חיים ויסמונסקי*

אכיפה אלטרנטיבית של עברות ביטוי במרחב הסייבר

המרחב המקוון הביא לפריחה של עברות ביטוי. תכונותיו המשפטיות־טכנולוגיות של המרחב אפשרו לבצע עברות ביטוי בעלות זניחה, בתפוצה רחבה, תוך סיכון מינימלי של מבצע העברה שייתפס ויובא לדין. לפיכך, יש לתור אחר חלופה משלימה לאכיפה הפלילית הקלאסית כלפי עברות ביטוי, חלופה שתוכל להגן על הערכים שבבסיס האיסורים על ביטויים מסוימים ולהפחית את נזקיהם כשהאכיפה הפלילית כושלת. החלופה הנדונה במאמר זה מכונה "אכיפה אלטרנטיבית" והיא מציעה אסטרטגיה של התמקדות בפרסום האסור ולא במפרסם; בעברה – ולא במבצעה. אסטרטגיה זו כוללת סינון תכנים, הסרת תכנים אסורים, חסימת גישה אליהם או ניתוק המשתמש מהשירות שבמסגרתו פעל להפצתם. פעולות האכיפה האלטרנטיבית נחלקות לפעולות במישור ההסכמי־וולונטרי אל מול ספקיות השירות המקוונות ולפעולות מכוח הוראות חוק מחייבות של המדינה האוכפת.

המאמר מציג את תפישת האכיפה האלטרנטיבית כלפי עברות הביטוי במרחב המקוון ואת ההצדקות ליישומה. כמו כן, המאמר בוחן בהרחבה את הביקורות האפשריות על גישה זו, במישור העקרוני ובמישור הפרקטי, ומציע להן מענים. בהמשך, המאמר מונה עקרונות יסוד בהפעלה של מנגנוני האכיפה האלטרנטיבית כלפי עברות הביטוי ברשת באופן שיגביר את השקיפות ואת שיתוף הציבור באשר להפעלת המנגנונים, וכן יבטיח את האיזונים בין האינטרס הציבורי באכיפת הדין הפלילי מחד גיסא לבין מארג הזכויות של המפרסם, הפלטפורמה המקוונת וציבור משתמשי המרחב המקוון מאידך גיסא.

* דוקטור למשפטים, חוקר במרכז למחקר סייבר בינתחומי על שם בלווטניק באוניברסיטת תל־אביב, מרצה מן החוץ באוניברסיטת תל־אביב ובאוניברסיטת חיפה. המחבר משמש מנהל מחלקת הסייבר בפרקליטות המדינה. האמור במאמר מבטא את עמדתו האישית בלבד. תודה למערכת כתב העת "משפט, חברה ותרבות" על ההערות לטיוטת המאמר. תודה למר עמוס וגנר־איתן על הערותיו המועילות למאמר זה.

מכיוון חופש הביטוי 2. ביקורת מכיוון חופש השימוש במרחב המקוון 3. ביקורת מכיוון חופש העיסוק של ספקיות השירות 4. ביקורת מכיוון טכנולוגי (יעילותה של אסטרטגיית ההתגוננות והמניעה) **ה. היישום של מודל האכיפה האלטרנטיבית על עברות ביטוי במרחב המקוון** 1. סיכום עד כאן 2. עקרונות בהפעלת מנגנוני האכיפה האלטרנטיבית א. שקיפות פעולתן של רשויות האכיפה ב. מקורות המידע של רשויות האכיפה בנוגע לעברות הביטוי המקוונות ושיתוף הציבור ג. ביקורת שיפוטית ולא מנהלית בכל הנוגע לאכיפה אלטרנטיבית במסלול הכוחני ד. הבניית שיקול הדעת המנהלי והשיפוטי בנוגע ליישום האכיפה האלטרנטיבית ה. מיקוד הטיפול בתחום האכיפה האלטרנטיבית

א. הקדמה

מהפכת האינטרנט והמרחב המקוון (המכונה גם "מרחב הסייבר")[1] מעצימים את חופש הביטוי. הרשת מאפשרת להרחיב את קשת הדעות: היא מנגישה לכל אדם פלטפורמות המאפשרות פרסום דעה; היא מאפשרת תקשורת המונים, תקשורת קבוצתית ותקשורת בין־אישית מגוונת, דינמית, מהירה ואנונימית; היא מאפשרת להתגבר על משוכות מוסדיות, חברתיות וכלכליות; היא מאפשרת לגוון את השיח, להעשירו ולשכללו. עם זאת, המרחב המקוון הוא גם כר פורה לביטויים אסורים. המרחב המקוון משופע בביטויים העולים כדי הסתה לגזענות ולאלימות, גילוי הזדהות עם ארגון טרור והסתה לטרור,[2] לשון הרע, פגיעה ברגשי דת, העלבת עובדי ציבור, איומים, הפרת איסורי פרסום (מכוח הדין או מכוח צו שיפוטי),[3]

1 ב"מרחב הסייבר" הכוונה לכל רשת בין מחשבים (או רכיבים המבצעים פעולות ממוחשבות של עיבוד מידע דיגיטלי), מקומית, רחבה או כלל־עולמית (כמו האינטרנט). כאשר עוסקים בעברות ביטוי, החלק הרלוונטי ביותר מתוך מרחב הסייבר הוא האינטרנט – הרשת הכלל־עולמית – שכן באמצעותה עברות הביטוי מגיעות לקהל רחב. על כן, במאמר זה אשתמש לעתים גם במונח ה"מרחב האינטרנטי".

2 עברה זו מנוסחת בס' 24 לחוק המאבק בטרור, התשע"ו–2016 (להלן: חוק המאבק בטרור). היא מחליפה את העברה של "תמיכה בארגון טרוריסטי", שהופיעה בס' 4 לפקודת מניעת טרור, התש"ח–1948, שהתבטלה עם חקיקת חוק המאבק בטרור.

3 בין הוראות איסור הפרסום הסטטוטוריות אפשר למנות את האיסור על פרסום של פרטי מתלונן בעברת מין, המעוגן ס' 352 לחוק העונשין, התשל"ז–1977 (להלן: חוק העונשין) ואת האיסור על פרסום פרטים מתוך דיון שנערך בדלתיים סגורות, המעוגן בס' 70(א) לחוק בתי המשפט [נוסח חדש], התשמ"ד–1984 (להלן: חוק בתי המשפט). בין ההוראות המסמיכות את בתי המשפט להוציא צווי איסור פרסום אפשר למנות את איסורי הפרסום בשלב החקירה והמשפט, המעוגנים בס' 70(ג1)–70(ה) לחוק בתי המשפט, איסור פרסום של חומר הפוגע בפרטיות, המעוגן בס' 29(א)(1) לחוק הגנת הפרטיות, התשמ"א–1981 (להלן: חוק הגנת הפרטיות), איסור פרסום של תוכן העולה כדי לשון הרע, המעוגן בס' 9(א)(1) לחוק איסור לשון הרע, התשכ"ה–1965 (להלן: חוק איסור לשון הרע) ואיסור פרסום פרטים מזהים של קטין, המעוגן בס' 24(א) לחוק הנוער (טיפול והשגחה), התש"ך–1960.

פרסומים מטרידים מינית[4] ופרסומים הפוגעים בפרטיות. כמו כן הרשת כוללת ביטויים פוגעניים שהדין הישראלי אינו מתייחס אליהם במישרין כגון בריונות רשת (Cyber bullying) או ביוש (Shaming).[5]

מאמר זה לא יתמקד בשאלת הסטנדרטים המשפטיים לקביעה אימתי ביטוי מסוים מהווה עברה פלילית או עוולה נזיקית,[6] אלא יעסוק בשאלת האכיפה וההתמודדות בפועל עם עברות הביטוי הקיימות[7] בראי המאפיינים הייחודיים של מרחב הסייבר. כפי שאפרט,

4 כוונתי כאן להטרדות מיניות באמצעות המרחב המקוון, הנעשות על דרך של פרסום; בראש ובראשונה הכוונה לעברה על ס' 3(א)(5א) לחוק למניעת הטרדה מינית, התשנ"ח-1998, שהוספה בחוק למניעת הטרדה מינית (תיקון 10), התשע"ד-2014 (תיקון שכונה "חוק הסרטונים") וקובעת איסור על פרסום של תצלום, סרט או הקלטה של אדם, המתמקד במיניותו, בנסיבות שבהן הפרסום עלול להשפיל את האדם או לבזותו ולא ניתנה הסכמתו לפרסום. חלופות נוספות המנויות בחוק למניעת הטרדה מינית, המדברות על התייחסויות או על הצעות בעלות אופי מיני, תתבצענה ככלל בשיח או בתכתובות מיחיד־אל־יחיד, אך יכולות גם להתבצע על דרך של פרסום ברבים.

5 ב"בריונות רשת" הכוונה להתנהגות תוקפנית חוזרת ונשנית ומתמשכת כלפי אדם אחר, הכרוכה בנידוי, בביזוי או בהשפלה פומביים לפני קבוצה, או באמצעות קבוצה, כשההתנהגות התוקפנית מתבצעת במרחב המקוון. לתיאור התופעה של בריונות רשת, לממדיה ולניתוח השלכותיה ראו, למשל, רויטל סלע־שיוביץ "התנהגויות של נטילת סיכון בקרב ילדים ובני נוער בעת גלישה באינטרנט" **במעגלי חינוך** 2, 52, 56-57 (2012); John Shakenborg, Richard Van Acker & Robert A. Gable, *Cyberbullying: Prevention and Intervention to Protect Our Children and Youth*, 55 Preventing School Failure 88 (2011). ב"ביוש" (Shaming) הכוונה לניסיון לכפות תחושת בושה על אדם באמצעים מקוונים, תוך יצירת מצג של הפרת נורמות חברתיות והצגתה בנסיבות מבזות לפני קבוצה. לניתוח תופעת הביוש ולהבחנתה מבריונות רשת ומהטרדות אחרות במרחב המקוון, ראו Kate Klonick, *Re-Shaming the Debate: Social Norms, Shame and Regulation in an Internet Age*, 75 Md. L. Rev. 1029, 1033-1035 (2016). הדין הישראלי אינו אוסר קונקרטית על בריונות רשת או על ביוש אף על פי שהתנהגויות אלה (במיוחד בריונות רשת) עשויות לכלול, בהתאם לנסיבות, אמרות העולות כדי לשון הרע, איומים, שידול להתאבדות או פגיעה בפרטיות.

6 שאלת ההצדקה לקביעתן של עברות ביטוי בכלל ושל עברות ביטוי חדשות ברשת בפרט היא שאלה כבדת־משקל, מתחום הדין המהותי, שבהחלט ראויה לניתוח ולדיון מעמיקים אך אינה חלק ממאמר זה. בכל הנוגע לסוגיית ההתמודדות עם תופעות של בריונות רשת וביוש ברשת, בימים אלה יושבת על המדוכה הוועדה הציבורית לגיבוש אמצעים להגנה על הציבור ובהם נושאי משרה בשירות הציבור מפני פעילות ופרסומים פוגעניים כמו גם בריונות ברשת האינטרנט (ועדת ארבל), שמונתה על ידי שרת המשפטים ביום 5.8.2015. אחת השאלות המרכזיות בנוגע להפללה ישירה של תופעות הבריונות והביוש ברשת היא השאלה אם נכון להעדיף אסטרטגיה של הפללה על פני אסטרטגיה של חינוך, הסברה ומניעה. לדיון בנושא ראו, למשל, Jessica P. Meredith, *Combating Cyberbullying: Emphasizing Education over Criminalization*, 63 Fed. Comm. L.J. 311 (2010).

7 לצורכי מאמר זה "עברות ביטוי" כוללות כל עברה פלילית שבדין, שהיסוד ההתנהגותי שלה הוא על דרך של ביטוי, פרסום, הפצה של מידע וכדומה.

מאפייניו המשפטיים־טכנולוגיים של המרחב המקוון מציבים לפני רשויות האכיפה אתגר אסטרטגי בבואן להתמודד עם בעיית הפרסומים האסורים במרחב המקוון. אתגר זה מחייב שינוי בפרדיגמת האכיפה בכל הנוגע לעברות הביטוי המקוונות.

מתודת האכיפה הפלילית הקלאסית של עברות ביטוי גורסת כי אין לנקוט אסטרטגיה של מניעה מוקדמת של הביטוי האסור, כי אם יש להעמיד לדין את המפרסם בדיעבד, לאחר הפרסום. דוקטרינה זו מבוססת על ההנחה שלעולם עדיפה הפללה בדיעבד – וכפועל יוצא ממנה הפחתת הכדאיות של ביצוע עברות עתידיות מאותו סוג – על פני מניעה מראש, העלולה ליצור אפקט מצנן מפני ביטויים הממוקמים בקצוות הסקאלה של הביטויים המותרים.

למעשה, באספקלריה רחבה יותר אפשר לראות שהאכיפה הפלילית הקלאסית כולה – לאו דווקא של עברות ביטוי – מבוססת על רעיון של הרתעה באמצעות הגדלת הסיכויים של מבצע העברה להיתפס (הגדלת הסיכויים נוגעת הן לאיתור מבצע העברה, הן לאיסוף ראיות קבילות להעמדתו לדין והן להרשעתו) והחמרת העונש (במקרה של הרשעה). עם זאת, המחקרים על הרתעה פלילית מצביעים על כך שהגדלת סיכויי התפיסה מביאה להפחתת פשיעה יותר מהחמרת הענישה במקרה של הרשעה.[8] רעיונות מתקדמים יותר של אכיפה פלילית גורסים כי יש מקום להתחשב ולהשפיע על משתנה נוסף – הגדלת עלות הביצוע של העברה הפלילית: בזכות מגבלות ארכיטקטוניות ואחרות יקשה להוציא אל הפועל את מעשה העברה, וכך תושג ההרתעה הן בשלב שלפני ביצוע העברה והן בשלב שלאחר ביצועה, היינו: תפיסת העבריין וענישתו.[9]

הרעיון המרכזי שיבוטא במאמר זה הוא שבכל הנוגע לעברות ביטוי ברשת, קשה מאוד ליצור מנגנונים שיעלו את סיכויי התפיסה. זאת הן מטעמים משפטיים, הן מטעמים טכנולוגיים־ארכיטקטוניים והן מטעמים פרקטיים. עם זאת, אפשר לנקוט פעולה אלטרנטיבית – להכשיל את ביצוע העברה על ידי פיתוח ויישום של מנגנוני התגוננות בכלים משפטיים, המותאמים למאפיינים של עברות הביטוי ברשת. מנגנוני ההתגוננות האלטרנטיביים שבהם יתמקד מאמר זה, ויכונו בשם הכולל "אכיפה אלטרנטיבית", נחלקים לשניים: מנגנונים וולונטריים

8 ראו Franklin E. Zimring & Gordon Hawkins, Deterrence: The Legal Threat in Crime Control (1973); Steven Shavell, *Criminal Law and the Optimal Use of Nonmonetary Sanctions as a Deterrent*, 85 Colum. L. Rev. 1232, 1236 (1985); David Huizinga & Kimberly L. Henry, *The Effect of Arrest and Justice System Sanctions on Subsequent Behavior: Findings from Longitudinal and Other Studies*, *in* The Long View of Crime: A Synthesis of Longitudinal Research 220 (Akiva M. Liberman ed., 2008).

9 בהקשר זה ראו את הגישה המוכרת בקרימינולוגיה כ־Crime Prevention Through Environmental Design (CPTED) למניעת פשיעה באופן ארכיטקטוני, על ידי עיצוב הסביבה באופן שיגרום לעבריינים בפוטנציה לשלם "מחיר" גבוה כדי לבצע את העברה, וכן את גישת Crime Reduction Through Production Design (CRPD), העוסקת בעיצוב מוצרים באופן שיקשה לבצע עברה בנוגע אליהם או באמצעותם. לסקירת הגישה הראשונה ראו, למשל, Tim Crowe, Crime Prevention Through Environmental Design (2nd ed. 2000); לסקירת הגישה השנייה ראו, למשל, Designing Out Crime from Products and Systems (Ronald V. Clarke & Graeme R. Newman eds., 2005). ראו גם Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. Pa. L. Rev. 1003, 1013-1020 (2001).

ומנגנונים של הוראות כופות. טכניקת ההתגוננות נחלקת לארבעה סוגים: הסרת התוכן הפוגעני ממקום פרסומו, חסימת גישה לאתרים שבהם מתפרסמים הביטויים האסורים, סינון התכנים האסורים וניתוק משתמש רשת מהשירות או מהאפליקציה שבה פעל שלא כחוק. מנגנונים אלה מתמקדים בצמצום פגיעתה של העברה ברמה הפרקטית. כתוצאת לוואי של פעולה זו, עשוי לעלות "מחיר" ביצועה של העברה, במובן זה שהשגת אפקט זהה מבחינת היקף הפרסום, מידת תפוצתו ומשך פרסומו תצריך מאמץ רב יותר מצד המפרסם.

סדר הדיון במאמר יהיה כדלקמן: **בפרק ב'** אציג את בעיית האכיפה הפלילית ה"קלאסית" במרחב הסייבר כלפי עברות הביטוי: אפרט את הטעמים להיווצרות הבעיה, המובילים למסקנה שהאסטרטגיה ההרתעתית – המבוססת על חקירה פלילית בדיעבד, העמדה לדין, הרשעה וענישה – אינה יכולה לספק מענה הולם להרתעה מפני עברות ביטוי במרחב הסייבר. **בפרק ג'** אציג את מודל האכיפה האלטרנטיבית של התגוננות ומניעה (במקום פעולה "התקפית" של גילוי מבצע העברה והבאתו לדין). כאמור, אלטרנטיבת ההתגוננות נחלקת לשני סוגים: האחד – התגוננות באמצעות הסדרה וולונטרית, בין שהמתגונן הוא משתמש האינטרנט או ספק שירות באינטרנט; האחר – התגוננות באמצעות פעולה כופה מטעם המדינה. אציג את המסלולים הדוקטרינריים שדרכם אפשר לייבא אל המשפט הישראלי פתרון של פעולות מגננתיות־כופות, ואראה כיצד פתרון זה הולם את אופן הביצוע של עברות ביטוי במרחב המקוון. **בפרק ד'** אציג את הביקורות שנמתחו על האסטרטגיה של התגוננות ומניעה בהקשר של עברות ביטוי במרחב הסייבר: הראשונה, מכיוון התאוריה של חופש הביטוי, הגורסת כי לעולם עדיפה הפללה בדיעבד של ביטוי אסור על פני מניעה מראש של ביטוי העלול להתברר בדיעבד כמותר; השנייה, מכיוון חופש השימוש במרחב המקוון – מצדו של המשתמש המבקש להשתחרר מפטרנליזם מדינתי הכופה עליו אמצעי הגנה או המייצר פעולה מגננתית הסכמית; השלישית, מכיוון חופש העיסוק של ספקיות השירות במרחב המקוון, העלולות להידרש לחובות ולנטלים שונים במסגרת האסטרטגיה המגננתית; הרביעית, ביקורת מכיוון טכנולוגי על היעילות של אמצעי ההתגוננות המוצעים, ככאלה שאינם מסוגלים להשיג את מטרותיהם. לאחר הצגת הביקורות האמורות, אטען כי אין בהן כדי לשמוט את הבסיס להצדקה העקרונית של שימוש באסטרטגיית ההתגוננות בסביבה האינטרנטית, אף אם יש בהן להטיל מגבלות וסייגים על השימוש במתודת אכיפה זו.

לבסוף, **בפרק ה'**, אציג הצעה ליישום המודל המוצע ואטען כי מוצדק וראוי לממש במרחב המקוון פעולות של אכיפה אלטרנטיבית – הן פעולות כופות והן פעולות וולונטריות – כדי להתמודד עם עברות הביטוי ברשת. כמו כן אציג כמה עקרונות ביישום מנגנוני האכיפה האלטרנטיבית כלפי עברות הביטוי במרחב המקוון.

ייאמר מייד כי אין מטרתי להציג את האכיפה האלטרנטיבית, שעיקרה התגוננות במרחב הסייבר בכלים משפטיים, כחלופה מלאה לאכיפה הפלילית הקלאסית של עברות הביטוי, המבוצעת על ידי המדינה לאחר ביצוע העברה במטרה לחשוף את מבצעה ולהביאו לדין; זו הייתה ונשארה דרך המלך. האכיפה האלטרנטיבית היא נתיב משלים, שנועד למנוע את הפגיעה הפוטנציאלית הכרוכה בעברות הביטוי ברשת היכן שאסטרטגיית האכיפה הפלילית הקלאסית כושלת. האכיפה האלטרנטיבית מגלמת שורה של צעדים מנהליים שתכליתם דומה לאלה של האיסורים הפליליים בתחום הביטוי, וצעדים אלה יינקטו במקרים שבהם

אסטרטגיה של אכיפה פלילית לא תוכל להגשים תכליות אלה, וזאת בשל המאפיינים הייחודיים של המרחב המקוון כזירת ביצוע העברות.

ב. בעיית האכיפה הפלילית במרחב הסייבר כלפי עברות הביטוי

הפשיעה ברשת גואה. פשיעת הסייבר נמצאת בעלייה רב־ממדית, הן במובן הכמותי (כמות העברות המבוצעות), הן במובן האיכותי (מידת הנזק הכרוך בהן) והן במספר הקרבנות.[10]

10 איסוף נתונים כמותיים על עברות באינטרנט אינו משימה קלה, ולמעשה סביר להניח שהנתונים הקיימים חסרים. יש לכך כמה טעמים: ראשית, יש צורך באיסוף נתונים סטטיסטיים מכל מדינות העולם שכן מדובר במרחב גלובלי; שנית, מרבית הנתונים נאספים על ידי עמותות פרטיות העוסקות בנושא מסוים אחד (פדופיליה מקוונת, התמכרות להימורים וכדומה) או על ידי חברות מסחריות לאבטחת מידע. נתונים רשמיים של המדינות כמעט אינם זמינים; שלישית, יש דיווח חסר על עברות מחשב מצד הקרבנות – בין בשל הקושי שלהם לזהות שנפגעו, בין בשל חששם לחשוף שנפגעו ובין בשל חוסר אמון ביכולת של רשויות האכיפה לחשוף את מבצעי העברה ולהביאם לדין. חרף הקשיים המתודולוגיים האמורים אמנה להלן כמה מחקרים האומדים את נזקי הפשיעה במרחב הסייבר: דוח ה־IC3 האמריקני, גוף מדינתי הכולל מרכז לקבלת תלונות על הונאות מקוונות, קובע כי בשנת 2013 התקבלו במרכז התלונות של הארגון יותר מ־260 אלף תלונות על פשעי מחשב בארצות־הברית, כשהנזק המצרפי מהתלונות עמד על יותר מ־780 מיליון דולר. נתון זה מציג עלייה של 48.8% בהשוואה לנתון בשנת 2012. ראו Federal Bureau of Investigation – Internet Crime Complaint Center, 2013 Internet Crime Report (2014), https://pdf.ic3.gov/2013_IC3Report.pdf. מטבע הדברים, הדוח אינו מכסה את כלל הנזקים הכלכליים בארצות־הברית מפשיעת הסייבר, שכן הוא מתייחס כאמור אך ורק לתלונות המגיעות לארגון. ראו גם Ponemon Institute, 2013 Cost of Cyber Crime Study: United States (2013), https://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf. עסקינן בדוח של חברת Ponemon Institute עבור HP Enterprise Security משנת 2013, שבדק את מידת הנזק שנגרם לתאגידים עסקיים גדולים בארצות־הברית סובלים מנזק ממוצע של 11.56 מיליון דולר בשנה לכל תאגיד, וכי נזק ממוצע זה מגלם גידול של כ־26% בהשוואה לנתון בשנה הקודמת. ראו גם PwC, 2014 Global Economic Crime Survey (2016), http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html. מדובר בדוח של חברת השירותים הפיננסיים הבין־לאומית PwC לשנת 2016, המראה שכ־32% מהתאגידים שנסקרו בדוח נפגעו מפשיעה כלכלית אינטרנטית. 53% מהנשאלים העריכו כי פשיעת הסייבר – כגורם סיכון לתאגיד שהם מייצגים – נמצאת בעלייה; תפישת איום הסייבר כאמור גברה בהשוואה לסקרים קודמים של חברת PwC משנים קודמות. אשר לעברה של פרסום תכנים פדופיליים באינטרנט ראו Internet Watch Foundation, 2010 Annual Report (2010), www.iwf.org.uk/report/2010-annual-report. על פי הדוח השנתי לשנת 2010, אותרו 16,739 אתרים בעלי שמות (URL) שונים, שכללו תכנים פדופיליים אסורים על פי דין המדינה שבה נמצאו השרתים שלהם. כמות זו שילשה את עצמה בהשוואה לשנת 2008; השוו עם Internet Watch Foundation, 2008 Annual Report (2008), www.iwf.org.uk/report/2008-annual-report. לגבי העלייה בעברה של ארגון הימורים מקוונים ראו, למשל, Edward M. Yures, *Gambling*

בכלל זה יש למנות את עברות הביטוי ברשת – המגיעות לתפוצה רחבה ונוגעות למספר רב של קרבנות.

את העלייה בפשיעה המקוונת, ובכלל זה בעברות הביטוי ברשת, אפשר להסביר בכך שהאכיפה הפלילית, בשיטה הקלאסית הנקוטה כיום, חלשה במרחב הסייבר. בהשאלה מדבריו של ארתור מילספאו (Millspaugh), שנכתבו בשנת 1937 בהקשר של הפשיעה במרחב הפיזי, הפשיעה נוטה לשגשג היכן שהאכיפה חלשה.[11] יתרה מזו: אכיפה פלילית חסרה או חלשה עלולה לפגוע בעצם ההצדקה להמשך קיומו של האיסור הפלילי, ובכך להעניק למחדל האכיפתי כוח לחולל שינוי נורמטיבי מהותי בכיוון של ביטול האיסור הפלילי או ביטול ההצדקה לו.[12]

החולשה של האכיפה הפלילית הקלאסית במרחב הסייבר נעוצה בקשיים הייחודיים של החקירה הפלילית במרחב המקוון. הקשיים נובעים משלוש קבוצות של טעמים: טעמים ארכיטקטוניים־טכנולוגיים, התלויים במבנה של המרחב המקוון ובטכנולוגיה המרכיבה אותו; טעמים משפטיים, הנובעים מההרכבה של כללי המשפט הנוהגים על המרחב המקוון; וטעמים מוסדיים.[13]

1. טעמים ארכיטקטוניים־טכנולוגיים

ארכיטקטורה משפיעה על פשיעה, הן במרחב הפיזי[14] והן במרחב המקוון.[15] הארכיטקטורה של המרחב המקוון נוצרת באמצעות הטכנולוגיה, והטכנולוגיה נוצרת על ידי האדם. לארכיטקטורה של המרחב המקוון יכולה להיות השפעה מרסנת פשיעה מחד גיסא או

---

on the Internet: The States Risk Playing Economic Roulette as the Internet Gambling Industry Spins Onward, 28 Rutgers Computer & Tech. L.J. 193 (2002); **כן ראו** Dana Gale, *The Economic Incentive Behind the Unlawful Internet Gambling Enforcement Act*, 15 Cardozo J. Int'l & Comp. L. 533, 534 (2007). **לגבי עברות של ריגול עסקי במרחב הסייבר, שחר ארגמן וגבי סיבוני הצביעו על עלייה, הן איכותית והן כמותית, בעברות של ריגול עסקי מקוון – הן בשל ההתאמה האופטימלית של המרחב המקוון לפעילות מסוג זה והן בשל המעבר הגורף לשמירה דיגיטלית של מידע עסקי. ראו שחר ארגמן וגבי סיבוני "חשיפת המשק הישראלי לריגול סייבר עסקי" צבא ואסטרטגיה 6, 41–42 (2014).**

11 **הציטוט המדויק הוא:** "Crime tends to flourish in the legal categories and the geographical areas where enforcement is weak". **ראו** Arthur C. Millspaugh, Crime Control by the National Government 278 (1937).

12 **אחת ההצדקות להפללה – קרי: לקביעת איסור פלילי – היא היכולת לאוכפו. ראו, למשל, יובל קרניאל הפרת אמונים בתאגיד במשפט האזרחי והפלילי 421–422 (2001). ראו עוד אסף הרדוף הפשע המקוון 62–72 (2010).**

13 **לדיון נוסף בקשיי האכיפה במרחב הסייבר ראו חיים ויסמונסקי חקירה פלילית במרחב הסייבר 51–63 (2015).**

14 Neal Kumar Katyal, *Architecture as Crime Control*, 111 Yale L.J. 1039, 1039-1071 (2002).

15 Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 Yale L.J. 2261 (2003).

מעודדת פשיעה מאידך גיסא, בהיותה כוח מסדיר להתנהגותו של הפרט.[16] להלן אמנה מאפיינים ארכיטקטוניים־טכנולוגיים של המרחב המקוון, המקשים על יכולת האכיפה הפלילית במרחב. בהצגת המאפיינים הללו אתבונן על המרחב המקוון מבחוץ, ברזולוציה המכלילה את מופעיו לכלל מרחב אחד:[17] **ראשית**, המרחב המקוון מאפשר **אנונימיות** יחסית, ולמשתמשים מתוחכמים הוא מאפשר אנונימיות מוגברת. האנונימיות היחסית נובעת מהאפשרות להתייצג ללא זהות, בזהות בדויה קבועה (פסבדונימיות)[18] או ארעית. היא מאפשרת גם להתחזות לאדם אחר לצורך הפללתו או ביזויו בפומבי על ידי כתיבת מסרים מבזים "בשמו".[19] הבסיס להסוואת הזהות במרחב המקוון נעוץ בכך שהזיהוי הבסיסי נעשה על פי כתובת IP המוענקת לכל מחשב ברשת. בכל הנוגע לאינטרנט, כתובת IP מוקצית למשתמש על ידי ספקיות הגישה, וככל שמדובר במשתמש פרטי, הכתובת הניתנת לו משתנה מעת לעת. במילים אחרות: כתובת IP אינה מזהה חד־ערכי לזיהוי משתמש באינטרנט.[20] יתרה מזו: גם אם אפשר לשייך כתובת IP למחשב מסוים, עדיין אין הדבר אומר שאפשר יהיה לשייך את המחשב לחשוד מסוים. זאת, משום שאפשר לגלוש באמצעות שרתי proxy שאינם שומרים את נתוני הגלישה של המחשבים שהתקשרו דרכם אל האינטרנט;[21] דרך רשתות ביתיות שמחוברים אליהן כמה מחשבים (ואי־אפשר לדעת איזה מהמחשבים ביצע את הפעולה הנחקרת); דרך רשתות אלחוטיות (wireless) **ציבוריות** וכדומה. יתר על כן,

16 לורנס לסיג (Lessig) מנה ארבעה כוחות המסדירים את התנהגות הפרט ואת פעילותו במרחב המקוון: המשפט, הנורמות החברתיות, כוחות השוק והארכיטקטורה של האינטרנט (המעוצבת על ידי הקוד). במסגרת התאוריה שפיתח טען לסיג כי ארבעת הכוחות האלה משפיעים לא רק על הפרט אלא גם זה על זה. **ראו** Lawrence Lessig, Code and Other Laws of Cyberspace (1999) 85-99, 235-239. **ראו גם** Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 507 (1999).

