התנועה לזכויות דיגיטליות
Digital Rights Movement (ע"ר)

יום שני, 29/11/2021

לכבוד חה"כ גלעד קריב – יו"ר ועדת החוקה חוק
חה"כ רם בן ברק – יו"ר ועדת החוץ והביטחון
חברי ועדת החוקה חוק ומשפט וחברי ועדת החוץ והביטחון
הייעוץ המשפטי של ועדת החוקה חוק ומשפט ושל ועדת החוץ והביטחון

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

מעקב, איכון, וניטור של אזרחים, תוך שימוש במאגרי מידע ובאמצעים טכנולוגיים מתוחכמים, עלול לגרום פגיעה קשה בפרטיות ובחירויות האזרח הבסיסיות. משום כך אלה צעדים אסורים במדינות דמוקרטיות. גם במצב הנוכחי, אין להפעיל אמצעים חודרניים שכאלה, באופן גורף כלפי המוני אזרחים, ללא פיקוח נאות. כמו כן יש לקבוע כללים ברורים לשימוש במידע המתקבל, ולהגבילו ככל האפשר. – חה"כ ניצן הורוביץ

תקציר

איכוני השב"כ ליוו אותנו במהלך שנת 2020. השימוש באיכוני השב"כ פסק בתחילת השנה בעקבות הביקורת הציבורית, היעילות שהוכחה כנמוכה ופסק הדין של בג"ץ בנושא. עתה הוחלט להחזיר את איכוני השב"כ לצורך איתור מגעים של חולים מאומתים שנושאים את הווריאנט הדרום אפריקאי: "**בדיון הקבינט הוחלט לעשות שימוש באיכונים סלולריים, שיופעלו על ידי שב"כ, לצורך מעקב אחר מאומתים לזן האומיקרון. באמצעות האיכון יוכל שב"כ לאתר את המאומתים ובכך לקטוע את שרשראות ההדבקה. החלטה זו תיכנס לתוקף לאחר אישור שרי הממשלה, בתקנות לשעת חירום, ובמקביל, יקודם הליך החקיקה בנושא**". ביום 28/11/2021 פורסמו ברשומות תקנות שעת חירום (הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות זן אומיקורן omicorn של נגיף הקורונה החדש), התשפ"ב-2021, ונכנסו לתוקף באופן מיידי.

סיוע השב"כ מתבסס (בעיקרו) על טכנולוגיה של איכונים סלולריים. הטכנולוגיה ומגבלותיה מוסברים בחלק הראשון של המסמך. 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. 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. מגבלה משמעותית של כלי השב"כ היא שהכלי לא מאתר מגעים של מי שמחזיק בטלפון ברשת דור 2. כלומר מי שמבקש להתחמק מאיכוני השב"כ יכול להעביר את הטלפון שברשותו לשימוש ברשת דור 2 – פעולה פשוטה יחסית בכל טלפון חכם[1].

החלק השני של המסמך מתייחס לשימוש באיכונים אזרחיים במקום איכוני השב"כ. איכוני השב"כ אינם פתרון קסם למיגור מגיפת הקורונה. רק 5% מהאנשים שהוכנסו לבידוד בשל האיכונים התגלו בדיעבד כחולים. בחלק זה נרחיב על כלים טכנולוגיים שיכולים לשמש לייעול מערך החקירות האפידימיולוגיות במקום איכוני השב"כ: **בקשה וקבלת הסכמת החולה לשימוש בנתוני מיקום כבסיס לחקירה ושימוש בכלים טכנולוגיים נוספים לפי הצורך.**

השימוש באיכוני השב"כ הביא ומביא נזק כפול ומכופל: ראשית, איכוני השב"כ גרמו להסתמכות יתר על טכנולוגיה שביצועיה בינוניים; שנית, הם מונעים פיתוח והטמעת טכנולוגיות אלטרנטיביות; ושלישית, הם פוגעים באמון הציבור, וללא אמון הציבור דינן של חקירות אפידמיולוגית להיכשל.

