

11 במרס 2024

הצעה לקווים מנחים להתמודדות ישראל עם השפעה זרה

במרחב הסייבר והרשתות החברתיות¹

עמית אשכנזי²

תקציר

מאמר זה מציע קווים מנחים למדיניות הגנה ישראלית מפני השפעה זרה במרחב הסייבר. על אף הסיכון הגובר בתחום זה, ובפרט השילוב של לוחמת סייבר עם מבצעי השפעה, טרם גובשה בישראל אסטרטגיה כוללת להתמודדות עם השפעה זרה, ובכלל זה תוכן שקרי או כוזב במרחב הסייבר. טענה מרכזית במאמר היא כי אף שמדובר באתגר ביטחוני, לנוכח מאפייני הפצת תכנים במרחב הסייבר, לא די בפעילות בעלת אופי ביטחוני בלבד מול היריב, ונדרשת פעילות גם מול הזירה בה הוא פועל. המדיניות הנדרשת צריכה להיות הוליסטית הן ברמה התוכנית הן ברמה הארגונית, ולשלב פעילות בתחום הביטחון עם פעילות אסדרה וחברה אזרחית, לקידום החלת כללים המקובלים באיחוד האירופי על מניעת הפצת מידע כוזב. כמקרה בוחן תתואר ההתארגנות המדינתית למניעת השפעה זרה בבחירות לכנסת.

¹ מאמר זה הינו חלק מגיליון הלכה ומעשה העוסק בהשפעה זרה. הגיליון הינו פרויקט משותף של המכון לחקר המתודולוגיה במרכז למורשת המודיעין (המל"מ), משרד המודיעין והמכון למחקרי ביטחון לאומי.

² עמית אשכנזי הוא עורך דין, חוקר ויועץ בתחומי מדיניות, משפט וטכנולוגיה (סייבר, פרטיות, בינה מלאכותית). בשנים 2014–2022 הקים וניהל את המחלקה המשפטית במערך הסייבר הלאומי והיה אחראי למדיניות המשפטית של המערך, ובשנים 2008–2014 הקים וניהל את המחלקה המשפטית של הרשות להגנת הפרטיות. לאחרונה ייעץ עמית למדיניות הבינה המלאכותית שגובשה בידי משרד המדע, ולמיזם UN CTECH של האו"ם. המחבר מבקש להודות לדודי סימן-טוב, ד"ר אסף וינר וד"ר גליה לינדנשטראוס על סיוע והערות למאמר.

מבוא – "השפעה זרה" ו-"התערבות זרה" במרחב הסייבר והצורך באסטרטגיית הגנה

בשנים האחרונות, ובפרט במלחמת "חרבות ברזל" יש עלייה בפעילות בהפצת "מידע כוזב" וניסיונות השפעה זרה באמצעות רשת האינטרנט ורשתות חברתיות הפועלות במרחב הסייבר. בישראל קודמה מדיניות לאומית להגנה בסייבר ברובד הטכנולוגי, מפני תקיפות מחשב כנגד פעילויות חיוניות והגנה על תפקודו התקין של מרחב הסייבר,³ לא קודמה מדיניות כוללת להתמודדות עם לחימה בתחום התוכן, כגון "השפעה זרה" והפצת "מידע כוזב".

מטרת המאמר לתאר בקצרה את האתגרים לקידום מדיניות כזו, את המצב בישראל ובאיחוד האירופי, ולהציע על רקע האמור קווים מנחים לקידום אסטרטגיה כוללת. טענה מרכזית במאמר היא כי אף שמדובר באתגר ביטחוני, לנוכח מאפייני הפצת תכנים במרחב הסייבר, לא די בפעילות בעלת אופי ביטחוני בלבד. המדיניות הנדרשת צריכה להיות הוליסטית הן ברמה התוכנית הן ברמה המוסדית, ולשלב פעילות בתחום הביטחון עם פעילות אסדרה במרחב האזרחי.

המאמר פותח בתיאור המצב הקיים והאתגרים לקידום מדיניות הגנה, ולאחר מכן מציע דרכי התמודדות, בהתבסס גם על עקרונות רלוונטיים מהחקיקה האירופית בתחום הפצת תכנים, שהם עוגן לקוד אתי המקובל על פלטפורמות הפצת התוכן. כמקרה בוחן, תתואר בקצרה ההתארגנות המדינתית למניעת השפעה זרה בבחירות לכנסת. התארגנות זו משקפת חלק מהמרכיבים הנדרשים למיסוד התמודדות עם השפעה זרה – מוסד משפטי בעל לגיטימציה וסמכות, מסגרת משפטית המאפשרת להתאים חובות משפטיות למאפייני זירת התוכן באינטרנט, שימוש בשפה אחידה, ממשקי עבודה שוטפים בין גופים ביטחוניים וגופים אזרחיים, וקביעת ממשקים עם פלטפורמות התוכן. בסוף המאמר המלצות מדיניות קונקרטיים.

³ בעניין תקיפות מחשב במרחב הסייבר, הכוונה לפעילות ברובד הטכנולוגי שמטרתה פגיעה במערכות, כגון תשתיות חיוניות, או ריגול, כגון גנבת מידע.

אתגרי התמודדות עם השפעה זרה, המצב הקיים בישראל והפערים בתחום

מרחב הסייבר, המורכב מרובד טכנולוגי של מחשבים ורשתות, והתכנים המועברים על גביהם, משמש גם "ממד לחימה", מרחב לחימה והשפעה שבמסגרתו מדינות ושחקנים אחרים פועלים לקדם את יעדיהם. למדינות מסוימות יש אסטרטגיה התקפית משולבת הכוללת גם פעילות ברובד התוכן וגם פעילות ברובד הטכנולוגי.⁴

"השפעה זרה", כלומר פעילות של מדינה להשפיע על הנעשה במדינה אחרת, באמצעות רובד התוכן במרחב הסייבר, משקפת איום משמעותי לתפקודו התקין של המשטר הדמוקרטי. באמצעות פעילות ברובד התוכן אפשר להשפיע על דעת הקהל ועל האופן שבו אנשים פועלים ומצביעים בבחירות, ליצור חוסר יציבות פוליטי או ציבורי, להביא לבהלה ולערעור אמון הציבור בשלטון, להפיק יתרונות בהקשר של עימות צבאי ולהשפיע על פעילותם של פוליטיקאים, ארגונים ויחידים. בד בבד יש עלייה בפעילות בהפצת "מידע כוזב" וניסיונות השפעה זרה באמצעות רשת האינטרנט ורשתות חברתיות הפועלות במרחב הסייבר. עקב כך גם ההתמודדות עם לחימה בתחום ה"מידע" - "השפעה זרה" - מחייבת התערבות הגנתית מדינתית.

לצד הצורך הגובר, פיתוח מדיניות לאומית הגנתית בהיבטי התוכן כנגד לוחמת מידע, נעשה על רקע כמה אתגרים ייחודיים:

(1) **הצורך בהמשגה אחידה ל – "השפעה זרה והתערבות זרה"** - לפעילות מדינתית ברובד התוכן במרחב הסייבר - "השפעה זרה" ו"התערבות זרה" - אין הגדרה אחידה הן בספרות הן בתחום המדיניות. מסקירת מאמרים בנושא עולה כי ל"השפעה זרה" המשגות שונות הן מבחינת המטרות והן מבחינת המאפיינים של פעילות זו.

(2) **התערבות מדינתית בתכנים והפצתם, גם אם היא לצורכי הגנה, מעוררת חשש מפני שימוש לרעה בסמכות המדינה, שיפגע בחופש הביטוי, בתנועה חופשית של מידע ובשיח**

⁴ ראו למשל: Google, Fog of war: How the Ukraine conflict transformed the cyber threat landscape, February 2023. <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/>

ראו עוד על אודות ישראל ומלחמת "חרבות ברזל":
Clint Watts - General Manager, Microsoft threat analysis center, Iran accelerates cyber ops against Israel from chaotic start, 06.02.24, <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>

הציבורי. הטיפול בהשפעה זרה ברשת האינטרנט מחדד דילמה מוכרת בשדה סמכויות הביטחון – מה מסוכן יותר: הפעילות של היריב או הסמכויות הנתונות למגן מפניו והסיכון שהוא מייצר לזכויות הפרט? למרות חששות אלה, מדינות רבות החלו בפעילות התמודדות עם התופעה, כפי שיתואר גם בהמשך.

