

מידע רפואי ופרטיות בסביבה טכנולוגית מורכבת

מיכאל בירנהק[§]

צפוי להתפרסם במחקרי משפט (2026)

תקציר

מה גורלה של הפרטיות במידע רפואי בסביבה טכנולוגית דינמית? מידע רפואי נוצר בהקשרים מגוונים ורבים: טיפול רפואי, רכישת תרופות, שימוש באביזרים רפואיים, חיפוש באינטרנט ופעילות ביישומי ספורט. למידע ערך רב – ערך רפואי למטופל לצורך טיפול מיטבי, ערך כלכלי לגורמים מסחריים, וערך ציבורי לקידום המחקר הרפואי, זיהוי מגיפות ושיפור הטיפול. מול זה, ניצבת הזכות לפרטיות במידע רפואי, המוגנת חוקתית וחוקית.

המאמר בוחן שלושה מפגשים של רפואה, טכנולוגיה ומשפט: כניסת נתוני עתק בעיקר למחקר הרפואי, כניסת הבינה המלאכותית למחקר ולטיפול הרפואי עצמו, והפיכת הזירה למצב מידעי מורכב, מרובה שחקנים מסוגים שונים שיש ביניהם זרימת מידע אינטנסיבית ורב-כיוונית. המאמר מבקש לזהות את הפגיעה בפרטיות בכל מפגש כזה ולדייק אותה, וטוען שהסיכון לפרטיות אינו מוגבל לחשש מדליפה, אלא נוגע לכל שלבי מהלך החיים של המידע. התממה אינה פתרון קסם לאתגרי הפרטיות. הפתרון המוצע משולב: משפטי – ביסוס שליטה נמשכת של נושא המידע במידע הרפואי שעל אודותיו, חיזוק ההסכמה מדעת, הקשחת חובות ואכיפה יעילה; אתי – הפנמת חשיבות הפרטיות בחינוך ומודעות; וטכנולוגי – תרגום כללים לעיצוב מערכות. המסקנה שעולה מהדברים היא כי יש לשאוף לשלב את הגנת הפרטיות עם קידום הטכנולוגיה, תוך הבנת הפרטיות כשליטה נמשכת במידע האישי.

MEDICAL DATA AND PRIVACY IN A COMPLEX TECHNOLOGICAL SETTING

Michael Birnhack

Forthcoming: Bar Ilan Law Studies (2026)

How does privacy fare in medical data within a dynamic technological environment? Medical data is generated across a wide range of contexts, including the provision of healthcare, the purchase of medications, the use of medical devices, health-related internet searches, and activity on fitness devices. Such data possesses considerable value: clinical value for patients in enabling optimal medical care, economic value for commercial entities, and public value in advancing medical research, identifying epidemics, and improving healthcare systems. At the same time, the right to privacy in medical data enjoys both constitutional and statutory protection.

This article examines three points of intersection between health, technology, and the law: the growing use of big data, particularly in medical research; the

[§] פרופסור מן המניין, הפקולטה למשפטים, אוניברסיטת תל אביב. תודתי לצוות המחקר של פרויקט "בעקבות המידע" (מענק מחקר מס' 1838/24 של הקרן הלאומית למדע במסגרת תכנית מפ"צ) עומרי לביא, ניצן רחמילביץ' ומשה שוורץ, וכן למשתתפות הכנס "בינה מלאכותית, רפואה ומשפט" (בר אילן, ינואר 2026), לאורי הכהן ולמערכת "מחקרי משפט", על הערות מועילות.

integration of artificial intelligence into both medical research and clinical practice; and the transformation of the medical information ecosystem into a complex, multi-actor environment characterized by intensive, multi-directional flows of information. The article seeks to identify and refine the distinct privacy harms arising in each of these contexts, arguing that privacy risks are not confined to concerns over data breaches but extend throughout the entire data lifecycle. The article further contends that anonymization is not a panacea for contemporary privacy challenges.

The article proposes a multidimensional solution. Legally, it advocates establishing individuals' continuous control over their personal medical information, strengthening informed consent, imposing more stringent legal obligations, and ensuring effective enforcement. Ethically, it calls for fostering greater awareness of the importance of privacy through education and public engagement. Technologically, it emphasizes embedding legal and ethical principles into system design. The article concludes that the protection of privacy and the advancement of technology should be pursued in tandem, with privacy understood as the individual's continuous control over their personal data.

3	מבוא
5	א. מסגרת הדיון
5	1. רשת הדינים
5	(א) חוק היסוד
6	(ב) חוק הגנת הפרטיות
7	(ג) פרטיות בחקיקת הבריאות
9	(ד) חוזים
10	(ה) אתיקה
10	2. שליטה נמשכת במידע
11	(א) מעגלי ההצדקות
13	(ב) פרטיות כשליטה
15	3. חשיבות הבירור של הפגיעה בפרטיות
16	ב. נתוני עתק רפואיים
16	1. מחקר רפואי בנתוני עתק
19	2. תמונת מצב מחקרית
20	3. אתגרי הפרטיות במחקר נתוני עתק
21	(א) הגיון לינארי מול מעגליות
21	(ב) מידע קטן, בינוני, גדול, ועתק
21	(ג) מזעור מידע?
22	(ד) תכלית השימוש וצמידות מטרה
23	(ה) הסכמה?
23	(ו) התממה: פתרון קסם או מקסם שווא?
26	(ז) סיכום ביניים
27	ג. בינה מלאכותית בשירות הרפואה
28	1. שימושים רפואיים בבינה מלאכותית
31	2. אתגרי הפרטיות הרפואית של הבינה המלאכותית
31	(א) קלט: נתוני עתק
33	(ב) עיבוד ושימוש
33	(ג) דליפה ופלט
33	(ד) מסגרת הפעולה
34	ד. מידע רפואי כמצב מידעי מורכב
34	1. זרימת מידע רב-כיוונית
36	2. זירת המידע הרפואי

36	(א) תמונה כללית (היער)
38	(ב) העברות מידע (חלק מהעצים)
41	(ג) האתגר
42	סיכום

מבוא

אנחנו מייצרים מידע רפואי באינספור מקומות והקשרים: למשל במהלך ביקור אצל רופאה ובבדיקות וטיפולים בקופת חולים ובבית חולים, ברכישת תרופות ומוצרים בבית המרקחת, ובשימוש באביזרים רפואיים כמו קוצב לב ומשאבת אינסולין. אנחנו מייצרים מידע רפואי גם בעת חיפוש באינטרנט או בשימוש בטכנולוגיה בינה מלאכותית, לעיתים בצירוף מסמכים ותוצאות בדיקות. מידע רפואי נוצר גם באופן אגבי, למשל במהלך פעילות שמתועדת ביישומון ספורט, כאשר אנחנו עונדים "שעון חכם" שמודד דופק ומנטר את השינה, או כאשר אנחנו מציינים מצב רפואי באתר היכריות או ברשת חברתית. מאמר זה בוחן את גורלה של הפרטיות במידע רפואי בסביבה טכנולוגית שמתפתחת במהירות, ואת מקומו של המשפט בזירה הזו.

למידע רפואי יש ערך רב, בראש ובראשונה עבורנו, כדי שנוכל לקבל טיפול רפואי מיטבי. למידע יש ערך כלכלי לגורמים מסחריים שונים שאוחזים במידע. בנוסף, למידע רפואי יש ערך ציבורי: צירוף נתונים של יחידים ועיבוד המידע מאפשר לזהות התפרצות מגיפות, לדייק ולהתאים טיפולים, לזהות התנגשויות בין תרופות ותופעות לוואי, לצמצם טעויות במרשמי תרופות, ולשפר את הרפואה בכלל. מידע רפואי משמש גם ל"אימון המכונה" של טכנולוגיות בינה מלאכותית: המידע הוא חומר גלם שמוזן למערכות, שיוצרות לברר דמיון ושוני בין נתונים שונים, לאתר מתאמים, להציע ניתוחים נוספים, תחזיות, ולעבד מידע בכלל. מערכת בינה מלאכותית שהוזנה במידע איכותי תדע לאבחן בעיה רפואית במהירות וכנראה בדיוק רב יותר מאשר מאבחן אנושי, או לכל הפחות, להיות כלי עזר מועיל באבחון. כבר כיום יכולה הבינה המלאכותית לפענח הדמיות כמו צילומי רנטגן, סי.טי., ו-MRI, ולהצליב את המידע עם מידע נוסף על המטופל ובדיקותיו. התועלת החברתית עצומה.

מול זה, ניצבת זכותנו לפרטיות במידע רפואי, זכות שיש לה עוגן חוקתי וחוקי מפורשים.¹ מידע רפואי נמצא בליבת הזכות לפרטיות. רשת דינים מגנה על הפרטיות בהקשרים רפואיים, בגיבוי מערכת אתית ותיקה ומבוססת. די להזכיר את שבועת היפוקרטס, היא שבועת הרופאים על גרסאותיה השונות, שכוללת התייחסות מפורשת לחובת הסודיות של רופא בקשר למידע של מטופלים. פגיעה בפרטיות בנוגע למידע הרפואי נתפסת כפגיעה חמורה מבחינה חברתית, משפטית ואתית. פרשות של דליפת מידע רפואי זוכות לתשומת לב רבה, למשל בעקבות הפריצה למחשבי בית החולים הלל יפה,² דליפת מידע מחברת הביטוח שירביט, או דליפת מידע מאתר ההיכריות הלהט"בי אטרף, שכלל בין היתר התייחסות ל-HIV.³

התוצאה היא התנגשות חזיתית בין פרטיות המטופלים לבין צרכים ציבוריים ומסחריים. לאחר שילוב הדרגתי של טכנולוגיות נתוני עתק (Big Data), אנחנו נמצאים כעת בשלב ההתפעמות הראשונית מהבינה המלאכותית שהתפתחה והבשילה במשך כמה עשורים, והתפרצה לחיינו בשלהי שנת 2022, עם הפצתן של טכנולוגיות של בינה מלאכותית יוצרת (Generative AI).⁴ יתרונותיה של הטכנולוגיה בכלל ובהקשר הרפואי בפרט, דרמטיים במיוחד. במקביל, הזירה הרפואית הופכת מורכבת יותר ויותר, עם שחקנים חדשים, פרטיים ומסחריים, שמצטרפים לשחקנים ציבוריים.

כיצד להתיר את ההתנגשות הזו? במבט ראשון, מתבקש להנגיד את זכות הפרט לפרטיות עם הקדמה הטכנולוגית על יתרונותיה העצומים להתפתחות הרפואה ולבריאות הציבור, ולבחור באחד הצדדים. מאמר זה מבקש להציע מבט שני, ולהתעכב, במקום לדלג מיד לאיזונים בינאריים. אטען שאין הכרח לבחור רק בהגנת

¹ סעיף 7 לחוק יסוד: כבוד האדם וחירותו, והסדרי חוק הגנת הפרטיות, התשמ"א-1981 (להלן: חוק הגנת הפרטיות).

² ראו דיווח אצל נבו טרבלסי "יתקלה קריטית: אירוע סייבר בביה"ח הלל יפה" גלובס (13.10.2021), <https://www.globes.co.il/news/article.aspx?did=1001387130>. בעקבות האירוע, מבקר המדינה נדרש להיבטים של אבטחת מידע בגופי בריאות שונים. ראו דוח מבקר המדינה 1133 (2022).

³ הפרשות נדונו בבתי המשפט. ראו ת"צ (מחוזי מ"ר) 6615-12-20 שור נ' אר.אפ.אי. גלובל בע"מ (לשעבר שירביט חברה לביטוח בע"מ) (נבו 4.4.2025) (שירביט); ת"צ (מחוזי מ"ר) 8696-11-21 פלונית נ' סייברסרב אינטרנט ותקשורת בע"מ (נבו 10.10.2024) (אטרף).

⁴ לדיון בהיבטים משפטיים שונים של הבינה המלאכותית, ראו את מאמרי הכרך בינה מלאכותית במשפט הישראלי – משפט חברה ותרבות ח (ניבה אלקין-קורן ומעייין פרל עורכות, 2025).

הפרטיות או רק בקידום הטכנולוגיה, ויש לשאוף לשלב את שתי התכליות, ששתיהן ראויות, באופן מיטבי. לשם כך, יש לברר את טיבה של הפגיעה בפרטיות, כדי שנוכל לדייק את המענה המתאים – ואציע, שזהו מענה משפטי, אתי, טכנולוגי וחברתי משולב.

המאמר בוחן שלושה מפגשים של הרפואה, הטכנולוגיה והמשפט בהיבט הפרטיות, שמצטברים זה לזה. הראשון הוא הכניסה של נתוני עתק לזירה, השני, הוא כניסת הבינה המלאכותית לזירה, שנסמכת על נתוני עתק, אבל מרחיבה את מעגל השימושים ומרחיבה מאוד את הזרימה של המידע. המפגש השלישי הוא הפיכתה של הזירה למה שאקרא לומצב מידעי מורכב, מונח שמבקש לתאר העברת מידע נמשכת, בין שחקנים רבים מסוגים שונים, שכל אחד כפוף למסגרת משפטית מעט שונה. לגבי כל אלה, אטען שהסיכון לפרטיות במידע הרפואי אינו מוגבל רק לחשש מפריצה למאגר מידע או דליפתו, אלא הוא טמון גם בשלבים מוקדמים יותר במהלך החיים של המידע. אטען שיש לפעול להגנת הפרטיות הרפואית באופן יזום בכל שלבי החיים של המידע, ובכלל זה איסוף המידע, עיבודו, העברתו בין גורמים שונים, וחשיפתו. אטען שהתממה של מידע (אנונימיזציה) אינה פתרון קסם לאתגרי הפרטיות. הפתרון המשפטי הוא ביסוס השליטה הנמשכת של נושא המידע במידע שעל אודותיו. באופן מעשי, הדברים אמורים בחיזוק ההסכמה, בשיפור וחיזוק של זכויות שונות, בהקשחת חובות שונות, ובאכיפה יעילה יותר. הפתרון האתי והחברתי הוא הפנמה של חשיבות הפרטיות, שבאה לידי ביטוי בחינוך, במודעות וברגישות למטופלים ולמידע האישי שעל אודותיהם. הפתרון הטכנולוגי הוא לתרגם את הכללים המשפטיים והאתיים לעיצוב של המערכות, כדי שיאפשרו את השימושים המותרים ויסכלו שימושים לא מורשים. החשיבה המשפטית צריכה להתאים את הנחות היסוד שלה למצבים כאלה. נקודת ההתחלה, כך אטען, היא הבנה של הפרטיות כשליטה נמשכת, כהמשגה אחודה, לכל מישורי הפעולה של הפרטיות.

פרק א יתווה את המסגרת לדיון. אציג את מארג הדינים הרלוונטי שמגן על הפרטיות במידע רפואי, את ההצדקות להגנת הפרטיות בכלל ובהקשר הרפואי בפרט, ואת האזהרה מפני דילוג מהיר מדי לאיזונים בינאריים. בסיס זה יאפשר לנו לדייק בהמשך הדרך את הפגיעות בפרטיות ולזהות קשיים בהתמודדות המשפטית הנוכחית. **פרק ב** יציג את האתגר הטכנולוגי שמציבות טכנולוגיות של נתוני עתק. אצביע על הקשיים שמתעוררים בנוגע לעקרונות ההסכמה מדעת וצמידות המטרה, ואראה את הקושי שיש בתפיסת ההתממה כפתרון קסם. **פרק ג** יבחן את המפגש של המידע הרפואי עם טכנולוגיות בינה מלאכותית. אלה כוללות מרכיב של נתוני עתק, ולכן הדיון בהן ממשיך את הדיון הקודם. השוני העיקרי אינו בהכרח בטכנולוגיה עצמה, אלא באופן השימוש – בעוד שבשימוש בנתוני עתק רפואיים הגורמים הפועלים היו חוקרים וארגונים ממוסדים, הרי שבזירה של הבינה המלאכותית יש (יותר) שחקנים מסחריים, השימוש הופרט לכולנו, ולכן בקורות משפטיות ואתיות נחלשות. **פרק ד** ימשיג את זירת המידע הרפואי כמצב מידעי מורכב. אפתח בהצגה כללית של מונח זה, אסביר מהו הקושי המשפטי שמתעורר, ואצביע על פתרון כללי של המשגה אחודה של הפרטיות כשליטה נמשכת של נושא המידע במידע האישי שעל אודותיו. אמשיך באפיון המידע הרפואי כמצב מידעי מורכב. לשם כך, אמפה את סוגי המידע הרפואי שנאסף ומעובד, ואדגיש שהמידע הרפואי נוצר לא רק "מתחת לפנס", כלומר במערכת הרפואית הממוסדת (מרפאות, קופת חולים, בית חולים, בית מרקחת), אלא גם במעגלים מוארים פחות, כמו אבזורי ספורט, מנועי חיפוש ברשת, ורשתות חברתיות. הדיון יסייע לאתר את האתגרים בנוגע למידע רפואי. **לבסוף**, אסכם.

סוגיות רבות של פרטיות מתעוררות בהקשר הרפואי, שלא אדון בהן כאן: לחולה שמאושפז במסדרון בית החולים יש מעט מאוד פרטיות,⁵ לאדם שמשוחח עם הרוקחת אין פרטיות מספקת מול מי שעומדים אחריו בתור, כאשר צוות רפואי מדבר על אודות מטופל במעלית, אחרים שנמצאים שם נחשפים למידע, כאשר רופאים מעבירים ביניהם מידע רפואי באמצעות יישומונים כמו WhatsApp, או כאשר מותקנות מצלמות (מכוח חוק) במצבים מסוימים,⁶ ועוד. אלה מפגשים שיש להם מענה משפטי וטכנולוגי, גם אם המענה לא תמיד קל ופשוט. יש לשפר את המענה, להטמיע ערכי פרטיות אצל העוסקים במלאכה ולהיעזר במנגנונים טכנולוגיים, למשל עיצוב אדריכלי מתאים של בית המרקחת.

⁵ ראו איתן חי-עם "הייתי הזקנה במסדרון: איתן חי-עם כותב לזכרה של אמו" **הארץ** (9.1.2011), <https://www.haaretz.co.il/news/health/2011-01-09/ty-article/0000017f-e762-da9b-a1ff-ef6fbfd40000>; מבקר המדינה דוח שנתי 2015, 537, 506, 165.

⁶ למשל בבתי חולים גריאטריים, לפי חלק ד'1 לחוק זכויות החולה, התשנ"ו-1996 (להלן: "חוק זכויות החולה").

א. מסגרת הדיון

פרק זה מניח את היסודות לדיון ומתווה את מסגרתו הכללית. **בחלק הראשון** אתאר את רשת הדינים שחולשת על מידע רפואי, שיש לה ציר מרכזי אחד בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות" או "החוק"), לפני ואחרי תיקון 13 לחוק זה.⁷ ציר מרכזי שני נמצא בדיני הבריאות, ועוגנים נוספים פזורים בחקיקה ובכללי אתיקה. **בחלק השני** אציג בקצרה את המסגרת העיונית שפיתחתי במחקרים קודמים, שמתארת את ההצדקות השונות של הזכות לפרטיות כאוסף מעגלים קונצנטריים שמכילים זה את זה. להצדקות השונות יש מכנה משותף, שהוא הבנתה של הפרטיות כשליטה נמשכת של האדם – נושא המידע – במידע האישי שעל אודותיו. למסגרת הזו אוסיף את ההיבטים הייחודיים של מידע רפואי, ואדגיש את החשיבות של הפרטיות ככלי ליצירת אמון לשם טיפול רפואי מיטבי. **החלק השלישי** יזהיר מפני קיצורי דרך ודילוגים משפטיים מהירים מדי, כלומר מפני הכרעה בהתנגשות בין הפרטיות לצרכים ציבוריים. אטען שיש לעצור, לבחון את הפגיעה ולדייקה, ולנסות לאתר פתרונות שהם בבחינת "גם וגם", במקום הכרעה בינארית.

1. רשת הדינים

היבטי הפרטיות במידע רפואי מוסדרים בכמה דינים, ויש לראותם כמכלול: בצד הבסיס החוקתי, יש שני צירים מרכזיים – של דיני הפרטיות ושל דיני הבריאות, ולצידם, עוגנים נוספים.

(א) חוק היסוד

הזכות לפרטיות מעוגנת במפורש בחוק יסוד: כבוד האדם וחירותו. סעיף 7(א) לחוק היסוד קובע: "כל אדם זכאי לפרטיות ולצנעת חייו". המונחים "פרטיות" ו"צנעת חייו" אינם מוגדרים שם או באף דבר חקיקה אחר. הסעיף החוקתי מפרט מצבים נוספים של הפרטיות, שמתייחסים לפרטיות בהקשר של חיפוש ברשות היחיד, בתקשורת, ובגוף האדם: "אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו". אין בחוק היסוד התייחסות מפורשת למידע בריאותי.

בהצעות שונות לעגן את הפרטיות בחוקה ובחוקי יסוד נזכרו בעיקר הבית ותקשורת בין-אישית.⁸ בשנות השמונים של המאה הקודמת נוספה בהצעות השונות התייחסות להגנה מפני חיפוש בגוף האדם,⁹ היבט שנכלל בסופו של דבר בנוסח שנחקק.¹⁰ ההתייחסות לחיפוש בגוף אינה מפתיעה – באותה עת נדונו בבית המשפט העליון מספר מקרים של חיפוש פולשני לשם גילוי סמים, ועלו שאלות בדבר כשרות הראיות: נדונה פרקטיקה של ביצוע חוקן כפוי בעצירים;¹¹ טכניקה של טבילת ידיים לחשיפת עקבות סם;¹² כפייה על עציר לשנות מי מלח, פעולה שגורמת להקאה;¹³ וניתוח חירום שבוצע לאסיר שבלע חבילות סם.¹⁴

כידוע, לחוק היסוד יש תחולה ישירה על רשויות המדינה ותחולה עקיפה על גופים אחרים;¹⁵ יש בו שריון לחקיקה שקדמה לחוק היסוד מפני ביקורת שיפוטית אך לא מפני פרשנות;¹⁶ ויש בו היתר לפגוע בזכויות בתנאים שמנויים בפסקת ההגבלה, במיוחד הצורך בהסמכה מפורשת בחקיקה ראשית ודרישת המידתיות, על

⁷ חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, ס"ח 1430 (להלן: "תיקון 13").

⁸ לסקירה, ראו מיכאל בירנהק **פרטיות חוקתית** 185–189 (2023).

⁹ סעיף 15 להצעת חוק-יסוד: זכויות האדם (12.11.1984) של חברת הכנסת שולמית אלוני; סעיף 9 להצעת חוק יסוד: זכויות היסוד של האדם (1989). בסעיף 6 להצעת חוק יסוד: זכויות האדם והאזרח, ה"ח התשל"ג 448 (12.8.1973) נזכר חיפוש על הגוף.

¹⁰ סעיף 6 להצעת חוק יסוד: כבוד האדם וחירותו, פ/1013/12 (13.11.1991).

¹¹ בג"ץ 355/79 **קטלן נ' שירות בתי הסוהר**, פ"ד לד (3) 294 (1980). הנשיא לנדוי התייחס ל"זכות לפרטיות גופו של אדם" (שם, בעמ' 308), והשוטף ברק ל"זכות יסוד לשלמות גופנית ולשמירת כבודו כאדם" (שם, בעמ' 298).

¹² ע"פ 663/81 **חורי נ' מדינת ישראל**, פ"ד לו (2) 85 (1982).

¹³ ד"נ 9/83 **בית הדין הצבאי לערעורים נ' משה ועקנין**, פ"ד מב (3) 837 (1988).

¹⁴ ע"פ 480/85 **קורטאם נ' מדינת ישראל**, פ"ד מ (3) 673 (1986).

¹⁵ ראו למשל ע"א 9474/03 **יורם גדיש תשתית ובנייה (1992) בע"מ נ' מוסא**, פ"ד סא (3) 603, 624–626 (2006).

¹⁶ סעיף 10 לחוק היסוד ("שמירת דינים"), וראו למשל בג"ץ 5158/21 **גורטלר נ' שר הרווחה**, פס' 36 לפסק-דינו של ממלא מקום הנשיא פוגלמן (נבו 28.12.2023).

מרכיביה.¹⁷ חוק היסוד מנוסח בצורה כללית, כדרך של הוראות חוקתיות, ואת אלה, כמצוות בית המשפט העליון, יש לפרש "במבט רחב", "מתוך תפיסה רחבה, ולא באופן טכני".¹⁸ אין קושי לפרש את המידע הרפואי ככזה שחוסה תחת ההגנה החוקתית.

(ב) חוק הגנת הפרטיות

עשור לפני חוק היסוד, נחקק חוק הגנת הפרטיות, שכלל תחילה אחד עשר מצבים שהוגדרו כ"פגיעה בפרטיות" (בהמשך נוספו עוד מצבים), שעוסקים בסוגיות כמו הטרדה, האזנת סתר, פתיחת מכתב, וחשיפת מידע אישי ופרסומו. החוק נחקק על סמך המלצות ועדת כהן, ושם הייתה רק התייחסות עקיפה ואגבית למידע רפואי.¹⁹ בחוק עצמו יש התייחסות מפורשת למידע רפואי. סעיף 2(11) קובע שפגיעה בפרטיות היא בין היתר "פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד". יש בחוק עוגנים נוספים להגנת המידע הרפואי: הפרת חובת סודיות שנקבעה בדין (סעיף 2(7)) או בהסכם (סעיף 2(8)). היא "פגיעה בפרטיות" – פרסום מידע שהושג באופן פסול גם הוא פגיעה בפרטיות, לפי סעיף 2(10). סעיף 2(9) קובע את עקרון צמידות המטרה – שימוש ב"ידיעה על ענייניו הפרטיים של אדם" למטרה שונה מאשר זו שלשמה נמסר המידע מלכתחילה, הוא פגיעה בפרטיות.²⁰ כל זה, נמצא בפרק א של החוק, שעניינו פרטיות קלסית, כלומר היחסים בין אדם אחד לגורם אחר. הגורם האחר הוא אדם אחר, מעסיק, חברת ביטוח, או המדינה, שהחוק חל עליה במפורש (סעיף 24).

בצד הפרטיות הקלסית, חוק הגנת הפרטיות מסדיר גם את הפרטיות המידעית.²¹ זהו התחום שמכונה בדין האירופי data protection, ובארצות הברית מוכר כ-informational privacy. לידת הענף הזה של הפרטיות בשנות השבעים של המאה הקודמת, והוא הצטרף לדין הישראלי בעקבות המלצות ועדת מומחים ("ועדת גלס").²² בדוח הוועדה הייתה התייחסות מפורשת למידע רפואי. ראשית, כדוגמה למאגרי מידע נזכרו מאגרים של קופות החולים;²³ שנית, הודגשה הוראה בחוק הצרפתי שנסקר שם, שלפיה זכות העיון במידע רפואי תיעשה רק באמצעות רופא שיוסמך לכך.²⁴ הוראה זו אומצה בהצעת הוועדה בישראל בשינוי מסוים: הוצע שבעל שליטה במאגר רשאי לסרב לבקשת עיון של אדם במידע הרפואי שעל אודותיו אם לדעתו המידע עלול לגרום לנזק חמור לבריאות גופנית או נפשית של המבקש. במקרה כזה, המידע יימסר לרופא מטעמו של נושא המידע שביקש לעיין במידע. ההצעה נקלטה בחוק.²⁵

החוק קובע עקרונות בנוגע לאיסוף מידע והשימושים השונים בו. עקרון יסוד אחד הוא ההסכמה, שהיא "הסכמה מדעת" אך יכולה להיות גם משתמעת.²⁶ עקרון שני הוא של צמידות המטרה.²⁷ החוק קובע זכויות

¹⁷ סעיף 8 לחוק היסוד.

¹⁸ בג"ץ 2481/93 דיין נ' וילק, מפקד מחוז ירושלים, פ"ד מח(2) 456, 470 (1994).

¹⁹ דין וחשבון הוועדה להגנה בפני פגיעה בצנעת הפרט 10, 17 (יצחק כהן, יו"ר, 1976), שמפנה לדין בארצות הברית וגרמניה, בהתאמה.

²⁰ המונח "ענייניו הפרטיים של אדם" פורש בפסיקה לעיתים באופן מרחיב (למשל בפסק דינו של השופט בך בע"א 439/88 רשם מאגרי מידע נ' ונטורה, פ"ד מח(3) 808, 821 (1994)), ולעיתים באופן תלוי-הקשר (למשל בג"ץ 844/06 אוניברסיטת חיפה נ' עוז, פ"ד סב(4) 167, 208–209 (2008)).

²¹ להרחבה, ראו מיכאל בירנהק ועמרי רחום-טוויג פרטיות מידעית (2026).

²² דין וחשבון הוועדה למניעת פגיעה באזרח באמצעות מאגרי מידע ממוחשבים (דוד גלס, יו"ר, 1981) (להלן: "דוח ועדת גלס"). להתפתחות הפרטיות המידעית בעולם, ראו בירנהק ורחום-טוויג פרטיות מידעית, שם, בפרק ג, ולהתפתחות הענף בישראל, בפרק ד.

²³ דוח ועדת גלס, שם, בעמ' 7.

²⁴ שם, בעמ' 23.

²⁵ שם, בעמ' 24, 30. ראו סעיף 13(ג) לחוק הגנת הפרטיות. הסדר משלים יש בסעיף 18(ג) לחוק זכויות החולה, התשנ"ו–1996, שמתיר למטפל שלא למסור מידע רפואי למטופל אם יש בכך כדי לסכן את המטופל. במקרה כזה, המטפל צריך לדווח לוועדת האתיקה, שיכולה, לפי סעיף 18(ד) לשנות את ההחלטה. בחוק הגנת הפרטיות אין דיווח כזה, אולם שם לא מדובר במסירת מידע לפני או במהלך טיפול רפואי, אלא בעיון במידע מתוך מאגר מידע, כלומר אחרי שהמידע נאסף. במילים אחרות, בהיבט הזה, חוק זכויות החולה פועל בנקודת זמן מוקדמת יותר מאשר חוק הגנת הפרטיות.

²⁶ סעיפים 1, 3 לחוק.

²⁷ בצד סעיף 2(9) שקובע את העיקרון בהקשר של פרטיות קלסית, סעיף 8(ב) לחוק (אחרי תיקון 13) קובע כי "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין". גם בחובת ההודעה (סעיף 11 לחוק) ובחובת הרישום במקומות המעטים שבהם נותרה על כנה, יש עוגן לעיקרון זה. לדיון, ראו בירנהק ורחום-טוויג, פרטיות מידעית, לעיל ה"ש 21, פרק ח.

