינוך אף אין רשימה מרוכזת של ספקים שזכו במכרזים, ולמעשה אין למשרד החינוך תמונה מלאה על אותם ספקים המחזיקים במאגרי מידע, ואין דרך ליישם את התקנות וההנחיות השונות הנוגעות לאבטחת המידע.

הגנת הפרטיות במידע רפואי

מידע רפואי הוא מסוגי המידע הרגישים ביותר ושמירה על סודיותו היא תנאי הכרחי לאמון המטופל ברופא. בהתפתחות הטכנולוגית כרוכים סיכונים ייחודיים בתחום ההגנה על המידע ובכלל זה גניבת מידע רפואי, מניעת שירות ושיבוש המידע הקיים, שעשויים להיות להם השלכות קשות על הפרט ועל אמונו של הציבור במוסדות הרפואיים במדינה.

חוזר מנכ"ל משרד הבריאות בנושא אבטחת מידע קובע כי עמידה בתקן לניהול אבטחת מידע במערכות בריאות⁴ הוא תנאי לקבלה ולחידוש רישיון למוסד רפואי ממשרד הבריאות. מכלל כ-1,500 מוסדות רפואיים הטעונים רישיון כ-150 בלבד קיבלו הסמכה לתקן (בעיקר בתי חולים וקופות חולים). שאר המוסדות הטעונים רישיון, ובהם בתי חולים גריאטריים, מרכזים למשתמשים בסמים, מרפאות כירורגיות ומרפאות שיניים, לא קיבלו הסמכה לתקן, ומשרד הבריאות אינו אוכף עליהם חובה זאת.

משרד הבריאות טרם הנחה את המוסדות הרפואיים בנוגע למקרים שיחייבו דיווח על אירועי אבטחת מידע, לצורך בקיום בקרה ואכיפה של הכללים לאבטחת מידע ועוד, הגם שחלפה שנה מהמלצותיה בנושא של ועדה במשרד הבריאות.

4 תקן בין-לאומי (ISO) לאבטחת מערכות מידע בתחום הבריאות שאומץ בישראל. מהווה תקן לווה לתקן אבטחת מידע ISO 27001 וקובע כללים מחמירים יותר לאור רגישות המידע הרפואי.

מערכת המידע המקוונת לשיתוף מידע רפואי, המאפשרת לבתי החולים לצפות במידע הרפואי שמחזיקות קופות חולים על המטופל, פועלת מבלי שהוסדרה בחקיקה ראשית או בחקיקת משנה, בניגוד לעמדתו של משרד המשפטים.

משרד הבריאות טרם קבע כללים ל"התממה" (הסרת מרכיבים מזהים מובהקים ממידע אישי והמרתם בערכים כלליים יותר) ולקידוד של מידע רפואי אישי לצורכי מחקר, לרבות מחקרים בנתוני עתק.

יש סתירה מובנית בין כללי משרד הבריאות, המחייבים התממה מלאה (שאינה מאפשרת כלל שיוך מחדש לנושא המידע) של מידע רפואי המועבר לחוקרים במחקרים רפואיים בנתונים⁵ ללא הסכמתם של נושאי המידע, ובין המידע הנדרש לצורך מחקר, שהוא מידע שניתן לזיהוי חוזר בעת הצורך. בשני בתי החולים שנעשתה בהם הביקורת, החוקרים מקבלים מידע רפואי מזוהה, בניגוד לכללי משרד הבריאות, ובאחד מבתי החולים, גם זים המחקר⁶ רשאי לעיין במידע המזוהה, בניגוד לעמדת משרד הבריאות. גם כשמוסד רפואי מעביר לחוקרים מידע שאינו מזוהה, הדבר נעשה באמצעות קידוד בלבד ולא בהתממה מלאה, כאמור בהנחיות משרד הבריאות.

ככלל, במסגרת בקורתיה על המחקרים במוסדות הרפואיים, המחלקה לניסויים קליניים במשרד הבריאות אינה בודקת אם הועבר מידע רפואי אישי על מטופלים לגורמים שאינם מורשים.

ההמלצות העיקריות

על משרד המשפטים לקיים עבודת מטה בעניין חוק הגנת הפרטיות, לבחון את התיקונים הנדרשים כדיני הגנת הפרטיות, לתעדפם ולקבוע לוחות זמנים לקידומם.

משרד המשפטים, משרד ראש הממשלה ומערך הסייבר הלאומי נדרשים למצוא את האיזונים המתאימים בין הזכות לפרטיות ובין צרכיו של מערך הסייבר בהגנת המידע שיאפשרו את המשך קידומה של הצעת החוק הנוגעת לסמכויות האכיפה של הרשם.

לאור רגישותו של המידע הנצבר אצל גופים ציבוריים, על הרשות להקפיד לדרוש ולקבל דיווחים על העברות המידע הנעשות דרך קבע בין גופים ציבוריים, בפרט בנוגע למאגרי על.

5 מחקר בו נאסף מידע מרשומות רפואיות, סיעודיות, פסיכולוגיות ואחרות ללא אינטראקציה עם המטופלים ובלבד שהמחקר אינו כולל ביצוע בדיקות, הליכים, מתן תרופות וכיו"ב בגופו של המשתתף.

6 אדם, תאגיד, או מוסד האחראים לייזומו, ניהולו ומימונו של הניסוי הרפואי. היום עשוי להיות החוקר עצמו אך במחקרים רבים היום הוא גורם החיצוני למוסד הרפואי.

על הרשות לקבוע מדיניות אכיפה בשים לב ליעדיה ולמפת הסיכונים של הפגיעה בפרטיות.

על משרד המשפטים בשיתוף עם גורמים רלוונטיים בתחום ההגנה על זכויות הילד לשקול הסדרת פרטיותם של ילדים, בחקיקה או בכללים, בהתאמה להתפתחויות הטכנולוגיות.

על משרד החינוך לפעול לאלתר להסדרת פעולתה של הרשות הארצית להערכה ומדידה בחינוך בחקיקה.

משרד החינוך מקדם את פרויקט "הסדרת מערך המידע", במסגרתו יתאפשר קישור בין נתונים מכמה מאגרי מידע קיימים. יש לבחון אם מאגר זה עומד בהגדרת 'מאגר מידע' חדש ו'מאגר על', הטעון רמת הגנה גבוהה יותר, וכן ניהול ורישום מיוחדים. על צוות ההיגוי המנהל את הפרויקט לשקול לערב את הרשות להגנת הפרטיות ואת מחלקת ייעוץ וחקיקה במשרד המשפטים בקידומו, על מנת שיוטמעו בו דרישות יסודיות מתחום אבטחת המידע והגנת הפרטיות.

על משרד החינוך לבחון באופן יסודי את מידת הטמעתן של הוראות חוזר המנכ"ל לעניין מצלמות בבתי ספר ולפעול לבקרת יישומן. כמו כן עליו לאכוף את הוראות החוזר ולקבל מהספק החיצוני דיווחים על בתי הספר הכוללים, בין השאר, נתונים על הצבת מצלמות או על הסרתן, ובהתאם לתמונה שתקבל לשקול פעולות נוספות לאכיפת ההוראות, שיבטיחו את מימוש התכליות המנויות בו.

על הנהלת משרד החינוך להטמיע לפני פרסום מכרזים להתקשרות עם ספקים, שלב מקדמי, הכולל בחינה על פי הדרישות שבתקנות אבטחת מידע ובהנחיית הרשם בנושא מיקור חוץ.

על משרד החינוך לפקח על עמידתם של ספקים בדרישות אבטחת מידע שנכללו בהסכמים עימם נוכח השלכות ופוטנציאל הפגיעה בפרטיות התלמידים, כדי להפחית את הסיכון שאירוע של גילוי מידע רגיש על תלמידים באינטרנט יישנה.

על משרד הבריאות למפות את המוסדות הרפואיים הטעונים רישיון שאינם מחזיקים בהסמכה לתקן לניהול אבטחת מידע במערכות בריאות ולהניעם להשיג את ההסמכה הנדרשת. בהמשך עליו לבחון דרכים להניע גם מרפאות שאינן טעונות רישיון להשיג את ההסמכה לתקן.

על משרד הבריאות לבנות תוכנית לפיקוח ובקרה על אבטחת המידע בכל המוסדות הרפואיים בהתאם לסדרי עדיפויות שיקבע.

על משרד הבריאות ומשרד המשפטים להגיע בהקדם להכרעה על ההסדר הנורמטיבי הנדרש להפעלתה של מערכת שיתוף המידע הרפואי ולפעול ליישומן.

על משרד הבריאות בשיתוף משרד המשפטים לפעול לקביעתם של כללי התממה מתאימים בשים לב לצורכי המחקרים מזה ולחובת ההגנה על

פרטיותם של נושאי המידע מזה. כמו כן עליו לפעול להנחות את ועדות הלסינקי והמוסדות הרפואיים העורכים את הניסויים בנושא ולפקח על יישום הכללים שייקבעו.

על משרד הבריאות לוודא שהמוסדות הרפואיים מבצעים בקרות על מחקרים רפואיים בהתאם לכללים שקבע, לרבות עמידה ברף הבקרה הנדרש; לבחון את דיווחיהם של גופי הבקרה במוסדות; ולוודא כי המוסדות פועלים ליישום הממצאים העולים מהם. עליו לבחון גם דרכים לפיקוח ובקרה על העברת המידע הרפואי במסגרת המחקר לחוקרים וליזמים.

סיכום

הזכות לפרטיות מאפשרת לכל אדם לחיות את חייו ללא התערבות ולממש את רצונותיו והחלטותיו באופן אוטונומי. רשם מאגרי המידע העומד בראש הרשות להגנת הפרטיות הוא הרגולטור המופקד על הגנת המידע האישי במאגרי מידע. דוח זה מציין ליקויים בפעולות הרשות שנמצאו בביקורת, ובכלל זה מעורבות מצומצמת של הרשות בסוגיות הגנת הפרטיות במאגרי מידע העולות במגזר הציבורי והיעדרה של מדיניות אחיפה ברורה.

הביקורת במשרדי הבריאות והחינוך העלתה תמונה מדאיגה, לפיה הם מבצעים פרויקטים מקיפים או פועלים לאיסוף מידע אישי רב מבלי שהוסדרה כראוי המסגרת הנורמטיבית לכך. נוסף על כך נמצאו ליקויים במדיניות אבטחת המידע וביישומה. בניגוד לנדרש בדיון, למשרד החינוך אין תמונה מלאה ומפורטת של מאגרי המידע שלו או של הספקים המחזיקים במאגרי המידע שלו; והוא אינו מפקח על הספקים בהיבטים של אבטחת מידע והגנה על פרטיות. משרד הבריאות אינו מקיים פיקוח מיטבי על אבטחת מידע במוסדות הרפואיים. אין למשרד מיפוי של המוסדות הטעונים רישיון שאינם מחזיקים בתקן לניהול אבטחת מידע במערכות בריאות, ורבים מהם אף אינם מוסמכים לתקן זה. המשרד אינו מקיים פיקוח מיטבי על ההגנה על פרטיות המידע של מטופלים שנעשה בו שימוש במחקרים רפואיים.

תנאי הכרחי לשיפור ההגנה על הפרטיות ולהטמעת הזכות לפרטיות הוא מחויבות ארגונית של המערכת הציבורית בישראל. הדברים באים לידי ביטוי גם בכמה החלטות ממשלה, המבססות את תפיסת השקיפות השלטונית ומחייבות שיקולים של הגנת פרטיות במסגרת יישומן. נוכח הממצאים המובאים בדוח זה, הנהלותיהם של משרדי החינוך והבריאות נדרשות להתגייס להכוונה ברורה של הגורמים האחראים לאבטחת המידע המשרדי, ולנקוט פעולה נמרצת לתיקון הליקויים ולהגנה אפקטיבית על הזכות לפרטיות, כנדרש בדיון.

כבר בתחילת שנות האלפיים הכיר משרד המשפטים בצורך בתיקונים בחוק הגנת הפרטיות ובתקנותיו, אך רובם לא קודמו או לא הושלמו. נראה כי בתחום זה של הגנת הפרטיות יש פער מובנה בין החקיקה, הממושכת

מטבעה, ובין ההתפתחות הטכנולוגית המהירה. פער זה מגביר את הצורך לפעול בנחישות ובמהירות, על מנת לשמור על רלוונטיות של הוראות הדין במציאות המשתנה. על משרד המשפטים לקיים עבודת מטה בעניין חוק הגנת הפרטיות, לבחון את התיקונים הנדרשים בדיני הגנת הפרטיות, לתעדפם ולקבוע לוחות זמנים לקידומם, הן לשם הגנה על זכויותיהם של נושאי המידע בישראל והן לשם שמירת מעמדה של ישראל כמדינה המבטיחה הגנה על מידע אישי ברמה נאותה התואמת את הדין האירופי.

מבוא

מידע רב זורם
מטלפונים סלולריים
חכמים, מיישומונים
(אפליקציות) מבוססי
מקום, ממצלמות
האבטחה במרחב
הציבורי, ממכשירים
חשמליים בבית, ועוד.
במקרים רבים האדם
אינו מודע ל"שובל
המידע הדיגיטלי"
שהוא מותיר אחריו
יום-יום

הזכות לפרטיות היא זכות יסוד ואחת מזכויות האדם החשובות בישראל. הזכות עוגנה בחוק יסוד: כבוד האדם וחירותו, הקובע כי כל אדם זכאי לפרטיות ולצנעת חייו. חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק) קובע את הכללים להגנה על פרטיותו של אדם: "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו", ומפורטים בו 11 מקרים המהווים "פגיעה בפרטיות". כמו כן נקבעו כמה הסדרים בחוקים אחרים המעגנים את הזכות לפרטיות.

שני העקרונות המרכזיים שנקבעו בחוק בקשר לזכות לפרטיות הם עקרון ההסכמה ועקרון צמידות המטרה. לפי עקרון ההסכמה, פגיעה בפרטיותו של אדם תיתכן בהסכמתו (במפורש או מכללא), בידיעתו ובהבנתו את משמעות הפעולה המתבקשת, את הפגיעה הצפויה ואת השלכותיה.⁷ לפי עקרון צמידות המטרה, הנגזר מעקרון ההסכמה, במידע שנמסר למטרה מסוימת מותר להשתמש לשם אותה מטרה בלבד.⁸ בדומה לזכויות יסוד אחרות, הזכות לפרטיות אינה מוחלטת, וכשהיא מתנגשת עם זכויות אחרות או אינטרסים ציבוריים אחרים, נדרש איזון בין הזכויות.⁹

החוקים המעגנים את הזכות לפרטיות מדגימים מהי פגיעה בפרטיות באמצעות איסורים הקבועים בהם אך אינם קובעים הגדרה של הזכות לפרטיות. הפסיקה הישראלית אימצה הגדרה רחבה של המושג פרטיות כ"אינטרס היחיד שלא להיות מוטד בצנעת חייו על ידי אחרים"¹⁰. גם בספרות המחקר המשפטי עמדו על כך שהזכות לפרטיות היא זכות מורכבת הקשורה באופן הדוק להתפתחות הטכנולוגית ולנורמות ודפוסים חברתיים.¹¹

ההתפתחות הטכנולוגית בעשורים האחרונים הביאה עימה שינויים רבים, במסגרתם הפך מידע למשאב מרכזי בחיי הפרט ובחיי הכלל, ולמשאב רב ערך, לרבות ערך כלכלי. לגורמים רבים יש אינטרס באיסוף המידע, בשמירתו ולעיתים אף במכירתו לשם רווח. ישנם יותר אמצעי תקשורת מתוחכמים ומידע רב זורם מטלפונים סלולריים חכמים, מיישומונים (אפליקציות) מבוססי מקום, ממצלמות האבטחה במרחב הציבורי, ממכשירים חשמליים בבית, ועוד. בד בבד, קיימים יותר אמצעים לאיסוף ולעיבוד של מידע באופן יעיל וזול יותר מבעבר.

- 7 ראו בהרחבה: מיכאל בירנהק, **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה**, (2010), עמ' 100.
- 8 יצוין כי שני עקרונות אלו מהווים יסודות לגישה בספרות המחקר לפיה עיקרה של הפרטיות הוא שליטה של האדם בעצמו ובמידע עליו באופן שרק הוא יקבע מה יעלה בגורל המידע על אודותיו ("פרטיות כשליטה").
- 9 כך עולה מהפסיקה, ראו למשל בג"ץ 6650/04 **פלונית נגד בית הדין הרבני האזורי נתניה**, פ"ד סא(1) 581.
- 10 ע"א 1211/96 **כהן נ' נשיונל קונסלטנטס**, פ"ד נב(1) 481; בג"ץ 2481/93 **דיין נ' וילק**, פ"ד מח(2) 456.
- 11 ראו: מיכאל בירנהק, "שליטה והסכמה מדעת: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9 (2007) וכן לעיל, הערה 7.

גם הנורמות החברתיות המשתנות מרגילות את הציבור למסור מידע אישי: הרגלי הצריכה של כל אדם, תחומי העניין, ההקשרים החברתיים, האישיים והמקצועיים; ולעיתים גם מרכיבים רגישים בזהותו, כמו נטייה מינית, אמונה דתית, דעה פוליטית או מצב רפואי. במקרים רבים האדם אינו מודע ל"שובל המידע הדיגיטלי" שהוא מותיר אחריו יום-יום, לאיסוף המידע עליו ולשימוש שנעשה בו - לעובדה שפרטיותו נפגעת הלכה למעשה¹². יתרה מזאת, התייעוד ברשת עשוי להוביל ליצירת פרופיל פסיכולוגי דיגיטלי אשר ילווה אדם לנצח. וכך, לצד תועלתה העצומה של ההתפתחות הטכנולוגית בשירות האדם והחברה, תיתכן גם פגיעה קשה בזכות לפרטיות.

האתגר כיום הוא לעגן את הזכות המהותית לפרטיות בכללים מעשיים. כלומר, לנסח כללים מחייבים במטרה להגן על המידע האישי המפוזר במאגרי מידע שונים, ברשתות החברתיות ובמאגרים ממשלתיים הכוללים מידע רב ורגיש, הנוגע לכל היבטי חייהם של בני אדם; ולא לאפשר פגיעה בפרטיות אלא במקרים המתאימים ובמידה שאינה עולה על הנדרש.

1. בשל פוטנציאל הפגיעה בפרטיות הגלום במאגרי מידע, חוק הגנת הפרטיות מצוין הסדר ספציפי העוסק במאגרי מידע ממוחשבים ובו הגדרות של "מידע"¹³, "מידע רגיש" ו"מאגר מידע". החוק קובע חובות החלות על בעלים, מנהלים ומחזיקים של מאגרי מידע, ובהן חובת רישומם של מאגרי המידע בפנקס המנוהל בידי רשם מאגרי המידע (להלן גם - הרשם), אחריות לאבטחת המידע האגור במאגר המידע, ושמירת סודיותו של המידע והימנעות משימוש בו שלא למטרה שלשמה נמסר. עוד כולל החוק זכויות של נושאי המידע כמו זכותו של אדם לעיין במידע המוחזק עליו במאגר המידע או לדרוש תיקון או מחיקה של מידע זה כאשר אינו נכון, שלם, ברור או מעודכן.

בשנת 1986 הוקמה המועצה הציבורית להגנה על הפרטיות (להלן - המועצה להגנת הפרטיות). על פי החוק היא מגישה לוועדת חוקה, חוק ומשפט של הכנסת, הערות על הדוח השנתי שמכין רשם מאגרי המידע על פעולות האכיפה והפיקוח שלו בשנה הקודמת להגשת הדוח; פועלת כגוף מייעץ לשר המשפטים בנושאי פרטיות; ומביעה עמדתה בהליכי חקיקה הנוגעים להגנת הפרטיות.

2. בינואר 2006 החליטה ממשלת ישראל¹⁴ על הקמת רשות משפטית לטכנולוגיות מידע והגנת הפרטיות במשרד המשפטים. בספטמבר 2017 החליטה הממשלה¹⁵ על שינוי שמה ל"רשות להגנת הפרטיות" שבמשרד המשפטים

12 ראו: **פרטיות בעידן של שינוי**, בעריכת תהילה שוורץ אלטשולר (2012).

13 "מידע" כולל נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

14 החלטת ממשלה מספר 4660 מ-19.1.06. בהחלטת ממשלה מספר 4820 מ-28.6.12 שונה שמה של הרשות ל"רשות למשפט, טכנולוגיה ומידע".

15 החלטת ממשלה מספר 3019 מ-7.9.17.

(להלן גם - הרשות) תוך העברת הדגש לתפקידה בתחום זה¹⁶. בראש הרשות עומד רשם מאגרי המידע, המופקד על אסדרתם של מאגרי מידע על פי חוק הגנת הפרטיות והתקנות שמכוחו. האסדרה נעשית בשלושה אפיקים מרכזיים: אכיפה פלילית ומינהלית, אסדרה משפטית ורישום.

3. במאי 2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע), הקובעות דרישות בתחום אבטחת המידע. התקנות חלות על בעלים, מנהלים ומחזיקים של מאגרי מידע, ומבדילות בין ארבעה סוגי מאגרים, לפי רמת האבטחה הנדרשת בהם.

4. במאי 2018 נכנסה לתוקפה גם "האסדרה הכללית להגנה על מידע"¹⁷ של האיחוד האירופי (General Data Protection Regulation - GDPR) (להלן - הרגולציה האירופית). הרגולציה מתייחסת לאיסוף, שמירה והעברה של נתונים אישיים באיחוד האירופי ומטילה חובות מוגברות על בעלים ומחזיקים של מאגרי מידע, באיחוד ומחוץ לו, ובמקרים מסוימים היא עשויה לחול גם על גופים ישראליים¹⁸. במקרי הפרה, הרגולציה קובעת סעדים וסנקציות, לרבות קנסות עד 20 מיליון יורו.

5. לאור ההתפתחויות הטכנולוגיות הרבות שחלו מאז שנחקק החוק ב-1981 - האינטרנט, הטלפונים הסלולריים, הרשתות החברתיות, כושר האגירה והניתוח של מידע בהיקפים עצומים - עלה הצורך לתקן ולעדכן את הסדרי החקיקה בתחום הגנת הפרטיות במאגרי מידע. אומנם תקנות אבטחת מידע חופפות בחלקן את הדרישות ברגולציה האירופית, אך החקיקה בתחום הגנת הפרטיות במאגרי מידע בישראל עדיין טעונה עדכון והתאמה לרוח הזמן.

16 שינוי שמה של הרשות נבע ממהלך ארגוני שעשתה בשנת 2016, ובמסגרתו נבחנו הכלים הרגולטוריים של הרשות והועלו הצעות לשיפור בתחומי הפעילות של הרשות, בהם גם ההצעה לשנות את שמה ולמקד את פעילותה בתחום זה.

17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

18 הרגולציה האירופית חלה גם על גופים המצויים מחוץ לשטחי האיחוד האירופי, אם מדובר בגוף שיש לו "מוסד" באיחוד ועיבוד המידע האישי מתבצע בקשר לפעילות של אותו מוסד; אם הגוף מציע מוצרים ושירותים המכוונים לאנשים באיחוד או אם הגוף מנטר התנהגות של אנשים באיחוד. ראו בהקשר זה טיוטת הבהרה של ה-GDPR לעניין התחולה הטריטוריאלית של הרגולציה:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

פעולות הביקורת

בחדשים מרץ עד אוגוסט 2018 בדק משרד מבקר המדינה היבטים בסוגיית ההגנה על הפרטיות במאגרי מידע בישראל. הבדיקה נעשתה ברשות להגנת הפרטיות, במשרד החינוך ובמשרד הבריאות. בדיקות השלמה נעשו במחלקת ייעוץ וחקיקה במשרד המשפטים, במערך הסייבר הלאומי וברשות התקשוב הממשלתי במשרד ראש הממשלה, בשתי קופות חולים ובשני בתי חולים ממשלתיים. בעבר עשה מבקר המדינה כמה ביקורות בתחום אבטחת המידע והפרטיות¹⁹.

19 **דוח שנתי 64ג** (2013), "רישום מאגרי מידע בישראל", עמ' 1147-1163 (2014); **דוח שנתי 62** (2012), "אבטחת מידע והגנת הפרטיות ברשויות המקומיות", עמ' 1513-1537; **דוחות על הביקורת בשלטון המקומי** (2017), "אבטחת מידע והגנת הפרטיות ברשויות מקומיות - מעקב מורחב", עמ' 201 - 245; **דוח שנתי 59ב** (2009) "הגנת הפרטיות - אבטחת מידע ואיכותו במאגרי מידע ממשלתיים", עמ' 859 - 878.

הרשות להגנת הפרטיות

חוק הגנת הפרטיות קובע כי הממשלה תמנה לניהולו של פנקס מאגרי המידע רשם בעל כשירות של שופט בית משפט שלום. הרשם הוסמך לרשום מאגר מידע או לסרב לרשמו, למחוק מאגר מן המרשם ולפקח על קיומן של הוראות החוק והתקנות שלפיו, באמצעות יחידת פיקוח שתוקם לצורך זה.

הרשות שהוקמה ב-2006 איחדה שלוש יחידות רגולטוריות שהיו קיימות עד אז: רשם מאגרי המידע לפי החוק, רשם גורמים מאשרים לפי חוק חתימה אלקטרונית, התשס"א-2001, ורשם שירותי נתוני אשראי ושירותי מידע לפי חוק שירותי נתוני אשראי, התשס"ב-2002.²⁰

במסמך הייזום של הרשות מ-2006 (להלן - מסמך הייזום) הוגדרו תפקידיה בקשר להגנת הפרטיות ובכללם: הפעלת מערך של רישום, פיקוח ואכיפה מנהלית מכוח חוק הגנת הפרטיות; יצירת הנחיות ונהלים למשק; סיוע למחלקת ייעוץ וחקיקה במשרד המשפטים (להלן - מחלקת ייעוץ וחקיקה) בליווי משפטי לפרויקטים ממשלתיים; העלאת הצעות לחקיקה וסיוע למחלקת ייעוץ וחקיקה, בליווי הליכי חקיקה ראשית וחקיקת משנה; הדרכה לציבור ומענה על פניותיו.

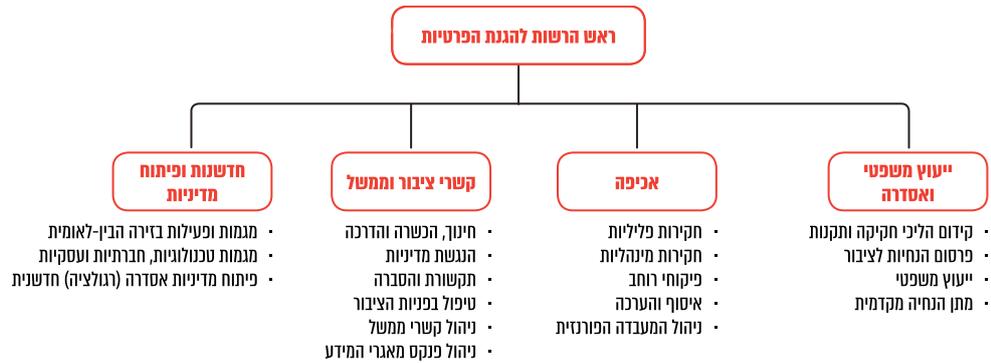
במהלך השנים ולאור ההתפתחויות הטכנולוגיות עודכנו וחדדו תפקידי הרשות ובין השאר הגדירה הרשות כי היא נדרשת להתוות את מדיניות ההגנה על המידע האישי במאגרי מידע דיגיטליים בישראל, לפעול לקידום שליטתו של הפרט במידע אישי עליו, ולהשפיע על תהליכי "עיצוב לפרטיות"²¹ בארגונים ובמערכות מידע בכל מגזרי המשק. לתכלית זו נדרשת הרשות להפעיל גולציה, לרבות אכיפה מינהלית ופלילית, על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים - המחזיקים או המעבדים מידע אישי דיגיטלי. לעבודת הרשות יש גם היבטים בין-לאומיים ולכן היא פועלת גם בזירה הבין-מדינתית, לרבות במישור התאימות לתקנים הבין-לאומיים בתחום.

עד שנת 2017 היו ברשות שלוש מחלקות: מחלקת רישוי ופיקוח, מחלקת חקירות ומחלקת משפטית. בשנת 2016 פתחה הרשות במהלך ארגוני שנועד לבחון את פעולתם של מנגנוני הרשות הקיימים ולזהות את המנגנונים החדשים הנדרשים (להלן - המהלך הארגוני): מופו תחומי הפעולה של הרשות, סוגי מאגרי מידע ומאפייניהם, נבחנו הכלים הרגולטוריים של הרשות והועלו הצעות לשיפור בתחומי פעילותה. בעקבות המהלך שונה המבנה הארגוני של הרשות. נכון לשנת 2018 הרשות מונה כ-40 עובדים. להלן תרשים המתאר את המבנה הארגוני הנוכחי של הרשות ותחומי הפעילות של המחלקות:

20 נושא נתוני אשראי הוסדר מחדש בחוק נתוני אשראי, התשע"ו-2016, שתחילתו באוקטובר 2018. על פי החוק, החל משנת 2019 הפיקוח על הגורמים הפועלים בתחום יבוצע על ידי בנק ישראל.

21 Privacy by design - תכנון פריוקטים בתחום מערכות המידע כבר מהשלב ההתחלתי באופן המביא בחשבון את הגנת המידע האישי ואת הציות לדיני הגנת הפרטיות. על פי עקרון זה יש לבצע הערכה של הסיכונים לפרטיות ולפעול לצמצום הסיכון.

תרשים 1: מבנה ארגוני של הרשות להגנת הפרטיות, מחלקותיה ותחומי פעילותן



המקור: הרשות להגנת הפרטיות.

בשנת 2016 מומשו מתקציבה של הרשות כ-10.7 מיליון ש"ח, בשנת 2017, ולצורך יישום המהלך הארגוני שביצעה, כ-15.9 מיליון ש"ח (גידול של כ-49%) ובשנת 2018 כ-17.9 מיליון ש"ח (גידול של כ-67% לעומת 2016 ושל כ-13% לעומת 2017).²²

הסדרת הגנת הפרטיות במאגרי מידע

בתחילת שנות האלפיים הגיע משרד המשפטים למסקנה כי בנושא הגנת הפרטיות במאגרי מידע אין להסתפק בתיקוני חקיקה נקודתיים ויש מקום לבחון מחדש את ההסדר החוקי, לאור השינויים מרחיקי הלכת והתפתחות הטכנולוגיה מעת חקיקת החוק בשנת 1981. בשנת 2006 מונה צוות בראשות המשנה ליועץ המשפטי לממשלה (חקיקה) דאז (להלן - צוות ההסדרה או הצוות), והוא התבקש "לבחון ולהמליץ למשרד המשפטים על הסדרת החקיקה בנושא מאגרי מידע (Data Protection) - בחינת ההסדר הרצוי, הגדרת תחולת ההסדר ואמצעי האכיפה"²³.

בינואר 2007 הגיש הצוות לשרת המשפטים דאז את המלצותיו לתיקונים שונים בפרק ב' לחוק הגנת הפרטיות, העוסק בהגנת הפרטיות במאגרי מידע.

בהערותיה על דוח רשם מאגרי מידע לשנת 2007, שהוגשו לכנסת באפריל 2008, ציינה המועצה להגנת הפרטיות כי המלצות צוות ההסדרה מצויות יותר

22 בעבר גבתה הרשות אגרות רישום מאגרי מידע ואגרות תקופתיות מכוח תקנות הגנת הפרטיות (אגרות) תשס"א-2000. ההכנסה הממוצעת של הרשות מאגרות בשנים 2014 - 2016 עמדה על כ-2.57 מיליון ש"ח לשנה. בחלוף השנים ובשל העובדה שהרשות סברה כי אין מקום עוד לגבות אגרות אלה היא פעלה לבטלן והן בוטלו ב-9.8.17.

23 הצוות לבחינת החקיקה בתחום מאגרי המידע, דין וחשבון, ינואר 2007. לפירוט אודות הרקע להקמת הצוות ראו בעמ' 5 לדוח הצוות.



בשנת 2006 מונה צוות
בראשות המשנה
ליועץ המשפטי
לממשלה דאז במטרה
לבחון את הסדרת
החקיקה בנושא
מאגרי מידע ולהמליץ
למשרד המשפטים
על דרכי פעולה
בנושא. אף שמשרד
המשפטים החל
במהלך השנים
בתהליכים ליישום
המלצותיו של צוות
ההסדרה, רובן לא
ישמו עד מועד סיום
הביקורת

משנה בידי משרד המשפטים, בהכנת תזכיר חוק, והיא מבקשת לזרז את התיקונים בחוק הגנת הפרטיות בעקבותיהן.

אף שמשרד המשפטים החל במהלך השנים בתהליכים ליישום המלצותיו של צוות ההסדרה, רובן לא יושמו עד מועד סיום הביקורת. במהלך השנים הביעו גורמים במשרד המשפטים וברשות להגנת הפרטיות את עמדתם כי שינוי חקיקה מקיף בכל דיני הגנת הפרטיות אינו ניתן ליישום בטווח זמן סביר ויש להנהיג את התיקונים "פרקים פרקים". עם זאת, גם גישה זו צלחה באופן חלקי בלבד ונמשכה שנים רבות. להלן הפרטים.

הסדרת סמכויות האכיפה של הרשם

1. החוק קובע סנקציות פליליות בגין הפרת כמה מהוראותיו²⁴. בנוסף, הרשם רשאי לבטל רישומו של מאגר מידע שמחזיקו או בעליו הפרו את הוראות החוק והתקנות, או להתלות את תוקף הרישום. לצורך פיקוח על מילוי הוראות החוק הוסמכו מפקחי הרשות לדרוש ידיעות ומסמכים, להיכנס למקום שמופעל בו מאגר מידע, לערוך בו חיפוש ולתפוס חפצים.

בתקנות העבירות המנהליות (קנס מינהלי-הגנת הפרטיות), התשס"ד-2004, נקבעו כמה הפרות של חוק הגנת הפרטיות כעבירות שאפשר להטיל בגין קנס מינהלי עד גובה של 25,000 ש"ח. מובן כי בסכומים אלה אין כדי להרתיע גופים גדולים השולטים במידע רב של הציבור. הרשם עושה שימוש מועט בכלי זה (ראו להלן בפרק על פיקוח ואכיפה), בין השאר משום שהגורם הנקנס רשאי להודיע כי ברצונו להישפט על העבירה ובכך להופכה להליך פלילי²⁵.

