התנועה לזכויות דיגיטליות
Digital Rights Movement [ע"ר]

יום שלישי, 14/07/2020

לכבוד: חה"כ צבי האוזר – יו"ר ועדת חוץ וביטחון
חברי ועדת חוץ וביטחון
הייעוץ המשפטי לוועדה

# נייר עמדה על הסמכת השב"כ לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה – ניתוח יכולות איכוני השב"כ, דיוקם ומגבלותיהם, ומקומם ביחס לחקירות אפידימיולוגיות מתקדמות

## תקציר

הדיון על הסמכת השב"כ לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה סובל מחוסר שקיפות. ניסיונות להתייחס לאספקטים הטכנולוגיים, לדיוק האיכונים ולמגבלותיהם, נענים באמירות שעל כך ניתן לדון רק בפורום סגור. אמירות אלו מונעת דיון ענייני בנושא. נייר עמדה זה מיועד להחזיר את הדיון המהותי לפורום הפתוח.

סיוע השב"כ מתבסס (בעיקרו) על טכנולוגיה של איכונים סלולריים. הטכנולוגיה ומגבלותיה מוסברים בחלק הראשון של מסמך זה. לפי מידע פומבי, איכון סלולרי רגיל יכול להגיע לדיוק של כ-50 מטר, ואיכון סלולרי של אות רציף יכול להגיע לדיוק של פחות מ-5 מטרים. אולם בתנאים לא אופטימליים דיוק האיכון יורד משמעותית. כמו כן, האיכון מספק מידע מרחבי דו-ממדי בלבד, ולכן אנשים ששהו באותו בניין אך בקומות שונות יזוהו כאילו שהו באותו אזור.

החלק השני של המסמך נוגע לחוק איכוני השב"כ. ההגדרות "מידע טכנולוגי" שבחוק אינן נכונות, ובפועל השב"כ אוסף ומעבד מידע נוסף שלא הותר בחוק. לעומת זאת, החוק מתיר עיבוד נתוני התקשרות, למרות שאינם נדרשים לצורך איתור מגעים. ההגדרות שבחוק דורשות התאמות, ויש להסיר את היתר שניתן לעיבוד נתוני התקשרות.

החלק השלישי כולל נתונים מספריים אודות יעילות כלי השב"כ: רק 5% מהאנשים שהוכנסו לבידוד התגלו עד כה כחולים. צריך לומר זאת בבהירות: הכלי של השב"כ הוא לא פתרון קסם למיגור מגיפת הקורונה. בחלק זה של המסמך נרחיב על הצורך במתן כלים טכנולוגיים שיבואו במקום איכוני השב"כ, ונציג רעיונות נוספים לייעול מערך החקירות האפידימיולוגיות: התייחסות לאיתורים של השב"כ כאל אינדיקציה ראשונית בלבד, הוספת תקנים למערך החקירות, בקשת הסכמת החולה לשימוש בנתוני מיקום כבסיס לחקירה, שימוש בכלים טכנולוגיים נוספים לפי הצורך, התייחסות דיפרנציאלית לסיכון ההידבקות במטרה להרחיב את רשת הבדיקות ולאתר נדבקים בסיכון נמוך.

## מבוא: חוק איכוני השב"כ

### הליכי החקיקה של חוק איכוני השב"כ

ביום 17/03/2020 פורסמו תקנות שעת חירום להסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש, התש"ף–2020. ביום 01/04/2020 התקבלה החלטה על הסמכת שירות הביטחון הכללי לפי סעיף 7(ב)(6) לחוק שירות הביטחון הכללי, התשס"ב–2002. בעקבות בג"ץ 2109/20 התחייבה הממשלה לעגן את הסמכת השב"כ בחקיקה ראשית. ביום 19/05/2020 פורסם תזכיר חוק איכוני שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020.

בתחילת מאי, התפרצות הקורונה החלה לדעוך, ולנוכח ההתנגדות הציבורית הרבה להמשך איכוני השב"כ[1] הממשלה החליטה לעצור את קידום הצעת החוק. אולם במהלך חודש יוני פרץ הגל השני של הקורונה

1 תזכיר החוק קיבל 1005 הערות באתר התזכירים הממשלתי, כולן מתנגדות לחוק, ורובן הוגשו על ידי אזרחים פשוטים, שהביעו את התנגדותם המוחלטת להפעלת יכולות השב"כ על אזרחים.

במלוא עוצמתו, והממשלה ביקשה מהכנסת לקדם את הצעת החוק בהליך בהול. הצעת החוק נדונה בוועדת החוץ והביטחון בימים 29-30/06/2020, כמעט ללא דיון ציבורי, ואושרה בכנסת למחרת היום.

הוועדה החליטה לפצל את החוק, כך שבשלב הראשון יוסמך השב"כ לסייע לאיתור מגעים לתקופה של שלושה שבועות בלבד, והדיון על ההסדרים הקבועים יערך במהלך תקופה זו. יו"ר הוועדה ח"כ צבי האוזר סיכם את ההחלטה כך: "אנחנו מאשרים כאן הסדר שהוא זמני אבל כזה שנותן בידי משרד הבריאות כלי יעיל מספיק למציאות הקיימת, ויאפשר לנו לדון לעומק בהסדר הרחב יותר".

**עתה הזמן לדון לעומק על יעילות הכלי של השב"כ, על חלופות טכנולוגיות, ועל אמצעים לייעול החקירות האפידימיולוגיות, שיש בהם כדי לייתר את הצורך בשימוש ביכולות המיוחדות של השב"כ.**

**<u>הפעלת חוק איכוני השב"כ</u>**

חוק איכוני שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020 (להלן – חוק איכוני השב"כ) פורסם ברשומות בלילה של יום רביעי ה-01/07/2020, והופעל מיד עם פרסומו. ביומיים הראשונים להפעלת הכלי, משרד הבריאות שלח כ-30,000 הודעות לאזרחים, המורות להם להיכנס לבידוד מכיוון ששהו בקרבת חולה קורונה מאומת. בשבוע הראשון להפעלת הכלי נשלחו 70,949 הודעות לאזרחים על מגעים עם חולים מאומתים. מתוך כלל האזרחים שנדרשו להיכנס לבידוד, רק כ-5% מתוכם, 3,495 איש, אובחנו עד כה כחולי קורונה.

במקביל התפרסמו דיווחים רבים על איכונים שגויים – אנשים שנטען ששהו ליד חולה קורונה מאומת בזמן ששהו בביתם, אנשים שנטען ששהו באזור בו לא נמצאו כלל, אנשי צוות רפואי ששהו ליד חולים במקום עבודתם, אנשים ששהו באזור כללי שבו נמצאו חולי קורונה ללא מגע קרוב או בכלל. גורם המעורה במערכת צוטט בעיתון "גלובס" אומר שהאיכונים טועים בכחמישה אחוזים מהמקרים[2]. המוקד הטלפוני של משרד הבריאות קרס, ואלפי אזרחים נדרשו לשהות בבידוד ביתי ללא אפשרות להגיש השגה על הקביעה כי עליהם לשהות בבידוד.

