

19 באוגוסט 2024
טו' באב, התשפ"ד

עקרונות הגנת פרטיות בהתמודדות עם אירועי חירום

נוסח מעודכן בעקבות תיקון 13

הקדמה

1. ככלל, התמודדות עם אירועי חירום – כגון מלחמה, אסונות טבע (רעידות אדמה, שיטפונות), אירועי טרור בהיקפים גדולים, ומגפות – מחייבת גורמים שונים, פרטיים וציבוריים, לפעול באופן שונה מאופן פעולתם בעת שגרה.
 2. במקרים מסוימים, הצורך להתמודד בדחיפות וביעילות עם אירועי החירום והשלכותיהם, מחייב נקיטת פעולות ואמצעים העלולים לפגוע קשות בפרטיות.
 3. בנסיבות שכאלו עלולות להיווצר מחלוקות, בין היתר, בדבר עצם הצורך בפגיעה בפרטיות לשם התמודדות עם אירוע החירום; מידת הפגיעה המתחייבת בנסיבות העניין; האמצעים הטכנולוגיים בהם ראוי להשתמש; אפשרות קבלת הסכמה לשימוש באמצעים שכאלו; פרק הזמן שיש לעשות בהם שימוש; וכן בדבר אבטחת המידע ואופן השימוש בו.
- לדוגמה, בעת התמודדות עם התפשטות נגיף הקורונה התעוררה מחלוקת בדבר השימוש באמצעים לצמצום התפשטות הנגיף. בין האמצעים נשקלו כאלו שנחשבו פוגעניים במיוחד לפרטיות, כגון שימוש במערכת לדירוג חברתי של אזרחים, או שימוש בכלי שירות הביטחון הכללי למעקב אחר מגעים של חולי קורונה. לעומתם היה ניסיון לנקוט אמצעים מתונים יותר מבחינת פגיעתם בזכות לפרטיות, כגון שימוש באפליקציית ה"מגן" של משרד הבריאות.¹
4. שאלת אופן ההתמודדות עם אירועי חירום והשלכותיהם על פרטיות היא שאלה מורכבת, שצריכה להתברר על פי נסיבותיו הייחודיות של כל אירוע ואירוע.
 5. ואולם, נקודת המוצא היא שגם באירועי חירום, ואולי דווקא בקרות אירועים שכאלו, חלה חובה לכבד את הזכות לפרטיות, ולהימנע, ככל הניתן, מפגיעה לא נדרשת בה. במובן זה, גם בעת התמודדות עם אירועי חירום בהם עלול להיווצר צורך אמיתי לפעול בדחיפות ובאופן העלול להביא לפגיעה בפרטיות, יש לעשות זאת תוך כיבוד הזכות לפרטיות, ותוך צמצום הפגיעה בה, ככל הניתן.

¹ לחוות הדעת הרשות בהתאם לחוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה ראו [כאן](#); חוקתיות השימוש בכלי זה לאיתור מגעים נדונה בהרחבה בבג"ץ 6732/20 [האגודה לזכויות האזרח בישראל נ' הכנסת](#) (1.3.21) (להלן: 'בג"ץ איכוני הקורונה'), ובית המשפט העליון הורה על צמצום משמעותי של השימוש בו. לעמדת הרשות להגנת הפרטיות בנוגע לשימוש באמצעים לדירוג חברתי ראו הרשות להגנת הפרטיות "[דירוג חברתי בראי הזכות לפרטיות](#): סקירת רקע בעניין שימוש במערכות לדירוג חברתי" (22.4.20).

6. במסמך זה מבקשת הרשות להגנת הפרטיות (להלן: 'הרשות') להציב זרקור על סוגיית הגנת הפרטיות באירועי חירום, ולהציג את העקרונות והכללים המרכזיים לפיהם יש לפעול לשם מניעת וצמצום הפגיעה בפרטיות בעת התמודדות עם אירועים אלו.

זכויות אדם והזכות לפרטיות בעת חירום: כללי

7. אירועי חירום,² והצורך להתמודד עימם בדחיפות וביעילות, מצדיקים לעיתים סטייה מהליכי קבלת ההחלטות החלים בעת שגרה, וכן קביעת איזון שונה בין האינטרס הציבורי לבין זכויות הפרט.³

8. במובן זה, התמודדות עם אירועי חירום מצדיקה לעיתים נקיטת אמצעים הפוגעים בזכויות אדם באופן שלא היה נחשב מידתי בעת שגרה. זהו מצב זמני שאמור לפוג עם סיום אירועי החירום והחזרה לשגרה.⁴

9. על פני הדברים, הזכות לפרטיות אינה שונה בהקשר זה מזכויות אדם אחרות. ואולם, התמודדות יעילה עם אירועי חירום דורשת לעיתים איסוף, העברה ועיבוד ללא הסכמה של מידע אישי רב ורגיש. התמודדות שכזו עשויה גם לגרום למעורבות גבוהה יותר של גורמים ציבוריים ופרטיים בחייו של הפרט באופן שעלול אף להביא לחדירה מסוימת למרחב הפרטי שלו, וזאת לשם הגנה על אינטרסים ציבוריים.

לאור כך ניתן לומר כי פוטנציאל הפגיעה בזכות לפרטיות בעת חירום הוא גבוה במיוחד, וכי ההגנה עליה בתקופות שכאלו מהווה אתגר ייחודי ומורכב.

10. ואולם, אין בדברים בכדי לומר שבעת חירום אין משמעות להגנה על הזכות לפרטיות. ההפך הוא הנכון. דווקא בתקופות שכאלו קיימת חשיבות רבה בעמידה על עקרונות ההגנה על הזכות לפרטיות, וזאת כדי להבטיח כי הפגיעה בה בעת חירום תיעשה רק כאשר הדבר הוא הכרחי, באופן המינימלי ביותר האפשרי, ותוך כיבוד זכויות נושאי המידע, ככל שהדבר ניתן.

² הדין הישראלי לא מגדיר באופן כולל ומפורש מה המצבים העשויים להיכנס תחת הגדרה של מצב או אירוע חירום. סעיף 38 לחוק-יסוד: הממשלה מאפשר לממשלה להכריז על קיומו של "מצב חירום" אשר נועד לאפשר לה להתמודד עם אירועי חירום, ומסמין אותה להתקין לשם כך תקנות שעת חירום. סעיף 9 לחוק ההתגוננות האזרחית, התי"א-1951 מאפשר הכרזה על "מצב מיוחד בעורף", אשר מקנה לפיקוד העורף סמכות התערבות בניהול מרקם החיים האזרחיים בשטח ההכרזה, וכן מקנה סמכויות שונות לגורמים נוספים בממשלה. סעיפים אלו אינם מפרטים מהם האירועים העולים בכדי מצב חירום או מצב מיוחד בעורף. הגדרה מפורטת ל"אירוע חירום אזרחי" מצאה מקומה בסעיף 90 לפקודת המשטרה [נוסח חדש], התשל"א-1971, אשר מגדיר אירוע שכזה כ"אירוע הגורם לפגיעה חמורה בשלום הציבור, בביטחון הנפש או ברכוש המתייחס לציבור גדול או לשטח גדול, או אירוע שיש בו חשש לפגיעה כאמור, לרבות מחמת פגע טבע, מפגע סביבתי, אירוע חומרים מסוכנים, אירוע כימי או ביולוגי, אירוע קרינה רדיולוגי, תאונה או פעילות חבלנית עוינת".

