משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة القانون التكنولوجيا والمعلومات

מדריך הגנת הפרטיות לעיר החכמה

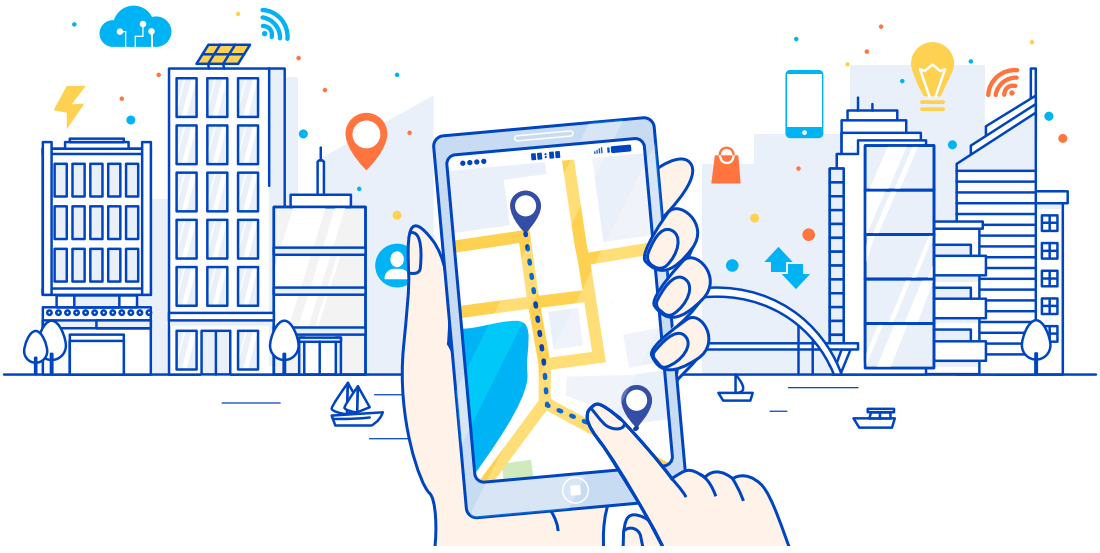
דצמבר 2018

03-7634050 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

חפשו אותנו גם בפייסבוק

תוכן עניינים

דבר ראש הרשות 3
פרק 1 | הקדמה 5
פרק 2 | העיר החכמה 6
תפישת העיר החכמה 6
מגמות בעולם ובישראל 7
עולמות תוכן 8
פרק 3 | פרטיות 9
הזכות לפרטיות על קצה המזלג 9
הרשות להגנת הפרטיות 10
פרק 4 | אתגרי פרטיות בערים חכמות 11
פרק 5 | ניהול סיכוני פרטיות בערים חכמות 14
רשימת דפי מידע בנושאים: 14
1. ניהול מאגרי מידע 14
2. תקנות אבטחת מידע 16
3. מצלמות לאיסוף מידע ואבטחה 20



מדריך זה מוגש כמידע כללי לשירות הציבור/בעלי התפקידים ברשויות המקומיות. הנוסח המחייב הוא הוראות חוק הגנת הפרטיות, התקנות שהותקנו מכוחו והנחיות רשם מאגרי מידע.

דבר ראש הרשות

שלום רב,

על פי התחזיות המקובלות, בעוד כעשור כ-75% מאוכלוסיית העולם וישראל תתגורר בערים. החזון לערים הללו ולעתיד שלנו, התושבים, ברור. אלו יהיו ערים חכמות. ערים שהדיגיטציה והטכנולוגיות החדשות בהן הוטמעו לייעל את תהליכי ניהולה של העיר ומערכותיה במטרה לשפר את איכות חיינו.

בערים אלה יותקנו מצלמות וחיישנים שונים ומגוונים - מפחי אשפה, חניות וכבישים ועד פארקים ציבוריים, שימוש במים ותאורת רחוב אשר ינטרו, בין היתר, גם את ההרגלים והצרכים שלנו למטרות שונות - ביטחון, תחבורה, חיסכון באנרגיה ועוד. אלה מצטרפים להפיכתם של שירותים רבים כמו אפליקציות המאפשרות דיווחים לעירייה, רישום לגנים ולבתי הספר ועוד, לדיגיטליים. כמות המידע האישי שטכנולוגיות אלה יאפשרו לאסוף עלינו בכל תחומי החיים, ובהם גם הרגישים ביותר כמו מצב הבריאות שלנו, מצבנו הרווחתי, מצבנו המשפחתי - עצומה.

היתרונות הרבים הגלומים באיסוף מידע אינם במחלוקת. עם זאת, הם מהווים בסיס פוטנציאלי למנגנוני מעקב תמידי אשר פוגעים בפרטיות התושבים. במובן זה העיר החכמה משקפת את אתגרי "הדור הבא" של הפרטיות. עידן שבו הטכנולוגיות מאפשרות מעקב תמידי אחר התושב, שלל שימושים במידע שנאסף, והפקת תובנות נוספות אודותיו, שאינן קשורות בצורך וברצון להעניק לו שירות מיטבי.

חשוב שנזכור כי למשתמשי העיר החכמה, התושבים, אין אלטרנטיבה אמיתית לקבלת שירותים ציבוריים. התושבים לא יכולים להימנע מאיסוף המידע עליהם, בפרט כאשר מדובר במידע שנאסף בתשתיות עירוניות חיונית.

לא מדובר בעתיד רחוק. טכנולוגיות רבות כבר מתחילות להיות מיושמות בערי מדינת ישראל, אשר קבעה בהחלטת ממשלה יעד כי כל עיר בישראל תהיה חכמה ובעלת תשתיות לפלטפורמות דיגיטליות, בין אם היא מטרופולין ובין אם היא עיר או ישוב קטן. האימוץ המהיר של טכנולוגיות עיר חכמה בישראל מחייב את כל הגורמים השותפים בניהולה ובתיכנונה של העיר החכמה להידרש עוד בשלבים המוקדמים לסוגיית ההגנה על פרטיותם ועל המידע האישי של התושבים המנוהל ברשויות המקומיות או מטעמן.

לכם, כמי שעומדים בראש הרשות המקומית, העיר, מובילים או שותפים לתכנון מיזמים בתחום העיר החכמה, תפקיד מפתח בהגנת פרטיותם של התושבים. חשוב שתדעו לנהל את סיכוני הפרטיות ולדון בשאלות קריטיות, עוד בשלבי התכנון של הטמעת שירותים דיגיטליים או טכנולוגיות חדשות. למשל האם קיבלתם את הסכמת התושבים לאיסוף המידע ושימוש בו? האם אתם עומדים ברמת אבטחת המידע הנדרשת על פי החוק והתקנות? איך תבטיחו לתושבים ותוודאו כי יעשה שימוש במידע האישי שלהם רק למטרה שלשמה מסרו לכם אותו? האם השימוש במידע שלהם יעשה במידתיות?

מדריך זה אשר נכתב על ידי הרשות להגנת הפרטיות, נועד עבורכם בדיוק לשם כך. מטרתו של המדריך היא להציג בפניכם בתמציתיות את הדרישות הרלוונטיות בהוראות חוק הגנת הפרטיות ואת העקרונות המנחים, והוא מעמיד לרשותכם מידע אודות דרישות אבטחת המידע והנחיות חשובות תוך סקירת מקרי בוחן מהעולם.

הפיכתן של הערים בישראל לחכמות נועד לשפר את איכות חייהם של התושבים ואת רווחתם. שמירה על פרטיותם לא רק שמתיישבת עם תכלית זו, אלא היא זו שמהווה תנאי מקדמי לאיכות החיים ולרווחת התושבים. בידכם האחריות והזכות הגדולה להבטיח זאת עבורם.