2. בשל כלי האכיפה המוגבלים שהיו בידי הרשם, פורסמה בנובמבר 2011 הצעת חוק²⁶, שתעניק לרשם סמכויות אכיפה נרחבות ובהן סמכויות חקירה, חיפוש ועיכוב, וכלים מינהליים יעילים כגון עיצומים כספיים²⁷, התראות ועירבון

24 החוק קובע כי מי שפוגע במזיד בפרטיות זולתו, ובכלל זה, משתמש בדיעה על ענייניו הפרטיים של אדם או מוסר אותה לאחר, שלא למטרה שלשמה נמסרה, דינו מאסר חמש שנים. עוד קובע החוק מספר עבירות שדיןן מאסר שנה ובכלל זה: מי שמנהל, מחזיק או משתמש במאגר מידע בניגוד להוראות החוק; אינו מקיים את הוראות החוק לעניין זכות העיון במידע המוחזק במאגר מידע; אינו מוסר פרטים או מוסר פרטים לא נכונים בהודעה המלווה בקשה לקבלת מידע ועוד.

25 הליך פלילי כרוך בהשקעת משאבים רבה של הגוף החוקר ושל הפרקליטות בהיבטי החקירה, איסוף הראיות וניהול התיק. ראו בהקשר זה הערות המועצה להגנת הפרטיות לדוח רשם מאגרי מידע לשנת 2014, מפברואר 2016.

26 הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב-2011, ה"ח ממסלה התשע"ב 627.

27 עיצום כספי הוא כלי אכיפה מנהלי המעניק סמכות להטיל קנס כספי על מי שמפר את הוראות החוק הרלוונטי. יעילות השימוש בכלי אכיפה זה עשויה לשמש גורם מרתיע כלפי מפרי חוק פוטנציאליים ולהביא להקטנת השכיחות של הפרת החוק. הטלת העיצום הכספי נבדלת מהטלת סנקציה פלילית בכך שהיא אינה גוררת רישום פלילי.



סלע המחלוקת בין
מערך הסייבר ובין
הרשות הוא מימוש
הסמכויות המוצעות
לרשות כך שלא
יפריעו לפעילות
המניעה וההכלה של
אירועים בתחום הגנת
הסייבר. לטענת
מערך הסייבר אין
הצדקה להמשיך
בפיתוח "תקינת
סייבר" עצמאית בידי
מאסדרים אחרים

כהתחייבות להימנע מהפרה. הצעת החוק עברה בקריאה ראשונה אך הליך החקיקה לא הושלם.²⁸

3. ב-2017 החליט משרד המשפטים לקדם מחדש את תיקון החוק המרחיב את סמכויות האכיפה של הרשם. במסגרת הדיונים על טיוטת החוק, התגלעו מחלוקות בין משרד המשפטים והרשות להגנת הפרטיות לבין מערך הסייבר הלאומי במשרד ראש הממשלה²⁹ (להלן - מערך הסייבר). משלא הושגה הסכמה בין-משרדית, הושגה פשרה שאושרה בוועדת השרים לענייני חקיקה³⁰ ולפיה הצעת החוק תונח על שולחן הכנסת, ושרת המשפטים תוסמך להביא לוועדת החוקה חוק ומשפט של הכנסת, תיקונים להצעת החוק בכפוף להסכמות שיושגו בין משרד המשפטים ובין מערך הסייבר. עוד סוכם, כי ככל שלא תהיה הסכמה, הצעת החוק לא תובא לדיון בוועדת הכנסת האמורה. בפברואר 2018 פורסמה הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח-2018³¹, והיא עברה בקריאה ראשונה.

הביקורת העלתה כי המחלוקות בין הצדדים לא יושבו ולכן לא קודם תיקון החוק המרחיב את סמכויות האכיפה של הרשם.

בתשובתו של מערך הסייבר למשרד מבקר המדינה מדצמבר 2018 נכתב, כי מאחר שתחום דיני הפרטיות כולל גם היבטים של אבטחת מידע והגנת סייבר, סלע המחלוקת בינו ובין הרשות הוא מימוש הסמכויות המוצעות לרשות כך שלא יפריעו לפעילות המניעה וההכלה של אירועים בתחום הגנת הסייבר. לטענת מערך הסייבר, ההצעה אינה הולמת את מדיניות הממשלה בתחום הגנת הסייבר, כפי שבאה לידי ביטוי בהחלטת הממשלה בנושא³², ולפיה יש גורם לאומי אחד המנחה בתחום הגנת הסייבר ולפיכך אין הצדקה להמשיך בפיתוח "תקינת סייבר" עצמאית בידי רגולטורים אחרים, לרבות הרשות להגנת הפרטיות.

28 הצעת החוק נדונה בוועדת חוקה, חוק ומשפט של הכנסת בהכנה לקריאה שנייה ושלישית, אך הטיפול בה לא הסתיים עד תום כהונת הכנסת ה-18. הוחל עליה דין רציפות בכנסת ה-19, אך גם בכנסת זאת לא הסתיים הדיון בהצעת החוק. הממשלה שבה והניחה את הצעת החוק, עם שינויים, על שולחן הכנסת ה-20.

29 באוגוסט 2011 החליטה הממשלה על הקמת המטה הקיברנטי הלאומי במשרד ראש הממשלה (להלן - מטה הסייבר), עליו הוטל לקדם היערכות לאומית להגנת הסייבר. בפברואר 2015 החליטה הממשלה להקים את הרשות הלאומית להגנת הסייבר, במטרה לנהל, להפעיל ולבצע את כלל מאמצי ההגנה ברמה הלאומית במרחב הסייבר, להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר ועוד. בדצמבר 2017 החליטה הממשלה לאחד את מטה הסייבר והרשות הלאומית להגנת הסייבר לגוף אחד - מערך הסייבר הלאומי.

30 החלטה מס' חק/2955 מ-21.1.18.

31 ה"ח הממשלה התשע"ח 1206. הצעת החוק דומה להצעת החוק משנת 2011 בשינויים קלים, שעיקרם הוספת פרק שעניינו פיקוח ובירור מינהלי בגופים בטחוניים.

32 החלטת ממשלה 2443 מ-15.2.15.

הרשות אינה מבצעת
אכיפה נגד תאגידים
בין-לאומיים שהם
גורמים מרכזיים
באיסוף מידע אישי
בעולם המודרני,
בעיקר בשל היעדר
כלי אכיפה מתאימים

משרד מבקר המדינה מעיר למשרד המשפטים, למשרד ראש הממשלה ולמערך הסייבר, כי לנוכח הימשכותו של תהליך החקיקה בנושא סמכויות האכיפה זה יותר משבע שנים, ולאור חשיבות הנושא הם נדרשים למצוא את האיזונים המתאימים בין הזכות לפרטיות ובין צרכיו של מערך הסייבר בהגנת המידע, שיאפשרו לקדם את הצעת החוק.

4. דוגמה לחשיבות שבתיקון החוק בנושא סמכויות אכיפה אפשר למצוא בסעיף 17 לחוק, הקובע כי בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע אחראים לאבטחת המידע שבמאגר המידע. הפרת החובה שבסעיף 17 לחוק לא נקבעה כעבירה מינהלית שאפשר להטיל בגינה קנס וגם לא כעבירה שדינה מאסר. אומנם הרשם רשאי להורות על התליית רישומו של המאגר בהפרת הסעיף, אך זו סנקציה שהפעלתה נדירה ביותר והיא אפשרית, מטבע הדברים, רק כלפי מאגרים רשומים, שהם מיעוט המאגרים³³. כמו כן הפרת החובה עשויה להוות עילה לתביעה אזרחית.

לאחר שנים רבות של עיכובים³⁴, פורסמו בשנת 2017 תקנות אבטחת מידע המפרטות את אופן יישומה של חובת אבטחת המידע הקבועה בסעיף 17 לחוק על כל גורם המנהל או מעבד מידע אישי. התקנות קובעות מנגנונים ארגוניים ודרישות לאבטחת המידע ובכלל זה החובה לקבוע נהלי אבטחה, הרשאות גישה, חובת דיווח על אירועי אבטחה ועוד. אך בהיעדר הסמכה מתאימה בחוק, לא נקבעו בהן מנגנוני אכיפה.

יוצא אפוא, כי כל עוד לא תוקן החוק בנושא סמכויות האכיפה, אין סנקציה יעילה בגין הפרתה של חובת אבטחת המידע הקבועה בחוק ובתקנות, והדבר פוגע ביכולת ההרתעה של הרשות.

5. הקנייתם של כלי אכיפה מתאימים לרשות חשובה גם לאכיפת החוק על תאגידים בין-לאומיים שהם גורמים מרכזיים באיסוף ושימוש במידע אישי בעולם המודרני המתאפיין בהיעדר גבולות. גורמים אלה פועלים לאיסוף המידע באמצעות תוכנות מחשב המפעילות אלגוריתמים משוכללים, שבאמצעותם ניתן לאפיין ולייצר "פרופיל" של נושאי המידע, שאפשר לעשות בו שימוש לצרכי שיווק מותאם אישית ולצרכים אחרים.

הפעלת סמכויות חוץ-טריטוריאליות על פי חוק הגנת הפרטיות אינה פשוטה מבחינה משפטית. במענה על פניית הרשות השיבה מחלקת ייעוץ וחקיקה (משפט בין-לאומי) בפברואר 2017, כי קיימות נסיבות המצדיקות הפעלת סמכויות מכוח הדין האזרחי והמינהלי על תאגידים הפועלים מחוץ לישראל

33 לגבי מאגר שאינו רשום, קיימת סנקציה פלילית עקיפה וניתן להאשים את מנהל המאגר או מחזיקו בניהול מאגר מידע ללא רישום.

34 בהתאם לדוח רשם מאגרי מידע לשנת 2009, כבר בינואר 2010 פורסם נוסח תקנות להערות הציבור.

ומנהלים מאגרי מידע על ישראלים, אך יש להיזהר בהטלת סנקציות מינהליות.

בהגדרת המשימות של מחלקת האכיפה לשנת 2019 צוין כי הרשות אינה מבצעת אכיפה נגד תאגידים בין-לאומיים, בעיקר בשל היעדר כלי אכיפה מתאימים³⁵. בהתייחסות ליעדי הרשות לשנת 2019 כתבה המחלקה המשפטית של הרשות, כי על הרשות לחזק את מעמדה כרשות אפקטיבית ועדכנית מול השוק הפרטי ובעיקר מול השוק הגלובלי. גם המועצה להגנת הפרטיות, בהערותיה לדוח השנתי של הרשם לשנת 2016, ציינה כי על הרשות "לשקול להעז יותר, ולפעול להגנת אינטרס הפרטיות של תושבי ישראל בבמות מרכזיות שבהן הוא יכול להיפגע - אל מול חברות בינלאומיות".

היעדר פעילות אכיפה נגד תאגידים בין-לאומיים, שהם השחקנים הגדולים והמרכזיים בתחום מאגרי המידע, מחזק את הצורך במתן כלי אכיפה אפקטיביים יותר בידי הרשות, להגנה על הפרטיות של תושבי ישראל, העשויים להרתיע ולחזק את מעמדה כרשות אפקטיבית וכן לחזק את אפשרותה לשתף פעולה עם רשויות עמיתות בעולם. זאת במסגרת בחינה כוללת של האופן בו הרשות נדרשת להתמודד עם הפרות של חוק הגנת הפרטיות מצד חברות גלובליות לגבי מידע אישי על ישראלים.

צמצום חובת הרישום של מאגרי מידע

חוק הגנת הפרטיות מחייב ברישום מאגרי מידע המקיימים אחד מהקריטריונים הקבועים בו ואוסר את ניהולם והחזקתם אלא אם נרשמו בפנקס מאגרי המידע. על פי החוק, הרשם ירשום את המאגר אלא אם כן המאגר משמש לפעולות בלתי חוקיות או שהמידע הכלול בו נתקבל או נאסף בניגוד להוראות הדין.

תכלית החוק בקביעתה של חובת רישומם של מאגרי המידע הייתה לאפשר לציבור לדעת על קיומו של מידע על אודותיו במאגרי המידע, לאפשר בקרה ופיקוח על המאגרים ובכך לתרום לשמירת פרטיותם של נושאי המידע.

35 כחריג לכך יצוין כי במרץ 2018 הודיעה הרשות כי פתחה בחקירה מנהלית כנגד חברת ענק המפעילה רשת חברתית בעקבות הפרסומים הנוגעים להעברות המידע האישי מהחברה לחברה אחרת, והאפשרות לביצוען של הפרות חוק נוספות במידע אישי של ישראלים. עם זאת וכאמור, גם אם הרשות תטיל קנסות על החברה הרי שמדובר בסכומים נמוכים בגין כל הפרה. כאשר מדובר במספר רב של הפרות הקנסות עשויים להצטבר לכדי סכומים משמעותיים יותר.

במרוצת השנים
התגבשה במשרד
המשפטים וברשות
ההכרה שתועלתו של
עצם הרישום מועטה
ועל כן יש לצמצם את
חובת הרישום

בפועל, על אף פעולות שונות שנקטה הרשות להגדלת מספרם של המאגרים הרשומים, במועד הביקורת היו רשומים כ-16,600 מאגרים בלבד, הגם שהרשות אומדת את מספר המאגרים החייבים רישום במאות אלפים. גם מבקר המדינה העיר בעבר שרוב המאגרים אינם רשומים³⁶.

במרוצת השנים התגבשה במשרד המשפטים וברשות ההכרה שתועלתו של עצם הרישום מועטה ועל כן יש לצמצם את חובת הרישום ולהמירה במנגנון אחר להגנה על פרטיות המידע, כגון חובת ניהול תקין. הכרה זו נבעה בין השאר מכך שההיקף הרחב של חובת הרישום מסיט את הרשות מעיקר עבודתה - ביקורת ופיקוח על המאגרים - ומן העובדה שחלק זניח בלבד של המאגרים נרשם, דבר הגורם לזילות החוק. נוסף על כך התברר, כי יכולתו המעשית של הרשם לברר, בפרק הזמן שקצב החוק, את מאפייני הפעילות של המאגר, את הסיכונים שהפעילות מייצרת ואת אופן ההתמודדות של הארגון עם סיכונים אלה מועטה, ובמקרים רבים אינה האמצעי המאסדר היעיל להגברת הציות לחוק. לפיכך המליץ צוות ההסדרה לצמצם את חובת רישומם של מאגרי המידע למאגרים בעלי רגישות מיוחדת בלבד.

בשנת 2009 הכין משרד המשפטים טיוטה ראשונה של תזכיר חוק המציעה לצמצם במידה רבה את חובת הרישום ולהמירה בכללים להבטחת פרטיות המידע שבמאגרי המידע, ולהמשיך להחיל את חובת הרישום על מאגרים רגישים, כגון מאגרים של גופים ציבוריים ומאגרי מידע שמטרתם איסוף מידע לצורך מסירתו לאחר. התזכיר פורסם, לאחר שהוכנסו בו שינויים, רק באוגוסט 2012³⁷.

נמצא כי בחלוף תשע שנים ממועד כתיבתה של טיוטת תזכיר החוק ושש שנים ממועד פרסומו תיקון החקיקה לא הושלם. הרשם ממשיך בהקצאת משאבים לרישום, שחובתו נקבעה לפני 40 שנה בקירוב, אף שהדעה הרווחת מזה שנים רבות היא שיש לבטלו ולהמירו בכללים המתאימים למציאות בת זמננו. יוצא אפוא, כי חובת הרישום ממומשת בידי שיעור נמוך של חייבי רישום, בעוד רוב בעלי המאגרים מוחזקים כמפירי חוק בלי שנעשות נגדם כל פעולות אכיפה.

בתשובתה למשרד מבקר המדינה מדצמבר 2018 מסרה הרשות להגנת הפרטיות כי במחצית השנייה של שנת 2017 הוקם צוות בהובלת מחלקת ייעוץ וחקיקה ובשיתוף הרשות, לשם היערכות להכנסת תיקונים נקודתיים בחוק הגנת הפרטיות (להלן - הצוות המשותף). הצוות עסק גם בצמצומה של חובת הרישום. עוד כתבה הרשות, כי אין זה נכון לנקוט מדיניות יזומה של אכיפת הרישום על

36 מבקר המדינה, **דוח שנתי 42** (1992), עמ' 496; מבקר המדינה, **דוח שנתי 64** (2013), עמ' 1152.

37 חוק הגנת הפרטיות (תיקון מס'...) (צמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולתיעודם במסמכים), התשע"ב-2012. פורסם באתר קשרי ממשל, 7.8.12.

מאגרים רגישים כדבר העומד בפני עצמו ולא אל מול מכלול החובות על פי החוק ותקנותיו.

משרד מבקר המדינה מעיר למשרד המשפטים, כי עליו לפעול באופן נמרץ לקידומו של תיקון החקיקה בנושא על מנת לאפשר לרשות למקד את משאביה בסוגיות בעלות תרומה יעילה יותר להגברת הצייות להוראות החוק. זאת לצד קידום הצעת החוק בדבר סמכויות האכיפה של הרשם ועל מנת שלא לגרוע מסמכויותיו בטרם יינתנו לו סמכויות מתאימות אחרות. מאחר שחובת הרישום צפויה להמשיך ולחול על גבי מאגרים רגישים, שסכנתם לפרטיות רבה יותר, על הרשות לפעול כבר עתה לאכיפת חובה זאת עליהם, יחד עם אכיפת מכלול החובות על פי החוק ותקנותיו.

תיקונים נוספים בחוק הגנת הפרטיות ובתקנותיו

1. **עיון במידע שבמאגר מידע:** תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-1981 (להלן - תקנות העיון), כוללות הסדרים לעיון של אדם במידע שנאסף עליו המצוי במאגר מידע, תשלום בעד העיון, סירוב לאפשר עיון ועוד. התקנות הותקנו סמוך לחקיקת החוק וכוללות הוראות שאינן בהירות כל צורך, הוראות ארכאיות והוראות שיש לבחון את הצורך בשינוי. חלק מהנושאים הטעונים שינוי עלו עוד בדיוני צוות ההסדרה ובהמלצותיו וחלקם הועלו על ידי הרשות עצמה. בהקשר זה יצוין, כי בינואר 2017 פרסם הרשם הנחיה שכותרתה "תחולת הוראות חוק הגנת הפרטיות על זכות העיון בהקלטות קול, וידאו ומידע דיגיטלי", המנסה לתת לתקנות העיון פרשנות המותאמת למציאות בת זמננו. טרם פרסום ההנחיה הסופית פרסמה הרשות טיוטת הנחיה להערות הציבור. במסגרת ההערות עלו תהיות אם פרשנות זאת אינה מרחיבה מדי, באופן שאינו עולה בקנה אחד עם התקנות הקיימות. כבר בינואר 2010 הציגה הרשות למחלקת ייעוץ וחקיקה את הצורך בעדכון של תקנות העיון, בהיבטים מהותיים ובהיבטים מינהליים.

נמצא כי תקנות העיון לא תוקנו. משרד מבקר המדינה מעיר למשרד המשפטים כי עליו לפעול לקידום תיקון התקנות ולהתאמתן לעידן הנוכחי.

2. צוות ההסדרה דן גם בעניינים אחרים הטעונים הסדרה בחוק הגנת הפרטיות ובין השאר ציין את הצורך בהגדרה חדשה ופשוטה יותר של "מידע" ו"מידע רגיש". עוד המליץ הצוות על תיקון חקיקה שיכליל את חוק הגנת הפרטיות בתוספת השנייה לחוק תובענות ייצוגיות, תשס"ו-2006,

ויאפשר לתבוע בגינו תביעה ייצוגית³⁸. גם בדיוני הצוות המשותף מ-2017 עלו כמה נושאים הטעונים הסדרה ואף נקבעו סדרי עדיפויות לקידום של תיקוני החקיקה הנדרשים ובראשם הגדרות "מידע", "בעל מאגר" ו"מחזיק" וצמצום חובת הרישום.

3. בפניות של ראש הרשות לשרת המשפטים ולמנכ"לית המשרד משנת 2017 הועלה הצורך לחדד ולהוסיף הגדרות בחוק, כגון "שימוש במידע" ו"עיבוד מידע", והבהרת המונחים "בעל מאגר", "מחזיק במאגר" ו"הסכמה מכללא".

עוד סוגיות של הגנת הפרטיות נדונו במשך השנים במשרד המשפטים, כגון פרטיות של נפטר, פרסום פרטים מזהים במסגרת פסקי דין, והזכות להישכח³⁹. עם כניסתה לתוקף של הרגולציה האירופית נתגלו בינה לבין החקיקה הישראלית פערים שיש לתת עליהם את הדעת - מהו "עיבוד מידע", מהי הסכמה לשימוש במידע, וכן כללים לעיבוד מידע, דרישה ל"עיצוב לפרטיות", חובת מינוי ממונה הגנה על הפרטיות בארגונים ועוד.

על משרד המשפטים לבחון את הצורך בביצוע התאמות להמלצות צוות ההסדרה, בשים לב לזמן שחלף. עליו גם להמשיך ולבחון אם יש מקום לתיקונים נוספים בנושאים שהחוק אינו מתייחס אליהם כיום וראוי להסדירם לאור ההתפתחויות הטכנולוגיות המואצות. על הצוות המשותף למצות את הליך הבחינה ולהעביר מסקנותיו למקבלי ההחלטות במשרד, לצורך בחירת הפעולה המתאימה.

בתשובתה למשרד מבקר המדינה מדצמבר 2018 מסרה מחלקת ייעוץ וחקיקה במשרד המשפטים כי התיקונים בהוראות הדין בנושא הגנת הפרטיות נעשים בשים לב לסדרי עדיפויות שנקבעו בשיתוף עם הרשות ולכן קודמו ראשונים נושאי סמכויות האכיפה ותקנות אבטחת המידע. הצוות המשותף בוחן דרכים אפקטיביות לתיקון החקיקה בשים לב לאילוצים העומדים לפניו.

בתשובתה למשרד מבקר המדינה מדצמבר 2018 מסרה המועצה להגנת הפרטיות כי לצד קידום החקיקה בנושא סמכויות אכיפה, היא קוראת להקמת צוות משימה מיוחד במשרד המשפטים, לשם גיבוש טיוטה לחוק הגנת מידע מקיף ומודרני.

האחריות לקידום החקיקה והתקנות בתחום הגנת הפרטיות

במדריך הפנימי לעבודת מחלקת ייעוץ וחקיקה, שפורסם בנובמבר 2017, נקבעה חלוקת האחריות בינה ובין יחידות אחרות במשרד המשפטים לקידום

38 אפשרות שלא קיימת היום, למעט במקום בו קיימים יחסי עוסק-צרכן המערבים הפרה של דיני הגנת הפרטיות.

39 הזכות שמידע הפוגע בפרטיות או בשם הטוב יימחק ממנועי חיפוש אינטרנטיים.

תיקוני החקיקה
והתקנות הנדרשים
בתחום הגנת
הפרטיות חשובים לא
רק לפרטיותם של
תושבי ישראל אלא
גם ביחס לגופים
וחברות ישראליים
המקיימים קשרים עם
מדינות האיחוד
האירופי או אוספים
ומעבדים מידע על
תושבי מדינות האיחוד

חקיקה ותקנות שבסמכות שרת המשפטים. בעניין חוק הגנת הפרטיות ותקנותיו נקבע כי החוק כולל נושאים תשתיתיים⁴⁰ מהותיים וייחודיים שמטבעם הם באחריותה של מחלקת ייעוץ וחקיקה ונושאים שאינם תשתיתיים ומטבעם באחריותה של הרשות להגנת הפרטיות (במדריך החוק מוגדר על כן כ"חוק מעורב"). לפיכך נקבע במדריך, כי יש להבחין בין חלקים או נושאים תשתיתיים שהאחריות לקידומם תחול על מחלקת ייעוץ וחקיקה ובין חלקים או נושאים שאינם תשתיתיים והאחריות להם תחול על הרשות.

עד מועד סיום הביקורת לא נעשתה הבחנה כאמור. מחלקת ייעוץ וחקיקה נדרשת לפעול לחלוקת העבודה בינה ובין הרשות, לצורך קידומם של הנושאים שבאחריותן.

נציגת מחלקת ייעוץ וחקיקה מסרה לנציגי משרד מבקר המדינה באוגוסט 2018 כי המחלקה מתעתדת לנסח מסמך עקרונות לחלוקת העבודה בין הגופים.

שמירת מעמדה של ישראל כמדינה בעלת מדיניות נאותה להגנה על הפרטיות

תיקוני החקיקה והתקנות הנדרשים בתחום הגנת הפרטיות חשובים לא רק לפרטיותם של תושבי ישראל אלא גם ביחס לגופים וחברות ישראליים המקיימים קשרים עם מדינות האיחוד האירופי או אוספים ומעבדים מידע על תושבי האיחוד.

משנת 2011 ישראל היא אחת מ-12 מדינות שהוכרו בידי האיחוד האירופי כמבטיחות הגנה נאותה על מידע אישי, ברמה התואמת את הדין האירופי (Adequate Protection) (להלן גם - החלטת ההלימה), ולכן מסוגלת להבטיח לאירופאים הגנת מידע שוות ערך להגנה שהם מקבלים באיחוד האירופי. משמעות ההכרה היא אפשרותם של חברות וגופים ישראליים להעניק שירותים של עיבוד מידע אישי על אירופאים, ללא המגבלות שחלות על העברת מידע למדינות שליטיות בהיעדרה של הכרה כזאת. החלטת ההלימה משנת 2011 ניתנה, בין השאר, על סמך ההבנה כי המלצות צוות ההסדרה צפויות להיות מיושמות, ובכלל זה תיקון החקיקה בנושא סמכויות אכיפה.

בעקבות פסק דין של בית הדין האירופי לצדק⁴¹ בקשר להעברת מידע על אירופאים לחברות אמריקאיות, בהחלטה נציבות האיחוד האירופי בנובמבר 2015, כי כחלק מיישומו של פסק הדין בכוונתה לקיים הערכות סדירות של החלטות הלימה

40 המדריך מגדיר חוק תשתית כחוק שמתקיים בו לפחות אחד מהמאפיינים האלה: נושא העוסק בהסדרה של תחומי התשתית של המשפט וחוקי היסוד; נושא העוסק באיון מורכב של זכויות אדם; נושא רחבי המשפיע על הציבור הרחב או על כלל משרדי הממשלה; נושא שמעצם טבעו דורש ידע משפטי רב-תחומי.

41 Schrems v. Data Protection Commissioner, Judgement (Summary), Case C-362/14, Court of Justice of the European Union, October 6, 2015.

הפרויקטים
הטכנולוגיים
הממשלתיים תופסים
בשנים האחרונות
תאוצה. כוח האדם
המצוי ברשות אינו
מאפשר מעורבות
בכל הפרויקטים
הרלוונטיים, על אחת
כמה וכמה מעורבות
הולמת ואפקטיבית

קיימות, ולבחון מחדש התאמת הדין במדינות השונות לסטנדרטים האירופיים בהווה ואכיפת הדין בפועל.

ואכן, בינואר 2017 פנו נציגי האיחוד למדינת ישראל בנושא זה, והנושא נידון במחלקת ייעוץ וחקיקה בשיתוף הרשות מול הגורמים הרלוונטיים באיחוד, שביקשו לשמוע על ההתקדמות שחלה בהגנת הפרטיות בישראל בשנים שחלפו מהחלטת ההלימה בשנת 2011.

משרד מבקר המדינה מעיר למשרד המשפטים, כי על מנת לשמור על מעמדה של מדינת ישראל כמדינה המבטיחה הגנה על מידע אישי ברמה העומדת בדרישות הדין האירופי, יש חשיבות רבה לקידום תיקון החוק הנוגע לסמכויות האכיפה של הרשם, בהמשך לתקנות אבטחת מידע שנכנסו לתוקפן. יש לתת את הדעת לכך שהחלטת ההלימה משנת 2011 ניתנה גם על סמך הצפי ליישום המלצותיו של צוות ההסדרה, עניין שעדיין מתקדם בעצלתיים.

ממשקי הפעילות של הרשות עם גופים ציבוריים

כאמור, במסמך היזום של הרשות נכתב כי היא תסייע למחלקת ייעוץ וחקיקה בליווי המשפטי למשרדי הממשלה בהתנהלותם בנושאי הגנת הפרטיות. בסיכומי הפעילות השנתיים של הרשות מצוין כי מתפקידי הרשות להשפיע על תהליכי "עיצוב לפרטיות" בארגונים ובמערכות מידע בכל מגזרי המשק.

בביקורת נמצא כי על אף החשיבות שהרשות מייחסת למעורבותה בסוגיות הגנת הפרטיות במאגרי מידע העולות במגזר הציבורי, פעילותה בנושא חלקית בלבד. להלן הפרטים:

1. הרשות תופסת את עצמה "כמוקד ידע של השירות הציבורי בסוגיות שונות של משפט וטכנולוגיה, הן בפן החקיקתי והן בפן הפרויקטלי". בהקשר זה כתב ראש הרשות: "הפרויקטים הממשלתיים תופסים בשנים האחרונות תאוצה ולמעשה כמעט כל פרויקט טכנולוגי עשוי לכרוך עימו נושאים של פרטיות, שחיוני לבדוק אותם בשלב היזום, ולפיכך מעורבותה של המו"ט [הכוונה לרשות להגנת הפרטיות] בשלב זה היא הכרחית... כח האדם המצוי ביחידה אינו מאפשר מעורבות בכל הפרויקטים הממשלתיים הרלוונטיים, על אחת כמה וכמה, בצורה הולמת ואפקטיבית"⁴². ואכן, הרשות

42 מסמך ראש הרשות "הרשות למשפט טכנולוגיה ומידע בראי המציאות של שנת 2015" מ-30.7.15.

- מסרה כי בעקבות השינוי הארגוני היא צמצמה מאוד ליווי של פרויקטים ממשלתיים (וגם מתן מענה וליווי פרטני לגופים שונים).
2. בהתייחסותה של המחלקה המשפטית של הרשות לאתגרי הרשות בשנים 2018 - 2019 נכתב כי "בשל משאבים מוגבלים אנו נדרשים לתעדף בין הנושאים ובהתאם הנוכחות של הרשות בכנסת מוגבלת ומצטמצמת לגדר נושאים קריטיים בלבד. כפועל יוצא, נערכים דיונים רבים בנושאים משיקים או בעלי השלכות על הזכות לפרטיות, ללא נוכחות נציגי הרשות וללא שמובאת נקודת המבט של הזכות לפרטיות".
3. בפגישת עבודה של הנהלת הרשות ביולי 2017 ציינה המחלקה המשפטית של הרשות כי גם מחלקת ייעוץ וחקיקה מצפה שהרשות תיתן מענה בהיבטים משפטיים טכנולוגיים הקשורים להגנת הפרטיות המתעוררים בקשר לחקיקה ולפעולות שונות של משרדי הממשלה, כגון ייעוץ בסוגיות הקשורות ל"עיצוב לפרטיות". עוד עלה בפגישה האמורה, כי הרשות צריכה לקבל החלטה עקרונית על מידת מעורבותה בפרויקטים של המגזר הציבורי בתחומים אלה. בפגישה בינואר 2018 נדונו פניותיהם של גופי שלטון לרשות בנושאי הגנת הפרטיות והצורך לשמור על הרלוונטיות של הרשות בהקשר זה. ראש הרשות הנחה לקבוע סדרי עדיפויות בקשר לפניות אלה, אך בשל הצמצום שנקטה הרשות בליווי פרויקטים ציבוריים, הדבר לא נעשה.
4. במסגרת המהלך הארגוני של הרשות נערכו ראיונות עם משרדי ממשלה והסתבר כי הם מתקשים בקבלת מענה וייעוץ מהרשות.

משרד מבקר המדינה מעיר לרשות כי יש חשיבות רבה למעורבותה בפרויקטים ממשלתיים בענייני הגנת הפרטיות במאגרי מידע, והנושא אף מצוי בליבת תפקידיה כפי שעולה מעמדתם של נציגי הרשות עצמה.

הרשות השיבה כי היא אכן פועלת להשפיע על תהליכי עיצוב לפרטיות, אך בשל מיעוט כוח האדם יחסית למספר הגופים המפוקחים והמאגרים הקיימים, גיבשה מדיניות מושכלת ולפיה היא משקיעה את משאביה בעיקר באסדרה של נושאים עקרוניים בעלי השפעה רוחבית על כלל מפוקחיה, ואינה מתמקדת בפרויקטים "שוטפים" של גופים ממשלתיים או פרטיים, אינה מלווה אותם ואינה מייעצת להם.

מחלקת ייעוץ וחקיקה השיבה כי היא זו שמסייעת ומנחה לשכות משפטיות של משרדי ממשלה בשאלות של הגנת הפרטיות, במיזמים הנוגעים למאגרי מידע ובהצעות חוק בנושא. הרשות משתלבת בייעוץ כאשר עולה צורך בכך לגבי היבטים שבהם יש לה מומחיות מיוחדת, למשל נושאים המשלבים טכנולוגיה ומשפט או נושאים הנוגעים ישירות לסמכויות הסטטוטוריות של הרשם.

הגם שהגורם המכריע מהבחינה המשפטית בנושא הגנת הפרטיות הוא מחלקת ייעוץ וחקיקה, הדבר אינו סותר את הצורך במעורבותה של הרשות להגנת הפרטיות בפרויקטים הקשורים להגנת הפרטיות במאגרי מידע. על הרשות לבחון דרכים למתן משקל ראוי לנושא זה, שכן ככלל, פרויקטים של משרדי הממשלה שכרוכה בהם הגנת פרטיות במאגרי מידע הם רלוונטיים לציבור כולו.

העברת מידע בין גופים ציבוריים

גופים ציבוריים (משרדי ממשלה, מוסדות מדינה, תאגידים סטטוטוריים, רשויות מקומיות וכיוצא באלה) מחזיקים מטבעם מידע בהיקף עצום על אזרחי המדינה, לצורכי פעולתם. על פי החוק, מסירת מידע מידי גוף ציבורי אסורה, אלא אם כן המידע פורסם או הועמד לעיון הרבים לפי סמכות כדין או שהאדם נושא המידע נתן הסכמתו למסירת המידע. על אף הוראה זו, מותרת קבלת מידע ומסירת מידע בין גופים ציבוריים בתנאים המנויים בחוק, שעיקרם כי המסירה לא נאסרה בחיקוק וכי היא דרושה במסגרת הסמכויות או התפקידים של מוסר המידע או של מקבלו. עוד נקבע בחוק, כי גוף ציבורי המקבל דרך קבע מידע מגוף ציבורי אחר והמידע נאגר במאגר מידע, יודיע על כך לרשם.

בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986, נקבע טופס דיווח לרשם מאגרי המידע ובו, בין השאר, תיאור המידע המתקבל. בהתאם לתקנות יש להקים בכל גוף ציבורי ועדה להעברת מידע בין גופים ציבוריים, שתפקידה לבחון בקשות מידע של הגוף הציבורי ובקשות מידע שלו מגופים אחרים, ולקבוע הוראות לעניין ההרשאות וההגבלות בעניין הגישה למאגרי המידע.⁴³

בשנת 2006 ובעקבות פסיקה של בית המשפט העליון⁴⁴ על העברת מידע מגוף ציבורי, ולפיה על רשויות המדינה להגביר את הפיקוח על הרשאות הגישה למאגרי המידע והיקף המידע המועבר, תוקנו התקנות האמורות. גם המשנה ליועץ המשפטי לממשלה (ייעוץ) דאז פרסם הנחיה ליועצים המשפטיים במשרדי הממשלה⁴⁵ על העברת מידע בין גופים ציבוריים ובכלל זה על בחינת הבקשות, על הצורך בקביעתם של כללי גישה למידע המועבר, על תפקידי הוועדה מול הממונה על אבטחת המידע ועל החובה לפרסם את רשימת הגופים שמידע מועבר אליהם דרך קבע.

בשנים 2010 - 2011 בדקה הרשות את עבודת הוועדות להעברת מידע ב-34 גופים ציבוריים ומצאה כשלים בפעולתן ובסדרי עבודתן, באי-פרסום רשימות

43 בעניין זה ראו פרק "טיפול משרד החקלאות בהגנת הפרטיות ובאבטחת מידע", המפורסם בדוח זה.

44 בג"ץ 8070/98 האגודה לזכויות האזרח נ' משרד הפנים ואח', פ"ד נח(4) 842.

45 הנחיה מיום 16.3.06.

של הגופים שמידע מועבר אליהם דרך קבע ובאי מינויו של ממונה אבטחת מידע כקבוע בחוק. בסיכום פיקוח שפרסמה הרשות צוין בין השאר כי אף אחד מהגופים אינו מדווח לרשם על העברת מידע דרך קבע. עוד צוין בסיכום הפיקוח כי בשנת 2013 תפרסם הרשות הנחיה שתבהיר את הנחיית המשנה ליועץ המשפטי לממשלה תוך התייחסות לכמה נושאים שצוינו בדוח הפיקוח וכי תפנה לרשות התקשוב הממשלתי⁴⁶ לצורך פיתוח מערכת להעברת מידע באופן מאובטח. הרשות לא פרסמה הנחיה כאמור.

האגף לביקורת פנים ופניות הציבור במשרד המשפטים ערך בשנת 2015 ביקורת בנושא ועדות להעברת מידע. בביקורת נמצא כי לרשות להגנת הפרטיות אין מידע על העברות מידע קבועות בין משרדי הממשלה, למעט לגבי גוף אחד.

בביקורת נמצא כי מכלל הגופים הציבוריים בישראל, ארבעה בלבד המקבלים מידע דרך קבע מגוף ציבורי אחר מדווחים לרשם מאגרי המידע כקבוע בחוק: הלשכה המרכזית לסטטיסטיקה, משרד הרווחה, משרד החינוך ונציבות שירות המדינה. עוד נמצא כי הרשות להגנת הפרטיות אינה מבצעת מעקב או אכיפה יזומה על גופים שאינם מעבירים דיווחים כחוק. למעשה, משנת 2011 לא פיקחה הרשות על העברות מידע בין גופים ציבוריים.

הרשות השיבה למשרד מבקר המדינה, כי נושא העברת המידע בין גופים ציבוריים לא תועדף במקום גבוה במניין משימותיה ויעדיה, שכן סברה שקיומה של חובה בירוקרטית בעיקרה אינו תורם רבות להגנת הפרטיות במגזר הציבורי. הרשות הוסיפה, כי רשות התקשוב הממשלתי פיתחה מערכת ממוחשבת לניהול הוועדות להעברת מידע בין גופים ציבוריים ובשנת 2018 היא מוטמעת במשרדי הממשלה בהדרגה. הרשות פנתה לרשות התקשוב הממשלתי על מנת ליצור ממשק בינה לבין מערכת זו, כך שהגופים יוכלו לדווח לרשות להגנת הפרטיות באותה מערכת.

המידע הנאגר במאגרי המידע של גופים ציבוריים נאסף מכוח חובה חוקית ולא דווקא מרצונו ובהסכמתו של נושא המידע. לנוכח האמור, ובשל רגישותו של המידע הנצבר בידי גופים ציבוריים, על הרשות להקפיד לדרוש ולקבל דיווחים על העברות המידע הנעשות דרך קבע בין גופים ציבוריים, בהתאם להוראות הדין. השקיפות תאפשר לציבור לעקוב אחר השימוש שעושים הגופים במידע ולוודא שהוא מועבר באופן סביר ומידתי.

בהחלטת ממשלה מספר 2097 מאוקטובר 2014 הוחלט על הקמת צוות לשיפור העברת מידע בין משרדים ויחידות סמך, לשם הקלת הנטל הבירוקרטי ושיפור

46 רשות התקשוב הממשלתי במשרד ראש הממשלה מנחה את אגפי מערכות המידע במשרדי הממשלה וביחידות הסמך, מקדמת את מאמצי ההגנה על תשתיות ומערכות המידע הממשלתיות, פועלת לפיתוח תשתיות, מערכות ושירותים ליעול עבודת הממשלה ולהנגשת מידע ושירותים ממשלתיים לציבור.

השירות הממשלתי לאזרח, תוך איזון אל מול הפגיעה בפרטיות הכרוכה בהעברת המידע. הצוות המליץ⁴⁷, בין השאר, להשאיר את הפיקוח על העברת המידע בין הגופים הציבוריים בידי הוועדות, והן יפעלו על פי לוח זמנים קשיח שיעוגן בתקנות המסדירות את פעולתן, לצד תיקונים אחרים שיבהירו את דרישות אבטחת המידע בתקנות. המלצות הצוות עוגנו בהחלטת ממשלה מספר 1933 מאוגוסט 2016, שנקבע בה עוד, כי התקנות יותקנו בתוך תשעה חודשים לכל היותר.

על אף האמור, ובניגוד להחלטת הממשלה, רק בספטמבר 2017 פורסמה להערות הציבור טיוטת תיקון לתקנות העברת מידע בין גופים ציבוריים, ועד סוף שנת 2018 טרם תוקנו התקנות.

מאגרי-על של גופים ציבוריים

בשנת 2014 החל צוות בין-משרדי⁴⁸ לפעול למיפוי "מאגרי-על" בגופים הציבוריים ולקביעת מדיניות לגביהם. במסגרת המדיניות הוגדר מאגר-על כמאגר הכולל פרטים אישיים מזהים; מורכב משני מיליון רשומות ייחודיות או יותר; והסיכון שבחשיפתו מוערך כבעל פוטנציאל נזק גבוה ברמה לאומית, בהיבטים מדיניים-ביטחוניים, כלכליים או אזרחיים. ביוני 2017 אישר ראש מערך הסייבר את המדיניות וביקש כי רשות הסייבר תבנה את מנגנון האסדרה והיישום מול כלל המשק.

על פי עיקרי המדיניות, מאגרי-על יזוהו על ידי הצהרה של הארגונים עצמם, מיפוי באמצעות גורמי ההנחיה המוסמכים של הרשות הלאומית להגנת הסייבר ובאמצעות הרשות, על פי הדיווחים המועברים לה לפי החוק.

לפיכך, בתוכנית העבודה של הרשות לשנת 2015 נקבע היעד "חיזוק הגנת מידע אישי במאגרי-על באמצעות פיקוח על העברות מידע בין גופים ציבוריים", ואחד ממדדי ההצלחה של היעד הוגדר כקבלת מידע על העברות מידע מ-100 גופים.

בביקורת נמצא, כי גם מהלך זה טרם קודם והרשות להגנת הפרטיות אינה מעודכנת על העברות מידע בין גופים ציבוריים גם בקשר למאגרי-על שהם, על פי הגדרתם, מאגרים בעלי מידע רגיש שפגיעה בחשאיותם, באמינותם, בשלמותם ובזמינותם עלולה לגרום נזק רב מאוד לציבור ולמדינה בהיבטים מדיניים-ביטחוניים, כלכליים או אזרחיים.

47 דוח מסכם - צוות לשיפור העברת מידע בין משרדים ויחידות סמך, יולי 2016.

48 שכלל נציגים ממטה הסייבר, הרשות להגנת הפרטיות (רמ"ט דאז), התקשוב הממשלתי - יה"ב (היחידה להגנת הסייבר בממשלה הפועלת במסגרת רשות התקשוב הממשלתי) וגופי ביטחון.

הנחיותיו של רשם מאגרי המידע

הנחיותיו של רשם מאגרי המידע הן הנחיות מינהליות שהרשם מפרסם ומביע בהן את עמדתו על דרכי הפעלתן של סמכויותיו. ההנחיות משקפות את הפרשנות המשפטית שתשמש את הרשות בעת ולצורך הפעלת הסמכויות המסורות לה בחוק.

קביעת הנחיות מייעלת את פעולת הרשות ופרסומן תורם לאחידות, ליציבות, לעקביות ולשוויון בהפעלת סמכויותיה. הן מאפשרות לאזרחים ולארגונים לצפות ולכלכל את צעדיהם במידה סבירה של ודאות והן מאופיינות בגמישות שאינה קיימת בחוק⁴⁹ אך חשובה מאוד במציאות הדיגיטלית המשתנה, שההתפתחויות בה תכופות, משמעותיות ומקדימות את החוקים והתקנות. משרד המשפטים רואה בהנחיות את אחת השיטות האפקטיביות בהתמודדות עם האתגרים החדשים המתפתחים בתחום ולקידום ואכיפה של הגנת הפרטיות במאגרי מידע.

הצורך והחשיבות שבפרסום הנחיות עולים גם ממסמך היזום של הרשות, מדוח צוות ההסדרה, מהערות המועצה להגנת הפרטיות על הדוחות של רשם מאגרי המידע ומישיבות ההנהלה של הרשות.

בביקורת נמצא כי על אף החשיבות הרבה שהרשות מייחסת לפרסום הנחיות, בשנים 2008 - 2018 היא פרסמה 15 הנחיות⁵⁰ בלבד בתחום הגנת הפרטיות, ובשנים 2013 - 2016 לא פרסמה הנחיות כלל.

הרשות להגנת הפרטיות השיבה כי בשנת 2018 ערכה עבודת מטה לטיוב פרסומיה כך שידורגו באופן המאבחן ביניהם - הנחיות, גילויי דעת, מדריכים וכדו'. בהתאם לכך, ונוסף על ההנחיות פרסמה הרשות בשנת 2018 נייר עמדה בנושא הצבת מצלמות בגני ילדים, גילוי דעת בנושא כתובות דואר אלקטרוני כמידע אישי, מדריכים ליישומן של תקנות אבטחת מידע ומדריך לערים חכמות.

השימוש בהנחיות ככלי להבהרתן של הוראות החוק ולהגברת הציות לחוק נפוץ גם במדינות אחרות. כך למשל, נציבות המידע בבריטניה (Information Commissioner's Office) פרסמה עשרות רבות של הנחיות המפרשות את עמדתה בנושאים כגון איסוף, עיבוד והעברה של נתוני עתק, "התממה" של מידע (הסרת מרכיבים מזהים מובהקים ממידע אישי והמרתם בערכים כלליים יותר), הנחיות פרטיות למפתחי יישומונים (אפליקציות), הנחיות להגנת הפרטיות במקומות עבודה ועוד. גם הרשות להגנת המידע הצרפתית (Commission Nationale de l'Informatique et des Libertés) פרסמה הנחיות המנגישות את החקיקה לציבור ובכלל זה בנושא זכות העיון במידע, מכשירים וכלי רכב "חכמים", חובות מנהליהם של מאגרי מידע, סוגיית ההסכמה ועוד.

49 ראו בהקשר זה עת"ם (מחזי"ת"א) 24867-02-11 אי.די.איי חברה לביטוח נ' משרד המשפטים הרשות למשפט טכנולוגיה ומידע-רשם מאגרי המידע (פורסם במאגר ממוחשב, 5.8.12).
50 שנת 2009 -1, שנת 2010 -1, שנת 2011 -2, שנת 2012 -4, שנת 2017 -3, שנת 2018 -4.

קביעת הנחיות
חשובה מאוד
במציאות הדיגיטלית
המשתנה,
שההתפתחויות בה
תכופות, משמעותיות
ומקדימות את החוקים
והתקנות. בשנים 2008
- 2018 פרסמה
הרשות להגנת
הפרטיות 15 הנחיות
בלבד

בביקורת נמצא, כי אף שהרשות זיהתה כי נכון יהיה לפרסם הנחיות בנושאים מסוימים, בשל חשיבותם והרלוונטיות שלהם לציבור, היא לא עשתה כן לבסוף. בכמה נושאים פורסמו טיוטות של הנחיות, אך הן לא הפכו להנחיות תקפות. להלן דוגמאות.

1. שירותי ענן; הנחיה למפתחי אפליקציות בעניין "עיצוב לפרטיות" - במסגרת סיכום פגישה בנושא "סיכום המהלך הארגוני ובחירת נושאים וסיגמנטים למיקוד" נכתב כי בשנת 2017 יפורסמו הנחיות בנושאים האמורים, אך הדבר לא נעשה.
2. רחפנים - בפגישת עבודה של הנהלת הרשות ביוני 2018 ביקשה המחלקה המשפטית לקדם את ההנחיה בנושא רחפנים המצויה על שולחנו של ראש הרשות, אך עד מועד סיום הביקורת היא לא פורסמה. ככלל, ההנחיה נועדה לחול על שימוש עסקי או שימוש של רשויות המדינה ברחפנים (בכפוף לסייגים ולהבדיל משימוש ביתי), ולקבוע תנאים מוקדמים להסדרת השימוש ברחפן. יצוין כי הרשות מסרה בתשובתה מפברואר 2019, כי בדצמבר 2018 פורסמה טיוטת הנחיה בעניין שימוש ברחפנים להערות הציבור.
3. הרשות להגנת הפרטיות פרסמה ארבע טיוטות של הנחיות וכללים להערות הציבור, שלא הפכו להנחיות תקפות: התנאים לאיסוף מספרי זהות למאגרי מידע והשימוש בהם; אחריות בעל מאגר מידע לקיים אמצעי אבטחה בעת מתן עיון במידע אישי; העברת בעלות במאגרי מידע. בדצמבר 2010 פרסמה הרשות את הטייטה "כללי אתיקה והתנהגות לבעלי מאגרים האוספים מידע על קטינים", וגם היא לא הפכה להנחיה תקפה.

הנחיותיו של רשם מאגרי המידע הן דרך פעולה מינהלית יעילה ומהירה בהתמודדות עם האתגרים החדשים המתפתחים חדשות לבקרים בתחום הגנת הפרטיות במאגרי מידע. הן עשויות גם לשפר את השירות לציבור ולצמצם את פניותיו לרשות. האמור לעיל מעיד על צורך בשיפור פעילות הרשות בתחום זה, בין בפרסום הנחיות ובין בגילויי דעת או מסמכים אחרים, לא כל שכן במציאות שתיקוני החקיקה נמשכים בה שנים ארוכות.

פיקוח ואכיפה

הכלי העיקרי של הרשות להגנה על פרטיות במאגרי מידע הוא פיקוח ואכיפה מינהלית ופלילית מכוח החוק, שהסמיך את הרשם לרשום מאגרי מידע ולפקח עליהם. כאמור, החוק קובע סנקציות פליליות בגין הפרת כמה מהוראותיו. בנוסף, הרשם רשאי לבטל רישומו של מאגר מידע שמחזיקו או בעליו הפרו את הוראות החוק והתקנות, או להתלות את תוקף הרישום. כמו כן, חלק מהפרות חוק הגנת הפרטיות נקבעו כעבירות שאפשר להטיל בגינן קנס מינהלי. פעילות אכיפה עשויה להינקט בין השאר בעקבות תלונה שהוגשה לרשות, בעקבות

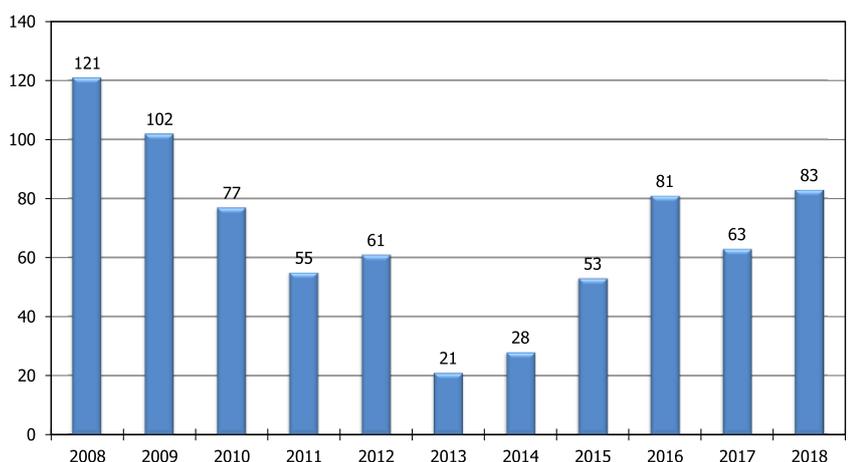
פרסום בכלי התקשורת, עקב מידע שהועבר מרשות אכיפה אחרת, או בעקבות פעילות יזומה של הרשות.

על החשיבות שמשרד המשפטים מייחס לקידום האכיפה בכל תחומי פעילותו אפשר ללמוד מתוכניות העבודה שלו. כך למשל, בתוכניות העבודה לשנים 2015 ו-2016 נקבע כיעד קידום וייעול אכיפה אפקטיבית, ובכלל זה פיתוח כלים חלופיים ומניעתיים למשפט הפלילי.

היקף פעולות האכיפה ברשות ואיכותן

1. להלן בתרשים מספר פעולות האכיפה הפלילית והמינהלית שנפתחו ברשות בשנים 2008 - 2018 בנושא הגנת הפרטיות⁵¹.

תרשים 2: מספר פעולות אכיפה בנושא הגנת הפרטיות שנפתחו ברשות בין השנים 2008 ל-2018



על פי נתוני הרשות.

מהתרשים עולה כי בעשור האחרון פחתו פעולות האכיפה שהרשות נקטה בהן בהשוואה לתחילתו, ואף שבשלהי העשור חלה עלייה, עדיין מספרן קטן משהיה בשנים 2008 - 2009. זאת, על אף הגידול בהיקפו של שוק המידע האישי בישראל ועל אף שכוח האדם ברשות בכלל ובתחום האכיפה בפרט, גדל במשך השנים עד להכפלתו: בשנת 2009 עסקו עשרה עובדים ברישום המאגרים ובאכיפה גם יחד ובשנת 2018 הועסקו במחלקת האכיפה לבדה 19 עובדים.

המועצה להגנת
הפרטיות כתבה כי
האכיפה בנושא הגנת
הפרטיות מצומצמת
מאוד לעומת היקפו
של שוק המידע
האישי בישראל

יצוין כי מכלל 363 פעולות האכיפה שנפתחו משנת 2012 עד 2018, 20 פעולות בלבד (כ-5.5%) הן פעולות אכיפה פלילית ואילו היתר הן פעולות אכיפה מינהלית (קנס מנהלי, קביעת הפרה והנחיות לתיקון ליקויים).

במסגרת הערותיה על הדוח השנתי של רשם מאגרי המידע לשנת 2014, תוך התייחסות לקיפאון החקיקתי בתחום האכיפה ולמגבלות כוח האדם של הרשות, כתבה המועצה להגנת הפרטיות כי האכיפה בנושא הגנת הפרטיות מצומצמת מאוד לעומת היקפו של שוק המידע האישי בישראל. גם בישיבת הנהלה מורחבת מדצמבר 2015 ציינה נציגתה של מחלקת רישוי ופיקוח ברשות כי "תמונת האכיפה של רמו"ט [הכונה לרשות להגנת הפרטיות] צריכה להשתפר משמעותית. צריך להוכיח עשייה".

2. במקרים בהם אין לרשות סנקציה יעילה, כגון במקרה של דלף מידע⁵², אין לרשם אפשרות מעשית לפעול והוא מודיע לבעל המאגר כי הוא פועל שלא כדין (קביעת הפרה)⁵³. קביעת ההפרה מפורסמת גם באתר הרשות ועשויה לפגוע במוניטין של בעל המאגר ולחשוף אותו לתביעות אזרחיות. הרשם גם נותן הנחיות לתיקון ליקויים בעקבות פעולות פיקוח שביצע, אך גם בעניין זה אין בידו סנקציה יעילה לאכיפתו.

נמצא כי לרשות אין נתונים מלאים על תוצרי האכיפה שלה: התיקים שנסגרו, התיקים שהסתיימו בקנס מינהלי, בקביעת הפרה, או במתן הנחיות. בחלק מהשנים נאספו הנתונים באופן ידני והם מופיעים בדוחות השנתיים. גם מתשובת הרשות למשרד מבקר המדינה על ממצאי הביקורת עלו פערים לעומת הנתונים שהועברו במהלך הביקורת. משרד מבקר המדינה מעיר לרשות, כי איסוף הנתונים האמורים וניתוחם הם כלי ניהולי בסיסי שבכוחו לשמש את הרשות בהערכת האפקטיביות של פעולותיה.

הרשות מסרה בתשובתה כי במהלך 2018 פותח כלי עזר מחשובי המאפשר לייצא את תוצרי האכיפה ממערכת המידע של הרשות, לנתחם ולהפיק דוחות מרוכזים, והכלי מצוי בתהליכי שיפור והטמעה.

להלן בלוח תוצריהן של פעולות האכיפה המינהלית שביצעה הרשות משנת 2010⁵⁴.

52 סעיף 17 לחוק קובע כי בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע, אך החוק אינו נוקט בסנקציה בקשר לסעיף זה.

53 לרשם סמכות להורות על התליית רישומו של המאגר אך השימוש בסנקציה נדיר ביותר ואפשרי רק כלפי מאגרים רשומים בלבד. לגבי מאגר שאינו רשום קיימת סנקציה פלילית עקיפה וניתן להאשימו בניהול מאגר מידע ללא רישום.

54 בשנת 2009 הוסמכה הרשות להטיל קנסות מינהליים.

לוח מס' 1: תוצרי אכיפה מינהלית ברשות בשנים 2010 – 2017⁽¹⁾

2017	2016	2015	2014	2013	2012	2011	2010	
8 ⁽⁵⁾	1	1	1	אין נתונים	אין נתונים	5 ⁽³⁾	13 ⁽²⁾	קנס מנהלי
16	10	4	2	אין נתונים	אין נתונים	אין נתונים	אין נתונים	קביעת הפרה
57	16	18 ⁽⁴⁾	21	אין נתונים	אין נתונים	אין נתונים	אין נתונים	הנחיה לתיקון ליקויים

המקור: דוחות שנתיים של רשם מאגרי המידע ונתוני הרשות.

(1) אם ידוע כי בתיק מסוים נעשו כמה פעולות אכיפה, נרשמה הפעולה המשמעותית מהן. למשל, הנחיות לתיקון ליקויים עשויות להינתן בנפרד או נוסף על סנקציות אחרות.

(2) נגד 12 גופים.

(3) נגד 4 גופים.

(4) מתוכם תיק אחד הוגדר כ"מעקב ובקרה".

(5) נתון זה מתייחס לקנס מנהלי או התליית רישיון המאגר.

אשר לתוצריה של אכיפה פלילית, הרשות מסרה כי משנת 2009 ניהלה 5514 חקירות פליליות: שש הסתיימו בהגשת כתב אישום, שתיים מצויות בתהליך להגשת כתב אישום, בארבע ניתנה המלצה לגניזה (מחוסר אשמה ומחוסר ראיות) ושתי חקירות נסגרו משום שהטיפול בהן הועבר לגורמים אחרים.

פעילות האכיפה היא בליבת עשייתה של הרשות להגנת הפרטיות לצורך שמירה על פרטיות הציבור. בעולם הטכנולוגי המתפתח, ובו גופי ענק האוספים ומעבדים מידע על בני אדם, יש צורך באכיפה משמעותית ואפקטיבית לצורך הרתעה וחיזוק מעמדה של הרשות. הנתונים שהובאו לעיל מעידים על הצורך בשיפור של ממש בפעילות האכיפה של הרשות ובתוצריה.

הרשות השיבה, כי אכן נדרשת אכיפה מוגברת והיא פועלת לשיפור היקפה של פעילות האכיפה ותוצריה, בשים לב לכוח האדם המוגבל שברשותה. עוד מסרה הרשות בתשובתה כי בשנים הראשונות להקמתה התבססו רוב תיקי האכיפה על תלונות שהגיעו לרשם, תיקי האכיפה נפתחו ללא סינון וחלק נכבד מהתיקים היו תיקים פשוטים שהטיפול בהם לא היה ארוך. בשנים 2011 - 2012 הרשות החלה לבחור תיקי אכיפה משמעותיים יותר ובעלי השפעה רחבה יותר. ב-2016 הוקמה מחלקת האכיפה המאוחדת, הנושא חודד אף יותר, והעבודה נעשת בהנחה שהיקף התיקים אינו מעיד בהכרח על איכות הטיפול. כן מסרה הרשות כי לשיטתה, למספר תיקי האכיפה שנפתחו בשנים 2017 - 2018 יש לצרף את תיקי הפיקוח הרוחבי (יחידת פיקוח ברשות המסתייעת במיקור חוץ של משרדי רו"ח) משנים אלה.

55 נתון זה אינו מתיישב במלואו עם נתוני הדוח הממוחשב שהעבירה הרשות לפיו בשנים 2012 - 2018 נפתחו 20 פעולות אכיפה פליליות.

פעילות האכיפה היא בליבת עשייתה של הרשות להגנת הפרטיות. בעולם הטכנולוגי המתפתח, ובו גופי ענק האוספים מידע על בני אדם ומעבדים אותו, יש צורך באכיפה משמעותית ואפקטיבית לצורך הרתעה וחיזוק מעמדה של הרשות

משרד מבקר המדינה מעיר לרשות, כי הדוחות השנתיים שלה לשנים 2007 - 2010 מלמדים כי גם בשנים אלה טיפלה בתיקים רבים בעלי משמעות. מעבר לכך, גם אם חל שינוי באופי התיקים, הפער במספר התיקים שנפתחו במהלך העשור אינו מוסבר, מה גם שבשנים הראשונות היו ברשות כולה 18 עובדים בלבד ובשנים האחרונות היה מספר עובדים דומה במחלקת האכיפה לבדה. אשר לתיקי הפיקוח הרחובי, יש להבחין בין אכיפה מינהלית ופוליטית ובין פיקוח רחוב, הבחנה שהרשות עצמה עושה בדוחות השנתיים.

הקמת מערך פיקוח רחובי: על מנת לשפר את האכיפה ברשות ולקבל תמונה רחבה יותר של כשלי השוק בתחום הגנת הפרטיות והנושאים הטעונים הסדרה, הוחלט ליצור הליך פיקוח מהיר ונרחב יותר. לשם כך הוקמה יחידת פיקוח רחוב ברשות המסתייעת במיקור חוץ של משרדי ר"ח בעלי התמחות בתחום מערכות מידע ואבטחת מידע (להלן - מערך פיקוחי רחוב). המערך פועל לאיתור הפרות של חוק הגנת הפרטיות ותקנותיו, להגברת מודעות המשק להוראות החוק, לאיתור כשלים ענפיים הדורשים התערבות והנחיות מיוחדות ולקבלת תמונת מצב מגזרית לגבי עמידה בהוראות החוק. במסגרת זאת נשלחים שאלונים לקבוצה גדולה של גופים המנהלים או מעבדים מידע אישי ובהתאם לתשובות הרשות בוחרת כמה גופים שיעשה בהם פיקוח.

בשנת 2017 הונחה התשתית למערך שהוקם ברשות ונעשה פיילוט לפיקוח רחוב ב-17 חברות ביטוח, לבדיקת עמידתן בהוראות החוק ובהנחיות הרשם. בכמה מן החברות נתגלו ליקויים והרשות מסרה להן הנחיות לתיקונם. בעקבות הפיילוט שלחה הרשות לחברות הביטוח הבהרה בדבר מחיקת מידע היסטורי על לקוחות ועוד. בשנת 2018 הופצו 236 שאלונים ובעקבות ניתוחם הופצו שאלוני המשך למקצת הגופים.

המהלך לפיקוח רחובי חשוב ויש לברך עליו. עם זאת, בהיעדר סנקציות יעילות שהרשות יכולה להטיל, עליה להיערך כראוי כדי שתוכל להמשיך את הטיפול בממצאי הפיקוח הצפויים בכלי האכיפה שבידיה וכדי שהמהלך ישיג את מטרתו.

הגדרתה של מדיניות אכיפה

בתוכנית העבודה של משרד המשפטים לשנים 2017 - 2018 נקבע כיעד משרדי פיתוח ויישום של מדיניות אכיפה בשיתוף פעולה ובסנכרון עם משרדי ממשלה וגופים אחרים.

בישיבת צוות בכיר של הרשות מפברואר 2015, שכותרתה "מדיניות אכיפה ופעילות רשותית סינרגטית", נדונו עקרונות אכיפה וקביעת עדיפות לאכיפה בנושאים ייחודיים לרשות ושלה בלבד יש עניין בהם. בדיון קבע ראש הרשות שיקולים שיש להתחשב בהם בקביעת מדיניות האכיפה, לרבות מידת ההשפעה

הרוחבית של האכיפה, אכיפה בנושא ייחודי לרשות, העדפת הטיפול בגופים חזקים, ומתן קדימות לנושאים רגישים (כגון מידע רפואי). עוד הוחלט כי יגובש מסמך של עקרונות האכיפה.

נמצא כי הרשות לא קבעה מדיניות אכיפה סדורה המתחשבת בשיקולים שקבע ראש הרשות. קביעה זו חשובה במיוחד נוכח כלי האכיפה והיקפי האכיפה המוגבלים של הרשות.

כך למשל בישיבת הרשות מאוגוסט 2018 בנושא הנחיית הרשות על מצלמות מעקב, ציין ראש הרשות כי צריך לכלול את אכיפת ההנחיות בתוכניות העבודה, ולקבוע כי יוקדש לה אחוז מסוים מפעילות האכיפה. בישיבת הנהלה מורחבת מדצמבר 2015 בנושא המהלך הארגוני ברשות, ציינה נציגתה של מחלקת רישוי ופיקוח, כי רצוי לבצע אכיפה לאחר פרסום של הנחיית שוק חדשה.

בביקורת נמצא כי הרשות לא קבעה שתבצע פעולות אכיפה של ההנחיות שהוציאה, וכי האכיפה בעניין זה הייתה אקראית ועל פי רוב נבעה ממידע חיצוני שהגיע לרשות.

הרשות השיבה כי אחת הסיבות להקמתו של מערך פיקוח הרוחב היא בדיקה מגזרית רוחבית יזומה ומקיפה ככל האפשר של יישום הנחיותיו של הרשם בגופים המנהלים מידע אישי בישראל.

הקמת מערך הפיקוח מחזקת את הצורך בקביעת מדיניות אכיפה כדי לכוון את פעילותו בהתאם ליעדי הרשות. על הרשות לקבוע מדיניות אכיפה בשים לב ליעדיה ולמפת הסיכונים של הפגיעה בפרטיות, על מנת שתשקיע את משאביה בתבונה ובדרך המיטבית להשגת תוצאות מרביות בכלים שבדיה.



פרק זה מעלה את הצורך להתאים את החקיקה בתחום הגנת הפרטיות להתפתחות הטכנולוגית המואצת של העשורים האחרונים. כבר בתחילת שנות האלפיים הכיר משרד המשפטים בנחיצותם של תיקונים מסוימים בחוק הגנת הפרטיות ובתקנותיו אך רובם לא קודמו או לא הושלמו. בתחום הגנת הפרטיות יש פער מובנה וקבוע בין תהליכי החקיקה, הממושכים מטבעם, ובין ההתפתחות הטכנולוגית המהירה. פער זה מגביר את הצורך בפעולה מהירה ונחושה לשמירת הרלוונטיות של הוראות הדין במציאות המשתנה. על משרד המשפטים לקיים עבודת מטה בעניין חוק הגנת הפרטיות, לבחון את התיקונים הנדרשים בדיני הגנת הפרטיות, לתעדפם ולקבוע לוחות זמנים לקידומם, הן לשם הגנה על זכויותיהם של נושאי המידע בישראל והן לשם שמירת מעמדה של ישראל באירופה כמדינה בעלת משטר המספק רמה נאותה של הגנה על הפרטיות.

על הרשות להגביר את מעורבותה בסוגיות הגנת הפרטיות במאגרי מידע במגזר הציבורי, לפעול לבניית תוכנית אכיפה סדורה וליישמה, ולפעול לשיפור פעילות האכיפה של הרשות ותוצריה באופן שיגביר את הציות להוראות הדין בנושא.



אחת ההשלכות של שיתוף מידע אישי על ילדים היא העובדה שהוא זורם ברשת, נאסף, נשמר ומעובד לצרכים שונים. המידע עשוי לשמש גופים מסחריים שינצלוהו לשיווק ממוקד של מוצרים, והוא עלול לחשוף ילדים לסכנות כמו פדופיליה, גניבת זהות ובריונות רשת

הגנה על פרטיות ילדים - משרד החינוך

ילדים ובני נוער זקוקים למרחב פרטי ואישי הנתון לשליטתם, לשם פיתוח מיטבי של זהותם ואישיותם. ואולם עם השינויים הטכנולוגיים, ובעקבותיהם הנורמות החברתיות והתגברות לחצי השוק להזרמה חופשית של מידע, מיטשטשים הגבולות בין הפרטי והציבורי. הנגישות היום-יומית של ילדים ובני נוער לאינטרנט, לרשתות החברתיות ולטלפונים חכמים מציפה אותם במידע בכל מקום, כל הזמן. מצד שני, ילדים גם משתפים מידע אישי⁵⁶, בדרך כלל ללא מחשבה יתרה על הדרך שהמידע מוצג בה, על מי שנחשף למידע ועל השלכות ההיחשפות.