17 כידוע, המרחב המקוון אינו אלא כותרת למכלול של מופעים – אתרי Web, פורומים, אתרי שיתוף קבצים, שירותי VoIP (כגון Skype), שירותי מחשוב ענן, ערוצי צ׳אט, שירותים להעברת מסרים מידיים, שירותי דוא״ל, שרתי FTP להחלפת קבצים, רשתות חברתיות, קבוצות דיון – כל אלה ואחרים מרכיבים את המרחב המקוון, אף שהם נבדלים אלה מאלה בטכנולוגיה שלהם, בפונקציה החברתית שהם ממלאים ובשאלות המשפטיות הקונקרטיות שהם עולים לעורר. אורין קֶר (Kerr) וברט פרישמן (Frischmann) כתבו על שתי הפרספקטיבות הללו: קר הציע לשמר את ההבחנה כדי למנוע בלבול קונספטואלי ואילו פרישמן טען כי ראוי לשלב את שתי הפרספקטיבות. **ראו** Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 Geo. L.J. 357 (2003); Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 Loy. U. Chi. L.J. 205 (2003).

18 על ההבחנה בין אנונימיות לבין פסבדונימיות ראו, למשל, אלעד אורג **זכות לזהות אינפורמטיבית: עקרון משפטי חדש להגנת קיומה של זהות אינפורמטיבית ויישומו בסביבת מידע מודרני** 23-26, 123-143 (חיבור לשם קבלת תואר "דוקטור למשפטים", אוניברסיטת תל־אביב, 2008).

19 בהקשר זה ראו, למשל, צ״א (שלום י־ם) 32145-07-13 **הוצאת עיתון הארץ בע״מ נ׳ משטרת ישראל** (פורסם בנבו, 12.8.2013).

20 מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 338-348 (2010).

21 לאתר אינטרנט המספק מידע על שרתי proxy שאפשר לגלוש מהם באינטרנט באופן שלא יסגיר את זהות הגולש ראו, לדוגמה, http://proxy.org.

משתמש יכול להשתמש בשירותי אנונימיזציה המגבירים את האנונימיות שלו באופן מיוחד.[22] כך, למשל, אפשר להשתמש בשירותים המציעים כתובת IP דינמית המשתנה מעת לעת ומעלימה את כתובת ה־IP האמתית של המחשב ברשת;[23] אפשר גם להשתמש בשיטות של Onion routing דוגמת דפדפן TOR (The Onion Routing), המסווה את המסר המועבר מגולש מסוים באמצעות העברתו דרך שרשרת של מחשבים, ואי־אפשר לאחזר בדיעבד את מקור ההתקשרות (לפחות בלי לפקח לאורך זמן ומראש על כל שרשרת המחשבים).[24] אמצעי אנונימיזציה מתוחכמים אלה מאפשרים לגורמים עבריינים לפתח אזורים מחתרתיים ברשת המכונים Darknets, שבהם רוחשת פעילות עבריינית ענפה.[25]

שנית, מרחב הסייבר **פתוח לכלל הציבור** וההצטרפות אליו כיום למעשה יכולה להיות חופשית ובלתי־מבוקרת (לפחות במדינות דמוקרטיות).[26] נגישות האינטרנט גדלה במידה ניכרת ובכמה מובנים: (1) עלויות הרכישה של מחשב ועלויות ההתחברות לאינטרנט הביתי והעברת המידע באינטרנט הוזלו עם השנים; (2) מקומות ציבוריים רבים (שדות תעופה, בתי קפה, בתי מלון ואף ערים שלמות) מציעים שירותי התחברות אלחוטית (Wireless) לאינטרנט,

22 ראו Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. Miami L. Rev. 991 (2004). במאמר זה ז'רסקי עורך בחינה נורמטיבית האם ראוי להכיר במודל של הגנה על אנונימיות ברשת. ז'רסקי מציג את בעיותיו של מודל האנונימיות, ובהן גם הפגיעה ביכולת האכיפה הפלילית של עברות ברשת. ראו שם, בעמ' 1334–1340. לסקירה של שיטות אנונימיזציה ראו בירנהק **מרחב פרטי**, לעיל ה"ש 21, בעמ' 388–395.

23 לדוגמה לשירותים המספקים כתובת IP דינמית, ומטשטשים עקבות IP כלפי שרתים ומחשבים אחרים בהם גלש המשתמש, ראו למשל www.anonymizer.com, www.no-ip.com.

24 אפשר להוריד דפדפן TOR חינם באינטרנט, באמצעות חיפוש פשוט במנוע חיפוש. התוכנה מספקת למשתמש כתובת IP מזויפת המאפשרת לו לפעול באנונימיות באינטרנט. לאחר החיבור נפתח דפדפן TOR, עם הכתובת המזויפת האנונימית שסופקה למשתמש, ובאמצעותו אפשר לחפש תכנים שמנוע חיפוש רגיל ודפדפן רגיל אינם מסוגלים לאתר. ראו http://www.torproject.org. כן ראו בירנהק **מרחב פרטי**, לעיל ה"ש 21, בעמ' 388–395.

25 המונח Darknet נטבע לראשונה בשנות השבעים של המאה הקודמת כדי לתאר רשתות מחשבים המבודדות מרשת ARPANET, שלימים התפתח ממנה האינטרנט העולמי. הרשתות בודדו מטעמי ביטחון לשימוש של כוחות הביטחון האמריקניים. ה־Darknets המקוריות תוכננו כך שיוכלו לקבל מידע מהרשת הכללית (ARPANET), אולם כתובותיהן לא הופיעו ברשימות של הרשת הכללית והן לא הגיבו לשאילתות "פינג" לצורכי זיהוי מקורן. ה־Darknets אינן רשתות המופרדות פיזית מהאינטרנט; למעשה מדובר באפליקציה ובפרוטוקול תקשורת ה"רוכבים" על האינטרנט ויוצרים בידוד והפרדה ברבדים אלה בלבד. בעשור האחרון נהפכה ה־Darknet לרשת המשמשת גם גורמי פשיעה וטרור, המנצלים את האנונימיזציה המוגברת לטובת ביצוע פעילות אסורה (מכונה גם "רשת אפלה" או "Darkweb"). עוד על Darknet ראו רועי גולדשמידט "שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה" **מרכז המחקר והמידע של הכנסת (2012)**, www.knesset.gov.il/committees/heb/material/data/mada2012-01-02.doc.

26 ראו בירנהק **מרחב פרטי**, לעיל ה"ש 21, בעמ' 339.

בתשלום או חינם; (3) מספר המכשירים וסוג המכשירים היכולים להתחבר לאינטרנט גדל מאוד גם הוא. האינטרנט כבר אינו מחבר רק בין מחשבים נייחים או ניידים: האינטרנט הסלולרי הנגיש את הרשת והעצים את השימוש במשאביה. ניוד האינטרנט מאפשר להגיע לכל "מקום" מכל מקום, ולא רק ממקום מסוים בו מצוי המחשב. כאשר החיבור לאינטרנט נעשה ממקומות ציבוריים, בהם מותקנת רשת אלחוטית שאינה דורשת הזדהות מוקדמת כתנאי להתחברות באמצעותה לאינטרנט, הרי שהיכולת לאתר בדיעבד את זהות הגולש נפגעת במידה ניכרת, והיכולת לחשוף את מבצע העברה הפלילית קטנה בהתאם.

שלישית, חלק ניכר מהעקבות הדיגיטליים שפעילות עבריינית מותירה במרחב הסייבר הוא **נדיף**. מקובל לטעון שהזיכרון הדיגיטלי הוא ארוך, כמעט אינסופי, ושבעיית הזיכרון ארוך־הטווח יוצרת אפקטים לא פשוטים של פגיעה בפרטיות ובשמו הטוב של אדם.[27] עם זאת, חלק ניכר מהמידע הדיגיטלי, שעשוי להיות יקר־ערך לצורכי חקירה פלילית עתידית, אינו נשמר דרך קבע. תכנים רבים נשמרים בספריות זמניות או שהם מאוחסנים עד ל"דריסתם" על ידי מידע אחר שיתפוס את מקום האחסון לצורך השימוש הבא באותו אתר אינטרנט, אפליקציה סלולרית וכדומה. ככל שהמידע הדיגיטלי מנוהל על ידי ספקיות שירות שונות, וככל שלא מוטלת עליהן כל חובה שבדין לשמור את המידע הזה עבור המדינה ולשימושה, אזי ניהול המידע נעשה לתועלת התאגיד המנהל את השירות ולתועלתו בלבד, וזו לא תמיד עולה בקנה אחד עם צורכי החקירה הפלילית. יש, למשל, ששמירת המידע נעשית על ידי ספקית השירות לצרכיה שלה, למשל לצורך בקרה על איכות השירות שלה או לצורך איתור תקלות ואבטחת מידע על ידי בדיקות בדיעבד.[28] תכונת הנדיפות של העקבות הדיגיטליים מעוררת דיון בשאלת הצורך של המדינה להטיל על ספקיות השירות חובות שימור מידע דרך קבע (Retention),[29] או מכאן ואילך במקרה קונקרטי (Preservation).[30] לחובות אלה – בעיקר

27 יש דיון ציבורי ומשפטי בדבר הזכות להישכח (the right to be forgotten) במרחב המקוון, כשהכוונה היא לזכות שמידע אישי לא ייאגר ויעמוד לדיראון עולם נגד אדם במרחבי האינטרנט. בארץ ראו, למשל, ע"א (מחוזי ת"א) 2319/08 **פלוני נ' פלונית** (פורסם בנבו, 1.6.2011); בעולם ראו את הפסיקה של בית המשפט האירופי לצדק בדבר החובה המוטלת על מנוע חיפוש למחוק, בתנאים מסוימים, תוצאות חיפוש של תכנים על פי דרישת האדם שהמידע נוגע אליו: Case C-131/12, Google Spain SL, Google Inc. v. Agencia Espanola de Protection de Datos (AEPD), Mario Costeja Gonzales, 2014 E.C.R. 317.

28 לאופן שבו ספקיות השירות באינטרנט נוהגות לאגור נתוני תוכן ונתוני תקשורת רבים על אודות הגולשים ראו Nimrod Kozlovski, A Paradigm Shift in Online Policing – Designing Accountable Policing 88-93 (2005) (J.S.D. Dissertation, Yale Law School). לדעת קוזלובסקי ספקיות השירות הן מוקד משמעותי מאוד בחקירות אינטרנט.

29 משטר Retention מוכר באיחוד האירופי. ראו Directive 2006/24/EC of the European Parliament and of the Council of 13 April 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Council Directive 2002/58/EC, O.J. (L 105).

30 לדוגמאות להוראות preservation בנוגע לראיות דיגיטליות ראו בארצות־הברית את 18 U.S.C. § 2703(f) (2012). כן ראו את אמנת מועצת אירופה בדבר פשעי מחשב (נקראת גם "אמנת

לחובת השימור דרך קבע – יש השלכות ניכרות על הזכות לפרטיות ובמיוחד על הזכות לאנונימיות (בין כזכות עצמאית ובין כזכות נגזרת מחופש הביטוי או מהזכות לפרטיות).[31]

רביעית, חלק ניכר מהעקבות הדיגיטליים **מבוזר** על פני כמה מחשבים באופן שאינו חופף את יעד ההתקשרות הסופי של המשתמש במרחב המקוון. הביזור של העקבות הדיגיטליים נובע מטכניקת העברת המידע באינטרנט, הכוללת פירוק של "חבילות" המידע ושיגורן על פני כמה מחשבים (Packet switched),[32] ומשיטת ההחזקה והשימוש במידע. מרחב הסייבר מאפשר שירותים של אגירת מידע במחשבים מרוחקים באופן המאיין את ההצמדה הפיזית בין המחזיק לבין הנכס המוחזק על ידו. שירותי דוא"ל (Webmail) כגון Gmail ו־Yahoo! מספקים, בצד שירות התקשורת, גם שירות של אחסון מידע אישי בנפחים שגדלו עם השנים.[33] שרתי FTP[34] רבים מציעים שירותים של אחסון מידע לצורך החלפת קבצים מהירה ויעילה בין כמה גורמים. בשנים האחרונות נהפכה שיטת מחשוב הענן (Cloud computing)[35] לשיטה מקובלת להחזקת שירותים, תכניות ומידע במחשבים מרוחקים, תוך

בודפשט"): Convention on Cybercrime, art. 16-17, Nov. 23, 2001, E.T.S. No. 185.

31 לדיון בנושא זה, החורג מגבולות המאמר, ראו מיכאל בירנהק "חשיפת גולשים אנונימיים ברשת" חוקים ב 51, 89–94 (2010) (לטיעון המצדד בתפישת הזכות לאנונימיות כזכות הנגזרת מהזכות לפרטיות); McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995); בירנהק **מרחב פרטי**, לעיל ה"ש 21, בעמ' 306–311 (לתפישת הזכות לאנונימיות כזכות הנגזרת מחופש הביטוי); אורג **זכות לזהות אינפורמטיבית**, לעיל ה"ש 19, בעמ' 116–143 (לתפישת הזכות לאנונימיות כזכות עצמאית); ויסמונסקי **חקירה פלילית במרחב הסייבר**, לעיל ה"ש 14, בעמ' 262–265, 301–303.

32 מידע היוצא ממחשב מקור דרך האינטרנט אל מחשב יעד מתפרק לחבילות מידע (packets): בכל חבילה יש פתיח (header) הכולל את יעד המידע, את תוכן המידע כן וסוגר (trailer) ובו מידע לגילוי שגיאות. הנתבים באינטרנט מבצעים שני תהליכים המאפשרים להעביר מידע מהמקור אל היעד: עיבוד מסלול (route processing) וקידום של חבילות המידע (packet processing).

33 עד לפני זמן לא רב, חלק מהתחרות בין ספקיות שירותי הדוא"ל מסוג Webmail כלל הגדלה של נפחי האחסון של התיבה. ראו, למשל, שירות בלומברג "מייקרוסופט תציע נפח אחסון מוגדל של דואר אלקטרוני – במענה לגוגל ויאהו" **גלובס Online** 24.6.2004. www.globes.co.il/news/docview.aspx?did=808555; אדר שלו "שירות הדוא"ל Live Hotmail גדל ל־5 גיגה בייט" **Ynet** 14.8.2007. www.ynet.co.il/articles/1,7340,L-3437367,00.html.

34 ראשי תיבות של File Transfer Protocol: מדובר בפרוטוקול תקשורת מבוסס TCP להעברת קבצים בין מחשבים דרך שרת ייעודי שאליו מתקשרים המשתמשים.

35 ב"מחשוב ענן" הכוונה לשירות שבו משתמש הקצה מעביר את התוכנות היישומיות והמידע האגור שברשותו לאינטרנט, ומחשבו האישי נהפך למעין מסוף בלבד. התוכנות והמידע מנוהלים עבורו על ידי תאגיד המספק שירותי מחשוב ענן. מבחינת משתמש הקצה, האינטרס להשתמש במחשוב ענן הוא להוזיל את עלויות הרכישה והתחזוקה של מחשבו האישי. על פי רוב משתמש הקצה אינו יודע (ואינו מתעניין) במקום הפיזי שבו המידע השייך לו אגור. ראו, למשל, Electronic Privacy Information Center: Cloud Computing http://epic.org/privacy/cloudcomputing/; כן ראו Mark Taylor et al., *Digital Evidence in Cloud Computing Systems*, 26 Computer L. & Sec. Rev. 304 (2010).

שמירה על שליטת המשתמש בהם. כמו כן, ריבוי האפליקציות ואתרי האינטרנט מוביל גם הוא לביזור העקבות הדיגיטליים של השימוש בהן.

ביזור המידע הדיגיטלי בעל הערך החקירתי מתרחש כחלק אינהרנטי מחוויית השימוש הרגילה במרחב המקוון, כשהמשתמש באינטרנט אינו מכוון לתוצאה זו ולעתים אף אינו מודע לה. לביזוריות העקבות הדיגיטליים יש כמה השלכות על אכיפת הדין הפלילי במרחב הסייבר. ראשית, הביזוריות חוצה גבולות מדיניים ומביאה לכך שהחקירה צריכה להתייחס לראיות פוטנציאליות המבוקשות מטריטוריה זרה.[36] שנית, הביזוריות מגדילה את מספר הגורמים שעמם יש לבוא במגע במסגרת החקירה הפלילית, ומטבע הדברים עלויות החקירה ועלויות ההתדיינות הכרוכות בה (הגשת בקשות לצווים שיפוטיים כלפי אותם גורמים, התדיינויות במקרה של התנגדות לאותם צווים שיפוטיים) נהפכות לגבוהות. שלישית, הביזוריות מקשה על חשיפת מבצעי העברות, שכן לעתים מקור packet עלול להצביע על מחשב חשוד שממנו בוצעה פעולה זדונית מסוימת, אך בפועל מחשב זה אינו אלא צומת תמימה שהמידע עבר דרכה.[37]

חמישית, אופן ההפצה והפרסום של תכנים ברשת שונה מזה המוכר בכלי התקשורת הקלאסיים. שיטת הפרסום הקלאסית היא מיחיד אל רבים (one-to-many), שבה יש מוציא לאור, עורך ודובר אחד המעבירים לקהל אנשים את התוכן, לאחר שנבחן על ידי העורך. מרחב הסייבר מאפשר פלטפורמות הפצה השוברות את ההגמוניה של המודל מיחיד־אל־רבים. ראשית, יש באינטרנט פלטפורמות פרסום מרבים אל רבים (many-to-many), המאפיינות את דור האינטרנט 2.0 (web 2.0), שבו כל משתמש רשת יכול להיות דובר, ללא עריכה מוקדמת, ולהפיץ את מסריו, ללא עלות, לכל משתמש אחר ברשת או לקבוצות משתמשים, שלעתים מתקבצות סביב רעיון מסוים, לרבות רעיונות קיצוניים שלא מצאו את מקומם באמצעי המדיה הטרום־אינטרנטיים.[38] לעתים ההפצה נעשית ללא השקעה על ידי פעולת "שיתוף" (share), ללא מאמץ מצדו של מפיץ ההמשך. שנית, יש אפליקציות המאפשרות הפצה בשרשרת ויראלית, מיחיד אל יחיד וכך הלאה. ההפצה הוויראלית מחלישה מאוד את אפקט הדובר או המשדר המרכזי. פעמים רבות היא משולה להתפשטות של אש בשדה קוצים – מהירה וכאוטית. כמו כן, כיום היא מאפשרת בפועל למוסס צווי איסור פרסום, הוראות איסור פרסום סטטוטוריות או הוראות צנזורה המכובדים על ידי כלי התקשורת הממוסדים, הכוללים דובר מרכזי – אך אינם נתפשים כחלים באופן מעשי על משתמשים פרטיים.[39] נראה, כי חקירה פלילית המבקשת לאתר את הדוברים ולאסוף ראיות

36 הצורך לפעול בנוגע למידע בעל ערך חקירתי האגור מחוץ לטריטוריה של המדינה החוקרת מעורר בעיות קשות בתחום סמכות האכיפה, כפי שאפרט להלן בפרק ב(2).

37 ראו Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture and Civil Liability*, 1 J.L. Econ. & Pol'y 197, 205 (2005).

38 ראו Raphael Cohen-Almagor, *Fighting Hate and Bigotry on the Internet*, 3 Pol'y & Internet Art. 6 (2011), *available at* http://onlinelibrary.wiley.com/doi/10.2202/1944-2866.1059/full; Raphael Cohen-Almagor, *Countering Hate on the Internet*, 22 Ann. Rev. L. & Ethics 431 (2014).

39 זאת משום שיש קושי פרקטי ליידע את כלל הציבור – להבדיל מיידוע של כלי התקשורת הממוסדים – בדבר קיומו של איסור הפרסום במקרה מסוים.

קבילות נגדם לצורך העמדה לדין, תהיה מוקשה בנסיבות של הפצת מידע בפלטפורמות המקוונות החדשניות יותר.

מכל האמור מתקבל שארכיטקטורת המרחב המקוון מאפשרת להפיץ תכנים פוגעניים, העולים כדי עברה פלילית, וליצור הפרדה קשה לפענוח בין התכנים לבין דוברם. בכך נוצר מצע גידול אידאלי לעברות הביטוי ותמריץ חיובי לביצוען. כתוצאה מכך אף גוברת בפועל ההקצנה בקרב חלק ממשתמשי המרחב המקוון[40] ואף מתבצעות עברות אלימות במרחב הפיזי.[41]

2. טעמים משפטיים

החלת הכללים המשפטיים הנוהגים במרחב הפיזי על מרחב הסייבר, על מאפייניו הטכנולוגיים־הארכיטקטוניים שמניתי לעיל, מכבידה באופן נוסף על החקירה הפלילית של עברות הביטוי. זאת בהקשרים המשפטיים שיפורטו להלן.

הקושי **הראשון** כרוך **בסמכות האכיפה** (Jurisdiction to enforce)[42] בנוגע למידע הנמצא בשרתים שמחוץ לטריטוריה של המדינה החוקרת. המרחב המקוון הוא מולטי־טריטוריאלי והוא מאפשר למשתמש לפעול דרך כמה מדינות. סמכות האכיפה בתחום הפלילי הייתה מאז ומעולם טריטוריאלית מובהקת, עם מעט מאוד חריגות אקסטרה־טריטוריאליות. עם המעבר למרחב המקוון, "הורכבו" עליו הגבולות המדיניים באופן שיצר מגבלות נוקשות על

40 ראו Ines von Behr et al., Radicalisation in the Digital Era – The Use of the Internet in 15 Cases of Terrorism and Extremism (2013), *available at* www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf; Dan Shefet, Policy Options and Regulatory Mechanisms for Managing Radicalization on the Internet 7-11 (2016), *available at* http://en.unesco.org/sites/default/files/rapport_dan_shefet.pdf.

41 בכל הנוגע לעברות של הסתה לגזענות ולאלימות ברשת, ראו מחקרם של ג'ייסון צ'אן (Chan), אינדיה גוסה (Ghose) ורוברט סימנס (Seamans), שמצא כי חשיפה מוגברת לתכנים של שנאה (Hate speech) ברשת הגבירה את הביצוע בפועל של פשעי שנאה במרחב הפיזי. ראו Jason Chan, Anindya Ghose & Robert Seamans, *The Internet and Racial Hate Crime: Offline Spillovers from Online Access*, 40 MIS Q. 381 (2016), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335637.

42 כאשר בוחנים את סמכותה המשפטית־פלילית של המדינה מקובל להבחין בין שלושה: (א) Jurisdiction to Prescribe – סמכות תחיקתית: החלת הדין המהותי המדינתי על המקרה הנדון; (ב) Jurisdiction to Adjudicate – סמכות שיפוט: סמכות לבית המשפט המדינתי לשפוט את המקרה הנדון; (ג) Jurisdiction to Enforce – סמכות אכיפה: סמכות לסוכני המדינה לאכוף בפועל מקרה מסוים המקים סמכות שיפוט. הבחנה זו מופיעה ב־Restatement לעניין המשפט הבין־לאומי האמריקני: Restatement (Third) of Foreign Relations Law of the United States (Am. Law Inst. 1987); בהקשר של כתיבה על סמכות באינטרנט ראו גם את ההבחנה בין סמכות תחיקתית, שיפוטית ואכיפתית, כפי שהיא מופיעה אצל ברנר וקופס: Susan W. Brenner & Bert-Jaap Koops, *Cybercrime Jurisdiction: An Introduction, in Cybercrime and Jurisdiction: A Global Survey 1–7* (Bert-Jaap Koops & Susan W. Brenner eds., 2006). ראו עוד Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. High Tech. L. 1 (2004). הטיעון שאביא להלן מתייחס לסמכות **אכיפה** במרחב המקוון.

סמכות האכיפה. בהתאם לכך, מקום הימצאם של המחשב או השרת, שבו המידע הממוחשב מאוחסן, הכתיב כי איסוף המידע לצורכי חקירה ייעשה על ידי המדינה שבה נמצא המחשב או השרת.[43] מכאן, שככל שהמדינה החוקרת נדרשת למידע ממוחשב האגור מחוץ לטריטוריה שלה, הרי שעל פי המשטר המשפטי המקובל כיום במרבית מדינות העולם היא נדרשת להגיש בקשה לעזרה משפטית. מאחר שהמרחב המקוון הוא מולטי־טריטוריאלי, החקירה תיחשב בין־לאומית מבחינת ההיזקקות לעזרה משפטית, ולעתים תידרשנה בחקירה אחת כמה וכמה בקשות לעזרה משפטית. אלא, שמנגנון העזרה המשפטית הוא אטי, מסורבל ותלוי בשיתוף פעולה ובהדדיות. על פי רוב, העזרה המשפטית מחייבת פליליות כפולה (Dual criminality) במובן זה שהמעשה שמבקשים לאכוף ייחשב לאסור על פי דין בשתי המדינות – המדינה החוקרת והמדינה שאליה הוגשה בקשת העזרה המשפטית.[44] המולטי־טריטוריאליות של המרחב המקוון עלולה ליצור תופעה של סחרור דינים: ככל שמיקום השרת ישפיע על הגדרת המיקום של הפעילות הפלילית, הנטייה של מנהלי האתרים תהיה להעתיק את פעילותם למדינות שאין בהן איסור פלילי על הפעילות, גם אם במדינות אחרות יש איסור כזה. כך, יוכלו אותן מדינות להימנע מחקירה ומהעמדה לדין בהיעדר פליליות כפולה במעשים הנחקרים.[45]

הקושי **השני** נוגע ל**התאמת הדין הפלילי המהותי** להתנהגויות במרחב המקוון. אין חולק כי מרבית איסורי הדין הפלילי נכתבו עבור התנהגויות המתבצעות במרחב הפיזי. עם העתקת חלק מהפעילות העבריינית למרחב הסייבר, ובכלל זה עברות הביטוי, מתעוררות שאלות בדבר ההתאמה או אי־ההתאמה של הוראות החוק הקיימות להתנהגות האסורה בגרסתה המקוונת. כך, למשל, מתעוררת השאלה אם ההגדרה של "פרסום" מתאימה לכל צורות ה"פרסום" המתקיימות כיום במרחב הסייבר – פרסומי שרשרת ויראליים, פרסומים אוטומטיים ברשימות תפוצה (mailing lists), פרסומים באמצעות שיתוף (share) ברשתות חברתיות וכדומה.[46]

---

43 להרחבה ולניתוח ביקורתי של בסיס זה ראו חיים ויסמונסקי "חקירה פלילית באינטרנט במגבלות הטריטוריה" **הפרקליט** נב 309 (2013).

44 מנגנון העזרה המשפטית קבוע בחוק עזרה משפטית בין מדינות, התשנ"ח-1988 (להלן: חוק עזרה משפטית). לעומת המודל של העזרה המשפטית הקלאסית, המגולם בחוק עזרה משפטית, אמנת מועצת אירופה בדבר פשעי מחשב (Convention on Cybercrime), שנחתמה בבודפשט בשנת 2001, מנסה להתמודד עם בעיות של צורך ב־transborder search באינטרנט על ידי פיתוח של מנגנוני שיתוף פעולה מהירים בין שתי מדינות. חרף זאת, מנגנוני אמנת בודפשט מוגבלים משום שהם חלים רק על המדינות שהצטרפו לאמנה.

45 ראו, למשל, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553, 577-580 (1998). ראו גם יובל קרניאל וחיים ויסמונסקי "חופש הביטוי, פורנוגראפיה וקהילה באינטרנט" **מחקרי משפט** כג 259, 294-298 (2006), בהקשר לעברות של פרסומי תועבה באינטרנט.

46 השוו עם הגדרת "פרסום" שבס' 34כד לחוק העונשין, וכן עם הגדרת "פרסום" שבס' 2 לחוק איסור לשון הרע. ההגדרה שבחוק העונשין היא ההגדרה הכללית ואילו ההגדרה שבחוק איסור לשון הרע חלה על חלק מהעברות הפליליות, על פי הפניה מיוחדת בדבר החקיקה שבו מדובר. ראו, למשל, הגדרת "פרסום" שבס' 3 לחוק הגנת הפרטיות, המפנה לחוק איסור לשון הרע.

הקושי **השלישי** נוגע ל**התאמה של סמכויות החקירה** הקיימות – שהניחו כי החקירה מתבצעת במרחב הפיזי – לצורכי החקירה במרחב המקוון. סמכויות החקירה מניחות כי הראיות המבוקשות נמצאות בטריטוריה של המדינה החוקרת, וכי הראיות מיוצגות במרחב הפיזי, באטומים ולא בביטים.[47] כך, סמכויות החקירה אינן כוללות התייחסות למגוון צרכים פוטנציאליים כגון סמכות לדרוש מספקיות שירות מקוונות לפתוח הצפנות והגנת ססמאות במסגרת שירותיהן, סמכות לערוך חדירה סמויה לחומרי מחשב או סמכות לחדור לחומרי מחשב האגורים מחוץ לטריטוריה של המדינה החוקרת.[48] ייאמר מיד כי אין אפשרות לספק את מלוא צורכי החקירה במרחב הסייבר, שכן הענקת סמכויות חקירה תואמות משמען גביית מחיר בלתי־נסבל מבחינת הפגיעה החוקתית בזכויות המשתמשים במרחב המקוון – ניטור ומעקב קבועים אחר הפעילות המקוונת של כלל משתמשי המרחב המקוון. זאת, מעבר לעובדה שהענקת סמכויות חקירה תואמות משמען נקיטה עצמאית של פעולות אקסטרה־טריטוריאליות (אוני־לטרלי), העלולה להתפרש כפגיעה בריבונות של מדינות זרות שהמידע הממוחשב הדרוש לחקירה הפלילית אגור בשטחן, כפי שציינתי לעיל בהקשר של מגבלות סמכות האכיפה במרחב המקוון. על כן, ערוץ האכיפה האלטרנטיבית מגלם חלופה שהפגיעה הגלומה בה פחותה ומידתית יותר מזו הכרוכה בחלופה של סיפוק כל צורכי החקירה של עברות ביטוי במרחב המקוון.[49]

3. טעמים מוסדיים

הקושי המוסדי **הראשון** הכרוך בחקירה פלילית במרחב הסייבר הוא שחקירה כזו מצריכה **מומחיות טכנית גבוהה** בתחום הרשתות ותקשורת נתונים, ואין די מומחיות כזו בקרב רשויות החקירה.[50] נוכח התפתחות המחשוב, ובמיוחד נוכח התפשטות המרחב, התפתח ענף חדש בתחום החקירה הפלילית שעניינו פורנזיקה של חקירות מחשב (Computer forensics)

עוד לעניין זה ראו את **הנחיית פרקליט המדינה** מיום 31.8.2016 בנושא פרסומים פדופיליים: "פרסום, החזקה וצריכה של חומר תועבה ובו דמותו של קטין" הנחיית פרקליט המדינה 2.22 (התשע"ו), שבה מופיעה פרשנות מרחיבה לאפשרות לראות כ"מפרסם", כמובנו בס' 34כד לחוק העונשין, מי שמעביר את התוכן המדובר לאדם אחד בלבד בנסיבות מסוימות.

