











## המכון הישראלי לדמוקרטיה

עוד מאפשר התזכיר לראש השב"כ להתיר בעצמו קבלה או איסוף של מאגר מידע, בנסיבות בהן קיים צורך דחוף בכך ולא ניתן בפרק הזמן הדרוש לקבל היתר כאמור מרה"מ. במקרה שכזה עדיין אין המאגר יכול לכלול מידע בעל רגישות מיוחדת ועל ראש השב"כ לשקול בעצמו את נחיצות הפגיעה בפרטיות ומידתיותה. על ראש השב"כ להודיע מיד לרה"מ וליועמ"ש על מתן היתר כאמור על ידו ולרה"מ סמכות לבטלו. עם זאת, לא ברור מהם השיקולים אותם על הרה"מ לשקול בבואו לבחון האם לבטל היתר שנתן ראש השב"כ או להשאירו על כנו. כמו כן, לא נדרשת חו"ד מטעם היועץ המשפטי לממשלה בנושא.<sup>22</sup>

על אף מגבלת המטרות הנדרשת לשם קבלה או איסוף של מאגר מידע, מרגע שניתן היתר, השב"כ רשאי לעשות שימוש במאגר מידע לצורך מילוי כל משרעת תפקידיו לפי סעיף 7 לחוק השב"כ, ובלבד שהשימוש לצורך התפקידים שאינם מנויים בסעיף 7(ב)(1) ו-2(2) יעשה בהתאם לכללים "ובאופן שיצמצם את מידת הפגיעה בפרטיות".<sup>23</sup> אם מאגר המידע כולל "אמצעי ביומטרי שניתן להפיק ממנו נתון ביומטרי", רשאי השב"כ להפיק נתון ביומטרי ולעשות בו שימוש על בסיס צורך פרטני בלבד, בהתאם לכללים ובאופן שיצמצם את הפגיעה בפרטיות.<sup>24</sup>

השב"כ רשאי, באישור ראש השב"כ, להעביר מאגר מידע לגורם אחר, ובלבד שמאגר המידע אינו כולל מידע על תושבי ישראל, שההעברה תעשה לפי "כללים", בהתקיים "טעמים מיוחדים", וכאשר ההעברה נחוצה לצורך מילוי כלל תפקידי השירות. בעת מתן אישור כאמור על ראש השב"כ לשקול, בין השאר, שיקולים פנימיים של השב"כ – האם ההעברה עלולה לפגוע במקורות מידע או בשיטות פעולה, לצד בחינת הפגיעה בפרטיות ולהשתכנע שהצורך בהעברה עולה על פגיעות אפשריות אלו.<sup>25</sup>

(2) **עדכונים לסמכות השימוש ב"כלי" של השב"כ.** לפי דברי ההסבר לתזכיר,<sup>26</sup> נוכח השינויים המשמעותיים בעולם התקשורת, בעיקר בכל הקשור לפעילות ברשת האינטרנט, יש צורך לעדכן את סמכות השירות לקבל מידע מ"ספק מורשה", בהגדרתו בחוק התקשורת, כך שהגדרת 'מידע' בחוק השב"כ תכלול עתה במפורש "נתוני תקשורת", "נתונים הנוגעים להפעלת מערכות תקשורת, למעט תוכן שיחה כמשמעותו בחוק האזנת סתר" ו"נתוני שימוש באינטרנט שאינם תוכן שיחה בין אנשים".<sup>27</sup>

סוגי המידע הדרושים לשב"כ לצורך מילוי תפקידיו לפי סעיף 7 לחוק השב"כ, ייקבעו בכללים על ידי ראש המשלה. לגבי נתוני שימוש באינטרנט, יקבע הרה"מ בכללים סוגי מידע הנחוצים לצורך סיכול טרור או ריגול ואבטחת אישים, לפי סעיף 7(ב)(1) ו-2(2) בלבד. בבואו לנסח את הכללים ישקול ראש המשלה את מידתיות הפגיעה בפרטיות וישתכנע שהתועלת שתופק מקבלת סוגי המידע שיקבעו על ידו עולה על מידת הפגיעה בפרטיות.

<sup>22</sup> סעיף 8א(ג) המוצע בתזכיר.

<sup>23</sup> סעיף 8א(ה)(1) לחוק השב"כ.

<sup>24</sup> סעיף 8א(ו) המוצע בתזכיר.

<sup>25</sup> סעיף 8ב המוצע בתזכיר.

<sup>26</sup> סעיף ג, עיקר 2 לדברי ההסבר בתזכיר.

<sup>27</sup> התיקון המוצע בתזכיר לסעיף 11(א) לחוק השב"כ, הגדרת "מידע".



## המכון הישראלי לדמוקרטיה

בכפוף לכללים, יהיה ראש השב"כ רשאי להורות לספק מורשה, כהגדרתו בחוק התקשורת, להעביר לשב"כ מידע המצוי בידיו, ובלבד שטרם מתן ההוראה ישקול את מידת הפגיעה בפרטיות ואת מידת הפגיעה בספק וסיק שהמדובר בפגיעה מידתית, כלומר שהמידע דרוש לצורך מילוי תפקידי השב"כ ושהתועלת שתופק מקבלתו עולה על הפגיעה. הוראה כאמור תעמוד בתוקפה חמש שנים, עם אפשרות להארכה ע"י ראש השב"כ לאחר בחינה מחודשת של נחיצות המידע ומידתיות הפגיעה. על ראש השירות לדווח לרה"מ וליועמ"ש בתוך 72 שעות על מתן ההוראה או הארכת ההוראה לספק מורשה, ולרה"מ הסמכות לבטלה או לסייגה.

השימוש במידע שיתקבל מהספק המורשה ייעשה בכפוף לקבלת אישור ראש השב"כ בהתקיים התנאים הבאים: (1) השימוש דרוש לצרכי מילוי תפקידי השב"כ; (2) השימוש יעשה באופן שיצמצם את מידת הפגיעה בפרטיות. לצורך קבלת המידע או שימוש בו מוסמך השב"כ לבצע פעולות נלוויות שמטרתן הנגשת סוגי המידע המתקבלים. מהותן של הפעולות הנלוות לשם הנגשה אינה מפורטת בתזכיר.<sup>28</sup>

3) **הרחבת סמכויות חיפוש גלוי בתחנת גבול וחיפוש סמוי** כך שיחולו גם בהקשרי מחשב וחומר מחשב. לצד ההבהרה שחיפוש גלוי בתחנת גבול כולל גם חיפוש בחומר מחשב<sup>29</sup>, החידוש העיקרי הוא מתן סמכות לבצע חיפוש סמוי בחומר מחשב, למשל החדרה חשאית של רוגלות מעקב למחשבים ולמכשירי טלפון סלולריים.

בהתאם לתזכיר, יוכל ראש הממשלה להתיר לשב"כ לבצע חדירה לחומר מחשב או ל"דבר המגלם חומר מחשב", עריכת חיפוש סמוי בו ואיסוף מידע, לרבות מאגר מידע, בהתקיים הדרישות הבאות: (1) רה"מ שוכנע שדבר המגלם חומר מחשב מצוי מידע החיוני לשם הגשמת תפקידי השב"כ לפי סעיפים 7(ב)(1), (2) ו-6 לחוק השב"כ; (2) מידתיות: לא ניתן באופן סביר להשיג את אותה מטרה בדרך שפגיעתה בפרטיות פחותה.

בבקשה לקבלת היתר על ראש השב"כ לפרט, בין השאר, את המידע שברצונו לאסוף, אופן ביצוע החיפוש והאיסוף, ככל שפרטי מידע אלו ידועים לו מראש, את הצורך באיסופו של אותו מידע ואת תקופת ההיתר המבוקשת. רק אם היה המחשב או הדבר המגלם חומר מחשב אצל עו"ד, רופא, פסיכולוג, עובד סוציאלי או כהן דת (להלן: **"בעלי מקצוע"**), יש לפנות לבית משפט לקבלת היתר לביצוע חיפוש סמוי כאמור. ראש השב"כ רשאי להתיר ביצוע חיפוש סמוי בעצמו אם הנסיבות אינן סובלות דיחוי. במקרה כזה עליו

<sup>28</sup> התיקון המוצע בתזכיר לסעיף 11 לחוק השב"כ.

<sup>29</sup> לפי התיקון המוצע לסעיף 9(א) לחוק השב"כ חיפוש גלוי בתחנת גבול הינו בסמכות בעלי התפקידים מהשב"כ בתחנת הגבול ובלבד שנעשה "לצורך" סיכול ומניעה של פעילות בלתי חוקית שמטרתה לפגוע בביטחון המדינה, בסדרי המשטר הדמוקרטי או במוסדותיו" לפי סעיף 7(ב)(1) לחוק השב"כ, לשם "אבטחת אנשים, מידע ומקומות, שקבעה הממשלה", לפי סעיף 7(ב)(2) לחוק השב"כ, או לשם "פעילות בתחום אחר שקבעה הממשלה, באישור ועדת הכנסת לענייני השירות, שנועדה לשמור ולקדם אינטרסים ממלכתיים חיוניים לביטחון הלאומי של המדינה", לפי סעיף 7(ב)(6) לחוק השב"כ. חיפוש סמוי בתחנת גבול מצוי אף הוא בתחום סמכותו של בעל התפקיד בשב"כ בתחנת הגבול, אולם לשם הפעלת הסמכות נדרשות: (1) סבירות: לבעל התפקיד יסוד סביר להניח שהחיפוש יוביל לתפיסת "חפץ" החיונית למילוי תפקידי השירות לפי סעיפים 7(ב)(1), (2) ו-6; (2) מידתיות: לא ניתן להשיג את מטרת החיפוש באופן סביר בדרך אחרת שפגיעתה בזכות לפרטיות פחותה. התיקון המוצע לסעיף 9(ב) לחוק השב"כ.



