הצעה לסדר 14

אתגר הפרטיות בפרסום יזום של מאגרי מידע ממשלתיים

רחל ארידור־הרשקוביץ | תהילה שוורץ אלטשולר

ספטמבר 2017

המכון הישראלי
לדמוקרטיה

אתגר הפרטיות בפרסום יזום של מאגרי מידע ממשלתיים

רחל ארידור־הרשקוביץ | תהילה שוורץ אלטשולר

המכון הישראלי לדמוקרטיה

הצעה לסדר 14

ספטמבר 2017

Transparency in the Digital Age: Privacy, Personal Information and Proactive Disclosure of Government Datasets

Rachel Aridor-Hershkovitz, Tehilla Shwartz Altshuler

עריכת הטקסט: מיכאלה קלי, ענת ברנשטיין
עיצוב הסדרה: יוסי ארזה
עימוד והבאה לדפוס: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים

מסת"ב ISBN 978-965-519-206-3

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר), תשע"ח
נדפס בישראל, 2017

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר – כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו"ל.

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים:
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800 ; פקס: 02-5300867

כל פרסומי המכון ניתנים להורדה חינם, במלואם או בחלקם, מאתר האינטרנט.

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס״ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

הדברים המתפרסמים בסדרת ״הצעה לסדר״ אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.

תוכן העניינים

תקציר 7

א. רקע 11

ב. חשיבות הפרסום היזום של מאגרי מידע ממשלתיים ותכליותיו 18

1. התכלית הדמוקרטית 18
2. התכלית הכלכלית 21

ג. הבעיה: פרסום יזום של מאגרי מידע ממשלתיים כבררת מחדל והפגיעה הצפויה בזכות לפרטיות 27

1. הזכות לפרטיות בעולם דיגיטלי: רקע 27
2. פרטיות ופרסום יזום של מאגרי מידע שלטוניים 30

ד. פרסום יזום ומזעור הפגיעה בפרטיות: סקירת הפתרונות המוצעים בספרות ובמשפט המשווה 33

1. סיווג של מאגרי מידע והגדרה מראש של מאגרים מותרים לפרסום יזום 34
2. פרסום יזום מתוך מזעור הסיכונים לפגיעה בפרטיות 36

(א) מהי התממה ומהן טכניקות ההתממה המוכרות? 38

(ב) התממה וסכנת הזיהוי החוזר 41

3. איזון בין האינטרסים המתנגשים 47

ה. פרסום יזום של מאגרי מידע בישראל 53

1. המצב החקיקתי הקיים 53

2. ההסדר המוצע בהחלטת הממשלה ובדוח הצוות הבין־משרדי 55

ו. דיון והמלצות 61

1. המצב הקיים 61

2. המלצות 64

(א) הטלת חובה בחוק חופש המידע לפרסום יזום של מאגרי מידע ממשלתיים 64

(ב) הסמכת גוף אחד לביצוע מכלול הפעולות הקשורות ביישום ההחלטה 65

(ג) קביעת כללי אצבע לסיווג מידע ולמיפוי מהיר של מאגרי מידע שאינם כוללים מידע מזהה 68

(ד) קביעה ואימוץ כללים מנחים להתממה ולזיהוי חוזר 70

(ה) קביעת מתווה למרחב השיקולים הרלוונטיים לאיזון בין אינטרסים מתנגשים 71

(ו) בניית מאגרי מידע חדשים 75

ז. סיכום 76

תקציר

בשנים האחרונות, כחלק מתפיסה של ממשל פתוח ובמסגרת מימוש של חוקים העוסקים בחופש מידע ובשקיפות שלטונית, מדינות מערביות נוקטות מדיניות פרסום יזום של מאגרי מידע וצבירי נתונים שבידי רשויות השלטון. מדינת ישראל הצטרפה רשמית למגמה זו באוגוסט 2016,[1] עם החלטת ממשלה 1933 לקידום הנגישות של מאגרי מידע ממשלתיים לציבור. בין השאר הטילה החלטה זו על רשויות השלטון, כברירת מחדל, את החובה לפרסם ביוזמתן את מאגרי המידע שברשותן.

לפרסום יזום של מידע ממשלתי יתרונות רבים, ואלה הוצגו במחקר המדיניות שלנו בנושא הטמעת מדיניות ממשל פתוח בעידן הדיגיטלי (2012), בדוח הצוות הבין־משרדי[2] ובהחלטת ממשלה 1933. בהיבט הדמוקרטי, פרסום יזום מוביל להגברת השקיפות של פעולות הממשלה, להידוק הפיקוח והבקרה על פעולותיה, לשיפור השירות שהיא נותנת ולחיזוק אמון הציבור בה. לפרסום יזום של מידע ממשלתי יש גם תכלית כלכלית: גלום בו פוטנציאל להגברת החדשנות המבוססת על מידע זה ולכן גם לרווח כלכלי, להתייעלות ולקידום המחקר והפיתוח.

בצד ההגשמה של תכליות אלה, פרסום יזום כרוך בסכנה לפגיעה בפרטיות. חלק ממאגרי המידע הממשלתיים כוללים מידע אישי שנאסף במסגרת הפעילות השלטונית ומכוח סמכות חוקית. יש להביא בחשבון שבדרך כלל אדם המוסר מידע אישי לרשויות השלטון אינו עושה זאת מרצונו החופשי או בכפוף להסכמה אמיתית וחופשית, אלא מכורח החלטה שלטונית וחובה חוקית ולשם מטרה

1 החלטה 1933 של הממשלה ה־34 "שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור" (30.8.2016). אין זו החלטת הממשלה הראשונה בנושא ממשל פתוח. קדמו לה שתי החלטות שנזכיר בהמשך המסמך, אך זו ההחלטה הראשונה המבקשת לראות במאגרי המידע כאלה שצריכים להיות פתוחים לציבור כברירת מחדל.

2 המלצות הצוות הבין־משרדי לשיפור העברת מידע בין משרדים ויחידות סמך (היחידה לשיפור השירות הממשלתי לציבור, רשות התקצוב הממשלתי, משרד ראש הממשלה), מיום 28 ביולי 2016.

ספציפית המוגדרת בחוק. פרסום יזום של מידע כזה בלי לבדוק מראש את רצונו והסכמתו של האדם שמסר אותו עלול לפגוע בזכותו לפרטיות באופנים שלא הובאו בחשבון בעת שנקבעה החובה החוקית למסור אותו. הפגיעה בפרטיות עקב הפרסום היזום עשויה להתבטא באובדן השליטה של אותו אדם על המידע שמסר (משום שהרשות הציבורית שאספה אותו מאבדת בעצמה את השליטה בו מרגע פרסומו); בניצול המידע שפורסם לשימושים שלא הסכים להם; בהפיכת המידע שמסר לנכס סחיר; ובפגיעות ממוקדות יותר כגון גנבת זהות, מציצנות ושימוש לרעה במידע. פגיעות אלה אינן נוגעות רק לפרטיותם של מוסרי המידע; הן כרוכות בפגיעה כללית יותר באמון של הציבור ברשויות השלטון, שכן הללו נתפסות כמועלות בחובתן להגן על פרטיות המידע שברשותן.

במצב החקיקתי הקיים אין הסדר למזעור הפגיעה הצפויה בזכות לפרטיות עקב פרסום יזום של מידע שלטוני. אמנם חוק חופש המידע, התשנ"ח-1998, מכיר בכך שזכות האזרח לקבל מידע מרשות ציבורית נסוגה מפני פגיעה בפרטיות (על פי חוק הגנת הפרטיות, התשמ"א-1981); ואולם הכרה זו מצומצמת – כמו החוק כולו – לנסיבות של בקשת מידע ספציפית (גם אם זו בקשה לקבל מאגר מידע) ואינה נוגעת לפרסום יזום שלא מכוח בקשה כזו. גם חוק הגנת הפרטיות אינו מתייחס במפורש לפרסום יזום של מאגרי מידע ממשלתיים.

ההסדר המוצע בהחלטת ממשלה 1933 מטיל על כל משרד ממשלתי מעמסה מורכבת: על כל משרד למפות את מאגרי המידע שברשותו ולבחון, עבור כל אחד מהם, אם יש בו מידע פרטי או מידע שיש בכוחו לזהות פרטים, לרבות מידע שיכול להוביל לזיהוי חוזר – כלומר לאפשרות להצליב את המאגר השלטוני שהונגש עם נתונים אחרים כדי לדעת את זהות הפרטים. על פי ההחלטה, בחינת הסיכויים לזיהוי חוזר תיעשה בידי מומחה מהתחום הטכנולוגי ותלווה בייעוץ משפטי ובייעוץ בתחום אבטחת מידע.

במצב שנוצר לאחר החלטת הממשלה אין חובה חוקית להנגיש באופן יזום מאגרי מידע שלטוניים. הדבר מעוגן רק בהחלטת ממשלה 1933 ועל כן מנוגד לאיסור הקבוע בסעיף 23ב לחוק הגנת הפרטיות, האוסר על רשות ציבורית למסור מידע בהיעדר סמכות או הרשאה בדין. כמו כן אין בהסדר המוצע בהחלטת ממשלה 1933 כדי להוות מדיניות ברורה, מפורטת ומלאה המאזנת בין האינטרס הציבורי שבפרסום יזום לאור תכליותיו הדמוקרטית והכלכלית לבין הפגיעה בפרטיות. ללא מתווה יעיל ומעשי שכזה תכנית הפרסום היזום של

מאגרי המידע הממשלתיים עלולה להתמוסס או, לחלופין, להתבצע באופן לא אחראי שעלול לפגוע בזכות לפרטיות.

במחקר זה אנו סוקרות את השיקולים העומדים על הפרק לעניין פרסום יזום של מאגרי מידע ממשלתיים ובוחנות כיצד מדינות אחרות מתמודדות עם הצורך לאזן בינו לבין הגנה על הפרטיות של האזרחים. בסופו של דבר, ובהתאמה למצב המשפטי בישראל, זו הצעתנו:

1. לתקן את חוק חופש המידע ולהוסיף לו חובה לפרסום יזום של מאגרי מידע שלטוניים. בדרך זו תעוגן בחוק חובת הפרסום היזום, הקבועה כעת רק בהחלטת ממשלה 1933. כך תוכפף החובה גם לעקרון המידתיות המעוגן ממילא בחוק חופש המידע וגם למנגנון הקיים בחוק לעניין עתירה לבית המשפט.
2. האחריות והפעולות הנדרשות לשם פרסום יזום של מאגרי מידע ממשלתיים ירוכזו בידי גוף מרכזי אחד כגון רשות התקשוב הממשלתי, נוסף על האחריות הפרטנית המוטלת על כל משרד ממשלתי לפי החלטת ממשלה 1933 כפי שתעוגן בחוק.

אלה יהיו תפקידי הגוף המרכזי:

א. הגוף המרכזי יפעל להבטיח שמשרדי הממשלה ינקטו פרסום יזום של מאגרי המידע שברשותם, שאינם כוללים מידע מזהה, ויפקח על הפעולות שיינקטו לשם כך.

ב. הגוף המרכזי ישמש גורם מייעץ ומנחה למשרדי הממשלה בכל שאלה הנוגעת לחובת הפרסום היזום.

ג. הגוף המרכזי יקבע, לאחר היוועצות בגורמים המתאימים מהאקדמיה ומהתעשייה, כללי אצבע למיפוי מהיר של מאגרי המידע שאינם כוללים מידע מזהה.

ד. הגוף המרכזי יקבע, לאחר היוועצות בגורמים המתאימים מהאקדמיה ומהתעשייה, כללים מנחים ליישום טכניקות של הַתְמָמה (אנונימיזציה; de-identification). הכללים יכללו הנחיות ברורות באשר לשיקולים שיש לשקול בעת היישום של טכניקת ההתממה ובאשר לבחינת יעילותה בהשגת מטרת הפרסום בצד מזעור הפגיעה בפרטיות.

ה. הגוף המרכזי יקבע, לאחר היוועצות בגורמים המתאימים מהאקדמיה ומהתעשייה, כללים מנחים לבדיקת הסיכויים לזיהוי חוזר ולבחינת הצורך בפרסום תחת הגבלות, על בסיס מבחן המידתיות המקובל כיום בביקורת שיפוטית על החלטת רשות מינהלית.

ו. הגוף המרכזי יבחן ויכריע בעצמו, לאחר היוועצות במומחה טכנולוגי וביועץ אבטחת מידע, באשר לסיכויים לזיהוי חוזר ובאשר לפרסום יזום של מאגר מידע, עם או בלי הגבלות הנובעות מעילת המידתיות. בדרך זו יובטח כי מדיניות הפרסום היזום תהיה אחידה וכי השיקולים שיישקלו יכללו הן שיקולים הנוגעים להגנת הפרטיות והן שיקולים הנוגעים להגברת השקיפות והאחריותיות של הממשלה כלפי האזרחים.

ז. הגוף המרכזי יקבע הנחיות ברורות, צופות פני עתיד, באשר להקמה, לארגון ולשמירה של מאגרי מידע חדשים באופן שיאפשר את פרסומם היזום בהליך מהיר, זול ויעיל.

א. רקע

מאגר מידע (data set)[1] הוא אוסף של נתונים המאורגנים בתבנית של עמודות ושורות (כגון טבלה או מערך מטריציוני אחר), שבה כל עמודה מייצגת משתנה מסוים וכל שורה מתייחסת לנושא מידע מסוים. בסופו של דבר מאגר המידע כולל ערכים (או נתונים, data) המתייחסים לכל אחד מהמשתנים עבור כל אחד מנושאי המידע. הנתון יכול להיות מספרי (כמו פירוט משקלו של אדם בק"ג) או מילולי (כמו השתייכותו האתנית של האדם). לעתים יש למונח "מאגר מידע" מובן כללי יותר – תיאור של נתונים המוצגים בטבלאות בנושא מסוים או תיאור אוסף של נתונים שבידי השלטון.

השלב הראשון של שיח השקיפות בישראל בא לידי ביטוי בחוק חופש המידע, התשנ"ח-1988, בהקמת היחידה לחופש מידע במשרד המשפטים ובמערך הפסיקה שדנה בחוק. שלב זה התמקד בחובה השלטונית למסור מידע לאזרחים, בגבולות החובה הזו ובהטמעתה הארגונית, באיזונים שבין זכות הציבור לדעת ובין זכויות אחרות (כמו הזכות לפרטיות והזכות לקניין) ובאיזונים שבין זכות הציבור לדעת ובין אינטרסים ציבוריים (כמו ביטחון המדינה ויעילות מינהלית).

בחמש השנים האחרונות מתפתחת בצד חופש המידע מדיניות של ממשל פתוח, שמתקדמת לעבר השלב השני של שיח השקיפות. שלב זה אינו מסתפק בחובה למסור מידע שלטוני בעקבות דרישה אלא מבקש לקדם שקיפות שלטונית יזומה ופרו־אקטיבית. לשם כך שלב זה מתייחס גם לארגון המידע השלטוני באופן שיאפשר את הנגשתו היזומה על ידי השלטון ואת השימוש השניוני בו על ידי מגזרים נוספים בחברה, כלומר הפיכתו למשאב בר־שימוש. גם בשלב זה השקיפות השלטונית מכירה בחשיבות של הנגישות למידע לעצם קיומו של הליך דמוקרטי תקין, ולכן היא דורשת הגנה על זכות הציבור לדעת, פיקוח על מעשי השלטון, לחימה בשחיתות שלטונית והגברת האחריותיות. כך למשל,

1 "מאגרי מידע" מכונים בחוק הגנת הפרטיות, התשמ"א-1981, ס"ח 1011 (להלן: חוק הגנת הפרטיות), "סדרות" או "בסיסי נתונים", ובהחלטת הממשלה שתידון להלן הם מכונים "מאגרי מידע". בחרנו להשתמש בביטוי "מאגרי מידע" כדי לשמור על הקשר בינו לבין הביטויים "חופש המידע" ו"עידן המידע". לתפיסתנו, הניתוק בין "נתונים" לבין "מידע" מקשה על אפשרות השיח בין עולמות אלה.

דרישות להנגשת מידע יזומה מטעמים של שמירה על הדמוקרטיה מתמקדות בתחומים כמו תקציב המדינה, התקשרויותיה הכלכליות של הממשלה, נתונים על פשיעה, תאונות דרכים, שכר העובדים בשירות הציבורי והישגי התלמידים במערכת החינוך הציבורית.

במסגרת הדיון בהנגשה יזומה של מידע שלטוני חשוב לזכור כי בעידן המידע הממשלה עצמה היא פלטפורמה של מידע. מערכות המידע שהשלטון יוצר הן בסיס לפעילות חוץ־שלטונית שיש לה ערך כלכלי וחברתי. המידע השלטוני נתפס כרכוש הציבור לא רק משום שהוא אכן מבוסס על נתונים שהציבור סיפק, אלא גם משום שהוא משמש תשתית וזרז לעושר של הזדמנויות עסקיות וחברתיות, לחדשנות ולמחקר יישומי. המידע השלטוני הוא תשתית המאפשרת יזמות ופיתוח של הכלכלה והחברה – בדיוק כפי שהיו בעבר התדרים האלקטרו־מגנטיים, הכבישים ורשתות החשמל והמים. מאגרי מידע שלטוניים בארצות הברית, למשל, משמשים בסיס למספר לא מבוטל של אפליקציות פרטיות ומסחריות: אפליקציית HDScores משתמשת במאגרי מידע ממשלתיים אמריקניים ומאפשרת לציבור לבחון את הציון שקיבלה מסעדה מסוימת בבדיקות התברואה הממשלתיות;[2] אפליקציית Spot Crime מספקת למשתמשים מידע על כל עברה, לרבות גנבה או שוד, המבוצעת בשכונת מגוריהם;[3] האתר USA Spending.gov מאפשר לאזרחים ללמוד על ההוצאות של משרדי הממשלה; ואפילו חברת האנימציה פיקסאר השתמשה במידע גאולוגי שפורסם באופן יזום על ידי ממשלת ארצות הברית כדי ליצור סצנות ריאליסטיות בסרט "הדינוזאור הטוב".[4] אלה הן אך דוגמאות ספורות מתוך מאות.

ואכן, ויכוח עקרוני מתקיים על הצורך לממן את פתיחת מאגרי המידע השלטוניים מכספי משלם המסים ולהנגיש מאגרי מידע אלו בחינם כאשר מי שעשוי להפיק מהם רווח כלכלי הם אנשים או חברות פרטיות. ואולם ויכוח זה חורג מגדר המחקר שלנו.

המדיניות של פתיחת מאגרים היא מגמה מתפתחת בעולם וחלק משינוי במדיניות של רשויות שלטוניות בנוגע לניהול מידע. נשיא ארצות הברית

2 למידע נוסף על האפליקציה ראו באתר **hdscores**.

3 למידע נוסף על האפליקציה ראו באתר **spotcrime**.

4 Beth Simone Noveck, *Is Open Data the Death of FOIA?,* 126 Yale L. J. (2016)

לשעבר ברק אובמה חתם בשנת 2013 על צו נשיאותי ברוח זו, וכך גם משרד ראש הממשלה הבריטי. בשתי המדינות היה בכך כדי להביא לעלייה גדולה בחשיפה של מאגרי מידע ממשלתיים. התייחסות לשימוש חוזר במידע ממשלתי מופיעה גם במסמכים ובניירות עמדה של ארגון המדינות המתועשות (G8), של ארגון OECD ושל האו"ם.[5]

מדינת ישראל הצטרפה אף היא למגמה העולמית של הנגשת מאגרי מידע שלטוניים. בהחלטת ממשלה משנת 2012 התחייבה ממשלת ישראל לקדם את תחום הממשל הפתוח בהקמת "פורום הממשל הפתוח", שאחד מתתי הצוותים שלו עסק במאגרי מידע שלטוניים. בשנת 2013 הצטרפה ישראל ל"יוזמת הממשל הפתוח הבינלאומית" (Open Government Partnership),[6] ובשנת 2015 הציעה היחידה הממשלתית לחופש המידע במשרד המשפטים תיקון לחוק חופש המידע והתקנות אשר עסק, בין השאר, בהרחבת רשימת התחומים שיש להנגיש באופן יזום והתייחסה גם להנגשה יזומה של סדרות נתונים.[7]

מדינת ישראל נמצאת בחזית הפיתוח הטכנולוגי בתחומים כמו בינה מלאכותית, "למידה עמוקה" על ידי מכונה וניתוח אלגוריתמי של נתוני עתק (big data). פתיחת מאגרי מידע היא צינור חמצן כלכלי. בריאיון שהתקיים בתחילת 2017 עם ד"ר קירה רדינסקי, המדענית הראשית של Ebay ישראל, התייחסה רדינסקי למאגרי המידע של קופות החולים בישראל וציינה כי "סביב המידע הזה אפשר לבנות כלכלה שלמה, וישראל יכולה להוביל אותה – צריך לחשוב על זה כעל הנפט שלנו".[8]

5 יש ויכוח עקרוני באשר לצורך לממן את פתיחת מאגרי המידע השלטוניים מכספי משלם המסים ולהנגיש אותם חינם, מאחר שאנשים או חברות פרטיות עשויים להפיק מהם רווח כלכלי; אך ויכוח זה חורג מענייננו.

6 ראו באתר **opengovpartnership**.

7 החלטה 4515 של הממשלה ה־32 "הצטרפות לשותפות הבינלאומית לממשל פתוח ומינוי הפורום הישראלי לממשל פתוח" (1.4.2012); החלטה 5124 של הממשלה ה־32 "הפורום הישראלי לממשל פתוח" (23.9.2012); הצעת חוק חופש המידע (תיקון – יישום שקיפות המידע לטובת הציבור), התשע"ה–2015, פ/20/1825.

8 אלירן רובין "ד"ר קירה רדינסקי: "המידע הרפואי של קופות החולים הוא הנפט של ישראל" **דה מרקר** 14.12.2016.

מסוף מידע לציבור הרחב
לשלוט בתנועה
לנהל תנועה
לאכוף תנועה
לתכנן תנועה
לנהל תנועה
לשלוט בתנועה
מרכז בקרה לתנועה
מרכז בקרה לתנועה
מרכז בקרה ל

התרשים לעיל, המבוסס על המחקר "מדיניות ממשל פתוח בישראל",[9] מתאר את "מודל החיים" של המידע השלטוני. באות בו לידי ביטוי האפשרויות החברתיות והכלכליות הגלומות בפתיחת מאגרי המידע השלטוניים, כמו גם התנועה המחזורית שתחילתה בפתיחה של מאגרי נתונים שלטוניים והמשכה בעיבודם על ידי יזמים וחברות. עיבודים אלה – פיתוחים חדשניים ואפליקציות לשימושים כלכליים וחברתיים לטובת משתמשי קצה – עשויים, בתורם, לתת משוב באשר לאיכות המידע ולצורך במידע נוסף.

בסוף אוגוסט 2016 קיבלה ממשלת ישראל החלטה בדבר הנגשה של מאגרי המידע הממשלתיים.[10] החלטת ממשלה 1933 הטילה על משרדי הממשלה שתי חובות מרכזיות חדשות:

(1) חובת פרסום יזום כברירת מחדל: על משרדי הממשלה למפות את מאגרי המידע הממשלתיים[11] שברשותם ולהנגישם לציבור, במטרה לעודד קידום חדשנות במתן שירותים לציבור, קידום הצמיחה במשק באמצעות פעילות המסתמכת על המידע וקידום השקיפות של עבודת הממשלה. עם זאת – בהיעדר עיגון בחוק – מעמדה המחייב של חובת הפרסום היזום הקבועה בהחלטת ממשלה 1933 מוטל בספק, בגלל סעיף 23ב לחוק הגנת הפרטיות האוסר על גוף ציבורי למסור מידע אלא אם "המידע פורסם לרבים או הועמד

9 תהילה שוורץ אלטשולר **מדיניות ממשל פתוח בישראל בעידן הדיגיטלי** 81 (מחקר מדיניות 91, 2012).

