רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה

מהם הדינים החלים בישראל על רשויות המדינה כשהן בולשות אחרי הפעילות המקוונת שלנו; האם דינים אלו נותנים מענה ראוי להתפתחויות הטכנולוגיות של השנים האחרונות; האם הפרטיות שלנו מוגנת די הצורך; והאם ישנן תובנות עדכניות בדין הזר שרצוי לתת עליהן את הדעת?

עמיר כהנא בשיתוף עם יובל שני

המכון הישראלי לדמוקרטיה

מרכז המחקר להגנת הסייבר
CYBER SECURITY RESEARCH CENTER

European Research Council

מחקר מדיניות 123

המכון הישראלי לדמוקרטיה

מרכז המחקר להגנת הסייבר

European Research Council

מחקר מדיניות 123

רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה

עמיר כהנא

בשיתוף עם יובל שני

ינואר 2019

Regulation of Online Surveillance in Israeli Law and Comparative Law
Amir Cahane
with Yuval Shany

עריכת הטקסט: יהודית ידלין, קרן גליקליך
עיצוב הסדרה והעטיפה: סטודיו תמר בר־דיין
ביצוע גרפי: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים

מסת"ב: 978-965-519-247-6

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר — כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו"ל.

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר) ולתוכנית המחקר להגנת הסייבר, הפקולטה למשפטים, האוניברסיטה העברית בירושלים
נדפס בישראל, 2019

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888, פקס: 02-5300867
דוא"ל: orders@idi.org.il
אתר האינטרנט: www.idi.org.il

מרכז פדרמן לחקר הסייבר – תכנית משפט וסייבר, האוניברסיטה העברית בירושלים
הפקולטה למשפטים, קמפוס הר הצופים
תא 80, מיקוד 9190501
דוא"ל: hcsrcl@mail.huji.ac.il
אתר האינטרנט: https://csrcl.huji.ac.il

הדברים המובאים במחקר מדיניות זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה או את עמדת מרכז פדרמן לחקר הסייבר.

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס״ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

מרכז פדרמן לחקר הסייבר – תוכנית משפט וסייבר

תוכנית משפט וסייבר פועלת כחלק ממרכז פדרמן לחקר הסייבר באוניברסיטה העברית בירושלים ומתמקדת ב־cyber security (ביטחון המרחב הקיברנטי) מפרספקטיבה משפטית וקרימינולוגית. החוקרים בתוכנית עוסקים במגוון נושאים ותחומים, בהם: רגולציה, אחריות משפטית, מניעת פשיעה, זכויות אדם ודיני מלחמה. התוכנית פועלת לייצר ידע ולכונן שיתופי פעולה בין חוקרים, ארגונים העוסקים בזכויות אדם, גופי ממשל ותעשייה. יתר על כן, כיוון שאנו מצויים בעידן של פיתוח רגולציות ומיסוד קודים להתנהגות במרחב הסייבר ואף שותפים לעיצוב הנורמות והפרקטיקות הנוהגות הללו, חוקרי התוכנית והמרכז רואים חשיבות בתרומה להתפתחותו של שיח ציבורי בנושא ביטחון המרחב הקיברנטי בצד השיח האקדמי.

מחקר זה נעשה במסגרת הפרויקט ״מידתיות במדיניות ציבורית״ שהתקיים במכון הישראלי לדמוקרטיה בשנים 2015–2019. המחקר נתמך חלקית על ידי מענק (מס׳ 324182) של המועצה האירופית למחקר – ERC (European Research Council).

תוכן העניינים

תקציר 9

פרק 1. מבוא: שיח הפרטיות ושיח הביטחון בישראל 17

פרק 2. מעקב אחר רשתות תקשורת בישראל: מסגרת נורמטיבית 23

2.1 הבחנות מקדימות 23

2.2 ישראל – מעטפת חוקתית 30

2.3 חוק הגנת הפרטיות 32

2.4 חוק נתוני תקשורת 34

2.5 חוק האזנת סתר 42

2.5.1 האיסור הכללי על האזנת סתר 42

2.5.2 האזנת סתר למטרת ביטחון המדינה 43

2.5.3 האזנת סתר למניעת עבריינות ולגילויה 45

2.5.4 האזנות סתר שאינן טעונות היתר 48

2.5.5 מחיקה וביעור של חומר האזנה 50

2.5.6 קבילות ראיות שהושגו בהאזנת סתר אסורה 51

2.6 חוק השב"כ 52

פרק 3. מעקב אחר רשתות תקשורת: דין השוואתי 54

3.1 ארצות הברית 54

3.1.1 הבחנות מקדימות 55

3.1.2 מעטפת חוקתית 61

3.1.3 חוק פרטיות בתקשורת אלקטרונית (ECPA) 67

3.1.4 חוק סיוע תקשורתי לרשויות אכיפה (CALEA) 79

3.1.5 חוק איסוף מודיעין זר (FISA) 81

3.1.6 חוק איסוף מודיעין זר (FISA) ואיסוף נתוני תקשורת 85

3.1.7 איסוף מודיעין על מטרות שמחוץ לארצות הברית 89

3.2 האיחוד האירופי 96
3.2.1 הערות מקדימות 97
3.2.2 הרמה החוקתית: הזכות לפרטיות מכוח אמנות האיחוד 100
3.2.3 המשטר האירופי להגנת המידע: דירקטיבת הגנת המידע (דירקטיבה 95/46/EC) והתקנות הכלליות בדבר הגנת מידע (GDPR) 104
3.2.4 דירקטיבת הפרטיות האלקטרונית (e-Privacy Directive) ודירקטיבת שימור הנתונים (Data Retention Directive) 114
3.2.5 עם הפנים לעתיד – משטר הגנת המידע החדש: התקנות הכלליות בדבר הגנת מידע (GDPR) ודירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) 118
3.3 בריטניה 131
3.3.1 מעטפת חוקתית 131
3.3.2 חוק הגנת מידע 1998 (DPA) 132
3.3.3 הצעת חוק הגנת מידע (DPB - Data Protection Bill) 135
3.3.4 חוק סמכויות חקירה 2016 (IPA) 138
3.4 גרמניה 187
3.4.1 מעטפת חוקתית 187
3.4.2 החוק הפדרלי להגנת מידע (BDSG) 195
3.4.3 דיני מעקב מקוון 199
3.5 הודו 215
3.5.1 מעטפת חוקתית ופרטיות יצירת הפסיקה 217
3.5.2 פרטיות והגנת מידע בחקיקה 219
3.5.3 מעקב אחר רשתות תקשורת בהודו: פרקטיקה 228

פרק 4. מעקב אחר רשתות תקשורת: הסדרת סוגיות קונקרטיות בדין המשווה 233
4.1 מעקב מקוון: תחולה טריטוריאליות ופרסונלית 233
4.2 זליגת מודיעין (intelligence creep) 239
4.3 הצפנה 243
4.4 שימור נתונים (data retention) 248
4.4.1 דרישה לשימור נתונים מבעל המאגר 249
4.4.2 שימור נתונים בגופי החקירה והביטחון 253

4.5 גישה לנתוני תקשורת ולנתוני תוכן 257
4.6 כריית מידע 261
4.7 שיתוף פעולה מודיעיני עם סוכנויות זרות 267

פרק 5. מדיניות 274
5.1 סוגיות שאינן מוסדרות בדיני המעקב המקוון בישראל 274
5.2 כללים חשאיים והיעדר שקיפות 280
5.3 בקרה והגנה על זכויות 281
5.3.1 ביקורת שיפוטית 281
5.3.2 רשות פיקוח עצמאית 287
5.3.3 ביקורת פרלמנטרית וציבורית 291
5.4 אסדרה מידתית של מעקב מקוון 292

Abstract iii

תקציר

בשנת 2013 חשף אדוארד סנודן, שהועסק אצל קבלן משנה בסוכנות לביטחון לאומי (NSA), מסמכים אשר תיארו את היקף המעקב המקוון ברשתות תקשורת שמנהלות סוכנויות הביון האמריקניות, בין השאר אחר אזרחי ארצות הברית. חשיפה זו הובילה לדיון ציבורי בנושא פרקטיקות המעקב של סוכנויות הביון האמריקניות, ובעקבותיו נערכו כמה רפורמות סטטוטוריות. חשיפת שיתוף הפעולה של הסוכנות לביטחון לאומי עם ארגונים־עמיתים זרים פתחה את הפתח לדיונים דומים במדינות אחרות על היקף שיתוף הפעולה הרצוי עם סוכנויות מודיעין זרות ועל שיטות האיסוף המקוונות של סוכנויות הביון הלאומיות.

מעקב מקוון (online surveillance), או מעקב אחר רשתות תקשורת, הוא פעילות מודיעינית שנועדה לאסוף מידע דיגיטלי שמקורו ברשתות תקשורת אלקטרונית, לשמרו, לעבדו ולנתחו – בין שהמידע מועבר באמצעות רשת טלפוניה קווית, בין בתקשורת סלולרית ובין בתקשורת מחשבים. המעקב יכול להתבצע במגוון דרכים, לרבות "יירוט" או "שליפה" של מידע מהרשת או ממכשירי קצה, איסוף נתוני תקשורת מספקי התקשורת ועיבוד מידע גלוי וסמוי, כולל טכניקות של כריית מידע או למידת מכונה. בתקופה שבה חלק ניכר מהתקשורת האנושית נעשה בתווך האלקטרוני, רתימת הטכנולוגיה המודרנית לאיסוף רחב היקף, לאגירה ולניתוח סטטיסטי רב־עוצמה של נתוני תקשורת יכולה להניב מודיעין עשיר ומפורט על מושאי המעקב יותר מאי פעם.

אלא שלצד יתרונותיו של מודיעין שמקורו במעקב מקוון ברשתות תקשורת יש להביא בחשבון גם את הפגיעה הניכרת בפרטיותם של מושאיו. במעגל הנפגעים נמצאים לא רק היעדים המודיעיניים שפרטיותם מופרת אלא גם אותם אנשים הבאים עימם במגע. יתר על כן, כאשר מופעלות שיטות של איסוף גורף (bulk collection), השואבות כמות עצומה של נתוני תקשורת ותוכן מעורק תקשורת מרכזי בלי לצמצם אותו ליעד מודיעיני מסוים, מעגל הנפגעים גדל דרמטית. הפגיעה בפרט בשל מעקב מקוון אינה מוגבלת לפגיעה בזכות לפרטיות. גם תחושת החירות הכללית עלולה להיפגם וחופש הביטוי להצטמצם בשל האפקט המצנן שמעקב שכזה מייצר. כאשר פלוני יודע שהוא במעקב, או אפשר שיהיה במעקב, הוא צפוי למשטר את התנהלותו בהתאם.

מופעים אחרים של מעקב מדינה טכנולוגי שתכליתם המוצהרת אינה התמודדות עם הטרור מעוררים דיון ער בציבוריות הישראלית. "חוק האח הגדול" וחוק המאגר הביומטרי זכו לדיון בתקשורת, ושניהם מצאו את דרכם לבית המשפט. לעומת זאת שיח על הכללים המסדירים את המעקב המקוון לתכליות ביטחוניות כמעט שאינו קיים, ובייחוד חסר שיח המציע בחינה של הדין הקיים ושל מידת התאמתו למציאות החברתית והטכנולוגית בת זמננו.

מסקנות עיקריות

1. אי־אסדרה של סוגיות מהותיות

בחינת הדינים הישראליים החלים על מעקב מקוון ברשתות תקשורת מעלה כי הדין הישראלי סובל מתת־אסדרה בשורת סוגיות שהדין המשווה נותן להן מענה. למשל, הדין הישראלי נעדר איסור כללי על פעילות של איסוף תקשורת גורף (bulk collection) שבצידו אסדרת מקרים יוצאי דופן שבהם אפשר שפעילות זו תותר, בכפוף לקריטריונים של מידתיות וצורך מוחלט. כמו כן, עדיין לא הוסדרה התחולה הטריטוריאלית של דיני המעקב המקוון הישראליים. יוצא שהשאלה בדבר המותר והאסור בתקשורת שמחוץ לתחומי מדינת ישראל, לרבות בשטחים מעבר לקו הירוק שבשליטת מדינת ישראל, עומדת בעינה.

נוסף על כך, אין בחוק הישראלי הסדרים להגבלת תקופת שימורה של תעבורת התקשורת (אם זה תוכן התקשורת עצמה ואם נתוני תקשורת, metadata,

שהם מידע הקשור בתקשורת שאינו התוכן שלה, אך יש בו ללמד, בין השאר, על הצדדים לתקשורת, על מיקומה ועל הזמנים שבהם נתקיימה) מטעם ספקיות התקשורת, כפי שניתן למצוא בדיני האיחוד האירופי ובדין הבריטי והגרמני.

גם באשר לפעילות של כריית מידע בהקשר הנידון – הפעלת טכניקות סטטיסטיות על מאגרי מידע שהושגו באמצעות מעקב מקוון, לרבות הצלבתם עם מאגרי מידע ממשלתיים אחרים – כמעט שאין בחוק הישראלי התייחסות כפי שיש בדין הזר. (במקרים מסוימים הדין האירופי מגביל קבלת החלטות המתבססת על נתונים שמקורם בפעילויות עיבוד מידע אוטומטיות ללא יכולת התערבות אנושית, גם בהקשרים של אכיפת חוק.)

נראה כי בדין הישראלי טרם נבחנה ההסמכה לאיסוף מודיעין גלוי (אוסינט; OSINT) ברשתות תקשורת. מודיעין גלוי מסורתי, אשר נשען על מקורות תקשורת המוניים גלויים, מטבעו ומטיבו אינו נדרש כלל להסמכה. אולם מודיעין גלוי שנוסף על מקורותיו אלה משתמש גם בפרסומים פומביים ברשתות חברתיות אפשר שיידרש להסמכה בחוק. מעקב המוני אחר פעילות אינדיווידואלית גלויה של משתמשים ברשתות חברתיות, לרבות ניתוחו באמצעים ממוכנים, עלול להביא לפגיעה של ממש בפרטיות. הגם שגופים פרטיים מפעילים פרקטיקות דומות למטרות מסחריות, הכוח העדיף של המדינה עלול גם לגרום פגיעה חריפה יותר בפרטיות וגם להביא להשלכות מעשיות חמורות יותר לתוצרי המודיעין הגלוי.

2. כללים חשאיים והיעדר שקיפות

אשר לפעילות המעקב ששירות הביטחון הכללי (שב"כ) מבצע ברשתות תקשורת – החקיקה הקיימת מאפשרת לממשלה מרחב שיקול דעת בקביעת הכללים המסדירים אותה ואת ההוראות הניתנות לבעלי רישיון בזק (רישיון למתן שירותי תקשורת, בכלל זה שירותי טלפוניה, אינטרנט וסלולר) בעניין סיוע לכוחות הביטחון (גם משטרת ישראל). כללים אלו, וגם חלק מהביקורת הפרלמנטרית והמינהלית עליהם ועל פעילות המעקב ברשתות התקשורת, הם חשאיים.

אומנם בחשאיות זו יש כדי לאפשר גמישות פרשנית והתאמת הדין לצורכי השעה ולצרכים המבצעיים הדוחקים, אלא שפרשנות גמישה וחשאית, שסבירותה אינה עומדת למבחן הציבור, עלולה להוביל לפריצת גדרות.

3. ביקורת שיפוטית חלקית

הפרישׂה בישראל של ביקורת שיפוטית על היתרים שונים למעקבים מקוונים היא חלקית. החוק פוטר את רשויות הביטחון המבקשות צו האזנת סתר מפנייה לבית המשפט ומסתפק בהיתר למפרע מאת השר, ובמקרים דחופים — די בהיתר בדיעבד ובתנאי שהפעלת סמכויות אלו מדוּוחת ליועץ המשפטי לממשלה. במקרים דחופים גם היתר להאזנות סתר למטרת מניעת עבירות וגילוי עבריינים אינו טעון צו שיפוטי אלא אם כן נדרשת הארכתו. חוק האזנת סתר פוטר סוגים מסוימים של האזנות מדרישה להיתר כלשהו, ואפשר שיש בהם גם ההסדר החוקי המאשר איסוף מידע גלוי ברשת, לרבות מרשתות חברתיות.

ביקורת שיפוטית בישראל על השגת נתוני תקשורת ואיסופם מוגבלת למקרים שאינם דחופים, שבהם המשטרה נדרשת לנתוני תקשורת למטרות חקירה ואכיפת חוק. אין כל הוראה האוסרת על המשטרה להשתמש בטכנולוגיות של איסוף נתוני תקשורת שאינן כרוכות בפנייה לבעלי רישיון בזק. אין כל דרישה לצו שיפוטי המתיר פעילות של איסוף נתוני תקשורת (על דרך של יירוט עצמאי, גישה מקוונת או בקשה עיתית) שעושה שירות הביטחון הכללי. יתר על כן, ניתן לפרש את לשון החוק כך שהוא אינו מתנה כלל את האיסוף של נתוני תקשורת בהיתר (מאת ראש השירות) אלא רק בעצם השימוש במידע.

הגם שסקירת הדין המשווה מעלה כי גם במדינות אחרות אין ביקורת שיפוטית גורפת על פרקטיקות של מעקב מקוון, נראה כי היא רחבה מזו המקובלת בישראל. למשל, גם בגרמניה וגם בארצות הברית פעילות איסוף של נתוני תוכן ותקשורת למטרות מניעת פשע ואכיפת חוק כפופות על פי רוב לביקורת שיפוטית. כמו כן בשתי המדינות יש הסדרים לבחינה שיפוטית או מעין־שיפוטית של היתרים להאזנות סתר לתכליות ביטחוניות.

עם זאת ביקורת שיפוטית אינה חזות הכול. בחינה אמפירית של נתוני הבקשות של משטרת ישראל לקבלת צווים מכוח חוק האזנת סתר וחוק נתוני תקשורת מלמדת כי שיעור הבקשות שנדחו בבית המשפט נמוך מ־0.5% לאורך כל התקופה המדווחת. תמונה דומה של שיעור דחייה נמוך עולה גם מדיווחי מינהלת בתי המשפט בארצות הברית בעניין בקשות להאזנות סתר למטרות אכיפת החוק ומניעת פשיעה. יש להיזהר מלהסיק מממצאים אלו כי מנגנון ביקורת שיפוטי אפריורי על האזנות סתר הוא לכאורה לא יותר מחותמת גומי, שכן בית המשפט

רשאי לאשר בקשות בכפוף לסייגים ולהקשחת הנהלים שבצו המבוקש. כמו כן הביקורת השיפוטית עצמה יכולה לייצר תמריצים לסינון בקשות לא ראויות מצד גופי החקירה עוד טרם הגשתם לבית המשפט. עם זאת, מספר המקרים הזעום שבית המשפט דוחה בקשות להאזנת סתר או למעקב מקוון מציב סימן שאלה על יעילות הביקורת השיפוטית ומצדיק את בחינת הצורך ביצירת ערובות נוספות. בדין המשווה ניתן למצוא מנגנונים המתמודדים עם החשש שביקורת שיפוטית על צווי האזנת סתר תהפוך למכנית או תיטה לתמוך בשיטתיות בעמדת רשויות החקירה. בדין הבריטי למשל יש הוראות המבנות את שיקול הדעת השיפוטי במפורט, ובדין האמריקאי קיים מתווה שמסתייע בידיד בית המשפט — אדם חיצוני בלתי תלוי שהופך את הליך בקשת הצו, שנעשה ברגיל במעמד צד אחד, להליך אדוורסרי יותר.

4. רשות פיקוח עצמאית ופיקוח פרלמנטרי

הביקורת השיפוטית והמעין־שיפוטית על פעילות של מעקב אחר רשתות תקשורת היא ריאקטיבית, והתגובה שלה מוגבלת לבקשות או לצווים קונקרטיים. ביקורת כזו אינה מטפלת במקרים שהרשויות נמנעו בהם מלבקש צווים מתאימים בגלל היעדר חובה חוקית לעשות כן או בשל פרשנות מצמצמת של החובה הקיימת. אשר על כן, שיטות משפט מסוימות הסמיכו רשויות מינהלתיות או מעין־שיפוטיות לפקח בעצמן על פעילות המעקב המקוון של גופי הביטחון.

בישראל רשות ההגנה על הפרטיות (לשעבר רמו״ט – הרשות למשפט וטכנולוגיה) היא הגוף המסדיר, המפקח והאוכף על פי חוק הגנת הפרטיות, חוק שירות נתוני אשראי וחוק חתימה אלקטרונית. עם זאת בשל הפטורים שבחוק הגנת הפרטיות אין הרשות מפקחת הלכה למעשה על פעילות מעקב מקוון של רשויות הביטחון ואכיפת החוק.

אפשר שהקמת גוף מפקח עצמאי או הרחבת סמכויותיה של רשות ההגנה על הפרטיות, כדי שזו תוכל לפקח על התקינות של פעולות עיבוד הנתונים — ובכלל זה איסוף ושימור — הנעשות במסגרת מעקב אחר רשתות תקשורת לתכליות ביטחוניות או משטרתיות, תכניס שחקן נוסף שישמור על האינטרס לפרטיות של מושאי המידע. רצוי שיהיה זה גוף, שנוסף על עצמאותו יהיו לו גם מלוא

סמכויות הפיקוח הנדרשות למילוי תפקידיו, כגון סמכויות חקירה בעקבות תלונות או ביוזמתו שלו וסמכויות ייעוץ והנחיה מקצועית בנוגע להיבטי הגנת פרטיות באסדרה רלוונטית. לצד סמכויות חקירה ובירור יש להעניק לו את היכולת להגיע להכרעה בעלת השלכות מעשיות על הפרקטיקות הנבדקות.

היקפה של הביקורת הפרלמנטרית של הכנסת על פרקטיקות המעקב המקוון של המשטרה ושירות הביטחון הכללי מוגבל לדיווחים סטטוטוריים לפי חוק האזנת סתר, שחלקם נעשה בדלתיים סגורות. דיווחים דומים לפי חוק נתוני תקשורת נעשו לתקופה מוגבלת מכוח הוראת שעה בחוק, שתוקפה פג. ניסיון להשיג את הדיווחים החשאיים באמצעות בקשה לפי חוק חופש המידע נדחה בבית המשפט העליון, שבהערת אגב המליץ על גילוי וולונטרי של פרטים אלה, למען אמון הציבור, לפני שאלו יודלפו.

המלצות

1. סוגיות החסרות אסדרה בדין הישראלי

(1) **היקף הסמכויות של כל אחד מגופי הביטחון ואכיפת החוק.** באסדרת היקף הסמכויות השונות של המשטרה, שירות הביטחון הכללי, אמ"ן, המוסד לתפקידים מיוחדים וגופי חקירה אחרים יש להתייחס לפרקטיקות המותרות להם, להיקף האיסוף המותר, לבקרות המופעלות עליהן ולשאלת התחולה הטריטוריאלית של סמכויות אלו.

(2) **איסוף גורף (bulk collection).** יש להחיל בדין הישראלי איסור כללי על איסוף גורף אלא אם יש צורך מוחלט בו לשם הגשמת תכליות צרות ומפורטות, ובכפוף לנהלים המבטיחים את צמצום הפגיעה בזכויות למינימום האפשרי.

(3) **שימור נתונים (data retention).** יש להחיל בדין הישראלי הוראות באשר לתקופת שימור הנתונים המרבית של ספקי שירותי בזק. יכולתן של הרשויות להורות לספקים לחרוג מתקופה זו ולשמור נתונים לפרק זמן ארוך יותר תהיה בכפוף לצו שיפוטי, לשם הגשמת תכליות צרות ומפורטות, ובכפוף לנהלים המבטיחים את צמצום הפגיעה בזכויות למינימום האפשרי.

(**4**) **כריית מידע (כר"מ) ואיסוף מודיעין גלוי (OSINT).** יש להסדיר את המותר והאסור בדין בכל מה שקשור להצלבת מאגרי נתונים שונים, לשימושים השונים שניתן לעשות בתוצרים של עיבודים סטטיסטיים ושל מידת המיכון והיעדר ההתערבות האנושית בתהליך. באשר לפרקטיקות של מודיעין גלוי (אוסינט) ברשתות חברתיות – יש להגדיר את סמכותן של הרשויות לפעול בזירה זו ולהגביל פרקטיקות איסוף שאינן פסיביות לחלוטין (כמו שימוש בפרופילים פיקטיביים על מנת להשיג גישה למידע שאינו פומבי לגמרי).

(**5**) **השגת מידע מספקי פלטפורמות תקשורת גלובליות.** יש להסדיר בדין את הנהלים להשגת מידע מספקי פלטפורמות תקשורת מקוונים, דוגמת פייסבוק וגוגל, ולהכפיפן לתכליות צרות של פשע חמור ושל ביטחון לאומי, לפי מבחן של ודאות קרובה, ולביקורת שיפוטית.

(**6**) **יירוט נתוני תקשורת.** בדומה לאיסור הכללי על האזנת סתר, יש להחיל איסור כללי על יירוט פעיל של נתוני תקשורת (שלא כמו השגתם דרך חוק נתוני תקשורת או לפי הכללים מכוח חוק השב"כ) ולהסדיר את המקרים שבהם יירוט כאמור יותר, בדומה למתווה של חוק האזנת סתר.

2. הגברת השקיפות

(**1**) יש להסיר את מעטה החשאיות מעל הכללים המסדירים את הדרכים ששירות הביטחון הכללי משיג נתוני תקשורת מספקי התקשורת ולפרסם בציבור הרחב את הדיווחים השנתיים על השימוש בהם וכן לדיווחים השנתיים על היקף השימוש של השב"כ בסמכויותיו לפי חוק האזנת סתר.

3. הרחבת הביקורת השיפוטית על פרקטיקות של מעקב מקוון

(**1**) יש להרחיב את היקף הביקורת השיפוטית על מעקב מדינה מקוון גם להאזנות סתר שמבצעים שירות הביטחון הכללי ואמ"ן לתכליות ביטחוניות, ולכל בקשה של נתוני תקשורת, בכלל זה בקשות דחופות.

(**2**) יש לחזק את מנגנון הביקורת השיפוטית הקיים. ניתן להבנות את שיקול הדעת השיפוטי במתן צווים באמצעות הוראות לבחינת חלופות שפגיעתן

בפרטיות קטנה יותר ולבחינת נוהלי צמצום שנועדו להבטיח כי לא ייעשה שימוש במידע למעלה מן הנדרש.

(**3**) אפשר לעצב הליך אדוורסרי שבמסגרתו יתאפשר לנציגי ציבור, לפרקליטים מיוחדים או לידידי בית המשפט להגן על אינטרסים של פרטיות הציבור ושל פרטיות היעד המודיעיני. חיזוק היסוד האדוורסרי בהליך אפשר שייעשה גם באמצעות מתן זכות עמידה לספקי תקשורת בהליך ובהכרה בזכות היידוע של מושאי המעקב ושל צדדים שלישיים גם כזכות יחסית הכפופה לשיקולי ביטחון אשר תאפשר תביעות נזיקיות לאחר מעשה.

4. רשות פיקוח עצמאית

(**1**) יש להקים גוף פיקוח עצמאי שיבקר את פעילות המעקב המקוון השוטפת של רשויות המדינה, שיבחן את הציות להוראות שבצווים ושייעץ וינחה מקצועית באשר להיבטי הגנת פרטיות באסדרה רלוונטית.

(**2**) חלופה להקמת גוף זה היא הרחבת סמכויותיה של הרשות להגנה על הפרטיות (לשעבר רמו"ט) כדי שיוקנו לה סמכויות לפיקוח על הגנת הפרטיות בפעילויות מעקב מקוון של רשויות הביטחון ואכיפת החוק.

(**3**) חלופה נוספת היא ייסוד פונקציה של אומבודסמן לענייני פרטיות במעקב מקוון – גוף עצמאי, נטול פניות, בעל סמכויות ריאקטיביות לחקור תלונות, למצוא להן, בלא פורמליות, פתרונות, ולעיתים לתת פומבי לממצאיו אגב שמירת המתלוננים בסוד.

5. פיקוח פרלמנטרי

(**1**) יש להחיל על ראשי רשויות הביטחון חובת דיווח שנתית לוועדת החוקה, חוק ומשפט ולוועדת חוץ וביטחון של הכנסת על מספר האזנות הסתר שבוצעו למטרות ביטחון המדינה. רמת פירוט הדיווח צריכה להיות זהה לזו שבדיווח השנתי של המשרד לביטחון פנים על הפעלת סמכויות אלו במשטרת ישראל.

(**2**) יש להפוך את הוראת השעה שבחוק נתוני תקשורת לקבועה ולחייב את משטרת ישראל בדיווח שנתי על הפעלת סמכויותיה לפי חוק זה.

פרק 1

מבוא:
שיח הפרטיות
ושיח הביטחון בישראל

בחודש יוני 2013 התפוצצה פרשת סנודן. אדוארד סנודן — לשעבר עובד בסוכנות הביון המרכזית (CIA), שהועסק אצל קבלן משנה בסוכנות לביטחון לאומי (NSA) — חשף מסמכים שתיארו את היקף המעקב המקוון ברשתות תקשורת שמנהלות סוכנויות הביון של ארצות הברית, בין השאר אחר אזרחיה שלה, ואת היקף שיתוף הפעולה של הסוכנות לביטחון לאומי עם סוכנויות שכמותה בבריטניה (מטה התקשורת הממשלתי — ה־GCHQ), באוסטרליה (מינהל האותות האוסטרלי — ה־ASD) ובקנדה (המוסד לביטחון בתקשורת — CSEC).[1]

זו איננה החשיפה הראשונה של היקף הסיגינט (מודיעין אותות או SIGINT)[2] שארצות הברית אוספת על אזרחיה. באמצע שנות השבעים של המאה העשרים נחשפו תוכניות שהפעילה הסוכנות לביטחון לאומי (NSA) למעקב אחר תקשורת כזאת, והביאו לידי דיון ציבורי ופרלמנטרי.[3] גם בעקבות פרשת סנודן התעורר דיון ציבורי על פרקטיקות המעקב של הסוכנויות האמריקאיות, דיון שבסופו של דבר הביא לידי רפורמות סטטוטוריות. בעקבות חשיפת שיתוף

1 Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, The Guardian (11.6.2013); Tim Leslie & Mark Corcoran, *Explained: Australia's Involvement with the NSA, the US Spy Agency at Heart of Global Scandal*, Australian Broadcasting Corporation (19.11.2013); Julian Borger, *GCHQ and European Spy Agencies Worked Together on Mass Surveillance*, The Guardian (1.11.2013); Glenn Greenwald, Greg Weston & Ryan Gallagher, *Snowden Document Shows Canada Set Up Spy Posts for NSA*, Canadian Broadcasting Corporation (10.12.2013)

2 SIGINT, או Signal Intelligence, הוא מודיעין שמופק באמצעות יירוט אותות – אם אותות תקשורת (Communications Intelligence – COMINT) ואם אותות אלקטרוניים שלא למטרות תקשורת (Electronic Intelligence – ELINT).

3 מבצע SHAMROCK ומבצע MINARET, ראו Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J.L. & Pub. Pol'y 75 (2014)

הפעולה של הסוכנות לביטחון לאומי עם ארגונים־עמיתים זרים, התקיימו גם במדינות אחרות דיונים על היקף שיתוף הפעולה הרצוי עם סוכנויות מודיעין זרות ועל שיטות האיסוף המקוונות של סוכנויות הביון הלאומיות.[4] בעקבות פרשת סנודן ביטל בית הדין האירופי לצדק (ECJ) את הסדרי העברת המידע בין אירופה לארצות הברית.[5]

מעקב מקוון (online surveillance), או מעקב אחר רשתות תקשורת, הוא פעילות מודיעינית שנועדה לאסוף, לשמור, לעבד ולנתח מידע דיגיטלי שמקורו ברשתות תקשורת אלקטרונית ומועבר באמצעות רשת טלפוניה קווית, בתקשורת סלולרית או בתקשורת מחשבים. המעקב יכול להתבצע במגוון דרכים, בין היתר "יירוט" או "שליפה" של מידע מהרשת או ממכשירי קצה, איסוף נתוני תקשורת מספקי התקשורת ועיבוד מידע גלוי וסמוי, לרבות טכניקות של כריית מידע (כר"מ).[6] בתקופה שבה חלק ניכר מהתקשורת האנושית נעשה באמצעים אלקטרוניים, רתימת הטכנולוגיה המודרנית לאיסוף רחב היקף, לאגירה ולניתוח סטטיסטי רב עוצמה של נתוני תקשורת יכולה להניב מודיעין עשיר ומפורט על מושאי המעקב. כך למשל המודיעין שאפשר להפיק באמצעות איסוף מידע מקוון — נתונים שנאספו במרשתת — וניתוחו הממוכן יכולים לייצר הבחנות דקות שבאמצעותן אפשר לחזות פיגועי טרור במתווה של "זאב בודד".[7]

4 ראו לדוגמה Jens Branum & Jonathan Charteris-Black, *The Edward Snowden Affair: A Corpus Study of the British Press*, 9 Discourse & Communication 199 (2015); Stefan Heumann, *German Exceptionalism? The Debate About the German Foreign Intelligence Service (BND)*, in Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair 349 (Russell A. Miller, ed., 2017); Matthias Schulze, *Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal*, 13 Surveillance & Soc. 197 (2015)

5 ראו בחלק 3.2.3.2 **להלן**.

6 במסמך זה המושג כריית מידע (כר"מ) יתייחס הן לשיטות ממוכנות של איסוף מידע מקוון (parsing או scraping) והן לשיטות העיבוד של מידע כזה, לרבות הצלבתו עם בסיסי נתונים אחרים, מתודולוגיות סטטיסטיות, למידת מכונה או שיטות עיבוד רלוונטיות של נתוני עתק (big data).

7 אהוד יערי ציין כי ניטור פעילות מקוונת היה אחת מדרכי ההתמודדות העיקריות של ישראל עם אינתיפאדת היחידים. לדבריו, כבר בראשית ההתקוממות, באוקטובר 2015,

מעקב מקוון מסוג זה מחליף איסוף מידע ממקורות אנושיים (HUMINT)[8] ועיבוד בידי אנליסטים אנושיים, ומכפיל את עוצמתם עשרות מונים.

קשה לחלוק על תפקידם החיוני של מעקבים מקוונים בהגנה על האינטרס הציבורי של שמירה על הביטחון האישי והלאומי. בעידן שבו ארגוני הטרור ופעילי טרור מרבים להשתמש ברשת לא רק ככלי תעמולה והסתה ולגיוס כספים, אלא גם ככלי מבצעי ומודיעיני,[9] ראוי שגופי הביטחון ינטרו את הפעילות הזאת. זאת ועוד, אחדים מאמצעי המעקב המקוונים פולשניים פחות מהחלופות הפיזיות האפשריות — החל בהתקנת אמצעים אלקטרוניים בסביבתו הפיזית של היעד המודיעיני, עבור במעקב פיזי אחריו וכלה בגיוס סוכנים מסביבתו הקרובה.

אלא שלצד היתרונות של מודיעין המבוסס על רשתות תקשורת, יש להביא בחשבון את פגיעתו הנרחבת של המעקב המקוון בפרטיותם של היעדים — לא רק זו של היעדים המודיעיניים, אלא גם זו של האנשים הבאים עימם במגע. יתר על כן, כשמופעלות שיטות של איסוף גורף (bulk collection), השואבות כמות עצומה של נתוני תקשורת ותוכן מעורק תקשורת מרכזי, מעגל הנפגעים גדל במידה ניכרת. יש לציין כי הפגיעה בפרט בשל מעקב מקוון איננה מוגבלת לפגיעה בזכות לפרטיות. גם תחושת החירות הכללית (החוסה בכבוד האדם או בזכות לחירות) וחופש הביטוי יכולים להצטמצם בשל האפקט המצנן של קיום בתוך פנאופטיקון וירטואלי.[10] כשפלוני יודע שעוקבים אחריו, או שאולי עוקבים אחריו, הוא צפוי למשטר את התנהלותו בהתאם.

איישו את המחלקות הטכנולוגיות שליש מכוח האדם של שירות הביטחון הכללי, וכי לצד מעקב מודיעיני אחר פעילות גלויה ברשת, נקט שירות הביטחון הכללי גם טכניקות של פיצוח מסרים מוצפנים. ראו Ehud Yaari, *How Israel Catches Lone Wolves*, 12 The American Interest (10.01.2017)

8 HUMINT, או human intelligence, הוא מודיעין שמופק באמצעות קשרים בין־אישיים, הפעלת סוכנים, מרגלים ושימוש במקורות אנושיים אחרים.

9 ראו לדוגמה עמיר פוקס "טרור ופרטיות: הצעה לחשיבה מחודשת על הכלים להתמודדות עם פעילות טרור באינטרנט" **פרטיות בעידן של שינוי** 231, 247–254 (תהילה שוורץ־אלטשולר עורכת, 2012).

10 פנאופטיקון הוא דגם אדריכלי שהציע ג'רמי בנת'האם למתקנים שדורשים פיקוח על השוכנים בהם – בתי מאסר, בתי חרושת, בתי ספר וכדומה. מדובר במבנה דמוי טבעת, שבמרכזו מגדל. הטבעת עשויה תאים־תאים, ובהם שוכנים אסירים, פועלים או בני כל קבוצה אחרת שבשבילם הוקם הבניין. לכל תא חלון שפונה אל החלק הפנימי של הטבעת,

אינטרסים של מאבק בטרור והגנה על חיי אדם עשויים להצדיק במקרים רבים שימוש באמצעי מעקב מקוונים חרף הפגיעה בזכות לפרטיות ובחופש הביטוי. עם זה אל הפוטנציאל המודיעיני של המעקב המקוון פוזלות גם סוכנויות ממשלה נוספות, דוגמת סוכנויות אכיפת חוק החפצות ליישם טכניקות של שיטור מנבא (predictive policing),[11] ואף רשויות המס.[12] תופעה זו מכונה "זליגה מודיעינית" (intelligence creep) — מצב שבו נתונים שהושגו מתוך הגבלת זכויותיו וחירויותיו של הפרט בהצדקה של תכליות ראויות של מניעת טרור, מוצאים את דרכם למאגרי מידע של רשויות ממשלה אחרות, שלהן אין דבר וחצי דבר עם תכליות אלו. אפשר גם שנתונים אלו ידלפו החוצה ויגיעו לידי אנשים או גופים פרטיים, או שאדם בתוך הארגון הביטחוני ישתמש בהם לרעה.[13] דיון כזה ביתרונות ובחסרונות של המעקב המקוון, שמביא לידי תובנות באשר

וכך המפקחים, היושבים במגדל ומוסתרים מעיני השוכנים במתקן, יכולים לראות את הנעשה בתא. דיירי הפנאופטיקון אינם יודעים כלל מתי המפקחים מתבוננים בהם, אבל הם מודעים לאפשרות זו. פוקו מתאר את הפנאופטיקון כמכניזם של כוח שגורם לאסיר (או לפועל, לתלמיד או למשתמש בפייסבוק) להפנים את יחסי הכוחות וּלְמַשטר את התנהגותו בלי שהמפקח יידרש להפעיל אמצעי משמעת. ראו Jeremy Bentham, The Works of Jeremy Bentham, published under the Superintendence of his Executor, John Bowring Vol. 11 (1838–1843); מישל פוקו **לפקח ולהעניש** פרק 3 (דניאלה יואל מתרגמת, 2015); להרחבה ראו גם David Lyon, Theorizing Surveillance: the panopticon and beyond (David Lyon ed., 2006)

11 Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion* 62 Emory L. J. 259 (2012). לדוגמה של מעין־שיטור מנבא ראו לאחרונה את הכרזתה של חברת פייסבוק על שימוש באינטליגנציה מלאכותית כדי לחזות, או לזהות בזמן אמת, כוונות התאבדות של משתמשים בשירותיה. החברה ציינה כי הם מתחילים לפרוס את יישום הבינה המלאכותית לזיהוי כוונות אלו ברחבי העולם, למעט באיחוד האירופי. ייתכן שבשל ההגבלות החלות שם על עיבוד ממוכן של מידע פרטי (ראו בחלק 3.2 **להלן** ובפרק 3 ה"ש 263, 279, 291); Guy Rosen, *Getting our Community Help in Real Time*, Facebook Newsroom (27.11.2017)

12 Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solutions or the End of Privacy as We Know It?*, 19 Vand. J. Ent. & Tech. L. 814 (2017)

13 ראו למשל את דברי השופט גרוניס בעניין בג"ץ 8070/98 **האגודה לזכויות אזרח בישראל נ' משרד הפנים**, פד נח(4) 842, 856 (2004), המתייחס ל"חשש מפני כוחה העודף של המדינה, שתרכז בידה מידע רב לגבי אזרחים ותושבים ותעשה שימוש לרעה באותו המידע".

לעיצובן הרצוי של הרגולציה (האסדרה) והבקרות המשפטיות החלות עליו, פסח כמעט לחלוטין על הציבוריות הישראלית.

אחדות מהשאלות שנסקרו במדד הדמוקרטיה לשנת 2016 מעלות כי כאשר רוב הציבור הישראלי, בעיקר היהודי, צריך לברור אמצעים למניעת פיגועים במסגרת המאבק בטרור, הוא אינו מייחס משקל רב לשיקולי מוסר.[14] יתר על כן, נראה כי רובו רוחש אמון רב למדי לשירות הביטחון הכללי ולמשטרה, ולדעתו עליהם לחקור חשודים בטרור לפי שיקוליהם. הסקר אף מצא רוב קל לתומכים במתן חופש ביטוי למתבטאים נגד המדינה. גם לאחר פרשת סנודן הסכימו יותר ממחצית הנשאלים בסקר עם ההיגד ש"כדי לשמור על הביטחון מותר למדינה לעקוב אחרי מה שאזרחיה כותבים באינטרנט".[15] כשהדבר נוגע לשיקולי ביטחון ומאבק בטרור, נראה כי הציבור הישראלי, ובעיקר היהודי, נכון להסיג זכויות אזרחיות מפני אינטרסים אלה.[16]

חברות בין־לאומיות פרטיות כגון פייסבוק, גוגל, אמזון ומייקרוסופט אוספות מידע רב על המשתמשים בהן באמצעות השירותים המקוונים שהן מציעות. אגירת נתונים זו מעוררת מדי פעם דיון על הפגיעה בפרטיות שבצידה, או על כוחן המתעצם של חברות אלו. אין לבטל חששות אלו כלאחר יד, אך יש להבחין בין מעקב מקוון שמפעילים גופים פרטיים לתכליות מסחריות ובין מעקב מקוון שמפעילה המדינה.

המדינה נהנית לא רק מהמונופול על הפעלת הכוח (שיש בו כדי להעצים את כוחו הממשטר של הפנאופטיקון); בכפוף לאסדרה מתאימה, ליכולות טכנולוגיות ולשיתוף פעולה של הספקים הפרטיים, מקורות המידע של המדינה יכולים

14 תמר הרמן, אלה הלר, חנן כהן, דנה בובליל ופאדי עומר **מדד הדמוקרטיה הישראלית 2016** (המכון הישראלי לדמוקרטיה, 2016) 128–133, 249.

15 **שם**, בעמ' 133, 249. לא נבדק הקשר בין תמיכה במתן חופש ביטוי להתבטאויות נגד המדינה ובין התומכים במעקב אחר אזרחים באינטרנט, אבל ייתכן שבתמיכה במתן חופש ביטוי כאמור מובא בחשבון האפקט המצנן של המעקב המקוון.

16 עם זה נוסח השאלה, המתייחס לנתוני תוכן ("מה שאזרחיה כותבים באינטרנט"), אינו מלמד על נכונות הציבור למעקב מדינה מלא, שכולל גם איסוף נתוני תקשורת. ראו גם מרדכי קרמניצר ונמרוד רוזלר "ההשלכות החברתיות והפסיכולוגיות של הטרור על החברה המותקפת" **על חבל דק: המאבק בטרור והמחויבות לזכויות אדם** 23 (מרדכי קרמניצר, אביעד בן יהודה, נמרוד רוזלר, גיל רוטשילד אליאסי ויונתן רום, 2017).

להיות עשירים מאלו של כל ספק פרטי. כך המדינה יכולה להשתמש הן בנתונים שמקורם בחברות פרטיות (מקומיות או בין־לאומיות), והן בנתונים שמקורם במאגרי מידע של רשויות. כוחה העדיף של המדינה אפוא עשוי לבוא לידי ביטוי לא רק במונופול על הפעלת כוח, אלא גם ביכולתה הפוטנציאלית הרבה לרכז מידע פרטי ממקורות שונים ולנטר את פעילות האזרחים.[17]

מעניין לציין כי באשר למופעים אחרים של מעקב מדינה טכנולוגי — שתכליתם המוצהרת איננה התמודדות עם הטרור — יש דיון ער בציבוריות הישראלית. "חוק האח הגדול" (להלן: חוק נתוני תקשורת)[18] וחוק המאגר הביומטרי[19] זכו לדיון בתקשורת, ושניהם מצאו את דרכם אל בית המשפט. לעומת זה הכללים המסדירים את המעקב המקוון לא נדונים כלל, בעיקר בכל הנוגע לבחינת הדין הקיים ומידת התאמתו למציאות החברתית והטכנולוגית בת זמננו.

מטרתו של מחקר זה לבחון בחינה השוואתית את הדינים החלים בישראל על מעקב מקוון שמבצעות הרשויות, ולהצביע הן על היבטים בדין שראויים לבחינה מחדש והן על החֲסָרים באסדרה הישראלית, שיש לתת עליהם את הדעת. הפרק השני מתאר את דין הישראלי המסדיר את המעקב המקוון, על היבטיו. הפרק השלישי מתאר את הדינים בארצות הברית, באיחוד האירופי, בבריטניה, בגרמניה ובהודו. בחינה השוואתית של אופן ההסדרה בסוגיות קונקרטיות של מעקב מקוון מצויה בפרק הרביעי. לנוכח ממצאי הבחינה ההשוואתית הפרק החמישי מצביע על סוגיות בדין הישראלי הטעונות התייחסות מפאת היעדר אסדרה או אסדרה חסרה.

17 ראו את תמונת המצב בהודו כמתואר בחלק 3.5 **להלן**. דוגמה קיצונית יותר היא סין, שמאז 2014 מפעילה מערכת דירוג חברתי (social credit system), שמאגמת נתונים ממקורות מגוונים כדי לנטר את אזרחי המדינה ולחנכם. ראו Yongxi Chen & Anne S. Y. Cheung, *The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System*, University of Hong Kong Faculty of Law Research Paper No. 2017/011; Mara Hvistendahl, *Inside China's Vast New Experiment in Social Ranking*, Wired (14.12.2017)

18 חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007, ס"ח 2122, 72.

19 חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009, ס"ח 2217.

פרק 2

מעקב אחר רשתות תקשורת בישראל: מסגרת נורמטיבית

המעטפת הנורמטיבית הקשורה להסדרת המעקב אחר רשתות תקשורת באמצעות גופי ביטחון ורשויות אכיפת החוק בישראל כוללת כמה רבדים, שחלקם נוגעים להוראות החלות על בעלי רישיון בזק[1] ועל שחקנים אחרים במגזר הפרטי המנהלים מאגרי מידע; ואחרים נוגעים להוראות המסדירות העברת נתונים מאותם שחקנים לרשויות האכיפה או לגופי הביטחון.

ראשית יתוארו ההבחנות המתודולוגיות כמו שהן באות לידי ביטוי בהסדרי החקיקה, ולאחר מכן יתוארו ההיבטים הרלוונטיים להסדרת המעקב אחר רשתות תקשורת בשלושת פרטי החקיקה העיקריים החולשים על התחום – חוק הגנת הפרטיות,[2] חוק נתוני תקשורת וחוק השב״כ.[3]

2.1. הבחנות מקדימות

סיווג הנתונים: מידע, מידע רגיש, מידע מוגבל, נתוני תוכן ונתוני תקשורת

חוק הגנת הפרטיות והתקנות מכוחו נוקטים לשון של ״מידע״ (information), בשונה מ״נתונים״ – data) ומבחינים בין סוגיו. הוראות פרק ב׳ לחוק נועדו להסדיר את השימוש במאגרי מידע בישראל – הן בידי שחקנים פרטיים והן בגופים ציבוריים. מאגר מידע מוגדר: ״אוסף נתוני מידע [...] המיועד לעיבוד ממוחשב״, למעט כמה חריגים. ״מידע״ הוא ״נתונים על אישיותו של אדם, מעמדו

1 כהגדרתו בחוק התקשורת (בזק ושידורים), התשמ"ב–1982, ס"ח התשמ"ג 1066, 4 (להלן: חוק הבזק).

2 חוק הגנת הפרטיות, התשמ"א–1981, ס"ח 1011, 128 (להלן: חוק הגנת הפרטיות).

3 חוק שירות הביטחון הכללי, התשס"ב–2002, ס"ח 1832, 179 (להלן: חוק השב"כ).

האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונותיו". כל הפריטים ברשימה זו, למעט הכשרה מקצועית ומעמד אישי, מוגדרים מידע רגיש.[4] כמו כן, אחת החלופות להגדרת "מידע מוגבל" בתקנות הגנת הפרטיות (שמירת מידע)[5] היא "מידע על מצב בריאותו של אדם או על צנעת אישותו", מידע השמור במאגרים מסוימים המנויים בחוק[6] או מידע אחר שקבע השר. תקנות הגנת הפרטיות (אבטחת מידע) מזהות מגוון רחב אף יותר של סוגי נתונים הראויים לאבטחה,[7] ובכללם מונות גם נתוני תקשורת כהגדרתם בחוק נתוני תקשורת.[8]

נתוני תוכן (content) ונתוני תקשורת (metadata)

המחוקק מבחין בין נתוני תוכן, שהם תוכן התקשורת ושהמעקב אחריהם מוסדר בחוק האזנת סתר;[9] ובין נתוני תקשורת,[10] שהם המידע על התקשורת

4 ס' 7 לחוק הגנת הפרטיות.

5 תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986, ק"ת 4931, 858 (להלן: תקנות הגנת הפרטיות (שמירת מידע)).

6 המנויים בסעיף 13(ה) לחוק הגנת הפרטיות, בכללם מאגרים בעלי אופי ביטחוני, מאגרים של רשויות חקירה ורשויות מס וכן מאגרים שהוקמו מכוח החוק לאיסור הלבנת הון.

7 ראו ס' 1 לתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), ק"ת 7809, התשע"ז (להלן: תקנות אבטחת מידע).

8 **שם**, בסעיף 1(ו).

9 חוק האזנת סתר, התשל"ט–1979, ס"ח 938, 118 (להלן: חוק האזנת סתר). עם זאת ס' 9ג לחוק האזנת סתר מאפשר לבקש לצד היתר להאזנת סתר, היתר להפקת נתוני תקשורת של יעד ההאזנה.

10 סעיף 1 לחוק נתוני תקשורת מגדיר "נתוני תקשורת" כך: "נתוני מיקום, נתוני מנוי או נתוני תעבורה, והכל למעט תוכנו של מסר בזק". נתוני מיקום מוגדרים: "נתוני איכון של ציוד קצה הנמצא ברשות מנוי" (GeoLoc), נתוני מנוי הם "כל אחד מאלה: (1) סוג שירות הבזק הניתן למנוי; (2) שם, כתובת ומספר זיהוי של המנוי; (3) פרטי אמצעי התשלום של המנוי; (4) כתובת שבה הותקן מיתקן בזק בשימוש המנוי; (5) נתונים מזהים של מיתקן בזק ברשות המנוי;" – מעין רשומת כרטסת לכל מנוי/משתמש בשירות. נתוני תעבורה הם נתוני תעבורת התקשורת של המנוי – סוג המסר שנשלח, מועד שידורו או קבלתו, משך השידור, נפחו או היקפו, וכן נתוני הזיהוי של מתקני הבזק שהשתתפו בתעבורה ונתונים מזהים של המנויים הקשורים בהם.

שאינו נוגע לתוכנה, שהעברה שלהם למשטרה ולרשויות חקירה אחרות מוסדר בחוק נתוני תקשורת. כך למשל התיעוד ביומן השיחות של ראש הממשלה של מועדי שיחותיו עם פלוני הוא של נתוני תקשורת, ואילו הקלטה של אותן שיחות, המגלה את תוכנן, תסווג כנתוני תוכן.[11]

באופן אינטואיטיבי תוכן התקשורת נתפס פרטי, והוא מוגן יותר משמוגנים נתוני המעטפת הטכניים כגון משך התקשורת, מיקומה והצדדים לה. אבל בפסיקה גם נתוני תקשורת הוכרו ככאלה שנוגעים ל"ענייניו הפרטיים של אדם",[12] ולכן לפי חוק הגנת הפרטיות אסור להשתמש בהם שלא למטרה שלשמה נמסרו.[13] עמדה דומה, שרואה בנתוני תקשורת גם "מידע רגיש", מצויה בהנחיותיו של היועץ המשפטי לממשלה לגופי החקירה בנוגע למסירת מידע מחברות הטלפון לגופים בעלי סמכות חקירה.[14]

הרשות החוקרת

גופים רבים שעוסקים בהיבטים של אכיפת החוק ושמירה על הביטחון יכולים לגלות עניין בתוצרי המעקב אחרי רשתות מידע, שטומנים בחובם פוטנציאל עשיר להשבחת התוצר המודיעיני. בהיעדר דבר חקיקה ישראלי שמסדיר

11 עע"מ 7678/16 **רביב דרוקר נ' הממונה על יישום חוק חופש המידע במשרד ראש הממשלה** (פורסם בנבו, 7.8.2017) (להלן: עניין **דרוקר**).

12 ראו למשל ע"א 439/88 **רשם מאגרי המידע נ' ונטורה ואח'**, פ"ד מח(3) 808, 821; ע"פ 9893/06 **אסנת לאופר נ' מדינת ישראל** (פורסם בנבו, 31.12.2007); ב"ש (ת"א) 2390/95 **סלקום ישראל בע"מ נ' מדינת ישראל** (לא פורסם); עניין **דרוקר, לעיל** בפרק זה ה"ש 11, בפס' 21 לפסק דינו של השופט מזוז. עם זאת ציין שם השופט מזוז כי בנסיבות המקרה – העוסק בבקשה לפי חוק חופש המידע לקבל את התיעוד של יומן ראש הממשלה על שיחות הטלפון שניהל עם שלדון אדלסון ועם עמוס רגב – "מדובר בפגיעה קלה, בשוליה של הזכות לפרטיות, שכן אין במידע משום חשיפת עצם הקשר בין המשיבים, עליו הצהירו הם עצמם, ואף לא חשיפת תוכן השיחות כמובן".

13 ס' 9(2) לחוק הגנת הפרטיות.

14 "מסירת מידע מחברות הטלפון לגופים בעלי סמכות חקירה" **הנחיות היועץ המשפטי לממשלה** 4.2102 (90.013) 6 (התשס"ג; עדכון – 16 במאי 2007). הנחיות אלו, שניתנו טרם נתקבל חוק נתוני תקשורת, מבחינות בין פרטי שם, מספר טלפון ומען (נתוני מנוי, במונחי חוק נתוני תקשורת) ובין "נתוני חיוג" – מספרי הטלפון שמהם ואליהם התבצעו שיחות, שעת החיוג או שעת קבלת השיחה ומשכה (נתוני תעבורה, במונחי חוק נתוני תקשורת). מעניין כי הנחיות אלו נעדרות התייחסות לנתוני מיקום.

באופן מקיף את הסמכות לעקוב מעקב מקוון, יש לדלות את זהותם של הגופים המוסמכים להפעיל סמכויות חקירה מתוך כמה הסדרים נורמטיביים.

הוראות פרק ב׳ לחוק האזנת סתר, הנוגעות להאזנת סתר למטרות ביטחון המדינה חלות על שירות הביטחון הכללי (שב״כ) ועל אגף המודיעין של צה״ל (אמ״ן). בנסיבות מסוימות החוק מאפשר האזנת סתר גם לגופים/פרטים נוספים בצבא.[15]

פרק ג׳ לחוק האזנת סתר כולל את ההוראות הנוגעות להאזנת סתר שמבצעת המשטרה במטרה למנוע עבירות או לגלות עבריינים. החוק מתיר ניטור של תקשורת פנים־משטרתית באמצעות האזנת סתר ללא צורך בהיתר ולכל מטרה שהיא.[16]

האזנת סתר לשיחות שנעשו ברשות הרבים מותרת למוסמכים ברשויות הביטחון ובמשטרה, למטרות שנקבעו בחוק, ללא צורך בהיתר. פטור זה (בסעיף 8 בחוק האזנת סתר)[17] יכול לייצר תשתית חוקית לאישור מעקב אחרי תקשורת גלויה ברשת האינטרנט, לרבות עיבוד הנתונים שהופקו ממנו.

המעקב אחר נתוני תקשורת מוסדר בנפרד לרשויות החקירה (משטרת ישראל, יחידת חקירות הפנים של מצ״ח, מחלקת חקירות שוטרים, הרשות לניירות ערך, רשות ההגבלים העסקיים ורשות המסים בישראל) ולשירות הביטחון הכללי. כך סעיף 11 לחוק השב״כ מקנה לראש הממשלה את הזכות לקבוע כללים לעניין העברה של נתונים אליו ממאגרי מידע של בעל רישיון בזק.[18]

גישתו של המוסד לתפקידים מיוחדים לנתוני תקשורת ולמאגרי מידע כמעט שאינה מוסדרת במפורש בחקיקה, חוץ מהתקנות המסדירות העברת נתונים אליו ממאגר המידע שהוקם מכוח חוק איסור הלבנת הון.[19] ייתכן שהסדרה

15 ראו ס"ק 8(2), 8(3) לחוק האזנת סתר.

16 **שם**.

17 ראו בחלק 2.5.4 **להלן**.

18 ראו חלק 2.6 **להלן**, העוסק בחוק השב"כ.

19 תקנות איסור הלבנת הון (כללים לבקשת מידע והעברתו מן הרשות המוסמכת למוסד למודיעין ולתפקידים מיוחדים), התשע"ד–2014, ק"ת 7425, 1786.

פורמלית של גישה כזאת למאגרי מידע אחרים ולנתוני תקשורת נעשית באמצעות החלטות חסויות של ראש הממשלה. עם זאת ההסדר הכללי בחוק הגנת הפרטיות פוטר את המוסד לתפקידים מיוחדים ואת עובדיו מאחריות בגין פגיעה בפרטיות שנעשתה בסבירות במסגרת התפקיד ולשם מילויו.[20]

המחזיקים בנתונים: בעלי רישיון בזק, שחקנים פרטיים וגופים ציבוריים

לצד יירוט תקשורת בזמן אמת, רשויות חקירה וגופי ביטחון יכולים להתעניין בנתוני תקשורת ששמורים במאגרי מידע. ההוראות בפרק ב׳ של חוק הגנת הפרטיות – שעוסק במאגרי מידע – חלות על כל מי שמחזיק מאגר כזה או מנהל אותו, לרבות המדינה[21] (בחריגים מסוימים). על המחזיק במאגר מידע חלות חובות שבין השאר נוגעות לשימוש המותר במידע, לזכות העיון בו, לדרכי איסופו ולאבטחתו.[22] על המחזיק במאגר מידע מוגבל חלות הוראות מחמירות מאלה.[23]

אשר למאגרי מידע של בעלי רישיון בזק, חוק נתוני תקשורת מאפשר לרשויות החקירה והביטחון לפנות למחזיקים במאגרים אלה ולבקש נתוני תקשורת בנסיבות מסוימות.[24] החוק והתקנות מכוחו גם מסדירים את הפעלתו ואת עדכונו של מאגר מידע משטרתי חסוי, שכולל נתוני זיהוי עדכניים של המנויים אצל בעל רישיון בזק.[25] עם זאת, חוק נתוני תקשורת אינו מתאר הסדר גורף בנוגע לספקים של שירותי תקשורת שאינם נופלים בגדר הגדרת בעלי רישיון בזק[26] – דוגמת

20 ס׳ 19(2) לחוק הגנת הפרטיות.

21 ס׳ 24 לחוק הגנת הפרטיות.

22 ראו חלק 2.2 **להלן**, העוסק בחוק הגנת הפרטיות.

23 ראו תקנות שמירת מידע והעברתו בין גופים ציבוריים.

24 ראו חלק 2.4 **להלן**, העוסק בחוק נתוני תקשורת.

25 ראו ס׳ 6–10 לחוק נתוני תקשורת, וכן ראו תקנות נתוני תקשורת **להלן** בפרק זה ה"ש 64.

26 חיים ויסמונסקי **חקירה פלילית במרחב הסייבר** 181 (2015). יוער כי גם המחוקק האמריקאי נמנע מלתת דעתו בעניין זה בכל הנוגע לתחולת הוראות חוק סיוע תקשורתי לרשויות האכיפה (CALEA), ראו הדיון בחלק 3.1.4 **להלן**.

ספקי שירותי דוא"ל או טלפוניה מבוססת טכנולוגיית VoIP.[27] כשגופי החקירה נדרשים לנתונים המצויים אצל חברות פרטיות שמספקות שירותים כאלה, יחולו לשם השגתם הוראות סדר הדין הפלילי הרגיל,[28] אבל לעיתים יכול שייעשה שימוש בערוץ לא פורמלי.[29]

נוסף על מאגרי מידע של בעלי רישיון בזק, אין להתעלם מהשחקנים החשובים ברשת האינטרנט – ספקיות גלובליות של שירותי תקשורת מקוונים כגון שירותי החיפוש, האחסנה והדוא"ל שמספקת גוגל או שירותי פלטפורמת הרשת החברתית של פייסבוק. אף שיש בישראל משתמשים המנויים אצל ספקים מקומיים של שירותים דומים, עיקר המשתמשים מנויים אצל ספקים גלובליים, שבעניינם תחולת הדין הישראלי מוגבלת. עם זאת הספקיות הגלובליות מאפשרות לגופי חקירה ואכיפה במדינות שהן פועלות בהן לפנות אליהן בבקשות לנתונים על מנויים. נראה כי היקף השימוש ושיתוף הפעולה של הספקיות הגלובליות עם הרשויות בישראל הוא במגמת הרחבה. כך לדוגמה בשנים 2013–2016 שולש מספר הבקשות מאת רשויות ישראליות לנתונים מחברות גוגל ופייסבוק.[30]

27 VoIP – Voice Over IP, שם כללי לטכנולוגיות שמשתמשות בפרוטוקולי תקשורת מסוג IP (דוגמת האינטרנט) כדי להעביר דרכן תקשורת קולית. בשנים האחרונות תקשורת מבוססת-VoIP היא חלופה נפוצה לתקשורת בזק (תקשורת שמבוססת על טלפון קווי או סלולרי). לדוגמה, 26% מבני הנוער ו־15% מהמבוגרים בישראל ערכו שיחות קוליות באמצעות אפליקציית ווטסאפ. ראו "החיים בעידן הדיגיטלי – דו"ח בזק לסיכום מצב האינטרנט בישראל לשנת 2015" 23; דוח מצב התקשורת לשנת 2013 של ה־OECD העריך שספקי תקשורת VoIP היו ספקי הטלפוניה הבין־לאומיים הדומיננטים דאז. ראו OECD, OECD Communications Outlook 2013 76 (2013).

28 ס' 43 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969.

29 השוו לדרכי ההתמודדות המשפטית עם הסתה מקוונת לטרור, לרבות השימוש שנעשה בערוץ אכיפה חלופי. ראו עמיר כהנא, תהילה שוורץ אלטשולר ויובל שני "טרור ברשת – תגובת נגד או תגובת יתר" **אתר המכון הישראלי לדמוקרטיה** (18.9.2017).

30 מעיון בדוחות השקיפות של חברת גוגל עולה כי בשנים 2010–2017 עלה מספר הבקשות לנתונים שהפנו רשויות ישראליות לגוגל מ־84 ל־251. גוגל נענתה מדי חצי שנה (התקופה המדווחת בדוחות השקיפות התקופתיים של החברה) לכ־53%–76% מבקשות אלו (אתר גוגל, דוח שקיפות, דוחות, סקירה כללית, בקשות למידע על משתמשים (נצפה לאחרונה בתאריך 22.6.2017)). דוחות השקיפות של חברת פייסבוק לשנים 2013–2016 מלמדים כי מספר הבקשות הישראליות לנתונים מהחברה עלה מ־242 ל־710, וכי שיעור הבקשות שפייסבוק השיבה להן, ולו חלקית, עלה מ־50.6% ל־73.9%. בבואנו לנתח נתונים אלו, בייחוד במבט השוואתי, יש להביא בחשבון שעלייה בשיעור ההיענות

ההסדר הכללי לשיתוף מידע בין רשויות ("גופים ציבוריים") מצוי בפרק ג' לחוק הגנת הפרטיות ותקנות שמירת מידע והעברתו לגופים ציבוריים. ככלל, מסירת מידע בין גופים ציבוריים מותרת אם לא נאסרה בחיקוק או בעקרונות של אתיקה מקצועית.[31]

יש עוד מאגרי מידע מיוחדים שדרכי ניהולם, החזקתם ושיתוף המידע שבהם עם רשויות חקירה ועם גופי ביטחון מוסדרים בנפרד, בכללם מאגרים פרטיים כגון אלה שהוקמו מכוח חוק שירות נתוני אשראי,[32] ומאגרים שרשויות מחזיקות ומנהלות כגון מאגר המידע מכוח חוק נתוני אשראי[33] או מאגר המידע הביומטרי.[34]

יעדי המעקב: מנויים או מושאי מידע (data subjects)

מושא מידע (data subject) הוא אדם (ולעיתים אישיות משפטית) שמידע עליו מוחזק במאגר הנתונים, ומידת שליטתו בנתונים אלה באה לידי ביטוי בהסכמתו לשימושים שונים של בעל מאגר המידע בנתונים וביכולתו לגשת לנתונים עליו, למחוק אותם או לשנותם. תפיסת הגנת הפרטיות השלטת בדין האירופי, וזו המשתקפת בחוק הגנת הפרטיות ובפרשנותו,[35] מדגישה את מושאי המידע (data subjects), ואת מידת שליטתם במידע האישי עליהם.

הדים לתפיסה זו ניתן למצוא בחוק האזנת סתר, המגדיר האזנת סתר כהאזנה ללא הסכמת אף אחד מ"בעלי השיחה".[36] שיח הסכמה זה נעדר מלשונו של חוק נתוני

יכולה להעיד על שיפור בנוהלי הרשויות המדינתיות ובתהליכי סינון הבקשות. כך למשל ההיענות לבקשות של רשויות הודו בתקופה הזאת נותר יציב כשהיה – כ־50%.

31 ס' 23ג לחוק הגנת הפרטיות.

32 חוק שירות נתוני אשראי, התשס"ב–2012, ס"ח 1825, 104.

33 חוק נתוני אשראי, התשע"ו–2016, ס"ח 2551, 838 (להלן: חוק נתוני אשראי).

34 חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשע–2009.

35 ראו מיכאל בירנהק **[מרחב פרטי] – הזכות לפרטיות בין משפט לטכנולוגיה** פרקים ג ו־ט (2011); עומר טנא "הזכות לפרטיות בעקבות חוק יסוד כבוד האדם: מהפך מושגי, חוקתי ורגולטורי" **קריית המשפט** ח 9–70 (2009); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 Yale L.J. 1151 (2004)

36 ס' 1 לחוק האזנת סתר. בעל שיחה הוא אחד מהצדדים — המעביר או הנעבר — של מסר התקשורת, אם באמצעות מתקן בזק ואם בעל פה. נותן שירות הבזק אינו בעל שיחה.

תקשורת, וכך גם התייחסות לנעקבים כאל מושאי מידע אוטונומיים. במקום זאת, הפרטים שפרטיותם נפגעת מכוח הוראות החוק מתוארים כ"מנויים" גרידא של בעל רישיון בזק. עם זאת יש בחוק הוראות מיוחדות בנוגע למנויים שהם בעלי מקצוע שבעניינם חל חיסיון מקצועי לפי כל דין.[37]

לוח 1
החקיקה המסדירה מעקב מקוון בישראל,
לפי סוג הנתונים והגוף החוקר

הגוף החוקר	נתוני תקשורת	נתוני תוכן
משטרת ישראל	חוק נתוני תקשורת	חוק האזנת סתר (פרק ב')
שירות הביטחון הכללי	ס' 11 לחוק השב"כ	חוק האזנת סתר (פרק ג')
אגף המודיעין במטה הכללי	אין הסדרה*	חוק האזנת סתר (פרק ג')
המוסד**	אין הסדרה	אין הסדרה

* למעט בחוק נתוני תקשורת, בנוגע למשטרה הצבאית החוקרת בכובעה כ"רשות חוקרת אחרת".

** למעט בחוק הגנת הפרטיות, המקנה למוסד או למי שנמנה עם עובדיו או פועל מטעמו פטור מאחריות על פגיעה בפרטיות שנעשתה בסבירות במסגרת תפקידם ולשם מילויו.

.2.2
ישראל - מעטפת חוקתית

בדין הישראלי הזכות לפרטיות היא זכות חוקתית, שקבועה בסעיף 7 לחוק־יסוד: כבוד האדם וחירותו: "(א) כל אדם זכאי לפרטיות ולצנעת חייו. (ב) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו. (ג) אין עורכים חיפוש ברשות היחיד של

37 ס' 3(ב) לחוק נתוני תקשורת.

אדם, על גופו, בגופו או בכליו. (ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו".[38]

בעקבות חקיקת חוק היסוד אימץ בית המשפט גישה פרשנית נדיבה לזכות זו.[39] כך למשל נקבע כי הזכות משתרעת גם על פרטיות בתקשורת מחשבים וטלפוניה, ובכלל זה מידע על זהות הצדדים המתקשרים או על האתרים שבהם פלוני גולש.[40] הזכות לפרטיות שבסעיף 7 אינה בלתי מוגבלת. בכפוף לתנאי פסקת ההגבלה שבסעיף 8 לחוק היסוד, ניתן לפגוע בה "בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שלא עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו".

בעניין **האגודה לזכויות האזרח בישראל נ' משרד הפנים**[41] עתרה האגודה לזכויות האזרח לבית המשפט בבקשה שיאסור על המדינה לאפשר גישה ישירה למאגר המידע לפי חוק מרשם האוכלוסין באמצעות חיבור המחשב של משרד הפנים למחשבי רשויות שונות ולמחשבי הבנקים המסחריים. באשר להעברת מידע לגופים ציבוריים נמצא כי ההסדר הקיים אינו מידתי מאחר שאינו מקיים את המבחן השני במבחני המידתיות – מבחן הצורך.[42] השופטת דורנר הצביעה על היעדרן של תקנות או הנחיות מינהליות המצמצמות את הגישה למידע למעט עובדי הציבור הנדרשים לו, וציינה כי "דרישת המידתיות מחייבת למזער את הפגיעה בזכות לפרטיות על־ידי צמצום מספר עובדי הציבור הנגישים למידע; על־ידי צמצום היקף המידע שנמסר

38 ס' 7 לחוק־יסוד: כבוד האדם וחירותו, ס"ח תשנ"ב 1391, 60 (להלן: חוק היסוד).

39 ראו בג"ץ 2481/93 **דיין נ' ניצב וילק, מפקד מחוז ירושלים**, פ"ד מח(2) 456, 470 (1994); בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האיזורי בנתניה**, פ"ד סא(1) 581 (2006); טנא, **לעיל** בפרק זה ה"ש 35.

40 ראו לדוגמה בש"פ 6640/06 **צבי קרוכמל נ' מדינת ישראל**, פס' ט"ו להחלטתו של השופט (כתוארו אז) רובינשטיין (פורסם בנבו, 7.9.2006); בש"פ 7368/05 **אסף זלוטובסקי נ' מדינת ישראל**, פס' 7 לפסק דינו של השופט (כתוארו אז) ריבלין (פורסם בנבו, 4.9.2005).

41 ראו **לעיל** בפרק 1 ה"ש 13.

42 לפי מבחן הצורך, או מבחן האמצעי שפגיעתו פחותה, פגיעה בזכויות יסוד באמצעי חקיקתי שפגיעתו בזכות היא הפחותה מכל החלופות. ראו אהרן ברק **מידתיות במשפט** 391 (2010).

כך שיועבר רק המידע הדרוש; על־ידי קביעת היקף המידע בהתחשב בחשיבות התכלית שלשמה הוא נדרש".[43] באשר לבנקים, ההסדר נפסל בהיעדר הסמכה מפורשת בחוק לפגיעה בזכויות אדם. בהמשך הוסיפה השופטת כי גם לפי גישה דווקנית פחות לדרישת ההסמכה לפגיעה בזכות, ההסדר אינו מידתי בראי מבחן הצורך, שכן "על פני הדברים כדי להגשים את התכליות שבהן מדובר אין הכרח לספק לבנקים מידע דווקא בדרך של התחברות ישירה למחשבי המדינה".[44]

.2.3
חוק הגנת הפרטיות

טרם חקיקת חוק היסוד נסמך עיקר ההגנה על הזכות לפרטיות על חוק הגנת הפרטיות. גרסתו הראשונה של חוק הגנת הפרטיות נעדרה התייחסות למאגרי מידע, ורק הנוסח שהוכן לקריאה השנייה והשלישית כלל פרק שעוסק בהם, ובו נערכה רוויזיה במסגרת תיקון מס' 4 לחוק.[45]

מלבד ההסדרים הפרטניים שיכולים לחול בענייני מעקב ברשתות תקשורת, ההסדר הכללי בחוק הגנת הפרטיות גם אוסר על פגיעה בפרטיות הזולת.[46] סעיף 2 לחוק מפרט רשימת מופעים של פגיעה בפרטיות, בכללם בילוש או התחקות (ס"ק 2(1)), האזנה אסורה (ס"ק 2(2)), העתקת תוכן של כתב (לרבות מסר אלקטרוני) שלא נועד לפרסום (ס"ק 2(5)), הפרה של חובת סודיות בדבר ענייניו הפרטיים של אדם, שמקורה בדין או בהסכם (ס"ק 2(7), 2(8)) ומסירת מידע שהושג לפי דרך של פגיעה בפרטיות (ס"ק 2(10)).

43 עניין **האגודה לזכויות אזרח בישראל נ' משרד הפנים**, **לעיל** בפרק 1 ה"ש 13, פס' 7 לפסק דינה של השופטת דורנר.

44 **שם**, בפס' 8. ראו ברק, **לעיל** בפרק זה ה"ש 42, בעמ' 143.

45 ראו דן חי **ההגנה על הפרטיות בישראל** 261 (2006). בריאיון מאוחר סיפר השופט קלינג, מחברי הוועדה שניסחה את פרק ב' בחוק ההגנה על הפרטיות, כי הם שאבו את השראתם מ־**1984** של אורוול ו**הטירה** של קפקא. ראו אורי ישראל פז, "גבריאל קלינג: 'על השופט בדימוס להמשיך להתנהג כשופט מכהן ולשמור על לשונו'" **תקדין** (19.10.2014).

46 ס' 1 לחוק הגנת הפרטיות.

חוק הגנת הפרטיות חל על המדינה (ס' 24), ויש בו הסדרים מיוחדים החלים על גופים ציבוריים ועל רשויות ביטחון. רשויות ביטחון, כהגדרתן בחוק,[47] נהנות מפטור מאחריות לפגיעה בפרטיות במקרים שבהם הפגיעה נעשתה לפי הסמכה בדין או בסבירות ובמסגרת התפקיד ולשם מילויו.[48]

על גופים ציבוריים חלות הוראות מיוחדות באשר למסירת מידע ושיתופו ביניהם (פרק ג' לחוק ותקנות שמירת מידע והעברתו בין גופים ציבוריים), ומסירת מידע שמותרת לפיו לא תהיה בבחינת פגיעה בפרטיות (ס' 23ז). הגבלות אלו על מסירה וקבלה של מידע אינן חלות על רשות ביטחון, אלא אם היא נאסרה בחיקוק (ס"ק 23ב(ב)).

פרק ב' לחוק הגנת הפרטיות קובע חובות על מנהלי מאגרים וזכויות של מושאי המידע. לצד החובה הטכנית של רישום מאגר המידע, החוק מחיל על מנהלי מאגרים או בעליהם כמה חובות מהותיות. האחת היא החובה המוטלת על מבקש המידע ליידע את בעל המידע (ס' 11). פנייה לאדם לקבלת מידע לשם החזקה או שימוש בו במאגר מידע תלווה בהודעה ־ שהיא הבסיס ליצירת הסכמה מדעת של מושא המידע (אם מושא המידע הוא מי שממנו המידע מבוקש) ובה יפורטו בין השאר מטרת השימוש במידע ולמי הוא יימסר. בירנהק מעיר כי הנושאים הכלולים בהודעה זו ממלאים בתוכן את עקרון צמידות המטרה, שלפיו אין להשתמש במידע אלא למטרה שלשמה הוא נאסף (ס'2(9) לחוק).[49] חובות נוספות הן שמירה על סודיות המידע שבמאגר (ס' 16) וחובת אבטחת המידע (ס'17, 17א ו־17ב).

לפי סעיף 13 לחוק הגנת הפרטיות, למושאי מידע יש זכויות עיון במאגרי מידע, אך מאגרים מסוימים (הנמנים בסעיף 13(ה) לחוק, בכללם מאגרי מידע של רשות ביטחון) מוחרגים מזכות זו. לצד זכות העיון, בסעיף 14 ניתן למצוא זכויות מוגבלות של מושא המידע לתיקון או למחיקה של מידע עליו, באפשרו לבית המשפט להורות על מחיקה או על תיקון של נתונים שבעל מאגר המידע סירב לבקשה למחוק או לתקן.

47 ס"ק 19(3) לחוק הגנת הפרטיות: "'רשות ביטחון' – לעניין סעיף זה – כל אחת מאלה: (1) משטרת ישראל; (2) אגף המודיעין במטה הכללי והמשטרה הצבאית של צבא־הגנה לישראל; (3) שירות בטחון כללי; (4) המוסד למודיעין ולתפקידים מיוחדים; (5) הרשות להגנה על עדים".

48 ס' 19 לחוק הגנת הפרטיות.

49 ראו בירנהק, **לעיל** בפרק זה ה"ש 35, בעמ' 231.

מאחר שלמושאי המידע של מאגרים ביטחוניים אין זכות עיון קנויה במידע עליהם השמור במאגרים אלה, האפשרות לבקש תיקון או מחיקה של מידע כזה נשללת מהם.

.2.4 חוק נתוני תקשורת

חוק נתוני תקשורת מסדיר את נוהלי ההעברה של נתוני תקשורת[50] מבעלי רישיון בזק – מפעילי שירותי טלפוניה קווית, סלולרית וספקי אינטרנט – למשטרת ישראל ולגופי החקירה האחרים המנויים בו. החוק מפרט שני נהלים עיקריים: הנוהל שלפיו יינתן היתר לגופי חקירה אלה לקבל נתוני תקשורת מבעלי הרישיון, ונוהלי ניהולו ועדכונו של מאגר משטרתי של נתוני זיהוי (נתוני תקשורת חלקיים, שכוללים נתונים על המנוי ומספר מזהה של מכשירי הטלפון שברשותו) ונתונים בדבר מיפוי אנטנות סלולריות של מפעיל השירות.

החוק מבחין בין בקשות רגילות (ס' 3) לבקשות דחופות (ס' 4). בקשות רגילות לקבלת נתוני תקשורת מותנות בצו של בית משפט השלום. היתר כאמור יינתן אם שוכנע בית המשפט שהדבר נדרש למטרות אלה: הצלת חיי אדם; הגנה עליהם; גילוי עבירות, חקירתן או מניעתן; גילוי עבריינים והעמדתם לדין; וחילוט רכוש על פי דין "ובלבד שאין בקבלת נתוני התקשורת כאמור כדי לפגוע, במידה העולה על הנדרש, בפרטיותו של אדם". כשהמנוי שבענייננו הוגשה הבקשה הוא בעל מקצוע שנהנה מחיסיון, יינתן היתר אם שוכנע בית המשפט שיש יסוד לחשד שבעל המקצוע מעורב בעבירה שבקשר אליה הוגשה הבקשה. פרק הזמן שבו יועברו נתוני תקשורת עתידיים מוגבל לשלושים ימים מיום מתן הצו.

החוק החיל הוראת שעה ולפיה בארבע השנים הראשונות לתחולתו, משנת 2008, ידווח מדי שנה השר לביטחון פנים (או השר הממונה על רשות חוקרת אחרת) לוועדת החוקה של הכנסת על מספר הבקשות לנתוני תקשורת ולנתוני זיהוי שהוגשו לפי הנהלים בחוק וכן על מספר העברות המידע לרשויות חוקרות אחרות שנעשו מכוחו.[51] בשנת 2014 הוגשה הצעת חוק פרטית המבקשת להפוך חובת דיווח זו

50 ראו בחלק 2.1 **לעיל**.

51 ס' 14 לחוק נתוני תקשורת.

לקבועה.[52] תוקפו של סעיף זה טרם הוארך, ומשנת 2012 הפעלת סמכויות לפי חוק נתוני תקשורת אינה מדווחת מדי שנה לכנסת. בעקבות בקשת חופש מידע שהגיש העיתון **דה מרקר**, מסרה משטרת ישראל נתונים משלימים לשנים 2012–2016.[53]

מדיווחי השר לביטחון פנים עולה שבארבע שנות הדיווח לכנסת לפי הוראת השעה שבסעיף 14 לחוק נתוני תקשורת (השנים 2008–2012),[54] חל גידול ניכר בהיקף הבקשות לנתוני תקשורת שהוגשו לבית המשפט, והן הכפילו את עצמן בתקופה זו. את הגידול הסבירו נציגי המשטרה בעובדה שבשנה הראשונה לתחולת החוק הוקמה מחלקת הסיגינט המשטרתית, והוטמעו נוהלי העבודה והשימוש בערוץ חקירה זה.[55] את ההסבר הזה מאששת היציבות היחסית במספר הבקשות בשנים 2013–2016, שעודנו במגמת עלייה אך בקצב מתון יותר (ראו בלוח 2 להלן).

52 פ/2055/19, הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת) (תיקון – חובת דיווח), התשע"ד–2014. יו"ר ועדת החוקה, חוק ומשפט, ח"כ דוד רותם, העיר כי "סעיף 14 לחוק שמחייב אתכם [את המשטרה] לדווח הוא הוראת שעה. יש לי הרגשה שאני הולך להפוך אותו להוראה קבועה. ככל שלא מפקחים עליכם, החגיגה הולכת וגדלה", ובהמשך הוסיף: "קודם כל נבקש לשנות את החוק ולהפוך את חובת הדיווח לחובה קבועה ולא להוראת שעה. אנחנו נתחיל לדרוש מכם דיווחים כל 6 חודשים ולא כל שנה. הדיווחים יהיו מפורטים". פרוטוקול ישיבה מס' 401 של ועדת החוקה, חוק ומשפט, הכנסת ה־18 (5.6.2011); כמו כן ראו עניין **חוק נתוני תקשורת**, **להלן** בפרק זה ה"ש 69, שם ציינה הנשיאה (בדימוס) ביניש בפס' 33 לפסק דינה כי "לא נעלמה מעיננו העובדה כי חובת הדיווח לכנסת הקבועה בחוק נקבעה כהוראת שעה שתוקפה לארבע שנים בלבד מיום כניסתו לתוקף של החוק (ראו סעיף 14(ג) לחוק). נראה לנו כי בשל הקשיים המלווים את הליכי לידתו של החוק שאף המדינה לא חלקה עליהם, משך הזמן הנדרש להטמעת העקרונות המחייבים את פעולות הרשות והחשיבות עליה עמדנו שבביקורת עקבית של הכנסת, יש מקום לפעול להארכת תוקפו של סעיף זה".

53 מקורות: דיווחי השר לביטחון פנים לוועדת החוקה, חוק ומשפט של הכנסת לפי חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 מתאריכים 31.7.2012, 1.10.2009). דיווחים אלה אינם כוללים נתונים על בקשות לנתוני תקשורת שאותן דחה בית המשפט, אם היו כאלו. דיווחים משלימים לתקופה זו הושגו באמצעות בקשה מכוח חוק לפי חופש המידע, כמו שפורסם אצל אמיתי זיו "סמסים, מיקום וכרטיסי אשראי: המידע שהמשטרה אוספת עליכם מהסלולר", **דה מרקר**, 1.4.2018; ראו גם תשובת משטרת ישראל לבקשת חופש המידע 5021 לקבלת נתונים סטטיסטיים על יישום חוק סדר הדין הפלילי בדבר נתוני תקשורת מיום 20.12.2017.

54 יולי 2008 עד יוני 2012, לפי הוראת השעה בס' 14 לחוק נתוני תקשורת.

55 ראו דבריה של רפ"ק ענת סיגל, יועמ"ש סיגינט, המשרד לביטחון פנים. פרוטוקול מס' 401, **לעיל** בפרק זה ה"ש 52.

לוח 2
בקשות להיתרים מכוח חוק נתוני תקשורת[56]

תקופה	יולי 2008 – יוני 2009	יולי 2009 – יוני 2010	יולי 2011 – יוני 2012	יולי 2012 – יוני 2013	אוגוסט 2013 – דצמבר 2013*	2014	2015	2016
בקשות שהוגשו ואושרו	9,603	14,133	17,597	22,381	6,510	21,060	23,004	24,801
בקשות שנדחו	–	–	–	–	9	50	34	39
שיעור דחייה	–	–	–	–	0.138%	0.237%	0.148%	0.157%
תכלית הבקשה								
הצלת חיי אדם	252	185	285	268	186	451	636	836
גילוי עבריינים וחקירת עבירות	9,227	13,946	17,309	22,110	6,425	20,775	22,661	24,384
חילוט רכוש	124	2	–	3	49	165	230	191
סוג נתוני תקשורת המבוקש**								
מנוי	14,636	30,855	25,955	31,099	10,705	35,586	41,142	49,423
תעבורה	15,108	26,968	22,579	25,034	23,787	66,701	8,5945	70,659
מיקום	6,884	10,835	8,410	21,479	21,822	65,928	41,457	65,387

* הנתונים על התקופה אוגוסט–דצמבר 2013 נמוכים מאחר שהם מתייחסים לתקופה קצרה יותר בשל ההתקנה של מערכת מחשוב חדשה.[57]

** בבקשה יחידה ייתכן שיבוקשו כמה סוגים של נתוני תקשורת.[58]

56 ראו בפרק זה ה"ש 53 **לעיל**.

57 עם זאת המגמות הכלליות הנלמדות מהנתונים נשמרות לאחר הפעלת אקסטרפולציה גסה (הכפלה ב־3) על נתוני השליש האחרון של 2013.

58 לפי רמ"ח סיגינט, נצ"מ גדי סיסו, המשרד לביטחון פנים, צו יכול לכלול כמה בקשות לנתונים תקשורת: "חוקר שהולך להוציא צו מבית המשפט, יכול להיות שהצו מתחלק לכמה צווים שונים. בפעולה מסוימת שאני מבקש, למשל, פעולה של נתוני מיקום, להבדיל מנתוני זירה או נתוני מנוי, שאז אני עושה שימוש, יכולים וימומשו בהדרגה בהתאם לצורך החקירתי. יכול להיות שקיים צו שיפוטי שעשיתי בו פעולה תקשורתית ומיצאתי חלק מהצו בעת הזאת מטעמים כלכליים והמימוש כבר לא רלוונטי כי כבר יצרתי פריצת דרך בחקירה או שהזימו את החקירה ואז אין צורך לממש את הצו במלואו. אתה גם חסכת כסף למדינה וגם לא עשית מימוש רחב מידי באלטרנטיבה שקיבלת מבית משפט. אין לנו תיעוד כזה. אנחנו לא מתעדים את כל הבקשות במימוש, כמה סירבנו ומה מומש ומה לא. נוכל לעשות את זה". ראו פרוטוקול מס' 401, **לעיל** בפרק זה ה"ש 52.

שיעור הבקשות לפי סעיף 3 לחוק נתוני תקשורת שבית המשפט דחה – זעום. לפי דיווחי המשטרה, בארבע השנים הראשונות לחוק, שבהן הופעלה הוראת השעה בדבר דיווחים שנתיים לכנסת, לא נדחו בקשות כאלה כלל. ואולם למרות השיעור המזערי של דחיית הבקשות, יש להיזהר מהנחת המבוקש: מקורו יכול להיות בנהלים קפדניים ובבקרות פנימיות של המשטרה שמונעות הגשת בקשות לא מוצדקות. ואולם, ייתכן שהדבר נובע מכך שהשופטים מייחסים לזכות לפרטיות משקל נמוך מזה שהם מייחסים לצורך להגן על שלום הציבור.

שיעורם של נתוני המיקום המבוקשים הלך וגדל עם השנים. בתקופה המדווחת הראשונה (יולי 2008–יוני 2009) היה שיעורם של נתוני המנוי כ־40% מסך נתוני התקשורת המבוקשים, ואילו שיעור נתוני המיקום – כ־19%. בשנת 2016 היה שיעורם של נתוני המיקום כ־35% מנתוני התקשורת המבוקשים. ייתכן שהדבר נובע מהתייעלות השימוש במאגר נתוני הזיהוי, המצוי ממילא בידי במשטרה (ראו להלן). עם זאת בהתחשב בגידול המוחלט בבקשות לנתוני מיקום,[59] יש לתת את הדעת על השימוש ההולך ורב של משטרת ישראל בנתונים אלה, שכן רמת הפגיעה בפרטיות הכרוכה בהשגת נתונים המלמדים על מיקומו של אדם גבוהה מזו של נתוני מנוי גרידא, המלמדים על זהותו של צד לשיחה.[60]

בקשות דחופות טעונות היתר פנימי של קצין מוסמך, בלא צו של בית משפט, אם יש צורך שאינו בר־דיחוי לקבל נתוני תקשורת לשם מניעת עבירות מסוג פשע, גילוי מבצעו או הצלת חיי אדם. היתר כזה מוגבל ל־24 שעות. לפי הדיווחים השנתיים של השר לביטחון פנים, בארבע השנים שבהן חלה חובת הדיווח גדל ב־50% מספר ההיתרים שנתנו כך קצינים מוסמכים. בתקופה העוקבת (2016–2012) שילש מספר ההיתרים את עצמו (ראו בלוח 3 להלן). בכל הנוגע לנוהלי שימורם וביעורם של נתוני תקשורת המתקבלים בדרכים אלה החוק שותק.

59 לצד הגידול המוחלט במספר הבקשות לנתוני מיקום בתקופה המדווחת, שהכפיל את עצמו פי עשרה כמעט — מ־6,884 בקשות לנתוני מיקום בתקופה הראשונה ל־65,387 בקשות כאלו בשנת 2016.

60 נוהל 03.344.306 "קבלת נתוני תקשורת וקבצי נתונים ממאגר מידע של בעל רישיון בזק" (עודכן ביום 4.4.2017) של משטרת ישראל מציין במפורש כי על קצין המשטרה המאשר הגשת בקשה לצו נתוני תקשורת נדרש להביא בחשבון, בין השאר, את סוג נתון התקשורת המבוקש: "יש להתייחס ביתר הקפדה לבקשות לקבלת נתוני מיקום (לעומת נתוני זיהוי ונתוני שיחות), שכן הפגיעה הנגרמת מבקשה כזו היא גבוהה יותר" (ס"ק ד.6.(1)(ו') לנוהל). כמו כן ראו עניין *Carpenter*, **להלן** בפרק 3 ה"ש 65 ,63.

לוח 3
בקשות להיתרים דחופים
מכוח חוק נתוני תקשורת[61]

תכלית הבקשה	יולי 2008– יוני 2009	יולי 2008– יוני 2009	יולי 2008– יוני 2009	2012	2013	2014	2015	2016
הצלת חיי אדם	1,513	2,192	2,602	2,982	3,273	4,754	5,781	6,530
גילוי מבצע ומניעת עבירה	518	847	879	916	1,208	1,670	2,110	2,987
סה"כ	2,031	3,039	3,481	3,898	4,481	6,424	7,891	9,517

לצד נתוני תקשורת המתקבלים בצו שיפוטי או בהיתר של קצין מוסמך, החוק מסמיך את ראש אגף החקירות והמודיעין במשטרה לדרוש מבעל רישיון בזק למתן שירותי בזק פנים־ארציים נייחים או שירותי רדיו טלפון נייד,[62] קובץ מידע עדכני של נתוני מנוי לצורך בנייה ותחזוק של מאגר מידע משטרתי שכולל נתוני זיהוי של מנויי בזק. פרשנות החוק מעלה כי נתוני הזיהוי המועברים הם שם המנוי, מספר תעודת זהות או מספר התאגיד, מען, מספר טלפון ומספר מזהה של המכשיר, וייתכן שניתן להוסיף לרשימה זו גם את "מספרי הברזל" של המכשירים עצמם, הטבועים בכל מכשיר. דן חי סבור שזו רשימה סגורה, שאינה כוללת היסטוריה של בעלויות עבר של המנוי במכשירים שונים, אמצעי תשלום ונתונים אחרים.[63]

61 למקורות ראו **לעיל** בפרק זה ה"ש 53.

62 הכוונה לבעלי רישיון להפעיל שירותי טלפוניה, להבדיל משירותי בזק כלליים, שכוללים גם ספקי אינטרנט; שאם לא כן, במאגר נתוני הזיהוי היה ניתן גם לקשור בין IP לבעליו. הצעת החוק כללה הרשאה להעברת קובץ של רשימת הלקוחות של בעל רישיון בזק למתן שירותי בזק באמצעות האינטרנט, אך זו הושמטה בהכנת החוק לקריאה שנייה ושלישית. ראו דן חי **נתוני תקשורת בישראל** 159 (2011).

63 **שם**, בעמ' 160.

נוסף על ההוראות בחוק נתוני תקשורת, בכל הנוגע לשימוש במאגר ולניהולו יש הנחיות גם בתקנות נתוני תקשורת, ובתוכן חובות אבטחה ותיעוד של הפעולות הנעשות במאגר.[64] השימוש במאגר לא ייעשה אלא לאותן המטרות שלשמן ניתן לבקש נתוני תקשורת (ראו לעיל). מערכות מקושרות לא יחוברו למאגר אלא באישור של ראש מחלקת הסיגינט במשטרה, בתנאים הקבועים בתקנות נתוני תקשורת.[65] החוק מאפשר להעביר נתונים מהמאגר לרשות חוקרת אחרת[66] ללא צו ובאופן מקוון למורשי גישה ברשות האחרת.[67] במקרים מסוימים יתאפשר להעביר נתונים לפי צו גם ל"נציגים" שאינם מורשי גישה.

נוסף על חוק נתוני תקשורת, במסגרת הליכי גילוי אזרחיים יש שבית המשפט נותן צו איכון לחברות תקשורת סלולרית. במקרה זה ישקול בית המשפט את מידת הפגיעה בפרטיות שיש בצו האיכון לפי ערכי חשיפת האמת, את מידת הרלוונטיות של דוח האיכון המבוקש ואת מידתיות הפגיעה בפרטיות.[68]

בעניין **האגודה לזכויות האזרח נ' משטרת ישראל** (להלן: עניין **חוק נתוני תקשורת**)[69] נתקפה חוקתיותו של ההסדר שבחוק נתוני תקשורת. העותרים

64 תקנות סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת) (מאגר נתוני זיהוי תקשורת), התשס"ט-2008, ק"ת 6735, 270 (להלן: תקנות נתוני תקשורת).

65 תקנה 3(ב) לתקנות נתוני תקשורת.

66 יובהר כי בחוק נתוני תקשורת יש רשימה סגורה של רשויות המוגדרות "רשות חוקרת אחרת" (ס' 1 לחוק). לאחרונה דחה בית המשפט לעניינים מקומיים (ת"א, תיק מס' 16-03-3789 **עיריית תל-אביב נ' פרטנר תקשורת בע"מ**, החלטה מיום 2.2.2017) בקשה של עיריית תל אביב שלפיה יורה בית המשפט לחברת פרטנר למסור נתוני זיהוי של מנוייה על מנת לאפשר לפקחי העירייה לזהות את בעליהם של מספרי טלפון המופיעים במודעות שהופצו בעיר.

67 ס' 8 לחוק נתוני תקשורת.

68 ת"א 16-07-7553 (שלום ב"ש) **טופ הובלות קוידר בע"מ נ' סקוריטס סוכנות בטוח בע"מ** (פורסם בנבו, 21.12.2017); ס"ע 12-02-53758 (אזורי ת"א) **בי.די.אר טכנולוגיות בע"מ נ' חפץ** (פורסם בנבו, 11.6.2013); ת"א 11-06-44411 (שלום, חד') **מוהנד מוגרבי ואחי נ' מ. בר תחזוקה בע"מ** (פורסם בנבו, 6.6.2012); ע"ע 17-04-40711 **פישר תעשיות פרמצבטיות בערבון מוגבל נ' אברהם שטטר** (פורסם בנבו, 4.3.2018).

69 בג"ץ 3809/08 **האגודה לזכויות אזרח נ' משטרת ישראל** (פורסם בנבו, 28.05.2012) (להלן: עניין **חוק נתוני תקשורת**).

טענו כי לשונו הרחבה של סעיף 3 לחוק מאפשרת לבית המשפט לתת צו להשגת נתוני תקשורת בנוגע לכל פעילות שנוקטות הרשויות החוקרות (ולמעשה לאפשר איסוף גורף וחסר הבחנה), דבר שאינו מתיישב עם מבחן המידתיות השני.

עיקר פסק דינה של הנשיאה ביניש בחן את מידתיות החוק וההסדרים שגובשו במסגרתו. במקום פסילת חוקתיותו של החוק, בחרה הנשיאה ביניש בדרך של פרשנות מצמצמת, התואמת את חוקי היסוד. נקבע כי כדי לעמוד במבחני המידתיות, הפרשנות החוקתית לסעיף 3 לחוק מחייבת את הרשות החוקרת לפנות ולבקש צווים רק כשהם דרושים לגילוי עבריין מסוים או בנוגע לחקירתה או למניעתה של עבירה מסוימת, ולא לצורכי פעילות מודיעין כללית בנוגע לעבירות או לעבריינים.[70]

לעומת זאת לא מצא בית המשפט עילה להתערבות בהיבטים אחרים של ההסדר בחוק. החלת ההסדר על עבירות מסוג עוון,[71] המשתרעות על פני עבירות רבות – מקצתן ברמת חומרה שאין בה כדי להצדיק בהכרח את הפגיעה בפרטיות המגולמת בחוק – נמצאה מידתית לפי הביקורת השיפוטית על מתן צווים לפי החוק.[72] גם ההסדר להיתר קבלת נתוני תקשורת במקרים דחופים ללא צו[73] נמצא מידתי, בכפוף לפרשנות המחייבת הפעלת שיקול דעת מינהלי קפדני.[74]

נוסף על התייחסות למידתיותם של הסדרים קונקרטיים בחוק, ניתח פסק הדין את מידתיות החוק כמכלול, ולפי בחינה זו לא מצא עילה להתערבות בית המשפט: הנשיאה ביניש ציינה כי ב"עצם קיומה של ביקורת שיפוטית על ההליך

70 עניין **חוק נתוני תקשורת**, **שם**, פס' 16 לפסק דינה של הנשיאה ביניש.

71 ס' 1 לחוק נתוני תקשורת.

72 עניין **חוק נתוני תקשורת**, **לעיל** בפרק זה ה"ש 69, פס' 18–19 לפסק דינה של הנשיאה ביניש.

73 ס' 4 לחוק נתוני תקשורת.

74 עניין **חוק נתוני תקשורת**, **לעיל** בפרק זה ה"ש 69, פס' 26–27 לפסק דינה של הנשיאה ביניש. השופט מלצר הסתייג מהחלת ההסדר על בעלי חיסיון מקצועי, ולגישתו במקרים שבהם חל לכאורה חסיון בעל מקצוע, יש לפנות לבית המשפט לפי המתווה שבסעיף 3 לחוק.

