12 ביולי 2020

לכבוד
ועדת חוץ וביטחון
כנסת ישראל

שלום רב,

הנדון: **הצעת חוק הפעלת מערכת אזרחית לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020**

אנו הח"מ, מומחים לפרטיות מתחומי הטכנולוגיה, המשפט ומדעי החברה, מצרפים בזה נוסח להצעת החוק שבנדון, המיועדת לקבוע אמות מידה לפיתוח חלופות לפעולות הסיוע של השב"כ לפי הצעת חוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020.

בכבוד רב,

פרופ' מיכאל בירנהק, הפקולטה למשפטים, אוניברסיטת תל אביב, ממייסדי פרטיות ישראל (עמותה בהקמה)

עו"ד חיים רביה - פרל כהן צדק לצר ברץ, ממייסדי פרטיות ישראל (עמותה בהקמה)

פרופ׳ קרין נהון, המרכז הבינתחומי הרצליה ונשיאת איגוד האינטרנט הישראלי, ממייסדות פרטיות ישראל (עמותה בהקמה)

עו"ד עמיר כהנא, מרכז פדרמן לחקר הסייבר, האוניברסיטה העברית

ד״ר ערן טוך, הפקולטה להנדסה, אוניברסיטת תל אביב, ממייסדי פרטיות ישראל (עמותה בהקמה)

ד"ר דלית קן-דרור פלדמן, הקליניקה למשפט טכנולוגיה וסייבר, הפקולטה למשפטים, אוניברסיטת חיפה

ד"ר ענת בן-דוד, המחלקה לסוציולוגיה, למדע המדינה ולתקשורת, האוניברסיטה הפתוחה, ממייסדות פרטיות ישראל (עמותה בהקמה)

עו"ד אבנר פינצ׳וק, האגודה לזכויות האזרח בישראל

עו"ד יורם הכהן, מנכ"ל, איגוד האינטרנט הישראלי (ע"ר) (לשעבר ראש הרשות למשפט, טכנולוגיה ומידע), ממייסדי פרטיות ישראל (עמותה בהקמה)

עו"ד נעמה מטרסו, מומחית לאבטחת מידע

ד"ר אלדר הבר, הפקולטה למשפטים, אוניברסיטת חיפה

ניר הירשמן, התנועה לזכויות דיגיטליות

פרופ' בני פנקס, מרכז הסייבר והמחלקה למדעי המחשב, אונ' בר-אילן

דורון שקמוני, מומחה סייבר ויזם טכנולוגיה (ממקימי איגוד האינטרנט הישראלי ונשיאו בעבר)

ד"ר ארנה ברי, לשעבר למדענית הראשית ומנהלת מערך המחקר ופיתוח התעשייתי של משרד התמ"ת, וממייסדות פרטיות ישראל (עמותה בהקמה).

הצעת חוק

הפעלת מערכת אזרחית לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020

דברי הסבר

כללי

במרץ 2020 הסמיכה הממשלה את שירות הביטחון הכללי להשתמש באמצעים טכנולוגיים המיועדים ללוחמה בטרור, כדי לסייע באיתור חשיפות של אזרחים לחולי Covid-19 (המחלה הנגרמת מנגיף קורונה החדש) לשם קטיעת שרשרת ההדבקה בנגיף. שימוש באמצעים טכנולוגיים על ידי השב"כ, טומן בחובו פגיעה קשה ומתמשכת בפרטיות כלל תושבי ישראל, שכן הוא מתבצע באמצעות מעקב מתמיד, בידי גוף ביטחון מסכל, אחר אותות מכשירי הטלפון הניידים של כל אזרחי המדינה ותושביה לצורך ניטור מקומם בלא ידיעתם ובלא הסכמתם.

לזכות לפרטיות יש מעמד חוקתי מפורש בסעיף 7 לחוק יסוד: כבוד האדם וחירותו . עוד קודם לכן נקבעה הזכות בחוק הגנת הפרטיות, התשמ"א-1981. הזכות הוכרה בפסיקה כ"אחת מן החשובות שבזכויות האדם" וכן "אחת החירויות המעצבות את אופיו של המשטר בישראל כמשטר דמוקרטי".

על הפגיעה האנושה בפרטיות הנגרמת מפעולות הסיוע של שירות הביטחון הכללי עמד בית המשפט העליון בפסיקתו בבג"ץ 2109/20, 2135/20, 2141/20, 2187/20 בן מאיר ואח נ' ראש הממשלה ואח' (26.4.2020, מפי כב' הנשיאה א' חיות):

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

בג"ץ קבע כי יש לבצע עבודת מטה לאיתור חלופה להתחקות השירות הביטחון הכללי, וכדבריו -

> "המאמץ לאיתורה של חלופה יעילה אחרת חייב להימשך ללא לאות... במיוחד יש לשקול אם ניתן להשיג את התועלות החשובות הנדרשות באמצעות שימוש במנגנון וולונטרי ושקוף למשתמש"

עמדה דומה הביעה גם ועדת המשנה לענין השירותים החשאיים של ועדת החוץ והביטחון של הכנסת, בדיון ביום 30.3.2020 שם נאמר כי "המדינה מחויבת, בצד השימוש באמצעי החריג הזה, חסר התקדים הזה על-ידי שירות הביטחון הכללי שתפקידו אחר והוקם לייעוד אחר, לבחון חלופות שונות אחרות" והוצע כי חיפוש החלופה יעשה בידי גוף מקצועי מוסמך שיערוך עבודת מטה מסודרת בשיתוף הציבור ומומחים לעניין.

אם נעשתה עבודת מטה כזו, היא לא פורסמה ברבים ואף לא דווחה לכנסת. בניגוד לכך, הסמכת שירות הביטחון הכללי עוגנה ב-1.7.2020 בחוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף–2020 ("חוק הסמכת שירות הביטחון הכללי").

כיום, קיימות טכנולוגיות אזרחיות המאפשרות ליצור חלופות להסתייעות בשב"כ. שלא כמו אמצעי המעקב של שירות הביטחון הכללי, טכנולוגיות כאלה מאפשרות זיהוי מהיר ומדוייק יותר של מגעים, תוך שמירה טובה על פרטיות. מדינות שונות עושות שימוש בטכנולוגיות שכאלה.

