23 ביוני, 2020

לכבוד
ח"כ צבי האוזר, יו"ר ועדת החוץ והביטחון
חברי ועדת החוץ והביטחון
הצוות המשפטי של ועדת החוץ והביטחון

ג.א.נ.,

הנדון: **<u>חלופות אזרחיות להפעלת אמצעים טכנולוגיים ע"י השב"כ</u>**

מסמך זה נועד לסייע לדיון הוועדה בהערכת חלופות אזרחיות אל מול הפעלת כלי השב"כ כחלק מהמאבק בנגיף הקורונה.

<u>רקע</u>

במרץ 2020, החליטה הממשלה, באופן חריג וחסר תקדים בעולם הדמוקרטי, להורות לשב"כ לעשות שימוש באמצעים טכנולוגיים המיועדים ללוחמה בטרור, כדי לסייע באיתור חשיפות של אזרחים לנשאי הנגיף ובקטיעת שרשרת ההדבקה.

שימוש באמצעים טכנולוגיים על ידי השב"כ, טומן בחובו פגיעה קשה ומתמשכת בפרטיות כל תושבי המדינה, שכן הוא מחייב מעקב מתמיד אחר האותות הסלולריים של מכשירי הטלפון שלהם, ואיגום המידע למאגר אחד עצום, ללא הסכמת הנעקבים. אולם, הסיפור הנרחב יותר של שימוש בכלי, כל כך חריג וקיצוני, הוא שינוי מאזן היחסים בין ממשל לאזרחים במשטר דמוקרטי.

לצד היעילות המיוחסת לכלי השב"כ בדיווחי משרד הבריאות,[1] עולות מהדיונים חולשות שיש לתת עליהן את הדעת (לדוגמה, עובדת היותו לא מדויק במקומות הומי אדם או בבניין רב קומות, מגבלותיו כאשר אנשים יוצאים לרחוב ללא טלפונים, המגבלות המובנות באיכון סלולרי בכלל ועוד). דרישת משרד הבריאות (שלא התקבלה) לבצע רישום של מיקום מבקרים בקניונים סגורים מעידה על החולשה המובנית של הכלי השב"כי. עקב כך, כלי מסוג זה יוצר לא מעט התראות שווא (False Positive) או מחסיר התראות אמת (False Negative).

וזהו לקח ראשון: **אין טכנולוגיה מושלמת. לכל טכנולוגיה לניטור נתיבי ההדבקה של חולי קורונה יש חסרונות לצד יתרונות. גם לכלי השב"כ. אין לטשטש זאת.**

<u>נחיצות השימוש במערכת השב"כ</u>

כל כלי שאמור לאתר שרשראות הדבקה יהיה יעיל במידה זו או אחרת, ויתרום למציאת עוד חולים. בחינת החלופות האזרחיות לכלי השב"כ אינה מערבת אך ורק שאלות של יעילות טכנולוגית. היא מצריכה דיון בנחיצות של הפעלת מערכת שכזו, כלומר לבדוק מה סדר הגודל של הבעיה, מה היתרונות והחסרונות של הפתרון המוצע בטווח הקצר והארוך, ואת היתרונות החסרונות הללו יש להשוות בהקשר לחלופות השונות.

מזווית הראיה הזו, השאלה אינה מתמצית בהשוואת מספרים (כמה איתרה טכנולוגיה לעומת טכנולוגיה אחרת; כמה איתרה טכנולוגיה לעומת תחקיר אנושי וכו'). היא מערבת מכלול שאלות. לדוגמה -

- עד כמה הכלי של השב"כ **יחסית לחלופות אזרחיות** אחרות מאתר יותר מגע עם חולים?
- מה מידת הדיוק באיכון של כלי השב"כ לעומת הטכנולוגיות האזרחיות החלופיות והחקירות האפידמיולוגיות?

1 בדו"ח מס' 9 של משרד הבריאות מצוין כי כלי השב"כ איתר 4070 חולים (23.9%) באופן בלעדי.

- איזו פגיעה ערכית קיימת בשימוש בכלי השב"כ לעומת כלים אזרחיים (להסרת ספק: בתצורות מסוימות עלולה להיות פגיעה ערכית גם מחלופות אזרחיות; לדוגמה אם הן כרוכות בהעברת מידע אישי רגיש מהמדינה למגזר הפרטי)?
- מה המשקל שיש לתת לפגיעה זו בהערכת יעילותן של החלופות?
- איזו משמעות חברתית נודעת להתחקות המדינה אחר כל אזרחיה - לדוגמה, בחינוכם (וליתר דיוק, אי-חינוכם) לאחריות ולערבות הדדית, לציות ולאמון גבוה במדינה - כל אלה רכיבים חיוניים במאבק במגפת הקורונה.

