



```
object to mirror  
or_mod.mirror object  
ation = "MIRROR_X":  
or_mod.use_x = True  
or_mod.use_y = False  
eration = "MIRROR_Y"  
or_mod.use_x = False  
or_mod.use_y = True  
eration = "MIRROR_Z"  
or_mod.use_x = False  
or_mod.use_y = False  
or_mod.use_z = True  
ection at the end -add  
b.select= 1  
_ob.select=1  
ext.scene.objects.active  
ected" + str(modifier  
or_ob.select = 0  
py.context.selected_obj  
a.objects[one.name].sel  
t("please select exact)  
OPERATOR CLASSES  
pes:operator :  
X mirror the sea  
ect mirror "or x"  
or x"  
text):  
tive_object
```

שיקולי פרטיות ומעקב אחר אזרחים

תהילה שוורץ אלטשולר | רחל ארידור הרשקוביץ

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

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 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.

נבהיר: השימוש בטכנולוגיות זמינות הוא צורך מתבקש בזמנים של מלחמה במגפה. ואולם נדרשת תשומת לב לשני עניינים - האחד, בחירת דרכי השימוש בטכנולוגיה, התפעול שלה והפיקוח על השימוש בה; השני, הצורך בהסברה ציבורית לגבי האמצעים שנקטים. אם לא יהיה אמון ציבורי בכך שהמידע נאסף באופן שקוף, גלוי, בהיר ושלא נעשים בו שימושים לא ראויים, הנזק שייגרם יהיה גדול יותר מהתועלת שבשימוש במידע לטובת טיפול במגפה.

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

המסגרת החוקית לחקירות ומעקב

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 מגפה 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. לפיכך חשוב להבין באילו מקרים יכולות להתבצע פגיעות בפרטיות, מהי המסגרת הנכונה להפעלתן, ומה תוחם אותן.

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 רישומי חברות האשראי, 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 ששרד הבריאות מפעיל סמכויות מכוח פקודת בריאות העם, והיעדר הסכמה למסור מידע יכול לגרור העמדה לדין פלילי וסנקציות, קשה לראות כיצד ההסכמה היא

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

חופשית. לכן אין הבדל בין מידע שנאסף ב"הסכמת" אדם לבין מידע שרשויות הבריאות אספו מיזמתן וללא הסכמה, וההסדרים בעניינם צריכים להיות זהים: מה מותר לאסוף ובאילו תנאים. 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 נתונה, 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 מזכירים 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 שהופיע 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.

מעיון בלקחי המאבק בהתפשטות מגפת הקורונה בקוריאה הדרומית אף עולה שמרבית האזרחים חששו יותר מעצם הפרסום, האנונימי לכאורה, של סדר יומם בציבור מאשר מההידבקות בוירוס עצמו.²

לכן, לתפיסתנו, יש לאסור פרסום פרטים רגישים במיוחד או שעלולים לפגוע בפרטיות סביבת החולה,³ כמו הימצאותו במקומות פרטיים או במקומות ציבוריים מסוימים כגון חדר דיסקרטי בבית מלון; ביקור במרפאה לצורך טיפול במחלה אחרת; פגישה אצל בעל מקצוע רגיש אחר כגון פסיכולוג; ביקור במועדונים מסוגים מסוימים המזהה נטייה מינית. במקרים כאלה ראוי לאתר את מי שעשוי היה להיחשף לחולה באמצעים אחרים

2 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)

3 מידע רגיש מוגדר בחוק הגנת הפרטיות בסעיף 7 כן: "נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו".

ולהודיע לו באופן פרטי, גם אם מדובר בפעילות מורכבת יותר, ואין לפרסם זאת לציבור.

ככל שנעבור לאורך זמן משלב המניעה הראשוני שבו החקירה האפידמיולוגית חשובה ויעילה לשלב הגידול האקספוננציאלי - כך תלך ותיעלם ההצדקה לפרסם לציבור מידע פרטי כזה.

3. איסוף מידע פרטי באופן יזום על ידי משרד הבריאות

איסוף המידע יכול להתבצע ממגוון מקורות מידע:

- גופים פרטיים (למשל חברות הסלולר, חברות האשראי, 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.

