

דיני הטלקומוניקציה הבינלאומית ודיני סייבר בינלאומיים

מאת

דבורה האוסן-כוריאל

תדפיס מתוך:

משפט בינלאומי

רופי סיבל ויעל רונן

מהדורה שלישית



המכון למחקרי חקיקה ולמשפט השואתי ע"ש הרי ומיכאל סאקר
האוניברסיטה העברית בירושלים, הפקולטה למשפטים



דיני הטלקומוניקציה הבינלאומית ודיני סייבר בינלאומיים

דבורה האוסן-כוריאל*

25.1 מבוא כללי

העברת מידע באמצעות תשתיות תקשורת בינלאומית מהווה היום מרכיב מרכזי בפעילותם של מדינות, ארגונים, חברות ויחידים. בהקשרים רבים – המדיני, הכלכלי, החברתי, המדעי, החינוכי והצבאי – השימוש בתשתיות האמורות הינו כיסוד חיוני בתפקוד השוטף של כל אלה.¹ דיני הטלקומוניקציה, או דיני "הבזק", עוסקים בשני ההיבטים העיקריים של השימוש בתשתיות תקשורת: הפונקציונלי והמהותי. ההיבט הפונקציונלי מתייחס לנומרות שחלות על הפעלתן בפועל של תשתיות בזק, כגון בהעברה בין מדינה למדינה של טלפוניה סלולרית (mobile roaming). ואולם ההיבט המהותי עוסק בנומרות התומכות, בין השאר, בגישה לתשתיות אלה שהיא יעילה, מוגנת, ושוויונית. בעת האחרונה, הגישה האמורה מתחשבת גם בשמירה על זכויות יסוד כגון חופש הביטוי, חופש העברת המידע, והגנה על פרטיות המשתמש.² מעבר לכך, נורמות של דיני הבזק הבינלאומיים מחייבות התנהלותן של מדינות בכל הנוגע לשימוש במשאב הספקטרום האלקטרו-מגנטי (להלן – הספקטרום), שבו מתקיימת התקשורת האלחוטית. בשנים האחרונות חל שינוי משמעותי ואף מהפכני ברמת השימוש בתשתיות הבזק הגלובאליות האמורות. ניצולן רק לצורכי תקשורת דרך האינטרנט (שימוש אחד מבין רבים של תשתיות בזק) עלה מפחות מ-1% מאוכלוסיית העולם בשנת 1995 ל-43% בשנת 2015.³ דהיינו, כיום יש כ-3.2 מיליארד בני אדם שהם משתמשים פעילים בתשתיות הבזק הבינלאומיות, בנוסף למיליארדי המכונות והחפצים שמחוברים לרשת האינטרנט ולרשות תקשורת אחרות (internet of things). תופעה זו, המכונה "המהפכה הדיגיטלית" או "מהפכת המידע",⁴ מצטרפת לשימושים

* תודתי נתונה לרם לוי, קרן שחר בן-עמי ודניאל רוזן על הערותיהם המועילות; ולמשה גלילי, יזהר טל, מרגית כהן, דניאל רוזן ואיל רק על הערותיהם המועילות לגרסה המקורית.

1 ה-World Economic Forum קרא לתופעה זו, המתארת את התלות הנוכחית במערכות תקשורת גלובאליות, *World Economic Forum, GLOBAL REPORT (2014) digital hyperconnectivity*.

2 למשל Patrick Breyer, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 EUR. L. J. 365 (2005); Australian Human Rights Commission, *Background Paper: Human Rights in Cyberspace*, September 2013.

3 נתוני ה-ITU, *ICT FACTS AND FIGURES (2015)*.

4 ראו NICHOLAS NEGROPONTE, *BEING DIGITAL (1995)*, שתיאר את המהפכה הדיגיטלית בתחילתה.

המסורתיים יותר של תשתיות הבזק, כגון טלפוניה, ומשלבת בהם פעולות בזק מסוג חדש ולא צפוי, כגון פשע מקוון ופריצות מקוונות לאתרים ומאגרי המידע של חברות פרטיות, מוסדות ממשל ויחידים, שהפכו לעניין של שגרה. על כן, היא מחייבת התמודדות משפטית ממוקדת במרחב חדש של פעילות אנושית שנוצרת כעת בנוסף למרחבי היבשה, הים, האוויר והחלל – והוא מרחב הסייבר.⁵

אמנם השימוש בתשתיות הבזק ופעילות במרחב הסייבר נערכים הן בתוך גבולות המדינה והן מעבר להם, אך עניינו של המשפט הבינלאומי מתעורר בעיקר כאשר השימוש בתשתיות הבזק חוצה גבולות מדינתיים.⁶ פעולות הבזק שכרוכות בהעברת מידע מעבר לגבול המדינה דורשות תיאום בין-מדינתי הדוק ומתמשך, על מנת לאפשר תקשורת רצופה ואמינה. תיאום זה מחייב הסכמה בין-מדינתית לגבי כל מרכיבי מערכות הבזק: נורמות משפטיות, הסדרים מנהליים, סטנדרטים טכניים, ואכיפת כל אלה.⁷ עם מהפכת המידע והשימוש הנפוץ של מרחב הסייבר, מתעורר גם הצורך לטפל בסוגיות חדשות כגון שמירה על זכויות יסוד במרחב הסייבר; המתח בין שמירת פרטיות המידע לבין שיקולי בטחון; משילות באינטרנט (internet governance); הגנה על תשתיות קריטיות; ודיני המלחמה במרחב הסייבר.⁸ פרשת Sony שאירעה בסוף שנת 2014 מדגימה חלק מהאתגרים המשפטיים החדשים במרחב. באותו המקרה, צפון קוריאה יזמה או תמכה ביוזמה של קבוצה בשם Guardians of Peace לפלוש לאתרים ולקבצים אלקטרוניים של החברה האמריקאית, לכאורה כדי לגרום לבעלי החברה להימנע מהקרנת סרט שמשפיל את מנהיג צפון קוריאה. הקבצים שנפרצו כללו מידע עסקי ומסחרי של החברה, כמו גם מידע אישי על אודות עובדיה וסקפיה. כאשר הפורצים פרסמו את המידע ברבים, גורמי ממשל בארצות הברית, כולל הנשיא אובמה, התייחסו לאירוע כעניין של בטחון המדינה, האשימו את צפון קוריאה בהפרה חמורה של זכויות אדם ואף הטילו סנקציות כלכליות עליה כתוצאה מהאירוע. בין שאר השאלות המשפטיות שעוררה הפרשה, נדונו שאלות של ייחוס

5 *War in the Fifth Domain*, THE ECONOMIST (July 1, 2010)

6 ואכן, בתוך גבולות המדינה, פעילות זאת והסדרתה שייכת באופן מסורתי ל-domain réservé של מדינות, בהדגש על העקרונות של ריבונות וסמכות טריטוריאלית. Sabine von Schorlemer, *Telecommunications, International Regulation*, in MAX PLANCK ENC'Y. PUB. INT'L L (2009). הסוגיה של ריבונות המדינה במרחב הסייבר מעוררת שאלות רבות: ראו, למשל, את חוות הדעת של ידידי בית המשפט בפרשת מיקרוסופט נגד ארצות הברית במהלך 2014: Briefs of Amicus Curiae, Republic of Ireland and Brennan Center, ACLU, and Electronic Frontier Foundation, In Re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 14-2985, Documents 164 and 82, US Court of Appeals for the 2nd Cir., 2014 (להלן – פרשת מיקרוסופט).

7 בעניין שיתוף הפעולה הנדרש במישור הבין-מדינתי כותב מלנצ'וק כי מעטים התחומים שבהם, מסיבות טכניות בעיקרן, הצורך בשיתוף פעולה בינלאומי הוא כה ברור ואכן יושם בפרקטיקה של מדינות כמו תחום הטלקומוניקציה Peter Malancuk, *Telecommunications, International Regulation*, in MAX PLANCK ENC'Y. PUB. INT'L L 386 (1986).