10 החלטה 1933 של הממשלה ה־34 "שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור" (30.8.2016) (להלן: החלטת ממשלה 1933). קדמה להחלטה עבודת מטה בין־משרדית, בהובלת רשות התקשוב הממשלתי במשרד ראש הממשלה. על חשיבות ההחלטה אפשר ללמוד מדברים שאמר ראש הממשלה בנימין נתניהו במעמד קבלת ההחלטה: "הגיע הזמן ש'הסטארט אפ ניישן' יגיע גם ל'סטארט אפ גוברנמנט'. אנחנו הולכים לחולל מהפכה בעניין הזה". ראו אתר משרד ראש הממשלה, מרכז תקשורת, הודעות הדובר 30.8.2016.

11 "מאגר מידע" מוגדר בהחלטת ממשלה 1933 "מסד נתונים או סדרת נתונים של מידע מכל סוג, לרבות כל אוסף מובנה של נתונים, בין אם מוגדר במשרד הממשלתי או ביחידת הסמך כ'מאגר' לצרכים פנימיים ובין אם לאו"; ראו שם.

לעיון הרבים על פי סמכות כדין", וכן משום שהחלטת ממשלה אינה נחשבת "דין" כהגדרתו בחוק הפרשנות.[12]

(2) חובת שיתוף מידע בין משרדי הממשלה: על משרדי הממשלה לשתף ביניהם מידע על האזרחים לשם שיפור השירות לאזרחים, חיסכון בזמן ובמשאבים שלהם והפחתת הנטל הבירוקרטי המוטל עליהם במסגרת מדיניות "Tell us Once".[13] מדיניות זו נועדה להבטיח כי אזרחים ועסקים יידרשו לספק לרשויות הציבוריות פרטי מידע הנוגעים לענייניהם פעם אחת בלבד, ועל הרשויות הציבוריות חובה לשתף ביניהן את המידע.[14]

על פי ההחלטה, תיקוני החקיקה ומסגרת משפטית הדרושים ליישומה המלא ייקבעו בהמשך, בתוך חצי שנה עד שנתיים מיום קבלתה.[15]

12 סעיף 23ב לחוק הגנת הפרטיות:

23ב. (א) מסירת מידע מאת גוף ציבורי אסורה, זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על סמכות כדין, או שהאדם שהמידע מתייחס אליו נתן הסכמתו למסירה.

סעיף 3 לחוק הפרשנות, התשמ"א-1981:

"דין" – כל אחד מאלה:

(1) חיקוק;

(2) דינים דתיים – בין שבעל פה ובין שבכתב – כפי תקפם במדינה;

(3) (א) אקט של הפרלמנט הבריטי או דבר המלך במועצתו או חלק מהם, או תקנות לפיהם, ודיני המשפט המקובל ועקרוני היושר של אנגליה, כפי תקפם במדינה;

(ב) דינים עותמאניים כפי תקפם במדינה.

13 מדיניות "Tell us Once" או "Once Only" אומצה בהצלחה במדינות כגון דנמרק, הולנד, שוודיה ואנגליה. ראו המלצות הצוות הבין־משרדי לשיפור העברת מידע בין משרדים ויחידות סמך (היחידה לשיפור השירות הממשלתי לציבור, רשות התקצוב הממשלתי, משרד ראש הממשלה), מיום 28 ביולי 2016 (להלן: דוח הצוות הבין־משרדי), בעמ' 11-14.

14 חובה זו מבוססת על דוח הצוות הבין־משרדי, שם.

15 ס' 10 להחלטת ממשלה 1933 נוגע לתיקון תקנות הגנת הפרטיות באופן שיאפשר שיתוף מידע בין משרדי הממשלה במסגרת "פעם אחת בלבד"; ס' 9(ד) להחלטה קובע מסגרת של שנתיים לקביעת תכנית מפורטת ליישום של מדיניות "פעם אחת בלבד".

משמעות החובה לפרסום יזום של מאגרי המידע השלטוניים, כברירת מחדל, היא שלמידע אישי אין כל ערך; ואולם הממשלה הבהירה כי אין מדובר בחובה מוחלטת וכי חובה זו נסוגה בהתקיים מניעה ביטחונית או משפטית כגון הגנת הפרטיות.[16] לפיכך הטילה החלטת ממשלה 1933 על משרד המשפטים לנסח מדיניות המאזנת בין האינטרס הציבורי בפתיחת מאגרי המידע לבין החשש מפני פגיעה בפרטיות. בד בבד הוטל עליו להציג מדיניות הנוגעת להעברת מידע בין משרדי הממשלה. כל אחת משתי המשימות הללו מציבה אתגרים משלה ולפיכך גם מחייבת מערך איזונים משלה.

בהצעה לסדר זו נתמקד בחובת הפרסום היזום של מאגרי מידע ממשלתיים כברירת מחדל ובפגיעתה האפשרית בזכות לפרטיות. תחילה נתמקד בהבנת החשיבות של פרסום יזום ובתכליות שהוא משרת. לאחר מכן נסקור בקצרה את תפיסת הזכות לפרטיות בפסיקה ובחקיקה בישראל ואת הקושי ליישמה בהקשרים של נתוני עתק ומאגרי מידע ונעמוד על הפגיעה האפשרית של חובת הפרסום היזום בזכות לפרטיות במסגרת מאגרי מידע ממשלתיים למיניהם. בהמשך נבחן את המנגנונים המשמשים במדינות אחרות להגנה על הזכות לפרטיות, אגב מימוש היתרונות הטמונים בפרסום יזום של מאגרי מידע ממשלתיים. במסגרת זו נסקור גם את המנגנונים המיושמים בפועל לסיווג של מאגרי מידע ממשלתיים לכאלה שיש לפרסמם ולכאלה שאסור לפרסם. לאחר מכן נציג את המצב המשפטי בישראל מכוח חוק הגנת הפרטיות, התשמ"א-1981, וחוק חופש המידע, התשנ"ח-1998, ונתאר את המתווה המוצע בהחלטת ממשלה 1933 ובדוח הבין־משרדי ליישומה של חובת הפרסום היזום של מאגרי מידע ממשלתיים. לבסוף נציג את המלצותינו למימושה היעיל של החלטת ממשלה 1933 ולשיפור ההסדר המוצע בה.

ראו החלטת ממשלה 1933, **לעיל** ה"ש 10. יצוין כי מדובר בפרק זמן ארוך במונחים של פיתוח טכנולוגי. ראו גם תהילה שוורץ אלטשולר "חכו רגע עם המעבר מסטארט אפ ניישן לסטארט אפ גברמנט" **דה מרקר** 19.9.2016.

16 ס' 1(א) ו־12(ו) להחלטת ממשלה 1933, **לעיל** ה"ש 10.

ב. חשיבות הפרסום היזום של מאגרי מידע ממשלתיים ותכליותיו

לפרסום יזום של מידע ממשלתי שתי תכליות עיקריות: תכלית דמוקרטית ותכלית כלכלית. מדובר בשתי תכליות של עקרון השקיפות השלטונית, וכל אחת מהן מייצגת היגיון אחר בהגברת השקיפות של רשויות השלטון. התכלית הדמוקרטית משמעה שיפור, שימור וייעול ההליך הדמוקרטי על ידי הגברת השקיפות של פעולות הממשלה והאחריותיות שלה, שיפור השירות לציבור וחיזוק אמון הציבור בה.[17] התכלית הכלכלית נוגעת למימוש הפוטנציאל הגלום בפרסום יזום של מידע ממשלתי – למחקר ולפיתוח, להתייעלות כלכלית ולקידום חברתי.

אכן, העיקרון בדבר שקיפות הפעולות של רשויות השלטון אינו חזות הכול. מולו עומדים לעתים זכויות ואינטרסים אחרים, למשל: עקרון השוויון, שימור היעילות המינהלית או הגנה על ביטחון המדינה.[18] במחקר זה לא נדון באיזונים מסוג זה, שדנו בהם בעבר,[19] אלא נתמקד במיוחד במתח שבין מימוש עקרון השקיפות באמצעות פרסום יזום של מאגרי מידע ממשלתיים לבין ההגנה על הזכות לפרטיות.

1. התכלית הדמוקרטית

חוקי חופש המידע ברוב מדינות המערב מחייבים את המדינה בפרסום יזום של מידע שיש בכוחו להגביר את השקיפות והאחריותיות השלטונית. במילים אחרות: חוקי חופש המידע מתמקדים בהגברת השקיפות לשם מימוש התכלית הדמוקרטית. על פי רוב מדובר בפרטי מידע כגון תקציב, דוחות ביקורת, דוחות

17 Teresa Scassa, *Privacy and Open Government*, 6 Future Internet 397, 402, 407–408 (2014)

18 ראו למשל: שוורץ אלטשולר, **לעיל** ה"ש 9; Mark Fenster, *The Opacuty of Transparency*, 91 Lowa L. Rev. 885 (2005); Archon Fung, Mary Graham, & David Weil, Full Disclosure: The Perils and Promise of Transparency (2007)

19 ראו יונתן ארבל ותהילה שוורץ אלטשולר, **מידע רוצה להיות חופשי: על הטמעת חוק חופש המידע בישראל** (מחקר מדיניות 74, 2008).

ממשלתיים שנתיים, בעלי התפקידים בממשל ומשכורותיהם, הוצאות נסיעה ואירוח של בעלי תפקידים מסוימים וחוזי התקשרות של משרדי הממשלה. 94% מהמדינות החברות ב־OECD מחייבות פרסום יזום של מידע ממשלתי הנוגע לתקציב, 84% – פרסום יזום של דוחות ממשלתיים שנתיים, 72% – פרסום יזום של דוחות ביקורת, ו־28% מהן מחייבות פרסום יזום המפרט את בעלי התפקידים בממשל ואת משכורותיהם.[20]

חוק חופש המידע האמריקני (Freedom of Information Act; FOIA) מחייב את רשויות השלטון לפרסם ביוזמתן מאגרי מידע ממשלתיים הנוגעים לפעולות הממשל.[21] ביומו הראשון בחדר הסגלגל הצהיר הנשיא לשעבר ברק אובמה כי הממשל בראשותו יביא להגברת השקיפות של השלטון ועל ידי כך להדגשת החשיבות של השקיפות לחיזוק הדמוקרטיה ולעידוד ממשל יעיל ואפקטיבי.[22] בדומה, משרדי הממשלה בקנדה מחויבים לפרסם ביוזמתם, באתר האינטרנט שלהם, מידע לפי הקטגוריות המצוינות בחוק, למשל הוצאות נסיעה ואירוח של בעלי תפקידים מסוימים, חוזים עם משרדי ממשלה בסכום העולה על 10,000

20 OECD, Government at a Glance 142 (2011)

21 הקטגוריות הן: חוות דעת סופיות והוראות הניתנות בהחלטות משפטיות; הצהרות מדיניות שלא פורסמו במרשם הפדרלי והפרשנויות שאימצו עבורן משרדי הממשלה הרלוונטיים; הוראות ותדריכים מינהליים לאנשי הצוות במשרד הממשלתי שיש בהם כדי להשפיע על הציבור; העתקים של כל מסמך, ללא קשר לפורמט שלו, שניתן לאדם בהתאם לבקשתו ושעל פי אופיו עשוי להיהפך בסבירות גבוהה למושא של בקשות חשיפה נוספות; ואינדקס של כל המסמכים שפורסמו על פי בקשות מהציבור. נוסף על כך, בהמשך להנחיית הנשיא אובמה משנת 2009 וכחלק מהגברת השקיפות של הממשל, על הרשויות לזהות ולפרסם ביוזמתן גם מסמכים אחרים – שפרסומם אינו מחויב על פי החוק אך הם משמעותיים מבחינת העניין שהם מעוררים בציבור, מהווים דרך יעילה ליידע את הציבור בדבר פעולת הרשות וחיוניים להמשך המחויבות לממשל פתוח. ראו *Department of Justice Guide to the Freedom of Information Act*, The Department of Justice Guide to the Freedom of Information Act, pp. 18–19 (2009 edition)

22 Administration of Barack H. Obama,Memorandum on Transparency and Open Government (January 21, 2009), 74 FR 4665

דולר קנדי, מלגות ופרסים בסכומים העולים על 25 אלף דולר קנדי, דוחות פיננסיים וכל דוח שמכינה רשות ממשלתית למטרות ביקורת.[23]

גם תנועת הממשל הפתוח (Open Government Partnership) הבינלאומית חרתה על דגלה את קידום הפרסום היזום של מאגרי מידע ממשלתיים – בעיקר למימוש התכלית הדמוקרטית (הגברת השקיפות והאחריותיות של הממשלה, והשתתפות הציבור בעבודת הממשלה והשפעתו על קביעת מדיניותה), אך גם מתוך הכרה בערכו הכלכלי של המידע הממשלתי ובשימושיו האפשריים לפיתוח טכנולוגיות חדשות.[24]

ממשלות רבות ברחבי העולם הצטרפו לתנועת הממשל הפתוח. הן קבעו אסטרטגיות שהציבו את התכלית הדמוקרטית כמטרה העיקרית לפרסום היזום, בהנחה שפרסום מידע ממשלתי בפורמט שמיש יביא להגברת השקיפות ולחיזוק המעורבות של האזרחים בשלטון. בהתאם לכך, הסכסוכים המשפטיים על הנגשת המידע נסבו סביב המתח שבין זכות הציבור לדעת, טיוב מעשי השלטון והזכות לפרטיות. דוגמאות טיפוסיות לפרסום יזום של מידע ממשלתי לשם מימוש התכלית הדמוקרטית הן: פרסום נתוני שכר (ונתונים אחרים) של עובדי המגזר הציבורי ופירוט של שיחות טלפון ויומני פגישות של נציגי ציבור; האתר "מפתח התקציב", המנוהל על ידי עמותת הסדנא לידע ציבורי והמאפשר מעקב אחר כל סעיף בתקציב המדינה השנתי והשוואה לסעיפי התקציב בשנים הקודמות;[25] האתר "כנסת פתוחה", המנוהל גם הוא על ידי הסדנא לידע ציבורי והמציג נתונים שהוא שואב מאתר הכנסת על פעילות הכנסת וחברי הכנסת;[26] והאפליקציה Augumented Crime Scene הבריטית, המספקת למשתמש מידע על פשעים שהתרחשו בפרק זמן של חודש מאז מועד שאילתת המשתמש ובמרחק של מייל אחד ממקומו על פי חיישן ה־GPS במכשיר הטלפון הנייד שלו.[27]

23 Government of Canada, Proactive Disclosure (January 30, 2017)

24 ראו Open Government Guide, Custom Report, 7–8 (November 2014), באתר **opengovguide**; Scassa, **לעיל** ה"ש 17, בעמ' 397-398.

25 ראו האתר **מפתח התקציב**.

26 ראו האתר **כנסת פתוחה**.

27 ראו האתר **Augmented Crime Scene**.

2. התכלית הכלכלית

הממשלה מחזיקה במאגרי מידע אדירים שהיא אוספת במסגרת פעילותה השגרתית, החל בנתונים רפואיים ובהצהרות הון ומיסוי וכלה בנתונים על תחבורה ומיפוי. בפרסום היזום של מאגרי המידע הממשלתיים, בשילוב עם שימוש בטכנולוגיית מתקדמות לעיבוד ולכריית מידע, גלום פוטנציאל מרחיק לכת בתחומים כמו מחקר, פיתוח, התייעלות כלכלית וקידום חברתי.

במחקר "מדיניות ממשל פתוח בישראל בעולם הדיגיטלי"[28] עסקנו ביתרונות הכלכליים הישירים של מדיניות הממשל הפתוח: התייעלות של מנגנוני הבירוקרטיה, צמצום העלויות של חיפוש מידע והשגתו, שיפור השירות הממשלתי, הפחתת הנטל הרגולטורי וייתור הצורך במתווכים (למשל, בתחום הזכויות הרפואיות או תיווך נדל"ן). טענו כי מידע שלטוני הוא משאב ציבורי בעל ערך רב בשל יכולתו לעודד ולהזין יזמות גם בתחומים רחוקים מן המטרות שלשמן נוצר.

לפני כעשור החלו גורמים ברחבי העולם לבצע מחקרי הערכה בנוגע לשוק הכלכלי של שימוש ואחזור של נתונים שלטוניים. תחילה התמקדו מחקרים אלה בתחומים דוגמת מיפוי, איכות הסביבה, מטאורולוגיה ואקלים.[29] בשנת 2011 העריכה חברת הייעוץ הכלכלי גרטנר את שווי הפתיחה של שוק המידע הדני

28 שוורץ אלטשולר, **לעיל** ה"ש 9.

29 Ed Mayo & Tom Steinberg, Power of Information: Taskforce Report (2007); David Newbery, Lionel Bently, & Rufus Pollock, Models of Public Sector Information Provision via Trading Funds (2008); Tim Berners-Lee, Putting Government Data online — Design Issues (2009); Rufus Pollock, *The Economics of Public Sector Information*, *in* Cambridge Working Papers in Economics 0920 (Faculty of Economics, University of Cambridge, 2009); Paul Uhlir, The Socioeconomic Effects of Public Sector Information on Digital Networks: Toward a Better Understanding of Different Access and Reuse Policies: Workshop Summary (2009); Marco Fioretti, Open Data, Open Society: A Research project about Openness of Public Data in EU Local Administration (2010); Rufus Pollock, Welfare Gains from Opening up Public Sector Information in the UK (2010)

ב־80 מיליון אירו ואת השווי של שוק המידע השלטוני באיחוד האירופי כולו ב־27 מיליארד אירו.[30] במחקר מאותה שנה העריכה חברת הייעוץ העולמית מקינזי את שווי השוק של נכסי המידע הציבורי באיחוד האירופי, עבור הכלכלה האירופית, ב־250 מיליארד אירו, אם ייעשה בהם שימוש נכון לקידום יזמות וחדשנות.[31]

בחמש השנים האחרונות חלה בעניין זה התקדמות, הן הודות לפרטים וארגונים חברתיים שהפעילו לחץ על פתיחת מאגרים ואף הראו דוגמאות לשימושים שפיתחו באמצעות מאגרי מידע פתוחים,[32] והן בעקבות יוזמות מסחריות שעשו בכך שימוש. חברות ישראליות כמו MySupermarket ו־Pricez פיתחו פתרונות טכנולוגיים המסוגלים לאסוף את המידע על מחירים של מוצרי מזון ולהנגישו לצרכן; חברת WOBI משתמשת במאגר המסלקה הפנסיונית שהנגיש משרד האוצר; אפליקציית BreezoMeter מאפשרת לדעת מה רמת זיהום האוויר לפי מיקום ומשתמשת במאגרי המידע של המשרד לאיכות הסביבה; אתר madlan מאפשר לקבל מידע על מחירי דיור ומשתמש במאגרי מידע של מיסוי מקרקעין; אפליקציית Moovit, המבוססת על מיקום, מאפשרת למשתמשים לנווט את עצמם בתחבורה הציבורית בארץ אגב שימוש במאגרי המידע של משרד התחבורה; ואפליקציית telobike מסייעת לאתר אופניים בשירות תל־אופן בתל אביב.

לפי התחזיות הטכנולוגיות והניתוחים הכלכליים המקובלים, כל אלה הם אך תחילתו של תהליך. בשנת 2016 פרסמה חברת דלויט תוצאות מחקר שערכה במימון "גוגל ישראל" שלפיהן הפתיחה של מאגרי המידע הממשלתיים בישראל תגדיל את התמ"ג בישראל בכ־700 מיליון ש"ח בשנה, ושילוב יכולות ניתוח

30 Catherine Lippert, *Public Sector Information Reuse in Denmark*, European Public Sector Information Platform, Topic Report no. 20 (2009)

31 James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, & Angela Hung Byers, Big Data: The Next Frontier for Innovation, Competition and Productivity (2011)

32 רותי לוי "בעולם מתחוללת מהפיכת מידע וישראל עוד לא החליטה אם היא מעוניינת להצטרף" **דה מרקר** 21.9.2016.

של מאגרי המידע כבסיס לקבלת החלטות מבוססות נתונים יביא למשק כ־7 מיליארד ש"ח בשנת 2020.[33]

שימושים עתידיים במאגרי מידע שלטוניים עשויים לתרום, למשל, גם לתחום הרפואה. הפקת תובנות מניתוח מאגרים אלה יכולה לסייע בחיזוי התפרצות של מחלות ובהערכת יעילותן של תרופות. מאגר מידע על עשרות אלפי חולי סרטן יכול, למשל, לאפשר השוואה בין מטופלים שהמבנה הגנטי שלהם דומה, להימנע מטיפולים שאינם מתאימים לחולים בעלי נתונים מסוימים, לחזות טוב יותר אחוזי הצלחה של טיפולים, לחסוך בעלויות לטווח הארוך ולהציל חיים. דוגמאות נוספות: בתחום הבנקאות והביטוח יכול ניתוח נתונים שנכרו על בסיס המידע האישי לקבוע בְּדיוק יחסי את הסיכונים ואת האפשרויות לביטוח ולמתן אשראי, ובתחום הפעילות הממשלתית הדבר עשוי לסייע בקביעת גובה התמיכה של הביטוח הלאומי. זהו רק מספר מצומצם של דוגמאות לטווח רחב מאוד של הזדמנויות ושימושים.

שלוש מגמות מובילות את ההתקדמות הטכנולוגית ולכן גם מעצימות את הצורך להתמודד עם סוגיית הפתיחה של מאגרי המידע הממשלתיים:[34]

(א) **מגמת ההתייעלות של הפיתוח הטכנולוגי** בהיבטים של חומרה (למשל, מזעור גודל הטרנזיסטורים המבוססים על סיליקון), מהירות העברת הנתונים באינטרנט ויכולת האחסון של מידע מביאה לכך שכולנו משתמשים במחשבים שלפני עשור או שניים בלבד נחשבו בעינינו בעלי יכולות של מחשבי־על. התוצאה היא שכל ארגון מסחרי או שלטוני יכול להרשות לעצמו לאגום ולשמור כמויות עצומות של מידע.

(ב) **מהפכת הקישוריות**, שבעבר נתפסה כמהפכה הגדולה של האינטרנט בתור כלי תקשורת בין אנשים, נוגעת היום ליכולת של מכשירים לתקשר זה עם זה ומגלמת פוטנציאל לעולם שבו יוכלו מכשירים לייצר מידע רב ולהעביר אותו בכל עת, באמצעות חיישנים, למוח מרכזי. חברת Concrete Sensor

33 דלויט [Deloitte], "הערך הכלכלי של חדשנות מבוססת מידע (Data Driven Innovation)", (2016), בעמ' 15.

34 להרחבה בעניין זה ראו רועי צזנה **המדריך לעתיד** (2017); תהילה שוורץ אלטשולר **המכונה והמדינה** (המכון הישראלי לדמוקרטיה, בהכנה).

האמריקנית, למשל, פיתחה חיישנים המוטבעים בתוך יציקת בטון, אומדים את הטמפרטורה והלחות בעומק של עד 2.4 מטרים ומעבירים את הנתונים בתקופה של כשנתיים ממועד הטבעתם ביציקת הבטון למכשיר טלפון נייד על מנת לספק מידע על יציבות החומר.[35] בעתיד יונהג סטנדרט אחיד לכל החיישנים, וכך יוכלו החיישנים של מוצרים שונים "לשוחח" זה עם זה והמידע יועבר לפלטפורמה מרכזית ("המוח המרכזי"). פלטפורמה זו תאפשר את שמירתו ואת עיבודו של המידע בקנה מידה נרחב. פלטפורמת Microsoft IoT Central של חברת מיקרוסופט היא ניסיון ליצור בדיוק פלטפורמה מרכזית שכזאת.[36] מהפכה זו, שיש המכנים אותה "האינטרנט של הדברים", נוגעת להמוני נתונים: תכולת המקרר, כלי הרכב, רשת החשמל המסגירה את מנהגי השינה של בני הבית ומכשירי טלוויזיה חכמים המעבירים מידע מדויק על הרגלי הצפייה. ככל שנעשה קל יותר להעביר מידע, כך מוצמדים ליותר ויותר מכשירים חיישנים המסוגלים לקלוט מידע כזה כדי להעבירו הלאה – חיישנים של אור וצבע, לחץ (ברומטר), טמפרטורה ולחות, שדות מגנטיים, מד־תאוצה, חיישן גירוסקפי וחיישן אינפרא־אדום, היודע, למשל, לזהות משתמש שמקרב את אוזנו לטלפון. על אלה אפשר להוסיף גם את חיישן GPS, המצורף כיום לכל טלפון חכם ומאפשר לנו, וגם למוח המרכזי, לקבל מידע על מקומנו במרחב, בכל מקום על פני כדור הארץ.

