

המטאטא יאה לנו – "הכלי" של השב"כ והחלטת הנאותות האירופית

עמיר כהנא*

ב-6 באוקטובר 2020 ניתנו בבית הדין לצדק של האיחוד האירופי (להלן: בית הדין האירופי) שני פסקי דין העוסקים בחקיקה המורה לִפְסָקִים של שירותי תקשורת לשתף פעולה עם רשויות הביטחון ואכיפת החוק, ולסייע בדרכים שונות לניהול מעקבים מקוונים: פסק הדין בעניין *Privacy*¹ ופסק הדין בעניין *Quadrature du Net*². שני פסקי הדין לא סטו מהקו שבו נוקט בית הדין האירופי בשנים האחרונות³ – קו של אפס סובלנות כלפי פרקטיקות של מעקב מקוון הפוגעות בזכויות הגנת הפרטיות המעוגנות בדין האירופי⁴ – והתמקדו בפרקטיקות של איסוף ושימור נתוני תקשורת.

נתוני תקשורת הם נתונים על אודות תקשורת שאינם נתוני תוכן – פרטי המוען והנמען של דבר הדואר, מספרי הטלפון המעורבים בשיחה, מיקום מכשיר הסלולאר שממנו נערכה השיחה וכד'. הבחנה זו, ששורשיה במאה התשע-עשרה,⁵ מניחה שרמת הפגיעה בפרטיות אגב עיון והשגת נתוני תוכן גבוהה יותר מהפגיעה בפרטיות הנגרמת בשל איסוף נתוני תקשורת –

אזכור הרשימה: עמיר כהנא "המטאטא יאה לנו – הכלי" של השב"כ והחלטת הנאותות האירופית" אתר משפט ועסקים 29.3.2021 www.idclawreview.org/2021/03/29/acahane

* בוגר תואר שני במשפטים (LL.M.) מאוניברסיטת קיימברידג'. חוקר במרכז לערכים ולמוסדות דמוקרטיים שבמכון הישראלי לדמוקרטיה. עמית מחקר במרכז פדרמן לחקר הסייבר באוניברסיטה העברית, התוכנית לסייבר ומשפט. תודתי נתונה לד"ר תהילה שוורץ-אלטשולר, לעו"ד דפנה דרוו-שפוליאנסקי וכן לעורכות כתב העת **משפט ועסקים** – שיר אברהם ורותם תמיר – על הערותיהן המועילות לרשימה זו.

1 CJEU, Cases C-623/17, [Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others](#), (להלן: עניין *Privacy*). (6.10.2020)

2 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, [La Quadrature du Net and Ordre des barreaux francophones et germanophone v. Premier ministre and Others](#) (6.10.2020)

3 CJEU, C-362/14, [Maximillian Schrems v. Data Protection Commissioner](#) (6.10.2015) (להלן: עניין *Schrems*); CJEU, C-311/18, [Maximillian Schrems v. Data Protection Commissioner](#) (16.7.2020) (*Schrems 2*); CJEU, Joined cases C-293/12 and C-594/12, [Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources, Seitlinger and Others](#), (18.4.2014) [2014] E.C.R. I-238; CJEU, Joined Cases C-203/15 and C-698/15, [Tele2 Sverige AB and Secretary of State for the Home Department v. Post- och telestyrelsen and Others](#), (21.12.2016) (להלן: עניין *Tele2*).

4 [Directive 2002/58/EC of 12 July 2002 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, as Amended by Council Directive 2006/24/EC and Council Directive Directive 95/46/EC of 24 October 1995](#); (להלן: *2009/136/EC (e-Privacy Directive)*); [Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive \(EU\) 2016/680 of the European Union Parliament and of the Council of 27 April 2016](#); ((GDPR)); [Directive \(EU\) 2016/680 of the European Union Parliament and of the Council of 27 April 2016](#); (להלן: *Directive 95/46/EC (General Data Protection Regulation)*), 2016 O.J. (L 119) 1 (EU) [on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data and Repealing Council Framework Decision 2008/977/JHA](#), OJ L 119, 4.5.2016, p. 89–131. [המשווה](#) 104–131 (מחקר מדיניות 123, המכון הישראלי לדמוקרטיה, 2019).