---

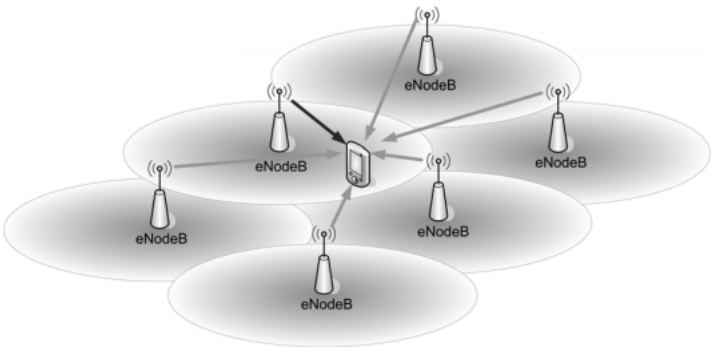
1 טלפונים חכמים מאפשרים לשנות את הגדרות התקשורת ולהגביל את התקשורת לרשתות דור 2 בלבד. למשל, בטלפונים מבוססי אנדרואיד, ניתן להיכנס להגדרות הטלפון: Settings → Wireless & Network → Mobile Networks → Preferred Network Type (או Network Mode), ולקבוע את פרוטוקולי התקשורת של הרשת הסלולרית.

חלק ראשון: טכנולוגיית האיכון הסלולרי, דיוקה ומגבולותיה

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

הטכנולוגיה שבבסיס איכון סלולרי

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[2]. כשהטלפון נמצא בתנועה, האנטנות מעבירות ביניהן את השליטה, כך שהמכשיר יקושר בכל זמן לאנטנה עם האות החזק ביותר.



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.

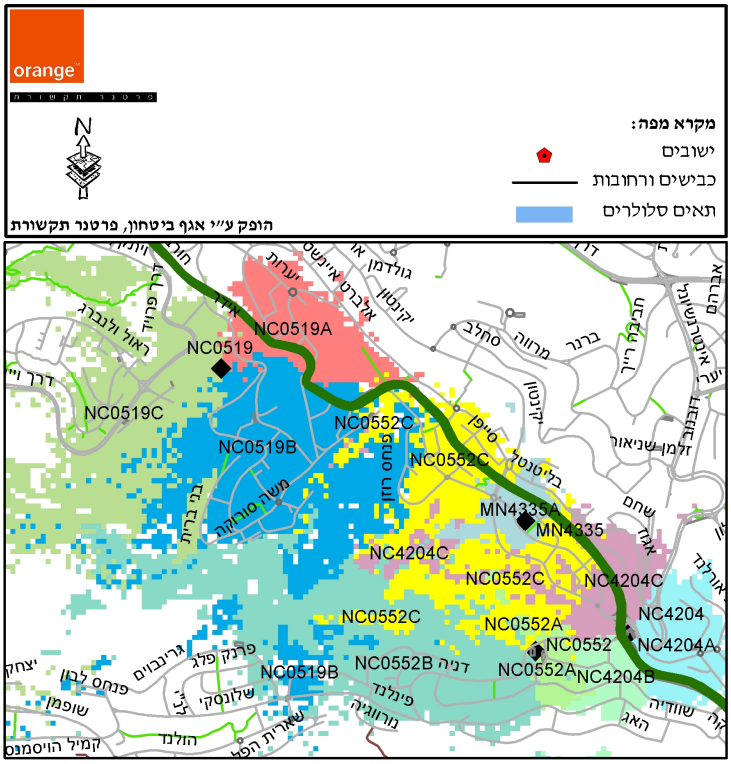
כאשר מדברים על איכונים סלולריים, כורכים יחדיו שתי טכנולוגיות שונות – איכון סלולרי בסיסי בזמן שיחה, ואיכון רציף של המכשירים המזוהים ברשת.

<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

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

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.



דוגמה למפת אזורי כיסוי של אנטנות סלולריות (רשת דור 2 של פרטנר)

הדיוק של איכון סלולרי

איכון סלולרי בסיסי

איכון סלולרי ברמת רשומות 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[3]. 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.

מפת אזורי הכיסוי תלויה בצפיפות הגאוגרפית של האנטנות[4]. 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.