(ג) **התפתחות הבינה המלאכותית** והלמידה העמוקה של מכונות נועדו להתמודד עם כמויות עצומות של מידע ולהפיק ממנו תובנות מופשטות, חדשות, ברמות תחכום גבוהות. לכן, ככל שהמכונות קולטות ומעבדות מידע רב יותר מכל התחומים, יכולותיהן משתפרות ואפשר להרחיב את תחומי ההטמעה שלהן. שנת 2016 תיזכר כשנה של פריצת דרך בלמידה על ידי מכונה ושל כניסת מודלים של למידה עצמית. שיפור דרמטי נרשם, למשל, ביכולות התרגום (הכלי הפופולרי ביותר המשתמש בלמידה עמוקה בתחום

35 Matt Burgess, *What is the Internet of Things WIRED? Explains*, WIRED (April 21, 2017); וכן האתר **Concrete Sensors**.

36 Burgess, **שם**; Richard Hay, *Microsoft Launches IoT Central to Simplify Internet of Things Management*, Data Centeral Knowledge (April 21, 2017)

של עיבוד שפה הוא מנוע התרגום של גוגל, "גוגל טרנסלייט"), בקריאת שפתיים, בהבנה קולית, ביכולות ניתוח והבנה של ראייה ממוחשבת, בפענוח ראייה ובחיפוש בתוכני וידאו, בשכלול של מערכות ההמלצות המספקות לאנשים המלצות על פרטים שעשויים לעניין אותם ושל היכולת הממוחשבת להבין הקשרים של שפה ושיחה אנושיות ולקיים שיחה קוהרנטית. בעולם של בינה מלאכותית ולמידת מכונה עולה יכולתן של המכונות ללמוד ככל שיש יותר מידע (ביג דאטא). מי שיש לו גישה למאגר מידע בנפח גדול ובאיכות גבוהה נהנה מיתרון, משום שריבוי המידע מאפשר למכונות הלומדות ליצור מודלים טובים יותר וחוויית משתמש טובה יותר, ואלה מביאים בתורם לריבוי משתמשים ולכן גם לריבוי תובנות ופיתוחים נוספים. משום כך, מאגרי מידע ממשלתיים שיכולים, עם פרסומם היזום, להביא להגדלת נפח הנתונים הזמינים לעיבוד, הם בעלי ערך רב יותר מבעבר.

צירוף של שלוש המגמות שתוארו משמעו יכולות חסרות תקדים. נדגים: היכולת של חיישנים לנטר את המציאות, הקישוריות המאפשרת לשלוח את המידע למוח מרכזי והאלגוריתמים החכמים המעבדים את המידע הרב – כל אלה יחד מאפשרים להציע שירותי ניטור (למשל – של לחץ הצמיגים במכונית או של פליטת מזהמים מעל מפעל), שירותי חיזוי (ניתוח של דפוסי הצעידה של קשישים מאפשר להתריע מפני נפילות והתקפי לב טרם התרחשותם; ניתוח של נתונים אחרים מאפשר לגלות מתי מדיח כלים, מקרר, מחשב, גשר או סכר עומדים להתקלקל או מתי כעס מתגנב לקולה של המורה בבית הספר בטרם תתפרץ); ושירותי מכירות (למשל, היכולת לעקוב אחר מבטם של קונים בחנויות ולזהות את המוצרים שהם בוחנים אבל לא רוכשים, לנטר את הדפים שהם מדלגים עליהם במגזין או להתאים פרסומות בשלטי רחוב למי שעובר לידם).

בתחום המוצרים הוביל השילוב של שלוש המגמות – התייעלות ומזעור, קישוריות ובינה מלאכותית – למהפכה האדירה שהתרחשה עם חדירת הטלפונים הניידים החכמים לשוק. שילוב דומה של מגמות אלה מתרחש כיום בתחום האווירונאוטיקה, ותוצריו הם הרחפנים וכלי הטיס הבלתי־מאוישים לשימושים אישיים, מסחריים, מדינתיים ומלחמתיים. ממש כמו הטלפונים החכמים, גם הרחפנים יעניקו מגוון עצום של שירותים (למן העברת חבילות ועד לניטור מסוגים שונים, מניעת פשיעה והשגת ראיות בתחום אכיפת החוק

והשמירה על הסדר הציבורי) ובה בעת יעוררו סוגיות חשובות של אחריות והגנה על זכויות אדם. דוגמה נוספת לשילוב כזה היא בתחום המכשירים האלקטרוניים הממוזערים והגמישים, המאפשר פיתוח מואץ של צמידים או קעקועים אלקטרוניים שמודבקים על עור הגוף ומפעילים חיישנים המנטרים מדדים רפואיים.

בצד היתרונות הכלכליים והחברתיים שיש בפרסום יזום של מאגרי מידע ממשלתיים עולה החשש מפני פגיעה אפשרית בזכות לפרטיות בעקבות פרסום מידע אישי שהרשויות אספו על כל אחת ואחד מהאזרחים בלי לבקש מראש את הסכמתם. נעסוק בכך בפרק הבא, אך כאן נעיר כי במרבית מדינות המערב אין עדיין מדיניות בהירה באשר לאיזון בין פתיחת מאגרים לתכלית כלכלית לבין הזכות לפרטיות, ועיקר השיח עוסק בפתיחת מאגרים כדי לממש את התכלית הדמוקרטית. עם זאת, מדינות אחדות כבר נתנו את הדעת גם לתכלית הכלכלית שממלא הפרסום היזום כאמור ובהן דנמרק, אוסטרליה, ספרד ובריטניה.[37] בפרק הבא נעמוד על משמעותה של הזכות לפרטיות ועל חשיבותה, ונסקור את הסכנות הצפויות לה לנוכח פרסום יזום של מאגרי מידע ממשלתיים.

37 Noor Huijboom & Tijs Van den Broek, *Open Data: An International Comparison of Strategies*, European Journal of ePractice (2011). בבריטניה הגדירה תכנית הממשל הפתוח את שתי התכליות כמטרה: הגברת השקיפות, ובהמשך לכך חיזוק האזרחים, והכרה בתכלית הכלכלית שבשימוש במידע הממשלתי בדרכים חדשניות כדי להביא תועלות כלכליות לאזרחים ולעסקים. התכלית הדמוקרטית והתכלית הכלכלית עומדות גם בבסיס המחויבות לממשל פתוח שקיבלו עליהן המדינות החברות בארגון המדינות המתועשות (G8). ראו G8 Open Data Charter and Technical Annex (June 18, 2013).

ג. הבעיה: פרסום יזום של מאגרי מידע ממשלתיים כברירת מחדל והפגיעה הצפויה בזכות לפרטיות

1. הזכות לפרטיות בעולם דיגיטלי: רקע

הזכות לפרטיות מעוגנת בדין הישראלי בחוק־יסוד: כבוד האדם וחירותו ובחוק הגנת הפרטיות. ואולם על אף עיגונה החוקתי של הזכות לפרטיות וחרף ההכרה בה בפסיקה, אין בנמצא הגדרה מדויקת, ברורה ואחידה של מהותה. היקפה של הזכות עמום: קל לזהות פגיעה בה ולהציג דוגמאות לפגיעות, אך קשה לנסח לה הגדרה קוהרנטית ומופשטת.[38]

יש המגדירים את הזכות לפרטיות ברוח הביטוי שטבעו וורן וברנדייס בסוף המאה ה־19 – הזכות "להיעזב במנוחה",[39] כלומר זכותו של אדם לנהל את חייו בדל"ת אמותיו, במרחב פרטי (לאו דווקא פיזי), כרצונו ובלא הפרעות מבחוץ.[40] תפיסה אחרת מגדירה את הזכות לפרטיות לפי הקטגוריות המוגנות באמצעותה. מקובל, למשל, להכיר בזכות לפרטיות במקומות שבבעלותו או בשליטתו של אדם ובמידע שקשור בו או בהחלטות שקיבל. הגדרות מסוימות מבחינות בין תוכן התקשורת, המוגדר כפרטי, לבין נתוני התקשורת (זהות המשוחחים, משך השיחה או שעת השיחה), שאינם זכאים להגנת הפרטיות.

על פי רות גביזון, הזכות לפרטיות מבוססת על הגבלת הגישה (access) של אחרים לאדם פלוני בשלושה ממדים: הגבלת הגישה הפיזית אליו, הגבלת הגישה למידע על אודותיו (סודיות) והגבלה של תשומת הלב אליו (כלומר, אנונימיות). הלן ניסנבאום מגדירה את הזכות לפרטיות כנגזרת מהציפייה לפרטיות, כאשר היא – הפרטיות – תלוית הקשר (contextual integrity). על פי גישה זו, הזכות לפרטיות נקבעת בכל מקרה בהתאם לציפייה הסבירה לפרטיות בנסיבות

38 הלל סומר, אלעד שרף ותמר שוויצר "מסמך רקע בנושא: הזכות החוקתית לפרטיות" (מוגש לוועדת החוקה, חוק ומשפט של הכנסת, נובמבר 2004); מיכאל בירנהק **[מרחב פרטי] הזכות לפרטיות בין משפט וטכנולוגיה** (2010).

39 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harvard L. Rev. 193 (1890)

40 סומר, שרף ושוויצר, **לעיל** ה"ש 38; בירנהק, **לעיל** ה"ש 38.

המסוימות. הגדרה אחרת של הזכות לפרטיות ממקדת אותה דווקא בעצם השליטה של אדם במידע עליו. לשון אחר: הפרט הוא היחיד שזכאי לקבוע מה יעלה בגורל המידע עליו. כדברי נשיא בית המשפט העליון לשעבר, אהרן ברק, כל אדם מוקף במעטפת שמחזיקה, בין היתר, גם את כל המידע עליו. מעטפת זו מהווה מרחב שבתוכו האדם זכאי להיות עם עצמו בלבד, והיא נעה אתו באשר ילך בהיותו יחידה אוטונומית עצמאית.[41]

כפי שכתבנו, המציאות הטכנולוגית הנוכחית מאופיינת גם ביכולות לכרות, לשמור ולאחסן מידע וגם ביכולות לעבדו ולהפיק ממנו תובנות חדשות. זהו עידן נתוני העתק. הטכנולוגיות הקיימות מאפשרות לאסוף כמויות עצומות של מידע אישי – באמצעות האינטרנט, החיישנים בטלפון הנייד, מצלמות רחוב, חיישנים בכניסות לבניינים ולמגרשי חניה וכמובן מכשירים "מקושרים" נוספים ("האינטרנט של הדברים"). חברות מסחריות המשמשות סוחרות ומתווכות של מידע (data brokers) אוספות כמויות אדירות של מידע אישי על מיליוני צרכנים כדי למכור או לתעל אותו לחברות אחרות. ואכן, חברות כמו גוגל ופייסבוק, אפליקציות כמו ווייז או פוקימון גו, אתרי סחר אלקטרוני כמו אמזון ומועדוני צרכנות של רשתות קמעוניות כמו שופרסל אוספים כמויות חסרות תקדים של מידע על אנשים. חברת Acxiom, למשל, פרסמה שיש בחזקתה פרופילים של יותר מחצי מיליארד אנשים מכל העולם; חברת גוגל מעבדת יותר מ־24 פטבייט (petabytes) של מידע אישי ביום – כמות השקולה למכפלת המידע המודפס הקיים בספריית הקונגרס האמריקני בכמה אלפים.[42]

באמצעות טכנולוגיות מתקדמות לכרייה ולניתוח של מידע ובעזרת בינה מלאכותית מעובד המידע שנאסף ביעילות וברמת דיוק וידע בהיקפים בלתי נתפסים. מכלול הפעולות שאנו מבצעים בחיי היום־יום – האתרים שגלשנו בהם באינטרנט, החנויות שבהן ערכנו קניות, המוצרים שקנינו, המקומות שאליהם נסענו, כיצד נהגנו, מה קראנו, מה אכלנו, מה בבעלותנו, עם מי שוחחנו, מי חברינו ומי קרובי המשפחה שלנו, מה מצב בריאותנו, כמה ספורט עשינו, מה

41 בירנהק, **לעיל** ה"ש 38; בג"ץ 6650/04 **פלונית נ' בית הדין האזורי בנתניה**, פ"ד סא(1) 581 (2004), פס' 21 לפסק דינו של הנשיא ברק.

42 ראו *Big Data and the Future of Privacy* באתר **epic**.

כתבנו ובמה צפינו – כל המידע הזה נאסף, מאורגן ביעילות, מנותח על ידי תוכנות מחשב מתוחכמות ומשמש (או נמכר) למטרות כמו הצלבה עם מידע נוסף להפקת תובנות חדשות, שיווק, שכנוע, מחקר ופיתוח. המידע לא נשכח ולא נמחק. הוא שם כל הזמן, ולתמיד.

העולם הדיגיטלי מאתגר את הזכות הבסיסית לפרטיות. האתגר מתגלה בעיקר בהקשר של הציפייה לפרטיות (החל במצלמות ברשות הרבים, עבור בטלפון הנייד הפרטי המשמש לעבודה, וכלה בגלישה באינטרנט ברשת הביתית) ובהקשר של יכולת ההצלבה והניתוח של מאגרי מידע, שמגדילה את הכמות וההיקף של סוגי המידע שאפשר להפיק (נתוני תקשורת או היסטוריית חיפוש, למשל).

יתרה מזו, השיטות המסורתיות להגנה על הזכות לפרטיות – המבוססות ברובן על קבלת הסכמה מדעת לפגיעה בפרטיות – לא בהכרח ישימות עוד. המידע הפך למשאב שנעשים בו שימושים רבים, והוא ממוחזר בדרכים ולמטרות שמרביתן אינן צפויות ואינן ניתנות לסיווג מוקדם לקטגוריות שאפשר לקבל עבורן הסכמה מדעת. גם הַתְמָמה (אנונימיזציה; de-identification), שמשמעה הפשטת המידע מרכיבים מזהים מובהקים, לא תמיד מספקת נמל מבטחים לנוכח הסיכון שהצלבת נתונים, גם אם הם אנונימיים, תוביל למידע מזהה.[43]

מחקרים מלמדים על תופעה בשם "פרדוקס הפרטיות", שפירושה חוסר יכולת של הציבור להתמודד עם התפתחויות טכנולוגיות מהירות ועם המשמעויות שלהן. כך, למשל, ניכר חוסר התאמה בין תפיסת הפרטיות כפי שהיא באה לידי ביטוי בהצהרות של משתמשים בשירותים מסוימים לבין מודעותם והתנהגויותיהם בפועל. משתמשים מצהירים כי לא ירצו לאפשר סרטוט של הפרופיל האישי שלהם (profiling) מחשש שתיפגע פרטיותם, אבל בפועל הם בקושי משתמשים בטכנולוגיות שמגִנות על פרטיותם, כמו הדפדפן תור (Tor) המאפשר תקשורת תחת מעטה של אנונימיות. משתמשים נכונים לוותר על פרטיותם כדי ליהנות משירותים מסוימים, לפעול ברשתות חברתיות, להירשם לכרטיסי מועדון ברשתות קמעוניות או להשתמש בשירותים

43 להלן נרחיב על הליך זה, המכונה "זיהוי חוזר"; ראו סעיף ד.2.ב **להלן**.

המבוססים על זיהוי מיקומם הגאוגרפי.[44] פרדוקס הפרטיות מקשה על ההערכה של שווי המידע האישי בעיני המשתמשים עצמם, והדבר מוביל לקושי של קובעי המדיניות למצוא את האיזון הנכון בין הזכות לפרטיות לבין היעילות הכלכלית שבגילוי מידע אישי ולהתרת השימוש בו, ואף להצביע על היקף ההגנה הראוי על הפרטיות.[45]

כדי להפוך את המצב למסובך אף יותר יש לזכור כי בעולם של אינטרנט – כלומר, עולם של טכנולוגיה גלובלית שלא שורר בה משטר משפטי אחיד – המידע האישי נאסף, נשמר ומעובד במשטרים משפטיים שונים זה מזה שלכל אחד מהם תפיסת פרטיות אחרת. במצב זה המימוש של הזכות לפרטיות נעשה מאתגר, וההגדרות התאורטיות של הזכות נתקלות בקשיים לא רק בשל אי־התאמה למציאות הטכנולוגית אלא גם בגלל אי־התאמה לסמכות השיפוט הגאוגרפית.[46]

2. פרטיות ופרסום יזום של מאגרי מידע שלטוניים

חלק ממאגרי המידע השלטוניים אינם כוללים כל מידע אישי, ולכן אין חשש שפרסום יזום שלהם יביא לפגיעה בזכות לפרטיות. כאלה הם, למשל, מאגרים של מידע תקציבי, מידע סטטיסטי "טהור" (למשל, מספר האזרחים במדינה המורשים לנהוג לפי מין, גיל וסוג כלי הרכב), מידע גאוגרפי (למשל, חלוקת המקרקעין במדינה לגושים לשם רישום מקרקעין) או זמני הגעה בפועל של אמצעי תחבורה ציבוריים.[47] לעומת מאגרים אלה, לפרסום יזום של מאגרים

44 Laura Brandimarte & Alessandro Acquisti, *The Economics of Privacy*, *in* The Handbook of the Digital Economy 563–564 (M. Peitz & J. Waldfogel, eds., 2012); Sören Preibusch*, Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments*, 71 Int. J Human Computer Studies 1133, 1134 (2013)

45 Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, & Rodrigo de Oliveira, *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online*, *in* Proceedings of The 22nd International Conference on World Wide Web 189 (2013)

46 The President's Council of Advisors on Science and Technology (PCAST), Big Data and Privacy: A Technological Perspective (May 1, 2014)

47 דוח הצוות הבין־משרדי, **לעיל** ה"ש 13, בעמ' 13–14.

ממשלתיים הכוללים מידע אישי, או מידע שהצלבתו עם מידע אחר עלולה להוביל לזיהוי חוזר, ייתכנו השלכות מרחיקות־לכת על הזכות לפרטיות. להלן נעמוד על כמה מהן.

(א) **אובדן השליטה במידע.** השיפור ביכולת לעבד מידע פרטי בהיקף נרחב, לנתחו, להגיע למסקנות המבוססות עליו ולהפיץ מידית הן את המידע והן את המסקנות – והעובדה שכל ערמות המידע הללו נשמרות וניתנות להעברה באינטרנט לעד ובלי קשר למטרה המקורית שלשמה ניתנו – מפחיתות במידה ניכרת את מידת השליטה של כל אחד במידע הנוגע אליו. הפחתה זו פוגעת בזכותו לפרטיות.[48] פרסום יזום של מידע אישי כזה, שנצבר במאגר מידע ממשלתי, יגדיל את היקף המידע הפומבי על האזרחים ויפחית את מידת שליטתם בו.

(ב) **"זליגת" השימוש במידע ופגיעה ביכולת להבטיח שימוש במידע למטרות שהוסכם עליהן.** מרגע פרסום המידע באינטרנט הממשלה כבר לא יכולה להבטיח את הגנת הפרטיות במידע כנדרש בחוק הגנת הפרטיות, משום שאי־אפשר להבטיח שהשימוש במידע ייעשה אך ורק למטרות שלגביהן נתן האדם את הסכמתו.[49] החשש העיקרי הוא מפני "זליגה" של מידע ממשלתי שפורסם באופן יזום לשימושים שלא נועדו לו מלכתחילה.

(ג) **פרדוקס הפרטיות והצורך להפוך אותה לנכס סחיר.** ממשלות, חברות טכנולוגיה ומוסדות פיננסיים מחזיקים בכמות עצומה של מידע אישי, והם מתרגמים אותו ליתרון תחרותי או לרווח כלכלי. הבעיה היא שמערכת היחסים בין המחזיקים במידע ובין האנשים שהמידע נוגע להם איננה שוויונית. רוב הציבור לא מודע לאפשרות שהוא יכול לסחור במידע הפרטי שלו או לדרוש כי יוצמד "תג מחיר" לכל פריט מידע אישי לפי תנאי השוק.

48 Scassa, **לעיל** ה"ש 17, בעמ' 407; יעקב הכט "הפרטיות ברשת כמושג אמורפי" אתר **איגוד האינטרנט הישראלי** 23.8.2014.

49 Maeve McDonagh, *E-Government in Australia: The Challenge to Privacy of Personal Information*, 10 (3) International Journal of Law and Information Technology 327, 330–331 (2002); הכט, **לעיל** ה"ש 48.

פתיחה יזומה של מאגרי המידע עלולה להקשות עוד יותר על הפיכת הזכות לפרטיות לנכס סחיר בידי נושא המידע ועל התמודדות עם פרדוקס זה.[50]

(ד) **שימוש לרעה במידע.** שימוש לרעה במידע המתפרסם כחלק ממאגרי מידע ממשלתיים יכול ללבוש צורות מגוונות – החל בגנבת זהות וכלה במציצנות וירטואלית ושימוש במידע למטרות פליליות.[51]

(ה) **פגיעה בלתי הפיכה.** מהרגע שמאגר מידע ממשלתי יפורסם באינטרנט, לא יהיה אפשר להחזיר את הגלגל לאחור. המידע האישי יהיה שם לעד.[52]

כאמור לעיל, הגנה על פרטיות במסגרת פרסום יזום של מאגרי מידע ממשלתיים היא אחת מני סוגיות רבות הקשורות בהגנה על פרטיות בעולם דיגיטלי. עם זאת, יש לה כמה מאפיינים העושים את הדיון בה לייחודי, ולכן יש להתחשב בהם בעת קביעת המנגנון המתאים לפרסום יזום של מאגרי מידע ממשלתיים:[53]

(א) המידע שברשות המדינה אינו מידע פרטי שאנשים מסרו מרצונם החופשי, בתמורה לכסף או לטובת הנאה או ללא תמורה. מדובר במידע שאזרחי המדינה חויבו בחוק למסור לרשויות השלטון כדי שהן יוכלו לבצע ביעילות את תפקידן. מנקודת המבט של המשפט החוקתי, המדינה חייבת, מלכתחילה, להימנע מפגיעה בזכות לפרטיות של אזרחיה אלא אם הפגיעה עומדת בדרישות שבפסקת ההגבלה שבחוק יסוד: כבוד האדם וחירותו. מעבר לכך, העובדה שהשליטה במאגרי המידע היא חלק מהפעילות השלטונית מחייבת עמידה בכללי המשפט המינהלי.[54]

50 Jaron Lanier, Who Owns the Future? (2013); **הכט, לעיל ה"ש 48.**

51 Sol Bermann, *Privacy and Access to Public Records in the Digital Age*, 40 Center for Interdisciplinary Law and Policy Studies Working Paper Series 4, 6 (April 2006)

52 **דוח הצוות הבין־משרדי, לעיל ה"ש 13, בעמ' 30.**

53 Kenin Iwersen, *Conflicting Identities — The Digital Government Dilemma*, SANS Institute InfoSec Reading Room (April 26, 2004); Scassa, **לעיל ה"ש 17, בעמ' 397-398, 400-401; בג"ץ 8070/98 האגודה לזכויות האזרח נ' משרד הפנים, פ"ד נח(4) 842 (2004).**

54 Scassa, **לעיל ה"ש 17, בעמ' 402; בג"ץ 8070/98 האגודה לזכויות האזרח נ' משרד הפנים, שם.**

(ב) עיקר השימושים שייעשו במידע שבמאגרים הם "כלכליים", כלומר שימושים בשוק הפרטי או בעולם המחקר היישומי ולא שימושים "דמוקרטיים", שמשמעם הגברת השקיפות השלטונית לצורכי פיקוח על השלטון. באיזון שבין הפגיעה בפרטיות לבין אינטרסים אחרים עשויה להיות חשיבות לתכלית שלשמה מתבצעת ההנגשה היזומה של מאגרי המידע.

(ג) על פי רוב, המידע שבמאגרים הוא פרטי, כך שהפגיעה הראשונה בפרטיות היא עצם פרסומו; עם זאת ייתכן ששימושים אחרים במידע זה – עיבודו, הצלבתו עם מאגרים אחרים וכיוצ"ב – יפיקו מידע חדש ונוסף, וזה יהיה בעצמו פגיעה נוספת, שנייה, בפרטיות של האזרחים.

