



3

הגנה על הפרטיות בעיר הדיגיטלית

מיכאל בירנהק

מיכאל בירנהק, "הגנה על הפרטיות בעיר הדיגיטלית", מתוך העיר בעידן הדיגיטלי: תכנון, טכנולוגיה, פרטיות ואי שוויון. עורכת שלי חתוקה, אוניברסיטת תל אביב, 2018, עמ' 56-85.

הגנה על הפרטיות בעיר הדיגיטלית

מיכאל בירנהק

"כשאתה מתחיל להזין תעודות זהות ומספרי טלפונים ומספרי רכב, זו כבר פרטיות שצריך להגן עליה, בוודאי. וכשזה עובר לחברה צד ג' אתה צריך לוודא שקודם כול הם לא מעבירים את החומר לעוד גורם אחר, שהם מגינים עליו כמו שצריך".¹

"אנחנו פשוט חיים בעידן שאין בו פרטיות אז צריך להבין את זה. הקטע של פרטיות בעיניי נגמר לחלוטין [...] היה פה דיון ראשון פעם על הצבת מצלמות בעיר, שכולם אמרו [זהו] סוף עידן הפרטיות שאני הולך ברחוב ותצלם אותי מצלמה. אמרתי נכון, סוף עידן הפרטיות. אני מעדיף, אבל זה גם סוף עידן הכפר".²

לתהליך העיור שמור מקום של כבוד – גם אם שנוי במחלוקת – בעלייתה של הזכות לפרטיות במאה התשע עשרה בחברה המערבית. כל עוד חיו בני אדם ביישובים קטנים – כפרים, עיירות וערים קטנות – הייתה להם רק מעט פרטיות מול שכניהם. הישוב הקטן מאופיין ברמת היכרות גבוהה ובזרימת מידע אינטנסיבית בין התושבים, ולכן היכולת של אדם "להיעזב במנוחה", כביטויים של סמואל וורן ולואיס ברנדייס, היא מצומצמת. המעבר לעיר הגדולה הביא לריחוק ולניכור בין התושבים. הסוציולוג גאורג זימל מדגיש בכתיבתו את הפיקוח ההדדי שהיה בין האזרחים בעיר הקטנה.³ את השינוי הזה – מהיכרות אינטימית כמעט של השכנים בישוב הקטן לניכור העירוני – אפשר להעלות על נס; זימל מדגיש, "השפעתם של ההסתייגות ושל שוויון הנפש ההדדיים, שהם תנאי החיים הרוחניים של המעגל הגדול, אינה ניכרת בשום מקום מבחינת עצמאות הפרט, כפי שהיא ניכרת היטב בהמולה הצפופה של העיר הגדולה; כל זאת מכיוון שדווקא הקרבה הגופנית והצפיפות מבליטות ביתר שאת את המרחק הרוחני".⁴ במילים אחרות, היעדר ההיכרות בין האנשים מאפשר חירות לכל פרט. מנגד, אחרים מדגישים שהאנונימיות שיש בעיר הגדולה גורמת לריחוק בין בני אדם. רם כרמי למשל כותב, ש"הוויית המטרופולין, שזה עתה התחילה להשתלט עלינו, מקרינה תחושת בדידות גדולה. מן האנונימיות השורה עליה ומתחושת הזרות החמורה למדי עולה ריחוק חדש ביחסי הגומלין בין הדמויות לבין סביבתן או בין המרחב הפרטי לבין המרחב הציבורי. ריחוק זה מערער את האינטימי שבממד הציבורי ואת השלווה שבממד הפרטי בעת ובעונה אחת".⁵

3 גאורג זימל, "העיר הגדולה וחיי הנפש", בתוך אורבניזם: הסוציולוגיה של העיר המודרנית, מתרגמת: מרים קראוס, עורך: עודד מנדהילוי (תל-אביב: רסלינג, סדרת ליבידו, 2004), 23-40. שם, 34.
4 רם כרמי, "הבית המשותף – לאן? כמה הרהורים על תרבות של פרטיות", בתוך קהילות מאודרות, עורך: אמנון להבי (שריגים-ליאון: נבו, 2010), 83-114.

1 יוסי בן סימון (מנמ"ר, עיריית אשדוד), 25.9.2016.
2 אסף זמיר (סגן ראש עיריית תל-אביב), 7.8.2016.

האנונימיות מזה והניכור מזה שבאו עם המעבר לערים, הביאו עימם גם צרכים שלטוניים חדשים של פיקוח. לא היה אפשר להסתפק בהיכרות האישית שבין ראש הכפר לתושבי הכפר – כלומר בין השלטון לאזרחים – או בין השלטון לאנשים מתוך הכפר שיכלו לספק לשלטון מידע אמין. בהתאם, גם הביורוקרטיה השלטונית הייתה צריכה להתאים את עצמה למצב החדש.⁶ התוצאה היא, שבד בבד עם יצירת האפשרות החדשה לפרטיות בעיר באה גם תגובה של הגברת הבקרה, השליטה והמעקב מצד השלטון, שמשמעותם היא צמצום הפרטיות. כך אפשר לראות שבין השלטון לבין תושבי העיר מתנהל משא ומתן נמשך על גבולות הפרטיות. ובהכללה, בין העיר לבין הפרטיות יש יחסים מורכבים ודינמיים – תלות מצד אחד, ומאבק מצד אחר; הפרטיות זקוקה לעיר, והעיר זקוקה לפרטיות ובו־זמנית להגבלת הפרטיות.

כיום העיר בעידן הדיגיטלי היא פרק נוסף בדיאלוג הנמשך הזה. כניסתן של טכנולוגיות חדשות מאפשרת איסוף של סוגי מידע נוספים שלא היה אפשר לאסוף קודם, את ההצלבה של המידע עם מקורות מידע אחרים בתוך העיר או מחוצה לה, את עיבוד המידע לשם זיהוי מגמות כלליות ולשם יצירת פרופילים אישיים של תושבים ואת העברת המידע על התושבים לגורמים אחרים בתוך המנהל העירוני או מחוצה לו – לשחקנים בשוק או לגורמי שלטון אחרים.

6 Kevin D. Haggerty & Richard V. Ericson, "The New Politics of Surveillance and Visibility", in *The New Politics of Surveillance and Visibility*, eds. Kevin D. Haggerty & Richard V. Ericson, 3-25 (Toronto, Canada: University of Toronto Press, 2006)

בין השלטון לבין תושבי העיר מתנהל משא ומתן נמשך על גבולות הפרטיות. בין העיר לבין הפרטיות יש תלות מצד אחד ומאבק מצד אחר



פרק זה בוחן את היבטי הפרטיות המתעוררים כאשר הערים שלנו הופכות ל"חכמות", מתוך כוונה לזהות את האתגרים ולהציע פתרונות. החלק הראשון מציג בתמציתיות את המסגרת הכללית של הזכות לפרטיות, את משמעותה ואת היקפה, ואת המישורים השונים שבו היא פועלת – ביחסי המדינה והאזרח, ביחסי השוק והצרכן ובין אזרחים לבין עצמם. מוצגת המסגרת המשפטית הכללית של הזכות לפרטיות, על השינויים שמתחוללים בה בעת הזו. החלק השני מתכנס לסוגיה של הפרטיות בעיר בעידן הדיגיטלי. המצבים המתעוררים בעיר העכשווית מדגישים את השילוב – או הקריסה – של המישורים הנפרדים האלה זה לתוך זה, כאשר המידע שנאסף על התושבים יכול לעבור מגורמים שלטוניים לגורמים פרטיים, בתוך העיר או מחוצה לה. מוצגים סוגי השאלות המתעוררות, והן מומחשות בכמה הקשרים כמו תשתיות דיגיטליות, מצלמות אבטחה או מעקב, כרטיסי תושב, רשתות אינטרנט אלחוטי ועוד. החלק השלישי מציג ומנתח ממצאים מן הראיונות שנערכו עם גורמים ברשויות מקומיות שונות בישראל, עם נציגי השלטון המרכזי ועם יועצים פרטיים שונים. החלק הרביעי מוקדש להמלצות שונות לניהול הפרטיות של התושבים בעיר העכשווית.

מושגי יסוד: פרטיות והגנת מידע אישי

אפשר לאסוף מידע דיגיטלי בקלות, ומידע שכזה נוצר כיום כחלק בלתי־נפרד מכל פעולה כמעט שאנו מבצעים – תנועה במרחב, פעילות פיננסית, מסחרית, רפואית, תקשורת בין־אישית ועוד. זהו השובל הדיגיטלי שלנו. נוכח הבשלות הטכנולוגית וירידת המחיר של אמצעי האיסוף והעיבוד עסקיים, שלטוניים ופרטיים של המידע מודגשים צרכים במידע.

הפרטיות היא בוזמנית נורמה חברתית וזכות משפטית. אין בהכרח חפיפה בין שתי אלה; פעולות מסוימות מותרות לפי החוק, אולם נורמות חברתיות מגבילות אותן.⁷ כך למשל, לפי הדין הישראלי מותר לצלם אדם ברשות הרבים, ואף לפרסם את הצילום כל עוד הוא אינו משפיל ומבזה.⁸ אולם רבים מאיתנו ירגישו אי־נוחות לצלם אדם מקרוב ברשות הרבים, ועוד יותר מכך אם אנו נהיה מושא הצילום. גבולות הפרטיות שנויים במחלוקת. טכנולוגיות חדשות יוצרות אופנים חדשים של איסוף מידע, עיבודו והשימוש בו. כיום קל, פשוט וזול יותר מאי פעם לצלם או להקליט בכל מקום. אפשר לאסוף מידע דיגיטלי בקלות, ומידע שכזה נוצר כיום כחלק בלתי־נפרד מכל פעולה כמעט שאנו מבצעים – תנועה במרחב, פעילות פיננסית, מסחרית, רפואית, תקשורת בין־אישית ועוד. זהו השובל הדיגיטלי שלנו. כעת, משאפשר לאסוף מידע, יש מי שמבקשים לאוספו ולעבדו. נוכח הבשלות הטכנולוגית וירידת המחיר של אמצעי האיסוף והעיבוד של המידע מודגשים צרכים עסקיים, שלטוניים ופרטיים במידע. לתאגידים שפועלים מול צרכנים מידע הוא בסיס לקבלת החלטות מושכלות, שיאפשרו למשל שיווק מותאם אישית, מיקוד בשיווק, הבנה טובה יותר של הלקוחות וניהול יעיל יותר של העסק בכלל. לרשויות השלטון יש עניין במידע כדי להתנהל ביתר יעילות; כך למשל כדי לאתר כפילויות שונות שמביאות לטעויות, להונאה או לבזבז משאבים, כדי להקל על האזרחים בהתנהלותם מול הרשויות באמצעות ריכוז מידע ויצירת ממשק פשוט, מדויק ואמין, ומוכן שבכל הנוגע למערכות שונות להגנה על שלום הציבור, על הסדר הציבורי ועל רכוש או לניהול נכון יותר של משאבים כמו מערכות מים, חשמל, תחבורה ציבורית ועוד. חלק זה מציג את עיקריה של הזכות לפרטיות מן הפן המשפטי בעולם ובהקשר הישראלי, תוך התמקדות בהיבטי הפרטיות בערים החכמות. בפתח הדברים נידונים היקפה של הזכות לפרטיות, מישורי הפעולה שלה והמרכיבים העיקריים של ההסדרה.

הזכות לפרטיות

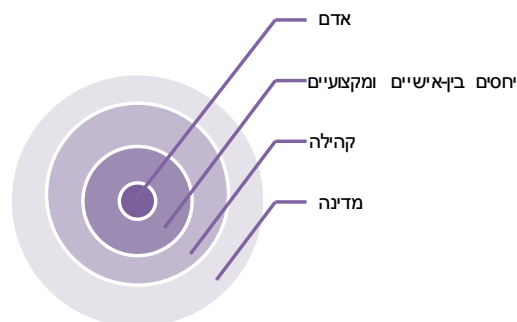
המופע הישיר הראשון של הפרטיות כזכות משפטית בעולם הדמוקרטי המערבי הוא במאמרם הידוע של וורן וברנדייס, שפורסם בשנת 1890.⁹ העיתוי אינו מפתיע. בסוף המאה התשע עשרה השלימה החברה המערבית במידה רבה את תהליך החילון והמודרניזציה ששם את האדם במרכז, בייחוד בתפיסה הליברלית; המהפכה התעשייתית הוטמעה, ובעקבותיה באו גידול ניכר בעויר, טכנולוגיות חדשות כמו צילום, בהמשך טכנולוגיות תקשורת כמו טלפון ופרקטיקות עסקיות חדשות כמו מדורי רכילות בעיתונות, ומאוחר יותר משרדי פרסום ולידתו של תחום השיווק. מן המאמר של וורן וברנדייס התפשטה הזכות למשפט האמריקני ולשיטות משפט אחרות. עלייתה של הזכות לפרטיות הביאה לדיון ער – במיוחד מהשליש האחרון של המאה העשרים – בהצדקות התאורטיות לזכות לפרטיות, כלומר בשאלה מדוע בכלל היא מוגנת. אין תמימות דעים בין הגישות השונות.¹⁰ קבוצה אחת של תאוריות מדגישה את החשיבות של הפרטיות לפרט: זכותו של האדם להחליט בעצמו החלטות שונות היא גזרת של התפיסה של האוטונומיה של האדם ושל כבוד האדם במונח הסגולי, הקאנטיאני, של מושג זה; זכותו של אדם לנסות ולשלוט בדימויו בעיני אחרים – מה שגופמן קורא לו "ניהול רושם";¹¹ והצורך הפסיכולוגי־אנושי שלנו במרחב פרטי שבו לא יטרידו אותנו, שבו נוכל להיעזב במנוחה, שבו נוכל לנסות, לתהות ולטעות, ללא צורך לתת דין וחשבון. זהו המרחב של "מאחורי

7 ליחס שבין פרטיות כזכות משפטית לפרטיות כנורמה חברתית, ראו מיכאל בירנהק, **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** (שריגים־ליאון: בר־אילן ונבו, 2010), 29-43.
8 ראו סעיפים 2(3) ו-2(4) לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: חוק הגנת הפרטיות).
9 Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, No. 5. (1890): 193-220.
10 לדיון מפורט בהצדקות הזכות לפרטיות, ראו Daniel Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008) ואילך.
11 ארווינג גופמן, **הצגת האני בחיי היומיום**, מתרגם: שלמה גונן (תל־אביב: רשפים, 1989).

הקלעים", כביטוי של גופמן, או המרחב לפיתוח "intellectual privacy", כביטוי של ניל ריצ'ארדס.¹² הצדקות אחרות מדגישות את חשיבות הפרטיות לקיומם של יחסים בין־אישיים תקינים כמו אינטימיות בין בני־זוג או יחסים מקצועיים כמו בין רופאה למטופל.

קבוצה נוספת של הצדקות מדגישה את הפן הציבורי של הפרטיות: היא חשובה לא רק בשל תרומתה לפיתוח הזהות והאישיות של הפרט והתנהלותו היומיומית, אלא גם לקהילה עצמה.¹³ הפרטיות יוצרת ערך של כבוד הדדי בין חברי הקהילה ומאפשרת להם לחיות יחד, דווקא למרות ההבדלים ביניהם.