בברכה,

עו"ד אלון בכר
ראש הרשות להגנת הפרטיות

פרק 1 | הקדמה

מדינת ישראל, לקחה על עצמה לבצע שינוי עמוק וקבעה יעד כי כל רשות מקומית בישראל תהיה חכמה ובעלת תשתיות לפלטפורמות דיגיטליות, בין אם היא עיר או מועצה מקומית או מועצה אזורית. זאת מתוך ראייה אסטרטגית ארוכת טווח וההבנה כי בעוד כעשור, 75% מאוכלוסיית ישראל והעולם יתגוררו בערים (כיום כבר ברור כי עד שנת 2030 יהיו בעולם 41 "גלובל מגה סיטיז" – ערים שמכילות 10 מיליון תושבים או יותר וכי עד שנת 2050, על פי הערכת האו"ם, כשבעה מכל תשעה אנשים יחיו בערים). כדי להתכונן לאתגר גדול זה, ערים בישראל ובכל רחבי העולם, פונות לטכנולוגיות מבוססות רשת ולניתוח מאגרי נתונים בכדי להפוך את עצמם לערים חכמות.

אין הגדרה אחת מוסכמת ל'עיר החכמה'. כל עיר מגדירה זאת על פי הערכים שהיא מאמינה בהם. נציין כי כולם מתבססים על הקשבה, על שיתוף התושבים ועל הנגשת כלים דיגיטליים עבורם וזאת בכדי שיוכלו לממש את זכויותיהם. לעיר החכמה מטרות נוספות כמו חיסכון בהוצאות, ניצול משאבים מיטבי ואספקת שירותים טובים יותר לתושבים. למרות התפתחויות שעיקרן טכנולוגיות, סביבתיות וסוציולוגיות הולכות וגוברות, יש בה בעיר החכמה איום פוטנציאלי גדול על הפרטיות. למשל, היעדר הסכמה שלנו לעיבוד נתונים אישיים, או סוגיות אחרות הכוללות את האופן שבו ערים חכמות אוספות נתונים פרטיים מאינטראקציות ציבוריות בלתי נמנעות, הפרטת הבעלות הן בתשתית והן בנתונים, עיבוד מחדש של נתונים גדולים (Big Data) שנלקחו מהאזרחים, אחסון נתונים אלה בענן ועוד.

כלומר, ערים חכמות מכילות פוטנציאל לאוטופיה עירונית ובאותו זמן הן נושאות זרעים של עולם דיסטופי, עולם בו קיימות מצלמות וחיישנים ברחבי העיר, עולם שבו מתקיים ניטור מתמיד וכריית מידע אישי של תושבי העיר, עולם שבו מערכות מנתחות את ההתנהגויות והנטיות שלנו.

בהינתן הטבות וסיכונים משמעותיים אלו, האימוץ המהיר של טכנולוגיות עיר חכמה בישראל מעלה את השאלה: כיצד יכולה העיר החכמה לאזן בין יתרונות של חברה עשירה במידע לבין צמצום האיומים על הפרטיות.

מדריך זה מרכז דפי מידע הקשורים לפרטיות, שיטות עבודה מומלצות ועוד המסייעים לקובעי המדיניות המקומית, ובדגש למנכ"ל העירייה, לנווט בנושאים מורכבים אלה וזאת במטרה לשמור על פרטיות התושבים בעולם הדיגיטלי המתפתח.

פרק 2 | העיר החכמה

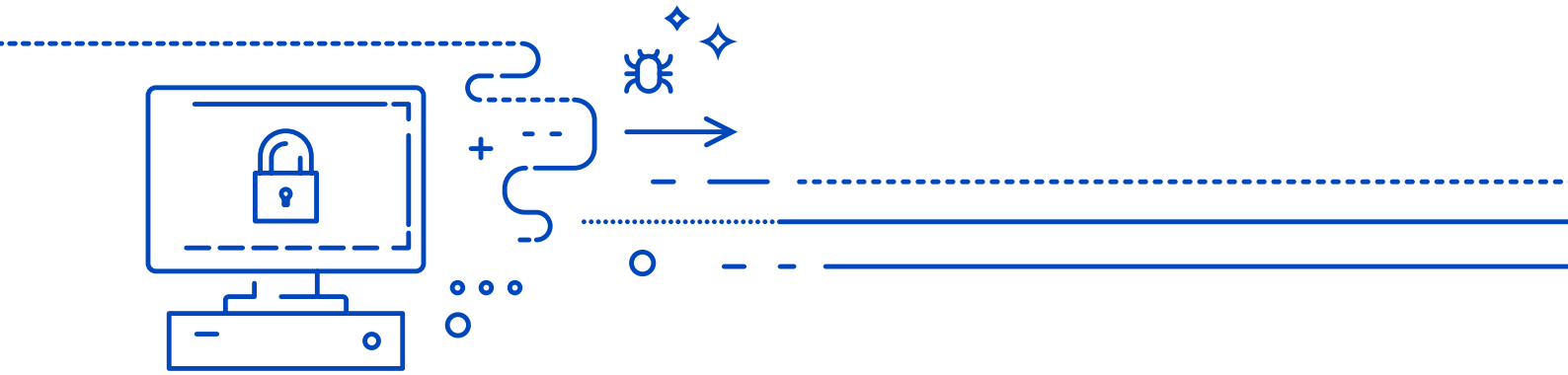
תפישת העיר החכמה

בשנים האחרונות אנו עדים להתחזקות מעמדן של ערים בתוך המערכת הלאומית והעולמית, כאשר נוצרות יותר ויותר ערי ענק (Mega Cities) חזקות ומבוססות, שבהן מתרכז העושר העולמי. הפיתוח של תפישת העיר החכמה ויישומה בעולם מקודם על-ידי ערי ענק אלו, אשר מובילות אסטרטגיה ומעודדות טרנדים ופיתוחים טכנולוגיים המהווים בסיס למידה עבור ערים, ממשלות מקומיות ואף מדינות אחרות.

מכיוון שערים אלו הן ערים גדולות וחזקות, הן מסוגלות למנף את נכסיהן הטכנולוגיים, לפתח את תפישת העיר החכמה וליישמה, לרוב בשיתוף הקהילה העסקית **ולטובת תושבי העיר ושיפור איכות חייהם**. כיום, לא קיימת כמעט עיר גדולה ומובילה בעולם שאינה משתמשת בטכנולוגיה כלשהי לניהול המתרחש בעיר, הביטחון בעיר, הקשר עם התושבים והענקת השירותים העירוניים.

למונח "עיר חכמה" טווח הגדרות יחסית רחב, כאשר מדינות, ארגונים ורשויות שונות מגדירות אותו באופן שונה. עם זאת, **עיקר התפישה מתמקדת בשימוש בטכנולוגיות מידע ותקשורת, ככלי להשגת מטרות חברתיות וכלכליות בעיר.** כלומר, מדובר בתפישת ניהול עיר השואפת להשיג שימוש יעיל במשאבי העיר וכן שליטה ובקרה על הפעילויות בה, כל זאת לטובת:

1. רווחת התושבים, איכות חייהם וביטחונם
2. הגדלת יעילות ואפקטיביות של גופי העיריה והרשויות הפועלות בעיר
3. הגברת שגשוג וצמיחה כלכלית
4. איכות סביבה וקיימות



מגמות בעולם ובישראל

מקובל למנות 3 שלבים באבולוציית הערים החכמות בעולם, אשר בעיקרה מתארת התפתחות ומעבר מהתרכזות בטכנולוגיה להתרכזות בתושבי הערים. כלומר, הטכנולוגיה, שבעבר נתפשה כליבת העיסוק בעיר החכמה, נתפשת כיום כמאפשרת, כמסייעת וכתשתית לטובת שיפור איכות חיי התושבים בערים:

1. **עיר חכמה 1.0 (Technology Driven)** – ערים המבקשות למקסם את השימוש בטכנולוגיה לטובת מינוף כלכלי והגברת יעילות ושליטה במתרחש בעיר. לרוב בערים מסוג זה, מי שהובילו את התפתחות ואימוץ הפתרונות היו ספקיות ענק מעולם הטכנולוגיה והטלקום (כדוגמת IBM, CISCO וכו') ולא הרשויות המוניציפליות עצמן.
2. **עיר חכמה 2.0 (Technology Enabled, City-Led)** – בשלב זה, הרשות המוניציפלית היא זו שמובילה אימוץ ואף יצירה של פתרונות טכנולוגיים בעיר החכמה, אך כאמצעי לשיפור איכות חיי התושבים הנמצאים בליבה.
3. **עיר חכמה 3.0 (Citizen Co-Creation)** – שלב זה באבולוציית הערים החכמות הולך ותופס תאוצה כיום כאשר ערים חכמות מובילות בעולם מאמצות מודלים ליצירה משותפת עם תושביהן (וינה, ברצלונה, מדיין ועוד). כלומר, מדובר ביוזמות של יצירת והטמעת פתרונות טכנולוגיים לטובת התושבים, אשר מתחילות מלמטה ועולות למעלה, תוך מתן דגש על המימד הקהילתי, על שוויון והכלה חברתית וכלכלה מקומית ומקיימת.

בשנים האחרונות אנו עדים ליותר ויותר מיזמים בתחום ערים חכמות הנכנסים גם לערים בולטות בישראל. ההתעניינות בתחום חוצה ערים ורשויות מקומיות, ואין כמעט עיר שאינה מגששת את דרכה בתחום צומח זה. השיח הציבורי סביב נושא הערים החכמות הולך ומתגבר, מספר הפרסומים והכנסים המקצועיים בנושא גדל מידי שנה ומיזמים של רשויות מקומיות ועיריות גדולות המבקשות לאמץ שיטות וטכנולוגיות חדשניות (כמו למשל תל-אביב יפו, ירושלים, חיפה, רמת גן, ראשון לציון, כפר סבא, אשדוד, אילת ועוד) מתפרסמים חדשות לבקרים. בנוסף לחלחול של טכנולוגיות חדשות וקיימות לערים בישראל, במקרים מסוימים טכנולוגיות אף מפותחות בגיבוי וביוזמה של הערים, במסגרת חזון מגובש ותכניות אסטרטגיות.

בהמשך למגמת צמיחה זו ולצורך ייעול תהליכי עבודה ושיפור השירות לתושבים בערי ישראל, החליטה הממשלה אף היא על קידום תפישת "עיר חכמה", והטילה את הובלת התחום **בהיבט הדיגיטלי** על המשרד לשוויון חברתי וישראל דיגיטלית ועל משרד הפנים (החלטת ממשלה 2733, 11.6.2017).

עולמות תוכן

בערים חכמות בעולם ניתן למצוא מאות מיזמים מסוגים שונים, באמצעים טכנולוגיים שונים ובנושאים שונים - החל מפריסת מצלמות וחיישנים מסוגים שונים בעיר ולמטרות ניטור שונות כמו תחבורה, ביטחון, חיסכון באנרגיה וקיימות, דרך אפליקציות ופלטפורמות המוקמות מטעם העיריה במטרה לעודד תיירות או צמיחת תעסוקה מקומית ועד פלטפורמות שנועדו לעודד שיתוף של מידע עירוני, כלי רכב, ציוד וכדומה.

מתוך סקירה רחבה שביצענו ומיפוי המיזמים והנושאים הרבים בהם עוסקות ערים חכמות בעולם ובישראל, **סווגנו והגדרנו 6 עולמות תוכן מובהקים שבהן מתמקדות הערים – חינוך, תחבורה, סביבה וקיימות, ביטחון ואבטחה, שירותים עירוניים וכלכלה**. תחת כל אחד ואחד מעולמות התוכן הללו, אגדנו והגדרנו קטגוריות של תחומים רבים על בסיס מידת הנפוצות שלהם בערים מובילות העולם.

למשל, עולם התחבורה מאגד תחתיו 3 תחומים בולטים – תחום אמצעי התחבורה וההתניידות, תחום ניהול ובקרת התנועה ותחום החנייה. עולם השירותים העירוניים הינו עולם תוכן רחב יותר ומאגד 5 תחומים – 'E-Muni', קהילה, רווחה ובריאות, תחזוקה ותפעול וממשל פתוח ומשתף. עבור כל אחד מעולמות התוכן שהוגדרו והתחומים המאוגדים תחתם, בצענו סקירה מעמיקה של תתי-תחומים ומיזמים בולטים בערים חכמות.

תוצאות התהליך סייעו במיקוד ותעדוף בתחומים שנכון להתייחס אליהם בטווח המיידי לעומת הטווח הארוך.

חינוך
- סביבת למידה
- אוריינות ומיומנות דיגיטלית
- הנגשת מידע וידע

תחבורה
- אמצעי תחבורה והתניידות
- ניהול ובקרת תנועה
- חניה

ביטחון ואבטחה
- ביטחון שוטף
- אבטחת נכסים
- חירום ואירועים חריגים

סביבה וקיימות
- איכות הסביבה
- אנרגיה ומים
- תברואה וניקיון

כלכלה
- מסחר ותעסוקה
- תיירות, תרבות ופנאי
- כלכלה שיתופית

שירותים עירוניים
- E-Muni
- קהילה
- רווחה ובריאות
- תחזוקה ותפעול
- ממשל פתוח ומשתף

פרק 3 | פרטיות

הזכות לפרטיות על קצה המזלג

הזכות לפרטיות היא זכות יסוד חוקתית אשר נקבעה בחוק-יסוד: כבוד האדם וחירותו. סעיף 7 לחוק היסוד קובע, בין השאר, כי "כל אדם זכאי לפרטיות ולצנעת חייו". בהמשך, מדגים הסעיף מהי פרטיות על ידי ציון מספר מצבים של פגיעה בפרטיות, כמו כניסה לרשות היחיד של אדם שלא בהסכמתו. יחד עם זאת, חוק היסוד קובע כי הזכות לפרטיות אינה זכות מוחלטת, והפגיעה בה כפופה לעמידה בתנאים מסוימים.

נוסף על מעמדה של הזכות לפרטיות כזכות יסוד חוקתית, זכתה הזכות, עוד לפני חקיקת חוק היסוד, להגנה מפורשת ונרחבת בחוק הגנת הפרטיות, התשמ"א- 1981. החוק חל הן על המגזר הציבורי והן על המגזר הפרטי, והוא קובע כי פגיעה בפרטיות תהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית שעונשה חמש שנות מאסר. אחד מעקרונות החוק הוא דרישת ההסכמה. החוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק לא מגדיר מהי הסכמה, אלא רק מציין שהיא יכולה להיות מדעת, במפורש או מכללא. הכוונה היא שאין לאסוף מידע על אדם אלא אם כן הוא מבין שהמידע נאסף אודותיו, הוא מסכים לאיסוף המידע וכן מסכים לשימושים השונים שאוסף המידע מבקש לעשות בו.

פרק ב' לחוק מתמקד בהגנה על מידע אישי, וקובע משטר הגנה על הזכות לפרטיות במאגרי מידע. פרק 5 למדריך זה יעסוק בנושא.

מכוח חוק הגנת הפרטיות הותקנו תקנות וצווים בעניינים שונים, ובהם תקנות הגנת הפרטיות (אבטחת מידע), אליהם נתייחס בהמשך המדריך.

אכיפת החוק בכל הנוגע להגנת הפרטיות במידע אישי נעשית בידי הרשות להגנת הפרטיות, הפועלת מכוח חוק הגנת הפרטיות.

הרשות להגנת הפרטיות

הרשות להגנת הפרטיות (להלן - הרשות) הינה הגוף המסדיר, המפקח והאוכף על פי חוק הגנת הפרטיות, התשמ"א – 1981.

