רותם מדזיני*

משטרי הגנת המידע באירופה: מעקרונות לתהליכים

א. מבוא

בשנת 2016 התקבלה באיחוד האירופי מסגרת חקיקתית מקיפה להגנת מידע ובמרכזה General Data Protection Regulation (להלן: GDPR), שנכנסה לתוקף בשנת 2018 והחליפה את דירקטיבת הגנת המידע (להלן: הדירקטיבה) משנת 1995.[1] המסגרת החדשה הביאה שינוי של ממש בכל הנהוג והמקובל במשטרים להגנת מידע ובמדיניות האינטרנט באירופה, ודרכם – במדיניות להגנת מידע ואינטרנט ברחבי העולם. השינוי שקידם האיחוד האירופי מחייב יישום של המסגרת החקיקתית בשלושה מישורים בו־זמנית: במישור האירופי העל־מדינתי,

* תלמיד מחקר לתואר שלישי, בית הספר לממשל ולמדיניות על שם פדרמן, הפקולטה למדעי החברה, האוניברסיטה העברית. עמית מחקר במרכז פדרמן לחקר הסייבר – תכנית סייבר ומשפט באוניברסיטה העברית וחוקר אורח ב־Antwerp Consortium on the Organization of Rulemaking and Multi-level Governance in Europe (ACTORE) באוניברסיטת אנטוורפן, בלגיה. עבודה זו נעשתה בתמיכת מרכז פדרמן לחקר הסייבר באוניברסיטה העברית ומערך הסייבר הלאומי בישראל.

1 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (להלן: GDPR). בצד GDPR אפשר למצוא רגולציות ודירקטיבות נוספות שיחד מהוות מסגרת חקיקתית רחבה יותר. כך, למשל, עם ה־GDPR אושרה דירקטיבה להגנת מידע ברשויות אכיפת מידע, ורגולציה חדשה בנוגע להגנת מידע בתקשורת מקוונת (e-Privacy) נמצאת בתהליכי חקיקה. ראו Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89; *Proposal for a Regulation of the European Paprliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC*, COM (2017) 010 final (Jan. 1, 2017). נוסף על כך אפשר להניח שבדומה לדירקטיבת הגנת המידע משנת 1995, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (להלן: דירקטיבת הגנת המידע) חקיקות עתידיות יפנו ל־GDPR כשהן יבקשו להתייחס לסוגיה של הגנת מידע בזמן שחקיקות ישנות כנראה יפורשו מעכשיו לפי ה־GDPR. לפיכך, ה־GDPR היא רק המרכז של המשטר החדש אך לא מהווה את כולו.

במישור המדינתי בקרב מדינות האיחוד ובמישור הארגוני. במישור העל־מדינתי, המסגרת החקיקתית החדשה כוללת שינויים מבניים משמעותיים בקרב המוסדות הפועלים כגורמי אכיפה וקביעת מדיניות. במיוחד יש לציין את הפיכתו של Article 29 Working Party (להלן: A 29 WP) – גוף מקצועי שבו היו חברים נציגים של כל מדינות האיחוד וייעץ במסגרת המשטר הישן בנוגע למדיניות הגנת המידע באיחוד האירופי – למוסד בשם European Data Protection Board, שביכולתו ליישב סכסוכים ולאכוף החלטות שאינן מתיישבות עם מדיניות הגנת מידע הכלל־אירופית.[2] במישור המדינתי, המסגרת החקיקתית החדשה מאפשרת למדינות החברות ליישם מדיניות מקומית להגנת מידע בסוגיות מוגדרות, לרוב אגב קביעת כלל נוקשה יותר מזה הקבוע בחקיקה האירופית. כך, למשל, מדינות רשאיות להוריד את גיל מתן ההסכמה של ילדים לקבלת שירותים המבוססים על חברת המידע ללא הסכמת הוריהם מגיל 16 עד לגיל 13, והן יכולות להוסיף תנאים והגבלות נוספות על עיבוד מידע אישי.[3] במישור הארגוני, המסגרת החקיקתית החדשה תובעת יישום של עקרונות וכללים שרובם התקיימו כבר קודם כפרקטיקות של אסדרה עצמית לא מחייבת; למשל: ביצוע של סקרי סיכונים, מינוי ממונים על הגנת מידע, אימוץ של מדיניות לאבטחת מידע ויישום של קודי התנהגות בארגון.

במאמר זה אטען שהמסגרת החקיקתית החדשה אינה רק אשרור של פרקטיקות קיימות והכנסתן לספר החוקים האירופי, אלא מעבר של האיחוד האירופי ממשטר הגנת מידע ישן, המבוסס על אסדרת עקרונות רחבים, לעבר משטר הגנת מידע חדש, המבוסס על כלי מדיניות תהליכיים. כלים אלו מצטרפים אל עקרון האחריותיות (accountability) שנקבע ב־GDPR כעיקרון יסודי.[4] כלי מדיניות אלה מהווים אסטרטגיה אסדרתית שלפיה מנהלים בארגונים נדרשים להכין תכניות העומדות בקריטריונים שנועדו לקדם מטרה חברתית – ובהקשר של מאמר זה: הגנה על פרטיות. הקריטריונים, למשל, יכולים לבקש זיהוי סיכונים, הנדסת פרטיות, תהליכי פיקוח, הכשרות עובדים ועוד. אבקש לזהות את כלי המדיניות הללו ולסדרם בקטגוריות של כלי מדיניות, וכך יתאפשר לזהות את הרכבם. זיהוי ההרכב יאפשר להבליט את יחסי הכוחות בין המאסדרים (regulators), מושאי האסדרה ומוטבי האסדרה (מושאי המידע) שמשטר הגנת המידע החדש מבקש לקדם.

המעבר ממשטר הגנת המידע הישן למשטר החדש אינו צריך להיעשות כלאחר יד. ראשית, מאז חקיקת הדירקטיבה שהייתה לבו של המשטר הישן, התפיסה האירופית הייתה

2 בין היתר, ה־GDPR מעניקה סמכויות חדשות למוסדות קיימים, אך גם משנה את מאזן הכוחות ביניהם. מחד גיסא, ה־GDPR מעניקה – ישירות – סמכויות לרשויות האכיפה והפיקוח (Data Protection Supervisory Authorities); מאידך גיסא, בעוד המשטר החדש מרכז את האכיפה לידי רשות אכיפה אחת עבור כל האיחוד האירופי, שנקבעת לפי מקום מושבו של הארגון, ה־European Data Protection Board הוקם כדי להכפיף את הרשויות ברמת המדינה לאינטרסים על־מדינתיים. ראו פרק 7 ל־GDPR, ובמיוחד את חלק 3 העוסק בהקמת ה־European Data Protection Board (EDPB) ובתפקידיו.

3 ראו ס׳ 8.1 ו־9.4 ל־GDPR.

4 ראו ס׳ 5.2 ל־GDPR, המגדיר את עקרון האחריותיות כחובתו של מנהל המאגר לעקרונות עיבוד המידע המוגדרים בסעיף 5.1 ל־GDPR. עקרון האחריותיות כולל את היכולת של מנהל המאגר להראות כי אכן עמד בעקרונות של עיבוד מידע.

שאין לקבל משטרי הגנת מידע מדינתיים שסטנדרט ההגנה שלהם למידע אישי נמוך מזה שבדירקטיבה. באמצעות הדירקטיבה ביקש האיחוד האירופי לקדם כללים זהים בנוגע לאיסוף, לעיבוד ולהעברה של מידע בין מדינות, תוך הקמת רשויות ייעודיות לפיקוח ואכיפה של אותם כללים. האיחוד ומוסדותיו נדרשו לפעול ברמה הבין־לאומית, הן כדי למנוע היווצרות של מדינות מקלט למאגרי מידע[5] והן כדי להסדיר העברת מידע למדינות מחוץ לאיחוד ("מדינות שלישיות") בהיעדר הגנה מתאימה. פעילות בין־לאומית זו במסגרת המשטר הישן הובילה לכך שהשינויים בפרקטיקות האסדרה – שהאיחוד מבקש לקדם במסגרת משטר הגנת המידע החדש – רלוונטיות גם למדינות שאינן אירופיות, וכן לעסקים שפועלים באותן מדינות ומבקשים לאסוף ולעבד מידע אישי אירופי, אף שה־GDPR אינה חלה במדינות אלה במישרין.[6]

שנית, בעידן של נתוני עתק (big data) והאינטרנט של הדברים (Internet of Things), כניסתו לתוקף של משטר הגנת המידע החדש משליכה על תפקידה ועל יישומה של הזכות לפרטיות במסגרת השיח הציבורי הגלובלי בנושא חברת המעקב. בהתחשב באתגרים שהטכנולוגיות הללו מציבות לפני הזכות לפרטיות, חשוב לזהות את כלי המדיניות שמסדירים פרטיות ולאפיינם. זיהוי ואפיון של כלי המדיניות ושל התהליכים מאפשרים – ביתר שאת – לזהות את יחסי הכוחות שמשטר האסדרה החדש ממסד. בהקשר הספציפי של הזכות לפרטיות, בשל חשיבותה של הזכות בהתמודדות עם אפשרות הפגיעה של טכנולוגיות המידע, זיהוי ואפיון כאמור יסייעו להבין כיצד קובעי המדיניות מצפים מכל שחקן הכפוף למשטר לפעול, וכשאלו לא ביצעו את שנדרש מהם – כיצד קובעי המדיניות של המשטר מאפשרים ליתר השחקנים להגיב להתנהגות זו.

בשני החלקים הבאים אעסוק באסדרה במובנה הרחב. בחלק הבא אעסוק בכלי מדיניות – אגדיר אותם ואדון בתפיסות שונות של תפקידם; בחלק ג אדון בשיטות אסדרה שונות העומדות לפני קובעי מדיניות המבקשים להשפיע על ההתנהגות של מושאי האסדרה. בחלק ד אתייחס למשטר הגנת המידע האירופי כמקרה מבחן, תוך סקירה של התפתחות חקיקות הגנת מידע – החל בחוקים הראשוניים בשנות השבעים של המאה הקודמת, דרך הדירקטיבה האירופית והשלכותיה הבין־לאומית ועד לנסיבות שהובילו לחקיקת ה־GDPR. בחלק ה אסקור את השינויים העיקריים שהביאה ה־GDPR למשטר הגנת המידע האירופי. לבסוף אציג ניתוח של הקטגוריות של כלי המדיניות שה־GDPR מתווה לצורך הבניית יחסי הכוחות בין השחקנים במשטר הגנת המידע האירופי החדש. לאחר ההתייחסות לשש הקטגוריות הללו, אסכם.

5 Abraham L. Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive,* 62 Int'l. Org. 103, 109 (2008).

6 ראו פרק 5 ל־GDPR, ובמיוחד ס' 45, העוסק בסמכות הבלעדית של הנציבות האירופית לבחון ולאשר כי רמת ההגנה במדינה לא־אירופית, חלק מסוים או סקטור עסקי במדינה לא־אירופית, או ארגון בין־לאומי תואמים את הדין האירופי להגנת מידע (adequacy decision). תחת ה־GDPR, ובשונה מהדירקטיבה, הנציבות נדרשת לבחון את החלטת התאימות לפחות כל ארבע שנים, ובמקרה של הפרה – לפתוח במשא ומתן לתקן את הפער. בהיעדר קביעה של תאימות כללית למדינה או חלקה, על ארגונים הרוצים להעביר מידע לאמץ אחד מההסדרים הספציפיים שמופיעים בפרק 5.

ב. בקטגוריות ותפיסות של כלי מדיניות

כלי מדיניות הם חלק מהותי בשיח של מדיניות ציבורית. בבסיסם הם מערכת של טכניקות שבהן קובעי מדיניות יכולים להשתמש לצורך יישום המדיניות שהם רוצים לקדם.[7] לפיכך, כלי מדיניות הם אחת מיחידות הבסיס לניתוח מדיניות ואמצעי מרכזי לשינוי ההתנהגות שהמדיניות מבקשת לקדם. על פי רוב כלים אלה כוללים שני רכיבים: רכיב הפעולה, הנושא אמירה על ההתנהגות הרצויה או הלא־רצויה שקובע המדיניות מעוניין, בהתאמה, לקדם או להגביל.[8] לעומתו, רכיב הכוח עוסק בסוג ובעוצמת ההגבלה שבה מעוניינים להשתמש לצורך שינוי ההתנהגות.[9] הנה דוגמה מחיי היום־יום: בעוד שרכיב הפעולה יאסור על חנייה שלא במקום חניה מוסדר, רכיב הכוח יכול להתבטא בדוח או בגרירה של המכונית.

אפשר לזהות בספרות כמה גישות לכלי מדיניות. לפי גישה אחת, קובעי המדיניות מעוניינים להשיג את מטרת המדיניות ולשם כך הם משתמשים בכלי מדיניות. בשלב הבא הם מכיילים את כלי המדיניות הנבחר לפי הנסיבות והלחצים הפוליטיים.[10] חוקרים המתבססים, בין היתר, על כתיבתו של אמיתי עציוני (Etzioni) התייחסו לדרך הבחירה של כלי מדיניות באופן זה.[11] לגישתם אפשר לזהות שלושה רכיבים של כלי מדיניות שקובעי מדיניות יכולים לבחור להפעיל: מקלות, גזרים ודרשות.[12] בשונה, יש חוקרים שלתפיסתם כלי המדיניות העומדים לרשות קובעי המדיניות הם למעשה תחליפיים זה לזה,[13] כלומר שאפשר להציבם

---

7 JOHN MCCORMICK, CARROTS, STICKS, AND SERMONS: POLICY INSTRUMENTS AND THEIR EVALUATION ((Marie-Louise-Bemelmans-Videc et al. eds., 1st ed., 1998); Michael Howlett, *Policy Instruments, Policy Styles, and Policy Implementation: National Approaches to Theories of Instrument Choice*, 19 POL'Y STUD. J. 1 (1991); Pierre Lascoumes & Patrick Le Gales, *Introduction: Understanding Public Policy through Its Instruments? From the Nature of Instruments to the Sociology of Public Policy Instrumentation*, 20 GOVERNANCE 1 (2007).

8 Kenneth Woodside, *Policy Instruments and the Study of Public Policy,* 19 CAN. J. POL. SCL. 775 (1986).

9 MCCORMICK, לעיל ה"ש 7.

10 Michael Howlett, *Governance Modeas, Policy Regimes and Operational Plans: A Multi-Level Nested Model of Policy Instrument Choice and Policy Design,* 42 POL'Y. SCI. 73 (2009).

11 לפי אמיתי עציוני יש שלושה סוגים של כוח שהם רלוונטיים לכלי מדיניות. כוח אוכף (Coercive power), הכולל את היישום או האיום ביישום של סנקציות פיזיות; כוח תמורתי (Remunerative power), הכולל שליטה על משאבים; וכוח נורמטיבי (Normative power), הכולל קידום של סמלים, השפעה על מדיה המונית ומתן פרסים וסמלים על ידי מנהיגים. AMITAI ETZIONI, A COMPARATIVE ANALYSIS OF COMPLEX ORGANIZATIONS: ON POWER, INVOLVEMENT, AND THEIR CORRELATES (2nd ed., 1975).

12 MCCORMICK, לעיל ה"ש 7. ראו גם COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2nd ed. 2006); Theodore J. Lowi, *Four Systems of Policy, Politics, and Choice*, 32 PUB. ADM. REV. 298 (1972).

