המכון הישראלי לדמוקרטיה

www.idi.org.il

מר אמיר אלשטיין
יו"ר הוועד המנהל
מר יוחנן פלסנר
נשיא
מר ברנרד מרכוס
יו"ר בינלאומי
פרופ' גרהרד קספר
יו"ר המועצה הבינלאומית
ד"ר ג'ורג' שולץ
יו"ר של כבוד

חברי הוועד המנהל
פרופ' ורד וניצקי-סרוסי
מר חן ליכטנשטיין
גב' מזל מועלם
מר סלי מרידור
עו"ד אבי פישר
מר אביעד פרידמן
ד"ר מיכל צור
מר יוסי קוצ'יק
מר עימאד תלחמי

המועצה הבינלאומית
השופטת רוזלי סילברמן אבלה, קנדה
מר אליוט אברמס, ארה"ב
ד"ר מרטין אינדיק, ארה"ב
גב' אן אפלבאום, ארה"ב
פרופ' ורנון בוגדנור, בריטניה
השופטת דורית ביניש, ישראל
השופט סטיבן ברייר, ארה"ב
השופט סלים ג'ובראן, ישראל
ד"ר איימי גוטמן, ארה"ב
ד"ר ג'וזף ג'ופה, גרמניה
פרופ' רונלד דניאלס, ארה"ב
פרופ' משה הלברטל, ישראל
פרופ' מייקל וולצר, ארה"ב
פרופ' רוברט מנוקין, ארה"ב
פרופ' כריסטוף מרקשיס, גרמניה
השופט אברהם סופר, ארה"ב
מר ברט סטפנס, ארה"ב
פרופ' ארווין קוטלר, קנדה
פרופ' יהודה ריינהרץ, ארה"ב
פרופ' גבריאלה שלו, ישראל

סגני נשיא
ד"ר ישי (ג'סי) פרס, אסטרטגיה
פרופ' קרנית פלוג, מחקר
פרופ' יובל שני, מחקר

עמיתים בכירים
פרופ' תמר הרמן
פרופ' מוסטפא כבהא
פרופ' עמיחי כהן
פרופ' יותם מרגלית
פרופ' עליה פישר
פרופ' יובל פלדמן
פרופ' מרדכי קרמניצר
פרופ' גדעון רהט
ד"ר תהילה שוורץ אלטשולר
פרופ' ידידיה צ' שטרן
פרופ' איתן ששינסקי

מייסד ונשיא לשעבר
ד"ר אריק כרמון

15 מרץ 2020

עד אתמול זה נחשב "סטוקינג", היום קוראים לזה "חקירה אפידמיולוגית"

חוות דעת: שיקולי פרטיות באיסוף ובפרסום מידע במאבק במחלת הקורונה

ד"ר תהילה שוורץ אלטשולר, עו"ד רחל ארידור הרשקוביץ

מבוא

בעקבות מגפת הקורונה והניסיונות ההירואיים של רשויות המדינה למנוע את התפשטותה ואת הנזק שהיא עלולה לגרום, נוצר צורך לנהל "חקירות אפידמיולוגיות" הנוגעות לאזרחים ולהעביר את ממצאיהן לגורמים הרלוונטיים, וכן לאכוף את הוראות הבידוד כאשר מתעורר הצורך בכך. צעדים אלו מעלים שאלות נרחבות הנוגעות לגישה למידע פרטי, פרסומו, עיבודו ושמירתו.

ניתן להגן על הזכות לפרטיות ועדיין לאפשר מימוש של אינטרסים ציבוריים חשובים כגון בריאות הציבור והגנה עליו בעת התמודדות המדינה עם מגפה עולמית. חשוב ליישם את ההגנה על הזכות באופן ראוי, להבין את חשיבותה ולא לראות בה מכשול שיש להסיר – לא בעת חירום ולא בעת שגרה.