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

ההתפתחות בעולם בהתמודדות עם הקורונה פונה אפוא לכיוון של זיהוי מגעים (contact tracing) ולא מעקב מיקום. זיהוי קירבה מבוסס על שימוש בטכנולוגיית Bluetooth, המובנית כיום בכל טלפון סלולרי מודרני. נכון לסוף חודש מאי, 39 מדינות מבססות את הצורך לאיתור מהיר של חשיפה על אפליקציות המותקנות על ידי המשתמשים במכשירי טלפון חכמים. 22 מתוכן – ובהן איטליה גרמניה, שוויץ, צרפת. פולין, סינגפור ואוסטרליה – מתבססות על טכנולוגיית Bluetooth מבוזרת (במצב שנקרא BLE - Bluetooth Low Energy, שייחודו בצריכת אנרגיה נמוכה), בצורה בה המידע על מגעים נשמר בנייד ולא במאגר מרכזי. גישה טכנולוגית זו מקודמת בשיתוף פעולה חד-פעמי בידי החברות Google ו-Apple, כך שהיא תיתמך גם במכשירי טלפון ניידים מבוססי אנדרואיד וגם ב-iPhone. מלבד שיתוף הפעולה של החברות, הפרויקט הפאן-אירופי DP3T יצר מערכת מבוזרת לזיהוי מגעים מבוססת Bluetooth שמיושמת בכמה מדינות. מערכת כזו מאפשרת זיהוי מגעים של אנשים ממדינות שונות. ביישומה בשוויצריה, לדוגמה, היא זוכה להצלחה מרשימה כאשר בתוך שלושה ימים בלבד שיעור החדירה שלה הגיעו לכ-13% מבעלי הטלפונים הניידים החכמים במדינה.

בישראל, השיק משרד הבריאות את אפליקציית "המגן". זהו אמצעי שתוכנן ונוצר בהקפדה תוך הגנה על פרטיות ואבטחה, בין השאר מפני שקוד המקור שלו שוחרר לציבור וכן מפני שהוא שומר את כל נתוני המיקום במכשיר המקומי של המשתמש, והצלבת מידע נעשית רק במכשיר המשתמש שבשליטתו. "המגן" מבוסס על ניטור מיקום באמצעות GPS ורשתות תקשורת אלחוטית (Wi-Fi). אלא שהממשלה לא קידמה את השימוש ב"המגן" באופן מספק, ולמעשה זנחה אותו מול מקסם הכלי של שירות הביטחון הכללי. מכיוון שהפצת "המגן" לא לוותה בקמפיין משמעותי, פוטנציאל השימוש של היישומון רחוק ממיצוי.

הצעת החוק מיועדת להפעיל מערכות טכנולוגיות אזרחיות לאיתור מגעים המעוצבות מלכתחילה באופן שמגן על פרטיות הציבור. הגנה על הפרטיות תקדם את האמון הציבור במערכות הללו ותרחיב את השימוש בהן באופן שיאפשר להחליף את הסיוע הטכנולוגי שמספק שירות הביטחון הכללי למשרד הבריאות.

לשם כך, הצעת החוק מורה כי הממשלה תפתח, בעצמה או בדרך אחרת, ותפיץ טכנולוגיות לאיתור מגעים שיכללו יישומון המיועד להתקנה במכשירי רדיו טלפון נייד וחומרה ייעודית למי שאינם משתמשים בטלפונים כאלה.

בעוד שהטכנולוגיה המובילה בעולם לניטור קירבה מבוססת באמור על בלוטות', הצעת החוק היא ניטרלית מבחינה טכנולוגית ואינה נוקבת בטכנולוגיה כזו או אחרת. במקום זאת היא קובעת עקרונות שכל טכנולוגיה לאיתור מגעים צריכה לציית להם.

ההצעה קובעת כי הטכנולוגיות לאיתור מגעים יטמיעו לתוכן מלכתחילה עקרונות של שמירה על הפרטיות, ברוח הגישה הידועה כ"הנדסת פרטיות" (Privacy by Design). בכלל זה הן יותקנו על-ידי המשתמש רק בכפוף להסכמתו מדעת ורצונו החופשי, יימנע מאיסוף, הפצת או מסירת מידע אישי מזהה, יעבדו רק מידע אנונימי, יישמרו ככל הניתן רק על גבי מכשיר הטלפון של המשתמש או החומרה הייעודית, יימחקו מאליהם לאחר פרק זמן שייקבע ולא יאפשרו העברת מידע לממשלה אלא בהסכמת המשתמש ומרצונו החופשי.

הטכנולוגיות לאיתור מגעים יפותחו ויופצו לציבור תחת רישיון קוד פתוח, המאפשר לצפות בקוד המקור שלהן (ובכך לאמת שלא גלומה בהן פגיעה בפרטיות), להעתיק, לשנות ולהפיץ את הטכנולוגיות בלא תשלום. השימוש בהן יהיה כפוף לרישיון קצר, בהיר וקל להבנה שאי-אפשר לשנותו באופן חד-צדדי. ההצעה מורה עוד שהטכנולוגיות תאפשרנה תאימות (interoperability) עם אמצעים דומים אחרים.

לפי ההצעה, על שר הבריאות לגבש תכנית לאומית לעידוד הציבור להשתמש בטכנולוגיות האזרחיות לניטור מגעים ולהקצות את התקציבים הדרושים לכך. הכנסת תקבע אמות-מידה להפסקת ההסתייעות בשירות הביטחון הכללי במאבק במגפת הקורונה בהתחשב במספר המשתמשים בטכנולוגיות אלה.

כדי להגביר את אמון הציבור נקבע כי תמונה ועדה בראשות שופט בדימוס או משפטן בכיר הכשיר להתמנות כשופט מחוזי, שתפקידה לייעץ לגבי המשך פיתוחן של הטכנולוגיות לאיתור מגעים, לרבות היבטים של קידום השימוש שלהן בציבור, ולפרסם דוחות לציבור. כן נקבע כי ככל שנאסף מידע גולמי מהאמצעים לאיתור מגעים, חובה לפרסמו במלואו לציבור וכן נקבעו חובות דיווח פרטניות למשרד הבריאות.

לבסוף, ההצעה קובעת עונשים שמטרתם להרתיע מפני שימוש לרעה במידע שייאסף באמצעות הטכנולוגיות לאיתור מגעים.

השר הממונה על החוק יהיה שר הבריאות והחוק יעמוד בתוקף כל עוד חובת בידוד מוכרזת בישראל מכוח צו בריאות העם (נגיף הקורונה החדש)(בידוד בית והוראות שונות)(הוראת שעה), התש"ף-2020.

סעיף 1 - מטרה

סעיף זה קובע את מטרת החוק, ברוח המבוא לדברי ההסבר, מתוך כוונה להשתמש בטכנולוגיות לאיתור מגעים לבלימת התפשטות המגיפה תוך שמירה על הזכות לפרטיות. אפיק אזרחי זה יש בו כדי לחזק את אמון הציבור במקבלי ההחלטות, במדינה, ובאופן ממוקד, בקשר לשימוש בטכנולוגיה. אפיק זה נועד להחליף את השימוש בטכנולוגיות שבידי שירות הביטחון הכללי.

סעיף 2 - הגדרות

החוק המוצע בא בתוך מסגרת משפטית קיימת של חקיקת החירום בקשר למאבק הלאומי בנגיף הקורונה, ומאזכר את החקיקה המתאימה - חוק ההסמכה וצו הבידוד. בהתאם, המונחים "המחלה" ו"נגיף הקורונה החדש" מבהירים את ההקשר הספציפי של הצעת החוק.

