



סקירה

הצורך במעבר למעקב וולנטרי

21 במאי 2020 | מאת: ד"ר תהילה שוורץ אלטשולר, עו"ד רחל ארידור הרשקוביץ, *ד"ר ערן טוך

אל מול המחיר של שימוש בשירותי השב"כ במעקב אחר אזרחים הכרוך בפגיעה נרחבת בזכות לפרטיות קיימות שתי חלופות מרכזיות: איסוף מידע מחברות הסלולר ועיבודו על ידי משרד הבריאות או שימוש וולנטרי באפליקציות לאיתור האזרחים המחויבים בבידוד. לפניכם מסמך המפרט את החלופות למעקב אחר אזרחים במסגרת המאבק בנגיף הקורונה



שומרים על הפרטיות של כולנו חלופות למעקבי השב"כ



ניווט מהיר בדף

תקציר מנהלים

מטרת מסמך זה היא להציג את החלופות השונות הקיימות לשימוש בשב"כ לצורך התמודדות עם התפשטות נגיף הקורונה באמצעות איתור מגעים דיגיטלי.

הניתוח שלנו כולל מספר היבטים מרכזיים:
יש חלופות לשימוש בשב"כ:

גם אם בימים הראשונים והמבולבלים של ההתמודדות עם המגיפה אפשר היה להבין את הטיעון של מקבלי ההחלטות לפיו אין בנמצא חלופות להפעלת השב"כ לצורך מעקב אחר אזרחי ישראל, הרי שכיום קיימים שני סוגי חלופות: הסוג האחד הוא שימוש במידע סלולרי ועיבודו על גבי שרתים של משרד הבריאות באמצעות מומחיות מתוך המשרד או באמצעות חברות פרטיות, והסוג השני הוא התקנת יישומון מעקב מגעים תוך מתן פתרון לפלח האוכלוסיה שאין בידיו טלפון חכם.

אין נחיצות בשימוש בשב"כ:

מצב ההדבקה בישראל הוא נמוך לאין שיעור מן התחזיות הראשוניות, וכולנו מברכים על כך. עם זאת, יש לפסול את הטיעון האומר שדווקא בשל כך יש להמשיך את השימוש באמצעי מעקב פולשניים. משך הזמן שעבר אמור היה לשמש את הרשויות להיערכות עתידית, הן בהיבטים של בדיקות; כוח אדם בבתי חולים; ציוד רפואי וגם בהיבט של חלופות למעקבים פולשניים. הטיעון לפיו בתחילת המשבר נדרשנו לשימוש ב"כלי" של השב"כ מחוסר ברירה ועתה עם היציאה מהמשבר, שחרור הסגר וחזרה הדרגתית לשגרה אנו זקוקים לשימוש ב"כלי" של השב"כ עוד יותר, הוא טיעון מטעה ומוטעה מיסודו. חריגותו של ה"כלי" של השב"כ מחייבת שימוש בו אך ורק בעתות מצוקה וחירום ואין להפוך אותו לכלי נוסף בארגז הכלים של משרד הבריאות שניתן לעשות בו שימוש לטווח ארוך ובעת שגרה, אף אם מדובר ב"שגרת קורונה". ה"כלי" שאותו מפעיל השב"כ אינו נותן מענה בחלק מן המרחבים החשובים למעקב מגעים, למשל בקניונים ובבתי דירות גבוהים, לעומת מעקב מגעים המבוסס על טכנולוגיית בלוטות' שבה יכולים לעשות שימוש ביישומונים. גם בהיבטי תוצאה אחרים הפער בין יישומונים לבין השב"כ אינו גדול באופן המצדיק את החסרונות העצומים לדמוקרטיה ולחברה בישראל הטמונים בהפעלת השב"כ. **תכלית מעקב אישי ומזוהה היא אך ורק איתור מגעים:**

גם אם יש צורך במעקב פרטני, הוא חייב להיות תחום אך ורק לצורך יידוע מי שנחשף לחולה קורונה מאומת שעליו להיכנס לבידוד. ניתוח כוללני לצרכי מדיניות (כגון יצירת מפות חום על מוקדי התפרצות, הצגה גרפית של נתונים, מערכות חיזוי והיערכות) צריך להסתמך על נתונים אגרגטיביים בלבד (או לפחות על נתונים מותממים). ניתוח כוללני לצרכי מדיניות המבוסס על מידע אישי מזהה הוא פעולה בלתי מידתית.

פגיעה בפרטיות צריכה להיות בהסכמת נושאי המידע ולא פגיעה כפויה:

העובדה שמדובר במשבר אזרחי, עומק הפגיעה בזכויות אדם, "מרחב הנשימה" שניתן כרגע בשל דעיכת ההתפרצות והצורך לבסס אמון עם האזרחים – מחייבים זאת. הבחירה בכל המדינות הדמוקרטיות עד כה היא ביישומונים (אפליקציות) ייעודיים לאיתור מגעים שהאזרחים מורידים אותם לטלפונים שלהם באופן וולונטרי.

מידע ממעקב מגעים צריך להיות תחום בידי רשויות בריאות ואין לערב רשויות שיש להן סמכויות אכיפה וחקירה:

קיימים הבדלים מהותיים בין גופים אוספי מידע אזרחיים לבין גופים אוספי מידע שיש להם גם סמכויות חקירה או אכיפה. הבדלים אלה נוגעים לתפיסת ההפעלה, גדר הסמכות וגדרי האחריות. יש לשאוף לכך שאיסוף המידע לא יהיה על ידי גופים מהסוג השני. גם במדינות שבהן נעשה איסוף מידע מיקום באופן מרכזי מחברות הסלולר - אף מדינה דמוקרטית לא הפעילה את השירות החשאי שלה לשם כך.¹

מה אנחנו מציעים?

על בסיס ניתוח החלופות וניסיון של מדינות אחרות אנו ממליצים על החלופה שיש לאמץ בישראל: **שידרוג יישומון "המגן" והפיכתו למבוסס בלוטות'; עידוד משמעותי להתקנת "המגן" ומתן פתרון ייעודי לבעלי טלפונים כשרים.**

א. יישומון המגן כיום

היישומון הושק על ידי משרד הבריאות בסוף מרץ 2020 כיישומון ייעודי לאיתור מגעים, שפותח במערכת של קוד פתוח בליווי מומחי פרטיות ואבטחה. התקנתו היא וולונטרית והוא נשען על איסוף נתוני איכון סלולרי של המשתמש והשוואתם לנתוני המיקום של חולה קורונה מאומתים כפי שמעודכנים בשרתי משרד הבריאות. משתמשי היישומון מקבלים התראה על שהיה בקרב חולה מאומת ויכולים לבדוק את אמינות המידע עבורם ולדווח על כניסה לבידוד או על שגיאה בנתונים. נתוני האיכון נשמרים בזיכרון הפנימי של מכשיר הסלולר האישי ומועברים לשרת משרד הבריאות בהסכמת המשתמש במידה שאובחן כחולה בקורונה (גישה ריכוזית). סביב היישומון לא הושק קמפיין ציבורי ובנוסף הוא סבל משגיאות רבות הנובעות הן מחוסר הדיוק באיכון סלולרי והן מטעויות אנוש בהזנת הנתונים בשרתי משרד הבריאות.² אלה הובילו לאחוזי התקנה נמוכים וכן להסרת היישומון לאחר שהותקן.³ ב-19 למאי 2020 פרסם משרד הבריאות מכרז לשידרוג יישומון המגן.⁴

ב. הצעה לפעולה: יישומון המגן משודרג

היישומון יעשה שימוש באותות בלוטות' ויפעל בהתאם ל"שיטה הריכוזית"⁵

הטכנולוגיה למעקב המגעים ביישומון תהיה מבוססת אותות BLE אשר אינם מצביעים על מיקומו או תנועותיו של המשתמש, נשמרים רק על מכשירו האישי ואינם נשמרים במקביל על ידי חברות הסלולר. בנוסף, היא תהיה מדויקת יותר מאשר נתוני איכון סלולריים, ביחוד בממד הגובה (ולכן תאפשר קירוב טוב יותר גם מרחב עירוני צפוף, במבני קומות ובקניונים).

