



חוות דעת הרשות להגנת הפרטיות

בהתאם לחוק הסמכת שירות הביטחון הכללי
לסייע במאמץ הלאומי לצמצום התפשטות נגיף
הקורונה החדש (הוראת שעה), התש"ף-2020





14.07.2020

חוות דעת הרשות להגנת הפרטיות בהתאם לחוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020

הרשות להגנת הפרטיות (להלן - "הרשות") מתכבדת להגיש את חוות דעתה בהתאם לסעיף 12 לחוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020 (להלן - "חוק הסמכת השירות" או "החוק").

חוק הסמכת השירות קובע כי ימונה צוות שרים לבחינת הצורך בהמשך ההסתייעות בשירות מכוח החוק "בהתחשב במצב התחלואה בישראל בשל נגיף הקורונה החדש, בתרומת תוצאות פעולות הסיוע לצמצום התפשטות המחלה ובקיומן של חלופות להסתייעות כאמור, והכל בהתחשב, בין השאר, בפגיעה בזכות לפרטיות" (להלן - "צוות השרים").

עוד קובע סעיף 12 לחוק כי בפני הצוות תונח חוות דעתה של הרשות להגנת הפרטיות במשרד המשפטים בעניין זה.

תקציר חוות הדעת

האמצעי בו נוקטת כיום מדינת ישראל לצורך איתורם של מי שבאו במגע עם חולה קורונה בפרק הזמן שקדם לאבחונם - קרי, שימוש ביכולות הטכנולוגיות של שירות הביטחון הכללי לצורך איכון החולה ומגעיו - טומן בחובו פגיעה קשה ביותר בפרטיותם של כל אזרחי המדינה לגביהם מופעל הכלי, ומעורר קשיים בהיבטים מרכזיים נוספים. כפי שקבע בית המשפט העליון בפסק הדין בעניין בן מאיר "הבחירה לעשות שימוש בארגון הביטחון המסכל של המדינה לצורך מעקב אחר מי שאינם מבקשים לפגוע בה, מבלי שניתנה הסכמה לכך מצד מושאי המעקב, מעוררת קושי רב ביותר".

הרשות להגנת הפרטיות ערה לצורך הדוחק שבהפעלת אמצעי יעיל לאיתור המגעים של חולי קורונה מאומתים, בשים לב לנתוני התחלואה ולהכרח בבלימת התפשטות המגפה. אולם, במצב הדברים הנוכחי, כאשר ברור שנגיף הקורונה אינו צפוי להיעלם בקרוב והעולם כולו נערך ל"שגרת קורונה" העשויה להימשך חודשים ואולי אף שנים, מתחזק הצורך באיתור ושימוש באמצעים חלופיים מידתיים, אשר יוכלו לשמש לטווח ארוך, גם בעתות גאות ושפל של המגפה.

בתוך כך, קיימה הרשות במרוצת השבועות האחרונים פגישות ובדיקות מקיפות לבחינת האמצעים הדיגיטליים השונים העומדים כיום בפני הממשלה לשם הגשמת התכלית של איתור מגעים וקטיעת שרשרת ההדבקה.

כפועל יוצא מתהליך בחינה זה, הרשות סבורה כי לעת הזו ישנה חלופה הולמת אחרת, והיא יישומון "המגן 2".

¹ בג"ץ 2109/20 בן מאיר נ' ראש הממשלה (26.4.20), פסקה 46 לפסק הדין.





יישומון המגן 2 פותח על ידי משרד הבריאות תוך שמירה על עקרונות העיצוב לפרטיות, באופן המאפשר איתור יעיל של מגעים בטווח זמן מיידי, ובד בבד שומר בצורה המיטבית על פרטיותם של המשתמשים. היישומון העדכני עוצב כך שהוא משקלל נתוני מיקום ונתוני קרבה, באופן שעתידי להגדיל דרמטית את יעילות איתור המגעים לעומת החלופות האחרות. הגם שנדרש עוד לטייב את היישומון האמור הן בהיבטים טכנולוגיים והן בהיבטי הגנת פרטיות ואבטחת מידע, הרי שלעת הזו, ובהינתן החלופות האחרות הזמינות כיום לתפעול מהיר - הרשות סומכת ידיה על יישומון זה. היישומון מוכן להפעלה אך טרם הושק, ובהתאם לאמור בחוות דעת זו - הרשות קוראת להפעלתו ולהטמעתו בקרב הציבור לאלתר.

היתרונות ביישומון המגן 2 על פני האמצעים המופעלים כיום גלומים בשורה ארוכה של מאפיינים – היישומון פועל על פי המודל הביזורי, כך שכל נתוני המיקום ונתוני הקרבה הנאספים על ידו נשמרים ומעובדים אך ורק על גבי המכשיר הנייד של המשתמש. ליישומון ישנה יכולת גבוהה לאיתור מגעים מבוססי קרבה, ברמת דיוק של עד סנטימטרים, לרבות בתוך שטח סגור ויכולת הבחנה בין קומות. הנתונים כלל אינם מדווחים למשרד הבריאות או לכל גורם אחר (להבדיל ממודל ריכוזי בו המידע מועבר למשרד הבריאות), ונמחקים במועד הפיכתם לבלתי-רלוונטיים; מדובר במערכת מבוססת-הסכמה, באופן שכל פעולה ביישומון טעונה הסכמה אקטיבית של המשתמש, וכך גם התקנתו על גבי המכשיר הנייד; המידע שנאסף ונשמר ביישומון הוא המידע המינימלי הדרוש להגשמת תכליתו, והסרת היישומון מביאה למחיקת המידע כולו. היישומון מבצע שימוש בנתוני מיקום ובנתוני קרבה, ועל כן הוא בעל פוטנציאל להגשים ביעילות רבה – שאינה נופלת מזו של מנגנון השב"כ – את התכלית של איתור המגעים, הן מבחינת דיוק הממצאים והן מבחינת ההגנה על הפרטיות.

להבדיל, השימוש באמצעי האיכון של השב"כ, המבוסס על נתוני מיקום במודל ריכוזי, מהווה פגיעה משמעותית בפרטיות. בנוסף, גם מנגנון איכון השב"כ אינו מיטבי מבחינת הדיוק ולראייה היקף האיכונים השגויים שבוצעו בתקופה האחרונה.

על כן, הרשות סבורה כי המשך השימוש באמצעים המופעלים על ידי השב"כ, על מידת דיוקם המוגבל ובהינתן שמידת פגיעתם בפרטיות גדולה לאין שיעור, גם לאחר שהיישומון בגרסתו המשודרגת יופעל, תהווה פגיעה לא מידתית בפרטיות, וכן עשויה להוביל לפגיעה באמון הציבור במערכות השלטון, לכרסם באופן משמעותי במעמדה של הזכות החוקתית לפרטיות, ולהביא לנרמול של שימוש ביכולות טכנולוגיות של גופי בטחון לצורך פרקטיקות של מעקב אחר אזרחים שומרי חוק.

נוסיף, כי עצם השקת היישומון אינה מספיקה. יעילותו והצלחתו כאמצעי חלופי תלויה בראש ובראשונה במידת התפוצה וההטמעה שלו בקרב הציבור הרחב. לשם כך יש להשקיע את מירב המאמצים בפעילות הסברתית מואצת ומאומצת בהיקף נרחב, לצד פעילות הסברה ממוקדת במגזרים מסוימים, שקיפות מלאה, הכל במטרה להעלות את אמון הציבור ביישומון ולגרום לציבור להתקינו.



יודגש, כי יישומון המגן 2 אינו חף מטעויות וכטבעה של טכנולוגיה מתפתחת – גם לו יידרש המשך שיפור וטיוב. עם זאת, וכפי שהשתקף בבירור במהלך השבועיים האחרונים, מנגנון השב"כ, מעבר לפגיעה הדרמטית בהיבטי פרטיות, מזמן אף הוא טעויות למכביר, ועל רבים נגזר בידוד והגבלה דרמטית על חופש התנועה, כאשר למעשה כלל לא באו במגע עם חולה קורונה (כמו כן, מנתוני הדיווח של משרד הבריאות מיום 9/7/2020 עולה כי אחוז החולים המאומתים מבין המבודדים שקיבלו התראת איכון עומד על כ 5% מסך המבודדים בלבד).

בהינתן שאף אחת משתי מהחלופות הקיימות כעת אינה מושלמת, ובכוחן של שתיהן להגשים את התכלית של איתור המגעים ביעילות ובמהירות – יש להעדיף את החלופה שפגיעתה בפרטיות פחותה לאין ערוך. כך מתחייב גם מפסיקת בית המשפט העליון, אשר קבע בעניין בן מאיר כי "המאמץ לאיתורה של חלופה יעילה חייב להימשך ללא לאות... 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 וולונטרי ושקוף למשתמש".

לפיכך, עמדת הרשות היא שיש להשיק ללא דיחוי את גרסת "המגן 2.0", שכן בהינתן החלופות הקיימות היא עדיפה לאין שיעור על פני שימוש בכלי מעקב פוגעני של גוף בטחון שאינו מיועד למטרה זו.

בכל הנוגע לאמצעים המשלימים שנבחנו כיום, סבורה הרשות להגנת הפרטיות כי לפני הטמעתם במסגרת פתרון כולל, יש לבצע תסקיר מעמיק לניתוח השפעה על הפרטיות, וכן לשלב את הרשות במסגרת תהליך האיפיון והפיתוח של אמצעים אלה, שכן הם נושאים בחובם פגיעה משמעותית בפרטיות.

חוות הדעת שלהלן סוקרת בהרחבה מגוון טכנולוגיות ניטור, לרבות אלו המשמשות מדינות שונות ברחבי העולם, מציגה את המודלים השונים הקיימים בתחום, ובונה מדרג אמצעים לאיתור מגעים בראי הפרטיות. לשם הנוחות, מדרג האמצעים מוצג גם בגרף ויזואלי (ראו עמוד 12).

כמו כן, כוללת חוות הדעת נספח רחב היקף הסוקר בהרחבה פרקטיקות ניטור בהקשרי מגפת הקורונה, הננקטות נכון להיום ב-16 מדינות מובילות ברחבי העולם.





תוכן העניינים

2	תקציר חוות הדעת
6	עקרונות דיני הגנת הפרטיות בקליפת האגוז
6	מבוא
7	התשתית הטכנולוגית
7	1. נתוני מיקום והסכנה לפרטיות
8	2. נתוני קירבה והסכנה לפרטיות
10	3. המודל הריכוזי אל מול המודל הביזורי
11	מדרג אמצעים לאיתור מגעים בראי הפרטיות
13	אמצעים לניטור דיגיטלי
14	עידוד התקנת היישומון ונשיאת המכשיר
15	אמצעים משלימים להרחבת הכיסוי
15	התממשקות לסטנדרט בינלאומי
16	עיצוב לפרטיות בשמירה על המידע
17	דגשים לפרטיות במאגרי משרד הבריאות
17	עמדת הרשות להגנת הפרטיות
18	1. יישומון המגן 2.0
19	2. שימוש באמצעים משלימים להרחבת הכיסוי
20	3. השימוש בכלי השב"כ
22	נספח א' – פרקטיקות ניטור ברחבי העולם





חוות דעת הרשות להגנת הפרטיות

במסגרת הוראות חוק הסמכת השירות מונחת בזאת בפניכם חוות דעת הרשות להגנת הפרטיות.

עקרונות דיני הגנת הפרטיות בקליפת האגוז

הזכות לפרטיות הינה זכות חוקתית הקבועה בסעיף 7 לחוק-יסוד: כבוד האדם וחירותו. זכות זו היא נגזרת של כבוד האדם כמו גם זכות אזרחית המבטאת את החירות הבסיסית של האדם "להיעזב במנוחה". פרטיות בהקשר זה מתיישבת עם הצורך של אנשים להישאר אונימיים וכן להיות מוגנים מפני התערבות פסולה של רשויות המדינה וגורמים אחרים, בחייהם. תפיסה זו באה לידי ביטוי בדין הישראלי, בין היתר, בהוראות סעיף 2 (1) לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") המגדיר פגיעה בפרטיות כ"בילוש או התחקות אחר אדם העלולים להטרידו".

חוק הגנת הפרטיות כולל מספר עקרונות מרכזיים. עיקרון אחד הוא **עיקרון ההסכמה**, המבטא את שליטתו של הפרט ביחס למידע הנוגע אליו, ולפיו הפרט הוא האחראי ביחס לאיזה מידע הנוגע אליו ייחשף, ולמי. עיקרון זה בא לידי ביטוי, בין היתר, בסעיף 1 לחוק הגנת הפרטיות, הקובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". על פי חוק הגנת הפרטיות, הסכמה בהקשר זה צריכה להיות "מדעת", קרי כזו הניתנת רק לאחר שאדם מבין את משמעות הסכמתו, ואת השלכותיה. עיקרון מרכזי נוסף הוא **עיקרון צמידות המטרה**. על פי עיקרון זה, המוסדר תחת סעיפים 2 (9) ו-8 (ב) לחוק הגנת הפרטיות, שימוש במידע יכול להיעשות אך ורק בהתאם למטרה שלשמה הוא נאסף מלכתחילה. שימוש במידע למטרה אחרת מזו שלשמה הוא נאסף, מהווה פגיעה בפרטיות.

אמנם, ככל הזכויות, גם הזכות לפרטיות אינה מוחלטת ובהחלט יתכנו נסיבות בהן אינטרסים אחרים יצדיקו פגיעה מסוימת בזכות לפרטיות. תפיסה זו מוסדרת, בין היתר, במסגרת ההגנות הקבועות בסעיף 18 לחוק הגנת הפרטיות. עם זאת, פגיעה שכזו צריכה להיעשות בהתאם לתכלית הוראות הדין ולעמוד בדרישת המידתיות.

מבוא

כחלק מהצורך למגר את התפשטות מגפת הקורונה, ישראל ומדינות רבות נוספות ברחבי העולם עושות שימוש באמצעים לניטור דיגיטלי. השימוש העיקרי באמצעים לניטור דיגיטלי נועד לאיתור אנשים אשר שהו בקרבת חולה קורונה, לצורך קטיעת שרשרת ההדבקה, וזאת בשל מאפייניה הייחודיים של המחלה. לפי מאפיינים אלה רבים מהחולים נושאים את הנגיף מבלי לגלות תסמינים כלשהם ולעיתים אלה מתגלים רק מספר ימים לאחר ההדבקות בנגיף.² מדובר בנשאים שטרם אובחנו, אשר מפיצים את הנגיף בסביבתם ולכן מדינות רבות מבקשות לבודד לא רק את מי שאומתו כחולי קורונה או נשאים של הנגיף, אלא גם את מי ששהו בקרבתם.