5 *Ex Parte Jackson*, 96 U.S. 727 (1877)

ובהתאמה, הוראות הדין נוטות להקל על סוכנויות המודיעין ואכיפת החוק בבואן להשיג נתוני תקשורת.⁶ בעידן של שימוש רחב היקף במכשירי קצה סלולאריים⁷ ובהתקני "האינטרנט של הדברים" (IoT),⁸ ובמיוחד לנוכח הפוטנציאל המודיעיני של פרקטיקות איסוף גורפות ויכולות העיבוד והניתוח הממוכנים של נתוני תקשורת,⁹ ספק אם הנחה זו עודנה בתוקף.¹⁰

בעניין *Privacy*, התבקש בית הדין האירופי על ידי טריבונל סמכויות החקירה הבריטי (IPT) – ערכאה מיוחדת הדנה בעניינים הנוגעים לשירותים החשאיים של הממלכה המאוחדת¹¹ – לדון בתחולת הדין האירופי ביחס להוראה בחוק הבריטי המקנה לשר הפנים סמכות להורות לספקי תקשורת להעביר נתוני תקשורת לשירותי המודיעין והביטחון,¹² בדומה לנעשה בישראל,¹³ ובמידה שיימצא כי הדין האירופי אכן חל, להבהיר אילו מדרישות בית הדין האירופי בעניין *Tele2* ביחס לשימור נתונים¹⁴ רלוונטיות ביחס להוראה כזו של השר.¹⁵

- 6 ראו והשוו, לדוגמה, בין ההוראות החלות על השגת נתוני תקשורת לתכליות ביטחוניות שבס' 11 לחוק שירות הביטחון הכללי, התשס"ב-2002 (להלן: חוק השב"כ) לבין אלו החלות על האזנות סתר לתכליות אלה שבס' 4 לחוק האזנות סתר, התשל"ט-1979; כן ביחס לחומרת העבירות המצדיקות השגת נתוני תקשורת לעומת האזנות סתר לתכליות של אכיפת חוק, השוו את ס' 6(א) לחוק האזנות סתר עם ס' 4(א2)-(2)-(3) לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007. ראו גם בג"ץ 3809/08 האגודה לזכויות האזרח בישראל נ' משטרת ישראל, פס' 18-21 לפסק דינה של הנשיאה (בדימי) ביניש (פורסם בפורטל המשפטי לאינטרנט, סייבר וטכנולוגיית, 28.5.2012). ראו גם את החלטת בית הדין האירופי בעניין *Case C-207/16 Ministerio Fiscal* (2.10.2018), שם נערך איוון עדין יותר הבוחן את היחס בין חומרת העבירה למידת החדירה לפרטיות הכרוכה בהשגת נתוני תקשורת במסגרת חקירתה. באותו עניין, נתוני התקשורת המבוקשים היו נתוני זיהוי המצליבים בין מנוי למספר המזהה של מכשיר הקצה שברשותו (International Mobile Equipment Identity code, IMEI).
- 7 ראו *Riley v. California*, 134 S. Ct. 2473 (2014), ובפרט המובאות מפסק הדין שצוטטו בפס' 200-201 אצל *National Council for Civil Liberties (Liberty), R (On the Application Of) v. Secretary of State for the Home Department & Anor* [2019] EWHC 2057 (Admin) (29.07.2019) (להלן: עניין *Liberty*).
- 8 הטכנולוגיה המאפשרת לחפצים פיזיים ולמוצרים לתקשר זה עם זה ועם סביבתם מכונה "האינטרנט של הדברים" (Internet of Things או IoT). זוהי הארכיטקטורה המאפשרת את קיומם של חפצים "חכמים" שאוספים, מעבדים ומעבירים נתונים על מנת ליעיל את פעולתם. ראו, לדוגמה, רועי צזנה **השולטים בעתיד** 56-64 (2017). ראו גם Amit Kumar Tyagi & M. Shamila, *Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices*, SSRN (20.3.2019); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016); GILAD ROSNER & ERIN E. KENNEALLY, **CLEARLY OPAQUE: PRIVACY RISKS OF THE INTERNET OF THINGS** (IoT Privacy Forum, 2018). ראו גם פס' 172 בעניין *Liberty*, שם, באשר לסוגים של "נתונים משניים" שחרף העובדה שאינם נתוני תוכן, ביכולתם להסגיר מידע רב על אודות מושאם.
- 9 בדו"ח ועדת המודיעין והביטחון הפרלמנטרית הבריטית (ISC) מחודש מרץ 2015, צוין כי סוכנות התקשורת הממשלתית (GCHQ) סבורה כי במסגרת החומר המופק מאיסוף חסר הבחנה (bulk collection), הנתונים הנלווים לנתוני התוכן, כלומר ה-metadatas, הם בעלי ערך משמעותי יותר מנתוני התוכן עצמם. *INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK* (12.3.2015); *EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW, REPORT ON THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES*, Par. 48 (15.12.2015); Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime*, submission 29 by the Law Council of Australia, Par. 71 (18.7.2019), ראו Tyagi & Shamila, *Listening in 15* (2017); שם; Ferguson & Rosner & Kenneally, שם; Susan Landau, *Listening in 15* (2017); שם; Patrick Breyer, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 EUR. L. J. 365, 370-371 (2005), ראו, למשל, עניין *Liberty*, לעיל ה"ש 7, בפס' 175.
- 10 על טריבונל סמכויות החקירה, ראו עמיר כהנא ויובל שני **פיקוח על מעקב מקוון בישראל** 132-135 (מחקר מדיני 149, המכון הישראלי לדמוקרטיה, 2020).
- 11 *Telecommunications Act 1984*, c.12, Sec. 94 (Eng.).
- 12 ס' 11 לחוק השב"כ; ס' 13 לחוק התקשורת (בזק ושידורים), התשמ"ב-1982 (להלן: חוק הבזק).
- 13 ראו עניין *Tele2*, לעיל ה"ש 3, פס' 119-125 לפסק הדין.
- 14 עניין *Privacy*, לעיל ה"ש 1, פס' 29 לפסק הדין.