(3) התפתחות תחום זה ללא אסדרה בשונה מהפצת תוכן בשידורי טלוויזיה ורדיו. בשונה

מפלטפורמות הפצת תוכן כמו שידורי טלוויזיה או רדיו, הפלטפורמות שפותחו על גבי האינטרנט אינן נמצאות תחת אסדרה מדינתית בתחום הפצת תכנים. כלומר הפצת תכנים ברשת האינטרנט אינה טעונה רישוי כלשהו ואינה בפיקוח רגולטורי. לצד העושר בייצור ובהפצת תכנים שמבנה זה מאפשר, הוא מאתגר את היכולת המדינתית להנחות את הפלטפורמות להגביל או לצמצם את ההפצה של תוכן פוגע או אסור, בשונה מהמודלים המקובלים ביחס לאסדרה על תכנים בתחום הטלוויזיה והרדיו. נוסף על כך במדינות רבות צומצמה מאוד האפשרות להטיל על הפלטפורמות אחריות משפטית גם בדיעבד לתכנים המופצים על ידן,⁵ וגם זאת בשונה מהכללים החלים על מפיצי מידע מחוץ למרחב הסייבר.⁶

(4) הכללים המשפטיים המרכזיים החלים על הפצת תכנים המופצים במרחב הסייבר, ברשת

האינטרנט וברשתות חברתיות, נקבעים ונאכפים ברובם על ידי הפלטפורמות עצמן, במסגרת "תנאי השימוש" שלהן. "תנאי השימוש" הם הסדר חוזי - המנוסח בידי הפלטפורמה - עם המשתמשים השונים, שיכולים להיות "דוברים", "מפיצים", "נמענים" ועוד. הפלטפורמות קובעות "מדיניות שימוש" ובמסגרת זו מגדירות את התכנים המותרים והאסורים, בהתאם למדיניות העסקית שלהן, שאינה בהכרח זהה לאופן שבו דין מדינתי או

⁵ בתמצית, בשנת 1996 נקבע בארה"ב סעיף 230 ל-communication Decency Act, שקבע פטור נרחב מאוד לגורמי ביניים, המפיצים תכנים של אחרים, לחבות בגין תכנים אלה. Goldman, Eric, The ten most important section 230 Rulings (August 1, 2017). Available at SSRN: <https://ssrn.com/abstract=3025943>, Santa Clara Univ. Legal Studies Research Paper, Vol. 20, 2017.

⁶ הנימוק המרכזי להסדרים אלה הוא הרצון לאפשר תנועה חופשית של מידע, והטענה כי לנוכח כמויות התוכן המופץ באמצעות פלטפורמות אלה אין להן יכולת ריאלית לנטר אותן. עקב כך, הטלת חובות ניטור או בדיקה יזומים של תוכן עליהן תביא למצב של "צנזורה". ראו בעניין זה: ע"א 5977/07 שוקן נגד האוניברסיטה העברית, ניבה אלקין קורן רוטר, המתווכים החדשים "בכיכר השוק" הווירטואלית, משפט וממשל (ו), 381.

ועדת דויד, סיכום עבודת הוועדה להתאמת המשפט לאתגרי החדשנות והאצת הטכנולוגיה, בנושא תכנים לא חוקיים במרחב הדיגיטלי, <https://www.gov.il/he/Departments/Guides/davidi-committee-main?chapterIndex=12>

בין לאומי מגדיר זאת. יוצא דופן מרכזי הוא ההסדרה בתחום הפרטיות במידע, אולם הסדרה זו אינה עוסקת במכלול ההיבטים הקשורים במנגנונים שתוארו.

(5) אקוסיסטם עשיר בדרכי הפצת מידע כמעט ללא פיקוח. בסביבה המשפטית המאפשרת שתוארה לעיל, התפתח אקוסיסטם הפצת מידע עשיר, הכולל מגוון רחב של אינטראקציות בין המשתמש-הדובר, המשתמש-הנמען והאלגוריתמים השונים של הפלטפורמות - כמעט ללא פיקוח משפטי-רגולטורי. מנגנוני הפצה מתוחכמים אלה, הכוללים פרסום בתשלום, יכולת לסמן תוכן, לשתף תוכן, להוסיף האשטאג ועוד, מכילים בהתאם לאינטרסים של הפלטפורמות - להגדיל צפיות ותשומת לב של המשתמש. במציאות הטכנולוגית והחברתית שהתפתחה, קיים מתח קבוע בין הרצון של הפלטפורמה לעודד תנועה של גולשים ומעורבות בתכנים, משיקולים מסחריים, לבין שיקולים אתיים הקשורים בסוג התוכן המופץ. אקוסיסטם עשיר ודינמי זה, ובפרט כיוול האלגוריתמים השונים של הפלטפורמות, הוא סוד מסחרי של הפלטפורמה ואינו ידוע לציבור.

(6) התכנים במרחב הסייבר - מופצים באופן גלובלי ומיידי לעשרות מדינות שונות לפחות על ידי תאגידים רב־לאומיים שיכולת ההשפעה של הדין הישראלי או שוק המשתמשים הישראלי על מדיניות התוכן שלהם מוגבלת מאוד ותלויה במידה רבה של שיתוף פעולה בין רשויות מדינתיות לתאגידי הטכנולוגיה. כפועל יוצא מכך עולה חשש מעשי, בפרט במדינות קטנות בעלות שפה ייחודית כמו ישראל, שניסיונות התערבות משפטיים "מקומיים" של מדינה אחת, יהיו לא אפקטיביים. תופעה זו הופכת מורכבת ומשמעותית יותר לנוכח המקום המרכזי של הפלטפורמות בהפצת מידע שהציבור הרחב צורך. בפרט יש פער משמעותי בין העושר של אקוסיסטם המידע במרחב הסייבר, התמריצים הכלכליים החלים בו והתפקיד המרכזי שלו בזירת השיח הציבורי, לבין הכלים המשפטיים המאפשרים להתערב בפעילות זו לצורך הגנה על אינטרסים ציבוריים במסגרתו.⁷ יודגש כי גם כיום הפלטפורמות עוסקות בהסרת תוכן מזויף או פוגעני, אולם השיקול הראשון המנחה אותן הוא שמירה על סביבה הולמת למשתמשים כדי לעודד אותם להשתמש בפלטפורמה.

⁷ כבר בשנת 2004 עמדה על כך פרופסור ניבה אלקין קורן במאמרה המתווכים החדשים בכיכר העיר.

המדיניות הביטחונית הציבורית בישראל בתחום זה מבטאת מורכבות זו. אף שלגופי הביטחון ואכיפת החוק פעילות הגנתית במרחב הסייבר, כולל מול תכנים פוגעניים מסוגים שונים, דומה כי אין אסטרטגיה כוללת לטיפול בסוגיה זו, בפרט בתחום סמכויות המדינה להתערב בהפצת תכנים במרחב הסייבר.

בהיבט הביטחוני-אסטרטגי אין כיום בישראל הגדרה מוסכמת או שפה משותפת לגבי הגדרת השפעה זרה, ומה הן הנגזרות שלה במרחב הסייבר. לפיכך הטיפול כיום בהשפעה זרה הוא חלקי. לא הוגדר גוף מתכלל לקידום המדיניות ולסנכרון הפעילות אף שאפשר להצביע על פעילות של שירות הביטחון הכללי, הפרקליטות ומערך הסייבר הלאומי כנגד מופעים של ניסיונות התערבות זרה או פעילות עוינת בהיבטי תוכן במרחב הסייבר-אינטרנט. פער זה הוא בניגוד להיערכות הלאומית להגנת הסייבר במישור הטכנולוגי אשר הוגדרה בסדרת החלטות מדיניות של הממשלה ובחיקה.⁸

בכל הקשור לסמכות לפעול למול מופעים של השפעה זרה ברשת האינטרנט, לרשויות המדינה סמכויות מוגבלות מאוד. סמכויות אלה ממוקדות בעיקר בהסרת תכנים בדיעבד מול ספקיות התקשורת המקומיות,⁹ לאחר שאותרו בידי גופי הביטחון והאכיפה. בכל הקשור לרשתות חברתיות, שפעילותן אינה טעונה רישיון לפי דיני התקשורת, ואשר הן גורם משמעותי מאוד בהפצת תכנים במרחב הסייבר-אינטרנט, ההסדר החל בישראל הוא וולונטרי בלבד. נוסף על כך עיקר הפעילות המשפטית של המדינה ממוקדת בתכנים המהווים הסתה לאלימות, כלומר תכנים שבהגדרה אפשר לזקוף אותם לגורם עויני.¹⁰ למרות החשיבות הביטחונית של פעילות זו במניעת

⁸ ראו: החלטת ממשלה 3611 מיום 07.08.2011, "קידום היכולת הלאומית במרחב הקיברנטי", https://www.gov.il/he/departments/policies/2011_des3611; החלטת הממשלה 2444 מיום 15.02.15, "קידום ההיערכות הלאומית להגנת הסייבר", https://www.gov.il/he/departments/policies/2015_des2444; החלטת הממשלה 2443 מיום 15.02.15, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", https://www.gov.il/he/departments/policies/2015_des2443; החלטת ממשלה 219 מיום 01.08.2019, "בחירת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה בתוך שקילת שיקולים כלכליים", https://www.gov.il/he/departments/policies/dec219_2021; חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998; חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023.

⁹ ראו חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע"ז-2017.
¹⁰ ראו דוח איגוד האינטרנט על פעילות מחלקת הסייבר בפרקליטות המדינה, איגוד האינטרנט, פעילות מחלקת הסייבר בפרקליטות להסרת תכנים מרשתות חברתיות: מגמות ונתוני עומק (אוקטובר 2023), <https://www.isoc.org.il/regulating-digital-services/israel/voluntary-content-removal-trends>

המשך הסתה ואסקלציה, היא נותנת מענה חלקי בלבד לאיום הביטחוני הנשקף מהשפעה זרה משום שאינה עוסקת במישרין בתכנים המבקשים להסתוות בשיח הלגיטימי וב"מידע כוזב".