מתוך הבנת ההכרח שבאיסוף הנתונים ובפרסום האזהרות, יש צורך לתת בידי משרד הבריאות כלים נכונים ומידתיים. במסמך זה נמפה אפוא את הסוגיות המרכזיות המתעוררות ואת המסגרת החוקית שיש לפעול לפיה, ואחר כך נציע דרכי פעולה.

לפני כן נבהיר: השימוש בטכנולוגיות זמינות הוא מתבקש בעידן של לוחמה במגיפה. ואולם נדרשת תשומת לב לשני הקשרים – ההקשר האחד הוא בחירת דרכי השימוש בטכנולוגיה, התפעול שלה והפיקוח על השימוש. ההקשר השני הוא הצורך בהסברה ציבורית לגבי האמצעים שננקטים. הרווח משימוש במידע לטיפול במגיפה יצא בהפסדו אם לא יהיה אמון ציבורי בכך שהמידע נאסף באופן שקוף, גלוי, בהיר ושלא נעשים בו שימושים לא ראויים.

1. <u>המסגרת החוקית לביצוע חקירות אפידמיולוגיות ומעקב אחר מי שיש חשש כי הוא מפר הוראות בידוד</u>

סעיף 20 לפקודת בריאות העם המנדטורית משנת 1947 מסמיך את שר הבריאות להכריז על מחלה מידבקת ומסוכנת כמחלה שנשקפת ממנה סכנה חמורה לבריאות העם. **סמכויות אלו, שעשויות להיחשב סמכויות חירום לאחר ששר הבריאות עשה שימוש בסמכותו והכריז על הקורונה כעל מגיפה בצו רשמי, כפופות לחוקי היסוד של המדינה ולזכויות המנויות בהם, ובכלל**

זה הזכות לפרטיות. לכן, גם אם מדובר בפגיעה מכוח פקודת בריאות העם, והתכלית שלה ראויה – הגנה על הבריאות של כולנו – עדיין הפגיעה צריכה להיות מידתית.

אסור לאפשר למצב חירום להפוך לכלי למעקב המוני אחר האוכלוסייה, כפי שפורסם באמצעי התקשורת אמש. לפיכך חשוב להבין באילו מקרים יכולות להתבצע פגיעות בפרטיות, מהי המסגרת הנכונה להפעלתן, ומה תוחם אותן.

2. הסוגיות המרכזיות הנוגעות לפרטיות

1. קבלת מידע בהסכמה

כפי שעולה מראיונות שניתנו בתקשורת על ידי אנשי משרד הבריאות,[1] במסגרת החקירה מתבקשים חולים מאומתים להעביר מידע על המקומות ששהו בהם בתקופה שלפני גילוי המחלה, ולאפשר לרשויות הבריאות לאמת את המידע הזה באמצעות חברות אשראי, נתוני מיקום ומצלמות. כן הם נדרשים לדווח על אנשים שבאו איתם במגע בתקופה זו. לכאורה, מידע פרטי שנמסר בהסכמה אינו בעייתי לפי סעיף 1 לחוק הגנת הפרטיות, במקרה שמדובר בהסכמה חופשית, מרצון ומדעת. יש להניח גם כי הרוב המוחלט של החולים ימסרו את המידע כי לא ירצו להזיק לאחרים. אבל מאחר שמשרד הבריאות מפעיל סמכויות מכוח פקודת בריאות העם, והיעדר הסכמה למסור מידע יכול לגרור העמדה לדין פלילי וסנקציות, קשה לראות כיצד ההסכמה היא חופשית. לפיכך לתפיסתנו **אסור למשרד הבריאות להסתמך רק על ההסכמה של החולים למסור לו מידע** אלא יש לבסס סמכות חוקית לכל איסוף של מידע פרטי לצורכי ההתמודדות עם המגפה. סמכות חוקית זאת קיימת, כאמור, מכוח הפקודה.