² שימושים באמצעי ניטור דיגיטלי ברחבי העולם נעשים ככלל לצורך קבלת נתונים אגרטיביים בדבר התפשטות המחלה, ולצורך אכיפת חובת בידוד. אמצעי ניטור לצורך אכיפת בידוד אינם מקובלים ברובן המכריע של הדמוקרטיות המערביות, כפי שעולה מהסקירה הבינלאומית הרצי"ב למסמך זה, ולכן המסמך עוסק באיתור קרבה לחולה קורונה.





איתור קרבה ונתוני מיקום³ מעוררים חששות כבדים לפגיעה בפרטיות הציבור, וביכולתו של אדם להתנהל במרחב הציבורי באופן אנונימי ובלתי מזוהה. מצב זה עלול להביא ליצירת תחושה של מעקב תמידי אחר מיקומו של היחיד במרחב הציבורי, ומכאן התפתחו טכניקות שונות המאפשרות לאתר קרבה לחולה קורונה גם מבלי לאסוף נתוני מיקום.

התשתית הטכנולוגית

1. נתוני מיקום והסכנה לפרטיות

1.1. נתוני מיקום מתייחסים לאזור בו שהה אדם ולמועד בו הוא שהה באותו אזור. שני המקורות העיקריים לאיסוף נתוני מיקום הם רשתות טלקומוניקציה המופעלות לפי דיני התקשורת המקומיים, וספקי שירותים שונים המוצעים (בדרך כלל במסגרת של יישומונים) על גבי רשתות תקשורת (דוגמת יישומוני ניווט, תחבורה חכמה, פעילות גופנית וכיו"ב). הנתונים נאספים במקרה הראשון על ידי בעלי רישיונות התקשורת, ובמקרה השני באמצעות יכולות המיקום המותקנות על המכשיר הנייד, הכוללות GPS, גישה לנתוני Wi-Fi ועוד, ונשמרות ומעובדות על ידי מערכת ההפעלה או היישומן הספציפי.

1.2. גם כאשר נתוני מיקום נאספים או מועברים בתצורה אנונימית, ישנם מקרים בהם ניתן לבצע הליך של זיהוי מחדש לנתונים שעברו תהליך אנונימיזציה (דה-אנונימיזציה). מכיוון שהמידע ה"אנונימי" כבר הועבר לידיים חיצוניות, ברגע שהמידע אשר זוהה מחדש - נחשף, לא ניתן להחזיר את הגלגל לאחור, ומידע אישי ורגיש חשוף לכל המבקש לנצלו לרעה. ככל שהזמן חולף טכנולוגיות המידע משתפרות, ומקורות מידע רבים נעשים פומביים, דבר המגביר את הסיכון של הצלבת המידע הגלוי עם המידע ה"אנונימי" באופן שיגרום לחשיפת המידע וזיהוי מחדש של המשתמש.

1.3. גם במקרה בו נתוני מיקום יהיו אנונימיים לחלוטין, ולא יהיו מקושרים לכל פרט אשר יאפשר זיהויו של אדם, הצלבתם עם מידע זמין אחר עלולה לגרום לזיהוי. כך למשל -

- הצלבת קואורדינטות של מכשיר נייד⁴ עם מספר ה-MSIN⁵, מספר ה-IMEI⁶ או מספר ה-MAC⁷ המצויים בידי ספק השירות, עשויה לגלות מי הוא בעליו והיכן היה;
- הצלבת כתובת IP המשמשת לגישה לאינטרנט עם חשבון האינטרנט של המשתמש, מגלה מי הוא בעליו והיכן שהה; הצלבת צילומי תנועת מכוניות עם מספר רישוי רכב מגלה נתוני מיקום של נהג הרכב, שהוא לעתים קרובות גם בעליו;

³ נתוני מיקום ואיכון דרך חברות הסלולר יאפשרו למשרד הבריאות לקבל מידע אישי מזהה אודות חולה מאומת או כל מי שנתוני המיקום של מכשיר הסלולר שלו יעידו ששהה במרחק מסוים מחולה הקורונה

⁴ רשתות סלולריות מחולקות לתאים, ובכל תא ממוקמת אנטנה. כאשר משתמש נקלט בתא מסוים, הרשת מכירה את המיקום ויודעת באיזה מרחק מהאנטנה נמצא המשתמש.

⁵ Mobile Subscriber Identification Number

⁶ מספר מזהה של המכשיר הסלולרי.

⁷ מזהה ייחודי המוטבע על רכיבי תקשורת נתונים (כגון כרטיס רשת או ראטר).





- הצלבת נתוני מיקום עם מידע המצוי ברשתות חברתיות, מצלמות אבטחה במרחב הציבורי, רישומי PNR, עסקאות אשראי וכיו"ב, עלולים גם הם לגרום לזיהוי פרטיו של אדם.

1.4. מחקרים מראים כי מעקב במשך שנה וחצי אחר נתוני מיקום אנונימיים של חצי מיליון איש, מעלה כי לרובם יש שובל ייחודי, המאפשר לזהות 95% מהם.⁸

1.5. שימוש בשירותי GPS, רשתות Wi-Fi ו-Bluetooth מייצר שובל דיגיטלי של נתוני מיקום, אשר מגלים מידע רגיש על חייו והרגליו של אדם, זאת הרבה מעבר למיקומים בהם שהה. כך למשל –

- מצבו הבריאותי והנפשי של אדם (כגון אדם המבקר במוסדות רפואיים);
- אמונותיו (ביקור בבית כנסת, מסגד או כנסייה, או העדר תנועה ושימוש בימי שבת);
- דעותיו הפוליטיות (ביקור במוסדות מפלגתיים או השתתפות בהפגנות);
- נטייתו המינית (ביקור במקומות בילוי ייעודיים לקהילה מסוימת);
- מצבו הכלכלי (אזור מגורים, מקום עבודה ומקומות בילוי עשויים כולם ללמד על מצב סוציו-אקונומי);
- קשריו החברתיים או המקצועיים, ומצב תעסוקתו (מקום הימצאו במהלך יום העבודה);
- מצבו האישי של אדם (כגון מקום לינה השונה מכתובת מגוריו).

1.6. נתוני מיקום הינם בסיס לשירותים מסחריים רבים (נתוני מיקום מאפשרים יצירת פרופילים המאפשרים הצעת שירותים ומוצרים באופן ממוקד ולחלופין במועד ההגעה למיקום מסוים), ולכן יש להם ביקוש רב בקרב סוחרים מידע וגורמים מסחריים למטרות כלכליות ואחרות. הביקוש הגובר לנתוני מיקום מייצר תמריץ לשימושים שלא כדין במידע (למשל, מכירת המידע לסוחרים מידע), הן ע"י מי שמורשים לגשת למאגר (עובדי הארגון המנהל או המחזיק במאגר) והן ע"י פורץ חיצוני, זאת באמצעות ניצול המידע לצרכי סחיטה, התנכלות, אפליה תעסוקתית, ביטוחית ועוד.

2. נתוני קירבה והסכנה לפרטיות

2.1. נתוני קרבה יכולים להיאסף במגוון של טכנולוגיות. קיימים אמצעים לאיתור נתוני קרבה האוספים ומצליבים נתוני מיקום (נתונים על תנועה של אדם, הנאספים ע"י חברות תקשורת או ספקי שירותים האוספים נתוני GPS, ניתוח צילומי וידאו וכיו"ב). בנוסף קיימים אמצעים טכנולוגיים אשר אוספים נתוני קירבה בלבד (קרי, מידע על העובדה שאנשים היו במרחק מסוים זה מזה), זאת מבלי לאסוף בהכרח מידע על המקום שבו ארעה האינטראקציה. כך למשל, לצורך איתור המקרים בהם חולה קורונה שהה במרחק מסוים לפרק זמן מסוים ליד אדם אחר, לא נדרש לדעת היכן בדיוק ארע המפגש ביניהם.

Scientific Reports, 3 article 1376 (2013), Unique in the Crowd: The Privacy Bounds of Human Mobility,⁸ <https://www.nature.com/articles/srep01376>



2.2. איתור באמצעות נתוני קירבה מתבסס בדרך כלל על אותות המועברים ב- Bluetooth בין משתמשים אשר הורידו יישומון רלוונטי למכשיר הנייד, ונמצאים בקרבה מספקת זה לזה. טכנולוגיה זו מכונה Bluetooth Low Energy (BLE).

2.3. קביעת קירבה בשיטת Bluetooth נעשית בדרך כלל באופן הבא: כל משתמש ביישומון הייעודי מקבל מספר רנדומלי אנונימי הנשמר במכשיר הטלפון הנייד שלו – טוקן. טוקן זה יכול שיתחלף בפרקי זמן קבועים ותדירים, מטעמי אבטחת מידע ושמירת פרטיו המזיהים של המשתמש. כאשר משתמשים נמצאים בקרבה מספקת מבחינה טכנולוגית, מכשירי הטלפון יוצרים קשר (Hand Shake) ומחליפים ביניהם את הטוקנים במקרה שעוצמת האות ומשך המפגש עומדים בקריטריונים המוגדרים במסגרת השירות (בדרך כלל על פי פרמטרים של זמן ומרחק מינימליים). כל מכשיר נייד שומר את הטוקן של המשתמש השני ובצמוד לו חתימת זמן המציינת את מועד המפגש.

לדוגמא: משתמש א' פוגש את משתמש ב' והמכשירים מתקשרים בינם לבין עצמם. אם פרטי המפגש עומדים בפרמטרים שהוגדרו במערכת (לדוגמא עד 2 מטר ומעל 15 דקות), היישומון של משתמש א' שומר את פרטי הטוקן של משתמש ב' בצמוד לחתימת הזמן, ולהיפך.

2.4. יצויין כי בהיבט הטכנולוגי, טכנולוגיה המבוססת על נתוני קירבה, מסוגלת לזהות את המרחק ממכשיר שכן בדיוק של סנטימטרים, ועל כן הינה מדויקת יותר ועדיפה בהרבה על נתוני מיקום שמקורם ב-GPS שעל המכשיר, המאפשר דיוק של מטרים בודדים, ואלה בתורם מדויקים יותר ועדיפים על איסוף נתוני מיקום מספקיות התקשורת, אשר באזורים בהם הכיסוי הינו חלקי יכול להגיע ל"דיוק" של מאות מטרים. רמת הרזולוציה שנתוני הקירבה מספקים היא גבוהה הרבה יותר מזו של נתוני מיקום מבוססי GPS ועוד יותר מזו של נתוני מיקום מבוססי ספקיות תקשורת. זאת משום שהפקת נתוני מיקום GPS תלויה בקישור ללוויינים ורשתות אלחוטיות וסלולריות, ונתוני מיקום ספקיות התקשורת תלויה בהצלבה טריאנגולרית שבין תאים סלולריים, אשר אינם מספקים נתונים במידת הדיוק הנדרשת לצורך קביעה כי אנשים שהו בקרבה זה לזה (אשר על פי הגדרות משרד הבריאות נדרשת קרבה של עד 2 מטר למשך 15 דקות), דבר המביא בפועל לרמה גבוהה של איתור שגוי (False positives) הגורם להכנסתם של אנשים לבידוד ולפגיעה חמורה בחופש התנועה שלהם, אף שהם לא נדרשים בפועל לכך. עוד יצויין כי טכנולוגיות לקביעת נתוני מיקום להבדיל מאלו של נתוני קירבה, אינן פועלות כנדרש במקומות סגורים ואינן מסוגלות להבחין באנשים הנמצאים בחללים בקומות נפרדות או במיקומים משתנים (כגון קרון רכבת נע).

2.5. בשל העובדה שנתוני מיקום מגלים מידע על תנועתו של אדם במרחב באופן שוטף, להבדיל מנתוני קירבה אשר רק מציינים כי אנשים שהו במרחק מסוים זה מזה ברמת דיוק גבוהה יותר, השיטה האחרונה עדיפה משמעותית בהיבט של שמירה על פרטיות המשתמשים.



3. המודל הריכוזי אל מול המודל הביזורי

השימוש בנתוני מיקום וקירבה לצורך זיהוי המגעים וקטיעת שרשראות ההדבקה נעשה על בסיס שני מודלים עיקריים;

3.1 **המודל הריכוזי** מתבסס על כך שכל משתמש במערכת מקבל מספר מזהה רנדומלי משרת מרכזי (לדוגמה של משרד הבריאות). כאשר משתמש מאובחן כחולה קורונה, הוא יישאל במסגרת החקירה האפידמיולוגית האם הוא משתמש ביישומון, וככל שהתשובה חיובית ותינתן הסכמתו להעברת המידע, היישומון/המכשיר יעביר לשרת מרכזי את היסטוריית האינטראקציות שלו אשר תכלול את פרטי כל המספרים המזהים עימם נפגש למשך התקופה הרלוונטית שקדמה למועד האבחון, באופן שהמשתמשים אשר היו בקרבתו יקבלו על כך הודעה.

בנוסף, יצוין כי על מנת שהמודל הריכוזי יוכל לנתח את המידע המועבר כהלכה, נדרש כי כל האינטראקציות של כל המשתמשים יועברו באופן גולמי לשרת המרכזי. ריבוי המידע מכלל המשתמשים במערכת מאפשר ללמוד על אינטראקציות בין ישויות גם ללא זיהויים, ועל הקשרים החברתיים בין משתמשים שונים, על אף היותם אנונימיים. שימוש בטכנולוגיות ביג דאטה מאפשרות אם כן ביצוע זיהוי חוזר של מידע אנונימי.

3.2 **במודל המבוזר** לעומת זאת, המספר המזהה הרנדומלי מונפק ע"י מכשיר הטלפון הנייד של המשתמש. כאשר משתמש אובחן כחולה, תישלח הודעה לשרת הכוללת את המספר האנונימי שלו (ומכיוון שבד"כ מספר זה מתחלף כל פרק זמן לצרכי אבטחה, יועלו כל המספרים המזהים של המשתמש וחתומות הזמן בהם השתנו). מידע זה יועבר לכלל המשתמשים האחרים במסגרת העדכון הקבוע שעורך היישומון. אם נמצא אצל משתמש אחר מידע אודות מפגש עם חולה שהיה בקרבה מספקת אליו, נוצרת הצלבה והוא יקבל על כך הודעה מהיישומון עצמו, כך שהמערכת המרכזית בשלב זה לא מיודעת על קיומו של מפגש כאמור.

יובהר כי במודל המבוזר, המידע המועלה למערכת אינו כולל כלל את פרטיהם של משתמשים אחרים, אלא רק את הטוקנים המשתנים וחתומות הזמן של המשתמש עצמו אשר נתגלה כחולה מאומת, ומידע זה כלל אינו מעובד במערכת המרכזית.

