המכון הישראלי
לדמוקרטיה

www.idi.org.il

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

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

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

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

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

מייסד ונשיא לשעבר
ד"ר אריק כרמון

28 אוגוסט, 2019

הצעת חוק הגנת הפרטיות, התשע"ט-2019
השלמות בנושא עיבוד מידע אישי על ידי גופי ביטחון והתנאים להכרת הנציבות האירופית בתאימות הדין המקומי (adequacy)
סקירת משפט משווה

עו"ד רחל ארידור הרשקוביץ

1. מבוא

האיחוד האירופי אינו עוסק בנושאים הקשורים בביטחון המדינות החברות באיחוד. משום כך, פגיעה בזכות לפרטיות כתוצאה מעיבוד מידע אישי על ידי גופי ביטחון אינה מוסדרת בתקנות להגנת מידע באיחוד האירופי (General Data Protection Regulation) (להלן: "GDPR").

עם זאת, במסגרת בחינת מידת התאימות (adequacy) של הדין המקומי במדינה זרה ל-GDPR, נבחנת גם מידת הפגיעה בזכות לפרטיות עקב עיבוד מידע אישי על ידי גופי ביטחון. זאת בעקבות פסק הדין של בית הדין של האיחוד האירופי (ה-Court of Justice of the European Union) בפרשת Schrems, שם נפסק כי הדין המקומי חייב להיות "שווה ערך במהותו" (בלשון פסק הדין - "essentiallyequivalent") ל-GDPR. בפסק הדין הובהר שאין צורך שהמדינה הזרה תאמץ את אותם אמצעי הגנה כמו אלו הנהוגים באיחוד האירופי אולם עליה לספק רמת הגנה זהה במידה מספקת.[1] אמת מידה זו אומצה בחוות הדעת שניתנה על ידי WP29 בעניין לאחר פסק הדין,[2] ובס' 104 להקדמה ל-GDPR.[3]

---

[1] Case C-362/14 , Decision 2000/520/EC מיום 6.10.15 (להלן "**פרשת Schrems**").

[2] Article 29 Data Protection Working Party, Adequate Referential (adopted on 28 Nov. 2017, as last revised and adopted on 6 Feb. 2018).

[3] ראו:

"Recital 104: Criteria for an adequacy decision
In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including

הסיכום שלהלן סוקר בקצרה מהם התנאים לפגיעה בזכות לפרטיות עקב עיבוד מידע אישי על ידי גופי ביטחון באיחוד האירופי וכיצד אילו מיושמים במדינות החברות באיחוד האירופי ובמדינות שנציבות האיחוד האירופי הכירה בתאימות הדין המקומי בהן ל-GDPR. מטרתו לספק את הרקע וההצדקות לתיקון הפטור הגורף שניתן כיום לגופי ביטחון לפי סעיף 19(ב) לחוק הגנת הפרטיות, התשמ"א-1981 לשם התאמתו לדרישות הנהוגות באיחוד האירופי. זאת על מנת להגדיל את הסיכוי שנציבות האיחוד האירופי תשוב ותכיר בתאימות הדין בישרא'ל לזה הנהוג באיחוד האירופי.

2. המסגרת המשפטית באיחוד האירופי

2.1. פרשת Schrems

Maximillian Schrems, אזרח אוסטריה ומשתמש פייסבוק, טען שהעברת המידע האישי עליו לשרתי פייסבוק בארה"ב אינה חוקית שכן לפי הגילויים בפרשת סנואודן גופי הביטחון בארה"ב מבצעים מעקב חודרני ובהיקפים גדולים ולכן רמת הגנת הפרטיות בארה"ב אינה מספקת.

בית הדין קיבל את התביעה וביטל את הסכם נמל המבטחים (safe harbour) בין האיחוד האירופי לבין ארה"ב. נפסק שהחלטת הנציבות האירופית המכירה בתאימות הדין המקומי במדינה זרה לדין באירופה צריכה להתבסס על בחינת הדין המקומי ובדיקה האם הוא שווה ערך במהותו (essentially equivalent) לזה שבאיחוד האירופי. אין צורך שהמדינה הזרה תאמץ את אותם אמצעי הגנה כמו אלו הנהוגים באיחוד האירופי אולם עליה לספק רמת הגנה שוות ערך באופן מהותי.

בכל מקרה, החלטה המכירה בתאימות הדין המקומי לזה האירופי אינה תקפה לעד. על הנציבות לחזור ולבדוק את מידת התאימות באופן עיתי, בהתאם לשינויי הדין במדינות זרות או כאשר עולה

---

legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."

החשד (כתוצאה מתלונה של אזרח אירופי) שהדין המקומי אינו תואם עוד את רמת ההגנה הקבועה באיחוד האירופי.

באשר להתרת עיבוד מידע אישי על ידי גופי ביטחון נפסק שלפי הדין הקובע באיחוד האירופי עיבוד מידע אישי באופן הפוגע בזכויות בסיסיות, בעיקר הזכות לפרטיות, חייב להיעשות לפי כללים ברורים ומדויקים. כללים אלה יבטיחו כי עיבוד המידע יעשה לפי מבחן הנחיצות להגשמת המטרה וכן שתינתן הגנה מספקת מפני גישה או שימוש לא חוקי במידע האישי. דרישה זו מתחדדת כאשר מדובר בעיבוד אוטומטי של מידע אישי שלגביו הסיכון לגישה או שימוש לא מורשה גדל.

עוד נפסק שבזמן אישור הסכם נמל המבטחים הנציבות לא בחנה האם החוק המקומי בארה"ב או הסכמים או אמנות בינ"ל שארה"ב חתומה עליהן מחילים רמת הגנה מספקת. הסכם נמל המבטחים חל מראש רק על חברות מסחריות בעוד החקיקה בארה"ב מתירה לרשויות ציבוריות לעבד מידע אישי שהועבר מהאיחוד האירופי שלא למטרה לשמה נמסר ומעבר למידה הדרושה משיקולי ביטחון, אינטרס הציבור או אכיפת חוק ואינה מציגה מנגנון המאפשר לנושא מידע לקבל סעד משפטי על מנת לעיין במידע אישי עליו, לתקן אותו או למחוק אותו.

משום כך, הכרת נציבות האיחוד האירופי בתאימות הדין המקומי בארה"ב לדין האירופי במסגרת הסכם נמל המבטחים אפשרה בפועל פגיעה בזכות לפרטיות.