מדובר בסוגי המידע הפרטי האלה:

- א. נתוני מיקום** ואיכון דרך חברות הסלולר יאפשרו למשרד הבריאות לקבל מידע אישי מזהה על חולה מאומת או על 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. אפשרי גם לחייב כל חולה קורונה מאומת, ואת סביבתו הקרובה, להוריד לסלולרי אפליקציות שיאפשרו מעקב אחריהם, כדי לאתר היכן שהו בדיעבד וכדי לוודא עמידה בדרישות הבידוד.
-

נסביר: במקרה שמתגלה חולה מאומת יש צורך בבדיקה היכן שהה ב־14 הימים האחרונים. הדרך היעילה לבצע זאת היא על ידי חקירה של הטלפון הסלולרי שלו, באמצעים שבידי חברות הסלולר. מידע זה מאפשר לומר מי שהה בקרבתו באותו "תא" סלולרי למשך יותר מ־15 דקות, ולפיכך לפנות לאנשים אלו ולהורות להם להיכנס לבידוד באמצעות הודעות SMS; להצליב מידע 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 כאמור מידע שנמצא בידי חברות הסלולר. חוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת) (להלן: "**חוק נתוני תקשורת**") מסדיר את אפשרות העברת הנתונים האלה בזירות רבה, משום שהם מהווים מכלול של מידע רגיש.⁴ העברה של נתוני תקשורת נעשית במקרי קיצון, מכוח צו בית משפט שלום, בין השאר לצורך הצלת חיי אדם, ולרוב מדובר בהצלת חיי אדם קונקרטי.⁵ החוק קובע גם הליך מהיר ודחוף בלא צו בית משפט, כשקצין משטרה בכיר משוכנע שמדובר בצורך דחוף שאינו סובל דיחוי, ל־24 שעות בלבד.⁶ 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 מתוך נקיטת אמצעי האבטחה המתאימים ומזעור הפגיעה הצפויה בזכות הפרטיות. נתוני מיקום הם מידע אישי רגיש לפי הגדרתו בחוק הגנת הפרטיות. עם זאת, איסוף ושימוש במידע רגיש מותרים בנסיבות מסוימות גם לפי חקיקת הגנת הפרטיות העדכנית ביותר כיום - תקנות הגנת הפרטיות האירופיות, ה־GDPR (General Data Protection Regulation) - ונדרש כי השימוש יהיה מעוגן בחוק, יכלול אמצעי אבטחה

4 סעיף 23ב(א) להצעת חוק הגנת הפרטיות (תיקון מס' 13).

5 סעיף 3 לחוק נתוני תקשורת; בג"ץ 3809/08 האגודה לזכויות האזרח נ' משטרת ישראל.

6 סעיף 4 לחוק נתוני תקשורת.

מתאימים, ושיתקיים אינטרס ציבורי בשימוש במידע, בייחוד בהקשר של מניעה או השתלטות על מחלות מידבקות.⁷ כאמור, מבחינתנו ההסמכה בפקודת בריאות העם עשויה לשמש 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 על 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 עימם.

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 אם אדם כלשהו מפר הוראת בידוד; זיהוי פנים מתקדם יוכל לומר אם לאדם כלשהו 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. הצלבת מידע עם מאגרי מידע נוספים. למשל מאגרי מידע בריאות ונתונים

נוספים שנמצאים בידי מרשם האוכלוסין כגון נתוני גיל או מקום מגורים. האפשרות להצליב מידע על אדם שזוהה על ידי איכון הטלפון שלו כמי שנמצא בסביבת חולה מאומת, עם מידע על הגיל שלו או ההיסטוריה הרפואית יכולה לגלות אם הוא בקבוצת סיכון.

7 טעיף הקדמה 52 ל-GDPR.