2. פרסום מידע פרטי על חולים מאומתים כדי להזהיר את הציבור

בכלי התקשורת מתפרסמים הנתיבים שבהם פסעו חולים מאומתים בימים שלפני גילוי המחלה, כדי שמי שבאו איתם במגע יוכלו להיכנס לבידוד. החולים אינם מוזכרים בשם אלא במספר (למשל, חולה מס' 29), ולכאורה הם נשארים אנונימיים אף שפרטיהם האישיים נחשפים לעין כול. אלא שהיכולת לבצע "זיהוי חוזר" של החולים היא גדולה, במיוחד במדינה קטנה כמו מדינת ישראל. ראוי לזכור שאם מתקיים זיהוי חוזר כזה, המידע הפרטי שמתפרסם נשאר לתמיד, משום שהתפרסם בכלי התקשורת ובאינטרנט, להבדיל ממידע שנאסף על ידי משרד הבריאות וניתן, כפי שנסביר להלן, לדרוש למחוק אותו. עשוי גם להתקיים נזק תדמיתי וכלכלי לבתי עסק, אם כל חיפוש עתידי יעלה שחולה כלשהו שהה בהם, ניהל אותם וכיוצא בזה.[2]

---

[1] ראו למשל רוני לינדר, "אדם חוטף שוק כשנודע לו שהוא חולה קורונה, יש מקרי הסתרה", **TheMarker**, 8.3.2020.

[2] ראו למשל את תיאור הפגיעות בפרטיותם של חולי קורונה מאומתים בקוריאה הדרומית עקב פירוט מסלול חייהם לציבור. Nemo Kim, "*More Scary Than Coronavirus:" South Korea's Health Alerts Expose Private Lives*, The Guardian (March 6, 2020)

כפי שעולה מראיונות שונים שניתנו לתקשורת על ידי אנשי משרד הבריאות[3], במסגרת החקירה מתבקשים חולים מאומתים להעביר מידע על מקומות ששהו בהם במהלך התקופה שלפני גילוי המחלה, ולאפשר לרשויות הבריאות לאמת את המידע הזה באמצעות חברות אשראי, נתוני מיקום ומצלמות. כן הם נדרשים לדווח על אנשים שבאו איתם במגע במהלך התקופה הזאת. לכאורה, מידע פרטי שנמסר בהסכמה אינו בעייתי לפי סעיף 1 לחוק הגנת הפרטיות, ככל שמדובר בהסכמה חופשית, מרצון ומדעת. אבל, כאשר משרד הבריאות מפעיל סמכויות מכוח פקודת בריאות העם, והיעדר הסכמה למסור מידע יכול לגרור העמדה לדין פלילי וסנקציות, קשה לראות כיצד ההסכמה היא חופשית.

לפיכך, לתפיסתנו **אסור למשרד הבריאות לסמוך על ההסכמה של החולים למסור לו מידע** אלא יש לבסס סמכות חוקית לכל איסוף של מידע פרטי לצרכי התמודדות עם המגיפה. לכן, אין הבדל בין מידע שנאסף "בהסכמת" אדם לבין מידע שרשויות הבריאות אספו מיוזמתן וללא הסכמה, וההסדרים לגביהם צריכים להיות זהים: מה מותר לאסוף ובאלו תנאים.

מעיון בלקחי המאבק בהתפשטות מגפת הקורונה בדרום קוריאה לאחרונה אף נמצא שמרבית האזרחים חששו יותר מעצם מהפרסום האנונימי לכאורה של סדר יומם בציבור מאשר מההדבקות בווירוס עצמו. בנוסף, עשוי להתקיים נזק תדמיתי וכלכלי לבתי עסק אם כל חיפוש עתידי יוביל לכך שחולה מסויים שהה בהם, ניהל אותם וכיוצא בכך.[4]

לכן, לתפיסתנו, יש לאסור פרסום פרטים רגישים במיוחד[5] או שעלולים לפגוע בפרטיות סביבת החולה (במקרים כאלה, ראוי לאתר באמצעים אחרים את מי שעשוי היה להיחשף לחולה ולהודיע לו באופן פרטי, גם אם מדובר בפעילות מורכבת יותר), **ואין לפרסם זאת לציבור**.