2.2. האמנה הבינלאומית בנושא ההגנה מפני עיבוד אוטומטי של מידע אישי

ביטחון המדינה הוא נושא המצוי מחוץ לתחום השיפוט של האיחוד האירופי. אולם, באפריל 2019 קיבלה מועצת האיחוד האירופי החלטה המתירה לכל המדינות החברות באיחוד האירופי לאשרר את התיקון ל אמנה הבינלאומית בנושא ההגנה מפני עיבוד אוטומטי של מידע אישי ("אמנה 108").[4] לפי ההחלטה, אישרור כאמור הוא אינטרס של האיחוד האירופי כולו.[5] ישראל אינה צד לאמנה.[6]

לפי אמנה 108 פגיעה בפרטיות עקב עיבוד מידע אישי על ידי רשויות ציבור מטעמים שונים תותר בתנאים הבאים:

---

[4] an amended Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (the "modernised Convention 108"; the Council of Europe adopted an amending Protocol on the 18 May 2018) (להלן: "אמנה 108").

[5] Council of Europe, Newsroom: EU Member States to Ratify Convention 108+ (April 9, 2019).

[6] לרשימת המדינות החתומות על האמנה: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa.

1. הפגיעה בפרטיות תותר בחוק אשר יתיר עיבוד מידע אישי לפי מבחני נחיצות ומידתיות, ובלבד שהעיבוד הוא לאחת מהמטרות הבאות:

(א) הגנה על ביטחון המדינה;

(ב) הגנה על ביטחון הציבור;

(ג) הגנה על אינטרסים כלכליים ופיננסיים חשובים;

(ד) הגנה על עצמאות הרשות השופטת ופעילותה ללא משוא פנים;

(ה) מניעה, חקירה והעמדה לדין בגין עבירות פליליות, ואכיפה של עונשים פליליים;

(ו) הגשמת מטרות אחרות שיש בהן אינטרס ציבורי.

2. הפגיעה בפרטיות מוגבלת לאי קיום הוראות סעיפי האמנה בנוגע לנושאים הבאים:[7]

(א) החובה לעבד מידע אישי באופן הגון ושקוף ולאסוף מידע אישי רק למטרה ספציפית לגיטימית ומפורשת.[8]

(ב) החובה לדווח על אירועי אבטחה.[9]

(ג) חובת ההודעה.[10]

(ד) זכות נושא המידע: הזכות שלא להיות נתון להחלטה המבוססת כולה או רובה על עיבוד אוטומטי, זכות העיון, הזכות לקבל הסבר, הזכות להתנגד לעיבוד מידע אישי על בסיס אינטרס לגיטימי של בעל שליטה במידע, זכות התיקון, זכות המחיקה, הזכות לקבל סעד בגין פגיעה בזכות לפרטיות, והזכות לקבל סיוע של נציבות הפרטיות המקומית במימוש זכויותיו.[11]

3. כאשר מטרת עיבוד המידע היא הגנה על ביטחון המדינה והציבור, מתירה האמנה גם אי קיום חובות נוספות:[12]

(א) החובה לאפשר לוועדה מטעם אמנה 108 לבדוק את האפקטיביות של האמצעים שנקבעו בחוק המקומי המיישם את האמנה.[13]

(ב) החובה לעדכן נציבות הפרטיות המקומית בנוגע להעברת מידע מחוץ לגבולות המדינה., להוכחת.[14]

---

[7] סעיף 11(1) לאמנה 108.
[8] סעיף 5(4) לאמנה 108.
[9] סעיף 7(2) לאמנה 108.
[10] סעיף 8(1) לאמנה 108.
[11] סעיף 9 לאמנה 108.
[12] סעיף 11(3) לאמנה 108.
[13] סעיף 4(3) לאמנה 108.
[14] סעיף 14(5),(6) לאמנה 108.

(ג) סמכות נציבות הפרטיות המקומית:[15]

1) לדרוש הוכחת האפקטיביות של אמצעי האבטחה.

2) לדרוש קיומו של אינטרס לגיטימי שגובר על זכויות נושא המידע.

3) לאסור, לעכב או להתנות העברת מידע מחוץ לגבולות המדינה.

4) לחקור ולפקח על העברת מידע מחוץ לגבולות המדינה

5) לקבל החלטות בנוגע להפרת סעיפי האמנה ולהטיל סנקציות מינהליות.

6) ליזום הליכים משפטיים.

4. בכל מקרה עיבוד מידע אישי למטרות הגנה וביטחון המדינה חייב להיות נתון לביקורת ולפיקוח עצמאי ויעיל במסגרת החוק המקומי של המדינה החתומה על האמנה.

GDPR .2.3

סעיף 104 להקדמה ל-GDPR מבהיר שהמבחן לקביעת תאימות הדין המקומי ל-GDPR הוא האם הדין המקומי שווה ערך במהותו ל-GDPR.[16]

סעיף 45(2)(a) ל-GDPR קובע שבבחינת תאימות הדין המקומי יש להביא בחשבון גם את הנושאים הבאים: חקיקה ודין נוהג בכל הקשור להגנה, ביטחון הציבור, ביטחון המדינה, אכיפה פלילית וגישה של רשויות ציבור למידע אישי; יישום החקיקה והדין הנוהג בפועל; כללי אבטחת מידע; כללי אתיקה וכללים מקצועיים, וכללים בנוגע להעברת מידע אישי למדינה שלישית או לארגונים בינלאומיים, זכויות נושא מידע ואכיפתן, קיומו של סעד לנושא מידע שמידע אישי עליו הועבר.[17]

---

[15] **סעיפים 14(5),(6) ו-15(2) לאמנה 108.**

[16] **ראו הערת שוליים 3 לעיל.**

[17] **סעיף 45(2)(a) ל-GDPR:**

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

2.4. חוות הדעת של WP29 בנוגע לתנאים להכרה בתאימות הדין המקומי ל-GDPR והחריג לגופי ביטחון[18]

לפי חוות הדעת התנאים להכרה בתאימות דין מקומי המאפשר עיבוד מידע לצרכי ביטחון המדינה הם:

1) עיבוד המידע האישי צריך להיעשות על בסיס משפטי ברור - כללים ברורים, מדוייקים וזמינים.
2) יש להוכיח נחיצות ומידתיות עיבוד המידע האישי לצורך הגשמת המטרות האובייקטיביות של עיבוד המידע האישי.
3) עיבוד המידע האישי נתון לפיקוח חיצוני.
4) קיים מנגנון המספק סעדים אפקטיביים זמינים לנושא מידע הנפגע כתוצאה מעיבוד המידע האישי.

2.5. סיכום הדין האירופי בנוגע להתרת עיבוד מידע אישי על ידי גופי ביטחון והכרה בתאימות הדין המקומי

בחינת החלטת תאימות נציבות האיחוד האירופי תתייחס למכלול החוקים הרלוונטיים, כללים מקצועיים, פסקי דין, אמצעי אבטחה, קיומה של רשות אחראית מתפקדת אחת לפחות, ומחויבויות בינ"ל.

הדין המקומי המאשר עיבוד מידע אישי על ידי גופי ביטחון חייב להיות לכלול כללים ברורים לגבי העברת מידע אישי למחוץ לגבולות המדינה, עיבוד מידע אישי למטרות ביטחון לאומי, אכיפה פלילית וגישה של רשויות ציבור למידע אישי, לרבות קיומה של ביקורת חיצונית ופנימית על פעולות רשויות ציבור תוך פגיעה בפרטיות ואפשרותו של נושא מידע החש שזכותו לפרטיות נפגעה לקבל סעד אפקטיבי.