קבוצה אחרונה של הצדקות מדגישה את חשיבות הפרטיות כערך חברתי ופוליטי בדמוקרטיה. בין השלטון לבין האזרח שוררים יחסים שבהם השלטון פועל עבור האזרח, והוא נאמן הציבור. ביחסים שכאלה המדינה צריכה לתפקד למען האזרחים, אך אין לה אינטרסים מעבר לכך. כל פעולה שלה צריכה להיות מוצדקת בהפניה לערכים שהיא מקדמת עבור האזרחים. כאן הפרטיות היא אמצעי נוסף, יחד עם זכויות אדם אחרות כמו חופש הביטוי, חופש ההפגנה ועוד, כדי לשמר את מערך הכוחות הדמוקרטי. שלטון לא־דמוקרטי מאופיין בהיעדר פרטיות; כך בברית המועצות לשעבר ובמזרח גרמניה בשעתן, או בסין או בצפון קוריאה של היום.



תרשים 3.1 מעגלים של "הצדקות פרטיות"

הפרטיות מקיפה הקשרים שונים. הדין האירופי מגן על פרטיות בקשר ל"פרטיות בחיים האישיים, בהקשר המשפחתי, בבית ובתקשורת."

הפרטיות מקיפה הקשרים שונים, וכאן אפשר גם לראות שונות בשיטות משפט שונות. הדין האירופי (הן במועצת אירופה הן באיחוד האירופי) מגן על פרטיות בקשר ל"private and family life, home and communications",¹⁴ כלומר פרטיות בחיים האישיים, בהקשר המשפחתי, בבית ובתקשורת. במדינות רבות אפשר לראות שמוענקת לאדם הגנה בקשר למידע מסוים שנחשב לאישי, בקשר למקומות מסוימים שנחשבים לפרטיים (המרכזי שבהם הוא הבית, אך הוא אינו היחיד) ובתקשורת. בארצות הברית, שבה הזכות לפרטיות אינה מנויה במפורש בחוקה, אפשר למצוא הגנה גם על החלטות אישיות של אדם, כך למשל באשר לשימוש באמצעי מניעה או באשר להחלטתה של אישה לבצע הפלה, החלטה שהומשגה שם בעבר במסגרת המושג של הזכות לפרטיות.

12 Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (New York: Oxford University Press, 2015).
13 Priscilla Regan, *Legislating Privacy: Technology, Social Values And Public Policy* (Chapel Hill: University of North Carolina Press, 1995).
14 סעיף 7 לצ'ארטר האירופי לזכויות יסוד, Charter of Fundamental Rights of the European Union (2000/C 364/01).

הגנת המידע האישי (data protection) נמצאת כיום במוקד השיח המשפטי, הרגולטורי והמחקרי על הזכות לפרטיות. בשאלה מהו מידע אישי ניתן למצוא הבדל בין הגישה האמריקנית לאירופית.

ישנה גם קטגוריה מרכזית של הגנה, והיא של פרטיות במידע אישי. בדין האירופי הזכות להגנת מידע אישי זוכה להגנה חוקתית נפרדת מהגנת הפרטיות, הגם שמבחינה רעיונית יש להן מקור משותף. סעיף 8 לצ'ארטר האירופי לזכויות יסוד של האיחוד האירופי קובע כך (התרגום שלי, מ' ב'):¹⁵

1. לכל אחד ואחת יש זכות להגנה על מידע אישי על אודותיו/ה.
2. עיבוד של מידע כאמור צריך להיעשות באופן הוגן, למטרות מוגדרות, על בסיס הסכמה של האדם מושא המידע או לפי בסיס לגיטימי אחר שנקבע בחוק. לכל אדם יש זכות לגישה למידע שנאסף על אודותיו/ה, ולתיקון המידע.
3. ציות לכללים אלה כפוף לפיקוח של רשות עצמאית.

הגנת המידע האישי, או במונח האירופי "data protection", נמצאת כיום במוקד השיח המשפטי, הרגולטורי והמחקרי על הזכות לפרטיות. השאלה הראשונה היא מהו "מידע אישי", וכאן אפשר למצוא שתי גישות שונות – האמריקנית והאירופית. בארצות הברית הוגדרו סוגי מידע מסוימים לפי תוכנם כרגישים במיוחד, ובהתאם לכך הם זכו להסדרה ייחודית. כך, אנו מוצאים חקיקה פדרלית בנוגע למידע גנטי, בנוגע למידע רפואי ובנוגע למידע פיננסי, אך גם בנוגע לסוגי מידע נקודתיים יותר כגון מידע הנוגע לתוכני הצפייה של מנוי טלוויזיה בכבלים או למשל חוק העוסק בהשכרת תוכני וידאו. בכל אחת ממדינות ארצות הברית יש חקיקה נוספת. בדין הפדרלי ישנו גם חוק שעוסק בפרטיות ילדים (בני 13 ומטה). חוקים אלה אינם אוסרים על איסוף המידע, אלא הם קובעים את הכללים לאיסופו ולעיבודו, את השימושים בו ואת העברתו. התוצאה היא מעשה טלאים חקיקתי. מידע שאינו בא בגדר אחד החוקים האלה אינו מוגן בדין הפדרלי. לכל אחד מהחוקים תנאי סף נוספים להגנה, לפי העניין. יש להקדים ולומר, כי מידע על מיקומו של אדם במרחב הציבורי, לדוגמה, אינו מוגן שם.

הגישה האירופית שונה. האירופים בחרו, ברוח הנחיתו של ארגון המדינות המתועשות, ה־OECD, להגדיר "מידע אישי" בהגדרה שאיננה מבוססת תוכן, אלא על אמת מידה של זיהוי האדם. כך מגדירה רגולציית הגנת המידע האישי החדשה (General Data Protection Regulation – GDPR), שנכנסה לתוקף בחודש מאי 2018, את המונח "מידע אישי" (התרגום שלי, מ' ב'):¹⁶

'מידע אישי' פירושו כל מידע שמתייחס לאדם מזוהה או לאדם טבעי שניתן לזהותו (להלן: 'מושא המידע'). אדם טבעי שניתן לזהותו הוא זה שניתן לזהותו במישרין או בעקיפין, במיוחד בהתייחס למזוהה כמו שם, מספר מזוהה, מידע על מיקום, מידע מקוון, או אחד או יותר גורמים בקשר לזהות הפיזית, הפסיכולוגית, הגנטית, הנפשית, הכלכלית, התרבותית או החברתית של האדם הטבעי.¹⁷

ה־GDPR אינה מחדשת כאן, וזהו הדין באיחוד האירופי מאז שנת 1995. במילים אחרות, כל מידע על אדם מזוהה או על אדם שניתן לזהותו מתוך המידע נחשב למידע אישי,

15 במקור:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority".

16 במקור:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

17 סעיף (1) ל־GDPR. הביטוי "אדם טבעי" (natural person) נועד להבחין בין בני אדם לבין תאגידיים.

והרגולציה חלה עליו. המשמעות היא כי גם פריטי מידע טריוויאליים מוגנים, אם הם מזוהים את האדם. גם כאן משמעות ההסדרה איננה איסור על איסוף המידע ועיבודו, אלא הסדרה של פעולות אלה. הפרטיות נחשבת כיום לזכות יסוד במדינות רבות וזוכה להגנה משפטית חזקה – עלי ספר. כך הדין האירופי וכך ההגנה האמריקנית, המעגנת היבטים מסוימים של הפרטיות.

הזכות לפרטיות בישראל

ומכאן לישראל. בדין הישראלי הפרטיות מעוגנת בחוק יסוד: כבוד האדם וחירותו, בחוק ספציפי, ופותחה בפסיקת בתי המשפט, המפרשים את הדינים הקיימים ומשלימים פערים שיש בהם.

חוק היסוד קובע בסעיף 7 כך:

פרטיות וצנעת הפרט

- א. כל אדם זכאי לפרטיות ולצנעת חייו.
- ב. אין נכנסים לרשות היחיד של אדם שלא בהסכמתו.
- ג. אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו.
- ד. אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו.

המונח "פרטיות" עצמו אינו מוגדר בחוק היסוד או בחוק אחר; הפרטיות מוגנת בקשר למקומות שהם "רשות היחיד", מונח נוסף שאינו מוגדר בדין, בקשר לאדם ובקשר לתקשורת. החלטות פרטיות אינן מוגנות בדרך כלל תחת הגג של הזכות לפרטיות, אלא במישרין, תחת הגנת כבוד האדם שבחוק היסוד. ההגנה החוקתית אינה מוחלטת, והיא כפופה ל"פסקת ההגבלה" שבסעיף 8 לחוק היסוד, הקובע כי "אין פוגעים בזכויות שלפי חוק יסוד זה אלא בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שאינה עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו". כלומר ניתן לפגוע בזכות לפרטיות, אולם יש צורך בחקיקה מפורשת בנושא, בחקיקה או בתקנות, והפגיעה צריכה להיות מוצדקת – לתכלית ראויה – ומידתית. פגיעה שאינה עומדת בתנאים אלה אינה חוקתית, והיא אסורה.

חוק הגנת הפרטיות, התשמ"א-1981 (להלן: חוק הגנת הפרטיות) מפרט את הזכות לפרטיות בכמה הקשרים. הקשר אחד הוא היחסים שבין אדם לחברו ובכלל זה בין תאגיד לאדם, ועניינו הוא "מצבי פרטיות קלאסיים". החוק מפרט שורה של מצבים שהם פגיעה בפרטיות, כך למשל בילוש או התחקות אחר אדם שעלולים להטרידו, האזנת סתר, צילום ברשות היחיד, פתיחת מכתב, הפרת חובת סודיות שנקבעה בהסכם או בדין, שימוש במידע שלא למטרה שלשמה נאסף (עקרון צמידות המטרה) ועוד. הקשר שני של הגנת הפרטיות בדין הישראלי עוסק במידע אישי, והוא מקביל לדין האירופי בקשר להגנת מידע אישי. הדין הישראלי צר מן הדין האירופי, אך עקרונית דומים. בהמשך יפורטו עקרונות אלה. בצד חוק זה ישנם דינים רבים נוספים שיש להם נגיעה לפרטיות, בין בהגנה נוספת שלה (למשל חוק זכויות החולה), ובין בכרסום בה (למשל חוק נתוני תקשורת או חוק המאגר הביומטרי, בשם המוכר).¹⁸

18 ראו בהתאמה: חוק זכויות החולה, התשנ"ו-1996; חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007; חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009.

בדין הישראלי הפרטיות מעוגנת בחוק יסוד: כבוד האדם וחירותו, בחוק ספציפי, ופותחה בפסיקת בתי המשפט, המפרשים את הדינים הקיימים ומשלימים פערים שיש בהם.

חוק הגנת הפרטיות מפרט שורה של מצבים שהם פגיעה בפרטיות: בילוש או התחקות אחר אדם, האזנת סתר, צילום ברשות היחיד, פתיחת מכתב, הפרת חובת סודיות, שימוש במידע שלא למטרה שלשמה נאסף.

טבלה 3.1: הגנה משפטית על מידע אישי – מבט השוואתי

סוג המידע	הדין האירופי	הדין האמריקני	הדין הישראלי
מידע אישי	על אדם מזוהה או שניתן לזיהויו.	אם המידע מוגן לפי תוכנו, החקיקה הפדרלית עשויה לדרוש תנאים נוספים לתחולתה, כמו זיהויו של אדם.	סעיף 7 לחוק הגנת הפרטיות: "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".
רשות היחיד	מוגן במישור החוקתי וכמידע מזהה.	מוגן בהקשר החוקתי של אכיפת חוק (התיקון הרביעי לחוקה) ולפי פרשנות בתי המשפט.	מוגן בחוק היסוד ביחס למדינה, ובקשר לפרט, במצבים רלוונטיים כמו איסור בילוש ואיסור צילום ברשות היחיד. המונח אינו מוגדר בחוק, ומפורש בידי בתי המשפט.
תקשורת	מוגן במישור החוקתי וכמידע מזהה.	מוגן בחקיקה ייעודית.	מוגן בחוק היסוד באופן כללי (סעיף 7(ד)); בחוק האזנת סתר, ובחוק הגנת הפרטיות בקשר למכתבים, לרבות דיגיטליים.
החלטות	מומשג במסגרות משפטיות אחרות.	"פרטיות בהחלטות" היא קטגוריה שעוצבה בידי בתי המשפט שם.	מומשג במסגרות משפטיות אחרות.

טבלה 3.2: מישורי הפעולה של הפרטיות וההסדר המשפטי

	מישור חוקתי	מישור הדין הרגיל
מישור חוקתי:	הרשות כפופה לחוק היסוד, ומותר לה לפגוע בפרטיות רק לפי פסקת ההגבלה.	החוק הרגיל חל על המדינה (סעיף 24 לחוק הגנת הפרטיות), הן בקשר לפגיעה בפרטיות קלאסית הן בקשר למאגרי מידע.
מדינה מול אדם	לשם בירור המידתיות, בתי משפט עשויים לפנות להסדרי פרק ב לחוק הגנת הפרטיות.	
מישור פרטי:	אין תחולה ישירה של חוק היסוד. עשויה להיות תחולה עקיפה.	חל פרק ב של החוק (הסדר מאגרי מידע).
תאגיד מול אדם		
בין אדם לחברו	אין תחולה ישירה של חוק היסוד. עשויה להיות תחולה עקיפה.	חל פרק א של החוק (מצבי פרטיות קלאסיים).

מישורי הפעולה

הצדקותיה של הזכות לפרטיות, היקפה על סוגי מידע שונים והמסגרת המשפטית הכללית של הזכות הוזכרו מוקדם יותר. הדיון מעלה, שהפרטיות מוגנת בהקשרים שונים, באופנים שונים, לפי זהות השחקנים המעורבים ולפי סוג המידע. מישורים אלה חשובים לענייננו, משום שבהקשר של העיר הדיגיטלית הם מתערבבים זה בזה, ערבוב המקשה במידת מה על עיצוב ההסדר המשפטי המתאים.

מישור ראשון הוא המישור החוקתי. הוא חל במישורין על המדינה ועל הרשויות השונות. רשויות עירוניות באות בגדר הקבוצה הזו; אסור לרשות מקומית לפגוע בפרטיות של אזרחים (תושבי העיר או מי שאינם תושביה). אם רשות מבקשת בכל זאת לפגוע בפרטיות, עליה לעשות זאת לפי הסמכה מפורשת בחוק או בתקנות (הכוונה היא לחוק של הכנסת, ואין די בחוק עזר עירוני), לתכלית ראויה ובאופן מידתי. כדי לבחון מהם אמצעים מידתיים בתי המשפט עשויים לפנות לפירוט שיש בחוק בקשר להגנת מידע אישי. לפי העניין עשוי לחול גם ההסדר שיש בחוק בקשר לפרטיות קלאסית. כך למשל, אם רשות מקומית תבקש לצלם אנשים ברשות היחיד, פעולה זו אסורה לפי סעיף 3(2) לחוק; אם היא תבקש לצלם ברשות הרבים, הרי אין איסור מפורש בחוק הגנת הפרטיות, אולם פעולה זו כפופה למסגרת החוקתית, וכדי לברר את המידתיות שלה בית משפט עשוי לפנות להסדר של מאגרי המידע. אם הרשות תבקש ליצור מאגר מידע חדש, הרי פעולה שכזו כפופה לדרישות שונות כמו חובת הודעה, מתן זכויות גישה למידע, חובת סודיות, חובת אבטחת מידע ועוד.