הגדרת "מידע אישי מזהה" מבוססת על הגדרת "מידע מזוהה" בסעיף 2 לחוק נתוני אשראי, התשע"ו-2016, המקיפה "מידע הכולל פרט מזהה של לקוח, או מידע שפרטים מזהים של לקוח הופרדו ממנו אך ניתן במאמץ סביר

לזהות את הלקוח שאליו מתייחס המידע." הגדרה זו מתאימה גם כאן, בשינוי של "לקוח" ל"משתמש". ההגדרה משקפת את התפיסה שכל פריט מידע, גם אם תמים לכאורה, עשוי להצטרף למידע אחר, כך שהצירוף עולה על סך חלקיו בהיבט רגישות המידע, או, שהמידע הוא מפתח למידע רגיש אחר. לפי גישה זו, שמשקפת את החשיבה האירופית ב-General Data Protection Regulation משנת 2018 (ה-GDPR) ועוד קודם לכן בדירקטיבת הגנת המידע האישי משנת 1995, העיקר הוא זיהויו של אדם. כאשר האדם אינו מזוהה ואין דרך לזהותו באופן סביר, נשמרת פרטיותו. בהתאם, ההגדרה מתייחסת הן למידע מזהה ישיר, כמו שם או מספר תעודת זהות, והן לאפשרות לזהות את נושא המידע (data subject) מתוך מידע שהותמם, אם ניתן במאמץ סביר לבצע זיהוי מחדש של האדם.

המערכת הטכנולוגית שבה עוסק החוק המוצע מורכבת תיקרא באופן כללי "טכנולוגיה לאיתור מגעים (Contact Tracing Technologies)", אשר כשלעצמו, הוא מונח כולל שאינו תלוי בטכנולוגיה מסוימת, אלא מבוסס על מטרתו - איתור מגעים של חולים, כדי להשיג את מטרת החוק. טכנולוגיה לאיתור מגעים יכולה להיות מורכבת מאחד או יותר הרכיבים הבאים: יישומון, חומרה ייעודית, ומערכות טכנולוגיות נלוות. "יישומון" מתייחס לתוכנה עצמה, כאשר היא מותקנת במכשיר נייד כמו "טלפון חכם". "חומרה ייעודית" היא מכשיר נייד שתותקן בו המערכת, אולם אין למכשיר שום פונקציה אחרת. הכוונה היא למשל לצמידים מיוחדים שבהם יוטמע שבב מתאים, שבו מותקנת התוכנה. חומרה ייעודית מתאימה לשימוש על ידי מי שאינם נושאים מכשיר טלפון חכם או התקן דומה, לרבות מטעמים הלכתיים. ה"משתמש" הוא מי שהתקין את היישומון במכשיר נייד או שברשותו חומרה ייעודית.

מטרת הטכנולוגיות לאיתור מגעים היא לזהות "מגעים", שפירושם מי שהיו בקרבה מסוימת לנשא הנגיף, ולכן יש חשש שנדבקו. הסייג המוצע של "ללא מיגון מספק" נועד לסייג את מי שהיו ממוגנים כיאות, למשל צוותים רפואיים במחלקות לטיפול בחולי קורונה. לפי הידוע כיום, לא כל מפגש בין נשא של הנגיף לבין אדם בריא מסתיים בהדבקה. הידע הרפואי נכון לעת הזו מעיד על קירבה של מרחק מסוים - 2 מטר או פחות, במשך פרק זמן של 15 דקות או פחות. בהתאם, הגדרת "מגע קרוב" מתייחסת למאפייני המרחק והזמן, אולם מפקידה את הקביעה בידי משרד הבריאות, שיוכל לעדכן אותה לפי הידע הרפואי העדכני בכל נקודת זמן. כאשר מתקיימים התנאים בדבר "מגע קרוב", נוצרים "נתוני קירבה."

"קוד המקור" של התוכנה מתייחסת באופן מרחיב לכל תוכנה וחומרה שיש בטכנולוגיה לאיתור מגעים, על מרכיביהם. "רישיון קוד פתוח" מפנה בדרך של המחשה לרישיון של MIT בנושא, אולם מרחיב לכל רישיון שמתיר שימושים מסוימים בתוכנה. תוכנה היא בדרך כלל בגדר "יצירה" מוגנת לפי חוק זכות יוצרים, התשס"ח-2007, ולבעליה אגד זכויות. רישיון קוד פתוח הוא אמצעי חוזי שלפיו בעל הזכויות אינו מוותר על זכויות היוצרים שלו בתוכנה אולם מקנה זכויות להעתיק, להכין יצירה נגזרת, ולהפיץ את התוכנה, כגון באמצעות ו העמדה לרשות הציבור, ביצוע פומבי ושידור. נעיר שלפי חוק זכות יוצרים, בתוכנה אין זכויות מוסריות.

הצעת החוק מגדירה את "השר" האחראי כשר הבריאות, שבידיו סמכויות ביצוע שונות, ומציעה להקים "ועדה מפקחת", שהרכבה וסמכויותיה מפורטים בסעיף 9 להצעה.

סעיף 3 - פיתוח טכנולוגיות לאיתור מגעים

זהו הסעיף האופרטיבי של החוק. הממשלה מחויבת לפתח טכנולוגיות לאיתור מגעים. חובה זו נובעת מהמטרה של החוק ומהצורך לבלום את התפשטות נגיף הקורונה החדש. הפיתוח יכול להיות פנים-ממשלתי או חיצוני, כל עוד נשמרים העקרונות המפורטים בחוק זה. בפיתוח טכנולוגיות לא די, ולכן יש חובה לקדם את השימוש בטכנולוגיה. על-פי הצעת החוק, השימוש צריך להיות חינמי - כדי להגיע לתפוצה מירבית, וזאת כדי להגביר את יעילות הטכנולוגיה, וכן, כדי להימנע ממצב שבו אדם שאין לו יכולת כספית לשלם עבור השימוש בטכנולוגיה יהיה חשוף יותר למחלה מאשר אחרים.

סעיף 4: טכנולוגיות לאיתור מגעים

מטרת הטכנולוגיות לאיתור מגעים, כשמן, הוא לאתר את מי שהיו בקרבת נשא של הנגיף, כדי לקטוע את שרשרת ההדבקה בנגיף הקורונה בשלב מוקדם ככל האפשר.

