שרון ברז־זיו*
וטל ז'רסקי**

פרטיות במשבר זהות: אסטרטגיות הסדרה בעידן ההתממה

א. מבוא

הסדרת הפרטיות היא סוגיה מורכבת המעוררת שאלות רבות בכמה ממדים. בצד שאלות המהות,[1] שאלות רבות נוגעות לדרכי ההסדרה, האסדרה והאכיפה של הזכות לפרטיות ולהגנת המידע.[2] מקרב שאלות אלו, הנוגעות לדרך ההסדרה, נובעת השאלה בדבר אסטרטגיית ההסדרה, המתמקדת באופי הגוף המסדיר או המאסדר וכן בגוף האוכף: האם ראוי שגוף כללי אחד יסדיר (או יאכוף) את כל סוגיות הפרטיות במדינה או שמא רצוי כי רגולטור סקטוריאלי יציע מתווה אסדרה ויפקח על הגופים הציבוריים והפרטיים בתחום מומחיותו? הסוגיה של אסטרטגיית ההסדרה מערבת שיקולים ייחודיים, הנוגעים לממשק שבין עולם המשפט לטכנולוגיה כמו גם להגנה על זכויות אדם מחד גיסא ולקידום מגוון אינטרסים חברתיים מאידך גיסא.

מאמר זה יציג וידגים את השאלות והקשיים העולים מסוגיית האסטרטגיה של הסדרת הפרטיות בישראל בהקשר חדשני, הנוגע להעברת מידע פרטי מגופים ציבוריים תוך שימוש בהתממה (anonymization או de-identification).[3] ההתממה היא תהליך הכולל הן רכיבים

---

* ד"ר, מרצה במכללה האקדמית ספיר, בית הספר למשפטים. עמיתת מחקר במרכז לחקר סייבר, משפט ומדיניות, אוניברסיטת חיפה.

** סגן דיקן ופרופסור, הפקולטה למשפטים, אוניברסיטת חיפה. ברצוננו להודות לפרופ׳ מיכאל בירנהק ולקורא החיצוני על הערותיהם מאירות העיניים, לפרופ׳ אור דונקלמן על הערותיו וסיועו להבנה של טכנולוגיות ההתממה ולמשתתפי פורום הסייבר הישראלי באוניברסיטת קולומביה ניו יורק (אוקטובר 2017). מחקר זה נתמך על ידי המרכז לחקר סייבר, משפט ומדיניות באוניברסיטת חיפה, שהוקם בשיתוף מערך הסייבר הלאומי במשרד ראש הממשלה, וכן על ידי המרכז הבינלאומי לסיכון, אחריות וביטוח על שם אפטוביצר.

1 דוגמה לשאלות מהות: על אילו אינטרסים ראוי להגן ואיזה הסדר משפטי חל בנסיבות מסוימות?

2 כך, למשל, ישויות פדרליות (דוגמת ארצות־הברית, גרמניה ואף האיחוד האירופי) נדרשות לשאלה אם ראוי להסדיר סוגיות הנוגעות לפרטיות בהסדרה מקומית, ארצית או על־מדינתית. לדיון בהסדרת הפרטיות ברמה המקומית ראו Ira Rubinstein, *Privacy Localism* (NYU Sch. of Law, Pub. Law Research Paper No. 18-18, 2018), https://goo.gl/YSjthp. כמו כן, מדינות רבות נדרשו לשאלה אם ראוי להסדיר סוגיות שונות הנוגעות לפרטיות במערך חקיקה כללי ואחיד או שמא רצוי לאמץ מערך של חקיקה פרטנית המבחין, למשל, בין סוגיות של פרטיות בסקטורים שונים (גישת הריבוד התוכני).

3 לדיון ראשוני בעניין ההתממה בישראל ראו מיכאל בירנהק "חשיפה מקוונת וחשיפה משפטית – על פרטיות ופומביות של פסקי דין ברשת" **משפטים** מח 31 (2018); רחל אריידור־הרשקוביץ ותהילה שוורץ־אלטשולר **אתגר הפרטיות בפרסום יזום של מאגרי מידע ממשלתיים** 18 (2017) https://goo.gl/JKBa25. לדיון ראשוני בדבר אסטרטגיות אסדרה לסוגיה זו ראו Daniel Goroff,

טכנולוגיים והן רכיבים מנהליים. מטרתו להפוך מידע אישי מוגן לכזה המנותק מכל מאפיין שמזהה את מושאו, וכך יתאפשר להשתמש במידע למטרות מגוונות. במאמר נטען ונראה כי בישראל מתפתחים בו־זמנית, במנותק וככל הנראה ללא כל יד מכוונת, כמה משטרים נפרדים הנוגעים להתממה או מסדירים אותה. כמו כן נטען כי לעתים משטרים אלו נשענים על מערכות דינים שונות. המאמר יציג את ההתפתחות של אסטרטגיות ההסדרה בהקשר זה, ינתח אותן בעין ביקורתית ויניח תשתית לדיון עתידי בהסדרת הפרטיות בהקשרים אחרים כגון הסדרה של מרחב הסייבר.

בשנים האחרונות, כמה גופים ציבוריים בישראל מקיימים פעילות מגוונת של ניתוח נתונים והנגשתם. דוגמאות מרכזיות הן משרד הבריאות וקופות החולים, הלשכה המרכזית לסטטיסטיקה ורשות התקשוב הממשלתי. פעילות זו מבוססת על נתונים ומידע אישי הנאספים עלינו באופן מתמיד ובהיקפים ניכרים הן על ידי גופים פרטיים והן על ידי גופים ציבוריים.[4] מגמה זו משתלבת היטב עם עידן נתוני העתק (big data) שבו טכנולוגיות מתקדמות אוספות מידע רב ואף מאפשרות את עיבוד המידע וניתוחו בהיקף רחב ולמטרות שונות.

עידן נתוני העתק בכלל, ואיסוף נתונים וניתוח מידע על ידי גופים ציבוריים בפרט, טומנים בחובם יתרונות ניכרים כמו העמקת ידע, שיפור בהליכי קבלת החלטות ושקיפות בממשל,[5] הגברת היעילות במגוון הקשרים, פיתוח חדשנות וקידום השיח הדמוקרטי כולו.[6] בצד יתרונות אלו, פעילות זו מעוררת חשש מפני פגיעה בפרטיות – שימוש במידע לשם פגיעה וביוש (shaming), מעקב, אפליה, הרחקה ואבדן שליטה על המידע ותוצריו. לפיכך, בדיקת ההשפעה של דיני הפרטיות מבחינת הדין הרצוי והמצוי היא הכרחית בכל מקרה של העברת מידע והנגשתו על ידי רשות ציבורית.

נראה שכאשר המידע הנאסף ניתן לזיהוי הוא חוסה תחת חוק הגנת הפרטיות, התשמ"א-1981 (להלן: חוק הגנת הפרטיות או החוק)[7] או תחת הגנתם של דיני הפרטיות בישראל בכלל. לעומת זאת, מידע שאינו מזהה את מושא המידע אינו נתון למגבלות החוק ואין הגבלה על איסופו, על עיבודו ועל השימוש בו. לפיכך, אחת הדרכים להימנע מתחולתו של חוק הגנת הפרטיות – והלכה למעשה להשתמש במידע כמעט ללא הגבלה – היא ביצוע התממה למידע אישי. כפי שנראה בהמשך, מנגנון זה יעיל גם בהקשר של חקיקה המגנה על פרטיות

Jules Polonetsky & Omer Tene, *Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data*, 675(1) Annals aapss 46, 55-56 (2018); Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703, 713 (2016).

4 להלן במאמר זה נניח כי המונח נתונים (Data) מתייחס לעובדות כגון מספרים, מילים או תמונות, ומידע (Information) הוא ארגון הנתונים באופן המעניק להם משמעות.

5 לדיון בנושא התכלית הדמוקרטית והכלכלית של פרסום מידע ממשלתי ראו אירידור־הרשקוביץ ושוורץ־אלטשולר, לעיל ה"ש 3, בעמ' 18.

6 ראו, לדוגמה, Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239 (2013).

7 חוק הגנת הפרטיות, התשמ"א-1981, ס"ח 128. חשוב לציין כי הגדרת "מידע" בס' 7 לחוק מתייחסת ל"נתונים [...] של אדם", וכלל לא ברור שאפשר ללמוד מכך על דרישת זיהוי; מכל מקום נניח שדרישה זו קיימת.

היחיד בהקשרים ספציפיים. אנו נוקטים עמדה זו בזהירות, שכן בשונה מהדין האירופי, רכיב הזיהוי (או ה"מזוהות"; identifiability) לא עוגן במפורש בחוק הגנת הפרטיות הישראלי ואנו נדרשים להקיש מחקיקה דומה מעבר לים.[8]

עם זאת, בעידן נתוני העתק מתעורר חשש מפני סכנות של תקיפת ההתממה וביצוע של זיהוי חוזר (re-identification), וכתוצאה מכך – חשיפה אפשרית של מידע אישי על ידי מי שלא אמור להיחשף אליו או להחזיק בו. תוקף פוטנציאלי עשוי לנסות להצליב מידע מכמה מקורות כך שיוכל להתגבר ולו חלקית על מנגנוני ההתממה, לזהות את המידע שבמאגר המותקף וליחס אותו לאדם ספציפי. מדובר בחשש משמעותי וממשי נוכח ההתפתחות הטכנולוגית בתחום זה. גם אופיו המבוזר של המידע האישי בעת הזו מאפשר לתוקף לרכז בידיו מידע רב ממקורות שונים ולא צפויים, ולהגדיל את הסיכוי להצלחת ההתקפה דנן.

כבר בשלב זה חשוב לציין כי על פי רוב התממה אינה תהליך המוביל לתוצאה מובחנת באופן דיכוטומי, כלומר המידע מזוהה או שאינו מזוהה. כמעט כל מאגר מידע (לרבות כאלו שעברו התממה) נתון בכל עת בנקודה כלשהי על טווח שבין שתי נקודות – מידע מזוהה ומידע שאינו ניתן לזיהוי. עם זאת, תפיסת התוצאה של הליך התממה ככזה המייצר תוצאה דיכוטומית היא עדיין נחלתם של רגולטורים, גופי ממשלה וגופים פרטיים רבים כאחד.[9] אימוץ הסתכלות גמישה יותר במונח ההתממה הוא מאתגר, אך לתפיסתנו הוא הכרחי להתמודדות עם סוגיות הפרטיות שנציג להלן.

בהתחשב בהיקפים של איסוף נתונים ושימוש במידע, סוגיות ההתממה והחשש מפני זיהוי חוזר נהפכו לאחרונה לחשובות ורלוונטיות כמעט לכל גוף בישראל – פרטי וציבורי כאחד – שבידו מידע בהיקף ניכר. כאמור, מדינות רבות בעולם כבר נתנו דעתן לדרך הראויה לביצוע התממה, הן ברמת התוכן והן ברמת האסטרטגיה. אולם, הליך דומה של עיצוב מדיניות מרכזית, כמו גם שיח בדבר עיצוב מדיניות זו, טרם נערך בישראל. לפיכך, מאמר זה מבקש לבחון באופן השוואתי התמודדות של אוצרי מידע ומאסדרים (רגולטורים) ציבוריים שונים, כמו גם של בתי המשפט בישראל, עם הסוגיות המתעוררות עקב הליכים של התממת נתונים ועם הדרכים להסדרתן. המאמר יתמקד בבחינה ביקורתית של ההתפתחות הבו־זמנית של משטרי התממה שונים. בסופו של דבר, ובאופן שאינו בהכרח אינטואיטיבי, נטען כי התפתחות בו־זמנית זו עשויה להיות ראויה ולהוביל לתוצאות מתאימות במובן של הגנת הפרטיות ושל קידום יעדים חברתיים.

הדיון במאמר ייערך כדלקמן: לאחר מבוא זה נציג רקע תאורטי קצר הדן במודלים של הסדרה, ובמיוחד הסדרה מקבילה של סוגיות הנוגעות לפרטיות. החלק השלישי יציג את המסגרת המשפטית בישראל בהקשר של התממת מידע אישי, תוך התייחסות לחקיקה כללית ופרטנית. כדי להבין את ההקשר הייחודי שבו עוסק מאמר זה, נציג בחלק הרביעי את האינטרסים שבבסיס ההתממה ואת הרבדים השונים שלה, תוך הסתמכות על שאלות

8 שם. ראו גם משרד המשפטים **הצוות לבחינת החקיקה בתחום מאגרי המידע** 20 (2007), אשר קובע כי יש לאמץ את הגדרת מידע, לעניין סעיף 7 לחוק כמידע מזוהה או ניתן לזיהוי https://goo.gl/TJJnGT.

9 ראו Jules Polonetsky, Omer Tene & Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara L. Rev. 593, 598 (2016).

וסוגיות שהתעוררו בעניינים אלו במדינות אחרות. החלק החמישי יציג את הפרקטיקה של התממת נתונים כפי שהיא באה לידי ביטוי בפסיקת בתי המשפט ובעמדות של גופים ציבוריים נבחרים בישראל. נראה את עליית השיטות להסדרת סוגיה זו בזרועות שלטון שונות; תוך הסתמכות על מקורות ידע אלו יציג החלק השישי ניתוח רוחבי של האסטרטגיות להסדרה של העברת מידע בין גופים ציבוריים. והחלק האחרון יסכם את הדיון בעניין זה ויתווה כיווני מחקר עתידיים.

ב. אסטרטגיות להסדרת פרטיות: מבט־על

במאמר זה נתמקד בהסדרה של תהליך ההתממה, סוגיה בעלת השלכות רחבות על כלל דיני הפרטיות בישראל. אחת השאלות הנובעות מסוגיה זו היא השאלה אם ראוי להפקיד את ההסדרה בידי גורם מרכזי אחד או לאפשר התפתחות הטרוגנית המקודמת על ידי גופים מקצועיים המתמודדים עם סוגיות משמעותיות הנוגעות לפרטיות.

סוגיה פרקטית זו – הרבדים של אסדרת הפרטיות – נהנתה מדיון תאורטי מקיף ובכמה הקשרים, כפי שיפורט בהמשך. הדיון בהקשרים אלו בחלקו אינו רלוונטי למצב העובדתי בישראל, אך אפשר להקיש מהתובנות העולות ממנו לענייננו. לדוגמה, הרובד המקובל הראשון לדיון בסוגיה של הסדרת הפרטיות נוגע לשאלה אם ראוי להסדיר סוגיות הנוגעות לפרטיות בהסדרה מקומית או שמא ארצית (או אולי אפילו על־מדינתית, במדינות שהן חלק מפדרציה או קונפדרציה).[10] עם אימוץ רגולציית הגנת הפרטיות האירופית (General Data Protection Regulation, GDPR)[11] ניכר כי האיחוד האירופי דוגל בהסדרה על־מדינתית, כאשר בארצות־הברית העניין המדובר פתוח ונתון לתמורות לאור שינויים בחקיקה ואכיפה ברמה המדינתית והפדרלית.[12]

הספרות שבחנה חלופות אלו מסבירה, מחד גיסא, כי פיצול מקומי יוביל ליתרונות שכן הוא מאפשר ריבוי דעות ומתן ביטוי להעדפות שונות.[13] מאידך גיסא, הפיצול האמור יוצר

10 למרות שהסוגיה נראית מנותקת לחלוטין מהדין הישראלי, ייתכן שהיא תתעורר בנוגע לחקיקה עירונית המגנה על פרטיות, ככל שתהיה כזו. להתמודדות עם סוגיה זו שאך מתעוררת בארצות־הברית ראו The California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code § 1798.198(a) (2018); Lothar Determann, Analysis: The California Consumer Privacy Act of 2018 *IAPP Privacy Tracker*, https://goo.gl/WvZ9Z1; ראו גם Rubinstein, לעיל ה"ש 2, הדן בחקיקה מקומית הנוגעת לפרטיות ברשויות מקומיות שונות בארצות־הברית.

11 Regulation 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 on the Free Advancement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1. The General Data Protection Regulation of the EU, (להלן: GDPR).

12 עניין זה שב לאחרונה לכותרות בארצות־הברית עם העברת חוק הגנת פרטיות מקיף ומחמיר במדינת קליפורניה, שייכנס לתוקף ב־2020. לעניין זה ראו The California Consumer Privacy Act, לעיל ה"ש 10.

13 ראו, לדוגמה, Regulatory Competition and Economic Integration: Comparative Perspectives (Daniel C. Esty & Damien Géradin eds, 2001).

בעיות, שכן ניהול של פעילות עסקית במשטר שבו החוקים משתנים ממקום למקום הוא עניין מורכב, יקר ומוביל לשגיאות. כמו כן, הדיון בסוגיה זו כולל התייחסות לניתוח ברמת הכלכלה הפוליטית, שעיקר הדיון הוא מי ממקבלי החלטות השונים "עמיד" יותר אל מול לחצים ואילו גורמי שלטון מועדים לשבי רגולטורי.[14]

למרות החשיבות של הדיון המתואר לעיל, לצורך בחינת המצב הרצוי בישראל רלוונטי יותר הדיון הנוגע לריבוד התוכני. בהקשר זה עולה השאלה אם ראוי להסדיר סוגיות הנוגעות למידע אישי ולפרטיות באמצעות הסדרה כללית או פרטנית. שאלה זו מתעוררת בכמה הקשרים. האחד נוגע לחקיקה ראשית: האם ראוי להסדיר סוגיות הנוגעות לפרטיות במערך חקיקה כללי ואחיד (הסדרה ריכוזית), או שמא רצוי לאמץ מערך חקיקה פרטנית שמבחין בין סוגיות של פרטיות בסקטורים שונים (הסדרה סקטוריאלית)? שאלה נוספת הנובעת ממנה נוגעת לאופי הגוף המסדיר או המאסדר: האם ראוי שגוף אחד יסדיר את כל סוגיות הפרטיות, או שמא רצוי כי רגולטור סקטוריאלי יציע מתווה אסדרה ויפקח על הגופים הציבוריים והפרטיים שבתחום מומחיותו?

האיחוד האירופי הוא דוגמה מובהקת להסדרת פרטיות ריכוזית ברמה החוקית והמוסדית. ה־GDPR קובע מסגרת החולשת על מכלול סוגיות הפרטיות, וה־Data Protection Agency (DPA) המדינתי אוכף את כללי הפרטיות.[15] למרות זאת, גם באיחוד האירופי יש לכלל זה חריגים דוגמת רגולטורים ייחודיים שממליצים על מדיניות מתאימה בתחום המידע הרפואי.[16] לעומת זאת, ארצות־הברית היא דוגמה להסדרה סקטוריאלית המותווית ברשימה ארוכה של חוקים ספציפיים. כמו כן, האחריות על חוקים אלו מתפרסת על פני רגולטורים שונים (וחלק מהאסדרה נעשה כאסדרה עצמית; self-regulation).[17]

על פני הדברים נראה כי ישראל נטועה עמוק בשיטה הדוגלת בהסדרה ובאכיפת פרטיות ריכוזית, כאשר חוק הגנת הפרטיות חולש על כל תחומי המשפט הפרטי והציבורי. יתרה מזו, הרשות להגנת הפרטיות אמורה לעסוק בהגנה על הפרטיות בכל ההקשרים, והדבר עומד לפני עיגון בהצעת חוק לעדכון דיני הפרטיות שנדונה בכנסת, למעט כמה חריגים הנוגעים לגופים ביטחוניים.[18] אולם, לעניין מדיניות התממה, נראה כי נותרו בישראל כמה כיסי אוטונומיה להסדרת הפרטיות דוגמת הלשכה המרכזית לסטטיסטיקה (להלן: הלמ"ס) וגורמים בריאותיים למיניהם דוגמת משרד הבריאות, קופות החולים ורשות התקשוב. גופים אלו עוסקים בשנים האחרונות בבחינה של הסדרת הפרטיות במידע שנוצר במסגרת פעילותם, והם אף אמונים על ריכוז מידע אישי רב מכורח תפקידם. לפיכך, הדיון האקדמי

14 השחיתות בחלק המקומי רבה יותר; ראו Guillermo Beylis, Frederico Finan & Maurizio Mazzocco, *Understanding Corruption: Theory and Evidence from the Audits of Local Governments* (2012), https://goo.gl/7PZ8kQ, המסתמך, בין היתר, על Susan Rose-Ackerman, Corruption and Government: Causes, Consequences, and Reform (1999).

15 GDPR, לעיל ה"ש 11, בס' 51, מתייחס לתפקיד הגוף המפקח בכל מדינה ולסמכויותיו.

16 European Medicines Agency Policy on Publication of Clinical Data for Medicinal Products for Human Use, EMA/240810/2013 (2014).

17 ראו דיון מפורט בעניין זה להלן בחלק ד(2)((2)) (הכולל פירוט של הגורמים המסדירים בארצות־הברית ובאיחוד האירופי).

18 הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח-2018, ה"ח 1206.

בסוגיה זו הוא בעל משמעויות פרקטיות לנעשה בישראל היום, במיוחד לעניין ההחלטה מי יוביל את הסדרת ההתממה.