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).⁸ עיקרון זה מעוגן גם ב-GDPR,⁹ מאזכר 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 באיתור אנשים הנמצאים בבידוד ושמירה שלא יעזבו את מקום הבידוד שלהם:

- 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.
- 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.
- 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.
- נדרש שהמידע יועבר ויישמר במאגר מידע שבידי משרד הבריאות באופן מאובטח בהתאם להוראות שבתקנות אבטחת מידע.¹⁰ פרק הזמן שבו

8 רותם מדיני "סוף פרטיות במחשבה תחילה: על הנדסת פרטיות והדרכים למימושה" 83 פרלמנט (אתר המכון הישראלי לדמוקרטיה; 27 בינואר 2019).
9 סעיף 25 ל-GDPR.
10 תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

המידע יישמר 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 ולתקופת הזמן הנדרשת לשם ביסוס טענת הגנה משפטית במקרה שייטבעו 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 כגון גוגל, שבמסגרתו יקבלו החברות נתוני מיקום חמן מדויקים והן תהיינה אחראיות לאיתור, זיהוי וגם לאזרה של מי שנחשפו לחולה מאומת.

כאשר מדובר בהשגת מידע רחב היקף במסגרת חקירה אפידמיולוגית - מי שזה בקרבת חולה מאומת:

1. לתפיסתנו, הדרך הראשונה להשגת המידע צריכה להיות באמצעות משלוח לינק דרך חברות הסלולר להתקנת אפליקציה. מדובר באפליקציה שיושבת על כרטיס הסיים של כל משתמש שהציבור יתבקש להתקין. האפליקציה תדאג לאגור את כל מידע המיקום על כרטיס הסיים 14 יום לאחור ולאחר מכן תמחק אותו. כאשר יאותר חולה מאומת יילקח כרטיס הסיים 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 והמטרה והשב"כ הם גופים שעשוי להיות להם עניין להמשיך ולהחזיק במידע, והסמכויות המסורות להם, במיוחד לשב"כ, רחבות מאוד ולא שקופות. אנו מציעות להעביר את המידע למטרה, למשרד הבריאות ואף לפיקוד העורף ורשות החירום הלאומית (שיש להם תשתית לטיפול בנתונים כאלה לשעת חירום אחרת, כמו רעידת אדמה). אכן, 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 המאפיינ את הגוף והן בהיבט של האינטרס לשמור את המידע לצורכי חקירות אחרות בעתיד – עולים על יתרונותיה.

3. במקום זאת אנו מציעות שחברות הסלולר יצטרכו להעביר פעם ב־24 שעות קובץ עם נתוני מיקום. פיקוד העורף ומשרד הבריאות יוכלו להפעיל מערכת שאילתות על הקובץ. אפשר אפילו לחשוב על הפרדה בין מספר הטלפון ומספר הסיים, כך שלגוף אחד יינתנו נתוני המיקום (מטרה או פיקוד העורף) ולגוף אחר (משרד הבריאות) יינתן המפתח להפוך את מספרי הסיים למספרי טלפון.

ב. 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 אם 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 ממשד 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"ל קופות החולים ויימחק גם הוא לאחר 21 יום.

ג. 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 מידי 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 בתוך 21 יום במקרה שהם נשמרים ומנגנון פיקוח על המחיקה. יש לקבוע קריטריונים קשיחים לאבטחת מאגר המידע שבו יישמרו, לגישה אליו וליכולת להדליף מתוכו.

6. יש לקבוע פיקוח פרלמנטרי הדוק על כל הפעולות האלה מצד ועדה פרלמנטרית מיוחדת שתוקם לצורך כך בכנסת באופן מיידי.

ד. הפעלת השב"כ וגופי ביטחון חשאיים אחרים

1. 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.

2. אכן, חוק השב"כ מתיר לעשות שימוש בנתוני תקשורת ללא צורך בצווים, אם הדבר דרוש לצורכי 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 מגפה 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 התת-ועדה לענייני שב"כ בכנסת ושל ועדה מיוחדת שתוקם לצורך כך בכנסת.

סקירה השוואתית

הוויכוח באשר לאמצעי המעקב הדיגיטליים שממשלת ישראל בחרה לאמץ במסגרת המאבק בנגיף הקורונה, בדמות תקנות שעת חירום (הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף קורונה החדש), התש"ף-2020, מחייב להתבונן בנעשה במדינות אחרות. בסקירה זו בדקנו, במגבלות הזמן הקצר שעמד לרשותנו, את ההסדרים במדינות שהתמודדו עם הנגיף עד כה ואת האמצעים שנקטו מכוחם.