אחת ההשלכות של שיתוף מידע אישי על ילדים היא העובדה שהוא זורם ברשת, נאסף, נשמר ומעובד לצרכים שונים. המידע עשוי לשמש גופים מסחריים שינצלוהו לשיווק ממוקד של מוצרים, והוא עלול לחשוף ילדים לסכנות כמו פדופיליה, גניבת זהות ובריונות רשת. מידע אישי על ילדים מופץ בידי ילדים עצמם או בידי הוריהם, אך גם ללא ידיעתם והסכמתם, עקב פרצות אבטחה באתרים או ביישומונים, העלולות להוביל לחשיפה של מידע רגיש ואף חסוי⁵⁷.

משרד החינוך אחראי להקניית ידע לילדים הזכאים לחינוך על פי חוק לימוד חובה, התש"ט-1949, וממונה על מוסדות החינוך ובכלל זה גנים, בתי ספר, מוסדות להשכלה גבוהה ומוסדות חינוך בלתי פורמלי. במסגרת אחריותו, המשרד נדרש לפקח על התנהלותם של מוסדות החינוך גם בנושא הגנת הפרטיות ואבטחת מידע.

בשנים האחרונות, כחלק מתוכנית הלימודים המחייבת בבתי הספר ובמסגרת התוכנית "כישורי חיים"⁵⁸, משרד החינוך מעביר לתלמידים מערך לימודי בנושא "חיים ברשת", הכולל גם תכנים לקידומה של התנהגות מיטיבה, נבונה ובטוחה באינטרנט, פרטיות ברשת ומניעת פגיעה בכל שלבי החינוך. נוסף על כך, ובמסגרת פיתוח אוריינות טכנולוגית ודיגיטלית⁵⁹ בקרב התלמידים, מועברים גם הנושאים אתיקה דיגיטלית ומוגנות ברשת.

56 ראו בעניין זה: **ילדים בישראל**, שנתון 2017, המועצה הלאומית לשלום הילד.

57 מדי פעם בפעם מפורסמים בתקשורת מקרים של דליפת מידע רגיש על ילדים באינטרנט. ראו פרסום על חשיפת שמות ותעודות זהות של תלמידים:

<https://www.calcalist.co.il/internet/articles/0,7340,L-3406501,00.html>

ופרסום על פרצות אבטחה בכמה אתרי ממשלה:

<https://www.globes.co.il/news/article.aspx?did=1001247374>.

58 התוכנית נובעת מן ההכרה כי בית הספר אחראי לא רק לקידום הידע העיוני והמקצועי של התלמידים, אלא גם לפיתוחם הרגשי, החברתי והערכי. התוכנית מתמקדת בהוראת כישורים תוך-אישיים ובין-אישיים ופועלת בכיתות א-ט כשעה שבועית, במסגרת שעת המחנך. ראו גם מבקר המדינה, **דוח שנתי 168** (2018), "קידום למידה משמעותית בבתי הספר", עמ' 753-818.

59 אוריינות טכנולוגית ודיגיטלית היא שם כולל לאוסף מיומנויות ידע ספציפיים שכל אדם צריך לפתח על מנת להשתתף באופן פעיל בעולם עתיר טכנולוגיה.

השוואה של המשפט
בישראל למצב
המשפטי במדינות
אחרות מלמדת כי
ההגנה על פרטיות
ילדים בישראל ועל
מידע הנוגע להם
לוקה בחסר, שכן
ברוב מדינות העולם
חלים הסדרים
המתייחסים במישרין
להגנת מידע על
ילדים

הסדרת הגנה על פרטיות ילדים בחקיקה

1. כאמור, הוראות הדין בנושא הזכות לפרטיות באות לידי ביטוי בחוק הגנת הפרטיות, בחוק יסוד: כבוד האדם וחירותו, ובהוראות ספציפיות המתייחסות להגנה על פרטיותו של אדם. לזכויות המנויות בחוק היסוד ובחוק הגנת הפרטיות אין מגבלת גיל, ולפיכך הוראותיהם חלות גם על קטינים⁶⁰. נוסף על כל אלה, יש הוראות חוק המגינות, במישרין או בעקיפין, על פרטיותם של ילדים ואוסרות גילוי מידע על ילדים בנסיבות מסוימות, כגון חוק זכויות התלמיד, התשס"א-2000 (להלן - חוק זכויות התלמיד), הקובע חובת סודיות ביחס למידע על אודות תלמיד.

האמנה הבין-לאומית בדבר זכויות הילד⁶¹ (להלן גם - האמנה) משנת 1989, קובעת כי "ילד לא יהא נתון להתערבות שרירותית או בלתי חוקית בפרטיותו... ואף לא לפגיעות שלא כחוק בכבודו ובשמו הטוב"⁶². עוד נקבע באמנה, כי במדינות החתומות עליה, ילדים זכאים להגנת החוק מפני התערבות או פגיעות כאמור.

יצוין כי בהתאם לחוק הכשרות המשפטית והאפוטרופסות, התשכ"ב-1962, ועקרונות האמנה, בכל הנוגע לפעולות העלולות לפגוע בפרטיותו של קטין, ההסכמה הנדרשת היא לא הסכמת הקטין עצמו אלא הסכמת הוריו.

איגוד האינטרנט הישראלי פרסם באוקטובר 2016 מסמך מדיניות של הסדרה מוצעת בנושא "פרטיות ילדים בעידן האינטרנט"⁶³ (להלן - מסמך המדיניות). במסמך עמד האיגוד על הצורך להסדיר את הגנת פרטיותם של קטינים בהוראות הדין, לתקן את חוק הגנת הפרטיות, לקבוע מסגרת "רכה" של המלצות לציבור ההורים, ולשנות את מדיניותם של משרדי ממשלה.

על פי מסמך המדיניות, השוואה של המשפט בישראל למצב המשפטי במדינות אחרות מלמדת כי ההגנה על פרטיות ילדים בישראל ועל מידע הנוגע להם לוקה בחסר, שכן ברוב מדינות העולם חלים הסדרים המתייחסים במישרין להגנת מידע על ילדים, בחקיקה ראשית או בהסדרים בין-לאומיים מחייבים.

60 חוק הכשרות המשפטית והאפוטרופסות, התשכ"ב-1962, מגדיר "קטין" כאדם שלא מלאו לו שמונה עשרה שנים.

61 אמנה בדבר זכויות הילד, כ"א 31, 221 (נפתחה לחתימה ב-1989) (אושרה ונכנסה לתוקף ב-1991).

62 בתי המשפט יכולים לאכוף רק את ההוראות שעוגנו באופן ישיר בחקיקה ואילו שאר הוראותיה משמשות מקור פרשני במשפט הישראלי.

63 עו"ד סאני כלב, "פרטיות ילדים בעידן האינטרנט - מדיניות הסדרה מוצעת", **איגוד האינטרנט הישראלי** (אוקטובר 2016); <https://www.isoc.org.il/sts-data/21282>

התפיסה המשפטית הכללית בקשר לילדים היא שיש להעניק להם הגנה מיוחדת וחזקה יותר מן ההגנה המוקנית לבגירים, בעיקר משום שאינם מודעים מספיק לסכנות, בתחומים שונים, ואינם מסוגלים להתמודד איתן. אף על פי כן, אין בחוק הגנת הפרטיות התייחסות מיוחדת לקטינים, וזכותם של קטינים לפרטיות אינה מוסדרת בחוק ייעודי. זאת, על אף חשיבות העניין ואף שהנושא מוסדר בחקיקה או בהסדרים בין-לאומיים ברוב מדינות העולם.

2. בדצמבר 2010 פרסמה הרשות להגנת הפרטיות (רמו"ט אז) להערות הציבור טיוטה של כללי אתיקה והתנהגות לבעלי מאגרים האוספים מידע על קטינים⁶⁴. כללים אלה היו אמורים להעניק הגנה משמעותית בתחום פרטיותם של ילדים ולהתוות עקרונות ספציפיים להגנה על קטינים, ובהם: קביעת חובה כללית ל"עיצוב לפרטיות" שתמזער את סיכוני הפגיעה בפרטיות ילדים, איסור פעולות לניצולן לרעה של חולשותיו של קטין ואיסוף מידע שאינו הוגן, איסור איסופו של מידע על ילדים בני פחות מ-14 ללא הסכמה הורית ואיסור איסוף מידע רגיש על קטינים.

הרשות המליצה על עיגון העקרונות האלה בחקיקת משנה, אך מאז שנת 2010 טיטת הכללים לא קודמה והעקרונות גם לא עוגנו בחקיקת משנה.

3. על שולחן הכנסת הונחו כמה הצעות חוק פרטיות להסדרה משפטית-חוקתית של ההגנה על פרטיות ילדים בישראל, אך הליך החקיקה בהן לא הושלם⁶⁵. הנושא עולה לעיתים גם בוועדות הכנסת השונות⁶⁶.

64 לפי מחקרים כ-60 אחוז מאתרי האינטרנט המובילים לילדים בישראל אוספים מידע פרטי על ילדים ללא הסכמת הוריהם, בהם כתובת דואר אלקטרוני, תאריך לידה, שם מלא או תמונה.

65 ראו מספר הצעות חוק פרטיות שהונחו על שולחן הכנסת אך לא נדונו: הצעת חוק הגנת הפרטיות (תיקון - פרטיותם של קטינים), התשע"ב-2012 (פ/18/4439); הצעת חוק הגנת הפרטיות (תיקון - הזכות להישכח של קטינים), התשע"ח-2018 (פ/4967/20); הצעת חוק הגנת הפרטיות (תיקון הגנה על פרטיותם של קטינים), התשע"ז-2017 (פ/3942/20) המבוססת על מסמך המדיניות של איגוד האינטרנט הישראלי כאמור. ב-12.3.18 הגיש ח"כ מיקי רוזנטל את הצעת חוק הגנת הפרטיות (תיקון - פרטיות קטינים), התשע"ח-2018 (פ/5241/20) אך הדיון לגביה נדחה.

66 כך למשל, דיון בוועדת החינוך מ-24.4.12 בנושא "ניצול ספרי מחזור של בתי ספר תיכוניים למטרות מסחריות"; דיון בוועדת מדע וטכנולוגיה מ-30.1.17 בנושא "הגנת הפרטיות בעידן הדיגיטלי".

החקיקה בתחום הגנת הפרטיות אינה תואמת את ההתפתחות הטכנולוגית של העשורים האחרונים ואף אינה כוללת התייחסות מיוחדת לילדים. גם הניסיונות להסדרתה של ההגנה על פרטיות הילדים בחקיקה או בכללים לא צלחו. האמור לעיל ממחיש את הצורך בהגנה על זכותם של ילדים לפרטיות באופן המשלב כמה תחומים: חינוך והדרכה של הורים וילדים לשמירת זכותם לפרטיות, חקיקה מעודכנת שתגביל את האיסוף והשימוש במידע על ילדים לאופן ולמידה הדרושים, ושימוש בכלים טכנולוגיים שישרתו את הזכות לפרטיות של ילדים בפיתוח המערכות ובאבטחתן.

על משרד המשפטים בשיתוף גורמים רלוונטיים בתחום ההגנה על זכויות הילד לשקול הסדרה של הגנה על פרטיות הילדים בחקיקה או בכללים, תוך התאמה לעידן המידע וההתפתחויות הטכנולוגיות.

עדכון והתאמה של חוזרי מנכ"ל משרד החינוך הנוגעים לזכות לפרטיות של תלמידים

בשנת הלימודים תשע"ח (2017 - 2018) למדו במערכת החינוך בישראל יותר משני מיליון ילדים בגילאי 3 עד 18⁶⁷, מהם כ-1.7 מיליון תלמידים בבתי הספר. ככלל, המידע האישי על תלמידים נאסף ומנוהל במספר רב של מערכות מידע, במשרד החינוך ובבתי הספר ברחבי הארץ. גם במאגרי המידע של הרשות הארצית למדידה והערכה (להלן - ראמ"ה) יש נתונים רבים על כלל תלמידי ישראל. המידע מתקבל מהורי התלמידים, מהתלמידים עצמם ומגופים ציבוריים אחרים (כגון משרד הפנים), ומשמש את משרד החינוך לצרכים שונים. למשל, "מדד הטיפוח", המשקף את מצבם החברתי-כלכלי של התלמידים, מחושב על סמך מידע אישי: השכלת הורים, הכנסות לנפש, פריפריאליות וארץ מוצא⁶⁸. חלק ממאגרי המידע כוללים גם מידע על מורים ועל צוותי ההוראה בבתי הספר.

גופים ציבוריים ומשרדי ממשלה אחרים אוספים מידע על ילדים במסגרות שונות, עושים בו שימוש ואף מעבירים אותו ביניהם. אם הגורם האוסף את המידע הוא גורם ממשלתי, כגון משרד החינוך המנהל מאגר מידע על תלמידים

67 התפתחות מערכת החינוך, עובדות ונתונים תשע"ח, מתוך אתר משרד החינוך, מינהל כלכלה ותקציבים.

68 מדד הטיפוח פותח במשרד החינוך ב-2006, כדי לסייע בהקצאת חלק מהמשאבים במערכת החינוך בהתאם למאפייני תלמידיו של כל ב"ס. המדד הבית-ספרי נקבע לפי ממוצע המדדים של כל תלמידיו ומשוקללים בו עבור כל תלמיד בנפרד ארבעה מרכיבים: השכלת ההורים (מבוסס על דווח ההורים בזמן רישום התלמיד); הכנסת המשפחה (מבוסס על נתונים המתקבלים ממס הכנסה ומהתנועה הקיבוצית); מידת הפריפריאליות של ביה"ס; ארץ הלידה של הורי התלמיד (מבוסס על נתוני משרד הפנים). מדד הטיפוח מדורג בטווח רציף שבין 1 ל-10: מדד טיפוח 1 משמעו שצורכי הטיפוח של תלמידי ביה"ס הם המועטים ביותר (כלומר, מצבם החברתי-כלכלי הוא הטוב ביותר), וביה"ס אינו זקוק לסיוע מעבר להקצאה התקנית המוערית; מדד טיפוח 10 משמעו שצורכי הטיפוח של תלמידי ביה"ס הם הרבים ביותר (כלומר מצבם החברתי-כלכלי הוא הגרוע ביותר), ולפיכך ביה"ס זקוק לסיוע המרבי שניתן מעבר להקצאה התקנית המוערית.

ומשפחותיהם, הרי שהגוף הממשלתי כפוף לעקרונות של המשפט המינהלי והחוקתי כפי שנקבעו בפסיקה⁶⁹, נוסף על הוראות חוק הגנת הפרטיות. הוא מחויב לעמוד בכמה דרישות של אבטחת מידע ופרטיות, הקבועות בהוראות חקיקה ותקנים מחייבים, שמטרתם למנוע חשיפה, שימוש או העתקה שלא כדין של המידע, ולהפחית את הסיכון לפרצות אבטחה.

1. במשרד החינוך יש כמה חוזרי מנכ"ל ובהם הנחיות העוסקות במישרין או בעקיפין בפרטיות של מידע המנוהל על קטינים⁷⁰. הוראות נוספות קבועות בחוזר המנכ"ל משנת 2003, "שמירה על הפרטיות באתרי אינטרנט הבית ספריים"⁷¹. משנת 2017 ואילך פועל משרד החינוך לעדכון ולהתאמה של הוראות החוזר לזמננו. עדכון החוזר עתיד לכלול הנחיות מפורטות לצוותי החינוך על שמירת פרטיותם של התלמידים באתרים בית ספריים וברשתות החברתיות, ודרישה להסכמת הורים מפורשת בכתב לשימוש במידע.

משרד החינוך עדכן בנובמבר 2018 כי הסתיימה כתיבת החוזר והוא יפורסם בהקדם. עוד ציין המשרד כי המדיניות הברורה בחוזרי המנכ"ל היא דרישת הסכמה של הורה לאיסוף מידע על הילד או להעברתו, ונקבעו בהם גם תבחינים למקרים חריגים, בכפוף להגנות הקיימות בחוק.

2. מערכת החינוך נדרשת לעיתים לאזן את זכותם של תלמידים לפרטיות עם חובותיה היסודיות כלפיהם בתחום החינוך, למשל כשנדרשת העברת מידע חינוכי או אישי ממוסד חינוכי שתלמיד לומד בו למוסד שהוא עתיד לעבור אליו. העברת המידע אמורה לסייע לתלמיד במסגרת החינוכית החדשה, אך מצד שני חשוב לשמור על פרטיותו, ולאפשר לו התחלה חדשה במסגרת החינוכית שהגיע אליה. בדרך כלל נדרשים הורי הקטין לחתום על טופס ויתור סודיות או על טופס הסכמה להעברת מידע לגורמים המקצועיים הרלוונטיים. אם לא התקבלה הסכמת הוריו של התלמיד להעברת המידע, מסגרות החינוך נדרשות להכריע בדבר המידע שיועבר, נסיבות ההעברה ומקבל המידע. ראוי כי החלטה כזו תתקבל על פי כללים והנחיות ברורים ומפורטים, תוך איזון כלל השיקולים שפורטו לעיל.

69 דוח צוות ההסדרה, עמ' 46.

70 חוזר מנכ"ל תשע"ה/9(א) מ-3.5.15 בנושא "מצלמות במוסדות החינוך - הסדרת הכנסתן ואופן התקנתן"; חוזר מנכ"ל תשע"ה/9(ב) מ-3.5.15 בנושא "הנהלים לפעילות מחקרית במערכת החינוך"; חוזר מנכ"ל תשע"ב/4(א) מ-1.11.12 בנושא "אתיקה ומוגנות ברשת האינטרנט"; חוזר מנכ"ל תש"ע/3(א) מ-1.11.09 בנושא "מאגרי מידע בבתי הספר - רישום, דיווח ואבטחת מידע".

71 חוזר מנכ"ל תשס"ג/7(א) מ-2.3.03 בנושא "שמירה על הפרטיות באתרי האינטרנט הבית-ספריים".



**במשרד החינוך יש
 הנחיות רבות
 להעברת מידע בין
 מסגרות חינוכיות.
 חלק מההנחיות
 פוזרות בחוזרי מנכ"ל
 ישנים ולא מעודכנים,
 והן מתייחסות
 לרישומים ומידע
 שנאספו בבתי הספר
 באופן לא אחיד
 ולעיתים אף סותר**

הביקורת העלתה כי במשרד החינוך יש הנחיות רבות להעברת מידע בין מסגרות חינוכיות. חלק מההנחיות פוזרות בחוזרי מנכ"ל ישנים ולא מעודכנים, והן מתייחסות לרישומים ומידע שנאספו בבתי הספר באופן לא אחיד ולעיתים אף סותר. מוזכרים בהן מונחים כמו "תיק אישי", "כרטיס תלמיד" ו"כרטיס רפואי" בלי שהוגדר במפורש מה שהם כוללים וללא התאמה בין המושגים⁷².

העברת מידע על תלמידים בין מסגרות חינוכיות וחתימה על ויתור סודיות הן סוגיות נפוצות יותר ויותר גם בפניות שהתקבלו ביחידה לפניות ותלונות הציבור במשרד החינוך משנת 2010 ואילך: שאלות בדבר חובת החתימה על טפסי ההסכמה להעברת מידע, טענות של הורים על העברה שלא כדין של מידע רגיש על ילדיהם במעברים בין גן הילדים לבית הספר ובין בתי הספר ועוד. בחלק מן התשובות על פניות אלה נכתב כי הנושא לקראת הסדרה מחדשת.

הביקורת העלתה כי גורמים מקצועיים, בהובלת אגף שירות פסיכולוגי ייעוצי במשרד החינוך (להלן - אגף שפ"י), פועלים לפחות מספטמבר 2013 עם הלשכה המשפטית במשרד החינוך לכתיבתה של טיוטת חוזר מנכ"ל העתידה להחליף את חוזרי המנכ"ל הישנים ולקבוע הנחיות אחידות וכללים לשיקול דעת בעת העברת מידע בין מוסדות חינוך, בכפוף לחובות על פי דין, תוך שמירה על פרטיות התלמיד. ואולם אף שחלפו למעלה מחמש שנים, עדכנו של חוזר המנכ"ל טרם הושלם.

משרד מבקר המדינה מעיר למשרד החינוך, כי כל עוד ההגנה על פרטיות ילדים אינה מוסדרת בחוק ייעודי ועדיין חסרות הוראות שיעגנו את זכותם של תלמידים לפרטיות, וחוזרי המנכ"ל על העברת מידע בין מוסדות חינוך מיושנים ואינם נותנים מענה ראוי, עליו להשלים לאלתר את עדכנו של חוזר המנכ"ל.

זאת ועוד, הוראות מעודכנות ותקפות על שמירת פרטיותם של תלמידים יסייעו גם לבתי הספר בהתנהלותם השוטפת וימנעו את הפגיעה בפרטיותם של תלמידים במעבריהם בין מוסדות חינוך.

72 כך למשל, בחוזר מנכ"ל מ-1994 המתייחס ל"כרטיס התלמיד" והפרטים האישיים שכלול, בהם גם מגבלות רפואיות המונעות מהתלמיד פעילות בבית הספר ופרטים שנמסרו על ידי ההורים הקשורים למצבו הגופני והבריאותי. בחוזר נקבע כי "כרטיס זה ייפתח עם כניסתו של התלמיד למערכת החינוך ויעבור עמו מבית ספר לבית ספר עד גמר לימודיו". עם זאת, בחוזר מנכ"ל מ-1997 נקבע כי רישומים ומידע שנאספו בבית הספר "כגון מידע בתיק אישי, תוצאות מבחני אבחון, תיק רפואי וכו', יישארו חסויים". בהקשר זה לא נמצאה הגדרה ל"תיק אישי" ולפרטי מידע שייכללו בו.

ניהול מידע על תלמידים במאגרי מידע גדולים

רשות ארצית להערכה ומדידה בחינוך (ראמ"ה)

בשנת 2006 הוקמה ראמ"ה כיחידה במשרד החינוך⁷³. מחקריה והערכותיה נועדו לספק למערכת החינוך תובנות מבוססות מחקר לשם קידום יעדיה המרכזיים, כמו צמצום פערים, קידום אקלים בית ספרי מיטבי וצמצום האלימות. ראמ"ה מופקדת, בין השאר, על פיתוחם של מבחני הישגים לתלמידים ושאלוני אקלים וסביבה פדגוגית (להלן - מבחני המיצ"ב⁷⁴), ניהול מבחנים בין-לאומיים בישראל והערכת פרויקטים חינוכיים-לאומיים.

באוגוסט 2007 החליטה הממשלה⁷⁵ להקים צוות בין-משרדי בראשותה של מנכ"לית ראמ"ה דאז ובהשתתפות נציגים ממשרדי החינוך, המשפטים והאוצר ומנציבות שירות המדינה, שיגבש הצעת חוק להסדרת תפקידיה וסמכויותיה של ראמ"ה כרשות פנים-ממשלתית עצמאית למדידה והערכה בחינוך (להלן בפרק זה - החלטת הממשלה). הצוות היה אמור לגבש את הצעת החוק עד סוף שנת 2007.

1. בשנת 2010 הוכנה הצעת החוק הממשלתית "רשות ארצית למדידה והערכה בחינוך, התש"ע-2010"⁷⁶ (להלן - הצעת החוק). היא נועדה לעגן ולהסדיר את עבודתה של ראמ"ה כאמור בהחלטת הממשלה, לרבות איסוף המידע מתלמידים ומעובדי הוראה והקמת מאגר מידע שיכלול את המידע המתקבל ונאסף לשם ביצוע תפקידיה.

על פי הצעת החוק, ראמ"ה תהיה רשאית לאסוף מידע על תלמידים, הכולל פרטים אישיים רבים. "איסוף מידע" על פי הצעת החוק כולל גם קבלת רשימות וקבצי מחשב, עריכת מבחנים, שאלונים, ראיונות, תצפיות או סקרים, או קבלת נתונים.

בדברי ההסבר להצעת החוק צוין כי איסוף המידע ייעשה בשים לב להוראותיו של חוק הגנת הפרטיות בקשר לאיסוף מידע מקטינים, ולצורך בהתאמת איסוף המידע לגיל התלמידים שנאסף מהם. בהצעת החוק נקבע כי מאגר המידע של ראמ"ה יהיה חסוי, ולא יימסר ממנו מידע מזוהה אלא למשרד החינוך, ייאסף מידע על הישגיו של תלמיד בלבד לצורך הפעלת

73 מקורה של החלטה להקים יחידה למדידה והערכה בחינוך הוא ביישום המלצות "התכנית הלאומית לחינוך" שהגיש כוח המשימה לקידום החינוך בישראל בשנת 2005 (דוח ועדת דברת).

74 מיצ"ב - ראשי תיבות "מדדי יעילות וצמיחה בית ספרית". מבחני המיצ"ב כוללים מבחני הישגים המשקפים את תוצרי הלמידה של בתי הספר בארבעה מקצועות ליבה וסקרי אקלים וסביבה פדגוגית, המשקפים את ההיבטים החברתיים-רגשיים-פדגוגיים של בתי הספר. נתוני מבחני המיצ"ב מיועדים לשמש את המנהלים ואת צוותי ההוראה ככלי לתכנון משאבים ולניצולם, כדי להביא למיצוי הפוטנציאל של תלמידיהם, לשפר את האקלים הבית ספרי ולייעל את מערך ההוראה בבית הספר.

75 החלטת ממשלה מס' 2314 בנושא "הרשות הארצית למדידה והערכה בחינוך (ראמ"ה)".

76 האמור כאן מתייחס לנוסח הצעת החוק כפי שפורסם באתר ראמ"ה:

http://cms.education.gov.il/EducationCMS/Units/Rama/OdotRama/hok_rama_2010.htm

מדיניותו של המשרד, ומשרד החינוך לא יעביר מידע כאמור אלא באופן בלתי מזוהה ולמטרות מחקריות.

ביולי 2010 העביר יו"ר המועצה הציבורית להגנת הפרטיות דאז לשר המשפטים דאז את הערות המועצה על טיוטת החוק (להלן בפרק זה - נייר העמדה). בנייר העמדה צוין כי אין ספק שהתכליות שלשמן הוקמה ראמ"ה הן ראויות, אך בנוסח החוק המוצע עדיין נשקפת סכנה רבה לפרטיותם של התלמידים, בני משפחתם ועובדי ההוראה שהמידע עליהם נאסף.

ביולי 2010 שלח לשר המשפטים דאז גם יו"ר הוועדה להגנת הפרטיות דאז בלשכת עורכי הדין את התייחסות הוועדה לטיטת הצעת החוק. הוועדה התנגדה להצעת החוק בשל הפגיעה בזכות היסוד לפרטיות ומשום שחסרה בה התייחסות לשאלות יסודיות בתחום זה.

התברר כי הליך החקיקה לא הושלם. הלכה למעשה, עד למועד סיום הביקורת, 11 שנים לאחר החלטת הממשלה, טרם נחקק חוק המסדיר את פעולתה של ראמ"ה, את תפקידיה וסמכויותיה.

תזכיר חוק נוסף להסדרת פעולתה של ראמ"ה פורסם באפריל 2014, אך גם הוא לא הושלם.

2. הנהלת ראמ"ה מסרה למשרד מבקר המדינה כי בנסיבות אלה היא פועלת על פי העקרונות שברוח הצעת החוק וכי במאגרי המידע שברשותה אין מידע מזוהה אלא לגבי מבחני המיצ"ב, הבחונים את הישגי התלמידים בארבעת מקצועות הליבה; שאר המידע שנאסף במאגרי המידע שלה הוא אנונימי.

בפועל, במסגרת מבחני המיצ"ב, ראמ"ה אוספת למאגרי המידע שלה נתונים מזהים, אישיים ורגישים רבים, לרבות שמות התלמידים, מספרי זיהוי, כיתה, אם התלמיד משולב, אם התלמיד הוא עולה חדש, יישוב, מגדר, מגזר, וציונים שקיבל תלמיד במקצועות שנבחן בהם. יתר על כן, תוצאותיהם של מבחני המיצ"ב משוקללים עם מידע נוסף כגון המדד החברתי-כלכלי של כל תלמיד⁷⁷. על פי הצעת החוק, אוספת ראמ"ה גם נתונים אישיים מזהים על עובדי הוראה בבתי הספר, לרבות שמות העובדים, מספרי זיהוי ופרטי זיהוי נוספים, מידע על הכשרה, השכלה וותק מקצועי, תפקיד, פרטי שיבוץ במערכת השיעורים ועוד. יוצא אפוא כי ראמ"ה אוספת נתונים שרובם מוגדרים כ"מידע רגיש" לפי חוק הגנת הפרטיות.

הזכות לפרטיות היא זכות יסוד ופגיעה בה בידי רשויות שלטוניות, כמו פגיעה בזכויות אחרות הקבועות בחוק-יסוד: כבוד האדם וחירותו, אינה מותרת על פי תנאי פסקת ההגבלה אלא "בחוק ההולם את ערכיה של מדינת-ישראל, שנועד לתכלית ראויה ובמידה שאינה עולה על הנדרש, או



ראמ"ה פועלת למן
הקמתה, זה 12 שנים,
בלי שנקבעו בחוק
כללים בכל הנוגע
לאיסוף מידע רגיש
ומזהה, לגורמים שהיא
רשאית לאסוף מהם
את המידע המזהה,
לסוגי המידע
שתאסוף, למגבלות
על פעולות האיסוף,
לדרכי ההחזקה
והשמירה של המידע
ולהעברתו ממאגריה
לגורמים אחרים

לפי חוק כאמור מכוח הסמכה מפורשת ב⁷⁸. הפסיקה קבעה כי ככלל, על הסמכה לפגיעה בזכות אדם להיות מפורשת ואין לפרש חוק כפוגע או כמסמך לפגוע בזכות אדם, זולת אם הדבר נקבע בו במפורש⁷⁹.

ראמ"ה פועלת למן הקמתה, מזה 12 שנים, בלי שנקבעו לה בחוק כללים לאיסוף מידע רגיש ומזהה, הגורמים שתהיה רשאית לאסוף מהם את המידע המזהה, סוגי המידע שתאסוף, המגבלות על פעולות האיסוף, דרכי ההחזקה והשמירה של המידע והעברתו ממאגריה לגורמים אחרים. הסדרה זו נדרשת מכוח החלטת הממשלה, אך גם ובמיוחד לנוכח הפגיעה הפוטנציאלית החמורה בזכותם לפרטיות של תלמידים, בני משפחותיהם ועובדי הוראה.

משרד החינוך השיב, כי ראמ"ה פועלת כחלק אינטגרלי ממשרד החינוך ולפי הסמכויות שנתונות לו. אף שהצעת החוק לא קודמה, היא מתווה את הדרך לפעילותה של ראמ"ה גם על פי חוק הגנת הפרטיות, ומאחר שראמ"ה פועלת על פי עקרונותיה של הצעת החוק, הרי שהיא פועלת בסמכות ולפי כל דין.

משרד מבקר המדינה מעיר למשרד החינוך כי כל עוד לא הושלם הליך החקיקה ולא הוכרעה בחקיקה סוגיית חסיון המידע שאוספת ראמ"ה, נשקפת סכנה לזכות הפרטיות של תלמידים ובני משפחותיהם באיסוף המידע, שמירתו והשימוש שנעשה בו. בפעולת ראמ"ה על פי עקרונותיה של הצעת חוק מלפני שמונה שנים אין כדי לייתר את הצורך בחקיקה בתחום רגיש זה.

על משרד החינוך לפעול לאלתר להסדרת פעולתה של ראמ"ה ולהגיש הצעת חוק מעודכנת להתייחסות הגופים הרלוונטיים ולהערות הציבור, בהתאם להחלטת הממשלה. עד ההסדרה בחוק יקבע משרד החינוך בכללים או בחוזר מנכ"ל הנחיות בקשר לפעולתה של ראמ"ה.

פרויקט הסדרת מערך המידע במשרד החינוך

מחסן נתונים (Data Warehouse) הוא מערכת מידע המהווה בסיס נתונים כלל-ארגוני ומאפשרת תחקור מידע לצורך תמיכה בקבלת החלטות בארגון ואיתור מקרים חריגים. הדרך השכיחה להקמת מחסן נתונים היא גזירת נתונים ממערכות תפעוליות, הסבתם, טיובם והתאמתם לסוגי השאילתות ולאחזור

78 סעיף 8 לחוק יסוד: כבוד האדם וחירותו.

79 ראו: בג"ץ 337/81 מיטריני נ' שר התחבורה, פ"ד לז(3) 337; בג"ץ 3267/97 רובינשטיין נ' שר הביטחון, פ"ד נב(5) 481; בג"ץ 8070/98 האגודה לזכויות האזרח בישראל נ' משרד הפנים, פ"ד נח(4) 842 (2004).



פרויקט "הסדרת מערך המידע" יאפשר שיקוף של נתוני תלמידים ונקודת מבט מתכללת על יותר מ-2 מיליון התלמידים בישראל, בעיקר לניתוחי מידע סטטיסטיים. ניתוח המידע שיתקבל אמור לשרת מטרות שונות, בהן זיהוי תלמידים בסיכון לצורך טיפול בהם

המידע הנדרשים בארגון. למעשה, כל הנתונים הנמצאים במחסן הנתונים כבר שמורים במערכת כלשהי בארגון.

הרשות פרסמה "תסקיר השפעה על הפרטיות"⁸⁰ ובו נקבעו עקרונות כלליים לשימוש בכל פרויקט הכרוך בשימוש במידע אישי באופן העשוי להשפיע על פרטיותם של בני אדם. מקרה המצדיק שימוש בתסקיר הוא הקמת מאגר מידע שיקלוט לתוכו מידע המוחזק בחלקים שונים של הארגון. הרשות פרסמה באתר שלה גם עמדה בנושא "ניהול סיכונים פרטיות", הכוללת פרמטרים שארגונים יוכלו להיעזר בהם להערכתה של רמת הסיכון הכרוכה בקיומו של מאגר מידע אישי ובהם: מספר האנשים שיש עליהם מידע, כמות המידע שנשמר על כל אדם, רגישות המידע הנשמר, כמות הממשקים החיצוניים למערכת המידע, ומידת הסיכון לנזק ממשי שבגילוי המידע.

במסמך מדיניות ההגנה למאגרי-על של הרשות הלאומית להגנת הסייבר הוגדרו כמה תנאים מצטברים לקיומו של "מאגר-על": מאגר הכולל פרטים אישיים מזהים; מורכב משני מיליון רשומות ייחודיות ויותר; ורמת הנזק שעלולה לגרום חשיפתו מוערכת כגבוהה. מסמך המדיניות נועד לסמן מאגרי מידע בעלי מאפיינים רגישים במיוחד מבחינה לאומית ככספי מידע, הטעונים רמת הגנה גבוהה יותר, ניהול ורישום מיוחדים.