לקיומה של ההסדרה הסקטוריאלית יש חסרונות מובהקים וחלקם נלמדים מהדיון לעיל בדבר ביזור גאוגרפי. הדבר מוביל להיעדר קוהרנטיות במערכת המשפט. כמו כן, הסדרה סקטוריאלית מובילה למצבים שבהם גופים דומים כפופים למערכות הסדרה שונות.[19] בעיה זו מתעצמת בהקשרים טכנולוגיים שבהם שווקים נוטים לשנות צורה ושחקנים עוברים מחסות תחת הגדרה אחת לאחרת תוך התרחבות לתחומי עיסוק ופעילות שונים. נוסף על כך, יש להניח שרשות מרכזית אחת תצבור ידע ומומחיות בסוגיות הנוגעות להסדרת הפרטיות, ועל כן יעיל יותר שרק היא תעסוק בכך. ביזור הסמכות בין כמה רשויות לא רק יפזר את הידע אלא גם יוביל לכפילות בתפקידים ולבזבוז משאבים ציבוריים. עוד ייתכן שמכוח האינטרס הלאומי בהקטנת השחיתות עדיף לרכז סמכויות אצל גוף אחד ולדאוג לחסנו ולבודדו מלחצים.[20]

בצד אלה יש גם יתרונות להסדרה סקטוריאלית (שהם חסרונות של ההסדרה הריכוזית). הטענה המעניינת והרלוונטית ביותר לענייננו נוגעת לחדשנות ולקיבעון רגולטורי.[21] חוקרי פרטיות מסבירים – תוך הסתמכות על תופעות דומות שהתרחשו בהקשרים של דיני איכות הסביבה ודיני עבודה[22] – כי הסדרה ריכוזית עשויה להוביל לקיבעון ולקיפאון. זאת, משום שחוקים רחבי־היקף קשים לשינויים התכופים הדרושים עקב השינויים החברתיים והטכנולוגיים.[23] הקושי שאנו רואים בישראל בעדכון חוק הגנת הפרטיות, כמו גם פרק הזמן הארוך שחלף עד לחיקוק ולאישור של ה־GDPR עשויים להיות אינדיקציה לנכונות טענה זו (ולפחות אינם מפריכים אותה). מצד שני, הביזור הרגולטורי לסקטורים, תוך מתן אוטונומיה לרגולטור הסקטוריאלי במסגרת סביבתו, מאפשר לערוך ניסיונות בכל אחד מההקשרים הללו, היכולים להתקדם גם ללא הצורך בחיקוק חוקים מרכזיים חדשים ובכך להתמודד עם המציאות המשתנה.[24] בכך, גופים סקטוריאליים אלו יכולים לעזור לשינוי הסטטוס קוו ולקדם את החברה ואף את הדמוקרטיה.[25] בדומה, האסדרה וההסדרה הסקטוריאליות מאפשרות לערוך ניסיונות רגולטוריים ואף טכנולוגיים בהקשרים מבודדים, ואם אלה יצלחו

19 Paul M. Schwartz, *Preemption and Privacy*, 118 Yale L.J. 902, 924 (2009).

20 ניתוח זה לקוח מעולם הכלכלה הפוליטית. ראו Antonio Cabrales, *Decentralization, Political Competition and Corruption*, 105 J. Devel. Econ. 103 (2013).

21 Bilyana Petkova, *The Safeguards of Privacy Federalism,* 20(2) Lewis & Clark L. Rev. 595, 599 (2016).

22 Schwartz, *Preemption and Privacy*, לעיל ה"ש 19, בעמ' 928, המפנה לעניין זה לכתיבתה של Cynthia L. Estlund; Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 Colum. L. Rev. 1527, 1574 (2002).

23 Schwartz, שם.

24 Paul M. Schwartz, *The Value of Privacy Federalism, in* Social Dimensions of Privacy: Interdisciplinary Perspectives 324, 334-33 (Beate Roessler & Dorota Mokrosinska eds., 2015).

25 Petkova, לעיל ה"ש 21, בעמ' 599.

הם יועתקו גם להקשרים אחרים.[26] אפשר גם להוסיף כי בגופים המבוזרים עשוי להימצא ידע ייחודי הנוגע לגוף המוסדר ועשוי להעשיר את הסדרת הסוגיה הטכנולוגית החדשנית.[27] לבסוף, תחרות בין מקבלי החלטות מובילה להחלטות טובות יותר (בבחינת "קנאת סופרים תרבה חוכמה").[28]

יתרונות אלו של ההסדרה הסקטוריאלית הובילו את חוקר הפרטיות פול שוורץ (Schwartz) לסבור כי מערך ההסדרה המבוזר הקיים בארצות־הברית כיום הוא רצוי. אולם, הוא הוסיף וסבר (תוך הסתמכות על מחקריהם הכלליים יותר של Feeley and Rubin) כי אף לסקטוריאליות יש גבול, וכי נדרש מוקד ריכוזי שיאתר את אותן הצלחות רגולטוריות וידאג ליישמן גם בהקשרים אחרים. מעבר לכך, יש אף אינדיקציות למקרים בארצות־הברית שבהם הפרתה ההסדרה הסקטוריאלית את זירת ההסדרה והובילה לאימוץ קווים חדשים על ידי הרגולטור הפדרלי.[29]

כאמור לעיל, ישראל, לפחות על פני הדברים, נוקטת מדיניות של הסדרה ריכוזיות, ככל שהדבר נוגע לפרטיות, עם איים של הסדרה סקטוריאלית, כפי שיודגם בפרק הבא. בפרק זה נטען כי בהקשר החדשני והייחודי של הסדרת ההתממה, המשפט הישראלי נתון בצומת דרכים העשויה להוביל לריכוזיות או שמא לביזור. לעת עתה נראה כי מגמת הביזור דומיננטית במשפט הקיים; סקירה תאורטית קצרה זו מראה כי יש לכך יתרונות גם מבחינת הדין הרצוי. בטרם נעסוק ברצוי, נעמיק חקר במצב הקיים.

ג. רקע: המסגרת המשפטית לדיון בהתממה

1. חקיקה כללית המסדירה פרטיות במידע אישי

חלק זה מציג את המסגרת המשפטית לדיון בסוגיה של העברת מידע אישי בין גופים ציבוריים, כחלק מהדיון הנוגע בזכות לפרטיות היוצרת את המניע לביצוע התממה.

הזכות לפרטיות היא מהחשובות בזכויות האדם המוסדרות בחוק הישראלי. מדובר בזכות חוקתית, המוגנת בחוק־יסוד: כבוד האדם וחירותו, ויש לה תרומה משמעותית לעיצוב אופיו של המשטר בישראל כמשטר דמוקרטי.[30] כמו כן, איסור הפגיעה בפרטיות מוסדר במסגרת חוק הגנת הפרטיות[31] שחל אף על רשויות המדינה.[32] סעיף 1 לחוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו".[33] פגיעה בפרטיות מוגדרת כאחת מכמה

26 Schwartz, *Preemption and Privacy*, לעיל ה"ש 19, בעמ' 932.

27 Petkova, לעיל ה"ש 21, בעמ' 624.

28 Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 Yale L.J. 868, 892 (2009); משנה, בבא בתרא, דף כ"א, עמ' א.

29 Schwartz, *Preemption and Privacy*, לעיל ה"ש 19, בעמ' 932.

30 בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי בנתניה**, פס' 8 לפסק דינו של הנשיא ברק (פורסם בנבו, 14.5.2006).

31 חוק הגנת הפרטיות.

32 ס' 24 לחוק הגנת הפרטיות.

33 החוק אינו מגדיר מהי הסכמה אלא מציין בסעיף 3 כי היא צריכה להיות "הסכמה מדעת, במפורש או מכללא".

אפשרויות המוזכרות בסעיף 2 לחוק,[34] בהן הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם,[35] שימוש בידיעה על ענייניו הפרטיים של אדם,[36] פרסום של עניין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, מצב בריאותו והתנהגותו ברשות היחיד.[37] למעשה, אפשר לראות שהמושג "ענייניו הפרטיים של אדם" חוזר בסעיף 2 שלוש פעמים ובמשפט הישראלי מקובלת פרשנות רחבה למושג זה.[38] כאמור, ההתממה למעשה שואפת לאפשר עקיפה של חוק הגנת הפרטיות על ידי הוצאת מידע שהגוף רוצה להעביר הלאה או לעבד מגדר "עניין פרטי".

פרק ב לחוק הגנת הפרטיות עוסק בהגנה על פרטיות במאגרי מידע. מאגר מידע מוגדר כ"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב".[39] "מידע" מוגדר שם כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו", ויש הגדרה נוספת ל"מידע רגיש" שלגביו יש חובות מוגברות.[40] מאגרי מידע הכוללים מידע בהתאם להגדרות אלו כפופים למערכת דינים ייחודית. כך, בהתקיים התנאים הקבועים בחוק הם חייבים ברישום,[41] ואין להשתמש במידע במאגר המידע אלא למטרה שלשמה הוקם (עקרון צמידות המטרה).[42] כמו כן, מחזיק המאגר כפוף לחובות נוספות,[43] לרבות חובה של אבטחת מידע.[44] זו, בין היתר, מערכת הדינים שממנה ינסה בעל המאגר להימנע באמצעות ביצוע התממה.

דרך מרכזית להגשמת ההגנה על הפרטיות היא בקרה על העברה של מידע פרטי ממחזיק אחד לאחר. הסוגיה של העברת מידע בין גופים ציבוריים עצמם ובין גופים ציבוריים לגופים פרטיים מוסדרת בפרק ד לחוק, הקובע כי מסירת מידע מגוף ציבורי אסורה זולת חריגים מסוימים.[45] זה ההקשר המרכזי שבו סוגיית ההתממה מתעוררת נוכח המידע האישי הרב

34 ס' 2 לחוק הגנת הפרטיות.

35 ס' 2(7) וס' 2(8) לחוק הגנת הפרטיות.

36 ס' 2(9) לחוק הגנת הפרטיות.

37 ס' 2(11) לחוק הגנת הפרטיות.

38 ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 222 (2010). המחבר בוחן את עמדת בית המשפט בישראל בנוגע ל"עניינו הפרטיים של אדם" וקובע כי ראוי להעניק למושג זה פרשנות מרחיבה. ראו גם דיונו של בירנהק בעניין **ונטורה**, שם, בעמ' 220. בירנהק מזכיר שהשופט בך קבע בפסק הדין כי "עניינים פרטיים" של אדם הם "כל מידע הקשור לחייו הפרטיים [...] לרבות שמו, כתובתו, מספר הטלפון שלו, מקום עבודתו, זהות חבריו, יחסיו עם אשתו ויתר חברי משפחתו וכדומה"; ראו ע"א 439/88 **רשם מאגרי המידע נ' ונטורה**, פ"ד מח(3) 808, 821 (1994).

39 ס' 7 לחוק הגנת הפרטיות.

40 שם.

41 ס' 8(ג) לחוק הגנת הפרטיות.

42 ס' 8(ב) לחוק הגנת הפרטיות.

43 ס' 16 לחוק הגנת הפרטיות.

44 ס' 17 לחוק הגנת הפרטיות; תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017, ק"ת 1022. ראו גם בירנהק **מרחב פרטי**, לעיל ה"ש 38, בעמ' 226.

45 ס' 23ב לחוק הגנת הפרטיות.

שנמצא בידי גופים ציבוריים, בצד רצונם של אלו לנצלו לצורך קידום אינטרס ציבורי, דבר הכרוך לעתים קרובות בהעברתו לישות אחרת. מסירת מידע אישי הנוגע לאזרחים על ידי גופים ציבוריים מותרת רק בדרכים המוגדרות בחוק. כמו כן, המסירה אפשרית כל עוד היא נעשית במסגרת הסמכויות או התפקידים של מוסר המידע וכל עוד היא דרושה לביצוע חיקוק או במסגרת הסמכויות של מוסר המידע או של מקבלו. כן אפשר להעביר מידע כאמור כשמסירת המידע היא לגוף ציבורי הרשאי לדרוש אותו על פי דין.[46] על פי החוק, גוף ציבורי המוסר מידע נדרש לקיים רישום בעניין.[47] הגוף המקבל את המידע לא ישתמש בו אלא במסגרת סמכויותיו ותפקידיו. מידע שנמסר לגוף ציבורי כמוהו כמידע שהגוף השיג מכל מקור אחר, ויחולו על הגוף המקבל כל ההוראות החלות על הגוף המוסר. כל אלה יוצרים תמריץ משמעותי לגופים הציבוריים להעביר מידע מותמם (בהנחה שהגוף המקבל עדיין יוכל למלא את משימותיו על סמך מידע מותמם בלבד), וכך להימנע מההגבלות הנוקשות שהוצגו כאן בבואם להעביר מידע.

עוד ראוי לציין כי חוק הגנת הפרטיות כולל הוראות והסדרים כלליים נוספים הקשורים לדיון שלפנינו. ראשית, החוק מתייחס "למעשה של מה בכך", וקובע כי לא תהיה זכות לתביעה אזרחית או פלילית לפי החוק בשל פגיעה שאין בה ממש.[48] כמו כן, סעיף 18 לחוק מתייחס להגנות החלות, בין היתר, כשנתבע או נאשם יכול לטעון כי ביצע את הפגיעה בתום לב, כשלא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות.[49] כמו כן, החוק כולל פטור למעשה שהוסמך על פי דין, אך מובן כי דין זה יידרש לעמוד במבחני המידתיות הקבועים בחוק היסוד.[50]

רובד הסדרתי נוסף הנוגע להעברת מידע בין גופים ציבוריים על פי חוק הגנת הפרטיות הוא הוראת המשנה ליועץ המשפטי לממשלה משנת 2006.[51] הוראה זו נועדה להנחות את הגופים הציבוריים בעניין היישום של תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986.[52] כך, נקבע כי בהמשך לסעיף 3א לתקנות, בכל גוף ציבורי המוסר או מקבל מידע יש למנות ועדה להעברת מידע. תפקיד הוועדה הוא לבחון את הבקשות למסירת מידע מהגוף הציבורי, כמו גם את הבקשות לקבלת מידע

46 ס' 23ג(1) לחוק הגנת הפרטיות. חשוב לציין כי על פי ס' 23 ההגדרה של "גוף ציבורי" היא רחבה מאוד וכוללת משרדי ממשלה ומוסדות מדינה אחרים, רשויות מקומיות וכל גוף הממלא תפקידים ציבוריים על פי דין. כמו כן, גופים ציבוריים הם אלו שנקבעו בצו. ראו לעניין זה צו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו–1986.

47 ס' 23ד לחוק הגנת הפרטיות.

48 ס' 6 לחוק הגנת הפרטיות.

49 ס' 18 לחוק הגנת הפרטיות. בנושא זה ראו בירנהק **מרחב פרטי**, לעיל ה"ש 38, בעמ' 242. ראו גם ה"ש 90 בספר האמור לדיון בשאלה אם ההגנות חלות גם על עוולות ועברות לפי פרק ב לחוק, או רק על עוולות לפי פרק א.

50 ס' 19(א) לחוק הגנת הפרטיות.

51 "העברת מידע בין גופים ציבוריים" (חוות דעת של המשנה ליועץ המשפטי לממשלה, 16.3.2006) (להלן: "העברת מידע בין גופים ציבוריים") https://goo.gl/D9y4AF.

52 תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986, ק"ת 858.

של הגוף הציבורי מגוף ציבורי אחר. ההנחיות אף קובעות כי על הוועדה לקבוע אמות־מידה הנוגעות למאגר מידע שברשות גוף ציבורי, ובין היתר להתייחס גם לאופן הגישה למאגר ולצמצום המידע שיש גישה אליו למינימום הנדרש.[53] גם על משוכות אלו אפשר לכאורה לדלג בעת ביצוע ההתממה, אך קיומן מלמד על ההיקף של הגנת הפרטיות (ברמה התוכנית והמוסדית) שהמחוקק ביקש להעניק לאלו שמידע אישי נאסף עליהם על ידי גוף ציבורי.

עוד ראוי לציין כי בספטמבר 2017 פורסמה טיוטה של תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) (תיקון), התשע"ז–2017.[54] התקנות המוצעות מתייחסות לנושאים טכניים הנוגעים להגשת בקשות לקבלת מידע. לענייננו, ההצעה מתייחסת לתקנה 3ד(ב). מדובר בהתייחסות לצורך בחינת בקשה למידע על ידי ועדה שתשקול, בין היתר, אם קבלת המידע המבוקש תביא להגשמת המטרה המוצגת בבקשה, אם יש אמצעי להגשמת המטרה שפגיעתו בפרטיות פחותה ואם יש יחס סביר בין התועלת שבהגשמת המטרה לבין עוצמת הפגיעה הכרוכה בהעברת המידע. כמו כן תבחן הוועדה את האפשרות להשמטת פרטים, לעריכת שינויים או להתניית תנאים בנוגע לאופנים של קבלת המידע, השימוש בו או מחיקתו.[55] אולם, אין בתקנות אלו כל התייחסות לסוגיית ההתממה – ולפיכך אנו עדים לריק ההסדרתי המשמעותי שנוצר לעניין ההתממה, לפחות ככל שהדבר נוגע לחוק הגנת הפרטיות ולתפיסת השימוש בו על ידי משרד המשפטים. קיומו של ריק זה עולה בקנה אחד עם חלק מהטענות שצוינו לעיל בדבר חסרונות ההסדרה הריכוזית, שייתכן כי אנו רואים סטייה ממנה בהקשר פרטני זה.

2. חקיקה ספציפית המסדירה הגנה על הפרטיות במידע

בצד חוק הגנת הפרטיות, שהוא מנגנון חקיקה מרכזי, הסוגיה של מידע והגנת הפרטיות מוסדרת גם בשורה של חוקים ספציפיים הנוגעים אף הם ישירות לאפשרות להעביר מידע מרשות ציבורית לגוף אחר ובתנאים להעברה כזו, ובכך ליכולות ולתמריצים לבצע התממה.

כך, למשל, חוק זכויות החולה, התשנ"ו–1996,[56] שנחקק לצורך הגנה על זכויות חולים ומטופלים.[57] חוק זה מתייחס בין היתר לנושא הרשומה הרפואית והמידע הרפואי, וקובע כי מטפלים ועובדי מוסד רפואי מחויבים לשמור בסוד כל מידע הנוגע למטופל שהגיע אליהם תוך כדי מילוי תפקידם או במהלך עבודתם.[58] עם זאת, מטפל או מוסד רפואי רשאים למסור מידע רפואי בכמה מצבים ותנאים, למשל כשמסירת המידע הרפואי על אודות מטופל חיונית להגנה על בריאות הזולת או הציבור, ועדת האתיקה אישרה את מסירתו לאחר

53 העברת מידע בין גופים ציבוריים, לעיל ה"ש 51, בס' 8.

54 תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) (תיקון), התשע"ז–2017. תקנות אלו מיועדות להחליף את תקנות הגנת הפרטיות, לעיל ה"ש 52.

55 ראו דיון בעניין זה בבג"ץ 8070/98 **האגודה לזכויות האזרח בישראל נ' משרד הפנים**, פ"ד נח(4) 842 (2004).

56 חוק זכויות החולה, התשנ"ו–1996, ס"ח 327.

57 הצעת חוק זכויות החולה, התשנ"ב–1992, ה"ח 2132.

58 ס' 19 לחוק זכויות החולה.

וניתנה הזדמנות למטופל להשמיע את דבריו.[59] מצב נוסף שבו תאושר מסירת מידע הוא מסירתו לצורך פרסומו בביטאון מדעי, למטרות מחקר או הוראה בהתאם להוראות שקבע שר הבריאות, ובלבד שלא נחשפו פרטים מזהים של המטופל.[60] החוק אף מציין כי מסירת המידע לא תיעשה אלא במידה הנדרשת לצורך העניין, ותוך "הימנעות מרבית" מחשיפת זהותו של המטופל.[61] כלומר, אפשר לראות שחוק זה מתייחס במפורש להסדר הנוגע להעברת המידע האישי באמצעות ביצוע התממה טרם העברתו, ואף קובע מנגנונים לביצועה (כגון מנגנון ועדת האתיקה, שהוא החלופה למנגנון הוועדות המשרדיות שתואר לעיל).

חקיקה נוספת מתייחסת למידע גנטי; נושא זה מוסדר בתקנות בריאות העם וכן בחוק מידע גנטי.[62] חוק זה מתייחס לסוגיה של מסירת מידע גנטי למטרות מחקר, וגם כאן הוא קובע שהמחזיק מידע או מאגר גנטי רשאי למסור את המידע למטרות של מחקר, הוראה או פרסום בביטאון מדעי – כל עוד המידע מועבר ללא זיהוי והנבדק נתן את הסכמתו הכתובה למסירת המידע. במילים אחרות, אפשר לזהות כאן מנגנון נוסף להסדרת התממה, המחייב גם הסכמה למסירת המידע המותמם.[63]

חקיקה ספציפית נוספת שעוסקת בהעברת מידע מגוף ציבורי, הפעם בהקשרים רחבים יותר, היא פקודת הסטטיסטיקה.[64] פקודה זו מגדירה את התפקידים של הלשכה המרכזית לסטטיסטיקה ושל הסטטיסטיקן הלאומי, הכוללים עריכת פעולות סטטיסטיות ופרסום של תוצאותיהן בנוגע לאוכלוסייה בתחומים חברה, בריאות, כלכלה, מסחר ותעשייה ועוד.[65] העוצמה הרבה שבפעילות הלמ"ס באה לידי ביטוי בסעיף 15, הקובע כי בהינתן אישור לאיסוף סטטיסטיקה הנוגעת לעניין פלוני, כל אדם שלדעת הסטטיסטיקן יוכל לספק מידע הנוגע לאותו העניין יהיה חייב לתת לעובדי הלמ"ס גישה למידע זה.[66] עם זאת, סעיף 17(ב) קובע כי ידיעות שנאספו לעניין פקודה זו לא יפורסמו באופן שיאפשר לזהות למי הן נוגעות – במילים אחרות, המידע לא יפורסם ללא ביצוע התממה.[67] כאן אנו רואים את

59 ס' 20 לחוק זכויות החולה.