בשל הביקורת על דיוק האיכונים, הודיע ח"כ צבי האוזר כי הוועדה ברשותו תשקול את המשך האישור לביצוע האיכונים, אם לא יוסדרו הערעורים על איכוני השב"כ: "**אם לא יוסדרו הערעורים על איכוני השב"כ, אשקול מחדש את הארכתם! אם המשרד לא ימצא פתרון למחדל בימים הקרובים אאלץ לשקול מחדש את אישור המשך האיכונים. זה כלי חשוב, אך הוא כלי משלים ואינו יכול בשום אופן לעמוד כאמצעי ללא בקרה ודיוק**".

## <u>חלק ראשון: טכנולוגיית האיכון הסלולרי, דיוקה ומגבולותיה</u>

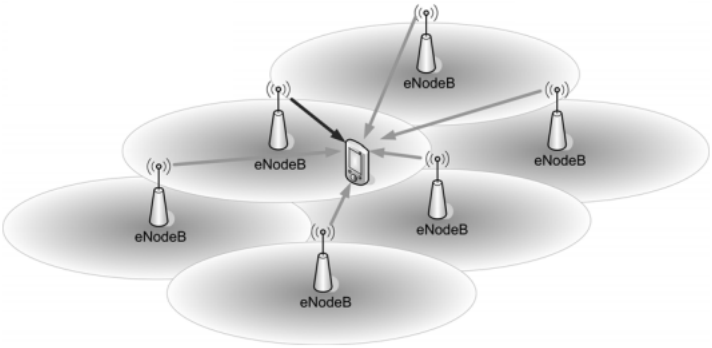
חלק זה מבוסס על נייר עבודה (White Paper) של צוות מומחים בתחום. העבודה על הנייר טרם הסתיימה ולכן יובא להלן תקציר על טכנולוגיית האיכון הסלולרי. התיאור הוא הפשטה מסוימת של עקרונות הפעולה של רשתות 3GPP (רשתות GSM, UMTS, LTE, 5G).

## <u>פרק ראשון: הטכנולוגיה שבבסיס איכון סלולרי</u>

רשת סלולרית מורכבת מאנטנות סלולריות הפרושות במרחב. בין מכשיר הטלפון הנייד לבין האנטנות יש תקשורת רציפה, המאפשרת העברת מידע ושיחות אל מכשיר הטלפון הנייד וממנו. כל מגדל סלולרי מורכב מכמה אנטנות כיווניות (סקטורים), שכל אחת מהן קולטת את המכשירים הקרובים אליה. כפי שניתן לראות בשרטוט מטה, תאי השטח חופפים – בכל אזור מכשיר הטלפון הנייד קולט אותות ממספר אנטנות, ומספר אנטנות קולטות את האותות של מכשיר הטלפון הנייד. בכל רגע נתון הטלפון משוייך לאנטנה דומיננטית, שקולטת את האות החזק ביותר ממכשיר הטלפון הנייד[3]. כשהטלפון נמצא בתנועה, האנטנות מעבירות ביניהן את השליטה, כך שהמכשיר יקושר בכל זמן לאנטנה עם האות החזק ביותר.

2 דני זקן, "איכוני השב"כ מפספסים בכחמישה אחוז מאז חמישי האחרון", גלובס 05/07/2020.

3 בפועל השליטה נקבעת לפי כמה פרמטרים, ביניהם איכות האות ועומס הרשת בכל אנטנה.




כדי שהרשת הסלולרית תוכל לשייך את הטלפון הנייד לאנטנה דומיננטית, הטלפון הנייד קולט אותות מהאנטנות שמסביבו, ומשדר בחזרה אותות שיוך. כל איתות נרשם אצל מפעילי הרשת, וכולל מזהה אות ייחודי, חתימת זמן, מידע אודות האנטנה (Cell ID), מזהה המכשיר (International Mobile Equipment Identity = IMEI), מזהה המנוי (International Mobile Subscriber Identity = IMSI), ומידע אודות עוצמת הסיגנל (Received Signal Strength Indicator = RSSI).

מפעיל הרשת הסלולרית מחייב את המנוי בתשלום על השימוש ברשת הסלולרית על ידי איסוף רשומות שימוש (Call Detail Record = CDR). רשומת השימוש כוללת את סוג התקשורת (שיחת טלפון, משלוח מסרון, העברת נתונים ברשת וכיוצ"ב), פרטי המקור, פרטי היעד, זמן תחילת התקשורת, זמן סיום התקשורת, פרטי האנטנה ומידע טכני נוסף. הרשומה אינה כוללת את תוכן התקשורת.

כאשר מדברים על איכונים סלולריים, כורכים יחדיו שתי טכנולוגיות שונות – איכון סלולרי בסיסי בזמן שיחה, ואיכון רציף של המכשירים המזוהים ברשת.

<u>איכון סלולרי בסיסי</u> מתבסס על נתוני האנטנה הפעילה בעת ביצוע תקשורת לפי רשומות השימוש. ברמה זו מתקבל מידע אודות האנטנה הדומיננטית (או האנטנות הדומיננטיות, אם המכשיר נע בין מספר תאים) בזמן נתון. האיכון הוא ברמת שטח הכיסוי של האנטנה, וניתן למקם את המכשיר ברזולוציה של כמה מאות מטרים, תלוי בצפיפות האנטנות במרחב.

<u>איכון סלולרי רציף</u> מתבסס על רישום האותות הרציפים של טלפונים ניידים. כאמור, כל פרק זמן קצר, כל מכשיר שולח הודעת "אני כאן" לאנטנות שסביבו. כל האנטנות רושמות את פרטי האיתות. עוצמת האות הנקלטת באנטנה מאפשרת לשערך את המרחק של המכשיר מהאנטנה. באמצעות נתוני עוצמת האות, אפשר לחשב את המרחק של המכשיר מהאנטנות שסביבו. ככל שיותר אנטנות מזהות את האות, כך ניתן לאכן את מיקום המכשיר באופן מדויק יותר. שיטת איכון אחרת מתבססת על השוואת הזמנים בהם אותו אות מגיע לאנטנות השונות. גם בשיטה זו, ככל שהאות נקלט על ידי יותר אנטנות, כך ניתן להגיע לאיכון ברמת דיוק יותר גבוהה.