³ מוסד שמואל נאמן למחקר מדיניות לאומית "שמירה על הדמוקרטיה כתשתית חיונית בזמן חירום" (ינואר 2024). לדוגמה בעניין זה ראו מכתבה של המשנה ליועצת המשפטית לממשלה (משפט ציבורי-חוקתי) בנושא "העברת מידע בין גופים ציבוריים בנסיבות הקשורות לאירועי החירום הנוכחיים" מיום 20.12.2023, אשר נועד לסייע בגיבוש האיזון בין האינטרסים הציבוריים (ובפרט צרכי הביטחון והסיוע לאוכלוסייה האזרחית), לבין הזכות לפרטיות, וזאת כדי להבטיח כי העברת מידע בין גופים ציבוריים תעשה בהתאם לדין, בצורה יעילה, ותסייע במימוש הצרכים הייחודיים של תקופת ההתמודדות עם אירועי מלחמת 'חרבות ברזל'.

⁴ מיכאל בירנהק "זמן חירום: פרטיות במלחמה" מעבר למסגרת (30.1.24).

11. לאור האמור, להלן יוצגו העקרונות והכללים המרכזיים להגנה על פרטיות בעת חירום באופן המבקש ליצור איזון בין הצורך לפעול בדחיפות וביעילות לשם התמודדות עם אירועי חירום, לבין החובה להגן על הזכות לפרטיות ולצמצם את הפגיעה בה, גם בקרות אירועים שכאלו.

עיקרון ההסכמה

12. עיקרון ההסכמה הוא עיקרון מרכזי בדיני הגנת הפרטיות. ככלל, ביצוע פעולה הפוגעת בפרטיותו של אדם כמפורט בסעיף 2 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות' או 'החוק'), לרבות שימוש בידיעה על ענייניו הפרטיים של אדם בניגוד למטרה שלשמה הוא נמסר, מהווה פגיעה אסורה בפרטיות והפרה של הוראות חוק הגנת הפרטיות.

חוק הגנת הפרטיות אוסר גם על שימוש במידע אישי שבמאגר מידע, בניגוד למטרת המאגר (קרי, שלא בהתאם למטרה שלאורה התקבלה ההסכמה לאיסוף ושימוש במידע, ככל שהוא נאסף בהסכמת נושא המידע). סעיף 8(ד)(1) לחוק מבהיר בעניין זה כי חל איסור על עיבוד מידע אישי במאגר אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע". הוראה זו חלה גם בנוגע למידע שנאסף שלא מתוקף הסכמה תקפה לפי החוק, אלא אם קיימת הסכמה בדין לאיסופו והאיסוף נעשה בהתאם להוראות הדין.

13. כלומר, בהיעדר הסכמה בדין המאפשרת אחרת, ביצוע פעולה הפוגעת בפרטיותו של אדם בניגוד להוראות חוק הגנת הפרטיות - חייבת להיעשות מכוח הסכמת האדם.

14. כוחו של עיקרון זה יפה לתקופות חירום באותה מידה בה הוא נכון לתקופת שגרה. במובן זה, **הצורך להתמודד עם אירועי חירום אינו מכשיר, כשלעצמו, נקיטת פעולה הפוגעת בפרטיות או המפרה את הוראות חוק הגנת הפרטיות.**

15. עם זאת, סעיף 18 לחוק הגנת הפרטיות קובע כי במצבים מסוימים עשויה לעמוד הגנה משפטית לגורם הפוגע שלא כדין בפרטיותו של אדם. הסעיף מפרט שורה של מצבים העשויים להיות רלוונטיים בהקשר של התמודדות עם אירועי חירום, כגון מצבים בהם הפוגע פעל בתום לב הייתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה (סעיף 18(2)(ב)); מצבים של פרסום תצלום שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי (סעיף 18(2)(ה)); ומצבים בהם היה ענין ציבורי בפגיעה המצדיק אותה בנסיבות העניין (סעיף 18(3)).⁵

16. סעיפים אלו עשויים כאמור להיות רלוונטיים בעת התמודדות עם אירועי חירום, שכן בעת אירועים כאלו עלול להיווצר קושי בקבלת הסכמה תקפה של אדם לפגיעה אפשרית בפרטיותו,

⁵ יצוין כי ההגנה הקבועה בסעיף 18 לחוק פורשו בפסיקה בצמצום רב. לעניין הסתמכות על ההגנה שבסעיף 18(3) ראו לדוגמה רע"פ 4743/20 **מרדכי לייבל נ' מדינת ישראל** (נבו 21.7.22), שם צוין כי העובדה שבפרסום מסוים יש ענין ציבורי אין בה בכדי להביא, כשלעצמה, לחלוקה של ההגנה, ועל הטוען לקיומה לשכנע שהעניין הציבורי חייב אותו לפגוע בפרטיותו של אחר. עוד צוין כי כדי להצדיק פגיעה בפרטיות יש להצביע על אינטרס לגיטימי ממשי – מעבר לעצם הרצון לפרסם – שבכוחו להטות את הכף לטובת הפרסום, במסגרת מלאכת האיזונים הנדרשת בין הזכויות והאינטרסים הנוגדים. כמו כן צוין כי יש לבחון אם פרטי המידע הכלולים בפרסום רלוונטיים להגשמת העניין הציבורי, וכן האם לשם הגשמת העניין הציבורי יש צורך בפרסום המידע ברבים דווקא.

וזאת במיוחד בנסיבות בהם מתקיים **צורך דחוף** בנקיטת פעולה מסוימת (כגון פעולה הנדרשת באופן מידי לשם הצלת חייו של אדם), או במצבים בהם קיים **עניין ציבורי** המצדיק את הפגיעה.

17. חשוב להדגיש כי מתוקף סעיפים 20(א) ו-20(ב) לחוק, כל המבקש לטעון לתחולת ההגנה הקבועה בסעיף 18(2) לחוק צריך להיות בעל היכולת להראות שפגיעתו בפרטיות לא חרגה מתחום הסביר באותן נסיבות וכי היא הייתה מידתית, קרי לא הייתה גדולה מהנחוץ באופן סביר באותן הנסיבות.

18. כמו כן יצוין כי בהתאם לפסיקת בית המשפט העליון בעניין **קצין התגמולים**, רשות מנהלית אינה רשאית להסתמך מראש על ההגנות שבסעיף 18 לחוק הגנת הפרטיות לצורך קביעת מדיניות כללית הכרוכה בפגיעה בפרטיות.⁶

19. לאור כל האמור, כאשר קיימת הצדקה מספקת לנקיטת פעולה הפוגעת בפרטיות הנובעת מאירוע החירום, וככל שבגין אופיו של האירוע לא ניתן היה לקבל הסכמה תקפה שהייתה מכשירה את הפגיעה, ייתכן שהפעולה לא תעלה כדי פגיעה אסורה בפרטיות, ובנסיבות אלו תעמוד לפוגע ההגנה המשפטית שבסעיף 18 לחוק.