בית הדין מצא כי חקיקה לאומית המורה לספקי תקשורת לאפשר לגופי ביטחון ואכיפת חוק גישה לנתוני תקשורת חוסה תחת דירקטיבת הפרטיות האלקטרונית, מאחר שהעברת נתונים מספק פרטי לרשות ציבורית היא כשלעצמה פעולת עיבוד.¹⁶ עוד קבע בית הדין כי הוראה מיניסטריאלית לספקי תקשורת להעביר נתוני תקשורת באופן גורף לסוכנויות הביטחון והמודיעין, גם לתכליות של בטחון לאומי בלבד, מהווה פגיעה בלתי מידתית בזכויות שלפי הדירקטיבה, וכי הדין הלאומי צריך להגדיר מראש את הנסיבות והתנאים שיאפשרו גישה לנתונים אלה.¹⁷

בישראל, שירות הביטחון הכללי הוסמך בשנה החולפת לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה.¹⁸ הסמכה זו, שהחלה בתקנות שעת חירום,¹⁹ ובעקבות פסק הדין בעניין **בן מאיר**,²⁰ עוגנה בחקיקה ראשית,²¹ העלתה את מודעות הציבור לקיומו של "הכלי".²² "הכלי" הוא כינויו של מאגר נתוני התקשורת של השירות. חוק השב"כ הוא הבסיס המשפטי המסמיך זה כעשרים שנה את השירות לאסוף את כל נתוני התקשורת של לקוחות של ספקי תקשורת בעלי רישיון בזק (חברות סלולר, אינטרנט וטלפוניה קווית).²³ הוראה משלימה להסמכה זו מצויה בסעיף 13 לחוק הבזק, שלפיו ראש הממשלה רשאי להורות לבעלי רישיון ל"ביצוע התאמה טכנולוגית... לרבות מתן גישה למתקן בזק, ככל שהדבר דרוש לצורך ביצוע תפקידיהם של כוחות הביטחון".²⁴

לנוכח פסק הדין בעניין *Privacy* נראה כי המצב בישראל אינו נמצא בהלימה עם הדין האירופי. סעיף 13 לחוק הבזק מדהדה את ההסדר שבסעיף 94 לחוק התקשורת הבריטי, לפיו נדרשים ספקי תקשורת להעביר על בסיס הוראה מיניסטריאלית נתוני תקשורת בהגדרתם הרחבה ביותר²⁵ לשירותים החשאיים. הסדר זה נמצא על ידי בית הדין האירופי כמפר את דרישת המידתיות ביחס לחקיקה החורגת מהוראות דירקטיבת הפרטיות האלקטרונית,²⁶ וסביר להניח שהתשתית המשפטית שמכוחה מוסמך השב"כ לעסוק באיסוף גורף של נתוני תקשורת המטואטאים אל תוך מאגר "הכלי" ללא הבחנה, גם היא אינה מידתית לשיטת בית הדין האירופי.