במסגרת תפקידה של הרשות כרגולטור של הזכות לפרטיות ולהגנת מידע אישי בישראל, הרשות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים מכוח חוק הגנת הפרטיות ועל ביצורה של הזכות לפרטיות. הרשות פועלת להשגת מטרה זו באמצעות התווית מדיניות, אסדרה, ביצוע הדרכות, אכיפה מנהלית, אכיפה פלילית ופיקוחי רוחב (Audit) על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי דיגיטלי.

הרשות היא שמתווה את מדיניות ההגנה על המידע האישי בישראל במאגרי מידע דיגיטליים. משימותיה המרכזיות של הרשות הן קידום שליטת הפרט במידע אישי על אודותיו, השפעה על תהליכי עיצוב לפרטיות בארגונים ובמערכות מידע בכל מגזרי המשק וחיזוק תחושת המוגנות של הציבור. כל זאת, במטרה לצמצם את הסיכונים הגוברים לפגיעה בפרטיות בעת שמירת מידע דיגיטלי, בעיבודו ובניהולו, והכל תוך איזון ומתן משקל ראוי לחידושים הטכנולוגיים וליתרונותיהם עבור השוק והמשתמשים.

הרשות להגנת הפרטיות, כשומרת הסף של זכויות האזרח בתחום הגנת המידע האישי, רואה כמשימתה העיקרית קידום של ציות לדיני הגנת המידע בכל ארגון, עסק וגוף ציבורי המנהלים מידע אישי על ישראלים, כך שיפעלו לניהול המידע שברשותם באופן תקין בהתאם לדיני הגנת הפרטיות.

פרק 4 | אתגרי פרטיות בערים חכמות[1]

ערים רבות בעולם משקיעות, כאמור, משאבים אדירים לצורך הפיכתן לערים חכמות ודיגיטליות. עם זאת, ועל אף יתרונות רבים שגלומים בעיר החכמה עבור כלל השחקנים, ישנם אתגרים וסיכונים לא מעטים לפרטיותם של התושבים המתגוררים בערים החכמות, אליהם על הרשויות המקומיות והעיריות להיות מודעות.

שיתוף מידע אישי, אשר בעבר נעשה בצורה 'אופקית' בין אנשים הופך יותר ויותר 'אנכי', כאשר תושבים נאלצים לשתף מידע רב באופן עקיף עם גופים כמו הרשות המקומית. למשל, אם בעבר ניהל תושב שיחה ישירה עם מכר לגבי הרגלי הצריכה שלו או הרגלי החניה שלו, בעיר החכמה הרבה פעמים מידע שכזה לא נמסר על-ידי התושב אלא נאסף עליו באופן עקיף וחד-צדדי באמצעים טכנולוגיים, ומעובד, מנותח ומתועל למאגרים קבועים שבבעלות העיריה. כלומר, אם בעבר זליגת מידע אישי ופגיעה בפרטיות יכלה להסתכם ברכילות, מבוכה או סנקציות חברתיות על הפרט, העיר החכמה משקפת את אתגרי "הדור הבא" של הפרטיות. אנו בעידן שבו הטכנולוגיות מאפשרות **מעקב תמידי אחר התושב, שלל שימושים במידע שנאסף, והפקת תובנות נוספות מהמידע**. תוצאות המציאות הזו עשויות להיות לטובת התושבים והחברה, אך יתכנו גם היבטים שליליים שיש להביא בחשבון כעודף התערבות מצד העיריה בחיי התושבים, הגברת המשטור שיוביל לצעדי אכיפה וענישה ופגיעה במרקם החיים האינדיבידואלי המשגשג דווקא בהיותו בלתי מפוקח.

איסוף מידע באמצעות מצלמות וחיישנים מסוגים שונים, משמש ערים חכמות כבר כיום לייעול תהליכי עבודה פנימיים, שיפור השירותים לתושבים וכן שמירה על בטיחותם וביטחונם.

היתרונות הרבים הגלומים באיסוף מידע שכזה אינם במחלוקת, עם זאת, הם גם מהווים **בסיס למנגנוני מעקב ציבורי תמידי, אשר עלולים לפגוע בפרטיות התושבים**.

בעיר ניו-יורק, לדוגמא, נתגלה כי סנסורים חכמים הפזורים בעיר קוראים את כרטיס ה- "EZ-Pass" של התושבים ללא ידיעתם וכך אוספים מידע לגבי מיקומם של כלי רכב. במקור כרטיס זה אמור לשמש לשם מעבר מהיר במחסומים של כבישי אגרה, כפי שסביר שמרבית המשתמשים בו הניחו, אולם בו בזמן אוספים מידע אודות מיקום המשתמשים, דבר העלול לפגוע בפרטיותם.

[1] Kelsey Finch and Omer Tene," Welcome to the Metropticon: Protecting Privacy In a Hyperconnected Town", 2015

בנוסף, הקו הדק שבין ניטור התנהגות לבין הרצון להכתיב אותה הולך ומיטשטש. ערים חכמות עוסקות כבר כיום בהכוונת התנהגות תושבים, בין אם מדובר בשינוי הרגלי צריכת אנרגיה ומים לטובת הגברת הקיימות, שינוי הרגלי חניה, נהיגה ונסיעה לטובת הפחתת עומסי תנועה בעיר או שינוי הדרך שבה תושבי העיר הצעירים לומדים וצורכים חינוך. יתכן שדוגמאות אלו יביאו להטבה באיכות חייהם ורווחתם של התושבים, אך ללא חשיבה, בקרה והצבת גבולות, ייתכנו גם שימושים במידע שייאסף על אנשים שלא יהיו לטובתם ויפגעו באינטרסים שלהם.

אתגר נוסף שעומד בפני תושבי הערים בהיבט הפרטיות, הוא **היעדר אלטרנטיבה**. בשוק הפרטי חברות רבות מעניקות שירות או מוצר בתמורה למידע שנמסר על-ידי המשתמש, וזאת מכיוון שמידע אישי רב על משתמשים מהווה לרוב יתרון תחרותי. בהנחה שהדבר הובא לידיעתם, למשתמשים אלה יש מידה מסוימת של שליטה מתי ואיך הם "סוחרים" במידע האישי שלהם בתמורה לשירותים.

לעומת זאת, למשתמשי העיר החכמה (התושבים) **אין אלטרנטיבה אמיתית לקבלת שירותים ציבוריים והם אינם יכולים להימנע מאיסוף המידע עליהם מבלי שישלמו על כך בביטחון, בנוחות ובאיכות החיים**, בפרט כאשר מדובר במידע שנאסף בתשתיות עירוניות חיונית, כמו במערכת רכבות יחידה בעיר, מערכת החשמל ומערכות המים וכו'.

בכך מתערער יסוד ההסכמה של התושב לשימושי הרשות במידע עליו, מאחר שאין לו אפשרות לבחור בחלופה אחרת, ומחייב זהירות רבה יותר של הרשות בשימוש במידע אישי של אנשים, שהיא נאמנה עליו.

בנוסף למחסור בכוחות שוק תחרותי שעשויים לסייע בשמירה על הפרטיות בעיר החכמה, איסוף המידע שמבצעת הרשות המקומית **מאתגר גם את עקרון צמידות המטרה**. כלומר, לא ברור תמיד האם השימוש שנעשה במידע הנאסף על-ידי העיריה הוא אכן למטרה שלשמו הוגדר בלבד. ישנן דוגמאות מערים בארה"ב ובאירופה שבהן מידע שהצטבר בידי השלטון המקומי "נדד" גם לגופים ציבוריים נוספים ברמות שונות (שלטון כללי או רשויות אכיפת החוק) ואף לשותפים מסחריים, ושימש למטרות שאינן המטרות אשר לשמן אישר התושב את איסוף המידע עליו או שהעיריה רשאית היתה לאסוף ולהשתמש בו כך מכח החוק.