3. סקירת משפט משווה

3.1. ארצות הברית

אחרי פסק הדין בפרשת Schrems אשר ביטל את החלטת נציבות האיחוד האירופי המכירה בתאימות הדין בארה"ב על בסיס הסכם נמל המבטחים,[19] החלו ארה"ב ונציבות האיחוד האירופי

---

[18] Article 29 Data Protection Working Party, Adequate Referential (adopted on 28 Nov. 2017, as last revised and adopted on 6 Feb. 2018).

[19] ראו דיון בסעיף 2.1 לעיל.

במשא ומתן לגיבוש מסגרת חדשה אשר תאפשר העברת מידע אישי על נושאי מידע מאירופה לארצות הברית.

ביולי 2016 קיבלה נציבות האיחוד האירופי החלטה המכירה בתאימות הדין המקומי בארה"ב ל-GDPR במסגרת ה- Privacy Shield Framework, מסמך שהוכן על ידי מחלקת המסחר האמריקאית,[20] ועל בסיס הצהרות גורמי ממשל אמריקאים.[21]

רק ארגונים שיבחרו וולונטרית לציית לדרישות הגנת הפרטיות המפורטות ב- Privacy Shield Framework יוכלו לקבל מידע אישי על נושאי מידע מאירופה. אף שהבחירה לציית לעקרונות ה Privacy Shield Framework היא וולונטרית, מרגע שארגון אישר באתר האינטרנט של מחלקת המסחר האמריקנית שהוא מציית למכלול דרישות ה Privacy Shield Framework ומיידע בזאת גם את כלל הציבור, ציות לעקרונות ה- Privacy Shield Framework הופך לחובה שיש בגין הפרתה סנקציות עונשיות הקבועות בחוק.[22]

לפי ה- Privacy Shield Framework פגיעה בזכות לפרטיות באמצעות עיבוד מידע אישי תותר בהתקיים התנאים הבאים:[23]

(1) הפגיעה בפרטיות היא למטרות של הגנה על ביטחון המדינה, אינטרס הציבור או אכיפת חוק, ובלבד שעיבוד המידע האישי למטרות אלו נעשה בהתאם למבחן נחיצות;

(2) הפוגע בזכות לפרטיות באמצעות עיבוד מידע אישי מוסמך לעשות זאת לפי חוק, תקנות ממשלה או פסיקה, ובלבד שבמימוש הסמכות האמורה הוא פועל בהתאם למבחן הנחיצות; או

(3) הפגיעה בפרטיות עקב עיבוד מידע אישי מותרת ומיושמת בהקשרים דומים ב-GDPR או בחוק במדינה החברה באיחוד האירופי.

בנוסף, חברה מסחרית שהתחייבה לפעול לפיה ה Privacy Shield Framework רשאית, אך אינה חייבת, לפרסם באופן עיתי דו"ח שקיפות המפרט את מספר הבקשות לקבלת גישה למידע אישי

---

[20] EU - U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce.

[21] Decision: Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (1/8/2016).

[22] למידע נוסף ראו: https://www.privacyshield.gov/Program-Overview.

[23] סעיף 1(5) בדברי ההקדמה ל-Supplementary Rules ב Privacy Shield Framework.

המכון הישראלי לדמוקרטיה

המאוחסן אצלה, שקיבלה החברה המסחרית מרשויות ציבוריות למטרות של אכיפת חוק או ביטחון המדינה, והמידה שגילוי כאמור לרשויות הציבוריות מותר לפי החוק.[24]

נציבות האיחוד האירופי הכריעה שהמסגרת המשפטית בארה"ב כוללת הגבלות מספקות על הגישה של רשויות ציבוריות למידע אישי המועבר מאירופה לארה"ב ועל השימוש שלהן במידע אישי כאמור למטרות של ביטחון המדינה. בנוסף נמצא שקיים מנגנון לקבלת סעדים אפקטיביים בגין פגיעה בזכות לפרטיות, וכן מיושמים אמצעי הגנה מספקים נגד פגיעה לא מורשית וסכנה לשימוש לרעה.

מסקנתה של הנציבות נשענה על הנימוקים הבאים:

(1) Presidential Policy Directive 28 מיום 17.1.14 מטילה מספר מגבלות על מבצעי מודיעין:[25]

(א) המבצע חייב להיעשות על בסיס חוק או הרשאה נשיאותית.

(ב) בכל מקרה, החלטה על התחלת מבצע צריכה להתקבל בהתאם למדיניות ולתהליכים שכל סוכנויות המודיעין האמריקניות נדרשות ליישם בהתאם ל Presidential Policy Directive 28, ואין היא יכולה להתקבל בהחלטה של סוכן יחיד. מדיניות היישום המנחה בנושא (National Intelligence Priorities Framework) מבטיחה שהעדיפויות המודיעיניות יקבעו על ידי דרגים גבוהים של קובעי מדיניות ויבחנו באופן שיגרתי על מנת להבטיח שנותרות רלוונטיות למטרה ספציפית לביטחון המדינה תוך בחינת כל הסיכונים לרבות הסיכון לפרטיות.

(ג) המבצע חייב להתבצע בהתאם לחוקה, בייחוד התיקון הרביעי לחוקה, והחוק התקף בארה"ב באותה העת. הנחת המוצא היא שכל בני האדם חייבים לקבל יחס הגון ומכבד ללא קשר ללאום שלהם ולמקום המגורים שלהם, ושלכולם זכות לגיטימית לפרטיות בטיפול במידע אישי עליהם.

(ד) איסוף מידע אישי יעשה רק למטרה מודיעינית לתמיכה במשימה לאומית ולא לשום מטרה אחרת (למשל לאפשר יתרון תחרותי לחברות אמריקאיות).

(ה) איסוף המידע יעשה לפי מבחן (as tailored as feasible) הדומה מבחינת משמעותו למבחני הנחיצות והמידתיות: נדרש שלא יבוצע איסוף גורף של מידע, ולא שהמידע ייאסף בהתאם לקביעת סדר עדיפויות תוך בחינת זמינותן של חלופות אחרות.

(ו) רק במקרים חריגים, לשם הגשמת אחת משש מטרות הביטחון הלאומי המנויות בהחלטה הנשיאותית (אמצעים לזיהוי ולהתגוננות מפני איומי נגד הנובעים מריגול, טרור, נשק להשמדה המונית, איומי סייבר, איומי על אנשי צבא, איומי פשיעה בינ"ל הקשורים לחמש המטרות האחרות. ששת המטרות יבחנו מידי שנה) וכשאין בנמצא

---

[24] סעיף 16 ל- Supplementary Rules ב Privacy Shield Framework.