המרכזי לקבלת נתונים על־פי החוק, יש כדי להעיד על מידתיותו".[75] בהבחנות שבחוק בין הסמכויות המוקנות לגופי החקירה השונים יש כדי לצמצם את הפגיעה הפוטנציאלית בזכות. גם הביקורת על יישומו של החוק, מכוח הוראות החוק, יש בה כדי לתרום לניתוח המידתיות – הפיקוח הפרלמנטרי הכללי על יישום החוק[76] והפיקוח המוסדי על השגת נתוני תקשורת ללא צו שיפוטי.

2.5. חוק האזנת סתר

2.5.1. האיסור הכללי על האזנת סתר

חוק האזנת סתר מגדיר האזנת סתר כהאזנה באמצעות מכשיר ללא הסכמה של אף אחד מבעלי השיחה.[77] שיחה יכולה להתבצע בדיבור, באמצעות מתקן בזק, או באמצעות תקשורת מחשבים ותקשורת סלולרית. בגדר האזנה נכללים גם קליטה או העתקה של תוכנה של שיחת הזולת. בעל שיחה הוא צד לשיחה, המשדר בבזק או נמענו.[78] מכאן שחוק האזנת סתר משתרע אל מעבר למשתמע

75 **שם**, פס' 38–39 לפסק דינה של הנשיאה ביניש.

76 בפס' 38 לפסק הדין, המונה את הוראות הדיווח לוועדת החוקה על יישום החוק לפי סעיף 14 לחוק נתוני תקשורת כגורם התורם למידתיות החוק, אין התייחסות לכך שהוראות אלו הן הוראת שעה שעמדה בתוקפה ארבע שנים מיום תחילת החוק. בפס' 33 לעומת זאת מציינת הנשיאה ביניש כי יש מקום להארכת הוראת השעה.

77 המושג "הסכמה" עשוי להתפרש גם ביחס לשימוש באמצעי תקשורת שהזולת יכול לקלוט. ראו פס' 11 לפסק דינו של השופט וינוגרד בעניין ע"פ 48/87 **איתן ציחנובר נ' מדינת ישראל**, פ"ד מא(3) 5814 (1987): "המשוחח במכשיר קשר עם אחר, והוא יודע או אמור לדעת שניתן לקלטו [ב]מכשיר מתאים (והקולט אף יכול לשדר אליו בחזרה ולשוחח עמו), הופך את כל מי שקלט את השיחה לבעל שיחתו. הקשבת 'בעל השיחה' הזה לדברים שנאמרו בשיחה אינה 'האזנה לשיחת הזולת' ואינה איפוא 'האזנה' לפי החוק, ולכן בוודאי אינה 'האזנת סתר'". בעניין ת"פ (נצ') 62/92 **מדינת ישראל נ' סלאמנה אבו־רקיק**, פ"ד תשנ"ג (2) 342 הוחל אותו רציונל בנוגע למכשיר סלולרי אם ניתן ל"לקלטו במכשיר דומה או מתאים". עם זאת בהתחשב בתפיסה של היום את השימוש במכשור סלולרי (בהתעלם מההתפתחויות הטכנולוגיות שעלולות להקשות על קליטה פשוטה של תוכן תקשורת סלולרית), ספק אם קביעה זו עומדת במבחן האמריקאי של הצפייה הסבירה לפרטיות, ראו בחלק 3.1.2.1 **להלן**.

78 ס' 1 לחוק האזנת סתר.

משמו ואינו מוגבל להאזנה לשיחות שבעל פה. מעקב אחר רשתות תקשורת בישראל, לרבות רשת האינטרנט, הוא בבחינת האזנת סתר.

ההסדר הכללי בחוק האזנת סתר קובע כי האזנת סתר טעונה היתר בדין, והאזנה בלא היתר כאמור וכן שימוש ביודעין ובהיעדר סמכות בידיעה או בתוכנה של שיחה שהושגו בהאזנת סתר – דינם חמש שנות מאסר. עם זה בנסיבות מסוימות החוק מתיר עיון ושימוש גם בחומרי האזנת סתר שנתקבלו שלא כדין.[79] לשם הנוחות הפרוצדורלית של הגורם המבקש ניתן להוסיף על בקשת ההיתר להאזנת סתר[80] גם בקשה לקבלת נתוני תקשורת של יעד ההאזנה.[81]

2.5.2. האזנת סתר למטרת ביטחון המדינה

ראש הממשלה או שר הביטחון רשאים להתיר האזנת סתר אם ביקשו זאת בכתב ראש שירות הביטחון הכללי או ראש אגף המודיעין במטה הכללי, אם הדבר דרוש מטעמי ביטחון המדינה ובהתחשב בשיקולים של פגיעה בפרטיות. ההיתר יפרט את האדם או את המתקן שלהם תבוצע ההאזנה ואת דרכי ההאזנה שהותרו. דרישת הפירוט שבחוק יכולה להעיד על היעדר הסמכה לביצוע האזנה גורפת או יירוט תקשורת גורף, אך ייתכן שבחלופה שלפיה יש לפרט בהיתר את המתקן המיועד "לשמש לקליטה, להעברה, או לשידור של בזק" יש כדי להתיר איסוף גורף רק ממתקן מסוים (למשל של כל השיחות שנקלטות באמצעות אנטנת סלולר מסוימת).[82] אחת לשלושה חודשים יש

79 ס' 2ב לחוק האזנת סתר.

80 ראו חלקים 2.5.2, 2.5.3 **להלן**.

81 ס' 9ג לחוק האזנת סתר.

82 ס' 4(ב) לחוק האזנת סתר. כמו כן סיוג דרישת הפירוט ב"...והכל אם הם ידועים מראש", יכול לשמש פתח לפרשנות המתירה איסוף גורף. ראו לדוגמה את עניין עפ 2996/09 **פלוני נ' מדינת ישראל** (פורסם בנבו, 11.5.2011), שבו בין השאר נדונה חוקיותה של האזנת סתר למכשיר טלפון שהוצב בקיוסק ושימש הלכה למעשה טלפון ציבורי, אך אין הוא "טלפון ציבורי שהציבה (לדוגמה) חברת בזק, אשר לגביו יש לאדם מן הישוב ציפיות סבירות הראויות להגנה" (**שם**, בפס' נט). בנוגע להאזנות סתר לשיחות טלפוניות וסלולריות, לצד האיסור המשפטי על פגיעה לא מידתית בפרטיות, המגבלות הטכנולוגיות של עיבוד החומר, הדורשות כוח אדם רב כדי להאזין לשיחה, לתמלל ולמצות את המודיעין הרלוונטי שבה, הן שמתמרצות את גופי החקירה להגביל את היקף האיסוף לכל הפחות למינימום ההכרחי מבחינה מבצעית.

לעדכן את היועץ המשפטי לממשלה על ההיתרים שניתנו.[83]

במקרי האזנות סתר לשיחה שהעדות עליה חסויה,[84] שירות הביטחון הכללי נדרש לאישורו של נשיא בית משפט מחוזי או של סגן נשיא שהוסמך לכך. אישור כאמור יינתן אם שוכנע בית המשפט, מן הבקשה בכתב מאת ראש השירות, שיש יסוד לחשד שעורך דין, רופא, פסיכולוג, עובד סוציאלי או כוהן דת מעורבים בעבירה מסוג פשע שיש בה סכנה לפגיעה בביטחון המדינה, ושהאזנת הסתר דרושה מטעמים של ביטחון המדינה.[85]

לצורך איתורה או מניעתה של דליפת מידע ביטחוני שעלולה לגרום נזק חמור לביטחון המדינה, יש הסדר מיוחד להאזנות לעובדי מדינה או עובדי מערכת הביטחון. היתר כאמור יינתן לפי כללים חסויים שיקבע השר או ראש הממשלה.[86] במקרים שאינם סובלים דיחוי, וכאשר אי־אפשר לקבל היתר מהשר, ראש רשות ביטחון רשאי להתיר בכתב האזנת סתר לתקופה מוגבלת של 48 שעות. מתן ההיתר ידווח לשר, וזה רשאי לבטלו. אם ההאזנה היא לשיחה חסויה, יש לדווח ליועץ המשפטי לממשלה, וזה בתורו רשאי לבטל את ההיתר.

הסמכויות שהוקנו לשר הביטחון ולראש הממשלה מכוח החוק אינן ניתנות להאצלה.[87] ראש הממשלה או שר הביטחון ידווחו מדי שנה לוועדה משותפת של ועדת החוקה, חוק ומשפט ושל ועדת החוץ והביטחון של הכנסת על מספר ההיתרים להאזנת סתר שניתנו למטרות אלו, והדיון ייערך בדלתיים סגורות.[88]

83 ס' 4 לחוק האזנת סתר.

84 ס' 9 לחוק האזנת סתר מבהיר כי אין בהוראותיו כדי להתיר האזנות סתר לשיחות שעדות עליהן חסויה לפי סעיפים 48–51 לפקודת הראיות – עדות של עורך דין, רופא, פסיכולוג וכוהן דת.

85 ס' 9א לחוק האזנת סתר. כאשר סעיף זה התווסף לחוק האזנת סתר (במסגרת תיקון מס' 1), העביר ראש הממשלה יצחק רבין מכתב לוועדת החוקה, חוק ומשפט, ובו סירב "להרחיב את הביקורת השיפוטית על כלל האזנות הסתר למטרות ביטחון המדינה מאחר שהדבר יביא לפגיעה בבטחון המדינה" והדגיש כי כבר בהסכמתו של ראש השב"כ להכפיף האזנת סתר לשיחות חסויות לביקורת שיפוטית "יש כדי לפגוע ביכולת השב"כ למלא את משימותיו". ראו אלון גדעון "הצעת חוק מטילה על השב"כ איסור לבצע האזנת סתר לכהני דת מוסלמים בישראל ובמז' י–ם ללא היתר בימ"ש" **הארץ** 28.3.1995.

86 ס' 4א לחוק האזנת סתר.

87 ס' 14(א) לחוק האזנת סתר.

88 ס' 4(ה) לחוק האזנת סתר.

2.5.3. האזנת סתר למניעת עבריינות ולגילויה

האזנות סתר למטרות של גילוי, חקירה או מניעה של עבירות מסוג פשע, או לגילוי ותפיסה של עבריינים שעברו עבירות כאמור, טעונה היתר בצו של נשיא בית משפט מחוזי או של סגן נשיא שהוסמך לכך, לבקשת קצין משטרה מוסמך, בהתחשב בשיקולי פגיעה בפרטיות.[89] ההיתר יפרט את האדם או את המתקן שלהם תבוצע ההאזנה ואת דרכי ההאזנה שהותרו. ההיתר מוגבל בזמן ולא יעלה על שלושה חודשים. במקרים שאינם סובלים דיחוי, אם שוכנע מפכ"ל המשטרה כי האזנת סתר נחוצה למטרות המנויות לעיל, הוא רשאי להתיר בכתב האזנת סתר לתקופה מוגבלת של 48 שעות. היתר כאמור ידווח ליועץ המשפטי לממשלה, וזה רשאי לבטלו.

לפי הוראות החוק,[90] על שר המשטרה לדווח מדי שנה לוועדת החוקה, חוק ומשפט של הכנסת על מספר ההיתרים להאזנה שניתנו למטרות אלו. בחינתם של דיווחים אלו בשנים 2016–2002 מעלה כי בתקופה זו מספר הבקשות לאישור האזנות סתר שהוגשו לבחינת בית המשפט שילש את עצמו. בכלל התקופה (2016–2002) דחה בית המשפט 0.34% מבקשות אלה, ובחמש השנים האחרונות (2016–2011) קטן שיעור הדחייה ועמד על 0.16% בלבד (לוח 4).

89 ס' 6 לחוק האזנת סתר.

90 ס' 6(ז) לחוק האזנת סתר. בשנת 2011 דחה הממונה על יישום חוק חופש המידע במשרד הביטחון את בקשת האגודה לזכויות האזרח לקבל נתונים על היקף השימוש בסמכות להתיר האזנות סתר למטרות ביטחוניות. עתירת האגודה לזכויות האזרח לבית המשפט נדחתה בבית המשפט המחוזי בשבתו כבית משפט לעניינים מינהליים (עת"מ (י-ם) 3 **האגודה לזכויות האזרח בישראל נ' משרד ראש הממשלה** (פורסם בנבו, 14.5.2014)), וכך גם הערעור על החלטת בית המשפט המחוזי בעניין (עע"מ 4349/14 **האגודה לזכויות האזרח בישראל נ' משרד ראש הממשלה** (פורסם בנבו, 3.11.2015)). עם זאת בדחיית הבקשה לדיון נוסף (דנ"מ 8020/15 **האגודה לזכויות האזרח בישראל נ' משרד ראש הממשלה** (פורסם בנבו, 8.6.2015)) ציין המשנה לנשיאה השופט אליקים רובינשטיין בפסקה יג לפסק דינו כי גם בהיעדר חובה סטטוטורית למסור את המידע, "לא בשמים היא מסירת מידע בגדרי האיזון [...] נהוג לדבר על אמון הציבור; זהו כמובן מושג עמום ולעתים חמקמק, אך עדיף עשרת מונים גילוי יזום על הידרשות מאוחרת להדלפות וסחרור. לדעתי, ככל שיגבר הגילוי הוולונטרי, כן יגבר האמון באותם מקרים שבהם עומדת הרשות על אי גילויו הלגיטימי של מידע בסייגים של החוק".

לוח 4
האזנות סתר למטרות של מניעת עבירות או גילוין[91]

שנה	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	1520	2016
בקשות להאזנת סתר	1,095	1,031	962	996	1,255	1,484	1,797	2,220	2,283	2,682	2,844	3,094	3,310	3,217	3,309
היתרים להאזנת סתר	1,089	1,025	959	982	1,248	1,473	1,781	2,213	2,276	2,676	2,840	3,092	3,300	3,214	3,303
בקשות שנדחו	6	6	3	14	7	11	16	7	7	6	4	2	10	3	6
מספר המואזנים		557	632	614	778	958	1,022	1,288	1,411	1,919	1,777	2,127	2,189	1,926	2,279
מספר קווי בזק	1,100	881	1,024	979	1,205	1,925	2,213					4,276	4,254	4,494	5,108
פרשיות שטופלו בהאזנת סתר						346	440	534	603	697	816				
שיעור דחיית הבקשות להאזנת סתר	0.55%	0.58%	0.31%	1.41%	0.56%	0.74%	0.89%	0.32%	0.31%	0.22%	0.14%	0.06%	0.30%	0.09%	0.18%

בדומה לאמור לעיל בדבר השיעור המזערי של דחיית הבקשות לפי חוק נתוני תקשורת, יש להיזהר מהסקת מסקנות גם מנתונים אלו לבדם. בדומה לבקשות לנתוני תקשורת, גם את שיעור הדחיות הנמוך של בקשות להאזנת סתר אפשר אולי להסביר בנהלים ובבקרות של משטרת ישראל, המקפידים על הגשת בקשות מוצדקות בלבד; ואולם אפשר גם ששיעור הדחיות הנמוך מקורו בנטייה של בית המשפט להעדיף את האינטרס של שלום הציבור על פני הגנה על הזכות לפרטיות. את הגידול במספר האזנות הסתר, בדומה לאמור לעיל בעניין הגידול בבקשות לפי

91 מקור הנתונים: דיווחי המשרד לביטחון פנים לוועדת החוקה, חוק ומשפט של הכנסת, כפי שהתפרסמו באתר הוועדה.

חוק התקשורת, אפשר לייחס גם לשינויים ארגוניים במשטרת ישראל, בין השאר ההקמה של חטיבת הסיגינט (שינויים שמעידים על החשיבות הגדלה והולכת של כלי חקירה זה). ועדת החקירה הפרלמנטרית בנושא האזנות סתר הביאה את עמדתה של הנהלת בתי המשפט, ולפיה השיעור הנמוך של דחיית בקשות להאזנות הסתר אינו מעיד על אי־יעילות הפיקוח השיפוטי: "בית המשפט נדרש לאזן בין צורכי החקירה ובין הפגיעה בפרטיות. הדרך לעשות כן אינה בדחיית הבקשות להאזנת סתר לבדה, אלא בהטלת מגבלות על אופן ביצוע האזנת הסתר".[92]

2.5.4. האזנות סתר שאינן טעונות היתר

לעניין המעקב אחר רשתות תקשורת, יש לתת את הדעת על החריג בסעיף 8 לחוק האזנת סתר, שפוטר מהצורך בהיתר האזנת סתר לשיחות שנעשות ברשות הרבים, אם נעשו בידי מי שהוסמך לכך לשם מטרות של שמירה על ביטחון המדינה או לתכליות של מניעת עבירות או גילוי עבריינים. משמע, ניתן לבצע האזנה לשיחות ברשות הרבים ללא דרישת הסמכה מיוחדת "אגב הקלטה גלויה שנועדה לפרסום ברבים או למחקר".[93] רשות הרבים מוגדרת לפי מבחן של סבירות – "מקום בו אדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו".[94] מאחר שלפי חוק האזנת סתר שיחה היא גם תקשורת מקוונת, אפשר לראות בסעיף כזה שמאפשר מעקב אחר תקשורת גלויה ברשת האינטרנט, לרבות תקשורת גלויה ברשתות חברתיות (לדוגמה פרסומים על גבי ה"קיר" בפייסבוק). ואכן, שירות הביטחון הכללי ומשטרת ישראל משתמשים בחומרי מודיעין גלויים שמקורם באינטרנט ובעיקר ברשתות חברתיות.[95]

92 ועדת החקירה הפרלמנטרית בעניין האזנות סתר, סיכום דיוני הוועדה (26.1.2009) סימוכין 00416809 בעמ' 9.

93 ס' 8 לחוק האזנת סתר.

94 בדין האנגלי המודרני, בעקבות הזרמת דיני זכויות האדם האירופיים (ראו חלק 3.3.1 **להלן**), נעשה שימוש במבחן ה"ציפייה הסבירה לפרטיות" (Reasonable Expectation of Privacy). ראו Tanya Alpin, Lionel Bently, Philip Johnson & Simon Malynicz, Gurry on Breach of Confidence 6.95–6.105, 13.16 (2012)

95 ראו לדוגמה עפרי אילני "האח הגדול מתעניין בשירה" **דה מרקר** 13.11.2007; נעה שפיגל "שוטרים איימו על פעיל שהתכוון להשתתף בהפגנה: 'כל אחד יכול לעמוד עם שלט'?" **הארץ** 25.6.2017; יניב קובוביץ' "הרשתות החברתיות הפכו לכלי משמעותי

לא ברור אם שירות הביטחון הכללי רואה במעקב אחר תקשורת מקוונת שאינו טעון היתר, לרבות מעקב אחר פרסומים גלויים ברשתות חברתיות, איסוף לגיטימי של אוסינט (מודיעין ממקורות גלויים; OSINT — open source intelligence)[96] או "כלי איסופי" פולשני יותר.[97] על אף היות הפרסומים ברשתות החברתיות גלויים, הם אינם בהכרח שקולים למקורות הקלסיים של אוסינט (עיתונות ותקשורת), בהיותם בעלי אופי אישי יותר. ההקשר השונה של פומביות המידע הזמין ברשתות החברתיות וכן היקפו מעלים דילמות חדשות בנוגע להחלת מתודולוגיות

עבור המשטרה. המטרה: פעילים חברתיים" **הארץ** 6.2.2016; ברק רביד "בלוגר זומן לשיחת אזהרה בשב"כ בגלל ציוץ בטוויטר" **הארץ** 19.05.2014; אילן ליאור "המשטרה עקבה אחר דפי הפייסבוק של מובילי המחאה החברתית כדי לגבש ראיות נגדם" **הארץ**, 11.2.2013. לדיון בנוהלי ההזמנות של שירות הביטחון הכללי לשיחות תחקור ראו בג"ץ 5277/13 **האגודה לזכויות האזרח בישראל נ' שירות הביטחון הכללי** (2017).

96 אמ"ן וגופים אחרים מנתחים מגמות מקרו ברשתות חברתיות במסגרת איסוף אוסינט. ראו לדוגמה מיה אפשטיין "כך אוסף צה"ל מידע מודיעיני על האיום הבא ברשתות החברתיות" **דה מרקר** 4.4.2013. לפי הנחיות ה־CIA (ראו **להלן** בפרק זה ה"ש 97), "מידע גלוי" (publicly available information) עשוי לכלול בין השאר ניטור פעילות ברשת טוויטר, חשבונות פייסבוק (שהגישה אליהם איננה מוגבלת) ומאגרי מידע שהגישה אליהם מבוססת על תשלום. לפי ההנחיות, על איסוף גורף (bulk collection, שנעשה ללא שימוש במילות חיפוש מוגדרות או במזהים ספציפיים) של מידע גלוי או לא גלוי, חלה לפחות החובה הבסיסית של תיעוד (**שם**, ס' 5,1(a)).

97 במכתבו מיום 26.4.2007 ליועץ המשפטי לממשלה (סימוכין מ/504688/0704) הבחין ראש שירות הביטחון הכללי יובל דיסקין בין מחקר מבוסס חומרים גלויים ובין שימוש ב"כלים איסופיים" שפוגעים בפרטיות כגון האזנות סתר: "אשר לפעילות שאינה בלתי חוקית – כאשר פעולתו של גוף 'מתחככת' עם פגיעה בסדרי המשטר הדמוקרטי ומוסדותיו, אזי מתפקידו של השירות לאסוף ולנתח מידע הנוגע לפעילותו של גוף זה [...] ככלל, כאשר מדובר בפעילות גלויה ופומבית, השירות ינקוט בדרך של ריסון ולא יפעיל בעניין זה כלים איסופיים, אלא יסתפק בעיון לימוד ומחקר על בסיס חומרים גלויים בלבד. לעומת זאת, כאשר יש בסיס לחשד כי מתקיימת פעילות בעלת מימדים חתרניים שלה מאפיינים חתרניים – פעילות זו עשויה להצדיק שימוש גם בכלים איסופיים [...] במטרה לחשוף את המסתתר מאחורי פעילות כזו ועל מנת להבטיח שאין בה הסתרה של פעילות שלא בהתאם לחוק" (אוחזר מתוך /www.acri.org.il/pdf shabakresponse.pdf). גם הנחיותיה של סוכנות הביון המרכזית (CIA) מבחינות בין סוגים של איסוף מודיעין על מי שהוא "אדם אמריקאי" לפי רמת החדירה לפרטיות: איסוף בסיסי, הכולל בין השאר בדיקת מקורות גלויים; איסוף סטנדרטי (איסוף שאינו בסיסי או מיוחד); ואיסוף מיוחד (לרבות חיפוש פיזי ומעקב אלקטרוני), ראו Central Intelligence Agency Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333 §4 (להלן: הנחיות ה־CIA).

של אוסינט בעניינם.[98] אף שגופי האיסוף הישראליים מודעים להיעדר ההסדרה בתחום,[99] לא ידוע כיצד הם – בייחוד אלה שעוקבים אחר החברה האזרחית בישראל – נוטים לסווג טכניקות של איסוף מודיעין ברשתות חברתיות כאיסוף של "מודיעין גלוי" גרידא:[100] האם בעיניהם "שאיבת" כל פרסום גלוי ברשתות החברתיות וניתוחו בכלים סטטיסטיים רבי עוצמה היא פרקטיקה לגיטימית של מודיעין גלוי? מה דינם של פרסומים המגבילים את הרשאתם ל"חברים בלבד"?

2.5.5. מחיקה וביעור של חומר האזנה

החוק אינו קובע כללים בקשר למחיקה, לביעור ולתנאי ההחזקה של חומר ששמירתו נדרשת מטעמי ביטחון המדינה, ומסתפק בהסכמת ראש הממשלה בהסכמת שר המשפטים לקביעת הכללים בעניין.[101] כללים אלו חשאיים ולא התפרסמו ברשומות או בדרך אחרת.

98 דייוויד קריס תוהה אם איסוף מידע גלוי מרשתות חברתיות צריך שיתבצע למשל על בסיס רמת חשד מסוימת, או אם סוכן מודיעין רשאי להקים משתמש פיקטיבי כדי לאסוף מידע פומבי־למחצה (דוגמת פוסטים ברשתות חברתיות הזמינים למשתמשים מקטגוריות מסוימות. David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FFA and Beyond*, 8 J. Nat'l Sec. L. & Pol'y 377 (2015–2016), בחלק 3(f).

99 מפקדה לשעבר של יחידת האוסינט חצ"ב מציין כי "מדובר בתחום בו ההסדרה החוקית נמצאת בחיתוליה. במצב כזה מתעוררות סוגיות חוקיות ואתיות, כגון יצירת דמויות פיקטיביות ('אווטארים') והפרה של תנאי השימוש ברשתות החברתיות לצורכי איסוף מודיעין. יש לציין, עם זאת, כי לא כל מה שמותר לגוף מודיעין רשמי לעשות מתוקף סמכותו החוקית, מותר לחברה אזרחית או מסחרית". סא"ל ר' "אתגרים במיצוי מודיעין מהמדיה החברתית" **אתגרי קהילת המודיעין בישראל** 129, 135 (שמואל אבן ודוד סימן טוב עורכים, 2017).

100 לפיד מציין כי "מרכז הכובד בדרך הפעולה של האוסינט עבר ממיון ותרגום של תקשורת ממסדית לכריית מידע ומידענות". שינוי זה כנראה הביא לידי "בלבול וערבוב בין מושגים, כגון בין אוסינט, ובינט, כריית מידע, אנליזה רשתית ועוד" שאותו מזכיר סא"ל ר' (**שם**, בעמ' 131). דוגמאות לעירוב מושגי זה ניתן למצוא במאמרו של לפיד על האתגרים הניצבים בפני האוסינט בסביבת המידע החדשה, שעימם הוא מונה את הצורך ל"מציאת פתרונות להתגברות על מידע מאובטח" ומזכיר כי רשתות מאפשרות "לשירותי מודיעין להפעיל אמצעי איסוף אקטיביים, כמו להחדיר סוכנים וירטואליים בזהויות בדויות או מושאלות". ספק אם מתודולוגיות אלו, שאינן אוסינט קלסי, נבחנו באספקלריה של פגיעה בפרטיות. ראו אפרים לפיד "אתגרי המודיעין הגלוי בעידן המידע" **אתגרי קהילת המודיעין בישראל** 123 (שמואל אבן ודוד סימן טוב עורכים, 2017).

101 ס' 9ב(א) לחוק האזנת סתר.

קצין משטרה מוסמך רשאי להורות על מחיקה וביעור של חומר שנאסף לצורך גילוי עבריינים ומניעת עבירות בתנאי שחומר זה אינו דרוש עוד למטרות אלה.[102] עם זאת חומר חקירה שהותר לביעור ולמחיקה יימחק רק בתום ההליכים המשפטיים ולאחר קבלת אישור בכתב מהתובע. זאת ועוד, לפי חוק האזנת סתר, מחיקת נתונים מסליל הקלטה מותנית בהיתר למחוק את כלל ההקלטות בסליל. כל עוד אי־אפשר למחוק את כל החומר המצוי על גבי דיסק אופטי, התקנות מורות על מניעת גישה, באמצעות תוכנה, לחומר שמחיקתו הותרה.[103]

2.5.6. קבילות ראיות שהושגו בהאזנת סתר אסורה

דברים שהושגו בדרך של האזנת סתר אסורה לא יהיו קבילים כראיה בבית המשפט אלא בהליך פלילי בשל עבירה לפי חוק האזנת סתר.

חריג נוסף לפסלות ראיות שנתקבלו בהאזנה אסורה הוא בהליך פלילי של פשע חמור (שעונשו מאסר של יותר משבע שנים), באישור בית המשפט מטעמים מיוחדים, לאחר שנשתכנע כי הצורך להגיע לחקר האמת גובר על שיקולי פרטיות. במקרה שבו האזנת הסתר בוצעה שלא כדין בידי מי שרשאי לקבל היתר להאזנת סתר, היא לא תהיה קבילה כראיה אלא אם נעשתה בטעות שבתום לב, אגב שימוש מדומה בהרשאה חוקית.

בעניין **אבוקסיס** דן בית המשפט המחוזי בקבילותה של האזנת סתר לשיחה בין המשיב לבן שיחו שבוצעה על סמך צו שהתיר האזנה לשיחות של אדם אחר. במקרה זה הניחו השוטרים המאזינים בטעות כי קיימת הרשאה חוקית, וכי ההאזנה למשיב הותרה להם בצו בלי שבדקו ביסודיות את לשונו. דעת הרוב בעניין **אבוקסיס** קבעה כי בהתחשב בנסיבות הקונקרטיות, טעות זו נעשתה בתום לב, וכי הראיות קבילות לפי החריג שבחוק.[104]

102 ס' 9ב(ג) לחוק האזנת סתר.

103 תקנת משנה 7(ב) לתקנות האזנת סתר.

104 ע"פ (ב"ש) 7336/97 **מדינת ישראל נ' שי אבוקסיס** (פורסם בנבו, 21.8.1998). להתייחסות לסעיף כדוגמה לכללי פסילת ראיות פרטיקולריים בדין הישראלי, ראו ע"פ 5121/98 **טורי רפאל יששכרוב נ' התובע הצבאי**, פ"ד סא(1) 461 (2006) בפס' 39, 69–79 לפסק דינה של השופטת ביניש.

2.6.
חוק השב"כ

בשנת 2002 נתקבל חוק השב"כ, המסדיר את מעמדו המוסדי של שירות הביטחון הכללי, את תפקידיו וסמכויותיו ואת הבקרה והפיקוח עליו.[105] סעיף 11 לחוק השב"כ מקנה לראש הממשלה את הזכות לקבוע כללים לעניין העברת נתונים ממאגרי מידע של בעל רישיון בזק לשירות הביטחון הכללי. מידע כאמור הוא "לרבות נתוני תקשורת ולמעט תוכן שיחה כמשמעותו בחוק האזנת סתר". לא ברור אם השירות מפרש מידע כזה פירוש מצמצם, שמוגבל לנתוני תקשורת של טלפוניה קווית וסלולרית; או שמא פירוש מרחיב, שכולל גם נתוני תקשורת על רשת האינטרנט (IP, נתוני תקשורת דוא"ל, היסטוריית גלישה וכדומה).

בכללים אלו רשאי ראש הממשלה לקבוע כי סוגי מידע מסוימים שמצויים במאגרים של בעלי רישיון דרושים לשירות הביטחון הכללי לצורך מילוי תפקידו, וכי על בעל הרישיון להעביר מידע כזה לשירות. שימוש במידע זה ייעשה לפי היתר מראש השירות, לאחר ששוכנע כי השימוש דרוש לצורך מילוי תפקידיו לפי חוק זה. ההיתר יהיה לתקופה שלא תעלה על שישה חודשים, אך ראש השירות רשאי לשוב ולחדשו. החוק קובע כי גם הוראות בדבר החזקת מידע, שמירתו, אבטחתו, ביעורו או מחיקתו ייקבעו בכללים שינסח ראש הממשלה. ייתכן שנוסח הסעיף המגביל את ה"שימוש" במידע – בשונה מהנסיבות שבהן על בעלי רישיון בזק להעביר את המידע – מהווה בסיס משפטי ליצירת מאגר מידע רחב היקף של נתוני תקשורת המוחזק בשירות הביטחון הכללי[106] בדומה למודל ה־mass surveillance האמריקאי.

יש לציין כי הכללים שנקבעו מכוח סעיף 11 לחוק השב"כ נותרו חסויים. בהערות אגב של בית המשפט בעניין **חוק נתוני תקשורת** אוזכר עניין **התנועה לחופש**

105 להרחבה ראו אריה רוטר **חוק שירות הביטחון הכללי – אנטומיה של חקיקה** (2010); אלי בכר **ייעוץ משפטי בארגון בטחוני** (2013).

106 כמו שמשתמע מעמדת שירות הביטחון הכללי בפרשת הרפז, ייתכן שמאגר מידע כזה אכן קיים (ראו **להלן** בפרק 4 ה"ש 45).

המידע נ' משרד התקשורת,[107] שלפיו "אכן ישנם נספחים ביטחוניים סודיים המסדירים העברת נתוני תקשורת מחברות התקשורת לשירות הביטחון הכללי. עם זאת המשיבים שם מבהירים כי נספחים אלו אינם מסדירים את סמכויות שירות הביטחון הכללי לקבל את נתוני התקשורת אלא רק את האמצעים הטכניים לקבלתם, וכי הסמכויות לקבלת הנתונים כפופות לדין המהותי המסדיר אותן."[108]

- הדין הישראלי בנוגע למעקב מקוון שמפעילה המדינה מסדיר בחוק האזנת סתר את היירוט של נתוני תוכן למטרות של אכיפת חוק ומניעת פשיעה וכן למטרות ביטחוניות.
- ההוראות של חוק נתוני תקשורת מסדירות את האופן שבו המשטרה ורשויות חוקרות אחרות רשאיות להשיג נתוני תקשורת מבעלי רישיון בזק לתכליות של אכיפת חוק.
- סעיף 11 לחוק השב"כ הוא הבסיס הסטטוטורי להשגת נתוני תקשורת כאלה על ידי שירות הביטחון הכללי, אך הוראותיו נותרות חשאיות.
- הביקורת השיפוטית על בקשות להאזנת סתר ולנתוני תקשורת מוגבלת רק לבקשות כאלה לתכליות של אכיפת חוק, ואילו פעילותו של שירות הביטחון הכללי אינה טעונה צו מבית המשפט. פעילות האיסוף של אגף המודיעין של צה"ל כמעט שאינה מוסדרת, וזו של המוסד לתפקידים מיוחדים כלל לא.
- סוגיות רבות נותרו בגדר צריכות ובירור פרשני או הסדרה קונקרטית כמו למשל רגולציה של אוסינט ברשתות חברתיות; הסדרה פרטנית של הכללים המתירים או אוסרים איסוף גורף (bulk collection) של נתוני תקשורת; או הסדרה של שימור נתונים (data retention).

107 עת"מ 890/07 **התנועה לחופש המידע נ' משרד התקשורת** (פורסם בנבו, 5.11.2007). העתירה בעניין התנועה לחופש המידע נ' משרד התקשורת נמחקה בהסכמת הצדדים.

108 כלשונה של הנשיאה (בדימוס) ביניש בפס' 37 לעניין **חוק נתוני תקשורת**, **לעיל** בפרק זה ה"ש 69.

פרק 3
מעקב אחר רשתות תקשורת: דין השוואתי

ישראל איננה המדינה היחידה שבה חלק ניכר מהאוכלוסייה משתמש ברשת המקוונת, חבר ברשתות חברתיות או מחזיק בכיסו מכשיר שעוקב בכל עת אחר מיקומו; והיא איננה המדינה היחידה המתמודדת עם איומי טרור וביטחון, שמתמרצים את הרשויות האמונות על סיכולם לאסוף מודיעין מכל מקור זמין, לרבות מרשתות תקשורת.

כמו שנראה בהמשך הניתוח ההשוואתי, בעקבות נתוני פתיחה היסטוריים ואידאולוגיים שונים עוצבו מגוון של דינים והשקפות בנוגע למקומה של הזכות לפרטיות ולאופן שבו יש לפקח על מעקב מקוון של המדינה. התפיסות השונות של הפרטיות יכולות להסביר את ההבדל בין המודל המבוזר של דיני הגנת הפרטיות במגזר הפרטי בארצות הברית ובין האסדרה הריכוזית והמפורטת באירופה; הזיכרון של אפלת ימי השטאזי והגסטאפו יכולים לבאר את הקנאות לפרטיות בגרמניה; וחקיקת החירום והסמכותניות, ירושת השלטון הבריטי, יכולים לשפוך אור על ההגנה הרופפת על הפרטיות בהודו.

3.1. ארצות הברית

בעמודים הבאים תתואר המסגרת הנורמטיבית הנוגעת לדיני ההגנה על הפרטיות החלים על מעקב של מדינה אחר רשתות תקשורת בארצות הברית. דיני הפרטיות שם פזורים לפי נושאיהם ומושאיהם, ואין בהם חובה כללית להגנה על פרטיות, שממנה נגזרים פטורים שונים לפי העניין. כך למשל חוק

הפרטיות (The Privacy Act)[1] חל על מאגרי מידע של סוכנויות פדרליות,[2] ולא על אלה של גופים פרטיים.[3]

ג'יימס ויטמן טוען כי ההבדלים בין דיני הפרטיות בארצות הברית לאלה שבדין האירופי נובעים בין השאר מתפיסות שונות של פרטיות: הדין האירופי עוצב על בסיס תפיסה של פרטיות כאלמנט של זהות עצמית וכבוד סגולי (dignity), ואילו דיני הפרטיות האמריקאיים מושתתים על תפיסה של הפרטיות כחירות משלטון עריץ,[4] שמקורה הנורמטיבי בתיקון הרביעי ובתיקון הראשון לחוקה.[5] הזכות הכללית לפרטיות אינה מופיעה שם כזכות חוקתית.[6]

3.1.1. הבחנות מקדימות

חוק הפרטיות בתקשורת אלקטרונית (ECPA - Electronic Communications Privacy Act 1986),[7] המסדיר ברמה הפדרלית מעקב של המדינה אחר

1 5 U.S.C. §552a

2 רק בשליש ממדינות ארצות הברית יש חקיקה כזאת הנוגעת לסוכנויות ברמת המדינה.

3 חוק זה נועד להגן על הפרט מחשיפה של נתונים עליו המצויים במאגרים אלה, וכן לאפשר לו גישה אליהם ולעדכנם או לתקנם במידת הצורך. בסעיף §552a(j) החוק מסמיך את ראשי הסוכנויות לקבוע כללים הפוטרים מהוראותיו מאגרי מידע שקשורים לאכיפת החוק ולביטחון לאומי. בהקשר זה יוזכר ה־Computer Matching and Privacy Act – תיקון לחוק הפרטיות שנועד להסדיר נהלים של שיתוף מאגרי מידע בין סוכנויות פדרליות. שימוש של סוכנויות פדרליות אזרחיות במאגרי "רשימות שחורות" שמקורן בסוכנויות הביטחון – כגון השימוש ברשימת המעקב אחר טרוריסטים או ברשימת מסורבי הטיסה של ה־FBI – כנראה אינו מוסדר בחוק זה, אלא בכללים פרטניים שנקבעו לפי החריגים בחוק. ראו Margaret Hu, *Big Data Blacklisting*, 67 Fl. L. Rev. 1735 (2015)

4 ראו Whitman, **לעיל** בפרק 2 ה"ש 35.

5 ראו למשל את דעת המיעוט של השופט ברנדייס בעניין Olmstead v. United States 277 U.S. 438, 471–85 (1928): "[The makers of our Constitution] conferred, as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men"

6 ראו טנא, **לעיל** בפרק 2 ה"ש 35, בעמ' 52-53.

7 Electronic Communications Privacy Act 1986, 18 U.S.C §§2510–2522, 2701–2711, 3121–3127 (להלן: ECPA).

תקשורת אלקטרונית, מבחין בין שלושה סוגי תקשורת: (1) תקשורת בעל פה (oral communication) – דברים שאומר בעל פה אדם שבצדק מצפה שהם לא ייורטו. כשתקשורת כזאת מיורטת, הדבר נעשה לרוב באמצעות מתקני ציתות, הקלטה ושידור;[8] (2) תקשורת קווית (wire communication) – כל תקשורת שמבוססת על קול אנושי (aural transfer) שבין שידורה לקליטתה נעשה שימוש בכבלים או בחיווט אחר;[9] (3) תקשורת אלקטרונית (electronic communication) המוגדרת ככל תקשורת שאינה קווית ואינה בעל פה.[10]

נתוני תוכן ונתוני תקשורת

הספרות מזהה בדרך כלל את מקור ההבחנה האמריקאית בין נתוני תוכן (data) לנתוני תקשורת (metadata), באמצעות החלטת בית המשפט בעניין *Ex parte Jackson*,[11] שהבחינה בין פתיחת מעטפה ועיון בתוכנה ובין קריאת פרטי השולח והנמען הכתובים עליה. בעניין *Jackson* הוציא בית המשפט את המעטפת החיצונית של דברי דואר מגדרי הגנת התיקון הרביעי לחוקה (ראו להלן).[12] פסקי הדין בעניין *Katz* ו־*Smith* חידדו את ההבחנה בין תוכן ל־metadata בכל הנוגע לתקשורת מודרנית.[13] בעניין *Katz* נקבע כי יירוט תוכנן של שיחות טלפון הוא בגדר חיפוש שכפוף להוראות התיקון הרביעי לחוקה, ובעניין *Smith* נקבע כי איסוף באמצעות מתקן pen register[14] של מספרי טלפון שחויגו אינו כזה.

8 18 U.S.C. §2510(2)

9 18 U.S.C. §2510(1)

10 18 U.S.C. §2510(12)

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

12 ראו חלק 3.1.2.1 **להלן**.

13 Katz v. United States, 389 U.S. 347 (1967); Smith v. Maryland, 422 U.S. 735 (1979)

14 מתקן pen register מוגדר כמכשיר שמקליט או מפענח אותות יוצאים של נתוני חיוג, ניתוב, הפניה או איתות "dialing, routing, addressing, or signaling information" ממכשיר או ממתקן לתקשורת אלקטרונית (3)§3127. מתקן דומה הוא trap and trace, שמיירט אותות אלקטרוניים נכנסים שהם נתוני חיוג, ניתוב, הפניה או איתות שיש בהם כדי לזהות את מקור התקשורת הנכנסת (4)§3127. והכול בתנאי שמידע המיורט באמצעות מתקנים משני הסוגים אינו כולל את תוכן התקשורת.

ההבחנה בין תוכן ל־metadata רלוונטית לא רק לתיקון הרביעי לחוקה, אלא נמצאת גם בחקיקה עצמה. במסגרת הסדרי החקיקה של חוק הפרטיות בתקשורת אלקטרונית (ECPA) שונתה ההגדרה של "תוכן" כדי שלא תכלול את זהות הצדדים המתקשרים ואת עצם קיומה של התקשורת ביניהם.[15] כך עולה גם מלשון חוק האזנות סתר (WTA – Wiretap Act),[16] שבעניינו נראה כי סעיף 2511 נועד בעיקר לאיסוף נתוני תוכן.[17] נתוני תוכן מוחרגים מתחולתו של חוק איסוף נתוני תקשורת (PRA – Pen Register Act),[18] שנועד להסדיר את כללי איסופם של נתוני תקשורת מסוימים.[19] גם חוק תקשורת שמורה (SCA – Stored Communication Act)[20] מבחין בין תוכן ל־metadata.[21]

עם זאת יש הטוענים כי הסדר החקיקה של חוק הפרטיות בתקשורת אלקטרונית (ECPA) משמיט קטגוריה שלישית של נתונים שמצויים בתווך בין "תוכן" לנתוני תקשורת במובנם הצר כ־"נתוני איתות".[22] ההבחנה הדיכוטומית בין תוכן ל־metadata מיטשטשת כשמדובר בסוגים מסוימים של מידע – נתוני גלישה

15 David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 1 Stan. Tech. L. Rev 1 (2005)

16 Wiretap Act,18 U.S.C §§2510-2522 (להלן: WTA).

17 הוראות אותו סעיף חוזרות ומדגישות את המילה "תוכן". גם המונח "יירוט" מתייחס ליירוט של תוכן (§2510(4)).

18 Pen Register Act, 18 U.S.C §§3121-3127 (להלן: PRA). ראו §3121(c) סיפה ו־§3121(d) סיפה.

19 ראו הגדרות pen register ו־trap and trace, **לעיל** בפרק זה ה"ש 14.

20 Stored Communications Act, 18 U.S.C §§2701-2711 (להלן: SCA).

21 השוו §2703(a)-(b), החל על נתוני תוכן, ל־§2703(c), שחל על נתונים שאינם בגדר תוכן.

22 ב"נתוני איתות" הכונה לסוג המידע שמתעדים מתקני Pen Register ו־Trap and Trace, כמשמעותם ב־PRA (ראו **לעיל** בפרק זה ה"ש 14). לאפשרות קיומה של קטגוריה שלישית, ראו Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. Rev 607 (2003)

(URL), שדה ה"from" בכתובת דוא"ל[23] או נתוני תוכן סלולריים[24] – וההסדר החל על נתונים אלה אינו ברור. במקרים מסוימים יש הסוברים כי סוגי נתונים שנדמים כנתוני "הפניה או איתות" יכולים להיות נתוני תוכן.[25] האם היסטוריית גלישה – המורכבת מכתובות URL המכילות בתוכן את מילות החיפוש – היא נתון איתות "המשמש לחיוג, ניתוב, מיעון או איתות של מידע"?[26] או שיש במילות החיפוש האלו כדי ללמד על תוכן התקשורת?[27]

מידע מזהה אישי (PII)

דיני הגנת הפרטיות האמריקאיים משתמשים לעיתים במונח "מידע מזהה אישי" (PII — Personally Identifiable Information) כדי לציין את מהות המידע הפרטי המוגן.[28] הגדרתו של "מידע מזהה אישי" איננה אחידה,[29] והיא גם שונה ממקבילתה האירופית.[30] כך למשל מידע מזהה אישי מוגדר "מידע המאפשר

23 Steven M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell, *It's Too Complicated: How The Internet Upends Katz, Smith, And Electronic Surveillance Law*, 30 Harv. J. L & Tech. 1 51-56 (2016)

24 לשאלת תחולתן של הוראות ה־SCA על נתוני מיקום סלולריים ראו Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Maryland L. Rev. 677 (2011). מנגד הפסיקה נוטה שלא להתייחס לנתוני מיקום סלולריים כאל "תוכן" – ראו לאחרונה בעניין United States v. Graham 824 F.3d 421 (4th Cir. 2016) (en banc)

25 ראו Kerr, **לעיל** בפרק זה, ה"ש 22, בעמ' 628.

26 18 U.S.C. §3127

27 ראו Kerr, **לעיל** בפרק זה ה"ש 22, בעמ' 644-648.

28 ראו Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev, 1814 (2011)

29 **שם**, בעמ' 1828-1836. חוסר האחידות אינו רק ברמת החקיקה הפדרלית, אלא גם בחקיקה המדינתית — ראו Lisa J. Sotto, Privacy And Data Security Law Deskbook §15.02[B] (2013)

30 Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877 (2014)

לזהות אדם באופן אינדיווידואלי",[31] "מידע אישי שאינו פומבי",[32] "פריט מידע שבאמצעותו או בהצלבתו עם מידע אחר, סביר שיאפשר לזהות את מי שהוא "אדם אמריקאי"[33] או רשימה סגורה של סוגי נתונים המפורטים בדבר החקיקה.[34]

יש לציין כי בעידן המידע שאילתה במאגר מידע עלולה לפגוע בפרטיותו של אדם לא רק בשל שימוש בנתון מזהה חד־חד־ערכי (מספר תעודת זהות, למשל); גם חיפוש ממוחשב המצליב נתונים שיש בהם כדי לזהות אדם יכול להניב תוצאות הפוגעות בפרטיות. אף שדיני הגנת הפרטיות במגזר הפרטי משתמשים במושג PII,[35] הדינים הנוגעים למעקב אחרי רשתות תקשורת כמעט שאינם משתמשים בו ואינם מגדירים מהו המידע הפרטי המוגן.[36]

הרשות החוקרת

נוסף על גופי האכיפה והחקירה של המשטרה המקומית הפועלים ברמת המדינה ומופקדים על חקירת עבירות ופשיעה, קיימת גם קהילת המודיעין האמריקאית, הפועלת ברמה הפדרלית. קהילת המודיעין מורכבת מ־17 גופים

31 16 C.F.R. §312.2

32 15 U.S.C. §6809(4)(A)

33 ראו הנחיות ה־CIA, **לעיל** בפרק 2, ה"ש 97.

34 כך למשל החקיקה של מדינת מסצ'וסטס המסדירה התראות על אירועי אבטחת מידע, מגדירה "מידע אישי" כך: שם המשפחה (בצירוף שם פרטי או האות הראשונה של שמו הפרטי) של תושב כשהוא מצורף לאחד מסוגי הנתונים האלה: מספר הביטוח הלאומי שלו, מספר רישיון הנהיגה או מספר זיהוי אחר שהונפק לו מטעם המדינה, מספר כרטיס אשראי, מספר חשבון פיננסי אחר או סיסמאות גישה לחשבונות פיננסיים. ראו Mass. Gen. Laws Ann. ch. 93H, §3

35 ראו למשל The Children's Online Privacy Protection Act, 15 U.S.C. §§6501-6506 (2006); the Gramm-Leach Bliley Act, 15 U.S.C. §§6801-6809; the Video Privacy Protection Act, 18 U.S.C. §2710; the HITECH Act, Pub. L. No. 111-5, 123 Stat. 226 (2009)

36 הנחיות ה־CIA משתמשות במונח USPII (United State Person Identifying Information) – פריט מידע שבאמצעותו או בהצלבתו עם מידע אחר סביר שיתאפשר לזהות את מי שלפי הנחיות אלה הוא "אדם אמריקאי" (U.S. Person). ראו הנחיות ה־CIA, **לעיל** בפרק 2 ה"ש 97, ס' 12.25. בהנחיות משרד ההגנה ננקט מונח דומה – USPI. ראו DoD Manual 5240.01, Procedures Governing The Conduct Of DoD Intelligence Activities

וסוכנויות האוספים מידע על איומים מבית ומחוץ, בכללם הסוכנות לביטחון לאומי (NSA — National Security Agency), סוכנות הביון המרכזית (CIA — Central Intelligence Agency) ולשכת החקירות הפדרלית (FBI — Federal Bureau of Investigation) או "הבולשת". בראש קהילת המודיעין עומד מנהל המודיעין הלאומי (ODNI - Director of National Intelligence), בעל תפקיד ברמה של חבר קבינט, המדווח ישירות לנשיא.[37]

הסוכנות לביטחון לאומי (NSA), השייכת למשרד ההגנה, היא שחולשת על פעילות הסיגינט של ארצות הברית. סוכנות הביון המרכזית (CIA) היא גוף הביון האזרחי לאיסוף, לעיבוד ולניתוח של מודיעין מחוץ לגבולותיה של ארצות הברית, על פי רוב באמצעים יומינטיים (HUMINT). הבולשת הפדרלית (FBI), הפועלת בחסות משרד המשפטים, פועלת כסוכנות ביון פנימית (לסיכול טרור וריגול־נגדי) וכן כגוף אכיפה וחקירה של פשיעה פדרלית. יש המבקרים את כפל המשימות שלה – כשירות חשאי וכגוף אכיפה – וקוראים להקמתם של שני גופים נפרדים.[38] מלבד החשש שמא ריבוי המשימות פוגע ביעילותה, עירוב התפקידים מעצים את החששות מזליגת מודיעין שהופק למטרות של ביטחון לאומי (ומכוח הסדרים המקלים על איסופו) לפעולות אכיפה ולחקירת עבירות.[39]

מעקב אחר אזרחים, מודיעין על זרים

דיני המעקב האמריקאיים עוצבו בהתאם להוראות התיקון הרביעי לחוקה (ראו להלן).[40] מי שאינם אזרחים אמריקאים או מצויים מחוץ לגבולותיה אינם זכאים – בהיעדר קשר הדוק למדינה – להגנות של תיקון זה.[41] מלבד

37 משרד מנהל המודיעין הלאומי הוקם בשנת 2005. קודם לכן שימש ראש ה־CIA גם בתפקיד מקביל של מנהל המודיעין המרכזי. לפי ההסדר הנוכחי, מנהל המודיעין הלאומי מנוע מלעמוד במקביל בראשותה של סוכנות מודיעין אחרת, לרבות ה־CIA.

38 ראו למשל Richard A. Posner, Uncertain Shield 101–102 (2006). יוער כי בגרמניה הפרדת התכליות בין השירות החשאי למשטרה (*Trennungsgebot*) היא עיקרון מעין חוקתי. ראו בטקסט המפנה לה"ש 849 **להלן** בפרק זה.

39 ראו גם Laura K. Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age Chap. 1 (2016)

40 Donohue, **שם**, בפרק 4.

41 United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990). ראו גם ויסמונסקי **לעיל** בפרק 2 ה"ש 26, בעמ' 237–238.

התכליות והסמכויות הטריטוריאליות של סוכנויות המודיעין, חשובה ההבחנה בין מושאי המעקב הזכאים להגנות התיקון הרביעי לחוקה ולאלו שאינם זכאים לה.[42] כך למשל בחוק איסוף מודיעין זר (FISA – Foreign Intelligence Surveillance Act)[43] ההגדרה של מעקב אלקטרוני (שיעדיו המודיעיניים הם על פי רוב ישויות זרות וסוכניהן) – שטעון צו[44] – כוללת בין יסודותיה זיקה מסוימת לארצות הברית: מעקב אלקטרוני מוגדר כאיסוף תקשורת שצד לה הוא "אדם אמריקאי" (United States person),[45] או צדדים לתקשורת שאינם אדם אמריקאי אבל מצויים כולם בתחומי ארצות הברית[46]. מעקב אלקטרוני אחר יעדי מודיעין אלה נעשה בכפוף לצו מבית המשפט למודיעין זר (FISC – Foreign Intelligence Surveillance Court).[47] בכל הנוגע לאישור איסוף מודיעין על יעדים מודיעיניים שאינם אדם אמריקאי או שכולם אינם בתחומי ארצות הברית – יש הסדר נפרד שנהליו נוקשים פחות,[48] והוא אינו מחייב צו מבית המשפט למודיעין זר.

3.1.2. מעטפת חוקתית

3.1.2.1 התיקון הרביעי לחוקה

סמכויות החקירה של רשויות השלטון ונציגיהן מוגבלות בתיקון הרביעי לחוקה:

> לא תופר זכותם של בני אדם לביטחון בגופם, ביתם, תעודותיהם וחפציהם מפני חיפושים ותפיסות בלתי סבירים, ולא יוצאו צו חיפוש וצו תפיסה אלא על יסוד עילה סבירה, מחוזקת

42 ראו Lubin, **להלן** בפרק 4 ה"ש 2.

43 ראו חלק 3.1.5 **להלן**.

44 ראו למשל (2)(a)1805§. להגדרת "ישות זרה" (Foreign Power), ראו §1801(a).

45 50 U.S.C. §1801(i)

46 50 U.S.C. §1801(f)(3)

47 ראו בחלק 3.1.5 **להלן**.

48 ראו בחלק 3.1.7 **להלן**.

> בשבועה או בהן־צדק, ועם תיאור מפורט של המקום שיש לערוך בו חיפוש, ושל האנשים או החפצים שיש לתופסם.[49]

כלל, כל מעקב מקוון של הרשויות הנערך בתחומי ארצות הברית או אחרי מי שיש להם זיקה מסוימת לארצות הברית, צריך להיעשות לפי ההליך הנ"ל (בתנאי שפרקטיקת המעקב הרלוונטית אכן נופלת בגדרי "חיפוש" או "תפיסה"). מכאן שאת פרקטיקת המעקב יש להפעיל על יסוד עילה סבירה. בעניין *Weeks v. United States*[50] נקבעה פסלותן של ראיות שהושגו אגב הפרת הוראות החוקה. בהלכות מאוחרות יותר בוססה גם דוקטרינת "פירות העץ המורעל", שמכוחה ייפסלו ראיות כשרות שהושגו בהסתמך על ראיות פסולות.

בעניין *Katz*[51] פיתח בית המשפט את דוקטרינת הציפייה הסבירה לפרטיות (reasonable expectation of privacy) כמבחן דו־שלבי שקובע אם פרקטיקת חיפוש אינה מפרה את התיקון הרביעי לחוקה. במבחן זה על הטוען להפרת זכויותיו לפרטיות לפי התיקון הרביעי להראות כי הייתה לו (א) ציפייה סובייקטיבית קונקרטית לפרטיות בנסיבות העניין; וכי (ב) אותן ציפיות לפרטיות נחשבות סבירות. יש הסוברים כי החלת דוקטרינת הציפייה הסבירה לפרטיות בעידן הרשתות החברתיות – שבהן המשתמשים חושפים, מדעת ושלא מדעת, מידע אישי חשוב – יש בה כדי לצמצם במידה ניכרת את ההגנות על פרטיותם.[52]

כשבית המשפט העליון מעריך את חוקיותה של פרקטיקת חיפוש או תפיסה, הוא משתמש בין השאר בדוקטרינת הצד השלישי. לפי דוקטרינה זו, כשפלוני חושף מידע לצד שלישי, הוא אינו יכול לצפות לפרטיות במידע שחשף.[53] דניאל סולוב

49 חוקת ארצות הברית של אמריקה (ארנון גטפלד, תרגום, ללא שנה). מקוון.

50 Weeks v. United States, 232 U.S. 383 (1914)

51 ראו עניין *Katz*, **לעיל** בפרק זה ה"ש 13.

52 Shannon M. Oltmann, *Katz Out of the Bag: The Broader Privacy Ramifications of Using Facebook*, 47 Proc. of the Assoc. for Information Sci.& Tech. 1–4 (2010)

53 ראו United States v. Miller, 425 U.S. 435 (1976), המתייחס לרשומות בנקאיות, ועניין *Smith*, **לעיל** בפרק זה ה"ש 13, המתייחס להשגת רשימת מספרי טלפון שחייג מנוי מסוים באמצעות מתקן Pen Register.

סבור כי במציאות שבה מידע אישי רב מצוי בידי צדדים שלישיים במגזר הפרטי,[54] דוקטרינה זו עלולה לאיים על הזכות לפרטיות גם כשזו מעוגנת בהסכמה חוזית.[55]

עם זאת נראה כי הפסיקה נוטה לצמצם את תחולת דוקטרינת הצד השלישי לנתוני תקשורת, ולא להחילה באופן גורף על נתוני תוכן. בעניין *Smith* קבע בית המשפט כי אין ציפייה סבירה לפרטיות בנוגע לנתוני metadata של תקשורת טלפונית,[56] ובהמשך הסתמך על פסיקה זו בית המשפט למודיעין זר (FISC)[57] כדי לדחות טענות בנוגע לחוקתיותו של איסוף metadata באמצעות סוכנויות המודיעין.[58] גישה זו מתיישבת עם פסיקה מעידן טכנולוגי קדום, שהבחינה בין קריאת פרטי הנמען והמוען הגלויים שעל דברי דואר, ובין פתיחת מעטפות במסגרת חקירה.[59] המחוקק הפדרלי בחר להגיב על פסקי הדין המנחים בעניין דוקטרינת הצד השלישי בדברי חקיקה שהגבילו את הפרקטיקות הקונקרטיות שנידונו בהן. יתר על כן, בכמה מדינות דוקטרינה זו נדחתה בחקיקה או בהלכה, וברמת המדינה נפסק שיש ציפייה סבירה לפרטיות גם כשיש צד שלישי לתקשורת המסוגל לעיין בה.[60] כך למשל במדינות איידהו

54 Daniel J. Solove, *Digital Dossiers and the Dissipation of Forth Amendment Privacy*, 75 S. Cal L. Rev. 103 (2002)

55 כך בעניין *Miller*, **לעיל** בפרק זה ה"ש 53, הותר שימוש ברשומות בנקאיות שהעביר הבנק לסוכני רשות לאלכוהול, טבק ונשק.

56 ראו *Smith*, **לעיל** בפרק זה ה"ש 13.

57 ראו בחלק 3.1.5 **להלן**.

58 ראו In re Application of the Federal Bureau of Investigations for an Order Requiring the Production of Tangible things from [REDACTED], No. BR 13-109 slip op. at 6

59 ראו *Ex Parte* Jackson, **לעיל** בפרק זה ה"ש 11. כמו כן יוער כי כיום החוק הפדרלי מגביל את רשויות הממשל בכל הנוגע לפתיחת דברי דואר מקומיים סגורים (39 U.S.C. §3623(d)). עם זאת הפסיקה התירה חיפוש בדואר שמקורו מחוץ למדינה, ראו United States v. Various Articles of Obscene Merchandise, 395 F. Supp. 791 (S.D.N.Y), aff'd, 538 F, 2d 317

60 ראו Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogues to Protect Third Party Information from Unreasonable Seizure*, 55 Cath. U. L. Rev. 373, 395 (2006)

ואילינוי קבע בית המשפט כי בנוגע למספרי טלפון שחויגו חלה ציפייה סבירה לפרטיות.[61]

לאחרונה נבחנו גבולותיה של דוקטרינת הצד השלישי בעניין *Carpenter*. בפרשה זו השיגה הבולשת את היסטוריית המיקום של התאים הסלולריים (CLSI — Cell Site Location Information)[62] של חשודים בשוד בתקופות של 127 ו־88 יום כדי להצביע על קרבתם לזירות הפשע. בעקבות נתונים אלה הורשעו החשודים בבית המשפט הפדרלי ונגזרו עליהם יותר ממאה שנות מאסר.[63] בפסק דינו ציין בית המשפט הפדרלי כי לפי דוקטרינת הצד השלישי, לא הייתה לנאשמים ציפייה סבירה לפרטיות באשר לנתוני ה־CLSI שלהם. בהיעדר ציפייה סבירה לפרטיות התיקון הרביעי לחוקה אינו חל, ולכן סוכני הבולשת שהשיגו את הנתונים מספק התקשורת לא נדרשו לצו ואכן היו רשאים לפנות לחברת הסלולר לפי הוראות החוק המיוחד בדבר נתוני תקשורת שמורים (חוק תקשורת שמורה: SCA – Stored Communication Act), המקילות יותר.[64]

בערעורו לבית המשפט העליון טען מר קרפנטר, הנאשם העיקרי, כי אין להחיל את דוקטרינת הצד השלישי על נתוני CLSI. חוק התקשורת השמורה (SCA) נחקק בעידן שבו מכשירי טלפון סלולריים עלו אלפי דולרים, ולא היו נפוצים עד כדי היותם חלק בלתי נפרד מהחיים המודרניים. לטענת קרפטנר, יש להפעיל גישה עדינה יותר כלפי נתונים סלולריים, בייחוד בהתחשב בהיקפם ובדיוקם, ולא להניח שהימצאותם בידי צד שלישי משמעהּ ויתור על ציפייה סבירה לפרטיות. בית המשפט העליון, בהתייחסו ל"תנודות הססמיות בטכנולוגיה דיגיטלית", קיבל את הערעור והפך את החלטת בית המשפט הפדרלי בקובעו כי אין להחיל

61 State v. Thompson, 760 P.2d 1162, 1163–65 (Idaho 1988); People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993)

62 Cell site location information (CSLI) הם נתונים על מתקני תקשורת הסלולר הנייחים שמכשיר נייד מסוים השתמש בהם במהלך התקשורת שלו. אלו אינם בהכרח נתונים המספקים נתוני מיקום מדויקים, אך הם מאפשרים בסיס להערכת מיקום המכשיר.

63 United States v. Carpenter, 819 F.3d 880, 884–885 (2016)

64 ראו **להלן** בחלק 3.1.3.2.

את דוקטרינת הצד השלישי על נתוני CLSI. עם זאת, חרף הביקורת של שופטי המיעוט נמנע בית המשפט העליון מביטולה הגורף של הדוקטרינה.[65]

נוסף על בקרה שיפוטית על פרקטיקות חקירה קונקרטיות – שבמסגרתה במשך השנים בחן בית המשפט העליון טכנולוגיות שונות של ציתות, האזנה, הקלטה ומעקב[66] לפי הוראות התיקון הרביעי לחוקה – הפעיל בית המשפט כמה פעמים את סמכותו לבחון דברי חקיקה במנותק מאופן הפעלתם במקרה קונקרטי. כך למשל בעניין *Berger* פסל בית המשפט העליון סעיפים מסוימים בחוקי האזנת הסתר של מדינת ניו יורק שהפרו את הוראות התיקון הרביעי באפשרם ביצוע האזנת סתר לפרקי זמן ארוכים ללא בקרה שיפוטית מספקת.[67]

ההליך הכללי המתווה את צווי החיפוש והתפיסה מצוי בתקנות הפדרליות המסדירות את סדרי הדין הפליליים.[68] לפי ההליך, על הקצין הפועל לפי צו חיפוש שמקנה לו גישה מרחוק למידע אלקטרוני מאוחסן, לנקוט מאמץ סביר כדי למסור

65 Carpenter v. United States, 138 S. Ct. 2206 (2018). כן ראו Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, *in* William & Mary Bill of Rights 495 (2017); Alex Abdo*, Why Rely on the Fourth Amendment To Do the Work of the First?*, 127 Yale L.J. F. 444 (2017); Jordan M. Blanke, *Carpenter v. United States Begs for Action*, U. Ill. L. Rev. Online 260 (2018); Orin S. Kerr, *Initial Reactions to Carpenter v. United State*s, 14 USC Law Legal Studies Paper (2018); Paul Ohm, *The Many Revolutions of Carpenter*, 32 Harv. J. L. & Tech (forthcoming, 2019)

66 כך, בין השאר, בחן בית המשפט העליון את חוקתיות השימוש במתקני הדמיה טרמית כדי לעקוב אחרי מעשיו של פלוני בביתו (עניין Kyllo v. United States, 533 U.S. 27 (2001)), והתקנת משדר אותות GPS בחשאי לצורכי מעקב אחרי תנועת כלי רכב (United States v. Jones 132 S. Ct. 945 (2012)), וכן את חוקתיותו של צו לחיפוש מידע דיגיטלי במכשיר סלולרי שנתפס בהליך מעצר (Riley v. California, 134 S. Ct. 2473 (2014)). בעניין Texas v. Brown 460 U.S. 730 (1983); בית המשפט העליון אף נדרש לטענה שהשימוש בטכנולוגיית התאורה של פנס פשוט באזור חשוך בחיפוש לפי צו מפר זכויות מוקנות מכוח התיקון הרביעי.

67 Berger v. New York, 388 U.S. 41 (1967)

68 Fed. R. Crim. P. 41

העתק מן הצו לבעלים של המידע שנתפס או הועתק, או לאדם שברכושו נעשה חיפוש כאמור.[69] שופט יכול לאשר בצו דחייה במתן הודעה כזאת לפי דין.[70]

בעבר התייחסה הפסיקה לתחולת התיקון הרביעי על איסוף מודיעין לצורכי ביטחון לאומי וקבעה כי כשהאיסוף מקומי, הוא נותר כפוף לתיקון הרביעי. נראה כי לאחרונה הפסיקה נוטה לקבוע כי שימוש במכשור המדמה תאים סלולריים (IMSI catcher או Stingray) לצורך איסוף נתוני תקשורת סלולריים כפוף לתיקון הרביעי וטעון צו.[71] עם זאת העיר בית המשפט שהמבחנים שלפיהם תיבחן ההלימה של פרקטיקת האיסוף של מודיעין מקומי למטרות ביטחוניות עם הוראות התיקון הרביעי לחוקה עשויים להיות נוקשים פחות מהסטנדרטים לבחינת פרקטיקות מעקב לצורכי שיטור.[72] כך או כך בכמה מקרים קבעה פסיקה פדרלית כי התיקון הרביעי לחוקה אינו חל על פרקטיקות איסוף מודיעין חיצוני לצורכי ביטחון לאומי.[73]

3.1.2.2. התיקון הראשון לחוקה

חופש הדיבור, העיתונות, ההתאגדות, הדת והפולחן מעוגן בתיקון הראשון לחוקה האמריקאית. ניל ריצ׳רדס העיר כי מעקב מקוון מצד המדינה עשוי במקרים רבים לפגוע בחירויות אלו בשל האפקט המצנן שהוא גורר על פעילויות

69 Fed. R. Crim. P. 41(f)(1)(c)

70 Fed. R. Crim. P. 41(f)(3)

71 Prince Jones v. United States (No. 15-CF-332) D.C. 9.21.2017. וראו גם United States v. Lambis (No. 15-CR-734), S.D.N.Y (12.7.2016); United States v. Purvis Lamar Ellis (No. 13-CR-00818), N.D. Cal. (24.8.2017). להרחבה ראו גם מסמך מדיניות של משרד המשפטים האמריקאי בעניין טכנולוגיית הדמיה של תאים סלולריים: Department of Justice Policy Guidance: Use of Cell-site Simulator Technology (3.9.2015)

72 ראו United States v. U.S. Dist. Court, 407 U.S. 297 (1972), המוכר גם כעניין *Keith*. בעניין *Keith* שלל בית המשפט העליון את טענתו של ממשל ניקסון שהתיקון הרביעי אינו חל כשהנשיא מנהל מעקב לשם ביצוע חקירות מקומיות למען הביטחון הלאומי, אך ציין כי מעקב למטרות של ביטחון לאומי עשוי לכלול שיקולי מדיניות שונים מאלה הנכללים במעקב במסגרת חקירת "פשעים רגילים".

73 ראו United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974), United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980)

החוסות בחירויות אלו או בשל יחסי הכוחות שבין העוקב לנעקב: משזיהתה המדינה מתנגדים למשטר באמצעות מעקב, בכוחה להסב להם נזק באמתלות שונות ומשונות.[74] כך למשל ההוראות בחוק איסוף מודיעין זר (FISA) מציינות במפורש כי כדי לקבוע שפלוני הוא ישות זרה או סוכן של ישות זרה לצורך אישור מעקב אחריו, אין להסתמך אך ורק על מידע שמקורו בפעילויות המוגנות בתיקון הראשון לחוקה.[75] גם הפסיקה האמריקאית זיהתה מקרים שבהם הגנה על חירויות אלו נקשרה בהגנה על הפרטיות: בכמה וכמה פסקי דין נקבע כי כדי להגן על חופש ההתאגדות, אין לפרסם ברבים חברות בארגונים פוליטיים או להכריח אנשים לחשוף את חברותם זו.[76]

3.1.3. חוק פרטיות בתקשורת אלקטרונית (ECPA)

ברמה הפדרלית מעקב אחר תקשורת אלקטרונית מוסדר בחוק הפרטיות בתקשורת אלקטרונית (ECPA – Electronic Communications Privacy Act 1986), המורכב משלושה דברי חקיקה, שיפורטו להלן: חוק האזנות סתר (WTA – Wiretap Act), חוק תקשורת שמורה (SCA – Stored Communication Act) וחוק איסוף נתוני תקשורת (PRA – Pen Register Act).

יובהר כי כאשר על פרקטיקה מסוימת של מעקב מקוון חל הסדר מיוחד, אין די בהלימה שלה עם הוראות התיקון הרביעי לחוקה, ועליה להלום גם את הוראות החוק של פרטיות בתקשורת אלקטרונית (ECPA). לכך חשיבות רבה, שכן ההסדר בחקיקה עשוי לכלול עוד מגבלות רציניות על מעקב של מדינה אחר רשתות תקשורת.

74 ראו Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1935 (2013)

75 ראו בחלק 3.1.5 **להלן**.

76 ראו NAACP v. Alabama, 357 U.S. 44 (1958), Shelton v. Tucker, 364 U.S. 479 (1960). עם זאת הזכות לשמירה על פרטיות השיוך הפוליטי יכולה גם לסגת בפני אינטרסים לאומיים, כמו בעניין Barenblatt v. United States, 360 U.S. 109 (1959), שם קבע בית המשפט העליון כי דרישתה של ועדת החקירה של הקונגרס לפעילות אנטי־אמריקאית ממי שהעיד לפניה להעיד על חברותו במפלגה הקומוניסטית אינה בגדר הפרה של התיקון הראשון לחוקה.

חוק הפרטיות בתקשורת אלקטרונית (ECPA) הוא דבר חקיקה פדרלי, שמסדיר את פעולותיהם של גופי החקירה הפדרליים. לעומת זאת פרקטיקות האיסוף של רשויות החוק המקומיות במדינות מתבססות על סמכויות החיפוש והתפיסה המוקנות להן לפי הדין המדינתי, ועל המגבלות הקבועות בתיקון הרביעי לחוקה. מעורבותם של גופים מדינתיים – כלומר רשויות חוק מקומיות – מייתרת לעיתים את הדיון בשאלות שנוגעות לתחולתם של הסדרים פדרליים על טכנולוגיות חדשות.[77] עם זאת לעיתים נמנע המחוקק המדינתי מלאמץ הסדרה מקומית של טכנולוגיות אלו. לאחרונה למשל דחתה ועדת התקציב של הסנאט במדינת קליפורניה הצעת תיקון לחוק[78] שלפיה השימוש של רשויות האכיפה בטכנולוגיות איסוף[79] קיימות וחדשות יהיה כפוף למדיניות השימוש[80] שתאושר בגוף המפקח עליהן.[81]

77 לאחרונה, בעניין State of Arkansas v. James A. Bates (Case No. CR-2016-370-2), הגישה משטרת בנטונוויל שבמדינת ארקנסו בקשה לצו המורה לחברת אמזון להעביר לידיה הקלטות שביצע מכשיר ה־Echo שנמצא בזירת רצח, לרבות כאלו שהוקלטו כבדרך אגב, בלי שמישהו פנה ישירות אל המכשיר בהוראה קולית. מעיון בתגובת החברה נראה כי הבקשה התבססה על צו חיפוש רגיל, ולא על הוראות ה־SCA המתאימות (ראו חלק 3.1.3.2 **להלן**). ראו Memorandum of Law in Amazon.com, Support of Amazon's Motion to Quash Search Warrant (February 17, 2017)

78 Rainey Reitman, *Innovative Police Transparency Measure Dies in California,* Electronic Frontier Foundation (01.09.2017); לנוסח התיקון המוצע ראו Bill No. SB21, "An act to add Chapter 15 (commencing with Section 54999.8) to Part 1 of Division 2 of Title 5 of the Government Code, relating to law enforcement agencies" (12.06.2017)

79 **שם**, בסעיף 54999.8(d): "טכנולוגיית איסוף" – כל מכשיר לאיסוף מידע תרמי, קולי או ויזואלי, נתוני מיקום או מידע דומה על אנשים פרטיים או קבוצות, לרבות טכנולוגיות לזיהוי תמונה, קוראי לוחות רישוי אוטומטיים, רחפנים וטכנולוגיית GPS.

80 מדיניות כאמור תפרט לכל הפחות את המטרות שלשמן יאושר להשתמש בטכנולוגיית האיסוף, את סוגי הנתונים שהיא מפיקה, את סוגי העובדים שישתמשו בה, את תקופת שימור הנתונים שייאספו באמצעותה, את הבקרות שיחולו על השימוש בה כדי להבטיח ציות לחוקי הפרטיות המתאימים, את הליכי תיעוד הגישה לנתונים ואת קיומו של כל מסמך הבנות עם רשות נוספת או צד שלישי הנוגע לשימוש משותף או העברה של הנתונים.

81 זאת ועוד, לפי הוראות התיקון, על רשויות האכיפה לדווח לגוף המפקח אחת לשנתיים, לכל הפחות, על השימוש בטכנולוגיות האיסוף השונות. דוחות אלו יפורסמו בפומבי.

3.1.3.1 חוק האזנות סתר (WTA – Wiretap Act)

חוק האזנות סתר (WTA) מחיל איסור כללי על האזנת סתר – יירוט תקשורת (מכל סוג) באמצעות מתקנים אלקטרוניים, מכניים או אחרים – וכן על גילוי מידע או שימוש במידע שהושג באמצעים אלו. ראיות שהושגו באמצעות יירוט אסור של תקשורת קווית או תקשורת בעל פה, פסולות. לעומת זאת כלל הפסלות אינו חל על תקשורת אלקטרונית.[82]

החוק מתיר לספקים של שירותי תקשורת קווית או אלקטרונית להעביר מידע לאלה המוסמכים מכוח ההוראות של חוק איסוף מודיעין זר (FISA)[83] או להושיט להם סיוע טכני בפעולות מעקב אלקטרוני כהגדרתן שם, בכפוף לצו בית משפט או תעודה בכתב ממי שמוסמך לאשר שלא נדרש צו כאמור.[84] עוד מתיר החוק ליירט כל תקשורת אלקטרונית שבשל הגדרותיה הטכניות הגישה אליה חופשית.[85]

לצד האיסור הכללי, חוק האזנות סתר (WTA) כולל נוהל לאישור האזנת סתר של רשות חקירה.[86] על המוסמכים מטעם התביעה – התובע הפדרלי הכללי, סגנו או בעלי תפקידים כאלה במדינות ארצות הברית – להגיש לשופט בקשה בכתב שמפרטת את העילה הסבירה (probable cause) שבעטיה נדרש אמצעי המעקב, את אמצעי החקירה האחרים שנוסו ונכשלו או שלא הופעלו מפאת מסוכנותם, ואת תקופת הזמן המבוקשת ליירוט התקשורת.

82 18 U.S.C. §2518

83 ראו חלק 3.1.5 **להלן**.

84 18 U.S.C. §2511(2)(a)(ii)

85 18 U.S.C. §2511(2)(g). כמה צורות של תקשורת רדיו הוחרגו מהגדרת "גישה חופשית", ראו ס' 2510(16). מנגד נראה כי ספקי התקשורת יכולים לנסות להערים קשיים על איסוף מודיעין גלוי. כך למשל ביום 13 במרץ 2017 הודיעה חברת פייסבוק כי היא משנה את מדיניותה ואוסרת על שימוש במידע שמקורו בשירותיה לפיתוח כלי מעקב. ספק אם מהלך זה ימנע סוכנויות ממשלתיות מפיתוח של כלי מעקב מקוון, אבל אפשר שהוא יציב חסמים בפני יכולתן להסתייע בקבלני משנה פרטיים, שעתה חשופים לתביעה אזרחית.

86 18 U.S.C. §2518

בקשה תאושר כאמור אם יש יסוד סביר להניח שהתבצעה, מתבצעת או עומדת להתבצע עבירה מתוך רשימת העבירות המנויה בסעיף 2516 לחוק,[87] וכי יש יסוד סביר להניח כי היירוט המבוקש יניב מידע בנוגע לעבירה זו, ובהיעדר חלופות אחרות שטרם נוסו ואינן מסוכנות. אישורים כאמור מוגבלים לשלושים יום, ואפשר להאריכם באישור נוסף לפי נוהל זה. השופט אף רשאי להורות לרשות החוקרת לדווח לו על ההתקדמות בחקירה במהלך הפעלתו של אמצעי היירוט המבוקש, כדי להעריך את ההצדקה להמשך השימוש בו.

במקרים דחופים – שבהם קצין של רשות חקירה (שהוסמך בידי המוסמכים להגיש בקשות יירוט מטעם התביעה) סבור שנדרש יירוט של תקשורת בנסיבות שבהן יש חשש לחייו של אדם או לפגיעה גופנית קשה בו, או יש פעילות שמאיימת על אינטרסים של ביטחון לאומי או קשורה לארגוני פשיעה – רשאי הקצין המוסמך לאשר יירוט של תקשורת מכל סוג שהוא בתנאי שבתוך 48 שעות מתחילת המעקב תוגש בקשה לשופט לפי ההוראות הכלליות של החוק.

87 בכללן עבירות שעונשן מוות או מאסר של יותר משנה הקשורות לאלה: נשק גרעיני, דלק גרעיני, נשק ביולוגי, ריגול, חטיפה, ריגול כלכלי, גנבת סודות מסחריים, חבלה, בגידה, מהומות אלימות, היזק בזדון לרכוש, השמדת כלי שיט או שוד ים; עבירות על איסורים על העברה וקבלה של כספים בין מעביד לנציגי ארגון עובדים; עבירות על חובות האמונאות של נציגי ארגוני עובדים; כל עבירה על דיני העבודה הכוללת רצח, חטיפה, שוד או סחיטה; כל עבירת אלימות בשדות תעופה בין־לאומיים; עבירות אלימות או איום באלימות באמצעות בעלי חיים; עבירות הצתה בתחומי השיפוט הימי והטריטוריאלי המיוחד של ארצות הברית; עבירות שוחד; שימוש שלא כדין בחומרי נפץ; הסתרת נכסים; שידור נתוני הימורים; בריחה ממשמורת; עבירות על איסורי החזקת כלי נשק במתקנים פדרליים; דיווח שגוי ביודעין לגופים פיננסיים; רצח או ניסיון לרצח של פקידי ממשל, פקידי ממשל זרים, אורחים רשמיים זרים או בעלי תפקידים בכירים זרים ובני משפחותיהם; פריעת צדק; הפרעה לשוטר במילוי תפקידו; ניסיון להשפיע על עד, על קצין או על חבר מושבעים או לפגוע בהם; סחר בבני אדם; עבדות; סחר בילדים; הברחה; התקשרות בעסקה לרציחתו של אדם; עבירות הימורים; עבירות הלבנת הון; עבירות הונאה באמצעות בזק, רדיו או טלוויזיה; עבירות הונאה בנקאיות; פיגועי טרור בתחבורה ציבורית; עבירות הנוגעות לפורנוגרפיית קטינים; שינוע בין־מדינתי של רכוש גנוב; עבירות מרמה; עבירות עינויים; עבירות הנוגעות להשגת אזרחות ומסמכי זיהוי שלא כדין או בהסתמך על הצהרות כוזבות; עבירות זיוף; עבירות מרמה הקשורות לפשיטת רגל; עבירות ייצור, ייבוא, קבלה, הסתרה, מכירה של סמים נרקוטיים, מריחואנה או סמים מסוכנים אחרים וסחר בהם; עבירות ציתות; עבירות על איסורים בקשר לפרסומי תועבה.

חשוב להדגיש כי נוהל זה מצמצם מאוד את פעילות המעקב העצמאית של רשויות החקירה, ונוסף על הבקרה של מערכת המשפט, הוא דורש גם מעורבות ובקרה משפטית של גופי התביעה בניסוח הבקשה – במקרים רגילים לפני תחילת הפעילות; ובמקרים דחופים – בתוך 48 שעות מתחילתה.

כל צו שיפוטי שמאשר בקשה ליירוט תקשורת כאמור, נדרש לכלול הוראות שנועדו לצמצם את היירוט למינימום ההכרחי למטרת המעקב. כך למשל יידרשו סוכני רשות החקירה המצותתים לקו הטלפון של חשוד להפסיק את ההאזנה כשבני משפחתו מנהלים שיחות אישיות בקו.

מינהלת בתי המשפט האמריקאית מפרסמת דיווח שנתי לקונגרס של מספר הבקשות להאזנות סתר שנידונו בבתי משפט פדרליים ומדינתיים לתכליות של אכיפת חוק ומניעת פשיעה.[88] נתונים אלו כוללים בקשות להאזנת סתר מכוח חוק האזנות סתר (WTA) וכן בקשות להאזנת סתר מכוח חקיקה דומה ברמת המדינה. חלק מהנתונים שמינהלת בתי המשפט מדווחת עליהם נשענים על דיווחים חלקיים של גופי התביעה בדבר יישום הצווים, ולכן ייתכנו עיוותים בניתוח הנתונים. בדומה לנתונים המדווחים בישראל,[89] שיעור הבקשות להאזנות סתר שדחתה מערכת בתי המשפט בארצות הברית – מזערי. עם זאת סדרי הגודל של מספרי הבקשות להאזנת סתר בארצות הברית ובישראל זהים – אלפי בקשות בשנה בארצות הברית ואלפי בקשות בשנה בישראל. נתון זה עלול להדאיג את הקורא הישראלי, אך ייתכן שניתן להסבירו בהבדלים טכניים באופי הצווים: הנתונים הישראליים מתארים ממוצע של 1.4–1.8 מואזנים לבקשה, ואילו בארצות הברית היתר אחד מתייחס ל־90–175 מואזנים בממוצע.

88 United States Courts, Wiretap Reports

89 ראו בלוח 3, **לעיל** בפרק 2 ה"ש 61.

לוח 5
בקשות והיתרים להאזנת סתר בארצות הברית למטרות אכיפת חוק ומניעת פשיעה[90]

שנה	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
בקשות להאזנת סתר	1,839	2,208	1,891	2,376	3,195	2,734	3,397	3,577	3,555	4,148	3,170
בקשות להאזנת סתר שאושרו	1,839	2,208	1,891	2,376	3,194	2,732	3,395	3,576	3,554	4,148	3,168
בקשות שנדחו	0	0	0	0	1	2	2	1	1	0	2
שיעור הדחייה	0.00%	0.00%	0.00%	0.00%	0.03%	0.07%	0.06%	0.03%	0.03%	0.00%	0.06%
בקשות להאזנת סתר – ברמה הפדרלית	461	457	386	663	1,207	792	1,354	1,476	1,279	1,403	1,551
בקשות להאזנת סתר – ברמת המדינה	1,378	1,751	1,505	1,713	1,987	1,940	2,041	2,100	2,275	2,745	1,617
מספר ממוצע של מואזנים*	129	94	92	113	121	113	104	97	100	114	173

* ממוצע המואזנים לבקשה, המחושב במינהלת בתי המשפט, מבוסס על דיווחים חלקיים מגופי התביעה, וייתכן שאינו מדויק.

90 מקור הנתונים: United States Courts, Wiretap Report 2016, tables 4,7. נתונים משלימים בנוגע לממוצע המואזנים בשנים 2015–2006 נלקחו מטבלה 4 בדיווחים לשנים אלו.

3.1.3.2 חוק תקשורת שמורה (SCA — Stored Communications Act)

לעומת חוק האזנות סתר (WTA) – החל על תקשורת שאפשר ליירט בעת שידורה או סמוך לו – הוראות חוק תקשורת שמורה (SCA) חלות על גישה לנתוני תקשורת המאוחסנים אצל ספקי שירותי מחשוב מרוחק (ספקי שירותי אינטרנט)[91] וספקי שירותי תקשורת אלקטרונית (המחזיקים בין היתר את נתוני המנויים שלהם). בדומה לחוק האזנות הסתר שפורט לעיל, חוק תקשורת שמורה (SCA) מחיל איסור כללי על גישה לא מורשית למאגרי מידע שנתוני תקשורת אלקטרונית נשמרים בהם.

חוק תקשורת שמורה (SCA) מתיר לספקי שירות להעביר נתוני תוכן שמורים של תקשורת אלקטרונית או קווית שמקורה ב־180 הימים האחרונים, באמצעות צו שיפוטי.[92] ההליך הרגיל למתן הצו דורש עילה סבירה לפי כללי סדר הדין הפליליים,[93] הכפופים להוראות התיקון הרביעי לחוקה והפסיקה המנחה הדנה בהן. הליך זה נוקשה פחות מזה הנוהג לפי חוק האזנות סתר (WTA), שתואר בסעיף הקודם.

אשר לנתוני תקשורת שמקורם בתקופה העולה על 180 הימים האחרונים, חוק תקשורת שמורה (SCA) מתיר לתת צו בהתקיים עילה סבירה (probable cause). נתוני תקשורת אלה יימסרו לפי צו חיפוש שיפוטי על פי כללי סדר הדין הפלילי, אבל ללא הודעה מוקדמת למנוי שהנתונים המבוקשים נוגעים לו,[94] ולחלופין – בדרך של מתן הודעה מוקדמת למנוי באמצעות מתן צו מינהלי (administrative subpoena) למנוי עצמו, או באמצעות צו שיפוטי מקל יותר, הדורש את התקיימותו של חשד סביר[95] – כאשר ישנו יסוד סביר להניח כי הנתונים

91 ספק שירותי מחשוב מרוחק, לפי 18 U.S.C. §2711(1), הוא מי שמספק לציבור שירותי אחסון או עיבוד ממוחשבים באמצעות מערכות תקשורת אלקטרוניות.

92 18 U.S.C. §2703(a)

93 Fed. R. Crim. P. 41

94 חברת גוגל הודיעה כי כעניין שבמדיניות, עם קבלת צו מכוח ה־ECPA המבקש מידע על מי ממנוייה, תודיע החברה למנוי על הבקשה לפני שתעביר את המידע המבוקש, אלא אם הודעה כזו אסורה עליה בדין. ראו המענה לשאלות נפוצות (FAQ) בדוח השקיפות של גוגל, **לעיל** בפרק 2 ה"ש 30.

95 ראו 18 U.S.C. §2703(a), המפנה ל־§2703(d).

המבוקשים הם בעלי חשיבות מהותית בחקירה פלילית. רף החשד הסביר הוא סטנדרט מקל מזה של העילה הסבירה. עם זאת בית המשפט רשאי שלא לאשר בקשה כזאת אם המידע המבוקש חריג בהיקפו או אם הבקשה עצמה מטילה מעמסה לא מוצדקת על ספק השירות. אין נפקות להיעדרה או לקיומה של הרשאת גישה מאת המנוי לספק השירות. עם זאת בעניין *Warshak*[96] הבהיר בית המשפט העליון כי מסירת נתוני תוכן של תקשורת דוא"ל כפופה לתיקון הרביעי לחוקה, ומשכך עליה להתבצע בכפוף לצו שיפוטי.

נוסף על נתוני תוכן, חוק תקשורת שמורה (SCA) מסדיר גם את ההליך של העברת נתוני תקשורת של מנויים של ספקי השירותים. בהקשר זה נתוני תקשורת הם כל הנתונים הנוגעים למנויי הספקים שאינם נתוני תוכן, ורשות חוקרת יכולה לדרוש אותם באמצעות צו חיפוש רגיל או לפי הצו השיפוטי המקל יותר לפי חוק תקשורת שמורה (SCA).[97] כמו כן ניתן לבקש באמצעות צו מינהלי[98] נתונים מסוימים של מנויים.[99] כל העברה של נתוני metadata אינה טעונה יידוע מראש של המנוי.

חוק תקשורת שמורה (SCA) אינו דורש מספקי שירותי תקשורת לשמור מידע כדבר שבשגרה, ואולם ספק שירות מחויב לשמור במשך תשעים יום (תקופה שניתנת להארכה) נתונים שרשות חקירה ביקשה בהליך האמור, כל עוד לא ניתן צו שיפוטי.[100] במסגרת בקשה כזאת הרשות יכולה להורות לספק להכין עותק גיבוי של הנתונים, נוסף על ההימנעות ממחיקתם.[101]

96 United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)

97 18 U.S.C. §2703(c), המפנה ל־§2703(d). באשר לחקירות של הונאת טלמרקטינג, רשות החקירה אינה זקוקה לצו כדי לבקש פרטים מזהים של מנוי.

98 18 U.S.C. §2703(c) (2)

99 שם, כתובת, היסטוריה של תעבורת שיחות טלפון, תקופת המנוי, השירותים שסופקו למנוי, מספר מזהה של מכשיר הטלפון או מכשור תקשורת אחר של המנוי לרבות כתובות IP זמניות שהוקצו לו ופרטי אמצעי התשלום של המנוי.

100 18 U.S.C. §2703(c)

101 18 U.S.C. §2704

בעניין *Microsoft Corp.* תקפה חברת מייקרוסופט צו שניתן לה מכוח חוק תקשורת שמורה (SCA), שלפיו עליה למסור נתוני דוא"ל שאוחסנו באירלנד. בית המשפט הפדרלי לערעורים קיבל את טענת החברה ולפיה תחולת החוק (SCA) טריטוריאלית בלבד, ואינה חלה על מידע שמאוחסן פיזית מחוץ לארצות הברית.[102] בעקבות זאת החלו ספקי שירותים באינטרנט, בכללם מייקרוסופט, גוגל ויאהו, לסרב יותר ויותר לצווים שניתנו מכוח החוק.[103] כדי לבלום את הסחף, ביקש משרד המשפטים האמריקאי רשות לערער לפני בית המשפט העליון על החלטה זו. בית המשפט דן בתיק במחצית הראשונה של 2018.[104] מעניין לציין כי במסגרת חוות דעת של ידידי בית המשפט שהוגשו בעניין *Microsoft Corp.*, הוגשה גם חוות דעת מטעמו של האיחוד האירופי;[105] חוות דעת זו אינה נוקטת עמדה לכאן או לכאן, אבל מצביעה על החשש מהתנגשות עם הדין האירופי החל על העברת מידע למדינות צד שלישי.[106]

ואולם הדיון בעניין *Microsoft Corp.* בסוגיית התחולה של החוק בדבר תקשורת שמורה (SCA) התייתר בעקבות התיקונים שנתקבלו במסגרת חוק הענן (The CLOUD Act).[107] חוק הענן תיקן את חוק תקשורת שמורה (SCA) בהוסיפו הוראה שלפיה על הספקים של שירותי תקשורת אלקטרונית או שירותי מחשוב מרוחק[108] לשמור, לגבות או למסור כל נתוני תוכן וכל תיעוד אחר שנוגע למנוייהם

102 Microsoft Corp. v. United States, No. 14-2985, 2016 WL 3770056 (2nd Cir. July 14, 2016)

103 Petition for Certiorari, United States of America v. Microsoft Corporation, No. 17-2 בעמ' 26-27.

104 בית המשפט דן בתיק ביום 27.2.2018, ראו Transcript of Oral Argument, United States of America v. Microsoft Corporation, No. 17-2.

105 Brief of the European Commission on Behalf of the European Union as Amicus Curiae, United States of America v. Microsoft Corporation, No. 17-2

106 ראו בחלק 3.2.3.3 **להלן**.

107 Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018, S. 4943, 115th Cong. (2018)

108 להגדרת "ספק שירות מחשוב מרוחק" ראו **לעיל** בפרק זה ה"ש 91.

או ללקוחותיהם אם הם מצויים בחזקתו או בשליטתו של הספק, וללא תלות באחסנתם בתוך גבולות ארצות הברית או מחוץ להם. ההסדר המוצע בחוק הענן כולל מנגנונים המאפשרים לספקים לעתור לביטול או לשינוי של צווים מכוחו, אם הגילוי המבוקש מפר את הדין הזר. ההצעה כוללת גם כמה מנגנונים שמקילים על בקשת מידע של רשויות חקירה זרות מספקי שירותים מקומיים בתנאי שבין ארצות הברית למדינה המבקשת יש הסכם מתאים, שאושר בקונגרס ובידי התובע הכללי, ומכיל הוראות, המפורטות בהצעת החוק, בדבר שימור המידע המבוקש והשימוש בו.[109]

החוק תקשורת שמורה (SCA) כולל נוהל לבקשת מידע בהסתמך על "מכתב ביטחון לאומי" (NSL — National Security Letter) שעשוי להתייחס גם לתקשורת שמעורבים בה אזרחים זרים ותושבי חוץ. לפי סעיף 2709 לחוק, על הספק של שירותי תקשורת קווית או אלקטרונית להעביר לבולשת נתוני זיהוי של מנויים (וכן את תקופת המנוי, ובמקרה של שיחות יוצאות מחוץ לארצות הברית – גם את פרטי נתוני הגבייה של שיחות כאלה), בתנאי שיש הוראה בכתב מראש הבולשת או ממי שהוא הסמיכו לכך, המאשרת כי הנתונים המבוקשים נדרשים לחקירה מאושרת בקשר לטרור בין־לאומי או לפעילות מודיעין חשאית. על בקשה מכוח "מכתב ביטחון לאומי" (NSL) אפשר לערער לבית המשפט.

הנתונים שהושגו באמצעות "מכתב ביטחון לאומי" (NSL) יופצו הפצה פנימית בכפוף לכללים שאישר התובע הכללי ולמטרות של איסוף מודיעין וריגול נגדי. מותר להפיץ נתונים כאלה לסוכנויות אחרות של ארצות הברית רק אם ברור שהמידע רלוונטי לתחומי האחריות של הסוכנות.[110] הנוהל חשאי כולו, ולספקי תקשורת אסור לגלות כי הבולשת ביקשה מידע לפיו.[111]

109 לביקורת על היבטים אלו של חוק הענן, ראו Neema Singh Guliani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them*, Lawfare (16.3.2018). לטענות נגד ראו Jennifer Daskaland Peter Swire, *Privacy and Civil Liberties Under the CLOUD Act: A Response*, Lawfare (21.3.2018)

110 18 U.S.C. §2709(e)

111 18 U.S.C. §2703(c)(1)(a). חוקתיותה של הוראה זו בהקשר של פעילויות המוגנות מכוח התיקון הראשון לחוקה נידון בעניין In re: National Security

3.1.3.3 חוק איסוף נתוני תקשורת (PRA – Pen Register Act)

חוק איסוף נתוני תקשורת (PRA) חל על מתקני pen register (המתעדים פרטי תקשורת נתונים יוצאת) ו־trap and trace (המתעדים פרטי תקשורת נכנסת) ועל מקביליהם המודרניים. מתקנים אלו נועדו לתעד בזמן אמת נתוני תקשורת קווית או אלקטרונית שאינם נתוני תוכן. כלומר, מדובר במתקני איסוף של metadata המתעדים למשל היסטוריית שיחות נכנסות או יוצאות למכשיר טלפון מסוים.[112] עם זאת באמצעים טכנולוגיים אפשר ליירט את המידע שהתקבל במתקנים, להקליט אותו ולשדר אותו הלאה. אמצעים אלה שקולים למעשה לחיפוש במאגר מידע. בעניין *Forrester*[113] נקבע כי פרטי הודעת דוא"ל (email headers)[114] וכתובת IP זהים ל־pen register, ומשכך אינם זכאים להגנה מכוח התיקון הרביעי לחוקה.[115] עם זאת חוק איסוף נתוני תקשורת (PRA) מחיל איסור כללי על שימוש במתקני pen register ו־trap and trace, אלא לצורכי תחזוקה של שירותי תקשורת קווית או אלקטרונית או בכפוף להוראות שבסעיף 3123 לחוק או להוראות שבחוק איסוף מודיעין זר (FISA).[116]

Letter, 930 F,Supp.2d (1064) (N.D. Cali 2013), המצוי בהליכי ערעור חסויים
במסגרת עניין In re: National Security Letter, Under Seal v. Holder
(Sealed)

112 השימוש במתקנים אלו הוסדר בחקיקה בתגובה להחלטת בית המשפט בעניין *Smith v. Maryland* (**לעיל** בפרק זה ה"ש 31), שלפיה הוראות התיקון הרביעי לחוקה אינן חלות על מתקני pen register, בין השאר בשל דוקטרינת הצד השלישי.

113 United States v. Forrester, 512 F. 3d 500 (9th Cir.2007)

114 לצד שדות נתונים בכותרת הדוא"ל שהם metadata במובהק, כמו שדה המוען, שדה הנמען, שעת המשלוח וכדומה, שדה נושא ההודעה, שהינו חלק מהנתונים המוגדרים כ־email header, עשוי להיות מסווג כשדה של נתוני תוכן. ראו למשל ע"ע 90/08 (ארצי) **טלי איסקוב ענבר נ' מדינת ישראל – הממונה על חוק עבודת נשים**, פס' 39 לפסק דינה של השופטת ארד (פורסם בנבו, 8.2.2011), שם הובחן שדה הכותרת מתוכן המסר האלקטרוני.

115 בהערת אגב ציין בית המשפט כי כתובת URL בעייתית יותר מבחינה חוקית, משום שהיא עלולה להסגיר מידע רב על פעילותו של פלוני באתר אינטרנט.

116 ראו בחלק 3.1.5 **להלן**.

סעיפים 3123–3122 לחוק מסדירים את נוהל הבקשה למעקב אחר נתוני תקשורת באמצעות הוצאת צו להתקנה של מתקני pen register ו־trap and trace ושימוש בהם. בית המשפט ייתן צו כאמור אם שוכנע שהמידע שהמתקן יפיק עשוי להיות רלוונטי לחקירה פלילית.[117] סוזן פרייוולד מעירה כי הקריטריונים שהחוק דורש למתן צו מציבים רף נמוך למדי (מבחן רחב של רלוונטיות לעומת מבחן העילה הסבירה הצר, הנדרש לפי חוק האזנות סתר (WTA),[118] שאין בו כדי למנוע "מסעות דיג" של רשויות אכיפה הבוחרות לעקוב אחר אנשים שמידת מעורבותם בעבירה פלילית קלושה, לרבות אחר קורבנות העבירה הנחקרת עצמם.[119] ההבדל בין ההוראות של חוק איסוף נתוני תקשורת (PRA) להוראותיו של חוק האזנות סתר (WTA) מעידים על יחסו השונה של המחוקק לנתוני תקשורת לעומת נתוני תוכן. כך למשל ראיות שהושגו מתוך הפרת הוראות ה־PRA לא ייפסלו, ואילו ה־WTA מחיל כלל פסלות ראיות.[120] לשון אחר, המגבלות שהדין בארצות הברית מטיל על רשויות אכיפת החוק בבואן להשיג נתוני תקשורת מעטות מאלה שהוא מטיל על השגה של נתוני תוכן.