לדוגמא, תושב המשתמש בפלטפורמה עירונית המאפשרת לדווח על מפגעים תשתיתיים בעיר באמצעות העברת תמונות, לא בהכרח יודע מה נעשה עם המידע שהעביר ועם מידע נוסף שייתכן ונאסף עליו באופן עקיף, וכיצד מידע זה מעובד ומועבר בתוך הסבך הביורוקרטי.

תושב זה, ככל הנראה, לא היה מעביר תמונות של מפגעים אם היה יודע שמידע זה עשוי לשמש גופים ציבוריים אחרים או גופים מסחריים למטרות שלהן לא נתן את הסכמתו.

אתגר נוסף לשלטון המקומי בעת הטמעת עיר חכמה, הוא **ריבוי המידע המצטבר במאגרים**. מאגרי מידע עצומים המגיעים מעשרות ואף מאות מקורות שונים ומצטלבים במקום מסוים, **מגדילים את הצורך של העיריה להשקיע באבטחת מידע, על מנת למזער זליגת מידע אישי של התושבים**. בנוסף, מאגרי המידע העצומים הללו, הגדלים במיליוני רשומות מידי יום, הרבה פעמים רוויים ב"רעשים" ועשויים להוביל **לניתוחים מוטים והסקת מסקנות על סיבתיות מזויפות**. בהיבט הניהול העירוני סיבתיות מזויפת עלולה להביא להקצאת משאבים לא נכונה, לאפליית אוכלוסיות שלמות ואף לצעדים לא אתיים הפוגעים בחרויות הפרט ובשוויוניות.

דוגמא לכך ניתן למצוא במקרה של משטרת ניו-יורק, שפעילותה מסתמכת רבות על מידע הנאסף מחיישנים ומצלמות בעיר, בעיקר לטובת מדיניות "Stop&Frisk" (סיורים בעיר, עיכוב חשודים וביצוע חיפוש גופני). עם זאת, מניתוח נתוני 4.4 מליון עיקובים ותשאולים שביצעה ה-NYPD בין 2004-2012, עלה כי בשל הטיה במאגרי מידע ובאלגוריתם הבונה את מסלולי הסיור, העיקובים והתשאולים היו באופן מובהק, שכיחים יותר כשמדובר בתושבים אפרו-אמריקאים והיספאנים מאשר לבנים, מה שהביא לדיון ציבורי בנושא ואף להגשת תביעות משפטיות כנגד העיריה והמשטרה.

טכנולוגיות הניטור השונות והניבוי האנליטי אמנם מייצרות אתגרי פרטיות אך הן עשויות גם להיות חלק ממסגרת המייצרת ערך רב לתושב ולעירייה, יחסי אמון עם השלטון המקומי והעצמת אוכלוסיות שלמות. על אף אתגרי הפרטיות הרבים והמורכבים העומדים בפני השלטון המקומי והתושבים בערים החכמות, **ישנן דרכים רבות למזעור האתגרים ולניהול הסיכונים**.

פרק 5 | ניהול סיכוני פרטיות בערים חכמות

רשימת דפי מידע בנושאים:

1 ניהול מאגרי מידע

בערים החכמות, **מצטברת כמות עצומה של מידע במאגרים שונים**. החל ממאגרים בסיסיים המכילים מידע על תושבי היישוב, כמו מאגר הארנונה העירוני או מאגרי נתוני החינוך העירוניים ועד מאגרים הייחודיים לערים החכמות, כמו מאגרי מידע המצטבר מרשת ה-WiFi העירונית, מכרטיסי התושב המקומיים או מאפליקציות שונות שמפעילה הרשות המקומית/העיריה לטובת התושבים, לעיתים קרובות באמצעות גורמים חיצוניים וקבלני משנה.

מאגרי מידע אלה, המגיעים ממקורות רבים, מצטלבים בנקודה מסוימת ומחייבים את הרשות/העיריה לנהלם בצורה מאובטחת, תוך הקפדה על דגשי ניהול מאגרי מידע ותקנות אבטחת מידע, על מנת למנוע זליגת מידע אישי של תושבים.

למעט מספר חריגים מצומצם, מאגר מידע הוא אוסף נתוני מידע על אדם הניתן לזיהוי והמוחזק באמצעים דיגיטאליים, כמוגדר בחוק הגנת הפרטיות, תשמ"א-1981.

במסגרת פרק ב' לחוק, נקבעו הוראות לעניין הגנה על הפרטיות במאגרי מידע, בין היתר בהיבטי חובת הרישום של המאגרים אצל רשם מאגרי המידע (הרשות להגנת הפרטיות), אופן החזקת המאגרים, זכויות האנשים שעליהם נאסף ונשמר המידע (המכונים "נושאי המידע") וכן השימושים המותרים במידע השמור במאגרים השונים.

בפרק זה מובאים בצורה מתומצתת ונגישה עקרונות מרכזיים עליהם מחויבת הרשות המקומית/העירייה להקפיד בעת הטמעת טכנולוגיות ומיזמים שונים של עיר חכמה, בהיבטי ניהול מאגרים ממוחשבים והמידע הנאסף בהם.

1. **חובת הרישום** - בנסיבות מסוימות, המפורטות בסעיף 8(ג) לחוק, נדרש בעל מאגר מידע לרשום את המאגר אצל הרשות להגנת הפרטיות. מאגר מידע של רשות מקומית בישראל חייב ברישום, שכן מדובר בגוף ציבורי על פי הוראות החוק.
2. **אין לעשות שימוש במידע שלא למטרה שלשמה נמסר ונאסף** - מחובתה של העיריה לעמוד בעקרון "צמידות המטרה", אשר קובע כי **ניתן לעשות שימוש במידע הנאגר אך ורק לטובת המטרה שלשמה הוא נאסף ולא לשם אף מטרה אחרת** (סעיף 8(ב)).

דוגמה

עיריית סן פרנסיסקו מקדמת מיזמי תעסוקה לאוכלוסיות מוחלשות בעיר, ועל כן יצרה פלטפורמה עירונית מקוונת אשר מתאימה בין בתי עסק וחברות המחפשות עובדים בעיר, לבין תושבים המחפשים תעסוקה בתחומים שונים.

אפליקציות מסוג זה, לרוב **מכילות מידע אישי רגיש** על מועסקים פוטנציאליים (קו"ח מפורטים, שנות ותק, השכלה ועוד), ולכן **העיריה נוקטת משנה זהירות** בכל הנוגע למידע זה, ומשתמשת בו **תוך יידוע וקבלת הסכמתם של התושבים לשימוש במידע לטובת המטרה שלשמה נאסף בלבד**, ולא לטובת הצעות ערך אחרות שיתכן וניתן היה להציע לאוכלוסייה מסוג זה בדחיפה (למשל, השתתפות במיזמי דיור ציבורי שמקדמת העיריה וכדומה).

3. **מחובתו של בעל מאגר המידע לעמוד על זכויותיהם של "נושאי המידע"** (האנשים עליהם נאסף ונשמר המידע):
   - **חובת מתן הודעה** - העיריה מחויבת ליידע את הפרט, בטרם איסוף המידע, האם מחובתו החוקית למסור את המידע או לא (למשל, לצורך קביעת גובה מיסי ארנונה, התושב מחויב למסור מידע רלוונטי), מה המטרה שלשמה נאסף המידע, למי יימסר המידע ומה תהיה מטרת המסירה (לפי סעיף 11 לחוק).
   - **זכות עיון במידע** - חובת העיריה לאפשר לכל פרט עליו נאגר מידע, את זכות העיון בנתונים שנאספו עליו, תחת כמה מגבלות (המפורטות בסעיף 13 לחוק).
   - **זכות תיקון המידע** - נושא המידע רשאי לדרוש תיקון של מידע אודותיו, ככל שהמידע במאגר אינו נכון (כמפורט בסעיף 14 לחוק).
   - **חובת הסודיות** - בעל מאגר המידע, המחזיק בו ומי מעובדיו, מחויבים בשמירת סודיות המידע אליו נחשפו כחלק מעבודתם (סעיף 16 לחוק).
4. בנוסף, **בעת פנייה לתושבים בדיוור ישיר**, מחויבת העיריה להקפיד על עמידה במספר כללים הנגזרים מחוק הגנת הפרטיות ומובאים בהרחבה בהנחיה בנושא שירותי דיוור ישיר, אשר מפורסמת באתר הרשות להגנת הפרטיות.
5. **חובה נוספת של בעל מאגר המידע והמחזיק בו, היא חובת אבטחת המידע** (המפורטת בסעיף 17 לחוק) וכן עמידה בתקנות אבטחת המידע אשר נכנסו לתוקף בחודש מאי 2018, ויובאו בהרחבה בחלק הבא.