סעיף זה מפרט את העקרונות שלפיו יפותחו ויופעלו הטכנולוגיות לאיתור מגעים. המסגרת הכללית היא של "הנדסת פרטיות" (Privacy by Design) שהוא עיקרון מנחה בדיני הפרטיות כיום בעולם. העיקרון מופנה למתכנני מערכות ומהנדסים, כדי שיכללו את הגנת הפרטיות במערכת המתוכננת מלכתחילה, כחלק מהגדרות הבסיס של המערכת. גישה זו זכתה לתמיכה בין-לאומית נרחבת, היא מעוגנת ב"הצהרת ירושלים" משנת 2010 של נציבי הגנת הפרטיות בעולם. באיחוד האירופי, היא חובה משפטית תחת ה-GDPR. בישראל, העיקרון נקלט לפי שעה בפסיקת בית המשפט המחוזי, בעניין עמותת חברות הסיעוד נ' משרד הביטחון (2019). הגישה של הנדסת פרטיות היא כללית, ומחייבת פירוט והתאמה לפי המערכת הטכנולוגית בה מדובר וצרכיה.

סעיף 4(א) מגדיר את מטרת הטכנולוגיות. הגדרה זו דרושה משום ששימושים אחרים בטכנולוגיות ייבחנו לאור המטרה הזו.

סעיף 4(ב) מפרט את היבטי הפרטיות העיקריים שיש לכלול במסגרת תכנון המערכות הטכנולוגיות לאיתור מגעים בישראל. העקרונות משקפות את הדין הישראלי - בעיקר את הכללים הקבועים בחוק הגנת הפרטיות, התשמ"א-1981, וכן את פרשנות בתי המשפט לזכות לפרטיות שקבועה בסעיף 7 לחוק יסוד: כבוד האדם וחירותו, וכן לסעיף 8 ("פסקת ההגבלה") שבחוק היסוד, ובעיקר, את דרישת המידתיות.

בהתאם, העיקרון המנחה הראשון הוא הסכמת המשתמשים. גם בג"ץ עמד על כך בפסק דינו בעניין בן-מאיר נ' ראש הממשלה (2020) בעניין איכון השב"כ. ההסכמה צריכה להיות על בסיס מידע מתאים, כדי שהמשתמש יוכל לקבל החלטה מדעת (informed consent). דרישת ההסכמה מופיעה במפורש בחוק הגנת הפרטיות (ס' 1, 3, 11). ההסכמה צריכה להיות מרצון חופשי. כפי שמצאו בתי המשפט, בהקשרים מסוימים, במיוחד של פערי כוחות בין הצדדים כמו במקום העבודה, אין משמעות להסכמה של הצד החלש, ולכן יש חשיבות רבה בכך שההסכמה היא מרצון חופשי.

שני העקרונות הבאים שמפרט הסעיף, משקפים את עיקרון המידתיות במובנו הצר: הפגיעה בפרטיות שכרוכה באיסוף מידע אישי ועיבודו, צריכה להיות רק במידה הדרושה. בהתאם, העיקרון השני מחייב שטכנולוגיות לאיתור מגעים לא יאספו, יפיצו או יעבירו מידע אישי מזהה, כפי שזה הוגדר בסעיף 2 להצעה זו. עיקרון משלים מופיע בסעיף קטן 3, שמבהיר כי גם בתוך המידע שמותר לאיסוף, יש לאסוף את המינימום הדרוש. עיקרון המינימיזציה מקובל בדיני הגנת הפרטיות, מעוגן במפורש ב-GDPR האירופי, וכאמור נובע בדין הישראלי גם מההקשר החוקתי.

העיקרון הרביעי, מחייב התממה (אנונימיזציה) של המידע והצפנתו. המטרה היא למזער את הסיכון שיש בדליפת המידע, כך שגם אם ידלוף או יגיע לידיים זרות, לא יהיה למידע כל שימוש, בשל היותו אנונימי ומוצפן.

העיקרון החמישי משקף גם הוא את השאיפה לצמצם סיכונים בדליפת המידע ושימושים נוספים בו, למטרות אחרות, בכך שהמידע הרגיש ביותר שהמערכת אוספת ומעבדת, נתוני הקירבה, יישמרו רק בשליטת המשתמש - במכשיר הטלפון הנייד או בחומרה הייעודית. עיקרון זה ידוע כ"ביזוריות של מידע". הוא נועד להבטיח שליטה מירבית של המשתמש במידע שעל אודותיו, בניגוד לריכוז המידע במערכת מרכזית. ביזור המידע משקף את המקובל בפיתוח מערכות לניטור-מגעים במדינות רבות בחו"ל ובהן קנדה, בריטניה, הולנד, בלגיה, גרמניה, שווצריה, אוסטריה, איטליה, ספרד, פורטוגל ועוד.

העיקרון השישי משקף גם הוא את הצורך בשליטת המשתמש במידע שעל אודותיו, ולצמצם את החשש משימושים נוספים במידע למטרות אחרות, ואת הסיכונים שיש בכך שהמידע ידלוף. בהתאם, מוצע לקבוע

שהמידע יימחק מאליו, באופן אוטומטי וללא צורך במעורבות המשתמש, בחלוף 21 ימים המרגע שנאסף. באותו שלב, אין למידע ערך לצורך המטרה של איתור המגעים.

העיקרון השביעי מתייחס לפונקציה המרכזית של הטכנולוגיות לאיתור מגעים, בדרך של זיהוי מגע קרוב ודורש כי יידוע בדבר מגע קרוב עם חולה ייעשה באופן כזה שישמור על זהות החולה. כך, המגע ייקבל חיווי, אבל לא ידע, לפחות לא מתוך המערכת, מי החולה.

העיקרון השמיני משקף את שליטת המשתמש במידע שעל אודותיו. בהתאם, יש לתכנן את הטכנולוגיות לאיתור מגעים כך שיימנעו גישה של אחרים אל המידע, ללא רצון המשתמש. העיקרון התשיעי משקף את הצורך בשליטה, וחוזר על עיקרון ההסכמה ועל אי העברת המידע, באופן ספציפי לידי הממשלה. אמצעים אלה נועדו להבטיח את פרטיות המשתמש אל מול הממשלה ואל מול אנשים או גורמים אחרים. העיקרון העשירי והאחרון משלים את מעגל זרימת המידע, ומתיר לקבל מידע על מגע קרוב, גם כן באופן מאובטח ומוצפן.

סעיף 4(ג) מתייחס לתנאי השימוש ומדיניות הפרטיות בטכנולוגיות לאיתור מגעים. מדיניות זו היא הבסיס להסכמה מדעת ומרצון חופשי של המשתמשים. הסעיף מתייחס לאופן העברת המידע, שצריך להיות פשוט, קצר וברור. המידע צריך להימסר בשפות הנפוצות בישראל. שינויים למדיניות המידע עלולים להשפיע על זכויות המשתמשים, ולכן מותרים רק בקבלת הסכמה מדעת נוספת.