60 משרד הבריאות **מסקנות הועדה ליישום המלצות השימושים המשניים במידע בריאות** 42 (2018) (להלן: דוח הבריאות 2018) https://goo.gl/CWceKj. מדוח זה עולה כי השר מעולם לא הפעיל את סמכותו לקבוע תנאים להעברת מידע לצורכי מחקר לפי ס' 20(א)(7) לחוק זכויות החולה.

61 ס' 20(ב) לחוק זכויות החולה.

62 חוק מידע גנטי, התשס"א-2000, ס"ח 62; תקנות בריאות העם (ניסויים רפואיים בבני אדם), התשמ"א-1980, ק"ת 292.

63 ס' 23 לחוק מידע גנטי.

64 פקודת הסטטיסטיקה [נוסח חדש], התשל"ב-1972. חשוב לציין כי בהתחשב בס' 10 (שמירת הדינים) לחוק־יסוד: כבוד האדם וחירותו, הפקודה אינה נתונה לביקורת שיפוטית; כלומר: חוק היסוד לא פוגע בתוקפו של דין שהיה קיים ערב תחילתו. עם זאת, מקובל לסבור שככל חוק אחר, פרשנותה צריכה להיעשות ברוח חוק היסוד.

65 ס' 2-3 לפקודת הסטטיסטיקה.

66 ס' 15 לפקודת הסטטיסטיקה.

67 ס' 17 לפקודת הסטטיסטיקה.

ההתממה כחלק אינטגרלי ממערך חקיקתי קיים. לפיכך, אין זה מפתיע שהלמ"ס מתמודדת עם סוגיית ההתממה הלכה למעשה זה זמן רב.

מערכת חקיקה נוספת שכבר יש בה התייחסות להתממה ככלי להגנת הפרטיות (שוב, בלי לקרוא לדברים בשם זה) נוגעת לשקיפות של גופים ציבוריים. סעיף 9(א)(3) לחוק חופש המידע, התשנ"ח-1998[68] קובע כי רשות ציבורית לא תמסור מידע שגילויו מהווה פגיעה בפרטיות.[69] דרך אחת להבטיח זאת היא התממה של המידע שנמסר למבקש.

ההתייחסות האחרונה שנציין להעברת מידע פרטי מרשות ציבורית מופיעה בחוק מרשם האוכלוסין, התשכ"ה-1965.[70] חוק זה קובע כי מנהל מִינהל האוכלוסין שבמשרד הפנים או מי מטעמו רשאים למסור לגופים המוזכרים בחוק פרטי רישום הדרושים לגופים הללו לצורך מילוי חובתם או תפקידם. זאת, תוך הטלת חובה על הגוף מקבל המידע שלא להשתמש בפרטי הרישום אלא למטרה שלשמה נמסרו.[71] מנגנון פרטני זה קובע הליך מסודר ומאוזן (לכאורה) של העברת מידע אישי לגופים חיצוניים. אולם, במקרה דנן מנגנון זה אינו מסתמך על עקרונות ההתממה שכן הם אינם מתאימים כאן. זאת, בשל הצורך לקבל את הנתונים הגולמיים ממש כדי להגשים את המטרות הנדונות כאן. לפיכך, דוגמה אחרונה זו מדגימה היטב את מגבלות ההתממה ואת אי־התאמתה בהקשרים מסוימים. עתה, לאחר הדגמת ההקשרים הרבים שבהם יש תמריצים ניכרים לשימוש בהתממה, נעבור להסבר ולניתוח של מונח חדשני זה.

ד. התממה: מפת דרכים

1. עיבוד מידע והתממה: מתחים מובנים

האינטרס שבבסיס ההתממה הוא הרצון להגן על הפרטיות של מושאי המידע. אינטרס זה מתעצם במצב שבו המידע נאסף על ידי המדינה וגופיה, במקרים רבים ללא הסכמה של מושאי המידע אלא כחלק מפעילות השלטון ומכוח הסמכה בחוק, משום שגופים אלו מחזיקים את המידע כנאמני האזרחים ועליהם לפעול לטובתם. ביצוע התממה מאפשר שימושים מסוימים במידע בלי לפגוע באינטרסים שבבסיס ההגנה על דיני הפרטיות (או לפחות תוך מזעור הפגיעה האמורה). יתרה מזו, ברמה הדוקטרינרית, תהליך ההתממה עשוי לאפשר יציאה מתחולת המנגנונים של הגנת הפרטיות ובראשם דרישת ההסכמה מדעת ועיקרון צמידות המטרה, שלפיו מותר להשתמש במידע שנמסר למטרה מסוימת רק לאותה מטרה.[72]

---

68 חוק חופש המידע, התשנ"ח-1998, ס"ח 226.

69 לדיון באיזון בין חופש המידע לבין הזכות לפרטיות ראו עע"ם 1386/07 **עיריית חדרה נ' שנרום בע"מ** (פורסם בנבו, 16.7.2012).

70 ס' 29א לחוק מרשם האוכלוסין, התשכ"ה-1965, ס"ח 270.

71 ס' 29א(א) לחוק מרשם האוכלוסין.

72 העיקרון של צמידות המטרה בא לידי ביטוי בס' 2(9) לחוק הגנת הפרטיות, המגדיר שימוש בידיעה שלא למטרה שלשמה נמסרה כפגיעה בפרטיות, וכן בס' 8(ב), האוסר על בעלי מאגר מידע להשתמש במידע שלא למטרה שלשמה הוקם המאגר; ראו גם בירנהק **מרחב פרטי**, לעיל ה"ש 38, בעמ' 106. חשוב להזכיר את העמדה שלפיה היעדר כפיפות לחוק הגנת הפרטיות תתקיים רק אם המידע נאסף מלכתחילה כך שהוא לא מזוהה. במקרים שבהם נאסף מידע מזהה

למעשה, ההתממה היא פתרון מסוים שמטרתו לתת מענה לבעיות הפרטיות במידע ובה בעת לשמר את התועלות שבעיבוד המידע. כאשר יגיע המידע לחברות פרטיות, אפשר יהיה להשיא את רווחי הפירמה שמנתחת את המידע וליצור עושר שבמקרים רבים עשוי להגיע לידיהם של רבים אחרים – משתמשי המוצר ובעלי המניות בחברה. מעבר לכך (וכטענה משכנעת יותר), עיבוד המידע עשוי לקדם את המחקר, לשפר את איכות החיים, להוביל לחדשנות ולקדמה אנושית וכן לעודד יעילות בהתנהלות הגופים.[73] עם זאת, הגנת הפרטיות ככלל והתממה של המידע בפרט פוגעות לעתים ביכולת לנתח את המידע בצורה מדויקת ואמינה ולקבל על בסיס זה החלטות מושכלות. לכן, במצב שבו נדרש מידע באיכות גבוהה למטרה מוצדקת, ייתכן שיופעל פתרון מידתי אחר להעברת המידע בשונה מההתממה שנדונה כאן (כמו שצוין לעיל לעניין רשות האוכלוסין).[74]

עיבוד מידע מותמם מעורר מתח נוסף – בין פרטיותם של יחידים ושל קבוצות. עיבוד המידע המותמם שואף למנוע מצב שבו מתבצעים היסקים על יחידים שמידע הנוגע להם נמצא במאגר, אך ההתממה עדיין מאפשרת להסיק מסקנות נרחבות לגבי קבוצות של בני אדם (ואפילו תת־קבוצות מצומצמות למדי). לכאורה, היסקים אלו אינם אישיים ואינם פוגעים בפרטיות היחיד; עם זאת, כאשר תיוחסנה מסקנות אלו ליחידים באותן הקבוצות, הם עלולים להיפגע מהן. כך, למשל, היסקים הנוגעים להיבטים דמוגרפיים כלליים (למשל: מצב כלכלי, משקל או מצב בריאותי) המוחלים על אזורים גאוגרפיים מסוימים (כגון רחוב או שכונה) עלולים לפגוע ביחידים הגרים באזורים אלו אך אינם משתייכים למאפיינים שזוהו, קרי: משקלם, מצבם הכלכלי או מצבם הבריאותי שונה במובהק מהממוצע הנקודתי באזור מגוריהם. לדוגמה, יחיד המתגורר ברחוב מסוים עשוי להיפגע אם יעלה ממידע מותמם שפורסם כי שכרם של תושבי הרחוב גבוה (או נמוך) במובהק משכרו. כאשר ייוודע פרט זה לאחרים היודעים את כתובתו של אותו יחיד, הם עשויים להסיק מסקנות בדבר הכנסתו וזאת בלי שנתן את הסכמתו לפרסום המידע האמור. היסקים אלו עשויים כמובן להיות שגויים. בעיה אחרונה זו – הנוגעת לזכויות הפרטיות של יחידים החברים בקבוצה בנוגע למידע כללי על מאפייני הקבוצה – היא בעיה מורכבת המאתגרת את ההתממה. הדיון בה נמצא בראשיתו והיא אינה נדונה במאמר זה.[75]

שהותמם לאחר מכן, יש לבקש את ההסכמה של מושא המידע לעצם ההתממה ולשימושים במידע המותמם, שכן ראוי שתוענק ליחיד שליטה בהליך זה. לעניין זה ראו Michael Birnhack, *A Process-based Approach to Informational Privacy and the Case of Big Medical Data*, 20 Theor. Inq. L. 257 (2019).

73 ראו רשימת שימושים בנספח ל־Polonetsky et al., *Shades of Gray*, לעיל ה"ש 9; ראו גם עניין **האגודה לזכויות האזרח**, לעיל ה"ש 55, בפס' 6 לפסק דינה של השופטת דורנר, הקובע כי "תכלית ההעברה – מתן שירות יעיל ומהיר לציבור – היא תכלית ראויה".

74 חוק מרשם האוכלוסין.

75 Micah Altman et al., *Towards a Modern Approach to Privacy-Aware Government Data Releases*, 30 Berkeley Tech. L.J. 1899, 2034, 2038 (2015).

2. רבדים בביצוע התממה

עד ראשית שנות האלפיים, מידע שעבר הליכי התממה מוגדרים ומוסדרים נחשב מוגן יחסית;[76] ההנחה הייתה שאי־אפשר לחשוף את מושאי המידע שבמאגר המותמם ובכך לפגוע בפרטיותם. לפיכך, סוגיית ההתממה נתפסה כסוגיה טכנית בעיקרה והדיון האקדמי בהיבטים משפטיים והסדרתיים היה מצומצם מאוד. לעומת זאת, בעשרים השנים האחרונות החלו לצוץ עדויות לגבי היכולת לבצע תקיפות התממה שיובילו לזיהוי חוזר של מושאי מידע מותמם.[77] מחקרים חשפו חולשות מובנות בהליך ההתממה, שהובילו לחשיפה ולזיהוי של מידע שלכאורה הותמם, וכל אלו הובילו לפקפוק ביכולת של ההתממה להשיג את מטרתה.[78]

בעקבות ממצאים אלו היו שקראו לנטוש לחלוטין את השימוש בהתממה כאמצעי להימנעות מתחולתם של דיני הפרטיות ומחשיפת מידע אישי, לפחות ככל שהדבר נוגע להעברת מידע ממאגרים הכוללים מידע אישי רגיש ורב.[79] מצד שני, היו שקראו להימנע מהפרזה בחשיבות הממצאים האמורים, החותרים תחת עקרון התממה, והוצאתם מהקשרם הנקודתי שהתייחס בעיקר לתהליכי התממה שבוצעו באופן שגוי או לא מקצועי.[80] בין שתי קריאות אלה החלה להתפתח דרך ביניים, המציגה את האפשרות לעצב את תהליך ההתממה הנכון ככזה המורכב מכמה רבדים שיפורטו להלן. לאור הדיון האמור, ניכר כי סוגיית ההתממה איננה צריכה להיות נחלת הסטטיסטיקאים ואנשי המחשוב בלבד (לפחות ככל שהדבר נוגע לצד הטכני של מלאכתם), והיא מחייבת התייחסות גם בהיבטים הנורמטיביים מצד אנשי המשפט

---

76 לדוגמה בהתאם לנהלי HIPPAA, The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

77 Rubinstein & Hartzog, לעיל ה"ש 3.

78 בשורה של מאמרים ידועים הצליחו חוקרים לאתר את מושאי המידע האישי שפורסם לאחר אנונימיזציה על ידי מדינת מסצ'וסטס, AOL ו־Netflix. ראו Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J.L. MED. & ETHICS 98 (1997); ראו גם Altman et al., לעיל ה"ש 75, בעמ' 2038; לעניין AOL ראו Michael Barbaro & Tom Zeller Jr., A Face Is Exposed for AOL Searcher No. 4417749, N.Y. TIMES (Aug. 9, 2006), https://goo.gl/RKvo8M; Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 705. לעניין Netflix ראו Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1717-18 (2010); Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, Proceedings of the 2008 IEEE Symposium ON Security and Privacy 111 (2008); כמו כן יש תקיפות חדשות יותר, המאפשרות זיהוי יחיד מאיסוף נתונים בדבר ניצולת של סוללה סלולרית. ראו, למשל, Andrew Griffin, Phone Batteries Can Be Used to Spy on Users, The Independent (Aug. 3, 2016), https://goo.gl/4RJoMq; ראו גם Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 Sci. 536, 537 (2015), המתייחס לקושי הרב בהתממה של נתוני תקשורת ואשראי.

79 Ohm, שם, בעמ' 1704.

80 Polonetsky et al., *Shades of Gray*, לעיל ה"ש 9, בעמ' 601-602; Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 723.

והמדיניות.[81] אכן, אנשי המשפט של המאה העשרים ואחת, בעיקר אלו העוסקים בענייני פרטיות והגנת מידע, נדרשים להתעמק הן בהיבטים הטכנולוגיים והן בהיבטים הפרקטיים הנוגעים לסוגיה זו.[82] להלן נתייחס לעניינים אלו, הן בהקשר של טכניקות להתממת מידע (לתפיסתנו – התממה במובנה הצר) והן בהקשר של מכלול התהליכים והנהלים הנוגעים לטיפול במידע (התממה במובן הרחב).[83]

(א) *שיטות להתממת מידע: סוגיות בסיסיות*

הליך ההתממה הוא הליך מורכב הטומן בחובו היבטים מכמה תחומי ידע. הרובד הפשוט, והבסיסי ביותר לביצוע התממה, הוא הסרת פריטים מזהים במאגר המידע האישי או החלפתם במשתנים אחרים (הרובד הסטטיסטי).[84] הכוונה לפריטים המאפשרים זיהוי חד־חד־ערכי של היחיד כגון שם,[85] כתובת, מספר תעודת זהות ועוד.[86] במקרים מסוימים יישמר "מפתח" שמאפשר חיבור לאחר מעשה (לעתים עקיף) של השדות למושאי המידע המקוריים ובכך למעשה מאפשר ביצוע זיהוי מחדש.[87] ברור כי לא די בצעדים אלו. כיום, בעידן נתוני העתק, מתברר שגם שדה נתונים הכולל פרטים רבים (ובעיקר בעל שדות רבים) ניתן לזיהוי במקרים רבים על אף הסרתם של פריטים מזהים.[88] יש כמה אמצעים סטטיסטיים מקובלים להתגבר על חשש זה ולהקשות על זיהוי כאמור, ובהם איחוד נתונים על יחידים לקבוצות, החלפת

---

81 ניבה אלקין־קורן ומיכאל בירנהק "הקדמה: משפט וטכנולוגיות מידע" **משפט, חברה ותרבות – רשת משפטית: משפט וטכנולוגית מידע** 11, 12 (2011). המחברים מתייחסים לפרדיגמה של משפט וטכנולוגיה כמסגרת מחקר אנליטית הבוחנת, בין היתר, את הטכנולוגיה כשינוי דינמי הנמצא בקשר עם המשפט ועם גורמים נוספים.

82 GDPR, לעיל ה"ש 11, בס' 25.

83 ראו, למשל, אצל אריאל־הרשקוביץ ושוורץ־אלטשולר, לעיל ה"ש 3, בעמ' 38, סקירה של טכניקות התממה.

84 Simson L. Garfinkel, De-identification of Personal Information, NISTIR 8053, National Institute of Standards and Technology (NIST), 15 (2015), https://goo.gl/VVVFRC.

85 גם בתוך קבוצה זו יש מורכבות. לדוגמה, יש שמות נפוצים ("משה כהן", "רחל לוי") שחשיפתם כמעט לא מאפשרת זיהוי. אולם, יש שמות אחרים ("טל ז'רסקי") שמאפשרים זיהוי בנקל. נוסף על כך יש משתנים המאפשרים זיהוי אך במקרה של חשיפה ניתנים לשינוי בקלות כגון מספר כרטיס אשראי או כתובת דוא"ל – ויש משתנים שאינם ניתנים לשינוי כמו מספר תעודת זהות. ראו גם Polonetsky et al., *Shades of Gray*, לעיל ה"ש 9, בעמ' 608.

86 נשאלת השאלה אם כתובות IP של יחיד נמנות בקבוצה זו; לעניין זה יש מחלוקת בדין האירופי, ראו Lee A. Bygrave, Data Privacy Law: An International Perspective, 137-38 (2014). נראה כי תחת ה־GDPR הגישה המחמירה היא המחייבת, אך נדרש זמן לראות כיצד יכריעו הרגולטוריים בעניין, במיוחד לעניין כתובות IP דינמיות. ראו GDPR, לעיל ה"ש 11, Recital 30, שלפיו אפשר לכאורה לזהות בני אדם על פי כתובות ה־IP שבהן הם משתמשים.

87 שאלה משפטית מעניינית, ופתוחה לעת עתה, היא אם מידע עשוי להיחשב מותמם אם יש מפתח כאמור בידי ישות מסוימת. ראו GDPR, לעיל ה"ש 11, Recital 26; וכן Polonetsky et al., *Shades of Gray*, לעיל ה"ש 9, בעמ' 614.

88 Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 710–711. ראו גם סקירת התקיפות, לעיל ה"ש 78.

מידע בין שדות והזזתו ואף הוספת "רעש" לנתונים.[89] זוהי ההתממה במובן הצר, העוסקת בהיבט הטכני של הסרה או החלפה של פריטים מזהים תוך שימוש באמצעים סטטיסטיים.

למרות חשיבותו של הרובד הסטטיסטי הוא לבדו אינו יכול לתת מענה לכל סוגי התקיפות והסיכונים הניצבים כיום לפני מאגר מידע אישי מותמם (או מותמם לכאורה); ההתקפות המוצלחות נגד מאגרים מותממים שבוצעו לאחרונה מוכיחים זאת. לפיכך, יש להתממה ממדים נוספים המתייחסים לאופן ההנגשה של המידע, הממומשים בכמה מודלים. מודלים אלו מגשימים ומדגימים את ההתממה במובנה הרחב וכוללים התייחסות להיבטים הטכנולוגיים, המנהליים והמשפטיים בפעולת הגוף ששולט במידע האישי.[90] המודל הראשון הוא מודל כללי שעל פיו שחרור מידע מותמם לציבור הרחב מתבצע כמעט ללא הגבלות – פעולה שאפשר לכנות "שגר ושכח" (release and forget). מודל זה כמעט אינו כולל רכיבים מעבר למודל הצר. הוא עשוי לכלול הגבלות שימוש שונות שיוטלו על מי שבוחר לקבל את המידע ולהשתמש בו, אך בפועל הגבלות כאלה כמעט אינן אכיפות. כפי שנראה, מודל זה מתאים בעיקר לפרסום של מידע סטטיסטי כוללני, ובעידן נתוני העתק הוא נהפך למוגבל ובעייתי מאוד. המודל השני דומה לקודמו, אך באמצעותו המידע המותמם מועבר לגוף פרטני. מודל זה מאפשר להטיל הגבלות משפטיות בנות־אכיפה על אותו גוף מכוח חוזה או רישיון שנכרת עמו. המודל השלישי הוא מודל הכולל – בצד המגבלות המשפטיות – הגבלת גישה למידע האישי באתר פיזי מוגדר בלבד, המאפשר בקרה מתמשכת על האופן של משיכת הנתונים (מודל "חדר המידע"). המודל הרביעי, הדומה למודל "חדר המידע", מאפשר גישה וירטואלית באמצעות שאילתות באמצעות חיבור מאובטח ומפוקח,[91] ובכך מבצע פיקוח על השימוש במידע בדרך בטוחה מעט פחות אך נוחה יותר לחוקר (מודל מחקר וירטואלי).

נוסף על ארבעת המודלים הכלליים האלו יש מודלים מורכבים אף יותר (וריאציות על המודלים שצוינו), הנמצאים בשלבים שונים של פיתוח ויישום ראשוני ומשתמשים בטכנולוגיות מתקדמות יותר. במסגרת מודלים אלו המידע מועבר אחרי הצפנתו לצד שלישי או אפילו לגוף המבקש לעבד את המידע בדרך מסוימת. פיתוחים טכנולוגיים מאפשרים להגיש למאגר המידע המוצפן שאילתות מסוימות, שגם לאחר שיינתן להן מענה הן לא יחשפו את הפרטים האישיים שבמאגר.[92] בשל ראשוניותם של מודלים אלו לא נרחיב את הדיון בהם כעת.