- 16 שם, פס' 40–49 לפסק הדין.
- 17 שם, פס' 74–81 לפסק הדין.
- 18 Amir Cahane, [Israel's SIGINT Oversight Ecosystem: COVID-19 Secret Service Location Tracking as a Test Case](#), U.N.H.L. REV. (Forthcoming 2021); Amir Cahane, [Who Will Watch the Watchmen? Oversight of Online Surveillance in Israel](#), ISRAEL PUBLIC POLICY INSTITUTE AND HEINRICH BÖLL FOUNDATION (2.12.2020)
- 19 תקנות שעת חירום (הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש), התש"ף-2020.
- 20 בג"ץ 2109/20 **בן מאיר נ' ראש הממשלה** (פורסם באר"ש, 26.4.2020).
- 21 חוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש וקידום השימוש בטכנולוגיה אזרחית לאיתור מי שהיו במגע קרוב עם חולים (הוראת שעה), התש"ף-2020.
- 22 רונן ברגמן ועידו שברצטוך "הכלי", מאגר המידע הסודי של השב"כ, אוסף נתונים על כל אזרחי מדינת ישראל ויודע: איפה הייתם, עם מי דיברתם, ומתי עשיתם את כל זה" **ידיעות אחרונות** (25.3.2020); עמיר כהנא "הרגע הסנוורני (המוחמץ) של ישראל? בעקבות הגילויים האחרונים על איסוף מטאדאטה על ידי השב"כ" **אתר משפט ועסקים** (13.4.2020); Amir Cahane, [The \(Missed\) Israeli Snowden Moment?](#), 34; INT'L J. OF INTELLIGENCE & COUNTERINTELLIGENCE (forthcoming 2021).
- 23 ראו ס' 11 לחוק השב"כ. ראו גם כהנא ושני, לעיל ה"ש 4, בעמ' 52–53; אלי בכר **שב"כ במבחן: ביטחון, משפט וערכי הדמוקרטיה** 150–165 (2020).
- 24 ס' 13(ב)(2) לחוק הבזק.
- 25 השוו את הגדרת "מידע" שבס' 11 לחוק השב"כ עם הגדרת communications data בחוק הסדרת סמכויות חקירה 2000 (שנדון בעניין *Privacy*, לעיל ה"ש 1) – (Eng.) – [Regulation of Investigatory Powers Act 2000](#), c.23, Sec 21(4)(b) (Eng.).
- 26 ראו ס' 15(1) לדירקטיבת הפרטיות האלקטרונית.

ואולם מדוע אי-הלימה עם הדין האירופי עשויה להטריד את מקבלי ההחלטות בישראל? בימים אלה בוחנת הנציבות האירופית מחדש את הסטטוס של ישראל כמדינה שרמת ההגנה על הפרטיות שבה נאותה לפי הדין האירופי. תחת תקנות הגנת הפרטיות הכלליות של האיחוד האירופי (GDPR), העברת נתונים לצדדים שלישיים שאינם חברים באיחוד אסורה, אלא אם ניתן להבטיח כי רמת ההגנה עליהם לא תפחת מרמת ההגנה שתחת ה-GDPR.²⁷ דרך המלך להבטיח זאת היא באמצעות החלטה של הנציבות הקובעת כי רמת ההגנה שאותם צדדים מספקים היא נאותה. משניתנה החלטה נאותה ביחס למדינה, ארגון בין-לאומי או טריטוריה מסוימת – אין צורך באישור מיוחד להעברת מידע בין אותו צד שלישי לאיחוד האירופי.²⁸