מן הממצאים עולה התמונה הזאת:

- בחלק ניכר מן המדינות יש חקיקה ייעודית ומעודכנת לטיפול במגפות, שבתוכה קבועות גם דרכי התמודדות עם איסוף מידע בעת מגפה. בישראל אין חקיקה כזאת, והסעיפים הרלוונטיים בפקודת בריאות העם 1940 אינם מעודכנים.
- במדינות שנבדקו, למעט סינגפור וסין, יש חקיקת הגנת פרטיות מעודכנת, ורובה גם בתהליך של תאימות עם תקנות הגנת המידע האירופיות (GDPR).
- בכל המדינות נעשה שימוש בטכנולוגיות שונות של איסוף מידע ושל מעקב כדי להתמודד עם המגפה. רוב השימוש הוא בנתוני איכון של טלפונים סלולריים.
- אמצעי מעקב בדמות שימוש בנתונים של איכון סלולריים לצורך מעקב אחר אדם ספציפי לטובת חקירה אפידמיולוגית או אכיפת בידוד מתבצעים במרבית המדינות, אם כי בכל מקום שהדבר נעשה, למעט סין, יש הסמכה בדין הקיים לביצוע מעקב כזה.

- בחלק מהמדינות קיימות אפליקציות להורדה, בהסכמה, המאפשרות סוגי מעקב אחר מי שנמצאים בבידוד.
- מעקב דיגיטלי רחב היקף שמטרתו לאכן מי שהה בסמוך לחולה מאומת קיים במדינות אסיה אך לא במדינות אירופה. באיטליה ובגרמניה הוא קיים באופן מותמם ואגרטיבי בלבד.
- **בשום מדינה מן המדינות שבדקנו, למעט סין שלגביה אין מידע, לא היה מעורב השירות החשאי.**
- בחלק מן המדינות ישנה מעורבות ישירה של המשטרה באכיפה, אך להבנתנו, בכל המדינות המידע מועבר מחברות תקשורת או חברות אחרות ישירות אל רשויות הבריאות המופקדות על ההתמודדות עם התפרצות מגפת הקורונה.
- טיוואן ודרום קוריאה, אשר נקטו גישה פוגענית יותר בכל הנוגע לפרטיות, צמצמו בד בבד את הפגיעה בחירויות יסוד אחרות ובראשן חופש התנועה. מדובר במדינות שמדורגות במיקומים גבוהים יותר מישראל במדד החירות הגלובלי של ארגון Freedom House.¹¹ נוסף על כך, שלא כמו ישראל, מדינות אלו מחזיקות בחקיקת פרטיות מעודכנת ברוח ה-GDPR, לנוכח שאיפתן לזכות בהכרה אירופית בתאימות הדין המקומי שלהן לדיני הפרטיות האירופיים. מוכנות חוקתית זו אפשרה להן להפעיל בזמן חירום אמצעי מעקב פוגעניים יותר, אך מתוך הקפדה על פיקוח, אבטחת מידע והגבלות על השימוש בו, מתן סעדים למי שפרטיותו נפגעה שלא בהתאם להסמכות בחוק, ומתוך שקיפות ושמירה על אמון הציבור במוסדות המבצעים את המעקב.

11 ישראל מדורגת במקום 76, ואילו דרום קוריאה מדורגת במקום ה-93 וטייוואן במקום ה-83. לשם השוואה, גרמניה מדורגת במקום ה-94 ואיטליה במקום ה-89. הנתונים נלקחו מ'[Global Freedom Score, Freedom House](#).

ההתבוננות במדינות שהפעילו טכנולוגיות מעקב עד כה מאפשרת לצייר סולם דירוג שבקצה האחד שלו נמצאת סין, שבה למעשה קיים מעקב חודרני אחר האזרחים גם בעיתות שגרה. בקצה השני של הסולם נמצאות מדינות אירופיות כמו איטליה וגרמניה. קשה להפגין שוויון נפש מול ההגבלות שנקבעו באיטליה, משום שבמדינה בעלת תרבות של חוסר ציות להוראות הממשלה הן כנראה תרמו ישירות לאסון. ייתכן שבגרמניה, שיש בה תרבות קשוחה יותר של ציות, יהיה פשוט יותר, אבל רק ימים יגידו. מכל מקום, אם יתברר שישראל דומה יותר לאיטליה משהיא דומה לגרמניה ברמת הציות להוראות, לא בטוח שזה המודל הנכון עבורנו.