---

89 **NISTIR Report**, לעיל ה"ש 84, בעמ' 16; **דוח הבריאות 2018**, לעיל ה"ש 60, בעמ' 113, שם מצוינים האמצעים המרכזיים כ"השמטה, הכללה, קידוד, ערבול, גיבוב, התמרה והרעשה".

90 ראו אצל Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 737. במידה רבה אנו מסתמכים על הממדים המוצעים במאמר זה. יש חלוקות דומות לממדים. לדוגמה, יש חלוקה לממדים שונים מעט במאמרם של Altman et al., לעיל ה"ש 75, בעמ' 2016–2017. אלה כוללים ממד פרוצדורלי, ממד טכני, ממד חינוכי, ממד כלכלי וממד משפטי. ראו גם The De-identification Decision-Making Framework, ix (2017), https://goo.gl/63LtcB (להלן: הדוח האוסטרלי).

91 להסבר טכני בנוגע להפעלת מערכות אלו ברשויות סטטיסטיות בארצות־הברית (דבר הדומה לישראל), ראו Altman et al., לעיל ה"ש 75, בעמ' 2026.

92 הליך של עיבוד המידע אצל צד שלישי, שלא יחשוף בדרך זו את המידע של שני צדדים המעבירים לו את המידע, מכונה "Secure multiparty computation". הליך עיבוד המידע אצל

השימוש בחדר מידע או במחקר וירטואלי מאפשרים אכיפה ופיקוח על ההתממה תוך שילוב אמצעים טכנולוגיים. הטכנולוגיה יכולה להציע כלים שיסייעו לסכל את תקיפת ההתממה על ידי חסימה של משתמש או של שימוש פרטני המעוררים חשד. היא אף תורמת להרתעת התוקפים המבקשים לעקוף את ההתממה באמצעות מערכת שתאפשר את איתורם לאחר מעשה – אמצעי מעקב (המכונים audit logs) אחר מספר השאילתות שכל גורם שואל.[93] המעקב יכול להתבצע אחר חוקרים פנימיים וגם אחר אלה שבוחנים את המאגר מבחוץ. מובן שהפעלה של מערכת מעין זו אינה מתאפשרת כששדה הנתונים מועבר בשלמותו לציבור כולו ("שגר ושכח"). לכן, שחרור מידע בדרך זו יהא במקרים רבים מעשה לא אחראי. לראיה, כמעט כל המקרים שבהם בוצעו תקיפות מוצלחות על מנגנוני התממה נבעו משחרור מידע בתצורה רחבה זו. אכן, נראה כי שיטת שחרור מורחבת זו עוברת מן העולם במידה רבה.[94] הרבדים הטכנולוגיים האמורים חסרים גם במודל השני שצוין להנגשת מידע, שעל פיו המידע מועבר לגורם פרטני. כדי להתמודד עם הסיכונים המתעוררים בהפעלת מודל זה (ולחזק את ההגנה במודלים אחרים) אנו נדרשים לרובדי הגנה משפטיים ומנהליים שהם רכיבים קריטיים בהגדרת ההתממה במובנה הרחב.

כאמור, יש גם צעדים מנהליים ומשפטיים שאפשר לנקוט לשם הקטנה של סיכוני ההתממה. לדוגמה, כשהמידע נמסר לגורם מסוים, ראוי לעגן את האיסור על זיהוי מחדש בחוזה מחייב בין מוסר המידע למקבל המידע (שלעתים מכונה רישיון לשימוש בו). חוזים אלו יגדירו את היקף העיבוד שייעשה במידע, יגבילו התקפות על ההתממה וידאגו להטמעת האמצעים הטכנולוגיים שנדונו כאן אצל מקבל המידע. כמו כן, ההסכם ידרוש אי־העברה מוחלט של המידע הלאה – או רק תוך הקפדה ואכיפה אפקטיבית של הדרישות שמקבל המידע הסכים להן בחוזה דנן. החוזה צריך לכלול גם סעדים משמעותיים ואפקטיביים כגון אכיפה ופיצויים מוסכמים בהיקף ניכר במקרה של הפרת העקרונות האמורים כאן, לדוגמה כשמקבלי המידע עצמם ניסו לחשוף את המידע האישי שהותמם.[95]

ההכרה ברובד חוזי הכרחי זה מעלה סדרת שאלות הנקשרות עתה לעולם ההתממה ומצריכות דיון ופתרון. לדוגמה, לעתים רישיון השימוש במידע יהיה חוזה שנכרת אגב הקלקה על תנאי שימוש. כלל לא פשוט לטעון כי גם במקרה זה מקבל המאגר כפוף לכל האמור בתניות ההסכם (לרבות סעדים מחמירים הנדרשים לתת להסכם זה משקל ומשמעות) וכי התבצע להצעה שברישיון קיבול כנדרש. ייתכן שבמקרה זה אף יחולו דיני החוזים האחידים, שאינם מאפשרים החלה של תניות חד־צדדיות על הצד המתקשר.[96] שאלות מעין

גוף אחר מכונה "הצפנה הומומרפית". להסבר ודיון על כלים אלו ראו Goroff et al., לעיל ה"ש 3.

93 להסבר על אופן היישום של מערך "Audit Logs" ראו Altman et al., לעיל ה"ש 75, בעמ' 2030.

94 ראו William W. Stead, Recommendations on De-identification of Protected Health Information under HIPAA, National Committee on Vital and Health Statistics (NCVHS) 10 (2017), https://goo.gl/3DQTqt; ראו גם Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 739. לתקיפה מפורטת על דרך פעולה זו ראו Ohm, לעיל ה"ש 77, בעמ' 1711–1712.

95 NCVHS, שם, בעמ' 12.

96 חוק החוזים האחידים, התשמ"ג–1982, ס"ח 8. ראו גם רע"א 5860/16 **Facebook Inc נ' בן חמו**, פס' 20 לפסק דינה של הנשיאה חיות (פורסם בנבו, 31.5.2018), שם נקבע כי תנאי

אלו עשויות להתעורר כבר כיום כשפרטים "מורידים" קובצי נתונים מאתרים של רשויות סטטיסטיות (כגון הלמ"ס).

נוסף על כך יש רובד של צעדים מנהליים, הכולל לפחות שלושה היבטים נוספים. לפי ההיבט הראשון, פעולת ההתממה צריכה לכלול גם הכנת תכניות לפעולות שיש לנקוט לאחר מעשה, במקרה של חשיפת מידע (כגון הדרך שבה יעודכנו הנפגעים מחשיפת המידע ואיזה סיוע יוצע להם);[97] לפי ההיבט השני, התממה צריכה לכלול תסקיר סיכונים שייערך טרם תחילת הפעולה ויבחן את כל היסודות שצוינו, כמו גם את ההקשר הרחב יותר של המידע, ויבדוק מה דרכי ההתממה הטובות ביותר.[98] לפי ההיבט השלישי, פעולת ההתממה יוצרת חובה מתמשכת להמשיך ולעקוב אחר סביבת המידע כדי להעריך אילו טכנולוגיות אִחזור מתווספות ואילו מאגרים נוספים קיימים אצל צדדים שלישיים, ובהתאם לכך לשנות את המדיניות ולנקוט צעדי מנע נוכח השינויים האפשריים במתווה הסיכונים.

(ב) *ביצוע וניהול של התממה: סוגיות מתקדמות*

לאחר שהכרנו את ההתממה במובנה הרחב על שלל רבדיה, נוכל לעבור לשאלות מתקדמות יותר שהליך זה מעורר (וכפי שנראה, זוכות למענה שונה אצל רשויות שונות), והן: מהי רמת הסיכון המותרת שהליך זה יכול לכלול? האם סיכונים שונים גוררים הכרה במספר סוגי מידע, מעבר לחלוקה בין מידע "אישי" למידע "שאינו אישי"? כיצד ראוי להסדיר דרכי התממה ומי הגופים שמסדירים את נושא ההתממה? אתגר התממת המידע האישי בכלל, והעברת המידע מגופים ציבוריים בפרט, משותף למדינות רבות. בכדי לתת מענה מתאים ומקיף לשאלות האמורות, נבחן את הדרך בה התמודדו מדינות שונות עם שאלות אלו, ובהמשך נלמד כיצד ניתן ליישם מהתובנות שעלו שם לעניין הסדרת הנושא בישראל, לרבות אסטרטגיית הסדרה.

(1) סיכוני ההתממה ומידת הפרטיות שהיא מעניקה

הסיכון לפריצת ההתממה נוצר בו־זמנית עם ביצוע ההתממה (על מכלול רבדיה). משמע, העברת מידע ציבורי מותמם יוצרת סיכון לפגיעה בפרטיות של מושאי המידע. לפיכך, יש צורך בהחלטת מדיניות באשר למידת הסיכון המותר, אם בכלל, שיהיה כרוך בהליך.[99] מבחינה פוזיטיבית, חוק הגנת הפרטיות בישראל אינו נותן את הדעת לסוגיית הסיכונים המותרים ונראה כי הוא ממוקד תוצאה; קרי: אם בסופו של דבר, אף לאחר ביצוע התממה

השימוש של פייסבוק הם חוזה אחיד ותניות ההסכם ניתנות לעתים לביטול אם נמצא כי הן מקפחות.

97 Omer Tene & Gabriela Zanfir-Fortuna, *Chasing the Golden Goose: What is the Path for Effective Anonymization,* PING (2017), https://goo.gl/YdhafM; NCVHS, לעיל ה"ש 94, בעמ' 10.

98 NCVHS, שם, בעמ' 12. ראו גם הדוח האוסטרלי, לעיל ה"ש 90, בעמ' xiii-xiv.

99 אפשר להמשיך ולהקשות בהמשך לשאלה אם די בהוכחה שאפשר לחשוף אדם אחד כדי לגזור גזירה שווה בדבר הסיכון החל על המאגר כולו – ואם לא, מה אחוז הנחשפים המאפשר זאת? נותיר שאלות אלו לפעם אחרת. לתחילת הדיון בסוגיה ראו Polonetsky et al., *Shades of Gray*, לעיל ה"ש 9 בעמ' 619.

מקיפה, תיפגע פרטיותו של אדם עקב אחזור המידע – יוביל הדבר לגיבוש עוולה. אל מול עמדה נוקשה זו אפשר להציג עמדה פוזיטיבית מרוככת יותר, שלפיה פגיעה בפרטיות עקב אחזור מידע לא תַקנה לנפגע סעד אם היא נבעה מהתממשות של סיכון קטן בהליך התממה שבוצע בהתאם לנהלים מקובלים. עמדה זו תישען על ההגנות שפורטו לעיל בחוק הגנת הפרטיות (הגנת "מעשה של מה בכך", אם הפגיעה תהיה מינימלית, ובעיקר הגנת תום הלב שבסעיף 18(2)(א) לחוק), כמו גם בדין הכללי (מידתיות הפגיעה בזכות הפרטיות החוקית, אם הסיכוי לפגיעה קטן) שיעמדו לכאורה לגורם שהפעיל התממה סבירה כהגנה מפני תביעה.[100] עמדה זו אף יכולה להישען על העובדה שתקנות הפרטיות לעניין אבטחת מידע מאמצות מתווה של הכרה בהגנת הפרטיות כפונקציה של ניהול סיכונים ולאו דווקא של מניעת תוצאות.[101] לפיכך, אפשר להקיש מהן את עמדת המשפט גם בסוגיה משיקה זו.[102]

בשל חוסר הבהירות האמור והמרווח הפרשני שהמשפט הישראלי מותיר, יש מקום להכרעה בעניין זה ככל שהדבר נוגע לדין הרצוי בישראל. לצורך כך ניעזר במשפט המשווה. בבריטניה, ה־Information Commissioner's Office (ICO, הגוף האמון, בין היתר, על אסדרת הפרטיות) מצא כי יש להתייחס לסוגיית ההתממה כתהליך שעוסק במזעור סיכונים.[103] בהתאם לכך הוא מצא כי יש לגלות יחס סלחני במצבים שבהם מוכח כי האנונימיות אינה מובטחת באופן מוחלט אך המידע ניתן לאחזור אך ורק במצבים נדירים.[104] גם אוסטרליה פרסמה מסמך קווים מנחים (שהסתמך על משוב שנתנו הרשות הסטטיסטית והרשות להסדרת המידע הרפואי שם), המכיר בכך שהתממה היא מהלך של ניהול סיכונים ולא מהלך היכול ליצור מציאות מוחלטת של יצירת מידע אנונימי.[105] אין תמימות דעים בסוגיה זו. קבוצת המומחים המקצועית של האיחוד האירופי לעניין הגנת מידע אישי סברה כי התממה צריכה להוביל למצב שבו הגילוי כבר איננו אפשרי; כלומר קבעה יעד המבוסס על תוצאה ולא

100 ראו דיון בהגנות לפי חוק הגנת הפרטיות. ראו גם ה"ש 49 (הנוגעת לפרשנות של בירנהק את תחולת ההגנות, תוך ציון העובדה שהן אינן חלות על עברות ועוולות לפי פרק ב). מעניין לציין כי חוק זכויות החולה, שלכאורה מגן מפני פגיעות במידע רפואי הנחשב רגיש מאוד, מסביר כי מסירת מידע תיעשה "תוך הימנעות מרבית" מחשיפת זהות המטפל – משמע משתמש בלשון של השתדלות ולא של תוצאה. עם זאת, סעיף זה נוסף על החובות המפורטות בסעיף 20(א)(6), המדבר על התממה בלשון של תוצאה ("לא נחשפו פרטים").

101 ראו תקנות הגנת הפרטיות: תקנה 2(א)(6) (הדורשת מבעל מאגר להגדיר במסמך את הסיכונים העיקריים לפגיעה באבטחת המידע ואת דרך ההתמודדות עמם), תקנה 5(ג) (המחייבת בעלי מאגרים מסוימים לבצע סקר סיכונים עתי), תקנה 12 (הדורשת מבעל מאגר להגביל חיבור של התקנים ניידים מתוך התחשבות בסיווגים המיוחדים של המאגר), תקנה 15(א)(1) (הדורשת מבעל מאגר לבחון את סיכוני האבטחה הכרוכים בעסקה בטרם יבצע התקשרות לעניין מיקור־חוץ) ועוד.

102 על ההיגיון שבביצוע היקש בין דיני אבטחת מידע לסוגיית ההתממה, לרבות לעניין הכרה בקיומו של סיכון, ראו Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 731.

103 ICO, Big data, Artificial Intelligence, Machine Learning and Data Protection, para. 134 (2017); ראו גם Tene & Zanfir-Fortuna, לעיל ה"ש 97, בעמ' 2.

104 ICO, שם, בפס' 134.

105 ראו גם הדוח האוסטרלי, לעיל ה"ש 90, בעמ' ix.

בהכרח על סיכון.[106] החלטה זו נסמכה על הלשון של דירקטיבת הגנת הפרטיות שתוקפה פג כעת,[107] אף על פי שהדירקטיבה מציינת במפורש (בסעיף 26 להקדמה) שיש לבחון אם נעשה שימוש באמצעים סבירים (likely reasonably to be used) – ומכך עולה נכונות לקבל סיכונים מסוימים בהליך ההתממה. לפיכך, המסקנה הפרשנית הנדונה של קבוצת המומחים היא קשה ונראה כי היא נשענת על היקש מהאמור בסוף סעיף 26 הנדון (המתייחס ל־codes of conduct בעניין זה ואכן קובע סטנדרט גבוה יותר).[108] נוסף על כך, מדינות מסוימות באיחוד האירופי (דוגמת צרפת) מחמירות אף יותר בקובען כי כל סיכוי לביצוע זיהוי לאחר מעשה מצריך סיווג של המאגר כולו ככולל מידע אישי.[109]

ראוי לציין כי ייתכן שהדין האירופי הנוכחי, המעוגן ברגולציית ההגנה על מידע (General Data Protection Regulation, GDPR) המחייבת את האיחוד האירופי מאז מאי 2018, שונה מחוות דעת המומחים האמורה, והוא מאמץ סטנדרט גמיש לבחינה של התממה ראויה, המבוסס על סיכון. לשון הסעיף בהקדמה לרגולציה זהה במידה רבה לזו של הדירקטיבה, בהגדירה את ההתממה כמצריכה שימוש ב"אמצעים סבירים" – אך ללא הסיפא שהובילה להיקש המחמיר של ועדת המומחים. לפיכך, נראה כי דיני האיחוד יהיו נכונים לקבל סיכון מסוים (אם כי נמוך) לזיהוי גם אחרי ההתממה, אם זו כללה שימוש באמצעים סבירים.[110]

חזרה למצב הרצוי בישראל: מאמר זה בוחן אסטרטגיית הסדרה. הדיון והשימוש בסוגיית הסיכון הוא מכשירני בעיקרו ומשמש כלי להערכה שתתבצע בהמשך בדבר היכולות של רשויות להתמודד עם הסוגיה המורכבת דנן. אך פטור בלא כלום אי־אפשר. נציין כי לדעתנו ראוי שהמשפט הישראלי יאמץ את גישת הסיכון נוכח המגמה המסתמנת בעולם, נוכח הגמישות המתאפשרת בחוק ובעיקר נוכח אופיו של העידן הטכנולוגי המשתנה כל העת ומחדיר סיכונים גם לתבניות שנראו בטוחות לחלוטין אך אתמול. כמו כן, הטלת אחריות מכוח דיני הפרטיות בגין התממשות סיכון נמוך תוביל לפגיעה אקראית ביזמים ולהרתעת־יתר מפני פיתוחים חדשניים בתחום, שיכולים להוביל לקדמה חברתית משמעותית. נראה שהדרך הנכונה להתמודד עם סיכון כאמור ועם הנזק (האקראי אך בהחלט משמעותי) שייגרם לאזרחים תהיה מנגנון ביטוחי.[111]

---

106 Article 29, Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, adopted 10 April 2014; ראו גם Tene & Zanfir-Fortuna, לעיל ה"ש 97 בעמ' 20: "Identification is no longer possible". ראו גם דיון בעניין זה אצל Rubinstein & Hartzog, לעיל ה"ש 3, עמ' 746.

107 Council Directive 95/46/EC, Recital 26, 1995 O.J. (L 281) 31, 31 (EC).

108 שם, Recital 26.

109 ראו Polonetsky et al., *Shades of Gray*, לעיל ה"ש 9, בעמ' 603. הכותבים מוסיפים ומציינים כי במצבים מעין אלו נראה שיש להחיל על המאגרים האמורים דרישות מופחתות, אף שלא ברור מהיכן הקלה זו נגזרת.

110 GDPR, לעיל ה"ש 11, Article 4(1), Recital 26.

111 כך, למשל, כדי לאפשר פיצוי לנפגעים בגין נזק צפוי אך נדיר, אפשר לחייב את מאגרי המידע הגדולים לבטח את עצמם מפני אירוע של פריצת התממה כאמור ולשלם פרמיה לחברת ביטוח שתפזר את הנזק בין המאגרים. בעת התרחשות של אירוע כאמור יפוצה הנפגע בסכום שייקבע מראש.

הכרעה בדבר שאלת ה"סיכון" ומקומו בדין היא אך שאלה מקדמית למכלול נרחב של שאלות כגון איך אפשר לאמוד את הסיכון ומי יעשה כן, מה המועד הראוי לבדיקת הסיכונים והאם נכון להחיל מערכת דינים נפרדת לסוגי מידע אישי בסיכונים שונים.

שאלה אחרונה זו נדונה בדין הזר, במסגרת האפשרות להכיר בכמה קטגוריות של מידע בהתבסס על עוצמת הפרטיות במידע מותמם ועל הסיכון בפגיעה. לדוגמה, יש הרואים את המשטר שיוצר ה־GDPR כמגדיר לא פחות מארבעה סוגי מידע – מידע אישי מזוהה, מידע הניתן לזיהוי בנקל, מידע אנונימי/אגרגטיבי ומידע המותמם בהתאם לסעיף 11 לרגולציה (המתייחס למצב שבו מחזיק המידע מוכיח כי הוא לא מסוגל לאחזר את המידע המותמם).[112] בסוגי המידע שחלה לגביהם הקטגוריה האחרונה, מחזיקים של מאגר מידע מותמם אינם מחויבים לעמוד בדרישות שהחוק מטיל כמו הענקת גישה למידע או מתן זכות למחיקתו; אולם, עקב הסיכוי המסוים לפגיעה עקב ביצוע אחזור למידע המותמם הם עדיין מחויבים בדרישות אחרות כגון אלה הנוגעות לאבטחת מידע. מלומדים בארצות־הברית הציעו רעיון דומה: ליצור תת־קבוצה חדשה, של מידע שעבר התממה ושיש סיכוי מסוים שיאוחזר ועל כן הוא כפוף רק למקצת הדרישות הרגולטוריות.[113] בהמשך נבחן אם סוגיה זו נשקלה בישראל.