לנושאי המידע (זכות עיון וזכות לבקש תיקון), חובות שמוטלות על בעלי השליטה במאגרי המידע (הודעה, סודיות, אבטחת מידע, מינוי ממונה הגנת פרטיות), וקובע הסדרי אכיפה.²⁸ החוק לקה במיקוד-יתר ברישום מאגרי מידע,²⁹ ובמשך שנים רבות עיקר העיסוק, המשאבים והאכיפה של רשם מאגרי המידע היו נתונים לפן הטכני של הרישום במקום בזכויות וחובות מהותיות. החוק קפא על שמריו במשך שנים רבות עד לתיקון 13 שנחקק בשנת 2024, ונכנס לתוקף בשנת 2025.

כבר מראשיתו, כלל פרק ב של החוק הגדרה של מידע, שלפיה "מידע" הוא "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונותיו."³⁰ בשנת 1996 תוקן החוק, ונוספה הגדרת "מידע רגיש", שכללה בין היתר מידע על מצב בריאותי.³¹ פרט לאזכורים אלה, לא היה בחוק הסדר מיוחד בנוגע למידע רפואי, וההסדרים הכלליים חלו גם על מידע כזה. תיקון 13 החליף את הגדרת "מידע" ב"מידע אישי": במקום מבחן מבוסס-תוכן, כלומר התייחסות לסוגי מידע מסוימים, ההגדרה כעת מתבססת על מבחן של זיהוי או האפשרות לזהות את נושא המידע.³² החוק הישראלי צעד כאן בעקבות הדין האירופי.³³ ההגדרה ממחישה – בדרך של הדגמה שאינה ממצה – מהו אמצעי זיהוי, וזה יכול להתייחס למשל למצבו הפיזי והבריאותי של אדם. בנוסף, במקום הגדרת "מידע רגיש", החוק מגדיר כעת "מידע בעל רגישות מיוחדת", וגם כאן צעד במידה רבה בעקבות הדין האירופי. ההגדרה מפרטת שניים עשר סוגי מידע כזה. הפרט השני הוא "מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי כהגדרתו בחוק זכויות החולה, התשנ"ו-1996".³⁴ סוגי מידע נוספים שקרובים למידע הרפואי ונוכחים הם מידע גנטי ומידע ביומטרי, וכן הערכת אישיות ומידע שחלה עליו חובת סודיות שנקבע בדין.³⁵ ההסדר לעניין זכות העיון נשמר. תיקון 13 מזכיר מידע בריאותי בהקשר נוסף – התיקון קבע חובה חדשה למנות ממונה הגנת פרטיות במצבים מסוימים. החוק מציין במפורש בית חולים וקופת חולים כדוגמאות לגופים שחייבים במינוי ממונה.³⁶

(ג) פרטיות בחקיקת הבריאות

הסדר משפטי מרכזי נוסף להגנת הפרטיות במידע רפואי נמצא בחוק זכויות החולה. החוק מפרט את מטרותיו: "לקבוע את זכויות האדם המבקש טיפול רפואי או המקבל טיפול רפואי ולהגן על כבודו ועל פרטיותו." עיקרו של החוק בזכות לטיפול רפואי נאות וללא אפליה,³⁷ ויש בו הוראה כללית, ללא פירוט, שלפיה "מטפל, כל מי שעובד בפיקוחו של המטפל וכן כל עובד אחר של המוסד הרפואי ישמרו על כבודו ועל פרטיותו של המטופל בכל שלבי הטיפול הרפואי" (סעיף 10(א)). מימוש ההוראה נתון למנהלי המוסד הרפואי, כלומר בית חולים או מרפאה (סעיף 10(ב)). בנוסף, סעיף 19(א) קובע חובת סודיות רפואית: "מטפל או עובד מוסד רפואי, ישמרו בסוד כל מידע הנוגע למטופל, שהגיע אליהם תוך כדי מילוי תפקידם או במהלך עבודתם."

החוק קובע גם את החובה לתעד את הטיפול ברשומה רפואית (סעיף 17), ובכך מחייב הקמה של מאגר מידע על המטופלים. מסירת המידע לגורם אחר אסורה (סעיף 20(א)), אלא לפי שבעה חריגים שמנויים בחוק: הסכמת המטופל, חובה בדין, מסירה לשם המשך הטיפול, החלטה של ועדת אתיקה של משרד הבריאות לאפשר מסירה של המידע לגורם אחר אם יש חשש שמסירת המידע למטופל תזיק לו,³⁸ או כאשר מסירת המידע לגורם אחר

²⁸ לדיון, ראו בירנהק ורחום-טוויג, **פרטיות מידעית**, שם, פרק ט (זכויות), פרקים י-יב (חובות), פרק יג (אכיפה).

²⁹ בירנהק ורחום-טוויג, **פרטיות מידעית**, שם, בעמ' 74, 86-87, 92, 99.

³⁰ ההדגשה הוספה. סעיף 7 לחוק הגנת הפרטיות. לאחר תיקון 13 לחוק ההגדרות נמצאות בסעיף 3.

³¹ סעיף 3 לחוק הגנת הפרטיות (תיקון מס' 4) (מאגרי מידע), התשנ"ו-1996, שהוסיף את ההגדרה לסעיף 7 בחוק בנוסחו דאז.

³² סעיף 3 מגדיר מידע אישי: "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי..."

³³ ראו סעיף 4(1) לרגולציה הגנת המידע האיחוד האירופי (הגדרת personal data). הרגולציה ידועה כ-GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC ("GDPR"). (להלן "GDPR"). 2016 O.J. (L 119) 1.

³⁴ סעיף 3 לחוק המתוקן, הגדרת "מידע בעל רגישות מיוחדת", פרט 2.

³⁵ שם, פרטים 3, 4, 8, 11, בהתאמה.

³⁶ סעיף 17(א)(4) לחוק.

³⁷ סעיפים 3-5 לחוק זכויות החולה.

³⁸ סעיף 18 לחוק זכויות החולה. הסדר זה דומה למגבלה שיש בחוק הגנת הפרטיות שנוכחה לעיל.

חיונית להגנה על בריאות הזולת, כאשר מסירת המידע היא למוסד המטפל לשם עיבוד המידע, תיקו או דיווח לפי דין, ולבסוף, מסירת המידע נועדה להוראה, מחקר או פרסום מדעי – "ובלבד שלא נחשפו פרטים מזהים של המטופל". כל זה, צריך להיעשות באופן מידתי (סעיף 20(ב)). אשוב לכך בפרק ד להלן. פקודת הראיות משלימה, וקובעת חיסיון על מידע רפואי (לטובת המטופל), כלומר לרופא אסור למסור מידע על מטופל כאשר "הוא מן הדברים שלפי טיבם נמסרים לרופא בדרך כלל מתוך אמון שישמרם בסוד".³⁹ המטופל עצמו יכול לוותר על החיסיון שלו.

הסדרי חוק זכויות החולה בקשר למידע רפואי תואמים להסדרי חוק הגנת הפרטיות ומצטרפים אליהם.⁴⁰ יש בהם הסמכה לאיסוף המידע, קביעת זכות עיון במידע במגבלות דומות לאלה שבחוק הגנת הפרטיות, הגבלת שימושים במידע, ומגבלות בקשר למסירתו. אנחנו רואים כאן את ההתממה בנוגע למחקר מדעי.

הסדרים משפטיים נוספים מתייחסים למידע בריאותי. פקודת בריאות העם, 1940 שהיא פקודה מנדטורית במקורה אבל כיום רובה מורכב מתיקוני חוק ישראליים, מסדירה היבטים שונים של בריאות הציבור, כמו שירות סניטרי ובתי עלמין. אבל יש שם גם הסדרים שעניינם מידע: חובת דיווח במקרה של "ציאה או הוצאה של עובר או ולד מת מרחם אמו" (סעיף 4 לפקודה), וחובת דיווח על מחלה מדבקת (סעיף 12). מכוח סעיף זה, מוסדות רפואיים מזווחים למשרד הבריאות על אנשים שנושאים את נגיף ה-HIV, ומכוחו נקבעה חובת הודעה בנוגע להידבקות בנגיף הקורונה. בפקודה יש הסדר שנחקק בשנת 2024 בקשר להקמת מאגר חיסונים לאומי, שמטרתו מוגדרת במפורש – לשם טיפול באדם, כדי לעודד אדם להתחסן, ובשימוש במידע לא מזהה, לשם מעקב אחרי הכיסוי החיסוני באוכלוסייה.⁴¹

לאחרונה נחקק חוק ניוד מידע רפואי, התשפ"ד–2024, שקובע את זכותו של אדם לבקש את העברת המידע הרפואי שעל אודותיו מגורם מטפל אחד לאחר, למשל לשם מעבר בין קופות חולים. החוק נכנס לפעולה בהדרגה, במהלך שלוש שנים מחקיקתו. המידע יועבר רק לפי הסכמת המטופל (סעיף 14), שיכול לחזור בו מהסכמתו (סעיף 16). חוק זה מצטרף לחוק הגנת הפרטיות ולחוק זכויות החולה ואינו גורע מהם (סעיף 26). הזכות לניוד מידע אישי קיימת כזכות כללית בדין האירופי,⁴² אבל נפקדת מהדין הישראלי למעט המופע החשוב הזה, בהקשר הרפואי. המטרה היא להקל על מטופלים לעבור ממטפל אחד לאחר וכך להגביר את התחרותיות בין ספקי השירות השונים. ההסדר ממוקם בדיני הפרטיות והבריאות, ולא דווקא בדיני התחרות בשל תוכן המידע שבו מדובר ומשום שהפקדת השליטה במידע בידי נושא המידע היא אבן יסוד של דיני הפרטיות המידעית.

חקיקה נוספת עוסקת במידע רפואי בהקשרים ספציפיים. למשל החוק לפיצוי נפגעי גזזת, התשנ"ד–1994 מחייב איסוף מידע לשם הפעלתו; החוק לגילוי נגיפי איידס בקטינים, התשנ"ו–1996 קובע הסדרים כעולה משמו, וקובע בין היתר חובת סודיות (סעיף 3); חוק הפסיכולוגים, התשל"ז–1977 קובע חובת סודיות. זו אינה רשימה ממצה.

בנוסף, יש הוראות דין במדרג נורמטיבי נמוך יותר. אזכיר את ההסדר שנקבע לפי פרק ד לחוק הגנת הפרטיות, שעוסק בהעברת מידע מגופים ציבוריים וקובע איסור כללי על העברה כזו (סעיף 23 לחוק), ובצידו חריגים. ההסדר חל על גופים ציבוריים, שהם משרדי ממשלה, רשויות מקומיות וגופים סטטוטוריים אחרים (סעיף 23). החוק מסמך את שר המשפטים לקבוע גופים נוספים שייחשבו לגוף ציבורי למטרה הזו, תוך הגדרה פרטנית של סוגי המידע שמותר להם למסור ולקבל. צו כזה הוצא, וכולל בין היתר גופי בריאות: לבית חולים מותר לקבל מידע על מצב בריאותו של אדם, פרטים אישיים כמו תאריך לידה, ארץ לידה ותאריך פטירה, ולבית חולים אוניברסיטאי מותר לקבל מידע נוסף לצורכי מחקר; קופת חולים יכולה לקבל מידע דומה, וכן מידע מהמוסד לביטוח לאומי על תאונות דרכים, ניצולי שואה ומידע נוסף שלפיו המבוטח זכאי להטבות.⁴³

³⁹ סעיף 49 לפקודת הראיות [נוסח חדש], התשל"א–1971. להרחבה, ראו יצחק עמית **חסינות ואינטרסים מוגנים: הליכי גילוי ועיון במשפט האזרחי והפילי** 639 (2021).

⁴⁰ בשני החוקים יש סעיף שמירת דינים, סעיף 29 לחוק זכויות החולה קובע שהוראותיו אינן גורעות מהוראות כל דין, וסעיף 35 לחוק הגנת הפרטיות קובע הוראה זהה שם.

⁴¹ סעיף 1ב65 לפקודת בריאות העם, 1940. הגבלת המטרות קבועה בסעיף 1ב65(ג).

⁴² סעיף 20 ל-GDPR.

⁴³ צו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו–1986.

אסיים בנהלים של מערכת הבריאות, שמופצים בדרך של חוזרי מנכ"ל משרד הבריאות. נהלים כאלה תקפים רק אם יש להם עוגן מסמך מספק, לפי עקרון חוקיות המנהל כאשר הנהלים פוגעים בזכות יסוד – פרטיות במקרה שדון כאן – ההסמכה צריכה להיות מפורשת דיה, לפי דרישת פסקת ההגבלה שבחוק היסוד.⁴⁴ נראה שלא תמיד הנהלים עומדים בדרישות.⁴⁵ במהלך הדברים אזכיר נהלים נוספים, לפי העניין.

בחקיקת הבריאות אפשר לזהות כמה עקרונות יסוד בנוגע למידע: החקיקה מבקשת, לפחות בהצהרותיה, להגן על פרטיות המטופלים ומפקידה בידיהם את השליטה במידע בדרך של מתן הסכמה מתאימה. החריגים להסכמה בודדים ומתוחמים למצבים שמוגדרים בחוק. בחקיקה יש שאיפה למידתיות, כלומר לצמצום הפגיעה בפרטיות למינימום הנדרש. שיקולים ציבוריים לא נעלמו מעיני המחוקק, למשל הצורך באיסוף מידע מצרפי לשם זיהוי מגיפות, קבלת תמונה כללית אודות חיסונים, או העברת מידע מותמם למטרות הוראה ומחקר.

כאמור, החוק מתיר העברת מידע מותמם לצורך מחקר, הוראה או פרסום מדעי. אין בחקיקה הראשית בישראל התייחסות לשימושים במידע רפואי לצורך עיבוד בדרך של נתוני עתק או בינה מלאכותית. ההיעדר אינו מקרי. הוא משקף גישה של חקיקה ניטרלית-טכנולוגית,⁴⁶ שהרי חוק שינקוב במפורש בטכנולוגיה מסוימת, צפוי להתיישן במהירות. ניסוח החקיקה ברמת הפשטה מעט יותר גבוהה מאפשר גמישות והכלה של מצבים טכנולוגיים חדשים, אם כי מחירו של הניסוח הכללי בציוד – יצירת עמימות משפטית. הנושא מוסדר ברובד של חקיקת משנה, בדרך של נהלים של משרד הבריאות. כמו כן, אין בחוק הישראלי חריג כללי לצורכי מחקר. בכך הוא שונה מהדין האירופי, שבו נמצא התייחסות מפורשת להתנגשות בין הזכות לפרטיות במידע עם אינטרסים ציבוריים, אך גם בדין האירופי אין העדפה מוחלטת של האינטרסים הציבוריים, אלא מסגרת לאיזון השיקולים היריבים.⁴⁷

(ד) חוזים

בצד הצירים המרכזיים של דיני הפרטיות ודיני הבריאות, נתח לא מבוטל של הפעילות הרפואית מתבצע במסגרת משפטית חוזית. למשל, כאשר מטופל מקבל טיפול במרפאה פרטית – חוק הגנת הפרטיות חל, דיני הבריאות יחולו אם המרפאה הפרטית באה בגדר ההגדרות בדינים המתאימים, ודיני החוזים ממלאים את התווך. בחוזים נקבע מה מותר ומה אסור, במפורש או במשתמע. למשל, מכוני אסתטיקה מצלמים תמונות של "לפני" ו"אחרי"; אסור להם להשתמש בתמונות למטרות אחרות כמו שיווק, אלא אם המצולם הסכים, הסכמה מדעת ומרצון חופשי, לפני השימוש.⁴⁸ דיני הפרטיות מצטרפים כאן. כאשר חובת סודיות בקשר לענייני הפרטיות של אדם

⁴⁴ לעניין מידת המפורשות, ראו למשל בג"ץ 6824/07 מנאע נ' רשות המסים, פ"ד סד(2) 479, 498-499 (2010).

⁴⁵ למשל חוזר משרד הבריאות 9/2024 ("אמות מידה לצילום בחדרי טראומה וטיפול נמרץ במחלקה לרפואה דחופה") שמבקש להחזיר צילום בחדרי טראומה, בתנאים מסוימים. על פניו, נראה שאין הסמכה מספקת לפעולה כזו, שיש בה פגיעה קשה בפרטיות המטופלים, שממילא, במצבים שבהם הם מגיעים לחדרי טראומה, אינם יכולים לקבל החלטה כלשהי בעניין. נוהל זה סוטה גם מהוראת סעיף 10(א) לחוק זכויות החולה, שלפיו יש לשמור על פרטיות המטופל בכל שלבי הטיפול הרפואי.

⁴⁶ פעמים רבות, גם כאשר חקיקה מבקשת לשמור על ניטרליות כזו, יש בה הנחות סמויות על הטכנולוגיה. לדיון, ראו Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J. L. & TECH. 24 (2012). כך למשל, חוק האזנת סתר מתייחס ל"שיחה", ומבקש להרחיב, אבל הוא מניח שיחה סינכרונית בין שני אנשים שמתנהלת באמצעות קו טלפון קווי, בבעלות חברה ממשלתית. לעומת זאת, שיחה בקבוצת ווטסאפ שונה משיחה כזו בכל ההיבטים האלה. לדיון בפרטיות בשיחות בין-אישיות, ראו מיכאל בירנהק ונועה דיאמונד "מהממ"ד לארכיון: פרטיות בתייעוד מלחמה" **מעשי משפט** יז (יתפרסם ב-2026).

⁴⁷ סעיף 1(89) ל-GDPR קובע כך:

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

למדיניות החברות באיחוד יש היתר לקבוע חריגים נוספים לעניין מימוש זכויות מסוימות לפי הרגולציה, לפי סעיף 1(89).

⁴⁸ שימוש לא מורשה בתמונות למטרות שיווק עשוי לפגוע בפרטיות לפי סעיף 4(2) לחוק (פרסום צילום משפיל), לפי סעיף 6(2) (שימוש בדמותו של אדם למטרות רווח; יש לבחון האם האדם מזהה או ניתן לזיהוי בתמונה), לפי סעיף 9(2) (עקרון צמידות המטרה), ולפי הנסיבות – הפרת חוזה לפי סעיף 8(2). בנוסף, עשויות לחול הגנות לפי הנסיבות. ראו למשל ת"א (שלום רח') 18326-05-18 **פלונית נ' שורץ** (נבו 30.9.2021).

נקבעה בהסכם, היא מוגנת הן בדיני החוזים והן בדיני הפרטיות. הפרת החובה היא פגיעה בפרטיות הקלסית לפי סעיף 8(2) לחוק הגנת הפרטיות.

(ה) אתיקה

אשלים בכללי אתיקה. הזכרתי את שבועת הרופאים. עוד ביוון העתיקה נכלל בנוסח של שבועת היפוקרטס המרכיב של הסודיות: "כל אשר אראה או אשמע [בנוגע ל]חיי המטופלים, בקשר לשירות המקצועי או מחוצה לו, ושלא נועד לפרסום, אשמור בסודיות, ואתייחס לדברים כפרטיים".⁴⁹ נוסח שבועת הרופא העברי, שחיבר פרופסור ליפמן היילפרין בשנת 1952 קובע בין היתר: "שמרו אמונים לאדם שהאמין בכם אל תגלו סודו ואל תלכו רכיל."⁵⁰ ההסתדרות הרפואית (הר"י) מציינת את האוטונומיה של המטופל כערך האתי הראשון שלה, שכולל גם את הפרטיות והסודיות הרפואית.⁵¹ הר"י פורטת את הערך הזה להנחיות קונקרטיים, למשל בבדיקת אזורים אינטימיים, פנייה לעובר אורח שמאובחן בו חולי, השתתפות סטודנטים בבדיקה, הופעות בתקשורת, והתייחסות להעברת מידע בדבר שימוש בתרופות לחברות מסחריות.⁵²

הפרת כללי אתיקה עלולה להביא לסנקציות במישור המשמעותי במקומות עבודה – פקודת הרופאים מסמיכה את שר הבריאות להתלות או לבטל רישיון של רופא אם "נהג בדרך שאינה הולמת רופא מורשה",⁵³ אם כי לא נמצאו החלטות שהתבססו על פגיעה בפרטיות לגבי עילה זו.

מעבר להעלאת המודעות והפנמת כבוד המטופלים אצל המטפלים, נראה שעיקר פועלם של כללי האתיקה הוא דווקא במישור המשפטי, בכך שהם יוצרים ציפייה לפרטיות. לכן, גם אם אין חוזה מפורש שמתייחס לפרטיות ולסודיות ביחסי המטופל והמטפל, אפשר לומר בבטחה שיש חוזה משתמע כזה. הפרת חובת הסודיות, כפי שראינו, היא פגיעה בפרטיות לפי סעיפים 7(2) ו-8(2) לחוק הגנת הפרטיות. בנוגע למחקר רפואי, כללי האתיקה מעוגנים ככלל משפטי: מחקר רפואי בבני אדם מחייב אישור של ועדת הלסינקי. נוסח הצהרת הלסינקי משנת 1964 כולל התייחסות מפורשת לפרטיות, אם כי ללא פירוט.⁵⁴

2. שליטה נמשכת במידע

ברשת הדינים שראינו זה עתה יש כמה עקרונות יסוד ולא מעט ביטויים חקיקתיים עמומים, למשל, המונח "ענייני הפרטיים של אדם" והיעדר ההגדרה של "פרטיות". התוצאה היא שחלק מהסדרי החוק מנוסחים בדרך של סטנדרטים רחבים ובלשון ניטרלית לטכנולוגיה להבדיל מכללים מדויקים תלויי-טכנולוגיה. אופן החקיקה הזה מאפשר גמישות והתאמה לנסיבות משתנות, אבל המחיר הוא עמימות משפטית. דרך אחת להפיג את העמימות במידת מה, היא פרשנות תכליתית של החקיקה הרלוונטית, כמקובל במשפט הישראלי.⁵⁵

מהי, אם כן, תכליתה של ההגנה על הזכות לפרטיות? במהלך הדברים עד כה פגשנו את הפרטיות הקלסית (אדם מול הזולת) ואת הפרטיות המידעית (נושא מידע מול בעל השליטה במידע), וגם מופעים של פרטיות חוקתית (אזרח מול המדינה, למשל בנוגע לחיפוש משטרתי או מעקב השב"כ במגפת הקורונה). האם יש הצדקה אחת לכל מישורי הפעולה האלה? מהי?

⁴⁹ ראו את הנוסח באנגלית כאן: <https://www.congress.gov/117/meeting/house/114995/documents/HHRG-117-IF02-20220719-SD007.pdf>. התרגום שלי, מ' ב'.

⁵⁰ שבועת הרופא העברי, אתר ההסתדרות הרפואית בישראל <https://www.ima.org.il/Main/ViewContent.aspx?CategoryId=1125>.

⁵¹ הלשכה לאתיקה, ההסתדרות הרפואית בישראל **אתיקה רפואית: כללים וניירות עמדה** 22 (תמי קרני עורכת, 2023).

⁵² שם, בעמ' 51, 207.

⁵³ סעיף 1(41) לפקודת הרופאים [נוסח חדש], התשל"ז-1976.

⁵⁴ ראו World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants. סעיף 24 שם קובע: "Every precaution must be taken to protect the privacy of research participants and the confidentiality of their personal information". <https://www.wma.net/policies-post/wma-declaration-of-helsinki/>.

⁵⁵ לפרשנות תכליתית, ראו אהרן ברק **פרשנות תכליתית במשפט** (2003).

בספרות יש הצדקות רבות מני-ים לפרטיות, שכל אחת מדגישה פן אחר שלה. יש הצדקות שתולות את הפרטיות במושגי יסוד אחרים כמו אוטונומיה וכבוד האדם. יש לה פן מכשירני, בכך שהיא מסייעת למימוש זכויות אחרות, כמו חופש הביטוי (האנונימיות) או שהיא מגנה על אדם מפני אפליה.⁵⁶ יש הצדקות שפונות אל מחוץ לעולם המשפט ומצביעות על צרכים פסיכולוגיים וחברתיים של בני אדם. לא זה המקום לבחון את ההצדקות, ולצורך הדיון, אסתמך על מסקנותיי מדיונים קודמים.⁵⁷ אציג את עיקר ההצדקות ואת יישומן בנוגע למידע רפואי, ולאחר מכן, את המכנה המשותף שלהן – פרטיות כשליטה.

(א) מעגלי ההצדקות

ניתן לארגן את הצדקות הפרטיות כאוסף מעגלים קונצנטריים, שכל אחד מכיל את קודמו. בליבה, במעגל הפנימי ביותר, נמצא האדם. במובן הזה, הפרטיות היא זכות ליברלית ביסודה, אולם אין לטעות בה: פרטיות היא תמיד מול משהו אחר או משהו אחר. לאדם שנמצא בבדידות מלאה באי נטוש יש פרטיות בפועל.⁵⁸ במעגל האדם יש הצדקות שמדגישות את הצורך הפסיכולוגי במקום שקט, "מאחורי הקלעים" כביטוי של הסוציולוג ארווין גופמן (Goffman).⁵⁹ המרחב הפרטי יכול להיות פיזי, נפשי, אינטלקטואלי, או וירטואלי, שבו אין מציקים לאדם, אין דורשים ממנו הסברים, לא עוקבים אחריו, ומניחים לו לנפשו. הפרטיות מאפשרת חירות. הפרטיות היא גם מגן מפני מבט פן-אופטי, כזה שמבקש להשיג כוח ושליטה באדם הנצפה רק מעצם קיומו של המבט הממשמע, וכל זה לפי פרשנותו של מי של פוקו את ההצעה של ג'רמי בנתי'האם לכלא שבו סוהרים שולטים באסירים בעיקר בכוח המבט.⁶⁰ הפרטיות במעגל זה מאפשרת לאדם למנוע את הוצאתו מהקשר ואת רידודו לפרט אחד.⁶¹

מעגל שני מתמקד בקשרים בין-אישיים. אלה יכולים להיות קשרים אינטימיים, כמו בין בני זוג או ביחידה משפחתית, או קשרים מקצועיים, כמו אלה שבין לקוח לעורכת הדין ובין מטופל לרופאה או גורם מטפל אחר. לפרטיות יש תפקיד מכשירני. היא מאפשרת לצדדים לקשר לנהוג כיחידה אחת, וכלפי חוץ ייהנו מפרטיות. כל עוד ירצו בכך, הזוגיות, התא המשפחתי והיחסים המקצועיים יהיו סגורים מפני שאר העולם. גם פה, ההסכמה היא מרכיב משמעותי. מי שמבקשים לפתוח לרווחה את היחסים המשפחתיים בשיחות עם חברים, ברשת החברתית או בתקשורת – זכאים לעשות זאת. מעגל זה אינו עומד בפני עצמו. ההמשגה של הצדקות הפרטיות כמעגלים שמכילים זה את זה פועלת כאן: מעגל הקשרים הבין-אישיים מכיל את מעגל האדם. לכן, לכל אחד מהיחידים בתוך היחידה הזוגית או המשפחתית, עדיין יש פרטיות מול האחרים בתוך היחידה הזו.⁶²

הפרטיות במעגל הקשרים הבין-אישיים חשובה משום שהיא יוצרת תנאי רקע נוחים לקשרים משמעותיים. פרטיות אינה תנאי מספיק ליצירת קשרים מיטביים – לשם כך צריך רצון של האנשים בנסיבות היחסים ביניהם, אבל כל עוד הצדדים לא ויתרו על הפרטיות, זהו תנאי הכרחי. ביחסים אינטימיים, הפרטיות מאפשרת יצירת ביטחון, אינטימיות ואמון.⁶³

גם ביחסים הבין-אישיים המקצועיים, ובמיוחד בהקשר הרפואי, האמון מרכזי.⁶⁴ היחסים הם מכשירניים. מצד המטופל – לשם קבלת טיפול רפואי מיטבי, ומצד המטפלת – זו עבודתה ושליחותה, לתת טיפול מיטבי. הפרטיות

⁵⁶ ראו בירנהק, **פרטיות חוקתית**, לעיל ה"ש 8, בעמ' 83–85.

⁵⁷ בירנהק, **פרטיות חוקתית**, שם, בעמ' 68–86.

⁵⁸ בשנים האחרונות יש מחברים שמדגישים את ההיבט היחסני (relational) של הזכות לפרטיות. ראו למשל, Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance*, 131 YALE L. J. 573, 593 (2021). לטעמי, ההיבט היחסני תמיד היה שם. ראו גם Ian Kerr, *Schrödinger's Robot: Privacy in Uncertain States*, 20 THEORETICAL INQ. L. 123, 129–132 (2019).

⁵⁹ ERVIN GOFFMAN, *THE PRESENTATION OF SELF IN EVERYDAY LIFE* 112 (1952).

⁶⁰ מישל פוקו **לפקח ולהעניש הולדת בית הסוהר** (1975; דניאלה יואל מתרגמת, 2015).

⁶¹ ראו JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* (2001).

⁶² במקרה שבו בני זוג נשואים היו בהליכי פרידה, הכיר בית המשפט בזכותה של האישה למנוע מבעלה להיכנס לביתה (שהיה בבעלות משותפת) ולצלם אותה כאשר הייתה במצב אינטימי עם גבר אחר. בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האיזורי בנתניה**, פ"ד סא(1) 581 (2006).

⁶³ ראו JEAN L. COHEN, *REGULATING INTIMACY: A NEW LEGAL PARADIGM* 3 (2002), שכתבה "Privacy is an enabling condition of intimacy".

⁶⁴ המשפטן האמריקני ארי ולדמן היטיב לתמצת את הטענה: "Information disclosed in contexts defined by trust should be legally protected as private". ראו ARI EZRA WALDMAN, *PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE*, 20–21 (2018). ראו גם Anita L. Allen, *Compliance-Limited Health Privacy Laws*, in SOCIAL.