היישומון יקבל היישומון מפתח הצפנה להפקת קודי זיהוי אקראיים וישדר אותם בפערי זמן של כחמש דקות באמצעות אותות BLE שהם אותות בעוצמה נמוכה יחסית וכך מובטח שלא יקלטו במרחקים פיזיים גדולים.⁶ מאחר ומדובר בקודי זיהוי אקראיים המופקים על ידי מפתח הצפנה הנמצא על גבי מכשיר הטלפון עצמו, שני אותות שנשלחו מהמכשיר של משתמש מסוים לא יראו אותו הדבר ולא יוכלו לסמן בעתיד כי נוצרו באותו המכשיר.⁷

כל מכשיר טלפון שעליו מותקן היישומון יקלוט וישמור אצלו "לוג אותות" של כל קודי הזיהוי המשודרים בסביבתו ממכשירים אחרים, בצירוף חותם זמן ועוצמת אות ה-Bluetooth שנקלטה, כדי להעריך את המרחק הפיזי בין המכשירים. הקביעה האם משתמש נחשף לחולה קורונה מאומת תיעשה על ידי השוואת קודי הזיהוי השמורים על מכשירו האישי עם אלו שנשמרו על מכשיר הסלולר של החולה.

"לוג האותות" שנשמר על גבי מכשיר הטלפון של מי שנמצא חולה קורונה, יועברו בהסכמת המשתמש, לשרת מרכזי שבמשרד הבריאות שבו יהיו המפתחות לפיענוח ההצפנה של המידע. משרד הבריאות יוכל לזהות את המשתמשים שנמצאו בסמיכות פיזית לחולה ויודיע להם להיכנס לבידוד. משרד הבריאות לא ידע בהכרח היכן היה המפגש בין הטלפונים אלא את עצם העובדה שמפגש כזה התרחש.⁸

יעד ההתקנה של היישומון – כארבעה וחצי מיליון משתמשים,⁹ וזאת בהסתמך על המחקר המשמעותי ביותר שנערך בעניין זה, באוניברסיטת אוקספורד, ואשר הצביע על הצורך שלפחות 60% מהציבור יתקין את היישומון כדי להבטיח את יעילותו.

הטמעת ההתקנה של היישומון:

1. עידוד "רך" להתקנת יישומונים:

יש להשקיע מאמצים פרסומיים ניכרים לעידוד הציבור להתקנת יישומונים, דוגמת דרכי פעולתה של ממשלת אוסטרליה בהשקת קמפיין עידוד התקנת היישומון COVIDSafe¹⁰ שהובילו לכך שבתוך עשרה ימים הותקן היישומון על ידי חמישה מיליון משתמשים;¹¹ ודוגמת ממשלת בריטניה העומדת להפיץ באמצע מאי יישומון (NHS CV19), ופועלת כבר עכשיו במאמצי הסברה מקיפים המבהירים כי התקנת היישומון היא שתאפשר לשמור ולהגן על המשתמשים ומשפחותיהם, תמנע את הצפת מערכת הבריאות וקריסתה ותהיה אמצעי מרכזי בהשבת המדינה והכלכלה לשגרה ולתפקוד מלא.¹²

יש להפסיק לאלתר את השימוש ב"כלי" של השב"כ משום שכל עוד הציבור חושב שממילא התקנת היישומון הינה למראית עין כיוון שמשרד הבריאות מסתמך על ה"כלי" של השב"כ, לא ניתן יהיה לגייס אמון להתקנה בהיקפים נרחבים של היישומון.¹³

חלק מהמאמץ הפרסומי צריך להיות מבוסס על העצמת המשתמשים: נדרש הסבר לגבי תכלית השימוש ביישומון וההקשר המוסרי של סיוע להצלת הזולת; הסבר לגבי אופן פעולת היישומון ואמצעי הגנת הפרטיות שהוטמעו בו. יש לבחור צעדים מתחום הכלכלה ההתנהגותית על מנת להגביר את היקף הטמעת היישומון בקרב האוכלוסייה. למשל, מתן עדיפות בקבלת שירותים ציבוריים מסויימים (מענקי סיוע, הנפקת רישיונות ותעודות שונות) או מתן תגמול חומרי (שוברי קנייה או הנחה) למי שהתקין את היישומון. יש להתאים את הקמפיין הפרסומי לצרכים שונים של אוכלוסיות שונות, וללוות אותו במחקר שיוכל לבחון את הצלחת הקמפיין ואת היקף התקנת היישומון. במקרה של "שגרת קורונה" ארוכת ימים, אפשר לשקול אימוץ מודל opt out במסגרתו היישומון יותקן מראש בכל מכשירי הסלולר ובידי המשתמשים תהיה האפשרות להסירו אם רצונם בכך. בבחינת ההיבטים האתיים בשימוש ביישומון איתור מגעים ואיזון למול צרכי בריאות הציבור, יש שהציעו את מודל ה opt out כחלופה שיש לבחור מלכתחילה.¹⁴

2. עידוד "אינטנסיבי" להתקנת יישומונים:

ניתן לחייב את התקנת היישומון באזורים ספציפיים בהם נרשמת התפרצות במספר הנדבקים בנגיף.¹⁵ התניית השימוש בתחבורה ציבורית בהתקנת היישומון. הטלת חובה על בעלי חנויות לוודא שהלקוחות המגיעים לחנות התקינו את היישומון. לתפיסתנו, שיטה זו עדיפה בהרבה על פני חובת הזדהות בכניסה לחנויות ולקניונים שהוצעה במקומות שונים.

הטלת חובה על מעסיקים שונים במשק לוודא שעובדים התקינו את היישומון כתנאי לחזרה לעבודה: עובדים חיוניים; עובדי השירות הציבורי; חברות גדולות. שיטה זו תאפשר להימנע ממצב שבו מעסיקים אוספים מידע בלתי נדרש על עובדים, וגם ממצב שבו מעסיקים גדולים יחליטו באופן עצמאי לפתח יישומונים משלהם ולחייב עובדים להתקין אותם.

3. כרטיס חכם כפתרון לאוכלוסיות שאין ברשותן טלפון חכם:

אין ספק שחכם בפני הטמעת השימוש ביישומון נעוץ בעובדה שלא כל האוכלוסייה מחזיקה ברשותה מכשיר סלולרי חכם המאפשר את התקנת היישומון והפעלתו. אין מדובר בבעיה ייחודית למדינת ישראל,¹⁶ ונדגיש, כי לפי מחקר של מכון Pew האמריקני, נכון לאביב 2018 היתה ישראל במקום השני בעולם (אחרי המובילה – דרום קוריאה) מבחינת אחוז האוכלוסייה הבוגרת המחזיקה במכשיר טלפון חכם.¹⁷

הערכות הנוגעות לחברה החרדית בישראל אומדות את מספר מנויי "הקומה הכשרה", כלומר האנשים המחזיקים במכשירי טלפון כשרים שאינם מכשירים חכמים, בכ-500,000 משתמשים¹⁸ וגם מתוך קבוצה זו יש מספר רב של משתמשים המחזיקים במקביל בטלפון חכם או לחלופין משתמשים בטלפון חכם כשר אשר ניתן להתקין בו אפליקציות מבוססות מיקום¹⁹ או יישומונים על מערכת ההפעלה של המכשיר.

בין אם המספר המדויק של מספר המשתמשים במכשירי טלפון שאינם חכמים עומד על 500,000 או על 10% מכלל האוכלוסייה הבוגרת, יש לאפשר למי שאין ברשותו טלפון חכם, או שאינו רוצה להתקין את היישומון, להשתמש בכרטיס חכם בגודל של כרטיס אשראי, שיפעל בדומה ליישומון באמצעות אותות BLE ובשיטה ריכוזית, בדומה ל-COVIDCard שהוצע כאחד מהפתרונות לאיתור מגעים דיגטלי בניו זילנד.²⁰ המדובר בכרטיס המסוגל לשדר ולקלוט אותות BLE ועל בסיסם לחשב את הסמיכות הפיזית של המחזיק בו למחזיק כרטיס אחרים. ניתן לתכנת את הכרטיס כך שישדר ויקלוט אותות BLE המגעים לא רק מכרטיסים אחרים אלא גם ממכשירי טלפון חכם שעליהן מותקן יישומון המגן. הנתונים נשמרים למשך 30 יום על גבי הכרטיס עצמו. במידה שמחזיק בכרטיס נמצא חיובי לנגיף הקורונה יכול נציג משרד הבריאות, בהסכמת מחזיק הכרטיס או במסגרת חיובו לשתף פעולה עם חקירה אפידמיולוגית, להעביר את הנתונים לשרת משרד הבריאות לשם איתור מגעים.²¹

4. שדרוגים אפשריים נוספים ליישומון

התרעה למשתמש באמצעות צליל או הודעה במידה ואינו שומר על המרחק הדרוש בינו לבין משתמש אחר כאשר הוא נמצא במרחב הציבורי התרעה למשתמש על כך שנחשף במהלך תקופת זמן שתוגדר לפי מדדים אפידמיולוגיים (למשל, שבוע) לכמות של אנשים שתיקבע (למשל, למעלה מעשרים וחמישה אנשים שונים) ועידודו ללכת להיבדק האם הוא חולה בקורונה. זהו נדבך פעולה קריטי שיאפשר איתור מגעים של חולים א-סימפטומטיים שעשויים להיות "מדביקי על" (super spreaders). הוספת האפשרות להסיר מיקומים מהיסטוריית משלוח האותות לפני שהם נשלחים אל משרד הבריאות או "לכבות" את היישומון לזמן מסוים (snooze) אם המשתמש מגיע למקום שלא היה רוצה שידעו לגביו. זאת, בשל הרצון לעודד את אמון המשתמשים, ולהתמודד עם אוכלוסיות העוסקות בפעילות רגישה כגון עיתונאים.