8 על מגוון הסוגיות במשפט הבינלאומי שעולות במרחב הסייבר, ראו Kristen Eichensehr, *The Cyber Law of Nations*, 103 GEORGETOWN L.J. 317 (2015). לגבי הגדרת המושג "מרחב הסייבר", ראו החלטת ממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011).

מעשים במרחב למדינה והטלת אחריות לביצועם, הגדרת הגבולות של המושג "שימוש בכוח" במרחב, ומגוון האפשרויות שעומדות לרשותה של מדינה במקרה דומה.⁹ שני המשטרים שנדונים בפרק זה חלים על העברת מידע ופעילות נוספת שמתבצעת באמצעות תשתיות תקשורת. דיני סייבר בינלאומיים והממשק בינם לבין דיני הטלקומוניקציה מהווים סוגיות חדשות של המשפט הבינלאומי, הנמצאות עדיין בהתפתחות. בפרק זה נסקור קודם כל את דיני הטלקומוניקציה ולאחר מכן דיני הסייבר והממשק בין שני המשטרים, בהתייחס גם להתפתחויות רלוונטיות שלהם בישראל.

25.2 דיני טלקומוניקציה בינלאומית

דיני הבזק הבינלאומיים חלים על תשתיות תקשורת החוצות גבולות מדינתיים, המורכבות מרשתות פיזיות ווירטואליות הפרושות על פני כדור הארץ. הן כוללות כבלים, לוויינים, תדרי הספקטרום, תחנות ממסר וציוד קצה כמו מחשבים וטלפונים ניידים ומכשירים רבים נוספים.¹⁰ תשתיות התקשורת מאפשרות העברה למרחקים של מידע מסוגים שונים – קולי, ויזואלי ונתונים – ברמה גבוהה של מהימנות ומהירות.¹¹ בעקבות המצאת הטלגרף והטלפון (1844 ו-1876, בהתאמה) החלו מדינות אירופה המערבית לגבש כללים להסדרת תקשורת הבזק ביניהן. ייסוד איגוד הטלגרף הבינלאומי בשנת 1865 יצר לראשונה מסגרת רב-צדדית ומחייבת ליישום ופיתוח כללים אלה.¹² בהתחלה הייתה התייחסות נפרדת לתקשורת קווית (הטלפון) ואל-חוטית (הטלגרף האלחוטית) במישור המשפטי והמנהלי, וארגונים רב-צדדיים נפרדים נוסדו כדי להסדיר כל תחום.¹³ בשנת 1932 השתלבו שתי המגמות למנגנון הסדרתי אחיד, ה-International Telecommunication Union או ITU.¹⁴ חוקת ה-ITU מגדירה עבור 193 המדינות החברות בארגון מושגי יסוד כגון "פעולת הבזק" (telecommunication), "שירות בזק בינלאומי" (international telecommunication service) ו"הפרעה מזיקה" (harmful interference), עליהם חל ההסדר הבינלאומי שהתפתח תחת חסותו –

- 9 ראו Statement by the Press Secretary on the Executive Order Entitled 'Imposing Additional Sanctions with respect to North Korea' (Jan. 2, 2015).
- 10 מרכיבים אלה של תשתית התקשורת אינם תמיד גלויים לעין המשתמש. כבלים הם צינורות פיזיים, המונחים מתחת לאדמה ולים, ועשויים חוטי מתכת או סיבים אופטיים. לוויינים סובבים את כדור הארץ בגבהים שונים. הספקטרום, שבאמצעותו מועברת תקשורת אלחוטית, הוא משאב טבעי הנמצא בתחום האווירי, המורכב משדות חשמליים ומגנטיים; תחנות ממסר מאפשרות העברה של תקשורת מנקודה לנקודה; ציוד קצה הוא המכשיר המאפשר תקשורת שנמצא בידי המשתמש, כגון מכשיר טלפון או מחשב.
- 11 שתי השיטות הנפוצות של העברת מידע בתשתיות בזק הן האנלוגית והדיגיטלית. מידע דיגיטלי מקודד באופן בינארי, באמצעות ספרות ופעימות של גלים אלקטרו-מגנטיים.
- 12 עשרים מדינות חתמו על אמנת פריס מיום 1865 17.5.1865 (130 CTS 198) George Coddin, *International Restraints on the Use of Telecommunications: The Role of the ITU*, in TELECOMMUNICATIONS: AN INTERDISCIPLINARY TEXT 2 (Leonard Lewin ed., 1984).
- 13 ה-International Radiotelegraph Conference בשנת 1865 וה-International Telegraph Union בשנת 1865.
- 14 ה-ITU הינו סוכנות מיוחדת של האו"ם מאז שהסכם בין שני הגופים נכנס לתוקף בשנת 1949 (U.N.G.A. Res. 124(II) (Nov. 15, 1947)).

ושכוללת היום גם התייחסות להעברת מידע במרחב הסייבר.¹⁵ המושג "פעולת בזק", למשל, מוגדר בצורה רחבה שאומצה על ידי מדינות רבות, כולל ישראל, בחקיקה הלאומית: "שידורים, העברה או קליטה של סימנים, אותות, כתב, צורות חזותיות, קולות או מידע, באמצעות תיל, אלחוטי, מערכת אופטית או מערכות אלקטרומגנטיות אחרות".¹⁶ לפי הגדרה רחבה זו, כל העברה של מידע באמצעים טכנולוגיים מהווה פעולת בזק, עליה חלות הנורמות הקבועות במסמכי היסוד של ה-ITU.¹⁷ ובכך הוכפפה להסדר בינלאומי אחיד כל פעולת בזק בינלאומית, לרבות שידורי לוויין ישירים, שידורי רדיו וטלוויזיה, שיחות טלפון, העברת נתונים בין מחשבים, ניווט מטוסים וספינות, משלוח דואר אלקטרוני, מחקר אסטרונומי, GPS ותקשורת בין חובבי רדיו. יודגש כי רמת התיאום והאכיפה של הסדרי ה-ITU היא גבוהה באופן כללי. בנוסף לאימוץ הגדרות היסוד של ITU במשפט המדינתי דוגמאות של הסדרי ה-ITU שאומצו באופן נרחב הן תיאומי התדרים שמתקיימים באופן קבוע בין מדינות, על מנת למנוע הפרעות לתקשורת אלחוטית; תיאום מסלולי לוויינים; העברת תקשורת טלפונים ניידים בין מדינות (roaming); ומתן קדימות לתקשורת חירום.¹⁸ בנוסף למשטר המשפטי שבמסגרת ה-ITU, התפתחו תחת חסות הארגון נורמות מהותיות ייחודיות. אלה כוללים החובה לנצל את משאב הספקטרום ומסלולי לוויין באופן שוויוני וכמשאב בינלאומי משותף; תכנון הספקטרום הגלובלי לטווח ארוך; פיתוח הטלפוניה ניידת; תכנון המשאב של מספרי טלפון,¹⁹ וניהול תשתיות בזק בחלל.²⁰

25.3 מקורות הדין והנחות יסוד משתנות

דיני הבזק הבינלאומי מרוכזים בעיקר במסמכי היסוד של ה-ITU.²¹ הנחת היסוד ההיסטורית שעל בסיסה התפתחה מערכת הדינים האמורה הייתה כי השליטה הבלעדית של המדינה על העברת כל מסר ומידע בתוך שטחה, על שיגור מידע מעבר לגבולות מדיניים ועל קליטתו פנימה – היא מרכיב של ריבונותה.²² הנחה זו מציבה אתגרים בעת הנוכחית. לצד הקשיים הטכניים בשליטה ופיקוח מדינתי על זרימת המידע הבין-אישית והבין-לאומית, מתגבשת בשנים אלה גם

- Constitution and Convention of the International Telecommunication Union as amended by the 15
2010 Plenipotentiary Conference, ITU BASIC TEXTS (2011) (להלן – החוקה והאמנה).
- 16 חוק התקשורת (בזק ושידורים), התשמ"ב-1982 (להלן – חוק התקשורת).
- 17 ס' 4 לחוקה קובע שמסמכי היסוד הם החוקה, האמנה והתקנות האדמיניסטרטיביות.
- 18 החוקה והאמנה, לעיל ה"ש 15.
- 19 על ההסדרה הבינלאומית של הבזק, באופן כללי, ראו von Schorlemer, לעיל ה"ש 6, ו-Nandasiri Jasantuliyana, *The Future of International Telecommunications Law, in* LEGAL VISIONS OF THE 21ST CENTURY 8 (Antony Anghie and Garry Sturgess eds., 1998).
- 20 על האתגרים האמורים ראו Joshua Pila, *Access to Global Telecommunications: A Comparative Discussion of the International Legal Issues Confronting the Telecommunications Relay Service*, 11 INT'L J. OF COMM. LAW AND POLICY 3 (2006).
- 21 החוקה והאמנה, לעיל ה"ש 15.
- 22 von Schorlemer, לעיל ה"ש 6; ראו גם החלטה 37/92 של העצרת הכללית בדבר שידורי לוויין ישירים Convention Relating to the Distribution of Programme-Carrying (A/RES/37/92, 10.12.1982) Signals Transmitted by Satellite, 1144 U.N.T.S. 3.