מכיוון שבמודל המבוזר רוב הפעולות מתבצעות במכשיר הטלפון הנייד של המשתמש ולא בשרת מרכזי (הקצאת המספרים הרנדומליים, מיקום הקביעה כי היתה אינטראקציה, וקביעה של היקף המידע המועבר למערכת המרכזית) וכי נדרשת הסכמתו לכל שימוש והעברה של המידע - **הרי שפרטיותו של נושא המידע מוגנת טוב יותר בהשוואה למודל הריכוזי**. היות והמידע האישי לא מועבר למערכת מרכזית, סיכוני האבטחה בגישה לא מורשית למידע זה או בדלף מידע, קטנים הרבה יותר.



מדרג אמצעים לאיתור מגעים בראי הפרטיות

פגיעה בפרטיות אשר הינה זכות יסוד, ועל אחת כמה וכמה פגיעה הנעשית על ידי המדינה, צריך שתיעשה לתכלית ראויה ובאופן מידתי. על כן, הכלל הוא כי יש לבחור באמצעי אשר מגשים את התכלית ואשר פגיעתו בפרטיות היא הפחותה ביותר.

כפועל יוצא מכך, כשמחליטה הממשלה כי מצב התחלואה במגפת הקורונה מצריך שימוש באמצעי ניטור דיגיטלי אשר יסייע בהשגת מטרת קטיעת שרשראות ההדבקה, יש לבחור באמצעי לניטור דיגיטלי שיגשים תכלית זו באופן שפוגע בפרטיות הציבור במידה הפחותה ביותר, ולהשתמש בו באופן ובתנאים שיפגעו גם הם בפרטיות במידה הפחותה.

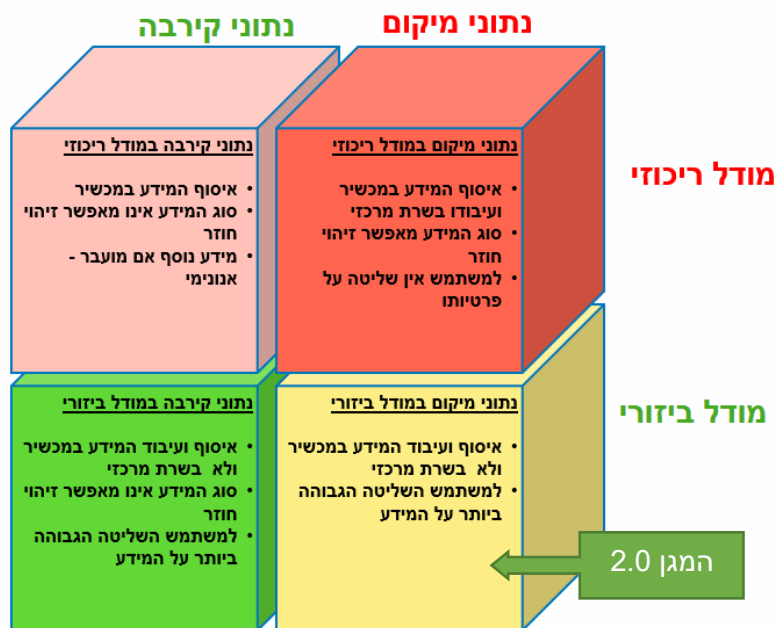
להלן מדרג מודלים לקטיעת שרשרת ההדבקה המוצגים בסדר יורד בראי הפרטיות. קרי, מהאמצעי המעניק למשתמש את ההגנה על הפרטיות ברמה הגבוהה ביותר ועד לאמצעי המספק הגנה על הפרטיות ברמה הנמוכה ביותר:

- 1. יישומון לאיתור מגעים, בהתבסס על נתוני קירבה (ללא נתוני מיקום) במודל ביזורי, בהסכמת המשתמשים - מודל זה מקנה את ההגנה הגבוהה ביותר לפרטיות, מבין המודלים לעיל, משום שהיקף איסוף המידע ועיבודו בשרת מרכזי הוא הקטן ביותר, והסכנה לפרטיות הנגרמת מסוג המידע שנאסף (נתוני קירבה), לרבות סכנה לזיהוי חוזר, היא הנמוכה ביותר. בנוסף, במודל זה בידי המשתמש השליטה הגבוהה ביותר במידע בהשוואה למודלים האחרים הקיימים היום.**
- 2. יישומון לאיתור מגעים וחקירה אפידמיולוגית, בהתבסס על נתוני קירבה ונתוני מיקום במודל ביזורי, בהסכמת המשתמשים - על אף שמודל זה אוסף גם את נתיב המיקומים של המשתמש מה-GPS של המכשיר, הוא עדיין מקנה הגנה גבוהה לפרטיות המשתמש, משום שאיסוף המידע ועיבודו נעשה על גבי מכשיר הטלפון, וכל העברת מידע לשרת מרכזי נעשית בהסכמת המשתמש.**
- 3. יישומון לאיתור מגעים בהתבסס על נתוני קירבה (ולא נתוני מיקום) במודל ריכוזי - מודל זה עדיין מקנה הגנה לפרטיות, כאשר אינו משולב עם שירותים נוספים. זאת משום שאין איסוף של נתוני מיקום אלא איסוף של נתוני קירבה בלבד. ככל שבמערכת מסוג זה משולבים שירותים נוספים, וככל שהרישום למערכת נעשה באמצעות מסירת מזהה חד ערכי (כדוגמת מספר טלפון, מספר ציוד קצה וכיו"ב), יש להפריד בין המידע המזהה ובין נתוני המיקום, ויש להקפיד על שימוש במנגנוני אנונימיזציה והרשאות גישה למערכת.**
- 4. יישומון לאיתור מגעים בהתבסס על נתוני קירבה (ולא נתוני מיקום), במודל מבוזר או ריכוזי (בהתאמה), בכפייה או בהתניית כניסה למקום (לדוגמה התניית כניסה למקומות עבודה, תחבורה ציבורית וכיו"ב בהורדת היישומון) - במודל זה למשתמש שליטה חלקית על המידע שלו, אולם בשל סוג המידע שנאסף, המודל מאפשר הגנה מסוימת על פרטיותו של המשתמש. ככל שנעשה שימוש במודל זה, ראוי כי השירות לא יהיה כרוך באיסוף מידע נוסף, מעבר לנתוני קירבה.**

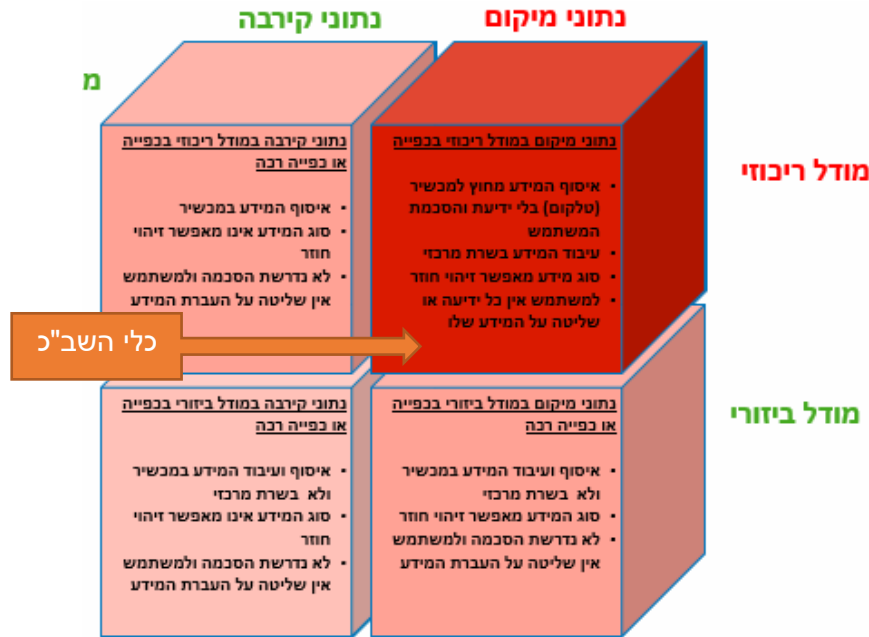
5. יישומון לאיתור קרבה וחקירה אפידמיולוגית בהתבסס על נתוני מיקום בהתניית כניסה למקום (לדוגמה התניית כניסה למקומות עבודה, תחבורה ציבורית וכיו"ב בהורדת היישומון) - לעמדתנו מודל זה גורם לפגיעה קשה בפרטיות הן מבחינת סוג המידע שנאסף והן מבחינת השליטה החלקית בלבד שיש למשתמש על המידע שלו (מודל מסוג זה אומץ ע"י ממשלת הודו).

6. איסוף נתוני מיקום ישירות מחברות טלפון על ידי רשויות המדינה ללא ידיעה או הסכמה של האזרחים - מודל זה גורם לפגיעה המשמעותית ביותר בפרטיות ובאמון הציבור. שימוש באמצעי ניטור מסוג זה גורם לאזרחים לתחושה שהם נתונים למעקב מתמיד מצד המדינה. היקף הפגיעה בפרטיות יושפע, בין השאר, גם מזהות הגורם הממשלתי שמנהל את המידע (גורם ממשלתי ייעודי לתחום בריאות הציבור או רשות בעלת סמכויות אחרות וטיבן) וכן ממתכונת היידוע, המחיקה, ניהול והעברת המידע.

מדרג האמצעים לאיתור מגעים – בהסכמה



מדרג האמצעים לאיתור מגעים – בכפייה



אמצעים לניטור דיגיטלי

הבסיס למנגנון אשר יאפשר קטיעתן של שרשראות הדבקה וכן יאפשר את פעילותו התקינה של המשק, תוך קיום "סגרת קורונה", מושתתת על ביצוען של חקירות אפידמיולוגיות לחולים מאומתים על ידי משרד הבריאות, תוך ניתוח אופן הידבקותם והגורמים עימם באו במגע.

האמצעים הטכנולוגיים נועדו לסייע ולתמוך בהליך חקירה זה, והינם רק מקטע אחד בשרשרת הפעולות הנדרשות לשם קטיעת שרשראות ההדבקה ;

1. **אמצעים מבוססי איכון** – דורשים את קיומו של מכשיר טלפון בחזקתו של האדם – דבר המגביל את יכולת הזיהוי באוכלוסיות כגון ילדים מתחת לגיל מסוים, אשר אינם נושאים עימם מכשיר סלולרי. אמצעים אלה מוגבלים בדיוק רזולוציית המיקום, וביכולת להפריד בין מגעים אשר נחזים כקרובים מבחינת שיטת הטריאנגולציה של רשת התקשורת, אך בפועל אינם עומדים בדרישות הקרבה, כגון בשל קיומם של פערים אנכיים (קומות אחרות בבניין), מקומות סגורים ומקומות ללא קליטה מלאה.

2. **אמצעים מבוססי נתוני מיקום וקירבה על בסיס יישומון** – דורשים את קיומו של מכשיר טלפון חכם ואת היכולת הטכנולוגית והאוריינות הנדרשת בהתקנת היישומון והשימוש בהם. דוגמאות למגבלות אפשר למצוא במגזרים מסוימים אשר אינם נושאים מכשיר נייד (טלפונים כשרים במגזר החרדי), בקבוצות גיל מסוימות (התקנת יישומון אצל קשישים, או ילדים קטנים נטולי מכשיר נייד) ובמגזרים המתנגדים להתקנתו של יישומון ממלכתי.



3. שימוש בתשתית Apple – Google לאיתור מגעים

- 3.1 Google ו-Apple (להלן – "החברות") פיתחו ממשק (API) אשר נועד לאפשר תאימות בין שתי הפלטפורמות במטרה לסייע לרשויות הבריאות ברחבי העולם להפעיל יישומונים לאיתור מגעים בטכנולוגיית BLE במודל המבוזר.
- 3.2 בחודש מאי 2020 פרסמו החברות את תנאי השימוש לשירות, בהם הן מתנות את השימוש בשירות בכך שהשירות יינתן רק לרשויות ממשלתיות רשמיות במטרה להתמודד עם משבר הקורונה אשר יקבלו את מדיניות הפרטיות. כל זאת בכפוף לקבלת הסכמת המשתמשים להורדת הממשק, קבלת הסכמת משתמשים שאובחנו כחולים להעביר דרך הממשק הודעה על דבר מחלתם, היעדר גישה לנתוני מיקום של משתמשים, והימנעות מאיסוף פרטים מזהים, לרבות מספרי טלפון.
- 3.3 כפי שנמסר ממשרד הבריאות, בין הסיבות בשלן הוחלט כי שירות זה לא ישמש תשתית ליישומון "המגן", היו תנאי השירות שקבעו כי לחברות עומדת האפשרות לקבוע את מועד התפוגה של השירות (עם סיום המשבר), ואף שהדבר יעשה בתיאום עם כל רשות מדינתית – ההחלטה הסופית נותרת בידי החברות. כמו כן דורש השירות כי היישומון העושה בו שימוש לא יפעל לאיסוף נתוני מיקום – ועל כן לא יהווה חלק מתהליך החקירה האפידמיולוגית של רשויות הבריאות בכל מדינה.

עידוד התקנת היישומון ונשיאת המכשיר

הקמתה של תשתית מינימלית אשר תאפשר זיהוי מגעים ותסייע בהליך החקירה האפידמיולוגית, מחייבת תפוצה מספקת של היישומון באוכלוסייה. זאת משום שקיומו של יישומון פעיל רק אצל אחד מהצדדים במפגש בין חולה מאומת לבין מגע, לא יאפשר את זיהוי המפגש, וכתוצאה מכך לא תישלח הודעה לאותו מגע לאחר זיהויו של החולה המאומת.

על כן, ובמטרה לעודד התקנה של היישומון בחלקים נרחבים מהאוכלוסייה, נדרשת היערכות הסברתית נרחבת בכל הנוגע לחשיבות התקנת היישומון והפעלתו, וכן התייחסות להיבטי ההגנה על הפרטיות והשקיפות, אשר מהווים נדבך משמעותי בהעלאת אמון הציבור בה ובחשיבות התקנתה.

1. **הסכמה** – בסיס וולונטרי להורדת היישומון, להתקנתו, להפעלתו וכן הסכמה להעלאת מידע לשרתי המערכת במקרה בו הפך המשתמש לחולה מאומת.
2. **פעילות הסברה ציבורית** – קמפיין נרחב בערוצים השונים לשם העלאת המודעות לשימוש באמצעי החליפי כמפתח לחזרה לשגרה, שקיפות ומתן דגש לחשיבות שניתנה לפרטיות המשתמשים בעיצוב הפתרון. דרך מהירה לקידום נרחב של ההתקנה הינה קריאת גורמי ממשל בכירים לציבור להתקין היישומון.
3. **פעילות הסברה מגזרית** – שיתוף פעולה עם מעצבי דעת הקהל במגזרים ספציפיים, ולדוגמה פנייה לגורמים מוכרים ואמינים, כגון פוסקי הלכה לשם בחינת האמצעי שיתאים לקהל הרלוונטי, וקידום קמפיין בשפה ובתרבות המתאימה למגזרים השונים.