לדווח על כך לרה"מ בתוך 48 שעות ולרה"מ הסמכות לבטל את ההיתר או להאריכו. לא ברור מן התזכיר אם סמכותו זו של ראש השב"כ מתקיימת גם כאשר מדובר בחיפוש סמוי אצל אחד מבעלי המקצוע, ואם מתקיימת האם על ראש השב"כ לפנות לקבלת היתר מבהמ"ש בדיעבד.<sup>30</sup>

4) **סמכות לביצוע פעולה בחשאי בחומר מחשב.** "פעולה" מוגדרת בתזכיר כחדירה לחומר מחשב, שיבוש פעולתו של מחשב או הפרעה לשימוש בו, מחיקה, שינוי או שיבוש של חומר מחשב או הפרעה לשימוש בו. העתקה, עיון והפקה של חומר מחשב אינן נחשבות ל"פעולה" כאמור.<sup>31</sup> לפי דברי ההסבר סמכות זו נדרשת נוכח השימוש הגובר מצד גורמי טרור במרחב הסייבר ובטכנולוגיות מתקדמות.

בהתאם לתזכיר ראש הממשלה מוסמך להיתר לשב"כ לבצע פעולה בחשאי בחומר מחשב ובלבד שמתקיימות הדרישות הבאות: (1) רה"מ שוכנע שהפעולה חיונית לשם סיכול או מנעה של פעילות טרור או ריגוש שיש בה סיכון חיי אדם או פגיעה חמורה בביטחון המדינה; (2) מידתיות – לא ניתן, באופן סביר, להשיג את המטרה בדרך אחרת שפגיעתה בזכויות פחותה; (3) אם מדובר בחומר מחשב המשמש בעלי מקצוע, הבקשה להיתר מוגשת לרה"מ באישור היועמ"ש או פרקליט המדינה. בבקשה להיתר על ראש השב"כ לפרט את העובדות והנימוקים למתן ההיתר, סוג הפעולה המבוקשת, תיאור חומר המחשב שביחס אליו מבוקש ההיתר, לרבות זהות מי שהמחשב בבעלותו או בשליטתו, ככל שהדבר ידוע, והוראות ותנאים לביצוע הפעולה המבוקשת.

כאשר ביצוע הפעולה חיוני ואינו סובל דיחוי, רשאי ראש השב"כ להתירה בעצמו לתקופה של 48 שעות, עם אפשרות להארכה בכפוף לקבלת היתר מרה"מ. אולם, על ראש השב"כ לדווח מיידי על מתן ההיתר לרה"מ, אשר מוסמך לבטלו. אם מדובר בביצוע פעולה בחומר מחשב המשמש בעלי מקצוע, על ראש השב"כ לדווח במידי גם ליועמ"ש, והאחרון מוסמך גם כן לבטלה.<sup>32</sup>

5) **סמכות שירות עתידית.** מוצע בתזכיר שוועדת השרים לענייני השירות, באישור ועדת הכנסת לענייני השירות, תוכל להעניק לשירות סמכות נוספת על אלו הקבועות בחוק השב"כ לעניין **מידע או סוגי מידע**, במידה שיתעורר צורך חיוני בסמכות שכזו והסמכויות הקיימות בחוק לא יתנו לו מענה. הסמכות השירותית תוענק לפרק זמן מוגבל הניתן להארכה.<sup>33</sup>

<sup>30</sup> התיקון המוצע לסעיף 10 לחוק השב"כ.

<sup>31</sup> סעיף 10ב המוצע בתזכיר.

<sup>32</sup> סעיף 10א המוצע בתזכיר.

<sup>33</sup> סעיף 11א המוצע בתזכיר.



## חלק ב: ביקורת על מתווה הפיקוח על סמכויות השב"כ המוצע בתזכיר

### 1. הדרישות לבחינת נחיצות ומידתיות אינן מספקות והן "למראית עין"

התזכיר מחייב בחינה של נחיצות מאגר המידע, המידע, החיפוש הסמוי או הפעולה בחומר מחשב, בעת מתן היתר על ידי ראש הממשלה או בנסיבות דחופות על ידי ראש השב"כ. "נחיצות" זו היא ביחס למילוי תפקידי השירות, ודורשת הערכה שהתועלת שתופק עולה על הפגיעה בפרטיות. לדעתנו, על אף שהתזכיר משתמש במינוחים הנכונים לכאורה, בפועל, אין מדובר במימוש מהותי של דרישות הנחיצות והמידתיות. זאת, מן הטעמים הבאים:

- התזכיר אינו מתעדף, בשום שלב, איסוף מידע באופן ממוקד על פני איסוף עיוור של מידע (bulk collection) ובכך למעשה מאיין את ההיבט הבסיסי ביותר של בחירה באפשרות פוגענית פחות, בהיבט של נחיצות ומידתיות.
- רשימת מטרות רחבה מאד שמולה מתבצעות בדיקת המידתיות והנחיצות: העניין המרכזי המשליך באופן ישיר על בחינת מידתיות ונחיצות הפגיעה בפרטיות, הוא המטרות לשמן מוענקת כל אחת מסמכויות המעקב הפולשניות. אולם רשימת מטרות זו מוגדרת לאורך התזכיר באופן רחב ביותר.

הנה כמה דוגמאות:

קבלה או איסוף מאגר מידע הם אפשריים לצורך<sup>34</sup> "סיכול ומניעה של פעילות בלתי חוקית שמטרתה לפגוע בביטחון המדינה, בסדרי המשטר הדמוקרטי או במוסדותיו",<sup>35</sup> וכן לשם "אבטחת אנשים, מידע ומקומות, שקבעה הממשלה",<sup>36</sup> שהיא מטרה מעורפלת העשויה להוות פתח לשימוש לרעה בסמכות, למשל לשם הרחקת ביקורת או יריבים פוליטיים;

לאחר קבלת מאגר המידע או איסופו, מותר השימוש בו להשגת כל אחד מתפקידי השב"כ ובכללם "קביעת הוראות בדבר סיווג ביטחוני לתפקידים ולמשרות",<sup>37</sup> או "קביעת נהלי אבטחת לגופים שקבעה הממשלה"<sup>38</sup>;

קבלת נתוני תקשורת ונתונים הנוגעים להפעלת מערכות תקשורת, מותרת למטרת מילוי כל תפקידי השירות לפי חוק השב"כ,<sup>39</sup> ומדובר במשרעת מטרות רחבה מאד; קבלה או איסוף נתוני שימוש באינטרנט מוגבלת רק למטרות סיכול טרור, ריגול או אבטחת אישים,<sup>40</sup> אולם הכללת המטרה של "אבטחת אישים" מעוררת חשש כבד לפוליטיזציה;

<sup>34</sup> סעיף 8א(ב)(1) המוצע בתזכיר.

<sup>35</sup> סעיף 7(ב)(1) לחוק השב"כ.

<sup>36</sup> סעיף 7(ב)(2) לחוק השב"כ.

<sup>37</sup> התיקון המוצע בתזכיר לסעיף 7(ב)(3) לחוק השב"כ.

<sup>38</sup> סעיף 7(ב)(4) לחוק השב"כ.

<sup>39</sup> התיקון המוצע בתזכיר לסעיף 11(ב), (ב1) לחוק השב"כ.

<sup>40</sup> התיקון המוצע בתזכיר לסעיף 11(ב), (ב1) לחוק השב"כ.







השירות לקבוע. כך, למשל, שימוש במאגר מידע מעבר למטרות לשמן התקבל היתר לקבלו או לאוספו, או שימוש בנתון ביומטרי שיופק ממאגר מידע הכולל אמצעי ביומטרי,<sup>49</sup> מותר לפי "הכללים".<sup>50</sup>

• **אי בהירות:** לא ברור מלשון התזכיר שבחינת הנחיצות והמידתיות תבצע כל אימת שמתקבלת החלטה המתירה שימוש בסמכות מעקב פולשנית. הנה כמה דוגמאות: לא ברור האם בעת בחינת היתר שנתן ראש השב"כ בנסיבות בהן קיים צורך דחוף או בעת הארכת תוקפו של היתר לקבלה או לאיסוף של מאגר מידע, או הארכת תוקפה של הוראה המחייבת ספק מורשה להעביר מידע לשירות, נדרשת בחינה מחודשת של נחיצות ומידתיות הפגיעה בפרטיות; נדרש ששימוש בפועל במידע ממאגר מידע או מידע שהתקבל מספק מורשה יעשה "באופן שיצמצם את מידת הפגיעה בפרטיות",<sup>51</sup> אולם לא ברור האם, כיצד ועל ידי מי יבוצעו בחינת הנחיצות והמידתיות בהקשר זה; בעת ביצוע חיפוש גלוי או סמוי בתחנת גבול ההחלטה בדבר נחיצות ומידתיות הפגיעה בפרטיות נתונה לבעל התפקיד בתחנת הגבול, אולם לא ברור מהי הכשרתו ומומחיותו להעריך את הנחיצות והמידתיות האמורה או לפי אלו כללים יבצע את ההערכה.