(ד) ההחלטה שראוי להנגיש את מאגרי המידע הממשלתיים נסמכת על שתיים – על ההערכה שהפגיעה בפרטיות הכרוכה בהנגשה היא פגיעה קלה או כזאת שאפשר להתמודד אתה באמצעות התממה (אנונימיזציה), ועל הטכנולוגיה המוכרת כיום. פיתוחים טכנולוגיים עתידיים ייתכן שיערערו, ואפילו יפריכו, את ההנחות הללו.

ד. פרסום יזום ומזעור הפגיעה בפרטיות: סקירת הפתרונות המוצעים בספרות ובמשפט המשווה

הספרות והפרקטיקה הלכה למעשה במדינות מסוימות מציעות פתרונות מדיניות להגנה על הפרטיות בעת פרסום יזום של מאגרי מידע ממשלתיים. ההבחנה המשותפת בכל הפתרונות היא ההבחנה בין מקרים שאין בהם פגיעה בפרטיות – בין משום שנקבע כי פרטי המידע המופיעים במאגרים אינם פוגעים בפרטיות ובין משום שננקטו במאגרים טכניקות של התממה (אנונימיזציה) – לבין מקרים שיש בהם פגיעה בפרטיות אבל אין שום אפשרות לנטרל אותה. על המקרים מהסוג השני יש להחיל איזונים – בין ההגנה על הפרטיות לבין אינטרסים ציבוריים אחרים – ולהחליט מראש אם הפגיעה במסגרתם בפרטיות מוצדקת.

1. סיווג של מאגרי מידע והגדרה מראש של מאגרים מותרים לפרסום יזום

מאגרי המידע המתאימים לפרסום יזום בלא חשש לפגיעה בפרטיות הם אלו שאין בהם כל מידע אישי. הקושי מתעורר במקרים שבהם אין במאגר מסוים מידע אישי, אבל שילוב של נתונים שכן כלולים בו עם נתונים חיצוניים – ממשלתיים או לא ממשלתיים – יכול ליצור מידע מזהה.

בדוח הצוות הבין־משרדי צוינה רשימה של מאגרים שלכאורה אין בפרסומם פגיעה בפרטיות, אולם לא צוינו בו סטנדרטים או קריטריונים שיאפשרו קביעה באשר למאגרים עתידיים – אם מתעוררת בעניינם סוגיית פרטיות. כמו כן לא נקבעו בדוח הקריטריונים שיאפשרו לזהות מתי שילוב של מאגר מידע ללא מידע אישי עם מידע אחר עלול להוביל לפגיעה בפרטיות.

מתוך מאגרי המידע של משרד החינוך המליץ הצוות להנגיש את המאגר העוסק בתקציב החינוך ולציין בו את תקציב המשרד עבור בית ספר מסוים אך בלי להנגיש את תקציב הרשות המקומית ותקציבים מסוימים אחרים (למשל, תשלומי הורים). מתוך המידע של משרד התחבורה המליץ הצוות להנגיש את מאגר המידע של זמני האמת של רכבת ישראל, כולל מקום הרכבות בזמן אמת וחיזוי הגעתן לתחנות, ואת מאגר ההמראות והנחיתות בזמן אמת, כולל שם חברת התעופה, מספר הטיסה, יעד ההמראה, זמני הנחיתה הצפויים והמעודכנים וסטטוס הטיסה (נחתה או מתעכבת). מתוך מאגרי המידע של משרד התרבות המליץ הצוות להנגיש את מאגר מתקני הספורט תוך ציון סוג המתקן ושמו, הגוף המפעיל אותו ומיקומו (כתובת מלאה). מתוך מאגרי המידע של משרד הפנים המליץ הצוות להנגיש את מאגר התקציב של הרשויות המקומיות, תוך פירוט נתונים על הרשות (מספר התושבים, מספר משקי הבית, דירוג חברתי־כלכלי של הרשות) ותמצית נתוני התקציב (הכנסות, הוצאות, ביצוע, תקבולים ותשלומים).[55]

על פני הדברים נראה כי אין במאגרים אלה כל חשש לפגיעה בפרטיות, ובכל זאת באלה לא נסתיימו המלצות הצוות הבין־משרדי. הצוות המליץ

55 דוח הצוות הבין־משרדי, **לעיל** ה"ש 13, בעמ' 42–44.

להנגיש גם את מאגר תאונות הדרכים של הלשכה המרכזית לסטטיסטיקה, תוך הנגשת מידע סטטיסטי בלבד על מקומות שאירעו בהם לפחות שלוש תאונות, תוך ציון שם הרחוב שבו אירעה התאונה (ללא קטע ספציפי ברחוב), חומרת התאונה, מספר הנפגעים וחומרת הפגיעות, וכן זמן התאונה במהלך היממה (ללא ציון תאריך או שעה מדויקים). כאן המקרה מורכב קצת יותר: אם, למשל, מדובר ברחוב קטן, המידע שהונגש על יותר משלוש תאונות דרכים באותו הרחוב יכול – בשילוב עם נתונים אחרים – להוביל לזיהוי המעורבים בתאונה על ידי תושבי השכונה האחרים, ואלה עלולים "לקחת את החוק בידיים" ולפעול בעצמם כנגד מי שהם חושדים בו שהוא עבריין תנועה סדרתי הפוגע באחרים כל אימת שהוא יוצא מן החניה.

עוד המליץ הצוות הבין־משרדי להנגיש – מתוך מאגרי המידע של המשרד לביטחון הפנים – את מאגר הפשיעה של משטרת ישראל, תוך פירוט נתונים סטטיסטיים בלבד: סוג הפשיעה (עברות בין בני זוג, עברות אלימות, עברות מחשב, עברות רכוש וכו'), פשיעת זרים, פשיעה של בני נוער, מעצרים ותאונות דרכים על פי חלוקה למחוזות המשטרה. גם כאן השאלה המתעוררת היא אם אפשר להניח אפריורית ששילוב של נתונים אלה – שאין בהם כל מידע אישי – עם נתונים נגישים אחרים יכול להוביל לזיהוי.

לדעתנו, סיווג המאגרים המתאימים לפרסום יזום ללא חשש מפגיעה בפרטיות צריך להסתמך על שני קריטריונים:

(א) **סוג הנתונים הנכלל במאגר המידע.** יש קטגוריות בסיסיות אחדות של מאגרי מידע שאין בהם חשש לפגיעה בפרטיות, ובראשם מאגרי מידע שיש בהם רק נתוני תקציב והתקשרויות; זמני הגעה של כלי תחבורה ציבורית ביבשה, באוויר או בים; נתונים גאו־ספאטיאליים (איתור וניטור תנועה של אובייקטים); ונתונים חברתיים־דמוגרפיים (מספר תושבים בעיר, ממוצע ציוני הבגרות בחתך בית־ספרי או יישובי). לעומת זאת, מאגרי מידע הכוללים נתונים סטטיסטיים (פשיעה, תאונות דרכים, מאגרים רפואיים וכיוצא באלה) אינם יכולים להיחשב אפריורית כמאגרים שאין בהם בעיית פגיעה בפרטיות.

(ב) **מבחן "הפורץ המעוניין".** בהמשך הפרק נעסוק בסוגיית הזיהוי החוזר לאחר התממה. כאן נציין שיש חשיבות גדולה לקביעת סטנדרטים להבחנה

ראשונית בין מאגרים בעייתיים למאגרים שאינם בעייתיים. לפיכך יש לשקול שימוש במבחן "הפורץ המעוניין" (motivated intruder) שפרסם בשנת 2012 נציב הפרטיות הבריטי בהקשר של זיהוי חוזר. לפי מבחן זה יש לשאול אם אדם בעל יכולות רגילות – שיש לו גישה למידע המתפרסם באינטרנט, במאגרי מידע ציבוריים או בספריות (או שצפויה להיות לו גישה כזו), כמו גם מוטיבציה לזהות אדם מסוים על בסיס המידע המפורסם במאגר – יצליח לעשות זאת.[56] כאשר התשובה למבחן "הפורץ המתעניין" שלילית, החשש לפגיעה בפרטיות עקב פרסומו היזום של מאגר המידע הממשלתי חלש.

מאגרים הכוללים מידע אחר מקטגוריות המידע שאינו מעורר חשש לפגיעה בפרטיות או מאגרים שהמענה בהם למבחן "הפורץ המתעניין" חיובי ייבחנו לפי המפורט בַּתת־פרק שלהלן.

2. פרסום יזום מתוך מזעור הסיכונים לפגיעה בפרטיות[57]

לאחר המיפוי הראשוני של מאגרי המידע הממשלתיים המתאימים לפרסום יזום, בלא חשש מפגיעה בפרטיות,[58] יש לפנות למאגרים שיש בהם מידע מזהה.

56 *Anonymisation: Managing Data Protection Risk Code of Practice*, Information Commissioner's Office (November 2012) 15–16, 19–23

57 באיחוד האירופי בחרו לדרוש יישום בו־זמני של טכניקות התממה אחדות כדי להקטין את הסיכון לפגיעה בפרטיות עקב פרסום יזום. רובינסטיין והרצוג (להלן) מבקרים עמדה זו בטענה שהתממה מוחלטת היא בלתי אפשרית, ולכן רגולציה יעילה אינה צריכה להתמקד במניעה מוחלטת של נזק לזכות לפרטיות. לטענתם, מאחר שהתממה מוחלטת היא מיתוס, עדיף להתמקד בתהליך, כלומר בדרישה לנקוט את כל האמצעים הסבירים למזעור הסיכונים לפגיעה בפרטיות. הואיל ולדעתנו התממה מוחלטת אינה אפשרית בעידן נתוני העתק, בעקבות ההתפתחויות בטכנולוגיות לכריית מידע, גם אנו בוחרות להדגיש את מזעור הסיכונים לפגיעה בפרטיות. ראו Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques,* 0829/14/EN WP216 (10.4.2014); Ira S. Robinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 713–714 (2016)

58 בהקשר זה נעיר כי יש חשיבות גם למטא־דאטא של המאגרים. אשר לעצם הסיווג – מה ייחשב מאגר הכולל מידע מזהה: בארצות הברית נקבע כי יש ליצור רשימת מצאי

עצם העובדה שמאגר מידע כולל מידע מזהה אינה מחייבת מיד את אי־פרסומו. מרבית המדינות מטילות חובה כללית לפרסם מאגרי מידע ממשלתיים, וחובה זו כוללת הוראות לאיזון בין הזכות לפרטיות לבין אינטרסים אחרים, לנקיטת צעדים סבירים ולמזעור סיכונים לפגיעה בפרטיות, בין השאר באמצעות טכניקות התממה של מידע פרטי. התממה נתפסת כמאפשרת פרסום יזום של המידע אגב מזעור הפגיעה בפרטיות בעלות נמוכה יחסית ובאמצעים זמינים.

מדינות רבות רואות בהתממה פתרון לפרסום יזום של מאגר מידע הכולל מידע מזהה. בארצות הברית, למשל, כאשר מאגר מידע כולל מידע מזהה או ניתן לזיהוי, כאשר יש בפרסום היזום משום פגיעה בפרטיות על פי מבחן הציפייה הסבירה וכאשר יש גם "אינטרס ציבורי משמעותי" בפרסום המידע למרות הפגיעה בפרטיות – הרשות השלטונית נדרשת לבחון אם אפשר להגשים את האינטרס הציבורי המשמעותי באמצעים שפגיעתם בפרטיות פחותה (למשל, התממה). על הפגיעה בפרטיות להיות אמיתית ולא־ספקולטיבית ולנבוע מעצם הפרסום היזום של המידע. "אינטרס ציבורי משמעותי" מוגדר בדין האמריקני כמימוש של התכלית הדמוקרטית. הכוונה למידע שיש בו כדי להגביר את השקיפות השלטונית, דהיינו להאיר במישרין את דרך הפעולה של הרשות ואת ביצוע חובותיה. ככל שיש במידע כדי להעיד על התנהגות לא ראויה של פקיד רשות בדרג גבוה יותר, כך גובר האינטרס הציבורי בחשיפת המידע. עם זאת, לא די בטענה בלבד או בתועלת היפותטית לציבור, ונדרשות ראיות משמעותיות שיובילו אדם סביר להאמין שהשחיתות הנטענת אכן עשויה הייתה להתרחש ושחשיפת המידע אכן תביא להגשמה או לקידום של האינטרס הציבורי בחשיפת המידע.

באיחוד האירופי – כאשר מדובר במאגר הכולל מידע על גזע, מוצא אתני, דעות פוליטיות, אמונה דתית או פילוסופית, חברות בארגון עובדים, מצב בריאותי, נטייה מינית, מידע גנטי או מידע ביומטרי – אין מתירים פרסום יזום אלא אם ננקטו אמצעי אבטחה ספציפיים ורק אם הפרסום הוא מידתי למטרה שנקבעה לו.

מקיפה המתעדכנת מעת לעת ולציין בה בבירור את כל מאגרי המידע המתאימים לפרסום יזום לציבור ואת אלה שהמשרד הממשלתי סבור כי הם כוללים מידע מזהה או מידע שעלול להוביל לזיהוי חוזר (בשילוב עם מידע נוסף).

בהתאם לכך נקבע כי ההחלטה אם לפרסם מידע אישי על פקידי ציבור תתקבל בהתאם לעקרונות הקבועים בדירקטיבה האירופית להגנה על פרטיות במידע בד בבד עם יישום של טכניקות התממה למזעור הסכנות לפגיעה בפרטיות.[59]

(א) מהי התממה ומהן טכניקות ההתממה המופרות?

התממה (אנונימיזציה; de-identification) משמעה הפשטת המידע מרכיבים מזהים מובהקים. טכניקות ההתממה משתנות כל העת, מתפתחות ומשתפרות בעקבות מחקר מתמיד בתחום. נכון להיום טכניקות ההתממה העיקריות הן רנדומיזציה והכללה.[60]

רנדומיזציה היא שם כולל לטכניקות התממה שעיקרן שינוי במהימנות ובדיוק המידע האישי במטרה להעלים את הקשר בינו לבין האדם נושא המידע. רנדומיזציה כוללת טכניקה של **הוספת רעש**, כלומר הוספה של פרטי מידע שאינם חלק ממאגר המידע המקורי; **טכניקת שינוי** (permutation), המערבבת את הנתונים שבמאגר המידע כך שיקושרו שרירותית לאנשים (נושאי מידע) אחרים שהמאגר כולל מידע על אודותיהם; וטכניקת **הפרטיות הדיפרנציאלית**, שבאמצעותה מחזיק המידע מאפשר עיון בחלק מהמידע שבמאגר באמצעות מערכת של שאילתות אגב מעקב שנועד לוודא כי מכלול התשובות הניתנות למגיש שאילתות יחיד לא יאפשר זיהוי של אדם מסוים.[61]

הכללה היא שם כולל לטכניקות התממה שנועדו לדלל את המידע האישי על אדם מסוים באמצעות שינוי של קנה המידה הרלוונטי או סדר החשיבות.

אחת מטכניקות ההכללה היא **טכניקת האגרגציה – k-anonymity**. הטכניקה מדללת פרטי מידע מסוימים ומביאה אותם לרמה שבה יש ל־K אנשים ערכים זהים מלבד הערך הרגיש. הדילול נעשה על ידי הכללה של פריטי המידע, למשל – החלפת עיר הלידה בארץ הלידה; ציון טווח של ערכים

59 Article 29 Data Protection Working Party, *Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector*, WP239 1806/16/EB (June 8, 2016)

60 *Opinion 05/2014 on Anonymisation Techniques*, **לעיל** ה"ש 57.

61 **שם**.

מספריים (למשל 10,000–20,000 ש"ח) במקום פירוט השכר המדויק; או מחיקת פרט המידע וציון "*" במקומו. מאגר מידע של מטופלים המאושפזים בבית חולים דמיוני כלשהו, הכולל 10 אנשים ו־6 פרטי מידע על כל אחד מהם, ייראה כך:

שם	גיל	מין	עיר מגורים	דת	מחלה
דרק	29	זכר	אילת	נוצרי	סרטן
רוחמה	24	נקבה	באר שבע	יהודי	וירוס
מוחמד	28	זכר	רהט	מוסלמי	מחלת לב
נורית	27	נקבה	חיפה	יהודי	בריאה
ג'ון	24	זכר	נצרת	נוצרי	מחלת לב
לאה	18	נקבה	קרית מלאכי	יהודי	סרטן
ג'ורג'	19	זכר	תל אביב	נוצרי	מחלת לב
עומר	24	זכר	כאבול	מוסלמי	וירוס
שמעון	29	זכר	אילת	יהודי	סרטן
ספא	17	נקבה	יפו	מוסלמי	מחלת לב

לאחר k-anonymity תיראה הטבלה כך:

שם	גיל	מין	אזור מגורים	דת	מחלה
**	30>גיל>20	זכר	אזור הדרום	**	סרטן
**	30>גיל>20	נקבה	אזור הדרום	**	וירוס
**	30>גיל>20	זכר	אזור הדרום	**	מחלת לב
**	30>גיל>20	נקבה	אזור הצפון	**	בריאה
**	30>גיל>20	זכר	אזור הצפון	**	מחלת לב
**	20>גיל	נקבה	אזור הדרום	**	סרטן
**	20>גיל	זכר	אזור המרכז	**	מחלת לב
**	30>גיל>20	זכר	אזור הצפון	**	וירוס
**	30>גיל>20	זכר	אזור הדרום	**	סרטן
**	20>גיל	נקבה	אזור המרכז	**	מחלת לב

K עבור נתוני הגיל, אזור המגורים והמין הוא 2, משום שבכל שילוב אפשרי של הנתונים בכל שורה בטבלה יש לפחות אותם פרטי מידע זהים בשתי שורות לפחות בטבלה.[62]

טכניקה נוספת ממשפחת ההכללה היא **l-diversity**. לפי שיטה זו, שפותחה כשיפור לשיטת k-anonymity, יש לבצע את שיטת k-anonymity כך שבכל קבוצה של K אנשים ייכללו L פרטי מידע שונים בעמודת המידע הרגיש. המטרה היא למנוע ככל האפשר קיום של קבוצות זהות עם שונות מעטה בפרטי המידע. בטבלה שלעיל, למשל, יש לוודא שבכל שתי שורות המציגות זהות בעמודות הגיל, המין ואזור המגורים תהא l שונות בעמודת המחלה (l צריך להיות קטן או שווה ל־k; בדוגמה שלנו l צריך להיות 2).

לבסוף, טכניקת **t-closeness** נחשבת שיפור נוסף של טכניקות L-diversity ו־k-anonymity. לפי טכניקת t-closeness יש לבצע מחדש את שיטת k-anonymity באופן שיבטיח כי l השונות בעמודת המידע הרגיש יהיה קרוב או זהה להתפלגות המידע הרגיש בכלל האוכלוסייה. למשל, אם 10% מהאוכלוסייה חולים בסרטן, אזי לאחר ההתממה בטכניקות האמורות הטבלה צריכה לשקף את המצב שבכל קבוצת k אנשים מופיעים רק 10% החולים בסרטן.[63]

לטכניקות של התממה יש גם חסרונות: התממה יכולה לפגוע בשימושיות המידע ובאפשרות להפיק ממנו ידע, שירותים או טכנולוגיות חדשות; היא גם מטילה עומס על כתפי המחזיק במידע, היות שהוא מחויב ליישם אותה, בדרך כלל על ידי החזקת שני מאגרי מידע פעילים – אחד שהמידע בו מלא ואחד ללא פרטים אישיים או פרטים מזהים. החיסרון המרכזי של שיטת ההתממה הוא שגם לאחר יישומה בטכניקות למיניהן עדיין יש אפשרות לזיהוי חוזר.[64]

62 Arvind Narayanan & Vitaly Shmatikov, Robust De-Anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset) (2008)

63 Ninghui Li, ;57 **לעיל** ה"ש ,*Opinion 05/2014 on Anonymisation Techniques* Tiancheng Li, & Suresh Venkatasubramanian, *T-closeness: Privacy Beyond k-anonymity and l-diversity*, 2007 IEEE 23rd International Conference on Data Engineering (2007)

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

יש אף הטוענים שאפשרות זו הופכת את ההתממה לשיטה שהיא אמנם מצוינת אך אינה בת השגה. בכך נעסוק בַּתת־פרק הבא.

חשוב לציין **שפסאודונימיזציה** (pseudonymisation) אינה טכניקת התממה אלא היא אמצעי לאבטחת מידע.[65] הנימוק הוא שפסאודונימיזציה מפחיתה את הסיכויים שמידע אישי יקושר עם אדם מסוים, אבל אינה מונעת אפשרות לזהות אותו באמצעות מאגרי מידע אחרים שמאפשרים לקשר את הכינויים או הקיצורים עם התכונות המזהות. משמעה החלפת פרט מידע אישי (תכונה) אחד באחר. שיטת פסאודונימיזציה נפוצה היא **הסתרת מידע** (data mask), כלומר החלפת פרט מידע אישי מסוים בערך אקראי כלשהו בניסיון לשמור על התצוגה הקודמת של המידע (look and feel). דוגמה לכך היא החלפה של תיבות מידע אישי קבועות (שם, כתובת או מספר זהות) בכינויים או בקודים: במקום להציג מספר תעודת זהות שלם (012345678) מופיע במאגר המידע רק מספר חלקי (01XXXX678). באחדות ממדינות ארצות הברית נקבע שכאשר מדובר בפרסום יזום של מידע רפואי יצוינו רק שתי ספרות מהמיקוד באזורים שבהם מתגוררים 20 אלף תושבים או פחות, כדי להפחית את הסיכויים לזהות אדם מסוים.

(ב) התממה וסכנת הזיהוי החוזר

(1) מהו זיהוי חוזר?

זיהוי חוזר משמעו הצלבת מידע בלתי מזהה עם מידע אחר (שפורסם באינטרנט או במקום אחר). הצלבה זו יכולה ליצור הפקת מידע מזהה, משמע פגיעה בזכות לפרטיות. ככל שיכולות הניתוח וכריית המידע משתפרות וככל שמידע רב יותר

Birnhack, S-M-L-XL: Big Data as a New Informational Privacy Paradigm, Big Data and Privacy: Making Ends Meet 7–10 (Stanford Law School, 2013); Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 (2) International Data Privacy Law 74 (2013); Rubinstein & Hartzog, **לעיל** ה"ש 57.

65 Amy Conroy & Teresa Scassa, *Promoting Transparency while Protecting Privacy in Open Government in Canada,* 53 (1) Alberta Law Review 3 (2015); מיכאל ביקסון **שימור פרטיות בכרייה ובפירסום של מידע מבוזר** 5 (2015); *Opinion 05/2014 on Anonymisation Techniques*, **לעיל** ה"ש 57.

נעשה זמין (גם אם הוא בלתי מזהה) – בין באמצעות חברות פרטיות המנגישות אותו ובין שמדובר במידע ממשלתי שהונגש או במידע שנפרץ או דלף – כך מתרבים הסיכויים לזיהוי חוזר, כלומר לאפשרות לחלץ את זהותו של אדם מתוך פרטים בלתי מזהים.[66]

כבר היום אין צורך בשמו של אדם, ודי בנתוני תקשורת בלתי מזהים שיוצלבו עם פרטי מידע אחרים כדי שתתאפשר הפקת מידע מזהה. כך למשל, אתר סחר אלקטרוני זקוק לפרטיו המזהים של הקונה. אגב המכירה, האתר אוסף על הקונה גם פרטים רבים בלתי מזהים. העברת המידע הבלתי מזהה לצד שלישי, לרבות כתובת IP, אינה מחייבת קבלת הסכמת הקונה באתר, מצב שעלול להביא לכך שכאשר הקונה ייכנס מאותה כתובת IP לאתר של הצד השלישי שאליו הועבר המידע, אותו צד שלישי כבר יחזיק בפרופיל הצרכני שלו, שהגיע אליו ללא ידיעתו או הסכמתו. כאשר כתובת ה־IP משמשת לגלישה מטלפון נייד, היא מהווה פרופיל מדויק יחסית של אדם אחד המשתמש באותו טלפון נייד ולא של כמה אנשים החולקים אותו מחשב או אותה גישה לאינטרנט.[67]

(2) כיצד אפשר לאמוד את הסיכויים לזיהוי חוזר?