[25] Presidential Policy Directive - Signals Intelligence Activities (PPD-28), (Jan. 17, 2014).

חלופה מתאימה לאיסוף מידע ממוקד משיקולים טכניים או מבצעיים, יורשה איסוף מידע באופן גורף. אבל, לפי הצהרות דירקטור המודיעין הבינלאומי (Director of National Intelligence) גם במקרה של איסוף גורף, יחולו המגבלות הבאות:

1. יאסף רק מידע שקשור למטרות מודיעין זרות מסוימות (למשל קבלת סיגנלים מודיעיינים על פעילות קבוצת טרור במחוז מסוים) והאיסוף יתמקד על תקשורת שיש בה סגינלים כאלו.
2. יוטמעו מסננים ואמצעים טכניים אחרים שימקדו את האיסוף ככל האפשר על מנת להבטיח מיזעור של המידע הלא רלוונטי שיאסף.

(ז) הגישה למידע אישי לאחר איסופו מוגבלת לאנשים מורשים על בסיס צורך לדעת את המידע (need to know) לשם ביצוע המשימה המוטלת עליהם. בנוסף, ככלל נדרש שהמידע האישי יעובד ויאוחסן בתנאים המבטיחים הגנה מתאימה וימנעו גישה לא מורשית, ברמה המתאימה להגנה על מידע רגיש.

(ח) שמירת המידע האישי מוגבלת ל-5 שנים מקסימום. תתאפשר שמירת מידע לתקופה העולה על 5 שנים לפי חוק או לפי החלטה של דירקטור המודיעין הבינלאומי, שהמשך השמירה היא עניין של ביטחון המדינה . החלטה זו תתקבל לאחר הערכה זהירה של החששות לזכות לפרטיות תוך התחשבות גם בדעתו של דירקטור השמירה על זכויות אדם כמו גם בעלי תפקידים רשמיים בתחום הגנת הפרטיות וזכויות אזרח.

(ט) הפצה של המידע האישי מוגבלת למקרים בהם המידע רלוונטי למטרה שבבסיס איסוף המידע ולכן כפופה לדרישה מוסמכת של קצין מודיעין זר או אכיפת חוק.

(2) חיפוש מידע אישי על ידי רשויות ביטחון מכוח ה - Foreign Intelligence Surveillance Act (FISA),[26] או לפי ה - National Security Letter (NSL) אם החיפוש מבוצע על ידי ה-FBI, מוגבל לשימוש במונחים מאבחנים מסוימים (כתובת דוא"ל למשל) על מנת למקד את החיפוש. לא נעשה חיפוש לפי מילות מפתח או שמות של אנשים מסוימים.

(3) קיומם של גופי ביקורת חיצונית ופנימית:

(א) פקידי פרטיות וזכויות אדם בגופים הביטחוניים. פקידי הפרטיות מוסמכים לפקח על פעולות בגוף הביטחוני על מנת להבטיח שאלו שוקלים באופן ראוי שיקולי פרטיות וזכויות אדם ומטמיעים הליכים מתאימים לטיפול בתלונות נושאי מידע הטוענים לפגיעה בזכותם לפרטיות. במקרים מסוימים מוסמכים פקידי הפרטיות לנהל באופן עצמאי חקירות בנוגע לפגיעה בפרטיות. על פקידי הפרטיות לדווח באופן תקופתי לקונגרס. הדיווח יכלול פירוט של מספר התלונות המתקבלות על ידם, אופי

[26] סעיפים 104, 402, 501 ו702 ל FISA.

התלונות, סיכום הטיפול בתלונה, ומידע על פעולות ביקורת וחקירה שבוצעו על ידו. על ראש הגוף הביטחוני להבטיח שפקיד הפרטיות מקבל את כל המידע הנחוץ על מנת למלא את תפקידו.[27] אף שהביקורת המבוצעת על ידי פקידי הפרטיות נחשבת מקיפה, לדעת נציבות האיחוד האירופי הם אינם עצמאיים באופן מספק ולכן אין מדובר בגוף ביקורת עצמאי.

(ב) מפקח כללי בכל גוף ביטחוני, שתפקידו לפקח על פעילות מודיעין זר. המפקח הכללי עצמאי על פי חוק ומוסמך לבצע ביקורות וחקירות על פעולות שסוכנות המודיעין מבצעת למטרות ביטחון לאומי, ולתת המלצות פעולה לא מחייבות. לשם כך, בסמכות המפקח הכללי לגשת לכל מידע רלוונטי, לרבות מכוח צו אם יש בכך צורך, ואף לזמן למתן עדות לפניו. דוחות הביקורת וההמלצות מועברים לעיון הקונגרס ומפורסמים לציבור.

(ג) משרד הפרטיות וזכויות האדם שבמשרד המשפטים (Office of Privacy and Civil Liberties) מוסמך לבקר את כל גופי המודיעין ולחקור כל מידע או תלונה בנוגע לפעילות בלתי חוקית או ניצול לרעה של סמכות.

(ד) הוועדה המפקחת על הפרטיות וזכויות האזרח (The Privacy and Civil Liberties Oversight Board) היא וועדה עצמאית בת 5 חברים הממונים על ידי הנשיא, באישור הסנאט, לתקופה של 6 שנים. הוועדה מוסמכת לערוך ביקורת על פעילות קהילת המודיעין בכל הקשור למדיניות מניעת טרור והגנה על הזכות לפרטיות וזכויות אדם אחרות ועל יישום הוראות ה- Presidential Policy Directive 28. במסגרת זו מוסמכת הוועדה לגשת לכל המידע המצוי בידי הגוף הביטחוני הנחקר, לקבל דיווחים מפקידי הפרטיות בכל הגופים הביטחוניים ולהעביר את המלצותיה לפקידי הפרטיות. הוועדה מדווחת באופן שיגרתי לוועדה ייעודית בקונגרס ולנשיא.

(ה) הוועדה הנשיאותית לביקורת על פעילות המודיעין (The President's Intelligence Oversight Board), שתפקידה לבחון ציות של כל גופי המודיעין לחוקה ולכללים המתאימים.

(ו) גופי הביטחון מתומרצים להטמיע באופן וולונטרי מערכות מידע שמאפשרות ניטור, תיעוד וביקורת של שאילתות או חיפוש אחר של מידע אישי. זאת על מנת להקל על הליך הביקורת הפנימי והחיצוני על פעולותיהם.

(ז) בעלי תפקידים בגופי הביטחון מחויבים לדווח במיידית לבכירים בגוף הביטחוני על אי ציות משמעותי הנוגע למידע אישי, ללא קשר ללאום נושא המידע או למקום מגוריו.

---

[27] לפי סעיף 4(a)(iv) ל-Presidential Policy Directive 28.