2 תקנות אבטחת מידע

ריבוי המידע המצטבר במאגרי המידע של עיריות בערים חכמות מחייב, כאמור, ניהול של המידע בצורה מושכלת והקפדה, בין היתר, על אבטחת המידע הנאסף. ביום 8.5.2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017, המפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות הישראלי על כל גורם המנהל או מעבד מאגר מידע. התקנות, שחלות על כלל המשק הישראלי, קובעות מנגנונים ארגוניים ודרישות מהותיות שמטרתן הפיכת אבטחת המידע לחלק משגרת הניהול השוטף של הארגון.

בפרק זה מובאים בצורה מתומצתת העקרונות המרכזיים של אבטחת המידע במאגרי המידע של העיריה, בהתאם לחובות המפורטות בתקנות. העיריה מחויבת להקפיד על יישום עקרונות אלה באופן שוטף, וכן טרם הטמעת טכנולוגיות ומיזמים שונים של עיר חכמה.

מחובת כל רשות מקומית להגדיר מהי רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותה. בהתאם להגדרת רמת האבטחה של המאגר, תבחן העיריה אילו תקנות חלות על המאגר. **מאגר שבבעלות גוף ציבורי, כמו עירייה, חלה עליו רמת האבטחה הבינונית, לכל הפחות. רמת האבטחה הגבוהה תחול על מאגר שבבעלות גוף ציבורי כאשר הוא מכיל מידע אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה לעיון ופעולות בו עולה על 100 מורשים.**

דוגמה

בעיר תל-אביב יפו סביר כי מאגר נתוני התלמידים במערכת החינוך אינו מכיל מידע על למעלה מ-100,000 תלמידים (וזאת בהנחה שמספר התלמידים בעיר עומד על כ-80 אלף תלמידים), לכן במידה ומספר מורשי הגישה למאגר אינו עולה על 100, **מאגר זה יוגדר ברמת אבטחה בינונית**.

מנגד, מאגר המידע הנאסף על בעלי הרכבים הפרטיים בעיר, המכיל ככל הנראה מידע על למעלה מ-200,000 אנשים, יוגדר כמאגר ברמת אבטחה גבוהה, ללא קשר למספר מורשי הגישה אליו.

נתונים: שנתון סטטיסטי עיריית ת"א יפו, 2016 – לוחות 6.1 ו-15.1

בהמשך, לאחר שנבדקה והוגדרה רמת האבטחה הנדרשת למאגר המידע, יש לפנות לטבלה המסבירה אלו תקנות חלות על המאגר. את הטבלה ניתן למצוא בעמוד 3 של המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע) שפרסמה הרשות להגנת הפרטיות. **להלן מובאות בתמצות התקנות הרלוונטיות למאגרים עליהם חלות רמות האבטחה הבינונית והגבוהה:**

1. **חובת העיריה לנהל "מסמך הגדרות מאגר", לכל מאגר בכל רמת אבטחה,** וזאת בהתאם לתקנה 2 בתקנות אבטחת המידע. מסמך זה צריך להיות מעודכן אחת לשנה בכל פעם שנעשה שינוי משמעותי, כמפורט בתקנה. המסמך יכלול: **תיאור כללי** של פעולות האיסוף והשימוש במידע (לדוגמא: איסוף מידע על קיבולת אפשרית ומידת תפוסה של פחי אשפה פרטיים וציבוריים בעיר, באמצעות חיישני תהודה), תיאור **מטרות איסוף המידע** (למשל: לשם ניתוח המידע ויצירת אופטימיזציה בבחירת מסלולי איסוף ופינוי האשפה בעיר), **תיאור סוגי המידע** השונים הכלולים במאגר (למשל: שם בעל הפח, כתובתו, מיקום מדויק של הפח כעת, רמת תפוסה נוכחית, רמת דחיפות הפינוי באזור), פרטים על העברת מאגר המידע או **שימוש מחוץ לגבולות ישראל** (למשל: המידע אינו מועבר לחו"ל ומעובד במאגרים המצויים על שרתי הרשות המקומית), האם נעשה **עיבוד באמצעות גורם זר/חיצוני** (לדוגמא: על אף שהמאגר מוחזק בשרתי העירייה, המיזם ופלטפורמת עיבוד המידע מופעלות על ידי חברת "XyZ", המשמשת כספק חיצוני בהסכם עם העירייה), **מיפוי סיכונים** אפשריים ודרכי התמודדות עמם (למשל: סיכון לזליגת מידע דרך הגורם החיצוני, איתו ניתן יהיה להתמודד באמצעות ביקורות יזומות מטעם ממונה אבטחת המידע של העירייה), **פרטים אישים** של מנהל/ת המאגר, מחזיק/ת המאגר וממונה אבטחת המידע.
2. **חובת העיריה למנות ממונה אבטחת מידע**, כמוגדר בתקנה 3 (וכן סעיף 17ב (א) לחוק). תנאים ודגשים ספציפיים מובאים בהרחבה במדריך תקנות הגנת הפרטיות.
3. **חובת העיריה לקבוע, במסמך ברור, נוהלי אבטחת מידע, שמטרתם לייצר מדיניות אבטחת מידע עקבית בארגון**, כך שניתן יהיה להתמודד עם סיכוני אבטחה אליהם חשוף המידע. חובה זו מוגדרת בתקנה 4, כאשר דגשים ספציפיים לכתיבת ולשמירת הנוהל מובאים בהרחבה במדריך המלא.
4. **העיריה מחויבת לבצע מיפוי של מערכות המאגר וכן סקר סיכונים.** כלומר, להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכוללת פרטים כמו: תשתיות ומערכות חומרה, סוגי רכיבים, תוכנות, ממשקים וכן פרטים נוספים המובאים בהרחבה בתקנה 5 במדריך המלא. **מאגר עליו חלה רמת האבטחה הגבוהה מחויב לערוך סקר לאיתור סיכוני אבטחת מידע** (סקר סיכונים) **אחת ל-18 חודשים לפחות** ולפעול לתיקון ליקויים, אם התגלו. כמו כן, על מאגרים אלה חלה חובה לבצע **מבדקי חדירות** אחת ל-18 חודשים לפחות, לבחינת עמידותם.

5. **חובת העיריה לשמור פיזית על תשתיות החומרה המשמשות את המאגר**, במקום מוגן המונע כניסה ללא הרשאה. כמו כן, **העיריה מחויבת לתעד כניסת ויציאת עובדים מאתרים בהם מצויות מערכות** (מצלמות, זיהוי ביומטרי וכד'), כמפורט בתקנה 6.

6. **העיריה מחויבת למזער את הסכנה הפוטנציאלית שמציב הגורם האנושי** באמצעות העסקת עובדים מתאימים המכירים בחשיבות אבטחת המידע. בנוסף, **מחובת העיריה לבחון את מידת התאמתם של העובדים הקיימים ולהעבירם סמינרים והדרכות אחת לשנתיים**, לכל הפחות. בתוך כך, על העיריה **לנהל הרשאות גישה למאגריה** בצורה מסודרת ואחראית, כמפורט בתקנות 7 ו-8 במדריך המלא.