בשנת 2012 פרסם נציב הפרטיות הבריטי נהלים מנחים מקיפים להתממה (לשימוש המגזרים הפרטי והציבורי), לאו דווקא בהקשר של פרסום יזום. בהנחיות נקבע כי הסיכויים לזיהוי חוזר צריכים להיות גדולים מ"סבירות רחוקה". עוד נקבע כי חשש לזיהוי חוזר מתקיים לא רק כשמתקבל זיהוי שמי וכי די ביצירת "קשר אמין" בין מידע מסוים לאדם מסוים.[68]

66 Scassa, **לעיל** ה"ש 17, בעמ' 397–398, 407–408; Elizabeth Denham, *Evaluating the Government of British Columbia's Open Government Initiative, Investigation Report F13-03*, Office of the Information & Privacy Commissioner for British Columbia (July 25, 2013) 33–34

67 Rubinstein & Hartzog, **לעיל** ה"ש 57; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701 (2010)

68 *Anonymisation: Managing Data Protection*, **לעיל** ה"ש 56, בעמ' 15–16, 19, 21.

חשיפת נתונים של תורמי DNA

בשנת 2013 הוכח כי לא די בהתממה של מאגר מידע על תורמי DNA באמצעות הסרת זהות התורם. באמצעות הצלבת נתונים מהמאגר (מועד התרומה, גיל התורם ומקום מגוריו) עם נתונים זמינים באינטרנט (כגון אילן יוחסין, מודעות אבל ותוצאות של שאילתות חיפוש) הצליחו חוקרים לזהות אחדים מהתורמים.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, p. 9, 0829/14/EN WP216 (April. 10, 2014)

המבחן שהציע נציב הפרטיות הבריטי כדי לבחון את סבירות ההצלחה של ניסיונות לזיהוי חוזר הוא מבחן **הפורץ המעוניין** (motivated intruder) שהוזכר לעיל: האם אדם בעל יכולות רגילות, שיש לו גישה למידע המתפרסם באינטרנט, במאגרי מידע ציבוריים ובספריות, כמו גם מוטיבציה לזהות אדם מסוים על בסיס המידע האנונימי – האם הוא יצליח לעשות זאת. סבירות הזיהוי החוזר במסגרת מבחן הפורץ המעוניין תיבחן על בסיס ההנחה שאפשר להצליב את המידע האנונימי עם מידע שכבר נמצא בידי הציבור או שצפוי להימצא בידיו בעתיד בלי להניח שלפורץ המעוניין יש יכולות מקצועיות ברמה של האקר. עוד המליץ נציב הפרטיות לבצע מדי תקופה הערכה מחודשת באשר לשחרור מידע נוסף לפרסום.[69]

בשנת 2014 קבע בית המשפט העליון הקנדי רף גבוה למדי להכרה באפשרות לזיהוי חוזר. נפסק כי האפשרות שמידע בלתי מזהה בשילוב עם מידע נוסף יוביל למידע מזהה תיבחן על פי הטכנולוגיות והמידע העומד באותה עת לפני בית המשפט. במילים אחרות, יש להוכיח כי אם המידע הבלתי מזהה יקושר במישרין למידע קיים אחר המוצג לפני בית המשפט כחלק מההליך המשפטי, אפשר לצפות בסבירות גבוהה שיתקבל מידע מזהה. חששות ספקולטיביים לזיהוי – למשל, שבעתיד יהיה יותר ויותר מידע זמין באינטרנט או ציפייה שהתפתחויות בטכנולוגיות המידע יביאו בעתיד לזיהוי על בסיס המידע המדובר לא יובאו בחשבון בהווה. על פסיקה זו נמתחה ביקורת בטענה שהיא אינה נותנת את הדעת

69 **שם**, בעמ' 15–16, 19–23.

לא להתקדמות בטכנולוגיית המידע, לא לשפע המידע הזמין לציבור באינטרנט ולא למידע שכבר נמצא בידי חברות פרטיות.[70]

באיחוד האירופי תיעשה בחינת קיומה של אפשרות לזיהוי חוזר בכל מקרה לגופו, בהתאם לנסיבות ולהקשר. דהיינו, לאחר נקיטת פעולות התממה יש לבדוק ולוודא שאכן אין אפשרות לזהות אדם מסוים גם כאשר משתמשים בכל האמצעים הסבירים שהמחזיק במידע או צד שלישי ישתמשו בהם, לפי ההקשר והנסיבות.[71]

(3) התחשבות בחשש מפני זיהוי חוזר במדיניות פרסום יזום של מאגרי מידע ממשלתיים

לכאורה, טכניקות של התממה מבטלות את החשש מפני זיהוי חוזר, אולם בשנים האחרונות מחלחלת ההבנה שלא תמיד זה כך. בבריטניה, למשל, קבע נציב הפרטיות שאין אפשרות להבטיח שהנתונים לא יהיו בני זיהוי חוזר, משום שאין דרך להעריך איזה מידע – שכבר נגיש בשוק – עלול להביא לזיהוי חוזר אם יוצלב עם המידע האנונימי שבמאגר הממשלתי. לפיכך נקבע בהנחיות הנציב שכאשר קשה לאמוד את הסבירות לזיהוי חוזר, יש להתחשב במידת הרגישות של המידע ששוקלים לפרסם. ככל שמדובר במידע אישי רגיש, מומלץ לקבל את הסכמת האדם לפרסום האנונימי של המידע על אודותיו או לאמץ אמות מידה מחמירות יותר לטכניקות ההתממה המיושמות. במקרים רגישים במיוחד מוצע להימנע לחלוטין מפרסום המידע.[72]

באיחוד האירופי הובהר, בדומה, שהסיכון של זיהוי חוזר הוא אינהרנטי לכל טכניקת התממה, בעיקר לנוכח ההתפתחות המתמדת בטכנולוגיית המחשוב. שום טכניקת התממה אינה הופכת את מאגר המידע לאנונימי לחלוטין, אך כולן מאפשרות להנגיש מידע מתוך מזעור הסכנה לפגיעה בפרטיות, ובלבד שהן מיושמות בו־זמנית, ביעילות ובהתאמה עם ההקשר והרגישות של המידע האישי שבמאגר. יתרה מזו, התממה אינה פעולה חד־פעמית. לנוכח הסיכויים לזיהוי חוזר צריך שהמחזיק במידע ישוב מעת לעת ויעריך מחדש את הסיכונים הטמונים בפרסום המידע לזכות לפרטיות של האנשים שהמידע הוא על

70 Conroy & Scassa, **לעיל ה"ש 65**.

71 *Opinion 05/2014 on Anonymisation Techniques*, **לעיל ה"ש 57**.

72 *Anonymisation: Managing Data Protection*, **לעיל ה"ש 56**, **בעמ' 15–16, 19–23**.

אודותיהם.[73] עם זאת, במציאות של פרסום באינטרנט, ספק אם לאחר פרסומו הראשוני של המידע יש טעם לבחון מחדש את הסיכונים הללו, היות שלאחר הפרסום הראשוני אין ביכולתו של המחזיק המקורי במידע לשלוט בשימוש שיעשו בו צדדים שלישיים. בחינה כזו תוכל להועיל רק לעתיד, למאגרי מידע שטרם פורסמו באינטרנט.

הספרות שדנה בדרכים להתמודד עם סיכוני הזיהוי החוזר מציעה אף היא להתמקד במזעור הסכנות לפרטיות ולא בניסיון למניעה מוחלטת של נזק לפרטיות. רובינסטיין והרצוג, למשל, ממליצים לאמץ רגולציה המתירה פרסום של מאגרי מידע ולהתמקד בתוך כך בהליך של ניהול ומזעור הסיכונים לזכות לפרטיות, ולא במימוש של אנונימיות מוחלטת. רגולציה כזו תקבע את התנאים ודרישות־הקדם שיש למלא, בהתאם להקשר ולמידת הרגישות של המידע, כדי להקטין את הסיכויים לזיהוי חוזר, בדומה לרגולציה הנהוגה בתחום אבטחת המידע; התנאים ודרישות־הקדם ייקבעו לפי הסטנדרט המקובל בתעשייה באותה עת. עם זאת, רובינסטיין והרצוג מתנגדים ככלל לפרסום יזום של מאגרי מידע תחת התממה ומציעים לבחון שיטות אחרות להנגשה מוגבלת יותר של מידע (דוגמת פרטיות דיפרנציאלית, המאפשרת להנגיש מידע חלקי בתגובה לשאילתה). שיטות אלו מספקות לדעתם הגנה טובה יותר על הזכות לפרטיות.[74]

טנא ופולונסקי עוסקים אף הם באפשרויות ההגנה על הזכות לפרטיות לנוכח הסיכונים האורבים לה, ובכללם הסיכון לזיהוי חוזר. הפתרון שהם מציעים אינו מתייחס לסוגיית הפרסום היזום של מאגרי מידע ממשלתיים, אלא עוסק ככלל בקושי להגן על הזכות לפרטיות בכלים המוצעים כיום במשפט המשווה. לשיטתם, יש לאמץ את האסטרטגיה של "שותפות ברווחה". במסגרתה יש לחייב את המחזיק במידע להעניק זכות גישה לאנשים שהמידע הוא על אודותיהם, בפורמט שמיש ונגיש הן לבני אדם והן בשפת מכונה, כך שיוכלו להשתמש באפליקציות למיניהן לשם ניתוח המידע האישי שנאגר עליהם ולהסיק ממנו מסקנות. לדעת טנא ופולונסקי, זכויות גישה כאמור יובילו ליצירת שוק משגשג של טכנולוגיות חדשניות הקשורות למימוש ויישום של זכותם של אנשים להיות בעלי גישה למידע האישי עליהם, ובסופו של דבר יאפשרו להם להצהיר על המדיניות,

73 *Opinion 05/2014 on Anonymisation Techniques*, **לעיל** ה"ש 57.

74 Rubinstein & Hartzog, **לעיל** ה"ש 57; Rubinstein, **לעיל** ה"ש 64.

ההעדפות והתנאים הרצויים להם ליצירת קשר אוטומטי עמם.[75] הצעתם של טנא ופולונסקי מעוררת ויכוח על הפיכת מידע אישי לנכס קנייני סחיר.[76]

חרף חשיבותם, שינוי מודל ההגנה על הזכות לפרטיות והוויכוח על מסחורה אינם מעניינו. אנו שותפות זה כבר להבנה שחוק הגנת הפרטיות, בנוסחו כיום, אינו מתאים למציאות הדיגיטלית ואשר על כן נחוצה חשיבה מחדש לגביו; לשם כך אף יזמנו הקמת קבוצת מומחים כדי שתנסח חוק הגנת פרטיות חדש למדינת ישראל. גם נושא זה אינו מעניינו של המסמך שלנו, המבקש להתמקד בפתרונות מידיים ליישום החלטת הממשלה בדבר פרסום יזום של מאגרי המידע הממשלתיים. עם זה, יש לפעול, בנפרד, לשינוי בחוק הגנת הפרטיות.

ובכן, חשובות מאוד השאלות כיצד אפשר לקבוע אם מידע שעבר התממה יכול להוביל לזיהוי חוזר וכיצד אפשר לאמוד את הסיכויים שכך אכן יקרה. כאשר יש סבירות גבוהה לזיהוי חוזר של פרטי המידע המזהים במאגר המידע למרות פעולות ההתממה, נותרת בעינה שאלת הפגיעה בפרטיות עקב פרסומו היזום של מאגר המידע.[77] השאלה אם מאגר מידע ממשלתי מסוים מתאים לפרסום יזום אינה באה על פתרונה על ידי נקיטת טכניקות של התממה. יש להמשיך, אם כן, לשלב השני – שלב האיזון בין הפגיעה בפרטיות ובין החשיבות הציבורית שבהשגת התכלית (הדמוקרטית או הכלכלית) של הפרסום.

אפשר כי מנגנון השאילתות שהציעו רובינסטיין והרצוג מנסה ליצור מצב של הגנה מושלמת על הזכות לפרטיות, אבל בטווח הרחוק הוא מונע מימוש של היתרונות הכלכליים והחברתיים הטמונים בניתוח המידע. מנגד, הטענות של חלק מהגורמים בתחום – שלפיהן יש בכוחן של טכניקות התממה מסוימות למנוע לחלוטין זיהוי חוזר – מתעלמות מכך שבכל הנוגע למעשים שלטוניים ולמידע שהושג בכפייה, ראוי לצאת מהנחת העבודה שאפשר להגיע לזיהוי חוזר של כל פריט מידע, אם לא בהווה אז ודאי בעתיד. הנחת עבודה זו, שלפיה אין לראות בהתממה פתרון קסם המעניק הגנה מושלמת לזכות לפרטיות, מקובלת גם בספרות[78] ובמדיניות הפרסום היזום או הגנת הפרטיות של האיחוד

75 Tene & Polonetsky, **לעיל** ה"ש 64.

76 ראו למשל Rubinstein, **לעיל** ה"ש 64; Birnhack, **לעיל** ה"ש 64.

77 Conroy & Scassa, **לעיל** ה"ש 65.

78 Rubinstein & Hartzog, **לעיל** ה"ש 57; Tene & Polonetsky, **לעיל** ה"ש 64.

האירופי[79] ושל בריטניה.[80] לפיכך מודל המכיר בכך שתמיד תיתכן פגיעה בזכות לפרטיות (גם לאחר נקיטת הטכניקות של התממה) ולכן פונה לאיזון מידתי בין האינטרס הציבורי לפגיעה בפרטיות על פי עקרון המידתיות – מודל כזה עדיף והוגן יותר מפתרונות המתעלמים מן הסיכון האפשרי.[81]

3. איזון בין האינטרסים המתנגשים

שלב האיזון בין האינטרסים מגיע לאחר בחינת המידע שבמאגר, לאחר ההכרה באינטרס הציבורי שבפרסום המידע (התכלית הדמוקרטית, התכלית הכלכלית או שתיהן), לאחר ההכרה בחשש לפגיעה בפרטיות של האנשים שהמידע הוא על אודותיהם, ולאחר ההכרה בכך שהתממה של המידע לא תוכל למנוע לחלוטין את הפגיעה בפרטיות (בין בשל היעדר האפשרות להתממה, בין בשל הסיכויים הרבים לזיהוי חוזר למרות ההתממה ובין בשל ההכרה שהתממה אינה יכולה לספק הגנה מלאה ומוחלטת על הזכות לפרטיות). בבואם ליישם את חובת הפרסום היזום נדרשים פקידי הממשל לאזן בין האינטרס הציבורי שבפרסום המידע – כלומר, החשיבות של הגשמת התכלית הדמוקרטית או הכלכלית – לבין הזכות לפרטיות, ולהכריע כיצד, אם בכלל, יתבצע פרסום המידע.

בארצות הברית, אם הרשות השלטונית מגיעה למסקנה שהפרסום היזום של מאגר המידע חיוני להגשמת האינטרס הציבורי (כלומר, להשגת התכלית הדמוקרטית) ומבינה שאי־אפשר להגשים את התכלית הדמוקרטית באמצעים חלופיים שפגיעתם בפרטיות פחותה – עליה לאזן בין הפגיעה בפרטיות לבין האינטרס הציבורי בהגשמת התכלית הדמוקרטית. לעניין האיזון פסקו בתי המשפט בארצות הברית כי הזכות לפרטיות גוברת כשמדובר בפרטי מידע אישיים כגון שם, כתובת, מספר טלפון, תאריך לידה, מצב משפחתי, חוקיות הילדים, זהות אבי הילדים, מצב רפואי, תשלומי סעד, צריכת אלכוהול, מאבקים משפחתיים, השתייכות דתית, תאריך קבלת אזרחות, מספר זהות, רישום פלילי, שהייה בבתי כלא במדינות אחרות, זהות של נפגעי עברה ומצב כלכלי. כמו כן נפסק שכאשר מדובר בפרסום יזום של מידע שנאסף לשם אכיפת חוק, די להוכיח ציפייה

79 *Opinion 05/2014 on Anonymisation Techniques*, **לעיל** ה"ש 57.

80 *Anonymisation: Managing Data Protection*, **לעיל** ה"ש 56, בעמ' 15–16, 19, 21.

81 Conroy & Scassa, **לעיל** ה"ש 65.

סבירה לפגיעה בפרטיות עקב חשיפת המידע כדי למנוע את פרסומו היזום.

בצד הכללים המנחים שנקבעו בפסיקה מותר בארצות הברית להיעזר במבחנים לקביעת הרמה הנאותה של אבטחת מידע (מוצעים במדריך של NIST — National Institute of Standards and Technology). המדריך מיועד, אמנם, לסייע לרשויות פדרליות לקבוע וליישם את סטנדרט אבטחת המידע המתאים, אבל המבחן המשמש לקביעת רמת האבטחה של המידע יכול לשמש גם כדי לקבוע אם אפשר לפרסם מידע באופן יזום אם לאו. אימוץ של מבחנים אלה עולה בקנה אחד עם הצעתם של רובינסטיין והרצוג ליישם רגולציה שאינה מתמקדת בהשגת הגנה מושלמת על הזכות לפרטיות אלא בדרישות מוקדמות למזעור הנזק לזכות לפרטיות, בדומה לרגולציה בתחום אבטחת המידע.[82]

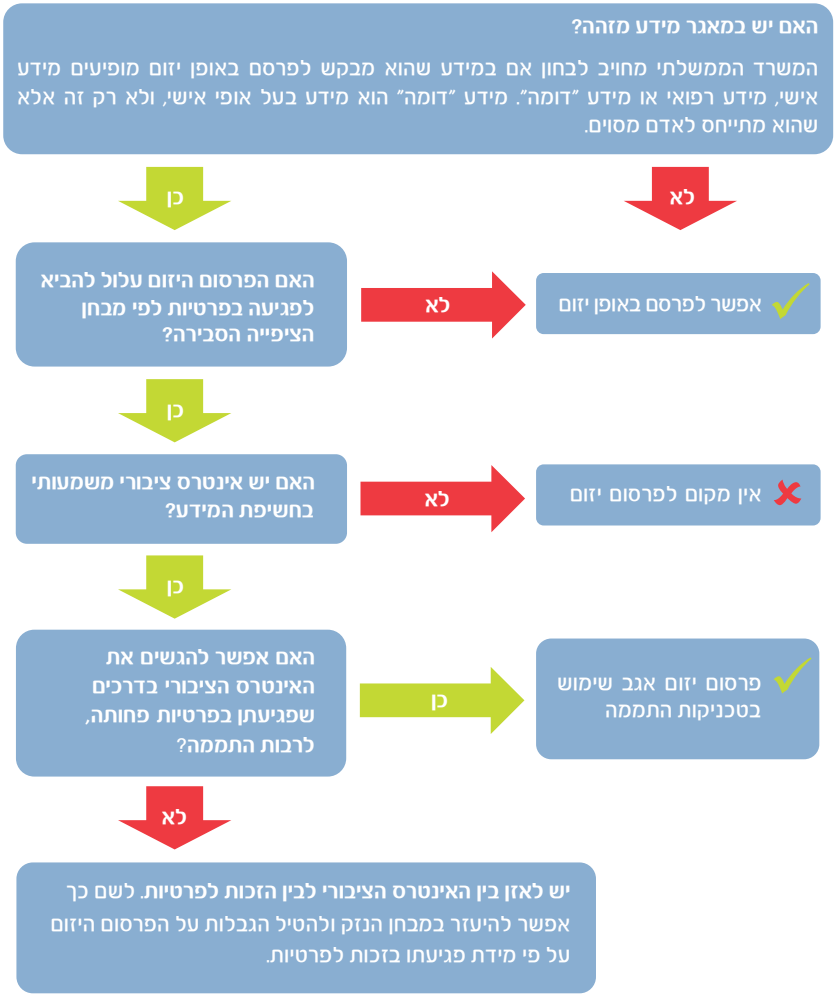
אם כן, לפי המדריך, רמת אבטחת המידע נקבעת על פי מבחן הנזק הפוטנציאלי שעלול להיגרם מפרצת אבטחה – לפעילות הרשות הממשלתית, לנכסיה או לבני אדם. ככל שהנזק האמור גבוה יותר, כך יש להטיל הגבלות מחמירות יותר על פרסומו היזום של המידע. **פגיעה קלה** נמדדת במונחים כלכליים בלבד; **פגיעה בינונית** משמעה פגיעה ניכרת ביעילות התפקוד של הרשות הממשלתית, נזק פיננסי ניכר או פגיעה ניכרת באדם (למעט פגיעה בחיי אדם או פציעה מסכנת חיים). **פגיעה חמורה או קטסטרופלית** משמעה ירידה חמורה ביכולת של הרשות לבצע את משימותיה המרכזיות או אובדן מוחלט שלה, נזק גדול לנכסיה, נזק פיננסי גדול, או נזק חמור או קטסטרופלי לאדם (לרבות פגיעה בחייו או פציעה מסכנת חיים).[83] אם תוצאת האיזון מובילה את הרשות הממשלתית האמריקנית להחלטה שמאגר מידע מסוים אינו מתאים לפרסום יזום, עליה לפרט בכתב את השיקולים שהובילו אותה להחליט כפי שהחליטה.[84]

82 ראו Rubinstein & Hartzog, **לעיל** ה"ש 57; Rubinstein, **לעיל** ה"ש 64; והדיון בטקסט הסמוך לה"ש 74.

83 National Institute of Standards and Technology, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories (August 2008)

84 The White House, National Strategy for Trusted Identities in Cyberspace 6–8 (April 2011); Sylvia M. Burwell, Steven VanRoekel, Todd Park, & Dominic J. Mancini, *Memorandum for the Heads of Executive Departments and Agencies: Open Data Policy-Managing Information as an Asset*, M-13-13 Executive Office of The President (May 9, 2013)

התרשים הבא מתאר את סדר הפעולות שפורט לעיל לפרסום יזום של מאגר מידע ממשלתי בארצות הברית.



המבחן המקובל ברוב חוקי חופש המידע בעולם למידת הנגשתו של מידע ממשלתי הוא גם מבחן הנזק, בדומה למבחן המוצע במדריך NIST בארצות הברית. במחוז אלברטה שבקנדה, למשל, נקבע בסוף שנת 2013 כי נתונים של משכורות, הטבות ופיצויי עובדים שמשכורתם עולה על 100 אלף דולר יפורסמו באופן יזום באתר אינטרנט ממשלתי ייעודי, כדי להגביר את אחריותיות הממשל במחוז כלפי משלמי המסים. קובעי המדיניות במחוז אלברטה החליטו שהתועלת הנובעת מהגשמת התכלית הדמוקרטית עולה על הנזק שבפגיעה בזכות לפרטיות של פקידי ממשל מעל דרג מסוים. גם ביפן, באירלנד, בבריטניה ובניו זילנד נקבע כי מידע ממשלתי ייחשף אם התועלת לציבור בזכות החשיפה עולה על הנזק שעלול להיגרם ממנה.

מערך הכללים של האיחוד האירופי, שעניינו הגנה על פרטיות מידע (The General Data Protection Regulation; או בקיצור – GDPR)[85] אומץ באפריל 2016 וייכנס לתוקף במאי 2018. מערך זה מפנה לבחינה של תכלית הפרסום היזום ולאיזון בינה לבין הפגיעה בפרטיות.[86]

מהו GDPR? מערך הכללים האירופי להגנת הפרטיות כולל גם דירקטיבה וגם רגולציה שאין צורך לאמצן בחקיקה מדינתית כדי להכניסן לתוקף. מטרת הרגולציה היא לחזק את ההגנה על הפרטיות במידע ולהבטיח את אחידותה בכל מדינות האיחוד האירופי, בראש ובראשונה באמצעות העצמת אזרחי האיחוד בכל מה שקשור ליכולת שלהם לשלוט במידע שנאסף עליהם. הרגולציה יוצרת מערך אחד של כללים לכל מדינות האיחוד. כל אחת מהן אמורה להקים רשות פיקוח עצמאית לטיפול בתלונות ולהפעלת סנקציות בתוכה ולפעול בשיתוף פעולה עם המדינות האחרות. העצמת האזרחים מתרחשת באמצעות החובה להודיע על איסוף המידע ועיבודו למטרות מסוימות ולפרסם את הכתובות של החברות שאליהן אפשר לפנות בבקשות לעיין במידע, לתקנו ולמוחקו או בתלונות ובירורים, וכן באמצעות מתן האפשרות לערער על החלטות הנוגעות לעיבוד מידע, גם כאשר הן מתבצעות על ידי אלגוריתמים. מערך הכללים האירופי כולל גם דרישה להטמעת נוהלי הגנה

85 Regulation (EU) 2016/679

86 GDPR Key Changes, באתר **EUGDPR.org**.

על מידע במסגרת פיתוח של מוצרים ושירותים באיחוד, דרישה להערכת השפעות איסוף ועיבוד המידע על האנשים שהמידע אודותיהם ודרישה להסכמה מודעת של האנשים שהמידע הוא על אודותיהם לשימושים שניוניים במידע הנאסף על ידי חברות. הרגולציה כוללת גם את החובה למנות ממונים על שמירת המידע, הוראות בדבר יכולתם של פרטים לשנע ולהעביר את המידע על עצמם וסנקציות שיכולות להגיע לקנסות של עשרות מיליוני אירו. אחד החידושים שברגולציה הוא שהיא חלה גם על חברות שמרכז הפעילות שלהן אינו באירופה אבל הן מעבדות מידע על תושבי האיחוד. הרגולציה מאפשרת להטיל על החברות האלה קנסות בגובה של עד 4% מהכנסותיהן הגלובליות.