מישור שני הוא המישור של הגנת המידע האישי. הוא חל על הרשויות, אך גם על גורמים פרטיים. כך, הרשות יכולה לבחור שלא לפגוע בפרטיות, ולכן היא לא תצטרך לפעול לפי המתווה החוקתי; אך היא תצטרך לעמוד בתנאים שיש בהסדר מאגרי המידע שבחוק הגנת הפרטיות, שעליו יורחב בסעיף הבא. גם תאגיד שמבקש לאסוף מידע על אזרחים, לרוב בכובעם כצרכנים, יכול לעשות זאת, אולם גם הוא צריך לפעול בתוך מסגרת הפעולה של הסדר מאגרי המידע. תאגיד פרטי אינו כפוף לחוק היסוד במישורין ואינו זקוק להסמכה בחקיקה או לפעולה מידתית, אך ההסדר של מאגרי מידע מביא לתוצאה דומה.

מישור שלישי הוא המישור שבין אדם לחברו. כאן חל ההסדר החוקי שעוסק במצבי פרטיות קלאסיים: כאשר אדם חושף את סודו של אדם אחר ללא רשות, מפרסם מידע אישי על אודותיו ופעולות דומות, הרי זו פגיעה בפרטיות. יש להקדים ולומר, כי בעיר בעלת התשתיות הדיגיטליות, ישנם כל סוגי הפרטיות וכל מישורי הפעולה שהוזכרו כאן.

מרכיבי ההסדרה

הענף של הגנת מידע אישי, data protection, שנמצא גם בדין הישראלי, מתיר את איסוף המידע ועיבודו, אך קובע כללים שונים לעניין זה. כלל סף אחד שנסקר כאן נוגע לשאלה מתי נכנס הדין לפעולה. בארצות הברית המבחן הוא נושאי, ובדין האירופי המבחן הוא זיהוי האדם. בדין הישראלי יש מזה ויש מזה, והעמדה הרווחת כיום היא כי הדין מופעל כאשר האדם מזוהה, ברוח הדין האירופי. כללים אחרים קובעים כיצד יש לנהוג במידע. ראוי לחזור שוב על ההוראה החוקתית האירופית, שלפיה "עיבוד של מידע [אישי] צריך להיעשות באופן הוגן, למטרות מוגדרות, על בסיס הסכמה של האדם מושא המידע או לפי בסיס לגיטימי אחר שנקבע בחוק. לכל אדם יש זכות לגישה למידע שנאסף על אודותיו/ה, ולתיקון המידע".

גישה זו משקפת את עקרונות המידע האישי שהחלו להופיע בשיטות משפט שונות בעולם בתחילת שנות השבעים של המאה הקודמת, והמגולמים גם בדין הישראלי.

הפרטיות מוגנת בהקשרים שונים באופנים שונים, לפי זהות השחקנים המעורבים ולפי סוג המידע. בעיר הדיגיטלית הם מתערבבים זה בזה ומקשים במידת מה על עיצוב ההסדר המשפטי המתאים.

עיבוד של מידע [אישי] צריך להיעשות באופן הוגן, למטרות מוגדרות, על בסיס הסכמה של האדם מושא המידע או לפי בסיס לגיטימי אחר שנקבע בחוק. לכל אדם יש זכות לגישה למידע שנאסף על אודותיו/ה, ולתיקון המידע.

Fair Information Practices
הם עקרונות מקובלים
שהתגבשו בהסדרים משפטיים
שונים בעולם, שמבקשים
להסדיר את זכויותיהם של
מושאי המידע ואת חובותיהם
של מעבדי המידע, לכל אורך
חיי המידע.

עיקרון יסוד הוא עקרון
צמידות המטרה, ולפיו מידע
שנאסף למטרה אחת – אסור
שישמש למטרה אחרת.

נדרשת הסכמה מדעת,
אקטיבית, של מושאי המידע.
בהיעדר הסכמה שכזו,
אין לאסוף מידע אישי על
אודותיהם.

עקרונות אלה מכונים באופן כללי Fair Information Practices, או בקיצור FIPs. כללים אלה זכו לתהודה גלובלית בעיקר בזכות הדין האירופי, שהעיקרון הרלוונטי בו הוא שהדין צועד בעקבות המידע.¹⁹ גישה זו הביאה לכך, שמדינות שביקשו לאפשר לעסקים מקומיים לעבד מידע על אזרחים אירופיים אימצו דין ברוח הדין האירופי. ישראל היא אחת המדינות הללו.²⁰

יש שוני בין מדינה למדינה ביישום הכללים האלה, אולם ניתן בכל זאת לתאר את המסגרת הכללית שלהם. בתמצית, הדין מבקש לעקוב אחר שלבים שונים בחיי המידע, וליצור אפשרויות למושא המידע (data subject, בעגה המשפטית האירופית) לשלוט במידע האישי על אודותיו, בין במישרין ובין באמצעות אכיפה ציבורית. זהו עקרון־העל של FIPs.

תחילה, באשר לאיסוף המידע – נדרש שהוא יהיה למטרה ראויה; האיסוף צריך להיות בהסכמה מדעת של מושא המידע ותוך מגבלות שונות על צורת האיסוף. את ההסכמה אפשר לקבל רק לאחר יידוע מתאים של מושא המידע בדבר מטרת האיסוף של המידע, השימושים במידע שייאסף, ואם יועבר ולמי. בחוק הגנת הפרטיות הישראלי אין דרישה מפורשת שמטרת האיסוף תהיה ראויה; אולם ככל שהגורם שאוסף את המידע הוא רשות ציבורית, דרישה זו נובעת מן המשפט החוקתי (כלומר מחוק־יסוד: כבוד האדם וחירותו) ומן המשפט המנהלי. משנאסף המידע, הדין קובע מגבלות על השימושים בו. עיקרון חשוב הוא עקרון צמידות המטרה, ולפיו מידע שנאסף למטרה אחת – אסור שימש למטרה אחרת. עיקרון זה חשוב במיוחד נוכח התופעה הרווחת של "זחילת מטרות" (function creep), או בביטוי המוכר "כיבוש זוחל". משמעות התופעה היא שמידע נאסף לכתחילה למטרה ראויה, וכעת מזהים מחזיקי המידע כי יכולים להיות בו שימושים מועילים נוספים. הדין אוסר על כך. אם ברצונם בכך, על מחזיקי המידע לפנות למושאי המידע שוב ולבקש את הסכמתם לשימוש במידע. במהלך עיבוד המידע מוטלות על מחזיקי המידע חובות נוספות; חלה עליהם חובת סודיות באשר למידע, כלומר למנוע את זליגתו (המכוונת או הרשלנית) מתוך הארגון החוצה, והם מחויבים באבטחת המידע, כלומר למנוע מגורמים עוינים לחדור למאגר המידע. בישראל יש גם חובת רישום של מאגר המידע, אולם היא נחשבת לכושלת, ובעבר הוצע לא אחת לבטלה. בצד אלה למושאי המידע יש זכויות לגשת למידע על אודותיהם ולדרוש את תיקונן במידת הצורך. הדין קובע כי הפרת החובות הללו בידי מחזיק המידע מקימה למושא המידע זכות תביעה לבית המשפט, וכי מדובר גם בעבירה פלילית. במקביל ישנו גורם אכיפה שלטוני. בישראל זו הרשות להגנת הפרטיות (שמה המחודש של הרשות למשפט וטכנולוגיות מידע – רמו"ט), יחידה הפועלת בכפוף למשרד המשפטים.

כל אלו הם סל הכלים הבסיסי של הגנת המידע האישי. אנו עדים כיום להופעה של סל כלים מעודכן, גרסה מתוקנת ומעודכנת של FIPs. המקום המרכזי שבו מעוגן סל כלים זה הוא ה־GDPR האירופי. רגולציה זו חוזרת על העקרונות הקודמים שיש בדין ומחזקת אותם. כך למשל, ה־GDPR מעלה את הרף הדרוש להסכמה של מושאי המידע; אין להסתפק בברירת מחזל של opt out – נדרשת הסכמה מדעת, אקטיבית, של מושאי המידע. בהיעדר הסכמה שכזו, אין לאסוף מידע אישי על אודותיהם. ה־GDPR מאפשרת

19 לפי גרהאם גרינליף ישנן כיום מעל 120 מדינות שאימצו דיני הגנת פרטיות במידע אישי הקרובים לדין האירופי. ראו: Graham Greenleaf, "Countries with Data Privacy Laws – By Year 1973-2016", 146 *Privacy Laws & Business International Report*, 18. Available at (April 2, 2017), SSRN: <https://ssrn.com/abstract=2996139>. תופעה זו הומשה כ"גלובליזציה משפטית רכה". ראו: Michael Birnhack, "The EU Data Protection Directive: An Engine of a Global Regime," *Computer Law & Security Review* 24, no. 6 (2008): 508–520.

20 בשנת 2011 הכיר האיחוד האירופי בישראל כבעלת משטר הגנת פרטיות "מספק" (adequate). ראו: EU Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, OJ L. 27/39(2011)

למושא המידע לחזור בו מהסכמתו, ומספקת שאר כללים שמחזקים את המסגרת הקיימת. אולם אפשר לראות גם מרכיבים נוספים. הבולטים שבהם הם הוספת "הזכות להישכח" (right to be forgotten), שמאפשרת למושא המידע לדרוש מחיקה של מידע על אודותיו בתנאים מסוימים, ומטילה חובה חדשה על מנהלי המאגרים לדווח לרשות המתאימה או לציבור, לפי העניין, על דליפת מידע.²¹ **יצוין כי חובה זו – הדיווח לרשות במקרה של דליפת מידע – נקבעה בדין הישראלי בתקנות חדשות משנת 2017, שנכנסו לתוקף במהלך שנת 2018.**²²

אולם החידוש המרכזי של סל הכלים המעודכן הוא הוספת אמצעי הגנה חוץ־משפטיים, שכעת זוכים לעיגון משפטי. אלה הם אמצעים ארגוניים וטכנולוגיים. ה־GDPR דורשת שלפני השמעת מערכת טכנולוגית חדשה שעוסקת במידע אישי, יבוצע הליך של Privacy Impact Assessment (PIA); ה־GDPR דורשת מינוי של "ממונה הגנת מידע" – Data Protection Officer (DPO);²³ וכן קיום תהליך של "הנדסת פרטיות" (בביטוי האירופי – Data Protection by Design, או בביטוי המוכר לפני כן, Privacy by Design – PbD), שמשמעו ניסיון להטמיע ערכים של פרטיות בתוך המערכת הטכנולוגית. כל אחד מהאמצעים החדשים האלה עודנו עמום, אולם הרוח הכללית ברורה: הגנת הפרטיות תושג, לפי גישת הדין האירופי, לא רק באמצעות קביעת זכויות וחובות, אלא באמצעות ניסיונות להטמיע את הגנת הפרטיות בתוך המערכות עצמן – אצל העוסקים במלאכה – מראש, ולא בדיעבד. בשל העיקרון האירופי שנוכר לעיל, שלפי הדין האירופי הוא נלווה ונצמד למידע אירופי, צפויה ה־GDPR ליצור גל שני של חקיקת פרטיות בעולם, בקרב מדינות שביקשו לעמוד בסטנדרט האירופי.

מתוך זה, בדין הישראלי הרובד הראשון קרוב אך אינו זהה לדין האירופי. מהרובד השני נקבעה חובת הודעה על דליפת מידע בתקנות, אולם אין בדין הישראלי זכות להישכח, אין בה חובה לעריכת תסקיר על הגנת פרטיות, למינוי ממונה על הגנת פרטיות,²⁴ או לקיים הליך של הנדסת פרטיות. יצוין שהאיחוד האירופי בוחן בימים אלה מחדש את מעמדה של ישראל בהקשר הזה.

דיון זה מעלה כי המלאכה רבה. פרטיות איננה עניין של מה בכך. השינויים המשפטיים מעידים כי הפרטיות חיה וקיימת, והמחוקקים לא רק שלא התייאשו ממנה, אלא הם מבקשים לחזקה. בעת כתיבת שורות אלה בוחן גם הקונגרס האמריקני שינויים בחקיקה, בעקבות פרשת "קיימברידג' אנליטיקה / פייסבוק". הדיון מעלה עוד כי פרטיות אינה רק עניין של סודיות מידע, וכי היא אינה רק עניינים של "צנעת הפרט"; המסגרת המשפטית כיום ערה לכך שכל פריט מידע, גם אם הוא נראה טריוויאלי ופשוט כשלעצמו, ראוי להגנה כל עוד ניתן לזהות את האדם מתוך המידע הזה או יחד עם פריטי מידע נוספים. זאת ועוד, אנו רואים שהגנת הפרטיות אינה מוגבלת להיבט של אבטחת מידע, אלא יש בה נקודות מפגש חשובות רבות בין מושא המידע לבין אוסף המידע לאורך חיי המידע.

21 מקור החובה הוא דווקא בדין האמריקני המדינתי, ומשם היא חצתה את האוקיינוס ונקלטה ב־GDPR.

22 תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

23 בכך מאמץ הדין האירופי את הפרקטיקה שצמחה בארצות הברית, מן השטח, ולא לפי דין. ראו Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, (Cambridge, MA.: Massachusetts Institute of Technology, 2015)

24 יש בדין הישראלי חובה למנות ממונה על אבטחת מידע, ראו סעיף 17 לחוק הגנת הפרטיות. אולם תפקיד זה הוא צר ומוגבל להיבט הטכנולוגי של אבטחת מידע.

החידוש המרכזי של סל הכלים
המעודכן הוא הוספת אמצעי
הגנה חוץ־משפטיים, שכעת
זוכים לעיגון משפטי. אלה הם
אמצעים ארגוניים וטכנולוגיים.

בגישה הנוכחית הגנת
הפרטיות תושג באמצעות
ניסיונות להטמיע את הגנת
הפרטיות בתוך המערכות
עצמן, מראש ולא בדיעבד.

המסגרת המשפטית כיום ערה
לכך שכל פריט מידע ראוי
להגנה כל עוד ניתן לזהות את
האדם מתוך המידע הזה או
יחד עם פריטי מידע נוספים.