7. **העיריה מחויבת לוודא שמי שניגש למאגר הוא אכן עובד מורשה, וזאת באמצעות זיהוי ואימות** (לכל הפחות באמצעות סיסמא). כמו כן, נדרש לנהל מנגנון המתעד באופן אוטומטי ועצמאי כל גישה למערכת, עליו תבוצע בקרה תקופתית, כמפורט בתקנות 9 ו-10 במדריך המלא.

8. **חובתה של העיריה לתעד אירועי אבטחה שהתרחשו, כדי לייצר "זיכרון ארגוני" ביחס לאירועים חריגים ולהפיק מהם לקח לעתיד**. תקנה 11 מגדירה מהו "אירוע אבטחה חמור" כשמדובר במאגר עליו חלה רמת האבטחה הגבוהה ומהו אותו אירוע כשמדובר ברמת אבטחה בינונית. במקרה של "אירוע אבטחה חמור", **מחויבת העיריה להודיע לרשות להגנת הפרטיות באופן מידי**, וכן לדווח על הצעדים שננקטו בעקבות האירוע (ניתן לדווח באופן מקוון באתר האינטרנט של הרשות).

9. **העיריה מחויבת להקפיד על מניעת זליגת מידע באמצעות התקנים ניידים** (לפטופים, סמארטפונים וכד'), במידת הצורך באמצעות הגבלת חיבור המאגרים להתקנים ניידים (תקנה 12). כמו כן, יש **להקפיד על ניהול מאובטח ומעודכן של מערכות המאגר** (תקנה 13). בנוסף, במידה ומערכות המידע והמאגרים מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, **מחובת העיריה לנקוט באמצעי אבטחה נוספים שימנעו גישה חיצונית ולא מורשית למידע** (תקנה 14).

10. **חובת העיריה לנקוט משנה זהירות כאשר מעניקים גישה לגורמים חיצוניים במיקור חוץ.** עוד בטרם ההתקשרות יש לבחון את סיכוני אבטחת המידע האפשריים, ובמידה והם גבוהים מידי יש להימנע ממיקור חוץ. כמו כן, יש לקבוע בהסכם מפורש עם הספק החיצוני קווים מנחים לפעילותו, בין היתר: סוג המידע אותו רשאי לעבד, מערכות אליהן רשאי לגשת, חובתו לסודיות ועוד (כמפורט בתקנה 15 וכן בהנחיית הרשות בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי).

11. **העיריה מחויבת לערוך ביקורת פנימית/חיצונית, אחת ל-24 חודשים לפחות,** באמצעות גורם בעל הכשרה מתאימה, שאינו הממונה על אבטחת המאגר מטעמה, על מנת לוודא עמידה בתקנות, כמפורט בתקנה 16. במאגרים עליהם חלה רמת אבטחה גבוהה, ניתן לבצע ביקורת במסגרת עריכת סקר סיכונים (כמוסבר בתקנה 5).

12. **העיריה מחויבת להקפיד על משך זמן שמירת נתוני האבטחה ועל גיבוי ושחזור נתוני אבטחה**, שיש לבצע אחת לתקופה ובהתאם לדגשים המובאים בתקנות 17-18.

13. חשוב לזכור כי **חוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על בעל המאגר, על מנהל המאגר ועל מחזיק המאגר**. כמו כן, מוזכר כי לרשות להגנת הפרטיות שמורה הזכות לפטור מאגרים ספציפיים מחובות אבטחת מידע מתוך התקנות, או לחלופין להטיל חובות נוספות בהתאם לנסיבות, כמפורט בתקנות 19-20.

מידע נוסף בנושא, ובכלל זה מדריך שאלות ותשובות בנושא תקנות אבטחת מידע, ניתן למצוא באתר הרשות להגנת הפרטיות.

3 מצלמות לאיסוף מידע ואבטחה

במהלך העשורים האחרונים גובר השימוש באמצעים טכנולוגיים המיועדים לפיקוח ולמעקב חזותי וקולי מרחוק על שטחי ציבור, הבא לידי ביטוי בהצבת מצלמות זעירות בכל מקום. טכנולוגיות אלה, הנקראות Closed Circuit Television (CCTV) או Surveillance Video, הן בעלות השפעה מהותית על המרחב הציבורי והשימוש בהן כרוך בפגיעה בפרטיות. מצלמות מעקב משמשות ערים בעולם ובישראל במגוון תחומים – החל ממצלמות אבטחה וביטחון המסוגלות לזהות פנים ולנתח דפוסי תנועה בשירות רשויות ההצלה ואכיפת החוק, דרך מצלמות המנטרות תנועת כלי רכב או ממוקמות על גבי כלי רכב ציבוריים למטרות שונות ועד מצלמות הממוקמות על עמודי תאורה ציבוריים ומנטרות תנועה למטרות חיסכון באנרגיה. במרחב ציבורי זה, תחושת המעקב התמידית הופכת מוחשית מאי פעם.

השפעה זו עשויה להיות חיובית, כאשר מצמצמת התנהגות עבריינית/בזבזנית המזיקה לזולת ולחברה כולה. מנגד, ההשפעה עלולה להיות שלילית, כאשר חלק ניכר מהפעילויות הנתפסות באמצעי התיעוד הדיגיטליים הן פעילויות שגרתיות ותמימות, שאינן מהסוג שהחברה מבקשת למנוע. בנוסף, ההתפתחויות ביכולת עיבוד הנתונים, דוגמת זיהוי פנים אוטומטי, זיהוי לוחיות רישוי, כמו גם ניתוח התוכן המצולם (למשל, ניתוח דפוס נהיגה או התנהגות במרחב הציבורי) והעובדה כי ישנה תפוצה רחבה של התופעה בערים בכל העולם, מעצימות את פוטנציאל הפגיעה בפרטיות הטמון במצלמות, ומחדדות את תחושת המעקב וניטור פעולות התושבים.

אי לכך, פרסמה הרשות להגנת הפרטיות בשנת 2012 הנחיה בנושא "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן". הנחייה זו מבהירה את תחולתם של דיני הפרטיות והגנת המידע על השימוש במצלמות המעקב, ומציגה את עקרונות השימוש במצלמות לאור דיני הפרטיות, שהפרתם עלולה להביא לצעדי אכיפה מנהלית ואף להגיע לכדי עבירה פלילית.

להלן מובאים בצורה מתומצתת, לנוחיותם של עובדי הרשות המקומית/העיריה ומנהליה, הקווים המנחים והעקרונות המרכזיים עליהם מחויבים להקפיד בעת הטמעת טכנולוגיות של פיקוח ומעקב חזותי מרחוק באמצעות מצלמות, וכן בניהול מאגרי המידע והצילומים הנקלטים בהן. הנוסח המלא והמחייב הוא הכתוב בגוף החוק וההנחיה עצמה.