מבחינת תכליתו של הפרסום היזום, הואיל וכל פעולה במידע (לרבות פרסומו) חייבת להיעשות למטרה ספציפית ולגיטימית, הרשות השלטונית נדרשת לבדוק קודם לכול אם הפרסום היזום מתאים לאינטרס הציבורי או מבוצע לשם מילוי חובה המוטלת עליה בחוק. כך למשל, יצירת מפתח (אינדקס) מידע אישי, שמונגש בפלטפורמה ממשלתית המיועדת להגברת השקיפות כלפי האזרח, מאפשרת לאזרח לחפש בתוך המידע ולכן תיחשב נחוצה להגברת השקיפות. לעומתה, יצירת מפתח של מידע מזהה על גבי מנוע חיפוש חיצוני לא תיחשב נחוצה להגשמה של מטרת השקיפות.

כאשר מתלבטים אם להנגיש מידע באופן גלובלי, באמצעות מנוע חיפוש חיצוני, יש להביא בחשבון את מידת הזמינות של המידע. אם אין אינטרס ציבורי גלובלי בהנגשה במידת זמינות בינלאומית כזו, כי אז הפצת המידע באופן זה אינה לגיטימית ויש לשקול את הנגשתו באינטרנט במידה מוגבלת יותר, למשל בפלטפורמה ממשלתית ייעודית שהכניסה אליה מותרת רק למשתמשים מורשים עם סיסמה.[87] אם אכן נמצאה תכלית לגיטימית לפרסום היזום, על הרשות האירופית לאזן – באמצעות מבחן מידתיות – בין תכלית זו לבין הפגיעה

87 לדעתנו, הגבלת הפרסום היזום במציאות הנוכחית לפלטפורמה ייעודית שהגישה אליה מותנית בשם משתמש ובסיסמה היא חסם מלאכותי שאינו יכול למנוע תפוצה גלובלית של המידע המפורסם. הסיבה לכך היא שאפשר להעתיק בקלות יחסית את המידע שהונגש לטובת מורשה גישה ולהציגו באתר אינטרנט אחר שהוא נגיש לכול.

בפרטיות. במסגרת האיזון והבטחת המידתיות של הפרסום היזום יש לבחון אם אפשר להשיג את התכלית בדרכים אחרות שפגיעתן בפרטיות פחותה. בין השאר יש לתת את הדעת לאופי המידע המדובר ולקבוצת האנשים שאליה הוא מתייחס. לדוגמה, יש להבחין בין בעלי תפקידים בשירות הציבורי על פי דרגתם בהיררכיה, על פי תפקידם ועל פי היקף שיקול הדעת והאחריות שלהם בקבלת החלטות. ייתכן, למשל, כי פרסום הכנסותיו והוצאותיו של בעל תפקיד בכיר בממשלה בתקופת שירותו הציבורית עשוי להיות רלוונטי לציבור.

בבחינת המידתיות יש לבדוק גם אם המידע המיועד לפרסום היזום מעודכן, נכון ומדויק ואם הוא נשמר בפורמט שמאפשר זיהוי של אדם מסוים לפרק זמן העולה על הנחוץ לשם השגת המטרה.[88] נדגיש כי התניית פרק הזמן לשמירת המידע בנחיצותו להשגת המטרה שלשמה נאסף היא בעייתית ליישום במציאות של פרסום יזום באינטרנט, שכן מרגע הפרסום מאבד המפרסם את השליטה במידע.

ולבסוף, כדי להבטיח את מידתיות הפרסום היזום, על המחזיק במידע לנקוט אמצעי אבטחה טכניים סבירים להגנה על מידע אישי ולמניעת אובדן מקרי, הרס, שינוי, גילוי בלתי מורשה או שימוש בלתי מורשה אחר במידע. לפיכך על המשרד הממשלתי לנקוט אמצעי אבטחה נאותים למזעור הסיכון שהמידע הזמין באינטרנט, יימחק, יתוקן, ישונה או יוצא מהקשרו. לשם כך מותר, למשל, לציין מקורות אמינים שאפשר לקבל מהם את המידע ומותר גם להשתמש בחתימה דיגיטלית.[89]

דוגמה לאיזון בין תכלית הפרסום לבין פגיעה בפרטיות היא ההחלטה של האיחוד האירופי בעניין פרסום מחקרים קליניים.[90] בהחלטה נקבע שתכלית הפרסום היא לעודד שימוש מושכל בתרופות, לשפר את בריאות הציבור בעתיד, לתת לִמְפַתחי תרופות אפשרות ללמוד מהצלחות ומכישלונות העבר ולהמשיך

88 GDPR, Article 6; Directive 95/46/ED, Article 7(c)

89 *Opinion 02/2016 on the Publication of Personal Data*, **לעיל** ה"ש 59.

90 European Medicines Agency, *European Medicines Agency Policy of Publication of Clinical Data for Medicinal Products for Human Use, in site* EMA.EUROPA.EU 4, 7 (October 2, 2014)

במחקר מדעי. עם זאת, בצד התכלית הכלכלית החשובה שבפרסום יזום של מחקרים קליניים יש לשמר ולהגן על הזכות לפרטיות במידע אישי. על כן, טרם פרסומו של מחקר קליני על הרשות המוסמכת לבחון – אגב היוועצות עם בעלי עניין דוגמת ארגוני חולים, חוקרים ותעשיית התרופות – מה הדרך המיטבית לשמור על פרטיות החולים המשתתפים במחקר ולמנוע את זיהוים, בהתחשב בטכנולוגיות כריית המידע הקיימות באותה עת. כמו כן יש לכבד את ההסכמה מדעת של המשתתפים במחקר הקליני.

ה. פרסום יזום של מאגרי מידע בישראל

1. המצב החקיקתי הקיים

חוק חופש המידע מעגן את זכותו של כל אזרח ישראלי או תושב בישראל לקבל מידע מרשות ציבורית.[91] זכות זו אינה מוחלטת ויש לה חריגים במקרים המנויים בחוק, בכללם, כאמור, בסעיף 9(א)(3) לחוק: "מידע שגילויו מהווה פגיעה בפרטיות, כמשמעותה בחוק הגנת הפרטיות, תשמ"א-1981, אלא אם כן הגילוי מותר על פי דין". מקרב הפגיעות בפרטיות המנויות בסעיף 2 לחוק הגנת הפרטיות, הפגיעה הרלוונטית ביותר לעניין פרסום יזום של מאגרי מידע ממשלתיים היא השימוש בידיעה על "ענייניו הפרטיים של אדם" (מונח שפורש בהרחבה על ידי בתי המשפט) או מסירתה לאחֵר שלא למטרה שלשמה נמסרה,[92] אלא אם יש בפרסום המידע משום עניין ציבורי ממשי הגובר על עוצמת הפגיעה בפרטיות בנסיבות העניין.[93]

בית המשפט העליון השתמש בסייג הגנת הפרטיות בפרשת **שנרום**, שבה נפסק כי רשות מקומית -עירייה חדרה באותו מקרה – אינה מחויבת, במסגרת

91 ס' 1 לחוק חופש המידע, התשנ"ח-1998 ס"ח 1667 (להלן: חוק חופש המידע).

92 ס' 9(א) לחוק חופש המידע וס' 2(9) לחוק הגנת הפרטיות.

93 ס' 9(א)(3) לחוק חופש המידע, ס' 18(3) לחוק הגנת הפרטיות, דוח הצוות הבין-משרדי, **לעיל** ה"ש 13, בעמ' 31-32.

בקשה על פי חוק חופש המידע, להעביר למגישת הבקשה – חברה פרטית העוסקת בייעוץ לענייני ארנונה – את שמותיהם של המחזיקים בנכסים ברשות, את כתובתם המדויקת או את גודל הנכס שבו הם מחזיקים ואף לא כל מידע על הנחות בארנונה שניתנו להם. הטעם להחלטת בית המשפט היה, ועודנו, שמסירת המידע האמור תהווה פגיעה בפרטיותם של המחזיקים בנכסים הנדונים לפי סעיפים 2(9) ו־2(6) לחוק הגנת הפרטיות.[94]

עם זאת, חוק חופש המידע מצומצם לנסיבות הספציפיות של מבקש המידע, והוא מאפשר להתנות את מסירת המידע הפוגע בפרטיות בתנאים שיש בכוחם להחליש את עוצמת הפגיעה בפרטיות. כאשר הבקשה למסירת מידע נוגעת למאגר מידע שלם, פרטיותם של אנשים רבים עלולה להיפגע. זו הסיבה שחוק חופש המידע מחייב את מי שהתבקש למסור את המידע לפנות טרם הפרסום אל כל הנפגעים הפוטנציאליים, לברר את עמדתם כלפי פרסום מאגר המידע ולאפשר להם לערער בבית המשפט על ההחלטה לפרסם את המידע על אודותיהם.

חוקים נוספים מחייבים רשויות ציבוריות להעניק לציבור את זכות העיון במאגרי המידע שברשותן (למשל: חוק המקרקעין, התשכ"ט–1969; וחוק הסדרת העיסוק במקצועות הבריאות, התשס"ח–2008). מחמת הפגיעה האפשרית בפרטיות – הרי מאגרי המידע המונגשים עשויים לכלול מידע אישי – זכות העיון ניתנת במתכונת של שאילתות בלבד.[95]

חוק הגנת הפרטיות מכיר בזכותו של אדם לעיין במידע על אודותיו המוחזק במאגר מידע ולבקש את תיקונו אם מצא שהוא שגוי, לא שלם או לא מעודכן. להסדר זה שני חסרונות: ראשית, זכויות אלו אינן חלות במאגרי מידע שמנוהלים על ידי גופים מסוימים המנויים בחוק, למשל: רשויות הביטחון, רשות המסים ושירות בתי הסוהר. שנית, זכויות העיון במאגר ותיקון המידע בו מוגבלת אך ורק לאדם שהמידע הוא על אודותיו, ואין בהן כדי לתת מענה לתכלית הדמוקרטית או לתכלית הכלכלית. הגשמתן של שתי אלו כרוכה בהגברת השקיפות הממשלתית ובעידוד החדשנות, שתבואנה בעקבות הפרסום היזום של כלל מאגרי המידע הממשלתיים.[96]

94 עע"מ 1386/07 **עיריית חדרה נ' שנרום** (פורסם בנבו, 16.7.2012).

95 דוח הצוות הבין־משרדי, **לעיל** ה"ש 13, עמ' 28.

96 ס' 13 וס' 14 לחוק הגנת הפרטיות.

לפיכך, לא חוק חופש המידע ולא חוק הגנת הפרטיות נותנים מענה מפורש לקשיים העולים מפרסום יזום של מאגרי מידע ממשלתיים, לא מצד התכלית הדמוקרטית או הכלכלית ולא מצד הגנת הפרטיות. אין חובה חוקית על משרד ממשלתי לפרסם ביוזמתו את מאגרי המידע שברשותו, ולכן גם אין היום כל הסדר חוקי להגשמת התכליות הדמוקרטית והכלכלית מתוך מזעור הפגיעה הצפויה מפרסום כזה בזכות לפרטיות.

2. ההסדר המוצע בהחלטת הממשלה ובדוח הצוות הבין־משרדי

ניצנים ראשונים להטמעת מדיניות של ממשל פתוח במדינת ישראל הופיעו באוגוסט 2010 בהחלטת ממשלה מס׳ 2201. בהחלטה זו נקבע כי תוקם ועדה בין־משרדית שסמכויותיה יכללו "גיבוש מדיניות והחלטות לביצוע בנושאי 'ממשל פתוח' על־בסיס עקרונות הממשל הפתוח: שקיפות, דיווח, שיתוף הציבור ואחריותיות".[97]

צעד נוסף לקראת פרסום יזום של מאגרי מידע ממשלתיים – הפעם לשם קידום של התכלית הכלכלית – נעשה בנובמבר 2010, בהחלטה של ועדת השרים לעניין השירות הממשלתי לציבור. בהחלטה זו נקבע כי משרדי הממשלה יפרסמו באתרי האינטרנט שלהם רשימה של כלל מאגרי המידע שברשותם ויפרטו את שם המאגר ואת שדות המידע הכלולים בו ולפחות שלוש סדרות נתונים שהן תוצאה של הרצת שאילתה על מאגר המידע, השולפת מספר רב של רשומות בעלות מכנה משותף, שפרסומן ייתן ערך מוסף לציבור, לאקדמיה ולרשויות המדינה. נקבע כי פרסום המידע ייעשה בכפוף לדין, לרבות חוק הגנת הפרטיות, וכי מטרתו "לאפשר שימוש במידע הממשלתי, עיבודו מחדש ופיתוחו על ידי הציבור ולטובת הציבור".[98]

97 החלטה 2201 של הממשלה ה־32 "שיפור השירות הממשלתי לציבור" (8.8.2010).

98 ההחלטה של ועדת השרים קיבלה תוקף של החלטת ממשלה ביום 14.3.2011. ראו החלטה 2985 של הממשלה ה־32 "שימוש במידע הממשלתי, עיבודו מחדש ופיתוחו על ידי הציבור ולטובת הציבור" (14.3.2011).

ביום 1.4.2012 התקבלה החלטת ממשלה מס׳ 4515 (להלן: החלטה 4515) בדבר הצטרפותה של ממשלת ישראל ליוזמה הבינלאומית לממשל פתוח על בסיס ארבעת העקרונות שלהלן:

(א) **עקרון השקיפות והדיווחיות.** הממשלה תנגיש לציבור מידע בעל חשיבות ציבורית – בשם קידום השקיפות, הדיווחיות והביקורת הציבורית, בד בבד עם ההכרה שהמידע שנאסף במאגרי מידע ממשלתיים הוא משאב ציבורי ולכן על הממשלה לספק לציבור גישה מרבית אליו ולאפשר בתוך כך לעבדו ולהשביחו.

(ב) **עקרון שיתוף הציבור.** הממשלה תגבש מדיניות לשיתוף הציבור בהליכי תכנון וביצוע מרכזיים בעבודת הממשלה – במטרה לתרום לתהליכי קבלת ההחלטות, לשפר את ביצוע מדיניות הממשלה ולחזק את אמון הציבור בה. עיקרון זה מוגבל על פי לשונו להגשמת התכלית הדמוקרטית.

(ג) **עקרון האחריותיות.** הממשלה תפרסם מידע על תכניות העבודה של משרדי הממשלה ועל יעדי הביצוע השנתיים שלהם – כדי לחזק את הפיקוח והביקורת הציבורית על עבודת הרשות המבצעת. גם עיקרון זה מוגבל על פי לשונו להגשמת התכלית הדמוקרטית.

(ד) **יישום טכנולוגיות חדשניות.** הממשלה תפעל ליישום טכנולוגיות חדשניות – כדי לקדם את שכלול השירות הציבורי וכדי להשביח את השיח בין הממשל לציבור. גם עיקרון זה, אף שהוא מכיר באפשרות להביא לפיתוח טכנולוגיות חדשניות על בסיס המידע שנמצא במאגרי המידע, מוגבל על פי לשונו להגשמת התכלית הדמוקרטית.

עוד נקבע בהחלטה 4515 כי יוקם ״הפורום הישראלי לממשל פתוח״, שישמש ״גוף מייעץ להשגת היעדים החברתיים והכלכליים הנגזרים מעקרונות הממשל הפתוח: שקיפות ודיווחיות, שיתוף הציבור, אחריותיות ויישום טכנולוגיות חדשניות״.[99]

באוקטובר 2014, כשנתיים וחצי לאחר החלטה 4515, חידשה ממשלת ישראל את מחויבותה לעקרון הממשל הפתוח בהחלטה נוספת (החלטה מס׳ 2097).

99 ס׳ 2 להחלטה 4515, **לעיל** ה״ש 7.

ההחלטה החדשה הדגישה את החשיבות וההכרח שבהנגשת מידע ושירותים ממשלתיים לציבור. בין השאר נקבע כי יש ליצור "סביבה תומכת לקהילת מפתחים מהמגזר הפרטי ('Hub') לפיתוח מענים לאתגרי המגזר הציבורי בנושאים מרכזיים שייקבעו מידי שנה" וכי המטרה הכללית של ההחלטה היא "לעודד חדשנות במגזר הציבורי ובשירותים הציבוריים [...] להביא ליעילות וחיסכון בעבודת משרדי הממשלה, לשפר את השירות הממשלתי לציבור, לצמצם את הנטל הבירוקרטי [...]".[100]

הצבת התכלית הדמוקרטית כעיקר ייעודה של מדיניות הממשל הפתוח ומיתוג התכלית הכלכלית ככלי להגשמת התכלית הדמוקרטית בולטים מאוד גם בתכנית הלאומית לממשל פתוח לשנים 2015–2017. בתכנית זו נאמר:

> ממשלת ישראל החליטה ביום 1.4.2012 להצטרף ליוזמת הממשל הפתוח על בסיס ההבנה שחידושי טכנולוגית התקשורת והמידע מאפשרים להעמיק ולשפר באופן משמעותי את מערכת היחסים הדמוקרטית המסורתית שבין הפרט לממשל. מטרת מדיניות הממשל הפתוח היא להעצים את הפרט, החברה והממשל בישראל, על בסיס ארבעת עקרונות ממשל פתוח:
>
> 1. שקיפות
> 2. שיתוף הציבור
> 3. אחריותיות
> 4. יישום טכנולוגיות חדשניות.[101]

החלטת ממשלה מס' 1933 מאוגוסט 2016, ודוח הצוות הבין־משרדי שאימצה,[102] מטילים על כל משרדי הממשלה חובת פרסום יזום שתיושם עד שנת 2022,

100 החלטה 2097 של הממשלה ה־33 "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית' " (10.10.2014).

101 ממשל פתוח – תכנית פעולה לשנים 2015–2017 (התכנית הלאומית לממשל פתוח, 8.9.2016).

102 ס' 12 להחלטת הממשלה 1933, **לעיל** ה"ש 10.

ובלבד שאין מידע מזוהה בפרסום של מאגרי המידע. "מידע מזוהה" מוגדר כ"מידע אישי כהגדרתו בחוק הגנת הפרטיות וכן כמידע שאינו מזוהה אך ניתן לזיהוי, כשלעצמו או במצטבר עם מידע נוסף".[103] בהחלטה נקבע כי הערכת הסיכויים לזיהוי חוזר תבוצע על ידי מומחה מהתחום הטכנולוגי בליווי ייעוץ משפטי וייעוץ אבטחת מידע.[104]

כאשר מאגר המידע כולל מידע מזהה, על המשרד הממשלתי להעריך אם יש חשיבות ציבורית בפרסום יזום של המידע. קביעה זו תתקבל לאחר בחינה של סוג המידע המזוהה, מידת רגישותו, העניין הציבורי בהנגשתו והאפשרות לקבל הסכמה לפרסום מהאנשים שהמידע נוגע להם.[105]

אם נקבע שיש חשיבות ציבורית להנגשת של מאגר מידע, אף שהוא כולל מידע מזהה, על המשרד הממשלתי לפעול להפיכת המידע שבמאגר למידע שאינו מזוהה. טכניקת ההתממה שתיושם תיקבע על סמך היוועצות במומחה מהתחום הטכנולוגי, יועץ משפטי ויועץ לאבטחת מידע, ולאחר עריכת סקר סיכונים לפרטיות שיכלול הערכה של הסיכויים לזיהוי חוזר עקב הצלבת המידע שבמאגר עם מידע אחר שפורסם לציבור. עוד נקבע בהחלטה 1933 כי רשות התקשוב תבחן פתרונות התממה מרכזיים ורוחביים עבור משרדי הממשלה.[106]

בדיונים של הצוות הבין־משרדי טענו הנציגים של מחלקת ייעוץ וחקיקה במשרד המשפטים, כמו גם אנשי הרשות למשפט וטכנולוגיה, כי לנוכח היקף המידע המפורסם והאפשרויות הרבות להצליבו עם מאגרים ומידע זמין אחר מתעצם החשש לזיהוי חוזר כשמדובר בפרסום של מאגרי מידע שלמים הכוללים מידע אישי. ככלל, הנציגים היו בדעה שפרסום בפורמט של שאילתות עדיף מפרסום של המאגר במלואו.[107]

רשות התקשוב הממשלתי ומטֶה ישראל דיגיטלית במשרד לשוויון חברתי גרסו שהמבחן לפרסום יזום של מאגרי מידע שעלולים לכלול מידע שיאפשר

103 ס' ג(2) להחלטת ממשלה 1933, **שם**.
104 ס' ג(2) להחלטת הממשלה 1933, **שם**.
105 דוח הצוות הבין־משרדי, **לעיל** ה"ש 13, בעמ' 30.
106 נספח ג, ס' א.2 ו־ב החלטת ממשלה 1933, **לעיל** ה"ש 10.
107 דוח הצוות הבין־משרדי, **לעיל** ה"ש 13, בעמ' 29.