זכות לתקשורת של הפרט במישור הבינלאומי, הקשורה באופן ישיר ליכולות הטכניות המוגברות של היחיד להעביר מידע מעבר לגבולות מדינתו.²³ שתי התפתחויות אלו מעוררות שאלות חדשות, בתחומי דיני הבזק כמו בתחומים אחרים, בנוגע לשמירה על ריבונות המדינה בתחומי התרבות, השפה, המשטר מדיני, ואף הביטחון הלאומי.²⁴ כמו כן, בעלותה הבלעדית של המדינה על תשתיות הבזק הנמצאות בשטחה אינה מובנת מעליה, כפי שהייתה בעבר. כך, תשתיות בינלאומיות כגון רשתות טלפוניה ולווינים שהתקיימו בעבר רק בבעלות מדינתית, מתפתחות כיום כמיזמים פרטיים. בנוסף לכך, אחסון מידע מכל הסוגים בענן (cloud computing and data storage),²⁵ או בשרתים מעבר לגבולות המדינה, הפכו לשגרה המעוררת שאלות משפטיות רבות ומעניינות.²⁶

שתי הבחנות נוספות שמאפיינות את דיני הבזק המסורתיים משתנות כעת באופן משמעותי, ההבחנה המסורתית בין תקשורת קווית לאלחוטית²⁷ וההבחנה בין ההסדרה של תשתיות תקשורת לבין המידע והתכנים שעוברים בהן. בעבר חלו נורמות משפטיות נפרדות על כל אחת מן הסוגיות האמורות. אמנם יש התלכדות (convergence) של כל סוגי התשתיות וסוגי המידע שעוברים בהן בעידן הנוכחי, אבל ההבחנות המקוריות ממשיכות להשפיע על הסדרת התחום ברמה הבינלאומית והמדינתית. למשל, קיימת מחלוקת בין מדינות בנוגע לזכותם של ספקי שירות בזק להבדיל בין סוגי מידע, סוגי לקוחות וסוגי ציוד קצה מבחינת מחיר השירות כללי הגישה לתשתיות הבזק (הסוגיה של "נייטרליות ברשת" או network neutrality).²⁸ בנוסף,

- 23 הזכות נוסחה לראשונה בס' 19 להכרזה האוניברסלית בדבר זכויות האדם (UNGA Res. 217 (III) (1948), ומוצאת ביטוי באמנה האירופית להגנת זכויות אדם וחירויות יסוד (European Convention for the Protection of Human Rights and Fundamental Freedoms (213 U.N.T.S. 211) ; באמנה האמריקאית בדבר זכויות אדם (American Convention on Human Rights, 1144 U.N.T.S. 123) ; באמנה בדבר זכויות אזרחיות ומדיניות, כ"א 31, 269 (בתוקף לגבי ישראל מ-1992) ועוד.
- 24 יש דוגמאות רבות להתפוררות הגבולות המסורתיים בהקשר זה. ראו, למשל, על החשש כי אזרחים רוסים תקפו מערכות תקשוב של אסטוניה ב-2007, Binoy Kampmark, *Cyber warfare between Estonia and Russia*, 289 CONTEMPORARY REVIEW 288 (2007). פרספקטיבה מעניינת לגבי חופש הביטוי והזכות להעביר מידע מצויה ב- International Law Association, Rule of Law and Freedom of Expression: Islamic Law Perspectives 244–293 (2014) (להלן – דוח ה-ILA).
- 25 "מחשוב ענן" מאפשר שיתוף תשתיות תקשורת ומחשוב למספר רב של משתמשים, ומאפשר אחסון של כמויות גדולות של מידע (big data). PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING (2011).
- 26 פרשת מיקרוסופט, לעיל ה"ש 6.
- 27 לעיל ה"ש 13; Codding, לעיל ה"ש 12, בעמ' 4–9. שרידים של ההבחנה הראשונית נמצאים בפרק VII לחוקת ה-ITU, המתייחס באופן נפרד לתקשורת אלחוטית. ההבחנה בין תשתיות ותכנים נשמרת אף היא בחוקה.
- 28 דברי ההסבר של הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 58) (איסור הגבלה או חסימה), התשע"ג–2013; ופרק 1 לחוק התקשורת.

הסוגיה של חסימת תכנים שעוברים בתשתיות בינלאומיות על בסיס אידיאולוגי, תרבותי או דתי שנויה במחלוקת ואינה מוצאת פתרון הולם.²⁹

25.4 התפתחויות בדין ובהיקף תחולתו

דיני הבזק הבינלאומי מוסדרים בארבע מסגרות עיקריות: (1) הדין הכללי; (2) מערכות נורמטיביות מיוחדות שחלות כדין מיוחד (*lex specialis*) על סוגי תקשורת ספציפיים, כגון תקשורת לווינית; (3) הסדרים של דיני בזק אזוריים, כמו במקרה של האיחוד האירופי; ו-(4) סחר בשירותי בזק במסגרת איגוד הסחר העולמי (WTO). בחלק זה נסקור קודם את מסגרת הדין הכללי כפי שהיא מתבטא במבנה והסמכויות של ה-ITU; אז נפנה לבחינת שלוש המסגרות הנוספת כפי שהן מתבטאות בארגוני הלווינים, בהסדרי האיחוד האירופי וב-WTO.

25.4.1 איגוד הבזק הבינלאומי (ה-ITU)

מערכת דיני הבזק האמורה החלה להתגבש במאה התשע-עשרה, בעקבות הצורך לקבוע כללים אשר יאפשרו תקשורת בינלאומית באמצעות מכשיר הבזק המודרני הראשון: הטלגרף. כמה שנים לאחר ייסוד ארגון הטלגרף הבינלאומי ב-1865, ומחשש לכשל בתקשורת בשעת חירום כגון זה שתרם לאסון הספינה טיטאניק בשנת 1912, הכירו מדינות בהכרח להגיע להסדרים בנוגע לתקשורת אלווית, ובמיוחד תקשורת במצבי חירום. בכנס שהתקיים במדריד בשנת 1932 אוחדו ההסדרים וה-ITU המאוחד הוכר כארגון הסדרה המרכזי של דיני הבזק הבינלאומי. מאז, עבודתו בקביעת מדיניות, הסדרה, תקינה, ופיתוח של הבזק הבינלאומי היא מרכזית ומובילה.³⁰ כיום, ל-ITU ארבעה תפקידים: קביעת נורמות מחייבות בתחום הבזק; גיבוש סטנדרטים טכנולוגיים ותפעוליים; ניהול משאב הספקטרום; והפצת מידע וסיוע למדינות מתפתחות.³¹ מסמכי היסוד שקובעים תפקידים אלה ומפרטים אותם מעט שונים מאלה הנהוגים בארגונים בינלאומיים. קיימות חוקה ואמנה (Constitution and Convention) שעוברים תיקון בכנסי המליאה שמתקיימים פעם בארבע שנים.³² בנוסף, תקנות מנהליות (Administrative Regulations) קובעות את אופן ביצוע החוקה והאמנה ברמה התפעולית: בהתאם להבחנה המסורתית בין תקשורת קווית ואלווית, תקנות הבזק (Regulations International Telecommunication) מתייחסות לתחום התקשורת הקווית; ותקנות הרדיו (Radio Regulations) לתחום התקשורת האלווית.³³ העבודה המקצועית ב-ITU מתחלקת בין שלושה מגזרים (sectors),

29 ראו, למשל, Charles Arthur, *Taking down ISIS material from Twitter or YouTube not as clear cut*, *as it seems*, THE GUARDIAN (June 23, 2014) "ITU Radio Regulations Board urges Iran to end interference hampering EUTELSAT satellite operations," ITU Press Release (March 26, 2010).