בשנת 2011 הצטרפה ישראל לקבוצת המדינות הספורות שהאיחוד האירופי הכיר בתאימות הדין שלהן למשטר הגנת הפרטיות שלהן,²⁹ והכרה זו נמצאת עתה בבחינה מחדש.³⁰ הנפקות הכלכלית של החלטת נאותות כזו היא משמעותית, מבחינת העלויות הרגולטוריות הנחשבות מעסקים ישראליים, וחברות הייטק במיוחד, הפועלים מול מדינות באירופה ונדרשים במהלך העסקים הרגיל שלהם לקבל מידע על אזרחי האיחוד.³¹ החלטת הנאותות של שנת 2011 ניתנה באקלים אחר. היא ניתנה לפני החשיפות של אדוארד סנודן,³² ולפני חקיקת תקנות הגנת הפרטיות הכלליות של האיחוד האירופי, המציבות סטנדרט מפורט יותר לנציבות בכוחה לקבל החלטת נאותות, ובפרט, לתת את הדעת על היבטים של שלטון החוק, זכויות אדם וגישה של רשויות ציבוריות למידע פרטי.³³ נראה, אם כן, שלנוכח ההחלטה בעניין *Privacy*, ובשורה של החלטות נוספות שנתן בית הדין האירופי,³⁴ כי תוצאת הלוואי של חשיפת קיומו של "הכלי" עשויה היתה להשפיע לשלילה על ההחלטה בדבר רמת הנאותות של ישראל.

אולם מספר מסמכים שפרסמה לאחרונה הנציבות מאותתים שמא החלטת הנאותות ביחס לדין הישראלי לא תושפע מ"הכלי". ב-10 בפברואר 2021 פרסמה מועצת האיחוד את נוסח הצעת תקנות הפרטיות האלקטרונית (EPR).³⁵ נראה כי הנוסח המוצע לסעיף (a)(2)2 ל-EPR נועד להתמודד עם עניין *Privacy*, בהחריגו במפורש מתחולת ה-EPR פעולות "הנוגעות לבטחון לאומי, ואין נפקא מינה אם הן מבוצעות על ידי רשות ציבורית או על ידי ספק פרטי הפועל לפי הוראה של רשות

27 ראו ס' 44 לתקנות הכלליות בדבר הגנת מידע (GDPR).

28 ראו ס' 45 לתקנות הכלליות בדבר הגנת מידע (GDPR).

29 2011/61/EU: [Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data](#).

30 רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר [הצעת חוק הגנת הפרטיות, התשע"ט-2019](#) 8 (המכון הישראלי לדמוקרטיה, 2019).

31 ראו, למשל, עומר כביר "צלי ההדף של החלטת בית הדין של האיחוד יכולים להפיל גם את ההייטק בישראל" [כלכליסט](#) (19.7.2020); פרוטוקול ישיבה מס' 12 של ועדת החוץ והביטחון (זמנית), ועדת המשנה למודיעין ולשירותים חשאיים (זמנית), הכנסת ה-23, 20-21 (התייחסות ד"ר שוורץ אלטשולר) (26.5.2020); פרוטוקול ישיבה מס' 19 של ועדת החוץ והביטחון, הכנסת ה-23, 24 (התייחסות עו"ד חיים רביה) (29.6.2020).

32 Glenn Greenwald & Ewen MacAskill, [Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data](#), THE GUARDIAN (11.6.2013).

33 ס' 45(2)(a) לתקנות הכלליות בדבר הגנת מידע (GDPR); והשוו עס' 25 המקביל בדירקטיבת הגנת הפרטיות.

34 ראו לעיל ה"ש 2 ר4.

35 ST 6087 2021 INIT, [Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC \(Regulation on Privacy and Electronic Communications\) - Mandate for negotiations with EP](#) (10.2.2021).

ציבורית.³⁶ הנוסח המוצע מאפשר לקרוא את עניין *Privacy* כפסק דין שדן אך ורק בשאלת התחולה של דירקטיבת הפרטיות האלקטרונית (ביחס לחקיקה החלה) על ספקי תקשורת המעבירים מידע לרשויות הביטחון. מתוך שכך, ספק אם מלכתחילה ההלכה שנקבעה בעניין *Privacy* רלוונטית לחוק הבזק, וגם אם כן – הנוסח המוצע של ה-EPR מחריג הוראות דומות לאלו שבסעיף 13 לחוק הבזק מתחולתה, או אז אין אנו נדרשים לניתוח המידתיות שעריך בית הדין האירופי לאיסוף הגורף של נתוני תקשורת בכריטניה.