13 כך, למשל, מייקל היולט (Howlett) מפנה לדוגמת המודל של רוברט דאל (Dahl) וצ'רלס לינדבלום (Lindblom). החוקרים מציעים להבחין בין כמה שאלות: מי בעלי הכלים, מה טיב ההשפעה

לאורך צירים וקריטריונים שונים, ובהתאם למטרה קובעי המדיניות יכולים לנוע על הצירים ולבחור אילו מאפיינים ירכיבו את כלי המדיניות המתאים. אם כלי המדיניות הנבחר נמצא חלש או חזק מדי לנסיבות האסדרה ולמטרותיה, אפשר לחזור לצירים וליישם כלי מדיניות עם מאפיינים אחרים.[14]

גישה נוספת לכלי מדיניות הציע כריסטופר הוד (Hood). לפי גישתו, אפשר לסווג את כלי המדיניות למשפחות. סיווג זה מסייע להבין כיצד ממשלות מיישמות מדיניות ומה הן עושות הלכה למעשה.[15] בהתאם למודל שפיתח הוד, פעילות הממשלה היא הדרך שבה הממשלה מיישמת ומשיגה מידע, וכתוצאה – הדרך שבה היא פועלת על בסיס המידע.[16] מודל זה מתייחס לארבעה משאבים שבהם המדינה יכולה להשתמש: מידע (Nodality), סמכות (Authority), כספים (Treasure) וכוח מארגן (Organization), והוא נקרא בהתאם NATO.[17] כך, בהקשר של אסדרת מידע, המדינה יכולה לקבל מידע בשל מרכזיותה ברשת שבה המידע זורם, בשל סמכותה לדרוש מידע, בשל בחירתה לקנות אותו או תוך שימוש בכוחה כדי להשיג את המידע במישרין. הנחת המוצא של הוד היא שכאשר קובעי מדיניות נתקלים בבעיה חדשה – בין בנושאי פרטיות ובין בנושאים אחרים – קבוצת כלי המדיניות הקיימת שבה הם יכולים למצוא פתרונות היא קבוצה סגורה. במילים אחרות, אין בנמצא כלי מדיניות שלא היה קיים או לא היה מוכר לקובעי המדיניות. אפשר להסיק מגישה זו שאם

הממשלתית, עד כמה השליטה השלטונית ישירה (או עקיפה), עד כמה החברות בארגונים היא רשות (או חובה) והאם רשויות נהנות מעצמאות או שהן כפופות למקבלי האחריות. דוגמאות נוספות לקטגוריות אפשריות אפשר למצוא אצל Howlett, *Policy Instruments, Policy Styles* לעיל ה"ש 7. למודל של דאל ולינדבלום ראו Robert A. Dahl & Charles E. Lindblom, *Politics, Economics, and Welfare* (1953).

14 Stephen H. Linder & Guy B. Peters, *Instruments of Government: Perceptions and Contexts*, 9 J. Pub. Policy 35 (1989); Guy B. Peters, *Policy Instruments and Public Management: Bridging the Gaps*, 10 J. Pub. Adm. Res. Theor. 35 (2000).

15 Christopher C. Hood, The Tools of Government (1986); בהמשך, בספרם משנת 2007, חזר כריסטופר הוד עם הלן מרג׳טס (Margetts) על המודל תוך יישומו לעידן הדיגיטלי. ראו Christopher C. Hood & Helen Z. Margetts, The Tools of Government in the Digital Age (2007).

16 הצעד התאורטי המשמעותי של מודל NATO נובע מההבחנה בין כלי מדיניות שנועדו לאסוף מידע מכל סוג (Detectors) לבין הכלים שבהם הממשלה יכולה להשתמש כדי להשפיע על הנעשה בעולם (Effectors). ראו Hood, The Tools of Government, שם.

17 כלי המידע (Nodality) עוסקים בהיבט של היות הממשלה מרכז או הצטלבות (Node) של רשת מידע. כתוצאה מהשימוש בכלים הללו, הממשלה יכולה לקבל מידע והיא יכולה גם לספק מידע. כלי הסמכות (Authority) נותנים בידי הממשלה כוח משפטי או רשמי לפעול, לדרוש, לאסור פעילות, להבטיח ולשפוט. כלי האוצר (Treasure) עוסקים במטבעות או במשאבים אחרים בני־חליפין. הכוח הארגוני (Organization) מאפשר לממשלה להפעיל את אנשיה (חיילים או בירוקרטיה) ואת משאביה (אדמה, בניינים, ציוד ומחשבים) במישרין. שלוש הקטגוריות הראשונות תואמות את הקטגוריות שהציע אמיתי עציוני ואת הקטגוריות שהציעו Bemelman-Videc ואחרים. ראו McCormick, לעיל ה"ש 7; וגם Hood, The Tools of Government, שם.

יש שונות ביישום של מדיניות בתחום מסוים בין מדינות, אזי ייתכן ששחקנים פוליטיים השפיעו על ההבדלים במדיניות שנבחרה בסופו של התהליך הפוליטי.[18]

לבסוף, יש גישות הרואות כלי מדיניות כחלק משיטה אסדרתית רחבה יותר, בעלת פוליטיקה עצמאית, ולא רק אמצעי להשגת מטרה.[19] לפי לסטר סלמון (Salamon) יש לכלי המדיניות כמה מאפיינים: ראשית, הם ניתנים לבידול זה מזה; שנית, יש לכל אחד מהם עיצוב שונה; שלישית, הם מעצבים התנהגות קולקטיבית כתגובה לבעיה חברתית או להגבלות רגולטוריות.[20] בהתאם להגדרה זו, כלי המדיניות קובעים כללים, מכתיבים התנהגות ומסדירים אחריות בין שחקנים במרחב הרגולטורי.[21] בהתחשב בכך שכלי המדיניות שייבחר ימסד התנהגויות מסוימות באמצעות חוקים, תקנות והנחיות, הרי שבצד השיח הפוליטי על אודות המדיניות הציבורית הרצויה, גם השיח על אודות כלי המדיניות עצמם הוא במה לשיח פוליטי בין המשתתפים בדיון על אודות המדיניות הרגולטורית.[22] מבחינה זו, תמהיל כלי המדיניות שייבחר על ידי קובעי המדיניות, כמו במקרה של הגנת מידע, יסדיר לעתיד את קשרי הגומלין ואת יחסי הכוחות בין השחקנים, יקבע מי יהיה מעורב באסדרה ומי לא יהיה מעורב בה וימסד את תפקידו של כל שחקן במרחב הרגולטורי. לעתים קובעי המדיניות עושים זאת בדרך של הבניית שיטה לאסדרת שוק. עמידה על שיטות אסדרה וכלי המדיניות שבבסיסן תאפשר בהמשך, בין היתר, לשייך את כלי המדיניות לשחקנים שהם באים להעצים.

ג. שיטות אסדרה וכלי מדיניות

1. אסדרה מנחה

השיח בתחום המדיניות הציבורית על אודות שיטות אסדרה מבחין בין שלושה שלבים עיקריים להתערבות: התערבות בשלב התכנון של תהליך הייצור, התערבות בשלב ביצוע

18 Colin J. Bennett, Regulating Privacy: data protection and public policy in Europe and the United States 7 (1992); **ראו גם** Hood, The Tools of Government, **שם**.

19 המצדדים בגישת כלי המדיניות כאמצעי להשגת המטרה יראו גישה זו כאחד השלבים לעיצוב מדיניות ציבורית על ידי קובעי המדיניות, במיוחד כחלק מהליך הכיול של כלי המדיניות למטרת המדיניות. **ראו, למשל,** Michael Howlett, *Beyond Legalism? Policy Ideas, Implementation Styles and Emulation-Based Convergence in Canadian and U.S. Environmental Policy*, 20 J. Pub. Pol'y. 305 (2000).

20 **לסטר סלמון הגדיר כלי מדיניות כך:** "Identifiable method through which collective action is structured to address a public problem." **ראו** Lester M. Salamon, *The New Governance and the Tools of Public Action: An Introduction*, 28 Fordham Urban L.J. 1611, 1641-42 (2001).

21 **שם;** Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 Law & Soc'y Rev. 691 (2003); Sharon Gilad, *It Runs in the Family: Meta-Regulation and its Siblings*, 4 Regul. & Gov. 485 (2010).

22 Salamon, **לעיל ה"ש 20.**

התהליך והתערבות בשלב התוצר של התהליך.[23] התערבות בכל אחד מהשלבים תשפיע על התוצר החברתי ועל דרך ההתנהגות של השחקנים המעורבים. הפרקטיקה המוכרת ביותר עוסקת בהתערבות בשלב הביצוע של התהליך מושא האסדרה. על פי רוב, פרקטיקה זו מכונה אסדרה מנחה או אסדרה של ציווי ושליטה (command and control regulation). על פי שיטת אסדרה זו, קובע המדיניות – או הגורם המאסדר, אם הוסמך לכך – מכתיבים (באמצעות כללים והנחיות) בדיוק איך להתנהג, אילו טכנולוגיות לאמץ ואלו פרוצדורות ליישם. לשיטה של אסדרה מנחה יתרונות וחסרונות בולטים. מחד גיסא, היא מחייבת רמה גבוהה מאוד של דיוק משום שהכלל המנחה מגדיר את גבולות האסדרה בין המאסדר לבין מושא האסדרה;[24] מאידך גיסא, האסדרה המנחה כוללת גם מספר רב של קשיים ובהם, למשל, משאבים מוגבלים. כמו כן, כשמה, האסדרה המנחה מניחה כי יש להכתיב למושאי האסדרה כיצד לנהוג – אך אם ההנחיה אינה די מדויקת או אינה בתוקף בשל שינוי בנסיבות, היא עלולה ליצור חוסר בהירות. זה, בתורו, עלול להוביל להבדלים בפרשנות שתקבל ההנחיה אצל כל אחד מהגורמים הרלוונטיים – המאסדר, השחקנים בשוק ולעתים גם מערכת המשפט. מצב זה אינו רצוי בשיטה המבוססת על הנחה שקובעי המדיניות מכתיבים כיצד יש לנהוג כדי לצמצם חוסר ודאות. לבסוף, פערים בהנחיה בין גורם האסדרה לבין מושאי האסדרה או המציאות בשטח יכולים לעורר ביקורת ציבורית על איכות ההנחיה או על דרך עבודתו של המאסדר.[25]

2. אסדרת ביצועים

הקטגוריה השנייה של שיטות מדיניות מכונה אסדרת ביצועים (performance-based regulation). שיטה זו עוסקת בתוצרים של הפעילות המוסדרת. בשונה מאסדרה מנחה, אסדרת ביצועים אינה מציינת את ההתנהגות או את הטכנולוגיות שיש לאמץ; במקום זאת, היא עוסקת באמירות בנוגע לתוצרים של התהליכים או בנוגע למדדים שיש להגיע אליהם או להימנע מהם.[26] כוחה של שיטת אסדרה זו נובע מכך ששיקול הדעת נשאר אצל השחקנים בשוק. אלה יכולים לפתח טכנולוגיות חדשות או לבחור טכניקות שונות ובלבד שיובילו לעמידה ביעדים שהוגדרו מראש על ידי קובעי המדיניות.[27]

מטבע הדברים, גם לאסדרת ביצועים יש יתרונות וחסרונות לתחום המוסדר. מצד היתרונות, כלל השחקנים במרחב המדיניות עסוקים, יחד ולחוד, בניסיון לעמוד במטרות המדיניות. יתר על כן: מושאי האסדרה מקבלים שיקול דעת להחליט כיצד לעמוד ביעדי

23 Coglianese & Lazer, **לעיל ה"ש 21**; David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 Ga. St. U. L. Rev. 287 (2013).

24 Peter J. May, *Regulatory Regimes and Accountability*, 1 Regul. Gov. 8, 9 (2007).

25 Cary Coglianese, *Performance-Based Regulation: Concepts and Challenges*, *in* Comparative Law and Regulation: Understanding the Global Regulatory Process 403 (Francesca Bignami & David Zaring eds., 2016).

26 Coglianese & Lazer, **לעיל ה"ש 21**.

27 Cary Coglianese, Jennifer Nash & Todd Olmstead, *Performance-based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection*, 55 Admin. L. Rev. 705 (2003); **ראו גם** May, **לעיל ה"ש 24**.

הביצוע שנקבעו בדרישות המדיניות, למשל באמצעות פיתוח של טכנולוגיות, פרקטיקות או מתודולוגיות חדשות. כמו כן, השוק מקבל תמריץ חיצוני קבוע לחדשנות מבחינת היצע הפתרונות הקיימים. האידאל הוא שכל פתרון חדש יהיה לרוב יעיל ואפקטיבי יותר. לבסוף, במקום שהמאסדרים יידרשו לכתוב כללים מנחים, הם נדרשים למדוד תוצרים ולאשר תהליכים קיימים.[28]

הבחירה במדיניות של אסדרת ביצועים צריכה להכיר גם בחסרונותיה. ראשית, אסדרת ביצועים דורשת העברה קבועה של מידע אמין ורלוונטי אל המאסדר, במיוחד כדי לוודא שאין חריגה ממסגרות הביצועים ומהמדדים שנקבעו.[29] צעד זה אינו תמיד פשוט למאסדר, משום שעליו להעריך באופן ביקורתי את הסיכונים שהעריך קודם לכן מושא האסדרה, שלפי התפיסה של אסדרת הביצועים הוא האחראי על הביצוע בשטח.[30] במצבים של חוסר מידע ומשאבים אצל המאסדר, חישוב זה נהפך למורכב אף יותר. נוסף על כך, ולעתים רבות, הדרישה לעמוד ביעדים יכולה להיות מורכבת גם עבור ארגונים קטנים ובינוניים. מעבר למגבלת כוח האדם (בהשוואה לארגונים גדולים), לארגונים קטנים ובינוניים לא תמיד יש די משאבים לפיתוח הטכנולוגיות והפרקטיקות הנדרשות כדי לעמוד בתחרות וביעדי הביצוע בעלות נמוכה. המשמעות של ההתייעלות הטכנולוגית, או של אימוץ הפרקטיקות החדשות, היא חיסכון בעלויות העמידה ביעדים, ולעתים זו מנת חלקם של ארגונים גדולים ומבוססים כלכלית בלבד. בדומה, גם העלות הכרוכה בהשכרת שירותם של מומחים חיצוניים יכולה להיות עול כלכלי גדול לארגון קטן או בינוני. פתרון אפשרי לבעיות אלו הוא ששחקנים הפועלים כמתווכי מדיניות[31] יפרסמו כללי התנהגות מקובלים או הנחיות ליישום נכון. פתרון זה כרוך בחשש ממשי שכללי ההתנהגות וההנחיות ייהפכו הלכה למעשה לאסדרה מנחה על שלל חסרונותיה.

3. אסדרת תהליכים

שיטת אסדרה שלישית עוסקת באימוץ תהליכים (process-based regulation) ובאסדרה באמצעות גורמי ההנהלה בארגונים (management-based regulation).[32] על פי גישה זו, קובעי המדיניות מצפים כי המנהלים של מושאי האסדרה יפתחו ויאמצו תכניות ארגוניות שיישמו את מטרות המדיניות בקרב העובדים והמנהלים. בפרק הזמן הזה (של פיתוח תכניות ארגוניות ואימוצן), כלי מדיניות כמו חקיקה, תקנות או הנחיה יכולים לציין שם של תהליך כמו הנדסת פרטיות, תהליכי בדיקה העוסקים בפריצה למידע או סקר השפעה על פרטיות (data protection impact assessment) שיש ליישם – אך משאירים את האחריות ואת דרך היישום למנהלים. כך, למשל, כשמתרחשת פריצה למידע, על המנהלים להעריך אם יש

28 שם.