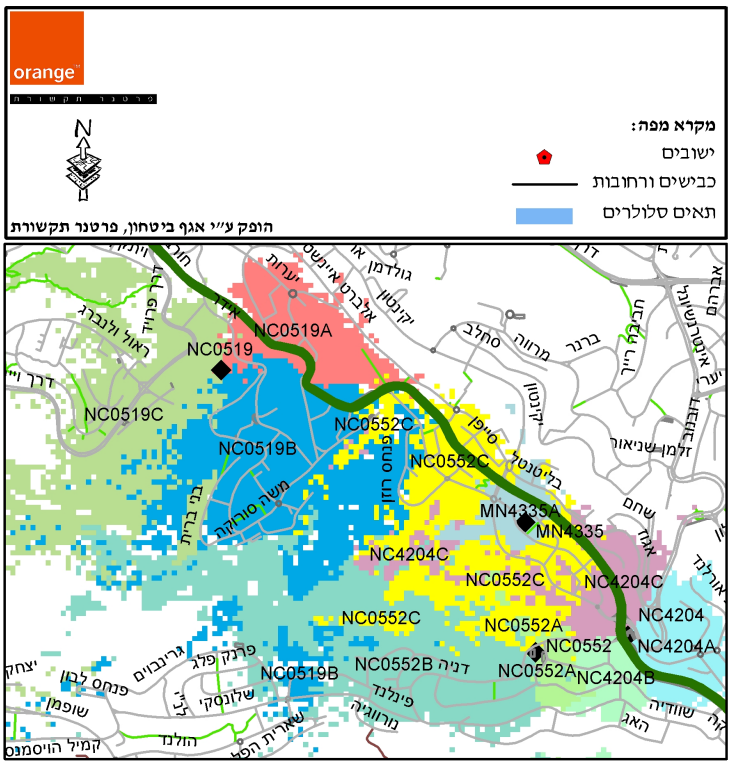
## <u>פרק שני: דיוק איכון סלולרי – נתונים מספריים</u>

### <u>איכון סלולרי בסיסי</u>

איכון סלולרי ברמת רשומו השימוש מספק נתוני מיקום בדיוק של תא של אנטנה סלולרית. לכל אנטנה יש אזור כיסוי, בו היא האנטנה הדומיננטית, כלומר האנטנה החזקה ביותר. ככל שהטלפון מתרחק מאזור הכיסוי של האנטנה, כך גדל הסיכוי שהוא ייקלט על ידי אנטנה אחרת. מפות הכיסוי הן מפות סטטיסטיות, ולכן איכון ברמת האנטנה קובע שבסבירות גבוהה מכשיר הטלפון הנייד נמצא בגבולות אזור כיסוי נתון[4]. אולם, גם אם לפי הנתונים מכשיר טלפון נייד נרשם כמשויך לאנטנה מסוימת, קיים סיכוי שהטלפון היה דווקא באזור של אנטנה סמוכה, ובשל תנאי מזג האוויר, תנועה של המכשיר או עומס מקומי על הרשת, המכשיר שויך באותו זמן לאנטנה אחרת.

4 זאת הפשטה מסוימת; בקו הגבול בין תאים סמוכים, יש סיכוי של 50% שהמכשיר יקלט באנטנה אחת ו-50% שיקלט באנטנה האחרת.

להלן דוגמה למפת אזורי כיסוי של אנטנות סלולריות (בדוגמה זו, רשת דור 2 של פרטנר):




מפת אזורי הכיסוי תלויה בצפיפות הגאוגרפית של האנטנות[5]. באזורים אורבניים צפופים, המרחק בין אנטנות הוא כ-100 עד 200 מטר, ולכן האיכון מספק מיקום ברזולוציה של 50 עד 100 מטרים. במקומות הומי אדם, כגון קניונים ובנייני משרדים, פרושות אנטנות זעירות, ואז האיכון מדויק ברמת תחומי המבנה וסביבתו הקרובה. באזורים מבודדים עם מעט אנטנות, כגון חוף הים, רמת הדיוק יורדת בהתאם, והאיכון עלול לפספס בכמה מאות מטרים.

## איכון סלולרי רציף

איכון עפ"י נתוני האיתות של הטלפונים הניידים תלוי בעיקר במספר האנטנות שקולטות את האותות של הטלפון. גם אנטנות של רשתות אחרות קולטות ורושמות את האותות. פרטי האותות הנקלטים בכל האנטנות יחדיו מאפשרים להעריך את המיקום של מכשיר הטלפון הנייד בדיוק רב. באזור אורבני צפוף, בהנחה שהמכשיר לא נע ואין הפרעות מיוחדות, ניתן לאכן את המכשיר הסלולרי בדיוק של פחות מ-5 מטרים.

המגבלה המשמעותית ביותר של איכונים סלולריים היא שהם מספקים מידע מרחבי דו-מימדי. נתוני מיקום מאפשרים למצוא את הבניין בו נקלט המכשיר הנייד, אך קשה מאוד לאתר באיזו קומה הוא נמצא. עם זאת קיים מכשור מיוחד המאפשר לאכן באופן מדויק מכשיר יעד.

**<u>סיכום ביניים</u>: בתנאים מיטביים איכון סלולרי רגיל מפיק נתוני מיקום בדיוק של כ-50 עד 100 מטר; בתנאים מיטביים איכון סלולרי רציף מפיק נתוני מיקום בדיוק של פחות מ-5 מטרים. האיכון מספק מידע מרחבי (דו-מימדי), ללא מימד הגובה.**

## השפעת תנאים שונים על דיוק האיכון

דיוק האיכון הסלולרי תלוי בפרמטרים סביבתיים רבים, להלן חלקם:

5 אתר GovMap של המרכז למיפוי ישראל מציג את פריסת האנטנות:
https://govmap.gov.il/?c=219355,631917&z=7&lay=CELL_ACTIVE,ANTENA_HAKAMA

- הצפיפות הגאוגרפית של האנטנות – ככל שיש יותר אנטנות בשטח, כך האיכון יותר מדויק.
- הדור של הטלפון ושל הרשת – איכון של טלפון מדור שני פחות מדויק מאיכון של טלפון מדור רביעי, גם בשל פרוטוקול שונה וגם בשל פריסה צפופה יותר של אנטנות דור רביעי.
- עוצמת האות – ככל שהטלפון פועל בעצמה גדולה יותר, כך האיכון יותר מדויק; הפחתת העצמה פוגעת באיכות התקשורת, מאריכה את חיי הסוללה ומורידה את דיוק האיכון.
- קצב האיתות – ככל שהקצב גבוה יותר, כך האיכון יהיה מדויק יותר, כי נאספים באותו פרק זמן יותר אירועים לניתוח נתוני המיקום.
- הפרעות ומיסוכים – קירות עבים מפחיתים את האות בעוצמה שונה לכל כיוון, ולכן יותר קשה לאכן את המיקום של טלפון הנמצא בבניין מאסיבי. גם מזג האוויר יכול להשפיע על דיוק האיכון.
- מצב הפעילות של הטלפון – בעת שיחה או העברת נתונים התקשורת הטלפון משדר בעוצמה רבה יותר, ולכן האיכון מדויק יותר לעומת איכון של טלפון במצב idle.
- פרופיל התנועה של הטלפון – ניתן לאכן באופן מדויק טלפון במכונית שנוסעת בכביש במהירות קבועה, גם באזורים עם צפיפות אנטנות נמוכה. באופן דומה, טלפון שלא זז ממקומו מאפשר איכון באמצעות מספר רב יותר של דגימות.
- יעילות פחותה במרחב צפוף (קניונים, שווקים ומרכזים הומי אדם) – אם יש הרבה מכשירי טלפון נייד במרחב, יותר קשה לזהות מיקום מדויק של מכשיר ספציפי.