הדרישה לחלופות אזרחיות הגיעה מגורמים שונים (בג"ץ, ועדת חוץ וביטחון, השב"כ והציבור). כך למשל, בג"ץ דרש לקיים "עבודת מטה רצינית לאיתור חלופות ... **המאמץ לאיתורה של חלופה יעילה אחרת חייב להימשך ללא לאות**". בית המשפט גם הצביע על הדרך הנכונה – "**במיוחד יש לשקול אם ניתן להשיג את התועלות החשובות הנדרשות באמצעות שימוש במנגנון וולונטרי ושקוף למשתמש**" (בג"ץ בן מאיר ואח' נ' ראש הממשלה ואח', 26.4.2020).

גם ועדת המשנה לשירותים חשאיים בראשות היו"ר דאז, ח"כ (כיום שר החוץ) גבי אשכנזי דרשה בדיון מיום 30.3.2020 לקבל עד 30.4.2020 עבודת מטה רצינית לבחינת החלופות האזרחיות לכלי השב"כ. אם נערכה עבודה כזו, היא לא פורסמה עד כה ברבים. אם לא פורסמה, אי אפשר להעריך את רצינותה אלא אם תונח מבעוד מועד על שולחן הוועדה ותובא לביקורת ציבורית.

כיום, קיימות טכנולוגיות אזרחיות המאפשרות ליצור חלופות להסתייעות בשב"כ. שלא כמו אמצעי המעקב של השב"כ, טכנולוגיות כאלה מאפשרות זיהוי מהיר ומדויק יותר של מגעים, תוך שמירה טובה על פרטיות. מדינות שונות עושות שימוש בטכנולוגיות שכאלה. אין לנו ספק שעל המדינה להעמיד את מיטב המאמצים, ההון האנושי והיכולות על מנת להכשיר חלופה שכזו. **תעשיית ההי-טק המפוארת של ישראל התמודדה בהצלחה עם אתגרים מורכבים לאין ערוך מזה.**

<u>מעקב מיקום מול זיהוי מגעים</u>

בבסיס המערכת של שב"כ נמצא, כאמור, מעקב אחרי מיקומם של כל התושבים כל הזמן. הדבר נגזר מייעודה המקורי של המערכת לסכל פעולות טרור, באמצעות איתור מהיר של מבוקשים. אבל זיהוי חשיפות לווירוס אינו מצריך לדעת את מיקומו של אדם, אלא רק לזהות אם אדם בא במגע קרוב וממושך מספיק עם נשא מאומת. לכן טכנולוגיה המזהה קרבה בין אנשים, בלא להתחקות אחר מיקומם, מספקת מענה איכותי – לעיתים קרובות אף יותר מטכנולוגיה המבוססת על איכון מיקום – לצורך לזהות במהירות מגעים חבי-בידוד. והיא עושה כן אגב שמירה טובה על הפרטיות.

ההתפתחות בעולם בהתמודדות עם הקורונה פונה לכיוון של זיהוי מגעים (contact tracing) ולא מעקב מיקום. זיהוי קירבה מבוסס על שימוש בטכנולוגיית Bluetooth, המובנית כיום בכל טלפון סלולרי מודרני.

<u>כיצד פועל זיהוי חשיפה באמצעות Bluetooth</u>

עקרון הפעולה של מערכות זיהוי חשיפה מבוססות Bluetooth הוא פשוט: המשתמש מתקין אפליקציה ייעודית. בכל מכשיר סלולרי שבו היא הותקנה נוצר מזהה ייחודי, כזה שאינו ידוע לאיש, ובכלל זה אינו ידוע למשתמש עצמו, למדינה או ליצרן המכשיר. המזהה הייחודי אף משתנה בצורה תכופה. המכשיר הסלולרי מאתר בכל זמן מכשירים אחרים שנמצאים בקרבתו ומיישמים את אותה טכנולוגיה. המספר המזהה הייחודי של כל מכשיר שנמצא בסמיכות אליו - במרחק פיזי ולמשך זמן מוגדרים מראש - נשמר באופן מקומי על גבי כל אחד ממכשירי הטלפון הניידים המשתתפים במפגש. כך נאספים המזהים המוצפנים של כל המכשירים בתוך המכשיר, ורק בו. בשלב זה, המידע שנאסף הוא חסר פשר ולא ניתן לעשות בו כל שימוש, לא כל שכן לא לזהות את בני האדם שנפגשו זה עם זה.