3.1.4. חוק סיוע תקשורתי לרשויות אכיפה (CALEA)

חוק סיוע תקשורתי לרשויות אכיפה (CALEA — Communications Assistance for Law Enforcement Act),[121] המוכר גם כ־Digital Telephony Act – מורה לספקיות תקשורת לעצב את רשתות התקשורת והשירותים שהן מספקות כך שיאפשר להן לבודד ולייַרט תקשורת אלקטרונית ולהעבירה לרשויות המוסמכות. ספקיות תקשורת המציעות שירותי הצפנה נדרשות בין השאר

117 הצו מוגבל לתקופה שלא תעלה על 60 יום, הניתנת להארכה בצו לתקופה שלא תעלה על 60 יום נוספים. מטבעו וטיבו של המתקן והצורך המודיעיני בו, אין חובת יידוע על השימוש שנעשה בו, ומנגד חלה חובת סודיות על כל צד שלישי שנדרש לסייע לרשות בהתקנה.

118 ראו בחלק 3.1.3.1 **לעיל**.

119 Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 Cal. L. Rev 949, 1005–1006 (1996)

120 18 U.S.C. §2518(10)

121 47 U.S.C. §§1001–1010, 1021

ליכולת לפענח נתוני תקשורת שהוצפנו באמצעות שירותים אלה. ההגדרה מיהן "ספקיות תקשורת" לפי חוק הסיוע לרשויות אכיפה (CALEA) מורכבת ותלויה בפרשנות דיני התקשורת האמריקאיים. בין השאר קבע בית המשפט כי ספקיות שירותי VoIP עולות כדי "ספקיות תקשורת", ומשכך הוראות ה־CALEA חלות עליהן, והן צריכות לעצב את שירותי התקשורת שהן מספקות לפי הדרישות.[122]

המגבלות של חוק הסיוע לרשויות אכיפה (CALEA) באו לידי ביטוי לאחרונה בפרשת החיפוש במכשירי האייפון, שהתעוררה בשנת 2016.[123] הבולשת הפדרלית (FBI) ביקשה צו שיורה לחברת אפל לסייע בפריצת מכשיר אייפון מוצפן שתפסה. CALEA אינו חל על שירותי מידע,[124] ועל כן אינו תקף לנתוני תקשורת ששודרו זה מכבר ומאוחסנים במכשירי אפל או בענן. אף שייתכן שבאמצעות פרשנות יצירתית ניתן היה, בנסיבות עובדתיות מסוימות, להחיל את הוראותיו למטרות של "דלתות אחוריות" ופענוח נתונים מוצפנים, נראה כי בשל הקושי נמנעה הבולשת אף מלנסות להציע מתווה פרשני כזה.[125] במקום זאת היא בחרה במסלול שנוי במחלוקת והגישה בקשה לצו על בסיס חוק ה־All Writs Act משנת 1789[126] – ששימש באמצע שנות השבעים בעניין *New York Telephone Co.*,[127] אז הורו סוכנים פדרליים בצו לחברת טלפוניה

122 Am. Council on Educ. v. FCC, 451 F.3d 266 (D.C.Cir. 2006)

123 USA In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (California Central District Court, 2016) (להלן: פרשת **האייפון**). ראו גם, Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 Stanford L. Rev 99 (2018)

124 ראו 47 U.S.C. §1002. בין השאר, "שירותי מידע", כהגדרתם בסעיף 1001, הם שירותים הכרוכים באחסנת מידע.

125 ראו טיוטת מאמרו של הורוביץ: Justin (Gus) Hurwitz, *Encryption Congress Mod (Apple + CALEA)* (University of Nebraska at Lincoln – College of Law 2016)

126 ראו Steven R. Morrison, *Breaking iPhones Under CALEA and the All Writs Act: Why the Government Was (Mostly) Right*, 38 Cardozo L. Rev., 2039 (2017)

127 United States v. New York Telephone Co., 434 U.S. 159 (1977)

לסייע בהתקנת מכשירי pen register. לאחר שנסתייעה במיקור חוץ כדי לפרוץ למכשיר האייפון ולהשיג את המידע המבוקש, משכה הבולשת את הבקשה, והחלטת בית המשפט בעניין נתייתרה.[128]

3.1.5. חוק איסוף מודיעין זר (FISA)

חוק איסוף מודיעין זר (Foreign Intelligence Surveillance Act)[129] מגדיר את הנהלים וההוראות שמכוחם ממשלת ארצות הברית מוסמכת לאסוף "מודיעין זר" בתחומי ארצות הברית ומחוצה לה. מטיבו ומטבעו משטר האיסוף שהחוק עוסק בו, הביטחוני באופיו, שונה מזה של חוק הפרטיות בתקשורת אלקטרונית (ECPA), שהוא ערוץ האסדרה העיקרי של מעקב מקוון לתכליות של מניעת פשיעה, חקירה ואכיפת החוק. כמו שציין בית המשפט בעניין *Butenko*: "איסוף מודיעין זר הוא פעילות חשאית ובלתי מובנית עד מאוד, ולעתים מזומנות אי־אפשר לצפות מראש את הצורך במעקב אלקטרוני".[130]

הפרק הראשון של החוק חל על מעקב אלקטרוני[131] לצורכי איסוף מודיעין זר – מידע הנוגע לגורמים זרים הקשורים לביטחון הלאומי של ארצות הברית או ליחסי החוץ שלה.[132] מעקב כזה טעון צו מטעם בית משפט מיוחד – בית המשפט

128 Russell Brandom, Apple's San Bernardino Fight is Officially over as Government Confirms Working Attack, The Verge (28.3.2016). לפי הפרסומים בעיתונות, נעזרה הבולשת בחברה ישראלית לשם כך, ראו אליחי וידל, "הישראלים שעוזרים ל־FBI לפרוץ לאייפון של אפל", **דה מרקר** (23.3.2016).

129 Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801–1885c (להלן: FISA).

130 ראו **לעיל** בפרק זה ה"ש 73.

131 מעקב אלקטרוני, המוגדר בסעיף 1801(e)§ של FISA, כולל מגוון פרקטיקות להשגת נתוני תוכן של תקשורת אלקטרונית, קווית או אחרת, בנסיבות שבהן יש ציפייה סבירה לפרטיות הטעונה בצו שיפוטי, ויש להן זיקה טריטוריאלית או פרסונלית מסוימת (המוגדרת בחוק) לארצות הברית.

132 מודיעין זר מוגדר בסעיף 1801(f)§ של FISA כמידע הקשור ליכולותיה של ארצות הברית להתגונן מפני פעילות עוינת חמורה, חבלנות, טרור בין־לאומי, הפצת נשק להשמדה המונית או פעולות ביון של ישויות זרות (לרוב מדינות זרות, ארגונים שהן שולטים בהם או ישויות העוסקות בטרור, בהפצת נשק להשמדה המונית וכו') או של

למודיעין זר (FISC — Foreign Intelligence Surveillance Court) – ערכאה חשאית ובה 11 שופטים פדרליים. מעל ערכאה זו יש ערכאת ערעור חשאית, ה־Foreign Intelligence Surveillance Court of Review. כדי שמעקב כאמור יאושר, יש להראות כי תכליתו המהותית היא איסוף מודיעין זר,[133] וכן כי מופעלים נהלים שתכליתם לצמצם את איסוף המידע למינימום ההכרחי ולהבטיח שכל מידע פרטי שאינו בגדר מודיעין זר על "אדם אמריקאי"[134] – אם נאסף אגב המעקב המבוקש – לא יופץ באופן שיסגיר את זהותו, אלא אם הדבר נדרש לשם הבנת המודיעין הזר או לאמידת ערכו.[135]

בדומה לנהלים של חוק הפרטיות בתקשורת אלקטרונית (ECPA), גם בקשות במסגרת חוק איסוף מודיעין זר (FISA) מבוקרות בגופי התביעה. בקשה לצו FISA יגיש קצין פדרלי מוסמך בכפוף לאישור התובע הכללי.[136] הבקשה תכיל, בין השאר, את פרטי היעד המודיעיני, את דרכי איסוף המידע, את תקופת הזמן הנדרשת למעקב והצהרה על נוהלי הצמצום המוצעים. עוד תכלול הבקשה מסמך מעוזר הנשיא לענייני ביטחון לאומי, מסגן הבולשת הפדרלית או מאחֵר שהנשיא הסמיכו לכך, המעיד כי הוא סבור שהמידע המבוקש הוא אכן בגדר

סוכניהן; או מידע הנוגע לישויות זרות או לטריטוריה זרה הקשור לביטחון הלאומי של ארצות הברית או ליחסי החוץ שלה. אם המידע האמור נוגע לאדם אמריקאי, כדי שיוגדר "מודיעין זר", עליו להיות הכרחי (ולא בעל קשר כלשהו) להגשמת המטרות המנויות לעיל.

133 בעקבות אירועי 11 בספטמבר 2001 ותיקוני החקיקה של חוק הטרור (USA PATRIOT Act), הורחבה התחולה של FISA מדרישה למעקב שתכליתו (purpose) מודיעין זר, למעקב שתכליתו המהותית (significant purpose) היא מודיעין זר. סוויר (Swire) טען כי הרחבה זו אפשרה לנהל מעקבים חשאיים מכוח FISA גם בחקירות של פשעים פליליים רגילים. ראו Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306, 1360–1365 (2004). ואכן נתברר כי חששות אלו אינם בלתי מבוססים – ראו לדוגמה את חוות הדעת של ידיד בית המשפט מטעם האיגוד האמריקאי לחירויות אזרחיות (ACLU) וה־Electronic Frontier Foundation בעניין United States v. Keith Preston Gartenlaub, Case No. 14-cr-00173-CAS

134 אדם אמריקאי (United States person) לרבות תאגיד או תושב קבע בעל אזרחות זרה, 50 U.S.C. §1801(i).

135 50 U.S.C. §1801(h)

136 50 U.S.C. §1804

מודיעין זר, וכי תכליתו המהותית של המעקב אחר המבוקש היא איסוף מודיעין זר שאינו ניתן להשגה סבירה באמצעות שיטות חקירה חלופיות.

בית המשפט למודיעין זר (FISC) ייתן צו על בסיס בקשה לפי FISA שהוגשה כנדרש ושרשויות התביעה המוסמכות אישרו, אם מהעובדות המתוארות בה יש יסוד סביר להניח שהיעד המודיעיני של המעקב המבוקש הוא ישות זרה או סוכן של ישות כזו,[137] וכן שהמתקנים או המקומות שבהם ייערך המעקב משמשים, או ישמשו, ישות זרה או סוכן זר. על נוהלי הצמצום המוצעים גם להלום את הוראות החוק. יוער כי החוק מציין במפורש כי הקביעה שפלוני הוא ישות זרה או סוכן של ישות זרה לא תיעשה על סמך פעילויות המוגנות בתיקון הראשון לחוקה, המגן על חופש הביטוי. כך למשל אם פלוני מצהיר כי הוא מזדהה עם עמדותיה של מעצמה זרה, אין לקבוע על סמך זה שהוא סוכן של ישות זרה.

צו FISA יורה על קיומם של נוהלי הצמצום ויוגבל לתקופה הנדרשת להשגת תכליתו ולתקופה שלא תעלה על 90 יום, 120 יום או שנה, לפי מיהותו של הנעקב.[138] אם בעת מתן הבקשה טיבם של המתקנים או של המקומות אינו ידוע, יידרש המבקש לעדכן את בית המשפט בתוך עשרה ימים מתחילת המעקב על מקומות חדשים שבהם הוחל במעקב כאמור, על נוהלי הצמצום שהופעלו, על הבסיס העובדתי שגרם להעתקת המעקב ליעד חדש וכדומה.[139]

במקרי חירום רשאי התובע הכללי לאשר שימוש במעקב אלקטרוני אם הוא סבור כי התעורר מצב חירום הדורש שימוש באמצעים אלו בטרם ניתן להשיג צו, וכי יש תימוכין עובדתיים למתן אישור כזה. כמו כן עליו ליידע את השופט המוסמך לכך כי הוחלט לאשר מעקב חירום אלקטרוני, וכן להגיש בתוך שבעה ימים ממתן האישור בקשה לצו לפי FISA.[140] בתחילתה של מלחמה רשאי הנשיא, באמצעות התובע הכללי, לאשר שימוש במעקב אלקטרוני לצורכי מודיעין זר לתקופה שלא תחרוג מחמישה עשר הימים שלאחר הכרזת המלחמה שהכריז הקונגרס.[141]

137 לפי הגדרת המונחים בסעיף 50 U.S.C. §1801

138 50 U.S.C. §1804(d)(1)

139 50 U.S.C. §1804(c)(3)

140 50 U.S.C. §1804(e)

141 50 U.S.C. §1811

ניתן להמשיך במעקב לצורכי מודיעין זר אחרי אדם שאינו אמריקאי שהתגלה שהוא בתחומי ארצות הברית למשך 72 שעות ממועד הגילוי ובכפוף לקביעה סבירה של ראש סוכנות ביון שהפסקת מעקב כזה עלולה להסב פגיעה גופנית חמורה או לסכן את חייו של מישהו, וכן בכפוף ליידוע של התובע הכללי ולהגשת בקשת חירום לחיפוש בגופו של אותו אדם.[142]

חוק איסוף מודיעין זר (FISA) מורה להשתמש במידע המודיעיני שהושג באופן חוקי ולפי נוהלי הצמצום. נתונים שהושגו בדרך אגב, בהיעדר כוונה להשיגם במסגרת האיסוף המודיעיני, יושמדו.[143] מידע שהושג לפי הוראות החוק יועבר לרשויות אכיפה בצירוף תצהיר שישמש במקרה הצורך בהליכים פליליים, בכפוף לאישור מוקדם של התובע הכללי. כשבכוונת הממשלה להשתמש במידע בהליכים משפטיים או מקדמיים, עליה ליידע בהקדם האפשרי את האדם שהמידע עליו נאסף. מידע מודיעיני שנאסף שלא כדין או שלא בסמכות עלול להיפסל כראיה.

התובע הכללי נדרש לדווח מדי שנה למינהלת בתי המשפט ולקונגרס על מספר הבקשות שהוגשו לפי FISA ועל מספר האישורים שניתנו.[144] עוד עליו לדווח מדי שישה חודשים[145] לוועדת בית הנבחרים למודיעין, לוועדת בית הנבחרים לשיפוט ולאותן ועדות בסנאט על מספר הבקשות והאישורים להפעלות מעקב אלקטרוני אחר יעדים לא ידועים,[146] על כל תיק פלילי שבמסגרתו אושר להשתמש במידע שהושג מכוח FISA, ועל מספר המקרים שבהם הופעל מעקב אלקטרוני בחירום לרבות אישורי מעקב אלקטרוני אחר מי שאינם אמריקאים שנתגלו בארצות הברית.[147]

142 50 U.S.C. §1805(f)

143 50 U.S.C. §1805(i)

144 50 U.S.C. §1807

145 50 U.S.C. §1808

146 ראו בטקסט המפנה לה"ש 139 **לעיל** בפרק זה.

147 ראו הנוהל לפי 50 U.S.C. §1805(f).

נתוני תקשורת, לרבות נתוני תוכן, שהושגו ללא הסכמת אחד מהצדדים לה ושלא באמצעות צו שיפוטי,[148] לרבות נתוני תקשורת מאוחסנים, לא יישמרו לתקופה העולה על חמש שנים,[149] ובתנאי שאחד מהצדדים לתקשורת הוא בגדר אדם אמריקאי אלא אם מדובר במידע שהוא מודיעין זר או נוגע לריגול נגדי; במידע שהוא ראיה פלילית ונשמר ברשות לאכיפת חוק; במידע שסביר להאמין שהוא מוצפן או שיש לו משמעות סודית; במידע שנדרש לשם הגנה מאיום מיידי לחיי אדם או שנדרש למטרות אשרור טכניות; או במידע שראש סוכנות הביון הרלוונטית אישר לשמור אותו לתקופה העולה על חמש שנים, בכפוף לטעמים שניתנו בכתב לוועדות המודיעין של הקונגרס.

3.1.6 חוק איסוף מודיעין זר (FISA) ואיסוף נתוני תקשורת

בעקבות אירועי 11 בספטמבר נחקק החוק לאיחוד וחיזוק אמריקה על ידי מתן כלים נאותים הנדרשים ליירוט ולסיכול טרור (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, או USA PATRIOT Act 2001, להלן: חוק הטרור),[150] שבמסגרתו תוקנו אחדות מההוראות של חוק איסוף מודיעין זר (FISA)[151] כדי להקל את הדרישות להפעלה של אמצעי איסוף מודיעין. בין השאר הגמישו הוראות סעיף 215 של חוק הטרור (USA PATRIOT Act)[152] את הכללים שלפיהם הבולשת (FBI) רשאית לפנות לבית המשפט למודיעין זר (FISC) בבקשה לקבל צו תפיסה של "רשומות עסקיות" (business records) למטרות חקירה שנועדה להגן מפני טרור בין־לאומי או פעילות מודיעין חשאית, הנערכת לפי כללים שאישר התובע הכללי מכוח הצו הנשיאותי מס' 12333.[153]

148 ראו למשל בחלק 3.1.7 **להלן**.

149 50 U.S.C. §1813

150 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, §215, 115 Stat. 272, 287-88

151 ראו למשל **לעיל** בפרק זה ה"ש 133.

152 50 U.S.C. §1861

153 הצו הנשיאותי מס' 12333 בדבר "פעולות המודיעין של ארצות־הברית" – שנתן לראשונה הנשיא רייגן בשנת 1981 ומאז תוקן כמה פעמים – הוא המסמך המסדיר את

כחלק מהשינויים בתיקון הורחבה ההגדרה של החומרים שעליהם חל צו תפיסה כאמור, עד שהמונח "רשומות עסקיות", שנותר רק בכותרת הסעיף, הוחלף ב"כל פריט מוחשי רלוונטי" (any relevant tangible item). התיקון אפשר לבולשת לבקש צו כאמור לתפיסת חומר המוחזק בידי כל צד שלישי, בניגוד למצב הקודם, אז הוגבלו הצווים לתפיסת חומר המוחזק על ידי רשימה סגורה של סוגי נותני שירותים. עוד הוסרה הדרישה שכאשר הבקשה מתייחסת למידע על אמריקאים, על מידע זה להיות **הכרחי** לחקירה.[154]

פרשנים אחדים סברו ששינויים אלו אינם מסכנים את חירויות הפרט, וכי החששות שהעלו מתנגדי התיקון מופרזים.[155] אלא שביוני 2013, בסדרת כתבות בעיתון הגרדיאן[156] שהתבססו על מסמכים מסווגים שחשף אדוארד סנודן, למד העולם על תוכניות ביון שהפעילה הסוכנות לביטחון לאומי (NSA), בין היתר התוכנית לאיסוף מודיעיני גורף (bulk collection) של נתוני תקשורת טלפוניים.[157] ראש ה־NSA וה־CIA בדימוס, הגנרל מייקל היידן, אף העיר בעבר כי "אנו הורגים אנשים בהסתמך על metadata".[158]

פעילותה של קהילת המודיעין האמריקאית ואת הגופים הפועלים במסגרתה. צו זה כולל כמה הגבלות על איסוף, על שימור ועל הפצה של חומרי מודיעין שנאספו מכוחו – ועיקרם נוגע להגנה על זכויותיהם של אזרחי ארצות הברית.

154 Charles Doyle, Terrorism: Section by Section Analysis of the USA PATRIOT Act, Congressional Research Service (2001)

155 Glenn Sulmasy & John Yoo, *Katz and the War on Terrorism*, 41 U.C. Davis L. Rev. 1219, 1228 (2007)

156 ראו **לעיל** בפרק 1 ה"ש 1.

157 תוכנית נוספת שנחשפה במסגרת התגליות של סנודן היא PRISM (ראו חלק 3.1.7 **להלן**) – תוכנית המעקב אחר אזרחים זרים מחוץ לארצות הברית. הוועדה להשגחה על הפרטיות ועל החירויות האזרחיות (PCLOB) לא מצאה שיש לערוך בה רפורמה רחבה, אך המליצה על כמה אמצעי בקרה על מעקב אגבי אחר אזרחי ארצות הברית במסגרתה (ראו Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014)). ה־FISC דחה כמה פעמים טענות בנוגע לחוקתיות תוכנית האיסוף מכוח סעיף 702 ולהלימתה את הוראות החוק. תוכנית זו לא בוטלה במסגרת הרפורמות של חוק החירות (USA Freedom Act).

158 David Cole, *We Kill People Based on Metadata*, N.Y. Rev. of Books (May 10, 2014). ראו גם דיון אצל Margaret Hu, *Metadeath – How Does*

תוכנית המעקב לאיסוף metadata של הסוכנות לביטחון לאומי (NSA) אושרה לראשונה בבית המשפט למודיעין זר (FISC) בשנת 2006. בית המשפט למודיעין זר קבע שלפי סעיף 215 של חוק הטרור (USA PATRIOT Act) רשאית ה־NSA לנהל את תוכנית המעקב שכחלק ממנה נאספו כל רשומות תקשורת הטלפוניה מכמה חברות טלפוניה אמריקאיות. עוד קבע בית המשפט שלפי סעיף 215 אפשר לתת לחברות אלו צו להעביר אליה את הנתונים. הנתונים שהועברו היו נתוני metadata בלבד, ללא נתוני תוכן ואיכון גאוגרפי.[159] במשך השנים אישר בית המשפט (FISC) כללים לשימוש בנתונים אלו בידי מומחי המודיעין של הסוכנות: הכללים שאושרו מגבילים את אופן החיפוש במאגר ומגדירים אילו בעלי תפקידים בסוכנות רשאים לאשר חיפושים כאלו; את תקופת השימור של תוצריהם; ואת כללי השיתוף במידע עם סוכנויות אחרות.[160]

הביסוס המשפטי של תוכנית האיסוף על סעיף 215 שנוי במחלוקת. בשנת 2014 בחנה ועדה עצמאית של הממשל – הוועדה להשגחה על הפרטיות ועל החירויות האזרחיות (PCLOB — Privacy And Civil Liberties Oversight Board) – את ההלימה של תוכנית המעקב של הסוכנות לביטחון לאומי (NSA) עם הוראות החוק,[161] ומצאה כי איסוף נתונים רחב היקף וללא הגבלה אינו עולה בקנה אחד עם סעיף 215, סוטה במידה ניכרת ממטרתו המקורית (הוצאת צו תפיסה במקרים קונקרטיים), וכי הפרשנות של הסוכנויות ושל בית המשפט למודיעין זר (FISC) לדרישת הרלוונטיות של המידע חורגת מהפרשנות המשפטית המקובלת. עוד ציינה הוועדה כי לא מצאה ולו מקרה אחד שבו תוכנית האיסוף תרמה לגילוי של פעילות טרוריסטית חשאית או לסיכולה.[162]

Metadata Surveillance Inform Lethal Consequences?, in Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair 229 (Russell A. Miller, ed., 2017)

159 ראו Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Jan. 23, 2014), 21-22

160 **שם**, בעמ' 25–33.

161 **שם**, בפרק 5.

162 **שם**, בעמ' 11.

בינואר 2014 הודיע ממשל אובמה על הוראת המדיניות הנשיאותית מס׳ 28 (להלן: PPD28),[163] שלפיה מודיעין סיגינטי ייאסף לפי חוק או לפי הוראת הנשיא ובכפוף להוראות התיקון הרביעי לחוקה. על בסיס הקביעה כי לכל אדם יש אינטרס לגיטימי בטיפול במידע האישי שלו נקבע כי בתכנון פעילויות הסיגינט של ארצות הברית יילקחו בחשבון שיקולים שנוגעים לפרטיות ולחירויות אזרחיות, ולפיכך עליהן לכלול בקרות מתאימות המגינות על המידע האישי של כל אדם ללא תלות במוצאו.

החלטת בית המשפט הפדרלי בעניין *ACLU v. Clapper*[164] קבעה כי תוכנית האיסוף חרגה מההסמכה שנחקקה בקונגרס, וכי היא מפרה את הוראות סעיף 215 לחוק הטרור (USA PATRIOT Act). בסמוך להחלטה זו במסגרת הרפורמה של חוק החירות (USA Freedom Act) בשנת 2015,[165] תוקן החוק, ופרקטיקת האיסוף של נתוני תקשורת שנקטה הסוכנות לביטחון לאומי (NSA) הוגבלה: מעתה היה צורך להגדיר את הפריטים שתפיסתם מבוקשת ״במידה הרבה ביותר המתאפשרת״[166] ולבקש רק רשומות המזהות ספציפית מכשיר או אדם יחיד.[167] עם זאת הוראות התיקון מאפשרות לתת צו המורה להעביר נתוני

163 Presidential Policy Directive 28. ראו גם Peter Margulies, *Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 Wash. & Lee L. Rev. 1283 (2015)

164 ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015)

165 בשמו המלא: החוק לאיחוד וחיזוק אמריקה על ידי הגשמת זכויות והבטחת משמעת אפקטיבית בניטור (Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act OF 2015, להלן: חוק החירות) USA Freedom Act of 2014, Pub. L. No. 114-23, 129 Stat. 268

166 50 U.S.C. §1861(k)(4)(A)(i)(II)

167 50 U.S.C. §1861(k)(4)(B)

תקשורת מסדר שני (two–hop)[168] בהסתמך על נתוני התקשורת שהופקו על בסיס המזהה הבודד בבקשה.[169]

3.1.7. איסוף מודיעין על מטרות שמחוץ לארצות הברית

תוכנית המעקב PRISM, שגם אותה חשף סנודן, הסתמכה במידה רבה על התיקונים שהכניס חוק הטרור (USA PATRIOT Act) לסעיף 702 של חוק איסוף מודיעין זר (FISA).[170] באמצעות תוכנית PRISM סוכנות הביון שולחת מזהה (selector) דוגמת כתובת דוא"ל לספק שירותי תקשורת בארצות הברית, והספק מעביר לידיה את התקשורת שנעשתה עם אותו. לא ברור אם "הגישה הישירה" לספקים דוגמת גוגל, פייסבוק או יאהו, המוזכרת במסמכים שחשף סנודן, אכן הייתה גישה ישירה ללא בקרה שיפוטית, או שהפרקטיקה עדיין כללה הליך משפטי כמו שטענו בדיעבד אחדים מהספקים שהוזכרו במסמכים.[171] תוכנית איסוף אחרת היא upstream collection, שדרכה נאספת

168 נתוני metadata מסדר ראשון (one–hop) על מזהה (selector) מסוים הם כל ה"חברים" של אותו מזהה. כך בנוגע למספר טלפון מסוים המשמש כמזהה: נתוני תקשורת מסדר ראשון יהיו כל מספרי הטלפון שאליהם התקשר מספר הטלפון או שהתקשרו אליו, או כאלה המצויים בספר הטלפונים שלו (לפי טיב הקשר הרלציוני שבמסד הנתונים המכיל את ה־metadata). נתוני תקשורת מסדר שני (two–hop) הם "חברים של חברים" – בדוגמה שלעיל כל מספרי הטלפון שמקיימים את היחס המבוקש (שיחה יוצאת/ נכנסת/ הימצאות בספר הטלפונים) עם כל המספרים המצויים בתוצאות החיפוש מסדר ראשון.

169 50 U.S.C. §1861(c)(2)(F)(ii)–(iii). בכלל הטענות של האיגוד האמריקאי לחירויות אזרחיות (ACLU) בערכאה הראשונה שדנה בעניין *Clapper* (**לעיל** בפרק זה ה"ש 164, לערכאה הראשונה, ראו ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013)), נטען כי שאילתות המחזירות נתוני metadata מסדר שלישי (three–hop) אינן מחייבות בניית מסד נתונים של כל שיחת טלפון שנעשתה. טענה זו נדחתה בערכאה הראשונה. אך ההבחנה בין נתונים מסדר שלישי לנתונים מסדר שני חשובה: אחזור נתוני סדר שלישי ("חברים של חברים של חברים") ברשת החברתית פייסבוק, עשוי להניב לפני אומדן מסוים יותר מ־1.3 מיליון פרופילים (*Three Degrees of Separation: Breaking Down the NSA's "Hops" Surveillance Method*, Guardian, Oct. 28, 2013).

170 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).

171 Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, 11:4 IEEE Security & Privacy 54, 54 (2013)

כל התקשורת העוברת דרך שדרת המידע של רשת האינטרנט (internet backbone)[172] והתקשורת הטלפונית.[173]

בהקשר זה רצוי לתת את הדעת על ההשלכות של מדיניות ההפעלה של איסוף מודיעין על מטרות זרות על יחסי החוץ של ארצות הברית. נוסף על הדיון הפנימי בארצות הברית בנושא הפעלת מעקבים ברשתות תקשורת, השפיעה חשיפתה של תוכנית PRISM גם על ההסדרים שאפשרו לחברות עתירות ידע אמריקאיות להוציא מידע פרטי על אזרחי האיחוד האירופי ולעבד אותו מחוץ לגבולות האיחוד. בעקבותיו חשיפותיו של סנודן באשר להיקף המידע הפרטי המצוי בידי סוכנויות הביון האמריקאיות, ערער מקסימיליאן שרמס (Schrems), סטודנט אוסטרי, על קביעתו של המפקח האירי על הגנת המידע (Irish Data Protection Commissioner) באשר לנאותות של רמת ההגנה על המידע הפרטי בהסדר העברת המידע בין חברות אמריקאיות לאיחוד האירופי (ה־Safe Harbor).[174] בעקבות פסק הדין של בית הדין האירופי לצדק (ECJ) (עניין *Schrems*)[175] בוטל ההסדר, ונוצרה תקופה של אי־ודאות בכל הנוגע לחוקיות של העברות הנתונים ממדינות האיחוד לחברות פרטיות בארצות הברית. חשיפותיו של סנודן הביאו גם לידי פרסומה של ההוראה הנשיאותית PPD28 שהוזכרה למעלה; וברוחה גם התיקונים בסעיף 702, שפורטו גם כן (ולפיהם מידע סיגינטי ייאסף לפי חוק ולפי התיקון הרביעי לחוקה ויכיל בקרות מתאימות להגנה על הפרטיות של יעדיו). הוראה זו הייתה הבסיס לקביעה האירופית בדבר נאותות ההסדר החלופי – ה־Privacy Shield.[176]

172 ראו [Redacted], 2012 WL 9189263, at *1 (FISA Ct. Aug. 24, 2012), *available at* http://fas.org/irp/agency/doj/fisa/fisc0912.pdf. כמו כן התבטאויות של מי שהעידו לפני ה־Privacy and Civil Liberties Oversight Board מתייחסות לאיסוף תעבורת תקשורת היישר משדרת המידע של רשת האינטרנט.

173 ראו Privacy and Civil Liberties Oversight Board, **לעיל** בפרק זה ה"ש 157, בעמ' 7.

174 ראו בחלק 3.2.3.3 **להלן**.

175 CJEU, C-362/14 (Maximillian Schrems v Data Protection Commissioner), 6.10.2015

176 ראו בחלק 3.2.3.3 **להלן**.

הרפורמה שהכניס חוק החירות (USA Freedom Act) בדיני המודיעין הזר בעקבות חשיפותיו של סנודן לא פסחה על הדינים שמכוחם ביססו הסוכנות לביטחון לאומי (NSA) ובית המשפט למודיעין זר (FISC) את הסמכות להפעלת תוכניות מעקב נוסח PRISM וה־upstream collection. עם זאת תוכניות אלו לא בוטלו, והיקפה של הרפורמה בדינים אלו – הנוגעים בעיקר למי שאינם בגדר אדם אמריקאי[177] – מצומצם מזה של הרפורמה בדינים הנוגעים לאיסוף מודיעין זר שבסעיף 215 או ל"מעקב אלקטרוני" למטרות איסוף מודיעין זר (שתואר לעיל בחלק 3.1.5, FISA). התיקון האחרון ל־FISA,[178] שאושר בקונגרס בתחילת 2018 ונועד להאריך את תוקף החוק, הוסיף בין השאר כמה בקרות סטטוטוריות על איסוף מודיעין זר ותקשורת, בייחוד בנוגע לפרקטיקות של איסוף תקשורת "על אודות" (about communication) של מטרה מודיעינית.[179]

כזכור, "מעקב אלקטרוני", כהגדרתו בחוק,[180] חל בנסיבות שבהן יש זיקה פרסונלית או טריטוריאלית לארצות הברית ("אדם אמריקאי"). במקרים שבהם אין זיקה כזאת, חל סעיף 702 ל־FISA.[181] סעיף זה נוגע לאיסוף מודיעין זר על מטרות מודיעיניות שיש יסוד סביר להניח שהן מחוץ לארצות הברית ואינן בגדר אדם אמריקאי.[182] סעיפים 703 ו־704 של FISA[183] חלים על איסוף מודיעין זר על מטרות שהן בגדר אדם אמריקאי ואינן בתחומי המדינה. עתירה לבית המשפט

177 להגדרת "אדם אמריקאי" ראו **לעיל** בפרק זה ה"ש 134.

178 FISA Amendments Reauthorization Act of 2017 (S.139, 115th Cong. 2017–2018) (להלן: FISA Amendments Act 2017).

179 תקשורת "על אודות" (about communication) היא תקשורת הכוללת התייחסות ליעד מודיעיני, והיא אינה תקשורת שהיעד הוא צד לה (סעיף 103(b)(1)(A) לחוק המתקן, 50 U.S.C. §1881a(m(4)(B)(ii) בחוק המתוקן.

180 50 U.S.C. §1801(e)

181 50 U.S.C. §§1881–1881a

182 לפי סעיף 702, ייתכן איסוף אחר מטרות שבדיעבד התברר שהן בגדר אדם אמריקאי, אך לא יאושר איסוף שנעשה בכוונה תחילה אחר אדם אמריקאי (§1881a(b)(3)).

183 50 U.S.C. §§1881b–1881c

העליון בעניין *Clapper v. Amnesty Int'l USA*[184] תקפה את סעיף 702, אך זו נדחתה בשל היעדרה של זכות עמידה.

שלא ככללים החלים על מעקב אלקטרוני אחרי מי שהוא אדם אמריקאי בתחומי ארצות הברית, מעקב אחר יעד מודיעיני לפי ההסדר שבהוראות סעיף 702[185] אינו טעון צו שיפוטי מבית המשפט למודיעין זר (FISC), ואף אין כל דרישה בעניין זהות היעד.[186] כדי לאסוף (עד תקופה של שנה) מודיעין מיעדים שיש יסוד סביר להאמין כי אינם מצויים בארצות הברית, די באישור הכתוב המשותף של התובע הכללי ומנהל המודיעין הלאומי (ODNI — Director of National Intelligence)[187] ובתנאי שאישור זה אינו מגדיר בכוונה מטרות מודיעיניות שהן בחזקת אדם אמריקאי או שידוע כי הן מצויות בארצות הברית, או שתכליתו בפועל לאסוף מודיעין על מטרות מודיעיניות בתחומי ארצות הברית, או שתכליתו להשיג תקשורת "על אודות" יעד מודיעיני,[188] ובתנאי שהפרקטיקה המודיעינית המופעלת במסגרת האישור אינה מפרה את התיקון הרביעי לחוקה.[189] על התובע הכללי, בהתייעצות עם מנהל המודיעין הלאומי, לגבש כללים שיבטיחו עמידה בתנאים מגבילים אלו ולהעבירה לוועדות המודיעין של הקונגרס, לוועדת בית הנבחרים לשיפוט ולבית המשפט למודיעין זר.[190]

התיקון האחרון לחוק איסוף מודיעין זר (FISA) מגדיר נוהל נפרד לאיסוף תקשורת "על אודות", ולפיו אם החליטו מנהל המודיעין הלאומי והתובע הכללי על יישום תוכנית לאיסוף מכוון של תקשורת מסוג זה, עליהם ליידע בכתב את הקונגרס שלושים יום טרם הפעלת התוכנית. על ההודעה לקונגרס לכלול

184 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013)

185 50 U.S.C. §1881a(a)

186 השוו לתנאי שבסעיף 1805(a)(2)§, שלפיו בית המשפט ייתן צו מעקב אלקטרוני אם יש יסוד סביר להניח שהיעד הוא ישות זרה (foreign power) או סוכן מטעמה.

187 לפי הפירוט ב־1881a(g)§.

188 סעיף זה התווסף במסגרת FISA Amendments Act 2017, **לעיל** בפרק זה ה"ש 178, סעיף 103(a)(3) לחוק שתיקן את סעיף 50 U.S.C. §1881a(b)(5) בחוק המתוקן.

189 50 U.S.C. §1881a(b)

190 50 U.S.C. §1881a(f)

צו, החלטה או חוות דעת מטעם בית המשפט למודיעין זר (FISC), המאשרים את התוכנית, ופירוט של הבקרות שנועדו לזהות הפרות מהותיות של הדין הרלוונטי.[191]

נוסף על כך, אישור לאיסוף מודיעיני לפי סעיף 702 ל־FISA טעון אימוץ נוהלי מזעור שיבטיחו כי האיסוף מוגבל למטרות המצויות מחוץ לארצות הברית ולא ייכללו בו תשדורות שכל הצדדים שבהן מצויים בתחומיה. זאת ועוד, איסוף כאמור מחייב לאמץ נוהלי צמצום דומים לאלו החלים במסגרת מעקב אלקטרוני פנימי.[192] על פי הוראות התיקון האחרון לחוק, על התובע הכללי ועל מנהל המודיעין הלאומי לבחון כל נוהל מזעור שאומץ ולפרסם גרסה לא מסווגת שלהם בהקדם האפשרי.[193]

ההסדר בסעיף 702 מאפשר לתובע הכללי ולמנהל המודיעין הלאומי להורות בכתב לספקי תקשורת אלקטרונית להעביר לרשויות כל מידע הנדרש להשלמת האיסוף המודיעיני באופן השומר על מרב החשאיות ואינו מפריע לשירותי התקשורת שהספק נותן למטרה המודיעינית ואינו פוגם בהם,[194] בתמורה לפיצויים מסוימים[195] ולפטירת הספק מכל אחריות משפטית.[196] ספק תקשורת רשאי לערער על בקשות כאלה לפני בית המשפט למודיעין זר (FISC).[197] על החלטת בית המשפט אפשר לערער לפני ערכאת הערעור (ה־Foreign Intelligence Surveillance Court of Review), ועל החלטתה של ערכאה זו אפשר לערער בגלגול שלישי לבית המשפט העליון.[198] התמודדותם של גופים

191 FISA Amendments Act 2017, Sec. 103

192 50 U.S.C. §1881a(c)–(e). כן ראו בטקסט המפנה לה"ש 135 **לעיל** בפרק זה.

193 FISA Amendments Act 2017, **לעיל** בפרק זה ה"ש 178, ס' 104 לחוק המתקן, 50 U.S.C. §1881a(e)(3) בחוק המתוקן.

194 50 U.S.C. §1881a(h)(1)

195 50 U.S.C. §1881a(h)(2)

196 50 U.S.C. §1881a(h)(3)

197 50 U.S.C. §1881a(h)(5)

198 50 U.S.C. §1881a(h)(6)

פרטיים בערכאה של בית המשפט למודיעין זר (FISC) אינה חפה מקשיים, שכן אחדות מהלכותיו חסויות, ולכן ערעורים של ספקי תקשורת פרטיים נדחים לעיתים בנימוק שמתבסס על חומר משפטי שאינו נגיש להם.[199]

אחת לתקופה שלא תעלה על שישה חודשים על התובע הכללי ועל מנהל המודיעין הלאומי להעריך עד כמה האיסוף הולם את נוהלי הצמצום והמזעור ואת הכללים המגבילים[200] שהם גיבשו.[201] הערכות אלו יוגשו לבית המשפט למודיעין זר (FISC) ולוועדות המודיעין והשיפוט בקונגרס. המפקח הכללי של משרד המשפטים והמפקחים הכלליים של גופי המודיעין הרלוונטיים רשאים לבחון בעצמם את מידת הציות לנהלים אלו, את מספר המטרות המודיעיניות שבדיעבד התגלה שהן מצויות בתחומי ארצות הברית ואת מידת הגישה לנתוני תקשורת ותוכן שנאספו מהן, וכן לבחון את מספר דוחות המודיעין שבהם מופיעים מי שהם בגדר אדם אמריקאי.[202]

ראשי סוכנויות הביון הרלוונטיות יבחנו מדי שנה כל איסוף שאושר לפי נוהלי סעיף 702 ל־FISA כדי לבדוק אם יש יסוד סביר להניח שיופק, או שאכן הופק, ממנו מודיעין זר, בהתייחס למידת המעורבות של מי שהם בגדר אדם אמריקאי בדוחות המודיעין שהופקו והופצו במסגרת פעולת האיסוף. תוצאות בחינה זו יופצו לבית המשפט למודיעין זר (FISC), לתובע הכללי, למנהל המודיעין הלאומי (ODNI) ולוועדות הקונגרס המתאימות.[203]

199 Aaron Mackey, *As a Provider Fought a Secret Surveillance Order, Court Access Denied It to Relevant Law*, Electronic Frontier Foundation (15.06.2017)

200 ראו בטקסט המפנה לה"ש 190 **לעיל** בפרק זה.

201 50 U.S.C. §1881a(d)–(e),(l)(1)

202 50 U.S.C. §1881a(l)(2)

203 50 U.S.C. §1881a(l)(3)

• הדין בארצות הברית הנוגע למעקב מקוון שמפעילה המדינה מושפע ברמה החוקתית משאלות הנוגעות לתחולה של התיקון הרביעי לחוקה – המגן על אזרחים מפני חיפוש ללא צו – על פרקטיקת איסוף ספציפית שנבחנת לנוכח שאלת הציפייה הסבירה לפרטיות בנסיבות העניין.

• הסדרה סטטוטורית של מעקב מקוון בתחומי ארצות הברית – בעיקר לתכליות של אכיפת חוק – מוסדר בחוק הפרטיות בתקשורת אלקטרונית (ECPA), שמתנה יירוט והשגה של נתוני תוכן ותקשורת בצו מאת בית המשפט. לצווים אלה רף משתנה של עילות, בהתאם לסוג הנתונים המבוקש.

• הדין האמריקני כמעט שאינו מתייחס לסוגיות של שימור נתונים (data retention).

• הסדר סטטוטורי נפרד מתיר מעקב מקוון לתכליות ביטחוניות (איסוף "מודיעין זר") בתחומי ארצות הברית בכפוף לצו מאת ערכאה חשאית מיוחדת, בית המשפט למודיעין זר (FISC). ההוראות החלות על איסוף נתוני תקשורת (metadata) למטרות של מודיעין זר הוקשחו בעקבות תיקוני חוק החירות (USA Freedom Act), אך גם לאחר שאלו נתקבלו, הסוכנות לביטחון לאומי (NSA) יכולה לבקש צו להעברת נתוני תקשורת על מזהה (identifier) מבוקש עד לרמה של נתונים מסדר שני (two-hop), או "חברים של חברים" של אותו מזהה).

• מעקב מקוון אחר יעדים שאין להם זיקה טריטוריאלית לארצות הברית (אינם בגדר "אדם אמריקאי") אינו כפוף לאישור בית המשפט.

.3.2 האיחוד האירופי

תפיסת הגנת הפרטיות האירופית שונה מזו האמריקאית.[204] בניגוד לארצות הברית, שבה החקיקה המסדירה את הגנת הפרטיות מתמקדת בהוראות החלות על רשויות המדינה בבואן לאסוף מידע על האזרחים ולהשתמש בו, דיני הגנת הפרטיות האירופיים עוצבו כמסגרת שחלה על המגזר הפרטי והציבורי גם יחד, לכאורה ללא הבחנה.[205] עם זאת בפועל חוקי הגנת הפרטיות האירופיים מתמקדים במגזר הפרטי, שכן חקיקת האיחוד האירופי מוגבלת לתחולה המהותית של דיני האיחוד.[206] לכן דברי החקיקה האירופיים העיקריים מחריגים מתחולתם עיבוד מידע פרטי לתכליות שאינן מצויות בתחולת דיני האיחוד כגון תכליות של ביטחון לאומי ואכיפת חוק – אלו יוסדרו בחקיקה לאומית בכל אחת מהמדינות־החברות.

עם זאת הפסיקה של בית הדין האירופי לזכויות אדם (ECtHR — European Court of Human Rights), ולאחרונה גם בכמה מקרים בבית הדין האירופי לצדק (ECJ — European Court of Justice) מציבה מגבלות גם על פרקטיקות של מעקב מקוון שנוקטות המדינות־החברות למטרות ביטחוניות או לצורכי משטרה. גם דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)[207]

204 ראו Whitman, **לעיל** בפרק 2 ה"ש 35.

205 Orla Lynskey, The Foundations of EU Data Protection Law 16–26 (2016)

206 דוגמת Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with regard to the Protection of Personal Data and on the Free Movement on such Data [1995] OJ L'281/31 (להלן: דירקטיבת הגנת המידע); 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 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) (להלן: התקנות הכלליות בדבר הגנת מידע (GDPR)).

207 Directive (EU) 2016/680 of the European Union Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities

עשויה לייצר בסיס סטטוטורי שמגביל פרקטיקות אלה, ולו באמצעות העקרונות הכלליים המנויים בה.

3.2.1. הערות מקדימות

פרטיות לעומת הגנה על מידע פרטי

הדין האירופי מבחין בין פרטיות (privacy) ובין הגנה על מידע (data protection). האמנה האירופית לזכויות אדם (ECHR — European Convention on Human Rights) נוקטת לשון של כיבוד "החיים הפרטיים" (private life),[208] וכך גם סעיף 7 למגילת זכויות היסוד של האיחוד האירופי (CFR — Charter of Fundamental Rights of the European Union).[209] מנגד, סעיף 8 למגילה (CFR) וכן סעיף 16 לאמנה בדבר תפקודו של האיחוד האירופי (TEFU — Treaty on the Functioning of the European Union)[210] נוקטים לשון של "הגנה על מידע". גם חקיקת המשנה האירופית מדגישה את יסוד ההגנה על מידע ועל עיבודו ההוגן,[211] אך

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 (להלן: דירקטיבה 2016/680 או דירקטיבת רשויות אכיפת החוק).

208 Convention for the Protection of Human Rights and Fundamental Freedoms, Art 8(1) (European Convention on Human Rights, as amended) (להלן: ECHR או האמנה האירופית לזכויות אדם).

209 Charter of Fundamental Rights of the European Union, 2010 O.J. C 83/02 (להלן: CFR או מגילת זכויות היסוד).

210 Treaty on the Functioning of the European Union (TEFU) (להלן: TFEUאו האמנה בדבר תפקודו של האיחוד האירופי).

211 דוגמת דירקטיבת הגנת המידע, התקנות הכלליות בדבר הגנת מידע (GDPR), דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), וכן ראו גם 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 2009/136/EC (e-Privacy Directive). (להלן: דירקטיבת הפרטיות האלקטרונית); Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and

לעיתים נוקטת לשון של פרטיות. התחולה המהותית של "חיים פרטיים" אינה חופפת את התחולה המהותית של דיני הגנת המידע, החלים על מידע על אדם בר־זיהוי,[212] וגם ההגבלה המותרת של זכויות אלה שונה בהתבסס על המסמך שבו כל זכות מופיעה – האמנה האירופית לזכויות אדם (ECHR) או מגילת זכויות היסוד (CFR), ועל פסקת ההגבלה המצויה בכל מסמך – סעיף 8(2) לאמנה (ECHR)[213] או סעיף 51 למגילה (CFR). כך למשל לפי סעיף 8(2) לאמנה (ECHR), התכליות הלגיטימיות שלמענן תותר פגיעה בזכות לפרטיות הן אינטרסים של ביטחון לאומי, ביטחון הציבור או טובתה הכלכלית של המדינה, או לשם מניעת פשע והפרות סדר, הגנה על בריאות, על המוסר ועל זכויותיהם וחירויותיהם של אחרים. במגילת זכויות היסוד (CFR) לעומת זה הנוסח רחב יותר, ומאפשר פגיעה בזכות לשם אינטרסים כלליים שהוכרו באיחוד.[214]

בהמשך הדברים נראה כי בניגוד למדינות אחרות, הדין האירופי כמעט שאינו שועה להבחנה בין נתוני תקשורת לנתוני תוכן הבחנה חשובה לדיני המעקב המקוון במדינות אחרות. מאחר שלפי שעה חקיקת המשנה האירופית מחריגה מתוכה פעילויות אלו,[215] הבחנה זו כמעט שלא הוזכרה בחקיקה האירופית – חוץ מאשר בדירקטיבת שימור הנתונים (Data Retention Directive) שנפסלה בבית הדין האירופי לצדק (ECJ), ובהוראות מסוימות בדירקטיבת הפרטיות האלקטרונית (e-Privacy Directive).[216] מטעמים דומים לא פותחו בדין האירופי

judicial cooperation in criminal matters. (להלן: החלטת המסגרת). כן ראו **להלן** בחלקים המתארים דברי חקיקה אלה.

212 ראו ס'1 לדירקטיבת הגנת המידע, ס'4(1) לתקנות הכלליות בדבר הגנת מידע (GDPR).

213 בהקשר זה יש להזכיר גם את סעיף 13 ל־ECHR, שלפיו מי שזכויותיהם לפי האמנה הופרו, זכאים לתרופה מרשות לאומית.

214 להרחבה ראו Juliane Kokott and Christoph Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 Int'l Data Privacy L. 222 (2013)

215 ראו חלק 3.2.3.5 **להלן**.

216 דירקטיבת הפרטיות האלקטרונית מתייחסת לנתוני תעבורה (traffic data) ולנתוני מיקום (location data), **להלן** בפרק 3 ה"ש 301, ומכילה מגבלות על עיבודם ועל שימורם. המדינות יכולות לצמצם את המגבלות האלו באמצעות חקיקה לתכליות של ביטחון לאומי (ס' 15(1) לדירקטיבה).

הבחנות דומות לאלו שבדין האמריקאי[217] בין אזרחי האיחוד למי שאינם, ודיני הגנת המידע האירופיים חלים על כל המצויים בתחומי האיחוד (לרבות בתקנות הכלליות בדבר הגנת מידע (GDPR – General Data Protection Regulation).

קטגוריות של דברי חקיקה

יש לזכור שהדין האירופי הוא דין משלים לדין המדינתי של כל אחת מהמדינות־החברות באיחוד האירופי. בדין האירופי יש מדרג נורמטיבי שמבחין בין דברי חקיקה, ויש הבחנה בין תקנות (regulations), דירקטיבות (directives), החלטות (decisions), המלצות (recommendations) וחוות דעת (opinions).[218] **לתקנות**, כמו ל**אמנות**, השפעה ישירה: תוקפן מחייב מיד את כל המדינות־החברות, ללא תלות בחקיקה של המדינה. המדינות־החברות מחויבות שלא להפריע לתחולה הישירה הטבועה בתקנות.[219] לצד תחולה ישירה, התקנות משפיעות ישירות על תושבי האיחוד, והם יכולים להסתמך עליהן בבתי משפט של המדינה.

דירקטיבות הן הנחיות בתחום מסוים שניתנות למדינות־החברות, והן מקנות להן מרחב פעולה בכל הנוגע ליישום המקומי שלהן בחקיקה או באסדרה. התחולה של דירקטיבה אינה ישירה או מיידית, וכך גם השפעתה: דירקטיבה תורה למדינות־החברות להתאים את דברי החקיקה שלהן להוראותיה, אבל ככלל אין הוראותיה משמשות בסיס ישיר לחובות ולזכויות בדין המדינתי. עם זאת עם הזמן חיזק בית הדין האירופי לצדק (ECJ) את תחולתן של הדירקטיבות ואת מידת השפעתן.[220]

217 ראו בחלק 3.1.5 **לעיל**.

218 ס' 288 לאמנה בדבר תפקודו של האיחוד האירופי.

219 ראו ECJ, Case 34/73 (Variola v. Italian Finance Administration), 10.10.1973

220 ראו למשל ליאור זמר ושרון פרדו, "הרהורים על אקטיביזם שיפוטי: מקרה בית־המשפט האירופי" **משפט ועסקים** ז 203–247, 230–233 (2007); Anthony Arnull, *the Effect of EU Law*, A Companion to Europian Union Law and International Law (2016, Dennis Patterson and Anna Sodersten eds.); Alina Kaczorowska, European Union Law 267-297 (3rd Edition, Routledge, 2013)

3.2.2. הרמה החוקתית: הזכות לפרטיות מכוח אמנות האיחוד

הגנת המידע האירופית מוסדרת בפרטי חקיקה ספציפיים.[221] הרפורמה שנכנסה לתוקף בשנת 2018 במסגרת התקנות הכלליות בדבר הגנת מידע (GDPR) ודירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), מרחיבה את תחולתם של הדינים האירופיים בדבר הגנת המידע גם למעבדי מידע (processors) ולמנהלי מאגרים (data controllers) שמקום מושבם אינו באיחוד האירופי ומחילה עליהם חובות חדשות, לצד הרחבת היקף הזכויות המוקנות למושאי המידע. על פרטי חקיקה אלו חולשת המסגרת החוקתית של דיני האיחוד, ובעיקר הסעיפים של מגילת זכויות היסוד (CFR) והאמנה לזכויות אדם (ECHR) המתייחסים להגנת הפרטיות. משטר הגנת המידע הקיים מחריג מתחולתו עיבוד נתונים למטרות ביטחוניות ומשטרתיות,[222] ולכן הזכות לפרטיות – על מופעיה ברמה החוקתית של דיני האיחוד – משחקת תפקיד נכבד. פרשנות התקנות הכלליות בדבר הגנת מידע (GDPR) תיעשה לאור הזכויות מכוח מגילת זכויות היסוד (CFR), האמנה לזכויות אדם (ECHR) או האמנה בדבר תפקודו של האיחוד האירופי (TFEU).

סעיף 8 לאמנה לזכויות אדם (ECHR) קובע כי לכל אחד הזכות שפרטיותו, חיי משפחתו, ביתו והתכתבויותיו יכובדו. פגיעה בזכות זו מצד רשות ציבורית תהא לפי דין, וכשהדבר נדרש בחברה דמוקרטית למטרות האלה: שמירה על אינטרסים של ביטחון לאומי וביטחון הציבור או על טובתה הכלכלית של המדינה; מניעת פשע והפרות סדר; הגנה על בריאות או על המוסר; ושמירת זכויותיהם וחירויותיהם של אחרים.

סעיפים 7 ו־8 למגילת זכויות היסוד (CFR) מהדהדים את הזכות שבסעיף 8 לאמנה לזכויות אדם (ECHR) ומוסיפים עליה את הזכות להגנה על מידע. סעיף 7 קובע כי לכל אחד הזכות שפרטיותו, חיי משפחתו, ביתו והתקשורת שהוא מקיים יכובדו. סעיף 8 למגילה (CFR) מוסיף על הזכות לפרטיות גם את הזכות להגנה על מידע: לכל אחד הזכות להגנה על המידע הפרטי שלו, ולכך שהוא יעובד בהגינות, למטרות מוגדרות ועל בסיס הסכמתו. נדרש שזכויות אלו ייפגעו רק לפי דין, בכפוף לעקרון המידתיות ובהתקיים צורך בשל אינטרסים כלליים המוכרים

221 ראו חלק 3.2.3 **להלן**.

222 ראו ביתר פירוט בחלק 3.2.3.5 **להלן**.

באיחוד.[223] בעניין *Digital Rights Ireland* (ראו להלן)[224] אימץ בית הדין האירופי לצדק (ECJ) סטנדרט של בחינה מחמירה (strict review) של מידתיות הפגיעה בזכויות מכוח סעיפים 7 ו־8 למגילת זכויות היסוד (CFR). סטנדרט כזה מתיר למחוקק האירופי מרחב צר של שיקול דעת, ודורש את קיומו של צורך מוחלט (strict necessity) כדי לאפשר פגיעה כזו.[225]

האמנה בדבר תפקודו של האיחוד האירופי (TFEU) חוזרת בסעיף 16(1) על רוח סעיף 8(1) למגילת זכויות היסוד (CFR), וקובעת כי לכל אחד תהא הזכות להגנה על המידע האישי הנוגע לו. יש הגורסים כי לזכות זו יש השפעה ישירה (direct effect) על הדין הפנימי של מדינות האיחוד, וכי אנשים פרטיים יכולים להסתמך עליה בבתי הדין של המדינה כדי לתקוף חקיקה מדינתית לפי דיני האיחוד.[226]

ההלכה האירופית בנוגע למעקב אחר תקשורת נתונים מקורה בעיקר בבית הדין האירופי לזכויות אדם (ECtHR),[227] ולאחרונה בכמה מקרים נשמעה בנושא גם

223 ס' 52 למגילת זכויות היסוד (CFR). כן ראו ECJ, joined cases C-465/00, C-138/01 and C-139/01 (Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v. Österreichischer Rundfunk), 20.05.2003, [2003] E.C.R. I-04989, פס' 86; ECJ, case C-275/06 (Productores de Música de España (Promusicae) v. Telefónica de España SAU), 29.01.2008, [2008] E.C.R. I-00271, פס' 54; ECJ, joined cases C-92/09 and C-93/09 (Volker und Markus Schecke GbR Hartmut Eifert v. Land Hessen), 9.11.2010, [2010] E.C.R. I-11063, פס' 72.

224 ראו חלק 3.2.4 **להלן**.

225 ראו גם ECJ, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy (16.12.2008), בפס' 56; ECJ, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen (9.11.2010)

226 Hielke Hijmans & Alfonso Scirocco, *Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty be Expected to Help*, 46 Common Market L. Rev 1485-1525, 1517 (2009); Hielke Hijhamns, The European Union as Guardian of Internet Privacy: the story of Art. 16 TFEU (Springer, 2016)

227 ראו למשל Klass & Others v. Germany, No. 5029/71, Eur. Ct. H.R. (1978); Malone v. UK, No. 8691/79 Eur. Ct. H.R. (1984); Huvig v. France, No.

דעתו של בית הדין האירופי לצדק (ECJ).[228] בשנת 2006 פירט בית הדין לזכויות אדם (ECtHR) בעניין *Huvig* את התנאים הנדרשים מכוח סעיף 8(2) לאמנה לזכויות אדם (ECHR) להפעלת מעקב טלפוני. כדי שהאמצעי המתערב בזכות לפרטיות של סעיף 8(1) לאמנה יהא "לפי חוק" (כדרישת סעיף 8(2)), עליו להיות מבוסס על הוראות הדין הלאומי,[229] על הדין להיות נגיש לנוגעים בדבר,[230] ועליהם להיות מסוגלים לצפות את השלכותיו עליהם. נוסף על כך, על האמצעי המתערב להלום את שלטון החוק.[231] מבחינה מהותית נאמר בעניין *Huvig* כי על החוק לפרט את אופן יישומו של שיקול הדעת של הרשות הציבורית ואת היקפו:[232] (1) סוג האנשים הנתונים במעקב; (2) אופי העבירות שבגינן מתבצע

11105/84, Eur. Ct. H.R. (1990); Rotaru v. Romania, No. 28341/95, Eur. Ct. H.R. (2000); Gilian & Quinton v. UK, No. 4158/05, Eur. Ct. H.R. (2010); Kennedy v. UK, No. 26839/05, Eur. Ct. H.R. (2010); Uzun v. Germany, No. 35623/05, Eur. Ct. H.R. (2010); Colon v. Netherlands, No. 49458//06, Eur. Ct. H.R. (2012); Zakharov v. Russia, No. 47143/06, Eur. Ct. H.R. (2015); Dragojevic v. Croatia, No. 68955/11, Eur. Ct. H.R. (2015); Sazbo and Vissy v. Hungary, No. 37138/14, Eur. Ct. H.R. (2016); Barbukescu v. Romania, No. 61498/08, Eur. Ct. H.R. (2016); Weber and 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 and Others v. The United Kingdom,* Nos. 58170/13, 62322/14 and 24960/15 Eur. Ct. H.R. (2018) (להלן: עניין **האח הגדול**).

228 ראו עניין *Schrems*, **לעיל** בפרק זה ה"ש 175, הדן בהשפעות של מעקב המונים (mass surveillance) על העברת נתונים לחברות פרטיות אמריקאיות, וכן ההחלטות המתייחסות לחקיקה המחייבת ספקי תקשורת בשימור נתונים: CJEU, Joined cases C-293/12 and C-594/12 (Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources, Seitlinger and Others), [2014] E.C.R. I-238 (18.4.2014) (להלן: עניין *DRI*); 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 Sverige AB*).

229 ראו עניין *Huvig*, **לעיל** בפרק זה ה"ש 227, בפס' 28. שם נאמר "דין", לרבות חקיקת משנה ודין שאינו חרות.

230 **שם**, פס' 29.

231 **שם**, פס' 26.

232 ראו גם עניין *Rotaru*, **לעיל** בפרק זה ה"ש 227.

המעקב; (3) הגבלה על משך המעקב; (4) נוהלי עיבוד הנתונים; (5) בקרות על העברת המידע; (6) התנאים למחיקת המידע או השמדתו.[233] דרישה שביעית, אופציונלית, נוגעת לבקרה שיפוטית אפריורית על אמצעי מעקב.[234]

ניתוח היישום של הלכת *Huvig*[235] מראה שבחינה מחמירה של הבקרות המנויות לעיל משתנה לפי נסיבות המקרה, וכי בהקשרים של טרור,[236] ביטחון הציבור[237] ומעקב בעבודה[238] לא ערך בית הדין (ECtHR) בחינה מחמירה. מלגירי ודה הרט סבורים שבית הדין נוטה לבחון בקרות כאלו בחינה מחמירה כשהאינטרס המונח על הכף אינו אינטרס ביטחוני "חיוני" (הפרות סדר או עבירות סמים), או כשהוא בעל יסוד פוליטי (מחאות אופוזיציוניות) או כלכלי.[239]

בעניין *Szabo*,[240] קבע בית הדין (ECtHR) כי חוק הביון ההונגרי סותר את הוראות סעיף 8 לאמנה לזכויות אדם (ECHR). לפי אותו חוק, סמכויות המעקב לצורכי ביטחון לאומי היו כפופות לאישור מיניסטריאלי, בבקרה שיפוטית, ללא קישור לעבירות מסוימות ועל בסיס צווים שניסוחם כללי למדי. בית הדין הסיק כי סמכויות אלו עלולות לסלול את הדרך למעקב לא מוגבל אחר אזרחים רבים.[241] מעקב כזה יחליף את איום הטרור באיום של חדירה לא מרוסנת לפרטיות

233 פס' 34 בעניין *Huvig*, **לעיל** בפרק זה ה"ש 227.

234 **שם**, בפס' 33, וראו גם Gianclaudio Malgieri & Paul De Hert, *European Human Rights, Criminal Surveillance and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably But Necessarily By Judges, in* Cambridge Handbook of Surveillance Law 509-532 (D. Gray & S. Henderson, eds.) (2017)

235 Malgieri & De Hert, **שם**, בחלק IV.

236 עניין *Uzun* (אפשר גם שבעניין *Klass*, שנגע למעקב שביצע השירות החשאי הגרמני, ותכליתו לא פורטה), **לעיל** בפרק זה ה"ש 227.

237 עניין *Colon*, **לעיל** בפרק זה ה"ש 227.

238 עניין *Barbulescu*, **לעיל** בפרק זה ה"ש 227.

239 Malgieri & De Hert, **לעיל** בפרק זה ה"ש 234, בחלק IV.

240 עניין *Szabo*, **לעיל** בפרק זה בה"ש 227.

241 **שם**, פס' 67.

האזרחים באמצעות סמכויות וטכניקות מעקב רבות עוצמה.[242] לפי בית הדין יש להראות את קיומו של צורך מוחלט באמצעי המעקב (strictly necessary) בשני מישורים: צורך מוחלט כללי לשם הגנה על המוסדות הדמוקרטיים; ובה בעת צורך מוחלט קונקרטי בנסיבות המסוימות של הפעלתו לצורכי השגת מודיעין על אדם ספציפי.[243] בהקשר זה קבע בית הדין כי אין די באישור המיניסטריאלי כדי להעריך במידה מספקת את דבר קיומו של צורך מוחלט. פסק דין זה מחזק את רוחה של הלכת *Huvig* הוותיקה, ובמצטבר עם ההלכה שנקבעה בפרשת *Zakharov*,[244] מעיד על עמדה נחושה שבית הדין האירופי לזכויות אדם (ECtHR) נוקט נגד תת־אסדרה של מעקב גורף וחסר הבחנה.

עם זאת, שתי החלטות שניתנו לאחרונה – בעניין **האח הגדול** ובעניין *Rättvisa*[245] – יכולות ללמד על גישה מורכבת יותר לפרקטיקות של איסוף גורף (bulk collection). בשני עניינים בחן בית הדין האירופי לזכויות אדם את משטרי האיסוף של בריטניה ושוודיה בהתאמה, ביוצאו מתוך נקודת הנחה שאיסוף גורף כשהוא לעצמו אינו אסור, אלא שיש להכפיפו לבקרות סטטוריות ברוח הלכת *Huvig*.[246]

3.2.3. המשטר האירופי להגנת המידע: דירקטיבת הגנת המידע (דירקטיבה 95/46/EC) והתקנות הכלליות בדבר הגנת מידע (GDPR)

ליבתו של המשטר האירופי הנוכחי להגנת המידע התבססה על דירקטיבה בת עשרים שנה – דירקטיבת הגנת המידע (דירקטיבה 95/46/EC) – שבשנת 2018 הוחלפה בתקנות הכלליות בדבר הגנת מידע (GDPR). התקנות הכלליות אינן

242 **שם**, פס' 68.

243 **שם**, פס' 73.

244 עניין *Zakharov*, **לעיל** בפרק זה בה"ש 227.

245 עניין **האח הגדול** ועניין *Rättvisa*, **לעיל** בפרק זה ה"ש 227.

246 להרחבה ראו עמיר כהנא "מעקב מקוון בישראל – לא להמתין לסנודן המקומי" **אתר המכון הישראלי לדמוקרטיה** (14.10.2018).

חלות על פעולות עיבוד נתונים הקשורות לאכיפת חוק ולביטחון לאומי,[247] שכן עליהן חלים הדין המקומי במדינות־החברות (הנתונות לביקורתו החוקתית של הדין האירופי, שתוארה לעיל); הנחיית המסגרת לעיבוד נתונים לצורכי שיתוף פעולה בין רשויות אכיפת החוק (החלה על העברות נתונים בין רשויות האכיפה והחקירה של מדינות האיחוד); ומאז מאי 2018 – עם כניסתה לתוקף – גם דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).[248]

מאחר שדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) עוצבה לאור העקרונות האירופיים של הגנת המידע – החלים על המגזר הפרטי – יש מקום לבחון אותם בקצרה. יתר על כן, ההוראות החלות על המגזר הפרטי עשויות להיות רלוונטיות בבואו להתמודד עם דרישות מטעם רשויות הביטחון והאכיפה להעברת מידע פרטי.

3.2.3.1. עקרונות של עיבוד מידע

דירקטיבת הגנת המידע מגדירה "מידע פרטי" (personal data) ככל מידע שקשור לאדם בר־זיהוי (בעיקר באמצעות מספר מזהה או מאפיין אחד או יותר המיוחדים לזהותו הפיזית, הפיזיולוגית, המנטלית, הכלכלית או החברתית).[249] עיבוד מידע פרטי הוא כל פעולה או מערך פעולות המתבצעות על מידע פרטי (לרבות אחסונו, איסופו והעברתו לצדדים שלישיים). בתקנות הכלליות בדבר הגנת מידע (GDPR) עודכנו הגדרות אלו כדי לכלול במפורש קטגוריות נוספות של מידע פרטי ודרכים לעיבודו.[250]

הדירקטיבה מורה למדינות־החברות להבטיח בחקיקה כי עיבוד מידע פרטי יתבצע לאור כמה עקרונות שיבטיחו את איכותו: (1) מידע פרטי יעובד בהגינות ולפי חוק; (2) איסוף מידע פרטי ייעשה לתכליות מוגדרות, מפורשות ולגיטימיות, ועיבודו לא יתבצע בחריגה מהן; (3) מידע פרטי צריך להיות הולם, רלוונטי ולא

247 ראו ס' 3(2), 13(1) לדירקטיבת הגנת המידע, וכן ס' 2(2)(1)23 ,(d) לתקנות הכלליות בדבר הגנת מידע (GDPR).

248 ראו חלק 3.2.5.2 **להלן**.

249 ס' 1 לדירקטיבת הגנת המידע.

250 ס' 4 לתקנות הכלליות בדבר הגנת מידע (GDPR).

לחרוג בהיקפו מהתכלית שלשמה הוא נאסף או מעובד; (4) מידע פרטי יהא מדויק, ולפי הצורך – עדכני. יש לנקוט כל אמצעי סביר כדי להבטיח שמידע אישי שלפי התכליות שלשמן נאסף או מעובד אינו שלם או מדויק, יימחק או יתוקן; (5) מידע אישי יישמר באופן שלא יתאפשר זיהוי מושאיו לפרק זמן העולה על הנדרש לפי תכליותיו.[251] התקנות הכלליות בדבר הגנת מידע (GDPR) הוסיפו גם עיקרון שישי של אבטחת מידע.[252]

עיבוד מידע פרטי מותר, לפי סעיף 7 לדירקטיבת הגנת המידע, בכפוף להסכמת מושא המידע[253] או בהתקיים תנאי אחר (לדוגמה, כשפעולת העיבוד מקורה בחובה לפי דין, כשהעיבוד נדרש לצורך קיום חוזה שמושא המידע הוא צד לו לצורך הגנת האינטרסים החיוניים של מושא המידע, ולצורך תכלית המגשימה אינטרס ציבורי). סעיף 8 לדירקטיבה מונה קטגוריות מיוחדות של מידע פרטי שעיבודן אסור: מידע המסגיר גזע, מוצא אתני, השקפות פוליטיות, דתיות או פילוסופיות, השתייכות לארגוני עובדים ומידע הנוגע לבריאות ולחיי אישות.[254] עיבוד מידע פרטי מקטגוריות אלו מותר בהסכמת מושא המידע או בהתקיים אחד מהחריגים האחרים שבסעיף, בכללם החריג שלפיו עיבוד כאמור מותר אם ההחרגה הותרה לפי חוק של המדינה החברה, ובלבד שהוראותיו כוללות הגנות מספקות.[255]

3.2.3.2. זכויות של מושאי המידע

דירקטיבת הגנת המידע מורה למדינות־החברות להטיל חובות על מנהלי המאגרים שנועדו להבטיח את זכויותיהם של מושאי המידע (data subjects).

251 ס' 6 לדירקטיבת הגנת המידע.

252 ס' 5(1)(f) לתקנות הכלליות בדבר הגנת מידע (GDPR).

253 ס' 7(1) לדירקטיבת הגנת המידע נוקט לשון של unambiguous consent. התקנות הכלליות בדבר הגנת מידע (GDPR) מפרטות את התנאים הנדרשים לקיום הסכמה כזו באשר לבגירים (ס' 7 ל־GDPR) ולילדים (ס' 8 ל־GDPR).

254 ס' 8(1) לדירקטיבת הגנת המידע. נוסח זהה מצוי בסעיף 9(1) לתקנות הכלליות בדבר הגנת מידע (GDPR), ואליו התווספו קטגוריות של מידע גנטי, ביומטרי ונטייה מינית.

255 ס' 8(5) לדירקטיבת הגנת המידע.

מנהל מאגר (controller) הוא מי שבכוחו לקבוע את מטרות העיבוד של מידע פרטי; מעבד (processor) הוא מי שמבצע את העיבוד.[256]

הדירקטיבה קובעת זכות ליידוע, שלפיה מנהל המאגר או מי מטעמו יספק למושא המידע לכל הפחות את פרטי הזהות של מנהל המאגר, את מטרות העיבוד, מידע נוסף הנוגע לצדדים שלישיים שלהם המידע מיועד, את קיומה של זכות גישה למידע והזכות לתיקונו וכל פרט אחר שעשוי להיות רלוונטי לעיבוד נתונים הוגן.[257] זכות היידוע תקפה גם למקרים שבהם המידע האישי לא נלקח ישירות ממושא המידע.[258] מושא המידע רשאי לקבל ממנהל המאגר את המידע שמנהל המאגר מחזיק עליו, ובמקרים מסוימים גם הסברים באשר ללוגיקת העיבוד שלו.[259] הוראות דומות מצויות גם בתקנות הכלליות בדבר הגנת מידע (GDPR).[260] פעולות של עיבוד מידע יפורסמו בפומבי במרשם שתנהל הרשות המפקחת.[261]

256 ס' 2 לדירקטיבת הגנת המידע.

257 ס' 10 לדירקטיבת הגנת המידע. ראו גם Deryck Beyeleveld, *The Duty to Provide Information to the Data Subject: Articles 10 and 11 of Directive 95/46/EC* in The Data Protection Directive and medical research across Europe, 69–88 (Aldershot, Ashgate, 2014)

258 ס' 11 לדירקטיבת הגנת המידע.

259 ס' 12 לדירקטיבת הגנת המידע. שימושם של ארגונים אזרחיים בזכות הגישה למידע (Right Of Access To Information) מאפשר חשיפה של היקף המידע שחברות פרטיות וספקי שירותים מקוונים אוצרים על המשתמשים שלהן (ראו למשל ג'ודית דאבפורטייל, "ביקשתי מטינדר את המידע שלי – קיבלתי את ההעדפות המיניות והסודות האפלים ביותר" **הארץ** 28.9.2017); מקרה נוסף מן העת האחרונה הוא של אקטיביסט אמריקאי שניסה להשתמש בזכות הגישה למידע האישי כדי לקבל את הנתונים עליו המוחזקים בחברת קיימברידג' אנליטיקה – חברה פרטית שמנתחת רשתות חברתיות – שהיו עשויים לחשוף מידע על הקמפיין המקוון של דונלד טראמפ ועל שיטות הפעולה שלו. ראו Carole Cadwallader, *British Courts May Unlock Secrets of How Trump Campaign Profiled US Voters*, The Guardian (1.10.2017). פעילותה של קיימברידג' אנליטיקה נחשפה בעקבות חשיפה של עובד לשעבר בחברה, ועליה ראו במקורות המפורטים **להלן** בפרק 4 ה"ש 139.

260 ס' 13 לתקנות הכלליות בדבר הגנת מידע (GDPR). ס' 13(2) הוסיף פרטים ליידועו של מושא המידע: תקופת שימור הנתונים, קיומה של הזכות למחיקה, תיקון או הגבלה של הגישה למידע הפרטי, הזכות לסגת מההסכמה בנסיבות מסוימות והזכות להתלונן לפני רשות הפיקוח. ס' 13(3) מורה למעבד ליידע את מושא המידע כשבכוונתו להשתמש במידע למטרות החורגות מאלה שלשמן הוא נאסף.

261 ס' 21 לדירקטיבת הגנת המידע.

בנסיבות מסוימות מושאי המידע רשאים להתנגד לעצם עיבוד המידע הפרטי שלהם.[262] למושאי המידע גם עומדת הזכות שלא להיות מושאים של החלטה שעשויה להשפיע עליהם באופן מהותי מבחינה משפטית או אחרת, ושתתבסס על תהליכים אוטומטיים בלבד,[263] אלא אם הדבר נעשה לפי חוזה שמושא המידע צד לו, או לפי דין המדינה־החברה ובכפוף לאמצעים השומרים על האינטרסים הלגיטימיים של מושא המידע. זכויות נוספות העומדות למושאי המידע הן הזכות לסודיות (confidentiality) בעיבוד[264] והזכות לאבטחת המידע.[265]

3.2.3.3. העברת מידע לצדדים שלישיים

דירקטיבת הגנת המידע כוללת הוראות מפורטות בדבר העברת הנתונים לצדדים שלישיים, בעיקר כאלה המצויים במדינות זרות.[266] הנחת המוצא היא כי משטר הגנת המידע בתחומי האיחוד מבטיח את זכויותיהם של מושאי המידע. צדדים שלישיים בתחומי האיחוד המקבלים מידע ממנהלי מאגרים או ממעבדים נדרשים לפעול בהתאם לעקרונות המשטר האירופי להגנת המידע. יש להבטיח כי המידע מועבר אליהם בהלימה עם הדין האירופי (בכפוף להסכמה המודעת של מושא המידע, בצמידות למטרות האיסוף וכדומה). כשהמידע מיוצא אל מחוץ לגבולות האיחוד, יש להבטיח כי משטר הגנת המידע של מדינת היעד מספק רמת הגנה ראויה למושאי המידע (ולחלופין – כי מושאי המידע הסכימו מדעת להעברת נתונים זו). ועדה אירופית[267] או המדינות־החברות יקבעו תוך כדי יידוע הדדי את רמת ההגנה במדינות היעד. מקרב המדינות שקבוצת העבודה האירופית שלפי סעיף 29 לדירקטיבה קבעה כי הן מספקות רמת הגנה ראויה נמצאת גם ישראל.[268]

262 ס' 18 לדירקטיבת הגנת המידע.

263 ס' 15(1) לדירקטיבת הגנת המידע.

264 ס' 16 לדירקטיבת הגנת המידע.

265 ס' 17 לדירקטיבת הגנת המידע.

266 ס' 25–26 לדירקטיבת הגנת המידע.

267 לפי ס' 31 לדירקטיבת המידע.

268 Article 29 Data Protection Working Party, Opinion 2009/6 on the level of protection of personal data in Israel (1.12.2009)

משטר הגנת המידע בארצות הברית אינו הולם את רמת ההגנה הנדרשת,[269] אך כדי לאפשר זרימת מידע בין מדינות האיחוד לארצות הברית יש הסדר חלופי. הסדר ה־Safe Harbor היה וולונטרי, ולפיו התחייבו חברות פרטיות בארצות הברית לעקרונות שימוש במידע ההולמים את רמת ההגנה הנאותה באירופה, ואם הן חסו בו, העברת מידע אליהן הותרה לפי הדין האירופי. אלא שבעניין *Schrems*[270] – שהורתו במסמכים שפרסם סנודן כמתואר למעלה – קבע בית הדין האירופי לצדק (ECJ) כי הסדר זה אינו מחייב את הרשויות בארצות הברית, שלהן הסמכות לאסוף ולשמור את כל המידע הפרטי של מושאי מידע אירופיים, ולכן מושאים אלה אינם זוכים להגנה נאותה על המידע האישי שלהם. משכך, ביטל בית הדין את החלטת האיחוד המאשרת את הסדר ה־Safe Harbor. עד כניסתו של ההסדר החדש לתוקף – הסדר וולונטרי דומה, ה־Privacy Shield – נסמך הבסיס החוקי להעברת נתונים מהאיחוד לארצות הברית על החריגים שבסעיף 26 לדירקטיבת הגנת המידע, ובעיקר על הסכמתם של מושאי המידע.

לפי החלטה מיוני 2016 של קבוצת העבודה האירופית שלפי סעיף 29 לדירקטיבה,[271] הסדר ה־Privacy Shield עומד בדרישות של דיני הגנת המידע

269 ארצות הברית מעולם לא פנתה לנציבות האירופית בבקשה שיכירו בה כמספקת רמת הגנה נאותה, והאירופים לא קבעו זאת רשמית. עם זאת גם בטרם עניין *Schrems* (**לעיל** בפרק זה ה"ש 175) – המשליך על נאותות הגנת המידע בדין האמריקאי בשל חשיפותיו של אדוארד סנודן – היה הקונצנזוס האירופי כי הדין האמריקאי כשהוא לעצמו אינו מספק רמת הגנה נאותה על מידע. בחוות דעת משנת 1999 ציינה קבוצת העבודה האירופית לפי ס' 29 לדירקטיבה, כי "בשלב זה, אין להסתמך על מלאכת הטלאים הקיימת של דינים סקטוריאליים צרים ושל אסדרה־עצמית על בסיס וולנטרי כמספקות הגנה נאותה בכל המקרים למידע פרטי המועברים מהאיחוד האירופי". ראו Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government) (26.1.1999 בעמ' 2.

270 עניין *Schrems*, **לעיל** בפרק זה ה"ש 175.

271 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 (notified under document C (2016) 4176)

האירופיים כמו שפורשו בעניין *Schrems*. לשם כך הסתמכה קבוצת העבודה על מצגים של מנהל המודיעין הלאומי האמריקאי (ODNI) ועל ההוראה הנשיאותית מס' 28 (PPD28). הסדר זה ייסד במחלקת המדינה האמריקאית פונקציה של אומבודסמן עצמאי לבחינת תלונות של מושאי מידע אירופיים על שהממשל האמריקני ניגש למידע האישי שלהם לתכליות של ביטחון לאומי,[272] וכן הקים ועדה משותפת לבחינה שנתית של פעולת ההסדר גם בהיבטים של ביטחון לאומי.

3.2.3.4. רשות להגנת מידע (DPA – Data Protection Authority)

דירקטיבת הגנת המידע מחייבת את המדינות־החברות להקים רשות פיקוח עצמאית להגנה על מידע (Supervisory Authority או Data Protection Authority),[273] שתבקר את יישום הוראות הדירקטיבה במדינה החברה. הרשות גם תהיה גוף מייעץ בכל הנוגע לחקיקה או להסדר רגולטורי שנוגע להגנה על זכויות הפרט ועל חירויותיו מפני פעולות של עיבוד מידע. הרשות היא מען לתלונות של מושאי מידע בדבר הפרת זכויותיהם מכוח הדירקטיבה, והיא גם אחראית למרשם של פעולות עיבוד המידע. סעיף 18 לדירקטיבה מורה למנהלי מאגרים או למי מטעמם ליידע את רשות הפיקוח המדינתית על פעולות עיבוד מידע, אך המדינות־החברות רשאיות – מטעמים שונים – להחריג ביד רחבה פעולות עיבוד מחובת הדיווח.

3.2.3.5. הפטור מטעמי ביטחון לאומי והחלטת המסגרת 2008/977/JHA של הנציבות האירופית

ההוראות של דירקטיבת הגנת המידע שפורטו בחלקים 3.2.3.1–3.2.3.4 למעלה אינן חלות על כל סוגי איסוף המידע ועיבודו. סעיף 3(2) לדירקטיבה מחריג מגדר תחולתה פעולות עיבוד הנוגעות לביטחון הציבור, להגנה, לביטחון המדינה (לרבות לכלכלת המדינה כשפעולת עיבוד הנתונים קשורה לענייני ביטחון המדינה) ולפעולות המדינה בתחומי הדין הפלילי. התקנות הכלליות בדבר הגנת

272 ראו חלק 5.3.2 **להלן**.

273 ס' 28 לדירקטיבת הגנת המידע.

מידע (GDPR) כוללות החרגה דומה בסעיף 2(2)(d), בנוסח צר יותר – הן אינן חלות על פעולות עיבוד נתונים שרשויות מוסמכות מבצעות למטרות של מניעה או חקירה של עבירות פליליות, תביעה וענישה, לרבות הגנה על ביטחון הציבור.

נוסף על ההחרגה הכללית של פעולות עיבוד הנוגעות לביטחון ולאכיפת החוק, הדירקטיבה מאפשרת למדינות־החברות להחריג בחקיקה את זכות היידוע[274] ואת החובה לפומביות העיבוד[275] כשהדבר נדרש להגנה על הביטחון הלאומי, לביטחון הציבור, להגנה, לשם מניעת עבירות, לחקירתן ולמיצוי ההליכים הפליליים בעניינן, ולמען אינטרסים כלכליים חשובים של המדינה־החברה.[276] התקנות הכלליות בדבר הגנת מידע (GDPR) אמנם כוללות רשימה ארוכה יותר של זכויות של מושאי המידע שאותן ניתן להחריג[277] (הזכות להימחק, הזכות לניידות נתונים,[278] הזכות להתנגד לעיבוד מידע והזכות שלא להיות מושא של החלטות אוטומטיות);[279] אבל מנגד הן קובעות כי חקיקה המחריגה זכויות אלו תכיל הוראות מיוחדות בנוגע למטרות העיבוד, לקטגוריות המידע הפרטי המעובדות, להיקף ההחרגות שבחקיקה, לאמצעי אבטחת המידע, למיהות מנהל המאגר או לסוגו, לתקופת שימור הנתונים, לסיכונים, לזכויות ולחירויות של מושאי המידע ולזכותם של מושאי המידע ליידוע (אם זו אינה פוגעת במטרות העיבוד).[280]

274 ס' 10 ו־11(1) לדירקטיבת הגנת המידע.

275 ס' 21 לדירקטיבת הגנת המידע.

276 ס' 13 לדירקטיבת הגנת המידע.

277 ס' 23(1) לתקנות הכלליות בדבר הגנת מידע (GDPR).

278 ניידות במידע (data portability) – הזכות של מושא המידע לקבל את המידע הפרטי שהעביר למנהל המאגר (העברה מוסדרת ובפורמט נתונים נפוץ, שמיש ומקובל. ראו ס' 20 לתקנות הכלליות בדבר הגנת מידע (GDPR)).

279 סעיף 22 לתקנות הכלליות בדבר הגנת מידע (GDPR) קובע את זכותו של מושא המידע לא להיות מושאה של החלטה העלולה להשפיע עליו מבחינה משפטית או מבחינה חשובה אחרת, המבוססת על פעולות אוטומטיות בלבד, לרבות פעולות של פרופיילינג. ראו גם ס' 15 לדירקטיבת הגנת המידע.

280 ס' 23(2) לתקנות הכלליות בדבר הגנת מידע (GDPR).

החלטת המסגרת בענייני חוק ופנים של הנציבות האירופית 2008/977/JHA על הגנה של מידע פרטי המעובד במסגרת שיתוף פעולה משטרתי ושיפוטי, מסדירה את משטר הגנת המידע בעמוד השלישי (third pillar) של דיני האיחוד האירופי.[281] החלטת המסגרת נועדה להבטיח את ההגנה על זכויותיהם וחירויותיהם של פרטים, ובייחוד על זכותם לפרטיות, במקרים שבהם מידע פרטי הועבר בין שתי מדינות־חברות והונגש או שודר במערכות מידע בין־מדינתיות שהוקמו על בסיס אמנות של האיחוד האירופי[282] או של הקהילייה האירופית למטרות מניעה או חקירה של עבירות פליליות, תביעה וענישה.[283]

החלטת המסגרת (2008/977/JHA) מחריגה מתוכה אינטרסים של ביטחון לאומי ופעילויות מודיעין לצורכי ביטחון לאומי.[284] משטר הגנת המידע האירופי הקיים (עד כניסתן לתוקף של התקנות הכלליות בדבר הגנת מידע (GDPR) ודירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)) חסר אפוא חקיקה ספציפית שמסדירה את זכויותיהם של מושאי מידע בעניין פעולות עיבוד מידע הנוגעות לביטחון לאומי, המוגנות רק ברמה ה"חוקתית" של משפט האיחוד.[285] הלאקונה בדיני הגנת המידע האירופיים מורגשת יותר, בהתחשב בתחולתה המהותית של החלטת המסגרת, המוגבלת לנתונים שהועברו בין הרשויות

281 מערכת "עמודי היסוד" של האיחוד האירופי בוטלה באמנת ליסבון (2009). עמוד היסוד השלישי של האיחוד האירופי עסק בשיתוף פעולה בעניינים פליליים בין המשטרה למערכת המשפט. ראו גם Hijmans and Scirocco, **לעיל** בפרק זה בה"ש 226.

282 ההחלטה מתייחסת בפרט ל־Title VI של אמנת האיחוד האירופי (TEU) המסדיר את שיתוף הפעולה בעניינים פליליים ובענייני פנים (Justice and Home Affairs) בין המדינות. זהו הגלגול הקודם של "'העמוד השלישי" (ראו ה"ש 282 **לעיל** בפרק זה) של האיחוד האירופי בטרם תחולתו – ולפי כותרתו – שצומצמה לשיתוף פעולה בעניינים פליליים בין המשטרה למערכת המשפט".

283 ס' 1(1) להחלטת המסגרת. יצוין גם כי לפי סעיף 39 למבוא להחלטת המסגרת, מערכות מידע אירופיות נוספות מוחרגות מתחולתה, כמו למשל מערכות המידע של סוכנות המשפט האירופית (Eurojust), המשטרה האירופית (Europol) ומערכות המידע של המכס (CIS).

284 ס' 1(4) להחלטת המסגרת.

285 ראו חלק 3.2.2 **לעיל**.

המוסמכות של מדינות האיחוד, וחסרה גם הסדרה של דיני הגנת מידע בכל נוגע לפעולות עיבוד פנימיות של רשויות אכיפת החוק.

לפי החלטת המסגרת (2008/977/JHA), פעולות עיבוד מותרות ברשויות המוסמכות בלבד,[286] ורק למטרות מפורשות, מסוימות וחוקיות שבגדרי תפקידיהן. פעולות עיבוד נתונים מותרות רק לצורך המטרות שלשמן נאספו, כשהן מדויקות, הולמות, רלוונטיות ואינן יותר מן הנדרש לאור מטרות אלו.[287] עיבוד נוסף, למטרות שונות מהן, יתאפשר אם המטרות החדשות אינן בלתי־תואמות את מטרות האיסוף המקוריות, ופעולת העיבוד חיונית ומתבצעת במידתיות ולפי הסמכה בחוק.[288] נוסף על האמור לעיל, אם מקורו של המידע הפרטי במדינה אחרת, עיבוד נוסף שלו במדינה המקבלת אפשרי רק למטרות של מניעה, אכיפה, גילוי וענישה של פשעים, הליכים משפטיים ומינהליים בקשר אליהם, מניעת איום מיידי ורציני לביטחון הציבור או למטרות אחרות שלהן הסכימו מדינת המקור או מושא המידע, ובכפוף לדין הלאומי.[289]

עיבוד של נתונים רגישים ייעשה אך ורק בהתקיים צורך מוחלט לכך, ובתנאי שקיימת דרישה ראויה למידתיות בחוק המדינה.[290] החלטות אוטומטיות המתקבלות על בסיס עיבוד נתונים אישיים של מושא המידע, ושהשפעתן עליו ניכרת או שהן מרעות את מצבו המשפטי, מותרות רק כשהן נקבעות מכוח חוק שקיימים בו אמצעים לשמירת האינטרסים של מושא המידע.[291]

סעיף 9 להחלטת המסגרת מאפשר למדינה המעבירה מידע פרטי למדינה אחרת לציין את תקופת הזמן המרבית לשמירת המידע במדינת היעד, שאם לא

286 "רשויות מוסמכות", לפי ס'2(h) להחלטת המסגרת, הן סוכנויות וגופים שהוקמו לפי חקיקה מכוח Title VI של אמנת האיחוד, וכן גופי משטרה, מכס וסוכנויות אחרות שהוסמכו בחקיקה מדינתית לבצע פעולות של עיבוד נתונים המצויות בגדרי החלטת המסגרת.

287 ס' 3(1) להחלטת המסגרת.

288 ס' 3(2) להחלטת המסגרת.

289 ס' 11 להחלטת המסגרת.

290 ס' 6 להחלטת המסגרת. השוו לסעיף 8 של דירקטיבת הגנת המידע.

291 ס' 7 להחלטת המסגרת. השוו לסעיף 15 של דירקטיבת הגנת המידע.

כן יחול על המידע הדין המקומי של מדינת היעד. כשהנתונים נדרשים לצורכי חקירה מתמשכת, תביעה פלילית או ענישה, שמירתם מותרת אף אם התקופה המותרת פקעה. החלטת המסגרת כוללת הנחיות באשר להעברת הנתונים לרשויות מוסמכות במדינות שאינן חברות באיחוד, לגופים בין־לאומיים[292] ולארגונים פרטיים.[293]

לפי החלטת המסגרת זכויותיהם של מושאי המידע הן הזכות ליידוע[294] (בכפוף לחוק המדינה), זכות הגישה לנתונים (לכל הפחות הזכות של מושא המידע לקבל אישור מהרשות המפקחת או ממנהל המאגר אם מידע פרטי שלו הועבר או הונגש),[295] והזכות למחיקה, לתיקון או לחסימת גישה.[296] החלטת המסגרת משאירה מרווח להגבלות על זכויות אלו אם הן נדרשות ומידתיות כדי למנוע הפרעות לנהלים, לבירורים ולחקירות רשמיות או משפטיות, למנוע הפרעות למניעה, לאכיפה, לגילוי ולענישה של פשעים, להגנה על ביטחון הציבור והביטחון הלאומי או להגן על זכויותיו ועל חירויותיו של מושא המידע או של אחרים.[297]

3.2.4. דירקטיבת הפרטיות האלקטרונית (e-Privacy Directive) ודירקטיבת שימור הנתונים (Data Retention Directive)

נדבך נוסף של המשטר האירופי להגנת המידע הוא דירקטיבת הפרטיות האלקטרונית, הכוללת הוראות ספציפיות לתקשורת אלקטרונית. בדומה לדירקטיבת הגנת המידע, גם דירקטיבת הפרטיות האלקטרונית מחריגה מתחולתה פעילויות שנוגעות לביטחון הציבור, להגנה, לביטחון המדינה (לרבות לכלכלת המדינה, כשעיבוד הנתונים נעשה למען עניינים של ביטחון המדינה)

292 ס' 14 להחלטת המסגרת.

293 ס' 13 להחלטת המסגרת.

294 ס' 16 להחלטת המסגרת.

295 ס' 17 להחלטת המסגרת.

296 ס' 18 להחלטת המסגרת.

297 ס' 17(2) להחלטת המסגרת.

ולפעולות המדינה בתחומי הדין הפלילי.[298] נוסף על כך, המדינות החברות רשאיות להחריג אחדות מהוראותיה של דירקטיבת הפרטיות האלקטרונית למטרות אלו, ובעיקר להורות בחוק על שימור נתונים לפרקי זמן מוגבלים, אם הדבר מוצדק.[299]

בשנת 2006 אומצה דירקטיבת שימור הנתונים (Data Retention Directive),[300] שכללה תיקונים לדירקטיבת הפרטיות האלקטרונית. הדירקטיבה הורתה למדינות־החברות לאמץ אמצעים המחייבים ספקי תקשורת אלקטרונית לשמור נתוני תעבורה[301] ומיקום[302] לתקופות שלא יפחתו משישה חודשים ועד שנתיים[303] למטרות של אכיפת חוק. לשון דירקטיבת שימור הנתונים מציינת במפורש כי אין היא חלה על נתוני תוכן.[304]

על פי הוראותיה של דירקטיבת שימור הנתונים, רק הרשויות המוסמכות (competent national authorities) יורשו לגשת לנתונים שמורים, ורק

298 ס' 1(3) לדירקטיבת הפרטיות האלקטרונית (ראו **לעיל** בפרק זה ה"ש 211), השוו לסעיף 3(2) לדירקטיבת הגנת המידע.

299 ס' 15(1) לדירקטיבת הפרטיות האלקטרונית.

300 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (להלן: דירקטיבת שימור הנתונים).

301 "נתוני תעבורה" מוגדרים בסעיף 2(b) לדירקטיבת הפרטיות האלקטרונית: נתונים המועבדים לצורכי תקשורת אלקטרונית או לשם חיוב המשתמשים (ומשכך נופלים בגדר נתוני מנוי/זיהוי, כמובנם בחוק נתוני תקשורת). השוו להגדרה של נתוני תעבורה בחוק נתוני תקשורת, **לעיל** בפרק 2 ה"ש 10. סעיפים 5(1)(a)–(e) לדירקטיבת שימור הנתונים מונים את סוגי נתוני התעבורה ששימורם נדרש.

302 "נתוני מיקום" (location data) מוגדרים בסעיף 2(c) לדירקטיבת הפרטיות האלקטרונית כנתונים המעובדים ברשת תקשורת אלקטרונית שיש בהם כדי ללמד על מיקום מכשור הקצה של המשתמש. סעיף 5(1)(f) לדירקטיבת שימור הנתונים מונה את סוגי נתוני המיקום ששימורם נדרש.

303 ס' 6 לדירקטיבת שימור הנתונים.

304 ס' 1(2) ו־5(2) לדירקטיבת שימור הנתונים.

במקרים ספציפיים ולפי דין, בהתאם לנהלים שתקבע כל מדינה־חברה בכפוף להוראותיו של הדין האירופי, ובעיקר הוראותיה של האמנה האירופית לזכויות אדם (ECHR) כמו שמפרש אותן בית הדין האירופי לזכויות אדם (ECtHR).[305] נתונים אלו יאוחסנו ויאובטחו[306] באופן המאפשר את העברתם ללא דיחוי לבקשת הרשויות המוסמכות.[307] המדינות־החברות ידווחו מדי שנה לנציבות האירופית על היקף השימוש בנתוני התקשורת השמורים.

בעניין *Digital Rights Ireland*[308] דן בית הדין האירופי לצדק (ECJ) בשאילתות שהפנו אליו בית הדין העליון של אירלנד ובית המשפט החוקתי האוסטרי בדבר תוקפה של דירקטיבת שימור הנתונים, לאחר שהאמצעים ליישום הוראות הדירקטיבה שנקטו אירלנד ואוסטריה נתקפו בערכאות הלאומיות. בית הדין האירופי לא התרשם מהגבלת תחולת הדירקטיבה לנתוני תקשורת בלבד,[309] וציין כי נתונים אלו יכולים לאפשר הסקת מסקנות מדויקות בנוגע לחיים הפרטיים של מושאי המידע, וכי שימור נתוני התקשורת לבדם עלול להשפיע לרעה על השימושים של המנויים על שירותי התקשורת בשירותים אלו, ומכאן גם על חופש הביטוי שלהם המעוגן בסעיף 11 למגילת זכויות היסוד של האיחוד האירופי (CFR).[310]

בהתייחסו להלימה של דירקטיבת נתוני התקשורת עם סעיפים 7 ו־8 למגילת זכויות היסוד (CFR), קבע בית הדין (ECJ) כי החובה שהוטלה על ספקים לשמור נתוני תקשורת פוגעת בזכויות לפרטיות מכוח סעיף 7 למגילה, והפגיעה גדלה

305 ס' 4 לדירקטיבת שימור הנתונים.

306 ס' 7 לדירקטיבת שימור הנתונים. ס' 9 מורה למדינות החברות להסמיך רשות עצמאית (לרבות רשות הגנת המידע שהוקמה מכוח סעיף 28 לדירקטיבת הגנת המידע, ראו בחלק 3.2.3.4 **לעיל**) לפקח על הלימה עם רמת האבטחה הנדרשת.

307 ס' 8 לדירקטיבת שימור הנתונים.

308 עניין *DRI*, **לעיל** בפרק זה ה"ש 228. לרקע ותיאור נוסף של הפרשה, ראו Lucia Zedner, *Why Blanket Surveillance is No Security Blanket*, *in* Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair 564 (Russell A. Miller, ed., 2017)

309 לרלוונטיות של הבחנה זו, ראו טנא, **להלן** בפרק 4 ה"ש 123.

310 עניין *DRI*, **לעיל** בפרק זה ה"ש 228, בפסקאות 26–28.