## 2. היעדר מנגנוני פיקוח עצמאיים; היעדר מומחיות בתחום הגנת הפרטיות בקרב גורמי הפיקוח

מסגרת הפיקוח על הפעלת הסמכויות שבתזכיר אינה שונה מהותית מזו שבהסדר הקיים. רובה מסורה לרשות המבצעת, בחלוקה בין ראש הממשלה, ראש השב"כ ומשרד המשפטים, ובדיווח לוועדת הכנסת לענייני השירות,<sup>52</sup> ובמרבית המקרים לא נדרש פיקוח מראש (אקס אנטה) של בית המשפט או אפילו של היועץ המשפטי לממשלה.<sup>53</sup> בכך למעשה התזכיר שלפנינו מבקש להרחיב באופן משמעותי את סמכויות שב"כ מבלי לשנות את המסגרת הבעייתית ממילא של הפיקוח עליו. עניין זה מקבל משנה חשיבות כאשר מדובר בכלי מעקב חשאיים, רחבי היקף ונוגעים לכלל אזרחי מדינת ישראל ללא כל חשד מוקדם נגדם.

בנוסף, התזכיר אינו כולל מנגנון ייעודי למתן סעד לנושאי מידע הרואים עצמם נפגעים עקב פעולות השב"כ. סעיף 18 לחוק השב"כ מעניק לשירות פטור רחב מאחריות אזרחית ופוליטית, ולכן הסיכוי לקבלת סעד אפקטיבי ויעיל במציאות בה מרבית מפעילות השב"כ נעשית באופן חסוי וסודי, הוא נמוך.

לכאורה, יכול נושא מידע לפנות לבג"צ בטענה לפגיעה בזכותו לפרטיות או לפנות לבג"ץ באופן כללי בטענה על חריגה מסמכות של השירות. הפניה לבג"צ אינה יכולה גם להחליף מנגנון פיקוח חיצוני מקצועי, המעורה בנושאים המשפטיים והטכנולוגיים הרלוונטיים לזכויות אדם, לצרכי ביטחון המדינה ואפשרויות והשלכות השימוש בטכנולוגיות מעקב שונות, ויש בידו לפקח על הפעלת הסמכות החשאית בזמן אמת. ביקורת שיפוטית בדיעבד בישראל, כמו בעולם, היא

<sup>49</sup> סעיף 8א(ו) המוצע בתזכיר.

<sup>50</sup> סעיף 8א(ה)(1) לחוק השב"כ.

<sup>51</sup> סעיף 8א(ה)(1) המוצע בתזכיר, והתיקון המוצע לסעיף 11 לחוק השב"כ.

<sup>52</sup> עמיר כהנא ויובל שני, רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה בעמודים 181-212 (2019).

<sup>53</sup> פיקוח אקס אנטה ע"י היועמ"ש או ביהמ"ש קיים רק ביחס למעקב על בעלי מקצוע. ראו סעיף 10א המוצע בתזכיר, והתיקון המוצע לסעיף 11(ה) לחוק השב"כ.



ריאקטיבית ותלויה ב"תאונות ליטיגציה".<sup>54</sup> בהקשר זה נפנה להצעתם של כהנא ושני לקדם את הקמתו של גוף פיקוח מקצועי, ייעודי ושלו סמכות לפקח מראש ובדיעבד על פעילות סיגינטית, בדומה למודל הבריטי של נציבות סמכויות חקירה (IPCO).<sup>55</sup>

מעבר לכל אלה נדגיש את הנקודות הבאות:

- **הדיווחים העיתיים אינם אופרטיביים.** לפי התזכיר, על ראש השב"כ למסור דיווחים עיתיים לרה"מ, ליועמ"ש ולוועדת הכנסת לענייני השירות. אולם, אין כל הוראה בדבר סמכויות הפיקוח האופרטיביות של גורמים אלו ובדבר מחויבות השב"כ לפעול במידה ויגיבו לדיווחים הנמסרים להם וידרשו הבהרות או תיקונים.<sup>56</sup> סמכות הפיקוח האופרטיבית של הרה"מ או היועץ המשפטי לממשלה (אף שהן שונות מהותית זו מזו) מוגבלת רק למקרים בהם התיר ראש השב"כ בעצמו איסוף מידע או ביצוע פעולה בעצמו.<sup>57</sup>
- **הדיווח ליועץ המשפטי לממשלה אינו מספק את דרישת הפיקוח העצמאי החיצוני הנדרש.** היועמ"ש משמש גורם מפקח נוסף ומען לדיווחי ראש השירות לפי ההסדר הקיים בסעיף 11 לחוק השב"כ היום, ולפי זה המוצע בתזכיר. הליכי בקרה דומים מופעלים בקשר עם האזנות סתר של על ידי המשטרה, שגם ביחס אליהן הפיקוח של היועץ המשפטי לממשלה אינו יורד לפרטי הפרטים של כל צו וצו.<sup>58</sup> לא רק שסביר שהעומס המוטל על היועמ"ש מקשה על ביצוע פיקוח אפקטיבי, הרי שגם הפיקוח הסטטוטורי המוטל עליו עשוי להתייחס לעיתים לנושאי רחב. מאחר שאין כל דיווח על הנעשה במסגרת זו קשה להעריך את מידת האפקטיביות של הפיקוח, אולם ספק אם יש בו די.<sup>59</sup> נוסף על כך, נעיר כי חרף עצמאותו היחסית של מוסד היועץ המשפטי לממשלה, הגישה האירופית ככל הנראה לא תראה בגורם שהוא בשר מבשרה של הרשות המבצעת, גוף עצמאי דיו ותבקש גוף חוץ ממשלתי.
- **מנגנון הפיקוח הפנימי הקבוע בסעיף 13 לחוק השב"כ, אינו ממוקד,** מבחינת סמכויותיו או הכשרתו המקצועית, בבחינת פעולות הקשורות בעיבוד מידע ובהגנת פרטיות. יתרה מכך, אין כל הוראה המחייבת את השב"כ לנקוט פעולות אופרטיביות כלשהן ביחס לממצאי הביקורת הפנימית.

<sup>54</sup> ראו עמיר כהנא ויובל שני, רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה, חלק 3.2.2 (2019); Menachem Hofnung and Keren Weinsahl-Margel, *Judicial Rejection as Substantial Relief, in COURTS AND TERRORISM: NINE NATIONS BALANCE RIGHTS AND SECURITY* 150, 155 (Mary L. Volcansek and John F. Stack eds., 2011)

<sup>55</sup> למתווה המלא ראו עמיר כהנא ויובל שני, רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה -176 (2019) 183.

<sup>56</sup> סעיפים 8א(ז), 10א(ו), 11א(ב), המוצעים בתזכיר, התיקון המוצע לסעיפים 10(ד), 11(ד) לחוק השב"כ.  
<sup>57</sup> סעיפים 8א(ג), 10א(ג), 11(ב) (2) המוצעים בתזכיר, התיקון המוצע בתזכיר לסעיף 10(ב) לחוק השב"כ.

<sup>58</sup> ראו דברי השופט בדימוס זיילר בדוח ועדת החקירה הפרלמנטרית בעניין האזנות סתר **סיכום דיוני הוועדה** 9 (סימוכין 00416809, 2009) שם, בעמ' 29-30.  
<sup>59</sup>





רה"מ טרם קבלת ההחלטה, לרבות פירוט נחיצות המידע המבוקש.<sup>70</sup> רק במקרה של ביצוע פעולה בחומר מחשב נדרש אישור מקדים של היועמ"ש או פרקליט המדינה.<sup>71</sup>

כלומר, בידי ראש הממשלה כגורם יחיד מרוכזת סמכות רחבה וכבדת משקל. אנו סבורים כי מדובר בהסדר לא נכון מהותית ותפקודית.

**ראשית, אין לרה"מ את המומחיות הדרושה לשם בחינת השלכות הפעולות שמאשר על הזכות לפרטיות והערכת מידתיות הפגיעה בפרטיות.** חוות דעת מטעם יועמ"ש העשויות לסייע בנושא מוגשות רק במקרה של היתר לאיסוף או לקבלת מאגר מידע,<sup>72</sup> ואף גורם מקצועי בתחום הגנת הפרטיות לא אמור לתת את דעתו להשלכות הפעלת הסמכות טרם מתן האישור על ידי רה"מ.

**שנית, עומס המשימות העומדות בפני רה"מ ותכיפותן יקשה על ציות דווקני למתווה שיקול הדעת המוסדר בתזכיר ועל בירור לעומק של הסיכון לפגיעה בפרטיות, מידתיותה ונחיצותה.** לכן, סביר להניח שהדבר יעבור לדרגים נמוכים יותר, וההצהרה לגבי העובדה שראש הממשלה בעצמו מפקח על המתרחש תהיה בפועל ריקה מתוכן. כך, למשל, היועץ העצמאי הבריטי לחקיקה בענייני טרור, ציין את "העובדה המדהימה (לכל הפחות לאיש מן החוץ), ששרת הפנים חותמת אישית, כדבר שבשגרה, על אלפי צווים מדי שנה [ההדגשות במקור]", ותהה – בהנחה שהשר אכן שוקל בכובד הראש הראוי כל בקשה ובקשה – אם זהו אכן הניצול המיטבי של זמנו היקר של השר.<sup>73</sup>

**שלישית, ריכוז סמכות רחבה זו בידי רה"מ מעורר חשש לפוליטיזציה.** רשיונות שימוש ברוגלות מעקב הובילו ל"חוסר יכולת להתאפק" במדינות שונות ובכללן מקסיקו, הונגריה, הודו ועוד, ולשימוש ברוגלות נגד יריבים פוליטיים, רגולטורים, שופטים, פעילי זכויות אדם ועיתונאים.<sup>74</sup> מתן סמכות זו בידי ראש הממשלה, באופן חסוי ובקשר ישיר עם שב"כ עשויה ליצור ניגודי עניינים, לחצים בלתי ענייניים ושימוש לרעה, והכל הרחק מעינו הבוחנת של הציבור. אכן, באיחוד האירופי, למשל, הציעו להתמודד עם חשש כאמור לפוליטיזציה ושימוש לרעה של שר בסמכותו להפעיל את שירותי הביטחון על ידי להגביל את תלותם של ראשי גופי הביטחון בשר, לצמצם את סמכויותיהם ולעצב מנגנונים עצמאיים שיאפשרו לעובדי גופי הביטחון להביע את עמדתם ולדווח מקום שהם חוששים משימוש שלא כדין בסמכות השר.<sup>75</sup>

<sup>70</sup> סעיפים 8א(ב)(2), 10א(ד) המוצעים בתזכיר, התיקון המוצע בתזכיר לסעיף 10(ג) לחוק השב"כ.