47 על תפישת המידע הממוחשב כמיוצג באטומים ולא בביטים ראו ניקולאס נגרופונטי **להיות דיגיטלי** 17–25 (עמנואל לוטם מתרגם, 1996).

48 להרחבה ראו ויסמונסקי **חקירה פלילית במרחב הסייבר**, לעיל ה"ש 14, בעמ' 139–142, 203–219.

49 עם זאת, אין זאת אומרת שאין מקום לערוך שינויים והתאמות לגבי חלק מצורכי החקירה במרחב המקוון, החסרים כיום אך ורק בשל העובדה שהסיטואציה החקירתית המקוונת לא התקיימה קודם לכן, ולכן הסמכויות שנוסחו עבור המרחב הפיזי לא כללו את קשת הפעולות הנדרשות כיום. לדיון בנושא זה ראו ויסמונסקי **חקירה פלילית במרחב הסייבר**, לעיל ה"ש 14, בעמ' 287–303.

50 **ראו** U.N. Office on Drugs and Crime, *Comprehensive Study on Cybercrime (Draft)* 152-156 (February, 2013), *available at* www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

או Cyber forensics).[51] בשל קצב ההתפתחות המואץ של עולם המחשוב נדרשת הכשרה רצופה של מומחי הפורנזיקה הדיגיטלית וכן נדרשת הצטיידות במכשור מתאים ועדכני. נוכח הקצב המואץ של ההתפתחות הטכנולוגית, המחייב את החוקרים הפליליים להכשרה מתאימה, ונוכח ההכרח לאסוף ראיות בלי לזהם את הזירה הממוחשבת, בלי לשבש את טיב הראיה המבוקשת ובלי להתערב בגרסתה המקורית – פער האכיפה רק הולך וגדל.[52] יצוין עוד כי המחוקק הישראלי הכיר, למשל, בדרישת המיומנות לחוקר המבצע פעולות של חדירה לחומר מחשב,[53] אולם החוק אינו מתייחס למידת המיומנות הדרושה. הפסיקה פירשה את דרישת המיומנות כדרישה גמישה, התלויה בפעולת האיסוף המסוימת שהחוקר ביקש לבצע ובמידת מורכבותה.[54] מכאן, שההימנעות של המחוקק או של הפסיקה מקביעת

---

51 ענף זה מתמודד עם סוגיות של מיצוי ראיות דיגיטליות המחייבות התמודדות עם סוגיות של הצפנה, אחזור מידע, שחזור מידע מחוק (ברמות שונות של עוצמת המחיקה), עקיפת סמאות ועוד. ראו: Linda Volonino, Reynaldo Anzaldua & Jana Godwin, Computer Forensics: Principles and Practice 22-52 (2006), שם המחברים מתארים את התפתחות התחום כתחום פורנזי עצמאי בעבודת המשטרה. למדריכי שטח לחוקרי משטרה בזירה האינטרנטית ראו, למשל, Bruce Middleton, Cyber Crime Investigator's Field Guide (2nd ed. 2005); Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes (Albert J. Marcella & Robert S. Greenfield eds., 1st ed. 2002).

52 ראו, למשל, Yee Fen Lim, Cyberspace Law: Commentaries and Materials 256-257 (1st ed. 2003); Computer Law 585-58 (Chris Reed & John Angel eds., 6th ed. 2007). כן ראו McAffe, McAffe Virtual Criminology Report: Cybercrime Versus Cyberlaw 14-16 (2010), *available at* http://img.en25.com/Web/McAfee/mcafee_VCR_US_lowResFinal_REV.pdf. עוד על הפיגור המובנה של המשטרה אחר התפתחות הפשיעה המקוונת ראו אצל Marc C. Goodman, *Why the Police Don't Care About Computer Crime*, 10 Harv. J.L. & Tech. 465, 482-488 (1997).

53 ראו ס' 23א(א) לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 (להלן: הפסד"פ). "בעל תפקיד מיומן" אינו מוגדר בפסד"פ או בשום חוק אחר. המשטרה, ובעקבותיה המשטרה הצבאית החוקרת (מצ"ח), הנהיגו קורס לחקירות מחשב.

54 ת"פ (מחוזי י-ם) 2077/06 **מדינת ישראל נ' אריש** (פורסם בנבו, 4.12.2007). בעניין זה נבחן מקרה שבו שוטר, שאינו חוקר מחשבים, חדר לטלפון סלולרי של חשוד לצורך עיון ותיעוד של מסרוני SMS שהיו שמורים במכשיר. השופטת בן־עמי כתבה: "[...] אף בהנחה כי טלפון סלולארי עונה על הגדרת מחשב, במישרין או בעקיפין, ברור כי לצורך הפקת מידע ממנו, כגון: רשימת שיחות נכנסות ויוצאות, מיסרונים שנשלחו וכו', אין צורך במיומנות מיוחדת מעבר למיומנות של אדם סביר [...] ובנסיבות אלו 'בעל תפקיד מיומן לביצוע פעולות כאמור' יכול להיות אף שוטר רגיל". למעשה, מדבריה של השופטת בן־עמי נובע כי "בעל תפקיד מיומן" הוא מושג גמיש ולא קבוע, וכגודל המשימה הפורנזית בחומר המחשב כך גודל המיומנות שתידרש מחוקר המחשבים. מכאן, שקורס חקירות מחשב של המשטרה אינו בהכרח מקנה מיומנות לכל פעולות איסוף הראיות הדיגיטליות, כפי שאי־השתתפות בקורס אינה בהכרח שוללת מיומנות לכל הפעולות. בהמשך לכך, אם יידרש חוקר מחשבים לבצע פעולה חקירתית מתוחכמת כגון התקשרות למחשב מרחוק, הורדת החומר, פיצוח הצפנתו ומיונו – בהחלט ייתכן שתעודת חוקר המחשבים המיומן לא תספיק כדי להוכיח מיומנות מספקת להתמודדות עם המשימה. "בעל

רף מיומנות מדויק למעשה יוצרת תמריץ שלילי מפיתוח מיומנות בסטנדרט ראוי ואחיד, שכן אין רף קבוע שהכרחי לעמוד בו.

הקושי המוסדי **השני** נובע מכך ש**מבנה המשטרה ותפישת ההפעלה שלה אינם מתאימים לחקירות בזירה המקוונת**. ההסבר לכך הוא שהמשטרה המקצועית־המודרנית פותחה להתמודדות עם עברות במרחב הפיזי, ונוכח העובדה שלפשיעה במרחב הסייבר יש מאפיינים שונים מאלה של הפשיעה במרחב הפיזי, המשטרה עלולה להיכשל בניסיונה להתמודד עמה. כך, למשל, טענה סוזן ברנר (Brenner) כי המשטרה המקצועית המודרנית מניחה שהפשע ניתן למיקום פיזי, שהוא מוגבל מבחינת היקפו ואופן ביצועו בהתאם למגבלות העולם הפיזי, שהוא מוגבל מבחינת כמות הנפגעים הפוטנציאליים בהתאם למגבלות הפיזיות, ושהוא מאופיין דמוגרפית וגאוגרפית (אזורי פשיעה). על כן, המשטרה מתמקדת בפורנזיקה של ניתוחי זירה (CSI) ובמיקוד מראש של מאמצי השיטור לאזורים מסוימים.[55] הנחות אלה אינן מתקיימות במרחב הסייבר, שם הפשיעה אינה ניתנת למיקום, אינה ממוקדת גאוגרפית, אינה מוגבלת מבחינת ההיקף ומבחינת כמות הנפגעים נוכח העובדה שהפשיעה היא אוטומטית ובעלת פוטנציאל לשכפל את עצמה ללא התערבות אנושית, ואין לה אפיון דמוגרפי או גאוגרפי מסוים. מכאן, שאין מדובר רק בהכשרה טכנית של החוקרים אלא בשינוי מערכתי כולל הנדרש לצורך שיטור במרחב הסייבר.

הקושי המוסדי השלישי נעוץ בעובדה שהזירה המקוונת נתפשת כווירטואלית, ולכן יש נטייה טבעית לשכוח שהפגיעות הנגרמות עקב פשיעה מקוונת הן ממשיות. במציאות של ריבוי משימות על המשטרה עלול להיווצר תמריץ שלילי **להזניח באופן יחסי**, בין במודע ובין שלא במודע, **את החקירות בזירה המקוונת** לטובת שאר המשימות. הבעיה מחריפה במיוחד כשמדובר בצורך בחקירת "חשיפה", כלומר: חקירה הנערכת שלא על פי תלונה או הנחיה מגבוה לפתיחה בחקירה, ושלא בעקבות התרחשות של אירוע מסוים ה"זועק" לחקירה (חקירת "זירה"), אלא בעקבות תובנה מודיעינית־משטרתית שתופעות פשיעה מסוימות מתקיימות במידה ניכרת המחייבת אכיפה יזומה של המשטרה באמצעים יזומים שלה, שיביאו לחשיפה של העברות ושל מבצעיהן.[56] חקירות החשיפה הן מורכבות ויקרות יותר והן אינן מניבות תוצאות מהירות. עם זאת, חקירות החשיפה חיוניות היכן שבהיעדרן

תפקיד מיומן" ייחשב מי שיוכיח בבית המשפט שמומחיותו מתאימה למשימה, בדומה לעדים מומחים אחרים הבאים לפני בית המשפט וכשלב מקדמי נדרשים להוכיח את מומחיותם בקשר לפעולה שעליה הם מתבקשים להעיד. לעומת זאת, דפדוף בספר טלפונים במכשיר טלפון נייד או קריאת תכתובות דוא"ל האגורות במחשב אינם פעולות המצריכות מיומנות מיוחדות, שכן הן פעולות המתבצעות כעניין שבשגרה על ידי כל אדם, וייתכן ששוטר שאינו בעל תעודת "חוקר מחשבים מיומן" יוכל לבצען כראוי.

55 ראו Susan Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. Sci. & Tech. L. 1, 62 (2004).

56 דוגמאות קלאסיות, מהמרחב הפיזי, לעברות המצריכות פעולות חשיפה יזומות של המשטרה הן עברות של שני מעורבים (או יותר) בעסקת העברה, כגון עברות סמים, שבהן יש קונה ומוכר של סם מסוכן – שניהם מבצעי עברות שלא ייטו לדווח למשטרה על הפעילות העבריינית. דוגמה אחרת היא עברות של סחיטה באיומים, שבהן סביר להניח שהנסחט לא יפנה למשטרה מחשש לשלומו – בדיוק כפי שאותו חשש הביא אותו להיסחט על ידי מבצע העברה.

יופקרו עברות פליליות מסוימות כבלתי־מטופלות כלל או כעברות המטופלות חלקית בלבד (בנסיבות שבהן לא נדרשת חשיפה ביוזמת המשטרה). אפשר להניח שחקירות חשיפה במרחב הסייבר תהיינה מורכבות אף יותר, בשל המאפיינים ה"מסבכים" הייחודיים של המרחב, הנוספים על המאפיינים ה"מסבכים" של חקירות החשיפה במרחב הפיזי. הכוונה בעיקר לשלושת המאפיינים הבאים: (1) חלק מתופעות הפשיעה במרחב הסייבר כוללות פיזור הנזק שבהתנהגות העבריינית על פני מספר רב של קרבנות, כשמידת הפגיעה לכל קרבן בנפרד לא תהיה גבוהה מדי ולא תביא אותו לחצות את הסף של הגשת התלונה (בדומה למתרחש, למשל, במקרים של זיהום אוויר או במקרים המצדיקים תובענות ייצוגיות);[57] (2) לעתים הקרבן אינו יודע כי נפגע בפועל מעברה משום שהעברה התבצעה ללא מגע כלשהו עמו ובאמצעים אוטומטיים;[58] (3) ספקיות שירות רבות הנופלות קרבן לעברות של חדירה לחומר מחשב, למתקפות DDoS[59] וכדומה יחששו לחשוף את פגיעותן בהגשת תלונה למשטרה מחשש לבריחת לקוחות.[60]

אל מול כל האמור לעיל לגבי הטעמים המוסדיים יצוין כי משטרת ישראל הכריזה על מפנה מתוכנן בתחום החקירות הפליליות במרחב הסייבר,[61] ופעלה בשלוש־ארבע השנים האחרונות להרחבה ניכרת של מערך חוקרי עברות המחשב שיעסקו בהגברת האכיפה

57 כדוגמאות אפשר לציין את התופעה של הפצת דואר זבל המגיע לרבבות משתמשי אינטרנט, או השתלטות על מספר רב של מחשבים לצורך "גיוסם" למתקפות מבוזרות של מניעת שירות DDoS (Distributed Denial of Service). הכוונה במונח זה הוא ל"מתקפה" מקוונת שבה שרת מסוים מותקף בבת אחת על ידי מספר רב של מחשבים, שכולם הודבקו מראש בתוכנה זדונית. תוכנה זו "מגייסת" את משאבי המחשוב של המחשבים הנגועים (המכונים Bots) כדי לבצע פעולה של התקשרות מתוזמנת עם השרת המותקף, כדי ליצור עליו עומס חריג במועד מסוים שיביא לקריסתו עקב "הצפתו" מעבר לקיבולתו התקשורתית. עצם ההשתלטות על המחשבים המבצעים את התקיפה (Bots) היא עברה פלילית של חדירה לחומר מחשב שלא כדין כדי לעבור עברה אחרת, לפי ס' 5 לחוק המחשבים, התשנ"ה–1995, כשדבר ההשתלטות אינו מורגש בפועל.

58 לאפיון זה של הפשיעה באינטרנט ראו, בהקשר כללי, Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, 4 N.C. J.L. & Tech. 1, 26-27 (2002).

59 להבהרת המונח ראו לעיל ה"ש 58.

60 לדיון בקושי זה (על רקע הדיון בחקיקה המחייבת יידוע של הרגולטור או של הציבור במקרה של אירוע אבטחת מידע) ראו Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible*, 24 Berkeley Tech. L.J. 1133 (2009).

61 ראו, למשל, משטרת ישראל "דין וחשבון שנתי 2013 ע"פ חוק חופש המידע, התשנ"ח–1998" 21, 24 (2013), www.police.gov.il/Doc/TfasimDoc/din_veheshbon_2013.pdf, שם מפורט תהליך ההקמה של יחידת הסייבר המשטרתית בלהב 433 וכן תהליך הפיכתה של מחלקת הסיגינט באגף החקירות והמודיעין לחטיבה. חטיבה זו עוסקת, בין היתר, באיסוף מודיעין במרחב הסייבר. כן ראו התיאור של יחידת הסייבר הארצית בלהב 433 באתר משטרת־ישראל: "אגף חקירות ומודיעין: יחידת הסייבר" **משטרת ישראל**. www.police.gov.il/contentPage.aspx?pid=308&mid=9. בצד היחידה הארצית התרחב מערך הסייבר המשטרתי גם למחלקי סייבר בתוך מִפְלַגי ההונאה במחוזות הטריטוריאליים של המשטרה.

הפלילית במרחב הסייבר. אפשר לסמן מפנה זה כחלק מתהליך של היערכות ביטחונית בתחום הסייבר.[62] כמו כן ראוי לציין את ההתפתחות האחרונה במשרד לביטחון פנים, בדמות החלטות הממשלה על הקמת מערך מאו"ר למניעת אלימות ופשיעה נגד ילדים ובני נוער ברשת.[63] במסגרת המערך אמורה להתגבש תפישה הוליסטית, משטרתית ואזרחית, לטיפול, לאכיפה ולמניעה של פשיעה ופרסומים פוגעניים ברשת כלפי קטינים. הקמת מערך מאו"ר להגנה על קטינים במרחב הסייבר עשויה להוביל לתגבור של מערך חוקרי המחשב המיומנים במשטרה. ככל שתהליכים אלה יבשילו, ייתכן כי יפחת משקלם של הטעמים המוסדיים שמניתי לעיל בנוגע לקשיי האכיפה במרחב הסייבר.

*

לסיכום: בפרק זה מניתי מגוון של טעמים – ארכיטקטוניים־טכנולוגיים, משפטיים ומוסדיים -שהובילו לפריחה של עברות הביטוי במרחב הסייבר. כפי שאפשר לראות, מרבית מהמאפיינים שמניתי אינו ייחודי לעברות הביטוי, והוא יכול להשפיע על ההזדמנויות והכדאיות לבצע עברות פליליות מסוגים אחרים.[64] עם זאת, המאפיין של אופן ההפצה והפרסום רלוונטי במישרין ובמיוחד לעברות הביטוי, הנעברות בדרך של "פרסום".

ניתן להגיע לכלל מסקנה כי למול העובדה שעברות הביטוי במרחב הסייבר מתפשטות ומתרבות, הרי שרשויות החקירה מוגבלות ביכולתן לטפל בהן כדבעי. מכאן לכאורה קמה הצדקה לחיפוש חלופות לאכיפה הפלילית המדינתית הנוהגת כיום בנוגע לעברות הביטוי ברשת. החלופות שייבחנו להלן הן החלופות המניעתיות.[65]

---

62 ברמה הלאומית הוקם בשנת 2011 מטה הסייבר הלאומי במשרד ראש הממשלה, האחראי להכוונה של הפעילות בכלל גופי הביטחון בתחום הגנת הסייבר. ראו החלטה 3611 של הממשלה ה־32 "קידום היכולת הלאומית במרחב הקיברנטי" (07.08.2011). נוסף על כך הוקם בשירות הביטחון הכללי אגף סיגינט־סייבר. ראו עמיר רפפורט "השב"כ העידן הקיברנטי: מבט מבפנים" **Israel Defense** (11.4.2014) www.israeldefense.co.il/en/content/%D7%94%D7%A9%D7%91%D7%9B-%D7%91%D7%A2%D7%99%D7%93%D7%9F-%D7%94%D7%A7%D7%99%D7%91%D7%A8%D7%A0%D7%98%D7%99-%D7%9E%D7%91%D7%98-%D7%9E%D7%91%D7%A4%D7%A0%D7%99%D7%9D. כמו כן, בשנת 2015 הוקמה הרשות הלאומית להגנת הסייבר; ראו החלטה 2444 של הממשלה ה־33 "קידום ההיערכות הלאומית להגנת הסייבר" (15.02.2015). באותה שנה הוחלט גם על הקמת זרוע סייבר בצה"ל. ראו יואב זיתון "הרמטכ"ל החליט להקים זרוע סייבר בצה"ל" **Ynet** 15.6.2015 www.ynet.co.il/articles/0,7340,L-4668869,00.html.

63 החלטה 1004 של הממשלה ה־34 "הקמת מערך למניעת אלימות ופשיעה נגד ילדים ובני נוער ברשת (מערך מאו"ר)" (17.01.2016) וכן החלטה 1972 של הממשלה ה־34 "מערך למניעת אלימות ופשיעה נגד ילדים ובני נוער ברשת (מערך מאו"ר)" (27.9.2016).

64 אכן, כאמור לעיל בה"ש 11, אפשר לראות עלייה בפשיעת הסייבר בתחומים אחרים, שאינם בגדר עברות הביטוי.

65 פרט לחלופות המניעתיות ברמת המדינה אפשר לחשוב על חלופות במישורים אחרים כגון אכיפה בין־לאומית, אכיפה "התקפית" (כגון שיבוש פעולתם של מחשבים או מחיקת תכנים ממחשבים הנמצאים במרחב המקוון), אכיפה כלכלית (התמקדות בסיכול אמצעי התשלום המקוונים – רלוונטי לעברות הכוללות רכיב של תשלום), התגוננות עצמית ברמת המשתמש

ג. אכיפה אלטרנטיבית כלפי עברות ביטוי במרחב הסייבר

כידוע, מטרות־העל המרכזיות המקובלות במשפט הפלילי נועדו לשרת תכליות של הפחתת נזקים כתוצאה מהתנהגויות אסורות,[66] ולהגן על ערכים מוגנים המצדיקים הפללה של התנהגויות הפוגעות בהם.[67] בכל הנוגע לעברות הביטוי, לפחות לגבי חלקן אי־אפשר להצביע – לא כל שכן לכמת – את הנזקים הנגרמים בעקבותיהן, וההצדקה שבבסיס האיסור המגולם בהן נובעת בעיקר מתכלית של הגנה על ערכים.[68] מכל מקום, בין ששיטת המשפט מבכרת את עקרון הנזק כעיקרון המנחה למשפט הפלילי ובין שהיא מבכרת את עקרון ההגנה על ערכים, המשפט הפלילי ככלל מבקש להשיג את מטרותיו באמצעות התמודדות עם מבצעי העברות (העושים) ולא ישירות עם העברות עצמן (המעשים). כך, החקירה הפלילית מתמקדת במבצעי העברות ולא בעברות כשלעצמן משום שמטרתה להוביל להעמדה לדין, להרשעה ולענישה.[69]

כפי שהראיתי בפרק הקודם, האכיפה הפלילית הקלאסית נתקלת בקשיים שלפחות חלקם אינם פתירים באופן הנראה לעין. לפיכך, יש לבחון פיתוח של תחום ההגנה מפני עברות הביטוי במרחב הסייבר באופן שישרת את התכלית שבבסיס עברות הביטוי, גם אם לא יוביל בהכרח להעמדה לדין של מבצעיהן. יש צורך ממשי בפיתוח אסטרטגיית הגנה מפני **עברות**

הפרטי, הקהילה המקוונת או ספקית השירות ועוד. לדיון בחלופות אלה ראו ויסמונסקי **חקירה פלילית במרחב הסייבר**, לעיל ה"ש 14, בעמ' 45–113.

66 זהו עקרון המוצא להגדרת מטרת־העל של המשפט הפלילי, לפחות בשיטת המשפט האנגלו־אמריקנית. ראו JOHN STEWART MILL, ON LIBERTY AND THE SUBJECTION OF WOMEN 13 (1879). העיקרון הראשוני הזה, שניסח מיל, אומץ על ידי רבים. ראו, למשל, H.L.A. HART, LAW, LIBERTY AND MORALITY 4-5 (1963); Ronald Dworkin, *Lord Devlin and the Enforcement of Morals*, 75 YALE L.J. 986, 992 (1966). כן ראו מחקרו המקיף של פיינברג: JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW: HARM TO OTHERS (1984).

67 זהו עקרון המוצא להגדרת מטרת־העל של המשפט הפלילי בשיטת המשפט הקונטיננטלית וזו גם התפישה המקובלת בנוגע לדיני העונשין בישראל. ראו, למשל, את מחקריו של מרדכי קרמניצר: מרדכי קרמניצר "הערות לחקיקה, האם חסרי עבירות אנחנו?" **משפטים** יג 159, 160 (1983); מרדכי קרמניצר **המרמה הפלילית** 39 (2009). ראו גם NINA PERSAK, CRIMINALISING HARMFUL CONDUCT: THE HARM PRINCIPLE, ITS LIMITS AND CONTINENTAL COUNTERPARTS 23-31 (2007).

להרחבה – הן על עקרון הנזק והן על עקרון ההגנה על ערכים – ראו עוד אצל אסף הרדוף "פסקת ההפללה: טיעון חוקתי נגד הפללה – על גבולות המשפט הפלילי וגבולות פסקת ההגבלה" **משפטים** מב 243 (2012); אסף הרדוף **הפשע המקוון** 39–44 (2010). הרדוף פיתח מודל מפורט יותר של הצדקות לקביעת התנהגויות מסוימות כעברות, ומובן כי עקרון הנזק יכול לשמש עיקרון מוצא בלבד ולא תבחין יחיד לקביעה מתי ראוי יהיה לאסור על התנהגות מסוימות כעברה ומתי לא.

68 לדוגמה, העברה הפלילית של פגיעה ברגשי דת, לפי ס' 173 לחוק העונשין, מנוסחת כך שאינה תלויה בהתממשות או בהסתברות להתרחשות נזק, וכך גם ס' 24 לחוק המאבק בטרור, האוסר על גילוי הזדהות עם ארגון טרור או הסתה לטרור.

69 ראו בהקשר זה קוזלובסקי "Paradigm Shift", לעיל ה"ש 29, בעמ' 106–107.

הביטוי בצד אסטרטגיית אכיפה כלפי **עברייני** הביטוי. אסטרטגיה זו תתמקד בהגנה מפני המעשה עצמו במקום בהתמודדות עם המעשה באמצעות התמודדות עם העושה.

כפי שהראיתי בסוף הפרק הקודם, קשה מאוד לזהות ולאתר מבצעים של עברות במרחב הסייבר, לאסוף נגדם ראיות קבילות ולהעמידם לדין באופן שיוביל לצמצום פגיעתם. עם זאת, מאחר שעסקינן בעברות ביטוי, הרי שמדובר בהתנהגויות שנועדו להגיע לקהל רחב ולפיכך, ככלל, הן גלויות וניתנות לאיתור בקלות יחסית. יוצא, אפוא, ש**המעשה** עצמו ניתן לאיתור ואף להפללה (קרי: לבחינת תוכנו ולקביעה שמדובר בפרסום אסור לכאורה על פי החוק), אך ההתמודדות בכלים משפטיים־ראייתיים עם **המבצע** קשה ומורכבת.

כעת אעבור להצגת הפעולות שאפשר לנקוט במסגרת פיתוח של אסטרטגיית אכיפה אלטרנטיבית. המשותף לכולן הוא כי המדובר בפעולות שנועדו למנוע את הפרסום האסור – את הפצתו בכלל ואת הפצתו לקהל היעד הרלוונטי לפרסום בפרט. לאחר מכן אציג את ההבחנה בין פעילות במישור הוולונטרי־ההסכמי, המבוססת על שיתופי פעולה בין המדינות לבין ספקיות השירות האינטרנטיות השונות ועל פעילות של הסדרה עצמית של הספקיות, לבין פעילות במישור הכופה, היינו: הוראות חוק וצווים שיפוטיים שנועדו לחייב מניעה או צמצום של הפרסום האסור, אף בניגוד לרצון של ספקית השירות או בניגוד לתנאי השימוש שלה.

1. מיון של פעולות ההתגוננות והמניעה

להלן אציג את פעולות ההתגוננות והמניעה השונות, תוך סיווגן בהתאם לפעולה הטכנולוגית המתבצעת במסגרתן.[70]

(א) הסרת תכנים אסורים. הסעד הישיר וה"כירורגי" ביותר הוא כמובן הסרת התוכן האסור עצמו. בהקשר זה יש להבחין בין שלושה סוגי פעולות: (1) מניעת פרסום מראש: פעולה של מניעה מוקדמת היכולה להתבסס על מערכות טכנולוגיות או אנושיות כמו "אישור עורך" לפני פרסום התוכן בפועל; (2) הסרת הפרסום לאחר העלאתו; (3) ניטור עותקים של התוכן והסרתם מכל מקום שבו הם נמצאים או יימצאו בעתיד. פעולה זו יכולה להתבצע באמצעים טכנולוגיים למיניהם כגון פעולת Hash[71] לתוכן האסור וניטורו כל אימת שמנסים לפרסמו מחדש. כמו כן, אפשר לבצעה גם באמצעות בקרה אנושית, אף שמטבע הדברים מדובר בפעולה יקרה בהרבה ואטית.

ייאמר מייד, כי בפועל, מניעת הפרסום מראש וכן ניטור של תוכן אסור שיפורסם בעתיד הן פעולות המחייבות להטיל על ספקיות השירות אחריות וחובה משפטית. אלה עשויות להשית על הספקיות עלויות ניכרות; הן מתערבות בחופש העיסוק שלהן ובנאמנותן כלפי המשתמשים בשירותיהן, והן עשויות לחייבן אף לשנות במידה מסוימת את ייעודן, ככל שאין הוא כולל מנגנון של אישור עורך או ניטור תכנים.

---

70 ניתוח המשמעות המשפטית של פעולות ההתגוננות והמניעה לסוגיהן יובא בהמשך המאמר.

71 הכוונה להרצת פונקציה מתמטית על הקובץ הכולל את התוכן האסור (תמונה, סרט או טקסט), באופן המייצר מספר מזהה חד־ערכי לתוכן. כאשר משתמש אינטרנט מבקש להעלות שוב את התוכן, אפשר לנטרו ולמנוע את פרסומו ביעילות באמצעות זיהוי "חתימתו" הדיגיטלית של הקובץ, המביאה לאותו מספר מזהה חד־ערכי כשהוא נסרק במערכת הניטור.

(ב) חסימת גישה לאתרים או לאפליקציות בהם מתפרסם תוכן אסור. מבחינה טכנית־אופרטיבית ניתן למנות כמה סוגי חסימה:[72] (1) חסימה לפי כתובת IP (IP Blocking): כל אתר אינטרנט נמצא בשרת כלשהו, ולשרת יש כתובת IP מזוהה וקבועה באינטרנט. ספקיות הגישה יכולות לחסום את הגישה לכתובת IP מסוימת, כך שכל אימת שמשתמש האינטרנט המנוי על שירותיהן יבקש להתקשר לכתובת IP אסורה תימנע היכולת לבצע את ההתקשרות האמורה; (2) הסרת רישום של אתר פוגעני (Deregistration). אפשר לקבוע בשרתי ה־DNS המדינתיים, המנהלים את כל שמות המתחם תחת הסיומת של המדינה (למשל: ".il" בישראל או ".fr" בצרפת) כי יוסר הרישום של שם מתחם מסוים שיש בו תוכן שמבקשים לחסום את הגישה אליו;[73] (3) חסימה לפי שרת DNS ספציפי הממען את גולש האינטרנט ליעדו. לפי שיטה זו, כל אימת שיוקלד שם מתחם של אתר אסור תופסק פעולתו של שרת DNS עבור הגולש המבקש, ושם האתר לא יתורגם לכתובת IP המובילה אליו; (4) חסימה באמצעות סינון על ידי פרוקסי (Http Proxy Filtering). שיטת חסימה זו מבוססת על כך שמשתמשי האינטרנט יחויבו "לגלוש" באמצעות שרת פרוקסי. שרת זה יפעיל סינון תכנים ויעביר אל הגולשים דרכו אך ורק תכנים מסוננים; (5) חסימה על ידי האתר עצמו כלפי משתמשי אינטרנט ממדינה מסוימת (Geo-blocking). סוג זה של חסימה שונה מקודמיו במובן זה שהוא מתבצע על ידי מנהלי האתר המפרסם את התוכן הנדון. מנהלי האתר יכולים להגביל גישה של משתמשי אינטרנט מטווח כתובות IP של מדינה מסוימת, ובכך למנוע ממשתמשי האינטרנט מאותה מדינה להיחשף אל התוכן, העשוי להיחשב פוגעני במדינתם, אף שאינו פוגעני על פי תפישתם ועל פי דיני מדינתם של מנהלי האתר.[74]

---

72 ראו Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering*, *in* Access Denied: The Practice and Policy of Global Internet Filtering 57, 59-63 (Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2008).