בשל האפשרות הניתנת לרשויות המוסמכות לגשת לנתונים הללו.[311] בית הדין קבע כי מנגד מטרותיה של הדירקטיבה – אכיפת חוק והגנה מפני טרור – הן תכליות מוצדקות באופן כללי,[312] ועל כן הוא נדרש לבחון את מידתיותה של הדירקטיבה. לנוכח חשיבותה של הגנת המידע בראי הזכויות הבסיסיות המוגנות בסעיפים 7 ו־8 למגילה, מצא בית הדין לנכון לערוך בחינה מחמירה (strict review) של מידתיות הפגיעה בזכות.[313]

בית הדין ציין כי הוראותיה של דירקטיבת שימור הנתונים מתערבות בזכויותיהם של כל אזרחי האיחוד ללא הבחנה, הגבלה או החרגה שמתחשבות בתכליות הדירקטיבה.[314] הדירקטיבה גם אינה מגבילה את הרשויות המוסמכות בכל הנוגע לגישה למידע ולשימוש שנעשה בו, ואינה קובעת קריטריונים להרשאות גישה.[315] פרק הזמן המינימלי לשימור אינו מבחין בין סוגי נתונים, והדירקטיבה חסרה קריטריון שמגביל את תקופת השימור למינימום ההכרחי.[316] מהמקובץ נקבע כי הדירקטיבה פוגעת באופן לא מידתי בזכויות מכוח סעיפים 7 ו־8 למגילה, ולכן היא בטלה.[317]

לאחר ביטולה של דירקטיבת שימור הנתונים בשנת 2014 בפסק הדין בעניין *Digital Rights Ireland*, בשלהי 2016 שב בית הדין האירופי להתייחס לנושא של שימור נתונים במסגרת עניין *Tele2 Sverige AB*,[318] שבו נבחנו ההוראות בדירקטיבת הפרטיות האלקטרונית המתירות שימור נתונים לצורכי ביטחון ואכיפת חוק.[319]

311 **שם**, פסקאות 34–35.

312 **שם**, פס' 44.

313 **שם**, פס' 48.

314 **שם**, פס' 57–58.

315 **שם**, פס' 60–62.

316 **שם**, פס' 63–64.

317 **שם**, פס' 69, 73.

318 ראו Tele2 Sverige AB, **לעיל** בפרק זה ה"ש 228.

319 ראו בטקסט המפנה לה"ש 299 **לעיל** בפרק זה.

בית הדין הדגיש שם כי שימור גורף וחסר הבחנה של נתוני תקשורת מכלל המשתמשים, גם בחקיקה מדינתית, פוגע בזכות לפרטיות יותר מן הצורך ואינו מידתי. עם זאת לא שלל בית הדין את האפשרות שהשימור של נתוני תקשורת יוסדר בחקיקה מדינתית.[320] הסדרה כזאת תתאפשר אם השימור מוגבל (לקטגוריות הנתונים הנשמרות, לאמצעי התקשורת שמהם נאספים הנתונים, להיקף מושאי המידע שבעניינם נשמרים הנתונים ולתקופת השימור).[321] חקיקה כזאת צריכה להגדיר מהם התנאים המהותיים והפרוצדורליים שבהם ייתנו ספקי שירותי התקשורת גישה לנתונים לרשויות המוסמכות, ובתנאי שהנתונים קשורים למי שמבצע "פשעים חמורים" (לרבות מעשי טרור), ואכן יש ראיות לתרומתם של הנתונים להגשמת המטרות. פרט למקרים דחופים, נדרשת ביקורת שיפוטית (או של רשות עצמאית) על הבקשות לנתונים אלו.[322]

3.2.5. עם הפנים לעתיד – משטר הגנת המידע החדש: התקנות הכלליות בדבר הגנת מידע (GDPR) ודירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)

במאי 2016, מכוח סמכותו לפי סעיף 16(2) לאמנה בדבר תפקודו של האיחוד האירופי (TEFU), חוקק הפרלמנט האירופי את התקנות הכלליות בדבר הגנת מידע (GDPR) ואת דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). שני דברי חקיקה אלו נועדו לעדכן את משטר הגנת המידע האירופי ולהתאימו לשינויים הטכנולוגיים של שני העשורים האחרונים ולהתפתחויות בתפיסת מרכיביה של הגנת המידע ושל זכויותיהם של מושאי מידע. התקנות והדירקטיבה השאירו למדינות החברות שנתיים ליישום הוראותיהן, ותוקפן מחייב מחודש מאי 2018.

320 לדעת ארגון Privacy International, סמכויות כאלה יש לעגן בחקיקה ראשית ולא להסתפק בנהלים ארגוניים פנימיים. ראו פס' 117 בעניין *Tele2 Sverige AB*, **לעיל** בפרק זה בה"ש 228; Privacy International, *Submission to the Home Office Investigatory Powers Act 2016 Consultation on the Draft Codes of Practice* (7.4.2017)

321 **שם**, פס' 108–109.

322 **שם**, פס' 120.

3.2.5.1. התקנות הכלליות בדבר הגנת מידע (GDPR)

בשונה מהדירקטיבות, לתקנות הכלליות של הגנת המידע השפעה ישירה,[323] והן אינן מצריכות תהליך מורכב של חקיקה פנימית שמיישמת אותן בכל אחת ממדינות האיחוד. יישומה של דירקטיבת הגנת המידע במדינות החברות הביא לידי שונות בדיני הגנת המידע הפנימיים,[324] והבחירה בכלי של תקנות לצורך עדכון דינים אלו נועדה לסייע להרמוניזציה בין המדינות החברות. עם זה יש המטילים ספק ביכולתן של התקנות להגשים מטרה זו.[325]

בשונה מ"המשטר הישן" של דירקטיבת הגנת המידע,[326] התחולה הטריטוריאלית של התקנות הכלליות בדבר הגנת מידע (GDPR) רחבה יותר, והיא חלה על עיבוד מידע בפעילות של כל מוסד, מנהל מאגר או מעבד באיחוד האירופי.[327] עקרונות עיבוד המידע של התקנות דומים לאלו שבדירקטיבה,[328] למעט כמה שינויי נוסח: התקנות דורשות במפורש שעיבוד מידע יתבצע בשקיפות, ואילו מנוסח הדירקטיבה דרישה זו רק משתמעת;[329] התקנות הוסיפו רכיב של זמן לעקרון דיוק המידע המצוי בדירקטיבה, ולפיו תיקונים של מידע שגוי או לא

323 ראו חלק 3.2.1 **לעיל**.

324 כך למשל כבר בשנת 2003 העירה הנציבות כי יישום הדירקטיבה "מטולא למדי". European Commission, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*' COM (2003) 265 final, 12. ראו לדוגמה גם את הדיון אצל David Erdos, *European Union Data Protection Law and Media Expression: Fundamentally Off Balance*, 65 Inte'l & Comp. L. Q.139–183 (2016)

325 Peter Blume & Christian Wiese Svanberg, *The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus*, 15 Cambridge Yearbook of European Legal Studies 27–46 (2013)

326 ראו חלק 3.2.3 **לעיל**.

327 ס' 3(1) לתקנות הכלליות בדבר הגנת מידע (GDPR). השוו לסעיף 3 לדירקטיבת הגנת המידע.

328 ראו חלק 3.2.3.1 **לעיל**.

329 ס' 5(1)(a) לתקנות הכלליות בדבר הגנת מידע (GDPR). השוו לסעיף 6(1)(a) לדירקטיבת הגנת המידע.

מדויק יתבצעו ללא דיחוי;[330] עקרון האחריותיות (accountability) דורש ממנהל המאגר יכולת להראות ציות והלימה עם שאר עקרונות עיבוד המידע;[331] התנאים להסכמתו של מושא המידע לעיבוד של מידע פרטי שלו פורטו בהרחבה בתקנות החדשות, והן כוללות הוראות נפרדות להסכמתם של קטינים.[332]

לפי התקנות החדשות מושאי המידע נהנים מאותן זכויות שהוקנו להם בדירקטיבה[333] וכן מהזכויות לשקיפות ומגישה למידע ולדיוק שאוזכרו לעיל. זכות חדשה שהוכרה בתקנות היא הזכות להישכח,[334] בכפוף להיעדרן של סיבות לגיטימיות אחרות המצדיקות את פעולת העיבוד ובשים לב לזכויות המתחרות – חופש הביטוי וחופש המידע[335] – ולטעמים מתחרים אחרים שבאינטרס הציבורי.[336] כחלופה למחיקת מידע פרטי במקרים שבהם אין הדבר מתאפשר, יצרו התקנות את הזכות להגבלת הגישה לנתונים אלו.[337] עוד זכות חדשה שנוספה בתקנות היא הזכות לניידות במידע[338] (data portability) – זכותו של מושא המידע לקבל את המידע הפרטי שהעביר למנהל המאגר בצורה מוסדרת ובפורמט נתונים נפוץ, שמיש ומקובל.

התקנות מדגישות את אחריותם של מנהלי המאגרים ושל המעבדים. אמנם אין בתקנות מקבילה לחובה החלה עליהם ליידע את רשות הגנת המידע הלאומית לפני הפעולה של העיבוד נתונים[339] – אך בתקנות קמו חובות חדשות לרישום

330 ס' 5(1)(d) לתקנות הכלליות בדבר הגנת מידע (GDPR). השוו לסעיף 6(1)(d) לדירקטיבת הגנת המידע.

331 ס' 5(2) לתקנות הכלליות בדבר הגנת מידע (GDPR).

332 ס' 7–9 לתקנות הכלליות בדבר הגנת מידע (GDPR).

333 ראו חלק 3.2.3.2 **לעיל**.

334 ס' 17 לתקנות הכלליות בדבר הגנת מידע (GDPR).

335 ס' 17(3)(a) לתקנות הכלליות בדבר הגנת מידע (GDPR).

336 ס' 17(3)(d)–(b) לתקנות הכלליות בדבר הגנת מידע (GDPR).

337 ס' 18 לתקנות הכלליות בדבר הגנת מידע (GDPR).

338 ס' 20 לתקנות הכלליות בדבר הגנת מידע (GDPR).

339 ס' 18 של דירקטיבת הגנת המידע.

פנימי של פעולות עיבוד. הוראות חדשות מורות למנהלי מאגרים להטמיע אמצעים ארגוניים וטכנולוגיים המבטיחים הגנת מידע מראש (data protection by design), לאור עקרונות של מזעור נתונים (data minimization).[340]

3.2.5.2. דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)

בחודש מאי 2016, מכוח סמכותו לפי סעיף 16(2) לאמנה בדבר תפקודו של האיחוד האירופי (TEFU), חוקק הפרלמנט האירופי את דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), שנועדה להגן על יחידים בכל הקשור לעיבוד מידע אישי ברשויות מוסמכות למטרות של מניעה, חקירה וגילוי של עבירות פליליות. הדירקטיבה החליפה את החלטת המסגרת 2008/977/JHA של הנציבות למן חודש מאי 2018, והיא מוסיפה עליה הרבה.

דירקטיבת הגנת המידע (דירקטיבה 95/46/EC) והתקנות הכלליות בדבר הגנת מידע (GDPR), שהחליפו אותה במאי 2018, מחריגות מתחולתן פעולות של עיבוד נתונים למטרות של מניעה, חקירה וגילוי של עבירות פליליות, לרבות הגנה על ביטחון הציבור.[341] תחולתה של החלטת המסגרת (2008/977/JHA)[342] הוגבלה, כאמור לעיל, לפעולות עיבוד שעיקרן העברת מידע בין רשויות מוסמכות לחקירה ולאכיפת החוק של מדינות האיחוד.[343]

340 ראו חלק 3.2.5.2.2 **להלן**.

341 ראו ס' 2(2)(d) לתקנות הכלליות בדבר הגנת מידע (GDPR). יוער כי הסייגים של דירקטיבת הגנת המידע (ס' 3(2)) רחבים יותר ומחריגים מתחולתה כל פעילות הנוגעת לביטחון לאומי ולדין הפלילי.

342 ראו בחלק 3.2.3.5 **לעיל**.

343 נראה כי על רקע העלייה במספר אירועי הטרור האסלאמי באירופה בשנים 2011–2016, פני האיחוד הם לביצוע רפורמה נוספת, הנוגעת לגישה של רשויות החוק למאגרי מידע במדינות־חברות אחרות. ביוני 2017 ציינה מפקחת הצדק האירופית, ורה יורובה, בריאיון לרויטרס כי תציג לשרי האיחוד אחת משלוש חלופות: מתן אפשרות לרשות אכיפת חוק לפנות לחברה פרטית המחזיקה במאגר מידע במדינה־חברה אחרת בבקשת מידע ללא צורך באישור המדינה־החברה האחרת; חיוב חברות פרטיות לספק נתונים שרשויות אכיפת חוק של מדינות־חברות אחרות מבקשות; או שימור הנתונים מראש בסוכנויות האכיפה — אמצעי פולשני יותר שיופעל במקרי חירום קיצוניים ובכפוף

בדומה למינוח בדירקטיבת הגנת המידע, גם בדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) ההגדרה של "מידע פרטי" היא "כל מידע הנוגע לאדם מזוהה או ניתן לזיהוי" ("מושא מידע" או data subject); אלא שהגדרת מושא המידע הורחבה, ובגדרה נופלים גם מי שניתנים לזיהוי באמצעות נתוני מיקום ומזהים מקוונים (online identifiers).[344] נוסח דומה של הגדרות אלו מצוי גם בתקנות הכלליות בדבר הגנת מידע (GDPR). "עיבוד נתונים", לפי הגדרתה של דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), הוא כל פעולה או סדרת פעולות, אם אוטומטיות ואם לא אוטומטיות, הנעשות במידע פרטי או באוסף נתונים פרטיים כאמור, לרבות איסוף, אחסון, מיון, שינוי והעברה של הנתונים לצד שלישי.[345]

סעיף 6 לדירקטיבה 2016/680 מורה למדינות החברות להבחין בין סוגים שונים של מושאי מידע – חשודים, עבריינים מורשעים, קורבנות עבירה וצדדים שלישיים (עדים, אנשים הקשורים לעבריינים או לחשודים, מודיעים וכו'). סעיף 7 מורה על הבחנה בין סוגי מידע: מידע שמבוסס על עובדות לעומת מידע שמבוסס על הערכה או אומדן אנושיים.

הדירקטיבה חלה על "רשויות מוסמכות" (competent authorities), שהן כל גוף מוסמך, לרבות באמצעות חוק פנימי של אחת ממדינות האיחוד, לפעול למטרות מניעה, גילוי וחקירה של עבירות פליליות או להוציא לפועל ענישה פלילית, ובכלל זה מטרות של סיכול איומים על ביטחון הציבור.[346] הרשות המוסמכת היא מנהלת מאגר אם היא קובעת את התכליות והאמצעים לעיבוד נתונים,[347] ואילו המעבד, בדומה להגדרות כאלה בדירקטיבת הגנת המידע ובתקנות הכלליות בדבר הגנת מידע (GDPR), הוא הגוף המבצע את פעולת העיבוד מטעם מנהל

לבקורות נוספות ראו Julia Fioretti, *EU Seeks to Expedite Police Requests for Data from Tech Firms*, Reuters (8.06.2017)

344 ס' 3(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

345 ס' 3(2) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

346 ס' 3(7) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). השוו לנוסח הצר של סעיף 2(h) להחלטת המסגרת, **לעיל** בפרק זה ה"ש 286, אשר מדגיש את העמוד השלישי של אמנת האיחוד האירופי.

347 ס' 3(8) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

המאגר.[348] על מנהלי מאגרים למנות קצין הגנת מידע (data protection officer) שמטרתו לפקח על הגנת המידע אצל מנהל המאגר,[349] לייעץ במסגרת של הערכת הסיכונים הסטטוטורית[350] ולשמש איש קשר עם רשות הגנת המידע העצמאית במדינה.[351]

3.2.5.2.1. עקרונות עיבוד המידע וזכויות מושאי מידע

העקרונות של עיבוד מידע המפורטים בדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)[352] דומים לאלה שבדירקטיבת הגנת המידע[353] ובתקנות הכלליות בדבר הגנת מידע (GDPR),[354] אך כפי שנראה להלן, הם אינם זהים לחלוטין: עיבוד המידע יבוצע לפי חוק ובהגינות;[355] למטרות מוגדרות, מפורשות ולגיטימיות, בלי לחרוג מהן; המידע יהיה רלוונטי ולא יחרוג בהיקפו ביחס למטרות שלשמן הוא מעובד;[356] המידע יהיה מעודכן ומדויק, ויש לנקוט כל צעד סביר כדי למחוק נתונים שאינם מדויקים או לתקנם (בהתייחס למטרות העיבוד); המידע לא יוחזק באופן שיאפשר את זיהוי מושאי המידע לתקופה העולה על הנדרש; ויש לשמור על שלמות המידע ולדאוג לאבטחתו מפני איומים פנימיים וחיצוניים.

מידע שנאסף למטרות המנויות בדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) לא יעובד למטרות אחרות אלא לפי דין (ובמקרים אלו יחולו ההוראות

348 ס' 3(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

349 ס' 42–44 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

350 ס' 27 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

351 ראו חלק 3.2.5.2.3 **להלן**.

352 ס' 4 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

353 ס' 6(1) לדירקטיבת הגנת המידע.

354 ס' 5(1) לתקנות הכלליות בדבר הגנת מידע (GDPR).

355 מנוסח דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) הושמט עקרון השקיפות המצוי בתקנות הכלליות בדבר הגנת מידע (GPDR).

356 דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) נוקטת לשון חריפה פחות מנוסח התקנות הכלליות בדבר הגנת מידע (GDPR), שלפיו היקף המידע יוגבל כנדרש למטרות שלשמן הוא מעובד.

של התקנות הכלליות בדבר הגנת מידע (GDPR).[357] לפי דירקטיבה 2016/680, עיבוד סוגים מיוחדים של מידע אישי שיש בהם רגישות יתרה[358] יותר רק כשהוא נחוץ וכן כשהוא לפי חוק,[359] נועד להגנה על האינטרסים החיוניים של אותו מושא מידע או של מושא מידע אחר[360] או מתייחס לנתונים שמושא המידע פרסם ברבים.[361]

זכויותיהם של מושאי המידע מפורטות בפרק השלישי של הדירקטיבה. למושא המידע עומדות הזכויות לקבל מידע על עיבוד המידע,[362] לגשת למידע האישי שלו,[363] לתקן מידע שגוי או לא מדויק עליו והזכות להישכח.[364] זכויות אלו כפופות לסייגים המתחייבים מאופי המטרות שלשמן נאסף ומעובד המידע האישי.[365]

357 ס' 9 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). סעיף שסתום זה נועד להסדיר בין השאר מעבר נתונים בין גופי אכיפת החוק למגזר הפרטי. ראו למשל ניתוחה של Nadezhda Purtova, *Between GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships* (March 1, 2017)

358 נתונים שיש בהם כדי לגלות מוצא אתני, השקפות דתיות, פילוסופיות או פוליטיות, חברות בארגונים עובדים, מידע מזהה גנטי או ביומטרי, מידע רפואי, נטייה מינית או לחשוף פרטים על חיי האישיות של פלוני.

359 ס' 10(a) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). השוו לס' 8 לדירקטיבת הגנת המידע, ולס' 9 לתקנות הכלליות בדבר הגנת מידע (GDPR), שאינן מאפשרות למדינות החברות להתיר התרה גורפת עיבוד של קטגוריות רגישות של מידע אישי.

360 ס' 10(b) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). ראו והשוו הסעיפים המקבילים בדירקטיבת הגנת המידע (ס' 8(2)(c)) ובתקנות הכלליות בדבר הגנת מידע (GDPR) (ס' 9(2)(c)), שלפיהם עיבוד מידע פרטי "מיוחד" רב יותר לשם הגנת אינטרסים חיוניים של מושא המידע או של אחר, רק בכפוף למניעות משפטית או פיזית של מושא המידע להביע את הסכמתו לכך.

361 ס' 10(c) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

362 ס' 13 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

363 ס' 14 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

364 ס' 16 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). במקום מחיקה יגביל מנהל המאגר גישה לנתונים שמושא המידע ביקש את מחיקתם כאשר מושא המידע טוען לאי־דיוק, לא ניתן לקבוע את מידת דיוקם, או כאשר הם נדרשים כראיות.

365 ס' 15 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), ראו והשוו לס' 13 לתקנות הכלליות בדבר הגנת מידע (GDPR).

במסגרת זכויותיו של מושא המידע לקבל מידע, הוא רשאי לברר אצל מנהל המאגר אם מתבצעות פעולות לעיבוד מידע אישי שלו, ועל מנהל המאגר ליידע אותו בנוגע למטרות של עיבוד המידע, לזכותו להתלונן לפני הרשות המפקחת ולהודיע לו על זכותו לבקש גישה, תיקון, מחיקה או הגבלת עיבוד של המידע האישי הנוגע לו.[366] במקרים מסוימים, נוסף על האמור לעיל, על מנהל המאגר ליידע את מושא המידע בנוגע לבסיס המשפטי שלפיו מתבצע עיבוד הנתונים למשך תקופת שימור המידע האישי (או למצער, הקריטריון שלפיו נקבע משכהּ של תקופה זו) ולסוגי הגורמים החשופים למידע האישי, לרבות מדינות זרות או ארגונים בין־לאומיים.[367] ואולם, מדינות־חברות רשאיות לקבוע בחוק נסיבות שבהן מידע כאמור לא יועמד לרשות מושאי המידע כשהדבר משרת תכליות מסוימות: הגנה על הביטחון הלאומי, על ביטחון הציבור או על זכויות וחירויות של אחרים; או מניעת הפרעות לחקירה משפטית או רשמית או למטרות של אכיפה, חקירה ומניעה של עבירות וענישה פלילית.[368]

בדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) הנוסח של הזכות להישכח מפורט יותר מהנוסח בדירקטיבת הגנת המידע,[369] אבל יש הבדלים ניכרים גם בינו ובין נוסח הזכות בתקנות הכלליות בדבר הגנת מידע (GDPR).[370] לצד הזכות להישכח, סעיף 16 של דירקטיבת רשויות אכיפת החוק כולל את הזכות לתקן את המידע או להגביל את הגישה אליו, והוא מונה נסיבות שבהן הגבלת הגישה למידע תהיה חלופה למחיקתו:[371] כשאי־אפשר לברר את טענת מושא המידע לאי־דיוק בנתונים, או כשיש לשמור את המידע לצורכי ראיות. מדינות רשאיות לסייג את החובה ליידע את מושא המידע כי בקשתו

366 ס' 13(1), 14 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

367 ס' 13(2), 14 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

368 ס' 13(3), 15 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

369 ס' 12(b) לדירקטיבת הגנת המידע.

370 ס' 17 לתקנות הכלליות בדבר הגנת מידע (GDPR). ניסוחו של הסעיף בתקנות מפורש במידה ניכרת ממקבילו בדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), ואף ניתנה לו בסוגריים הכותרת המבארת, "הזכות להישכח".

371 ס' 16(3) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

נדחתה[372] במקרים שבהם הגבלה כאמור של הזכות להישכח או לדיוק במידע הוא אמצעי הכרחי ומידתי בחברה דמוקרטית להגשמת התכליות שצוינו לעיל. הדירקטיבה מורה למדינות החברות להגביל את תקופת שימור הנתונים בסבירות ולהקים נהלים לבחינה מעת לעת של הצורך בשימור שלהם ובקרה על מחיקתם.[373] הוראות דומות מצויות בתקנות הכלליות בדבר הגנת מידע (GDPR).[374]

התייחסות לעיבוד אוטומטי ולכריית מידע אפשר למצוא בסעיף 11 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), האוסר על מדינות־חברות להגיע להחלטות שמבוססות על תהליכים אוטומטיים בלבד, אלא אם הדבר מותר לפי חוק ויש אפשרות להתערבות אנושית בהחלטה. בהיעדר בקרות מיוחדות אין להשתמש בסוגים רגישים של מידע אישי,[375] ופרופיילינג[376] שתוצאותיו מובילות לאפליה על רקע אותם סוגים של מידע רגיש – אסור.[377]

הגנה מראש על מידע (data protection by design)

דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) כוללת הוראות בדבר הגנה מראש על מידע (data protection by design), שמיועדות להביא לידי תכנון מערכות מידע ונהלים ארגוניים שיהיה בהם כדי להטמיע את העקרונות האירופיים בדבר הגנה על המידע. סעיף 20 לדירקטיבה מורה למדינות־החברות לאפשר למנהלי מאגרי המידע להטמיע במערכות המידע אמצעים

372 ס' 16(4) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

373 ס' 5 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

374 ס' 5(1)(e) לתקנות הכלליות בדבר הגנת מידע (GDPR).

375 ראו **לעיל** בפרק זה ה"ש 358.

376 "פרופיילינג" מוגדר בסעיף 3(4) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) כעיבוד נתונים אוטומטי שמשתמש במידע פרטי כדי להעריך היבטים פרטיים שקשורים לאדם מסוים, במיוחד לצורך חיזוי תפקודו בעבודה, מצבו הכלכלי, בריאותו, העדפותיו האישיות, התנהגותו, אמינותו ומיקומו.

377 הד מטרים לגישה זו ניתן למצוא בחוות דעתו של היועץ המשפטי לפרלמנט האירופי בעניין ההסכם על העברת נתוני נוסעים (PNR – Passenger Name Record) בין האיחוד לקנדה. בפסקה 258 לחוות דעתו העיר היועץ כי אין לבסס את נתוני הנוסעים או את קריטריוני הערכת הסיכון שלהם על מוצא אתני, גזע, השקפות פוליטיות או פילוסופיות, מצב הבריאות או נטייה מינית. לדעת היועץ המשפטי (**שם**, בפסקה 259), נדרשת בקרה לא אוטומטית על תוצרי ההשוואה בין בסיס נתוני ה־PNR לקריטריוני הערכת הסיכון (המניבים רשימת חשודים), ראו AG Mengozzi, Opinion 1/15 (8 September 2016)

טכניים וארגוניים שנועדו ליישם ביעילות את העקרונות של הגנת המידע. בין יתר האמצעים מוזכרים מזעור נתונים (data minimization) ומעין־התממה (pseudonymisation).

מעין־התממה מוגדרת בדירקטיבה כעיבוד נתונים באופן המונע ייחוס של מידע אישי למושא מידע מסוים ללא מידע נוסף, בכפוף לכך שמידע נוסף כאמור נשמר בנפרד ונתון לבקרות טכניות וארגוניות המבטיחות מפני הצלבת נתונים כאמור.[378]

הדירקטיבה אינה מבארת מהו מזעור נתונים (data minimization). בתקנות הכלליות בדבר הגנת מידע (GDPR) המונח משמש לתיאור אחד מעקרונות הגנת המידע,[379] ולפיו מידע אישי יהיה רלוונטי ומוגבל בהיקפו למה שנדרש לתכלית עיבודו. מסמך של קבוצת העבודה למשטרה ולצדק הדן בהגנת מידע מתאר מזעור נתונים כעיקרון שלפיו מערכות מידע ייבחרו או יעוצבו באופן שעיבוד, איסוף ושימוש במידע אישי באמצעותן יהיה מינימלי (ורצוי שלא יתקיים כלל).[380]

לפי הוראות סעיף 20 לדירקטיבה, מנהל המאגר ינקוט את האמצעים הטכניים והארגוניים המתאימים כדי להבטיח שברירת המחדל תהיה שרק מידע אישי הנדרש להגשמת תכלית העיבוד יעובד. בעיקר יוגדרו כמות המידע המעובד, משך עיבודו, תקופת שמירת הנתונים והגישה אליהם, כברירת מחדל, הגדרה שתבטיח זאת. לפני שייעשה שימוש בשיטה חדשה של עיבוד נתונים, על מנהל המאגר להעריך את הסיכונים (impact assessment) באשר להשפעתה הפוטנציאלית על זכויות הפרט וחירויותיו, ובעיקר על ההגנה על מידע אישי.[381] הערכת סיכונים זו תדווח לרשות הפיקוח[382] כדי שזו תוכל לבחון את רמת הציות להוראות הדירקטיבה. הדירקטיבה כוללת הוראות נוספות בנוגע לתיעוד של עיבוד הנתונים שיאפשרו להתחקות אחר מועד ביצוען, ההצדקות להן ומי שנחשפו למידע.[383]

378 ס' 1(5) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

379 ס' 5(1)(c) לתקנות הכלליות בדבר הגנת מידע (GDPR).

380 Working Party on Police and Justice, *The Future of Privacy*, 13 (December 1, 2009)

381 ס' 27 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

382 ס' 28(4) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

383 ס' 25 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

רשות פיקוח עצמאית (Data Protection Authority)

דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) מורה למדינות־החברות להקים רשות פיקוח עצמאית שתעקוב אחר יישומה כדי להגן על זכויות בסיסיות ועל חירויות אנוש במסגרת פעולות עיבוד ומידע ולהבטיח זרימת מידע חופשית בתוככי האיחוד.[384] למטרה זו אפשר להסמיך את רשות הפיקוח העצמאית שתוקם מכוח ההוראות של התקנות הכלליות בדבר הגנת מידע (GDPR) לשמש רשות פיקוח עצמאית לפי הדירקטיבה.[385]

לצד הפיקוח על יישום הוראות הדירקטיבה, רשויות הפיקוח אחראיות להגברת המודעות הציבורית לנושאים הקשורים להגנת מידע ולסיכונים, לאיזונים ולכללים הנוגעים לעיבוד נתונים, לרבות הגברת המודעות של מנהלי המאגרים והמעבדים לחובותיהם לפי דין.[386] הרשות העצמאית תייעץ לפרלמנט ולממשלה בנושאי חקיקה ואסדרה בתחום של הגנת המידע הפרטי[387] או בתחום החקיקה והאסדרה שנוגעות בעקיפין בפעולות עיבוד נתונים,[388] תחקור תלונות של מושאי מידע[389] ותעקוב אחר ההתפתחויות הרלוונטיות להגנה על מידע פרטי.[390] עצמאותה של הרשות ביחס למדינה־החברה ניכרת גם בהוראות הדירקטיבה שלפיהן הרשות תשתף פעולה עם רשויות־הגנת־מידע דומות באיחוד, לפי הצורך.[391] כדי לאפשר לרשויות הפיקוח העצמאיות להגשים את מטרותיהן, על המדינות החברות להעניק להן סמכויות חקירה[392]

384 ס' 41 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

385 ס' 41(3) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

386 ס' 46(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

387 ס' 46(1)(c) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

388 ס' 28(2) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

389 למטרה זו על המדינות החברות להקים מנגנונים שמעודדים דיווח חשאי על הפרות של הוראות סטטוטוריות שאומצו בעקבות הדירקטיבה. ראו ס' 48 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

390 ס' 46(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

391 ראו ס' 51 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

392 ס' 47(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

ואכיפה[393] מתאימות וכן סמכויות ליזום או לנהל הליכים משפטיים בנוגע להפרות.[394]

רשות הפיקוח תהיה סטטוטורית,[395] עצמאית[396] ושקופה במינוי חבריה.[397] על המדינות־החברות להסמיך את רשויות הפיקוח העצמאיות ככל שנדרש לשם הגשמת תכליתן, אך ניתן להחריג מסמכותן פיקוח על עיבוד נתונים שנעשה בבתי משפט ובערכאות משפטיות אחרות, בהליך שיפוטי.[398]

על מנהלי המאגרים או המעבדים להתייעץ עם רשות הפיקוח לפני שהם פותחים בפעולות לעיבוד נתונים שיביאו לידי הקמתה של מערכת קבצים חדשה, אם בהערכת הסיכונים המקדימה[399] מתגלה כי רמת הסיכון לפרטיות – בהיעדר אמצעים מספיקים להפחתתה – גבוהה; או אם סוג עיבוד הנתונים – בשים לב לשימוש בטכנולוגיות חדשות[400] – יש בו כדי לסכן במידה רבה את פרטיותם ואת זכויותיהם של מושאי המידע.[401] חובת התייעצות מקדימה עם רשות הפיקוח העצמאית חלה גם על בית המחוקקים במהלך הכנת דברי חקיקה או הוראות רגולטוריות שקשורים לעיבוד מידע.[402]

393 ס' 47(2) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) מונה כמה דוגמאות לסמכויות אכיפה, בכללן אזהרה לפני הפרה צפויה, הסמכות לצוות על מעבדים או על מנהלי מאגרים לציית להוראות סטטוטוריות שאומצו לפי הדירקטיבה, לרבות צו למחיקת נתונים או לתיקונים, וכן לאסור על עיבוד נתונים.

394 ס' 47(3) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

395 ס' 44 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

396 ס' 42 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

397 ס' 43 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

398 ס' 45 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

399 impact assessment מכוח סעיף 27 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

400 על המדינות החברות להסמיך את הרשות המפקחת להגדיר מהן פעולות העיבוד המחייבות התייעצות מקדימה (ס' 28(3) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)).

401 ס' 28(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

402 ס' 28(2) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

כשהרשות סבורה כי פעולה של עיבוד נתונים שמנהל מאגר או מעבד הפנו אליה להתייעצות אינה ממתנת די הצורך את הסיכון הגלום בה, או שרמת הסיכון שייחסו לה מנהל המאגר או המעבד הוערכה בחסר, עליה לספק חוות דעת מתאימה למנהל מאגר או למעבד, ולפי הצורך להפעיל את סמכויות האכיפה שלה.[403]

- דיני הגנת המידע האירופיים בגלגולם הראשון כדירקטיבת הגנת המידע, היו מסגרת כללית לחקיקה ברמה הלאומית של מדינות האיחוד. התקנות הכלליות בדבר הגנת מידע (GDPR) שנכנסו לתוקף במאי 2018 הן בעלות השפעה ישירה בדין הלאומי של המדינות החברות. עם זה בשל הדינים הכלליים של האיחוד, מידת ההתערבות של המחוקק האירופי בהוראות החלות על פרקטיקות של מעקב מקוון למטרות של ביטחון לאומי ואכיפת חוק היא מוגבלת.
- דירקטיבת רשויות אכיפת החוק אינה כוללת הוראות קונקרטיות ביחס למעקב מקוון, אלא מסדירה את העקרונות הכלליים של עיבוד מידע אישי על ידי רשויות מוסמכות. עם זאת הוראות הדירקטיבה עשויות ללמד על העקרונות שלאורן יש לעצב את הדינים הלאומיים בדבר מעקב מקוון כך שיבטיחו כי איסוף המידע, עיבודו ושימורו ייעשו באופן מידתי ובשמירה על עקרון צמידות המטרה.
- הדין האירופי כולל הוראות מיוחדות ביחס לפעולות עיבוד אוטומטיות (כר"מ) של מידע אישי.
- הפסיקה של בתי הדין האירופיים מתייחסת מעת לעת לחוקיותן של פרקטיקות לאומיות של מעקב מקוון, ושבה ומגדירה את רמת הפירוט הנדרשת מהחקיקה הלאומית המסדירה אותן. בית הדין האירופי לצדק (ECJ) אף ביטל חקיקה אירופית שלפיה על המדינות החברות לאמץ חקיקה לאומית המורה על שימור נתוני תקשורת, בקובעו שאינה מידתית.

403 כמפורט **לעיל** בפרק זה ה"ש 393.

3.3. בריטניה

3.3.1. מעטפת חוקתית

לבריטניה אין חוקה. במקום זאת הזכות לפרטיות מוגנת בחוק זכויות אדם (HRA — Human Rights Act 1998),[404] שהוא הצינור המזרים לדין הבריטי את הוראותיה של האמנה האירופית לזכויות אדם (ECHR) ומאפשר לערכאות הבריטיות ולבית הדין האירופי לזכויות אדם (ECtHR) להכריז על אי-התאמתו של דבר חקיקה בריטי לאמנה.[405]

המהפכה החוקתית של חוק זכויות אדם (HRA) הציגה לבריטים שיח זכויות שהיה זר למסורת החוקתית המקומית. גם דיני הפרטיות הבריטיים – שמקורם בעילת תובענה של הפרת אמונים (breach of confidence) – התגלגלו לעילת השימוש לרעה במידע פרטי (misuse of private information),[406] שפיתוחה הפסיקתי נעשה דרך חוק זכויות אדם (HRA) על בסיס תפיסת הפרטיות של הדין האירופי.[407]

בעקבות הכפפתו של הדין הבריטי למשטר זכויות האדם האירופי ולסמכותו של בית הדין האירופי לזכויות אדם (ECtHR), הותקפה לא פעם חקיקה בריטית שנוגעת למעקב מקוון בטענה שאיננה הולמת את האמנה.[408] כך למשל בשנת

404 Human Rights Act 1998,c. 42 (Eng.)

405 **שם**, בס' 3-4.

406 Campbell v. MGN Ltd [2004] 2 AC 457, 465

407 להרחבה ראו Alpin, **לעיל** בפרק 2 ה"ש 94, בפרקים 1-3, 7.

408 Liberty & Others v. UK, No. 58243/00, Eur. Ct. H.R. (2008) (להלן: עניין *Liberty*); עניין *Kennedy*, **לעיל** בפרק זה ה"ש 227. כמו כן יש פניות תלויות ועומדות בפני בית הדין האירופי לזכויות אדם בקשר לפרקטיקות איסוף המודיעין הבריטיות שחשף סנודן – Big Brother Watch and Others v. UK, No. 58170/13 (9.01.2014); Bureau of Investigative Journalism and Alice Ross v. UK, No. 62322/14 (5.01.2015); 10 Human Rights Organizations and Others v. UK, No. 24960/15 (20.05.2015)

2008 הכריז בית הדין האירופי כי היעדר הוראות ברורות ופומביות בחוק יירוט שידורים (Interception of Communication Act 1985) בדבר הנהלים החלים על עיון, שיתוף, אחסנה וביעור של החומר שיורט, מפר את סעיף 8 לאמנה, שלפיה פגיעה בזכות לפרטיות מצד רשות ציבורית תהא "לפי דין".[409]

3.3.2. חוק הגנת מידע 1998 (DPA)

בדומה למדינות־חברות אחרות באיחוד האירופי, נדרשה גם בריטניה ליישם את הוראותיה של דירקטיבת הגנת המידע.[410] יישום הדירקטיבה נעשה באמצעות החוק הבריטי בדבר הגנת מידע 1998 (DPA — Data Protection Act).[411]

לפי החוק, נתונים אישיים (personal data)[412] יעובדו לפי עקרונות עיבוד הנתונים המפורטים בתוספת הראשונה לחוק: בהגינות[413] ולפי דין[414] בהתאם

409 עניין *Liberty*, **שם**. חוק יירוט שידורים הוחלף בחוק הסדרת סמכויות חקירה 2000 (RIPA), שחלקים מתוכו הוחלפו בהוראות חוק סמכויות חקירה 2016 (IPA) (ראו **להלן** בהמשך הפרק).

410 ראו חלק 3.2.3 **לעיל**.

411 Data Protection Act 1998, c.29 (Eng.) (להלן: החוק הבריטי בדבר הגנת מידע 1998 או DPA).

412 "נתונים אישיים" לפי הגדרת סעיף 1 לחוק הבריטי בדבר הגנת מידע 1998 (DPA), הם נתונים שבאמצעותם או בדרך של הצלבתם עם נתונים נוספים אפשר לזהות אדם חי. נתונים בהקשר זה הם מידע שמעובד באמצעים אוטומטיים, נשמר לקראת עיבוד אוטומטי עתידי או שייך לקטגוריות מסוימות של נתונים (רשומות רפואיות, חינוכיות או פומביות, כהגדרתם בס' 68 ובתוספות ה־11 וה־12 לחוק בהתאמה). "מידע אישי רגיש" לפי סעיף 2 לחוק הוא נתונים אישיים המתייחסים לגזעו או למוצאו האתני של פלוני, לעמדותיו הפוליטיות, לאמונותיו הדתיות, לחברותו בארגון עובדים, לבריאותו הגופנית או הנפשית, לחיי המין שלו, לעברו הפלילי או להליכים פליליים בנוגע לעבירות שביצע או שנטען שביצע.

413 להערכת מידת ההגינות של עיבוד הנתונים יש להתייחס לשיטה שהושגו בה, ובעיקר אם הושגו באמצעות הטעיית המקור שממנו הושגו. ראו סעיף 1 לחלק 2 של התוספת הראשונה לחוק הגנת מידע.

414 "לפי דין" – לפי כל דין ובכפוף להתקיימות אחד התנאים המפורטים בתוספת השנייה לחוק (מושא המידע הסכים לעיבוד; עיבוד הנתונים דרוש לקיום חוזה שמושא המידע הוא צד לו, למילוי התחייבות של מנהל המאגר שאינה מכוח חוזה, להגנה על

למטרות מוגדרות וחוקיות, בלי לחרוג מהמידה הנדרשת ומתוך שמירה על דיוק ועדכניות ועל זכויותיהם של מושאי המידע לפי החוק הבריטי בדבר הגנת מידע 1998 (DPA). נתונים אישיים יישמרו רק למשך הזמן שהם נדרשים למטרות העיבוד, ויינקטו אמצעים מתאימים כדי למנוע עיבוד נתונים לא חוקי או ללא הרשאה וכן הרס או אובדן מקריים של מידע. העברת מידע מחוץ לתחומי האיחוד האירופי מותנית ברמה נאותה של הגנת המידע במדינת היעד.[415]

בהלימה עם דירקטיבת הגנת המידע האירופית[416] החוק מקנה למושאי המידע זכות גישה למידע,[417] זכות למנוע עיבוד נתונים בנסיבות מסוימות,[418] זכות להגנה מהחלטות שהתקבלו על בסיס עיבוד אוטומטי של מידע[419] וזכות לתקן או למחוק נתונים אישיים.[420]

אינטרסים חיוניים של מושא המידע, או לשם השלטת צדק, מילוי פונקציות של הכתר או פונקציות פרלמנטריות, סטטוטוריות או פונקציות שטבען ציבורי למען האינטרס הציבורי) ובנוגע לעיבוד מידע אישי רגיש – גם בהתקיים אחד התנאים המפורטים בתוספת השלישית לחוק (מושא המידע הסכים מפורשות לעיבוד, העיבוד נדרש מכוח חובה החלה על בעל המאגר במסגרת דיני העבודה או לפי הוראה של שר הפנים (Secretary of State) מטעמים שיירשמו).

415 להרחבה, ראו Information Commissioner's Office, Guide to Data Protection (11.05.2016); Ian Brown, *Government Access to Private-Sector Data in the United Kingdom*, 2 Int'l Data Privacy Law 230 (2012); והשוו בין התוספת השנייה לחוק הגנת מידע ובין עקרונות הגנת המידע המפורטים בסעיף 6 לדירקטיבת הגנת המידע האירופית (ראו בחלק 3.2.3.1 **לעיל**) ובסעיף 5 לתקנות הכלליות בדבר הגנת מידע (GDPR). בנוגע להגנות הדין האירופי על העברת מידע מחוץ לאיחוד, ראו חלק 3.2.3.3 **לעיל**.

416 ראו חלק 3.2.3.2 **לעיל**.

417 ס' 7–9a לחוק הבריטי בדבר הגנת מידע 1998 (DPA), השוו לסעיף 15 לדירקטיבת הגנת המידע.

418 ס' 10–11 לחוק הבריטי בדבר הגנת מידע 1998 (DPA), השוו לסעיף 18 לדירקטיבת הגנת המידע.

419 ס' 12 לחוק הבריטי בדבר הגנת מידע 1998 (DPA). השוו לסעיף 21–22 לדירקטיבת הגנת המידע.

420 ס' 14 לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

נוסף על החובות החלות על מנהלי המאגרים (controllers) בשל הזכויות שמושאי המידע רשאים לתבוע מהם (מכוח היחס ההופלדיאני בין השניים), חלה עליהם גם חובת רישום של מאגרי המידע[421] במשרד המפקח על המידע (Information Commissioner's Office) – רשות הפיקוח הבריטית העצמאית (Data Protection Authority), שהוקמה בהמשך לדרישת הדירקטיבה.[422]

החוק הבריטי בדבר הגנת מידע 1998 (DPA) כולל רשימה ארוכה של נסיבות שפוטרות מכמה מהוראותיו.[423] כשהפטור נדרש מטעמים של ביטחון לאומי – שעל הנסיבות המצדיקות אותו תעיד תעודה חתומה בידי שר[424] – נתונים אישיים (ועיבודם) פטורים מתחולת העקרונות של עיבוד הנתונים שפורטו לעיל וכן מהוראות החוק המתייחסות לזכויות מושאי המידע ולחובות מנהלי המאגרים.[425] כמו כן סעיף שנדחק לתוספת השביעית של החוק מחריג מתחולתו מקרים שבהם מילוי הוראותיו בעניין נתונים אישיים מסוימים עשוי לסכן את הכשירות הקרבית של הכוחות המזוינים של הכתר.[426]

בנסיבות שבהן הדבר נדרש לתכליות של זיהוי פשיעה או מניעתה, מעצרם של עבריינים, קיום הליכים פליליים נגדם או למטרות של אומדן או גבייה של כל

421 ס 16–26 לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

422 ס' 51–54a לחוק הבריטי בדבר הגנת מידע 1998 (DPA). בנוגע להוראות הדירקטיבה, ראו בחלק 3.2.3.4 **לעיל**.

423 חלק 4 לחוק הבריטי בדבר הגנת מידע 1998 (DPA), ס' 27–39.

424 שר, לפי סעיף 28(10), הוא חבר בקבינט, התובע הכללי הבריטי או מקבילו הסקוטי (the Lord Advocate).

425 ס' 28 לחוק הבריטי בדבר הגנת מידע 1998 (DPA). יובהר כי התעודה אינה מקבילה של צו. התעודה משמשת אך ורק ראיה בדיעבד שהפטור התקיים. עיבוד מידע למטרות ביטחון לאומי אינו טעון אישור מיניסטריאלי מראש (אקס אנטה) לצורך פטור כאמור. עם זאת כל מי שנפגע ישירות מהוצאת תעודה כאמור רשאי לערער לפני בית דין מינהלי לפי כללי בתי הדין המינהליים (ס' 28(4)–(7),(12) וס' 70 לחוק הבריטי בדבר הגנת מידע 1998 (DPA)). לסדרי הדין בבתי הדין המינהליים הבריטיים, ראו Tribunals, Courts and Enforcement Act 2007, c.15 (Eng)

426 ס' 2 לתוספת השביעית של החוק הבריטי בדבר הגנת מידע 1998 (DPA).

היטל או מס,[427] היקפו של הפטור מהוראות החוק מצומצם יותר. עיבוד נתונים לתכליות אלו פטור מהעיקרון הראשון של עיבוד הנתונים,[428] שלפיו נתונים אישיים יעובדו לפי דין ובהגינות (הדרישה המשלימה של העיקרון הראשון להתקיימות אחד התנאים שבתוספת השנייה או השלישית לחוק[429] נותרה בעינה) ומתחולת זכות הגישה למידע.[430] כמו כן להגשמת תכליות אלו מוחל פטור מכל איסור על העברת מידע לצד שלישי.[431]

3.3.3. הצעת חוק הגנת מידע (DPB – Data Protection Bill)

בחודש ספטמבר 2017 פרסמה ממשלת בריטניה טיוטה ראשונה להצעת חוק הגנת מידע (DPB).[432] מטרת החוק להחליף את החוק הבריטי בדבר הגנת מידע 1998 (DPA) הקיים לקראת כניסתן לתוקף ב־2018 של התקנות הכלליות בדבר הגנת מידע (GDPR) ודירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680),[433] וכחלק מהיערכותו של הדין הבריטי לעידן שאחרי הפרישה מהאיחוד. לצד המשטר הכללי של הגנת המידע שבהצעת החוק (DPB), נכללות בה גם הוראות בנוגע לעיבוד מידע על־ידי רשויות אכיפת החוק וסוכנויות המודיעין.[434]

427 ס' 29(1) לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

428 ס' 1 לתוספת הראשונה לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

429 ראו **לעיל** בפרק זה ה"ש 414.

430 ראו ס' 29(1) וס'7 לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

431 ס' 29(3) לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

432 Data Protection HL Bill (2017-19) 66. (להלן: הצעת החוק הבריטי בדבר הגנת מידע (DPB)).

433 ראו חלק 3.2.5 **לעיל**.

434 לפי דברי ההסבר להצעת החוק, עיבוד מידע לתכליות של ביטחון לאומי מוחרגים מתחולת הרפורמה האירופית של התקנות הכלליות בדבר הגנת מידע (GDPR) ודירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), ולכן התבססו מנסחי הצעת החוק על הסטנדרטים המנוסחים בהצעה עדכנית לתיקון אמנה 108 של המועצה האירופית (Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981).

מאחר שלתקינה האירופית תחולה ישירה רק ממועד כניסתה לתוקף, הצעת החוק הבריטי בדבר הגנת מידע (DPB) אינה יישום של התקנות הכלליות בדבר הגנת מידע (GDPR), אלא התאמה מקומית של הדין להוראותיהן. כך למשל בחלקה השני של ההצעה[435] מצויה בין היתר רשימת החרגות מזכויות מושאי המידע לפי תקנות ה־GDPR בעניינים שונים;[436] הפחתת גיל ההסכמה לשירותי עיבוד מידע מ־16 ל־13 שנים;[437] והבהרות בנוגע לפרשנות התקנות ובכלל זה כי לצורך העמידה בדרישה לעיבוד על פי דין, התנאי החלופי המנוי בתקנות של עיבוד נתונים למטרות שבאינטרס הציבורי[438] יכלול עיבוד נתונים אישיים לתכליות של השלטת צדק או של מילוי פונקציות פרלמנטריות, סטטוטוריות או מלכותיות.[439]

חלקה השני של הצעת החוק הבריטי בדבר הגנת מידע (DPB) מחיל את הוראות התקנות הכלליות בדבר הגנת מידע (GDPR) על מקרים שבהם תקנות אלה אינן חלות (other processing), בכפוף להחרגות, בין השאר החרגה של עיבוד נתונים לתכליות של ביטחון לאומי והגנה[440] (המלווה בנוהל של הסמכה בתעודה מאת השר), ולצרכים ראייתיים, בדומה לנוהל הקיים בחוק הבריטי בדבר הגנת מידע 1998 (DPA).[441] החלקים השלישי הרביעי של ההצעה יידונו בהרחבה להלן, ואילו החלקים החמישי והשישי מתייחסים למשרדו של המפקח על המידע ולכללים החלים על אכיפת החוק.

435 ס' 3–18 להצעת החוק הבריטי בדבר הגנת מידע (DPB).

436 ס' 14–15 להצעת החוק הבריטי בדבר הגנת מידע (DPB) והתוספות השנייה, השלישית והרביעית להצעה.

437 ס' 18 להצעת החוק הבריטי בדבר הגנת מידע (DPB), המפנה לסעיף 8 של התקנות הכלליות בדבר הגנת מידע (GDPR). ס'8(2) ב־GDPR מאפשר למדינות החברות להוריד את גיל ההסכמה הנקוב בתקנות עד ל־13 שנים.

438 ס' 6(1)(e) לתקנות הכלליות בדבר הגנת מידע (GDPR).

439 ס' 7 להצעת החוק הבריטי בדבר הגנת מידע (DPB) השוו עם התוספת השנייה לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

440 ס' 24–26 להצעת החוק הבריטי בדבר הגנת מידע (DPB).

441 ס' 25, להצעת החוק הבריטי בדבר הגנת מידע (DPB) השוו לסעיף 28 לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

חלקה השלישי של ההצעה[442] מיישם בחקיקה את הוראותיה של דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680)[443] ומחיל אותה על רשימה של רשויות מוסמכות[444] – למעט שירותי המודיעין,[445] שעליהם חלות הוראות החלק הרביעי של ההצעה. הנוסח בחלק הרביעי מתבסס על נוסח ההצעה העדכנית לתיקון אמנה מס' 108 של המועצה האירופית להגנת זכויותיהם של יחידים בנוגע לעיבוד אוטומטי של נתונים אישיים.[446] בחלק זה נמנים שישה עקרונות לעיבוד נתונים, בשינויים המתאימים;[447] זכויות של מושאי המידע;[448] והחובות של מנהלי מאגרי המידע ומעבדי הנתונים.[449] אלא שבנסיבות שבהן מטעמים של ביטחון לאומי נדרש לחרוג מרוב עקרונות העיבוד של הנתונים, מזכויותיהם של מושאי המידע או מהחובה לדווח על פרצת אבטחה למשרד המפקח על המידע, הצעת החוק מתירה חריגות כאמור.[450] סעיף 107 להצעת החוק אוסר להעביר

442 ס' 27–79 להצעת החוק הבריטי בדבר הגנת מידע (DPB).

443 ראו חלק 3.2.5.2 **לעיל**.

444 ס' 28 להצעת החוק הבריטי בדבר הגנת מידע (DPB), המפנה לתוספת השביעית המונה את הרשויות המוסמכות, ובהן משרדי הממשלה, משרד המשפטים של צפון אירלנד, גופי שיטור שונים בבריטניה ובכוחות הביטחון הבריטיים, המכס, רשות הפשיעה הלאומית, התובעים הכלליים באנגליה, בסקוטלנד ובצפון אירלנד, גופים העוסקים בעבריינות נוער וכו'.

445 ס' 28(2) להצעת החוק הבריטי בדבר הגנת מידע (DPB). שירותי המודיעין המנויים, ובהם מטה התקשורת הממשלתי (GCHQ), סוכנות הביון הבריטית (Secret Intelligence Service, המוכרת גם כ־SIS או כ־MI6 והשירות החשאי (Security Service, או MI5).

446 ראו **לעיל** בפרק זה ה"ש 435.

447 ס' 83–89 להצעת החוק הבריטי בדבר הגנת מידע (DPB).

448 בס' 90–98 להצעת החוק הבריטי בדבר הגנת מידע (DPB) מנויות – בעניין עיבוד נתונים אישיים בשירותי המודיעין – זכות הגישה למידע, זכויות בנוגע לעיבוד נתונים אוטומטי, זכות להתנגדות מושא המידע לעיבוד הנתונים והזכות לתיקון הנתונים האישיים או למחיקתם.

449 בס' 99–106 להצעת החוק הבריטי בדבר הגנת מידע (DPB) מנויות – בעניין עיבוד נתונים אישיים בשירותי המודיעין – חובות מנהלי מאגרי המידע ומעבדי הנתונים, ובתוכן החובה לעיבוד נתונים בהלימה עם החוק, חובת עיצוב מערכות בהתייחסות להגנת מידע (data protection by design), חובת עיבוד נתונים רק מכוח הרשאה מוסכמת וחובות אבטחת מידע.

450 ס' 108 להצעת החוק הבריטי בדבר הגנת מידע (DPB). נוסף על נסיבות אלו, בתוספת ה־11 לחוק נמנים גם מקרים אחרים שבהם מותר לחרוג מהוראות החוק בפעולות

נתונים אישיים אל מחוץ לתחומי הממלכה המאוחדת, אלא אם ההעברה הכרחית ומידתית ביחס לתכליות הסטטוטוריות של הגוף שהעבירן או לתכליות המנויות בדברי חקיקה אחרים.[451]

התגובות הראשונות להצעת החוק[452] מלינות על הנוסח הסבוך שלה ומציינות כי היא שמרנית ונצמדת – ככל שהתקנות הכלליות בדבר הגנת מידע (GDPR) מאפשרות לה – למתווה העקרוני של החוק הקיים להגנת המידע. הביקורות גם תוהות אם ההפרדה לחלקים שמיועדים לכוחות הביטחון מכאן ולשירותי המודיעין מכאן אכן נחוצה, ומצביעות על מגוון ההחרגות והפטורים הכלולים בהצעה. עוד הובע החשש מזליגת מידע פרטי מחוץ לתחומי בריטניה בחסות הפטורים הרחבים שבסעיף 107.[453]

3.3.4. חוק סמכויות חקירה 2016 (IPA)

3.3.4.1 רקע: החוק להסדרת סמכויות החקירה 2000 (RIPA) וחוק סמכויות חקירה ושימור נתונים 2014 (DRIPA)

חוק סמכויות חקירה (IPA — Investigatory Powers Act)[454] הבריטי משנת 2016 הוא גלגול שני של תיקונים בדיני המעקבים המקוונים במדינה זו. כאמור

עיבוד נתונים של שירותי המודיעין, למשל כשהדבר עלול לפגום בחסינות פרלמנטרית או בחסיון עורך דין-לקוח, לפגוע בכשירות המבצעית של הכוחות המזוינים, או לצורכי בחינות, ארכיון או מחקר.

451 הוראה זו – וההחרגה שבצידה - חלות כאמור רק על שירותי המודיעין. לצד התכליות הסטטוטוריות הספציפיות של כל אחד משירותי המודיעין, ס' 107 להצעת החוק הבריטי בדבר הגנת מידע (DPB) מפנה לתכליות מכוח חוק השירות החשאי וחוק שירותי המודיעין.

452 Francis Aldhouse, *The UK Government Publishes the Data Protection Bill* (20.09.2017); Privacy International, *Briefing on the Data Protection Bill for Second Reading in the House of Lords* (6.10.2017)

453 Privacy International, **שם**, בעמ' 10.

454 Investigatory Powers Act 2016, c.25 (Eng.) (להלן: חוק סמכויות חקירה 2016 (IPA)).

בפרק הקודם, בפרשת *Digital Rights Ireland* (*DRI*)[455] פסל בית הדין האירופי לצדק (ECJ) את דירקטיבת שימור הנתונים (Data Retention Directive)[456] כשקבע שהוראותיה מתערבות בזכויותיהם של אזרחי האיחוד ללא הבחנה, הגבלה או החרגה. בעקבות קביעה זו ובהיעדר הגבלות על הגישה למידע, על השימוש שנעשה בו ועל תקופת השימור – בוטל בעקיפין גם תוקפה של החקיקה הלאומית הרלוונטית.[457] כדי להתאים את הדין הבריטי לתוצאות עניין *Digital Rights Ireland*,[458] בשנת 2014 חוקק בית הנבחרים הבריטי את חוק סמכויות חקירה ושימור נתונים (DRIPA — Data Retention and Investigatory Powers Act).[459] כדי לאשר את החוק בפרלמנט הוכנס בו סעיף המגביל את תוקפו לשנתיים,[460] שבסופן ישובו לקדמותן הוראות החוק להסדרת סמכויות החקירה משנת 2000 (RIPA - Regulation of Investigatory Powers Act) הנוגעות לנתוני תקשורת.[461]

חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA) הסמיך את שר הפנים[462]

455 עניין *DRI*, **לעיל** בפרק זה ה"ש 228.

456 ראו **לעיל** בפרק זה ה"ש 300.

457 אין מדובר בביטול ישיר. בעקבות עניין *DRI*, חקיקה מדינתית ניתנת לתקיפה בערכאות הלאומיות על בסיס תוצאות DRI, כפי שנעשה בהמשך בבריטניה (ראו **להלן**). להרחבה ראו F. Boehm & M. D. Cole, *Data Retention after the Judgment of the Court of Justice of the European Union Study*, Study for the Greens/EFA Group in the European Parliament, (30.6.2014).

458 ראו דברי המבוא לחוק סמכויות חקירה ושימור נתונים 2014 (DRIPA).

459 Data Retention and Investigatory Powers Act 20, 14 c.27 (Eng.) (להלן: חוק סמכויות חקירה ושימור נתונים (DRIPA 2014)). ראו גם Zedner, **לעיל** בפרק זה ה"ש 308, בעמ' 577–583.

460 סעיף 8(3) לחוק סמכויות חקירה ושימור נתונים 2014 (DRIPA).

461 Regulation of Investigatory Powers Act 2000, c.23 (Eng.) (להלן: חוק הסדרת סמכויות חקירה 2000 (RIPA)).

462 השר המופקד על חוק סמכויות חקירה 2016 (IPA) הוא שר הפנים (Secretary of State for the Home Department), ובאשר למודיעין שמעבר לים – שר החוץ (Secretary of State for Foreign and Commonwealth Affairs). על פי רוב, דברי החקיקה הבריטיים אינם מציינים את המשרד שעליו השר מופקד. חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA) וגם חוק סמכויות חקירה 2016 (IPA) נוקטים

להורות לספק תקשורת לשמור נתוני תקשורת מסוימים[463] אם השר סבור כי שימורם נדרש ומידתי ביחס למטרות הקבועות בתקינה.[464] מאז שנחקקו שני החוקים (RIPA ו־DRIPA) נעשה בסמכויות שהם מקנים שימוש רב. לפי נתוני משרד הפנים הבריטי בשנת 2014 ניתנו 517,236 אישורים לבקשות של המשטרה (ורשויות אחרות) לנתוני תקשורת (לרבות נתונים ששימורם נדרש לפי DRIPA), שמקורן ב־267,373 בקשות, ושרים אישרו 2,765 צווי יירוט.[465]

ואולם עד מהרה הוגשה לבית המשפט הגבוה הבריטי עתירה נגד חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA) בטענה שהחוק אינו הולם את סעיף 8 לאמנה האירופית לזכויות אדם (ECHR), שלפיה לכל אחד הזכות שפרטיותו, חיי משפחתו והתכתבויותיו יכובדו (בכפוף לסייגים). העתירה טענה כי את סעיף 8 לאמנה – שלו תחולה ישירה בדין הבריטי מכוח הוראותיו של חוק זכויות אדם (HRA) – יש לפרש בדומה לפרשנות שפירש בית הדין האירופי בעניין *DRI* את סעיפים 7 ו־8, המקבילים לו במגילת זכויות היסוד (CFR). העותרים טענו כי כדי שהחקיקה הבריטית בדבר שימור המידע תהלום את הלכת *DRI*, עליה להגביל את הסמכות להורות על שימור מידע לנתונים שנוגעים לביטחון הציבור, להגביל את היקפו הגאוגרפי של השימור או את תקופת הזמן שלו, לכלול הוראות מיוחדות בנוגע לשימור נתונים שחל עליהם חיסיון מקצועי, להגביל את הגישה

את הלשון "Secretary of State", שלפי חוק הפרשנות הבריטי הוא "אחד משרי הקבינט המופקד על משרד ממשלתי" (על משרד האוצר, למשל, אין מופקד Secretary of State אלא ה־Chancellor of the Exchequer). ראו Schedule 1 of the Interpretation Act 1978, c. 30 (Eng.)

463 הגדרת "נתוני תקשורת" מצויה בסעיף 21 של חוק הסדרת סמכויות חקירה 2000 (RIPA). נתוני תקשורת הם (1) נתוני תעבורה המצורפים לתקשורת; (2) נתונים שאינם תוכנה של תקשורת, והם נתונים על שימוש בשירותי תקשורת או דואר, או (3) נתונים שמחזיק ספק תקשורת או דואר על המשתמשים.

464 מטרות אלה כוללות אינטרסים של ביטחון לאומי, מניעת פשיעה והפרות סדר, אינטרסים כלכליים של הממלכה המאוחדת (אם אלה רלוונטיים לאינטרסים של ביטחון לאומי), ביטחון הציבור והגנה על בריאות הציבור. עוד נכללות מטרות של גבייה או אומדן של מיסים, היטלים וחיובים אחרים לרשות ממשלתית, הצלת חיים ומניעת נזק בגוף ובנפש בעת חירום, או כל מטרה אחרת המפורטת בצו מאת השר. ראו ס' 22(2) של חוק הסדרת סמכויות חקירה 2000 (RIPA).

465 Report of Interception of Communications Commissioner, March 2015, Annex B.

למידע ואת השימוש בו לתכליות הנוגעות למניעה, לחקירה ולגילוי של פשעים, ומעל הכול להבטיח כי גוף מינהלי או שיפוטי עצמאי יבקר מראש בקשות לגישה למידע זה על בסיס צורך מוחלט.

ביולי 2015 קבע בית המשפט כי ממרץ 2016 יתבטלו הוראות DRIPA אם הגישה לנתוני תקשורת שנשמרו מכוח צו שנתן השר לפי הוראות אלה והשימוש בהם ייעשו למטרות שאינן מניעה או זיהוי של פשעים חמורים או למטרות של ניהול תביעות משפטיות הקשורות בהם, וכן אם הגישה לנתוני תקשורת והשימוש בהם לא יהיו כפופים לביקורת שיפוטית שבכוחה להגבילם לפי סטנדרט של צורך מוחלט.[466] המדינה ערערה על החלטת בית המשפט הגבוה,[467] כדי להכריע בערעור הפנה בית הדין לערעורים שתי שאילתות לבית הדין האירופי לצדק (ECJ),[468] שנתבררו בעניין *Tele2 Sverige AB*.[469]

והנה, בעת שישב בית הדין האירופי לצדק על המדוכה בעניין *Tele2 Sverige AB*, החל המחוקק הבריטי לקדם רפורמה מקיפה בדיני המעקב המקוון,[470] שנוסף

466 ראו פס' 122 לפסק דינו של השופט בין (Bean), Davis and Others v. Secretary of State for the Home Department [2015] EWHC 2092 (Admin). להרחבה ראו Lornea M. Woods*, High Court Strikes down Data Retention Laws in Ruling on DRIPA* 1 Eur. Data Prot. L. Rev. 236 (2015)

467 Secretary of State for the Home Department v. David Davis MP and others [2015] EWCA Civ 1185; להרחבה, ראו Lornea M. Woods*, Court of Appeal Refers to CJEU on DRIPA* 4 Eur. Data Prot., L. Rev. 307 (2015)

468 בפסקה 118 לפסק דינו של השופט ג'ונס, **שם**, מפורטות השאילתות: (1) האם פסק הדין בעניין *DRI* (**לעיל** בפרק זה ה"ש 228), מכיל הנחיות מחייבות בדבר החקיקה הלאומית של המדינות החברות? (2) האם התכוון בית הדין האירופי להרחיב את תחולת הסעיפים 7 ו־8 לאמנה האירופית מעבר לתחולת סעיף 8 כמו שזו באה לידי ביטוי בפסיקת בית הדין האירופי לזכויות אדם (ECtHR)?

469 ראו עניין *Tele2 Sverige AB*, **לעיל** בפרק זה ה"ש 228.

470 לא רק כדי להתמודד עם הקושי המשפטי שנוצר, אלא גם בשל תום תוקפו של חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA) שהתקרב. דברי ההסבר לחוק אינם מזכירים לא את תוצאות עניין *Davis*, **לעיל** בפרק זה ה"ש 467, ולא את עניין *Tele2 Sverige AB*, שהיה תלוי ועומד כשאושר חוק סמכויות חקירה 2016 (IPA). עם זאת סעיף 24 לדברי ההסבר מאזכר את עניין *DRI*, שבעקבותיו בוטלה דירקטיבת שימור הנתונים. ראו Investigatory Powers Act 2016 Explanatory Notes.

על ההסדרים המצויים בחוק סמכויות חקירה ושימור נתונים 2014 (DRIPA), שהתייחסו לשימור נתונים, מטפלת גם ביירוט נתוני תוכן, פעילות סייבר ואיסוף גורף (bulk collection) של נתוני תקשורת וכן מציגה בקרות מוסדיות ופרוצדורליות המתייחסות לשיקולי מידתיות, צורך והגנה על פרטיות. כבר בשלבי החקיקה של החוק החדש (חוק סמכויות חקירה 2016 — IPA) זכתה הרפורמה לכינוי "the UK snooper's charter" (ובתרגום חופשי: "מגילת זכויות החטטן").

כשנכנס החוק החדש (IPA) לתוקף, צייץ אדוארד סנודן ממחבואו כי "המעקב הקיצוני ביותר בהיסטוריה של הדמוקרטיה המערבית נעשה עתה לחוקי בממלכה המאוחדת, והוא חורג מהנעשה באוטוקרטיות רבות".[471] מלבד סנודן, הביעו גם ארגונים רבים בחברה האזרחית את מורת רוחם מהחקיקה,[472] וכך גם הדַוָּוח המיוחד של האומות המאוחדות (UN Special Rapporteur) לנושא פרטיות, שדחק בבריטניה לנצל את ההזדמנות לרפורמה, לתת דוגמה חיובית ולסגת מעיגון בחקיקה של אמצעי מעקב לא מידתיים.[473]

3.3.4.2 איסור כללי על יירוט תקשורת

חוק סמכויות חקירה (IPA) מחיל איסור כללי על יירוט שלא על פי דין של תקשורת העוברת דרך בריטניה,[474] ממערכות תקשורת אלקטרונית ומשירותי דואר ציבוריים.[475] מהאיסור הכללי הוראות החוק מחריגות יירוט של תקשורת

471 Edward Snowden, Twitter (13.11.2016)

472 ראו לדוגמה EDRi, *UK's Mass Surveillance Law Being Rushed through Legislative Process* (9.3.2016); Gus Hosein, *From Britain, with Bulk Love: A Dark Digital Magna Carta*, Privacy International (11.11.2015); National Council for Civil Liberties, *Failure to Balance Privacy and Surveillance: Liberty Responds to the Draft Investigatory Powers Bill* (4.11.2015); ראו גם העצומה שהוגשה לביטול החוק: Closed Petition, *Repeal the new Surveillance Laws (Investigatory Powers Act)* (closed on 07.05.2017)

473 ראו פס' 38 לדיווח השנתי של שנת 2016, Report of the Special Rapporteur on the right to privacy, A/HRC/31/64 (24.11.2016)

474 ס' 3(1)(b) וכן ס' 8 לחוק סמכויות חקירה 2016 (IPA).

475 ס' 3 לחוק סמכויות חקירה 2016 (IPA).

שנועדה להיקלט באמצעות הכלל (general reception)[476] ויירוט של תקשורת שנעשה בסמכות חוקית,[477] ובייחוד יירוט מכוח צו.

3.3.4.3 שיקולי פרטיות שיש להביא בחשבון

לשונו של חוק סמכויות חקירה 2016 (IPA) מכירה בכך שהפעלת סמכויות המעקב הנתונות בו עלולה לפגוע בזכות לפרטיות,[478] ועל כן בעת החלטה על הפעלתן יש להביא בחשבון שיקולים של פגיעה בפרטיות. כשרשות ציבורית מחליטה האם לאשר, לבטל, לשנות או לחדש צווים מכוח חוק סמכויות חקירה 2016 (IPA) (לרבות הוראות שימור נתוני תקשורת לספקי תקשורת) או לאשר החלטות כאמור, עליה להתייחס להיבטים של הגנה על הפרטיות.[479] על הרשות לבחון אם ניתן להשיג את מטרת הצו או האישור באמצעים פולשניים פחות,[480] והאם בשל רגישות הנתונים המבוקשים[481] נדרשת רמה גבוהה יותר של הגנה עליהם.[482] עוד על הרשות לשקול את האינטרסים הציבוריים הנוגעים ליציבות ולביטחון של מערכות התקשורת והדואר,[483] וכל אינטרס ציבורי אחר הנוגע להגנה על הפרטיות.[484]

476 ס' 5(1) לחוק סמכויות חקירה 2016 (IPA).

477 ס' 6 לחוק סמכויות חקירה 2016 (IPA). עוד מוחרג יירוט תקשורת שנעשה בהסכמת אחד הצדדים לה (ס' 44). כמו כן יש הוראות מיוחדות ליירוט של תקשורת במוסדות כוללניים: בתי כלא (ס' 49), מוסדות פסיכיאטריים (ס' 50) ומתקני מעצר של מהגרים (ס' 51).

478 ס' 1(2) לחוק סמכויות חקירה 2016 (IPA).

479 ס' 2 לחוק סמכויות חקירה 2016 (IPA).

480 ס' 2(2)(a) לחוק סמכויות חקירה 2016 (IPA).

481 מידע רגיש כולל בין השאר פריטי מידע חסויים, מידע שיש בו כדי לזהות מקור עיתונאי או לאשר את זהותו, וכן פריטי מידע מסוימים שנוגעים לחברי פרלמנט. ראו הדוגמאות המנויות בסעיף 2(5) לחוק סמכויות חקירה 2016 (IPA).

482 ס' 2(2)(b) לחוק סמכויות חקירה 2016 (IPA).

483 השוו לזכות הגרמנית לסודיות ולשלמות של מערכות מידע אלקטרוניות. ראו עניין **המעקב המקוון, להלן** בפרק זה ה"ש 786.

484 ס' 2(2)(d)–(c) לחוק סמכויות חקירה 2016 (IPA).

מנגד, החובה להביא בחשבון היבטים אלו של הגנה על הפרטיות כפופה לרלוונטיות שלהם לנסיבות המסוימות ולצורך לשקול שיקולים אחרים, בכללם אינטרסים של ביטחון לאומי ושגשוגה הכלכלי של בריטניה וכן אינטרס הציבור במניעת פשיעה וזיהויה.[485] שיקולים אחרים שנמנים בחוק החדש הם ההוראות של חוק זכויות אדם הבריטי (HRA), הוראות אחרות בדין הציבורי וכן שיקולי צורך ומידתיות.[486]

כמו שנראה להלן, נוסף על ההוראה הכללית לשקול אינטרסים אלה, החוק מגדיר לכל סוג של צו את התכליות שלאורן יש לשקול את מידתיותו ואת נחיצותו.

3.3.4.4 השגת נתוני תוכן: צווים ממוקדים (targeted warrants)

לפי ההוראות בפרק השני של החוק (IPA), ניתן להוציא צווי יירוט ממוקדים, צווי בדיקה ממוקדים וצווי סיוע הדדי. צווים ממוקדים אלה עוסקים ביירוט של נתוני תוכן שנאספו בהקשרים שונים ובעיון בהם, ויש להבחין בינם ובין צווי יירוט או השגה כלליים, שיתוארו בהמשך. צווים ממוקדים מתייחסים ליעדי מודיעין מוגדרים ולמטרות איסוף ממוקדות, בשונה מהאיסוף גורף (bulk collection), הנעשה במסגרת צווי האיסוף הכלליים (bulk warrants).[487]

צווים ממוקדים יכולים להיות בנוגע לאדם או לארגון מסוימים, או בקשר לחצרים מסוימים. צווי יירוט ובדיקה ממוקדים גם יכולים לציין קבוצה של אנשים בעלי מטרה משותפת העוסקים בפעילות מסוימת או למטרת מבצע או חקירה יחידים – אף יותר מארגון, מאדם או מחצרים יחידים.[488] לשון הצו תתאר את אלה במפורש.[489]

485 ס' 2(4)(b)–(a) לחוק סמכויות חקירה 2016 (IPA).

486 ס' 2(4)(e)–(c) לחוק סמכויות חקירה 2016 (IPA).

487 ראו חלק 3.3.4.8 **להלן**.

488 ס' 17 לחוק סמכויות חקירה 2016 (IPA).

489 ס' 31(3)–(5) לחוק סמכויות חקירה 2016 (IPA).

צווים של יירוט ממוקד (targeted interception warrant) מורים או מאשרים למושאיהם ליירט שידורים (לרבות נתוני תוכן), להשיג נתונים משניים (secondary data)[490] ולהעבירם למי שמאושר לכך בצו.[491]

יש שני סוגים של צווי עיון ממוקדים (targeted examination warrant): הסוג הראשון, הכלול בפרק הראשון של החוק, הוא צו לעיון בנתוני תוכן שיורטו בצו יירוט כללי (bulk interception warrant).[492] הסוג השני, הכלול בהוראות הפרק החמישי של החוק, הוא צו לעיון במידע מוגן[493] שהושג בצו סייבר כללי (bulk equipment interference warrant).[494] התיאור שלהלן מתייחס לצווי עיון ממוקדים מהסוג הראשון.

490 "נתונים משניים" הם נתוני זיהוי (identifying data) שכלולים בשדר התקשורת, מצורפים אליו או מתלווים לו, וכן ניתנים להפרדה לוגית משאר השדר באופן שאין בהם כדי ללמד על משמעותו (ס' 16(6) לחוק סמכויות חקירה 2016 (IPA)). בנתוני זיהוי יש כדי לזהות כל אדם, מכשיר, מערכת, שירות, אירוע או את מיקומם, או לסייע בזיהוים (ס' 263 (2) לחוק סמכויות חקירה 2016 (IPA). נתונים משניים יכולים להיות גם נתוני מערכת (systems data) הכלולים בשדר התקשורת, מחוברים אליו או מקושרים אליו לוגית (ס' 16(5) לחוק סמכויות חקירה 2016 (IPA)). "נתוני מערכת" הם נתונים המזהים מערכות או שירותי תקשורת, או מאפשרים את פעילותם (ס' 263(4)–(5) לחוק סמכויות חקירה 2016 (IPA)).

491 ס' 15 (2) לחוק סמכויות חקירה 2016 (IPA).

492 ס' 15 (3) לחוק סמכויות חקירה 2016 (IPA). לתיאור צווי יירוט כלליים, ראו חלק 3.3.4.8.1 **להלן**.

493 "מידע מוגן", בהתייחס לצו בדיקה ממוקד (מכוח פרק 5 לחוק סמכויות חקירה 2016 (IPA)), הוא כל חומר שהושג מכוח צו יירוט כללי, חוץ מנתוני ציוד ומידע שאינו מידע פרטי (ס' 99(9) לחוק סמכויות חקירה 2016 (IPA). "נתוני ציוד" הם נתוני מערכת ונתונים נוספים הכלולים בפעילות התקשורת של המערכת שניתן להפרידם מהתקשורת הפרדה לוגית ובלי שתוצר הפרדה זו ילמד על תוכן התקשורת. נתוני ציוד יכולים לכלול למשל אותות או מסרים שנשלחים בין חלקים ברשת לצורך ניהול תעבורת התקשורת, הגדרות חומת האש או נתב התקשורת, גרסת מערכת ההפעלה, מיקום של פגישה שתועדה ביומן, metadata נלווה לקובצי תמונות, זמני פעילות נתב התקשורת במערכת או כתובות דוא"ל שאליהן אתר אינטרנט מפנה (mailto) (ס' 100 לחוק סמכויות חקירה 2016 (IPA) וכן ס' 296 לדברי ההסבר לחוק). מידע פרטי נוגע לחייו הפרטיים או לחיי המשפחה של פלוני (ס' 135(1) לחוק סמכויות חקירה 2016).

494 ס' 99(9) לחוק סמכויות חקירה 2016 (IPA), ראו חלק 3.3.4.8.3 **להלן**.

צווי סיוע הדדיים מסמיכים אדם לבקש מרשויות זרות מוסמכות (competent authorities) מידע (גולמי או מעובד) שהושג בקשר עם יירוט תקשורת, להעניק להן סיוע בקשר למידע כאמור, או להעבירו אליהן בכפוף להסכמי סיוע הדדיים אירופיים ובין-לאומיים.[495] בנסיבות מסוימות רשאי השר (secretary of state), לבקשת ראש סוכנות מודיעין, להוציא צווים משולבים.[496]

השר[497] רשאי להוציא צו ממוקד לבקשתו של ראש רשות יירוט (Interception Authority),[498] ובתנאי שהוא סבור שהצו נחוץ ושהמבוקש בו מידתי ביחס למטרתו.[499] ביטחון לאומי, מניעת פשע ושמירה על רווחתה הכלכלית של הממלכה[500] הם טעמים המצדיקים צו יירוט ממוקד או צו עיון ממוקד.[501] צו

495 ס' 15 (4) לחוק סמכויות חקירה 2016 (IPA). ראו גם אמנת שיתוף הפעולה ההדדי בעניינים פליליים בין חברות האיחוד האירופי, ובעיקר בפרק 3 (ס' 18–22): 2000/c/197/01 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union

496 ס' 248 לחוק סמכויות חקירה 2016 (IPA) והתוספת השמינית לחוק. צווים משולבים עשויים לכלול אחד או יותר מהצווים האלה: צו יירוט ממוקד, צו עיון ממוקד, צו הפרעה ממוקדת למכשור (targeted equipment interference warrant, ראו חלק 3.3.4.8.3 **להלן**) וצווי מעקב מכוח דברי חקיקה אחרים המפורטים שם.

497 על הצו צריך להחליט השר בעצמו, וכשהדבר אינו אפשרי – אישיות בכירה בשירות הציבורי שהשר הסמיכה (ראו ס' 30 לחוק סמכויות חקירה 2016 (IPA)). ראו גם **לעיל** בפרק זה ה"ש 462.

498 ס' 18 לחוק סמכויות חקירה 2016 (IPA). כל אחד משלושת ראשי סוכנויות הביון הבריטיות (MI6, MI5, GCHQ), ראש מודיעין ההגנה (DI), מפקדי המשטרה (משטרת לונדון, משטרת צפון אירלנד, משטרת סקוטלנד), ראש הסוכנות הלאומית לפלילים (NCA), רשויות המס (HMRC) וכל מי שיש לו סמכות מדינתית למטרות של סיוע מודיעיני הדדי (מכוח האמנה האירופית או מכוח הסכם אחר, ראו ה"ש 495 **לעיל** בפרק זה).

499 ס' 19(1)(b)–(a), 19(2)(b)–(a), 19(3)(b)–(a) לחוק סמכויות חקירה 2016 (IPA).

500 צו למטרת שמירה על רווחתה הכלכלית של הממלכה ייחשב נדרש רק כשהמידע המבוקש נוגע לפעילות או לגורמים מחוץ לגבולות האיים הבריטיים. ס' 20 (4) לחוק סמכויות חקירה 2016 (IPA).

501 ס' 20(2) לחוק סמכויות חקירה 2016 (IPA).

יירוט ממוקד יינתן בתנאי שהשר סבור שיש די בקרות סטטוטוריות על אבטחת המידע ותפוצתו,[502] ומתן צו עיון ממוקד יינתן בתנאי שהשר בוחן, בנסיבות הרלוונטיות, אם הצו הכרחי או יכול להיות הכרחי לאישור עיון סלקטיבי בנתוני תוכן על אנשים פרטיים בתחומי בריטניה.[503]

החלטת השר להוציא צו ממוקד כפופה לאישורו של נציב שיפוטי (Judicial Commissioner),[504] אלא אם השר סבור שהדבר דחוף.[505] במקרים דחופים ידווח השר לנציב השיפוטי לאחר מעשה, וזה יחליט (לכל המאוחר בתוך שלושה ימי עבודה מיום הוצאת הצו הדחוף) אם לאשרו בדיעבד.[506] צו ממוקד דחוף יעמוד בתוקפו חמישה ימים.[507]

בהחלטתו לאשר צו ממוקד, על הנציב השיפוטי לבחון את נחיצותו ואת מידתיותו.[508] אף שהנציב אינו ערכאה משפטית, כשהוא בוחן את הצו עליו להפעיל את אותם עקרונות של ביקורת שיפוטית שמפעיל בית המשפט, וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[509] החלטתו של הנציב השיפוטי שלא לאשר צו ממוקד תנומק בכתב.[510]

מנגנון זה של אישור כפול – הן של גורם מיניסטריאלי והן של גורם מעין־שיפוטי – המכונה "נעילה כפולה" (double lock), הוא אחד ההיבטים החדשניים

502 ראו ס' 53–54 לחוק סמכויות חקירה 2016 (IPA).

503 ראו האיסור בס' 152 לחוק סמכויות חקירה 2016 (IPA), חלק 3.3.4.8.2 **להלן**.

504 ראו חלק 3.3.4.9.1 **להלן**.

505 ס' 19(1)(d), 19(2)(d), 19(3)(d) לחוק סמכויות חקירה 2016 (IPA).

506 ס' 24 לחוק סמכויות חקירה 2016 (IPA).

507 ס' 31 לחוק סמכויות חקירה 2016 (IPA).

508 לפי קריטריונים לנחיצות שעל השר לשקול, המנויים בס' 20 לחוק סמכויות חקירה 2016 (IPA).

509 מכוח ס' 2 לחוק סמכויות חקירה 2016 (IPA), ראו חלק 3.3.4.3 **לעיל**.

510 ס' 23(4)–(5) לחוק סמכויות חקירה 2016 (IPA). כשהנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (Investigatory Powers Commissioner), מבקש הצו רשאי לערער לפני נציב סמכויות החקירה על הדחייה.

ברפורמה של חוק סמכויות חקירה 2016 (IPA). אלא שבדומה לדיני המעקב המקוון בשיטות משפט אחרות, לא כל צווי המעקב בבריטניה כפופים אליו (ראו למשל בחלק 3.3.4.5 להלן). זאת ועוד, רמת הביקורת השיפוטית שיפעילו הנציבים השיפוטיים טרם נבחנה בפועל, ואין לדעת אם הם יסתפקו בבחינה של נושאים פרוצדורליים בהליכי קבלת ההחלטות של השר, או שמא הם יבחרו לבחון נושאים מהותיים הקשורים לצו.[511] עם זאת מסתמן כי בכוונת משרד נציב סמכויות החקירה שלא להסתפק בבחינה מינהלית של החלטת השר, אלא לבחון את מידתיות הבקשה ביחס לתכלית שאותה היא מבקשת להשיג.[512]

צווים ממוקדים שמטרתם ליירט תקשורת של חברי פרלמנט[513] טעונים אישור מאת ראש הממשלה.[514] כמו כן יש הוראות מיוחדות בנוגע לצווים ממוקדים הקשורים לפריטי מידע הנהנים מחיסיון משפטי[515] ולפריטים הנהנים מחיסיון עיתונאי.[516]

נראה כי הדרישות הצורניות מהצווים הממוקדים מזעריות. על הצו לפרט את סוגו (צו יירוט ממוקד, צו עיון ממוקד או צו סיוע הדדי) ואת מבקש הצו, וכן לתאר את המטרה המודיעינית (לרבות רשימה מפורטת ככל האפשר של האנשים שיש יסוד להניח שהתקשורת שלהם תיורט, או פירוט של המזהים הטכניים המתייחסים לנתונים המשניים, לפי העניין).[517] מאחר שצווים אלה

511 ראו Daragh Murray, *Regulating Surveillance in the UK*, HCSRC Blog (5.7.2017)

512 IPCO, Advisory Notice 1/2018 on Approval of Warrants, Authorisations, and Notices by Judicial Commissioners (8.3.2018), Sec. G

513 חברי הפרלמנט הבריטי וכן החברים בבתי המחוקקים של ויילס, סקוטלנד, צפון אירלנד וחברי הפרלמנט האירופי.

514 ס' 26 לחוק סמכויות חקירה 2016 (IPA).

515 ס' 27 לחוק סמכויות חקירה 2016 (IPA).

516 ס' 28–29, 264 לחוק סמכויות חקירה 2016 (IPA).

517 ס' 32 לחוק סמכויות חקירה 2016 (IPA).

אינם מוגבלים לצרכים פנימיים של גופי האיסוף והחקירה,[518] לא מפתיע שאין בהם דרישה לפירוט של השיקולים הסטטוטוריים שהשר או נציב שיפוטי הביאם בחשבון.[519]

צווים ממוקדים תקפים למשך שישה חודשים,[520] והם ניתנים להארכה, הטעונה בחינה מחודשת של השר ושל נציב שיפוטי (מנגנון הנעילה הכפולה). צו ממוקד רגיל אפשר להאריך רק בשלושים הימים שלפני פקיעת תוקפו (צו ממוקד דחוף אפשר להאריך בתקופה שבה הוא עומד בתוקף – חמשת ימי העבודה מהיום שניתן).[521]

על השר להבטיח כי בכל צו ממוקד יש בקרות על היקף התפוצה שלו ועל הסדרי השימור שלו.[522] תפוצה של חומר שהושג בצו צריכה להיות מזערית[523]: יש להבטיח כי מספר האנשים הנחשפים אליו, היקף החשיפה, היקף ההעתקה ומספר ההעתקים – כל אלה יהיו מינימליים.[524] החומר שהושג מכוח צו ממוקד

518 ראו למשל ס' 41(3) ו־ס' 42 לחוק סמכויות חקירה 2016 (IPA), העוסקים בהמצאת העתק מן הצו לכל מי שביכולתו לסייע לרשות המיירטת בקשר לצו. סעיף 43 מחייב את מפעילי שירותי דואר או שירותי טלקומוניקציה לסייע בכל דרך למילוי הוראות הצו. הימנעות ביודעין מסיוע כאמור היא עבירה פלילית שבצידה מאסר לתקופה שלא תעלה על 12 חודשים.

519 דוגמת שיקולי מידתיות וצורך, או השיקולים המנויים בסעיף 2 לחוק סמכויות חקירה 2016 (IPA) (ראו חלק 3.3.4.3 **לעיל**).

520 ס' 32 לחוק סמכויות חקירה 2016 (IPA).

521 ס' 33 לחוק סמכויות חקירה 2016 (IPA).

522 ס' 53 לחוק סמכויות חקירה 2016 (IPA).

523 צורך מתעורר, או סביר שיתעורר, אם מתקיימים הקריטריונים לנחיצות שעל השר לשקול, המנויים בס' 20 לחוק סמכויות חקירה 2016. נוסף עליהם, לשם בחינה של התפוצה המינימלית, צורך יכול שיהא גם למטרות הנוגעות למילוי תפקידי טריבונל כוחות החקירה (ראו חלק 3.3.4.9.2 **להלן**) או של הנציב השיפוטי; כשהמידע נדרש לתביעה הפלילית לצורך הבטחת הוגנות ההליך (ס' 53(3)(d) לחוק סמכויות חקירה 2016), או למילוי חובות מכוח חוק המרשם הציבורי (Public Records Act 1958).

524 ס' 53(2) לחוק סמכויות חקירה 2016 (IPA).

ועותקיו יהיו מאובטחים[525] ויובערו כשלא יהיה בהם עוד צורך.[526] נוסף על בקרות אלו, אם שדר תקשורת שייורט מכוח צו ממוקד כולל מידע שנהנה מחיסיון עיתונאי[527] או מחיסיון משפטי,[528] על האדם מושא הצו ליידע בהקדם את נציב סמכויות החקירה (Investigatory Powers Commissioner).

3.3.4.5 השגת נתוני תקשורת – ללא צורך בצו

לפי ההגדרה בחוק סמכויות חקירה (IPA), נתוני תקשורת הם נתונים על ישויות (entity data)[529] או על אירועים (event data)[530] במערכת תקשורת שאינם נתוני תוכן, המוחזקים אצל (או ניתנים להשגה באמצעות) ספק תקשורת, או שהם זמינים ישירות במערכת התקשורת.[531]

רשויות ציבוריות רבות נהנות מהסמכות שמקנה להן חוק סמכויות חקירה (IPA) להשיג נתוני תקשורת לתכליות שונות.[532] התכליות שלשמן מותרת הפעלת

525 ס' 53(4) לחוק סמכויות חקירה 2016 (IPA).

526 ס' 53(5)–(6) לחוק סמכויות חקירה 2016 (IPA). צורך בשימור מוגדר כהגדרת הצורך שלמולו יש לבחון את התפוצה המינימלית המותרת (ס' 53(4) לחוק סמכויות חקירה 2016).

527 ס' 53(7) לחוק סמכויות חקירה 2016 (IPA).

528 ס' 55 לחוק סמכויות חקירה 2016 (IPA). על נציב סמכויות החקירה להחליט אם מידע הנהנה מחיסיון משפטי יבוער, ואם לא – להגביל את אופני השימוש בו ואת שימורו.

529 "נתוני ישות" (entity data) הם נתונים על ישות (אדם או דבר), על קשר בין ישות לישות אחרת או למערכת תקשורת, הכוללים נתונים המזהים או מתארים את הישות, ושאינם בגדר נתוני אירוע (event data). ראו ס' 261(3) לחוק סמכויות חקירה 2016 (IPA).

530 "נתוני אירוע" מתארים אירוע, לרבות באמצעות פרטים על מיקומו, במערכת תקשורת שבו ישות אחת או יותר השתתפו בפעילות מסוימת במועד מסוים. ראו ס' 261(4) לחוק סמכויות חקירה 2016 (IPA). בתזכיר תקנות שימור והשגת נתונים ובכללי ההתנהגות המוצעים בעניין תקשורת נתונים שהופצו להערות הציבור, צוין כי העמדה הפרשנית של ממשלת בריטניה לנתוני אירוע היא כנתונים הכוללים נתוני תעבורה (ראו ה"ש 301 **לעיל** בפרק זה) ונתוני מיקום (ראו ה"ש 302 **לעיל** בפרק זה) כהגדרתם בדירקטיבת הפרטיות האלקטרונית. לתזכיר ראו ה"ש 777 **להלן** בפרק זה.

531 ס' 261(5) לחוק סמכויות חקירה 2016 (IPA).

532 התוספת הרביעית לחוק סמכויות חקירה 2016 (IPA) מפרטת את הגופים שלהם מותר להשיג נתוני תקשורת, ואת דרגותיהם של בעלי התפקידים המוסמכים להורות

הסמכות הן אינטרסים של ביטחון לאומי, גילוי או מניעה של פשע או מניעת הפרות סדר, שמירה על רווחתה הכלכלית של הממלכה (כשאינטרס זה עולה בקנה אחד עם אינטרס של שמירה על ביטחון לאומי), שלום הציבור, בריאות העם, גביית מיסים והיטלים, מניעת מוות או נזקי גוף, סיוע בחקירה של הפרות צדק נטענות, זיהוי מתים ומטרות שקשורות בהסדרת שירותים פיננסיים, שוקי הון והבטחת היציבות הפיננסית.[533]

פקיד בכיר ברשות מסוימת שהוסמך לכך[534] רשאי להסמיך נושא משרה ברשות לפעול כדי להשיג נתוני תקשורת שנדרשים לאחת או יותר מן התכליות שפורטו לעיל בחקירה או במבצע מסוימים.[535] לפי אומדן חלקי מחודש מרץ 2017, המתבסס על נתונים שהועברו מרשויות בריטניה בעקבות בקשות מכוח חוק חופש המידע, בבריטניה יש יותר מ־16,318 נושאי משרה בדרגה זו (או גבוהה ממנה).[536] את נתוני התקשורת אפשר להשיג על ידי פנייה ישירה לכל אדם או ספק נתוני תקשורת, על ידי בבקשה לקבלם מכל מי שיכול להחזיק בהם או

על השגת נתוני תקשורת: גופי המשטרה בבריטניה (משטרת לונדון, שירות המשטרה של סקוטלנד, משטרת צפון אירלנד, משטרת התחבורה, משטרת הצי, המשטרה הצבאית ומשטרת חיל האוויר), סוכנויות הביון הבריטיות (MI6, MI5, ו־GCHQ), משרד ההגנה, גורמים מסוימים במשרד הבריאות, גורמי הגירה במשרד הפנים, גורמי מודיעין במינהלת העבריינים הלאומית (National Offender Management Services), רשויות המס (HMRC), הסוכנות הלאומית לפלילים (NCA), גורמי חקירת הונאות במחלקת הרווחה, משמר החוף, חוקרי תאונות אוויר, רכבת וים במשרד התחבורה, סוכנות התקנים למזון, נציבות ההימורים, המפקח על המידע (ICO), הרשות להצלה ועוד. יוער כי התוספת הרביעית מגדירה לכל גוף המנוי בה את התכליות (מתוך אלה המנויות בסעיף 61(7) של חוק סמכויות חקירה 2016) שמכוחן הוא רשאי להשיג נתוני תקשורת.

533 ס' 61(7) לחוק סמכויות חקירה 2016 (IPA).

534 ראו ס' 70 לחוק סמכויות חקירה 2016 (IPA), וכן Schedule 4. "Designated Senior Officer" (להלן: פקיד בכיר מוסמך). התוספת הרביעית מפרטת את הדרגה בכל רשות של נושאי המשרה שהם פקידים בכירים מוסמכים. מי שדרגתו גבוהה מהדרגה המינימלית המתוארת בתוספת, ייחשב גם לפקיד בכיר מוסמך.

535 ס' 61(1)–(2) לחוק סמכויות חקירה 2016 (IPA).

536 Claire Broadley, *Now 16,318 + British Cops, Suits & Spooks Can See Every Website You Visit*, whoiswhostingthis.com (25.3.2017)

באמצעות מתן הוראה לספק תקשורת להעבירם,[537] אך לא על דרך של יירוט תקשורת בזמן אמת.[538]

בקשה לאישור להשיג נתוני תקשורת יש להגיש בכתב.[539] האישור עצמו כפוף לדרישות צורניות מסוימות, ובכללן פירוט הגורם המאשר, הנסיבות המקימות את אחת התכליות המוגדרות, את אופן השגת המידע המאושר, את המידע או את תיאור המידע המבוקש ואת מי שניתן להם להפיץ מידע זה.[540] כשמבוקש אישור להורות לספק תקשורת להעביר נתונים, יש לציין אותו ואת אופי הדרישות המוחלות עליו. ההוראה עצמה תימסר בכתב ותכלול פירוט מינימלי של תפקידו או דרגתו של מוסר ההוראה, את הדרישות בהוראה ואת פרטי ספק התקשורת שעליה היא חלה.[541] אישורים והוראות כאמור תקפים חודש מהיום שניתנו בו, ואפשר להאריך אותם כל עוד הם בתוקף.[542]

בעלי תפקידים בכירים ברשויות מקומיות (local authorities)[543] רשאים, בדומה לפקיד בכיר מוסמך,[544] לאשר השגה של נתוני תקשורת, אך רק לתכליות של מניעת פשיעה או הפרות סדר. אישורים שניתנו ברשות המקומית כפופים לביקורת שיפוטית של ערכאה נמוכה.[545] סמכותם של פקידים בכירים מוסמכים מטעם רשות מקומית מותנית בהסכם שיתוף פעולה בינה ובין רשות ציבורית[546]

537 ס' 61(4) לחוק סמכויות חקירה 2016 (IPA).

538 ס' 61(6)(a) לחוק סמכויות חקירה 2016 (IPA).

539 ס' 64(4) לחוק סמכויות חקירה 2016 (IPA).

540 ס' 64(1) לחוק סמכויות חקירה 2016 (IPA).

541 ס' 64(3) לחוק סמכויות חקירה 2016 (IPA).

542 ס' 65 לחוק סמכויות חקירה 2016 (IPA).

543 "רשות מקומית" לצורך זה היא מועצה מחוזית, מועצה של אחד מרובעי העיר לונדון ועוד גופים המנויים בסעיף 86(2) לחוק סמכויות חקירה 2016 (IPA).

544 ס' 73 לחוק סמכויות חקירה 2016 (IPA).

545 ס' 75 לחוק סמכויות חקירה 2016 (IPA). ערכאה נמוכה – justice of the peace באנגליה ויילס, שריף בסקוטלנד ושופט מחוזי בצפון אירלנד.

546 המנויה בתוספת הרביעית לחוק סמכויות חקירה 2016 (IPA).

שמסמיך את הפקיד הבכיר המקומי להורות לבעלי תפקידים ברשות הציבורית להשיג נתוני תקשורת.[547]

הסמכות לאשר השגת נתוני תקשורת אינה בלתי מוגבלת, וכדי למנוע את ניצולה לרעה, פקיד בכיר מוסמך אינו רשאי לתת אישורים שנוגעים לחקירה או למבצע שבהם הוא מעורב כחוקר, חוץ מבנסיבות חריגות.[548]

אישור על השגת נתוני תקשורת על פעילות משתמשים ברשת – רשומות חיבור לאינטרנט (ICR – Internet Connection Record) – כפוף לסייגים נוספים. רשומות אלה הן נתוני תקשורת שכוללים נתונים שיצר או עיבד ספק שירות התקשורת (ה־ISP) תוך כדי מתן השירות.[549] הנתונים הללו כוללים נתוני זמן ומיקום, נתונים על מכשור הקצה של המשתמש, מספר מזהה של המשתמש (לרבות מספר טלפון סלולרי), כתובות IP וכתובות domain.

לא כל פקיד בכיר מוסמך רשאי לאשר השגה של נתוני ICR – סמכות זו אינה מסורה לבעלי תפקידים בכירים ברשויות מקומיות, אלא לפקידים בכירים מוסמכים בלבד, לפי המפורט בתוספת הרביעית לחוק. בכפוף להרשאות שבתוספת הרביעית, פקיד בכיר מוסמך רשאי לאשר השגה של נתוני ICR אם לשם הגשמה של אחת התכליות המוגדרות[550] (1) נדרשים נתונים המזהים משתמש או את מכשור הקצה שבו נעשה שימוש, כשמועד הפעילות המקוונת ידוע; או (2) שנתוני ה־ICR דרושים כדי לזהות את שירות התקשורת או האינטרנט שנעשה בהם שימוש ואת אופן השימוש בהם[551] בידי אדם או מכשור קצה שזהותם ידועה, או כשפעילותם המקוונת של אדם או מכשור קצה שזהותם ידועה כרוכה בהשגת

547 ס' 74, 78–80 לחוק סמכויות חקירה 2016 (IPA).

548 דוגמת איום מיידי על חיי אדם, מצב חירום, צורך בחשאיות, התקיימותו של חלון זמנים להשגת מידע שהוא צר מכדי לפנות לבעל סמכות מאשר אחר, או היעדרו של פקיד מוסמך אחר ברשות, מפאת גודלה. ראו ס' 63(3) לחוק סמכויות חקירה 2016 (IPA).