בעלי התפקידים הבכירים חייבים להעביר את דיווחים ו/או לוועדה הנשיאותית לביקורת על פעילות המודיעין. כאשר מדובר באי ציות הנוגע למידע אישי על נושא מידע ממדינה זרה על הדירקטור למודיעין לאומי בהיוועצות עם מזכיר המדינה וראש הגוף הביטחוני המדווח לקבוע האם יש להודיע על הפגיעה בפרטיות לממשלה הזרה הרלוונטית.

(ח) וועדת המודיעין וועדת המשפטים בקונגרס מקבלות מגופי הביטחון דיווחי ביקורת, החלטות בית משפט, דוחות שנתיים של המפקח הכללי, דוחות ציות של הדירקטור למודיעין לאומי והחלטות בנוגע לאי ציות.

(ט) על ממשלת ארה"ב לחשוף מידי שנה בפני הקונגרס והציבור את מספר ההוראות במסגרת ה-FISA שהתבקשו ושהתקבלו וכן הערכה של מספר נושאי המידע, אזרחי ארה"ב, ושאינם אזרחי ארה"ב, שהיו מושא למעקב ממוקד.

(י) עיבוד מידע אישי על ידי גופי הביטחון כפוף גם לביקורת שיפוטית. ה-FISA Court הוא טריבונל עצמאי, שהחלטותיו ניתנות לערעור בפני ה Foreign Intelligence Court of Review ואח"כ בית המשפט העליון. מתפקידו לתת הרשאות לגופי ביטחון לעיבוד מידע אישי. לפני פנייה לבית המשפט לקבלת הרשאה על הגוף הביטחוני להעביר טיוטת בקשה לאישור עורכי הדין במחלקת הביטחון הלאומי במשרד המשפטים. עורכי הדין הם שמעבירים את הבקשה להחלטת בית המשפט. בית המשפט רשאי לתת החלטה מיקדמית או לזמן לשימוע. בהחלטותיו מסתייע בית המשפטי בפאנל בן 5 מומחים מתחום הביטחון הלאומי וזכיות האזרח שמתוכם הוא רשאי למנות מומחה שישמש כידיד בית המשפט ויסייע בשקילת כל בקשה לצו או ביקורת שלדעת ביהמ"ש מהווה פרשנות חדשנית או משמעותית של החוק. מטרת מינוי ידיד בית המשפט היא להבטיח ששיקולי פרטיות יילקחו בחשבון באופן ראוי.

(4) קיומם של מנגנונים למתן סעד אפקטיבי לנושא מידע שזכותו לפרטיות נפגעה עקב עיבוד מידע אישי על ידי גופי ביטחון. אחד ממנגנונים ו/או הוא נציב קבילות הציבור לעניין ה- Privacy Shield Framework (Privacy Shield Ombudsperson). נציב תלונות הציבור הוא עצמאי ואינו כפוף לקהילת המודיעין האמריקאית. תפקידו לטפל בכל אותם מקרים שבהם נושא מידע מאירופה לא יוכל לתבוע סעד בגין פגיעה בפרטיותו בארה"ב. נושא מידע מהאיחוד יגיש תלונה בשפתו לנציבות המדינתית העוסקת בשימוש במידע אישי על ידי גופי ביטחון, זו תעביר את התלונה לגוף המרכזי באיחוד האירופי שיעביר את התלונה לנציב תלונות הציבור. בנוסף, משמש נציב התלונות גם כאיש הקשר לממשלות הזרות להעלאת חששותיהם בנוגע למבצעי איסוף מודיעין של ארה"ב.

3.2. אנגליה

חוק הגנת הפרטיות האנגלי שעמד בתוקפו עד 2018 התיר עיבוד מידע אישי לשם הגנה על ביטחון המדינה לפי מבחן הנחיצות.[28] אולם, בשנת 2018 נכנס לתוקפו חוק חדש להגנת פרטיות במידע. ההסדר בחוק החדש נועד לאפשר לגופי ביטחון להמשיך בפעילות החיונית הנדרשת לביטחון המדינה ואזרחיה לצד עמידה בסטנדרטים בינ"ל נדרשים להגנת פרטיות במידע.[29]

במסגרת ההסדר החדש, כאשר עיבוד המידע האישי נחוץ לשמירה על ביטחון המדינה, גופי המדינה פטורים מציות להוראות החוק בנושאים הבאים:[30]

(1) עיבוד המידע האישי נחוץ להגשמת מטרה ברורה ולגיטימית.

(2) המידע האישי נכון, מדויק ומעודכן ונשמר בהתאם למבחן הנחיצות ולדרישות אבטחת מידע.

(3) לנושא המידע הזכות לקבל הודעה, לעיון, לקבל הסבר, להתנגד לעיבוד אוטומטי של מידע אישי עליו, לתיקון ולמחיקה.

(4) חובת דיווח על אירועי אבטחה.

(5) סמכויות האכיפה של נציבות הפרטיות האנגלית, לרבות סמכותה להבטיח שיתוף פעולה בינלאומי.

כאשר עיבוד המידע על ידי גופי הביטחון נחוץ למטרות של אכיפה פלילית, פעולה צבאית או כאשר סביר שציות להוראות החוק יפגע ברווחה הכלכלית של המדינה, יורשה הגוף הביטחוני להימנע מציות להוראות המופיעות בסעיף 1-4 לעיל. בסמכות מזכיר המדינה להוסיף או להסיר חריגים למטרות נוספות.[31]

אישור בחתימת שר בקבינט או היועץ המשפטי לממשלה נחשב ראייה מספקת, מכריעה וסופית לנחיצות עיבוד המידע האישי על ידי הגוף הביטחוני למטרת הגנה על ביטחון המדינה. אולם, נושא מידע הרואה עצמו נפגע כתוצאה מהאישור רשאי לערער לפני בפני בית המשפט המוסמך. מצא בית המשפט שלשר לא היו סיבות סבירות להוצאת האישור רשאי הוא להתיר את הערעור ולשלול את אישור השר.[32]

החידוש המרכזי של החוק משנת 2018 הינו בהגברת דרישת השקיפות ביחס לאישור נחיצות העיבוד להגשמת אחת מהמטרות המותרות בחוק. על שר שנותן אישור כי עיבוד המידע האישי ואי ציות להוראות חוק הגנת הפרטיות דרוש לצורך הביטחון הלאומי, לשלוח עותק מהאישור לנציבות

---

[28] סעיף 28 ל-Data Protection Act 1998 .
[29] Data Protection Act 2018, sec. 82-113 .
[30] סעיף 110 ל-Data Protection Act 2018 .
[31] נספח 11 ל-Data Protection Act 2018.
[32] סעיף 111 ל-Data Protection Act 2018 .

הפרטיות, שחייבת לפרסם תיעוד של האישור.[33] כעיקרון יש לפרסם את האישור במלואו, לא אם השר קובע שהפרסום מנוגד לאינטרס הביטחון הלאומי או לאינטרס הציבור או עלול לסכן את ביטחונו של אדם.