30 ב-ITU חברות 193 מדינות. על פעילות הארגון, ראו Alfons Noll, *The ITU in the 21st Century*, 5 *SINGAPORE J. OF INT'L & COMP. L.* 63 (2001) בעמ' 369-370.

31 Coddling, לעיל ה"ש 12.

32 לעיל ה"ש 15.

33 כל 4 מסמכי היסוד הם בעלי מעמד של אמנה בינלאומית. בנוגע למעמד התקנות UNITED NATIONS LEGAL ORDER vol. 2, 806 (Oscar Schachter and Christopher C. Joyner eds., 1995).

תחת המזכ"ל: 34 ITU-R לתקשורת אלחוטית; 35 ITU-T לתקשורת קווית; 36 ו-ITU-D לפיתוח שתיהן. 37 ב-1998 נפתחו המגזרים להשתתפותם של גורמים מסחריים ותעשייתיים, דבר שהווה חידוש בכך שחיבר בין החברות מובילות בתעשיית הבזק לבין הממשלות שקובעות את הסדרת התחום. 38 התפתחות נוספת, יותר שנויה במחלוקת, הייתה עיסוק ה-ITU-T בנושאים שנוגעים למשילות באינטרנט בכנס לתיקון תקנות הבזק שהתקיים בסוף דצמבר 2012 וגרם למחלוקת משפטית ומדינית בין המדינות החברות, שטרם הוכרעה. 39

כפי שנראה בחלק הבא, הסמכויות הבינלאומיות הרחבות של ה-ITU משמשות בסיס לעבודתם של גופים נוספים העוסקים בהיבטים מיוחדים של דיני הבזק הבינלאומי. 40 בנוסף, האיחוד האירופי גיבש בשנים האחרונות מערכת ענפה של דיני בזק, הכפופה למערכת ה-ITU; וה-WTO קבע הסדרים בתחום הסחר הבינלאומי בשירותי בזק.

25.4.2 הסדרים בינלאומיים נוספים

במחצית השנייה של המאה העשרים הביאו מספר התפתחויות טכנולוגיות לפיתוח תשתיות בזק גלובאליות מסוג חדש, שהיו אמנם כפופות להסדרת ה-ITU אך לא נכנסו באופן ישיר תחתה. כך, בעקבות הנחת כבל הטלפון הראשון באוקיינוס האטלנטי בשנת 1956 (TAT-1) החלו חברות מסחריות, ולא רק מדינות, להפעיל כ-100 מערכות של כבלים תת-ימיים. 41 לוויין החלל הראשון Sputnik שוגר בשנת 1957, 42 וארגוני הלוויין הרב-צדדיים הראשונים נוסדו בשנות השבעים של המאה העשרים, בראשית דרכם כארגונים בינלאומיים בין-מדינתיים. בשנות התשעים, הם הפכו למיזמים משותפים של מדינות וחברות מסחריות 43 שמשגרים לווייני תקשורת ומסדירים את השימוש המסחרי במערכות לוויין, בכפוף לכללי ה-ITU בענין שיגור

- 34 פירוט הסמכויות נמצא באמנת ה-ITU, לעיל ה"ש 15.
- 35 מגזר הרדיו אחראי על ניהול הספקטרום ומסלולי הלוויין, וממונה על הועדה (allocation) והקצאה (assignment) לשימושיהם השונים. מסגרת זו מחויבת לשמירה על קני מידה סבירים ושוויוניים. מתפקיד זה נובעת החובה לפעול למניעת הפרעה מזיקה.
- 36 מגזר זה אחראי על קביעת תקנים להעברת מידע דרך תשתיות בזק, ומפתח מודלים להתחשבות בין מפעילים.
- 37 מגזר ה-ITU-D אחראי על קידום תחום הבזק במדינות המתפתחות על ידי מתן סיוע טכני ועריכת מחקרים מקצועיים.
- 38 ס' 3 לחוקה; ס' 19 לאמנה, לעיל ה"ש 15.
- 39 Wayne Rash, *WCIT Treaty Talks End in Dubai with Walkout of US Allies*, E-WEEK (Dec. 15, 2012); דבורה האוסן-כוריאלי "העימות בוועידת WCIT-12 בדובאי: על חופש מידע, זכויות גישה ובטחון קיברניטי" משפט ובטחון לאומי (פנינה ברוך-שרביט וענת קורץ עורכות, 2014).
- 40 כגון ארגון התקינה הבינלאומי (ISO), OECD, WIPO, UNESCO, וקבוצת העבודה של האו"ם בעניין בזק במצבי חירום (WGET).
- 41 הגנה על כבלים תת-ימיים המונחים בלב ים מוסדרת בס' 112-115 של אמנת האו"ם בדבר דיני הים מ-1982. ראו גם <http://submarine-cable-map-2015.telegeography.com>.
- 42 לוויין התקשורת הראשון, Telstar, שוגר בשנת 1962.
- 43 מדובר בהתפתחות תקדימים, ראו THE TRANSFORMATION ON INTERGOVERNMENTAL SATELLITE ORGANIZATIONS (PatriciaMcCormick and Maury Mechanik eds., 2013) ואזכור חוות הדעת של שבתאי רוזן בעמ' 56, הערה 34.

לווינים הארגונים העיקריים. ארגוני הלוויין המובילים כיום הם Intelsat (מאז 2001, ITSO), Inmarsat (מאז 2001, IMSO), Eutelsat, Intersputnik, Arabsat, Palapsat ו-Rascom.⁴⁴ האיחוד האירופי מקדם הסדרת בדיני הבזק באופן שמשלב עם הגישה הכללית של פרק זה, העומדת על שני היבטים של דיני הבזק כעת – הפונקציונלי והמהותי. מדובר באימוץ בשנת 2002 של "סל רגולטורי" המורכב מארבע דירקטיבות תחת דירקטיבת מסגרת (Framework Directive), הקובעות הסדרים מקיפים לגבי תקשורת אלקטרונית (electronic communications) ושמשכיכות להתעדכן ככל שהתקשורת האלקטרונית מתפתחת.⁴⁵ בזכות ההגדרה הרחבה שאימץ האיחוד ומדינותיו, הסל מתאים גם לתקשורת בזק במובנו המסורתי וגם לפעילות במרחב הסייבר. למשל, הדירקטיבות חלות על הסוגיות של שירות אוניברסלי במערכות בזק, שמירת הפרטיות של משתמשים, כללי הגישה למערכות ורישוי של מפעילי מערכות וספקי שירותים.⁴⁶ בשנת 2013 פרסמה מועצת אירופה הצעה לדירקטיבה נוספת בנושא בטחון מידע ורשתות (information and network security), והמדינות החברות אמורות לקבלה עד סוף שנת 2015.⁴⁷

ההפרטה המתמשכת של מגזר הבזק משתקפת גם בכללים של ארגון הסחר העולמי (World Trade Organization – WTO) שחלים על הספקת שירותי בזק בסיסיים. הסכם הגאט"ס שנחתם בשנת 1994 כולל נספח בנושא שירותי בזק, המשקף את גישת ה-WTO כי תחום הבזק הוא גם תחום מסחרי בפני עצמו; וגם משמש תחום תשתית של מערכת הסחר העולמית. הפרוטוקול הרביעי של הסכם ה-WTO משנת 1997 יוצר מערכת לפיתוח מגזר הבזק הלאומי, לרבות כללי גישה שוויונית דומים שמזכירים את גישת ה-ITU לסוגיה.⁴⁸ כיום יש, ל-108 מדינות התחייבויות בתחום הבזק במסגרת ה-WTO, כולל ישראל.⁴⁹

44 ראו מסמכי היסוד של ארגוני הלוויין: אינטלסט (909 INT'L LEGAL MATERIALS 10); אינמרסט (5 INT'L LEGAL MATERIALS 1051); יוטלסט (Misc. No. 25, Cmnd. 9069), אינטרספוטניק (862 U.N.T.S. 3); ערבסט (2 Manual on Space Law 345) ופולפסט (NICHOLAS MATEESCO MATTE, AEROSPACE LAW 159 (1982)).