בעת התמודדות עם אירוע של רעידת אדמה, שליחת נתוני מיקום של אדם המצוי בסכנת חיים לגורמי שיטור, כבאות והצלה, גם ללא קבלת הסכמתו לכך, לא תהווה פגיעה אסורה בפרטיותו.

20. עם זאת, גם באירועי חירום יש לעשות כל מאמץ שלא לנקוט בפעולות הפוגעות בפרטיותו של אדם ללא קבלת הסכמתו לכך, או לכל הפחות להקפיד הקפדה יתרה שלא לפגוע בפרטיות מעבר לנדרש בנסיבות שכאלו. לעמדת הרשות, ניסיון להסדיר הסכמה לפעולות מבעוד מועד בטרם קרות מקרה החירום או עשיית כל מאמץ לקבל הסכמה בזמן אמת, עד כמה שהדבר ניתן, משליכים גם על תום הלב של הפוגע, שקיומו נדרש לתוקפן של ההגנות לפי סעיף 18(2).

באירוע טרור, בו עשוי להיות עניין לציבור בפרסום דחוף של תמונות או סרטונים מהאירוע, וקבלת הסכמה מצד פרטים מסוימים (כגון קורבנות או פצועים) אינה אפשרית בנסיבות העניין, פרסום התכנים תוך טשטוש פניהם של פרטים אלו, וכן של כל נתון נוסף העשוי להביא לזיהויים, עשוי להוות פתרון ראוי בהיבט של דיני הגנת הפרטיות.⁷ יובהר כי גישה זו אמורה לחול ביחס לכל תמונה או סרטון שפרסומם עלול להביא לפגיעה בפרטיותו של אדם, לרבות תמונות מתוך פנים ביתו של אדם, ולא רק כאלו בהן מופיעה דמותו.⁸

⁶ רע"א 2558/16 פלונית נ' קצין התגמולים – משרד הביטחון, פסקה 59 לפסק הדין (נבו 5.11.2017).

⁷ יצוין כי על-פי סעיף 2(א4) לחוק הגנת הפרטיות, פרסום ללא הסכמה של תצלום אדם שנפגע מפגיעה גופנית או נפשית עקב אירוע פתאומי ושפגיעתו ניכרת לעין ברבים, שצולם בזמן הפגיעה או סמוך לאחריה באופן שניתן לזהותו ובנסיבות שבהן עלול הפרסום להביכו (למעט פרסום תצלום בלא השהיות בין רגע הצילום לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות), מהווה פגיעה בפרטיות.

⁸ לעניין הפגיעה בפרטיות בפרסום מידע על פנים ביתו של אדם ראו ע"א 1697/11 גוטסמן אדריכלות בע"מ נ' אריה ורדי (נבו 23.1.13). על היבט הפגיעה בפרטיות במסגרת פרסום תמונות של בתי יישובי עוטף עזה לאחר אירועי ה-7 באוקטובר ראו בירנהק "זמן חירום: פרטיות במלחמה", לעיל ה"ש 4.

21. כמו כן, יובהר כי לגישת הרשות, גם באירוע חירום – כל הפוגע בפרטיותו של אדם שלא מתוקף הסכמתו (או מתוקף הסמכה בדין), צריך להיות מסוגל להצביע על הצורך שחייב אותו לפעול כפי שפעל, ועל כך שלא עמדה לו היכולת הסבירה לקבל את ההסכמה האמורה, על מנת שניתן יהיה לבחון האם עומדת לו הגנה מכוח החוק, והאם פעל בתום לב ובמידתיות.

חובת היידוע

22. סעיף 11 לחוק הגנת הפרטיות קובע כי פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצוינו בה המטרה אשר לשמה מבוקש המידע; האם חלה על נושא המידע חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; למי יימסר המידע ומטרות המסירה; שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עימו; קיומן של זכות עיון במידע האישי לפי סעיף 13 לחוק, ובדבר הזכות לבקש את תיקון המידע לפי סעיף 14 לחוק; ומהי תוצאת אי-ההסכמה למסירת המידע.

23. הוראות סעיף 11 חלות בכל מקום בו איסוף מידע אישי על אודות אדם נעשה על יסוד פנייה אליו לקבלת המידע, וזאת בין אם המידע נאסף מכוח הסכמת נושא המידע, ובין אם איסוף המידע נעשה מכוח הסמכה שבדין.⁹

24. ככלל, חובת היידוע חלה גם בעת חירום. בעניין זה יובהר כי סעיף 18 לחוק, המעמיד, בנסיבות מסוימות, הגנה משפטית ביחס לפגיעה בפרטיות הנעשית ללא הסכמה, אינו מעמיד הגנה שכזו במקרים של אי-עמידה בחובה היידוע.

25. לפיכך, כל גורם הפועל בעת חירום והמבקש לאסוף מידע אישי מאדם לצורך כך, אם מתוקף הסמכה בדין ואם מתוקף הסמכה, צריך ליידע את נושא המידע בדבר הפרטים המנויים בסעיף 11. על גורמים אלו לבחון דרכים שונות לעמידה בחובה זו גם בעת חירום.

כך לדוגמה, פרסום באמצעי התקשורת המקובלים עשוי להיחשב יידוע מספק בעת התמודדות עם אירוע חירום דחוף המקשה על פנייה אישית לנושאי המידע הרלוונטיים.

26. ברם, הרשות מכירה בכך שבעת אירועי חירום, הדורשים נקיטת פעולה דחופה, עשוי להתעורר קושי אמיתי לעמוד בחובת היידוע בטרם איסוף המידע. עמדת הרשות היא שגם אם לא עלה בידי הגורם האוסף לקיים את החובה במועדה כנדרש בחוק, עדיין יש לקיימה לכל הפחות במועד מאוחר יותר, ובהזדמנות הראשונה האפשרית.¹⁰ במקרים חריגים אלו, ככל

⁹ לעמדת הרשות בנושא ראו הרשות להגנת הפרטיות "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (18.7.22).
¹⁰ עמדה זו דומה במהותה לחובת עריכת "שימוע מאוחר", לפיה רשות מינהלית שנמנע ממנה לערוך שימוע במועד מטעמי דחיפות, תהא מחויבת בקיום ההליך במועד מאוחר יותר. זמיר טען בעניין זה כי: "הדחיפות עשויה לפטור מחובת שימוע מוקדם, כלומר שימוע לפני מעשה, אך אין בה בהכרח כדי לפטור מחובת שימוע מאוחר, כלומר שימוע לאחר מעשה. אמנם, אפשר שהשימוע, אם לא ניתן לפני מעשה, עבר זמנו ובטל קורבנו, אך בנסיבות מסוימות אפשר שעדיין יהיה טעם, ולפיכך גם תהיה חובה, לקיים לאחר מעשה שימוע שלא קוים לפני מעשה מחמת הדחיפות." יצחק זמיר **הסמכות המינהלית**, כרך ב - ההליך המינהלי, 1168-1169 (2011). ראו גם: ע"מ 1038/08 **מדינת ישראל נ' חסין געאביץ** (נבו 11.8.09).