טבלה 3.3: עקרונות ההגנה על המידע האישי

חיי המידע האישי	FIPs 1.0 מגולם בעקרונות OECD	FIPs 2.0 מגולם ב-GDPR	הדין הישראלי
איסוף	תכלית ראויה חובת יידוע דרישת הסכמה	תכלית ראויה חובת יידוע דרישת הסכמה בתוספת חיזוק דרישת ההסכמה מדעת, אפשרות חזרה מהסכמה	תכלית ראויה - דרישה לגופים ציבוריים ולמעסיקים פרטיים; אין דרישה בדין לגורמים פרטיים; חובת יידוע (ס' 11 לחוק) - אם יש חובה חוקית למסור את המידע, מטרת השימוש במידע, ןאם יועבר הלאה הסכמה מדעת (ס' 3 לחוק); מחלוקת בבתי המשפט בקשר לחזרה מהסכמה
שימוש במידע ועיבודו	עקרון המינימיזציה - מותר לאסוף ולעבד רק מידע שלשמו נתקבלה ההסכמה. עקרון צמידות המטרה - אסורים שימושים נוספים במידע	עקרון המינימיזציה - מותר לאסוף ולעבד רק מידע שלשמו נתקבלה ההסכמה. עקרון צמידות המטרה - אסורים שימושים נוספים במידע	עקרון המינימיזציה - מותר לאסוף ולעבד רק מידע שלשמו נתקבלה ההסכמה. עקרון צמידות המטרה - אסורים שימושים נוספים במידע
העברת המידע לצדדים שלישיים	רק בהסכמה, רק במסגרת התכלית הראויה הראשונה	רק בהסכמה, רק במסגרת התכלית הראויה הראשונה	רק בהסכמה, רק במסגרת התכלית הראויה הראשונה
חובת סודיות, אבטחת מידע	קבועה בדין	קבועה בדין	קבועה בדין ובתקנות
זכות גישה למידע ותיקונו	קבועות בדין	קבועות בדין	ס' 1, 13, 14 לחוק, עם חריגים לרשויות ביטחון
אכיפה	עוולה אזרחית; אכיפה של רשות להגנת פרטיות	עוולה אזרחית; אכיפה של רשות להגנת פרטיות. במדינות שונות - תביעה ייצוגית	עוולה אזרחית, עבירה פלילית, סמכויות אכיפה מסוימות לרשות להגנת הפרטיות; אפשרות תביעה ייצוגית - במקרים מסוימים לפי חוק תביעות ייצוגיות
רישום מאגרי מידע	אין חובה	אין חובה	יש חובה, שכמעט שאינה מיושמת ואינה נאכפת
זכות להישכח	נקבעה בפסיקת בית הדין האירופי, בקשר למידע שאינו רלוונטי עוד	נקבעה ב-GDPR באופן רחב	לא קיים
חובת הודעה על דליפת מידע	אין	יש	יש, בתקנות אבטחת מידע, לפי הערכת הסיכון הרלוונטי
עריכת תסקיר הגנת פרטיות	אין	יש	אין
ממונה פרטיות ארגוני	אין	יש	ממונה על אבטחת מידע בלבד
הנדסת פרטיות	אין	יש	אין

התשתית של עיר בעלת
תשתיות דיגיטליות היא
מידע. בנוסף ל"אינטרנט של
הדברים" ואפשרויות עיבוד של
נתוני עתק, התוצאה היא שינוי
מערך היחסים והכוחות בין
הרשות המקומית לתושבים.

חלק זה מבקש ליישם את המסגרת הכללית שתוארה בחלק הקודם להקשר של ערים בכלל (בסעיף הראשון) ושל ערים עם תשתיות דיגיטליות בפרט (בסעיף השני); הוא מצביע על היסודות שברוכים בכך (הסעיף השלישי) ועל המסגרת המשפטית המתאימה (הסעיף הרביעי).

1. איסוף מידע בידי רשויות מקומיות

התשתיות השונות שמצטרפות יחד לכך שעיר מכריזה על עצמה כ"חכמה" הן איסופו של מידע, עיבודו ושימוש בו. בעוד שהתשתית לעיר הפיזית היא מערכות פיזיות כמו בינוי, כבישים ומערכות תחבורה, צנרת וכדומה, התשתית של עיר בעלת תשתיות דיגיטליות היא המידע. הוסיפו לכך התפתחויות טכנולוגיות כמו "האינטרנט של הדברים" (Internet of Things) ואפשרויות עיבוד של נתוני עתק (big data),²⁵ והתוצאה היא מצב עירוני חדש, שמשנה את מערך היחסים והכוחות שבין הרשות לתושבים.

כאשר אין מדובר במידע על בני אדם, הרי סוגיית הפרטיות כלל אינה מתעוררת. אם עיריית חיפה מבקשת לספור את חזירי הבר שיש בעיר, אין זו סוגיה של פרטיות. אם עירייה מבקשת להסדיר זיהום שנגרם מכלי רכב מבלי לאסוף מידע על הנהגים, אין כאן מידע אישי. יתרה מכך, כאשר המידע נאסף באופן אנונימי מלכתחילה, הרי כל עוד לא ניתן לזהות מתוך המידע את מושאי המידע הוא אינו נחשב ל"מידע אישי". כך, אם עיריית תל-אביב מבקשת לדעת כמה אנשים נכנסים לעיר בשעות שונות של היממה, אולם מבלי לאסוף כל מידע מזהה עליהם, הרי הדין אינו מופעל. אולם כאשר נאסף מידע אישי מזהה, הדין מופעל וחל. המסגרת המשפטית היא כאמור מורכבת יותר: יש לברר מי אוסף את המידע, איזה סוג של מידע, לאיזו מטרה, ולאן עובר המידע.

אפשר להביא דוגמאות לכמה מצבים:

- לעיתים פעולת העירייה עשויה לפגוע בפרטיות הקלאסית. לדוגמה, צילום ברשות היחיד אסור לפי חוק הגנת הפרטיות. המושג "רשות היחיד" אינו מוגדר בחוק, אולם הוא אינו מוגבל רק לבתים פרטיים. כך למשל, מצלמה המותקנת בפארק ציבורי אך שדה הראייה שלה כולל גם חצר של בית פרטי סמוך – מדובר בפעולה אסורה. כדי להתיר אותה יש לבחון את הפעולה לפי המתווה של פסקת ההגבלה שבחוק יסוד: כבוד האדם וחירותו.
- כאשר העירייה אוספת את המידע בעצמה, מעבדת אותו לשם ניהול שירותים עירוניים רגילים, הרי היא כפופה למסגרת החוקתית ולהסדר של מאגרי מידע (פרק ב לחוק הגנת הפרטיות) גם יחד. כך, מאגר מידע על ילדים במערכת החינוך המקומית, מאגר מידע על משלמי ארנונה, מאגר מידע על מי שמופלים בידי רשויות הרווחה המקומיות וכדומה הם כולם מאגרי מידע כהגדרתם בחוק הגנת הפרטיות. לעירייה מותר להקים מאגרים שכאלה, אולם היא צריכה להצביע על מקור הסמכה חוקי. מקור שכזה נמצא בדרך כלל בפקודת העיריות, הכוללת רשימה ארוכה של סמכויות לרשויות המקומיות, וכן סמכות להתקין חוקי עזר לביצוע סמכויותיה.²⁶ בהיעדר וו שאפשר להיאחז בו בחוק לקיום הפעולה – תנאי פיסקת ההגבלה אינם מתקיימים, ואין לאסוף מידע אישי. מאחר שמדובר בגוף ציבורי, אין די בעוגן המסמיך בחוק, והתכלית צריכה להיות ראויה. השאלה מהי תכלית ראויה נבחנת בבתי המשפט מעת לעת. גם אם יש מקור הסמכה מספק, הפעולה צריכה להיות מידתית. כדי לבחון את המידתיות, אפשר לפנות להסדר של מאגרי מידע (פרק ב לחוק הגנת הפרטיות):

²⁵ לדיון בשילוב של גורמים אלה ראו: Lilian Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective," *European Data Protection Law Review (Lexion)* 2, no.1 (2016): 28–58

²⁶ סעיף 249 לפקודת העיריות [נוסח חדש].

העירייה ממילא כפופה גם להוראות הסדר זה, כך שהדברים מתלכדים. את המאגר יש לרשום אצל רשם מאגרי המידע. יש להודיע לתושבים על איסוף המידע ולקבל את הסכמתם. בהיעדר הסכמה – מדובר בפגיעה בפרטיות, ואז האפיק הוא החוקתי בלבד. במקרים אחרים דרושה הודעה ודרושה הסכמה. יש לשמור על המידע מפני זליגתו מבפנים או מפני חשיפתו מבחוץ; יש לאפשר זכות גישה למידע ואת תיקונו.

- כאשר העירייה מבקשת להעביר מידע שנאסף אצלה לגורם מחוץ לעירייה, עליה להראות את מקור ההסמכה לכך, לערוך יידוע מתאים וכן הלאה. המידע של התושבים אינו יכול להיות מקור להכנסות לעירייה, ואין לסחור בו סתם כך.
- כאשר העירייה מבקשת להצליב מאגרי מידע שונים שיש אצלה, היא צריכה גם כן להצביע על מקור מסמיך מתאים לשימוש המיועד במידע, ועליה לכבד את עקרון צמידות המטרה. כך למשל, מידע שנאסף על ילדים שלומדים במערכת החינוך המקומית, אין להשתמש בו כדי לשווק לתושבים מוצרים בתשלום מטעם העירייה או מטעמו של גורם מסחרי שעובד עימה. בדוגמה זו ספק אם יש מקור מסמיך לשימוש הנוסף במידע, וספק אם שיווק מסחרי הוא תכלית ראויה לגוף ציבורי.
- כאשר תאגיד אוסף מידע עבור העירייה או עבור תושביה ולצרכיו המסחריים שלו, כגון חברה שמציעה שירות מסוים, כמו חברת מוניות (דוגמת Gett), חברה שנסמכת על מידע פומבי של זמני האוטובוסים (דוגמת Moovit) או כל שירות אחר שכרוך באיסוף מידע, תאגיד זה כפוף להוראות ההסדר של מאגרי מידע שבפרק ב לחוק הגנת הפרטיות: מותר לאסוף מידע רק לאחר יידוע מספק למושאי המידע, לאחר קבלת הסכמתם, לאחר עמידה בעקרונות של צמידות המטרה, של סודיות, של אבטחת מידע ושל קיום הזכויות של גישה למידע ותיקונו. חשוב לשים לב: העירייה אינה יכולה להתחמק מחובותיה המנהליים בהפרשת שירות מסוים לגוף פרטי. במקרה שכזה הגוף הפרטי שמבצע את השירות עבור העירייה ייחשב לזרועה הארוכה ויוכפף לדין המנהלי והחוקתי, ומוכן שהעירייה נותרת כפופה לחובותיה אלה.

2. מידע בעיר בעידן הדיגיטלי

הגם שהמושג "עיר חכמה" אינו חד דיו, וחלק ניכר מן המרואיינים מקרב הרשויות המקומיות השונות אומרים בפה מלא כי מדובר במושג עמום ופעמים רבות ריק מתוכן, המשמש ליחסי ציבור, אפשר לזהות כמה סוגי פעולות נפוצים הנכללים תחת הכותרת הזו. חלקם מוסדרים ישירות בחקיקה ראשית, חלקם מעוגנים בפקודת העיריות, ואחרים מקור ההסמכה שלהם אינו ברור דיו לפי שעה. בחלק מן המקרים ישנם כללים משפטיים נוספים. בשורות הבאות ייבחנו בקצרה השירותים העיקריים העולים מן הראיונות: חיישני אשפה, תשתיות דיגיטליות כמו איסוף מידע על צריכת מים ואיגום מאגרי מידע בתוך הרשות, יישומונים (אפליקציות) פרטיים שהופכים לחלק מחיי היומיום בעיר ושירותי אינטרנט אלחוטי (WiFi), כרטיסי תושב, ומצלמות אבטחה או מעקב במרחב הציבורי.²⁷ זו רשימה שאינה ממצה, ובמקומות שונים בעולם אפשר לראות מערכות

²⁷ כל אחד מן השירותים הללו מעלה סוגיות חברתיות ומשפטיות נוספות, שלא נרחיב עליהן כאן. כך למשל, כאשר רשות מקומית מעמידה רשת אינטרנט אלחוטית לשימוש התושבים, עשויות לעלות שאלות של חופש ביטוי: האם מותר לרשות להגביל את הביטויים ברשת הזו? לדיון, ראו: Enrique Armfio, "Government-Provided Internet Access: Terms of Service as Speech Rules," *Fordham Urban Law Journal* 41 (March 2016): 1500–1524; Timothy Zick, "Clouds, Cameras, and Computers: The First Amendment and Networked Public Places," *Florida Law Review* 59 (2007): 06–0062. סוגיה אחרת שהתעוררה בארצות הברית היא מתחום ההגבלים העסקיים והמשפט המנהלי: ספקיות אינטרנט נאבקות ברשויות מקומיות שהציעו גישה חנימית לאינטרנט אלחוטי. לדיון, ראו: Adam Christensen, "Wi-Fi'ght Them When You Can Join Them? How the Philadelphia Compromise May Have Saved Municipally-Owned Telecommunications Services," *Federal Communications Law Journal* 58 (2006): 683–704

המידע של התושבים אינו יכול להיות מקור להכנסות לעירייה, ואין לסחור בו סתם כך.

העירייה אינה יכולה להתחמק מחובותיה המנהליים בהפרשת שירות מסוים לגוף פרטי.

נוספות, בין ביוזמת הרשות ובין ביוזמת תושבים;²⁸ ודאי נראה מערכות נוספות בעתיד, כגון מערכות זיהוי ביומטריות שיופעלו במשולב עם מצלמות מעקב או באופן אחר,²⁹ מעקב באמצעות רחפנים או מערכות שונות כמו מכוניות אוטונומיות, ששוב ישנו את אופי החיים העירוניים.³⁰ כל מערכת שכזו מעלה סוגיות משלה, אך הדיון כאן נועד לתת מסגרת כללית כדי לבחון את היבטי הפרטיות שעשויים להתעורר.

• **חיישני אשפה.** דוגמה ראשונה זו ממחישה את הצורך בבירור משפטי. בכמה רשויות מיישמים אמצעים אלקטרוניים שונים לבירור נפח האשפה בפחי האשפה.³¹ מידע שכזה, שנאסף באמצעות חיישנים שונים, יכול לסייע לעירייה לתכנן טוב יותר את מסלולי איסוף האשפה ואת תדירות האיסוף. היתרון ברור – שירות טוב יותר, יעיל יותר וחסכוני יותר. המידע הוא על הפחים, לא על בני אדם. משקלו ונפחו של פח אשפה שממוקם באזור מסחרי הומה אדם אינו מזהה אנשים. אולם בשכונות של בתים צמודי קרקע, שלכל אחד מהם פח אשפה נפרד משלו, משקל האשפה והנפח שלה הם נתונים שמוצמדים לפח מסוים בכתובת מסוימת. מאחר שהמידע על זהות בעלי הבית הוא פומבי (מתפרסם במרשם המקרקעין – הטאבו), זכות הדיירים בבית (ככל שהם אינם הבעלים, אלא שוכרים למשל) ידועה לעירייה (ממרשם משלמי הארנונה), ובכלל זה ילדים שגרים שם (ממרשם התלמידים), הרי מושאי המידע ניתנים לזיהוי. המידע עשוי להעיד מי נמצא הרבה בביתו ומי פחות, באילו מועדים וכן הלאה. מידע שכזה עשוי לעניין סוחרים שונים, כמו גם פורצים וחברות ביטוח, והוא עשוי לעניין את העירייה עצמה, כאינדיקציה למידת השימוש בנכס, מידע שעשוי להשפיע למשל על גובה הארנונה. כך, גם מאגר מידע תמים לכאורה עשוי לבוא בגדר המסגרת המשפטית.