45 אוסף הדירקטיבות והמדיניות נמצא באתר ה-European Agency for Network and Information Security, www.enisa.europa.eu.

46 בית הדין האירופי פסק עד כה בכ-140 פסקי דין בנוגע ליישום הדירקטיבת האמורות. European Commission Guide to the Case Law of the European Court of Justice in the Field of Telecommunications, updated January 2010.

47 Proposal for a Directive of the European Parliament and Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union, Brussels, (Feb. 7, 2013).

48 הפרוטוקול הרביעי הוא חלק ממכלול של הסכמים בתחום הבזק שנכרתו במסגרת ה-WTO בשנות התשעים, כלהלן: Ministerial Decision on Annex on Negotiations on Basic Telecommunications, Fourth Protocol to the GATS Negotiations on Basic Telecommunications, 108 מדינות קיבלו על עצמן מחויבויות במסגרת ה-WTO בתחום הבזק. www.wto.org/english/tratop_e/telecom_e/telecom_e.htm.

49 הדוח של יו"ר סבב השיחות בדוחה מיום 26.5.2008; L. Lee Tuthill and Laura Sherman, *Telecommunications: Can Trade Agreements Keep Up with Technology?* in OPENING MARKETS FOR TRADE IN SERVICES 151 (Juan Marchetti, Martin Roy eds., 2009).

25.5 דיני סייבר בינלאומיים

כאמור לעיל, מערכת המשפט הבינלאומי נדרשת להתייחס לפעילות במרחב הסייבר של מדינות, ארגונים, חברות ויחידים, לרבות הפעילות העוינת שבו. אירועים כמו פרשת סטוקסנט ב-2010,⁵⁰ הפריצה לחברת לוקהיד-מרטיין ב-2011,⁵¹ והניטור האלקטרוני הנרחב שביצע ה-NSA של ארצות הברית ושנחשף על ידי סנודן בקיץ 2013,⁵² מעוררים שאלות חדשות שנוגעות לתחולתן במרחב של סוגיות מסורתיות של המשפט הבינלאומי. למשל, ריבונות ואחריות המדינה, הגנה על זכויות אדם כגון חופש הביטוי ושמירת פרטיות, ודיני המלחמה – כל אלה תחומי משפט שמציבים אתגרי תפיסה ואכיפה בפני מדינות במרחב. אם כן, יחד עם הקידום שמאפשר המרחב, מדובר גם בחשיפות, סכנות ואיומים מסוג חדש.⁵³ אמנם מתגבשת הבנה רחבה לפיה המשפט הבינלאומי אכן חל במרחב, אבל הדרכים שבהן הוא מותאם ומיישם בו עדיין מתגבשות. למשל, הניתוק במרחב בין ריבונות המדינה ושטח פיזי-גאוגרפי מציב אתגרים חדשים גם בתחומים של סמכות שיפוט, הסדרה ואכיפה.⁵⁴ נוסף ונאמר: אמנם הצורך להסדיר פעילות במרחב הוא לכאורה עז ודחוף, בפועל קיים מספר יוזמות הבוחנות את התחולה של תחומי משפט בינלאומי פרטניים במרחב.⁵⁵ כעת, ההסדרים הפורמליים הקיימים במישור הרב-צדדי הם ספורים. חלקם נסקרים להלן, כמו גם תהליכים שעשויים להשפיע על הסדרים רב-צדדיים שיתפתחו בהמשך.

בניגוד לדיני הבזק, המסתמכים על הגדרות ונורמות שמוסדרים במקורות המשפטיים שנסקרו לעיל, בדיני מרחב הסייבר טרם נקבעו הגדרות אחידות של מושגי מפתח כגון "מרחב הסייבר", "מידע", ואפילו המושג "סייבר" עצמו. הגדרת המרחב שנקבעה בהחלטת ממשלת ישראל 3611 מתייחסת למרכיבים הנפוצים בהגדרות רבות של מחשבים, אנשים, מידע, ותקשורת הבזק ביניהם. הגדרה זו קובעת כי מרחב הסייבר הוא "המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה

- 50 Michael Gross, *A Declaration of Cyber War*, VANITY FAIR (April 2011)
- 51 Mathew J. Schwartz, *Lockheed Martin Suffers Massive Cyberattack*, INFORMATION WEEK (May 30, 2011)
- 52 Glenn Greenwald, *NSA Prism program taps into user data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013)
- 53 Michael N. Schmitt, *Introduction*, in NICHOLAS TSAGOURIAS AND RUSSELL BUCHAN, RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 1 (2015); and Nicholas Tsagourias, *The Legal Status of Cyberspace*, שם, בעמ' 13.
- 54 Shabtai Rosenne, *The Perplexities of Modern International Law*, 291 ; 8 ע"ש 8; EICHENSEHR COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt and Brian O'Donnell eds., 2002); Terry Gill and Paul Ducheine, *Anticipatory Self-Defence in the Cyber Context*, Vol. 89, INTERNATIONAL LEGAL STUDIES OF THE US NAVAL WAR COLLEGE 438 (2013)
- 55 David Johnson and David Post, *The Rise of Law on the Global Network*, in BORDERS IN CYBERSPACE (B. Kahin and C. Nesson, eds., 1999)

ובקרה והמשתמשים של כל אלה.⁵⁶ יודגש כי המרכיבים הפיזיים, דהיינו תשתיות התקשורת, המחשבים והמשתמשים, ממוקמים בשטח מדינה ולכן כפופים לסמכות שיפוט מדינתית לפי המבחן הטריטוריאלי (כמו גם מבחיני סמכות שיפוט נוספים). לגבי מרכיב המידע (data), ההכרעה בענין סמכויותיהן של מדינות ספציפיות יותר בעייתית, כיוון שמרכיב זה אינו קבוע בשטח פיזי מסוים, אלא מטבעו חוצה גבולות.

הצעדים הראשוניים לגבש הבנות בין-מדינתיות בין מדינות בנוגע למותר ולאסור במרחב מתקדמים כעת במספר מישורים.⁵⁷ בחלק הזה נסקור 3 יוזמות כאלה: (1) אמנת בודפשט בדבר פשע מקוון משנת 2001; (2) מדריך טאלין למשפט הבינלאומי שחל על לוחמת סייבר משנת 2013; ו- (3) ועדת המומחים של מזכ"ל האו"ם, ה-GGE. מדובר ביוזמות שנועדו לבחון נורמות שיחולו על חלקים ספציפיים של פעילות במרחב, בהיעדר הסדר בינלאומי. סוגיות נוספות שאינם מטופלות בפרק זה כוללות ההתמודדות עם טרור מקוון, הגנה על תשתיות קריטיות, היוזמה של סין ורוסיה לגייס תמיכה ל-International Code of Conduct for Information Security והמחלוקת סביב המשילות באינטרנט (internet governance).⁵⁸