לכן, לתפיסתנו, יש לאסור פרסום פרטים רגישים במיוחד או שעלולים לפגוע בפרטיות סביבת החולה, [6] הימצאותו במקומות פרטיים או במקומות ציבוריים מסויימים כגון חדר דיסקרטי בבית מלון; ביקור במרפאה לצורך טיפול במחלה אחרת; פגישה אצל בעל מקצוע רגיש אחר כגון פסיכולוג; ביקור במועדונים מסוגים מסויימים המזהים נטייה מינית. במקרים כאלה ראוי לאתר את מי שעשוי היה להיחשף לחולה באמצעים אחרים ולהודיע לו באופן פרטי, גם אם מדובר בפעילות מורכבת יותר, **ואין לפרסם זאת לציבור**.

ככל שמימד הזמן יביא אותנו משלב המניעה הראשוני שבו החקירה אפידמיולוגית חשובה ויעילה לשלב הגידול האקספוננציאלי – תלך ותיעלם ההצדקה לפרסם לציבור מידע פרטי כזה.

---

[3] ראו למשל כאן: https://www.themarker.com/allnews/.premium-1.8637388

[4] ראו למשל תיאור הפגיעות בפרטיותם של חולי קורונה מאומתים בדרום קוריאה עקב פירוט מסלול חייהם לציבור Nemo Kim, *'More Scary Than Coronavirus': South Korea's Health Alerts Expose Private Lives*, THE GUARDIAN (March 6, 2020).

[5] מידע רגיש מוגדר בחוק הגנת הפרטיות בסעיף 7: נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

[6] מידע רגיש מוגדר בחוק הגנת הפרטיות בסעיף 7 כך: "נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו".

המכון הישראלי לדמוקרטיה

3. **<u>איסוף מידע פרטי באופן יזום על ידי רשויות משרד הבריאות</u>**

איסוף המידע יכול להתבצע ממגוון מקורות מידע:

- גופים פרטיים (למשל חברות הסלולר, חברות אשראי, חנויות, מסעדות, עסקים אחרים);
- רשויות מדינה אחרות (למשל רשות האוכלוסין);
- גופים מפוקחים על ידי המדינה (למשל חברת רב קו).

מטרותיו הן:

- לוודא ולדייק את דבריו של חולה מאומת, או כאשר מתעורר חשש שחולה מאומת לא דיבר אמת בחקירה אפידמיולוגית;
- לאסוף מידע לצורך אזהרה של מי ששהו בקרבת חולה מאומת;
- לוודא עמידה בדרישת הוראות הבידוד.

<u>המדובר בסוגי מידע פרטי כמתואר להלן:</u>

א. **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. היסטוריית מיקום ונסיעות הנמצאת אצל פלטפורמות האינטרנט, ובראשן גוגל תאפשר דבר דומה. קיימת גם אפשרות לחייב כל חולה קורונה מאומת וכל סביבתו הקרובה להוריד לסלולרי שלהם אפליקציות מסוגים שונים שיאפשרו מעקב אחריהם, כדי לאתר היכן שהו בדיעבד וכדי לוודא עמידה בדרישות הבידוד.

נסביר: כאשר מגיע חולה מאומת יש צורך בבדיקה היכן שהה בארבעה עשר הימים האחרונים. הדרך היעילה לבצע זאת היא באמצעות חקירה של הטלפון הסלולרי שלו, באמצעים הנמצאים בידי חברות הסלולר. המידע המועבר לידי חברת הסלולר מאפשר לה לומר מי שהה בקרבתו באותו "תא" סלולרי, למשך יותר מחמש עשרה דקות. מידע כזה מאפשר לפנות אל מי ששהו בקרבתו ולהורות להם להיכנס לבידוד באמצעות הודעות סמס; להצליב ולהבין מה פוטנציאל ההדבקה במידה וחולה כזה שהה במקום הומה אדם; ולדעת בצורה טובה יותר היכן סביר שנדבקו חולים חדשים שנדבקו בארץ.