הקדמה

מטרת מסמך זה היא להציג את החלופות השונות הקיימות לשימוש בשב"כ לצורך התמודדות עם התפשטות נגיף הקורונה באמצעות איתור מגעים.

בדיונים בוועדת החוץ והביטחון ובתשובת המדינה לבג"ץ בעתירה נגד הסמכת השב"כ לבצע מעקב מגעים,²² טענה המדינה²³ כי על אף הפגיעה חסרת התקדים בזכות לפרטיות של אזרחי ישראל ולמרות שאף אחת מן המדינות הדמוקרטיות בעולם איננה מפעילה את השירות החשאי שלה לצורך איתור מגעים בזמן הקורונה, אין חלופה לשימוש בשב"כ.

בפסק הדין מיום 26 באפריל, 2020 העלתה נשיאת בית המשפט העליון, כבוד השופטת אסתר חיות, את הצורך בהצגת חלופות לשימוש בשב"כ:

"אכן, המאמץ לאיתורה של חלופה יעילה אחרת חייב להימשך ללא לאות... על רשויות המדינה לשקול כל העת אם צרכי השעה עודם מצדיקים את האמצעים הקשים שבהם היא נוקטת... במסגרת חיפוש חלופה כאמור, יש ליתן את הדעת לפגמים המהותיים הקיימים במנגנון הנוכחי, ובמיוחד יש לשקול אם ניתן להשיג את התועלות החשובות הנדרשות באמצעות שימוש במנגנון וולנטרי ושקוף למשתמש".²⁴

בנוסף, הפניה המקורית אל השב"כ לצורך איסוף נתונים נעשתה, באופן מוצהר, לתכלית איתור חבי בידוד. ואולם, ביום 05.05.20 האריכה הממשלה את הסמכת השב"כ עד ליום 26.05.20²⁵ ובמקביל הודיעה כי תפעל לעיגון הסמכה זו בחוק ולהרחבת השימוש בו.²⁶ זאת, לפי הטענה, דווקא בשל הרצון לשחרר את הסגר והמגבלות ולאפשר חזרה חלקית לשגרה.²⁷ בדיון בוועדת החוץ והביטחון שנערך ביום 05.05.20 הוצג מסמך של המועצה לביטחון לאומי הקובע כי אין חלופות לשב"כ במעקב מגעים.

אכן, מן ההיבט של יעילות ואפקטיביות קיימים יתרונות לשימוש בשב"כ לצורך איתור מגעים – יכולת טכנולוגית זמינה לעיבוד המידע, דאטה זמין (אין צורך לעבור דרך חברות הסלולר בשל קיומו של "הכלי"), תרבות של שמירת סוד וקבוצה קטנה של אנשים שתיגע בחומר.

ואולם, המחירים של השימוש בשירות הביטחון מבחינה דמוקרטית כבדים גם הם: מעקב של המדינה אחר אזרחיה, שאינם חשודים בדבר, באמצעות השירות החשאי שלה; פגיעה חסרת תקדים, נרחבת, עמוקה ובהיעדר שקיפות בזכות לפרטיות תוך שימוש בכלים קיצוניים המיועדים לחימה בטרור; גוף שלטוני יודע היכן נמצאים כל אזרחי מדינת ישראל לפרקי זמן ארוכים; תפיסה של חשד מוקדם ואימוץ גישת "Command and Control" נגד אזרחים, המנוגדת לממצאים מתחום הכלכלה ההתנהגותית ולמחקרים מתחום האפידמיולוגיה; חוסר השקיפות האינהרנטי הכרוך בהפעלת השב"כ: אין לדעת מה בדיוק נאסף, כיצד והאם נמחק; הפיקוח המשפטי, הפרלמנטרי והציבורי המוגבל על השב"כ; והנזק שנגרם לשב"כ עצמו בחשיפת שיטות פעולה שלו ופגיעה באמון הציבור בו.

בנוסף, כפי שנפרט להלן, יש מספר סיבות להסיק כי השימוש בכלי של השב"כ אינו מדויק ומוביל לאחוז גבוה של שגיאות מסוג של False Positives ו-False Negatives. נתוני מיקום באמצעות הרשת הסלולרית פחות מדויקים לעומת אותו BLE (Bluetooth Low Energy) ו-WIFI. זאת בשל חוסר הדיוק הנובע מגודל התאים הסלולריים והעובדה שאיכון סלולרי מבוסס על אותות GPS, שעשויים להיות חלשים כתוצאה מתנאי מזג אוויר או הפרעות פיזיות. באיכון סלולרי רמת דיוק של עד 500 מטר ובמעקב BLE מדובר ברמת דיוק של 2 מטר. איכון סלולרי גם מתקשה בזיהוי קירבה בממד הגובה, ולכן אינו מדויק בבניינים רבי קומות.

המועצה לביטחון לאומי קבעה כי השב"כ מאתר רק שלושה מבין עשרה חולי קורונה חדשים ולכן המליצה על הקמת 500 צוותי חקירה אפידמיולוגית "מסורתיים", מה שכלל הידוע לנו לא נעשה עד כה.²⁸

מכל מקום, חסרונות אלה מובילים, בין השאר, לכך שהשב"כ צריך להשתמש בסוגי מידע פרטי נוספים כמו היסטוריית שיחות והודעות, מידע ממצלמות ועוד, וכן לכך שמקבלי החלטות בכירים בתוך משרד הבריאות דרשו במקביל סוגי מעקב נוספים, כגון מערכות מעקב שיהיו בשימוש בתוך קניונים.²⁹

מהו "איתור מגעים"

"איתור מגעים" (Contact Tracing Apps) מיועדים לאתר אנשים שהיו בסמיכות פיזית לחולה קורונה מאומת, וכך לאפשר בידוד מהיר של אנשים שיתכן שנדבקו בנגיף הקורונה. הסמיכות הפיזית לחולה קורונה מאומת נקבעת בהתאם למדדים אפידמיולוגיים של משך זמן החשיפה ומרחק מהחולה במשך תקופת הזמן במהלכה היה החולה מדבק.³⁰ כאשר ההיסק בנוגע לסמיכות הפיזית

המבוצע על ידי איסוף וניתוח של נתונים ממכשירי הסלולר של אזרחים, כגון נתוני מיקום, קשר ישיר בין משתמשים בעזרת אותות Bluetooth Low Energy (BLE) או טכנולוגיות אחרות (למשל, תקשורת אקוסטית) הוא נקרא "איתור מגעים דיגיטלי".

