המלחמה בדואר זבל (ספאם)

דוח מדיניות

מאת
פרופ' מיכאל בירנהק וד"ר מיקי זר
הפקולטה למשפטים, אוניברסיטת תל אביב

ינואר 2024

אוניברסיטת תל אביב TEL AVIV UNIVERSITY
מרכז הנשיא מאיר שמגר
למשפט דיגיטלי וחדשנות
אוניברסיטת תל אביב

תודות

אנו מבקשים להודות לעוזרות המחקר תמר נגר ואסתר סגל, ולעוזר המחקר יובל אלי-עז על סיוע בהכנת הדוח, ולפעילים שונים בזירת הספאם ששוחחו איתנו לשיחות רקע בנושא.

אנו מודים לוועדה לניהול וחלוקת כספים שנפסקו כסעד בתובענות ייצוגיות על תמיכתה במחקר זה (לפי מענק 38/2022), ולמרכז הנשיא מאיר שמגר למשפט דיגיטלי וחדשנות על תמיכתם.

תמצית המלצות הדוח

1. לגבי **בעלי המסר:**

א. בעת פסיקת פיצויים, על בתי המשפט לשקול את היקף הפעילות של החברה המפרסמת, כדי לצמצם הן את הרתעת-החסר והן את הרתעת-היתר שיש במבנה הדין האחיד הנוכחי.

ב. יש להפנות מאמצים של אכיפה פלילית במקרים המתאימים.

2. לגבי **גורמים מסייעים בשלב שלפני ההפצה:** ראוי לשפר את נגישות האכיפה הפרטית לפי חוק הגנת הפרטיות, בכמה דרכים:

א. הרחבת הפיצוי הסטטוטורי גם לעוולות לפי פרק ב;

ב. הארכת תקופת ההתיישנות לשבע שנים, כמו בכל תביעה אזרחית;

ג. הוספת האפשרות לתבוע בגין הפרת חוק הגנת הפרטיות, בדרך של תובענה ייצוגית.

3. לגבי **גורמים מסייעים בשלב ההפצה:**

א. יש להפנות מאמצי חקירה ומחקר בנושא "רשתות השותפים" בישראל,

ב. יש לעקוב לבחון את השפעותיהן של ההנחיות החדשות של משרד התקשורת לעניין הסדרת הפצת מסרונים, תוך שימת לב לאפשרות של אסדרת-יתר של פעילות חברות ההפצה.

4. לגבי **ספקיות התקשורת:**

א. כיום ספקיות תקשורת, ולעיתים חברות הפצה, נהנות מ**פטור מאחריות**. ראוי להקיש מהסדרים קיימים בנוגע לאסדרת פעילות גורמי ביניים כמו פלטפורמות של רשתות חברתיות, ולאמץ נוהל הודעה והסרה בליווי חזקות מתאימות לעניין הספאם.

ב. ראוי לקבוע בחקיקה וברישיונות בזק רף מינימלי של שירות סינון שחברות תקשורת יחויבו לספק ללקוחותיהן.

ג. יש ליצור תשתית אזרחית-צרכנית אחידה לשם הקניית אוריינות דיגיטלית בסיסית בכל הנוגע לספאם ולדרכים להימנע ממנו.

5. בנוגע ל**רשתות חברתיות:**

א. יש להציב רף מינימלי מחייב של הגנה על משתמשים מפני ספאם באמצעות מסננים ייעודיים, כאשר יוטל על החברות בנוסף לדאוג לכך שמשתמשים יידעו על מסננים אלה ועל האופן להפעילם.

ב. ראוי לעודד מחקר שמבקש לפתח טכניקות לאיתור חתימה מלאכותית של בוטים ברשתות, תוך שיתוף פעולה של מומחי אבטחת סייבר וחוקרי למידת מכונה.

6. יש לשקול הקמת גוף מדינתי שיהיה אמון על אכיפה מנהלית בתחום הספאם;
7. המדינה צריכה לעודד אוריינות דיגיטלית בכלל ואוריינות בכל הנוגע למערכת הספאם בפרט;
8. יש לעודד יצירת שירותים, דוגמת "ספאם אוף", שיסייעו להתגבר על כשלים באכיפה, ואין מקום לעוינות משפטית ושיפוטית כלפי מיזמים כאלה;
9. יש לעודד פתרונות טכנולוגיים לספאם, ולשם כך לבחון מחדש את מערך התמריצים הכלכליים ואת יעילותו, וליצור תמריצים מתאימים, למשל על ידי תמריצים כלכליים לחברות טכנולוגיה שיטמיעו במוצריהן עקרונות של הנדסת ניקיון;
10. ראוי לבחון מחדש את הגדרת "מפרסם" ו"דבר פרסומת" והתאמה מחודשת להתפתחויות בזירה הטכנולוגית, למשל לסוגים חדשים של מכשירי קצה או של דרכי תקשורת חדשות.
11. לבסוף, אנו ממליצים על **השקעה במחקר ופיתוח** מטעם המדינה של כלים טכנולוגיים למלחמה בספאם, בהם יוטמעו מראש ערכי הנדסת ניקיון, ושיוכלו לשמש את כלל האוכלוסייה, בדומה למשל לאפליקציית המגן שפותחה בעת המאבק של מדינת ישראל במגפת הקורונה.

תקציר הדוח

דואר זבל, או ספאם, הוא **מסר שנשלח אל הנמען באמצעים שונים, ללא הסכמתו המוקדמת, ובניגוד לרצונו, ומהווה בשל כך מטרד.** זירת הספאם אינה יציבה: יש בה תמריצים כלכליים שמשתנים, הפעילות בה תלוית-טכנולוגיה, והיא משתנה כאשר הטכנולוגיות הרלוונטיות משתנות, ויש כללים משפטיים שונים ממקום למקום. דוח מדיניות זה ממפה את השחקנים המרכזיים השונים שפועלים במערכת האקולוגית של הספאם, מנתח את האינטרסים השונים שלהם, ומציע סקירה וניתוח שיטתיים של מפת השינויים בנושא הספאם מעת חקיקת חוק הספאם הישראלי ועד היום. זאת הן בזירת החקיקה והפסיקה, תוך בחינה מפורטת של מסלולי האכיפה הקיימים, והן בזירה הטכנולוגית, תוך בחינת טכנולוגיות ספאם וטכנולוגיות אנטי-ספאם קיימות.

הדוח מתמקד בממשק שבין המשפט לטכנולוגיה ולפיכך, בצד בחינה פרטנית של סל הכלים המשפטיים (ובכלל זה באופן השוואתי) וסל הכלים הטכנולוגיים, הדוח בוחן את החפיפה בין הפתרונות השונים ואת השפעותיהם ההדדיות. בחינת הממשק שבין הפתרונות השונים, המשפטיים והטכנולוגיים, נועדה לאפשר הבנה טובה ומלאה יותר של המערכת האקולוגית של הספאם. כל טכנולוגיה למלחמה בספאם מעוררת קשת של שאלות משפטיות. במקביל, פתרונות משפטיים משפיעים על עיצוב טכנולוגיות הספאם וטכנולוגיות האנטי-ספאם. המטרה היא לזהות סוגי פתרונות אפשריים ולהבין את אופן פעולתם. הגישה המחקרית במסגרתה נכתב הדוח גורסת כי המשפט לבדו, או הטכנולוגיה לבדה, אינם יכולים למגר את תופעת הספאם.

הדוח מסתמך על מסגרת רעיונית שלפיה, כדי להבין את ההיבטים המשפטיים של מערכות המבוססות על מידע, יש ללמוד אותן בתוך ההקשר הרחב שבו הן פועלות. סביבות המידע בהן מועברים מסרים אלקטרוניים הן סביבות מורכבות, מרובות זרמי מידע ומרובות שחקנים המעורבים בזירת הספאם. כלכלת הספאם בעידן הדיגיטלי היא מערכת טכנולוגית-עסקית סבוכה ומרובת שחקנים, שלהם אינטרסים שונים ומגוונים, שלעיתים מתלכדים עם האינטרסים של שחקנים אחרים ולעיתים סותרים אותם.

שרשרת הערך של הספאם היא סך השחקנים והמשאבים שמעורבים במאמץ להפוך ספאם לרווחי. ניתוחים כלכליים מקובלים של מערכת הספאם רואים את שרשרת הערך כיחידת ניתוח נפרדת, שניתנת ללימוד ולהבנה במנותק משאר הכוחות הפועלים נגדה. בשונה, הדוח נוקט גישה הוליסטית לניתוח מערכת הספאם, ומרחיב אותה כך שתכלול גם את הצד השני של המטבע – את השחקנים המעורבים **במאבק בספאם.** גישה זו רואה בספאם מערכת אקולוגית שמורכבת הן משרשרת הערך של הספאם והן מכוחות שפועלים נגדה.

הדוח עוסק בספאם צרכני בעיקרו, ובפן האזרחי שלו. הדגש הוא על טכנולוגיות למלחמה בספאם בדוא"ל, במסרונים ובהודעות קוליות, שהם אפיקי הספאם אליהם מתייחס הדין הישראלי במפורש. בשינויים המתחייבים, הדיון ניתן ליישום לטכנולוגיות אחרות. כמו כן, הדוח בוחן צורות שונות של **"הנדסת ניקיון"**, כלומר ההיתכנות של תכנון מוקדם של טכנולוגיה על מנת לסייע בשמירה על "ניקיון" המערכת האקולוגית התקשורתית, כדי לצמצם פעילות של דואר זבל לא חוקי.

הדיון נערך במסגרת הדין הישראלי, תוך בדיקה משווה למדינות אחרות.

תקציר מפורט

כלכלת הספאם וגישת הניתוח

1. ספאם היא תופעה מורכבת ורבת פנים. כלכלת הספאם בעידן הדיגיטלי היא מערכת טכנולוגית-עסקית סבוכה ומרובת שחקנים, שלהם אינטרסים שונים ומגוונים, שלעיתים מתלכדים עם האינטרסים של שחקנים אחרים ולעיתים סותרים אותם. לפיכך, כלכלת הספאם יוצרת מערכת אקולוגית מורכבת. כדי להעריך את הפתרונות השונים לבעיה עלינו להביא בחשבון טווח רחב של שיקולים ואינטרסים של גורמים רבים. לשם כך, יש למפות את השחקנים שמעורבים בתמונה.

2. **שרשרת הערך של הספאם** היא סך השחקנים והמשאבים שמעורבים במאמץ להפוך ספאם לרווחי. בשרשרת שני שלבים מרכזיים: הראשון כולל את כל הפעילות המתרחשת לשם יצירת ספאם ושליחתו, עד לרגע שבו מגיע הספאם אל הנמען. השני כולל את כל הפעילות המתרחשת במידה שספאם "הצליח", והניע את הנמען לרכישה. ניתוחים כלכליים מקובלים של מערכת הספאם רואים את שרשרת הערך כיחידת ניתוח נפרדת, שניתנת ללימוד ולהבנה במנותק משאר הכוחות הפועלים נגדה.

3. חוקרי מערכות מידע שהתמקדו במחקר שרשרת הערך של הספאם הסיקו שנדרש **ניתוח הוליסטי** של "שרשרת הערך" כולה, כזה שיעריך את היחסים המתקיימים בין החוליות השונות בשרשרת, וכך יוכל לזהות חולשות אפשריות. הדוח נוקט גישה הוליסטית לניתוח מערכת הספאם, ומרחיב אותה כך שתכלול, בנוסף לשרשרת הערך של הספאם, גם את הצד השני של המטבע – את השחקנים המעורבים במאבק בספאם. גישה זו רואה בתופעת הספאם מערכת אקולוגית שמורכבת הן משרשרת הערך של הספאם והן מכוחות שפועלים נגדה.

4. כלכלת הספאם הדיגיטלי אינה פועלת כיום לפי מודל פשוט של מוען ונמען שנמצאים בקשר ישיר, אלא זו תעשייה מסועפת, מרובת שחקנים ומתווכים, שלכל אחד מהם אינטרסים שונים ולחלקם זכויות משפטיות. זו מערכת טכנולוגית-עסקית סבוכה. בבחינת פתרונות חדשים במסגרת המאבק למיגור הספאם, יש לזנוח את הגישה הבינארית, שבוחנת רק את המשווק כמוען ואת משתמשי האינטרנט והטלפון כנמענים, ולראות את התמונה הרחבה יותר, שבה שחקנים רבים.

5. נקודת המוצא של הדוח היא ההנחה שללא הבנה מלאה של מערכת הספאם ושל השחקנים שמעורבים בה, מרבית ההתערבויות נגד ספאם עלולות להתמקד בהיבטים מסוימים בלבד, למשל סינון דוא"ל או רשימות שחורות של כתובות אתרים, ולהתעלם מהיבטים אחרים, כמו השלב המקדמי של קצירת כתובות דוא"ל ומספרי טלפון, או שלבי ביניים כמו שימוש בשירותי תיווך לשם הפצת מסרים.

השחקנים בזירת הספאם

6. מערכת הספאם היא זירה רבת-משתתפים, בנוסף לשחקני הקצה – המוען והנמענים – יש שורה של גורמי בי־ניים שמעורבים בשלבים שלפני ההפצה, בהפצה, ובמאבק בספאם. בכל אחת מהחוליות האלה יש סוגים שונים של שחקנים – חלקם מעורב באופן ישיר וחלקם באופן עקיף, חלקם פועל בצורה חוקית ולגיטימית וחלקם פועל בצורה לא חוקית. השחקנים העיקריים הם: בצד שמרוויח מספאם, שחקנים מרכזיים נוספים, מלבד המוענים, הם ספקי לִידִים (מלשון lead), שמספקים למשווקים את רשימות התפוצה; בעלי מאגרי מידע, שכוללים רשימות תפוצה; חברות הפצה שמספקות פלטפורמות להפצת תכנים שיווקיים במסות גדולות, שאינן בהכרח בעלות רי־שיון בזק; חברות תקשורת (בעלות רישיון בזק); ורשתות שותפים, שהן פלטפורמות שמקשרות בין גורמים העוס־קים בפרסום בזירות טכנולוגיות שונות (השותפים), לבין בעלי עסק שמעוניינים לפרסם את עסקיהם. בצד שעניינו המלחמה בספאם, שחקנים מרכזיים הם המדינה, שהיא שחקן רב גופים ופנים; הציבור, שהוא הנפגע המרכזי מתופעת הספאם; גופים פרטיים מסוגים שונים שפועלים למיגור התופעה; ושחקנים שונים בזירה הבין-לאומית.

7. לשחקנים הלגיטימיים יש אינטרסים וזכויות שונות, שיש לאזן ביניהם: הזכות לפרטיות והזכות להימנע ממטרדים של הנמענים, זכויות קניין, חופש עיסוק וחופש ביטוי מסחרי של המפרסמים, זכויות קניין וחופש פעולה עסקי של גורמי ביניים חוקיים.

8. הדוח טוען שזירת הספאם אינה יציבה: יש בה תמריצים כלכליים שמשתנים, הפעילות תלוית-טכנולוגיה ולכן גם משתנה כאשר הטכנולוגיות הרלוונטיות משתנות, ויש כללים משפטיים שונים.

9. מהדיון עלו גם מספר מסקנות נקודתיות בנוגע לשחקנים ספציפיים:

א. בין בעלי המסר, שתי הבחנות חשובות שעלו בדיון הן גודל העסק, וחוקיות התוכן המופץ.

ב. בנוגע לאחריות להפצת ספאם, הדיון העלה שהיא אינה מתחלקת באופן שווה בין השחקנים בשרשרת הערך. עיקר האחריות המשפטית לשליחת ספאם נופלת היום על בעלי המסר, ועל ספקי הלידים. כמו כן, בעקבות תקנות חדשות, חברות ההפצה עשויות לסבול מהרתעת יתר. מנגד, חברות התקשורת אינן נושאות היום כלל באחריות להפצת ספאם.

ג. גורמי ביניים מרכזיים שמסייעים למשווקים להפיץ הודעות מסחריות (שלב ההפצה) הם "רשתות שותפים" וחברות ההפצה. בעוד שרשתות השותפים אטרקטיביות עבור ספאמרים מקצועיים ועבור כל שחקן שמבקש להרחיק את עצמו מאחריות מידית לשליחת ספאם, מקומן של חברות ההפצה בזירה אמביוולנטי יותר ביחס לספאם. הן מציעות שירות שאינו בלתי חוקי כשלעצמו, אבל יש חשש שינוצל לרעה. למעשה, שולחי ספאם מקצועיים מסכנים את עסקיהן של חברות ההפצה, ולהן יש אינטרס לעמוד על המשמר בקשר לשימוש בשירות שלהן.

ד. בצד שעניינו המלחמה בספאם המדינה היא שחקן מרכזי. המדינה מצויה בצומת של אינטרסים רבים שלעיתים מתנגשים, וביניהם עליה לנווט. רצונה של המדינה למגר את תופעת הספאם מציף מתחים מול שחקנים שונים בשרשרת הערך של הספאם, שמבקשים הגנה על זכויות הקניין וחופש העיסוק שלהם. המדינה גם מחויבת להגן על חופש הביטוי של משתמשי שירותי התקשורת, ולכן עליה להיזהר מלהטיל רשת צפופה מדי של סייגים על משלוח מסרי תקשורת. המדינה גם מבקשת להגן על יכולותיה להשתמש באופן מיטבי בכלי תקשורת על מנת להעביר מסרים מטעמה, וכן להגן על מעמדה בזירה הבין-לאומית המקוונת.

ה. צרכני שירותי תקשורת אינם עשויים מקשה אחת, גם לא בעניין הספאם. יכולת ההתגוננות של האזרח מפני תקשורת לא רצויה תלויה במידה לא מבוטלת באוריינות דיגיטלית.

ו. שחקנים פרטיים שפועלים נגד ספאם מטעמים עקרוניים, למשל עורך דין בתחום או חברה שמטרתה לסייע לנפגעי ספאם, עשויים למצוא את עצמם בדילמה כלכלית. האינטרס הכלכלי של שחקן כזה עשוי לעמוד בסתירה לאינטרס הערכי שלו להילחם בספאם לטובת כלל הציבור.

ז. חברות התקשורת הן שחקן מרכזי בזירת הספאם, שתפקידו במערכת האקולוגית של הספאם מורכב. הסיבה המרכזית לכך היא שחברות התקשורת אוחזות בשני כובעים: הן מחזיקות ומפעילות תשתיות תקשורת ובנוסף הן מספקות ללקוחותיהן שירותי תקשורת שונים. כלומר, חברות התקשורת משרתות שני שחקנים מרכזיים שהאינטרסים הבסיסיים שלהם מנוגדים בתכלית: מחד גיסא, המשווקים והמפרסמים, ומאידך גיסא, לקוחותיהן, משתמשי הקצה, שהם גם הנמענים של המסרים השיווקיים.

המצב המשפטי בזירת הספאם

10. לספאם יש הגיון כלכלי משלו, והכללים המשפטיים מנסים לעקוב אחריו. נורמות כלכליות משולבות בנורמות משפטיות.

11. ההסדר המשפטי בישראל, על התיקונים השונים שחלו בו במהלך חמש עשרה השנים האחרונות, מטיל אחריות בעיקר על מועני המסר, תוך שהוא מחריג את מי שעוסק בהפצת מסרים. מנגנון האכיפה העיקרי הוא של הפרטת האכיפה, כלומר מתן אפשרות ליחידים שנפגעים לתבוע בעצמם. החוק מאפשר פיצוי סטטוטורי, ובצידו, אפיק של תובענה ייצוגית.

12. ההסדר המשפטי הקיים מצליח להתמודד עם חלק מהסוגיות, בכך שהוא נותן כלי משפטי אפקטיבי למדי בידי הנפגעים, מול בעלי העסקים המשווקים את עסקיהם, ובעיקר – מול הלגיטימיים שביניהם, אבל למרות זאת, עדיין מתעוררים קשיים ואתגרים ניכרים.

13. האתגרים העיקריים של ההסדר המשפטי הם: התמודדות עם ספקיות התקשורת ועם שאלת אחריותן להפצת ספאם, על רקע העובדה שספקיות משרתות שחקנים בעלי אינטרסים סותרים; קושי בזיהוי גורמים מפרים,

שמוביל לשימוש-חסר בכלים משפטיים; מכשולים בפני תמריצים כלכליים יעילים; אי-אחידות במידת האוריינות המשפטית והטכנולוגית של נפגעים; עוינות מצד המערכת המשפטית לתביעות ספאם; תחולה צרה מדי של החוק לעניין הגדרת "מפרסם" ו"דבר פרסומת".

הזירה הטכנולוגית

14. פרדיגמת המחקר של משפט וטכנולוגיה, מלמדת אותנו שהמשפט אינו בהכרח הפתרון היחיד או הראשון במעלה. בצד המשפט, יש גורמים מאסדרים אפשריים נוספים: נורמות חברתיות, נורמות שוק, והטכנולוגיה.

15. הנורמות החברתיות מתאימות פחות להסדרת יחסים בין גורמים מסחריים לבין צרכנים. הנורמות שחלות במרחב הזה הן נורמות שוק שונות. לספאם יש הגיון כלכלי משלו, והכללים המשפטיים מנסים לעקוב אחרי הכללים האלה, לשבש את התמריצים של הספאמרים להפיץ דברי פרסומת לא רצויים, וליתן בידי הצרכנים תמריצים לתבוע, ולאכוף את הדין בעצמו. הכלי האחרון הוא הטכנולוגיה. מטבע הדברים, הטכנולוגיה היא זו שיוצרת את הבעיה מלכתחילה, בכך שהיא מאפשרת הפצה מהירה, זולה ופשוטה של הודעות, שלא כולן רצויות; והקושי הוא לבדל בין הודעה רצויה להודעה לא רצויה, וזאת, לאורך החוליות השונות של שרשרת הספאם.

16. כל עוד ספאם הוא עסק רווחי מספיק, איננו עומדים לחזות בקץ התופעה בקרוב.

17. בעוד שמרוץ החימוש סביב הספאם בדוא"ל אכן הגיע לסטטוס קוו בעת הזו, באפיקי ספאם נוספים, כמו שיחות טלפוניות או הודעות טקסט, המצב רחוק מלהיות מאוזן.

18. בנוגע לספאם בדוא"ל, בעשורים האחרונים, מסנני דוא"ל הוכיחו את עצמם ככלי יעיל ביותר למניעת ספאם. עם זאת, בנוגע למסנני ספאם **ברמת השרת**, ההגנה על המשתמשים תלויה ברצון הטוב (כלומר באינטרס העסקי) של ספקיות השירות. בנוסף, כל עוד שירותי הגנה כאלה אינם ממומנים על ידי המדינה, התחרות בשוק נוטה לטובת החברות הגדולות ומעלה את רף הכניסה לשוק.

19. בנוגע למסנני ספאם **ברמת המשתמש**, פערים משמעותיים באוריינות דיגיטלית בין משתמשים שונים מצביעים על כך שפתרונות כאלו אפקטיביים רק עבור פלח קטן של האוכלוסייה.

20. בנוגע לספאם בהודעות טקסט, קיימות מספר שיטות סינון עיקריות עם אפקטיביות מוגבלת: **מסנני נפח**, שהאפקטיביות שלהם ירדה מעת שספאמרים למדו לעקוף אותם; **מסנני תוכן ישיר**, שמנתחים את נתוני ההודעה ואת תוכנה. מסננים אלה מתקשים להתמודד עם מיעוט המידע בהודעות טקסט, עם סימנים מיוחדים וקיצורים שמאפיינים הודעות כאלה, ועם מיעוט התוכן בכותרת ההודעות; **מסנני תוכן שיתופי**, שמבוססים על דיווחי משתמשים. אפקטיביות של מסנן כזה תלויה בכמות המשתתפים ובאיכות הדיווח. בנוסף לקשיים אלה, לספקיות השירות יש אינטרסים סותרים: מצד אחד הן מבקשות להגן על לקוחותיהן מפני ספאם, אך מהצד השני כל חסימה של מקור ממנו נשלחות הודעות רבות תעלה להן בהפסד כלכלי.