25.5.1 אמנת בודפשט בדבר פשע מקוון משנת 2001

האמנה של מועצת אירופה בדבר הפשע המקוון ("אמנת בודפשט") היא האמנה הרב-צדדית העיקרית שנכרתה עד כה שעוסקת בפעילות מדינתית במרחב.⁵⁹ חברות באמנה מדינות מועצת אירופה ואחרות (רוסיה, ארה"ב, קנדה, יפן) וישראל מצויה בתהליכי הצטרפות. האמנה קובעת לראשונה הגדרות אחידות של עבירות מקוונות ומחייבת אימוץ של הגדרות אלה על ידי המדינות החברות. למשל, בפרק האמנה שמתייחס לעבירות מחשב קיים איסור על גישה למחשב שלא כדין (illegal access), יירוט התקשורת בין מחשבים (illegal interception), והפרעות למידע או עיוותו (data interference). האמנה גם מתייחסת לאחריות תאגידית (corporate liability), נושא חיוני בהקשר של ייחוס מעשים במרחב. מעבר לקביעות הסובסטינטיביות באמנה, היא מחייבת מנגנונים של שיתוף פעולה בינלאומי במישורים של החלפת מידע בין מדינות, עזרה משפטית הדדית באיסוף ראיות והיבטים נוספים של אכיפה. ועדה קבועה, מנחה את המדינות החברות ביישום האמנה, מתאמת ביניהן ומפתחת דפוסי שיתוף פעולה.⁶⁰

56 החלטת ממשלה 3611, לעיל ה"ש 8. אמנם אין הגדרה מוסכמת של המרחב מבחינת המשפט הבינלאומי, אך "מרחב הסייבר" כולל, על פי מרבית התפיסות, את המרכיבים שבהגדרה של ה-Joint Chiefs of Staff של ארצות הברית. הגדרה זאת מתייחסת להעברת מידע, אחסונה ועיבודו דרך מכשירים אלקטרוניים, הספקטרום האלקטרומגנטי, מערכות מרושתות ותשתיות פיזיות (Joint Terminology for Cyberspace Operations, p.15, undated) הגדרות אחרות המקובלות על המחברת מוסיפות את האנשים שמפעילים מערכות אלה.

57 ראו הסקירה של Joseph Nye, *The Regime Complex for Managing Global Cyber Activities*, GCIG (May 20, 2014).

58 המעוניינים בסוגיות אלה מופנים לחומרים הרבים שמתפרסמים באתרי ה-ENISA, ITU, ו-US Tsagourias and Buchan; Department of Homeland Security, לעיל ה"ש 54.

59 Convention on Cybercrime, E.T.S. No. 185, 23.11.2001.

60 ראו את עבודת הוועדה ב-http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp.

25.5.2 מדריך טאלין למשפט הבינלאומי החל על לוחמת סייבר

בשנת 2009 יזם מרכז מצוינות הסייבר של נאט"ו שבאסטוניה (CCDCOE)⁶¹ תהליך לבחינת דיני המלחמה במרחב. היוזמה מצד נאט"ו לא הייתה מקרית: באביב 2007 התרחשה במשך כמה שבועות פעילות עוינת כלפי אסטוניה, מדינה שנחשבה באותה עת אחת ה"מחוברות" מבחינת אחוז האוכלוסיה שניצל את האינטרנט לפעילות מול גורמי ממשל ומסחר, על בסיס שוטף. הפעילות העוינת, חסימת אתרים ממשלתיים ופרטיים והשחתתם.⁶² אירועים אלו, שיוחסו לרוסיה, חשפו חוסר אונים משפטי ותפעולי מובהק מצד אסטוניה ומצד ארגון נאט"ו, שכבר החל בתכנונים להקים באסטוניה את מרכז המצוינות האמור.⁶³ על כן, אירועי 2007 זירזו את הקמת ה-CCDCOE בטאלין בירת אסטוניה.⁶⁴ הוחלט גם ליזום פרויקט בקרב קבוצת מומחים לשם בחינת השאלה העקרונית אם דיני השימוש בכוח ודיני המלחמה, *jus ad bellum* ו-*jus in bello*, חלים במרחב, ואם כן – כיצד. בחורף 2013 פרסמה קבוצת המומחים את מדריך טאלין,⁶⁵ שמסקנתו היא ברורה: דיני המלחמה הקיימים אכן חלים במרחב, וניתן ליישם באופן שמתאים לתכונותיו הייחודיים בשינויים המתחייבים.⁶⁶ המדריך זוכה לתמיכה מצד מדינות ומומחים, כמהלך בינלאומי ראשון לבחינת האפשרות של החלת מערכת דינים בינלאומית מסורתית במרחב.⁶⁷ השלב הבא של העבודה שנקבעה על ידי ה-CCDCOE, המכונה "טאלין 2.0" החל ב-2014. תהליך זה בוחן את התחולה במרחב של מערכות דינים כפופים למערכות דינים אחרות כגון אחריות המדינה, חסינויות, דיני הבזק, דיני החלל וזכויות האדם.

25.5.3 ועדת המומחים של מזכ"ל האו"ם ה-GGE

במסגרת העבודה של הוועדה הראשונה של העצרת הכללית של האו"ם, הגישה רוסיה בשנת 1998 הצעה לטיפול הוועדה בנושא בטחון המידע (information security) ונושאים נוספים בנוגע

61 ראו <https://ccdcoe.org>.

62 בגלל קשיי ייחוס של המעשים לרוסיה באופן רשמי, התוצאה הסופית של בירור האחריות על המתקפות הייתה הרשעה של סטודנט בודד, דמיטרי גלושקביץ, על השחתת האתר של ראש ממשלת אסטוניה. הוטל עליו קנס של פחות מ-USD 2,000. ראו, *Student Fined for Attack against Estonian Website*, COMPUTER WORLD (Jan. 4, 2008).

63 Rain Ottis, *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY (2008).

64 המרכז נפתח באופן רשמי במאי 2008, שנה אחרי המתקפות הרוסיות, אבל הדיונים על הקמתו החלו בשנת 2006 (<https://www.ccdcoe.org/history.html>).

65 TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed., 2013) (להלן – מדריך טאלין).

66 המבוא למדריך טאלין, שם, בעמ' 1–11.

67 MARCO ROSCINI, CYBER OPERATIONS – דינשטיין במבוא ל- AND THE USE OF FORCE IN INTERNATIONAL LAW (2014). לגבי המשך הבירור של דיני מלחמה במרחב, ראו Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269 (2014).

לפעילות מדינתית במרחב.⁶⁸ מאז התכנסו בחסות הוועדה הראשונה והמזכ"ל, שלוש קבוצות של נציגי מדינות החברות בקבוצה (Group of Government Experts Developments in the Field) של נציגי מדינות החברות בקבוצה (of Information and Telecommunications in the Context of International Security – GGE) שבוחנת סיכונים המרחב הקיימים והפוטנציאליים, ודרכי שיתוף הפעולה הבינלאומיות שעשויות לקדם את הביטחון הקולקטיבי במרחב.⁶⁹ ה-GGE פרסם עד כה שלושה דוחות. באחרון, מחודש יוני 2015, קבעה הקבוצה מספר גישות ("views") לפיהן חלות במרחב נורמות של הדין הבינלאומי הקיים. באופן ספציפי נקבע שנורמות שנובעות מריבונות המדינה חלות על פעילות במרחב ("State sovereignty and international norms and principles that flow from sovereignty")⁷⁰. (apply to State conduct of ICT-related activities). ישראל חברה בקבוצת המומחים.