מאמרים מדעיים ודוחות יישומיים ממדינות שונות מלמדים כי לאיתור מגעים דיגיטלי פוטנציאל גבוה לתרום למאבק במגפת הקורונה, וכי הוא משמש כתוספת (או תחליף לעתים) לחקירה אפידמיולוגית מסורתית. בעיקר, הוא יעיל לבידוד אנשים שהיו בקרבת "מפצי על" (Super-Spreaders) המוגדרים כחולים מאומתים ששהו בקרבת אנשים רבים מאוד טרם אובחנו, במקומים ספציפיים דוגמת מרכולים, בתי כנסת ומקומות בילוי.³¹

שתי החלופות המרכזיות לאיתור מגעים המבוצע על ידי השב"כ הן:

איתור מגעים בכפיה אך על ידי גופים שלטוניים אזרחיים, באמצעות איסוף מידע מחברות הסלולר ועיבודו בעזרת פיתוח יכולות בתוך משרד הבריאות או באמצעות חברות פרטיות על גבי שרתים מאובטחים של המדינה, בשקיפות ותחת פיקוח שיפוטי, פרלמנטרי וציבורי.
מעקב מגעים וולנטרי באמצעות שימוש ביישומונים ייעודיים לאיתור מגעים המותקנים על ידי הציבור במכשירי הטלפון הסלולרי.
חלופה א': איסוף מידע מחברות הסלולר ועיבודו בעזרת חברות פרטיות
יתרונות:

שקיפות באשר ליכולת הטכנולוגית, לאיסוף המידע ולשימושים בו.
 מעקב אחר כלל האוכלוסייה המחזיקה בטלפון סלולרי ללא תלות בסוג מכשיר הטלפון או בהורדת יישומון.
 יכולות פיקוח על השימושים במידע ומחיקתו הן באמצעות תנאי התקשרות הן באמצעות שקיפות ציבורית ושיפוטית.
 משרד הבריאות איננו גוף חקירה ואכיפה ולכן אין חשש שמידע שגיע לידיו ישמש לצורך אכיפת חוק (אכיפת בידוד, פיזור התקהלויות בזמן אמת וכיו"ב).
 חסרונות:

נתוני מיקום באמצעות הרשת הסלולרית פחות מדויקים לעומת אותות BLE, אותות אקוסטיים, או מיקום בעזרת WiFi. זאת בשל חוסר הדיוק הנובע מגודל התאים הסלולריים והעובדה שנתוני מיקום מבוססי אותות GPS עשויים להיות חלשים כתוצאה מתנאי מזג אוויר או הפרעות פיזיות. באיכון סלולרי רמת דיוק של עד 500 מטר ובמעקב BLE מדובר ברמת דיוק של 2 מטר. איכון סלולרי גם מתקשה בזיהוי קירבה בממד הגובה, ולכן אינו מדויק ברבי קומות.
 אם חברה פרטית תקבל את המידע מחברות הסלולר ישירות אליה יתכן שימוש לרעה בדאטה; היעדר אבטחת מידע מספקת שעלולה להוביל לדליפת מידע; הפיכת המאגר למטרה לארגוני בין זרים.
 פתרונות:

שימוש במידע ממקורות שונים (איכון סלולרי ו-BLE).
 עיבוד המידע יתבצע רק בשרתים מאובטחים בניהול המדינה והמידע לא יועבר לשרתים של חברות פרטיות.
 ההסכמים עם חברות פרטיות יכללו איסורים על שימוש במידע (גם אם תהיה אפשרות של גישה למידע בזמן הטמעה או שדרוג של המערכת) לכל מטרה שחורגת מאיתור מגעים; הגבלת תחולת ההסכם ואיסוף ועיבוד מידע מכוחו לתקופה מוגבלת עם אפשרות להארכה כל עוד צו הבידוד בנוגע למצב החירום עקב מגיפת הקורונה עומד בעינו;³² חובת מחיקת מידע בנוגע לכל נושא מידע בתום תקופת הזמן הרלוונטית לאיתור מגעים.
 האחריות לאבטחת המידע ולמניעת שימוש לרעה בו תהיה על המדינה. יש להניח כי במשרד הבריאות כשלעצמו, אבטחת המידע נמוכה מזו של השב"כ. עם זאת, ככל שמדובר בתכנון לטווח ארוך, יהיה צורך ביצירת סטנדרט אבטחה ואמינות עובדים גבוה. חובת השקיפות החלות על המדינה מכוח חוק חופש המידע יוחלו גם על איסוף ועיבוד המידע המדובר.
תתי חלופות:
תת חלופה ראשונה: יצירת "משפך" לצורך העברה ישירה של דאטה מכל חברות הסלולר אל שרתים מאובטחים של משרד הבריאות.

אפשרות 1: עיבוד המידע על ידי משרד הבריאות עצמו - פיתוח מומחיות "In House" במשרד הבריאות כדי לעבד את המידע, לאתר מגעים וליידע את מי שנדרש להיכנס לבידוד.

אפשרות 2: האלגוריתמיקה והניתוח של המידע למטרת איתור מגעים יתבצעו על ידי חברות פרטיות אבל על גבי שרתי משרד הבריאות בלבד. מוצרים כאלה לאיתור מגעים מוצעים על ידי חברות כדוגמת NSO, Verint, Palantir.

חברת NSO מציעה את Fleming - מערכת שפותחה יחד עם מפא"ת, המסוגלת לספק מגוון שירותים שונים הכוללים איתור מגעים, יצירת מפות חום ומערכות חיזוי התפרצויות; זיהוי שרשרות הדבקה ומיקום ההדבקה על ידי מפצי על (למשל חנויות מזון, בתי כנסת, מקומות בילוי וכיו"ב) ויצירת ציון אישי לפוטנציאל הדבקה של אדם אם נחשף לחולים. המערכת המוצעת אינה עוסקת באיסוף המידע

ותופעל על מידע שיימצא על שרתים של משרד הבריאות בשילוב איכון סלולרי מרשתות הסלולר. מוצר זה הוצע למשרד הביטחון בישראל ולמדינות אירופאיות.³³

חברת Palantir משתפת פעולה עם חברת הסטארט-אפ הבריטית Faculty לשם מתן שירות ניתוח, עיבוד והצגת מידע עבור שירותי הבריאות הבריטיים (NHS). המידע איננו נאסף על ידי החברות אלא על ידי שירותי הבריאות עצמם וגופים אחרים עבורם נשמר על שרתי שירותי הבריאות הבריטיים. ההסכם בין NHS ופלטנר פורסם לציבור, וכן גם התחייבות של NHS למחוק את המידע מן השרתים בתום המשבר.³⁴

לתפיסתנו, במיוחד אם מדובר בצפי ארוך זמן של התמודדות עם הנגיף, יש לפתח ולחדד יכולות ניתוח מידע וכן אבטחת מידע בתוך משרד הבריאות, ולהיעזר לצורך כך במומחיות מארגונים ממשלתיים אחרים (כגון התקשוב הממשלתי או יחידות בצבא כמו 8200) מבלי שאלה יהפכו להיות מנתחי המידע. במידה ונבחרת חלופה א, זו צריכה להיות החלופה העדיפה ויש לפעול כדי לממש אותה.

תת חלופה שניה: יצירת מערכת שאילתות מוצפנות ממשרד הבריאות ישירות אל חברות הסלולר.

אפשרות 1: קידום יכולת עיבוד מידע אין האוס בחברות הסלולר בצורה שתאפשר למשרד הבריאות לבקש מהן את הנתונים הרלוונטיים לקביעת סמיכות המגעים לחולה קורונה מאומת (אותות Bluetooth או בעדיפות פחותה יותר - נתוני המיקום) ושיפוי החברות על עבודתן.

אפשרות 2: מערכת אשר תאפשר להעביר "שאלות" מוצפנות מגוף לגוף, בלא שיהיה צורך להוציא דאטה או להעביר אותו לשרת נפרד או לענן.³⁵ מדובר בתוכנה "מצפינה" היושבת במחשבי משרד הבריאות ובתוכנה "מחשבת" היושבת במחשבי חברות הסלולר, וזאת בלא שיש צורך בהעברת כלל נתוני המיקום של כלל האזרחים אל שרתי המדינה או אל החברה הפרטית או שמי מעובדיה חשוף אליו. התוכנה המותקנת במשרד הבריאות מצפינה את זהותו של אדם שאובחן כחולה קורונה, ומעבירה את השאלות המוצפנות אל התוכנה היושבת בחברות הסלולר. כך, מקבל השאלות המוצפנות אינו יכול לדעת מיהו החולה, מיהם האנשים שאיתם בא במגע והיכן. כאשר הוא מחזיר את המידע אל משרד הבריאות, נעשה שימוש במפתח ההצפנה בתוכנה הנמצאת במחשבי משרד הבריאות ומשרד הבריאות יכול לדעת את זהותם של מי שבאו במגע עם החולה ולשלוח אליהם הודעה לגבי בידוד. מערכת שמישה כזאת היא למשל זו המוצעת על ידי חברת Duality והטכנולוגיה שלה מבוססת על מה שמכונה בעולם המתמטי פרטיות דיפרנציאלית (מבדלת), ונעשה בה שימוש בחקירת הלבנות הון, למשל.³⁶

חלופה ב': התקנת יישומון ייעודי לאיתור מגעים

יתרונות:

הסכמה של המשתמשים המתבטאת בהתקנת היישומון הייעודי על מכשיר הסלולר שלהם. העצמת המשתמשים, הפנמת התפיסה שלפיה במשבר אזרחי יש צורך באמון הציבור שלא יושג בכפיה. מודעות המשתמשים לגבי הפגיעה בפרטיותם אשר תתבסס על חשיפתם לתנאי השימוש ולמדיניות הפרטיות ביישומון ושליטה שלהם בפונקציות השונות. שמירה על פרטיות המשתמשים (ברמות שונות – ראו להלן הגישה הריכוזית מול הביזורית). ביישומונים המבוססים רק על אותות BLE - דיוק רב יותר באיתור מגעים מאשר התבססות על איכון סלולרי. חסרונות:

ככל שמדובר ביישומון שאינו מעביר מידע אחורה לשרת מרכזי (ראו להלן מודל ביזורי מול ריכוזי) – אין למדינה כלים לדעת מיהם חבי הבידוד ולפקח עליהם. היישומון מאפשר איתור מגעים וידוע מי שחייב בבידוד רק ביחס למי שהתקין אותו ולא לכלל הציבור. בכך הוא נתפס ככלי "תומך לחימה" בלבד. על פי הערכות נדרש כי אחוז משמעותי מהציבור (מחקר מאוניברסיטת אוקספורד הצביע על הצורך שלפחות 60% מהציבור במדינה) יתקין את היישומון הייעודי לאיתור מגעים על מנת שהוא ישמש ככלי יעיל ומדויק לאיתור מגעים. יישומון מיועד לרוב להתקנה על טלפון סלולרי חכם ובישראל ציבור גדול של משתמשי טלפונים "כשרים". עם זאת, מדובר לפי הנתונים הקיימים על כ-חצי מיליון בעלי טלפונים כשרים מתוך ציבור של כמיליון חרדים בישראל, וגם מתוך קבוצה זו יש מספר רב

של משתמשים המחזיקים במקביל בטלפון חכם או לחלופין משתמשים בטלפון חכם כשר אשר ניתן להתקין בו אפליקציות מבוססות מיקום³⁸ או יישומונים על מערכת ההפעלה של המכשיר. יש צורך בהשקעת מאמצים בפרסום נרחב ופעולות מתחום הכלכלה ההתנהגותית כדי שהציבור יוריד באופן מסיבי את היישומון (למשל תגמול כספי באמצעות שוברים (וואוצ'רים) על הורדת יישומונים ועל הסכמה להעביר נתונים אחרים לשרת מדינתי). יש צורך בשכבת הגנת סייבר שלא תאפשר לגורמים עוינים לפרוש משדרים או מקלטים שיעוותו את נתוני המגעים הנשמרים על גבי היישומון או יעשו בהם שימוש לרעה.

תתי חלופות, מאפיינים של יישומונים לאיתור מגעים, היבטי פרטיות וקשיים אפשריים:

א. עיקרון מיזעור המידע,³⁹ פרטי המידע הנאספים וטכנולוגיית האיסוף (נתוני איכון סלולרי, GPS, WIFI, Bluetooth)

נתוני איכון סלולרי ניתנים לאיסוף באמצעות רשת הסלולר עצמה, כלומר, באופן רחב ועל ידי חברות הסלולר, ואף ללא התקנת יישומון ייעודי או שמירתם על מכשיר הסלולר האישי של המשתמש. כך, למשל, הם ניתנים למעקב ע"י השב"כ.

מנגד, אותות (BLE) אינם מצביעים על מיקומו או תנועותיו של המשתמש, הם נשמרים רק על מכשירו האישי של המשתמש ואינם נשמרים במקביל על ידי חברות הסלולר.

בנוסף, נתוני איכון סלולרי פחות מדויקים לעומת אותות BLE ו-WIFI. באיכון סלולרי רמת דיוק של עד 500 מטר ובמעקב BLE מדובר ברמת דיוק של 2 מטר. חוסר הדיוק נובע מגודל התאים הסלולריים והעובדה שנתוני איכון סלולרי מבוססים על אותות GPS שעשויים להיות חלשים כתוצאה מתנאי מזג אויר או הפרעות פיזיות. איכון סלולרי גם מתקשה בזיהוי קירבה בממד הגובה, ולכן אינו מדויק במרחב עירוני צפוף ובמבני קומות.

כמו כן, לשם השגת התכלית של איתור מגעים בלבד אין צורך במעקב אחר תנועותיו של חולה הקורונה במרחב הגיאוגרפי אלא רק בידיעה מי היה בסמיכות פיזית אליו לפי מדדים אפידמיולוגיים.⁴⁰ לשם כך אין צורך בידיעת המועד המדויק (יום ושעה מדויקים) בו הגיע אדם למיקום גיאוגרפי מסוים אלא די בידיעת התאריך ומשך זמן שהייה בקרבת מכשירי סלולר סמוכים.

יישומון המבוסס על אותו BLE אומד את הסמיכות הפיזית באופן הבא: עם התקנת היישומון על מכשיר הטלפון מקבל היישומון מפתח הצפנה להפקת קודי זיהוי אקראיים. אין מדובר ב"שם בדוי" (פסדונים) קבוע ובוודאי שאין מדובר בנתוני זיהוי של המכשיר. לפי מפתח ההצפנה נשלח צופן שונה בכל פרק זמן נתון (בין דקה לחמש עשרה דקות) והיישומון משדר את קודי זיהוי האקראי בפערי זמן אלה. ככל שפערי הזמן בין שידור לשידור נמוכים חישוב משך הזמן לקיומה של סמיכות פיזית מדויק יותר. שידור קודי הזיהוי האקראיים נעשה באמצעות אותות BLE שהם אותות בעוצמה נמוכה יחסית וכך מובטח שהאותות לא יקלטו במרחקים פיזיים גדולים.⁴¹ בנוסף, מאחר ומדובר בקודי זיהוי אקראיים המופקים על ידי מפתח הצפנה הנמצא על גבי מכשיר הטלפון עצמו, שני אותות שנשלחו מהמכשיר של משתמש מסוים לא ייראו אותו הדבר ולא יוכלו לסמן בעתיד כי נוצרו באותו המכשיר.⁴² כל מכשיר טלפון שעליו מותקן היישומון קולט ושומר אצלו "לוג אותות" של כל קודי הזיהוי המשודרים בסביבתו ממכשירים אחרים, בצירוף חותם זמן ועוצמת אות ה-Bluetooth שנקלטה, כדי להעריך את המרחק הפיזי בין המכשירים. הקביעה האם משתמש נחשף לחולה קורונה מאומת נעשית על ידי השוואת קודי הזיהוי השמורים על מכשירו האישי עם אלו שנשמרו על מכשיר הסלולר של החולה ובדיקה האם נתקבלו קודי זיהוי זהים ברצף, כדי לוודא שהסמיכות הפיזית היתה אכן לפרק זמן הנדרש לפי המדדים האפידמיולוגיים. במקרה של חפיפה המסקנה המתבקשת היא שחולה הקורונה והמשתמש היו בסמיכות פיזית זה עם זה ועל המשתמש להיכנס לבידוד.

כלומר, אותות BLE מספקים בדיוק את נתוני מידע דרושים אלו, ועומדים משום כך בעיקרון מיזעור המידע. הם אינם מאפשרים איסוף נתוני מידע נוספים שאינם נדרשים לשם השגת התכלית של איתור מגעים.

לכן, ההבדלים בין נתוני איכון סלולרי לבין אותות BLE מלמדים שפוטנציאל השמירה על הפרטיות באמצעות BLE גדול בהרבה לעומת נתוני איכון סלולרי. משום כך גם המליץ האיחוד האירופי לעשות שימוש בטכנולוגיות BLE ביישומונים למעקב מגעים בזמן הקורונה.⁴³

מסקירת יישומי איתור המגעים הקיימים כיום בשימוש במדינות דמוקרטיות בעולם עולה כי מרביתם מבוססים על איסוף מידע באמצעות אותות BLE. במובן זה, איסוף המידע שלהם מדויק בהרבה מזה של השב"כ והם אינם זקוקים למידע נוסף משלים (כגון היסטוריית שיחות, הודעות וגלישה) ולחקירה אפידמיולוגית מקיפה על ידי אנשי מקצוע.

הקושי הטכנולוגי

יישומן המתבסס על איסוף מידע באמצעות אותות BLE מחייב הפעלה פרואקטיבית תמידית וקבועה של משדר ה Bluetooth במכשיר הטלפון הסלולרי. כלומר, מכשיר הסלולר חייב להישאר פתוח (לא נעול) כל העת על מנת לאפשר את שידור אותות ה BLE בפרקי זמן קצרים.⁴⁴ כתוצאה מכך, יישומנים אלו צורכים חיי סוללה ועל כן ההיענות הקיימת להתקנים עשויה להיות נמוכה.