מסמך נוסף המאותת על כך שהחלטת הנאותות האירופית ביחס לדין הישראלי עשויה שלא לייחס חשיבות רבה ל"כלי" הוא טיוטת החלטת הנאותות ביחס לדין הבריטי, שפורסמה ב-19 בפברואר 2021.³⁷ לאחר פרישתה מהאיחוד האירופי בשלהי ינואר 2020, נותרו לבריטניה 11 חודשים עד תום שנת 2020 עד שזו תיחשב צד שלישי לצורכי העברות מידע תחת ה-GDPR, ומועד זה נדחה בקשה חודשים נוספים בעקבות החתימה על הסכם הסחר ושיתוף הפעולה בריטניה-אירופה בחודש דצמבר.³⁸ מכאן הצורך להחליט בדבר נאותות הדין הבריטי, ואכן, טיוטת החלטתה מציעה לקבוע כי דיני הגנת הפרטיות הבריטיים מעניקים רמה נאותה של הגנה על המידע האישי המועבר משטח שיפוט של האיחוד האירופי לזה של הממלכה המאוחדת.³⁹ טיוטת החלטת הנאותות תיקרא בעיון על ידי הגורמים במשרד המשפטים האמונים על המשא ומתן עם הנציבות האירופית על החלטת הנאותות בנוגע למשטר הגנת הפרטיות הישראלי. הטיוטה בוחנת בפרוטרוט את הדין הבריטי החל על עיבוד מידע פרטי,⁴⁰ היבטים הנוגעים לגישה למידע פרטי המועבר מהאיחוד האירופי, והשימוש בו על ידי רשויות ציבוריות בבריטניה – הן את המסגרת הסטטוטורית הכללית החלה על גישה כזו,⁴¹ הן את המשטר החל על גישה למידע פרטי לתכליות של אכיפת חוק⁴² ולתכליות של ביטחון לאומי.⁴³

תחת חוק סמכויות חקירה הבריטי,⁴⁴ סוכנויות הביטחון ואכיפת החוק בממלכה המאוחדת מוסמכים להשתתף בשלל פרקטיקות סיגינטיות – יירוט ממוקד⁴⁵ ובלתי ממוקד⁴⁶ של נתוני תוכן, השגה ממוקדת של נתוני תקשורת,⁴⁷ הוראה לספקי

36 ראו שם, בפס' 7a למבוא ל-EPR (התרגום שלי, ע"כ).

37 European Commission, [Draft decision on the adequate protection of personal data by the United Kingdom - General Data Protection Regulation](#) (19.2.2021) (להלן: טיוטת החלטת הנאותות).

38 [Trade And Cooperation Agreement Between The European Union And The European Atomic Energy Community, Of The One Part, And The United Kingdom Of Great Britain And Northern Ireland, Of The Other Part](#), OJ L 444, 31.12.2020, Article FINPROV.10A, p. 14–1462.

39 ס' 1 לטיוטת החלטת הנאותות.

40 ראו פס' 7-111 למבוא לטיוטת החלטת הנאותות. לתיאור של הצעת החוק הבריטי בדבר הגנת מידע, ראו כהנא ושני, לעיל ה"ש 4, בעמ' 135–138.

41 ראו פס' 116–130 למבוא לטיוטת החלטת הנאותות.

42 שם, בפס' 131–171.

43 שם, בפס' 172–265.

44 [Investigatory Powers Act 2016](#), c.25 (Eng.) (להלן: חוק סמכויות חקירה הבריטי).

45 כהנא ושני, לעיל ה"ש 4, בעמ' 144–150.

46 שם, בעמ' 163–165.

47 שם, בעמ' 150–154.