29 שם.

30 שם.

31 Kenneth W. Abbott at al., *Introducing Regulatory Intermediaries*, 670 Annals. Am. Acad. Pol. & Soc. Sci. 6 (2017); Kenneth W. Abbott et al., *Theorizing Regulatory Intermediaries: The RIT Model*, 670 Annals. Am. Acad. Pol. & Soc. Sci. 14 (2017).

32 Coglianese & Lazer, לעיל ה"ש 21.

חשש לפגיעה בזכויות ובחירויות של מושאי המידע. אם אין חשש כזה, המנהלים יכולים להמשיך ולעבד מידע בלי ליידע אף גורם, אך עליהם לתעד את האירוע כמיטב יכולתם.[33] כך, יתרונם של המנהלים נובע מהידע האיכותי שלהם בנוגע לפעילות ולסיכונים. כתוצאה מקרבה זו הם יכולים להיות במצב מועדף לביצוע התאמות של התהליך ויישומו בארגון כדי לעמוד בקריטריון הכללי שנקבע כמטרת מדיניות.

שיטת אסדרה זו – אימוץ תהליכים על ידי מנהלים – יעילה בשלושה מצבים. ראשית, כאשר השוק הרלוונטי מורכב משחקנים הטרוגניים. במצב זה, שבו כל מושא אסדרה שונה מאוד מרעהו, קשה לקובעי המדיניות לנסח וליישם אסדרה מכוונת אחידה לכלל השוק. מכאן היתרון של שיטה שנוקבת בתהליך (כמו "סקר השפעה על פרטיות" או "הנדסת פרטיות") אך משאירה למנהלים שיקול דעת באשר ליישומו בהתאם לנסיבותיהם. במצב השני הרלוונטי לשיטת אסדרה זו, האפשרות למדוד תוצרים ולעמוד ביעדים היא מורכבת ויקרה.[34] במצבים כאלה אסדרת ביצועים אינה כדאית ועדיף להתמקד בתהליך שמיישמים. שלישית, אסדרת תהליכים טובה למצבים שבהם הכוח הפוליטי של מושאי האסדרה בשוק המוסדר מאפשר להם לעמוד אל מול הרצון של קובעי המדיניות ליישם כלי מדיניות שמתווים אסדרה מנחה או התחייבות לציות.[35] במצבים אלו, הסכמה על כלי מדיניות של אסדרת תהליכים היא פשרה אפשרית השומרת את שיקול הדעת אצל מושאי האסדרה. למעשה – בדומה לאסדרת הביצועים – גם אסדרת תהליכים מתאימה לשוק הטרוגני ודינמי. כך, גם אסדרה תהליכית יכולה לתמרץ לחדשנות, למציאת פתרונות ולהפחתת עלויות.[36]

לאסדרת תהליכים יש גם כמה חסרונות. ראשית, היא מניחה שהאצלת שיקול דעת למנהלים בהקשר הרלוונטי היא נכונה ושיש אמון במשטר האסדרה הרלוונטי בין קובעי המדיניות, המאסדר ומושאי האסדרה. כך, למשל, אם קשה לנו לקבל את הרעיון שחברות אינטרנט המנהלות פלטפורמות ורשתות חברתיות יקבלו שיקול דעת לסנן תכנים פוגעניים כמו ביטויי שנאה או הפרות זכויות יוצרים – האם נסכים לתת להן שיקול דעת ביישום אסדרת תהליכים של הגנת מידע? שנית, בדומה לחסרונותיה של אסדרת הביצועים, היישום של אסדרת תהליכים משתנה בהתאם לגודל החברה, ובכלליות אפשר לומר שהיא מתאימה יותר לארגונים גדולים מאשר לארגונים קטנים. מעבר לכך, על פי רוב ארגונים גדולים מאורגנים ומאוגדים בצורה מורכבת, בכמה אתרים, לעתים תחת משטרי אסדרה שונים – מה שמקשה אף יותר על הטלת אחריות ניהולית ריכוזית. שלישית, ובהתאם למורכבות הארגון, אסדרת תהליכים צריכה להתמודד עם חוסר האמון האפשרי בתוך הארגון – בין המנהלים הבכירים שקובעים את מדיניות היישום של התהליך לבין העובדים שמיישמים אותו בפועל. כל חיכוך או חוסר־אמון הקיימים ממילא בארגון רק מתעצמים כשצריך ליישם את אסדרת

33 לעומת זאת, אם יש חשש, על המנהלים לידע את רשויות הגנת המידע תוך 72 שעות מרגע היוודעות המקרה. אם החשש גבוה יש ליידע גם את מושאי המידע, אלא אם קוימו כמה תנאים שנקבעו בסעיף 34.3 ל־GDPR. ראו ס׳ 33 ו־34 ל־GDPR.

34 ס׳ 33 ו־34 ל־GDPR.

35 Gilad, *It Runs in the Family*, לעיל ה״ש 21.

36 Coglianese & Lazer, לעיל ה״ש 21.

התהליכים בארגון.[37] כך, למשל, מה יהיו ההשלכות אם יעלה מתוך סקר הסיכונים שיש לעצב מחדש חלקים גדולים ממערכת עיבוד הנתונים כדי להפנים עקרונות של הגנת מידע? מה תהיה עמדת העובדים כשתעלה דרישה כזו ותחייב אותם לשעות עבודה נוספות רבות?

על אף קווי הדמיון בין אסדרת תהליכים לאסדרת ביצועים יש גם הבדל בין השתיים. כאידאל, היכולת לעמוד ביעדים לאורך זמן היא חלק חשוב משיטת אסדרה נכונה. לכן, כשהעלויות למדידת התוצרים נמוכות, יש להעדיף אסדרת ביצועים; לעומת זאת, כשעלויות המדידה גבוהות, כשהשוק הטרוגני או כשהשוק חזק פוליטית, העדיפות צריכה להינתן לאסדרת תהליכים. במצבים אלו, אסדרת תהליכים מתמקדת בשלב התכנון ומאפשרת למנהלים בארגונים להתאים את האסדרה לנסיבות האינדיבידואליות של כל ארגון, ומאפשרת לבחון את דרך היישום בלי להידרש לבחינת התוצר הסופי (כאמור, עלות מדידתו יכולה להיות גבוהה).

באסדרת תהליכים תפקיד המאסדרים לדאוג שמנהלי הארגונים יטלו אחריות לתכניות שאימצו ולהחלטות שקיבלו.[38] לעתים על המאסדרים להעריך אם התהליכים שאימצו המנהלים אכן מסוגלים לעמוד במטרות שהוצבו.[39] נוסף על כך, המאסדרים צריכים לקבוע את קריטריון האסדרה – הקריטריון המגדיר אילו אלמנטים צריכים לבוא לידי ביטוי בתהליכים שיישמו המנהלים. כך, למשל, אפשר לקבוע קריטריונים לתהליכים כמו זיהוי סיכונים והפחתתם, קביעת פרוצדורות לפיקוח ולתיקון תקלות, ויישום של הכשרות מקצועיות לעובדים. במקרים אחרים קובעי המדיניות יכולים לקבוע שהמנהלים יצטרכו לאשר את תכניותיהם אצל המאסדרים טרם יישומן, או לחייב את המנהלים לתעד את מעשיהם – צעד שיאפשר בחינה בדיעבד של פעילות הארגון בהתאם לקריטריון.

משהגדרנו את כלי המדיניות ואת שיטות האסדרה, בהמשך המאמר אבקש לבחון את משטרי הגנת הפרטיות האירופיים בהקשר של כלי מדיניות, לתאר את השינויים שמשטרים אלו עוברים ביחסי הכוחות בין השחקנים, ולהצביע על המגמה שעולה בהקשר של משטר הגנת הפרטיות החדש – אסדרת תהליכים.

37 Neil Gunningham & Darren Sinclair, *Organizational Trust and the Limits of Management-Based Regulation*, 43 Law & Soc'y. Rev. 865 (2009).

38 שם; Gilad, *It Runs in the Family*, לעיל ה"ש 21.

39 Coglianese & Lazer, לעיל ה"ש 21. כמו באסדרת המטרות, גם כאן יש צורך להעביר לרגולטורים מידע על אודות הסיכונים. ההשערה היא שדרישה זו תוביל לתאימות גבוהה יותר בין האכיפה לבין המאפיינים של נשואי הרגולציה. ראו Lori Snyder Bennear, *Evaluating Management Based Regulation: A Valuable Tool in the Regulatory Toolbox?*, *in* Leveraging the Private Sector: Management-Based Strategies for Improving Environmental Performance (Cary Coglianese & Jennifer Nash eds., 2006); Sharon Gilad, *Process-Oriented Regulation: Conceptualization and Assessment*, *in* Handbook on the Politics of Regulation (David Levi-Faur ed., 2011).

ד. התפתחותו של משטר הגנת המידע האירופי

1. חוקי הגנת המידע הראשונים

ראשיתם של חוקי הגנת המידע בשנות השישים והשבעים של המאה העשרים. לפי ויקטור מאייר־שונברגר (Mayer-Schönberger), אפשר להבחין בתקופה זו בארבעה משטרים קלאסיים להגנת מידע, בהתאם לתקופות ולהתפתחות הטכנולוגית. דור המשטרים הראשון נוצר כתגובה להתגברות הפעילות של עיבוד מידע אישי על ידי ממשלות, מוסדות מדינת הרווחה וארגונים פרטיים גדולים כמו בנקים שיכלו להרשות לעצמם להחזיק מחשבי mainframe. לפתע הייתה לארגונים אלו ולמוסדות המדינה יכולת לתכנן, לנהל ביעילות וליישם חקיקה ותקנות, למשל לצורך אספקת זכויות כלכליות־חברתיות לאזרחים ללא חשש מתרמיות.[40] השיח הציבורי נגד הכוונה ליצור מאגרי מידע ענקיים הוביל לחקיקה של חוקי הגנת המידע הראשונים של שנות השבעים. אלה נחקקו לאו דווקא כדי להגן על פרטיות האינדיבידואל אלא לאסדרת הפונקציה של עיבוד המידע בחברה.[41] נקודת המוצא של החקיקה הייתה שמספר מאגרי המידע מוגבל מאוד ולכן אפשר לשלוט ולאסדר אותם באמצעות תהליכים מיוחדים. במיוחד יש לומר שמטרתם של חוקי הדור הראשון הייתה פונקציונלית: אם עיבוד מידע הוא בעיה, אזי החקיקה צריכה להתמקד בפעילות המחשב תוך "אילוף" הטכנולוגיה לפי רצונות ושיקולים חברתיים כתלות במאפייני המדינה.[42] כתוצאה מכך התמקדו חקיקות אלו בעיקר בדרישות רישום ורישוי, ובהקמת מוסדות לפיקוח על פעולות הרשות המבצעת. נוסף על כך ניתנו לאזרחים זכויות פונקציונליות כמו האפשרות לתקן מידע שגוי. אפשרות זו נועדה לאפשר את המשך עיבוד המידע על בסיס מידע נכון, אך לא את הפסקתו של תהליך עיבוד המידע עקב פגיעה בפרטיות של מושאי המידע.[43]

בשנות השבעים של המאה הקודמת, עם הופעתם של ה־minicomputers שאפשרו גם ליחידות קטנות בארגונים לקבל גישה לעיבוד מידע ממוחשב, התעורר צורך במשטרי הגנת מידע שיתמודדו עם אתגרי עיבוד המידע במחשבים פרטיים. לכן, במשטרים מהדור השני הוסט הדגש מ"האח הגדול" של מדינת הרווחה אל עבר המחשבים הפרטיים. כתוצאה מכך התפתחה הכרה במגבלות ובמורכבות של הדרישה לרישום ורישוי של אלפי יחידות עיבוד מידע הפרוסות ברחבי המדינה. הפתרון שעלה הוא לאפשר לאזרחים להילחם על פרטיותם בעזרת זכויות פרט חזקות. בין היתר, קובעי מדיניות במשטרים אלו החלו לקדם

40 Newman, *Building Transnational Civil Liberties*, לעיל ה"ש 5, בעמ' 108.

41 שם.

42 כך, למשל, פרנצ'סקה ביגנאמי (Bignami) מצאה כי סגנונות האכיפה בצרפת, בגרמניה, בבריטניה, ובאיטליה השפיעו על החקיקה של חוקי הגנת מידע במדינות לפני חקיקת הדירקטיבה ואחריה. Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 Am. J. Comp. L. 411 (2011).

43 בשונה מהפסקתו המוחלטת או ממחיקת המידע, כפי שהתאפשר במשטרים מאוחרים יותר. ראו Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* Technology and Privacy: The New Landscape 219, 221-25 (Philip E. Agre & Marc Rotenberg eds., 1997).

זכויות המאפשרות להתערב בתהליך עיבוד המידע ובהגבלתו, בצד קידום תהליך לרישום של מאגרי מידע כתחליף לפעולות הרישוי של הדור הראשון, כמו גם דרישה שאלו יפעלו כנציבי תלונות.[44] כך, למשל, הסכמת האזרחים נדרשת לצורך עיבוד המידע או לצורך ביטול איסור בחוק לעבד מידע. אף שזכויות אלו העניקו לאזרח במישרין כוח לקבל החלטות ויכולת לאסדר, רעיונות פוליטיים אלו לא באו לידי ביטוי במציאות. הסיבה לכך: בפועל, האפשרויות העומדות לרשות הפרט כדי להגביל את עיבוד המידע על אודותיו היו מצומצמות. בהתחשב בכך שאנשים חיים בחברה ומשולבים בה, המשמעות של הגבלת מידע או של איסור מוחלט לעבד מידע היא הוצאת אזרחים מתהליכים חברתיים. בשל העלות החברתית והגישה של "הכול או כלום", נוצר דור שלישי של חוקי הגנת מידע.[45]

דור זה של חקיקות הגנת מידע חיזק אף יותר זכויות אינדיבידואליות. בין היתר, אם בדור השני התחילו לסגת מרעיון האסדרה האקטיבית של הטכנולוגיה והתחילו להתמקד בחירויות פרט מופשטות ובזכויות השתתפות, בדור השלישי התמקדו המחוקקים בעקרון בדבר informational self-determination (מונח שניתן לתרגמו כ"אוטונומיה מידעית") ובאמונה שאזרחים יפעילו את זכויות הפרט שלהם. כמו כן, זכויות הפרט הורחבו לכל השלבים של תהליכי עיבוד המידע, מאיסוף המידע ועד הסקת המסקנות.[46] בדומה לחוקי הדור השני, המציאות שוב הכתה בחוקי הדור השלישי. למרות כלי המדיניות החדשים בלבוש של זכויות פרט, ולמרות היכולת להשתתף בתהליך עיבוד המידע, מושאי המידע עדיין לא הסכימו לשלם את המחיר החברתי והכלכלי של הפעלת הזכויות שמשטרי הגנת מידע הראשוניים סיפקו.[47] למעשה, הרטוריקה של קבלת החלטות על ידי הפרט נותרה פוליטית.