<sup>71</sup> סעיף 10א(א) המוצע בתזכיר.

<sup>72</sup> סעיפים 8א(ב)(1) המוצעים בתזכיר.

<sup>73</sup> DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW Para 14.49 (2015).

<sup>74</sup> פיניאס רוקרט, פורבידן סטוריז, **הדלפת ענק חושפת את המדינות שהפכו עיתונאים למטרות מעקב** - בסיוע NSO הישראלית. מאזרבייג'ן, דרך הודו והונגריה ועד סעודיה ואיחוד האמירויות: הנתונים שדלפו מגלים כיצד נהפכה תוכנת פגסוס של NSO הישראלית לכלי למעקב ממשלתי אחר עיתונאים חוקרים. NSO טוענת שהמטרה היא לוחמה בטרור, אבל המציאות מספרת סיפור שונה. **דה מרקר**, 18.7.2021.

<sup>75</sup> European Commission for Democracy Through Law, *Report On The Democratic Oversight Of The Security Services*, Para. 150 (2015).



## חלק שלישי: חולשת מתווה דרישת המידתיות ומתווה הפיקוח שבתזכיר למול הדין הבינלאומי, השלכותיה

בחלק זה נסקור ארבעה משטרי אסדרה של מעקב על ידי רשויות ביטחון. הראשון היא הדין האירופי המשמש סטנדרט בין לאומי בתחומי הפרטיות, כפי שבא לידי ביטוי במסמך ההנחיות,<sup>76</sup> שגיבש ה-European Data Protection Board (להלן: "EDPB"),<sup>77</sup> ובפסיקת בית המשפט האירופי לזכויות אדם ובפסיקת בית המשפט האירופי לצדק.<sup>78</sup> השנייה היא החלטה נשיאותית 14086 של הנשיא ביידן,<sup>79</sup> המהווה את הבסיס להסכם החדש בין ארה"ב לנציבות האיחוד האירופי, EU-U.S. Data Privacy Framework, לאסדרת העברת מידע אודות נושאי מידע מהאיחוד האירופאי לארצות הברית.<sup>80</sup> השלישית היא הדין הבריטי הנתפס כמתיישב עם המשטר האירופי, הוא מבין המקיפים ביותר בתחום, ובו נדונות מרבית הסמכויות שבתזכיר חוק השב"כ. והרביעית היא הצהרת ה-OECD בדבר גישה ממשלתית למידע אישי,<sup>81</sup> שפורסמה בשלהי 2022 וחרף היותה מסגרת וולנטרית ויחסית רחבה בהגדרותיה, חשוב לבחון אותה מאחר שמדינת ישראל חתומה עליה.

### 1. האיחוד האירופי

ככל שמדובר בדין האירופי, המסגרת המשפטית הרלוונטית היא הוראות התקנות הכלליות להגנה על מידע (להלן: "GDPR") בנוגע להעברת מידע אישי אודות נושאי מידע מהאיחוד האירופי למדינות שאינן חברות באיחוד,<sup>82</sup> והתחולה האקס-טריטוריאליות הקבועה בהן.<sup>83</sup> שילובן הביא

---

<sup>76</sup> EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance Measures (Adopted on 10 November 2020) (להלן: "מסמך ההנחיות").

<sup>77</sup> ה-EDPB הוקם לפי סעיף 68 ל-GDPR ותפקידו להבטיח ציות נאות ל-GDPR, בין השאר באמצעות פרסום קווים מנחים, במסגרת סמכויותיו לפי סעיף 70 ל-GDPR.

<sup>78</sup> המדובר בעיקר בפסיקותיו של בית הדין האירופי לזכויות אדם (להלן: "CJEU") לעניין הסדרי נמלי ביטחון להעברת מידע ממדינות האיחוד לארצות הברית. ראו: CJEU judgment of 6 October 2015, Maximilian Schrems v. Data Protection Commissioner, Case C-362/14, EU: C: 2015: 650 (להלן: "שרמס I"); CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook (להלן: "שרמס II") וכן Ireland Ltd, Maximilian Schrems, case C-311/18, ECLI: EU: C: 2020: 559 (להלן: "Big Brother Watch and Others v. the United Kingdom" [GC, Applications no. 58170/13, 62322/14 and 24960/15], מרבית מהמלצות ה-CJEU כלולות במסמך ההנחיות.

<sup>79</sup> Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities"

<sup>80</sup> European Commission, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*, (July 10, 2023). נציין שגם הפעם טוען ארגון NOYB, שבראשו עומד מקס שרמס, שההסכם אינו מעניק הגנת זכויות שווה למי שאינם אזרחי ארה"ב, וכי בכונתו לאתגר אותו ב-CJEU. ראו *EU-US data transfer third round at CJEU* (July 10, 2023).

<sup>81</sup> OECD, *Declaration on Government Access to Personal Data held by Private Sector Entities*, OECD/LEGAL/048 available on <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487> (להלן: ההצהרה או הצהרת ה-OECD בדבר גישה ממשלתית).

<sup>82</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016 Para. 45-46



## המכון הישראלי לדמוקרטיה

למה שמכונה "אפקט בריסל"<sup>84</sup> במסגרתו הובילה חקיקת ה-GDPR לשינוי עולמי בתחום הגנת המידע. מדינות כגון קנדה, אוסטרליה וברזיל אימצו חקיקת פרטיות חדשה. כפי שנראה להלן, גם ארצות הברית נאלצה ליצור מסגרת משפטית חדשה בעניין זה. מנגד, מדינות שיימצאו ככאלה שאינן עומדות בסטנדרט הבינלאומי החדש לא רק ייפגעו מבחינה תפקודית וכלכלית, אלא ימצאו את עצמן בחברת מדינות שאינן חלק מן הגוש המערבי, כגון סין ורוסיה.<sup>85</sup>

אחד הנושאים המשמעותיים המשפיעים על החלטת נציבות האיחוד האירופי בשאלה האם להתיר העברת מידע אישי אודות נושאי מידע המצויים באיחוד האירופי למדינות מחוץ לאיחוד, הוא האם השימוש של רשויות ביטחון ואכיפת חוק באמצעי מעקב, עומד בדרישת הנחיצות והמידתיות.

דרישות הנחיצות והמידתיות הפגיעה שאובות מצ'ארטר זכויות היסוד האירופי,<sup>86</sup> ומהותן מפורטת במסמך ההנחיות של ה-EDPB המונה שורה של תנאים מצטברים:<sup>87</sup>

1. עיבוד המידע המוביל לפגיעה בפרטיות נעשה לפי חוק מחייב, למטרה ספציפית, על בסיס הסכמת נושא המידע או בסיס לגיטימי אחר המעוגן בחוק. החוק אמור לספק לאזרחים אינדיקציה ברורה לגבי הנסיבות והתנאים במסגרתן מוסמכות רשויות המדינה לנקוט באמצעי מעקב – ובכלל זה התנאים במסגרתם ניתן לעשות שימוש באמצעי מעקב, משך זמן השימוש, הקטיגוריות של נושאי מידע שעלולים להיות נתונים למעקב, ההליך לבחינת השימוש והאיחסון של המידע שייאסף, אמצעי הזהירות שיש ליישם כאשר מעבירים את המידע לגורמים נוספים, וכן אמצעי הגנה מינימליים.<sup>88</sup> היותו של החוק "מחייב" תיבחן בהתאם להכרה בחוקתיותו על ידי בית משפט במדינה בה נחקק.
2. מטרות עיבוד המידע לגיטימיות והפגיעה בפרטיות נחוצה ומידתית לשם השגתן. כך, למשל, נפסק שדרישה מספק תקשורת אלקטרונית לחשוף בפני רשויות הביון במדינה נתוני תעבורה ומיקום באופן כוללני וללא אבחנה, אינה עומדת בדרישת הנחיצות.<sup>89</sup> בנוסף, בפרשת "שרמס וו" נפסק שחקיקה במדינה זרה המאפשרת אחסון של מידע אישי על

<sup>83</sup> שם בסעיפים 3(2), 45-46.

<sup>84</sup> ANU BRADFORD, THE BRUSSELS EFFECT (2020).

<sup>85</sup> European Data Protection Board, Government access to data in third countries: Final Report (EDPS/2019/02-13).

<sup>86</sup> סעיף 52 ל Charter of Fundamental Rights of the European Union (להלן: "הציארטר").