4. **סקיפות ויצירת אמון במערכת** – פרסום של כל האמצעים אשר נועדו לשמור על פרטיותם של המשתמשים, על ידי קביעת מנגנונים וולונטריים בהורדה, בהתקנה, בהפעלה הקבועה של היישומון ובנשיאת המכשיר בכל עת. בתהליך זה יש להדגיש את העובדה שבמודל הביזורי עיבוד המידע מתבצע במכשיר ואינו כולל כל העברת מידע לשרת מרכזי של משרד הבריאות או לכל גורם אחר. התייחסות לנושא צריכת החשמל ועידוד אי-כיבוי של מנגנון ה-BLE/GPS אשר מאפשר את זיהוי המגעים, בשימוש בקוד פתוח – וקבלת ופרסום תוצאות הבדיקות של המערכת על ידי גורמים בלתי תלויים. כן יש לשקף כי היישומון לא חף מקשיים ושיפורים נוספים יוטמעו בהמשך.

אמצעים משלימים להרחבת הכיסוי

לכל אמצעי טכנולוגי אשר יופעל על ידי הממשלה במאבק בקורונה ישנן מגבלות המונעות איתור מושלם של כלל המגעים (False Negative) וכאלה המזהים חשודים במגע אף שבפועל לא נחשפו לחולה מאומת (False Positive). על כן, ישנה האפשרות כי ידרשו אמצעים משלימים לזיהוי גורמים אשר אינם נושאים טלפונים ניידים.

הרשות בוחנת בימים אלו מספר אפשרויות שעלו לדיון בדיוני צוות החלופות שמוביל המל"ל. יודגש כי לגבי כל אחד מהאמצעים המשלימים יש לבצע בחינה של מידת הפגיעה בפרטיות, הן מבחינת טכנולוגיית האמצעי (כרטיס חכם, קורא QR וכו'), הן מבחינת הגישה של אמצעי זה למאגרים חיצוניים (כגון ניתוח מצלמות במרחב הציבורי לזיהוי פנים או ניטור פעילות בכרטיס אשראי, שהינם בעלי פוטנציאל כבד לפגיעה בפרטיות וליצירת אפקט של תחושת מעקב מתמדת), הן מבחינת האופן בו יידרש הציבור לעשות בו שימוש (בכפייה/הסכמה) והן מבחינת המצבים בהם יופעל וייאכף (חזרה מחו"ל, כניסה לאיזור הומה אדם, כניסה/יציאה מאיזור בסגר וכו'). הרשות להגנת הפרטיות תעביר חוות דעתה בנושא זה לצוות השרים ככל שתקודם ותישקל הטמעת אמצעים אלו.

התממשקות לסטנדרט בינלאומי

קיימת חשיבות לכך שכל פתרון יתייחס לאפשרות ההתממשקות לסטנדרט הבינלאומי אשר פותח באירופה (אינטראופרביליות), אשר יאפשר לתיירים ומבקרים מחו"ל, כמו גם לישראלים הנוסעים לנסיעות עסקים או לטיול בחו"ל, לשמור על רצף אפידמיולוגי ולחזור לארץ. נדרש במקביל גם לפתח שיתוף פעולה עם גופי בריאות בחו"ל לשם השלמת החקירה האפידמיולוגית, כאשר זהו מגעים בחו"ל או עם זרים אשר עושים שימוש ביישומון "זר".

מבחינה זו, התממשקות עתידית של המגן לאפליקציות בעלות תאימות עולמית הינה בעלת יתרון משמעותי, ויש לשקול הטמעתה בעתיד.





עיצוב לפרטיות בשמירה על המידע

הפעלתם של אמצעים טכנולוגיים לקטיעת שרשרת ההדבקה, כוללים ניטור של פעולות האזרחים, שמירת מידע והעברות מידע מרובות בין היישומונים וכן למערכת המרכזית. כל מערכת הכוללת אספקטים של מידע רגיש, נדרשת לעמוד בדרישות החוק, קל וחומר כשמדובר במידע רגיש ביותר ועוד לפני שהושלמו כל הבדיקות לפעילותה התקינה של המערכת.

כדי למנוע דלפים ופגיעה בפרטיות המשתמשים, נדרש לבצע מראש עיצוב לפרטיות (Privacy by Design) לכלל האספקטים של המערכת, וכן פיתוח ותיקוף נוהל ומערכת הרשאות לאיסוף המידע ולהעברתו בין המערכות והגופים השונים לשם יידוע מגעים, למערכות האבטחה והבקרה.

להלן מפורטים האלמנטים העיקריים שיש לוודא עמידתם בכללי העיצוב לפרטיות.

1. ווידוא חיוניות שדות המידע שנאספים על ידי המערכת

- א. פרטי זיהוי של המכשיר ושל המשתמש.
- ב. מידע שנמסר באופן וולונטרי על ידי המשתמש בעת ההתקנה.
- ג. נתוני שימוש ביישומון ובשירותים הנדרשים להפעלתו.
- ד. נתוני מיקום - היקף האיסוף ורזולוציית המיקום.
- ה. נתוני קירבה - היקף המידע המועבר בעת יצירת מגע (Hand Shake) – טוקן רנדומלי מתחלף ללא פרטי זיהוי של המגע.
- ו. כל כמה זמן מתבצע רישום ללוג.
- ז. נתונים נוספים שנשמרים.

2. מחיקת מידע

- א. מחיקה של כל מידע שנאגר במכשיר ובמערכת המרכזית עם הפיכתו ללא רלבנטי (לדוגמה נתוני מיקום וקרבה לאחר 14 או 10 ימים).
- ב. מחיקת המידע מהמכשיר בעת הסרת היישומון.
- ג. מנגנון יציאה מהשירות (Opt out) או השהייה זמנית – אשר יאפשר למשתמש לעבור למצב לא מנטר של המערכת.

3. העברת המידע מהמכשיר למערכת המרכזית

- א. וולונטריות והסכמת המשתמש להעלאת המידע רק במקרה בו זוהה כחולה מאומת.
- ב. אופן העלאת המידע – הצפנת המידע ופתיחתו במערכת המרכזית, המעבר דרך שרתים ועננים בארץ ובחו"ל.
- ג. היקף המידע המועבר. למשל, מידע הכולל נתוני מיקום יעביר מיקומים וזמנים בלבד. מידע הכולל נתוני קירבה יעביר את רשימת המפתחות המשתנים ו-Time stamp של המשתמש בלבד ולא של המגעים שלו.
- ד. יש לשים דגש על כך שהיישומון לא יעדכן את המערכת המרכזית במקרה בו זוהה מגע על ידי המערכת, אלא יעדכן רק את המשתמש על כך ויידע אותו בדבר חובתו להיכנס לבידוד, אפשרויות הערעור העומדות בפניו, וחובתו לדווח למשרד הבריאות (באמצעי אחר וחיצוני ליישומון) על כניסתו לבידוד.





דיווח אוטומטי של המערכת למשרד הבריאות – ללא קבלת הסכמתו או ללא ידיעתו של המשתמש – תהווה משבר אמון של המשתמשים במערכת, ותפגע אנושות ביכולת להטמיע את היישומון בחלקים נרחבים באוכלוסייה.

דגשים לפרטיות במאגרי משרד הבריאות

1. **תשתית המאגר** – הטכנולוגיה בה מאוחסן המידע, המערכת בה מנוהל, מיקום פיזי של המידע;
2. **הרשאות הגישה** - למשתמשים (לאיזה צרכים ובאיזה היקפים) ולשירותים השונים בהם עושה המערכת שימוש, אופן קבלת והכשרת כוח האדם בעל ההרשאות לגישה למידע;
3. **טיוב המידע** – במסגרת החקירה האפידמיולוגית אל מול נושא המידע – רק ביחס לנתוני המיקום - מחיקת נקודות פרטיות (כגון בית מגורים), זיהוי טעויות, הגדלת רזולוציה (מיקום במבנה, לעומת מיקום בקומה 8 במבנה), אגרגציה של נתונים וכד'.
4. **השימוש במידע רק על ידי בעלי הרשאה ובמסגרת הסמכות** –
- **צרכי החקירה האפידמיולוגית**
- **פרסום נתוני החקירה האפידמיולוגית** – כגון אתר המשרד.
- **העברת המידע הרלוונטי למשתמשי היישומון** – לשם עיבוד וזיהוי מגעים באופן מקומי על גבי המכשיר.
- **אנונימיזציה של הנתונים לצורך ניתוח סטטיסטי וקביעת מדיניות** – כגון זיהוי של אזורים אדומים, זיהוי מגמות בדבר אופן ההדבקות.
5. **העברת מידע מהמערכת לצדדים שלישיים** - כגון ספקים חיצוניים (לצרכי משלוח הודעות) ופנימיים (לצורך Call center) גופי ממשלה, דוחות מנהלים וכד' ;
6. **העברת מידע מהמערכת למגעים** – עדכון שעתו של תוצר החקירה האפידמיולוגית למכשירים עליהם מותקן היישומון – לצורך עיבוד מקומי על גבי המכשיר, הצלבת נתונים וזיהוי ועדכון המשתמש בדבר קיום מגע עם חולה מאומת. העברת מידע לצרכי בירור וערעור על החלטת בידוד וכד' ;
7. **מנגנוני הבקרה והתיעוד** ;
8. **אבטחת המידע** – מערכות, כלים ובקורות מפצות לשם השמירה על אבטחת המידע ביישומון ובמערכת המרכזית, מנגנוני הצפנה וזיהוי המשתמש, מבחני חוסן מחמירים של הקוד, הפלטפורמה והתשתיות וכד'.

עמדת הרשות להגנת הפרטיות

הרשות ערכה פגישות ובדיקות מקיפות לבחינת האמצעים השונים אשר עומדים כיום בפני הממשלה לצורך הגשמת התכלית של קטיעת שרשראות ההדבקה של מחלת הקורונה, לרבות הפתרון מבוסס כלי השב"כ, אפליקציית המגן (בגרסת המגן 2.0 הכוללת נתוני מיקום וקרבה) ותשתיות נתוני קרבה המסופקות על ידי חברות Google ו-Apple.





על יסוד כלל המידע המונח בפניה נכון להיום, להלן עמדתה של הרשות להגנת הפרטיות:

1. יישומון המגן 2.0

הרשות ערכה פגישות עם צוות הפיתוח של משרד הבריאות, ועברה על מפרטי היישומון והעיצוב לפרטיותו, לבחינת פתרון יישומון המגן (בגרסה 2 הכוללת נתוני מיקום וקרבה) ויישומו להגשמת התכלית שהוגדרה ובראי של עיצוב לפרטיות ואבטחת המידע.

בהמשך למדרג שפורט לעיל ונכון למועד כתיבת חוות דעת זו, יישומון "המגן 2" מהווה פתרון ברמה 2 – שכן הוא כולל איסוף של נתוני מיקום ונתוני קירבה, ואף שהגרסה הנוכחית כוללת בעיות בהפעלת הרקע בנייד⁹ - נכון לעת הזו ובראי כלל החלופות האפשריות – הרשות להגנת הפרטיות סומכת את ידיה על פתרון זה, וקוראת לוועדת השרים לקדם את העלאתה של אפליקציית "המגן 2" בגרסתה המחודשת בהקדם האפשרי, לצד קידום קמפיין הסברתי ואינטנסיבי, אליו יש לגייס גם מקבלי החלטות, לשם הטמעתו באוכלוסייה בהיקף נרחב מהר ככל האפשר.

ככל שפתרון זה יתפוס פלח נרחב יותר ויותר מההצלחה באיתורם של מגעים ובקטיעתן של שרשראות ההדבקה, יהיה מקום לבחון גם את הכנסתם של אמצעים משלימים לתורת ההפעלה.

בעת אפיונו ופיתוחו של יישומון המגן אומצו עקרונות העיצוב לפרטיות (- Privacy By Design (PbD) בצורה המגנה באופן מיטבי על פרטיותם של המשתמשים בה –

א. **מערכת ביזורית** – כל המידע שנאסף ביישומון – הן נתוני המיקום והן נתוני הקירבה – נשמרים על גבי המכשיר, מעובדים על גבי המכשיר, ונמחקים במועד הפיכתם ללא רלוונטיים. היישומון והמכשיר אינם מדווחים כלל למשרד הבריאות או לכל גורם אחר על כל ממצא שנמצא במסגרתו (ובכלל זה גם על מציאתו של מגע עם חולה מאומת);

המקרה היחיד בו מופעל מודל ריכוזי ביישומון הוא כשהמשתמש עצמו מאובחן כחולה מאומת, אז – בהסכמתו בלבד וכחלק מתהליך החקירה האפידמיולוגית – מועלה המידע שנאגר ביישומון למערכת המרכזית של משרד הבריאות באופן הבא:

- **נתוני מיקום** – מטוייבים ביחד עם המשתמש לצורך יצירת נתיב אפידמיולוגי אשר יפורסם (אנונימית באתר המשרד ודרך האפליקציה) ואינם מגלים דבר על מי שהיה בקרבת המשתמש. הדבר ישמש לצורך קביעת מדיניות הממשלה על ידי ניתוח המידע באופן סטטיסטי ואגרטיבי – דבר שאיסוף נתוני קירבה בלבד לא יסייע בו (כגון לצורך זיהוי של אזורים בהם יש ריכוז גבוה של חולים, לצורך קבלת החלטות בנושא סגרים מקומיים והקצאת משאבים לבתי חולים לפי נתוני התחלואה).

- **נתוני קירבה** – לא מועלים כלל לשרת, אלא רק הטוקנים הרנדומליים שיצר היישומון למשתמש. אלה נשלחים ללא כל עיבוד לכל המשתמשים האחרים ביישומון, לשם עיבוד מקומי אצלם וקבלת חיווי מקומי אם שהו בקרבת המשתמש שזוהה כחולה קורונה - למשרד הבריאות אין כל מידע לגבי מגעים אלה.