## חלק שני: איכוני השב"כ, דיוקם ומגבולותיהם

### פרק שלישי: מדוע צריך את עזרת שירות הביטחון הכללי?

כדי להתמודד עם התפרצות מגפה, חייבים לערוך חקירות אפידימיולוגיות מהירות ויעילות כדי לקטוע את שרשראות ההדבקה. לנתונים אודות המקומות בהם שהה חולה קורונה, לפני שהתגלה ונכנס לבידוד, חשיבות עליונה לחקירות אלו. לא ניתן לצפות שהחולה יזכור את כל המקומות בהם הוא שהה. אחת הדרכים המעשיות לרענן את זכרונו של החולה, היא להשתמש בנתוני המיקום של מכשיר הטלפון הנייד, ולברר מה עשה בכל מקום בו שהה.

רוב החולים מתנגדים, מן הסתם, לעריכת חיפוש פורנזי במכשיר בטלפון הנייד. בדיקה כזו חושפת את המידע האישי הפרטי השמור בטלפון של החולה. במקום זאת, אפשר לפנות אל מפעילי הרשת ולקבל את נתוני המיקום של מכשיר הטלפון הנייד.

חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (להלן – חוק נתוני תקשורת) מסדיר את האופן בו רשויות החקירה יכולות לקבל נתוני תקשורת אודות מנויים ברשת. סעיף 3 לחוק נתוני תקשורת מתיר שקבלת נתוני תקשורת עם צו בית משפט, וסעיף 4 מאפשר לקבל נתונים במקרים דחופים גם ללא צו של בית משפט.

חוק נתוני תקשורת נותן לרשויות כלים חוקיים לקבל נתוני מיקום לצורך חקירות אפידימיולוגיות. אם חולה הקורונה נותן אישור לאיכון מכשיר הטלפון הנייד שלו, לא צריך צו בית משפט, כי ניתנת הסכמת בעל הטלפון לביצוע בדיקת איכון אודותיו.

#### למה נעשה שימוש באיכונים של השב"כ?

החוק הקיים מספק מענה לצורך איתור מסלול התנועה של חולה קורונה. אם החולה מאשר איכון תנועותיו, אין בעיה לקבל את המידע ללא צו; אם אינו מאשר, ניתן להוציא צו לקבלת הנתונים ללא הסכמתו. הכלי של השב"כ מיועד לאתר אנשים שאינם חולים, אשר קיימת חפיפה בין נתוני המיקום שלהם ונתוני המיקום של חולים מאומתים. לשם כך, השב"כ בוחן את נתוני האיכון של כל המכשירים הידועים ברשת, ומצליב את הנתונים עם נתוני המיקום של חולים ידועים.

רונן ברגמן פרסם כתבת תחקיר מעמיקה ומאירת עיניים על הכלי של השב"כ[6]. לפי הכתבה, השב"כ מקבל נתוני איכון מחברות הסלולר מכוח סעיף 11(ב) לחוק שירות הביטחון הכללי, התשס"ב–2002: "**ראש הממשלה רשאי לקבוע בכללים כי סוגי מידע המצויים במאגרי מידע של בעל רישיון, שיפורטו בכללים, דרושים לשירות לצורכי מילוי תפקידיו לפי חוק זה, וכי על בעל הרישיון להעביר מידע מסוגים אלה לידי השירות**". לפי הכתבה, בעלי הרישיון נדרשים להעביר באופן שוטף את נתוני המיקום הרציפים של כל המכשירים ברשת, ולכן השב"כ לא צריך הרשאה מיוחדת לצורך איכון כל אזרחי המדינה. נקודה ראויה לציון היא שלפי התחקיר, לא נסתרת ההנחה כי המידע נשמר לצמיתות[7].

סעיף 11 לחוק שירות הביטחון הכללי, התשס"ב–2002 לא מגדיר את טיבו של המידע המועבר. עו"ד אלי בכר, לשעבר יועמ"ש השב"כ, פרסם לאחרונה את ספרו "**שב"כ במבחן: ביטחון, משפט וערכי הדמוקרטיה**". לדבריו, סוגי המידע שבעלי הרישיונות מצווים להעביר לשב"כ מצויים בכללים ואינם מפורטים בחוק. לדבריו מדובר בנתוני מיקום (איכון של ציוד הקצה שנמצא בידי המנוי); נתוני מנוי (סוג השירות הניתן לו, שמו, כתובתו, מספר הזיהוי של המנוי, פרטים של אמצעי התשלום, הכתובת שבה הותקן מתקן הבזק ונתונים מזהים של המתקן ברשת המנוי); ונתוני תעבורה (סוג המסר המועבר, נתונים מזהים של מתקן בזק שהוא מקור המסר, יעדו או נתיב שלו, נתונים מזהים של המנוי שהוא מקור המסר או יעדו, מועד השידור או הקבלה של המסר, משך המסר, נפחו או היקפו). סוגי מידע אלו תואמים את הגדרה "נתוני תקשורת" בחוק נתוני תקשורת – נתוני זיהוי, נתוני מיקום, נתוני מנוי ונתוני תעבורה.

## <u>פרק רביעי: הגדרות "מידע טכנולוגי" שבחוק איכוני השב"כ</u>

החוק מגדיר "מידע טכנולוגי" כנתוני זיהוי, נתוני מיקום ונתוני התקשרויות. בפועל השב"כ אוסף ומעבד נתונים שלא הוגדרו בחוק, ועושה שימוש בנתוני התקשרויות, שאינם נדרשים לצורך איכון מכשירי הטלפון הנייד.

### <u>הגדרת "נתוני זיהוי" כוללת מידע שאינו נמצא בידי ספקי התקשורת</u>

"נתוני זיהוי", לפי חוק איכוני השב"כ, כוללים – שם, מספר זהות, מספר טלפון ותאריך לידה. בחוק נתוני תקשורת, "נתוני זיהוי" כוללים – שם, מספר זיהוי או מספר תאגיד, מען ומספר טלפון.