מרגע שאדם כלשהו אובחן כנשא של הנגיף, מסומן המזהה הייחודי של הטלפון הסלולרי שלו כ"מזהה של חולה". מידע זה מופץ אוטומטית לכל הטלפונים האחרים. כעת, יכול היישום המופעל אצל כל שאר בעלי

הטלפונים שבהם הותקן, לראות אם (ומתי) נחשף בעליו למישהו שנושא את הנגיף - ואם אכן קרה הדבר, להתריע בפניו שעליו להיכנס לבידוד.

השימוש ב-Bluetooth, בשילוב עם היכולות המיוחדות ש-Google ו-Apple יוסיפו במערכות ההפעלה של הטלפונים, גורם לכך שפעולתו תהיה יעילה, ולפיכך תמעט בצריכת אנרגיה מסוללת המכשיר. כיוון שזמן הסוללה הוא אחת הסיבות העיקריות שגורמות למשתמשים להמשיך ולהפעיל את היישומון, יכולות אלו הן חשובות ביותר. אגירת המידע על מכשיר הקצה, תוך ביצוע ההצלבות על גבי המכשיר עצמו, מפחיתה באופן דרמטי את הפגיעה בפרטיות (בהבדל משליחת מידע רגיש ומזוהה על מיקום אל רשות מרכזית אחת המצליבה כך בין מיקומו של חולה מאובחן לבין מי שניקרו בדרכו או נפגשו איתו). אפליקציות שכבר מבוססות על טכנולוגיה זו הושקו בשוויץ, צרפת, איטליה ועוד.

<u>השוואה</u>

זיהוי חשיפה (Bluetooth)	**איכון (סלולרי, או מבוסס GPS וכד')**
זיהוי חשיפה לנשא מאומת, באמצעות זיהוי קירבה	מעקב אחר מיקומו של אדם במרחב הציבורי, הצלבת מיקומים לזיהוי חשיפה
מיושם בעולם באופן וולונטרי. אינו דורש איסוף מידע מתמיד בידי רשות מרכזית.	כופה. מעקב אחר כל התושבים כל הזמן
דיוק גבוה ביותר בזיהוי קירבה, גם באזורים מקורים ובבניינים, ובאיזורים הומי אדם	דיוק נמוך. אין אבחנה בין קומות או באזורים מקורים כדוגמת קניונים
פגיעה קטנה יותר בפרטיות	בכלי של שב"כ, פגיעה קשה בפרטיות
סיכון מזערי לשימוש במידע שלא למטרה שלשמה נאסף (לדוגמה: ניטור הפגנות)	איום קרוב ומיידי של Function Creep
בלתי תלוי בגורמים חיצוניים	תלות בזמינות הרשת הסלולרית, החשופה לתקלות, התקפות סייבר וכיסוי לא מספק
התוצאה: עידוד השימוש באמצעים שהם וולונטריים	עידוד לעקיפת הניטור באמצעות הימנעות מנשיאת טלפון סלולרי או כיבויו לפרקים

<u>יתרונות מערכת מבוזרת מבוססת Bluetooth</u>

ראשית, מערכת מבוססת Bluetooth מזהה קירבה, ולא מיקומים. לכן, היא עובדת בצורה טובה בהרבה ברכבות מהירות, אוטובוסים, ומבנים גדולים כגון קניונים או רבי קומות. כדי שמערכת לזיהוי התפשטות הנגיף תצליח היא חייבת לזכות באמון הציבור. מערכות מרכזיות עם איכון סלולרי מזהות מגעים בדיוק של כמה עשרות או מאות מטרים ולכן גורמות להתראות שווא רבות. התראות שווא מצידן גורמות להתעלמות מסוכנת. על-פי נתוני משרד הבריאות בדיווחיו לוועדה, כ- 12.5% ממקבלי ההתראות הסלולריות בעקבות נתוני השב"כ שוחררו מחובת הבידוד לאחר שהשיגו על כך. זהו שיעור גבוה מאד של התראות שווא.