3.3. יפן

ב-23 בינואר 2019 נציבות האיחוד האירופי הכריזה על החלטתה להכיר בתאימות הדין ביפן ל-GDPR. לפני מתן ההחלטה וכתנאי לקבלת ההכרה ממשלת יפן נדרשה:

1) לאמץ כללים נוספים (Supplementary Rules) שנועדו לגשר על הפער בין הדין ביפן ל-GDPR בכל הקשור להגנה על מידע רגיש, מימוש זכויות נושא המידע והתנאים להעברת מידע אישי על אזרחי אירופה מחוץ לגבולות יפן למדינה אחרת שאינה חברה באיחוד האירופי.

2) ממשלת יפן התחייבה בפני נציבות האיחוד האירופי שאפשרות הגישה של רשויות ציבור למידע אישי על נושאי מידע מהאיחוד האירופי למטרות של אכיפת הדין הפלילי ולצרכיי ביטחון המדינה תהיה מוגבלת לדרוש, מידתית ונתונה לביקורת חיצונית ולמנגנון פיצוי יעיל.

3) לאמץ מנגנון לניהול תלונות, המנוהל ומפוקח על ידי רשות הגנת פרטיות עצמאית ביפן, שתפקידה יהיה לחקור ולטפל בתלונות אזרחי האיחוד האירופי בנוגע לגישה למידע אישי עליהם על ידי רשויות ציבור יפניות.

שנתיים מקבלת החלטת התאימות תבוצע ביקורת משותפת על מנת לבחון את היישום של הכללים הנוספים ושל התחייבות ממשלת יפן בכל הנוגע לגישת רשויות הציבור למידע אישי על נושאי מידע מהאיחוד האירופי לצרכיי אכיפה פלילית וביטחון המדינה. לאחר הביקורת הראשונית הנ"ל תבוצע ביקורת כאמור מידי 4 שנים.[34]

3.4. קנדה

בשנת 2001 קיבלה נציבות האיחוד האירופי החלטה בדבר תאימות הדין בקנדה לזה שבאיחוד בהתאם לדירקטיבה להגנה על הזכות לפרטיות במידע משנת 1995. אולם, בשנת 2013 קראה ועדה בנושא זכויות אדם של פרלמנט האיחוד האירופי (the European Parliament's Committee on

---

[33] **סעיף 130 ל-Data Protection Act 2018.**

[34] **להודעת האיחוד:** http://europa.eu/rapid/press-release_IP-19-421_en.htm?mkt_tok=eyJpIjoiWmpJNE56UXhOMkl6TnpRdyIsInQiOiJIWlhXd0xLNGZLaWVDalwvVWR4ejRkZzBXZlQ3VjlzaDFpb2lFQ1djekg4QOsrRONiRmJEZGIrdlBNQThPMjRrZUhOaW1XdWNZUG9Jb2NyZ3BZbWlKRO5kQjZCKOhYNDhHTGFjYVY1QkdVRE0renczWHR2NXJVSnZxNWh6ajlSeVUifQ%3D%3D.

(Civil Liberties, Justice and Home Affairs (the LIBE committee לבחון מחדש את החלטת התאימות. הנימוק לקריאה זו היה הגילויים למעורבותה של קנדה ב Five Eyes Alliance (ארה"ב, קנדה, אנגליה, אוסטרליה וניו זילנד), שהעלו חששות בנוגע לגישה ולשימוש שעושים שירותי הביטחון בקנדה במידע אישי.[35]

מחלקת מדיניות החוץ בקנדה (Global Affairs Canada) פרסמה ביולי 2016, בעקבות כניסתו לתוקף של ה Privacy Shield Framework בין האיחוד האירופי לארה"ב מזכר בו העלתה את החשש שבבחינת החלטת התאימות מחדש ב-2020, או קודם לכן אם יוגש הליך משפטי בעניין, תדרוש נציבות האיחוד האירופי מקנדה להתחייב לסטנדרט הגנת פרטיות במידע קשוח יותר מזה המקובל כיום, בדומה להתחייבויות שנדרש הממשל בארה"ב לספק. במזכר, שרק חלקו פורסם לציבור, הוזכר גם שמתקיימת בחינה משותפת למחלקת החוץ ולרשות החדשנות בקנדה (Innovation, Science and Economic Development (ISED) federal department) לבדיקת השפעת שלילת הכרת התאימות על עסקים בקנדה. קיימת מחלוקת בנוגע למידת ההשפעה, אך ההנחה הרווחת היא שחברות קטנות ובינוניות לא יוכלו להמשיך בהעברת מידע מאירופה לקנדה בהיעדר החלטת תאימות.[36] יתרה מכך, בעקבות חתימת הסכם הסחר בין קנדה לארה"ב בשנת 2017 (Canada – European Union Comprehensive Economic and Trade Agreement), הפגיעה בעסקים קנדיים בעקבות הסרת ההכרה בתאימות עלולה להיות חמורה.[37]

בשנת 2017 החלה ה House of Commons Standing Committee on Access to Information, Privacy and Ethics בקנדה בבחינה מהם התיקונים הנחוצים בחוק הגנת הפרטיות במידע הקנדי (PIPEDA). לשם כך זימנה הוועדה מגוון אנשי מקצוע למתן עדות. מהדיונים עולה ההנחה שה-PIPEDA במצבו הנוכחי, ללא תיקון משמעותי, לא יאפשר חידוש ההכרה האירופית בתאימות לדין האירופי לפי דרישת השווה ערך במהותו (essentially equivalent). זאת משום שה - PIPEDA חסר הוראות בנוגע לסמכות נציבות הפרטיות לקבוע מדיניות, להטיל קנסות מינהליים וכן אין זכות מפורשת למחיקה ולניוד. בנוסף המעורבות של קנדה ב Five Eyes, כמו גם הצעת החוק Bill C-51, Security of Canada Information Sharing Act מהווה אבן נגף משמעותית בפני ההכרה

---

[35] European Parliament Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188 (INI)) (23.12.2013).

[36] Ethan Lou, Canda Privacy Law May Be Held to EU-U.S. Model: Internal Memo, Reuters (July 12, 2016).

[37] Ryan Chiavetta, *Could Canada Lose Its Adequacy Standing?*, International Association of Privacy - The Privacy Advisor (Jun. 27, 2017).

בתאימות.[38] כמו כן, נטען שהחלטת התאימות משנת 2001 ניתנה כבר אז ברגשות מעורבים מצד האיחוד האירופי ומלכתחילה היתה חלקית וצומצמה רק לחברות ולארגונים פרטיים שה-PIPEDA חל עליהם. מאז 2001 בעוד מדינות אחרות בעיקר באיחוד האירופי קידמו ושיפרו את חקיקת הגנת הפרטיות שלהן, קנדה נותרה בעינה.