• **"תשתיות חכמות"** (smart grid) נוגעות להמרת מערכות אספקה חד־כיוונית של חשמל, של מים, של גז וכדומה במערכות דיגיטליות דו־כיוונית.³² כיום כאשר אנו פותחים את ברז המים, ישנו מונה דירתי או מונה של הבית המשותף שמסמן את היקף הצריכה, ונתון זה משמש לחישוב התשלום בידי תאגיד המים העירוני. המידע אינו מפורט. ניתן ללמוד ממנו באופן השוואתי, למשל מי צורך יותר מים מהמוצא, או אם בפרק זמן ממושך אין צריכה בכלל – אפשר ללמוד ממנו שאין גרים בבית.³³ במערכת "חכמה" כל פתיחה של ברז המים תתועד בזמן אמת. מערכת שכזו תאפשר לאיסוף מידע על מועד השימוש ועל היקפו. בהצלבה עם נתונים סטטיסטיים כלליים יהיה אפשר לשער אם הדייר השתמש בשירותים, התקלח, הפעיל מכונה לשטיפת כלים או מילא מים בקומקום. מידע שכזה משקף את אורחות החיים של אנשים בצורה מדויקת בהרבה, וודאי יימצאו לו שימושים מסחריים שונים. האם תאגיד המים העירוני

28 ראו למשל מערכות מידע שכונתיות במקומות שונים בארצות הברית (neighborhood information systems), שאוספות מידע סטטיסטי לא־מוזה על אירועים בשכונה, כגון לידות, פשיעה או הישגים של תלמידים: Steven J. Balla, "Municipal Environments, Nonprofit Entrepreneurs, and the Development of Neighborhood Information Systems," *I/S Journal of Law and Policy for the Information Society* 5, no. 1 (2008): 117–140

29 חוקר אמריקני סבור, ששימוש בזיהוי ביומטרי במרחב הציבורי הוא בגדר "חיפוש" לא־חוקי שאסור לפי התיקון הרביעי לחוקה האמריקנית. ראו: Marc Jonathan Blitz, "The Dangers of Fighting Terrorism with Technocommunitarianism: Constitutional Protections of Free Expression, Exploration, and Unmonitored Activity in Urban Spaces," *Fordham Urban Law Journal* 32 (2004): 667–721

30 לדיון ראשון בהיבט הפרטיות של מכוניות אוטונומיות, ראו: Dorothy Glancy, "Sharing the Road: Smart Transportation Infrastructure," *Fordham Urban Law Journal* 41 (2013): 1617–1664

31 כך למשל בהרצליה, באילת, בבאר שבע, בירושלים, ושוקלים ליישם זאת בערים נוספות.

32 לדיון בהיבטים הרגולטוריים של רשתות כאלה, ראו: Kevin B. Jones et al., "The Urban Microgrid: Smart Legal and Regulatory Policies to Support Electric Grid Resiliency and Climate Mitigation," *Fordham Urban Law Journal* 41 (2014): 1695–1759

33 דוגמה זו עלתה גם בראיונות, כך למשל דרור מרגלית, (סגן לטכנולוגיות, ישראל דיגיטלית, המשרד לשוויון חברתי), 1.12.2016.

רשאי לאסוף את המידע ולמכור אותו, למשל, לחברה שמציעה מוצרים לחיסכון במים? המידע נוצר אגב אספקת השירות. אנו סבורים, שכל שימוש במידע מעבר למטרה של אספקת השירות עצמו מחייבת עוגן חקיקתי מסמך. חיוב החשבון או זיהוי של דליפות מים הם בגדר אספקת השירות; מכירת מידע לצד שלישי אינה בגדר השירות הבסיסי. תאגיד מים שיבקש לאסוף מידע למטרה שכזו לא יוכל להסתמך על הסמכות הכללית הקיימת, ויצטרך לפעול לפי המתווה של פרק ב לחוק: תאגיד המים יצטרך ליידע את הלקוחות בדבר האפשרות של איסוף המידע, לבקש הסכמה (וזו צריכה להיות הסכמה מדעת), לשמור על המידע ולא להשתמש בו למטרות חדשות וכן הלאה, כמפורט לעיל. מובן שיהיה אסור להתנות את שירות אספקת המים בהסכמה לשימושים נוספים, שאחרת יהיה קשה לומר שמדובר בהסכמה חופשית.

• **איגום מאגרי מידע.** לרשויות היו מאז ומעולם מאגרי מידע שונים על תושבי העיר, בעבר בנייר וכיום בצורה אלקטרונית דיגיטלית. האם מותר לעירייה להצליב את המידע שיש לה למשל ממרשם התלמידים שהיא מנהלת עם מידע שיש לה על מי שביקשו תו חנייה עירוני? עירייה עשויה להתעניין בהצלבת מידע שכזה כדי ללמוד על דפוסי התנהגות שונים של התושבים, כדי לשפר שירותים וכדומה. לעירייה יש סמכות נפרדת לכל מאגר, וכל עוד ההצלבה מיועדת לעיבודי מידע נוספים כדי לשפר את הביצוע של השירותים האלה, נראה שאין מניעה לאגם את המאגרים. השימושים החדשים באים בגדר המטרה המקורית. אולם אם איגום המאגרים נעשה למטרה חדשה, הרי יש להצביע על מקור סמכות לפעולה החדשה, על התכלית – ולשכנע שהיא ראויה – ולאסוף את מינימום המידע הדרוש למימוש התכלית הזו, ולא יותר.

• **אינטרנט אלחוטי, שירותי תחבורה.** שירותים חדשים שהעירייה בעיר בעידן הדיגיטלי מציעה, כמו פריסה עירונית של גישה אלחוטית חנימת לאינטרנט, שירותי אופניים או מכוניות בהשכרה (דוגמת תל־אופן או תל־אוטו) מחייבים בדיקה פרטנית: מהו סוג המידע שנאסף? האם המידע מזהה? כך למשל, כאשר העירייה מספקת גישה אלחוטית לאינטרנט, האם היא אוספת מידע על המשתמשים? אם לדוגמה המשתמשים נדרשים להירשם בצורה מזהה, או שנאסף מידע אחר שממנו אפשר לזהותם, הרי הדיון חל, והעירייה יכולה לבחור באחד משני אפיקים משפטיים: האחד הוא להצביע על מקור הסמכה בחוק, ולפעול לפי המתווה החוקתי; האחר הוא לפעול לפי המתווה של פרק ב לחוק הגנת הפרטיות. במקרה שכזה דרוש יידוע, דרושה הסכמה, העירייה כפופה לעקרון צמידות המטרה, לחובת הסודיות ולחובת אבטחת המידע, ועליה לאפשר גישה ותיקון של המידע, כמו גם לרשום את המאגר אצל רשם מאגרי המידע. כל זה חל למשל במקרה של שירותי השכרת האופניים והרכב בתל־אביב, אך לא בהכרח בנוגע לשירותי האינטרנט.

• **כרטיסי תושב** הם מקרה חשוב אחר, והדוגמה המובילה היא של כרטיס דיגיטל בתל־אביב. מאחר שאין בפקודת העיריות הסמכה מיוחדת לכרטיסים שכאלה, האפיק שיש לעירייה הוא לפעול לפי פרק ב לחוק הגנת הפרטיות – ליידע את התושבים באשר לאיסוף המידע, לבקש את הסכמתם מדעת וכן הלאה. לפי תקנון השירות, מטרת הכרטיס היא "קידום רווחת תושבי העיר, שיפור השירות וחיזוק הקשר בין העירייה לתושב" (סעיף 2 לתקנון).³⁴ הכרטיס מקנה הטבות שונות (סעיפים 16–20 לתקנון). במסגרת החברות נדרשים התושבים להזדהות (סעיפים 6–10 לתקנון), כלומר חוק הגנת הפרטיות צריך לחול במלואו. העירייה מאפיינת את התושבים בדרכים שונות.³⁵

34 לתקנון דיגיטל, ראו באתר עיריית תל־אביב-יפו בכתובת: <https://www.tel-aviv.gov.il/Residents/Digital/Pages/Terms.aspx>

35 כך עולה מסעיף 17 לתקנון: "העירייה ו/או דיגיטל שומרים על הזכות להעניק חלק מההטבות לחלק מהחברים, בהתאם למאפיינים רלבנטיים של החברים, כפי שייקבעו על ידי העירייה ו/או דיגיטל".

כל שימוש במידע מעבר למטרה של אספקת השירות עצמו מחייבת עוגן חקיקתי מסמך. מכירת מידע לצד שלישי אינה בגדר השירות הבסיסי.

כל שירות ומערכת המבוססים על איסוף מידע בעיר הדיגיטלית מעלים סוגיות בהיבט של פרטיות.

במבט ראשון נראה שדיגיטל ועיריית תל־אביב פועלים לפי הדין, אולם חשוב לשים לב למרחבי העמימות שיש בתקנון.

ניכר שמנסחי התקנון היו ערים לחוק הגנת הפרטיות, שאף נזכר במפורש בתקנון, והם מיידעים את המצטרפים בקשר לכך שאין להם חובה חוקית למסור את המידע, שהמידע ישמש "לשבת דיגיטל ולמימוש משרותיו, לרבות באמצעות צדדים שלישיים ובלבד ששימוש כאמור לא יאפשר את זיהויו של החבר בידי צדדים שלישיים" (סעיף 21.2 לתקנון). התקנון מבהיר, שהמידע יוצלב עם מידע ממרשם האוכלוסין (סעיף 21.3), ושהמידע יעובד ויונתח (סעיף 21.4). מאגר המידע נרשם כחוק (סעיף 22.1) שמפרט את מספר המאגר אצל רשם מאגרי המידע). עם זאת העירייה שומרת לעצמה את הזכות לשנות את התקנון (סעיף 26), ומנסה לנכס לעצמה את הסמכות הבלעדית לפרשנותו ("הסמכות הבלעדית לפרשנות הוראות התקנון הינה בידי העירייה", כאמור בסעיף 27). במבט ראשון נראה שדיגיטל ועיריית תל־אביב פועלים לפי הדין, אולם חשוב לשים לב למרחבי העמימות שיש בתקנון. **המטרה** מנוסחת באופן כללי מאוד; האם העירייה יכולה להציע שירותים בתשלום לתושבי העיר מבלי להעביר את המידע לצד שלישי? האם העירייה יכולה להשתמש במידע בקשר לגביית חובות? האפשרות החד־צדדית לשינוי התקנון פוגמת במשמעותה של הסכמה, ואם שינוי שכזה ישפיע על השימושים במידע, ספק אם הוא יכול להכשיר סטייה מן המטרה המקורית. **ההוראה הפרשנית החריגה** מבקשת לאפשר לעירייה להרים את עצמה בשרוכי נעליה שלה; ספק אם יהיה לה תוקף בבחינה שיפוטית, אולם עשוי להיות לה אפקט מרתיע לתושבים שיבקשו לפנות לבית משפט.

• **מצלמות עירוניות**. רשויות רבות מתקינות מצלמות במרחב הציבורי בשנים האחרונות. המטרה המוצהרת היא בדרך כלל ביטחונית – מניעת פשיעה וטרור. חלק מן הרשויות פועלות בהיבט זה במסגרת פרויקט "עיר ללא אלימות" של המשרד לביטחון פנים, ואז מוסיפות למטרותיהן גם צמצום של "התנהגות אנטי־חברתית" ו"הגברת תחושת הביטחון של התושב".³⁶ ב"זירות" אפשר למצוא בתי ספר ופארקים ציבוריים, אבל גם חופי ים, תחנות אוטובוס ועוד. לכל אחת מן הזירות הללו מאפיינים ייחודיים, וכניסתם של אמצעי מעקב משנה את מערך יחסי הכוחות שבאותה זירה.³⁷ במישור העקרוני עולה השאלה, אם יש לאדם פרטיות במרחב הציבורי, והתשובה בספרות המחקר היא חיובית.³⁸ הדין האירופי במיוחד אינו מתעניין באופיו של המקום שבו נמצא האדם, אם הוא פרטי או ציבורי, אלא באדם עצמו – אם הוא ניתן לזיהוי או לא. ואכן כאשר אדם נמצא במרחב הציבורי צופים בו אנשים אחרים, אולם המבט האלקטרוני שונה; הוא "זוכר" את המידע על מיקומו של אדם, הוא מדויק, ואין בו את הממד של נורמות חברתיות שיש בין אדם לחברו. כך, מטופלים שרואים זה את זה בחדר המתנה לרופא, משתתפים בקבוצות טיפוליות שונות כמו אלכוהוליסטים אנונימיים או קבוצות לנפגעי נפש או מבקרים במועדונים של הקהילה הלהט"בית לא ימהרו לשתף את המידע על נוכחות אנשים אחרים. לא כך הוא כאשר מדובר במערכות מעקב מבוססות־טכנולוגיה.³⁹

36 ראו את אתר הפרויקט בכתובת: https://www.gov.il/he/Departments/topics/city_without_violence, ובמיוחד את ההסברים על "תחום האכיפה" שם.

37 ראו למשל את השינויים הפדגוגיים בבתי ספר בישראל בעקבות כניסת מצלמות למרחב החינוכי: Lotem Perry-Hazan and Michael Birnhack, "The Hidden Human Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy, and Trust," *Cambridge Journal Of Education* 48, no. 1 (2018): 47–64

38 לדין, ראו Edwards, "Privacy, Security and Data Protection"

39 סוגיה זו קשורה לשאלה רחבה יותר, של ההבחנה שבין הפרטי לציבורי. לדין, ראו: Helen Nissenbaum, "Toward an Approach to Privacy in Public: Challenges of Information Technology," *Ethics & Behavior* 7, no. 3 (1997): 207–219

העוגן המסמיך להתקנת מצלמות ולשימוש בהן נמצא כיום בפקודת העיריות.⁴⁰ **התכלית** צריכה להיות ראויה. רשות שתאמר למשל, שהתכלית היא לחנך את התושבים שלא לדרוך על דשא בגינה ציבורית, תצטרך לשכנע שזו תכלית המעוגנת בפקודת העיריות ושהיא תכלית ראויה, המצדיקה פגיעה בפרטיות. **האמצעי** צריך להיות מידתי. בשנת 2012 פרסם רשם מאגרי המידע (שהוא ראש הרשות למשפט, טכנולוגיה ומידע כשמה אז) הנחיות בדבר "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן".⁴¹ ההנחיות מבהירות כי השימוש במצלמות צריך להיבחן בתנאי פסקת ההגבלה החוקתית, וכי לפני קבלת החלטה על הצבת מצלמות "יש לערוך בדיקה מקיפה של השלכת השימוש במצלמה על זכויות הציבור ובמיוחד על הזכות לפרטיות". ההנחיה קובעת כללים מנחים מפורטים, כך למשל באשר למיקום המצלמות ולזווית הצילום, באשר למספר המצלמות, זמני הצילום, הרזולוציה של התמונה ואיכותה, חובת יידוע של הציבור, זמנים לשמירת הצילומים ועוד. ההנחיה משקפת את עמדת הרשם בנוגע לחוק ומנחה אותו בקשר להפעלתו.

במקרים מיוחדים אפשר למצוא עוגנים משפטיים ייעודיים, כמו למשל הסמכות להתקין מצלמות בנתיבי תחבורה ציבוריים.⁴² בתקנות המתאימות יש פירוט שמשקף את עקרונות הגנת המידע ואת העקרונות החוקתיים. כך למשל, נדרש אישור של מליאת מועצת הרשות המקומית להצבת מצלמה נייחת; התקנות מנחות, שהמצלמה תוצב כך שזווית הצילום שלה תכסה ככל הניתן רק את החלק הדרוש לתיעוד העבירה ושמשפר המצלמות הדרוש יהיה המינימלי; התקנות מטילות חובה ליידע את הציבור, חובה לשמור את המאגר בנפרד מכל מאגר אחר, חובת סודיות, חובת אבטחת מידע וכן הלאה.

3. הסיכונים שבשימוש במידע

לכאורה המטרות השונות שנמנו לעיל הן חשובות וראויות. ואכן כך: אם מצלמות יכולות למנוע פשיעה או לסייע בתפיסת עבריינים – מה טוב; אם מערכות יכולות להוזיל עלויות של השירותים השונים ולהציע שירותים חדשים – מה טוב. אולם החשש הוא לפגיעה בפרטיות, בכמה רבדים.