עם זאת ניתן להתגבר על קושי זה. כך, ממשלת אוסטרליה ניהלה מגעים עם חברת אפל בנושא יישומן איתור המגעים האוסטרלי (COVIDSafe). בסופם נקבע שהיישומן יתוכנן כך שיהיה חייב להיותר פתוח על מנת לפעול אך ימשיך בפעולתו גם אם המשתמש נועל את מסך מכשיר הטלפון. באופן זה מצטמצמת צריכת חיי הסוללה של היישומן.⁴⁵

בנוסף, החל מאמצע מאי קושי זה כנראה לא יהיה רלוונטי לחלק מיישומי איתור המגעים. זאת משום שענקיות הטכנולוגיה אלפבית ואפל הודיעו על שיתוף פעולה נדיר ביניהן שבמסגרתו ישחררו באמצע חודש מאי API אשר יאפשר פיתוח והתקנת יישומנים שיעשו שימוש באותות Bluetooth ברקע של מערכת ההפעלה וכך להימנע מזלילת חיי סוללה. החברות הודיעו כי יאפשרו זאת באופן מוגבל אך ורק ליישומנים למטרת איתור מגעים (מכונה על ידן "exposure notification") שיופעלו על ידי או עבור ממשלות או שירותי בריאות כחלק מהמאבק בהתפשטות נגיף הקורונה.⁴⁶

אולם ההישענות על ה API של חברות אלו מחייב ציות לדרישות הארכיטקטורה, לסטנדרט הגנת הפרטיות ולתנאי השימוש שיקבעו ענקיות הטכנולוגיה בעצמן ועל דעתן.⁴⁷ בכל הקשור לפרטי המידע הנאספים על ידי יישומי איתור מגעים ייעודיים כבר הודיעו ענקיות הטכנולוגיה כי לא יאפשרו שימוש באיכון סלולרי במערכת חשיפת המגעים שבכוונתן להטמיע במערכות ההפעלה שלהם בתחילת יוני ושתייטר את הצורך בהתקנת יישומן ייעודי נוסף.⁴⁸

ב. שמירת המידע ומחיקתו

על מנת לאפשר איתור מגעים יעיל יש לשמור את המידע הנחוץ להגשמת תכלית זו למשך תקופה של לפחות 14 יום שזהו, ככל הידוע כיום, משך זמן דגירת נגיף הקורונה בגוף האדם לפני התפרצות מחלת הקורונה. בתום תקופת הזמן הרלוונטית לאיתור מגעים מבחינה אפידמיולוגית המידע אינו נחוץ עוד להגשמת התכלית של איתור המגעים, ועל כן מבחינת הגנת הזכות לפרטיות יש למחוק אותו.⁴⁹

נציבות האיחוד האירופי, למשל, הנחתה את מפתחי יישומי איתור המגעים לשמור את המידע כל עוד הוא נחוץ לשם איתור ואזהרת אנשים העלולים להיחשף לחולה קורונה. על בסיס הנחיה זו גזרה הנציבות תקופת זמן שאינה עולה על חודש (תקופת דגירה של הנגיף המוערכת בכ-14 ימים + מרווח ביטחון). בסיום תקופת זמן זו או במידה שהמשתמש נבדק ונמצא שלילי לנגיף הקורונה יש לפי הנחיית הנציבות למחוק את המידע גם ממכשיר הסלולר של המשתמש.⁵⁰

באשר למיקום המידע במהלך תקופת שמירתו, שמירת המידע בזיכרון הפנימי של מכשיר הסלולר האישי של המשתמש והכרה בזכותו להסיר את היישומן בכל עת ולמחוק בדרך זו את כל המידע שנאגר עליו ע"י היישומן מאפשרת את שליטתו של המשתמש במידע ומהווה מדד להגנה חזקה יותר על זכותו לפרטיות. כאשר המידע שנאסף על המשתמש מועבר מראש לשרת מרכזי שבידי גוף ציבורי או פרטי האמון על ביצוע איתור המגעים המדובר במידע רב הנחשף לעיני אותו גוף שלא לצורך, בכל הקשור במשתמשים שלא חלו בקורונה או שלא נחשפו לחולה כאמור, ופוטנציאל הפגיעה בפרטיות גבוה יותר.

ג. מקום הפיענוח של ההצפנה, ביצוע עיבוד המידע ומורשי הגישה אליו - גישה ריכוזית מול גישה ביזורית

על מנת לבצע איתור מגעים, כלומר לבחון מי היה בסמיכות פיזית למשתמש שנמצא חולה קורונה, יש צורך בעיבוד המידע שנאגם עליו על ידי היישומון ובחינה לפי נתוני האיכון הסלולרי או "לוג האותות", כאשר מדובר ביישומון הנשען על איסוף אותות BLE, מיהם המשתמשים ששהו בסמיכות פיזית אליו.

בכל הנוגע למידע שנשמר על מכשיר הסלולר האישי של המשתמש, קיימות כיום שתי חלופות למורשיי הגישה למידע ולעיבודו לשם איתור מגעים:

הגישה הריכוזית: המידע (או "לוג האותות") שנשמר על גבי מכשיר הטלפון של משתמש א', שנמצא חולה קורונה, מועברים, אם משתמש א' מסכים לכך, לשרת מרכזי שבשליטת רשות הבריאות הממשלתית במדינה. בידי המדינה או רשות הבריאות נמצאים המפתחות לפיענוח ההצפנה של המידע המותמם שנאגם על המשתמש וכך היא מזהה את המשתמשים שנמצאו בסמיכות פיזית למשתמש א' חולה הקורונה ומודיעה להם להיכנס לבידוד. משרד הבריאות לא יודע בהכרח היכן היה המפגש בין הטלפונים אלא את עצם העובדה שמפגש כזה התרחש.

הגישה הריכוזית, המבוססת על הפרוטוקול של קבוצת המומחים שהקימה את פרויקט PEPP-PT⁵¹ שבהובלת חברת הבינה מלאכותית Arago הגרמנית,⁵² או על ארכיטקטורה אחרת, מוטמעת ביישומון איתור המגעים "המגן" הישראלי,⁵³ "TraceTogether" בסינגפור,⁵⁴ ביישומון האוסטרלי COVIDSafe המבוסס עליו,⁵⁵ ביישומון StopCovid שבשימוש ממשלתי צרפתי,⁵⁶ ביישומון NHS CV19 שבשימוש ממשלתי אנגלי,⁵⁷ ובישומון Aarogya Setu שבשימוש ממשלתי הודו.⁵⁸ גרמניה שתחילה אצדה אף היא בגישה הריכוזית חזרה בה והודיעה ב 27.04.20 שבכוונתה לפתח אפליקציה שתתבסס על הגישה הביזורית.⁵⁹

היתרון: למדינה יש שליטה במידע שממנו אפשר להבין מי חייב בידוד ולגבי שרשרת ההדבקה.

החשש: כאשר המידע מועבר לשרת מרכזי שבשליטת המדינה ובידה גם המפתחות לפיענוח ההצפנה מתעורר החשש מפני זיהוי חוזר של נושא המידע וחשיפת זהותו ומכלול תנועותיו. למשל, על ידי קישור לכתובת ה-IP של מכשיר הסלולר האישי שלו אפשר לגלות את כתובת המגורים של בעל המכשיר ולזהותו. זיהוי חוזר עלול להוביל לשימוש לרעה במידע על ידי המדינה או גופים מסחריים שיצליחו לשים את ידם על המידע.⁶⁰ למשל, המדינה עלולה לפענח אותות המשודרים ממכשירים של משתמשים שלא זוהו כחולי קורונה, לדוגמה – לזהות את כל האנשים שהגיעו להפגנה מסוימת.