שבעקבות קיום חובת היידוע הבהיר נושא המידע כי הוא אינו מסכים שייעשה שימוש במידע האישי אודותיו, ועיבוד המידע נסמך על הסכמתו, בעל שליטה במאגר מידע אינו רשאי להמשיך ולעשות שימוש במידע זה.

27. מצב עניינים זה יאפשר לאדם לדעת כי מידע על אודותיו נאסף במסגרת אירוע חירום, ויאפשר לו, בין היתר, להעמיד את ההחלטה לביקורת שיפוטית, וכן לעמוד על זכויותיו במידע הנתונות לו מכוח חוק הגנת הפרטיות, לרבות הזכות לעיון במידע והזכות לבקש את תיקונו.¹¹

28. למען הסר ספק יצוין כי **קיום הליך יידוע מאוחר יכול להיות מיושם אך ורק במקרים קיצוניים, בהם הייתה לגורם האוסף את המידע מניעה מוחלטת ליישם חובה זו במועדה.**¹²

עיקרון צמידות המטרה

29. סעיף 9(2) לחוק הגנת הפרטיות קובע כי שימוש בידעה על ענייניו הפרטיים של אדם מותר אך ורק למטרה שלשמה נמסרה. סעיף 8(ב) לחוק קובע כי לא יעבד אדם מידע אישי שבמאגר מידע אלא למטרת המאגר שנקבעה לו כדין. סעיפים אלו מעגנים את עיקרון צמידות המטרה.

30. אירועי חירום עלולים להביא לכך שמידע אישי רב, לרבות מידע שלא נאסף בזמני שגרה, יימסר ויישמר למטרת התמודדות עם האירועים והשלכותיהם בדחיפות, במהירות וביעילות.

31. בשל אופיים של אירועי חירום, במקרים רבים המידע הנאסף יהיה מידע בעל רגישות מיוחדת, כגון מידע רפואי או ביומטרי. כמו כן, כפי שצוין קודם לכן, במקרים מסוימים המידע עלול להיאסף ולהישמר במאגרי מידע שלא מתוקף הסכמה תקפה, או מבלי שקוימה למשל חובת היידוע לפי סעיף 11 לחוק הגנת הפרטיות.

32. בנסיבות שכאלו חלה חובה להקפיד הקפדה יתרה על כך שאיסוף המידע והשימוש בו ייעשו אך ורק למטרה הנובעת מהצורך להתמודד עם אירוע החירום, ולהימנע מלעשות שימוש במידע זה למטרות אחרות.

באירוע חירום בו מתעורר קושי בזהוי מספר רב של נפטרים עלול להתעורר צורך באיסוף ובשימוש במידע ביומטרי של אנשים אחרים, וזאת למטרת זיהוי או אימות זהות הנפטרים והבאתם לקבורה תוך זמן מהיר ככל האפשר. בנסיבות שכאלו, השימוש במידע שנאסף יכול להיעשות אך ורק למטרות אלו, ושימוש בו למטרות אחרות, ללא הסכמת נושאי המידע לכך, יהווה פגיעה בפרטיות והפרה של חוק הגנת הפרטיות.

¹¹ סעיף 13 לחוק הגנת הפרטיות מעמיד לנושא מידע זכות לעיון במידע על אודותיו המוחזק במאגר מידע. סעיף 14 לחוק קובע כי נושא מידע שמצא כי מידע על אודותיו המוחזק במאגר אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל השליטה במאגר בבקשה לתקן את המידע או למוחקו.

¹² השוו: זמיר, לעיל ה"ש 10, בעמ' 1169.

עיקרון המידתיות

33. עיקרון המידתיות מבטא במהותו את התפיסה לפיה מטרה ראויה אינה מקדשת תמיד את כלל האמצעים שניתן לנקוט לשם הגשמתה.¹³

34. עיקרון המידתיות חל על כל החלטה של רשות ציבורית ועל כל פעולה או אמצעי הננקטים על-ידה. העיקרון חל גם על כל גורם – פרטי או ציבורי – המבקש לעשות שימוש בהגנות הקבועות בסעיף 218(2) לחוק הגנת הפרטיות וזאת מתוקף הוראות סעיף 20 לחוק.

35. לפיכך, על כל רשות ציבורית המבקשת לפעול מתוקף סמכותה ולנקוט אמצעים העלולים לפגוע בפרטיות במסגרת התמודדות עם אירוע חירום, וכן על כל גורם – ציבורי או פרטי – המבקש לפגוע בפרטיות בגין אירוע החירום ללא הסכמה תקפה של מי שפרטיותו עלולה להיפגע בהסתמך על ההגנות הקבועות בסעיף 218(2), להקפיד כי פעולותיהם יעמדו במבחני המידתיות.¹⁴ חובה זו חלה ביחס לכל "מחזור חייו" של פריט מידע, ובכלל זה: איסוף וקבלה של מידע; שימוש ועיבוד המידע; העברתו של המידע לאחר; ואחסון המידע עד למועד מחיקתו.¹⁵

36. בהקשר זה הרשות מבקשת להדגיש ארבעה מרכיבים מרכזיים שיש לבחנם בעת יישום מבחני המידתיות ביחס לפעולה או אמצעי הננקטים לשם התמודדות עם אירוע החירום, ואשר עלולים להביא לפגיעה בפרטיות:

- יעילות האמצעי – המבחן הראשון מבין שלושת מבחני המידתיות המקובלים בוחן האם קיים קשר רציונאלי בין האמצעי למטרה. במסגרת מבחן יש לתת משקל גם לשאלת יעילות השימוש באמצעי להשגת המטרה המבוקשת;
- סוג המידע ורגישותו – ככל שמידע הוא רגיש יותר, כך גם הפגיעה הנגרמת כתוצאה מהשימוש בו תיחשב חמורה יותר בהיבטי פרטיות, וזאת במיוחד אם השימוש במידע נעשה ללא הסכמה תקפה. מצב עניינים זה משליך על איזון הפגיעה אל מול התכלית שלשמה היא נעשית במסגרת מבחן המידתיות השלישי (מבחן המידתיות במובן הצר);
- היקף המידע והשימוש בו – ככל שנאסף מידע אישי רב יותר, וככל שנעשה במידע זה שימוש בהיקפים גדולים יותר, כך מועצמת הפגיעה בפרטיות הנגרמת מעיבוד המידע. לפיכך שיקולים

¹³ דפנה ברק-ארז משפט מינהלי כרך ב (2010), בעמ' 771.