איכון טלפונים סלולריים, כלומר מעקב אחר מיקום האדם לפי הטלפון שלו, הוא מידע שנמצא בידי חברות הסלולר. חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת) (להלן: "**חוק נתוני תקשורת**") מסדיר את אפשרות העברת הנתונים האלה מאד בזהירות משום שהם מהווים מכלול

של מידע רגיש.[7] העברה של נתוני תקשורת נעשית במקרי קיצון, מכוח צו בית משפט שלום, בין השאר לצורך הצלת חיי אדם, כאשר לרוב מדובר בהצלת חיי אדם קונקרטי[8]. החוק קובע גם הליך מהיר ודחוף בלא צו בית משפט, כשקצין משטרה בכיר משוכנע שמדובר בצורך דחוף שאינו סובל דיחוי וזאת ל- 24 שעות בלבד[9]. בכל מקרה החוק דורש הקפדה על סודיות המידע בעת השימוש בו והחזקתו, והתרת גישה רק למי שמורשה לכך.

הפעלת סמכות החירום מכוח פקודת בריאות העם כדי לעקוף את ההסדרים שבחוק נתוני תקשורת, צריכה להתקיים תוך נקיטת אמצעי האבטחה המתאימים ומיזעור הפגיעה הצפויה בזכות לפרטיות. נתוני מיקום מהווים מידע אישי רגיש לפי הגדרתו בחוק הגנת הפרטיות. עם זאת, איסוף ושימוש במידע רגיש מותר בנסיבות מסוימות גם לפי חקיקת הגנת הפרטיות העדכנית ביותר כיום – תקנות הגנת הפרטיות האירופאיות – ה"GDPR" ונדרש כי השימוש יהיה מעוגן בחוק, יכלול אמצעי אבטחה מתאימים, ושיתקיים אינטרס ציבורי בשימוש במידע, בייחוד בהקשר של מניעה או השתלטות על מחלות מדבקות.[10] כאמור, מבחינתנו ההסמכה בפקודת בריאות העם עשויה להוות מקור חוקי כזה, אבל יש לפעול ליישם אותו בהתאם לכללים שנפרט להלן.

ב. **גישה להיסטוריית קניות דרך חברות האשראי** תאפשר למשרד הבריאות לקבל מידע אישי אודות הזמן והמקום שבו רכשו חולים, או מי שיש חשד שנמצאו בסביבתם, מוצרים בבתי עסק; גישה ישירה לנתונים של בתי עסק ומקומות שמהם נרכשו מוצרים ושירותים אחרים, כגון חנויות, מסעדות, כרטיסים למשחקי ספורט ואירועי תרבות תאפשר לדעת מתי והיכן היו חולים או מי שהיו במגע עמם.

ג. **זיהוי פנים** דרך מצלמות במרחב הציבורי ובבתי עסק יאפשר לדעת מתי והיכן הסתובב חולה מאומת וכן לזהות אחרים שהיו בסביבתו ולהעריך את המרחק שלהם ממנו; זיהוי פנים דרך מצלמות גוף של שוטרים יוכל לאפשר מידע האם אדם מסויים מפר הוראת בידוד; זיהוי פנים מתקדם יוכל לומר האם לאדם מסויים יש חום גוף גבוה, כפי שנעשה בסינגפור.

ד. מעקב אחר **כניסות ויציאות מהמדינה** – מידע הנמצא בידי רשות האוכלוסין במשרד הפנים – יאפשר לדעת מי יצא ומי נכנס ומתי ולכן לדעת מתי חלה חובת בידוד.