ראשית, ברובד העקרוני, תפקיד הרשות הוא לפעול למען הציבור והתושבים, ולא לרגל אחריהם. ככל שנאסף מידע כך נפגעת הזכות לפרטיות של האזרחים. זהו המובן של "האח הגדול", גם אם כוונותיו מקורן בתום לב. החשש הוא של אפקט מצנן, של מי שיימנעו מפעולות חוקיות ולגיטימיות רק בגלל העין הבוחנת של הרשות – בין אם מדובר במסיבת חוף, ביחיד או בזוג שמבקשים להתבודד, ובין אם מדובר במי שמבקש לחיות בצורה שונה מהמקובל, וכעת יידרש לתת דין וחשבון משום שיסומן כיוצא דופן לעומת הכלל. זכויות האזרח מגבילות את הרשויות, ואין להן רשות לעשות ככל העולה על רוחן, גם אם כוונותיהן טובות. כפי שקלסי פינץ' ועומר טנא מדגישים, הפגיעה בפרטיות בעיר מתעצמת, משום שלתושבים אין חלופות של ממש.⁴³ הם אינם יכולים להימנע מלהיות במרחב הציבורי או משימוש במערכות תחבורה שונות. פינץ' וטנא מציינים פגיעות עקרוניות נוספות. אחת מהן, שתידון גם בהמשך הפרק, היא שהמערכות

40 סעיף 249(29) לפקודת העיריות (נוסח חדש) קובע סמכות "לעשות בדרך כלל, כל מעשה הדרוש לשם שמירה על תחום העיריה, בריאות הציבור והבטחון בו", וסעיף 249(33) קובע סמכות "להסדיר עניינים של שמירה, אבטחה וסדר ציבורי בתחומה, בנושאים, בתנאים ובסייגים שקבעו [שר הפנים] והשר לביטחון הפנים כאחד, בהסכמת שר המשפטים".

41 ראו: משרד המשפטים - הנחיית רשם מאגרי מידע מס' 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן" (21.10.2012), <http://www.justice.gov.il/Units/liita/subjects/HaganatHapratiyut/MeidaMerasham/Hanchayot/42013.pdf>.

42 ראו תקנות התעבורה (הפעלת מצלמות בידי רשות מקומית לשם תיעוד שימוש שלא כדין בנתיב תחבורה ציבורית), התשע"ז-2016.

43 Kelsey Finch and Omer Tene, "Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town," *Fordham Urban Law Journal* 41 (2014): 1581–1759

תפקיד הרשות הוא לפעול למען הציבור והתושבים, ולא לרגל אחריהם.

הפגיעה בפרטיות בעיר מתעצמת, משום שלתושבים אין חלופות של ממש. הם אינם יכולים להימנע מלהיות במרחב הציבורי או משימוש במערכות תחבורה שונות.

ישנה סכנה מובנית בשל שינוי האיזון במערכת היחסים שבין הרשות לאזרח; ישנו חשש של זליגת השימוש למטרות אחרות, וישנה סכנה של שימוש לרעה במידע בידי מי שיש להם גישה אליו.

העירוניות השונות בעיר החכמה "מנרמלות" – כלומר מרגילות – את התושבים לכך שאיסוף מידע הוא חלק בלתי־נפרד מחיי היומיום.⁴⁴

שנית, יש חשש לשימוש לרעה במידע מצד מי שיש להם גישה למידע.⁴⁵ ניצול שכזה יכול להיות לשם בירור על אדם אחר או לשם מכירת המידע לגורם מתעניין. ניצול נוסף לרעה הוא שהמידע עלול לשמש לאפליה. המידע שנצבר בידי הרשויות עשוי להיות מפורט ומדויק, וכפי שפינץ' וטנא מציינים, בשילוב עם טכנולוגיות של נתוני עתק, התוצאה עשויה להיות של אפליה שאחרת אסורה על פי חוק.⁴⁶ שלישי, יש חשש לזליגת שימושים בידי הרשות עצמה, לשימושים שלגביהם מושאי המידע לא יודעו ולא הסכימו.

התמונה הכללית שמתקבלת היא זו: הרשות העירונית יכולה, כעניין טכני, לאסוף מידע רב יותר מאי פעם, מסוגים שונים. המידע יכול להתייחס לתושבי העיר, לכלול מידע אישי על מקום מגוריהם, על מצבם המשפחתי (האם יש להם ילדים במערכת החינוך?), על מצבם הרפואי והפיננסי (מי שזכאים לסיוע מרשות הרווחה), על אורחות חייהם (היקף השימוש בפחי האשפה, בתשתיות או בהטבות שהעירייה מעניקה), על התנהגותם במרחב הציבורי (באמצעות מצלמות שונות), וככל שהעירייה משתפת את המידע עם גורמים אחרים – מידע נוסף. המידע יכול לשמש לשיפור השירות לאזרחים ולייעול השירות, אולם יש בו סכנה מובנית בשל שינוי האיזון במערכת היחסים שבין הרשות לאזרח; ישנו חשש של זליגת השימוש למטרות אחרות, וישנה סכנה של שימוש לרעה במידע בידי מי שיש להם גישה אליו.

האתגר של העיר בעידן הדיגיטלי הוא ליזום שירותים ומערכות חדשות לטובת האזרחים והתושבים, לעודד חדשנות ושימוש נכון ויעיל יותר בכספי המיסים של התושבים כדי לממש את תפקידה השלטוני, אך לעשות את כל זה מבלי לפגוע בזכות הפרטיות, לפחות לא במידה העולה על הנדרש לשם השגתה של התכלית הראויה.⁴⁷ כעת אפשר לפנות ולבחון כיצד מתבצעים הדברים בפועל.

4. התאמת המסגרת המשפטית

כיצד אם בכלל יכולה המסגרת המשפטית הכללית של הגנת מידע אישי שהוצגה לעיל לחול על איסופי המידע השונים ועל עיבודיו בהקשרים השונים? הקושי נובע ממאפייני המידע שנאסף כ"נתוני עתק", שבהם השימוש שיהיה במידע אינו ידוע בהכרח בשלב האיסוף,⁴⁸ ממקור האיסוף של המידע במרחב הציבורי ומזהות השחקנים שבהם מדובר – הרשות ומולה האזרח.

44 שם, 1601.

45 מקרים שכאלה מגיעים מעת לעת לבתי הדין למשמעת או לבתי המשפט. ראו למשל מ"ח 7/07 ברמן נ' מדינת ישראל (2007) (פורסם בנבו, 22.8.2007) (מפקח ברשות המיסים ביצע שאילתות על אדם שהיה מסוכסך עימו); ע"פ 4496/14 פלוני נ' מדינת ישראל (2015) (פורסם בנבו, 4.5.2015) (חוקר במשטרה הוציא מידע ממאגרי מידע משטרתיים על נשים שהגישו תלונות שונות); ת"פ (שלום, י-ם) 10845-06-15 מדינת ישראל נ' רימר (2017) (פורסם בנבו, 11.6.2017) (עובדת במשרד החוץ בדקה מידע על אדם מסוים שהיה בסכסוך כספי עם בנה).

46 Finch & Tene, "Welcome to the Metropticon," 1602

47 סוגיה נוספת היא של "מידע פתוח" (open data). גישה זו קונה לה אחיזה, גם אם אישית, בתפיסה שעל השלטון מוטלת חובה להנגיש חנינם מידע של הציבור. מידע שכזה יכול לשמש שחקנים בשוק כדי להציע שירותים חדשים (כגון יישומונים שמתבססים על מידע מחברות תחבורה ומן הרשויות, על מנת להציע מידע בדבר אפשרויות נסיעה בעיר) או לצורכי מחקר. בהקשר הנוכחי החשש הוא, שהמידע הפתוח יאפשר לזהות תושבים וכך לפגוע בפרטיותם. מתעוררות כאן סוגיות נוספות, למשל של קניין רוחני במידע. לדיון, ראו: Teresa Scassa, "Public Transit Data Through an Intellectual Property Lens: Lessons About Open Data," *Fordham Urban Law Journal* 41 (2014): 1759–1789

48 לקוצר היד של הדין בהתמודדות עם נתוני עתק, ראו: Omer Tene & Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property* 11, no. 5 (2013): 239–273; Kate Crawford and Jason Schultz, "Big

מן הדברים עולה התמונה הבאה: אין הסדרה משפטית ייחודית של ערים דיגיטליות או של פעילות הרשויות הנוגעת למיזמים טכנולוגיים ספציפיים שקשורים לעיר. רשויות מקומיות כפופות לדין הכללי של פקודת העיריות ולדיני הפרטיות. איסוף המידע ועיבודו צריכים לעמוד בדרישות חוק היסוד; כלומר אם ישנה פגיעה בפרטיות הרי דרושה הסמכה בחוק, אשר עשויה להימצא בפקודת העיריות או בחוק מסמך ספציפי, הפגיעה צריכה להיות לתכלית ראויה, ובעיקר – עליה להיות במידה שאינה עולה על הנדרש. הרשויות צריכות לוודא שהן אינן מפרות את הפרטיות הקלאסית של התושבים (כך למשל צילום ברשות היחיד או האזנת סתר בכל מקום), והן צריכות לציית גם להסדר של מאגרי מידע, ככל שישנו מאגר מידע.

כל רשות נדרשת לבחון את ההיבטים המשפטיים הללו באשר לכל מערכת טכנולוגית חדשה שהיא מבקשת להטמיע. ברשויות שונות עשויות להיות נסיבות ייחודיות שיביאו לתוצאה שונה, ולכן כל רשות אחראית לקבל החלטה עצמאית. התעלמות משיקולים רלוונטיים עשויה להביא לפסילת ההחלטה. מובן שלרשות מותר לשקול רק שיקולים ענייניים, ואסור לה לשקול שיקולים זרים.

משמעות הדברים היא, שדרושה עבודת מטה ברשות המקומית כחלק מן התכנון ולפני ההשמעה שלה בשטח. לשם כך דרושים תהליכים פנים־ארגוניים. על הרשות לברר את התכלית שלשמה נאסף המידע, להגדירה ולבחון את הלגיטימיות שלה. הרשות צריכה להצביע על עוגן מסמך בחקיקה, ועליה לפעול לפי עקרון המידתיות; עליה לבחון חלופות שאינן כרוכות בפגיעה בפרטיות, ואם אין מנוס מפגיעה זו – לאסוף את מינימום המידע הדרוש, ולציית להוראות השונות שבדין. חלק מהוראות אלה ניתנות ליישום בצורה פשוטה יחסית, כמו רישום מאגר המידע אצל רשם מאגרי המידע. דרישות אחרות שיש בדין קשות יותר ליישום.

הקושי המרכזי הוא דרישת ההסכמה. כאשר המידע נאסף בעיר אגב תנועה ושימוש רגיל במרחב הציבורי, אין יכולת של ממש ליידע כל תושב בנפרד ולבקש את הסכמתו, שצריכה להיות הסכמה מדעת ומרצון חופשי. בהינתן תנאי העיר, בנוגע לשירותים רבים אין לתושבים חלופות של ממש; תושב יכול אמנם לבחור שלא להשתמש ברשת האינטרנט האלחוטית שהעיר מציעה, אך אין לו אפשרות להימנע ממבטן של מצלמות המעקב או מאמצעים אחרים האוספים מידע בתחבורה הציבורית. כאשר הרשות מבקשת לאסוף מידע בדרכים שכאלה, אין דרך ממשית אפקטיבית לקבל הסכמה. התוצאה היא פגיעה בפרטיות. פגיעה שכזו מותרת אם היא עומדת בתנאי פסקת ההגבלה שבחוק היסוד. אפשר למזער את הפגיעה, למשל בהצבת שילוט מתאים.

כאשר ישנה נקודת מפגש ישירה בין הרשות לבין התושבים, אפשר וחשוב לבקש את הסכמתם המפורשת – מדעת – ויש להקפיד שהיא תהיה מרצון חופשי. כך למשל באשר לשירותים כמו כרטיסי תושב, אולם רק כל עוד יש אפשרות לתושב לסרב מבלי להיפגע, שאחרת אין מדובר בהסכמה של ממש, ודאי שלא הסכמה חופשית. אם לדוגמה רישום ילדים לבתי הספר יותנה ב"הסכמה" לכרטיס תושב שמהותו היא איסוף מידע, הרי אין לומר שמדובר בהסכמה חופשית. אם מדובר בהטבות שאינן קשורות לשירותים הכרחיים, ניתן להתקדם ולבחון את התכלית של איסוף המידע ואת שאר המרכיבים.

Data and Due Process: Towards A Framework to Redress Predictive Privacy Harms," *Boston College Law Review* 55, no. 1, (2014): 93–128

אין הסדרה משפטית ייחודית של ערים דיגיטליות או של פעילות הרשויות הנוגעת למיזמים טכנולוגיים ספציפיים שקשורים לעיר.

דרושה עבודת מטה ברשות המקומית כחלק מן התכנון ולפני ההשמעה שלה בשטח. עליה לבחון חלופות שאינן כרוכות בפגיעה בפרטיות, ואם אין מנוס מפגיעה זו – לאסוף את מינימום המידע הדרוש.

אתגרים והזדמנויות: הזירה הישראלית

**ברשויות בישראל ישנה
התמקדות בהיבטים של
אבטחת מידע ופחות תשומת
לב להיבטים אחרים של
פרטיות.**

הראיונות שנערכו עם גורמים שונים ברשויות מקומיות, עם יועצים ועם גורמים בשלטון המרכזי עסקו גם בסוגיות של פרטיות. התשובות התמקדו בדרך כלל בסוג השירותים שמציעות הערים שבהן נערכו הראיונות. התמונה המצטיירת היא שישנה מודעות מסוימת לנושא, תוך הפניה מהירה לחוק, בדרך כלל במתכונת של אמירה בדבר הציות לחוק. אולם מעבר למודעות הכללית אפשר לראות התמקדות בהיבטים מסוימים של הפרטיות, בעיקר בסוגיה של אבטחת מידע, ופחות תשומת לב, אם בכלל, להיבטים אחרים של הפרטיות. אפשר לזהות גם שורה של הנחות חברתיות-תרבותיות של מקבלי ההחלטות, בדרך כלל ללא ביסוס עובדתי, ובמקרים אחדים בניגוד לממצאים של מחקרים בנושא. סוגיות מרכזיות שעלו בקשר לעצם הפרויקט הן של אמון הציבור במערכות העירוניות, ובעניין זה הודגשו היבטים של אבטחת מידע, של היעדר מסחור ושל ציות לחוק. הנה כמה דוגמאות.

זהר שרון, מנהל מנהלת הידע העירוני בעיריית תל-אביב, מסביר באשר לכרטיס התושב דיגיתל, שהוא גולת הכותרת של העירייה בהקשר של היותה "עיר חכמה":⁴⁹

"הרי העירייה לא בונה על [דיגיתל] ביזנס. אין לה צורך בזה...חשוב לנו כל הזמן לשמור על הניקיון של דיגיתל, זאת אומרת, לא לערב שום ביזנס בדבר הזה. כדי לא לגרום לתושבים שיחשבו שהנה, העירייה מנסה עכשיו לקחת עוד כסף ולהרוויח עוד, ממש לא...ועובדה שאנחנו מקבלים את האמון של התושבים. הנתונים מועברים לצד שלישי אך ורק לצורך ניהול הפרויקט, כמובן בצורה מאובטחת. הנתונים לא עוברים עם תעודת הזהות, הם עוברים עם תעודת זהות מוצפנת. אי-אפשר לזהות מי התושב. הצד השלישי לא יודע לזהות שום דבר".