שנית, כדי שמערכת תזכה לאמון היא צריכה לשכנע את משתמשיה שהיא מגנה על פרטיותם. נתיב התנועה של אדם כורך בחובו פרטים טריוויאלים (הלכתי לעבודה או לספר) אבל גם פרטים מאד רגישים (הלכתי לפסיכולוג או למי שאני נמצא איתו בקשר אינטימי). מכאן שיש העדפה ברורה למערכת שאינה מנטרת מיקום אלא אך ורק קירבה לחולים. מערכת מבוססת Bluetooth ניתנת לעיצוב כך שהמידע על מי שנמצאו בקירבה לבעל המכשיר הסלולרי נשמר במכשיר עצמו ואינו יוצא ממנו הלאה אלא בפעולה רצונית של המשתמש. בכך נמנעת הסכנה של שימוש לרעה במאגר מידע ריכוזי. כמובן שאין זה מונע את קבלת הנתונים בידי המדינה אם וכאשר מתברר שמשתמש פלוני הוא חולה, שאז היא יכולה להתריע בפני מי שנמצאו איתו במגע למשך זמן מספיק ובקירבה מסוכנת שעליהם להיכנס לבידוד.

שלישית, קבוצה זו ממליצה על הפעלה וולונטרית של אפליקציה מבוססת Bluetooth, אולם הוולונטריות אינה מובנית בתוך הטכנולוגיה אלא היא תולדה של החלטה של הרשויות המסרבות, בצדק לדעתנו, לחייב התקנה של האפליקציה.

ולבסוף, בנוסף על החשש ממעקב תמידי של המדינה, עלולים להביא לכך שהציבור לא ישתמש בטלפונים דווקא במקומות מועדים להידבקות, כגון סופרמרקטים או הפגנות.

<u>סטנדרט עולמי נוצר</u>

על-פי דיווחי משרד הבריאות עצמו, נכון לסוף חודש מאי, 39 מדינות מבססות את הצורך לאיתור מהיר של חשיפה על אפליקציות המותקנות על ידי המשתמשים במכשירי טלפון חכמים. 22 מתוכן – ובהן בריטניה, איטליה גרמניה, שוויץ, צרפת. פולין, סינגפור ואוסטרליה – מתבססות על טכנולוגיית Bluetooth מבוזרת (במצב שנקרא BLE - Bluetooth Low Energy, שייחודו בצריכת אנרגיה נמוכה), בצורה בה המידע על מגעים נשמר בנייד ולא במאגר מרכזי. גישה טכנולוגית זו מקודמת בשיתוף פעולה חד-פעמי בידי החברות Google ו-Apple, כך שהיא תיתמך גם במכשירי טלפון ניידים מבוססי אנדרואיד וגם ב-iPhone. מלבד שיתוף הפעולה של החברות, הפרויקט הפאן-אירופי DP3T יצר מערכת מבוזרת לזיהוי מגעים מבוססת Bluetooth אשר עובדת בכמה מדינות. מערכת שכזו מאפשרת זיהוי מגעים של אנשים ממדינות שונות. יש לציין כי מספר מדינות מבססות את האפליקציות שלהן על תוצרי הפרויקט (דוגמת שוויץ).

<u>שילוב זיהוי מגעים מבוסס Bluetooth ביישום "המגן"</u>

בישראל, השיק משרד הבריאות את אפליקציית "המגן". זהו אמצעי שתוכנן ונוצר בהקפדה תוך הגנה על פרטיות ואבטחה, בין השאר מפני שקוד המקור שלו שוחרר לציבור וכן מפני שהוא שומר את כל נתוני המיקום במכשיר המקומי של המשתמש. אלא שמשרד הבריאות לא קידם את השימוש ב"המגן" באופן מספק, ולמעשה זנח אותו מול מקסם השב"כ. בסיס ההתקנות של "המגן" אינו מספק (כ-870,000 משתמשים לפי נתוני משרד הבריאות שנמסרו לוועדת המשנה לשירותים חשאיים בכנסת ביום 26.5.2020 לעומת מצב רצוי של 4 מיליון). מכיוון שהפצת "המגן" לא לוותה בקמפיין משמעותי, פוטנציאל ההתקנה של היישומון רחוק ממיצוי. כיום, מתבסס גם "המגן" על איכון (מעקב מיקום), אם כי באופן אחר מזה של כלי השב"כ (בעיקר, איכון באמצעות GPS) **וללא שיתוף מידע פרטי אלא אך ורק ביוזמת המשתמש**. משרד הבריאות מסר לוועדה באותו דיון כי ב-7.6.2020 יתחיל בהרצת גירסה של "המגן" המשמשת גם זיהוי מגעים באמצעות Bluetooth (מסמכי תכן וקוד קריפטוגרפי כבר שוחררו). כעת מדבר המשרד על כך שהדבר יקרה "בשבועות הקרובים."[2]