73 DNS הם ראשי תיבות של Domain Name System. מדובר בפרוטוקול שנועד להקל על השימוש ברשתות תקשורת. התקשורת האינטרנטית מבוססת כתובות IP, שהן כתובות מספריות, ואילו DNS הוא שֵׁמי. כדי שיתאפשר למשתמשי האינטרנט להגיע לאתרים המבוקשים על־ידם מתנהלת מערכת של תרגום שמות המתחם המילוליים לכתובות ה־IP המספריות. זו המהות של מערכת ה־DNS. מערכת זו היא גם הירכית: מרמת ה"שורש" הגבוהה ביותר (הכוללת כיום 13 שרתים, Root servers, שחלקם מבוזרים פיזית ומופעלים באמצעות ראוטרים מיוחדים הנקראים "anycast"), דרך הרמה המתייחסת לסיומת המדינה שבה נמצא אתר האינטרנט, דרך רמת־המשנה (המתייחסת לסוג השירות בתוך המדינה – סיומת gov ממשלתית, סיומת co מסחרית, סיומת org של ארגונים לא־ממשלתיים ועוד), ועד לרמה הפרטנית (המתייחסת לשם האתר עצמו במדינה מסוימת ובסוג שירות מסוים).

74 ראו פירוט ודוגמאות אצל Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World 74-75 (2006). לדוגמאות עדכניות יותר, של חסימת תוכני Youtube לגולשים מטורקיה ומפקיסטן, ראו (בהתאמה) Dara Kerr, *YouTube cedes to Turkey and uses local Web domain*, Cnet (Oct. 2, 2012), www.cnet.com/news/youtube-cedes-to-turkey-and-uses-local-web-domain/; M. Ilyas Khan, *What will Pakistanis See on Youtube?*, BBC News (Feb. 8, 2016), www.deccanherald.com/content/527559/what-pakistanis-see-youtube.html.

(ג) סינון תכנים אסורים. מבחינה אופרטיבית אפשר לדבר על שני מנגנונים: (1) ככל שמדובר בספקיות גישה לאינטרנט או בספקיות תוכן, אפשר להתקין תוכנות סינון לצורך איתור התכנים המוגדרים כאסורים בטרם הגיעם אל משתמשי הקצה, וחסימת הגישה אל הדפים המציגים תכנים אלה או למחוק תכנים אלה מתוך הדפים; (2) ככל שמדובר במנועי חיפוש אפשר להסיר תוצאות חיפוש מסוימות או לשנות את סדר ההצגה של תוצאות החיפוש, כך שדפי אינטרנט הכוללים תוכן בלתי־רצוי לא ייחשפו או יידחקו לשוליים. מאחר שבפועל מנוע החיפוש הוא השער למרחב המקוון, הסרת תוצאות החיפוש עשויה להפחית במידה ניכרת את הנגישות המעשית לאתר אינטרנט הכולל תכנים אסורים, גם אם הגישה הישירה אליו אינה חסומה והתוכן לא הוסר ממנו.[75]

(ד) ניתוק משתמש מהאינטרנט, מהשירות או מהאפליקציה. זו הסנקציה הקשה ביותר מבחינת הפגיעה בחופש הביטוי, שכן היא תלוית אדם ולא תלוית תוכן. הכוונה כאן היא לניתוק החשבון של המשתמש, בין שמדובר בחשבון של משתמש פרטי, בחשבון של דף עסקי, בעמוד ברשת חברתית וכדומה. מבחינה טכנית, הניתוק יכול להתבצע על ידי מנהל היישום שבו עברת הביטוי מתבצעת, שאז יחול הניתוק על השימוש באותו יישום. לחלופין, הניתוק יכול להתבצע על ידי ספקית הגישה לאינטרנט, תוך הוראה לשאר הספקיות במדינה לא לאפשר למשתמש האינטרנט החשוד להתחבר באמצעותן. במקרה כזה תחולתה של הוראת הניתוק רחבה בהרבה – על כל שימוש באינטרנט. ניתוק המשתמש אינו מחייב זיהוי מלא של האדם העומד מאחורי שם המשתמש או כתובת IP או כתובת מזהה אחרת שלו (כגון Mac address[76]), ומכאן שסנקציה זו יכולה להינקט בקשת רחבה יותר של מצבים מאלה שאפשר להביא בגינם את משתמש האינטרנט לדין. כמו כן, ניתוק המשתמש יכול להתבצע באופן זמני (על דרך של השעיה) או קבוע, ומכאן שמדובר בסנקציה גמישה במהותה. עד כה הדיון בשיטת אכיפה זו – ניתוק משתמש – התפתח בכל הנוגע למשתמשי רשת המפרים בעקביות זכויות יוצרים מוגנות באתרים לשיתוף קבצים באינטרנט. כמה מדינות בעולם חוקקו חוקים המטמיעים מודל של "שלוש פסילות" (Three Strikes Policy), שלפיו משתמש אינטרנט שנתפס שלוש פעמים בפרק זמן מסוים בהפצה של חומר המפר זכויות יוצרים מוגנות ינותק מכל ספקיות הגישה לאינטרנט במדינתו. חקיקה מעין זו התקבלה בצרפת, בטאיוואן, בדרום־קוריאה, בניו־זילנד ובבריטניה והיא נשקלת במדינות נוספות.[77] באירלנד יש מנגנון דומה שאינו פרי חקיקה, אלא פרי הסכם בין ספקיות הגישה לאינטרנט לבין נציגי תעשיית המוזיקה והסרטים.[78] ואולם, השימוש ב"סנקציות אלקטרוניות" מעין

75 עוד על הדומיננטיות של מנועי החיפוש במסגרת גלישה באינטרנט ראו Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. Dayton L. Rev. 179, 180-185 (2001).

76 ראשי תיבות של Media Access Control Address, דהיינו: הכתובת המוטבעת על התקני הרשת של המחשב הפיזי המחובר לאינטרנט.

77 לסקירת המדינות שאימצו את המודל בחקיקתן ראו Eldar Haber, *The French Revolution 2.0: Copyright and the Three Strikes Policy*, 2 Harv. J. Sports & Ent. L. 297, 300-306 (2011).

78 ההסדר באירלנד הוא פרי הסכם בין ספקית הגישה לאינטרנט הגדולה באירלנד, Eircom, לבין נציגי תעשיית המוזיקה האירית. על פי ההסכם, Eircom תספק לפדרציית התקליטים האירית

אלה – הרחקת משתמש מהמרחב הווירטואלי בכלל או מכניסה לאפליקציה מסוימת – גם יכול להיות מיושם בהקשר של עברות נוספות ובהן עברות ביטוי ברשת.[79]

עד כאן הדגמתי סוגי פעולות של אכיפה אלטרנטיבית מבחינה טכנולוגית. כל הפעולות שנמנו לעיל מתמקדות בצמצום הפגיעה של הפרסומים האסורים במרחב הסייבר, בין פרסומים קיימים ובין פרסומים עתידיים של מפרסם או של אתר אינטרנט מועד להפרות חוזרות. חלק מהפעולות מגלמות פגיעה רחבה יחסית בפרט המפרסם (ניתוק משתמש מהאינטרנט, מהשירות או מהאפליקציה) או בקהל המשתמשים במרחב המקוון (חסימת גישה לאתרים או לאפליקציות מתפרסם תוכן אסור). מבחינה משפטית אפשר להבחין בין שני אופנים ליישום ולביצוע של פעולות האכיפה האלטרנטיבית: אופן וולונטרי־הסכמי ואופן כופה־מחייב. אפרט על כל אחד מהשניים.

2. פעולות אכיפה אלטרנטיבית וולונטריות־הסכמיות

קטגוריה זו כוללת פעולות של אכיפה אלטרנטיבית או של התגוננות המבוצעות **ביוזמה** של המבצע או כתוצאה **מהסכמה** שלו עם המדינה. פעולות ההתגוננות הוולונטריות יכולות להתבצע על ידי משתמש האינטרנט עצמו, למשל באמצעות התקנה של תוכנות לסינון

(Irish Recorded Music Association – IRMA) פרטים מזהים על משתפי־קבצים העוברים על דיני זכויות היוצרים תוך יישום בו־זמני של מודל "שלוש הפסילות". בארצות־הברית נחתם הסכם בין מרבית ספקיות הגישה הגדולות לאינטרנט לבין נציגי תעשיית הסרטים והמוזיקה ליישום של מודל "שש הפסילות". על פי שמו, מודל זה מאפשר להטיל סנקציות אלקטרוניות על מי שהפר לכאורה בפרק זמן מסוים זכויות יוצרים מוגנות בשש הזדמנויות. על פי ההסכם מדובר לא רק בסנקציה של ניתוק הגישה לאינטרנט באמצעות הספקיות החתומות על ההסכם, אלא גם בסנקציות מרוככות יותר כגון האטת קצב הגלישה, העלאת דף בדפדפן האינטרנט הדורש ליצור קשר עם ספקית השירות וכדומה. ראו Fahmida Y. Rashid, *ISPs Agree to Six Strikes System Warning Users of Suspected Online Piracy*, eWeek (July 8, 2011), www.eweek.com/c/a/Messaging-and-Collaboration/ISPs-Agree-to-Six-Strikes-System-Warning-Users-of-Suspected-Online-Piracy-668389/. לאחרונה הגיע הסכם זה לסוף דרכו, בין השאר על רקע הטענה שהסנקציות שהוטלו במסגרתו לא הוכיחו את עצמן כאפקטיביות. ראו Ian Paul, *The Controversial "Six Strikes" Copyright Alert System for Piracy Warnings is Dead*, PCWorld (Jan. 30, 2017), www.pcworld.com/article/3162790/internet/the-controversial-six-strikes-copyright-alert-system-for-piracy-warnings-is-dead.html.

79 לדיון במבט כוללני יותר על סנקציות אלקטרוניות, ובכללן הרחקת משתמש מהאינטרנט או מיישום מסוים, ראו Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. Ottawa L. & Tech. J. 213, 228-229 (2003-2004). ריידנברג התייחס להטלת סנקציות כאלה על ידי המדינה. לגישה הגורסת שגם תאגידים יכולים ליזום הפעלת סנקציות אלקטרוניות נגד מחשבים שתקפו אותם, בבחינת עזרה עצמית התקפית, ראו Michael E. O'neil, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 Geo. Mason L. Rev. 237 (2000); Curtis E. A. Karnow, *Counterstrike*, *in* Cybercrime – Digital Cops in a Networked Environment 135, 140-148 (Jack M. Balkin et al. eds., 2007).

תכנים פוגעניים על פי הגדרת המשתמש או שימוש בשירותי חיפוש מסוננים,[80] או על ידי ספקית השירות, ה"קבוצה" או ה"קהילה" הווירטואלית,[81] באמצעות קביעת תנאי שימוש הנוגעים לתכנים אסורים ולאכיפתם של התנאים, בין באופן יזום ובין בתגובה לתלונה בגין הפרה של התנאים.[82]

ביום 5.12.2016 פורסמה הצהרה משותפת מטעם ארבע הספקיות – פייסבוק, טוויטר, יוטיוב ומיקרוסופט – בנוגע ליוזמתן למאבק משותף בתוכן תומך טרור ואלימות המפורסם ברשתות שהן מפעילות.[83] בהצהרה משותפת זו דובר על הקמת מנגנון משותף לארבע החברות, שבו תשתפנה ארבע החברות חתימה דיגיטלית (Hash) של תוכני טרור אלימים וסרטוני גיוס לארגוני טרור שאותרו בכל אחת מהפלטפורמות המקוונות של ארבע החברות. שיתוף המידע יאפשר לכל אחת מהחברות לאתר בקרבן חתימות דיגיטליות של התכנים הפסולים שהעלו החברות האחרות ולהסירם. בהצהרה הודגש כי בהתחלה ישותפו במאגר המשותף רק תכנים קיצוניים ומובהקים, שכן סביר להניח שתוכן מסוג זה יפר את תנאי השימוש בכל אחת מהחברות. בצד זאת הודגש בהצהרה כי כל חברה תשמור על שיקול דעתה הבלעדי בנוגע להחלטה איזה תוכן מתוך המידע ששותף מפר את תנאי השימוש בפלטפורמה שלה. הצהרה משותפת זו מגלמת סוג נוסף של פעילות התגוננות וולונטרית – על בסיס פעולה

---

80 קיימות אפשרויות סינון תכנים במערכות הפעלה, ברמה של ספק הגישה לאינטרנט וברמת המשתמש המתקין תוכנה במחשבו. כדוגמה לאפשרויות לפיקוח הורי (Parental control) במערכת ההפעלה חלונות **10** ראו /http://windows.microsoft.com/en-US/windows7 products/features/parental-controls. כדוגמה לשירות לסינון תכנים לא רצויים ברמה של ספק הגישה לאינטרנט ראו, למשל, מערכת Ynet "נטוויז'ן השיקה שרות סינון תכנים" **Ynet** www.ynet.co.il/articles/0,7340,L-2675037,00.html **30.6.2003**; כן ראו "שמרטף – שירות בקרת ההורים של **012** "Smile www.012.net/products/advanced-services/babysitter. לדוגמאות לתוכנות סינון להתקנה עצמית ראו Net Nanny, www.netnanny.com (last visited Feb. 21, 2017). ראו גם Cyber Sitter, www.cybersitter.com (last visited Feb. 21, 2017); את Safe search for Google images של גוגל: Google Advanced Image Search, www.google.com/advanced_image_search (last visited Feb. 21, 2017).

81 הווארד ריינגולד (Rheingold) טבע את המונח "קהילות וירטואליות". בספרו "The Virtual Community" תיאר ריינגולד את חוויותיו כמשתתף קבוע בקהילת WELL (ר"ת של "Whole Earth `Lectronic Link", רשת מחשבים פופולרית בשנות השמונים של המאה הקודמת, טרם עידן ה־World Wide Web) בין השנים 1985–1993, על בסיס של שעתיים גלישה ביום בממוצע באתר זה. בניסיונו להמשיג את המונח "קהילה וירטואלית" הציע ריינגולד הגדרה רחבה, שלפיה כל אימת שנוצר באתר אינטרנט כלשהו דיון ציבורי ממושך, שבמהלכו מובעים רגשות ומתהווים קשרים בין־אישיים בין הגולשים – הרי שלפנינו קהילה וירטואלית. ראו Howard Rheingold, The Virtual Community 23-25 (1993).

82 ראו, למשל, בפייסבוק את אופציית "דווח על בעיה – תוכן פגעני"; ביו־טיוב ראו את אופציית "דווח על סרטון זה" הכולל תת־קטגוריות לבחירה תחת השאלה "מה הבעיה?": "תוכן מיני", "תוכן אלים או דוחה", "תוכן רווי שנאה או פגעני", "התעללות בילדים" ועוד.

83 ראו *Partnering to Help Curb Spread of Online Terrorist Content*, Facebook Newsroom (Dec. 5, 2016), https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.

משותפת יזומה בין כמה ספקיות שירות. על הצהרה ברוח דומה, שהתמקדה בהגנה על קטינים ברשת, חתמו כמה ספקיות שירות בשנת 2009 והיא הוחלה בנוגע לפעילות מקוונת בקרב מדינות האיחוד האירופי.[84]

מובן שכאשר מדובר בפעולות התגוננות וולונטריות של המשתמש, הנחת המוצא היא שהפעולה משליכה רק על המשתמש עצמו; לעומת זאת, כאשר פעולת ההתגוננות הוולונטרית מתבצעת על ידי ספקית השירות – מנהלת הקבוצה או הקהילה הווירטואלית – אזי פעולת ההתגוננות מתבצעת לא עבור המתגונן עצמו אלא עבור אחרים, הנהנים מהשירות המוצע או המנוהל על ידי מבצע הפעולה. משמעות הדברים היא שבמקרה זה פעולת ההתגוננות היא סוג של רגולציה עצמית, המשליכה על צדדים שלישיים ומסדירה את פעילותם.

ראוי לציין כי בצד פעולות יזומות של הספקית עצמה, להסרה או להגבלת גישה לתכנים פוגעניים המופצים באמצעותה, ובצד תלונות משתמשים המועברות אל הספקית כדיווח על הפרה לכאורה של תנאי השימוש של ספקית השירות,[85] צמחו עמותות ששמו להן למטרה "לנקות" את מרחב הסייבר מתכנים אסורים ופוגעניים. כך, למשל, איגוד האינטרנט הישראלי הקים את "המרכז לאינטרנט בטוח", הכולל מוקד לדיווח על תכנים אסורים או פוגעניים; לאחר הדיווח המרכז יוצר קשר עם ספקיות השירות בבקשה להסרת התכנים האסורים.[86] בתחום הפדופיליה באינטרנט מוכרת תופעה של ארגונים ללא מטרת רווח ששמו להם למטרה לסרוק את הפעילות באינטרנט ולדווח לספקיות השירות על אתרים או תכנים שיש בהם תוכן פדופילי.[87] גופים אלה של המגזר השלישי פועלים במישור הוולונטרי וצמחו כמתווכים בין משתמשי האינטרנט הפרטיים לבין ספקיות השירות המקוונות הגדולות.

אשר לפעולות התגוננות הסכמיות, הכוונה היא לשיתוף פעולה בין המדינה לבין ספקית השירות, כאשר הפן ההסכמי יכול לשאת משמעויות שונות: החל במצב שבו המדינה היא

84 ראו Safer Social Networking Principles for the EU (2009), *available at* www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/European%20Commission%20-%20Safer%20Social%20Networking%20Principles.pdf.

85 ככלל, ספקיות השירות המקוונות הגדולות תמעטנה בפעולות יזומות להסרה של תכנים או להגבלת גישה אליהם, ותעדפנה לבחון תכנים שהמשתמשים מדווחים עליהם. זאת, משום שפעילות יזומה בנוגע לתכנים משמעה ניטור של כלל התכנים על ידי ספקית השירות. ניטור כזה עלול להיות יקר ואף להרתיע משתמשים מלהתבטא בחופשיות במסגרת השירות המקוון. כמו כן, ניטור יזום כזה עלול להעמיד את הספקית לפני מציאות משפטית של הודאה מכללא בכך שהיא אחראית לתכנים שהמשתמשים מעלים באמצעות השירות המקוון שהיא מספקת, בניגוד לאינטרס המשפטי שלה.

86 ראו "המרכז לאינטרנט בטוח" safe.org.il.

87 לדיון בשיטת אכיפה זו ראו, למשל, Yaman Akdeniz, *Controlling Illegal and Harmful Content*, *in* Crime and the Internet 113, 121-124 (David Wall ed., 2001). לעמותות העוסקות בעזרה עצמית בנושאי פדופיליה מקוונת ראו, למשל, Internet Watch Foundation, www.iwf.org.uk/ (last visited Feb. 21, 2017) ; Family Watch Dog, www.familywatchdog.us (last visited Feb. 21, 2017); Enough is Enough, www.enough.org/ (last visited Feb. 21, 2017); International Association of Internet Hotlines (Inhope), www.inhope.org/gns/home.aspx (last visited Feb. 21, 2017).

בבחינת מדווח מהימן (Trusted reporter או Trusted flagger), המדווח על הפרות של תנאי השימוש של ספקית השירות העולות גם כדי הפרת החוק המדינתי, וכלה במצב שבו המדינה כורתת הסכמים שונים לצורך הבטחת טיפול מהיר בפניותיה ובתלונותיה על עברות ביטוי המתפרסמות באמצעות ספקית השירות. הדוגמה הבולטת ביותר להסכם בין ספקיות השירות לבין מדינות בכל הנוגע לאכיפה אלטרנטיבית כלפי עברות ביטוי היא ההסכם שנחתם בין האיחוד האירופי (European Union) לבין ספקיות האינטרנט גוגל, יוטיוב (שבבעלות גוגל), פייסבוק וטוויטר בנוגע לפרסומי שנאה (Hate Speech). בהסכם, שפורסם ברבים ביום 31.5.2016,[88] נקבע בין היתר כי ספקיות האינטרנט מתחייבות לנסות לפעול לטיפול בדיווחים של מדינות האיחוד על פרסומי שנאה תוך פחות מ־24 שעות מעת מסירת הדיווח; הספקיות מתחייבות לפעול לעורר מודעות בקרב משתמשיהן בנוגע לשאלה מהו תוכן אסור לפרסום; הספקיות יכשירו את עובדיהן להתמודדות עם דיווחים על פרסומי שנאה ולניתוח מדויק שלהם כדי לבחון אם הם ראויים להסרה. הסכם זה, יותר משהוא נושא אופי מחייב ומדיד, מגלם הצהרת כוונות משותפת של המדינות ושל ספקיות השירות הגדולות.[89]

הרעיון המרכזי בהתגוננות המקוונת ההסכמית בין המדינה לבין ספקית השירות הוא שהמדינה האוכפת אינה פועלת מכוח החוק המדינתי שלה או מכוח דיני העזרה המשפטית, אלא באמצעות התקשרות ישירה עם ספקית השירות, והתאמת הבקשה לתנאי השימוש (Terms of Service) של ספקית השירות. תנאי השימוש הופכים למעין דבר חקיקה שהמדינה האוכפת מנסה לפעול לפיו, מתוך הבנה שניסוח הבקשה לפי מידותיהם של תנאי השימוש תקל על ספקית השירות למלא את הבקשה בלי לפגוע בחובות האמון שלה כלפי לקוחותיה. הפרה של תנאי השימוש פוטרת לכאורה את הצורך להוכיח כי הפרסום שבו מדובר אכן אינו מוגן על פי הסטנדרט החוקתי – הן של המדינה האוכפת, הן של המדינה שבמסגרתה ספקית השירות פועלת והן של המדינה שממנה מבצע העברה פועל. זאת, משום שבהיותה גוף פרטי, תנאי השימוש של ספקית השירות יכולים בפועל להתנות על חופש הביטוי כפי שהוא מוגן בכל אחת מהמדינות הרלוונטיות למקרה הנדון, בהתאם למטרות השימוש שהוגדרו על ידי הספקית. כך, למשל, פייסבוק אוסרת להעלות תכנים פורנוגרפיים,[90] אך לאו דווקא תכנים העולים כדי תועבה מינית (Obscenity) פלילית, הנחשבת לסוטה באופן ניכר מפרסום פורנוגרפי רגיל.[91] בסיכומו של דבר, בכל הנוגע לאכיפה אלטרנטיבית במישור ההסכמי, תנאי השימוש של הספקית נהפכים למעין דבר חקיקה המכתיב את גבולות השיח ברשת, והמדינות מתאימות את עצמן אליהם.

88 ראו Code of Conduct on Countering Illegal Hate Speech Online, *available at* http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

89 כך, למשל, ההסכם כולל שאיפה לטיפול בפניות תוך 24 שעות ללא התחייבות לכך. ההסכם לא מדבר על סנקציות במקרה של סירוב או השתהות בטיפול כאמור.

90 Facebook Community Standards, www.facebook.com/communitystandards (last visited Feb. 21, 2017).

91 לניתוח היחס בין פורנוגרפיה לתועבה ראו, למשל, Miller v. California, 413 U.S. 15 (1973); קרניאל וויסמונסקי "חופש הביטוי, פורנוגראפיה וקהילה באינטרנט", לעיל ה"ש 46, בעמ' 263–275.

3. פעולות אכיפה אלטרנטיבית מכוח הוראה כופה

בצד פעילות במישור הוולונטרי וההסכמי ייתכנו פעולות אכיפה אלטרנטיבית מכוח הוראה כופה, בין הוראה בדין הפנימי האוסרת לפרסם תכנים מסוימים ובין מכוח צו שיפוטי או הוראה של גורם מנהלי על פי סמכותו בחוק, המתייחס למקרה מסוים ומחייב את הסרת התוכן, את חסימת הגישה אליו, את סינון תוכנו או את הרחקת המשתמש. תחילה אציג דוגמאות למהלכים להענקת סמכות לביצוע פעולות אכיפה אלטרנטיבית מכוח הוראה כופה בישראל ובכמה מדינות אחרות. לאחר מכן, אציג את המתח המובנה בין האינטרס של המדינה להחיל את דיניה על פעילות מקוונת המשפיעה על משתמשי אינטרנט משטחה לבין עצמאותן של ספקיות השירות הזרות ורצונן להשתחרר מסמכות האכיפה (Jurisdiction to enforce) של כל המדינות שבהן שירותיהן נצרכים.

בישראל מוכר הניסיון לחסום גישה לאתרי אינטרנט המציעים הימורים בלתי־חוקיים והנגישים למשתמשי אינטרנט מישראל. משטרת ישראל פעלה מכוח סעיף 229(א)(1) לחוק העונשין, התשל"ז–1977, שנחקק טרם עידן האינטרנט: "מפקד משטרת מחוז במשטרת ישראל רשאי להורות על **סגירתו** של **מקום משחקים אסורים** או מקום לעריכת הגרלות או הימורים" (ההדגשה הוספה). סעיף 224 לחוק העונשין מגדיר "מקום משחקים אסורים" כדלקמן: "'מקום משחקים אסורים' – **חצרים** שרגילים לערוך בהם משחקים אסורים, בין שהם פתוחים לציבור ובין שהם פתוחים לבני אדם מסוימים בלבד [...]" (ההדגשה הוספה).

ספקיות הגישה לאינטרנט ניאותו לציית להוראות משטרת ישראל; לעומת זאת, איגוד האינטרנט הישראלי הגיש עתירה מנהלית נגד ההוראה ובית המשפט המחוזי, בשבתו כבית משפט לעניינים מנהליים, קיבל את העתירה וקבע כי אין למשטרה סמכות להורות על חסימת גישה לאתרי הימורים מכוח סעיף זה.[92] ערעור המדינה על פסק הדין נדחה ברוב דעות.[93] חשוב לציין כי שופטי הרוב בבית המשפט העליון לא שללו עקרונית את הסמכות להורות על חסימת גישה לאתרי אינטרנט פוגעניים, ועיקר ההנמקה התבסס על כך שסעיפי החוק הקיימים אינם יכולים לסבול קריאה מכללא של סמכות לחייב צדדים שלישיים – ספקיות הגישה לאינטרנט – לבצע פעולת חסימה עבור משטרת ישראל. הנשיא גרוניס כתב כי בסוגיה זו "למחוקק הפיתרונים".[94] אכן, זמן מה לאחר פרסום פסק הדין של בית המשפט העליון קודמה הצעת חוק ממשלתית, שהציעה לקבוע לראשונה סמכות מפורשת לסגירת אתרי אינטרנט המשמשים לניהול הימורים אסורים; נוסף על כך הוצע להכיר בסמכות מעין

92 עת"מ (מחוזי ת"א) 45606-10-10 **איגוד האינטרנט הישראלי נ' מפקד משטרת מחוז תל־אביב** (פורסם בנבו, 2.4.2012). השוו עם פסיקת בית המשפט העליון של אוסטרליה בדבר שאלת אחריותן של ספקיות הגישה לאינטרנט לתכנים פרי זכויות יוצרים. נפסק כי ככל שהאחריות לסינון התכנים לא נקובה במפורש ב־*Copyright Act 1968* (Cth) (Austl.), אי־אפשר לקרוא סמכות מעין זו יש מאין, שכן יש לה מאפיינים מובהקים של צנזורה על אתרים. ראו *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16 (Austl.).

93 עע"מ 3782/12 **מפקד מחוז תל־אביב־יפו במשטרת ישראל נ' איגוד האינטרנט הישראלי** (פורסם בנבו, 24.3.2013).

94 שם, בעמ' 40 לפסק הדין.

זו גם לגבי אתרים המציגים תכנים פדופיליים.[95] על פי הצעת החוק אפשר יהיה להגביל גישה לאתר אינטרנט, או לחייב סינון של תוצאות חיפוש של אתר אינטרנט, שיש חשש כי ימשיך לבצע אחת מהעברות הללו: ארגון הימורים אסורים בקשר עם ארגוני פשיעה, סחר בסמים מסוכנים למעט חשיש וקנאביס ופרסומי תועבה פדופיליים. הגבלת הגישה תהיה לתקופה קצובה, ובית המשפט יהיה רשאי להאריכה מעת לעת.

נוסף על ניסיון זה, הועלו בעבר כמה הצעות חוק לסינון תכנים פוגעניים על ידי ספקיות הגישה לאינטרנט. הצעות החוק לא הבשילו לכדי מהלך חקיקה מתקדם. הן ביקשו לקבוע בררת מחדל של סינון תכנים על ידי ספקית הגישה לאינטרנט, עם אפשרות של משתמש האינטרנט לבטל את מגבלת סינון התכנים.[96] מכאן, שאפשר למקם הצעות אלה כהצעות לפעולה מגננתית כופה עם ריכוך לכיוון הוולונטרי.

לאחרונה קודמה הצעת חוק נוספת שנועדה להעניק סמכות לביצוע פעולות אכיפה אלטרנטיבית מכוח הוראה כופה – הצעת חוק להסרת תוכן שפרסומו מהווה עברה מרשת האינטרנט, התשע"ז-2016.[97] הצעת החוק נועדה לאפשר התמודדות עם פרסומים באינטרנט העולים כדי עברה פלילית, שהמשך פרסומם יפגע בביטחונו של אדם, בביטחון הציבור או בביטחון המדינה. הצעת החוק קובעת כי בית המשפט לעניינים מנהליים יוכל להוציא צו להסרת תוכן, שיכול כי יופנה אל מפרסם התוכן, אל בעליו, אל מנהלו או אל מפעילו של אתר האינטרנט שבו פורסם התוכן, או אל מנוע החיפוש המנגיש את התוכן האסור בתוצאות החיפוש. כמו כן, על פי הצעת החוק, היה והועמד אדם לדין בגין פרסום התוכן האסור והורשע – יהא התובע רשאי לבקש מבית המשפט כי במסגרת גזר הדין יינתן צו

95 ראו הצעת חוק הגבלת שימוש במקום למניעת ביצוע עברות (תיקון מס' 2), התשע"ד-2014, ה"ח הממשלה 839. ההצעה כללה סמכות לסגירת מקומות פיזיים וסמכות לחסימת גישה לאתרי אינטרנט. לאחר קריאה ראשונה פוצל החלק המגביל גישה לאתרי אינטרנט מהצעת החוק המקורית, הדיון בחלק הפיזי התקדם וההצעה עברה בקריאה שנייה ושלישית. בתאריך 8.2.2017 התחדש הדיון בוועדת החוקה, חוק ומשפט של הכנסת בנוגע לחלק בהצעת החוק המתייחס לאתרי אינטרנט, כהכנה לקריאה שנייה ושלישית.