¹⁴ לפירוט על מבחני המידתיות בהקשר לפגיעה בפרטיות ראו מכתבה של היועצת המשפטית לממשלה מיום 13.6.2023 "עקרונות חוקתיים בעיבוד מידע אישי בגופים ציבוריים ובשירות הביטחון הכללי בפרט", עמ' 2-4 והפסיקה הנוכרת שם. המכתב זמין כאן. ראו גם ברק-ארז, לעיל ה"ש 13, בעמ' 777.

¹⁵ מכתבה של היועצת המשפטית לממשלה, שם, בעמ' 4.

אלו רלוונטיים לבחינת מידתיות הפעולה הפוגעת בפרטיות אל מול התכלית שלשמה היא נגרמת.

- **ממד הזמן** – במסגרת בחינת מידתיות שימוש במידע אישי לשם התמודדות עם אירועי חירום יש לשקול גם את משך הזמן בו נאסף המידע, ואורך התקופה בה נעשה בו שימוש. במובן זה, שימוש באמצעים הפוגעים בפרטיות לצורך התמודדות עם אירועי חירום, מעבר לפרק הזמן שנדרש לשם כך, עלול במובן זה להוות התנהלות שאינה מידתית. לאור האמור, ייתכן שלא ניתן יהיה להצדיק אמצעי שימוש בו היה מוצדק בתחילת אירוע החירום, לאחר תקופת זמן מסוימת ושינוי מאפייניו של אירוע החירום שבגינם נעשה השימוש באמצעי מלכתחילה.

כזכור, עם תחילת ההתמודדות מדינת ישראל עם נגיף הקורונה, ובשל הצורך לפעול בדחיפות לצמצום התפשטות הנגיף, נעשה שימוש בכלי שבידי שירות הביטחון הכללי לצורך איתור מגעים של חולי קורונה. שימוש זה נעשה חרף הפגיעה הקשה בפרטיות שהייתה כרוכה בהפעלת הכלי, ומתוך הנחה כי הוא ייעשה באופן זמני. לאחר כמעט שנה, בעקבות הגידול במערך הבדיקות האפידמיולוגיות והשיפור ביעילותן, במקביל לעלייה בשיעור ציבור המתחסנים, המחלוקות שהתגלעו בדבר יעילות השימוש בכלי, והפגיעה הקשה בפרטיות הציבור הכרוכה בשימוש זה, פסק ביהמ"ש העליון כי יש לצמצם באופן משמעותי את השימוש בכלי, רק למקרים שבהם חולה מאומת אינו משתף פעולה בחקירה האפידמיולוגית, או שלא מסר כלל דיווח על מגעים.¹⁶

37. עוד יובהר כי שני מבחני מידתיות – מבחן האמצעי שפגיעתו פחותה ומבחן המידתיות במובן הצר – חלים גם ביחס לשימוש בהגנת סעיף 18(3) לחוק, החלה כאשר "בפגיעה היה ענין ציבורי המצדיק אותה בנסיבות הענין". לפיכך, **כל גורם הפועל בעת חירום באופן הפוגע בפרטיות ומבקש להסתמך על כך שבפעולתו יש 'ענין ציבורי' המצדיק את הפגיעה בנסיבות הענין, צריך להצביע על אינטרס לגיטימי ממשי; להראות שהתועלת בפעולתו הכרחית לצורך הגשמת הענין הציבורי;**¹⁷ **שפעולתו עולה על הנזק שנגרם בגינה; ושלא ניתן היה להשיג את מטרת פעולתו באמצעים פוגעניים פחות.**¹⁸

38. חשוב לזכור כי ככלל, **הכרה בשימוש באמצעי הפוגע בפרטיות כמידתי בעת התמודדות דחופה עם אירוע חירום, אינה מהווה הכרה במידתיות השימוש באמצעי בעת שגרה (או בעת תקופת**

¹⁶ ראו 'בג"ץ איכוני הקורונה', לעיל ה"ש 1, בפס' 48-50 לפסק דינה של הנשיאה חיות. יצוין כי בשלב מאוחר יותר, לאור עלייה נוספת בתחלואה והתפשטות זן חדש של נגיף הקורונה, הוחלט לתקופה קצרה מאוד לחזור לעשות שימוש בכלי. שימוש נוסף זה הופסק בחלוף ימים אחדים. ראו: בג"ץ 8196/21 **האגודה לזכויות האזרח בישראל נ' הממשלה** (נבו) (2.12.21).

¹⁷ ראו פסק דינו של בית המשפט העליון בעניין **לייבל**, לעיל ה"ש 5, פסקאות 6-7 לפסק דינה של השופטת וילנר. ¹⁸ לפי פסיקת בתי המשפט, פעולה אשר הנזק הגרם בגינה לפרטיותו של אדם עולה על התועלת שבצידה, או שניתן להשיג את מטרתה גם באמצעים פוגעניים פחות, עשויה להיחשב כפעולה שאינה מוצדקת בנסיבות הענין, ומכאן שאינה חוסה תחת הגנת סעיף 18(3) לחוק. ראו והשוו: ע"א 439/88 **רשם מאגרי מידע נ' משה ונטורה**, מח(3) 808 (1994); ע"א 8954/11 **פלוגי נ' פלוגי** (נבו, 24.4.2014), בפס' 117-120 לפסק דינו של השופט סולברג; ת"א 41627-02-19 **בספלוב נ' שידורי קשת בע"מ** (נבו, 10.1.2022); ת"א (ירושלים) 3213/09 **פלוגי נ' פלוגי** (נבו, 11.10.2011); ת"א (הרצליה) 21945-07-14 **פלוגי נ' אריאל סמל** (נבו, 31.1.2016), בפס' 64-65 לפסק דינו של השופט סלע.

“שגרת חירום” שבין מועד קרות האירוע למועד החזרה המלאה לשגרה). לפיכך, ולאור החשש מ”נרמול” שימוש באמצעים שכאלו באופן שיביא לעליית היקף השימוש בהם גם בעת שגרה,¹⁹ יש לנקוט באמצעים שכאלו במשורה, רק כאשר מדובר באירועי חירום הדורשים זאת, ותוך הקפדה על הפסקת השימוש בהם בעת שגרה.

עיקרון צמצום המידע

39. מטבע הדברים, התמודדות עם אירועי חירום כרוכה באי-וודאות, בין היתר, ביחס להיקף האירועים, השלכותיהם על הציבור, ואופן ההתמודדות המיטבי עימם.

40. ככלל, אי-וודאות שכזו יוצרת אי-בהירות ביחס לסוג והיקף המידע האישי הנדרש לשם התמודדות עם האירועים. מצב שכזה עלול להביא לכך שגורמים שונים יאספו וישתמשו במידע אישי רב מן הדרוש בפועל לשם מטרת ההתמודדות עם אירוע חירום מסוים והשלכותיו. מצב עניינים זה מהווה אתגר מבחינת דיני הגנת הפרטיות ועיקרון צמצום המידע.