של הבדיקה והטיפול במרפאה, בחדר הטראומה, בחדר הניתוח ובאשפוז חשובה משום שהיא מאפשרת למטופל לשאת פעולה, לטובתו שלו. זה האינטרס שלו, כמובן, אבל יש כמה חסמים. חסם ראשון הוא בוש. למרבה הצער, יש לא מעט מצבים רפואיים שיש לגביהם סטיגמה חברתית שלילית. מחלות נפש, מחלות מין, בעיה רפואית באיברים אינטימיים, מגבלות קוגניטיביות, בעיות אסתטיות מסוימות, או מחלות שמזוהות עם מעמדות בשולי החברה. מטופל עלול להתבייש מחשיפת המידע או מחשיפת גופו, ולא לספר לרופאה את כל המידע שדרוש לטיפול. הטיפול יהיה חלקי וחסר. חסם שני, הוא שלעיתים למטופל יש אינטרס אחר שמביא אותו להעדיף סודיות של המידע הרפואי. למשל, מחלות או תופעות שנחשבות לתורשתיות – אם ייודעו, עלולות לפגוע בסיכויי השידוך של ילדיו בחברות מסוימות, בסיכוי לקבל עבודה, או ביחס חברתי חיובי בכלל. בסטיגמה, בבושה ובמגבלות חברתיות כאלה יש להיאבק. אבל האמצעי לכך אינו ביטול הפרטיות בהקשר הרפואי. חסם שלישי, שעליו עמדה הפילוסופית אניטה אלן (Allen) הוא צורך של המטופל עצמו במרחב, גם מול הרופאה, כדי להתמודד עם מצוקה שמתעוררת בעקבות קיומה של מחלה.⁶⁵

גם כאן, הצדקת הפרטיות במעגל היחסים הבין-אישיים כגורם יוצר-אמון שמסייע לשיפור הטיפול, מצטרפת להצדקות שבמעגל האדם. הפרטיות במעגל היחסים המקצועי מבהירה שהמידע הוא של המטופל, לא של המטפל ולא של אף גורם אחר. אין לטעות בפרשנות הביטוי "שלי": אין מדובר במידע קנייני שניתן לסחור בו, אלא במידע פרטי.⁶⁶ המטופל הוא שיחליט – כביטוי למימוש האוטונומיה והרצון החופשי שלו, האם לחשוף את המידע, למי, ואיך. גם ההסדר שבפקודת הראיות פועל באופן דומה: החיסיון הוא של המטופל, והרופא אינו רשאי למסור מידע רפואי אלא בהסכמת המטופל.⁶⁷ תפקידו של המשפט בהגנת הפרטיות הוא ביצירת תנאים נוחים לשיתוף המידע בין המטופל למטפל, תוך הבטחה בדבר סודיותו. במילים אחרות, הפרטיות חיונית ליצירת מסגרת טיפולית מיטבית באופן שמשמר את האוטונומיה של הפרט ואת כבוד האדם של המטופל. גם בית המשפט העליון הכיר בכך, למשל: "מובן מאליו כי מצבו הרפואי של אדם ועובדות הקשורות לגופו, לתחלואיו או למכאוביו, מצויים בליבת אותו מתחם בו ראוי להניח לו לנהל את חייו ללא מעורבות הזולת".⁶⁸

כל זה אמור בבדיקה ובטיפול ממש. ההצדקות חלות גם בנוגע למידע על הטיפול, שהוא הייצוג הבירוקרטי של הטיפול הרפואי. הרשומה הרפואית שסעיף 17 לחוק זכויות החולה מחייב, מייצגת את הבדיקה, את הממצאים, ואת הטיפול המוצע. הרשומה הכרחית לשם המשך הטיפול והמעקב הרפואי ומאפשרת גם את נידוד המידע, כלומר את החלפת הגורם המטפל. המידע הרפואי שנכלל ברישום עשוי להיות מצומצם יותר ממה שקרה במרפאה ובחדר הניתוח. למשל, הרופאים והמנתחים רואים איברים מוצנעים, אבל לא יצינו זאת ברשומה, אלא אם יש ממצא רפואי רלוונטי. המידע שמצטבר עשיר, רחב, וכיום – ובישראל כבר כמה עשורים – המידע דיגיטלי. קל לצבור מידע דיגיטלי, להעבירו ממקום למקום, להצליבו עם סוגי מידע אחרים, לעבד אותו, ולהפיק ממנו תובנות נוספות. התובנות האלה מתייחסות למידע על המידע, meta-data. למשל, רשומה רפואית מתעדת את תוכן התלונה של המטופל, את האבחון והטיפול, ובנוסף, מידע על התוכן, כמו מועד הפניה, תדירות פניות קודמות, השוואה למידע נוסף כמו ביקורים אצל רופאים אחרים. אלה אינם בהכרח חלק מהרשומה עצמה, אבל עשוי להיות להם ערך מחקרי וטיפולי.

המעגל הבא של הצדקות הפרטיות הוא מעגל הקהילה, ושם הפרטיות ממלאת תפקיד חשוב ביצירת המרקם הקהילתי, בכך שהיא מבטיחה את "הלחוד" לצד "הביחד".⁶⁹ מעגל זה פחות רלוונטי לדיון הנוכחי. המעגל האחרון הוא מעגל המדינה, שם ניצב האזרח (או התושב, וגם העובד הזר, התייר והפליט) מול המדינה רבת-הכוח. הפרטיות כזכות יסוד ממלאת תפקיד במערך האיזונים והבלמים החוקתי, מגבילה את כוחה של המדינה, יוצרת מרחב פרטי, שמותר לפרוץ אותו רק בהתקיים התנאים המחמירים שיש בפסקת ההגבלה שבחוק היסוד.

DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 261, 266 (Beate Roessler & Dorota Mokrosinska eds., 2015); וכן (2015) NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE, 147.

ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY 118 ⁶⁵ (2003).

⁶⁶ כדבריו הקולעים של פילוסוף הטכנולוגיה לוציאנו פלורדי: "My" as in "my information" is not the same as "my" as in "my car" but rather the same as "my" as in "my body" or "my feelings" Luciano Floridi, *Four Challenges for a Theory of Informational Privacy*, 8(3) ETHICS & INFO. TECH. 109 (2006).

⁶⁷ ראו לעיל ה"ש 39.

⁶⁸ רע"א 7828/17 הסתדרות מדיצינית הדסה נ' פלוגי, פס" 13 לפסק דינה של השופטת וילנר (נבו 9.1.2018).

⁶⁹ להרחבה, או בירנהק, פרטיות חוקתית, לעיל ה"ש 8, בעמ' 78.

(ב) פרטיות כשליטה

בספרות המחקרית לאורך השנים היו ניסיונות להגדיר את הפרטיות, להעמידה על בסיס כולל אחד או לאתר הצדקה שיכולה להסביר מדוע יש לנו פרטיות מול אדם אחר, מול תאגידים ומול המדינה, בקשר למידע רפואי ופיננסי אבל גם ביחס למידע טריוויאלי.⁷⁰ הניסיונות האלה לא עלו יפה. כפי שהמשפטן האמריקני דניאל סולוב (Solove) העיר בעבר, ההגדרות שהוצעו היו הגדרות-יתר או הגדרות-חסר.⁷¹ בהתבססו על הפילוסופיה של ויטגנשטיין, סולוב הציע להתייחס לפרטיות כאוסף מושגים נפרדים שיש ביניהם "דמיון משפחתי", ובמקום הגדרה, הציע טקסונומיה של פרטיות, שיש בה כמה קטגוריות ובכל אחת כמה מצבי משנה.⁷² המהלך של סולוב מועיל לפיצוח מהותה של הפרטיות ואופני פעולתה, אבל היה מעט מהיר מדי. אכן, קשה לאתר הצדקה אחת לפרטיות על כל מופעה, אבל הקשר בין המופעים השונים יותר חזק מאשר אוסף המצבים שתיאר בטקסונומיה שלו. אסביר.

כפי שתיארתי במקומות אחרים, אני סבור שאין צורך לבחור בהצדקה אחת בלבד לפרטיות.⁷³ יש כמה הסברים שמצדיקים את קיומה של הזכות. במקרים רבים ההצדקות יכולות לדור בכפיפה אחת, ורק לעיתים הן יתנגשו, ואז יהיה צריך לבחור מביניהן את ההצדקה המשכנעת ביותר.⁷⁴ עם זאת, קיומן של מספר הצדקות אינו רק אוסף אקלקטי אקראי. בין ההצדקות יש מדרג מסוים שבא לידי ביטוי במעגלים הקונצנטריים, ההצדקות מכילות זו את זו ומאפשרות לנו לדייק אותן, את תחומי הפעולה וההתפרשות שלהן במישורי פעולה שונים. הצדקות שייחודיות למעגל המדינה (למשל הגנה מפני כוחה העודף של המדינה או היותה אמצעי למימוש זכויות אחרות) אינן רלוונטיות ליחסים בין שכנים שמרפסותיהם פונות זו לזו במרחק ישראלי-עירוני מצוי של שישה מטר. לעומת זאת, ההצדקות במעגל היחיד מוכלות בצורך של אנשים לפרטיות גם מול המדינה.

בהמשך לסולוב, אני סבור שלהצדקות המגוונות לפרטיות יש מכנה משותף: הפרטיות כשליטה. זו אינה הצדקת-על אחת שמכילה את כל הקודמות, אלא תיאור שמתאים לכל ההצדקות. במונחים של ויטגנשטיין ושל סולוב, "הפרטיות כשליטה" היא שם המשפחה של מופעה המגוונים של הפרטיות. במעגל היחיד – כאשר אדם שולט במידע האישי שלו, הוא מממש את האוטונומיה ואת כבוד האדם הסגולי שלו. האדם אדון לעצמו, ואין מישהו אחר ששולט בו. כאשר יש לנו מרחב פרטי – פיזי, נפשי, אינטלקטואלי ווירטואלי – אנחנו שולטים באותו מרחב, ושולטים בעצמנו. במעגל הקשרים הבין-אישיים, כאשר לבני הזוג או לצדדים ביחסים המקצועיים, ובכלל זה בהקשר הרפואי, יש שליטה בנעשה ביחסים ביניהם, הם יכולים לנסות לממש את האמון שדרוש לטיפול מיטבי.

את ההגדרה לפרטיות כשליטה הציע המשפטן האמריקני אלן וסטין (Westin) לפני כמעט שישים שנה: "The claims of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".⁷⁵ וסטין התייחס לפרטיות מול תאגידים, ועל רקע הדין האמריקני באותה עת, אבל ההגדרה ניתנת להרחבה ועדכון. הרחבה – הפרטיות כשליטה מתאימה לא רק לפרטיות המידעית, אלא גם ליחסים בין אדם לזולת (פרטיות קלסית) וליחסים בין אזרחים למדינה (פרטיות חוקתית). כפי שהראתה החוקרת הקנדית ליסה אוסטין (Austin), החשיבות אינה רק השליטה בפועל, אלא האפשרות לשליטה.⁷⁶ היכולת של אדם להחליט בעצמו, האם לחשוף מידע, מתי, למי, באילו תנאים ונסיבות, לכמה זמן ושאר החלטות כאלה, חשובה כשלעצמה, גם אם אין הוא מממש אותה בפועל.

כאמור, הפרטיות כשליטה אינה הצדקה עצמאית של הפרטיות, אלא היא מאפיין שמשותף לכל ההצדקות, בכל מישורי הפעולה. במובן הזה, הפרטיות כשליטה היא מושג ברמת הפשטה אמצעית – בין ההצדקות הפילוסופיות

⁷⁰ לדיון, ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 56–86 (2011).

⁷¹ DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

⁷² שם, בעמ' 101.

⁷³ ראו למשל בירנהק, **פרטיות חוקתית**, לעיל ה"ש 8, בעמ' 86.

⁷⁴ תופעה זו אינה ייחודית לפרטיות. ראו למשל בקשר לחופש הביטוי: אילנה דיין אורבך "המודל הדמוקרטי של חופש הביטוי" **עיוני משפט** כ 377 (1996).

⁷⁵ ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

⁷⁶ Lisa M. Austin, *Rereading Westin*, 20 THEORETICAL INQ. L. 53 (2019). ראו גם Jordan Francis, Woodrow Hartzog, Neil Richards, *Privacy's Autonomy Thicket: Disentangling Choice, Consent and Control*, 1 GEO. WASH. J.L. & TECH. 36 (2026). שמדגישים את החשיבות של הזדמנות משמעותית לקבלת החלטות.

שברומו של עולם לבין כללי המשפט בשטח. זהו קיצור דרך מושגי שמקל עלינו לתרגם את ההצדקות העיוניות להנחיה מעשית; זהו כלי שמאפשר לנו לזהות, לפחות באופן ראשוני, את הפגיעה בפרטיות. ברוב המקרים, יהיה בכך די. אם נזהה פגיעה בשליטה של אדם במידע האישי שעל אודותיו, נוכל לומר שיש פגיעה בפרטיות, ואז נוכל לבדוק האם הפגיעה מוצדקת ומותרת, למשל לפי ההגנות שיש בחוק או לפי פסקת ההגבלה שבחוק היסוד. במצבים חדשים ייתכן שהפנייה למושג הביניים של הפרטיות כשליטה לא תספק, ונצטרך לחזור לעקרונות ראשוניים, כלומר להצדקות עצמן. אבל אלה מצבים נדירים.

הפרטיות כשליטה מתאימה היטב לפרטיות קלסית. למשל, צילום אדם ברשות היחיד היא פגיעה בפרטיות לפי סעיף 2(3) לחוק הגנת הפרטיות. אולם, אם אדם מסכים לצילום – אין בכך פגיעה. המשפט מפקיד את הכוח להחליט, כלומר את השליטה במידע ובפעולה של איסופו, בידי האדם עצמו. לעיתים נתלבט האם מקום מסוים הוא "רשות היחיד", אולם זו שאלה נפרדת. השליטה היא בידי המצולם, נושא המידע. המידע הוא תוכן הצילום.

הפרטיות כשליטה באה לידי ביטוי גם בדיני הפרטיות המידעית. עיון באוסף הזכויות והחובות שיש בדין עלול להותיר את הקוראים תוהים – יש שפע של כללים, והקשר ביניהם לא ברור במבט ראשון. מה בין חובת ההודעה לנושא המידע על איסוף המידע (סעיף 11 לחוק) לבין החובה לאבטחת מידע (סעיף 17 לחוק)? במשקפיים של הפרטיות כשליטה, התמונה מתבהרת. הדין מזהה נקודות מפגש קיימות בין נושא המידע לבין מי שמבקש לאסוף את המידע ולעבדו, ויוצר נקודות מפגש נוספות. בכל אחת מנקודות המפגש האלה, ניתן לנושא המידע כוח מסוים (לנסות) לשלוט במידע שעל אודותיו. ההסכמה הראשונית קריטית, אבל היא לא ממצה את השליטה. הזכות של נושא מידע לעיין במידע האישי שלו שמוחזק אצל "בעל השליטה במאגר המידע", למשל, משקפת את היכולת של נושא המידע לבקר את המידע שלו, לבחון שהוא נכון, שלם, רלוונטי ומדויק. בדין האירופי – אך לפי שעה לא בדין הישראלי – יש כללים משלימים שמחזקים את ההסכמה והעיון, למשל האפשרות של נושא המידע לחזור בו מהסכמתו, זכות לדרוש הגבלה של עיבוד המידע, או זכות לדרוש את מחיקת המידע באופנים שונים, ובכללם "הזכות להישכח".⁷⁷ גם הזכות לניוד מידע, שקיימת בישראל בקשר למידע רפואי, משקפת את השליטה של נושא המידע במידע.⁷⁸

הרעיון של פרטיות כשליטה קנה אחיזה גם בדיני הפרטיות החוקתית, הפעם בפסיקה. אזכיר שלושה מקרים. בעניין מעקב השב"כ בתקופת הקורונה שהגיע לפתחו של בג"ץ, העירה השופטת ברק-ארז כי המעקב הוא "היפוך התפיסה של הפרטיות כשליטה... במובן זה שהוא מבטא אובדן מידי של שליטת האדם עצמו במידע הנוגע לחייו".⁷⁹ במקרה שני, בערעור פלילי, פירש בית המשפט את האיסור על "הטרדה אחרת" וקבע שתליית כרזות באזור מגוריה של עובדת סוציאלית בשירות המדינה, שכללו סמל של גולגולת ביחד עם תמונתה וציון כתובתה ובליוי טקסט פוגעני הייתה הטרדה כזו, הגם שלא דובר במעקב פיזי. בית המשפט הסביר שההטרדה פוגעת בשליטה של האדם המוטred במרחב הפרטי שלו.⁸⁰ בעניין שלישי, בג"ץ קבע שנוהל משטרה שביקש להתיר למשטרה להסתמך על "הסכמה" של חשודים לעיון במכשיר הטלפון הנייד שלהם פסול, משום שנדרש צו של בית משפט, ואין בחוק הסכמה להסתפק בהסכמה, ומשום שממילא, הסכמה כזו אינה חופשית. המשנה לנשיאה סולברג ציין "ככלל, הסכמה היא יסוד מרכזי בדיני הפרטיות, המבטא את יכולת שליטתו של האדם במידע הקיים על אודותיו".⁸¹

חוקרי פרטיות, בעיקר אמריקניים, מבקרים בתוקף את תפיסת הפרטיות כשליטה.⁸² הם מצביעים על כישלונה הכמעט מוחלט של חובת ההודעה שעל בסיסה ניתנת הסכמה. עניינם הוא בפרטיות המידעית, והם צודקים שעקרונות ההודעה וההסכמה כושלים בפועל, ולכן מכשילים את נושאי המידע. רבים מהמשתמשים ברשת

⁷⁷ ראו סעיפים 7(3) (חזרה מהסכמה), 18 (הגבלת עיבודי מידע), 17 (מחיקת מידע), ל-GDPR.

⁷⁸ ראו חוק ניוד מידע רפואי, התשפ"ד-2024.

⁷⁹ בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת**, פס' 13 לפסק-דינה של השופטת ברק-ארז (נבו 1.3.2021). הפניה פנימית הושמטה.

⁸⁰ רע"פ 4743/20 **לייבל נ' מדינת ישראל**, פס' 21 (נבו 21.7.2022) (בנוגע לפרשנות התיבה "הטרדה אחרת" בסעיף 2(1) לחוק: "מדובר בהוראת 'סלי' גמישה אשר מספקת הגנה למרחב הפרטי של האדם. גם חדירה למרחב הפרטי היורטואלי של האדם פוגעת ביכולתו של האדם להיעזב במנוחה במרחב זה ולשלוט בו, ובכך פוגעת באוטונומיה שלו ובכבודו.")

⁸¹ בג"ץ 8298/22 **הסגוריה הציבורית נ' היועצת המשפטית לממשלה**, פס' 41 לפסק דינו של המשנה לנשיא סולברג (נבו 31.8.2025).

⁸² ראו למשל Woodrow Hartzog, *The Case against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018); וכן IGNACIO COFONE, *THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY* (2024).

וביישומונים אינם מבינים מה פשר "מדיניות הפרטיות", אינם קוראים אותה, אינם מבינים את תוכנה, ואינם מבינים שיש להם אפשרות מסוימת לשלוט במידע.⁸³ אוספי המידע נוקטים גישות מפקפקות של "דפוסים אפלים" לבלבל את נושאי המידע או להטות אותם לכיוון שרצוי לאוספי המידע, ולא לנושאי המידע עצמם.⁸⁴ תאגידים משתמשים ברטוריקה של "פרטיות כשליטה", אבל הם מתכוונים לאפשרויות של שליטה במידע שמוענקות למשתמשים זה מול זה, למשל ברשתות חברתיות, ורק הם מצניעים את היעדרה של הפרטיות המידעית מול הפלטפורמות עצמן.⁸⁵

הביקורת מוצדקת, אבל היא אינה מחייבת את ביטולה של הפרטיות כשליטה.⁸⁶ ראשית, הפרטיות כשליטה חלה גם במישורי הפעולה האחרים, של הפרטיות הקלסית והפרטיות החוקתית. שנית, השליטה אינה מתמצה רק בנקודת המפגש הראשונה בין נושא המידע לבעל השליטה במידע. נקודות המפגש שהמשפט זיהה או יצר מאפשרות שליטה נמשכת, גם לאחר שהמידע נאסף ויצא מידי נושא המידע. למשל האפשרות לחזור מהסכמה או לדרוש מחיקה של המידע. שלישית, המבקרים טועים בכריכה הדוקה מדי של חובת ההודעה עם דרישת ההסכמה.⁸⁷ גם אם אופן ביצוע דרישת ההסכמה כושל בפועל, יש ערך בחובת ההודעה. כלפי חוץ – זהו פתח לאחרים לקרוא את ההודעה ולנקוט פעולה: מאסדרים (רגולטורים), עיתונאים, עורכי דין בתובענות ייצוגיות, או משתמשים שיספרו לחבריהם מה גילו;⁸⁸ וכלפי פנים – זהו אירוע משפטי שבו, בארגונים מסודרים, יצופו שאלות – מה בעצם אנחנו אוספים? לאילו מטרות? רביעית, המבקרים טועים בהסקת הראוי (זניחת הפרטיות כשליטה כעקרון מארגן) מתוך המצוי (המצב הכושל של ההסכמה). זהו כשל לוגי-פילוסופי.⁸⁹

במילים אחרות, למרות הקשיים, הפרטיות כשליטה עדיין מספקת מסגרת תיאורטית ראויה. אין להתעלם מהקשיים הרבים שיש בפועל, למשל בקשר להסכמה. הפתרון אינו לוותר על השליטה, אלא לחפש דרכים לתקן את הפגמים והליקויים. המסקנה שנלמדת מכל זה היא שפרטיות כשליטה היא מכנה משותף להצדקות השונות של הפרטיות ומשמשת מושג ביניים ברמת ההפשטה, שמאפשר יישום ופרשנות נוחים יותר. הפרטיות כשליטה היא הפוטנציאל לקבל החלטות בקשר למידע האישי שלנו. השליטה שבה מדובר – נמשכת, לאורך כל מהלך החיים של המידע. הפרטיות אינה מתמצית אחרי השלב הראשון של איסוף המידע, וצריכה להימשך גם לאחר האיסוף הראשוני, בשלבים של עיבוד, שימוש בפועל, העברה לאחרים או פרסום, וגם, במות המידע. המסקנה הזו תשמש אותנו בהמשך הדיון.

3. חשיבות הבירור של הפגיעה בפרטיות

בין אם מחמת העמימות המובנית של הפרטיות, התזזיתיות שלה, או מושגי השסתום המשפטיים הרבים שיש בדיון, בין אם מחמת השינויים הטכנולוגיים, החברתיים והעסקיים התכופים שמאתגרים את המשפט בכלל ואת הפרטיות במיוחד, ובין אם מטעמים של יעילות שיפוטית, בתי משפט נוטים להניח שהייתה פגיעה בפרטיות במקרים שמובאים אליהם, ולכן מדלגים לשלב הבא בדיון, של איזונים מול צרכים ציבוריים שונים. כפי שטענתי במקום אחר, זהו דילוג מהיר מדי, ויש לו מחיר חוקתי.⁹⁰ כאשר אנחנו מדלגים היישר להנגדה של הפרטיות עם

⁸³ לכל אלה, ראו בירנהק ורחום-טוויג, **פרטיות מידעית**, לעיל ה"ש 21, בעמ' 189-192; Ella Corren, *Gaining or Losing Control? An Empirical Study on the Real Use of Data Control Rights and Policy Implications*, 109 IOWA L. REV. 2017 (2024).

⁸⁴ דפוסים אפלים מתייחסים לעיצוב של האתר והמערכות, שמטה את המשתמשים לקבל החלטה שאינה בהכרח הטובה ביותר עבורם. למשל, הדגשה של אפשרות מסירת מידע בצבעים שמחים, בוהקים ובשפה חיובית, לעומת הצגת האפשרות לסרב למסירת המידע. דפוסים כאלה נמצאים בדרך כלל בתחום האפור, ואינם עולים בהכרח לכדי הטעיה לפי דיני הגנת הצרכן. עם זאת, יש כבר ניצנים לאיסור השימוש בהם בקשר לאיסוף מידע אישי, למשל בחוק רב-ההשפעה של קליפורניה. ראו (CCPA, §1798.40(l)).

⁸⁵ Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (2021).

⁸⁶ להרחבה, ראו Michael Birnhack, *In Defense of Privacy-as-Control (Properly Understood)*, 65 JURIMETRICS 143 (2026).

⁸⁷ Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POL'Y 148 (2019).

⁸⁸ לטענה דומה, בקשר לחוזים אחידים בכלל, ראו Samuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOM. & TECH. L. REV. 303, 311 (2008).

⁸⁹ לדיון בביקורת על הגישה האמריקנית, ראו Jordan Francis, Woodrow Hartzog, Neil Richards, *Privacy's Autonomy Thicket: Disentangling Choice, Consent and Control*, 2 GEO. WASH. J. L. & TECH. 36, 52-55, 58 (2026).

⁹⁰ בירנהק, **פרטיות חוקתית**, לעיל ה"ש 8, בעמ' 218-219, 323.

אינטרס ציבורי, האמורפיות והעמימות של הזכות מול האינטרס שהוא בדרך כלל מידי וקונקרטי, מביאה לניצחון האינטרס על פני הזכות. בין אם מדובר באינטרס אזרחי של בריאות הציבור במהלך מגיפה, אינטרס משטרתי-ציבורי להיאבק ב"מכת מדינה", ובוודאי באינטרס ביטחוני – קל לבית המשפט לומר שהפרטיות ניגפת מפני האינטרס החשוב.

זהו מהלך מהיר מדי, שמוזיל את ערכה של הפרטיות, וראוי לזנוח אותו. במקומו, יש להתעכב, ולנסות לברר מהי הפגיעה בפרטיות. לעיתים, נגלה שמה שנחזה כפגיעה איננו כזה. למשל, במקרה אחד דן בית המשפט באריכות בהתנגשות בין האינטרס של שקיפות וחופש המידע עם הפרטיות. אולם, דובר שם בתאגידים. דיון מתוך עולם הפרטיות היה מעלה שתאגידים כלל אינם זכאים לפרטיות. השופטת נאור העירה כך בפסק הדין, אבל בכל זאת, השופטים האריכו והכריעו בסוגיה תוך התעלמות מנקודה זו.⁹¹

ההנחה שיש פגיעה בפרטיות והמעבר המהיר לאיזונים גורמים לעיתים להתמקדות בפגיעה מסוג אחד והחמצה של פגיעה אחרת. למשל, בפסק דין שעסק בחוקתיות החוק שמכוחו נאספים נתונים ביומטריים לשם שמירתם בתעודות זהות ודרכונים, התמקד בית המשפט בשאלה האם יש חשש שהמאגר הביומטרי ידלוף.⁹² זהו בהחלט שיקול חשוב, ובוודאי שאילו הייתה דליפה כזו, הייתה פגיעה קשה בפרטיות. אבל ההתמקדות בדליפה אפשרית מתעלמת מהאפשרות שיש פגיעה בפרטיות גם בשלבים קודמים במהלך החיים של המידע. הנטייה לצמצם את הפגיעה בפרטיות לשלב הדליפה והפרסום הלא מורשה, נפוצה, ונראה אותה גם בקשר למידע רפואי, אבל היא שגויה. כל הפעולות בקשר למידע, גם אלה שקדמו לפרסום ולדליפה, כמו איסוף, שמירה ועיבוד המידע, כפופות לזכות לפרטיות, ולנושא המידע אמורה להיות שליטה נמשכת במידע האישי גם באותם שלבים מוקדמים.

המסקנה היא שאין מנוס, ולמרות האתגרים, יש לנסות לברר את הפגיעה בפרטיות, כדי לברר מה בדיוק נפגע, האם כצעתה, וגם כדי לאתר פתרונות מותאמים. במקום איזון בינארי, הבירור יכול לסייע לנו להשיג גם את האינטרס הציבורי וגם לממש את הזכות לפרטיות בכבוד שראוי לה. במילים אחרות, הבירור של הפגיעה בפרטיות נדרש על ידי המסגרת החוקתית עצמה.

כעת, אפשר לבחון את המפגש של הפרטיות עם שינויים בזירה: טכנולוגיות חדשות של עיבוד מידע, בינה מלאכותית, והפיכת הזירה למצב מידעי מורכב.

ב. נתוני עתק רפואיים

השלם גדול מסך חלקיו. עיבוד מידע רפואי בהיקפים עצומים ובכלים טכנולוגיים מאפשר להגיע לתובנות חדשות שמקדמות את המחקר הרפואי, פיתוח תרופות ומיכשור רפואי וטיפול, ובאופן רחב יותר, את בריאות הציבור ורווחתו. בעשורים האחרונים שתי טכנולוגיות חוללו מהפכה בתחום הזה, כבתחומי חיים רבים אחרים, והאיצו מאוד את התחום: טכנולוגיות של נתוני עתק ובינה מלאכותית. פרק זה בוחן את הכניסה של נתוני עתק לתמונה, והפרק הבא יעסוק בממשק של המידע הרפואי עם הבינה המלאכותית. אבחן את המפגש שבין המשפט לטכנולוגיה, ואציג תמונת מצב כללית של מחקר מבוסס-מידע רפואי בישראל. אתאר באופן כללי את האפשרויות ואתמקד באתגרי הפרטיות המשפטיים שמתעוררים, בעיקר בקשר להסכמה ולעקרון צמידות המטרה. אסביר גם מדוע התממה אינה פתרון קסם.

1. מחקר רפואי בנתוני עתק

המפגש העיקרי של המידע הרפואי עם הטכנולוגיה של נתוני עתק נוגע למחקר רפואי, והביא לשינוי דרמטי באופני המחקר המסורתיים. נתוני עתק הם שם כולל שמתייחס לטכנולוגיות לעיבוד נתונים בהיקפים גדולים, ממגוון מקורות ובמגוון תצורות, ובמהירות. מקובל לאפיין את הטכנולוגיות האלה כשלושה V: Volume, Variety, Velocity.⁹³ המידע הרפואי של כל אחד מאיתנו חשוב לנו, אבל באמצעות צירוף נתונים אפשר לזהות

⁹¹ עע"מ 7744/10 המוסד לביטוח לאומי נ' מנגל, פ"ד סו(1), 116, 162–163 (2012).

⁹² בג"ץ 1946/17 זידאן נ' ממשלת ישראל (נבו 12.7.2022).

⁹³ בספרות הטכנולוגית יש מי שמוסיפים עוד מאפיינים, כמו Value. לדיון בהגדרות השונות, ראו Isitor Emmanue & Clare Stanie, Defining Big Data, BDAW'16, 10 (2016).