549 ס' 62(7) לחוק סמכויות חקירה 2016 (IPA).

550 ראו בטקסט המפנה לה"ש 533 **לעיל** בפרק זה.

551 השגת נתוני ICR המלמדים על אופן השימוש באינטרנט אינה מותרת כשמדובר בעבירות פליליות שאינן מסווגות כפשע (serious crime).

גישה או בהרצה של קובץ מחשב או תוכנית מחשב שעיקרה הנגשה או השגה של חומר שהחזקתו פלילית.[552]

אישור להשגה של נתוני תקשורת שמטרתו לזהות או לאשרר מקור מידע עיתונאי יהיה תקף רק בכפוף לאישורו של נציב שיפוטי (אלא אם הוא נדרש בשל איום מיידי על חיי אדם).[553]

3.3.4.6 הודעה על שימורם של נתוני תקשורת (retention notice)

השר רשאי להורות באמצעות הודעה (notice) לספק תקשורת לשמור נתוני תקשורת אם לדעתו הדבר נחוץ ומידתי להשגת אחת התכליות המנויות בסעיף 61(7) לחוק,[554] ואם נציב שיפוטי אישר את ההחלטה.[555]

הודעה על שימור נתונים אינה יכולה לכלול דרישה לשימור נתונים של צד שלישי – נתוני תקשורת של צדדים שלישיים שנגישים לספק התקשורת וניתנים להפרדה לוגית מנתוני התקשורת שלו. כך למשל אי־אפשר להורות לספק תקשורת סלולרי לשמר נתוני תקשורת של אפליקציות המצויות במכשירי הקצה של המשתמשים שלו, גם אם מבחינה טכנית הספק מסוגל להפריד את נתוני התקשורת של האפליקציות מתעבורת האינטרנט הכללית של המשתמש.[556]

לפני ששר מורה על שימור נתוני תקשורת, עליו להביא בחשבון את התועלת, את מספר המשתמשים המשוער המוקף בהודעה, את האפשרות הטכנית לקיים את הוראותיה ואת העלות שבצידה. כמו כן, טרם מתן ההודעה עליו לנקוט צעדים סבירים כדי להתייעץ עם ספק התקשורת שאליו ההודעה מתייחסת.[557]

552 ס' 62(2)–(5) לחוק סמכויות חקירה 2016 (IPA).

553 ס' 77 לחוק סמכויות חקירה 2016 (IPA).

554 ראו בטקסט המפנה לה"ש 533 **לעיל** בפרק זה.

555 ס' 87(1) לחוק סמכויות חקירה 2016 (IPA).

556 ס' 87 (4) לחוק סמכויות חקירה 2016 (IPA).

557 ס' 88 (1) לחוק סמכויות חקירה 2016 (IPA).

ההודעה על שימור של נתוני תקשורת כפופה למנגנון הנעילה הכפולה, ונוסף על אישור השר, דרושה ביקורת של נציב שיפוטי.[558] על הנציב לבחון את נחיצותה ואת מידתיותה של ההודעה[559] ולהפעיל את אותם העקרונות שבית משפט מפעיל כשהוא בוחן אותה, וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[560] החלטתו של נציב שיפוטי שלא לאשר הודעת שימור נתוני תקשורת תנומק בכתב.[561] יוער כי נכון למועד כתיבת שורות אלה ההוראה בדבר מנגנון הנעילה הכפולה בכל הנוגע להודעה על שימורם של נתוני תקשורת טרם הוחלה בחוק סמכויות חקירה 2016 (IPA), ועד שהשר יכניס אותה לתוקף באמצעות תקינה, הודעות השימור כפופות אך ורק לאישורו.[562]

ספק נתוני תקשורת רשאי לפנות לשר בבקשה לבחון מחדש הודעה, ובמהלכה של הבחינה הוא אינו חייב למלא את הוראותיה. על השר להתייעץ עם גורמים טכניים בדבר ההיבטים הטכניים והכלכליים של הודעת השימור; ועם נציב שיפוטי בדבר המידתיות שלה. בבואם לקבל החלטה בנושא, על הגורמים הטכניים והנציב השיפוטי לאפשר לספק התקשורת ולשר להביא ראיות או להציג מצגים מתאימים. החלטותיהם ידווחו לספק התקשורת ולשר, ועם קבלתן השר רשאי לשנות, לאיין או להשאיר בתוקף את ההודעה על שימורם של נתוני התקשורת (החלטה לשנות או להשאיר את ההודעה בתוקפה טעונה אישור של נציב סמכויות החקירה).[563]

558 ס' 89 לחוק סמכויות חקירה 2016 (IPA).

559 לפי הקריטריונים לנחיצות שעל השר לשקול, המנויים בסעיף 20 לחוק סמכויות חקירה 2016 (IPA).

560 מכוח סעיף 2 לחוק סמכויות חקירה 2016 (IPA) (ראו בחלק 3.3.4.3 **לעיל**).

561 ס' 89(4)–(5) לחוק סמכויות חקירה 2016 (IPA). כשהנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (investigatory powers commissioner), מבקש הצו רשאי לערער בפני נציב סמכויות החקירה על הדחייה.

562 ראו (Commencement No. 1 and Transitional Provisions) The Investigatory Powers Act 2016 Regulations 2016, S.2(c), המורה על כניסתו לתוקף של סעיף 87 לחוק סמכויות חקירה 2016 (IPA), המסמיך את השר להורות לספק תקשורת על שימור נתונים, פרט לס"ק 87(1)(b), המתנה את סמכותו של השר להורות כן באישורו של נציב שיפוטי.

563 ס' 90 לחוק סמכויות חקירה 2016 (IPA).

שימור של נתוני תקשורת לפי הודעת שימור לא יעלה על תקופה של 12 חודשים ממועד השדר המסוים שאליו הבקשה מתייחסת או מהמועד שבו הפסיק היעד המודיעיני את ההתקשרות עם ספק התקשורת (אם הבקשה מתייחסת לישות מסוימת), ובכל מקרה אחר – 12 חודשים מהמועד שבו התקבלו נתוני התקשורת לראשונה אצל הספק.[564]

ההודעה על שימורם של נתוני תקשורת צריכה לכלול את פרטי הספק או מפעיל השירות, את הנתונים ששימורם מבוקש, את תקופת השימור וכל דרישה אחרת או הגבלה אחרת על שימור הנתונים (לרבות הוראות הנוגעות לאחסון החומר שיקל את העברתו לרשות).[565] על ספק התקשורת לוודא כי נתוני תקשורת שנשמרים מכוח הודעה על שימור נתוני תקשורת יהיו מאובטחים ושלמים, להגביל את הרשאות הגישה אליהם ולהגן עליהם מפני השמדה מכוונת או מקרית.[566]

3.3.4.7 צווי סייבר: התערבות ממוקדת בציוד תקשורת (equipment interference)

חוק סמכויות חקירה (IPA) כולל שני סוגים של צווי התערבות בציוד (להלן: צווי סייבר) – הראשון, **צו התערבות ממוקדת בציוד** (targeted equipment interference warrant), והשני **צו עיון ממוקד** (targeted examination notice).[567] התערבות בציוד[568] פירושה פצחנות (hacking) או פעילות סייבר לצורך השגת מידע שאי־אפשר ליירטו באופן פסיבי. יש להבהיר כי אין בצווי סייבר כדי להסמיך פעילות שלא נועדה להשגת מידע (ראו להלן), ולכן אין בהם כדי לאשר לוחמת סייבר, שנועדה למשל לשבש תשתיות מחשוב. יש הסוברים

564 ס' 87(3) לחוק סמכויות חקירה 2016 (IPA).

565 ס' 87(8) לחוק סמכויות חקירה 2016 (IPA).

566 ס' 92 לחוק סמכויות חקירה 2016 (IPA).

567 ס' 99(1) לחוק סמכויות חקירה 2016 (IPA). זהו צו השונה מהצו הנידון בחלק 3.3.4.4 **לעיל**.

568 "ציוד" הוא כל מכשיר שמפיק גלים אלקטרומגנטיים, גלים אקוסטיים או שידורים אחרים, או כל מכשיר שאפשר להשתמש בו בקשר לציוד כזה (ס' 135 לחוק סמכויות חקירה 2016).

כי הגדרת "ציוד" בחוק רחבה דיה כדי לכלול גם תקשורת בין רכיבי "האינטרנט של הדברים".[569]

החוק מורה לסוכנויות הביון שלא לעסוק בפעילות שאפשר לאשרהּ בצו התערבות ממוקדת בציוד או בצו סייבר כללי (bulk equipment interference warrant)[570] שלא מכוח צו כאמור, אם לפעילות מודיעינית זו, ליעד המודיעין שלה או לתקשורת שנועדה ליירוט יש זיקה טריטוריאלית לאיים הבריטיים,[571] ויש בהם כדי להיות עבירה על חוק המחשבים.[572] מכלל לאו שומעים הן, וניתן להניח שפעילות סייבר שאינה בעלת זיקה טריטוריאלית כזאת אינה טעונה צו.[573]

צו התערבות ממוקדת בציוד מורה למושאו או מסמיך אותו להתערב בציוד כדי להשיג תקשורת,[574] נתוני ציוד או כל מידע אחר.[575] נוסף על ההסמכה לפעול כדי להתערב בציוד, על צו כאמור להסמיך את מושאו גם להשיג את המידע המבוקש בהתערבות זו[576] (השגת מידע יכולה להתבצע בהאזנה, בניטור או בהקלטה של

569 Lornea M. Woods, *Draft Investigatory Powers Bill,* 2 Eur. Data Prot. L. Rev. 103 (2016)

570 ראו חלק 3.3.4.8.3 **להלן**.

571 לתנאים המקימים זיקה טריטוריאלית, ראו ס' 13(2) לחוק סמכויות חקירה 2016 (IPA).

572 ראו ס' 13(1)(a) לחוק סמכויות חקירה 2016 (IPA), המפנה לעבירות המנויות בחוק המחשבים הבריטי (חדירה לא מורשית למחשבים, חדירה לא מורשית למחשבים בכוונה לעבור עבירות נוספות, מעשים שנעשו בכוונה לסכן, או ברשלנות שיש בה לסכן, פעילות תקינה של מחשבים ומעשים שלא באישור שיש בהם כדי להסב נזק ניכר), ראו Computer Misuse Act 1990, c. 18 (Eng.), Sec. 1–3A.

573 למרות שלפי ס"ק 13(3) לחוק סמכויות חקירה 2016 (IPA) במקרים בהם אין זיקה כאמור, אין בהוראות החוק ביחס לצווי סייבר כדי למנוע מראש שירות ביון מלבקש צו.

574 "תקשורת", לצורך סעיף זה, היא כל דבר המורכב מדיבור, מוסיקה, קולות, דימויים ויזואליים או נתונים, וכן אותות המשמשים לתעבורה בין אדם לחברו, אדם לחפץ, או בין שני חפצים להפעלה או לשליטה בחפצים (ס' 135 לחוק סמכויות חקירה 2016).

575 ס' 99(2) לחוק סמכויות חקירה 2016 (IPA).

576 ס' 99(3)(a) לחוק סמכויות חקירה 2016 (IPA).

תקשורת), וניתן להסמיכו גם להעביר נתונים אלו לצדדים שלישיים.[577] צו סייבר כללי אינו מסמיך את מושאו לנקוט פעולות הטעונות צו יירוט,[578] אלא ביחס לתקשורת מאוחסנת.[579]

צו סייבר יכול להיות בנוגע לציוד השייך לאדם מסוים, לארגון מסוים או לקבוצת אנשים שחולקים מטרה משותפת ועוסקים בפעילות מסוימת, לציוד במיקום מסוים, לציוד שמצוי בכמה מקומות (לצורך חקירה או מבצע מסוימים) או לציוד ששימש, או ישמש, לפעילות מסוימת.[580]

צו עיון ממוקד מסמיך את מושאו לבחור מידע מוגן[581] שהושג מכוח צו סייבר כללי (bulk equipment interference warrant), למטרות עיון בו.[582] צו כאמור יכול שיהיה בנוגע לאדם מסוים, לארגון מסוים או לקבוצת אנשים שחולקים מטרה משותפת ועוסקים בפעילות מסוימות, או ליותר מארגון, מאדם או מחצרים יחידים (לצורך חקירה או מבצע מסוימים).[583] החוק מחייב ספקי תקשורת ליישם את הוראות צווי הסייבר, אם הוגשו להם כאלה, ולנקוט את כל האמצעים הסבירים לשם כך.[584] לבקשה של ראש סוכנות ביון,[585] רשאי השר לאשר צו סייבר

577 ס' 99(3)(b) לחוק סמכויות חקירה 2016 (IPA).

578 היינו, פעולות המהוות יירוט אסור, כהגדרתו בס' 3(a) לחוק סמכויות חקירה 2016 (IPA). ראו חלק 3.3.4.2 **לעיל**.

579 "תקשורת מאוחסנת" משמעה נתוני תקשורת, לפני שידורם או אחריו, המאוחסנים במערכת תקשורת (ס' 99(8) לחוק סמכויות חקירה 2016 (IPA).

580 ס' 101(1) לחוק סמכויות חקירה 2016 (IPA).

581 "מידע מוגן", בהתייחס לצו בדיקה ממוקד (מכוח פרק 5 לחוק סמכויות חקירה 2016 (IPA)), הוא כל חומר שהושג מכוח צו יירוט כללי, לבד מנתוני ציוד ומידע שאינו מידע פרטי (ס' 99(9) לחוק סמכויות חקירה 2016 (IPA)). ראו **לעיל** בפרק זה ה"ש 493.

582 ס' 99(6) לחוק סמכויות חקירה 2016 (IPA).

583 ס' 101(2) לחוק סמכויות חקירה 2016 (IPA).

584 ס' 128 לחוק סמכויות חקירה 2016 (IPA).

585 ראש אחת משלוש סוכנויות הביון הבריטיות: מנהל מטה התקשורת הממשלתי (GCHQ), ראש סוכנות הביון הבריטית (Secret Intelligence Service, המוכרת גם כ־SIS או כ־MI6) והמנהל הכללי של השירות החשאי (Security Service, או MI5). ראו ס' 263 לחוק סמכויות חקירה 2016 (IPA).

אם לדעתו הצו נדרש לתכליות הנוגעות לאינטרסים של ביטחון לאומי, מניעה או זיהוי של פשיעה או לאינטרסים כלכליים של הממלכה המאוחדת (אם אלה רלוונטיים לאינטרסים של ביטחון לאומי),[586] והוא נחוץ ומידתי ביחס למבוקש בו.[587] בכל הנוגע למתן צווי סייבר ביחס לסקוטלנד, קיימת הפרדה בין סמכויות טריטוריאליות.[588]

נוסף על זה, מתן צו התערבות ממוקדת בציוד יינתן בתנאי שהשר סבור שיש די בקרות סטטוטוריות על אבטחת המידע ותפוצתו.[589] כשהצו נועד אך ורק למנוע פשע או לזהות אותו, השר אינו רשאי לאשרו.[590] הסמכות לאשר צווי התערבות ממוקדת בציוד לתכליות אלו מסורה לראשי גופי השיטור והאכיפה השונים בבריטניה, לבקשת קצין מוסמך[591] ובהתקיים תנאים דומים של צורך, מידתיות ובקרות סטטוטוריות, בכפוף לביקורת שיפוטית,[592] ובנוגע לאחדים מגופי החקירה – בתנאי שמתקיימת זיקה טריטוריאלית לאיים הבריטיים.[593] קצין מוסמך רשאי לאשר צו התערבות ממוקדת לתכלית של הצלת חיי אדם או מניעת נזקי גוף, בתנאים דומים.[594]

צו עיון ממוקד יינתן בתנאי שהשר בוחן, בנסיבות הרלוונטיות, אם חרף מגבלות סטטוטוריות מסוימות, הצו הכרחי או עשוי להיות הכרחי לאישור עיון סלקטיבי במידע מוגן על אנשים פרטיים בתחומי בריטניה.[595]

586 ס' 102(5) לחוק סמכויות חקירה 2016 (IPA).

587 ס' 102(1)(a)–(b), 102(3)(a)–(b) לחוק סמכויות חקירה 2016 (IPA).

588 ס' 103, 102(2)(b), 102(4) לחוק סמכויות חקירה 2016 (IPA).

589 ראו ס' 129–130 לחוק סמכויות חקירה 2016 (IPA).

590 ראו ס' 102(2) לחוק סמכויות חקירה 2016 (IPA).

591 גופי השיטור והאכיפה ודרגותיהם של הקצינים המוסמכים מפורטים בתוספת השישית לחוק סמכויות חקירה 2016 (IPA).

592 ס' 106 לחוק סמכויות חקירה 2016 (IPA).

593 ס' 107 לחוק סמכויות חקירה 2016 (IPA), זיקה כהגדרתה שם.

594 ס' 106(3) לחוק סמכויות חקירה 2016 (IPA).

595 ראו האיסור בס' 193לחוק סמכויות חקירה 2016 (IPA), חלק 3.3.4.8.3 **להלן**.

ההחלטה של השר, ראש גוף השיטור והאכיפה או הקצין המוסמך לאשר צו סייבר כפופה למנגנון הנעילה הכפולה, ומכאן שגם לאישורו של נציב שיפוטי,[596] פרט למקרים שבהם מי שמאשר סבור שהצו דחוף.[597] במקרים דחופים ידווח השר לנציב השיפוטי לאחר מעשה, והוא יחליט (לכל המאוחר בתוך שלושה ימי עבודה מיום הוצאת הצו הדחוף) אם לאשרו בדיעבד.[598] צו סייבר דחוף יעמוד בתוקפו חמישה ימים.[599]

בהחלטתו לאשר צו התערבות ממוקדת בציוד, על הנציב השיפוטי לבחון את נחיצותו ואת מידתיותו,[600] ולהפעיל את אותם העקרונות שהיה מפעיל בית משפט בבואו לבחון את הצו, וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[601] החלטתו של נציב שיפוטי שלא לאשר התערבות ממוקדת תנומק בכתב.[602]

צווי סייבר שמטרתם ליירט תקשורת של מחוקקים[603] טעונים אישור מאת ראש הממשלה[604] (צווים שאושרו לתכליות של אכיפת חוק ומניעת פשע טעונים בנסיבות אלו גם אישור מאת השר). כמו כן יש הוראות מיוחדות בנוגע לצווים

596 ס' 109 לחוק סמכויות חקירה 2016 (IPA).

597 ס' 102(1)(d), 102(3)(d), 106(1)(d), 106(3)(d) לחוק סמכויות חקירה 2016 (IPA).

598 ס' 109 לחוק סמכויות חקירה 2016 (IPA).

599 ס' 116(2) לחוק סמכויות חקירה 2016 (IPA).

600 ס' 108 לחוק סמכויות חקירה 2016 (IPA).

601 מכוח ס' 2 לחוק סמכויות חקירה 2016 (IPA) (ראו חלק 3.3.4.3 **לעיל**).

602 ס' 106(4) לחוק סמכויות חקירה 2016 (IPA). כשהנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (Investigatory Powers Commissioner), מבקש הצו רשאי לערער בפני נציב סמכויות החקירה על הדחייה.

603 חברי הפרלמנט הבריטי וכן חברי בתי המחוקקים של ויילס, סקוטלנד, צפון אירלנד וחברי הפרלמנט האירופי.

604 ס' 111 לחוק סמכויות חקירה 2016 (IPA).

ממוקדים הקשורים לפריטי מידע הנהנים מחיסיון משפטי[605] ולפריטים הנהנים מחיסיון עיתונאי.[606]

הדרישות הצורניות מצווי סייבר מזעריות: הצו נדרש לתאר את סיווגו ואת פרטיו של מי שאישר אותו, וכן לתאר את המטרה המודיעינית.[607] צווי סייבר תקפים למשך שישה חודשים,[608] וניתנים להארכה לאחר בחינה מחודשת של הצו בידי מי שאישר אותו לראשונה (לפי סוג הצו שניתן) ובידי נציב שיפוטי (מנגנון הנעילה הכפולה). צו סייבר רגיל אפשר להאריך רק בשלושים הימים שלפני פקיעת תוקפו (צו סייבר דחוף אפשר להאריך בתקופה שבה הוא עומד בתוקף – חמשת ימי העבודה מהיום שניתן).[609]

על השר להבטיח כי בכל צו סייבר יש בקרות על היקף התפוצה שלו ועל הסדרי השימור שלו.[610] תפוצה של חומר שהושג בצו צריכה להיות מזערית[611]: יש להבטיח כי מספר האנשים הנחשפים אליו, היקף החשיפה, היקף ההעתקה ומספר ההעתקים – כל אלה יהיו מינימליים.[612] החומר שהושג מכוח צו סייבר ועותקיו יהיו מאובטחים[613] ויבוערו כשלא יהיה בהם צורך עוד.[614] נוסף על בקרות אלו, אם שדר תקשורת שיירט מכוח צו ממוקד כולל מידע הנהנה מחיסיון

605 ס' 112 לחוק סמכויות חקירה 2016 (IPA).

606 ס' 113–114, 264 לחוק סמכויות חקירה 2016 (IPA).

607 ס' 115 לחוק סמכויות חקירה 2016 (IPA).

608 ס' 116 לחוק סמכויות חקירה 2016 (IPA).

609 ס' 117 לחוק סמכויות חקירה 2016 (IPA).

610 ס' 129 לחוק סמכויות חקירה 2016 (IPA).

611 צורך מתעורר, או סביר שיתעורר, אם קיימים הקריטריונים לנחיצות הרלוונטיים לסיווגו של צו הסייבר הנידון. נוסף עליהם, לשם בחינה של התפוצה המינימלית, צורך יכול שיהא גם למטרות הנוגעות למילוי תפקידי טריבונל סמכויות החקירה (ראו חלק 3.3.4.9.2 **להלן**) או של נציב השיפוטי; כשהמידע נדרש בהליכים משפטיים או לצורך מילוי כל תפקיד של אדם לפי דין (ס' 129(3) לחוק סמכויות חקירה 2016).

612 ס' 129(2) לחוק סמכויות חקירה 2016 (IPA).

613 ס' 129(4) לחוק סמכויות חקירה 2016 (IPA).

614 ס' 129(6) לחוק סמכויות חקירה 2016 (IPA).

עיתונאי או מחיסיון משפטי, על האדם מושא הצו ליידע בהקדם את נציב סמכויות החקירה.[615]

3.3.4.8 צווי איסוף כלליים (bulk warrants)

בדוח מיוחד מחודש מרץ 2015 ציינה ועדת המודיעין והביטחון הפרלמנטרית כי חבריה הופתעו לגלות שסוכנות התקשורת הממשלתית (GCHQ) סבורה כי במסגרת החומר המופק מאיסוף גורף, לנתונים הנלווים לנתוני התוכן – ה־metadata – ערך רב מזה של נתוני התוכן עצמם.[616] הערה זו חשובה לסוגיה הכללית של ההקלות הניתנות בדינים השונים המסדירים מעקב אחר נתוני תקשורת לעומת מעקב אחר נתוני תוכן. בהקשר הבריטי הדבר מלמד על החשיבות המיוחסת לצווי האיסוף הכלליים, שיתוארו להלן, ועל האופן שבו מופק מודיעין מתוצרי האיסוף.

חוק סמכויות חקירה 2016 (IPA) מאפשר להוציא צווי איסוף כלליים, שמכוחם אפשר ליירט מידע רחב היקף שאינו מתייחס למטרות ממוקדות או ליעדי מודיעין ספציפיים, לתופסו או להחזיק בו. ככלל, הצווים מאפשרים איסוף גורף רחב היקף מסוגים שונים, אך מגבילים את העיון בחומר המודיעיני שהושג לפי קריטריונים של רגישות המידע או קריטריונים טריטוריאליים[617] (עיון כאמור נעשה מכוח צו עיון ממוקד, ראו בחלק 3.3.4.4 לעיל). התכליות שלאורן אפשר להוציא צו איסוף כללי מצויות ברשימות חשאיות שמנהלים ראשי שירותי הביון והכפופות לביקורות עיתיות של ועדת המודיעין הפרלמנטרית, של השר ושל ראש הממשלה.

הסמכויות לאיסוף גורף ורחב היקף הן מן החידושים המצויים בחוק זכו לביקורת ציבורית רבה, בייחוד על רקע הדיון הער שהחל בעקבות פרשת סנודן. כבר בשלבי החקיקה של חוק סמכויות חקירה 2016 (IPA) קבע הדַוָח המיוחד

615 ס' 129(8) לחוק סמכויות חקירה 2016 (IPA).

616 Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* (12.3.2015)

617 ניסוחן של מגבלות טריטוריאליות על עיון בחומר שנאסף מכוח צווי איסוף כלליים הוא הכרחי: לפי ה־Guardian, המידע שאספה סוכנות התקשורת הממשלתית (GCHQ) באמצעות יירוט תקשורת בין־לאומית הכיל כ־85% מתעבורת התקשורת הבריטית. Nick Davies, *MI5 Feared GCHQ Went 'Too Far' Over Phone and Internet Monitoring*, The Guardian (22.6.2013)

של האומות המאוחדות לנושא פרטיות כי סמכויות אלה אינן מידתיות וקרא להוצאתן מנוסח החוק.[618]

3.3.4.8.1. צוו יירוט כללי (bulk interception warrants)

צווי יירוט כלליים חלים על יירוט גורף של תקשורת חו"ל ושל נתונים משניים[619] הקשורים בה. תקשורת חו"ל מוגדרת כתקשורת שאחד מהצדדים המקבלים אותה או משדרים אותה הוא מחוץ לאיים הבריטיים.[620] צו יירוט כללי יורה למושאו ליירט תקשורת כאמור בזמן אמת, למצות מתוכה נתונים משניים, לבחור לצורך העיון נתוני תוכן או נתונים משניים שהוגשו מכוח צו יירוט כללי או להעביר חומר שהוגש מכוח צו יירוט כללי לצד שלישי כלשהו.[621]

השר רשאי, לבקשה של ראש סוכנות ביון, להוציא צו יירוט כללי בתנאי שמטרתו העיקרית ליירט תקשורת חו"ל או להשיג נתונים משניים מתקשורת זו, ואם השר סבור שהצו נחוץ לתכליות של ביטחון לאומי, מניעת פשע או לאינטרסים כלכליים של הממלכה המאוחדת (אם אלה רלוונטיים לאינטרסים של ביטחון לאומי), שהצו מידתי ביחס למבוקש בו, וכי הוא דרוש לתכליות המבצעיות[622] המפורטות בו.[623] על השר לבחון אם רמת הבקרות הסטטוטוריות שבצו מספקת[624] ולהביא בחשבון שאולי יהיה צורך בסיוע מספק תקשורת שאינו בבריטניה.[625]

618 ראו פסקה 39 לדיווח השנתי של שנת 2016, Report of the Special Rapporteur on the Right to Privacy, A/HRC/31/64 (24.11.2016)

619 להגדרת נתונים משניים, ראו **לעיל** בפרק זה ה"ש 490.

620 ס' 136(3) לחוק סמכויות חקירה 2016 (IPA).

621 ס' 136(4) לחוק סמכויות חקירה 2016 (IPA).

622 ס' 142()3 לחוק סמכויות חקירה 2016 (IPA).

623 ס' 138(1) לחוק סמכויות חקירה 2016 (IPA).

624 ס' 138(1)(e) לחוק סמכויות חקירה 2016 (IPA), המפנה לבקרות הסטטוטוריות המנויות בסעיפים 150–151.

625 במקרים כאלו על השר להתייעץ עם המפעיל הזר ולהביא בחשבון את ההיתכנות הטכנית של המבוקש בצו, את היתרונות שבצידו, את מספר המשתמשים המשוער המבוקש בצו מאותו מפעיל, את העלויות הכרוכות בצו וכל השפעה אחרת של הצו על המפעיל (ס' 139 לחוק סמכויות חקירה 2016).

החלטתו של השר לתת את הצו כפופה, לפי מנגנון הנעילה הכפולה, לאישורו של נציב שיפוטי. בהחלטתו לאשר צו יירוט כללי, על הנציב השיפוטי לבחון את נחיצותו ואת מידתיותו ביחס למטרות המבצעיות ולתכליות שלאורן השר סבור שהצו נחוץ, ולהפעיל את אותם העקרונות שהיה מפעיל בית משפט בבואו לבחון את הצו, וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[626] החלטה של נציב שיפוטי שלא לאשר צו יירוט כללי תנומק בכתב.[627]

בדומה לצווים שתוארו לעיל, צו יירוט כללי כפוף לדרישות צורניות מזעריות. יש לאזכר בו במפורש שזהו צו יירוט כללי, לציין את ראש סוכנות הביון שאליו הוא מופנה ולתאר את התכליות המבצעיות שבהתקיימן יהיה ניתן לבחור ולבדוק נתוני תוכן או נתונים משניים שהושגו מכוחו. הצו יהיה בתוקף שישה חודשים,[628] והוא ניתן להארכה לאחר שהשר ונציב שיפוטי בחנו אותו מחדש (מנגנון הנעילה הכפולה) בשלושים הימים לפני שפג תוקפו.[629]

התכליות המבצעיות שבצו היירוט הכללי ייבחרו מתוך רשימה סגורה שמנהלים ראשי סוכנויות הביון, הכוללת את התכליות שלדעתם רלוונטיות לצווי יירוט כלליים. אל הרשימה אפשר להוסיף תכלית, בכפוף לאישור השר, בתנאי שרמת הפירוט של התכלית החדשה עולה על רמת הפירוט של תכליות צווי היירוט הכלליים שבלשון החוק.[630] מדי שלושה חודשים על השר להגיש העתק של הרשימה לוועדת המודיעין והביטחון הפרלמנטרית, ועל ראש הממשלה לבחון את הרשימה מדי שנה.[631]

626 ס' 140 (1) לחוק סמכויות חקירה 2016 (IPA).

627 ס' 140(3) לחוק סמכויות חקירה 2016 (IPA). כאשר הנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (Investigatory Powers Commissioner), מבקש הצו רשאי לערער בפני נציב סמכויות החקירה על הדחייה.

628 ס' 143 לחוק סמכויות חקירה 2016 (IPA).

629 ס' 144 לחוק סמכויות חקירה 2016 (IPA).

630 כמפורט בס' 138(1)(b), 138(2) לחוק סמכויות חקירה 2016 (IPA), וראו בטקסט המפנה לה"ש 623 **לעיל** בפרק זה.

631 ס' 142 לחוק סמכויות חקירה 2016 (IPA).

על השר לוודא כי לכל צו יירוט כללי יש בקרות על היקף התפוצה שלו, על הסדרי השימור שלו ועל אופני הגישה אליו (הנעשית בדרך של עיון (examination), הטעונה צו עיון ממוקד).[632] התפוצה של חומר שהושג בצו צריכה להיות מזערית: יש להבטיח כי מספר האנשים הנחשפים לחומר, היקף החשיפה, היקף ההעתקה ומספר ההעתקים יהיו מינימליים.[633] החומר שהושג מכוח צו יירוט כללי, על העתקיו, יאובטח[634] ויבוער לכשיתאיין הצורך בו.[635] יש הגנות נוספות החלות על חומר הנהנה מחיסיון משפטי.[636] ועיתונאי.[637]

מאחר שהמידע הנרכש מכוח צו יירוט כללי אינו ממוקד אלא מבוסס על איסוף גורף, מצא המחוקק הבריטי לנכון להגביל את הגישה לחומר שנאסף. עיון בחומר שנאסף מכוח צו יותר רק בחומר שנבחר לעיון (יש להניח כי באמצעות שאילתה מתאימה) לאור התכליות המבצעיות המנויות בצו,[638] כפי הנדרש ובמידתיות[639] ובתנאי שהקריטריון לבחירה (המזהה של השאילתה) אינו מזהה של אדם המצוי בטריטוריה בריטית, כשמדובר בעיון בתוכן של נתוני תקשורת שלו או תקשורת שיועדה לו.[640]

632 ס' 150(1) לחוק סמכויות חקירה 2016 (IPA). לצו עיון ממוקד, ראו חלק 3.3.4.4 **לעיל**.

633 ס' 150(2) לחוק סמכויות חקירה 2016 (IPA).

634 ס' 150(4) לחוק סמכויות חקירה 2016 (IPA).

635 ס' 150(6) לחוק סמכויות חקירה 2016 (IPA).

636 ס' 153 לחוק סמכויות חקירה 2016 (IPA).

637 ס' 154 לחוק סמכויות חקירה 2016 (IPA).

638 ס' 251(1)(a) לחוק סמכויות חקירה 2016 (IPA).

639 ס' 251(1)(b) לחוק סמכויות חקירה 2016 (IPA).

640 ס' 152 לחוק סמכויות חקירה 2016 (IPA). במקרים שבהם בעבר היה השימוש במזהה של יעד המודיעין מושא השאילתה מותר, ועקב שינוי בנסיבות עבר היעד לאיים הבריטיים או שהתחוור כי הערכה קודמת שהיעד אינו בטריטוריה (ומכוחה הותר עיון בנתוני התקשורת שלו) שגויה – קצין בכיר רשאי לאשר בכתב את המשך השימוש במזהה זה למשך חמישה ימי עבודה נוספים.

3.3.4.8.2. צו תפיסה כללי של נתוני תקשורת (bulk acquisition warrant)

בשונה מהשגה ממוקדת של נתוני תקשורת, שאינה טעונה צו,[641] תפיסה גורפת של נתוני תקשורת (bulk acquisition) טעונה צו תפיסה כללי. שלא כצו יירוט כללי – שמסדיר יירוט גורף וחסר הבחנה של תקשורת, לרבות ובעיקר של נתוני תוכן, באמצעות סוכנויות הביון – צו תפיסה כללי מתייחס לתפיסה גורפת וחסרת הבחנה של נתוני תקשורת[642] המצויים אצל ספק תקשורת או שאינם בחזקתו וביכולתו להשיגם.[643] 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[644] וכן לאשר את העברתם לצדדים שלישיים.[645] החוק מחייב ספקי תקשורת ליישם את הוראות צווי התפיסה הכלליים, אם הוגשו להם כאלה, ולנקוט את כל האמצעים הסבירים לשם כך.[646]

השר, לבקשתו של ראש סוכנות ביון, רשאי להוציא צו תפיסה כללי אם לדעתו הצו נחוץ לתכליות של ביטחון לאומי, מניעת פשע או לאינטרסים הכלכליים של הממלכה המאוחדת (אם אלה רלוונטיים לאינטרסים של ביטחון לאומי), שהצו מידתי ביחס למבוקש בו, וכי הוא דרוש לתכליות המבצעיות[647] המפורטות בצו.[648] עוד על השר לבחון ולוודא שרמת הבקרות הסטטוטוריות בצו מספקת.[649]

641 ראו בחלק 3.3.4.5 **לעיל**.

642 כהגדרתם בס' 261 (5) לחוק סמכויות חקירה 2016 (IPA).

643 ס' 158(6)(a) לחוק סמכויות חקירה 2016 (IPA).

644 ס' 158(6)(b) לחוק סמכויות חקירה 2016 (IPA).

645 ס' 158(6)(c) לחוק סמכויות חקירה 2016 (IPA).

646 ס' 170 לחוק סמכויות חקירה 2016 (IPA).

647 ראו ס' 161()3 לחוק סמכויות חקירה 2016 (IPA).

648 ס' 158(1) לחוק סמכויות חקירה 2016 (IPA).

649 ס' 158(1)(d) לחוק סמכויות חקירה 2016 (IPA), המפנה לבקרות הסטטוטוריות המנויות בסעיף 171.

בדומה לצווים שתוארו לעיל, צו תפיסה כללי כפוף למנגנון הנעילה הכפולה וטעון אישור של נציב שיפוטי.[650] בהחלטתו לאשר צו תפיסה כללי על הנציב השיפוטי לבחון את נחיצותו ואת מידתיותו ביחס למטרות המבצעיות ולתכליות שלאורן השר סבור שהצו נחוץ,[651] ולהפעיל את אותם העקרונות שהיה מפעיל בית משפט בבואו לבחון את הצו, וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[652] החלטת נציב שיפוטי שלא לאשר צו תפיסה כללי תנומק בכתב.[653]

התכליות המבצעיות שבצו התפיסה הכללי ייבחרו – בדומה לתכליות המבצעיות לצורכי צווי יירוט כלליים – מתוך רשימה סגורה שמנהלים ראשי סוכנויות הביון[654] (לכל סוג של צו כללי יש רשימת תכליות מבצעיות נפרדת). אפשר להוסיף תכלית לרשימה באישור השר ובתנאי שרמת הפירוט של התכלית החדשה עולה על רמת הפירוט של תכליות צווי התפיסה הכלליים שבלשון החוק.[655] מדי שלושה חודשים על השר להגיש העתק של הרשימה לוועדת המודיעין והביטחון הפרלמנטרית, ועל ראש הממשלה לבחון את הרשימה מדי שנה.[656]

צו תפיסה כללי יעמוד בתוקפו למשך שישה חודשים,[657] והוא ניתן להארכה לאחר בחינה מחודשת של הצו בידי השר ובידי נציב שיפוטי (כחלק מהמתודולוגיה של הפעלת מנגנון הנעילה הכפולה) במהלך שלושים הימים שלפני פקיעת תוקפו.[658]

650 ס' 158(1)(e) לחוק סמכויות חקירה 2016 (IPA).

651 ס' 159 לחוק סמכויות חקירה 2016 (IPA).

652 ס' 159 (1) לחוק סמכויות חקירה 2016 (IPA).

653 ס' 159(3) לחוק סמכויות חקירה 2016 (IPA). כשהנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (Investigatory Powers Commissioner), מבקש הצו רשאי לערער בפני נציב סמכויות החקירה על הדחייה.

654 ס' 161 לחוק סמכויות חקירה 2016 (IPA).

655 כמפורט ב־ס' 158(1)(a), 158(2) לחוק סמכויות חקירה 2016 (IPA).

656 ס' 161 לחוק סמכויות חקירה 2016 (IPA).

657 ס' 161 לחוק סמכויות חקירה 2016 (IPA).

658 ס' 162 לחוק סמכויות חקירה 2016 (IPA).

על השר לוודא כי לצו תפיסה כללי יש בקרות על היקף התפוצה שלו, על הסדרי השימור שלו ועל אופני הגישה אליו (הנעשית בדרך של עיון).[659] התפוצה של חומר שהושג בצו צריכה להיות מזערית: יש להבטיח כי מספר האנשים הנחשפים לחומר, היקף החשיפה, היקף ההעתקה ומספר ההעתקים יהיו מינימליים.[660] החומר שהושג מכוח צו תפיסה כללי, על העתקיו, יאובטח[661] ויבוער לכשיתאיין הצורך בו.[662]

מאחר שבדומה לצו יירוט כללי, המידע הנרכש מכוח צו תפיסה כללי אינו ממוקד אלא מבוסס על איסוף גורף, מצא המחוקק הבריטי לנכון להגביל את הגישה לחומר שנאסף. עיון בחומר שנאסף מכוח צו יותר רק בחומר שנבחר לעיון (יש להניח כי באמצעות שאילתה מתאימה) לאור התכליות המבצעיות המנויות בצו,[663] לפי הנדרש ובמידתיות.[664]

3.3.4.8.3. צו סייבר כללי (bulk equipment interference warrant)

צו סייבר כללי[665] מסמיך את מושאו להתערב בציוד – לנקוט פעולות סייבר ולא להתבסס על יירוט פסיבי גרידא – כדי להשיג נתוני תקשורת, נתוני ציוד או כל מידע אחר, ובתנאי שתכליתו העיקרית של הצו היא להשיג תקשורת חו״ל,[666] מידע הנוגע לאנשים המצויים מחוץ לאיים הבריטיים או נתוני ציוד חו״ל.[667] צו סייבר כללי גם יכול להסמיך את מושאו לבחור נתונים לעיון מתוך הנתונים

659 ס' 171(1) לחוק סמכויות חקירה 2016 (IPA).

660 ס' 171(2) לחוק סמכויות חקירה 2016 (IPA).

661 ס' 171(4) לחוק סמכויות חקירה 2016 (IPA).

662 ס' 171(6) לחוק סמכויות חקירה 2016 (IPA).

663 ס' 172(1)(a) לחוק סמכויות חקירה 2016 (IPA).

664 ס' 172(1)(b) לחוק סמכויות חקירה 2016 (IPA).

665 ס' 176 לחוק סמכויות חקירה 2016 (IPA).

666 ראו בטקסט המפנה לה"ש 621 **לעיל** בפרק זה.

667 "נתוני ציוד חו"ל" – נתוני ציוד בעלי זיקה לתקשורת חו"ל או לאנשים המצויים מחוץ לאיים הבריטיים, שיכולים לסייע בקביעת התקיימותם או בהשגתם של נתונים כאלו או בפיתוח יכולות איסוף שלהם. ראו ס' 176(3) לחוק סמכויות חקירה 2016 (IPA).

שהושגו מכוחו או להעבירם לצד שלישי,[668] שכן נתונים שהושגו כך סביר שיהיו ממוקדים פחות מנתונים שהושגו באמצעות צו ממוקד. צו סייבר כללי אינו מסמיך את מושאו לנקוט פעולות הטעונות צו יירוט,[669] אלא בנוגע לתקשורת מאוחסנת.[670]

השר רשאי להוציא צו סייבר כללי לבקשתו של ראש סוכנות ביון אם לדעתו הצו נדרש לתכליות הנוגעות לאינטרסים של ביטחון לאומי, מניעה או זיהוי של פשיעה, או אינטרסים כלכליים של הממלכה המאוחדת (אם אלה רלוונטיים לאינטרסים של ביטחון לאומי),[671] ושהוא נחוץ ומידתי ביחס למבוקש בו.[672] הצו יינתן רק אם שהשר סבור שיש די בקרות סטטוטוריות על אבטחת המידע ותפוצתו,[673] התכליות המבצעיות המפורטות בצו[674] נחוצות לצורך עיון בחומר שהושג מכוחו; ובנסיבות הקונקרטיות נדרש לעיין בחומר לאור כל אחת מהתכליות המבצעיות המפורטות בו.[675]

החלטת השר לאשר צו סייבר כללי כפופה למנגנון הנעילה הכפולה, ומשכך – לאישורו של נציב שיפוטי,[676] לבד ממקרים שבהם השר סבור שהצו דחוף.[677] במקרים דחופים ידווח השר לנציב השיפוטי לאחר מעשה, והוא שיחליט

668 I, ס' 176(4) לחוק סמכויות חקירה 2016 (IPA).

669 היינו, פעולות שהן יירוט אסור כהגדרתו בס' 3(a) לחוק סמכויות חקירה 2016 (IPA). ראו בחלק 3.3.4.2 **לעיל**.

670 "תקשורת מאוחסנת" – נתוני תקשורת, לפני שידורם או אחריו, המאוחסנים במערכת תקשורת. ראו ס' 176(8) לחוק סמכויות חקירה 2016 (IPA).

671 ס' 178(2)–(3) לחוק סמכויות חקירה 2016 (IPA).

672 ס' 178(1)(c) לחוק סמכויות חקירה 2016 (IPA).

673 ס' 191–192 לחוק סמכויות חקירה 2016 (IPA).

674 ס' 183 לחוק סמכויות חקירה 2016 (IPA).

675 ס' 178(1)(d) לחוק סמכויות חקירה 2016 (IPA).

676 ס' 179 לחוק סמכויות חקירה 2016 (IPA).

677 ס' 178(1)(f) לחוק סמכויות חקירה 2016 (IPA).

(לכל המאוחר בתוך שלושה ימי עבודה מיום הוצאת הצו הדחוף), אם לאשרו בדיעבד.[678] צו סייבר כללי דחוף יעמוד בתוקפו חמישה ימים.[679]

בהחלטתו לאשר צו סייבר כללי על הנציב השיפוטי לבחון את נחיצותו ואת מידתיותו ביחס לתכליות המבצעיות המפורטות בו,[680] ולהפעיל את אותם עקרונות שהיה מפעיל בית המשפט בבחינת הצו, וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[681] ההחלטה של נציב שיפוטי שלא לאשר התערבות ממוקדת תנומק בכתב.[682]

התכליות המבצעיות שבצו הסייבר הכללי ייבחרו – בדומה לתכליות מבצעיות לצורכי צווי יירוט או צווי תפיסה כלליים – מתוך רשימה סגורה שמנהלים ראשי סוכנויות הביון[683] (לכל סוג של צו כללי יש רשימת תכליות מבצעיות נפרדת). אפשר להוסיף תכלית לרשימה באישור השר, ובתנאי שרמת הפירוט של התכלית החדשה עולה על רמת הפירוט של תכליות צווי הסייבר הכלליים שבלשון החוק.[684] מדי שלושה חודשים על השר להגיש העתק של הרשימה לוועדת המודיעין והביטחון הפרלמנטרית, ועל ראש הממשלה לבחון את הרשימה מדי שנה.[685]

צו סייבר כללי יעמוד בתוקפו למשך שישה חודשים,[686] והוא ניתן להארכה לאחר בחינה מחודשת של הצו בידי השר ובידי נציב שיפוטי (מנגנון הנעילה הכפולה)

678 ס' 180 לחוק סמכויות חקירה 2016 (IPA).

679 ס' 184 לחוק סמכויות חקירה 2016 (IPA).

680 ס' 179(1)(c) לחוק סמכויות חקירה 2016 (IPA).

681 מכוח ס' 2 לחוק סמכויות חקירה 2016 (IPA) (ראו בחלק 3.3.4.3 **לעיל**).

682 ס' 178(3) לחוק סמכויות חקירה 2016 (IPA). אם הנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (Investigatory Powers Commissioner), מבקש הצו רשאי לערער לנציב סמכויות החקירה על הדחייה.

683 ס' 183(4) לחוק סמכויות חקירה 2016 (IPA).

684 כמפורט בס' 178(2), 178(1)(a) לחוק סמכויות חקירה 2016 (IPA).

685 ס' 183(9), 183(11) לחוק סמכויות חקירה 2016 (IPA).

686 ס' 184 לחוק סמכויות חקירה 2016 (IPA).

במהלך שלושים הימים שלפני פקיעת תוקפו.[687] על השר לוודא כי בצו סייבר כללי יש בקרות על היקף התפוצה שלו, על הסדרי השימור שלו ועל אופני הגישה אליו (הנעשית בדרך של עיון).[688] תפוצה של חומר שהושג בצו צריכה להיות מזערית: יש להבטיח כי מספר האנשים הנחשפים לחומר, היקף החשיפה, היקף ההעתקה ומספר ההעתקים יהיו מינימליים.[689] החומר שהושג מכוח צו תפיסה כללי, על העתקיו, יאובטח[690] ויבוער לכשיתאיין הצורך בו.[691]

מאחר שעסקינן בצו סייבר כללי – שהמידע שנרכש מכוחו אינו ממוקד, אלא נאסף ללא הבחנה – מצא המחוקק הבריטי לנכון להגביל את הגישה לחומר שנאסף. עיון בחומר שנאסף מכוח צו יותר רק כשמדובר בחומר שנבחר לעיון לאור התכליות המבצעיות המנויות בצו,[692] לפי הנדרש ובמידתיות.[693] אם החומר שנבחר לעיון הוא מידע מוגן,[694] יש לוודא כי הקריטריון לבחירתו (המזהה, identifier, של השאילתה) אינו מזהה של אדם המצוי בטריטוריה בריטית.[695] יש בקרות נוספות בנוגע למידע הנהנה מחיסיון משפטי[696] או עיתונאי.[697]

687 ס' 185 לחוק סמכויות חקירה 2016 (IPA).

688 ס' 191(1) לחוק סמכויות חקירה 2016 (IPA).

689 ס' 192(2) לחוק סמכויות חקירה 2016 (IPA).

690 ס' 192(4) לחוק סמכויות חקירה 2016 (IPA).

691 ס' 192(6) לחוק סמכויות חקירה 2016 (IPA).

692 ס' 193(1)(a) לחוק סמכויות חקירה 2016 (IPA).

693 ס' 193(1)(b) לחוק סמכויות חקירה 2016 (IPA).

694 לפי הגדרתו בס' 193(9) לחוק סמכויות חקירה 2016 (IPA), הזהה להגדרתו בס' 100 לחוק – ראו **לעיל** בפרק זה ה"ש 493.

695 ס' 193 לחוק סמכויות חקירה 2016 (IPA). במקרים שבהם היה בעבר שימוש מותר במזהה של היעד המודיעיני מושא השאילתה, ועקב שינוי בנסיבות – היעד עבר לאיים הבריטיים או שהתחוור כי הערכה קודמת שלפיה היעד אינו בטריטוריה (ומכוחה הותרה עיון בנתוני התקשורת של היעד) היא שגויה – קצין בכיר רשאי לאשר בכתב את המשך השימוש במזהה זה למשך חמישה ימי עבודה נוספים.

696 ס' 194 לחוק סמכויות חקירה 2016 (IPA).

697 ס' 195 לחוק סמכויות חקירה 2016 (IPA).

3.3.4.8.4. צווי מידע אישי (BPD — bulk personal dataset warrant)

מאגר מידע אישי (bulk personal dataset)[698] הוא מאגר נתונים שהושג ומוחזק בשירות ביון למטרת מילוי תפקידיו ומוחזק או יוחזק באמצעים אלקטרוניים כדי לנתחו למטרות אלו, וכולל נתונים אישיים[699] על בני אדם שסביר כי רובם אינם, ולא יהיו, מעניינו של השירות.

החזקה של שירות ביון במאגר מידע אישי כאמור ועיון בנתונים שבו טעונים כל אחד צו מידע אישי.[700] עם זאת יובהר כי החזקה של מאגרי מידע אישי שהושגו מכוח צו אחר שבחוק סמכויות חקירה (IPA) ועיון בהם אינם כפופים להשגה של צו מידע אישי.[701] הוראות ה־IPA בנוגע למאגרי מידע אישיים, כך נראה, הן המסגרת המשפטית המסדירה בין השאר איסוף של מידע גלוי ברשתות חברתיות ואת ניתוחו לאחר מכן.

יש שני סוגים של צווי מידע אישי (BPD warrant): צו מידע אישי ספציפי (specific BPD warrant), שמתייחס למאגרים מסוימים של מידע אישי; וצו מידע אישי קטגוריאלי (class BPD warrant), שמתייחס לקטגוריות של מאגרי מידע אישי – מקרים שבהם מבוקש לעיין או לשמור מאגרי מידע לפי קטגוריה של מידע אישי – למשל "נתונים רפואיים" ו"נתוני תנועה". צווי מידע אישי קטגוריאליים – בהיותם גורפים כל כך על אף ההגבלות המפורטות בפסקה הבאה – הם חידוש שנוי במחלוקת של חוק סמכויות חקירה (IPA), ויש הסבורים כי היה ראוי להסתפק ברמת הפגיעה בפרטיות הכרוכה בצווי מידע אישי ספציפיים.[702]

698 ס' 199(1) לחוק סמכויות חקירה 2016 (IPA).

699 ראו **לעיל** בפרק זה ה"ש 412.

700 ס' 200 לחוק סמכויות חקירה 2016 (IPA).

701 ס' 201(1) לחוק סמכויות חקירה 2016 (IPA).

702 ראו למשל Report of the Joint Committee on the Draft Investigatory Powers Bill (11.02.2016), Recommendation 42; Report of the Draft Investigatory Powers Bill – The Intelligence and Security Committee Recommendation F (9.02.2016)

שירות ביון אינו רשאי להחזיק במאגר מידע אישי או לבוחנו בהסתמך על צו מידע אישי קטגוריאלי אם ראש השירות סבור כי המאגר כולל מידע מוגן,[703] רשומות רפואיות[704] או מידע אישי רגיש,[705] או אם טבעו של המאגר, הנסיבות שנוצר בהן או השימוש שהשירות עושה בו עלולים להעלות סוגיות חדשות או שנויות במחלוקת, המצריכות בחינה של השר ושל נציב שיפוטי.[706]

השר רשאי לתת צו מידע אישי ספציפי לבקשתו בכתב של ראש שירות ביון במקרים שבהם (1) מאגר המידע האישי מושא הצו אינו בגדרי קטגוריה המתוארת בצו מידע אישי קטגוריאלי שהשירות מבקש את אישורו (כגון מאגר ששייך לקטגוריה חדשה של מאגרי מידע),[707] או (2) כשמאגר המידע מושא הצו הוא בגדרי קטגוריה המתוארת בצו מידע אישי קטגוריאלי שהשירות מבקשו, אך השירות מנוע מלהסתמך על צו מידע אישי קטגוריאלי בשל הסייגים שבחוק,[708] או שהשירות סבור שראוי לבקש צו כאמור.[709]

703 ס' 202(1) לחוק סמכויות חקירה 2016 (IPA). ההגדרה של "מידע מוגן" לצורך צווי מידע אישי שונה מההגדרה של "מידע מוגן" בהקשר של צווי יירוט. "מידע מוגן" הוא כל מידע שבמאגר מידע אישי פרט לנתוני ציוד ולמידע שאינו מידע פרטי ולמידע שניתן להפרדה מהמאגר, ושאין בו כדי לגלות את משמעות יתר הנתונים שבמאגר (IPA, ס' 203).

704 ס' 202(2) לחוק סמכויות חקירה 2016 (IPA). "רשומות רפואיות", כהגדרתן בס' 206(6) לחוק סמכויות חקירה 2016 (IPA), הן נתונים הכוללים מידע המתייחס למצבו הגופני או הנפשי של פלוני שערך איש מקצועות הרפואה, ושירות הביון השיג אותן ממי שפועל בשם גוף שירותי רפואה בנוגע לרשומה או להעתקה (איש מקצועות הרפואה וגוף שירותי רפואה, כמשמעם בסעיף 69 לחוק הבריטי בדבר הגנת מידע 1998 (DPA)).

705 ס' 202(2) לחוק סמכויות חקירה 2016 (IPA). "מידע אישי רגיש" הוא מידע על פלוני מהסוג המנוי בסעיף 2(a)–(f) לחוק הבריטי בדבר הגנת מידע 1998 (DPA): מוצא אתני, עמדות פוליטיות, אמונה דתית, חברות בארגון עובדים, מצב רפואי וחיי מין (ההפניה שבחוק סמכויות חקירה 2016 משמיטה מהרשימה את סוגי המידע המנויים בשארית סעיף 2לחוק סמכויות חקירה 2016 (IPA) – נתונים בקשר לביצוע או טענות ביחס לביצוע של עבירות פליליות, ומידע על הליכים בקשר לכך).

706 ס' 202(3) לחוק סמכויות חקירה 2016 (IPA).

707 ס' 205(2) לחוק סמכויות חקירה 2016 (IPA), וכן ס' 590 לדברי ההסבר.

708 ס' 202 לחוק סמכויות חקירה 2016 (IPA), ראו **לעיל** בטקסט המפנה לה"ש 703–706.

709 ס' 205(3) לחוק סמכויות חקירה 2016 (IPA).

השר רשאי לתת צו מידע אישי (קטגוריאלי או ספציפי), לבקשתו בכתב של ראש שירות ביון. על הבקשה לכלול תיאור של הקטגוריה או של מאגרי המידע האישי הרלוונטיים לה, לפי סוג הצו. אם מבוקש לקבל אישור לעיון במאגרי מידע, על הבקשה לכלול גם את פירוט התכליות המבצעיות[710] של העיון.[711] כאשר מבוקש צו מידע אישי ספציפי בשל מניעותו של השירות לפעול מכוח צו מידע אישי קטגוריאלי בשל הסייגים שבחוק,[712] יש להסביר זאת בכתב.[713]

השר ייתן את צו המידע האישי בתנאי שהוא סבור שהצו מידתי ביחס למבוקש בו[714] ונדרש לתכליות של ביטחון לאומי, מניעה או זיהוי של פשיעה או לקידום אינטרסים של איתנותה הכלכלית של הממלכה (אם אינטרסים אלה רלוונטיים לאינטרסים שבביטחון הלאומי).[715] הצו יינתן בתנאי שהשר סבור שהסדרי אבטחת המידע והגבלת החשיפה אליו נאותים,[716] ובתנאי שהוא סבור כי חל צורך בתכליות המבצעיות המפורטות בצו[717] לצורך עיון בחומר שהושג מכוחו, וכי בנסיבות הקונקרטיות יש צורך בעיון בחומר לאור כל אחת מהתכליות המבצעיות המפורטות בו.[718] על השר לוודא כי יש הסדרים בצו המבטיחים את הגבלת העיון בחומר החוסה בו לתכליות המבצעיות המפורטות בו.[719]

צו מידע אישי ספציפי שנוגע למאגר מידע הכולל רשומות רפואיות יינתן רק בנסיבות יוצאות דופן שבהן יש צורך דחוק בהחזקת רשומות אלו או בעיון בהן.[720]

710 ס' 212 לחוק סמכויות חקירה 2016 (IPA).

711 ס' 204(1)–(2), 205(4) לחוק סמכויות חקירה 2016 (IPA).

712 ס'205(3)(i)(b), 202 לחוק סמכויות חקירה 2016 (IPA).

713 ס' 205(5) לחוק סמכויות חקירה 2016 (IPA).

714 ס' 204(3)(b), 205(6)(b) לחוק סמכויות חקירה 2016 (IPA).

715 ס' 204(3)(a), 205(6)(a) לחוק סמכויות חקירה 2016 (IPA).

716 ס' 204(3)(d), 205(6)(d) לחוק סמכויות חקירה 2016 (IPA).

717 ס' 212 לחוק סמכויות חקירה 2016 (IPA).

718 ס' 204(3)(c), 205(6)(c) לחוק סמכויות חקירה 2016 (IPA).

719 ס' 221(1) לחוק סמכויות חקירה 2016 (IPA).

720 ס' 206 לחוק סמכויות חקירה 2016 (IPA).

השר רשאי להתנות בצו תנאים לפני שיתיר לעיין במידע מוגן על אדם שנמצא באיים הבריטיים בעת העיון.[721] אם קבע השר תנאים כאלה, עליו לוודא כי יש הסדרים בצו המבטיחים את קיומם.[722]

צו מידע אישי (ספציפי או קטגוריאלי) כפוף גם כן למנגנון הנעילה הכפולה וטעון גם אישור של נציב שיפוטי, חוץ מבמקרים שבהם השר סבור שהצו דחוף.[723] במקרים דחופים ידווח השר לנציב השיפוטי לאחר מעשה, וזה יחליט (לכל המאוחר בתוך שלושה ימי עבודה מיום הוצאת הצו הדחוף) אם לאשרו בדיעבד.[724] צו מידע אישי דחוף יעמוד בתוקפו למשך חמישה ימים.[725]

בבואו לאשר צו מידע אישי, על הנציב השיפוטי לבחון את נחיצותו ואת מידתיותו ביחס לתכליות המבצעיות המפורטות בו,[726] ולהפעיל את אותם העקרונות שהיה מפעיל בית משפט בבואו לבחון את הצו וברמת נאותות שיש בה כדי לעמוד בחובה לשקול שיקולי פרטיות.[727] החלטת נציב שיפוטי שלא לאשר התערבות ממוקדת תנומק בכתב.[728]

התכליות המבצעיות שבצו המידע האישי ייבחרו – בדומה לתכליות מבצעיות בצווים כלליים – מתוך רשימה סגורה שראשי סוכנויות הביון מנהלים.[729] אפשר להוסיף תכלית לרשימה באישור השר ובתנאי שרמת הפירוט של התכלית

721 ס' 207 לחוק סמכויות חקירה 2016 (IPA). ל"מידע מוגן" – ראו **לעיל** בפרק זה ה"ש 703.

722 ס' 221(3) לחוק סמכויות חקירה 2016 (IPA).

723 ס' 204(3)(e), 205(6)(e) לחוק סמכויות חקירה 2016 (IPA).

724 ס' 209 לחוק סמכויות חקירה 2016 (IPA).

725 ס' 213 לחוק סמכויות חקירה 2016 (IPA).

726 ס' 208(1)(c) לחוק סמכויות חקירה 2016 (IPA).

727 מכוח סעיף 2 לחוק סמכויות חקירה 2016 (IPA) (ראו חלק 3.3.4.3 **לעיל**).

728 ס' 208(3) לחוק סמכויות חקירה 2016 (IPA). אם הנציב השיפוטי המסרב לאשר את הצו אינו נציב סמכויות החקירה (Investigatory Powers Commissioner), מבקש הצו רשאי לערער בפני נציב סמכויות החקירה על הדחייה.

729 ס' 212(5) לחוק סמכויות חקירה 2016 (IPA).

החדשה עולה על רמת הפירוט של תכליות צווי המידע האישי (הספציפיים או הקטגוריאליים) שבלשון החוק.[730] מדי שלושה חודשים על השר להגיש העתק של הרשימה לוועדת המודיעין והביטחון הפרלמנטרית, ועל ראש הממשלה לבחון את הרשימה מדי שנה.[731]

החוק מאפשר לסוכנויות הביון לבחון בחינה ראשונית מאגרי מידע שהגיעו לחזקתן שלא באמצעות צו מכוח חוק סמכויות חקירה (IPA). טיפול ראשוני כאמור יותר לתקופה מוגבלת ללא צורך בצו מידע אישי כדי לבחון את תוכן המאגרים, את הצורך בהמשך ההחזקה בהם, ועל פי אלה – את הצורך בצו מידע אישי.[732]

3.3.4.9 מנגנוני הפיקוח

3.3.4.9.1. נציב סמכויות החקירה ונציבים שיפוטיים

במסגרת חוק סמכויות חקירה 2016 (IPA) הוקם מנגנון פיקוח מעין-שיפוטי, שבראשו עומד נציב סמכויות החקירה (Investigatory Powers Commissioner), ולצידו מכהנים נציבים שיפוטיים (Judicial Commissioners). הנציבים ממונים לתקופה של שלוש שנים בידי ראש הממשלה בהסכמת שר המשפטים (Lord Chancellor) וראשי מערכות המשפט של אנגליה ויילס, סקוטלנד ואירלנד, ומינוי הנציבים השיפוטיים כרוך גם בהסכמת נציב סמכויות החקירה.[733] יובהר כי נציבות סמכויות החקירה, אף שחבריה הם שופטים לשעבר, אינה בית דין, והיא אינה מקיימת הליך אדוורסרי, אלא הליך של בחינת הצו באמצעות אותם עקרונות של ביקורת שיפוטית שבהם משתמש בית המשפט.[734]

על נציב סמכויות החקירה לפקח על הרשויות העוסקות ביירוט תקשורת, בהתערבות בציוד או בהשגה ושימור של נתוני תקשורת או של מידע משני.

730 כמפורט בס' 204(3)(a), 205(6)(a) לחוק סמכויות חקירה 2016 (IPA).

731 ס' 183(9), 183(11) לחוק סמכויות חקירה 2016 (IPA).

732 ס' 220 לחוק סמכויות חקירה 2016 (IPA).

733 ס' 227(1)-(4) לחוק סמכויות חקירה 2016 (IPA).

734 ס' 23(2)(a) לחוק סמכויות חקירה 2016 (IPA).

פיקוח זה יכול להתבצע בדרכים שונות, לרבות ביקורות, חקירות או בדיקות של הנציב. ראש הממשלה רשאי להורות לנציב סמכויות החקירה לפקח על עניינים נוספים הנוגעים לפעילותם של שירותי המודיעין או לפעילות מודיעינית של גופי הביטחון.[735]

החוק מורה לנציבים – נציב סמכויות החקירה והנציבים השיפוטיים – לפקח על הבקרות הסטטוטוריות שנועדו להגן על הזכות לפרטיות, אבל גם לא לפעול בניגוד לאינטרס הציבורי או בדרך הפוגעת בביטחון הלאומי או בתקינותה הכלכלית של הממלכה. על הנציבים להבטיח שהם נמנעים מלסכן פעולות של מודיעין או אכיפת החוק או את ביטחונם של המשתתפים בפעולות אלו, וכן שאינם מכבידים ללא צורך על האפקטיביות המבצעית של שירותי המודיעין, של כוחות המשטרה והביטחון או של משרדי ממשלה.[736]

אם נעשתה טעות חמורה בעניינו של אדם מסוים שהסבה לו נזק רציני, חובה על נציב סמכויות החקירה לדווח לו על הטעות, ובתנאי שהדיווח משרת את האינטרס הציבורי.[737] עם זאת החוק מציין כי עצם הפגיעה בזכויות מכוח האמנה האירופית לזכויות אדם (ECHR)[738] די בה כדי להיות טעות חמורה. כשהנציב מחליט אם לדווח על טעות, עליו לשקול את חומרתה, את מידת הפגיעה באינטרסים הלאומיים שבחשיפתה ואת השפעתו של הגילוי על הפעילות השוטפת של שירותי המודיעין.

על נציב סמכויות החקירה למסור דיווח שנתי לראש הממשלה על פעילותם של הנציבים השיפוטיים.[739] הדיווח צריך לכלול נתונים כמותיים על היקף הפעלת הסמכויות שבחוק, לרבות על מידת הצלחתן של פעולות המודיעין שאושרו

735 ס' 231 לחוק סמכויות חקירה 2016 (IPA).

736 ס' 229(5)–(8) לחוק סמכויות חקירה 2016 (IPA). עם זאת החובה להימנע מפגיעה באינטרסים ביטחוניים או לאומיים, וכן ביעילות המבצעית, אינה חלה בהחלטות שנוגעות להטלת קנסות, מתן צווים, ביעור, אשרור של הסמכה מכוח החוק, אישור מתן צו שימור נתונים, ערעור על החלטה של נציב שיפוטי אחר, ובשאר העניינים המפורטים בסעיף 299(8).

737 ס' 231 לחוק סמכויות חקירה 2016 (IPA).

738 ראו חלק 3.3.1 **לעיל**.

739 ס' 234 לחוק סמכויות חקירה 2016 (IPA).

מכוח הצווים שניתנו, על מספר הבקשות לצווים לסוגיהם, על מספר הבקשות שאושרו ועל הפעלת הבקרות על פריטי מידע חסויים, וכן פירוט התכליות המבצעיות ששימשו לצורך צווי איסוף כלליים. נוסף על הדוחות השנתיים, ראש הממשלה רשאי להורות לנציב סמכויות החקירה להכין דוח בעניין מסוים, והנציב רשאי ליזום דיווחים אם הוא רואה זאת לנכון.

לנציב סמכויות החקירה הסמכות לפתוח בחקירה או בביקורת לשם מילוי תפקידו, ובעלי תפקידים בשירות הציבורי, ספקי תקשורת ואחרים לפי צו חייבים לשתף עימו פעולה.[740] כמו כן ועדת המודיעין והביטחון הפרלמנטרית רשאית להפנות לנציב עניינים שלדעתה ראוי שיחקור אותם.[741]

עצמאות הגוף השיפוטי המפקח על מעקב מדינה (וכן מראית העין של עצמאות כזו) היא דרישה שהודגשה בדין האירופי.[742] עם זאת יש המציינים שעצמאותו של נציב סמכויות החקירה אינה מלאה.[743] כך למשל השר רשאי לשנות את סמכויותיו של הנציב (למעט אלה שנוגעות לאישור, לתיקון או לחידוש צווים) בתקנות,[744] וראש הממשלה יכול לקבוע את מספר הנציבים השיפוטים שעליו למנות.[745]

3.3.4.9.2. טריבונל סמכויות החקירה (Investigatory Powers Tribunal)

טריבונל סמכויות החקירה הוא מותב עצמאי שהוקם מכוח הוראות החוק להסדרת סמכויות החקירה (RIPA)[746] כדי לעמוד בהוראות סעיף 13 לאמנה

740 ס' 235 לחוק סמכויות חקירה 2016 (IPA).

741 ס' 236 לחוק סמכויות חקירה 2016 (IPA).

742 עניין *Zakharov*, **לעיל** בפרק זה ה"ש 227, פס' 257–260; עניין *DRI*, **לעיל** בפרק זה ה"ש 228, פס' 62.

743 Byron Karemba, *The Investigatory Powers Bill: Putting the Investigatory Powers Commissioner in Focus (Part II)*, U.K. Const. L. Blog (15.4.2016)

744 ס' 239 לחוק סמכויות חקירה 2016 (IPA).

745 ס' 227(b) לחוק סמכויות חקירה 2016 (IPA).

746 ס' 65–70 לחוק הסדרת סמכויות חקירה 2000 (RIPA), וכן התיקונים לו המפורטים בס' 242 לחוק סמכויות חקירה 2016 (IPA).

האירופית לזכויות אדם (ECHR), שלפיו כל אדם יהא זכאי לפנות לרשות לאומית בבקשה לסעד אפקטיבי בגין הפרת הזכויות המנויות בה. הטריבונל מורכב משופטים בכירים (פעילים או בדימוס) וממשפטנים בכירים, הממונים לתקופה של חמש שנים. הטריבונל נועד לשמש כתובת לתלונות על הפעלה שלא כדין של סמכויות מעקב וחקירה, בין השאר מכוח החוק להסדרת סמכויות החקירה (RIPA) וחוק סמכויות חקירה (IPA), ולפתוח בחקירה עצמאית כדי לקבוע את נכונות התלונה.

הטריבונל רשאי[747] לקבוע פיצויים למתלוננים שזכויותיהם נפגעו בשל הפעלת סמכות שלא כדין, לבטל צווים, הוראות ואישורים שניתנו מכוח החקיקה הרלוונטית (IPA או RIPA), להורות על השמדת חומר שהושג ונשמר מכוח צו או אישור שבדין או מוחזק בגוף ציבורי, ולבטל צווים שיפוטיים שניתנו לרשויות מקומיות.[748] הטריבונל אינו כפוף לביקורת שיפוטית, אלא אם השר הורה אחרת בצו.[749]

בעקבות גילוייו של סנודן על היקף האיסוף המקוון של שירותי הביון הבריטיים, הגישו כמה ארגוני זכויות אדם תלונה לטריבונל סמכויות החקירה. לשיטתם, פרקטיקות האיסוף הבריטיות והמידע המודיעיני שמקורו בחומר שאספו סוכנויות הביון האמריקאיות לפי תוכניות PRISM ו־upstream collection,[750] סתרו את הוראות האמנה האירופית לזכויות אדם (ECHR). הטריבונל קבע כי הכללים שהסדירו בקשות של שירותי הביון הבריטיים לקבלת מידע שמקורו בתוכניות אלו (כמו שאלו נמסרו לטריבונל בתצהירי הגילוי של שירותי הביון) נמצאו בהלימה עם מסגרת זכויות האדם של האמנה האירופית, למעט חריג

747 ס' 67 לחוק הסדרת סמכויות חקירה 2000 (RIPA).

748 מכוח ס' 75 לחוק סמכויות חקירה 2016 (IPA).

749 ס' 67(8) לחוק הסדרת סמכויות חקירה 2000 (RIPA). ראו גם עניין Privacy International, R (on the application of) v. Secretary of State for Foreign and Commonwealth Affairs & Ors, [2017] EWCA Civ 1868 (23.11.2017), שם דחה בית המשפט לערעורים את הטענה שאת הסעיף יש לפרש פירוש צר ודווקני, המקנה סמכות לבית המשפט הגבוה לדון בהחלטות הטריבונל.

750 ראו בחלק 3.1.7 **לעיל**.

אחד שנכון למועד התצהירים טרם נעשה בו שימוש.[751] הטריבונל הדגיש כי איסוף גורף ורחב והיקף יכול שיהיה מידתי, אבל הגישה אליו מוגבלת לתכליות הסטטוטוריות.[752] גישה זו, המבחינה בין איסוף נתונים לעיון בהם, הקדימה את חוק סמכויות חקירה 2016 (IPA), וכנראה עמדה לנגד עיניהם של מנסחיו. עם זאת בשימוע מאוחר יותר באותו עניין קבע הטריבונל כי המשטר שחל על הנתונים שמקורם בסוכנויות האמריקאיות הפר את סעיפים 8 ו־10 לאמנה האירופית. עוד הוסיף הטריבונל וקבע כי נכון למועד הכרעתו תוקנה התנהלותם של שירותי הביון הבריטיים בכל הנוגע לשיתוף מידע מודיעיני עם ארצות הברית באופן שהולם את הוראות האמנה.

3.3.4.10 היועץ העצמאי לחקיקה בענייני טרור (Independent Reviewer of Terrorism Legislation)

ראשיתו של מוסד היועץ העצמאי לחקיקה בענייני טרור בשלהי שנות השבעים,[753] כשבמסגרת הדיון הציבורי שהתנהל בבריטניה בנושא ההתמודדות עם הטרור האירי, מינה הפרלמנט יועץ עצמאי שיבחן את יישום החקיקה בענייני טרור, מינוי שחודש מדי שנה בשנה. עיגון סטטוטורי ראשון לתפקיד נעשה על פי החוק למניעת טרור משנת 2005 (Prevention of Terrorism Act),[754] וכיום הבסיס הסטטוטורי לפעולתו של היועץ העצמאי לחקיקה בענייני טרור מצוי בסעיף 36 לחוק הטרור מ־2006 (Terrorism Act 2006), המסמיך אותו לבחון מעת לעת את הוראות חוק הטרור של 2006 ואת הוראות חוק הטרור של 2000. לצד פונקציות סטטוטוריות אלו היועץ העצמאי לחקיקה בענייני טרור רשאי ליזום דיווחים משל עצמו בנושאים כלליים הנוגעים לחקיקה זו.

751 IPT/13/77/H IPT13/92/CH IPT/13/168-173/H IPT/13/194/CH IPT/13/204/CH: Reported in [2015] 3 AER 142 (להלן: עניין *Liberty 1*).

752 IPT/13/77/H etc as above: Reported in [2015] 3 AER 212 (להלן: עניין *Liberty 2*).

753 David Anderson, *Independent Review of Terrorism Laws: Searchlight or Veil?* (February 24, 2014)

754 ס' 14 ל־Prevention of Terrorism Act 2005

היועץ העצמאי לחקיקה בענייני טרור נהנה מעצמאות בחקירה, ועל דיווחיו לכלול את עמדתו האישית. שלא כמבקרים עצמאיים אחרים, היועץ נהנה מסיווג ביטחוני ומגישה לחומרים מסווגים שמקילים את עבודתו. דוחות החקירה של היועץ מפורסמים בפומבי, וכשהוא מצליח ללכת בין הטיפות וזוכה באמון הציבור והממשל גם יחד, חשיבותו בבקרה על הפעלת סמכויות שלטון יכולה להיות רבה.[755]

סעיף 7 של חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA) הורה לשר למנות את היועץ העצמאי לחקיקה לענייני טרור כדי שיבחן את אופן ההפעלה של סמכויות החקירה (מכוח DRIPA ו־RIPA).[756] עם זה ההוראה לא שרדה את הביטול של IPA את רוב סעיפי DRIPA, ואם ישמש מוסד זה לבחינת פעולתו של ה־IPA, ייעשה הדבר על בסיס מינוי אד הוק של היועץ, כמו שנעשה הדבר לפני שעוגן התפקיד בחקיקה (כך למשל בהליכי חקיקת ה־IPA התבקש היועץ לחקיקה בענייני טרור לחבר דוח עצמאי על איסוף גורף (bulk powers)).[757]

3.3.4.11 עתיד ה־IPA

עיון בפסיקה – הן האירופית והן הבריטית – מעלה ספקות באשר לתוקפו של חוק סמכויות החקירה 2016 (IPA), אם פסיקה זו אכן תהיה רלוונטית כמקור סמכות בעידן שלאחר הברקזיט. כאמור לעיל, החלטתו של בית הדין האירופי

755 Vanessa Sauter, *The Lawfare Podcast: David Anderson on the United Kingdom's Intelligence Policies,* LawFare (13.1.2018)

756 ראו לדוגמה את דוח היועץ העצמאי לענייני חקיקת טרור לפי סעיף 7 לחוק סמכויות חקירה ושימור נתונים 2014 (DRIPA): David Anderson, *A Question of Trust* (Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation, June 2015)

757 David Anderson, *Report of the Bulk Powers Review* (Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation, August 2016). הדוח בחן את יעילותם של אמצעי איסוף חסרי הבחנה שהוסדרו במסגרת חוק סמכויות חקירה 2016 (IPA): סמכויות יירוט גורף (bulk interception), סמכויות תפיסה כלליות (bulk acquisition), סמכויות סייבר כלליות (bulk equipment interference) וסמכויות הנוגעות למאגרי BPD (להרחבה ראו בחלק 3.3.4.8 **לעיל**).

לצדק (ECJ) בעניין *Tele2 Sverige AB*[758] – שקבעה כי חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA) אינו מצוי בהלימה עם הדין האירופי[759] – קבעה אמות מידה לאסדרה מדינתית של שימור נתונים. בינואר 2018, כחלק מעניין *Watson*, נתן בית המשפט לערעורים סעד הצהרתי שלפיו סעיף 1 ל־DRIPA (אף שכבר לא היה בתוקף בעת מתן פסק הדין) – שהוראותיו מתירות, לתכליות של אכיפת חוק, גישה לנתונים שמורים שאינה לשם מניעת עבירות מסוג פשע (serious crime), או שהוא מאפשר גישה לנתונים שמורים ללא ביקורת שיפוטית או של רשות מינהלית עצמאית אחרת – אינו תואם את הדין האירופי.[760]

יש שסברו, עוד בטרם ניתן פסק הדין בעניין *Watson*, כי עניין *Tele2 Sverige AB* רלוונטי לא רק ל־DRIPA, אלא גם ל–IPA, שהחליף אותו, בשל הדמיון בין שני דברי החקיקה בכל הנוגע לסמכויות שימור הנתונים.[761] הוראות ה־IPA כוללות הסדרים שאינם מתיישבים עם הנחיות בית הדין האירופי בעניין *Tele2 Sverige* AB:[762] נראה כי התכליות שמכוחן ה־IPA מתיר שימור נתונים וגישה אליהם[763] רחבות מאלה המותרות בפסק הדין; צווי היירוט הכלליים מכוח ה־IPA[764] אינם מתיישבים עם הסטנדרט של צורך מוחלט שהתווה ב־*Tele2 Sverige* AB;[765]

758 ראו Tele2 Sverige AB, **לעיל** בפרק זה ה"ש 228.

759 ראו בחלק 3.3.4.1 **לעיל**.

760 *Tom Watson MP v. Secretary of State for the Home Department*, 70 EWCA [2018] Civ, פס' 27 (להלן: עניין *Watson*). ראו גם עמיר כהנא "זה אלמנטרי, ווטסון: שימור נתונים בבריטניה ובישראל" **אתר המכון הישראלי לדמוקרטיה** (16.2.2018).

761 Eliza Watt, *The Right to Privacy and the Future of Mass Surveillance*, 7 Int'l J.Hum. Rts. 773 (2017)

762 Isabella Buono & Aaron Taylor, *Mass Surveillance In The CJEU: Forging A European Consensus*, 76 The Cambridge Law Journal 250–253 (2017)

763 ס' 61(7) לחוק סמכויות חקירה 2016 (IPA), ראו בחלק 3.3.4.6 **לעיל**.

764 ראו חלק 3.3.4.1 **לעיל**.

765 ראו עניין *Tele2 Sverige AB*, **לעיל** בפרק זה ה"ש 228, פס' 95–96, 107, 118–119.

ביקורת שיפוטית אינה נדרשת בכל המקרים,[766] ויש שמטילים ספק באשר לעצמאותה מלכתחילה.[767] אמות המידה המחמירות יותר של התקנות הכלליות בדבר הגנת מידע (GDPR) מחזקות את ההערכה שאם יגיע ה־IPA לדיון בבית הדין האירופי לצדק, יימצא שהוא בחוסר הלימה עם הדין האירופי.[768]

ביוני 2017 נתן בית המשפט הגבוה הבריטי רשות לארגון זכויות האדם ליברטי (Liberty) לפתוח בהליכים משפטיים התוקפים את ה־IPA.[769] בשלב זה אישר בית המשפט לפתוח בהליכים התוקפים את חלקו הרביעי של ה–IPA, המסדיר את ההוראות החלות על שימור נתוני תקשורת.[770] לטענת ליברטי, משטר שימור הנתונים של חוק סמכויות חקירה 2016 (IPA) אינו שונה מהותית מזה של חוק סמכויות חקירה ושימור נתונים 2014 (DRIPA), שבעניין *Tele2 Sverige AB* הוכרז שאינו תואם את הדין האירופי. שימור נתונים ב־IPA אינו מוגבל לעבירות מסוג פשע (serious crime), והוא מותר גם למטרות של הגנה על בריאות הציבור, אסדרה פיננסית וגביית מיסים, וכן אין מנגנון של ביקורת שיפוטית על הודעות שימור.[771] קשה להעריך את סיכוייה של עתירת ליברטי בשל אי־הוודאות המשפטית הנוגעת לברקזיט, שהשלכותיה על תחולת הדין האירופי

766 ראו למשל השגת נתוני תקשורת, בחלק 3.3.4.5 **לעיל**.

767 ראו **לעיל** בחלק 3.3.4.9.1 סיפה.

768 Phil Muncaster, *GDPR and Snoopers' Charter: A Marriage Made in Hell* (24.02.2017); Patsy Ciardullo, *The E.U.'s General Data Protection Regulation and Its Impact on England's Investigatory Powers Act of 2016* (draft, Spring 2017)

769 Rebecca Hill, *Civil Rights Warriors Get Green Light to Challenge UK Mass Surveillance*, The Register (30.6.2017). ראו גם עיקרי הטענות בשימוע מיום 27.2.2018 בעניין Claimant's Skeleton Argument for Hearing on 27-28 February 2018, Claim No. CO/1052/2017, Liberty v. The Secretary of State for the Home Department and the Secretary of State for Foreign and Commonwealth Affairs (להלן: עתירת **ליברטי**).

770 ס' 87–95 לחוק סמכויות חקירה 2016 (IPA). ראו בחלק 3.3.4.6 **לעיל**.

771 ראו **לעיל** בפרק זה ה"ש 562.

בבריטניה אינן ודאיות. תחולת הדין יציר הפסיקה של בית הדין האירופי לצדק בבריטניה בעידן שאחרי הברקזיט, טרם הוסדרה.[772]

יוער כי העתירה המקורית של ליברטי תקפה את מכלול ההוראות שב־IPA ולא רק את הפרק הרביעי, העוסק בשימור נתוני תקשורת, שבו דן בית המשפט. הביקורת של ליברטי ושל ארגוני זכויות אדם אחרים על ההסדרים שב־IPA נוגעת לשאלות בדבר עצמאותו האפקטיבית של מוסד הנציבות השיפוטית, שאינו חלק ממערכת בתי המשפט, וכן המערך המסועף של הפרקטיקות המודיעיניות המוסדרות בחוק, בייחוד אלה שמאפשרות איסוף נתונים גורף וחסר הבחנה, התערבות בציוד ועיבוד מידע אישי לפי צווי BPD. פרקטיקות אלה פותחות פתח לפגיעה לא מידתית בזכות לפרטיות ובחופש הביטוי (בשל האפקט המצנן שבצידן), ואין בהסדרתן בדין, כך נטען, כדי להכשירן.

זאת ועוד, אם תפרוש בריטניה מהאיחוד האירופי, העברת מידע מחוץ לגבולות האיחוד לתחומי בריטניה תהא בכפוף להסדרים שמחילות התקנות הכלליות בדבר הגנת מידע (GDPR) על העברת מידע למדינות שאינן חברות, ולכן יהיה על דיני הגנת הפרטיות הבריטיים להלום סטנדרט נאותות מסוים או לכונן הסדר וולונטרי בדומה ל־Privacy Shield.[773] בשל תקדים *Schrems*[774] סביר להניח שהסדר זה ייבחן בקפידה ובהתייחס לדינים החלים על מעקב מדינה מקוון בבריטניה.[775] מנגד, במשא ומתן על תנאי פרישתה מהאיחוד בריטניה מצהירה על כוונתה ליישם בחקיקה את הסטנדרטים העדכניים ביותר של הדינים האירופיים להגנת המידע, ומנסה לפעול להקמת מתווה של שיתוף פעולה רגולטורי בנושאים אלה.[776]

772 ראו למשל את דבריו של הנשיא בדימוס נויברגר על הצורך בוודאות משפטית אחרי הברקזיט: Kevin Rawlinson, *Judge Calls for Clarity on Status of ECJ Rulings in UK after Brexit,* The Guardian (8.8.2017).

773 ראו חלק 3.2.3.3 **לעיל**.

774 עניין *Schrems*, **לעיל** בפרק זה ה"ש 175.

775 ראו גם Simon Jay, Colin Pearson & Natalie Farmer, *Some Reflections on Brexit and the U.K. Data Protection Regime,* 28 Intellectual Property & Technology L. J. 28 18-23 (2016).

776 Department for Exiting the European Union, *The Exchange and Protection of Personal Data: A Future Partnership Paper* (24.8.2017).

החלטתו של בית הדין האירופי לצדק (ECJ) בעניין *Tele2 Sverige AB*, פסק הדין בעניין *Watson*, וייתכן שגם שיקולים שנובעים מהתקיפה של חוק סמכויות חקירה (IPA) בבית המשפט הגבוה בבריטניה ומהשלכות הברקזיט על ההסדרים העתידיים של העברת נתונים בין בריטניה לאיחוד, כפי שתוארו לעיל – כל אלה הביאו לידי הפצתם של תזכיר הצעת החוק לתיקון ה־IPA, תקנות השגת נתונים ושימור שלהם וכללי ההתנהגות המוצעים לתקשורת נתונים, להערות הציבור.[777] במסגרת התיקון מוצע בין השאר לשנות את התכליות שמכוחן השר רשאי להורות על שימור נתוני תקשורת,[778] להוסיף שיקולים נוספים על אלה שעליו להפעיל בעשותו זאת[779] וכן לשנות את אופן ההשגה שלהם. עוד מוצע שחלק מסמכויותיו של הפקיד הבכיר להורות על השגת נתוני תקשורת יועברו לנציב סמכויות החקירה.[780]

777 Investigatory Powers Act 2016 Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data

778 מוצע להחליף את התכליות הקיימות (ראו ה"ש 533, 554 **לעיל** בפרק זה) בתכליות האלה: אינטרסים של ביטחון לאומי; כשמדובר בנתוני אירוע – מניעת פשע חמור, וכשמדובר בנתוני ישות – מניעת פשע או הפרת סדר; שמירה על אינטרסים הנוגעים לרווחתה הכלכלית של הממלכה, בתנאי שאלו נוגעים לביטחון הלאומי; אינטרסים של ביטחון הציבור; תכליות של מניעת מוות, נזק גופני או נפשי, או הקטנתם; סיוע בחקירת טענות בקשר להרשעת חפים מפשע. **שם**, Schedule showing changes to the Investigatory Powers Act, p. 19.

779 על השיקולים המנויים בחוק (ראו בה"ש 557 **לעיל** בפרק זה) שעל השר להפעיל בבואו לתת הודעת שימור מוצע להוסיף את השיקולים האלה: התועלת שבצד ההודעה בדבר תכליות השימור (המנויות בה"ש 778 **לעיל** בפרק זה); שירות התקשורת שאליו מופנית ההודעה; נאותות הקריטריון המגביל את שימור הנתונים (מיקום או האנשים המשתמשים בשירותי התקשורת). ראו **שם**, בעמ' 21–22.

780 השוו **שם** בעמ' 2–19, 28–33 לחלק 3.3.4.5 **לעיל**. התיקון המוצע מצמצם את התכליות שעבורן פקיד בכיר מוסמך להורות על השגת נתוני תקשורת, ובמקומן מוצע שנציב סמכויות החקירה יורה על כך. כך למשל מוצע כי קציני משטרה בכירים יורשו להורות על השגת נתוני תקשורת לתכליות של ביטחון לאומי ושמירה על רווחתה הכלכלית של הממלכה, כשהדבר נוגע לאינטרסים של ביטחון לאומי (ס' 61(7)(a),(c) לחוק סמכויות חקירה 2016 (IPA)); **שם**, בתיקון המוצע לתוספת הרביעית, עמ' 28); אך לתכליות של מניעת פשע, יורשו הקצינים להורות על השגת נתוני תקשורת רק במקרי חירום, ואילו בשגרה תהא הסמכות להורות על השגת נתוני תקשורת לתכליות של מניעת פשע מסורה בידי נציב סמכויות החקירה.

- הדינים הבריטיים בדבר מעקב מקוון מוסדרים בחוק סמכויות חקירה 2016 (IPA). החוק מאפשר, בין השאר, לשר לתת צווים ליירוט נתוני תוכן, להפעלת אמצעי סייבר להשגת נתוני תוכן ותקשורת ולעיון בחומר שנאסף על סמך צווים כלליים (bulk warrants).

- החוק הבריטי כולל מנגנונים למתן צווים לאיסוף גורף וחסר הבחנה (bulk collection), שמכוחו ניתן ליירט, לתפוס או להחזיק במידע רחב היקף בלי להתייחס ליעדים מודיעניים מודיעין מוגדרים. צווים כלליים ניתן להפעיל בנוגע לאיסוף של נתוני תקשורת ונתוני תוכן, וכן לשם השגת מידע באמצעות התערבות בציוד תקשורת (על ידי הפעלת אמצעי סייבר).

- השגת נתוני תקשורת באופן ממוקד (בהתייחס ליעד מודיעיני קונקרטי), אינה טעונה צו, ופקידי ממשל רבים מוסמכים לדרוש אותם מספקי תקשורת שונים.

- כשנדרש צו לצורך הפעלת סמכות שבחוק סמכויות חקירה 2016 (IPA), מנגנון הנעילה הכפולה שבחוק מחייב שנוסף על יבחן את הצו מראש גם נציב שיפוטי (Judicial Commissioner) – גורם מינהלי מעין־שיפוטי פנימי שמפעיל כלים של ביקורת שיפוטית על הצווים.

3.4. גרמניה

3.4.1. מעטפת חוקתית

הזכות לפרטיות כמעט שאינה מוזכרת במפורש בחוק היסוד הגרמני.[781] סעיף 10 לחוק היסוד אמנם מגן על הפרטיות בהתכתבות, בדברי דואר ובתקשורת אלקטרונית,[782] וסעיף 13 מגן על ביתו של הפרט מפני חדירה, אבל הזכות הכללית לפרטיות היא יצירתה של הפסיקה.[783]

עניין מרשם התושבים

בפסק הדין בעניין **מרשם התושבים**[784] גזר בית המשפט את הזכות להגדרה עצמית מידעית (informational self-determination) מהזכות לכבוד שבסעיף 1(1) לחוק היסוד ומהזכות לאוטונומיה אישית שבסעיף 2(1) לחוק היסוד. הזכות להגדרה עצמית מידעית נועדה להבטיח את יכולתו של הפרט לקבוע בעיקרון את הפצתו של מידע אישי עליו ואת השימוש בו. ההלכה הפסוקה מאז עניין **מרשם התושבים** מתירה לרשות ציבורית לאסוף, לעבד ולהעביר מידע אישי בתנאי, בין השאר, שהפעולה נעשית מכוח הוראה תקפה בחוק ובכפוף לעקרון המידתיות.[785]

781 מיכל קרמר "כבוד האדם במשפט הגרמני" **כבוד האדם כערך עליון ומוחלט במשפט הגרמני – האם גם בישראל?** 54 (מרדכי קרמניצר ומיכל קרמר, 2011); Ronald J. Krotoszynski, *A Prolegomenon to Any Future Restatement of Privacy*, 79 Brook. L. Rev. 505 (2014); Ronald J. Krotoszynski, *The Polysemy of Privacy,* Ind. L.J. 881 906 (2013)

782 Grundgesetz für die Bundesrepublik Deutschland [GG] (להלן: חוק היסוד הגרמני). נוסח התרגום העברי של הסעיף לקוח מקרמר, **שם**, בה"ש 83.

783 Donalad Kommers & Russell A. Miller, The Constitutional Jurisprudence of the Federal Republic of Germany 408–413 (3rd ed. 2009)

784 BVerfGE 65,1 (1983). (להלן: עניין **מרשם התושבים**).

785 Paul M. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, 2 Int'l Data Privacy Law 289 290 (2012)

עניין המעקב המקוון

זכות נוספת שניסח בית המשפט החוקתי בפרשת **המעקב המקוון**[786] היא הזכות לסודיות ולשלמות של מערכות מידע אלקטרוניות. הזכות נגזרת מתוך הקביעה כי הוראות חוק החיפוש המקוון שבחוק הגנת החוקה של מדינת נורדריין־וסטאפליה אינן חוקתיות. הוראות אלו הסמיכו את סוכנות הביון של מדינה זו לחדור למערכות תקשורת דרך האינטרנט ולאסוף מידע, וכן לנטר וליירט תקשורת מבוססת־אינטרנט. על פי בית המשפט, מעקב חשאי מקוון יוצדק אם יהיו ראיות שיצביעו על איום ממשי למושא של הגנה משפטית בעלת חשיבות עליונה כגון בריאותו, חייו או חירותו של אדם,[787] ובכפוף לביקורת שיפוטית. לא כל שימוש פרטי בטכנולוגיה מתקדמת נוגע לזכות לסודיות ולשלמות של מערכות מידע אלקטרוניות, אך זו משחקת תפקיד בהגבלת הנפח והמגוון של הנתונים שאליהם יכולה המדינה לגשת. הזכות חלה במקרים של חדירה למערכות IT אישיות אם יש בהן כמות רבה של נתונים אישיים, ואם החדירה מפירה את ריבונותו של האדם באשר לנתונים שהוא שומר.[788]

סעיף 10(1) לחוק היסוד הגרמני מורה כי אין לפגוע בפרטיות של התכתבות, דברי דואר ותקשורת אלקטרונית. בשנת 1968 תוקן חוק היסוד ושונה נוסחו של ס"ק 10(2), שלפיו "ניתן להורות על סייגים רק מכוח חוק". בשנת 1968, בעקבות תיקון בחוק היסוד, התווספה הסיפה, שלפיה "במקרה שהסייג משמש להגנת הסדר הציבורי החופשי והדמוקרטי או להגנת הקיום או הביטחון של הפדרציה או של מדינה ממדינותיה, יכול החוק לקבוע שהאדם שיושפע מכך לא יקבל

786 120 BVerfGE 274 302 (2008) (להלן: עניין **המעקב המקוון**); ראו גם קרמר, **לעיל** בפרק זה ה"ש 781, בעמ' 57; Kommers & Miller, לעיל בפרק זה ה"ש 487, בעמ' 416-417; Russell A. Miller, *Balancing Security and Liberty in Germany*, 4 J. Nat. Security L. & Pol. 369 390-391 (2010); Gerrit Hornung & Christoph Schnabel, *Data Protection in Germany II: Recent Decisions on Online Searching of Computers, Automatic Number Plate Recognition and Data Retention*, 25 Computer L. & Security Rev. 115 116-118 (2009)

787 עניין **המעקב המקוון**, **שם**, בפס' 247.

788 Russell A. Miller, *A Pantomime of Privacy: Terror and Investigative Powers in German Constitutional Law*, Washington & Lee Legal Studies Paper No. 2017-5 fn 266-267

הודעה על הסייג, ושפנייה לבית־המשפט תוחלף בבדיקת המקרה על־ידי אורגן שמינה המחוקק". משכך, כפי שיתואר בחלקים הבאים, במקרים שסעיף 10(2) מתיר זאת, מעקב מקוון אינו טעון צו שיפוטי, והדבר נותר כדבריו של קלאוס גרדיץ כ"פצע שותת בגוף המוסדי של ארכיטקטורת המודיעין הגרמנית".[789]

נוסף על עניין **מרשם התושבים** ועניין **המעקב המקוון** – שהקימו את הזכויות החוקתיות להגדרה עצמית מידעית ולהגנה על מערכות מידע כזכויות נגזרות מהזכות לפיתוח האישיות – במשך השנים גילה בית המשפט הגרמני לחוקה מעורבות רבה בתחום ההגנה על הפרטיות בכמה תיקים הרלוונטיים לפרקטיקות של מעקב ברשתות תקשורת:[790]

עניין האזנות הסתר

בפסק דין זה אשרר בית המשפט החוקתי את חוקתיותם של סעיף 10(2) ושל החוק לסייגים על הפרטיות של התכתבויות, דואר ותקשורת אלקטרונית (להלן: חוק סעיף 10 או G10),[791] שנחקק סמוך לתיקון. עם זאת פסל בית המשפט סעיף קטן של אחד מסעיפי החוק (G10) בנוסחו אז, שאסר על יידוע מטרות מודיעיניות בדבר קיום המעקב, ללא סייגים, ומצא אותו לא מידתי.[792] מילר מעיר

789 Klaus Gärditz, *Legal Restraints on the Extraterritorial Activities of Germany's Intelligence Services, in* Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair 401 431 (Russell A. Miller, ed., 2017)

790 BVerfGE 30, 1(1970) (להלן: עניין **האזנות הסתר**); 115 BVerfGE 320, (2006) (להלן: עניין **סינון המידע**); (1999) 100 BVerfGE 313, (להלן: עניין **המעקב האסטרטגי**); (2004) 109 BVerfGE 279, (להלן: עניין **הציתות**); 125 BVerfGE 260,, (2010) (להלן: עניין **שימור הנתונים**); BVerfG, 1 BvR 1299/05 (24.01.2012) (להלן: עניין **בנק המידע**); (2005) 113 BVerfGE 348, (להלן: עניין **מעקב התקשורת המונע**); BVerfG, 1 BvR 966/09 (20.04.2016) (להלן: עניין **חוק ה־BKA**) (2013) (להלן: עניין **מאגר ה־ATD**).

791 Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2007 I S. 154), das zuletzt durch Artikel 12 des Gesetzes vom 14. August 2017 (BGBl. I S. 3202) geändert worden ist, ראו חלק 3.4.3.3 **להלן**.

792 Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance,* 54 Hastings L.J. 751 773-776 (2002); ראו גם Kommers & Miller, **לעיל** בפרק זה ה"ש 487, בעמ' 413-414.

כי התקיפה החוקתית של סעיף 10(2) ושל חוק סעיף 10 לא הלינה על פגיעה בפרטיות, מאחר שסעיף 10 לחוק היסוד הוא *lex specialis* ביחס לפרטיות בתקשורת.[793]

עניין המעקב האסטרטגי[794]

חוק סעיף 10 (G10) מבחין בין מעקב אינדיווידואלי,[795] אחרי יעד מודיעיני; ובין מעקב אסטרטגי,[796] שאינו כולל יעד כזה. בעניין **המעקב האסטרטגי** נדונה חוקתיותה של חקיקה שהתירה לסוכנות הביון הפדרלית הגרמנית (BND – Bundesnachrichtendienst) לעסוק במעקב אסטרטגי ולחלוק מודיעין עם סוכנויות ביון זרות. בית המשפט לחוקה מצא כי תחולת ההגנה החוקתית של סעיף 10 אינה מוגבלת לתקשורת שנעשתה בתוך גבולות גרמניה, וכי היא משתרעת מעבר לה, ובתנאי שיש זיקה מספקת בין פעילות האיסוף לטריטוריה הגרמנית. בנסיבות המקרה – שבהן פעילות האיסוף, המקור או היעד של חלק מהתקשורת שיורטה במסגרתה היו בגבולות גרמניה – קבע בית המשפט כי זיקה כאמור מתקיימת.[797] בית המשפט הצביע על הסכנות הטמונות במעקב כזה, שעשוי להשפיע על חופש הביטוי ועל דפוסי תקשורת.[798] חרף סיכונים אלה מצא בית המשפט שפרקטיקות איסוף אלה מוצדקות, שכן הן משפיעות במידה רבה על מדיניות החוץ והביטחון של הרפובליקה. מאחר שהחוק התיר איסוף מידע הנחוץ לאיתור סכנות לגרמניה, ברוב המקרים מצא בית המשפט שהוא אינו בלתי הולם, אבל חלקים מסוימים של חוק סעיף 10 (G10), הנוגעים להעברת מידע לסוכנויות פדרליות אחרות, נמצאו לא מידתיים כמו למשל הסעיף שהתיר

793 Russell M. Miller, *Intelligence Oversight – Made in Germany, in* Global Intelligence Oversight: Governing Security In The Twenty-First Century 258, 278 (Zachary K. Goldman, Jane Harman & Samuel James Rascoff, eds., 2016)

794 ראו גם Schwartz, **לעיל** בפרק זה ה"ש 792, בעמ' 778–782.