הגישה הביזורית: כאשר משתמש א' נמצא חייב לנגיף הקורונה ומעדין בכך, מרצונו החופשי, את היישומון, שולח היישומון (דרך שרת מרכזי כחלק מתעבורת המידע) את המפתחות ששימושו להצפנת המידע על משתמש א' לכל המשתמשים האחרים של היישומון (להלן יכונה במרכז "משתמש ב"). אז מתבצע בכל מכשיר סלולרי שעליו מותקן היישומון פיענוח של המידע המוצפן שהתקבל ממשתמשים אחרים ועיבודו על מנת לבחון האם התקיימה סמיכות מגעים בין משתמש א' למשתמש ב'.⁶¹ כלומר, הבדיקה האם התקיימה סמיכות פיזית לחולה קורונה מתבצעת על מכשיר הסלולר האישי של כל משתמש ולא על גבי שרת מרכזי שבשליטת משרד הבריאות או גוף ציבורי או פרטי אחר. למשתמשים מסור שיקול הדעת מה לעשות והאם להיכנס לבידוד נוכח הידיעה ששהו בסמיכות פיזית לחולה קורונה. כמו כן, בגישה הביזורית לא ניתן לחבר את הזהות האמיתית של המשתמש אל האותות המשודרים ממכשיר הסלולר שלו, והשליטה האם לחשוף את הזהות (כלומר המפתח לחשיפה) נמצאת בידי המשתמש ולא בידי משרד הבריאות או החברה המספקת את היישומון. כלומר, המידע המועבר למשרד הבריאות לא מאפשר למשרד הבריאות לדעת היכן היתה החשיפה; האם שני אנשים שונים נחשפו לאותו חולה אלא רק שהתקיימה חשיפה.

לפי הדיווחים, ביישומונים הפועלים לפי השיטה הביזורית נוספה בימים האחרונים אפשרות המקנה למשתמש את זכות הבחירה האם לאשר את העברת מספר הטלפון שלו או פרטים מזהים אחרים על מכשיר הנייד שלו לרשויות הבריאות וכך להקל על רשויות⁶² הבריאות להיות עמו בקשר ולספק לו עצות כיצד עליו לנהוג במידה וקיים חשש שנחשף לחולה קורונה או נדבק בעצמו בנגיף. כך, למשל, היישומון המוצע על ידי חברת TrackVirus בשיתוף עם ארגון איחוד הצלה נוקט את הגישה הביזורית תוך הותרת הבחירה בידי המשתמש. היישומון מנטר את מסלול תנועתו של המשתמש ושומר את המידע על גבי מכשיר הסלולר האישי. בקבועי זמן מוגדרים משווה היישומון את המידע שאגור אצלו למסד הנתונים של משרד הבריאות ובדק האם קיימת חפיפה. במידה שנמצאה חפיפה מקבל המשתמש התראה כי נחשף לחולה קורונה וכי עליו ליצור קשר עם רשות הבריאות המקומית ולדווח על כך. אם משתמש נמצא חולה קורונה ואותר על ידי רשות הבריאות, באפשרותו לייצא את היסטוריית המיקומים שלו לשרת משרד הבריאות.⁶³

בקווים המנחים שפרסמה נציבות האיחוד האירופי נקבע שהגישה הביזורית עומדת בצורה טובה יותר בדרישת מיזעור המידע לפי ה-GDPR, אולם לא ניתנה הנחייה המחייבת העדפת הגישה הביזורית על פני הגישה הריכוזית.⁶⁴ הגישה הביזורית, המבוססת על הפרוטוקול של קבוצה אקדמית המכונה DP-3T,⁶⁵ תוטמע ביישומון שבשימוש ממשלתי גרמני,⁶⁶ ב Immuni שבשימוש ממשלתי איטליה וב-DP-3T שבשימוש ממשלתי שווייץ ואוסטריה.⁶⁸ היו שהציעו כי הגרסה העתידית של יישומון "המגן" הישראלי תנקוט אף היא בגישה הביזורית לפחות בנוגע לאותות ה-BLE.⁶⁹

בנוסף, כחלק מהתווית הארכיטקטורה והעדפות הפרטיות שדורשות ענקיות הטכנולוגיה אלפבית ואפל הודיעו החברות שיאפשרו שימוש ב-API שלהן רק ליישומונים שינקטו את הגישה הביזורית, כאשר למשתמש שאובחן כחולה קורונה ניתנת הבחירה האם להעביר את לוג האותות שלו למאגר המידע של רשות הבריאות המקומית המכיל את לוג האותות של חולי קורונה מאומתים. רשות הבריאות המקומית לא תוכל לדעת את זהותו אך מידע על תנועותיו הנדרש לשם בחינת הסמיכות הפיזית למשתמשים אחרים יועבר לשרת מרכזי שלה.⁷⁰ עמדתן של ענקיות הטכנולוגיה כבר משפיעה על מדינות נוספות שתחילה דווח שיעשו שימוש בגישה הריכוזית אולם עתה הן שבו להתלבט בנושא. כך, למשל, נטישת הגישה הריכוזית ואימוץ גישה ביזורית על ידי גרמניה הושפעה, לפי הדיווחים,

מסירובה של חברת אפל לאפשר שימוש באותות BLE ע"י יישומון המבוסס על גישה ריכוזית.⁷¹ ממשלת צרפת שיישומון איתור המגעים שפיתחה מבוסס על הגישה הריכוזית במטרה, לטענתה, לאפשר שליטה בניהול משבר הקורונה לרשות הבריאות הממשלתית, תקפה לאחרונה את חברת אפל על סירובה של זו לאפשר שימוש באותות BLE ברקע מערכת ההפעלה גם במסגרת הגישה הריכוזית.⁷²

כפיית הארכיטקטורה הביזורית על ידי ענקיות הטכנולוגיה אלפבית ואפל הינה בעלת השלכות מרחיקות לכת. היא הובילה לפיצול בין המדינות החברות באיחוד האירופי, שחלקן (צרפת, אנגליה ונורבגיה) בחרו בגישה הריכוזית בנימוק שזו הגישה אשר תאפשר לשירותי הבריאות להתכונן ולנהל ביעילות גל התפרצות נוסף של הנגיף, בעוד גרמניה, שווייץ, אוסטריה ואיטליה בחרו לאמץ את הגישה הביזורית בעיקר בכדי ליצור יישומון שהפעלתו קלה בניסיון להביא לאימוצו המהיר ע"י מספר רב של משתמשים.⁷³

נציבות האיחוד האירופי פועלת לגישור על הפערים בניסיון להביא לאימוצה של גישה אחידה ע"י כל מדינות האיחוד ואף רואה בשיתוף הפעולה בין אלפבית וגוגל הזדמנות ל"שלום" בין נציבות האיחוד האירופי לענקיות הטכנולוגיה, כל עוד אלה יפעלו בשקיפות.⁷⁴

יש הטוענים שבכל הקשור לאיתור מגעים, התעקשות זו הובילה להיווצרותה של משוואת איזונים שגויה בין פרטיות ליעילות ומיצבה את הזכות לפרטיות ככזו הפוגמת באופן בלתי מידתי ביכולתן של מדינות לנהל ביעילות את מאבקן בנגיף הקורונה ולהגן על בריאות הציבור.⁷⁵ בנוסף, היא מבליטה בכל העוצמה את כוחן של ענקיות הטכנולוגיה לכפות מדיניות אף אם זו מנוגדת לרצון של ממשלות נבחרות. מעניין שבארה"ב, מדינת הבית של ענקיות הטכנולוגיה, נראה שמחלחלת דווקא ההבנה שהפעם התפיסה כאילו ביכולתה של הטכנולוגיה לתקן את כל בעיות העולם היא יותר מיתוס מאשר אמת, ויישומונים ביזוריים לא יועילו. מדינות כגון ניו יורק, קליפורניה ומסצ'וסטס וערים כגון בולטימור וסאן פרנסיסקו בחרו שלא להישען כלל על הטכנולוגיה במאמציהן לאיתור מגעים בנימוק לחוסר יעילות והעדפת גיוס כוח אדם נוסף למשימה.⁷⁶

היתרון: הגנה על פרטיות המשתמשים ברמה גבוהה יותר לעומת הגישה הריכוזית, כתנאי מוקדם לכך שמשתמשים ירצו להוריד את היישומון וכן לא ינסו "לרמות" אותו באמצעות כיבוי או הותרתו בבית.