⁹ בעיקר בטלפונים סיניים וכן ביחס לגרסאות היישומון המותקן על מערכת ההפעלה iOS אשר אינה משדרת נתוני קירבה





ב. **מערכת וולונטרית מבוססת הסכמה** – לכל פעולה ביישומון נדרשת הסכמה אקטיבית של המשתמש – להורדת היישומון ולהתקנתו על גבי המכשיר, למתן גישה ליישומון לתשתית המיקום והקירבה הקיימים במכשיר, להעלאת המידע שנאגר במכשיר לשרתי משרד הבריאות במסגרת של חקירה אפידמיולוגית (וואת רק במקרה בו החולה הינו מאומת, ורק במסגרת החקירה), ואף לדיווח על איתורו של מגע עם חולה מאומת (היישומון אינו מעדכן את משרד הבריאות או כל גורם אחר בדבר מגע כאמור – אלא רק מעדכן את המשתמש בדבר חובת הבידוד, ומפנה את המשתמש לטופס הדיווח על באתר משרד הבריאות).

ג. **מערכת מאובטחת ומעוצבת לפרטיות** – המידע שנאסף ונאגר ביישומון הינו המידע המינימלי שנדרש להגשמת תכלית היישומון, המידע שאינו רלוונטי נמחק ואינו נשמר, והסרת היישומון מוחקת את כל המידע שנאגר בה.

המערכת נכתבה בקוד פתוח, לוותה, אומצה ונבדקה על ידי מומחים וגורמים חיצוניים ובלתי תלויים, כמו גם על ידי גופים ממשלתיים.

כמובן, ייתכן שבהמשך ייתגלו בהפעלת המערכת באגים, פירצות אבטחה או בעיות פרטיות, אך אפיון המערכת, פיתוחה והפצתה מהווה תשתית מיטבית להגנה על פרטיותם של המשתמשים.

2. שימוש באמצעים משלימים להרחבת הכיסוי

הן כלי השב"כ והן השימוש ביישומון המגן או כל יישומון אחר, אינם כוללים כיסוי מלא של כלל האוכלוסייה, שכן יש פלחים בקרב האוכלוסייה אשר אינם עושים שימוש בטלפונים סלולריים או ממילא מתנגדים לשימוש ביישומון ממלכתי. לשם הגשמת קטיעת שרשרת ההדבקה גם בפלחים אלה, נבחנת כעת אפשרות הטמעת אמצעים משלימים על ידי משרד הבריאות, אך אלה טרם נבחנו על ידי הרשות באספקטים של עיצוב לפרטיות.

הרשות להגנת הפרטיות סבורה ביחס לאמצעים המשלימים, כי לפני הטמעתם במסגרת פתרון כולל, יש לבצע תסקיר מעמיק לניתוח השפעה על הפרטיות, וכן לשלב את הרשות במסגרת תהליך האיפיון והפיתוח של אמצעים אלה, שכן הם נושאים בחובם פגיעה משמעותית בפרטיות.

בשלב זה הרשות ממליצה שלא לשלב אמצעים משלימים אלה, שכן תהליך בחינתם טרם הושלם. הרשות סבורה כי נכון יהיה להכניס את יישומון "המגן 2" לשימוש מסיבי המלווה בהליך הסברה והטמעה לציבור, ורק לאחר ניתוח ממצאי ההטמעה בקרב האוכלוסייה הכללית, לבצע בחינה של האמצעים המשלימים.

יודגש כי, אמצעים משלימים הנסמכים על שימוש במאגרים חיצוניים – כגון מידע מיקום מחברות כרטיסי האשראי או חברת רב-קו, זיהוי פנים ממצלמות במרחב הציבורי או במרחבים עסקיים וכד' – אלה כאמור טומנים בחובם פגיעה קשה ביותר בפרטיות הציבור.

דווקא השימוש באמצעים לבישים – דוגמת צמיד – באזורים ייעודיים אשר יוגדרו מראש (כגון בתי חולים, מוסדות חינוך וכד') ובמסגרת של התניית כניסה למקום בענידתם, נראה כניתנים לעיצוב לפרטיות – במיוחד אם הם יהוו נדבך נוסף ביישומון "המגן" או ישתמשו בטכנולוגיה דומה.





3. השימוש בכלי השב"כ

הרשות כבר הביעה לא אחת את עמדתה בנושא זה, כי בהיבטי הגנה על הפרטיות, ישנו קושי רב ומהותי לבצע פעילות ניטור על ידי גוף שיייעודו העיקרי הינו מאבק בסיכול פעילות טרור והגנה על בטחון המדינה.

עמד על כך בית המשפט העליון בפסק הדין בעניין בן מאיר מיום 26.4.20:

"הפגיעה בפרטיות במקרה דנן היא קשה במיוחד משתי סיבות עיקריות: האחת עניינה במיהות הגורם אשר מפעיל את האמצעים הנדונים, היינו בעובדה כי השב"כ – שירות הביטחון המסכל של המדינה – הוא זה אשר מפעיל אמצעי מעקב אחר אזרחי ותושבי המדינה; והשנייה עניינה במיהות האמצעים שנבחרו, קרי בעובדה שמדובר במנגנון כופה ששקיפותו אינה מלאה.

אשר למיהות הגורם המפעיל את האמצעים הנדונים – השימוש בכלים אשר פותחו במטרה להילחם בגורמים עוינים והפנייתם כלפי אזרחי ותושבי המדינה שאינם מבקשים להרע לה, הוא מהלך העשוי להדיר שינה מעיניו של כל שוחר דמוקרטיה. [...] הבחירה לעשות שימוש בארגון הביטחון המסכל של המדינה לצורך מעקב אחר מי שאינם מבקשים לפגוע בה, מבלי שניתנה הסכמה לכך מצד מושאי המעקב, מעוררת קושי רב ביותר"¹⁰.

בהינתן הנתונים העדכניים בדבר היקף ואופן התפשטות המגיפה, ובוודאי כשברור כי נגיף הקורונה אינו עומד להיעלם בקרוב וצפוי להיות חלק בלתי נפרד משגרת חיינו למשך חודשים ארוכים (ואולי שנים) של גלים ונסיגות של המגיפה, עולה הצורך למצוא פתרונות שימשו לטווח בינוני-ארוך.

יש הכרח לבחון בכל רגע מחדש את הצורך וההצדקה העדכניים בשימוש באמצעי מעקב של גוף ביטחון, אשר נועדו לסיכול טרור ולביטחון המדינה, ואשר פוגעים באופן ישיר ומובהק בזכותם לפרטיות של אזרחים ותושבים, כמו גם את המידתיות של אמצעים אלו, בהתחשב בחלופות השונות וכחלק מאסטרטגיית היציאה הכוללת.

ללא הגדרה ברורה לגבי מטרת ותכלית השימוש בכלי, עלול להיווצר מדרון חלקלק, בו ניתן יהיה לעשות שימוש בכלים דרקוניים למיגור שלל תופעות הפוגעות בצורה כלשהי בביטחון הציבור או אף ברווחתו. כך למשל, מדוע לא להיעזר בגופי בטחון בעתיד לאיתור מגעים של חולי חצבת? פעילות פדופילים? נהגים מועדים אשר נוהגים ללא רישיון ולפיכך מעמידים בסכנת חיים ברורה ומיידית נהגים אחרים בכביש? וההמשך ברור ומובן, גם אם נשמע כעת רחוק (כפי שנראתה עד לא מכבר האפשרות לעשות שימוש בשב"כ כדי לאתר את מי שבא במגע עם חולה במחלה כזו או אחרת).

חשש זה הובע גם על ידי בית המשפט העליון בפסק הדין בעניין בן מאיר: "עלינו לשמור מכל משמר שהאירועים החריגים שעמם אנו מתמודדים לא יותירו אותנו עם מדרון חלקלק של שימוש באמצעים חריגים ופוגעניים ללא הצדקה".

¹⁰ בג"ץ 2109/20 בן מאיר נ' ראש הממשלה (26.4.20), פסקאות 38 ו-46 לפסק הדין.





הנוסחה המידתית לבחינת הפגיעה בפרטיות צריכה להגדיר באופן ברור ושקוף מה היא מטרת הכלי הטכנולוגי מבחינת צמצום המחלה, ולהבהיר את הפרמטרים על פיהם תיגזר החלופה הרלוונטית מבין שלל החלופות האפשריות בכל מועד. כך למשל, יש לבחון במסגרת ניהול סיכונים את רמת ההצלחה והדיוק של כל כלי באיתור מגעים, את קלות השימוש בו ואת ההצלחה שלו בהפחתת נתוני התחלואה.

כפי שהשתקף בבירור במהלך השבועיים האחרונים, מנגנון השב"כ, מעבר לפגיעה הדרמטית בהיבטי פרטיות, מזמן הוא טעויות (False Positive) למכביר, ועל רבים נגזר בידוד והגבלה דרמטית על חופש התנועה, כאשר למעשה כלל לא באו במגע עם חולה קורונה. כמו כן, מנתוני הדיווח של משרד הבריאות מיום 9/7/2020 עולה כי אחוז החולים המאומתים מבין סך המבודדים על בסיס מנגנון איכוני השב"כ עומד על כ-5% בלבד.





נספח א' – פרקטיקות ניטור ברחבי העולם

מבוא

סקירה זו נכתבה ברקע משבר הקורונה כאשר נבחנים בארץ ובעולם פתרונות שונים למיגור המגפה, הכוללים גם אמצעים לניטור דיגיטלי. שימוש במערכות טכנולוגיות לניטור דיגיטלי עשוי להיות כרוך בפגיעה של ממש בזכות הפרטיות. **מטרת סקירה זו הינה להציג את עיקרי ההתפתחויות בעולם בנושא זה ואת הפרקטיקות הננקטות על ידי המדינות השונות.**¹¹

הדגש העיקרי בסקירה זו הינו על שימוש בטכנולוגיות מעקב דיגיטליות לצורך אכיפת חובת בידוד וסגרים ולצורך איתור מקרים של שהייה בסמוך לחולה קורונה.

מהסקירה עולה כי הדמוקרטיה המערביות אינן משתמשות בטכנולוגיות ניטור דיגיטלי לצורך אכיפת חובת בידוד וסגרים. עוד עולה מהסקירה, כי מדינות דמוקרטיות רבות מפתחות ממש בימים אלה טכנולוגיות אשר מטרתן לאתר קרבה לחולה קורונה.

מהסקירה עולה כי קיימות שתי שיטות עיקריות לאיתור קרבה: שימוש בנתוני קרבה המעידים על שהות בסמוך לחולה קורונה באופן אשר עלול לגרום להדבקה, מבלי לחשוף את תנועת המשתמש ומבלי לחשוף היכן התרחשה האינטראקציה. לעומתם, שימוש בנתוני מיקום, המתייחסים לאזור בו שהה אדם בזמן נתון, עלול לגרום לפגיעה קשה יותר בפרטיות, ולכן מדינות המערב אימצו מנגנונים המתבססים על נתוני קרבה ולא על נתוני מיקום.

קיימות שתי שיטות לאיתור נתוני קרבה בהסתמך על נתוני מרחק: שיטה ריכוזית, בה המידע נאסף לשרת מרכזי (שיטה זו אומצה ע"י אוסטרליה, אנגליה ופולין), ושיטה ביזורית, בה רוב איסוף המידע ועיבודו מרוכזים במכשיר הטלפון הנייד של המשתמשים, באופן אנונימי ומוצפן. השיטה הביזורית נתפסת ככזו המעניקה הגנה חזקה יותר לפרטיות ולמידע אודות המשתמשים (שיטה זו אומצה ע"י גרמניה, שוויץ, אירלנד, פינלנד ועוד).

האיחוד האירופי

1. ברחבי אירופה נעשה שימוש ביישומים אשר אוספים מידע מטלפונים ניידים של משתמשים בכדי לייצר "מפת קורונה", כלומר, כדי לאתר אזורי התפרצות (והמידע הנאסף הינו מידע אנונימי או אגרגטיבי) או כדי לאתר קרבה לחולה מאומת. השימוש באמצעים אלה כדי לאתר קרבה לחולה **נעשה בדרך כלל בהסכמה** (יצוין כי ההסכמה נדרשת הן בשלב הורדת היישומון והתקנתו, והן בהפעלתה הסדירה - כלומר למשתמש יש את היכולת להסירה, להגביל את הרשאות היישומון, לכבות את ה-GPS או את תקשורת ה-BT במכשיר או לכבותו כליל).
2. בשל השימוש ההולך וגובר באמצעי מעקב דיגיטליים, ראש ה-European Data Protection Supervisor הדגיש כי לאמצעים אלה עלולות להיות השלכות על חייהם האישיים של התושבים ולפיכך יש צורך בגישה פאן-אירופית לנושא.¹²

¹¹כל האמור בסקירה זו נכון ליום מועד פרסומה. הסקירה מתבססת על אתרים רשמיים וכאלה שאינם רשמיים.
https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf¹²





3. ראש הוועדה לזכויות הפרט של הפרלמנט האירופי הכריז כי השימוש באמצעים לעיל כפוף להוראות ה-GDPR ולהוראות דירקטיבת ה-E-Privacy, וכי אמצעי מעקב מעוררים חשש לפגיעה קשה בפרטיות.¹³
4. הנציבות האירופית פרסמה המלצה ל"ארגז כלים משותף" לשימוש מאוחד בטכנולוגיה ליציאה ממשבר הקורונה. במסגרת ההמלצה, הוצע לפתח גישה מתואמת פאן-אירופאית לשימוש באפליקציות סלולריות על מנת לאפשר בידוד ממוקד ויעיל, והוסבר הצורך בפיתוח מודל משותף לחיזוי התפתחות הנגיף, וזאת ע"י שימוש בנתוני מיקום ניידים אנונימיים ומוצפנים.
5. בתאריך 16/04/2020 הנציבות האירופאית פרסמה הבהרות בנושא עקרונות לפיתוח אפליקציות לאיתור קרבה בהסכמת משתמשים. לפי הבהרות אלו, כדי לאתר קרבה עדיף להתבסס על העברת אותות Bluetooth ולא על נתוני GNSS/GPS, וזאת הן משום שמחד אותות Bluetooth מדויקים יותר ומאידך הם מונעים מעקב ובכך ממלאים אחר העיקרון החשוב של מזעור המידע המועבר. בנוסף, נקבע כי אין לאסוף נתונים אודות השעה בה נוצרה הקרבה, אולם כדאי לשמור את התאריך בכדי להעריך את משך זמן הבידוד הנדרש.
6. לגבי ההודעה למשתמשים עמם משתמש חולה בא במגע, קיימות שתי גישות. גישה מבוזרת - המשתמש מודיע דרך היישומון כי הוא נגוע, באישור רשות הבריאות, אליו מצורף קוד TAN (נוסח ההודעה ייקבע ע"י משרד הבריאות). המספר הפסדונימי רנדומלי של מכשיר הנייד נותר מוצפן על מכשיר הסלולר של המשתמש. גישה ריכוזית - המספר הפסדונימי רנדומלי של הטלפונים הניידים של המשתמשים (אשר כאמור לעיל, משתנה מעת לעת) נשמר גם בשרת של רשות הבריאות, באופן שבו הנתונים בשרת אינם מאפשרים זיהוי ישיר של המשתמשים. דרך המזהים הללו, משתמשים יקבלו הודעה על כך שהיו בקרבת משתמש חולה. רשויות הבריאות תידרשנה לקבל הסכמה של משתמש אשר שהה בקרבת חולה כדי לקבל את מספר הטלפון, להתקשר אליו או לשלוח הודעת SMS. במקרה זה נדרש לתעד לוגים לשרת.
7. בתאריך 19/03/2020 התפרסמה הודעת ה-European Data Protection Board¹⁴ לפיה באיסוף נתוני מיקום יש להעדיף שימוש במידע אנונימי ואגרטיבי באופן שבו לא ניתן יהיה לבצע זיהוי חוזר של נושאי מידע. לפי דירקטיבת ה-E-Privacy, הכלל הוא כי ניתן לעשות שימוש בנתוני מיקום רק כאשר המידע אנונימי או אגרטיבי או כאשר ניתנה הסכמה לכך.¹⁵ יחד עם זאת, כאשר השימוש בנתוני מיקום מזוהים הכרחי לצרכי בטחון הציבור, הדירקטיבה מאפשרת למדינות לעשות שימוש במידע בנסיבות חריגות ביותר, ובלבד שהשימוש מוסדר בחקיקה פנים מדינתית, הכוללת אמצעי בקרה ראויים אשר יבטיחו מידתיות.
8. משמעות עקרון המידתיות היא כי יש להעדיף תמיד את האמצעי אשר פגיעתו בפרטיות פחותה. אמצעי חודרני כגון מעקב אחר הפרט (לדוגמא: עיבוד היסטוריית התנועה של אדם באופן שוטף ושאינו אנונימי) יחשב לפי הדין האירופי כמידתי רק בנסיבות יוצאות דופן ובהתייחס לאופן