תמונת המצב המבצעית והמשפטית בעניין משתקפת בפסק הדין של בית המשפט העליון בעתירת ארגון עדאלה שבו נדונה שאלת סמכותה של המדינה להודיע לפלטפורמות התוכן על כך שהן מפיצות או מנגישות תוכן אסור, כגון הסתה לפעילות טרור. מאחר שאין חקיקה ספציפית הקובעת את אופן פעולת המדינה בנושא זה, ארגון עדאלה מיקד את העתירה בטענה כי פעילות זו הינה בחוסר סמכות, משום שיש בה פגיעה בחופש הביטוי, ופגיעה בזו טעונה הסדרה בחקיקה ראשית.

בתגובתה הציגה המדינה את אופן פעולתה. מדובר במקרים שבהם פרקליטות המדינה בחנה תוכן מסוים, והגיעה למסקנה כי יש בסיס לקביעה כי התוכן מהווה עבירה פלילית לפי הדין הישראלי.¹¹ בשונה מאופן הפעולה הרגיל של העמדה לדין בגין התוכן, ולנוכח קשיי האכיפה הכרוכים בכך, פיתחה הפרקליטות תפיסה שלפיה היא מבקשת מהפלטפורמה "להסיר" את התוכן, כדי למנוע את המשך ביצוע העבירה באמצעות החשיפה לתוכן זה, ולצמצם את השפעתו והנזק ממנו. המדינה הדגישה כי היא פונה לפלטפורמות בבקשות הסרה של תוכן, רק אם נוסף על כך התוכן מפר את תנאי השימוש של הפלטפורמה.¹² בהתאם לעמדה זו, המדינה בסך הכול "מודיעה" לפלטפורמה שיש תוכן המפר את תנאי השימוש של הפלטפורמה ויש להסירו. עקב כך, לעמדת המדינה היא אינה מפעילה סמכות כופה אלא פועלת בהתאם לתנאי השימוש של הפלטפורמה. עמדה זו מחדדת את המצב המשפטי החסר שבו גם אם רשויות התביעה הכללית

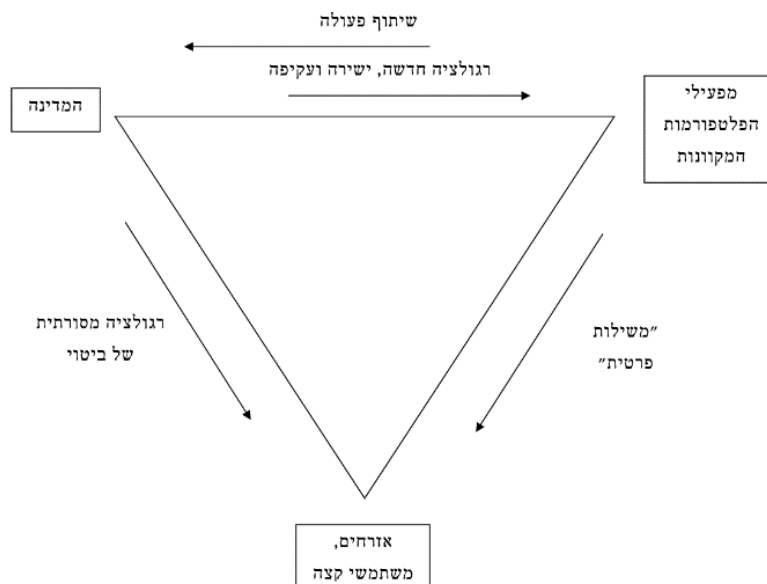
לפי הפרסום בשנת 2020 הוגשו לפלטפורמות 1199 בקשות בתחום ההסתה לאלימות, ו-101 בקשות בתחום "מידע כוזב". דומה כי גם בפעילות הענפה של מחלקת הסייבר במלחמת "חרבות ברזל" המוקד הוא הסרת תכנים ופרסומים אסורים המהווים הסתה לאלימות או לטרור. כלומר מדובר בתכנים שאפשר לקבוע בנוגע אליהם אי-חוקיות מובהקת. ראו: פרקליטות המדינה, דשבורד פעילות מחלקת הסייבר בפרקליטות המדינה בתחום הסרת תכני טרור, הסתה ותכנים בלתי חוקיים ברשת, <https://www.gov.il/he/Departments/General/cyber-dashboard>

¹¹ התגובה הרגילה של מערכת אכיפת החוק היא העמדה לדין של הדובר, אך בשל מאפייני השיח ברשת אי אפשר להגיש כתב אישום כנגד הדובר כי הוא אינו ידוע או נמצא במדינה אחרת.

¹² בעת כתיבת שורות אלה מתנהל בארה"ב דיון דומה שבו ערכאה מחוזית קיבלה עתירה דומה כנגד המדינה, וביקשה למנוע ממנה להודיע על הפרות לכאורה לרשתות החברתיות. עד 20.10.23 עיכב בית המשפט העליון האמריקני את מימוש הצו. מבלי להתעמק בכל ההבדלים בין ההליכים, מעניין לציין את מגוון הגורמים השלטוניים העומדים בקשר עם הפלטפורמות בנושא זה. בישראל, לעומת זאת, יש תפיסה ריכוזית שלפיה בנושא רגיש זה יש גורם קשר אחד עם הפלטפורמות, ודומה כי יש לכך יתרונות משמעותיים.

Amy Howe, Justices allow federal government continued communication over social media content moderation, SCOTUSblog, 20.10.23, <https://www.scotusblog.com/2023/10/justices-allow-federal-government-continued-communication-over-social-media-content-moderation/>

סבורות שתוכן מסוים מפר את הדין בישראל, הן נדרשות להוכיח לפלטפורמות כי התכנים מפירים גם את "תנאי השימוש", שאינו דין מדינתי אלא הסדר משפטי שנקבע בידי חברה פרטית. במסגרת פסק הדין דן בית המשפט בחשש מפני "צנזורה" ומחדד, בין היתר, כי אין הצדקה להגן על חופש הביטוי של "בוטים" וירטואליים. בכך, הטענה בדבר פגיעה בחופש הביטוי שעומדת כחלק משמעותי מהעתירה מוצגת בתוך ההקשר הכללי. קביעה זו של בית המשפט מסייעת לאפיין את עיסוק המדינה במניעת השפעה זרה והפצת תכנים פוגעניים. מקביעתו של בית המשפט גם אפשר לומר כי כדי להגן על חופש הביטוי במרחב הסייבר וכדי להגן על שיח ציבורי אמיתי, נדרשת פעולת הגנה של המדינה, בכלים שונים. פסק הדין גם עוסק במערכת היחסים שבין המשפט המדינתי, כלומר הדין החל בישראל, לבין כללי ההתנהגות שקובעות הפלטפורמות שהן אמצעי הפצה מרכזי. השופט מלצר מדגים זאת באמצעות תרשים המבוסס על מחקר חשוב של פרופסור ג'ק בלקין (Jack Balkin) מאוניברסיטת ייל.



כפי שעולה בצורה ברורה בתרשים זה, שמופיע בפסק הדין בהקשר של הסרת תכנים, פרקליטות המדינה ובית המשפט מכירים בכך שעל מרחב משמעותי של ביטוי במרחב הסייבר, המופיע בצד ימין של התרשים, חלה "משילות פרטית". "משילות פרטית" זו היא למעשה הפרקטיקות המסחריות, הטכנולוגיות וההסדרים המשפטיים בעניין הפצת תכנים, אופן הפיקוח על רישום משתמשים ואופן הפיקוח על הפצת תכנים, שנכתבים ונאכפים בידי הפלטפורמות עצמן.

עקב כך, בעניין עדאלה הכיר בית המשפט העליון דה־פקטו במעמדה המשפטי של "משילות פרטית" זו.¹³ התוצאה המעשית היא שעמדתה המשפטית של פרקליטות המדינה ביחס לקיומה של עבירה פלילית בהפצת תכנים, בהתאם לדין המדינתי, נסוג בפועל מפני ה"משילות הפרטית" שקובעת הפלטפורמה. עמדות אלה משקפות הגנה עוצמתית מאוד על חופש הביטוי בפלטפורמות, אך מעוררות אתגר כאשר המדינה מבקשת להגן על האינטרס הציבורי במרחב זה. בשנים 2017–2018 קידמו הממשלה והכנסת חקיקה שמטרתה הסדרת חסימת תכנים ברשת האינטרנט.¹⁴ מטרת החקיקה הייתה לאפשר לפרקליטות ולבית המשפט לפעול להסרת תכנים, **שלא על בסיס וולונטרי**. הצעת החוק כללה עילות להסרת תכנים וכן את ההליך לביצוע ההסרה. ההצעה אינה מגדירה בצורה ישירה "השפעה זרה" או "מידע כוזב", אולם אפשר להניח כי חלק מהתכנים המהווים "השפעה זרה" במרחב הסייבר מקיימים עילה לבקשת הסרה לפי החוק.¹⁵ הצעת החוק לא אושרה לבסוף. חשוב גם להדגיש כי ההצעה ממוקדת רק בהסרת תוכן בדיעבד, כלומר ביכולת של המדינה לפנות ולבקש, לאחר שתוכן מסוים הופץ, את הסרתו. **ההצעה אינה עוסקת כלל בשאלה מה היכולת, ובהתאמה - מה החובה, של הפלטפורמה לצמצם או לאתר מראש תכנים פוגעניים**. ההצעה משאירה נושא זה ל"משילות פרטית" של הפלטפורמה. בכך גם הצעת החוק הממשלתית שקודמה בנושא זה נשענת במידה רבה על משילות פרטית של הפלטפורמות.