<sup>87</sup> EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance Measures (Adopted on 10 November 2020), בעמ' 3. המלצות אלו גובשו לאחר שבית הדין האירופאי לזכויות אדם (להלן: "CJEU") פסל בשתי החלטות שונות את החלטותיה של הנציבות האירופאית להכיר בהסדרי נמלי ביטחון להעברת מידע ממדינות האיחוד לארצות הברית. ראו: CJEU judgment of 6 October 2015, Maximilian Schrems v. Data Protection Commissioner, Case C-362/14, EU: C: 2015: 650 (להלן: "שרמס א"); CJEU judgment of 16 July 2020, Data Protection Commissioner v (להלן: "שרמס וו"); Facebook Ireland Ltd, Maximilian Schrems, case C-311/18, ECLI: EU: C: 2020: 559 (להלן: "שרמס וו").

<sup>88</sup> Recommendations 02/2020 on the European Essential Guarantees for surveillance Measures (Adopted on 10 November 2020), בעמ' 8-10.

<sup>89</sup> סעיף 71 לפסק הדין בפרשת Privacy International, ראו CJEU, CASE c-623/17, Privacy International.







משימתה של רשות המדינה.<sup>96</sup> אולם, גם במקרה שלא ניתן לספק הודעה כאמור יש להעמיד לרשות נושא המידע סעד אפקטיבי אשר יאפשר לו לפנות לבית משפט במידה שהופעל אמצעי מעקב נגדו.<sup>97</sup>

## 2. הסדר ה-EU-U.S Data Privacy Framework והוראה נשיאותית 14086

ניסיונותיה של ארצות הברית להסדיר העברת מידע על אודות נושאי מידע אירופים לחברות בארצות הברית, באופן שיעמוד בדרישות הגנת הפרטיות האירופיות, נכשלו פעמיים עם פסילת ההסדרים שגובשו בינה לבין נציבות האיחוד האירופי על ידי ה-CJEU בפרשות **שרמס I** ו**שרמס II**.

ביולי 2023 הכריזה נציבות האיחוד האירופי על הסכם חדש, EU-U.S. Data Privacy Framework, לאסדרת העברת מידע אודות נושאי מידע מהאיחוד האירופי לארצות הברית.<sup>98</sup> ההסכם החדש מבוסס על הוראה נשיאותית שפרסם הנשיא בידן באוקטובר 2022 (להלן: "**הוראה נשיאותית 14086**"),<sup>99</sup> שביקשה לספק מענה לחששות שהעלה ה-CJEU בפרשת שרמס II ולהגביל את הגישה של שירותי הביון האמריקאים למידע אישי אודות נושאי מידע מהאיחוד בהתאם לדרישת הנחיצות והמידתיות. במסגרת זו מפרטת ההוראה הנשיאותית את הדרישות הבאות:

1. מבחינת הדרישה האירופית שעיבוד המידע יעשה למטרה ספציפית ולגיטימית על בסיס הסכמת נושא המידע או בסיס לגיטימי אחר המפורט בחוק, קובעת הוראה נשיאותית 14086 שפעולות מודיעין אותות יבוצעו רק למימוש אחת מן המטרות הלגיטימיות המפורטות בהוראה.<sup>100</sup> כן מפורטות מטרות שאין לבצע בשמן פעולות כאלה.<sup>101</sup>
2. באשר לדרישה האירופית להוראות שהפגיעה בפרטיות נחוצה ומידתית לשם השגתן של מטרות לגיטימיות, דורשת הוראה נשיאותית 14086 שלפני איסוף מידע למטרות מודיעיניות יש לבחון האם מטרת האיסוף מותרת ולגיטימית, האם היא נחוצה לשם קידום המטרה הלגיטימית, תוך התחשבות בזמינות אמצעים אחרים שפגיעתם פחותה, ויש להבטיח הטמעת אמצעי הגנה על הזכות לפרטיות ועל חירויות יסוד אחרות.<sup>102</sup> כן נדרש שתינתן עדיפות לאיסוף מידע ממוקד. איסוף כוללני (bulk collection) יעשה רק באישור וועדה או בעל תפקיד שאין דרך אחרת להגשים את המטרה הלגיטימית ותוך הטמעת אמצעים טכניים סבירים לשם הגבלת האיסוף לזה הנחוץ למטרות המנויות בהוראה

---

<sup>96</sup> סעיף 191 לפסק הדין בפרשת La Quadrature du Net and others and CJEU, Opinion 1/15.  
<sup>97</sup> Recommendations 02/2020 on the European Essential Guarantees for surveillance Measures (Adopted on 10 November 2020), בעמ' 13.

<sup>98</sup> European Commission, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*, (July 10, 2023).

<sup>99</sup> Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities"

<sup>100</sup> סעיף 2(b)(i) להוראה נשיאותית 14086.

<sup>101</sup> סעיף 2(b)(ii) להוראה נשיאותית 14086.

<sup>102</sup> סעיף 2(b)(iii) להוראה נשיאותית 14086.



בלבד.<sup>103</sup> עוד מפרטת ההוראה דרישות לגבי מיזעור המידע הנשמר, מגבלות על הפצתו בהתאם לנחיצות ומידתיות, הגבלת הגישה למידע, והוראות לעניין שמירת המידע.<sup>104</sup>

3. בנוגע לדרישה האירופית בדבר קיומו של מנגנון פיקוח עצמאי, קוראת הוראה נשיאותית 14086 ל - Privacy and Civil Liberties Oversight Board (PCLOB) לקיים ביקורת על המדיניות המעודכנת של כל גוף ביטחון על מנת לוודא שהיא כוללת את אמצעי הזהירות הנדרשים בהוראה הנשיאותית. מנהלי גופי הביטחון מחוייבים לבחון, ליישם או להתמודד עם המלצותיה של ה - PCLOB.<sup>105</sup> בנוסף, על כל גוף ביטחון להחזיק במנגנון פיקוח פנימי באמצעות העסקת משפטנים בתפקידים בכירים שיטמנו כקציני פיקוח וצוות ויבצעו באופן עיתי ביקורות על פעילות איסוף המידע. על גופי הביטחון לספק לקצינים אלו את כל המידע הדרוש להם תוך שמירה על המקורות המודיעיניים. כן עליהם להימנע מנקיטת כל פעולה שעלולה להשפיע באופן לא ראוי על קצינים אלו בביצוע תפקידם. עוד נדרש כי כל העובדים הרלוונטיים בגופי המודיעין יעברו הכשרות מתאימות להבנת ההגנות על הזכות לפרטיות הנדרשות לפי הוראה נשיאותית זו. במידה וקצין פיקוח או צוות כאמור או כל עובד אחר מוצא שהתרחשה תקרית משמעותית של חוסר ציות לחוק רלוונטי, יש לדווח על כך לראש הארגון. על ראש הארגון לוודא, עם קבלת דיווח כאמור, שננקטות על הפעולות הנחוצות על מנת לתקן את אי הציות ולמנוע את הישנותו.<sup>106</sup>

4. באשר לדרישה האירופית לסעדים אפקטיביים וזמינים לנושא המידע, הוראה נשיאותית 14086 קובעת מנגנון מדורג לבחינת תלונה, המועברת על ידי רשות ציבורית מתאימה במדינה זרה בנוגע לפעילות מודיעין אותות של ארה"ב: חקירה ראשונית של תלונה כאמור תבוצע על ידי ה - Civil Liberties, Privacy and Transparency (CLPO) אשר יוסמך לחקור, לבדוק ולפי הצורך להוראות על נקיטת פעולות לתיקון במקרה של תלונה מזכה (qualifying complaints). ה CLPO עצמאי ואסור לאחראי המודיעין להתערב בהחלטותיו או להעבירו מתפקידו אלא במקרה של התנהגות שאינה הולמת, הפרת חובת זהירות, חוסר יכולת או פגיעה בביטחון.<sup>107</sup> המתלונן או ראש הגוף הביטחוני יכולים לפנות לבחינת החלטת ה CLPO על ידי ה Review Court (DPRC) Data Protection. המדובר בבית משפט ייעודי המוקם לפי הוראה נשיאותית 14086 בהתאם להחלטת התובע הכללי, ויפעל בהרכב של 3 שופטים עצמאיים ומקצועיים. להחלטות ה - DPRC תוקף מחייב.<sup>108</sup>

### 3. הדין הבריטי

חוק סמכויות החקירה הבריטי מעניק לשירותי הביון הבריטיים שלוש סמכויות עיקריות: לקבל מאגרי מידע אישי, לבצע פעולות איסוף גורפות (bulk personal datasets) ולבצע פעולות סייבר. מימוש כל אחת מהסמכויות מותנה בהגשת בקשה מטעם ראש סוכנות הביון ואישורה בצו

<sup>103</sup> סעיף 2(c)(ii) להוראה נשיאותית 14086.

<sup>104</sup> סעיף 2(c)(iii) להוראה נשיאותית 14086.

<sup>105</sup> סעיף 2(c)(v) להוראה נשיאותית 14086.

<sup>106</sup> סעיף 2(d) להוראה נשיאותית 14086.

<sup>107</sup> סעיף 3(c) להוראה נשיאותית 14086.

<sup>108</sup> סעיף 3(d) להוראה נשיאותית 14086.