מן הרבעון הראשון של 2017 מקדם מינהל כלכלה ותקציבים במשרד החינוך פרויקט "הסדרת מערך המידע" (להלן - הפרויקט). במסגרתו נעשה מיפוי של נתונים מכמה מאגרי מידע הקיימים במשרד החינוך, על תלמידים, עובדי הוראה ובתי ספר בכל הארץ, כדי לקשר ביניהם באופן אינטגרטיבי באמצעות מערכת ממוחשבת בעלת יכולות ניתוח מתקדמות, מבוססת בינה עסקית (BI). את הפרויקט מנהל צוות היגוי ובו בכירים ממשרד החינוך.

בין יעדי הפרויקט גיבוש מדיניות חינוך מושכלת, התייעלות ארגונית ותפעולית, והפחתת הנטל הביורוקרטי על המערכת המדווחת, קרי בתי הספר, מאחר שהמידע על התלמידים מפוזר בין גורמים רבים במשרד החינוך ומחוץ לו. הפרויקט יאפשר שיקוף של נתוני תלמידים ונקודת מבט מתכללת על יותר משני מיליון התלמידים בישראל, בעיקר לניתוחי מידע סטטיסטיים. ניתוח המידע שיתקבל אמור לשרת מטרות שונות, בהן זיהוי תלמידים בסיכון לצורך טיפול בהם.

במסגרת הפרויקט מופו סוגי הנתונים (שדות דיווח) הדרושים על תלמידים וקיימים במערכות המידע השונות של המשרד⁸¹: פרטי התלמיד והוריו, פרטים על בית הספר שהוא לומד בו, לרבות זרם החינוך, השתייכותו לחינוך מיוחד או הוראת שילוב, נתונים דמוגרפיים וסוציו-אקונומיים, צרכים מיוחדים, לקויות למידה מאובחנות, אוכלוסייה בסיכון (נוער נושר, למשל), מגמות לימוד או תוכניות חינוכיות שהוא משתתף בהן, היותו במעקב של קצין ביקור סדיר או בטיפול האגף לקידום נוער, קבלת התאמות לבחינות הבגרות, נתוני זכאות

80 ראו: https://www.gov.il/he/Departments/General/privacy_by_design.

81 מערכות מידע פנימיות, מערכות של מוסדות החינוך ומערכות המצויות אצל ספקים.

לתעודת בגרות, ציונים, זכאות לסיוע במשאבים כמו שיעורי עזר לעולים, סייעות רפואיות, מלגות, ועוד.

על פי לוח הזמנים שנקבע לפרויקט, בשנת הלימודים התשע"ט (2018 - 2019) החל מחקר חלוץ (פיילוט) במוסדות החינוך בשיתוף אחת הרשויות המקומיות, שמטרתו בחינת הפוטנציאל שבתכלול נתונים על "ישות תלמיד" בקשר לסוגיית הנשירה ולסוגיית התנודה בין ארבע לחמש יחידות לימוד במתמטיקה.

במועד סיום הביקורת, אוגוסט 2018, טרם הושלמו התשתית הבסיסית לתכלול הנתונים ומיפוי צורכי המידע. לצדה של עבודה זאת, מינהל כלכלה ותקציבים והלשכה המשפטית בוחנים שאלות משפטיות העולות משדות הנתונים שמופ, בהן הזכות לפרטיות וההגבלות המתחייבות מתכלול המידע, על מנת להבטיח שלא ישוקף מידע עודף. בתהליך שולבה גם חטיבת אבטחת המידע במשרד.

פרויקט הסדרת מערך המידע, המתכלל פרטים רגישים מזהים כה רבים והמקשר בין כלל סוגי הנתונים במערכות הקיימות מצוי ברמת סיכון גבוהה יותר מרמת הסיכון של מערכות מפוזרות נוכח כמות התלמידים ורגישות המידע הנאסף, ולכן נדרשת בו רמה גבוהה יותר של אבטחת מידע.

משרד מבקר המדינה מעיר למשרד החינוך כי אם יתברר שהפרויקט מהווה "מאגר מידע חדש" על פי הגדרותיו של חוק הגנת הפרטיות, יהיה צורך לבחון אם מאגר המידע מקיים גם את הגדרת "מאגר-על", הטעון רמת הגנה גבוהה יותר, וכן ניהול ורישום מיוחדים.

בתשובתו מנובמבר 2018 כתב משרד החינוך, כי הפרויקט נועד לייתר רבים מאיסופי המידע הקיימים כיום במערכת החינוך באופן לא מאובטח ולא מתוקשב ובכך יתרום לשיפור ההגנה על פרטיותם של תלמידים, ולא לפגיעה בה. קישור הנתונים ישמש לחקירה סטטיסטית בלתי מזוהה לצורך ניתוח אוכלוסיות, ולא לצורך עיון בנתוני תלמיד מזוהים. עם זאת ציין המשרד, כי צוות ההיגוי עוסק במיפוי צורכי המידע ובהסדרת מערך ההרשאות לצפייה בשדות מסוימים במתכונת מזוהה. רק לאחר השלמתו של תהליך זה, וככל שתידרש גישה של בעל תפקיד למידע מזוהה לצורך מתן מענה לתלמיד ספציפי, תתאפשר גישה למידע מזוהה, אך המידע יוגבל לשדות מסוימים ולאוכלוסיות מסוימות, בהתאם לתפקידו של בעל הגישה. עוד הסביר המשרד, כי הוא מצוי בעיצומו של מהלך מקיף וסדור לבחינת ההיבטים המשפטיים של הפרויקט ברוח הוראות תסקיר ההשפעה על הפרטיות, ובתהליך זה נבחנות סוגיות הליבה המשפטיות הנוגעות בהגנת הפרטיות, לרבות הסמכות לאסוף או לנהל נתון כלשהו, הסכמת אפטרופוס לאיסופו, ופרק הזמן הראוי שבו המשרד ישמור נתונים אלה במתכונת מזוהה. בדצמבר 2018 הוסיף המשרד, כי למען הזהירות הוא בוחן גם אם ייתכן שזהו מאגר מידע חדש, אף על פי שהפרויקט כאמור, לא ייצור מאגר מידע חדש ועצמאי אלא יתבסס על מאגרי מידע קיימים אחרים.

להפעלה של מצלמות
מעקב במסגרות
חינוכיות יש מחיר
פסיכולוגי רב
השפעה: הצילום פוגע
בצורך הנפשי הבסיסי
של כל אדם למרחב
פרטי מוגן החופשי
ממעקב חיצוני
מתמיד. לכן יש לנהוג
זהירות בשימוש
במצלמות מעקב
במתקנים שיש בהם
ילדים ובני נוער

על צוות ההיגוי המנהל את הפרויקט לשקול לערב את הרשות להגנת הפרטיות ואת מחלקת ייעוץ וחקיקה בקידומו, על מנת שיוטמעו בו דרישות יסודיות מתחום אבטחת המידע והגנת הפרטיות של התלמידים, משפחותיהם ועובדי ההוראה.

בתשובתנו מפרוואר 2019 ציין משרד החינוך כי פנה למחלקת ייעוץ וחקיקה, ובכוונתנו לפנות גם לרשות להגנת הפרטיות.

פיקוח ובקרה בתחום הגנת הפרטיות של תלמידים

מצלמות בבתי הספר

בעשורים האחרונים גובר בישראל השימוש באמצעים טכנולוגיים המיועדים לפיקוח ולמעקב מרחוק, חזותי או קולי, בשטחים ציבוריים ופרטיים. השימוש במצלמות במרחב הציבורי, שהצילומים הנקלטים מהן נאגרים במאגרי מידע ממוחשבים, מעלה את השאלה המשפטית בדבר איזון הזכות החוקתית לפרטיות עם אינטרסים ציבוריים כגון הגנה על רכוש, מניעת עבירות וגילויין ושמירת הסדר הציבורי וביטחון הציבור⁸².

בשנים האחרונות נפוץ השימוש במצלמות אבטחה או מעקב בבתי ספר ברחבי הארץ. המצלמות הותקנו ביוזמה ותקצוב של גורמים שונים ובהם בתי ספר, ועדי הורים או רשויות מקומיות. בתי הספר שונים מאוד במספר המצלמות, במיקומן, בשימוש שעושים בהן מנהליהם, בנהלי הגישה לחומר המצולם, במטרות השימוש בחומר המצולם ועוד⁸³. ככלל, מצלמות מותקנות בבתי הספר לצורך שמירה על ביטחון התלמידים והגנה מפני אלימות, בריונות והתנהגויות מסכנות אחרות, ולצורך שמירה על רכוש בית הספר לאחר שעות הלימודים.

להפעלה של מצלמות מעקב במסגרות חינוכיות יש מחיר פסיכולוגי רב השפעה: הצילום פוגע בצורך הנפשי הבסיסי של כל אדם למרחב פרטי מוגן החופשי ממעקב חיצוני מתמיד. לכן יש לנהוג זהירות בשימוש במצלמות מעקב במתקנים שיש בהם ילדים ובני נוער⁸⁴.

1. רשם מאגרי המידע פרסם כמה הנחיות המבהירות את תחולתם של דיני הגנת הפרטיות על השימוש במצלמות מעקב במרחב הציבורי ובמקומות

82 בעניין זה ראו גם: דוחות על הביקורת בשלטון המקומי לשנת 2013, "פעולות פיקוח ואכיפה של הרשויות המקומיות לטיפול בתופעות של הפרות סדר ואלימות במרחב הציבורי", 133 מעמ' 156-164.

83 מבוסס על מחקר בנושא:

Lotem Perry-Hazan & Michael Birnhack, *Privacy, CCTV, and School surveillance in the shadow of imagined law*, 50 Law & Society Review (2016)

84 חוות דעת רשם מאגרי מידע בנושא "מצלמות מעקב - הדין החל ואופן השימוש", מיום 3.11.10.

עבודה⁸⁵ (להלן - ההנחיות). בהתאם להנחיות אלה, התקנת מצלמות במרחב הציבורי פוגעת בפרטיות⁸⁶ ולכן צריכה לעמוד במבחני חוק יסוד: כבוד האדם וחירותו. ההחלטה על שימוש במצלמות צריכה להתקבל רק לאחר בחינת צרכים וחלופות, בחינה מוקדמת של השפעה על הפרטיות, ובכפוף למגבלות המפורטות בהנחיות.

בהנחיות אין התייחסות ספציפית להתקנת מצלמות מעקב בבתי הספר, אך צוין בהן כי יש לנקוט זהירות יתרה בכל הנוגע להתקנת מצלמות מעקב במקומות כינוס של קטינים כגון מוסדות חינוך או מתנ"סים, לצמצם ככל האפשר את עצם השימוש במצלמות ולהקפיד על מיקומן ועל השימוש במידע הנאסף באמצעותן. עוד נקבע בהנחיות, כי במוסדות חינוך ראוי במידת האפשר ליידע באופן אקטיבי את ההורים על הצבת מצלמות.

ביולי 2018, בעקבות דיון בממשלה ובכנסת ביוזמת חקיקה בנושא התקנת מצלמות מעקב בגני ילדים, פרסמה הרשות להגנת הפרטיות את עמדתה בנושא זה⁸⁷. הרשות סבורה כי יש לנקוט זהירות יתרה במעקב קבוע אצל ילדים ובני נוער, מפני שהדבר עלול לחבל ביכולתם להתפתח ובשל החשש לדליפה של צילומי הילדים לאינטרנט וניצולם לרעה.

2. תופעת המצלמות המותקנות בבתי הספר חידדה מאוד את הצורך באיזון זכותו של התלמיד לאקלים מיטבי ולקידום רווחתו בבית הספר עם זכותו לפרטיות, בשים לב להיבטים חינוכיים כמו פיתוח תחושת שייכות, אמון וקידום ערכים חברתיים בקהילה הבית ספרית.

במאי 2015, ולאחר שכבר הותקנו מצלמות בחלק מבתי הספר ברחבי הארץ, פרסם משרד החינוך את חוזר המנכ"ל "מצלמות במוסדות החינוך - הסדרת הכנסתן ואופן התקנתן" (להלן - חוזר המנכ"ל בנושא מצלמות). הוראות החוזר תקפות גם לגבי מצלמות שהותקנו לפני פרסומו ונקבע בו כי התקנתן תותאם להוראות החוזר, ככל שתידרשנה, עד תחילת שנת הלימודים התשע"ו (2015 - 2016). על פי החוזר, הגורמים האחראיים הם מנהל היחידה לקידום אקלים בטוח ולמניעת אלימות באגף שפ"י ומנהל תחום ביטחון באגף הבכיר לביטחון, לשעת חירום ולבטיחות סביבתית במשרד החינוך (להלן - אגף ביטחון). חוזר המנכ"ל אושר בידי משרד המשפטים לאחר שנבחנו בו היבטים הנוגעים לזכות לפרטיות.

חוזר המנכ"ל בנושא מצלמות קובע כי "שימוש רציף במצלמות הוא בגדר אמצעי אחרון, שלצד תועלתו כרוך בפגיעה בפרטיות ולפיכך יש לשקול

85 הנחיית רשם מאגרי מידע מס' 4/2012 בנושא "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן"; חוות דעת בנושא "מצלמות מעקב - הדין החל ואופן השימוש", מיום 3.11.10; הנחיית רשם מאגרי מידע מס' 5/17 בנושא "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה".

86 צילום אדם כשהוא ברשות היחיד מהווה פגיעה בפרטיות לפי סעיף (3) לחוק. צילום אדם ברשות הרבים עשוי להגיע כדי בילוש או התחקות אחרי אדם, העלולים להטרידו ומהווה פגיעה בפרטיות לפי סעיף (1) לחוק.

87 עמדת הרשות להגנת הפרטיות בעניין השימוש במצלמות מעקב בגני ילדים כפי שפורסמה באתר הרשות: <https://www.gov.il/he/Departments/news/kindergardens>

בזהירות את עצם השימוש בו, ואם נעשה בו שימוש יש לעשות זאת במידה שאינה עולה על הנדרש". החוזר מסדיר בפירוט ניכר את השיקולים שיש לשקול בקשר להתקנת המצלמות, בחירת מיקומן, זוויות הצילום, אבטחת המידע, סדרי הצפייה בחומר המוקלט והשימוש בו. למשל, אסור להתקין מצלמות בכיתות הלימוד ובמקומות שמתקיימות בהם פעילויות פרטיות ומעין-פרטיות כמו חדרי שירותים, חדרי מורים, חדר היועץ החינוכי והמרפאה. משהוחלט על הצבת מצלמות בתחום הפנימי של בית הספר, תימסר על כך הודעה להורים ולתלמידים. החומר שיוקלט במצלמות יבוער כעבור שלושה ימים לכל המאוחר, אלא אם כן מתקיימות נסיבות חריגות המצדיקות את שמירתו. מנהל בית הספר, או מנהל מחלקת החינוך ברשות החינוך המקומית, יעביר מדי שנה למשרד החינוך, במסגרת הדיווחים המוגשים לו, נתונים על המצלמות שהותקנו ועל המצלמות שהוסרו.

בשנת 2017 פרסם אגף ביטחון מכרז לבקרה ולבדיקת תקינות של אמצעי ביטחון ומערכות התרעה המותקנים במוסדות חינוך, כ-2,000 בתי ספר בשנה. בשנת 2018 נבחר ספק חיצוני, שביצע בקרות ב-1,000 בתי ספר בקירוב מיולי 2018 עד נובמבר 2018. להערכת משרד החינוך, עד סוף שנת 2019 ייאספו נתונים על כלל אמצעי הביטחון ומערכות ההתרעה המותקנים במוסדות החינוך, לרבות מצלמות.

מעיון בדרישות המכרז ובדוח הבקרה לדוגמה שהועבר למשרד מבקר המדינה עולה, כי הבקרה כוללת רשימת בדיקות של 200 ויותר נתונים הנוגעים למערכות ביטחון המותקנות במוסדות החינוך, לרבות בדיקה של מצלמות המותקנות בבית הספר - אם ישנן, מספרן, אם הן ממוקמות בשטח ציבורי ואם הן מותקנות על פי חוזר המנכ"ל.

מדוח הבקרה לדוגמה נראה כי הבקרה בעיקרה היא טכנית ואינה כוללת פרטים נוספים על הפעלת המצלמות בהתאם לחוזר המנכ"ל, פרט לציון אם החיווי תקין או לא תקין.

יצוין כי בתשובותיו על כמה בקשות שהוגשו לו מהציבור מ-2015 ואילך לפי חוק חופש המידע, התשנ"ח-1998, בנושא הסדרת פעילותן של מצלמות המעקב בבתי הספר, ציין משרד החינוך כי אין לו נתונים בנושא.



 חוזר המנכ"ל כולל

 הוראות מפורטות

 להסדרת ההתקנה

 של מצלמות בבתי

 הספר. ואולם הבקרה

 הנעשית כיום על ידי

 משרד החינוך אינה

 בודקת את מילוי

 דרישות הוראותיו של

 החוזר

חוזר המנכ"ל כולל הוראות מפורטות להסדרת ההתקנה של מצלמות בבתי הספר, לרבות זוויות הצילום, אבטחת המידע, סדרי הצפייה בחומר המוקלט, הודעה להורים ולתלמידים על הצבת המצלמות וביעור החומר המוקלט לאחר תקופה קצובה. ואולם הבקרה הנעשית כיום על ידי משרד החינוך אינה בודקת את מילוי דרישות הוראותיו של החוזר. משרד מבקר המדינה מעיר למשרד החינוך, כי עליו לבחון באופן יסודי את מידת הטמעתן של הוראות חוזר המנכ"ל ולפעול לבקרת יישומן. כמו כן, עליו לאכוף את הוראות החוזר ולקבל מהספק החיצוני דיווחים על בתי הספר הכוללים, בין השאר, נתונים על הצבת מצלמות או על הסרתן, ובהתאם לתמונה שתתקבל לשקול פעולות נוספות לאכיפת ההוראות, שיבטיחו את מימוש התכליות המנויות בו.

אבטחת מאגרי המידע של משרד החינוך

1. בתחום אבטחת המידע והגנתן של מערכות מידע ממוחשבות יש הסדרים נורמטיביים רבים, בחוק הגנת הפרטיות, בתקנות אבטחת מידע ובהנחיות רשם מאגרי המידע מכוחם, ובהחלטות ממשלה המחילות גם חובות מתחום התקינה הבין-לאומית.

"מאגר מידע" מוגדר בחוק הגנת הפרטיות כאוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי ומיועד לעיבוד ממוחשב, למעט חריגים המוזכרים בחוק. "אבטחת מידע" מוגדרת כ"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין". החוק קובע כי האחריות לאבטחת המידע שבמאגר המידע חלה על כל אחד מבעלי התפקידים: בעל המאגר, מחזיק במאגר ומנהל מאגר מידע. מחזיק הוא "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". ככלל, חובות אבטחת המידע נגזרות ממידת רגישותו של המידע השמור במאגר המידע ומאופן שמירתו בו. ככל שאדם עלול להיפגע יותר מגילוי המידע עליו ברבים, כן המידע נחשב לרגיש יותר וכן עולה רמת האבטחה שיש לנקוט בשמירתו⁸⁸. במהלך השנים פרסם רשם מאגרי המידע כמה הנחיות ליישומם של תקנות אבטחת מידע ועיבוד מידע אישי בשירותי מיקור חוץ, כפי שיפורט להלן.

בשנים האחרונות קיבלה ממשלת ישראל כמה החלטות על מרחב הסייבר וההגנה עליו. למשל, בהחלטת ממשלה מספר 2443 מפברואר 2015, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (להלן - החלטה 2443), נקבע כי המנכ"לים של משרדי הממשלה שמפעילים סמכויות אסדרה על גופים או פעילויות החשופים לאיומי סייבר, יקדמו את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שהם אחראים לו, בין

88 ראו דוח צוות ההסדרה בקשר לאבטחת מידע במאגרי מידע ממשלתיים, בעמ' 46 וראו מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2017**, "אבטחת מידע והגנת הפרטיות ברשויות מקומיות - מעקב מורחב", עמ' 201 - 245.

השאר על ידי הגדרת המדיניות ודרישות האסדרה. בהתאם להחלטה זו הוקמה במשרד ראש הממשלה היחידה להגנת הסייבר בממשלה (להלן - יה"ב), המנחה את הממשלה בתחום הגנת הסייבר והנחיתה מחייבות את משרדי הממשלה ואת יחידות הסמך⁸⁹. על פי "הנחיית המסגרת להגנת הסייבר בממשלה" (להלן - הנחיית המסגרת), שפרסמה יה"ב בספטמבר 2016, בנסיבות שמשולבים בהן במשרדי הממשלה ספקים רבים המאפשרים שירותי מיקור חוץ בתחומי פעילות שונים, ולחלקם הרשאות גישה גורפות לכלל מערכות המידע המשרדיות - קיים סיכון בתחום הסייבר.

באפריל 2017 פרסם מערך הסייבר את "תורת ההגנה בסייבר לארגון" (להלן - תורת ההגנה), המגדירה שיטה סדורה להובלת ארגונים להכרת הסיכונים הרלוונטיים בתחום הסייבר, גיבוש מענה הגנתי ומימוש תוכנית להפחתת הסיכונים. על פי תורת ההגנה, על הארגון לכתוב וליישם מדיניות ונהלים רלוונטיים לשם הגנה על המידע ולעדכןם באופן תקופתי.

2. ההתפתחות הטכנולוגית בשנים האחרונות משרתת גם את עולם החינוך בישראל - דרכי הלמידה במאה ה-21 מבוססות על אמצעים דיגיטליים שונים, מבוססי אינטרנט. התוכנית הלאומית לתקשוב⁹⁰ המופעלת בבתי ספר רבים בארץ מקדמת את הפיכתם של בתי הספר לארגונים מתוקשבים, פועלת לשיפור תהליכי ההוראה, הלמידה וההערכה ולפיתוח אוריינות טכנולוגית ודיגיטלית בקרב התלמידים.

חלק מהתהליכים נעשים באמצעות התקשרות של משרד החינוך עם חברות פרטיות או גורמים חיצוניים (להלן - ספקים) לפיתוח מוצרים טכנולוגיים חינוכיים המבוססים על מידע אישי. משרד החינוך מתקשר עם ספקים באמצעות מכרזים או בהתקשרויות הפטורות ממכרז, בכפוף לכללים הקבועים בחוק חובת המכרזים, התשנ"ב-1992, ובתקנותיו.

ככל משרד ממשלתי, גם משרד החינוך משתמש בשירותי מיקור חוץ משיקולי יעילות, הוזלת עלויות ופינוי משאביו לליבת העיסוק המקצועי שלו. ואולם כשספק מחזיק במאגרים של מידע אישי או רגיש, על תלמידים ועל משפחותיהם, זהו סיכון הטעון הסדרה משפטית וארגונית מפורטת.

הסיכונים הכרוכים במערכות מידע ממוחשבות הם רבים ומגוונים: דליפת מידע רגיש וחשיפה של נתונים אישיים לגורמי חוץ, גישה לא מורשית למאגרים, שימוש במידע מן המאגרים למטרות זרות (לרבות לצורכי הפקת רווח כספי ממכירתו), פגיעה או השבתה של מאגר המידע ועוד.

89 על פי נספח ה' להחלטה 2443 יה"ב תפעל בכפיפות למונה על התקשוב הממשלתי שבמשרד ראש הממשלה ובהנחיה מקצועית של מערך הסייבר.

90 מדובר בשיטת הוראה ולמידה של תכנים המותאמים למציאות המשתנה. ההוראה נעשית תוך שימוש בטכנולוגיה לקידום תהליכי ההוראה בשילוב טכנולוגיה ומידע. ראו פרטים באתר התוכנית:

<http://cms.education.gov.il/EducationCMS/Units/PituachMiktzoie/PituachMiktzoi/yihudiot/tikshuv.htm>

משרד מבקר המדינה בחן את יישומן של חלק מההוראות הנוגעות לאבטחת המידע והגנת הפרטיות במאגרי המידע שבבעלות משרד החינוך. נבדק גם יישום החובות הקבועות בדין למיפויים של מאגרי המידע וביצוע סקרי סיכונים ומבדקי חדירות⁹¹. להלן הממצאים.

התקשרויות משרד החינוך עם ספקים

הרגולציה האירופית שמה דגש ב"עיצוב לפרטיות": הערכת הסיכונים הנשקפים לפרטיות עוד בשלב עיצוב המוצר ופעולה לצמצום, הגבלה לכתחילה של המידע שייאסף למידע הנחוץ באופן ספציפי לשירות הנדרש, והחזקתו רק אם המידע אכן נחוץ להפעלת אותו שירות.

"העיצוב לפרטיות", הביטוי הטכנולוגי לעקרון המידתיות, הנגזר מן הזכות החוקתית לפרטיות, אינו קבוע בחוק הגנת הפרטיות, אך היבט מצומצם שלו נכלל בתקנות אבטחת מידע המחייבות בעל מאגר מידע לבחון אחת לשנה "אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר"⁹².

בשנת 2011 פרסם רשם מאגרי המידע את ההנחיה⁹³ "שימוש בשרותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי" (להלן - הנחיית הרשם בנושא מיקור חוץ). על פי ההנחיה, יש כמה בדיקות מקדמיות שעל ארגון המזמין שירות מספק לעשות בקשר לשירות המבוקש, ובהן אם הארגון רשאי בכלל להוציא את המידע אל מחוץ לשליטתו ואם אפשר להסתפק בהרשאות גישה או עדכון למידע במאגר המידע ללא העברתו. ככלל, הנחת היסוד היא שככל שהמידע המועבר רגיש יותר, כך אמצעי אבטחת המידע צריכים להיות קפדניים יותר ונדרשת זהירות רבה יותר בבחירת הספק.

תקנה 15 לתקנות אבטחת מידע, הדומה ברובה להנחיית הרשם בנושא מיקור חוץ⁹⁴, מתייחסת להתקשרות עם ספק לצורך קבלת שירות הכרוך בגישה למאגר מידע של בעל המאגר, וגם בה מפורטת חובתו של בעל המאגר לבחון, לפני ההתקשרות עם הספק, את סיכוני אבטחת המידע הכרוכים בהתקשרות⁹⁵.

91 מבדקי חדירות (Penetration tests) הם מתקפות מתוכננות ומבוקרות על מערכת ממוחשבת הנעשית בידי בודק במטרה למצוא חולשות אבטחה ואת פוטנציאל הגישה אל המידע שהן מאחסנות.

92 סעיף 2(ג) לתקנות.

93 שמספרה 2/2011.

94 וראו גם המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע) באתר הרשות:

https://www.gov.il/he/Departments/Guides/data_security_guide

95 רשות התקשוב פרסמה הנחיות נוספות הנוגעות לתכנון והיערכות להתקשרות במיקור חוץ: כך למשל, הנחיה בנושא "היערכות לפעילות תקשורתית במיקור חוץ", בתוקף מ-1.12.17; וראו גם הנחיית רשות התקשוב הממשלתי בנושא "שיקולים בבחירת מיקור חוץ" בתוקף מ-16.7.17 והנחיה בנושא "מיקור חוץ - הנחיית אב", בתוקף מ-16.7.17.



אין גורם במשרד
החינוך שבוחן את
עצם הצורך בהוצאת
שירות הכרוך בגישה
למאגר מידע למיקור
חוץ, ולא נבחנים היקף
המידע האישי שנדרש
להעביר לצורך
אספקת השירות,
מטרת העברתו
לספק, ואם יש
חלופות שאינן כרוכות
בהעברת המידע

יצוין כי על פי תקנון שירות המדינה, האחריות להפעלת מערכות מידע ממוחשבות וסמכות ההחלטה בתחום זה נתונות בידי המנכ"ל של כל משרד משלתי ובידי מנהלי יחידות הסמך. במשרד החינוך פועלת ועדת היגוי לאבטחת מידע וסייבר, שחברים בה נציגים בכירים במשרד, בהם המשנה למנכ"ל⁹⁶.

כשמשרד החינוך שוקל התקשרות עם ספק, הכרוכה בגישה למאגרי המידע של המשרד או בהחזקת מאגרי המידע הללו בשרתי הספק, מצורף למכר "נספח אבטחת מידע" המנוסח בידי חטיבת אבטחת מידע שבמינהל תקשוב, טכנולוגיה ומערכות מידע (להלן - מינהל תקשוב), בהתאמה לדרישות המכרז. נספח אבטחת המידע, הכולל דרישות אבטחת מידע והוראות להגנת הפרטיות, כאמור בתקנות⁹⁷, הוא תנאי סף להתקשרות וחלק מההסכם עם הספק.

משנת 2013 ואילך היה מינהל תקשוב מעורב בהכנת כ-250 מכרזי רכש של שירותי מיקור חוץ עבור משרד החינוך. חלק מהמכרזים כללו דרישות לפיתוח תוכניות המבוססות על מאגרי מידע רגישים, כמו מכרז לפיתוח תוכנית לשילוב בני נוער בסיכון בפעולות התנדבות, מכרז להפעלת שירותי חינוך והשכלה לנוער מנותק, מכרז להפעלת תוכנית חינוכית לקליטה והשתלבות של תלמידים יוצאי אתיופיה במערכת החינוך, ועוד.

בביקורת נמצא, כי משרד החינוך אינו עושה בדיקות מקדמיות כנדרש בתקנות אבטחת מידע ובהנחיית הרשם בנושא מיקור חוץ, לפני פרסום מכרזים לשירותי מיקור חוץ, הכוללים גישה למאגרי מידע או קבלת מידע ממאגרי מידע שבבעלותו: אין גורם במשרד החינוך שבוחן את עצם הצורך בהוצאת השירות למיקור חוץ, ולא נבחנים היקף המידע האישי שנדרש להעביר לצורך אספקת השירות, מטרת העברתו לספק, ואם יש חלופות שאינן כרוכות בהעברת המידע. למעשה, הדרישות שבנספח אבטחת המידע המצורף למכרז נקבעות מבלי שנדונו ונענו השאלות המקדמיות האמורות.

עוד נמצא בביקורת כי משהתקבלו הצעות המציעים במכרזים, לא נעשת בדיקה עם מינהל תקשוב, הגורם המקצועי הרלוונטי, אם הספקים עומדים בדרישותיו של נספח אבטחת המידע שצורף למכרז.

96 על פי החלטה 2443 תפקידה של הוועדה לפעול לשיפור רמת הגנת הסייבר של המשרד, ולפיקוח על הפעילות השוטפת המבוצעת במשרד בתחום הגנת הסייבר. בהתאם להחלטה 2443, מנכ"ל המשרד הממשלתי הוא העומד בראש הוועדה.

97 דרישות לסיווג המידע, הוראות על הגנת המידע בשימוש, אחזקה או ניהול מאגר המידע, דרישה לאישור על עמידה בדרישות אבטחת מידע, ניהול סיכונים אבטחת מידע, שמירה על כללי אבטחה פיזית, סביבתית ולוגית (קביעת אמצעי אבטחה הולמים שימנעו חדירה למערכת המידע, עדכון המערכות למניעת ניצול פרצות אבטחת מידע ועוד), ותיעוד ובקרה על מערכות מידע בעלות גישה למאגרי המידע של משרד החינוך.

המצב חמור יותר בהתקשרות הפטורה ממכר⁹⁸. להסכם ההתקשרות עם הספק כלל לא מצורף נספח אבטחת מידע, ולמעשה אין גורם מקצועי במשרד החינוך המנסח דרישת עמידה בחובות וסטנדרטים של אבטחת מידע.

משרד החינוך ציין בתשובתו כי ככל שלא היה צורך במיקור חוץ, לא היה הנושא מובא לדיון בוועדת המכרזים, ולפעמים הוועדה אינה מאשרת קבלת שירות במיקור חוץ ודוחה את הבקשה (כגון כשמתבקשת העברה של סמכויות שלטוניות). עם זאת הוסיף המשרד כי יפעל לחידוד הנהלים כך שבכל מכרז לשירות שמועבר בו מידע אישי הוועדה תבחן את מטרת ההעברה, את היקף המידע ואם אפשר להסתפק בחלופות. עוד מסר המשרד על התקשרויות עם ספקים כי הפיקוח והבקרה על עמידת המציעים במכרזים בדרישות נספח אבטחת המידע ישולבו בתוכנית העבודה של מינהל תקשוב, וכי גם בהתקשרויות הפטורות ממכרז יופנו היחידות לחטיבת אבטחת מידע, כדי שתנסח עבורן דרישות אבטחת מידע.

משרד מבקר המדינה מעיר למשרד החינוך, כי עצם העובדה שהנושא הובא לדיון בוועדת המכרזים איננה מבטיחה שנעשתה בחינה מקדמית באופן שיטתי של עצם הצורך בהוצאת השירות למיקור חוץ, כאמור בתקנות אבטחת מידע והנחיית הרשם בנושא מיקור חוץ. לפיכך, ככל שהמידע המועבר רגיש ורב יותר, כן יש להקפיד יותר בהחלטה אם להוציא את השירות למיקור חוץ, בדרישות אבטחת המידע שייקבעו במכרז ובבחירת הספק.

במהלך הביקורת באוגוסט 2018 אישר משרד החינוך את ההנחיה המשרדית "העברת מידע מוגן בהתאם לחוק הגנת הפרטיות, תשמ"א-1981 ממאגרי מידע של המשרד", ובנובמבר 2018 הפיץ בקרב עובדי המשרד תוכנה ללמידת ההנחיה. ההנחיה מתייחסת למקרים שיש בהם צורך להעביר מידע מוגן ממערכות המידע המשרדיות, ומטרתה להבהיר את הפעולות הראויות על פי דין שיש לנקוט כשמתקבלות בקשות מסוג זה, למשל במקרים של העברת מידע או עיבוד מידע אישי בידי ספק חיצוני במסגרת התקשרות או מכרז.

משרד מבקר המדינה מעיר כי בנוסף להנחיה המשרדית, על הנהלת משרד החינוך להטמיע, לפני פרסום מכרזים להתקשרות עם ספקים, שלב מקדמי הכולל בחינה על פי הדרישות שבתקנות אבטחת מידע ובהנחיית הרשם בנושא מיקור חוץ.

98 ככלל, התקשרות משרד ממשלתי לביצוע עסקה לרכישת טובין, שירותים, עבודות או מקרקעין מחייבת ביצוע הליך מכרז פומבי. עם זאת, על פי תקנות חובת המכרזים, התשנ"ג-1993, במקרים מסוימים יכול להינתן פטור מעריכת מכרז בתנאים שנקבעו בהן. כך למשל, במקרה של התקשרות בחוזה לביצוע עבודה או לרכישת שירותים אשר שווה אינו עולה על 50,000 ש"ח.