¹³ <https://www.europarl.europa.eu/news/en/press-room/20200406IPR76604/use-of-smartphone-data-to-manage-covid-19-must-respect-eu-data-protection-rules>

¹⁴ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

¹⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN>





שבו עיבוד המידע נעשה. פעילות כזו כפופה לביקורת מוגברת ולמגבלות מובנות (כגון משך זמן המעקב, היקף המעקב, משך הזמן בו המידע יישמר, מגבלת המטרה ועוד), ובכל מקרה, יש להעדיף את האמצעי אשר פגיעתו בפרטיות פחותה.

9. בהמשך פורסמו הנחיות ה-EDPB לשימוש בכלים דיגיטליים לאיתור קרבה לנגועים בקורונה.¹⁶ ההנחיות כוללות אמצעים אשר נועדו להבטיח אחריות (קביעת משרד הבריאות כבעל המאגר), קבלת הסכמה, שקיפות, מזעור המידע, הצמדות למטרות איסוף המידע, אבטחת המידע, מחיקת המידע, קביעת האופן והמועד בו היישומון יפסיק לפעול עם תום המשבר והמידע יושמד בשרתים מרכזיים ובמכשיר הנייד ועוד.

יוזמת ה-PEPP-PT¹⁷

10. מטרת יוזמת ה-Pan European Privacy Proximity Tracing הינה לספק פלטפורמה פאן-אירופית לתמיכה ביוזמות של מדינות אירופה לעשות שימוש בטכנולוגיות מעקב דיגיטליות לאיתור קרבה לנגועים בקורונה.

11. באמצעות מומחים מתחומי המדע והטכנולוגיה, הצפנה, אבטחת מידע, תקשורת ועוד, PEPP-PT מציעה פתרונות טכנולוגיים, סטנדרטים ושירותי תמיכה, זאת במטרה לאפשר למדינות אירופיות ומדינות נוספות ברחבי העולם, להשתמש באמצעי מעקב יעילים, המסוגלים לתקשר זה עם זה (אינטראופרבייליים), העומדים בהוראות ה-GDPR וזאת מתוך ראייה אירופית (ואף בינלאומית), אשר תאפשר איתור קרבה לנגוע גם במעבר של יחידים ממדינה למדינה.

12. יוזמה זו מסתמכת על אותות טלפונים ניידים אשר ישודרו ב-Bluetooth. הסטנדרט של PEPP-PT קובע כי קרבה לנגוע הינה שהייה של חצי שעה במרחק של עד שני מטרים ממנו, ולכן נתונים יישמרו רק אודות אירועים מסוג זה (קרי, האפליקציה לא תאסוף נתונים אודות מי ששהו במרחק רב יותר או לזמן קצר יותר). היישומון אוסף נתוני זיהוי אנונימיים של ציוד הקצה ואינו אוסף נתוני מיקום או מזהה את נושא המידע.

13. כאשר משתמשים נמצאים בקרבה, הם מחליפים מספרים מזהים רנדומליים ואנונימיים מבלי לקבל נתוני מיקום או מידע מזהה אחר. משתמש לא מקבל גישה להיסטוריית התנועה של עצמו או של המשתמש השני. נתון שהופך ללא רלבנטי (בשל חלוף הזמן) נמחק.

14. כל עוד משתמש לא נמצא נגוע, היסטוריית הקרבה האנונימית נותרת מוצפנת והוא אינו יכול לצפות בה. אולם, כאשר משתמש א' נמצא נגוע, רשויות הבריאות יקצו למשתמש א' קוד TAN למטרות אבטחת מידע ולמניעת זיהום מערך ה-PEPP-PT. באמצעות הקוד, משתמש א', אשר הסכים לכך, מעביר ל-Trust Service, אישור להודיע לכל המשתמשים של אפליקציות PEPP-PT על כך שהיו בקרבת משתמש נגוע. מאחר והטלפונים שומרים נתונים אנונימיים של ציוד קצה, לא ניתן לזהות את בעל ציוד הקצה.

15. המכניזם המייצר את המזהה הרנדומאלי מכיל פיסת קוד המאפשרת לזהות מאיזו מדינה מגיע כל משתמש.

¹⁶ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en
¹⁵ <https://www.pepp-pt.org/>





16. כאשר משתמשים מגיעים מאותה מדינה ויש חשש שמשתמש חולה בקורונה, המספר שלו מסומן בהתאם, ב- Trust Service, וכאשר הוא יבקש לברר מה מצבו האפליקציה תיודע כי יש חשש לכך שהמשתמש נגוע.

17. כאשר המשתמשים הינם ממדינות שונות - מידע אודות משתמש אי משודר ל- Trust Service של מדינה ב'. השידור מוצפן וחתום אלקטרונית. גם ה- Trust Service במדינה אי מעבד מידע במקרה זה.

18. במהלך חודש יוני פורסמו הנחיות טכניות ראשוניות, אשר מטרתן לייצר אינטראופרביליות בין אפליקציות ממדינות שונות באירופה, במטרה לאפשר לאפליקציות להתממשק למערכת ההתערות, כדי לבצע איתור מגעים, של אנשים העוברים ממדינה למדינה, מבלי להוריד אפליקציה נוספת. בינתיים ההנחיות רלבנטיות רק עבור אפליקציות לאיתור קרבה המתבססות על נתוני מרחק במודל המבוזר¹⁸.

איטליה

19. איטליה השיקה את אפליקציית Immuni בתאריך 1.6.20. איטליה בחרה במודל הביזורי על בסיס ממשק אפל-גוגל. עשרה ימים לאחר השקתה, האפליקציה זכתה ל – 2.7 מיליון הורדות (באיטליה כ- 60 מיליון תושבים). בהתחשב בשיעור הילדים ותושבים נוספים אשר אינם מחזיקים בטלפונים ניידים, פוטנציאל ההורדות עומד על כ- 30 מיליון¹⁹.

גרמניה²⁰

20. הוחלט לאמץ מודל וולונטארי של הורדת אפליקציה על בסיס טכנולוגיית Bluetooth, אשר תבדוק אינטראקציות, ללא איסוף נתוני מיקום. האפליקציה תשלח למשתמשיה הודעה על כך ששהו בקרבת אדם נגוע, מבלי לחשוף את זהות האדם הנגוע. האפליקציה פותחה בידי ה- Fraunhofer Heinrich Hertz Institute (HHI) לחקר תחום הטלקומוניקציה יחד עם ה- Robert Koch Institute - מרכז לבלימת מחלות. ה- Federal Commissioner for Data Protection הגרמני אישר את השימוש בטכנולוגיה, והסביר כי איסוף מידע כאמור ייתכן אך ורק בהסכמת המשתמשים. ה- Commissioner הדגיש כי המידע יישמר לתקופה מוגבלת ומוגדרת מראש, ולאחר מכן יימחק.

18

https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilitydet_aidelements_en.pdf

https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

¹⁹ <https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html>

²⁰ <https://www.thelocal.de/20200402/privacy-mad-germany-turns-to-app-to-track-virus-spread>





21. הרשות להגנת הפרטיות של מחוז Rhineland Palatinat הבהירה כי יש לשלב באפליקציה את האלמנטים הבאים: הסכמה מדעת של משתמשים, האפשרות לחזור מההסכמה בכל רגע נתון, מגבלת מטרה (אין לעשות שימוש במידע אלא לצורך איתור קרבה לנגוע בנגיף), שימוש בפסדונימים חזקים והעברת מידע מאובטחת, שמירת המידע על ציוד הקצה ולא בשרת מרכזי ומחיקת המידע תוך 14 ימים.
22. בתחילת הדרך ממשלת גרמניה תמכה במודל הריכוזי, אולם בשל ביקורת רבה אשר הושמעה על כך, גרמניה בחרה במודל המבוזר, והסתייעה במיזם של Google ו-Apple עליו נרחב בהמשך.
23. האפליקציה, "Corona – Warn – App", הושקה בתאריך 25.6.20, ובינתיים זכתה ל- 13 מיליון הורדות (אוכלוסיית גרמניה מונה כ- 83 תושבים). קנצלרית גרמניה, קידמה את האפליקציה והסבירה לציבור כי מדובר באמצעי חשוב לאיתור מגע ולניתוק שרשרת ההדבקה במחלה.²¹

נורבגיה

24. קבינט השרים הודיע על אימוץ דירקטיבה לפיה הרשות לבריאות הציבור תפתח אפליקציה לאיתור קרבה עם חולה/נשא. השימוש באפליקציה יעשה בהסכמה, והאפליקציה תודיע למשתמשים בה במקרה הצורך, על כך ששהו בקרבת חולה בקורונה. על האפליקציה יחולו הוראות ה-GDPR והוראות חוקי הבריאות בנושא סודיות רפואית. האפליקציה (Smittestopp) הושקה באפריל ומבוססת על טכנולוגיית Bluetooth ועל טכנולוגיות לאיסוף נתוני מיקום.²²
25. הרשות הנורבגית להגנת הפרטיות Datatilsynet הבהירה כי כתנאי לשימוש באפליקציה, יש להודיע למשתמשים מה המידע שנאסף, מטרת איסוף המידע, משך הזמן בו יישמר המידע, וכיצד ניתן לחזור מההסכמה. הובהר כי המידע יישמר למשך 30 יום, ומחיקת האפליקציה עיני המשתמש תגרום למחיקת המידע או הפיכתו לאנונימי.
26. נתונים מזהים כגון מספר טלפון, יוחזקו בנפרד מנתוני המיקום, ורק עובדים מורשים של משרד הבריאות יקבלו גישה למידע מזוהה. המידע לא יועבר לצד שלישי ללא הסכמה מפורשת של נושא המידע, לא ניתן להשתמש במידע כדי לוודא ציות להוראה חוקית ואין להשתמש במידע למטרות מסחריות. בנוסף, אין לעשות שימוש במידע רפואי או נתוני מיקום לצרכי אכיפה, ביטוח ותעסוקה.
27. האפליקציה הושקה במהלך חודש אפריל 2020.
28. בחודש יוני 2020 הרשות להגנת הפרטיות הודיעה למשרד הבריאות כי עליו להשעות את השימוש באפליקציה, בשל העובדה שהאפליקציה אוספת מידע רב, למטרות שונות (האפליקציה אוספת מידע גם לצרכי מחקר), וזאת מבלי לאפשר למשתמשים בחירה אמיתית בין השימושים השונים של האפליקציה. הרשות אף ציינה כי בשל מספר ההורדות הנמוך של האפליקציה, הפגיעה בפרטיות אשר נגרמת ממנה אינה מידתית בהשוואה לתועלת הנמוכה

²¹ <https://www.bbc.com/news/53168438>

²² <https://www.forbes.com/sites/davidnikel/2020/04/25/norway-14-million-people-download-coronavirus-tracking-app-despite-security-concerns/#676e68a57832>





אשר ניתן להפיק מהאפליקציה (האפליקציה הורדה ע"י 600,000 משתמשים בלבד, בשים לב לכך שאוכלוסייה נורבגיה מונה 5.4 תושבים)²³.

בריטניה²⁴

29. ה- National Health Institute ואוניברסיטת אוקספורד מפתחות אפליקציה לאיתור קרבה. האפליקציה החלה לפעול כפיילוט ב- Isle of Wight. השימוש באפליקציה יעשה בהסכמת המשתמשים ומבוסס על אותות אשר יועברו בין משתמשים באמצעות ה- Bluetooth. כאשר משתמש לוקה בתסמיני קורונה, המשתמש רשאי להודיע על כך לרשות הבריאות באמצעות האפליקציה. הרשות תעבד את המידע ובהתאם לניתוח הסיכונים, תחליט הרשות, אם לשלוח הודעה למשתמשים אחרים אשר שהו בקרבת המשתמש. האפליקציה תייעץ למשתמשים אשר שהו בקרבת משתמש הסובל מסימפטומים, כיצד לנהוג והאם יש צורך בכניסה לבידוד. הייעוץ יינתן ע"י רופא בכיר.

30. בעתיד האפליקציה תאפשר למשתמשים לשלוח מידע נוסף, בהסכמתם, על מנת לאפשר לרשויות לאתר התפרצויות.

31. המודל בו בחרה בריטניה להפעיל את האפליקציה שלה הינו המודל הריכוזי.

32. בתאריך 4/05/2020, לקראת דיון בוועדה המשותפת לזכויות אדם בפרלמנט הבריטי, הרשות להגנת המידע הבריטית פרסמה מסמך הכולל עקרונות להגנת פרטיות אותם יש לצפות כי יישמו בתהליך הפיתוח וההפעלה.²⁵

33. ראשת הרשות להגנת המידע בבריטניה הסבירה כי הייתה מעדיפה להפעיל את האפליקציה במודל מבוזר ולא במודל הריכוזי שנבחר. גורם במשרד הבריאות הבריטי הסביר כי האפליקציה מבוססת על מודל ריכוזי בשל הרצון לנתח את התנהגות הווירוס,²⁶ וכי לו שיקולי פרטיות היו השיקולים היחידים שיש לבחור, בריטניה הייתה בוחרת במודל המבוזר.