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

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

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.

איכונים סלולריים 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:

- 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 – התווך העירוני כולל הרבה רפלקטורים, בולעים ומפזרי קרינה. קירות עבים מפחיתים את האות בעוצמה שונה לכל כיוון, ולכן יותר קשה לאכן את המיקום של טלפון הנמצא בבניין מאסיבי. גם למזג האוויר השפעה 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.

<u>חלק שני: איכוני השב"כ, דיוקם ומגבלותיהם</u>

מדוע אין צורך בעזרת 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 החולה 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 קבלת 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.

אז למה נעשה שימוש באיכוני השב"כ?

התשובה הקצרה היא "כי אפשר". החוק הקיים מספק כאמור מענה לאיתור 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 גם 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 במרץ 2020 כתבת תחקיר מעמיקה ומאירת עיניים על כלי השב"כ[5]. 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 הרשיון 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[6].

סעיף 11 לחוק שירות הביטחון הכללי, התשס"ב–2002 לא מגדיר את טיבו של המידע המועבר. עו"ד אלי בכר, יועמ"ש השב"כ לשעבר, הסביר כי 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 ההגדרה "נתוני תקשורת" בחוק נתוני תקשורת – נתוני זיהוי, נתוני מיקום, נתוני מנוי ונתוני תעבורה.

יעילות איכוני השב"כ

נתוני משרד הבריאות מהגל השני מראים שהיעילות של כלי השב"כ, כלומר אחוז החולים שהתגלו מבין המגעים האפשריים שאותרו בלעדית בעזרת איכוני השב"כ, נע בין 3% ל-5%. משרד הבריאות טוען ליעילות של 6.3%, אולם לפי הדיווחים האחרונים של סוף הגל השני (דיווחים 17 עד 21), השב"כ איתר בלעדית 83,073 אנשים שהיו בסבירות גבוהה במגע קרוב עם חולה ולכן נדרשו להיכנס לבידוד. מתוכם, רק 2,220 אנשים אובחנו לבסוף כחולים. **אם כן, יעילות איכוני השב"כ עומדת על 2.7% בלבד.** בתקופה זו התגלו 24,408 חולים חדשים. כלומר איכוני השב"כ הביאו לגילוי של 9.1% מהחולים בלבד, בעוד 90.9% מהחולים התגלו בעזרת חקירות אפידמיולוגיות אנושיות או בבדיקות קורונה.

---

5 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.

6 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.

מבקר המדינה התייחס בדו"ח המיוחד ליעילות הפחותה של איכוני השב"כ. הנתונים ששוחררו על ידי משרד הבריאות מראים כי מספר המאומתים בקרוב מי שבא במגע עם חולי קורונה לא שונה מבחירה מקרית בקרב האוכלוסייה באזורים באזורים עם תחלואה גבוהה. זאת ועוד, לפי מחקר של ד"ר ערן טוך ואשרת איילון מאוניברסיטת תל אביב, שימושו של הכלי של השב"כ לאיתור מגעים דוחק את המוטיבציה של האזרחים לעסוק בפעילויות אחרות שהוכחו כיעילות יותר, למשל איתור מגעים בעזרת יישומון ייעודי (הרמזור).

הדיוק הנמוך של איכוני השב"כ מכניס מאות אלפי אנשים לבידוד כפוי, שמתגלה בדיעבד כלא הכרחי. משרד האוצר העריך את הנזק הישיר כתוצאה מימי בידוד לא נדרשים בכמיליארד ש"ח, בחודש אוקטובר 2020 בלבד. לכן המשרד תומך בצמצום השימוש באיכוני השב"כ לטובת חקירות אפידמיולוגיות אנושיות:

> **אייל טולדנו, נציג אגף התקציבים, הציג את עלות הבידוד. באוקטובר [2020] דווח על 300 אלף חייבי בידוד, מתוכם כמחצית מאיכוני השב"כ. המשמעות המשקית היא אובדן תוצר של כ-970 מיליון ש"ח מאובדן תוצר בלבד. אם וכאשר יאושר תשלום חלקי של המדינה על ימי הבידוד, העלות התקציבית תהיה בסדר גודל של מאות מיליוני ש"ח בחודש. בשל כך, המשרד תומך בקיצור הבידוד במידת האפשר, וכן בצמצום האיכונים והתבססות על חקירות אפידמיולוגיות אנושיות.**