בשנת 2015 התברר כי חיפוש באינטרנט מגלה מידע רגיש מאתר האינטרנט של ספק, ובו שמות של יותר מ-2,000 תלמידים ומורים. בדוח תחקיר האירוע הומלץ על בדיקת עמידתם של כלל הספקים בדרישות אבטחת המידע וחוק הגנת הפרטיות

פיקוח ובקרה על ספקים

על פי תקנות אבטחת מידע, בעל מאגר מידע המתקשר עם ספק יקבע במפורש בהסכם: את המידע שהספק רשאי לעבד ואת מטרות העיבוד; את המערכות שהספק רשאי לגשת אליהן; את סוגי העיבוד שהוא רשאי לבצע; את משך ההתקשרות ואופן השבתו של המידע לבעלים בסיומה; והנחיות על אמצעי אבטחת המידע שהספק יהיה חייב בהן. על בעל המאגר לנקוט אמצעי בקרה ופיקוח גם על עמידתו של הספק בהוראות ההסכם ובהוראותיהן של תקנות אבטחת מידע, בשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות.

גם בהנחיית הרשם בנושא מיקור חוץ נקבע כי יש לבצע פיקוח ומעקב שהספק מקיים את הוראות החוק והוראות ההסכם באמצעים טכנולוגיים מקובלים, כגון התקנת מערכות ניטור ובקרה, ככל שאפשר.

נמצא כי לאחר בחירתו של הספק הזוכה וכל תקופת ההתקשרות אתו, משרד החינוך לא עושה פעולות לבקרה ופיקוח בתחום אבטחת מידע, בהן בדיקת יישום הוראותיו של נספח אבטחת המידע, הגם שכבר ב-2014 ציינה חטיבת אבטחת מידע במינהל תקשוב את הצורך בבדיקת כשירותם של המועמדים במכרזים ובבקורות שוטפות על ספקים.

הצורך בבקרה ופיקוח על ספקים עלה גם מתחקור אירוע אבטחת מידע: בשנת 2015 התברר כי חיפוש באינטרנט מגלה מידע רגיש מאתר האינטרנט של ספק, ובו שמות של 2,000 ויותר תלמידים ומורים המלמדים אותם. בדוח תחקיר האירוע נכתב כי הספק לא עמד בדרישות מהותיות שנכללו בנספח אבטחת המידע שהתחייב לו. בדוח הומלץ לוודא שהמידע המוגן המצוי אצל הספקים השונים מאובטח בהתאם להוראות אבטחת מידע וחוק הגנת הפרטיות, והומלץ על בדיקת עמידתם של כלל הספקים בדרישות אבטחת המידע האמורות. המלצה ברוח דומה עלתה גם בתחקור אירוע אחר, שהתרחש בפברואר 2016, ונפרצו בו שני אתרי אינטרנט בית ספריים, הושתלו בהם מילים בוטות, תמונות מאיימות ומחקו מהם נתונים.

הרשות להגנת הפרטיות מסרה בתשובתה כי אירוע אבטחת המידע האמור מ-2015 טופל מול משרד החינוך והספק, ובעקבותיו נפתח ברשות תיק אכיפה רחבי להסדרת מדיניות הגנת הפרטיות בפורומים של משרד החינוך, ובמיוחד בפורומים הבית ספריים שמשותפים בהם תלמידים. נבדקו כ-400 אתרי אינטרנט שכללו מידע אישי רגיש של משתמשיהם. בממצאי הבדיקה נכללו הנחיות לתיקון ליקויים בתחומי הגנת הפרטיות.

משרד מבקר המדינה מעיר למשרד החינוך, כי בהתאם לתקנות אבטחת מידע עליו לפקח על עמידתם של ספקים בדרישות אבטחת מידע שנכללו בהסכמים עימם נוכח ההשלכות ופוטנציאל הפגיעה בפרטיות התלמידים, כדי להפחית את הסיכון שאירוע של גילוי מידע רגיש על תלמידים באינטרנט יישנה. בנסיבות הקיימות, של היעדר בדיקות שיבטיחו את הגנת המידע האישי המצוי במאגרי המשרד ומועבר לידי ספקים חיצוניים, נשקפת סכנה לפרטיותם של נושאי המידע, בהם תלמידים ומשפחותיהם. הדברים מקבלים משנה תוקף נוכח אירועי אבטחת מידע באתרים בית ספריים, ודורשים בחינה של כלל הספקים.

משרד החינוך השיב, כי פיקוח ובקרה על יישומן של הוראות אבטחת המידע בידי הספק ישולבו בתוכנית העבודה של מינהל תקשוב, וציין כי בעקבות אירוע אבטחת המידע הורה על ביצוע בדיקות חדירות אצל כלל ספקי המשרד.

אבטחת מידע במוסדות חינוך

בתי ספר רבים מקימים מאגרי מידע מקומיים לשימושם, חלקם מכילים רשימות תלמידים שננקטו לגביהם פעולות חינוכיות שונות, רשימות תלמידים בעלי בעיות משפחתיות או כלכליות ועוד. דוגמה למאגר מידע המכיל פרטים רבים על תלמידים, משפחותיהם וצוותי ההוראה בבתי הספר היא מערכת המנב"ס-נט⁹⁹. התוכנות הנלוות למערכת זאת כוללות אף מידע על לקויות למידה ובעיות רפואיות שונות של תלמידים.

בחוזר המנכ"ל "מאגרי מידע בבתי הספר - רישום, דיווח ואבטחת מידע" מנובמבר 2009, קבועות הוראות המסדירות את אבטחת המידע שמצוי במאגרים של בתי הספר, חובת מינוי ממונה אבטחת מידע בבית הספר, מיפוי כל מאגרי המידע, מתן הרשאות גישה לפי הצורך ועוד. לפיקוח על יישומן של הוראות החוזר אחראי מינהל תקשוב.

לצד התקשרויות של יחידות משרד החינוך עם ספקים נתונה למנהליהם של מוסדות חינוך האפשרות להתקשר במישרין עם ספקים כדי להפעיל מוצרים טכנולוגיים שונים, כמו יישומונים, אתר אינטרנט בית ספרי וסביבות למידה מתוקשבות. מנהלי בתי הספר¹⁰⁰ מונחים שלא להתקשר אלא עם ספקים שאישר המשרד (להלן - ספקי החינוך)¹⁰¹. תנאי סף לקבלת אישור זה הוא התחייבות הספק לעמידה ב"תקן אבטחת מידע - גרסה 2.5" מדצמבר 2016 -

99 מנב"ס-נט היא מערכת מינהל בית ספרי אינטרנטית שפיתח מינהל תקשוב ומיועדת לתמוך בניהול המידע בבתי הספר, לרבות בניית מערכת שעות, דיווח מהלכי שיעור, דיווח נוכחות תלמידים והתנהגויות, ניהול הערכות תלמידים ודיווח מצבת עובדי הוראה. הגישה למערכת אפשרית מכל עמדה המחוברת לאינטרנט.

100 בפרט לאור המעבר של בתי הספר היסודיים לשיטת "ניהול עצמי", הכוללת מתן אוטונומיה וסמכות לבתי הספר תוך העברת המשאבים אליהם.

101 במידע הקיים באתר משרד החינוך בקשר ל"פורטל הבית ספרי" מפורטים פרטי הספקים המאושרים לשימוש על ידי משרד החינוך.

מקבץ של דרישות אבטחת מידע שקבע משרד החינוך לספקי מוצרים חינוכיים טכנולוגיים. על פי נתוני משרד החינוך, יש 72 ספקי חינוך המספקים למוסדות חינוך 105 שירותים טכנולוגיים, מוצרי תוכנה ותכנים דיגיטליים.

במרץ 2018 התרחש אירוע דליפת מידע רגיש מיישומון שפיתח אחד מספקי החינוך. היישומון מאפשר לצוותים של גני ילדים לתקשר עם הורים ולחלוק איתם תמונות, מידע אישי ולוח אירועים של גן הילדים. המידע שדלף מן היישומון חשף באינטרנט כשישה מיליון תמונות של ילדים ופרטים של יותר מ-100,000 הורים. דליפת המידע טופלה בידי הרשות להגנת הפרטיות ובמועד סיום הביקורת טרם נסתיימו פעולות האכיפה בקשר לאירוע.

בעקבות האירוע ובהנחיית סמנכ"ל תקשוב, טכנולוגיה ומערכות מידע במשרד החינוך, פתח המשרד בבדיקות אבטחת המידע לכלל המוצרים של ספקי החינוך. לנציגי משרד מבקר המדינה נמסר כי בסוף 2018 הושלמו פעולות הבקרה על כלל ספקי החינוך, והמשרד מתכנן לבצע בשנת 2019 בדיקות שוטפות שנתיות ואף רבעוניות של כלל ספקי החינוך.

משרד החינוך מעודד את בתי הספר לנהל את התכנים והידע המקומיים בסביבות ענן¹⁰² שקיבלו את אישורו, לרבות תיבות דוא"ל ארגוניות מאובטחות. עם זאת, כיוון שהמידע נשמר בשרתים של חברות מסחריות, בתי הספר הונחו להימנע בסביבות אלה משימוש במידע אישי, בעיקר מספרי זיהוי, תאריכי לידה, כתובות, וכדומה. על צוותי ההוראה נאסר להשתמש בתיבות דוא"ל פרטיות אלא בתיבות הדואר הארגוניות המאובטחות¹⁰³. נוסף על כך, חלות על עובדי משרד החינוך הנחיות ארכיון המדינה, המחייבות אותם לנהל את הדוא"ל שלהם בתיבת הדואר הארגונית-ממשלתית ולא בפרטית, ולהפריד בין דואר פרטי לארגוני.

הביקורת העלתה כי הגם שהוקצו לעובדי משרד החינוך תיבות דוא"ל ארגוניות במערכת "יונת דואר", כמעט שלא נעשה בהן שימוש. מדוח פעילות שהופק עבור משרד מבקר המדינה ביולי 2018 עולה, שאף כי בתיבות הדואר של המערכת מתקבלות הודעות רבות, מספר המשתמשים השולחים הודעות באמצעות המערכת הוא אפסי¹⁰⁴.

102 "מחשוב ענן" הוא שירותי מחשוב הניתנים למשתמש באמצעות מחשב מרוחק אליו מתחבר המשתמש דרך רשת האינטרנט או קו תקשורת ייעודי. בחיבור כזה המשתמשים אינם צריכים לרכוש ולנהל מערכות מחשוב אלא שוכרים את שירות "סביבת הענן" מספקים המעמידים כוח מחשוב שהגישה אליו היא מרוחק. בסביבת ענן הניתנת לבתי הספר ניתן לבצע יצירה ושמירה של מסמכים, עריכה ושיתוף של התכנים החינוכיים, למידה משותפת, השתתפות בכיתות וירטואליות ועוד.

http://sites.education.gov.il/cloud/home/svivot_anan_hinuch/Pages/havtacha.aspx

103 ראו לעניין זה:

http://sites.education.gov.il/cloud/home/tikshuv/Documents/hanchayot_havtachat_mida_batisefer.pdf

104 ההערכה היא שההודעות שמתקבלות לתיבות הדואר הן הודעות ארגוניות הנשלחות על ידי גורמים במשרד החינוך לעובדיו.



בסקר אבטחת המידע
נמצא כי אין בבתי
הספר תקן אחד
לשמירה ולגיבוי של
מידע. הגיבויים נעשים
על פי שיקול דעת
מקומי ובמקרים רבים
באופן לא מאובטח.
עוד נמצא, כי מידע
פדגוגי ואישי על
תלמידים מועבר בבתי
הספר בתיבות דוא"ל
פרטיות שאינן
מאובטחות

בחדשים מאי-יולי 2017 ערך משרד החינוך סקר אבטחת מידע שנועד למפות את הפערים הקיימים בתחום אבטחת המידע ב-406 בתי ספר ברחבי הארץ, ולבנות תוכנית עבודה ארוכת טווח לצמצום הפערים שיימצאו.

בסקר אבטחת המידע נמצא, בין היתר, כי אין בבתי הספר תקן אחד לשמירה ולגיבוי של מידע. הגיבויים נעשים על פי שיקול דעת מקומי ובמקרים רבים באופן לא מאובטח. למשל, 28% מבתי הספר שהשתתפו בסקר דיווחו כי הם מגבים מידע בהתקן נייד, המהווה סיכון לאבטחת המידע. עוד נמצא, כי מידע פדגוגי ואישי על תלמידים מועבר בבתי הספר בתיבות דוא"ל פרטיות שאינן מאובטחות.

במסמך סיכום הסקר מיולי 2017 הומלץ על הגדרת מדיניות משרדית לגיבוי המחשבים ומערכות המידע בבתי הספר, אשר תכלול הנחיה על המידע שיש לגבות, על אופן הגיבוי ועל תדירותו. עוד הומלץ, על מציאת פתרון טכנולוגי מאובטח לגיבוי המידע, ועל אכיפת חובת השימוש בתיבות הדוא"ל המאושרות בידי משרד החינוך לצורכי העבודה בבתי הספר והתקשורת עם הורים ותלמידים.

בעקבות הסקר פרסם משרד החינוך באוגוסט 2017 עלוני מודעות והנחיות אבטחת מידע לבתי הספר הכוללים הוראות לניהול גישה והרשאות למערכות המכילות מידע על תלמידים, לטיפול באירועי אבטחת מידע, לשימוש בדוא"ל ארגוני מאובטח בלבד ולגיבוי המידע המצוי בבתי הספר.

נמצא כי מעבר להנחיות המפורסמות באתר המשרד ובעלון אבטחת המידע שנשלח לבתי הספר, לא התקבלה החלטה מעשית על אכיפת האיסור לעשות שימוש בתיבות דוא"ל פרטיות להעברת מידע פדגוגי או אישי על תלמידים.

משרד החינוך השיב, כי הוא מייחס חשיבות רבה לאבטחת מידע ולהגנת הפרטיות והוא פועל לצמצום השימוש בתיבות דוא"ל פרטיות, באמצעות הנחיות אבטחת מידע ובביקורות אבטחת מידע על מוסדות חינוך, שבמסגרתן כל בית ספר שעבר בקרה מקבל דוח ליקויים.

משרד מבקר המדינה מעיר למשרד החינוך, כי עליו לזהות את הסיבות להימנעותם של צוותי ההוראה משימוש בתיבות הדוא"ל הארגוניות ולפעול ביתר תקיפות להגברת השימוש בהן. נדרשת גם בחינה של השימוש השכיח ביישומונים להעברת מסרים וברשתות החברתיות, האם גם בהם מועבר מידע מוגן או רגיש, ואם כן, לבחון דרכי טיפול בכך.

מדיניות אבטחת מידע ומיפוי מאגרי המידע שבבעלות משרד החינוך

1. על פי החלטה 2443 מפברואר 2015, על המנכ"לים של משרדי הממשלה להגדיר תוכנית מדורגת להטמעה, התעדה¹⁰⁵ והסמכה לתקן אבטחת מידע ארגוני - ISO27001 (להלן - תקן 27001)¹⁰⁶. תקן זה מפרט דרישות ליישום אמצעי בקרת אבטחה המותאמים לצורכי הארגון כדי להגן על "נכסי מידע"¹⁰⁷.

הביקורת העלתה כי רק בשנת 2018 החל משרד החינוך בהטמעת תקן 27001, ועל פי ההערכות, מועד עמידתו של המשרד בדרישות אבטחת המידע שבתקן יהיה יוני 2019.

2. בהתאם להחלטה 2443 הקים משרד החינוך יחידה להגנה בסייבר שמטרתה להעלות את רמת הגנת הסייבר של הגופים המפוקחים על ידי משרד החינוך, בהתאם לתהליך ניהול סיכונים ארגוני. בהתאם להנחיית המסגרת והנחייה בנושא "מדיניות להגנת הסייבר בממשלה" שפרסמה יה"ב בספטמבר 2016, על הנהלות משרדי הממשלה לפעול בהתאם לעקרונות מדיניות הגנת סייבר, המבוססת על סיכונים למידע, תוך התאמה לצרכים התפעוליים והארגוניים של המשרד. על פי ההנחיה, פגיעה במידע עלולה לגרום לנזקים תפעוליים, טכנולוגיים וכספיים הקשורים לביטחון ולשלומו של אדם או של הציבור, וכן להוביל לפגיעה בפרטיות של אזרחי המדינה.

באוקטובר 2017 נעשה במשרד החינוך "סקר סיכוני אבטחת מידע על תשתיות המשרד" (להלן - סקר סיכוני אבטחת מידע), באמצעות חברה פרטית. סקר הסיכונים העלה צורך בעדכון מדיניות אבטחת המידע המשרדית, פיתוח יכולת התיעוד והטיפול באירועי אבטחת מידע וקיום סקרים נוספים לבקרת האבטחה במערכות המשרד.

נכון למועד סיום הביקורת אין למשרד החינוך מדיניות אבטחת מידע וסייבר מאושרת.

105 תהליך שבו גורם מקצועי מאשר שתהליך מסוים או שירות תואם דרישות מוגדרות.

106 תקן 27001 הוא אחד התקנים הלא-רשמיים שפרסם מכון התקנים הישראלי העוסק במיסוד מערכת לניהול אבטחת מידע ארגונית. התקן שימש כנורמה מקיפה לאבטחת מידע בארגונים עד להחלטה 2443 אשר קבעה, כאמור, את הדרישה ממשרדי הממשלה לעמוד בתקן זה על פי התכנית שפורטה בהחלטה.

107 "נכסי המידע" מוגדרים בהנחיית המסגרת: "המידע, מערכות המחשוב המעבדות ומאחסנות אותו והתקשורת, האמצעים והציוד עליו הוא מושתת".

עד מועד סיום הביקורת לא היה למשרד החינוך מיפוי של מאגרי המידע שלו או רשימת מצאי של מערכות המידע. הפעילות למיפוי מאגרי המידע נמצאת רק בראשית דרכה, והיא חלק מעבודת המשרד להסמכה לתקן ישראלי העוסק באבטחת מידע ארגוני

משרד החינוך מסר למשרד מבקר המדינה, כי הליך אישור מדיניות אבטחת מידע וסייבר ייעשה כחלק מההסמכה לתקן 27001 כאמור והוא מדווח על ההתקדמות בהליך הטמעת התקן לתקשוב הממשלתי.

3. בהחלטת ממשלה 1933¹⁰⁸ נקבע, כי עד סוף שנת 2017 על כל משרד ממשלתי להשלים תהליך של מיפוי מאגרי המידע המצויים ברשותו ולשלב בתכניות העבודה השנתיות פעילות להנגשת מאגרי המידע. החלטה זו משקפת את תפיסת השקיפות השלטונית שאומצה בישראל במספר החלטות ממשלה הכוללות גם שיקולי הגנת הפרטיות במסגרת יישומן. חובת המיפוי וההכנה של רשימת מצאי מעודכנת של מאגרי המידע קיימת גם מכוח תקנות אבטחת מידע ותקן 27001¹⁰⁹.

במועד הביקורת, על פי הערכת מינהל תקשוב מתוך כ-150 מאגרי מידע של משרד החינוך היו רשומים בפנקס מאגרי המידע שברשות להגנת הפרטיות רק כ-33 מאגרים.

עד מועד סיום הביקורת לא היה למשרד החינוך מיפוי של מאגרי המידע שלו או רשימת מצאי של מערכות המידע. עוד עלה, כי הפעילות למיפוי מאגרי המידע נמצאת רק בראשית דרכה כחלק מעבודת המשרד להסמכה לתקן 27001.

העדר מיפוי מאגרי המידע של משרד החינוך והצורך למפות את כלל הנכסים הארגוניים, עלו גם בסקר סיכוני אבטחת המידע מאוקטובר 2017.

משרד החינוך מסר בתשובתו כי הוא פועל ליישום של החלטה 2443, של תקן אבטחת מידע 27001 ולעמידה בתקנות אבטחת מידע החדשות, לרבות מיפוי כל מאגרי המידע המשרדיים.

זאת ועוד, הועלה כי באגף הרכש והמכרזים במשרד החינוך אין רשימה מרוכזת של ספקים שזכו במכרזים, ולפיכך למעשה אין למשרד החינוך תמונה מלאה על אותם ספקים המחזיקים במאגרי מידע, ואין דרך ליישם את הוראות התקנות וההנחיות השונות המחייבות למפות ולסווג את סוגי המידע ואת הסיכונים הנוגעים לאבטחתם.

על משרד החינוך למפות את הספקים שיש לו התקשרות עימם ולפעול למפות ולסווג את מאגרי המידע שברשותם ואת הסיכונים הנוגעים לאבטחתם.

108 החלטת ממשלה מס' 1933 מ-30.8.16 בנושא "שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור".

109 יצוין כי גם במסגרת פרויקט "הסדרת מערך המידע" נעשה מיפוי של מאגרי המידע המשרדיים אך הוא שונה במאפייניו מהמיפוי הנדרש על פי תקנות אבטחת מידע והחלטה 1933.

סקרי סיכונים ובדיקות חדירות

על פי תקנות אבטחת מידע, יש חובה לערוך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים) ומבדקי חדירות על מאגרי מידע הטעונים רמת אבטחה גבוהה, אחת ל-18 חודשים לפחות, כדי לבחון את עמידותם לסיכונים פנימיים וחיצוניים. ניהול הסיכונים הוא תהליך מחזורי המורכב מכמה שלבים: זיהוי הסיכון, הערכת הסיכון בהקשר של תהליכים ארגוניים, קביעת הטיפול בסיכון והטמעת הטיפול בתוכנית עבודה, מדידת תוצאות לאחר ההטמעה וביצוע פעילות מתקנת.

גם על פי תקן 27001 קיימת חובה לקיים מערכת לניהול אבטחת מידע ארגונית, שתכלול זיהוי של הסיכונים לנכסי המידע, ניתוח ומדידה של הסיכונים, בחירה של אמצעי בקרה לטיפול בסיכונים ועוד.

על פי החלטת ממשלה 2097 מאוקטובר 2014¹¹⁰, בתחומי הפעילות של התקשוב הממשלתי כלולים, בין היתר, גיבוש מדיניות לניהול סיכוני תקשוב, סיוע בהטמעת מתודולוגיה לניהול סיכוני תקשוב באגפי מערכות המידע והטמעת חובות אבטחת מידע לפי דין. התקשוב הממשלתי אחראי לסייע למשרדי הממשלה בהנעת סקרים של סיכוני תקשוב וביישום תוכניות להפחתת הסיכונים, גם באמצעות הכלים הטכנולוגיים הממשלתיים. בהתאם להחלטה 2097, ראש רשות התקשוב הממשלתי פרסם כמה הנחיות לניהול סיכוני תקשוב שעל משרדי הממשלה לבצע. אלה רק חלק מהבקורות הנדרשות בתחום הגנת הסייבר, ותורת ההגנה כוללת מבדקים נוספים.

מסקר של סיכוני אבטחת המידע מאוקטובר 2017 עולה, כי נעשו מבדקי חדירות בשש מעשרים המערכות המשרדיות. מבדקי החדירות העלו ממצאים חמורים, בהם האפשרות לקבל שליטה מהירה על כל המידע המשרדי, גניבתו ומחיקתו. במועד סיום הביקורת היה הטיפול בליקויים שנמצאו במבדקי החדירות תלוי בטיפולם של גורמים במינהל תקשוב, ורק בחלקם היה קצב הטיפול סביר. משרד מבקר המדינה מעיר למשרד החינוך כי עליו לנקוט פעולה נמרצת לתיקון הליקויים שנמצאו במבדקי החדירות מאוקטובר 2017.

משרד החינוך השיב, כי עצם ביצוע יזום של סקר אבטחת מידע מלמד על החשיבות שהוא מייחס לאבטחת מידע ולהגנת הפרטיות. זאת ועוד, תוכנית העבודה עודכנה על פי ממצאי הסקר, ממצאים חמורים טופלו לאלתר ולגבי שאר הליקויים נערכו פגישות עם מנהלי המערכות להצגת הממצאים ולקבלת לוחות זמנים לטיפול בליקויים.



110 החלטת ממשלה מס' 2097 מ-10.10.14 בנושא "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'".

ככל שהסיכונים הכרוכים במערכות מידע ממוחשבות נעשים שכיחים יותר, דרושות פעולות נחרצות יותר של משרדי הממשלה לאבטחת המידע ולהגנה על פרטיותם של נושאי המידע. הממצאים בפרק זה מציגים תמונה מדאיגה ובה אין למשרד החינוך תמונה מלאה ומפורטת, כנדרש בדין, של מאגרי המידע שלו או של הספקים המחזיקים במאגרי המידע שלו; מערכות המידע של הספקים המחזיקים במידע אישי רגיש על תלמידים ועל משפחותיהם אינן נבדקות לא בשלב בחינת ההתקשרות ולא במהלך תקופת ההתקשרות; ואין בקרה ופיקוח על הספקים בהיבטי אבטחת מידע והגנה על הפרטיות. בנסיבות אלה יש חשש כבד לאבטחת המידע ולהגנת הפרטיות של נושאי המידע.

משרד מבקר המדינה מעיר להנהלת משרד החינוך, כי מחויבות ההנהלה היא חלק בלתי נפרד ממדיניות האבטחה של כל ארגון והיא חשובה במיוחד לנוכח הממצאים המובאים בפרק זה ולנוכח השלכותיהם. כך גם עולה מן ההנחיות בתחום הגנת הסייבר והתקינה הבין-לאומית¹¹¹. על מנכ"ל המשרד להתגייס להכוונה ברורה של הגורמים האחראים לאבטחת המידע המשרדי, כדי ליצור מחויבות ואחריות כוללת. יש לנקוט פעולה נמרצת לצמצום הפערים בין דרישות הדין ובין המצב הקיים במשרד, ולפעול בנחישות להגנה אפקטיבית על הזכות לפרטיותם של תלמידים ומשפחותיהם, כנדרש בדין.

הגנת הפרטיות במידע רפואי

מידע רפואי הוא מסוגי המידע הרגישים ביותר ושמירה על סודיותו היא תנאי הכרחי לאמון המטופל ברופא ולעידודו לתת לרופא מידע שלם ואמיתי על מצבו הרפואי. בשאלון לציבור שערכה הרשות במסגרת השינוי הארגוני שעברה, ציינו הנשאלים כי מידע רפואי נחשב בעיניהם כמידע הרגיש והפרטי ביותר הנאסף כיום במערכות מידע.

חוק הגנת הפרטיות קובע כי מידע על מצבו הבריאותי של אדם הוא בגדר מידע רגיש, ובחוק זכויות החולה התשנ"ו-1996 (להלן - חוק זכויות החולה) אף זכתה הזכות לסודיות המידע הרפואי להגנה נוספת על הזכות לפרטיות שנקבעה בחוק היסוד ובחוק הגנת הפרטיות.

לצד החשיבות הרבה של חובת הסודיות, לימינותו ולשלמותו של המידע הרפואי של המטופל עשויה להיות חשיבות רבה לצורך טיפולים נוספים, לצורך שמירה על אינטרסים של הציבור, ובראשם בריאות הציבור, ולצורכי מחקר רפואי. לכן, חוק זכויות החולה קובע את המקרים שמטפל או מוסד רפואי רשאים למסור בהם מידע רפואי: בהסכמת המטופל; למטפל אחר לצורך טיפול במטופל אחר; למטרות מחקר או הוראה, ובלבד שלא נחשפו פרטים מזהים של המטופל. עוד

111 סעיף 5 להנחיית המסגרת וסעיף 5 בתקן 27001 בנושא "אחריות הנהלה".



האתגר שבשמירת פרטיותו של המטופל גדל והולך ככל שהטכנולוגיה מתפתחת, ועימה דרכי שמירת המידע. בהתפתחות הטכנולוגית כרוכים סיכונים ייחודיים בתחום ההגנה על המידע, ובכלל זה גניבת מידע רפואי, מניעת שירות ושיבוש המידע הקיים

קובע החוק כי לא יימסר המידע אלא במידה הנדרשת לצורך העניין, ותוך הימנעות מרבית מחשיפת זהותו של המטופל.

האתגר שבשמירת פרטיותו של המטופל גדל והולך ככל שהטכנולוגיה מתפתחת, ועימה דרכי שמירת המידע. בעבר היה מידע על המטופל מתועד ברשומות נייר ומפוזר במקומות שונים, וכיום הוא נשמר במדיה דיגיטלית וניתן לחבר בין כל מקורות המידע הרפואי ולהעבירם בקלות ובמהירות. ואולם בהתפתחות הטכנולוגית כרוכים סיכונים ייחודיים בתחום ההגנה על המידע ובכלל זה גניבת מידע רפואי, מניעת שירות ושיבוש המידע הקיים, שעשויים להיות להם השלכות קשות על הפרט ועל אמונו של הציבור במוסדות הרפואיים במדינה.

משרד הבריאות נושא באחריות הממלכתית להבטחת שירותי הבריאות לתושבי המדינה. המשרד קובע את המדיניות לשירותי הבריאות והרפואה, ומופקד על תכנון שירותיה של מערכת הבריאות, הפיקוח עליהם, בקרתם, רישום ותיאומם. המשרד עוסק גם במחקר בעצמו ובאמצעות מוסדות רפואיים. במסגרת אחריותו הוא נדרש לפקח על התנהלותם של המוסדות הרפואיים, לרבות בנושא הגנת הפרטיות ואבטחת מידע.

נהלי משרד הבריאות בתחום אבטחת מידע והגנת הפרטיות

למשרד הבריאות הנחיות רבות בתחום אבטחת מידע והגנת הפרטיות במאגרי מידע¹¹². נוסף עליהם יש נהלים של יחידות במשרד הבריאות הנוגעות לעניינים אלה, כגון הנחיות אגף המחשוב בנושא אבטחת מידע. ריבוי הכללים ופיזורם בנהלים שונים מצריך ריכוזם והנגשתם לקהל היעד שלהם במשרד ובמוסדות הרפואיים.

במסקנותיה של ועדה שהוקמה במשרד הבריאות בעניין ההגנה על פרטיות¹¹³, נקבע כי יש לתקף את נהלי אבטחת המידע של המשרד ולהנגיש אותם למערכת הבריאות ולכלל הציבור, שכן הם אינם עדכניים ואינם זמינים אלא בפורטל הפנימי של משרד הבריאות.

בעקבות המלצות הוועדה פורסמה טיוטת קוד אתי, הצפויה להתפרסם בחוזר מנכ"ל, המתייחסת לצילום מטופלים באמצעות התקנים פרטיים שאינם

112 העיקריים שבהם הם חוזרי מנכ"ל 3/15 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות"; 12/15 בנושא "העברת מידע ושמירת מידע בתחום בריאות הנפש"; 5/14 בנושא "שיתוף מידע רפואי במדינת ישראל" (לא בתוקף); 1/18 בנושא "שימושים משניים במידע בריאות"; 2/18 בנושא "שיתופי פעולה המבוססים על שימושים משניים במידע בריאות". ראוי לציין גם את חוזרי מנכ"ל 4/96 בנושא "הסודיות הרפואית וצנעת הפרט", ו-19/96 בנושא "הסודיות הרפואית", המפרטים את הבסיס העקרוני של חובת הסודיות הרפואית.

113 מסקנות ראשוניות, הוועדה להתמודדות עם איום הפגיעה בפרטיות המטופל ובסודיות המידע הרפואי וגיבוש תכנית פעולה לצמצום התופעה ומיגורה, אוגוסט 2017.

מאובטחים (סלולרי, טאבלט). על פי הטיוטה אין לצלם מטופלים ואין לפרסם תמונות וסרטונים של מטופלים באמצעות התקנים כאמור ללא הסכמתם.

למשרד הבריאות אין ריכוז של כל הנחיותיו הרלוונטיות לאבטחת מידע ולהגנת הפרטיות. ריכוז ההנחיות והנגשתן חשובים לאנשי אבטחת המידע והגנת הפרטיות במוסדות הרפואיים, שכן בכוחו לסייע בידם לעמוד בכלל ההנחיות שהם נדרשים ליישם ולהתעדכן בשינויים החלים בהן מדי פעם. על משרד הבריאות לפעול לבחינה ולתיקוף של ההנחיות בהתאם להמלצות הוועדה ולפעול להנגשתן לקהל היעד שלהן.

אבטחה של מערכות מידע רפואי

בתחום אבטחת המידע והגנת הסייבר של מערכות מידע ממוחשבות יש הסדרים נורמטיביים רבים. למן כניסתן לתוקף של תקנות אבטחת מידע במאי 2018, כל גורמיה של מערכת הבריאות המחזיקים מידע אישי מחויבים ברמת אבטחה לפי מאפייני המוסד הרפואי שהם עובדים בו, בהתאם למבחנים שנקבעו בתקנות.

כבר בשנת 2015, הנחה חוזר מנכ"ל משרד הבריאות 3/15 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" (להלן - חוזר אבטחת מידע), את המוסדות הרפואיים על אבטחת מידע רפואי שברשותם. חוזר אבטחת מידע חל על קופות חולים, בתי חולים ומרפאות שהוגדרו בו כ"מרפאה בה פועלים חמישה מטפלים לפחות" (להלן כולם יחד - מוסדות רפואיים). הגדרת מרפאה בחוזר המנכ"ל היא רחבה וכוללת גם מרפאות פרטיות בתחומי רפואה שונים שאינן טעונות רישיון ממשרד הבריאות¹¹⁴, ובלבד שהרופאים פועלים במשותף במסגרת המרפאה למתן שירות בתחום רפואי מסוים¹¹⁵. החוזר אינו מבדיל בין המוסדות השונים לפי גודלם ואופי פעילותם והכללים שנקבעו בו זהים לכולם.

עוד קובע החוזר כי מטפל העובד במסגרת שיש בה פחות מחמישה מטפלים, אחראי באופן אישי להגנה על המידע הרפואי הנוצר והנאגר אצלו על מטופליו.

עמידה בתקן לניהול אבטחת מידע במערכות בריאות: חוזר אבטחת מידע קובע כי על המוסדות הרפואיים לקבל הסמכה לתקן ישראלי 27799 (ISO) העוסק בניהול אבטחת מידע במערכות בריאות¹¹⁶ (להלן - התקן), וכי תהליכי אבטחת המידע בהתאם לתקן יוטמעו בכלל המערכות במוסד הרפואי ובכלל זה

114 בהתאם לפקודת בריאות העם, 1940, והתקנות שהותקנו מכוחה, חלה חובת רישוי של מוסדות רפואיים מסוגים שונים.