עבור מנויים בתוכניות תשלום מראש (Prepaid), כגון Big Talk, Talkman, Hotalk, Talk&Go ודומיהן, אין בידי ספקי התקשורת מידע אודות שם המנוי או תעודת הזהות שלו, ומידע זה לא מועבר לשב"כ. כמו כן, ספקי התקשורת לא מחזיקים בהכרח את תאריך הלידה של מנוייהם, וגם מידע זה לא מועבר לשב"כ.

כיצד השב"כ מעבד מידע טכנולוגי הכולל נתונים שלא נמסרו לו על ידי ספקי התקשורת? חוק איכוני השב"כ מתיר לעשות שימוש רק בחלק קטן ומוגדר של היכולות הטכנולוגיות של הכלי. חיבור של מידע שנמסר לשב"כ מספקי התקשורת יחד עם מידע שהגיעו ממקורות אחרים, פירושו שלמרות הגבלות החוק, נעשה שימוש ביכולות טכנולוגיות נוספות, כגון חיבור הכלי עם מאגרי מידע ממשלתיים[8].

### <u>האם המידע הטכנולוגי כולל את מספר המכשיר (IMEI)?</u>

כפי שהוסבר בחלק הראשון, ספקי התקשורת מעבירים רשומות שימוש ורשומות איכון שוטף הכוללות מספר ייחודי של המנוי (IMSI) ומספר ייחודי של המכשיר (IMEI). סעיף 6(א)(1) לחוק נתוני תקשורת מסדיר העברה של "נתוני זיהוי של מנוי", כלומר IMSI, וכן "מספר מזהה של מכשירי טלפון או רכיב מרכיביהם", כלומר IMEI. לעומת חוק נתוני תקשורת, חוק איכוני השב"כ מתיר לעשות שימוש במידע טכנולוגי, שאינו כולל את נתוני הזיהוי של מכשירי הטלפון. לכן לפי החוק, כפי שהוא מנוסח כיום, נאסר על השב"כ לעשות שימוש ברשומות השימוש וברשומות האיכון השוטף, הכוללות בין היתר גם נתוני IMEI.

---

6 רונן ברגמן ועידו שברצטוך, "הכלי", מאגר המידע הסודי של השב"כ, אוסף נתונים על כל אזרחי מדינת ישראל ויודע: איפה הייתם, עם מי דיברתם, ומתי עשיתם את כל זה", ידיעות אחרונות 27/03/2020.

7 תגובת השב"כ, לפיה "נקבעו כללים והוראות מפורטות בדבר דרכי שמירת המידע וביעורו" אינה סותרת את ההנחה לפיה לא נקבע מועד מוגדר לביעור המידע, ומכאן שהמידע יכול להישמר לצמיתות.

8 כל המאגרים הממשלתיים פתוחים בפני שירותי הביטחון עפ"י היתר לגילוי ידיעות, ללא צורך בצו משפטי.

**<u>מדוע מידע טכנולוגי כולל "נתוני התקשרויות"?</u>**

אחד הנושאים המטרידים ביותר בהגדרת "מידע טכנולוגי", הוא ההיתר לעבד נתוני התקשרויות כחלק מהמידע הטכנולוגי המותר. "נתוני התקשרויות" כוללים את מספר הטלפון של המתקשר, מספר הטלפון של יעד ההתקשרות ומועד ההתקשרות. זו הגדרה מקבילה להגדרה "נתוני תעבורה" בחוק נתוני תקשורת. מבחינה טכנית, מדובר על הנתונים הנאספים כחלק מרשומות השימוש של ספקי התקשורת.

לצורך איכון מכשירי הטלפונים הניידים, השב"כ עושה שימוש בנתוני מיקום שמתקבלים מספקי התקשורת. מדוע השב"כ צריך גם את נתוני ההתקשרות? מכיוון שאיננו יודעים כיצד הכלי של השב"כ פועל, ניתן להעלות על הדעת כמה סיבות אפשריות לשימוש בנתוני התקשרויות כחלק מהמידע הטכנולוגי.

<u>הסיבה הראשונה</u> היא סיבה טכנית. הכלי של השב"כ הוא מערכת טכנולוגית שנבנתה ופועלת באופן מסוים. אופן הפעולה הרגיל של המערכת הוא קבלת נתוני השימוש ונתוני המיקום באופן ממוכן מספקי התקשורת. ייתכן שהדרך בה הכלי בנוי לא מאפשרת להפעיל אותו רק עם נתוני האיכון השוטף, ללא נתוני השימוש.

<u>הסיבה השנייה</u> נוגעת לזיהוי מנויים לא רשומים. ספקי התקשורת אינם מעבירים לשב"כ נתונים אודות זהות מנויים בתוכניות עם תשלום מראש. מערכות האיכון יכולות לאתר שמנוי מסוים היה בקרבת חולה מאומת, אך לא יודעות לתרגם את מספר הטלפון לנתוני זיהוי, שישמשו לאחר מכן את משרד הבריאות. דרך לקשר בין מספר הטלפון לבין זהות המנוי היא באמצעות מחקר תקשורת. מחקרי תקשורת מתבססים על ניתוח התקשרויות בין המנוי הלא ידוע לבין מנויים ידועים. הבעיה עם אפשרות זו היא שחוק איכוני השב"כ לא מאפשר ביצוע מחקרי תקשורת מסוג זה.

<u>הסיבה השלישית</u> היא מקרים של כמה מכשירי טלפון נייד עם אותו מספר מנוי. מנויים רבים מחזיקים מכשיר טלפון נייד אישי, וטלפון נייד נוסף, עם אותו מספר, ברכב. כלומר, עבור אותו מספר מנוי (IMSI), יש שני מכשירים עם נתוני זיהוי (IMEI) שונים. ייתכן שהשב"כ נדרש לנתוני ההתקשרויות כדי להבחין איזה מכשיר טלפון נייד שימש את המנוי.

<u>סיבה רביעית</u> היא שדיוק האיכון תלוי במצב הפעולה של מכשיר הטלפון הנייד. בעת ביצוע התקשרות עוצמת השידור של הטלפון עולה, ולכן האיכון הרבה יותר מדויק. נתוני ההתקשרות מאפשרים לדעת האם הטלפון היה במצב תקשורת בעת מדידת האות.