<u>מגבלות טכנולוגיות של איכוני השב"כ</u>

הדיוק המוגבל של איכוני השב"כ והחיקוף הגבוה של איתור מגעים שגוי הוא רק חלק מהבעיה הטכנולוגית של כלי השב"כ. נחום ברנע חשף לפני כשנה כי הכלי של השב"כ לא מסוגל לאתר מגעים של טלפונים פשוטים, כמו הטלפונים הכשרים שבשימוש האוכלוסייה החרדית[7]:

נבצר מהשב"כ

> בגיליון סוכות של "משפחה" מסתתר סקופ: בטור שכתבו [יוסי] אליטוב ואבי בלום מסופר שראש השב"כ, נדב ארגמן, דיווח בתחילת המשבר לקבינט, בסודי סודות, שיש בעיה – הטכנולוגיה של השב"כ לא מסוגלת לפרוץ[8] לטלפונים הכשרים של החרדים. "אין לנו שום יכולת לאכן אותם", אמר.
>
> ביררתי את הסיפור עם גורם מוסמך. הידיעה נכונה, הודה. לחרדים יש שני סוגים של טלפונים כשרים: מכשירים ישנים, דמויי קונכיה, ממורשת נוקיה, וסמארטפונים שהוגבלו בשימוש. בסוג השני השב"כ יודע לטפל; בראשון נבצר ממנו.
>
> שרי הקבינט בחרו להתעלם מהבעיה. "נתניהו גילגל את עיניו לשמיים ועבר לנושא הבא", כתב העיתון. "באותם רגעים בחרה מדינת ישראל לוותר על 15 אחוז מאזרחיה, להפקיר את החרדים ולהפוך את המגזר למדגרת קורונה".

הטענה של אליטוב, בלום וברנע היא שהשב"כ לא יודע להתמודד עם איכון של טלפונים פשוטים[9]. כלומר, כל אדם שרוצה להימנע מאיכוני השב"כ צריך לעדכן את הגדרות מכשיר הטלפון הנייד שברשותו כך שהטלפון יפעל ברשתות דור 2 בלבד – פעולה טכנית פשוטה יחסית ברוב הטלפונים החכמים[10].

יודגש כי אין זאת מגבלה טכנולוגית הנובעת מאופן הפעולה של האיכונים הסלולריים, אלא מגבלה בפיתוח של כלי השב"כ. נראה כי הכלי לא תוכנן ולא נבנה כדי להתמודד עם איכונים של טלפונים מדור 2, ולכן אינו יכול לספק מענה נאות לאיתור מגעים של בעלי טלפונים העושים שימוש ברשת דור 2.

---

7 נחום ברנע, "שייגעצ, תוריד את המסכה", ידיעות אחרונות 08/10/2020.

8 השב"כ לא פורץ לטלפונים הסלולריים אלא רק מאכן את מיקומם, ולכן השימוש במילה "לפרוץ" בהקשר זה מטעה.

9 מבחינה טכנולוגית, אין מגבלה המונעת מכלי השב"כ לאכן טלפונים דור 2, למעט מידת דיוק פחותה של האיכון שנובעת מהבדלים טכנולוגיים בין רשתות GSM (דור 2) ורשתות UMTS (דור 3) ו-LTE (דור 4). נראה כי המגבלה היא במערכת שמחשבת את ההסתברות (הסיכוי) למגע קרוב בין מכשירים סלולריים לפי נתוני המיקום. ככל הנראה המערכת הותאמה לעבוד עם נתוני מיקום רציפים של טלפונים מתקדמים (טלפונים דור 3 ודור 4), שהם רוב הטלפונים שבשימוש בארץ, אך המערכת לא הותאמה לעבוד עם נתוני מיקום רציפים של טלפונים פשוטים וטלפונים כשרים (טלפונים דור 2). נראה גם שהמערכת לא יודעת להשוות בין נתוני המיקום של טלפונים מתקדמים לעומת נתוני המיקום של טלפונים פשוטים. אם כך, אין מדובר במגבלה טכנולוגית אלא במגבלת פיתוח של המערכת.