ה. **שילוב מידע עם מאגרי מידע נוספים** – למשל מאגרי מידע בריאות, נתונים נוספים שנמצאים בידי מרשם האוכלוסין כגון נתוני גיל או מקום מגורים. האפשרות להצליב בין

---

[7] סעיף 23יט(א) להצעת חוק הגנת הפרטיות (תיקון מס' 13).
[8] סעיף 3 לחוק נתוני תקשורת; בג"ץ 3809/08 האגודה לזכויות האזרח נ' משטרת ישראל.
[9] סעיף 4 לחוק נתוני תקשורת.
[10] סעיף הקדמה 52 ל-GDPR.

אדם שזוהה על ידי איכון הטלפון שלו כמי שנמצא בסביבת חולה מאומת, יחד עם מידע על הגיל שלו או היסטוריה רפואית יכולה להביא למידע האם הוא בקבוצת סיכון.

4. המלצות

לצד מתן הכלים המתאימים בידי משרד הבריאות לשם הגנה על בריאות הציבור, הכרחי ליישם את סמכותו לאסוף מידע פרטי מתוך נקיטת אמצעי האבטחה המתאימים ומזעור הפגיעה הצפויה בזכות לפרטיות. העיקרון המרכזי שצריך להנחות את איסוף המידע בהקשר שלנו הוא עקרון "העיצוב לפרטיות" (Privacy By Design) [11]. עיקרון זה מעוגן גם ב-GDPR (General Data Protection Regulation; האסדרה הכללית להגנה על מידע),[12] מאוזכר ומוטמע בהנחיות של הרשות להגנת הפרטיות ובפרויקטים ציבוריים כגון מערכת הסליקה הפנסיונית, המאגר הביומטרי ומערכת הרב-קו.

א. שימוש בנתוני איכון ומיקום סלולריים:

כאשר מדובר על איתור מבודדים ושמירה שלא יעזבו את מקום הבידוד שלהם:

1. יש להגדיר מנגנון ברור ושקוף לאופן הגשת הפנייה ממשרד הבריאות לחברות הסלולר לשם קבלת המידע הדרוש וליצור הגדרה ברורה של פרטי המידע שמשרד הבריאות דורש את העברתם.
2. חובה על משרד הבריאות להודיע באופן יזום וברור לכל מי שמתבצע מעקב ספציפי אחר נתוני המיקום שלו או שהוגשה בקשה לחברות אחרות לקבל נתונים אחרים על אודותיו.
3. יש להגדיר מראש מי רשאי לגשת למידע שנאסף, הן במשרד הבריאות הן בחברות או בגופים שמהם מתבקש המידע. מורשי הגישה יחויבו בחתימה על טופס מיוחד לשמירה על סודיות המידע.
4. נדרש שהמידע יועבר ויישמר במאגר מידע שבידי משרד הבריאות באופן מאובטח בהתאם להוראות שבתקנות אבטחת מידע.[13] פרק הזמן שבו יישמר המידע בידי משרד הבריאות לא יעלה על תקופה של 30 ימים – תקופת הבידוד והמחלה; בתום פרק זמן זה על משרד הבריאות להשמיד את המידע שהועבר אליו.
5. על חברות הסלולר וחברות פרטיות אחרות להעביר את המידע הדרוש בהתאם לפניית משרד הבריאות ולשמור ברשותן את פניית משרד הבריאות באופן מאובטח

---

[11] רותם מדזיני "סוף פרטיות במחשבה תחילה: על הנדסת פרטיות והדרכים למימושה" 83 **פרלמנט** (אתר המכון הישראלי לדמוקרטיה; 27 בינואר 2019).
[12] סעיף 25 ל-GDPR.
[13] תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

ולתקופת הזמן הנדרשת לשם ביסוס טענת הגנה משפטית במקרה שייתבעו בגין העברת המידע.