96 ראו הצעת חוק הגבלת גישה לאתרי אינטרנט למבוגרים, התשס"ו-2006, פ/892/17. ההצעה נדונה בוועדת הכלכלה של הכנסת בתאריכים 21.5.2007, 16.7.2007, 4.2.2008, 13.2.2008. הצעת החוק הוגשה שוב, לאחר כמה שינויים, על ידי שר התקשורת אריאל אטיאס מש"ס. ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 41) (שירות סינון של תכנים בלתי הולמים לקטינים באינטרנט), התשס"ח-2008, פ/892/17, שנדונה בישיבת ועדת הכלכלה של הכנסת ביום 30.6.2008. להצעת חוק עדכנית יותר ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון – חובת סינון אתרים פוגעניים), התשע"ד-2013, פ/1733/19. כדוגמה להצעת חוק מרוככת יותר, של הטלת חובות על ספקיות הגישה לאינטרנט ליידע את משתמש האינטרנט בדבר אתרים ותכנים פוגעניים באינטרנט ואפשרויות ההגנה מפניהם, לרבות סינון תכנים או מניעת גישה אל האתרים, ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 47) (אתרים ותכנים פוגעניים באינטרנט), התשע"א-2011, פ/456/18, שאף היא נדונה כמה פעמים בוועדת הכלכלה של הכנסת.

97 הצעת חוק להסרת תוכן שפרסומו מהווה עבירה מרשת האינטרנט, התשע"ז-2016, ה"ח הממשלה 1104. ההצעה פורסמה ביום 28.12.2016 ועברה קריאה ראשונה.

להסרת התוכן, אף אם לא הוכח אלמנט הסיכון לביטחונו של אדם, לביטחון הציבור או לביטחון המדינה.

בדברי ההסבר להצעת חוק זו צוין כי הכלים שההצעה מעניקה נועדו לשמש את רשויות האכיפה בצד הכלי הפלילי ולא במקומו, שכן מטרתו להעניק אפשרות להתמודדות יעילה ומהירה עם התוכן המזיק במטרה להקטין את הסיכון הנשקף ממנו. על פי דברי ההסבר, הרקע להצעת החוק הוא העלייה שזוהתה ברף האלימות וההסתה לטרור במרחב המקוון. עיקרה של הצעת החוק הוא אפוא בהתמודדות לפני משפט עם פרסומים מקוונים העולים כדי עברה פלילית ומקימים סיכון, וזאת כשני תנאים מצטברים.

נוסף על המהלכים בישראל אסקור כמה מהלכי חקיקה בולטים במשפט המשווה, שבהם נקבעה סמכות להורות על נקיטה של אמצעי אכיפה אלטרנטיביים מכוח הוראה כופה. כפי שאפשר לראות, מהלכים שונים שננקטו בארצות־הברית כשלו מבחינה משפטית ואילו מהלכים אחרים – בצרפת, באוסטרליה ובניו־זילנד – צלחו מבחינה משפטית.

בארצות־הברית נחקקו כמה חוקים לחיוב בסינון תכנים פוגעניים ובחסימת גישה לאתרי האינטרנט המציגים אותם. שניים מהם – CDA (Communications Decency Act) מ־1996 ו־COPA (Child Online Protection Act) מ־1998 – נפסלו על ידי בית המשפט העליון האמריקני כבלתי־חוקתיים, משום שהטילו מגבלות עמומות ורחבות מדי על חופש הביטוי של אתרי האינטרנט.[98] חוק נוסף, CIPA (Children's Internet Protection Act) מ־2000,

98 CDA הופיע כ־47 U.S.C. §§ 223(a)-(h) (1996). החוק אסר על פרסום תכנים הנחשבים בלתי־מהוגנים ("indecent") ופוגעניים ("patently offensive"), ולא צמצם את תחולתו רק על פרסום תכנים מתועבים ("obscene"), הנחשבים ככאלה המקימים עברה פלילית של פרסומי תועבה. כשנה וארבעה חודשים לאחר חקיקתו פסל בית המשפט העליון את הגדרות החוק לגבי התכנים האסורים בפרסום באינטרנט, בהיותם עמומים ורחבים מדי באופן הסותר את התיקון הראשון לחוקה האמריקנית המעגן את חופש הביטוי. ראו Reno v. ACLU, 521 U.S. 844 (1997). ה־COPA הופיע כ: 47 U.S.C. § 231 (1998). על פי COPA, אתרי אינטרנט מסחריים בגבולות ארצות־הברית בלבד חויבו להימנע מהעלאת תכנים המזיקים לקטינים ("harmful to minors"), כשהתוכן המזיק לקטינים ייקבע על פי הסטנדרט הקהילתי הלוקאלי בכל מקום ומקום בארצות־הברית. החוק חולל סדרה של דיונים משפטיים בכמה סבבים, ובסיומם נקבע כי החוק אינו חוקתי בהיותו פוגע בחופש הביטוי. נקבע כי החוק נקט מונח עמום כקריטריון לחסימת אתרים פוגעניים, הוא לא יכול היה להשיג תוצאה אפקטיביות בשל תחולתו המוגבלת לאתרים מסחריים בתוככי ארצות־הברית בלבד, ויש קושי טכני ליישם סטנדרט קהילתי לוקאלי באינטרנט. ראו את פסק הדין של בית המשפט הפדרלי לערעורים: ACLU v. Reno, 217 F.3d 162 (3rd Cir. 2000); בבית המשפט העליון האמריקני הוחלט על החזרת הדיון לערכאה דלמטה, ראו Ashcroft v. ACLU, 535 U.S 564 (2002). החוק נפסל שוב; ראו ACLU v. Ashcroft, 322 F.3d 240 (3rd Cir. 2003). בית המשפט העליון שוב השיב את התיק לערכאה הדיונית כדי לבחון אם כיום אפשר לבצע סינון אפקטיבי של גולשים לפי גיל. ראו Ashcroft v. ACLU, 542 U.S. 656 (2004). בסבב הבא שוב נפסל החוק, ראו ACLU v. Mukasey, 534 F.3d 181 (3rd Cir. 2008). לבסוף דחה בית המשפט העליון את הבקשה לדון בערעור (ראו Mukasey v. ACLU, 129 S. Ct. 1032 (2009)) והחוק נותר בבטלותו.

נפסל תחילה בבית המשפט לערעורים ולבסוף הוכשר בבית המשפט העליון האמריקני.[99] ניסיונות אלה מעידים על הקושי, במיוחד בעברות ביטוי, לחסום גישה לאתרים, בשל החשש שיהיה בכך משום אפקט מצנן על הפעילות באינטרנט, על מפרסמי התכנים ברשת ועל פיתוח השיח בו.

בצרפת, צו שהוצא בפברואר 2015 (מכוח חוק מסמיך שנחקק באוקטובר 2014) קובע כי בסמכותו של מנהל יחידת הסייבר המשטרתית הצרפתית להורות לספקיות הגישה לאינטרנט לחסום גישה של משתמשי רשת בצרפת לאתרים הכוללים תוכן פדופילי ולאתרים המסיתים לביצוע פעולות טרור או המקדמים זאת.[100] נוסף על כך נקבע בצו שאפשר להורות למנועי החיפוש לסנן תוצאות חיפוש (Delist) לאתרים מעין אלה. על ספקיות הגישה לציית לצו המנהלי תוך 24 שעות. הספקיות תוכלנה לקבל החזר הוצאות מהמדינה אם חסימת הגישה תשית עליהן עלויות. באתרים החסומים תופיע הודעה מטעם משרד הפנים הצרפתי, המסבירה כי הגישה אליהם נחסמה על פי חוק, ומסבירה גם איך אפשר להשיג על ההחלטה בדבר חסימת הגישה אל התכנים שבאתרים החסומים.[101]

---

99 החוק מופיע כ־17 U.S.C. §§ 1701-1703, 1711-1712, 1721, 1731-1733, 1741. מדובר בחוק מימוני המוחל על ספריות ציבוריות ובתי־ספר במימון ציבורי. במסגרת החוק חויבו מוסדות אלה – כתנאי למימון פדרלי – להתקין תוכנות סינון לתכנים מתועבים, פדופיליים או מזיקים לקטינים ("harmful to minors"). עתירה נגד חוקתיותו של החוק התקבלה תחילה בבית המשפט הפדרלי של מחוז פנסילבניה, American Library Association v. United States, 201 F. Supp .2d 401 (E.D. Pa. 2002), אך בסופם של ההליכים נדחתה העתירה על ידי בית המשפט העליון. ראו United States v. American Library Association, 539 U.S. 194 (2003). הטענה המרכזית נגד חוקתיותו של החוק הייתה שמבחינה טכנולוגית אי־אפשר לבצע סינון תכנים אפקטיבי, שלא יביא להכללת־יתר (יסוננו גם תכנים שהם בגדר ביטוי מוגן) או להכללת־חסר (לא יסוננו כל התכנים האסורים). מאחר שהנטייה של הספריות ובתי הספר תהיה להימנע מהכללת־חסר (שאז ייחשבו כמי שלא עמדו בדרישות החוק, ולא ייהנו מהתמריץ הכלכלי המוצע למי שמיישם את החוק), הנטייה תהיה לכיוון של הכללת־יתר וחסימת ביטויים מוגנים. נפסק שאפשר לרפא את הפגם האמור אם יוכל בגיר, הגולש בספריה או בבית הספר, לבקש את הסרת הסינון במקרה מסוים, והמוסד שבו מותקנת תוכנת הסינון יבצע את הדרישה ללא דיחוי. לדיון עקרוני בסינון תכנים במסגרת מוסד ציבורי בפרט ובאינטרנט בכלל ראו מיכאל בירנהק "החופש לגלוש בספריות ציבוריות" **משפט וממשל** ו 421 (2003) (המאמר מתייחס לפסיקת הערכאה הראשונה של בית המשפט הפדרלי, שכן פסיקת בית המשפט העליון ניתנה לאחר פרסום המאמר).

100 **ראו** Loi 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique [Law 2015-125 of February 5, 2015 on the blocking of sites causing acts of terrorism or advocacy and sites broadcasting images and depctions of pornographic minors], Journal Officiel de la République Française [J.O.] [Official Gazette of France], 2015.

101 ארגונים שונים עתרו לבית הדין המנהלי הגבוה של צרפת (Conseil d'Etat) בטענה שהחוק האמור פוגע בצורה לא מידתית בחופש הביטוי, ושלמצער ראוי שתהליך החסימה והסרת התכנים יאושר על ידי בית המשפט ולא על ידי רשות מנהלית. בהחלטה מיום 15.2.2016 דחה בית

באוסטרליה הוסמכה רשות התקשורת האוסטרלית ACMA (Australia Communications & Media Authority) לפקח על תכנים באינטרנט בהתאם לחוק משנת 1999.[102] הפיקוח מתבצע בתהליך המתחיל בהכרזה על ספקית השירות האינטרנט כגוף מפוקח, ש־ACMA יכולה להפעיל עליה את סמכותה. לאחר מכן נאספות תלונות מהציבור לגבי תכנים אסורים על פי חוק והתוכן נבחן על ידי ACMA. אם נמצא שהתוכן אכן נוגד את החוק האוסטרלי, ACMA שולחת לספקית השירות דרישה להסרת התוכן או לחסימת הגישה אליו (תלוי בסוג הספקית בה מדובר) עד לסוף יום העבודה הבא שלאחר מסירת הדרישה. אם ההוראה אינה מתבצעת במועד האמור, נשלחת אל ספקית השירות התראה חוזרת. סירוב של ספקית השירות למילוי הדרישה הוא עברה פלילית נמשכת העשויה לגרור קנסות על כל יום איחור במילוי הדרישה.

ניו זילנד הסדירה את ההסרה של תכנים אסורים ואת הגבלת הגישה אליהם בחקיקה חדשה משנת 2015.[103] על פי סעיף המטרה שבחוק הניו־זילנדי, מטרתו להרתיע, למנוע ולמזער נזק העלול להיגרם לאדם באמצעות תקשורת דיגיטלית, וכן לספק לנפגעי התכנים הפוגעניים כתובת ומענה יעיל לפנייתם. סעיף 6 לחוק קובע את טיב התכנים האסורים בתקשורת הדיגיטלית שאליהם החוק מתייחס: תכנים הפוגעים בפרטיותו של אדם, תכנים מאיימים, תכנים תוקפניים במיוחד (grossly offensive), תוכני תועבה, תכנים העולים כדי הטרדה, האשמות שווא, הפרה של חובות סודיות או של חובות אמון, הסתה לפגיעה מקוונת, שידול להתאבדות, תכנים מפלים וגזעניים במכוון. בית המשפט המחוזי רשאי לצוות על הסרה או על מניעת גישה (disable public access) אל התוכן האסור, אך הוא יצווה כאמור רק בהינתן הפרה חמורה מהסוגים שצוינו לעיל ובהינתן שההפרה עלולה לגרום נזק ממשי לאדם.[104]

*

מטבע הדברים, ההבחנה בין פעולות התגוננות וולונטריות־הסכמיות לבין פעולות מכוח הוראה כופה אינה דיכוטומית. בפועל, הן המדינות והן ספקיות השירות מנהלות הערכת סיכונים וסיכויים זו מול זו. ספקיות השירות, מצדן, חוששות מפני שינויי חקיקה שירחיבו את סמכויות המדינות להטיל עליהן הוראות כופות שיתערבו באופן שבו הן מווסתות את התכנים המפורסמים באמצעותן. החשש האמור מדרבן את הספקיות להגביר את שיתוף הפעולה הוולונטרי־הסכמי עם המדינות. דוגמה לכך מתקיימת בכללים להסדרה עצמית של תוכן משתמשים באינטרנט (תגוביות (טוקבֶּקים), פוסטים וכו'), שנערכו על ידי איגוד

הדין את העתירה. נפסק כי אין הכרח שהחלטה לחסימה או להסרת קישור תינתן דווקא על ידי שופט, ובכל מקרה הצד הנפגע רשאי לעתור נגד ההחלטה של הגורם המנהלי לבית המשפט. **ראו** CE, Feb. 15, 2016, 389140, *available at* www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000032064635&fastReqId=104&fastPos=2.

102 **ראו** *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) (Austl.).

103 Harmful Digital Communications Act 2015 (N.Z.).

104 **שם, ראו** ס' 12(2) ביחד עם ס' 19(2)(a) לחוק.

האינטרנט הישראלי בשיתוף עם אתרי האינטרנט הישראליים הגדולים.[105] כללים אלה קובעים קריטריונים לסינון תכנים פוגעניים של משתמשי אינטרנט. טל ז׳רסקי טען כי ספקיות השירות הגיעו למסמך כללים זה בשל חששן מהצעת חוק פרטית שהציעה לכפות עליהם בחקיקה חובות נרחבות לפיקוח על תוכני גולשים,[106] ובכך מתערער במידה מסוימת יסוד הוולונטריות וייתכן להציג את המהלך כמהלך כופה של המדינה, גם אם סמוי במידת מה.

דוגמה מסוג אחר לטשטוש בין פעולה וולונטרית לבין פעולה מכוח הוראה משפטית כופה באה לידי ביטוי במכתבי התראה משפטיים, בין מצד משתמשים או גופים פרטיים ובין מצד המדינה, המועברים למנועי חיפוש דוגמת גוגל. הפונים במכתבים אלה עומדים על כך שמנוע החיפוש לא יציג דפי אינטרנט מסוימים בתוצאות החיפוש שלו, משום שמגולמת בהם עברה פלילית או הפרה של קניין רוחני. ג׳ונתן זיטריין (Zittrain) ובנג׳מין אדלמן (Edelman) הראו, כבר בשנת 2002, ש־Google.de (גרמניה) ו־Google.fr (צרפת) לא הציגו יותר ממאה דפי אינטרנט בעלי תכנים גזעניים ופרו־נאציים בעקבות מכתבי התראה משפטיים על כך שפרסומם אסור על פי הדין הגרמני והצרפתי.[107] גם גוגל האמריקנית ניאותה לסנן דפי אינטרנט מתוצאות החיפוש שלה, לאחר שקיבלה שורה של מכתבי התראה משפטיים על כך שדפים אלה כוללים תכנים המפרים זכויות יוצרים והגנה של סימני מסחר לפי הדין האמריקני.[108]

עד כאן דוגמאות לפעולות אכיפה אלטרנטיבית מכוח הוראה כופה או בעקבות חשש מפני פעולה כופה שבוצעו בכמה מדינות. שאלה מכבידה היא מה סמכות האכיפה (Jurisdiction to Enforce) של המדינה כלפי ספקיות השירות, שרובן חברות זרות ששרתיהן נמצאים מחוץ לטריטוריה הישראלית. לכאורה, הוראת חוק ישראלית האוסרת פרסום של תוכן מסוים, מחייבת את הסרתו או את הגבלת הגישה אליו או כדומה, אינה מחייבת את ספקית השירות הזרה. עם זאת, ספקית השירות הזרה פועלת גם כלפי משתמשי אינטרנט מישראל ועל כן היא עשויה לחוב באחריות על הפרות הדין הישראלי. על כן, הספקיות עצמן בחרו לכפוף את עצמן, במסגרת תנאי השימוש שלהן, להוראות ולצווים מחייבים של המדינות שבהן הן מעניקות שירות, וזאת כדי להימנע מחידוד המחלוקות הבין־מדינתיות האפשריות.[109]

---

105 ראו ״כללים להסדרה עצמית של תוכן משתמשים באינטרנט״ **איגוד האינטרנט הישראלי** 2008 www.isoc.org.il/docs/Rules-Self_regulation_users_content.pdf.

106 ראו טל ז׳רסקי ״שקיפות בסינון תכנים: הצעה לפעולה״ **חוקים** ב 133, 147 (2010). הצעת החוק הפרטית שעליה דיבר ז׳רסקי היא הצעת חוק בדבר אחריותן המשפטית של הנהלות אתרי האינטרנט על דברי הגולשים המגיבים באתריהן (תיקוני חקיקה), התשס״ח–2007, פ/3171/17. להצעת חוק חדשה יותר, שנועדה להטיל על הרשתות החברתיות חובות ניטור אקטיביות לצורך סינון של תוכני הסתה לטרור, ראו הצעת חוק הסרת פרסום הסתה שהתפרסם ברשת החברתית המקוונת, התשע״ו–2016, פ/3110/20.

107 ראו Jonathan Zittrain & Benjamin Edelman, Localized Google Search Result Exclusions (2002), https://cyber.harvard.edu/filtering/google/#intro.

108 ראו גם Goldsmith & Wu, לעיל ה״ש 75. כן ראו Steven Alan Childress, *The Empty Concept of Self-Censorship*, 70 Tul. L. Rev. 1969, 1971, 1975 (1996).

109 ראו, כדוגמה בלבד, *Statement of Rights and Responsibilities*, Facebook (Jan. 30, 2015), www.facebook.com/terms.

עם זאת, כאשר מדובר בספקיות המעניקות שירותים במסגרת שמות מתחם מקומיים־מדינתיים,[110] אלה עשויות ליישם את ההוראה המדינתית בדבר הסרת התוכן במסגרת השירות המקוון המקומי שלהן באותה מדינה ולא כלפי כולי עלמא. כדוגמה אפשר לציין את פרשת Yahoo!. תחילתה של הפרשה בשנת 2000 בצרפת, שם עתרו שני ארגונים למלחמה באנטישמיות נגד אתר יאהו! שבו הוצגו למכירה פומבית מזכרות נאציות – מעשה המהווה עברה על הקוד הפלילי הצרפתי האוסר על הצגת סמלים נאציים. בית המשפט הגבוה בפריז קבע כי יאהו! הפרה את הקוד הפלילי הצרפתי. נפסק כי מצד אחד אמנם לא דובר באתר אינטרנט שכוון מראש לקהל צרפתי אלא באתר הנגיש לכלל הציבור וניתן לצפייה גם על ידי קהל צרפתי; מצד שני דובר באתר מסחרי (מכירות פומביות) השואף להגיע לקהל יעד רחב ככל האפשר מטעמים רווחיים, ולכן יש בפעולה זו של האתר משום הכפפה רצונית לסמכויות שיפוט של המדינות שבהן נמצאים משתמשי האינטרנט הגולשים אל האתר. על כן, נפסק, מחובתה של יאהו! למנוע גישה של משתמשי אינטרנט צרפתים לדפי התוכן האסורים. בית המשפט פסק לא רק כלפי יאהו! בצרפת (Yahoo.fr) אלא גם כלפי יאהו! האמריקנית (Yahoo.com).[111] לאחר מכן התנהל מאבק משפטי בארצות־הברית, שבסופו נקבע כי הרחבת הסמכות בידי בית המשפט הצרפתי לא הוכרה בארצות־הברית כהרחבה מותרת כלפי חברת האם, יאהו! האמריקנית.[112]

נוסף על כך, ככל שמדובר בשירות מרוכז שאינו נחלק לשמות מתחם מדינתיים, נשאלת השאלה אם ספקית השירות רשאית לכבד צו או הוראה מדינתית להסרת התוכן באופן שיחסום את הגישה אליו מכתובות IP של המדינה. במילים אחרות: האם מגבלות סמכות האכיפה של המדינה יכולות להתפרש על ידי הספקית כחסימת גישה על בסיס טריטוריאלי (Geo-blocking) – והאם תגובה כזו של ספקית שירות להוראת הסרה תיחשב כציות לה? על פני הדברים נראה כי פתרון כזה, שיינקט בידי ספקית השירות, יוכל לשמש פתרון טכנולוגי מאזן בין סמכותה של המדינה מחד גיסא לבין ההכרח שלא להשפיע ולפגוע יתר על המידה באינטרסים של המדינות האחרות ושל ספקית השירות מאידך גיסא. אחרת, הסרת התוכן כלפי כולי עלמא משמעה בעצם הרחבה דה פקטו של סמכות המדינה הדורשת את ההסרה אל יתר המדינות.

---

110 הכוונה בשמות מתחם מקומיים או מדינתיים לכך שאתר אינטרנט מסוים, דוגמת google.com, כולל לא רק את האתר האמריקני (סיומת *.com) אלא גם אתרים ברמת המדינות דוגמת google.co.il לישראל, google.co.uk לבריטניה, google.co.nl להולנד וכיוצא באלה.

111 ראו La Ligue Contre le Racisme at I'Antisemitisme (LICRA) v. Yahoo!, Inc., Tribunal de Grande Instance [T.G.I.] Paris, Ordonnance de Refere (2000) (Fr.), *available at* http://juriscom.net/2000/05/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/.

112 להשתלשלות ההליכים בארצות־הברית ראו Yahoo!, Inc. v. La Ligue Contre le Racisme et I'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); Yahoo!, Inc. v. La Ligue Contre le Racisme et I'Antisemitisme 379 F.3d 1120 (9th Cir. 2004); Yahoo!, Inc. v. La Ligue Contre le Racisme et I'Antisemitisme, 433 F.3d 1199 (9th Cir. 2006) (en banc), *cert. denied*, 126 S. Ct. 2332 (2006).

4. אכיפה אלטרנטיבית משולבת ומשתלבת

אסטרטגיה מדינתית של אכיפה אלטרנטיבית להתמודדות עם עברות ביטוי במרחב הסייבר צריכה להיות משולבת ומשתלבת. ב"אסטרטגיה משולבת" כוונתי לדרך פעולה וולונטרית־הסכמית בצד דרך פעולה במסלול הכופה (הכוחני). ב"אסטרטגיה משתלבת" כוונתי לדרך פעולה משלימה בצד דרך הפעולה הקלאסית של חקירה פלילית והעמדה לדין במקרים המתאימים. תחילה אתייחס לשילוב בין פעולה וולונטרית־הסכמית לבין פעולה במסלול הכוחני, ולאחר מכן ליחס בין האסטרטגיה האלטרנטיבית לבין האסטרטגיה הפלילית הקלאסית.

(א) *אכיפה משולבת: מסלול וולונטרי־הסכמי בצד מסלול כופה*

ברמה היישומית, המסלול הוולונטרי־ההסכמי עדיף על המסלול הכופה מכמה טעמים: **ראשית**, מסלול זה עשוי להיות מהיר יותר מהמסלול הכופה, שכן הוא מתבסס על איחוד אינטרסים בין המדינה לבין הספקית – ולא על ניגוד אינטרסים, שבו המדינה מבקשת לכפות על הספקית פעולה והספקית בוחנת כיצד לציית לדרישת המדינה באופן מינימלי, למשל בדרך של חסימה על בסיס גאוגרפי (Geo-blocking). במקרה של פעולה במסלול הכופה תיתכן התדיינות משפטית בין המדינה, ספקית השירות ואולי אף גורמים נוספים (המפרסם עצמו, עותר ציבורי). **שנית**, מבחינת ספקית השירות המקוונת – המדינה נחשבת כמדווחת ולא כדורשת. הסרת התוכן או צמצום הגישה אליו מתבצעים על ידי ספקית השירות, מן הטעם שהופרו תנאי השימוש של הספקית כפי שהיא עצמה הגדירה אותן. לדידה של ספקית השירות, לא הופעלה כלפיה כל סמכות משפטית פורמלית של גורם חיצוני. **שלישית**, מבחינת המדינה האוכפת, הלכה למעשה אין הפעלה של סמכות במובן של מתן הוראה או דרישה מחייבת. למעשה מדובר בהגשת בקשה, הנסמכת על ההבנה שספקית השירות תבחן אותה בהתאם לתנאי השימוש שהיא עצמה הגדירה ועל פי תבחיניה. יוצא אפוא, ככלל, שעל המדינה להעדיף תמיד את המסלול הוולונטרי־הסכמי, של דיווח על תוכן אסור לספקית השירות, על המסלול הכוחני.

הלכה למעשה, פעולה במישור הוולונטרי־ההסכמי אינה הפעלה של סמכות במובן של מתן הוראה או דרישה מחייבת. למעשה מדובר בהגשת בקשה, הנסמכת על ההבנה שספקית השירות תבחן אותה בהתאם לתנאי השימוש שהיא עצמה הגדירה ועל פי תבחיניה. במקרה כזה נדרשת הצדקה בסיסית לפעולה של המדינה, גם אם לא ברמה של עילה המקימה סמכות כוחנית. ההצדקה לפעולה נדרשת מן הטעם שראוי להבטיח כי המשאבים הציבוריים המממנים את פעולתן של רשויות האכיפה המדינתיות ינוצלו להתמודדות עם פרסומים אסורים בחוק בלבד, ולא לפרסומים שהחוק אינו אוסר. זאת, אף אם הסטנדרט העצמי של ספקית השירות הוא מצמצם יותר מבחינת חופש הביטוי ומאפשר הסרה של תכנים המותרים בדין הישראלי. במילים אחרות: אם תנאי השימוש של ספקית השירות המקוונת מגבילים סוגים מסוימים של ביטויים המותרים דווקא בדין הישראלי, אזי לגבי אותם ביטויים מותרים אין זה ראוי שהמדינה תפעל אל מול הספקית, אף אם הפעולה מצטמצמת לכדי דיווח בלבד במישור הוולונטרי ואינה עולה כדי פעולה במישור הכוחני.

(ב) *פעולה משולבת: אכיפה אלטרנטיבית בצד אכיפה פלילית קלאסית*

אכיפה אלטרנטיבית כלפי עברות ביטוי במרחב הסייבר נועדה ליטול את העוקץ מהפרסום. בכוחה למנוע את פוטנציאל הסיכון הגלום בו, כאשר מדובר בעברות ביטוי הכוללות יצירת סיכון כגון הסתה לאלימות, גילוי הזדהות עם ארגון טרור והסתה לטרור או פרסומים מטרידים מינית. בכוחה אף להפחית את היקף הפגיעה ולצמצם את משכה, אף כשמדובר בעברות ביטוי שאינן יוצרות סיכון לביטחון המדינה, לביטחון הציבור או לביטחונו של אדם. כפי שציינתי לאורך המאמר, האכיפה האלטרנטיבית מתמקדת בעברה, בפרסום עצמו ובנזקים ובסיכונים הגלומים בו; לעומת זאת, האכיפה הפלילית בנוגע לעברות הביטוי במרחב הסייבר משרתת מטרות מסוימות של הרתעה צופה פני עתיד וכן תכליות נוספות של גמול ושיקום – וכל אלה מכוונות כלפי מבצע העברה (ואולי מבצעי עברה פוטנציאליים נוספים, אם נניח שיש להרתעה אפקט ציבורי ולא רק אישי).

אמנם האכיפה האלטרנטיבית משרתת תכליות שונות מאלו של האכיפה הפלילית הקלאסית, אולם לעתים בכוחה להשפיע על האינטרס הציבורי בהמשך, באמצעות הליכים במסלול הקלאסי של חקירה, העמדה לדין וניהול משפט. זאת, משום שעוצמת הנזק – בכלל זה היקף תפוצתו, משך פרסומו וכדומה – כל אלה הם בהחלט שיקולים רלוונטיים להחלטה בדבר ההצדקה להעמדה לדין בגין הפרסום האסור.[113] במילים אחרות: במקרים של עברות ביטוי קלות ערך, כשנקיטת פעולות לצמצום נזקי הביטויים תצלח, הרי שייתכן שיפחת האינטרס הציבורי בהעמדה לדין של המפרסמים אף אם תיאספנה ראיות מספיקות להעמדה לדין.

ככלל, נקיטה של אמצעי אכיפה אלטרנטיבית נועדה להשיג תוצאה יעילה ומהירה של צמצום תפוצתו של הפרסום האסור, וזאת בקצב שאמור להתאים לאופן ההפצה והפרסום במרחב המקוון, כדי למנוע את התפשטותו והתפזרותו על פני מחשבי קצה רבים. ככל שהפרסום מגיע למספר רב יותר של מחשבים, כך יקשה להבטיח שהפרסום לא ישוב ויופץ עוד ועוד. מכאן, שהאכיפה האלטרנטיבית נועדה לשלבים מוקדמים ואף מידיים לאחר הפצת הפרסום, לפני מיצוי ההליכים הפליליים הרגילים. עם זאת, ייתכן בהחלט שאמצעים להסרת הפרסום או לצמצום החשיפה אליו יינקטו גם בשלב מאוחר, לאחר שיינקטו הליכים פליליים קלאסיים, וזאת כשמדובר בפרסום שלא שיקף סיכון ולכן לא זכה למענה חיובי במסלול הוולונטרי־ההסכמי ולא הצדיק פעולה במישור הכוחני. במקרה כזה, קביעה מאוחרת שהפרסום עולה כדי עברה, במסגרת הליך משפטי חלוט, תוכל להצדיק נקיטה של אמצעי אכיפה אלטרנטיבית במסלול הכופה, דהיינו: בקשה למתן צו שיפוטי להסרת התוכן, לסינונו מתוצאות החיפוש או לחסימת הגישה אליו – וזאת אף אם לא נשקף מהפרסום סיכון לביטחון המדינה, לביטחון הציבור או לביטחונו של אדם. הקביעה השיפוטית החלוטה שהפרסום עולה כדי עברה פלילית יכולה להצדיק פעולה במישור האלטרנטיבי הכופה, בבחינת סעד של הפסקת המשך ביצוע העברה ומניעת הרחבה של פגיעתה של העברה.