21. שיחות קוליות מאתגרות אף יותר מהודעות טקסט. קשה ליישם טכניקות פשוטות נגד ספאם בשיחות קוליות, ואתגרי המערכת האקולוגית הטלפונית דורשים היערכות מסוג שונה מההיערכות שנדרשה לקראת ספאם בדוא"ל או בהודעות טקסט. האתגרים הייחודיים, טכנית ורגולטורית, של ספאם באמצעות טלפון אותם מנינו הם: אילוצי מידיות; קושי טכני עם עיבוד שמע; היעדר נתוני כותרת (header); קושי בהשגת הסכמה של משתמשים לשימוש במערכת אנטי-ספאם; זיוף זהות המתקשר; קושי טכנולוגי במעקב אחר שיחות ספאם ומקורן; ניצול נקודות תורפה של מערכת ישנה, כמו למשל היעדר יכולת לאמת את זהות המתקשר. בנוסף, הרגולציה אינה אפקטיבית בשל מחסור בתמריצים כלכליים לתעשייה להשתתף במאמץ נגד הספאם. פתרונות חדשים כמו מאגר "אל תתקשר אליי" או יישומוני צד שלישי לחסימת תכנים, אף הם אינם חפים מקשיים.

22. בנוגע לספאם ברשתות חברתיות, מרוץ החימוש הטכנולוגי בעיצומו. פתרונות סינון עכשוויים מתמקדים בניסיון לאפיין ולזהות את השולח ולא בתוכן ההודעה.

השילוב בין משפט וטכנולוגיה בזירת הספאם

23. "**הנדסת ניקיון**" הוא השם הכולל לפתרונות המשלבים חשיבה משפטית וטכנולוגית, ומבקשים להתערב בנעשה בזירה בטרם מעשה (ex ante). פתרונות אלה מקדמים הטמעה מראש של עקרונות וערכים רצויים בטכנולוגיה

שנועדה להתמודד עם ספאם, עוד בשלבי העיצוב הטכנולוגי. להנדסת הניקיון שני מרכיבים, האחד, הוא הרעיון של השפעה משפטית על תכנון המערכות (וזו ה"ההנדסה"), והשני, הוא מרכיב הניקיון. זו מטפורה מארגנת, שמסייעת לנו להאיר היבטים שנותרו סמויים עד כה.

24. "הנדסת-ניקיון", או הנדסה-מראש של פתרונות טכנולוגיים המתמודדים עם ספאם, מסיטה את כובד המשקל ממשתמשת-הקצה אל המפתחת. במקום שהמשתמשת תנסה לאתר פתרונות בעצמה, הטכנולוגיה תעוצב מראש כך שהפגיעה תמוזער. באופן זה, ההגנה מפני ספאם אינה תלויה באוריינות הדיגיטלית של המשתמשת, וכך גם נמנעים קשיים בדיעבד. הדבר דומה לניקיון: כל אדם דואג לניקיון ביתו שלו, אבל יש לנו מערכות ציבוריות שנועדו לדאוג לניקיון המרחב הציבורי והשירותים הציבוריים השונים.

25. בדומה לזירות טכנולוגיות נוספות, להנדסת ניקיון יש סיכוי טוב יותר להצליח במגזר הציבורי. לפיכך, המלצנו לפעול בתחום זה ראשית במגזר הציבורי, ורק לאחר שייצבר ידע מספיק לנסות ולהטמיע את המסקנות בבנייה מוקדמת של טכנולוגיות במגזר הפרטי.

תוכן עניינים

תמצית המלצות הדוח 3

תקציר הדוח 5

תקציר מפורט 6

פרק א: מבוא 12

1. מבוא: המלחמה בספאם 13
   א. הגדרת הספאם 13
   ב. כלכלת הספאם 14
   ג. שחקנים, שיקולים ואינטרסים 15
2. מיקוד 18
3. שיטת המחקר 19
4. מפת דרכים 20

פרק ב: ספאם ואנטי-ספאם כמערכת אקולוגית סבוכה: השחקנים 21

1. מבוא 22
2. צד המוען: שרשרת הערך של הספאם 23
   א. כללי 23
   ב. בעלי המסר 26
   ג. גורמים מסייעים *לפני* ההפצה 29
   ד. גורמים מסייעים *בשלב* ההפצה 30
3. צד הנמענים: המלחמה בספאם 32
   א. המדינה 32
   ב. הציבור (משתמשי קצה) ומייצגיו (עמותות הפועלות נגד ספאם) 35
   ג. גורמים פרטיים 37
   ד. הזירה הבין-לאומית: רשימות שחורות, אגודות בין-לאומיות ללוחמה בספאם 39
4. גופי ביניים: ספקי תשתית ושירותים מקוונים 40
5. סיכום 42

פרק ג: דיני הספאם 44

1. מבוא 45
2. דיני הספאם בישראל: תמונת מצב עכשווית 46
   א. הגדרות החוק ותחולתו 46
   ב. תיקוני החקיקה 47
   ג. מגמות בפסיקה 49
3. מנגנוני אכיפה: תמונת מצב בשטח 51

א. מנגנון ראשון: תביעה אישית ותביעות בהליכים מקוצרים 51
ב. מנגנון שני: תובענה ייצוגית 52
ג. מנגנוני הסדרה נוספים 53
4. פתרונות משפטיים בעולם ומידת התאמתם לישראל 54
5. ניתוח: הישגים, כשלים ופתרונות 59
6. סיכום 62

פרק ד: טכנולוגיות אנטי-ספאם 64
1. מבוא: מרוץ חימוש אינסופי 65
2. טכנולוגיות מרכזיות בשימוש 66
א. ספאם ואנטי ספאם בדוא"ל 67
ב. ספאם ואנטי ספאם בהודעות טקסט למכשירי הטלפון 70
ג. ספאם ואנטי ספאם בהודעות קוליות 71
ד. ספאם ואנטי ספאם בפלטפורמות חברתיות 75
ה. פתרונות טכנולוגיים: הדור הבא 76
3. סיכום 77

פרק ה: ספאם, זבל, והנדסת ניקיון 79
1. מבוא: משפט וטכנולוגיה בזירת הספאם 80
2. התערבות משולבת: לפני ואחרי מעשה 80
א. פתרונות לפני מעשה (*ex ante*): הנדסת ניקיון 80
(1) הנדסה ערכית 81
(2) מטפורת הניקיון 81
ב. פתרונות לאחר מעשה (*ex post*): "ספאם אוף" כמשל 85
3. הטלת חבות משפטית: שחקנים אפשריים 86
א. שחקנים בשרשרת הערך 87
(1) שלב ראשון – בעלי המסר 87
(2) שלב שני: גורמים מסייעים לפני ההפצה 88
(3) שלב שלישי: גורמים מסייעים בשלב ההפצה 90
(4) שלב רביעי: הנמענים והשחקנים שאמונים על הגנתם 93
5. סיכום 95

ספאם: מילון מונחים וקיצורים 99
רשימת קיצורים 102

פרק א | **מבוא**

1. מבוא: המלחמה בספאם **13**

א. הגדרת הספאם 13

ב. כלכלת הספאם 14

ג. שחקנים, שיקולים ואינטרסים 15

2. מיקוד **18**

3. שיטת המחקר **19**

4. מפת דרכים **20**

1. מבוא | המלחמה בספאם

חוק הספאם הישראלי (סעיף 30א לחוק התקשורת (בזק ושידורים), התשמ"ב-1982) שמטרתו צמצום הפצת דואר זבל (ספאם) נכנס לתוקפו לפני 15 שנה, בשלהי שנת 2008. בהמשך, על רקע הטענה שישראל היא אחת מהשיאניות העולמיות בבעיית דואר הזבל ולאור הכרה גוברת בנזקי התופעה, קודמה חקיקה נוספת.[1] לאורך השנים, במענה לשינויים טכנולוגיים הן בדרכי הפצת ספאם והן בדרכים למניעתו, ובמענה לפרקטיקות עסקיות חדשות, תוקנה החקיקה מעת לעת. עם זאת, בעיית הספאם לא מוגרה. כדי להציע מענה מעודכן לעת הזו, נדרשת הבנה מעמיקה של ההתמודדות עם בעיית הספאם, ובחינה מקיפה של הפתרונות הקיימים, הן המשפטיים והן הטכנולוגיים, וזאת כדי לאתר את הכשלים הקיימים. דוח מדיניות זה ממפה את השחקנים המרכזיים השונים הפועלים בתוך המערכת האקולוגית של הספאם, מנתח את האינטרסים השונים שלהם, ומציע סקירה וניתוח שיטתיים של מפת השינויים בנושא הספאם מעת חקיקת חוק הספאם הישראלי ועד היום, הן בזירת החקיקה והפסיקה, והן בזירה הטכנולוגית, מצביע על כשלים אחדים, ומציע הצעות מדיניות בהתאם.

מבחינה משפטית, בחמש עשרה השנים שחלפו מעת חקיקת חוק הספאם, הוגשו רבבות תביעות לערכאות השונות בבתי המשפט בישראל, ולאורך השנים תרמו בתי המשפט את חלקם בפרשנות החוק ובעיצובו. הדוח ממפה ומנתח את מסלולי האכיפה המשפטיים הקיימים ואת יעילותם בפועל. שיטת האכיפה המרכזית בחוק הישראלי היא הפרטת אכיפה בדרך של אפשרות לתביעה אישית (בדרך כלל תביעה קטנה) עם פיצוי סטטוטורי, ובצידה מסלול של תובענה ייצוגית. בצד הדיון המשפטי, הדוח סוקר באופן שיטתי את הפתרונות הטכנולוגיים המרכזיים שהוצעו ויושמו עד כה במאבק בספאם, וממפה אותם בהתאם לפונקציה הטכנולוגית שלהם, בהתאם לנקודת ההתערבות שלהם במערכת זרימת המידע, ובהתאם ליעילותם בפועל. בהסתמך על אלה, הדוח בוחן את תופעת הספאם במבט רחב, באופן המיטיב לזהות קשיים ואתגרים, ומציע דרכי פעולה אפשריות לשם שיפור המענה המשפטי-טכנולוגי.

פרק זה פותח בהגדרת עבודה לספאם, ממשיך בתיאור כלכלת הספאם, ועובר למיפוי ראשוני של הזירה על השחקנים השונים והאינטרסים והזכויות שלהם. מסקנת הביניים היא שכלכלת הספאם בעידן הדיגיטלי היא מערכת טכנולוגית-עסקית סבוכה ומרובת שחקנים, שלהם אינטרסים שונים ומגוונים, שלעיתים מתלכדים עם האינטרסים של שחקנים אחרים ולעיתים סותרים אותם. במובן זה, כלכלת הספאם יוצרת מערכת אקולוגית מורכבת. מכאן, שיש לפצח את המערכת הזו, כדי להיטיב ולהסדירה.

א. הגדרת הספאם

היסטורית, הדוגמה הראשונה לספאם דיגיטלי היא דואר אלקטרוני (דוא"ל), שעדיין מככב כסוג התקשורת שסביבה התפשטות תופעת הספאם וקנה המידה שלה גדולים במיוחד.[2]

בראשית שנות האלפיים, עם עלייתן של הרשתות החברתיות והצלחתן, הופיעו צורות חדשות רבות של ספאם. החוק הישראלי קובע איסור על שיגור דבר פרסומת באמצעי תקשורת שונים כמו הודעות טקסט (סמס – short message service), דוא"ל ומערכות חיוג אוטומטי. בהתאמה, אפיקי התקשורת המרכזיים בהם עוסק דוח זה הם דוא"ל, יישומי העברת מסרונים ותוכנות להעברת מסרים מידיים (כגון וואטסאפ), הודעות שנשלחות ישירות למכשיר הנייד באמצעות רשתות חברתיות כגון פייסבוק או X (לשעבר טוויטר); וכן שיחות קוליות, מוקלטות או לא מוקלטות.

כל אפיק תקשורת מאפשר, בצד תקשורת רצויה לנמען, גם תקשורת שאינה כזו. **"ספאם" הוא הכינוי למסר שנשלח אל הנמען באמצעים שונים, ללא הסכמתו המוקדמת, ובניגוד לרצונו, ומהווה בשל כך מטרד**. קשה למצוא בדין או בספרות הגדרה חובקת-כל של "ספאם", משום שלתופעה מגוון צורות והיא מתרחשת במערכות טכנולוגיות שונות. באופן רחב, וכהגדרת עבודה לצורך הדיון, נאמץ את הגדרתו של Emilio Ferrara, שלפיה, ספאם הוא "ניסיון להשתמש

1 ראו איגוד האינטרנט הישראלי, ניתוח נתוני עתק של תביעות דואר זבל אלקטרוני (ספאם) בישראל, בפרק המבוא. נמצא ב: https://www.isoc.org.il/research/spam-data-analysis.

2 דן חי **תורת המסר: בין דיוור ישיר לספאם** 84-85 (2012); Emilio Ferrara, *The History of Digital Spam*, 62.8 Communications Of The Acm 82 (2019).

לרעה במערכת טכנו-חברתית או לתמרן אותה על ידי ייצור תוכן לא מוזמן ו/או לא רצוי והזרמתו, במטרה לכוון את התנהגותם של בני אדם או של המערכת עצמה, לשם מתן יתרון ישיר או עקיף, מידי או לטווח ארוך, לספאמר(ים)."[3]

המושג משמש גם לתיאור דבר דואר מודפס מהסוג שמונח בתיבות הדואר שלנו בפתח הבית או הבניין, אך דוח זה עוסק בספאם אלקטרוני בלבד. בקטגוריה של ספאם אלקטרוני נכללות מספר קטגוריות משנה, שמבחינות בין ספאם שמטרתו שיווק מוצרים ושירותים, וספאם שמטרתו דייג (פישינג) של פרטים אישיים לשם הונאה, או פגיעה במחשבי משתמשים באמצעות שתילת נוזקות. דוח זה אינו עוסק בקטגוריה האחרונה אלא בשולי הדברים, ומתמקד בספאם שמטרתו שיווק מסחרי. ההבחנה החשובה כאן היא בין ספאם לבין דיוור ישיר של משווקים ומפרסמים לגיטימיים, כפי שיובהר בהמשך.

במשפט הישראלי, הגדרת הספאם מופיעה בסעיף 30א(ב) לחוק התקשורת, האוסר על "מפרסם" לשלוח "דבר פרסומת" לנמען ללא הסכמתו המפורשת מראש. "דבר פרסומת" הוא מסר מסחרי שנועד לעודד רכישה של מוצר, ו"מפרסם" הוא מי שנהנה מפירות הפרסום. החוק תוקן שלוש פעמים במהלך השנים, כך שהוא חל גם על חומרי תעמולה, על בקשות תרומה, ועל מסרים הכוללים הצעה ליצירת תקשורת עם המפרסם לקבלת מסר מסוים.[4]

האיסור על משלוח "ספאם" שקבוע בסעיף 30א לחוק התקשורת מובחן מההוראות הקשורות ל"דיוור ישיר" בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות"). ראשית, סעיף 17ג לחוק הגנת הפרטיות מגדיר "דיוור ישיר" כ"פניה אישית לאדם, בהתבסס על השתייכות לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע." לעומת זאת, דואר זבל בדרך כלל אינו מופנה באופן אישי לנמען, והוא אינו מבוסס בהכרח על מאפייני הנמען או על השתייכותו לקבוצה. להיפך. דואר זבל נשלח בכמות גדולה, באופן גורף, ללא אבחנה בין הנמענים (bulk).

כמו כן, במקרים רבים שיגור ספאם אינו מסתמך על רשימות נמענים העונות להגדרת "מאגר מידע" שבחוק הגנת הפרטיות, למשל משום שהן רשימות אקראיות של כתובות, ללא אפיון מוגדר של פרטים ברשימה.[5] אולם כפי שנראה בפרקים הבאים, קיימים הבדלים נוספים בין הגדרת הספאם להגדרתו של דיוור ישיר בחוק הישראלי,[6] הבאים, העידן הדיגיטלי, על ריבוי גורמי הביניים שלוקחים חלק בשרשרת ההפצה של מסרים אלקטרוניים, הביא במקרים רבים לטשטוש הגבולות בין דיוור ישיר לגיטימי לבין ספאם, ולקושי ממשי להבחין בין השניים.

> בהתאם, בדוח זה ספאם מוגדר כ:
>
> **מסר פרסומי המופץ באמצעים אלקטרוניים באופן המוני וללא הסכמה מפורשת מראש של הנמען**

ב. כלכלת הספאם

פרסום מבוסס ספאם הוא עסק; תעשיית הספאם ממשיכה להתקיים משום שהיא מפעל רווחי. כלכלת הספאם בעידן הדיגיטלי היא בפועל מערכת אקולוגית-טכנולוגית-עסקית סבוכה ומרובת שחקנים, שלכל אחד מהם אינטרסים שונים ומגוונים, שלעיתים מתלכדים עם האינטרסים של שחקנים אחרים ולעיתים סותרים אותם. המטרד שיש בספאם מביא מטבע הדברים למיקוד בנמענים, אולם זהו רק קצה הקרחון. כאשר אנו מתמקדים רק במשלוח המסר אל הנמען, אנו

---

3 "[t]he attempt to abuse of, or manipulate, a techno-social system by producing and injecting unsolicited, and/or undesired content aimed at steering the behavior of humans or the system itself, at the direct or indirect, immediate or long-term advantage of the spammer(s)", ראו: Ferrara, *The History of Digital Spam*, ibid, at 84.

4 החוק תוקן באוגוסט 2016 באופן שיאפשר את תחולתו על בקשות תרומה ועל תעמולה (בסייגים מסוימים). ראו חוק התקשורת (בזק ושידורים) (תיקון מס' 63), התשע"ו-2016. במאי 2018 תוקן החוק באופן שמרחיב את הגדרת המושג "דבר פרסומת", כך שיכלול גם את תופעת ה"צנתוק", כלומר משלוח מסרים חלקיים לנמען תוך עידודו להתקשר למספר ממנו התקבלה ההודעה, ובכך לאלצו לקבל מסרים פרסומיים. ראו חוק התקשורת (בזק ושידורים) (תיקון מס' 72), התשע"ח-2018.

5 ס' 7 לחוק הגנת הפרטיות, התשמ"א-1981, מגדיר מאגר מידע כך: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט - (1) אוסף לשימוש אישי שאינו למטרות עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".

6 ראו בהרחבה חי **תורת המסר**, לעיל ה"ש 2, בעמ' 21-27.

מתמקדים רק בחלק הגלוי של מיזם גדול ורב פנים; בפועל, מערך שלם של שחקני ביניים ומשאבים משמש כדי לייצר רווח משליחת ספאם.

בשל העלויות הנמוכות של דיוור אלקטרוני המוני (עם הבדלים בין אופני השיגור ואפיקי התקשורת השונים) ובשל זמינותו הגבוהה, תופעת הספאם נפוצה ביותר. מצד שולחי המסרים, די באחוז קטן של משתמשים שייענו להצעה שיווקית, כדי שהמהלך ישתלם. הפצת ספאם היא דרך יעילה ופשוטה מאוד להגיע באופן כמעט מידי לכמות עצומה של נמענים בלחיצת כפתור, ובעלויות נמוכות מאוד, העלות השולית של משלוח הודעה נוספת פוחתת. כלכלת הספאם מעודדת משלוח עוד דוא"ל שיווקי, גם אם רבים מהנמענים לא מתעניינים בו. הכמות היא שם המשחק.

מסיבה זו, לא רק מפרסמים משתמשים בשיטה זו, אלא גם פוליטיקאים, וגם נוכלים למיניהם שמבקשים "לדוג" פרטים אישיים של משתמשים או לשתול וירוסים זדוניים במכשיריהם. אזרחים וצרכנים ("משתמשים", בשפת האינטרנט) חשופים באופן יומיומי ומתמיד לתכנים שמגיעים אליהם באמצעות מגוון אפיקי תקשורת דיגיטלית. בעידן המידע, תשומת הלב של הפרט הפכה למשאב רב ערך, ועבור מי שמתחרים על תשומת לב זו, כל משתמשי האינטרנט הם מטרות נוחות. לדוגמה, בשנת 2022 הופצו מדי יום כ-14.5 מיליארד הודעות ספאם בעולם, כלומר בין 45% ל-73% מכלל הדואר האלקטרוני היומי העולמי היה ספאם.[7]

מדובר בהפרעה משמעותית לשימוש באמצעי התקשורת האלקטרוניים, ובנזקים הן למשתמשי קצה והן לספקיות שירותי האינטרנט; מבחינת המשתמש – אובדן זמן ותשומת לב בסינון מסרים,[8] חשיפה לתכנים פוגעניים,[9] סיכון ליפול בפח של נוכלים, ואף הימנעות משימוש במערכות אלקטרוניות על מנת להימנע מהטְרדה. מבחינת ספקיות שירותי הגישה לאינטרנט, מדובר בהכבדה ארגונית וכלכלית, בשל הצורך להגדיל את כוח המחשוב בשל עומסי מסרים, ולעיתים עלולה להיות להן אחריות משפטית כלפי משתמשי הקצה בגין המסרים שמגיעים אליהם דרכן. לאורך השנים התפתחו מסלולים שונים של התמודדות עם תופעת הספאם, במיוחד באמצעים משפטיים וטכנולוגיים.

בהתאם, בשל מבנה כלכלת הספאם, שמעודדת משלוח דוא"ל לא רצוי בהיקפים גדולים, תוך החצנת העלויות לנמענים ולספקי השירות, ולעיתים תוך ניצול לרעה של גורמים עוינים למשתמשים, הפן הכלכלי של הספאם משמעותי ביותר לשם התמודדות עם התופעה.

ג. שחקנים, שיקולים ואינטרסים

כאמור, הספאם היא תופעה מורכבת ורבת פנים. כדי להעריך את הפתרונות השונים לבעיה, עלינו להביא בחשבון טווח רחב של שיקולים ואינטרסים של גורמים רבים. לשם כך, יש למפות את השחקנים שמעורבים בתמונה. הזכרנו את שולחי הספאם, את הנמענים, וביניהם את ספקי השירות. התמונה מורכבת עוד יותר. בצד שמרוויח מספאם, שחקנים מרכזיים נוספים, מלבד המועינם, הם ספקי לִידִים (מלשון lead), שמספקים למשווקים את רשימות התפוצה; בעלי מאגרי מידע, שכוללים רשימות תפוצה; חברות הפצה שמספקות פלטפורמות להפצת תכנים שיווקיים במסות גדולות, שאינן בהכרח בעלות רישיון בזק; חברות תקשורת (בעלות רישיון בזק); ורשתות שותפים, שהן פלטפורמות שמקשרות בין גורמים העוסקים בפרסום בזירות טכנולוגיות שונות (השותפים), לבין בעלי עסק שמעוניינים לפרסם את עסקיהם.

7 Spam statistics and Facts, Spam Laws 2022, available at: https://www.spamlaws.com/spam-stats.html. נתוני הספאם משתנים כל העת. לאתר שמביא נתונים עדכניים בזמן אמת, ראו Cisco Talos Intelligence Group https://talosintelligence.com/reputation_center/email_rep#email-country-senders.