3.5. הודו

הודו נמצאת בימים אלו בתחילתו של תהליך עם נציבות האיחוד האירופי לקבלת הכרה בתאימות הדין ההודי להגנה על הזכות לפרטיות הנהוגה באיחוד האירופי. כחלק מהתהליך על הודו לחוקק חוק הגנת פרטיות שטיוטה שלו פורסמה לראשונה ביולי 2018 אך טרם הוצגה לאישור הפרלמנט ההודי.[39]

לפי הצעת החוק, עיבוד מידע על ידי גופי ביטחון לטובת ביטחון המדינה או למטרה של מניעה, גילוי, חקירה והעמדה לדין של עבירה או על הפרה של חוק מותר רק אם מעוגן בחוק, מבוצע בהתאם למנגנון שיקבע באותו החוק ועומד במבחן הנחיצות והמידתיות.[40] שמירת מידע אישי שעובד מכוח חריגים אלו תעשה בהתאם למבחן הנחיצות או לצורך תיעוד.

3.6. צרפת

בדצמבר 2018 התקבל בצרפת חוק הגנת פרטיות במידע חדש אשר החליף את החוק משנת 1978 ונחקק במטרה להגביר את התאימות עם דרישות האיחוד האירופי כפי שהן מפורטות ב-GDPR.

לפי החוק החדש הוראה מהשר או השרים האחראיים, שתינתן לאחר פרסום חוות דעת מנומקת של נציבות הפרטיות בצרפת, תתיר עיבוד מידע אישי הנעשה בשם המדינה ו - (1) נוגע לביטחון המדינה, הגנה או ביטחון הציבור; או (2) שמטרתו מניעה, חקירה או הוכחה של עבירה פלילית, העמדה לדין של העבריינים או הוצאה לפועל של ענישה פלילית או אמצעי אבטחה. עיבוד מידע אישי רגיש (דעה פוליטית, פילוסופית, מצב רפואי או חיי מין) יבוצע רק לאחר הסמכה בצו ובכפוף לחוות דעת של מועצת המדינה (ה Conseil dÉtat),[41] שתינתן לאחר פרסום חוות דעת מנומקת של נציבות

---

[38] Timothy M. Banks, Should PIPEDA be amended to meet GDPR requirements?, Privacy Tracker (Apr. 4, 2017).

[39] Abhimanyu Ghoshal, *India to Seek EU's Approval on GDPR Compliance for 'adequacy' Status, The Next Web (30 July, 2019)*; Megha Mandavia, *India to Approach the EU Seeking 'Adequacy' Status with the GDPR, Economic Times (July 30, 2019).*

[40] סעיף 42 ו 43 להצעת החוק ההודית.

[41] מועצת המדינה מתפקדת כגוף לייעוץ משפטי לרשות המבצעת והן כבית המשפט העליון בנושאים הקשורים במשפט המינהלי.

הפרטיות. חוות הדעת והצו יפורסמו לציבור, לא אם מועצת המדינה קבעה שאין לפרסמם.[42] מועצת המדינה רשאית גם להתיר בצו, לאחר קבלת החלטה מנומקת של נציבות הפרטיות, עיבוד פרטי מידע רגישים ומזהים כגון תעודת זהות ומידע ביומטרי, ובלבד שהמידע המעובד לא ישולב עם עיבוד מידע אישי שנעשה למטרות ציבוריות על ידי רשויות ציבור שתפקידן לקבוע את התנאים והיקף זכויות אזרחים, שליטה או איסוף מס או למטרות סטטיסטיות.[43]

4. המצב בישראל

4.1. חוק הגנת הפרטיות

סעיף 19 לחוק הגנת הפרטיות, התשמ"א - 1981 קובע:

(א) לא ישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין.

(ב) רשות ביטחון, או מי שנמנה עם עובדיה או פועל מטעמה, לא ישאו באחריות לפי חוק זה על פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו.

(ג) "רשות ביטחון", לענין סעיף זה - כל אחד מאלה:

(1) משטרת ישראל;

(2) אגף המודיעין במטה הכללי והמשטרה הצבאית של צבא הגנה לישראל;

(3) שירות ביטחון כללי;

(4) המוסד למודיעין ולתפקידים מיוחדים;

(5) הרשות להגנה על עדים.

החוק קובע פטור כללי לגופי ביטחון המוגבל לפי התנאים הבאים:

1) מבחן סבירות

2) פעילות במסגרת התפקיד ולשם מילויו.

בדיון הראשון בפרשת ועקנין[44] קבע השופט בך בדעת הרוב שהשקיית המערער במי מלח מהווה הטרדה אחרת לפי ס' 2(1) לחוק הגנת הפרטיות ויכולה להתבצע רק מכוח הסמכה מפורשת בחוק. נפסק שס' 19(ב) לחוק הגנת הפרטיות אינו מהווה הסמכה שכזו. בנוסף, ולמעלה מן הצורך קבע השופט בך שאין הפעולה עומדת במבחן הסבירות הנדרש בס' 19(ב). לבד מפסק דין זה, בתי המשפט לא עסקו בפרשנות שיש לתת לס' 19(ב).

---

[42] סעיף 26 ל-Loi n°2018-493 on the protection of personal data .

[43] סעיף 27 ל-Loi n°2018-493 on the protection of personal data .

[44] בג"ץ 249/82 ועקנין נ' בית הדין הצבאי לערעורים, פ"ד לז(2) 393.

במסגרת זו לא נראה שס' 19(ב) מספק את התנאים לחריג לגופי ביטחון הנדרשים באירופה. החריג אינו דורש בסיס משפטי ברור לפגיעה ולא מסתפק בהצהרה שהפעולה נעשתה במסגרת התפקיד או לשם מילויו. החריג אינו מחייב שהפעולה תעשה בהתאם למבחן נחיצות ומידתיות ולא מסתפק במבחן סבירות בלבד. הפגיעה בפרטיות אינה כפופה לפיקוח חיצוני ברור. באשר לסעדים האפקטיביים, לכאורה אדם שנפגעה פרטיותו עקב מעשה של גוף ביטחון יכול לפנות לביהמ"ש בטענה לפגיעה בפרטיותו, אולם אם ימצא ביהמ"ש שמתקיימים תנאי ס' 19(ב), כלומר שפעולת גוף הביטחון היתה סבירה ובמסגרת תפקידיו, בין אם נקבעו בדין ובין אם לאו, לא יעמדו בידי הנפגע כל סעדים אפקטיביים שכן הקביעה היא שלא נעשתה כל פגיעה בפרטיות.

4.2. חוק שירות הביטחון הכללי, תשס"ב 2002

חוק שירות הביטחון הכללי, תשס"ב 2002 קובע בס' 8(א)(1) שלצורך מילוי תפקידו השירות באמצעות עובדיו מוסמך לקבל ולאסוף מידע. ס' 18 לחוק קובע סייג כללי לאחריות פלילית או אזרחית, שאינו מתייחס במפורש לפגיעה בפרטיות:

"עובד השירות או הפועל מטעם השירות לא יישא באחריות פלילית או אזרחית למעשה או למחדל שעשה בתום לב ובאופן סביר במסגרת תפקידו ולשם מילויו; ואולם אין בהוראות סעיף זה כדי לגרוע מאחריות משמעתית לפי כל דין."