בניגוד לדור השלישי, בדור הרביעי של משטרי הגנת מידע ניסו קובעי המדיניות להתמודד עם פערי הכוחות שבין האינדיבידואל לבין המוסד שאוסף ומעבד את המידע, ונוסף על כך גם להפוך חלק מהחירויות להגנות מחייבות שאינן פתוחות למשא ומתן גם אם מושא המידע הסכים לכך פרטנית. כך, למשל, נקבעו כללים ותיקוני חקיקה בנוגע להענקת פיצויים אוטומטיים, ובאירופה נוספו סעיפים האוסרים עיבוד של מידע רגיש או מונעים את היכולת להגביל בחוזה זכויות כמו גישה, תיקון ומחיקת מידע. לפי מאייר־שונברגר, ההתפתחות של ארבעת דורות חקיקה אלו באה לידי ביטוי בדירקטיבה והביאה כלאחר יד לחקיקתה כמסמך של פשרה בין סוגי המדיניות שהתקיימו קודם לכן במדינות,[48] וכתוצאה מכך – לעלייתו של משטר הגנת המידע האירופי הישן.

2. משטר הגנת המידע הישן כצעד ראשון להרמוניזציה על־מדינתית

כמה אמנות בין־לאומיות ועל־מדינתיות עוסקות בהגנת מידע והיוו, יחד ולחוד, את הבסיס לחקיקה אירופית ולקודי התנהגות מחוצה לה: ההנחיות של OECD בנושא הגנה על פרטיות וזרימת מידע אישי בין מדינות, האמנה להגנה על אינדיבידואלים ביחס לעיבוד

44 שם, בעמ' 226.
45 שם, בעמ' 226–229.
46 שם, בעמ' 229–232.
47 שם, בעמ' 232.
48 שם, בעמ' 232–234.

מידע אוטומטי של מועצת אירופה, והדירקטיבה להגנת מידע של האיחוד האירופי.[49] לשתי האמנות הראשונות היה חלק משמעותי בהפנמה של עקרונות מקובלים להגנת מידע, עקרונות המוכרים כ־FIPPs (Fair Information Practices Principles),[50] ושל הצורך שלא לעבד אוטומטית מידע רגיש אלא אם מיושמים אמצעים מתאימים שייקבעו בהתאם לחקיקה מדינתית.[51] למרות חשיבותן הרבה, בשתי אמנות אלו נעדר מכניזם שיבטיח כי העקרונות נאכפים בפועל. כך, למשל, עד סוף שנות השמונים, רק תשע מדינות אירופיות אשררו את האמנה של מועצת אירופה; חמש מדינות לא פעלו או לא הצליחו לבצע אסדרה מדינתית של הגנת מידע.[52] דוגמה מובילה היא ספרד, שאמנם אשררה את האמנה האירופית אך לא

---

49 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S No. 108, https://rm.coe.int/1680078b37. Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Jan. 23, 2001, C.E.T.S No. 181, https://goo.gl/z7gYUa; OECD מטרתו של ארגון הוא לקדם מסחר בין שלושים המדינות החברות. בשנות השבעים עמדו האמריקנים והאירופים משני צדי הדיון על אודות הצורך במדיניות ציבורית לפרטיות. כ־17 מדינות אירופיות חברות בארגון מאז שנות השישים, ועם השנים נוספו עוד כמה מדינות אירופיות. ראו Organisation for Economic Co-operation and Development [OECD], *OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL (Sept. 23, 1980), https://goo.gl/f6vkxU; בשנת 2013 פורסם עדכון לאמנה, ראו Organisation for Economic Co-operation and Development [OECD], *OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data,* C(2013)79 (Jul. 11, 2013), https://goo.gl/gVkTbm; ראו גם Bennett & Raab, The governance of privacy, לעיל ה"ש 12, בעמ' 84–93; Paul M. Schwartz, *The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966, 1970 (2013).

50 ראשיתם של ה־FIPPs בדוח אמריקני משנות ההשבעים של מחלקת הבריאות, החינוך והרווחה הפדרלית: Records, Computers and the Rights of Citizens: report of the Secretary's Advisory Committee on Automated Personal Data Systems. עם זאת, הנוסח החשוב של ה־FIPPs מופיע ב־OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. בהתאם ל־FIPPs יש לשמור על שמונה עקרונות: 1) collection limitation; 2) data quality; 3) purpose specification; 4) use limitation; 5) security safeguards; 6) openness; 7) individual participation; and 8) accountability. ראו *OECD Guidelines*, שם.

51 ראו ס' 6 ל־Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, לעיל ה"ש 49.

52 תשע המדינות שאשררו את האמנה היו אוסטריה, בריטניה, גרמניה, דנמרק, לוקסמבורג, נורבגיה, ספרד, צרפת ושוודיה. חמש המדינות שלא פעלו לבצע אסדרה היו איטליה, בלגיה, יוון, פורטוגל וספרד. ראו Newman, *Building Transnational Civil Liberties*, לעיל ה"ש 5, בעמ' 110.

הצליחה (באותה תקופה) לחוקק חקיקת הגנת מידע מדינתית.[53]

בשונה מהשתיים הראשונות, דירקטיבת הגנת המידע האירופית נתפסה ככלי בעל משמעות רבה בתחום הגנת המידע. בדין האירופי, דירקטיבות הן מעיקרן כלי משפטי ליצירת הרמוניזציה. הן מחייבות את המדינות החברות באיחוד האירופי לחוקק חקיקה מדינתית המיישמת את העקרונות וכלי המדיניות הקבועים בדירקטיבה במסגרת זמן נתונה. כך, וכיאה לדירקטיבות אחרות, הדירקטיבה להגנת מידע חייבה יישום של עקרונות הגנת מידע בדרך של חקיקה מדינתית.[54] בפועל התבססה הדירקטיבה על חוקי הגנת המידע שנחקקו עד שנות התשעים במדינות האיחוד, וכתוצאה מכך למעשה קידמה הרמוניזציה בין החוקים האירופיים.[55]

לאחר שכנועים ולחצים רבים[56] הגדירו קובעי המדיניות האירופים שתי מטרות־על. הראשונה – הבטחה שמידע אישי על מושאי מידע אירופיים יוכל לעבור באופן חופשי בין מדינות, ובמיוחד בין מדינות האיחוד;[57] השנייה – הבטחת רמת הגנה גבוהה לזכויות ולחירויות היסוד של אנשים ובמיוחד לזכותם לפרטיות. הלכה למעשה הדירקטיבה מבוססת

53 שם.

54 משחוקקה הדירקטיבה, המדינות החברות קיבלו מסגרת זמן של שלוש שנים לחוקק חקיקה מיישמת. ראו ס׳ 32 לדירקטיבת הגנת המידע.

55 כתוצאה מחקיקת הדירקטיבה, חמש המדינות – איטליה, בלגיה, יוון, פורטוגל, וספרד – נדרשו לחוקק חקיקת הגנת מידע מקומית, ויתר המדינות נדרשו לתקן את החקיקה המדינתית שלהן בהתאם. ראו Newman, *Building Transnational Civil Liberties*, לעיל ה״ש 5, בעמ׳ 118. דוגמה בולטת למדינות עם גישות שונות לכלי מדיניות אפשר למצוא בגרמניה וצרפת. צרפת ובנות בריתה רצו להמשיך עם מודל רישום נוקשה וגרמניה פעלה לקדם מודל אסדרה עצמית על בסיס ממונה הגנת המידע בארגונים. בסופו של משא ומתן הוסכם כי ס׳ 18 יחייב דיווח כשאחד החריגים לחובה זו יהיה מינוי הממונה. Bignami, *Cooperative Legalism*, לעיל ה״ש 42.

56 בשנות השמונים דחתה הנציבות האירופית את המלצות הפרלמנט לחוקק חקיקת הגנת מידע. הנציבות הפנתה לאמנה של מועצת אירופה כמקור מספק לחקיקה מדינתית ותמכה בעמדת התעשייה לשמור על החקיקה המדינתית. רק בתחילת שנות התשעים החלה הנציבות לתמוך בכללים כלל־אירופיים. חוקרים כמו אברהם ניומן (Newman) מציינים כי היו אלו רשויות הגנת המידע, שהוקמו לפני הדירקטיבה האירופית, שלמעשה נתנו את הדחיפה העיקרית למוסדות האיחוד לאמץ כללים כלל־אירופיים אל מול האתגר של מדינות אירופיות עם חקיקת הגנת מידע מקלה או כלל לא־קיימת. שם, בעמ׳ 110.

57 עקב עלייה בהעברות מידע בין־מדינתיות ובהיעדר אסדרה על־מדינתית, על פי רוב עבר מידע בין המדינות על בסיס עקרון ההדדיות. כך, בשנת 1989, כשרשות הגנת המידע הצרפתית (CNIL) התערבה בהעברת מידע לאיטליה כי מצאה שהמשטר האיטלקי לא מספק רמת הגנת מידע מספקת לזו הצרפתית, נדרשו קובעי המדיניות האירופיים להתערב. אלו הבינו כי בהיעדר חקיקה אחידה בין המדינות האירופיות תיתכן פגיעה ניכרת בהקמה של השוק האירופי המאוחד – עיקרון־על במדיניות האיחוד האירופי. צעד זה של רשות הגנת המידע התבסס על כוונתן של רשויות הגנת המידע להוביל לשינוי מדיניות. לפירוט התהליכים ולצעדים נוספים שהובילו לשינוי המדיניות, לרבות עמדת CNIL בנוגע לבלגיה, ראו Newman, *Building Transnational Civil Liberties*, לעיל ה״ש 5, בעמ׳ 114.

על הסכמות ופוליטיקות פנים־אירופיות. כך, בצד הפוליטיקה המדינתית שעלתה לרמה העל־מדינתית, בעת החקיקה הפעילו המדינות החברות לחצים כבדים על מוסדות האיחוד להנמיך את הדרישות שהופיעו בהצעות הראשונות של הדירקטיבה. בו בזמן, מדינות שכבר חוקקו חקיקות הגנת מידע מדינתית ביקשו שייבחרו לחקיקה בכלי מדיניות שהן כבר יישמו ולא כלי מדיניות המשמשים במשטרי הגנת מידע של מדינות אחרות.[58] אכן, אף שמוסדות האיחוד שאפו לקבוע סטנדרט הגנת מידע גבוה כאידאל, כדי להגיע להסכמה ולהרמוניזציה בין האינטרסים של המדינות המעורבות הם העדיפו לאזן בין החוקים האירופים הקיימים במקום לשאוף לחדשנות יתרה בחקיקה.[59] ההבנה הייתה שללא הדירקטיבה, הניסיון של המדינות החברות להגן על המידע של אזרחיהן במסגרות אירופיות ובין־לאומיות היה נתקל בפעילות של כלכלת המידע שהחלה לצמוח באירופה בשנות התשעים.[60] לאחר דיונים רבים, מתחים ופשרות, ועם שאיפה ליצור הרמוניזציה כלל־אירופית, הגיעו השחקנים שדנו בהצעת הדירקטיבה לגרסה מוסכמת שאפשרה הן העברות מידע בין־לאומיות והן הגנה על האזרחים האירופיים.

בסופו של התהליך הפוליטי הגדירו קובעי המדיניות האירופיים בנוסח הסופי של הדירקטיבה את ההגנה הקבועה בה כהגנה בסיסית ומקיפה. ברמת המעשה, המשמעות של הגנה כזו היא שהדירקטיבה הגדירה למדינות החברות מסגרת הגנת מידע עם סטנדרט הגנה רחב ועקרונות בסיס, ומדינות חברות יכולות להוסיף על עקרונות אלו הגנות נוספות אך לא להחליפם.[61] נוסף על כך, הדירקטיבה שמה דגש רגולטורי על קביעת הגבלות על איסוף מידע, כללים על איכות המידע והענקת זכויות פרטניות כמו גישה למידע ותיקון

58 לעתים מזומנות מדיניות האיחוד האירופית מבוססת על המודלים הקיימים של המדינות. כאשר המודלים המדינתיים שונים זה מזה, המדינות יתחרו על אימוץ את המודל שלהן כמדיניות כלל־אירופית. אימוץ כאמור יחסוך למדינה את הצורך לבצע התאמות ושינויים קיצוניים. כאשר למדינה אחרת יש מודל שונה והיא אינה מעוניינת לוותר בקלות, יתחרו ביניהן המדינות איזה מהמודלים ייהפך לסטנדרט הבין־לאומי המחייב. ראו Bignami, *Cooperative Legalism*, לעיל ה"ש 42, בעמ' 435. לדיון רחב בתחרות בין מדינות על מדיניות ראו Daniel W. Drezner, *Globalization, Harmonization, and Competition: The Different Pathways to Policy Convergence*, 12 J. Eur. Pub. Pol'y. 841 (2005). לפירוט על עמדת התעשייה האירופית נגד הדירקטיבה האירופית, במיוחד בשנות השמונים, ראו Newman, *Building Transnational Civil Liberties*, לעיל ה"ש 5, בעמ' 112.

59 Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 Iowa L. Rev. 445, 449 (1995). בשונה, בנט וראאב מציינים כי חדשנות מסוימת התקיימה בהוצאתם של עקרונות מלאכותיים ושל עקרונות שכבר אינם רלוונטיים. ראו Bennett & Raab, The governance of privacy, לעיל ה"ש 12, בעמ' 98.

60 Schwartz, לעיל ה"ש 49, בעמ' 1972.

61 הגורם שהוסמך לדאוג ליישום הרמוני של הדירקטיבה הוא A 29 WP. קבוצת העבודה פעלה כגוף משותף לרשויות הגנת המידע המדינתיות ודאגה להוציא חוות דעת. בשונה, כאשר חשבה הנציבות האירופית שמדינות יישמו את הדירקטיבה באופן שגוי, היא פעלה משפטית נגד אותן מדינות. אחד הכלים שבידי הנציבות הוא האפשרות לפנות ל־European Court of Justice כנגד מדינות אירופיות שחוקיהן לא עמדו ביעדים ובסטנדרטים שנקבעו בדירקטיבה. כך, למשל, פעלה הנציבות נגד לוקסמבורג, גרמניה, אוסטריה והונגריה. לסקירה של פסקי

מידע שגוי. כמו כן, משטר הגנת המידע הישן יישם כמה עקרונות הגנת מידע באופן ייחודי לאיחוד האירופי. כך, הדירקטיבה דרשה כי איסוף ועיבוד מידע יתבצעו על בסיס לגיטימי כמו הסכמה מדעת, חוזה או הגנה על אינטרסים לגיטימיים. עוד דרשה הדירקטיבה יישום של הגבלות על קבלת החלטות אוטומטיות, מלאות וחלקיות, בהקשר של עיבוד המידע האישי, וכן אספקה של שכבת הגנה נוספת למידע רגיש.[62] בצד עקרונות אלו וכלי אכיפה אחרים, דרשה הדירקטיבה – כחלק מעיקרון השקיפות – כי יתקיים פיקוח רגולטורי עצמאי על ידי רשות מדינתית להגנת מידע, וכי הרשויות המדינתיות יקבלו הודעה בטרם יחל עיבוד מידע אוטומטי או חצי־אוטומטי. אף כי חובת היידוע החלה כבר אז להיות מיושנת וקשה לתחזוקה, גם מאגרי מידע נדרשו להירשם עם אותה רשות.[63]

מעבר להשפעה הפנים־אירופית הייתה למשטר הישן גם השפעה על מדינות שאינן אירופיות. ככלל, כאשר מדינות לא־אירופיות ביקשו לקבל הכרה כמדינות שדיניהן תואמים לדין האירופי, הן נדרשו להראות שהמשטרים המשפטיים שלהם אימצו גם הם את העקרונות הנוספים שבדירקטיבה כחלק ממשטר הגנת המידע המקומי, ובמיוחד את קיומה של רשות עצמאית מפקחת.[64] יישום עקרונות אירופיים במדינות לא־אירופיות אינו ייחודי לתחום הגנת המידע; חוקרים כבר זיהו את הפרקטיקה שבה מדינות מנסות להשפיע פוליטית על המדיניות המאומצת במדינות אחרות ועל הסטנדרטים הבין־לאומיים שייבחרו כמקובלים

הדין ראו Summaries of EU Courts Decisions Relating to Data Protection 2000-2015 (Laraine Laudati ed., 2016), https://goo.gl/w9gyHE.