## המכון הישראלי לדמוקרטיה

גורפת וחסרת הבחנה של נתוני תקשורת<sup>120</sup> המצויים אצל ספק תקשורת או שאינם בחזקתו וביכולתו להשיגם.<sup>121</sup> צו תפיסה כללי יכול להורות לספק תקשורת להשיג נתוני תקשורת כאלה או להעבירם לידי הגוף המפורט בצו. צו תפיסה כללי גם יכול לאשר בחירה של נתוני תקשורת שהושגו מכוחו כדי לעיין בהם<sup>122</sup> וכן לאשר את העברתם לצדדים שלישיים.<sup>123</sup> החוק מחייב ספקי תקשורת ליישם את הוראות צווי התפיסה הכלליים, אם הוגשו להם כאלה, ולנקוט את כל האמצעים הסבירים לשם כך.<sup>124</sup>

מבחינת ההתאמה לדרישות האירופיות, IPA מציג את הדרישות הבאות:

1. מטרות עיבוד המידע: כלל הסמכות המוקנות בחוק סמכויות חקירה מוגבלת לתכליות הנוגעות לאינטרסים של ביטחון לאומי, מניעה או זיהוי של פשיעה או לאינטרסים כלכליים של הממלכה המאוחדת (אם אלה רלוונטיים לאינטרסים של ביטחון לאומי).<sup>125</sup> בנוסף, ביחס לצו לתפיסת נתוני תקשורת ולצו לקבלת מאגר מידע, נדרשת גם הוכחת נחיצות הצו להשגת תכלית מבצעית. התכליות המבצעיות בכל צו מוגבלות לאלו המנויות ברשימה סגורה שמנהלים ראשי סוכנויות הביון<sup>126</sup> (לכל סוג של צו כללי יש רשימת תכליות מבצעיות נפרדת). הוספת תכלית לרשימה מותנית באישור השר.<sup>127</sup> מדי שלושה חודשים על השר להגיש העתק של הרשימה לוועדת המודיעין והביטחון הפרלמנטרית, ועל ראש הממשלה לבחון את הרשימה מדי שנה.<sup>128</sup>

2. דרישת המידתיות והנחיצות: לפני מתן צו לביצוע כל אחת מהסמכויות, בין אם מדובר בסמכות להשגה או לתפיסה של מידע ובין אם מדובר על צו לשימוש במידע שהושג מכוח צו, על השר וכן על נציבות סמכויות החקירה לוודא שהצו נחוץ ומידתי ביחס למבוקש בו.<sup>129</sup> בחינת נציבות סמכויות החקירה צריכה להיעשות בהתאם לעקרונות שהיה מפעיל בית משפט בבואו לבחון את הצו, וברמת נאותות שיש בה כדי לעמוד בחובה לפי חוק סמכויות חקירה לשקול שיקולי פרטיות.<sup>130</sup>

ביחס לצו לקבלה או לשימוש במאגר מידע, במידה שהמאגר כולל רשומות רפואיות יינתן צו מידע אישי ספציפי רק בנסיבות יוצאות דופן שבהן יש צורך דחוק בהחזקת רשומות אלו או בעיון בהן.<sup>131</sup>

<sup>120</sup> כהגדרתם בס' 261(5) לחוק סמכויות חקירה.

<sup>121</sup> ס' 158(6)(a) לחוק סמכויות חקירה.

<sup>122</sup> ס' 158(6)(b) לחוק סמכויות חקירה.

<sup>123</sup> ס' 158(6)(c) לחוק סמכויות חקירה.

<sup>124</sup> ס' 170 לחוק סמכויות חקירה.

<sup>125</sup> ס' 102(5) לחוק סמכויות חקירה; ס' 204(a)205, (3)(a)(6) לחוק סמכויות חקירה;

<sup>126</sup> ס' 161 לחוק סמכויות חקירה.

<sup>127</sup> כמפורט ב-ס' 158(1)(a), (2) לחוק סמכויות חקירה.

<sup>128</sup> ס' 161 לחוק סמכויות חקירה.

<sup>129</sup> ס' 102(1)(b)-(a)(3), (b)(3)(6) לחוק סמכויות חקירה; ס' 204(b)205, (3)(b)(6) לחוק סמכויות חקירה.

<sup>130</sup> מבוח ס' 2 לחוק סמכויות חקירה, ס' 204(d)205, (3)(d)(6) לחוק סמכויות חקירה.

<sup>131</sup> ס' 206 לחוק סמכויות חקירה.





## המכון הישראלי לדמוקרטיה

על נציבות סמכויות החקירה החובה לדווח על טעות חמורה שנעשתה באשר לאדם מסוים והסבה לו נזק ניכר, בתנאי שהדיווח משרת את האינטרס הציבורי.<sup>141</sup> אף שהחוק אינו מגדיר מהי "טעות חמורה", מובהר בו כי עצם הפגיעה בזכויות המוקנות באמנה האירופית לזכויות אדם די בה כדי להוות טעות חמורה.<sup>142</sup> על הנציבות לשקול, בהחליטו אם לדווח על טעות, את חומרת הטעות, את מידת הפגיעה באינטרסים הלאומיים שחשיפת הטעות תגרום, ואת ההשפעה של הגילוי על הפעילות השוטפת של שירותי המודיעין.<sup>143</sup>

#### 4. הצהרת ה-OECD בדבר גישה ממשלתית למידע אישי

הצהרת ה-OECD בדבר גישה ממשלתית למידע אישי מגדירה "גישה ממשלתית" כ"גישה ממשלתית או עיבוד של מידע אישי המוחזק על ידי ישויות במגזר הפרטי (לרבות המגזר השלישי) לתכליות אכיפת חוק וביטחון לאומי תחת מסגרת משפטית לאומית, לרבות מקרים בהם המסגרת המשפטית המדינתית מסמיכה מדינות להורות לישויות אלו להעביר מידע אישי כאמור כשהיישות המדוברת או המידע האישי אינם בתחומיה הטריטוריאליים של אותן מדינות."<sup>144</sup> אף שהצהרה חסרה נפקות משפטית ואין בה כדי לחייב את המדינות החתומות עליה, יש בה כדי לשפוך אור על העקרונות המרכזיים של המשטר המשפטי הרצוי לשם גישה ממשלתית למידע אישי. עקרונות אלו גובשו על בסיס ערכים משותפים וקווי דמיון בין המסגרות המשפטיות הקיימות של המדינות החתומות,<sup>145</sup> ובתוכן מדינת ישראל.

העקרונות המופיעים בהצהרה הם:

1. גישה ממשלתית למידע אישי המוחזק על ידי ישויות פרטיות תיעשה לפי חוק, בהתבסס על מסגרת משפטית המחייבת את רשויות המדינה ומיושמת על-ידי מוסדותיה הדמוקרטיים הפועלים בחסות שלטון החוק.
2. גישה ממשלתית למידע אישי נועדה לתמוך במטרות ספציפיות ולגיטימיות בלבד.
3. נדרש אישור מראש לפני מימוש גישה ממשלתית למידע אישי. הכללים החלים על מתן היתרים מראש לגישה צריכים להיות בהלימה עם מידת החדירה לפרטיות והפגיעה בזכויות אדם ובחירויות הכרוכים במתן גישה ממשלתית למידע האישי. כאשר מדובר ברמת פגיעה חמורה, על הדרישות לאישור מראש צריכות להיות נוקשות ולהסתמך על אישור מאת גופים שיפוטניים או רשויות לא-שיפוטיות אובייקטיביות די הצורך.
4. מידע אישי שהושג על ידי הממשלה יעובד ויטופל רק על ידי גורמים מאושרים, ובכפוף לדרישות שבדין שנועדו להגן על הפרטיות, הבטיחות, הסודיות והשלמות של המידע. נדרשים מנגנונים המבטיחים שהמידע מעובד לפי חוק ונשמר רק למשך פרק הזמן המגודר בחוק.

<sup>141</sup> ס' 231(1) לחוק סמכויות חקירה.

<sup>142</sup> ס' 231(3) לחוק סמכויות חקירה.

<sup>143</sup> ס' 231(4) לחוק סמכויות חקירה.

<sup>144</sup> הצהרת ה-OECD בדבר גישה ממשלתית.

<sup>145</sup> הצהרת ה-OECD בדבר גישה ממשלתית, בעמ' 5-6.





שימור נתוני תקשורת,<sup>147</sup> ספק אם הדין האירופי מאפשר איסוף גורף של נתוני שימוש ברשת האינטרנט.

4. **פיקוח ובקרה:** בספרות האקדמית ובניירות עבודה של ארגונים בינלאומיים ניתן למצוא עקרונות וקווי מתאר למודל מיטבי של מערך פיקוח על ארגוני מודיעין ואכיפת חוק ועל פעילות מעקבים טכנולוגיים בפרט. מערך פיקוח אפקטיבי צריך לכלול לכל הפחות גורם אחד שהוא עצמאי ובלתי תלוי, להיות בעל סמכות לקביעת אי-חוקיותם של אמצעי מעקב ולמתן סעד; לכלול אלמנטים אדוורסריים; להיות שקוף במידת האפשר; ושיוקצו משאבים מספקים לפעילותו.<sup>148</sup>

כך, למשל, הדו"ח המיוחד של האו"ם לקידום זכויות אדם ולהגנה עליהן בעת התמודדות עם טרור, המליץ שבפיקוח מראש על פעילות מעקב דיגיטלי שבצידה פגיעה מהותית בזכויות אדם ייקח חלק, לצד האישור המיניסטריאלי, גורם עצמאי שאינו כפוף לרשות המבצעת או לסוכנויות המודיעין ואכיפת החוק.<sup>149</sup>

גם בית המשפט האירופי לזכויות אדם הדגיש את הצורך באישור מראש של איסוף גורף על ידי גורם עצמאי, על אף שלא נדרש שגורם זה יהיה בהכרח ערכאה שיפוטית.<sup>150</sup>

בבריטניה משמשת נציבות סמכויות החקירה כגוף פיקוח וביקורת גם פרטנית על ידי אישור נוסף לכל צו למימוש אחת מסמכויות המעקב וגם באופן רחבי על ידי פיקוח והגשת דוחות שנתיים, שחלקים מהם זמינים אף לציבור.