1. **תכלית הצבת המצלמות ושמירה על עקרון צמידות המטרה והמידתיות** – עוד בטרם הצבת מצלמות בעיר ושימוש במערכות ניתוח תמונה, כחלק ממיזמי עיר חכמה וככלל, **מחובת קברניטי העיריה לוודא כי נערך תסקיר השפעה על פרטיות**. תסקיר הינו הליך המבוצע על ידי הארגון בשלב מוקדם של תכנון, לפני הטמעת הטכנולוגיה המשתמשת במידע, על מנת לזהות את הסיכונים האפשריים לפרטיות ולעצב את המערכות כך שמראש ימנעו אותם. באחריות העיריה לוודא כי אכן נערכת בדיקה מקיפה הבוחנת את השלכות השימוש במצלמות על זכות הציבור לפרטיות, תוך התייחסות לנושאים הבאים:

   - תכלית הצבת המצלמות - **מטרת הצבת המצלמות חייבת להיות מוגדרת באופן חד, ספציפי ומפורש**. לדוגמא - "מצלמות ניטור ומעקב תנועה, אשר אוספות מידע ומנתחות אותו בזמן אמת לשם ייעול מערך התנועה העירוני והגדרת מדיניות תחבורתית בעיר". **המטרה צריכה להיות בעלת בסיס עובדתי** ("ראויה") – כלומר, קשורה לבעיה שפתרונה מצריך הצבת מצלמות. כמו כן, יש לוודא מראש כי המטרה אותה מבקשים להשיג היא אכן בתחום סמכותה של הרשות המקומית/העירייה. **לאחר שנקבעה המטרה, חל איסור להשתמש בצילומים למטרות זרות, אין להעבירם לגורמים זרים ואין לשמור אותם לאחר שאינם נחוצים עוד**.

   - מידתיות לאור המטרה - הזכות לפרטיות היא זכות חוקתית מוגנת, ולכן עצם קבלת ההחלטה על **הצבת מצלמה בידי רשות ציבורית מחייבת עמידה במבחן המידתיות**: האם מצלמות הן האמצעי מתאים ביותר לאור המטרה? האם המטרה מחייבת הקלטה של הצילומים או שניתן להסתפק בצילום חי (ככל שיש צורך להקליט, יש להגדיר את משך התקופה בה ישמרו ההקלטות)? האם התועלת לתושב עולה על העלות (במונחי פרטיות)? האם ניתן להשיג את המטרה באמצעים פחות פוגעניים? אמצעים נוספים למזעור פגיעה בפרטיות ודגשים בנושא שמירת הצילומים ומחיקתם ניתן למצוא בהנחיה המלאה.

   - דגשים נוספים - יש לנקוט משנה זהירות כשמדובר במצלמות המנטרות אוכלוסיות מוחלשות כמו קטינים או קשישים (קירבה למוסדות חינוך או סיעוד וכד'). בנוסף, מומלץ לקבל החלטה על הטמעת טכנולוגיות מסוג זה בשיתוף הציבור ולקיים שימוע ציבורי שיאפשר לתושבים שפרטיותם תושפע להביע את עמדותיהם, וכן לחברם למיזמים המקומיים של העיר החכמה. **בנוסף, יש לציין כי אין להשתמש במצלמות מעקב לצורך הקלטה קולית**. על מעקב קולי, הנתפס כרגיש וחודרני, חלות חובות והוראות סדורות כמפורט בחוק האזנת סתר, התשל"ט-1917.

2. **"תכנון לפרטיות"** – בעת הטמעת מיזמי עיר חכמה המשלבים מצלמות, **מחובת הרשות המקומית להקפיד על "תכנון לפרטיות", כבר משלב התסקיר, ולוודא כי מספר פרמטרים עומדים במבחן הרלוונטיות למטרה** ולתכליתן של הצבת המצלמות. למשל: **מיקום וזווית המצלמות** - כך שלא יאספו יותר מידע מהמינימום הנדרש. **מספר המצלמות** - לא יותר מהמינימום הנדרש. **זמני צילום** - למשל, אם מדובר במצלמות לניתוח תנועה וניתובה, הן יפעלו בשעות עומסי התנועה בלבד. **רזולוציה** - למשל, אם המטרה היא מיזם לניתוב תנועת כלי רכב, אזי קיים צורך לזהות לוחיות רישוי, ולכן יש צורך בצילום ברזולוציה גבוהה. מנגד, מיזם תאורה חכמה שנועד לחסוך בצריכת אנרגיה עירונית אינו מחייב צילום ברזולוציה גבוהה. **בנוסף, כמפורט בהנחיה המלאה, מחובת הרשות להקפיד כאשר מדובר בפונקציות מיוחדות של מצלמות מעקב ובמיזמים הכוללים: טכנולוגיות זיהוי פנים ודפוסי הליכה, טכנו' ניתוח תנועה ושפת גוף, צילום תרמי/אינפרא-רד, טכנו' תיוג צילומים מתוחכמות ו/או הצלבה עם מאגרים נוספים. טכנולוגיות אלה מסוגלות להפיק מידע הנחשב לבעל פוטנציאל סיכון גבוה לפרטיותם של תושבי העיר.**

3. **יידוע הציבור על הצבת המצלמות** – סעיפו הראשון של חוק הגנת הפרטיות, המציין כי חל איסור על פגיעה בפרטיותו של אדם מבלי לקבל את אישורו, וכן דרישת השקיפות בסעיף 11 לחוק, **מחייבים את הרשות המקומית/העיריה על יידוע הציבור בעת הצבת מצלמות מעקב**. אמצעי היידוע המינימלי לו מחויבת העיריה/הרשות הוא **הצבת שילוט קריא וברור בסמוך למקום בו מותקנת המצלמה, בדגש על מקום הכניסה לאזור הכיסוי**. כמו כן, **מחובת העיריה לפרסם באתר האינטרנט שלה מיפוי מלא של פריסת המצלמות** (מידע נוסף בהנחיה המלאה).

4. **זכות העיון** – כפי שהוזכר בחלק המפרט על מאגרי מידע, **מחובת העירייה לאפשר לאנשים שעליהם נאסף מידע לעיין במידע זה**, זאת תחת תנאים ספציפיים המוסדרים בסעיף 13 לחוק ובתקנות הגנת הפרטיות. הקלטות המצלמות גם הן מאגר מידע עליו חלה זכות העיון, אולם במימוש זכות העיון במאגר צילומים **ישנם דגשים פרקטיים ומשפטיים עליהם יש לתת את הדעת, בעיקר כדי למנוע פגיעה בפרטיות צדדים שלישיים העשויים להופיע בצילום**. הרחבה בסעיף 3.1.5 להנחיה המלאה.

5. **אבטחת המידע הנאסף** – בהמשך לאמור בחלקים הקודמים, המנגישים את נושא ניהול מאגרים ואבטחתם, סעיף 17 לחוק הגנת הפרטיות מטיל אחריות על אבטחת המידע על בעל המאגר, מנהלו ומחזיקו. בתוך כך, **מחובת העיריה לוודא קיום הגנה** פיזית ולוגית על מערכת מצלמות המעקב, **להגדיר נהלים ברורים להקלטת הצילומים**, לעיבודם ולהפצתם ולאבטחת המידע בהם ולקבוע **רשימה מוגבלת של מורשי גישה**. כמו כן, באחריות העירייה **לנקוט במשנה זהירות בעת האצלה לגורמים חיצוניים**, כפי שנהוג לא אחת במיזמי עיר חכמה המשתמשים בפריסת המצלמות העירונית, שכן **במידה וישנה הפרה של החוק האחריות נותרת של העירייה**. מידע נוסף ניתן למצוא באתר הרשות ובמדריך המלא ליישום תקנות אבטחת המידע.

דוגמה

ברשות מקומית מסוימת הוחלט על הצבת מצלמות בחופי הים שבתחומה למטרה אחת ויחידה - שמירה על שלום הציבור ומניעת ונדליזם. לאור זאת, נקבעה רזולוציית צילום גבוהה משום שייתכן שיהיה צורך לזהות את פניהם של המבקרים בחוף.

כעת, מעוניינת העירייה לעשות שימוש בצילומי המצלמות לצרכי קמפיין תיירותי.

לאור העובדה שהשימוש בצילומים למטרות עידוד תיירות לא הוגדרה כתכלית הצבת המצלמות בחופים, חל איסור להשתמש בצילומים למטרה זו.

אם מבקשת הרשות המקומית להשתמש בצילומים למטרות תיירות, עליה להגדיר זאת מראש, להקפיד על "תכנון לפרטיות" ולוודא, בין השאר, שימוש ברזולוציית צילום נמוכה יותר.