34. במהלך חודש יוני התברר כי הפיילוט ב- Isle of White לפיתוח המערכת במודל ריכוזי לא צלח. מודל זה עבד טוב בזיהוי והערכת המרחק בין שני משתמשים אבל לא עבד טוב על מכשירי אייפון של אפל בהם היה זיהוי של כ- 4% מן המשתמשים בלבד (בשל מגבלות שאפל מעמידה על אפליקציית בלוטות' אשר אינה משתמשת בממשק "אפל גוגל" המבוזר). כרגע העוסקים במלאכה ממשיכים לפתח את האפליקציה במודל המבוזר, על בסיס ממשק גוגל-אפל. האפליקציה תושק ככל הנראה במהלך חודש אוגוסט²⁷.

²³ <https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns>

²⁴ <https://www.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives>

²⁵ <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf>

²⁶ <https://www.reuters.com/article/us-health-coronavirus-britain-apps/uk-to-test-covid-19-tracing-app-on-the-isle-of-wight-this-week-idUSKBN22G24U>

²⁷ לפי דיווח של נציג ה- ICO (Information Commissioners Office) בבריטניה.





צרפת

35. ממשלת צרפת פיתחה אפליקציה בשם StopCovid²⁸. האפליקציה פותחה במודל הריכוזי ולא המבוזר ואוספת נתוני מרחק. האפליקציה מבוססת על טכנולוגיית BLE. כאשר משתמש מאובחן כחולה בקורונה הוא מקבל מספר קוד אותו הוא רשאי להזין למערכת. אם החולה בחר להזין את הקוד במערכת, האפליקציה תעביר לשרת מרכזי את רשימת האינטראקציות של החולה המאובחן.

36. האפליקציה הושקה בתאריך 2.6.20, וזכתה עד כה לכ- 2 מיליון הורדות. נכון ליום 23.6.20 רק 70 משתמשים הודיעו באמצעות האפליקציה כי אובחנו כחולי קורונה, ורק 14 משתמשים קיבלו הודעה כי שהו בקרבת חולה קורונה²⁹.

פולין³⁰

37. אכיפת חובת בידוד ומתן סיוע למבודדים - אפליקציית Home Quarantine App פותחה ע"י המשרד לנושאים דיגיטליים ומשרד הבריאות, במטרה לאכוף את הוראות הבידוד של הממשלה. הממשלה העמידה בפני מי שחלה עליו חובת בידוד שתי חלופות: הורדת האפליקציה או ביקורים רנדומליים של המשטרה בביתם. מבודדים אשר בחרו להוריד את האפליקציה מוסיפים לה תמונת סלפי כחלק מתהליך הרישום. כדי לוודא שהות המבודד בביתו, רשויות האכיפה שולחות דרישה להעלאת סלפי מזוהה מיקום, דרך האפליקציה, תוך 20 דקות ממועד קבלת הדרישה. בנוסף, על מי שהוריד את האפליקציה חלה חובה להודיע על הופעת סימפטומים של המחלה.

38. האפליקציה מאפשרת למשתמשים לתקשר עם רשויות הרווחה ולבקש סיוע בקבלת מצרכים חיוניים וטיפול דחוף.

39. חובת הבידוד חלה על מי שחזר מחו"ל או מי שנמצא חולה.

איסלנד

40. איסלנד השיקה את אפליקציית Ranking C-19 בראשית חודש אפריל 2020. האפליקציה אוספת נתוני GPS (נתוני מיקום ותנועה). 38% מתושבי איסלנד הורידו את האפליקציה³¹.

<https://techcrunch.com/2020/06/02/france-releases-contact-tracing-app-stopcovid-on-android/>²⁸

<https://www.ft.com/content/255567d5-b7ec-4fbc-b8a9-833b3a23f665>²⁹

<https://www.businessinsider.com/poland-app-coronavirus-patients-mandatory-selfie-2020-3>³⁰

<https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/>³¹





שוויץ

41. שוויץ השיקה את אפליקציית SwissCovid בתאריך 25.6.20³². שוויץ בחרה במודל המבוזר המתבסס על ממשק אפל וגוגל. האפליקציה הורדה ע"י כמיליון משתמשים³³, (בשוויץ כ- 8.5 מיליון תושבים). 30 משתמשים הודיעו דרך האפליקציה כי חלו בקורונה.

ניו-זילנד

42. אפליקציית NZ COVID Tracer app. האפליקציה סורקת קודי QR המופיעים על פוסטרים ושלטים במקומות ציבוריים ועסקים, ובכך מייצרת "יומן מיקום" של משתמשים. האפליקציה הושקה בתאריך 25.5.20, ומשתמשים בה כ- 541,000 תושבים. האפליקציה נסרקה 1,035,154 פעמים ופורסמה ע"י 56,552 עסקים.

אוסטרליה

43. בתאריך 26/04/2020, מחלקת הבריאות של ממשלת אוסטרליה השיקה אפליקציה לאיתור קרבה בשם COVID Safe המתבססת על אותות Bluetooth³⁴. אוסטרליה בחרה לפתח אפליקציה לאיתור קרבה במודל הריכוזי. השימוש באפליקציה כפוף להסכמת המשתמשים. במסגרת תהליך הרישום המשתמש מתבקש להזין שם, מספר טלפון, מיקוד וטווח גילאים. ההתקנה תלויה בהודעת טקסט המאשרת את תהליך הרישום וכוללת מספר PIN. בתום תהליך הרישום המערכת מייצרת עבור המשתמש קוד ייחודי ומוצפן.

44. כאשר האפליקציה מזהה קרבה למשתמשים אחרים, היא מתעדת את קוד המשתמש, תאריך, שעה ומשך זמן הקרבה. האפליקציה לא אוספת נתוני מיקום.

45. משתמשים יקבלו תזכורת להפעיל את ה-Bluetooth מדי יום.

46. המידע מוצפן על מכשיר הטלפון הנייד של המשתמשים ואין באפשרותם לגשת אליו.

47. מידע אודות משתמשים אשר שהו בקרבה יימחק לאחר 21 יום.

48. כאשר אדם אובחן כנשא של הנגיף, במסגרת החקירה האפידמיולוגית, רשויות הבריאות יפנו אליו ושאלו אם הוריד את האפליקציה. אם התשובה חיובית, המשתמש יתבקש לתת הסכמתו להעלאת רשימת המשתמשים אשר שהו בקרבתו, לשרת מאובטח. ההסכמה תינתן ע"י הזנת קוד ה-PIN אשר הונפק למשתמש בתהליך הרישום. רשויות הבריאות יצרו קשר עם המשתמשים האחרים כדי להודיע להם כי שהו בקרבת אדם נגוע בקורונה וכדי לתת הנחיות נוספות. רשויות הבריאות לא ימסרו למשתמשים מידע מזהה אודות מי שאובחן כחולה בקורונה ושהה בקרבתם.

<https://www.thelocal.ch/20200629/more-than-800000-downloads-for-switzerlands-covid-app-in-three-days>

³² נציג שוויץ בוובינר סגור מטעם GPA ארגון מיום 6 ליולי 2020
³³ להסברים אודות האפליקציה ראו <https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#about-the-app>
³⁴ ולמדיניות הפרטיות של האפליקציה ראו <https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app>





49. לאחרונה פורסמה הצעת חוק לפיה שימושים לרעה באפליקציה הם עבירה פלילית. לפי הצעת החוק, דרישה להורדת היישום כתנאי לאספקת שירות, כניסה למקומות ציבוריים או מסחריים וכיו"ב הינה עבירה פלילית.³⁵

50. נכון ליום 11.6.20, האפליקציה זכתה ל – 6.2 מיליון הורדות, ושימשה לאיתור קרבה ב- 30 מקרים (בתקופה זו התגלו בסך הכל כ- 565 מקרים חדשים). בכל אותם מקרים לא התגלו קשרים נוספים מעבר לקשרים אשר התגלו בחקירה "ידנית". נטען כי האפליקציה לא גילתה מידע נוסף ומשמעותי בשל העובדה שבאוסטרליה מספר החולים המאומתים נמוך³⁶.

סינגפור

51. **אכיפת בידוד ותיעוד תנועה של חולה מאומת** - חבים בחובת בידוד (חולים מאומתים ובני משפחותיהם) מקבלים מגורמי אכיפה הודעת טקסט מספר פעמים ביום. הודעת הטקסט כוללת לינק עליו יש ללחוץ, כדי להעביר לגורמי האכיפה את נתוני המיקום של המבודד על מנת לאשר כי המבודד שוהה בביתו.

52. בנוסף, על מנת לייצר מפה אפידמיולוגית לאיתור המקומות בהם שהה חולה ב-14 הימים לפני שאומת כחולה, הממשל עושה שימוש במצלמות אבטחה, נתוני מיקום סולריים ותיעוד עסקאות אשראי.³⁷

53. **איתור שהייה בקרבת חולה/נשא מאומת** - סוכנות הטכנולוגיה של הממשלה הסינגפורית פיתחה אפליקציה, בשם Trace Together³⁸ המודיעה למשתמשים אם שהו בקרבת חולה מאומת (עד 6.5 פייט משך 30 דקות לפחות). השימוש באפליקציה כפוף להסכמת המשתמש. האפליקציה מתבססת על טכנולוגיית Bluetooth Low Energy ומזהה משתמשים אחרים אשר הורידו את האפליקציה. האפליקציה מעניקה לכל משתמש מספר מזהה זמני המגלם מספר זיהוי המוחזק ע"י משרד הבריאות, ועבר אנונימיזציה. כאשר משתמש א' נמצא בקרבת משתמש ב', הטלפון של משתמש א' מעביר את המספר האנונימי למשתמש ב', ולהיפך (משתמש א' מקבל את המספר האנונימי של משתמש ב'), והמספר האנונימי של מי ששהה בקרבת המחזיק נשמר בטלפון הנייד באופן מוצפן. אם משתמש יתגלה כחולה, האפליקציה תבקש מהמשתמש לאשר גישה לרשימת המספרים המוצפנים ותשלח לבעליהן הודעה כי שהו בקרבת החולה המאומת. **האפליקציה לא אוספת נתוני מיקום או מידע מזוהה אחר.**

54. כ- 35% מתושבי סינגפור הורידו את האפליקציה. התגלו קשיים טכניים במכשירים של אפל, בהפעלת הבלוטותי (יש להפעיל את האפליקציה כל הזמן, באופן שמקשה על השימוש באפליקציות אחרות, ובנוסף, הבטרייה מתרוקנת במהירות) ולכן, ממשלת סינגפור מתכוונת לחלק לתושבים אשר אין ברשותם טלפון נייד או תושבים אשר משתמשים ב- iPhone, אפליקציית Bluetooth לבישה. האפליקציה תזהה אותות, אולם לא ניתן יהיה לשלוח את

<https://www.theguardian.com/australia-news/2020/may/04/government-releases-draft-legislation-for-covidsafe-tracing-app-to-allay-privacy-concerns>³⁵

<https://www.abc.net.au/news/science/2020-06-11/coronavirus-contact-tracing-app-covid-safe-no-close-contacts/12343138>³⁶

<https://www.businessinsider.com/singapore-coronavirus-containment-new-challenges-2020-4>³⁷
<https://www.tracetgether.gov.sg/>³⁸





המגעים ברשת, והדבר יעשה באופן ידני ע"י רשויות הבריאות, עם אימות המשתמש כנגוע בנגיף³⁹.

55. בנוסף, כחלק מהמאמץ לבצע איתור מגעים, הוחלט להוסיף מערך ניטור לאומי בשם SafeEntry. מדובר במערכת check in אשר פותחה ע"י ממשלת סינגפור, ומטרתה לתעד כניסות ויציאות של עובדים ומבקרים, במקומות ציבוריים. המערך מתבסס על סריקת קודי QR בכניסה וביציאה, סריקת ת.ז. אלקטרונית או סריקת אפליקציית ה-Singpass אשר מקנה כניסה לשירותי ממשל. מבקרים ועובדים סורקים קוד QR בכניסה למקום, ומעבירים שם, מספר ת.ז. ומספר טלפון למערכת⁴⁰. המידע מועבר לשרת של הממשלה ורק מורשי גישה מטעם הממשלה מקבלים גישה למידע (למפעילי המוסדות בהם מותקנת המערכת ולעובדיהם אין גישה למידע⁴¹).

56. להלן רשימה חלקית של גורמים אשר חוייבו להתקין את המערכת כדי לתעד כניסה של עובדים ומבקרים: משרדים, בתי חרושת, בתי ספר ומוסדות חינוך, גנים, מוסדות בריאות, מוסדות קהילתיים, מוסדות דת, מלונות, בנקים ומוסדות פיננסיים, חנויות, מספרות (כולל ספרים המקבלים לקוחות בבתים), מוסדות תרבות, מרכזי ספורט, בתי קולנוע, עסקים המתנהלים מבתים פרטיים ככל שהלקוחות מגיעים לעסקים אלה, מוניות ועוד⁴².

הונג קונג⁴³

57. **אכיפת חובת בידוד** - בהונג קונג נקבע כי כל הנכנסים למדינה חבים בחובת בידוד בית, ומי ששב עם סימפטומים או היה במגע עם חולה יושם בבידוד במתקן ממשלתי. לצורך אכיפת ההוראה הנכנסים למדינה נדרשים לענוד צמיד מעקב. הצמיד מתבסס על טכנולוגיית Bluetooth. הצמיד לא אוסף נתוני מיקום אולם ביכולתו לאתר יציאה משטח הבידוד (אשר בעקבותיה נשלחת הודעה לרשויות).

דרום קוריאה

58. **אכיפת חובת בידוד על הנכנסים למדינה** - מי שנכנס למדינה חב בבידוד של 14 יום. חובת הבידוד נאכפת באמצעות חיוב להוריד אפליקציה אשר שולחת לרשויות הודעה, כאשר חב הבידוד מתרחק ממקום הבידוד (בנוסף, יש חובת דיווח על סימפטומים)⁴⁴.

59. **איתור קרבה לחולה/נגוע** - דרום קוריאה מאתרת שהייה בקרבת חולה/נגוע בשלושה אופנים: איסוף מידע מחברות אשראי על עסקאות (ניטור המידע מאפשר לדעת היכן בוצעו), מצלמות CCTV להן פריסה רחבה ברחבי הערים, ונתוני מיקום מחברות הסלולר.