תקשורת לשמור נתוני תקשורת,⁴⁸ סמכויות סייבר התקפי,⁴⁹ וסמכויות לתפוס נתוני תקשורת באופן גורף (bulk acquisition warrant).⁵⁰ החלטת הנאותות בוחנת כל אחת מהסמכויות האלו, ובכלל זה את הבקורות הסטטוטוריות על הפעלתן,⁵¹ מנגנוני הפיקוח המתאימים ואת הסעדים בגין פגיעתן בזכויות.⁵²

בהתייחסה לסמכויות סוכנויות המודיעין והביטחון הבריטיות לתפוס נתוני תקשורת באופן גורף (bulk acquisition), טיטת החלטת הנאותות קובעת כי סמכויות אלו "אינן נוגעות בדרך כלל למידע פרטי של מושאי מידע אירופאיים המועבר לבריטניה מכוח החלטה זו".⁵³ גישת הטיטה היא כי החובה להעביר נתוני תקשורת תחת חוק סמכויות חקירה הבריטי נוגעת למידע שנאסף על ידי ספקי תקשורת בבריטניה ישירות מלקוחותיהם, ולכן אינו נוגע להחלטת הנאותות שעיקרה בהעברת מידע מהאיחוד האירופי לצד שלישי.⁵⁴ משכך, גם פרקטיקת האיסוף הגורף נתוני תקשורת מבעלי רישיון בזק על ידי השב"כ, והשימוש במאגר "הכלי" מזה שני עשורים, אינם רלוונטיים לעניין החלטת הנאותות ביחס לדין הישראלי.

אפשר שהחלטת הנאותות הבריטית, אם תתקבל בנוסח המוצע, תיתקף בבית הדין האירופי, בדומה לאופן שבו נתקפו הסדרי העברת המידע בין האיחוד לאירופה בעניין *Schrems I* ובעניין *Schrems 2*.⁵⁵ עם זאת, במוקד ההחלטות האלו עמדו פרקטיקות איסוף גורף של נתוני תוכן (תוכנית PRISM של הסוכנות לביטחון לאומי (NSA) האמריקנית) מכוח סעיף 702 של חוק איסוף מודיעין זר (FISA),⁵⁶ להבדיל מאיסוף גורף של נתוני תקשורת פנים ארציים (דוגמת תוכנית 215 האמריקנית).⁵⁷ עם זאת, יש לזכור כי מדובר בטיטה, שנוסחה עשוי להשתנות בחודשים הקרובים, וכבר עתה יש המבקרים אותה.⁵⁸ יתר על כן, הסמכויות הסטטוטוריות לתפיסה גורפת של נתוני תקשורת בבריטניה אינן מעוגנות בסעיף בודד בחקיקה, דוגמת סעיף

- 48 שם, בעמ' 154–156.
- 49 שם, בעמ' 156–162 ו-166–171.
- 50 שם, בעמ' 166–168.
- 51 ראו, למשל, את הוראות 2 לחוק סמכויות חקירה הבריטי; וכן כהנא ושני, שם, בעמ' 143.
- 52 ראו בהרחבה כהנא ושני, לעיל ה"ש 11, בעמ' 120–136.
- 53 ראו פס' 225 למבוא לטיטת החלטת הנאותות (התרגום שלי, ע"כ).
- 54 שם. ה"ש 393 לטיטת החלטת הנאותות מפנה גם לס' 261 לחוק סמכויות חקירה הבריטי, המגדיר שירות תקשורת כבעל זיקה לבריטניה. השוו עם הגדרות בעל רישיון בזק לפי ס' 1 ו-13 לחוק הבזק.
- 55 לעיל ה"ש 3.
- 56 50 U.S.C. §§ 1881–1881a. לסקירה של המסגרת הנורמטיבית שמכוחה הוסמכה PRISM טרם תיקוני חוק החירות (USA Freedom Act), ראו Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117 (2015). ראו גם כהנא ושני, לעיל ה"ש 4, בעמ' 89.
- 57 על תוכנית 215 ראו כהנא ושני, לעיל ה"ש 11, בעמ' 13–17. כן ראו Casey J. McGowan, *The Relevance of Relevance: Section 215 of the USA Patriot Act and the NSA Metadata Collection Program*, 82 FORDHAM L. REV. 2399 (2014); Susan Landau & Asaf Lubin, *Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?*, 11 HARV. NAT'L SEC. J. 308, 313–317 (2020); Bart Forsyth, *Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection*, 72 WASH. & LEE L. REV. 1307, 1309–1315 (2015); *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (2014).
- 58 ראו, למשל, Douwe Korff, *The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK* (3.3.2021). עם זאת, חרף הביקורת של Korff על טיטת החלטת הנאותות, אין הוא מוצא פסול בהחלטה של תפיסה גורפת של נתוני תקשורת ממנה (שם, בפס' 255 לטיטה).