8 לדוגמה, סקר משנת 2004 העריך שעלות אובדן יעילות למשתמשי האינטרנט בארצות הברית מסתכמת ב-21.58 מיליארד דולר). מחקר משנת 2012 העריך את האובדן היעילות ב-14 מיליארד בשנה (על בסיס מידע מ-2010). ראו: Justin M. Rao & David H. Reiley, The Economics of Spam, 26 J. Econ. Persp., 87 (2012), 99-100. דיווח מ-2023 מדבר על עלות של 20.5 מיליארד, ראו ס' 9 ל, "What's On the Other Side of Your Inbox – 20 SPAM Statistics for 2023" **Dataprot** (2023) נמצא ב: https://dataprot.net/statistics/spam-statistics.

9 קטגורית הספאם השנייה בשכיחותה קשורה לתכנים "למבוגרים" והיא מהווה בערך 31.7% מכלל הספאם. הסוג הנפוץ ביותר של דואר זבל קשור לפרסום, והוא מהווה כ-36% מכלל הודעות הספאם; שם.

בצד שעניינו המלחמה בספאם, שחקנים מרכזיים הם המדינה, שהיא שחקן רב גופים ופנים; הציבור, שהוא הנפגע המרכזי מתופעת הספאם; גופים פרטיים מסוגים שונים שפועלים למיגור התופעה; ושחקנים שונים בזירה הבין-לאומית.

לכל אחד מהשחקנים זכויות ואינטרסים שונים, שאותם נתרגם לשיח המשפטי.

ראשית, לאזרחים ולצרכנים עומדת זכותם לפרטיות והזכות להגנה מפני מטרדים. שנית, מכיוון שמדובר במסרי תקשורת, הרי שמעבר להגנה על פרטיות הנמענים, חשוב לזכור שפרסום לגיטימי נהנה מהגנת חופש הביטוי המסחרי (וקל וחומר הפוליטי, כאשר מדובר במסרים לא מסחריים). שלישית, מכיוון שמדובר במסרים שיווקיים, זכויות נוספות נכנסות לתמונה: זכויות הקניין וחופש העיסוק של גופים מסחריים, קטנים כגדולים, הזקוקים לפעול בתחום השיווק על מנת לקיים את עסקיהם באופן רווחי.

בתוך כך, לפעילות בזירה המקוונת יש ייחוד משלה, ושיקולים נוספים שיש להביא בחשבון. כחלק מהגנה וטיפוח פעילות איכותית בזירה המקוונת, יש להגן על האינטרסים של ספקיות שירות, הן בתחום התשתיות והן בתחום הפעילות באינטרנט. זו משימה לא פשוטה, משום שחברות המספקות שירותים ותשתיות מספקות אותן הן לשולחי מסרים והן למקבליהם. ספקי השירות מצויים בצומת שמחייב לעיתים הכרעה בין אינטרסים של הגנה על ביטוי לעומת אינטרסים של פגיעה בפרטיות (למשל, אחריות לתכנים מצד ספקיות שירות עשויה להביא לאחריותן לחשוף שמות משתמשים ובכך להפר את פרטיותם).[10] כמו כן, מכיוון שזירת הפעילות של תעבורה דיגיטלית היא הרשת המקוונת העולמית, קיימים שיקולים הנוגעים לשיתוף פעולה בין-מדינתי לשם הגנה על הזירה המקוונת מפני תעבורה לא רצויה.

טבלה א.1 מסכמת את השיקולים המרכזיים שיש להביא בחשבון בבואנו להעריך פתרונות מדיניות משפטיים וטכנולוגיים שמטרתם מיגור תופעת הספאם.

---

10 זאת בהתאם להלכת רמי מור: רע"א 444/07 **מור נ' ברק אי. טי. סי. (1995) החברה לשירותי בזק בינלאומיים בע"מ,** פ"ד סג(3) 664 (2010). מנגד ראו ת"א (שלום, פ"ת) 48690-01-23 **כהן נ' טלזר 019 שרותי תקשורת בינלאומיים בע"מ** (נבו 21.5.2014), שם התקבלה בקשת התובע לחשיפת הגורם העומד מאחורי המסרונים שנשלחו בעניינו.

טבלה א.1.: שחקנים מרכזיים בזירת הספאם

השחקן	אינטרסים	זכויות	חובות
מפרסמים: לגיטימיים ספאמרים מקצועיים	שיווק ומכירה חלוקת נטל החבות המשפטית עם שחקנים נוספים בידול ומאבק בספאמרים שמטרתם הונאה שימוש ברשת שותפים שתסווה את פעילותו	זכות קניין חופש עיסוק חופש הביטוי המסחרי	ציות להוראות חוק הספאם וחוק הגנת הפרטיות
ספקי לידים בעלי מאגרי מידע	להתפרנס ממסחור מאגרי מידע שברשותם חלוקת נטל החבות המשפטית עם שחקנים נוספים		ציות להוראות החוק [אם הוא חל] בדבר ניהול מאגר
חברות הפצה	בירור אופי פעילות הלקוח, "תפיסת" ספאמרים הימנעות מתיוג שלילי		
המדינה	קיום תשתית מקוונת תקינה שירותים מקוונים ברמה טובה איכות טובה של פעילות בזירה המקוונת הגנה על עובדי חברות הפצה ושיווק הגנה על המערך המקוון של המדינה מפני ספאם השתתפות בהגנה על הזירה המקוונת הגלובלית		הגנה על זכויות האזרחים הגנה על שחקני שוק
הציבור הרחב	קבלת מסרי תקשורת רצויים, אי-קבלת מסרים לא רצויים אוריינות דיגיטלית	חופש ביטוי פרטיות הגנה מפני מטרד	
חברות תקשורת	מול משתמשי קצה: מתן שירותים מיטביים, לרבות תקשורת "נקייה" מהפרעות מול מפרסמים: הגדלת היקפי הפרסום	זכאות לפטור מאחריות על תכנים	הגנה על פרטיות מידע של משתמשים הגנה על אינטרסים משותפים לחברה ולשותפיה העסקיים

2. מיקוד

לשם מיקוד הדיון ומיקום הסוגייה במכלול הרחב יותר, נדגיש כמה היבטים לפני הפירוט.

ראשית, המיקוד בדוח הנוכחי הוא המשפט הישראלי. נדון מעת לעת בשיטות משפט זרות ובכלים שהנהיגו למאבק בספאם, כדי להבין את סל הכלים המשפטי האפשרי וכדי לחדד כמה סוגיות, ובהמשך נבחן אמצעים טכנולוגיים שונים, לשם לימוד על אופני התמודדות שונים. במקרה של פתרונות שהצליחו במקומות אחרים בעולם, נבחן את מידת התאמתם לזירה המקומית. אולם המיקוד פה הוא המשפט והחברה הישראליים.

שנית, הדוח עוסק בספאם צרכני בעיקרו, ובפן האזרחי שלו. לא נעסוק בהודעות פוליטיות (אם כי נזכיר אותן, לפי הצורך). כמו כן, בדוח זה לא נדון בפעילות פלילית מובהקת כמו למשל ספאם שמטרתו מכירת סמים לא חוקיים, או ספאם שמטרתו הונאה, אלא רק מקום שדיון כזה נחוץ לשם השוואה.

שלישית, דוח זה מתמקד בממשק שבין המשפט לטכנולוגיה ולפיכך, בצד בחינה פרטנית של סל הכלים המשפטיים וסל הכלים הטכנולוגיים, נבחן את החפיפה בין הפתרונות השונים ואת השפעותיהם ההדדיות. כל טכנולוגיה למלחמה בספאם מעוררת קשת של שאלות משפטיות. במקביל, פתרונות משפטיים משפיעים על עיצוב טכנולוגיות הספאם וטכנולוגיות האנטי-ספאם. בחינת הממשק שבין הפתרונות השונים, המשפטיים והטכנולוגיים, תאפשר הבנה טובה ומלאה יותר של המערכת האקולוגית של הספאם. בהתאם לכך היא תאפשר לקובעי מדיניות לשקול באופן מעמיק את הפתרונות השונים, הקיימים והמוצעים.

רביעית, מדובר במגוון טכנולוגיות ובמגוון אפיקי ספאם. הספרות התייחסה למגוון תופעות כאל ספאם.[11] הדגש כאן הוא על טכנולוגיות למלחמה בספאם בדוא"ל, במסרונים ובהודעות קוליות, שהם האפיקים שאליהם מתייחס הדין הישראלי במפורש. בשינויים המתחייבים, הדיון ניתן ליישום לטכנולוגיות אחרות, ובדוח נתייחס לצורות נוספות של ספאם לשם השוואה נקודתית, לפי הצורך. כמו כן, בעיצוב מדיניות יש להביא בחשבון טכנולוגיות חדשות שטרם זכו להתייחסות משפטית, אך השפעתן כבר ניכרת, כמו כלי בינה מלאכותית (Artificial Intelligence – AI), בהן משתמשים גם בטכנולוגיות ספאם ובטכנולוגיות נגד.

חמישית, לכל שימוש בטכנולוגיה יש היבטים חלוקתיים, ופערים לא-מקוונים בין אזרחים ואוכלוסיות עלולים להיות משועתקים לזירה המקוונת. בענייננו, חשוב לזכור שלא לכל האוכלוסייה יש מכשיר סלולרי או מחשב, ולאלו שיש – לא לכולם אוריינות טכנולוגית מספקת לשם הבנת פתרונות שונים ויישומם.[12] בנוסף, גם הגישה למשפט בכלל ולערכאות דיוניות בפרט, אינה נחלקת באופן שוויוני בין אוכלוסיות שונות. בעיצוב מדיניות כוללת יש להביא בחשבון את הפריסה הלא אחידה של טכנולוגיות חסימה שונות, את הרמות השונות של פגיעות אצל אוכלוסיות יעד שונות, את הפערים באוריינות הדיגיטלית של משתמשי הטכנולוגיות, ואת הפריסה הלא אחידה של הגישה לערכאות, ולשקול שיקולים אלה במכלול השיקולים בהתמודדות עם בעיית הספאם.

11 המרכזיות שבהן הן (א) תמרון מנועי חיפוש, כלומר העלאה של מיקום אתר מטרה במנועי חיפוש, באמצעות אלגוריתמי גיימינג; (ב) ספאם וויקי (החדרת לינקים לספאם לתוך עמודי וויקיפדיה); (ג) ספאם של ביקורות ודעות (קידום או השמצה של מוצרים באמצעות ביקורות מזויפות אונליין); (ד) בוטים חברתיים (חשבונות שמופעלים באמצעות תוכנה במטרה ליצור אינטראקציות בקנה מידה גדול עם משתמשי רשתות חברתיות); (ה) אתרי חדשות מזויפים (שנועדו להפיץ במכוון דיסאינפורמציה); (ו) ספאם-מולטימדיה המבוסס על בינה מלאכותית. לסקירה מקיפה, ראו פררה, לעיל ה"ש 3.

12 בשנת 2015, מספר הטלפון הניידים בישראל הוערך בכ-9.6 מיליון מכשירים, יותר ממספר התושבים באותה העת (8.6 מיליון). ראו איגוד האינטרנט הישראלי, אינטרנט בחברה הערבית בישראל: *תמונת מצב ראשונית והמלצות מדיניות* (18.10.2018), בעמ' 7: https://www.isoc.org.il/public-action/digital-gap/the-internet-in-arab-society-in-israel. בשנת 2023, ההערכה היא שבישראל יש 10.65 מיליון **חיבורים סלולריים**. ראו: Simon Kemp, “DIGITAL 2023: Israel”, Datareportal (13.2.2023): https://datareportal.com/reports/digital-2023-israel.

3. שיטת המחקר

המחקר ממוסגר בפרדיגמת המחקר של "משפט וטכנולוגיה", שעֵרה לקשר המורכב שבין משפט לטכנולוגיה. לפיה, הטכנולוגיה עצמה אינה נתפסת כבעיה, ולעיתים היא אף יכולה להיות הפתרון.[13] גישה זו גורסת שהמשפט לבדו, או הטכנולוגיה לבדה, אינם יכולים למגר את תופעת הספאם. גם בספרות המחקרית בנושא, משתרשת ההבנה שעל מנת להתמודד עם התופעה באופן אפקטיבי נדרש שילוב של כלים טכנולוגיים עם מדיניות משפטית עדכנית.[14] כך, בנוסף על בחינת טכנולוגיות ספאם ואנטי ספאם קיימות, הדוח מתחקה אחר ההיסטוריה המשפטית של החקיקה והפסיקה בישראל, תוך בחינה של מסלולי אכיפה קיימים. המטרה היא לחלץ סוגי פתרונות אפשריים, ולהבין את אופן פעולתם.

הדוח מסתמך על מסגרת רעיונית שפיתחנו בדוח מדיניות קודם, שבה טענו שכדי להבין את ההיבטים המשפטיים של מערכות המבוססות על מידע, יש ללמוד אותן בתוך ההקשר הרחב שבו הן פועלות.[15] סביבות המידע הן סביבות מורכבות, מרובות זרמי מידע ומרובות שחקנים המעורבים בזירת הספאם. בהתאם, **הדוח ממפה את השחקנים השונים ואת האינטרסים שלהם, וכן ממפה את זרמי המידע במערכות כאלה, על מנת לאתר את אותן הנקודות במערכת שבהן התערבות רגולטורית או טכנולוגית תהיה מיטבית.**

הדוח בוחן צורות שונות של "הנדסת ניקיון", כלומר ההיתכנות של תכנון מוקדם של טכנולוגיה על מנת לסייע בשמירה על ניקיון המערכת האקולוגית התקשורתית, כדי לצמצם פעילות של דואר זבל לא חוקי.[16] הטמעת ערכים רצויים בטכנולוגיות עוד בשלב העיצוב, היא תוצאה מתבקשת של תובנות הגישה המחקרית של "משפט וטכנולוגיה".[17] בנוסף, בדרך של השוואה, הדוח סוקר את התמודדותן של מדינות נוספות עם הספאם, בתחום המשפטי והטכנולוגי, ומשווה זאת להתמודדות הישראלית. כך, נאיר הצלחות בולטות ונבחן את התאמתן לישראל, נצביע על פתרונות שנכשלו, ומדוע, כדי למנוע הליכה עתידית בדרכי חתחתים.

בהתאם, הדיון בדוח מבוסס על ניתוח משפטי של הדין בישראל – החקיקה הקיימת וההיסטוריה החקיקתית שלה, עיון בפסיקה הרבה ובמגמותיה, על ניתוח משפטי השוואתי, בצד לימוד הטכנולוגיה הרלוונטית – הן טכנולוגית ההפצה של הספאם והן טכנולוגיות-נגד, שמבקשות לחסום את הספאם בשלבים שונים של זרימת המידע. הניתוח ממוקם בפרדיגמת המחקר של "משפט וטכנולוגיה" שבוחנת מקרוב את הקשר ההדדי שבין הגורמים. בנוסף, ערכנו שיחות רקע עם מספר שחקני מפתח בזירת הספאם המקומית. שסיפקו לנו מידע רקע רב ערך מנקודות מבט שונות, מה שסייע לנו לכוון מבט לפינות פחות שגורות וללמוד לעומק את התופעה על מורכבותה.

---

13 ניבה אלקין-קורן ומיכאל בירנהק "הקדמה: משפט וטכנולוגיות מידע" **רשת משפטית: משפט וטכנולוגיות מידע** 11 (ניבה אלקין-קורן ומיכאל בירנהק עורכים 2011).

14 Roderic Broadhurst & Mamoun Alazab, *Spam and Crime*, in Regulatory Theory, Foundations And Applications 517, 527 (Peter Drahos, ed., 2017).

15 ראו מיכאל בירנהק ומיקי זר "עקרונות פעולה משפטיים לפיתוח טכנולוגיות לאיתור מגעים" (דוח מדיניות עבור משרד המדע והטכנולוגיה, 2020), נמצא ב: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3683166.

16 מטפורת ה"ניקיון" היא כלי מארגן שנועד להאיר היבטים שונים של תופעת הספאם (מהו "זבל" לא רצוי, מהו פרסום לגיטימי שאינו "זבל", מה נדרש על מנת "לנקות" את המערכת, וכדומה). מטפורת הניקיון, ככל מטפורה, עשויה לאפשר השוואות ולהבין היבטים חדשים של תופעה, אך ככל מטפורה יש לה מגבלות. למשל, לעיתים היא משרתת אינטרסים מסוימים אך מטשטשת אחרים. כחלק ממסקנות הדוח נבחן את היתרונות והחסרונות של השימוש במטפורת הניקיון.

17 ראו Mickey Zar & Niva Elkin-Koren, וגם Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (2011) *The By-Design Approach Revisited: Lessons from COVID-19 Contact Tracing Apps*, 33 Intell. Prop., Media & Ent. L.J. 635, 640-645 (2023). למקרים ספציפיים של הנדסת פרטיות ראו מיכאל בירנהק "הנדסת פרטיות ציבורית: המקרה של העברת מידע ממרשם האוכלוסין למפלגות" **דין ודברים** יב 15 (2019); מיכאל בירנהק "פרטיות במשבר: הנדסה חוקתית והנדסת פרטיות" **משפט וממשל** כד 149 172-176 (2022).

4. מפת דרכים

פרק ב ממפה את השחקנים השונים שמעורבים בשרשרת הערך של הספאם. הפרק מצביע על השחקנים השונים, מעבר למוען, לנמען ולספקי השירות שביניהם, מנתח את האינטרסים של השחקנים שפועלים בזירה הסוציו-טכנולוגית של הספאם, ומאתר באופן ראשוני את נקודות התורפה בשרשרת. החוליות החשובות בשרשרת הספאם הן המדינה (לרבות המערכת המשפטית וגופים שאמונים על הסדרה טכנולוגית), חברות שמספקות תשתיות אינטרנט, שירותי הפצת מסרים (דואר אלקטרוני, הודעות קוליות, הודעות טקסט) לרבות פלטפורמות של רשתות חברתיות, גופים פרטיים (מסחריים ולא מסחריים) שעניינם מלחמה בספאם, לרבות עורכי דין, יצרני טכנולוגיות אנטי-ספאם, משווקים, משתמשי קצה, ושחקנים שונים המעורבים בתעשיית הספאם, כמו חברות שקוצרות ומוכרות רשימות קשר, ומפעילי רשתות בוטים.

הניתוח נשען על התובנה שלפיה היעדר הבנה מלאה של שרשרת הספאם והשחקנים שמעורבים בה מביאה לכך שרוב ההתערבויות נגד ספאם מתמקדות רק בהיבטים מסוימים, למשל סינון דוא"ל או רשימות שחורות של כתובות אתרים, ומתעלמות מהיבטים אחרים, כמו השלב המקדמי של קצירת כתובות דוא"ל ומספרי טלפון, או שלב ביניים של שימוש בשירותי תיווך להפצת מסרים. הפרק מאתר ומצביע על צמתים בהם יש התערבות רגולטורית מספקת (ולעיתים התערבות-יתר), ועל הצמתים שסובלים מתת-התערבות. לגבי כל אחד מהשחקנים, נזהה את הזכויות והאינטרסים, ואת קשרי הגומלין בין השחקנים השונים והאינטרסים שלהם. במרכזו של הדיון עומדים צרכיו של הציבור, לפי קבוצות שונות של האוכלוסייה.

פרק ג מציג את הדין הישראלי הקיים בתחום זה, ואת הדרך שעבר עד היום. הפרק פותח בסקירת את תמונת המצב העכשווית, ולאחר מכן פונה לסקירת תמונת המצב בשטח. זו כוללת את מנגנוני האכיפה המשפטיים המרכזיים של חוק הספאם, שהם מסלול התביעה האישית ומסלול התובענה הייצוגית, וכן את ההתפתחויות המרכזיות בפסיקה בנוגע לספאם. לאחר מכן ננתח את החוק ואת התיקונים לחוק. הניתוח כולל בחינה של התפתחות החקיקה בראי השיקולים השונים, לעיתים הסותרים, שהביאו לעיצוב הדין, והאופן בו השפיעו אינטרסים שונים של שחקנים שונים, כפי שהוצגו בפרק ב, על עיצובו של הדין. בהמשך, הפרק בוחן את החקיקה המרכזית בתחום הגנת הפרטיות, בעיקר באיחוד האירופי (ה-GDPR) והשפעות אפשריות שלה על תופעת הספאם. בחלקו האחרון, סוקר הפרק פתרונות משפטיים נוספים שהוצעו או שנבחנו במדינות אחרות, ומנתח אותם ואת מידת התאמתם למצב המשפטי הקיים בישראל.

פרק ד סוקר ומנתח את מנגנוני האכיפה הטכנולוגיים המרכזיים בתחום הספאם, ומתאר את מרוץ החימוש האינסופי במאבק בין טכנולוגיות ספאם לטכנולוגיות אנטי-ספאם. הפרק בוחן את מנגנוני הספאם והאנטי-ספאם בנוגע לדואר אלקטרוני, למסרונים, ולשיחות קוליות, ובוחן את ההשלכות והאתגרים המשפטיים של הטכנולוגיות השונות. בהמשך, הפרק פונה לתיאור וניתוח זרמי המידע בזירת הספאם, שמטרתם לאתר נקודות תורפה הן מבחינת טכנולוגיות הספאם, והן מבחינת טכנולוגיות האנטי-ספאם.

פרק ה קושר את כל המרכיבים, ומציע דרכי פעולה לקובעי מדיניות. נבחן פתרונות שמשלבים חשיבה משפטית וטכנולוגית. ראשית, פתרונות טכנולוגיים מקדימים (ex ante), שנכנה "הנדסת ניקיון", כלומר הטמעת עקרונות וערכים רצויים בטכנולוגיה שנועדה להתמודד עם ספאם, עוד בשלבי העיצוב הטכנולוגי. שנית, פתרונות שמשלבים את המשפטי והטכנולוגי לאחר מעשה (ex post). נפתח בניתוח כולל של הממשק שבין משפט לטכנולוגיה בזירת הספאם. לאחר מכן, נציג את מטפורת הניקיון, שהיא מטפורה שמארגנת את השיח סביב הסדרת נושאים הקשורים לאשפה באופן כללי, ולספאם, כאשפה דיגיטלית, בפרט. בהמשך, ננתח צמתים טכנולוגיים שאין בהם התערבות משפטית, אך התערבות כזו עשויה להיות יעילה. באופן משלים, נדון בהטלת חבות משפטית על שחקנים בשרשרת הספאם שפעילותם הנוכחית אינה מוסדרת.

פרק ב

ספאם ואנטי-ספאם כמערכת אקולוגית סבוכה: השחקנים

1. **מבוא** **22**
2. **צד המוען: שרשרת הערך של הספאם** **23**
   א. כללי 23
   ב. בעלי המסר 26
   ג. גורמים מסייעים לפני ההפצה 29
   ד. גורמים מסייעים בשלב ההפצה 30
3. **צד הנמענים: המלחמה בספאם** **32**
   א. המדינה 32
   ב. הציבור (משתמשי קצה) ומייצגיו (עמותות הפועלות נגד ספאם) 35
   ג. גורמים פרטיים 37
   ד. הזירה הבין-לאומית: רשימות שחורות, אגודות בין-לאומיות ללוחמה בספאם 39
4. **גופי ביניים: ספקי תשתית ושירותים מקוונים** **40**
5. **סיכום** **42**

1. מבוא

בעשורים האחרונים חלו התפתחויות משמעותיות במבנה שוק הספאם הדיגיטלי. מה שהיה, בראשית ימי העידן הדיגיטלי רשת רופפת ומבוזרת של שולחי ספאם עצמאיים שניהלו חנויות מקוונות משלהם וניסו לשווק את מרכולתם, הפך היום לתעשייה מסועפת, עם רמת מומחיות גבוהה ביותר שכוללת רשת מאורגנת היטב של סוחרים, מפיצי דואר זבל (דוגמת בוֹטנֶטים - Botnet), מפרסמים לגיטימיים ומפרסמים שהם ספאמרים, ומגוון גורמי ביניים שמתווכים בין כל אלה.[1] כל הגורמים הללו מעורבים במה שמכונה **"שרשרת הערך"** של הספאם, שהזכרנו בתמציתיות בפרק המבוא, ונרחיב בסמוך.[2] כלכלת הספאם בעידן הדיגיטלי היא מערכת טכנולוגית-עסקית סבוכה ומרובת שחקנים, שלהם אינטרסים שונים ומגוונים, שלעיתים מתלכדים עם האינטרסים של שחקנים אחרים ולעיתים סותרים אותם. במובן זה, כלכלת הספאם יוצרת מערכת אקולוגית מורכבת, שבה גורמים רבים קשורים זה בזה, התנהגות האחד משפיעה על האחר, וקשה לזהות נקודה אחת שהיא הבריח התיכון של המערכת. מאפיין זה של מערכת הספאם כמערכת אקולוגית מקשה על הסדרתה המשפטית.