לסיכום, המצב המשפטי הנוכחי אינו מאפשר יישום אפקטיבי של מדיניות התמודדות עם השפעה זרה משום שבהתאם למצב המשפטי הקיים, יישום המדיניות תלוי בכך שפעולות ההשפעה הזרה מהוות גם הפרה של תנאי השימוש, כפי שהן מתפרשות ונאכפות בידי הפלטפורמות. נוסף על

¹³ אף שבהקשרים אחרים מתח בית המשפט העליון ביקורת על המסגרת המשפטית החוזית המסדירה את פעולת הפלטפורמות. למשל: ת"צ 46065-09-14 בן חמו נגד פייסבוק, (תיק חיצוני רע"א 5860/16), החלטה מיום 05.07.23, רע"א 1901/20 טרויס מילר נגד limited facebook Ireland.

¹⁴ הצעת החוק הממשלתית: הצעת חוק להסרת תוכן שפרסומו מהווה עבירה מרשת האינטרנט, התשע"ז-2016, הצעת חוק הממשלה 28.12.16, 1104.

<https://main.knesset.gov.il/activity/legislation/laws/pages/lawbill.aspx?t=lawsuggestionssearch&lawitemid=2011567>

¹⁵ בהתאם לנוסח שהוכן לקראת קריאה שנייה ושלישית, הוצע הסעיף הזה: "שופט בית המשפט המחוזי שנשיא בית המשפט המחוזי הסמיכו לכך רשאי, על פי בקשה של תובע, לתת צו המחייב מפרסם תוכן, או בעלים, מנהל או מפעיל של אתר אינטרנט שבו פורסם תוכן, להסיר את התוכן מאתר האינטרנט, אם שוכנע כי נעברה עבירה פלילית באמצעות פרסום התוכן באתר האינטרנט, וכי בנסיבות העניין יש אפשרות ממשית שהמשך הפרסום כאמור יפגע בביטחונו של אדם מסוים או בלתי מסוים או בביטחון המדינה, או יביא לפגיעה חמורה בכלכלת המדינה או בתשתיות חיוניות בחוק זה צו להסרת – תוכן". (ההדגשה שלי, ע"א). אפשר להניח שהפצה של תוכן בידי גורם עוין זר לצורכי השפעה תעמוד בתנאים אלה.

כך גם אם הייתה מחוקקת הצעת החוק הממשלתית שקודמה בנושא זה, היא לא הייתה פותרת את כל הפערים משום שהיא ממוקדת באכיפה בדיעבד בלבד, ובכך אינה עוסקת כלל בשאלה של התפקיד האקטיבי של הרשתות החברתיות בהפצת תוכן כוזב. ברמה המבצעית המעשית, על אף הפעילות העצומה של פרקליטות הסייבר בהסרת תכנים, פעילות זו היא בהיקף קטן לאין שיעור מהתכנים שמופצים בפלטפורמות וגם בהשוואה לפעילות ההסרה של הפלטפורמות עצמן.

היערכות מדינתית כנגד השפעה זרה ותכנים כוזבים ברשת לנוכח עליית האיומים והסיכונים, נדרש גורם ממשלתי מתכלל שיוביל גיבוש מדיניות כוללת, שתסייע בהכוונת היערכות, ההתמודדות וההכלה של ניסיונות השפעה זרה ושימוש בתכנים כוזבים. גיבוש מדיניות כוללת שיש בה המשגה מסודרת וחלוקת תפקידים, יאפשר להיערך להתמודדות עם ההשפעה הזרה בהקשר הרחב וכחלק ממכלול הצעדים של היריב, הגדרת האיום והמערכה נגדו. הגדרה ברורה מאפשרת למקד את מאמצי ההתערבות כדי לסכל את פעילות היריב ולעצב הסדרים משפטיים שיתמודדו עם החששות מפני התערבות בחופש הביטוי, כלומר באופן שחותר להשיג את היעד הביטחוני המוגדר בתוך צמצום החשש לפגיעה שעולה על הנדרש. היא גם מאפשרת לקבוע את המסגרת לפעילות זו בהתאם למאפייני הפעילות במרחב הסייבר, לאחר בחינת הסיכונים לזכויות יסוד ואינטרסים ציבוריים ממאמצים אלה ואופן ההתמודדות עם סיכונים אלה.

(1) הצורך במדיניות הוליסטית לקידום מדיניות כנגד "השפעה זרה", "התערבות זרה" ותכנים

כוזבים במרחב הסייבר

כדי להתמודד באופן אפקטיבי עם השפעה זרה במרחב הסייבר, נדרשת מדיניות הוליסטית, המשלבת לצד מדיניות אסטרטגית-ביטחונית גם מדיניות משפטית-טכנולוגית העוסקת באופן שבו משפיעים על מנגנוני הפצת התכנים במרחב הסייבר.

נקודת המבט האסטרטגית בוחנת את ה"השפעה זרה" בזירת הסייבר כחלק מהמטרות, האמצעים והכלים של היריב בתחום ההשפעה הזרה באופן כללי. נקודת המבט הטכנו-משפטית

בוחנת את זירת הפעולה, את מרחב הסייבר ואת המאפיינים הייחודיים של ייצור, הפצה ואסדרה של תכנים בזירת הסייבר, ובהתאמה מניעת הפצה של תכנים מזיקים בו. שילוב נקודות מבט אלה מאפשר להגדיר כיצד השפעה זרה באה לידי ביטוי במרחב הסייבר, מה הם הכלים הקיימים והנדרשים בידי המדינה להתמודדות איתה, וכיצד אפשר לאזן בין הצורך הביטחוני לבין החשש מפני התערבות של המדינה בתכנים.

(2) מבט ביטחוני-אסטרטגי: הגדרות ושפה משותפת על איומי השפעה זרה והתערבות זרה

התמודדות עם תופעה, ובהתאמה בניין כוח והפעלת אמצעים כנגדה, מחייבת הבנה של מטרותיה ותיאור מאפייניה. מכאן עולה החשיבות להגדרה ברורה של מהי "השפעה זרה" המהווה שפה משותפת לגופים הרלוונטיים בהמשגת האיום, ובהתאמה לכך מאפשרת עיצוב הסדרים מתאימים.

עופר פרידמן מציע להתבונן על "השפעה זרה" כחלק ממכלול האמצעים ששחקן בין-לאומי עושה כדי להשפיע על שחקן בין-לאומי אחר בזירה הבין-לאומית. על רקע זה הוא מגדיר "השפעה זרה" כשימוש בכל המקורות הזמינים של עוצמה לאומית (דיפלומטיים, מידעיים, צבאיים, כלכליים, דתיים וכולי), על ידי שחקן בין-לאומי אחד כדי להשפיע על שחקן אחר, במטרה להשיג יעד פוליטי". בהמשך לכך מגדיר פרידמן "התערבות זרה" ("foreign interference") כסוג מסוים של השפעה זרה.¹⁶ לפי גישה זו, "השפעה זרה" (foreign influence) תיחשב התערבות זרה (foreign interference) כאשר השימוש של שחקן אחד בעוצמה לאומית כדי להשפיע שחקן אחר נחשב על ידי השחקן האחר כמנוגד לערכים, לנורמות או לחוקים שלו. בהקשרי תכנים, ובפרט במרחב הסייבר, מאפיין מרכזי של השפעה זרה הוא באופן שהיא נעשית בו - שנועד להסוות את מקורה ולהיראות כמידע אותנטי שהוא חלק מהשיח הציבורי הלגיטימי. פעמים רבות השפעה זרה באה לידי ביטוי במרחב הסייבר על ידי "מידע כוזב". כלומר מידע שאינו נכון או שהדובר שייצר אותו מתחזה להיות אחר או שהוא פיקטיבי.

¹⁶ עופר פרידמן, "השפעה והתערבות זרה – המשגה ומונחים", פירסום מיוחד, 2 בינואר 2024, המכון למחרי ביטחון לאומי והמכון לחקר המתודולוגיה של המודיעין. [/ https://www.inss.org.il/he/publication/influence-and-interference](https://www.inss.org.il/he/publication/influence-and-interference)

המבט הרחב שמציע פרידמן על "התערבות זרה" כשימוש בעוצמה לאומית כדי להשפיע על שחקן בין-לאומי אחר באופן המנוגד לערכים, נורמות או חוקים שלו, מסייע להערכת היעדים של מדינות יריבות, ובהתאמה - הערכה של האמצעים שבהם ייעשה שימוש גם בפעילות בתחום המידע במרחב הסייבר. כך אפשר להעריך כי לעיתים הרכיב של לוחמת המידע בפעילות יהיה הדומיננטי, כגון בהפצת מידע שמטרתו ערעור אמון הציבור במוסדות השלטון או יצירת חוסר יציבות חברתי, ולעיתים רכיב המידע יהיה רכיב תומך במכלול האמצעים האחרים. במילים אחרות, האופן שבו היריב ירצה להפעיל השפעה בזירת הסייבר צריך להיבחן בפריזמה הרחבה של מטרותיו וכלים אחרים העומדים לרשותו. כך למשל, אם למדינה מסוימת עניין בהשגת השפעה על פעילותה של מדינה אחרת באמצעות הזירה הכלכלית (למשל, באמצעות השקעה בפעילויות כלכליות אסטרטגיות), אפשר להניח כי תפעל גם בזירת הסייבר לקדם מסרים המסייעים לפעילותה זו.