החששות:

הכניסה לבידוד בהתאם לממצא של איתור המגעים מותנה ברצונו הטוב של המשתמש חולה הקורונה כאשר לרשות האחראית על בריאות הציבור אין כל שליטה או מידע על זהותו ועל מעשיו ולכן אין תועלת שלטונית. עם זאת, ניתן לחייב משתמש שנמצא חיובי לנגיף הקורונה ושנתוני המגעים שלו נשמרו על המכשיר האישי שלו באמצעות היישומון, להעביר את הנתונים לשרת של משרד הבריאות או של חברה פרטית. חלק מהמומחים הטכנולוגיים טוענים שמכשירי הסלולר האישיים לא יוכלו לעמוד, מבחינת כוח המיחשוב שלהם, בעיבוד הנדרש לפיענוח ההצפנה של כל קודי הזיהוי של כל חולה קורונה שיעביר את הנתונים לגביו (ככל שיותר אנשים ישתמשו ביישומון וככל שיהיו יותר חולים שאת הנתונים שלהם יהיה צריך לבדוק יהיה מדובר בכמויות אדירות של דאטה). אחד הפתרונות (למשל זה שהוצע על ידי קואליציית אלפבית ואפל) הוא לחלק לאיזורים ומדינות ומשתמשים יקבלו מידע רק בנוגע לאיזור שלהם. עם זאת הפתרון מעורר שני קשיים – רמת הרזולוציה של המיקום (יכולה להגביר אפשרות לזיהוי חוזר); צורך בנתוני מיקום באמצעות GPS בנוסף על אותות BLE.

ד. יעילות איתור המגעים באמצעות יישומון ייעודי - בהתחשב בהיקף התקנתו על ידי הציבור

(1) נכונות אחוז ניכר מהציבור להתקין את היישומון על מכשיר הסלולרי

יעילותו של יישומון ייעודי לאיתור מגעים תלויה בהיקף התקנתו ע"י אחוז ניכר מהאוכלוסייה.⁷⁸ אחד החששות המרכזיים בהישענות על יישומון ייעודי שהתקנתו וולונטרית היא היעדר שיתוף פעולה מצד הציבור אשר ימנע מהתקנת היישומון. ככל שהיישומון יקשה על השימוש במכשיר הטלפון החכם, אם על ידי האטתו או צריכת חיי סוללה מוגברת, תפחת גם נכונות הציבור להתקינו.

אי עמידתו של היישומון בסטנדרט הגנת הפרטיות שדורשות ענקיות הטכנולוגיה אפל וגוגל עשוי למנוע את האפשרות לעשות שימוש ב-API שיפרסמו לשם הפעלת היישומון ברקע מערכת ההפעלה וכתוצאה קשיים אלו הבאים לידי ביטוי בצריכת חיי סוללה מוגברת והכבדה על פעילות המכשיר עלולים להתגבר.⁷⁹

נכונות נמוכה בקרב הציבור להתקין את היישומון עלולה להתרחש גם אם היישומון יספק דיווחים מוטעים בנוגע לחשיפה לחולה קורונה מאומת והצורך להיכנס לבידוד, כפי שהיה עם יישומון "המגן" בתחילת דרכו.⁸⁰

החשש מפני היעדר שיתוף פעולה מצד הציבור והימנעות מהתקנת היישומון על ידו אינו מנת חלקה של ישראל לבדה. מדינות דמוקרטיות רבות מתמודדות עתה עם סוגיה זו. בבחינת חוקיות השימוש ביישומון איתור מגעים ייעודי אף המליצה נציבות האיחוד האירופאי שהתקנת היישומון תהיה וולונטרית וכי חיוב התקנת היישומון יכול להיעשות רק מכוח חוק נחוץ, ראוי ומידתי לשם השגת מטרות מסוימות.⁸¹

באוסטרליה, למשל, הסביר ראש הממשלה טרם הפצת היישומון לאיתור מגעים COVIDSafe לציבור, כי אינו פוסל הפיכת התקנתו לחובה על כלל האוכלוסייה.⁸² אולם, בחוק שנחקק לקראת הפצת היישומון לציבור נאסר על התניית כניסה למקומות שונים או קבלת שירות או מוצר בחיוב התקנת היישומון,⁸³ ועם הפצת היישומון לציבור הכריזו ראש הממשלה ושריו כי מדובר ביישומון שהתקנתו וולונטרית.⁸⁴ עם זאת ממשלת אוסטרליה השקיעה רבות בשיווק היישומון לציבור ובהסברת חשיבות התקנתו על ידי מספר רב ככל האפשר של אנשים באמצעות קמפיין תקשורתי מקיף שכלל סרטונים, כרזות רחוב, דיווחי רדיו ופוסטים ברשתות החברתיות.⁸⁵ ראש ממשלת אוסטרליה התראיין פעמים רבות בתקשורת והסביר שהתקנת היישומון היא המפתח לחזרה הדרגתית לשגרה, להתנעת הכלכלה. עוד השווה את היישומון לקרם הגנה מפני חשיפה לשמש. היישומון, כך הסביר, יגן על המשתמש ומשפחתו, על עובדי מערכת הבריאות ובסופו של דבר יגן על מקור הכנסתו של המשתמש ומשפחתו שכן יאפשר התנעת הכלכלה האוסטרלית מחדש.⁸⁶ מאמצי התקשורת נשאו פרי ובתוך 10 ימים הותקן היישומון על ידי מספר שיא של 5 מיליון משתמשים.⁸⁷

באנגליה העומדת להפיץ באמצע מאי יישומון איתור מגעים בפיתוחה (NHS CV19), פועלת הממשלה כבר עכשיו במאמצי הסברה מקיפים המבהירים כי התקנת היישומון היא שתאפשר לשמור ולהגן על המשתמש ומשפחתו, תמנע את הצפת מערכת הבריאות וקריסתה ותהיה אמצעי מרכזי בהשבת המדינה והכלכלה לשגרה ולתפקוד מלא.⁸⁸

בהודו שווק היישומון (Aarogya Setu) בתחילה להתקנה וולונטרית. שמונים מיליון אזרחים התקינו את היישומון. אולם, ככל שהחלו צעדי החזרה לשגרה הפכה הורדת היישומון לחובה על אוכלוסיות מסוימות וכיום מחויבים בהתקנתו עובדים חיוניים, כלל העובדים במגזר הפרטי והציבורי ותושבים באיזורים המוגדרים בסיכון גבוהה להתפרצות המגיפה. האחריות לוודא את התקנת היישומון מוטלת על המעסיקים ומנהלי מתחמי מגורים באיזורים שבסיכון.⁸⁹

בסינגפור מתמודדת הממשלה עם אחוזי התקנה נמוכים יחסית של היישומון, בעיקר עקב צריכת חיוב הסוללה המוגברת שלו והכבדתו על פעילות המכשיר הסלולרי עקב אי התאמתו לארכיטקטורה הנדרשת ע"י שותפות אלפבית ואפל, ועל כן גוברים שם עתה הקולות הקוראים לחיוב התקנת היישומון לכלל האוכלוסייה, רק לעובדים חיוניים או לכלל העובדים כתנאי לחזרה לשגרה מלאה.⁹⁰ עם שחרור המגבלות וחזרת המשק לפעילות השיקה ממשלת סינגפור יישומון נוסף בשם SafeEntry.⁹¹ המדובר במערכת מעקב כניסה ויציאה דיגיטלית העוקבת אחר מי שנכנס ויוצא ממקומות שונים כסיוע לאיתור מגעים. המעקב נעשה באמצעות סריקת כרטיס הזיהוי או קוד QR במכשיר הסלולר האישי של האדם עם כניסתו ויציאתו ממקום העבודה, החנות, המסעדה, הסופרמרקט או בית הספר. האחריות להתקנת המערכת הוטלה על מקומות עבודה, מפעלים, בתי ספר ומוסדות חינוך, גני ילדים, מוסדות בריאות, בתי אבות, מספרות, סופרמרקטים, שווקים מסוימים, קניונים ובתי מלון החייבים בהתקנתה החל מה 12 במאי, 2020. רשימת המקומות החבים בהתקנתה תתעדכן ככל שתחודש הפעילות הכלכלית במדינה.⁹² המידע הנאסף באמצעות SafeEntry כולל שם, קוד הזהות, מספר טלפון נייד, המקום בו שהה, מועד השהייה המדויק (זמני כניסה ויציאה). מסירת המידע היא מנדטורית והמידע יישמר בשרת שירותי הבריאות באופן מותמם והגישה אליו תינתן רק לבעל מקצוע מוסמך לתכלית איתור מגעים. המידע ישמר רק למשך הזמן הדרוש לשם איתור מגעים.⁹³



הטבלה שלהלן מציגה את החלופות הקיימות היום ליישומונים אלה,
בהתאם למאפיינים שצוינו לעיל



הסקירה המלאה

*ד"ר ערן טוך, מרצה בכיר, הפקולטה להנדסה, אוניברסיטת תל אביב

רשימת מקורות ששימשה לטבלה ההשוואתית

הערות שוליים

תגיות:

נגיף הקורונה, זכויות אדם, בריאות, פרטיות, התוכנית לדמוקרטיה בעידן המידע, המרכז לערכים ולמוסדות דמוקרטיים

לכל הנושאים