בארה"ב מוסמך ה-PCLOB, סוכנות עצמאית שהיא חלק מהרשות המבצעת, ומוסמכת ליעץ לנשיא ולראשי גופים בכירים ברשות המבצעת בנושאים הקשורים לזכות לפרטיות ולחירויות אזרח,<sup>151</sup> לבקר את המדיניות המעודכנת של כל גוף ביטחון על מנת לוודא שהיא כוללת את אמצעי הזהירות הנדרשים בהוראה הנשיאותית ומחובתם של מנהלי הביטחון, ליישם או להתמודד עם ממצאי הביקורת. בנוסף, כל גוף ביטחוני מחויב להעסיק משפטנים

---

Joined Cases C 793/19 and C 794/19 Bundesrepublik Deutschland v. SpaceNet AG (Sept. 20, 2022).

<sup>148</sup> ראו עמיר כהנא ויובל שני, רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה, פרק 6.1 (2019);

Nico Van Eijk, *Standards for Independent Oversight – The European Perspective*, in BULK COLLECTION – SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 381 (Fred H. Cate and James X. Dempsey eds., 2017); The United Nations Special Rapporteur on the Right to Privacy, *Working Draft Legal Instrument on Government-led Surveillance and Privacy* (2018), '3(1)–(2)'; EU Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU vol. II*, 86 (2017).

<sup>149</sup> *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, Martin Scheinin, para. 35 (A/HRC/14/46, part II: Compilation of Good Practices on Legal and Institutional Frameworks for Intelligence Services and Their Oversight, 2010)

<sup>150</sup> *Big Brother Watch and Others v. the United Kingdom* [GC, Applications no. 58170/13, 62322/14 and 24960/15], פסקה 351 לפסק הדין.

<sup>151</sup> U.S. Privacy and Civil Liberties Oversight Board, *History and Mission*, <https://www.pclob.gov/About/HistoryMission>









### חלק רביעי: היעדר הגנה על עיתונאים ועל מוסד החיסיון העיתונאי בתזכיר

התזכיר מגביל את סמכות השב"כ לבצע פעולה בחומר מחשב,<sup>154</sup> חיפוש סמוי בחומר מחשב<sup>155</sup> או לעשות שימוש בנתוני תקשורת, נתונים הנוגעים להפעלת מערכות תקשורת ונתוני שימוש באינטרנט,<sup>156</sup> מטעמי הגנה על "בעלי מקצוע". כך, בקשה להיתר לביצוע פעולה בחומר מחשב המשמש "בעלי מקצוע" צריכה להיעשות באישור היועמ"ש או פרקליט המדינה, ובמידה שראש השב"כ היתר לבצע פעולה כאמור ללא היתר, עליו לדווח על כך ליועמ"ש ולאחרון סמכות לבטלו.<sup>157</sup> חיפוש סמוי אצל בעלי מקצוע יכול להתבצע רק באישור בית משפט,<sup>158</sup> ושימוש בנתוני תקשורת, נתונים הנוגעים להפעלת מערכות תקשורת ונתוני שימוש באינטרנט צריך להיעשות באופן שיצמצם את הפגיעה בפרטיות תוך התייחסות גם ל"בעלי מקצוע".<sup>159</sup>

"בעלי המקצוע" אליהם מתייחס התזכיר הם אלו המוגדרים בסעיף 9א לחוק האזנת סתר והם עורך דין, רופא, פסיכולוג, עובד סוציאלי או כהן דת.<sup>160</sup> בולטים בהיעדרם עיתונאים, שאינם מקצוע המוגדר בחקיקה בישראל, והמשמעות היא שהתזכיר אינו מספק להם כל הגנה.

אכן, החיסיון העיתונאי בישראל הוא יציר הפסיקה בלבד ובפרשת ציטרין הבהיר בית המשפט העליון מתי ניתן לדרוש מעיתונאי חומרים שהשיג.<sup>161</sup> אולם, חשוב להבהיר שהחיסיון העיתונאי אינו מוגבל רק לחיובם של עיתונאים להעיד, אלא גם להסדרת הדרכים הטכנולוגיות שבהן נעשה שימוש כדי לחלץ מידע מעיתונאים, לדעת אם בכלל יש מקום לאלץ עיתונאים להעיד ופרקטיקות נוספות שמטרתן לייצר הפחדה של עיתונאים. פרקטיקות אלו יכולות לרוקן הלכה למעשה את החיסיון העיתונאי, גם אם הוא מעוגן בחוק. לכן, לאורך השנים הכיר בית המשפט בחשיבות החיסיון העיתונאי ככל שמדובר במעקבים מקוונים. בפסק הדין בעניין חוק נתוני תקשורת נקבע שיש ליצור נהל ייחודי לגבי קבלת נתוני תקשורת של עיתונאים,<sup>162</sup> ובפסק הדין בעניין איכוני השב"כ בתקופת מגפת הקורונה נקבע שיש להחריג עיתונאים מן האיכוניים.<sup>163</sup>

להבדיל מבעלי חסיונות אחרים שלגביהם אין חיסיון על עצם העובדה שאדם מסויים פנה לבעל מקצוע מסויים, אלא רק על התכתובת והשיחות ביניהם, כשמדובר בחיסיון עיתונאי – ובשל הרצון לאפשר למי שיש לו מידע חשוב לציבור למסור אותו לעיתונאי תחת חיסיון – עצם הקשר וזהותו של המקור הם עיקר המידע שנרצה לשמור על חסיונו. מידע כזה ניתן לגילוי באמצעות קבלת נתוני תקשורת (מטה דאטה) – נתונים על מיקום (פגישה), קיומן של שיחות (בטלפון, במייל או בתוכנת מסרים מיידיים (P2P), וגם היסטוריית חיפוש. זוהי הסיבה שבעטיה קבעו גם בתי

<sup>154</sup> לפי סעיף 10א המוצע בתזכיר.

<sup>155</sup> סעיף 11(ה) המוצע בתזכיר.

<sup>156</sup> סעיף 11(ג1) המוצע בתזכיר.

<sup>157</sup> סעיף 10א(א), (ג2) המוצע בתזכיר.

<sup>158</sup> סעיף 11(ה) המוצע בתזכיר.

<sup>159</sup> סעיף 11(ג1) המוצע בתזכיר.

<sup>160</sup> סעיף 9א לחוק האזנת סתר, תשל"ט – 1979.

<sup>161</sup> ב"ש 298/86 ציטרין נ' בית הדין המשמעתי של לשכת עורכי הדין במחוז תל אביב, פ"ד מא(2) 337

(1987), וכן ראו גם שירן ירוסלבסקי קרני ותהילה שוורץ אלטשולר, הסדרת החיסיון העיתונאי, מחקר מדיניות 104 המכון הישראלי לדמוקרטיה (2015).

<sup>162</sup> בג"צ 3809/08 האגודה לזכויות האזרח נ' משטרת ישראל (פורסם בבנו, 2012) (להלן: "עניין חוק האח הגדול").

<sup>163</sup> בג"צ 2109/20 בן מאיר ואח' נגד ראש הממשלה ואח', (פורסם בבנו, 26.04.2020).



המשפט כי יש להתייחס למתן צו לקבלת נתוני תקשורת של עיתונאים בחומרה ובמעמד קבלת ההחלטה על מתן הצו יש לשקול שיקולים הנוגעים לחופש העיתונות.

היעדר התייחסות לעיתונאים בתזכיר חוק בשנת 2023 משקפת התעלמות מן הפסיקה שניתנה עד היום בעניין זה וכן את המחדל של הכנסת שלא הטריחה את עצמה עד היום לעגן את החיסיון העיתונאי בחוק. אכן, עיתונות אינה טעונה רישוי, ובעולם שבו אנו חיים ניתן להיות "עיתונאי" מבלי לעבוד בבלי תקשורת ממוסד. אבל לצורך תחולת חקיקה, כמו גם לצורך קבלת תעודות לע"מ, ניתן למצוא הגדרות מספקות ולעגן אותן בחקיקה כפי שהצענו כבר בשנת 2015.<sup>164</sup>

יתרה מזאת, יש להניח כי כפי שהתרחש בעניין חוק נתוני תקשורת, הטענה תהיה כי יוכן נוהל מיוחד לעניין עיתונאים, אך הוא לא יעוגן בחוק. "נוהל" משקף למעשה את האופן בו מפרשת הרשות את החוק ביחס לעניינם של עיתונאים, אבל הוא לא יוצר זכויות או הגנות והדבר יוצר הגנה פחותה, שאינה מאפשרת לעיתונאים לפנות לקבל סעד מבתי משפט.

הפגיעה בעיתונאים חמורה עוד יותר כאשר מדובר בסמכויות הניתנות לשב"כ, שכן המדובר בגוף הפועל בהיעדר שקיפות ומוסמך לבצע תפקידים רגישים, כמו, למשל, הגנה על הדמוקרטיה. כפיפות שב"כ לראש הממשלה שהוא דמות פוליטית שיכולה להימצא בניגוד עניינים כשמדובר בעיתונאים, מחמירה את החשש.