11 לחוק השב"כ, אלא בדבר חקיקה ארוך ומפורט, שעמו מפורסמים כללים פנימיים של סוכנויות המודעין ואכיפת החוק (codes of practice),⁵⁹ ושביישומו מעורבים מספר גופי פיקוח. טיוטת החלת הנאותות המשיכה, "לשם השלמת התמונה" לתאר את ההוראות החלות ביחס לתפיסה גורפת של נתוני תקשורת,⁶⁰ וייתכן שבראיה הוליסטית של משטר הגנת הפרטיות בבריטניה, הוראות אלו מאפשרות לנציבות לקבוע ביתר קלות כי פרקטיקה זו אינה נוגעת להחלטת הנאותות.

אם כן, חרף הרוחות הנושבות מפסיקת בית הדין האירופי, ישנם סימנים לפיהם "הכלי", אותו מטאטא שגורף את כל נתוני התקשורת בישראל, לא ימצא במוקד החלטת הנאותות האירופית. עם זאת, יש לזכור כי ההחלטה אינה תלויה אך ורק בנכונות של הנציבות האירופית להכיל את "הכלי", אלא במשטר הגנת הפרטיות הישראלי כולו, הנשען על חקיקה שמרביתה שייך לעידן טכנולוגי אחר,⁶¹ שטרם עברה רענון מהותי (להבדיל מהדין הבריטי) נוכח כניסתן לתוקף של תקנות הגנת המידע הכלליות (GDPR).

בין אם תקבל החלטת הנאותות האירופית ביחס למשטר הגנת המידע הישראלי חרף "הכלי" ובין אם דווקא האיסוף הגורף של נתוני תקשורת על ידי השב"כ יהא זה שיכשיל אותה, רצוי לתת את הדעת על כך שהתמריצים הכלכליים של החלטת הנאותות האירופית אינם הנימוק היחיד בעד בדיקה מחודשת ושינוי של דיני המעקב המקוון בישראל. הזכות לפרטיות בישראל היא זכות חוקתית המעוגנת בחוק-יסוד: כבוד האדם וחירותו, ופגיעה בה צריכה להיות מידתית.⁶² שאלת מידתיות הפגיעה של מאגר נתונים הפועל במחשכים מזה עשרים שנה ושואב לתוכו את כל נתוני התקשורת מבעלי רישיון בוק בישראל טרם נבחנה על ידי בית המשפט העליון ואולם ספק אם ההסדר הנוכחי עונה על אמות מידה המקובלות במשפט המשווה,⁶³ בכל הנוגע לרמת הפירוט של הדין, הבקורות הסטטוטוריות, השקיפות, ומנגנוני הפיקוח החלים עליו.

59 ראו, לדוגמה, [Code of Practice on Bulk Acquisition of Communications Data](#), Home Office (2018).

60 ראו פס' 226–232 למבוא לטיוטת החלטת הנאותות.

61 ראו ארידור הרשקוביץ ושוורץ אלטשולר, לעיל ה"ש 30, בעמ' 7–8.

62 ס' 7 לחוק-יסוד: כבוד האדם וחירותו. כן ראו לאחרונה את בג"ץ 6732/20 [האגודה לזכויות האזרח בישראל נ' הכנסת](#), פס' 8 לפסק דינו של המשנה לנשיאה מלצר, פס' 9–15 לפסק דינה של השופטת ברק-ארז ופס' 6 לפסק דינו של השופט הנדל (פורסם באר"ש, 1.3.2021).

63 נוסף על פסיקת בית הדין האירופי שהובאה לעיל, ניתן להפיק תובנות גם מהלכת בית הדין האירופי לזכויות אדם (ECtHR), ובפרט ראו *Zakharov v. Russia*, No. 47143/06, EUR. CT. H.R. (2015); *Sazbo & Vissy v. Hungary*, No. 37138/14, EUR. CT. H.R. (2016); *Liberty & others v. The United Kingdom* No. 58243/00 EUR. CT. H.R. (2008); *Weber & Saravia v. Germany*, No.54934/00 EUR. CT. H.R. (2006); *Centrum för Rättvisa v. Sweden*, No. 35252.08, EUR. CT. H.R. (2018); *Big Brother Watch & others v. The United Kingdom* Nos. 58170/13, 62322/14 and 24960/15 EUR. CT. H.R. (2018).