סעיף 4(ד) טכנולוגיות לאיתור מגעים לא יכולות לפעול כ"אי בודד" כך שיחליפו מידע רק בינן לבין עצמן. הן חייבות לאפשר אינטרקציה בינן לבין טכנולוגיות מקבילות, באופן שאזרח ממדינה אחת, לדוגמה, המשתמש ביישום לניטור קירבה המקובל במדינתו, יוכל להחליף נתוני קירבה עם אזרח ממדינה שניה, המשתמש ביישום המקובל בארצו-שלו. לדבר חשיבות יתרה גם לקראת פתיחת הגבולות מחדש לתנועה בין-מדינתית. משום כך דורש הסעיף שטכנולוגיות לאיתור מגעים תאפשרנה פעולה הדדית (אינטראופרביליות, בלעז) עם טכנולוגיות מקבילות.

סעיף 4(ה) מציע שהיישומונים יועמדו לשימוש כלל הציבור בחינם. הממשלה תממן חומרה ייעודית כך שתוצע בחינם או תקבע לה מחיר מירבי שווה לכל נפש.

סעיף 4(ו) נועד לעודד את המגזר הפרטי לפתח טכנולוגיות מתאימות, ומבהיר כי גם אלה צריכות לעמוד בדרישות החוק.

סעיף 5 - קוד פתוח

פרסום קוד המקור שבו נכתבת התוכנה שבבסיס הטכנולוגיה לאיתור מגעים מאפשר בקרה חיצונית ובלתי תלויה של הטכנולוגיה. בקרה כזו חשובה כדי לקדם את אמון הציבור בטכנולוגיה, כדי לעודד את השימוש. פרסום התוכנה בקוד פתוח מאפשר גם שיתוף ידע עם מדינות אחרות, במסגרת הסולידריות הבין-מדינתית הדרושה במאבק הגלובלי המשותף לבלימת המגיפה העולמית. ואכן, חלק גדול מהמדינות שפיתחו מערכות לניטור קירבה, כדוגמת שוויץ, גרמניה, צ'כיה, הודו, איטליה, מרוקו, סינגפור ואף ישראל עצמה ביישומון "המגן" - פירסמו את קוד המקור בפומבי תחת רישיון קוד פתוח.

סעיף 6 - הגבלת שימושים וסודיות

חוק הגנת הפרטיות קובע את עקרון צמידות המטרה, שלפיו אין להשתמש בידיעה על ענייניו הפרטיים של אדם שלא למטרה שלשמה נושא המידע מסר את המידע מלכתחילה (סעיפים 2(9), 8(ב) לחוק). סעיף 6 להצעה הנוכחית מבהיר כי מלכתחילה אין להשתמש במידע שהופק באמצעות טכנולוגיות לאיתור מגעים אלא לשם מניעת הידבקות במחלה. כדי למנוע לחצים על משתמש להעברת המידע לצד שלישי למטרות החורגות מהמאבק במגפה, הסעיף אינו מאפשר שימוש כזה גם בהסכמת המשתמש. מתלווה לאיסור חובת סודיות. הצורך בקביעת חובת

סודיות ייחודית נובעת מהרצון להנגיש את החובה למי שמעורבים בפיתוח ובשימוש בטכנולוגיות, וכדי לאותת לציבור שהמידע על אודותיו מוגן. לבסוף, כדי להבטיח זאת, הסעיף קובע כי אין להשתמש במידע מטכנולוגיות לאיתור מגעים במסגרת הליכים משפטיים או חקירות, בהתאם לנאמר ביחס למידע שמסר שירות הביטחון הכללי במסגרת חוק הסמכת שירות הביטחון הכללי.

סעיף 7 - לוחות זמנים

כדי שהוראות החוק תיושמנה במהירות, מוצע לקבוע לוחות זמנים שלפיהם מחויבת הממשלה לפעול בפיתוח יישומון (תחילה) וחומרה ייעודית (לאחר מכן) שהן חלק מהטכנולוגיות לאיתור מגעים. לוח הזמנים לפיתוח חומרה ייעודית ארוך יותר, שכן פיתוח חומרה משובצת-תוכנה מורכב יותר מפיתוח תוכנה בלבד. עוד מורה הסעיף כי על הממשלה לדאוג לעדכן את הטכנולוגיות הללו באופן שוטף כדי להבטיח את תפקודן התקין.

סעיף 8 - עידוד הציבור

בקיומן של טכנולוגיות לאיתור מגעים אין די. היות שהשימוש בהן הוא וולונטרי, יעילותן תלויה גם בשיעור המשתמשים מקרב הציבור שיבחר לאמץ אותן. בהתאם, מוצע לקבוע כי שר הבריאות יגבש תוכנית לאומית לעידוד השימוש בטכנולוגיות לאיתור מגעים וידאג לתקצובה המתאים.

סעיף 9 - פקיעת תוקף הסמכת השב"כ

בשל הפגיעה החמורה בפרטיות המגולמת בהתחקות שירות הביטחון הכללי אחר כלל אזרחי המדינה במסגרת הסיוע במאבק הלאומי במגפת הקורונה, חוק זה מיועד למסד חלופות לאיכון הטכנולוגי של השירות את נתיבי התנועה של חולי קורונה וזיהוי האנשים שעימם נפגשו. בהתאם, מוצע לקבוע שהממשלה תקבע, באישור ועדת חוץ וביטחון של הכנסת, את אמות המידה, שבהתקיימן תפקע הסמכת השירות לסייע למשרד הבריאות במאבק בקורונה.

סעיף 10 - ועדה מפקחת

מוצע להקים ועדה ציבורית מפקחת, שהרכבה כמפורט בסעיף. הוועדה תייעץ לשר ותפקח על פיתוח הטכנולוגיות לאיתור מגעים. הסעיף מפרט את חובת ההיוועצות בוועדה לפני פרסום הטכנולוגיה לאיתור מגעים לציבור. ייעוץ ופיקוח ציבורי דרושים כדי להגביר את אמון הציבור במערכת הטכנולוגית. הסעיף קובע את סמכויות הוועדה, ואת אי-תלותה.

סעיף 11 - פירסום

סעיף זה קובע חובת פרסום של נתונים גולמיים, בצורה אגרגטיבית ושאינה מזהה את נושאי המידע. השקיפות דרושה כדי לאפשר בקרה ציבורית, שיח ציבורי, וכדי להגביר את אמון הציבור במערכת הטכנולוגית, וכך לעודד את השימוש בה.