פרק זה ממפה את השחקנים השונים שמעורבים ביצירה ובתפעול המערכת האקולוגית של הספאם, הן בצד הייצור וההפצה של מסרים המוניים, והן בצד שמבקש להילחם בתופעת הספאם. נזהה את הזכויות והאינטרסים של כל אחד מהשחקנים, ונמפה את קשרי הגומלין בין השחקנים השונים והאינטרסים שהם מקדמים. דיון זה ישמש אותנו כבסיס לפרקים הבאים: לניתוח המשפטי בפרק ג, לניתוח הטכנולוגי בפרק ד, ולהמלצות המדיניות, בפרק ה.

השחקנים המרכזיים במערכת, שמעורבים ב"תעשיית" הספאם, לפי סדר הפעולה שלהם, הם: תחילה, משווקים שמבקשים להפיץ מסר; לאחר מכן, חברות שקוצרות ומוכרות רשימות קשר וחברות דיוור ישיר; גורמי ביניים שונים, בעיקר ספקיות תשתית מקוונת (חיבור לרשת, למשל) וספקיות שירותי הפצת מסרים ויצרני טכנולוגיות ספאם ואנטי-ספאם; בהמשך, בקצה השרשרת, נמעני המסרים השיווקיים; ובצד כל אלה, המדינה (לרבות המערכת המשפטית וגופים האמונים על הסדרה טכנולוגית), וגופים פרטיים (מסחריים ולא מסחריים) שעניינם מלחמה בספאם.

מטרת הדיון היא לפענח את המערכת האקולוגית ולהתיר את הסבך. שחקנים רבים, מוסדיים ולא מוסדיים, מעורבים במערכת האקולוגית של הספאם. ספאם היא תופעה מורכבת ורבת פנים. כדי להעריך את הפתרונות השונים לבעיה עלינו להביא בחשבון טווח רחב של שיקולים ואינטרסים של גורמים רבים. לשם כך, יש למפות את השחקנים שמעורבים בתמונה. הזכרנו את שולחי הספאם ואת הנמענים, וביניהם את ספקי השירות. התמונה מורכבת יותר.

לכל שחקן יש זכויות ואינטרסים שונים. ראשית, לאזרחים ולצרכנים עומדת זכותם לפרטיות והזכות להגנה מפני מטרדים. תקשורת נכנסת לא רצויה עשויה לפגוע בפרטיות הנמען ולהטרידו, ולהפריע לו להשתמש בקניינו כרצונו. אולם, מכיוון שמדובר במסרי תקשורת, פרסום לגיטימי נהנה מהגנת חופש הביטוי, ובכלל זה חופש הביטוי המסחרי. בנוסף, מכיוון שמדובר במסרים שיווקיים, זכויות נוספות נכנסות לתמונה: זכויות הקניין וחופש העיסוק של הגופים המסחריים ששולחים את המסרים, קטנים כגדולים, שזקוקים לפעול בתחום השיווק על מנת לקיים את עסקיהם הלגיטימיים באופן רווחי.

הדיון שנציע אינו מתמצה בקשר שבין המוען לנמענים. כחלק מהגנה וטיפוח פעילות איכותית בזירה המקוונת, יש להגן גם על האינטרסים של ספקיות שירות, הן בתחום התשתיות והן בתחום הפעילות באינטרנט. זו משימה לא פשוטה, משום שחברות שמספקות שירותים ותשתיות נמצאות בתווך: הן מספקות שירותים הן לשולחי מסרים והן לנמענים. כמו כן, מכיוון שזירת הפעילות של תעבורה דיגיטלית היא הרשת המקוונת העולמית, קיימים שיקולים הנוגעים לשיתוף פעולה בין-מדינתי לשם הגנה על הזירה המקוונת מפני תעבורה לא רצויה.

מנגד, גם בהתמודדות עם ספאם מעורבים שחקנים רבים, שמושפעים מתוצאות הפעילות בשרשרת הערך של הספאם או מבקשים להשפיע עליה. בראש הגורמים הללו עומדת המדינה, שהיא שחקנית מרכזית שבפני עצמה

---

1 ראו Justin M. Rao & David H. Reiley, *The Economics of Spam*, 26(3) J. Econ. Persp. 87,88 (2012).

2 לעניין שרשרת הערך בפרסום דיגיטלי, ראו: Matti Leppäniemi, Heikki Karjaluoto, Jari Salo, *The Success Factors of Mobile Advertising Value Chain*, Iv E-Business Rev. 93 (2004); לעניין שרשרת הערך של הספאם, ראו: Guido Schryen, Anti-Spam Measures: Analysis And Design, 56 (2007). להגדרה מפורשת של שרשרת הערך של הספאם, ראו: Kirill Levchenko et al., *Click Trajectories: End-to-end Analysis of the Spam Value Chain*, IEEE Symposium on Security & Privacy 2 (2011).

אוחזת בכובעים רבים ומייצגת אינטרסים רבים ומורכבים ביותר. בנוסף למדינה, נמצא הציבור הרחב שנפגע מפעילות הספאם, ועליו נוספים שחקנים פרטיים רבים שמעורבים במאבק בספאם.

הניתוח בפרק זה ובפרקים הבאים שונה מניתוחים כלכליים מקובלים של מערכת הספאם, שרואים את שרשרת הערך כיחידת ניתוח נפרדת, שניתנת ללימוד ולהבנה במנותק מהכוחות שפועלים נגדה. חוקרי מערכות מידע שהתמקדו במחקר שרשרת הערך של הספאם הסיקו שנדרש ניתוח הוליסטי של "שרשרת הערך" כולה, כזה שיעריך את היחסים המתקיימים בין החוליות השונות בשרשרת, וכך יוכל לזהות חולשות אפשריות.[3] הניתוח כאן מקבל עמדה הוליסטית כזו, ומרחיב אותה כך שתכלול, בנוסף לשרשרת הערך של הספאם, גם את הצד השני של המטבע – את השחקנים המעורבים במלחמה בספאם. גישה זו רואה בתופעת הספאם מערכת אקולוגית שמורכבת הן משרשרת הערך של הספאם והן מהכוחות שפועלים נגדה. בהמשך לכך, הניתוח בפרק נשען על ההנחה שללא הבנה מלאה של המערכת ושל השחקנים שמעורבים בה, מרבית ההתערבויות נגד ספאם עלולות להתמקד בהיבטים נקודתיים בלבד, למשל סינון דוא"ל או רשימות שחורות של כתובות אתרים, ולהתעלם מהיבטים אחרים, כמו השלב המקדמי של קצירת כתובות דוא"ל ומספרי טלפון, או שלבי ביניים כמו שימוש בשירותי תיווך לשם הפצת מסרים.

בהתאם, הניתוח בפרק זה נועד לאתר את נקודות התורפה במערכת, ולהצביע על הצמתים בהם יש התערבות רגולטורית מספקת (ולעיתים אף התערבות-יתר), כמו על הצמתים הסובלים מתת-התערבות. הפרק מחולק לשלושה חלקים. חלק 1 עוסק בשחקנים שמעורבים בשרשרת הערך של הספאם, כלומר בצד המוען. חלק 2 בוחן את השחקנים שמנגד, שמבקשים להילחם בתופעת הספאם, כלומר, בצד הנמענים. חלק 3 עוסק בשחקני הביניים, שמשרתים את השחקנים בכל אחת משתי הקודמות: ספקיות תשתיות ושירותי תקשורת. בכל אחד מהחלקים, נברר את הצרכים, המגבלות והאינטרסים הייחודיים של כל אחד מהשחקנים המרכזיים במערכת. לבסוף נסכם.

- **שרשרת הערך של הספאם** היא סך השחקנים והמשאבים שמעורבים במאמץ להפוך ספאם לרווחי.
- בשרשרת הספאם יש **שני שלבים מרכזיים**: הראשון כולל את כל הפעילות המתרחשת לשם יצירת ספאם ושליחתו עד לרגע שבו מגיע הספאם אל הנמען. זה השלב שבו מתמקד דוח זה. השני כולל את כל הפעילות המתרחשת במידה שספאם "הצליח", כלומר הניע את הנמען לרכישה. נסביר את החלק הזה, ונתייחס אליו באופן נקודתי בעת הצורך.
- **שוק הספאם הדיגיטלי** אינו פועל כיום לפי מודל פשוט של מוען ונמען שנמצאים בקשר ישיר, אלא זו תעשייה מסועפת, מרובת שחקנים, שלכל אחד מהם אינטרסים שונים ולחלקם זכויות משפטיות.
- **כלכלת הספאם בעידן הדיגיטלי** היא מערכת טכנולוגית-עסקית מרובת שחקנים. זו **מערכת אקולוגית מורכבת**, שבה כל השחקנים, הטכנולוגיות, והאינטרסים שלהם סבוכים זה בזה, באופן שמקשה על הסדרה פשוטה וישירה.

2. צד המוען: שרשרת הערך של הספאם

א. כללי

פרסום מבוסס ספאם הוא עסק לכל דבר. לולא היה מדובר במפעל רווחי – תעשיית הספאם הייתה חדלה מלהתקיים. ביום יום, כאשר אנו חושבים על ספאם, בדרך כלל נתאר לעצמנו תקשורת בין מוען לנמען – הספאמר השולח את ההודעה, והמשתמש המקבל אותה – ותו לא. אלא שמשלוח המסר עצמו הוא רק קצה הקרחון; אנו נוהגים להתייחס רק לחלק הגלוי של מה שהוא למעשה מיזם עסקי גדול ורב פנים. בפועל, מערך שלם של שחקני ביניים ומשאבים

3 ראו *Click Trajectories*, Levchenko, שם. מחקר זה סיפק עדות לקיומה של חוליה חלשה בשרשרת הערך, כלומר כזו שאפשר לנתק בקלות יחסית - קומץ הבנקים המספק שירותי מסחר לספאמרים, ומאפשר מוניטיזציה של 95% ממכירות שבוצעו בעקבות שליחת ספאם. שם, בעמ' 14-13.

משמש כדי לייצר רווח משליחת ספאם. אם בראשית שנות האלפיים ספאמרים יכלו לטפל בכוחות עצמם בכל ההיבטים של העסק (כמו הפצת הדואר, עיצוב האתר אליו הם מבקשים להפנות את הנמענים, מימוש התשלומים על רכישה, וכדומה) הרי שהיום, בין השאר בעקבות התפתחויות טכנולוגיות וצמיחה עצומה של הרשת המקוונת, עסקי הספאם כוללים מגוון גדול של שחקנים וספקי שירות שספאמר ממוצע נזקק לשירותיהם ולעיתים אף תלוי בהם.

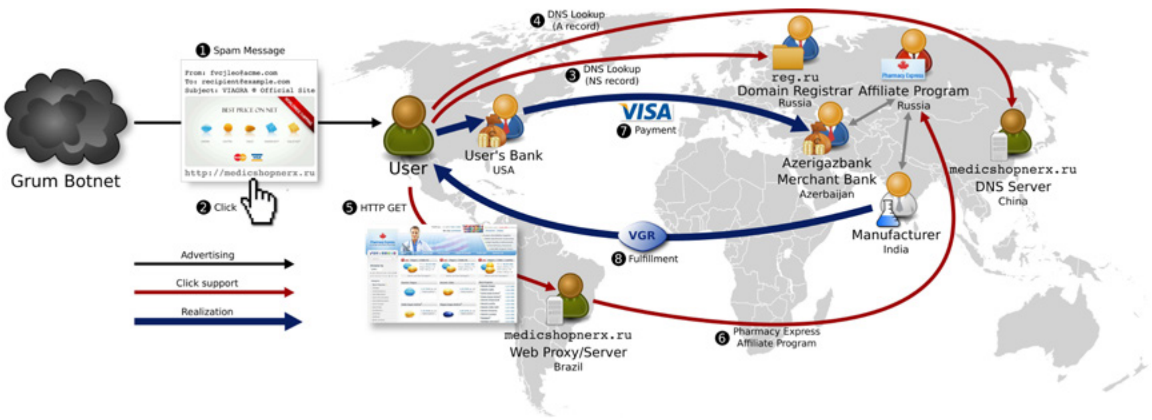
שחקנים שונים מעורבים בהפעלת המערך שמאפשר שליחה המונית (במובן של mass) של מסרים שיווקיים. זהו השלב הראשון. בהמשך, לאחר שהודעת ספאם הגיעה ליעדה, כל קליק על קישור שהופץ כספאם הוא רק תחילתו של מסלול ארוך ומורכב, שמשתרע על פני טווח של רכיבים טכניים ועסקיים, שביחד יוצרים את התשתית לייצור רווח מביקור של משתמש-לקוח באתר.

באופן כללי, שרשרת הערך של הספאם נחלקת לשלושה שלבים מובחנים:

1. שלב **ההפצה**;
2. שלב **התמיכה** בהקלקה (כלומר, פעולות שתומכות ומקדמות "הקלקה" של משתמשים על כתובת האתר המשווק);
3. שלב **המימוש** (כלומר, מה שקורה לאחר שמשתמש "הקליק", ואפשר לממש את ההכנסה מהקנייה).

בנוגע לכל שם מתחם רשום שמשמש למשלוח ספאם,[4] אפשר לנסות לנקוט הגנה מפני ספאם בכל אחד משלושת השלבים של שרשרת הערך. למשל, בשלב ההפצה, אפשר לחסום אותו באמצעות מסננים שונים; בשלב התמיכה בהקלקות, אפשר להפיל אתרי אחסון אם שם השרת שלהם מאותת על בעיה; ובשלב המימוש, אפשר להתגונן באמצעות סגירה של חשבון הסוחר.[5] תרשים ב.1, שלקוח ממחקרם של Levchenko ואח' משנת 2011,[6] מדגים את מורכבותה של התשתית המעורבת בשרשרת הערך של כתובת URL אחת בלבד:

תרשים ב.1: התשתית הטכנולוגית של שרשרת הערך של הספאם



<u>שרשרת הערך: המצב הנוכחי בישראל</u>

בישראל היום, שרשרת הערך של הספאם כיום מורכבת, באופן כללי, מכמה גורמים:

1. **בעלי המסר**, שהם עסקים, קטנים וגדולים, פרטיים וציבוריים, שמבקשים לשווק את עסקיהם;
2. **גורמים מסייעים *לפני* ההפצה:**

- ספקי לִידים, שמספקים למשווקים את רשימות התפוצה, אליהן בהמשך יופצו מסרים שיווקיים;

4 שם מתחם (domain name) הוא שמו הייחודי של אתר אינטרנט. לכל אתר אינטרנט שם מתחם משלו, המאפשר לזהותו. בישראל, איגוד האינטרנט הישראלי הוא הגוף היחיד המורשה לרשום שמות מתחם. שם המתחם מקושר לכתובת האתר במרחבי הרשת.

5 Levchenko, *Click Trajectories*, לעיל ה"ש 2, בעמ' 12.

6 שם, בעמ' 4.

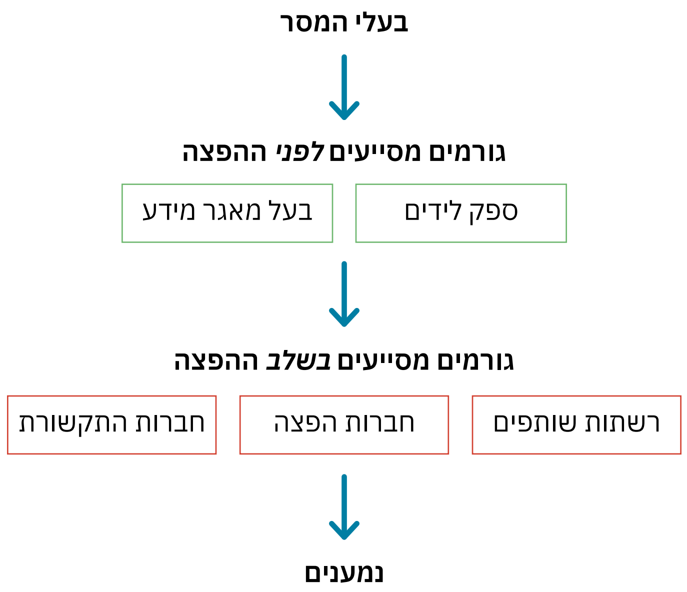
- בעל מאגר מידע, שכולל את רשימות התפוצה, שבהן, לכל הפחות כלולים אמצעי הקשר של הנמענים (כתובות דוא"ל, מספרי טלפון).
[לעיתים, ספק הלידים הוא בעצמו בעל מאגר מידע.]

3. **גורמים מסייעים *בשלב* ההפצה:**

- חברות הפצה שמספקות פלטפורמות להפצת תכנים שיווקיים במסות גדולות, שאינן בהכרח בעלות רישיון בזק;
- חברות התקשורת (בעלות רישיון). שלגביהן נרחיב בחלק ב.3.

4. **רשתות שותפים**, שהן פלטפורמות המקשרות בין גורמים העוסקים בפרסום בזירות טכנולוגיות שונות (השותפים), ובין בעלי עסק המעוניינים לפרסם את עסקיהם.[7]

תרשים ב.2: שחקנים בשרשרת הערך



אם כך, שרשרת הערך מורכבת משלבי פעולה שונים, שבכל אחד מהם פועלים שחקנים שונים, כאשר כל אחד מהם, הוא למעשה קבוצה שאינה תמיד הומוגנית וחד-ממדית. כך למשל, החולייה הראשונה בשרשרת הערך היא עסקים שמבקשים לשווק את עסקם, הם בעלי המסר. העסק עצמו יכול שיהיה לגיטימי (למשל, סופרמרקט או מכון כושר), לגיטימי פחות (למשל שירות הלוואות בשוק האפור), או בלתי חוקי (מכירת סמים). תוכן המסרים עצמם יכול שיהיה לגיטימי (שיווק ענייני ונכון) או פחות לגיטימי (תוכן שכולל הטעיה של הנמענים), או בלתי חוקי ממש שחקנים שונים משמשים כגורמי ביניים בין העסקים המשווקים לבין נמעניו של המסר השיווקי, שעשויים להפוך ללקוחות. חלק מגורמי הביניים אינם נתונים לפיקוח ישיר של הרגולטור (למשל, חברות ההפצה), וחלקם כפופים לרגולציה אך נהנים מפטור מאחריות, כמו חברות תקשורת (ולעיתים גם חברות ההפצה, אם מתייחסים אליהן כאל חברת תקשורת, נושא שנעסוק בו בחלק ב.3).

בשרשרת הערך יש גורמים נוספים, כמו בעלי רשתות בוטים ומפעיליהן שמספקים שירותי מימוש ערך לספאמרים: למרות שאין ספק ששחקנים אלה מעורבים בתפעול שרשרת הערך של הספאם, דוח זה אינו מתמקד בהם, משתי סיבות מרכזיות. ראשית, רשתות בוטים שנועדו להפצת ספאם פועלות מתחת לרדאר, הן לא בהכרח נמצאות בתחום השיפוט של המדינה, והן מחוץ ליכולת פיקוח ממשית של רגולטור מקומי. שנית, חלק לא מבוטל של פעילות השחקנים האלה היא פלילית, למשל הפצת ספאם למטרות פישינג.[8]

7 כך תיארה זאת השופטת ברון: "'רשת שותפים' הכוונה לפלטפורמה המקשרת בין השותפים (Affiliates), שהם חברות וגורמים שעוסקים בקידום ופרסום במגוון זירות טכנולוגיות, ובין מפרסמים המעוניינים לפרסם את עסקיהם." ראו רע"א 1326/18 **סמארט קלאב אחזקות בע"מ נ' כהן** (נבו 31.12.2020), בפס' 2.

8 פישינג או דיוג (באנגלית: phishing) הוא ניסיון לגנוב מידע באינטרנט על ידי התחזות לגורם לגיטימי המבקש את המידע.

נפרט בנוגע לכל אחד מהשחקנים הנ"ל, את האינטרסים, החבויות והזכויות שלו.

ב. בעלי המסר

עסקים ומשווקים: לגיטימיים ולא לגיטימיים

ראשיתו של הספאם הוא בבעל עסק שמבקש לקדם את עסקיו – לגייס לקוחות, לפרסם מוצר או שירות וכדומה. זהו המוען, או בלשון החוק, "המפרסם." השאלה מיהו "מפרסם" נדונה בכנסת, בדיוני הוועדה שדנה בחקיקת חוק הספאם, שם הבחינו המשתתפים בין בעל עסק שמבקש לפרסם את שירותיו לבין מי שמספק את שירותי השיווק, כמו חברות דיוור ישיר,[9] וכן בין אלה לבין בעלי מאגרי מידע והסוחרים בהם.[10] תת פרק זה עוסק בשחקן הראשון ברשימה: בעל עסק המבקש לפרסם את שירותיו.

האינטרס המובהק של שחקן זה הוא **שיווק ומכירה**, והרצון להשתמש באופן היעיל ביותר באמצעי השיווק ההמוני הדיגיטלי. לבעלי עסקים מסוגים שונים יש אינטרס בהפצת תוכן שיווקי למספר גדול ככל האפשר של לקוחות קיימים ופוטנציאליים, לשם קידום מכירות ופרסום בכלל. הפיתוי גדול: הפצת מסרים המוניים זולה יחסית, כך שגם מכירות ספורות מכל קמפיין שיווקי כזה הופך אותו למשתלם, ביחס לעלות הפרסום. בדיוני הוועדה בכנסת בשנת 2007, לקראת חקיקת חוק הספאם, ניתנה דוגמה: שליחת מסר שיווקי למיליון בתי עסק עלתה בשעתה כ-1500 ש"ח.[11]

התרגום המשפטי של חלק מהאינטרסים האלה הוא לזכויות של העסקים המוענים. בנוסף ל**זכות הקניין** של בעל עסק לנהל את עסקו כרצונו, עומדת לו גם זכותו ל**חופש העיסוק**. לכן, הגבלה על האפשרות לשווק עסקים עשויה לעלות לכדי פגיעה בקניין ובחופש העיסוק. בנוסף, פרסום לגיטימי נהנה מהגנת **חופש הביטוי המסחרי**.[12] חסימת מסרים לפי תוכנם, או חסימה גורפת מדי, עלולה לפגוע בחופש הביטוי של המפרסם. כפי שנראה בהרחבה בשני הפרקים הבאים, שיעסקו בהתאמה, במשפט הספאם ובטכנולוגיות ספאם, חשש מרכזי מפני סינון-יתר של תכנים הוא הפגיעה בחופש הביטוי של העסקים, מפיצי המסר.

קבוצת העסקים המוענים, בעלי המסרים, אינה עשויה מקשה אחת. אבחנה אחת היא גודל העסק, והשנייה היא תוכן המסרים.