795 ס' 3–4 לחוק סעיף 10 (G10). ראו חלק 3.4.3.3 **להלן**.

796 ס' 5–8 לחוק סעיף 10 (G10). ראו חלק 3.4.3.3 **להלן**.

797 עניין **המעקב האסטרטגי**, **לעיל** בפרק זה ה"ש 790, בעמ' 363–364.

798 **שם**, בעמ' 381.

העברת מידע שמקורו בחיפושים אסטרטגיים לשם מימוש תכליות של אכיפת האיסור על זיוף כספים.[799] זאת ועוד, בעניין **המעקב האסטרטגי** נדון גם מעמדה של ועדת סעיף 10 (G 10-Kommission), גוף עצמאי שנועד לפקח על המונחים הספציפיים שישמשו לצורך חיפוש בתוצרי המעקב האסטרטגי (ראו להלן). בית המשפט לא הסתפק בהיקף בקרה צנוע זה של הוועדה, והסמיך אותה לבקר היבטים נוספים של עיבוד מידע אישי בסוכנות הביון הפדרלית (BND), בכלל זה העברת מידע לסוכנויות אכיפת החוק, ביעור מידע ויידוע מושאי המידע על היותם במעקב.[800]

שוורץ מעיר כי על אף היעדר התחולה של הזכות להגדרה עצמית מידעית (בדומה לעניין **האזנות הסתר**, גם כאן עניין **המעקב האסטרטגי** התרכז בסעיף 10 לחוק היסוד), ציין בית המשפט כמה הקבלות בין הזכות להגדרה עצמית מידעית ובין ההגנות החוקתיות על תקשורת. בהקשר זה הדגיש בית המשפט את היחס בין פרטיות ובין חירות השיח בחברה, והצביע על העובדה שהסכנות במעקב אינן נוגעות רק לפרט, אלא לחברה כולה.[801]

עניין סינון המידע[802]

כריית מידע (כר"מ) היא כלי שכבר מלווה את סוכנויות אכיפת החוק בגרמניה משנות השבעים של המאה העשרים במאבקן נגד סיעת הצבא האדום (כנופיית באדר־מיינהוף),[803] ומכונה בגרמנית Rasterfahndung או "מכמורת" (dragnet)

799 **שם**, בעמ' 385.

800 **שם**, בעמ' 402.

801 Schwartz, **לעיל** בפרק זה ה"ש 792, בעמ' 781.

802 ראו גם Kommers & Miller, **לעיל** בפרק זה ה"ש 387, בעמ' 614; Paul M. Schwartz, *Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and New Technology*, 53 Wm. & Mary L. Rev. 351 361-376 (2011); Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609 653-655 (2007).

803 עניין **סינון המידע**, **לעיל** בפרק זה ה"ש 790, פס' 3.

לסינון המידע. בעניין **סינון המידע** מצא בית המשפט לחוקה כי פעולות כריית מידע שביצעה המשטרה לאחר אירועי 11 בספטמבר אינן חוקתיות.

בעקבות אירועים אלה פעלה ועדת שרי הפנים של מדינות גרמניה, בהנהגת המשטרה הפדרלית של גרמניה (BKA – Bundeskriminalamt), לאיתור תאי טרור רדומים באמצעות כריית מידע, בהתבסס על מידע אישי שמקורו במאגרי מידע של האוניברסיטאות, במרשם התושבים ובמרשם המרכזי למהגרים.[804] מפקדות המשטרה השונות אספו את הנתונים ברמת המדינה, חיפשו בתוכם לפי קריטריונים מוגדרים[805] והעבירו את התוצרים למשטרה הפדרלית (BKA). המשטרה הפדרלית יצרה מאגר מידע פדרלי משולב של תאים "רדומים", ובו כ־32 אלף רשומות. משרדי המשטרה במדינות השונות קיבלו גישה למאגר מידע זה.

מבצע כר"מ זה הגיע אל בית המשפט החוקתי בדרך של ערעור, שקבע כי הערכאות שקדמו ומצאו כי המבצע חוקתי, פירשו את הסעיף בחוק המשטרה של מדינת נורדריין־וסטאפליה (שעליו הסתמכה משטרת נורדריין–וסטאפליה בביצוע הכר"מ)[806] פירוש הפוגע בזכות החוקתית להגדרה עצמית מידעית. פרקטיקות של סינון מידע – קבע בית המשפט החוקתי – מקיימות את תנאי המידתיות רק כשיש סכנה ממשית לאינטרס שבדין.[807] עם זאת לא בחן בית המשפט את חוקתיות הכר"מ כפרקטיקה, אלא את התנאים המידתיים המאפשרים אותה: הפרה כבדת משקל של זכות יסוד מותרת בעת סכנה ברמה מתאימה, ובעיקר כשמדובר באמצעי שנקט מראש, שאז יש לאמוד את הסיכוי להתממשותה של הסכנה.[808] לצד סכנה ממשית וקרובה היה בית המשפט נכון להכיר במצבים של איום מתמשך. ואולם תמיד יש מתיחות

804 **שם**, בפס' 7–10, 26.

805 גברים בגיל 18–40, סטודנטים או סטודנטים לשעבר ומוסלמים, שנולדו או שמוצאם במדינות מסוימות (שבהן רוב מוסלמי). **שם**, בפס' 26.

806 Polizeigesetz des Landes Nordrhein-Westfalen [PolG NRW]; 10 GV NTE 70 §31

807 עניין **סינון המידע**, **לעיל** בפרק זה ה"ש 790, בפס' 133–153.

808 **שם**, בפס' 140.

פוליטית שטרוריסטים עלולים לנצל, וזו יכולה להימשך זמן רב. לכן התייחס בית המשפט קונקרטית לאיום הטרור המתמשך מאז 11 בספטמבר וקבע שאין בו כדי להצדיק פעולות כר"מ.[809]

וסף על עניינים אלה, התייחס בית המשפט לסוגיית המעקב המקוון גם במקרים נוספים. כשלושה חודשים לאחר כניסת דירקטיבת שימור הנתונים האירופית לתוקף[810] קיבל בית המשפט החוקתי של גרמניה החלטה נדירה ונתן צו מניעה זמני המקפיא חלק מהוראותיו של החוק הגרמני המיישם אותה. בעניין **שימור הנתונים**,[811] בחלוף שנתיים הורה בית המשפט על ביטולו של החוק. יישום הדירקטיבה נעשה על דרך של הוספת שני סעיפים לחוק הטלקומוניקציה הגרמני (TKG):[812] הראשון מורה לספקי תקשורת לשמור נתונים לתקופה של שישה חודשים, והשני מתאר את התנאים שמכוחם יותר לסוכנויות אכיפת החוק לגשת אליהם.

בית המשפט לחוקה ציין בהכרעתו כי גם מנתונים שאינם נתוני תוכן אפשר להסיק מסקנות קשורות־תוכן החודרות לספרה הפרטית.[813] עם זאת ניתן לעצב משטר שימור מידע ההולם את סעיף 10(1) לחוק היסוד, בהתחשב בחשיבותו למניעת סכנה. כדי שיהא חוקתי, חוק שימור מידע זקוק להוראות מוגדרות היטב של אבטחת מידע, להגבלות על הגישה לנתונים המגבילות את השימוש בהם לחקירות של פשעים חמורים במיוחד, לשקיפות מספקת ולבקרה שיפוטית על השימוש בנתונים השמורים ועל הפצתם.[814]

809 **שם**, בפס' 147.

810 ראו **לעיל** בפרק זה ה"ש 300.

811 ראו גם Gerrit and Schnabel, **לעיל** בפרק זה ה"ש 786, בעמ' 120–122; Kommers & Miller, **לעיל** בפרק זה ה"ש 784, בעמ' 417–418.

812 Telekommunikationsgesetz [TKG] BGBl. I 1190 (2004) (להלן: חוק הטלקומוניקציה הגרמני (TKG)), ראו חלק 3.4.3.2 **להלן**.

813 עניין **שימור הנתונים לעיל** בפרק זה ה"ש 790, בעמ' 319.

814 **שם**, בעמ' 260–261.

בעניין **בנק המידע** הסתמך בית המשפט על החלטתו בעניין **שימור הנתונים** וקבע כי סעיף בחוק הטלקומוניקציה (TKG), המורה לספקי תקשורת לאסוף מידע מזהה של לקוחותיהם, הוא חוקתי, מאחר שאינו כולל מידע בעל אופי אישי במיוחד, ואין בו כדי לאפשר הפקת פרופילים או ניתוח תנועה במרחב הגאוגרפי של המשתמשים.[815] יתר על כן, בית המשפט מצא גם מצא כי סעיף אחר, המקים נוהל העברת מידע מקוון לרשויות ממשלה שונות, חוקתי גם הוא. עם זאת הגביל בית המשפט את הגישה לכתובות IP, המאפשרות דה־אנונימיזציה של פעילות ברשת ולמספרי זיהוי אישיים (PIN).[816]

ב**עניין הציתות** נדונו חוקתיותן של הוראות בסדר הדין הפלילי הגרמני שהתירו מעקב אחר חשודים במעורבות בפשע מאורגן, לרבות בדרך של האזנה לדירתם. בהסתמך על ההגנה על המעון שבסעיף 13 לחוק היסוד קבע בית המשפט שמעקב אחר שיחותיו הפרטיות של פלוני הנעשות בדירתו, ושהן בעלות אופי אישי מיוחד, עולה כדי חדירה לליבת הזכות שההגנה עליה מוחלטת. רק כשסביר להניח שהשיחה המצותתת קשורה למעשה פשע, ההאזנה לה תותר.[817]

בעניין **מעקב התקשורת המונע** פיתח בית המשפט את התנאים המתירים האזנת סתר. מעקב מונע יהיה מותר חוקתית רק אם יהיה אינטרס חוקי רם־דרג ומצב מוגדר שבו נקודות עצירה קונקרטיות. מאחר שאת תוכנה של שיחה אין לדעת מראש, הורה בית המשפט לרשויות המאזינות להפסיק את ההאזנה לאלתר כשמזוהה חדירה לגרעין האינטימי של הפרטיות. יש להבטיח גם כי לא ייעשה שימוש בתוכן של תקשורת כאמור המתייחס לליבת הספרה הפרטית, לרבות העברתו לצדדים שלישיים, וכי הקלטות המכילות מידע כאמור יבוערו לאלתר.[818]

815 עניין **בנק המידע**, **לעיל** בפרק זה ה"ש 790, פס' 139, 159.

816 **שם**, פס' 172–174.

817 מיכל קרמר "מידתיות במשפט הגרמני" **מידתיות במבט ביקורתי ומשווה** 103 182–191 (מרדכי קרמניצר עורך, 2016).

818 ראו גם בטקסט המפנה לה"ש 856 **להלן** בפרק זה.

3.4.2. החוק הפדרלי להגנת מידע (BDSG)

בגרמניה יש 17 חוקי הגנת מידע – החוק הפדרלי להגנת מידע (BDSG)[819] וחוק נפרד לכל אחת מ־16 המדינות ברפובליקה הפדרלית. למרות דקויות מסוימות, חוקים אלו דומים למדי.[820] החוק הפדרלי להגנת מידע משנת 1990 תוקן כדי ליישם את הוראות דירקטיבת הגנת המידע,[821] בדומה לחקיקה דומה במדינות־חברות אחרות באיחוד האירופי. החוק נועד להסדיר את הטיפול[822] (היינו האיסוף, העיבוד[823] והשימוש)[824] בנתונים אישיים,[825] והוא חל הן על המגזר הפרטי והן על המגזר הציבורי.[826] מאחר שהחוק הפדרלי להגנת מידע (BDSG) ותיק

819 Bundesdatenschutzgesetz [BDSG] Bundesgesetzblatt I. [BGBl. I.] 66 (2003) (להלן: החוק הפדרלי להגנת מידע (BDSG)).

820 Nils Zurawski, *Exercising Access Rights in Germany, in* The Unaccountable State of Surveillance: Exercising Access Rights In Europe 109 (Clive Norris, Paul de Hert, Xavier L'Hoirt and Antonella Galetta, eds. 2017)

821 ראו בחלק 3.2.3 **לעיל** והשוו לחלק 3.3.3 **לעיל**.

822 ס' 1(1)–(2) לחוק הפדרלי להגנת מידע (BDSG).

823 ס' 3(4) לחוק הפדרלי להגנת מידע (BDSG) – עיבוד, לרבות שימור, שינוי, העברה, חסימה ומחיקה של נתונים אישיים, כהגדרתן של פעולות אלו שם.

824 ס' 3(5) לחוק הפדרלי להגנת מידע (BDSG) – שימוש הוא כל ניצול של נתונים אישיים שאינו בגדר עיבוד.

825 "נתונים אישיים", לפי ס' 3(1) לחוק הפדרלי להגנת מידע (BDSG), הם כל מידע הנוגע לנסיבות אישיות או מהותיות של אדם מזוהה או ניתן לזיהוי (מושא המידע). החוק אינו מגן על פרטיותם של אישיות משפטית שאינה בן אדם או של מתים. עם זאת יש דברי חקיקה אחרים המגינים עליהם, דוגמת חוק הטלקומוניקציה הגרמני (TKG), המגן על ישויות משפטיות או דינים רפואיים החלים על מתים. הקישור בין המידע למושא המידע יכול שיהיה ישיר או עקיף, אך פירוש סביר לנתונים אישיים כולל למשל כתובות IP (לדוגמה ראו עניין **בנק המידע**) ומספרי רישוי של מכוניות (ראו לדוגמה את פסק הדין בעניין BvR 2074/05, 1 BvR 1254/071, הנוגע לחוקתיות מערכות זיהוי של לוחיות רישוי אוטומטיות, וכן ראו גם Gerrit and Schnabel, **לעיל** בפרק זה ה"ש 786, בעמ' 117–120).

826 ניתן למצוא הגדרות לגופים ציבוריים שונים בס' 2(1)–(3) לחוק הפדרלי להגנת מידע (BDSG). "גופים פרטיים" לפי ס' 2(4) לחוק הם בני אדם, תאגידים וישויות משפטיות שאינם גופים ציבוריים. אם גוף פרטי מבצע פעולות מינהליות ציבוריות ריבוניות, הוא ייראה גוף ציבורי.

מהדירקטיבה, הוא אינו מנסח במפורש את עקרונות עיבוד המידע שבדירקטיבה, אך ניתן לקרוא אותם לתוכו.[827] עם עקרונות ה־BDSG ניתן למנות את עקרון צמידות המטרה[828] ועקרון החיסכון במידע (data economy).[829] איסוף נתונים אישיים צריך להתבצע ישירות ממושא המידע,[830] ואיסוף ממקורות אחרים יותר רק מכוח הוראה מפורשת בחוק, או אם איסוף ישיר ממושא המידע הוא בגדר מאמץ לא מידתי ובהיעדר אינדיקציות לקיפוח האינטרסים הלגיטימיים שלו עקב האיסוף העקיף.

איסוף מידע מטעם גופים ציבוריים יתאפשר כשהוא נחוץ לשם מילוי חובותיהם ויידוע מושא המידע (כשהאיסוף אינו ישירות ממנו).[831] כמה תנאים חלופיים מתירים איסוף קטגוריות מיוחדות של מידע אישי,[832] ותחתם סוכנויות ממשל האוספות מידע מקוון יכולות לחסות. כך למשל יותר איסוף מידע אישי מיוחד כשהאיסוף הוא מכוח הוראה מפורשת בדין או שהוא הכרחי בשל אינטרס ציבורי חשוב; כשהאיסוף הכרחי כדי להגן על אינטרסים חיוניים של מושא המידע או של צד שלישי, ומושא המידע אינו יכול לתת את הסכמתו לכך מטעמים משפטיים או פיזיים; כשהאיסוף הכרחי כדי למנוע איום רציני על ביטחון הציבור, על טובת

827 Douwe Korff, *New Challenges to Data Protection Study – Country Report: Germany* (2010), European Commission DG Justice, Freedom and Security Report. השוו למשל לחוק הבריטי בדבר הגנת מידע 1998 (DPA), **לעיל** בחלק 3.3.2, שנוסח כדי ליישם את הוראות הדירקטיבה.

828 ס' 9 לחוק הפדרלי להגנת מידע (BDSG), המורה על נקיטת אמצעי בטיחות ואמצעים טכניים המבטיחים הלימה עם הוראות החוק, מפנה לנספח לחוק המכיל סטנדרטים ספציפיים שבהם יש לעמוד, ובכללם הוראה למנהלי מאגר המידע שלפיה עליהם לוודא כי נתונים שנועדו לתכליות שונות יעובדו בנפרד.

829 ס' 3a לחוק הפדרלי להגנת מידע (BDSG) מורה כי איסוף מידע אישי, עיבודו ושימוש בו יהיו מזעריים, ולפיו מערכות מידע יתוכננו בהלימה עם מטרה זו. ככל האפשר, יש לדאוג להתממה (אנונימיזציה) של נתונים אישיים.

830 ס' 4(2) לחוק הפדרלי להגנת מידע (BDSG).

831 ס' 13(1)–(1a) לחוק הפדרלי להגנת מידע (BDSG).

832 מידע אישי מיוחד, לפי ס' 3(9) לחוק הפדרלי להגנת מידע (BDSG), כולל מוצא אתני, השקפות פוליטיות, דתיות או פילוסופיות, חברות באיגודים או על בריאות וחיי המין של מושא המידע.

הכלל או לשם הגנה על אינטרסים חשובים של טובת הכלל; כשהאיסוף הכרחי כדי לאפשר לגוף ציבורי של הפדרציה למלא את חובותיו, לתכליות של הגנה או למילוי חובות בין־לאומיות בתחומי ניהול משברים, מניעת סכסוכים או לצרכים הומניטריים.[833]

אחסון מידע אישי אצל גופים ציבוריים, שימוש שלהם בו ושינויו מותרים אם הם נדרש לצורך מילוי תפקידו של מנהל המאגר ולתכליות שלשמן נאסף.[834] חריגה מעקרון צמידות המטרה תותר אם תימצא אחת מכמה חלופות, בין השאר אם הדבר נדרש למניעת פגיעה קשה בטובת הכלל, איום על ביטחון הציבור או להגנה על אינטרסים חשובים של הכלל וכן למטרות של הליכים פליליים וכדי למנוע הפרה חמורה של זכויותיו של אדם אחר.[835] השימוש, השינוי והאחסון של קטגוריות מיוחדות של מידע אישי ייעשו בכפוף להימצאותן של חלופות אחרות, בדומה לאלו החלות על איסופן.[836]

העברת מידע לגופים ציבוריים תותר כשהדבר הכרחי למילוי תפקידיו של הגוף הציבורי (המקבל את הנתונים), ובתנאי שהוראות סעיף 14 (הנוגע לשימוש, לשינוי ולאחסון של מידע אישי) מתקיימות. העברת מידע אישי לגופים פרטיים תותר כשהדבר הכרחי למילוי תפקידיו של הגוף הציבורי (מקבל הנתונים), בהתקיים הוראות סעיף 14 ובתנאי שהצד השלישי המקבל את הנתונים מוכיח שהאינטרס שלו במידע זה מוצדק, וכי למושא המידע אין אינטרס הנוגד את ההעברה. העברת נתונים מקטגוריות מיוחדות של מידע אישי לגופים פרטיים תותר לצורכי מחקר מדעי, או אם המידע ככלל נגיש (או שמנהל המאגר רשאי לפרסמו), או אם המידע נדרש למימוש זכויות משפטיות או להגנה עליהן.[837]

833 ס' 13(2) לחוק הפדרלי להגנת מידע (BDSG).

834 ס' 14(1) לחוק הפדרלי להגנת מידע (BDSG).

835 ס' 14(2) לחוק הפדרלי להגנת מידע (BDSG).

836 ס' 14(5) לחוק הפדרלי להגנת מידע (BDSG) מפנה לרוב התנאים החלופיים שבסעיף 13(2) לחוק. כל החלופות שתוארו לעיל בנוגע לאיסוף רלוונטיות גם לשימוש.

837 ס' 15–16 לחוק הפדרלי להגנת מידע (BDSG).

בהלימה עם דירקטיבת הגנת המידע האירופית[838] החוק מקנה למושאי המידע זכות גישה למידע אישי שלהם המוחזק אצל גופים ציבוריים,[839] וכן זכות יידוע על דבר איסוף המידע,[840] זכות להגנה מהחלטות שהתקבלו על בסיס עיבוד אוטומטי שלו[841] וזכות לחסימת עיבוד נתונים בנסיבות מסוימות ולתיקון או למחיקה של נתונים אישיים.[842]

זכות הגישה למידע והזכות ליידוע אינן מוחלטות. כשהמידע המבוקש נוגע להעברת מידע אישי למשרדי ההגנה על החוקה, לסוכנות הביון הפדרלית (BND), למחלקת הריגול הנגדי של המודיעין הצבאי, או במקרים שהדבר נוגע לביטחון הפדרציה – לרשויות אחרות של משרד הביטחון – בקשות מכוח זכות זו ייענו בכפוף להסכמתם של גופים אלה.[843] כמו כן לא יועבר מידע במסגרת מימוש זכות הגישה אם הדבר פוגע במילוי תפקידו של מנהל מאגר המידע, מסכן את ביטחונם של הציבור, של הפדרציה או של אחת ממדינותיה, או אם מכוח חובה שבדין או בשל טיבם וטבעם הנתונים המבוקשים סודיים.[844]

עם כניסתה לתוקף של התקנות הכלליות בדבר הגנה על מידע (GDPR) במאי 2018,[845] נכנס לתוקפו החוק הפדרלי החדש להגנת מידע (ה־BDSG החדש).[846] שלא כקודמו, החוק החדש לא נועד ליישם את הוראות ה־GDPR (מאחר שלאלה,

838 ראו חלק 3.2.3.2 **לעיל**.

839 ס' 19, 34, 6(1) לחוק הפדרלי להגנת מידע (BDSG), השוו לסעיף 15 לדירקטיבת הגנת המידע.

840 ס' 19a לחוק הפדרלי להגנת מידע (BDSG).

841 ס' 6a, 8 לחוק הפדרלי להגנת מידע (BDSG). השוו לסעיפים 21–22 לדירקטיבת הגנת המידע.

842 ס' 20 לחוק הפדרלי להגנת מידע (BDSG).

843 ס' 19(3) לחוק הפדרלי להגנת מידע (BDSG), וביחס לזכות ליידוע ראו ההפניה שבסעיף 19a(3) לחוק.

844 ס' 19(3) לחוק הפדרלי להגנת מידע (BDSG), וביחס לזכות ליידוע ראו ההפניה שבסעיף19a(3) לחוק.

845 ראו חלק 3.2.5.1 **לעיל**, והשוו לחלק 3.3.3 **לעיל**.

846 BGBl. I 2017, p. 2097 (להלן: ה־BDSG החדש).

בשונה מדירקטיבת הגנת המידע, תחולה ישירה), אלא להרחיב את הוראות ה־GDPR במקומות שזו מאפשרת חקיקה מקומית נוספת. נוסף על הרחבת הוראות ה־GDPR, חלקו השלישי של החוק החדש מיישם את דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680),[847] וכולל הוראות להגנת מידע למטרות של אכיפת חוק.[848] היחס בין הוראותיו של ה־BDSG החדש ובין חקיקה פרטנית שנוגעת לפעילותה של סוכנות הביון הפדרלית (BND) והמשטרה הפדרלית (BKA) טרם נבחן.

3.4.3. דיני מעקב מקוון

הניסיון ההיסטורי הגרמני עם גופי ביטחון בעלי עוצמה, כגון הגסטאפו והשטאזי, יש בו כדי להסביר את הרגישות הגרמנית בת זמננו למעקב של כוחות ביטחון ושיטור אחר האזרחים. אבל על עיצובם של כוחות הביטחון הפדרליים – המשטרה הפדרלית (BKA), סוכנות הביון הפדרלית (BND) והמשרד הפדרלי להגנת החוקה – משפיעים גם המתחים בין הממשל הפדרלי ובין האוטונומיה של מדינות הפדרציה.

גורמים אלו הביאו לידי פיתוחו של ה־Trennungsgebot,[849] עקרון ההפרדה בין סוכנויות אכיפת החוק לסוכנויות המודיעין. בין השאר נלקחו מסוכנויות המודיעין סמכויות האכיפה,[850] ועל המשטרה נאסף לאסוף מודיעין. הפרדה זו אינה טריוויאלית, שכן המשטרה נדרשת בחקירותיה לאסוף מודיעין. על אף

847 ראו חלק 3.2.5.2 **לעיל**.

848 ס' 45–85 ל־BDSG החדש.

849 ראו Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 Am. J. Comp. L. 4937 (2007); Codrin Timu and Martin Ibler, *The German Separation between Police and the Offices for the Protection of the Constitution. Legal Framework,* 2016 Rev. Dr. Const. 36 (2016)

850 ראו למשל ס' 1(1) לחוק סוכנויות הביון הפדרלית (BNDG).

הדבקות הפורמלית בו, ובעיקר בשל איום הטרור, מבחינה מעשית עם השנים חלה שחיקה מסוימת בעיקרון זה.[851]

3.4.3.1 סדר הדין הפלילי

התנאים המתירים יירוט תקשורת מוסדרים בקוד סדר הדין הפלילי הגרמני.[852] יירוט תקשורת והקלטתה ללא ידיעת הצדדים לה מותר בתנאי שיש חשד המבוסס על עובדות שפלוני ביצע עבירה חמורה[853] או עבירה נגזרת חמורה, שהיא כבדת משקל גם בנסיבות הפרטיקולריות של הבקשה, ובהיעדר חלופות לא מסובכות לבירור העובדות שבעניין או לאיתור הנאשם.[854] אפשר לתת צו כאמור רק בנוגע לחשוד או בנוגע למי שאפשר להניח שמקבל או משדר תשדורות שמקורן או יעדן הוא החשוד, או בנוגע למי שאפשר להניח שהחשוד משתמש בקו הטלפון שלו.[855] מידע שיורט ונוגע לגרעין הזכות לחיים פרטיים לא יהיה קביל, לא ייעשה בו שימוש, והוא יושמד לאלתר.[856] יירוט תקשורת כאמור יכול להתבצע באמצעות התערבות באמצעים טכניים במערכות ה־IT של מושא המידע, כלומר בשימוש באמצעי סייבר.[857] החוק גם מתיר להשתיל אמצעי מעקב במכשירים ניידים.[858]

851 ראו למשל Gert-Joachim Glaeßner, *A Change of Paradigm? Law and Order, Anti-Terrorism Policies, and Civil Liberties in Germany*, 19 German Politics, 479 487 (2010); Miller, **לעיל** בפרק זה ה"ש 788, בעמ' 8.

852 Strafprozessordnung [StPO] BGBl. I S. 1074, 1319 (להלן: StPO או קוד סדר הדין הפלילי הגרמני).

853 לרשימת העבירות, ראו ס' 100a(2) לקוד סדר הדין הפלילי הגרמני.

854 ס' 100a(1) לקוד סדר הדין הפלילי הגרמני.

855 ס' 100a(3) לקוד סדר הדין הפלילי הגרמני.

856 ס' 100a(4) לקוד סדר הדין הפלילי הגרמני. וראו גם עניין **הציתות** ועניין **מעקב התקשורת המונע**, **לעיל** בפרק זה ה"ש 790.

857 ס' 100a(1) לקוד סדר הדין הפלילי הגרמני.

858 ס' 100i לקוד סדר הדין הפלילי הגרמני.

התביעה הפלילית רשאית לבקש בכתב מתן צו יירוט תקשורת מבית המשפט, ובמקרי חירום רשאית לתת אותו בעצמה, בכפוף לאישור של בית המשפט בתוך שלושה ימי עבודה. הצו יעמוד בתוקף למשך שלושה חודשים, וניתן להאריכו מפעם לפעם בשלושה חודשים ללא הגבלה על התקופה המצטברת. על הצו לפרט את יעד היירוט, את מספר הטלפון או את ציוד הקצה מושאי היירוט, את אמצעי היירוט ואת משכו. מכוח הצו, על כל מי שמספק שירותי טלקומוניקציה לסייע במימושו.[859]

ממשלות המדינות בגרמניה והתובע הכללי חייבים לדווח מדי שנה למשרד המשפטים על השימוש באמצעי יירוט כאמור, ומשרד המשפטים יפרסם באינטרנט את סיכום הדיווחים מהמדינות.[860] כשאין ביידוע כדי לסכן את מטרות החקירה, חיי אדם, את שלמותו הגופנית או את חירותו, חובה ליידע את הנעקבים על השימוש באמצעי היירוט השונים, לרבות השגת נתוני תקשורת. דחייה ביידוע הנעקבים יותר משנה לאחר השלמת המעקב כפופה לאישור של בית המשפט.[861]

הוראות דומות, בשינויים המחייבים, חלות גם על השגה של נתוני תעבורת תקשורת,[862] הטעונה צו מבית המשפט (ובמקרי חירום, באישור בדיעבד של בית המשפט).[863] העבירות שמכוחן בית המשפט רשאי לתת צו להשגת נתוני תעבורת תקשורת הן בעלות חשיבות רבה לחקירה ספציפית, ובייחוד העבירות החמורות המנויות בסעיף(2)100a לקוד סדר הדין הפלילי הגרמני (StPO), או כשפלוני ביצע עבירה באמצעות תקשורת אלקטרונית. הצו יינתן בתנאי שהשגת הנתונים המבוקשים מידתית ביחס לחשיבות החקירה, ובמקרה של ביצוע עבירה באמצעות תקשורת אלקטרונית, לא יימסרו נתוני מיקום בזמן אמת.

859 ס' 100b לקוד סדר הדין הפלילי הגרמני (StPO). ראו גם הנהלים המפורטים בס' 10e לקוד.

860 **שם**.

861 ס' 101 לקוד סדר הדין הפלילי הגרמני (StPO).

862 ראו ס' 96(1), 113a לחוק הטלקומוניקציה הגרמני (TKG).

863 ס' 100g לקוד סדר הדין הפלילי הגרמני (StPO).

3.4.3.2 שימור נתונים ושיתוף פעולה עם סוכנויות ביון וחקירה לפי חוק הטלקומוניקציה הגרמני (TKG)

חוק הטלקומוניקציה הגרמני (TKG), שנועד להסדיר את התחרות בשוק התקשורת הגרמני, כולל הוראות מיוחדות בנוגע לפרטיותם של המשתמשים.[864] החוק מתיר בין השאר לספקים של שירותי תקשורת לאסוף "נתוני מלאי" (Bestandsdaten) – נתונים מזהים שנאספים לצורך התקשרות, יישום, שינוי או סיום היחסים החוזיים בין המשתמשים לספקים – ולהשתמש בהם. בתום השנה הקלנדרית שבה הסתיימו היחסים החוזיים בין משתמש לספק לתכליות תפעוליות, על הספק להשמיד את נתוני המלאי של אותו משתמש.[865] ספק התקשורת גם רשאי לאסוף נתוני תעבורה מתוך רשימה סגורה של סוגי נתונים,[866] ושימוש למטרות אחרות מותנה בהסכמת המשתמש. עיבוד נתוני מיקום של משתמשים מותר רק במידה הנדרשת לסיפוק שירותי תקשורת בעלי ערך מוסף,[867] והדבר מותנה בהסכמת המשתמשים.[868] החוק מאפשר למשתמשים שלא להסכים להעברת נתוני מיקום לשיחות הנעשות למוקדי חירום, על דרך של opt-out.[869]

864 ס' 91–107 לחוק הטלקומוניקציה הגרמני (TKG). הוראות אבטחת מידע מצויות בס' 109–109a לחוק הטלקומוניקציה הגרמני (TKG).

865 ס' 95, 3(3) לחוק הטלקומוניקציה הגרמני (TKG).

866 "נתוני תעבורה", כהגדרתם בס' 3(30) לחוק הטלקומוניקציה הגרמני (TKG), נאספו, עובדו או היו בשימוש במהלך מתן שירותי תקשורת. סוגי נתוני התעבורה המותרים באיסוף לפי ס' 96(1) לחוק הטלקומוניקציה הגרמני (TKG) הם מספר השרתים המעורבים בתקשורת, מזהים אישיים שנעשה בהם שימוש, השימוש בכרטיסי לקוח לרבות מספרם, נתוני מיקום (בעניין שרתי קצה ניידים), זמני השימוש בשירות, נפח הנתונים המשודרים (בתנאי שמחיר השירות תלוי בו), סוג שירות התקשורת, נקודות הקצה של התקשורת (בתנאי שמחיר השירות תלוי בהם) או כל נתון תעבורה אחר הנדרש לצורך קיום התקשורת או לחישוב עלותה למשתמש.

867 "שירותי תקשורת בעלי ערך מוסף" (value-added services) מוגדרים בס' 3(5) לחוק הטלקומוניקציה הגרמני (TKG) שירותים ככל שירות הדרוש איסוף נתוני תעבורה או מיקום ושימוש בהם בהיקף החורג מהנדרש לצורך תשדורת או תשלום בגינו.

868 ס' 98 לחוק הטלקומוניקציה הגרמני (TKG).

869 ס' 108, 98(3) לחוק הטלקומוניקציה הגרמני (TKG). השוו לתזכיר חוק למניעת הטרדות של מוקדי חירום, **להלן** בפרק 4 ה"ש 137.

נוסף על משטר הפרטיות הכללי שחוק הטלקומוניקציה הגרמני (TKG) מחיל על ספקי התקשורת, יש בו כמה הוראות שמקנות לגופי חקירה וביטחון גישה מקוונת לנתונים. ספקי התקשורת נדרשים לוודא, על חשבונם, כי ביכולתם הטכנית להפעיל אמצעי מעקב סטטוטוריים[870] או להסכים להם.[871] על הספקים להעביר לרגולטור (ה־Bundesnetzagentur, הסוכנות הפדרלית המאסדרת את שירותי התקשורת, הגז, החשמל, הדואר והרכבת) מידע הנוגע למבנה מערכות התקשורת שלהם, בכפוף לבקשה בכתב מסוכנות הביון הפדרלית (BND) שמצוין בה כי הדבר נדרש למימוש תכליות סטטוטוריות מסוימות[872] בנוגע לאמצעי מעקב.[873]

ספקי תקשורת נדרשים לאסוף נתוני זיהוי מסוימים[874] ולהעבירם למאגר מידע שמנהל הרגולטור. מאגר מידע זה נועד לאפשר לו לאכוף את דיני התחרות, אבל גם לספק מענה ממוכן לבקשות למידע של רשויות אחרות, בכללן משרדי ההגנה על החוקה, סוכנות הביון הפדרלית (BND), בתי המשפט וסוכנויות אכיפת החוק, המשטרות הפדרליות והמדינתיות, משטרת המכס ומוקדי החירום.[875] תקנות נתוני לקוחות[876] שהותקנו מכוח חוק הטלקומוניקציה הגרמני (TKG) אינן כוללות מגבלות מהותיות על בקשות לקבלת מידע ממאגר נתוני הזיהוי.

870 ס' 110 לחוק הטלקומוניקציה הגרמני (TKG).

871 ס' 110(5)(1a) לחוק הטלקומוניקציה הגרמני (TKG) מפנה לאמצעי המעקב לפי ס' 5, 8 לחוק סעיף 10 (G10), ולס' 6, 12, 14 לחוק סוכנות הביון הפדרלית (BNDG) (ראו חלקים 3.4.3.4 ו־3.4.3.5 **להלן**).

872 ראו ס' 5, 8 בחוק סעיף 10 (G10), וס' 6, 12, 14 בחוק סוכנות הביון הפדרלית (BNDG)

873 ס' 114 לחוק הטלקומוניקציה הגרמני (TKG).

874 מספרי טלפון ומזהי חיבור אחרים, שם וכתובת המנוי, תאריך לידה וכתובת החיבור (אם מדובר בחיבור קבוע לשירות).

875 ס' 112 לחוק הטלקומוניקציה הגרמני (TKG).

876 Kundendatenauskunftsverordnung (14.06.2017), BGBl. I S. 1667, 3343

לצד ההליך האוטומטי להשגת נתוני לקוח, רשויות התביעה, הרשויות האחראיות למניעת איומים על ביטחון הציבור ועל הסדר הציבורי וארגוני המודיעין (סוכנות הביון הפדרלית (BND), המודיעין הצבאי ומשרדי ההגנה על החוקה) רשאים לבקש בכתב מספקי תקשורת לקבל נתוני מלאי נוספים על אלו המצויים במאגר. נתונים אלו יועברו לידי המבקש, ובתנאי שהדבר נעשה לתכליות של מניעת איומים על ביטחון הציבור ועל הסדר הציבורי, או לשם מימוש מטרותיהם הסטטוטוריות של ארגוני המודיעין, לפי העניין.[877]

חוק הטלקומוניקציה הגרמני (TKG) מורה לספקי תקשורת לשמור נתוני מיקום לתקופה של ארבעה שבועות, ונתוני תעבורה מסוימים[878] – למשך עשרה שבועות.[879] ניתן להעביר נתונים אלו לרשויות אכיפת החוק בכפוף להוראה סטטוטורית שמתירה למבקש לאסוף נתונים אלו בקשר לפשעים חמורים במיוחד; לסוכנויות ביטחון מדינתיות, בכפוף להוראה סטטוטורית המתירה למבקש לאסוף נתונים אלו על מנת למנוע סכנה ספציפית לחייו, לגופו או לחירותו של אדם או לקיומה של הממשלה הפדרלית.

עם זאת הסדר שימור הנתונים בחוק הותקף בבית המשפט הגבוה לעניינים מינהליים במדינת נורדריין-וסטפאליה בטענה שהוא אינו תואם את פסק הדין של בית הדין האירופי לצדק (ECJ) בעניין *Tele2 Sverige AB*.[880] הערכאה הגרמנית מצאה כי החוק הגרמני אכן אינו עומד בדרישות שקבע בית הדין האירופי בעניין זה שכן הוא מתיר שימור גורף וחסר הבחנה, ופטרה את התובע – ספק שירותי תקשורת ממינכן[881] – מהחובה לעמוד בהוראות החוק הטלקומוניקציה הגרמני (TKG) לעניין

877 ס' 113 לחוק הטלקומוניקציה הגרמני (TKG).

878 ס' 113b(2) לחוק הטלקומוניקציה הגרמני (TKG) מונה בתוכם את מספר הטלפון או מזהה אחר של השיחה, תחילתה וסיומה, סוג שירות התקשורת, מספר מזהה בין־לאומי של הצדדים לשיחה ופרוטוקול האינטרנט שבו בוצעה השיחה, לפי העניין.

879 ס' 113 לחוק הטלקומוניקציה הגרמני (TKG).

880 ראו עניין *Tele2 Sverige AB*, **לעיל** בפרק זה ה"ש 228.

881 ראו Simon Assion and Sven-Erik Heun, *German Traffic Data Retention Law considered invalid by Higher Administrative Court of North Rhine-Westphalia* (26.07.2017)

שימור נתונים. הרגולטור הודיע כי הוראות סעיף 113b לחוק הטלקומוניקציה הגרמני לא ייאכפו על ספקי תקשורת אחרים עד החלטה עקרונית בעניין.[882]

3.4.3.3 חוק ההגבלות על הפרטיות בהתכתבות, בדברי דואר ובתקשורת אלקטרונית (חוק סעיף 10, G10)

חוק סעיף 10 (G10) – או חוק ההגבלות על הפרטיות בהתכתבות, בדברי דואר ובתקשורת אלקטרונית – נועד להסדיר את סמכויות המעקב הכלליות של סוכנויות המודיעין הגרמניות (המשרדים להגנה על החוקה, סוכנות הביון הפדרלית (BND) והמודיעין הצבאי (הגופים המוסמכים)). חוק סעיף 10 מתיר לסוכנויות מודיעין אלו לנטר ולשמור תשדורות לתכליות של מניעת איומים על הסדר הציבורי החופשי והדמוקרטי או להגנה על הקיום או הביטחון של הפדרציה או של מדינה ממדינותיה, לרבות ביטחון הכוחות של מדינות נאט"ו המוצבים בגרמניה.[883] סוכנות הביון (BND) רשאית להשתתף במעקבים אלו במסגרת מילוי תפקידה לפי חוק סוכנות הביון הפדרלית (BNDG – Gesetz über den Bundesnachrichtendienst)[884] ולתכליות המנויות בסעיף 5 לחוק סעיף 10 (G10), המתירות מעקבים אסטרטגיים (ראו להלן). לפי חוק זה ספקי שירותי תקשורת נדרשים לספק מידע תקשורת מושא צו ולאפשר לגופים המוסמכים לעקוב אחריהם ולנטרם.[885]

חוק סעיף 10 (G10) מבחין בין מעקב אינדיווידואלי אחרי יעד מודיעיני ובין מעקב אסטרטגי – יירוט של "חבילות תקשורת" (Gebündelte Übertragung) שאינו מגדיר יעד מודיעיני ספציפי. מעקב אינדיווידואלי יותר במקרים שבהם יש חשד

882 לדיווח על המקרה, ראו Julian Von Lucius, *Data Retention: Bundesnetzagentur Stops Enforcement after Ruling by Higher Administrative Court*, Noerr (29.06.2017)

883 ס' 1 לחוק סעיף 10 (G10).

884 Gesetz über den Bundesnachrichtendienst [BNDG]§1(2) BGB I.S. 2954 2979 (להלן: BNDG או **חוק סוכנות הביון הפדרלית**), שלפיו ה־BND אוסף ומעריך את המידע הנדרש על מדינות זרות למטרות של מדיניות חוץ וביטחון של הרפובליקה הפדרלית הגרמנית.

885 ס' 2 לחוק סעיף 10 (G10).

ממשי לביצוע עבירות שונות, בכללן בגידה, סיכון הדמוקרטיה החוקתית, פגיעה בביטחון הלאומי, פגיעה בביטחונם של כוחות נאט"ו זרים בגרמניה, עבירות טרור ופשעי שנאה, או עבירות אלימות אם הן נגד החוקה או נגד קיומה או ביטחונה של הפדרציה או מדינה ממדינותיה.[886] ראיות שנאספו באמצעות מעקב אינדיווידואלי שיש בהן משום פגיעה בגרעין הזכות להגנה על החיים הפרטיים לא יהיו קבילות בבית משפט, וכשמדובר בהקלטה אוטומטית יש להפסיקה אם יש אינדיקציה לפגיעה כזו.[887] הגוף שאסף את המידע יבחן מדי חצי שנה אם שימורו נדרש לתכליות המותרות בחוק, ואם לא – יבערו בהשגחת אדם המוסמך להחזיק במשרה שיפוטית. העברת המידע שנשמר לגופים אחרים מותרת רק למטרות של מניעת העבירות שנמנו לעיל או למטרות הקשורות להוצאתן מחוץ לחוק של מפלגות המסכנות את הסדר הדמוקרטי הבסיסי בגרמניה.[888]

סוכנות הביון הפדרלית (BND) רשאית לבקש צו למעקב אסטרטגי אחר "חבילות" של תקשורת בין־לאומית, ובתנאי שהאיסוף נדרש כדי למנוע סכנה של מתקפה חמושה על הרפובליקה הפדרלית הגרמנית, מתקפות טרור בין־לאומי שמכוונות ישירות לרפובליקה, הפצת אמצעי לחימה, מקרים בולטים של הפצה מסחרית לא מאושרת של סמים נרקוטיים לשטחי האיחוד האירופי או במסגרת פשיעה מאורגנת, ערעור היציבות המוניטרית של גוש האירו באמצעות מעשי זיוף מעבר לים, מקרים חמורים של הלבנת הון בין־לאומית מאורגנת, סוגים מסוימים של סחר בבני אדם ותקיפות סייבר בין־לאומיות של גופי טרור או פשיעה.[889] ההגנות החלות על גרעין הזכות לחיים פרטיים במסגרת מעקבים אינדיווידואליים[890] יחולו בשינויים המתאימים גם על מעקבים אסטרטגיים.[891]

886 ס' 3(1) לחוק סעיף 10 (G10).

887 ס' 3a לחוק סעיף 10 (G10).

888 ס' 4 לחוק סעיף 10 (G10). להוראה החוקתית בנוגע להוצאת מפלגות מחוץ לחוק, ראו ס' 21 לחוק היסוד הגרמני.

889 ס' 5(1) לחוק סעיף 10 (G10).

890 ס' 3a לחוק סעיף 10 (G10).

891 ס' 5a לחוק סעיף 10 (G10).

בנוגע לתקשורת אלקטרונית, סוכנות הביון הפדרלית (BND) רשאית להשתמש במילות החיפוש המוגדרות בצו, אך אין להשתמש במילות חיפוש שיובילו לאיסוף ממוקד של תקשורת אלקטרונית מסוימת, או כאלה שנוגעות לגרעין הזכות לחיים פרטיים. מגבלות אלה אינן חלות אם מדובר בתקשורת שהמשתמשים הקבועים בה או בעליה לבטח אינם גרמנים.[892] יוער כי הממשלה הפדרלית הפרידה בין מעקב אסטרטגי בעל זיקה טריטוריאלית או פרסונלית לגרמניה – שעליו חלות ההגנות של סעיף 10 לחוק היסוד הגרמני ומשכך גם הוראות חוק סעיף 10 (G10) ביחס למעקב אסטרטגי – ובין מעקב אסטרטגי חסר זיקה כזו (Ausland-Ausland-Fernmeldeaufklärung), שעליו לכאורה לא חלות ההגנות החוקתיות וההסדרים שבחוק סעיף 10 (G10), אלא ההוראות שבחוק סוכנות הביון הפדרלית (BNDG).[893]

לתכליות של זיהויה מבעוד מועד של סכנה לחייו או לגופו של אדם מחוץ לגבולות גרמניה, שיש בה כדי להשפיע במיוחד על האינטרסים של הרפובליקה הפדרלית הגרמנית, מותר לנקוט מעקב אסטרטגי, בתנאי שוועדת הביקורת הפרלמנטרית (ראו להלן) אישרה זאת ברוב של שני שלישים, ולמשך חודשיים (ניתן לחדשה בתנאי שהתנאים עדיין עומדים בתוקפם). במקרים כאלו ניתן להשתמש במילות חיפוש שיש בהן כדי לזהות את אותו אדם.[894]

מעקב אסטרטגי או מעקב אינדיווידואלי מותנים בבקשה לצו שיפנו בכתב סוכנויות המודיעין הרלוונטיות למשרד הפנים הפדרלי (ובמקרה של הרשויות המדינתיות להגנה על החוקה, למשרד הפנים המדינתי המקביל לו), בכפוף לאישור ועדת סעיף 10 (ראו להלן). הבקשות יפרטו את היעדים המודיעיניים למעקב, את אופיו, את היקפו ואת משכו. בקשות לחיפוש אינדיווידואלי או לחיפוש אסטרטגי במצב של סכנה לחיי אדם יאושרו רק אם אין דרך אחרת להשיג את המידע.

892 ס' 5(2) לחוק סעיף 10 (G10).

893 ראו חלק 3.4.3.4 **להלן**.

894 ס' 8 לחוק סעיף 10 (G10).

עם סיומו של מעקב אינדיווידואלי יש ליידע את היעד המודיעיני שלו על ביצוע המעקב, אלא אם היידוע מאיים על תכלית המעקב. אם לא מומשה זכות היידוע בתוך שנה, כל דחייה נוספת כרוכה באישורה של ועדת סעיף 10 (ראו להלן).[895] אין לפתוח בהליכים משפטיים נגד צו המאשר מעקב כאמור טרם יידוע מושאו.[896]

משרד הפנים ידווח לוועדת הביקורת הפרלמנטרית ליישומו של חוק סעיף 10 מדי שישה חודשים על יישום הוראות החוק, וזו תדווח לבית הנבחרים.[897] לצד ועדת הביקורת הפרלמנטרית הקים החוק את ועדת סעיף 10 (G10-Kommission).[898] בוועדת סעיף 10 מכהנים שמונה חברים, ובראשם שופט, שאותם ממנה לתקופה קצובה ועדת הבקרה הפרלמנטרית על סוכנויות המודיעין הפדרליות (PKgR).

ועדת סעיף 10 אינה גוף שיפוטי (ראו ס׳ 10(2) סיפה לחוק היסוד, המתיר זאת). תחומי אחריותה משתרעים על כל היבט של חדירה לתחומים המוגנים בסעיף 10 לחוק היסוד – איסוף, ניתוח והעברה של נתוני תקשורת מזהים, וכן שימוש בהם.[899] על המשרד הפדרלי האחראי לדווח מדי חודש לוועדת סעיף 10 על אמצעי המעקב שעליהם הורה בצו בטרם הפעלתם (במקרה של סכנה ממשית ניתן להתחיל באיסוף ביום הגשת הבקשה, אך להשתמש בו רק לאחר מתן הצו), והוועדה יכולה להורות על בטלותם.[900]

מילר מצביע על היקף הבקשות לאישור אמצעי מעקב שהוגשו לוועדה בשנת 2013 כאינדיקציה אפשרית למידת האפקטיביות של הבקרה שהוועדה מפעילה, ומציין שלפי אחד הדיווחים בתקשורת, הקדישה הוועדה חמש דקות לכל צו.[901] יתר על כן, על אף הגישה הרחבה לעבודת המודיעין הגרמני שחוק סעיף 10 (G10) מקנה לוועדה, תקציבהּ ומצבת כוח האדם הצנועים שלה עשויים להצביע

895 ס' 12 לחוק סעיף 10 (G10).

896 ס' 13 לחוק סעיף 10 (G10).

897 ס' 14 לחוק סעיף 10 (G10).

898 ס' 15 לחוק סעיף 10 (G10).

899 ס' 15(5) לחוק סעיף 10 (G10).

900 ס' 15(6) לחוק סעיף 10 (G10).

901 ראו Miller, **לעיל** בפרק זה ה"ש 793, בעמ' 268–269.

על מיצוי חסר של סמכויותיה.[902] עם זאת בעניין *Klass*[903] ומאוחר יותר בעניין *Weber*[904] מצא בית הדין האירופי לזכויות אדם (ECtHR) שהסדרי הבקרה של ועדת סעיף 10 נאותים, וכי אין צורך בביקורת שיפוטית כדי שהחוק הגרמני יהלום את הוראות הדין האירופי, במיוחד בשים לב לעצמאותה של הוועדה.

3.4.3.4 חוק סוכנות הביון הפדרלית (BNDG)

כאמור למעלה, פעילות המעקב (האסטרטגי או האינדיווידואלי) של סוכנות הביון הפדרלית (BND) שלה זיקה (טריטוריאלית או פרסונלית, לפי העניין) לגרמניה, מוסדרת בחוק סעיף 10 (G10). מנגד, פרקטיקות של מעקב אחר תוכן של תקשורת נתונים ללא זיקה טריטוריאלית לגרמניה, שכל הצדדים לה אינם גרמנים, וכן פעילויות איסוף כללי (איסוף גורף – bulk data acquisition) וסייבר של סוכנות הביון הפדרלית (BND) לא הוסדרו בחקיקה, אלא בכללים סודיים.[905] חוק סוכנות הביון הפדרלית (BNDG) מסדיר את הכללים החלים בעניין מעקב אסטרטגי זר.

מלומדים רבים טענו כי הבחנתה של ממשלת גרמניה בין מעקב אסטרטגי זר למעקב אסטרטגי מקומי אינה ראויה, וכי פרקטיקות המעקב האסטרטגי הזר לפי ה־BNDG אינן חוקתיות. לטענתם מבחינה טכנית יש מקום להניח שתקשורת בעלת זיקה לגרמניה תמצא את דרכה לשרתים בין־לאומיים מחוץ לגרמניה ותימצא בחבילות התקשורת המיורטות. עוד טענו המתנגדים להבחנה כי סמכויות המדינה נדרשות לכבד את סעיף 10 לחוק היסוד, שלפי פרשנויות מסוימות מגן גם על מי שאינם גרמנים ומצויים מחוץ לגבולות הרפובליקה הפדרלית של גרמניה.[906]

902 **שם**. לביקורת נוספת, ראו גם Jan-Hendrik Dietrich, *Of Toothless Windbags, Blind Guardians and Blunt Swords: The Ongoing Controversy about the Reform of Intelligence Services Oversight In Germany* 31 Intelligence and Nat. Sec. 397 (2016)

903 ראו **לעיל** בפרק זה ה"ש 227.

904 ראו **לעיל** בפרק זה ה"ש 227.

905 Thorsten Wetzling, *Germany's Intelligence Reform: More surveillance, Modest Restraints and Inefficient Controls* 4 (16.06.2017)

906 ראו Miller, **לעיל** בפרק זה ה"ש 793, בעמ' 274-273; Wetzling, **לעיל** בפרק זה ה"ש 905.

הרפורמה שערכה הממשלה הפדרלית בחוק סוכנות הביון הפדרלית (BNDG) בשנת 2016 לא אימצה השקפה זו, ובמקום זאת טענה הממשלה כי הזכות המוגנת בסעיף 10 לחוק היסוד ניתנת להגבלה טריטוריאלית.

עם זאת הרפורמה של 2016 הציגה כללים חדשים, שהחילו בקרות חדשות על מעקב אסטרטגי זר לצד איסוף לא מוגבל של נתוני תקשורת. החוק מבחין בין גרמנים (אזרחים, תושבים ומי שמצויים בגבולותיה של גרמניה, וכן ישויות משפטיות גרמניות), שעליהם חלות ההוראות של חוק סעיף 10 (G10) (ה־BNDG אינו חל עליהם),[907] ובין אזרחי האיחוד ומוסדותיו, שעליהם חלות הגנות חלשות יותר. על מידע שאינו נופל בגדר קטגוריות אלו חל המשטר המקל ביותר בעניין מונחי החיפוש המותרים בו.

לשם מילוי תפקידיה[908] רשאית סוכנות הביון הפדרלית (BND) לנקוט אמצעים טכניים לאיסוף מידע ולעיבודו, לרבות נתוני תקשורת אלקטרונית בין־לאומית ולרבות מידע שמקורו ברשתות תקשורת אלקטרונית זרות, אם הדבר נחוץ לזיהוי ולמניעה מוקדמת של איומים מבית ומחוץ לביטחונה של הרפובליקה הפדרלית של גרמניה, לשמירה על יכולתה של הרפובליקה לפעול או לצורך ממצאים אחרים בעלי חשיבות דיפלומטית או ביטחונית.[909] החוק אוסר במפורש על ביצוע מעקב תקשורת זרה לתכליות של ריגול תעשייתי.[910]

האיסוף יתבצע רק מתוך רשתות תקשורת שהוגדרו בצו, ואיסוף של נתוני תוכן של תקשורת זרה (Ausland-Ausland) ייעשה אך ורק באמצעות מילות חיפוש המתאימות למטרות האיסוף המותרות.[911] אם הדבר הכרחי לזיהוי עבירות המנויות בחוק סעיף 10 (G10),[912] ניתן להשתמש במילות חיפוש הקשורות

907 ס' 6(4) לחוק סוכנות הביון הפדרלית (BNDG).

908 ס' 1(2) לחוק סוכנות הביון הפדרלית (BNDG).

909 ס' 6(1) לחוק סוכנות הביון הפדרלית (BNDG).

910 ס' 6(5) לחוק סוכנות הביון הפדרלית (BNDG).

911 ס' 6(2) לחוק סוכנות הביון הפדרלית (BNDG).

912 ס' 3(1) לחוק סעיף 10 (G10).

לאזרחי האיחוד האירופי ומוסדותיו.[913] ה־BNDG מורה במפורש שיש להגן על גרעין הזכות לחיים פרטיים, וכשאמצעי מעקב כאמור מספק תובנות בנוגע לגרעין הזכות לפרטיות, אמצעי זה אינו קביל, אין להשתמש בו, ויש להשמיד לאלתר כל נתון שהתקבל באמצעותו.[914]

צו המורה על מעקב כאמור יינתן מאת משרד הקנצלר, לבקשתו של ראש שירות המודיעין הפדרלי.[915] תוקף הצווים המרבי יהיה למשך שישה חודשים, והם יהיו ניתנים להארכה כל עוד התנאים המאפשרים אותם מוסיפים להתקיים.[916] משרד הקנצלר ידווח לוועדה העצמאית (Unabhängige Gremium) – גוף בקרה שהוקם ברפורמת 2016 – על הצווים שניתנו, וזו רשאית להורות על ביטולם לאלתר. הוועדה, המתכנסת מדי שלושה חודשים לפחות, כוללת שלושה חברים ושלושה סגנים להם, שאותם ממנה הקבינט. על נשיא הוועדה ועל חבר נוסף בה להיות שופטים פדרליים, ועל החבר השלישי להיות תובע פדרלי.[917]

לא ברור אם סמכויותיה של הוועדה העצמאית יהיו רחבות כשל ועדת סעיף 10, המשתרעות אל מעבר לבקרה מעין־שיפוטית של צווי מעקב. מלומדים מעירים על המשך הפרגמנטציה של מערך הביקורת על גופי המודיעין הגרמניים ועל אינדיקציות להיעדר עצמאות של הוועדה (שאותה ממנים גורמים ברשות המבצעת).[918]

3.4.3.5 חוק המשטרה הפדרלית של גרמניה (BKAG)

סמכויותיה של המשטרה הפדרלית (BKA) מוגדרות בחוק המשטרה הפדרלית של גרמניה (BKAG — Bundeskriminalamtgesetz),[919] שתוקן לאחרונה בעקבות

913 ס' 6(3),7(2) לחוק סוכנות הביון הפדרלית (BNDG).

914 ס' 11 לחוק סוכנות הביון הפדרלית (BNDG).

915 ס' 9(1)–(2) לחוק סוכנות הביון הפדרלית (BNDG).

916 ס' 9(3) לחוק סוכנות הביון הפדרלית (BNDG).

917 ס' 16 לחוק סוכנות הביון הפדרלית (BNDG).

918 Wetzling, **לעיל** בפרק זה ה"ש 905, בעמ' 20–22.

919 Bundeskriminalamtgesetz vom (7.7.1997) (BGBl. I S. 1650), as amended by Article 2 of (1.6.2017) (BGBl. I S. 1354) (להלן: BKAG או חוק המשטרה הפדרלית).

החלטת בית המשפט בעניין חוק זה (להלן: עניין **חוק ה־BKA**).[920] סמכותה המקורית של המשטרה הפדרלית בגרמניה שלאחר מלחמת העולם השנייה הייתה שיורית – התמודדות עם פשיעה שזיקתה הטריטוריאלית אינה מוגבלת למדינה-חברה אחת בפדרציה.[921] באותה תקופה הדהד ביזור הסמכויות את המחויבות הגרמנית לפדרליזם אדמיניסטרטיבי, שלפיו הפדרציה אחראית בעיקר לחקיקה; והמדינות, על הרשויות הציבוריות שבתוכן, ליישומה.[922]

חוק המשטרה הפדרלית (BKAG) תוקן בשנות השבעים כדי להתמודד עם הטרור משמאל של סיעת הצבא האדום. החוק הרחיב את סמכויותיה של המשטרה הפדרלית (BKA) והסמיך אותה גם לחקור ולנהל חומרי חקירה בפשעים מסוימים. תיקון נוסף, שנעשה בשלהי שנות התשעים, הסמיך אותה לאסוף מידע אישי, לשומרו, להשתמש בו ולהעבירו, בכפוף לבקרות מסוימות ולמשטר הגנת מידע. בעשור הראשון של שנות האלפיים – בעקבות אירועי 11 בספטמבר – תוקן החוק כדי לאפשר הרחבה נוספת של סמכויותיה, אם כי גם ברפורמה זו לא היה כדי לשנות את קדימות המשטרות המקומיות על פני המשטרה הפדרלית באכיפת החוק הפלילי.[923]

רפורמה חשובה בחוק המשטרה הפדרלית (BKAG) נעשתה בשלהי 2008, אז נוספו לחוק המקורי כשלושים סעיפים, בכללם, כפי שיתואר להלן, סעיפים שמסמיכים אותה לנקוט אמצעי איסוף מיוחדים,[924] לבצע פעולות כריית מידע, לנקוט באמצעי סייבר ואיסוף נתונים ממערכות IT, וכן סמכויות לאסוף תקשורת אלקטרונית,

920 עניין **חוק ה־BKA**, **לעיל** בפרק זה ה"ש 790, בפס' 357.

921 ראו Miller, **לעיל** בפרק זה ה"ש 788, בעמ' 4.

922 ראו Kommers & Miller, **לעיל** בפרק זה ה"ש 783, בעמ' 114–115, 120, 144; Arthur Gunlicks, The Länder and German Federalism 5, 61, 344 (2003)

923 ראו Miller, **לעיל** בפרק זה ה"ש 788, בעמ' 5–6.

924 ס' 20g לחוק המשטרה הפדרלית (BKAG). אמצעי איסוף מיוחדים הם מעקב פיזי רגיל, אמצעים טכנולוגיים המאפשרים מעקב מחוץ לבית, וכן שימוש במודיעים ובסוכנים סמויים.

לרבות נתוני תוכן ונתוני תקשורת. בעקבות פסק הדין בעניין **חוק ה־BKA**[925] הוכנסו כמה שינויים לחוק.

המשטרה הפדרלית (BKA) רשאית לאסוף מידע אישי לפי חוק הטלקומוניקציה הגרמני (TKG)[926] למטרות של מניעת עבירות טרור, בתנאי שיש עבירה קונקרטית ויעד האיסוף עומד לבצע אותה, או שהוא מצוי בקשר שאינו מזדמן עם מי שעומד לבצע אותה ומודע לה, או עשוי להיות מעורב בה.[927]

סמכויות כריית מידע (Rasterfahndung)[928] המסורות לפי החוק בידי המשטרה הפדרלית (BKA) מתירות לה לבקש מבית המשפט צו לקבלת מידע מגופים ציבוריים או שאינם ציבוריים למטרות של השוואה אוטומטית למאגרי מידע אחרים כדי למנוע סכנה לקיומה או לביטחונה של המדינה או לחייו או לגופו של אדם או לרכוש בעל ערך רב, ובתנאי שקבלת מידע זה נדרשת לשם אינטרס ציבורי, ושבלעדי אמצעי זה יהיה קשה מאוד או בלתי אפשרי להשיג את המידע המבוקש. סמכות זו אינה מסורה למודיעין הצבאי, לסוכנות הביון הפדרלית (BND) או למשרדי ההגנה על החוקה.[929]

המשטרה הפדרלית (BKA) רשאי לנקוט פעולות סייבר (או הפרעה מכוונת למערכות IT) כדי לאסוף נתונים כשקיים בסיס עובדתי לחשש לסיכון חייו, גופו או חירותו של אדם, או סיכון לטובין ציבוריים שנוגע ביסודות קיום המדינה או הקיום האנושי. יש להבטיח כי במסגרת פעולות הסייבר ייעשו במערכות ה־IT רק שינויים הכרחיים לאיסוף המידע המבוקש, וכי יהיה ניתן להשיב את המצב לקדמותו אוטומטית בתום האיסוף.[930] פעולות סייבר מותרות לפי צו שייתן בית המשפט בעקבות בקשה בכתב

925 עניין **חוק ה־BKA**, **לעיל** בפרק זה ה"ש 790.

926 ראו **לעיל** בחלק 3.4.3.2.

927 ס' 20 לחוק המשטרה הפדרלית (BKAG).

928 ראו בחלק 3.4.1 **לעיל**, המתאר את עניין **סינון המידע**.

929 ס' 20j לחוק המשטרה הפדרלית (BKAG).

930 לאחרונה דווח כי משטרת גרמניה נעזרה בחברת פצחנות פרטית כדי לפרוץ למכשיר האייפון של צעיר החשוד ברצח. במקרה זה הוצלבו נתוני מיקום עם נתונים מרחביים שנאספים באמצעות אפליקציית הבריאות של אפל כדי לאשש את החשד כי החשוד עלה וירד במדרגות בזמן שנפטר מהגופה. ראו: *Apple Health Data Used in Murder Trial*, BBC, (12.1.2018)

מנשיא המשטרה הפדרלית (BKA) או מנציגו, ושיעמוד בתוקפו לא יותר משלושה חודשים. מידע שנוגע לגרעין של הזכות לחיים פרטיים לא יהיה קביל, ויש לוודא כי במידת האפשר לא ייאסף מידע כזה.[931]

יירוט של נתוני תקשורת ונתוני תוכן מכוח חוק המשטרה הפדרלית (BKAG) נועד למנוע סכנה לקיומה או לביטחונה של המדינה או לחייו או לגופו של אדם או לרכוש בעל ערך רב או כדי למנוע עבירות טרור. פעולות יירוט (הן של נתוני תוכן והן של נתוני תעבורה) מותנות בקבלת צו מבית המשפט בעקבות בקשה בכתב שהגיש נשיא המשטרה הפדרלית (BKA) או נציגו.[932] אישור בקשת היירוט מותנה בכך שבלעדי אמצעי זה יהיה קשה מאוד או בלתי אפשרי להשיג את המידע המבוקש.

פסק הדין בעניין **חוק ה־BKA**[933] קבע כי בעיקרון הסמכתה של המשטרה הפדרלית לנקוט את אמצעי המעקב החשאיים שברפורמת 2008 היא חוקתית. עם זאת היו מקרים שבהם מצא בית המשפט כי דקויות מסוימות בעיצובם של הסדרים קונקרטיים להפעלתם אינן מידתיות. כך למשל באשר לחלק מההוראות החלות על פעולות סייבר ועל יירוט תקשורת נקבע כי הן אינן חוקתיות למרות הניסיון להתאים אותן לסטנדרט הפסיקתי הרלוונטי שנקבע בעניין **המעקב המקוון**.[934] הוראות אחרות בנוגע להעברת מידע, שמירתו וביעורו, גם הן נמצאו לא חוקתיות. מילר טוען כי אף שהציבור קיבל את פסק הדין בחיוב, הזכות לפרטיות במובנה הרחב נזנחה בו לטובת מראית העין של ההגנה עליה בדרך של דיון דקדקני בפרטיהן של הוראות מחיקה ותיעוד של מעקבים. רוב הסמכויות לעומת זה נותרו בעינן.[935]

931 ס' 20k לחוק המשטרה הפדרלית (BKAG).

932 ס' 20l–m לחוק המשטרה הפדרלית (BKAG).

933 עניין **חוק ה־BKA**, **לעיל** בפרק זה ה"ש 790. להרחבה, ראו Miller, **לעיל** בפרק זה ה"ש 788.

934 עניין **המעקב המקוון**, **לעיל** בפרק זה ה"ש 786.

935 Miller, **לעיל** בפרק זה ה"ש 788, בחלק IV.

• הדינים הגרמניים בדבר מעקב מקוון מבחינים בין פרקטיקות איסוף ועיבוד נתונים לתכליות של מניעת פשע ואכיפת חוק, המוסדרות בקוד סדר הדין הפלילי (StPO), ובין פרקטיקות שתכליתן ביטחונית.

• יירוט והשגה של נתוני תוכן ונתוני תקשורת למטרות של אכיפת פשיעה (עבירות חמורות) טעונים צו מאת בית המשפט.

• למשטרה הפדרלית של גרמניה (BKA) מותר ליירט ולהשיג נתוני תוכן לתכליות של מניעת פשיעה פדרלית וטיפול בעבירות טרור וכן לקבל מידע לצורכי כר"מ ופעולות סייבר בכפוף לצו מאת בית המשפט.

• לסוכנות הביון הפדרלית הגרמנית (BND) מותר לעסוק במעקב מקוון לתכליות של מניעת איומים על הסדר החופשי והדמוקרטי או על ביטחון הפדרציה הגרמנית, בכפוף לצו ממשרד הפנים הפדרלי, שאותו מאשרת בדיעבד ועדת סעיף 10 – גוף ביקורת מעין־שיפוטי.

• ההסדרים בחוק הגרמני מבחינים בין מעקב ממוקד ל"מעקב אסטרטגי", בהיעדר יעד מודיעיני קונקרטי; ובין מעקב אסטרטגי בעל זיקה טריטוריאלית או פרסונלית לגרמניה, למעקב אסטרטגי שנעדר זיקה זו. מעקב אסטרטגי חסר זיקה לגרמניה (Ausland-Ausland-Fernmeldeaufklärung) נעשה בכפוף לצו מאת הקנצלר, אותו מאשרת או מבטלת בדיעבד ועדה עצמאית.

3.5. הודו

בהודו, בדומה לישראל, רוב האוכלוסייה היא חלק מקהילה דתית דומיננטית (הינדית ויהודית בהתאמה), שרואה בעצמה "אומת ליבה" (core nation).[936]

936 איילת הראל־שלו ושרינה חן, "ישראל והודו בין דמוקרטיה ללאומנות – דואליות נורמטיבית בחברות שסועות" **תיאוריה וביקורת** 44, 151–175, 152 (2015).

שתי המדינות מתמודדות עם טרור אתני/דתי,[937] ושיטות המשפט של שתיהן ירשו שכבה של דין קולוניאלי/מנדטורי, לרבות הדינים שנועדו להתמודדות עם טרור. כך למשל בשתי המדינות נותרה חקיקת החירום המנדטורית על כנה עשרות שנים לאחר עזיבת הבריטים, עד שהוסדרה מחדש בחקיקת אנטי־טרור.[938] בחינת האופן שבו – אם בכלל – דיני המעקב המקוון ההודיים מאזנים אינטרסים של ביטחון לאומי עם הזכות לפרטיות הייתה עשויה לסייע בחידוד ההבנה של סוגיות דומות בדין הישראלי.

ואולם דיני הגנת הפרטיות ההודיים אינם מפותחים די הצורך. כמעט שאין בנמצא חקיקה המוקדשת להגנת הפרטיות או להגנת מידע,[939] וההכרה בזכות לפרטיות כזכות יסוד חוקתית נעשתה רק לאחרונה.[940] היעדר הסדרה מלאה של תחומים אלה מפליא עוד יותר בהתחשב בזינוק הכלכלי של הודו בתחומי טכנולוגיית מידע וניהול המוצרים העסקיים (BPM – business product management) ובגידול בהשקעות הזרות (בעיקר למטרות של מיקור חוץ),[941] המצריכים תשתית משפטית נאותה להגנה על מידע אישי. ואכן, בהעדרהּ של תשתית כזו סירב האיחוד האירופי להכיר בדין ההודי ככזה המעניק רמת הגנה נאותה למושאי המידע.[942] בו בזמן בשנים האחרונות ממשלת הודו פועלת

937 Wasbir Hussain, Ethno-Nationalism and the Politics of Terror in India's Northeast, South Asia: J. of South Asian Studies 30 93-110 (2007); Rohan Mukherjee & David M. Malone, Indian Foreign Policy and Contemporary Security Challenges, International Affairs 87 87-104 91-92 (2011)

938 יעל ברדה, "ניהול 'אוכלוסיות מסוכנות': מפרקטיקות חירום קולוניאליות לחוקי המאבק בטרור בהודו ובישראל" **תיאוריה וביקורת** 44 97-126 (2015).

939 למעט הוראות מסוימות בכלל 419 לכללי חוק הטלגרף ההודי, ראו חלק 3.5.2.2 להלן.

940 בעניין Justice K.S. Puttaswamy (Retd.) & Another v. Union of India S.C.C. 494 of 2012 (24.8.2017)

941 NASSCOM, *The IT-BPM: Strategic Review 2015* (2015)

942 Nayamina Basu, *Data Adequacy Grant to India Non-Negotiable, Says EU Envoy*, Business Standard (17.05.2013); השוו להחלטת האיחוד בעניין ישראל, **לעיל** בפרק זה ה"ש 266.

ביתר שאת להצגה של מערכות מעקב וניטור שהתשתית החוקית לפריסתן כמעט שאיננה קיימת.

3.5.1. מעטפת חוקתית ופרטיות יצירת הפסיקה

החוקה ההודית אינה מכירה במפורש בזכות לפרטיות. עם זאת סעיף 21 לחוקה ההודית קובע כי הגבלת זכות הפרט לחירות אישית או לחיים לא תיעשה אלא בנוהל מכוח הדין.[943] נוסח סעיף זה פורש בעבר בצמצום, כמתיר פגיעה כזאת בכל חקיקה,[944] אך בשלהי שנות השבעים של המאה ה־20 החל בית המשפט העליון ההודי לקרוא לתוכו את הוראות סעיף 19 לחוקה ההודית.[945] סעיף זה מתיר פגיעה בחירויות המוקנות לפיו[946] בחקיקה המגבילה חירויות אלו בסבירות ולתכליות מסוימות.[947]

הזכות לפרטיות הוכרה בהודו כזכות החוסה בזכות לחירות אישית שבסעיף 21,[948] אך רק לאחרונה, ובעקבות פסיקות סותרות, הכריע בית המשפט העליון בעניין *Puttaswamy* כי הזכות לפרטיות היא זכות יסוד חוקתית מלאה.[949] בפסקי דין קודמים פותח המושג מהתייחסות לפרטיות במובנה הפיזי[950] דרך

943 Constitution of India (as of 9.11.2015)

944 ראו למשל Gopalan v. State of Madras (1950) S.C.R 88

945 *Maneka v. Union of India*, A.I.R 1978 S.C. 579; וכן ראו דעת המיעוט בעניין *Gopalan*, **שם**. להרחבה ראו Durga Da Basu, Introduction to the Constitution of India 79–150 (2008); Burt Neuborne, *The Supreme Court of India*, 1 Int'l J. Const. L. 476 (2003)

946 סעיף 19(1) לחוקה ההודית מונה את חופש הביטוי, האספה, ההתאגדות, התנועה, המגורים והעיסוק.

947 סעיף 19(2) לחוקה ההודית מונה עם תכליות אלו תכליות של ביטחון המדינה, יחסים דיפלומטיים, שמירת הסדר או המוסר הציבוריים, או בקשר לביזיון בית המשפט, ללשון הרע או להסתה לביצוע עבירות.

948 People's Union for Civil Liberties (PUCL) v. Union of India and Anr. (1997) 1 S.C.C.301 (להלן: עניין *PUCL*).

949 עניין *Puttaswamy*, **לעיל** בפרק זה ה"ש 940.

950 Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295

פרטיות כחירות מפגיעה במוניטין[951] ועד לפרטיות כזכות הכוללת תקשורת בין־אישית.

בעניין *Rajagopal* נקבע כי הזכות לפרטיות מוגנת בסעיף 21 לחוקה, ועל כן אין לפגוע בה שלא באמצעות נהלים שבדין. ואולם בפסק הדין בעניין *PUCL* (People's Union for Civil Liberties) – שבו נדונו פרקטיקות יירוט של תקשורת טלפוניה קווית בין השאר בעקבות האזנות סתר שביצעה הבולשת ההודית לחברי פרלמנט מכל קצות הקשת הפוליטית ואף לשרים מכהנים – נמנע בית המשפט העליון מלקבוע כי הסעיף בחוק הטלגרף ההודי (TA) (ראו להלן) המתיר יירוט תקשורת טלגרפיה, אינו חוקתי.[952] במקום זאת הדגיש בית המשפט את חובתן של הרשויות להשתמש בסמכות היירוט בכפוף לתנאים המקדימים בחוק[953] ואת התכליות הסטטוטוריות שמכוחן ניתן להורות על יירוט.[954]

על ההגבלות הסטטוטוריות הדלות שבחוק הוסיף בית המשפט בקרות נוספות, יצירות הפסיקה, על הוצאה של הוראות יירוט: (1) צווי האזנת סתר ייתן שר הפנים בלבד (של האיחוד הפדרלי או של המדינה, לפי העניין), הרשאי במקרי חירום להאציל מסמכותו לפקיד מוסמך; (2) בעת מתן צו יש לשקול חלופות אחרות להשגת המידע המבוקש; (3) תוקפם של צווים מכוח חוק הטלגרף ההודי (TA) לא יעלה על חודשיים; (4) יוקמו ועדות ביקורת שיקבעו אם צווי האזנת סתר הוצאו כדין, ואם לא – יורו על השמדת התקשורת שיורטה על כל עותקיה; (5) על הרשות שנתנה את הצו לתעד את התקשורת שיורטה, ובכלל זה את

951 R. Rajagopal v. State of Tamil Nadu, (1994), 6 SCC 632

952 India Telegraph Act 1885 § 5(2), No. 13 of 1885 INDIA CODE (להלן: חוק הטלגרף ההודי (TA)) ראו בחלק 3.5.2.2 להלן. לחשיפות שהובילו לעניין *PUCL* ראו Prabhu Chawla, *Secret Report by CBI Contains Shocking Details of Phone Tapping Ordered by Congress(I) Govts*, INDIA TODAY (28.2.1991)

953 יירוט יותר במצב חירום לאומי (public emergency) או לשם אינטרסים של ביטחון הציבור. **שם**, בס' 5(1) רישה.

954 חמש התכליות הסטטוטוריות להוצאת הוראת יירוט לפי החוק הטלגרף ההודי (TA) הן הריבונות והשלמות של הודו, ביטחון המדינה, יחסים דיפלומטיים, סדר ציבורי ומניעת הסתה לביצוע עבירות. **שם**, ס' 5(2).

תפוצתה, זהותם של אלה שלהם הופצה והיקף ההעתקה שלה.[955] בית המשפט נמנע מפורשות מהוספת תנאי של בקרה שיפוטית על צווי האזנת סתר.

3.5.2. פרטיות והגנת מידע בחקיקה

תפיסה ויירוט של תקשורת בהודו מוסדרים בכמה דברי חקיקה, בכללם קוד סדר הדין הפלילי ההודי, חוק הטלגרף ההודי (TA) והחוק ההודי בדבר טכנולוגיות מידע (ITA – Information Technology Act 2000).[956] על ספקי תקשורת חלים כללים נוספים מכוחו של החוק ההודי בדבר טכנולוגיות מידע (ITA), המאפשרים לרשויות לגשת לנתוני תקשורת ותוכן: כללי האבטחה והגנת המידע האישי,[957] הכללים המנחים לספקים-מתווכים,[958] כללי הסייבר־קפה,[959] כללי יירוט, ניטור ופענוח המידע[960] וכללי ניטור ואיסוף של נתוני תעבורה.[961]

ההגנה הסטטוטורית על הזכות לפרטיות דלה. נוסף על כלל 419 לכללי הטלגרף ההודיים (Indian Telegraph Rules) – קודיפיקציה של הכללים המנחים יצירי

955 עניין *PUCL*, **לעיל** בפרק זה ה"ש 948 בפס' 35.

956 Information Technology Act 2000 No. 21 of 2000 India Code as amended by The Information Technology (Amendment) Act 2008 No. 10 of 2009 India Code (להלן: החוק ההודי בדבר טכנולוגיות מידע (ITA)).

957 Section 43A. Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011 (להלן: כללי אבטחת המידע).

958 Information Technology (Intermediaries guidelines) Rules, 2011 (להלן: הכללים המנחים לספקי תקשורת).

959 Information Technology (Guidelines for Cyber Cafe) Rules, 2011 (להלן: כללי הסייבר־קפה).

960 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (להלן: כללי יירוט, ניטור ופענוח המידע).

961 Information Technology (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (להלן: כללי ניטור ואיסוף נתוני תעבורה).

הפסיקה שהתווה בית המשפט העליון בעניין *PUCL* (ראו בחלק 3.5.2.2 להלן)[962] – החוק ההודי בדבר טכנולוגיות מידע (ITA) כולל הגנה מוגבלת על חדירה לפרטיות בנסיבות של צילום אבריו המוצנעים של אדם.[963] כמו כן עבירות פליליות קלסיות, כגון האיסור על הפרת אמונים שבקוד הפלילי ההודי,[964] מאפשרות הגנה על פרטיות משזו הופרה בנסיבות של הפרת אמונים.[965]

3.5.2.1 צווי חיפוש ותפיסה כלליים: סדר הדין הפלילי

גם בלי הסמכה בחוק מיוחד, הדין ההודי מאפשר לרשויות גישה כללית למידע המוחזק אצל גופים פרטיים באמצעות צו תפיסה של "כל מסמך או דבר אחר".[966] מי שמוסמך לתת צו תפיסה לפי סעיף 91 לקוד סדר הדין הפלילי ההודי הוא בית המשפט או כל קצין משטרה המופקד על תחנת משטרה. סעיף 92 לקוד מסמיך שופט מחוזי (district magistrate), שופט מחוזי ראשי (chief judicial magistrate),[967] את הערכאה הפלילית (court of sessions) או את בית המשפט העליון להורות על המצאת מסמך או כל דבר אחר המצוי בחזקת רשויות הדואר או הטלגרף, ועל חיפוש אחר פריטים כאלו ככל שהדבר נדרש.

962 Rule 419-A of the Indian Telegraph Rules, as amended by the Indian Telegraph (Amendment) Rules, 2007; ראו בחלק 3.5.2.2 **להלן** (להלן: כללי הטלגרף ההודיים).

963 ס' 66E לחוק ההודי בדבר טכנולוגיות מידע (ITA), ראו **לעיל** בפרק זה ה"ש 956.

964 India Pen. Code, 1860, No. 45 of 1860 § 406

965 סעיף זה שימש גם בהקשרים של פשעי מחשב. ראו P. Kumar, *Growing Cyber Crimes in India: A Survey,* 2016 Int'l Conference on Data Mining & Advanced Computing (SAPIENCE) 246-251 2016; T. N. Varma and DA Khan, *Curbing Cyber Crimes by Indian Law* (23.02.2017)

966 Code of Criminal Procedure, 1973 §91 No. 2 of 1974 India Code

967 מערכת המשפט ההודית כוללת שלוש ערכאות מחוזיות פליליות (Second Class Judicial Magistrate Court, First Class Judicial Magistrate Court, Chief Judicial Magistrate Court)

לעיתים גופי אכיפת חוק משתמשים בסעיפים אלו כדי להשיג מידע מספקי תקשורת שלא דרך הנהלים שבחקיקה הרלוונטית.[968] היעדרה של בקרה שיפוטית מתמרץ גופים אלו לפנות לספקי תקשורת בצווים מכוח סעיף 91 לקוד בדרישה לנתוני תוכן. היקף ההיענות של הספקים לצווים אלה אינו ידוע.[969]

3.5.2.2 חוק הטלגרף ההודי (TA – Indian Telegraph Act 1885)

סעיף 5 לחוק הטלגרף ההודי (TA) מסמיך את הממשלה לתפוס טלגרפיה[970] ליירט תקשורת. במקרי חירום או מתוך אינטרס של ביטחון הציבור הממשלה המרכזית (הפדרלית) או המקומית או פקיד מוסמך רשאים לתפוס זמנית (כל עוד מתקיים אחד מהתנאים לעיל) כל טלגרפיה מורשית, בתנאי שהדבר נדרש או רצוי (expedient).[971] כמו כן לשם האינטרסים האלה – שמירה על הריבונות והשלמות של הודו, על ביטחון המדינה, על יחסים דיפלומטיים, על הסדר הציבורי ולמניעת הסתה לביצוע עבירות[972] – הם רשאים להורות בכתב כי כל תשדורת או סוג של תשדורות לא ישודרו, יעוכבו, ייורטו או יימסרו לממשלה.[973]

התיקון לכלל 419 לכללי הטלגרף ההודיים משקף את הנחיות בית המשפט בפסק הדין בעניין *PUCL* והוסיף בקרות על יירוט תקשורת מכוח סעיף 5 של חוק הטלגרף ההודי (TA). לפי כלל 419 לכללי הטלגרף, יירוט תקשורת לא ייעשה אלא בהוראת שר הפנים בלבד (של האיחוד הפדרלי או של המדינה, לפי

968 ראו בחלקים 3.5.2.2 ו־3.5.2.3 **להלן**.

969 Sunil Abraham and Elonnai Hickok, *Government Access to Private-Sector data in India*, 2 Int'l Data Privacy Law 302, 304 (2012)

970 "טלגרפיה" – כל מכשור שנועד לשידור או לקליטה של אותות, טקסט, תמונות וצלילים באמצעות חיווט, גלי רדיו, קרינה אלקטרומגנטית, אמצעים מגנטיים ואחרים. ראו ס' 3(1AA) לחוק הטלגרף ההודי (TA).

971 ס' 5(1) לחוק הטלגרף ההודי (TA).

972 לשם השוואה, סעיף 26 של חוק הדואר ההודי (The Indian Post Office Act, 1898) אינו מתיר יירוט דברי דואר רק בנסיבות של חירום או מתוך אינטרס של ביטחון הציבור או שלומו – ואינו כולל את התוספת שבס"ק 5(2) לחוק הטלגרף ההודי (TA).

973 ס' 5(2) לחוק הטלגרף ההודי (TA).

העניין), והוא גם רשאי במקרי חירום – מטעמים מבצעיים או במקרים שבהם השגת אישור מהשר אינה מתאפשרת מפאת מרחק – להאציל מסמכותו לפקיד מוסמך.[974] צו יירוט כאמור יהיה מנומק,[975] יפרט את יעדי ההאזנה ככל הניתן[976] ויינתן בהיעדר חלופות סבירות אחרות.[977] הצו יציין מפורשות שהשימוש במידע שיורט מכוחו מותר רק בכפוף להוראות סעיף 5(2) של חוק הטלגרף ההודי (TA), ויעמוד בתוקף למשך שישים יום. ניתן לחדשו לתקופה שלא תעלה על 180 יום במצטבר.[978]

יירוט תקשורת, תפוצת החומרים שהושגו באמצעותו ועותקיהם יתועדו בידי הקצין האחראי.[979] הכללים מסדירים את הממשק בין הרשויות לבעלי רישיון הטלגרף, ומטילים על בעלי הרישיון את החובה לנקוט אמצעים אפקטיביים כדי למנוע יירוט לא מורשה.[980] על בעלי רישיון טלגרף למנות אחראים ארגוניים (nodal officers) למטרות אלו. על האחראים הארגוניים לאשר בתוך שעתיים את דבר קבלתו של צו יירוט, ומדי חמישה עשר יום להעביר לרשויות את רשימת הבקשות שנתקבלו אצלם כדי לאמת את מקורן.[981]

ועדת ביקורת – שמורכבת ממזכיר הקבינט, מזכיר משרד המשפטים ומזכיר משרד התקשורת הפדרליים, ומהמזכיר הראשי, המזכיר המשפטי ומזכיר אחר ברמת הממשל המקומי – תיוועד מדי חודשיים לבחון אם צווי היירוט[982] ניתנו

974 כלל 419A(1) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

975 כלל 419A(2) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

976 כלל 419A(4) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

977 כלל 419A(3) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

978 כלל 419A(6) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

979 כלל 419A(8) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

980 כלל 419A(14) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

981 כללים 419A(9)–(13) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

982 כלל 419A(2) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962, מורה על מסירת העתק של צו יירוט לוועדת הביקורת בתוך שבעה ימים מהיום שבו ניתן.

בהלימה עם הוראות סעיף 5(2) לחוק הטלגרף ההודי (TA).[983] חומר הקשור לצווים אלה ולתשדורות שיורטו מכוחם יבוער בחלוף שישה חודשים, אלא אם יש בו צורך,[984] ועל ספקי התקשורת לבער תיעוד הקשור לצווים הללו בחלוף חודשיים מתום היירוט.[985]

זאת ועוד, מסמכי הרישוי של ספקי שירותי האינטרנט בהודו כוללים הוראות שמקנות לממשלה את הזכות לבחון את מערכותיהם של הספקים או לנטר אותן, וכן הם כוללים הוראות המטילות על הספקים את האחריות לנטר תקשורת מטרידה ולתעד את זהות המשתמשים בשירותיהם בכל רגע באופן שיהא זמין לממשלה לפי דרישה. הספקים נדרשים גם להעמיד לרשות הממשלה נתוני זיהוי של המשתמשים ולשמור את תעבורת התקשורת במערכותיהם לתקופה שלא תפחת משנה.[986]

3.5.2.3 החוק ההודי בדבר טכנולוגיות מידע (ITA – Information Technology Act 2000)

במקורו נועד החוק ההודי בדבר טכנולוגיות מידע (ITA) להסדיר מסחר אלקטרוני.[987] התיקון משנת 2008 עיבה את הגנת המידע באמצעות הרחבת אחריותם של תאגידים, כך שתחול גם על אבטחת מידע אישי רגיש שבחזקתם.[988] במסגרת התיקון נוספו גם עבירות על עבירות המחשב שבנוסחו המקורי של

983 כללים (17)-(16)19A לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

984 כלל 419A(18) לכללי הטלגרף ההודיים, **לעיל** בפרק זה ה"ש 962.

985 כלל 419A(19) לכללי הטלגרף ההודיים **לעיל** בפרק זה ה"ש 962.

986 Prashant Iyengar, *IP Addresses and Expeditious Disclosure of Identity in India*, 9 Indian J. L & Tech. 1 8–10 (2013). וראו גם Abraham, **לעיל** בפרק זה ה"ש 969, בעמ' 308. כמו כן תנאי הרישיון האחיד מורים לספקי שירותי תקשורת סלולרית להנפיק כרטיסי SIM אך ורק ללקוחות שזהותם אומתה ותועדה. ראו Privacy International, *The Right to Privacy in India* (22.11.2016).

987 ראו דברי המבוא לחוק ההודי בדבר טכנולוגיות מידע (ITA), **לעיל** בפרק זה ה"ש 956.

988 ס' 43A לחוק ההודי בדבר טכנולוגיות מידע (ITA).

החוק,[989] בין השאר עבירות הנוגעות לשימוש לרעה במידע פרטי (כגון גנבת זהות[990] או קבלת חומרי מחשב שהושגו במרמה)[991] ולפגיעה בפרטיות.[992] ואולם עבירת הפגיעה בפרטיות לפי ה־ITA מוגבלת לנסיבות שבהן פלוני משיג, משדר או מפיץ תמונה של אברים מוצנעים של הזולת ללא הסכמה במצבים שהם הפרה של פרטיות.[993]

היקפה של הגנת המידע הסטטוטורית אינו רחב במיוחד, ותחולתה משתרעת רק על תאגידים (body corporate) (ולא על הסקטור הציבורי)[994] במקרים שבהם רשלנות בהטמעה של נהלים סבירים לאבטחת מידע – כשמדובר במידע אישי רגיש שהוחזק במערכות ממוחשבות שבבעלותן או בשליטתן – הסבה נזק או הניבה רווחים שלא כדין לפלוני. הגדרת מהותו של "מידע אישי רגיש" נותרה כלקונה עד התקנתם של כללי אבטחת המידע בשנת 2011.[995]

כללי אבטחת המידע, המשמשים בסיס לדיני הגנת המידע המסחריים בהודו, מפרטים את נוהלי אבטחת המידע הסבירים לצורך סעיף 43A של החוק ההודי בדבר טכנולוגיות מידע (ITA).[996] כללי אבטחת המידע מורים לתאגידים לנסח ולפרסם את מדיניות הפרטיות שלהם. איסוף מידע אישי ייעשה בתנאי שהוא נדרש למטרות חוקיות מוגדרות הקשורות לפעילותו של התאגיד, ובהסכמת מושא המידע. על התאגיד האוסף מידע אישי רגיש לנקוט צעדים סבירים לשם

989 ס' 65–66 לחוק ההודי בדבר טכנולוגיות מידע (ITA).

990 ס' 66C,66D לחוק ההודי בדבר טכנולוגיות מידע (ITA).

991 ס' 66B לחוק ההודי בדבר טכנולוגיות המידע (ITA).

992 66E לחוק ההודי בדבר טכנולוגיות מידע (ITA).

993 הסעיף מחיל דוקטרינה של ציפייה סבירה לפרטיות כמבחן להתקיימות נסיבות של הפרת פרטיות – נסיבות שבהן הקורבן התערטל בפרטיות בלי לחשוש מצילומו בידי צד שלישי, או כשהיה יכול לצפות שאזוריו המוצנעים לא ייחשפו, אם במרחב הפרטי ואם בציבורי. ס' 66E(e) לחוק ההודי בדבר טכנולוגיות מידע (ITA).

994 ראו Privacy International, **לעיל** בפרק זה ה"ש 986, בס' 44.

995 ס' 3 לכללי אבטחת המידע, **לעיל** בפרק זה ה"ש 957. "מידע אישי רגיש" הוא הכולל סיסמאות, מידע פיננסי, מידע בריאותי, נטייה מינית או מידע ביומטרי.

996 ובעיקר בסעיף 8 לכללי אבטחת המידע, **לעיל** בפרק זה ה"ש 957.

יידוע מושא המידע, וכן להימנע מהחזקת הנתונים יותר מן הנדרש ומשימוש בהם החורג מהמטרה שלשמה נאספו.[997]

האיסור בכללי אבטחת המידע על העברה של מידע אישי רגיש לצדדים שלישיים מחריג מתוכו העברת מידע לסוכנויות ממשלה שהוסמכו לפי דין להשיגו למטרות של אימות זהות או למניעת עברות, זיהוין, חקירתן, תביעה וענישה בגינן, ובכפוף לדרישה בכתב; או לכל צד שלישי מכוח צו לפי דין.[998] לפי כללים אלו, הרשויות המוסמכות, שאומנם נדרשות לפרט בכתב את הטעמים לכך, יכולות לדרוש המצאת מידע אישי רגיש ללא צו שיפוטי. מידע שהושג בדרך זו יכול שיעבור לרשויות מוסמכות אחרות לשימושים אחרים לפי התכליות הרחבות שלעיל.[999]

החוק ההודי בדבר טכנולוגיות מידע (ITA) עצמו מקנה לממשלה סמכויות יירוט רחבות ללא צורך בצו שיפוטי. סעיף 69 לחוק מתיר לממשלה המרכזית של הודו, לממשלה מקומית או לכל פקיד שהן הסמיכו לכך, להורות לכל סוכנות ממשלתית ליירט, לנטר או לפענח – או להביא לכדי יירוט, ניטור או פענוח של – כל תקשורת ממוחשבת, ובתנאי שהדבר נדרש לשמירה על האינטרסים של ריבונותה ושלמותה של הודו, הגנתה, ביטחון המדינה, יחסיה הדיפלומטיים, הסדר הציבורי או לשם מניעת הסתה לביצוע עבירות. יוער כי שלא כהוראות חוק הטלגרף (TA), יירוט תקשורת ממוחשבת אינו מותנה במצב חירום או בביטחון הציבור.

זאת ועוד, סעיף 69B בחוק[1000] מתיר לממשלה המרכזית של הודו לאשר בפרסום רשמי לכל רשות ממשלתית לנטר ולאסוף נתוני תעבורת תקשורת ממוחשבת (traffic data)[1001] למטרות הגנת סייבר (cyber security) ולמניעת תפוצה של

997 ס' 5 לכללי אבטחת המידע, **לעיל** בפרק זה ה"ש 957.

998 ס' 6 לכללי אבטחת המידע, **לעיל** בפרק זה ה"ש 957.

999 ראו Abraham, **לעיל** בפרק 3 ה"ש 969, בעמ' 305.

1000 ס'69B לחוק ההודי בדבר טכנולוגיות מידע (ITA).

1001 "נתוני תעבורת תקשורת ממוחשבת" (traffic data) מוגדרים בסעיף 69B(4)(ii) לחוק ההודי בדבר טכנולוגיות מידע (ITA) ככל מידע מזהה או שביכולתו לזהות כל אדם, מערכת מחשב, רשת מחשבים, מיקום (יעד ומטרה) של תקשורת מחשבים, הכולל נתוני מקור, יעד, נתיב, זמן, תאריך, נפח, משך התקשורת וסוגה.

נוזקות (computer contaminant).[1002] הרשות שהוסמכה לכך רשאית להורות לספקי תקשורת או לכל מתווך אחר לסייע לה או לשתף פעולה בניטור ובאיסוף נתונים אלה, לרבות בדרך של מתן גישה מקוונת לתעבורה זו. אי־ציות ביודעין להוראות אלו דינו מאסר לתקופה של עד שלוש שנים.

שני קובצי כללים נוספים לפי החוק ההודי בדבר טכנולוגיות מידע (ITA) מפרטים את הכללים שמכוחם יתאפשר יירוט מכוח סעיף 69 או מכוח סעיף 69B (כללי יירוט, ניטור ופענוח המידע[1003] וכללי ניטור ואיסוף נתוני תעבורה,[1004] בהתאמה). לפי כללי יירוט, ניטור ופענוח המידע, על הרשות המוסמכת לשקול חלופות ליירוט המבוקש טרם מתן הוראת יירוט, ויש כמה דרישות מהותיות בנוגע לתוכן הוראות היירוט שבכתב.[1005] הכללים אינם מאפשרים מתן הוראה לאיסוף גורף (bulk collection), והם דורשים שזו תכלול את יעדי האיסוף הפרטניים (בין שהיעד הוא אדם ובין שהוא מכונה) או את סיווגם.[1006] לפי כללים אלו, ההוראות יעמדו בתוקפן למשך שישים יום, וניתן להאריכן לתקופה שלא תעלה על 180 יום במצטבר.[1007] אחת לחודשיים תבחן ועדת הביקורת מכוח חוק הטלגרף ההודי (TA)[1008] את ההוראות שניתנו לפי כללים אלו ואת מידת הלימתן עם הכללים.[1009] הכללים גם כוללים הוראות באשר לממשק בין ספקי התקשורת

1002 כהגדרתו בס' 43 (i) לחוק ההודי בדבר טכנולוגיות מידע (ITA).

1003 ראו **לעיל** בפרק זה ה"ש 960.

1004 ראו **לעיל** בפרק זה ה"ש 961.

1005 ס' 7–8 לכללי יירוט, ניטור ופענוח המידע.

1006 ס' 9 לכללי יירוט, ניטור ופענוח המידע.

1007 ס' 11 לכללי יירוט, ניטור ופענוח המידע.

1008 ראו בטקסט המפנה לה"ש 982 **לעיל** בפרק זה.

1009 ס' 22 לכללי יירוט, ניטור ופענוח המידע.

לרשות המוסמכת[1010] וכן איסורים על יירוט לא מורשה[1011] ועל שימוש הספק או מי מעובדיו במידע המבוקש או העברה שלו לצדדים שלישיים.[1012]

הוראות דומות מצויות בכללי ניטור ואיסוף של נתוני תעבורה. מתן הוראה לניטור ולאיסוף של נתוני תעבורה מכוח סעיף 69B ייעשה בכתב, לתכליות הקשורות להגנת סייבר ויכלול הגדרה של יעדי האיסוף הפרטניים (או סיווגם).[1013] על ספק התקשורת להבטיח כי יש בקרות נאותות על ניטור לא מאושר ולשמור על חשאיות.[1014] ועדת הביקורת שלפי חוק הטלגרף[1015] תבחן אחת לחודשיים את ההוראות שניתנו לפי כללי הניטור והאיסוף של נתוני תעבורה אלו ואת מידת הלימתן עם הכללים.[1016] בדומה לכללי יירוט, ניטור ופענוח המידע, גם הכללים לניטור ואיסוף נתוני תעבורה כוללים הוראות בעניין הממשק בין הספקים[1017] לרשות המוסמכת ואוסרים על יירוט לא מורשה של נתוני תעבורה.[1018] הכללים המנחים לספקי תקשורת[1019] מורים להם לשמור למשך תשעים יום[1020] נתונים שהם הסירו (בכללם חומרים שהוסרו בשל היותם בגדר איום על ריבונותה, שלמותה, ביטחונה או הגנתה של הודו ועל הסדר הציבורי, והם בבחינת הסתה לביצוע עבירות או עלבון לאומות אחרות).[1021] לפי הוראה אחרת בכללים המנחים,

1010 ס' 13–21 לכללי יירוט, ניטור ופענוח המידע.

1011 ס' 24 לכללי יירוט, ניטור ופענוח המידע.