10 ראו ה"ש מס' 1 לעיל.

הפתרון האמיתי – שיפור מערך החקירות האפידימיולוגיות

מטרת חקירות אפידמיולוגיות היא לאתר מגעים אפשריים של החולה הנחקר עם אנשים אחרים. ההנחה הבסיסית היא שהנחקר מעוניין לשתף פעולה ולצמצם את התפשטות המחלה. גם נחקר משתף פעולה יתקשה להיזכר עם מי הוא נפגש בעשרת הימים שקדמו לגילוי המחלה. חקירה אפידמיולוגית יעילה מיועדת לרענן את זיכרונו של הנחקר באמצעים טכנולוגיים. אחד האמצעים היעילים הוא לעבור עם הנחקר על המקומות השונים בהם הוא שהה, וכך לנסות לאתר מגעים אפשריים. לשם כך ניתן לעשות שימוש בנתוני המיקום של הטלפון הסלולרי של הנחקר, אם ניתנת לכך הסכמה מצדו.

מילות המפתח הן "הסכמה" ו"שקיפות": ההסכמה היא הסכמת הנחקר לאיסוף המידע עליו, והשקיפות היא השקיפות בנוגע למידע שנאסף ולאופן השימוש בו.

הסכמה: כאשר הנחקר נותן את הסכמתו לפנות אל חברת הסלולר ולהפיק את נתוני המיקום שלו, אין בעיה חוקית להעביר את הנתונים לידי מערך החקירות האפידמיולוגיות. חוק נתוני תקשורת קובע את המסגרת החוקית להעברת נתוני איכון סלולרי. קיימים ממשקים טכנולוגיים להעברת נתוני איכון מחברות הסלולר לרשויות החקירה בארץ, ואין סיבה שמערך החקירות לא ישתמש באותם ממשקים לקבלת איכון אזרחי.

שקיפות: השקיפות היא הצגת המידע המתקבל בפני הנחקר, כדי לשחזר את המקומות בהם הוא שהה. השקיפות נוגעת גם לאופן השימוש המידע ולהגבלת תפוצתו. טופס ההסכמה צריך להבהיר שהמידע יכול לשמש אך ורק לצורכי החקירה האפידמיולוגית, לא יעשה בו כל שימוש אחר והוא ימחק כעבור זמן ידוע מראש.

באיכוני השב"כ אין לא ההסכמה ולא שקיפות. במקום שיוגשו בקשות פרטניות לקבלת נתוני איכון מחברות הסלולר באפיק אזרחי, המערך עושה שימוש בנתוני האיכון שמגיעים מהשב"כ[11]. הנחקר לא מתבקש לתת את הסכמתו להפקת נתוני האיכון, הוא לא מודע להיקף המידע שנאסף אודותיו, ואין לו כל שליטה על מידע זה.

נראה כי משרד הבריאות מעדיף להסתמך על נתוני האיכון של השב"כ משתי סיבות. הסיבה הראשונה היא קלות השימוש בממשק קיים. בידי משרד הבריאות ממשק מידע שמקבל את נתוני המיקום מהשב"כ ומזין אותם למערך החקירות הקיים[12]. נראה שמשרד הבריאות ומפקדת "אלון" לא הקימו ממשק מקביל לקבלת נתוני מיקום רציפים מחברות הסלולר. הסיבה השנייה היא כספית. חברות הסלולר זכאיות לקבל תשלום בגין עלות הפקת מידע, אך משרד הבריאות מעדיף לקבל את נתוני האיכון של השב"כ חינם אין כסף.

מערך החקירות האפידמיולוגיות צריך לפעול באופן מיטבי גם ללא סיוע מצד השב"כ. לא ניתן לחזור ולהסתמך על איכוני השב"כ רק בגלל שהמערכות הטכנולוגיות של מערך החקירות לא יודעות לקבל את המידע ישירות מחברות הסלולר.