2 אנחנו מודעים לכך שישנם קשיים טכניים בשילוב Bluetooth באפליקציית המגן, מאחר וחברות אפל וגוגל אינן מאפשרות לאפליקציות ניטור קירבה להשתמש <u>גם</u> בנתוני Bluetooth <u>וגם</u> בנתוני מיקום. לדעתנו, על משרד הבריאות לפעול מול אפל וגוגל ביחד עם רשויות בריאות אחרות המתמודדות עם אתגר בזה, או להשתמש רק בנתוני Bluetooth.

<u>איך יכולה ועדת החוץ והביטחון לפעול?</u>

- להורות לבחון את המידתיות של כלי השב״כ אל מול חלופות שונות. מידתיות תחייב למצוא מדדים המשקללים את העלויות והיתרונות של כל פתרון.
- להקים ועדה ייעודית בכנסת שתפקידה לקדם, להוביל ולבסוף להביא להפעלת חלופה אזרחית לזו של השב״כ.
- לתבוע קבלת עבודת מטה מסודרת, מגובה ומעמיקה כפי שדרשה הוועדה עוד בשלהי חודש מרץ.
- לדרוש כי בבחינת החלופות יעורבו גורמים מהציבור שהם בעלי מומחיות בתחומי טכנולוגיה, חברה, רפואה ציבורית, כלכלה התנהגותית, משפט, אתיקה, וכל דיסציפלינה מקצועית אחרת שהוועדה תמצא לנכון. יש לשים לב ששילובם של אלה יגביר את האמון בהמלצות.
- לקבוע לכל אלה לוחות זמנים קצרים ביותר, בהתחשב בדחיפות הזמנים הללו.
- ליזום דיונים מקצועיים, בהשתתפות מומחים מקצועיים מתחומי הטכנולוגיה, החברה, רפואה ציבורית, כלכלה התנהגותית, ומשפט לליבון היתרונות והחסרונות של פתרונות וחלופות מגני-פרטיות למעקב השב״כ.
- להורות כי פיתוח ״המגן״ ושילוב טכנולוגיות מתקדמות בו יימשכו בקצב המקובל לפיתוח אפליקציות במגזר האזרחי, תוך עידוד הציבור לעשות בה שימוש, ולדרוש מהאוצר להקצות בלא דיחוי כל תקציב שנדרש לפיתוח ״המגן״, לתפעולה ולעידוד השימוש בה .

אנו עומדים לרשות הוועדה בכל שאלה בנושא,

בברכה

פרופ׳ קרין נהון - המרכז הבינתחומי הרצליה ונשיאת איגוד האינטרנט הישראלי
עו״ד חיים רביה - פרל כהן צדק לצר ברץ
פרופ׳ מיכאל בירנהק, הפקולטה למשפטים, אוניברסיטת תל אביב
פרופ׳ בני פנקס, אוניברסיטת בר-אילן - המחלקה למדעי המחשב, וראש מרכז הסייבר
פרופ׳ אור דונקלמן, אוניברסיטת חיפה - החוג למדעי המחשב ומרכז חקר הסייבר, משפט ומדיניות
ד״ר ערן טוך, הפקולטה ל׳הנדסה, אוניברסיטת תל אביב
פרופ׳ ניבה אלקין-קורן, הפקולטה למשפטים אוניברסיטת חיפה
ד״ר דלית קן-דרור פלדמן, הקליניקה למשפט, טכנולוגיה וסייבר, הפקולטה למשפטים, אוניברסיטת חיפה
עו״ד יורם הכהן, מנכ״ל איגוד האינטרנט הישראלי (ע״ר), לשעבר ראש הרשות למשפט, טכנולוגיה ומידע (היום - הרשות להגנת הפרטיות)
עו״ד דנה יפה, הקליניקה לזכויות אדם במרחב הסייבר, האוניברסיטה העברית בירושלים.
עו״ד רבקי דב״ש, יועצת בתחום המשפט והטכנולוגיה, לשעבר ראש הרשות להגנת הפרטיות בפועל
ד״ר ענת בן-דוד, המחלקה לסוציולוגיה, למדע המדינה ולתקשורת, האוניברסיטה הפתוחה.