41. עיקרון צמצום המידע הוא עיקרון הנגזר מעיקרון צמידות המטרה, ולפיו יש להימנע ככל הניתן מאיסוף, אחסון, או ביצוע פעולה אחרת של עיבוד מידע אישי שאינם הכרחיים למטרת האיסוף או למטרת המאגר בו הוא שמור. כלומר, על-פי עיקרון זה, יש לאסוף ולאחסן במאגר אך ורק את המידע האישי המינימלי הנדרש וההכרחי ליישום המטרה, וזאת מבחינת היקף המידע, סוג המידע, וכן הלאה.

42. בנוסף, על-פי עיקרון זה, ובהתאם לאמור בתקנה 2(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע”ז-2017 (להלן: ‘תקנות אבטחת מידע’ או ‘התקנות’), על בעל השליטה במאגר לבחון, אחת לשנה, האם אין הוא מחזיק במאגרו מידע רב מן הנדרש למטרות המאגר, כלומר מידע עודף שהוא כבר לא נזקק לו לשם הגשמת מטרות המאגר. לגישת הרשות, במצב בו בעל השליטה מגיע למסקנה כי הוא מחזיק מידע עודף, עליו לצמצם מידע זה, בין היתר, באמצעות מחיקתו או התממתו.²⁰

43. לאור כל האמור, הרשות ממליצה כי עם קרות אירוע חירום, ועל אף אי-הוודאות הקיימת בו, **על כל גורם המבקש לאסוף מידע אישי ולהשתמש בו למטרת התמודדות עם אירוע החירום לבצע, ככל הניתן, בסמוך לקרות האירוע, הערכה זהירה ביחס למידע האישי הנדרש למטרה זו, ולהקפיד לאסוף, לאחסן ולהשתמש אך ורק במידע זה.**

¹⁹ על החשש מנרמול השימוש באמצעים קיצוניים ראו פס’ 3 לפסק דינו של השופט עמית בבג”ץ איכוני הקורונה, לעיל ה”ש 1. בין דבריו ציין השופט עמית כי: “לא בכדי, הרשות להגנת הפרטיות התריעה כבר בתחילת הדרך כי השימוש באמצעים המופעלים על ידי השב”כ עלול להביא לנרמול של שימוש ביכולות טכנולוגיות של גופי בטחון לצורך פרקטיקות של מעקב אחר אזרחים שומרי חוק”. מה שמתחיל כשימוש חד-פעמי ביכלי, כאמצעי קצה לא קונוונציונלי בסיטואציה של חירום קיצוני, עלול להביא להליכי גמילה קשים מהשימוש ביכלי לנוכח הפיתוי לעשות בו שימוש על חשבון אמצעים קונוונציונליים אחרים.”

²⁰ להרחבה ראו טיוטת מסמך מדיניות הרשות להגנת הפרטיות בנושא “[צמצום מידע \(Data Minimization\)](#) – טיוטת מסמך מדיניות” (25.3.21).

44. מטבע הדברים, קיימת מורכבות בביצוע הערכה שכזו בעת קרות אירוע חירום. לפיכך, הרשות ממליצה כי גורמים המיועדים לפעול בעת חירום (כגון משרדי ממשלה, רשויות מקומיות, עמותות, וארגוני חברה אזרחית) יערכו, כעניין שבשגרה, הערכה בדבר סוג והיקף המידע האישי שיידרש להם, בסבירות גבוהה, לשם התמודדות עם אירועי חירום שבתחומי אחריותם וסמכויותיהם.²¹ ביצוע הערכה שכזו, בעת שגרה, יהפוך את הליך איסוף ועיבוד המידע בחירום ליעיל יותר, יביא לצמצום איסוף ואחסון המידע העודף, ומכאן לצמצום הפגיעה בפרטיות בעת חירום. ביצוע הליך שכזה יוכל להביא גם ליצירת הסדרים משפטיים ולעיצוב כלים טכנולוגיים מתאימים שיאפשרו איסוף ושימוש במידע בעת קרות אירוע חירום באופן מידתי וראוי מבחינת היבטי פרטיות ואבטחת מידע.²² יובהר כי ככלל, אין באמור כדי לקבוע כי ניתן לאסוף מידע אישי העשוי להידרש בעת חירום, כבר בעת שגרה, אלא אם הגוף האוסף הוסמך לכך בחקיקה.

45. כמו כן, בהתאם לחובה הקבועה בתקנות אבטחת מידע, על גורמים שכאלו להקפיד לבחון, לכל הפחות אחת לשנה, האם המידע השמור במאגריהם אשר נאסף לצורך התמודדות עם אירוע חירום, לא הפך למידע עודף עם החזרה לעת שגרה. לאור רגישות המידע הנאסף בעת התמודדות עם אירוע חירום, ולאור ההנחה שבעת חירום קיימת נטייה לאיסוף מידע רב מן הדרוש בפועל, הרשות ממליצה כי בחינה שכזו תיעשה סמוך למועד סיום תקופת ההתמודדות עם אירוע החירום והחזרה לשגרה, וככל האפשר באופן עתי גם במהלך הימשכו, ולא רק פעם בשנה, כמתחייב בתקנות.

בעת התפשטות מגפה המונעת מאנשים מקבוצות סיכון מסוימות לצאת מביתם (כגון אנשים מבוגרים), על עמותה המבקשת להקים מאגר מידע המכיל מידע אישי על אנשים מקבוצות שכאלו למטרת שליחת אריזות מזון לביתם, להקפיד שמאגר המידע יכיל רק את המידע המינימלי הרלוונטי למטרה זו. ככלל, מאגר שכזה אמור להכיל נתונים הרלוונטיים לצורך משלוח האריזות, כגון שם וכתובת מגורים, ולא מידע שאינו דרוש לשם כך, כגון מידע רפואי שאינו נדרש. כמו כן, בעת סיום ההתמודדות עם המגפה, וכאשר אין עוד צורך בהחזקתו של המידע, רצוי כי העמותה תבחן את אפשרות מחיקת המידע או התממתו.

גישה למידע על אודות נפטרים

²¹ לביצוע הערכה שכזו ניתן להיעזר במדריך הרשות להגנת הפרטיות לעריכת "תסקיר השפעה על הפרטיות" (2022). ככלל, תסקיר השפעה על פרטיות הוא תהליך שנועד לסייע לארגון באיתור, הערכה וניהול של סיכונים לפרטיות בפרויקטים או פעילויות עסקיות וארגוניות אחרות הכוללות עיבוד של מידע אישי.

²² לעניין זה ראו לדוגמה, תקנות שוויון זכויות לאנשים עם מוגבלות (נגישות אירועי פינוי אוכלוסייה וקליטתה במצב חירום), התשפ"ב-2022.

46. אירועי חירום מעוררים שאלות קשות ביחס לגישות למידע על אודות נפטרים ולשימוש בו. סוגיה זו היא חלק מדיון נרחב יותר בנוגע לפרטיות נפטרים והשימוש במידע האישי שלהם לאחר מותם. הדיון האמור חורג מגדרו של מסמך זה.²³

במסגרת מסמך זה מבקשת הרשות להתייחס לשלוש נקודות מרכזיות מתוך נושא זה, הרלוונטיות לאירועי חירום ולמקרים של מוות הנגרם באופן פתאומי.