---

113 שיקולים אלה נכנסים תחת פרמטר "חומרת המעשה" שאמור להישקל בבחינת האינטרס הציבורי בהעמדה לדין לפי ס' 62 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב–1982. ראו לעניין זה "שיקולים לסגירת תיק בשל העדר 'עניין לציבור'" **הנחיות פרקליט המדינה** 1.1, ס' 4(א) (התשס"ג).

ד. הביקורות על אסטרטגיית התגוננות ומניעה בהקשר של עברות ביטוי במרחב הסייבר

כפי שהצגתי בפרק הקודם, אסטרטגיית ההתגוננות והמניעה של עברות ביטוי במרחב הסייבר מבוססת על ארבע טכניקות: הסרת תכנים אסורים, חסימת גישה לתכנים אסורים, סינון תכנים אסורים מתוצאות החיפוש וניתוק המשתמש מהאינטרנט או מהשירות שבו פרסם תכנים אסורים. ארבע טכניקות אלה יכולות להינקט במסגרת הסכמית־וולונטרית או במסגרת ציות להוראה כופה (בין בחוק, בין בצו שיפוטי ובין בהוראה מנהלית מכוח החוק). בחלק זה של המאמר אבחן ארבע ביקורות נגד האסטרטגיה המוצעת של התגוננות ומניעה בהקשר של עברות ביטוי במרחב הסייבר. הביקורת הראשונה היא מכיוון התאוריה של חופש הביטוי. ביקורת זו מתחלקת לשתי סוגיות: סוגיית ההפללה בדיעבד אל מול מניעה מראש של ביטויים אסורים וסוגיית ההשלכות של המנגנונים הוולונטריים וההסכמיים לאכיפה אלטרנטיבית כלפי ביטויים אסורים על חופש הביטוי. הביקורת השנייה היא מכיוון חופש השימוש במרחב המקוון, מצד המשתמש המבקש להשתחרר מפטרנליזם מדינתי הכופה עליו אמצעי הגנה או יוצר פעולה מגננתית הסכמית. הביקורת השלישית היא מכיוון של חופש העיסוק של ספקיות השירות במרחב המקוון, העלולות להידרש לחובות ונטלים למיניהם במסגרת האסטרטגיה המגננתית. הביקורת הרביעית היא מכיוון טכנולוגי – בדבר אי־היעילות של אמצעי ההתגוננות במובן זה שאין בו כדי להשיג את מטרותיו. אדון בביקורות כסדרן, וכפי שאראה, אפשר להעמיד להן הסברים ומענים, ולו חלקיים. בסופו של דבר, אין בביקורות אלה כשלעצמן, או בהצטברותן, כדי לשמוט את הבסיס מתחת לצורך ולהצדקה לנקוט אסטרטגיה של אכיפה אלטרנטיבית בנוגע לעברות ביטוי ברשת. כפי שאטען, המקרה שלפנינו הוא מקרה מובהק שבו הדוקטרינה המשפטית המקובלת ביחס למניעה מוקדמת של עברות על דרך הביטוי אינה ניתנת להעתקה אל מרחב הסייבר, ומכאן שיש לסרטט את גבולות הדוקטרינה בנוגע לעברות הביטוי במרחב המקוון באופן מותאם למאפייני המרחב, בראי הביקורות שיימנו להלן.

1. ביקורת מכיוון חופש הביטוי

הביקורת מכיוון חופש הביטוי נחלקת למעשה לשתי סוגיות נפרדות הנוגעות לענייננו: ראשית, על פי הגישה המקובלת, ראוי להימנע מהגבלה מראש של ביטויים ללא הליך משפטי מלא של בירור אשמה, כפי שמתבצע במסגרת מנגנוני האכיפה האלטרנטיבית; הגבלה מראש של ביטויים אסורים תותר רק במקרה של ודאות קרובה לפגיעה בשלום הציבור או ביטחונו, ולא בכל מקרה שקמה לכאורה עברה פלילית, כפי שהצעתי במאמר; שנית, נשאלת השאלה מה השפעתן של פעולות וולונטריות או הסכמיות על חופש הביטוי.

(א) *מניעה (מוקדמת) בתנאי ודאות קרובה לעומת הפללה (בדיעבד)*

ככלל, בית המשפט העליון מבכר הפללה בדיעבד של ביטוי אסור, או תביעת פיצוי בגינו, על פני מניעתו מראש. כך נפסק, למשל, בנוגע לביטוי גזעני[114] ובנוגע ביטוי המהווה לשון

114 בג"ץ 399/85 **כהנא נ' רשות השידור**, פ"ד מא(3) 255 (1987).

הרע.[115] בבסיס הכלל האמור – העדפת ביקורת שיפוטית בדיעבד על פני מניעה מוקדמת – עומדת התפישה שלפיה אף אם מניעה מוקדמת היא הפתרון האפקטיבי ביותר למניעת הביטוי האסור, המחיר החוקתי של מניעה מוקדמת ככלל עולה על התועלת שבה.[116] נוסף על כך, בהקשרים שונים של חופש ביטוי (אם כי במרחב הפיזי) קבע בית המשפט העליון, ככלל, שכדי להכשיר מניעה מראש של ביטוי לא די בהוכחת פוטנציאל לפגיעה בזכות או באינטרס מוגן לגיטימי, ויש להראות ודאות קרובה לפגיעה ממשית בזכות או באינטרס (מבחן הוודאות הקרובה).[117]

כאמור בהקדמה, מאמר זה עוסק בביטויים העולים כדי עברה פלילית, ולכן יש להידרש לשאלה אם מותר למנוע מראש ביטויים המהווים עברה פלילית או שמא גם ביחס לעברות אלה יש לבכר ענישה בדיעבד על פני מניעה מוקדמת. בשאלה זו נחלקו דעותיהם של השופטים ברק ובך בפרשת **כהנא**.[118] השופט (כתוארו דאז) ברק גרס כי אחריות פלילית אינה תנאי הכרחי ואינה תנאי מספיק להצדקת מניעה מוקדמת של ביטוי.[119] לשיטתו, גם כשביטוי עולה בוודאות כדי עברה אין זאת אומרת בהכרח שראוי להגבילו מראש, שכן המבחן להגבלה מראש של ביטוי הוא ודאות קרובה לפגיעה ממשית בזכות או באינטרס מוגן. השופט בך חלק בנקודה זו על השופט ברק: לדידו, אם הביטוי מהווה עברה פלילית אין צורך להראות שמתקיים מבחן הוודאות הקרובה כדי לאסור עליו ולהגבילו. למעשה, התפלגות עמדות זו קשורה במידה מסוימת לשאלה נוספת: האם חופש הביטוי חל גם על ביטוי המהווה עברה? גישת הרוב בפסיקה הישראלית היא שחופש הביטוי אכן חל גם על ביטוי המהווה עברה מכל סוג שהוא, ולמעשה הוא חל על כל התנהגות שהיא על דרך של פרסום, הצגה או התבטאות.[120] מכאן נובעת המסקנה שדוקטרינת המניעה המוקדמת תחול

---

115 ע"א 214/89 **אבנרי נ' שפירא**, פ"ד מג(3) 840 (1989).

116 ראו Ariel L. Bendor, *Prior Restraint, Incommensurability, and the Constitutionalism of Means*, 68 Fordham L. Rev. 289, 297-300 (1999).

117 מבחן זה מופיע באין־ספור פסקי דין העוסקים בהגבלה של חופש הביטוי. להמחשה בלבד ראו עניין **כהנא**, לעיל ה"ש 115; עניין **אבנרי**, לעיל ה"ש 116; בג"ץ 806/88 **Universal City Studios Inc נ' המועצה לביקורת סרטים ומחזות**, פ"ד מג(2) 22 (1989); בג"ץ 4804/94 **חברת סטיישן פילם בע"מ נ' המועצה לביקורת סרטים**, פ"ד נ(5) 661 (1997); בג"ץ 680/88 **שניצר נ' הצנזור הצבאי הראשי**, פ"ד מב(4) 617 (1989).

118 באותו מקרה נבחנה החלטתה של רשות השידור להגביל במידה ניכרת את התבטאויותיהם הפוליטיות של אנשי מפלגת כך, בראשות חבר הכנסת דאז מאיר כהנא. על פי ההחלטה שנתקפה בבג"ץ, ישודרו רק תכנים בעלי "ערך חדשותי מובהק" הקשורים באנשי התנועה, ואילו כל הנוגע לדעותיהם, להשקפותיהם ולעמדותיהם הפוליטיות של אנשי כך לא ישודר.

119 ראו עניין **כהנא**, לעיל ה"ש 115, בעמ' 298–301. כן ראו אביגדור קלגסבלד "עבירה פלילית ומניעה מוקדמת" **פלילים** ב 93 (1991).

120 בנוגע לביטוי גזעני ראו ע"פ 2831/95 **אלבה נ' מדינת ישראל**, פ"ד נ(5) 221, בעמ' 286, 288, 295, 298 302 ו־308 (1996) (גישת שופטי הרוב – השופטים ברק, בך, גולדברג ודורנר). כן ראו גישת השופט ברק בעניין **כהנא**, לעיל ה"ש 115, בעמ' 282. בנוגע לביטוי העולה כדי תמיכה בארגון טרור ראו דנ"פ 8613/96 **ג'בארין נ' מדינת ישראל**, פ"ד נד(5) 193, 208, 217 (2000) (גישות השופטים אור ולוין). בנוגע לפרסומי תועבה ראו עניין **סטיישן פילם**, לעיל ה"ש 118,

על ביטוי המהווה לכאורה עברה פלילית. גישת המיעוט גורסת את ההפך, ולפיה ביטויים מסוימים, העולים כדי עברה פלילית, אינם חוסים תחת הגנתו של חופש הביטוי[121] ולכן אפשר למנוע אותם בלי לעמוד בתנאים של מבחן הוודאות הקרובה.

בחזרה אל השאלה – מה דינו של ביטוי העולה לכאורה כדי עברה פלילית ומתפרסם במרחב המקוון? האם יש להחיל עליו את מבחני הוודאות הקרובה, שלפיהם תותר הגבלתו במקרים מצומצמים יותר מאלה שבהם הפרסום מגיע כדי עברה, או שמא כל פרסום עברייני ניתן להגבלה? לטעמי, ברמה העיונית ראוי להגביל ביטויים העולים כדי עברה במרחב המקוון אף אם אין הם עומדים בתנאים של מבחן הוודאות הקרובה. זאת, משום שתנאים אלה פותחו לגבי מניעה מראש של ביטוי, בנסיבות שונות בתכלית מהנסיבות של הפרסום במרחב הסייבר. שינוי הנסיבות מהמרחב הפיזי למרחב המקוון מצדיק את שינוי המבחן המשפטי להגבלת הביטוי. אפרט.

ראשית, הנחת העבודה לגבי פרסומים במרחב הפיזי היא שיש חלופה בדמות העמדה לדין בדיעבד בגין הביטוי הפוגעני – ועל כן יש להעדיף את החלופה האמורה על פני מניעת הביטוי ללא הליך משפטי של בירור אשמה. הנחה זו אינה מתקיימת כשמדובר בפרסום במרחב הסייבר, בשל מאפייניו המשפטיים־טכנולוגיים ובראשם מאפיין הבין־לאומיות ומאפיין האנונימיות, המאפשרים למפרסם לחמוק מאחריות פלילית. מכאן, שמניעה של המשך פגיעתו של הפרסום לא תוכל להתבצע אלא הליכי אכיפה אלטרנטיביים.

שנית, הפרסום במרחב המקוון הוא לא אחת ויראלי, ומועבר באופן בלתי־נשלט על ידי המפרסם המקורי.[122] מכאן, שיש הכרח לסכל את המשך ההפצה של הביטוי האסור בשלב המוקדם ביותר האפשרי, שכן אחרת יוכל הפרסום "לחיות" ברשת גם אם ייקבע שהוא אסור וגם אם יתקבל נגד הנאשם צו המורה למוחקו.

שלישית, בכל הנוגע לאתרים או למפרסמים בין־לאומיים, מבחינתם יש הבדל בין פעולה של חסימת גישה או סינון תכנים כלפי קהל משתמשי אינטרנט ממדינה מסוימת

בעמ' 675–676 (גישת השופט ברק). בנוגע לפרסום העולה כדי לשון הרע ראו עניין **אבנרי**, לעיל ה"ש 116, בעמ' 860 (גישת השופט ברק). בנוגע לארגון הימורים באינטרנט כ"ביטוי" ראו עניין **איגוד האינטרנט הישראלי**, לעיל ה"ש 93, בעמ' 6 (גישת השופטת רובינשטיין מבית המשפט לעניינים מנהליים בתל־אביב) וכן עניין **איגוד האינטרנט הישראלי**, לעיל ה"ש 94, בעמ' 35 (התייחסותו של השופט פוגלמן בבית המשפט העליון לסוגיה).

121 בנוגע לביטוי גזעני ראו את דעת היחיד של השופט מצא בעניין **אלבה**, שם, בעמ' 259; בנוגע לביטוי העולה כדי תמיכה בארגון טרור ראו עניין ג'בארין, שם, בעמ' 211 (גישת השופט טירקל).

122 אריאל בנדור הבחין בין ביטוי משודר לבין ביטוי כתוב וציין, בהקשר של פרסום ספר העלול להוציא לשון הרע, כי ההצדקות למניעה מוקדמת של ביטוי כתוב, במיוחד של ספר, הן לכאורה מוגברות לעומת ההצדקות למניעה מוקדמת של ביטוי משודר. זאת משום שבמקרה של ספר (ביטוי כתוב), משוחרר הביטוי אין עוד תקנה של ממש ב"מניעה מאוחרת". ראו אריאל בנדור "חופש לשון־הרע" **משפטים** כ 549, 568 (1991). הבחנה זו רלוונטית ביתר שאת במרחב הסייבר, שבו הפרסום הוא כתוב או מוקלט, והוא "חי" ברשת שהיא בעלת זיכרון בלתי־מוגבל למעשה. אולם בעניינו יש אלמנט נוסף המחזק טיעון זה ביתר שאת והמאפיין את המרחב המקוון – המשך פרסום והפצה של הפרסום המקוון, ולא רק המשך ההחזקה והשימוש בפרסום.

לבין פעולה של הסרת תכנים. ככל שפעולת ההתגוננות שבה עסקינן אינה מביאה להסרת התוכן אלא אך לצמצום קהל היעד של הפרסום, עוצמת הפגיעה בחופש הביטוי פוחתת.

רביעית, מבחינה משפטית נתונות למשטרת ישראל, כרשות אכיפת חוק, סמכויות (ואף חובה) לעסוק במניעת עברות;[123] כן נתונות לשוטר סמכויות לתפוס כל "חפץ", לרבות "חומר מחשב",[124] שיש יסוד סביר להניח כי עומדים לעבור בו עברה. החקיקה המסמיכה את המשטרה לא מבחינה בין עברת ביטוי לבין עברה הנעברת בהתנהגות מסוג אחר. עוד יצוין בהקשר זה כי הפסיקה שפותחה בנוגע למניעה מוקדמת של ביטויים עסקה בגופים מנהליים שאינם עוסקים באכיפת חוק כגון רשות השידור או המועצה לביקורת סרטים ומחזות, שאינם מופקדים על מניעת עברות אלא על אינטרסים אחרים הנוגעים לתוכני שידור. האינטרס לפעול להפסקת עברה לכאורה – ואפילו עברת ביטוי – הוא אינטרס בעל משקל שהוכר באופן מפורש על ידי המחוקק.

חמישית, חלק ניכר מפעולות האכיפה האלטרנטיביות אינן מביאות למניעה מראש של ביטוי אלא להסרה או צמצום הגישה אליו **בדיעבד**, לאחר פרסומו. חריגים לכך הם הרחקה או ניתוק של משתמשים משירות מקוון מסוים (כמו רשת חברתית), שאז ייחסמו מראש גם ביטויים עתידיים של אותו משתמש. ברי כי ככל שמדובר בהגבלה של ביטוי שתוכנו כבר ידוע, הבחינה המשפטית של ההצדקה להגבלתו יכולה לגלם איזון מדויק יותר.

שישית, פעולות האכיפה האלטרנטיבית הן פעולות הניתנות לביטול ול"החזרה לאחור" ב"לחיצת כפתור". יכולת התיקון בדיעבד קלה ומהירה יותר מאשר באמצעי המדיה הטרום־אינטרנטיים. כך, למשל, אם הוחלט להסיר תוכן מסוים מרשת חברתית, ומאוחר יותר מנהלי הרשת מתחרטים על ההחלטה – אפשר לתקן את העניין בלחיצת כפתור. לעומת זאת, בעיתונות המודפסת למשל, אם הוחלט על פרסום כתבה מצונזרת וכעבור זמן מוחלט על ביטול ההחלטה הצנזוריאלית, הרי שעקב מגבלות המקום ועלות ההפקה של העיתון, לא תמיד יתאפשר לפרסם מחדש, במלואו, את התוכן הלא־מצונזר. יתרה מזו ובהמשך לדוגמה הקודמת: הפרסום ברשת החברתית הוא בעל אופי מתמשך ולא חד־פעמי ואילו הפרסום העיתונאי או הטלוויזיוני הוא על פי רוב חד־פעמי ומוגבל בזמן. יוצא אפוא כי בכל הנוגע לפרסום במרחב המקוון, פגם בהחלטת ההגבלה של הפרסום ניתן בנקל לריפוי ולצמצום נזקים בדיעבד.

הנה כי כן, הכלל היונק את חיותו מתאוריה של חופש הביטוי בנוגע למניעה מוקדמת של ביטויים מוגנים אינו מותאם לנסיבות של פרסום תכנים אסורים, המהווים לכאורה מעשה של עברה פלילית, בסביבה המקוונת. מסקנתי היא אפוא שברמה העקרונית יוכל קיומה של עברת ביטוי לכאורה במרחב המקוון לשמש בסיס מספיק לנקיטת מהלכי אכיפה אלטרנטיביים.

כיצד יוכח קיומה של עברה פלילית ברמת ודאות גבוהה? דומה כי ככל שמדובר במהלכים מכוח הוראה כופה (המסלול הכוחני), ראוי כי הקביעה בדבר קיומה לכאורה של עברה פלילית תימסר לבית המשפט. עם זאת, יש לשים לב לחריגותו של ההליך המדובר: אין

123 ס' 3 לפקודת המשטרה [נוסח חדש], התשל"א–1971, קובע כי "משטרת ישראל תעסוק במניעת עברות ובגילוין, בתפיסת עבריינים ובתביעתם לדין [...] ובקיום הסדר הציבורי ובטחון הנפש והרכוש".

124 לפי ס' 1 לפסד"פ, "חפץ" כולל "חומר מחשב".

מדובר בהליך פלילי של בירור אשמה – שכן על פי רוב המפרסם עצמו לא יהיה צד להליך שבו יתבקש הצו השיפוטי שיורה על הגבלת הביטוי, בין משום שלא יתייצב לדיון, בין משום שזהותו לא תהיה ידועה (בעקבות שימוש באמצעים להשגת אנונימיות), ובין משום שיהיה מחוץ לישראל (מפרסם זר). לפיכך, אין רלוונטיות לבחינת היסוד הנפשי שבעברה, הנוגע בנאשם עצמו, דהיינו: יסוד המתמקד ב"עושה" ולא ב"מעשה". למעשה, הבחינה השיפוטית תתמקד בשאלה אם מתקיימים היסודות העובדתיים של העברה (התנהגות, נסיבות, ואם מדובר בעברת תוצאה – גם תוצאה).[125]

(ב) *ההשפעה של פעולות וולונטריות או הסכמיות על חופש הביטוי של משתמשי המרחב המקוון*

הדיון דלעיל, בסוגיה של מניעה מוקדמת לעומת הפללה בדיעבד, הניח שהגורם האחראי להגבלת הביטויים האסורים הוא גורם מדינתי. אולם, כפי שציינתי לעיל, חלק ניכר מהסדרת הנושא של התכנים האסורים מתבצע באופן פרטי, בידי ספקיות השירות, המצנזרות ביטויים בהתאם לתנאי השימוש שהגדירו בעצמן (פעילות וולונטרית), העשויים להיות קפדניים יותר מסטנדרט חופש הביטוי של המדינה, או בהתאם להסכמות שהגיעו אליהן עם המדינות השונות (פעילות הסכמית). לכאורה, פעילות וולונטרית ואף הסכמית, המתבצעת על ידי ספקית השירות, בלא כפייה מאת המדינה ובהתאם לתנאי השימוש שפורטו מראש בפני המשתמש – מגלמת פגיעה קטנה יותר בחופש הביטוי.[126]

עם זאת, עיון מדוקדק יותר בפעילות הוולונטרית וההסכמית של ספקיות השירות המקוונות הגדולות מעלה כי ההתנהלות ההסכמית ואף הוולונטרית שלהן עלולה לנבוע למעשה מניהול סיכונים מושכל אל מול המדינות, באופן שאפשר למעשה לראותו כהשפעה עקיפה של המדינות על חופש הביטוי של משתמשי השירות המקוון שהספקיות מפעילות.[127] החצנה עקיפה זו של פעולת ההסרה, הסינון והמניעה של ביטויים אסורים עשויה לכאורה להפוך את ספקיות השירות הפרטיות ל"ציבוריות", מבחינה זו שפעולתן כבר לא תיתפש עוד

125 כדי להמחיש את האמור ניטול כדוגמה את העברה של לשון הרע. "לשון הרע", כמעשה, מוגדר בס' 1 לחוק איסור לשון הרע. ס' 6 לחוק מוסיף שני תנאים כדי שהפרסום יעלה כדי עברה פלילית: יסוד נפשי של "כוונה לפגוע" ויסוד עובדתי של פרסום לשני אנשים או יותר זולת הנפגע. ס' 7 לחוק קובע תנאי אחד, מצומצם יותר, לכך שהפרסום יעלה כדי עוולה נזיקית של לשון הרע – שהפרסום יגיע לאדם אחד זולת הנפגע. על פי הגישה שהצגתי, כדי לפעול להסרת התוכן במסלול האכיפה האלטרנטיבית, די להראות כי מתקיימים כל היסודות העובדתיים של העברה הפלילית, דהיינו: היסודות שבס' 1 לחוק, המגדירים את טיב הפרסום, והתנאי השני שבס' 6 לחוק, קרי: שהפרסום הגיע לשני אנשים או יותר זולת הנפגע. כוונת המפרסם לפגוע אינה יכול להיות מוכחת בפלילים בלא הליך פלילי, ולצורך מניעת פוטנציאל הפגיעה או הפגיעה בפועל שבפרסום, היסוד הנפשי רלוונטי פחות.

126 לעמדה זו ראו, למשל, קרין ברזילי־נהון וגד ברזילי "חופש הביטוי המעשי והמדומיין באינטרנט: על בטלותה והולדתה המחודשת של הצנזורה **שקט, מדברים! התרבות המשפטית של חופש הביטוי בישראל** 483, 508–510 (מיכאל בירנהק עורך, 2006).

127 הרחבתי על הנושא לעיל בחלק ג(3).

כפעולה אוטונומית של גוף פרטי אלא כפעולה של סוכן מדינתי (State action).[128] נוסף על כך, נוכח התפשטותה של המדיה החברתית ונוכח העובדה שההצטרפות למדיה החברתית היא בחינם ובקלות רבה, עם מעט מאוד חסמי כניסה,[129] אפשר לטעון שהפרסומים ברשתות הציבוריות הם ביטויים הנאמרים במרחב הציבורי השייך לכלל, ולא ניתן להגבילם בניגוד לסטנדרט חופש הביטוי החל באותו מרחב ציבורי.

אף אילו היו טענות אלה מתקבלות הן היו בלתי־אכיפות, בהתחשב בעובדה שלא ברור מה יהיה סטנדרט חופש הביטוי שיחול על אותו "מרחב ציבורי". הלכה למעשה מדובר ב"מרחבים ציבוריים" כמספר המדינות שבהן התוכן המקוון נצפה. בעיית אכיפות זו מאפשרת לספקיות השירות המקוונות הבין־לאומיות לנצל ארביטראז' זה ולהימנע מהכפפה ישירה לסטנדרט של מי מהמדינות. במילים אחרות: מנקודת מבט של חופש הביטוי, אי־אפשר יהיה לאכוף על ספקיות השירות זכות לחופש ביטוי באופן שיחייב אותן להתיר ביטויים הסותרים את תנאי השימוש שלהן, שכן האוטונומיה שלהן תגבר על הסטנדרט המדינתי של חופש הביטוי – אם לא מטעמים של חופש העיסוק אזי בוודאי כך מטעמים מעשיים של אכיפות. עם זאת, מבחינת ספקית השירות נכון – ומבחינת המדינה ודאי הכרחי – לשקף לציבור המשתמשים את הכמות והסוג של התכנים שהוסרו על פי בקשה או דרישה של המדינות, וזאת כדי למנוע את האלמנט המצנן הנוסף שלפיו לא זו בלבד שביטויים מוגבלים, אלא שלא ידוע אילו ביטויים וכמה ביטויים הוגבלו ומאילו עילות. על כך – להלן.

2. ביקורת מכיוון חופש השימוש במרחב המקוון

הביקורת הקודמת עסקה במפרסמים, במנהלי האתרים ובאחראים על ייצור התוכן האסור שהמדינה מבקשת להסיר או לחסום את הגישה אליו. הביקורת הנוכחית מעבירה את הזרקור אל הצד של משתמשי המרחב המקוון. משתמשים אלה זכאים לחופש גלישה, שבמסגרתו הם יכולים להגיע אל המידע ה"רוצה להיות חופשי".[130] מיכאל בירנהק טען כי חופש הגלישה באינטרנט נגזר, כזכות, מחופש הביטוי ברשת,[131] אולם נראה שאפשר לראות בחופש האמור משום זכות עצמאית המהווה יישום של האוטונומיה של הרצון של משתמש האינטרנט, ולא בהכרח זכות החופפת לחופש הביטוי של מפרסם התכנים השונים ברשת. אפשר אף לחבר

128 התפישה הרווחת היא שהזכות לחופש ביטוי מחייבת את רשויות המדינה ואינה מחייבת גופים פרטיים. כך מנוסח, למשל, התיקון הראשון לחוקה האמריקנית המגביל את הקונגרס ("Congress shall make no law […]") מלפגוע בחופש הביטוי. U.S. Const. amend. I. ראו עוד Kevin Park, *Facebook Used Takedown and it Was Super Effective; Finding a Framework for Protecting User Rights of Expression on Social Networking Sites*, 68 N.Y.U. Ann. Surv. Am. L. 891, 900, 911-921 (2013). דוקטרינת State Action פותחה בארצות־הברית וקובעת אימתי פעולה המגבילה חופש ביטוי תעלה כדי פעולה מדינתית, הכפופה לתיקון הראשון לחוק האמריקנית, ולא רק כפעולה במסגרת האוטונומיה של גוף פרטי שאינו כפוף לתיקון הראשון לחוקה. ראו Lugar v. Edmondson Oil Co., 457 U.S. 922, 936-37 (1982).

129 ראו לעיל בחלק ב(1).

130 בפרפרזה על המשפט הידוע "מידע רוצה להיות חופשי" (Information wants to be free), שטבע סטיוארט ברנד (ריאיון בכנס ההאקרים הראשון), מחוז מארין, קליפורניה, 1984.

131 בירנהק "החופש לגלוש בספריות ציבוריות", לעיל ה"ש 100.

את הזכות לחופש שימוש במרחב המקוון להקשרים רחבים יותר, שאינם מסתיימים בזכות של המשתמש היחיד: חופש השימוש מאפשר זרימה חופשית של המידע, ניוד של מידע ובכך שיפור וקידום הידע האנושי הכולל, כמו גם פיתוח עצמי וקהילתי.[132]

מעניין לציין כי הרטוריקה של חופש השימוש במרחב המקוון נעדרת מפסק דינו של בית המשפט העליון בפרשת **איגוד האינטרנט הישראלי**,[133] שבו נבחנה סמכות המשטרה להורות לספקיות הגישה לאינטרנט על חסימת גישה לאתרי הימורים בהסתמך על סעיף 229 לחוק העונשין. דומני, כי ההיזקקות לחופש השימוש במרחב המקוון עשויה הייתה לשמש הנמקה נוספת לעמדת הרוב, שפסקה כי נדרשת הוראת חוק מפורשת שתעניק סמכות לחסימת גישה לאתרי הימורים.

מטבע הדברים, חופש השימוש במרחב המקוון אינו זכות מוחלטת. עם זאת, הוא עשוי להצדיק את הקביעה שכל אימת שתינקט פעולה של חסימת גישה, סינון תכנים הכוללים עברות ביטוי או ניתוק משתמש שביצע את העברות – ספקיות הגישה ומנועי החיפוש יציינו כי הדף המבוקש או תוצאות החיפוש המבוקשות (בהתאמה) נחסמו על פי דין. כך, אף שתיפגע האפשרות להגיע אל המידע המבוקש, לפחות תישמר הידיעה של משתמש הרשת שבוצעו פעולת חסימה או סינון כאמור.[134] עצם הידיעה כאמור ממתנת את תחושת הפגיעה בשלמות של תמונת המידע המתקבלת על ידי ספקית השירות. במילים אחרות: הידיעה על גבולותיו של חופש השימוש במרחב המקוון (במובן של יידוע על חסימת תוכן מסוים או משתמש מסוים, יידוע על היקפי החסימה, על מועדי ביצועם ועוד) מעצימה את חופש השימוש.

3. ביקורת מכיוון חופש העיסוק של ספקיות השירות

הביקורת מכיוון זה נקשרת לתכונה של מרחב הסייבר כמרחב שבו המידע מבוזר ומתווך על ידי ספקיות שירות. תכונה זו הופכת את ספקיות השירות, שלא בהכרח בטובתן, ל"שחקניות" מרכזיות בתהליך האכיפה הפלילית במרחב הסייבר. מאחר שפעולות האכיפה האלטרנטיביות מתבצעות באמצעות ספקיות שירות – בין שזו ספקית הגישה ובין שזו ספקית הפלטפורמה להעלאת תכנים על־ידי אחרים – הרי שככל שמדובר באכיפה אלטרנטיבית במסלול הכוחני, מכוח הוראה כופה, היא מגלמת פגיעה לא רק בחשוד אלא במידה רבה גם בחופש העיסוק של ספקיות השירות.[135] מובן שספקיות של שירותים מסוימים פועלות גם במרחב הפיזי, והן עשויות לקבל צווים לביצוע פעולות שונות עבור הרשות החוקרת, אולם במרחב המקוון

132 בצד חופש השימוש במרחב המקוון אפשר לפתח דיון – החורג מהדרוש לצורך מאמר זה – בזכות להתחבר לאינטרנט, בדומה לדיון בזכות להתחבר לתשתיות יסודיות אחרות כמו חשמל, מים, טלפון וכו'. הזכות להתחבר עניינה בעצם הזכות להתחבר אל המרחב המקוון, ואילו חופש השימוש במרחב המקוון עניינו "חופש התנועה" בתוככי המרחב המקוון, לאחר ההתחברות אליו.