סעיף 12 - עונשין

מוצע לקבוע עבירות פליליות בקשר להפרת החובה שלא להשתמש במידע למטרות שחורגות מתכלית הטכנולוגיות לאיתור מגעים, ולהפרת חובת הסודיות. מוצע לקבוע גם עבירה לגבי מי שדורש מאדם למסור לו מידע שהתקבל באמצעות הטכנולוגיה, וכן, עבירה של סירוב לשתף פעולה עם הוועדה המפקחת המוצעת. הענישה המוצעת היא ברף הנמוך, עד שנת מאסר או קנס לפי סעיף 61(א)(3) לחוק העונשין (עד 75,300 ש"ח). כמו כן, מוצע לקבוע עבירה ברף ענישה גבוה יותר, של עד שלוש שנות מאסר או כפל הקנס, כאשר מעסיק של המשתמש

בטכנולוגיות לאיתור מגעים, או מי שיש לו יחסי מרות עם משתמש בטכנולוגיות כאלה, דורש לקבל מידע שנאגר באמצעותן. מוצע עוד לקבוע את אחריותם של נושאי משרה בתאגיד. הצורך בקביעת עבירות אלה נועד להבטיח את שליטת נושא המידע במידע שעל אודותיו, ולמנוע נסיונות לעקוף את המגבלות שמוטלות על השימוש במידע לצרכים שלשמם לא נועד מראש. הרשעה פלילית יכולה גם לסייע לתביעה אזרחית של מי שנפגע מהתנהגות אסורה כנגדו.

סעיף 13 - ביצוע ותקנות

מוצע כי השר הממונה על ביצועו של חוק זה יהיה שר הבריאות והוא יהיה רשאי להתקין תקנות לביצועו, באישור ועדת חוץ וביטחון של הכנסת.

סעיף 14 - תוקף

החוק מיועד להיות הוראת שעה, שתעמוד בתוקפה כל עוד מגפת הקורונה מהווה סכנה לבריאות תושבי ישראל. אינדיקציה לסיום הסכנה הנשקפת מהמגפה תימצא בביטול חובת הבידוד, החלה מכוח צו בריאות העם (נגיף הקורונה החדש)(בידוד בית והוראות שונות)(הוראת שעה), התש"ף-2020. לפיכך מוצע שתוקף החוק ייתם עם ביטולו של הצו או דבר חקיקה שיבוא במקומו.

נוסח

הצעת חוק זו נוסחה בידי פרופ' מיכאל בירנהק, הפקולטה למשפטים, אוניברסיטת תל אביב ועו"ד חיים רביה ראש קב' הסייבר במשרד עוה"ד פרל כהן צדק לצר ברץ, שניהם ממייסדי פרטיות ישראל (עמותה בהקמה) - בשיתוף ובתמיכת פרופ׳ קרין נהון, המרכז הבינתחומי הרצליה ונשיאת איגוד האינטרנט הישראלי, ממייסדות פרטיות ישראל (עמותה בהקמה); עו"ד עמיר כהנא, מרכז פדרמן לחקר הסייבר, האוניברסיטה העברית; ד"ר ערן טוך, הפקולטה להנדסה, אוניברסיטת תל אביב, ממייסדי פרטיות ישראל (עמותה בהקמה); ד"ר דלית קן-דרור פלדמן, הקליניקה למשפט טכנולוגיה וסייבר, הפקולטה למשפטים, אוניברסיטת חיפה; ד"ר ענת בן-דוד, המחלקה לסוציולוגיה, למדע המדינה ולתקשורת, האוניברסיטה הפתוחה, ממייסדות פרטיות ישראל (עמותה בהקמה); עו"ד אבנר פינצ'וק, האגודה לזכויות האזרח בישראל; עו"ד יורם הכהן, מנכ"ל, איגוד האינטרנט הישראלי (ע"ר) (לשעבר ראש הרשות למשפט, טכנולוגיה ומידע), ממייסדי פרטיות ישראל (עמותה בהקמה); עו"ד נעמה מטרסו, מומחית לאבטחת מידע; ד"ר אלדר הבר, הפקולטה למשפטים, אוניברסיטת חיפה; ניר הירשמן, התנועה לזכויות דיגיטליות; פרופ' בני פנקס, מרכז הסייבר והמחלקה למדעי המחשב, אונ' בר-אילן; דורון שקמוני, מומחה סייבר ויזם טכנולוגיה (ממקימי איגוד האינטרנט הישראלי ונשיאו בעבר) וד"ר ארנה ברי, לשעבר למדענית הראשית ומנהלת מערך המחקר ופיתוח התעשייתי של משרד התמ"ת וממייסדות פרטיות ישראל (עמותה בהקמה).

נוסח הצעת החוק

1. מטרה

מטרתו של חוק זה היא להפעיל מערכות טכנולוגיות אזרחיות לאיתור מגעים במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש, המעוצבות מלכתחילה באופן שמגן על פרטיות הציבור כדי לקדם את האמון והשימוש בהן, כדי להחליף את הסיוע הטכנולוגי שמספק שירות הביטחון הכללי למשרד הבריאות לפי חוק ההסמכה.

2. הגדרות

בחוק זה –

"הוועדה המפקחת" - הוועדה הפועלת לפי הוראת סעיף 10 לחוק זה.

"חוק ההסמכה" - חוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף-2020 [1].

"חוק העונשין" - חוק העונשין, התשל"ז-1977 [2].

"יישומון" – תוכנה לאיתור מגעים המיועדת לשימוש בהתקן נייד, לרבות מכשירי רדיו טלפון נייד; ולרבות תוכנה לאיתור מגעים שהיא משובצת (embedded) בחומרה ייעודית.

"חומרה ייעודית" – התקן המיועד להפעלת יישומון שאיננו רדיו טלפון נייד.

"טכנולוגיה לאיתור מגעים" - יישומון, חומרה ייעודית ומערכות טכנולוגיות נלוות.

"מידע אישי מזהה" - מידע הכולל פרט מזהה של משתמש, או מידע שפרטים מזהים של משתמש הופרדו ממנו אך ניתן במאמץ סביר לזהות את המשתמש שאליו מתייחס המידע.

"השר" - שר הבריאות.

"מגע קרוב" - מרחק ופרק זמן שייקבע משרד הבריאות בקירבה המעלה חשש להידבקות בנגיף הקורונה החדש.

"מגעים" - מי שהיה במגע קרוב עם נשא מאומת של נגיף הקורונה החדש, ללא מיגון מספק.

"המחלה" - מחלה הנגרמת מנגיף קורונה החדש.

---

[1] ס"ח התש"ף, עמ' 166.

[2] ס"ח התשל"ז, עמ' 226.

"משתמש" - אדם שהתקין יישומון במכשיר שברשותו או משתמש בחומרה ייעודית, ומשתמש בהם למטרתם.

"נגיף קורונה החדש" - Novel Coronavirus 2019 – nCov.

"נתוני קירבה" - מידע בדבר מגע קרוב.

"רישיון קוד פתוח" - רישיון תוכנה חופשית של MIT או רישיון אחר כדוגמתו שאישרה הוועדה המפקחת, המתיר שימוש, העתקה, יצירת יצירה נגזרת והפצה של טכנולוגיות לאיתור מגעים בלא תשלום ותוך גישה מלאה לקוד המקור ושל התוכנות המשמשות בהן.

"קוד המקור" - כל קוד תוכנה ומפרט חומרה המשמשים בטכנולוגיה לאיתור מגעים.