קשרים ביניהם, מגמות ושינויים שהחוקרים לא העלו על דעתם לבחון. כך, אפשר לזהות מחלות, התפרצות מגיפות ומוטציות בנגיפים, טעויות בטיפול הרפואי, קשרים וסיבתיות בין גורמי מחלה, אופני אבחון, שימושים לא צפויים בתרופות, יעילות של תרופות, תופעות לוואי לא ידועות, ועוד. היתרונות ברורים.⁹⁴ המידע שבו מדובר הוא התוכן הרפואי עצמו, אבל גם מידע על המטופלים – גיל, מין, מוצא, מידע סוציו-אקונומי, מידע מנהלי שנצבר במערכות הבריאות, ועוד.

כמו כל מחקר ושיטת מחקר, יש חשש שהמידע הגולמי אינו משקף נכונה את האוכלוסייה שרלוונטית למחקר. אמנם, מידע בהיקפי עתק עשוי להיות שיקוף טוב יותר של האוכלוסייה מאשר מדגם אקראי, אולם עדיין, במונחים סטטיסטיים, ההנחה $N=All$ אינה נכונה.⁹⁵ יש חשש מהטיות שונות בהרכב הקבוצה שלגביה נאסף המידע, ובניתוח הנתונים יש ליצור מכנה משותף למידע ממקורות שונים; בהסקת מסקנות, יש חשש מבלבול בין מתאם (correlation) לסיבתיות (causality), כלומר זיהוי של קשרים לא צפויים בין נתונים שונים שמוביל חוקרים לחשוב שיש קשר סיבתי ביניהם, בעוד שהמתאם מקרי. בנוסף, עלולות להיות טעויות במחקר עצמו. חוקרים ממכון ויצמן הצביעו על כמה ממדים של מחקר בנתוני עתק רפואיים, כמו היקף האוכלוסייה שכלולה במחקר, ממד הזמן, עירוב מקורות שונים ואתגרים נלווים, ועוד, ועל כך שהעדפה של ממד אחד עלולה לבוא על חשבון מידת הדיוק בממד אחר.⁹⁶

כדי להבין את היבטי הפרטיות במחקרים רפואיים בנתוני עתק, אשווה אותם למחקרים שמבוצעים ללא תיווך טכנולוגי, כלומר, מחקר מסורתי-אנושי. מחקר רפואי מסורתי מציג מקרי מבחן נקודתיים – תיאור מקרה רפואי מסוים או מחקר קליני, כלומר ניסוי.⁹⁷ סוג אחר של מחקרים רפואיים אוסף ממצאים מהסוג הראשון, ומציע מבט-על (meta-analysis).⁹⁸ חוקרים באקדמיה הרפואית ובמדעי החיים מזהים בעיות ואתגרים ומחפשים פתרונות. הידע נוצר נדבך על גבי נדבך. במחקר מסורתי-אנושי, החוקרת תתחיל בדרך כלל עם שאלת מחקר מוגדרת. למשל, היא תבקש לבחון כיצד משפיעה תרופה מסוימת על גידול סרטני, והאם היא יעילה יותר מתרופות אחרות. מחקר אנושי מצריך משאבים של כוח אדם, זמן וכסף, ויסתפק במדגם קטן יחסית של מטופלים. מחקר כזה כפוף לאישור ועדת הלסינקי של מערכת הבריאות,⁹⁹ ואם הוא נערך במסגרת אקדמית, גם לאישור של ועדת אתיקה מוסדית.¹⁰⁰

בהיבט הפרטיות, במחקר מהסוג הזה יש בדרך כלל מפגש ישיר בין המטופל לצוות המחקר, שבדרך כלל כולל את הרופאה המטפלת. במפגש פנים אל פנים אפשר להסביר למטופל במה מדובר ולבקש הסכמה מדעת בטופס ייעודי. ההסכמה עלולה להיות "חשודה" בהיבט של הרצון החופשי, למשל כאשר המטופל תלוי ברופאה להמשך הטיפול וחושש שסירוב להשתתף במחקר ישפיע על הטיפול, או שהמטופל חש הכרת תודה ומתקשה לסרב, גם אם היה מעדיף אחרת. כאן נכנס לתמונה הפן האתי, שמבהיר למטופל שזכותו לסרב להשתתף במחקר ושהטיפול בו לא ייפגע. יש אמצעים נוספים להרחיק בין המטפל לחוקר כדי לצמצם את הסיכונים האלה.

במחקר בשיטה מסורתית, המטופל (במסגרת הרפואית) הופך לנסיין (במסגרת המחקרית) ולנושא מידע (בהמשגה של דיני הפרטיות), שפרטיו ידועים לחוקרת אבל אינם מתפרסמים במחקר.

לעומת זאת, במחקר טכנולוגי שמנתח נתוני עתק, יש הבדלים בכל ההיבטים האלה. ראשית, הגם שניתן להגדיר שאלת מחקר נקודתית, במקרים רבים, שאלת המחקר אינה ידועה מראש. החוקרת תזין נתונים גולמיים למערכת הטכנולוגית כדי שזו תאתר קשרים בין הנתונים. עיבוד המידע הטכנולוגי עשוי לאתר הרבה קשרים

⁹⁴ ראו למשל Lidong Wang & Cheryl Ann Alexander, *Big Data Analytics in Medical Engineering and Healthcare: Methods, Advances and Challenges*, 44 J. MEDICAL ENG. & TECH. 267, 269-270 (2020).

⁹⁵ לדיון, ראו danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15(5) INFO., COMM. & SOC'Y, 662 (2012).

⁹⁶ Smadar Shilo, Hagai Rossman, Eran Segal, *Axes of A Revolution: Challenges and Promises of Big Data in Healthcare*, 26 NATURE MEDICINE 29 (2020).

⁹⁷ ליתרונות וחסרונות של מחקרים קליניים מסוגים שונים, ראו A. Schultz, B.R. Saville, J.A. Marsh, T.L. Snelling, *An Introduction to Clinical Trial Design*, 32 PAEDIATRIC RESPIRATORY REV. 30 (2019).

⁹⁸ לדיון במחקרים מסוג זה, ראו Joseph L. Mathew, *Systematic Reviews and Meta-Analysis: A Guide for Beginners*, 59 INDIAN PEDIATR. 320 (2022).

⁹⁹ ראו תקנות בריאות העם (ניסויים רפואיים בבני-אדם), התשמ"א-1980, ונהלים לפיו.

¹⁰⁰ ראו למשל את הוועדה למחקרים בבני אדם של אוניברסיטת תל אביב: https://acad-sec.tau.ac.il/info/ma_1654_1655.

מקריים, או כאלה שאין בהם עניין (האם גובה המטופל קשור לסיכויי לחלות בסרטן העור?), אבל העיבוד עשוי להניב מתאמים מפתיעים. מתאם אין פירושו סיבתיות, וכאן על בסיס הממצאים הראשונים שהמערכת הניבה, החוקרת תגבש שאלות מתאימות למחקרי המשך. **שנית**, אמנם יש עלויות של למידת הטכנולוגיה והשימוש בה, אבל לאחר ההוצאה החד-פעמית הזו, המחקר יכול להתנהל במהירות, ביעילות, ובדיוק. מחקר טכנולוגי מאפשר להצליב נתונים מבדיקות דם, עם פרטי המטופלים (גיל, מגדר, מוצא אתני, היסטוריה של חיסונים, מקום מגורים – האם גרים קרוב למפעל מזהם, למשל), ומידע רפואי אחר (למשל הדמיות MRI, נתוני לחץ דם, והיסטוריה של נטילת תרופות). כל זה אפשרי בהיקף עצום. המחקר יתייחס לרובבות, מאות אלפים, או מיליוני בני אדם. כאמור, האפשרויות רבות וחשובות; מחקר רב-משתתפים משקף טוב יותר את המציאות מאשר מדגם קטן; העושר של המידע מאפשר להגיע לתובנות מעמיקות יותר, שאי אפשר היה להגיע אליהן במחקר אנושי. בצד זה, יש גם חסרונות, כבכל מחקר.

המיקוד במאמר הנוכחי הוא בהיבט הפרטיות. במחקר מבוסס-נתונים אין מפגש אישי מקדים בין החוקרת לבין מאות אלפי האנשים שהמידע הרפואי שלהם מעובד במחקר. האפשרות לפנות מראש למטופלים ולבקש הסכמה להשתתף במחקר אמנם קיימת, ולפחות קופת חולים אחת (מכבי) נוהגת כך במסגרת מיזם "טיפה למחקר".¹⁰¹ אבל, הקמת מערך מחקר כזה יקרה, ממושכת, ועלולה לסבול מהטיות מסוימות – לא כולם יסכימו להצטרף ומאגר הנתונים לא יהיה מייצג.¹⁰² כך או כך, במאגר כזה יהיה יותר מידע מאשר במחקר שמבוסס על מדגם של עשרות בודדות של מטופלים. בשל הקשיים להשיג הסכמה מראש או בדיעבד, מתברר שבמקרים רבים, במחקר הטכנולוגי, החוקרים אינם מבקשים את הסכמת המשתתפים. בבדיקה שערכתי לפני מספר שנים, כאשר מחקרים רפואיים-טכנולוגיים מעין אלה רק החלו להתפרסם בעולם, עלה שמחקרים רבים לא ציינו דבר בקשר להיבט ההסכמה, בקבוצה לא קטנה צוין שניתן אישור של ועדת האתיקה הרלוונטית, ובחלק צוינה הסיבה: התממה, כלומר הסרת פרטים מזהים מהמידע הגולמי.¹⁰³ נוהל של משרד הבריאות מתיר שימוש משני במידע רפואי לצורכי מחקר, באישור של תת ועדת הלסינקי ייעודית. כאשר המידע מזהה את נושאו או שניתן לזהותו מתוך המידע, נדרשת הסכמה פרטנית, חופשית ומדעת, ואילו כאשר המידע מותמם בצורה נאותה, תת-הוועדה יכולה לפטור את החוקרים מקבלת הסכמה פרטנית.¹⁰⁴

במחקר בנתוני עתק, המטופל (במסגרת הרפואית) הופך להיות נסיין במחקר, אבל שלא בידעיתו, ותוך דילוג על השלב שבו הוא נחשב לנושא מידע (בהמשגה של דיני הגנת הפרטיות), משום שהוא אינו מזוהה.

טבלה 1 משווה בין היבטי הפרטיות במחקר רפואי אנושי מסורתי למחקר בנתוני עתק.

טבלה 1: מחקר אנושי מסורתי מול מחקר בנתוני עתק

מחקר בנתוני עתק	מחקר מסורתי-אנושי	שאלת המחקר
לא בהכרח ידועה מראש	מוגדרת מראש	תוצאות המחקר
איתור מתאמים בין נתונים	אישוש או הפרכת השערות המחקר	מקור המידע
מכל מקור אמין	אגב טיפול רפואי או השתתפות בניסוי	היקף המידע
עשרות אלפים ועד מיליונים	ממקרה יחיד ועד מאות בודדות	מפגש חוקר-מטופל
אין	ישיר	מסגרת משפטית ואתית
אישור תת-ועדת הלסינקי למחקר רפואי שאינו בבני אדם	אישור ועדת הלסינקי בבתי חולים אישור מוסדי באקדמיה	פרסום המידע
אנונימי	אנונימי	המשגת מושא המחקר
מטופל – [נסיין] – [נושא מידע] ¹⁰⁵	מטופל – נסיין – נושא מידע	

¹⁰¹ ראו https://www.maccabi4u.co.il/23085/kahn-segol/tipa_project/.

¹⁰² יש הבדלים רלוונטיים למחקר הרפואי בין אנשים שמתנדבים להשתתף במחקרים רפואיים למי שבחורים אחרת. ראו Shilo, Rossman, Segal, Axes, לעיל ה"ש 96, בעמ' 31.

¹⁰³ ראו Michael Birnhack, *A Process-Based Approach to Informational Privacy and the Case of Big Medical Data*, 20 THEORETICAL INQ. L. 257 (2019).

¹⁰⁴ חוזר מנכ"ל משרד הבריאות, שימושים משניים במידע בריאות (17.1.2018) (להלן: "חוזר שימושים משניים").

¹⁰⁵ אני מציין את הסטטוס של המטופל כנסיין וכנושא מידע בסוגריים, משום שנושא המידע אינו יודע שהוא נסיין במחקר, ומשום כך הוא גם אינו יודע שבצד היותו מטופל, הוא הופך ל"נושא מידע" במובנו של המונח בדיני הפרטיות.

2. תמונת מצב מחקרית

בזכות מערכת הבריאות הציבורית שנהוגה בישראל עוד מתקופת המנדט הבריטי,¹⁰⁶ כל אזרחי המדינה ותושביה מבוטחים בביטוח בריאות,¹⁰⁷ ולגבי כולם יש מידע רפואי כלשהו. קופות החולים הטמיעו מערכות מחשוב עוד בשנות התשעים של המאה הקודמת לצורכי ניהול, וצברו לאורך השנים מידע רב. בשל השימוש בתעודות זהות (בשונה למשל מאשר בבריטניה וארצות הברית), קל לשייך מידע שנמצא במקום אחד עם מידע ממקור אחר, למשל מידע מקופת החולים עם מידע מבית מרקחת.¹⁰⁸ אמנם ניתן לעבור מקופת חולים אחת לשנייה בלי שהזכאות לטיפול רגיל תיפגע, וחוק ניוד מידע רפואי שנזכר לעיל אמור להקל מעבר כזה, אבל לפי שעה, היקפי המעבר בין קופות החולים קטנים.¹⁰⁹ רובנו מבוטחים שנים רבות מאוד באותה קופת חולים. התוצאה היא שבישראל יש עושר עצום של מידע רפואי, רובו מוחזק בידי קופות החולים. הקופות הבינו בעשורים האחרונים שמאגרי המידע שהקימו לצורכי ניהול הם מכרה זהב לצורכי מחקר ומסחר. בשתי הקופות הגדולות, כללית ומכבי, יש מחלקות למחקר נתוני עתק ושיתופי פעולה עם אוניברסיטאות מחקר.¹¹⁰ לפחות במקרה אחד מידע רפואי נמכר לגורם מסחרי (חברת תרופות).¹¹¹ בשתי הקופות האחרות, לאומית ומאוחדת, יש מסגרות פעולה למכירת מידע לצורכי מחקר.¹¹² אחרי המחקר הבסיסי שנשמך על הנתונים, עשוי להגיע שלב של מחקר יישומי, כלומר תרגום הידע שהתגלה באמצעות ניתוח המידע להליכי טיפול, תרופות, ציוד רפואי, או מרכיבים אחרים שניתן למסחר.

בצד קופות החולים, משרד הבריאות הקים מערך מחקרי בשם תמנ"ע: תשתית מחקר לנתוני עתק.¹¹³ כפי שהמשרד מסביר, מדובר ב"פלטפורמה לאומית לביצוע מחקרי ביג דאטה בנתוני בריאות... [ש]מאפשרת ניתוח מידע קליני באמצעות סביבות מחקר וירטואליות מאובטחות, תוך שימוש בשיטות מתקדמות להתממת המידע... תמנ"ע מאפשרת לחוקרים להצליב מידע ממספר ארגוני בריאות, בסביבת מחקר ניטרלית, אשר בה המידע נגיש רק לחוקרים אשר קיבלו את הסכמת ארגוני הבריאות השותפים למחקר."¹¹⁴ הפלטפורמה הממשלתית מאפשרת גישה ליותר מידע מאשר יש בכל קופת חולים בנפרד והמידע מגוון יותר, באופן שמצמצם הבדלים אפשריים בין סוגי האוכלוסיות המבוטחות בכל קופה בנפרד. המאגרים שמוגשים במערכת הממשלתית כוללים מרשמים על לידות ופטירות וסיבת המוות, אשפוזים וביקורים במרפאות חוץ בבתי חולים,

¹⁰⁶ לשורשים המנדטוריים של מערכת הבריאות הישראלית, ראו גבי בן-נון, יצחק ברלוביץ, מרדכי שני **מערכת הבריאות בישראל** 29 (2020). אחד מעמודי התווך של המערכת הוא הרעיון של קופות החולים, שמבוססות על עזרה הדדית. כדברי המחברים "אפיון זה של קופת החולים הכללית טבע את חותמו לא רק על הקופה אלא על כל מערכת הבריאות הישראלית למשך שנים רבות". שם, בעמ' 33.

¹⁰⁷ סעיף 3 לחוק ביטוח בריאות ממלכתי, התשנ"ד-1994 קובע את הזכות לשירות בריאות לכל תושב. הגדרת "תושב" בסעיף 2 מפנה לחוק הביטוח הלאומי [נוסח משולב], התשנ"ה-1995. בן-נון, ברלוביץ ושני מתייחסים לזכות זו כאל חובת ביטוח. שם, בעמ' 285.

¹⁰⁸ זה נתון חשוב, משום שלא תמיד המטופלים רוכשים את התרופות שנרשמו להם. מחקר שיתבסס רק על רישום הקופה עלול שלא לשקף את המצב לאשורו. הצלבה עם מידע מבתי מרקחת מצמצם את החשש, אך עדיין, יש מי שירכשו את התרופה ולא ייטלו אותה.

¹⁰⁹ לפי משרד הבריאות, בשנת 2024, היו 181,736 מבוטחים שעברו בין קופות חולים. ראו משרד הבריאות **דוח מסכם על פעילות קופות החולים** לשנת 2024, 19 (2025). https://www.gov.il/BlobFolder/reports/dochhashvaatui2024/he/files_publications_units_shaban_dochhashvaatui2024.pdf. 4. הנתון דומה לשנים קודמות. ראו משרד הבריאות **עזיבת מבוטחים את קופות החולים 2022** 3 (2023). https://www.gov.il/BlobFolder/reports/switching-hmo-2022-n/he/files_publications_units_financial-strategic-planning_publications_misc_leaving_between_HMO2022.pdf. בטווח של עשרים שנים מהתקופה שנסקרה, שיעור המבוטחים שעברו בין קופות החולים נע בין 0.86% ל-2.61%.

¹¹⁰ זרוע המחקר של קופת חולים כללית מציעה שיתופי פעולה מחקריים לניתוח המידע שברשותה. ראו Clalit, Ocean Platform, נמצא ב: <https://www.clalit-innovation.org/ocean>. "קטלוג המידע" שמוצג שם כולל מידע על מעל 1.3 מיליארד אבחונים; מעל 5.2 מיליארד ממצאי מעבדה, מעל 32 מיליון אשפוזים, 1.9 מיליארד נתונים מבתי מרקחת, ועוד. זרוע המחקר של קופת חולים מכבי מתהדרת גם כן במידע בהיקפי ענק, עם מידע על מיליון דגימות ביולוגיות. ראו <https://www.ksminnovation.com>.

¹¹¹ קופת חולים מכבי העבירה לחברת תרופות נתונים סטטיסטיים אנונימיים ללא פרטים אישיים חסויים של המבוטחים. תביעה ייצוגית שהוגשה בעניין נמחקת. ראו ת"צ (מחוזי מרכז) 283-10-13 **זוחוביצקי נ' מכבי שירותי בריאות** (נבו 7.5.2015).

¹¹² קופת חולים לאומית מציעה למכירה מידע סינטטי, כלומר מידע שנוצר באופן מלאכותי על בסיס מידע אמיתי. ראו <https://pay-and-research.leumit.co.il>. באוניברסיטת תל אביב מוקם מרכז נתונים גלובלי בשיתוף חברת התרופות אסטרזהניקה, למחקר במידע שמגיע מקופות החולים לאומית ומאוחדת וארגונים דומים בעולם. ראו דיווח כאן: <https://tinyurl.com/5br5a3rf>.

¹¹³ <https://govextra.gov.il/ministry-of-health/big-data-research/home>

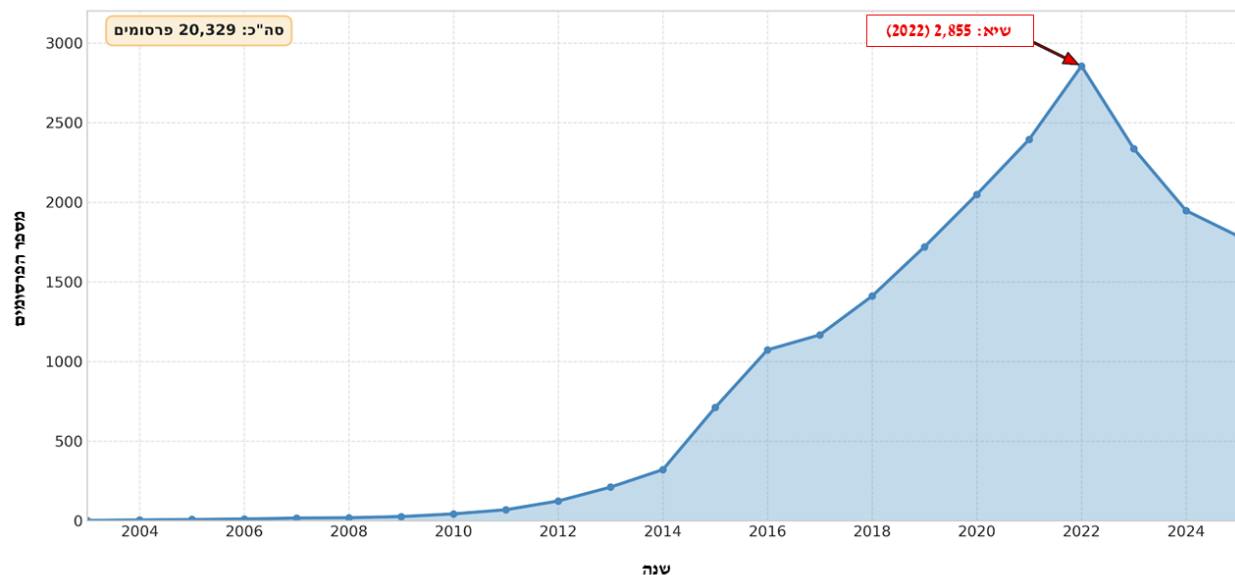
¹¹⁴ שם.

מידע על קורונה, רישוי קנאביס, סרטן, סוכרת, טיפולי דיאליזה, ועוד.¹¹⁵ המידע מפורט. למשל, בקשר לאשפוזים פסיכיאטריים הוא כולל, בצד מספר תעודת זהות מוצפן, תאריך לידה, גיל, מצב משפחתי, לאום, דת, שנות לימוד, כתובת מגורים וקופת חולים, מידע על מועדי האשפוז, האם נעשה בהסכמה או בכפייה, את האבחנות הפסיכיאטריות, שימוש באלכוהול וסמים, וניסיון אובדני, אם היה כזה. יש להניח שגורם בעל עניין ויכולות טכנולוגיות (או כספיות, לרכוש שירות של גורם טכנולוגי מיומן) יוכל לזהות את זהות האדם מתוך המידע הזה. המידע קיים מאז שנת 1950, לגבי כלל האוכלוסייה.¹¹⁶

כיום, אנו רואים עליה רצופה במחקרים רפואיים שמשתמשים בנתוני עתק בעולם עד לשנת 2022, ומאז, יש התמתנות מסוימת. חיפוש המונח "big data" בכותרות ובתקצירים של מאמרים רפואיים במאגר PubMed שכולל מעל 35 מיליון מחקרים רפואיים עד לשנת 2025 ועד בכלל, העלה 20,329 מחקרים כאלה, בהתפלגות הבאה:¹¹⁷ אקדים ואעיר שההתמתנות משנת 2022 אינה מעידה על צמצום השימוש בנתוני עתק, אלא על כך שמילת מפתח חדשה כבשה את השיח – בינה מלאכותית.

איור 1: מחקרים רפואיים בנושאי נתוני עתק 2025–2003

שמאזכרים "נתוני עתק" בכותרת או בתקציר המאמר



3. אתגרי הפרטיות במחקר נתוני עתק

דיני הפרטיות מתקשים להתמודד עם נתוני עתק – בהיבט הרפואי ובכלל. משפטנים עמדו על האתגר הזה בעבר.¹¹⁸ איור הנחות יסוד סמויות שיש בדיני הפרטיות הקיימים בדבר לינאריות של מהלך החיים של המידע ומערך השחקנים, ואצביע על האתגרים שהטכנולוגיה מציבה לעקרונות של מזעור מידע, הסכמה, וצמידות מטרה. בפועל, מי שמעבדים מידע בהיקפי עתק מצביעים על כך שהמידע שמשמש אותם כחומר גלם מותמם

¹¹⁵ ראו שקף 3 במצגת הפרויקט: <https://govextra.gov.il/media/og1f55je/timna-catalog-2024.pdf>.

¹¹⁶ ראו שקף 7, שם.

¹¹⁷ ראו PubMed, National Library of Medicine, <https://pubmed.ncbi.nlm.nih.gov/?term=%28big+data%5BTitle%2FAbstract%5D%29&filter=dates.2003%2F1%2F1-2025%2F12%2F31>. האתר אינו מציג מידע מלפני שנת 2003 בשאלתה זו.

¹¹⁸ לדיון בהקשר האמריקני ראו Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of* Tal Z. Zarsky, *Incompatible: The GDPR in the*, ובהקשר אירופי, *Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013); *Age of Big Data*, 47 SETON HALL L. REV. 995 (2017).

ולעיתים אגרגטיבי-סטטיסטי, ולכן, הם טוענים, הם פטורים מעולם של דיני הפרטיות. הבנת הפרטיות כשליטה נמשכת מערערת על טענה זו.

(א) הגיון לינארי מול מעגליות

כפי שראינו בפרק הקודם, דיני הפרטיות מבוססים על הנחת יסוד של מהלך החיים של המידע, החל באיסופו, המשך בעיבודו, בשימוש בו, העברתו לאחרים, ואולי גם מותו של המידע. זו חשיבה לינארית. לעומת זאת, נתוני עתק אינם פועלים בהכרח בהגיון לינארי. מנקודת המבט של נתוני עתק, המידע כבר קיים – ולכן אין עיסוק בשאלת איסופו; המידע מועבר מגורמים רבים ומלוכד יחדיו, ומעובד. לעיתים, השימוש במידע נעשה תוך כדי העיבוד (ולא אחריו). מידע מעובד ותוצרי העיבוד מוזנים שוב לתוך המערכת. היבטים אלה מתעצמים כאשר מדובר ב"לימוד המכונה" בנוגע לטכנולוגיות של בינה מלאכותית.

בנוגע למידע רפואי: המידע נוצר במהלך הטיפול הרפואי, נעשה בו שימוש, אבל המידע מוסיף להצטבר במהלך הטיפול (בדיקות נוספות, הטיפול עצמו, הערכת ההצלחה של הטיפול בדרך של בדיקות נוספות), ומוזן שוב לתוך מערכת המידע. אין פה פעולה חד-פעמית, אלא תהליך נמשך.

(ב) מידע קטן, בינוני, גדול, ועתק

בדיני הפרטיות במתכונתם המוכרת, כלומר שלושת מישורי הפעולה של הפרטיות הקלסית, המידעית והחוקתית, גלומות עוד הנחות בנוגע למספר השחקנים, גודל המידע, וממד הזמן.¹¹⁹

הפרטיות הקלסית מתייחסת ליחסים בין אדם אחד לאחר, ולמידע "קטן". בדרך כלל מדובר באירועים נקודתיים – צילום, פרסום מידע, שימוש לא מורשה במידע. לעיתים הפעולה הפוגענית נמשכת זמן מה, אבל היא מתוחמת.

הפרטיות החוקתית מתייחסת ליחסים בין אזרח למדינה. יש פה שני צדדים בלבד. לעיתים יהיה מדובר באזרחים רבים, אבל הם דומים בהקשר הנדון, ומולם ניצב שחקן אחד בעל מאפיינים משפטיים ברורים – המדינה. בממד הזמן, הפעולה יכולה להיות חד-פעמית (פעולת חקירה משטרתית) או נמשכת (למשל איכון השב"כ בתקופת הקורונה, לגבי כלל מחזיקי טלפון נייד במדינה).

הפרטיות המידעית מתייחסת למידע בהיקף בינוני עד גדול. מערך השחקנים הוא של אנשים רבים, כלומר נושאי המידע שהמידע על אודותיהם נכלל במאגר המידע, מול שחקן אחד, בעל השליטה במאגר המידע. המידע מוחזק בדרך כלל למשך זמן ארוך יותר. מאגרי המידע שבהם מדובר מוקנים, ולכן ניתן לנהל אותם, גם בהיבטי הפרטיות, למשל להסיר מידע מסוגים מסוימים. הכללים המשפטיים מבקשים להתמודד עם הגודל ומשך הזמן, וקובעים, למשל, חובות כלליות ונמשכות של סודיות ואבטחת מידע.

נתוני עתק אינם מתאימים להנחות האלה. הם אינם בבחינת "עוד מאותו דבר". מדובר במידע בהיקפים גדולים, ממגוון מקורות – כלומר אין מדובר בשני שחקנים זה מול זה (שני אנשים, אזרח מול המדינה, או נושא מידע מול בעל השליטה במאגר מידע), אלא בריבוי של בעלי שליטה במאגרים – לא רק קופת החולים, אלא גם הגוף שמקבל את המידע. המידע עובר ביניהם בכל מיני דרכים, לזמן ממושך. במקרים רבים, המידע שבו משתמשים כולל מידע ישן שזוכה לחיים חדשים. אופן העיבוד אינו מובנה. כל פיסת מידע עשויה להיות רלוונטית לניתוח של נתוני עתק. החשוב הוא שהמידע מתויג – כלומר שאנחנו יודעים אם מדובר בנתון שהוא שם, אבחון רפואי, מצב כלכלי וכדומה.

נתוני עתק רפואיים ממחישים את ההבדלים האלה. כוחם הוא בהיקף העצום, שמתייחס למגוון אנשים, שנאסף ומעובד באופן נמשך, בלי התחלה או סיום ברורים של השימוש במידע.

(ג) מְזַעֵר מידע?

השימוש בנתוני עתק מבוסס על עיבוד מידע בהיקף ניכר. כל פרט מידע מוזמן להיכנס לחומרי הגלם, הרי אחת ההבטחות של עיבוד נתוני עתק היא איתור קשרים בין נתונים, שלא נצפו קודם על ידי עין אנושית. ייתכן שעיבוד הנתונים יחשוף את העובדה שיש מתאם בין נתון מסוג אחד לנתון מסוג אחר שאיש לא העלה על דעתו לבחון

¹¹⁹ להערות תמציתיות בנושא, ראו Michael Birnhack, *S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm*, BIG DATA AND PRIVACY: MAKING ENDS MEET 7 (Future of Privacy Forum, 2013).