47. ראשית, במסגרת התמודדות עם אירועי חירום עלול להתעורר צורך בהעברת מידע רגיש על אודות נפטרים, כגון מידע ביומטרי מסוג טביעות אצבע למטרות של זיהוי גופה, אימות זהות או איתור של נעדר. יש להקפיד כי העברה שכזו תיעשה על-פי הקבוע בהוראות הדיון.²⁴

48. שנית, בכל הנוגע לפרסום תמונה של נפטר, סעיף 2א לחוק הגנת הפרטיות קובע כי פרסום ברבים של תצלום גופת אדם גלויה באופן שניתן לזהותה מהווה פגיעה בפרטיות, בכפוף למספר חריגים שנקבעו בסעיף (הסכמת הנפטר בעודו בחיים, הסכמת בני משפחתו אם הנפטר לא התנגד בחייו, חלופי 15 שנים מועד הפטירה ועוד). משמעות הדבר היא שפרסום תמונה או סרטון בהם מופיעה דמות של גופת אדם, באופן שניתן לזהותו (תוך שימוש באמצעים סבירים), עלול להוות עוולה אזרחית.²⁵ הרשות מבקשת להבהיר כי פרסום בהקשר זה כולל גם הפצה של התמונה או הסרטון ברשתות חברתיות או באפליקציות להעברת מסרים מידיים, כגון WhatsApp.²⁶

49. נקודה שלישית נוגעת לרצון בני משפחה של נפטר לקבל גישה למידע אישי השמור במכשירים הדיגיטליים שהיו ברשותו, כגון טלפונים חכמים ומחשבים ניידים.

50. הרצון של בני משפחה לקבל גישה למידע שבמכשירים של יקיריהם שנפטרו, לרבות כחלק מתהליך ההתמודדות עם האובדן, הוא ברור ומובן. מנגד, מכיוון שמידע זה עלול לכלול מידע אישי רב ורגיש (כגון התכתבויות אישיות ותמונות אינטימיות), "כניסה" של קרובי משפחה

²³ לדיון בנושא הזכות לפרטיות של נפטרים ראו לדוגמה: רע"א 1917/92 סקולר נ' גרבי, פד"י מז(5) 764 (1993), פס" 7 לפסק הדין של השופט גולדברג; סעיף 9(ב)(10) לחוק חופש המידע, התשנ"ח-1998, אשר קובע חריג לעניין מסירת "מידע שיש בגילוי פגיעה בצנעת הפרט של אדם שנפטר"; תקנה 8(ג)(2) לתקנות הארכיונים (עיון בחומר ארכיוני המופקד בגנזך), התש"ע-2010; סעיף 25 לחוק הגנת הפרטיות, העוסק בהגשת תובענה או קובלנה בגין פגיעה בפרטיות לאחר מותו של אדם; בג"ץ 52/06 חברת אלאקסא לפיתוח נכסי ההקדש המוסלמי בא"י בע"מ נ' Simon Wiesenthal Center Museum Corp, (נבו 29.10.2008), פס" 144-145 לפסק דינה של השופטת פרוקצ'יה. ראו גם מיכאל בירנהק פרטיות חוקתית, 279-286 (2023); אהרון ברק "הזכות החוקתית לפרטיות וצנעת הפרט: תכלית, חשיבות והיקפה", 401 ספר עדנה ארבל (שלי אביב ייני, דורית ביניש, אריאל בנדור, הדר דנציג-רוזנברג וקרן מילר עורכים, 2022), עמ' 447-448.

²⁴ כך לדוגמה, לצורך התמודדות עם אירועי ה-7 באוקטובר נחקק חוק העברת מידע לצורך זיהוי או אימות זהות של אדם לרבות גופה, ואיתור נעדר או שבוי, הנדרשים בשל פעולות האיבה או פעולות המלחמה (הוראות שעה - חרבות ברזל), התשפ"ד-2023.

²⁵ לעניין הגדרת פגיעה בפרטיות כעוולה אזרחית ראו סעיף 4 לחוק הגנת הפרטיות. לעניין הגשת תובענה אזרחית בהקשר של פגיעה בפרטיות נפטרים ראו גם סעיף 2א(ב) לחוק.

²⁶ לעניין הגדרת "פרסום" ראו סעיף 3 לחוק הגנת הפרטיות, אשר מנפה ל"פרסום" כמשמעותו בסעיף 2(ב)(1) לחוק איסור לשון הרע, התשכ"א-1965, שכולל גם פרסום אשר היה מיועד לאדם נוסף זולת הנפגע, ואשר הגיע לאותו אדם או לאדם אחר זולת הנפגע. לעניין איסור הפצה של תכנים ברשת ובאפליקציות להעברת מסרים מידיים ראו גם סעיף 3(א)(5) לחוק למניעת הטרדה מינית, התשנ"ח-1998.

למכשירו של אדם שנפטר, עלולה לחשוף מידע רגיש על אודותיו שלא היה בכוונתו שייחשף בפניהם, וכן לפגוע, לעתים פגיעה קשה, בפרטיותם של אנשים אחרים עימם היה בקשר.

בעניין זה יש לזכור שבמקרים רבים, רצונם של אנשים למנוע גישה של אחרים למידע רגיש על אודותיהם, כגון מידע על צנעת חייהם ונטיותיהם המיניות, יהיה דווקא מול האנשים הקרובים אליהם, כגון הוריהם ובני משפחתם.²⁷

51. לפיכך, ובהיעדר הסדרה חוקית של העניין, רצוי שהחלטות בנושא זה תתקבלנה ברגישות, תוך כיבוד רצון הנפטר (ככל שניתן להעריך מה היה רצונו), ותוך כיבוד פרטיותם של אנשים שהיו עימו בקשר, ושמידע על אודותיהם, לרבות מידע רגיש הנוגע אליהם, מצוי במכשירו.

כך למשל, אפליקציה להעברת מסרים מידיים, כגון WhatsApp, מכילה מעצם מהותה התכתבויות אישיות של הנפטר עם אחרים, וכניסה אליה בעלת פוטנציאל של ממש לפגוע בפרטיותם של האנשים עמם קיים הנפטר תכתובות.²⁸

אבטחת מידע בעת חירום

52. כל גורם – פרטי או ציבורי – האוסף ומשתמש במידע אישי מחויב על-פי דין באבטחתו של המידע והמאגר בו הוא מוחזק.²⁹ חובה זו חלה בעת שגרה כמו גם בעת חירום.

53. עם זאת, התמודדות עם אירועי חירום מציבה אתגר ייחודי בנוגע לאבטחת מידע, וזאת משתי סיבות מרכזיות:

א. בעת חירום, ובוודאי בעת התמודדות עם אירוע חירום בעל מאפיינים ביטחוניים, תיתכן עלייה במספר ובאיכות תקיפות הסייבר מטעם גורמים עוינים, אשר יבקשו, בין היתר, לתקוף מאגרי מידע במטרה להביא לחשיפתו של מידע אישי, וכן להשתמש בו למטרות אחרות, כגון יצירת פאניקה בקרב הציבור, הפצת דיסאינפורמציה, וערעור תחושת הביטחון האישי.³⁰ דוגמה מרכזית בהקשר זה היא בתי חולים ומוסדות רפואיים אחרים, המחזיקים מידע רפואי רגיש, והמהווים יעד מרכזי לתקיפות סייבר בעת אירועי חירום.