השאלות האחרות עדיין ממתינות לפתרון. אומדן הסיכון, לדוגמה, מקבל בהקשרים מסוימים מענה מתמטי־פורמלי כגון תוך שימוש בשיטת ה־Deferential Privacy להגנה על מאגרי מידע. שיטה זו כבר הופעלה בכמה הקשרים מצומצמים ולרוב היא מיושמת באמצעות מערכת השולטת במענה שניתן לשאילתות ממוקדות למאגר מידע אישי.[114] השימוש בשיטה זו מאפשר למיישמיה להגדיר את הפרמטר אפסילון (ε) שייצג את הסיכוי לפגיעה בפרטיות ולחשיפת מידע אישי מהמאגר. סיכון זה הוא מוחלט ולא תלוי זמן.[115] פרמטר זה מאפשר להגדיר "תקציב פרטיות" (privacy budget) הקובע את היקף הסיכון הכולל לפגיעה בפרטיות בהנגשת מידע, שבהתאם לגובהו המוגדר ייקבעו מספר השאילתות המותרות והיבטים נוספים בהליך ההתממה.[116]

אומדן הסיכונים במודלים אחרים הוא סבוך בהרבה (ודאי שהדבר כרוך גם בהיבטים משפטיים ומנהליים); אין ספק שבעלי מקצוע יידרשו לפתח מתודולוגיה בעניין זה בשנים הקרובות. לדוגמה, הרשות הסטטיסטית בארצות־הברית מתעתדת לייעד סמכות זו לוועדה מיוחדת – Data Stewardship Executive Policy Committee (DSEP).[117] נוסף על כך

112 Mike Hintze, *Viewing the GDPR through a De-identification Lens: A Tool for Clarification and Compliance*, 8 Int. Data Protection Law (Oxford Uni. Press) 86 (2017), https://goo.gl/cKdR9m.

113 Paul Schwartz & Dan Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. Rev. 1814 (2011).

114 ליישום השיטה בפועל ראו Kobbi Nissim et al., *Differential Privacy: A Primer for a Non-technical Audience* (2018), https://goo.gl/WyRR1z; להסבר כללי על דרך הפעולה של מודל זה ראו בעמ' 6–7.

115 ראו Goroff et al., לעיל ה"ש 3, בעמ' 57.

116 Nissim, et. al, לעיל ה"ש 114, בעמ' 23–24.

117 U.S Census Bureau, The Modernization of Statistical Disclosure Limitation at the U.S. Census Bureau 9 (2018), https://goo.gl/PXYv8n.

נראה שאומדן סיכון מעין זה יידרש להתבצע על בסיס מתמשך ומתגלגל. גם שאלת זהותו של הגוף שיבצע פעולה זו נותרה פתוחה והיא תידון בהמשך המאמר.

(2) אסטרטגיה של הסדרת ההתממה: מבט משווה

כאמור, מאמר זה מתמקד בבחינת האסטרטגיה הישראלית להתמודדות עם אתגר ההתממה, ובעיקר בשאלות אם ראוי שזו תהיה מרוכזת או סקטוריאלית ואיזה גופים צריכים ליטול תפקיד מרכזי במערכה זו. גם בנקודה זו ראוי להיבנות מניסיונן של מדינות אחרות בעולם.

ההסדרה בארצות־הברית מתקיימת בכמה רבדים, מצב שאינו מפתיע בהתחשב בכך שהסדרת הפרטיות ממילא מרובדת שם באופן כללי.[118] בהקשרים מסחריים, ברמה הכללית ביותר יש הסדרה על פי עקרונות שהתוותה רשות הסחר הפדרלית (Federal Trade Commission; FTC).[119] התייחסות כללית זו מחייבת גופים המבצעים התממה לנקוט אמצעים סבירים. כמו כן, עליהם לכלול בהתקשרויות שלהם התחייבויות המונעות ניסיון לבצע פעולות זיהוי של המידע המותמם ואף לדרוש התחייבות דומה מגופים שיקבלו מהם את המידע המותמם.[120] הסמכות הכללית, כמו גם נטילת ההובלה של ה־FTC, נדרשות בסוגיה זו מאחר שכמעט אין הגדרה קוהרנטית וקונסיסטנטית בארצות־הברית למושג "מידע מזוהה" או "מידע ניתן לזיהוי"; במקום זאת יש בליל של הגדרות שונות בחוקים שונים.[121]

כמו כן, שחרור מידע מידי רשויות המדינה מוסדר בדברי חקיקה פרטניים ובמיוחד Privacy Act, 1974 ו־Freedom of Information Act.[122] חוקים אלו קובעים נהלים מורכבים שבתי המשפט פירשו בדרכים שונות. לדעת אלטמן וחד ואחרים, בשל ההטרוגניות והמורכבות של החלטות אלו קשה מאוד ללמוד על בסיסן את הסטנדרטים שהפקידים השונים נוקטים לעניין זה.[123]

נוסף על כך, כמה הקשרים משפטיים מתייחסים פרטנית וביתר־הרחבה לנושא ההתממה. המרכזי שבהם[124] הוא התחום הרפואי המוסדר ב־Health Insurance Portability and Accountability Act (HIPAA).[125] על פי חוק זה, עיקר הסמכויות בעניני מידע רפואי (לרבות דרכי התממתו) מרוכזות בידי שני גופים – Department of Health and Human

---

118 ראו Schwartz, לעיל ה"ש 19, בעמ' 910, המסביר את החקיקה הסקטוריאלית של פרטיות והגנת מידע בארצות־הברית.

119 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, 21 (2012), https://goo.gl/wMGaay.

120 שם.

121 Schwartz & Solove, לעיל ה"ש 113, בעמ' 1828–1838. במקום זאת, חיקוקים רבים קובעים הגדרות אד הוק של Covered Information – מידע המכוסה על ידי החוק.

122 Freedom of Information Act, 5 U.S.C. § 552 (2012); Privacy Act of 1974, 5 U.S.C. § 552a (2012).

123 Altman et al., לעיל ה"ש 75, בעמ' 1977–1983.

124 יצוין כי יש רשויות נוספות הפועלות בארצות־הברית בתחום זה (בתחומי חינוך וכן ברמה המדינתית בלבד) כגון The Family Educational Rights and Privacy Act and the MA Data Security Regulation, ראו Altman et al., לעיל ה"ש 75, בעמ' 2038.

125 לעיל ה"ש 76.

Services (HHS), Office of Civil Rights (OCR). הכלל הגדול בהקשר זה הוא שאין להעביר מידע רפואי לגופים שלישיים, בכפוף לכמה חריגים, שאחד הבולטים בהם הוא מידע שעבר התממה.[126]

תקנות HIPAA קובעות את כללי הפרטיות (Privacy Rule) ואלה מגדירים שני מסלולים לביצוע התממה המאפשרת העברה של מידע רפואי לגופים שלישיים בלא בהסכמה.[127] מסלול אחד הוא שימוש במומחה להתממה והמסלול האחר הוא שימוש ב"נמל מבטחים". שיטת המומחה[128] כשמה כן היא: די בכך שמומחה יקבע כי הסיכון לאחזור המידע קטן מאוד. עם זאת, חסרות הגדרות עדכניות המתייחסות לשאלות שהוצגו לעיל באשר למהות הסיכון הקטן ולמיהות המומחה הרלוונטי. שיטת נמל המבטחים מעניקה הגנה מפני תביעות המבוססות על חשיפת מידע אישי לאחר התממה אם זו כללה הסרה של 18 מאפיינים מזהים מרכזיים.[129] אלה כוללים, למשל, שם, כתובת ומיקוד. המאפיין האחרון ברשימה זו הוא כוללני – "כל מזהה ייחודי אחר". הגנת נמל המבטחים תוענק רק במצב שבו לבעל המאגר אין ידיעה בפועל שאפשר לבצע זיהוי ליחיד בתוך המאגר. גם הפרשנות של רכיב זה סבוכה וטעונה כיום, לאור מכלול הגילויים בדבר חולשות ההתממה במובנה הצר. אכן, ההנחיות משאירות חוסר ודאות נרחב ונראה כי אינן עדכניות.[130]

עוד בארצות־הברית חשוב לציין את הוראות החוק שמסדיר את רשויות הסטטיסטיקה.[131] הגדרת המידע המוגן לפי חוק זה כוללת מידע המאפשר את זיהוי המשיב באמצעות היסק סביר, באמצעים ישירים או עקיפים.[132] החוק מחייב כי ועדה רלוונטית תבחן את המידע טרם השחרור ומפנה לנהלים שיש להשתמש בהם לשם כך. נהלים וועדות אלו בוחנים את אמצעי ההתממה שננקטו תוך התחשבות בנתונים שכבר נמצאים בידי הציבור.[133] לפיכך, גם בהקשר האמריקני אפשר לראות כי גופי הסטטיסטיקה עוסקים בהתממה הלכה למעשה מזה זמן, מתוקף תפקידם ומכוח חקיקה ייחודית. הכתיבה האקדמית מצביעה על כך שהדבר נעשה במיומנות רבה ותוך שימוש באמצעים מגוונים.[134]

באירופה יש כמה מודלים אסדרתיים, ריכוזיים יותר, להתמודדות עם אתגר ההתממה. במדינות האיחוד האירופי העניין מוסדר לרוב על ידי הרשות המקומית להגנת הפרטיות

126 ראו Altman et al., לעיל ה"ש 75, בעמ' 1990.

127 לדיון עדכני וקריאה לשינוי ראו National Committee on Vital and Health Statistics, Recommendations on De-identification of Protected Health Information under HIPAA (2017), https://goo.gl/ZfPtxx (להלן: המלצות לגבי מידע רפואי).

128 45 CFR § 164.514(b)(1).

129 45 CFR § 164.514(b)(2).

130 המלצות לגבי מידע רפואי, לעיל ה"ש 127, בעמ' 6.

131 Confidential Information Protection and Statistical Efficiency Act of 2002, Pub. L. No. 107-347, tit. V, 116 Stat. 2899 (2002).

132 "any representation of information that permits the identity of the respondent to whom the information. applies to be reasonably inferred by either direct or indirect means", שם, בס' 502(4).

133 ראו Altman et al., לעיל ה"ש 75, בעמ' 1993–1995.

134 שם, בעמ' 2006.

(ה־DPA); אך כמו בארצות־הברית, חלק מהמקרים מוסדרים באמצעות גופים פרטניים דוגמת רשות התרופות האירופית (European Medicines Agency; EMA).[135] גם היקף ההתערבות של הרגולטור משתנה באירופה ממדינה למדינה. בבריטניה, לדוגמה, בחרה רשות ICO (שסמכותה מקבילה, פחות או יותר, לרשות הגנת הפרטיות) בהסדרה ישירה (יחסית) בהציעה code of practice מקיף לדרכי הפעולה.[136]

לעתים הדברים מתגלגלים לפתחו של בית המשפט. כך, למשל, בית המשפט הצרפתי בחן את ההתנהלות של תאגיד הפרסום JCDecaux, שאסף כתובות MAC של טלפונים ניידים באזור מסוים.[137] התאגיד העביר את הכתובות תהליך של התממה שלדעתו היה מספק וסבר שבכך מיצה את כפיפותו לחוקי הגנת הפרטיות בכל הנוגע למידע זה. בית המשפט אימץ את העמדה של רשות הגנת המידע הצרפתית (CNIL), שטענה כי פעולות ההתממה שביצע התאגיד אינן מספקות ושהוא עדיין כפוף לחוקי הגנת הפרטיות לעניין מידע זה.[138]

נוסיף כי אוסטרליה שוקלת ממד אסדרתי נוסף על הנאמר עד כה, לאחר שורה של כשלי אבטחה סדרתיים שהובילו לחשיפת מידע אישי רב הנוגע לאזרחים אוסטרליים. כעת ממשלת אוסטרליה מקדמת הצעת חוק שלפיה תהא זו עברה פלילית לבצע אחזור זהות של מידע ציבורי שהותמם ופורסם ברבים.[139] הצעה זו עשויה להוביל לסיווג של פעילות מחקרית הנוגעת לסוגיית ההתממה כפלילית, על כן נמתחה עליה ביקורת.[140] אם תתקבל הצעת החוק, יעבור חלק מהאכיפה של דרכי ההתממה לידי רשויות האכיפה המרכזיות האמונות על אכיפת הדין הפלילי (קרי: בתי המשפט והפרקליטות).

לסיכום, אפשר לראות כי זרועות מדינתיות למיניהן פועלות במגוון דרכים להסדרת ההתממה במידות הצלחה משתנות. בארצות־הברית יש כמה מוקדי מומחיות, שמידת יעילותם משתנה, וייתכן שהם מעשירים אלו את אלו; באירופה אפשר לראות ריכוזיות ובצדה, באופן מפתיע, אוטונומיה סקטוריאלית מסוימת.

הניתוח שהצגנו לעיל דילג בחופשיות רבה יחסית בין מדינות ומשטרים והביא תובנות מפה ומשם, תוך התעלמות מהבדלים מהותיים בין המדינות – גודלן, ההיסטוריה התחיקתית שלהן, המבנה הכלכלי והרגולטורי והתחרות בשווקי המידע שלהן. התעלמות זו, שברגיל

---

135 European Medicines Agency Policy, לעיל ה"ש 16.

136 ICO, Anonymization: Managing data protection risk, Code of Practice 2012, Information Commissioner's Office, https://goo.gl/e4hhS3.

137 Media Access Control, מזהה ייחודי המוטבע על רכיבי תקשורת, לרבות מכשירי סלולר.

138 ראו Tene & Zanfir-Fortuna, לעיל ה"ש 97, בעמ' 3.

139 Leon ;Privacy Amendment (Re-identification Offence) Bill 2016, https://goo.gl/q1j2N2 Spencer, *Public Data Legislation Could See White Hats Face Jail,* **ARN** (13.10.2016), https://goo.gl/93UDuF; הצעות דומות צצות עתה גם במלכה המאוחדת ובניו זילנד: Polly Ralph & Sylvia Ng, *Will There Be a New Data Protection Offence for the UK* Asha McLean*, NZ Privacy* ;*Beyond GDPR*, **PWC** (8.9.2017), https://goo.gl/vMJSmi *Commissioner Recommends Australia's Data Re-identification Criminalisation* Lead, **ZDNet** (9.2.2017), https://goo.gl/FhwMFA.

140 אף על פי שקדמו לה הצעות דומות מפי מלומדים אמריקנים. ראו Rubinstein & Hartzog, לעיל ה"ש 3, בעמ' 740, המחברים מתייחסים לעבודתם של Yakowitz-Bambauer ו־Gellman.

היא רעה חולה הראויה להוקעה, סבירה בהקשר זה בשל רמת ההפשטה הגבוהה יחסית של הדיון. אף על פי שישראל קטנה לאין ערוך מהאיחוד האירופי וריכוזית הרבה יותר מארצות־הברית, עדיין יש חסרונות דומים העולים מביזור סמכויות ויתרונות מפתיעים בפעולה בו־זמנית. לפיכך, סקירה זו מקנה בסיס לבחינה ביקורתית של האסטרטגיה להסדרת התממה בישראל שאליה נפנה כעת.

ה. התממה בישראל הלכה למעשה

עד כה עסקנו במסגרת המשפטית לדיון בסוגיית ההתממה, ברובדי ההתממה השונים ובשאלות המרכזיות שבהן דנו מדינות שונות בהקשר של סוגיית ההתממה. בחלק זה נבקש להציג את האופן שבו גופים ציבוריים שונים בישראל מתייחסים להעברת מידע. ביתר פירוט, נציג את המסגרת המוגבלת שבה הרשות השופטת עוסקת בסוגיה זו, ובצדה את המורכבות ואת רמת המקצועיות המשתקפת מהתנהלותם של גופים ציבוריים שונים, בהם הרשות להגנת הפרטיות, רשות התקשוב, משרד הבריאות והלשכה המרכזית לסטטיסטיקה. לבדיקה שנבצע שתי מטרות: ראשית, היא תאפשר שרטוט כללי של אסטרטגיית ההסדרה של סוגיית ההתממה בישראל; שנית, היא תאפשר אומדן של רמת המקצועיות והמומחיות ולפיכך גם של התאמת הגופים השונים להתמודדות עם הסוגיה, בעיקר תוך השוואה לנעשה מעבר לים.

1. התממה בפסיקת בית המשפט העליון בישראל

סוגיית ההתממה אמנם התעוררה בשנים האחרונות בפסקי דין של בית המשפט העליון, אך נדונה בעקיפין בלבד, אגב דיון בשאלה אם מידע קיים הוא מידע אישי או מותמם או אגב בחינת דרכים להעברת מידע. להלן נבקש לדון בשני היבטים אלו כפי שהשתקפו בארבעה פסקי דין מרכזיים.[141] מדיון זה נבקש לגזור את ההתאמה של המערכת המשפטית לדון בעניינים אלו כחלק מאסטרטגיה כוללת וננסה להבין את הדין הפוזיטיבי בישראל בעניין זה.

141 מלבד פסקי הדין שבהם נעסוק להלן חשוב להזכיר לעניין זה את עניין **ונטורה**, לעיל ה"ש 38, שבו הוצגה עמדה מרחיבה בהגדרת העניינים הפרטיים של אדם. מעניין לראות שכבר אז ציינה השופטת שטרסברג־כהן כי בעוד שכל פריט מידע אינו בהכרח עניין פרטי, צירופם עשוי להיות עניין פרטי מוגן. ראו גם בירנהק, **מרחב פרטי**, לעיל ה"ש 38, בעמ' 221. עוד ראו בג"ץ 6824/07 **מנאע נ' רשות המסים**, פ"ד סד(2) 479 (2010), שבחן את ההעברה של מספרי תעודות הזהות של החולפים במחסומי דרכים במזרח ירושלים לממונים על גביית מס הכנסה כדי לבחון קיומו של חוב אפשרי במס. בג"צ בחן את השאלה אם חלה ההגנה שבסעיף 23ג לחוק הגנת הפרטיות, המתיר למסור מידע אם המסירה "דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו", והשאיר את השאלה בצריך עיון. בעניין זה ראו את חוות הדעת של רשם מאגרי המידע באשר לתנאים לאיסוף מספרי זהות למאגרי מידע ולשימוש בהם: https://goo.gl/AJHz5Q. ראו גם עס"ק (ת"א) 7541-04-14 **הסתדרות העובדים הכללית החדשה נ' עיריית קלנסווה** (פורסם בנבו, 15.3.2017), שם דובר בחיוב למסור טביעת אצבע לצורך שימוש בשעון נוכחות ביומטרי. בית הדין התייחס להיעדר האפשרות לשחזר את טביעת האצבע המקורית מההעתק שלה, אך קבע כי היעדר

נפתח בעניין **גוטסמן נ' ורדי**, שם נדונה השאלה אם שימוש בהדמיות ממוחשבות, המציגות תכנון אדריכלי של בית לקוח, פוגע בפרטיות של אותו לקוח. בית המשפט המחוזי קיבל את תביעת הלקוח (ורדי) וקבע כי פרטיותו נפגעה עקב החשיפה של הדמיות ביתו באתר האינטרנט של האדריכל. זאת, משום שהדמיות אלו מאפשרות להתרשם מאורח החיים בבית, מהרגלי הדיירים וממצבם הכלכלי.[142] בית המשפט העליון דחה את הערעור על פסק הדין אך הוסיף וקבע כי לא תתגבש פגיעה בפרטיות כשדרישת הזיהוי אינה מתקיימת, שכן סעיפי החוק מגנים על "צנעת חייו האישיים של אדם". ללא זיהוי אי־אפשר לדבר על פגיעה ב"אדם". אם כן, ככל שאי־אפשר לקשור בין המידע שפורסם לבין אדם ספציפי – לא תתקיים פגיעה בפרטיות.[143] למרות זאת הכיר בית המשפט באפשרות של פגיעה בפרטיות על ידי מידע המוצג בצורה אנונימית כשנוצר קשר לאדם ספציפי באמצעות ממצאים ונתונים אחרים המאפשרים להסיק מיהו. במצב כזה, אם יש אפשרות לשייך את המידע שפורסם לאדם ספציפי, יש לומר כי המידע היה מזהה מלכתחילה. במקרה זה, בשל העובדה כי הוסכם שבית הלקוח הנדון הוא "פרויקט יחיד מסוגו",[144] אפשר היה לקשור בין הדמיות הבית לבין הלקוח וכך נוצרה פגיעה בפרטיות.

בית המשפט הכיר באתגר שסוגיית הזיהוי מציבה ומכאן בצורך לבדוק את טיב ההתממה. עם זאת, בית המשפט השאיר סוגיות רבות פתוחות להכרעה עתידית (למשל, הוא לא דן בהיבטים של בדיקת הסיכונים והסיכויים לזיהוי). לפיכך, פסק הדין אינו נותן כלים להעריך מתי התממה, אם תבוצע, תעמוד בדרישות החוק להגנת הפרטיות ותחריג את מושאי המידע מתחולתו.

גם בעניין **פלוני נ' פלונית** התייחס בית המשפט לסוגיית המידע האישי ולשאלה אם אפשר לזהות אדם מסוים. בפרשה זו נדון רומן ספרותי שלטענת פלונית התבסס על תיאור אוטוביוגרפי מדויק של חיי המחבר ושל מערכת היחסים האינטימית שהייתה להם, ולפיכך פוגע בפרטיותה.[145] מנגד העלה המחבר שלל טענות הגנה ובהן כי הרומן שכתב איננו אלא יצירה בדיונית וכי אין בדמויות הנזכרות בספר משום תיאור אוטוביוגרפי נאמן. בית המשפט דחה את טענות המחבר וקבע כי הספר כולל פרטי זיהוי רבים וייחודיים שיש

הזיהוי אינו מכריע לעניין פגיעה בפרטיות שכן הפגיעה נוצרת מעצם ההרכשה. זהו נדבך נוסף שעמו ההתממה לא מתמודדת, אך הוא חורג מגבולותיו של מאמר זה.