"צו הבידוד" - צו בריאות העם (נגיף הקורונה החדש)(בידוד בית והוראות שונות)(הוראת שעה), התש"ף-2020 [3].

3. פיתוח טכנולוגיות לאיתור מגעים

(א) הממשלה תפתח טכנולוגיות לאיתור מגעים, בין באמצעות משרד ממשלתי או רשות מרשויות המדינה, ובין בסיוע חברות פרטיות, לפי העקרונות המפורטים בחוק זה.

(ב) הממשלה תפיץ את הטכנולוגיות לאיתור מגעים ותקדם את השימוש בהן בקרב הציבור הרחב בישראל – והכל, על-פי הוראות חוק זה.

4. טכנולוגיות לאיתור מגעים

(א) הטכנולוגיות לאיתור מגעים ינטרו מגע קרוב.

(ב) טכנולוגיות לאיתור מגעים יתוכננו ויופעלו לפי עקרונות של הנדסת פרטיות (Privacy by Design) במטרה לצמצם את הפגיעה בפרטיות למידה שאינה עולה על הנדרש, לשם השגת תכליתן. בכלל זה –

1) התקנת הטכנולוגיות לאיתור מגעים והשימוש בה ייעשו רק לפי הסכמתו מדעת של המשתמש, ומתוך רצונו החופשי.

2) טכנולוגיות לאיתור מגעים לא יאספו, יפיצו או ימסרו מידע אישי מזהה.

3) טכנולוגיות לאיתור מגעים יאספו את המידע המינימלי הדרוש להן למילוי ייעודן.

4) כל המידע על אודות המשתמשים שיעובד בטכנולוגיות לאיתור מגעים יהיה אנונימי ומוצפן, באופן שלא יאפשר לאחזר את מיקום המשתמשים או את הקירבה שלהם לאחרים.

[3] ק"ת התש"ף, עמ' 516.

5) המידע הדרוש לטכנולוגיות לאיתור מגעים לשם מילוי ייעודן, ובפרט נתוני קירבה, יישמר ככל הניתן רק על-גבי ההתקן הנייד או החומרה הייעודית שבה היא מותקנות.

6) נתוני קירבה שנאספו ונשמרו בטכנולוגיות לאיתור מגעים יימחקו מאליהם לאחר 21 יום.

7) טכנולוגיות לאיתור המגעים תאפשרנה למשתמש שאומת כנשא של המחלה לעדכן משתמשים אחרים בטכנולוגיות לאיתור מגעים ,שהיו במגע קרוב איתו ב-14 הימים שקדמו לאבחונו, אגב ציון מועד מקורב של השהות - וזאת מבלי לזהות את המשתמש החולה.

8) טכנולוגיות לאיתור מגעים יכללו אמצעים למנוע העברת מידע מן הטכנולוגיות אלא בהסכמה: בפעולה רצונית ומודעת של המשתמש.

9) לא יועבר מידע מן הטכנולוגיות לאיתור מגעים לידי הממשלה, אלא בהסכמת המשתמש ומרצונו החופשי.

10) החומרה הייעודית תאפשר קבלת עדכונים בדבר מגע קרוב עם משתמש שאובחן כחולה במחלה, באופן מאובטח ומוצפן ובלא לזהות את המשתמש בה.

(ג)

1) השימוש בטכנולוגיות לאיתור מגעים ילווה במדיניות פרטיות ותנאי שימוש פשוטים, קצרים ובהירים בשפות הרלוונטיות. מדיניות הפרטיות ותנאי השימוש לא ישונו אלא בהסכמה מדעת ומרצון חופשי של המשתמש.

2) הודעה על שינוי מדיניות הפרטיות תתפרסם לפני כניסת השינוי לתוקף ולא יאוחר משבעה ימים לפני השינוי בשפות רלוונטיות;

3) "שפות רלוונטיות" בסעיף זה: עברית, ערבית, רוסית, אנגלית ואמהרית.

(ד) טכנולוגיות לאיתור מגעים יאפשרו תאימות (Interoperability) עם אמצעים דומים אחרים לאיתור מגעים.

(ה) השימוש ביישומונים יוצע לכל הציבור ללא תשלום כלשהו. הממשלה תממן חומרה ייעודית כך שתוצע בלא תשלום למשתמשים או תקבע מחיר מירבי שווה לכל נפש לחומרה הייעודית.

(ו) הממשלה תעודד יצרנים פרטיים לייצר, לייבא ולשווק את החומרה הייעודית, בהתאם לאמור בחוק זה.

5. קוד פתוח

(א) הממשלה תפיץ את הטכנולוגיות לאיתור מגעים לציבור תחת רישיון קוד פתוח.

(ב) הממשלה תפרסם את קוד המקור העדכני של הטכנולוגיות לאיתור מגעים במאגר מידע מקובל לצורך זה, ותאפשר בכל עת גישה חופשית לקוד המקור. הממשלה תפרסם באופן שוטף כל

עדכון לקוד המקור שביצעה. הממשלה לא תפיץ טכנולוגיות לאיתור מגעים אלא לאחר פירסום קוד המקור המלא שלהן.

6. הגבלת שימושים וסודיות

(א) לא ייעשה שימוש בטכנולוגיות לאיתור מגעים ובנתוני קירבה אלא לשם מניעת הידבקות במחלה.

(ב) אדם שהגיע אליו מידע אישי מזהה על משתמש, לרבות נתוני קירבה ומידע רפואי, ישמרנו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לצורך ביצוע הוראות חוק זה.

(ג) לא ייעשה שימוש בנתוני קירבה לצורך הליך משפטי, לרבות חקירה על פי דין, והם לא יתקבלו כראיה במשפט.

7. לוחות זמנים

(א) הממשלה תעמיד גרסה ראשונה של היישומונים לרשות הציבור לא יאוחר מ-30 יום מכניסת חוק זה לתוקף וגרסה ראשונה של החומרה הייעודית לא יאוחר מ-60 יום לאחר מכן.

(ב) הממשלה תעדכן את הטכנולוגיות לאיתור מגעים באופן שוטף, רצוף ומהיר במטרה לתקן כל תקלה שהתגלתה בתפקודן בהקדם האפשרי .

8. עידוד הציבור להשתמש בטכנולוגיות לאיתור מגעים

השר יגבש תכנית לאומית לעידוד הציבור להשתמש בטכנולוגיות לאיתור מגעים ויקצה את התקציב הדרוש לשם מימושה.

9. פקיעת תוקף הסמכת השב"כ לפי חוק ההסמכה

הממשלה תקבע באישור ועדת חוץ וביטחון בכנסת את מספר החולים במחלה ומספר המשתמשים בטכנולוגיות לאיתור מגעים ואמות מידה נוספות, אשר בהתקיימן תפקע הסמכת שירות הביטחון הכללי לסייע למשרד הבריאות על-פי חוק ההסמכה.