115 כגון מרפאה פרטית לבריאות הנפש או מרפאת שיניים ולהבדיל ממספר רופאים המצויים פיזית במרפאה אחת אך ללא קשר ביניהם (למעט שירותי משרד וכד').

116 תקן בין-לאומי (ISO) לאבטחת מערכות מידע בתחום הבריאות שאומץ בישראל, מהווה תקן לווה לתקן אבטחת מידע ISO 27001 וקובע כללים מחמירים יותר לאור רגישות המידע הרפואי.

מכ-1,500 מוסדות
רפואיים הטעונים
רישיון, כ-150 בלבד
קיבלו הסמכה לתקן
(בעיקר בתי חולים
וקופות חולים)

מערכות המידע, המכשור הרפואי, מערכות הלוגיסטיקה וכוח האדם. עוד נקבע בחוזר, כי מ-1.14.14 עמידה בתקן היא תנאי לרישוי של מוסד רפואי והיא תיבדק במסגרת הבקורות שעורך משרד הבריאות. החוזר קובע חובות נוספות בתחום אבטחת המידע ובכלל זה בקשר להתקשרויות עם ספקים, קיום בקרות, ביצוע תיעוד וניטור של גישות משתמשים למערכות המידע הרפואי והחובה למנות ממונה אבטחת מידע.

בביקורת נמצא כי על אף האמור בחוזר אבטחת מידע, מכלל כ-1,500 מוסדות רפואיים¹¹⁷ הטעונים רישיון כ-150 בלבד קיבלו הסמכה לתקן¹¹⁸ (בעיקר בתי חולים וקופות חולים). שאר המוסדות הטעונים רישיון, ובהם בתי חולים גריאטריים, מרכזים למשתמשים בסמים ומרפאות שיניים, לא קיבלו הסמכה לתקן ומשרד הבריאות אינו אוכף עליהם חובה זאת.

עוד העלתה הביקורת כי גם מרפאות רבות אחרות, שחוזר אבטחת מידע חל עליהן על אף שאינן טעונות רישיון ממשרד הבריאות, לא קיבלו הסמכה לתקן ומשרד הבריאות אינו אוכף עליהן חובה זאת. במועד סיום הביקורת המשרד אף אינו מחזיק ברשימת המוסדות המוסמכים לתקן - מוסדות טעוני רישיון ושאנים טעוני רישיון.

משרד מבקר המדינה מעיר למשרד הבריאות, כי עליו למפות את המוסדות הטעונים רישיון שאינם מחזיקים בהסמכה לתקן ולהניעם להשגת ההסמכה הנדרשת. בהמשך עליו לבחון דרכים להניע גם מרפאות שאינן טעונות רישיון לעמוד בהוראות חוזר אבטחת מידע, לרבות עמידה בתקן. במסגרת זו עליו לבחון אם נכון לקבוע מדרג של דרישות אבטחת מידע למרפאות לפי גודלן ובהתאם לאופי פעילותן.

בתשובתו למשרד מבקר המדינה מדצמבר 2018 כתב משרד הבריאות כי מכוחן של תקנות אבטחת המידע, על כל מנהל של מוסד רפואי מוטלת האחריות לשמירת הסודיות הרפואית, גם אם המוסד אינו טעון רישיון. עוד נכתב בתשובת משרד הבריאות, כי הוא בודק עמידה בתנאי התקן במסגרת בקורותיו במוסדות רפואיים. המשרד הוסיף כי תקנות אבטחת המידע מחייבות אותו לבחון מחדש את הנחיותיו בתחום ולהיערך בהתאם - תהליך שכבר החל סמוך לפרסום התקנות, ובמסגרתו יהיה אפשר לשקול קביעת מדרג של דרישות למרפאות בהתאם לגודלן ולאופי פעילותן.

117 ביניהם כ-50 בתי חולים, 4 קופות חולים, כ-230 מוסדות סיעוד גריאטריים, כ-900 מרפאות שיניים, כ-60 מוסדות לטיפול במשתמשים בסמים, כ-40 מרפאות דיאליזה וכ-13 מוסדות לבריאות הנפש.

118 בישראל שני גופי התעדה - מכון התקנים והמכון לבקרה ואיכות (IQC) - המעניקים את ההסמכה לתקן. נכון לאוגוסט 2018 יש 123 גופים בעלי הסמכה לתקן ממכון התקנים, מרביתם מוסדות רפואיים הטעונים רישיון ומיעוטם גופים אחרים (כגון ספקים הפועלים מול מוסדות רפואיים שבהתאם לחוזר 3/15 נדרשים אף הם לעמוד בתקן). כמו כן נכון למועד האמור, יש כ-50 גופים שהמכון לבקרה ואיכות (IQC) העניק להם הסמכה כאמור, חלקם מוסדות בריאות הטעונים רישיון וחלקם גופים אחרים.



תיעוד ובקרה של
הפעולות המבוצעות
במערכות המידע הם
מן הדרישות
החשובות ביותר
לאבטחתו של מידע
רפואי אישי, ונועדו
לסייע בחשיפת
שימוש לא ראוי
במערכות אלה או
במידע שבהן

משרד מבקר המדינה מעיר למשרד הבריאות, כי הבקורות שהוא עורך לעמידה בהוראות התקן מתקיימות במוסדות שכבר הוסמכו לתקן ועל שאר המוסדות הוא אינו אוכף את עצם קבלת ההסמכה הנדרשת. מאחר שכ-10% בלבד מן המוסדות הרפואיים הטעונים רישיון מוסמכים לתקן, גם אם הם מוסדות משמעותיים כגון בתי חולים וקופות חולים, עליו לפעול בנחישות לאכיפת החובה הקבועה בחוזר המנכ"ל על שאר המוסדות.

פיקוח ובקרה: כאמור, חובת העמידה בהוראות הדין וההנחיות על אבטחת מידע רפואי חלה על כלל המוסדות הרפואיים בישראל ואף על מטפלים פרטיים.

נמצא כי עד תחילת שנת 2018 לא ערך משרד הבריאות בקורות בנושא אבטחת מידע במוסדות רפואיים.

ממשרד הבריאות נמסר לנציגיו של משרד מבקר המדינה, כי בתחילת שנת 2017 הוא החל במיפוי מוסדות רפואיים הטעונים רישיון, לשם פנייה אליהם בעניין אבטחת המידע. באותה שנה הוקמה במשרד הבריאות יחידת הכוונה מגזרית בתחום הסייבר¹¹⁹, שבתחילת 2018 ביצעה בקורות בנושא אבטחת מידע וסייבר בשבעה בתי חולים ממשלתיים, במסגרת בקורות הרישוי הכלליות של בתי החולים, ומתחילת 2017 עד אמצע 2018 ליווה נציג היחידה 30 בדיקות הסמכה לתקן שבוצעו בבתי חולים בלבד.

משרד הבריאות הסביר בתשובתו, כי מערכת המידע על רישוי המוסדות מיושנת ופילווח המידע שבה הוא פעולה מורכבת עד בלתי אפשרית. לכן, המשרד החל בתהליך פיתוח של מערכת עדכנית שתאפשר את מיפוי המוסדות. עוד הוסיף המשרד, כי הגנת הסייבר היא נושא המתפתח בכל מגזרי הממשלה וטרם הושלמה החקיקה בו, עובדה שגורמת חוסר בהירות ביחס לסמכויות המשרד כגורם המספק הכוונה והנחיה מגזרית בתחום הסייבר. אף על פי כן החל המשרד להיערך לכך, ובין השאר נכתבה טיוטה לחוזר מנכ"ל על הנחיות של יחידת הסייבר למגזר הבריאות.

על משרד הבריאות להשלים בהקדם את מיפויים של מוסדות אלה ולבנות תוכנית לפיקוח ובקרה על אבטחת המידע בכל המוסדות, בהתאם לסדרי עדיפויות שיקבע.

ניטורן של מערכות מידע רפואי: בתקן נכתב כי תיעוד ובקרה של הפעולות המבוצעות במערכות המידע הם מן הדרישות החשובות ביותר לאבטחתו של מידע רפואי אישי, שנועדו להבטיח את מחויבות הארגונים לנושאי המידע,

119 יחידה של אנשי מקצוע בתחום הגנת הסייבר במשרד ממשלתי, שתפקידה להסדיר את הגנת הסייבר במגזרים שבתחומי אחריותו. הרשות הלאומית להגנת הסייבר מנחה מקצועית את היחידה.

לתמרץ את המשתמשים במערכות המידע הרפואי לפעול בהתאם לכללים ולסייע בחשיפת שימוש לא ראוי במערכות אלה או במידע שבהן.

בהתאם לתקן, מערכות מידע המכילות מידע רפואי אישי ייצרו יומן פעילות שוטפת מאובטח (audit log) בכל פעם שמשתמש מבצע בהן פעולה בקשר למידע רפואי אישי. רשומת הבקרה צריכה לזהות באופן ייחודי את המשתמש, את נושא המידע ואת הפעולה שביצע, ואת התאריך והשעה שהפעולה נעשתה בהם. הוראות דומות נקבעו בחוזר אבטחת מידע וכן נקבע בו כי יש לבצע ניטור סדיר של מערכות המידע - זיהוי חריגות (אנומליות) ופעולות חשודות (כלומר ניטור יזום ולא תחקור אירועים בדיעבד). יצוין, כי גם תקנות אבטחת מידע קובעות כי יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע¹²⁰ וכי בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, יערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

בביקורת נמצא כי במכבי שירותי בריאות (להלן - מכבי), מבין 46 מערכות מידע המכילות מידע רפואי אישי של מטופלים, מנוטרת רק המערכת לניהול תיקים רפואיים, המערכת המרכזית של הקופה, אך גם היא לא באופן סדיר. בשירותי בריאות כללית (להלן - כללית), מבין 54 מערכות מידע המכילות מידע רפואי אישי, שתיים בלבד, המערכות העיקריות¹²¹, מנוטרות באופן סדיר, אך חלקי בלבד. על פי הערכת הקופה, יחלפו עוד חמש שנים עד שיתאפשר ניטור מלא של המערכות. במרכז הרפואי אסף הרופא (להלן - בית חולים אסף הרופא) 46 מערכות מידע המכילות מידע רפואי אישי וכולן אינן מנוטרות באופן סדיר. במרכז הרפואי ע"ש חיים שיבא, תל השומר (להלן - בית החולים שיבא) כ-20 מערכות מידע המכילות מידע רפואי אישי וכולן אינן מנוטרות באופן סדיר.

בהתאם לדרישות שבחוזר אבטחת מידע, על כלל המוסדות הרפואיים לפעול להרחבת ניטור סדיר של רשומות ההתחברות לכלל מערכות המידע שברשותם הכוללות מידע רפואי אישי. משרד מבקר המדינה מעיר למשרד הבריאות כי עליו לקיים פיקוח ובקרה על המוסדות הרפואיים בנושא זה.

בתשובתו של בית החולים שיבא למשרד מבקר המדינה מדצמבר 2018 נכתב, כי במערכות מידע רפואיות קשה להגדיר חריגות (אנומליות) ופעולות חשודות ולכן הגדרת פעולות הניטור שיימסר עליהן דיווח אוטומטי היא פעולה מורכבת ביותר שמשרד הבריאות צריך לעסוק בה ולתת הנחיות ואמצעים טכניים לביצועה.

בית החולים אסף הרופא מסר לנציגי משרד מבקר המדינה בספטמבר 2018, כי הוא נמצא בתהליך הטמעה של מערכת אשר תאפשר לקבל התרעות בזמן

120 החובה נוגעת למערכות מידע ברמת אבטחה בינונית או גבוהה ובכלל זה מאגרי מידע רפואיים.

121 מערכות קליקס וקמיליון לניהול תיקים רפואיים ממוחשבים.

אמת על ניסיון גישה למידע לא מורשה במערכת המידע המרכזית של בית החולים - מערכת נמ"ר¹²².

משרד הבריאות כתב בתשובתו כי הוקמה מערכת SIEM (Security Information and Event Management) מגזרית, אשר תאפשר לכלל המוסדות הרפואיים להתחבר אליה בהתאם לצרכיהם ולנטר מערכות ומאגרי מידע, לרבות זיהוי אנומליות ופעולות חשודות. הטמעת המערכת החלה ברבעון השני של שנת 2018 ובמועד סיום הביקורת היו מחוברים למערכת ארבעה בתי חולים כלליים ו-14 בתי חולים גריאטריים ופסיכיאטריים ממשלתיים.

על החשיבות שבהגנה על פרטיות המידע הרפואי ואבטחתו, בין השאר באמצעות ניטור, אפשר ללמוד מהמקרים הבאים: בתחקיר אירוע אבטחת מידע מיולי 2017, שנערך בבית החולים אסף הרופא, עלה חשד לחשיפת מידע קליני ממערכת נמ"ר לקרוב משפחה של מטופל. במסקנות התחקיר נכתב כי יש לאפשר תחקור של כניסות לא חוקיות למערכת כדי שיהיה אפשר להתחקות על הגורם שחשף את המידע.

מקרה אחר הוא תיק חקירה פלילית של הרשות להגנת הפרטיות שעסק בסחר במידע רפואי של מאושפזים והעברתו בידי עובדי קופות חולים ובתי חולים לחברות סיעוד באמצעות מתווכים. בדיון שנערך בעקבות מקרה זה במרץ 2017, בהשתתפות משנה למנכ"ל משרד הבריאות ונציגי הרשות, סוכם כי אגף המחשוב של משרד הבריאות יבחן את אפשרותה של קבלת התרעה על שימוש לא מורשה במערכות מידע רפואי.

המשנה למנכ"ל משרד הבריאות הקים בעקבות מקרה זה ועדה משרדית לבחינתן של דרכי התמודדות עם הפגיעה בפרטיות המטופל ובסודיות המידע הרפואי, כדי לגבש תוכנית פעולה לטיפול בתופעה. ממסקנות הוועדה מאוגוסט 2017 עולים כמה נושאים הטעונים הסדרה ובכלל זה היעדר נהלים לבקרה שוטפת על הגישה לרשומות רפואיות ושימוש בשם משתמש כללי בצידוד מחשוב ומכשור רפואי במחלקות בתי החולים, המהווים איום ממשי מבחינת אבטחת מידע. בין המלצות הוועדה: כתיבת קוד אתי לנושא פרטיות; מינוי ממונה הגנת פרטיות בכל ארגון במערכת הבריאות; חיוב כניסה אישית מזוהה לכל מחשב ולכל מערכת רפואית; ניטור פעולות המשתמשים ובקרה שוטפת של הפעילות במערכות המידע; אכיפה של אבטחת המידע באמצעות כלים טכנולוגיים; קביעת חובות דיווח של ארגוני בריאות על אירועים חריגים למשרד הבריאות, ועוד.

הנהלת המשרד אימצה את המלצות הוועדה. בעקבות זאת הוכנו טיוטת קוד אתי וטיוטת הגדרות תפקיד לממונה פרטיות והן צפויות להיות מפורסמות כחוזרי מנכ"ל משרד הבריאות. כמו כן הופץ מסמך מדיניות להגברת מודעותם של העובדים לאבטחת מידע וסייבר.

122 נמ"ר - ניהול מרכזים רפואיים - מערכת ממוחשבת בה מבוצעות פעולות מינהליות וקליניות הנמצאת בשימוש במספר בתי חולים ממשלתיים.



מערכת ממוחשבת
לשיתוף מידע רפואי
כרוכה גם בחששות
לפגיעה בזכויות
המטופלים לפרטיות
ולסודיות רפואית
ולסיכוני אבטחתו של
המידע האישי
שמבקשים לשתף

נמצא כי בחלוף שנה ויותר מיום שניתנו המלצות הוועדה, משרד הבריאות טרם הנחה את המוסדות הרפואיים בנוגע למקרים שיחייבו דיווח על אירועי אבטחת מידע, לצורך בקיום בקרה ואכיפה של הכללים לאבטחת מידע ועוד. על משרד הבריאות לפעול להמשך יישומן של מסקנות הוועדה ולהטמעתן במוסדות הרפואיים.

מערכת ממוחשבת לשיתוף מידע רפואי

שנים רבות פעל משרד הבריאות להקמת מערכת ממוחשבת שתאפשר לגורמים המטופלים בבתי החולים גישה מקוונת לתיקו הרפואי של המטופל במרפאות ובמוסדות הרפואיים השונים. היתרונות במערכת כזו חשובים ורבים: קיצור התהליך האבחוני והגברת דיוקו; מניעת בדיקות כפולות ושיפור הרצף הטיפולי והתיאום בין הגורמים המטופלים; אפשרות למתן טיפול גם כשאי אפשר לתקשר עם המטופל, ועוד. ואולם מערכת מסוג זה כרוכה גם בחששות לפגיעה בזכויות המטופלים לפרטיות ולסודיות רפואית ולסיכוני אבטחתו של המידע האישי שמבקשים לשתף. ועדות ציבוריות שדנו בנושא במהלך השנים ניסו לגבש מתווה להפעלתה של מערכת שיתוף מידע, שיאזן בין ייעול הטיפול הרפואי לבין פרטיות המטופלים.

כבר בשנת 2007 נכתבה במשרד הבריאות טיוטה לתזכיר חוק¹²³ שנועדה להסדיר סוגיה זו באמצעות הקמת מאגר רשומה רפואית לאומית. על אף דיונים רבים שנערכו בנושא, הליך החקיקה לא קודם.

במהלך השנים, ומשיקולים של אבטחת מידע והגנת הפרטיות, החליט משרד הבריאות כי לא יוקם מאגר מידע מרכזי שישלח אליו המידע מקופות החולים. בשנת 2011 החל המשרד לפעול להקמת מערכת תקשורת סגורה¹²⁴ המאפשרת לבתי החולים לצפות במידע הרפואי של המטופל השמור בקופות החולים ומתפוגג לאחר הצפייה בו (להלן - מערכת שיתוף מידע). משרד הבריאות סבר כי אין צורך בחקיקה ראשית להפעלתה של מערכת זאת¹²⁵, אך משרד המשפטים סבר כי יש להסדיר נושא זה בחקיקה ראשית.

בינואר 2014 פרסם מנכ"ל משרד הבריאות את חוזר 5/14, "שיתוף מידע רפואי במדינת ישראל" (להלן - חוזר שיתוף מידע רפואי), והנחה בו את כל ארגוני הבריאות בישראל (בתי חולים, קופת חולים, מערך שירותי הרפואה של צה"ל ומוסדות אחרים הנותנים שירותי בריאות) להתחבר למערכת שיתוף מידע. החוזר כלל הוראות על פעולתה של רשת שיתוף המידע, על ניהול משתמשים, על

123 תזכיר חוק רשומה רפואית לאומית התשס"ז-2007.

124 "מערכת אופק" המבוססת על פלטפורמה טכנולוגית קיימת של שירותי בריאות כללית לניהול תיקים רפואיים.

125 על העמימות שבאבחנת משרד הבריאות ראו מסמך מרכז המחקר והמידע של הכנסת בנושא "רשומה רפואית לאומית" מ-15.5.14.



משרד המשפטים
אומנם דרש להקפיא
את החוזר, אך לא
קבע שאין להפעיל
את מערכת שיתוף
המידע בטרם הוסדרה
פעילותה בחקיקה
ראשית

הגנת הפרטיות, על קביעת מידע חסוי שלא יועבר למערכת (כגון מידע על בריאות הנפש ועל הפסקת הריון), על אפשרות לצאת מהמערכת (opt out)¹²⁶ ועוד. כעבור כמה ימים, ולאחר שהתברר כי עמדתו של משרד המשפטים שיש להסדיר את פעילות המערכת בחקיקה ראשית, הקפיא משרד הבריאות את תוקף החוזר, עד שישלים את אסדרת הפרויקט. עם זאת, הפעלת מערכת שיתוף מידע רפואי נמשכה.

בדיון בנושא "רשומה רפואית לאומית - בין ייעול הטיפול הרפואי לבין שמירה על פרטיות החולה" שנערך בוועדת המדע והטכנולוגיה של הכנסת בפברואר 2016, ציין סמנכ"ל המחשוב במשרד הבריאות כי יש להשלים את אסדרת הנושא באמצעות חקיקה או תקנות.

יוצא אפוא, כי מערכת שיתוף המידע פועלת לפחות חמש שנים בלי שהוסדרה בחוק או בתקנות ולמרות עמדתו של משרד המשפטים, לפיה יש להסדיר סוגיה רגישה זאת בחקיקה ראשית, גם אם מדובר במערכת שיתוף מידע ולא במאגר מידע מרכזי.

ממחלקת יעוץ וחקיקה נמסר לנציגי משרד מבקר המדינה, כי אכן ראתה צורך בחקיקה ראשית על מנת להפעיל את המערכת, אך במועד סיום הביקורת שאלת הצורך בחקיקה ראשית נדונה שוב במסגרת כתיבת טיוטת תקנות ביטוח בריאות ממלכתי (שמירת רצף הטיפול במעבר בין בית חולים וקהילה), התשע"ח-2018¹²⁷ (להלן - תקנות רצף הטיפול).

משרד הבריאות כתב בתשובתו, כי משרד המשפטים אומנם דרש להקפיא את החוזר אך לא קבע שאין להפעיל את מערכת שיתוף המידע בטרם הוסדרה פעילותה בחקיקה ראשית. לשיטת משרד הבריאות, הסדרתה של מערכת שיתוף מידע אפשרית גם שלא בחקיקה ראשית מכוח חוק זכויות החולה, והמשרד יפעל לקידום ההסדרה גם בנושא זה בהתאם לסדרי העדיפויות שלו, ובשים לב לתוכנית החקיקה הממשלתית. המשרד הוסיף, כי עד שתושלם הסדרת הנושא יש להחזיר לתוקפו את החוזר שהוקפא. כמו כן, על פי עמדת המשרד, אין מקום לאסדרת פעילותה של מערכת שיתוף מידע "בדרך אגב" וכחלק מתקנות רצף הטיפול, והוא דן בנושא עם מחלקת יעוץ וחקיקה.

126 המידע אודות המטופלים שהם נושאי המידע ניתן לצפייה במערכת אלא אם ביקש נושא המידע לבטל אפשרות זו לגביו.

127 טיוטת התקנות עוסקת בשיפור השמירה על רצף בטיפול, בעיקר בחילופי מטופלים או מסגרות טיפול, כאשר יש חשיבות רבה לקשר בין מערכות המידע של הגורמים השונים. יצוין כי טיוטת התקנות נכתבה כבר בשנת 2015. בדוח מבקר המדינה בנושא "אסדרה ופיקוח בתחום הרוקחות" (דוח שנתי 2017) עמ' 465 צוין מאת משרד הבריאות, כי התקנות הועברו למשרד המשפטים לקראת פרסום. נכון לסוף שנת 2018 הן עדיין מצויות בדיונים פנימיים בין משרד המשפטים למשרד הבריאות.

אין חולק על חשיבותה הרבה של מערכת שיתוף מידע רפואי להצלת חיים ולשיפור איכות הטיפול הרפואי. ואולם, משרד מבקר המדינה מעיר למשרד הבריאות, כי אין להשלים עם התעלמותו מעמדת משרד המשפטים על הצורך להסדיר את הנושא בחקיקה. מנגד, משרד המשפטים לא פעל באמצעים המקובלים במחלוקות משפטיות מעין אלה¹²⁸, ומערכת שיתוף המידע המשיכה לפעול במשך השנים ללא הסדרה ראויה. על משרד הבריאות ומשרד המשפטים להגיע בהקדם להכרעה על ההסדר הנורמטיבי הנדרש ולפעול ליישמו.

יציאה ממערכת שיתוף מידע רפואי

אחד העוגנים לחוקיות פעילותה של מערכת שיתוף מידע, שהודגש בדיוניה של מינהלת פרויקט שיתוף המידע¹²⁹, היה יידוע הציבור על קיום המערכת ומתן האפשרות ליציאה ממנה. בחוזר שיתוף מידע רפואי שהוקפא נכתב, כי סמוך לכניסת החוזר לתוקף יביא משרד הבריאות לידיעת הציבור, באמצעים המקובלים למסירת מידע בנושא זכויות (כגון בדיוור ישיר, בטפסי ההצטרפות לקופה ובשילוט), את דבר הקמתה וקיומה של רשת שיתוף המידע, מידע על השימוש בה ומידע על הזכות לצאת ממנה. עוד נקבע כי גם בתי החולים וקופות החולים יביאו עניין זה לידיעת המטופלים ולידיעת הצוותים הרפואיים.

באוגוסט 2014 פרסם אגף המחשוב במשרד הבריאות תסקיר להשפעה על הפרטיות של מערכת שיתוף מידע. התסקיר נועד לוודא עמידה בדרישותיו של חוק הגנת הפרטיות והתקנות המחייבות בכל הנוגע להיבטי הפרטיות ואבטחת המידע של המערכת והוא חוזר על ההוראות האמורות בחוזר שיתוף מידע רפואי.

בדיון האמור של ועדת המדע והטכנולוגיה של הכנסת מפברואר 2016 ציין סמנכ"ל משרד הבריאות, כי חלק מהבעיה הוא "שהציבור לא מספיק מכיר ולא יודע את זכויותיו בהקשר זה". הסמנכ"ל הבהיר כי הטיפול בסוגיה טרם הושלם.

נמצא כי בשל הקפאת חוזר שיתוף מידע רפואי, קופות החולים לא ידעו את הציבור בנושא כפי שקבעה מינהלת הפרויקט לשיתוף מידע וכפי שהומלץ גם בתסקיר ההשפעה על הפרטיות משנת 2014. עוד נמצא, כי הסבר על הזכות ליציאה מהמערכת וטופס למימוש זכות זאת קיים באתרי האינטרנט של כללית, מכבי וקופת חולים מאוחדת, אך אינו קיים באתר לאומית שירותי בריאות. גם הפרסום שעשה משרד הבריאות בנושא נעשה באינטרנט בלבד והופסק לאחר מספר ימים.

128 ראו בהקשר זה הנחיית היועץ המשפטי לממשלה 9.1000, "היועצים המשפטיים למשרדי הממשלה".

129 פורום שמינה מנכ"ל משרד הבריאות לדיון וקבלת החלטות בסוגיות עקרוניות בפרויקט שיתוף המידע.

בתשובתה למשרד מבקר המדינה מנובמבר 2018 ציינה שירותי בריאות כללית, כי לאור הסוגיות העקרוניות כבודות המשקל הכרוכות ביציאה מהמערכת, הוקפא מהלך היידוע בדבר יציאה ממערכת שיתוף המידע, וכי היא שותפה לדעה כי אם יוחלט לקבוע כללים חדשים בנושא, יש לעגנם בחקיקה.

משרד הבריאות מסר בתשובתו, כי מערכת שיתוף המידע חשובה לטיפול רפואי מיטבי ולשיפור התקשורת בין מטפלים שונים במערכת הבריאות, וכי לכל מטופל הזכות לצאת מהמערכת, אך היציאה מהמערכת היא החריג והיא עלולה לפגוע באיכות הטיפול הרפואי שיקבל ולהזיק לבריאותו.

בדיון של מינהלת הפרויקט לשיתוף המידע מפברואר 2013, שכותרתו "פורום רפואי - מידע חסוי בפרויקט שיתוף מידע", ציין סמנכ"ל משרד הבריאות, כי יציאת מטופל ממערכת שיתוף המידע תחייב ביקור של המטופל במרפאה, קבלת הסבר על הנזק שעלול להיגרם וחתימה על טופס. בסיכום הדיון נכתב כי מטופל יוכל לבקש שביקור מסוים שלו אצל הרופא יוגדר כחסוי ולא יופיע במערכת שיתוף המידע, שכן מטופלים רבים מבקשים להישאר במערכת אך מבקשים גם למנוע חשיפה של ביקור נקודתי הנוגע לנושא רגיש.

על אף האמור, האפשרות להסתיר ביקור יחיד במערכת שיתוף המידע קיימת בבתי החולים אך לא בקופות החולים.

משרד הבריאות השיב, כי טרם נקבעה האפשרות להסתיר ביקור גם בקופות החולים. עוד ציין כי אפשרויות הבחירה למטופלים נבחנות באופן שוטף בהתחשב באיזונים בין הצורך הרפואי וחסרונות הצגתו של מידע חלקי לבין הרצון לחזק את שליטת המטופל במידע עליו ובהתחשב במגבלות הטכנולוגיה.

על משרד הבריאות לבחון את אפשרות חסיונו של ביקור מסוים לבקשת מטופל גם בקופות החולים, וזאת בהתאם לקביעת מינהלת הפרויקט לשיתוף מידע.

שימוש במידע רפואי לצורכי מחקר

אחד הכלים העיקריים להתפתחות הרפואה ובריאות הציבור הוא עריכת מחקרים רפואיים מסוגים שונים. תועלתו של המחקר הרפואי ניכרת במישרין בהצלת חיי אדם, בגילוי תרופות ובשיפור איכות החיים, ובעקיפין - תועלת כלכלית ועוד.

בשנת 1964 גיבש ארגון הבריאות העולמי המלצות המנחות רופאים במחקר ביו-רפואי שמשותפו בני אדם, במסמך רשמי המכונה "הצהרת הלסינקי"¹³⁰. בהצהרה


עמדת משרד
הבריאות היא שנתוני
החולים שבידי
המוסדות הרפואיים
נועדו אך ורק לצורך
טיפול רפואי וכל
שימוש אחר במידע
מחייב הסכמה של
המטופל

נקבע כי מחקרים בבני אדם יבוצעו בידי אנשי מדע כשירים ובפיקוחו של איש רפואה בעל סמכות קלינית; כי יינקטו כל אמצעי הזהירות לשמירת פרטיותו של האדם המשתתף במחקר ולמזעור פגיעתו של המחקר בשלמותו הגופנית והנפשית ובאישיותו; כי על הרופא לקבל את הסכמתו המודעת של המועמד להשתתף במחקר; וכי המחקר יאושר בידי ועדה שתוקם לשם כך (להלן - ועדת הלסינקי).

הצהרת הלסינקי עוגנה בדין הישראלי בתקנות בריאות העם (ניסויים רפואיים בבני אדם), התשמ"א-1980¹³¹ (להלן - תקנות הניסויים). תקנות הניסויים קובעות כי לא ייעשה ניסוי רפואי בבן אדם בבית חולים בניגוד לתקנות אלה ובניגוד להצהרת הלסינקי.

כבהצהרת הלסינקי, גם עמדת משרד הבריאות היא שנתוני החולים שבידי המוסדות הרפואיים נועדו אך ורק לצורך טיפול רפואי וכל שימוש אחר במידע מחייב הסכמה של המטופל¹³².

ככלל יש להבחין בין שני סוגים עיקריים של מחקרים רפואיים:

1. מחקר הכרוך בהתערבות בגוף האדם - ניסויים רפואיים בבני אדם - מוגדר בתקנות הניסויים כ"עשיית שימוש בתרופה, בקרינה או בחומר כימי, ביולוגי, רדיולוגי או פרמקולוגי, בניגוד לאישור שניתן לאותו שימוש לפי חיקוק, או כאשר השימוש האמור אינו מקובל בישראל לצרכים שמבוקש לייעדו להם, או שטרם נוסה בישראל, ויש בו או שמיעדים אותו להשפיע על בריאותו, גופו או נפשו של אדם או של עובר, או חלק מהם, לרבות המערך הגנטי", וכן "עשיית כל הליך, פעולה או בדיקה בבן אדם, שאינם מקובלים".
2. מחקר שאינו כרוך בהתערבות בגוף האדם (ניסוי רפואי מיוחד) - מחקר שנאסף בו מידע מבני אדם תוך אינטראקציה איתם (להלן - מחקר בשאלונים) או מחקר שנאסף בו מידע מרשומות רפואיות, סיעודיות, פסיכולוגיות ואחרות ללא אינטראקציה עם המטופלים (להלן - מחקר בנתונים); ובלבד שהמחקר אינו כולל ביצוע בדיקות, הליכים, מתן תרופות וכיוצא באלה בגופו של המשתתף. יצוין כי בהתאם לתקנות הניסויים, גם מחקר זה נכלל בגדר "ניסויים רפואיים בבני אדם" אך חלים עליו כללים שונים, שכן רמת הסיכון שבו נמוכה יותר.

תקנות הניסויים מחייבות הקמתן של 'ועדות הלסינקי' לבחינת בקשות לאישור מחקרים רפואיים הכוללים ניסויים בבני אדם בכל מוסדות הרפואה והמחקר בארץ, ומעליהן ועדה עליונה¹³³. בנוסף, יש ועדות מרכזיות של משרד הבריאות

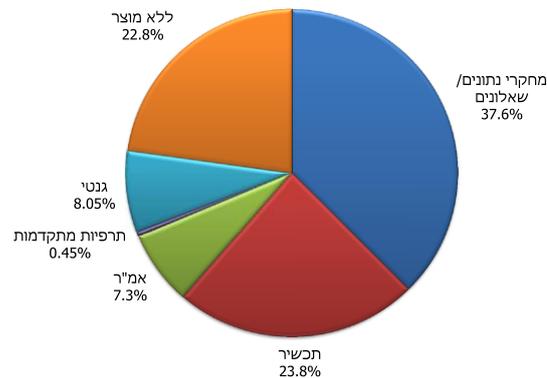
131 התוספת לתקנות מתייחסת לנוסח ההצהרה בדבר המלצות המנחות רופאים במחקר ביו-רפואי שכרוכים בו בני אדם, הלסינקי, 1964, כפי שתוקנה בטוקיו, 1975.

132 מסקנות הוועדה להתמודדות עם איום הפגיעה בפרטיות, לעיל בהערות שוליים 113.

133 ועדת הלסינקי העליונה לניסויים רפואיים בבני-אדם, הינה ועדה סטטוטורית המורכבת מרופאים וחוקרים מתחומים שונים, משפטנים, אתיקנים ואנשי ציבור, העוסקת בבחינה ואישור הצעות לכלל המחקרים בישראל הנוגעים למערך הגנטי של בני אדם, למחקרים הנוגעים להפריית נשים, למחקרים המבוצעים על ידי עובדי המשרד הראשי של משרד הבריאות, וכל מחקר בעניין אחר על פי בקשת מנכ"ל משרד הבריאות. כמו כן עוסקת הוועדה בבחינת מדיניות בתחום עיסוקה.