62 לפי פול שוורץ, הכלל על הגנה יתרה על מידע רגיש הוא תוספת מהדין הצרפתי של שנת 1978. ויקטור מאייר־שונברגר מציין שהכלל הוא סממן של הדורות השלישי והרביעי להגנת מידע. ראו Schwartz, לעיל ה"ש 49; Mayer-Schönberger, לעיל ה"ש 43. הדבר נכון במיוחד באיסור שהחקיקה האירופית מיישמת – על עיבוד מידע שעוסק בסממנים של מידע בנוגע לגזע, למוצא אתני, לעמדות פוליטיות, לאמונות דתיות או פילוסופיות, לחברות באיגודים מקצועיים, למידע בריאותי ולהעדפות מיניות. ראו ס' 8(1) לדירקטיבת הגנת המידע.

63 בעוד ס' 18 לדירקטיבת הגנת המידע קבע את חובת יידוע, ס' 19 ו־21 עסקו בפרטי ההודעה וחובת הרישום. לפי ס' 19, ההודעה צריכה לכלול כמה פרטים לרבות פרטיו של מנהל המאגר, המטרות של עיבוד המידע, הקטגוריות של מושאי המידע או קטגוריות המידע על אודותיהם, למי יימסר המידע, העברות מידע למדינות שלישיות והגדרות של אמצעי אבטחת המידע המיושמים. לפי ס' 21, המדינות החברות נדרשות לדאוג שתהליכי עיבוד המידע יהיו פומביים ושיהיה רישום שלהם. לפי קולין בנט (Bennett) וצ'רלס ראאב (Raab), חובת הרישום הייתה רחוקה מאוניברסליות מדינתית והיו חריגים רבים. כמו כן, לדבריהם היו ניסיונות להפחית מחובת היידוע – בין על ידי אוטומטיזציה של ההליך ובין על ידי הרחבת החריגים. ראו Bennett & Raab, The governance of privacy, לעיל ה"ש 12, בעמ' 123. ראו בנוסף Paul de-Hert & Vagelis Papakonstantinou, *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?* 32 Comp. L. & Sec. Rev. 179, 191 (2016).

64 השוו ס' 25 לדירקטיבת הגנת המידע, עם ס' 45 ל־GDPR. ראו גם *Workin Paper of The Working Party of EU Data Protection Authorities*, 18/EN WP 254 rev.01 (Feb. 6, 2018), https://goo.gl/1XcZ4r.

במוסדות בין־לאומיים.[65] בהקשר של הגנת מידע, ובמיוחד לאור הצורך לאפשר העברות מידע בין־לאומיות, כמה מדינות לא־אירופיות ביקשו לקבל הכרה רשמית כי הדין בהן תואם את הדין האירופי. היתרון של צעד זה לכל הצדדים ברור: המדינה הלא־אירופית מוכרת כבעלת משטר הגנת מידע שמספק הגנה בסטנדרט אירופי. ארגונים ומוסדות הממוקמים באירופה יכולים להעביר מידע למדינה זו ללא סיכון הפרה של כללי העברת מידע מחוץ לגבולות אירופה, וכן הם נמנעים מהצורך לפנות לתהליך ייעודי פרטני אל מול רשויות הגנת המידע במדינות אירופיות. לבסוף, המשמעות המרכזית למדינות האיחוד היא הפחתת החשש שמידע אישי על אודות אזרחים אירופיים ינוצל לרעה מחוץ לאיחוד. בהתאם לדירקטיבה, אם הנציבות מצאה פערים ביישום של הסדרי הגנת מידע במדינות לא־אירופיות, היא דאגה לפתוח במשא ומתן לצורך תיקונם.[66] במקרים קיצוניים הכריזו הנציבות או בית המשפט האירופי לצדק על בטלות ההכרה בתאימות.[67]

---

65 הספרות מבחינה בין היכולת של מדינות עשירות וחזקות ללחוץ פוליטית על מדינות חלשות מהן להוריד סטנדרטים גבוהים תוך יצירת **מרוץ לתחתית** (אפקט דלוור), לבין יכולתן של מדינות חזקות להוביל מדינות עם סטנדרטים נמוכים להעלות אותם לסטנדרט הגבוה והמקובל במדינה החזקה תוך יצירת **מרוץ לפסגה** (אפקט קליפורניה). ראו David Vogel, Trading Up: Consumer and Environmental Regulation in a Global Economy (1995); David Vogel, *Trading up and governing across: transnational governance and environmental protection*, 4 J. Eur. Pub. Pol'y 556 (1997); Drezner, **לעיל ה"ש 58**. **בהקשר של הגנת מידע ראו** Anu Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012); David Bach & Abraham L. Newman, *The European Regulatory State and Global Public Policy: Micro-institutions, Macro-Influence*, 14 J. Eur. Pub. Pol'y 827 (2007). **על גישות שונות להשפעת הגלובליזציה על מדיניות מקומית, ובין היתר בהקשר של הגנת מידע, ראו** William J. Long & Marc Pang Quek, *Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, 9 J. Eur. Pub. Pol'y 325 (2002).

66 **לפי הדירקטיבה, בצד היכולת לשאת ולתת עם מדינות בנוגע לתאימות של הדין המקומי לחקיקה האירופית, הנציבות יכולה להכיר במדינות לא־אירופיות כבעלות דין התואם את הדין האירופי. גם המדינות החברות רשאיות לקבוע תאימות, להתערב ולבטל החלטות אלו; ראו ס' 25 לדירקטיבת הגנת המידע, לעיל ה"ש 4.**

67 **במסגרת המשטר הישן הוכרו כמה מדינות כעומדות בדרישות האיחוד לתאימות, לרבות ישראל, קנדה ושוויץ. מדינות מספר כבר הכריזו שהן מתכוונות לעבור תהליך הכרה תחת משטר הגנת המידע החדש. לרשימת המדינות שהוכרו כתואמות את האיחוד האירופי ואת חוות הדעת בעניינן של הנציבות או של ה־**WP 29 A, **ראו** https://goo.gl/VLmieS. **בשונה, בשנת 2015 קבע ה־**European Court of Justice, **בפסק דין** *Schrems*, **כי ההסכם להעברת המידע בין האיחוד האירופי לארצות־הברית והצהרת התאימות שלו מצד הנציבות האירופית משנת 2000** (US-EU safe harbor), **אינם מבטיחים הגנה מספקת ולכן בטלים. האיחוד וארצות־הברית חתמו על הסכם חדש** (EU-US Privacy Shield), **שכמו ההסכם הקודם קיבל גם הוא הכרזת תאימות. יש לשים לב לכך שהסכמי העברת המידע הם שקיבלו הכרה בהכרזת הנציבות ולא המשטר האמריקני להגנת מידע. לעניין ההחלטה בעניין** *Schrems* **ראו** Case C-362/14, Schrems v. Data Protection Commissioner, 2015 E.C.R I-1. **להכרזת התאימות ראו** Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/

אכן, הדירקטיבה קובעת מערכת עקרונות הוגנים בנוגע לפרטיות ולעיבוד מידע, ומדינות אירופיות ולא־אירופיות המעוניינות בהכרה צריכות ליישם אותם לצורך אסדרת השוק המקומי שלהן. עקרונות אלו חורגים לעתים מהעקרונות המקובלים במסגרת FIPPs. כתוצאה מכך, בתקופת המשטר הישן עסק שיח הפרטיות בעקרונות הגנת הפרטיות הקיימים, בניסיונות להוסיף עקרונות חדשים ובמחשבה כיצד אלו באים לידי ביטוי בפועל בעת עיבוד מידע. כך, למשל דנו קובעי המדיניות בהוספת עקרונות כגון אחריותיות, שקיפות והנדסת פרטיות.[68]

מניתוח זה עולה שיטת אסדרה נוספת בהקשר של הגנת מידע, הנקראת בספרות העוסקת במדיניות ציבורית ורגולציה אסדרה מבוססת עקרונות (principles-based regulation). בהתאם לשמה, שיטה זו מתמקדת בקביעת עקרונות מסגרת ליישום המדיניות. יתרונה של שיטה זו נעוץ בגמישות לנסיבות שהיא מאפשרת הן למדינות המבקשות ליישם את הכלל העל־מדינתי והן לארגונים הנדרשים ליישם את הכלל המדינתי. על המדינות ועל הארגונים לפעול תוך שמירה על מסגרת העקרונות. חסרונה של שיטת קביעת מדיניות זו ברור: כאשר קובעי מדיניות מבקשים לבצע אסדרת התנהגויות באמצעות קביעת עקרונות מסגרת, הם למעשה מבקשים להגדיר תוצאות מדיניות בדרך של כללים וחובות מופשטים. בכך הם נמנעים מלהגדיר אילו אמצעים ותהליכים יש ליישם. היעדר שימוש באמירות ברורות ובכלי מדיניות קונקרטיים יכול להקשות על יישום המדיניות ולא להוביל להתנהגות הרצויה שבמוקד המדיניות הציבורית. בין היתר, העקרונות דורשים פרשנות קבועה באשר לרלוונטיות של העיקרון המופשט לנסיבות ספציפיות. מעבר לכך, אסדרה בדרך של עקרונות יוצרת מצב מובנה של חשש וסיכון שמא יקבע גורם אכיפה (או בית משפט) כי הדרך שנבחרה בפועל ליישם את העקרונות אינה עומדת בסטנדרט ההתנהגות הסביר או כי ההתנהגות הייתה שלא בתום לב.[69] הפרק הבא דן בהשלכות השימוש בשיטה זו בהקשר של הגנת מידע באירופה.

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), 2016 O.J. (L 207) 1.

68 לפי ארגון OECD, עקרון האחריותיות אומר כי על מעבד המידע להיות אחראי ליישום אמצעים שיאפשרו קיום לשבעת העקרונות האחרים של ה־FIPPs; ראו שם. בשנת 2010 הוציא WP29 מסמך מדיניות המציע לתקן את הדירקטיבה על ידי הוספת עיקרון של אחריותיות, שיחייב ליישם אמצעים מתאימים ואפקטיביים שיבטיחו את יישום העקרונות שבדירקטיבה ולהציגם לרשויות הגנת המידע לפי בקשה. ראו *Opinion 3/2010 of the Article 29 Data Protection Working Party on the principle of accountability*, 62/10/EN WP 173 (July 13, 2010). העיקרון של Privacy-by-Design, למשל, קיבל הכרה של הכנס הבין־לאומי של רשויות הגנת המידע. ראו *The 32nd International Conference of Data Protection and Privacy Commissioners: Resolution on Privacy by Design* (Oct. 27-29, 2010), https://goo.gl/ahrXZb.

69 Julia Black, *Forms and Paradoxes of Principles-based Regulation*, 3 Cap. Mark. L.J. 425 (2008); (Arie Freiberg, The tools of regulation (2010).

3. פערים ביישום: דירקטיבת הגנת המידע והשוק האירופי המאוחד

עקב השימוש של הדירקטיבה באסדרת עקרונות, כאשר התבקשו מדינות האיחוד ליישם את הדירקטיבה בחקיקה מדינתית הן השתמשו לשם כך בדרכים שונות. ההבדלים נבעו מפוליטיקה מדינתית, מההיסטוריה ומהתרבות הרגולטורית ומהנסיבות של כל מדינה. כך, למשל, ספירוס סימיטיס (Simitis) – שבין היתר היה נציב הפרטיות הראשון של מדינת הסן (Hessen) הגרמנית, בה נחקק חוק הגנת הפרטיות הראשון בשנת 1970 – הדגיש את השונות בין המדינות ביישום של כלי המדיניות להגנת מידע. בעוד שהבריטים וההולנדים העדיפו ליישם כלי מדיניות כמו קודי התנהגות, מדינות כמו צרפת, ספרד, בלגיה ופורטוגל קידמו את האיסור על עיבוד מידע רגיש.[70] גרמניה פעלה במישורים של אסדרה עצמית, כמו בדרישתה למנות קציני הגנת מידע בארגונים, והגדירה מידע אישי תוך התבססות על הפעולות לעיבוד המידע ולא על סוג המידע שמעבדים.[71]

בדומה לסימיטיס, חוקרים נוספים התייחסו להבדלי היישום של הפרקטיקות להגנת המידע במדינות השונות. בכמה מאמרים השוו החוקרים קנת׳ במברגר (Bamberger) ודיירדרה מוליגן (Mulligan) בין פרקטיקות הממונים על הגנת מידע בארצות־הברית לבין אלו של ארבע מדינות החברות באיחוד האירופי – גרמניה, צרפת, אנגליה וספרד. החוקרים הראו כי למרות המסגרת האחידה של הדירקטיבה עדיין היו הבדלים משמעותיים ביישום המדינתי של הפרקטיקות העוסקות בממונים על הגנת מידע. כך, בין היתר, הייתה שונות בנוגע לתפיסת התפקיד של הממונים על הגנת המידע ובנוגע לדרך פעילותם במסגרת משטר הגנת המידע המדינתי הרלוונטי.[72]

מחקרים אלו ואחרים הראו כי אף שהדירקטיבה נועדה להשיג הרמוניזציה, הפערים ביישומה בין המדינות נותרו בעינם. פערים אלו עמדו בסתירה למטרות־העל של האיחוד האירופי[73] כגון פיתוח של חברת המידע האירופית, השקעה במחקר ופיתוח של טכנולוגיות

70 Simitis, לעיל ה״ש 59, בעמ׳ 449–450.

71 שם, בעמ׳ 450.

72 Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe (2015); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe : Initial Data on Governance Choices and Corporate Practices*, 81 Geo. Wash. L. Rev. 1529 (2013); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011).

73 על נקודות אלו חזר הפרלמנט האירופי בהחלטה נוספת בשנת 2007, והדגיש שלושה עקרונות־מפתח: (1) הצורך לחזק את אמון הצרכנים האירופיים בסביבה המקוונת; (2) הצורך להתגבר על הקיטוע וההבדלים בין המדינות, המונע מצרכנים ומסוחרים לנצל ולהרוויח מהשוק האירופי הרחב; (3) הצורך לחזק את ההגנה על המשתמשים בסביבה המקוונת. ראו Resolution on Consumer Confidence in the Digital Environment Eur. Parl. Doc.2006/2048(INI) (2007).

מידע[74] וחיזוק של השוק האירופי המקוון המאוחד.[75] בהקשר של תחום הגנת המידע, מטרות־העל הללו עומדות בצד הרצון לאפשר לאירופה להתחרות בשוק טכנולוגיות המידע הבין־לאומי התחרותי,[76] ובצד הרצון לקדם את המטרות שבלב הדירקטיבה להגנת מידע – ראשית, ההגנה על חירויות הפרט וזכויותיו (במיוחד בהקשר של עיבוד מידע אישי) ושנית, השגתו של השוק האירופי המאוחד דרך זרימת מידע חופשית. בין היתר, בעוד שמוסדות האיחוד מצאו כי מטרות הדירקטיבה והעקרונות שבמרכזה עדיין רלוונטיים, עקב אתגרי הגלובליזציה והפיתוחים בטכנולוגיות המידע היו גורמים באיחוד שביקשו לאמץ גישה מקיפה ומעודכנת להגנת מידע. בגישה מקיפה זו וביישומה ב־GDPR אדון בחלק הבא.