1012 ס' 25 לכללי יירוט, ניטור ופענוח המידע.

1013 ס' 3 לכללי ניטור ואיסוף נתוני תעבורה.

1014 ס' 5–6 לכללי ניטור ואיסוף נתוני תעבורה.

1015 ראו בטקסט המפנה לה"ש 982 **לעיל** בפרק זה.

1016 ס' 7 לכללי ניטור ואיסוף נתוני תעבורה.

1017 ס' 4 לכללי ניטור ואיסוף נתוני תעבורה.

1018 ס' 9 לכללי ניטור ואיסוף נתוני תעבורה.

1019 ראו **לעיל** בפרק זה ה"ש 958.

1020 ס' 3(4) לכללים המנחים לספקי התקשורת.

1021 רשימת העילות המלאה להסרת תוכן מצויה בסעיף 3(2) לכללים המנחים לספקי התקשורת.

על ספקי התקשורת לסייע לסוכנויות הממשלה המוסמכות או להעביר להן מידע לתכליות של אימות זהות או מניעת עבירות, זיהוין, חקירתן, תביעה וענישה בגינן, ובכפוף לדרישה בכתב; או לכל צד שלישי מכוח צו לפי דין.[1022]

גם על ספקי שירותי תקשורת מסדר שני – כמו מפעילי הסייבר־קפה (קפה־אינטרנט) – חלות הוראות רגולטוריות לתיעוד זהותם של המשתמשים (לרבות צילומם)[1023] ופעילותם המקוונת.[1024] על המפעילים לשמור את לוג הפעילות של לקוחותיהם למשך שנה לכל הפחות. כללי הסייבר־קפה מורים למפעילים לאפשר לפקיד שהסמיכה סוכנות הרישוי לבחון נתונים אלה בכל עת.[1025]

3.5.3. מעקב אחר רשתות תקשורת בהודו: פרקטיקה

סקירת הדינים שבחלק הקודם מתארת הסדרה משפטית רזה מאוד של מעקב אחר רשתות תקשורת בהודו. התכליות המותרות בדין ליירוט נתוני תוכן ותקשורת ולאיסופם רחבות מאוד, ואין שום ביקורת שיפוטית על צווים ועל הוראות ליירוט, לאיסוף או לפענוח של מידע[1026] (ובית המשפט העליון נמנע במפורש מהקמת חובת ביקורת שיפוטית על האזנות סתר).[1027] האסדרה החלה על ספקים של שירותי תקשורת דורשת מהם לשתף פעולה עם הרשויות המוסמכות בכל הנוגע להעברת נתוני תוכן ותקשורת, לעיתים באופן מקוון, לשם הגשמת אותה קשת רחבה של תכליות.

1022 ס' 3(6) לכללים המנחים לספקי התקשורת.

1023 ס' 4 לכללי הסייבר־קפה. ראו גם Privacy International, **לעיל** בפרק זה ה"ש 986, בס' 37.

1024 ס' 5(2) לכללי הסייבר־קפה.

1025 ס' 7 לכללי הסייבר־קפה. אף שתפקידו של קצין זה לפקח על מילוי הוראות החוק באשר לסייבר־קפה, מאחר שבין השאר הכללים אוסרים על שימוש לא חוקי בציוד המחשבים במקום, ניתן לנצל פתח זה למטרות החורגות מפיקוח גרידא, במיוחד בהיעדר דרישות סף למינויו של קצין מוסמך.

1026 גם צו מכוח סעיף 91–92 לסדר הדין הפלילי ההודי (ראו בחלק 3.5.2.1 **לעיל**) אינו מחייב ביקורת שיפוטית, וקצין מוסמך רשאי ליתן אותו.

1027 עניין *PUCL*, **לעיל** בפרק זה ה"ש 948.

זאת ועוד, בשנים האחרונות הממשל ההודי מקים מערך ניטור מקיף של אזרחי המדינה ותושביה, כשראש החץ של הפרויקט הוא מערכת הניטור המרכזית (CMS – Central Monitoring System). פרויקט זה, שתחילתו בשנת 2006, נועד לייצר ממשק מרכזי של הממשלה עם ספקי התקשורת ולהבטיח גישה מרוכזת ומקוונת לנתוני תוכן ותקשורת.[1028] הפרויקט לא לווה ברפורמה בחקיקה, פרט לתיקונים טכניים בתנאי הרישיון של הספקים.[1029] ספקי תקשורת מורשים נדרשים להתקין מערכות המעבירות נתוני תקשורת ותוכן ישירות למערכת הניטור (CMS), והדבר מייתר את הממשק האנושי עם האחראים הארגוניים שלהם לפי כללי חוק הטלגרף.[1030] מערכת הניטור (CMS) מעבירה את נתוני התוכן והתקשורת שהיא מיירטת לתשע סוכנויות ביון ואכיפת חוק.[1031] לפי דיווחים מסוימים תוכל המערכת לנטר ולפענח פרוטוקולי תקשורת מתקדמים, לאתר מיקום גאוגרפי על סמך נתוני מיקום ולכרות מידע למטרות של פרופיילינג.[1032]

חוסר השקיפות שליווה את הפרויקט, לרבות היעדר מידע על היקף פריסתה, יכולותיה והארכיטקטורה הטכנית של המערכת, זכה לביקורת של ארגוני החברה

1028 Ranesh Prakash, *How Surveillance Works in India*, the New York Times (10.07.2013); *MHA Plans Phone Tapping Agency*, The Times of India (4.2.2006)

1029 Maria Xynou, *India's Central Monitoring System (CMS): Something to Worry About?*, the Centre for Internet and Society (30.01.2014). לתיקונים עצמם ראו File No. 800-12/2013-AS.II, Amendments to the Unified License agreement, Unified Access Services (UAS) License agreement, Unified License (Access Services) agreement, CMTS License agreement (11.10.2013)

1030 ראו בטקסט המפנה לה"ש 979–981 **לעיל** בפרק זה.

1031 Addison Litton, *The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression,* 14 Wash U, Global Stud. L. Rev. 799 (2015)

1032 Snehashish Ghosh, *The State is Snooping: Can You Escape?*, the Centre for Internet and Society (26.06.2013)

האזרחית.[1033] המבקרים הצביעו גם על היעדרן של בקרות סטטוטוריות נאותות על המערכת – היעדר ביקורת שיפוטית מראש (אקס אנטה) ובקרות על גופי האיסוף והצדדים שאליהם המידע מופץ.[1034] עם זאת, לטענת הממשלה, עיצובה של המערכת מאפשר מניעת שימוש לרעה במודיעין שהיא אוספת. כך למשל צרכניה – רשויות אכיפת החוק – מנועים מגישה עצמאית לנתונים שנאספו על יעד מסוים, ואילו הספק שלהם מנוע מלבחון את נתוני התוכן שנאספו. בקרה נוספת נעשית באמצעות תיעוד פעילותם של המשתמשים בה.[1035] עם זאת, בניגוד לאיסוף המתבסס על הכללים הקיימים – הדורש הגדרה של יעדים מודיעיניים פרטניים[1036] – מערכת הניטור המרכזית, השואבת את נתוני הספקים שלא לפי דרישה פרטנית בכתב, מאפשרת לדלג על בקרה זו ולבסס איסוף מודיעיני גורף וחסר הבחנה.[1037]

לצד מערכת הניטור המרכזית (CMS) פועלות ומתוכננות לפעול בהודו עוד כמה מערכות מודיעין שעוקבות אחר אזרחי המדינה, ושמידת שילובן עם המערכת המרכזית אינו ברור. רשת המודיעין הלאומית (NATGRID – National Intelligence Grid) היא מיזם של משרד הפנים ההודי שנועד לסייע במיכון תהליכים ידניים של איסוף מודיעין ולאפשר עיבוד מודיעין למטרות כגון פרופיילינג או זיהוי תבניות. רשת מודיעין זו מתבססת בעיקרה על נתונים שמקורם במאגרי מידע של בנקים, סוכנויות אשראי, רשויות ההגירה והתעבורה.[1038]

1033 Jaideep Reddy, *The Central Monitoring System and Privacy: Analysing What We Know So Far*, 9 Indian J. L & Tech. 41 (2014)

1034 ראו Prakash, **לעיל** בפרק זה ה"ש 1028; Shalini Singh, *Lethal Surveillance versus Privacy*, The Hindu (22.6.2013)

1035 ראו Prakash, **שם**, בעמ' 53.

1036 כלל 419A(4) לכללי הטלגרף ההודיים, **לעיל** בפרק זה בה"ש 962, וכן ראו ס' 7–8 לכללי יירוט, ניטור ופענוח המידע וס' 3 לכללי ניטור ואיסוף נתוני תעבורה.

1037 ראו Reddy, **לעיל** בפרק זה ה"ש 1033.

1038 Chautanya Ramachandran, *PUCL V. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned FOR The Digital Age*, 7 NUJS L. Rev. 105 (2014); P. Arun, *Surveillance and Democracy in India:*

מערכת מודיעין נוספת לניטור תקשורת היא מערכת ניטור תעבורת התקשורת (NETRA — Network Traffic Analysis), שנועדה לניתוח תעבורת אינטרנט, ובכלל זה מידע הקשור לרשתות חברתיות, דוא"ל ותקשורת מבוססת-VoIP. עדיין לא ברור אם וכיצד עתידה המערכת הזאת להתממשק עם מערכת הניטור המרכזית (CMS).[1039]

המעקב אחר רשתות תקשורת בהודו הוא חלק ממגמה רחבה יותר של ניטור אזרחי המדינה באמצעים דיגיטליים. הרטוריקה של תוכנית "הודו הדיגיטלית", שהושקה ב-2014, מתארת העצמה של האזרח באמצעות טכנולוגיות מידע והגברת הגישה לשירותים חברתיים, אך יש החוששים שהמעבר לעסקאות אלקטרוניות ולזיהוי ביומטרי, במשולב עם מערכות דוגמת מערכת הניטור המרכזית (CMS), יקנו לממשלה כלים רבי עוצמה למעקב אחר אזרחיה ולמשטורם.[1040]

Analysing Challenge to Constitutionalism and Rule of Law, 1 J. Pub. Affairs & Change 47 (2017)

1039 Ramachandran, **שם**.

1040 ראו לדוגמה P. Arun, *Uncertainty and Insecurity in Privacyless India: A Despotic Push towards Digitalisation*, 15 Surveillance & Soc. 456-464 (2017)

- רק לאחרונה (יולי 2017) הכיר בית המשפט ההודי בזכות לפרטיות כזכות חוקתית.
- חוק הטלגרף ההודי (TA) מסמיך את הממשלה לתפוס טלגרפיה ליירט תקשורת למנעד רחב של תכליות, לרבות ביטחון לאומי ומניעת פשיעה. יירוט תקשורת לפי חוק הטלגרף ייעשה באמצעות צו שנותן שר הפנים, והוא אינו כפוף לביקורת שיפוטית, אלא לבחינה עיתית של ועדה ממשלתית, שלא נראה כי הוקנו לה סמכויות לביטול צווים שניתנו בחריגה מהוראות החוק.
- הוראות משלימות מצויות בחוק ההודי בדבר טכנולוגיות מידע (ITA), המקנה לממשלה את הסמכות ליירט תקשורת מחשבים ללא צורך בצו.
- ערוצים אחרים שמאפשרים להשיג נתוני תוכן ותקשורת מצויים בסדר הדין הפלילי, המסמיך קצין משטרה האחראי על תחנת משטרה לתת צווי תפיסה כלליים, שבאמצעותם המשטרה דורשת נתונים מספקי תקשורת.
- בהתאם לרגולציה שחלה על ספקי תקשורת אינטרנט, עליהם להעביר לפי דרישת סוכנויות הממשלה המוסמכות מידע לתכליות נרחבות, לרבות מניעת פשיעה וביטחון לאומי, ללא צו מאת בית המשפט.
- מנגנון הניטור המקוון הקורם עור וגידים בהודו – מערכת הניטור המרכזית (CMS) וכן מערכות מודיעין נוספות שעוקבות אחרי אזרחי המדינה – התאפשרו, יש להניח, בשל ההגנה הרופפת בדין ההודי על פרטיותם של אזרחים מפני עינה הבולשת של הממשלה.

פרק 4

מעקב אחר רשתות תקשורת: הסדרת סוגיות קונקרטיות בדין המשווה

4.1. מעקב מקוון: תחולה טריטוריאליות ופרסונלית

השאלות בדבר תחולה טריטוריאלית ופרסונלית בקשר לאיסוף ראיות ומודיעין ברשתות תקשורת – מורכבות. בפעולת אלה עלול להתעורר מתקל דינים שמקורו בשונות הדינים הלאומיים החלים בנוגע למיקום ולזהות הנפרדים של סוכנות האיסוף, יעד המעקב, ספקי שירותי התקשורת או הצדדים השלישיים שמידע עליהם נאסף אגב אורחא, וכן בעניין מיקום הנתונים המבוקשים או התקשורת.[1]

הזיקה הפרסונלית והטריטוריאלית למדינה משפיעה על רמת ההגנה על פרטיותם של יעדי האיסוף ושל הצדדים השלישיים שמידע עליהם נאסף באקראי. הדינים המגינים על זכויותיהם של מושאי המעקב המקוון נוטים להחליש את המגבלות החלות על גופי החקירה והביטחון לפי זיקות טריטוריאליות ופרסונליות של היעד המודיעיני (ושל צדדים אחרים לתקשורת) למדינה. כך למשל אין שיטת משפט בעולם שבה רמת ההגנה על פרטיותם של אזרחים זרים במעקב חוץ־טריטוריאלי למטרות ביטחון גוברת על רמת ההגנה על פרטיותם של אזרחי אותה מדינה או משתווה לה.[2]

1 ראו ויסמונסקי, **לעיל** בפרק 2 ה"ש 26, בעמ' 240–242.

2 Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 Chi. J. Int'l L (2018)

לפי הדין האמריקאי, איסוף מודיעין מקוון בתחומי ארצות הברית או על מי שלהם זיקה מסוימת אליה ("אדם אמריקאי") כרוך על פי רוב בהוצאת צו חיפוש או תפיסה מכוח ההגבלות של התיקון הרביעי לחוקה והפרשנות שלו בהלכה.[3] כפועל יוצא מעניין *Verdugo-Urquidez*,[4] לצורך חיפוש או תפיסה ראשית יש להבחין היכן הפעילות תבוצע. אם החיפוש או התפיסה יבוצעו מחוץ לארצות הברית, יש לבחון גם את זהות היעד המודיעיני ואת זיקתו לארצות הברית. ההסדרים של חוק איסוף מודיעין זר (FISA) – שלפיהם נאסף מודיעין מחוץ לארצות הברית – מקילים כשמבוקש לאסוף מודיעין אחר יעדים שאינם בגדרי "אדם אמריקאי",[5] וכשהיעד הוא "אדם אמריקאי", הם מציבים דרישות מחמירות יותר. בנסיבות שבהן קיימת אי־ודאות מודיעינית באשר להיבטים הפרסונליים והטריטוריאליים של המעקב, נדרשות סוכנויות הביון להעריך את זהותו של היעד לפני האיסוף. חלק מאי־הוודאות נפתר באמצעות חזקות שונות,[6] וחלק באמצעות ייתורה, כאשר ניתן לאסוף את הנתונים אגב אורחא.[7] בעידן של תעבורת מידע בין־לאומית ושל מחשוב הענן שאלות של זיקה טריטוריאלית עולות גם בנוגע ליירוט תקשורת נתונים לפי חוק האזנות סתר (WTA), או בנוגע לצווים מכוח חוק תקשורת שמורה (SCA) – האם החוקים חלים על נתונים השמורים פיזית בתחומי ארצות הברית, או גם על נתונים שאפשר לגשת אליהם מתחומי ארצות הברית מתחומיה?[8]

הדינים האירופיים נוטים להימנע מהבחנות טריטוריאליות או פרסונליות. דירקטיבת הגנת המידע (דירקטיבה 95/46/EC), התקנות הכלליות בדבר הגנת מידע (GDPR) שירשו אותה וכן דירקטיבת רשויות אכיפת החוק (דירקטיבה

3 ראו **לעיל** חלק 3.1.2.1.

4 **לעיל** בפרק 3 ה"ש 41.

5 להגדרת "אדם אמריקאי", ראו **לעיל** בפרק 3 ה"ש 134.

6 כך למשל כשמיקום היעד אינו ידוע או שהוא מחוץ לארצות הברית, היעד מזוהה כמי שאינו אדם אמריקאי בהיעדר יסוד סביר לסתור זאת. ראו Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 Yale L. J. 326 (2015) בה"ש 70.

7 **שם**, בעמ' 349–350.

8 **שם**.

(2016/680) נועדו להגן על בני אדם (natural persons) ללא הבחנה באשר לזהותם או למושבם.[9] אם עיבוד מידע אישי נעשה בתחומי האיחוד, הדין האירופי החל עליו אינו מבחין אם יש למידע האישי המעובד זיקה טריטוריאלית או פרסונלית לאיחוד אם לאו. ואולם מאחר שהתחולה המהותית של ה־GDPR ושל דירקטיבה 2016/680 מחריגה עיבוד מידע לתכליות של ביטחון לאומי, היעדרן של הבחנות אלו אין בו כדי להבטיח את דבר היעדרה של הבחנה כזאת מהדין הלאומי החל על מעקב מקוון לתכליות אלה.

בדין הבריטי האיסור הכללי של חוק סמכויות חקירה 2016 (IPA) על יירוט תקשורת חל על תקשורת העוברת דרך בריטניה.[10] חוק סמכויות חקירה מורה לסוכנויות הביון שלא לעסוק בפעילות סייבר שניתן לאשרהּ בצו ממוקד או כללי שלא לפי צו כאמור, אם לפעילות זו, ליעדיה המודיעיניים או לתקשורת שתיורט יש זיקה טריטוריאלית לאיים הבריטיים.[11] אך מכלל הלאו שומעים את ההן, וניתן להניח שפעילות סייבר שאינה בעלת זיקה טריטוריאלית כזו אינה טעונה צו.[12]

גם הדין הבריטי החל על פעולות איסוף גורף בוחן שאלות של טריטוריאליות. השגת תקשורת חו"ל שאחד מצדדיה מצוי מחוץ לטריטוריה הבריטית מותנית בצווי יירוט וסייבר כלליים[13] ובצווים שמכוחם תיעשה פנייה לסוכנות מודיעין זרה בבקשה ליירוט תקשורת.[14] נוסף על כך, צו עיון ממוקד לא יתיר עיון בתוכן או בנתוני תקשורת שיורטו אם העיון נעשה על סמך קריטריון המזהה אדם המצוי

9 ראו ס' 1–2 למבוא לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), ס' 2 למבוא לדירקטיבת הגנת המידע, וכן ס' 2 למבוא לתקנות הכלליות בדבר הגנת מידע (GDPR).

10 ראו חלק 3.3.4.2 **לעיל**.

11 לתנאים המקימים זיקה טריטוריאלית ראו ס' 13(2) לחוק סמכויות חקירה 2016 (IPA).

12 אף שלפי ס"ק 13(3) לחוק סמכויות חקירה 2016 (IPA) ראש שירות ביון אינו מנוע במקרים כאלו מלבקש צו.

13 ראו חלקים 4.1.4.8.1 ו־3.3.4.8.3 **לעיל**.

14 ס' 9 לחוק סמכויות חקירה 2016 (IPA).

בטריטוריה הבריטית.[15] עם זאת, שלא כדין האמריקאי, במעקב חוץ־טריטוריאלי הדין הבריטי אינו מבחין בין יעדים שהם אזרחי הממלכה המאוחדת ובין אלו שאינם אזרחים.

בכל הנוגע לגרמניה, בספרות קיימת מחלוקת בנוגע לתחולה האקס־טריטוריאלית של ההגנות החוקתיות בדין הגרמני על הזכות לפרטיות. ככלל, הדינים הגרמניים החלים על מעקב מקוון אינם כוללים הבחנה טריטוריאלית, למעט בהקשר של מעקב אסטרטגי. על אף העמדות השוללות הבחנה זו, חוק סוכנות הביון הפדרלית (BNDG) מבחין בין מעקב אחר גרמנים ואזרחי האיחוד ולבין כל תקשורת אחרת.[16] עם זאת גם מעקב אסטרטגי זר כפוף להגבלות המגינות על גרעין הזכות לחיים פרטיים.[17]

בהודו, כפי שראינו לעיל, הדין החל על מעקב מקוון דל,[18] ולכן הוא אינו מציע הבחנות טריטוריאליות או פרסונליות. יתר על כן, נראה כי פרקטיקות המעקב שלאחרונה קורמות עור וגידים במדינה מופנות בעיקר כלפי פנים, ולכן הבחנות טריטוריאליות או פרסונליות אינן במוקד הדיון הציבורי, המתייחס לפגיעות כלליות יותר בפרטיות.

הפסיקה הישראלית כמעט שאינה דנה בהיבטים של תחולה טריטוריאלית ופרסונלית של חוק האזנת סתר. בעניין **אלמצרי**[19] קבע בית המשפט העליון כי בשטחים אין תחולה טריטוריאלית לחוק האזנת סתר, וכי תחולתו מוגבלת רק לתושבי השטחים שהם אזרחי מדינת ישראל. על פי פסק הדין בעניין **אלמצרי** בשטחים מותר לבצע האזנת סתר ללא צו שיפוטי אחר יעדים שאינם אזרחים ישראלים, בכפוף לעקרונות כלליים של המשפט המינהלי.[20] פרשנותו של

15 ראו חלק 3.3.4.8.1 **לעיל**.

16 ראו חלק 3.4.3.4 **לעיל**.

17 ס' 11 לחוק סוכנות הביון הפדרלית (BNDG).

18 ראו חלק 3.5 **לעיל**.

19 ע"פ 4211/91 ***מדינת ישראל נ' אלמצרי***, פ"ד מז(5) 624 (1993).

20 בעניין **אבו־רקיק**, **לעיל** בפרק 2 בה"ש 77, נקבע כי חוק האזנת סתר אינו חל על האזנת סתר שבוצעה בדרום לבנון בתקופה שבה פעלו הרשויות הישראליות באזור זה.

ויסמונסקי להלכת **אלמצרי** היא כי אין לקרוא לתוכה היתר כללי להאזנות סתר "מינהליות" אקס־טריטוריאליות, וכי נגזר ממנה גם כי סמכויותיה של משטרת ישראל להאזנות סתר הן טריטוריאליות כל עוד לא נקבע אחרת במפורש.[21]

בעניין **עסאף**[22] הבהיר בית המשפט כי די בהיתר להאזנה לאחד מהצדדים לשיחה היושב בתחומי המדינה – לענייננו, די בכך שצד מהצדדים לתקשורת בעל זיקה טריטוריאלית כדי להחיל עליו את הוראות חוק האזנת סתר.

האיסוף של נתוני תקשורת על ידי המשטרה לפי חוק נתוני תקשורת הוא טריטוריאלי מטבעו, שכן הוא חל על מאגרי מידע מקומיים של בעלי רישיון בזק מקומיים. עם זאת אם ספקי התקשורת אוספים נתונים על פעילות מנוייהם מעבר לים או בשטחים שבשליטת ישראל – החוק אינו מחיל מגבלות טריטוריאליות על הנתונים שעל הספק להעביר למשטרה.

באשר לסמכויותיו של שירות הביטחון הכללי ושל סוכנויות הביון האחרות הנוגעות להאזנות סתר למטרות של ביטחון המדינה, הדין הישראלי אינו מכיל הגבלה טריטוריאלית או פרסונלית. יש יסוד סביר להניח כי האזנות הסתר ליעדים שאינם ישראליים המצויים מחוץ לשטחה של ישראל (ובכלל זה, בשטחי יהודה ושומרון) וכן המעקב המקוון אחריהם שמבצעים אמ"ן[23] או השב"כ למטרות ביטחוניות אינם נופלים בגדרי ההוראות של חוק האזנת סתר. תחולת הדין באשר לאזרחי ישראל המצויים מחוץ לישראל ולשטחים שבשליטתה אינה ברורה. מקל וחומר סביר להניח כי הדין אינו מחיל במפורש הגבלות טריטוריאליות או פרסונליות על האיסוף שאוספים שירות הביטחון הכללי או גופי ביון אחרים נתוני תקשורת, אם מדובר בתכליות ביטחוניות.

אף שלפי המקובץ נראה שתחולת סמכויות האיסוף של גופי החקירה והביטחון בדין הישראלי אינה מבחינה לרוב בין אזרחים ישראלים לאזרחים זרים, או בין

21 ויסמונסקי, **לעיל** בפרק 2 ה"ש 26, בעמ' 120–122.

22 ע"פ 568/99 **עסאף נ' מדינת ישראל**, פ"ד נה(4) 374 (2001).

23 לטענות יוצאי יחידת 8200 בנוגע להפרת פרטיותם של יעדים מודיעיניים בשטחים ראו לדוג' אליאור לוי "'היינו שם. עשינו את זה ואנחנו לא מסוגלים עוד להמשיך'." סרבני 8200 מדברים" **Ynet** (12.09.2014).

הצדדים לתקשורת במקום מושבם (לרבות מקום המושב – או המעבר – של התקשורת עצמה), הפעלת סמכויות אלו מוגבלת בחוק־יסוד: כבוד האדם וחירותו. אבל גם שאלת תחולתה של חזקת הטריטוריאליות שבדין הישראלי על חוק־יסוד: כבוד האדם וחירותו, לרבות על הזכות לפרטיות המוקנית מכוחו, טרם הוכרעה.[24]

בעניין **המועצה האזורית חוף עזה**[25] נקבע כי לחוקי היסוד יש תחולה פרסונלית על מתיישבים ישראלים בשטחים שבשליטת ישראל. עם זאת את שאלת תחולתם על מי שאינם ישראלים ומצויים בשטחים שבתפיסה לוחמתית ישראלית, או על ישראלים המצויים בשטח שאינו בשליטת ישראל – את אלה השאיר בית המשפט בצריך עיון.[26]

לדעת ברק, על הסדרים חוקתיים העוסקים בזכויות אדם אין להחיל חזקה טריטוריאלית, והחובה של בעל הסמכות השלטונית לכבד את הזכויות שבהסדרים אלה חלה על כל פעולה שהוא מבצע – אם בתחומי המדינה ואם מחוץ לה.[27] לפי גישה זו, גם על מעקב מקוון אקס־טריטוריאלי, לרבות אחר אזרחים זרים, חלות המגבלות החוקתיות המגינות על הזכות לפרטיות. עם זאת המגבלות החוקתיות על מעקב מקוון לתכליות של הגנה על ביטחון המדינה, במיוחד לאור הדין המשווה, הן יחסיות. בחינת המידתיות של אמצעי מעקב שונים אחר יעדים אקס־טריטוריאליים או זרים לפי תכליות אלו עשויה לייצר את ההבחנות הקיימות בדין המשווה באשר לרמת הפגיעה המותרת בפרטיות של היעד המודיעיני (או של צדדים שלישיים) לפי רמת הזיקה הטריטוריאלית או הפרסונלית שלו לישראל.

24 ראו אהרן ברק **כבוד האדם – הזכות החוקתית ובנותיה** 403–402 (2014). עם החזקות הפרשניות שתכליתן להבטיח את קיומו של שלטון חוק פורמלי ברק מונה את חזקת הטריטוריאליות, שלפיה לחוק הישראלי יש תחולה מקומית, ואת חזקת היעדר התחולה של החוק הישראלי באזורי יהודה, שומרון וחבל עזה. אהרן ברק **פרשנות במשפט, כרך שני: פרשנות החקיקה** 581–578 (1993).

25 בג"ץ 1661/05 **המועצה האזורית חוף עזה נ' ראש הממשלה**, פ"ד נט(2) 481 560–559 (2005).

26 ראו **שם**; וכן ראו ויסמונסקי, **לעיל** בפרק 2 ה"ש 26, בעמ' 151, וכן פס' 99–104 לתגובת היועץ המשפטי לממשלה בחודש נובמבר 2017 לעתירות ולבקשות לצווי ביניים בבג"ץ 2055/17 **עיריית סילואד נ' הכנסת**.

27 ראו ברק (2014), **לעיל** בפרק זה ה"ש 24, **שם**.

.4.2 זליגת מודיעין (intelligence creep)

הדין החל על רשויות ממשל לאומיות בבואן לאסוף מידע אישי, לעבדו או להשתמש בו במסגרת או בעקבות מעקב אחר רשתות תקשורת, כולל מגוון הסדרים, לפי תכליות המעקב. למעקב מקוון ייתכנו תכליות שונות, למשל: הגנה על הביטחון הלאומי, מניעת פשיעה, אכיפת דיני המס או אכיפה מוניציפלית[28] וכן שיפור השירות לאזרח. על רמת הפגיעה בחירויות ובזכויות של מושאי המידע להיות במידה הנדרשת לפי התכלית.

מאחר שברוב המקרים ההסדרים החלים על מעקב מקוון למטרות של ביטחון לאומי נוטים להקל בהשוואה לאלו החלים על מעקב למטרות של אכיפת חוק, המידע שנאסף לתכליות של ביטחון לאומי עשוי להיות רב ואיכותי יותר. אין תמה אפוא כי בקרב רשויות אכיפת החוק רב הפיתוי למצוא דרכים להשיג מידע שנאסף לתכליות אלו ולהשתמש בו למטרותיהן אם הדין אינו מתיר להן לאסוף אותו לתכליות של אכיפת חוק או מניעת פשיעה. לכן, לצד עיצוב הסדרים שונים לתכליות שונות של מעקב מקוון, שיטות משפט שונות מבקשות לצמצם מצבים של זליגת מידע בין הרשויות לתכליות שאין בהן כדי להצדיק את איסופו המקורי.

כך למשל בארצות הברית עיצב התיקון הרביעי לחוקה הסדרים נפרדים לסוכנויות מודיעין וביטחון לאומי ולרשויות אכיפת החוק. מודיעין שנאסף

28 לפי פרסומים בעיתונות, העבירה משטרת ישראל לעיריית ירושלים שמות של חשודים בעבירות ביטחון כדי שזו תפעיל נגדם סמכויות אכיפה מוניציפליות. יובהר כי אין זה מקרה מובהק של זליגת מודיעין שבו השתמשה העירייה במודיעין שאספה המשטרה כדי לשרת את מטרותיה. עם זאת זו דוגמה של שימוש לרעה של המשטרה במידע (הנעשה באמצעות זליגת מודיעין) לשם הפעלה בררנית של סנקציות מוניציפליות כאמצעי המייצר לחץ אפור, שבו העירייה פועלת כזרועה הארוכה של המשטרה. ראו ניר חסון "הרשימות השחורות של עיריית ירושלים לענישת תושבים ערבים ממזרח העיר" **הארץ** 10.3.2015.

למטרות של ביטחון לאומי, לפי כללים מקילים ובקרה שיפוטית רופפת, עשוי – בהיעדר חומות סיניות בין סוכנויות הביון לגופי אכיפת החוק – לשמש לצורכי חקירות פליליות או למטרות אחרות שחורגות ממטרת האיסוף המקורית.[29] מבחינת מוסדית, בהתחשב בכך שסוכנות אכיפת החוק הפדרלית – ה־FBI, שהיא גם לשכת החקירות הפדרלית – ממלאת גם תפקידים הקשורים למטרות של ביטחון לאומי, החשש אינו בלתי מבוסס. טרם הרפורמה של חוק הטרור (USA PATRIOT Act) בשנת 2001 עיצב משרד המשפטים האמריקאי שורה של הסדרים שנועדו להפריד בין מודיעין זר שמקורו ב־FISA ובין חומרי חקירה אחרים, ועשה שימוש דל בסעיף 215 של FISA. אלא שרפורמת חוק הטרור של 2001 (USA PATRIOT Act) הביאה לידי קריסתם של הסדרים אלה.[30]

בגרמניה עקרון ה־Trennungsgebot,[31] המפריד בין סוכנויות אכיפת החוק לסוכנויות המודיעין, חולש על זליגת המודיעין. עיקרון זה נשחק בשנים האחרונות במידת מה בשל איום הטרור, ואנו עדים להקמתם של מרכזי ניתוח מודיעין משותפים לסוכנויות המודיעין והשיטור השונות ולמאגרי נתונים משותפים למטרות סיכול טרור. דוגמה לשחיקת עקרון ההפרדה הגרמני מצויה בעניין **מאגר ה־ATD** (Antiterrordatei). המאגר, שהוקם מכוח חוק מאגר המידע נגד טרור (ATDG – Antiterrordateigesetz),[32] ריכז נתונים שנאספו מארבעים סוכנויות ממשלה על חשודים בטרור, לרבות נתוני תקשורת; וכן מידע על מקומות מגורים, רישיונות נשק ורכב, לאום ודת.[33] המאגר נגיש לסוכנויות המודיעין הגרמניות וכן למשטרה הפדרלית של גרמניה (BKA) ולגופי המשטרה במדינות לתכליות של לוחמה בטרור.[34] עם זאת ניתן להשתמש במידע לתכליות

29 ראו **לעיל** בפרק 3 ה"ש 385. כן ראו גם Donohue, **לעיל** בפרק 3 ה"ש 39, בפרק 5 לספרהּ.

30 ראו Donohue, **לעיל** בפרק 3 ה"ש 39 **לעיל**, במבוא ובפרק הראשון לספרהּ.

31 ראו בחלק 3.4.3 **לעיל**.

32 Antiterrordateigesetz [ATD] BGBl. I, 3409 (להלן: חוק מאגר המידע נגד טרור (ATDG)).

33 ראו Miller, **לעיל** בפרק 3 ה"ש 788, בעמ' 8–9.

34 ס' 5 לחוק מאגר המידע נגד טרור (ATDG).

אחרות אם הדבר הכרחי לצורך חקירת פשע חמור או למניעת סכנה לחיי אדם, לגופו, לבריאותו או לחירותו, ובהסכמת הרשות שהזינה את המידע למאגר.[35] בפסק הדין בעניין **מאגר ה־ATD**[36] קבע בית המשפט החוקתי הגרמני כי מבנהו הכללי של ה־ATDG תואם את הזכות להגדרה עצמית מידעית (informational self-determination), אך הורה על כמה שינויים בפרטי ההסדר.[37]

הדין הישראלי כולל הוראות נפרדות בנוגע ליירוט תקשורת למטרות של ביטחון לאומי ולמטרות אכיפת חוק, וכן הסדרים נפרדים בנוגע לאיסוף נתוני תקשורת לכל אחת מתכליות אלה. לפי הוראות חוק השב"כ,[38] זליגה – או העברה – של מודיעין מהמשטרה לשירות הביטחון הכללי מתאפשרת לפי סמכותו של השירות לקבל ולאסוף מידע. זליגת מידע בכיוון ההפוך – מהשירות לגופים אחרים – מותרת לפי סמכות השירות להעביר מידע לגופים אלה, הכפופה לכללים חשאיים ולפי כל דין. מכל מקום, העברת מידע כאמור אל שירות הביטחון הכללי ומחוץ לו צריכה להיות לשם מילוי תפקידי השירות.[39]

עם זאת סעיף 7 לחוק השב"כ נוקט מינוח רחב בהגדרת ייעוד השירות ותפקידיו, ומינוח זה מאפשר לשירות מרווח תמרון פרשני, שבשילוב עם האופי החשאי של מלאכת הפרשנות עשוי לפתוח פתח לזליגת מודיעין לגופי חקירה אחרים.[40] החלטות ממשלה יכולות לתחום את גבולות סמכויות השירות[41] או להסדיר את חלוקת התפקידים בין השירות לגופי החקירה האחרים.[42] אבל גם השירות עצמו

35 ס'(1)(1)6 לחוק מאגר המידע נגד טרור (ATDG).

36 ראו **לעיל** בפרק 3 ה"ש 790.

37 עניין **מאגר ה־ATD**, בפס' 230–231.

38 חוק השב"כ, ס' 8(א).

39 כמפורט בחוק השב"כ, ס' 7.

40 ראו אריאל צימרמן **הצעת חוק השב"כ – ניתוח משווה** 18–28 (1997); רוטר, **לעיל** בפרק 2 ה"ש 105, בעמ' 37–40.

41 ראו למשל ס' 7(6) לחוק השב"כ.

42 ראו למשל החלטת ממשלה 2040 – הממשק בין משטרת ישראל לבין שירות הביטחון הכללי – הסדרת תחומי האחריות בין גופים אלה בנושא המודיעין בכל הקשור להפרות סדר (13.6.2004).

יכול לקבל החלטות המפרשות את הגדרת תפקידיו, כמו שהתברר בעניין **האגודה לזכויות אזרח נ' שירות הביטחון הכללי**,[43] שם תוארה החלטת השירות משנת 2009 בדבר הגדרת המונח "חתרנות". עם זאת יש לציין כי בדוח מבקר המדינה בעניין פרשת הרפז[44] סירב שירות הביטחון הכללי להעביר נתוני תקשורת לידי מבקר המדינה בטענה שלא ראוי שהשירות ישתמש ביכולותיו למען עניינים שלדעתו אינם נוגעים ישירות לתחומי אחריות והסמכות של השירות.[45] אין לדעת אם מקרה זה הוא בבחינת היוצא מן הכלל המעיד על הכלל, או אם שירות הביטחון הכללי אכן מקפיד בקלה כבחמורה להימנע מהעברת נתוני תקשורת לגופי חקירה וביטחון אחרים.

פסק הדין בעניין **האגודה לזכויות אזרח נ' משרד הפנים**,[46] שהתנה העברת נתונים בין רשויות העולה כדי פגיעה בפרטיות בעמידה במבחני המידתיות, עשוי לשמש פסק דין מנחה בהקשרים של העברת מידע מודיעיני בין רשויות. לפי פסק הדין, בהתאם לעקרונות המידתיות יש לצמצם את הפגיעה בזכות לפרטיות במקרים אלו באמצעות הסדרים פרטניים המבטיחים את מזעור היקף המידע המועבר לרשות המבקשת וצמצום מספר עובדי הממשל הנחשפים לחומר, והכול בהתחשב בתכלית שלשמה מבוקש המידע.

43 בג"ץ 5277/13 האגודה לזכויות אזרח בישראל נ' שירות הביטחון הכללי (7.2.2017), פס' כח.

44 מבקר המדינה **דו"ח ביקורת על פרשת "מסמך הרפז"** (2012), עמ' 24–25.

45 המינוח שנוקט שירות הביטחון הכללי בהמשך עשוי ללמד על הבחנה פנימית בין איסוף נתונים גולמיים מספקי התקשורת ("נתוני תקשורת שהוזרמו למערכותיו") למידע המופק מהם ("מחקר תקשורת" ובהמשך "איסוף" לשימוש במידע המופק (ראו **שם**, בעמ' 25). בעניין הרפז התנגד שב"כ להפקת מידע על סמך נתוני תקשורת גולמיים לבקשת מבקר המדינה. לא ברור אם עמדת השירות הייתה אחרת לו נעשה מחקר התקשורת במנותק מפניית המבקר.

46 **לעיל** בפרק 1 ה"ש 13. כן ראו בחלק 2.2 **לעיל**.

4.3. הצפנה

מקום שיש בו תקשורת, קם שם הסיכון שהיא תגיע לידי מי שלא נועדה לו. שיטות הצפנה של מסרים מלוות את האנושות מימים ימימה,[47] ובעידן המודרני הן משמשות שכבת הגנה נוספת של המשתמש מפני גישה לא מורשית של אחרים למידע השייך לו. הרשויות החוקרות וגופי האכיפה מעוניינים, על פי רוב, בהחלשת אמצעי ההצפנה העומדים לרשות המשתמשים בשוק כדי שתתאפשר להם גישה נוחה יחסית לנתונים המוצפנים, וכן ביצירת הסדרים המורים לצדדים שלישיים (ולעיתים למושא החקירה, לפי הנסיבות) לספק את מפתחות ההצפנה או לפענח בכוחות עצמם את ההצפנה של נתוני תוכן מוצפנים.

בארצות הברית ההוראות שבחוק הסיוע לרשויות אכיפה (CALEA) נועדו להבטיח את קיומה של תשתית טכנולוגית שתאפשר לספקיות התקשורת (כהגדרתן בחוק) לסייע לגופי החקירה והביטחון הלאומי לפי דין. החוק מורה לספקיות התקשורת לתכנן את מערכות התקשורת שלהן כך שיאפשרו בידוד תקשורות והעברתן לידי רשויות האכיפה או הביטחון הלאומי, ואם שירותים אלו כוללים יכולות הצפנה של תקשורת – על הספקיות להיות מסוגלות לפענחה.[48] אלא שתחולת הוראות ה־access by design של CALEA מוגבלת לספקיות תקשורת, ותחולתן על סוגים מסוימים של טכנולוגיית תקשורת מקוונת שנויה במחלוקת – כעולה בפרשת הפריצה למכשיר האייפון[49]

47 המקורות העבריים מכילים דוגמאות להצפנה. לפי פירוש רש"י, "ששך" שבירמיהו כה 26 ("ומלך ששך ישתה אחריהם") ו"לב קמי" שבירמיהו נא 1 ("הנני מעיר על בבל ואל ישבי לב קמי") הם בבל וכשדים בצופן אתב"ש, בהתאמה.

48 ראו בחלק 3.1.4 **לעיל**.

49 ראו **לעיל** בפרק 3 ה"ש 125, 126 והטקסט המפנה אליהן. ראו והשווה לשימוש הגרמני בפצחנות במיקור חוץ, **לעיל** בפרק 3 ה"ש 930.

ולמכשיר האקו (Echo)[50] ועל שאלות הכרוכות ב"אינטרנט של הדברים" (IoT) שטרם התעוררו.[51]

עם זאת לצד הוראות החקיקה שנועדו לאפשר גישה למידע המוצפן באמצעות שירותיהן של ספקיות תקשורת, נטתה ארצות הברית לאפשר שימוש בטכנולוגיית הצפנה חזקות בתחומיה והסתפקה בהחלת מגבלות על ייצוא טכנולוגיות הצפנה חזקות למדינות זרות, שרובן הוסרו בשלהי המאה ה־20.[52] אלא שמדיניות זו, לטענת סוכנויות המודיעין, מעיבה על יכולות האיסוף שלהן. ואכן, בשנים האחרונות העלו סוכנויות המודיעין האמריקאיות טענות בדבר "החשכת" מקורות האיסוף שלהם ("going dark") משום שאימצו טכנולוגיות הצפנה שאינן מכוסות ב־CALEA.[53] בהיעדר רגולציה חלופית קראו הסוכנויות לחברות התקשורת לפתח וולונטרית דלתות אחוריות שיאפשרו לסוכנויות

50 ראו **לעיל** בפרק 3 ה"ש 77.

51 היעדר הבהירות בנוגע לתחולת CALEA על טכנולוגיות אלו יכול דווקא לשרת את הממשל. יש המפרשים את CALEA כאוסר על הממשל להוציא צו לפי ה־All Writs Act, המורה ליצרנים או לספקים של טכנולוגיות שה־CALEA חל עליהן, לתכנן את הארכיטקטורה שלהם עם "דלתות אחוריות" מסוימות.
ראו (1)(b)47 U.S.C. §1002, וכן Lidiya Mishchenko, *The Internet of Things: Where Privacy and Copyright Collide*, 33 Santa Clara Computer & High Tech. L. J. 90, 92 (2016–2017)

52 ראו תעתיק ממסיבת עיתונאים בבית הלבן מיום 16 בספטמבר 1999, Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, White House, Office of the Press Sec'y (Sept. 16, 1999)

53 ראו עדותה של היועצת המשפטית של ה־FBI בפני ועדת המשנה של בית הנבחרים לפשע, טרור וביטחון פנים: Valerie Caproni, *Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security* (February 17, 2011); כן ראו את הנאום שנשא לאחרונה סגן התובע הכללי באקדמיה של הצי: Department of Justice, *Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy* (10.10.2017)

האכיפה והביטחון גישה לפי דין לנתוני תקשורת ותוכן.[54] יש הסוברים כי על היעדר הגישה לתקשורת מוצפנת אפשר לחפות באמצעות פוטנציאל ה־metadata העשיר של מכשירי IoT.[55]

הדין הבריטי כולל הסדר לעניין הסמכות להורות על מסירת מפתח הצפנה (decryption key או סיסמת הגישה).[56] הסדרים דומים קיימים בין השאר בדין האוסטרלי, בדין הקנדי, בדין הניו־זילנדי[57] ובדין הרוסי.[58] גם הדין ההודי, בכללי יירוט ניטור ופענוח המידע, כולל הסדר דומה, ולפיו הממשלה רשאית להורות למי שמחזיק במפתח ההצפנה למסור אותו, לאפשר גישה לחומר המוצפן או לפענח אותו.[59] יתר על כן, הממשלה המרכזית (הפדרלית) של הודו מוסמכת, מכוח סעיף 84A בחוק ההודי בדבר טכנולוגיות מידע (ITA), לקבוע את שיטת ההצפנה הלאומית המותרת. רמת ההצפנה המרבית המותרת לפי רישיונות ספקי האינטרנט היא של 40 ביט, הנחשבת חלשה ומיושנת,[60] והיא חלה לא רק

54 ראו David Kravets, *FBI Chief Tells Senate Committee We're Doomed Without Crypto Backdoors,* Ars Technica (Jul. 8, 2015)

55 Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybsecurity-Centric Encryption Era*, 17 N.C. J.L. & Tech. 599 (2015-2016)

56 ס' 49–56 לחוק הסדרת סמכויות חקירה 2000 (RIPA) והתוספת השנייה לחוק.

57 ראו ויסמונסקי, **לעיל** בפרק 2 ה"ש 26, בעמ' 217.

58 בשנת 2016 התקבלו בפרלמנט הרוסי תיקוני חקיקה המורים לגופים המפיצים מידע מקוון (לשון אחר, כל רשת חברתית, פלטפורמה או אתר המאפשר החלפת מסרים בין משתמשיו) להעביר את מפתחות ההצפנה שלהם לסוכנות הביטחון הפדרלית הרוסית (FSB). לאחרונה קבע בית המשפט העליון ברוסיה כי לפי הוראות החוק, על חברת טלגרם – מפתחת פלטפורמת המסרים המיידיים בעלת אותו השם – למסור לידי סוכנות הביטחון הפדרלית את מפתחות ההצפנה לתקשורת בין משתמשיה. ראו Evgeny Berg, *Russia's Controversial "Yarovaya Package" Targets Missionaries, Threatens Privacy*, Legal Dialogue (November 2016); "בית המשפט ברוסיה: טלגרם חייבת לשתף פעולה עם גורמי המודיעין במדינה" **הארץ** 21.3.2018.

59 ס' 2(h), 5 לכללי יירוט, ניטור ופענוח המידע, **לעיל** בפרק 3 ה"ש 960.

60 ראו למשל Robert Sanders, The Only Legally Exportable Cryptography Level is Totally Insecure; UC Berkeley Grad Student Breaks Challenge Cipher in Hours, University of California at Berkeley Public Information Office (29.0.1997)

על הספקים עצמם, אלא גם על אנשים פרטיים, על תאגידים או על גופים אחרים המשתמשים בהצפנה.[61]

בשונה מהמחלוקת בין חברת אפל לבולשת הפדרלית האמריקאית בפרשת האייפון,[62] בסופו של העימות בין ממשלת הודו לחברת בלקברי בשנת 2010 בחרה בלקברי לאפשר גישה חלקית ליירוט ולניטור של שירותי התקשורת שלה באמצעות שירותי הביטחון ההודיים, אך לא סייעה בפיענוח תקשורת של מתקני האינטרה־נט שלה.[63]

בשנת 2015 הפיצה ממשלת הודו את טיוטת מדיניות ההצפנה הלאומית. לפי ההוראות של מדיניות זו, יש לשמור נתונים בפורמט טקסט טהור (לא מוצפן) למשך 90 יום. בהמשך הופץ נספח הפוטר מהמדיניות רשתות חברתיות ופלטפורמות דומות (ווטסאפ, פייסבוק, טוויטר, פלטפורמות מסחר אלקטרוני וכו'). לאחר שהועלו הסתייגויות מהמגמה הכללית של מסמך המדיניות, הטיוטה נזנחה.[64]

הדין הישראלי כמעט חף מהתייחסויות להצפנה.[65] ההתייחסויות המעטות בפסיקה לאמצעי הצפנה והתממה של משתמשים נעשו בהקשרים שבהם אמצעים אלה משחקים לרעת המשתמשים בהם. בעניין **זלטוקובסקי** היה השימוש באמצעי ההצפנה אינדיקציה למסוכנות.[66] בעניין **לוריא** סייע השימוש באמצעי הצפנה ובדפדפנים המאפשרים גלישה אנונימית לקבוע כי התכנים

61 Pranesh Prakash & Japreet Grewal*, How India Regulates Encryption,* the Centre for Internet and Society (30.10.2015)

62 **לעיל** בפרק 3 ה"ש 123.

63 Sanjay Singh, No Secrets on Blackberry: Security Services to Intercept Information After Government Gets Its Way on Popular Messenger Service, Daily Mail (7.4.2012)

64 ראו Arun, **לעיל** בפרק 3 בה"ש 1040, בעמ' 461.

65 ראו ויסמונסקי, **לעיל** בפרק 2 ה"ש 26, ה"ש 140, **שם**, בעמ' 216.

66 ראו עניין **זלוטובסקי**, **לעיל** בפרק 2 ה"ש 40.

המוצפנים הם פדופיליים.[67] במקרים אלה ההצפנה נתפסה כמרכיב של metadata שיש בו כדי להעיד על התוכן המוצפן או על יסודות נסיבתיים אחרים.

לא ברור אם הסמכת ראש הממשלה לתת הוראות לבעלי רישיון בזק בדבר "התקנת מיתקן, ביצוע פעולת בזק, או ביצוע התאמה טכנולוגית למיתקן בזק, בידי בעל הרישיון או בידי נציג כוחות הביטחון בסיוע בעל הרישיון, לרבות מתן גישה למיתקן, ככל שהדבר דרוש לצורך ביצוע תפקידיהם של כוחות הביטחון או להפעלת סמכויותיהם לפי כל דין"[68] מתייחסת גם למתן גישה לחומר מוצפן או ל־access by design בדומה להוראות האלה שבדין האמריקאי (CALEA).

בהקשר אחר, בהכרה שהשימוש באמצעי הצפנה יכול לשמש חרב פיפיות ושגורמים עוינים ופליליים ישתמשו באמצעים אלה למטרות פסולות,[69] מסדיר הדין הישראלי את השימוש באמצעי הצפנה בצו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), התשל"ה–1974.[70] לפי הצו, לא יעסוק אדם באמצעי הצפנה מבלי שיקבל לשם כך רישיון מאת מנכ"ל משרד הביטחון.[71] עיסוק באמצעי הצפנה אינו מוגבל לשימוש גרידא וכולל גם פיתוח, ייצור, שינוי,

67 ת"פ 42667-02-15 **מדינת ישראל נ' לוריא** (פורסם בנבו, 15.01.2017). ראו אסף הרדוף "'לא משחק ילדים': חוקיות חיפוש ותועבה פדופילית בעקבות ת"פ 42667-02-15 מדינת ישראל נ' לוריא" 5 **המשפט ברשת: זכויות אדם** 70 (2017); יהונתן קלינגר "מדינת ישראל נ' לוריא: הרשעה על סמך שמות קבצים" Intellect Or Insanity (19.1.2017).

68 ס' 13(ב)(2) לחוק הבזק.

69 מערכת אתר משרד הביטחון "עיסוק באמצעי הצפנה". מקוון.

70 צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), התשל"ה–1974, ק"ת 3232 תשל"ה (6.10.1974), בעמ' 45, כפי שתוקן לאחרונה באכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) (תיקון), התשנ"ח–1998, ק"ת 5917 תשנ"ח 5917 (13.8.1998), בעמ' 1107 (להלן: צו הצופן ואכרזת הצופן).

71 ס' 2(א) לצו הצופן. "אמצעי הצפנה" כמשמעותם באכרזת הצופן הם "(1) מניעת הבנה של מידע באופן מוחלט או חלקי, הנעשית על ידי שינוי של המידע או של דרך העברתו, תוך שימוש בנוסחאות מתמטיות או מתכוני (אלגוריתמי) חישוב, בין באמצעות מפתח ובין בלעדיו, ובדרך שניתן לשחזר בעזרתה את המידע המקורי או חלק ממנו; (2) תיאום מפתחות הצפנה".

שילוב, החזקה, העברה, ייבוא, הפצה, מכירה או ייצוא שלהם.[72] עם זאת משרד הביטחון רשאי להכריז על אמצעי הצפנה כעל "אמצעי חופשי" שאינו דורש רישיון.[73] מאחר שרוב התקשורת באינטרנט משתמשת באמצעי הצפנה שונים, שרובם שקופים למשתמש, נשמעה ביקורת כלפי צו הצופן על שאינו מתאים לפרקטיקה, שכן הוא גזרה שאין הציבור יכול לעמוד בה.[74] לכן במסגרת הקלות שביצע המשרד בשנת 2000 הורחב הפטור מרישיון כך שיכלול אמצעי הצפנה מסחריים שהוסרו מרשת האינטרנט לצורכי שימוש עצמי, לאבטחת מידע או לחתימה אלקטרונית.[75]

4.4. שימור נתונים (data retention)

לשני היבטים של שימור נתונים יש להתייחס: הראשון הוא היקף החובה שבדין החלה בעיקר על בעלי מאגרי מידע וספקי שירותי תקשורת – לשמור נתוני תקשורת ותוכן כדי שבשלב מאוחר יותר יהיה המידע זמין לגופי החקירה לפי צו או דרישה אחרת. ככל שהחוק נותן לגופי החקירה סמכויות נרחבות יותר של יירוט תקשורת, כך מתייתר הצורך (של אותם גופים) בהחלתה של חובת שימור נתונים, ולהפך – ככל שהחוק מגביל את יכולתם של גופים אלו לעסוק ביירוט ישיר של תקשורת, כך הם תלויים יותר בשימור נתונים על ידי ספקי התקשורת.

ההיבט השני של שימור נתונים עוסק במידע המודיעיני המצוי אצל גופי החקירה ובמגבלות החלות על שימורו (או בהיעדרן של כאלה). ככל שהוראות לביעור

72 ס' 1 לאכרזת הצופן.

73 ס' 3א–3ב לצו הצופן.

74 חיים רביה, "אי סבירותו של צו הצופן (חלק ראשון)" (25.1.2000) **law.co.il**; חיים רביה, "אי סבירותו של צו הצופן (חלק שני)" (2.2.2000) **law.co.il**; חיים רביה, "אי סבירותו של צו הצופן (חלק שלישי)" (9.2.2000) **law.co.il**.

75 ס' 2(א)(2) למדיניות פיקוח ורישוי אמצעי הצפנה מסחריים, כפי שפרסם משרד הביטחון ביום 24.9.2000.

מידע המוחזק אצל גופים אלו יהיו מתירניות יותר, כך גדל החשש לשימוש במידע החורג מתכליות האיסוף המקוריות שלו, לרבות שימוש לרעה במידע או זליגת מודיעין. מנגד, ככל שהדרישה לבער מידע כאמור נוקשה יותר, כן הדבר גורע מיכולות הניתוח המודיעיניות של גופי החקירה.

4.4.1. דרישה לשימור נתונים מבעל המאגר

הדין האמריקאי חסר הוראה כללית לשימור נתונים, למעט החריג שבהוראה לחברות טלפוניה לשמור על נתוני תקשורת מסוימים לתקופה שלא תפחת מ־18 חודש.[76] אף שגם בהיעדר הוראה סטטוטורית לעשות כן ספקי שירותי התקשורת שומרים נתוני תקשורת ותוכן במשך תקופות ארוכות,[77] הנשיא אובמה ניסה להתנות את סיום תוכנית האיסוף הנרחבת של נתוני תקשורת[78] בהחלתה של חובת שימור נתונים על ספקי שירותי התקשורת.[79] בהיעדר דרישה כללית לשימור נתונים, ספק נתוני תקשורת מחויב לשמור ל־90 יום (תקופה שניתנת להארכה) נתונים שביקשה ברשות חקירה מכוחו של חוק תקשורת שמורה (SCA) כל עוד לא ניתן צו שיפוטי המורה להעבירם לרשות.[80] כחלק מבקשה כזאת הרשות יכולה להורות שנוסף על ההימנעות ממחיקת הנתונים המבוקשים יכין ספק השירות עותק גיבוי של אותם נתונים.[81]

76 ראו 47 C.F.R. §42.6 (2012), שלפיו ספקים של שירותי תקשורת טלפונית נדרשים לשמור את אלה: שם המנוי, כתובתו, מספר הטלפון שאליו התקשר, מספר הטלפון שממנו התקשר, מועד השיחה ואורכה.

77 ראו לדוגמה את נתוני השימור של ספקיות הסלולר הגדולות בארצות הברית כפי שרוכזו במשרד המשפטים האמריקאי משנת 2010 במסמך שחשפה ופרסמה האגודה לזכויות אזרח, Department of Justice, *Retention Periods of Major Cellular Service Providers* (August 2010)

78 ראו חלק 3.1.6 **לעיל**.

79 ראו Michael J. Woods, *Data Retention Requirements and Outsourced Analysis: Should Private Entities Become Government Surrogates in the Collection of Intelligence*, 4 Am. U. Bus. L. Rev. 49, 62 (2015)

80 18 U.S.C. §2703(f)

81 18 U.S.C. §2704

במשטר הגנת הפרטיות האירופי שימור נתונים הוא סוגיה רגישה יותר. בשל הזכות להישכח – שמושאי המידע נהנים ממנה לפי דיני האיחוד[82] –מושא מידע רשאי לפנות בנסיבות מסוימות למעבד בדרישה לתיקון או למחיקה של מידע בקשר אליו. זכות זו נוגדת אינטרסים ביטחוניים ואחרים לשימור המידע, וכדי להתגבר עליה יש צורך בחקיקה שמחריגה נתונים מסוימים לשימור (דוגמת דירקטיבת שימור הנתונים)[83] או בהגברה של מאמצי האיסוף המודיעיניים בזמן אמת (יירוט ועיבוד תקשורת טרם הפעלת הזכות להישכח).[84]

בעניין *Digital Rights Ireland* (*DRI*) פסל בית הדין האירופי לצדק (ECJ) את דירקטיבת שימור הנתונים,[85] ומאוחר יותר – בעניין *Tele2 Sverige AB* – הוא קבע כי הסדרה לאומית של שימור נתונים לפי חוקי האיחוד אינה יכולה להיות כללית וחסרת הבחנה. אפשר לחייב ספקי נתונים לשמור נתונים רק במקרים שבהם חל צורך מוחלט בשימור ורק במסגרת הסדרה בחקיקה מדינתית של שימור נתוני תקשורת. הסדרה כזאת צריכה לכלול הגבלות ובקרות מתאימות לקטגוריות הנתונים הנשמרות, לאמצעי התקשורת שמהם נאספים הנתונים, להיקף מושאי המידע שהנתונים הנשמרים הם עליהם ולתקופת השימור.[86] חקיקה כזאת נדרשת להגדיר תנאים מהותיים ופרוצדורליים שלפיהם ייתנו ספקי שירותי תקשורת לרשויות המוסמכות גישה לנתונים אלו, ועל הנתונים להיות קשורים למי שמבצע "פשעים חמורים" (לרבות מעשי טרור) אם יש ראיות שהנתונים המבוקשים תורמים להגשמת המטרות. פרט למקרים

82 זכות זו אינה מוכרת במפורש בדירקטיבת הגנת המידע; עם זאת זכותו של מושא המידע לדיוק ולרלוונטיות במידע יכולה לשמש בסיס לזכות להישכח, ראו ECJ, Case 131/12 (Google Spain and Google v. AEPD and Costeja González) (2014). התקנות הכלליות בדבר הגנת מידע (GDPR) מתייחסות במפורש לזכות להישכח.

83 ראו בחלק 3.2.4 **לעיל**.

84 לפי ההנחה שיירוט תקשורת נעשה בלי הסכמתו של מושא המידע, על מנת להכשיר אותו יש לעשותו, במשטר הגנת המידע הקיים, למטרות המחריגות אותו מתחולתה של דירקטיבת הגנת המידע, ובכפוף לתנאים שהציבה ההלכה האירופית (ראו בחלק 3.2.2 **לעיל**).

85 ראו בחלק 3.2.4 **לעיל**.

86 עניין *DRI*, **לעיל** בפרק 3 ה"ש 228, פס' 108–109.

דחופים, נדרשת ביקורת שיפוטית (או של רשות עצמאית) על בקשות לנתונים אלו.[87]

ההסדר החדש שבחקיקה הבריטית, המצוי בחוק סמכויות החקירה 2016 (IPA), כולל הוראות בדבר שימור נתוני תקשורת אצל הספקים מכוח הודעה שנותן השר. שימור הנתונים אצל הספקים לפי צו כאמור מוגבל לתקופה של 12 חודשים.[88] עם זאת גם ללא הודעת שימור נתונים הספקים עדיין יכולים לשמור נתונים לצורך מתן השירות או לתכליות אחרות בתנאי שהדבר הולם את דיני הגנת הפרטיות הכלליים (עקרונות הגנת המידע שבחוק הבריטי בדבר הגנת מידע 1998 (DPA), ובעתיד – לפי ההתפתחויות שאחרי הברקזיט – עקרונות הגנת המידע שבתקנות הכלליות בדבר הגנת מידע (GDPR) או שבהצעת החוק הבריטי בדבר הגנת מידע (DPB).[89] כפי שתואר לעיל, יש הסבורים כי נוסח ההסדר ב־IPA עדיין אינו תואם את הדין האירופי בשל התכליות הרחבות שלשמן יתאפשר לתת הודעת שימור נתוני תקשורת.[90] יש לציין כי ב־IPA אין מגבלה נוקשה על תקופת שימורם של נתונים שהושגו מכוח הודעת שימור נתוני תקשורת, והם יוחזקו כל עוד יש בהם צורך. כמו כן החוק אינו מגביל במפורש את היקף החומר המבוקש בהודעת שימור, אך הוא מתווה אמות מידה כלליות שלפיהן על השר לשקול את מתן ההודעה, בין השאר את מספר המשתמשים,[91] וכן קובע הוראות לנציב הבוחן את ההודעה להביא בחשבון שיקולי פרטיות.[92]

חוק הטלקומוניקציה הגרמני (TKG) מורה לספקי תקשורת לשמור נתוני מיקום לתקופה של ארבעה שבועות, ונתוני תעבורה מסוימים – למשך עשרה שבועות. הסדר זה נתקף בבית המשפט הגבוה לעניינים מינהליים במדינת נורדריין־וסטפאליה, שמצא כי ההסדר, בהתירו שימור נתונים גורף, אינו עומד בדרישות

87 **שם**, פס' 120.

88 ראו חלק 3.3.4.6 **לעיל**.

89 ראו חלקים 3.3.3–3.3.2 **לעיל**.

90 ראו חלק 3.3.4.10 **לעיל**.

91 ס' 88(1) לחוק סמכויות חקירה 2016 (IPA).

92 כמפורט בחלק 3.3.4.3 **לעיל**.

שקבע בית הדין האירופי לצדק (ECJ) בעניין *Tele2 Sverige AB*. בעקבות החלטת בית המשפט הודיע הרגולטור כי הוראות שימור הנתונים שבסעיף 113b לחוק הטלקומוניקציה הגרמני (TKG) לא ייאכפו על ספקי תקשורת אחרים עד להחלטה עקרונית בעניין.[93]

בשונה מהרגישות האירופית לשימור נתונים ולאדישות האמריקאית בעניין, הדין ההודי מורה לספקי התקשורת, לפי תנאי הרישיונות שלהם, לשמור את תעבורת התקשורת במערכותיהם לתקופה שלא תפחת משנה.[94] נוסף על כך, הכללים המנחים לספקי התקשורת מורים על שימור נתונים שהוסרו לתקופה של תשעים יום.[95] ספקים מסדר שני, כגון מפעילי סייבר־קפה, נדרשים לשמור תיעוד של פעילות לקוחותיהם לתקופה של שנה לפחות.[96]

בישראל חוק הגנת הפרטיות והתקנות מכוחו אינם כוללים הוראות כלליות הנוגעות לתקופת שמירת הנתונים במאגר המידע, לנתונים המותרים לשמירה מבחינתם תוכנם, לתקופת החזקה מרבית בנתונים או כל היבט אחר של שימור נתונים (data retention).[97] יש הרואים בחקיקה של חוק נתוני תקשורת כמכוננת את החובה לשמירת הנתונים שהמשטרה רשאית לבקש מכוחו.[98] עם זאת נראה כי במקרים מסוימים חברות התקשורת נמנעות משימור נתונים.[99]

93 ראו חלק 3.4.3.2 **לעיל**.

94 ראו Iyengar, **לעיל** בפרק 3 ה"ש 986; Abraham, **לעיל** בפרק 3 ה"ש 969, בעמ' 308.

95 ס' 3(4) לכללים המנחים לספקי התקשורת.

96 ראו חלק 3.5.2.3 **לעיל**.

97 ראו גם חי, **לעיל** בפרק 2 ה"ש 45, בעמ' 45. כמו כן בתקנות שמירת מידע והעברתו בין גופים ציבוריים (תקנת משנה 13) יש הוראה לביעור אמצעי רישום מגנטיים ופלט מחשב כתוב של הליכי ביניים של עיבוד נתוני מידע — אך אין התייחסות לביעור נתונים מתוך מאגר המידע גופא.

98 **שם**, בעמ' 46, מפנה חי לעמדת היועץ המשפטי לממשלה מיום 7 ביוני 2009 במסגרת ת"א 1994/06 (מחוזי ת"א) **אמיר לירן נ' פלאפון תקשורת ואחי** (להלן: עניין **לירן**).

99 לדוגמה, בעקבות בקשה לאישור תובענה ייצוגית שהוגשה נגד חברת פלאפון תקשורת בע"מ על שהיא שומרת את המסרונים שנשלחים למנוייה (ת"צ (מחוזי מר') 21185-07-09 **סודרי נ' פלאפון תקשורת בע"מ** (פורסם בנבו, 7.9.2011)), וההד התקשורתי שנלווה לה, הודיעה חברת פלאפון כי היא תחדל מלשמור את המסרונים. ראו אמיתי זיו "סימוס הוגן: פלאפון תפסיק לשמור הודעות SMS של לקוחות" **הארץ** 29.7.2009.

עם זאת סעיף 11(ה) לחוק השב"כ מקנה לראש הממשלה את הסמכות לקבוע בכללים הוראות שלפיהן ייקבעו הדרך שבה על בעל רישיון הבזק לשמור את המידע, תקופת השמירה ודרכי העברת המידע לשירות. חובה זו חלה אפוא לכל היותר על נתונים שאינם נתוני תוכן. מנגד, דן חי מציין כי בתי המשפט הגיעו כדי מסקנה שספקיות אינטרנט אינן חייבות לשמור כתובות IP.[100] כמו כן בדין אין איסור על עצם שימורו של מידע רגיש או מגבלות על תקופת שימורו של מידע רגיש בחברות תקשורת סלולרית.[101] בדברי חקיקה אחרים יש הוראות לשימור הנתונים בהקשרים הרלוונטיים להם – הוראות מס הכנסה (ניהול פנקסי חשבונות) או כללי הבזק (ביעור חומר ארכיוני שבידי החברה), התש"ן–1989.

עיון בדיווחי המשטרה על הפעלת סמכויותיה לפי חוק נתוני תקשורת[102] מעלה כי שיעור הצווים הניתנים בנוגע להשגת נתוני תקשורת "ישנים", מתקופה שעולה על שלושה חודשים ממועד הגשת הבקשה, נמוך יחסית (כ־6% עד 12% מתוך כלל הבקשות), אף שמשנת 2014 הוא במגמת עלייה. לא ברור אם הדבר נובע מצרכים מבצעיים של המשטרה או מהיקף מוגבל של שימור נתונים בחברות התקשורת.

מן המקובץ באשר לישראל, רב הנסתר על הגלוי, ולא ברור מהו היקף שימור הנתונים בחברות התקשורת. האם כללי השב"כ מורים על שימור מידע ללא הבחנה, או לפי מטרות מודיעיניות ספציפיות? האם רשויות אחרות השתמשו בנתונים שנשמרו לתכליות ביטחוניות מכוח כללי השב"כ לתכליות שאינן ביטחוניות (למשל במסגרת צו לפי חוק נתוני תקשורת)? האם המשטרה מסתמכת על שימור נתונים וולונטרי של בעלי רישיון בזק?

4.4.2. שימור נתונים בגופי החקירה והביטחון

הדין האמריקאי נוטה לשתוק בכל האמור לשימור נתונים בסוכנויות המודיעין ואכיפת החוק. עם זאת נתוני תוכן המיורטים לפי חוק האזנות סתר (WTA)

100 ראו חי, **לעיל** בפרק 2 ה"ש 45, בעמ' 46–47.

101 ראו פס' 9 לפסק דינה של השופטת ברון בעניין **לירן**, **לעיל** בפרק זה ה"ש 98.

102 בהסתמך על הנתונים שבדיווחי המשטרה. ראו **לעיל** בפרק 2 בה"ש 53.

יישמרו לתקופה של עשר שנים לפחות (בעודם חתומים), ולאחר מכן יושמדו בכפוף לצו שיפוטי.[103] הוראות מסוימות בנוגע לשימור נתונים מצויות בחוק איסוף מודיעין זר (FISA), המגביל את שימורם של נתוני תקשורת ותוכן שהושגו מכוחו ללא הסכמת הצדדים להם ובלי צו שיפוטי, לרבות נתוני תקשורת מאוחסנים, לתקופה של חמש שנים לכל היותר בתנאי שמי מהצדדים לתקשורת הוא אדם אמריקאי, ובכפוף לחריגים רחבים.[104]

ההתייחסות של דיני האיחוד האירופי לשימור נתונים בגופי חקירה וביטחון מצויה בדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680),[105] המורה למדינות־החברות להגביל את שימור הנתונים לתקופה סבירה[106] ולהקים נהלים לבחינה מעת לעת של הצורך בשימור נתונים ולבקרה על מחיקתם.[107] עם זאת שימור נתונים שנאספו כחלק מעיבוד נתונים לתכליות ביטחוניות שחורגות מתחולת הדירקטיבה אינו מוסדר בדיני האיחוד.

בדין הבריטי מצויות הוראות רלוונטיות בחוק סמכויות החקירה 2016 (IPA), שכלל מורה על ביעור מידע שהושג לפי רוב הצווים מכוחו (צו יירוט ממוקד[108]

103 18 U.S.C. § 2518(8)

104 ראו חלק 3.1.5 **לעיל**. החריגים נוגעים למידע שהוא מודיעין זר או נוגע לריגול נגדי, מידע שהוא ראיה פלילית ונשמר ברשות לאכיפת חוק, מידע שסביר להאמין שהוא מוצפן או שיש לו משמעות סודית, נדרש לשם הגנה מאיום מיידי לחיי אדם, נדרש למטרות אשרור טכניות, או שאושר לשימור לתקופה העולה על חמש שנים בידי ראש סוכנות הביון הרלוונטית, בכפוף לטעמים שניתנו בכתב לוועדות המודיעין של הקונגרס.

105 ראו חלק 3.2.5.2.1 **לעיל**.

106 סוגיית שימור נתונים פנימיים של המשטרה נדונה בעניין *Khelili v. Switzerland*, No. 16188/07 Eur. Ct. H.R. (2011). בפסק הדין נדונה מידת הפגיעה בזכות לפרטיות לפי סעיף 8 לאמנה האירופית לזכויות אדם (ECHR), באשר לתקופה של 15 שנים שבה העותרת סווגה בבסיסי הנתונים של משטרת ז'נווה כ"פרוצה".

107 ס' 5 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

108 ס' 53(5)–(6) לחוק סמכויות חקירה 2016 (IPA).

או כללי,[109] צו סייבר ממוקד[110] או כללי[111] וכן צו תפיסה כללי)[112] כשאין במידע צורך.

הדין הגרמני מקפיד על ביעורו לאלתר של כל מידע שהשיגו גופי הביטחון ואכיפת החוק אם הוא נוגע לגרעין של הזכות לחיים פרטיים – כך בהוראות קוד סדר הדין הפלילי הגרמני,[113] בחוק סעיף 10 (G10),[114] בחוק סוכנות הביון הפדרלית (BNDG)[115] ובהוראות המתאימות בחוק המשטרה הפדרלית (BKAG). נחיצות שימור המידע שהושג לפי אלו ייבחן מעת לעת, ולכשיתאיין הצורך בו – הוא יושמד.[116]

הדין ההודי מורה לספקי התקשורת, בכללם הטלגרף, לבער את התיעוד הפנימי שלהם בנוגע לצווי יירוט בחלוף חודשיים מתום היירוט.[117] רשויות הממשלה ידאגו לביעור החומר הקשור לצווים אלה ולתשדורות שיורטו מכוחם בחלוף שישה חודשים אלא אם יש בהם צורך.

כאמור לעיל, הדין הישראלי שותק בכל הנוגע לדרישות שימור של מאגרי מידע אצל בעל רישיון בזק. נוסף על כך, חוק נתוני תקשורת אינו כולל הוראות בנוגע לאופן השימוש בנתוני תקשורת שנתקבלו בהיתר לפי סעיפים 3 או 4 לחוק, בנוגע להחזקתם ולשימורם. לצד נתוני תקשורת שנתקבלו לפי ההיתרים שבחוק

109 ס' 150(6) לחוק סמכויות חקירה 2016 (IPA).

110 ס' 129(6) לחוק סמכויות חקירה 2016 (IPA).

111 ס' 192(6) לחוק סמכויות חקירה 2016 (IPA).

112 ס' 171(6) לחוק סמכויות חקירה 2016 (IPA).

113 ס' 100a(4) לקוד סדר הדין הפלילי הגרמני (StPO) וראו גם עניין הציתות ועניין מעקב התקשורת המונע, **לעיל** בפרק 3 ה"ש 790.

114 ס' 5a לחוק סעיף 10 (G10).

115 ס' 11 לחוק סוכנות הביון הפדרלית (BNDG).

116 ראו ס' 4 לחוק סעיף 10 (G10), ס' 100c(6)(1) לקוד סדר הדין הפלילי הגרמני (StPO), ס' 6 לחוק סוכנות הביון הפדרלית (BNDG) וכן ס' 20v לחוק המשטרה הפדרלית (BKAG).

117 כלל 419A(19) לכללי הטלגרף ההודיים, **לעיל** בפרק 3 ה"ש 962.

נתוני תקשורת, הסדיר החוק הקמת מאגר נתוני זיהוי המוגבלים יותר בהיקפם. תקנת משנה 5(ב) לתקנות נתוני תקשורת קובעת כי הנתונים שתועדו במאגר נתוני הזיהוי ותיעוד השימוש במאגר יישמרו לתקופה של חמש שנים לפחות. דן חי סבור כי בשל היסטוריית החקיקה, הארכת התקופה ליותר מחמש שנים טעונה הצדקה ראויה.[118]

באשר להוראות החלות בדין הישראלי בדבר שימור נתוני תוכן אצל גופי חקירה, ביעור של נתוני תוכן שהושגו בהאזנת סתר למטרות ביטחון מוסדר באמצעות כללים חסויים שיקבע ראש הממשלה. תנאי לביעורם של נתוני תוכן כאמור הוא ששמירתם אינה נדרשת.[119] ביעור נתוני תקשורת שהושגו בהאזנת סתר למטרות של מניעת עבריינות מותנה בקביעה של קצין משטרה מוסמך שהחומר אינו דרוש למניעת עבריינות או לגילוי עבריינים. הוראות אלו הוחלו גם על האזנות סתר שאינן טעונות היתר (למטרות השונות). כפי שנאמר לעיל, האזנות סתר שאינן טעונות היתר עשויות לכלול מעקב אחרי פרסומים גלויים ברשת וברשתות חברתיות.[120]

שימורם של נתוני תקשורת המצויים אצל שירות הביטחון הכללי והושגו מכוח סעיף 11 לחוק השב״כ,[121] מוסדר בכללים חסויים שאותם קובע ראש הממשלה.

נראה אפוא כי בדין הישראלי (וברוב הדינים הדומים במקומות אחרים) אין חסם עליון קשיח לתקופת שימורם של נתוני האזנת סתר, והוא מותנה בשיקול דעת מקצועי לפי הצורך בהם. שיקול הדעת של שירות הביטחון הכללי הוא ככל הנראה רחב מזה של גורמי המשטרה (שמירת חומר שאינו נדרש לעומת שמירת חומר שאינו נדרש למטרות גילוי עבריינות). עוד יוער כי בשני המקרים אין דרישה לצמידות המטרה – התנאי לביעור אינו צמידות בין חומר שהושג בתיק מסוים לבין חוסר דרישה לחומר למטרות הקשורות לאותו תיק, אלא למטרות הכלליות של האזנות סתר. גישה זו מאפשרת שיקול דעת רחב בשימור נתוני תוכן.

118 ראו חי, **לעיל** בפרק 2 ה"ש 45, בעמ' 179.

119 ראו חלק 2.5.5 **לעיל**.

120 ראו חלק 2.5.4 **לעיל**.

121 ראו חלק 2.6 **לעיל**.

4.5. גישה לנתוני תקשורת ולנתוני תוכן

ההסדרים בדינים במדינות השונות בדבר פרקטיקות של מעקב מקוון נוטים להבחין בין ההוראות הנוגעות להשגת נתוני תקשורת ולאיסופם, ובין אלה החלות על איסוף של נתוני תוכן, בהנחה מובלעת שנתוני תוכן רגישים יותר. למטריצה זו יש להוסיף את תכליות המעקב המקוון: אם אלו משקפות אינטרסים חיוניים של הגנה על הביטחון הלאומי, ייטו המחוקקים לכיוון של הסדר מתירני.[122] עם זאת יש לציין כי ההנחה בדבר הפגיעה הגדולה יותר בפרטיות הגלומה בגישה לתוכן לעומת נתוני תקשורת איננה מובנת מאליה: במציאות שבה בכיסם של אזרחים רבים מצוי מכשיר סלולרי, ניתוח מצרפי של נתוני התקשורת המופקים ממנו עשוי להניב מידע רגיש, שבשונה מנתוני התוכן, קשה למושא המידע לשלוט בו.[123]

תפיסה כזאת אנו רואים בדין האמריקאי. כך ההסדרים הנוגעים להשגת נתוני תוכן נוקשים יותר מאלה הנוגעים נתוני תקשורת; אלה הנוגעים לאיסוף שתכליתו אכיפת חוק או חקירת פשיעה נוקשים יותר מאלה הנוגעים לאיסוף לתכליות של ביטחון לאומי; ואלה הנוגעים לאיסוף שיעדיו המודיעיניים הם בעלי זיקה פרסונלית או טריטוריאלית לארצות הברית נוקשים יותר מאלה שנוגעים לאיסוף שיעדיו המודיעיניים זרים. איסוף מודיעיני למטרות הנוגעות

122 ראו לדוגמה את הדין האירופי. אמנם בכל הנוגע למעקב מקוון דיני האיחוד אינם מבחינים בין נתוני תקשורת לנתוני תוכן (כך למשל בעניין *DRI*, **לעיל** בפרק 3 ה"ש 228, נפסלה דירקטיבת שימור הנתונים), אך תחולתם מסויגת כשמדובר בתכלית של עיבוד הנתונים.

123 לדוגמה, ראו עומר טנא "הסתכל בקנקן וראה מה יש בו: נתוני תקשורת ומידע אישי במאה העשרים ואחת" 287 **רשת משפטית: משפט וטכנולוגית מידע** (ניבה אלקין־קורן ומיכאל בירנהק עורכים, 2011). גם סוכנויות האיסוף הבריטית והאמריקאית מייחסות ל־metadata ערך רב, לעיתים ברמה העולה על נתוני תוכן. ראו **לעיל** בפרק 3 ה"ש 158, 616.

לביטחון לאומי מוסדר בחוק איסוף מודיעין זר (FISA),[124] ובו יש הוראות נפרדות הנוגעות לאיסוף נתוני תוכן למטרות מודיעין זר כשיש זיקה טריטוריאלית או פרסונלית לארצות הברית,[125] ובהיעדר זיקה טריטוריאלית – החוק מבחין בין יעדים שהם בגדר אדם אמריקאי ובין אלה שאינם. איסוף נתוני תוכן לתכליות שנוגעות לאכיפת חוק מוסדר בחוק האזנות סתר (WTA), המסדיר יירוט של נתוני תוכן; הוראות חוק איסוף נתוני תקשורת (PRA) חלות על יירוט נתוני תקשורת, ואילו ההוראות של חוק תקשורת שמורה (SCA) חלות על קבלת נתוני תקשורת שמורים מהספקים.[126]

בכל הנוגע ליכולת אופרטיבית הראו חשיפותיו של סנודן כי בניגוד למצב הקיים בנוגע לנתוני תוכן, בכל הנוגע לאיסוף נתוני תקשורת יכלה הסוכנות לביטחון לאומי (NSA) לאסוף נתוני תקשורת בהיקפים חסרי תקדים. פוטנציאל זה נבלם בעקבות הרפורמות של חוק החירות (USA Freedom Act). עם זאת לא נראה כי תוכניות איסוף נתונים נוסח PRISM או ה־upstream collection (המכונות גם תוכניות 702) הוגבלו במידה רבה ברפורמה שעניינה העיקרי היה לעצב נהלים שמצמצמים את היקף האיסוף המודיעיני שיעדיו הם – אם כבדרך אגב ואם מלכתחילה – אזרחי ארצות הברית או אחרים המוגנים בתיקון הרביעי לחוקה.

גם באשר למעקב שתכליותיו אכיפת חוק וחקירת פשיעה ההוראות של חוק הסיוע לרשויות אכיפה (CALEA)[127] מבטיחות שלספקי טלקומוניקציה תהיה תשתית טכנית מסוימת שתאפשר לסייע (על בסיס צו או הוראה על פי דין) לרשויות אכיפת החוק ביירוט ובהשגת נתוני תוכן ותקשורת. עם זאת החוק טרם הדביק את השינויים בארכיטקטורה הטכנולוגית של תקשורת הנתונים בת זמננו, שעוברת למי שאינם "ספקי תקשורת", כהגדרתם בחוק.

הבחנות דומות אפשר למצוא בדין הבריטי. לפי חוק סמכויות החקירה (IPA), יירוט נתוני תוכן (וכן שימוש באמצעי סייבר למטרה זו) כפוף לבקרה של

124 ראו חלקים 3.1.7–3.1.5 **לעיל**.

125 ראו חלק 3.1.5 **לעיל**.

126 ראו חלק 3.1.5 **לעיל**.

127 ראו חלק 3.1.4 **לעיל**.

מנגנון הנעילה הכפולה ומותנה בצו מאת השר ובבחינה של נציב שיפוטי[128] – שני אישים נפרדים שעליהם החובה לשקול שיקולי פרטיות ומידתיות. הדין הבריטי אף מבחין בין צווי איסוף ממוקדים, שהסמכות לבקשם מסורה לראשי רשויות יירוט; ובין צווי איסוף כלליים, שאותם רשאים לבקש רק ראשי סוכנויות המודיעין, ולתכליות מוגדרות. הגישה לחומר שנאסף במסגרת צו כללי מותנית בצו עיון (examination) נפרד, המגביל את העיון בחומר לתכליות מסוימות וליעדים מוגדרים ומפורטים.[129] מנגד, לצד גישה אגבית לנתוני תקשורת שנאספים במסגרת צווי יירוט (secondary data), הדין הבריטי מאפשר לקשת רחבה של בעלי תפקידים להשיג נתוני תקשורת לתכליות שונות[130] ללא צורך בצו וללא הבקרה של נעילה כפולה.[131] הגדרת סוגי הנתונים שהם נתוני תקשורת רחבה למדי (נתוני ישות או אירועים שאינם נתוני תוכן),[132] ואשר לנתוני שימוש באינטרנט (ICR), הגדרתם אינה ברורה, ורמת הפירוט שלהם שנויה במחלוקת.[133]

הדין הגרמני, אף שהוא מבחין בין נתוני תקשורת לנתוני תוכן, נוטה להוראות נוקשות באשר להשגתם לתכליות של אכיפת חוק, הטעונה צו בית משפט (בשונה ממעקבים לתכליות של מודיעין זר, שם הגופים המפקחים הם מעין־שיפוטיים ומפעילים את הבקרה שלהם בדיעבד).[134]

128 ראו חלקים 3.3.4.8.3, 3.3.4.8.1, 3.3.4.4 **לעיל**.

129 ראו חלק 3.3.4.4 **לעיל**.

130 ראו **לעיל** בפרק 3 ה"ש 532.

131 ראו חלק 3.3.4.5 **לעיל**.

132 ראו **לעיל** בפרק 3 ה"ש 529–530.

133 עולה כי לפי ההגדרה שבחוק, ICR כולל נתוני היסטוריית גלישה. לא ברור אם היסטוריית הגלישה מפורטת ברמת ה־Domain בלבד (היינו, כתובת האתר, או ה־URL, בלעדי הלוכסן הראשון המפרט את העמוד הספציפי שאליו גלש המשתמש) או שהיא כוללת פירוט מלא של כל כתובות ה־URL שאליו ניגש המשתמש בתוך ה־Domain. לטענת ממשלת בריטניה, היסטוריית הגלישה ב־ICR מוגבלת לרמת ה־Domain. ראו Camilla Graham Wood, *The Database of You: Internet Connection Records Will Allow the UK Government to Document Everything We Do Online*, Privacy International (11.10.2016)

134 ראו חלק 3.4.3.3–3.4.3.4 **לעיל**.

בהודו, בשל המסגרת הרופפת ממילא של הדינים המגינים על הפרטיות, ההבחנה בין סוגי הנתונים כמעט שאינה משחקת תפקיד. נראה כי הכללים השונים החלים בהודו על יירוט ועל השגת נתוני תקשורת – המבססים פרוצדורות לממשק אנושי בין הרשות המבקשת את המידע ובין אחראי ארגוני (nodal officer) אצל ספק השירות – מבחינים בין סוגים שונים של נתונים.[135] ואולם הארכיטקטורה של מערכת הניטור המרכזית מסתמנת כעוקפת ממשק זה כדי לאפשר גישה ישירה לנתונים של ספקי השירות.[136] לטענת ממשלת הודו, מערכת הניטור המרכזית (CMS) אינה מאפשרת לגופי אכיפת החוק גישה ישירה לנתונים שברשותה, אלא משמשת מתווך חלף ה־nodal officer.

ההסדרים שבחוק הישראלי מבחינים בין נתוני תקשורת לבין נתוני תוכן. ההסדר להשגתם של נתוני תוכן מצוי בחוק האזנת סתר, הכולל הוראות נפרדות להשגת תוכן על בסיס צורכי המשטרה ועל בסיס צורכי ביטחון. אותה הפרדה נעשית גם בכל הנוגע לנתוני תקשורת: חוק השב"כ מסדיר את גישתו לנתונים של שירות הביטחון הכללי; וחוק נתוני תקשורת – את גישת המשטרה וגופי החקירה האחרים.

לפי ההוראות של חוק נתוני תקשורת למשטרת ישראל אין סמכות כללית ליירט נתוני תקשורת או לקבל נתוני תקשורת באופן מקוון, אלא בכפוף להיתר מבית המשפט, ובמקרים דחופים באישורו של קצין מוסמך. משטרת ישראל מכירה בכך שאי־אפשר לקבוע קביעה גורפת כי כל מקרה שבו מנוי בזק מתקשר למוקדי החירום הוא מקרה "דחוף", שמאפשר לקבל עליו נתוני תקשורת מקוונים. עם זה לאחרונה הופץ תזכיר חוק שמציע לאפשר למשטרת ישראל לקבל נתוני איכון, נוסף על נתוני הזיהוי, של המנויים המתקשרים למוקדי החירום.[137] מנגד נראה כי

135 כללים (13)–(9)419A לכללי הטלגרף ההודיים, **לעיל** בפרק 3 ה"ש 962; ס' 21–13 לכללי יירוט, ניטור ופענוח המידע; ס' 4 לכללי ניטור ואיסוף נתוני תעבורה.

136 ראו חלק 3.5.3 **לעיל**.

137 ראו תזכיר חוק למניעת הטרדות של מוקדי חירום (תיקון־איכון אוטומטי של שיחות למוקדי חירום), התשע"ז–2016, פרסם משרד המשפטים ביום 29.11.2016 [עותק מצוי בידי המחבר].

שירות הביטחון הכללי מסוגל ליירט נתוני תקשורת בזמן אמת ובאופן גורף, וכי יש תשתית נורמטיבית העשויה להסמיך אותו לכך.[138]

ככלל, לפי הוראות הדין הישראלי האזנת סתר יכולה להתבצע במקוון באמצעות יירוט ישיר של נתונים או באמצעות הוראה למפעיל הבזק לספק את הנתונים הנדרשים לחקירה. חוק האזנות סתר אינו מפרט את טכניקת הביצוע של האזנת הסתר, ואין בו הוראות מיוחדות בנוגע לבעלי רישיון בזק. ייתכן שהוראות אלו מוסדרות מכוח סעיף 13(ב)(2) לחוק הבזק – המסמיך את ראש הממשלה להורות לבעל רישיון בזק בעניינים הנוגעים, בין השאר, ל"התקנת מיתקן, ביצוע פעולת בזק, או ביצוע התאמה טכנולוגית למיתקן בזק, בידי בעל הרישיון או בידי נציג כוחות הביטחון בסיוע בעל הרישיון, לרבות מתן גישה למיתקן, ככל שהדבר דרוש לצורך ביצוע תפקידיהם של כוחות הביטחון או להפעלת סמכויותיהם לפי כל דין;". הוראות שנתן ראש הממשלה לפי סעיף זה הן חסויות (ס"ק 13(ד) לחוק הבזק).

נראה כי האזנת סתר ממקורות גלויים ברשת האינטרנט, לפי סעיפים (א)–(ג) לחוק האזנות סתר, יכולה להתבצע על דרך של יירוט (מעקב ישיר אחרי הפעילות באתרי האינטרנט הרלוונטיים) ועל דרך של השגת נתונים מספקי האינטרנט.

4.6. כריית מידע

כריית מידע (כר"מ) היא שימוש במאגרי מידע גדולים ובהצלבתם למטרת הפקה של ידע או תובנות סטטיסטיות. מבחינה מודיעינית כריית מידע יכולה לשמש לצורכי חיזוי, אך גם לחקירה של נתוני עבר, יחסי גומלין בין ישויות שונות ופרופיילינג. הסיכון לפרטיות הטמון בכריית מידע הוא רב, שכן בהסתמך על צבר נתונים אקראיים שלכאורה אינם קשורים זה בזה, אפשר לעיתים להפיק

138 ראו חלק 2.6 **לעיל**.

מידע אישי רגיש.[139] יתר על כן, למושא המידע יש יכולת מוגבלת להבין את הפוטנציאל הגלום בצבירה עקיבה של רסיסי מידע זניחים עליו.

הדיון באסדרה המשפטית של המותר והאסור בפעילות כר"מ נדרש כחלק מהאסדרה של הפעלת סמכויות מעקב מקוון אף שניתוח סטטיסטי למטרות אלה יכול להיעשות גם על נתונים ממאגרי מידע שמקורם אינו בנתוני תקשורת. הגידול המעריכי בנפח התעבורה של נתוני התקשורת העולמית הופך את ניתוחם באמצעים ממוכנים לפרקטיקה אפקטיבית במיוחד, וסוכנויות ביון ברחבי העולם משתמשות בו תדיר. ואולם על האיכות של כריית המידע יכולים להשפיע רבות גם הסדרים הנוגעים לשימור מידע: ככל שהמידע ההיסטורי המצוי אצל הגוף החוקר – הנובע מהסדרים שמתירים שימור מידע לטווח ארוך או אף מורים עליו – רב יותר, כך ישתפרו גם הדיוק הסטטיסטי והאיכות של תוצרי הכר"מ, ועימם תגדל גם פגיעתם הפוטנציאלית בזכות לפרטיות.

139 להגדרת כר"מ, ראו גם **לעיל** בפרק 1 ה"ש 6. בהתייחס לסיכונים פרטיות הגלומים בכר"מ, לדוגמה, בשנת 2009 פיתחו חוקרים ב־MIT מודל סטטיסטי המנבא נטייה מינית של משתמש פייסבוק לפי ניתוח רשת החברים שלו. Carter Jernigan, Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, 14(10) First Monday (2009). אף שבתקופה שחלפה מביצוע המחקר השתנו דפוסי השימוש ברשת החברתית והשתנתה גם רמת השליטה של המשתמשים במידת החשיפה של הפרופיל שלהם (חסימת היכולת לעיין ברשימת החברים של פרופיל מסוים מקשה עד מאיינת את היכולת להשתמש בטכניקה שפותחה במסגרת המחקר), לא בלתי סביר להניח שבדרכים דומות ניתן להשתמש במידע גלוי אחר כדי ללמוד על משתמש מסוים. ראו גם Lemi Baruh & Mihaela Popescu, *Big Data Analytics and the Limits of Privacy Self-Management*, 19 New Media & Soc. 1-18 (2017). המודלים שפיתחו קוסינסקי וסטילוול בהסתמך על אפליקציית myPersonality אפשרו להם לחזות נטייה מינית והשקפה פוליטית של משתמשי פייסבוק בהסתמך על חיבובים (likes), והם שימשו בסיס רעיוני לחברת קיימברידג' אנליטיקה בפיתוח מודלים דומים ששימשו בקמפיין הבחירות של דונאלד טראמפ. ראו Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior,* 110 Proc. of the National Academy of Sciences, 5802-5805 (2013); Keith Collins and Gabriel J.X. Dance, *How Researchers Learned to Use Facebook 'Likes' to Sway Your Thinking*, The New York Times (20.3.2018)

הבעיה בשימוש בכר"מ נובעת ממה שטרייב כינה "trial by mathematics".[140] השימוש בשיטות ניתוח אלה מעביר את שיקול הדעת האנושי למודלים אוטומטיים שכוח ההסבר האינטואיטיבי שלהם דל, והם קשים לניתוח שלאחר מעשה ונדמים כקופסה שחורה.[141] השימוש בכר"מ כמעין קופסה שחורה שאין להרהר אחריה יכול גם לספק דרכים לשירותי הביטחון להלבין מידע שהושג בדרכים לא כשרות ולהציגו כתוצר של ה"מכונה".[142] גם בלי שימוש לרעה בכר"מ להלבנת ידיעות, היכולת לזהות טעויות סטטיסטיות במודלים המופעלים במסגרתו מוגבלת, אבל השלכותיהן של טעויות כאלה על מושאי העיבוד עלולות להיות הרות גורל.

דיני האיחוד האירופי כוללים הוראות באשר לכר"מ. דירקטיבת הגנת המידע אסרה על קבלת החלטות המבוססות על עיבוד אוטומטי בלבד, ללא שיקול דעת אנושי,[143] ולמעשה על כר"מ ללא בקרה אנושית. אך הוראותיה אינן חלות על פעולות עיבוד מידע לצורכי ביטחון ושיטור. עם כניסתה לתוקף של דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), הוחל האיסור על פעולות עיבוד מידע שמובילות להחלטות אוטומטיות ללא התערבות ושיקול דעת אנושיים,

140 Laurence H. Tribe, *Trial by Mathematics: Precision and Ritual in the Legal Process*, 84 Harv. L. Rev (1971). ראו גם ביקורות על פרקטיקות מקומיות של חיזוי מבוסס־כר"מ אצל ג'ון בראון "'ידו"ח מיוחד': על סמך מה עוצרת ישראל מאות פלסטינים על פשעים שלא ביצעו?" **הארץ** 19.04.2017 וכן אצל הירשאוגה ושיזף, **להלן** בפרק זה ה"ש 158.

141 Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); כן ראו Kiel Brennan-Marquez, *"Plausible Cause": Explanatory Standards in the Age of Powerful Machines*, 70 Vand. L. Rev. 1249 (2017); Andrew D. Selbst, *A Mild Defense of Our New Machine Overlords*, 70 Vand. L. Rev. En banc 87 (2017)

142 בהקשרים אחרים זיהה המחוקק את השימוש האפשרי במודלים סטטיסטיים לטשטוש אפליות אסורות. כך למשל ס' 51 לחוק נתוני אשראי אוסר את השימוש בנתוני גיל, גזע, מין, דת, מוצא, לאום, מקום מגורים ומצב משפחתי לצורך בניית מודל סטטיסטי. מנגד, בהסדר זה לא התייחס המחוקק לשימוש אינדיקטורים אחרים שמהם ניתן ללמוד בעקיפין על מאפיינים אלה.

143 ס' 15 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

לרבות פרופיילינג וכר"מ – הן על גופי ביטחון והן על גופי אכיפת החוק. עם זאת דירקטיבה 2016/680 מתירה שימוש בכר"מ אוטומטי בכפוף להתקיימותם בדין של אמצעים נאותים לשמירה על זכויות הפרט של מושא המידע ושל חירויותיו, ולכל הפחות יהיו יכולת להתערבות אנושית של מנהל מאגר. ביסוס החלטות כאמור על קטגוריות רגישות של מידע יותרו רק בכפוף להתקיימותם של אמצעים נאותים לשמירה על זכויות הפרט של מושא המידע ועל חירויותיו.[144]

דירקטיבה 2016/680 גם אוסרת לעבד נתונים השייכים לקטגוריות רגישות.[145] חריגה מאיסור זה אפשרית בין השאר כשאת המידע המעובד פרסם מושאו בגלוי, ובכפוף לאמצעים נאותים לשמירה על זכויות הפרט של מושא המידע ועל חירויותיו. סעיף זה יכול לשמש מקור המתיר איסוף נתוני תקשורת גלויים ברשתות חברתיות, לרבות עיבודם המאוחר במסגרת כר"מ.

בחוק הבריטי בדבר הגנת מידע 1998 (DPA) – שיישם את הוראותיה של דירקטיבת הגנת המידע האירופית – כולל איסורים ברוח זהה,[146] וכך גם הצעת החוק הבריטי בדבר הגנת מידע (DPB).[147] אלא שדירקטיבת הגנת המידע וכן החוק הבריטי בדבר הגנת מידע 1998 (DPA) מחריגים מתחולתם עיבוד מידע לצורכי ביטחון לאומי: כשמדובר בעיבוד נתונים שנעשה לתכליות של ביטחון לאומי, החוק הבריטי בדבר הגנת מידע 1998 (DPA) פוטר את המעבדים מההוראות החלות על עיבוד מידע אוטומטי.[148]

יש לציין כי הצעת חוק הגנת מידע (DPB) מתיישרת לפי הוראותיה של דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) בנוגע לעיבוד נתונים אוטומטי שמבצעים כוחות הביטחון, ואולם הוראות דומות בנוגע לעיבוד נתונים אוטומטי

144 ס' 15(2)–(3) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

145 ס' 10 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

146 ס' 7–9a לחוק הבריטי בדבר הגנת מידע 1998 (DPA), השוו לס' 15 לדירקטיבת הגנת המידע.

147 בשל התחולה הישירה של התקנות הכלליות בדבר הגנת מידע (GDPR), התייחסות בסעיף 13 להצעת החוק הבריטי בדבר הגנת מידע (DPB) לעיבוד אוטומטי היא לצורכי הבהרה ויישום מקומי.

148 ס' 28 לחוק הבריטי בדבר הגנת מידע 1998 (DPA).

שמבצעים שירותי המודיעין,[149] חלות רק בהיעדר פטור מטעמים של ביטחון לאומי.[150] אפשר שצווי מידע אישי[151] יכולים לשמש תשתית המאפשרת לשירותי המודיעין הבריטיים להחזיק, על בסיס הדין הקיים, מאגרי מידע שמקורם אינו בפעולות שנעשו מכוח צו שניתן לפי חוק סמכויות חקירה 2016 (IPA), ולהצליבם באופן ממוכן עם נתוני תוכן ועם metadata שהושגו לפי צווי ה־IPA.