קודם לכן. משמעות המתאם עדיין תהיה טעונה בירור (מחקרי או עסקי). כל זה תקף גם לגבי נתוני עתק רפואיים.

לעומת זאת, אחד העקרונות של דיני הפרטיות המידעית הוא של מזעור מידע: יש לאסוף ולעבד רק את מינימום המידע שדרוש לתכלית הלגיטימית שלשמה נאסף המידע מלכתחילה. מכאן ההתנגשות הישירה בין נתוני עתק לפרטיות המידעית:¹²⁰ המחקר תובע עוד ועוד מידע מבלי שעורכי המחקר יכולים לומר מהי בדיוק מטרתו (מעבר לאמירה הכללית: לצורכי מחקר), ואילו עקרון מזעור המידע מבקש להגביל את איסוף המידע ועיבודו רק למה שנחוץ למימוש התכלית המוגדרת.

לעיקרון המזעור יש מופעים ישירים בדין האירופי.¹²¹ בדין הישראלי, לפני ואחרי תיקון 13 לחוק, אין התייחסות ישירה לעיקרון זה, למעט בתקנות שעוסקות בהעברת מידע מגופים ציבוריים,¹²² בתקנות שעוסקות במידע שמגיע לישראל מהאיחוד האירופי,¹²³ וכן באופן משתמע, בתקנות בדבר אבטחת מידע.¹²⁴ אולם אין פירוש הדבר שהכול מותר. בעל השליטה במאגר מידע שאוסף מידע צריך להודיע לנושא המידע על איסוף המידע (לפי סעיף 11 לחוק) ולקבל את הסכמתו מראש, וזו צריכה להיות הסכמה מדעת. הודעה כללית, שלפיה המידע ישמש לכל מטרה שהיא, גם אם תהיה חתימה ברורה של נושא המידע בצידה, תהיה הודעה חשודה, וההסכמה לפיה תהיה חשודה עוד יותר. הסכמה גורפת לכל פעולה חושפת את העובדה שתכלית האיסוף אינה ברורה דיה, ושיש בה משום ויתור גורף על הזכות לפרטיות. אילו כל זה היה מותר, לא היה צורך ברוב רובם של דיני הפרטיות המידעית. בעלי שליטה במאגרים היו מנסחים הודעה כוללת, דורשים "הסכמה", וידם הייתה חופשית.

במישור הפרטיות החוקתית, עקרון מזעור המידע נובע ממבחני המשנה של עקרון המידתיות. צריך להיות קשר בין האמצעי למטרה ("מבחן ההתאמה"), תוך בחינת חלופות פוגעניות פחות ("מבחן הצורך"), ובאופן שהיתרון עולה על הנזק לזכות היסוד ("מבחן המידתיות הצר").¹²⁵ שילוב מבחני המשנה דומה לעיקרון של מזעור המידע. הדין החוקתי חל במישרין על גופים ציבוריים, וגם על גופים דו-מהותיים (לענייננו, בתי חולים וקופות חולים נכללים בשתי הקבוצות האלה), ובאופן עקיף, על גופים פרטיים.

(ד) תכלית השימוש וצמידות מטרה

בדיני הפרטיות המידעית, תכלית האיסוף של המידע והשימושים בו היא נקודת מוצא הכרחית. בעל השליטה במאגר המידע חייב לפרט את המטרות שלשמן ישמש המידע, לפני איסוף המידע. על בסיס זה ניתנת ההסכמה (מדעת) ומרצון חופשי, ועל בעל השליטה מוטלת החובה שלא לחרוג מהמטרות – חריגה תפר את עקרון צמידות המטרה.¹²⁶

פעמים רבות קורה שלאחר שמידע נאסף למטרה אחת, מתברר שאפשר להשתמש בו למטרות נוספות. למשל, במוסדות להשכלה גבוהה נוצר מידע על אודות סטודנטים, שנועד לשמש לניהול הלימודים שלהם – קבלה, עמידה בדרישות התואר וכדומה. אפשר להשתמש במידע גם כדי לזהות סטודנטים חלשים או קבוצות

¹²⁰ ראו גם Zarsky, *Incompatible*, לעיל ה"ש 118, בעמ' 1010–1011, שמסיק מכך שיש לצמצם את עקרון מזעור המידע כדי לאפשר שימוש בנתוני עתק.

¹²¹ ראו למשל בהערות הפתיחה (recital) 78 ו-156 של ה-GDPR, ובסעיף 5(1)(c) שם, שלפיו, המידע האישי צריך להיות "adequate, 'relevant and limited to what is necessary in relation to the purposes for which they are processed'".

¹²² תקנה 6 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986.

¹²³ תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג–2023, סעיף 3 (חובה למחוק מידע שאינו נחוץ עוד למטרות שלשמן התקבל); סעיף 4 (הגבלת ההחזקה של מידע שאינו נחוץ עוד).

¹²⁴ לפי ס' 2 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017 (להלן: "תקנות אבטחת מידע"), בעל מאגר מידע צריך לחבר מסמך הגדרות למאגר, שכולל בין היתר את מטרות השימוש במידע, עליו לעדכן את המסמך אחת לשנה, ולבחון "אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר." (סעיף 2(א)). אין זו חובת מזעור מראש, אלא חובה שוטפת.

¹²⁵ לדיון במבחן המידתיות בהיבט הפרטיות, ראו בירנהק, **פרטיות חוקתית**, לעיל ה"ש 8, בעמ' 412–421.

¹²⁶ לעקרון צמידות המטרה יש כעת כמה מופעים בדין. האחד הוא בפרטיות הקלסית, בסעיף 9(2), שלפיו "שימוש בידיעה על ענייני הפרטים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה", הוא פגיעה בפרטיות. לפני תיקון 13 העיקרון הופיע גם בפרק שעוסק בפרטיות מידעית, ושם השימוש נצמד למטרה שנרשמה בקשר למאגר המידע, אצל רשם מאגרי המידע. לפי סעיף 8(ב) בנוסחו הקודם: "לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר". תיקון 13 צמצם את חובת הרישום (סעיף 8א), ובהתאם, נוסח סעיף צמידות המטרה מחדש. סעיף 8(ב) קובע כעת "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין".

אוכלוסייה שמתקשות בלימודים. המטרה מבורכת, אבל היא שונה מהמטרה המקורית של איסוף המידע. במקומות עבודה, חישבו על מידע שנאסף לצורך זיהוי בכניסה למפעל כדי למנוע גישה של מי שאינם מורשים. האם ניתן להשתמש במידע הזה לצרכים משמעותיים מול עובדים? זו מטרה שונה. הדין האירופי מאפשר מרחב תמרון מסוים – כל עוד השימוש השני תואם (compatible) למטרה הראשונה, אפשר להתייחס לכך כאל אותה מטרה.¹²⁷ בדין הישראלי אין התייחסות מפורשת לעניין זה, אבל אפשר להגיע לתוצאה דומה בדרך של פרשנות. למשל, בדוגמת המידע שנוצר במוסדות להשכלה גבוהה, אפשר לומר שאיתור סטודנטים שמתקשים הוא חלק מהמטרה הראשונית, או גרסה קרובה של המטרה של הצלחת התלמידים בלימודים. הפרשנות צריכה לבחון את שתי התכליות ולהשוות ביניהן כדי לראות אם השימוש השני נכלל או דומה לראשון, או שיש שוני מהותי ביניהם.¹²⁸

בנוגע למידע רפואי, ראינו שהמידע שבידי קופות החולים נאסף בראשיתו כדי לייעל את ניהול המערכות בקופת החולים, ובכל מקרה, המידע נאסף לצורך הטיפול הרפואי. שימוש במידע לצרכים אחרים, למשל מסחר, אינו תואם למטרה הראשונה, ולכן הוא אסור. שימוש מחקרי במידע מותר, אולם לא משום שזו אותה מטרה, אלא משום שהחוק מרשה זאת במפורש, בתנאים מסוימים, לפי הוראות שקבע שר הבריאות ובאופן מותמם, כל זה לפי סעיף 20(א)(7) לחוק זכויות החולה.

(ה) הסכמה?

כאשר השימוש שצפוי במידע שנאסף אינו ידוע מראש, כלומר כאשר התכלית אינה מוגדרת בצורה ברורה, קשה לדעת למה בדיוק הסכים נושא המידע. האם הסכים שהמידע ישמש רק לתכלית אחת? לתכליות נוספות? האם הסכים שהמידע יעובד? שיועבר לגורמים אחרים? כמו עקרון צמידות המטרה, ההסכמה תלויה קשר הדוק בתכלית שלשמה נאסף המידע. אזכיר, שההסכמה בדיני הפרטיות ובדיני הבריאות צריכה להיות מדעת ומרצון חופשי. האם ניתן להתגבר על כך בדרך של הסכמה כללית (בנוסף "כל שימוש מחקרי")? אני סבור שההסכמה כללית אינה ממלאת את התנאים של "מדעת" ו"רצון חופשי".¹²⁹

פתרון אחד יכול להיות הסכמה מדורגת. למשל, בהקשר הרפואי, המטופל יסכים לאיסוף המידע ועיבודו למטרת הטיפול הרפואי, ובנפרד, תוצג לו בקשה להסכמה לשימוש מחקרי במידע, באופן ברור ובהיר, שאינו כורך בין שתי ההסכמות. את השימוש המחקרי אפשר לפרט במידה מסוימת. למשל, אפשר לפנות למטופלות ולבקש את הסכמתן שהמידע שנוצר אגב הטיפול בהריון, ישמש למחקר בנושא איתור מומים אצל עוברים. תיאור כזה הוא עדיין רחב, אבל צר יותר מאשר "כל שימוש מחקרי". באופן כזה, המטופלת תוכל להחליט האם היא מסכימה. למשל, אם ייאמר למטופלת שהמידע ישמש לקידום טכניקות להפלה מלאכותית, עשויות להיות נשים שיסרבו לשתף פעולה בשל התנגדותן העקרונית להפלות כאלה.

(ו) התממה: פתרון קסם או מקסם שווא?

לאור הקשיים בסוגיות מזעור המידע, הגדרת התכלית, ההודעה, ההסכמה וצמידות המטרה, מחקרים רפואיים בנתוני עתק נתלים בהתממה כפתרון קסם שפוטר אותם מהכפיפות לדיני הפרטיות, ובמידה רבה, גם מכללי האתיקה במחקר. זהו גם הדין בישראל, לפי נוהל של משרד הבריאות.¹³⁰ הטענה פשוטה: החוקרים ממילא אינם מתעניינים בזהותו של אדם אחד מתוך מאות האלפים שנכללים במאגר המידע שמשמש למחקר, אלא בזיהוי קשרים, מגמות, ודפוסים, כדי להפיק תובנות כלליות ותחזיות. בשלב פרסום המחקר ממילא לא יציינו את שמותיהם של נושאי המידע. בכך הם עומדים בדרישה של חוק זכויות החולה שראינו לעיל.¹³¹ אם כך, אין, לפי הטענה הזו, פגיעה בפרטיות, ומשום כך, אין מידע שצריך למזער, אין צורך להגדיר את התכלית ולבקש את הסכמת נושאי המידע.¹³² לפי גישה זו, התממה המידע משנה את הסטטוס של האדם מ"מטופל" ל"נושא מידע"

¹²⁷ ראו סעיף 5(1)(b) ל-GDPR, וביקורת אצל Zarsky, *Incompatible*, לעיל ה"ש 118, בעמ' 1006.

¹²⁸ לדיון והצעה לגישה הפרשנית המתאימה, ראו בירנהק ורחום-טוויג, **פרטיות מידעית**, לעיל ה"ש 21, בעמ' 213–214.

¹²⁹ ראו לעיל ה"ש 54, 99, 104.

¹³⁰ חוזר שימושים משניים, לעיל ה"ש 104.

¹³¹ סעיף 20(7) לחוק זכויות החולה קובע שמסירת מידע רפואי מותרת, כאשר היא "נועדה לפרסום בבטאון מדעי, למטרות מחקר או הוראה בהתאם להוראות שקבע השר ובלבד שלא נחשפו פרטים מזהים של המטופל".

¹³² בצד זה, גם מצדדי ההתממה יסכימו שהם כפופים לאישור תת ועדת הלסינקי, ושם נדרש פירוט של מטרת המחקר בכללותו.

תוך דילוג על המשוכה של ההסכמה. מתוסף פה שיקול פרקטי: איסוף הסכמות של נושאי מידע בהיקפי ענק, לפעמים מילוני אנשים, יקר ומסורבל.

האמנם? האם ההתממה פוטרת את המשתמשים בנתוני עתק מהוראות הדין? בעבר, משפטנים נטו להשיב בחיוב, אולם הידע שנצבר בנושא בתחום מדעי המחשב חלחל לשיח המשפטי, וכיום, התשובה נוטה לשלילה.¹³³

שאלה ראשונה שיש לבחון היא עובדתית: האם המידע באמת ובתמים מותמם? כאשר המידע נאסף מלכתחילה באופן אנונימי, למשל מערכת שסופרת כמה אנשים נכנסים לבית חולים במהלך היממה בלי איסוף פרט נוסף כלשהו – האיסוף חומק בהצלחה מתחת לרדאר המשפטי. המידע אינו ניתן לזיהוי. אבל מידע רפואי רגיל נוצר באופן מזוהה, במהלך הטיפול הרפואי. גם אם נמחק מזהים ישירים כמו שם ומספר תעודת זהות, האם עדיין אפשר לזהות את המטופל מתוך המידע, ומה צריך לעשות לשם זיהוי כזה? במילים אחרות, השאלה היא האם ניתן לזהות את האדם מחדש בדרך של הנדסה חוזרת (reverse engineering) של המידע הקיים, מתוך עצמו או בהצלבה עם מאגרים נגישים אחרים?¹³⁴

הדין האמריקני נוקט גישה של כלל, שמבקש להשיג ודאות יחסית. הדין הפדרלי שעוסק בשימושים במידע רפואי (HIPAA) קובע רשימה של שמונה עשר נתונים מזהים, שאם הוסרו, המידע ייחשב למותמם.¹³⁵ המזהים כוללים שם, כתובת, תאריכים כמו יום הולדת, מועד אשפוז או פטירה, מספרי טלפון, כתובת דוא"ל, מספרים מזהים כמו מספר הביטוח הלאומי, מספר התיק הרפואי או חשבונות בנק, מספרי רכב, כתובת IP, ומידע ביומטרי.¹³⁶

הדין האירופי, ובעקבותיו, גם הדין הישראלי בתיקון 13, מגדירים "מידע אישי" לפי האפשרות לזהות את האדם. ההגדרה בסעיף 3 לחוק הישראלי מסבירה: "מידע אישי" – נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזוהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי".

בהתאם, האפשרות לזיהוי מחדש אינה עניין בינארי, והחוק מתייחס למידת המאמץ הדרושה לשם כך.¹³⁷ ככל שנדרשים יותר משאבים – תחכום טכנולוגי, גישה למאגרי מידע נוספים שאינם פומביים ואינם בהישג כל, זמן ועלויות – ניטה למסקנה שהמאמץ הדרוש לזיהוי מחדש חורג מגדרי המאמץ הסביר. ככל שקל, פשוט וזול יותר לפצח את המידע המותמם-לכאורה ולזהות את נושאי המידע, ניטה למסקנה שהמאמץ הדרוש לזיהוי מחדש סביר, ולכן נתייחס למידע כאל מידע מזוהה. אפשרות הזיהוי מחדש אינה עניין סטטי, והיא משתנה לפי היכולות הטכנולוגיות הזמינות למי שמנהל את המידע, וגם לגורם העוין שמנסה להשיג את המידע. יש מידע שכיום ייחשב אנונימי, משום שלשם הזיהוי מחדש צריך לגשת למאגר אחר שאינו נגיש, ולהצליב מידע, אבל מחר, המאגר האחר יוגש (ביוזמת בעליו או בגלל דליפה או פריצה למאגר, ואין זה משנה מדוע לעניין הערכת המאמץ שדרוש לזיהוי מחדש). או שהיכולות הטכנולוגיות שנדרשות כיום לזיהוי מחדש יקרות, ובהמשך, המחיר שלהן ירד משמעותית, כפי שקורה לא אחת עם טכנולוגיות חדשות. בפועל, יש אינספור דוגמאות למצבים שבהם מידע מותמם לכאורה זוהה מחדש.

שאלה שנייה היא משפטית-עקרונית. מצדדי ההתממה מדגישים את השלב האחרון של מהלך החיים של המידע – שלב פרסומו ברבים. אכן, פרסום מידע רפואי על אדם מזוהה ללא הסכמתו פוגע פגיעה קשה בפרטיותו, והדין

Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010).¹³³

¹³⁴ לאתגר זה, ראו שרון בר-זיו וטל ז'רסקי "פרטיות במשבר זהות: אסטרטגיות הסדרה בעידן ההתממה" **משפט חברה ותרבות ב** 125 (מיכאל בירנהק עורך, 2019).

¹³⁵ ההנחיה מכונה Privacy Rule, והותקנה לפי ה-Health Insurance Portability and Accountability Act of 1996. ראו 65 F.R. 82462. לביקורת הדין האמריקני בנושא התממת מידע רפואי, ראו 71 DUKE L.J. 985 (2022) Stacey A. Tovino, *Not So Private*.

¹³⁶ 45 C.F.R. § 164.514(b).

¹³⁷ ההגדרה הישראלית שונה במעט מהדין האירופי. סעיף 1(4) ל-GDPR שקובע את ההגדרה של מידע אישי שותק בעניין, אבל הערת הפתיחה 26 מזכירה "אמצעים סבירים" שצריך כדי לזהות מחדש אדם, להבדיל מ"מאמץ סביר" בדין הישראלי.

מתייחס לכך.¹³⁸ גם דליפה של מידע ממאגר מידע מפרה את חובת הסודיות או את חובת אבטחת המידע.¹³⁹ לכן, הדגש על שלב פרסום המידע מובן.

אבל, ההתמקדות בשלב פרסום המידע מצמצמת את הפרטיות לחולייה האחרונה במהלך החיים של המידע, ומחמיצה את השלבים הקודמים: איסוף המידע, עיבודו, והשימוש בו.¹⁴⁰ ראינו שהחוק משקף את התפיסה של מהלך החיים של המידע, הן ברשימת הפעולות שהן בגדר "פגיעה בפרטיות" במסגרת הפרטיות הקלסית, והן באוסף הזכויות והחובות בנוגע למידע אישי, במסגרת הפרטיות המידעית. איסוף מידע ללא הסכמה חותר תחת ההצדקות של הזכות לפרטיות, למשל במעגל היחיד. אדם שמצולם ללא רצונו – נפגע מעצם פעולת הצילום, שמתעלמת מהמצולם, מרצונו ומכבודו, והופכת אותו מסובייקט לאובייקט, גם אם בשימוש הסופי פניו יטושטשו. שימוש במידע בלי לשאול את האדם אם הוא מסכים לכך הוא שימוש באדם עצמו. העברת מידע לגורם אחר מתעלמת מרצונו של נושא המידע – אולי היה מסכים להעברה אילו נשאל, אבל אם לא נשאל, ממילא לא ניתנה לו האפשרות לשלוט במידע על אודותיו. הבנת הפרטיות כשליטה, שמשקפת את ההצדקות הרבות של הפרטיות, מספקת לנו אמת מידה לבחינת הפעולות בהן מדובר.

מצדדי ההתממה כפתרון קסם אוחרים בפסק דין של בית המשפט העליון, במקרה שבו נעשה שימוש משפטי במידע רפואי מותמם.¹⁴¹ דובר בתביעת נזיקין בשל רשלנות רפואית. עד מומחה של אחד הצדדים הציג בעדותו מסמכים רפואיים של מטופל אלמוני, כדי להמחיש את אופן הטיפול שהיה ראוי במקרה שנדון. נתוניו של המטופל האחר הושחרו. השופטת וילנר מצאה שאין פגיעה בפרטיות:

"במקרה כזה, בו הציבור שנחשף למידע הרפואי אינו יכול לקשור בין המידע המוצג לבין אדם ספציפי, פרטיותו של אותו אדם אינה נפגעת, שכן ללא האפשרות להצביע על זהות המטופל, איש לא חודר למרחב האישי שלו. המידע הרפואי נותר תלוש מהקשר ובלתי-קונקרטי, ומשכך הצגתו אינה מפירה את החיסיון הרפואי או את זכותו של המטופל לפרטיות."¹⁴²

חשוב לשים לב: פסק הדין עסק במסירת מידע על המטופל האלמוני, כלומר בשלב הפרסום של המידע. אכן, השחרת הפרטים – התממה בדרך אנלוגית פיזית – הייתה אפקטיבית, ולא הייתה בגדר פרסום מידע רפואי על המטופל האחר. משום כך, אפשר לומר שלא הייתה פגיעה בפרטיות בדרך של פרסום מידע הנוגע למצבו הבריאותי של אדם (לפי סעיף 11(2) לחוק). אולם השופטת לא הסתפקה בכך. היא העירה שיש ממש בטענת המשיב באותו הליך, שהפגיעה בפרטיות נעשתה בשלב מוקדם יותר, כאשר העד המומחה חיפש את המידע במאגרי בית החולים.¹⁴³ בקשר לפגיעה מוקדמת זו, הורתה השופטת, על הערכאה הדיונית לשקול האם לקבל את הראייה, לפי שיקול הדעת שמסור לבית המשפט בסעיף 32 לחוק הגנת הפרטיות.¹⁴⁴ במילים אחרות, פסק הדין מבהיר שהתממה נאותה מאיינת את הפגיעה בפרטיות בשלב פרסום המידע, אבל לא בהכרח מאיינת פגיעות אחרות בפרטיות בשלבים המוקדמים של מהלך החיים של המידע.

אם כך, כדי להשתמש במידע שנאסף בצורה מזוהה והותמם יש להצביע על עוגן חוקי מתאים שמתיר שימוש כזה. התממת המידע בשלב הפרסום פוטרת את המפרסם מפגיעה בפרטיות לגבי אותו שלב בלבד, אך לא לגבי שלבים מוקדמים במהלך החיים של המידע.¹⁴⁵ מהו עוגן חוקי מתאים? באיחוד האירופי יש עוגן כזה בחקיקה

¹³⁸ סעיף 11(2) לחוק קובע שפרסום מידע הנוגע למצב בריאותו של אדם הוא פגיעה בפרטיות. סעיף 19 לחוק זכויות החולה קובע חובת סודיות רפואית.

¹³⁹ לפי סעיפים 16, 17 לחוק. חובת הסודיות חלה על מי שיש להם גישה למידע, וההפרה היא בדרך כלל כאשר הם מתרשלים בשמירה על הסודיות, או חלילה מדלפים באופן מכוון. אבטחת מידע מכוונת למנוע פריצה מבחוץ. עם זאת, הגבול בין שתי החובות פחות חד, ועשויים להיות מצבים שהם הפרה של שתיהן גם יחד.

¹⁴⁰ הרחבתי על כך במקום אחר: Birnhack, *A Process-Based Approach*, לעיל ה"ש 103.

¹⁴¹ עניין הסתדרות מדיצינית הדסה, לעיל ה"ש 68.

¹⁴² שם, בפס' 14.

¹⁴³ שם, בפס' 26.

¹⁴⁴ שם, בפס' 28, 30.

¹⁴⁵ בית הדין האירופי לצדק פיצל את האפיון המשפטי של מידע, לפי היכולת של מי שמחזיק בו לזהות את נושאי המידע. כאשר המידע היה פסבדונימי, כלומר הוסרו מזהים ישירים, אבל בידי המחזיק היה מפתח שאפשר זיהוי מחדש – המידע נחשב ל"מידע אישי",

עצמה.¹⁴⁶ כאמור לעיל, בדין הישראלי, כיום, חוק זכויות החולה מתיר מסירת מידע מותמם לגורם אחר במצבים מסוימים, ובין היתר למטרות מחקר והוראה, לפי הוראות שר הבריאות. בהתאם, חוזר מנכ"ל משרד הבריאות קובע שמחקר במידע מותמם יכול לקבל פטור מהחובה לקבל הסכמה של נושאי המידע.¹⁴⁷ עוגן שני שעשוי להכשיר את השימוש במידע גם בשלבים הקודמים, עוד לפני פרסום המידע, הוא הסכמת נושא המידע. ההסכמה צריכה להתייחס גם לפעולת ההתממה. החוק מגדיר (כיום, לאחר תיקון 13) את פעולת העיבוד בצורה רחבה: "כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו". הגדרה רחבה זו ("כל פעולה"), מובאת בחוק על דרך ההדגמה ("לרבות"), כוללת גם את פעולת ההתממה.

כל זה לא נועד להפחית מחשיבות ההתממה: היא אמצעי חשוב שממזער את הפגיעה בפרטיות בשלבים מסוימים של מהלך החיים של המידע. יש חשיבות לשאלות כמו מי מתמים (מוטב גורם שהמידע נמסר לו בהסכמה), מתי (מוטב מוקדם ככל האפשר), ומה אופי ההתממה, וכאן יש שיטות שונות שמשתכללות כל העת. אולם פרסום מידע מותמם אינו פתרון קסם שמאפשר לחמוק מכל דיני הפרטיות, ועלול להיות מקסם שווא: המשתמש עדיין חב בחובות בקשר לשלבים המוקדמים של איסוף המידע ועיבודו. ספק עם חוזר שהפיץ מנכ"ל משרד הבריאות יכול להתגבר על חובות שיש בחקיקה הראשית. השלב הבא הוא השימוש המתגבר בבניה מלאכותית בעולם הרפואה, לא רק במחקר.

(ז) סיכום ביניים

סעיף זה הציג שורה של אתגרים שנתוני עתק מציבים לפני הזכות לפרטיות בכלל, ותפיסת הפרטיות כשליטה בפרט. הצבעתי על ההיגיון הלינארי של הדין מול מעגליות העיבוד של המידע, על כך שהיקף המידע מאתגר את הגדרות הדין שמותאם למידע בהיקפים קטנים בהרבה, את הקושי ביישום עקרונות יסוד של דיני הפרטיות כמו עקרון מזעור המידע, הגדרה ברורה של תכלית עיבוד המידע, ועקרון צמידות המטרה. ראינו את הקושי ביישום ההסכמה כאשר מטרת השימוש אינה מוגדרת, ואת מקסם השווא של ההתממה.

כיצד, אם כן, יכולה תפיסת הפרטיות כשליטה לסייע כאן? התשובה טמונה במימד הזמן. השליטה צריכה להתמשך לאורך כל מהלך החיים של המידע. אין לוותר על מפגשים קיימים או יצירת מפגשים נוספים בין נושא המידע לבין המידע האישי שעל אודותיו שמוחקר אצל אחרים, ויש לחזק את כל נקודות המפגש האלה: את שלב ההסכמה יש לחזק, למשל בדרישה ליידוע מפורט יותר תוך שמירה על בהירותו, על צורת מתן ההסכמה (בדרך של opt in שעדיפה על פני צורה של opt out). יש ליצור מנגנונים טכנולוגיים ומשפטיים שיאפשרו מחיקת מידע, ועוד. אין פה פתרון קסם, והמלאכה רבה.

גישה אחרת היא שהמחוקק יקבע איזון עקרוני, שבו יאוזנו צורכי המחקר והגנת הפרטיות, תוך נקיטת אמצעים מידתיים שונים. כך נקבע ב-GDPR באיחוד האירופי.¹⁴⁸ המחוקק האירופי החריג שימושים מסוימים שיש להם ערך ציבורי מתחולת הרגולציה, אולם תוך קביעת אמות מידה כלליות למיתון הפגיעה בפרטיות. מהלך כזה מותאם למסגרת החוקתית הישראלית, שבה בצד הזכות לפרטיות מותרת הפגיעה בה, לפי כללי פסקת ההגבלה

והדין חל עליו; לעומת זאת, כאשר המידע הפסבדונימי הועבר לצד שלישי, ללא המפתח, ולמקבל המידע לא הייתה דרך לזהות מחדש את נושא המידע, הרי שבידיו, המידע לא נחשב לניתן לזיהוי, ולכן לא היה בגדר "מידע אישי". המשמעות המעשית היא שמקבל המידע פטור מחובות החוק. ראו *EDPS v. SRB*, C-413/23 P, ECLI:EU:C:2025:645 (4 September 2025). עמדה זו משקפת התייחסות לשלבים השונים בחיי המידע, ולכך שבידיים שונות, בשלבים שונים, יכולה להיות פגיעה בפרטיות אך לא בהכרח בשלבים אחרים.

¹⁴⁶ סעיף 89 ל-GDPR.

¹⁴⁷ חוזר שימושים משניים, לעיל ה"ש 104.

¹⁴⁸ סעיף 89 ל-GDPR, קובע כך:

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

שבחוק היסוד. בחוק זכויות החולה יש החרגה מסוימת של העברת מידע לצורכי מחקר, אולם ההחרגה צרה יותר מאשר ב-GDPR (שם ההחרגה אינה עוסקת רק בהעברת המידע), והמגבלות על ההעברה עמומות יותר, ויש בהן הסתמכות יתר על התממה.

ג. בינה מלאכותית בשירות הרפואה

בעוד שנתוני העתק נכנסו בצעד מתון למערכת הרפואית וסימנו כיוונים חדשניים ומבטיחים למחקר, הבינה המלאכותית הופיעה בסערה, ובעת הזו, נראה שהיא עומדת לשנות את המערכת באופן רדיקלי – לא רק במחקר, אלא גם בטיפול הרפואי, על שלביו השונים.

לבינה המלאכותית הגדרות רבות, ולא זה המקום להכריע בהן.¹⁴⁹ לצורך הדיון הנוכחי, אתייחס לבינה מלאכותית כטכנולוגיות שונות ומגוונות לעיבוד מידע אישי: על בסיס חומרי גלם שהוזנו לטכנולוגיות אלה ועובדו באמצעותן, ניתן לזהות דפוסים כלליים וליישם ליחידים. בהתאם, בטכנולוגיות בינה מלאכותית יש קלט – המידע הגולמי שמוזן למערכת המחשוב ומעובד בה, ובדרך כלל מדובר בנתוני עתק. במטפורה המאנישה, זהו השלב של "אימון המכונה". שלב העיבוד הוא של "לימוד המכונה".