ה. GDPR ועקרון האחריותיות

הדיונים וההתייעצויות בנציבות האירופית באשר לצורך בגישה חדשה להגנת מידע החלו באמצע 2009 ונהפכו לרשמיים ב־2010, עם פרסום הקריאה להתייעצויות בנושא הגישה המקיפה להגנת מידע באיחוד האירופי (Comprehensive approach on personal data protection in the European Union).[77] לפי הנציבות האירופית, בעוד שהדירקטיבה

74 כך, למשל, מוסדות האיחוד האירופי שמו לב לפערי ההשקעה בין אירופה, ארצות־הברית ויפן בהשקעה בפיתוח טכנולוגיות מידע (Information and Communication Technologies): 80 יורו לאדם באירופה אל מול 350 יורו ו־400 יורו ביפן ובארצות־הברית (בהתאמה). ראו Resolution on a European Information Society for Growth and Employment, Eur. Par. Doc. 2005/2167(INI) (2006).

75 בסקר שערכה הנציבות האירופית בין המדינות החברות נמצא כי במקרים רבים אפשר למצוא באינטרנט מוצרים זולים במידה ניכרת במדינה אירופית אחרת, ולעתים אף אפשר להשיג מוצר מסוים רק במדינה אירופית אחרת. לעומת זאת זיהתה הנציבות כי ברוב המדינות, ביותר מ־50% מהמקרים, סוחרים היו מפסיקים עסקת סחר מקוון שהחלה לאחר שזיהו כי הצרכן מגיע ממדינה אירופית אחרת. ראו *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cross-Border Business to Consumer e-Commerce in the EU*, COM (2009) 557 final (Oct. 22, 2009).

76 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions A Digital Agenda for Europe*, COM (2010) 245 final (May. 19, 2010).

77 בתקופה הרלוונטית טרם גובש הרעיון לאמץ חקיקה חדשה כרגולציה, ולכן ההתייחסות של הגופים היא עדיין באופן של "comprehensive approach", בלא אמירה קונקרטית איך גישה מקיפה זו תבוא לידי שינוי בחקיקה. הנציבות החלה בהתייעצויות בנושא משטר הגנת המידע החדש בשנת 2009, ורק בשנת 2012 הוציאה הנציבות את הצעתה ל־GDPR ובצדה את מסמך המדיניות המנתח למה רגולציה חדשה היא כלי המדיניות המשפטי הנכון. לעמדת הנציבות ורשויות הגנת המידע משנת 2010 ו־2009 (בהתאמה) ראו *Communication From The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee Of The Regions on a Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010); *The Future*

ועקרונותיה הם ניטרליים טכנולוגית,[78] אתגרים כמו תהליכי הגלובליזציה, התמודדות עם העברות מידע בין־לאומיות ופיתוחים בטכנולוגיות מידע מחייבים התייחסות מקיפה. בין היתר ציינה הנציבות כי יכולת התחרות של אירופה מוגבלת בשל הקיטוע בין המדינות והשפעתו על הסחר והצרכנים האירופים. לכן, לפי הנציבות, דרך חשובה להתמודדות עם חוסר אמון מצד צרכנים, ועם חוסר קוהרנטיות משפטית בין משטרי הגנת המידע המדינתיים, היא בחינת המסגרת הרגולטורית של הגנת מידע ועדכון הכלים הקשורים אליה. כלים כאלה הם, למשל, אחריות משותפת (shared responsibility) של אזרחים, של ארגונים פרטיים ושל מוסדות ציבוריים, אימוץ עקרונות של הנדסת פרטיות וחובה להודיע על כשלים באבטחת מידע.[79] בהקשר המוסדי ביקשו בנציבות האירופית להסדיר את ההסדרים המוסדיים ולחזק את רשויות הגנת המידע.[80] לבסוף ביקשה הנציבות לשפר את הקוהרנטיות של כלל המסגרות המשפטיות העוסקות בהגנת מידע ולהפנים את עקרונות הגנת המידע לתוך ארגונים וספקי שירותים באמצעות עקרון האחריותיות.[81]

בתחילת 2012, לאחר קבלת התייחסויות רבות מהמוסדות האירופים ומשחקנים רבים בשוק, פרסמה הנציבות את טיוטת ה־GDPR,[82] דירקטיבת הגנת המידע לרשויות אכיפה,[83] ואת דוח הערכת השפעות הרגולציה החדשה.[84] העבודה על הטיוטה עברה לפרלמנט ולמועצה

---

of Privacy: Joint Contribution of Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the Legal Framework for the Fundamental Right of Data Protection, 2356/09/EN WP 168 (Dec. 1, 2009) (להלן: מסמך עתיד הפרטיות).

78 לעניין ניטרליות טכנולוגית ראו Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 Yale J.L. & Tech. 24 (2012).

79 *Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, COM (2010) 245 Final (May. 19, 2010).

80 שם.

81 לפחות לפי קבוצות העבודה האירופיות שעוסקות בהגנת מידע, התפיסה שהגנת המידע היא חלק אינטגרלי מהארגון אמורה לסייע לרשויות הגנת המידע בתהליכי הפיקוח והאכיפה. כתוצאה מכך, נטען, האפקטיביות של משטר הגנת המידע תשתפר. מסמך עתיד הפרטיות, לעיל ה"ש 77.

82 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012).

83 *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, (COM (2012) 10 final, (Jan. 25, 2012).

84 The European Commission, *Commission Staff Working Paper, Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council*

האירופיים, שהם הגופים המחוקקים של האיחוד. הפרלמנט סיים את העבודה על הטיוטה בתחילת 2013, אך הדיונים במועצה בקרב המשלחות נמשכו כשלוש שנים. רק כשהגיעה המועצה לנוסח מוסכם ביוני 2015 החלו דיונים בין הנציבות, המועצה והפרלמנט בניסיון למצוא גרסה מוסכמת. הנוסח הסופי אושר רק באפריל 2016.

הלכה למעשה, עקב לחץ מצד הנציבות בחר האיחוד האירופי בכלי משפטי של רגולציה ולא של דירקטיבה. להחלטה זו השפעה חשובה על מדיניות האיחוד בתחום הגנת המידע, מאחר שלרגולציה יש השפעה משפטית ישירה על המדינות החברות, ועד כה הוגבל השימוש בה לתחומים מסוימים כמו דיני תחרות וסימני מסחר ולהקמת סוכנויות אירופיות וניהולן.[85] בכל יתר סוגיות המדיניות שמוסדות האיחוד מבקשים לאסדר, העדיפות היא לדירקטיבות, המאפשרות למדינות גמישות ביישומן.[86] כך, למשל, תחת משטר הגנת המידע הישן, המבוסס על דירקטיבה, היו המדינות האירופיות נדרשות לעדכן את חוקי הגנת הפרטיות שלהן ולהוסיף את עקרון האחריותיות – צעד שהיה מוביל ליישום מדינתי שונה של עיקרון זה. משטר הגנת הפרטיות החדש קבע מראש, בדרך של רגולציה, את הרכב כלי המדיניות שהוא מבקש להחיל על מושאי האסדרה.

בתחומים רבים המשטר החדש מסתמך על הדירקטיבה שקדמה לו.[87] כך, למשל, בהגדרות השחקנים – מנהלים, מחזיקים, מקבלים וצדדים שלישיים. בו בזמן, הרגולציה הביאה עדכונים חשובים. ה־GDPR מעגן את העקרונות לעיבוד מידע אישי מהמשטר הישן בעקרונות דוגמת חוקיות, הוגנות ושקיפות, הגבלת מטרה, צמצום מידע, דייקנות, הגבלות על אחסון, יושרה וסודיות. במסגרת עקרון האחריותיות, מנהל המאגר אחראי לעמוד בעקרונות אלו ועליו להוכיח תאימות אליהם.[88] במיוחד יש לציין כי הזכויות של מושאי המידע חודדו ואף הורחבו בנושאים כמו מתן הסכמה, זכות למחוק מידע, זכות לקבל מידע, זכות להעביר מידע וזכות

---

on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, SEC (2012) 72 final (Jan. 25, 2012).

85 בד בבד נדרש מהמדינות החברות לחוקק בשטחן חקיקה מיישמת. חקיקה זו לא נועדה להחליף את החקיקה האירופית אלא לעסוק בסוגיות שהחקיקה האירופית השאירה לשיקול הדעת של המדינות, במיוחד כאלה שבהן המדינות מבקשות להחמיר יתר על שנקבע בחקיקה האירופית. נוסף על כך, החקיקה האירופית דורשת מהמדינות החברות לקבוע מי יהיו המאסדרים הפועלים בשטחם כרשויות הגנת מידע. מרגע שאלו הוסמכו או הוקמו, החקיקה האירופית היא שמגדירה את סמכויותיהם ואת המשימות שעליהם לבצע. ראו פרק 6 ל־GDPR ובמיוחד ס׳ 57 ו־58 לעניין הגדרת המשימות והסמכויות של רשויות הגנת המידע.

86 ראו de-Hert & Papakonstantinou, לעיל ה״ש 63, בעמ׳ 182.

87 ס׳ 4 ל־GDPR.

88 ס׳ 5 ל־GDPR. להסבר מפורט על ההבדל בעקרונות בין דירקטיבה לרגולציה, לרבות לעניין חוקיות עיבוד המידע, ראו de-Hert & Papakonstantinou, לעיל ה״ש 63, בעמ׳ 185–187.

להתנגד לעיבוד מידע, במיוחד בהקשר של פרופיילינג וקבלת החלטות באופן בלעדי על ידי עיבוד מידע אוטומטי.[89]

בגזרת רשויות האכיפה התרחשה התפתחות חשובה. אף שתחת המשטר הישן נחשבו רשויות הגנת המידע אמצעי מוצלח לפיקוח ואכיפה על הגנת המידע בתחומיהן,[90] הורגשו הבדלי סמכויות גדולים ושיתופי פעולה במקרים של העברות מידע בין־לאומיות. כתוצאה מכך, המשטר החדש מיישר קו בין הרשויות, עצמאותן, כשירותן, סמכויותיהן ומשימותיהן.[91] כך, למשל, האחריות לאכיפה בגין הפרות מוטלת על רשות הגנת המידע המובילה (lead DPA) שבתחום שיפוטה יושב מרכז פעילותו של מנהל או מחזיק מאגר המידע. רשות זו נדרשת לשתף פעולה עם יתר הרשויות הרלוונטיות, וכדי להבטיח את שיתוף הפעולה נוצר מנגנון של עקביות (consistency mechanism).[92] כדי להבטיח את השימוש בהליך זה וכדי להבטיח אחידות בפרשנות החקיקה וביישומה, הוחלף A 29 WP במוסד אירופי חדש – European Data Protection Board. אמנם הנציבות תכננה שגוף זה יחזיק בסמכויות זהות לאלו של קבוצת העבודה שקדמה לו, אך התוצר הסופי של הליך החקיקה היה ישות משפטית עצמאית, עם נשיאות ומזכירות, משימות, סמכות לקבלת החלטות ולאכיפתן.[93]

היחסים בין רשויות הגנת המידע לבין מושאי האסדרה עודכנו גם הם. ראשית, בוטלה חובת היידוע של הרשויות מצד המנהלים על פעילויות עיבוד המידע שלהם – חובה שראשיתה כאמור בשנות השישים והשבעים, כשעיבודי המידע היו מעטים ונשארו ברמת המדינה. חובת יידוע זו נהפכה בלתי־אפשרית ליישום כבר בשנות התשעים, ולכן ההחלטה של הנציבות לבטלה לא נתקלה בהתנגדות מצד הפרלמנט והמועצה.[94] את חובת היידוע החליף עקרון האחריותיות: המנהלים אחראים ליישם את העקרונות ואמצעי הביטחון, וחובה עליהם לתעד את פעילותם כדי להוכיח בעתיד לרשויות הגנת המידע כי עמדו בעקרונות אלו. למעשה, מדובר בהפיכה של חובת ההוכחה: במקום רישום מראש – הוכחה בדיעבד. הרגולציה כוללת גם תמהיל ייחודי של כלי מדיניות, כזה המכניס באופן משמעותי כלי מדיניות שעניינם אסדרת תהליכים וקבלת אחריות על ידי המנהלים אל מול הצורך בפיקוח אפקטיבי מצד המאסדרים.

נוסף על כך, אף שעקרון האחריותיות לא חל ישירות על המחזיקים, בכמה מקרים המשטר החדש מטיל עליהם חובה ישירה ליישם תהליכים בנוגע לפעילותם. כך, למשל, אף שמנהלים עדיין צריכים לדאוג לאסדרת המחזיקים, מחזיקים נדרשים לדאוג הן לאסדרה של עצמם והן לאסדרה של מחזיקים מסדר שני – השחקנים שהם עובדים איתם ושמעבדים עבורם

89 ראו פרק 3 ל־GDPR. בנוסף ראו de-Hert & Papakonstantinou, לעיל ה"ש 63, בעמ' 187–190. במיוחד יש לציין כי עמדת הנציבות שיש צורך בהסכמה מפורשת (explicit consent) לא התקבלה על ידי המועצה והפרלמנט.

90 de-Hert & Papakonstantinou, שם, בעמ' 190. ראו גם Newman, *Building Transnational Civil Liberties*, לעיל ה"ש 5.

91 ראו פרק 6 ל־GDPR.

92 ראו ס' 56 ו־60 ל־GDPR.

93 ראו פרק 7 ל־GDPR; וגם de-Hert & Papakonstantinou, לעיל ה"ש 63, בעמ' 193.

94 ראו de-Hert & Papakonstantinou, לעיל ה"ש 63, בעמ' 191.

מידע.[95] על כלל הגופים הללו מפקחות במישרין רשויות הגנת המידע. הפרה של חובות אלו, מצד מנהל מאגר או מחזיק, יכולה להביא להטלת קנסות מנהליים גבוהים.[96] אפשר להבין שמטרתו של המשטר החדש היא ליצור הגדרות אחידות של המוטל על מנהלים ועל מחזיקים האוספים ומעבדים מידע באירופה, ולהבנות את יחסי הכוחות בהקשר של הצורך באסדרה ופיקוח יעילים. החלק הבא מַבנה לתוך עקרון האחריותיות את הקטגוריות של כלי המדיניות ומראה כיצד אלו מבנים את יחסי הכוחות בין השחקנים.