6. חברות הסלולר, האשראי וחברות פרטיות אחרות ומשרד הבריאות ימנו, כל אחד בנפרד, ממונה הגנת פרטיות אשר יפקח על מנגנון הפנייה, השימוש ואבטחת המידע אישי.
7. כאשר מדובר במידע אולטרה-רגיש, ניתן לשקול שיתוף פעולה שקוף בין משרד הבריאות לבין חברות הסלולר והאשראי, או חברות בגון גוגל, שבמסגרתו יקבלו החברות נתוני מיקום וזמן מדויקים והן תהיינה אחראיות לאיתור, זיהוי וגם לאזהרה של מי שנחשפו לחולה מאומת.

כאשר מדובר על השגת מידע רחב היקף במסגרת חקירה אפידמיולוגית – מי שהה בקרבת חולה מאומת:

1. לתפיסתנו, הדרך הראשונה להשגת המידע צריכה להיות באמצעות משלוח לינק ובו אפליקציה דרך חברות הסלולר. מדובר באפליקציה שיושבת על כרטיס הסים של כל משתמש וכל אחד יתבקש להתקין אותה. האפליקציה תדאג לאגור את כל מידע המיקום על כרטיס הסים ארבעה עשר יום לאחור ולאחר מכן תמחוק אותו. כאשר מגיע חולה מאומת יילקח כרטיס הסים שלו ונתוני המיקום ייבדקו ויוצלבו עם הנתונים שבידי חברות הסלולר. חברות הסלולר ישלחו הודעה לכל מי שנמצא בתא סלולרי זהה בזמן זהה שעליו להיכנס לבידוד.

2. הואיל והמשטרה והשב"כ הם גופים שעשוי להיות להם עניין להמשיך ולהחזיק במידע, והסמכויות המסורות להם, במיוחד לשב"כ, רחבות מאד ולא שקופות. אנו מציעות להעביר את המידע למשטרה, למשרד הבריאות ואף לפיקוד העורף ורשות החירום הלאומית (שיש להם תשתית יכולות טיפול בנתונים כאלה לשעת חירום אחרת, כמו רעידת אדמה). אבן, לשב"כ יכולות טכנולוגיות מיידיות והוא גם יכול לקבל חיבור ישיר אל תשתית הסלולר. אבל לתפיסתנו השימוש בשב"כ בעת הזאת יפעיל סמכות דרקונית שאיננה נדרשת ושחסרונותיה – הן בהיבט של אמון הציבור במערכת, הן בהיבט של חוסר השקיפות המאפיין את הגוף והן בהיבט של האינטרס לשמור את המידע לצרכי חקירות אחרים בעתיד – עולים על יתרונותיה.

3. במקום זאת אנו מציעות שחברות הסלולר יצטרכו להעביר פעם בעשרים וארבע שעות לאחור קובץ נתוני מיקום. פיקוד העורף, משרד הבריאות יוכלו להפעיל מערכת שאילתות על הקובץ. אפשר אפילו לחשוב על הפרדה בין מספר הטלפון ומספר הסים, כך שלגוף אחד יינתנו נתוני המיקום (משטרה או פיקוד העורף) ולגוף אחר (משרד הבריאות) יינתן המפתח להפוך את מספרי הסים למספרי טלפון.

המכון הישראלי לדמוקרטיה

השגת מידע מגופים ציבוריים אחרים

1. מדובר בעיקר במידע ממשרד הפנים על כניסות ויציאות מן הארץ או מידע אחר ממרשם האוכלוסין, וכן מידע מתוך מצלמות במרחב הציבורי שנמצא בידי רשויות מקומיות, עיריות וגופים כגון בתי חולים. כן עשויה להיות העברת מידע בריאות מקופות חולים (למשל כדי לדעת האם מדובר באוכלוסיית סיכון עם מחלות רקע). העברת מידע כזה צריכה להיות כפופה להוראות שבפרק ד לחוק הגנת הפרטיות.
2. העברת המידע תהיה באישור ועדה שבראשה יעמוד מנכ"ל משרד הפנים; יש להקפיד שיועבר רק המידע שיש בו צורך מידתי וסביר ושיובטח כי הגישה למידע תהיה מצומצמת ומפוקחת.
3. מידע ממרשם האוכלוסין ומידע בעניין כניסות ויציאות המועבר ממשרד הפנים אל משרד הבריאות או מידע מתוך מצלמות של רשויות ציבוריות יישמר באופן מאובטח ויימחק גם הוא לאחר 21 ימים.
4. מידע בריאות יועבר באישור מנכ"לי קופות החולים, ויימחק גם הוא לאחר 21 יום.