התנאים לסייג הם:

(1) תום לב

(2) מבחן סבירות

(3) פעולה במסגרת התפקיד ולשם מילויו.

באשר לפיקוח, סעיף 13 לחוק השב"כ מעגן את מנגנון הביקורת הפנימית על פעולות השב"כ. לפי ס' 6, 7 ו-12 לחוק השב"כ קיימת מידה מסוימת של פיקוח חיצוני על פעולות השירות על ידי ועדת השרים לענייני השירות. עם זאת, לפי החוק השב"כ חייב רק בדיווח לוועדה מידי 3 חודשים ודיוני הוועדה חסויים. החוק אינו מפרט סמכויות פיקוח ואכיפה כלשהן לוועדה.

גם בחוק השב"כ נראה שהסייג אינו עומד בדרישות האיחוד האירופי. הבסיס המשפטי עשוי להיחשב מספק, על אף שמדובר בהסמכה כללית למדי. המבחן הנקט הוא מבחן הסבירות ולא מבחן מידתיות ונחיצות. בידי אדם הנפגע האפשרות לפנות לבית המשפט בטענה לפגיעה בזכויותיו, אם כי לא מדובר בסעדים זמינים הקשורים בהכרח לעיבוד המידע.

4.3. תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018

בתזכיר חוק הסייבר ההתייחסות לשימוש במידע לצורך ביצוע תפקידי המערך ברורה ומפורשת.

ס׳ 16(א)(1)-(3) מסמיך את המערך לאסוף, לעבד ולהפיץ ״מידע בעל ערך אבטחתי״ לצורך מילוי תפקידי המאגר. תפקידי המאגר מפורטים בס׳ 3 בהרחבה (כלל כל הדרוש להגנת הסייבר ולמובילות ישרא׳ בתחום הסייבר). עיבוד המידע ואיחסונו צריכים להיעשות בהתאם לסעיף 38 ו-39 המחייבים עיצוב לפרטיות (PBD) ושמירת על סודיות המידע.

ס׳ 8 לתזכיר חוק הסייבר קובע סייג לאחריות זהה לזה שבחוק השב״כ. כלומר, המבחן הוא מבחן סבירות ולא מידתיות ונחיצות.

ס׳ 64(ב) לתזכיר חוק הסייבר קובע חריג ייחודי לאחריות עובד מערך הסייבר לפי חוק הגנת הפרטיות שאף הוא מציב את סטנדרט הסבירות כסטנדרט הקובע ואינו מכפיף את הסייג לאחריות למבחני מידתיות ונחיצות הנהוגים באירופה.

מבחינת רמת הפיקוח והבקרה החיצונית על מערך הסייבר מתקבלת תמונה שונה מזו שבחוק השב״כ. ס׳ 12-10 לתזכיר עוסקים במינוי מפקח פרטיות פנימי. המפקח הוא עובד המערך וכפוף לראש המערך, ולכן אין מדובר בפיקוח עצמאי. לעומת זאת, ס׳ 13-15 קובע שראש המשלה ימנה ועדת פיקוח חיצונית אשר תפקח על פעילות המערך בהקשר של השפעת פעילותו על הזכות לפרטיות. לוועדה סמכויות לאסוף מידע רלוונטי ולזמן למתן עדות בפניה. עם זאת לפי ס׳ 15(ב) אם עולה חשד הועדה לפעילות המפרה את הדין עליה להפסיק את הטיפול בנושא ולהעביר את הבירור והטיפול בהפרת הדין לגורם המוסמך.

החוק אינו מפרט מנגנון לקבלת סעד אפקטיבי ועל כן ההנחה היא שהסעד ינתן מכוח תביעה לבית המשפט לעניינים מינהליים או לבג״ץ בגין פעולתה של רשות ציבורית. עם זאת, מאחר וכל פעולות המערך חסויות לפי ס׳ 72 לתזכיר החוק, לא ברורה מידת היכולת של האדם הנפגע לדעת על הפגיעה בו ולפנות לבית משפט.

4.4. סיכום המצב המשפט בישראל

הפטור הניתן לגופי ביטחון בישרא׳ ככלל אינו עומד בדרישות האיחוד האירופי.

הפטור מבוסס בחוק הגנת הפרטיות, חוק השב״כ ותזכיר חוק הסייבר על מבחן סבירות ולא על מבחן מידתיות.

הפטור הקבוע בחוק הגנת הפרטיות אינו מפרט בסיס משפטי ברור.

מידת הפיקוח החיצוני אינה ברורה בכל הנוגע לפטור הקבוע בחוק הגנת הפרטיות. גם בחוק השב״כ לא ברורות מהן סמכויות הפיקוח של ועדת השרים לענייני שירות הביטחון.

ולבסוף, אף אחד מהחוקים אינו מפרט מנגנון סעדים אפקטיבי וזמין.

התפיסה שפסיקותיו של בג״ץ בעבר וחוזקו כיום בשמירה על הדמוקרטיה בישרא׳ ועל זכויות האדם הם שיתנו מענה אשר יספק את נציבות האיחוד האירופי היא לדעתנו תפיסה שגויה. בג״ץ אומנם יכול לשמש כמנגנון ביקורת חיצונית אפקטיבית על פעולותיהם של גופי הביטחון בכל הקשור לפגיעה בזכות לפרטיות ואף לספק סעד יעיל לנושאי מידע שזכותם לפרטיות נפגעה. אולם, לדעתנו

הישענות על קיומו של בג"ץ לבדו אינה מספקת. הניסיונות להחליש את כוחו של בג"ץ בשנים האחרונות והיסטוריה ארוכה של אי ציות מלא לפסיקותיו מלמדים שכדי לספק הגנה מתאימה לזכות היסוד לפרטיות יש לקבוע בחוק מנגנון מקיף וברור אשר יכיר בצורך החשוב להגן על ביטחון המדינה והציבור ובאינטרס אכיפת החוק, אולם גם יבטיח שפגיעה בזכות לפרטיות למטרות אלו תעשה רק כאשר היא נחוצה להגשמתן ובאופן מידתי.[45]

[45] אהרון ברק, **זכויות אדם וביטחון לאומי, משפטים** לח(1) 29 (תשס"ח); יעל כהן רימר, **בית המשפט פוסק והמדינה מצפצפת: על היכולת לאכוף משטר של זכויות אדם ועל ביזיון בית המשפט ב-2008, המכון הישראלי לדמוקרטיה** (10 בפברואר, 2009); עמיקם הרפז ומרים גולן, **משפט ושיטור: זכויות אדם וסמכויות המשטרה** (המכון הישראלי לדמוקרטיה, נבו, 2018).