המאשרות מחקרים מסוגים שונים. בהתאם להנחיות משרד הבריאות, על ועדות הלסינקי המוסדיות¹³⁴ לדווח מדי שנה למשרד הבריאות על המחקרים הרפואיים שאישרו. בהתאם לדיווחי הוועדות, בשנת 2017 אושרו יותר מ-5,600 מחקרים (הן ניסויים בבני אדם הן מחקרים בנתונים ושאלונים)¹³⁵. להלן בתרשים המחקרים לפי נושאים:

תרשים מס' 3: מחקרים רפואיים שאושרו בשנת 2017 לפי נושאים (באחוזים)



המקור: דיווחי ועדות הלסינקי המוסדיות למשרד הבריאות.

* תרפיות מתקדמות - תכשירים ביולוגיים רפואיים; אמ"ר - אביזרים ומכשור רפואי; ללא מוצר - ניסוי רפואי הכרוך בלקיחת דם או דגימות ביולוגיות, בפרוצדורה חדשה שאינה נהוגה בפרקטיקה הרפואית או המקצועית ואינה כרוכה בשימוש בתכשיר או באמ"ר ועוד.

מהתרשים עולה כי מחקרים בנתונים ושאלונים מהווים נתח משמעותי מכלל המחקרים הרפואיים שאושרו, ובשנת 2017 עמד מספרם על כ-2,100.

מחקרים בנתוני עתק

ככל שמתפתחים כלי האיסוף, השמירה והעיבוד של מידע, כן גדל הפוטנציאל לפריצות דרך רפואיות באמצעות מחקר במידע רפואי. מקורות המידע הרפואי רבים ובהם מידע קליני, מידע גנטי ומידע הנאסף ממכשור רפואי ומחיישנים (כגון משאבות אינסולין, קוצבי לב וכדומה). בשימוש בנתוני עתק (Big Data) יש פוטנציאל לשיפורן של שיטות הטיפול הרפואי, להתאמתן באופן אישי למטופל, ולזיהוי סיכונים להתפרצות מחלות ביחידים ובאוכלוסייה כולה.

משרד הבריאות הכיר בכך שהכללים הנהוגים כיום בנוגע לביצוע מחקרים רפואיים ואישורם באמצעות ועדות הלסינקי אינם מספקים בכל הנוגע למחקרים בנתוני עתק. לכן, המשרד מקדם מזה שנים אחדות מהלך לגיבוש כללים

134 ועדה המוקמת בבית חולים ונועדה לאשר ניסויים רפואיים בבני אדם המונה לפחות 7 חברים וביניהם נציג ציבור. נכון למועד סיום הביקורת קיימות 54 ועדות הלסינקי.

135 המידע אינו שלם שכן 5 מוסדות מתוך 54 לא דיווחו למשרד הבריאות כנדרש.



משרד הבריאות הכיר
בכך שהכללים
הנהוגים כיום בנוגע
לביצוע מחקרים
רפואיים ואישורים
באמצעות ועדות
הלסינקי אינם
מספקים בכל הנוגע
למחקרים בנתוני
עתק. המשרד מקדם
זה שנים אחדות מהלך
לגיבוש כללים חדשים
ועדכניים לשימוש
משני בנתוני בריאות

חדשים ועדכניים לשימוש משני בנתוני בריאות, המוגדר כשימוש במידע בריאות לכל צורך שאינו טיפול רפואי. בינואר 2018 פורסמו המלצות הוועדה ליישום המלצות השימושים המשניים במידע בריאות שמיינה מנכ"ל משרד הבריאות¹³⁶.

בעקבות המלצותיה של הוועדה התקבלה במרץ 2018 החלטת ממשלה 3709 - "תוכנית לאומית לקידום תחום הבריאות הדיגיטלית כאמצעי לשיפור הבריאות וכמנוע צמיחה". מטרת ההחלטה היא מיצוי התועלות הטמונות בפיתוחים חדשניים בתחום הבריאות הדיגיטלית ומינוף יתרונותיה של ישראל בחדשנות הטכנולוגית, ברפואה ובמחקר. לשם כך אימצה החלטת הממשלה תוכנית לאומית לקידום הבריאות הדיגיטלית כמנוע צמיחה לאומי, באמצעות שימוש בכלים של נתוני עתק במגזר העסקי ובאקדמיה, תוך הגברת שיתופי הפעולה בין הגורמים הרלוונטיים בתחום. בהחלטה נקבעו כמה פרויקטים שיקודמו לשם מימושן של המטרות ובהם הקמת תשתית לאומית למחקרי בריאות בתחום הגנטיקה והמידע הרפואי, פיתוח כלים טכנולוגיים לאסדרת השימוש במידע משני, מעבר לתיעוד נתוני בריאות בצורה אחידה כדי לאפשר ביצוע המחקרים, ועוד.

בהחלטת הממשלה נכתב כי שר הבריאות "יפעל לגיבוש נוסח חקיקה או חקיקת משנה, בהתאם להכרעה משפטית שתתקבל בעניין, לצורך יישום המלצות הוועדה ליישום המלצות השימושים המשניים במידע בריאות שפרסם משרד הבריאות, ובכפוף לבחינת הצורך בשינויים מהמלצות הוועדה, לצורך שיפור ההגנה על פרטיות המטופלים". על פי ההחלטה, נוסח החקיקה או חקיקת המשנה יתייחס למטרות השימוש במידע, לשמירה על הפרטיות, לכללי התממה, לשקיפות, להנגשת נתונים, ועוד. ההכרעה המשפטית על ההסדר הנורמטיבי הרצוי תתקבל לאחר שהסוגיה תלובן בין משרדי הבריאות והמשפטים.

בהתאם לסיכום התקציבי עם משרד האוצר ממרץ 2018, משרד הבריאות נדרש להגיע להסכמות עם המשרדים החתומים על הסיכום, ובכלל זה משרד המשפטים, בדבר המנגנון הנורמטיבי המתאים ליישום התוכנית שבהחלטת הממשלה עד סוף יולי 2018, ועד סוף יולי 2019 עליו לממש את ההסדר הנורמטיבי המוסכם.

משרד הבריאות כתב בתשובתו, כי הוא נמצא בעיצומם של דיונים אינטנסיביים עם נציגי משרד המשפטים על מנת להסכים בהקדם האפשרי על המנגנון הנורמטיבי המתאים וכי הוא נמצא בשלבי גיבוש.

136 הוועדה מונתה במטרה לקבוע את העקרונות המנחים לרגולציה של שימושים משניים במידע בריאות. הוועדה הורכבה מארבעה צוותים שדנו בהיבטים שונים של הנושא: הגדרת קוד אתי, הגדרת דרכים לשיתוף הציבור, הגדרת סוגיות של טכנולוגיה ומימוש וקביעת תמריצים לעידוד השימוש במידע.

זה שנים נערכים במוסדות הרפואיים מחקרים בנתוני עתק ללא אסדרה המתאימה להתפתחות הטכנולוגית

משרד מבקר המדינה מעיר למשרד הבריאות, כי מזה שנים נערכים במוסדות הרפואיים מחקרים בנתוני עתק ללא רגולציה המתאימה בין השאר להתפתחות הטכנולוגית, ולכן עליו להחליט בהקדם על המנגנון הנורמטיבי המתאים, בהסכמת המשרדים הרלוונטיים, כדי שיתאפשר לקדם ולסיים את השלב המהותי של מימוש המנגנון שיוסכם עליו.

עד שייקבע ההסדר הנורמטיבי ליישומן של המלצות הוועדה, משרד הבריאות ניסח בחוזרי מנכ"ל 1/2018 ו-2/2018, שפורסמו בינואר 2018, כללים לשימוש משני במידע בריאות ולשיתופי פעולה הכרוכים בשימוש משני במידע בריאות. במסגרת החוזרים חודד נושא ההתממה ונקבע כי אחד מחברי ועדת הלסינקי יהיה בעל ידע בסטטיסטיקה המסוגל להעריך רמת סיכון לזיהוי מידע; כי את הבקשה למחקר יש למסור לעיונו של הממונה על אבטחת מידע בארגון¹³⁷; הוראות שייכללו בהסכמי שיתוף פעולה בין ארגוני בריאות ובין גופים חיצוניים; והובהרו נושאי אבטחת המידע והרשאות הגישה. יצוין כי הן החלטת הממשלה והן חוזרי המנכ"ל מתייחסים לשימוש במידע משני בהיקף כלשהו, ולא בהכרח למחקר בנתוני עתק, אך משרד הבריאות כתב לנציגי משרד מבקר המדינה כי ההחלטה והחוזרים מתייחסים בעיקר למחקרים בנתוני עתק.

התממה של המידע הרפואי המשמש למחקר

התממה (de-identification) של מידע היא הפחתת הסיכון לזיהוי או לחשיפה של נושא המידע באמצעות הסרת מרכיבים מזהים מובהקים ממידע אישי והמרתם בערכים כלליים יותר, בין השאר באמצעות: הצרפה (אגרגציה, צירוף נתונים), הפחתת דיוקם של הנתונים באמצעות שימוש בטווח במקום בערך ייחודי, השמטת פרטים, קידוד, הצפנה, וכדומה¹³⁸. אחת משיטות ההתממה היא "פסידו-אנונימיזציה" - עיבוד המידע האישי באופן שלא מאפשר לשייכו לנושא מידע מסוים ללא שימוש במידע אחר שלו, הנשמר בנפרד וכפוף לאמצעים טכניים וארגוניים המבטיחים שהמידע האישי לא ישוּיך לאדם מזהה או ניתן לזיהוי, כגון שימוש בקוד במקום מספר זיהוי וכדומה. קטגוריה משנית של התממה היא אנונימיזציה מלאה, שאינה מאפשרת כלל שיוך מחדש לנושא המידע.

יצוין כי בארצות הברית, על פי הכללים שנקבעו ב- Health Insurance Portability and Accountability Act of 1996 (להלן - HIPAA), יש 18 פרטי מידע שיש להסתיר על מנת להתמים מידע לצורכי מחקר רפואי ובכלל זה שם, מספר זיהוי, כתובת ומיקוד, תאריך לידה (למעט שנה), מידע ביומטרי, מספר תיק רפואי, טלפון ודוא"ל.

הנחת היסוד היא שככל שמידת ההתממה ורמת ההגנה על המידע גבוהות יותר, כך פוחתת יעילות השימוש במידע. לכן מבקשים למצוא את שיטות ההתממה

137 החוזרים מגדירים ארגון בריאות ככל גורם המחזיק מידע רפואי מזהה עקב אחריותו לטיפול במטופלים, בין אם הוא ציבורי או פרטי.

138 ראו: חוזר מנכ"ל משרד הבריאות 1/2018 "שימושים משניים במידע בריאות".

עד מועד סיום
הביקורת טרם קבע
משרד הבריאות כללי
התממה למחקרים
בנתוני עתק
ולמחקרים אחרים

בעלות האיזון המיטבי בין אובדן המידע ובין רמת ההגנה עליו. החיסרון המרכזי של ההתממה הוא שגם לאחר יישומה בטכניקות השונות עדיין מתאפשר "זיהוי חוזר"¹³⁹ של מידע שהותמם (למעט באנונימיזציה מלאה).

ניסויים רפואיים בבני אדם נעשים על פי תקנות הניסויים, חוק מידע גנטי, התשס"א-2000, הנוהל לניסויים רפואיים בבני אדם¹⁴⁰, חוזר מנכ"ל 15/06 "תת ועדת הלסינקי לאישור מחקר שאינו ניסוי רפואי בבני אדם" (להלן - חוזר אישור מחקר שאינו ניסוי רפואי בבני אדם), חוזר מנכ"ל 1/2018 בנושא שימושים משניים במידע בריאות (להלן - חוזר שימושים משניים במידע בריאות), עקרונותיה של הצהרת הלסינקי וכללים בין-לאומיים בנושא¹⁴¹.

1. בהתאם לחוזר שימושים משניים במידע בריאות, שימוש משני במידע בריאות למטרות מחקר ייעשה לפי הוראות הדין ובאישור ועדת הלסינקי, בהתאם לנוהל ניסויים רפואיים בבני אדם וחוזר אישור מחקר שאינו ניסוי רפואי בבני אדם. עוד נכתב בחוזר, כי עד אמצע יולי 2018 יקבע משרד הבריאות "כללים/אמצעים טכנולוגיים מינימליים מקובלים לביצוע התממה, על מנת שתהיה בתחום אחדות". עוד נקבע, כי על ארגוני בריאות העושים שימוש משני במידע פרטני מזוהה להציג תוכנית לפתרון המבוסס על התממה למירב השימושים שהתממה אפשרית בהם.

עד מועד סיום הביקורת טרם קבע משרד הבריאות כללי התממה למחקרים בנתוני עתק ולמחקרים אחרים.

משרד הבריאות כתב בתשובתו, כי קביעת כללי התממה למערכת הבריאות הישראלית היא נושא טכני מורכב הנמצא בתהליך מתמשך, בין-משרדי ובשיתוף ארגוני הבריאות וגורמים אחרים, וכי הוא פועל ליצירת עקרונות להתממה. עוד כתב המשרד כי הגם שטרם נקבעו הנחיות פרטניות בעניין זה, כללים ראשוניים לחובת ההתממה, המחייבים את כלל ארגוני הבריאות, פורסמו בחוזר שימושים משניים במידע בריאות לכל סוגי המחקרים, ובשלב הביניים נדרשים ארגוני בריאות המשתמשים במידע רפואי שברשותם למטרות מחקר, לקבוע כללים כאלה בהתאם להנחיות שבחוזר זה. המשרד הוסיף כי בכונתו להשלים במרוצת 2019 את הסדרת השימושים המשניים במידע רפואי, לרבות ההתממה, התקנת תקנות ופרסום חוזרי מנכ"ל.

139 הצלבה של מידע בלתי מזוהה עם מידע אחר באופן שיוצר מידע מזוהה.

140 נוהל 14 של אגף הרוקחות מהדורה שניה מיום 1.2.16.

141 Harmonized Tripartite Guideline for Good Clinical Practice (ICH-GCP E6).

ועדת הלסינקי
 העליונה במשרד
 הבריאות כתבה
 לנציגי משרד מבקר
 המדינה כי כאשר
 החוקר הראשי איננו
 הגורם המטפל של
 המשתתפים במחקר
 בנתונים או שאלונים,
 הוא אינו אמור
 להיחשף לתיקים
 הרפואיים שלהם ולא
 תהיה לו גישה ישירה
 אליהם

הסיכון הנשקף לפרטיות במחקרי נתונים רב יותר מאשר במחקרים אחרים, בעיקר משום שאין מבקשים מנושאי המידע את הסכמתם לשימוש בנתונים לצורכי מחקר. הסיכון רב אף יותר במחקרים בנתוני עתק. מחקרי נתונים נערכים מזה שנים במוסדות רפואיים וקביעת כללי ההתממה נועדה למעשה ליצור אחידות בקרב המוסדות הרפואיים ולטפל בתחום פעיל שהסיכון בו כבר קיים. על הנהלת משרד הבריאות לפעול לזירוז הסדרתה של הסוגיה ולהטמעת הנחיותיה בנושא.

2. בהתאם לחוזר אישור מחקר שאינו ניסוי רפואי בבני אדם, חלק מהתנאים לאישור מחקר בנתונים ובשאלונים הם: "ניתן פירוט של דרכי השמירה על פרטיות במחקר" והסכמתם של המשתתפים במחקר. עם זאת, על פי החוזר, במחקר בנתונים שנאסף בו מידע מתוך רשומות רפואיות באנונימיזציה מלאה, תת-הוועדה רשאית לפטור את החוקר מהסכמה מודעת של המטופלים-המשתתפים ובלבד שהחוקר הראשי של המחקר הוא מבית חולים אוניברסיטאי. על פי נוהל ניסויים רפואיים בבני אדם, הפטור האמור ניתן ל"מחקר המתבסס על נתונים לא מזוהים (שהפרטים המזהים הופרדו מהם באופן שלא ניתן בכל דרך שהיא לחזור אליהם), הנלקחים מתיקים רפואיים, או רשומות רפואיות/ סיעודיות/ סוציאליות של חולים...". הסיבה לדרישת האנונימיזציה המלאה במחקר בנתונים נובעת מכך, שבניגוד לסוגי מחקרים אחרים, במחקר בנתונים לא מבקשים את הסכמת נושאי המידע לביצוע המחקר באמצעות המידע האישי שלהם.

ועדת הלסינקי העליונה במשרד הבריאות כתבה לנציגי משרד מבקר המדינה, כי כאשר החוקר הראשי איננו הגורם המטפל של המשתתפים במחקר בנתונים או שאלונים, הוא אינו אמור להיחשף לתיקים הרפואיים שלהם ולא תהיה לו גישה ישירה אליהם. המידע הרפואי אמור להיות מועבר אליו כשהוא לכל הפחות מקודד, ולעיתים אף אנונימי לחלוטין בהתאם לסוג המחקר. המחלקה לניסויים קליניים במשרד הבריאות (להלן - המחלקה לניסויים קליניים) הוסיפה שאין מניעה להיחשפות החוקר הראשי למידע רפואי מזוהה כשהוא גם הגורם המטפל בנושאי המידע שמשמשים כבסיס המחקר, וזאת מתוך הבנה כי הוא נגיש גם כך למידע על אודותיו.

מנהלי משרד הבריאות משתמע שבמחקר בנתונים שלא התבקשה בו הסכמת משתתפים, התממת המידע באמצעות אנונימיזציה מלאה צריכה להיעשות טרם העברת המידע לחוקר, כאשר ההבחנה בין חוקר שהוא הגורם המטפל ובין חוקר שאינו הגורם המטפל אינה מופיעה בחוזר אישור מחקר שאינו ניסוי רפואי בבני אדם או בנוהל ניסויים רפואיים בבני אדם.

מעבר לכך, במחקרים רבים בנתונים החוקר אינו הגורם המטפל, כך שגם לשיטת משרד הבריאות אין הצדקה לחשיפתו למידע הרפואי טרם התממתו או קידודו. נמצא, כי במחקרים רפואיים בנתונים בבית החולים שיבא החוקר מקבל מידע רפואי מזהה גם אם אינו הגורם המטפל, והוא המבצע את הקידוד.

בית החולים שיבא מסר בתשובתו כי מדובר במחקרים שאינם בנתוני עתק וברובם יש לחוקר "קשר טיפולי" למשתתפים במחקר, וכי החוקר מחויב לסודיות על פי הוראות הדין וכללי המחקר. בית החולים גם אינו רואה מניעה שהחוקר יקבל מידע מזהה, שכן הדבר חשוב לאמינות המחקר ולמקצועיותו, והקידוד נעשה בשלב מאוחר יותר.

נמצא כי גם במחקרי נתונים בבית החולים אסף הרופא החוקר מקבל מידע רפואי מזהה אף אם אינו הרופא המטפל. יתר על כן, על פי גישתו של בית החולים, המנוגדת לעמדתו של משרד הבריאות, כל החומר והמידע שנאסף בידי החוקר הראשי חשוף ליזם המחקר¹⁴², משום שהמידע "שייך" לו וההתממה נועדה לגורמים אחרים שאינם מורשים לעיין במידע המזהה, כגון חוקרים שאינם החוקר הראשי במחקר¹⁴³.

ואולם בתשובתו של בית החולים אסף הרופא מדצמבר 2018 נכתב, כי מידע רפואי מזהה מקבל רק חוקר שהוא גם מטפל, וזים מקבל מידע מזהה רק אם הוא גם החוקר הראשי והמטפל.

תשובת בית החולים אסף הרופא אינה עולה בקנה אחד עם הדברים שנמסרו לביקורת מוועדת הלסינקי של בית החולים. על בית החולים לברר הסוגיה ולחדד את הכללים בנושא.

משרד הבריאות כתב בתשובתו, כי נהליו אינם מחייבים התממה גורפת לפני העברת המידע לחוקר וכי נוהל אישור מחקר שאינו ניסוי רפואי בבני אדם מביא בחשבון שכמה מן המחקרים המועילים ביותר אינם יכולים להתבצע אם ההתממה נעשית לפני מתן גישה לחוקרים. עוד הוסיף המשרד, כי ההבחנה בין גורם שהוא מטפל לבין גורם אחר היא רלוונטית, שכן חוקר שהוא גם גורם מטפל חשוף ממילא למידע המזהה על מטופליו. על כן יש לבחון כל מקרה לגופו, גם בהתאם לשיקול דעתה של ועדת הלסינקי, ואם המידע עובר בין גופים ציבוריים - גם בהתאם לשיקול דעתן של הוועדות להעברת מידע של הגוף המבקש ושל הגוף המוסר.

142 אדם, תאגיד, או מוסד האחראים לייזום, לניהול ולמימון של הניסוי הרפואי. הזים עשוי להיות החוקר עצמו אך במחקרים רבים הזים הוא גורם החיצוני למוסד הרפואי.

143 מכתב מוועדת הלסינקי של בית החולים אסף הרופא מ-8.8.18 במענה לשאלות הביקורת.



יש סתירה מובנית בין כללי משרד הבריאות, המחייבים אנונימיזציה מלאה של מידע המועבר ללא הסכמה במחקרי נתונים, ובין המידע הנדרש לצורך מחקר, שהוא מידע שניתן לזיהוי חוזר בעת הצורך

נמצא כי בשני בתי החולים שנבדקו לא הוקמו ועדות להעברת מידע בין גופים ציבוריים. מבית החולים שיבא נמסר כי באוקטובר 2018 הוקמה ועדה ומבית החולים אסף הרופא נמסר כי תוקם ועדה.

משרד מבקר המדינה מעיר למשרד הבריאות, כי תשובתו אינה משתמעת מנהלי המשרד המחייבים את המוסדות הרפואיים. בנוסף, גם אם החוקר הוא גורם מטפל הנחשף למידע אישי של מטופליו במסגרת הטיפול הרפואי בהם, אין הדבר מלמד שבאפשרותו להיחשף למידע רפואי נוסף, לאוספו ולהשתמש בו לצורכי מחקר, בפרט כשהדבר נעשה ללא הסכמת המטופלים. תשובת המשרד גם אינה תואמת את הדברים שנמסרו לנציגיו של משרד מבקר המדינה מוועדת הלסינקי העליונה, שהבהירה כי חוקר שאינו המטפל לא ייחשף למידע מזהה. לפיכך עליו לחדד עמדתו בעניין זה, להבהירה למוסדות הרפואיים ולתקן את נהליו בהתאם.

3. עוד נמצא כי גם כשהמוסד הרפואי מעביר לחוקרים מידע שאינו מזהה, הדבר נעשה באמצעות קידוד בלבד ולא באנונימיזציה מלאה כאמור בהנחיות משרד הבריאות, בכל מוסד רפואי בהתאם לשיטתו. מהמחלקה לניסויים קליניים נמסר לצוות הביקורת, כי למעשה אי אפשר לבצע מחקר במידע אנונימי והדרישה האמורה בנוהל ניסויים רפואיים בבני אדם אינה ישימה.

למשל, בבקרה של משרד הבריאות על ועדת הלסינקי של בית החולים שיבא במרץ 2017 ביקשו נציגי בית החולים מנציגי המשרד התייחסות לדרישות רגולטוריות סותרות בנושא חסיון מידע - מצד אחד, ויתור על הסכמה מדעת מחייב הפרדת הפרטים המזהים כך שלא יתאפשר לחזור למטופל. מצד שני, במסגרת המחקר יש להוכיח כי הנתונים מבוססים וניתנים לאימות. הפתרון שמצא בית החולים הוא קידוד כפול של המידע, שמפתחותיו מצויים אצל הוועדה המוסדית.

משרד הבריאות כתב בתשובתו, כי ככלל מידע שהפרטים המזהים המובהקים הוסרו ממנו, וקודדו בדרכים המקובלות במחקר רפואי, עשוי להיחשב כמידע ברמת התממה מספקת למחקר - בהתאם לטיב המידע ובשיטות שנקטו.

מהאמור לעיל עולה סתירה מובנית בין כללי משרד הבריאות, המחייבים אנונימיזציה מלאה של מידע המועבר ללא הסכמה במחקרי נתונים, ובין המידע הנדרש לצורך מחקר, שהוא מידע שניתן לזיהוי חוזר בעת הצורך (על מנת להוכיח כי הנתונים אמיתיים ואף לטובת המשתתפים בניסוי, אם יתגלה במחקר מידע חשוב לבריאותם). מהאמור עולה, כי מחקרי נתונים בישראל נערכים בניגוד לכלל האנונימיזציה האמור, ועל משרד הבריאות לבחון מחדש את הסוגיה כולה.

מספר נושאי המידע במחקר עשוי להיות מטופלים ספורים עד מאות או אלפים, למשל במחקר הנערך במקביל בכמה בתי חולים, ורבים עוד יותר במחקרים בנתוני עתק. על משרד הבריאות בשיתוף משרד המשפטים לפעול לקביעתם של כללי התממה מתאימים, בשים לב לצורכי המחקרים מזה ולחובת ההגנה על פרטיותם של נושאי המידע מזה. כמו כן עליו לפעול להנחות את ועדות הלסינקי והמוסדות הרפואיים העורכים את הניסויים בנושא ולפקח על יישום הכללים שייקבעו.

פיקוח על מחקרים

בהתאם להוראות הדין ונהלי משרד הבריאות, הפיקוח על עריכת המחקרים נעשה באמצעות שלושה גורמים: ועדת הלסינקי המוסדית, ועדת בקרה מוסדית¹⁴⁴ והמחלקה לניסויים קליניים. הבקורות נועדו להבטיח את רמתם המקצועית של המחקרים, את בטיחותם ואת שמירת כללי האתיקה, לרבות בקשר להסכמתם של המטופלים נושאי המחקר למחקר ובקשר להגנה על פרטיותם.

בנוהל 144/01 של המחלקה לניסויים קליניים מפרברואר 2017 בנושא פיקוח ובקרה על ניסויים רפואיים בבני אדם (להלן - נוהל פיקוח ובקרה על ניסויים רפואיים) נכתב, כי אחד הנושאים שייבדקו במסגרת הבקורות הוא שמירה על זכויות המשתתפים. שמירה על סודיות המידע היא מן הזכויות הבסיסיות של המשתתפים. בנוהל האמור מובאת דוגמה לרשימת בקרה שאחד הנושאים הנבדקים בה, תחת הכותרת "הגנת הפרטיות", הוא היות המידע הרפואי מקודד טרם העברתו לגורמים חיצוניים ושמירת נתונים במחשב באמצעות מפתח קידוד. בהתאם לנוהל יש לבצע מדי שנה ביקורות בהיקף שלא יפחת מ-5% עד 10% מהמחקרים הפעילים, ובמוסד רפואי שנערכים בו פחות מ-30 מחקרים בשנה - יש לבצע ביקורות על 50% מהמחקרים לפחות. עוד קובע הנוהל, כי יו"ר גוף הביקורת ישלח למחלקה לניסויים קליניים דוח שנתי המסכם את הביקורות שערך¹⁴⁵. הדוח השנתי יועבר עד סוף חודש מרץ של השנה העוקבת.

על פי נתוני המחלקה לניסויים קליניים, מכלל 54 מוסדות, בשנת 2016 לא העבירו דיווחים כנדרש 34 גופי ביקורת, בשנת 2017 - 25 גופים, ובשנת 2018 - 22 גופים.

משרד הבריאות כתב בתשובתו מפרברואר 2019, כי המחלקה לניסויים קליניים פועלת להעלאת שיעור הדיווחים באמצעות שלילת האפשרות לביצוע מחקרים חדשים, עריכת בקורות ועוד.

144 ועדה פנימית של מוסד רפואי המבקרת את אופן ביצוע המחקר הרפואי ומונה שלושה חברים לפחות - על היו"ר להיות נציג בכיר של הנהלת המוסד שהוא בעל מקצוע רפואי או יועץ משפטי.

145 בחזור מנכ"ל משרד הבריאות 7/05 שקדם לנוהל 144 נקבעה חובת דיווח חצי שנתי של גוף הבקרה למשרד הבריאות.

נמצא, כי בית החולים אסף הרופא אינו מבצע ביקורת בנושא התממה אף שעמדת משרד הבריאות היא שעליו לבדוק הנושא במסגרת הבקורות. מעיון ב-66 דוחות הבקרה לשנים 2015 - 2017 של גוף הבקרה באסף הרופא עולה, כי באחד מהם בלבד הייתה התייחסות - לקונית - לנושא המידע האישי וצוין כי המחקר נערך על סמך נתונים מתיקים רפואיים תוך שמירה על אלמוניותם של המטופלים.

מבית החולים אסף הרופא נמסר לנציגי משרד מבקר המדינה, כי נושא ההתממה והעברת המידע אינו עיקר עיסוקה של ועדת הבקרה, ותפקידה לבדוק את הפן הקליני של המחקר. בעניין הגנת הפרטיות, יש לפעול בהתאם לנהלי אבטחת המידע של משרד הבריאות לגבי מידע רפואי. בתשובתו למשרד מבקר המדינה הוסיף בית החולים, כי בקרת ההגנה על הפרטיות אינה נדרשת במפורש בנוהל משרד הבריאות אך לאור עמדתו של משרד מבקר המדינה יוכנס הנושא כדגש לבקורות הבאות שתערוך הוועדה.

נמצא שככלל במסגרת בקורתה על המחקרים במוסדות הרפואיים, המחלקה לניסויים קליניים במשרד הבריאות אינה בודקת אם הועבר מידע רפואי אישי על מטופלים לגורמים שאינם מורשים.

משרד הבריאות ציין בתשובתו כי הוא רואה חשיבות רבה בשמירת סודיות ופרטיות של מטופלים ופועל לחידוד ההנחיות והנהלים בנושא. עוד ציין המשרד כי הוא עורך בקורות גם בנושא זה אך בשל מחסור חמור בכוח אדם במחלקה לניסויים קליניים הוא פועל בהתאם לתוכנית ניהול סיכונים.

משרד מבקר המדינה מעיר למשרד הבריאות, כי עליו לוודא שהמוסדות מבצעים בקורות בהתאם לכללים שקבע, לרבות עמידה ברף הבקורות הנדרש, לבחון את דיווחיהם של גופי הבקרה במוסדות ולוודא כי המוסדות פועלים ליישום הממצאים העולים מהם. כמו כן עליו לשקול לכלול במפורש בנוהל פיקוח ובקרה על ניסויים רפואיים את ההגנה על הפרטיות בכלל ואת ההתממה בפרט. עליו גם לבחון דרכים לפיקוח ובקרה על העברת המידע הרפואי במסגרת המחקר לחוקרים וליזמים.



מידע רפואי הוא מסוגי המידע הרגישים ביותר. הביקורת העלתה כי משרד הבריאות אינו מקיים פיקוח מיטבי על אבטחת המידע במוסדות הרפואיים ורבים מהם אף אינם מוסמכים לתקן לניהול אבטחת מידע במערכות הבריאות. על משרד הבריאות להרחיב את היקף הפיקוח בנושא זה, בשם לב לסיכונים הקיימים. עליו להשלים את תהליך האסדרה בנוגע להגנה על פרטיות המידע במסגרת מחקרים רפואיים, ובפרט במחקר בנתונים ללא הסכמת נושאי המידע, ולקיים פיקוח גם בנושא זה במסגרת הבקורות על מחקרים רפואיים. משרד הבריאות נדרש גם לפעול להסדיר את פעילותה של המערכת לשיתוף מידע רפואי, בחקיקה ראשית או משנית, כפי שייקבע בתיאום עם משרד המשפטים.

סיכום

הזכות לפרטיות מאפשרת לכל אדם לחיות את חייו ללא התערבות ולממש את רצונותיו והחלטותיו באופן אוטונומי. רשם מאגרי המידע העומד בראש הרשות להגנת הפרטיות הוא הרגולטור המופקד על הגנת המידע האישי במאגרי מידע. דוח זה מציין ליקויים בפעולות הרשות שנמצאו בביקורת, ובכלל זה מעורבות מצומצמת של הרשות בסוגיות הגנת הפרטיות במאגרי מידע העולות במגזר הציבורי והיעדרה של מדיניות אכיפה ברורה.

הביקורת במשרדי הבריאות והחינוך העלתה תמונה מדאיגה, לפיה הם מבצעים פרויקטים מקיפים או פועלים לאיסוף מידע אישי רב מבלי שהוסדרה כראוי המסגרת הנורמטיבית לכך. נוסף על כך נמצאו ליקויים במדיניות אבטחת המידע וביישומה. בניגוד לנדרש בדיון, למשרד החינוך אין תמונה מלאה ומפורטת של מאגרי המידע שלו או של הספקים המחזיקים במאגרי המידע שלו; והוא אינו מפקח על הספקים בהיבטים של אבטחת מידע והגנה על פרטיות. משרד הבריאות אינו מקיים פיקוח מיטבי על אבטחת מידע במוסדות הרפואיים. אין למשרד מיפוי של המוסדות הטעונים רישיון שאינם מחזיקים בתקן לניהול אבטחת מידע במערכות בריאות, ורבים מהם אף אינם מוסמכים לתקן זה. המשרד אינו מקיים פיקוח מיטבי על ההגנה על פרטיות המידע של מטופלים שנעשה בו שימוש במחקרים רפואיים.

תנאי הכרחי לשיפור ההגנה על הפרטיות ולהטמעת הזכות לפרטיות הוא מחויבות ארגונית של המערכת הציבורית בישראל. הדברים באים לידי ביטוי גם בכמה החלטות ממשלה, המבססות את תפיסת השקיפות השלטונית ומחייבות שיקולים של הגנת פרטיות במסגרת יישומן. נוכח הממצאים המובאים בדוח זה, הנהלותיהם של משרדי החינוך והבריאות נדרשות להתגייס להכוונה ברורה של הגורמים האחראים לאבטחת המידע המשרדי, ולנקוט פעולה נמרצת לתיקון הליקויים ולהגנה אפקטיבית על הזכות לפרטיות, כנדרש בדיון.

כבר בתחילת שנות האלפיים הכיר משרד המשפטים בצורך בתיקונים בחוק הגנת הפרטיות ובתקנותיו, אך רובם לא קודמו או לא הושלמו. נראה כי בתחום זה של הגנת הפרטיות יש פער מובנה בין החקיקה, הממושכת מטבעה, ובין ההתפתחות הטכנולוגית המהירה. פער זה מגביר את הצורך לפעול בנחישות ובמהירות, על מנת לשמור על רלוונטיות של הוראות הדיון במציאות המשתנה. על משרד המשפטים לקיים עבודת מטה בעניין חוק הגנת הפרטיות, לבחון את התיקונים הנדרשים בדיון הגנת הפרטיות, לתעדפם ולקבוע לוחות זמנים לקידומם, הן לשם הגנה על זכויותיהם של נושאי המידע בישראל והן לשם שמירת מעמדה של ישראל כמדינה המבטיחה הגנה על מידע אישי ברמה נאותה התואמת את הדיון האירופי.