³⁹ <https://www.bbc.com/news/technology-53146360>

⁴⁰ <https://www.gov.sg/article/digital-contact-tracing-tools-for-all-businesses-operating-during-circuit-breaker>

⁴¹ הרצאתו של ראש הרשות להגנת המידע pdpc בסינגפור

⁴² https://www.safeentry.gov.sg/latest_news#news-15

⁴³ <https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html>

⁴⁴ https://www.theregister.co.uk/2020/03/19/hong_kong_wearable_trackers_mandatory/
https://www.youtube.com/watch?v=ljSBHaD_FDs





60. הצלבת הנתונים משלושת מקורות המידע לעיל מאפשרת איתור הגורם המדביק ואיתור מי ששהה בקרבת אדם אשר אותר כחולה.⁴⁵
61. בנוסף, הממשל בדרום קוריאה משתמש במידע כדי לפרסם לציבור הרחב מפות קורונה, המתבססות על מידע אנונימי, כדי לסייע לציבור לבצע הערכה עצמית, באמצעות אפליקציות בהן ניתן לעשות שימוש בהסכמה.

הודו⁴⁶

62. ממשלת הודו פיתחה בשיתוף עם חברה פרטית אפליקציה לאיתור קרבה לחולה קורונה, בשם ArogyaSetu. האפליקציה מנתחת אינטראקציות של משתמשים, ומתבססת על Bluetooth ונתוני GPS, בינה מלאכותית ואלגוריתמים. האפליקציה מקבלת מידע על משתמשים השוהים בקרבת המכשיר, ואוספת נתונים על תנועה (מייצרת גרף תנועה) ומידע רפואי. תהליך הרישום לאפליקציה כולל מסירת פרטים כגון מגדר, מספר טלפון, תאריך לידה, מקצוע, מידע רפואי ופרטים לגבי שהייה מחוץ למדינה במהלך 30 הימים אשר קדמו להורדת האפליקציה (עם הרישום המידע לגבי שהייה בחו"ל יוצלב עם מאגר מידע אודות חולי קורונה).
63. המידע יישמר על מכשיר הטלפון באופן אנונימי ומוצפן, עד למועד שבו יהיה צורך בהתערבות רפואית. האפליקציה אוספת נתוני מיקום ואותות Bluetooth⁴⁷. המידע מועבר לשרת ממשלתי, יעבור האשינג עם מספר זיהוי דיגיטלי ייחודי. המידע מוצפן על הנייד, בתהליך ההעברה לשרת ובשרת עצמו. נתוני מיקום יימחקו לאחר 30 יום (ממועד הקרבה למשתמש, אלא אם נמצא כי המשתמש חולה בקורונה. במקרה האחרון, המידע יימחק 60 ימים לאחר שהמשתמש הבריא). מידע רפואי לא יימחק, ויועבר לגורמים רלבנטיים ככל שיהיה צורך בהתערבות רפואית.
64. **עובדי הממשל הפדרלי ועובדי תעשיית המזון חייבים להוריד את האפליקציה, ובראשית חודש מאי הודיעה הממשלה, כי תנאי הגעה לכל מקום עבודה (ציבורי או פרטי), יהיה התקנת האפליקציה.**⁴⁸
65. בדומה לסין, האפליקציה נותנת חיווי באשר למצבו הבריאותי של המשתמש, ובממשל הפדרלי יש דרישה כי רק מי שבריא יורשה לעבוד.⁴⁹
66. לפי דיווחים לא רשמיים, האפליקציה תותקן בטלפונים ניידים כברירת מחדל, ויש כוונה להתנות את התקנתה גם כתנאי לשימוש בתחבורה ציבורית.
67. ארגוני זכויות אדם ביקרו את האפליקציה בשל העדר שקיפות, צמידות מטרה, מזעור מידע ואחריותיות. בנוסף, הועלה חשש לפגיעה בפרטיות המשתמשים לאור העובדה שבהודו אין רשות פרטיות וחקיקה מסדירה.
68. האפליקציה זכתה ל-131 מיליון הורדות⁵⁰.

<https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068>

<https://economictimes.indiatimes.com/tech/software/how-to-use-aarogya-setu-app-and-find-out-if-you-have-covid-19-symptoms/articleshow/75023152.cms?from=mdr>

<https://thenextweb.com/in/2020/03/25/india-is-building-a-coronavirus-tracker-app-fueled-by-your-location-data/>

<https://www.reuters.com/article/us-health-coronavirus-india-app/india-makes-government-tracing-app-mandatory-for-all-workers-idUSKBN22E07K>

<https://www.reuters.com/article/us-health-coronavirus-tech-trfn/privacy-debate-heats-up-over-india-contact-tracing-app-idUSKBN22C2AV>

<https://www.bbc.com/news/53168438> ⁵⁰





69. האפליקציה זיהתה 900,000 מגעים. בנוסף, האפליקציה כוללת אפשרות לבצע הערכה לגבי חשיפה לנגיף (דיווח סימפטומים). בהתאם לניתוח הנתונים, האפליקציה ממליצה על ביצוע בדיקת קורונה. כשני שליש מהמשתמשים השתמשו באפשרות זו. נמצא כי כרבע מהמשתמשים אשר זוהו כמי שהיו בקרבה לחולה קורונה או נשלחו לבדיקה בהמשך להערכה, אכן נדבקו בנגיף⁵¹.

ארה"ב

70. כחלק מההתמודדות עם משבר הקורונה, הממשל קיבל מהשוק הפרטי נתונים על מגמות תנועה והתקהלויות. הנתונים מסייעים בחיזוי התפרצויות וניתוב משאבים בהתאם והממשל מקיים מגעים עם גורמים רבים בשוק הפרטי לצורך קבלת נתונים אלה.
71. יש מדינות בהן הממשל השיק אפליקציה לאיתור קרבה. כך למשל מושל צפון דקוטה הודיע כי משרדו, בשיתוף עם מחלקת הבריאות, השיקו אפליקציה לעצירת התפשטות נגיף הקורונה. האפליקציה מעניקה לכל משתמש מספר זיהוי אקראי, ואוספת את נתוני המיקום במהלך היום. המשתמשים מתמרצים לקטלג את הפעילות שלהם במהלך היום לפי סוג הפעילות. המשתמשים אינם מזוהים. אם משתמש מתגלה כחולה, עומדת בפניו האפשרות להסכים להעביר את פרטיו למחלקת הבריאות כדי לאתר קרבה וכדי לסייע בחיזוי מקומות התפרצות.
72. גם במדינת יוטה הושקה אפליקציה לאיתור קרבה Healthy Together. השימוש באפליקציה כפוף להסכמת המשתמשים. האפליקציה מתבססת על נתוני GPS ו-Bluetooth, ויש לה גישה לאנשי הקשר של המשתמש. האפליקציה אוספת נתוני תנועה, ומודיעה למשתמשים על כך ששהו בקרבת חולה קורונה. ניתן לדווח דרך האפליקציה גם על סימפטומים ולקבל מידע לגבי מיקום מעבדת בדיקות קורונה. המשתמש מחליט איזה סוג של מידע להעביר. נתוני מיקום יימחקו תוך 30 יום ומידע רפואי יישמר כמידע אנונימי⁵².
73. **הצעת חוק חדשה**⁵³ - בתאריך 30/04/2020 פורסמה הודעה על כוונה לפרסם הצעת חוק פדרלית חדשה בשם "Covid-19 Consumer Data Protection Act" אשר מטרתה להגן על נתוני מיקום, נתוני מרחק ומידע רפואי (מידע), המשמשים חברות פרטיות המנסות לסייע במניעת התפשטות הנגיף, כאשר הן מציעות שירותים המאפשרים לבדוק קרבה לחולה או לצפות התפרצות הנגיף באזורים מסוימים.
74. הצעת החוק לא חלה על מידע אנונימי ואגרגטיבי או מידע פומבי.
75. לפי ההצעה, החוק יחול על גופים מסחריים המפוקחים ע"י הרשות לסחר הוגן (FTC), חברות המספקות שירותי טלקומוניקציה הכפופות לחוק התקשורת ועמותות.
76. לפי ההצעה, ככל שאין חובה חוקית לכך, יש צורך בהסכמה ויידוע מראש, לאסוף, להעביר או לעבד מידע למטרות של התמודדות עם משבר הקורונה.
77. כמו כן, נקבע בהצעה כי יש להודיע למשתמשים, במועד האיסוף, כיצד יעשו שימוש במידע שלהם, למי יעבירו את המידע וכמה זמן המידע יישמר. יש להבהיר מהו מידע אנונימי ומהם האמצעים בהם החברה תנקוט למניעת זיהוי חוזר. חברות העוסקות בעיבוד מידע כאמור

⁵¹ <https://pib.gov.in/PressReleasePage.aspx?PRID=1626979>

⁵² <https://qz.com/1843418/utahs-new-covid-19-contact-tracing-app-will-track-user-locations/>

⁵³ <https://www.commerce.senate.gov/2020/4/wicker-thune-moran-blackburn-announce-plans-to-introduce-data-privacy-bill>





יפרסמו דוחות ציבוריים בהם תתואר פעילותן. חברות כאמור כפופות לכללים של מזעור המידע ואבטחתו. החברות ימחקו את המידע כאשר המידע לא יהיה נחוץ לצורך התמודדות עם נגיף הקורונה. התובע הראשי יהיה בעל הסמכות לאכיפת הוראות החוק.

קנדה

78. במשך תקופה ארוכה הממשל הפדראלי הקנדי לא אמר את דברו בנושא אפליקציות לאיתור קרבה, אולם יש מחוזות אשר החלו לפתח אפליקציות וולונטריות לאיתור קרבה. במחוז אלברטה פותחה אפליקציה בשם ABTraceTogether אותה ניתן להוריד למכשיר הטלפון הנייד. כאשר נרשמים לאפליקציה, מוסרים מספר טלפון. האפליקציה אוספת נתוני קרבה ולא נתוני מיקום,⁵⁴ ולכן הרשויות והמשתמשים לא מקבלים נתוני מיקום. גם באפליקציה זו, משתמשים אשר נמצאים בקרבה (קרבה של עד 2 מטר), מחליפים מספר רנדומלי מוצפן המעיד על כך.

79. כאשר משתמש מאובחן כחולה, הוא יישאל ע"י הרשויות האם הוריד את האפליקציה. אם התשובה חיובית, הוא יישאל אם הוא מסכים להעלות את המספרים הרנדומליים המוצפנים לשרת של שירותי הבריאות. אם המשתמש מסכים, הרשויות ייצרו קשר עם מי שהיה בקרבת המשתמש, לאחר קבלת המידע המוצפן. ניתן לבקש להימחק מהאפליקציה בכל שלב, ואינטראקציות תשמרנה באפליקציה למשך 21 ימים בלבד.

80. בתאריך 7/05/2020 פורסמה הודעה משותפת של הרגולטורים הקנדיים בתחום הגנת המידע (Daniel Therion, ראש ה- Office of the Privacy Commissioner, אשר הינו הרגולטור הקנדי יחד עם הרגולטורים של המחוזות). לפי ההודעה,⁵⁵ אפליקציות לאיתור קרבה מעוררות חששות בתחום הפרטיות ולכן יש לוודא כי הן יעמדו בכל אלה: הסכמה ובסיס חוקי, הכרח ומידתיות, מגבלת מטרה, אנונימיזציה, מגבלת זמן, שקיפות, אחריותיות, אמצעי אבטחה.

81. באמצע חודש יוני הודיע ראש ממשלת קנדה על הכוונה להשיק אפליקציה לאומית לאיתור קרבה. האפליקציה וולונטארית, תתבסס על טכנולוגיית BLE ולא תאסוף נתוני מיקום. חולה מאומת יקבל קוד אנונימי רנדומלי. האפליקציה תושק בתחילת חודש יולי כפיילוט באונטריו, וכל פרובינציה תחליט אם בכוונתה לאמץ את השימוש בה⁵⁶. האפליקציה פותחה ע"י הממשלה בשיתוף עם BlackBerry ו-Shopify.

פתרון Google ו-Apple לתשתית אפליקציות איתור קרבה והמחלוקת בין לבין בריטניה וצרפת

תיאור הטכנולוגיה של החברות

82. Google ו-Apple (החברות) פיתחו ממשק (API) אשר נועד לאפשר תאימות בין שתי הפלטפורמות במטרה לסייע לרשויות בריאות ברחבי העולם להפעיל אפליקציות לאיתור קרבה בטכנולוגיית BLE במודל המבוזר.

83. גם במודל זה מועברים אותות Bluetooth בין משתמשים הנמצאים בקרבה. המידע אשר יועבר לשרת מרכזי יכלול את תאריך המגע, משך זמן הקרבה וחוזק האות.⁵⁷

⁵⁴ ראו הבהרות באתר האינטרנט של האפליקציה <https://www.alberta.ca/ab-trace-together-faq.aspx>

⁵⁵ להודעה הרשמית ראו https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/

⁵⁶ <https://globalnews.ca/news/7079851/coronavirus-tracing-app-launch-nationally/>

⁵⁷ https://blog.google/documents/63/Exposure_Notification_-_FAQ_v1.0.pdf





84. בחודש מאי 2020, פרסמו החברות תנאי שימוש חדשים ובהם הן מתנות את השימוש בממשק שלהן בכך שהשירות יינתן לרשות ממשלתית רשמית, במטרה להתמודד עם משבר הקורונה, בכפוף לקבלת הסכמת המשתמשים להורדת הממשק, קבלת הסכמת משתמשים אשר חלו להעביר דרך הממשק הודעה על דבר מחלתם, היעדר גישה לנתוני מיקום של משתמשים, הימנעות מאיסוף פרטים מזהים לרבות מספרי טלפון ועוד.⁵⁸
85. החברות מתנות את הגישה לממשק, בכך שמדינות המבקשות לעשות בו שימוש יתיישרו עם מדיניות הפרטיות שלהן הכוללת מודל BLE מבוזר, איסור על איסוף מידע מזהה כגון מספר טלפון, ואיסור על איסוף נתוני מיקום.
86. מדיניות זו של החברות אינה תואמת את המודל הריכוזי בו בחרו מדינות כמו אנגליה, צרפת ואוסטרליה, ולכן בשלב זה לא ניתנה לאפליקציות של מדינות אלה גישה לממשק, למרות שמתקיימים מגעים בין רשויות הבריאות של מדינות אלה לחברות.
87. נציין כי רשות הגנת המידע הבריטית, ה-ICO, בחנה את הפלטפורמה והתרשמה כי היישום משמר עקרונות פרטיות⁵⁹, אם כי ציינה את העובדה שהאפליקציה ממשיכה לפעול גם כאשר משתמש כיבה את מוד ה-Bluetooth.

<https://techcrunch.com/2020/05/04/apple-and-google-release-sample-code-and-detailed-policies-for-covid-19-exposure-notification-apps/>
<https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf>