בנוסף, הצורך בהגנה על עיתונאים מתעורר בעיקר נוכח הדיווחים בשנים האחרונות לפיהם היו עיתונאים יעד מרכזי לביצוע חיפוש סמויים, באמצעות שימוש ברוגלות מעקב, במדינות שונות בעולם.<sup>165</sup> בארצות הברית אף תלויים ועומדים הליכים נגד חברות אשר פיתחו נזקות מעקב ואיפשו מעקבים כאמור.<sup>166</sup> בארץ, הודתה המדינה כי נעשה שימוש במאגר נתוני התקשורת של חברות התקשורת שבידי השב"כ לשם מעקב אחר פעילות עיתונאים, ללא צו בית משפט.<sup>167</sup>

בגרמניה התעוררה שאלה דומה בנוגע לחוק שירותי הביון הפדרלי (Federal Intelligence Service Act) המסמיך את שירותי הביון הפדרליים במדינה לבצע מעקבים, לרבות איסוף נתוני תקשורת. במאי 2020, בעקבות תלונה של ארגון עיתונאים ללא גבולות (Service Act Reporters Without Borders) והאגודה לזכויות האזרח במדינה (Society for Civil Rights), קבע בית המשפט הפדרלי לחוקה (German Federal Constitutional Court) שעל שירותי הביון לכבד זכויות יסוד כגון חופש הביטוי וחיסיון עיתונאי וחייב את הממשלה לתקן את חוק שירותי הביון בהתאם. לאחר תיקון החוק הוא אוסר על ניטור של תקשורת בין עיתונאים ובין מקורות, מן הצד העיתונאי.

---

<sup>164</sup> שירן ירוסלבסקי קרני ותהילה שוורץ אלטשולר, הסדרת החיסיון העיתונאי, מחקר מדיניות 104 המכון הישראלי לדמוקרטיה (2015).

<sup>165</sup> ראו, למשל, Phineas Rueckert, *Pegasus: The New Global Weapon for Silencing Journalists*, FORBIDDEN STORIES (July 18, 2021); Ronen Farrow, *How Democracies Spy On Their Citizens*, THE NEW YORKER (April 18, 2022).

<sup>166</sup> Whatsapp Inc., and Facebook Inc., v. NSO Group Technologies Limited and QCyber Technologies Limited, United States District Court Northern District of California, Complaint Apple Inc., v. NSO Group Technologies Limited ;Demand for Jury Trial (Filed Oct. 29, 2019) and Q Cyber Technologies Limited, N.D. Cal., No. 5:21-cv-9078, complaint filed Nov. 23, 2021. Dada v. NSO Group, No. 3:22-cv-07513 (N.D.Cal.) ;2021

<sup>167</sup> חן מענית, שב"כ חשף כי עקב אחר פעילות עיתונאים באמצעות מאגר נתוני תקשורת סלולרית, הארץ (11.11.2022).









## המכון הישראלי לדמוקרטיה

מיוחדת בלבד, אלא אם כן "לא ניתן היה לבצע הפרדה בין שני סוגי המידע". אולם, לא ברור מי יבצע הפרדה כאמור, ובאיזה שלב – טרם האיסוף או הקבלה, במהלכן או לאחריה.

הוראת סעיף 8א(ה)(1) המוצע בתזכיר מעוררת את השאלה האם כאשר השימוש במאגר המידע נעשה לשם אחת מהמטרות לשמן נתקבל או נאסף, די בכך שרה"מ שוקל את מידתיות הפגיעה בפרטיות בעת מתן ההיתר, ואין צורך לנסות ולמזער את הפגיעה בפרטיות בעת השימוש עצמו. זאת, לאור ניסוח הסעיף הקובע שכאשר נעשה שימוש שלא למטרות שלשמן נתקבל או נאסף מאגר המידע, ייקבעו כללים בדבר אופן מיזעור הפגיעה בפרטיות.

### ג. הסמכות להעביר מאגר מידע

סעיף 8ב המוצע מסמיך את ראש השב"כ להעביר מאגר מידע מ"טעמים מיוחדים", שטיבם אינו מפורט, ל"גורם" שייקבע בכללים ושגם זהותו אינה בהירה. ניסוח זה הוא מעורפל ומנוגד לצורך לקבוע בחקיקה לפחות מסגרת סמכות כללית ברורה.

### ד. הסמכות לבצע חיפוש גלוי או סמוי

לפי התיקון המוצע בתזכיר לסעיף 10(1) לחוק השב"כ במידה שאגב החדירה לדבר המגלם חומר מחשב "התקבל מידע מתקשורת בין מחשבים" לא תחשב קבלת המידע האמור להאזנת סתר. עם זאת אין התזכיר קובע מה יעשה עם מידע כאמור. לא ברור לפיכך האם חלה חובה למחוק אותו והאם יכול השב"כ לעשות בו שימוש למטרות אחרות.

### ה. הסמכות לבצע איסוף גורף של נתוני תקשורת, נתונים הנוגעים להפעלת מערכות תקשורת ונתוני שימוש באינטרנט

סעיף 11(ג) המוצע בתזכיר מפרט מסגרת לכללים שיקבעו ויפרטו את אופני השימוש במידע שיקבל השב"כ במסגרת סעיף 11 לחוק השב"כ באופן אשר יצמצם את הפגיעה בפרטיות. בין השאר מונה הסעיף "נסיבות שיאפשרו עיבוד המידע באופן שאינו ממוכן". בעידן של היום עיבוד מידע, בכמויות ובהיקפים עליהם מדובר במסגרת המידע המועבר לשב"כ תחת סעיף 11 לחוק השב"כ, אינו אפשרי. משום כך, הצעת האפשרות לעיבוד שאינו ממוכן כשלעצמה, ויתרה מכך כאפיק לצמצום הפגיעה בפרטיות, אינה ברורה ויש לתקנה.

### ו. הסמכות השירות

סעיף 11א המוצע בתזכיר מבקש לאפשר לוועדת השרים לענייני השירות, באישור ועדת הכנסת לענייני השירות להקנות לשב"כ סמכויות נוספת "לעניין מידע או סוגי מידע" לשם מניעת עבירות בתחומים של "סיכול ומניעה של פעילות בלתי חוקית שמטרתה לפגוע בביטחון המדינה, בסדרי המשטר הדמוקרטי או במסודותיו",<sup>175</sup> "אבטחת אנשים, מידע ומקומות, שקבעה הממשלה",<sup>176</sup> או "פעילות בתחום אחר שקבעה הממשלה, באישור ועדת הכנסת לענייני השירות, שנועדה לשמור ולקדם אינטרסים ממלכתיים חיוניים לביטחון הלאומי של המדינה",<sup>177</sup> ובלבד שאין מענה מתאים בהוראות סעיפים 8-11 לחוק השב"כ. אף אם כוונת הסעיף היא לאפשר התמודדות עם טכנולוגיות חדשות שיופיעו בעתיד ולא ניתן לצפותן כעת, הרי שהעובדה שהגוף המוסמך להעניק

<sup>175</sup> סעיף 7(ב)(1) לחוק השב"כ.

<sup>176</sup> סעיף 7(ב)(2) לחוק השב"כ.

<sup>177</sup> סעיף 7(ב)(6) לחוק השב"כ.





## המכון הישראלי לדמוקרטיה

לשב"כ סמכות חדשות כאמור פועל שלא בשקיפות וללא דיון ציבורי, בדומה המתנהל עתה ביחס לתזכיר, אינה תקינה. לפיכך ראוי לקבוע בחוק כבר עתה מנגנון שקוף להקניית סמכויות נוספות.

אם כוונת הסעיף היא לייצר ערוץ הסמכה לשירות שבאמצעותו יוסמך השירות לעשות שימוש בשיטות ואמצעים שחשיפתם הפומבית עשויה לסכל את תכליתן המבצעית, הרי שהפניה לערוץ זה נדרשת להיות מרוסנת. משכך, יש להגבילה הסמכה חשאית למקרי חירום חריגים בלבד, לפרקי זמן מוגבלים בימים, ומתוך כוונה לעגן סמוך לכך בחקיקה ראשית באמצעות מהלך פרלמנטרי שקוף,<sup>178</sup> והכל בכפוף לפיקוח חיצוני ולדיווח פומבי על עצם הפניה לערוץ זה.

בנוסף, ראוי שסמכות שירותית כאמור תוענק למטרות בחרות, מצומצמות ומדויקות יותר ובכפוף לדרישת מידתיות, ולא רק לדרישת נחיצות.

### ז. הוראות לעניין שמירה ומחיקה של מידע

סעיף 11ב המוצע בתזכיר קובע כי הוראות לעניין שמירה ומחיקה של מידע, לרבות מאגר מידע, שהתקבל בשב"כ לפי החוק והתזכיר, יקבעו ע"י רה"מ בכללים שהינם חסויים. ההוראות השקופות היחידות לציבור הן קביעה כי תקופת השמירה של מידע או מאגר מידע לא תעלה על חמש שנים, אלא אם ראש השב"כ יקבע תקופה ארוכה יותר וכן שעם ביטול היתר לביצוע איסוף או קבלה של מאגר מידע, לחיפוש סמוי או לביצוע פעולה בחומר מחשב של בעלי מקצוע יימחק המידע שהתקבל או נאסף מכוחו.

מאחר ומדובר בכללים טכניים לשמירה ומחיקה של מידע שיש חשיבות ציבורית בידיעתם, בעיקר על מנת לספק לציבור מושג כללי בנוגע להיקף ומשך הפגיעה בפרטיות, ראוי שכללים אלו יקבעו בחוק ולא בכללים חסויים.

---

<sup>178</sup> ר' למשל את עניין בגץ 8196/21 האגודה לזכויות האזרח בישראל נ' הממשלה (2.12.2021) במקרה זה, ניתן פומבי להסמכה של השב"כ לאבן נשאי וריאנט אומיקרון וכאשר הדיון נסוב על פרק הזמן הנדרש עד לעיגון סמכויות אלו בחקיקה ראשית, דובר על "פרק זמן קצר הנמדד בימים."