לסיכום נקודה זו, מאחר שהאיום הוא אסטרטגי וביטחוני, נדרשת המשגה משותפת אחידה כלל-מערכתית בנושא זה. בתוך שילוב גופי המחקר המודיעיניים השונים, בהיבט האסטרטגי. עוד נראה כי נדרש תכלול מדינתי לגבי אופן פעולת היריב במרחב הסייבר במסגרת מכלול האמצעים העומדים לרשותו. תכלול זה מאפשר היערכות לסוג הפעילות הצפוי ודרכים לאיתורה. במישור המבצעי, גופי הביטחון אמונים על זיהוי האיומים, התמודדות איתם וסיכולם, ודומה כי האופן שבו נושא זה פועל בישראל ממוסד היטב.

לצד גיבוש ההמשגה והטלת התפקידים על הגופים השונים, יש לקדם את החקיקה המאפשרת למדינה לפנות בבקשה להסרת תכנים, כדי להקנות סמכות מסודרת לגופי הביטחון, באמצעות פרקליטות המדינה, לפנות במקרים המתאימים ולהסיר תכנים, גם במקרים שהתכנים אינם מפירים את "תנאי השימוש" של הפלטפורמות. כמו כן יש לבחון האם חקיקה זו מקנה כלים מספקים להסרת תכנים אסורים מסוג "מידע כוזב".

(3) הצורך בגישה הוליסטית – הממשק בין המערכת הביטחונית למערכת האזרחית

כדי להתמודד כראוי עם אתגרי ההשפעה הזרה, אי־אפשר להסתפק בגיבוש אסטרטגיה והמשגה מדינתית בנושא ובהסדרת הסמכויות לפעול **לאחר שתוכן מופץ**, ונדרשת הסדרה ברובד נוסף, המגביר את האחריותיות של הפלטפורמות לפעולות **למניעת הפצת מידע כוזב**.

כפי שהוצג לעיל, פעילות אכיפה ביטחונית של המדינה מול הפצת תכנים אינה מספקת משום שהיא נעשית בדיעבד, ואינה מסוגלת להתמודד עם שטף המידע המופץ ברשתות. כך, כדי להשפיע על אופן הפצת התכנים בפועל, נדרש להשפיע על ה"משילות הפרטית" במובנים מהותיים יותר, באופן שישפיע על הפלטפורמות בפעולות שהן מסוגלות לזהות ולמנוע, ולנקוט אמצעים של מניעה מראש. לנוכח כמות התוכן המופץ בפלטפורמות, קשה לגופי הביטחון לנטר את כולו ולהורות על הסרתו. כבר כיום יש הבדל משמעותי בכמות התוכן שמזהות הפלטפורמות בעצמן ומסירות, בהתאם למדיניות העצמית שלהן, שהוא גדול בהרבה מבקשות ההסרה, לבין בקשות ההסרה של אותו סוג תוכן מטעם המדינה.

כדי ליישם באופן אפקטיבי את המדיניות למניעת שימוש לרעה בפלטפורמות נדרשת קביעת כללים המטילים על הפלטפורמות חובות למנוע שימוש לרעה בהן. פעילות מעין זו היא קריטית להגנה על הזירה הציבורית ובסופו של דבר על היכולת לממש את חופש הביטוי בזירת המקוונת. עם זאת, קביעת כללים ופיקוח עליהם בתחום זה אינם מתאימים לגופי הביטחון.¹⁷ בזירת האינטרנט מתנהל חלק משמעותי מהשיח הציבורי הדמוקרטי המודרני. במישור המבצעי, גופי הביטחון פועלים באופן כללי בצורה חשאית, הם אינם מומחים לאסדרת המרחב האזרחי, ועלולים להימצא בניגודי עניינים בתחומים אלה. מכאן עולה כי כחלק ממדיניות הוליסטית נדרשת - לצד הפעילות הביטחונית המובהקת המכוונת ליריב - הוספה של אסדרה אזרחית המופנית אל הזירה שבה הוא פועל.

¹⁷ ראו למשל את דבריו של בית המשפט העליון בעניין הסמכת ש"כ לסייע באיכוני נדבקים בקורונה, בג"צ 2109/20, שחר בן מאיר ואחי נגד ראש הממשלה.

תשתית אזרחית להתמודדות עם השפעה זרה באמצעות אחריותיות של הפלטפורמות בישראל

(1) קידום קומה אזרחית להתמודדות עם השפעה זרה - אחריותיות של הפלטפורמות בישראל,

בתוך שימוש בתקדים האירופי

מהפרק הקודם עולה הצורך בקידום אסדרה אזרחית העוסקת באופן ההפצה של תכנים ברשתות חברתיות. העיסוק באסדרה של תכנים ברשתות חברתיות הוא רחב מההקשר הנוכחי של השפעה זרה, אולם כפי שתואר לעיל, הוא חיוני כדי לאפשר יישום אפקטיבי של אסטרטגיה להגנה מפני השפעה זרה. באיחוד האירופי פותחה חקיקה שמטרתה הגברת האחריותיות וניהול הסיכונים של הרשתות החברתיות באופן אפקטיבי, ולא רק תגובה בדיעבד על פניות המדינה, ה־ Digital Services Act.¹⁸ חקיקה זו היא דגם לאסדרה שנקבעה בהתאם לתפיסה חוקתית המגינה על חופש הביטוי, אבל מבקשת למנוע ניצול לרעה. המטרה של חקיקה זו היא גיבוש כללי התנהגות **מחייבים** המצפים מה"משילות הפרטית" של הפלטפורמות לשקף בצורה טובה יותר את האינטרסים הציבוריים.

סוגיית האסדרה של פלטפורמות בישראל בעניין תכנים פוגעניים נדונה לאחרונה בוועדה בראשות מנכ"לית משרד התקשורת לירן בן חורין.¹⁹ מסקנת הוועדה הייתה כי **נדרש שינוי מהותי במדיניות הציבורית כלפי הפלטפורמות בתחום התכנים**. הניסיון המצטבר הוא שהשארית מדיניות התכנים לשיקול הדעת המלא והבלעדי של הפלטפורמות אינה מקדמת בהכרח את חופש הביטוי או מאזנת בצורה מקובלת ציבורית בין חופש הביטוי לבין ערכים אחרים. דוח בן חורין דן ב־ Digital Services Act ובהסדרים שיש בו כדי להתמודד עם האתגרים הייחודיים של הפצת תוכן בפלטפורמות השונות.²⁰ מבין הסדרים אלה הוועדה מציעה להטיל חובה על הפלטפורמות לנהל

European Commission, The digital services act package, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. לסקירה בהקשר הישראלי ראו: **ד"ר תהילה שורץ אלטשולר**, ד"ר אסף וינר, אייל זילברמן, מתווה לאסדרת רשתות חברתיות בישראל, המכון הישראלי לדמוקרטיה ואיגוד האינטרנט, 2023, <https://www.idi.org.il/books/49130>.

¹⁹ משרד התקשורת, **דוח הצוות המייעץ לשר התקשורת לבחינת האסדרה על פלטפורמות תוכן דיגיטליות**, 14.12.2022, <https://www.gov.il/he/Departments/publications/reports/14122022>.

²⁰ European Commission, The digital services act package, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

סיכונים כנגד שימוש לרעה בפלטפורמה, בדרך של הפצת תכנים מזויפים או פוגעניים. כלל זה מבטא את הציפייה כי הפלטפורמה תביא בחשבון לצד השיקולים העסקיים הטהורים שלה, תופעות לוואי הנובעות מהפצה נרחבת של תכנים פוגעניים.

מדוח בן חורין עולה מסקנה חשובה לגבי אופן ההתמודדות הממשלתי בנושא זה. כדי להגן מפני השפעה זרה, נדרש לייצר קומה אזרחית לגבי משילות התוכן בפלטפורמות. קומה זו תשלים את הפעילות שיש למסד של פרקליטות המדינה למול הפלטפורמות בהסרת תכנים. אכן, נדרשת זהירות מופלגת בכניסה של המדינה לתחום זה. אולם לנוכח האיום של השפעה זרה, קיומה של תשתית כזו הוא חיוני. באופן מעשי אפשר להעריך כי ככל שהשיח ימוסד והפלטפורמות יטפלו באופן ראוי בתכנים מזיקים, אפשר יהיה ביתר קלות למנוע הפצה של תכנים מזיקים שמטרתם השפעה זרה, וכן לאתר תכנים כאלה.

בהקשר הרלוונטי להפצת תכנים פוגעניים, עקרון החובה לניהול סיכונים ב־ Digital Services Act הוא בסיס ל־Code of Practice on Disinformation²¹. הקוד גובש בתהליך ממושך מול הפלטפורמות באופן וולונטרי, ועתה הוא מחייב פלטפורמות גדולות מאוד. הקוד כולל המשגה מפורטת לגבי אופן הפצת תכנים ברשתות חברתיות, באופן שמאפשר בסיס משותף ליצירת חובות התנהגותיות. כלומר הקוד מבקש לתאר בשפה משפטית את השיטות השונות שבהן מידע מופץ בידי הפלטפורמות, ולהציב ציפיות לגבי אופן ההתמודדות שלהן עם שימוש לרעה. ההסדר מצביע על סדרת דרישות התנהגותיות המכבדות את חופש הביטוי אולם מצפות לאחריותיות מצד הפלטפורמות ושחקנים נוספים כדי לצמצם את החשש לשימוש לרעה. הסדר זה לא הוכתב באופן חד־צדדי בידי המחוקק אלא פותח עם הפלטפורמות, בשים לב למאפיינים הייחודיים לפעילותם.