אחרי האימון, הלימוד, והעיבוד, מגיע שלב הפלט. למשל, אם המכונה הוזנה בנתונים על גובה, צבע שיער, וגיל, העיבוד עשוי לזהות מתאמים כלשהם בין הנתונים. כעת נשאל לגבי אדם מסוים, ונמסור רק את אחד הנתונים, למשל את גובהו. המערכת תדע לשער את צבע השיער ואת הגיל, בהסתברות מסוימת. דוגמה מופרכת זו מכוונת להראות שהמכונה פועלת לפי המידע שהוזן לה, ומזהה מתאמים ולא דווקא סיבתיות. המתאמים עשויים להיות חסרי משמעות. אבל, במקרים אחרים, השימושים יכולים להיות מועילים, למשל, זיהוי העדפות. כאשר שירות מקוון מציע לנו מוצר או שירות מסוימים (ספר באמזון, המלצת צפייה בנטפליקס, וכדומה), ההמלצות בדרך כלל קולעות היטב לטעמנו. ההמלצה מבוססת על היסטורית הרכישות והעיון שלנו באתר, תוך השוואה למה שאנשים אחרים, שדומים לנו בתחומי העניין, רכשו.¹⁵⁰ ההמלצה עצמה משפיעה על ההתנהגות – אנחנו עשויים לצפות בסרט משום שהמערכת המליצה עליו, גם אם אחרת לא היינו צופים בו.

אחרי שאיתרו דפוסים נפוצים, מערכות בינה מלאכותית יודעות לזהות חריגים וסטיות. גם השימוש הזה מוכר זה מכבר, עוד לפני ההתלהבות הנוכחית מהבינה המלאכותית, למשל בנוגע לשימוש בכרטיסי אשראי. חברות האשראי אוספות נתונים על הלקוחות ועל פעילותם, על כל לקוח בנפרד (לשם ביצוע הפעולה הכספית) ועל כולם ביחד, וכך הן יודעות לזהות שימוש חריג שעשוי להדליק נורה אדומה. אם יש עסקה בסכום גבוה מהממוצע של הלקוח, שנערכה בשעת לילה, במדינה אחרת שבה הלקוח לא ביקר מעולם, הסטייה תבלוט, וחברת כרטיסי האשראי תחסום את הכרטיס ותפנה ללקוח לבירור. גם כאשר יש עסקה בסכום שגרתי, לא גבוה במיוחד, לחנות מקוונת כלשהי, המערכת עשויה לזהותה כניסיון לגניבה והונאה.

התיאור של מערכת בינה מלאכותית כשלבים נפרדים (קלט, עיבוד, פלט) נועד לצורך הבהירות, אבל תהליכיה של הבינה המלאכותית אינם לינאריים – ההזנה, האימון והלימוד מעגליים. שוב, בהמשך למטפורה האנושית, כמו האדם, המכונה מוסיפה ללמוד כל הזמן, גם תוך כדי השימוש.

ומה באשר לפרטיות? שימושים רבים של הבינה המלאכותית אינם עוסקים כלל במידע אישי; נתוני מזג אוויר מצטברים יכולים ללמד על שינויים אקלימיים ולזהות בצורת או סערה. באלה אין היבטי פרטיות. כאשר מדובר במידע אישי, וכאשר נבחן את הדברים באופן מדורג לפי השלבים במהלך החיים של המידע, נראה שיש סוגיות שכבר מוכרות לנו. למשל, שלב הקלט מוכר: המידע האישי שמוזן למערכות לצורך האימון והלמידה הוא נתוני עתק. במובן הזה, הבינה המלאכותית אינה טכנולוגיה חדשה לגמרי, והיא ממשיכה ומתבססת על טכנולוגיות קודמות. בהתאם, כל אתגרי הפרטיות שנדונו בפרק הקודם מתקיימים גם באשר לבינה המלאכותית, ונוספים להם אתגרים חדשים. גם כאן אעיר על השימושים הרפואיים בבינה מלאכותית, ואבחן את אתגרי הפרטיות הייחודיים.

¹⁴⁹ ראו עמיר כהנא ותהילה שוורץ אלטשולר אדם, מכונה, מדינה: לקראת אסדרה של בינה מלאכותית 28–31 (2023); עמית חיים מהי בינה מלאכותית? לקראת הגדרה במשפט וברגולציה בישראל (טרם פורסם).

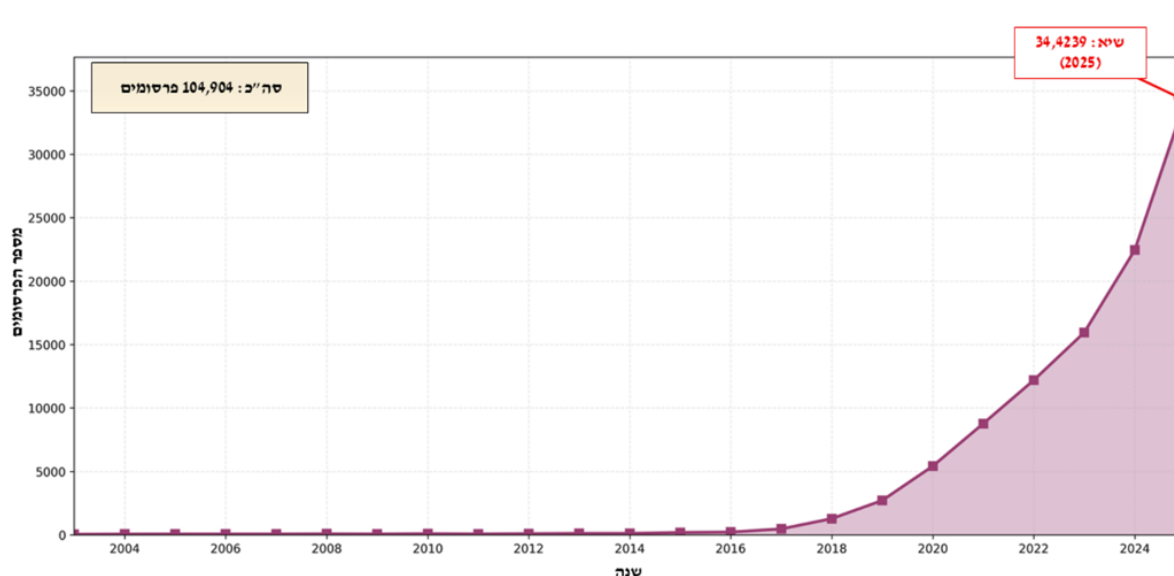
¹⁵⁰ להיבטי הפרטיות, ראו מיקי זר "אנשים שקראו מאמר זה התעניינו גם ב...": על הקשר בין פרטיות לפרופילינג" משפט חברה ותרבות ב 69 (מיכאל בירנהק עורך, 2019).

1. שימושים רפואיים בבינה מלאכותית

ההתלהבות מהבינה המלאכותית ניכרת בספרות המחקרית הרפואית. חיפוש בכותרות ותקצירים של מאמרים רפואיים של המונח Artificial Intelligence במאגר המאמרים הרפואיים PubMed מראה עלייה מעריכית דרמטית (עד לשנת 2025 ועד בכלל) עם 104,904 מאמרים, פי חמישה ויותר ממספר המאמרים בקשר לנתוני עתק בתקופה הזו.¹⁵¹

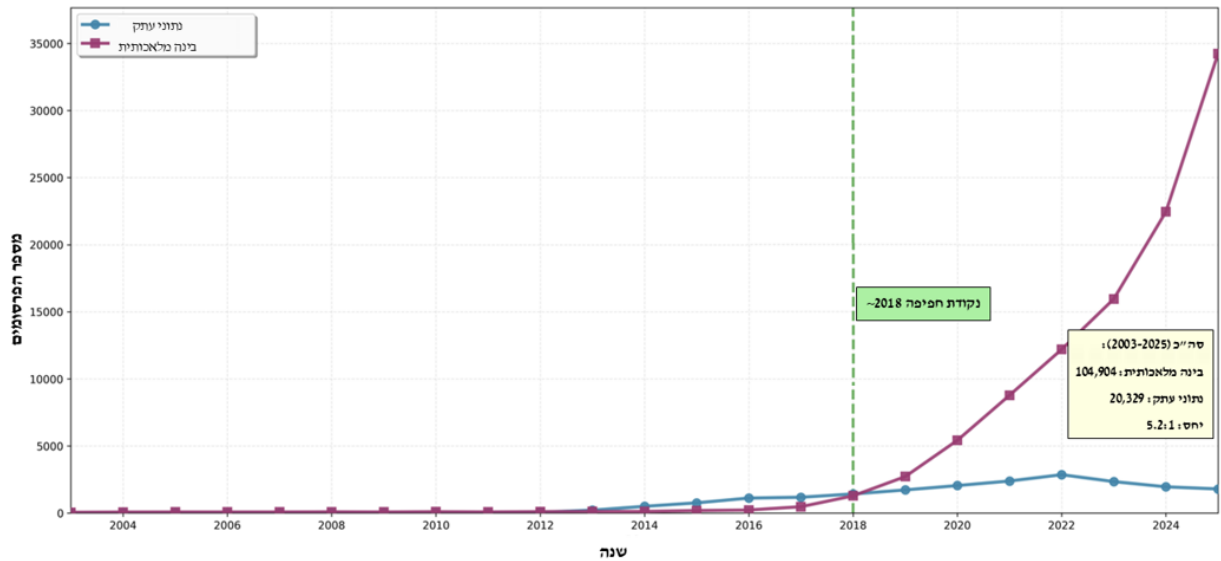
איור 2: מחקרים רפואיים בנושאי בינה מלאכותית 2003–2025

שמאזכרים "בינה מלאכותית" בכותרת או בתקציר המאמר



איור 3 משווה בין ההתפלגויות של המאמרים בנושא נתוני עתק לאלה בנושא בינה מלאכותית.

איור 3: מחקרים רפואיים בנושאי נתוני עתק ובינה מלאכותית 2003–2025



עיון אקראי במאמרים אלה מעלה שרבים מהם כורכים את נתוני העתק והבינה המלאכותית, ומתייחסים אליהם כשתי טכנולוגיות מצטברות.¹⁵² בעוד שעיקר השימוש בנתוני עתק הוא מחקרי – כיצד לזהות תופעות ולאחר מתאמים בין נתונים רבים ומגוונים, הרי שהחידוש העיקרי של הבינה המלאכותית הוא בשלב היישום, בהליך הרפואי עצמו. בעת הזו, היישומים הם לצרכים כמו פיענוח הדמיות (MRI, רנטגן וכדומה),¹⁵³ אבחון (דיאגנוזה), הערכת התפתחות המחלה (פרוגנוזה),¹⁵⁴ הצבעה על אפשרויות טיפול שונות,¹⁵⁵ ולפעמים מעורבות בטיפול עצמו. גם חוקרים ישראלים מעורבים במחקרים ופיתוחים בתחומים האלה, למשל פיתוח סטטוסקופ לזיהוי היצרות מסתם אבי העורקים,¹⁵⁶ איתור מהיר יותר של דימום תוך-גולגלתי,¹⁵⁷ או זיהוי מוקדם של כליאת כתפיים של עוברים בלידה.¹⁵⁸

כמו לגבי נתוני עתק, לטכנולוגיות הבינה המלאכותית יש יתרונות ברורים – אבחון מהיר יותר, מדויק יותר, ובמקרים רבים פולשני פחות, והתאמה טובה ויעילה יותר של שיטת הטיפול והמעקב. לכל אלה השלכה ישירה על בריאות הציבור ועל עלויות הטיפול למטופלים ולמשק בכלל.

וגם כאן יש חסרונות. חוקרים מצביעים על חסמים בהטמעת הטכנולוגיות במערכת הבריאות, כמו דרישות רגולטוריות, עלויות ראשוניות גבוהות, קושי לפענח את אופן הפעולה של האלגוריתמים (זו בעיית "הקופסה

¹⁵² למשל מחקר על שימושים אפשריים של נתוני עתק בנייתיים: Christopher Prien, Eddy P. Lincango, Stefan D. Holubar, *Big Data in Surgery*, 103(2) SURG. CLIN. N. AM. 219 (2023).

¹⁵³ למשל סקירת מחקרים שהתבססו על בינה מלאכותית לפיענוח הדמיות MRI בנוגע לאלצהיימר: Tory O. Frizzell et al, *Artificial Intelligence in Brain MRI Analysis of Alzheimer's Disease Over the Past 12 Years: A Systematic Review*, 77 AGING RESEARCH REV. 101614 (2022). המחברים הדגישו שהטמעת הבינה המלאכותית צריכה להיעשות בזהירות, בשקיפות, עם תיקוף ויכולת להכללה, דיוק ושימויות קלינית. שם, בעמ' 14.

¹⁵⁴ למשל סקירת מחקרים על אבחון ופרוגנוזה של שברים בעצם הירך: Johnathan R. Lex, et al, *Artificial Intelligence for Hip Fracture Detection and Outcome Prediction: A Systematic Review and Meta-analysis*, 6(3) JAMA NETWORK OPEN. e233391 (2023).

¹⁵⁵ למשל, טכנולוגיות לפענוח הדמיות של סרטן הריאה שמסייעות להתאים את הטיפול לחולה: Mitchell Chen, et al, *Radiomics and Artificial Intelligence for Precision Medicine in Lung Cancer Treatment*, 93 SEMINARS IN CANCER BIO. 97 (2023).

¹⁵⁶ Tamer Ghanayim et al, *Artificial Intelligence-Based Stethoscope for the Diagnosis of Aortic Stenosis*, 135(9) AM. J. MED. 1124 (2022).

¹⁵⁷ Daniel Ginat, *Implementation of Machine Learning Software on the Radiology Worklist Decreases Scan View Delay for the Detection of Intracranial Hemorrhage on CT*, 11 BRAIN SCI. 832 (2021).

¹⁵⁸ A. Tsur, *Development and Validation of a Machine-Learning Model for Prediction of Shoulder Dystocia*, 56 ULTRASOUND OBSTET. GYNECOL. 588 (2020).

השחורה", שאדון בה בהמשך), ופיקוח מצומצם בדיעבד.¹⁵⁹ חסרון נוסף של טכנולוגיות בינה מלאכותית הוא הטיות שונות, לפי הקלט שהוזן להן. זהו חסרון מוכר עוד מטכנולוגיות נתוני עתק. אם המידע אינו משקף את האוכלוסייה הרלוונטית, גם יכולות הזיהוי יהיו מוטות. חשש אחר, שמתייחס לשלב השימוש בטכנולוגיות כאלה, הוא הסתמכות-יתר של הרופאים על ממצאי הבינה המלאכותית במקום על הידע והניסיון שרכשו.

בדיונים הרפואיים על יתרונותיה של הבינה המלאכותית וחסרונותיה, הגנת הפרטיות נזכרת לעיתים רחוקות, ובדרך כלל בשולי הדברים או בצורה חלקית בלבד. למשל, מאמר שבחן את האפשרויות והאתגרים שיש בשימוש ב-ChatGPT בהקשרים רפואיים (בלימודים, במחקר ובשימוש בפועל) הצביע על חסרונות, בסדר הזה: הפרת זכויות יוצרים, אתגרים משפטיים אחרים, ופוטנציאל לאי-דיוק בתוצאות בשל הטיות בנתוני הקלט או בשל "הזיות" של הטכנולוגיה, כלומר המצאות שלה שאין להן אחיזה במציאות.¹⁶⁰ הגם שהמאמר עוסק בהיבטים אתיים, פרטיות נזכרת שם רק כבדרך אגב.¹⁶¹ סקירה אחרת של מחקרים שבחנו היבטי בינה מלאכותית בעולם הרפואה מציינת את הפרטיות כאתגר ראשון מתוך שבעה (בצד אחריותיות, הטיה והוגנות, אוטונומיה של המטופל, אחריות משפטית, ציות לחוק, ושונות תרבותית), אבל מסתפקת באמירה שיש לציית לדין.¹⁶² טור דעה אחר מדגיש את חשיבות הפרטיות, אבל מרדד אותה לאבטחת מידע.¹⁶³ מאמר קצר נוסף מדגיש את הקלות שבה ניתן לזהות מחדש נושאי מידע מתוך מידע מותמם לכאורה.¹⁶⁴ בדומה, בהקשר האמריקני, משפטנים שפנו לקהל הרפואי הדגישו את קוצר ידו של החוק הפדרלי.¹⁶⁵ מאמרים אחרים דנים בהיבטי פרטיות מסוימים, ובמקרים רבים הדיון מניח שיש פגיעה בפרטיות ומתמקד בטכנולוגיות שמצמצמות את הפגיעה.¹⁶⁶

במחקר הישראלי, נחום קרייטי ועמיתיו בחנו את השימוש השני במידע רפואי, כלומר שימוש במידע שנוצר לצורך הטיפול ויכול לשמש כעת "ללמידה עמוקה".¹⁶⁷ מתוך נקודת מבט קניינית, שבוחנת למי הבעלות במידע, הם הציעו לפתח את מה שכינו "אפיק המטופל", שלפיו למטופל תהיה גישה ישירה וחינמית לרשומה הרפואית שלו, שאותה יוכל להעביר לאיגוד מטופלים, ושה בתורו יעביר את המידע לחוקרים. רואי קידר ותמר תבורי בחנו שימושים במידע רפואי לצורכי בינה מלאכותית ומצאו שבדין הישראלי "הזכות לפרטיות במידע רפואי ולהגנה מפני פגיעה בה מבוססת היטב".¹⁶⁸ אלה דיונים חשובים, אולם הראשון עוקף את סוגיית הפרטיות ומטמיע אותה בפתרון הקנייני, והשני מניח שהדין הקיים מצליח להתמודד עם היבטי הפרטיות. מסגרת משפטית – אכן יש, אבל אתגריה רבים: הן אתגרי המחקר בנתוני עתק שראינו, והן אלה של הבינה המלאכותית, שמצטרפים לקודמיהם, שאותם אבחן כעת.

¹⁵⁹ ראו למשל Likhitha Kolla & Ravi B. Parikh, *Uses and Limitations of Artificial Intelligence for Oncology*, 130(12) *CANCER* 2101 (2024), בנוגע לשימושי בינה מלאכותית בטיפול בסרטן.

¹⁶⁰ Tirth Dave, Sai Anirudh Athaluri, Satyam Singh, *ChatGPT in Medicine: An Overview of its Applications, Advantages, Limitations, Future Prospects, and Ethical Considerations*, *FRONT. AI* 6: 1169595 (2023).

¹⁶¹ שם, בעמ' 3.

¹⁶² Shinae Yu, Sang-Shin Lee, Hyunyoung Hwang, *The Ethics of Using Artificial Intelligence in Medical Research*, 39(4) *KOSIN MEDICAL J.* 229 (2024).

¹⁶³ Andrea Alonso & Jeffrey J. Siracuse, *Protecting Patient Safety and Privacy in the Era of Artificial Intelligence*, 36 *SEMINARS IN VASCULAR SURGERY* 426 (2023).

¹⁶⁴ Eyal Lotan et al, *Medical Imaging and Privacy in the Era of Artificial Intelligence: Myth, Fallacy, and the Future*, 17(9) *J. AM. COLL. RADIOL.* 1159 (2020).

¹⁶⁵ W. Nicholson Price & I. Glenn Cohen, *Privacy in the Age of Medical Big Data*, 25 *NATURE MEDICINE* 37 (2019). ראו גם Blake Murdoch, *Privacy and Artificial Intelligence: Challenges for Protecting Health Information in A New Era*, 22 *BMC MEDICAL ETHICS* 122 (2021).

¹⁶⁶ Nazish Khalid et al, *Privacy-preserving Artificial Intelligence in Healthcare: Techniques and Applications*, 158 *COMP. BIO. & MED.* 106848 (2023).

¹⁶⁷ נחום קרייטי, טניה ברסקי, אור גלרט, יובל לנדאו "קניין גופני ולמידה עמוקה" **ספר יורם דנציגר** 567 (לימור זר-גוטמן ועידו באום עורכים, 2019).

¹⁶⁸ רואי קידר ותמר תבורי "היבטים משפטיים ורגולטוריים של בינה מלאכותית בעולם הרפואה" **טכנולוגיות מתפרצות: אתגרים בדין הישראלי** 59, 72 (ליאור זמר דב גרינבאום ואביב גאון, עורכים, 2022). המחברים עמדו על ארבעה אתגרים בשימוש בבינה מלאכותית בעולם הרפואה, שאינם אתגרי פרטיות: חשש מאפליה אלגוריתמית, אופן הפעולה של המערכות שעלול להביא לטעויות, אתגר הקופסה השחורה (חוסר שקיפות של האלגוריתם), דבר שמקשה על זיהוי טעויות, והיחס בין הטכנולוגיה לעבודת הצוות הרפואי.

2. אתגרי הפרטיות הרפואית של הבינה המלאכותית

מהם, אם כן, אתגרי הפרטיות שמביאה איתה הבינה המלאכותית בהקשר הרפואי? אצביע על אתגרים בשלב הקלט – שהם אתגרים שמוכרים מהדיון בנתוני עתק, ועל אתגרים טכנולוגיים ומשפטיים בשלבי המשך של העיבוד ועל מסגרת הפעולה בכלל.

(א) קלט: נתוני עתק

בשלב הראשון, כל האתגרים שמעוררות הטכנולוגיות של נתוני עתק מתקיימים גם כאן. איסוף מידע בהיקפי ענק ממגוון מקורות לשם עיבוד המידע, מתנגש במישרין עם עקרון מזעור המידע. פעולות האיסוף הרחבות מקשות על תיאור מוקדם של תכלית האיסוף, והתוצאה היא שאין באמת יכולת לעמוד בחובת ההודעה שיש בחוק הגנת הפרטיות, וממילא, גם לא בעקרונות ההסכמה וצמידות המטרה.¹⁶⁹

בשימוש בבינה מלאכותית, הקושי לתאר את מטרות איסוף המידע מתגבר,¹⁷⁰ וכל שיכול הגורם שאוסף מידע לומר, הוא תיאור כללי וכוללני על כך שהמידע ישמש ל"עיבוד לשם בינה מלאכותית". זאת, משום שבשלב האיסוף, עדיין לא ידוע כיצד יעובד המידע ומה יהיו תוצריו, וממילא, קשה לשער מה יהיו השימושים. זהו פן אחד של אתגר "הקופסה השחורה" – המידע יוצא מהאדם ונכנס לקופסה, אולם איננו יודעים מה עוד יש בה, מה קורה בתוכה, כיצד מעובד המידע שם, ומה ייצא ממנה. בהקשר הרפואי, אפשר לכל היותר לומר שהמידע ישמש למחקר רפואי, או "לשיפור שיטות אבחון", אבל גם אלה אמירות כלליות. קשה גם לסמוך על הסכמה משתמעת, משום שבעת הזו, יש להניח, שרוב הציבור אינו מבין מה בדיוק נעשה עם המידע האישי מאחורי הקלעים, בתוך קרביה של המכונה, וכיצד משתמשים בו.

כאשר אין הגדרה ברורה של התכלית לשמה נאסף המידע, הרי שגם אם ניתנת הסכמה, לא ברור למה מתייחסת ההסכמה, ולכן ממילא קשה לבחון את עקרון צמידות המטרה. בלי לדעת מה המטרה הראשונית, אי אפשר לדעת אם המטרה השנייה זהה או נכללת במטרה הראשונה, או סוטה ממנה ועד כמה. גם כאן, התממה אינה פתרון קסם.

אתגר נוסף בשלב הקלט קשור באופן איסוף המידע. בשונה מגופי בריאות ממוסדים, חברות שמפתחות טכנולוגיות בינה מלאכותית וזקוקות למידע כחומר גלם לצורך אימון המכונה, רוכשות מידע קיים או קוצרות אותו מהרשת. פעולת הקציר הזו (או בלעז, scraping, שתרגומה המילולי הוא גירוד) מעוררת סוגיות בדיני חוזים, דיני זכות יוצרים ודיני הפרטיות. שאלות אלה מתעוררות גם ביחס למידע רפואי.¹⁷¹

תחת הדין הישראלי, איסוף מידע אישי שלא במישרין מנושא המידע עלול להיתקל בקשיים נוספים. המידע שמשמש חומר גלם לאימון ולימוד המכונה אינו מגיע בהכרח מנושאי המידע, אלא מגורמי ביניים כמו קופות החולים או בתי חולים, אבל כפי שנראה בפרק הבא, גם מגורמים אחרים לגמרי, כמו חברות אינטרנט שמציעות שירותים כמו מנועי חיפוש, יישומי ספורט ובריאות, ועוד. במצבים כאלה, בוודאי שקשה לתאר לנושאי המידע את המטרה לשמה נאסף המידע ואין מבקשים את הסכמתם מראש.

בדין האירופי יש פירוט של שישה "בסיסים לגיטימיים" לעיבוד מידע, כלומר שישה עוגנים חוקיים.¹⁷² העוגן הראשון קיים גם בדין הישראלי – הסכמה. לחלק מהעוגנים האחרים יש הד בדין הישראלי. העוגן האירופי השני הוא כאשר המידע נדרש במסגרת עסקה חוזית. עוגן זה מקביל להסכמה משתמעת בדין הישראלי.¹⁷³ כאשר אישה מתבקשת למסור פרטים כדי להירשם ליישומון למעקב אחרי המחזור, גם אם בתהליך התקנת היישומון במכשיר האישי שלה אין שלב שבו מוצגים תנאי השימוש ומדיניות פרטיות, יש הסכמה משתמעת למסירת

¹⁶⁹ לדיון במגבלות ההסכמה נוכח הבינה המלאכותית, או Etye Steinberg, *AI, Radical Ignorance, and the Institutional Approach to Consent*, 37 PHIL. & TECH. 101 (2024).

¹⁷⁰ לדיון, ראו מיכאל בירנהק "פרטיות ובינה מלאכותית" משפט חברה ותרבות ח 139, 158–162 (2025).

¹⁷¹ בירנהק "פרטיות ובינה מלאכותית", שם, בעמ' 163–165. בהיבט זכויות היוצרים עשוי להיות הבדל, שכן המידע הרפואי שנקצר הוא בדרך כלל בגדר עובדות, ואלה אינן מוגנות לפי דיני זכות יוצרים. ראו סעיף 5 לחוק זכות יוצרים, התשס"ח–2007.

¹⁷² סעיף 6 ל-GDPR.

¹⁷³ סעיף 3 לחוק הגנת הפרטיות מגדיר "הסכמה" כ"הסכמה מדעת, במפורש או מכללא".

המידע לצורך קבלת השירות של היישומון.¹⁷⁴ ההסכמה אינה משתרעת על שימושים נוספים, ויהיה צריך לפרש את הנסיבות כדי לקבוע למה התייחסה ההסכמה. העוגן השלישי הוא ציות לחובה חוקית. בדין הישראלי יש ביטוי עקיף לעוגן זה, בדרך של פטור.¹⁷⁵ מצב זה עשוי להיות רלוונטי בקשר לחובות דיווח של גורמים מטפלים על מחלות מדבקות,¹⁷⁶ או מחלות שיש חובת דיווח בקשר אליהן, למשל סרטן.¹⁷⁷ בפרק ד להלן נפגוש עוד שורה של מצבים שבהם הדין מחייב העברת מידע מגורמי הבריאות לגופי המדינה. העוגן האירופי הרביעי הוא הגנה על אינטרס חיוני של נושא המידע או אדם אחר. בדין הישראלי, פעולה כזו עשויה ליהנות מהגנה, כאשר הפוגע פעל בתום לב בנסיבות שבהן הייתה מוטלת עליו חובה חוקית, מוסרית, חברתית או מקצועית לפעול כך.¹⁷⁸ בכל מקרה, עוגן זה נראה פחות רלוונטי להקשר של הבינה המלאכותית ברפואה. עוגן חמישי הוא כאשר עיבוד המידע נדרש למימוש אינטרס ציבורי. אזכיר שבדין האירופי יש החרגה מסוימת של שימוש במידע אישי לצורכי מחקר. גם אם השימוש בבינה מלאכותית יכול לקדם את בריאות הציבור – אינטרס ציבורי ראשון במעלה – לא די בהצבעה על האינטרס הזה, ויש להראות עוגן חוקי מתאים – הסמכה בחוק או הסכמה מתאימה של נושא המידע. העוגן השישי והאחרון הוא הגנה על אינטרסים לגיטימיים של בעל השליטה במידע, תוך איזון עם זכויות ואינטרסים של נושאי המידע. זהו עוגן שמתמקד תחילה בבעלי השליטה במידע, אבל מציב מולם את נושאי המידע. לא כל פעולה אפשרית כאן.

אם כן, איסוף המידע ועיבודו מותר לפי הסכמה מדעת או לפי הסמכה מפורשת דיה בחקיקה, ובשל מאפייני הבינה המלאכותית, קשה לראות כיצד מתקיימת הסכמה מתאימה.

פתרון אפשרי אחד לאתגר ההסכמה בדיני הפרטיות, הוא כאשר ההסכמה מדעת שדרושה לטיפול הרפואי מתלכדת עם ההסכמה מדעת שדרושה לעיבוד המידע. כשם שהמטופל אינו צריך לאשר כל אמצעי טיפול פרטני (כיצד בדיוק יתנהל ניתוח), הרי כאשר המידע האישי מעובד בדרך של בינה מלאכותית לצורך הטיפול הפרטני, די בהסכמה הכללית (למשל, בנוסח כמו "אני מסכים לעיבוד המידע שלי במסגרת טכנולוגיות AI לצורך הטיפול ביי"). אולם התלכדות כזו תחול רק בקשר לשימוש במידע, ולא בשלב הקודם של איסוף מידע כללי יותר לצורך לימוד המכונה. איסוף מידע והזנתו נועדו לאימון ולימוד, ועדיין לא לטיפול עצמו. רק בשלב שבו הרופאה משלבת את הבינה המלאכותית בטיפול באדם מסוים, נוכל לומר שיש התלכדות של דרישת ההסכמה לטיפול הרפואי ודרישת ההסכמה לעיבוד המידע.

בדיון בנתוני עתק בפרק הקודם, בחנתי את האפשרות להתממת מידע כפתרון, והצבעתי על מגבלותיה. גם כאן, בהקשר של בינה מלאכותית, התממה אינה פתרון קסם. הדיון לעיל בקשר להתממה במחקרי נתוני עתק חל גם פה, וביתר שאת. כפי שמאמר אמריקני היטיב לתאר זאת, נוצר מעגל שוטה:¹⁷⁹ בשלב הראשון, הבינה המלאכותית מחלישה את ההתממה: הבינה המלאכותית עצמה מסוגלת ביתר קלות לזהות את נושאי המידע מחדש. ולכן, הרף הדרוש להתממה עולה. בשלב השני, ההתממה מחלישה את הבינה המלאכותית: מידע מאופיין – בהיבטי מצב כלכלי, גזע וכדומה – חושף הטיות סמויות באלגוריתם, ואמינותו עלולה להיפגע.