גודל העסק המפרסם

בין העסקים המפרסמים, יש תאגידי ענק ויש בהם עסקים קטנים. ההבדל בין אלה עולה בבירור מבחינת זהותם של נתבעי ספאם סדרתיים (נושא שנדון בו בפרק ג של הדוח). עיון זה מעלה שבעוד שלתאגידי ענק יש אמצעים משפטיים, כלכליים וטכנולוגיים להתמודד עם תביעות ספאם, הרי שעסק קטן שנתבע בעילה של הפצת ספאם עלול לספוג מכה אנושה, עד כדי סגירה. במילים אחרות, לכלל המשפטי יש השלכה חלוקתית, ויש חשש שכלל משפטי אחיד יפגע באופן לא אחיד בשחקנים שונים. הטענה שחוק הספאם פוגע בעיקר בעסקים קטנים עלתה כבר בדיונים בכנסת, והטענה הייתה שהחוק יצמצם את אפשרויות הפרסום הזולות של בתי עסק ויותיר בידם רק אפיקי פרסום יקרים כמו פרסום בטלוויזיה שהוא יקר במיוחד. הנפגעים העיקריים הם עסקים קטנים.[13]

---

9 ראו פרוטוקול ישיבה 4 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 6 (25.12.2007) (להלן: **דיון הוועדה המשותפת מיום 25.12.2007**), בדבריו של עו"ד חיים רביה.

10 ראו למשל את דבריה של היועצת המשפטית של הוועדה, שם, בעמ' 14.

11 דיון הוועדה המשותפת מיום 25.12.2007, לעיל ה"ש 9, בעמ' 8, בדבריו של עופר האפרתי, בעל השליטה בחברת הדיוור אי-מיילון.

12 כידוע, המשפט הישראלי מגן גם על ביטויים מסחריים תחת הגג של חופש הביטוי, אם כי לעיתים באופן מופחת. ראו בג"ץ 606/93 **קידום יזמות ומולו"ת (1981) בע"מ נ' רשות השידור**, פ"ד מח(2) 1, בפס' 8-10 לפסק דינה של השופטת דורנר (1994); בג"ץ 7647/16 **האגודה לזכויות האזרח בישראל נ' שרת התרבות והספורט**, בפס' 71 לפסק דינו של המשנה לנשיאה מלצר (נבו 13.5.2020); בג"ץ 6536/17 **התנועה למען איכות השלטון בישראל נ' משטרת ישראל**, בפס' 21 לפסק דינה של השופטת חיות (נבו 8.10.2017); יפה זילברשץ "על חופש הביטוי המסחרי" **משפט וממשל** ג 509 (1996).

13 ראו למשל דבריו של אלי שחף, מנכ"ל חברת "עסקה טובה" שעוסקת במכירה דרך קטלוגים, איגוד לשכות המסחר, בפרוטוקול ישיבה 2 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 6 (31.01.2007). שחף טען שיש לקבל את המודל האמריקני, שלפיו יוקם מאגר מידע מרכזי, שאליו ירשמו נושאי מידע שאינם מעוניינים לקבל הצעות פרסום, ומולו כל עסק יהיה חייב לסמן את הרשימה שלו לפני משלוח הודעת מסחריות.

חוקיות התוכן המפורסם

אבחנה שניה בתוך קבוצת העסקים המוענים היא לפי חוקיות התוכן המופץ.

קבוצה אחת, היא של חברות לגיטימיות שעליהן נמנות לעיתים קרובות חברות גדולות במשק, וכן רשתות שיווק שאנשים נרשמים למועדון הלקוחות שלהן, ובמקרים רבים מַתְנות את קבלת השירות באישור הלקוח לקבלת הודעות שיווקיות. תוכן המסרים עצמו חוקי, ועומד בהוראות הדין הכללי, למשל חוקיות השירותים המשווקים, היעדר הונאה, ועמידה בהוראות דיני הגנת הצרכן. יש להניח שספאמרים מסוג זה ימהרו להתפשר במקרה של הפרה ותביעה, ובמקרים רבים יפסיקו לגמרי להפיץ ספאם. משיחות שערכנו עם גורמים בשרשרת הערך של הספאם בישראל, עולה שלפחות מנקודת המבט שלהם, רוב התביעות המוגשות בארץ הן דווקא נגד משווקים לגיטימיים, או בניסוח של אחד מבעליה של חברת הפצה מקומית: "בתביעות בבית המשפט נתבעים ה-good guys".

קבוצה שניה היא של ספאמרים סדרתיים, אותם ניתן לכנות ספאמרים "מקצועיים". לאלה יש מערך משפטי מיומן שמייצג אותם בבית המשפט, והם שחקן משפטי חוזר בעל יתרון ניכר מול תובע יחיד. ספאמרים רבים בקבוצה זו שולחים הודעות שהן בעצם פיתיון להונאה, ולמרות שאין להם ספק שהם פועלים באופן לא חוקי, לא תמיד הם מוטרדים מכך במיוחד.

הפרה יעילה?

לעסקים השונים, אבל במיוחד אצל הגדולים, הן אצל כאלה שמפיצים תכנים חוקיים והן כאלה שפועלים באופן בלתי חוקי, נוסף שיקול כלכלי. והמפרסמים נחלקים לשני סוגים:

1. עסקים שפועלים לפי שיטת ה"הפרה היעילה", כלומר אלה שגם אם ייאלצו לפצות נפגעים, עדיין יהיה להם משתלם להמשיך ולפעול. רק במקרה שבו ייתבעו באופן שיהפוך את הפרת החוק ללא משתלמת, הם יחפשו שיטת פרסום חדשה.
2. עסקים שזו שיטת הפרסום היחידה שבה יוכלו לפעול, למשל כאלה שמטרתם להונות את הנמענים. חברות מסוג זה פועלות, בהגדרה, באופן לא חוקי. אפשרות האכיפה הפרטית נגד חברות כאלה מוגבלת, בשל העבודה שבמקרים רבים אין "כתובת", כלומר מדובר בחברות קש ואנשי קש או חברות שביום אחד מתפרקות ונעלמות, או כאשר מאתרים אותן, בשל הייצוג המשפטי המיומן שלהן – לעומת התובעים שהם אנשים פרטיים ברוב המקרים. ספאמרים כאלה נוטים להתחמק מתביעות משפטיות או לא לקיים את פסקי הדין גם לאחר שניתנו, ולפעול באופן כללי באופנים "בעייתיים".

במהלך תקופת הפעילות של חברת "ספאם אוף", שהייתה חברה שסייעה לנפגעי ספאם בהגשת תביעות קטנות, אפשר היה ללמוד הרבה על זהותם ואופיים של הספאמרים הסדרתיים בישראל.[14] זהות החברות הללו משתנה, אך אופי וטיב פעולתן דומה. כתבה שהתפרסמה בשנת 2017 ב"וואלה" תיארה את חמש קבוצות הספאמרים הסדרתיים הגדולים שפעלו בישראל באותה עת.[15] הכתבה הציגה את חברת "אור הקסם" שהפיצה הודעות המשווקת דיאטות טבעיות שונות, דיאטת איזי-לייף, תחליפים לריטלין מצמחים, הלוואות בריבית ופתרון לבעיית צ'קים חוזרים, כמפיצת הספאם הגדולה בישראל באותו מועד. לטענת חברת "ספאם אוף", למרות שהוגשו נגד "אור הקסם" עשרות תביעות, גם כאשר בתי המשפט פסקו שעליה לפצות תובעים, החברה התחמקה מתשלום הפיצוי.[16] ריבוי התביעות ופסקי הדין נגד החברה לא הרתיעו אותה, וההערכה של חברת "ספאם אוף" לפי סקרים שערכה, הייתה ש"אור הקסם" הייתה אחראית בשעתה ל-10% מתעבורת הספאם בהודעות טקסט טלפוניות (סמס), כאשר הרוב המוחלט של הודעות הקשורות להלוואות ולפתרון בעיות צ'קים – מקורו היה בחברה זו. כמו כן, ההנחה הייתה שחברה זו מורכבת מ"אנשי קש" ומחברות שקמות ונופלות לפי הצורך של מפעיליה לשמור על זהותם מוסתרת.

14 "ספאם אוף" ביקשה לפעול למיגור הספאם, בדרך של סיוע בהגשת תביעות קטנות לנפגעי ספאם. במהלך תקופת פעילותה, אספה החברה חומר רב על פעילות ספאמרים בישראל. להרחבה על החברה ופעילותה, ראו בחלק 2ג.

15 אירה אימרגליק "נמאס לכם מהספאם? אלו החברות שתוכלו לתבוע" **וואלה** (6.2.2017), https://finance.walla.co.il/item/3038144.

16 ראו למשל ת"צ (מחוזי, חיפה) 10316-02-14 **זילברג נ' אור הקסם בע"מ** (נבו 19.11.2014); וכן: אימרגליק, שם.

חברות נוספות שהוזכרו בכתבה פעלו באופן דומה. חלקן נסגר ונעלם בן לילה, או החל לפעול מול לקוחות מחוץ לישראל.[17] כך למשל חברת "מנקס אונליין טריידינג", הציעה באמצעות סמס ללקוחות פוטנציאליים לעשות כסף קל מהבית. החברה, שהייתה אחת משולחות הספאם הגדולות בישראל שעסקה בסחר באופציות בינאריות, הפסיקה ככל הנראה להציע את שירותיה ללקוחות מקומיים לאחר שהסחר באופציות בינאריות הוצא מחוץ לחוק בישראל בשנת 2017.[18] דוח איגוד האינטרנט משנת 2023 מזכיר את החברה כנתבעת סדרתית בולטת, ומצא שהיא חויבה ב-74% מתוך 670 תיקים הספאם הקטנים בהם נתבעה.[19]

כוחם של ספאמרים "מקצועיים" להשיב מלחמה למתנגדי הספאם גדול, ובמקרה של חברת "ספאם אוף", כפי שעלה משיחות רקע שערכנו, הם גם אלה שבסופו של דבר הכניעו את החברה, שפסקה מפעילותה.

נדגיש, העובדה שחברה היא נתבעת סדרתית אין משמעה שהחברה פועלת באופן לא לגיטימי; מדוח איגוד האינטרנט עולה גם שיש חברות שהן אמנם נתבעות סדרתיות, אך בתי המשפט מוצאים אותן חייבות לעיתים רחוקות.[20] השערת מחברי הדוח היא כי "ישנם מקרים שבהם קיים בציבור **פער ידע ביחס להגדרת הודעת ספאם**, מה שגורם לבזבוז משאבי תביעה במקרים ללא עילה." נשוב לכך בפרק ג שעוסק במנגנוני האכיפה המשפטיים. הסבר מצטרף הוא שחברות אלה פועלות מתחת לפנס, וקל יותר לתבוע אותן מאשר עסקים לא לגיטימיים.

לבעלי עסקים שמבקשים לשווק תכנים שיווקיים לגיטימיים יש אינטרס ב**מלחמה בספאם זדוני** שמטרתו הונאה, משום שספאם מסוג זה פוגע בדרכים שונות באמינותם כמשווקים. ראשית, משתמש ש"נפל בפח" של ספאמר זדוני ינהג בחשדנות ובמשנה זהירות כלפי כל תוכן שיווקי שיגיע אליו. בנוסף לכך, ספאם זדוני עשוי להתחזות לבעל עסק לגיטימי קיים, למשל לרשת שיווק מזון קיימת או לדואר ישראל; במקרה כזה, המשתמש שנפגע יכול לתבוע את בעל העסק הלגיטימי שבשמו השתמש הספאמר. בנוסף לפגיעה באמינותו, בית העסק הנפגע עשוי לסבול מנזק כלכלי. למעשה, השחקן שאנו מכנים "משווק" נחלק לשתי קבוצות, שלאחת יש אינטרס להילחם בשנייה. במילים אחרות, האינטרס של משווקים שאינם ספאמרים "מקצועיים" מתלכד לעיתים עם האינטרס של שחקנים מהעבר השני של המתרס, שאותם נציג בחלק הבא.

בין כל השחקנים שמעורבים בשרשרת הערך של הספאם, עסקים משווקים הם הנושאים בעיקר הנטל מבחינת הטלת חבות משפטית; כפי שציין באוזנינו עו"ד ועו"פ זיו גלסברג, פעיל בנושא ספאם וממייסדי עמותת "אל-ספאם": "מי שנתבע בתכל'ס כל הזמן, זה העסקים, כי אותם קל לזהות, וספקי הלידים."[21]

עובדה זו עשויה להיות המקור לאינטרס נוסף של משווקים, והוא **לחלק את נטל החבות המשפטית** בינם לבין שחקנים נוספים בשרשרת הערך. עם זאת, מכיוון שלעיתים קרובות עסקים מפיצי ספאם הם שחקנים חוזרים במערכת, הם צוברים ידע ומומחיות הולכים וגדלים לגבי דרכי התמודדות עם אתגרים כלכליים, טכנולוגיים, ומשפטיים.

> **לסיכום חלק זה**: מפרסמי המסרים אינם עשויים מקשה אחת. יש בהם עסקים גדולים ויש בהם עסקים קטנים – היבט שמשפיע על מידת החשיפה שלהם לרגולציה ויכולתם לשרוד מול תביעות ספאם; עסקים שמשווקים תכנים חוקיים וכאלה שמשווקים תכנים לא חוקיים; ועסקים שנוקטים גישה של הפרה יעילה, כלומר יודעים שיספגו הפסדים משפטיים בדרך של פיצוי לקוחות, ועדיין משתלם להן להמשיך בפעילותן, מול עסקים שאינם נוקטים גישה זו.

17 אימרגליק, שם.

18 ס' 44ב1 לחוק ניירות ערך, התשכ"ח-1968.

19 ראו איגוד האינטרנט הישראלי, ניתוח נתוני עתק של תביעות דואר זבל אלקטרוני (ספאם) בישראל (להלן: **דוח איגוד האינטרנט**), בפרק "ממצאים ודיון", תת פרק 6 "נתבעים סדרתיים". נמצא ב: https://www.isoc.org.il/research/spam-data-analysis.

20 עמ' 31-32. הדוגמאות בדוח הן "למשל רק 1% מ- 216 התביעות שהוגשו נגד משרד הפנים נמצאו מוצדקות ורק 2% מתוך 135 התביעות שהוגשו נגד חברת "גלוגובר" נמצאו מוצדקות".

21 הדברים נאמרו במהלך שיחה שנערכה ב-30.4.2022.

ג. גורמים מסייעים לפני ההפצה

ספקי לידים ובעלי מאגרים

בצד המשווקים, מלבד העסקים המשווקים עצמם, ספקי הלידים (מלשון lead) הם שחקן נוסף שנגדו מוגשות תביעות בעילת ספאם. עסקים רבים אינם מקושששים את רשימת הנמענים שלהם בעצמם, אלא נעזרים בגורמי ביניים, שיש ברשותם מאגרי מידע, או שיש להם גישה למאגרי מידע חוקיים - או שאינם חוקיים. אלה הם ספקי הלידים. ספק לידים הוא מי שאוסף פרטי קשר – מספרי טלפון, כתובות דוא"ל, וכדומה – של אנשים שידוע או שאפשר לשער שהם מעוניינים בשירות מסוים, וסוחר במאגר המידע שיצר. לעיתים, ספק הלידים הוא בעצמו בעל מאגר מידע. ספק הלידים הוא הגורם שמחפש נמענים שהם צרכנים פוטנציאליים, ויכול למצוא אותם בצורה לגיטימית (רשימות מאושרות, פרסומות, דפי נחיתה של אתרים שאליהם גולשים פונים מיוזמתם שלהם) או בדרכים לא חוקיות (למשל רכישת מאגרי מידע שנגנבו ונמכרו ברשת האפלה, ה-dark net). לספקי הלידים גם יש מידע בנוגע לטיב הרשימות, למשל איזו רשימה תביא לאחוזי היענות גבוהים יותר מרשימות אחרות. לעיתים קרובות, ספקי הלידים ישלחו ספאם בעצמם. במקרה כזה, יש לראותם כמפיצי המסר, שנדונו בסעיף הקודם.

נציגי עסקים שעיסוקם הוא סחר במאגרי מידע השתתפו בדיוני הוועדה בכנסת לקראת חקיקת חוק הספאם.[22] בעלי מאגרי מידע הביעו דאגה מהצורך להסיר ממאגר מידע את פרטיו של אדם שביקש זאת. כך למשל, אלי שחף, שפרנסתו באותה עת הייתה פרסום בקטלוגים, טען שהעלות של יצירת תיעוד של הסכמה לקבלת פרסומים גבוהה מדי, וכי הוא לא יוכל לעמוד בנטל הכלכלי של שמירת הסכמות של לקוחות 20 שנה אחורה.[23] התשובה בוועדה הייתה שאם ביכולתו לשמור את פרטיו של אדם במשך 20 שנה למטרות פרסום, אין סיבה שלא יוכל לשמור גם את הסכמתו של האדם לקבלת דבר פרסום.[24]

האינטרס העסקי של ספקי הלידים הוא **להתפרנס ממסחור מאגרי המידע** שברשותם. בהנחה שברשות ספקי הלידים מאגרי מידע העונים על הגדרת "מאגר מידע" בסעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות"), עליהם **לציית להוראות החוק בנוגע לניהול מאגר** כזה ולשימושים בו. החוק מגדיר מאגר מידע כך: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט "(1) אוסף לשימוש אישי שאינו למטרות עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף."

נקודה משמעותית בהגדרה זו היא הסייג – שמחריג רשימות של שם, מען ודרכי התקשרות מהגדרת מאגר מידע, ובהתאם, מאגרים כאלה אינם כפופים לחובות רבים שיש בחוק, אולם לחריג זה יש סייגים – הראשון שבהם משמעותי לענייננו – שברשימה אין איפון. מרגע שיש מאפיין נוסף לרשימה, הרי היא בגדר "מאגר מידע", והחובות שבחוק ביחס למאגר כזה, נכנסות לפעולה.

כאשר מדובר במאגר מידע כהגדרתו בחוק, בין היתר, חלה על בעליו חובת ההודעה לאדם בדבר מטרות השימוש במידע (סעיף 11 לחוק), מתן אפשרות לגישה למידע (סעיף 13), תיקון מידע שגוי (סעיף 14), חובת סודיות (סעיף 16), וחובת אבטחת מידע (סעיף 17, ותקנות נלוות). בעיקר, מטרות המאגר צריכות להיות ברורות ומפורשות – חריגה בשימושים ממטרות המאגר הן הפרה של עקרון צמידות המטרה, וזו עוולה הן לפי פרק א של החוק (סעיף 2(9)), והן לפי פרק ב שם (סעיף 8(ב)). בנוסף, יש כיום חובה לרישום מאגר המידע (סעיף 8(ג)).

בהיותם נתבעים נפוצים בעילה של ספאם עם המשווקים, ספקי הלידים חולקים עם האחרונים אינטרס משותף, והוא הרצון **לחלק את נטל החבות המשפטית** בינם לבין שחקנים נוספים בשרשרת הערך.

22 למשל בדיון הוועדה המשותפת מיום 25.12.2007, לעיל ה"ש 9, נכח יובל בן ניר, מנכ"ל חברת לינקו המספקת רשימת דיוור לבעלי תפקידים בכירים.

23 בדיון הוועדה המשותפת מיום 25.12.2007, לעיל ה"ש 9, בעמ' 14.

24 שם, בעמ' 15.

ד. גורמים מסייעים בשלב ההפצה

רשתות שותפים (Affiliate Programs)

לעיתים, הקשר בין העסק המשווק לבין ספק הלידים מתוַּוך דרך גורם ביניים: רשתות שותפים. כבר לפני יותר מעשור, רשתות-שותפים שלטו בשימוש בספאם לשם שיווק ומכירת מוצרים, ובשוק הספאם הן היו דומיננטיות ביחס לשחקנים "חופשיים".[25] רשתות אלה תיווכו בין עסקים לבין ספקי לידים ובכך ניתקו את הקשר הישיר ביניהן, באופן שאפשר הן לעסק והן לספק הלידים לטעון שאינם מכירים זה את זה ולכן אינם מודעים לפעילותו של הצד האחר ובוודאי שאין להם חבות משפטית בקשר למעשיו. לגבי ספאמרים מקצועיים בעיקר, רשתות השותפים חולקות תשתיות, הן בשלב התמיכה בהקלקות (למשל רישום דומיין או שירותי אירוח אתרים) והן בשלב מימוש הרווח (למשל טיפול בתשלומים ובפדיון).[26]

הידע המחקרי בנוגע לתפעול ולניהול רשתות שותפים בישראל דל. למרות שבשיחות הרקע שערכנו עלה שרשתות אלה הן גורם מוכר בשרשרת הערך המקומית של הספאם, הן בדרך כלל אינן מגיעות לבתי המשפט, בין השאר מכיוון שלתובע אין דרך להגיע אליהן ללא אמצעי חקירה משמעותיים. קל יותר לזהות ולתבוע את המשווק ואת ספק הלידים. עצם הימצאותו של שחקן זה – רשתות השותפים – בזירת הספאם מאפשרת לנו לזהות אינטרס אפשרי נוסף של שני השחקנים הקודמים. במקרה שבו הספאמר המקצועי פועל במודע באופן לא חוקי, יש לו אינטרס להשתמש ברשימת שותפים שתתווך בינו לבין ספק הלידים, באופן שיקשה לזהות את מקור הספאם ולהגיע אליו. הדבר נכון גם בנוגע לספק לידים. בית המשפט העליון היה ער להיבט זה. בעניין **סמארט קלאב נ' כהן** ציין בית המשפט שהמטרה של שימוש בגורמי ביניים היא הסתרת מקור הספאם: "יבואר בנקודה זו כי תנאי 'השיגור' איננו מצמצם את תחולת החוק רק לחברות שיווק או פרסום שבאמצעותן משוגר דואר זבל של גופים מסחריים לנמענים, שכן ישנם לא מעט גורמים מסחריים הנכללים בהגדרה 'מפרסם' שמשגרים בעצמם הודעות לנמענים ללא 'תיווך'; אולם, הוא מעורר חשש לא מבוטל שגופים מסחריים יעדיפו לפרסם את עסקיהם באמצעות גורם שלישי על מנת לעקוף את הוראות חוק התקשורת – והדבר עלול לרוקן מתוכן את האיסור על משלוח ספאם."[27]

רשתות שותפים מציבות אתגר בפני נפגעי הספאם, משום שהן מאפשרות לטשטש את מקורו. חקירה רגולטורית ומחקר אקדמי בנושא רשתות השותפים בישראל עשויים לסייע להבנה כיצד יש להתמודד עם שחקן זה ועם האתגרים שהוא מציב בזירת הספאם.

חברות הפצה

חברות ההפצה מספקות פלטפורמות לשיגור מסרים. מדובר בכלי תוכנה שמאפשרים ניהול רשימת לקוחות ושליחת מסרים שיווקיים בפשטות יחסית. חברות ההפצה מוכרות רישיונות שימוש בכלי התוכנה שלהם, ומסייעות ללקוחותיהן לעצב מסרים ולהפיץ אותם בערוצים שונים כמו דוא"ל, מסרונים והודעות צ'אט ברשתות חברתיות. הלקוחות גם יכולים לצפות בדוחות ובסטטיסטיקות של פעילותן באמצעות הממשק של חברת ההפצה.[28] לקוח יכול לבחור לבקש להשתמש ברשימת תפוצה של החברה ולשלוח מסר לרשימה דרך החברה, להתקין יישומון של חברת ההפצה וממנו מבצעים את שליחת המסרים, או להשתמש ביישומון קיים, כאשר חברת ההפצה מספקת רק כתובת לשליחה דרכה אפשר להפיץ את המסרים. בכל אחד מאופנים אלה, יש לבצע הזדהות מרחוק מול חברת ההפצה.