ו. קטגוריות של כלי מדיניות לפרטיות בהתאם למשטר החדש

עקרון האחריותיות שהוכנס אל משטר הגנת הפרטיות החדש נושא עמו הרבה מעבר לעיקרון נורמטיבי האומר שמנהלים המעבדים מידע צריכים להיות אחראיים לעיבוד זה. כך, משטר הגנת המידע החדש מגדיר בהרחבה את כלי המדיניות, ודרכם – את הציפיות ואת יחסי הכוחות בין השחקנים הפועלים בו. ככלל, אפשר להבחין בין שש קטגוריות של כלי מדיניות שמוסדו לתוך משטר הגנת המידע החדש.[97]

טבלה מס׳ 1: קטגוריות של כלי מדיניות להגנת מידע במסגרת האירופית

	כלי מדיניות הממוקדים באסדרה עצמית	כלי מדיניות הממוקדים במוטבי האסדרה	כלי מדיניות הממוקדים במאסדרים
כלים תהליכיים	כלי מדיניות תהליכיים הממוקדים באכיפה עצמית	כלי מדיניות תהליכים הממוקדים במשתמשים	כלי מדיניות תהליכיים הממוקדים במאסדרים
כלים אופרטיביים	כלי מדיניות אופרטיביים הממוקדים באכיפה עצמית	כלי מדיניות אופרטיביים הממוקדים במשתמשים	כלי מדיניות אופרטיביים הממוקדים במאסדרים

כלי מדיניות תהליכיים הם כלים שמטרתם לעסוק בשלב המקדים לפעולות האיסוף והעיבוד של המידע, שבו המנהלים עדיין מתכננים את הפעילות. בשלב זה אפשר למנוע או לצמצם את הפגיעה על ידי עידוד אסדרה מקדימה. בשונה, כלים אופרטיביים הם כלי מדיניות המכוונים לשלב הביצוע – איסוף המידע, עיבודו והסקת מסקנות ממנו. חלוקה זו, הבנויה

95 כך, בין היתר, ה־GDPR מחייבת את מחזיק המאגר להשתמש רק במחזיקים המבטיחים רמה מספקת של הגנת מידע על ידי אימוץ אמצעים טכניים וארגוניים (ס׳ 28.1), לשתף פעולה עם רשות הגנת המידע (ס׳ 31), לדאוג לאבטחת מידע (ס׳ 32) ובהתאם לנסיבות – למנות ממונה הגנת מידע (ס׳ 37). אם מחזיק מאגר אינו אירופי, הוא נדרש להחזיק נציג באיחוד האירופי (ס׳ 27). ראו ב־GDPR.

96 יש לציין כי גם שחקנים נוספים, שאינם מנהלי מאגר או מחזיקים, יכולים להיקנס אם לא יעמדו בדרישות ה־GDPR. כך, למשל, גורמים המאשרים (certifiers) עמידה בסטנדרטים וגורמים המפקחים על עמידה בקודי התנהגות יכולים להיקנס בקנסות מנהליים אם לא עמדו בחובות הפיקוח. ראו ס׳ 83.4 ל־GDRP.

97 במסגרת משטר הגנת המידע החדש אין כלי מדיניות שעוסקים באסדרת ביצועים. אין זה אומר כי אלו לא יכולים להיווצר בעתיד, במסגרת הנחיות של אסדרה עצמית.

על הקשר בין תזמון ההתערבות הרגולטורית לבין השיטה, אינה נקייה מביקורת;[98] אולם ההבחנה על בסיס מועד ההתערבות חשובה משום שהיא בוחנת אם המנהלים התחילו את שלב איסוף המידע ועיבודו או שמא הם עדיין בשלב המקדמי של תכנון פעולותיהם. בשלב מקדמי זה אפשר, למשל, לבחון סיכונים ולהנדס את המערכת לפרטיות לפני שפרטיותם של מושאי המידע נפגעת בפועל.

בד בבד עם ההבחנה על ציר הזמן בין השלב המקדים לשלב הביצועי, כלי המדיניות מתייחסים גם לשלושה שחקנים וכתוצאה מכך מעצימים אותם – כלי מדיניות של אסדרה עצמית, כלי מדיניות שמתמקדים במושאי האסדרה וכלי מדיניות שמתמקדים במאסדרים. על פי רוב אנו משייכים את פעילות האסדרה לקבוצת כלי המדיניות שעוסקת במאסדרים ומעצימה אותם. שחקנים אלו אמורים לדאוג לאינטרס הציבורי, להגן על הציבור קולקטיבית באמצעות אכיפה ולספק לציבור מידע.[99] בשונה, אסדרה יכולה גם לתמוך באסדרה עצמית המאפשרת לארגון לאסדר את עצמו באופן שיוכר על ידי המאסדרים או לתת כוח לארגון אחד או יותר לאסדר ארגונים אחרים הפועלים בשוק.

לבסוף, כלי מדיניות יכולים לתת כוח למוטבי האסדרה (מושאי המידע בהקשר של הגנת מידע), ובהתאם לחייב שחקנים אחרים בשוק ליישם אמצעים שיאפשרו למושאי האסדרה לממש את זכויותיהם. כלי המדיניות יכולים לתת למוטבי האסדרה קול – את האפשרות להשתתף בשיח, להתערב בנעשה בעניינם ולהביע את מורת רוחם.[100] כמו כן, כלי המדיניות יכולים גם לספק למוטבי האסדרה בחירה – את היכולת לברור בין אפשרויות; אך משטר הגנת המידע החדש מבקש, בין היתר, לפעול נגד החשש שמושאי האסדרה לא יפעלו לטובת האינטרס שלהם. במיוחד המשטר נותן אפשרות לייצוג של מושאי האסדרה על ידי ארגוני חברה אזרחית. אלה הם לרוב שחקנים חוזרים: הם נהנים מגישה טובה יותר לשחקנים אחרים, הם יכולים לסייע באספקת מידע ובחינוך לשימוש נכון במידע אישי והם יכולים לפעול לשינוי חקיקה ובמסגרות משפטיות.[101] כעת, בהתאם לטבלה, אפשר להתמקד בהרחבה בשש הקטגוריות של כלי המדיניות הקיימים במסגרת משטר הגנת המידע החדש.

---

98 במיוחד יש לציין את טענתו של דיוויד ת׳או (Thaw) כי הטיפולוגיה המדוברת חסרה בכל הנוגע לאסדרה של אבטחת מידע. לפי ת׳או, הקושי של הטיפולוגיה המקובלת נובע מכך שלאבטחת מידע אין תוצר התואם את ההגדרות של האסטרטגיות. כך, למשל, לפי ת׳או, הפעולה של שמירת מערכת המחשבים בטוחה היא בעצמה שירות או טובין, אך פגיעה חד־פעמית לא אומרת כי אותו טובין לא נוצר או כי השירות המדובר לא נמסר. משכך, לפי ת׳או יש לדבר על שלושה שלבים אחרים: שלב התכנון, שלב היישום, ושלב התוצרים/היעילות. Thaw, לעיל ה״ש 23, בעמ׳ 300–301.

99 Martin Lodge, *Accountability and Transparency in Regulation: Critiques, Doctrines and Instruments*, *in* THE POLITICS OF REGULATION: INSTITUTIONS AND REGULATORY REFORMS FOR THE AGE OF GOVERNANCE 124 (Jacint Jordana & David Levi-Faur eds., 2004).

100 שם.

101 להתייחסות מקיפה לתפקידי החברה האזרחית בהקשר של הגנת מידע ראו COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008). דוגמה בולטת בהקשר האירופי היא European Digital Rights (EDRi). הארגון מרכז תחת פעילותו ארגוני זכויות אדם מרחבי אירופה וכך מגן על זכויות וחירויות בסביבה הדיגיטלית. בצד הגופים

1. כלי מדיניות אופרטיביים הממוקדים באכיפה עצמית

כלי מדיניות הם אופרטיביים כשהם מספקים למנהלים כללים ומטילים עליהם אחריות או הגבלות שהם חייבים ליישם בזמן שהם מתפעלים את הארגונים, אוספים מידע, מעבדים מידע ומספקים שירותים לאחרים על סמך המידע שאספו ועיבדו. כלי מדיניות אלו גם מאפשרים למנהלים להתמודד עם מצבים לא צפויים. במצבים אלו, ארגונים ומנהלים יכולים לקחת שליטה על ארגונים אחרים הפועלים במרחב מדיניות הגנת המידע ולאסדרם. כך, למשל, משטר הגנת המידע החדש קובע כי מנהלים של מאגרי מידע יכולים לעבוד רק עם ארגונים אחרים שהרגולציה מתייחסת אליהם כמחזיקים, ורק אם אלו המבטיחים באופן מספק ליישם אמצעים טכניים וארגונים מתאימים והולמים.[102] אסדרת היחסים בין המנהלים למחזיקים במצבים לא צפויים היא אופרטיבית ומתרחשת בזמן אמת. בו בזמן, משטר הגנת המידע החדש מספק כלים אופרטיביים ממוקדי אסדרה עצמית גם לאיגודי תעשייה וסחר. למשל, משטר הגנת המידע החדש מאפשר לשחקנים פרטיים אלו להקים גופי פיקוח עם סמכויות אכיפה כדי לאכוף את קודי ההתנהגות שאותם שחקנים מבקשים לאשר על רשויות הגנת המידע.[103] מטרתם של גופי הפיקוח הפרטיים היא להבטיח כי ארגונים יהיו מפוקחים באופן אפקטיבי – קודם כל באופן של אסדרה עצמית ורק לאחר מכן על ידי המאסדרים המדינתיים.

2. כלי מדיניות תהליכיים הממוקדים באכיפה עצמית

כלי מדיניות תהליכיים אלו הם כלי מדיניות המחייבים מנהלי מאגרים, ובמצבים מסוימים גם מחזיקים, ליישם פרוצדורות פנימיות בתוך הארגון. כלי מדיניות אלו מאופיינים בכך שהחקיקה לא מגדירה למושאי האסדרה כיצד ליישם את התהליכים הלכה למעשה, אלא מפנה לתהליכים מוכרים מהפרקטיקה ומצפה שהמנהלים יישמו אותם נכונה. השאיפה של קובעי המדיניות היא שיישום נכון של התהליכים הכרוכים בכלי המדיניות הוא שיבטיח עמידה במטרות של הגנת מידע. כך, לדוגמה, כלי המדיניות יכולים לדרוש מארגונים לבצע סקר סיכונים להגנת מידע, למנות ממונים על הגנת מידע בארגון או לבצע הכשרות של עובדים.[104] דוגמה בולטת במשטר הגנת המידע החדש היא הדרישה להנדסת פרטיות. כאשר הנדסת פרטיות נתפסת כתהליך, מנהלים נדרשים ליישם אמצעים טכניים וארגוניים מתאימים והולמים בשלבים המוקדמים של תכנון המוצר או השירות. לפי ה־GDPR, אמצעים אלו

האירופים משתפים פעולה עם הארגון גם כמה גופים אמריקנים ובין־לאומיים כגון Privacy International וה־EFF.

102 ראו ס׳ 28.1 ל־GDPR. מעבר לכך, המונח appropriate technical and organizational measures מופיע כמה פעמים נוספות ב־GDPR, בין היתר תחת האחריות הכללית של מנהלי מאגרי המידע (ס׳ 24), הנדסת פרטיות (ס׳ 25), חובות המחזיקים כלפי עצמם וכלפי מחזיקים נוספים (ס׳ 28) ואבטחת עיבוד המידע (ס׳ 32). יישום תקין של האמצעים יכול להשפיע על חובות כגון חובת הדיווח למושאי המידע לפי ס׳ 34 ל־GDPR (data breach communication) בשונה מחובת הדיווח למאסדר לפי ס׳ 33 ל־GDPR (data breach notification).

103 ראו ס׳ 40 ו־41 ל־GDPR.

104 ראו ס׳ 35, 37, ו־39 ל־GDPR.

יבטיחו יישום בפועל של עקרונות המשטר להגנת מידע.[105] נוסף על כך, ייתכן שארגונים יצטרכו להטמיע למערכות עיבוד המידע גם אמצעי אבטחת מידע. אמנם דרישות אלו ליישום תהליכים, ובמיוחד הדרישה להנדסת פרטיות, נכונות גם לשלב האופרטיבי שבו הארגון אוסף ומעבד מידע, אבל חשיבותן נובעת מהעובדה שהדרישות עוסקות בעיקר בשלב המוקדם של תכנון האמצעים לעיבוד מידע וקביעתם. בה בעת, השוק גם יכול להידרש להכין קודי התנהגות והנחיות שיסבירו לארגונים מהו עיבוד מידע הוגן, או שיבהירו לאותם ארגונים מה הם אמצעי אבטחה תקינים לעיבוד מידע.[106] תחת כלי מדיניות אופרטיביים הממוקדים באכיפה עצמית אפשר למצוא את כלי הפיקוח והאכיפה העצמאיים, אך תהליך ההכנה של קודי ההתנהגות והסטנדרטים – כמו גם תכנון העמידה בהם – מחייבים פעולה מראש מצד השחקנים.

3. כלי מדיניות אופרטיביים הממוקדים במוטבי האסדרה

משטר הגנת המידע החדש מעניק גם כלי מדיניות אופרטיביים הממוקדים במוטבי אסדרה. כלי מדיניות אלו עוסקים במושאי המידע ומספקים להם "קול" ו"בחירה", ומאפשרים למושאי המידע לקבל מידע באשר לאופן שבו הגופים מחזיקים או מעבדים את המידע האישי, ונותנים בידם יכולת לשנות מידע שגוי או חלקי. בו בזמן, כלי המדיניות הללו באים לידי מימוש רק על בסיס שיקול דעתם המוחלט של מושאי המידע. כתוצאה מכך רק מושאי המידע יכולים להבטיח כי ישתמשו בכלי המדיניות האופרטיביים הממוקדים בהם. דוגמה לכלי אופרטיבי ממוקד מושאי המידע הוא הזכות למחיקה. כלי מדיניות זה מוכר לעתים גם בשם הזכות להישכח. השימוש בכלי זה הוא אופרטיבי אך הוא כרוך בכמה שלבים: ראשית, על מושא המידע להשיג גישה למידע האישי המוחזק על אודותיו במאגר מידע; שנית, מושא המידע צריך לקבל החלטה בעניין המידע האישי, למשל: האם לתקן את המידע או למחוק אותו; שלישית ולבסוף, מושא המידע צריך לפעול על פי החלטתו ולבקש למחוק מידע אישי מהמאגרים הרלוונטיים. בפועל, כלי המדיניות יכול לקבל צורות שונות בהתאם לארגון. כך, למשל, ארגון אחד יאפשר פנייה לשירות לקוחות טלפוני ואילו ארגון אחר יפתח ממשק משתמש מקוון ייעודי. כפי שיוסבר להלן, התכנון של תצורת הממשק או שירות הלקוחות הוא תהליכי. כתוצאה מכך, השיח על אודות הפעלתם ויישומם של כלי המדיניות האופרטיביים הממוקדים במוטבי האסדרה הוא קריטי להגנה על מידע אישי. זיהוים ופיתוחם חשוב להצלחת הפעלתם באופן יעיל על ידי מושאי המידע.

4. כלי מדיניות תהליכיים ממוקדי מוטבי האסדרה

בהקשר של הגנת מידע יש כלי מדיניות תהליכיים המתמקדים במוטבי האסדרה ומחייבים מנהלים ליישם תהליכים ואמצעים ייעודיים כדי לשמור על האינטרסים והזכויות של מושאי המידע. בשונה מהכלים האופרטיביים – המופעלים, כאמור, על פי שיקול הדעת של מושא המידע – כלי מדיניות תהליכיים הממוקדים במוטבי האסדרה מקבלים ביטוי בשלב מוקדם של פעילות הארגון. כתוצאה מכך, כלי המדיניות התהליכיים יישומו במנותק מהשאלה אם

105 ראו ס' 25 ל־GDPR.

106 ס' 40 ל־GDPR.