זיהוי חוזר צריך להיות מבחן הסבירות. מבחן כזה יתחשב בכך שפרסום יזום נעשה לכלל הציבור ולא למבקש מסוים, שידוע שאפשר להחיל עליו דרישות סודיות ושמדובר בפעולה בלתי־הפיכה. כמו כן, בבחינת הסבירות של זיהוי חוזר בגלל הצלבת המאגר עם נתונים אחרים יש להתייחס לטכנולוגיות העדכניות ביותר בתחום כריית המידע ולסקור גם מאגרים קיימים וגם מאגרים שסביר כי יוקמו בעתיד.[108]

כצעד ראשון ליישום ההחלטה בחן הצוות הבין־משרדי כמה מאגרי מידע שאינם כוללים מידע מזהה והתיר לפרסם את מאגרי המידע של משרד התחבורה והבטיחות בדרכים (עסקי תחבורה מורשים, המראות ונחיתות בזמן אמת, זמן אמת של רכבת ישראל), של משרד החינוך (תקציב משרד החינוך בחתך בית ספרי), של המרכז למיפוי ישראל (מפתח הגושים), של משטרת ישראל (בסיסי נתונים – נתוני פשיעה), של משרד הבינוי והשיכון, של משרד האוצר (מינהל התכנון ורשות מקרקעי ישראל; מלאי תכנון) ושל משרד הפנים (תקציב הרשויות המקומיות).[109]

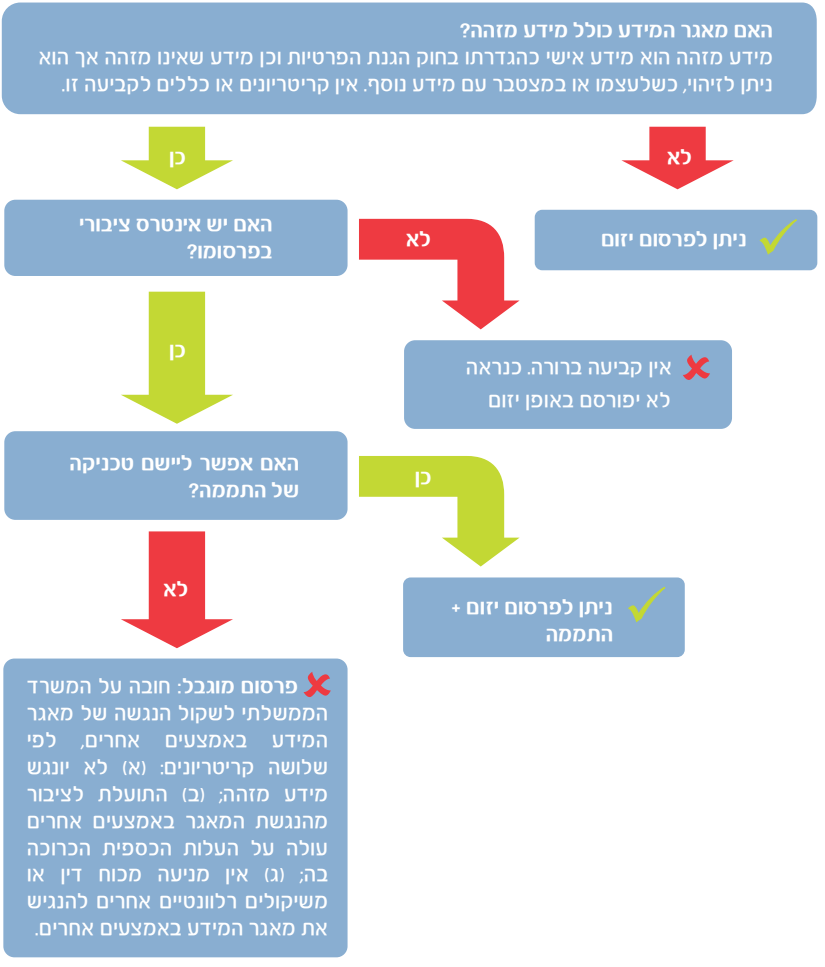
הצוות הבין־משרדי הציע כי אם וכאשר יוחלט שלא לפרסם מאגר מידע מסוים בפורמט פתוח לכלל הציבור, חובה על המשרד הממשלתי לשקול את הנגשתו באמצעים אחרים, לפי שלושה קריטריונים: (א) לא יונגש מידע מזהה; (ב) התועלת לציבור מהנגשת המאגר באמצעים אחרים עולה על העלות הכספית הכרוכה בה; (ג) אין מניעה מכוח הדין או משיקולים רלוונטיים אחרים להנגיש את מאגר המידע באמצעים אחרים.[110]

התרשים שלהלן מתאר את סדר הפעולות לפרסום יזום של מאגר מידע ממשלתי על פי החלטת ממשלה מס׳ 1933 מאוגוסט 2016.

108 דוח הצוות הבין־משרדי, **שם**, בעמ׳ 30.

109 ס׳ 12.ג להחלטת ממשלה 1933, **לעיל** ה״ש 10.

110 ס׳ ג׳ הגדרות, 12.א ו־12.ו להחלטת ממשלה 1933, **שם**.


האם מאגר המידע כולל מידע מזהה?
מידע מזהה הוא מידע אישי כהגדרתו בחוק הגנת הפרטיות וכן מידע שאינו מזהה אך הוא ניתן לזיהוי, כשלעצמו או במצטבר עם מידע נוסף. אין קריטריונים או כללים לקביעה זו.
לא
כן
ניתן לפרסום יזום
לא
האם יש אינטרס ציבורי בפרסומו?
כן
אין קביעה ברורה. כנראה לא יפורסם באופן יזום
האם אפשר ליישם טכניקה של התממה?
כן
לא
ניתן לפרסום יזום + התממה
פרסום מוגבל: חובה על המשרד הממשלתי לשקול הנגשה של מאגר המידע באמצעים אחרים, לפי שלושה קריטריונים: (א) לא יונגש מידע מזהה; (ב) התועלת לציבור מהנגשת המאגר באמצעים אחרים עולה על העלות הכספית הכרוכה בה; (ג) אין מניעה מכוח דין או משיקולים רלוונטיים אחרים להנגיש את מאגר המידע באמצעים אחרים.

ו. דיון והמלצות

1. המצב הקיים

החלטת ממשלה מס׳ 1933 ודוח הצוות הבין־משרדי בעניין פתיחה יזומה של מאגרי מידע שלטוניים הם משמעותיים וחשובים. החלטת הממשלה אינה קובעת, ולא התיימרה לקבוע, מדיניות סדורה להנגשה של מאגרי המידע הממשלתיים מתוך התמודדות עם אתגר ההגנה על הזכות לפרטיות; ההחלטה רק ביקשה להצהיר על המדיניות הממשלתית ״פתוח כברירת מחדל״ (ובאנגלית: open by default), מתוך שאיפה ותחושת דחיפות להתחיל מוקדם ככל האפשר ביישום המדיניות, למרות הותרת ההתמודדות עם פרטי היישום ומשמעויותיו למשרדי הממשלה, בסיוע ובהנחיה של רשות התקשוב הממשלתי.[111] בהחלטה נקבע כי רק בעתיד ״יפורסמו הנחיות משפטיות ומקצועיות, שבהן ייקבעו בין היתר, קווים מנחים להנגשת מאגרי מידע, בדגש על היבטי הפרטיות [...]״.[112] לטענתנו, ללא תכנית יעילה ומעשית, שתאפשר את יישום ההחלטה בהקדם האפשרי, יוזמת הפרסום היזום של מאגרי מידע ממשלתיים עלולה להתמוסס בשל הקשיים הרבים הטמונים במהלך, בעיקר מול החובה להמשיך ולהגן על הזכות החוקתית לפרטיות.

נכון להיום הוגדרו רק מעט מאגרי מידע המתאימים לפרסום יזום מיידי.[113] באשר לשאר מאגרי המידע הממשלתיים, ההחלטה מטילה משא כבד ומורכב על המשרדים הממשלתיים, אף שהחלטת הממשלה הקצתה משאבים להתמודדות עם עומס זה: (א) החלטת הממשלה הקנתה למשרדי הממשלה ליווי מקצועי ותשומות נוספות כדי שיוכלו לעמוד במשימה; (ב) הוטל על רשות התקשוב הממשלתי להנחות את משרדי הממשלה בתהליך של הנגשת מאגרי המידע. כמו כן הוטל עליה לפעול עם מחלקת הייעוץ והחקיקה במשרד המשפטים ועם גורמים נוספים כדי לבחון פתרונות להנגשת מאגרי מידע, מתוך התפיסה

111 דוח הצוות הבין־משרדי, **לעיל** ה״ש 13, בעמ׳ 19.

112 ס׳ ב לנספח ג להחלטת ממשלה 1933, **לעיל** ה״ש 10.

113 ס׳ 12.ג להחלטת ממשלה 1933, **שם**.

שההנגשה מגשימה אינטרס ציבורי חשוב גם כאשר תיתכן פגיעה ממשית או מסתברת בפרטיות.[114]

לפי החלטה 1933, על כל משרד ממשלתי למפות את מאגרי המידע שברשותו ולהכריע עבור כל מאגר אם הוא כולל מידע מזהה, לרבות מידע שיש בכוחו להוביל לזיהוי חוזר. בחינת הסיכויים לזיהוי חוזר תיעשה בידי מומחה מהתחום הטכנולוגי ובליווי ייעוץ משפטי וייעוץ בתחום אבטחת מידע. מלשון הדברים משתמע שגיוסם של מומחים אלו נתון לאחריותו של כל משרד. בהמשך צפויה רשות התקשוב – בשיתוף עם מטה ישראל דיגיטלית ובתיאום עם היחידה הממשלתית לחופש המידע במשרד המשפטים – לנהל שיח "פתוח ומתמשך" עם הציבור בדבר האינטרס הציבורי בפרסום המידע ותעדוף הפרסום במשרדי הממשלה.[115]

מסלול זה נהוג ברוב מדינות העולם: תחילה מיפוי של מאגרי המידע ואחר כך בדיקה אם יש בהם מידע אישי. עם זאת, החלטת ממשלת ישראל, על אף חשיבותה, מציבה שני אתגרים מרכזיים, שהם למעשה שני פנים של אותו מטבע: (א) אין קריטריונים ברורים לסיווג הראשוני של מאגרים בעייתיים לעומת מאגרים לא בעייתיים; (ב) בחינת הסיכויים לזיהוי חוזר בכל אחד ממשרדי הממשלה תיעשה למעשה על ידי מומחה מתחום הטכנולוגיה והוא שייתן את הטון (בהתייעצות עם מומחה משפטי ומומחה לאבטחת מידע). החלטת הממשלה אינה מפרטת מתווה מלא לשיקולים שיש להתחשב בהם בבחינת הסיכויים לזיהוי חוזר ובכך היא מותירה למעשה את הבמה לדיון טכני בעיקרו. התוצאה תהיה שפקידי הממשל לא יהיו צד בהחלטה, ולכן שיקולים באשר לחשיבות הגשמתן של התכליות הדמוקרטית והכלכלית עלולים להיוותר מחוץ לדיון.

ולא זו אף זו: למעט חובות דיווח לוועדת ההיגוי אין בהחלטה כל אמצעי ענישה או כלי אחר בעל שיניים שיהיה בו כדי לתמרץ את המשרד הממשלתי לפעול לפרסום יזום של מאגרי המידע שברשותו. אמנם נקבע כי רשות התקשוב – בשיתוף עם מטה ישראל דיגיטלית, משרד המשפטים ומשרדי ממשלה רלוונטיים

114 ס' 12.ז.3, 12.ז.5 להחלטת ממשלה 1933, **שם**.

115 ס' 12.ז.1 להחלטת ממשלה 1933, **שם**.

אחרים – תבחן את האפשרות להטיל חובה כזו בחוק,[116] אולם נכון לעכשיו ההחלטה מעניקה למשרדי הממשלה מפלט מפני חובת הפרסום היזום על בסיס "שיקולים רלוונטיים אחרים"- חזרה אל הקרקע הנוחה של פרסום מוגבל, בהתאם להסדר הקבוע בחוק חופש המידע. גם ההנגשה באמצעים אחרים היא מצומצמת וניתנת לביטול על ידי המשרד הממשלתי, משום שהיא מותנית בכך שלא יונגש מידע מזהה, בכך שהתועלת לציבור עולה על העלות הכספית הכרוכה בהנגשה המוגבלת ובכך שאין מניעה מכוח דין או שיקולים רלוונטיים אחרים לפרסם את המידע במסגרת ההגבלות שיקבע המשרד הממשלתי.[117] כך המשרד הממשלתי יכול להימנע מהנגשת המידע לציבור תחת מעטה רחב ומעורפל של "שיקולים רלוונטיים אחרים".

בסופו של דבר, ההסדר שנקבע בהחלטת הממשלה אינו מלא ושלם בפני עצמו: הוא עמום, הוא מעניק עדיפות אפריורית לאנשי הטכנולוגיה על פני פקידי הציבור, והוא מאפשר התנערות ממנו בקלות רבה. עם זאת – בהיעדר עיגון בחוק – מעמדה המחייב של חובת הפרסום היזום הקבועה בהחלטת ממשלה 1933 מוטל בספק, בגלל סעיף 23ב לחוק הגנת הפרטיות האוסר על גוף ציבורי למסור מידע אלא אם "המידע פורסם לרבים או הועמד לעיון הרבים על פי סמכות כדין", וכן משום שהחלטת ממשלה אינה נחשבת "דין" כהגדרתו בחוק הפרשנות.[118]

116 ס' 6.ז.12 להחלטת ממשלה 1933, **שם**.

117 ס' 12.ו להחלטת ממשלה 1933, **שם**.

118 סעיף 23ב לחוק הגנת הפרטיות:

> 23ב. (א) מסירת מידע מאת גוף ציבורי אסורה, זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על סמכות כדין, או שהאדם שהמידע מתייחס אליו נתן הסכמתו למסירה.
>
> סעיף 3 לחוק הפרשנות, התשמ"א-1981:
>
> "דין" – כל אחד מאלה:
>
> (1) חיקוק;
>
> (2) דינים דתיים – בין שבעל פה ובין שבכתב – כפי תקפם במדינה;
>
> (3) (א) אקט של הפרלמנט הבריטי או דבר המלך במועצתו או חלק מהם, או תקנות לפיהם, ודיני המשפט המקובל ועקרוני היושר של אנגליה, כפי תקפם במדינה;
>
> (ב) דינים עותמאניים כפי תקפם במדינה.

2. המלצות

(א) הטלת חובה בחוק חופש המידע לפרסום יזום של מאגרי מידע ממשלתיים

כדי להאיץ ולעודד משרדי ממשלה לפעול לפרסום יזום של מאגרי מידע אנו מציעות להטיל חובה כזו בחוק חופש המידע. על פי המנגנון שבחוק זה אפשר יהיה לעתור לבית משפט נגד החלטת רשות ממשלתית שלא לפעול כאמור; כך תהיה החלטת הרשות חשופה לביקורת ציבורית.

החלטה לאפשר פרסום יזום של מאגרי מידע ממשלתיים עשויה להוביל לפגיעה בזכות לפרטיות. פגיעה כזו בזכות חוקתית מנוגדת, כאמור, לסעיף 23ב לחוק הגנת הפרטיות ואינה יכולה להתבסס על החלטת ממשלה, וגם מסיבה זו יש לעגנה בחוק. עיגון של חובת הפרסום היזום בחוק חופש המידע יעניק מקור חוקי לפגיעה יזומה בזכות לפרטיות ויעמיד אותה במבחנים החוקתיים לפגיעה בזכות לפרטיות.

לאור כל האמור אנו ממליצות לתקן את חוק חופש המידע ולהוסיף לו הגדרה של "מאגר מידע" וכן סעיף כדלקמן:

> "מאגר מידע" – מסד נתונים או סדרת נתונים של מידע מכל סוג, לרבות אוסף מובנה של נתונים, בין שהוגדר ברשות הציבורית כ"מאגר" לצרכים פנימיים ובין שלא.
> על פי המגבלות הקבועות בסעיף 9, על הממשלה ומשרדי הממשלה, לרבות יחידותיהם ויחידות הסמך שלהם, להעמיד לעיון הציבור כל מאגר מידע שברשותם באתר האינטרנט של המשרד.

עוד אנו מציעות לקבוע כי סעיף 13 לחוק חופש המידע[119] – שעניינו פנייה לצד שלישי במקרה של בקשת חופש מידע שכלולים בה פרטים שעלולים לפגוע בצד

119 זו לשון הסעיף:

> (א) נתבקש מידע הכולל פרטים על אודות צד שלישי, אשר מסירתם עלולה לפגוע בצד השלישי, והרשות הציבורית שוקלת לאפשר למבקש המידע לקבל את המידע, תודיע הרשות לצד השלישי, בכתב, על דבר הגשת

השלישי – לא יחול במקרה של פרסום יזום של מאגרי מידע ממשלתיים. פנייה למספר אדיר של צדדים שלישיים תכשיל את המטרה, הלוא היא הנגשת מאגרי המידע. ומעבר לכך, האיזונים שנציע להלן להגנה על הפרטיות יעניקו לאותם "צדדים שלישיים" הגנה מספקת ולכן מייתרים למעשה את הפנייה.

בשנתיים האחרונות עמלה היחידה לחופש המידע במשרד המשפטים, בליווי צוות מומחים, על הכנת נוסח לתקנות העמדת מידע יזום לציבור. התקנות כוללות, בין השאר, רשימת פריטי מידע ציבורי שיש להעמיד לרשות הציבור בלי שנדרשת לשם כך בקשת חופש מידע. הצעתנו משתלבת היטב גם בתקנות אלו, שככל שידוע לנו טרם אושרו על ידי משרד המשפטים.

(ב) הסמכת גוף אחד לביצוע מכלול הפעולות הקשורות ביישום ההחלטה

כאמור, על פי החלטת ממשלה מס' 1933, הקביעה אם יש סיכון לזיהוי חוזר תתקבל בנפרד בכל משרד ומשרד, על ידי מומחה מהתחום הטכנולוגי בליווי ייעוץ משפטי וייעוץ אבטחת מידע. לדעתנו, נוהל זה מעורר כמה חששות.

ראשית, הטלת האחריות לבחינת הסיכון לזיהוי חוזר על המשרד הממשלתי עצמו משמעה פיזור המומחיות בין משרדי הממשלה, ולכן היא עלולה לגרום פערי מומחיות. שנית, מדובר בנטל כספי נוסף – לגיוס המומחים הנדרשים, להקצאת כוח אדם ולזמן לבחינת הסיכון. נטל כספי נוסף זה עלול להרתיע משרדי ממשלה מלבחון לעומק כל מאגר שברשותם, בעיקר כשנתונה בידיהם דרך מילוט בדמות

הבקשה ועל זכותו להתנגד למסירת המידע ותודיע על כך למבקש; קיבל אדם הודעה כאמור, רשאי הוא להודיע לרשות, בתוך 21 ימים, כי הוא מתנגד לבקשה, בנימוק שאין למסור את המידע, כולו או מקצתו, מכוח הוראות סעיף 9 או הוראות כל דין; 21 הימים האמורים, לא יבואו במנין המועדים המנויים בסעיף 7.

(ב) החליטה הרשות הציבורית לדחות את התנגדותו של הצד השלישי, תמציא לו, בכתב, את החלטתה המנומקת, ותודיע לו על זכותו לעתור נגד החלטתה על פי חוק זה.

(ג) על אף האמור בסעיף 7(ב), לא תאפשר הרשות הציבורית את קבלת המידע המבוקש, בטרם חלפה התקופה להגשת העתירה או בטרם הוחלט לדחותה, לפי העניין, אלא אם כן הודיע הצד השלישי שהתנגד, בכתב, כי הוא מוותר על זכותו להגישה.

הקביעה שאין מקום לפרסום יזום של מאגר מסוים "משיקולים רלוונטיים", ולכן תותר הנגשתו רק במסגרת הקיימת – למשל, על פי חוק חופש המידע. שלישית, בהיעדר מסגרת ברורה למגוון השיקולים שיש לשקול בהערכת הסיכון לזיהוי חוזר, הקביעות שיתקבלו בסיום הליכי ההערכה יתבססו על שיקולים שונים בכל משרד ממשלתי או, לחלופין, יהיו טכניות ולא רחבות מספיק. רביעית, אם כל משרד ממשלתי יקבל לבדו את ההחלטה על אפשרות הסיכון לזיהוי חוזר, הוא עלול לקבל אותה בלי שיהיה מודע לקיומם של מאגרי מידע אחרים הנמצאים ברשות משרדים אחרים, העומדים לפני פרסום יזום ואשר תוכנם יכול להשפיע על האפשרות לזיהוי חוזר במאגר שהוא בוחן.

לפיכך אנו מציעות להעביר את סמכות ההחלטה בדבר סיכון לזיהוי חוזר לגוף אחד – למשל, רשות התקשוב הממשלתי. גוף זה ישתף בהחלטתו את כל הגורמים המנויים בהחלטה – פקידי ממשל מהמשרד הרלוונטי שיציגו את המידע שבמאגר, מומחה טכנולוגי, יועץ משפטי ויועץ אבטחת מידע. יתרונה של ההצעה באחידות שהיא מאפשרת. המדד לזיהוי חוזר ייקבע פעם אחת, על ידי גוף אחד ועל פי אותם קריטריונים, וכך תובטח מדיניות הנגשה אחידה בכל משרדי הממשלה. גוף אחד כאמור גם יוכל לבחון ממעוף הציפור את כלל מאגרי המידע העומדים לפני פרסום יזום ולהתחשב בכך – למשל, בבחינת הסוגיה של זיהוי חוזר. נוסף על כך יוסר העול התקציבי מכל אחד ממשרדי הממשלה ויועבר לגוף המרכזי שיתוקצב בנפרד. זאת ועוד: כאשר ההחלטה נתונה לגוף החיצוני למשרד ממשלתי מסוים, המתוקצב למטרה זו, גדולים הסיכויים שגוף זה יפעל לפרסום יזום של כמה שיותר מידע ולא יתפתה להימנע מהנגשת המידע בתואנה של "שיקולים רלוונטיים" מפאת חוסר זמן, חוסר תקציב, חשש מתביעות משפטיות עתידיות בגין פגיעה בפרטיות, היעדר ידע מקצועי הדרוש לקבלת החלטה מושכלת, היעדר חזון דיגיטלי למשרד ועוד.

הגוף האמור אף יהיה אחראי לביצוע כל הפעולות הנדרשות לפרסום יזום של מאגרי מידע ממשלתיים:

- לפקח על הפעולות שינקטו משרדי הממשלה ולהבטיח שכלל מאגרי המידע שאינם כוללים מידע מזוהה יפורסמו באופן יזום;
- לשמש גורם מייעץ למשרדי הממשלה בכל שאלה הנוגעת לחובת הפרסום היזום;

- לקבוע, לאחר היוועצות בגורמים המתאימים מהאקדמיה והתעשייה, כללי אצבע למיפוי מהיר של מאגרי המידע שאינם כוללים מידע מזהה;
- לקבוע כללים מנחים ליישום טכניקות של התממה;
- לקבוע כללים מנחים לבדיקת הסיכון לזיהוי חוזר ולבחינת הצורך בפרסום מוגבל על בסיס מבחן המידתיות המקובל כיום בביקורת שיפוטית על החלטת רשות מינהלית.

מטבע הדברים, להסמכה של גוף אחד למגוון התפקידים הקשורים בהבטחת פרסום יזום של מאגרי מידע ממשלתיים, כמוצע לעיל, יש חסרונות משלה. העברת ההחלטה לגוף חיצוני עלולה להיתפס כהתערבות של גוף חיצוני בהחלטות שבתחום סמכותו של המשרד הממשלתי ולעורר התנגדות מצד המשרד. נוסף על כך ייתכן עיכוב בקבלת ההחלטות עקב עומס שיצטבר בגוף המרכזי. לדעתנו, השפעתם של חסרונות אלו ניתנת לצמצום באמצעות שיתוף פעולה מלא ואמיתי עם המשרדים, יצירת מנגנון מסודר ומאובטח להעברת מידע וקביעת מועדים ברורים להתכנסות של מקבלי ההחלטות הרלוונטיים מהגוף החיצוני (ובכלל זה המומחה הטכנולוגי, היועץ משפט והיועץ לאבטחת מידע) ונציג המשרד הממשלתי הרלוונטי.[120]

ריכוז הטיפול במכלול הנושאים הקשורים בפרסום יזום של מאגרי מידע ממשלתיים נעשה גם במדינות אחרות. בגרמניה הוסמך משרד הפנים לרכז בידיו את מכלול הפעולות הקשורות בשיתוף הפעולה בין משרדי הממשלה השונים לשם פרסום יזום של המידע שבידיהם ולפעול לגיבוש מתווה אחיד לכלל הפעולות שעל כל משרד ממשלתי לבצע על מנת להביא לפרסום יזום של מאגרי המידע שברשותו, לרבות אימוץ סטנדרטים טכנולוגיים זהים שיאפשרו הנגשה

120 התלבטנו רבות בסוגיית הסמכתו של גוף מרכזי. ידוע לנו שהעמדה של רשות התקשוב הממשלתי שונה מעמדתנו. לשיטתם, אין להטיל סמכות כאמור על גוף מרכזי אחד ויש לשמר את המצב הקיים, שבו רשות התקשוב משמשת גוף מרכזי מנחה ומסייע בלבד בסוגיית הפרסום היזום ומותירה את ההכרעה למשרד הממשלתי הרלוונטי, שהוא הגורם האחראי לניהול של מאגר המידע הממשלתי ולכן אמור להחזיק בסמכות ההכרעה בשאלת פרסומו. עם זאת, מהטעמים שפורטו בגוף המסמך, אנו איתנות בדעתנו שנכון וצריך להסמיך בישראל גוף מרכזי כאמור.