25.6 ישראל

מדינת ישראל בעלת יכולות בזק וסייבר מתקדמות: תשתיות בזק פנים-ארציות מהמפותחות בעולם,⁷¹ שילובן בתשתיות בזק האזוריות וגלובליות;⁷² רמה גבוהה של שימוש בטלפונים ניידים (122 יחידות לכל 100 תושבים);⁷³ וחיבור לאינטרנט (78% מתושביה). תוצר מגזר ה-ICT (Information and Communication Technology) הסתכם בשנת 2012 ב-17% מכלל התוצר במשק;⁷⁴ וה-OECD ממקם אותה במקום יחסית גבוה מבחינת רישום פטנטים בתחום ה-ICT.⁷⁵ ישראל גם מדורגת בין המדינות המובילות בפיתוח יכולות הגנה במרחב הסייבר.⁷⁶

25.6.1 דיני טלקומוניקציה בישראל

חוק התקשורת (בזק ושידורים), התשמ"ב-1982 (להלן – חוק התקשורת) מאמץ בסעיף ההגדרות שלו את הגדרת ה-ITU למונח "בזק", ובכך מסמן מושגית את החיבור של דיני הבזק

- A/RES/53/70, "Developments in the field of information and telecommunications in the context of international security". סקירה כללית של עבודת ה-GGE נמצא ב-<http://www.un.org/disarmament/-topics/informationsecurity> 68
- UN Doc. A/RES/60/45 69
- ראו פרסום לא רשמי של הדוח מיום 27.8.2015, בפס' 28 ו-27, בהתאמה (<http://www.csistech.org/blog/2015/8/27/un-publishes-latest-report-of-the-group-of-government-experts>) 70
- Telecommunications in Israel 2013 באתר של משרד התקשורת (http://www.moc.gov.il/sip_storage/FILES/5/605.pdf) 71
- ראו סקירת ההתפתחויות בתחום בישראל ב-Daniel Rosenne, *Liberalization of Markets and New Regulatory Framework: The Israeli Case*, in THE MEDA AREA FIRST REGULATORY FORUM ON TELECOMMUNICATIONS REFORM IN SHAPING REGULATORY REGIMES (26.4.01) רגולטורית בישראל ראו י' טל, ד' עברי-עומר "הרגולציה של שירותי התקשורת האלקטרונית בישראל" (נובמבר 2009). 72
- ITU Country Profile – Israel (2013) (<http://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx>) 73
- הודעה לעיתונות של דובר הלשכה המרכזית לסטטיסטיקה, 7.11.13. 74
- OECD, Science, Technology and Industry Scoreboard 2013; and OECD, Communications Outlook 2013, pp. 43, 47, 53 75
- McAfee and Security & Defense Agenda, Cyber-security: The Vexed Question of Global Rules (2012). 76

הישראליים למערכת ההסדרה הבינלאומית. בנוסף לחוק זה וחקיקת המשנה הנובעת ממנו, קובעת פקודת הטלגרף האלחוטי [נוסח חדש], התשל"ב-1972 הסדרים ספציפיים לגבי תקשורת אלחוטית.⁷⁷ סעיף 13(4) לפקודה מעניק לשר התקשורת, באופן חריג במשפט הישראלי, סמכות להתקין תקנות "...הנותנות תוקף להוראותיה של אמנה בינלאומית שמדינת ישראל צד לה ולכל תקנה שנעשתה לפיה, במידה שהן נוגעות לטלגרף האלחוטי".⁷⁸ הסדרת התחום של שידורי רדיו וטלוויזיה לציבור, לרבות שידורים למנויים, נבקעה בחלקים הרלוונטיים של חוק התקשורת וחקיקה נוספת כגון חוק רשות השידור, התשכ"ה-1965 וחוק הרשות השנייה לטלוויזיה ורדיו, התש"ן-1990.

ישראל חברה ב-ITU משנת 1948.⁷⁹ התקשורת הבינלאומית לישראל וממנה עוברת דרך מפעילים המספקים שירותי תקשורת בהתאם לרישיונות הניתנים על ידי שר התקשורת,⁸⁰ ביניהם המתגים הבינלאומיים המרכזיים של ישראל והתשתיות שמאפשרות העברת תקשורת בזק אל המדינה וממנה. לווייני התקשורת הישראליים בסדרת "עמוס", שוגרו לראשונה בשנת 1996 (עמוס 1) ושיגורים נוספים מתוכננים לשנת 2016 (עמוס 6).

ישראל מעורבת בארגוני בזק נוספים באופן פעיל. בשנות התשעים של המאה העשרים השתתפה ישראל במשא ומתן על הפרוטוקול הרביעי של ארגון הסחר העולמי בנוגע לשירותי טלקומוניקציה בסיסיים, והייתה בין 69 המדינות אשר הגישו התחייבויות ספציפיות (Specific Commitments) לפתיחת תחום הבזק לתחרות בינלאומית על פי כללי הגאט"ס.⁸¹ בתחום הלוויינים, ישראל הייתה חברה מייסדת של ארגון אינטלסט בשנת 1971 והצטרפה לארגון אינמרסט בשנת 1987. בשנת 1997 ישראל התקשרה עם הקהילה האירופית בהסכם בדבר רכישות ממשלתיות בתחום הבזק;⁸² והצטרפה אותה השנה להסכם בחסות אינמרסט בדבר השימוש בתחנות קרקע במים הטריטוריאליים.⁸³ ישראל משתתפת מאז 1995 בליבון סוגיות הבזק שכרוכות בתהליך ברצלונה בין הקהילה האירופית ומדינות אגן הים התיכון, ומאז 2010 היא חברה בוועדת ה-OECD שעוסקת בתשתיות בזק. לישראל יש כ-30 הסכמים דו-צדדיים עם מדינות שונות בעניין שיתוף פעולה בתחומי הבזק.⁸⁴ מעבר למערכת ההתחייבויות שחלה על

77 הפקודה מבוססת על חקיקה מנדטורית משנת 1937.

78 סמכות השר על פי ס' 13(4) טרם הופעלה, למיטב ידיעת המחברת הסבורה שהתקנת תקנות על פי ס' 13(4) אינה מייצרת את החובה לאשרר אמנות בינלאומיות כאמור, אלא יוצרת מסלול נוסף ומיוחד, המאפשר הפנמת התחייבות בינלאומית של המדינה לתוך המשפט הישראלי. מסלול כזה נדרש בשל האופי המיוחד של דיני ניהול הספקטרום במישור הבינלאומי.

79 אמנה בינלאומית לענייני טלקומוניקציה, כ"א 3, 267.

80 ס' 1 לחוק התקשורת מגדיר את סוגי הרישיונות, שפתוחים לעיון הציבור באתר משרד התקשורת (www.moc.gov.il). רשימת בעלי רשיון נמצאת באתר משרד התקשורת (-191/<http://www.moc.gov.il>).

81 לעיל הערה 48. ישראל בין המדינות שצירפו WTO, Telecommunications Services: Reference Paper, April 24, 1996, https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

82 הסכם בין מדינת ישראל והקהילה האירופית בדבר רכש על ידי מפעילי בזק (10.7.1997, לא פורסם).

83 הסכם בינלאומי לשימוש של תחנות קרקע של אינמרסט בנמלים שבמים טריטוריאליים (16.10.1985). 14 INTERNATIONAL JOURNAL OF MARINE AND COASTAL LAW 432 (1999).

84 הרשימה המלאה ב-http://www.moc.gov.il/sip_storage/FILES/4/3094.pdf.

מדינות האזור מכוח חברותן ב-ITU, לישראל הסדרי תקשורת ספציפיים עם מצרים וירדן. סעיף 6.6 לנספח III של חוזה השלום עם מצרים מחייב את הצדדים לקיים קשרי בזק.⁸⁵ גם בסעיף 16 להסכם השלום עם ירדן סוכם לנרמל קשרי בזק, לרבות קשרי בזק ישירים בין שתי המדינות.⁸⁶ בשנת 1996 נחתם מזכר הבנה בתחומי הבזק והדואר בין ישראל וירדן, שקבע מסגרת משפטית לשיתוף פעולה רחב יותר.⁸⁷

במסגרת הסכם הביניים משנת 1995 נקבעו הסדרי בזק שחלים עד כה בין ישראל לרשות הפלסטינית.⁸⁸ עקרונות ההסדר כוללים חופש פעולה לצד הפלסטיני בכל הנוגע לפיתוח ותכנון מערכות תקשורת ומעניק לרשות סמכות לתת רישיונות בזק, מלבד לתקשורת בינלאומית ישירה.⁸⁹ לישראל שמורה השליטה הבלעדית על הספקטרום, כאשר זכות שימוש בלעדית או משותפת של תחומי תדרים מסוימים מוענקת לצד הפלסטיני.⁹⁰ ניהול הספקטרום ברצועת עזה נשאר בידי ישראל לאחר ההתנתקות בקיץ 2005, בהתאם לתוכנית ההתנתקות המתוקנת שאומצה באוקטובר 2004.⁹¹ מנגנון לתיאום ענייני בזק בין הצדדים קיים (ה-Joint Technical Committee). בניגוד לעמדת ישראל ולמוסכם בהסכם הביניים, הרשות הפלסטינית קיבלה מעמד של משקיף בעל סמכויות מיוחדות ב-ITU.⁹²