גם בדין הגרמני ניתן למצוא הוראות בדבר עיבוד אוטומטי המצויות בהלימה עם ההסדרים שבדירקטיבת הגנת המידע או בתקנות הכלליות בדבר הגנת מידע (GDPR). החוק הפדרלי להגנת מידע (BDSG) מקנה למושאי המידע זכות להגנה מהחלטות שהתקבלו על בסיס עיבוד אוטומטי של מידע,[152] בכפוף לחריגים. שאלת חוקתיותם של הקמת מאגרי מידע למטרות כר"מ נידונה בפסיקה הגרמנית, שמצאה לנכון לסייג אותם במקרים מסוימים.[153]

בהקשר זה, לצד הוראות חקיקה קונקרטיות החלות על פעולות כר"מ, יש מקום להתייחס להסדרים שמכוחם גופי חקירה וביטחון יכולים לקבל גישה למאגרי מידע ציבוריים־ממשלתיים לצורך הצלבה, טיוב ואגירת נתונים שעיבודם יחדיו עשוי לעלות כדי פגיעה מהותית בפרטיות. כך למשל, הדין הגרמני מסמיך את המשטרה הפדרלית של גרמניה (BKA) לבצע פעולות כר"מ.[154] חוק המשטרה הפדרלית (BKAG) מתיר לה לבקש מבית המשפט צו לקבלת מידע מגופים ציבוריים או שאינם ציבוריים למטרות השוואה אוטומטית למאגרי מידע אחרים, לתכליות ביטחוניות. סמכות זו אינה מסורה לסוכנויות המודיעין הגרמניות.[155]

149 ס' 94–96 להצעת החוק הבריטי בדבר הגנת מידע (DPB).

150 ס' 108 להצעת החוק הבריטי בדבר הגנת מידע (DPB).

151 ראו בחלק 3.3.4.8.4 **לעיל**.

152 ס' 6a,8 לחוק הפדרלי להגנת מידע (BDSG). השוו עם ס' 21–22 לדירקטיבת הגנת המידע.

153 ראו לדוגמה את עניין **סינון המידע**, ועניין **מאגר ה־ATD**.

154 ראו בחלק 3.4.1 **לעיל**, המתאר את עניין **סינון המידע**.

155 בישראל ההגבלות החלות על גופים ציבוריים בנוגע למסירת מידע ושיתופו ביניהם אינן חלות על רשות ביטחון אלא אם היא נאסרה בחיקוק (חוק הגנת הפרטיות, ס"ק 23ב(ב)). ראו **לעיל** בחלק 2.3.

במקרים שבהם מקור המידע הוא בעל מאגר נתונים פרטי (כגון ספק שירותים של רשת חברתית), יש לבחון גם את ההסדרים הקונקרטיים בין בעל המאגר למושאי המידע (כדי לשמור על עקרון צמידות המטרה שבסעיף2(9) לחוק הגנת הפרטיות. הסדרים אלו מעוגנים לפי רוב ברישיונות שימוש (EULA — End User License Agreement) או בתנאי שימוש (TOS — Terms of Service).[156]

המחוקק הישראלי מגלה לאחרונה מודעות לפוטנציאל הפגיעה בפרטיות של כר"מ, כפי שניתן ללמוד מהכללת נתונים "אודות הרגלי הצריכה של אדם שיש בהם כדי ללמד על מידע [שבשל אופיו נדרשת רמת אבטחה בינונית] או על אישיותו של אדם, אמונתו או דעותיו" בסוגי הנתונים שאגירתם מחייבת רמת אבטחה בינונית ומעלה.[157]

בחוק הישראלי אין הוראות הנוגעות ישירות לרגולציה של פעילות הכר"מ של גופי הביטחון והחקירה. עם זאת במטריצת הדינים הישראלית שתוארה לעיל יש הוראות שעשויות להשפיע על טיבו ואיכותו של כר"מ, לרבות זו המתבצעת כבר עתה.[158]

דן חי מעיר כי הוראותיו של חוק נתוני האזנת סתר בקשר לביעור מידע שאינו נדרש עוד לצורך גילוי עבירות ועבריינים ולמניעת עבירות, נועדו לאזן בין הרצון

156 ראו **לעיל** בפרק 2 ה"ש 30.

157 ראו תקנות אבטחת מידע, תוספת ראשונה, ס' 1(ט).

158 בהתייחסו ל"אינתיפאדת הבודדים" רמז ראש הממשלה נתניהו כי לסיכול פיגועים נעשה שימוש בנתוני עתק (big data). ראו עמוס הראל "ישראל עצרה מאות פלסטינים כחשודים בכוונה לבצע פיגועים בגלל פרסומים ברשת" **הארץ** 16.04.2017. גם סא"ל ר', **לעיל** בפרק 2 ה"ש 99, בעמ' 133, מעיר כי פיתוחן וניצולן של יכולות ניבוי אנליטיות מבוססות־נתוני־מדיה־חברתית יכולים לסייע בהתמודדות עם מפגעים בודדים. דברים דומים אמר גם ראש השב"כ נדב ארגמן כשציין כי יכולות הסיכול של פיגועי מפגעים בודדים השתפרו הודות לשיפורים טכנולוגיים פורצי דרך, ראו גילי כהן "ראש השב"כ: איתרנו יותר מ־2,000 מפגעים בודדים פוטנציאליים מתחילת 2016" **הארץ** 27.06.2017; אור הירשאוגה והגר שיזף "סיכול ממוקד: השיטה החדשה להתמודדות עם הטרור נחשפת" **הארץ** 26.05.2017; עוד ראו לדוגמה הצעות למשרות בשירותי הביטחון: "עובד כריית מידע (כר"מ)/ Data Mining" באתר שירות הביטחון הכללי (האתר נדגם ביום 18.01.2017. תדפיס מצוי בידי המחבר); וכן הצעת משרה "כריית מידע ומיצוייו" באתר המוסד למודיעין ולתפקידים מיוחדים (האתר נדגם ביום 18.01.2017. תדפיס מצוי בידי המחבר).

למנוע צבירת נתונים במאגרי מידע של המשטרה ובין הרצון לשמור על חומר חקירה.[159] עם זאת הנוסח של סעיף 9ב(ג) לחוק – שלפיו הוראת קצין משטרה לביעור חומר האזנת סתר תבוסס על קביעה שלפיה החומר "אינו דרוש למניעת עבירות או לגילוי עבריינים" – משאיר מרחב שיקול דעת לקצין המוסמך. יש להניח כי ככל שילך השימוש בטכניקות חקירה המבוססות על כריית נתונים ויתרחב, כן יכביד הטיעון שלפיו שימור מידע יסייע ליעילותן של טכניקות אלו על נטל ההוכחה כי חומר זה או אחר אכן אינו נדרש עוד למטרות המנויות בחוק.

.4.7 שיתוף פעולה מודיעיני עם סוכנויות זרות

משלהי מלחמת העולם הראשונה מקיימות סוכנויות המודיעין של ארצות הברית, בריטניה, קנדה, ניו זילנד ואוסטרליה שיתוף פעולה בתחום מודיעין התקשורת,[160] המכונה "חמש העיניים" (Five eyes).[161] לפי דיווחים בתקשורת, במסגרת שיתוף פעולה זה יירטו הסוכנות האמריקאית לביטחון לאומי (NSA) ומטה התקשורת הממשלתי של בריטניה (GCHQ) את התשדורות של משתמשי תקשורת מצלמות הרשת של חברת יאהו.[162] מסמכי סנודן חשפו מבצע אחר של מטה התקשורת (GCHQ), שבמסגרתו יירטו הבריטים תקשורת בהיקף נרחב

159 ראו חי, **לעיל** בפרק 2 ה"ש 45, בעמ' 801.

160 British-U.S. Communication Intelligence Agreement, HW 80/4 (5.03.1945)

161 Patrick F. Walsh & Seumas Miller, *Rethinking "Five Eyes" Security Intelligence Collection Policies and Practice Post Snowden*, 31 Intelligence and National Security 345 (2016)

162 Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, The Guardian, (28.02.2014)

באינטרנט באמצעות שאיבת מידע מתעבורת רשת שעוברת בכבלים אופטיים. את המודיעין הזה שיתפו עם הסוכנות לביטחון לאומי (NSA).[163]

המדיניות הבריטית בעניין שיתוף פעולה זה אינה גלויה לציבור, ובעיקר לא ברור מהם הכללים שלפיהם סוכנויות המודיעין חולקות מידע (בייחוד מידע על אזרחים בריטים) עם ארצות הברית או עם מדינות אחרות החברות בפורום "חמש העיניים". כמו כן טרם נבחנה מידת ההלימה של פרקטיקות שיתוף הפעולה המודיעיניות עם הוראות החוק הבריטי בדבר הגנת מידע 1998 (DPA) או עם הצעת החוק הבריטי בדבר הגנת מידע (DPB), על ההחרגות הנרחבות בהן בכל הנוגע לעניינים של ביטחון לאומי.

חוק סמכויות חקירה 2016 (IPA) אינו כולל הוראות בדבר בקרות או פיקוח על שיתוף מידע מודיעיני שהושג מכוחו.[164] עם זאת הוא מכיל הוראות בנוגע להשגת מודיעין מסוכנויות זרות.[165] בקשות בריטיות לסוכנויות זרות כדי שהללו יירטו תקשורת שצד לה מצוי בתחומי האיים הבריטיים, ייעשו מכוח צו יירוט או צו עיון ממוקדים.[166] גם בקשות לסיוע הדדי מגופים זרים (mutual assistance) בעניין תקשורת כזו מותנות בצו מתאים.[167]

נוסף על שיתוף הפעולה האנגלו־אמריקאי, חשפו מסמכי סנודן גם את קשרי המודיעין בין הסוכנות האמריקאית לביטחון לאומי (NSA) לסוכנות הביון

163 Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, The Guardian (21.06.2013)

164 ראו Edin Omanovic, *Briefing: UK-US Intelligence Sharing Arrangements*, Privacy International 2 (6.07.2017)

165 עם זאת בעניין *Liberty 2*, **לעיל** בפרק 3 ה"ש 752, קבע טריבונל סמכויות החקירה כי עד לדצמבר 2014 הייתה מידת חשאיותו של המשטר המשפטי שחל על מידע שקיבלה GCHQ מהסוכנות לביטחון לאומי (NSA) כה ניכרת, עד שהדבר פגע באינטרס הצפיות המהותית של הציבור, כמתחייב מסעיף 8 לאמנת זכויות האדם האירופית.

166 ס' 9 לחוק סמכויות חקירה 2016 (IPA).

167 ס' 10 לחוק סמכויות חקירה 2016 (IPA), וכן ס' 15(4) וההוראות החלות על צווים כאמור בסעיפים 15–43.

הפדרלית הגרמנית (BND).[168] גרמניה חברה בפורום "14 העיניים" – פורום שיתוף פעולה מודיעיני רחב מזה של "חמש העיניים", כנרמז משמו.[169] במסגרת שיתוף הפעולה בין שתי הסוכנויות העבירה סוכנות הביון הפדרלית הגרמנית (BND) ל־NSA נתוני תקשורת בהיקף עצום, ובדיון הציבורי לאחר החשיפה טענו נציגי הממשל הגרמני כי שיתוף הפעולה נעשה כחוק.[170]

חוק סעיף 10 הגרמני מתיר לסוכנות הביון הפדרלית (BND) להעביר מידע פרטי שנאסף מכוחו לגופי מודיעין זרים בתנאי שההעברה הכרחית להגנה על אינטרסים ביטחוניים או על אינטרסים של מדיניות החוץ הפדרלית, או על אינטרסים ביטחוניים מהותיים של מדינה זרה, בכפוף לכיבוד עקרון ההדדיות בין הצדדים ובתנאי שהדבר אינו פוגע באינטרסים המהותיים של מושא המידע. בעיקר על המדינה הזרה להבטיח הגנה נאותה על המידע, והכול בהנחה שהשימוש שיעשה המקבל במידע יהיה על פי עקרונות היסוד של שלטון החוק.[171] העברת המידע כפופה לאישור משרד הקנצלר. הוראות דומות מצויות בחוק סוכנות הביון הפדרלית הגרמנית (BNDG) בדבר שיתוף של גופי מודיעין זרים ברשימות שעורכת הסוכנות יחד עם גופי מודיעין אחרים בגרמניה (Gemeinsame Dateien).[172]

חוק סוכנות הביון הפדרלית (BNDG) מתיר לסוכנות הביון הגרמנית לאסוף מידע ולחלוק אותו עם גופי מודיעין זרים בהקשר של נתוני תקשורת זרה,[173]

168 Hubert Gude, Laura Poitras & Marcel Rosenbach, *Transfers from Germany Aid US Surveillance*, Der Spiegel (5.8.2013)

169 Leo Kelion, *NSA-GCHQ Snowden Leaks: A Glossary of the Key Terms*, BBC (28.1.2014); Giuseppe Zappalà, *Killing by Metadata: Europe and the Surveillance-Targeted Killing Nexus,* 1 Global Affairs 251–258 (2015)

170 **שם**. לניתוח השיח הציבורי בפרשה, ראו Schulze ו־Heumann, **לעיל** בפרק 1 ה"ש 4.

171 ס' 7a לחוק סעיף 10 (G10).

172 ס' 26,27,30 לחוק סוכנות הביון הפדרלית (BNDG).

173 ס' 13 לחוק סוכנות הביון הפדרלית (BNDG). לנתוני תקשורת זרה, ראו בחלק 3.4.3.4 **לעיל**.

בתנאי שהדבר משרת את התכליות הסטטוטוריות לאיסוף מידע;[174] שהיעדר שיתוף פעולה עם גוף המודיעין הזר יקשה על שירות הביון הפדרלי במילוי תפקידו; ובתנאי שסוכנות הביון הפדרלית וגוף המודיעין הזר ניסחו מזכר הבנות בכתב.[175] נדרש ששיתוף פעולה מודיעיני כאמור ייועד להשגת מידע (1) על איומי טרור בין־לאומי; (2) המסייע לצבא הרפובליקה הפדרלית (ה־Bundeswehr); (3) על התפתחויות משבריות מעבר לים; (4) הנועד לזיהוי איומים שמקורם בהפצה של נשק להשמדה המונית ולהתמודדות עימם; (5) על איומים ומצבם הביטחוני של בני הלאום הגרמני או של בני הלאום שעימו נערך שיתוף הפעולה, המצויים מעבר לים; (6) על פעילויות פוליטיות, כלכליות או צבאיות בעלות חשיבות; (7) במקרים בני השוואה.[176]

סוכנות הביון הפדרלית הגרמנית (BND) תורשה לאסוף מידע אישי בשיתוף פעולה מודיעיני כאמור אם הוא נועד להגשים את תכליות שיתוף הפעולה, ואם הוא משתמש רק במילות החיפוש המתאימות להגשמת תכליות אלו, ובהלימה עם האינטרסים הביטחוניים ועם מדיניות החוץ של הרפובליקה הגרמנית.[177]

חשיפת פעולותיה של הסוכנות האמריקאית לביטחון לאומי (NSA), ובעיקר קשרי העבודה שלה עם מקבילותיה באחדות ממדינות אירופה, עוררה דיון ציבורי על פרטיות ברשת, על שיתופי פעולה מודיעיניים ועל אסדרה של מעקב מקוון. לצד הדיון הציבורי אחדות מהחשיפות נדונו גם בערכאות שונות

174 המנויות בסעיף 6(1) לחוק סוכנות הביון הפדרלית (BNDG), ראו **לעיל** בפרק 3 ה"ש 909.

175 ס' 13(3) לחוק סוכנות הביון הפדרלית (BNDG) מפרט את רכיבי המזכר: (1) מטרות שיתוף הפעולה המודיעיני; (2) תוכן שיתוף הפעולה; (3) משך שיתוף הפעולה; (4) הסכמת הצדדים שהשימוש שייעשה במידע יוגבל למטרות שלשמן נאסף, ובהלימה עם עקרונות יסוד של שלטון החוק; (5) הסכמת הסוכנות הזרה לספק, לבקשת שירות הביון הפדרלי, נתונים על השימוש שנעשה במידע, וכן הבטחה מהסוכנות הזרה לציית להודעת חדילה מאת שירות הביון הפדרלי.

176 ס' 13(4) לחוק סוכנות הביון הפדרלית (BNDG).

177 ס' 14(1) לחוק סוכנות הביון הפדרלית (BNDG).

במדינות־החברות,[178] ונבחנו מחדש הסדרי העברת המידע במגזר הפרטי בין מדינות האיחוד האירופי לארצות הברית.[179]

נוסף על חברותה של בריטניה ב"חמש העיניים" יש עוד מדינות אירופיות החברות במסגרות של שיתוף מידע מודיעיני פנים־אירופי[180] וחוץ־אירופי.[181] ככל הנראה, העברת מידע במסגרת שיתוף פעולה מודיעיני וההוראות החלות על שימוש במידע שנתקבל במסגרת יחסים כאמור, מוחרגות מתחולת דיני הגנת המידע האירופיים הכלליים, המחריגים מתחולתם עיבוד מידע לתכליות הנוגעות לביטחון הציבור (בנוסח הרחב של דירקטיבת הגנת המידע, או בנוסח הצר יותר של התקנות הכלליות בדבר הגנת מידע (GDPR)).[182] עם זאת דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680), הרלוונטית לפעולות עיבוד לתכליות אלו (במובנן הצר),[183] כוללת הוראות להעברת מידע שכזה.[184] על העברת המידע להיות הכרחית לתכליות אלו; על הגוף המקבל להיות רשות מוסמכת לתכליות אלו[185] בכפוף להחלטת נאותות (adequacy decision) של המועצה האירופית[186]

178 ראו לדוגמה את הדיונים בטריבונל סמכויות החקירה הבריטי על שיתוף הפעולה עם ה־NSA – עניין *Liberty 1*, **לעיל** בפרק 3 ה"ש 751, ועניין *Liberty 2*, **לעיל** בפרק 3 ה"ש 752.

179 עניין *Schrems*, **לעיל** בפרק 3 ה"ש 175.

180 דוגמת המשטרה האירופית (Europol).

181 דוגמת פורום "תשע העיניים" (Nine Eyes), הכולל, נוסף על המדינות החברות ב"חמש העיניים", את דנמרק, צרפת, הולנד ונורווגיה, או את פורום "14 העיניים", הכולל גם את גרמניה, בלגיה, איטליה, ספרד ושוודיה. להרחבה, ראו Zappalà, **לעיל** בפרק זה ה"ש 169.

182 סעיף 3(2) לדירקטיבת הגנת המידע, סעיף 2(2)(d) לתקנות הכלליות בדבר הגנת המידע (GDPR). ראו בחלק 3.2.3.5 **לעיל**.

183 סעיף (2) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680). ראו בחלק 3.2.3.5 **לעיל**.

184 פרק 5 של דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

185 ס' 35(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

186 ס' 36 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

או בכפוף לבקרות מתאימות.[187] בהיעדר החלטת נאותות או בקרות מתאימות, יאפשרו מדינות־חברות העברת מידע לצד שלישי רק בתנאי שזו נועדה להגן על האינטרסים החיוניים של מושא המידע או של אדם אחר; להגנת אינטרסים לגיטימיים של מושא המידע כשהדין של המדינה המעבירה את המידע מתיר זאת; למניעת איום מיידי וחמור לביטחון הציבור במדינה חברת האיחוד או במדינה אחרת; במקרים פרטניים לשם הגשמת תכליות הדירקטיבה; ובמקרים פרטניים למטרות של ביסוס, הגנה או מימוש של טענות משפטיות בקשר לתכליות אלו.[188]

לפי דיווחים בעיתונות, שחלקם מתבססים על החשיפות של סנודן, לישראל שיתוף פעולה סיגינטי עם ארצות הברית.[189] כך למשל נחשף מזכר הבנות בין הסוכנות לביטחון לאומי (NSA) ובין יחידת הסיגינט הלאומית של ישראל, הנוגע להגנה על מי שהוא "אדם אמריקאי".[190] מבחינת הדין הישראלי פעילות זו חוסה ככל הנראה בפטור בסעיף 19 לחוק הגנת הפרטיות, החל על רשויות ביטחון בכללן אגף המודיעין במטכ"ל.[191] קונסטרוקציה משפטית חלופית שבה ניתן להסתייע להעברת מידע פרטי במסגרת שיתוף פעולה מודיעיני מצויה בתקנות הגנת הפרטיות (העברת מידע).[192] תקנות אלה מתירות העברת מידע מישראל

187 ס' 37 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

188 ס' 38(1) לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680).

189 רונן ברגמן "סוד ושבר" **ידיעות אחרונות** 18.05.2017; יוסי מלמן "קירבה יוצאת דופן: על שיתוף הפעולה המודיעיני בין ישראל לארה"ב" **מעריב** 11.9.2013; Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel"* THE GUARDIAN (11.9.2013); אמיר אורן "מסמך סודי של NSA חושף שיתוף פעולה אמריקאי־ישראלי למעקב מודיעיני במצרים" **הארץ** 4.8.2014.

190 Memorandum of Understanding between The National Security Agency/Central Security Service (NSA/CSS) and the Israeli Sigint National Unit (ISNU) Pertaining to the Protection of U.S. Persons

191 **לעיל** בפרק 2 ה"ש 48.

192 תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א–2001, ק"ת 6113 תשס"א (2.7.2001), בעמ' 900 (להלן: תקנות הגנת הפרטיות (העברת מידע)).

אל מחוץ לגבולותיה אם העברת המידע בין השאר הכרחית להגנה על שלום הציבור או ביטחונו;[193] אם לא ניתן לקבל את הסכמתו של מושא המידע, וההעברה הכרחית לשם הגנה על בריאותו או על שלמות גופו;[194] כשהמידע מועבר למאגר מידע במדינה שהיא צד לאמנה האירופית להגנת הפרט בקשר לעיבוד אוטומטי של מידע רגיש, או שהיא מקבלת מידע ממדינות־חברות בקהילה האירופית לפי אותם תנאי קבלה, או שרשם מאגרי המידע הודיע ברשומות שקיימת בה רשות להגנת הפרטיות לאחר שהגיע עם אותה רשות להסדר על שיתוף פעולה.[195]

193 תקנה 2(6) לתקנות הגנת הפרטיות (העברת מידע).

194 תקנה 2(2) לתקנות הגנת הפרטיות (העברת מידע).

195 תקנה 2(8) לתקנות הגנת הפרטיות (העברת מידע).

פרק 5

מדיניות

מסקירת הדין המשווה בפרקים הקודמים, עולה כי דיני המעקב המקוון בישראל סובלים מתת־אסדרה ומאסדרת־חסר בהיבטים מסוימים. בפרק זה נבחן מהן הסוגיות שאינן מוסדרות בדין הישראלי, אילו היבטים בהסדרה מוסדרים בכללים חשאיים, וכן נבחן לעומק כל סוגיה וסוגיה. לכל סוגיה נציע מתווה כללי להסדרה ולאחר מכן נתייחס להסדרים שיש לרענן כדי להבטיח בהם הגנות ראויות על אינטרסים של פרטיות. לבסוף, נתאר את הדרכים שבהן יש ליישם את עקרונות המידתיות בהקשר של מעקבים מקוונים.

5.1. סוגיות שאינן מוסדרות בדיני המעקב המקוון בישראל

מידת ההתאמה של הדינים החלים על מעקב מקוון בישראל לעומת זו של ההסדרים הקיימים בארצות הברית ובמדינות אירופה בעניין זה וכן אופני התאמתם הפרשניים לשינויים בסביבה הטכנולוגית והמשפטית – טעונים עיון.

רוב דברי החקיקה הישראליים הרלוונטיים לענייננו נוצרו בעידן שקדם[1] לפרוליפרציה של התקני תקשורת סלולריים ושל מתקני ה"אינטרנט של הדברים" (IoT) ולשימוש הענף שנעשה בטכניקות כר"מ למטרות ביטחוניות.[2] עלייתם של ספקי תקשורת רבי עוצמה שאינם נדרשים לרישיון בזק – מפעילי הפלטפורמות החברתיות למשל – מעלה דילמות של מדיניות בדבר אופני השגת המידע מהם, המתווה של שיתוף הפעולה הרצוי עימם (בייחוד לאחר גילוייו של סנודן) והיכולת המשפטית לכפות עליהם ציות. אשר על כן ספק רב

1 ראו **לעיל** בפרק 2 ה"ש 45.

2 ראו **לעיל** בפרק 1 ה"ש 7 ובחלק 4.6 **לעיל**.

אם הדין הישראלי, והאיזונים המוצעים בו בין שיקולי ביטחון לבין זכויות הפרט, מתאים למציאות הטכנולוגית החדשה. עוד בולטת העובדה כי הדין הישראלי סובל מתת־אסדרה של סוגיות שיש להן מענה בדין המשווה.

ראשית, ההסדרה בדין של סמכויות המעקב המקוון בין גופי החקירה והביטחון השונים חלקית. מאחר שמעמדו של המוסד לתפקידים מיוחדים טרם הוסדר בחקיקה,[3] אין פלא שכאשר מסורות בידיו אי אילו סמכויות מעקב אחר רשתות תקשורת, הדין הישראלי שותק. ואולם גם באשר לפעילותם של שירות הביטחון הכללי, אגף המודיעין במטה הכללי ומשטרת ישראל מתעוררות שאלות של מותר ואסור בנוגע לתקשורת זרה וליעדים מודיעיניים זרים, לרבות הבחנות דקות יותר באשר להוראות החלות על מעקב מקוון שיעדיו הם תושבי שטחים שבשליטת ישראל.[4]

נדרשת אפוא הסדרה מלאה ופרטנית של היקף הסמכויות של כל אחד מגופי הביטחון ואכיפת החוק השונים – הן מבחינת הפרקטיקות המותרות להם, היקף האיסוף המותר והבקרות המופעלות עליהן והן מבחינת ההיקף הטריטוריאלי/פרסונלי של סמכויות אלו.

הדין הישראלי אינו מתיר במפורש פעילות איסוף גורפת וחסרת הבחנה. יתר על כן, בעניין **חוק נתוני תקשורת** הובהר כי אין לפרש אותו כמתיר מתן צווים לאיסוף כללי של נתוני תקשורת לתכליות של אכיפת חוק.[5] ואולם אין להקיש מכך על איסור זהה בנוגע לאיסוף גורף של נתוני תקשורת למטרות ביטחון המדינה שעושה שירות הביטחון הכללי.[6]

הדין הישראלי אף נעדר איסור מפורש על איסוף גורף של נתוני תוכן. עם זאת צווים או היתרים לפי חוק האזנת סתר מותנים בפירוט של "זהות האדם אשר האזנה לשיחותיו הותרה, או זהות הקו או המיתקן המשמשים או המיועדים

3 ראו **לעיל** בפרק 2 ה"ש 19, 20.

4 ראו בחלק 4.1 **לעיל**.

5 ראו בחלק 2.2 **לעיל**.

6 ראו בחלק 2.6 **לעיל**.

לשמש לקליטה, להעברה או לשידור של בזק",[7] ובתנאי שאלו ידועים מראש. אפשר שפרשנות מרחיבה לסעיף תתיר איסוף גורף למטרות מסוימות כשהתנאי שבסיפה אינו מתקיים, או כשדי בציון מתקן הבזק המיורט כדי לקבל גישה לתעבורת תקשורת בנפח גדול.[8]

בדין הישראלי גם אין הסדרים בעניין הגבלת התקופה של שימור הנתונים אצל ספקיות התקשורת, הקיימים בדין האיחוד האירופי ובדין הבריטי והגרמני.[9] אם יש הסדרים כאלו בעניין נתוני תקשורת, הם מצויים בכללים החשאיים שקבע ראש הממשלה לפי חוק השב"כ, שאינם כפופים לביקורת ציבורית.

הפסיקה האירופית, אף שאיננה שוללת פרקטיקות מעקב חסרות הבחנה,[10] נוטה לראות בהן כלי לא מידתי – קשה להצביע על צורך מוחלט ביירוט גורף של חומר ללא הבחנה מינימלית בין ידיד לאויב או בשימורו לתקופה בלתי מוגבלת. לפיכך ההוראות הסטטוטוריות החלות על פרקטיקות אלו במדינות אירופה וגם בארצות הברית מכילות הסדרים שנועדו לתחום את האיסוף בזמן או בקריטריון גאוגרפי או פרסונלי מסוים ולתכליות של ביטחון לאומי. בדין הישראלי נדרשת הסדרה של פרקטיקות אלו כך שתגביל אותן לקריטריונים של מידתיות וצורך מוחלט.

גם זכויותיהם של מושאי המידע במעקבים מקוונים – היעדים המודיעיניים וצדדים שלישיים שנקלעו אגב אורחא לפעילות המעקב – טרם הוסדרו בדין הישראלי, ובייחוד הזכות להישכח, הזכות לסעד והזכות ליידוע. עם זאת יש לציין כי בכל הנוגע להסדרת זכויות אלו רב הנסתר על הגלוי גם בדיני האיחוד

7 ס' 4(ב), 6(ד) לחוק האזנת סתר.

8 שלא כהיתרי האזנת סתר מכוח ס'6(ד) לחוק האזנת סתר, היתרי האזנה לפי ס'4(ב) אינם כפופים לביקורת שיפוטית. אך גם ביקורת שיפוטית, גם אם נעשית בחשאי, אינה מונעת פרשנות מרחיבה – ראו תוכנית איסוף ה-metadata של ה־NSA, בחלק 3.1.6 **לעיל**. עם זאת יש יסוד סביר להניח כי בהישמע ביקורת שיפוטית על האזנות סתר למטרות מניעת פשיעה, לא יתאפשר למשטרה יירוט גורף של נתוני תוכן, במיוחד לאור הפרשנות המצמצמת של חוק נתוני תקשורת בעניין **חוק נתוני תקשורת**, **לעיל** בפרק 2 ה"ש 69.

9 ראו בחלק 4.4 **לעיל**.

10 ראו עניין **האח הגדול** ועניין *Rättvisa*, **לעיל** בפרק 3 ה"ש 227; כהנא, **לעיל** בפרק 3 ה"ש 246.

האירופי[11] או בדין הגרמני,[12] ואפשר כי גם שם המתח בין החשאיות הנדרשת לשם האפקטיביות של פעילות המודיעין ובין זכות היידוע מרוקן במידה רבה את הזכויות האלה מתוכן.

כך גם באשר למותר ולאסור בנושא פעולות כר"מ, שלתוצאותיהן, במיוחד בהקשר הביטחוני או המשטרתי, עלולות להיות השלכות הרות גורל על מושאי המידע.[13] הדין האירופי מנסה לפחות להגביל קבלה של החלטות המתבססת על נתונים שמקורם בפעילויות כר"מ ללא יכולת התערבות אנושית, גם בהקשרים של אכיפת חוק.[14] אסדרה דומה נעדרת מהדין הישראלי. נראה כי טרם נבחנה ההסמכה בדין הישראלי לאיסוף מודיעין גלוי (אוסינט) ברשתות תקשורת. אוסינט מסורתי, שנשען על מקורות גלויים של תקשורת המונים, אינו נדרש כלל מטבעו ומטיבו להסמכה; ואולם אוסינט שלצד מקורות אלה משתמש גם בפרסומים פומביים ברשתות חברתיות – כן נדרש לה. מעקב המוני אחר פעילות אינדיווידואלית גלויה של משתמשים ברשתות חברתיות, לרבות ניתוחו באמצעים ממוכנים, עלול להביא לכדי פגיעה של ממש בפרטיות. אף שגופים פרטיים מפעילים פרקטיקות דומות למטרות מסחריות, הכוח העדיף של המדינה עשוי להביא הן לידי פגיעה חריפה יותר בפרטיות, והן להשלכות מעשיות חמורות אף יותר.[15]

הרשתות החברתיות כשלעצמן מציבות שורה של אתגרים משפטיים חדשים, בהיותן גורם על־לאומי, דו־מהותי, שאינו נוטה להתיישר עם הדין המקומי. שלא כספקי תקשורת בין־אישית שקדמו להם, ספקי פלטפורמות אינם נדרשים לרישיון הפעלה, והוראות הדין החלות על בעלי הרישיונות בכל הנוגע לשיתוף פעולה עם גופי החקירה והביטחון – דוגמת ההסדר שבחוק נתוני תקשורת או סעיף 13 לחוק

11 ראו בחלק 3.2.5.2.1 **לעיל**.

12 ראו למשל ס' 101 לקוד סדר הדין הפליל הגרמני (StPO), ס' 19a, (1)13–(1a) לחוק הפדרלי להגנת מידע (BDSG), וס' 13 לחוק סעיף 10 (G10).

13 ראו הירשאוגה ושיזף, **לעיל** בפרק זה ה"ש 158.

14 סעיף 11 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) (ראו בחלק 3.2.5.2.1 **לעיל**). כמו כן ראו ס' 15(1) לדירקטיבת הגנת המידע וס' 22 לתקנות הכלליות בדבר הגנת מידע (GDPR).

15 ראו בחלק 2.5.4 **לעיל**.

הבזק[16] – אינם נוגעים להם. גופי חקירה וביטחון שמבקשים להשיג נתוני תקשורת – ונתוני תוכן – מספקי פלטפורמות, נדרשים להתמודד עם חוסר נכונות עיקש לשיתוף פעולה, הכרוך בהליכים משפטיים ארוכים;[17] להסתמך על רצונם הטוב של ספקי הפלטפורמות להעביר את המידע המבוקש;[18] או לפתח יכולות יירוט ופענוח של התקשורת ללא הסכמת הספקים. למותר לציין כי במשא ומתן כזה קולם של מושאי המידע כמעט שאינו נשמע, אלא בעקיפין, ורק במקרים שבהם הספקים מעדיפים מטעמיהם שלהם שלא לשתף פעולה עם הרשות החוקרת. מושאי המידע יכולים להשמיע את קולם באמצעות המחוקק ולקבוע הסדר שלפיו יוגדרו בדין נוהלי בקשות המידע מספקי פלטפורמות כאמור ולהכפיפן לתכליות צרות של פשע חמור ושל ביטחון לאומי לפי מבחן של ודאות קרובה ולביקורת שיפוטית.

בשונה מהאיסור הכללי שבדין על האזנת סתר,[19] חוק נתוני תקשורת נעדר הוראה כזאת.[20] יתר על כן, חוק נתוני תקשורת – שמסדיר את דרכי השגתם מבעל רישיון הבזק – שותק באשר להסדרים המתירים איסוף פעיל של נתוני תקשורת, דוגמת החוק האמריקאי בדבר איסוף נתוני תקשורת (PRA).[21] בארצות הברית ובעולם גופי אכיפת חוק משתמשים בטכנולוגיות לאיסוף נתוני תקשורת, דוגמת ה־stingray,[22] שהפעלתן אינה מוסדרת בחקיקה הישראלית.

16 ראו חלק 2.4 וחלק 4.5 **לעיל**.

17 למשל, בפרשת **האייפון**, **לעיל** בפרק 3 ה"ש 123.

18 ראו נתונים אמפיריים בדוחות השקיפות של פייסבוק וגוגל, **לעיל** בפרק 2 ה"ש 30.

19 ס' 2 לחוק האזנת סתר.

20 לדוגמה האיסור שב־18 U.S.C. §2518, החל על תקשורת אלקטרונית מכל סוג (ללא הבחנה בין data ל־metadata), כך גם האיסור על יירוט תקשורת בסעיף 3 לחוק סמכויות חקירה 2016 (IPA).

21 ראו חלק 3.1.3.3 **לעיל**.

22 ראו **לעיל** בפרק 3 ה"ש 71. המתווה בדין הבריטי, בהיעדר הסדר קונקרטי, לשימוש באמצעים אלה הוא כהקבלתם לאמצעי ציתות ("הפרעה לרכוש" או property interference), ראו Sam O'Neill, *Police Sweep Up Phone Data with Secret Snooping Device*, The Times (1.11.2014). לאחרונה העלתה חקירתו של המפקח הקנדי על הפרטיות כי משטרת קנדה השתמשה כשש פעמים בטכנולוגיה זו ללא צו, בהסתמכה על מדיניות זמנית (משנת 2011, אשר עודנה בתוקף) ראו Office Of The Privacy Commissioner of Canada, *Cell Site Simulators used by RCMP not Capable of Intercepting Private Communication* (21.9.2017)

סוגיות שיש להסדיר בדיני המעקב המקוון הישראליים

- **היקף הסמכויות של כל אחד מגורמי הביטחון ואכיפת החוק.** במסגרת אסדרת היקף הסמכויות של גופים אלו (המשטרה, שירות הביטחון הכללי, אגף המודיעין של צה"ל, המוסד לתפקידים מיוחדים וגופי חקירה אחרים) יש להתייחס לפרקטיקות המותרות להם, להיקף האיסוף המותר, לבקרות המופעלות עליהן, ולשאלת התחולה הטריטוריאלית של סמכויות אלו.

- **איסוף גורף (bulk collection).** יש להחיל איסור כללי בדין על איסוף חסר הבחנה, אלא בהתקיימות צורך מוחלט, לשם הגשמת תכליות צרות ומפורטות, ובכפוף לנהלים המבטיחים את צמצום הפגיעה בזכויות למינימום האפשרי.

- **שימור נתונים (data retention).** יש להחיל בדין הישראלי הוראות בנוגע לתקופת שימור הנתונים המרבית של ספקי שירותי בזק. היכולת של הרשויות להורות לספקים לחרוג מתקופה זו ולשמור נתונים לפרק זמן ארוך יותר תהיה בכפוף לצו שיפוטי, לשם הגשמת תכליות צרות ומפורטות, ובכפוף לנהלים המבטיחים את צמצום הפגיעה בזכויות למינימום האפשרי.

- **כריית מידע (כר"מ) ופעילות אוסינטית (OSINT).** יש להסדיר את המותר והאסור בדין בנוגע להצלבת מאגרי נתונים, לשימושים השונים שניתן לעשות בתוצרים של עיבודים סטטיסטיים, ולמידת המיכון והיעדר ההתערבות האנושית בתהליך. נוסף על כך, בנוגע לפרקטיקות של מודיעין גלוי (אוסינט) ברשתות חברתיות – יש להגדיר את סמכויותיהן של הרשויות לפעול בזירה זו ולהגביל פרקטיקות איסוף שאינן פסיביות לחלוטין (כגון שימוש בפרופילים פיקטיביים כדי להשיג גישה למידע שאינו פומבי לחלוטין).

- **השגת מידע מספקים של פלטפורמות תקשורת גלובליות.** יש להסדיר בדין את נוהלי השגת מידע מספקי פלטפורמות תקשורת מקוונות, דוגמת פייסבוק וגוגל, ולהכפיפן לתכליות צרות של פשע חמור ושל ביטחון לאומי לפי מבחן של ודאות קרובה וכן לביקורת שיפוטית.

- **יירוט נתוני תקשורת.** בדומה לאיסור הכללי על האזנת סתר, יש להחיל איסור כללי על יירוט פעיל של נתוני תקשורת (להבדיל מהשגתם דרך חוק נתוני תקשורת או לפי הכללים מכוח חוק השב"כ), ולהסדיר את המקרים שבהם יירוט כאמור יותר, בדומה למתווה של חוק האזנת סתר.

5.2. כללים חשאיים והיעדר שקיפות

גוף הדינים שתואר בחלק 2 לעיל – המעטפת החוקתית ודיני הגנת הפרטיות הישראליים הכלליים, חוק נתוני תקשורת, חוק האזנת סתר וחוק השב"כ – הוא גוף חקיקה רזה יחסית שאינו מעניק מענה סטטוטורי לסוגיות רבות.

המקרה ההודי (ראו בחלק 3.5 לעיל) – של דיני הגנת הפרטיות הכלליים הסובלים מחסרים וממגבלות מעטות על פעילות ביון ממשלתי – מראה כי את החלל הסטטוטורי הריק עלולות לתפוס יוזמות ממשלתיות לניטור מרחיק לכת של אזרחי המדינה. מערכת הדירוג החברתית הסינית (social credit system) שהושקה ב־2014 היא דוגמה נוספת, קיצונית ומטרידה, לאופן שבו ריק כזה יכול להתמלא.[23]

בכל הנוגע לפעילות המעקב ברשתות תקשורת שמבצע שירות הביטחון הכללי, חוק האזנת סתר וחוק השב"כ מתירים מרחב שיקול דעת לממשלה בקביעת הכללים המסדירים אותם – כך באשר לכללים החשאיים המסדירים היתרים למטרות איתור או מניעה של דליפת מידע ביטחוני;[24] לכללים בדבר מחיקה וביעור של חומר האזנה ששמירתו נדרשת מטעמי ביטחון, החשאיים אף הם;[25] לכללים הקובעים את סוגי נתוני התקשורת הדרושים לשירות לצורך מילוי תפקידיו;[26] להוראות החלות מכוח סעיף 11 לחוק השב"כ על שימור, החזקה,

23 ראו **לעיל** בפרק 1 ה"ש 17.

24 ס' 4א(ב) לחוק האזנת סתר. סעיף 4א(ג) מורה כי "הכללים האמורים בסעיף קטן (ב) לא יפורסמו ברשומות או בדרך אחרת והם יוצגו רק בפני הועדה המשותפת".

25 ס' 9ב(א) לחוק האזנת סתר. לפי סעיף 9ב(ב) סיפה: "הכללים לא יפורסמו ברשומות או בדרך אחרת".

26 יתר על כן, פרשנותם של ראש הממשלה ושל השירות באשר לתפקידיו של השירות נהנית ממידה מסוימת של גמישות, ראו בחלק 4.2 **לעיל**.

אבטחה וביעור של נתוני תקשורת שבידי השירות;[27] ולהוראות הניתנות לבעלי רישיון בזק בעניין סיוע לכוחות הביטחון (לרבות משטרת ישראל).[28]

אין ספק כי החשאיות האופפת את הכללים הללו וכן חלק מהביקורת הפרלמנטרית והמינהלית עליהם ועל פעילות מעקב ברשתות תקשורת,[29] יש בה כדי לאפשר גמישות פרשנית ויכולת התאמה של הדין לצורכי השעה ולצרכים המבצעיים הדוחקים. אלא שגמישות זו עלולה להביא לידי פריצת גדרות לפי פרשנות חשאית שסבירותה אינה עומדת למבחן הציבור.[30]

- יש להסיר את מעטה החשאיות מעל הכללים המסדירים את האופן שבו שירות הביטחון הכללי משיג נתוני תקשורת מאת ספקי התקשורת, ולתת פומבי לדיווחים השנתיים על השימוש בהם וכן לדיווחים השנתיים על היקף השימוש של השב"כ בסמכויותיו לפי חוק האזנת סתר.

5.3. בקרה והגנה על זכויות

5.3.1. ביקורת שיפוטית

פריסתה של ביקורת שיפוטית בישראל על היתרים שונים למעקבים מקוונים היא חלקית. החוק פוטר את רשויות הביטחון המבקשות צו האזנת סתר מפנייה לבית המשפט ומסתפק בהיתר מראש (אקס אנטה) מאת השר, ובמקרים

27 ס' 11 (ב), (ד) לחוק השב"כ.

28 ס' 13 לחוק הבזק.

29 ראו ס' 11(ג),11(ה) לחוק השב"כ; ההוראות בדבר בקרה של משרד המשפטים או של הוועדה המתאימה בסעיפים 4(ד)–(ה), 5(ג), 9ב(ב) לחוק האזנת סתר, באשר לסוגי האזנות להן אין בקרה שיפוטית או בקרה פרלמנטרית גלויה.

30 ראו **לעיל** בטקסט המפנה לה"ש 159 **לעיל** בפרק 3.

דחופים, די בהיתר בדיעבד.[31] במקרים דחופים היתר להאזנות סתר למטרת מניעת עבירות וגילוי עבריינים אף הוא אינו טעון צו שיפוטי אלא אם נדרשת הארכתו.[32] חוק האזנת סתר פוטר סוגים מסוימים של האזנות מדרישה להיתר כלשהו, ואפשר שניתן למצוא בהם את ההסדר החוקי המאפשר איסוף מידע גלוי ברשת, לרבות מרשתות חברתיות.[33]

ביקורת שיפוטית בנושא השגת נתוני תקשורת ואיסופם מוגבלת למקרים שאינם דחופים, בהם המשטרה נדרשת לנתוני תקשורת למטרות חקירה ואכיפת חוק.[34] אין כל הוראה האוסרת על המשטרה לנצל טכנולוגיות של איסוף נתוני תקשורת שאינן כרוכות בפנייה לבעלי רישיון בזק.[35] כמו כן אין כל דרישה לצו שיפוטי שמתיר איסוף נתוני תקשורת (על דרך של יירוט עצמאי, גישה מקוונת או בקשה עיתית) שעושה שירות הביטחון הכללי. יתר על כן – נראה כי האיסוף עצמו אינו מותנה כלל בהיתר (מאת ראש השירות), אלא רק עצם השימוש במידע.[36]

סקירת הדין המשווה מעלה כי גם במדינות אחרות אין ביקורת שיפוטית גורפת על מעקב ברשתות תקשורת. ברירת המחדל של הדין האמריקאי היא אמנם צו שיפוטי כשמדובר בחיפוש לפי התיקון הרביעי לחוקה[37] – דרוש צו שיפוטי כדי להתיר בקשות להאזנות סתר לפי חוק האזנות סתר (WTA), בקשות לנתוני תוכן שמורים מספקי תקשורת לפי כוח חוק תקשורת שמורה (SCA) (למעט במקרים שבהם הבקשה מסתמכת על מכתב ביטחון לאומי (NSL), שם הביקורת השיפוטית תתאפשר בדיעבד אם הספק יבחר לערער) ובקשות לשימוש במתקני

31 ס' 4(א), 5(א)–(ב) לחוק האזנת סתר.

32 ס' 7 לחוק האזנת סתר.

33 ראו בחלק 2.5.4 **לעיל**.

34 ראו בחלק 2.4 **לעיל**.

35 ראו **לעיל** בפרק זה ה"ש 22. עם זאת ייתכן שאם תאומץ הגישה הבריטית, שימוש משטרתי בטכנולוגיות stingray יהיה כפוף לכללים החלים על פעילויות סייבר משטרתיות.

36 ס' 11 לחוק השב"כ.

37 ראו בחלק 3.1.2.1 **לעיל**, וכן בעניין **חוק נתוני תקשורת**, פס' 17 לפסק דינה של הנשיאה ביניש, **לעיל** בפרק 2 ה"ש 69.

יירוט של נתוני תקשורת.[38] ואולם מעקב מקוון אחר מודיעין זר נעשה לפי היתרים חשאיים מבית המשפט למודיעין זר (FISC), ובנסיבות שונות התערבותו אינה נדרשת, במיוחד כשמדובר ביעדים שאינם בגדרי "אדם אמריקאי".[39]

מגנון הנעילה הכפולה, שהוצג בבריטניה ברפורמת חוק סמכויות חקירה (IPA) ב־2016[40] – המתנה החלטה מיניסטריאלית־אקזקוטיבית של השר ליתן צו באישורו של גורם מעין־שיפוטי (נציב שיפוטי) – אינו חל על כל צווי המעקב שבגדרי החוק (אין נדרש צו לצורך השגת נתוני תקשורת למשל).[41] נוסף על כך יש הסוברים כי מוסד המפקח על סמכויות החקירה אינו עצמאי די הצורך.[42]

גם בגרמניה לא כל פרקטיקות המעקב המקוון מותנות בצו שיפוטי. השגת נתוני תקשורת והאזנות סתר טעונות צו שיפוטי מראש (אקס אנטה) לפי הוראות סדר הדין הפלילי, שבמקרי חירום יכול להינתן בדיעבד.[43] לפי החריג שבחוק היסוד הגרמני, צווים הקשורים למעקב מקוון של סוכנויות הביון למטרות ביטחוניות אינם טעונים צו שיפוטי. הבקרה על היתרים נעשית כאמור בדיעבד – באמצאות דיווח לוועדת סעיף 10 או לוועדה העצמאית (מכוח חוק סוכנות הביון הפדרלית (BNDG)) – לפי העניין, ואלה רשאיות לבטל את ההיתר.[44]

במסגרת התנאים שקבע בית הדין האירופי לזכויות אדם (ECtHR) בעניין *Huvig*,[45] לצורך הפעלת מעקב מקוון נותרה הביקורת השיפוטית האפריורית על אמצעי מעקב בבחינת דרישה אופציונלית בלבד. גם הדין ההודי כמעט

38 ראו בחלק 3.1.3 **לעיל**.

39 ראו בחלקים 3.1.5–3.1.7 **לעיל**.

40 ראו חלק 3.3.4 **לעיל**.

41 ראו חלק 3.3.4.5 **לעיל**.

42 ראו Karemba, **לעיל** בפרק 3 ה"ש 743.

43 ראו חלק 3.4.3.1 **לעיל**.

44 ראו בחלקים 3.4.3.3, 3.4.3.4 **לעיל**.

45 ראו עניין *Huvig*, **לעיל** בפרק 3 ה"ש 227. וראו גם Malgieri & De Hert, **לעיל** בפרק 3 ה"ש 234.

שאינו דורש צו שיפוטי כתנאי להפעלת מעקב מקוון, אלא כאשר המידע מבוקש באמצעות צו המצאה.[46]

נראה אפוא שגם בדין המשווה שנסקר מעקב מקוון אינו כפוף לביקורת שיפוטית גורפת. עם זאת הן בגרמניה והן בארצות הברית פעילות האיסוף של נתוני תוכן ונתוני תקשורת למטרות מניעת פשע ואכיפת חוק כפופה על פי רוב לביקורת שיפוטית, על פי רוב אפריורית ולפחות בדיעבד. עם זאת בשתי המדינות יש הסדרים לבחינה שיפוטית או מעין־שיפוטית של היתרים להאזנות סתר לתכליות ביטחוניות.

להשלמת התמונה יש להתייחס גם לנתונים האמפיריים. בשל הוראות החקיקה היקף המידע המצוי ברשותנו מוגבל לדיווחי המשרד לביטחון פנים לפי חוק האזנות סתר, המתייחסים להאזנות לתכליות של מניעת פשע ואכיפת חוק בלבד ולדיווחים לפי הוראת השעה שבחוק נתוני תקשורת.[47] שיעור הבקשות שנדחו בבית המשפט נמוך ממחצית האחוז בכל התקופה המדווחת (תמונה דומה של שיעור דחייה נמוך עולה גם מדיווחי מינהלת בתי המשפט בארצות הברית בקשר לבקשות להאזנות סתר למטרות אכיפת החוק ומניעת פשיעה).[48] עם זאת בנתון האמפירי של שיעור הדחייה הנמוך של בית המשפט של בקשות לצווי האזנת סתר אין די כדי להסיק כי מנגנון הביקורת השיפוטי האפריורי על האזנות סתר הוא לכאורה לא יותר מחותמת גומי, שכן בית המשפט רשאי לאשר בקשות בכפוף לסייגים ולהקשחת הנהלים שבצו המבוקש, וכך אכן נעשה, לפי הנטען בוועדת החקירה הפרלמנטרית בנושא האזנות סתר.[49] כמו כן עצם הביקורת השיפוטית עשוי לייצר תמריצים לגופי החקירה לסנן בקשות לא ראויות עוד טרם הגשתן לבית המשפט.

עם החשש שביקורת שיפוטית על צווי האזנת סתר תהפוך מכנית או תיטה לתמוך בשיטתיות בעמדתן של רשויות החקירה אפשר להתמודד בכמה אופנים.

46 ראו חלק 3.5.2.1 **לעיל**.

47 ראו בחלקים 2.5.3, 2.4 **לעיל**.

48 ראו לוח 5, **לעיל** בפרק 3 ה"ש 90.

49 ראו **לעיל** בפרק 2 ה"ש 92.

דוגמה אחת מצויה בחוק סמכויות החקירה הבריטי (IPA), המבנה את הביקורת השיפוטית.[50] בשונה מההנחיה הכללית לשופט (או לשר, לפי העניין) המצויה בחוק האזנת סתר – לשקול "את מידת הפגיעה בפרטיות" (והדומות לה בחוק נתוני תקשורת)[51] – ההנחיות שבסעיף 2 ל־IPA נועדו לעצב מסגרת כללית לשיקול הדעת המינהלי והשיפוטי המופעל במתן צווים מכוח החוק: בקבלת החלטה הקשורה להפעלת סמכויות לפי ה־IPA יש לבחון אם ניתן להשתמש באמצעים שפגיעתם בפרטיות קטנה יותר,[52] את מידת ההגנה שיש להפעיל במסגרת השגת הנתונים המבוקשים, את רגישותם, אינטרסים ציבוריים בעניין שלמותן של מערכות תקשורת וכל היבט אחר של אינטרסים ציבוריים בהגנת הפרטיות.[53] מנגד, שיקולים אלו כפופים לשיקולים אחרים, בכללם אינטרסים של הביטחון הלאומי ושגשוגה הכלכלי של בריטניה והאינטרס הציבור בזיהוי פשיעה ובמניעתה.[54]

שיקולים נוספים הנמנים במסגרת ה־IPA הם הוראותיו של החוק הבריטי לזכויות אדם (HRA), הוראות אחרות שבדין הציבורי וכן שיקולי צורך ומידתיות.[55] עם זאת נראה כי ההסדר בסעיף 2 ל־IPA, המבנה את שיקול הדעת השיפוטי, אינו מספק הנחיה שחורגת מפירוט מערך שיקולים שנדמה כמובן מאליו, וספק אם ניתן להגדיר מראש את משקלו היחסי הרצוי של כל שיקול ושיקול. דרך חלופית להבניה של שיקול דעת שיפוטי דומה היא על דרך הדרישות מתוכן הבקשה

50 ראו חלק 3.3.4.2 **לעיל**.

51 סעיפים 4(א), 6(א) לחוק האזנת סתר. סעיף 3(א) לחוק נתוני תקשורת. יוער כי ההיתרים הניתנים במקרים דחופים ללא ביקורת שיפוטית אינם מחייבים ולו שקילה כללית של מידת הפגיעה בפרטיות. ראו ס' 5(א), 7(5) לחוק האזנת סתר וס' 4(א) לחוק נתוני תקשורת.

52 ס'2(2)((aלחוק סמכויות חקירה 2016 (IPA), והשוו לעניין **חוק נתוני תקשורת**, **לעיל** בפרק 2 ה"ש 69, פס' 15–16 לפסק דינה של הנשיאה ביניש, וכן עניין **האגודה לזכויות אזרח בישראל נ' משרד הפנים**, **לעיל** בפרק 1 ה"ש 13, בפס' 7–8 לפסק דינה של השופטת דורנר.

53 ס' 2(2) לחוק סמכויות חקירה 2016 (IPA).

54 ס' 2(4)(b)–(a) לחוק סמכויות חקירה 2016 (IPA).

55 ס' 2(4)(e)–(c) לחוק סמכויות חקירה 2016 (IPA).

והצו (דוגמת הדרישה להכללת נוהלי צמצום בצווי חוק האזנות סתר (WTA) או בבקשות ליירוט תקשורת לפי חוק איסוף מודיעין זר (FISA)).[56]

אפשרות אחרת להגברת המודעות השיפוטית לשיקולים שבהגנת הפרטיות במסגרת מתן צווים לפעילות של מעקב ברשתות תקשורת, היא להפוך את ההליך לאדוורסרי. מתן זכות ערעור במקרים שבהם הנתונים המבוקשים הם אצל צד שלישי – ספק שירותי בזק או מפעיל של פלטפורמות מקוונות – אפשר שייתן קול עקיף גם למושאי המידע. עם זאת לא בכל המקרים יש צד שלישי כזה, או שהאינטרסים של אותו צד שלישי אינם חופפים כלל את אלו של מושא המידע, ומנגד – יידוע מושא המידע ישירות בנוגע לבקשה לצו המתיר מעקב מקוון אחריו, יש בו כדי לסכל את תכלית הבקשה. הרחבת האדוורסריות של ההליך יכולה אפוא להיות רק למיהותו של הצד השלישי המייצג את מושא המידע או את האינטרס הציבורי בפרטיות בכללותו. אם מדובר במתווה דמוי ידיד בית המשפט – שבמסגרתו ארגונים אזרחיים יטענו בשם מושא המידע או הציבור – יש למצוא דרך ליידע אותם בחשאי על הליכים כאלה ולהבטיח כי חשאיותם תישמר בלי שעצמאותם תיפגע.

חיזוק הגנות הקיימות בדין הישראלי בעניין הפעלת סמכויות מעקב מקוון יכול שיתבצע באמצעות בקרה מעין־שיפוטית כשאין נדרש צו שיפוטי. גוף פיקוח עצמאי, מעין־שיפוטי, שיאשר בקשות להיתרי האזנת סתר או לאיסוף נתוני תקשורת לתכליות ביטחוניות, עשוי לחזק את ההגנה על פרטיותם של מושאי המידע, מושאי הבקשות. צירוף גוף שמייצג את האינטרס הציבורי בהגנה על הזכות לפרטיות כצד להליכים כאלה עשוי לחזק במידה ניכרת את האפקטיביות שלהם ככלי פיקוח ובקרה.[57]

56 ראו בחלק 3.1.5 **לעיל**.

57 השוו למשל להסדר ידיד בית המשפט (amicus curiae) שבהליכי בית המשפט למודיעין זר (FISC). על שופטי ה־FISC למנות לכל הפחות חמישה ידידים לבית המשפט ולפנות אליהם במקרים שבהם במסגרת החלטה או צו שבית המשפט נדרש לתת, מתעוררת שאלה משמעותית או חדשנית שבדין. ידיד בית המשפט שמונה בדרך זו נדרש להיות מומחה לפרטיות ולחירויות אזרח, וכן להיות בעל סיווג ביטחוני מתאים. ראו 50 U.S.C. §1803(i). להרחבה ראו Ben Cook, *The New FISA Court Amicus Should Be Able to Ignore its Congressionally Imposed Duty*, 66 Am. U. L. Rev. 539 (2017)

כמו כן הכרה בזכות היידוע של מושאי המעקב וצדדים שלישיים, גם כזכות יחסית הכפופה לשיקולי ביטחון,[58] העשויה להתממש רק בחלוף זמן שימזער את הפגיעה הביטחונית הכרוכה בגילוי דבר ההפעלה של סמכות מעקב מקוון, יכולה לאפשר תביעות נזיקיות או אחרות בקשר להפעלת הסמכות. ביקורת שיפוטית כזאת, גם אם תתבצע בדיעבד, אפשר שתתרום תרומה חשובה להבטחת החוקיות של פעילות המעקב המקוון.

5.3.2. רשות פיקוח עצמאית

הביקורת השיפוטית והמעין־שיפוטית על פעילות מעקב אחר רשתות תקשורת היא ריאקטיבית, ותגובתה מוגבלת לבקשות או לצווים קונקרטיים. ביקורת כזאת אינה עוסקת במקרים שבהם הרשויות נמנעו מלבקש צווים מתאימים בשל היעדר חובה חוקית לעשות כן, או בשל פרשנות מצמצמת של החובה הקיימת. מסיבה זו שיטות משפט אחדות הסמיכו רשויות מינהלתיות או מעין־שיפוטיות לפקח בעצמן על פעילות המעקב המקוון של גופי הביטחון. כך למשל על בסיס דיני הגנת הפרטיות הכלליים של האיחוד האירופי חייבת כל מדינה־חברה להקים רשות להגנת מידע (DPA)[59] – גוף פיקוח עצמאי מדינתי שמפקח

58 זכות היידוע בדיני האיחוד חלה על יידועו של מושא מידע כי נאסף מידע אישי על אודותיו שלא בהסכמתו (בשונה מהזכות הריאקטיבית לגישה למידע, הכפופה לפנייה מאת מושא המידע למנהל המאגר – ראו ס' 12 לדירקטיבת הגנת המידע והסייגים לה מטעמי ביטחון לאומי שהמנויים בסעיף 13; ס' 14–15 לדירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680); ס' 13 לתקנות הכלליות בדבר הגנת מידע (GDPR) והסייגים לו בס' 23). ראו ס' 6(4)(a) לתקנות הכלליות בדבר הגנת מידע (GDPR). כמו כן ס' 23(2)(h) ל־GDPR מציין כי דברי חקיקה המגבילים את חובות המדינות החברות באיחוד כלפי מושאי מידע מכוח ה־GDPR צריכים להכיל הוראות בנושא זכותם של מושאי המידע ליידוע על הגבלות אלו כל עוד היידוע אינו מאיין את תכלית החקיקה. חובת יידוע דומה מצויה בדין הגרמני הכללי (ס' 19a לחוק הפדרלי להגנת מידע (BDSG)), והיא אינה חלה כשיידוע מושא המידע הוא לא מידתי או אם יש הוראה אחרת בדין. חוק סעיף 10 מורה על יידוע היעד המודיעיני על ביצוע מעקב אינדיווידואלי משהסתיימה פעולת המעקב, אלא אם הדבר מהווה איום על תכלית המעקב. אם זכות היידוע לא מומשה בתוך שנה, כל דחייה נוספת כרוכה באישור ועדת סעיף 10 (ראו **להלן**). ביקורת שיפוטית של כל צו המאשר מעקב כאמור אסורה טרם יידוע מושאו. (ס' 12 לחוק סעיף 10 (G10)); זכות היידוע בחוק המשטרה הפדרלית (BKAG) קמה בעניין השגת נתוני תוכן ותקשורת מספקי טלקומוניקציה, ובתנאי שאין ביידוע מושא המידע כדי לפגוע בתכליות האיסוף (ס' 20b(6) לחוק המשטרה הפדרלית), ובעניין איסוף מידע כללי מטעם ה־BKA (ס' 7(6) לחוק המשטרה הפדרלית).

59 ראו בחלק 3.2.3.4 **לעיל**.

על יישום החקיקה על פי דירקטיבת הגנת המידע והתקנות הכלליות בדבר הגנת מידע (GDPR)). גם ההוראות של דירקטיבת רשויות אכיפת החוק (דירקטיבה 2016/680) – החלות על רשויות החקירה – מורות להקים רשות פיקוח עצמאית שתפקח על יישום הדירקטיבה (שאפשר למזגה אותה עם ה־DPA שהוקם מכוח ה־GDPR או קודם לכן, מכוח דירקטיבת הגנת המידע).[60]

בבריטניה, כמה סמכויות חקירה ופיקוח מסורות לטריבונל סמכויות החקירה, המוסמך לפתוח בחקירה עצמאית בתגובה לתלונות על הפעלת סמכויות מכוח חוק סמכויות חקירה 2016 (IPA) שלא כדין.[61] לצד הביקורת השיפוטית של נציב סמכויות החקירה והנציבים השיפוטיים במסגרת מנגנון הנעילה הכפולה, מסורות לנציב סמכויות החקירה גם סמכויות חקירה ופיקוח כלליות על הרשויות העוסקות בפעילויות של יירוט תקשורת, התערבות בציוד או השגה ושימור של נתוני תקשורת או מידע משני, לרבות פיקוח בדיעבד על הציות בפועל להוראות הצווים.[62] עם זאת החוק מורה לנציבים שלא לפעול נגד האינטרס הציבורי ולהקפיד לא לפגוע בביטחון הלאומי או במצבה הכלכלי של הממלכה. בעיקר עליהם לוודא שהם נמנעים מלסכן פעולות של מודיעין או אכיפת חוק או את ביטחונם של המשתתפים בפעולות אלו, וכן שאינם מכבידים ללא צורך על האפקטיביות המבצעית של שירותי המודיעין, כוחות המשטרה והביטחון או משרדי הממשלה.[63]

בישראל רשות ההגנה על הפרטיות (לשעבר רמו"ט – הרשות למשפט וטכנולוגיה) היא הרגולטור המופקד על הפיקוח והאכיפה של חוק הגנת הפרטיות, חוק שירות נתוני אשראי וחוק חתימה אלקטרונית. עם זאת בשל הפטורים שבחוק הגנת הפרטיות,[64] למעשה אין הרשות מפקחת על פעילות שנוקטות רשויות הביטחון ואכיפת החוק בכל הנוגע למעקב מקוון.

60 ראו בחלק 3.2.5.2.3 **לעיל**.

61 ראו בחלק 3.3.4.9.2 **לעיל**.

62 ראו לדוגמה את עניין **אבוקסיס**, **לעיל** בפרק 2 ה"ש 104, שבו נדונו קבילותן של ראיות שהושגו באיסוף שחרג מהוראות שניתנו בצו.

63 ראו בחלק 3.3.4.9.1 **לעיל**.

64 ראו בחלק 2.3 **לעיל**.

הקמתו של גוף מפקח עצמאי או הרחבת סמכויותיה של רשות ההגנה על הפרטיות כדי שזו תוכל לפקח על התקינות של פעולות עיבוד הנתונים – לרבות איסוף ושימור – הנעשות כחלק ממעקב אחרי רשתות תקשורת לתכליות ביטחוניות או משטרתיות, יכולה להכניס שחקן נוסף ששומר על האינטרס לפרטיות של מושאי המידע. רצוי שיהיה זה גוף, שנוסף על עצמאותו יהיו לו גם מלוא סמכויות הפיקוח הנדרשות למילוי תפקידיו, כגון סמכויות חקירה בעקבות תלונות או ביוזמתו שלו וסמכויות ייעוץ והנחיה מקצועית בנוגע להיבטים של הגנת פרטיות באסדרה רלוונטית. לצד סמכויות חקירה ובירור יש לתת לו גם את היכולת להכריע באופן שישפיע על הפרקטיקות הנבדקות.[65]

עם זאת יש לזכור כי עבודת הפיקוח על ארגונים ביטחוניים, ששקיפותה מוגבלת, עלולה להיחשד בשיתוף פעולה עם הגוף המפוקח, בייחוד במקרים שבהם לא נמצא כל פסול בו.[66] בנסיבות אלה יש לחייב את הגוף המפקח לדווח על עבודת הביקורת שלו לגוף עצמאי אחר כמו ועדת המשנה לענייני מודיעין ושירותים חשאיים של ועדת חוץ וביטחון.

חלופה אחרת מצויה בהסדר ה־Privacy Shield להעברת מידע בין אירופה לארצות הברית, שהורתו בביטול הסדר ה־Safe Harbor בבית הדין האירופי במסגרת עניין *Schrems*.[67] במכתבים נלווים להסכם ה־Privacy Shield מונה המתאם הבכיר לדיפלומטיית IT בין־לאומית[68] לאומבודסמן לענייני

65 ראו לדוגמה אחדים מהעקרונות הנמנים אצל Sarah Eskens, Ot van Daalen & Nico van Eijk, *Ten Standards for Oversight and Transparency of National Intelligence Services*, Institute for Information Law (2015); Eleni Braat & Floribert Baudet, *Intelligence Accountability in a Globalizing World. Towards an Instrument of Measuring Effectiveness, in* Perspectives on Military Intelligence from the First World War to Mali 236–239 (Floribert Baudet, Eleni Braat, Jeoffrey van Woensel, & Aad Wever, eds., 2017)

66 ראו למשל יותם ברגר, "מאות נחקרים התלוננו, אך משרד המשפטים לא פתח בחקירה נגד איש שב"כ" **הארץ** (7.12.2016); מרדכי קרמניצר "אמצעים להתמודדות עם עינויים" בתוך קרמניצר ואח', **לעיל** בפרק 1 ה"ש 16, בעמ' 63–67, 109–115.

67 ראו **לעיל** בפרק 3 ה"ש 175.

68 תפקיד זה הוקם בעת ממשל אובמה, לפי הוראת המדיניות הנשיאותית 28 (Presidential Policy Directive 28, Sec. 4(d)).

ה־Privacy Shield.[69] אומבודסמן, בקווים כלליים, הוא גוף עצמאי, נטול פניות, בעל סמכויות ריאקטיביות לחקור תלונות, למצוא באופן לא פורמלי פתרונות להן, ולעיתים לתת פומבי לממצאיו תוך שמירה על דיסקרטיות המתלוננים[70] (כך למשל רשויות הגנת המידע (DPA) הפיניות מכונות "אומבודסמן"). האומבודסמן האמריקאי לענייני ה־Privacy Shield משמש כתובת להעברת תלונות פרטניות שהתקבלו ברשויות האירופיות להגנת הפרטיות אל קהיליית המודיעין האמריקאית. האומבודסמן לא יאשר את נכונות התלונה או יכחישה, אבל יאשר כי זו נתקבלה אצלו, וכי לאחר בירורה נמצא כי הפרקטיקה המודיעינית מושא התלונה מצויה בהלימה עם החקיקה האמריקאית, או שבעקבות הבירור אי־ההלימה תוקנה.

- יש להקים גוף פיקוח עצמאי לבקרה על פעילות המעקב המקוון השוטפת של רשויות המדינה, לבחינת הציות להוראות שבצווים, וכן לייעוץ ולהנחייה מקצועית בנוגע להיבטי הגנת פרטיות באסדרה רלוונטית.
- חלופה להקמת גוף זה היא הרחבת סמכויותיה של הרשות להגנה על הפרטיות (לשעבר רמו"ט), כך שיוקנו לה סמכויות לפקח על הגנת הפרטיות בפעילויות מעקב מקוון של רשויות הביטחון ואכיפת החוק.
- עוד חלופה היא ייסוד פונקציה של אומבודסמן לענייני פרטיות במעקב מקוון – גוף עצמאי, נטול פניות, בעל סמכויות ריאקטיביות לחקור תלונות, למצוא באופן בלתי פורמלי פתרונות להן, ולעתים לתת פומבי לממצאיו, תוך שמירת הדיסקרטיות של המתלוננים.

69 ראו נספח A למכתב מזכיר המדינה לנציבת האיחוד לצדק, צרכנות ושוויון בין המינים מיום 7.7.2016.

70 ראו Colin Bennett, Redress, the International Protection of Privacy and National Security and Intelligence Agencies: The Role for an Ombudsperson (2017); Maria Tzanou, The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance 244-246 (2017)

5.3.3. ביקורת פרלמנטרית וציבורית

הביקורת הפרלמנטרית של הכנסת על פרקטיקות המעקב המקוון של המשטרה ושירות הביטחון הכללי מוגבלת לדיווחים סטטוטוריים לפי חוק האזנת סתר (משתמה הוראת השעה על דיווחים לפי חוק נתוני תקשורת),[71] וחלקם אף נעשה בדלתיים סגורות. ניסיון להשיג את הדיווחים החשאיים באמצעות בקשה לפי חוק חופש המידע נדחה בבית המשפט העליון, שבהערת אגב המליץ על גילוי וולונטרי של פרטים אלה למען אמון הציבור לפני שיודלפו.[72]

רצוי לדווח בפומבי על הפעלה של סמכויות מעקב מקוון (האזנות סתר ואיסוף נתוני תקשורת) למטרות של ביטחון המדינה ברמת פירוט זהה לזו שבדיווחי המשרד לביטחון פנים על הפעלת סמכויות אלו בידי המשטרה (בשונה מהרף המינימלי שנקבע בסעיף 4(ה) בחוק האזנת סתר). ספק אם ניתן למצוא נימוק ביטחוני כבד משקל להותרת דיווחים אלו – נתונים מספריים על היקף פעילותו של שירות הביטחון הכללי – מאחורי דלתיים סגורות.

כמו כן, כפי שהוצע, יש להפוך את הוראת השעה שבחוק נתוני תקשורת לקבועה.[73] כמו שעולה מתשובת המשטרה לבקשת חופש המידע בעניין חוק נתוני תקשורת, בתקופה שלא חלה עליה החובה לדווח לכנסת חל גידול ניכר במספר ההיתרים לבקשות דחופות מכוח סעיף 4 לחוק נתוני תקשורת, שאינם כפופים לביקורת שיפוטית.[74]

אך גם דיווח עיתי וגלוי של נתונים אלה במלואם, לרבות אלו החסרים,[75] יכול שיהיה אפקטיבי רק בהישמע ביקורת פרלמנטרית מהותית בעניינו, או לפחות

71 ס' 4(ד), 6(ז) לחוק האזנת סתר.

72 ראו **לעיל** בפרק 2 ה"ש 90. על הדלפה כזרז של רפורמה, ראו Robert Dover, *Regulation by Revelation: The Opportunities and Challenges of Information Control in an Intelligence Era*, 36 SAIS Rev. Int'l. Affairs 103 (2016)

73 ראו **לעיל** בפרק 2 ה"ש 52.

74 ראו **לעיל** בפרק 2 לוח 3 וה"ש 53.

75 ראו **לעיל** בפרק 2 ה"ש 76, ו**לעיל** בפרק זה ה"ש 29.

ביקורת ברורה מצד ארגוני החברה האזרחית או האקדמיה על הנתונים המדווחים. לצד הדיווח העיתי המוצע יש לאפשר לוועדה – או לגוף ביקורת עצמאי אחר – להגיב לנתונים המדווחים, להשתמש בסמכויות חקירה וביקורת כדי ללבן עם רשויות החקירה, הביטחון ואכיפת החוק סוגיות שעולות מהם, ולתת המלצות לפעולה.

- יש להחיל על ראשי רשויות הביטחון חובת דיווח שנתית לוועדת חוק, חוקה ומשפט ולוועדת חוץ וביטחון של הכנסת על מספר האזנות הסתר שבוצעו למטרות ביטחון המדינה, ברמת פירוט זהה לדיווח השנתי של המשרד לביטחון פנים על הפעלת סמכויות אלו על ידי משטרת ישראל.
- יש להפוך את הוראת השעה שבחוק נתוני תקשורת לקבועה, ולחייב את משטרת ישראל בדיווח שנתי על הפעלת סמכויותיה לפי חוק זה.

5.4. אסדרה מידתית של מעקב מקוון

חוק־יסוד: כבוד האדם וחירותו מתיר פגיעה בזכות לפרטיות המנויה בסעיף 7 "בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שלא עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו".

בעת מתן צווים לא דחופים לפי חוק האזנת סתר וחוק נתוני תקשורת יש להפעיל מבחן של צורך המביא לידי ביטוי שיקולים של מידת הפגיעה בפרטיות.[76] לצד ניסוח דרישה מפורשת שכזאת, ההסדר הרגולטורי כשלעצמו יכול שיהיה מידתי, ואכן, בעניין **חוק נתוני תקשורת** שימשו מבחני המידתיות להבניית

76 ס' 4(א), 6(א) לחוק האזנת סתר; ס' 3(א) לחוק נתוני תקשורת.

פרשנות מידתית לחקיקה שלא תחייב את פסילתה.[77] בדין המשווה ניתן למצוא הוראות שמחייבות לפרט בצו המתיר מעקב מקוון את נוהלי הצמצום שיופעלו במסגרתו[78] או הוראות המתירות שימוש באמצעי מעקב אלו בהיעדר חלופות שפגיעתן פחותה.[79]

הקריטריון שלאורו תיבחן מידתיותם של הסדרים בדין הוא מבחן האמצעי שפגיעתו פחותה. רציונל זה מסביר את המבנה המטריציוני של דיני המעקב המקוון, המבחינים בין סוגי נתונים (נתוני תוכן ונתוני תקשורת), בין תכליות מעקב (למטרות אכיפת חוק ושיטור או לתכליות ביטחוניות), ולעיתים גם נוגעים לשיקולים של זיקה טריטוריאלית או פרסונלית של יעד האיסוף.

יחס מידתי קיים כשהדין מכיל הסדרים בדרגות חומרה שונות לתכליות השונות שלשמן יופעלו האמצעים של מעקב מקוון, כך שמידת הבקרה על הפגיעה בזכות עומדת ביחס הפוך לחשיבות התכלית שביסוד האמצעי הפוגע בה.[80] גם ההבחנה בין רמות שונות של פגיעה בזכות המוגנת המתבססת על השוני בין נתוני תקשורת ובין נתוני תוכן נועדה להבנות היבט זה של מידתיות לתוך הדין. ואולם מאחר שנכונותה של הבחנה זו מוטלת בספק, ייתכן שלא רצוי להשתמש בה שימוש גורף.[81] תחולת הרציונל המידתי על ההבחנה בין רמת הזיקה הטריטוריאלית או הפרסונלית של היעד המודיעיני לישראל כמצדיקה מידות שונות של חומרת הבקרה על אמצעי המעקב אף היא עלולה להיות לא ראויה.[82] עם זאת אם השונות בעוצמת הפגיעה בזכות לפי התכליות השונות

77 ראו בחלק 2.2 **לעיל**.

78 לדין האמריקאי ראו **לעיל** בפרק 3 ה"ש 192, וכן ראו הטקסט המפנה לה"ש 135 בפרק 3 **לעיל**; לדין הבריטי ראו ס' 53(2)–(6) לחוק סמכויות חקירה 2016 (IPA).

79 דוגמת ה־WTA, בחלק 3.1.3.1 **לעיל**. ראו גם בדיני הגנת הפרטיות הכלליים בגרמניה, הוראות כגון ס'14(4) לחוק הפדרלי להגנת מידע (BDSG); ובדין ההודי, כלל 419A(3) לכללי הטלגרף ההודיים, **לעיל** בפרק 3 ה"ש 977. ראו גם ע"פ 1668/98 **היועץ המשפטי לממשלה נ' נשיא בית־המשפט המחוזי בירושלים**, פ"ד נו(1) 625 (1998).

80 ראו עניין **חוק נתוני תקשורת**, **לעיל** בפרק 2 ה"ש 69, פס' 19–20 לפסק דינה של הנשיאה ביניש.

81 ראו טנא, **לעיל** בפרק 4 ה"ש 123.

82 ראו בחלק 4.1 **לעיל**.

תימצא מידתית ללא בקרות לצמצום זליגת מודיעין,[83] ההבחנה בין התכליות השונות ובין האמצעים המותרים להגשמתן תרוקן מתוכן. היבט נוסף שלאורו תיבחן מידתיות ההסדר הוא ההוראות החלות על שימור נתונים: האם חלה על ספקי התקשורת חובה לשמור נתוני תקשורת ותעבורה ללא הבחנה לפרקי זמן ארוכים? האם חובה זו חלה רק לפי הוראה קונקרטית בצו מאת רשויות החקירה? והאם יש כלל תיחום בזמן של משך השימור?[84]

ככלל, איסוף גורף אינו נתפס כמידתי (כך גם פעולות עיבוד אחרות, לרבות שימור, הנעשות ללא הבחנה),[85] ורוב הדינים החלים על מעקב מקוון דורשים פירוט של יעדי האיסוף.[86] כדי לצמצם את הפגיעה בזכות, יש לוודא כי יעדי האיסוף מוגבלים למינימום הנדרש. המתווה המסדיר איסוף גורף (bulk collection) בחוק הבריטי לסמכויות חקירה (IPA) מנסה להבחין בין שלב האיסוף לשלב העיון בנתונים.[87] הבחנה זו בין איסוף לשימוש יש בה כדי למתן את חומרת הפגיעה בזכויות המוגנות של פרקטיקות איסוף גורפות כאלו, אך עמידתה במבחני המידתיות מותנית בעיצוב המפורט של ההסדר ובאופן שבו מובטח שהעיון בחומר מוגבל לתכליות מסדר ראשון, למטרות אופרטיביות ספציפיות (בשונה מ"מסעות דיג"), בהגבלת הגישה לחומר על בסיס של צורך מבצעי בלבד. שיקול נוסף בהקשר זה הוא משך תקופת ההחזקה בתוצרי האיסוף חסר ההבחנה.

שיקולים נוספים בבחינת המידתיות של הסדרת פרקטיקת מעקב ברשתות תקשורת הם מידת הביקורת השיפוטית או המינהלית עליה;[88] מידת ההגבלות החלות על השיתוף של הנתונים הגולמיים או תוצרי האיסוף עם סוכנויות מודיעין ואכיפת חוק אחרות או עם רשויות ציבוריות אחרות; טיבם של כללי

83 ראו בחלק 4.2 **לעיל**.

84 ראו בחלק 4.4 **לעיל**.

85 ראו עניין *Tele2 Sverige AB*, **לעיל** בפרק 3 ה"ש 228.

86 ראו עניין **חוק נתוני תקשורת**, **לעיל** בפרק 2 ה"ש 69, פס' 17 לפסק דינה של הנשיאה ביניש. ראו גם בחלק 5.1 **לעיל**.

87 ראו בחלקים 3.3.4.8, 3.3.4.4 **לעיל**.

88 ראו בחלק 5.3 **לעיל**.

פסלות הראיות החלים עליהם; מידת ההגנה על גרעין הזכות לפרטיות הבאה לידי ביטוי בנהלים המפרידים בין תכנים שרלוונטיים למטרה שלשמה מופעל אמצעי המעקב ובין תכנים פרטיים שאינם קשורים בו, לרבות מידע פרטי שנאסף אגב אורחא על צדדים שלישיים;[89] וכן, ההגנות המיוחדות, אם ישנן, על יעדים מודיעיניים שנהנים מחסינות (דוגמת חברי פרלמנט ועיתונאים ובעלי מקצועות שעל סוד שיחם חלה חסינות סטטוטורית דוגמת עורכי דין, אנשי דת ופסיכולוגים).

כדי לבחון את מידתיותה של פרקטיקת מעקב או של האסדרה החלה עליה, יש לבחון את ההיבטים המצוינים לעיל ואת יחסי הגומלין ביניהם כמכלול. עם זאת יש הסבורים כי מידתיות אינה חזות הכול. מילר טוען שמבחני המידתיות שהפעיל בית המשפט הגרמני על חוק המשטרה הפדרלית (BKAG)[90] התמקדו בדקויות של כיולן של בקרות סטטוטוריות על אמצעי המעקב המקוון של ה־BKA, המגדירות לוחות זמנים לשימור נתונים ולביעורם, למשל, ולא בהגנה היקפית על הזכות לפרטיות כ"זכות להיעזב במנוחה" (the right to be left alone) באמצעות איסור קטגורי על פרקטיקות מסוימות של מעקב מקוון.[91]

89 ראו לדוגמה עניין **היועץ המשפטי לממשלה נ' נשיא בית־המשפט המחוזי בירושלים**, **לעיל** בפרק זה ה"ש 79.

90 Miller, **לעיל** בפרק 3 ה"ש 788, כן ראו חלק 3.4.3.5 **לעיל**.

91 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARVARD L.R. 193 (1890)

THE ISRAEL DEMOCRACY INSTITUTE

CYBER SECURITY RESEARCH CENTER

Policy Paper 123

REGULATION OF ONLINE SURVEILLANCE IN ISRAELI LAW AND COMPARATIVE LAW

Amir Cahane
with Yuval Shany

January 2019

Text Editors [Hebrew]: Yehudit Yadlin, Keren Gliklich
Series and Cover Design: Studio Tamar Bar Dayan
Typesetting: Nadav Shtechman Polischuk
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-247-6

No portion of this book may be reproduced, copied, photographed, recorded, translated, stored in a database, broadcast, or transmitted in any form or by any means, electronic, optical, mechanical, or otherwise. Commercial use in any form of the material contained in this book without the express written permission of the publisher is strictly forbidden.

Copyright © 2019 by the Israel Democracy Institute (RA) and The Federmann Cyber Security Center – Cyber Law Program
Printed in Israel

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-800; Fax: (972)-2-5300-867
E-mail: orders@idi.org.il
Website: en.idi.org.il

The Federmann Cyber Security Center – Cyber Law Program
The Faculty of Law, The Mount Scopus Campus Jerusalem
Box 80, ZIP Code: 9190501
E-mail: hcsrcl@mail.huji.ac.il
Website: https://csrcl.huji.ac.il

The views expressed in this policy paper do not necessarily reflect those of the Israel Democracy Institute or those of The Federmann Cyber Security Center – Cyber Law Program.

ABSTRACT

In 2013, Edward Snowden, who was employed by a National Security Agency (NSA) subcontractor, exposed documents that described the extent of online surveillance of communication networks conducted by American intelligence agencies, including of U.S. citizens. These revelations ignited a public debate about the agencies' surveillance practices and led to a number of statutory reforms. The exposure of the NSA's cooperation with its foreign counterparts opened the door to similar discussions in other countries concerning the desirable degree of their cooperation with foreign intelligence agencies, and the online methods of intelligence collection used by national intelligence agencies.

Online surveillance, or the surveillance of communication networks, is an intelligence activity designed to gather, retain, process, and analyze digital information from electronic communication networks—whether landline telephony networks, cellular communication networks, or computer data communication networks. Surveillance can be conducted in various ways, including interception and retrieval of information from the network or from front-end devices; collection of communications data (metadata) from communications service providers; and processing

open and hidden information, which can include data-mining techniques or machine learning. In an era in which a significant portion of human communication is conducted via electronic media, harnessing modern technology for the widescale collection, storage, and powerful statistical analysis of communications data can yield richer and more detailed intelligence information on surveillance targets than ever before.

However, alongside the advantages of intelligence gathered from online surveillance of communication networks, consideration must also be given to the significant violation of privacy inflicted on the subjects of surveillance. Those whose rights are harmed by the process include not only the intelligence targets themselves, but also those with whom they are in contact. Moreover, when bulk collection methods, which extract massive amounts of communications data and content from a main communications link rather than targeting a particular subject of surveillance are employed, the circle of those affected grows dramatically. The harm caused to individuals by online surveillance is not limited to infringement of their right to privacy. More broadly, the chilling effect caused by such surveillance may impair their general sense of freedom and their freedom of expression. When individuals are aware that they are, or may be, under surveillance, they are likely to modify their conduct accordingly.

Instances of technological surveillance by the state, other than those perceived as related to terror threats, prompt lively public debate in Israel. The "Big Brother Law" and the Biometric Database Law were discussed extensively in the media, and both found their way to the courts. By contrast, there has been almost no discussion of the rules regulating online surveillance for security purposes; in particular, there has been little discussion of existing legislation and its compatibility with today's social and technological realities and with human rights norms.

Main Conclusions

1. Lack of regulation addressing essential issues

Examination of Israeli legislation applying to online surveillance of communication networks shows that Israeli law suffers from under-regulation of a series of issues for which comparative law offers solutions. For example, Israeli law has no general ban on bulk collection of communications, not even a ban coupled with provisions for exceptional cases in which such activity would be permitted, subject to criteria of proportionality and absolute need. Similarly, the territorial application of Israeli online surveillance laws has not yet been regulated. Thus, the question remains of what is permitted or prohibited with respect to communications beyond the borders of the State of Israel, including in the Occupied Territories under Israel's control.

In addition, there are no provisions in Israeli law with respect to temporal limitations on the retention of communications data by communications providers, as can be found in legislation in the European Union, the United Kingdom, and Germany. This refers both to the communications content itself and to metadata, which consist of information about the communication other than its content, and from which (among other things) details of the parties to the communication, and of where and when it occurred, can be ascertained.

Similarly, data-mining activities carried out in this context—that is, using statistical techniques to analyze databases obtained by means of online surveillance, including cross-referencing them with other government databases—are barely addressed in Israeli legislation, in contrast to foreign law. (In certain cases, European law restricts decision-making based on data derived from automatic information-processing activities conducted without any human involvement, even in law enforcement contexts.)

It appears that in Israel, the possibility of requiring authorization for the collection of open-source intelligence information (OSINT) from telecommunications networks has yet to be explored. Due to its nature, traditional intelligence gathering, which relies on open sources of mass communication, does not require authorization. However, it may be now necessary to legislate provisions for the use of open-source intelligence gathering that also utilizes publicly available information on social media. This is because mass monitoring of the publicly available activities of social media users, including automated analysis of this information, may lead to actual privacy violations. While similar practices are used by private organizations for commercial gain, the state's exceptional police powers may lead to more severe violations of privacy and have more severe practical implications for the products of open-source intelligence.

2. Confidential rules and lack of transparency

Current Israeli legislation affords the government broad discretion in setting rules to regulate the Israel Security Agency's (the ISA or General Security Service) surveillance of communications networks, and to regulate the orders issued to telecommunication licensees (licensed to provide telecommunications services including telephony, internet, and cellular services) to assist the security forces (including the Israel Police). These rules, and a portion of the parliamentary and administrative oversight thereof and of online surveillance practices, are kept secret.

While this secrecy facilitates flexible interpretation and application of the law to meet pressing operational needs, the concealed nature of this interpretive flexibility—the soundness of which is not open to public scrutiny—means that it is liable to lead to breaches of human rights protections.

3. Partial judicial review

In Israel, judicial review of various authorizations for online surveillance is limited in scope. The law absolves security agencies seeking a wiretapping order from applying to the courts and settles for a permit granted in advance by the minister responsible; in urgent cases, retroactive ministerial authorization is allowed, as long as the use of these powers is reported to the attorney general. In urgent cases, the use of wiretapping even for crime prevention and detection purposes does not require authorization by a judicial order, except when its extension is needed. The Wiretap Act exempts certain types of wiretaps from requiring any authorization at all, and these may fall under the legal arrangement that allows collection of open information on the internet, including from social networks.

Judicial review in Israel with respect to obtaining and collecting metadata is limited to non-urgent cases in which the police require metadata for investigation purposes and law enforcement. There is no provision that prohibits the police from employing communications data collection technologies that do not involve requesting data from telecommunication licensees. Collection of communications data by the ISA (via direct interception, online access, or occasional request) is not subject to any judicial authorization. Moreover, the applicable legal provisions may be interpreted so that the mere collection of communications data does not require authorization from the head of the ISA, and such authorization is only necessary for using of the acquired information.

Although a review of comparative law reveals that in other countries as well there is no sweeping judicial review of online surveillance practices, it seems that the scope of judicial review elsewhere is broader than in Israel. For example, in Germany and the United States, collecting content and metadata for purposes of crime prevention and law enforcement is generally subject to judicial review. In these two countries, there are

also arrangements for the judicial or quasi-judicial review of wiretapping permits for national security purposes.

At the same time, judicial review is not the be-all and end-all means of oversight. An empirical examination of the data regarding Israel Police requests for orders under the Wiretap Act and the Criminal Procedure Law (Enforcement Powers—Communication Data) shows that the proportion of requests rejected by the court was lower than 0.5% throughout the entire period reported. A similarly low rejection rate can be found in the reports of the Administrative Office of the U.S. Courts regarding wiretapping requests for law enforcement and crime prevention purposes. We should be wary of concluding from these data that the mechanism of *a priori* judicial review of wiretapping requests is seemingly nothing more than a rubber stamp, since the court may approve requests while also imposing restrictions on the orders issued, and may issue orders that contain stricter procedures. Likewise, judicial review itself can create incentives for investigative bodies to filter out inappropriate requests before they are even submitted to the court. Still, the very small number of wiretapping or online surveillance requests that are rejected by the court calls into question the efficacy of judicial review and justifies an examination of the need to create additional guarantees.

In comparative law, mechanisms can be found that address the concern that judicial review of wiretapping orders will become automatic or will tend to systematically support the position of the investigative authorities. In UK law, for example, there are provisions that give detailed structure to the considerations that must be taken when applying judicial review; and in U.S. law, there are provisions enabling the court to appoint an *amicus curia* (an independent external individual) so that the application hearing for the order, which is usually held *ex parte*, becomes more adversarial.

4. An independent supervisory authority and parliamentary supervision

Judicial and quasi-judicial review of surveillance of communication networks is reactive, and its response is limited to specific applications or orders. This kind of oversight does not address cases in which the authorities avoided applying for the relevant orders due to the absence of a legal obligation to do so or due to a narrow interpretation of the existing statutory obligations. As a result, some legal systems have empowered administrative or quasi-judicial authorities to oversee the security bodies' online surveillance activity.

In Israel, the Privacy Protection Authority (formerly the Israel Law and Technology Authority—ILTA) is the regulatory, supervisory, and enforcement body under the Protection of Privacy Law, the Credit Data Law, and the Electronic Signature Law. However, due to exemptions in the Protection of Privacy Law, the Authority does not, in practice, oversee the online surveillance activity of security and law enforcement agencies.

Establishing an independent supervisory body—or alternatively, expanding the powers of the Privacy Protection Authority so that it can oversee the propriety of data processing activities, including collection and retention, carried out as part of the surveillance of communication networks for security or policing purposes—may serve to introduce an additional actor dedicated to protecting the privacy interests of those under surveillance. It is desirable that such a body, in addition to being independent, should have the full oversight powers required to fulfill its role, such as powers to investigate in response to complaints lodged or at its own initiative, and powers to provide advisory and professional guidance regarding aspects of privacy protection in relevant regulation. Alongside investigative and inquiry powers, it should be granted the ability to make rulings with practical implications for the practices being scrutinized.

Currently, the scope of the Knesset's parliamentary review of police and Israel Security Agency online surveillance practices is restricted to statutory reports pursuant to the Wiretap Act, some of which are delivered behind closed doors. Similar reports under the provisions of the Communications Data Act were submitted for a limited period by virtue of a temporary provision in the law, which has since expired. An attempt to obtain these secret reports through a request under the Freedom of Information Law was rejected by the Supreme Court which, in a side comment, recommended that the state disclose these details voluntarily and before they are leaked, in order to secure public trust.

Recommendations

1. Issues lacking regulation under Israeli law

(1) The extent of the powers granted each of the security and law enforcement bodies. Regulation of the extent of the various powers of the police, the Israel Security Agency, the Military Intelligence Directorate, the Mossad, and other investigatory bodies should refer to the practices in which they are allowed to engage, the scope of collection permitted, the controls to be put in place, and the territorial application of these powers.

(2) Bulk collection. Israeli law should implement a general ban on bulk collection, unless strictly necessary for attaining narrow and detailed objectives, and subject to procedures that guarantee that the violation of rights is kept to the bare minimum.

(3) Data retention. Israeli law should apply provisions regarding the maximum period for which telecom providers can retain data. The authorities' ability to order providers to deviate from these provisions and retain data for a longer period would be subject to judicial order, limited to the attainment of narrow and detailed objectives, and subject

to procedures that guarantee that the violation of rights is kept to a minimum.

(**4**) **Data-mining and collection of open-source information (OSINT)**. Legislation should permit and prohibit actions related to cross-referencing of various databases, the different uses that can be made of the products of statistical processing, and the extent of automation and lack of human involvement in the process to be allowed. With respect to OSINT practices in social networks, the powers of the authorities to act in this arena should be defined, and limits placed on collection practices that are not absolutely passive (such as the use of fictional profiles to obtain access to information that is not entirely public).

(**5**) **Obtaining information from global communications platform providers**. Procedures for obtaining information from online communications platform providers, such as Facebook and Google, should be regulated by law. They should be limited to narrow objectives involving serious crime and national security and subjected to a test of near certainty and to judicial review.

(**6**) **Intercepting communications data**. Similar to the general ban on wiretapping, a general prohibition should apply to active interception of communications data—as opposed to the procurement of non-real-time data under the terms of the Criminal Procedure Law (Enforcement Powers—Communication Data), or according to the rules promulgated pursuant to the Israeli Security Agency Law. Regulations should be created to provide for cases in which said interception would be permitted, similar to the arrangements in the Wiretap Act.

2. Increasing transparency

(**1**) The veil of secrecy should be removed from the rules that govern the methods used by the Israeli Security Agency to obtain communications data from telecom providers, and the annual reports of the use of these

methods should be publicly disseminated to the extent possible. Similarly, the annual reports of the ISA's use of its powers under the Wiretap Act should also be published, to the extent possible.

3. Expansion of judicial review of online surveillance practices

(**1**) The scope of judicial review of online state surveillance should be extended to wiretapping carried out by the Israeli Security Agency and the Military Intelligence Directorate for security purposes, and to every request for communications data including urgent requests.

(**2**) The existing judicial review mechanism should be strengthened. Judicial discretion in granting orders may include instructions to consider alternatives with lesser violations of privacy, as well as restrictive procedures intended to ensure that no use of the information will be made beyond that which is required.

(**3**) It is possible to create an adversarial process by means of which public representatives, special advocates, or *amici curiae* could protect the interests of both public privacy and the privacy of the subject of the surveillance. Strengthening the adversarial basis of the process could be achieved by granting *locus standi* to communications providers, and by recognizing the surveillance subjects' and third parties' notification rights as a relative right subject to security considerations, which would enable compensation claims to be filed after the fact.

4. An independent supervisory authority

(**1**) An independent supervisory authority should be established, to review government authorities' ongoing online surveillance activities, to assess compliance with the provisions of orders, and to advise and provide professional guidance regarding the privacy protection aspects of relevant regulation.

(**2**) An alternative to the establishment of such a body would be an expansion of the Privacy Protection Authority's (formerly ILTA) powers, granting it supervisory powers over privacy protection in the online surveillance activities of the security and law enforcement authorities.

(**3**) Another alternative is the establishment of an ombudsman for privacy issues in online surveillance—an independent, impartial body with reactive powers to investigate complaints, find solutions without the need for extensive formalities, and periodically publicize its findings while keeping the complainants' identities secret.

5. Parliamentary supervision

(**1**) The heads of the security services should be obligated to report annually to the Knesset's Constitution, Law and Justice Committee and the Foreign Affairs and Defense Committee regarding the number of wiretaps carried out for state security purposes. The level of detail reported should be identical to that reported annually by the Ministry of Public Security on the exercise of these powers by the Israel Police.

(**2**) The temporary order contained in the Criminal Procedure Law (Enforcement Powers—Communication Data) should become permanent and require the Israel Police to report annually on their use of the powers granted by this law.

מהם הדינים החלים בישראל על רשויות המדינה כשהן בולשות אחרי הפעילות המקוונת שלנו; האם דינים אלו נותנים מענה ראוי להתפתחויות הטכנולוגיות של השנים האחרונות; האם הפרטיות שלנו מוגנת די הצורך; והאם ישנן תובנות עדכניות בדין הזר שרצוי לתת עליהן את הדעת?

חשיפותיו של אדוארד סנודן על היקף המעקב המקוון שסוכנויות הביון של ארצות הברית מקיימות ברשתות תקשורת, בין השאר אחר אזרחיה שלה, פתחו בשנת 2013 דיון ציבורי רחב היקף וחוצה מדינות. הוראות החוק האמריקאי והחקיקה האירופית שהסדירו פעילות זו נבחנו מחדש ועברו רפורמה. ואולם דיון ציבורי ביתרונות ובחסרונות של המעקב המקוון, שמעלה תובנות באשר לעיצובן הרצוי של האסדרה ושל הבקרה המשפטית החלות עליו, פסח כמעט לחלוטין על ישראל.

מטרת המחקר המובא כאן לבחון את ההסדרים בדין הישראלי החלים על פעילות של מעקב מקוון מטעם רשויות המדינה. סקירה השוואתית של הסדרים משפטיים בתחום במדינות זרות – בארצות הברית, באיחוד האירופי, בבריטניה, בגרמניה ובהודו – מלמדת על היבטים חסרים בדין הישראלי ועל היבטים הטעונים תיקון והשלמה.

עו״ד עמיר כהנא הוא חוקר בתוכנית לביטחון לאומי ודמוקרטיה במכון הישראלי לדמוקרטיה וחוקר אורח בתוכנית לסייבר ומשפט במרכז פדרמן לחקר הסייבר באוניברסיטה העברית בירושלים. בוגר תואר ראשון במשפטים מהמרכז הבינתחומי הרצליה ותואר שני במשפטים מאוניברסיטת קיימברידג׳.
פרופ׳ יובל שני הוא סגן נשיא למחקר במכון הישראלי לדמוקרטיה וחוקר במרכז לערכים ולמוסדות דמוקרטיים ובמרכז לביטחון ודמוקרטיה. בעבר היה דיקן הפקולטה למשפטים באוניברסיטה העברית בירושלים וכיום משמש בה ראש תוכנית לסייבר ומשפט במרכז פדרמן לחקר הסייבר ומופקד על הקתדרה למשפט בינלאומי פומבי ע״ש הרש לאוטרפרכט (Hersch Lauterpach). פרופ׳ שני חבר בוועדת זכויות האדם של האו״ם מאז 2013. ב־2018 הוא מונה ליו״ר הוועדה.

מחיר מומלץ: 45₪

ינואר 2019

מסת״ב:
978–965–519–247–6

0 4500001191 5
דאנאקוד 450-1191

www.idi.org.il