לכן, בין שני קצות הסולם מעניין לראות שתי מדינות אחרות, טיוואן ודרום קוריאה, שאף שהן מצטיירות לעיתים כמדינות אסייתיות רחוקות שמתאפיינות בתרבות קשיחה של צייתנות, ההתמודדות שלהן עם האיזון שבין הקורונה לבין הגבלת זכויות ומעקב מרשימה הרבה יותר.

ההסדרים להתמודדות עם הקורונה בדרום קוריאה ובטייוואן דומים יותר למתרחש אצלנו מלהסדרים באירופה. אבל למרבה הפתעה מתברר שאפשר להתמודד גם ללא עירוב השירותים החשאיים, ואפשר להסתפק בהעברת מידע מחברות תקשורת ישירות אל רשויות הבריאות. במובן הזה ישראל צעדה צעד אחד רחוק יותר משאר הדמוקרטיות.

שמירה על הפרטיות גם במצב חירום איננה בכינות יפת נפש מול הצורך בהצלת חיים, אלא חשיבה על היום שאחרי הקורונה. צריך לומר בבירור: גם אם כעת השימוש בטכנולוגיות מעקב נרחבות הוא מוצדק והכרחי, הוא צריך להיות מלווה בפיקוח הולם ובשקיפות כלפי האזרחים. השקיפות כוללת הסברה - איזה מידע נאסף, לאיזה צורך ומתי הוא יימחק; והפיקוח צריך להיות אפקטיבי, כזה שיאפשר לוודא שתנאי האיסוף, העיבוד והשימוש במידע - נשמרים. ההקפדה על השקיפות בטייוואן ובדרום קוריאה הייתה קריטית ליצירת האמון הציבורי שנדרש לצורך נקיטת צעדים קיצוניים כאלה.

אצלנו, המאפיינים של השב"כ, שנוגעים לכך שכל מסמך שקשור אליו - מתקנות והנחיות ועד דוחות - הוא חסוי, אינם מאפשרים שקיפות. גם הפיקוח על השב"כ, הן באמצעות ועדות בכנסת הן באמצעות בתי המשפט, הוא צר יחסית.

נגיף הקורונה אינו נוגע אך לאפידמיולוגיה. הוא נמצא ביחסי גומלין עם התנהגויות אנושיות, עם מוסדות חברתיים, עם תרבות של ציות ועם היסטוריה של אמון בממשל. השילוב הזה מגביר את הנכונות שלנו לבטוח בשלטון ולהקריב כפרטים עבור הכלל. בכך טמון גם הוויכוח על הפרטיות מול הצורך במעקב דיגיטלי אישי.