אחידה של כלל המידע הממשלתי באופן יזום גם בעתיד.[121] כמו כן נמצאת בתהליכי גיבוש תכנית מדיניות להקמת רשות מידע פתוח (באנגלית: Federal Open Data Bureau), אשר תשמש גורם מנחה ומייעץ לציבור ולמגזר העסקי בכל הקשור להנגשת מידע.[122]

בטייוואן, המדורגת מאז 2015 כמדינה הראשונה בעולם ברמת הממשל הפתוח שלה,[123] מונתה באוקטובר 2016 מומחית בתחום הטכנולוגיה לתפקיד השרה לעניינים דיגיטליים. השרה החדשה אחראית, בין השאר, ליישום המדיניות הממשלתית לפרסום יזום של מאגרי מידע ממשלתיים.[124] גם בבריטניה, המדורגת שנייה בעולם ברמת הממשל הפתוח שלה[125] משמש השירות הדיגיטלי הממשלתי (Government Digital Service) האחראי ליישום מדיניות הממשל הפתוח במדינה, לקביעת סטנדרטים מנחים ולייעוץ למשרדי הממשלה האחרים בין השאר בנושא יישום מדיניות הממשל הפתוח.[126]

(ג) קביעת כללי אצבע לסיווג מידע ולמיפוי מהיר של מאגרי מידע שאינם כוללים מידע מזהה

בדיקה פרטנית של כל מאגר ומאגר על ידי המשרד הממשלתי תהיה אטית ולא יעילה, ולכן יש לנסות ולהגדיר כללי אצבע שיאפשרו למשרד הממשלתי לקבוע במהירות וביעילות יחסיות, כבר בעת מיפוי מאגרי המידע שברשותו, מהם מאגרי המידע שפרסומם היזום אינו מעורר חשש לפגיעה בפרטיות.

121 Federal Ministry of the Interior, *Digital Administration 2020: The Federal Government's National Action Plan to Implement the G8 Open Data Charter* (November 2014)

122 Daniel Delhaes & John Blau, *Germany Opens to Open Data*, Handelsblatt Global (July 7, 2016)

123 Ralph Jennings, *How Taiwan Fostered the World's Most Open Government*, Forbes (December 15, 2015); ובאתר **Global Open Data Index**.

124 Yoon Sung-won, *Taiwanese Digital Minister Sresses Open Government*, The Korea Times (April 12, 2014)

125 באתר **Global Open Data Index**.

126 HM Government, *UK Open Government National Action Plan 2016 18* (May 2016)

אנו מציעות כי כללי האצבע יגדירו רשימה סגורה (שאפשר לעדכנה מעת לעת) של סוגי מידע המתאימים לפרסום יזום בלא חשש לפגיעה בפרטיות. ברשימה זו אפשר לכלול (למשל):

- מבנה המשרד הממשלתי, הפעולות והמשימות שבתחום אחריותו;
- דוחות תקציב שנתיים;
- רשימת החוזים, ההתקשרויות והמכרזים שהמשרד הממשלתי חתם עליהם או פרסם אותם;
- החלטות מינהלית והחלטות מדיניות שהתקבלו במשרד הממשלתי;
- מידע מבוקש בשכיחות גבוהה על פי חוק חופש המידע;
- מידע גאו־ספאטיאלי;
- זמני הגעה של תחבורה ציבורית – ביבשה, באוויר ובים.

חלק ניכר מפריטים אלה מופיעים בטיוטה של תקנות העמדת מידע יזום לציבור, שעליהן עמלה בשנתיים האחרונות היחידה לחופש מידע במשרד המשפטים ואשר ככל הידוע לנו טרם אושרו.

היתרון שבהגדרת רשימה של סוגי מידע המתאימים לפרסום יזום הוא שחרור מהיר יחסית של מידע לפרסום יזום. מנגד, חסרונה נובע מחוסר גמישות וחוסר התאמה לשינויים טכנולוגיים וחברתיים, ולכן מוצע לעדכן אותה מעת לעת.

עוד אנו מציעות לקבוע רשימה של סוגי מידע שאינם מתאימים בכלל לפרסום יזום. כוונתנו למידע רגיש כהגדרתו בתקנות האירופיות או למידע מזהה כהגדרתו בחוק הפרטיות האוסטרלי: שם פרטי, שם משפחה, שם קודם, כתובת מגורים ושתי כתובות קודמות, מספר זהות, תאריך לידה, מגדר, מספר רישיון נהיגה, מקום עבודה נוכחי או מקום עבודה אחרון ידוע, מצב בריאותי, נטייה מינית, מוצא אתני, גזע, דעות פוליטיות, אמונה דתית או פילוסופית, חברות בארגון עובדים, מידע גנטי, מידע ביומטרי.[127]

127 סעיף 6 לחוק הפרטיות האוסטרלי:

The Privacy Act 1988 (Australia), sec. 6:
Identification information about an individual means: (a) the individual's full name; or (b) an alias or previous name of the individual; or (c) the

הדרך המוצעת תאפשר, כבר בשלב הראשוני, להתמקד בשתי שאלות חשובות: השאלה הראשונה היא אם בכל זאת אפשר, באמצעות התממה, לפרסם מאגרי מידע שיש בהם מידע מזהה הכלול ברשימה של סוגי המידע שאינם ניתנים לפרסום; השאלה השנייה מתמקדת במאגרי המידע הנותרים – אלו שאינם מתאימים לפרסום יזום מיידי וללא חשש וגם אינם כוללים מידע רגיש כהגדרתו ברשימה – ובודקת את הסיכון לזיהוי חוזר.

חסרונה של שיטה זו הוא, במידה מסוימת, חוסר היעילות שבה, משום שהיא מותירה על כנו את הצורך לבחון פרטנית את יעילות ההתממה ואת הסיכון לזיהוי חוזר בכל מאגרי המידע הנותרים. לפיכך אנו מציעות לקבוע גם כללים מנחים להתממה ולזיהוי חוזר.

(ד) קביעה ואימוץ כללים מנחים להתממה ולזיהוי חוזר

בדומה לכללים המנחים שפרסם נציב הפרטיות בבריטניה, אנו מציעות לקבוע ולפרסם כללים מנחים שיסייעו למשרדי הממשלה, כמו גם לארגונים פרטיים, להבין באילו שיקולים עליהם להתחשב כדי ליישם טכניקות התממה יעילות ואפקטיביות. את הכללים יגבש הגוף שיוסמך ליישום ההחלטה, בשיתוף פעולה עם הרשות למשפט טכנולוגיה ומידע במשרד המשפטים (רמו"ט) ועם רשות התקשוב הממשלתי. הנחיות ההתממה צריכות לכלול, בין השאר, הגדרות והסברים ברורים לנושאים המפורטים להלן:

---

individual's date of birth; or (d) the individual's sex; or (e) the individual's current or last known address, and 2 previous addresses (if any); or (f) the name of the individual's current or last known employer; or (g) if the individual holds a driver's licence—the individual's driver's licence number.

סעיף 9(1) ל־GDPR:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(1) מהם מידע אישי, הדרכים לזיהויו, הנסיבות שבהן נדרשת התממה והנסיבות שמותר לפרסם בהן מידע אנונימי.

(2) מהן טכניקות התממה ומתי מתאים ליישם אותן. טכניקות ההתממה העיקריות הקיימות כיום הן טכניקות ממשפחת הרנדומיזציה וממשפחת ההכללה. טכניקות ממשפחת הרנדומיזציה מתמקדות בשינוי המהימנות והדיוק של המידע, ומטרתן להעלים את הקשר שבין המידע האישי לבין האדם המסוים. למשל, טכניקה של "הוספת רעש" מוסיפה למאגר המידע המקורי נתונים שאינם חלק ממנו. טכניקות ממשפחת ההכללה מתמקדות ב"דילול" המידע האישי באמצעות שינוי קנה המידה הרלוונטי או סדר החשיבות. לדוגמה, במאגר מידע שיש בו נתונים על מקום היישוב שבו מתגורר אדם מסוים אפשר להסתפק בציון האזור בארץ.

מאחר שטכניקות ההתממה עשויות להשתנות בהתאם למחקר ולהתפתחויות הטכנולוגיות התמידיות בתחום, אנו מציעות שפעם בשלוש שנים יבדוק הגוף המרכזי – אגב היוועצות במומחים מתחומי הטכנולוגיה, אבטחת המידע והמשפט – את טכניקות ההתממה הקיימות באותה עת ואת זמינותן. חשוב לומר שגם אם יחול שינוי בטכניקות ההתממה המקובלות ובקביעת אלו שיש ליישם, הקביעה תחול רק על מקרים בעתיד ולא על מידע שכבר פורסם באופן יזום.

(3) מהם הסיכונים הפוטנציאליים בפרסום מידע לאחר התממה. בשנים האחרונות גוברת ההבנה שאין באמת התממה מושלמת; ולכן יש להעריך מחדש את חוק הגנת הפרטיות, המניח שדי בהתממה כדי למזער את הפגיעה האפשרית בזכות לפרטיות.

(ה) קביעת מתווה למרחב השיקולים הרלוונטיים לאיזון בין אינטרסים מתנגשים

חשוב להגדיר מפורשות את מרחב השיקולים הרלוונטיים בהחלטה על ההיקף והאופן שבו יונגשו לציבור מאגרי מידע ממשלתיים. הגדרה כזו תאפשר למשרדי הממשלה לשקול את הסיכונים לפגיעה בפרטיות מחד גיסא, ומאידך גיסא תמנע

מהם את האפשרות להסתתר מאחורי מעטה עמום של "שיקולים רלוונטיים" כפי שנקבע בהחלטת הממשלה ובדוח הצוות הבין־משרדי.[128]

אנו מציעות לאמץ מבחן מידתיות לקביעת ההיקף והדרך של הנגשת מאגרי מידע ממשלתיים לציבור. יישום המבחן לא הכרחי בכל מקרה ומקרה, שכן לפעמים יישום של טכניקות התממה יוביל למסקנה שאין סיכון לזיהוי חוזר. עם זאת, מאחר שהיכולות לכרות מידע ולעבד אותו משתנות ומשתכללות תדיר, אפשר שבעוד שנים מספר טכניקות ההתממה של היום לא יספיקו, ויגדל הסיכון לזיהוי חוזר. באיחוד האירופי התמודדו עם חשש זה וקבעו כי בשלב הנוכחי יש ליישם בעת ובעונה אחת טכניקות התממה אחדות, כדי שהסיכון לזיהוי חוזר יהיה חלש. בד בבד נקבע כי יש לשוב ולבחון את הסיכון האמור מדי כמה שנים, על פי ההתפתחויות הטכנולוגיות בתחום.[129]

כפי שציינו, יעילות הבחינה מחדש של הסיכונים לזכות לפרטיות מוטלת בספק לאחר פרסומו הראשוני של המידע, בעיקר משום שאין דרך לשלוט בשימוש שיעשו בו צדדים שלישיים. לפיכך אנו ממליצות לאמץ עמדה הרואה בסיכון לזיהוי חוזר סיכון אינהרנטי לכל טכניקת התממה. העמדה המוצעת מתמקדת בניסיון למזער ככל האפשר את היקף הפגיעה בזכות לפרטיות באמצעות החלת מבחן המידתיות בכל מקרה של פרסום יזום של מאגר מידע ממשלתי המכיל מידע מזהה או שיכול להיות מזהה בשילוב עם מידע אחר.

אף שרשות התקשוב ומטה ישראל דיגיטלית הציעו אמת מידה של סבירות ולא של מידתיות, אנו סבורות כי מבחן של סבירות מתאים בעיקר לאיזון בין אינטרסים חברתיים או בין זכויות. לעומתו, מבחן של מידתיות הולם מצבים שבהם החלטת הרשות המינהלית פוגעת בזכות אדם, ואז נדרש לאזן בין הזכות הנפגעת לבין האינטרס הציבורי. מבחן המידתיות מתמקד ספציפית באיזון בין המטרה לבין האמצעי המשמש להשגתה ובוחן אם אמצעי זה מתאים למטרה או שיש חלופות אחרות ופוגעניות פחות, בהתאם לחשיבות היחסית של המטרה. מבחן המידתיות מתאים לענייננו גם בגלל אימוצו בחוק־יסוד: כבוד האדם וחירותו וחוק־יסוד: חופש העיסוק. נציין כי גם במתווה שהוצע בדוח הצוות

128 ראו הדיון **לעיל** בסעיף ו.1.

129 *Opinion 05/2014 on Anonymisation Techniques*, **לעיל** ה"ש 57.

הבין־משרדי ובהחלטת הממשלה יש רכיבים מסוימים של מידתיות, אם כי אלה אינם מפורטים וברורים דיים.[130]

אנו ממליצות לפעול כדלקמן:

1. תחילה יש לאמוד את הנזק הפוטנציאלי לזכות לפרטיות בעקבות פרסום יזום של מידע הכרוך בסיכון לזיהוי חוזר.[131]
2. לאחר מכן יש לקבוע את מטרת ההנגשה ואת חשיבותה ליישום התכליות הדמוקרטית והכלכלית:

(i) בהיבט הדמוקרטי יש לבדוק אם הפרסום היזום יוסיף על הידע הקיים בנוגע לפועלן של רשויות השלטון (עקרון השקיפות) או יעורר דיון חשוב בעניינן (הזכות למידע כנגזרת של חופש הביטוי).

(ii) בהיבט הכלכלי יש לבדוק אם הפרסום היזום יעודד חדשנות, התייעלות כלכלית או אינטרס ציבורי אחר (למשל, קידום בריאות הציבור).

3. משנקבעו מידת הפגיעה בפרטיות עקב הפרסום היזום, מחד גיסא, ומידת התועלת הציבורית (הדמוקרטית או הכלכלית) שבו, מאידך גיסא, יש ליישם את מבחן המידתיות באמצעות שלושה מבחני משנה:

(i) **מבחן האמצעי המתאים** לבדיקת הרציונליות של ההחלטה המינהלית – האם האמצעי שבחרה הרשות מתאים וראוי להשגת התכלית, הן מבחינה

130 אמנם מבחן המידתיות משמש לרוב לביקורת שיפוטית על החלטות מינהליות ולא כבסיס להבניה או נימוק של החלטות מינהליות. ובכל זאת יש לדעתנו לאמץ אותו כאן משתי סיבות: ראשית, משום שמדובר באיזון בין זכות חוקתית לאינטרס אחר (או אפילו בין זכויות חוקתיות) ולא באיזון בין אינטרסים שונים, שאז אכן מתאים יותר מבחן של סבירות. שנית, משום שזהו המבחן המקובל לאיזון בין הזכות לפרטיות לפרסום יזום של מאגרי מידע ממשלתיים במדינות נוספות בעולם, כמו למשל במדינות האיחוד האירופי, והתאמה זו תמנע חיכוכים מתחום המשפט הבינלאומי בעתיד.

131 ברור לנו כי אין מדובר באומדן כמותי או מדעי מדויק, אולם כך נעשה גם בהקשרים אחרים של מבחני המידתיות במשפט החוקתי והמינהלי. להרחבה ראו דפנה ברק ארז **המשפט המנהלי ב** 771 ואילך (2010).

לוגית והן מבחינה ערכית? ובמקרה שלנו: האם פרסום יזום הוא יעיל וראוי להשגת התכלית הדמוקרטית והתכלית הכלכלית?

(ii) **מבחן האמצעי שפגיעתו פחותה** בהשוואה לחלופות שעמדו לפני הרשות ושעלותן דומה – למשל, כאשר רמת הפשיעה בעיר מתגברת בשעות החשכה, הטלת עוצר על כל תושבי העיר במשך כל שעות החשכה אינה "האמצעי שפגיעתו פחותה" משום פגיעתו הגורפת בזכות לחופש תנועה. במקרה שלנו: האם פרסום יזום הוא החלופה שפגיעתה בפרטיות פחותה מכל שאר החלופות להשגת התכלית הדמוקרטית והתכלית הכלכלית?

(iii) **מבחן האמצעי המידתי** – גם אם האמצעי שבחרה הרשות מתאים וגם אם פגיעתו פחותה, עדיין יש לבחון אם הפגיעה הצפויה בזכות האדם עקב החלטת הרשות עומדת ביחס סביר לתועלת הצפויה ממנה. מדובר בהכרעה נורמטיבית, הבוחנת אם המטרה שהרשות מבקשת להשיג חשובה דיה כדי להצדיק את הפגיעה האמורה. למשל – איסור על נסיעה בלילה עשוי להפחית במידה ניכרת את מספר תאונת הדרכים במדינה, הוא מתאים להשגת המטרה, וייתכן גם שפגיעתו בזכויות האדם היא הפחותה. אף על פי כן מדובר בפגיעה בלתי־סבירה בחופש התנועה ובזכויות יסוד אחרות.[132]

במקרה שלנו: ככל שהנזק לזכות לפרטיות עקב הפרסום היזום גדול יותר, כך יש להקפיד ולבדוק את תכלית הפרסום. כאשר מדובר בהנגשת מידע לשם תכלית כלכלית טהורה (למשל, הגדלת רווח כלכלי של חברה פרטית שמשתמשת במידע כדי לשפר את טכניקת השיווק של מוצריה), אפשר לטעון בזכות הגבלה גדולה יותר של פרסום יזום; מאידך גיסא, כאשר מדובר בהנגשת מידע לתכלית דמוקרטית, יש לשאוף לפרסם ולהנגיש את המידע ככל האפשר. ייתכנו מקרי ביניים – תכליות ציבוריות כמו קידום בריאות הציבור או בטיחות בדרכים. גם במקרים אלה אמצעי אבטחת המידע צריכים להיבחר בהתאם. את ההחלטה באשר לאיזון הראוי יקבל הגוף המרכזי הבוחן את הסיכון לזיהוי חוזר.

132 **שם**, בעמ' 771–792.

(ו) בניית מאגרי מידע חדשים

מוצע להתוות מסגרת לבניית מאגרי מידע ממשלתיים חדשים באופן שיאפשר הן פרסום יזום מהיר של מאגרי מידע שאין בהם מידע מזהה והן בחינה קלה ומהירה של האפשרות להנגשה מוגבלת של מאגרי מידע שיש בהם מידע מזהה. הטמעת התכנית תאפשר בעתיד למשרדי הממשלה לפעול עצמאית לפרסום יזום (עם או בלי הגבלות) על פי המסגרת שהוצעה לעיל ועל פי כללים מנחים מטעם הגוף המרכזי ופנייה אליו רק במקרים שהמשרד הממשלתי מתקשה לתת להם מענה.

בגרמניה, למשל, הומלץ כי מלכתחילה יישמרו במאגרי המידע הממשלתיים פרטים אישיים ופרטי מידע רגיש בנפרד משאר פרטי המידע, וכך הנגשת המאגרים ללא פרטים אלו תהיה קלה יותר לביצוע.[133] המלצה זו תואמת גם את לשון חוק הפרטיות במידע הגרמני, המחייב כל מחזיק במידע אישי, בין שהוא חברה פרטית ובין שהוא גוף ציבורי, לשמור את המידע בנפרד מפרטי מידע אחרים שנמצאים במאגרי מידע.[134]

אנו ממליצות שכל משרד ממשלתי המבקש להקים מאגר מידע חדש יקבע – כבר בתחילת הדרך – שפרטי מידע אישיים יוחזקו בנפרד, ברמת אבטחת מידע מחמירה יותר או במסגרת המאפשרת להסירם במהירות. פרטי מידע כאלה הם, למשל, שם, מספר זהות, תאריך לידה, פרטי בעלות בנכס או בכלי רכב, כתובת מגורים, פרטי יצירת קשר, מצב משפחתי, חוקיות הילדים, זהות אבי הילדים, מצב רפואי, תשלומי סעד, צריכת אלכוהול, השתייכות דתית, רישום פלילי, שהייה בבתי כלא במדינות אחרות, זהות של נפגעי עברה, מצב כלכלי, גזע, מוצא אתני, דעות פוליטיות, נטייה מינית, מידע גנטי, מידע ביומטרי. רשימת פרטי המידע האישיים תיקבע ותעודכן מעת לעת על ידי הגוף המרכזי, האחראי לבחינת הסיכון לזיהוי חוזר ולקביעת ההגבלות על פרסום במקרה של מידע מזהה שאינו ניתן להתממה.

133 Federal Ministry of the Interior, *Short Version of the Study on Open Government in Germany* 22 (July 2012)

134 Federal Data Protection Act, published on December 20, 1990 (BGBl.I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325), §27, §40

ז. סיכום

במסמך זה עסקנו בהחלטת ממשלת ישראל להטיל על משרדי הממשלה חובת פרסום יזום של מאגרי המידע שברשותם כברירת מחדל. עמדנו על כך שיש לפרסום יזום שתי תכליות – דמוקרטית וכלכלית – והסברנו כי ההחלטה מטילה על כל משרד ממשלתי לקבוע מדיניות להבטחת הזכות לפרטיות בצד החובה לפרסום יזום. ללא מתווה מלא וברור, נטל זה מסכן את יישומה של ההחלטה.

הצגנו את החשיבות וההכרח שביצירת מתווה ברור ומעשי ככל האפשר, כדי לאפשר פרסום יזום של מאגרי מידע ממשלתיים בלי לוותר על ההגנה על הזכות לפרטיות. סקרנו את דרכי הפעולה במדינות אחרות בעולם, במסגרת המגמה הכלל־עולמית של ממשל פתוח.

אלה המלצותינו בקצרה:

1. מומלץ לתקן את חוק חופש המידע ולהוסיף לו חובת פרסום יזום של מאגרי מידע ממשלתיים. חובה זו תהיה כפופה לביקורת ציבורית באמצעות המנגנונים הקבועים בחוק חופש המידע, כמו גם לכללים לבחינת החוקיות של פגיעה אפשרית בזכות החוקתית לפרטיות עקב הפרסום היזום האמור.
2. מומלץ לקבוע כללי אצבע לסיווג המידע ולמיפוי מהיר של מאגרי מידע שאינם כוללים מידע מזהה ולכן מתאימים לפרסום יזום מהיר. כללים אלה יכללו רשימה סגורה, שתעודכן מעת לעת, של סוגי המידע המתאימים לפרסום יזום בלא חשש לפגיעה בפרטיות.
3. מומלץ לקבוע כללים מנחים להתממה ולזיהוי חוזר: מתי נדרשת התממה, אילו טכניקות התממה קיימות וכיצד ליישמן, ואילו סיכונים כרוכים בפרסום יזום לאחר התממה. יש להדגיש בתוך כך שהתממה אינה פתרון קסם מוחלט ומושלם.
4. מומלץ לקבוע מתווה המבוסס על מבחן המידתיות לבחינת האפשרות לפרסום יזום של מאגרי מידע ממשלתיים, עם או בלי הגבלות.

5. מומלץ להסמיך את רשות התקשוב הממשלתי, או גוף אחר, לשמש גוף מרכזי ייעודי לבחינת סוגיות הנוגעות לפרסום יזום, למשל: עדכון פרטי המידע שאינם מתאימים לפרסום יזום; בחינה של מידתיות הפרסום היזום או של ההגבלות שנקבעו לו; הערכת הסיכון לזיהוי חוזר.
6. ולבסוף, מתוך ראייה צופה פני עתיד ומתוך רצון לחזק ולהטמיע את ההכרח הדמוקרטי ואת הרצון הציבורי בממשל פתוח, כפי שהם באו לידי ביטוי בהחלטת הממשלה – מומלץ לגבש כללים מנחים לבניית מאגרי מידע מעתה ואילך באופן שיקל את סיווגם ואת הפרסום היזום והמהיר שלהם, עם או בלי הגבלות.

אנו סבורות כי המלצותינו יסייעו למקבלי ההחלטות בישראל לקדם, ביעילות ובאפקטיביות, את יישומה המעשי של מדיניות הפרסום היזום של מאגרי מידע ממשלתיים.

רחל ארידור־הרשקוביץ היא חוקרת בתכנית "דמוקרטיה בעידן המידע" שבמרכז לערכים ולמוסדות דמוקרטיים במכון הישראלי לדמוקרטיה. בעלת תואר ראשון ושני במשפטים. עתידה להשלים בקרוב את עבודת הדוקטור שלה באוניברסיטת חיפה בנושא מסגרות לשיתופי פעולה בין הממשל לתעשייה לשם הגברת הגנת המרחב הקיברנטי.

ד"ר תהילה שוורץ אלטשולר היא מנהלת המרכז לערכים ולמוסדות דמוקרטיים במכון הישראלי לדמוקרטיה ועומדת במסגרתו בראש התכנית "דמוקרטיה בעידן המידע". מלמדת בבית הספר למדיניות ציבורית באוניברסיטה העברית בירושלים ומשמשת נציגת ציבור בנשיאות מועצת העיתונות. מומחית לאסדרת תקשורת ולממשק שבין טכנולוגיה, משפט ומדיניות.

מסת"ב: 978-965-519-206-3
www.idi.org.il

המכון הישראלי לדמוקרטיה