142 ע"א 1697/11 **א. גוטסמן אדריכלות בע"מ נ' ורדי** בפס' 4 לפסק דינו של השופט פוגלמן (פורסם בנבו, 23.01.2013).

143 שם, בפס' 18 לפסק דינו של השופט פוגלמן. הערת אגב מעניינת מתייחסת למקרים חריגים שבהם יפורסם מידע רגיש במיוחד, העלול ליצור תחושה של חילול הפרטיות ללא אפשרות לקשור בין המידע לבין האדם.

144 שם, בפס' 23 לפסק דינו של השופט פוגלמן.

145 ע"א 8954/11 **פלוני נ' פלונית** (פורסם בנבו, 22.5.14). לדיון בהיבטים משפטיים אחרים של פרשייה סבוכה זו ראו את מאמרה של יעל ברוידא־בהט "מעבר לקהילתנות ולאינדיבידואליזם: התפיסה המורכבת של משפחה ושל הזכות לפרטיות בתוך המשפחה" **משפט, חברה ותרבות** ב 311 (מיכאל בירנהק עורך, 2019).

בטיבם ובהצטברותם כדי לזהות את המשיבה.[146] בית המשפט לא ציין אמות־מידה ברורות לבחינה מתי מידע אנונימי נהפך למזוהה ולפיכך כפוף לחוק הגנת הפרטיות וסעדיו, אך ציין דבר מה שנראה כקריטריון עמום: כאשר טיב הפרטים והצטברותם מבססים זיהוי על ידי מכר רחוק סביר. כמו כן, הפרטים שהיו ברומן, שכללו את הרגליה המיניים של פלונית, במידה רבה מתקבעים אף יותר בתודעתו של הקורא ומאפשרים זיהוי לאחר מעשה.[147] אפשר לומר שפסק דין זה עסק באפקטיביות ההתממה שביצע הסופר ליצירתו ולפרטים האישיים הנוגעים לתובעת. עם זאת, קשה להסיק מאמירות אלו כלל שיוכל לסייע לבעלים של מאגר מידע בבואו להחליט על מדיניות התממה בהקשרים אחרים (כמו הקשר של נתוני עתק).

בעניין **חשבים ה.פ.ס מידע עסקי בע"מ נ' הנהלת בתי המשפט** התעוררה שאלת ההתממה במובן רחב יותר אף שהשופטים לא זיהו אותה ככזו.[148] פסק דין זה עסק בתנאים שהציבה הנהלת בתי המשפט לפני חברת תקדין בטרם תמסור לה את פסקי הדין שפורסמו לצורך הפצה באמצעים שונים, לרבות אמצעים מקוונים. הנהלת בתי המשפט התנתה את מתן הגישה למאגר פסקי הדין וההחלטות שברשותה בהתחייבות של העותרת למנוע מִפתוח (אינדוקס) של המידע על ידי מנועי חיפוש. מניעת המִפתוח תגרום לכך שאי־אפשר יהיה לאתר את פסק הדין באמצעות מנועי חיפוש ברשת הפתוחה (לדוגמה באמצעות מנוע החיפוש של Google). למעשה, כדי להגן על הפרטיות של בעלי הדין ושל אנשים אחרים שפסקי הדין מתייחסים אליהם מצד אחד, וכדי להגשים את יעד פומביות הדיון מצד שני, דן עניין **חשבים** באופן עקיף בהתממה שהיא דרך ביניים אפשרית לאיזון בין שני האינטרסים הללו.[149]

בפרשה זו בחן בית המשפט, ראשית, את הסמכות של הנהלת בתי המשפט לקבוע את ההגבלה הנדונה וקבע כי אין כזו.[150] מעבר לכך, לענייננו, בית המשפט בחן את מידתיות הדרישה לחסימת המִפתוח ומצא אותה בלתי־מידתית מבחינת פגיעתה ביכולת הציבור ללמוד על תוכנם ועל קיומם של פסקי דין.[151] בית המשפט קבע כי היעדר מפתוח של פסקי הדין לא יגן על פרטיות בעלי הדין מסיבות שונות כגון העובדה שפסקי דין שיפורסמו ברשת על ידי צדדים שלישיים (כמו משרדי עורכי דין) ימופתחו ממילא.

מעבר לכך, במסגרת מבחן הסבירות ציין בית המשפט כי יש כלים חלופיים שעשויים להספיק ושבאמצעותם אפשר להפיץ את פסקי הדין ללא פגיעה בפרטיות. כך, למשל, אפשר לפרסם את פסקי הדין לבעלי הדין בלבד טרם הפרסום באינטרנט, תוך מתן אפשרות לבקש

146 בין ממצאים אלו אפשר למנות תיאור של מראה החיצוני, פרטים על אודות גילה, עיסוקה הייחודי, מקום לימודיה, מקום עבודתה ומקום מגוריה. שם, בפס' 141.

147 שם, בפס' 142.

148 בג"ץ 5870/14 **חשבים ה.פ.ס. מידע עסקי בע"מ נ' הנהלת בתי המשפט** (פורסם בנבו, 12.11.2015).

149 לחברת חשבים יש עניין מובהק בביצוע המפתוח משום שהוא מבטיח מספר ניכר של קישורים לפסק הדין המופיע במאגר תקדין לייט במענה לחיפושים במנועי חיפוש. קבלה של תוצאות אלו עשויה להוביל לרכישת גישה לפסק הדין הנדון. ראו גם בירנהק "חשיפה מקוונת וחשיפה משפטית", לעיל ה"ש 3, בעמ' 80–82. בירנהק מסביר את חשיבות השימוש בכתיבה זהירה מצד השופטים ונותן המלצות נוספות להגנה על פרטיות בפסיקה.

150 עניין **חשבים**, לעיל ה"ש 148, בפס' כה לפסק דינו של השופט רובינשטיין.

151 שם, בפס' לח.

מחיקה של פרטים מזהים; כלי אחר הוא שימוש באלגוריתמים לצורך איתור ומחיקה של פרטי מידע אישיים לא הכרחיים ועוד. במילים אחרות, בית המשפט הציע לבצע התממה במובן הצר והציג כלים שונים להגשמת יעד זה. הכלים שהוצגו הם סטטיסטיים (מחיקת מאפיינים מזהים), טכנולוגיים (סריקת פסיקה לראות אם מופיעים בה מספרי תעודת זהות), מנהליים (העברת פסקי הדין לבדיקת הצדדים בטרם פרסום, רענון נהלים אצל הסגל הרלוונטי) ומשפטיים (מעבר לפרסום פסק הדין רק עם ראשי התיבות של הצדדים, כמקובל בחלק ממדינות אירופה).[152] כל האמצעים הללו מרוכזים בנקודה כרונולוגית אחת – טרם פרסום פסק הדין. לדעתנו טעה בית המשפט משום שלא נתן את דעתו לכך שתהליך ההתממה הוא תהליך נמשך ורב־שלבי, ושגם ביתר שלביו אפשר וראוי להפעיל כלים שונים לצורך הגשמה של יעד ההתממה.[153] מעבר לכך, בית המשפט לא הכיר בכך שצורת הפעולה שעליה המליץ לפרסום פסקי הדין – שהיא בעצם מימוש המודל של "שגר ושכח" – היא מהלך מסוכן שכן מדובר במסמכים בעלי פוטנציאל אחזור.

לאחרונה, בעניין **הדסה**, שוב נדרש בית המשפט לדון בסוגיה אחרת שממנה אפשר להקיש לעניין ההתממה. מדובר בשאלה הנוגעת לקבילותו של מסמך רפואי, שפרטי המטופל בו הושחרו, כראיה בתביעה נזיקית הנוגעת לרשלנות רפואית.[154] השופטת יעל וילנר, כדנה יחידה, קבעה כי פרטיות המטופל אינה נפגעת מאחר שהמידע הרפואי מנותק מהקשרו ואינו קונקרטי.[155] כמו כן, בית המשפט הכיר בחשיבות של פרסום מידע אנונימי – במקרה זה כמו גם במקרים אחרים – לשם קידום אינטרסים חברתיים. בכך קבע בית המשפט במפורש כי העברת מידע שעבר התממה אינה כפופה לכללים הנוקשים החלים על העברת מידע אישי מגוף אחד לאחר.[156] גם כאן לא עסק בית המשפט בקביעת כללים או גבולות לביצוע התממה כדין.

לסיכום: בתי המשפט נאלצים להתמודד עם שאלות הנוגעות להליך ההתממה וסביר להניח שייאלצו להמשיך לעשות כן, וביתר שאת, עם התפתחות הטכנולוגיה והתקדמות עידן המידע. ההתמודדות היא אך בראשיתה. ברוב התיקים שנדונו (למעט עניין **חשבים**) אין התייחסות למאגרי מידע עצומים שמהם אפשר לבצע היסקים לא צפויים בעיבוד של נתוני עתק. ייתכן שבמקרים אחרונים אלו יבחרו השופטים לבצע איזונים שונים או יעסקו בשאלות משפטיות שונות. התמודדות זו של המערכת המשפטית היא ברגיל הבסיס לעיצוב הכללים המשפטיים שינחו את שאר גופי המדינה בהתמודדות עם התממה; אולם, במקרה שלפנינו בתי המשפט אינם נותנים מענה מקיף לסוגיות שנסקרו לעיל בדבר ביצוע ההתממה על רבדיה והיקף הסיכון המותר. אין באמירה זו בהכרח משום ביקורת על בתי המשפט, שכן אין זה מתפקידם לדון בסוגיות שלא הונחו לפניהם; אולם, כפי שצוין לעיל, גם במקרים שבהם הדיון בעניין נדרש לא בהכרח זוהו סוגיות ההתממה ככאלה ולא נותחו

152 שם.

153 בירנהק "חשיפה מקוונת וחשיפה משפטית", לעיל ה"ש 3, בעמ' 54–55; כן ראו בעמ' 80 ביקורת מקיפה על פסק דין זה.

154 רע"א 7828/17 **הסתדרות מדיצינית הדסה נ' פלוני** (פורסם בנבו, 9.1.2018).

155 שם, בפס' 14.

156 שם, בפס' 17.

בצורה מדויקת. לפיכך, נראה כי המפתח להסדרה של התממה ראויה נמצא בידי גורמים אחרים בעת הזו. נדרשת מחשבה מעמיקה כיצד להביא לכך שהחלטות בעניין זה יתקבלו על ידי גורמים מתאימים, שיראו את מכלול ההיבטים של הסוגיה ויוכלו להתייחס להיבטים החדשניים הכרוכים בה. לדיון בגורמים אלו נפנה כעת.

2. התממת מידע: עמדתם של גופים ציבוריים נבחרים

(א) *משרד המשפטים – הרשות להגנת הפרטיות*

על פי חוק הגנת הפרטיות, הרשות להגנת הפרטיות (שהיא חלק ממשרד המשפטים) היא הגוף האמון על ההסדרה, הפיקוח והאכיפה של הנושאים הנדונים בחוק זה.[157] לפיכך, מתבקש לבדוק את דרך ההתמודדות של הרשות עם סוגיית ההתממה. כפי שנראה, מדובר בעמדה משתנה ועמומה. על פני הדברים נראה היה שרשות זו היא המתאימה ביותר להתמודד עם אתגר ההתוויה של מדיניות התממה ראויה, אך האופי הטכני והמורכב של העניין מעמיד הנחה זו בסימן שאלה. נדגים זאת באמצעות עיון בכמה הנחיות ומסמכים שהנפיקה הרשות האמורה, המתייחסים לסוגיית ההתממה.

התייחסות ראשונה של הרשות לסוגיה אפשר, ככל הנראה, למצוא בהנחיה של רשם מאגרי המידע מפברואר 2012, העוסקת באיסוף מידע במסגרת גיוס עובדים ומבחני התאמה כשמידע זה כולל פרטים הנוגעים לניסיון תעסוקתי קודם, השכלה, מצב בריאותי, מצב משפחתי ועוד.[158] בין היתר, הנחיה זו מתמקדת בזהות של מחזיק המידע[159] ובמשך הזמן המותר לשמירת המידע. בהתייחס למשך הזמן האמור נקבע שכל עוד השימוש במידע הוא לצורך הליכי המיון למקום עבודה ספציפי, על המעסיק או מכון המיון להשמיד את המידע מיד לאחר סיום השימוש בו.[160] אולם, ההנחיה גם קובעת כי "חובת המחיקה חלה רק על 'מידע' שמזוהה עם אדם או ניתן לזיהוי עמו. לכן, אם המידע במאגר עובר הליך

157 סמכות הרשות נובעת מכמה מקורות סמכות: ס' 10(ד) לחוק הגנת הפרטיות; ס' 3(א) לחוק נתוני אשראי, התשס"ב-2002, ס"ח 104; ס' 9(א) לחוק חתימה אלקטרונית, התשס"א-2001, ס"ח 210.

158 ס' 1.2 להנחיית רשם מאגרי מידע 2/2012 "הבהרה לעניין תחולה" (13.3.2012) (להלן: הנחיית רשם מאגרי מידע) – תחולת הוראות חוק הגנת הפרטיות על הליכי מיון לקבלה לעבודה ופעילות מכוני מיון. חשוב לציין כי בצד תפקידי הרשות כגוף מסדיר היא אמונה גם על הגנת המידע האישי במאגרי מידע אלקטרוניים מכוח חוק הגנת הפרטיות. ראו גם הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח-2018, וההנחיות שם.

159 ס' 3 לחוק הגנת הפרטיות מגדיר מחזיק כ"מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש".

160 ס' 2.8.2 להנחיית רשם מאגרי מידע. כפי שההנחיה מציינת, אחד מעקרונות היסוד הוא שמידע אישי יש לשמור רק לפרק הזמן ההכרחי למימוש המטרות שלשמן נאסף המידע. עיקרון זה נובע מעקרון צמידות המטרה, ס' 2(9) וס'-8(ב) לחוק הגנת הפרטיות, וכן ס' 14 לחוק, שלפיו המידע צריך להיות נכון ומעודכן; התוצאות של אבחונים פסיכולוגיים ומבדקי התאמה כנראה מאבדות ממהימנותן לאחר זמן מה בהיותן מבוססות על הנחות, ועל כן יש מקום למוחקן בחלוף פרק זמן זה.

של אנונימיזציה מוחלטת שאינה מאפשרת לייחס אותו לאדם אפילו בעקיפין – אזי אין עוד צורך למוחקו".[161]

מלשון הוראה זו אנו למדים כי הרשות מאפשרת לגופים לצאת מתחולתו של חוק הגנת הפרטיות אם המידע שבידיהם יעבור "אנונימיזציה מוחלטת" – אך בלי להסביר איך לבצע מהלך זה. מעבר לכך, עצם השימוש במושג "אנונימיזציה מוחלטת" הוא בעייתי, משום שראוי לדבר על הליכים אלו במונחים הסתברותיים, להבדיל ממושגים דיכוטומיים ומוחלטים.

התייחסות נוספת לעניין ההתממה יש בהנחיה של רשם מאגרי מידע לעניין שימוש בשירותי מיקור־חוץ לעיבוד מידע אישי, וזאת על דרך שאלות ותשובות הנוגעות לעניין זה.[162] הנחיה זו עוסקת בסוגיית ההיעזרות בשירותי מיקור־חוץ בפעילות של ארגונים, הכרוכה בניהול מידע אישי המעובד בארגון באופן ממוחשב. בהתייחס לשאלה אם הנחיה זו חלה במקרים של שימוש בשירותי מיקור־חוץ לניטור תעבורה של אתרי אינטרנט, ההנחיה קובעת כי ככל שמדובר בשירות השומר מידע אישי מזוהה או כזה שניתן לזיהוי על אודות הגולשים – אזי ההנחיה חלה;[163] עם זאת, ככל שמדובר בשירות המספק שירותי סטטיסטיקה, הנאספים לאחר שהמידע עבר הליך אנונימיזציה להנחת דעתו של בעל המאגר – לא תחול ההנחיה.

מהתייחסות זו אנו רואים הרחבה של מושג המידע האישי המוגן אף לכזה ה"ניתן לזיהוי". מצד שני, אנו רואים במסמכים של הרשות חזרה על המושג "אנונימיזציה" והסתמכות עליו בלי לפרט אמות־מידה לביצוע הפעולה. חמור מכך: אנו רואים כי ההחלטה בעניין טיב האנונימיזציה ניתנת תוך הסתמכות על חוות דעתו של בעל המאגר.

לסיום, נציין התייחסות מצד הרשות לסוגיית ההתממה במסמך שפרסמה לעניין האופן והחשיבות של תסקיר השפעה על הפרטיות (privacy impact assessment). במסמך זה הרשות ממליצה להכין תסקיר כאמור כשארגון מקים או מנהל פרויקטים חדשים שעשויה להיות להם השפעה על הפרטיות.[164] ממסמך זה עולות הכרה והבנה עמוקות יותר של עקרונות ההתממה ואף נכונות להתמודד עמן, אף על פי שעדיין יש מקום רב לשיפור. לדוגמה, לצורך אותו מסמך, "מידע אישי" מוגדר כמידע מזוהה או ניתן לזיהוי (ובכך הורחבה היריעה של סוגי המידע שהחוק חל עליהם, בדומה לדין האירופי שהוזכר לעיל).[165] הרשות מוסיפה

---

161 ס' 2.8.3 להנחיית רשם מאגרי מידע. בהמשך מודגש כי כמובן אין באמור למנוע מן המכון או מהמעביד לארכב את המידע ככל שמוטלת עליהם חובה חוקית מפורשת לעשות כן, או לצורך מטרות אחרות הנובעות ישירות מהליכי הקבלה לעבודה של אותו עובד. חשוב לציין כי הנחיה זו הובילה לתביעה מטעם חלק ממכוני ההשמה שדרשו לשנותה, וזו אכן שונתה וצומצמה מעט בהסדר פשרה שקיבל תוקף של פסק דין. אין בשנויים שהתקבלו שם כדי להשפיע על עיקרי הדברים שהוצגו בגוף המאמר. ראו עת"מ 4749-04-12 **אדם מילא בע"מ נ' רשם מאגרי המידע** (פורסם בנבו, 21.2.2013).

162 הרשות למשפט, טכנולוגיה ומידע (רמו"ט) (כיום הרשות להגנת הפרטיות), שאלות ותשובות בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי https://goo.gl/au46wp.

163 **שם**.

164 הרשות למשפט, טכנולוגיה ומידע (רמו"ט) (כיום הרשות להגנת הפרטיות), **תסקיר השפעה על הפרטיות** (2015) https://goo.gl/AXdSEY. ראו והשוו להטמעת השימוש בכלי זה **באיחוד האירופי**, GDPR, לעיל ה"ש 11, Recital 35.

165 **שם**, Article 4(1), Recital 26.

ומחדדת כי במקומות ובתהליכים שבהם נשמר מידע שאיננו מזהה, עדיין יתכן שמדובר במידע הניתן לזיהוי "על ידי הצלבת מידע זה עם מידע אחר".[166] לפיכך, תסקיר הפרטיות צריך לכלול התייחסות לסיכון בדבר הנדסה חוזרת של תהליך ההתממה.[167] הרשות גם מכירה בצורך לסקור את ההתממה של בעלי המאגר.[168] במילים אחרות, אפשר לראות במסמך את ראשית התמודדות עם נושא הזיהוי החוזר של נתונים ומידע מותמם, לכל הפחות בדרישה שנושא זה יובא בחשבון על ידי בעלי המאגר. אולם, במסמך זה – כמו בשאר המסמכים שהזכרנו – אין הכוונה נורמטיבית מטעם הרשות המסבירה מהו אופן ההתממה המקובל. תחת זאת נראה כי האחריות לכך מגולגלת אל מחזיקי המידע או אל בתי המשפט (ספק אם אלו או אלו יוכלו לתת מענה הולם). אם כן, אף על פי שהדבר נמצא במסגרת תפקידה, סמכותה ותחום מומחיותה, עד עתה לא נתנה רשות זו מענה הולם לסוגיית ההתממה. לפיכך, נפנה לחפש כיסי מומחיות בנושא התממה אצל רשויות שלטון אחרות ונשקול את ההשפעה של מומחיות זו על אסטרטגיית ההסדרה של הנושא בישראל.

(ב) *רשות התקשוב הממשלתי*

רשות התקשוב הממשלתי אמונה על מטרות שונות בתחום המחשוב במדינה, לרבות "ממשל זמין" ו"הנגשת מידע ושירותים ממשלתיים לציבור".[169] בעניין אחרון זה פרסמה הרשות בשנת 2016 דוח לציבור שזכה ליישום בהחלטת ממשלה באוגוסט 2016.[170] מטרת הדוח היא יצירת חדשנות במתן שירותים לציבור על בסיס חשיפה של מאגרי המידע ושקיפות הפעילות הציבורית.[171] מאחר שחלק ממאגרי המידע העתידים להיחשף כוללים מידע אישי (או מידע שחשיפתו תוביל לפגיעה בפרטיות אחרי ביצוע הצלבות עם מידע אחר), דוח זה עסק בהיבטים שונים של פרטיות ואף של התממה. באופן בלתי־מפתיע מצא הדוח שאין בישראל מדיניות אחידה באשר להליכי אנונימיזציה, לרבות הסרת מידע פרטי ממאגרי מידע. לעומת זאת, הוא מצא שמשרדים שונים מבצעים תהליכי אנונימיזציה מגוונים, בהתאם לכלים הטכנולוגיים שברשותם ועל סמך בחינה מקצועית של שיטות אנונימיזציה יעילות.[172] באמירות אלו יש משום חיזוק נוסף לצורך בבדיקה המוצגת במאמר – סקירה של אסטרטגיית ההסדרה של התממה בישראל ושל אופניה – ובהמלצה על מתווה מתאים. ניתוח האמור בדוח זה מאפשר לבחון את אסטרטגיית ההסדרה של רשות התקשוב ולהשוותה לזו של גורמים אחרים.