העברת מידע אל המשטרה

1. אם לא מוכרז מצב חירום אזרחי , הכללים והמגבלות החלים על המשטרה בתפקידה כגוף חוקר אינם שונים מאלה החלים עליה בשגרה. נזכיר כי המשטרה פועלת כבר תקופה ארוכה ללא מפכ"ל קבוע, וכי יש לה היסטוריה עגומה של טיפול במאגרים ושל הדלפות מידע מהם. לכן:
2. אין להתיר גישה גורפת של כל שוטרי משטרת ישראל למידע שהושג אלא יש לקבוע הרשאות גישה קונקרטיות לפי סוגי מידע שונים.
3. יש לחייב הודעה באופן מיידי ואוטומטי למי ששוטר ניגש אל פרטי האיכון או פרטים אחרים שלו .
4. יש להגביל את האפשרות להעביר נתונים כאלה למאגר מידע אחר או להצליב אותם עם מידע אחר.
5. יש לקבוע הוראות לעניין מחיקת הנתונים תוך 21 יום במקרה שהם נשמרים ומנגנון פיקוח על המחיקה. יש לקבוע קריטריונים קשיחים לאבטחת מאגר המידע שבו יישמרו לגישה עליו וליכולת להדליף מתוכו.
6. יש לקבוע פיקוח פרלמנטרי הדוק על כל הפעולות האלה מצד וועדה פרלמנטרית מיוחדת שתוקם לצורך כך בכנסת באופן מיידי.

הפעלת השב"כ וגופי ביטחון חשאיים אחרים

7. **לתפיסתנו אין לערב את השב"כ בפעילות מעקב בעת הזאת**. ככל שמדובר במעקב אחר ציות להוראות הבידוד, ממילא השב"כ אינו הגוף לטפל בכך ואין לאפשר לו לבצע מעקב המוני אחר כל אזרחי ישראל. מדובר בצעד לא מידתי ולא חוקי שפוגע פגיעה קשה בפרטיות ומעביר לידי השב"כ מידע רגיש על כל האזרחים. יש למצות את טווח היכולות של משרד הבריאות, פיקוד העורף והמשטרה ולהיעזר בקבלני משנה לצורך הביצוע ככל שיש בכך צורך.
8. אכן, לפי חוק השב"כ יש אפשרות לעשות שימוש בנתוני תקשורת ללא צורך בצווים, אם הדבר דרוש לצרכי מילוי תפקידו לפי החוק. תפקידיו לפי סעיף 7 לחוק יכולים להיות "פעילות בתחום אחר שקבעה הממשלה, באישור ועדת הכנסת לענייני השירות, שנועדה לשמור ולקדם אינטרסים ממלכתיים חיוניים לביטחון הלאומי של המדינה" וכן "איסוף וקבלת מידע לשמירה ולקידום העניינים המפורטים בסעיף זה". אבל, תפיסה של מגיפה כאיום על הביטחון הלאומי היא תקדים מסוכן. לתפיסתנו עדיף להשתמש בטווח הסמכויות הרחב מכוח פקודת בריאות העם ולא להסמיך את השב"כ לטפל בכך. בכל מקרה של הפעלת השב"כ יידרש פיקוח פרלמנטרי הדוק של תת הוועדה לענייני שב"כ בכנסת ושל וועדה מיוחדת שתוקם לצורך כך בכנסת.