שימוש בכלי חקירה טכנולוגיים לפי צורך

ניתן לתת לחוקרים האידימיולוגיים כלים טכנולוגיים נוספים 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 מסר 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.

---

11 סעיף 5(א)(2)(א) לחוק הסמכת השב"כ מתיר להעביר את נתוני האיכון למשרד הבריאות לצורך חקירות אפידמיולוגיות: "[השירות מוסמך] להעביר למשרד הבריאות את פרטי המידע כמפורט להלן [...] לגבי החולה – נתוני מיקום בתקופה שחל עד 14 ימים לפני תאריך אבחונו כחולה ולפי ההנחיות המקצועיות של נציג משרד הבריאות".

12 ראו דיאגרמה בדו"ח מבקר המדינה בנושא התמודדות מדינת ישראל עם נגיף הקורונה, עמ' 162.

- 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.

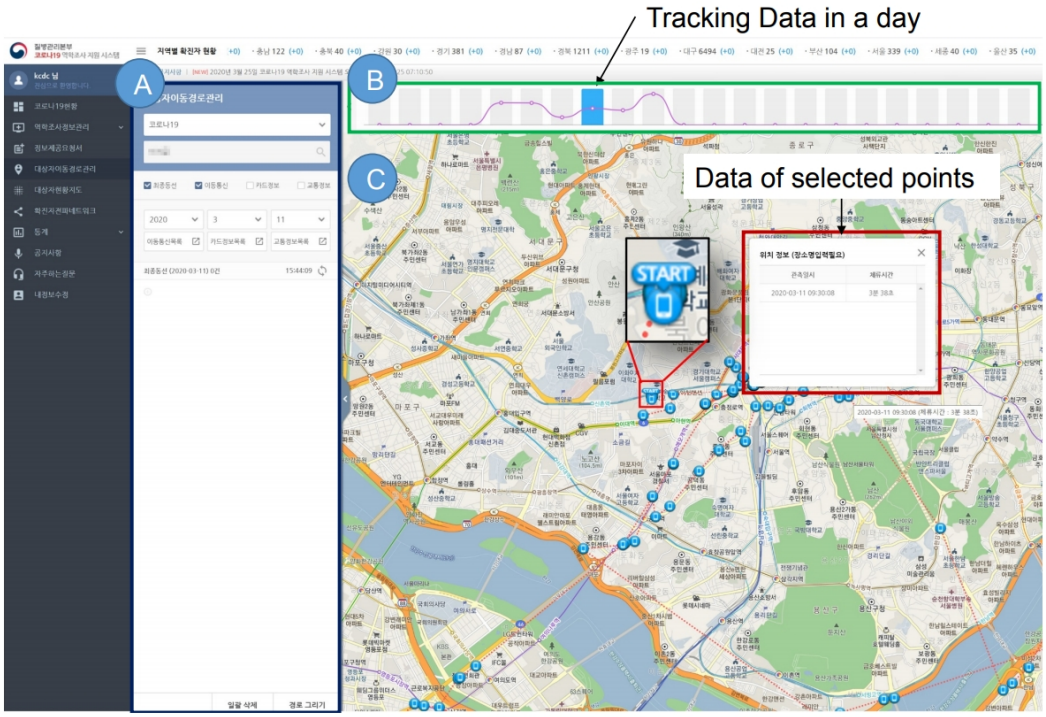
אלו כמובן דוגמאות בלבד. כל הפעלה של כלי טכנולוגי גורמת פגיעה בפרטיות, אך הפגיעה מידתית כי היא מצומצמת לצורך הישיר של חקירה נקודתית.