133 לעיל ה"ש 94.

134 אפרט על כך עוד להלן, בפרק ה(2)(א).

135 ראו גם ויסמונסקי **חקירה פלילית במרחב הסייבר**, לעיל ה"ש 14, בעמ' 274. מעניין לציין שכאשר ספקיות השירות מנהלות פעולות של אכיפה עצמית (כגון הסרת תוכן או הרחקת משתמש המפר את תנאי השימוש שהגדירו), הספקיות תטענה דווקא **לזכותן** לבצע את הפעולות

המרכזיות של ספקיות השירות היא חלק אינהרנטי ממבנה הרשת ומאופן תפקודה. על כן, יש הבדל מהותי מבחינת הפגיעה בחופש העיסוק של ספקיות השירות. מובן שביקורת זו רלוונטית אך ורק למקרה של פעולות אכיפה אלטרנטיביות במישור הכוחני, מכוח הוראות כופות, שכן אכיפה במישור הוולונטרי היא בהסכמה מלאה של ספקית השירות.[136]

ספקיות השירות אינן מקשה אחת. להבחנה ביניהן עשויה להיות משמעות ניכרת בנוגע לעוצמת הטענות הנכרכות בחופש העיסוק שלהן. ככל שמדובר בספקיות שירות "פרטיות" יותר (למשל: מנהלות אתרים של חברות מסחריות), כך נראה כי הטענות לפגיעה בחופש העיסוק תזכינה למשנה־תוקף; לעומת זאת, ככל שמדובר בספקיות גישה "ציבוריות" יותר – ובראשן ספקיות הגישה או התשתית לאינטרנט, המקבלות רישיון מכוח חוק התקשורת (בזק ושידורים), התשמ"ב – 1982[137] ויושבות על צומת שליטה רחבה יותר באינטרנט – כך אפשר יהיה לראות בהן משום גופים דו־מהותיים ולהטיל עליהן אחריות ונטלים שונים.[138] כאשר מדובר בספקיות אינטרנט "ציבוריות", מחד גיסא יגבר הצורך של המדינה להטיל עליהן חובות, ומאידך גיסא תיחלש הטענה לפגיעה אסורה בזכותן לחופש העיסוק.[139]

האמורות. ראו לדוגמה Eugene Volokh & Donald M. Falk, *Google: First Amendment Protection for Search Engine Results*, 8 J.L. Econ. & Pol'y 883 (2012).

136 אפשר אף לטעון שאכיפה אלטרנטיבית במישור הוולונטרי היא לא רק בהסכמה של הספקיות אלא ביוזמתן, מתוך אינטרס שלהן בטיהור השיח במסגרת הפלטפורמה שלהן. כך, למשל, אפשר לטעון שרשת חברתית מסוימת תהיה מעוניינת למנוע פרסומים פדופיליים או פרסומים גזעניים כדי למנוע "בריחת" משתמשים לרשתות חברתיות מתחרות. במקרה כזה, אינטרס כלכלי של הרשת החברתית יניע אותה לשאוף לנקות את הפרסומים מתכנים כאלה, והיא תשמח לרתום למשימה זו את רשויות המדינה (בבחינת החצנה מהספקית אל המדינה).

137 החיוב ברישיון הופך פורמלית את המשאב או הטובין שהגוף הפרטי מספק למשאב ציבורי (Public utility), ומאפשר לראות את הגוף הפרטי כגוף דו־מהותי החב בחובות של המשפט המנהלי. כך אפשר, למשל, לטעון לגבי עיתונות כתובה, שהוצאתה לאור טעונה רישיון לפי ס' 4 לפקודת העיתונות, 1933, כי היא משתמשת במשאב ציבורי ומספקת טובין ציבוריים ולכן אפשר להטיל עליה חובות מהמשפט המנהלי. ראו אהרן ברק "על העיתונות הפרטית" **עלי משפט** ב 293, 294, 296 (2002). עם זאת, לגבי אתר חדשות הפועל באמצעות האינטרנט בלבד, אין חובה לקבל רישיון, שכן תנאי להגדרת "עיתון" על פי ס' 1 לפקודת העיתונות הוא כי העיתון יהיה "דבר־דפוס". מכאן, שאתר האינטרנט אינו משתמש במשאב ציבורי.

138 ב"ספקיות שירות ציבוריות" כוונתי לחברות פרטיות המשתמשות במשאב ציבורי מוגבל, ובמקרה שלפנינו – המשאב הציבורי של גישה לאינטרנט או תשתית החיבור לאינטרנט. אמנם ספקיות אלה חופשיות לפעול באופן פרטי, אולם נוכח העובדה שהן פועלות מכוח רישיון בזק כ־Common carrier, הן כפופות לחובות מן המשפט המנהלי. ראו גם אמל ג'בארין "הזכות לאנונימיות, זכות הגישה לערכאות סמכות טבועה ומה שביניהן" **מחקרי משפט** כט 309, 325–326 (2013).

139 בעניין **איגוד האינטרנט הישראלי**, לעיל ה"ש 94, שבו נדונה הסמכות להטיל חובה על ספקיות הגישה לאינטרנט לחסום גישה לאתרי הימורים, לא עלתה במישרין השאלה אם ספקיות הגישה הן גופים דו־מהותיים, אולם אפשר ללמוד כי דעת הרוב, מפי השופט פוגלמן, הניחה שמדובר בגופים פרטיים (פסקה 13 לפסק דינו), ואילו השופט סולברג, שכתב את דעת המיעוט, סבר

באילו מובנים אפשר לדבר על פגיעה באוטונומיה של ספקיות השירות? ראשית, אפשר לבקר באופן כללי את ההחצנה של נטל האכיפה מהמדינה אל גורמים פרטיים הפועלים במרחב הסייבר. שנית, ככל שהמדינה תחייב את ספקיות השירות לבצע בפועל את הפעולות של חסימת הגישה, הסינון, ההסרה של תכנים, ההרחקה או הניתוק של משתמשים – הדבר עלול להשית עליהן עלויות כלכליות. שלישית, חיוב של ספקיות השירות לבצע את פעולות ההתגוננות המשפטית עלולה להתערב בחופש ההתקשרות שלהן בהסכם מול לקוחותיהן, ואף בציפייה הנוצרת אצל הלקוחות שספקית הגישה לא תפעל בשירותן של רשויות המדינה.[140]

אשר לטענה הראשונה, אמנם הכלל המשפטי הוא שנטל האכיפה אמור ליפול על כתפי המדינה;[141] אולם נראה כי אין מנוס מהחצנה מסוימת, הנובעת מטבעו של מרחב הסייבר, הכולל ראיות מבוזרות ומתווכות על ידי ספקיות השירות, הנהפכות לצומתי מידע שבלעדיהם אין. אין חלופה סבירה אמתית להחצנה האמורה זולת מצב של מעקב מדינתי, און־ליין ובדיעבד, באופן שיטתי ומתמיד, אחר כלל הפעילות המקוונת. על כן, חוקרים רבים צידדו בהטלת נטל האכיפה על ספקיות השירות ברשת.[142]

אשר לטענה השנייה, ברי כי נוכח העובדה שספקיות השירות האמורות מנהלות את צומתי השליטה במידע ובגישה אל המידע ברשת, הרי הן בבחינת מונעות הנזק הזולות ביותר – ולכן התוצאה היעילה היא להטיל עליהן את האחריות לפעולות המניעה. ככל

כי ספקיות הגישה נושאות באחריות ציבורית בהתחשב ברישיון שהוענק להן מטעם המדינה ובשל העובדה שהן שולטות במרחב המקוון כצומת מרכזי (פסקה 45 לפסק דינו).

140 ראו ויסמונסקי **חקירה פלילית במרחב הסייבר**, לעיל ה"ש 14, בעמ' 100–103, 274.

141 ראו ע"פ 1761/04 **שרון נ' מדינת ישראל**, פ"ד נח(4) 9, 15 (2004), שם נפסק: "שימוש שיגרתי בסעיף [סעיף 43 לפסד"פ המתיר לשופט לדרוש המצאת מסמכים, בשלב החקירה, למשטרה; ח' ו'] אינו ראוי. כשקיימות למשטרה דרכים להגיע בכוחותיה אל מסמכים הדרושים לה, אין הצדקה שמלאכת או טרחת המצאתם תוטל על הפרט, בין שהוא חשוד ובין אם לאו. אין לשכוח, כי הוצאתו של צו מכוח סעיף 43 גוררת אחריה חובה למסור חפצים, אשר עלולה לגזול, לעיתים, מאמץ וזמן, ואף להיות כרוכה בהוצאות כספיות והשקעות ומשאבים אחרים. פגיעה כזו תהיה מוצדקת רק באותם המקרים בהם הוצאתו של צו כנגד אותו האדם, או קבוצת בני אדם אשר הוא משתייך אליה, הנה האפשרות הסבירה להתחקות אחר החפצים הדרושים לצורכי חקירה או משפט. בית המשפט, בהפעילו את שיקול דעתו אם להוציא את הצו להמצאת מסמכים, יתן גם משקל למידת המאמץ, ההוצאה הכספית והשקעת הזמן, הכרוכים במילוי הצו מצד האדם הנדרש לבצעו". עמדה זו אף הובעה בהקשר לפעולות חקירה באינטרנט. ראו ב"ש (מחוזי ת"א) 90868/00 **חב' נטוויז'ן נ' צבא ההגנה לישראל** (פורסם בנבו, 22.6.2000); ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף** (פורסם בנבו, 5.2.2007).

142 ראו Jonathan Zittrain, *Internet Points of Control* 44 B.C. L. Rev. 653 (2003); Reidenberg, *States and Internet Enforcement*, לעיל ה"ש 80. לניתוח כלכלי המצדד בהעברת חובות האכיפה לספקיות השירות משום שהן מונעי הנזק הזולים ביותר ראו, למשל, Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 Harv. J.L. & Tech. 395 (2003); Douglas Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 Sup. Ct. Econ. Rev. 221 (2006); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 Wm. & Mary L. Rev. 239 (2005).

שהדבר משית עליהן עלויות, אפשר ליצור מנגנון להחזר הוצאות, בדומה לזה הקבוע כיום בסעיף 10 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007. ככל שמנגנון החזר ההוצאות יהיה תלוי במספר הבקשות לחסימת גישה, לסינון תכנים או לניתוק משתמש מהשירות, ולא יבוסס על תעריף תקופתי קבוע ("גלובלי"), יהיה בו כדי להוות מעין גורם מרסן נוסף על רשויות האכיפה מפני הפרזה בשימוש בסמכות לחסום גישה או לסנן תכנים.

אשר לטענה השלישית, יש לזכור שספקיות שירות שונות כבר כללו מיוזמתן הוראה ב"תנאי השימוש", שלפיה הן תצייתנה להוראות כדין שתקבלנה מגורמי אכיפת החוק. כמו כן נקבעו בתנאי השימוש הוראות הכוללות איסורים בתחום התכנים הפוגעניים, וכן ציון של הסנקציה בדבר הסרת התוכן אם יפרו התכנים את תנאי השימוש. נוסף על כך, חלק ניכר מהספקיות קבעו בתנאי השימוש שלהן כי הן תצייתנה להוראות חוק מדינתיות או לצווים שיפוטיים המורים להן להסיר תכנים או להגבילם לגישה מהמדינה.[143] מכאן, שהספקיות נטלו על עצמן למעשה את ההתחייבות לכבד הוראות כופות של המדינה בנוגע להסרת תכנים או להגבלת גישה אליהם. חרף זאת, בהחלט יש מקום להכיר במעמד המיוחד של ספקיות השירות השונות ברשת כנושאות לא רק את זכויותיהן־שלהן אלא גם את המידע ואת הזכויות במידע של לקוחותיהן.[144] הכרה זו צריכה לבוא לידי ביטוי באופן שבו תישקל בקשה להורות לספקיות השירות לבצע את פעולות החסימה או הסינון הנדרשות. ככל שמדובר בהתערבות בתוכן החורג מתנאי השימוש הפנימיים של ספקית השירות לגבי תכנים אסורים, כך יגבר משקלו של השיקול בדבר הפגיעה בספקית, נוסף על הפגיעה הישירה במפרסם.

4. ביקורת מכיוון טכנולוגי (יעילותה של אסטרטגיית ההתגוננות והמניעה)

הטיעון הביקורתי הרביעי הוא במישור התועלת של יישום אמצעי האכיפה האלטרנטיביים. על פי טיעון זה, צעדי האכיפה האלטרנטיבית אינם מסוגלים להשיג באופן אפקטיבי את התוצאה המצופה – מניעת המשך התממשותן של עברות הביטוי במרחב הסייבר. הטיעון הכללי נחלק לטיעוני־משנה קונקרטיים יותר (שכל אחד מהם רלוונטי לחלק מצעדי האכיפה האלטרנטיביים, גם אם לא לכולם): (1) הגבלת גישה אל תוכן מסוים – למשל על ידי סינונו מתוצאות החיפוש או על ידי חסימת הגישה אליו ממדינה מסוימת – אינה מונעת הגעה אל הכתובת בדרך של גלישה by proxy, קרי: באמצעות גורם מתווך; (2) חסימת הגישה לכתובת IP מסוימת עלולה להוביל להכללת־יתר, שכן כשמדובר באתר אינטרנט הכולל עשרות, מאות ואף אלפי דפֵי־משנה, הרי שכל דפי־המשנה האמורים עלולים להיחסם גם אם רק דף־משנה אחד כולל את התוכן האסור. נוסף על כך, אף אם יסונן או יוסר תוכן של דף אינטרנט אחד, חלק ממנו עשוי להיות לגיטימי וראוי להגנת חופש הביטוי; (3) סינון

143 לעיל ה"ש 110.

144 בדומה להכרה במעמדן המיוחד של ספקיות השירות במסגרת דברי ההסבר לס' 72 בהצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד-2014, ה"ח הממשלה 867, הכולל הגדרה של "ספק שירות". הצעת החוק קובעת את סמכויות הראיות על ידי רשויות החקירה וקובעת מגבלות ייחודיות על הסמכות לקבל מידע האגור ברשותו של ספק שירות מקוון.

תכנים פוגעניים מתוצאות החיפוש או הסרה של דף מסוים הכולל תכנים אסורים עלולים לסבול גם מהכללת־חסר, במובן זה שלא כל התכנים האסורים יסוננו או יוסרו. להלן ארחיב על כל אחד מטיעוני־המשנה ואתמודד עמם.

אשר לטיעון־המשנה הראשון, אין ספק שגלישה by proxy, כששרת הפרוקְסי נמצא בחו״ל ואינו פועל באמצעות ספקיות הגישה לאינטרנט, מאפשרת לעקוף מנגנון של חסימת גישה או של סינון תוצאות חיפוש, המבוסס על הוראה הניתנת לספקיות הגישה לאינטרנט בישראל או למנוע החיפוש ביחס לכתובת IP מישראל בלבד.[145] אולם, אין בעובדה זו כדי לשלול את ההצדקה בדבר השימוש באמצעים אלה לצורך התמודדות עם עברות ביטוי. זאת מן הטעם שחלק ניכר מעברות הביטוי נועדו לפרסום ברבים, לקהל מזדמן או מעוניין ברמה מוגבלת. כך הוא לדוגמה ביחס לעברת ההסתה לאלימות: עברה זו נעברת בדרך של התקשרות מיחיד אל רבים. ה״יחיד״ הוא המפרסם, וה״רבים״ הם קהל היעד. המטרה של עברות אלה היא להגיע לקהל יעד רחב ככל האפשר, בלתי־מסוים, היכול להיות מושפע מהתכנים. צרכני התכנים האמורים יכולים להיות קהל המעוניין לצרוך את התוכן – אבל הוא אינו מעורב בעסקת העברה, הוא אינו מסוים, והוא אינו בהכרח מכיר את מפרסם התכנים. ההתקשרות בין הצרכנים לבין המפרסם אינה ישירה אלא מתווכת באמצעות הפרסום. עבור קהל יעד כזה, חסימת הגישה או סינון תוצאות החיפוש בהחלט ישיגו תוצאה אפקטיבית יחסית – צמצום החשיפה אל התכנים האסורים. זאת, משום שקהל היעד לא יחוש צורך מיוחד לתור אחר תוכני ההסתה בדרך של עקיפת המנגנונים הטכנולוגיים. לעומת זאת, במקרה של שני מעורבים בעסקת העברה, למשל שני אנשים המתכננים יחד, באמצעות התקשרות אינטרנטית, להוציא לפועל פיגוע טרור – מדובר בהתקשרות מסוג יחיד אל יחיד, בין שני אנשים המעוניינים לתקשר זה עם זה באופן בלעדי, ועל כן יוכלו לעקוף מנגנונים של חסימה שאינם יעילים טכנולוגית. הדברים האמורים לגבי עברת ההסתה לאלימות נכונים גם לגבי עברות ביטוי נוספות כגון לשון הרע, העלבת עובד ציבור, הסתה לגזענות, פרסום תכנים פדופיליים[146] וכדומה, והם נכונים גם לגבי עברות נוספות המתבצעות בדרך של פרסום כגון ארגון הימורים, סחר בסמים ועוד.

145 ההוראה בדבר חסימת הגישה נמסרת לספקיות הגישה לאינטרנט. ספקיות אלה נדרשות לחסום בקשת גלישה לכתובת IP מסוימת המצוינת בהוראה. כאשר משתמש אינטרנט מישראל גולש לשרת פרוקסי מסוים, ומשם הוא גולש הלאה לאתר החסום, אזי מבחינתה של ספקית הגישה לאינטרנט בוצעה גלישה לכתובת IP מותרת (של שרת הפרוקסי). ככל ששרת הפרוקסי נמצא בחו״ל ופועל באמצעות ספקיות גישה זרות, לא תיאסר בקשה לגלוש ממנו אל האתר החסום, שכן הוראת החסימה אינה חלה על ספקית הגישה לאינטרנט שאליה מנוי שרת הפרוקסי הזר. בדומה, הוראת סינון של מנוע החיפוש, שלפיה לא תוצג תוצאת חיפוש מסוימת כשהשאילתה מגיעה ממשתמש ישראלי, לא תתקיים כשהמשתמש הישראלי יגלוש אל מנוע החיפוש דרך שרת פרוקסי מחוץ לישראל. יוצא אפוא כי גלישה באמצעות שירות פרוקסי שכזה מאפשרת עקיפה של מנגנון חסימת הגישה למשתמשי אינטרנט מישראל ואת מנגנון סינון תוצאות החיפוש למשתמשים ישראליים.

146 עוד על המענה לטיעון־משנה זה, בהקשר של פרסומים פדופיליים, ראו חיים ויסמונסקי ״קידום המאבק בפדופיליה המקוונת – בעקבות חוק העונשין (תיקון מס׳ 118), התשע״ה-2014, והצעת

אשר לטיעון־המשנה השני, סביר להניח שיימצאו אתרים מעורבים שבהם יפורסמו תכנים אסורים בצד תכנים לגיטימיים. החשש הוא אפוא מפני חסימת ביטוי מוגן מעבר לחסימה של ביטויים מותרים. יצויין כי בכל הנוגע לסגירת מקומות פיזיים, חוק הגבלת שימוש במקום לשם מניעת ביצוע של עברות מכיר כיום בסמכות להורות על סגירת המקום גם אם מתקיימת בו פעילות לגיטימית בצד הפעילות הבלתי־חוקית.[147] ברי כי העובדה שהביטוי האסור מוטמע בתוכן שחלקו מותר אינה יכולה לחסן את הביטוי מפני הסרה או צמצום גישה. עם זאת, ברור גם שככל שהחלק הלגיטימי גדול יותר והחלק האסור מצומצם יותר וחמור פחות – כך יגבר המשקל של הנזק החוקתי, בגין צינון ביטוי מותר, על התועלת שבהגבלת הביטוי האסור, גם אם מדובר בהקשר של ביטוי מקוון.

אשר לטיעון־המשנה השלישי, בדבר הכללת־חסר, אכן יש להכיר בכך שהגבלת תכנים לא יכולה ללכוד את כל התכנים האסורים, וזאת לנוכח תכונותיו של המרחב המקוון, המאפשר לכל אדם להעלות את תכניו בעלות נמוכה עד אפסית, במהירות רבה, מכל מקום. התכנים מועלים על גבי פלטפורמות מבוזרות והם ניתנים לשכפול והעברה מ"מקום" ל"מקום" במהירות הבזק במרחב האינטרנטי. בכל הנוגע לטיעון בדבר הכללת־חסר, חשוב לציין את האתגר החדש המסתמן בשנים האחרונות לרשויות אכיפת החוק בדמות ה־Darknet.[148] כאמור, מדובר באזורים באינטרנט שאינם ניתנים לאיתור באמצעות מנועי החיפוש, והכניסה אליהם והשימוש בהם נעשים באמצעות דפדפן כגון TOR להסוואת הזהות. חלק נכבד מהתכנים ב־Darknet כולל פרסומים אסורים לסוגיהם: תכנים פדופיליים, תכנים תומכי טרור ומסיתים, מידע אישי גנוב ועוד.[149] ככלל, האתרים ב־Darknet אינם ניתנים לחסימת גישה שכן הם מבוססים על כתובת IP פיקטיבית, ופעולת החשיפה של כתובת האתר המרכז את הפעילות האסורה או של משתמשי הרשת הפועלים בו עלולה להיות מאומצת ובלתי־צליחה. גם ניסיון להביא להסרת התכנים מכוח הוראה כופה – לא כל שכן מכוח שיתופי פעולה עם משתמשים הפועלים ב־Darknet – אינו ישים. המענה לטיעון־משנה זה דומה למענה לטיעון־המשנה הראשון: הפעילות ב־Darknet מתאימה במיוחד לשני מעורבים או יותר בעסקת העברה, המעוניינים לפעול במחתרת, ולכן זירה זו רלוונטית פחות למאבק בפרסומים מסוג יחיד אל רבים, כאשר הרבים הם משתמשי אינטרנט שאינם עושים מאמץ מיוחד כדי להגיע אל התכנים. במילים אחרות: בכל הנוגע לפרסומים פדופיליים, ייתכן בהחלט שמשתמש אינטרנט פדופיל, המעוניין מאוד להגיע אל תכנים אלה, יגלוש אל "הרשת

חוק הגבלת שימוש במקום לשם מניעת ביצוע עבירות (תיקון מס' 2), התשע"ד–2014" **מאזני משפט** י 181, 199–202 (2015).

147 ראו חוק הגבלת שימוש במקום לשם מניעת ביצוע עברות, התשס"ה–2005, ס' 2(א)(1) ו־3(א)(1). כן ראו ס' 4–5 להצעת חוק הגבלת שימוש במקום לשם מניעת ביצוע עברות (תיקון מס' 2), התשע"ד–2014, ה"ח הממשלה 839 שנועדו להחליף את ההוראות שמניתי לעיל ולקבוע תחתן הוראה חדשה. ההוראה החדשה אינה משנה את העיקרון הרלוונטי לענייננו, שלפיו אפשר להורות על סגירת מקום שמתקיימת בו פעילות אסורה על פי החוק גם אם בצדה מתקיימת פעילות לגיטימית.

148 לעיל ה"ש 26.

149 גולדשמידט "שימוש ברשתות תקשורת אנונימית על גבי האינטרנט למטרות פשיעה", לעיל ה"ש 26.

האפלה"; עם זאת, בכל הנוגע לפרסומי הסתה, לשון הרע, פגיעה ברגשי דת, העלבת עובד ציבור וכיוצא באלה – אלה הם פרסומים שקהל היעד אינו נמשך אליהם במיוחד ולכן לא סביר שיפנה במיוחד אל הרשת האפלה כדי לתור אחריהם. מהרשת האפלה חזרה אל הטיעון הכללי יותר: המענה לטיעון הכללת־החסר הוא שטיעון זה אינו צריך לשלול את ההצדקה להשתמש באמצעי האכיפה האלטרנטיביים, כל עוד מושגת תוצאה של צמצום החשיפה אל חלקים משמעותיים מהתכנים האסורים המתפרסמים ברשת.

לסיכום: הביקורת מהכיוון הטכנולוגי היא בעלת משמעות דו־כיוונית – בכיוון של הכללת־יתר ובכיוון של הכללת־חסר. בכל הנוגע להכללת־חסר, כל עוד יש למנגנוני האכיפה האלטרנטיביים אפקטיביות מסוימת, לא־מבוטלת, אין החלל החסר מכתים את המתודה כולה. בכל הנוגע להכללת־יתר, כאן בהחלט יש משמעות לפוטנציאל הפגיעה האפשרית, להיקפו ולאפשרות למזער את הפגיעה העודפת. משמעות זו צריכה למצוא את ביטויה באופן שבו יגולמו איזונים ובלמים בתהליך היישום של פעולות האכיפה האלטרנטיבית, כפי שאפרט להלן.

ה. היישום של מודל האכיפה האלטרנטיבית על עברות ביטוי במרחב המקוון

1. סיכום עד כאן

ככלל, המשפט הפלילי מבכר את המתודה של איתור, חקירה ועניש בדיעבד בגין התנהגות מזיקה על פני מניעה וסיכול של אותה התנהגות. הנחת המוצא היא שהרתעה אפקטיבית מושגת באמצעות העלאת סיכויי האיתור של מבצע העברה והשגת ראיות קבילות נגדו להעמדה לדין ולהרשעתו.[150]

עם זאת, כפי שהראיתי בנוגע לעברות ביטוי, מרחב הסייבר כזירה לביצוע עברות מערער את מושכלות היסוד של האכיפה הפלילית הקלאסית. נוכח תכונת הבין־לאומיות של האינטרנט, כמו גם היכולת להשתמש באמצעים להסוואת זהות (אנונימיזציה) ולהצפנה של התכנים, החקירה הפלילית בדיעבד עלולה להגיע לא אחת למבוי סתום, הן משפטית (היעדר סמכות אכיפה בין־לאומית) והן טכנולוגית (היעדר יכולת להתגבר על אמצעי האנונימיזציה וההצפנה שנקטו החשודים). באותם המצבים שבהם החקירה הפלילית הקלאסית אינה יכולה להגשים את האינטרס הציבורי שבענישת מבצעי העברות וביצירת הרתעה מפני ביצוע עברות נוספות, יש מקום לשקול אסטרטגיה הגנתית. אסטרטגיה זו תתמקד במניעת ההתפשטות של התוכן האסור ובצמצום פגיעתו. כתוצאה מכך, כדי להשיג אפקט זהה מבחינת היקף הפרסום, מידת תפוצתו ומשך פרסומו, יידרש המפרסם (מבצע העברה) למאמץ גדול בהרבה.

אסטרטגיה זו – התגוננות משפטית באמצעות מהלכי אכיפה אלטרנטיביים – מתאימה להתקשרויות מקוונות מסוג יחיד אל רבים ומסוג רבים אל רבים, כשמטרת הפרסום היא להגדיל את קהל היעד ככל האפשר (כמו בעברות ביטוי) – להבדיל, למשל, מהתקשרויות אישיות או חשאיות מסוג יחיד אל יחיד. אמנם אסטרטגיות של התגוננות ומניעה רחוקות משלמות מבחינה טכנולוגית, ואפשר לעקוף את המנגנונים לחסימת הגישה או לסינון התכנים,

150 לעיל ה"ש 9.

אולם מנגנונים אלה מקטינים את החשיפה האינצידנטלית לתכנים המגלמים עברה פלילית. חשיפה אינצידנטלית זו, המייצרת זמינות של התוכן האסור, היא משתנה מרכזי בהגדלת קהל היעד של הפרסום המדובר. במילים אחרות: עקיפת המנגנונים לחסימת הגישה או לסינון התכנים יכולה להיות מנת חלקם של משתמשי רשת אקטיביים (המודעים לפרסום האסור ומנסים להשיגו), אולם היא אינה יכולה להיות מנת חלקו של משתמש רשת פסיבי שאינו מגלה עניין מיוחד בחשיפה אל הפרסום המדובר. מבצעי עברות הביטוי שואפים להגיע לקהל יעד גדול ככל האפשר, כך שלאיבוד קהל משתמשי הרשת הפסיביים יש משמעות רבה.

מבחינה משפטית, ככל שהבחירה היא בין שתי אפשרויות -אסטרטגיה של התגוננות ומניעה ואסטרטגיה של חיזוק מערך הסמכויות של רשויות האכיפה במרחב המקוון, כדי להתגבר על מכשלות האכיפה המשפטיות והטכנולוגיות במרחב – בהחלט אפשר לומר שהאמצעי שפגיעתו פחותה הוא האמצעי ההגנתי. חיזוק האמצעים החקירתיים הקלאסיים כדי להתאימם לצורכי החקירה במרחב המקוון עלול לגבות מחיר גבוה יותר מבחינת הפגיעה בזכויות מוגנות. כך, ההתגברות על בעיית האנונימיזציה וההצפנה עלולה לחייב סמכות לשימור דרך קבע של כלל נתוני התקשורת של משתמשי הרשת כדי שאפשר יהיה לאתר בדיעבד את הגורם שערך את הפרסום האסור, הפיצו וכדומה. התגברות על בעיית הבין־לאומיות של הרשת תגרור טענות לפגיעה חוקתית אקסטרה־טריטוריאלית.

2. עקרונות בהפעלה של מנגנוני האכיפה האלטרנטיבית

בשים לב לביקורות שהוצגו בפרק ד׳, חשוב להציב בקרות ואיזונים אל מול פעולות האכיפה האלטרנטיביות שיובילו למחיקה או לצמצום הגישה לביטויים ברשת. להלן אציג כמה עקרונות מוצעים לפעולתן של רשויות האכיפה בשדה האכיפה האלטרנטיבית.

(א) *שקיפות פעולתן של רשויות האכיפה*

חובת התיעוד והשקיפות של פעולת הרשויות משרתת בהקשרנו שתי מטרות מרכזיות. המטרה הראשונה היא שקיפות מלאה כלפי מי שנפגעים במישרין מפעולת הרשות. בזכות התיעוד והשקיפות יוכלו נפגעים אלה לממש את זכויותיהם ולטעון נגד פעולת הרשות. המטרה השנייה של חובת התיעוד והשקיפות היא מתן מידע לציבור הכללי, שאפשר לראותו כנפגע מסדר שני מפעולתן של הרשויות בזירת האכיפה האלטרנטיבית. עיקרון של תיעוד ושקיפות מאפשר ביקורת אפקטיבית **בדיעבד** על פעולתן של רשויות האכיפה ובית המשפט, ולמעשה יש בכוחו כדי להרתיע **מראש** את הרשות מפני הרחבת הרשת לעבר ביטויים שלא ראוי להגבילם. תיעוד ושקיפות מפתחים אחריותיות (Accountability) של רשויות האכיפה. נוסף על כך, הם משמשים רכיב חשוב בביסוס הלגיטימציה של הרשות המנהלית. יידוע הציבור – בדבר כמות הבקשות על בסיס וולונטרי וכמות ההוראות הכופות (מכוח חוק או צו שיפוטי) להסרת תכנים פוגעניים או לצמצום הגישה אליהם – יוכל למתן את האפקט המצנן על חופש השימוש במרחב המקוון,[151] העלול להיווצר בשל אי־ידיעת ההיקפים והסוגים של התכנים שהוגבלו. כך יצטמצם הנזק ההיקפי שנגרם עקב פעולות האכיפה האלטרנטיביות, העלולות ליצור הרתעת־יתר בשל התחושה שהציבור לא מיודע

151 לפגיעה זו ראו לעיל בפרק ד2.