**תהא הסיבה אשר תהא, אין מקום להתיר לשב"כ לעשות שימוש בנתוני ההתקשרות, ויש להסיר את נתוני ההתקשרות מהמידע הטכנולוגי שהותר לשב"כ לעבד לפי חוק איכוני השב"כ.**

## <u>חלק שלישי: יעילות איתורים בעזרת השב"כ וייעול חקירות אפידימיולוגיות</u>

קיימת תפיסה הרואה בטכנולגיות האיכון של השב"כ פתרון קסם למיגור התפרצות הקורונה. זו תפיסה שגויה ומסוכנת. לכלי של השב"כ יכולות מסוימות, אבל היעילות שלו מוגבלת. בחלק זה נבחן את יעילות הכלי של השב"כ ויעילות חקירות אפידימיוליגיות. נתייחס לאיכות תוצרי האיכונים של השב"כ, כפי שעולה מהנתונים הפומביים ונרחיב על הצורך במתן כלים טכנולוגיים שיבואו במקום איכונים אלו.

## <u>פרק חמישי: דיוק טכנולוגית האיכונים של השב"כ</u>

### <u>יעילות האיתורים של השב"כ</u>

עפ"י דיווחים מס' 6 ו-7 של משרד הבריאות, בשבוע מיום 10/05/2020 ועד ליום 16/05/2020, נשלחו בקשות ביחס ל-190 חולים; התקבל מידע אודות 93 חולים מאומתים ונשלחו 765 מסרונים אודות מגעים אפשריים; אותרו 20 חולים ע"י השב"כ ו-71 חולים ע"י חקירה אפידמיולוגית.

עפ"י דיווח מס' 7 ו-8 של משרד הבריאות, בשבוע מיום 17/05/2020 ועד ליום 24/05/2020, נשלחו בקשות ביחס ל-91 חולים; התקבל מידע אודות 35 חולים מאומתים ונשלחו 546 מסרונים אודות מגעים אפשריים; אותרו 18 חולים ע"י השב"כ ו-46 חולים ע"י חקירה אפידמיולוגית.

עפ"י דיווח משרד הבריאות מיום 09/07/2020, בשבוע מיום 01/07/2020 בלילה ועד ליום 08/07/2020 בלילה, נשלחו בקשות ביחס ל-6,321 חולים; נשלחו 70,949 מסרונים אודות מגעים אפשריים; אותרו 3,495 חולים ע"י השב"כ, מתוכם 1,027 עלו גם בחקירות אפידימיולוגיות. לפי אתר "נגיף הקורונה בישראל – תמונת מצב" של משרד הבריאות, באותו השבוע התגלו כ-7,500 חולים חדשים.

<u>יעילות האיתורים</u>: בשבוע של ה-10/05/2020, התגלו בעזרת השב"כ 20 מקרים מתוך 765 חשדות, כלומר זיהוי נכון ב-2.6% מהמקרים. בשבוע של ה-17/05/2020, התגלו בעזרת השב"כ 18 מקרים מתוך 546 חשדות, כלומר זיהוי נכון ב-3.3% מהמקרים. בשבוע של ה-01/07/2020, התגלו בעזרת השב"כ 3,495 מקרים מתוך 70,949 חשדות, כלומר זיהוי נכון ב-4.9% מהמקרים.

**סיכום ביניים: לפי נתוני משרד הבריאות, אחוז ההצלחה של זיהוי חולים על ידי השב"כ עומד על בין 3% ל-5%.**

**<u>איתורים בעזרת השב"כ לעומת איתורים בעזרת חקירות אפידימיולוגיות</u>**

לפי דיווח מס' 9, עד יום 31/05/2020, התגלו כ-17,000 חולים בישראל. מתוכם, השב"כ איתר כ-5,800 חולים, וחקירות אפידימיולוגיות איתרו כ-13,000 חולים. 1,730 חולים אותרו גם בעזרת השב"כ וגם בעזרת חקירות אפידימיולוגיות. כלומר, הכלי של השב"כ, כשלעצמו, תרם לאיתור 25% מהחולים. 75% מהחולים אותרו בעזרת חקירות אפידימיולוגיות או פניות של החולים.

בשבוע מיום 01/07/2020 עד 08/07/2020, השב"כ איתר באופן בלעדי רק כשליש מהחולים (2,468 מקרים מתוך כ-7,500 חולים חדשים), בעוד שני שליש מהחולים אותרו בעזרת חקירות אפידימיולוגיות או פניות של החולים.

**נתונים אלו אינם מצדיקים שימוש בכלי של השב"כ, אלא מוכיחים כי נדרש עיבוי החקירות האפידימיולוגיות בכלי חקירה דיגיטליים. על כך בפרק הבא.**

## <u>פרק שישי: שיפור מערך החקירות האפידימיולוגיות</u>

**<u>קריסת מערך החקירות האפידימיולוגיות</u>**

הגענו למצב בו המערכת אינה יכולה לטפל בלמעלה מאלף מקרי הדבקות חדשים מדי יום. הכישלון של הנוגעים בדבר לא יכול להכשיר פגיעה קבועה ומתמשכת בפרטיות האזרחים, בדמות הפעלת הטכנולוגיות המיוחדות של השב"כ לבלוש אחר אוכלוסיית המדינה. הוראת השעה שנקבעה, עד ליום 22/07/2020, כבר גורמת לפגיעה קשה מאוד בפרטיות באזרחים. המינימום הנדרש, הוא לתת להיתר לביצוע איכוני השב"כ לפקוע בתום התקופה, ולחייב את הרשויות לעשות שימוש בחלופות אזרחיות, כפי שנעשה בשאר העולם.

במצב החירום הנוכחי, חלה על הרשויות חובה כפולה ומכופלת לפעול בכל דרך כדי לעבות ולייעל את מערכי החקירות האפידימיולוגיות. הרשויות חייבות ולבחון דרכים לשיפור המערכים הקיימים ולהטמעה מהירה של חלופות טכנולוגיות אזרחיות. **מערך החקירות הקורס אינו כרטיס פתוח להפעלת איכוני השב"כ.**

**<u>השב"כ אינו הפתרון לטיפול במשבר הקורונה</u>**

השב"כ מתנגד נחרצות להפעלת יכולותיו הטכנולוגיות המיוחדות לצורך סיוע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה. בהקלטות שהובאו בחדשות 12[9], נשמע ראש השב"כ נדב ארגמן מסביר שהפתרון נמצא במערכים האזרחיים:

"מה שאני מבקש ששב"כ לא נכנס כרגע לחקיקה ראשית. מה שצריך ברמת ההכשרה למקצוע ששב"כ יהיה מוכן לתת פתרון אם תהיה התפרצות ואין מענה, ולעבוד חזק, אבל חזק למען הפרוייקטור שיודע לנהל את זה, בשביל שיהיה פתרון אזרחי למדינת ישראל לשנים הקרובות... זה אומר שצריך להיות מספיק שיודעים לעשות את זה – יודעים לבוא בדברים עם אותם חולים ולסגור מעגל מקצה לקצה תוך פרק זמן קצר. כשמדובר ב-200, 300, 400 חולים ניתן לעשות את זה, כשמדובר באלפים אי אפשר לעשות את זה כנראה

9 "ההקלטות חושפות: ראש השב"כ ביקש להימנע ממעקב אחר אזרחים – נתניהו לחץ", חדשות 12, 21/06/2020.