10. הוועדה המפקחת

(א) תמונה ועדה שתפקידה לייעץ לגבי המשך פיתוחן של הטכנולוגיות לאיתור מגעים, לרבות היבטים של קידום השימוש שלהן בציבור, ולפרסם דוחות לציבור.

(ב) הרכב הוועדה יהיה כדלקמן –

1) שופט בית משפט מחוזי בדימוס או משפטן בכיר שהוא בעל כשירות לשמש כשופט בית משפט מחוזי, שימנה השר – והוא היו"ר.

2) נציג משרד הבריאות שימנה השר;

3) נציג מן האקדמיה שהתמחותו בטכנולוגיה ומדעי המחשב שימנה שר המדע והטכנולוגיה;

4) נציג ציבור שהתמחותו היא במדעי החברה שימנה שר החינוך;

5) נציג ציבור שהוא משפטן שהתמחותו בפרטיות שימנה שר המשפטים;

6) נציג היועץ המשפטי לממשלה;

7) נציג אירגונים מן החברה האזרחית שעיסוקם בפרטיות שימנה שר המשפטים.

(ג) על השר להיוועץ בוועדה המפקחת לפני פרסום הטכנולוגיה לאיתור מגעים לציבור. הוועדה תהיה מוסמכת להביע עמדה פומבית.

(ד) חבר הוועדה המפקחת לא יהא נתון לכל מרות במילוי תפקידיו לפי חוק זה זולת מרות החוק ויפעיל שיקול דעת עצמאי.

(ה) הוועדה המפקחת תהיה רשאית לקבל מכל אדם כל מידע וכל מסמך הדרוש לה לצורך מילוי תפקידה. אדם שהוועדה פנתה אליו, חייב יהיה להעביר כל מידע ומסמך שהתבקשו בתוך פרק זמן סביר.

(ו) הוועדה המפקחת תפרסם מעת לעת דוחות לציבור בדבר השימוש בטכנולוגיות לאיתור מגעים, תקלות שהתגלו בשימוש בהן, התפתחות הטכנולוגיות לאיתור מגעים בעולם תוך דגש על טכנולוגיות משמרות פרטיות, המלצות להמשך הטכנולוגיות לאיתור מגעים בישראל וכל עניין אחר שהוועדה סבורה כי יש חשיבות ציבורית לפרסמו.

11. פרסום מידע לציבור

(א) משרד הבריאות יפרסם באתר המשרד באינטרנט, באופן שוטף ורצוף, את כל המידע הגולמי המצטבר שנאסף באמצעות טכנולוגיות לאיתור מגעים, ככל שנצבר בידי המשרד מידע כזה, ובלבד שלא יפורסם מידע מזהה אישי מזהה.

(ב) משרד הבריאות יפרסם באתר המשרד באינטרנט מידע מעובד מתוך המידע הגולמי שנאסף כאמור בסעיף-קטן (א) הכולל לפחות את אלה -

(1) מספר המשתמשים המצטבר שהתקינו או רכשו טכנולוגיות לאיתור מגעים;

(2) מספר המשתמשים בפועל בטכנולוגיות לאיתור מגעים תוך אבחנה ביניהן.

(3) מספר האנשים שדיווחו כי קיימו מגע קרוב עם חולה במחלה בעקבות התראה שקיבלו באמצעות הטכנולוגיות לאיתור מגעים;

(4) מספר האנשים המצויים בבידוד בעקבות התראה שקיבלו באמצעות טכנולוגיות לאיתור מגעים;

(5) מספר האנשים שהתגלו כחולים מבין מי שדיווחו כי קיימו מגע קרוב עם חולה במחלה בעקבות התראה שקיבלו באמצעות טכנולוגיות לאיתור מגעים.

(6) נתונים נוספים כפי שתקבע הוועדה המפקחת, בהיוועצות עם משרד הבריאות

(ג) משרד הבריאות יפרסם באתר המשרד באינטרנט מידע משלים הכולל לפחות את אלה -

(1) מספר האנשים המצויים בבידוד שלא בעקבות התראה שקיבלו באמצעות טכנולוגיות לאיתור מגעים;

(2) מספר האנשים שהתגלו כחולים מבין מי שדיווחו כי קיימו מגע קרוב עם חולה במחלה שלא בעקבות התראה שקיבלו באמצעות טכנולוגיות לאיתור מגעים.

(3) נתונים נוספים כפי שתקבע הוועדה המפקחת, בהיוועצות עם משרד הבריאות

12. עונשין

(א) העושה אחת מאלה, דינו מאסר שנה או קנס כאמור בסעיף 61(א)(3) לחוק העונשין -

1) העובר על סעיף 6(א) או סעיף 6(ב) לחוק זה.

2) משתמש במידע אישי מזהה שנאסף או התקבל באמצעות טכנולוגיות לאיתור מגעים, שלא למטרה שלשמה נועד.

3) דורש מאדם למסור לו מידע שנאסף או התקבל באמצעות הטכנולוגיות לאיתור מגעים, אולם אין בהוראת סעיף זה כדי למנוע בקשה מאדם להפיץ נתוני קירבה לכל משתמשי החלופות לאחר שנמצא כי נדבק במחלה.

4) נמנע ממסירת מידע או מסמכים לוועדה המפקחת.

(ב) העושה אחת מאלה, דינו מאסר שלוש שנים או כפל קנס כאמור בסעיף 61(א)(3) לחוק העונשין -

1) דורש מעובדו או מי שנתון למרותו בדרך אחרת למסור לו מידע שנאסף או התקבל באמצעות טכנולוגיות לאיתור מגעים, אולם הוראת סעיף זה לא תחול על הורה כלפי ילדיו.

(ג)

1) נושא משרה בתאגיד חייב לפקח ולעשות כל שניתן למניעת עבירה מהעבירות המפורטות בסעיף זה (בסעיף זה – עבירה) בידי התאגיד או בידי עובד מעובדיו; הפר את חובתו האמורה, דינו – הקנס הקבוע בסעיף 61(א)(4) לחוק העונשין.

2) נעברה עבירה בידי תאגיד או עובד מעובדיו, חזקה היא כי נושא המשרה הפר את חובתו לפי סעיף קטן (א), אלא אם כן הוכיח כי עשה כל שניתן כדי למלא את חובתו האמורה.

3) בסעיף זה, "נושא משרה" – מנהל פעיל בתאגיד, שותף, למעט שותף מוגבל, ופקיד האחראי מטעם התאגיד על התחום שבו בוצעה העבירה.

13. ביצוע ותקנות

השר רשאי להתקין תקנות לביצועו של חוק זה, באישור ועדת החוץ והביטחון של הכנסת.

14. תוקף

חוק זה יעמוד בתוקף כל זמן שצו הבידוד - או כל הוראה אחרת בעלת פועל תחיקתי הבאה במקומו - עומד בתוקף.