ב. בשל אופיו, התמודדות עם אירוע חירום נעשית על-פי רוב בתנאים של חוסר וודאות, בלחץ של זמן, בתנאים פיזיים שונים מהרגיל, ותוך מעורבות גורמים רבים, פרטים וציבוריים.

²⁷ חס"מ (תל אביב-יפו) 105-05 יפת חזה נ' משרד הבריאות (נבו 12.9.06).

²⁸ להשוואה ראו חוק הגישה לתוכן דיגיטלי לאחר מותו של אדם, התשפ"ד-2024, אשר מחריג מתחולתו שירותי תוכן דיגיטליים לתקשורת בין-אישית, כגון אפליקציות מסרים מידיים. החוק אף מבהיר במפורש כי הוא אינו גורע מהוראות חוק הגנת הפרטיות.

²⁹ ראו סעיף 17 לחוק הגנת הפרטיות, ותקנות אבטחת מידע.

³⁰ לעניין זה ראו לדוגמה: חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023. להרחבה ראו גם: מערך הסייבר הלאומי "מלחמת חרבות ברזל" במימד הסייבר: תובנות ודרכי התמודדות" (דצמבר 2023); תהילה שוורץ אלטשולר "הממד הרביעי של המלחמה מערער את יכולת הישראלים לברר את המציאות" המכון הישראלי לדמוקרטיה (7.11.2023).

בתנאים מורכבים שכאלו מידע אישי רגיש עלול, בין היתר, להיות חשוף לגורמים שאינם אמורים להיחשף אליו, ולהיות מועבר באמצעים שאינם מאובטחים דיים.

54. לפיכך, בעת התמודדות עם אירועי חירום, על אף המורכבות הקיימת באירועים אלו ואולי דווקא בשל מורכבות זו, יש להקפיד הקפדה יתרה על עמידה ויישום הדרישות המפורטות בתקנות אבטחת המידע.

55. בשל אופיים, הדחיפות ואי הוודאות הכרוכה בהתמודדות עם אירועי חירום, וכן החשש הגובר מקיומם של אירועי אבטחת מידע בתקופה שכזו, ראוי כי תינתן התייחסות מיוחדת לנושאים הבאים:

- קביעת הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר בהתאם להגדרות תפקיד. הרשאת הגישה לכל בעל תפקיד צריכה להיות אך ורק במידה הנדרשת לביצוע התפקיד.³¹ בהקשר זה יש לוודא, בין היתר, כי רק לגורמים המורשים יש גישה למידע הרלוונטי להם במאגר המידע, ולמערכות המאגר. כמו כן, יש להקפיד לנהל את הרשאות הגישה לאורך תקופת החירום ולבטל את הגישה למידע עם סיום הצורך בכך.
- מיפוי מערכות המידע הרלוונטיות לתהליכי איסוף ושמירת המידע בעת חירום, וכן מיפוי המערכות המשמשות לאבטחתו.³²
- קביעת הוראות בדבר האבטחה הפיזית והסביבתית של המאגר ומערכות המאגר, כהגדרתן בתקנות אבטחת המידע.³³ בהקשר זה יש להקפיד שלא להשאיר מכשירים דיגיטליים, כגון מחשבים ניידים וטלפונים חכמים, באופן המאפשר גישה חופשית אליהם ולמידע השמור בהם.
- שימוש באמצעי אבטחה למכשירים ולתוכנות בהם נעשה שימוש להעברת מידע אישי, כגון שימוש בסיסמת כניסה חזקה ומורכבת למכשירים, אימות דו-שלבי, זיהוי ביומטרי וכו'.³⁴ מומלץ להקפיד שלא לעשות שימוש בסיסמה אחת למגוון מכשירים. יש להקפיד גם על אופן ומקום שמירת הסיסמאות וזאת על מנת למנוע את חשיפתן בפני גורמים לא מורשים או בפני כאלו העלולים לעשות שימוש לא מותאם במידע.
- הקפדה כי נתוני התיעוד (לוגים) לכל מערכות המאגר נשמרים לתקופה של 24 חודשים לפחות.³⁵

³¹ תקנות 8 ו-9 לתקנות אבטחת מידע.

³² תקנה 5(א) לתקנות אבטחת מידע.

³³ תקנה 6(א) לתקנות אבטחת מידע.

³⁴ תקנה 14(א) ו-1(ב) לתקנות אבטחת מידע.

³⁵ תקנה 10(ד) לתקנות אבטחת מידע.

- איסור חיבור מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.³⁶
 - גיבוי נתונים במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, באופן שיבטיח שיהיה ניתן, בכל עת, לשחזרם.³⁷ כמו כן, יש לבצע סריקת מערכות הגיבוי לבחינת תקינותן ואבטחתן. עוד מומלץ להחזיק העתק גיבוי "קר" (שאינו מחובר לרשת), ולבצע תרגילי שחזור מידע אחת לרבעון בכדי לוודא תקינות מערכות הגיבוי.
 - קביעת נהלי עבודה ביחס לאבטחת מידע אישי בעת חירום, לחידוד נהלים אלו לאורך זמן, ולהגברת מודעות עובדיהם לנושא, בין היתר על-ידי ביצוע הדרכות תקופתיות.³⁸
56. כאשר בשל כורח הנסיבות מועבר מידע אישי רגיש באפליקציות להעברת מסרים מידיים (כגון WhatsApp) או חשבונות דוא"ל שאינם מוסדיים (כגון Gmail), רצוי למחוק את המידע כאשר הדבר מתאפשר או במידת הצורך להעבירו למערכת מאובטחת המיועדת לכך.

סיכום

57. למרבה הצער, הצורך להתמודד עם אירועי חירום שונים אינו זר למדינת ישראל. מתוך ניסיון העבר ניתן לראות כי התמודדות עם אירועי חירום עשויה לעיתים לחייב נקיטת פעולות ואמצעים הפוגעים בפרטיות באופן ובמידה שאינם מקובלים בעת שגרה. הזכות לפרטיות היא, אפוא, אחת מזכויות האדם המאותגרות ביותר בעת חירום.
58. במסמך זה הציגה הרשות להגנת הפרטיות עקרונות וכללים להגנה על פרטיות בראי קרות אירועי חירום שונים. לגישת הרשות, **יישום עקרונות וכללים אלו, באופן המתואר, עשוי לאפשר איזון ראוי בין הצורך לפעול בדחיפות וביעילות בעת חירום, לבין החובה להגן על הזכות לפרטיות ולצמצם את הפגיעה בה, גם בתקופות מורכבות שכאלו.**

³⁶ שם.

³⁷ תקנה 17(ה) לתקנות אבטחת מידע.

³⁸ תקנה 7(ג) לתקנות אבטחת מידע.