25.6.2 דיני הסייבר בישראל

בשנת 2011 הוקם מטה הסייבר הלאומי של ישראל מכוח החלטת ממשלה 3611 מיום 7.8.2011, ובכך נקבע לראשונה גוף ממשלתי שיעודד לרכז את מדיניות הסייבר ברמה הלאומית ולשמש "גוף מטה לראש הממשלה, לממשלה ולוועדותיה, אשר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום [הסייבר], בכפוף לכל דין והחלטות ממשלה". המטה מקדם יוזמות שונות, לרבות יוזמות חקיקה ורגולציה כגון ההקמה של רשות לאומית להגנת סייבר במגזר האזרחי. בתחילת 2015 אישרה הממשלה שתי החלטות בעניין פרויקטים רגולטוריים רחבי היקף שעוסקות בתחום הגנה מוגברת של ישראל במרחב ("קידום ההיערכות הלאומית להגנת מרחב

85 חוזה שלום בין מדינת ישראל ובין הרפובליקה הערבית של מצרים, כ"א 25, 695 (בתוקף מ-1979).

86 חוזה שלום בין מדינת ישראל לבין הממלכה הירדנית ההאשמית, כ"א 32, 271 (בתוקף מ-1994).

87 מזכר הבנה בדבר שיתוף פעולה בתחומי הבזק והדואר בין ממשלת מדינת ישראל לבין ממשלת הממלכה הירדנית ההאשמית (18.1.1996, לא פורסם).

88 ס' 36 לנספח האזרחי, הסדר הבזק שנקבע בהסכם הביניים הישראלי-פלסטיני בדבר הגדה המערבית ורצועת עזה, ושינגטון הבירה, 28 בספטמבר 1995, כ"א 33, 1 (בתוקף מ-1995).

89 הרשות חוקקה חוק תקשורת בינואר 1996. משרד התקשורת פלסטיני העניק זיכיון לחב' פלטל מספר חודשים לאחר מכן.

90 השליטה על הספקטרום היא אחת הסמכויות השמורות למדינה המחזיקה בשטח כתוצאה מתפיסה לוחמתית. ראו בג"ץ LSM Law in the Service Of Man 270/88 נ' מפקד כוחות צה"ל ביהודה ושומרון, פ"ד מב(3) 260 (1988), המצטט את Gerhard Von Glahn בנושא זה. זו הייתה גם גישתם של כוחות המערב לגבי איזורים שהיו תחת כיבוש בעירק ואפגניסטן.

91 תוכנית ההתנתקות המתוקנת, 6 ביוני 2004, ס' 8, באתר של משרד ראש הממשלה (www.pmo.gov.il).

92 Resolution 99 (Minneapolis, 1998) Status of Palestine in ITU; Resolution 99 (Rev. Guadalajara, 2010). ראו החלטות נוספות של מליאת ה-ITU בנושא הפלסטיני ב-ITU BASIC TEXTS, לעיל ה"ש 15.

הסייבר" ו-"קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר).⁹³ החלטות אלו מצויות בתהליכי יישום.

היריעה קצרה מלהכיל פירוט מלא של דיני הסייבר המתפתחים בישראל כעת ונציין רק את עיקרי הדברים. ראשית, כפי שצוין לעיל, החלטת ממשלה 3611 מגדירה בצורה מפורשת את מרחב הסייבר כ-"המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה". ההגדרה רחבה, והניסוח כולל "רשתות תקשורת" הכפופות לדיני הבזק שנסקרו לעיל. דברי חקיקה אחרים שחלים על בפעילות במרחב כוללים, בין השאר, את חוק המחשבים, התשנ"ה-1995 (העוסק בעבירות מחשב); חוק הגנת הפרטיות, התשמ"א-1981 (העוסק בהגנה על מאגרי מידע ופרטיות מידע); חוק להסדרת בטחון בגופים ציבוריים, התשנ"ח-1998 (המחייב גופים מוגדרים בהיערכות מיוחדת מפני מתקפות במרחב); והחלטה 84/ב של וועדת שרים לענייני בטחון לאומי של הכנסת משנת 2002 (העוסקת בהגדרת מערכות ממוחשבות קריטיות ומעניקה סמכויות הנחיה ופיקוח לרשות הממלכתית לאבטחת מידע במשרד ראש הממשלה (רא"ם)).⁹⁴ דברי חקיקה נוספים – חוק העונשין, דיני הנזיקין, דיני החוזים וכו' – עשויים לחול במרחב בהתאמות הנדרשות.⁹⁵ בתי המשפט בישראל התחילו להתייחס לסוגיות שמתעוררות במרחב, כגון הגנה על פרטיות,⁹⁶ "גניבה" של מידע,⁹⁷ מעקב סתר אחר דואר אלקטרוני⁹⁸ והימורים מקוונים.⁹⁹ בנוסף לכך, ובדומה לתהליכים המדינות אחרות של "מגזור" דיני הסייבר, פרסם בנק ישראל בחודש מרץ 2015 הוראה שמחייבת מוסדות בנקאיים שבפיקוחו לאמץ אסטרטגיה ומדיניות להגנת סייבר.¹⁰⁰

25.7 מגמות וסיכום

דיני הטלקומוניקציה הבינלאומית קובעים הסדרים רב-צדדיים מקיפים בנוגע לשימוש בתשתיות תקשורת גלובאליות מכל הסוגים. בממשק בינם לבין דיני הסייבר החדשים, דיני הבזק מספקים בסיס משפטי ורגולטורי איתן ומוכר לחשיבה משפטית חדשה על פעילות במרחב, שהיא בתחילת דרכה. הנורמות המשפטיות שקובעות חלוקת משאבי הבזק באופן יעיל ושוויוני,

- 93 החלטה 2443 (קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר) והחלטה 2444 (קידום ההיערכות הלאומית להגנת הסייבר), שתיהן מיום 15.2.2015.
- 94 החלטה ברשות המחברת.
- 95 אך ראו את דברי השופט רובינשטיין ברע"פ 11066/03 מדינת ישראל נ' רום (פורסם בנבו, 14.5.2007).
- 96 ת"צ (ת"א) 52961-03-12 שטולצמן נ' אדם-מילא בע"מ (פורסם בנבו, 30.6.2014); בג"ץ 5977/13 קליס נ' מדינת ישראל (פורסם בנבו, 22.10.2013).
- 97 רע"פ 11066/03 רום, לעיל ה"ש 95, החלטה מיום 28.5.2007.
- 98 ת"פ (מחוזי ת"א) 40206/05 מדינת ישראל נ' פילוסוף (פורסם בנבו, 5.2.2007).
- 99 דנ"פ 4409/12 עובד נ' מדינת ישראל (פורסם בנבו, 10.6.2012).
- 100 המפקח על הבנקים, הוראה 361, "ניהול הגנת הסייבר" (16.3.2015). הממונה על שוק ההון ביטוח וחסכון במשרד האוצר פרסם טיוטת חוזר דומה בחודש אוקטובר 2015.

והשמירה על זכויות יסוד שנוגעות להעברת המידע מעבר לגבולות מדינתיים ועוד נורמות שנובעות ממשטר דיני הבזק עשויות להשפיע באופן משמעותי על גיבוש הדין החדש במרחב. סוגיות אחרות, כגון האיזונים המשפטיים הנדרשים במרחב בין זכויות הפרט לבין שיקולי בטחון ברמה הבינלאומית וברמה הלאומית, דורשות בחינה נוספת. הדרכים שבהן המשטרים של דיני הבזק הבינלאומי ודיני הסייבר הבינלאומיים משפיעים אחד על השני, כאשר שניהם בשלבי התפתחות, ממשיכות להתגבש.