בשיטה הזאת וצריך ללכת לטכנולוגי... במצב שיש תחלואה רחבה מאוד ולא יהיה פתרון אחר יהיה נכון להעביר אל השירות."

אריק ברבינג, לשעבר ראש אגף הסיגינט-סייבר בשב"כ, הסביר בראיון שזה אינו תפקידו של השב"כ: "אנחנו לא במצב החירום שהיה בסבב ראשון אלא בשגרה מבצעית של קורונה, ולכן הדרך הנכונה הייתה לפתח באופן מידי אפליקציה אזרחית, שתבצע את אותה משימה".

**<u>איכוני השב"כ כאינדיקציה ראשונית לחקירה אפידימיולוגית</u>**

איכוני השב"כ אינם כלי מדויק. השב"כ יכול לספק אינדיקציה שבסבירות של 90%, או בסבירות של 50%, או בסבירות של 10%, או בסבירות של 5%, זוהה מגע קרוב עם חולה מאומת. הנתונים אודות יעילות איתורי השב"כ, לפיהן רק בין 3% ל-5% מההחשדות מתגלות כמקרי הדבקה אמיתיים, מראים כי סף ההחלטה שנבחר מכניס אנשים רבים לבידוד שלא לצורך.

איכוני השב"כ מספקים מידע הסתברותי, ועל הרשויות להתייחס לנתונים בהתאם. לפי פרסומים בתקשורת[10], ראש השב"כ הביע את דעתו שאיכוני השב"כ אמורים להוות חומר גלם עבור מערך חקירה אפידמיולוגי מלא ויעיל באחריות משרד הבריאות. לפי אותם פרסומים, בדיון שנערך ביום 08/07/2020 הוא דרש ממשרד הבריאות לשפר באופן מידי את תהליכי העבודה ואת התייחסותם לנתונים.

משרד הבריאות מתייחס לכל הודעה אודות מגע קרוב כאל הדבקה ודאית – עד שיוכח אחרת. לכן המשרד מחייב את מי שמקבל הודעה אודות זיהוי מגע קרוב להיכנס לבידוד למשך שבועיים. כאמור, הכלי של השב"כ מספק רק אינדיקציה סטטיסטית אודות אפשרות לקיום מגע קרוב. אינדיקציה זו אמורה להיות נקודת פתיחה של חקירה אפידימיולוגית, שלאחריה יוחלט אם האדם נדרש להיכנס לבידוד מלא או לא.

במקום לשלוח את כל המאוכנים לבידוד של 14 יום, המשרד צריך לשלוח אותם לבידוד זמני, עד לקבלת תוצאות בדיקת הקורונה ולסיום חקירה אפידימיולוגית מקדמית.

**<u>הוספת תקנים</u>**

לפי ניתוח האגודה לזכויות האזרח בישראל, בישראל עוסקים כיום בחקירות אפידימיולוגיות כ-300 אחיות אפידימיולוגיות, שיעור של כ-5.5 חוקרים לכל 100,000 תושבים. לעומת זאת, בקליפורניה עומד השיעור על 50.6 חוקרים לכל 100,000 תושבים, ובמחוז ווהאן שבסין על 81.1 חוקרים לכל 100,000 תושבים. אין פלא אם כך שמערך החקירות האפידימיולוגיות בישראל לא מסוגל להתמודד עם ההתפרצות הנוכחית.

חובה על המדינה לעבות את מערך החקירות באופן משמעותי עם כוח אדם איכותי. כמו כן, חובה לספק לחוקרי המערך כלים טכנולוגיים לייעול החקירה האפידימיולוגיות. כוח אדם לבדו לא יספק את התוצרים הנדרשים, אם לא ניתנים לחוקרים כלים מתאימים לביצוע עבודתם.

**<u>בסיס חקירה עפ"י נתוני איכון של החולה</u>**

הבסיס לחקירה אפידימיולוגית הוא התחקות אחר תנועות החולה בימים שלפני גילוי המחלה. רוב החולים מתקשים לשחזר את תנועותיהם, ואיכון באמצעות מכשיר הטלפון הנייד מספק בסיס אמין לפתיחת החקירה.

הכלי של השב"כ מאתר מסלולי תנועה של החולים, אך זה שימוש בפטיש של חמש קילו מקום בו נדרש אזמל מנתחים. ברגע שאדם מאותר כחולה קורונה, צריך לבקש ממנו הסכמה לאיכון מכשיר הטלפון הנייד שברשותו, תוך הסבר כי המידע יישמר בסודיות ולא ישמש לכל מטרה אחרת. אין סיבה שאדם שנדבק בנגיף לא יסכים לאיכון, שהרי הוא מגיע לחקירה אפידמיולוגית כדי לעזור לעצור את התפשטות המחלה[11].

לאחר הפקת נתוני האיכון, החוקר האפידימיולוג יכול לשבת עם החולה ולהתחקות יחדיו אחרי המקומות בהם ביקר בימים שלפני גילוי המחלה. בכל מקום בו נראה כי קיימת סכנת הדבקה, החוקר יבדוק מי

10 "דיון דחוף על 'איכוני השב"כ' והתוכנית לגל השני - שנגנזה", כיכר השבת, 07/07/2020.

11 אם החולה אינו מוכן לתת את הסכמתו לאיכון מכשיר הטלפון הנייד שברשותו, ללא סיבה מספקת, אפשר לקבל את הנתונים ללא הסכמתו מכוח צו בית משפט או מכוח החלטת קצין משטרה.

חשוף להידבקות אפשרית, וכך החקירה תוכל להביא לקטיעה מהירה של שרשראות הדבקה. נתוני האיכון הגולמיים לא ימסרו לאף גורם ויושמדו עם השלמת החקירה האפידימיולוגית.

**<u>שימוש בכלי חקירה טכנולוגיים לפי צורך</u>**

רצוי לתת לחוקרים האידימיולוגיים כלים טכנולוגיים לצורך איתור מגעים אפשריים. ככלל, עדיף שכלים אלו יינתנו לשימוש חוקרים אזרחיים, תוך הקפדה על סודיות, ביטחון מידע וצמצום הפגיעה בפרטיות, במקום לתת היתר כללי לרשויות הביטחון שיפעילו את אותם כלים ללא הבחנה, עם מינימום פיקוח ותוך פגיעה בלתי מידתית בפרטיות האזרחים.