בישראל פועלות היום כחמש חברות הפצה גדולות. ככל הידוע, פעילות החברות אינה מקומית בלבד, ויש להן לקוחות בכל העולם. לחברות ההפצה יש מידע על זהות הלקוח שלהן, משום שזה מקור ההכנסה שלהן. מעבר לכך, לחברות ההפצה יש אינטרס **בבירור אופי הפעילות של הלקוח**. הסיבה לכך היא שהתנהגות הלקוחות עלולה

---

25 לבצ'נקו, לעיל ה"ש 3, בעמ' 11.

26 שם, בעמ' 9.

27 רע"א 132618 **סמארט קלאב אחזקות בע"מ נ' כהן** (נבו 31.12.2020), בפס' 11 לפסק דינה של השופטת ברון.

28 בדרך כלל, חברות אלה אינן נתבעות; מספר מקרים בודדים של תביעות נגד חברות הפצה התנהלו בישראל, נגד "פולסים" ונגד "טלזר". ראו ת"ק (קריות) 6028-04-16 **אלרון נ' גליקום שיווק בע"מ ופולסים בע"מ** (נבו, 30.3.2017) וכן: ת"ק (ת"א) 14072-02-18 **חיים נ' פולסים בע"מ** (נבו 6.5.2019); וגם ת"ק (טבריה) 2881-03-19 **דהרי נ' טלזר 019 שרותי תקשורת בינלאומיים בע"מ** (נבו, 7.4.2014). בכל זאת, קיים הבדל בין שתי החברות: ל"טלזר" יש רישיון מכוח חוק התקשורת כך שלכאורה לפחות היא הייתה אמורה להיות מוחרגת מהגדרת "מפרסם", בעוד ש"פולסים" אינה מחזיקה ברישיון והיא עושה שימוש בחברת תקשורת לצורך ההפצה בפועל.

להשליך על הפעילות של חברות ההפצה. כאשר לקוחות מפרים את חוק הספאם (או חוקים אחרים) ושולחים ספאם מכתובת ה-IP של חברות ההפצה, יש חשש שחברות ההפצה יסומנו ברשימות שחורות של שירותי אנטי-ספאם, והשירות שלהן ייחסם חלקית או בכלל, גם עבור לקוחות אחרים שעסקיהם כשרים.[29] בהתאם, אינטרס חשוב של חברות ההפצה הוא **ל"תפוס" ספאמרים**. כדברי נאור מן, בעל חברת הפצה מקומית, בשיחה איתנו, "לי יש אינטרס לתפוס אותו יותר מהמדינה." הסיבה לכך היא שהרשימות השחורות של חברות האנטי-ספאם הן גורם מרתיע יותר מהמדינה וממערכת החוק שלה, או כדברי בעל החברה בשיחה איתנו, "הם [חברות האנטי-ספאם] האכיפה דה פקטו, הם החוק והם אכזריים. הם לא מושפעים מכלום אבל משפיעים המון."[30] אם פלטפורמה של חברת הפצה נכנסת לרשימה שחורה, קשה מאוד ל"צאת" מהרשימה לפני שייפגעו לקוחות נוספים של החברה. חברות ההפצה חוסמות לפיכך חשבונות רבים עוד בטרם דווחו כחשבונות מהם נשלח ספאם, רק כדי להימנע מכניסה לרשימה שחורה.

במילים אחרות, המענה הטכנולוגי לספאם של יצירת רשימות שחורות, יוצר מנגנון שוק שהופך את חברות ההפצה לגורם שיכול, וכנראה גם פועל, לצמצום הספאם, בשל הרצון להגן על האינטרסים שלו עצמו. הפתרון, כמובן, אינו מושלם.

שאלה מרכזית היא הדין שחל על חברות ההפצה, נושא שנרחיב בו בפרק הבא. נקדים ונאמר, שבישראל, חוק התקשורת (בזק ושידורים), התשמ"ב-1982, אינו חל על חברות ההפצה.[31] החוק הישראלי מתייחס להפצת ספאם, אבל מחריג את חברות התקשורת מאחריות על הפצה אסורה: סעיף 30א(א), מגדיר מיהו "מפרסם", ומחריג "מי שביצע, בעבור אחר, פעולת שיגור של דבר פרסומת כשירות בזק לפי רישיון או תקנות ההיתר הכללי, לפי העניין". שינוי המצב הקיים בישראל אינו בטווח הנראה לעין. אחת הסיבות לכך היא ככל הנראה היעדר תקציבים של משרד התקשורת, והישענותו על תשתית משפטית של חוק התקשורת. נרחיב על כך בפרק ג.

אינטרס נוסף של חברות ההפצה הוא **להימנע מתיוג שלילי**. בדיון בכנסת, בעלי העסקים שמרכולתם נוגעת לדיוור ישיר התלוננו על תיוגם על ידי החוק החדש כפושעים וכעבריינים.[32]

לסיכום חלק זה: רשתות השותפים וחברות ההפצה הם גורמי ביניים מרכזיים שמסייעים למשווקים להפיץ הודעות מסחריות (בשלב ההפצה). בעוד שרשתות השותפים אטרקטיביות עבור ספאמרים מקצועיים ועבור כל שחקן שמבקש להרחיק את עצמו מאחריות מידית לשליחת ספאם, מקומן של חברות ההפצה בזירה אמביוולנטי יותר ביחס לספאם. הן מציעות שירות חוקי כשלעצמו, אבל יש חשש שינוצל לרעה.

בפועל, שולחי ספאם מקצועיים מסכנים את עסקיהן של חברות ההפצה, ולכן יש להן אינטרס לעמוד על המשמר בקשר לשימוש בשירות שלהן. בהתאם, בשלב זה בשרשרת הערך, יעד מרכזי לרגולציה הוא רשתות השותפים, ובצד זה, יש לטפח את האינטרס של חברות ההפצה להמשיך ולעמוד על המשמר. בעת הזו יש להן אינטרס מסחרי שלהן לעשות כך, אולם יש לגבותו גם בהטלת אחריות משפטית במקרים המתאימים.

---

29 בפרק ד נרחיב על אודות שירותי אנטי-ספאם. נקדים ונאמר כי מדובר בעיקר בשירותים פרטיים הפועלים בשרתי חברות המספקות שירותי תקשורת, או בהתקנים של המשתמשים עצמם. Duncan Cook, Jacky Hartnett, Kevin Manderson and Joel Scanlan, *Catching Spam Before it Arrives: Domain Specific Dynamic Blacklists*, 54 Proceedings of the 2006 Australasian Workshops on Grid Computing and E-Research-Volume 2 (2006); "ואלה שמות: רשימה שחורה של אתרי ספאם", **Ynet** (3.3.10), נמצא ב: https://www.ynet.co.il/articles/0,7340,L-3857218,00.html.

30 מתוך שיחה שהתקיימה ביום 1.6.2022.

31 ראו ההגדרה למונח "מפרסם" בס' 30א(א) לחוק התקשורת (בזק ושידורים), התשמ"ב-1982: "'מפרסם' – מי ששמו או מענו מופיעים בדבר הפרסומת כמען להתקשרות לשם רכישת של נושא דבר הפרסומת, מי שתוכנו של דבר הפרסומת עשוי לפרסם את עסקיו או לקדם את מטרותיו, ובכלל זה לקדם קבלת תרומות או תעמולה, או מי שמשווק את נושא דבר הפרסומת בעבור אחר; לעניין זה, לא יראו כמפרסם מי שביצע, בעבור אחר, פעולת שיגור של דבר פרסומת כשירות בזק לפי רישיון או תקנות ההיתר הכללי, לפי העניין.

32 דיון הוועדה המשותפת מיום 25.12.2007, לעיל ה"ש 9, דברי מיכה בצלאלי בעמ' 29 ודברי עו"ד אמנון זכרוני בעמ' 37.

3. צד הנמענים: המלחמה בספאם

סקרנו את הצד שיוזם את הפצת המסרים השיווקיים ואת מי שמסייעים לו מאחורי הקלעים בשלב שלפני ההפצה (חברות הלידים, רשתות השותפים), ובשלב ההפצה (חברות ההפצה). שחקנים משמעותיים בזירת הספאם הם מי שנמצאים מנגד, ומנסים להיאבק בהיבטים השליליים של התופעה. בכך עוסק חלק זה. נפתח במדינה, שהיא שחקן מרכזי בזירת הספאם. נעבור לציבור, הנפגע המרכזי מתופעת הספאם, ונדון בגופים פרטיים מסוגים שונים שפועלים למיגור התופעה. לבסוף, נתייחס לזירה הבין-לאומית, שם המדינה שותפה במאבק בספאם כשחקן אחד מיני רבים.

א. המדינה

בצד שעניינו המלחמה בספאם, המדינה היא שחקן מרכזי. הטעם לכך, מעבר לכוחה לחוקק ולאכוף סנקציות, הוא ריבוי הכובעים בהם היא אוחזת בזירת הספאם. הדבר ניכר עוד בשנת 2005, כשנערך בכנסת דיון לשם קביעת הוועדה שתטפל בהליכי החקיקה של חוק הספאם, ועלו ארבע חלופות בתשובה לשאלה מי הוועדה המתאימה לעסוק בנושא: ועדת הכלכלה, ועדת מדע וטכנולוגיה, ועדה משותפת לשתי אלה, וכן ועדת האינטרנט. ריבוי החלופות מעיד על מורכבות הנושא ועל הרלוונטיות שלו למגוון שחקנים בזירה הפוליטית.[33] נפרט כעת את החבויות והאינטרסים של המדינה.

<u>הגנה על האזרח:</u> המדינה אמונה על הגנה על זכויות אזרחיה,[34] כמו **זכותם לפרטיות**[35] וזכותם ל**הגנה מפני מטרדים**,[36] שלגביהן נפרט בהרחבה בפרק הבא, העוסק במשפט הספאם.

<u>הגנה על השוק:</u> המדינה אמונה על הגנת זכויותיהם של סקטורים שונים באוכלוסייה, למשל על **זכויות הקניין וחופש העיסוק** של גופים מסחריים, קטנים כגדולים, שפרסום ושיווק הם צורך הכרחי עבורם, לשם קיום רווחי של עסקיהם. בדיונים בכנסת טען אלי שחף, יו"ר חטיבת השיווק הישיר ומנכ"ל חברת "עסקה טובה", שהפעילה אתרי מכירות באינטרנט, שחוק הספאם יביא לפגיעה בחופש העיסוק של משווקים.[37] בעלי חברות שעוסקות במתן שירותי מוקד טלפוני טענו מפורשות שחוק הספאם יפגע אנושות בעסקיהם.[38] שאלת הפגיעה בחופש העיסוק עלתה סביב סוגיות שונות, לדוגמה סביב השאלה מה יהיו סוגי התקשורת שהחוק יחול עליהם. כך למשל ראש ועדת המדע והטכנולוגיה דאז, ח"כ בנימין אֱלון, הציע להחיל את החוק רק על פקסים ועל דוא"ל, שכן לטענתו הם המטרד הגדול ביותר (דוא"ל דורש מיון; פקסים צורכים נייר ודיו), לעומת שיחות והודעות טקסט, שחשובות לשוק חופשי. אֱלון טען שהדבר יכרות ענף שלם של שיווק, ולכן הציע שבנוגע לשיחות ולהודעות טקסט, יתקבל המודל האמריקני שהיה בשעתו.[39] נעיר שדוגמאות אלה מעידות גם על היותה של זירת הספאם תלוית-טכנולוגיה: עלויות ההפצה משליכות על כדאיות השימוש באפיקי הפצה שונים, ואלה משתנים לפי שינויים טכנולוגיים. נרחיב על כך בפרק ד.

גם היום, המדינה מבקשת להגן על התקשורת המקוונת, אך בלי לפגוע בפעולתו החופשית ככל האפשר של השוק. ספקיות שירות, הן בתחום התשתיות והן בתחום שירותי התקשורת, הן חלק מרכזי משוק התקשורת. למדינה יש אינטרס בקיומה של **תשתית מקוונת תקינה** ובקיומם של **שירותים מקוונים ברמה טובה** הן עבור האזרחים והן עבור

33 ראו פרוטוקול ישיבה 259 של ועדת הכנסת, בעמ' 12 (9.8.2005). בעוד שח"כ מיכאל איתן ניסה לשכנע את המשתתפים בכך שנכון להעביר את ההצעה לוועדת המדע והטכנולוגיה, יו"ר הוועדה רוני בר-און מציין שהתחייב בפני יו"ר וועדת הכלכלה, שאינו נוכח, שהעניין לא יוכרע בהעדרו. הדיון נפסק וההחלטה נדחתה.

34 ראו למשל אהרן ברק "הזכות החוקתית והפגיעה בה: תורת שלושת השלבים" **משפט וממשל** יט 119, 133 (2018).

35 מיכאל בירנהק **פרטיות חוקתית** 258 (2023).

36 למקורות ממארג חקיקתי שנועד להגן על הזכות להגנה מפני מטרד, ראו חוק למניעת הטרדה מינית, התשנ"ח-1998; חוק הגנת הפרטיות, התשמ"א-1981, ס' 2(1) ("בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת"); חוק המקרקעין, התשכ"ט-1969, ס' 14 ("בעלות וזכויות אחרות במקרקעין, אין בהן כשלעצמן כדי להצדיק עשיית דבר הגורם נזק או אי נוחות לאחר"); פקודת הנזיקין [נוסח חדש], פרק ג', סימן ה' ("מיטרדים"); חוק למניעת מפגעים, התשכ"א-1961.

37 פרוטוקול ישיבה 3 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 35 (27.11.2007).

38 ראו למשל דבריו של אלדד גת, מנכ"ל חברת טלאול קונטקט סנטר, בפרוטוקול ישיבה 1 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (20.11.2006), וכן בפרוטוקול ישיבה 2 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (31.1.2007).

39 פרוטוקול ישיבה 6 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (1.4.2008).

פעילותה של המדינה עצמה, על אורגניה השונים. בהמשך לכך, אינטרס חשוב של המדינה הוא **הגנה ואף טיפוח איכות טובה של פעילות בזירה המקוונת**. לשם כך על המדינה להגן על האינטרסים של ספקיות שירות, הן בתחום התשתיות והן בתחום שירותי התקשורת. על אינטרסים אלו נרחיב בחלקו הבא של הפרק.

אינטרס נלווה הוא **הגנה על עובדי חברות** הפצה ושיווק. במהלך חקיקת התיקון הגיב יו"ר הוועדה המשותפת, משה כחלון לטענה לפיה קבלת התיקון לחוק התקשורת תביא לפיטורי מאות עובדים בחברות שיווק שהחוק יהפוך לאסור, בדברים הבאים: "אנחנו באים להגן על מיליונים שסובלים. אז או שנגן על מאות או שנגן על מיליונים. צריך למצוא את האיזון המתאים."[40]

המתח המובנה בין חובת המדינה להגן על אזרחים מפני הצפה של תקשורת לא רצויה, לבין חובתה להגן על זכויותיהם של שחקני שוק שונים, התבטאה בדיונים שנערכו לקראת חקיקת חוק הספאם. המתח בלט ביותר בדיונים סביב השאלה האם יש ליישם את המודל האמריקני, של הקמת מאגר מרכזי שבו פרטיהם של אזרחים המסרבים לקבל דואר שיווקי. תומכי המודל טענו שהקמת המאגר תשמש איזון ראוי בין הגנה על האזרח מפני תקשורת לא רצויה, לבין חופש העיסוק של המשווקים. מתנגדי המודל האמריקני סברו שבהקמתו יש הטיה לכיוון המשווקים שלהם הכוח הכלכלי: "הקו האמריקאי הלך לכיוון של המשווקים. אלה הלוביסטים שאני רואה מול העיניים שלי. מה הם דוחפים? זה יותר הצד של החברות שרוצות להשתמש בזה ולהרוויח מזה כסף. זה לא פוסל, אבל הם האינטרסנטים היותר גדולים. בצד השני, עומדים אנשים... אנחנו צריכים להגן מפניהם."[41] לדברי יו"ר ועדת הכלכלה דאז, ח"כ גלעד ארדן, הממשלה הציבה שתי אופציות – לקבל את החוק כמו שהוא, ללא המאגר, או לא לקבל אותו כלל. ארדן אמר מפורשות שהוא בעד יישום המודל האמריקני, אולם מכיוון שהוא מעדיף את הצרכנים, הוא יקבל את החוק גם אינו מושלם בעיניו, משום שהוא "עדיף מכלום".[42]

בתמונה הכללית יש שיקולים נוספים, מסדר שני, שעשויים גם הם להיכנס לתמונה, למשל **הגנת הסביבה**. כאמור, לאפיקי הפצה שונים עלויות שונות. הגבלות על אפיקים מסוימים עשויות להביא לעליית השימוש באפיקים חלופיים. לכל אפיק כזה השלכה שונה על הסביבה. בדרך כלל, יש העדפה ציבורית לתקשורת מקוונת על פני תקשורת פיזית, מפני שהיא מבטלת צורך בשימוש בנייר. לעומת זאת, הרטוריקה סביב הספאם היא הפוכה, בשל הפן הכלכלי האמור: למשל, הגבלות על שיווק מקוון כדי לצמצם מטרד לאזרחים עשויות להגביר את השימוש בנייר לצורך הפצת מסרים שיווקיים.[43]

<u>המערך המקוון של המדינה עצמה:</u> בנוסף, חלק לא מבוטל של פעילות המדינה עצמה, על גופיה הרבים, נעשה תוך שימוש בכלים מקוונים. לפיכך, המדינה עצמה מבקשת להגן על עצמה כנמענת מפני תקשורת לא רצויה. בימים הראשונים של הדיונים לקראת חקיקת חוק הספאם, הפרויקט הממשלתי תהיל"ה עמל על סינון דואר זבל, כפי שציין נציג איגוד האינטרנט בדיונים, עו"ד חיים רביה. לטענת רביה עובדה זו הביאה לכך שמשרד המשפטים אינו רגיש לסוגיית הספאם.[44]

<u>שימוש במערך המקוון של המדינה לשם הפצת מסרים</u>

גופים שונים במגזר הציבורי מבקשים להפיץ מסרים לאזרחים, ולכן למדינה יש אינטרס שהגדרת הספאם לא תהיה רחבה מדי ושלא תכלול תקשורת רצויה למדינה עצמה. דוגמה לכך ניתנה בדיון בכנסת, שם נציג קופת חולים כללית טען שההגדרה שבחוק שכוללת "מסר המופץ באופן מסחרי שמטרתו לעודד רכישת מוצר או שירות" רחבה מדי ויש

---

40 בפרוטוקול ישיבה 1 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 14 (20.11.2006).

41 דברי ח"כ מיכאל איתן, פרוטוקול ישיבה 139 של ועדת המדע והטכנולוגיה, בעמ' 18 (26.7.2005).

42 פרוטוקול ישיבה 6 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (1.4.2008).

43 במהלך דיוני הוועדה המשותפת, נציגי חברות העוסקות בשיווק ישיר טענו שהדיוור הישיר הפיזי, דוגמת דואר זבל פיזי המגיע לתיבות הדואר הפיזיות של אזרחים ותושבים, פוגע יותר מבחינה סביבתית, ושבהצעת החוק משרד התקשורת קורא לעסקים לזהם יותר את הסביבה, בכך שהוא אוסר על דיוור טלפוני: "בוודאי, זה נזק הרבה יותר גדול לסביבה. בואו נסתכל לאן דוחף משרד התקשורת את עולם העסקים הישראלי: לצרוך עוד נייר, לגדוע עוד יערות בכל העולם – והרי עכשיו מאוד פופולרי הנושא האקולוגי - לזהם לנו את תיבות הדואר ואת השכונות כשאף אחד לא מנקה אחריהם. זה כן חוקי, אבל הודעה קולית שזה הדבר הנקי ביותר, שמשך הזמן שלה הוא 30 שניות ואדם יכול לשמוע שנייה אחת ואם זה לא מוצא חן בעיניו לסגור את הטלפון, זה יהיה אסור." דברי אלדד גת, מנכ"ל טלאול, בדיון השני של הוועדה המשותפת. בפרק ה נדון במטפורה של הניקיון ובקשריה עם עולם הספאם.

44 ראו דיון ראשון של הוועדה המשותפת (20.11.2006).

להחריג קופות חולים. הדוגמה שהביא היא מקרה בו שולחים הודעה למבוטח הקופה לפיה מגיע לו טיפול שיניים חינם. בתגובה הובהר שהכוונה לא הייתה להגביל שירותים חינמיים, ושהחוק חל על פעולות שהן שידול לרכישה.[45]

סוגיה דומה עלתה בדיון בנוגע להחרגת מסרים פוליטיים מ"דבר פרסומת" שבהגדרת החוק. בדיון בסעיף ההגדרות, שאל עו"ד דן חי, אז יו"ר הוועדה להגנת הפרטיות בלשכת עורכי הדין, מדוע לא לכלול ב"דבר פרסומת" גם מסרים פוליטיים. בתשובה לכך טען ח"כ ארדן שהדבר נועד **לעודד מעורבות חברתית בפוליטיקה**.[46]

הזירה הבין-לאומית: לאלה, יש להוסיף את מקומה של המדינה כאחת מני רבות בזירה הבין-לאומית. למדינה יש אינטרס להפגין את מאמציה **להגן על הזירה המקוונת הגלובלית** ולשמר סטנדרט שלא יפגע במעמדה בזירה הבין-לאומית בתחום ההגנה על משתמשי האינטרנט. משכך, עליה להתאים את הכללים המשפטיים למקובל בעולם, לכל הפחות בעולם המערבי, וכן להפנות מאמצי אכיפה לספאם שמקורו בישראל. כבר בדיון הראשון של הוועדה בכנסת עלתה הטענה שלפיה ספאם הוא תופעת רוחב הדורשת שיתופי פעולה בין-לאומיים והגוררת נזקים במיליארדי דולרים, וזאת בניגוד לעמדתו לכאורה של משרד המשפטים, שהדגישה את הנזק לפרט הבודד שנפגע.[47] ח"כ ארדן טען שישראל "הופכת להיות גם הכר שממנו שולחים למדינות אחרות בעולם, וזה לא הדבר הכי טוב למדינת ישראל משום שכרגע צוות בודק את הצטרפותנו ל-OECD, וגם נפגש איתנו, והעלה את הנושא הזה".[48]

מהאמור נובע שהמדינה מצויה בצומת של אינטרסים רבים שלעיתים מתנגשים, וביניהם עליה לנווט. רצונה של המדינה למגר את תופעת הספאם מציף מתחים מול שחקנים שונים בשרשרת הערך של הספאם, שמבקשים הגנה על זכויות הקניין וחופש העיסוק שלהם. המדינה גם מחויבת להגן על חופש הביטוי של משתמשי שירותי התקשורת, ולכן עליה להיזהר מלהטיל רשת צפופה מדי של סייגים על משלוח מסרי תקשורת. המדינה גם מבקשת להגן על יכולותיה להשתמש באופן מיטבי בכלי תקשורת על מנת להעביר מסרים מטעמה, וכן להגן על מעמדה בזירה הבין-לאומית המקוונת.