שרון מדגיש את החשיבות של יצירת אמון בין התושבים לעירייה בהיבט של כרטיס התושב, וההיבט הזה מתורגם לשני מרכיבים – היעדר מרכיב עסקי והקפדה על אבטחת מידע. בהסבר הזה אבטחת מידע פירושה הגבלה של המידע שמועבר לצדדים שלישיים – המידע עובר בצורה שאינה אמורה לזהות את התושבים.

איציק כרמלי, מנמ"ר עיריית ראשון לציון, מציג עמדה דומה, שלפיה אין מועבר מידע לגורמים פרטיים חיצוניים: "לא רואה סיבה שכן נעביר. לא רואה סיבה שמישהו יאשר להעביר לגורם עסקי כלשהו כזה או אחר", אולם גם בראשון לציון, כמו בערים נוספות, מעבירים מידע למשטרה, לפי נהלים שגובשו בעניין.⁵⁰ בדומה, יוסי בן סימון, מנמ"ר עיריית אשדוד, מתאר את אחריות העירייה למידע של תושביה גם כשהוא עובר הלאה: "כשאתה מתחיל להזין תעודות זהות ומספרי טלפונים ומספרי רכב, זו כבר פרטיות שצריך להגן עליה, בוודאי. וכשזה עובר לחברה צד ג אתה צריך לוודא שקודם כול הם לא מעבירים את החומר לעוד גורם אחר, שהם מגינים עליו כמו שצריך".⁵¹

אדי בית הזבדי, מנהל אגף ניהול משאבי תשתית במשרד האנרגיה, מדגיש גם הוא את החשיבות של אבטחת מידע: "ברגע שהכנסת טכנולוגיה, דבר ראשון שאת צריכה לעשות זה לראות מה רמת אבטחת המידע שלך".⁵² סוגיה קשורה לכך היא השאלה בידי מי האחריות. בית הזבדי מזכיר את התפקיד של מנמ"ר – מנהל מערכות מידע ראשי – שקיים ברשויות מקומיות רבות, אך לא בכולן: "הרבה פעמים כשיש מנמ"ר הוא קצת יותר טכנאי, הוא מתעסק [בכך] שהמדפסת תעבוד ושהמחשבים יעבדו ... יש תמיד את השאלה האם הם צריכים להוביל את התהליכים או שיותר הביזנס צריך להוביל את התהליכים". מהסיבה הזו, הוא מסביר, רשויות רבות מסתמכות על השוק הפרטי שמספק את השירותים הדרושים.

49 זהר שרון (מנהל מנהלת הידע העירוני, עיריית תל-אביב), 10.8.2016.

50 איציק כרמלי (מנמ"ר ומרכז תוכנית עיר חכמה, עיריית ראשון לציון), 8.9.2016.

51 יוסי בן סימון (מנמ"ר, עיריית אשדוד), 25.9.2016.

52 אדי בית הזבדי (מנהל אגף ניהול משאבי תשתית, משרד האנרגיה), 18.8.2016.

בדומה, אלון אופיר, מנהל תחום דיגיטל וערים חכמות בעיריית נתניה, מסביר: "אנחנו פועלים לפי כל חוקי אבטחת המידע של המדינה, החוק לפרטיות, החוק לכבוד האדם".⁵³ מנמ"ר עיריית נתניה, ירון ריבו, מציג גישה דומה: "צריך להכניס את השיקולים של אבטחת מידע מתחילת הדרך... אני רוצה לקבוע מדיניות בנושא הזה, אני מביא יועצים חיצוניים של אבטחת מידע גם מבחוץ. ככל שאתה מעלה את נושא המידע בתחילת הדרך, אתה מביא לרמת אבטחה טובה יותר".⁵⁴

גם בעיריית הרצליה בחנו סוגיות של הגנה על מידע אישי בצורה דומה. האמצעים שנבחנו כללו לא רק "הצפנה" כתיאור כללי, אלא אפשרויות של ערפול מידע רפואי או טשטוש צילומים במצלמות המוצבות במרחב הציבורי, למשל.⁵⁵ גישתה של העירייה, כפי שמתארת באוזנינו סגנית ראש העירייה מאיה כץ, היא של בדיקה משפטית ושל יצירתיות: "ישבנו וחשבנו ועלו הרבה מאוד פתרונות, כי בסוף אתה צריך להיות מאוד יצירתי במסגרת החוק". גם בעיריית תל-אביב שמענו דברים דומים מזהר שרון, בעניין כרטיס התושב דיגיתל: "השירות המשפטי, בצדק, אמרו 'מה פתאום! אנחנו יכולים להתחזות אליך, לשים את מספר הארנונה שלקחו לך מתיבת הדואר ואת רישיון הנהיגה שלך. [לכן] הרישום צריך להיות פרונטלי. צריך להזדהות. אז הנה, מוצאים כל מיני פתרונות, אבל לא חורגים מהחוק".⁵⁶ הגישה של שמירה על החוק תוך ניסיון לאתר פתרונות יצירתיים עלתה גם בבאר שבע. יהוד מרסיאנו, מנהל אגף חדשנות ומערכות מידע בעיריית באר שבע, מסביר:

"השיקולים של הפרטיות ושל אבטחת המידע הם רלוונטיים לכל פרויקט שאנחנו נבצע. בעצם, לפני שאנחנו נבצע וכחלק מההכנה של התוכנית, זה יהיה על השולחן וזה ייבחן לעומק עם כל בעלי המקצוע... הסייבר וה- security זה משהו שצריך להסתכל עליו, צריך להתמודד איתו, אבל אסור שהוא יעצור אותנו. זאת אומרת, הוא לא יכול לעצור את הביזנס, הוא לא יכול לעצור את השירותים שאנחנו צריכים לתת לתושבים – תמיד אפשר למצוא פתרונות. תמיד".⁵⁷

ובאשר למצלמות עירוניות הוא אומר כך:

"אנחנו מאוד מקפידים על המאגר של המצלמות. זו גם רשת נפרדת אצלנו. יש שני אנשים שיש להם גישה בשוטף למידע. למשטרה אין גישה לנתונים – היא צריכה להגיש טופס מיוחד. אנחנו מאוד מקפידים על העניין של המידע מהמצלמות. יש את ההנחיות של רשות משפט וטכנולוגיה שהן עדיין לא נכנסו לתוקף, אבל אנחנו מכירים אותן על בוריין ואנחנו משתדלים – לפחות את הסבירות – ליישם, כי יש שם כמה דרישות באמת... אני לא יודע מי כתב את זה אבל אי אפשר פשוט ליישם אותן".⁵⁸

רבים מן המרואיינים מציגים עמדות אישיות שלהם בדבר מצבה של הפרטיות כיום, ונראה שמתוך המצוי – כפי שהם מאבחנים אותו – הם מסיקים את הלגיטימציה של פעילות הרשויות. כך למשל אבי בן-חמו, מנכ"ל עיריית נתניה, מספר:

"אנחנו כבר בדור שלנו לא הולכים לבנקים, עושים הכול באינטרנט, עושים העברות כספים, הכול. אז אין מה לעשות, חלק מההתפתחות שקורית בעולם היא הדבר הזה. עכשיו זה נכון ואנחנו יודעים שכשאתה משתמש באינטרנט וכשאתה משתמש בכרטיסי אשראי, אז יודעים את הצרכנות שלך ויודעים איפה אתה נמצא, זה חלק מהחיים, אין מה לעשות. זה חלק מההתפתחות. אני לא יכול להגיד שראיתי פה, וראיתי הפגנות בנתניה, לא ראיתי אפילו לא קמצוץ של פנייה אחת של מישהו שבא

53 אלון אופיר (מנהל תחום דיגיטל וערים חכמות, עיריית נתניה), 8.8.2016.

54 ירון ריבו (מנמ"ר, עיריית נתניה), 8.8.2016.

55 מאיה כץ (ממלאת מקום ראש העיר, וסגנית ראש עיריית הרצליה), 14.9.2016.

56 זהר שרון (מנהל מנהלת הידע העירוני, עיריית תל-אביב), 10.8.2016.

57 יהוד מרסיאנו (מנהל אגף חדשנות ומערכות מידע בעיריית באר שבע), 15.9.2016.

58 שם.

**רבים מן המרואיינים מציגים
עמדות אישיות שלהם בדבר
מצבה של הפרטיות כיום,
ונראה שמתוך המצוי – כפי
שהם מאבחנים אותו – הם
מסיקים את הלגיטימציה של
פעילות הרשויות.**

"כשאני מדבר על דיגיתל בעולם, הרבה הרבה ראשי עיר אומרים לי שזה הדבר הראשון שנראה להם שאין סיכוי שיצליחו לצלוח".

ואמר 'אתם הופכים להיות האח הגדול', לא. ההפך, אנשים צורכים את השירות הזה, יותר נכנסים, יותר פונים, יותר מצטרפים לפייסבוק".⁵⁹

רון ברזני, מנהל מנהלת אופק אזורי תעסוקה בעיריית מודיעין מכבים רעות, מתאר ציזון לחוק בדרך של יידוע הציבור, ובריזמינית הוא ממעט בחשיבות הצורך בכך:

"מכיוון שהפארק מצולם זה מכבר במערכת ה־safe city, ומכיוון שאנחנו הוספנו מצלמות ובפארק יש שלטים שמציינים שהפארק מצולם, זה מסוג הדברים שאנשים לא שואלים, אני חושב. שוב בציבור שלנו אנשים מבינים את זה. מסתכלים על זה ... לא ככלי שחודרים לפרטיות אלא זה מרחב ציבורי, והמרחב הציבורי מצולם, ואני יודע שהוא מצולם".⁶⁰

עמדה דומה נשמעת גם מסגן ראש עיריית תל-אביב, אסף זמיר:

"אתה יודע, אין בישראל פרטיות. כולם מכירים אותך, כולם מכירים את בת-דודה שלך, בגלל הצבא ובגלל הקטע היהודי. אז זה לא נראה להם מוזר, כולם פה קונים באינטרנט, כולם שמים את האשראי שלהם בכל מקום. נראה לי שכולם גם מבינים עד כמה אין לנו בעצם פרטיות בלאו הכי וזה ההבדל הגדול לעומת העולם... פה נותנים [את המידע הפרטי] בלי לחשוב אם זה משיג לך משהו. ודיגיתל משיג לך משהו, אתה מקבל כיסא יותר זול בים וכל מיני דברים כאלה. יש פה גם איזה ארון כנראה בעירייה, כנראה, שאומר אני מוכן לתת לך את הפרטים שלי. יש אותם לכל החברות, לקופת חולים שלי יש אותם ולאשראי שלי יש אותם אז למה לא לך? אבל זה מאוד מאוד חריג. כשאני מדבר על דיגיתל בעולם, הרבה הרבה ראשי עיר אומרים לי שזה הדבר הראשון שנראה להם שאין סיכוי שיצליחו לצלוח".⁶¹

למרות זאת, אסף זמיר מתאר את הניסיון הכושל של Woosh – חברה שהציבה ברזיות מים מינרליים בעיר, בחינם, וביקשה לאסוף מידע מהתושבים:⁶²

"איפה כן הייתה מחאת פרטיות מאוד מעניינת – ווש היה ניסוי בעיני מדהים בעל פוטנציאל רב שנכשל בצער, אולי גם בגלל התנהלות לא נכונה של היזמים שלו, של חינוך לשתיית מים בחינם. הם אמרו אנחנו ניתן לך מים בחינם, אנחנו נממן את זה שהמים יהיו באיכות של מים מינרליים שאתה קונה ב־10 שקלים. תעבור עם כוס ותמלא לך מים באיכות של מינרליים, קרים, איך שאתה רוצה, אנחנו נגיד לך כמה שתית כבר, אם שתית מספיק והכול, אתה רק צריך להכניס פרטים, וזה שהיא לא מחויבת אבל שיהיה את הפרטים שלך וזהו. הייתה נגד זה התקוממות גדולה וזה נכשל, ואנשים לא שותים מהברזיות. במקום, הם כן קונים מים מינרלים ב־10-12 שקלים בקבוק, כי לא הסכימו לתת את הפרטים. עכשיו יכולת גם בלי [לבקש מידע אישי]... הם היו קיצוניים מדי, לפעמים רעיון טוב הוא מתקדם מדי".

זהר שרון כורך את האבחנה בדבר אדישות הישראלים לפרטיותם לסוגיה של ארון:

"תמיד – בתחילת הדרך, אבל גם היום – מדברים על ה'אח הגדול', הסיפור הזה של אבטחת מידע. אבל תראו איזה גיחוך זה: זאת אומרת, כשאתה תושב בתל-אביב אין לך שום בעיה לתת לסופרמרקט שלך את תעודת הזהות שלך ולאפשר לו לעקוב אחרי הרגלי הקניות שלך. אין לך בעיה. כל ישראלי ממוצע שמגיע לקופה בסופרמרקט, הדבר הראשון ששואלים אותו: "מה תעודת הזהות? יש לך כרטיס מועדון?... אין לי בעיה לרוץ בפייסבוק ושכל העולם עוקב אחריי ויכול לדעת עליי הרבה מה קורה. אין לי בעיה בטוויטר, אין לי בעיה בוואטספיים. יש לי בעיה עם לתת לעירייה או למגזר הציבורי מידע כי הוא האח הגדול. שזה האבסורד הכי

59 אבי בן חמו (מנכ"ל עיריית נתניה), 8.8.2016.

60 רון ברזני (מנהל מנהלת אופק אזורי תעסוקה, עיריית מודיעין מכבים רעות), 26.8.2016.

61 אסף זמיר (סגן ראש עיריית תל-אביב), 7.8.2016.

62 הברזיות הוסרו בסופו של דבר. ראו עידו קינן "אפילו העירייה לא מצליחה להיפטר ממיזם המים של חברת ווש", **הארץ**, 24.9.2015.