מעקבים דיגיטליים אחר אזרחים: השוואה בינלאומית

אמצעי מעקב	ההסדרים לאיסוף מידע והגנה על הפרטיות	חקיקה ייעודית למגפות
<p>מאגר המידע משלב מידע ממחלקות ההגירה והבריאות. מי שחויב בבידוד מושם במעקב אחר תנועותיו לפי נתוני המיקום שלו המועברים על ידי חברת הסלולר</p>	<p>הסמכה לביצוע חקירה אפידמיולוגית הכוללת מידע על ההיסטוריה הרפואית של החולה.</p> <p>עיבוד המידע מותר כל עוד ננקטים אמצעי הזהירות והאבטחה המתאימים לפני העיבוד</p>	<p>חקיקה נרחבת לטיפול במצבי חירום הנגרמים עקב התפרצות מגפות</p>  <p>טייוואן</p>
<p>הצלבת נתונים על תנועות חולה מאומת לפי איכון סלולרי, נתוני אשראי, מצלמות מעקב במרחב הציבורי, מידע ממחלקת ההגירה ומחברות תעופה.</p> <p>פרסום לציבור של היסטוריית התנועה ללא שם ומשלוח הודעות SMS למי שלפי הנתונים שהוצלבו שהה בקרבתו.</p> <p>מעקב אחר מי שנדרש להיות בבידוד על ידי שיחת טלפון דו־יומית או באפליקציה שהורדתה וולונטרית</p>	<p>שיטות המעקב ייקבעו בצו נשיאותי בהתאם למחלה המידבקת הרלוונטית.</p> <p>חובת סודיות על מידע אישי על חולה או על מי שנמצא בבידוד</p>	<p>חקיקה נרחבת לטיפול במצבי חירום הנגרמים עקב התפרצות מגפות</p>  <p>דרום קוריאה</p>
<p>אכיפת הוראות הסגר רק באמצעות קבלת נתוני איכון סלולרי באופן מותמם ואגרסיבי</p>	<p>החוק מתיר לעיין בדברי דואר ובמסרים כתובים הממוענים לאדם המצוי בבידוד, ובלבד שעיבוד המידע האישי נחוץ להגשמת מטרת החוק</p>	<p>חקיקה נרחבת לטיפול במצבי חירום הנגרמים עקב התפרצות מגפות</p>  <p>גרמניה</p>
<p>המעקב אחר חולים, מבדדים או המפריים את הוראות הסגר נעשה לפי דיווחים מאזרחים מודאגים, באמצעות פטרולים של המשטרה או לפי מידע המתקבל מאיכון סלולרי באופן מותמם ואגרסיבי</p>	<p>איסוף המידע מותר אך חייב להיעשות בהתאם לכללי ה-GDPR. בסיום מצב החירום יש למחוק את המידע האישי שנשמר</p>	<p>צו חירום המעניק מסגרת משפטית מיוחדת לאיסוף ושיתוף מידע אישי לתקופת מצב החירום</p>  <p>איטליה</p>



האיחוד האירופי

ה-GDPR קובע התנהלות בנוגע לעיבוד מידע אישי ורגיש במצבי חירום הכוללים מגפות או איומים על ביטחון הציבור

בעל השליטה במידע חייב להבטיח הגנה על המידע האישי ועיבודו בהתאם להוראות ה-GDPR



סינגפור

חקיקה נרחבת לטיפול במצבי חירום הנגרמים עקב התפרצות מגפות

החוק מעניק לראש שירותי הבריאות במדינה סמכויות נרחבות לבצע מעקב למטרות בריאות הציבור, לרבות חקירה אפידמיולוגית

החקירה האפידמיולוגית מבוצעת בסיוע חוקרי משטרה ומבוססת על תחקור החולה ובחינת נתונים מאמצעי התחבורה במדינה, נתוני מיקום מאפליקציות שונות ובעיקר ממצלמות המעקב במרחב הציבורי



סין

מערכת מעקב חודרנית המבוססת על אפליקציה ייעודית שהורדתה מנדטורית, המספקת נתוני איכון סלולרי ומידע בריאותי המוזן על ידי המשתמש, מצלמות רחוב וטכנולוגיות זיהוי פנים. עובדי ממשלה מוצבים במקומות מרכזיים וסורקים את נתוניו של המשתמש מהאפליקציה. הנתונים מועברים לרשויות האכיפה.

ד"ר תהילה שוורץ אלטשולר היא עמיתה בכירה במכון הישראלי לדמוקרטיה ועומדת בראש התוכניות "רפורמות במדיה" ו"דמוקרטיה בעידן המידע". עמיתת מחקר בכירה במרכז פדרמן למשפט וסייבר באוניברסיטה העברית בירושלים וחברת נשיאות מועצת העיתונות. מומחית לאסדרת תקשורת ולמשק שבין טכנולוגיה, משפט ומדיניות.

עו"ד רחל ארידור הרשקוביץ היא חוקרת בתוכנית "דמוקרטיה בעידן המידע" שבמרכז לערכים ולמוסדות דמוקרטיים במכון הישראלי לדמוקרטיה. בעלת תואר ראשון ושני במשפטים. עבודת הדוקטור שלה בפקולטה למשפטים באוניברסיטת חיפה עוסקת בנושא מסגרות לשיתופי פעולה בין הממשל לתעשייה לשם הגברת ההגנה על מרחב הסייבר.

הדברים המובאים במסמך זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.



המכון הישראלי
לדמוקרטיה