אורגנים של המדינה העוסקים (גם) באנטי-ספאם

<u>בתי המשפט</u>

החוק מסמיך את בתי המשפט לפסוק בעניין קנסות ופיצויים בגין עבירות על חוק הספאם. כך, במקרה של פרסום בניגוד לסעיפים 30א(ב) או 30א(ג) בית המשפט מוסמך להטיל קנס עד 226,000 ש"ח.[49] במקרה של פרסום שלא צוינו בו הפרטים האמורים בסעיף 30א(ה) באופן בולט וברור, או שיש בפרטים שצוינו כדי להטעות, בניגוד להוראות אותו סעיף, בית המשפט מוסמך להטיל קנס עד 75,300 ש"ח.[50] במקרה של הפרה לפי סעיף 30א לחוק התקשורת בית המשפט רשאי להטיל פיצויים לדוגמה, ללא הוכחת נזק, עד לסכום של 1,000 ש"ח.51 החוק מפרט את השיקולים שעל בית המשפט לשקול כאשר הוא פוסק פיצויים לדוגמה. אלה הם אכיפת החוק והרתעה, עידוד מימוש זכויות ושאלת היקף ההפרה.[52]

<u>הרשות להגנת הפרטיות</u>

הרשות, שהיא יחידה בתוך משרד המשפטים ובראשה עומד רשם מאגרי המידע שיש לו סמכויות שונות לפי חוק הגנת הפרטיות, אחראית על פיקוח חוק הגנת הפרטיות, לפי סעיף 10(ה) לחוק. לרשות אין סמכויות ישירות בנושא הספאם, למעט בכל הנוגע לדיוור ישיר אליו מתייחס חוק הגנת הפרטיות. סימן ב בפרק ב של החוק מכיל הוראות בדבר

45 פרוטוקול ישיבה 6 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (1.4.2008).

46 פרוטוקול ישיבה 5 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (25.3.2008).

47 דברי עו"ד חיים רביה מטעם איגוד האינטרנט, פרוטוקול ישיבה 1 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (20.11.2006).

48 פרוטוקול ישיבה 5 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 11 (25.3.2008).

49 ס' 30א(ו)(1) לחוק התקשורת, ס' 61(א)(4) לחוק העונשין.

50 ס' 30א(ו)(2) לחוק התקשורת, ס' 61(א)(3) לחוק העונשין.

51 ס' 30א(י)(1) לחוק התקשורת.

52 ס' 30א(י)(3).

דיוור ישיר, שמוגדר כ"פנייה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע". פניה היא "לרבות בכתב, בדפוס, בטלפון, בפקסימליה, בדרך ממוחשבת או באמצעי אחר".[53] כאשר מדובר ב"מגארי מידע" כהגדרתם בחוק (סעיף 7), ובאיסוף ועיבוד מידע בקשר למאגר כזה, יש לרשות סמכויות לפי פרק ב של החוק.

<u>משרד התקשורת</u>

משרד התקשורת אחראי על הענקת רישיונות בזק, כאשר גוף תקשורת הפועל עם רישיון מוחרג מהגדרת "מפרסם" בחוק הספאם, בעוד שגוף תקשורת הפועל ללא רישיון כזה לא ייהנה מהגנה דומה של החוק. הסמכות להעניק רישיונות בזק היא של שר התקשורת.[54] עם זאת סמכות זו הואצלה בחלקה למנהל הכללי של משרד התקשורת.[55] שר התקשורת האציל למנהל הכללי של משרד התקשורת את הסמכות לדרוש, לפי סעיף 4ג1 לחוק, מבעל רישיון או ממי שפועל מטעמו למסור לו כל מידע הנחוץ לשם הפעלת סמכויות שר התקשורת לפי החוק או כדי להקל על ביצוען.[56]

<u>הרשות להגנת הצרכן</u>

הרשות אחראית להקמת מאגר "אל תתקשרו אליי", אליו ניתן להירשם כדי למנוע שיחות שיווקיות.[57] המאגר החל לפעול בסוף שנת 2022. על המאגר נרחיב בפרק ג, העוסק במשפט הספאם, ובפרק ד העוסק בטכנולוגיות אנטי-ספאם.

לסיכום חלק זה: למדינה אינטרס להגן על הציבור מפני הטרדה, אבל גם חובה שלא לפגוע באופן לא מידתי בזכויות ואינטרסים של בעלי עסקים; למדינה אינטרס לאפשר דיוור של מידע מגופים ציבוריים כמו גם לא לפגוע בחופש הביטוי הפוליטי. במדינה יש מספר רשויות שיש להן נגיעה לנושא הספאם, אבל כל אחת מהן עוסקת במקטע אחר של השרשרת, ואין אף גורם שיש לו סמכות מלאה.

ב. הציבור (משתמשי קצה) ומייצגיו (עמותות הפועלות נגד ספאם)

(1) הציבור הרחב – נפגעי הספאם

בעוד שהציבור הרחב עשוי להתרעם על פרסום שלא הוזמן (unsolicited) באופן כללי, סביר שצרכנים מנוסים התרגלו לרעיון שפרסום הוא מחיר שיש לשלם עבור גישה לתוכן ולשירותים שהם מעריכים או זקוקים להם. לעומת זאת, ספאם, או פרסום לא רצוי ללא הסכמה, כופה על צרכנים חשיפה שלילית, ללא כל תועלת חיובית כלכלית, וללא יכולת לחזור בהם מהסכמה.

<u>צרכני שירותי תקשורת</u>: האינטרסים של ציבור צרכני שירותי התקשורת נחלקים לשניים – כנמענים, לציבור הצרכנים יש אינטרס **לקבל מסרי תקשורת רצויים**, לא יותר מכך (ספאם) ולא פחות מכך (מסר שסונן כי נחשב בטעות לספאם). לעיתים, צרכני שירותי התקשורת משתמשים בשירותים אלה כדי לשלוח מסרים בעצמם, שאז הם הופכים להיות המוענים. כמוענים, לציבור הצרכנים עומדת זכותם ל**חופש הביטוי**, והגנה על זכות זו משמעה שמסרים מוגנים יגיעו לנמעניהם.

53 ס' 17ג לחוק הגנת הפרטיות. ס' 17ו לחוק מונה מספר חובות על פניות בדיוור ישיר וזכויות של נושאי המידע במאגרים המשמשים לדיוור ישיר.

54 ס' 4(א) לחוק התקשורת.

55 ראו י"פ תשע"ד מס' 6800 מיום 12.5.2014 עמ' 5465: סמכות לפי ס' 4 לחוק התקשורת, להעניק רישיון מיוחד, לשנות תנאי רישיון מיוחד, להוסיף עליהם או לגרוע מהם; הסמכות לפי ס' 4(ה) לחוק התקשורת, לשנות תנאי רישיון כללי, להוסיף עליהם או לגרוע מהם; הסמכות לפי ס' 4(ד2)(1) לחוק התקשורת, לאשר שינוי בהחזקה, העברה או רכישה של אמצעי שליטה בבעל רישיון כללי.

56 ראו י"פ תשע"ה מס' 7078 מיום 20.7.2015 עמ' 7453.

57 ראו באתר הרשות להגנת הצרכן: https://www.gov.il/he/departments/news/altitkasher.

צרכני שירותי תקשורת אינם עשויים מקשה אחת, גם לא בעניין הספאם. יכולת ההתגוננות של האזרח מפני תקשורת לא רצויה תלויה במידה לא מבוטלת **באוריינות דיגיטלית**.[58] אוריינות דיגיטלית גבוהה תורמת ליכולתו של הפרט להבין טוב יותר את אופני הפעולה של הזירה המקוונת ולהיטיב להתגונן מפני פעילות שאינה רצויה לו. לעומת זאת, אוריינות דיגיטלית נמוכה, מונעת הבנה ובעקבות כך גישה לאמצעי הגנה, אפילו בסיסיים, כמו למשל הפעלה של אופציית סינון טכנולוגי במכשיר הנייד. במקרים של אוריינות דיגיטלית נמוכה, המשתמש הופך לטרף קל לשחקנים זדוניים. לא כל אחד יכול להתמודד בעצמו או להבין כיצד להתקין ולהסיר תוכנות ויישומים שיוכלו למנוע ולסנן תקשורת לא רצויה.

(2) מייצגי הציבור

שחקנים שונים בזירת הספאם מבקשים להגן על הציבור בכללותו, ומקדישים לכך את פעילותם. במובן זה, הם מיצגיו של הציבור ושל האינטרסים שלו ולכן נכללים עמו באותה קטגוריה.

<u>עמותות למלחמה בספאם</u>

שחקן בולט בקבוצה זו הוא עמותת "אל ספאם", שהוקמה במיוחד לשם מיגור תופעת הספאם בישראל, ושמה לעצמה למטרה "להילחם, למען הציבור, עבור סביבה נקייה מפרסומות לא רצויות."[59] העמותה מבקשת "למגר את תופעת דואר הזבל באמצעות הנגשת מידע לציבור ופעולה באפיקים משפטיים."[60] העמותה פועלת באמצעות השתתפות נציגיה בדיונים בוועדות הכנסת, סיוע במימון ערעורים לבית המשפט, הצטרפות להליכים בתור ידיד בית משפט בהליכים עקרוניים והתנגדויות לפשרות בתביעות ייצוגיות,[61] הפצה והנגשת מידע לציבור.[62] העמותה מנהלת אתר מקוון המכיל חומר עזר לנפגעי ספאם.[63] משתמשים שואלים שאלות משפטיות בנוגע לספאם (למשל איך לתבוע; מתי הודעה מסוימת עונה להגדרת הספאם, והאם ספאם מסוים מוכר למישהו). מימון העמותה מתבסס בעיקר על תרומות ועל הכנסות מדמי חבר. בשנים 2020 ו-2022 נתח מכובד מהמימון הגיע ממתן "שירותים כללים".[64]

עמותה נוספת שפעילה בנושא היא "העמותה למלחמה בספאם",[65] שמטרתה היא "מתן סיוע מקיף לציבור הרחב בהתמודדותו בתופעת ההפצה ההמונית של הפצת פרסומות בלתי רצויות המכונה 'ספאם'" ולמיגור התופעה".[66] דרכי הפעולה העיקריות שלה הן דיווח לגורמי ממשל על עברייני ספאם, ובכלל זה המשטרה, ובקשות לשיפור המצב המשפטי הקיים לטובת נפגעי ספאם; סיוע לנפגעי ספאם במיצוי זכויותיהם (הדרכה והכוונה ללא תשלום בהגשת תביעות ספאם, מענה לשאלות); העלאת מודעות; הגשת בקשות חופש מידע לרשויות ציבוריות בעניינים הקשורים למניעת ספאם, פגיעה בפרטיות והטרדה טלפונית; השתתפות נציגי העמותה בדיונים בוועדות הכנסת בעניינים קשורים; ועוד.[67]

58 אוריינות דיגיטלית היא שליטה במגוון הולך וגדל של מיומנויות טכניות, קוגניטיביות וסוציולוגיות הנדרשות לשם ביצוע מטלות ולפתרון בעיות בסביבות דיגיטליות. ראו יורם עשת-אלקלעי "אוריינות דיגיטאלית: מסגרת מושגית עבור מיומנויות חשיבה בעידן הדיגיטאלי", איגוד האינטרנט הישראלי (6.11.2004). ראו https://www.isoc.org.il/research/magazine/digital-literacy-a-conceptual-framework-for-think-ing-skills-in-the-digital-age.

59 על העמותה, ראו באתר גיידסטאר: https://www.guidestar.org.il/organization/580607182.

60 מתוך עמוד הפייסבוק של העמותה, ראו: https://www.facebook.com/alspamisrael. זאת גם לפי תעודת רישום העמותה: https://tinyurl.com/3xsmkdhk.

61 פסק דין יחיד שבו העמותה הייתה צד להליך הוא ע"א 6521/21 **עמותת אל ספאם נ' חאיק** (נבו 7.2.2022). העמותה התנגדה להסדר פשרה של תובענה ייצוגית. אחד ממייסדי העמותה הפעיל בה עד היום, עו"ד זיו גלסברג, היה מעורב כתובע בתיקים רבים, שאחד מהם, הנוגע לגובה הפיצוי על הודעות זבל, הגיע לבית המשפט העליון. ראו רע"א 2904/14 **גלסברג נ' קלאב רמון בע"מ** (נבו 27.7.2014).

62 ראו: https://tinyurl.com/35md7u2c.

63 ראו: https://alspam.org/#. וכן ראו עמוד פייסבוק https://www.facebook.com/alspamisrael.

64 https://www.guidestar.org.il/organization/580607182/finances.

65 לעמוד הפייסבוק של העמותה, ראו: https://www.facebook.com/amutaspam/?locale=he_IL.

66 https://www.guidestar.org.il/VF_View_File?guid=7eda203f2f2e997-6864b9a911648f3a-d5c342f47900c8e793d-d308cbb3491374658eef60f35e1b5054edf7e98d4bf46-920fe24b493c4be8-ef3fd706305f55911.

67 https://www.guidestar.org.il/VF_View_File?guid=72ced9a846b0d58-07b0caaf2f1a87c0-b05ed2b9ce80edf97b04596217eb43574e0c37310e4d4878a4a5ccd9f8e5cc6c-26d95c7a8e9b5388-6ffcd4fe02934751e.

בשני המקרים, העמותות הוקמו על ידי עורכי דין שעוסקים בתביעות ספאם ומכירים את התופעה על בוריה. חבר הוועד בעמותת אל ספאם ואחד ממקימיה הוא עו"ד זיו גלסברג,[68] שהוא שחקן חוזר בבית המשפט בעניין תביעות ספאם. ב"עמותה למלחמה בספאם" חבר הוועד עו"ד עמית זילברג הוא בעל משרד שמתמחה בין השאר בתביעות ספאם.[69]

<u>איגוד האינטרנט הישראלי</u>

בין ארגוני החברה האזרחית הפועלים לשם מיגור תופעת הספאם והגברת מודעות ציבורית לנושא, בולט איגוד האינטרנט הישראלי. נציגי הארגון השתתפו בדיונים לקראת חקיקת חוק הספאם והשמיעו את קולם בסוגיות הקשורות לספאם במהלך השנים שחלפו מעת החקיקה ועד היום.[70] באתר האיגוד אפשר למצוא בין השאר כתב תביעה לדוגמה למי שמבקש לתבוע בגין ספאם.[71]

ג. גורמים פרטיים

בצד המדינה, וארגונים בחברה האזרחית, פועלים בזירה גם שחקנים פרטיים, שפועלים באופן משפטי למיגור הספאם. מבין אלה, נציג בקצרה את חברת "ספאם אוף", שהייתה מיזם פרטי שפעל לסייע לנפגעי ספאם להגיש תביעות קטנות, את עורכי הדין שמתמחים בתביעות ספאם ייצוגיות, ואת חברות הטכנולוגיה המייצרות טכנולוגיות אנטי-ספאם.

(1) עסקים פרטיים שפועלים נגד ספאם

אחת התופעות המעניינות בתחום המלחמה בספאם היא מיזם טכנולוגי-משפטי שהציע כלי סיוע לאזרח הפשוט לתבוע ספאמרים. המיזם, שנקרא "ספאם אוף", אינו פועל יותר, אולם ניתוח פעילותו, שד"ר אסף וינר מאיגוד האינטרנט כינה בשם "ניסוי טבעי", מאפשרת לימוד של טווח הכלים העומדים לרשות מי שעניינו המלחמה בספאם.

<u>"ספאם אוף"</u>

החברה פעלה בשנים 2015-2017. היא הוקמה כדי לשרת שני אינטרסים מרכזיים. הראשון היה האינטרס הערכי במיגור הספאם, לטובת הציבור. השני היה אינטרס כלכלי, כאשר ככל עסק פרטי אחר החברה ביקשה להרוויח מהמלחמה בספאם. החברה הדגימה את הפרדוקס שבהתנגשות שני האינטרסים הללו. כל מי שעיסוקו אנטי-ספאם והוא עסק רווחי, עשוי להיקלע לדילמה: מובן שחברה כזו מסתכנת בכריתת הענף עליו היא יושבת, שהרי אילו הייתה מצליחה במיגור מלא של תופעת הספאם, לא הייתה לה פעילות כלכלית.

החברה הוקמה בעקבות ההכרה של מייסדיה בכך שלמרות שהחוק קבע פיצוי סטטוטורי, בתקווה שנפגעים יתבעו ובכך תיווצר הרתעה, קיים כשל שוק: רוב נפגעי הספאם אינם משתמשים בכלי המשפטי ואינם תובעים. למרות שהליך התביעות הקטנות אמור להיות נגיש, פשוט וזול, הוא אינו כזה עבור נפגעי ספאם רבים. סכומי התביעה קטנים, ונפגעים אינם יודעים את מי לתבוע. "ספאם אוף" ביקשה להפוך את התהליך לפשוט יותר עבור הנפגעים, בין השאר באמצעות אוטומציה של חלק מההליך המשפטי (החברה בנתה שבלונות מודולריות לשם הגשת תביעה), ובאמצעות ידע שצברה במהלך טיפול במאות תביעות ספאם.

השלב הראשון בתביעת ספאם הוא איתור מקור ההודעה. לא כל המפרסמים הם חברות לגיטימיות שניתן בקלות לאתר את זהותן, וחלקן לדוגמה משתמשות במספרי טלפון לא מקומיים כדי לעקוף את איום התביעה. אתר "ספאם אוף" אפשר שליחת צילום מסך של הודעת הספאם, בדק את מקור השולח והסיק האם המקרה עמד בקריטריונים על פיהם ניתן לתבוע פיצוי. לחברה היה מאגר מידע של פרטי ספאמרים, ובסופו של תהליך הבירור הוכן כתב תביעה בבית המשפט לתביעות קטנות. המודל הכלכלי של החברה התבסס על "מס זכייה", כלומר על גבייה של 20%

68 ראו: https://www.guidestar.org.il/organization/580607182/people.

69 https://zilaw.co.il.

70 ראו דוח איגוד האינטרנט הישראלי לעניין ספאם שהוזכר כאן: https://www.isoc.org.il/research/spam-data-analysis.

71 https://www.isoc.org.il/freedom-of-internet/spam/filing-a-lawsuit-spam.

אחוזים מסכום הפיצוי שקיבל לקוח שזכה בתביעה. אין בידינו נתונים על היקף הפעילות המלא של החברה, הזכיות או ההפסדים של הלקוחות בבתי המשפט, והפיצויים שבהם זוכו.

בתי המשפט לתביעות קטנות ואחריהם בתי המשפט המחוזיים התקשו להתמודד עם החברה, וקבעו פעם אחר פעם שפעילותה מעוררת קשיים מגוונים ובהם הרתעת יתר, עומס על בתי המשפט, הסגת מקצוע עריכת הדין (מייסדי ומפעילי האתר, עידו לוין ואורן שגב, לא היו עורכי דין), ועוד.[72] הדבר הגיע לכדי כך שכאשר נתבעה חברת האופציות הבינאריות "היימרקט", איגדה השופטת מאה חמישים תביעות, שחלקן הוגשו בעזרת "ספאם אוף" וחלקן הוגשו באופן עצמאי, אבל השופטת פסקה פיצוי רק לתובעים העצמאיים.[73] השופטים תפסו לעיתים קרובות את "ספאם אוף" כשחקן אופורטוניסט, מי שלא נגרם לו נזק אמיתי והוא מחפש רווח קל על גב הנפגעים. ערעור החברה נדחה בבית המשפט המחוזי, אבל בערעור נוסף, בית המשפט העליון קבע שפעילות של גופים שמסייעים לתובעים במימוש זכויותיהם עולה בקנה אחד עם תכליות חוק הספאם ומסייעת להגשמתן, ועל כן אין הצדקה בשלילת פיצוי לתביעות שמוגשות בסיוע גופים כאלה, גם מטעמים של "עומס" על בתי המשפט ואחרים.[74] אלא, שעד לפסיקה זו, "ספאם אוף" כבר חדלה מלפעול.

"ספאם אוף" הכניסה מספר חידושים לזירת הספאם הישראלית והמאבק בספאם, שאנו סבורים שהיטו את המאזן לטובת נפגעי הספאם. החידושים העיקריים היו אוטומציה של הליך התביעה; אסטרטגיית פעולה שחילקה תביעת ספאם להרבה מאוד תביעות קטנות, ש"הציקו" לגורם השולח; וכן תביעת נושאי משרה בחברות שהפיצו ספאם. בשילוב של כל אלה יחדיו, "ספאם אוף" הדגימה פתרון המשלב את ההיבטים המשפטיים עם ההיבטים הטכנולוגיים של ההתמודדות עם ספאם. לכך נשוב בפרק ה, בדיון על הממשק בין המשפט והטכנולוגיה בזירת הספאם.

בסופו של דבר, החברה נתבעה בשלל עילות, כמו פגיעה בשמן הטוב של החברות, מתן שירות משפטי בידי מי שאינו משפטן, ועוד. בעקבות זאת, חדלה החברה מלפעול.

<u>עורכי דין המתמחים בתביעות ספאם</u>

עורכי דין פרטיים שעוסקים בהגשת תביעות ייצוגיות שעניינן ספאם, הם שחקנים חוזרים קלאסיים: הם רכשו ידע לגבי הפעילות בזירה, ניסיון מעשי, ומיומנות גבוהה בהליך המשפטי, כך שעלות הגשת תביעה נוספת עבורם היא קטנה יחסית. כפי שהסביר לנו עו"ד זיו גלסברג שפעיל בנושא ספאם והוא גם ממייסדי ופעילי עמותת "אל ספאם", "יש יתרון במומחיות, בזה שיש לך כתבי טענות ואתה יודע כבר לטעון חלק גדול מהטענות. בדרך כלל יש הרבה מאוד אלמנטים עובדתיים חוזרים."[75] האינטרס של שחקנים אלה משולב: הם פועלים כנציגים של האינטרס הציבורי של מאבק בתופעת הספאם בכלל, ויש להם אינטרס כספי, כחלק מהגמול לתובעים ייצוגיים ושכר הטרחה שמקובל לפסוק בתביעות כאלה, ובכלל זה בפשרות.[76]

אם כך, בדומה למקרה של "ספאם אוף", שחקן פרטי שפועל נגד ספאם מטעמים עקרוניים עשוי למצוא את עצמו בדילמה כלכלית. האינטרס הכלכלי של עורך דין בתחום עשוי לעמוד בסתירה לאינטרס הערכי שלו להילחם בספאם לטובת כלל הציבור.

<u>מפתחי, יצרני ומשווקי טכנולוגיות ספאם ואנטי-ספאם</u>

הזירה הטכנולוגית של פיתוח, יצור ומכירה של חומרה ותוכנה שמאפשרת לייצר ולהפיץ ספאם אך גם להילחם בהפצת ספאם, היא זירה שלמה בפני עצמה. פרק ד בדוח זה יוקדש לטכנולוגיות ספאם ואנטי-ספאם, ושם נרחיב את היריעה הטכנולוגית. נטרים ונאמר שפיתוח טכנולוגי בזירת הספאם הוא מרוץ חימוש אינסופי; מרגע שנמצאה טכנולוגיית

---

72 ראו רת"ק (ת"א) 31506-05-17 **ארד נ' מנקס אונליין טריידינג בע"מ** (נבו 23.7.2017); ת"ק (עכו) 48592-12-16 **יעקובוב נ' אל.טי. - פאוור טכנולוג'יס בע"מ** (נבו 5.4.2017); ת"ק (נת') 12510-11-16 **ריקס נ' פלאפון תקשורת בע"מ** (נבו 27.3.2017); ת"ק (נת') 8791-11-16 **חינצוק נ' קבוצת קידום בע"מ** (נבו 22.3.2017); וגם ת"ק (נת') 26251-11-16 **קמחי נ' כוכבית סטארפון ישראל בע"מ** (נבו 20.3.2017); ת"ק (חד') 42711-03-17 **זיסו נ' המרכז הישראלי ל.ע. ברשת בע"מ** (נבו 19.8.2017).

73 ת"ק (ת"א) 26210-04-16 **בוקובזה ו-59 נוספים נ' מנקס אונליין טריידינג בע"מ** (נבו 30.4.2017).

74 רע"א 7064/17 **ארד נ' מנקס אונליין טריידינג בע"מ** (11.12.2018), בפס' 34-36.

75 הדברים נאמרו בשיחה שהתקיימה ב-30.4.2022.