על המידע שאינו חשוף לו במרחב המקוון. חלק מספקיות השירות המסירות תכנים או מגבילות גישה אליהם מפרסמות כיום את הנתונים בדבר מידת ההתערבות שלהן בתכנים על פי דרישת המדינות, במסגרת חובות שקיפות שגזרו על עצמן.[152] עם זאת, ובשים לב לכך שמדובר בדיווח וולונטרי של הספקיות, אין בכך כדי לייתר את חובת השקיפות ברמה המדינתית, הנגזרת מחובת הרשות המנהלית כפי שציינתי לעיל. כך, אפשר יהיה לחייב את המדינה לפרסם את נתוני הבקשות שהגישה בפילוח לפי סוג העברה הפלילית שבה מדובר, לפי הגורם שאליו הופנו הדרישות – בין במסלול הוולונטרי־ההסכמי מול ספקית השירות ובין במסלול הכוחני מכוח צו שיפוטי, וכיוצא באלה.

(ב) *מקורות המידע של רשויות האכיפה בנוגע לעברות הביטוי המקוונות ושיתוף הציבור*

כיצד ייאסף המידע בדבר הפרסומים האסורים במרחב המקוון? האם תנקוטנה רשויות האכיפה את כלי האכיפה האלטרנטיביים – הן ההסכמיים, אל מול ספקיות השירות המקוונות, והן הכופים, באמצעות דרישות משפטיות שתוצגנה לספקיות השירות – אך ורק במענה לתלונות, או שמא על הרשויות לנטר את הפרסומים האסורים ביוזמתן? מטבע הדברים, ככל שהרשויות תנטרנה מיוזמתן את התכנים יהיה בכך כדי להגביר את האפקט המצנן של פעילות מעין זו על חופש הביטוי של כלל משתמשי המרחב המקוון ועל חופש השימוש שלהם במרחב.[153] עם זאת, פעולות יזומות לאיתור תכנים אסורים בידי הרשויות, בדרך של

---

152 כך, לדוגמה, חברת גוגל העולמית מפרסמת נתונים מעין אלה באתר לומן Lumen, www. lumendatabase.org (last visited Feb. 22, 2017). מדובר בארכיב דיגיטלי שנוסד בשנת **2001**, שבו ספקיות שירות המקבלות הוראות מחייבות להסרת תכנים או לצמצום הגישה אליהם נוהגות לדווח על אודות טיב ההוראות, מקורן, המועד שבו ניתנו וכדומה. לדיווחים של חברת פייסבוק על בקשות שהתקבלו מממשלות להסרת תכנים ראו Facebook, Government Requests Report, https://govtrequests.facebook.com/ (last visited Feb. 22, 2017).

153 על תופעת האפקט המצנן בשל תחושת המעקב הכללית כתב במקור ג׳רמי בנת׳ם (Bentham), שתיאר את מודל הפאן־אופטיקון כהצעה למבנה שיאפשר לאדם אחד בלבד לפקח על כלל האסירים בבית הסוהר, או על תלמידים בבית ספר, על חולים בבית חולים וכו׳. המבנה העגול ייבנה כך שהאסירים לא יוכלו לדעת להיכן מביט השומר בכל רגע נתון, וכך הם יניחו כל העת שהם מפוקחים בפועל – וכתוצאה מכך יתאימו את התנהגותם להתנהגות תחת מעקב (קרי: יימנעו מלהפר את נוהלי בית הסוהר). ראו Catherine Pease-Watkin, *Jeremy and Samuel Bentham – The Private and the Public*, 5 J. Bentham Studies 3 (2002). מישל פוקו (Foucault) חזר אל המודל הארכיטקטוני של הפאן־אופטיקון מאוחר יותר כמטאפורה למשמעת ולהתנהגות ה״נורמלית״ שהחברות המודרניות מנסות להשליט על כלל האנשים. ראו Michel Foucault, The Foucault Reader 188–193 (Paul Rabinow ed., 1984). היו חוקרים שחזרו אל מטאפורת הפאן־אופטיקון לתיאור ההשפעה של טכנולוגיות מעקב על התנהגות הפרטים בחברה. ראו, למשל, Oscar H. Gandy Jr., The Panoptic Sort: A Political Economy of Personal Information (1993), שם המחבר דן בפאן־אופטיקון בשל השימוש ההולך וגובר בטכנולוגיות מעקב ובמחשוב (נכון לתקופת כתיבת הספר). כן ראו Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace* 28

איסוף מידע גלוי ברשת (WebInt), כפי שיכול לבצע כל גורם פרטי שהוא, יכולות להתבצע גם על ידי הרשויות. ככל שהפעולות להצפת תכנים אסורים אינן כוללות הפעלת סמכויות שלטוניות ייחודיות, האסורות על גורם פרטי, נראה כי אין מקום לאוסרן על רשויות האכיפה. נכון שכאשר הפעולות הללו מתבצעות על ידי המדינה, האפקט המצנן הפוטנציאלי שונה בהשוואה למצב שבו הן מתבצעות על ידי גורם פרטי כגון מכון מחקר או גורם עיתונאי; אולם פעולות אלה הן ברף הנמוך ביותר מבחינת פעולות החשיפה להצפת תכנים אסורים בעלי פוטנציאל פגיעה בערכים מוגנים.

נוסף על פעילות יזומה זו של רשויות האכיפה נכון ליצור מנגנון דיווח יעיל וזמין עבור הציבור, כדי שיוכל לדווח לרשויות האכיפה על תכנים אסורים. כיום אין למעשה כתובת לאומית לדיווח על פגיעות ברשת, ותחת חֶסֶר זה התפתחו מנגנוני דיווח לגורמי המגזר השלישי דוגמת עמותת "כפתור אדום",[154] עמותת "אשנב"[155] ואיגוד האינטרנט הישראלי.[156] פעילותן של עמותות אלה מגוונת וכוללת הסברה, העלאת מודעות, חינוך וכדומה. בהקשרנו, עמותות אלה מדווחות לעתים לספקיות השירות ולעתים למשטרה, כשיש חשד לעברה פלילית. כמו כן, כפי שציינתי לעיל,[157] חלק מספקיות השירות המקוונות הקימו מנגנוני דיווח של המשתמשים על תכנים אסורים. יצירת מעין "מוקד 100" לאומי לדיווח על תכנים אסורים באינטרנט תוכל לשמש גם כמקור מידע משמעותי לרשויות האכיפה על תכנים אסורים. כמו כן, מוקד כזה יוכל להגביר את תחושת הביטחון ברשת, שכבר לא תיתפש כשטח הפקר, וכן להגביר את הלגיטימציה לפעילות אכיפה ברשת.

(ג) *ביקורת שיפוטית ולא מנהלית בכל הנוגע לאכיפה אלטרנטיבית במסלול הכוחני*

בדיני החקירה מוכרת הבחנה בין פעולות חקירה מסוימות הדורשות הסמכה מנהלית לבין פעולות אחרות המחייבות הסמכה שיפוטית.[158] הבחנה זו מתקיימת כמובן גם בחקיקה

(1996) Conn. L. Rev. 981, שם המחברת דנה בחשש מפני עידוד טכנולוגיות של מעקב אחרי הרגלי הגלישה באינטרנט לצורך מניעת הפרות של זכויות יוצרים באינטרנט. ראו גם מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 61 (2007).

154 "הכפתור האדום" /redbutton.org.il.

155 "אשנב – אנשים למען שימוש נבון באינטרנט" /eshnav.org.il.

156 "המרכז לאינטרנט בטוח" www.isoc.org.il/safe (פועל במסגרת איגוד האינטרנט הישראלי).

157 לעיל ה"ש 83.

158 ראו, למשל, את ס' 23א לפסד"פ, הדן בצו שיפוטי המתיר חדירה לחומר מחשב, וכן את ס' 43 לפסד"פ, הקובע כי שופט רשאי להורות בצו על הצגת חפצים הנדרשים כראיה. לעומת זאת ראו, למשל, את ס' 7 לחוק האזנת סתר, התשל"ט-1979 (להלן: חוק האזנת סתר), הקובע אפשרות לקבל היתר מנהלי (של מפכ"ל המשטרה) להאזנת סתר במקרים דחופים, או את ס' 32 לפסד"פ המתיר לשוטר לתפוס כל חפץ שיש לו יסוד להניח שנעברה בו עברה, שעומדים לעבור בו עברה, או שהוא עשוי לשמש ראיה בהליך משפטי או שניתן כשכר בעד ביצוע עברה או כאמצעי לביצועה.

הזרה.[159] בניסיון לתור אחר ההצדקות להסמכה מנהלית ולא שיפוטית אפשר להציג שתי טענות. ראשית, לעתים פעולת האיסוף נתפשת כפעולה לא פוגענית במיוחד, ועל כן לכאורה אין הצדקה בביקורת שיפוטית, שהיא בדרגה גבוהה משל ביקורת מנהלית. שנית, לעתים צורכי החקירה דחופים במיוחד, ולכאורה אין שהות לקיים הליך שיפוטי במעמד צד אחד לצורך הסמכת הרשות החוקרת.

לדעתי, הטענה הראשונה אינה תקפה כשמדובר בפעולות במסלול הכוחני, שתוצאתן פגיעה בביטוי מקוון – שלא על בסיס תנאי השימוש של ספקית השירות שבפלטפורמה שלה פורסם התוכן המדובר. ההפך הוא הנכון: הפעולות המשפטיות הייחודיות של מניעת ביטוי, צמצום הגישה אליו וסיכול היקף פרישתו – אלה הן פעולות משפטיות רגישות ומורכבות, המגלמות פגיעה במפרסם, בפלטפורמה המנגישה את הפרסום ובציבור משתמשי האינטרנט הצורך תכנים ברשת. כאשר מדובר בפעולות אכיפה אלטרנטיבית מכוח הוראת חוק כופה, הקביעה הקונקרטית שהפגיעה היא מידתית וראויה צריכה להימסר אפוא לבית המשפט, שכן מדובר בקביעה שיפוטית מדרגה ראשונה, המחייבת איזון עדין בין הצרכים של רשויות האכיפה לבין הזכויות החוקתיות המושפעות מפעולת האכיפה האלטרנטיבית. כאשר מדובר באכיפה מכוח הסכמות וולונטריות עם ספקיות השירות, אין מקום לביקורת שיפוטית אולם יש מקום, כפי שציינתי לעיל, להגברת השקיפות והדיווח לציבור על נקיטת פעולות אלה, שתוצאתן צמצום החשיפה לביטויים ברשת.

אשר לטענה השנייה, בדבר צורכי דחיפות מיוחדים: כאשר ביטויים אסורים מסוימים עלולים לגלם סיכון ממשי לביטחון המדינה או לביטחונו של אדם, יש מידה לא מבוטלת של דחיפות מבחינת רשויות האכיפה. אפשר לומר שעיכוב בהסרת התכנים עלול להוביל לשכפולם ולהמשך הפצתם באופן שיקשה לאתר את כל ההעתקים ולהוביל להסרתם או לחסימתם. עם זאת, דומה שאי־אפשר יהיה לוותר על בקרה שיפוטית בכל הנוגע לפעולה בערוץ הכוחני – חיוב ספקיות השירות המקוונות להסיר תכנים פוגעניים או לצמצם את הגישה אליהם – ופעולה כזו תצטרך להיות מתואמת לדיון קצר מועד ככל האפשר, בדומה לדיונים אצל שופטי מעצרים.[160]

נוסף על האמור עד כה, ראוי בהחלט לכונן גם "תחנה" מקדימה במסגרת הרשות המבצעת בכל הנוגע לנקיטת פעולות להסרת תכנים או לצמצום החשיפה אליהם. זאת, הן במקרה של פעולות במסלול הוולונטרי־ההסכמי והן במקרה של פעולות במסלול הכוחני. ראוי שתחנה זו תהיה בדמות אישור מקדים של גורם ממונה בכיר, חיצוני לרשות החוקרת, שיפעיל ביקורת מנהלית־פנימית טרם הנקיטה בפעולת האכיפה האלטרנטיבית. במסלול הכוחני תהיה זו תחנה מקדימה, פנימית, טרם הפנייה לבית המשפט לבחינה שיפוטית־חיצונית; במסלול הוולונטרי־ההסכמי תהיה זו תחנה מאשרת טרם הפנייה בבקשה לספקית השירות. הבקרה

159 לדוגמה, בדין האמריקני הסמכות להורות על שמירת מידע מכאן ולהבא (Preservation) היא סמכות בהיתר מנהלי. ראו 18 U.S.C. § 2703(f) (1986). לעומת זאת, סמכות החיפוש בחצרים או במחשב, למשל, היא שיפוטית (Search warrant).

160 כידוע במציאות הישראלית המרחקים הגאוגרפיים קצרים, ובית המשפט מציב שופטים תורנים גם בשעות הלילה. מכאן, שאפשר להגיע לקבועי־זמן קצרים עד לפתיחת דיון שיפוטי בבקשת המדינה להסיר תוכן מהאינטרנט או לצמצם גישה אליו.

המנהלית המקדימה תבחן את עצמת הצורך של רשויות האכיפה, את האפשרות לפעול בדרך של אכיפה פלילית קלאסית לעומת ההצדקה לנקיטת דרכי פעולה אלטרנטיביות, את מידת האפקטיביות הפוטנציאלית של האמצעים האלטרנטיביים בשים לב לטיב הפרסום ולקהל היעד, את היקף המידע העשוי להיחסם או להימחק במסגרת הפעולה האלטרנטיבית ועוד. ה"תחנה" המנהלית, במיוחד אם היא חיצונית לרשות החוקרת או לרשות הביטחון, מגבירה את הבקרה והסינון של בקשות לא ראויות המגלמות פגיעה לא מידתית בערכים מוגנים.[161] כאשר מדובר בפעולות אכיפה אלטרנטיבית במסלול הכופה תיתכן טענה שקביעת תחנה נוספת של בקרה מנהלית מקדימה, טרם הפנייה לבית המשפט, עלולה לסרבל הליכים שמטבעם צריכים להתנהל במהירות, במטרה למנוע מהפרסום האסור להתפשט. על כן, המנגנון המנהלי הפנימי צריך להיות מותאם וערוך למתן מענה דחוף.

(ד) *הבניית שיקול הדעת המנהלי והשיפוטי בנוגע ליישום האכיפה האלטרנטיבית*

הבניית שיקול הדעת בחקיקה היא טכניקה המנסה לחבר בין האיזון החוקתי העקרוני, המכונה גם "definitional balancing", ברמת הערכים המתנגשים, לבין האיזון החוקתי הקונקרטי, המכונה גם "ad-hoc balancing", ברמת המקרה הנתון.[162] במסגרת האיזון החוקתי העקרוני נקבעות קטגוריות קשיחות של תנאי כניסה, פעולות מותרות ופעולות אסורות. במסגרת האיזון החוקתי הקונקרטי, בעל הסמכות (בחקיקה המסדירה פעולות האכיפה יהיה זה בדרך כלל גורם שיפוטי או גורם מנהלי, תלוי בסוג הסמכות שבה מדובר) מחליט במקרה מסוים אם הפעולה המבוקשת ראויה לביצוע בנסיבות העניין.

לדעתי, יש מקום לצדד בהבניה של שיקול הדעת השיפוטי, כמו גם של שיקול הדעת המנהלי, בבוא המדינה לנקוט פעולות מתחום האכיפה האלטרנטיבית, בעיקר במישור הכוחני. זאת, בשל מורכבות האיזון החוקתי שתוצאתו עשויה להיות הסרה או צמצום החשיפה לביטויים מסוימים ברשת. כמו כן, קבלת ההחלטות במסגרת הפעלה יעילה של אכיפה אלטרנטיבית מתקיימת בתנאים חסרים: לרוב מדובר בהליכים דחופים; ההליכים עשויים להתקיים במעמד צד אחד (ex parte) שכן אי־אפשר להתדיין עם המפרסם (העשוי כאמור להימצא מחוץ לטריטוריה של המדינה האוכפת, לשמור על אנונימיות וכו'); יתר על כן: נדרשת הבנה ברמה גבוהה למדי של המדיום האינטרנטי על מופעיו השונים. בשל כל אלה, הבנייתו של שיקול הדעת – הן השיפוטי (בהקשר של הפעלת המסלול האלטרנטיבי הכוחני)

161 כדוגמה למנגנון של בקרה מנהלית חיצונית, שלאחריה בקרה שיפוטית, אפשר לציין את ס' 9א לחוק האזנת סתר, העוסק בהיתר להאזנת סתר לבעלי מקצועות חסויים (עורכי־דין, רופאים, פסיכולוגים, עובדים סוציאליים וכהן דת). על פי הסעיף, האזנה לבעל מקצוע חסוי, לבקשת רשות ביטחון או רשות חוקרת מוסמכת, צריכה לעבור שתי "תחנות": הראשונה היא אישור מוקדם של היועץ המשפטי לממשלה, של פרקליט המדינה או של הפרקליט הצבאי הראשי בעניין שבתחום סמכותו; השנייה היא אישור בית המשפט.

162 להבחנה זו ראו, למשל, Melville B. Nimmer, *The Right to Speak from Times to Time: First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 Cal. L. Rev. 935, 942 (1968).

והן המנהלי (בהקשר של הגשת בקשות במסלול האלטרנטיבי הכוחני, ובמידה מסוימת גם בהקשר של הפעולה במישור הוולונטרי) – משרתת מטרות רצויות של ודאות, אחידות, צפיות ויכולת אפקטיבית יותר לבקר בדיעבד את ההחלטות שהתקבלו. מנגד, ההבניה אינה נוטלת את עצמאות שיקול הדעת, שכן מלאכת האיזון בין האינטרסים, הערכים והזכויות המתנגשות במקרה הנתון לעולם תחייב הפעלה עצמאית של שיקול דעת.[163]

לא אתיימר לפרט במסגרת המאמר את כל כללי ההבניה, אולם אמנה שלושה כללים: לפי **הכלל הראשון**, ראוי לקבוע כי פעולה להסרת ביטוי[164] פוגעני או צמצום גישה אליו באפיק הכוחני, שאינה תואמת את כללי השימוש של ספקית השירות המציגה או מנגישה את הפרסום, תתבצע רק כשמוכח סיכון לביטחון המדינה, לביטחון הציבור או לביטחונו של אדם. במילים אחרות, לא די בהוכחת עצם קיומה של עברה פלילית המגולמת בפרסום הפוגעני, אלא יש להראות כי העברה הפלילית מגלמת במקרה המסוים גם סיכון ממשי לביטחון.[165] מטבע הדברים, הוכחת הסיכון לא תוכל להתבצע על פי מבחנים של משפט פלילי, שכן מדובר בהליך מזורז שיתבצע ללא משפט. הוכחת הסיכון תתבצע בדומה למבחנים הראייתיים של דיני המעצרים – הוכחת "יסוד סביר לחשש"[166] שייגרם סיכון לביטחון המדינה, לביטחון הציבור או לביטחונו של אדם. יובהר כי מבחן ה"יסוד הסביר לחשש" מצוי במדרגה נמוכה יותר ממבחן הוודאות הקרובה שבו נעשה שימוש להגבלת ביטויים בפסיקת בית המשפט העליון בעבר,[167] וזאת מהטעמים שפורטו לעיל בפרק ד(1).

אפשר לקבוע לכלל זה שני חריגים: החריג הראשון הוא במקרה של פעולה באפיק הוולונטרי־ההסכמי, שאז כאמור די בכך שמתקיימת הפרת חוק לכאורה של הדין הישראלי,

163 ראו אהרן ברק **פרשנות במשפט** כרך ראשון – תורת הפרשנות הכללית 307–317 (1992). ברק טען כי לעולם לא יתאפשר להימנע מהותרת שיקול דעת שיפוטי, גם במשטר של הגבלה ותחימה של שיקול הדעת השיפוטי. יתרה מזו: ברק עצמו פעל להבניה (אמנם שיפוטית) של שיקול הדעת השיפוטי. ראו יגאל מרזל "'לו יהי כן!': על תרומתו של אהרן ברק להבניית שיקול הדעת השיפוטי" **ספר ברק: עיונים בעשייתו השיפוטית של אהרן ברק 103** (איל זמיר, ברק מדינה וסיליה פסברג עורכים, 2009). הטיעון של ברק מתחבר לטיעונו של הארט, שלפיו לעולם ייוותר מתחם של שיקול דעת בפירוש החוק, ושהוא מטיל ספק בעצם יכולתו של המשפט להבנות את שיקול הדעת השיפוטי באופן כה מושלם עד שלא יהיה מקום עוד למושגים שהם רקמה פתוחה (open texture) ותורת המשפט תהיה מכנית. ראו H.L.A. Hart, The concept of Law 121-150 (2nd ed. 1994).

164 עשויה להתעורר שאלה בדבר דינן של עברות מקוונות אחרות, שלא נמנו במאמר, הכוללות אלמנט של "פרסום" או "הצגה" אך אינן נתפשות כעברות המגלמות פגיעה בחופש הביטוי. אלה הן עברות כגון מכירת סמים מסוכנים באינטרנט, ארגון הימורים מקוונים, הצעת שירותי זנות באינטרנט ועוד. אלה הן עברות של "עסקאות עברה" המקודמות על דרך של "דיבור", אולם אין לראות בהגבלתן משום הגבלה של ביטוי מוגן. על כן, ההתנגשות החזיתית עם חופש הביטוי של המפרסם (מבצע העברה) אינה מתקיימת כאן. לפיכך, אפשר לקבוע תנאי סף נמוכים יותר להסרה או להגבלה של העברות המקוונות במסגרת מהלכי אכיפה אלטרנטיביים.

165 כך, למשל, פרסום העולה כדי העלבת עובד ציבור או לשון הרע אך אינו מגלם איום, סחיטה או עברות שמגולם בהן פן של מסוכנות, לא יוכל להיחסם באפיק הפעולה האלטרנטיבי הכוחני.

166 ראו ס' 13(א)(2) ו־21(א)(1)(ב) לחוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996.

167 לעיל בה"ש 118.

ובה בעת מתקיימת הפרה של תנאי השימוש של ספקית השירות, כדי שתהיה הצדקה להסרת תוכן או לצמצום הגישה אליו. החריג השני הוא במקרה של פסק דין חלוט הקובע כי הפרסום הנדון מגלם עברה פלילית, שאז ראוי לאפשר הכרה בסעד של הסרת הפרסום או צמצום הגישה אליו מכוח צו שיפוטי, אף אם הפרסום אינו מגלם מסוכנות לביטחון כשלעצמו, שכן הסעד המבוקש הוא למעשה הפסקת המשך ביצוע עברה, שעליה החליט בית משפט מוסמך במסגרת הליך משפטי מלא של בירור אשמה.[168]

לפי **הכלל השני** ראוי לקבוע כי בבוא הגורם המנהלי או הגורם השיפוטי (בין במסלול הכוחני ובין במסלול הוולונטרי) לבחון את הסרת התוכן הפוגעני או את צמצום הגישה אליו, יהיה עליו לבחון את השאלה אם אפשר להגביל את הפרסום האסור באופן "כירורגי" ולהימנע מפגיעה היקפית בביטויים מוגנים. שאלה זו תלויה בטיב הפרסום, בפלטפורמה שבה פורסם וביכולות של ספקית השירות לבצע את ההגבלה הכירורגית. ככל שהפגיעה ההיקפית בפרסומים מותרים תהא רחבה יותר, כך מטבע הדברים תהיה הנטייה לאשר את הגבלת הביטוי נמוכה יותר.

לפי **הכלל השלישי**, בקבלת החלטות בדבר הסרת תכנים אסורים או צמצום הגישה אליהם, במיוחד באפיק הכוחני, יש לבחון את כמות האנשים החשופים לפרסום כגון כמות האנשים המנויים על דף הפייסבוק שבו התפרסם התוכן האסור או כמות האנשים שביצעו פעולות אוהדות לפרסום כגון "חיבוב" (like) או "שרשור" (retweet) וכדומה. נוסף על כך יש לנסות לאפיין את קהל היעד של הפרסום – האם הוא הומוגני ושייך לקבוצה מוגדרת או שמא הוא כללי ומגוון. לעניין זה תיתכן משמעות מבחינת פוטנציאל המסוכנות בפרסום. עוד יש לבחון את כמות הפרסומים ואת מידת ההשפעה הציבורית של המפרסם, במיוחד כשמדובר בבחינת הסנקציה של הרחקת המשתמש (שאז תיתכן משמעות לעוצמת הקול שהושתק).

168 לדיון בסעד של הפסקת המשך ביצוע העברה ראו רע"א 2920/90 **קופת חולים של ההסתדרות הכללית של העובדים בארץ ישראל נ' מדינת ישראל**, פ"ד מז(1) 397, פס' 15 לפסק דינו של הנשיא שמגר (1993). באותו מקרה נדונה שאלת סמכותו הטבועה של בית המשפט להורות על הפסקת המשך ביצועה של עברה פלילית. להסדרה ספציפית בחקיקה של סעד זה, בהקשרים של לשון הרע ופגיעה בפרטיות, ראו ס' 29(א)(1) לחוק הגנת הפרטיות, וכן ראו ס' 9(א)(1) לחוק איסור לשון הרע. לא ברור אם במסגרת הליך פלילי שאינו בגין עברות של לשון הרע או פגיעה בפרטיות אפשר לבקש סעד של הסרת הפרסום הפוגע ואיסור המשך הפצתו. מכל מקום, אין ספק בעיניי שגם אם אין הוראת חוק המאפשרת לקבל סעד כזה, מדובר בלאקונה הנובעת מתפישה פיזית של המחוקק שלא ייתכן פרסום שייקבע לגביו שהוא עברה ואי־אפשר יהיה "לתפוס" אותו פיזית ולאסור את המשך פרסומו. התוצאה שבה עברה תוכל להמשיך להתקיים – ובית המשפט לא יוכל להורות על הפסקת המשך ביצועה, חרף העובדה שניתן פסק דין חלוט הקובע כי אכן מדובר בעברה – היא תוצאה בלתי־סבירה בעיניי. מעבר לכך, כאמור לעיל בחלק ג(3), בהצעת חוק להסרת תוכן שפרסומו מהווה עבירה מרשת האינטרנט, התשע"ז–2016, ה"ח הממשלה 1104, נקבע כי אם הועמד אדם לדין בגין פרסום התוכן האסור והורשע – התובע רשאי לבקש מבית המשפט במסגרת גזר הדין כי יינתן צו להסרת התוכן אף אם לא הוכח אלמנט הסיכון לביטחונו של אדם, לביטחון הציבור או לביטחון המדינה.

(ה) *מיקוד הטיפול בתחום האכיפה האלטרנטיבית*

אכיפה אלטרנטיבית במרחב הסייבר היא דרך פעולה חדשנית, מאתגרת מבחינה משפטית־טכנולוגית, וכרוכה בה מלאכת איזון עדינה ומורכבת בין הצרכים של רשויות האכיפה מחד גיסא לבין החשש מפני פגיעה עודפת בשיח הפתוח ברשת מאידך גיסא. לפיכך, נכון לייחד את הטיפול בנושאים אלה לגורמים מסוימים ומצומצמים ברשויות האכיפה, שיוסמכו לעסוק במאטריה משפטית זו. בכך אפשר יהיה להשיג כמה יתרונות: (1) מיקוד הטיפול הוא תהליך מוסדי חשוב המשמר את האקסקלוסיביות של השימוש בכלי האכיפה האלטרנטיבית, ובכך הוא מעצב את הכלים הללו ככלים שהשימוש בהם ייעשה ברגישות ובזהירות הראויים; (2) ייחוד הגורמים שיעסקו באכיפה האלטרנטיבית יבטיח את מחויבותם לפעולות אלה, באופן שיאפשר לקצר את טווחי הזמן עד לפעולה באפיקים האלטרנטיביים; (3) בכל הנוגע למסלול הוולונטרי של האכיפה האלטרנטיבית, אין ספק שייחוד הטיפול יאפשר מיסוד אפקטיבי יותר של קשרי העבודה אל מול ספקיות השירות, כמו גם לימוד והבנה מעמיקים יותר של תנאי השימוש שלהן. אלה יאפשרו למיין את הפרסומים המתאימים להסרה, לחסימה וכדומה על פי התבחינים של ספקיות השירות.

*

ארכיטקטורת המרחב המקוון היא שאפשרה את חדירתו לכל תחומי החיים, ובה בעת היא שהובילה לפריחה בתופעות פשיעה שונות, ובהן עברות הביטוי. תופעות של הסתה לגזענות ולאלימות, לשון הרע, פגיעה ברגשי דת, העלבת עובדי ציבור ואיומים עליהם עלו ונפוצו ברשת. מחיר ביצוען של עברות אלה במרחב הסייבר הוא כמעט אפסי; פוטנציאל התפוצה של הדברים גדול עשרות מונים מאשר במרחב הפיזי; האפשרות לחמוק מאחריות פלילית פשוטה וקלה. עם זאת, הפגיעה המגולמת בעברות האמורות אינה מוגבלת לגדרי המרחב המקוון, והסיכון והפגיעה הנגרמים בעטיין מורגשים במרחב הפיזי. לכן, ברי כי הסיכון והפגיעה האמורים מחייבים תגובה מצד רשויות האכיפה – אך נקודת שיווי המשקל בין רשויות האכיפה לבין מבצעי העברות מתערערת משמעותית.

התגובה המוצעת במאמר זה היא אפוא פיתוח של אסטרטגיית אכיפה אלטרנטיבית ומשלימה לאכיפה הפלילית הקלאסית (הפועלת לאיתור מבצע העברה, לחקירתו, להעמדתו לדין במקרים המתאימים, להרשעתו ולענישתו במקרה של הרשעה). האסטרטגיה של אכיפה אלטרנטיבית תוכל להיות אפקטיבית מצד אחד ומתקבלת מבחינה חוקתית מצד שני. יש לאמצה כאסטרטגיה להפחתת פגיעתן של עברות הביטוי ברשת, תוך שמירה על כמה עקרונות יסוד – שקיפות, ביקורת שיפוטית על פעילות האכיפה האלטרנטיבית, הבניית שיקול הדעת המנהלי והשיפוטי בתהליך היישום של אסטרטגיית האכיפה האלטרנטיבית ומיקוד הטיפול המוסדי בתחום רגיש וחדש זה.