מושאי המידע אכן ישתמשו בכלי המדיניות האופרטיביים הקשורים לתהליך המדובר. כך, למשל, הזכות למחיקה היא כאמור זכות אופרטיבית. בצדה, משטר הגנת המידע החדש דורש ממנהלים להוביל תהליכים פנים־ארגוניים מקדימים כדי ליישם אותה, למשל באמצעות ממשק משתמש באתר או מערך שירות לקוחות. אלו התהליכים שיאפשרו להביא את מימוש הזכות אל הפועל. שלוש נקודות הזמן הללו – שלב ההכנה, שלב הממשק עם המשתמשים ושלב היישום של רצון מושאי המידע – מהוות תהליך הממוקד במוטבי אסדרה. בהקשר אחר, משטר הגנת המידע החדש מחייב מנהלים ליישם תהליכים ואמצעים שישמרו על האינטרסים והזכויות של מושאי המידע. כך, למשל, המשטר החדש מתייחס לצורך לשמור על האינטרסים של מושאי המידע בהקשר של קבלת החלטות אוטומטיות על בסיס חוזה או הסכמה מדעת.[107] משטר הגנת המידע דורש מהמנהלים להפעיל את התהליכים והאמצעים הללו באופן שוטף, וזאת גם אם הלכה למעשה אף מושא מידע לא יבקש, למשל, להפעיל את זכותו ויתנגד לעיבוד אוטומטי של המידע על אודותיו.

5. כלי מדיניות אופרטיביים הממוקדים במאסדרים

משטר הגנת המידע החדש מספק גם כלי מדיניות המתמקדים בפעילותם של המאסדרים ומעצימים את כוחם לפעול. כלי מדיניות אופרטיביים הממוקדים במאסדרים נועדו לאפשר למאסדרים להתמודד עם מצבים לא צפויים בזמן שהארגונים בשוק אוספים ומעבדים מידע. כך, למשל, ארגונים נדרשים להעביר מידע ייחודי אל המאסדר. מידע זה לא תמיד יגיע אל מושאי המידע. דוגמה לפער זה באה לידי ביטוי בסוגיות של פריצה למידע: המשטר החדש מקדם יישום של תהליכים לזיהוי פריצות למידע ושליטה בהן, שהם למעשה כלי מדיניות תהליכיים ממוקדי אכיפה עצמית;[108] בה בעת הוא גם מבחין בין שני סוגי דיווחים הנוגעים לפריצה למערכות ולמידע.[109] בשונה מתהליכי המניעה, עצם החיוב בדיווח הוא כלי מדיניות אופרטיבי. זיהוי ושליטה בפריצות מידע מחייב ארגונים, במקרה של פריצה למערכת, לדווח על הפריצה למאסדרים בתוך זמן קצר. בשונה, הדיווח הנדרש למושאי המידע מוגבל יותר וכולל חריגים ברורים לחובת הדיווח.[110] דוגמה נוספת ובולטת נוגעת לחובה המוטלת על ארגונים שאינם אירופיים למנות נציג באחת ממדינות האיחוד שבהן הארגון מעבד מידע על אודות מוטבי האסדרה. תפקידו של אותו נציג הוא לייצג את הארגון ואת מקבל ההחלטות בו

107 ראו ס׳ 22.3 ו־35.7(d) ל־GDPR.

108 בין היתר, כאשר ס׳ 32–34 ל־GDPR מתייחסים לחובת הדיווח על פריצות מידע ולחובת יישום אבטחת מידע בארגון, הסעיפים מתייחסים גם להשלכות של יישום נכון של אמצעים ארגוניים וטכנולוגיים על חובת הדיווח. ראו גם *Guidelines of The Working Party On the Protection of Individuals with Regard to the Processing of Personal Data on Personal Data Breach Notification Under Regulation 2016/679*, 18/EN WP 250 (Feb. 6, 2018).

109 ס׳ 4(12) ל־GDPR מגדיר personal data breach כפריצת אבטחה שמובילה באופן מכוון או לא חוקי להרס, לאיבוד, לשינוי, לחשיפה לא מותרת או לגישה למידע אישי שמועבר, נשמר או מעובד. דוגמאות לפריצה הן, למשל, גנֵבה או איבוד של מכשיר אלקטרוני שבו מאגר עם מידע אישי, אך גם מצבים שבהם התבצעה הצפנה של המידע על ידי תוכנת ransomware או סיסמה שנשכחה ואין יותר גישה למידע.

110 השוו את ס׳ 33 לס׳ 34 ל־GDPR.

בכל הנוגע למחויבויות של הארגון תחת המשטר החדש, ולשמור תיעוד של כלל הפעולות לעיבוד מידע שתחת אחריותו.[111] הבחירה היכן למקם את הנציג בקרב המדינות החברות יכולה להשתנות בהתאם לדרישות המשפטיות של כל מדינה ומדינה, והמאסדרים ומוטבי האסדרה באירופה מקבלים את היכולת להשפיע מקרוב על התהליכים בארגון, תוך קיום אכיפה טובה ויעילה יותר.

6. כלי מדיניות תהליכיים הממוקדים במאסדרים

כלי מדיניות תהליכיים הממוקדים במאסדרים מתמקדים בשלב תכנון הפעילות של הארגונים, ובפועל מעצימים את המאסדר בהשוואה לארגון מושא האסדרה. זאת, משום שהארגון נדרש לפנות אל המאסדר בטרם ימשיך את תכנון פעילותו. אפשר לזהות כמה כלי מדיניות תהליכיים כאלו:[112] קבוצה אחת של כלי מדיניות עוסקת בהעצמת המאסדרים על ידי יכולת לצמצם חוסר ודאות בקרב מושאי האסדרה. במצבים אלו, משטר הגנת המידע למעשה ממקם את המאסדר כמנהיג שוק המוסמך להוציא הנחיות או החלטות לכלל השוק או לחלקו.[113] כך, למשל, המאסדר יכול לכתוב קודי התנהגות ולאשר מראש תניות חוזיות אחידות להעברת מידע.[114] בעזרתם של כלים אלו המאסדר מצמצם את חוסר הוודאות המשפטי לארגונים, וחוסך את הצורך לאשר כל תניה חוזית או תהליך שיובאו לפניו בכל הזדמנות שארגונים יהיו מעוניינים להבטיח את פעילותם. במצב אחר, כלי מדיניות תהליכיים הממוקדים במאסדרים יכולים להעצים אותם על ידי תמרוץ ארגונים לפנות אל המאסדרים ולהתייעץ עמם בשלב שבו מנהלי הארגון עדיין מתכננים את פעילות הארגון. דוגמה בולטת לכלי מדיניות תהליכיים הממוקדים במאסדרים היא BCRs (Binding Corporate Rules).[115] הסדרים אלו מאפשרים לתאגיד בין־לאומי, או לכמה ארגונים המאורגנים כאשכול חברות, להעביר מידע בין מדינות, תוך שהארגון או האשכול מתחייבים לאפשר אכיפה למושא המידע

111 ראו ס׳ 27 ו־30 ל־GDPR.

112 במסגרת משטר הגנת המידע האירופי יש כלי מדיניות המסדירים את דרך הפעולה של מאסדרים מדינתיים שונים ברמה העל־מדינתית. מאמר זה אינו מתייחס בהרחבה לכלי מדיניות אלו; ראו פרק 7 ל־GDPR.

113 ראו פרק 4, חלק 5 ל־GDPR.

114 עד כה אושרו שני מודלים כאלו. ראו Commission Decision 2001/497/EC of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Counties, Commission Decision 2004/915/EC ;under Directive 95/46/EC, 2001 O.J. (L 181) 19 of 27 December 2004, Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data .to Third Countries, 2004 O.J. (L 385) 74

115 *Working Document of The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, at 5-6, 11639/02/EN/ WP 74 (June 3, 2003). ראו גם ס׳ 47 ל־GDPR.

ושיתוף פעולה עם המאסדרים לאחר שאלו אישרו את התניות.[116] אף על פי שההסדר נותן פתרון לארגונים ולאשכול חברות, מי שלמעשה צריך לאשר את התניות הוא המאסדר. בלי המאסדר אין ל־BCR תוקף. בהקשר אחר, לאחר שארגון מבצע סקר סיכונים על פרטיות, אם זוהו סיכונים המנהלים נדרשים לפנות למאסדרים לייעוץ בטרם ימשיכו בתהליך עיבוד המידע.[117] באינטראקציה הזו, הארגון צריך להעביר מידע רלוונטי הקשור לסקר הסיכונים ולעיבוד המידע והמאסדר, מצדו, צריך לייעץ למנהלי הארגון כיצד להפחית את הסיכונים שהתגלו בסקר.

ז. סיכום

משטר הגנת המידע האישי האירופי, שנכנס לתוקף במאי 2018, הביא שינוי משמעותי במשטרי הגנת המידע. משטר הגנת המידע האירופי הישן היה חוד חנית בקביעת סטנדרט הגנת המידע, הן למדינות האיחוד והן למדינות לא־אירופיות, אך הוא יצר מגוון רחב של משטרי הגנת מידע מדינתיים עם יישום שונה. בשונה ממנו, משטר הגנת המידע החדש מביא עמו הרמוניזציה בהרכב של כלי מדיניות עם דגש על רגולציה תהליכית, בצד אמירות על השלב האופרטיבי של פעילות עיבוד המידע וחיוב של מושאי האסדרה להיצמד לתוצרים של אותם תהליכים. בכך למעשה המשטר החדש קובע עקרונות, מטיל על מושאי האסדרה את האחריות ליישומם ודואג לקבוע לצדם את כלי המדיניות התהליכיים שיבטיחו את יישום המשטר בתוך הארגונים. אמנם, המשטר האירופי החדש יכול היה להטיל את האחריות על מושאי האסדרה בדרך של עקרון אחריותיות שאינו מפרט את דרך יישומו, אך הבחירה באסדרת תהליכים מצפה כי לאור יישום התהליכים שנבחרו על ידי המנהלים, יפתחו המנהלים מדיניות ויישמו בארגון אמצעים שיתמודדו עם התוצרים של תהליכים אלו. שיטת אסדרת התהליכים מבוססת על הציפייה הזו.

במסגרת זו, המשטר החדש דואג גם לחלוקה חדשה של יחסי הכוחות בין השחקנים הפועלים במשטר. בצד היישום של אסדרת תהליכים, מושאי האסדרה והמאסדרים קיבלו התייחסות גם בשלב התכנון ולא רק בשלב הביצוע. לשינוי זה השלכה חשובה על הדרך שבה יתפקד המשטר בהמשך. תוך כדי התכנון, יישום התהליכים ופיתוח התכניות, המנהלים יכולים לפנות לרשויות הגנת המידע, להתייעץ איתן או לאשר את פעילות עיבוד המידע שלהן. על המנהלים גם ליישם תהליכים שיאפשרו למושאי המידע לממש את זכויותיהם. כל

116 בשלב מסוים נוצרה בעיה כי ארגונים בין־לאומיים נדרשו לאשר את ה־BCRs עם כל אחת ואחת מרשויות הגנת המידע האירופיות אף שבקשתן זהה. כפתרון, אפשר האיחוד האירופי לאחד את התהליך דרך טופס אלקטרוני אחיד. *Recommendation 1/2007 of Article 29 Data Protection Working Party on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data,* WP 133 (Jan. 10, 2007). הבהרות נוספות ניתנו בשנת 2008 על ידי ה־WP A 29. *Working Document of Article 29 Data Protection Working Party on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules,* 1271-04-02/08/EN, WP 155 (June 24, 2008). השוו לפתרון שמוצע בס׳ 47 ל־GDPR.

117 ס׳ 36 ל־GDPR.

הפעילות הזו קודמת לשלב הביצוע – השלב שבו המנהלים והמחזיקים מעבדים את המידע האישי הלכה למעשה. בכך ישפיע המשטר החדש הן על ארגונים בין־לאומיים העוסקים בעיבוד מידע ופועלים בין היתר בשוק האירופי, והן על מדינות לא־אירופיות שיתבקשו כעת לעמוד בדרישות תאימות חדשות, תוך שהן נדרשות להמשיך ולהוכיח מדי ארבע שנים את עמידתן לפני הנציבות האירופית.

מעל לכול, משטר הגנת המידע האירופי החדש מסמל מעבר ממצב של אסדרה סביב – ובעיקר על ידי – רשויות הגנת מידע, למשילות סביב כמה שחקנים הפועלים במרחב האסדרה. כתוצאה מכך המשטר החדש מעלה שאלות הנוגעות להאצלת סמכויות לשחקנים שלישיים ולהפעלתן באופן אחראי. לאחר התהליך הפוליטי המשמעותי שעבר האיחוד האירופי, קובעי המדיניות של משטר הגנת המידע החדש הפנימו לתוכו כלי מדיניות תהליכיים העוסקים ביחסי כוחות, בחובות ובזכויות. התוויית יחסי הכוחות באמצעות כלי המדיניות ואימוץ התהליכים לתוך ארגונים הן דרישות שיופנו לכל ארגון – ציבורי או פרטי – שיבקש לאסוף מידע אישי על אודות אזרחים אירופים ולעבד אותו. מדובר בהשלכה בעלת היקף נרחב על הזכות לפרטיות. רבות מהזכויות המרכיבות את הזכות לפרטיות במידע הן זכויות שניתנות למושאי המידע בשלב הביצוע של עיבוד המידע, אך השינוי האסדרתי שאליו שואפים כלי המדיניות החדשים כולל מעבר למשטר שמתכנן מראש את ההגנה על המידע האישי של אנשים. אמירה זו מסתמכת במידה רבה על אמון במנהלים של הארגונים שמעבדים מידע אישי ועל הצלחתם ליישם נכונה את התהליכים ולהפנימם בארגון ובקרב העובדים. אף שמשטר הגנת המידע החדש עושה סדר ביכולות האכיפה המאוחדות של רשויות הגנת המידע וביכולת להטיל קנסות מנהליים גבוהים, ואף מעניק זכויות נרחבות למושאי המידע – בפועל המנהלים הם האחראים העיקריים להגנת המידע ולפרטיות.

שינוי זה אינו עניין פשוט. במאמר זה טענתי כי המסגרת החקיקתית שנכנסה לתוקף בשנת 2018 מסמלת מעבר למשטר חדש, שבלבו עקרון האחריותיות ואסדרת תהליכים. השינוי נעשה באמצעות הבניה של כלי מדיניות תהליכיים בצד כלי מדיניות המכוונים לשלב הביצוע של עיבוד המידע. הכנסת כלי מדיניות אלו, המיישמים את עקרון האחריותיות לארגונים, נבעה מפער המידע הניכר שהיה בין השחקנים במרחב האסדרה של הגנת המידע. הכלים גם מבנים את יחסי הגומלין בין השחקנים הפועלים במרחב המדיניות של הגנת המידע. כתוצאה מכך, ההתמקדות בשיטה תהליכית ולא רק בעקרונות עיבוד מידע תקין גרדא מראה כי חלק מהאינטראקציות בין השחקנים יעסקו בתוצרים של אותם תהליכים ועמידה בהם לאורך זמן. במיוחד יש לזכור כי אסדרת תהליכים אולי מעבירה את עלויות האסדרה לשחקן שמחזיק במידע הקרוב ביותר לסיכונים לפרטיות בשטח, אך המאסדרים הם שנדרשים לשמר את יכולתם להעריך באופן עצמאי את אמינות המידע ואת איכות התהליכים שיתקבלו לבחינה. לתוצרים אלו יש חשיבות ביכולת להתמודד עם האתגרים שחברת המעקב מציגה, ביכולת לפקח על אלגוריתם חכם ובתכנון לקראת עליית האינטרנט של הדברים.