<u>חקירות אפידמיולוגיות במדינות אסיה – מה ניתן ללמוד מדרום קוריאה</u>

בדרום קוריאה ובסינגפור נעשה שימוש נרחב בכלים טכנולוגיים לייעול ולטיוב מערך החקירות האפידמיולוגיות. במדינות אלו נעשה שימוש בנתוני איכון סלולריים, במידע מאפליקציות שונות, במידע מכרטיסי אשראי, במידע משימוש בתחבורה ציבורית ועוד. כפי שמוסבר במסמך העמדה של התנועה לזכויות דיגיטליות מיום 14/07/2020, גם בישראל ניתן לעשות שימוש בכלים טכנולוגיים דומים **כל עוד נשמרים עקרונות ההסכמה והשקיפות**. כפי שהשימוש בנתוני האיכון כפוף להסכמת הנחקר להפקתם, כך גם השימוש בנתוני אשראי או במידע אודות נסיעות בתחבורה ציבורית, כפופים להסכמת הנחקר להפקתם.

איסוף נתונים בלבד לא מספיק. החכמה היא לעשות שימוש נכון בנתוני האיכון לצורך ייעול החקירה האפידמיולוגית. כדאי שנלמד כאן מהקוריאנים: דרום קוריאה פיתחה "מערכת תמיכה לחקירות אפידמיולוגיות" (EISS = Epidemic Investigation Support System), שתרמה תרומה מכרעת להתמודדות המוצלחת שלה עם נגיף הקורונה.

בדרום קוריאה, חקירה אפידמיולוגית מתחילה עם נתוני המיקום של הנחקר, שמתקבלים מחברת הסלולר. מנתונים אלו אפשר לבנות מפה של תנועות הנחקר במהלך הימים האחרונים. החוקר והנחקר עוברים יחדיו על הנקודות השונות במפה, ומאתרים מקומות בהם יש חשש להדבקה.



בתמונה מוצגת המערכת הקוריאנית. החלק המסומן (A) כולל את נתוני החקירה ואת פרטי הנחקר. החוקר יכול להוסיף נקודות עניין בהתאם לראיון עם הנחקר. (B) הוא ציר הזמן. כל מלבן אפור מסמן יום. ניתן לבחור להציג על המפה את נתוני איכון עבור כל יום מבוקש. בחלק (C) מופיעה מפה דינמית, עליה מוצגים נתוני האיכון של הנחקר והמסלול המשוער שהוא עבר בו באותו יום. כאשר לוחצים על נקודה מסומנת במפה, מוצגים נתונים אודות מועד האיכון ואורך השהות באותו אזור. החוקר יכול למלא פרטים אודות מעשיו של הנחקר באותו מקום ובאותו זמן. בהתאם לממצאים, החוקר יציין מגעים אפשריים שיש לבחון בבדיקה נוספת או באמצעים טכנולוגיים נוספים.

פיקוד העורף פיתח את מערכת "אבן יסוד". זו מערכת מידע לניהול חקירות אפידמיולוגיות, שהחליפה את המערכת המיושנת של משרד הבריאות. המערכת היא למעשה מערכת של טפסי חקירה חכמים. המערכת כוללת ממשק למאגרי הנתונים של משרד הפנים, וכך ניתן לאתר במהירות ובקלות אנשים שקיים חשש שהיו במגע קרוב עם חולה מאומת. עם זאת המערכת היא מערכת טקסטואלית בבסיסה. אין למערכת ממשק אינטואיטיבי להצגת נתוני המיקום של הנחקר. נתוני האיכון המתקבלים מהשב"כ משמשים כדי לוודא שהנחקר לא השמיט פרטים אודות המקומות בהם שהה. הנתונים לא משמשים חלק מתהליך התשאול מכיוון שאינם מתקבלים בהסכמת הנחקר ועקב מגבלות החוק.

סיכום

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.

ההחלטה להמשיך את השימוש באיכוני השב"כ במקום להפיק, בהסכמת הנחקר, נתוני איכון אזרחיים, מונעת שימוש יעיל בנתוני המיקום ופוגעת באופן ממשי ביעילות החקירות האפידמיולוגיות. ראוי שהוועדה תבקש ממשרד הבריאות הסברים מדוע לא נעשה שימוש באיכונים סלולריים על פי חוק נתוני תקשורת עבור חולים מאומתים הנושאים את זן האומיקורן או כל זן אחר.

נשמח לעמוד לרשותכם לכל צורך,

בכבוד רב ובברכה,

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

טל' 054-5260678 | zdevir@gmail.com