הטלת חובות בעניין חיזוק משתמשים, קהילת המחקר וקהילת "בודקי העובדות", מסייעת בהגנה על חופש הביטוי בתוך צמצום ההתערבות החיצונית בתוכן. לצד זאת, הקוד כולל אמצעים

European Commission, The 2022 code of practice on disinformation, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> ²¹

לאכיפת ההתחייבויות באמצעות מרכז שקיפות, צוות משימה קבוע, ואכיפה של הקוד.²² הסדר זה הוא דגם שאפשר לעשות בו שימוש באופן מיידי בישראל כדי לסייע בהתמודדות עם השפעה זרה ומידע כוזב. מאחר שמדובר בהסדר מפורט שגובש שנים ארוכות עם הפלטפורמות הגדולות, הוא משקף את כללי התנהגות המקובלים עליהן. על כן מוצע לקדם את ההחלה בישראל של ההסדר האירופי המטיל חובה לנהל סיכונים, בשלב ראשון בפלטפורמות שנקבעו כ"פלטפורמות גדולות מאוד",²³ ובתוך הפניה לקוד למניעת הפצת מידע כוזב.

להתבססות על ההסדר האירופי בשלב ראשון יש כמה יתרונות. היתרון הראשון הוא שההסדר משמש "קיצור דרך" ליצירת שיח משותף על מניעת הפצת תכנים בפלטפורמות, כי הוא מציב את אבני הבניין המרכזיות. יתרון שני הוא החשיבות של התאמת ההסדרים בישראל לכללים המתהווים בעולם ברמה האסדרתית. יתרון שלישי הוא שאימוץ ההסדר כפי שהוא, בשלב ראשון, מתגבר על החשש שהשיח הציבורי המקוטב בישראל יוביל להסדרה שתוצאתה פגיעה בחופש הביטוי, בפרט לנוכח האיומים המשמעותיים שהושמעו לאחרונה על עקרונות יסוד של שלטון החוק, והרצון להתערבות ממשלתית בשיח הציבורי. ההישענות על הסדרת האיחוד האירופי בתחום זה מחלישה את החשש מפני התערבות במרחב התוכן באופן שנועד להשפיע על השיח הפנים-ישראלי באופן ספציפי.

(2) קידום הקומה האזרחית - היבטים ארגוניים

ברמה הארגונית, דוח בן חורין מצביע על הצורך במעורבות ממשלתית כדי לוודא כי ניהול הסיכונים הוולונטרי של הפלטפורמות תואם את האינטרסים הציבוריים. כלומר כדי לקדם את ניהול הסיכונים וההתמודדות עם תוכן כוזב, נראה כי יש לקבוע מנגנון שמטרתו קיום דיאלוג או אף פיקוח למול הפלטפורמות כדי לוודא כי הקוד האמור לעיל מיושם באופן הולם בישראל.

²² פרסום תקופתי של פעילות לפי הקוד: <https://disinfocode.eu/reports-archive/?years=2023>; ²³ European Commission, Digital services act: Commission designates first set of very large online platforms and search engines, 25.04.23, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

בעקבות זאת עולה השאלה של זהות הגוף הממשלתי שיעסוק בהיבטים אזרחיים אלה. כפי שתואר לעיל, הארגונים הפעילים בתחום הביטחון והאכיפה אינם נראים כמועמדים טבעיים לתפקיד זה. פרקליטות המדינה פועלת להסרת תכנים בדיעבד. גופי הביטחון פועלים במישור הביטחוני ובאופן חשאי בדרך כלל. נוסף על כך אין כיום רשות מאסדרת טבעית אחת למרחב הסייבר. ועדת בן חורין הציעה להעביר את האחריות לליווי נושא זה לרשות תקשורת עצמאית. מחקר מקיף של המכון הישראלי לדמוקרטיה הציע להישען על סמכויותיו של הממונה על הגנת הצרכן במשרד הכלכלה.

לנוכח האתגרים המשמעותיים באסדרה הישראלית כיום, מוצע להתקדם בשלב זה בתחום הקומה האזרחית באמצעות שני מהלכים. המהלך הראשון הוא יצירת כלי מעקב ומתן תמריצים לאימוץ הקוד שתואר לעיל באמצעות גופי החברה האזרחית, ובמרכזם איגוד האינטרנט הישראלי, שהוא מלכ"ר עצמאי בעל מעמד בתחום האינטרנט, המייצג במידה רבה את האינטרסים של תפקודה התקין והבטוח של רשת האינטרנט לכל משתמשיה. מוצע כי בשלב ראשון השיח יחל באמצעות החברה האזרחית, ויעודד את הפלטפורמות הפועלות בישראל **להחיל על עצמן גם בישראל את המדיניות שעליה הסכימו באיחוד האירופי**. תוצאה אפשרית של מהלך כזה היא התחייבות וולונטרית של הפלטפורמות לאתר ולמנוע תוכן מפר באופן יזום, ללא קשר לפנייה של גופי הביטחון, בדיעבד. למהלך זה צפויה השפעה חיובית על זירת התוכן במרחב הסייבר, וממילא במניעה של תכנים שמטרתם השפעה זרה.

לנוכח הפעילות החלקית של רשויות המדינה בתחום התכנים, לגופי חברה אזרחית חשיבות רבה באיתור ובהתמודדות עם תכנים כוזבים. עם זאת, גופים אלה אינם זוכים באופן רציף למידע או שיתוף פעולה של הפלטפורמות, ובכך האפקטיביות של פעולתם עלולה לפחות. תועלת מרכזית באימוץ הקוד הוולונטרי בישראל היא מיסוד דרכי תקשורת עם הפלטפורמות בהתאם לכללים שקופים וניתנים לבקרה.

המהלך השני המוצע הוא מיסוד ועדה ממשלתית מלווה של נושא זה, באמצעות צוות משימה משולב של הרשות להגנת הפרטיות, הרשות להגנת הצרכן, ורשות התחרות. צוות זה יוכל

לשמש גם ממשק אל הקומה הביטחונית (הכוללת את גורמי הביטחון והמודיעין ומערך הסייבר הלאומי), ולקבל מידע נדרש בכל הקשור למקרים שבהם אין מדובר רק במידע כוזב אלא מידע הקשור בפעילות גורמים עוינים. בשונה מההצעה של דוח בן חורין להטיל תפקיד זה על רשות תקשורת, ולנוכח אי-קיומה של רשות תקשורת עצמאית בשלב זה, מוצע לרכז את הסמכויות העוסקות בתחומים אלה בשילוב רשויות אלה. לכל אחת מרשויות אלה נגיעה למקטע אחר בפעילות הפלטפורמות, ורק שילוב הידע והכלים האסדרתיים יכול להתמודד באופן ראוי עם האתגר שהן מציבות. הרשות להגנת הפרטיות נדרשת משום שהתשומה המרכזית בתהליכי העבודה של הפלטפורמות היא המידע האישי הנאסף ונועד להפקת מידע המשמש למסרים ממוקדים באמצעות הפלטפורמה, בין אם אלה מסרים שיווקיים או מסרים רגילים. הרשות להגנת הצרכן נדרשת משום החשיבות של גילוי נאות למשתמשים ולאחרים על אודות אופן הפעולה של הפלטפורמות. רשות התחרות נדרשת משום שהפלטפורמות הגדולות הן בעלות כוח שוק ניכר, ועולה חשש שאופן האסדרה של אקוסיסטם, המידע וההתערבות שלהם בתכנים, מושפעים גם משיקולים כלכליים הקשורים בגישה או בחסימה של מתחרים. תפקידם של גורמי הביטחון ומערך הסייבר הלאומי הוא להצביע על כוונות עוינות ולהבטיח ראייה הוליסטית.

כדי לקדם היבטים אלה, מוצע כי בהמשך לשיתופי פעולה שכבר נקטו בעבר במרחב המקוון, יפעלו גם בתחום זה.²⁴ לדגם זה של שיתוף פעולה יש תקדים גם בבריטניה,²⁵ ודומה כי הוא מאפשר קידום מהיר על בסיס החקיקה הקיימת. נוסף על כך כל אחת מרשויות אלה בעלת עצמאות מסוימת ממשרדי הממשלה, ובעלת כשירות לגבי מקטע מסוים בלבד של תחום הפעילות. מבנה זה מצמצם את הסיכון של התערבות מדינתית לא מידתית בתכנים. **מוצע לקבוע תקנון פעולה מוסכם המגדיר את יחסי הגומלין שבין הפעילות הוולונטרית של איגוד האינטרנט,**

²⁴ משרד המשפטים, הרשות להגנת הפרטיות, הרשות להגנת הפרטיות רשות התחרות והרשות להגנת הצרכן ולסחר הוגן ממליצות לאמץ זכות לניוד מידע בדין הישראלי, 03.01.2021,

https://www.gov.il/he/departments/news/data_portability
UK information commissioner's office, ICO and CMA set out blueprint for cooperation in digital markets, 19.05.2021,²⁵
<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/05/ico-and-cma-set-out-blueprint-for-cooperation-in-digital-markets/>

לבין פעילותן של רשויות אלה, כל אחת בתחום אחריותה, על פי עקרונות פעולה שגובשו באיחוד האירופי.