166 שם, בס' 1.2.4.

167 שם, בס' 2.1.1.10.

168 שם, בס' 1.9.1, 3.3.3.

169 ראו אתר רשות התקשוב הממשלתי https://goo.gl/KSYxhV.

170 החלטה 1933 של הממשלה ה־34 "שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור" (30.8.2016).

171 רשות התקשוב הממשלתי, משרד ראש הממשלה, "דו"ח מסכם – הצוות הבין משרדי להנגשת מאגרי מידע לציבור", 6 (07.2016). מטרות נוספות הוגדרו כהמלצות בדבר עשרת המאגרים שיקבלו עדיפות להנגשה במשך 2015 וליצירת מתווה לעריכת תחרויות לפיתוח אפליקציות המשתמשות במאגרי מידע.

172 שם, בעמ' 36.

הדוח מבקש להתוות דרך ואסטרטגיה כללית לחשיפה של מאגרי מידע ציבוריים על אף החשש המתמיד שהחשיפה תוביל לפגיעה בפרטיות. הדוח ממליץ, באופן כללי, כי טרם החשיפה ייערך תסקיר פרטיות שיבחן את מידת ההשפעה של החשיפה על הפרטיות, תוך ליווי של נציגי מחלקת ייעוץ וחקיקה (במשרד המשפטים) בהתאם לצורך.[173] אולם, אם מדובר במאגר שבפרסומו אינו עלול לפגוע בפרטיות, אזי מנהל המאגר רשאי לקבוע כי אין צורך בעריכת תסקיר כזה. הקביעה תיעשה בהחלטה מנומקת בכתב, תוך התייעצות בגורמים הרלוונטיים, לרבות היועץ המשפטי של המשרד הרלוונטי והממונה בו על אבטחת המידע.[174] אנו רואים כי השאלה המורכבת – האם המידע שבמאגר עשוי להוביל לחשיפת מידע אישי לאחר הצלבתו עם מידע ממאגרים אחרים – מנותבת למחלקת ייעוץ וחקיקה במשרד המשפטים או לייעוץ המשפטי ולאנשי מערכות המידע של המשרד הרלוונטי. מובן כי הצלחה של מהלך מעין זה תלויה בקיומה של מדיניות תומכת ובהכשרה מתאימה למי שהופקד על ביצועו. ייתכן שביזור המוסמכים לקבל החלטה בעניין איננו צעד נבון בסוגיה המצריכה ידע ומומחיות ייחודיים.

כדי לאפשר חשיפה של מאגרים עם מידע אישי הדוח פונה להתממה ומציע למשרדי הממשלה לבחון, משפטית וטכנולוגית, אם אפשר להפחית או אפילו לבטל את הפגיעה בפרטיות באמצעות הסרת הנתונים המזהים טרם הנגשת המאגר. הדוח מציין כי גם במקרים שבהם אין במאגר מידע פרטי יש לבחון אם הצלבתו עם מאגר נוסף תאפשר להסיק מידע פרטי. ככל שהדבר אפשרי, הדוח מבקש לבחון אם השמטה של שדות מסוימים תבטל את הסיכון לפגיעה בפרטיות.[175]

נראה כי כמה אמירות בדוח מעידות על כך שכותביהן הפנימו את התובנות המתקדמות בנוגע להתממה שכבר התקבלו במדינות אחרות (והוזכרו לעיל). ראשית, בבואו להכריע בשאלות הנוגעות לפרטיות והתממה, הדוח מציין כי אין ודאות שאפשר להוכיח באופן מוחלט כי התממה מסוימת תמנע אפשרות של זיהוי חוזר ולכן ראוי לשקול החלה של מבחני סבירות המקובלים במדינות אחרות.[176] לעניין זה אימץ הדוח תפיסה של ניהול סיכונים להבנת מנגנון ההתממה, תוך הכרה בכך שהחלטה אם לפרסם מאגר מידע דורשת איזון אל מול אינטרסים אחרים.[177]

שנית, נראה כי הדוח מאמץ את ההכרה שהתממה היא תהליך רב־שלבי. הדוח מכיר בכך שביצוע התממה דורש היעזרות במומחים מתחומי הטכנולוגיה, אבטחת המידע והייעוץ המשפטי, ואיננו נחלת הסטטיסטיקאים בלבד.[178] הדוח מציין דרכים סטטיסטיות להקטין את הפגיעה בפרטיות, והוא אף מסביר כי לעתים הפצה של מאגר מידע (אפילו אחר התממה) באופן פתוח אינה מומלצת ולכן יש לנקוט אמצעים טכנולוגיים למיניהם (כגון שאילתות או חדרי מחקר) כדי להבטיח הנגשה חלקית.[179] גם ההיבט המשפטי של ההתממה מוזכר ומוכר.

173 שם, בעמ' 35.
174 שם.
175 שם, בעמ' 36.
176 שם, בעמ' 34.
177 שם, בעמ' 37.
178 שם, בעמ' 38.
179 שם, בעמ' 20.

הנספח לדוח מתייחס לתנאי השימוש באתר data.gov.il, ואלה כוללים קביעה שהמשתמש אינו רשאי להשתמש במידע, בין היתר באמצעות שימוש שיפגע בפרטיותו של אדם, לרבות על ידי הצלבת מידע עם מקורות אחרים.[180]

שלישית, הדוח מכיר בצורך לפרסם הנחיות ברורות לכל משרדי הממשלה ומסביר כי רשות התקשוב הממשלתי, מחלקת ייעוץ וחקיקה והרשות להגנת הפרטיות יצטרכו לחקור את השאלות שעלו לצורך הכנת הנחיות כאמור.

לסיכום, למרות היעדר ידע ומקצועיות בתחום הפרטיות, נראה כי בניסיונה להתמודד עם המשימה פיתחה הרשות היכרות והבנה של תחום ההתממה. לאור זאת, ייתכן שיש לשקול בחיוב את המשך המעורבות של רשות זו בהתוויית אופני ההתממה ככל שהדבר נוגע לרשויות המדינה. יש לציין כי לפי המתווה שבדוח חלק מהאחריות מנותב למחלקת ייעוץ וחקיקה במשרד המשפטים, אולם יש להמשיך ולבדוק אם יש רשויות בעלות מומחיות רבה יותר בתחום מורכב זה ואם נבון להותיר את ההחלטות הנוגעות לענייני התממה בסמכותן של הרשויות שתוארו בחלק זה.

(ג) *התממת מידע רפואי*

המידע הרפואי העשיר שנאגר בארגוני בריאות, במוסדות אקדמיים, במכוני מחקר ובחברות מסחריות נועד ויכול לשרת צרכים שונים. בצד הצרכים הרפואיים והניהוליים (שלשמם בדרך כלל נמסר המידע מלכתחילה) אפשר להשתמש במידע לצרכים מחקריים ואף מסחריים.[181] במקרים רבים המידע שמור במאגרים הרפואיים בצורה דיגיטלית וסדורה. בשנים האחרונות חלחלה בישראל ההכרה שמידע זה הוא אוצר בלום שאפשר להפיק ממנו תובנות ויתרונות רבים.[182] זאת, בין היתר, בשל תיעוד מקיף ורב שנים יחסית, זיהוי אחיד (באמצעות מספר תעודת זהות), ריכוזיות גבוהה במאגרים וקישוריות גבוהה ביניהם.[183]

מובן שהעברה של מידע רפואי אישי מהגורם שקיבלו למטרה מסוימת אל גורמים אחרים ולהגשמת מטרות אחרות (או אף למטרות אחרות של אותו גוף) מעוררת בעיות פרטיות קשות המוסדרות בחוקים ייחודיים, כפי שהוסבר לעיל. במיוחד עולה בהקשר זה המתח בין הרצון להגן על פרטיות היחידים במידע רפואי רגיש לבין הרצון להגיע לתובנות מחקריות מדויקות שייטיבו עם כלל הציבור, ישפרו את בריאותו ואולי אף יובילו להצלת חיים. על

180 שם, בעמ׳ 103–105. עוד מצוין כי כל הפרה של תנאי הרישיון תביא לסיום תוקפו לאלתר, אך לא ברור כיצד הוראה זו תמנע או תצמצם מקרים של פגיעה בפרטיות.

181 המכון הלאומי לחקר שירותי הבריאות ומדיניות הבריאות (ע״ר) ״כנס ים המלח ה־16 – נתוני בריאות – קריאה להסדרה״, 67 (2016) (להלן: דוח המכון הלאומי).

182 החלטה 3709 של הממשלה ה־34 ״תוכנית לאומית לקידום תחום הבריאות הדיגיטלית כאמצעי לשיפור הבריאות וכמנוע צמיחה״ (25.3.2018) https://goo.gl/oJnwEK. מצוין כי המטרה שבבסיס ההחלטה היא ״להאיץ את הצמיחה הכלכלית, למצות את התועלות הכלכליות והחברתיות הטמונות בפתרונות חדשניים בתחום הבריאות הדיגיטלית ולמנף את היתרונות היחסיים של ישראל בחדשנות הטכנולוגית ברפואה ובמחקר״. ראו גם רוני לינדר־גנץ ״התוכנית של נתניהו: חוקרים וחברות פרטיות יקבלו גישה למידע הרפואי של הציבור״ **דה־מרקר** (25.3.2018) https://goo.gl/Ne9heD.

183 **דוח הבריאות 2018**, לעיל ה״ש 60, בעמ׳ 39.

פני הדברים נראה כי התממה היא פתרון מתאים להשגת יעדים אלו. אולם, דווקא בהקשר זה ההתממה לעתים בעייתית משום שביצועה עלול לפגוע באיכות הנתונים – וכך גם בטיב המסקנות שאפשר ללמוד מהם.[184] כמו כן, ביצוע ההתממה מקשה על היכולת לחזור אל הנבדקים כדי לטייב את הנתונים או כדי לתת להם המלצות פרטניות על בסיס הממצאים.

בעניין זה הוגשו בשנים האחרונות שני דוחות מקיפים שמהם עולה המומחיות של העוסקים בתחומי הבריאות בהתמודדות עם אתגרי ההתממה (בדומה למה שהתרחש במדינות אחרות): הראשון נערך על ידי המכון הלאומי לחקר שירותי הבריאות; השני הוא מסקנות הוועדה ליישום המלצות השימושים המשניים במידע בריאות (להלן: דוח היישום).[185] הממשלה אימצה דוח אחרון זה בהחלטת ממשלה ונראה כי הפרויקט שנדון בו יוצא לדרך במסגרת פרויקט תמנע.[186] יש לציין כי הדוחות עסקו במגוון נושאים והתממה היא רק אחד מהם.[187]

הדוחות פורשים את דרכי ההתממה שאפשר לאמץ כדי להתמודד עם האתגרים שניצבו לפני כותביהם: ניצול טוב יותר של נתוני הבריאות בישראל תוך עמידה בדרישות של חוק הגנת הפרטיות, כמו גם באלו של דינים נוספים הנוגעים לפרטיות ולשימוש במידע רפואי.[188] קריאת הדוחות מלמדת כי מחבריהם קיבלו בהם כמה עקרונות שאומצו במדינות אחרות כגון המשגת ההתממה במונחים של סיכון (הדוחות אף מפרטים בצורה מושכלת את גורמי הסיכון).[189] כמו כן, דוח היישום משרטט מפת דרכים לבניית מודל התממה תוך הבחנה בין ארבעה סוגי מידע: מידע מזוהה – הכולל מאפיינים המצביעים חד־משמעית על מטופל מסוים,[190] מידע ללא מזהה מובהק (שאולי ייהפך למזהה עם הצלבת מידע ממאגר אחר),[191] מידע מחקרי ומידע סטטיסטי. חלוקה זו מעידה על חדשנות ועל הכרה בכך שרמות סיכון שונות מצדיקות אסדרה משפטית שונה (תובנה שאין סיבה להגביל רק להקשר הרפואי). כמו כן, הדוח עוסק ביתרונות ובתועלות שעשויות לצמוח מהתהליך ונראה כי יתרונות רבים יותר יצדיקו התממה מסוכנת יותר. בכך הדוח מבדיל בין מתן טיפול או שירות רפואי, מחקר לקביעה של מדיניות בריאות, הנגשת נתונים לציבור ולבסוף העברתם למטרות שיווקיות. גם נקודה זו מלמדת על הבנה מתקדמת יותר של פרמטר הסיכון במשוואת ההתממה. הדברים

184 שם, בעמ' 110.

185 **דוח הבריאות 2018**, לעיל ה"ש 60.

186 החלטת ממשלה 3709, לעיל ה"ש 182.

187 דוח המכון הלאומי התייחס גם לאתגרים נוספים: היעדר אחידות באיכות הנתונים, סוגיות הנוגעות לבעלות במידע, מגבלות המשאבים לכריית משאבים, חשש מפגיעה במוניטין של ארגון המשתף מידע וכן סוגיות של קניין רוחני, סודות מסחריים ושמירה על יתרונות עסקיים. ראו **דוח המכון הלאומי**, לעיל ה"ש 181, בעמ' 83.

188 לדוגמה, דוח המכון הלאומי מבחין בין התממה מבוזרת שכל גוף נוקט לבין התממה מרכזית. שם, בעמ' 91.

189 שם, בעמ' 90–91.

190 למשל מספר תעודת זהות, שם המטופל, פרטי התקשרות ועוד. ראו **דוח הבריאות 2018**, לעיל ה"ש 60, בעמ' 111.

191 למשל תאריכים הקשורים למטופל כגון תאריך לידה, תאריך טיפול ושיוך לקבוצה מוגדרת כגון כתובת, מקצוע ועוד.

מעידים גם על הפנמה נוספת של התובנה שהתממה איננה מהלך דיכוטומי המוציא את הנתונים הרלוונטיים לחלוטין מתחולתם של דיני הפרטיות.

המסמכים העוסקים בהתממת מידע רפואי מכירים בכך שיש דרכי התממה נוספות, מעבר למנגנונים הסטטיסטיים של הסרת שדות או עיוותם ("התממה במובן הצר");[192] במילים אחרות, יש בהם הכרה בכך שלהתממה יש לא רק היבט טכנולוגי או סטטיסטי אלא גם היבט ארגוני.[193] כמו כן יש בהם הכרה בצדדים המשפטיים של המהלך, תוך פירוט ההסכמים שעליהם יידרשו הנעברים לחתום, לרבות פירוט סנקציות בגין הפרה.[194] לבסוף, יש בהם התייחסות לשימוש בבסיס נתונים סינטטי, כלומר בסיס נתונים ששומר על ההתפלגות והקשרים בין המשתנים אבל לא שומר על התצפיות המקוריות – עדות נוספת להיכרות עם החדשנות בהליך הסדרה זה.[195]

החדשנות שבדוחות מתבטאת גם בהתייחסות לאסטרטגיית ההסדרה. דוח היישום מציע מתווה לגוף שיאשר שימושים משניים במידע רפואי. גוף זה יורכב מוועדות אתיקה מוסדיות כמו גם מוועדה מרכזית שתדון בעררים על החלטות של הוועדות המוסדיות. ועדות אלו תפעלנה בכל ארגון האוסף מידע רפואי, ללא תלות בסוג הארגון – בתי חולים, קופות החולים, מוסדות אקדמיים, חברות מסחריות וכדומה.[196] הוועדות יידרשו ליישם כללים לשמירה על פרטיות ולשם כך ייעזרו בסטטיסטיקאי;[197] בתוך כך יינתן דגש גם לשקיפות ההליך.[198] שוב, בכל אלו אנו רואים הפנמה של השינוי בעולם הידע הנדרש להשלמה של מטלות ההתממה כמו גם לאסדרתה הראויה. כמו כן, אנו רואים בדוחות יצירה של מסלול מקביל לאישור של העברות מידע, המתקיים בנפרד מנתיבי האישור שהוצגו לעיל על פי חוק הגנת הפרטיות.[199]

לסיכום, דוחות אלו והחלטות הממשלה המבוססות עליהם מראים כי הגורמים המסדירים הרלוונטיים התקדמו כברת דרך בהתמודדות עם סוגיית ההתממה. הדוחות וההחלטות מעידים על ידע, מחשבה ותחכום. אפשר להתווכח אם האיזונים שאומצו אכן נותנים משקל מתאים לעקרונות הפרטיות. שאלה זו תתחדד אם נבחר להטיל על רשויות הבריאות את הובלת ההתמודדות עם סוגיית ההתממה ככלל. מעבר לכך, כמובן שראוי אף לבחון אם נכון להותיר את סוגיית ההתממה הרפואית בידי גורמי הרפואה או שמא יש להעבירה לגורמים ריכוזיים יותר (כמשרד המשפטים).

192 לדוגמה, מוזכר מודל חדרי מחקר המופעל כיום בלשכה המרכזית לסטטיסטיקה ובחיל הרפואה. חדר מחקר כזה נגיש לחוקרים מורשים בלבד. ראו **דוח המכון הלאומי**, לעיל ה"ש 181, בעמ' 95. מובן שלקיום של חדרים כאלו יש משמעות כלכלית ומשמעות בהקשר של נגישות למידע.

193 **דוח הבריאות 2018**, לעיל ה"ש 60, בעמ' 58.

194 שם, בעמ' 22.

195 להרחבה ראו גם **דוח המכון הלאומי**, לעיל ה"ש 181, בעמ' 95, 118.

196 **דוח הבריאות 2018**, לעיל ה"ש 60, בעמ' 14.

197 שם, בעמ' 16.

198 שם, בעמ' 138.

199 ראו דיון בהעברת מידע בין גופים ציבוריים, לעיל ה"ש 51.

(ד) *התממת מידע סטטיסטי הלשכה המרכזית לסטטיסטיקה*

כפי שהוסבר לעיל, הלמ"ס – מכוח תפקידה כמרכזת ומפיצה של מידע סטטיסטי ומלשון פקודת הסטטיסטיקה – נדרשה זה מכבר לסוגיה של התממת מידע. עיון בדוחות הלמ"ס ובמסמכיה מגלה בקיאות והתמודדות עם שאלות ומונחים של עולם ההתממה זה שנים רבות. הדבר שונה מאוד מרשויות אחרות, שרק לאחרונה מגלות את עומק השאלות הנדונות, אם בכלל. ממסמכים שהכין גוף זה עולה כי עמדת הלמ"ס מתקדמת למדי ורואה את הצורך לשלב כמה אמצעים להגנה על מידע.

נדגים ונוכיח אמירות אלו תוך הצגת הוועדה המייעצת לנושא הרחבת השימוש בקבצים עם נתוני פרט למטרות מחקר – ועדת אקשטיין (2005).[200] בתחילת דבריה הסבירה הוועדה כי ועדות סודיות של הלמ"ס התמודדו עם סוגיות התממה כבר בשנות התשעים של המאה הקודמת. הדבר התבטא בקביעתן שאפשר לפרסם קבצים שהסיכוי לזיהוי בהם מזערי, המכונים PUF – Public Use Files. גם בקבצים אלו, שהוועדה מבקשת להנגיש לכל הציבור, יש להפריד לשתי קבוצות (קבצים כבדים וקבצים קלים) ולכל קבוצת קבצים יינתן רישיון שימוש שונה.[201]

הדוח מסביר כי התמודדות עם הסיכון תיעשה באמצעים טכנולוגיים שימזערו את הסיכוי לזיהוי מידע בצד יצירה של "סביבה משפטית בטוחה".[202] "סביבה משפטית בטוחה" מתבססת על מסירה של קובצי מידע תחת חוזה (Microdata Under Contract, MUC) רק לגורמים שנתפסים כאמינים ובעלי אינטרס לקיים את החוזים.

אכן, ועדת אקשטיין שאפה להרחיב את השימוש בנתוני הלמ"ס למחקר אקדמי ועסקי באמצעות הרחבת השימוש בקובצי MUC, תוך צמצום הפגיעה בצנעת הפרט ותוך יצירת סביבה בטוחה לקבצים אלו. סביבה בטוחה זו תתבסס על כלים טכנולוגיים להגנה על נתונים שאינם מאפשרים שמירה או ביצוע חיתוכים בין קובצי MUC שונים. כמו כן, השימוש בקבצים ייעשה תוך פיקוח צמוד של הלמ"ס ותוך מעקב אחר החזרת הקבצים בסיום העבודה.[203] הגופים שיורשו לקבל את הקבצים ייקבעו על פי מטרות הארגון, מטרות המחקר, מאפייני האוכלוסייה, קיומן של חלופות למסירת מידע וקיומו של חשש לזליגת מידע.[204]

מדברים אלו שבדוח אנו למדים כי כבר לפני שנים רבות הפנימה הלמ"ס שסוגיית ההתממה מצריכה הערכת סיכון, להבדיל מהערכה דיכוטומית, וששימוש בה מוביל ליצירת תת־קטגוריות של מידע וקבצים. עוד אנו רואים הכרה בכך שהתממה דורשת אלמנטים סטטיסטיים, טכנולוגיים וגם משפטיים.