לסיום הדיון בנושא זה, אעיר שבעת הזו באתרי ארבע קופות החולים בישראל לא נמצאה התייחסות לשימוש בבינה מלאכותית בעיבוד המידע, למעט התייחסות של קופות החולים כללית ומאוחדת לשימוש במידע בציאטבוט שירות שהן מפעילות באתריהן.¹⁸⁰

¹⁷⁴ אי הצגת המידע היא הפרה של חובת ההודעה שלפי סעיף 11 לחוק, אולם עדיין ניתן יהיה לאתר הסכמה משתמעת למסירת המידע, למטרה מצומצמת שנובעת בבירור מהנסיבות.

¹⁷⁵ סעיף 19(א) לחוק הגנת הפרטיות קובע כי "לא ישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין". נטל ההוכחה הוא על הטוען לפטור.

¹⁷⁶ ראו סעיף 12 לפקודת בריאות העם, 1940; תקנות בריאות העם-הודעות על מחלות מדבקות, התשכ"א-1961.

¹⁷⁷ תקנות בריאות העם (דיווח ומידע מיוחד על מחלת הסרטן), התשמ"ב-1982.

¹⁷⁸ סעיף 18(2)(ב) לחוק הגנת הפרטיות.

¹⁷⁹ Lauren Quinn, *Are Your Secrets Safe?: Imposing A Fiduciary Duty on Healthcare AI Developers Dealing with Sensitive Health Information*, 94 FORDHAM L. REV. 383, 400-402 (2025).

¹⁸⁰ ראו סעיף 6 לתנאי השימוש של הכללית: https://www.clalit.co.il/he/info/about_site/Pages/terms_of_use.aspx; ובאתר מאוחדת - <https://tinyurl.com/593fnc7t>.

(ב) עיבוד ושימוש

השלב הבא במהלך החיים של המידע האישי הוא עיבודו. גם פה, חלק מאתגרי הפרטיות שמתעוררים בקשר לבניה מלאכותית מוכרים לנו מהעיסוק בנתוני עתק, ונדון לעיל: כיצד לעבד את המידע בלי לחרוג מהמטרה הראשונה, שצריכה להיות מטרה לגיטימית וחוקית שהתקבלה לגביה הסכמה של נושא המידע, וכיצד להימנע מזיהוי מחדש של נושאי מידע אנונימיים. אתגר נוסף שמתעורר בשלב זה הוא אתגר "הקופסה השחורה": איננו יודעים איך בדיוק האלגוריתם פועל וכיצד עובד המידע. היכולת האנושית לבקר את הפעולה הטכנולוגית מוגבלת, והרי זה מותר המכונה מן האדם.

(ג) דליפה ופלט

חשש מרכזי שמתעורר בדרך כלל בקשר למאגרי מידע הוא של דליפת מידע, בין מתוך הארגון, ברשלנות או בזדון, ובין בשל פריצה מבחוץ. בשלב הקלט – טכנולוגיות בינה מלאכותית מרכזות כמות עצומה של מידע ממקורות שונים, ולכן עשויה להיות יעד לגורמים זדוניים ועוינים, אולם בשלב הזה אין ייחוד למידע רפואי. המידע פגיע כמו כל מאגר מידע אחר.

חוק הגנת הפרטיות ותקנות לפיו קובעים חובות סודיות ואבטחת מידע.¹⁸¹ ככל שהמידע מותמם בשלבים מוקדמים יותר של התהליך, אצל מי שמוסמך להחזיק את המידע ועוד לפני תחילת העיבוד וההעברה לגורם המעבד, קטנה הסכנה לדליפה. אולם, אין לסמוך על ההתממה לבדה, הן משום שהמידע עלול לדלוף לפני ההתממה, והן משום שלגורמים עוינים, חישבו על מדינת אויב, יש תמריץ ויכולות לנסות לזהות מחדש את נושא המידע.

השלב שבו משתמשים בבינה מלאכותית כדי להפיק תובנות, התאמות, תחזיות וכדומה, מעורר פחות קשיים. עבודת העיבוד האינטנסיבית שנעשית בטכנולוגיות אלה מעמעמת מידע פרטי ואת היכולת לזהות את נושא המידע. עם זאת, החשש מתקלות שבהן מידע גולמי שהוזן למערכת יוצג גם כפלט שלה באופן שמזהה את נושא המידע – קיים.¹⁸²

(ד) מסגרת הפעולה

השוואת אתגרי הבינה המלאכותית לאתגרים של נתוני עתק מחדדת שוני מוסדי. עד להופעת הבינה המלאכותית, עיקר השימוש בנתוני עתק רפואיים היה במסגרות מחקריות. מחקר כזה נערך במוסדות אקדמיים, במסגרות מחקר מדינתיות, או בחברות גדולות, ומופקדים עליו חוקרים ורופאים ולצידם מערך משפטי תומך. בדין הישראלי, גופים כאלה כפופים למשפט הציבורי במישרין (מחקר ממשלתי), מכוח היותם גופים דו-מהותיים (קופות חולים ומוסדות להשכלה גבוהה), ובעקיפין (חברות פרטיות). החוקרים-רופאים כפופים לחובות הסודיות שיש בחוק זכויות החולה, בפקודת בריאות העם, בדיני הראיות ובאתיקה מקצועית. בגופים כאלה יש מסגרות לאישור אתי מקדים של המחקרים (ועדת הלסינקי כאשר מדובר במחקרים בבני אדם, ובכלל זה בנתונים על בני אדם,¹⁸³ ועדות אתיקה מוסדיות).

לעומת זאת, עיבוד המידע והפיתוח של הבינה המלאכותית נעשים בדרך כלל במסגרות לא-אקדמיות, מסחריות, וזרות. מי שמעבדים את המידע בגופים כאלה הם מהנדסים, לאו דווקא רופאים. המהנדסים אינם כפופים לאתיקה רפואית או לדיני הבריאות.¹⁸⁴ בגופים המסחריים אין ועדות אתיקה. גם אם החברות שוקלות שיקולים

¹⁸¹ ראו סעיפים 16–17 לחוק הגנת הפרטיות, ותקנות תקנות אבטחת מידע.

¹⁸² ארגון הבריאות העולמי ציין חשש כזה בדיון על בינה מלאכותית בשדה הרפואי. ראו World Health Organization, Ethics and Governance of Artificial Intelligence for Health: Guidance on Large Multi-Modal Models 14 (2024), נמצא ב: <https://www.who.int/publications/i/item/9789240084759>.

¹⁸³ למחקרים רפואיים בבני אדם, ראו תקנות בריאות העם, לעיל ה"ש 99. השימוש בנתונים קיימים לצורך מחקרים רפואיים הוסדר בעבר בחוזר מנכ"ל משרד הבריאות 15/06 "תת ועדת הלסינקי לאישור מחקר שאינו ניסוי רפואי בבני אדם" (2006), וכיום מוסדר בנהל משרד הבריאות לניסוי רפואי בבני-אדם (מס' 14) (2020). ראו סעיף 24 (הגדרת "מחקר בנתונים קיימים ושאלונים"), ובחלק היישומי, בסעיף 4.2 לעניין מינוי תת-ועדת הלסינקי לעניין זה.

¹⁸⁴ בישראל – משום שאינם באים בגדר הגדרת "מטפל" בסעיף 1 לחוק זכויות החולה. בארצות הברית, HIPAA מגדיר מיהם הגופים המוסדרים שם (covered entities). ריצ'ארדס הצביע על גופים מסחריים רבים שמחזיקים מידע רפואי ואינם באים תחת הגדרת החוק. ראו RICHARDS, INTELLECTUAL PRIVACY, לעיל ה"ש 64, בעמ' 59.

אתיים, ניתן להניח שהדבר נעשה כדי לשרת אינטרסים כלכליים-מסחריים שלהן, כמו שמירת המוניטין שלהן, יחסי ציבור וכדומה, ולא לשם שמיים או לשם הגנה על פרטיות נושאי המידע.

* * *

מהדיון עולה שהשימוש בנתוני עתק רפואיים במערכות בינה מלאכותית טומן בחובו יתרונות רבים למחקר ולטיפול הרפואי, אולם הוא יוצר אתגרי פרטיות רבים. מטרת איסוף המידע אינה מוגדרת ואינה ידועה מראש לבד ממטרות כלליות וכוללניות. משום כך, אין משמעות לעקרון מזעור המידע; יש קושי ליידיע את נושא המידע בדבר השימושים המיועדים במידע; הסכמה שניתנה על בסיס הגדרת מטרות כללית מפוקפקת; וקשה לברר האם הייתה סטייה מהמטרה הראשונה באופן פסול, שכן המטרה הראשונה לא הוגדרה כלל. יש קשיים נוספים בשלב עיבוד המידע, של זיהוי מחדש וסודיות, וחשש מדליפה בשלבים השונים. משום שהמידע נאסף ממגוון מקורות, גם מחוץ למערכת הרפואית, כללי אתיקה רפואיים ומחקריים אינם מיושמים. לדיני הפרטיות כלים מוגבלים להתמודד עם כל זה. הבינה המלאכותית ממחישה את הגידול במספר הגורמים שעוסקים במידע רפואי ואת השונוות המשפטית ביניהם. זהו מצב מידעי מורכב.

ד. מידע רפואי כמצב מידעי מורכב

בישראל, רוב המידע הרפואי נוצר ומוחזק במסגרות ממוסדות. בזכות מערך הרפואה הציבורית, מדובר בעיקר בקופות החולים ובבתי החולים (הגם שיש בתי חולים פרטיים). ואכן, ההסדרה המשפטית מכוונת בעיקר אליהם, ובצדק. אבל בסביבה הטכנולוגית המשתנה, מידע רפואי נוצר בעוד שלל מקומות והקשרים. פרק זה מרחיב את המעגל ובוחר את הסוגייה לא רק במקום המתבקש – גורמי הבריאות, אלא גם במעגלים ההיקפיים. בצד תהליכי הפרטה במערכת הרפואית (ביטוחים פרטיים ושירותי רפואה פרטית), נכנסים שחקנים חדשים לזירה, ומידע שעבר רק בין המטופל לגורם המטפל המידי, ורק במקרים מסוימים עבר לרשויות המדינה, זורם כעת בין עוד גופים, ציבוריים ופרטיים, בכל הכיוונים. פרק זה ממשיג את זירת המידע הרפואי כמצב מידעי מורכב. זו אינה תופעה שייחודית להקשר הרפואי, והמידע הרפואי מספק לנו מקרה מבחן להבין את התופעה הכללית. החלק הראשון יציג את המסגרת של מצב מידעי מורכב. החלק השני יראה את המקרה של המידע הרפואי. אציע מיפוי מפורט – אך לא מלא – של זרימת המידע הרפואי בישראל. החלק השלישי יצביע על האתגרים שמתעוררים.

1. זרימת מידע רב-כיוונית

בפרק א ראינו שדיני הפרטיות מתפרשים על פני שלושה מישורי פעולה מרכזיים: פרטיות קלסית, שעוסקת ביחסים בין אדם אחר לגורם אחר; פרטיות חוקתית, שעוסקת ביחסים בין אזרח למדינה, ופרטיות מידעית, שמאופיינת לא רק לפי זהות הצדדים ויחסיהם אלא לפי הדגש על התוכן – מידע אישי. התוצאה היא קיטוע משפטי.¹⁸⁵

דיני הפרטיות הקיימים מבוססים על הנחה של יחסים דו-צדדיים וחד-פעמיים. במישור הפרטיות הקלסית, כאשר אדם מפרסם מידע פרטי של אחר ללא רשות, למשל רופא שמספר ברבים על מצבו של מטופל מזוהה, הרי זו הפרה של הפרטיות. הדין מגיב למצבים כאלה בקביעת עוולות נזיקיות. במישור הפרטיות החוקתית, נבחן אירוע נקודתי כמו חיפוש משטרתי, או מדיניות של הרשות, למשל שימוש משטרתי במערכות מעקב. במישור הפרטיות המידעית הדין עוסק במאגרי מידע, וגם שם המשפט מניח יחסים דו-צדדיים, של בעל שליטה במאגר המידע מול נושאי המידע, כלומר האנשים שהמידע על אודותיהם מוחזק במאגר. גם כאן למשפט יש מענה, בדיני הפרטיות המידעית.

ובינתיים, אנחנו עדים, בשטח, להופעתם של מצבי מידע מורכבים, שאינם מתיישבים עם דפוסי החשיבה של המשפט, ומשום כך המשפט מתקשה להתמודד איתם. חוסר ההתאמה של מצב מידעי מורכב למבנה של דיני הפרטיות הוא רב-ממדי: ראשית, האבחנה בין שלושת מישורי הפעולה קורסת.¹⁸⁶ קשה לתחום פעולה רק

¹⁸⁵ להרחבה, ראו מיכאל בירנהק "פרטיות בעיר הדיגיטלית" מחקרי משפט לג 911, 923 (2022); בירנהק, פרטיות חוקתית, לעיל ה"ש 8, בעמ' 113 ואילך.

¹⁸⁶ בירנהק, פרטיות חוקתית, שם, בעמ' 147.

למישור אחד, והיא גולשת בין המישורים – היחסים הפרטיים הופכים למסחריים, הציבורי הופך לפרטי וכדומה. סיבה מרכזית לכך היא שהשחקנים הם מסוגים משפטיים שונים – אנשים פרטיים, גופים מסחריים ורשויות שלטוניות. כל אחד מהם כפוף למערכת משפטית שונה. **שנית**, ההנחה של יחסים דו-צדדיים אינה רלוונטית. במצב מידעי מורכב יש מספר רב של שחקנים (ולא רק שניים). **שלישית**, בממד הזמן, זרימת המידע במצב המורכב אינה אירוע חד-פעמי, אלא נמשכת, בכל הכיוונים.

בחינה קרובה של מצבי מידע מורכבים למשל בנוגע לערים דיגיטליות (או בכינוי הרווח יותר, ערים חכמות),¹⁸⁷ באשר לסוגייה של ניטור פעילות של עובדים ברשתות חברתיות על ידי מעסיקיהם,¹⁸⁸ ובנוגע למעקב השב"כ אחרי כלל הציבור שהחזיק במכשירי טלפון במהלך מגפת הקורונה,¹⁸⁹ מחדדת את הקשיים של המשפט להתמודד עם מצבים כאלה:

קושי אחד הוא שיש צורך בבדיקה משפטית קפדנית ומכבידה, כדי להבין מהו הדין שחל במצב מידעי מורכב – על המצב בכללותו ועל כל אחד ממקטעיו. בדיקה כזו מחייבת לאתר את כל השחקנים, לאפיין אותם מבחינה משפטית (נושא מידע / אזרח / אדם, שניצבים מול גורם פרטי / שלטוני / בעל שליטה במידע – והחלוקה אינה חפה מחפיפות), לזהות את כל זרימות המידע ביניהם ולאפיין אותן (מי מעביר איזה מידע למי, מתי, באיזו תדירות), לקבוע אילו כללים משפטיים חלים על כל מקטע, ולתכלל את הכול לתמונה גדולה.

קושי שני, הוא החשש שבשל מורכבות הניתוח וסתירות אפשריות בין הכללים שחלים במקטעי זרימת המידע השונים במצב המורכב, ענף משפטי אחד יצבע את התמונה כולה וישתלט עליה. למשל, כאשר גופים פרטיים אוספים מידע מאזרחים, הם כפופים לדיני הפרטיות המידעית, אבל כאשר הגוף הפרטי מעביר מידע למדינה – האם נבחן את העברת המידע במשקפי הפרטיות המידעית (לפי זהות הגוף המעביר), שיש בהם סל כלים עשיר, או במשקפי הפרטיות החוקתית (לפי זהות הגוף המקבל), שעשויה להציב מגבלות נוקשות יותר לגוף המדינתי? החשש הוא ששיתוף פעולה מסחרי-מדינתי יעקוף כללים חוקתיים חשובים מכאן, ויתעלם מכללים מפורטים משם.¹⁹⁰ הפרטיות עלולה להיפגע במעברים בין המקטעים המשפטיים השונים.¹⁹¹

כיצד נתמודד עם מצבי מידע מורכבים? דרך אחת היא הפירוק והתכלול שהוצעו כאן, תוך ייחוד המקטע המשפטי המתאים לכל מישור פעולה: פרטיות קלסית ליחסים בין אנשים, פרטיות חוקתית ליחסים בין אזרחים לרשויות, ופרטיות מידעית היכן שיש פעולות מבוססות-מידע (תוך חפיפה אפשרית למקטעים הקודמים). המלאכה רבה מאוד, אבל יש לה יתרון של העשרה הדדית בין המקטעים המשפטיים. למשל, כללי הפרטיות המידעית, שעוקבים עקב בצד אגודל אחרי המידע לאורך מהלך החיים שלו, יכולים להעשיר את תוכנה של המידתיות בהקשרה החוקתי. דרך שנייה להתמודד עם המורכבות והחששות, היא להתעלות מעל הקיטוע המשפטי, ולאתר תפיסה אחודה של הפרטיות, שתסייע לראות לא רק את העצים (המקטעים הנפרדים), אלא גם את היער (התמונה הכללית). תפיסת הפרטיות כשליטה מתאימה כאן.¹⁹² כמובן, מתעורר אתגר של יישום – כיצד ניישם את הפרטיות כשליטה בהקשר הזה, הרי האתגרים המעשיים הרבים לא ייעלמו רק בשל ההמשגה הזו. אבל, הבנת הפרטיות כשליטה נמשכת על אדם במידע האישי שעל אודותיו עשויה להביא את מעצבי המדיניות, המהנדסים והמהנדסות, החוקרות והרופאים להיות ערים להיבטי הפרטיות כבר בתחילת הפעולה, לעצב כלים משפטיים שיגבירו את שליטת נושא המידע, למשל בנוגע לאופן היידוע וצורת ההסכמה, לכוון את עיצוב הטכנולוגיה כך שהיא תאפשר לממש את הזכות (כלומר, התשובה "אי אפשר" אינה קבילה), ובכלל, לכבד את המטופלים ואת האוטונומיה שלהם.

אעיר, שגישתי שונה מזו של הלן ניסנבאום (Nissenbaum), שהציעה לבחון האם כללים שמסדירים העברות מידע בהקשרים חברתיים ספציפיים, הופרו. לשיטתה, שאותה כינתה Contextual Integrity, יש לזהות תחילה

¹⁸⁷ בירנהק "פרטיות בעיר הדיגיטלית", לעיל ה"ש 185.

¹⁸⁸ בירנהק, **פרטיות חוקתית**, לעיל ה"ש 8, בעמ' 158–162.

¹⁸⁹ בירנהק, **פרטיות חוקתית**, שם, בעמ' 162–164.

¹⁹⁰ בניתוח ההסדרים המשפטיים שנחקקו בארצות הברית לאחר מתקפות הטרור של האחד עשר בספטמבר, ניבה אלקין-קורן ואני קראנו לתופעה הזו בשם "לחיצת היד הנעלמה": Michael Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003).

¹⁹¹ בירנהק, "פרטיות בעיר הדיגיטלית", לעיל ה"ש 185, בעמ' 963; בירנהק, **פרטיות חוקתית**, לעיל ה"ש 8, בעמ' 158.

¹⁹² בירנהק, **פרטיות חוקתית**, שם, בעמ' 169–170.

את ההקשר שבו מדובר, למשל "הקשר רפואי" או "הקשר חינוכי", לזהות את הכללים שעוסקים במידע, ומתוכם, את הכללים שעוסקים בהעברת מידע. כעת, יש לבחון שינוי שהוכנס בהקשר (או "שדה"), ולבחון האם השינוי השפיע על הכללים האלה.¹⁹³ כמוה, גם אני סבור שיש לזהות את השחקנים, את המידע שמועבר, ואת כללי העברת המידע.¹⁹⁴ אבל גישתה נשארת תחומה ל"הקשר" מסוים, ולא מספקת לנו הנחיות כיצד לזהות את ההקשר ולהגדירו. אחד המאפיינים הבולטים במצבי מידע מורכבים הוא החריגה מהקשר נתון, יצירה של הקשרים חדשים, מיזוג הקשרים קודמים, ושינויים של ההקשרים עצמם.¹⁹⁵ למשל, "עיר חכמה" היא הקשר חדש לגמרי; ניטור גלישה של עובדים ברשתות חברתיות – האם ההקשר הוא מקום העבודה או הפעילות ברשת? ההקשרים קורסים זה לתוך זה. ולעניינו, איסוף מידע רפואי על ידי מכשור ספורט ויישומונים מסחריים – האם נכון לאפיין אותם כהקשר רפואי או כהקשר ספורטיבי? או אולי בכלל ההקשר מסחרי? לכל הקשר כללים שונים בדבר זרימת המידע. בנוסף, אין אצל ניסנבאום הנחיות כיצד להעריך את השינוי בכללים. אצלה, כל שינוי מביא להנפת דגל אדום. היא אינה מציעה אמת מידה להערכת השינוי, לבד מהפניה לערכים כלליים ולנורמות של ההקשר.¹⁹⁶ גישתי מציע את הפרטיות כשליטה כמסגרת ערכית לבחינת השינויים.

כעת, ניתן לבחון את גורלו של המידע הרפואי, שהוא מקרה מובהק של מצב מידעי מורכב.

2. זירת המידע הרפואי

מידע רפואי נוצר כיום בשלל מקומות והקשרים, פרטיים וציבוריים, טיפוליים, מחקרניים ומסחריים, ועובר בין שחקנים שונים בזירה, שהולכת ומתרחבת. המידע נוצר במהלך טיפול רפואי, אבל אינו מוגבל לתחומי המרפאה וחדרי הניתוח ויוצא אל מחוץ למסגרת הפיזית הרפואית, כמו הבית וחיי היום-יום, ולעיתים קרובות המידע יוצא מחוץ להקשר הרפואי המיידי. שימוש ביישומון היכרויות למשל עשוי לכלול מידע רפואי. התוצאה היא שמידע רפואי מתייחס לבעיה רפואית ולטיפול, לתרופות, מדדים שונים, היסטוריה רפואית, תזונה וכושר, וגם לפעילות מקוונת, וכל זה ביחד עם מידע אישי אחר על האדם – מין, גיל, מקום מגורים, פרטי קשר, נתוני מיקום ומידע פיננסי, ועוד.

(א) תמונה כללית (היער)

סקירה שיטתית של החקיקה והפסיקה בישראל ושל הספרות המחקרית, ובדיקה של שירותים רפואיים ישירים כמו ציוד רפואי ויישומוני בריאות, מעלות שורה של שחקנים בזירה: המטופל, המטפלים הישירים (רופאים, מטפלים אחרים, אחים, צוות סיעודי); המוסד המטפל (מרפאה פרטית, בית חולים ציבורי או פרטי); צוות מטפל נוסף (עובדים סוציאליים, מרפאים בעיסוק, קלינאים, צוותי מעבדה); גופי בריאות – כלומר קופות החולים וספקי השירות שלהן; בתי מרקחת (שמקושרים לקופות החולים או פרטיים); מוסדות מדינה, כמו משרד הבריאות, המוסד לביטוח לאומי, המשטרה, צה"ל ומשרד הביטחון, המכון הרפואי לבטיחות בדרכים, מאגר החיסונים הלאומי, ועוד; חברות פרטיות שמפתחות ציוד רפואי; חברות שמפתחות פלטפורמות, אתרים ויישומונים עבור השחקנים הקודמים (בעיקר עבור בתי החולים וקופות החולים); חברות שמספקות שירותים לגופים אלה, כמו מכוני כושר שמקושרים עסקית לקופות חולים; חברות פרטיות מסחריות שמציעות שירותים מקוונים שונים בלי קשר לגופי הבריאות, כמו יישומני כושר; חברות אינטרנט שמציעות שירותים שבמבט ראשון אינם קשורים להקשר הרפואי, אולם נוצר בהם מידע רפואי, כמו מנוע חיפוש ואתרי היכרויות; ובנוסף, גופי מחקר (של השחקנים הקודמים או באקדמיה), מעסיקים וחברות ביטוח.

כפי שעולה מהרשימה הלא ממצה הזו, יש בזירה שחקנים ציבוריים (גופי הממשלה והמדינה), שחקנים מעין-ציבוריים (בתי החולים, שחלקם ממשלתי וחלקם פרטי, קופות החולים שכפופות לאסדרה מפורטת, חוקרים באקדמיה), שחקנים פרטיים-מסחריים בשירות הגורמים הציבוריים, ושחקנים פרטיים-מסחריים בשירות

¹⁹³ HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE* (2010).

¹⁹⁴ לשיטתה, הפרמטרים שמגדירים את ההקשר הם הנושא, מעביר המידע, מקבל המידע, סוג המידע, והכללים בדבר העברת מידע. לדיון מעודכן שלה בנושא, ראו Helen Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, 20 THEORETICAL INQ. L. 221, 228 (2019).

¹⁹⁵ לביקורת זו, ראו Michael Birnhack, *A Quest for A Theory of Privacy: Context and Control: Review of Helen Nissenbaum's Privacy in Context*, 51(4) JURIMETRICS J. 447, 470 (2011).

¹⁹⁶ ראו Birnhack, *A Quest for A Theory of Privacy*, שם, בעמ' 471.

עצמם. זיהוי השחקנים הוא רק השלב הראשון בבירור התמונה. השלב הבא הוא לאתר את זרימות המידע ביניהם, ואת הבסיס המשפטי שלהן. עוגנים חוקיים להעברת המידע כוללים את הסכמת המטופל, דינים שאוסרים או מתירים העברת מידע (חקיקה, תקנות, נהלים והנחיות), וחוזים – בין השחקנים השונים למטופלים, או בין השחקנים השונים לבין עצמם, ואת אלה, קשה הרבה יותר לחשוף ולבחון.

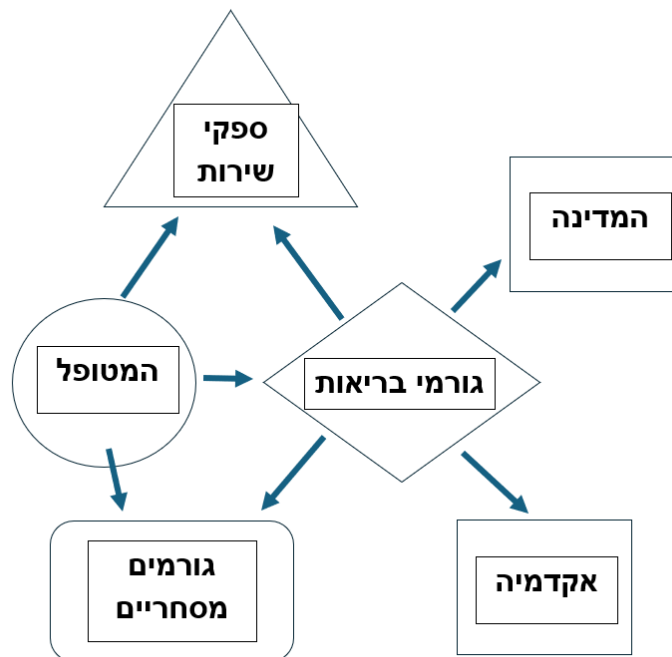
תצוגה ויזואלית של העברת המידע חורגת מהאפשרויות של הדפוס, והקוראות והקוראים מוזמנים לעיין בתצוגה דינמית מקוונת.¹⁹⁷ התצוגה ממחישה את ריבוי השחקנים, את כיוון זרימת המידע – מי מוסר מידע לומי מקבל מידע. התצוגה אינה משקפת את תוכן המידע, את היקפו ואת מאפייניו. בחלק מהמקרים המידע שעובר מגוף אחד לאחר מזהה, מלא ומפורט, למשל בין המטופל לגורמי הטיפול, בחלק מהמקרים המידע אמור להיות אגרגטיבי ואנונימי, כמו המידע שמועבר מקופות החולים למערכת המחקר הממשלתית (תמני"ע) וממנה לגורמי מחקר חיצוניים. בחלק מהמקרים המידע נקודתי, למשל דיווח של קופת חולים על מחלה מדבקת, או מידע על מרשם שמועבר מקופת החולים לבית מרקחת שמקושר לקופה. לעיתים מעבר המידע יהיה חד-פעמי, ולעיתים העברת המידע נמשכת באופן רציף.

היער חשוב לא פחות מאשר העצים: יש סוגי שחקנים רבים, ובמקרים רבים, לכל מטופל, עשויים להיות כמה וכמה ספקי שירות תחת כל סוג של שחקנים. למשל, שימוש בכמה מנועי חיפוש, בכמה סוגי מיכשור לביש ומכשור רפואי. מתכלול זרימות המידע עולה שבזירה הישראלית, **המטופל** הוא בעיקר מקור של מידע, וממנו המידע עובר במישורין לגורמי הבריאות (לשם הטיפול הרפואי), ולשורה של ספקי טכנולוגיה פרטיים, אם כי לא לכולם, וכן למעסיק ולחברת הביטוח. המטופל כמעט שאינו מעביר מידע במישורין לגורמי המדינה. **קופות החולים** הן מוקד מרכזי של מידע – הן כמקבלות מידע והן כמעבירות מידע. בכובע המעביר, הקופות מעבירות מידע בעיקר לגורמי בריאות אחרים, לגופי המדינה, וכן לחברות פרטיות מסוג מסוים – אלה שמספקות לה שירותים, כמו חברות פרסום, מפתחי יישומונים וספקי שירותי ענן, וכן לחברות תרופות. **הגורמים המטפלים האחרים** – בתי חולים, רופאים ומד"א הם מוקדים חשובים גם כן, וגם אצלם מידע מתקבל (בעיקר מגורמי בריאות) ומועבר (בעיקר לגורמי בריאות אחרים ולגופי המדינה). **גורמי המדינה נמצאים** בעיקר בצד שמקבל מידע, בעיקר מגורמי הבריאות. **גורמים מסחריים** שונים בעיקר מקבלים מידע, בשתי קבוצות – האחת מהמטופל, והשנייה מקופות החולים. **גופי המחקר וההוראה** מקבלים מידע בעיקר מקופות החולים. בכל התמונה הזו – המטופל הוא רק עוד גורם בתמונה הכללית.

אם נקבץ את סוגי הגופים יחדיו, מתקבלת תמונה כללית.