(3) הקומה האזרחית – אוריינות דיגיטלית – הדרכה והעלאת מודעות – המשתמשים

בפלטפורמות

מודעות ונורמות כנגד השימוש במידע שקרי או מטעה כחלק מהשיח הפוליטי הפנימי

יש להזכיר כי בזירת השיח פועלים גם שחקנים המבקשים לעשות שימוש בכל היכולות של הפלטפורמות כדי להשפיע על הציבור לתמוך בעמדותיהם. קיומו של מרחב ציבורי שיש בו מידע כוזב שניזום בידי פוליטיקאים או פעילים ציבוריים, מייצר מורכבות ערכית ומבצעית להתמודדות עם השפעה זרה. ברור כי גופי הביטחון, שאמונים על ציות לדרג הפוליטי המייצג את הציבור, נדרשים להימנע מעימות חזיתי עם פוליטיקאים או התערבות בפעילותם. לכן כהשלמה לפעילות מול הפלטפורמות, נדרשת פעילות מול השחקנים השונים העוסקים בייצור מידע ובהפצתו, כדי לצמצם את החשש שבפעילותם יגבירו את החשיפה להשפעה זרה. דוגמה לכך היא האמנה שיזם המכון הישראלי לדמוקרטיה לגבי אופן שימוש בפרסום דיגיטלי במערכת בחירות.

אוריינות דיגיטלית והעלאת מודעות בעניין צריכת תכנים והפצתם

חלק ממהלכי המניעה כוללים גם הדרכה והגברת מודעות של ציבור המשתמשים – הדוברים – המפיצים בפלטפורמות. בהקשר זה, ככל שיהיה מידע רב יותר ושקוף יותר על אודות אופן הפעולה של הפלטפורמות והשיקולים להפצת מידע, כך אפשר יהיה להנגיש מידע זה לציבור. בנקודה זו גם יש חשיבות עצומה לגופי החברה האזרחית אשר מסוגלים לבקר את המידע המופץ בידי הרשתות החברתיות על אודות פעולתן ולהנגיש מידע זה באופן אובייקטיבי למשתמשים השונים. ברמה הארגונית נדרש לקדם עבודת מטה העוסקת בממד זה, ובדרכים השונות של העצמת המשתמשים, בין במסגרת שירותים ממלכתיים כמו חינוך ובין בשיתוף פעולה עם גופי החברה האזרחית.

נושא המודעות מוזכר אחרון בסל הכלים בשל הרצון להדגיש את הצורך במיקוד המבט בכוחות המעצבים את זירת השיח, וההנחה כי "חינוך" משתמשים וצרכנים יהיה אפקטיבי יותר רק לאחר

טיפול בכוחות אלה. ככלל נראה כי יש לשלב אוריינות דיגיטלית הכוללת גם אתיקה בשימוש ברשתות חברתיות וגם הבנה רחבה יותר של האקוסיסטם, כחלק מלימודי אזרחות. משרד החינוך עסק בנושאים אלה אולם נראה כי יש מקום לעיסוק רחב יותר, כולל תוכניות הכשרה ייעודיות. החברה האזרחית, כגון איגוד האינטרנט, ולעיתים גם התעשייה, יכולים להיות מעבדה לפיתוח תכנים מתאימים וגם להם תפקיד בהגברת הבטיחות. אולם לנוכח התפקיד המרכזי של מרחב הסייבר בחיים הדיגיטליים, יש חשיבות לעיסוק שיטתי פדגוגי בהקניית כלים באמצעות מערכת החינוך. לצד זאת יודגש כי מחקרים מראים כי גם לאוכלוסייה בוגרת יותר, שהיא חלק מאוכלוסיית הבוחרים, יש נטייה להיות מושפעת ממידע כוזב, ולכן יש חשיבות במשרעת רחבה של כלים שיתאימו לסוגי אוכלוסייה שונים.²⁶

מקרה הבוחן של התמודדות עם "השפעה זרה" בבחירות

ועדת הבחירות היא מוסד עצמאי בעל מטה ומנגנון מקצועי, אשר בראשה עומד שופט בית המשפט העליון, ותפקידה להגן בין היתר על "טוהר הבחירות". בעקבות החשיפה של קמפיינים מדינתיים שמטרתם התערבות בבחירות לנשיאות בארה"ב²⁷ ובאירופה,²⁸ גם ועדת הבחירות המרכזית פעלה להתמודדות עם חשש להשפעה זרה בעת מערכת בחירות בישראל.²⁹

אופן ההתמודדות של ועדת הבחירות המרכזית עם החשש מפני "השפעה זרה" במערכת הבחירות מדגים את החשיבות של הסדרה הוליסטית, הכוללת פעילות ביטחונית ופעילות אזרחית, וכן שיתוף פעולה ארגוני בין גופי ביטחון לבין גופים אזרחיים. כפי שתואר לעיל, יריבים

²⁶ ראו למשל: Alice Hugué, Julia H. Kaufman, Melissa Kay Diliberti, Social media posts have power, and so do you: stop the spread of false and misleading information during voting season, RAND Corporation, 2024, <https://doi.org/10.7249/TLA2909-1>

²⁷ ראו למשל: U.S. department of justice, special counsel Robert S. Mueller, III, Report on the investigation into Russian interference in the 2016 presidential election, Volume I, March 2019, <https://www.justice.gov/storage/report.pdf>

²⁸ Eric Brattberg & Tim Maurer, Russian election interference, Europe's counter to fake news and cyber attacks, May 2018, <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>

²⁹ ראו למשל: השפעה זרה על תוכני השיח הפוליטי: אתגר אסטרטגי חדש, מבט על, גיליון 1129, 14 בינואר 2019, <https://www.inss.org.il/he/publication/foreign-influence-on-political-discourse-a-new-strategic-challenge>

עושים שימוש בהשפעה זרה באופן שוטף ובמגוון הקשרים, אולם יש רגישות מיוחדת בפעילות זו לקראת מערכת בחירות, עקב הניסיון להשפיע על הבוחרים ועל דעת הקהל.

ועדת הבחירות עשתה שימוש ביכולת הפעולה והמעמד המשפטי העצמאיים שלה כדי להתמודד עם האיומים במרחב הסייבר ולמקסם את המשאבים העומדים לרשותה כדי לשפר את ההיערכות. הוועדה ניגשה לאיום הסייבר לטוהר הבחירות באופן משולב, הכולל הן איומים בתחום הטכנולוגי³⁰ הן חשש מפני התערבות בתחום התוכן. בגישה זו ביקשה ועדת הבחירות להתמודד באופן שלם עם האיום.

במישור הארגוני כינסה הוועדה את גורמי המקצוע מרשויות המדינה השונות לדיוני היערכות ותיאום. בדיונים אלה השתתפו גורמי מודיעין, ביטחון, אכיפת חוק, הגנת סייבר, אסדרה ופרקליטות המדינה. פעולה זו חיזקה את התשתית לשיתוף הידע וליכולות שיתוף הפעולה לקראת הבחירות ובמהלכן.

בהקשר זה יצוין כי מערך הסייבר הלאומי, המופקד על תחום הגנת הסייבר, כלומר מניעת תקיפות מחשב וגנבת מידע, פעל לסייע לוועדת הבחירות להגן על תקינות תהליך הבחירות בהיבטי הגנת הסייבר. המערך לא עסק בהיבטים הקשורים בתוכן. המערך פעל בהתאם למתווה שהציע לוועדת הבחירות לסיוע לפעולתה, כאשר העיקרון המנחה ברמה המשפטית, וכפועל יוצא ברמה התפעולית, הוא שוועדת הבחירות ונציגיה המוסמכים הם מקבלי ההחלטות בנושאים עקרוניים או מהותיים, ואילו מערך הסייבר הלאומי פועל כגורם מומחה לאומי עבורם. בהתאם להגדרת תפקידו של מערך הסייבר הלאומי, הוא אינו עוסק בתכנים, אולם מנגנוני התיאום שריכז עבור ועדת הבחירות, כללו את כלל הנציגים המוסמכים מקרב גורמי הביטחון והאכיפה, כולל נציגי מחלקת הסייבר בפרקליטות המדינה, ובכך אפשרו יצירת תמונה מצב אחודה עבור יו"ר ועדת הבחירות.