להלן כמה דוגמאות לכלים כאלו.

- שימוש בנתוני האשראי של החולה כדי לזהות מקומות בהם שהה. כמו נתוני האיכון, הפקת הנתונים כפופה להסכמת החולה, הנתונים לא ימסרו לאף גורם ויושמדו עם השלמת החקירה.
- שימוש בנתוני נסיעה בתחבורה הציבורית לפי היסטוריית השימוש בכרטיס רב-קו אישי. כמו נתוני האיכון, הפקת הנתונים כפופה להסכמת החולה, הנתונים לא ימסרו לאף גורם ויושמדו עם השלמת החקירה.
- שימוש בצילומים ממצלמות אבטחה. אם אותר שחולה הסתובב בשטח ציבורי, אפשר לעשות שימוש במצלמות אבטחה כדי לאתר מגעים קרובים עם עוברי אורח.
- שימוש בנתוני קופה. אם החולה שהה בחנות, אפשר לגלות מי עמד יחד עם החולה בתור לקופה על ידי בחינת העסקאות שנערכו באותה קופה.

אלו כמובן דוגמאות בלבד. כל הפעלה של כלי טכנולוגי גורמת פגיעה בפרטיות, אך הפגיעה מידתית כי היא מצומצמת לצורך הישיר של חקירה נקודתית.

**<u>הרחבת היקף הנבדקים עפ"י שיטה דיפרנציאלית</u>**

מומלץ לחלק את הנדבקים הפוטנציאליים לקטגוריות בהתאם למידת הסיכון. הכנסת כל אדם שהיה בקרבת חולה מאומת לבידוד כפוי, גורמת כבר עכשיו לזלזול בהנחיות משרד הבריאות ומקטינה את מידת ההיענות הציבורית להוראות הבידוד. אם במקום התייחסות בינארית (היה מגע קרוב, כן או לא?), תהיה התייחסות עפ"י מידת הסיכון, מן הסתם מידת שיתוף הפעולה של הציבור תגבר.

להלן דוגמה לשיטה דיפרנציאלית כזו:

- קטגוריה ירוקה – אנשים עם חשש מועט ביותר להידבקות. למשל, שהות בחנות בה נוכח חולה מאומת, אבל לא בקרבה פיזית; שהות בקרבת אדם שנכנס לבידוד בשל חשש בינוני או גבוה. אנשים אלו ידרשו להיבדק מיידית אך לא ידרשו להיכנס לבידוד. ידרשו למעקב ולבדיקת המשך לאחר שלושה ימים.
- קטגוריה צהובה – אנשים עם חשש נמוך להידבקות. למשל, שהות בקרבה פיזית למשך זמן קצר עם חולה מאומת. אנשים אלו ידרשו להיבדק מיידית ולהיכנס לבידוד לשלושה ימים. ידרשו למעקב ולבדיקת המשך לאחר שלושה ימים. הארכת תקופת הבידוד בהתאם לתוצאות הבדיקות או להתפתחות תסמינים.
- קטגוריה כתומה – אנשים עם חשש בינוני להידבקות. למשל, שהות בקרבה פיזית חד פעמית למעלה מ-15 דקות עם חולה מאומת. אנשים אלו ידרשו להיבדק מיידית ולהיכנס לבידוד לשבוע. ידרשו למעקב ולבדיקת המשך לאחר שלושה ימים ולאחר שבוע. הארכת תקופת הבידוד בהתאם לתוצאות הבדיקות או להתפתחות תסמינים.
- קטגוריה אדומה – אנשים עם חשש גבוה להידבקות. שהות בקרבה פיזית רצופה עם חולה מאומת; בני ביתו של החולה. אנשים אלו ידרשו להיבדק מיידית ולהיכנס לבידוד מלא של 14 יום. ידרשו למעקב ולבדיקת המשך לאחר שלושה ימים ולאחר שבוע. אפשרות לקיצור תקופת הבידוד בהתאם להחלטות גורמי הבריאות.

כמובן שזו דוגמה בלבד. יודגש שקביעת מידת הסיכון להדבקה תהא בהתאם לפרמטרים רפואיים אובייקטיביים בלבד.

## פרק שביעי: חלופות טכנולוגיות נוספות

נסיים בהפניה למסמכים מקיפים שנכתבו ופורסמו על ידי מגוון חוקרים מובילים בתחומם, המציגים מגוון חלופות טכנולוגיות לאיתור מגעים. אין מדינה בעולם המערבי העושה שימוש בכלי מודיעין שנועדו למלחמה בטרור כדי לבלוש אחר אזרחים ששהו בקרבת חולי קורונה. קיימים פתרונות מידתיים יותר, המקטינים את מידת הפגיעה בפרטיות, ומספקים דיוק טוב בהרבה מהאיכונים הסלולריים של השב"כ. להלן סקירה של פרסומים אלו:

- ד"ר תהילה שוורץ אלטשולר, ד"ר ערך טוך וע"ד רחל ארידור הרשקוביץ, המכון הישראלי לדמוקרטיה, "חלופות לשימוש בשב"כ לצורך "איתור מגעים דיגיטלי" במאבק בנגיף הקורונה" – חוות דעת וסקירה בינלאומית מיום 24/05/2020.
- ד"ר תהילה שוורץ אלטשולר וע"ד רחל ארידור הרשקוביץ, המכון הישראלי לדמוקרטיה, "חלופות לשימוש בשב"כ לצורך "איתור מגעים דיגיטלי" במאבק בנגיף הקורונה", מכתב מיום 22/06/2020.
- פרופ' קרין נהון ואח', "חלופות אזרחיות להפעלת אמצעים טכנולוגיים ע"י השב"כ", מכתב מיום 23/06/2020.
- פרופ' מיכאל בירנהק ואח', "הצעת חוק להפעלת מערכת אזרחית לצמצום התפשטות נגיף הקורונה החדש", מכתב מיום 12/07/2020.
- מרכז המידע והידע הלאומי למערכה בקורונה, מסמך מס' 133, "שימוש באמצעים טכנולוגיים לאיתור מגעים בין חולים ולניטור אוכלוסיה ברבי העולם – ריכוז מידע עיתי", מסמך מיום 23/06/2020.
- אגף מערכות מידע ומחשוב, משרד הבריאות, "המגן – האפליקציה הלאומית למלחמה בקורונה", מצגת מיום 23/06/2020.
- המטה לביטחון לאומי, "חלופות לאמצעי שב"כ כעזר לשבירת שרשראות הדבקה", מצגת מיום 23/06/2020.

נשמח לעמוד לרשותכם לכל צורך,

בכבוד רב ובברכה,

צבי דביר // התנועה לזכויות דיגיטליות (ע"ר)

טל' 054-5260678 | zdevir@gmail.com