גדול כי זה הגוף שבעצם איכשהו – במצב תקין – אמור לשמור עליך. הם אמורים לשמור על הפרטיות שלך, הם אמורים לשמור על המידע שלך, הם לא האויב".⁶³

והוא ממשיך ואומר, כי "אנחנו חיים בעידן שהאזרח צריך להבין את זה כבר, שנגמרה הפרטיות. אנחנו עדיין חושבים במונחים האלה של האח הגדול, מישהו שבכוונה רוצה... אין בכוונה. אין כבר אח גדול כזה". גישה דומה שמענו גם מיועצים חיצוניים, כך למשל נתן פרדיחי, סמנכ"ל קבוצת מערכות בחברת טלדור:

"אני חושב שכל מי שחושב שיש לו פרטיות הוא כנראה חולם. אין לו פרטיות, זה לא קשור לערים חכמות. מצלמות מצלמות אותנו כל הזמן, אני נמצא בבית מלון, נמצא עם אשתי באיזשהו מקום, שאני חושב שהוא פרטי, אין לי מושג מי מצלם אותי, מי מקליט אותי. יכולתם לא להגיד לי שאתם מקליטים אותי והייתם מקליטים אותי, על פי החוק מותר לכם. החוק מאפשר את זה".⁶⁴

יועצים אחרים מדגישים את חשיבות הפרטיות. כך למשל שי אפל מחברת הייעוץ דלויט, שעובדת עם המשרד לשוויון חברתי ועם עיריית באר שבע, מציין כי "אבטחת הסייבר והפרטיות הם נושאים מרכזיים בכל תהליך של טרנספורמציה דיגיטלית. ככל שיגבר השימוש בכלים דיגיטליים בערים, צפויים נושאים אלה להפוך לאקוטיים".⁶⁵ ירון ריבו, מנמ"ר בעיריית נתניה, שואף לאסוף מידע על התושבים לפי אפיון עצמי ולפי המיקום שלהם באמצעות כרטיס תושב: "כוונת העירייה לעבור מכרטיס תושב פיזי לדיגיטלי על מנת לספק לו הטבות לפי אזור בבתי עסק ולחזק את הכלכלה המקומית. לתת שירות ככל הניתן מכוון לצרכיו".⁶⁶ מנמ"ר עיריית אילת, אבינועם נהרי, ער לרגישות המידע שנאסף, אולם מסתמך למעשה על בורות התושבים בעניין:

"יש סיכון כלשהו. אי-אפשר להגיד שלא. יש לרשות כלים שיכולים גם למרר את החיים לתושבים אם רוצים, וצריך עוד פעם לדעת להשתמש בזה בצורה נכונה. אם אני יש לי מצלמה ליד הבית שלך, אני יכול לדעת מה קורה איתך, ואני יכול לחקור את העבר שלך, ואני יכול לדעת את הילדים שלך ומי נמצא איתך, ויש לזה השפעות מאוד רציניות. אני חושב שהתושבים לא מבינים עד כמה יש לרשות כוח, ואי-הידיעה גם נותן את השקט הזה".⁶⁷

לשאלה, אם יצאה הודעה לתושבי העיר באשר לאמצעים השונים שנקטים ואם נתבקשה הסכמתם, מפנה המנמ"ר את האחריות לדוברות העירייה.

מנגד ישנם מרואיינים שמזהים את הפרטיות כערך חשוב וראוי להגנה, ואינם ממעטים מערכו. כך מנמ"ר עיריית תל-אביב, ליאורה שכטר, מתארת מודעות גבוהה ורגישות לפרטיות:

"בהיבט של אבטחת מידע ופרטיות, אנחנו שומרים על המידע על התושב באדיקות, איננו חושפים מידע על תושב, לא לגורמי חוץ מחוץ לעירייה ולא לשימוש של מחלקות שונות בתוך העירייה. לדוגמה איננו משתמשים במידע על מנת לגבות יותר תשלומים, לא יגיע אדם בעת מימוש הטבה, לראות הצגה, ונגיד לו – אה, יש לך חוב בארנונה... הרעיון הינו שכל אחד מאתנו הוא תושב בעצמו ואף אחד מאיתנו, ברמה האישית, לא היה רוצה שיאספו עליו מידע. בכל סוגיה אנחנו מתייעצים עם היועץ המשפטי, מקבלים ייעוץ ואף הכתבה".⁶⁸

63 זהר שרון (מנהל מנהלת הידע העירוני, עיריית תל-אביב), 10.8.2016.

64 נתן פרדיחי (סמנכ"ל קבוצת מערכות חברת טלדור), 12.12.2016.

65 שי אפל (מוביל תחום העיר החכמה, דלויט ישראל), 25.12.2016.

66 ירון ריבו (מנמ"ר, עיריית נתניה), 8.8.2016.

67 אבינועם נהרי (מנהל אגף ארגון ושיטות ומנמ"ר, עיריית אילת), 23.11.2016.

68 ליאורה שכטר (מנהלת אגף מחשוב ומערכות מידע, עיריית תל-אביב), 1.11.2016.

"יש לי בעיה עם לתת לעירייה או למגזר הציבורי מידע כי הוא האח הגדול. שזה האבסורד הכי גדול כי זה הגוף שבעצם איכשהו – במצב תקין – אמור לשמור עליך".

"מי שחושב שיש לו פרטיות הוא כנראה חולם".

"יש סיכון כלשהו. אי-אפשר להגיד שלא. יש לרשות כלים שיכולים גם למרר את החיים לתושבים אם רוצים".



התמונה שעולה מן הראיונות היא, כי מקבלי ההחלטות ומנהלי המערכות ברשויות המקומיות ובסביבתם – בקרב היועצים ובקרב הממשלה – ערים לסוגיה של פרטיות. דגש ניכר מושם על אבטחת מידע, והרקע הטכנולוגי של רבים מן המרואיינים, שממלאים תפקידי מנמ"ר, מסביר את הדגש הזה. הובאו דוגמאות גם לאמצעים אחרים שנועדו לצמצם את איסוף המידע – עיבוד מידע אנונימי, טשטוש צילומים וערפול מידע. המרואיינים מדגישים כי הם פועלים לפי החוק, וחלקם אף מזכיר חקיקה או תקנות רלוונטיות, כמו למשל הנחיית רמו"ט בנוגע למצלמות במרחב הציבורי. הם גם מדגישים שהם פועלים לפי ייעוץ משפטי צמוד, אך במסגרתו הם מבקשים להיות יצירתיים. למרות הערנות הזו, חלק ניכר מן המרואיינים ממעט בערכה של הפרטיות. מרואיינים אלה סבורים כי ממילא אין לנו עוד פרטיות בחיי היומיום, ברור ועולה מכך כי הם סבורים שאין לה חשיבות גם בממד ובהקשר העירוניים. כאן אפשר לראות גם את ה"נרמול" של המעקב; כאשר בכל זירה והיבט של חיינו נאסף מידע, עוד זירה ועוד הקשר אינם מרגשים את העוסקים במלאכה יתר על המידה. הסבר נוסף הוא האמון. הרשויות מצפות מן התושבים לתת בהן אמון. למרות הגישה הזו של חלק מן העוסקים במלאכה, הם עדיין מנסים לבצע פעולות של הגנה על הפרטיות, בין בתחום אבטחת המידע, בין בנוגע להעברת המידע לצדדים שלישיים, ובעיקר בהסתמכות על ייעוץ משפטי.

מקבלי ההחלטות ומנהלי המערכות ברשויות המקומיות ערים לסוגיה של פרטיות. אך, למרות הערנות הזו, חלק ניכר מן המרואיינים ממעט בערכה של הפרטיות.

המלצות מדיניות בתחום הפרטיות

האתגר של מקבלי ההחלטות בערים עם תשתיות דיגטליות, הוא כיצד להשיג את המטרות של יעילות, חדשנות, ביטחון ובטיחות ובו־זמנית לשמור על זכות היסוד לפרטיות.

הכלים המשפטיים מספקים – או צריכים לספק – מורה דרך ראשוני למקבלי ההחלטות, אולם החוק לבדו אינו אמצעי מספיק להטמעת החשיבות של הפרטיות בקרב הרשויות. בין השיח הטכנולוגי לשיח המשפטי ישנם פערי שיח ידועים וקשים לגישור. בהתאם לכך ראוי, שלצד הכלים המשפטיים יופעלו גם כלים המלצתיים של פינץ' ושנא,⁶⁹ וכן המלצתה של ליליאן אדוארדס.⁷¹ המלצותיהם באו לפני כניסת ה־GDPR לתוקף, וכעת יש לגישות חוץ־משפטיות אלה ביטוי שם – בחוק עצמו.

האתגר של מקבלי ההחלטות בערים עם תשתיות דיגטליות הוא האתגר השלטוני המוכר מהקשרים רבים אחרים – גם וגם. הוא נוגע לשאלה, כיצד להשיג את המטרות של יעילות, של חדשנות, של ביטחון ושל בטיחות ובו־זמנית לשמור על זכויות היסוד, ובענייננו זכות היסוד לפרטיות.

מן הדיון עולה כי יש בנמצא מסגרת משפטית כללית, וליתר דיוק כמה מסגרות משפטיות. הרשויות כפופות להוראה הכללית של חוק היסוד, ואסור להן לפגוע בפרטיות התושבים, אלא בדרך שעולה בקנה אחד עם פסקת ההגבלה: הפגיעה מותרת רק כאשר היא נשענת על הסמכה חקיקתית ברורה, רק כאשר היא נעשית לתכלית ראויה ובמידה שאינה עולה על הנדרש להשגת אותה מטרה ראויה. הרשויות כפופות גם לחוק הגנת הפרטיות, הן לחלק העוסק במצבי פרטיות קלאסית, הסדר שהוא רלוונטי בייחוד לשימושים כמו מצלמות מעקב, הן לחלק העוסק במאגרי מידע. נכון למועד כתיבת שורות אלה המסגרת המשפטית הזו עדיין חסרה בישראל, וספק אם היא עומדת בסטנדרט האירופי החדש שנקבע ב־GDPR. בין לבין, ישנן הנחיות ספציפיות בודדות, כך למשל הנחיית הרשות להגנת הפרטיות (לשעבר רמו"ט) בדבר מצלמות במרחב הציבורי. ואולם בחוק היסוד, בחוק הגנת הפרטיות ובהנחיות אלה יש עדיין מרחב פרשני ניכר.

הכלים המשפטיים מספקים – או צריכים לספק – מורה דרך ראשוני למקבלי ההחלטות, אולם החוק לבדו אינו אמצעי מספיק להטמעת החשיבות של הפרטיות בקרב הרשויות. כיום – וכפי שעולה בצורה ברורה מן הראיונות – המלאכה מבוצעת בידי גורמי מקצוע טכנולוגיים ועירוניים שעניינם במידע, ושמירת הפרטיות מוטלת לפתחה של המחלקה המשפטית. בין השיח הטכנולוגי לשיח המשפטי ישנם פערי שיח ידועים וקשים לגישור.⁶⁹ בהתאם לכך ראוי, שלצד הכלים המשפטיים יופעלו גם כלים ארגוניים וטכנולוגיים. זו גם המלצתם של פינץ' ושנא,⁷⁰ וכן המלצתה של ליליאן אדוארדס.⁷¹ המלצותיהם באו לפני כניסת ה־GDPR לתוקף, וכעת יש לגישות חוץ־משפטיות אלה ביטוי שם – בחוק עצמו.

עד שיתוקן הדין הישראלי ברוח ההסדר האירופי אנו סבורים, בהמשך להצעות בספרות, שמוטב להקדים ולאמץ בפרקטיקה אמצעים ארגוניים־טכנולוגיים שונים, שמטרתם להביא להפנמה טובה יותר של הפרטיות בתהליכי קבלת ההחלטות בנוגע לעיר בעידן הדיגיטלי בישראל. אמצעים אלה מתאימים גם לדרישה המשפטית בדבר הליך מסודר של קבלת החלטות, והם יכולים לסייע בעת בדיקה שיפוטית של תהליכים כאלה; כך למשל, הם עשויים להראות שהרשות בדקה ביסודיות אמצעים מידתיים, כלומר אמצעים שעדיין יכולים להשיג את המטרות המצופות מהטכנולוגיה החכמה, אך תוך פגיעה מופחתת בפרטיות התושבים.

בשורות הבאות יוצגו כמה אמצעים ארגוניים שרשויות יכולות – ואנו סבורים שהן צריכות – לנקוט במסגרת עבודת מטה לקראת אימוץ טכנולוגיה חדשה, במהלך הטמעתה, ובניהול השוטף שלה.



תסקיר הגנת פרטיות (PIA) – לפני תחילתו של תכנון מערכת טכנולוגית חדשה בעיר, יש לבצע תסקיר שכזה. יש להגדיר את התכלית של המערכת, לבחון אם היא לגיטימית וראויה, ואם התשובה חיובית – ובהתאם – יש לגזור את סוגי המידע הדרושים. יש לבחון אם כל סוג מידע אכן דרוש להפעלת המערכת. יש לבחון אם ישנם אמצעים חלופיים להשגת התכלית הראויה. יש להגדיר אמצעים לאי־איסוף מלכתחילה של מידע עודף, או למחוק, לערפל ולהסיר מידע מזהה, לפי העניין. יש לנקוט אמצעים של אבטחת מידע להגנה מפני תקיפה חיצונית, אבל גם אמצעים של הטמעת סודיות בתוך המערכת. הטמעת החשיבות של הסודיות צריכה להיעשות בתוך הארגון – באמצעים טכנולוגיים של מידור ושל בקרת גישה, באמצעים חינוכיים של הדרכות ושל הסברים, ובדיעבד – במקרה הצורך – באמצעים משמעותיים.



מינוי ממונה הגנת פרטיות (DPO) – כיום חוק הגנת הפרטיות דורש רק תפקיד של ממונה אבטחת מידע, אולם הפרטיות היא כאמור רחבה מאבטחת המידע. כיום סוגיות הפרטיות נבחנות בראייה משפטית או בראייה טכנולוגית, ולא תמיד התוצאה מיטיבית. גורם בכיר בארגון, שיש לו גם הבנה משפטית וגם הבנה טכנולוגית וכמובן גם הבנה של צרכי העירייה והתושבים, יכול לתכלל את הפעילות. זהו הגורם שיהיה אחראי לביצוע תסקיר הגנת הפרטיות, על מעקב אחר יישומו ואשר ישמש גם כתובת לתושבים לברור זכויותיהם.



הנדסת פרטיות (privacy by design) – התוצאה המקווה של שני האמצעים הקודמים צריכה לבוא לידי ביטוי בתכנון המערכת הטכנולוגית שבה מדובר. דוגמאות לכך הן איסוף מידע סטטיסטי מראש ולא איסוף מידע מזהה ואז הסרתו, צילום מטושטש מלכתחילה או ערפול מידע בטכניקות שונות.



פיתוח מנגנוני שקיפות שלטונית עירונית – את פעילות הרשות בהיבטים האלה, יש להם השלכה על פרטיות התושבים, יש ללוות בשקיפות שלטונית כלפי האזרחים. לצד הסברים שיווקיים על הטוב שהעירייה מבקשת להעניק לתושבים, יש להסביר להם גם את המשמעות של איסוף המידע, את היתרונות, את הסיכונים ואת האפשרויות שלהם בנושא, בעיקר את האפשרות שלא להיכלל באיסוף המידע מבלי שזכויותיהם ייפגעו. ההסברים צריכים להיות נגישים, פשוטים וברורים. הנגישות צריכה להיות הן באתר העירייה ובפרסומיה השונים בדפוס, הן בצמוד לשירות שבו מדובר – בין אם מדובר ביישומון, במתקן, בטופס הרשמה לכרטיס תושב וכן הלאה. ההסברים נדרשים הן לפי החוק – דרישת היידוע שבעקבותיה מגיעה ההסכמה, הן מטעמים של אחריות שלטונית ושקיפות שלטוניים, שלהן מחויבות הרשויות בהיותן גופים מנהליים.

לצד הסברים שיווקיים על הטוב שהעירייה מבקשת להעניק לתושבים, יש להסביר להם גם את המשמעות של איסוף המידע, את היתרונות, את הסיכונים ואת האפשרויות שלהם בנושא, בעיקר את האפשרות שלא להיכלל באיסוף המידע מבלי שזכויותיהם ייפגעו.

69 ראו למשל Michael Birnhack, Eran Toch, Irit Hadar, "Privacy Mindset, Technological Mindset," *Jurimetrics Journal of Law, Science and Technology* 55, no. 1 (2014): 55–114.
70 Finch & Tene, "Welcome to the Metropticon," 1607
71 Edwards, "Privacy, Security and Data Protection"