³⁰ לסקירה על פעילות ועדת הבחירות בנושא זה ראו: מבקר המדינה, דו"ח שנתי 2022, מערכות המידע והגנת הסייבר בבחירות לכנסות ה-21, ה-22 וה-23 - תחום ביקורת מערכות מידע, 09.03.2022, <https://www.mevaker.gov.il/sites/DigitalLibrary/Pages/Reports/7413-23.aspx>

במישור התוכני פותחו במסגרת פעילות הוועדה כללים תקדימיים מכוח חוק הבחירות (דרכי תעמולה), התשי"ט-1959, כגון על אודות הצורך בזיהוי מודעות פוליטיות מטעם מפלגות בפלטפורמות המקוונות.³¹ החלטה זו התקבלה במסגרת עתירה ציבורית מטעם בעלי זכות בחירה לכנסת, כנגד המפלגות. במסגרת ההחלטה התקדימית, השופט מלצר הבהיר כי מטרת החלטה זו היא למנוע תופעה של יכולת גורמים עוינים "להסתוות" במסגרת השיח הפוליטי הלגיטימי. מעניין לציין כי להסדרה זו היו מתנגדות מקרב המפלגות הפוליטיות, הן מסיבות מוסדיות, כלומר שההחלטה צריכה להתקבל בידי המחוקק הן מסיבות מהותיות. ההחלטה חשובה בכך שהיא קובעת כלל שמיועד להתמודד ישירות עם השפעה זרה הנחזית להיות תוכן פוליטי לגיטימי. נוסף על כך ולא פחות חשוב, ההחלטה מופנית גם כלפי הפלטפורמות, וקובעת שפלטפורמה אשר לא תנקוט אמצעים לזיהוי המפרסם של מודעה פוליטית, תיחשב כאחראית אף היא להפרה. מהחלטה זו עולה כי אף שהמטרה היא מטרה ביטחונית, האמצעי שננקט הוא כלל רגולטורי מחייב כלפי המפלגות והפלטפורמות. מהלך זה מדגים את הקשר בין התכלית הביטחונית לבין הצורך בסל כלים משפטי אסדרתי מידתי. נוסף על כך כללים אלה נועדו לחול מראש, לצד פעולות משפטיות להתמודדות עם תכנים קונקרטיים ככל שהדבר נדרש בידי גופי הביטחון והאכיפה, ובוצעו בידי פרקליטות המדינה.

סיכום

נקודת המוצא של המאמר היא כי נדרשת המשגה חדשה ומשולבת של תופעת ההשפעה הזרה במרחב הסייבר. התמודדות עם תופעה, ובהתאמה בניין כוח והפעלת אמצעים כנגדה, מחייבת הבנה של מטרותיה ותיאור מאפייניה. ההתמודדות עם השפעה זרה במרחב הסייבר מחייבת שילוב בין שתי נקודות מבט מרכזיות - נקודת מבט אסטרטגית-ביטחונית ונקודת מבט טכנו־משפטית. נקודת המבט האסטרטגית בוחנת את ה"השפעה זרה" בזירת הסייבר כחלק מהמטרות, האמצעים והכלים של היריב בתחום ההשפעה הזרה באופן כללי. נקודת המבט הטכנו־משפטית בוחנת את זירת הפעולה, מרחב הסייבר, והמאפיינים הייחודיים של ייצור, הפצה

³¹ ועדת הבחירות המרכזית לכנסת ה-21, תב"כ 8/21 שחר בן מאיר נגד מפלגת הליכוד ואח, <http://bit.ly/489jMz1>

ואסדרה של תכנים בזירת הסייבר, ובהתאמה מניעת הפצה של תכנים מזיקים בו. שילוב נקודות מבט אלה מאפשר להגדיר כיצד השפעה זרה באה לידי ביטוי במרחב הסייבר, מה הם הכלים הקיימים והנדרשים בידי המדינה להתמודדות איתה, וכיצד אפשר לאזן בין הצורך הביטחוני לבין החשש מפני התערבות של המדינה בתכנים.

התמודדות אפקטיבית עם תוכן המזוהה כחלק מהתערבות זרה, מחייבת הסדרה מאוזנת, המתאימה בין ההגדרות המבצעיות לבין ההגדרות המשפטיות, וקביעת סמכות מפורשת, במסגרת הכללים החוקתיים החלים על סמכות המדינה, להנחות את הפלטפורמות להסיר או לחסום תוכן זה. על בסיס האמור מוצע להפריד בין פעולות שמטרתן להעלות את ה"עמידות" בפני השפעה זרה, פעולות שמטרתן להתמודד עם "השפעה זרה" בעת שהיא קורית, למול נמעניה, ופעולות שמטרתן פעולה מול היריב שעושה שימוש בהשפעה זרה.

מבחינה מעשית, כדי שהתערבות למניעת השפעה זרה תהיה אפקטיבית, יש צורך בהעלאת רמת האחריות וניהול הסיכונים של הפלטפורמות, בהתאם להסדרים שהסכימו להם בעולם. פעילות זו צריכה להתבצע באמצעות שיח של חברה אזרחית ורשויות אזרחיות, ולא באמצעות גופי הביטחון.

תפיסה אסטרטגית המחברת בין פעילות גופי הביטחון לבין החברה האזרחית מאפשרת להתאים את המאמצים המדינתיים לסביבה האזרחית והרגולטורית החלה על מרחב זה, בתוך ניצול היתרון המוסדי היחסי של הארגונים השונים הפועלים במרחב זה. בהמשך לכך היא מאפשרת להפעיל את הכוח הביטחוני או המבצעי בנסיבות הנדרשות לכך, ובאופן ממוקד המפחית את החשש מפני שימוש לרעה. יישום אסטרטגיה אחידה המחברת בין הממד הביטחוני לאזרחי, והמייצרת ממשקים מסודרים ושקופים אל הפלטפורמות, יאפשר התמודדות טובה יותר עם אתגר זה.

על רקע זה מוצעות ההמלצות האלה:

1. יש להטיל על גורם ביטחוני מרכזי את האחריות לתכלול את היערכות המדינתית להתמודדות עם "השפעה זרה" באופן שמביא בחשבון את מאפייניה ההיברידיים של הסוגיה – היבטים ביטחוניים אסטרטגיים והיבטים משפטיים אסדרתיים. לצורך גיבוש היערכות מדינתית יש

לגבש המשגה אסטרטגית וטקטית למאפייני "השפעה זרה" ויחס בינה לבין "מידע כוזב" במרחב הסייבר.

2. יש להקים יכולת אזרחית ממשלתית להתמודדות עם מידע כוזב מסוגים שונים במרחב הסייבר, ולחזק ולהרחיב את הממשקים בין מערכת הביטחון המכוונת לטפל ביריבים, לבין המערכת האזרחית העוסקת בהיבטים של תכנים פוגעניים במרחב הסייבר.

3. כדי למנוע את התופעה של "הסתוות" השפעה זרה בתוך שיח פנים־מדינתי, יש להביא ליתר אחריות של שימוש פוליטיקאים ואישי ציבור אחרים בפלטפורמות הפצת התוכן. לצד החשיבות הרבה של מגוון אמצעי התקשורת הישירים של אישי ציבור ומגוון דרכי הביטוי בענייני השעה, יש לוודא כי מגוון זה אינו מייצר סיכונים למניפולציה בידי יריב. לצורך כך יש לגבש אמצעים משפטיים, אתיים, והסברתיים כלפי השחקנים הפוליטיים בזירה הציבורית.

4. יש לקדם הסדרים משפטיים המגבירים את פעילות הפלטפורמות המקוונות לגבי במניעת שימוש לרעה בפלטפורמות שלהן להפצת תוכן פוגעני או כוזב ולהגביר את מעורבותן בהסרתו, כמפורט להלן:

א. הוספת חובות ניהול סיכונים על פלטפורמות גדולות

- מוצע להתבסס על הנורמה שנקבעה באיחוד האירופי שבמסגרתה נדרשת פלטפורמת תוכן לקבוע מדיניות ניהול סיכונים כנגד הפצת תוכן כוזב. נורמה זו משמשת בסיס לקוד למניעת הפצת מידע כוזב. היתרון בקוד שהוא משקף הסדר מקובל במדינות העולם, ולכן הוא אמת מידה מאוזנת להסדר ישראלי, ומצמצם את הסיכון להתערבות שלטונית מקומית לא מידתית באסדרת תכנים.
- על כן מוצע, בשלב ראשון, להשתמש בקוד כסטנדרט מהותי לגבי הציפיות מפלטפורמות התוכן. יש להדגיש כי אימוץ הקוד למניעת הפצת מידע כוזב הוא נקודת מוצא בלבד, ואינו פתרון שלם. אולם אימוץ הקוד יאפשר לייצר את סל המונחים, השיח והממשקים הנדרשים לבניית היכולות בנושא זה.

ב. פיקוח על ניהול סיכונים בידי הפלטפורמות

- לגבי אופן הפיקוח והאכיפה כדי לוודא שהקוד מיושם בצורה אפקטיבית בישראל, מוצע לפעול באמצעות מיסוד שקיפות ודיווחים של פלטפורמות הפצת התוכן מול החברה האזרחית, שבמוקד שלה איגוד האינטרנט הישראלי וגופי חברה אזרחית נוספים העוסקים במניעת הפצת תוכן כוזב באינטרנט.
 - בו בזמן מוצע לפתח מעגל רגולטורי משולב הכולל את הרשות להגנת הפרטיות (המפקחת על שימוש במידע), הרשות להגנת הצרכן (המפקחת על גילוי נאות), ורשות התחרות (המפקחת על השווקים). במדינות העולם המפותחות לרשויות אלה ממשקים שונים לפלטפורמות התוכן.
5. יש להגביר את מאמצי ההסברה והמודעות והחינוך של הציבור הרחב לסיכונים של מידע כוזב, ובפרט לאופן שהפצתו או שימוש בו עלולים לשרת גם יריב מדינתי.
6. יש להקים שולחן עגול קבוע של גורמים העוסקים בתחום המודעות וההגנה באינטרנט כדי לסנכרן מאמצים של החברה האזרחית ושל המדינה בתחום זה.