---

200 המועצה הציבורית לסטטיסטיקה **דוח הוועדה לבדיקה ואפיון של קבצי פרט** (2005) https://goo.gl/BDBWYR (להלן: דוח ועדת אקשטיין).

201 הוועדה יוצרת סיווג־משנה לקובצי PUF כבדים או קלים, שהשימוש בהם יחייב רישוי מסוג שונה. ראו שם, בעמ' 2. לעיון בתנאים של רישיון PUF לשימוש עצמי, ללא זכות הפצה, ראו https://goo.gl/aStQE9. הקובץ ה"קל" לא מחייב רישוי הואיל ו"איננו מאפשר הורדת קבצי פרט", והקובץ הכבד מאפשר הורדת קובץ ולכן דורש תוספת סייגים משפטיים.

202 **דוח ועדת אקשטיין**, לעיל ה"ש 200, בעמ' 1.

203 שם, בעמ' 3.

204 שם.

בצד הידע המקיף והניסיון המצטבר, הטיפול של הלמ"ס בהתממה ידע גם כישלונות. לדוגמה, חוקרים באוניברסיטת תל־אביב הצליחו לבצע כמה התקפות על מידע שפרסמה הלמ"ס בפומבי (בעיקר תוך איתור קבוצות בעלות מספר חברים קטן מאוד).[205] נוסף על כך, הלמ"ס מנגישה מאגרי מידע עם "נתוני פרט" לא מזוהים בשלושת חדרי המחקר שהיא מפעילה במשרדיה בירושלים, בחיפה ובתל־אביב.[206] עם זאת, לטענת החוקרים חדרי מחקר אלו מיושנים ואינם מותאמים לעבודת מחקר.[207] ייתכן שיש פער בין הרטוריקה המקצועית של הלמ"ס לבין ביצוע הדברים בשטח.

ו. עמדות של גופים בישראל בסוגיית ההתממה: ניתוח רוחבי

בחלק זה תוצג טבלה המסכמת את עמדות הגופים שנסקרו בסוגיית ההתממה. סקירה זו חשובה משום שהיא מסייעת לבחון את אסטרטגיית ההסדרה הקיימת ומאפשרת זיהוי של כמה תובנות שיסייעו בגיבוש ההסדרה העתידית. סוגיה זו קריטית במיוחד כעת, כשחלק מיוזמות ההתממה שנדונו לעיל ימשיכו להתקדם ויחייבו יצירה של מבנה ניהולי ומשפטי סדור. במצב מעין זה, אפשר היה להניח שהאפשרות הטבעית היא נטילת ההובלה בידי משרד המשפטים ובתי המשפט, תוך צמצום עד למינימום של תפקיד הגופים האחרים. למרות זאת, סקירה של מקרי המבחן, של הניסיון הבין־לאומי ושל הניתוח התאורטי שהובא בתחילת הדברים עשויה להוביל למסקנה מעט שונה.

הניתוח הרוחבי מתמקד בשלושה קריטריונים עיקריים: התייחסות להתממה כמונח דיכוטומי לעומת התייחסות לסיכונים, התייחסות לחשיבות של תסקיר הבוחן את הפגיעה בפרטיות והכרה בסוגיית ההתממה כתהליך רב־שלבי. לצורך ההדגשה, קריטריונים שניתן עליהם מענה נצבעו באפור.

205 אמיתי זיו "עניתם לסקר אנונימי של הלמ"ס? מישהו יודע את כל הסודות שלכם" **דה־מרקר** (6.1.2013) https://goo.gl/beM7pn.

206 ראו הלשכה המרכזית לסטטיסטיקה **חוק חופש המידע: דין וחשבון שנתי 2016 של הלשכה המרכזית לסטטיסטיקה** 37 (2017) https://goo.gl/GDUAgY. יצוין כי לבנק ישראל יש חדר מיוחד המבוסס על מערכת גישה מרחוק. כדי להכפיף את החוקרים להוראות של פקודת הסטטיסטיקה, לצורך שימוש בחדרי מחקר, החוקרים מוגדרים כמתנדבים של הלמ"ס.

207 עודד ירון "מסע התלאות של החוקרים בלשכה המרכזית לסטטיסטיקה" **הארץ** (28.3.2014) https://goo.gl/QNe6N5.

הקריטריון / הגוף	התממה כמודל דיכוטומי או כמודל הבוחן סיכונים	הכרה בחשיבות של תסקיר הבוחן את הפגיעה בפרטיות	הכרה בהתממה כתהליך רב־שלבי
בתי המשפט	אין דיון (פסק דין **גוטסמן**)[208]	אין דיון	אין הכרה בכך שהליך ההתממה הוא מתמשך ורב־שלבי (פסק דין **חשבים**)[209]
משרד המשפטים – הרשות להגנת הפרטיות	התייחסות לאפשרות של גופים לצאת מתחולתה של הגנת הפרטיות אם המידע יעבור "אנונימיזציה מוחלטת",[210] כלומר התייחסות דיכוטומית ללא התייחסות לסיכונים.	המלצה: לערוך תסקיר השפעה על פרטיות לכל ארגון המקים או מנהל פרויקטים שעשויה להיות להם השפעה על הפרטיות.[211]	אין התייחסות
רשות התקשוב הממשלתי	המלצה: כאשר אין במאגרים מידע פרטי יש לבחון אם הצלבת המידע שבמאגר עם מאגר אחר תאפשר להסיק מידע פרטי.[212]	המלצה: לערוך תסקיר פרטיות שיבחן את מידת ההשפעה של חשיפת מידע על הפרטיות, בהתאם לצורך בליווי נציגים ממחלקת ייעוץ וחקיקה (משרד המשפטים).[213]	הכרה בכך שהתממה היא תהליך רב־שלבי והתייחסות לדרכים סטטיסטיות להקטנת הפגיעה בפרטיות ולכלים טכנולוגיים נוספים.[214]
התממת מידע רפואי	המשגה של התממה במונחים של סיכון תוך הבחנה בין סוגי מידע.[215]	הצעת מתווה לגוף שיאשר שימושים במידע רפואי ויורכב מוועדות אתיקה מוסדיות.[216]	הכרה בדרכי ההתממה השונות, כולל מעגלים של אבטחה ובקרה.[217]
הלשכה המרכזית לסטטיסטיקה	קביעה של סוגי קבצים שהסיכוי לזיהוי בהם מזערי, הפרדת רישיונות השימוש בהתאם לסוגי הקבצים[218] והגדרה של "סביבה משפטית בטוחה".	התייחסות להליך היצירה של סביבה בטוחה לשימוש בקבצים תוך פיקוח צמוד של הלמ"ס. העברת הקבצים לגופים תוך התחשבות בפקטורים שונים.[219]	הכרה בדרכי התממה שונות ומגוונות.[220]

208 עניין **גוטסמן**, לעיל ה"ש 142.

209 עניין **חשבים**, לעיל ה"ש 148.

210 **הנחיית רשם מאגרי מידע**, לעיל ה"ש 158.

211 "תסקיר השפעה על הפרטיות", לעיל ה"ש 164.

212 דוח מסכם – הצוות הבין־משרדי, לעיל ה"ש 171.

213 שם, בעמ' 36.

214 שם, בעמ' 20.

215 **דוח הבריאות 2018**, לעיל ה"ש 60 בעמ' 111.

216 שם, בעמ' 14.

217 שם, בעמ' 85.

218 **דוח ועדת אקשטיין**, לעיל ה"ש 200.

219 שם, בעמ' 3.

220 שם.

בטרם נמשיך נעיר כי ספק אם מערך ההסדרה המקביל והמרובד שנוצר כעת בישראל הוא תוצאה מכוונת. אמנם, במידה רבה מערך זה הוא תולדה של חוקים נפרדים שנחקקו בדורות שונים (לדוגמה, פקודת הסטטיסטיקה המנדטורית וחוק הגנת הפרטיות משנות השמונים), אך לאו דווקא מתוך כוונה ליצור משטרי אסדרה מקבילים. גם אם הדבר נעשה במכוון, ספק אם עומדות מאחורי כוונה זו הצדקות כגון הרצון לעודד חדשנות או פיתוח מהיר ואוטונומי של הדין. בסופו של יום, משטרי ההסדרה הנפרדים נוצרו בעיקר משום שהם מתייחסים לסוגי מידע שונים (למשל, מידע רפואי או מידע שנמצא בידי המדינה) או לתהליכי עיבוד שונים (למשל, שחרור המידע בידי המדינה או שימושים כלליים של חברות פרטיות במידע). לפיכך, לכאורה קשה להשוות בין משטרי מידע אלו ולהקיש מאחד על האחר.

עם זאת, בשל המאפיינים של עידן נתוני העתק ושל אתגר ההתממה, ראוי כי הדיון באסטרטגיית ההסדרה יתעלם מההבדלים בין התפקידים של זרועות השלטון השונות, מאופי המידע השונה הנאסף על ידן ומהשימושים העתידיים בו. הסיבה לכך היא שבעבר אפשר היה לייחס, ברמה הקטגורית, רמות סיכון שונות לחשיפת מידע שונה (למשל, מידע רפואי ומידע פיננסי) ובכך להצדיק משטר משפטי שונה לכל אחד מההקשרים. כמו כן אפשר היה להצביע בכלליות על סוגי עיבוד מידע פוגעניים יותר (על ידי המדינה, באופן כללי), פוגעניים פחות (על ידי רשות סטטיסטית), חשובים יותר (למחקר רפואי) וחשובים פחות (לצורך שיווק מוצרי מותרות). לעומת זאת, כיום עידן נתוני העתק מאפשר היסקים רגישים ופוגעניים ממידע שבעבר לא נחשב כשלעצמו למידע רגיש. כך, לדוגמה, נתונים מדינתיים הנוגעים למגורים, להשכלה ולצריכת שירותים ציבוריים מאפשרים היסקים באשר למצבו הכלכלי של היחיד ולמאפיינים אישיים אחרים. יתרה מזו, השימוש בהתממה מאפשר היסקים בנאליים ממידע רגיש. מובן שיש מצבים מסוכנים יותר או חשובים יותר. ההתממה ללא ספק תלוית הקשר ודורשת התמודדות שונה במצבים שונים.[221] לדוגמה, אומדן הסיכון וקביעת סף עליון לסיכון מקובל צריכה להיעשות בצורה שונה וייחודית בכל הקשר והקשר, בהתחשב הן במידע הגולמי והן במטרות השימוש.[222] עם זאת, אתגרים אלו עשויים להתעורר בכל הקשר ותחת כל חוק. החלוקה הגסה של משטרי הפרטיות וההתממה שקיימים היום ונדונו לעיל אינם מעניקים (או יכולים להעניק) מענה ממוקד, על פי סוגי הסיכון וחשיבות הפרויקט. לפיכך, האתגרים של הסדרת ההתממה ואיזונה אל מול הזכות לפרטיות הם משותפים במידה רבה לכל הגופים הנוגעים בתחום זה. ועדיין, כפי שנסביר להלן, אפשר להצדיק הסדרה סקטוריאלית ייחודית מסיבות אחרות.

מבחינת המצב הפוזיטיבי בישראל כיום, הניתוח והטבלה לעיל מדגימים כמה מנגנונים ומשטרי התממה. ההשוואה ביניהם מלמדת על שונות במקצועיות ובחדשנות בהפעלת המנגנונים. מעבר לכך מסתמן יתרון לגופים הסקטוריאליים דווקא. לדוגמה, התייחסות לסוגיית הסיכון – שהיא נחלתם של רגולטורים רבים בעולם – לא חלחלה למסדירים המרכזיים בישראל (משרד המשפטים ובתי המשפט), אך בהחלט מצאה נחלה אצל מסדירים אחרים. בדומה לכך, גם ההבנה וההכרה בריבוד שבהתממה מתקיימים אצל גורמים מסדירים

221 Tene & Zanfir-Fortuna, לעיל ה"ש 97, בעמ' 3.

222 ראו לעיל חלק ד2(ב)(1) במאמר זה, "סיכוני ההתממה ומידת הפרטיות שהיא מעניקה".

פרטניים (תחילה בלמ"ס ולאחר מכן גורמים באחרים) ולא במשרד המשפטים על שלוחותיו או בבתי המשפט.[223]

אפשר להציע כמה הסברים לתוצאה זו בהסתמך על הרקע התאורטי שבו פתחנו את המאמר. אפשר לסבור שהגופים המשפטיים ה"מרכזיים" אינם בקיאים או אינם פתוחים לשנויים שעברו על עולם ההתממה. ייתכן גם שדרך עבודתם אטית ומחושבת יותר נוכח העובדה שתהיה לפעולתם השלכה רוחבית על מכלול השחקנים, מדינתיים ופרטיים כאחד. לעומת זאת, רגולטורים מקצועיים כגון הלמ"ס או גורמי בריאות הם בעלי היכרות עמוקה עם העולם הסטטיסטי ובעלי קשר קרוב לגורמים מסדירים דומים במדינות אחרות (שכבר עשו כברת דרך בנושא ההתממה). בחלק מהמקרים הם אף בעלי מומחיות טכנולוגית (בעיקר בלמ"ס) שאפשרה להם להעשיר את ההסדרה הישראלית. נראה כי עם הזמן הידע הזה חלחל – דרך הלמ"ס או מסגרות אחרות בישראל או מחוץ לה – גם לרגולטורים מקצועיים אחרים כגון הרשות לתקשוב.[224] לחילופין ניתן לסבור כי היעדר הרתיעה מהשפעה מרחיבה אפשר לאותה חדשנות הסדרתית לפרוח באותן מסגרות. ראוי עוד לציין כי תוצאה זו של הרבוד איננה ברורה מאליה. לדוגמה, סקירת המצב בארצות הברית הראתה כי לפחות חלק מהמסדירים הסקטוריאליים (או מערכות ההסדרה הסקטוריאליות) אינן מתנהלות באופן אופטימאלי בהקשר ההתממה. ייתכן שבישראל, לפחות בעת הזו בשלו תנאים מסוימים המובילים להצלחת הרגולטורים הסקטוריאליים.

כך או כך, אפשר לסכם ולומר שהתממה מבליטה את יתרונות ההסדרה הסקטוריאלית המעטה שנותרה במשפט הישראלי. מסקנה ראשונה זו של המחקר מובילה להמלצה שלפיה אולי ראוי להמשיך ולשמר את המבנה הסקטוריאלי, וזאת בניגוד למתווה הריכוזי המסדיר את דיני הפרטיות בישראל באופן כללי. לפיכך, גם עתה, אם וכאשר יבקשו בתי המשפט והרשויות המקצועיות במשרד המשפטים לקחת את ההובלה בנושא ההתממה, עליהם לשקול היטב את צעדיהם. ייתכן שתובנות אלו מחייבות אותם לקחת על עצמם תפקיד זה בצניעות, תוך הסתמכות על פעולות הנעשות ברשויות אחרות ועל הידע והמומחיות שנרכשו שם; ייתכן שאף ראוי כי כל אחת מהרשויות שצוינו תמשיך לפעול באוטונומיה מסוימת בעניין זה, כדי שיוכלו – כל אחת מהן בנפרד – לקדם את הידע והמומחיות בנוגע להתממה. אכן יש בכך משום בזבוז משאבים וכפילות תפקידים, אבל גם הזדמנות להיעזר בידע ובקשרים הייחודים שרכשו הפועלים במסגרות אלו.

ראוי לצמצם את היקפה של המלצה זו. תחילה כדאי לתהות אם יש להגביל את מספר הרשויות הלוקחות על עצמן את ההתוויה של מדיניות התממה – שהרי גם בנק ישראל פרסם מסמך מתווה למדיניות התממה.[225] ייתכן כי מעבר למספר מסוים של רגולטורים, ריבוי סוגי המדיניות בסוגיה ייהפך מורכב ובזבזני (בדומה לביזור בארצות־הברית, המוביל

223 כך, למשל, גם בהקשר של תקנות הגנת הפרטיות, לעיל ה"ש 52, אפשר לזהות קיבעון מסוים מצד מחלקת ייעוץ וחקיקה במשרד המשפטים.

224 אירידור־הרשקוביץ ושוורץ־אלטשולר סבורות כי יש להטיל על רשות התקשוב את האחריות להסדיר את הסוגיה. ראו אירידור־הרשקוביץ ושוורץ־אלטשולר, לעיל ה"ש 3, בעמ' 66.

225 ראו אריאל מנצורה **התממה של קבצים עם מידע פרטני** (2017) https://goo.gl/Eok5Qz.

גם רגולטורים סקטוריאליים לקיבעון), ועל כן ראוי להגבילו לרשויות שנסקרו, המביאות ערך מוסף להליך ההתוויה של מדיניות זו.

חשוב להתייחס גם לשתי בעיות מרכזיות במשטר המבוזר דנן. ראשית, המשטר המבוזר עשוי לאפשר לכוחות פוליטיים וכלכליים להפעיל לחצים ביעילות רבה יותר על אותם גופי אסדרה והסדרה סקטוריאליים ופריפריאליים, אשר עשויים להיות מחוץ לתשומת הלב הציבורית והמשפטית, ובכך להשפיע על מדיניות ההתממה כך שתפגע באינטרס הציבורי. שנית, יש חשש שרגולטורים סקטוריאליים לא יהיו רגישים דיים לרבדים החוקתיים של זכות הפרטיות העשויה להיפגע עקב ההתממה. ייתכן שלשתי הבעיות יש פתרון אחד: הגברת המודעות והמקצועיות של הגורמים המשפטיים הרלוונטיים לקשיים ולדקויות הכרוכים בסוגיית ההתממה. הדבר נכון הן לייעוץ המשפטי של המשרדים והגופים והן לשופטים שידונו בעניינים אלו. הגברת המודעות תיעשה באמצעות סדנאות והשתלמויות משותפות שיתמקדו בהקניה ובהעברה של ידע בתחום חשוב אך מורכב זה.

ז. סיכום ומסקנות

התממה היא אמצעי חשוב. למרות חולשותיה היא מאפשרת הנגשת מידע לצורך קידום של יעדים חברתיים וכלכליים מרכזיים. כמו כן, מידע מותמם פחות חשוף ממידע מזהה לתקיפות של גופים המעוניינים לפגוע או להעתיק את המידע. לפיכך, ככל שגופים ציבוריים ופרטיים ימשיכו לשמור מידע אישי ולהעבירו, קיומה של חלופה זו מקדם את האינטרס בהגנה על הפרטיות.

ישראל עושה את צעדיה הראשוניים והחשובים בהתמודדות עם סוגיית ההתממה, אך אין ספק שבהמשך הדרך צפויות תקלות שיובילו לכך שמידע אישי ייחשף לפני תוקפים או לעין כול. לכן חשוב כבר עתה לגבש מדיניות מערכתית וכוללת לסוגיות הנוגעות להתממה, הממוקמות בצומת המחבר סטטיסטיקה, טכנולוגיה, מנהל ומשפט. כפי שהראנו לעיל, יש בישראל מחשבה על סוגיות אלו. בו־זמנית, זרועות שונות של הממשלה מתמודדות עם סוגיות שונות הנוגעות להתממה. זו התוצאה של מערכת חקיקתית מסועפת, כמו גם של יוזמות שונות המתקדמות בו־זמנית. אם כן, האתגר הניצב לפני גורמי המדיניות ומקבלי ההחלטות הוא שילוב של תחומי הידע השונים והמתפתחים – כמו גם הגדרת הגורמים המובילים ובעלי היכולת לאזן כראוי בין האינטרסים השונים.

במאמר זה סקרנו באופן ביקורתי את אסטרטגיית ההסדרה בישראל והמלצנו על מתווה לשינויים ולהמשך הפיתוח של אסטרטגיה זו. בכך, למעשה, מאמר זה מניח את התשתית לפיתוח הדיון בדרכי ההתמודדות עם התממה במוסדות הציבוריים המרכזיים בישראל, וזאת תוך עיון בעמדות העדכניות של מקבלי ההחלטות בגופים אלו.

מובן כי מעבר להסדרת ההתממה יש לדיון זה השלכות על הסדרת הפרטיות בכלל. ראוי לבחון אם המלצתנו האמורה לעיל – להמשיך בצורה מדודה עם הסדרה סקטוריאלית – מתאימה לשאלות אחרות הנוגעות להגנת הפרטיות ולאבטחת מידע וסייבר. שאלה זו קריטית במיוחד בישראל כיום, בשעה שהצעות חוק מבקשות להתוות את הסמכויות של הרשות להגנת הפרטיות ומערך הסייבר, תוך הרחבת סמכויותיהן לפינות רבות במערך ההסדרה

בישראל.[226] בהחלט ראוי לשקול שימוש במתודולוגיה היסודית שהוצגה כאן לבדיקת סוגיות פרטיות אחרות, כמו זו הנוגעת להגנת הסייבר, ולהתאמתן למודלים שונים של הסדרה. אנו תקווה כי מחקרים עתידיים ימשיכו לעסוק בנושא זה, במישורים נוספים, תוך הסתמכות על אבני הדרך שהנחנו בסקירה זו.

226 ראו, למשל, תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018.