איור 4: סוגי השחקנים בשדה הרפואי וזרימת המידע

197 האיוור נוצר באמצעות תוכנת Kumu. התרשים זמין באופן דינמי כאן: <https://embed.kumu.io/6c9eed3b74ad91fa93eaf68c2fb87003> <https://embed.kumu.io/1d87b7d1f61e639906e21b4da0e6ebf7#>



איור 4 הוא איור סכמטי, ויש גם מצבים שבהם הקצוות – המטופל, ספקי השירות וגופי המדינה מעבירים מידע ביניהם במישרין, למשל כאשר אדם פונה למוסד לביטוח לאומי בבקשה לגמלה, ונדרש להוכיח את מצבו הרפואי שמקנה לו את הזכאות, או כאשר המשטרה דורשת מספקי שירות פרטיים מסירת מידע לפי סמכות שנתונה לה בחוק. אולם, ברוב המקרים, רוב הזמן, אין קשר ישיר בין המטופל לגורמי המדינה, וגורמי הבריאות הם המתווכים. מסקנה זו חשובה בהיבט של עיצוב מדיניות. יש לרכז מאמץ ניכר באסדרה של גורמי הבריאות בהיבט הפרטיות, כלומר באופן שבו הם מנהלים מידע ומעבירים אותו הלאה.

(ב) העברות מידע (חלק מהעצים)

לא אוכל לתאר כאן את כל העברות המידע בין השחקנים, ובוודאי יש עוד רבות שהחמצתי, במיוחד בזירה של הגורמים הפרטיים-מסחריים, שהיא נסתרת מהעין. בהתאם, הפירוט שלהלן אינו מתיימר למצות את הדברים, אלא להציג את עיקרם ולהמחיש את סוגי ההעברות.

ליבת הטיפול הרפואי היא המפגש בין המטופל לצוות רפואי, במרפאה או בבית החולים. המידע עובר מהמטופל (וגופו) למטפל (הרופאה) ולגורם המטפל (בית חולים, קופת חולים ובתי מרקחת, מד"א), בהסכמת המטופל. ההסכמה היא הסכמה מדעת – הן במובן הרפואי והן במובן המידעי. הסודיות הרפואית צמחה ועוגנה במפגש הטיפולי המידי הזה; לשם מכוונת שבועת היפוקרטס כבר אלפי שנים, ושם מתלכדים דיני הבריאות ודיני הפרטיות בהגנת כבוד האדם של המטופל. נקודת המוצא של הדין היא שהמידע נתון לשליטת המטופל. חוק זכויות החולה מתאר את ההגנת הפרטיות כאחת מתכליותיו (סעיף 1), קובע חובה כללית לשמור על פרטיות המטופל (סעיף 10), וחובת סודיות של המטפל והארגון המטפל כלפי המטופל (סעיף 19). מידע רפואי הוא בגדר "עניינו הפרטי של אדם" בכמה הקשרים של פגיעה בפרטיות לפי חוק הגנת הפרטיות (סעיפים 2(7), 2(8), 2(9)), זהו מידע בעל רגישות מיוחדת (לפי הפרט השני של הגדרת מידע כזה, סעיף 3), ואין חולק שהוא בא תחת הגג הכללי של חוק היסוד, הן כנגזרת של הזכות לפרטיות שמעוגנת שם במפורש, והן כנגזרת של הזכות לבריאות.¹⁹⁸

המידע הרפואי שנוצר בהקשר הטיפולי המידי אינו נשאר שם. כפי שראינו בפרק א לעיל, חוק זכויות החולה קובע את החובה ליצור רשומה רפואית שמתעד את פרטי המטופל ואת המידע הרפואי על אודותיו (סעיף 17).¹⁹⁹ סעיף 20 לחוק זכויות החולה קובע מצבים מוגדרים שבהם ניתן להוציא מידע ממעגל הטיפול המידי. אתאר

¹⁹⁸ בג"ץ 3071/05 לוזון נ' ממשלת ישראל, פ"ד סג(1) 1, 20 (2008).

¹⁹⁹ ראו גם את חוזר מנכ"ל משרד הבריאות 09/2019 "אמות מידה לניהול רשומת מטופל במערכת הבריאות" (15.12.2019).

אותם לפי מהותם, לאו דווקא לפי הסדר שבחוק. המצב הראשון הוא הסכמת המטופל.²⁰⁰ ההסכמות שבדיני הפרטיות ובדיני הבריאות מתלכדות ומשקפות את האוטונומיה של האדם ואת שליטתו במידע שעל אודותיו. המידע דרוש לאדם למשל כדי לעבור למטפל אחר, פעולה שחוק ניווד מידע רפואי אמור להקל עוד יותר, לשם קבלת חוות דעת רפואית נוספת או לכל צורך אחר של המטופל, למשל לצורך משפטי של בחינת תביעה בגין רשלנות רפואית. המצב השני הוא ההקשר הטיפולי.²⁰¹ החוק מתיר העברת מידע בין מטפלים לשם המשך הטיפול. למשל, כאשר מטופל מועבר מבית חולים אחד לאחר, או מידע שמועבר ממכון דימות לגורם המטפל. מצב שלישי הוא העברת מידע ניהולי. מידע כזה יכול לעבור גם לפי הסכמת המטופל.²⁰² מצב רביעי עוסק באינטרסים ציבוריים שונים. לפי החוק, ועדת אתיקה במשרד הבריאות יכולה לקבוע שמסירת המידע חיונית להגנה על בריאות הזולת או בריאות הציבור, ובכך, לבטל את רצונו של המטופל.²⁰³ מצב חמישי הוא מסירת מידע לצורכי מחקר ופרסום מדעי.²⁰⁴ המידע אמור להיות לא מזוהה, אם כי ניתן לקרוא את החוק בשתי דרכים: האחת, שההתממה צריכה להיעשות עוד לפני העברת המידע, והשנייה, שדרישת ההתממה חלה רק בשלב פרסום המחקר. אני סבור שהקריאה הראשונה היא הראויה.²⁰⁵

היתר שישי, כללי יותר, הוא כאשר יש חובה לפי דין למסור את המידע.²⁰⁶ היתר זה פותח את הפתח לחקיקה אחרת שקובעת חובה למסור מידע. זהו צינור רחב להעברת מידע רפואי. הנה רשימה לא ממצה של דינים שמחייבים או מתירים העברת מידע מגורמי הבריאות (רופא, קופת חולים, בית חולים) לגורמי מדינה: העברת נתונים למוסד לביטוח לאומי שדרושים לפעילותו;²⁰⁷ מידע על מחלות מדבקות;²⁰⁸ על מקרי סרטן;²⁰⁹ דיווח למכון הרפואי לבריאות בדרכים על מחלות מסוכנות לנהיגה,²¹⁰ דיווח של גורם מטפל למשרד הבריאות שיכול להעביר את המידע לפקיד רישוי נשק או לצה"ל, על מסוכנות בקשר להחזקת נשק;²¹¹ דיווח למשטרה או פקיד סעד על פגיעה בקטינים וחסרי ישע,²¹² דיווח למאגר החיסונים הלאומי.²¹³ לפי צו שהוצא לפי פרק ד לחוק הגנת הפרטיות שמסדיר העברת מידע בין גופים ציבוריים, מותר להעביר "ידיעות על מצב בריאותו של אדם לצורך הטיפול בו" מהמדינה, ונראה שהכוונה היא בעיקר למרשם האוכלוסין ולמוסד לביטוח לאומי, אל בתי החולים וקופות החולים, וכן מותר להעביר מידע דמוגרפי (תאריך ומקום לידה, ארץ לידת ההורים, שנת עלייה, ותאריך פטירה).²¹⁴ בנוסף, נזכיר את האפשרות של מסירת מידע במסגרת הליכים משפטיים – שם חל הכלל של חיסיון מידע רפואי, אבל לעיתים יש בצידו חריגים.²¹⁵

²⁰⁰ סעיף 20(א) לחוק זכויות החולה.

²⁰¹ סעיף 20(א) לחוק זכויות החולה. ראו גם את ההגדרה של "מטפל" בסעיף 2 לחוק.

²⁰² סעיף 20(א) לחוק זכויות החולה ("מסירת המידע הרפואי היא למוסד הרפואי המטפל או לעובד של אותו מוסד רפואי לצורך עיבוד המידע, תיוקו או דיווח עליו על פי דין).

²⁰³ סעיף 20(א) לחוק זכויות החולה. הסעיף קובע זכות טיעון למטופל. ועדת אתיקה מוקמת לפי סעיף 24 לחוק זה.

²⁰⁴ סעיף 20(א) לחוק זכויות החולה ("מסירת המידע הרפואי נועדה לפרסום בבטאון מדעי, למטרות מחקר או הוראה בהתאם להוראות שקבע השר ובלבד שלא נחשפו פרטים מזוהים של המטופל").

²⁰⁵ זו גם הקריאה של בר-זיו וזירסקי, "פרטיות במשבר זהות", לעיל ה"ש 134, בעמ' 135.

²⁰⁶ סעיף 20(א) לחוק זכויות החולה ("חלה על המטפל או על המוסד הרפואי חובה על פי דין למסור את המידע הרפואי").

²⁰⁷ לפי סעיף 40 לחוק ביטוח בריאות ממלכתי, התשנ"ד–1994. נראה שהתפקיד המרכזי הרלוונטי הוא חלוקת תקבולים, לפי סעיף 18 לחוק זה. החוק מציין, בסעיף 41, כי "מסירת מידע ונתונים לפי הוראות חוק זה לא תיעשה אלא במידה הנדרשת לביצוע הוראותיו, ותוך הגנה על הפרטיות של המבוטח ושמירה על הסודיות של המידע הרפואי הנוגע לו."

²⁰⁸ סעיף 12 לפקודת בריאות העם (1940); תקנות בריאות העם-הודעות על מחלות מדבקות, התשכ"א–1961.

²⁰⁹ תקנות בריאות העם (דיווח ומידע מיוחד על מחלת הסרטן), התשמ"ב–1982.

²¹⁰ סעיף 12(א) לפקודת התעבורה [נוסח חדש], התשכ"א–1961; סעיף 12 לחוק הטיס.

²¹¹ סעיף 11 לחוק כלי היריה, התש"ט–1949.

²¹² סעיף 368(ב) לחוק העונשין, התשל"ז–1977.

²¹³ סעיף 165 לפקודת בריאות העם, לפי חוק לתיקון פקודת בריאות העם (מס' 43), התשפ"ד–2024.

²¹⁴ צו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו–1986.

²¹⁵ לדיון, ראו עמית חסיונות ואינטרסים מוגנים, לעיל ה"ש 39, בעמ' 654.

אזכיר את המובן מאליו: קיומו של הסדר חוקי אינו מעיד בהכרח על המצב בשטח. דוח פיקוח של הרשות להגנת הפרטיות חושף פערים ניכרים. למשל, רק שניים מתוך 28 בתי חולים שנבדקו עמדו ברמה גבוהה בהוראות החוק בנוגע להעברת מידע בין גופים ציבוריים; שמונה – ברמה נמוכה, והשאר ברמה בינונית.²¹⁶

העברת מידע מגורמי הבריאות לגורמים פרטיים מוסדרת כמעט רק באופן כללי. נקודת המוצא היא חובת הסודיות והאיסור על העברת מידע, אלא לפי אחד ההיתרים הקודמים שצוינו. הראשון שבהם הוא הסכמת המטופל.²¹⁷ על גבי העוגן הזה, באות התקשרויות חוזיות משלושה סוגים שונים, שמאפשרים לגורמי הבריאות להיעזר בשירותים טכנולוגיים של גורמים פרטיים:

האחד, ספקי שירותים שגורם הבריאות מציע למטופלים, למשל יישומון כושר או שימוש באביזר כמו צמיד כושר לאיסוף מידע על דופק, מספר צעדים, ניטור שינה, ושריפת קלוריות. במקרה כזה, העוגן החוקי להעברת המידע הוא הסכמת המטופל/משתמש, שנדרש להסכים לתנאי השימוש של היישומון בעת התקנתו.

הסוג השני הוא מיקור חוץ, כלומר ספקי שירותים טכנולוגיים פרטיים שגורם הבריאות מתקשר איתם ישירות, כמו ספק שירותי ענן או מפתחי יישומונים. העוגן החוקי כאן להעברת המידע הוא ההתקשרות החוזית, ולפי נהלים של משרד הבריאות (אם יש כאלה), למשל בקשר לשימוש בשירותי רפואה מרחוק. במקרים אחרים, גורמי הבריאות מתקשרים עם ספקי שירות רפואיים או שירותים נספחים.

למשל, קופת חולים מכבי מציעה למבוטחיה שירות "מכבי UpApp" לפעילויות ספורט (פילאטיס, למשל) וסדנאות שונות, למשל הדרכת הורים. לפי תנאי השימוש, היישומון מופעל על ידי חברה אחרת, בשם "מובמנט וולנס בע"מ", ובמדיניות הפרטיות נזכרת חברה נוספת, פריפייט בע"מ שמתוארת כחלק מקבוצת החברות של מובמנט וולנס. במצבים האלה, המטופל/משתמש נדרש להסכים לתנאי השימוש של הגורם המסחרי הפרטי.²¹⁸ במדיניות הפרטיות נזכרים גופים רבים שהמידע עשוי לעבור אליהם: לבד מ"מכבי", גם "חברות אחרות בקבוצת מובמנט ו/או לספקים שלנו ו/או גופים העובדים בשיתוף פעולה איתנו ואשר מעניקים לנו שירותים שונים הכוללים גישה ו/או עיבוד של מידע אישי אותם מותר לנו לבצע בעצמה, כגון הפקת חשבוניות, גביית חובות, עיבוד מידע, שיווק, פרסום, שירות לקוחות, שירותים דיגיטליים ומסחר אלקטרוני, שירותי שליחויות ודואר, שירותי טכנולוגית מידע IT, שירותי סליקה, סוקרים ויועצי שיווק וכיו"ב". ובנוסף, נזכרת שם העברה לגורמים שלישיים אחרים, למשל לפי צו שיפוטי או במקרה של הפרת תנאי השימוש על ידי המשתמש. בסוף הרשימה נזכרת גם "העברת מידע למפרסמים בנושאים שאנחנו חושבים שיעניינו אותך". ברובד ההצהרתי, נראה שהגופים האלה (מכבי והחברות המסחריות) עומדים בדרישות החוק – הם מקיימים את חובת ההודעה הדרושה לפי סעיף 11 לחוק הגנת הפרטיות. הדוגמה לא נועדה לבקר את הגופים האלה, אלא להמחיש כיצד מידע רפואי שעובר מגורם הרפואה לספק שירות (והעוגן החוקי הוא של הסכמת המשתמש), עשוי לעבור בהמשך לגורם מסחרי (שוב, לפי העוגן של הסכמת המשתמש). הקושי נמצא בעומס הניכר שמוטל על כתפיה של ההסכמה.

פעולתם המקוונת של גורמי הבריאות ברשת מלווה לא אחת בטכנולוגיות נלוות, כמו Google Analytics.²¹⁹ גם כאן יש התקשרות חוזית, אבל היא נקבעת לפי תנאי השימוש של השירות הטכנולוגי המוצע, ויש להניח שלא אחרי משא ומתן פרטי. עד כמה מגנים תנאי השימוש של גוגל, בדוגמה הזו, על המידע הרפואי? ואזכיר, שגוגל היא חברה מסחרית, זרה. יש להניח שמידת הפיקוח של קופות החולים על השימושים שגוגל עושה במידע מוגבלת, ומידת הפיקוח של המטופל/משתמש – אפסית.

סוג שלישי של גורמים פרטיים שמסייעים לגורמי הבריאות הוא טכנולוגיות שהצוותים המטפלים משתמשים בהם בעצמם, שלא דרך ארגון הבריאות, כלומר העברת מידע על מטופלים בשיחות ווטסאפ ודוא"ל לא-ארגוני. גם כאן יש פערים בין ההסדר לבין יישומו בפועל.²²⁰

²¹⁶ הרשות להגנת הפרטיות דוח פיקוח רוחב: ממצאי הליך פיקוח רוחב בקרב מגזר בתי החולים (2024).

²¹⁷ סעיף 20(א)(1) לחוק זכויות החולה.

²¹⁸ ראו https://www.move-club.co.il/upapp_privacy/.

²¹⁹ בקשה לאישור תובענה ייצוגית בעניין נדחתה משום שחוק התובענות הייצוגיות, התשס"ו–2006 אינו כולל אפשרות לתביעות ייצוגיות בגין הפרת חוק הגנת הפרטיות, והיחסים בין מטופל לקופת חולים אינם יחסי עוסק-צרכן. ראו ת"צ (מחוזי ת"א) 68316-11-22 שבתאי אוסקר ז"ל נ' איכילוב המרכז הרפואי ת"א ע"ש סוראסקי (נבו 20.1.2025).

²²⁰ ראו הרשות להגנת הפרטיות הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעים דיגיטליים (2024).

התיאור כאן אינו ממצה – ואינו יכול להיות ממצה, שכן נוספים יישומונים חדשים כל העת, והשונויות בין האנשים גבוהה. אנשים שונים משתמשים ביישומונים שונים ותנאי השימוש משתנים מעת לעת. אבל המשותף הוא שהמידע שנאסף, עובר מיד ליד, מעובד, ומשמש חומר גלם בידי ספקי השירות, לא רק כדי להציע את השירות המידי, אלא גם כדי למסחר את המידע בדרכים שונות. בפן המשפטי, גם כן יש מן המשותף: המידע נאסף על בסיס הסכמה של המשתמשים, אולם ראינו את קוצר ידה של ההסכמה.

(ג) האתגר

המשגת הזירה של המידע הרפואי כמצב מידעי מורכב מאפשרת לחדד את האתגרים של ניהול המידע הרפואי. האתגר הראשון הוא המורכבות. אנחנו מתקשרים לא רק עם גורם הבריאות, אלא עם גורמים רבים נוספים, בדרך כלל פרטיים. גורמי הבריאות מעבירים מידע לגורמים אחרים – גופי מדינה, גורמים פרטיים ואחרים. מרגע שהמידע יצא מידינו (או ליתר דיוק, מגופנו), היכולת שלנו לשלוט בו הולכת ופוחתת ככל שהוא עובר מיד ליד, למשל מקופת החולים לספק שירות שמפעיל עבודה יישומון וממנו לספקי שירותים נלווים (שיעורי ספורט), ומהם לגורמים מסחריים.

האתגר השני הוא ההתבססות היתרה של בעלי השליטה במידע על ההסכמה כעוגן החוקי להעברות המידע, במיוחד מגורמי הבריאות לגורמים הפרטיים. ההסכמות של המטופלים מבססות את העברת המידע ממעגל הגופים שכפופים בצורה ישירה לדיני הפרטיות ולדיני הבריאות, למעגלים חיצוניים. אבל כאן נכנסות לתמונה המגבלות הרבות של עקרון ההודעה וההסכמה של דיני הפרטיות המידעית – ההודעות הארוכות, המסורבלות לעיתים, שמעטים קוראים ומעטים מבינים. ההקשר משתנה – מהקשר רפואי אנחנו עוברים בלי משים להקשר מסחרי. במעבר הזה, דיני הבריאות וכללי אתיקה רפואית, נזנחים, ולכל היותר מומרים בכללי הגנת הפרטיות "הרגילים" שההקשר שלהם הוא בעיקר מסחרי. במעבר מההקשר הרפואי למדינתי יש להוסיף את הרובד החוקתי, ואין להסתפק רק ברובד המקורי של דיני הפרטיות המידעית.

האתגר השלישי הוא זה של קריסת הקיטוע המשפטי. ניסיון להתחקות אחרי זרימת המידע מוביל מגוף מאוסדר לגוף מדינתי ולגוף פרטי, מגוף אחד לאחר, כשכל מקטע כפוף למערכת דינים ספציפית וכללית (כללי המשפט הציבורי, למשל) שונה. ההפרדה בין מישורי הפעולה של הפרטיות קורסת, ההקשרים שהיו שונים קורסים זה לתוך זה (ולכן, כאמור, גישתה של ניסנבאום אינה מועילה מאותו רגע), והכללים המשפטיים מתערבבים. בנוסף, מאחורי הקלעים יש מערכת חוזית בין הגופים השונים – שאינה חשופה לציבור. קופות החולים אמנם כפופות לחוק חופש המידע, התשנ"ח-1998,²²¹ אולם לחוק זה חריגים רבים, ובין היתר אין חובה למסור מידע בנוגע לסוד מסחרי.²²² גופים פרטיים אינם כפופים לחוק זה.

דוחות של הרשות להגנת הפרטיות ממחישים את האתגר של הקיטוע המשפטי שמצבי מידע מורכבים מציבים למשפט. מספר מסמכי מדיניות ודוחות פיקוח בחנו היבטי פרטיות בקשר למידע רפואי. בחלקם, ההסתכלות נקודתית, על שחקן אחד, למשל מרפאות לבריאות הנפש,²²³ מכונים רפואיים ומעבדות מחקר,²²⁴ בתי חולים,²²⁵ או גופים שמספקים שירותי רפואה מרחוק ("רפואה דיגיטלית").²²⁶ פיקוחי הרוחב בוחנים בקרה ארגונית בגופים שנבדקו, את אופן ניהול מאגרי מידע, והיבטים של אבטחת מידע, ולפי העניין מיקור חוץ והעברת מידע בין גופים ציבוריים. הדוחות מתמקדים ביחסים שבין הגורם שנבדק לבין נושאי המידע ומעירים, לפי הצורך, על מיקור חוץ. במונחים שתיארת כאן, המסמכים מתמקדים במקטע אחד של המערכת הרפואית, ואינם רואים את התמונה הכללית של מצב המידע המורכב. אין כאן ביקורת על הרשות – היא מוסמכת לבחון את יישומו של החוק הקיים, ופעילותה חשובה בהיבט הציות לחוק והעלאת המודעות. הקושי נמצא במבנה הבסיסי של הדין – הקיטוע המשפטי של שלושת מישורי הפעולה והיחסים הדו-צדדיים בכל מישור כזה.

²²¹ ראו צו קביעת רשות ציבורית לפי חוק חופש המידע, התשנ"ח-1998, י"פ 5157 (10.2.2003). ליישום, ראו למשל עת"ם (מנהלי ת"א) 2032/08 התנועה לחופש המידע נ' שירותי בריאות כללית (21.2.2011).

²²² סעיף 9(ב)6 לחוק חופש המידע.

²²³ הרשות להגנת הפרטיות דוח פיקוח רוחב: ממצאי הליך פיקוח הרוחב בקרב מגזר מרפאות בריאות הנפש בישראל (2020).

²²⁴ הרשות להגנת הפרטיות דוח פיקוח רוחב: הגנת הפרטיות בקרב מכונים רפואיים ומעבדות מחקר משרד הבריאות (2020).

²²⁵ הרשות להגנת הפרטיות דוח פיקוח רוחב: ממצאי הליך פיקוח רוחב בקרב מגזר בתי החולים (2024).

²²⁶ הרשות להגנת הפרטיות דוח פיקוח רוחב: ממצאי הליך פיקוח הרוחב בקרב מגזר הרפואה הדיגיטלית (2024).

בדיקה מעניינת בהיבט הזה היא של העברת מידע רפואי באמצעים דיגיטליים, כלומר תוכנות תקשורת של הארגון הרפואי או תוכנות מסחריות במכשירים הפרטיים, או בקיצור, ווטסאפ. הרשות הצביעה על חשש מזליגת המידע וחשיפתו, גניבתו ושיבושו, והיבט של היעדר הסכמה של המטופלים. במסמך הייתה התייחסות חשובה שמאפיינת את המצב המידעי המורכב:

”שמירת והעברת מידע רפואי על אודות מטופלים בתוכנות הנמצאות בבעלות חברות תקשורת ומידע מסחריות עלולות להביא גם לכך שחברות אלו ישתמשו במידע (או בחלקים ממנו) לצרכיהן. חשש זה הוא קריטי בעיקר ביחס לתוכנות ואפליקציות 'חינמיות' להעברת מידע, אשר המודל הכלכלי שלהן מבוסס על מתן שירותים ללא עלות כספית בתמורה לאיסוף ועיבוד המידע הנשמר והמועבר באמצעותן.”²²⁷

הרשות המליצה לצמצם שימוש כזה, להימנע משמירת מידע רפואי במכשירים פרטיים, כשאין מנוס, להשמיט פרטים מזהים של המטופל, למחוק את המידע בהקדם, ולא לשמור את המידע בשירותי ענן, ועוד. מסמכים נוספים שמעידים על ערנות למצב מידע מורכב הם המלצות של הרשות למשתמשים במכשירי כושר, כמו צמידי כושר ומשתמשים ביישומי בריאות וכושר.²²⁸ גם כאן, נקודת המוצא היא שגוף מסחרי אוסף מידע פרטי, בחלקו בריאותי. הסיכונים שזוהו הם של אבטחת מידע, איסוף מידע עודף, שימוש במידע למטרות נוספות, וגנישה למידע שאגור במכשיר הפרטי.

האתגרים מצטרפים זה לזה, ומדגישים את הצורך בחשיבה מחודשת על מבנה הדין.

סיכום

המידע הרפואי שלנו יקר ערך – לנו, וגם לגורמי ביניים שמחזיקים במידע הזה, ולציבור בכללותו. אנחנו מקור המידע הרפואי שעל אודותנו, אבל המידע נוצר בדרך כלל במהלך טיפול עם גורמי רפואה, נשמר אצלם, או נמסר להם. המידע הרפואי נוצר בעוד שלל זירות, לא רק בליבת הטיפול הרפואי אלא גם בפעילויות נלוות של המטופלים במסגרות והקשרים מסחריים. במאמר זה בחנתי את המפגש של המידע הרפואי עם טכנולוגיות חדשות של נתוני עתק ובינה מלאכותית, והצגתי את זירת המידע הרפואי כמצב מידעי מורכב.

הדיון מעלה כמה מסקנות ולקחים. למרות הפיתוי להתחיל את הדיון בנקודת הסיום – איזון בין האינטרס הציבורי בגישה למידע רפואי לבין הזכות לפרטיות – יש לברר את הסוגיות לעומקן, לבחון האם יש פגיעה בפרטיות בשלבים קודמים של השימוש במידע, ומהי. רק אז אפשר לגשת למלאכת האיזונים. בבירור הפגיעה, אין להצטמצם לחשש מדליפת המידע ושימושים לרעה במידע, ויש לבחון את המידע לכל אורך מהלך החיים שלו. הבנת הפרטיות כשליטה נמשכת בכל שלבי מהלך החיים של המידע, משקפת את ההצדקות השונות של הזכות לפרטיות, וממחישה את הצורך בבחינה מלאה. מאותה סיבה, התממה של המידע יכולה לכל היותר לאיין פגיעות בפרטיות בשלב השימוש הגלוי במידע הרפואי, אבל היא אינה מאיינת פגיעה בפרטיות בשלבים קודמים של מהלך החיים של המידע, לפני שהותמם.

בפן המשפטי, ראינו את העומס הרב שמוטל על כתפיו של עקרון ההודעה וההסכמה, ואת הקשיים הרבים ביישומו. יש לחזק את ההסכמה בדיני הפרטיות בכלל, ולענייננו, בנוגע למידע רפואי. יש להעדיף באופן נחרץ בררת מחדל של opt in על פני בררת מחדל של opt out, יש לאפשר חזרה מהסכמה, יש לדרוש הודעה ברורה ככל האפשר, שאינה כורכת את נושאי הפרטיות בסוגיות שאינן קשורות.²²⁹ המסגרת של המצב המידעי המורכב מדגישה את הצורך לעקוב אחרי המידע גם כאשר הוא עובר מהקשר אחד לאחר, כלומר מהקשר רפואי למסחרי או בכיוון ההפוך. המעברים האלה אינם חלקים, יש בהם חרכים ופערים, ויש לוודא שהגנת הפרטיות בהקשר אחד לא נעלמת או נחלשת רק משום שהמידע עבר להקשר אחר.

כמו בכל הקשר משפטי-טכנולוגי, הפתרון לאתגרים השונים אינו רק משפטי, אלא פתרון משולב: על רקע הכללים המשפטיים, דרושה חשיבה טכנולוגית – כיצד לאפשר שליטה טובה יותר של נושא המידע במידע

²²⁷ ההדגשה במקור. הרשות להגנת הפרטיות המלצות להתנהלות הציבור בשימוש במכשירים לבישים למטרות ספורט ובריאות (2021); הרשות להגנת הפרטיות הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעים דיגיטליים פסקה 9.9 ד (2024).

²²⁸ הרשות להגנת הפרטיות המלצות להתנהלות הציבור בשימוש באפליקציות בריאות וכושר (2021).

²²⁹ לפירוט, ראו בירנהק ורחום-טוויג, פרטיות מידעית, לעיל ה"ש 21, בעמ' 193.

הרפואי שעל אודותיו, באופן נוח, פשוט וזול ככל האפשר, תוך ערנות לפערים באוריינות הבירוקרטית של אנשים שונים. דרושה הפנמה ארגונית – אצל גורמי הבריאות ואצל שחקנים אחרים שעוסקים במידע רפואי, של החשיבות, הזהירות שיש לנקוט, הסכנות, והפתרונות. נראה שאצל גורמי הבריאות יש ערנות כזו, בעיקר בזכות האתיקה הרפואית שמושרשת בחינוך הרפואי, אולם תמיד חשוב לחזקה. בדין האירופי אנו רואים שורה של כלים ארגוניים, בדרך של משפט הליכי – שמחייב ארגונים להטמיע הליכים מסוימים, לאו דווקא בדרך של דרישה משפטית לתוצאות. הכוונה היא לחובה לקיים תהליכים של הנדסת פרטיות, לערוך תסקיר הגנת פרטיות מקדים, ולמנות ממונה הגנת פרטיות.²³⁰ מכל אלה, בדין הישראלי יש כיום חובה למנות ממונה הגנת פרטיות,²³¹ וחובה מצומצמת יותר ליצור "מסמך הגדרות מאגר", בהיבטי אבטחת מידע.²³²

האתגרים רבים, המשימות רבות, אבל על הפרק נמצאות שתי זכויות יסוד – הזכות לבריאות והזכות לפרטיות, וכל אחת מהן דרושה לשנייה.

²³⁰ ראו סעיפים 25 ל-GDPR (הנדסת פרטיות), 35 (תסקיר), 37 (ממוני הגנת פרטיות).

²³¹ סעיף 17ב1 לחוק הגנת הפרטיות.

²³² תקנה 2 לתקנות אבטחת מידע.