76 ראו ס' 22 לחוק תובענות ייצוגיות, התשס"ו-2006, וכן אלון קלמנט "קווים מנחים לפרשנות חוק התובענות הייצוגיות, התשס"ו-2006" **הפרקליט** מט 131, 157-162 (2006).

סינון חדשה שמצליחה לזהות ולמנוע הפצת ספאם, ימהר מפיץ הספאם המאוכזב למצוא דרך חדשה להספים. השוק למוצרים טכנולוגיים שמטרתם מניעת ספאם נאלץ להשתכלל ללא הרף, ומנגד מוצאים ספאמרים דרכים חדשות לעקוף כל המצאה וכל שכלול. במובן זה, שוק טכנולוגיות האנטי-ספאם חי על קיומו של ספאם.

ד. הזירה הבין-לאומית: רשימות שחורות, אגודות בין-לאומיות ללוחמה בספאם

שחקנים שונים בזירה הבין-לאומית מעורבים במאבק בספאם, ולעיתים השפעתם על המתרחש בזירה המקומית היא מכרעת. על אלה נמנות רשימות שחורות ואגודות שונות שמטרתן מיגור תופעת הספאם.

<u>רשימות שחורות</u>

לרשימות שחורות יש השפעה משמעותית על שרשרת הערך של הספאם. רשימה שחורה היא מאגר של כתובות הנחשדות ככתובות שמהן נשלח ספאם. המאגר מאפשר חסימת שירותים והטלת סנקציות על שחקנים "שסרחו". שירות רשימה שחורה מאפשר לשרת דואר לחפש בהן את כתובת ה-IP ממנה מגיע מסר, ולדחות מסרים המגיעים מכתובות המופיעות ברשימה השחורה. מנהלי מערכות יכולים לבחור מתוך מגוון גדול של רשימות, כאשר כל רשימה משקפת סטנדרט עצמאי של סינון, בהתאם למדיניות הרשימה. חלק מהרשימות השחורות פועלות כעסק מסחרי, וחלקן כשירות חינמי. כזה הוא למשל פרויקט Spamhaus, שהוא אחד הארגונים הוותיקים והידועים ביותר שעוקב אחר ספאמרים.[77] הפרויקט הוא ארגון בין-לאומי ללא מטרות רווח, שנוסד במקור בלונדון ב-1998, העוקב אחר ספאם ואיומי סייבר הקשורים לספאם כמו פישינג או בוטנטים זדוניים. הפרויקט מנוהל כיום על ידי צוות של 38 חוקרים, מומחי זיהוי פלילי ומהנדסי רשת ב-10 מדינות שונות בעולם.[78]

כפי שהזכרנו לעיל, בדיון על חברות ההפצה, הסיבה המרכזית שחברות הפצה וחברות התקשורת מבקשות לזהות ספאמרים אינה החשש מסנקציות משפטיות; החשש הגדול הוא מפני הכללה של שרתי המשווק, חברת ההפצה או חברת התקשורת ברשימה שחורה. לחברות הפצה יש אינטרס לקבל "ציונים גבוהים" ובכך להגן על ציבור הלקוחות שלהן, שייפגעו מכניסת החברה לרשימה שחורה. לכן, חברות ההפצה מחתימות את לקוחותיהן על הסכמים האוסרים עליהם להשתמש בשירותי החברה כדי לשלוח ספאם. בעליה של אחת מהחברות האלה הסביר לנו שיש לו אינטרס לתפוס ספאמרים אפילו יותר מאשר למדינה, מפני שמעבר לחוקי המדינה "יש את חוקי האינטרנט ששם מענישים על זה, עולמות של בלקליסט. אם משתמש שלי עושה את זה הפלטפורמה או חלק מכתובות ה-IP שלי נכנסות לבלקליסט. אנחנו כל היום במרדף על זה." ברגע שמפעיל רשימה שחורה מזהה ספאם שנשלח מדומיין או כתובות IP של אחת מחברות ההפצה – הוא מסמן את הדומיין או את כתובות ה-IP הספציפיות. חברות קבלת הדוא"ל כמו גוגל, מיקרוסופט ואחרות מחוברות לרשימות הללו וכאשר כתובת מסומנת אצלן הן חוסמות את המיילים הנשלחים מאותן כתובות מלהגיע לתיבת הדואר הנכנס של הנמענים. מבחינת העסק המשווק, חברת ההפצה או חברת התקשורת, חסימה כזו יכולה להתרחש באופן פתאומי, ללא הודעה, וללא יכולת ערעור. בעל חברת ההפצה הוסיף ואמר: "הרשימות השחורות עבדו מאז ומתמיד הרגולציה לא שינתה כלום. הרשימות השחורות הן האכיפה דה פקטו, הן החוק והן אכזריות. הן לא מושפעות מכלום אבל משפיעות המון." [79]

---

77 Meg Kawalkowska, *What Do I Need to Know About Email Blacklists*, Woodpecker (2.3.2023), available at: https://woodpecker.co/blog/avoid-email-blacklist.

78 https://www.spamhaus.org/organization. דוגמה נוספת היא SpamCop, שהוקמה על ידי ג'וליאן הייט (Haight) בשנת 1998 כפרויקט אישי, שהתרחב ככל שהפופולריות שלו גדלה. ב-2003 השירות נרכש על ידי חברת אבטחת הדוא"ל IronPort Systems, והפך לשירות של סיסקו מערכות ב-2007. עם זאת, השירות הבסיסי עדיין ניתן למשתמשים בחינם. ראו https://www.spamcop.net/bl.shtml.

79 הדברים נאמרו במהלך שיחה עם נאור מן, מנכ"ל חברת הפצה מקומית, שנערכה ביום 1.6.2023.

לסיכום חלק זה, בצד שעניינו המלחמה בספאם, המדינה היא שחקן מרכזי. המדינה מצויה בצומת של אינטרסים רבים שלעיתים מתנגשים, וביניהם עליה לנווט. רצונה של המדינה למגר את תופעת הספאם מציף מתחים מול שחקנים שונים בשרשרת הערך של הספאם, שמבקשים הגנה על זכויות הקניין וחופש העיסוק שלהם. המדינה גם מחויבת להגן על חופש הביטוי של משתמשי שירותי התקשורת, ולכן עליה להיזהר מלהטיל רשת צפופה מדי של סייגים על משלוח מסרי תקשורת. המדינה גם מבקשת להגן על יכולותיה להשתמש באופן מיטבי בכלי תקשורת על מנת להעביר מסרים מטעמה, וכן להגן על מעמדה בזירה הבין-לאומית המקוונת.

צרכני שירותי תקשורת אינם עשויים מקשה אחת, גם לא בעניין הספאם. יכולת ההתגוננות של האזרח מפני תקשורת לא רצויה תלויה במידה לא מבוטלת באוריינות הדיגיטלית שלו.ה.

שחקנים פרטיים שפועלים נגד ספאם מטעמים עקרוניים, למשל עורך דין בתחום או חברה שמטרתה לסייע לנפגעי ספאם, עשויים למצוא את עצמם בדילמה כלכלית. האינטרס הכלכלי של שחקן כזה עשוי לעמוד בסתירה לאינטרס הערכי שלו להילחם בספאם לטובת כלל הציבור.

4. גופי ביניים: ספקי תשתית ושירותים מקוונים

חברות התקשורת הישראליות, כמו בזק או סלקום, הן שחקן מרכזי בזירת הספאם, שתפקידו במערכת האקולוגית של הספאם הוא מורכב. הסיבה המרכזית לכך היא שחברות התקשורת אוחזות בשני כובעים: הן מחזיקות ומפעילות תשתיות תקשורת (בדומה לחברות ההפצה והדיוור), ובנוסף הן מספקות ללקוחותיהן שירותי תקשורת שונים. כלומר, חברות התקשורת משרתות שני שחקנים מרכזיים שהאינטרסים הבסיסיים שלהם מנוגדים בתכלית: מחד גיסא, המשווקים והמפרסמים, ומאידך גיסא, לקוחותיהן, משתמשי הקצה, שהם גם הנמענים של המסרים השיווקיים. החברות משרתות הן את המפרסמים, ומרוויחות יותר כאשר חבילות המסרים גדולות יותר; והן את ציבור המשתמשים ושם הן מבקשות להציע שירותים נקיים ככל האפשר מהפרעות לא רצויות. בנוסף, החברות מחויבות גם שלא לפגוע בחופש הביטוי של מפיצי מסרים. לכך נוסף גם האינטרס המשפטי-עסקי הישיר שלהן, להימנע מחשיפה משפטית. במילים אחרות, מבחינה עסקית לפחות, חברות התקשורת נמצאות בין הפטיש לסדן.

<u>כובע ראשון: תשתיות תקשורת</u>

כמובן, חברות התקשורת חייבות לציית לחוק. חוק הספאם הישראלי החריג את אחריותן של חברות התקשורת בסעיף 1 לחוק, בהגדרה של "מפרסם": "לעניין זה, לא יראו כמפרסם מי שביצע, בעבור אחר, פעולת שיגור של דבר פרסומת כשירות בזק לפי רישיון או תקנות ההיתר הכללי, לפי העניין." הטעם לכך משתקף בדבריו של עו"ד חיים גרון, סמנכ"ל בכיר באגף הנדסה ורישוי של משרד התקשורת דאז, במהלך הדיונים בכנסת: "האחריות - לא על הצינור."[80] על ההחרגה לחול רק על "מי שהוליך, או ניתב את דבר הפרסומת במסגרת שירות בזק."[81] או אם לחזור לדבריו של גרון – "הכוונה ברורה - לפטור את הפלטפורמות כצינורות, כל עוד הם צינורות..."[82] לפי החוק, פיצוי על הפרה יינתן רק אם ההפרה נעשתה ביודעין, והחוק מחריג מפורשות את כל חברות התקשורת, הנהנות מהגנה מוחלטת של אי ידיעה בנוגע לתכני תקשורת.[83]

החרגה זו מספקת לחברות חסינות מעשית מפני דרישה לחשוף את זהות לקוחותיהן. חשיפה כזו עשויה להתנגש עם מחויבויות משפטיות אחרות של החברות, בעיקר כלפי לקוחות (מחויבות החברות להגנה על פרטיות המידע של לקוחותיהן) ושותפים עסקיים (למשל הגנה על סודות מסחר). הפרת מחויבויותיה של חברת תקשורת ללקוחות או לשותפים משמעה, בנוסף לחבות המשפטית, פגיעה באינטרסים העסקיים שלה:

80 פרוטוקול ישיבה 5 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 40 (25.3.2008).

81 דברי עו"ד חיים רביה, שם, בעמ' 48.

82 שם.

83 סיפא 30א.ב – פעולות לפי רישיון.

א. **מול לקוחות**: חברות התקשורת מחויבות כאמור להגן על פרטיות המשתמשים. לקוחות שיהיו מוטרדים מהגנה לקויה על זכויותיהם עלולים למחות בדרכים שונות, לרבות עזיבת החברה. אחריות לתכנים מצד ספקיות שירות עשויה להביא לאחריותן לחשוף שמות משתמשים ובכך להפר את פרטיותם.[84]

ב. **מול שותפים עסקיים**: חברות התקשורת מחויבות להגן על אינטרסים משותפים להן ולשותפיהן העסקיים, כמו למשל אינטרסים של הגנה על סודות מסחריים, כמו שיטות אבטחת המידע של החברה, או טכנולוגיית הסינון שהיא משתמשת בה, או הגנה על רשימות לקוחות.

ג. **מול מתחרים עסקיים**: בין חברות התקשורת עשויה להתקיים תחרות הן על רקע הגנת המידע של לקוחותיהן, והן לעניין הגנה על סודות מסחר או פטנטים הקשורים לאבטחת מידע ולהגנות טכנולוגיות מפני ספאם. נקודה זו חוזרת בדיון שבסמוך, על חברות התקשורת בכובען כספקיות שירותים, ושם היא אף מרכזית יותר.

גם כאן, יש הבדל משמעותי בין ספקיות גדולות לקטנות; למשל, חברות גדולות יכולות להשתמש בטכנולוגיות המאפשרות להן לקרוא הודעות ולסנן אותן בהתאם לתכנים. חברות קטנות יותר, מסוג חברת "רב מסר",[85] יפסידו כלכלית אם ירכשו שירות כזה משום שהוא יקר יותר מהרווח שלהם מכל מסרון.

<u>כובע שני: שירותי תקשורת (דוא"ל, הודעות טקסט, שיחות קוליות)</u>

בכובען כספקיות שירותי תקשורת, חברות התקשורת הביעו את עמדתן בנוגע לחשיבות החקיקה במהלך דיוני הוועדה המשותפת. החברות ביקשו להחריג את עצמן מהחוק, ולחדד את הגדרתו של "דבר פרסומת" כך שלא יכלול על התקשורת שלהן עם לקוחותיהן. בקשה זו נענתה בשלילה.[86]

בהגדרה רחבה, חברות הסלולר הישראליות הן ספקיות שירותי תקשורת, אך כך גם חברות המספקות שירותי דוא"ל כמו גוגל או מיקרוסופט, שמספקות שירותי העברת מסרים מהירים כמו פייסבוק (וואטסאפ) או X (לשעבר טוויטר). תאגידי הטכנולוגיה הגדולים כמו גוגל או פייסבוק מפתחים בעצמם טכנולוגיות להגנת מידע, לרבות טכנולוגיות אנטי-ספאם. ספקיות שירותי התקשורת מצהירות שהן מצייתות בקפדנות למגבלות חיצוניות על פעילותן. אלא שבעוד שחוק התקשורת באופן קונקרטי, והחוק הישראלי בכלל, חל על ספקיות שירותי התקשורת המקומיות, הרי שספקיות תקשורת לא מקומיות – כלומר תאגידי הטכנולוגיה הגדולים – פועלות בהתאם לתכתיבים שונים שהחוק הישראלי אינו המרכזי שבהם.[87]

בשנים 2019 ו-2022 הונחה על שולחן הכנסת הצעת חוק שמבקשת לשנות את המאזן הנוכחי, שהוא במובהק לטובת פטור מלא מאחריות לחברות התקשורת.[88] לפי הצעת החוק, במקרה בו חברת תקשורת מסרבת לחשוף את זהות הגורם ששלח ספאם, יבוטל הפטור באופן נקודתי. במהלך דיוני תיקון 76 לחוק, הציג יוגב עזרא, נציג עמותת "אל ספאם" עמדה דומה, שלפיה שמי שמוחרג מהחוק יוכל לשמור על ההגנות הנתונות לו אם ימסור את פרטי הלקוח המספים ללא צו בית משפט, אלא בעקבות בקשה של הנפגע. במקרה של סירוב למסירת פרטים, לא ייהנה עוד המוחרג מהגנת החוק, ואפשר יהיה לתבוע אותו באופן אישי.[89] תגובת נציג משרד התקשורת, זיו גלעדי, להצעה של עזרא הייתה שאינו חושב ש"אנחנו בשלים להביע עמדה בנושא הזה." נכון לזמן כתיבת דוח זה, המחוקק טרם טיפל בסוגיה.

84 זאת בהתאם להלכת רמי מור: רע"א 4447/07 **מור נ' ברק אי. טי. סי. (1995) החברה לשירותי בזק בינלאומיים בע"מ**, פ"ד סג(3) 664 (2010). מנגד ראו ת"א (שלום, פ"ת) 48690-01-23 **כהן נ' טלזר 019 שירותי תקשורת בינלאומיים בע"מ** (נבו 21.5.2023), שם התקבלה בקשת התובע לחשיפת הגורם העומד מאחורי המסרונים שנשלחו בעניינו.

85 לפי אתר החברה, רב מסר היא מערכת הדיוור (בדוא"ל וסמס) ודפי הנחיתה, היא מספקת גם תבניות לעיצוב ועריכת מסרים ודפי נחיתה. היא מתגאה בכך שיש לה "עבירות מצוינת", כך שהדיוור יוכל לעבור את המסננים ולהגיע אל היעד. לפירוט באתר החברה: https://www.re-sponder.co.il/רסמ-רב-תולוכי/.

86 פרוטוקול ישיבה 5 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה (25.3.2008), בו ביטאו נציגי בזק ומיקרוסופט את הקושי בהחלת החוק על התקשורת שלהן עם מנויהן.

87 ניבה אלקין-קורן "המתווכים החדשים 'בכיכר השוק' הווירטואלית" **משפט וממשל** ו 381 393-387 (2003).

88 הצעה זו עלתה בשלוש כנסות שונות: הכנסת ה-22, הכנסת ה-24 והכנסת ה-25. ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התש"ף-2019 (פ/690/22); הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התשפ"ב-2022 (פ/3368/24); הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התשפ"ג-2022 (פ/276/25).

89 פרוטוקול ישיבה 138 של ועדת הכלכלה, בעמ' 42-45 (4.1.2022).

5. סיכום

בפרק זה הצגנו את השחקנים השונים שמעורבים במערכת הספאם, הן בצד "שרשרת הערך", הן בצד המלחמה בספאם. בנוסף, הצגנו את מערכת השחקנים המורכבת שנמצאת בצומת שבין חזית הספאם וחזית המלחמה בספאם: חברות התקשורת. תיארנו את זכויותיהם וחובותיהם של השחקנים השונים, ומיפינו את האינטרסים שלהם בכל הנוגע להפצה או למניעת הפצה של ספאם.

בצד שרשרת הערך, השחקנים המרכזיים שבחנו היו בתי העסק המשווקים, ספקי לידים, וחברות ההפצה. שחקנים שהוזכרו ולא עסקנו בהם בהרחבה היו למשל ספקי רשתות בוטים המאפשרות פעילות ענפה בתחום הספאם; הסיבה היא שעיקר מטרתו של דוח זה היא לבחון את המדיניות הקיימת, בין השאר באמצעות זיהוי שחקנים שאפשר להשפיע על פעילותם ולכוון אותה באופן טוב יותר. במקרה של רשתות בוטים, אלה מנוהלות ברובן באופן שאינו מאפשר להתחקות אחר פעילותן או להתערב בה באופן מקומי, והאכיפה בה מדובר אינה בסדרי הגודל של אכיפת ספאם שיווקי. בצד המלחמה בספאם, בחנו בעיקר את המדינה, הציבור, ומגוון של שחקנים פרטיים שמעורבים במלחמה בספאם. כל אחד מהשחקנים מקדם אינטרסים משלו שמצטלבים או שאינם קשורים לאלה של שחקנים אחרים, שנמצאים איתם בקונפליקט או שהם משותפים. האינטרסים השונים משפיעים על מערכת הספאם באופן חיובי או שלילי.

מהדיון בפרק זה עולות כמה מסקנות ביניים:

- בבחינת פתרונות חדשים במסגרת המאבק למיגור הספאם יש לזנוח את הגישה הבינארית, שבוחנת רק את המשווק כמוען ואת משתמשי האינטרנט והטלפון כנמענים, ולראות את התמונה הרחבה יותר, שבה שחקנים רבים. מערכת הספאם היא מערכת אקולוגית סבוכה ומורכבת.
- מערכת הספאם היא זירה רבת-משתתפים, בנוסף לשחקני הקצה – המוען והנמענים – יש שורה של גורמי ביניים שמעורבים בשלבים שלפני ההפצה, בהפצה, ובמאבק בספאם. בכל אחת מהחוליות האלה יש סוגים שונים של שחקנים – חלקם מעורב באופן ישיר וחלקם באופן עקיף, חלקם פועל בצורה חוקית ולגיטימית וחלקם פועל בצורה לא חוקית.
- לשחקנים הלגיטימיים יש אינטרסים וזכויות שונות, שיש לאזן ביניהם: הזכות לפרטיות והזכות להימנע ממטרדים של הנמענים, זכויות קנין, חופש עיסוק וחופש ביטוי מסחרי של המפרסמים, זכויות קניין וחופש פעולה עסקי של גורמי ביניים חוקיים.
- הזירה אינה יציבה: יש בה תמריצים כלכליים שמשתנים, הפעילות תלוית-טכנולוגיה ולכן גם משתנה כאשר הטכנולוגיות הרלוונטיות משתנות, ויש כללים משפטיים שונים.

מהדיון עלו גם מספר מסקנות נקודתיות בנוגע לשחקנים ספציפיים:

- בין בעלי המסר, שתי הבחנות חשובות שעלו בדיון הן גודל העסק, וחוקיות התוכן המופץ. חלק מהחברות פועלות לפי שיקול של "הפרה יעילה", ואינן מורתעות מפיצויים שנפסקים כנגדן.
- בנוגע לאחריות להפצת ספאם, הדיון העלה שהיא אינה מתחלקת באופן שווה בין השחקנים בשרשרת הערך. עיקר האחריות לשליחת ספאם נופלת היום על בעלי המסר ועל ספקי הלידים. כמו כן, בעקבות תקנות חדשות שעליהן נרחיב בפרק הבא, חברות ההפצה עשויות לסבול מהרתעת-יתר. מנגד, חברות התקשורת אינן נושאות היום כלל באחריות להפצת ספאם.
- גורמי ביניים מרכזיים שמסייעים למשווקים להפיץ הודעות מסחריות (שלב ההפצה) הם רשתות השותפים וחברות ההפצה. בעוד שרשתות השותפים אטרקטיביות עבור ספאמרים מקצועיים ועבור כל שחקן שמבקש להרחיק את עצמו מאחריות מידית לשליחת ספאם, מקומן של חברות ההפצה בזירה אמביוולנטי יותר ביחס לספאם. הן מציעות שירות שאינו בלתי חוקי כשלעצמו, אבל יש חשש שינוצל לרעה. למעשה, שולחי ספאם מקצועיים מסכנים את עסקיהן של חברות ההפצה, ולהן יש אינטרס כלכלי לעמוד על המשמר בקשר לשימוש בשירות שלהן.

- בצד שעניינו המלחמה בספאם, המדינה היא שחקן מרכזי. המדינה מצויה בצומת של אינטרסים רבים שלעיתים מתנגשים, וביניהם עליה לנווט. רצונה של המדינה למגר את תופעת הספאם מציף מתחים מול שחקנים שונים בשרשרת הערך של הספאם, שמבקשים הגנה על זכויות הקניין וחופש העיסוק שלהם. המדינה גם מחויבת להגן על חופש הביטוי של משתמשי שירותי התקשורת, ולכן עליה להיזהר מלהטיל רשת צפופה מדי של סייגים על משלוח מסרי תקשורת. המדינה גם מבקשת להגן על יכולותיה להשתמש באופן מיטבי בכלי תקשורת על מנת להעביר מסרים מטעמה, וכן להגן על מעמדה בזירה הבין-לאומית המקוונת.
- צרכני שירותי תקשורת אינם עשויים מקשה אחת, גם לא בעניין הספאם. יכולת ההתגוננות של האזרח מפני תקשורת לא רצויה תלויה במידה לא מבוטלת באוריינות דיגיטלית.
- שחקנים פרטיים שפועלים נגד ספאם מטעמים עקרוניים, למשל עורך דין בתחום או חברה שמטרתה לסייע לנפגעי ספאם, עשויים למצוא את עצמם בדילמה כלכלית. האינטרס הכלכלי של שחקן כזה עשוי לעמוד בסתירה לאינטרס הערכי שלו להילחם בספאם לטובת כלל הציבור.
- חברות התקשורת הן שחקן מרכזי בזירת הספאם, שתפקידו במערכת האקולוגית של הספאם הוא המורכב ביותר. הסיבה המרכזית לכך היא שחברות התקשורת אוחזות בשני כובעים: הן מחזיקות ומפעילות תשתיות תקשורת ובנוסף הן מספקות ללקוחותיהן שירותי תקשורת שונים. כלומר, חברות התקשורת משרתות שני שחקנים מרכזיים שהאינטרסים הבסיסיים שלהם מנוגדים בתכלית: מחד גיסא, המשווקים והמפרסמים, ומאידך גיסא, לקוחותיהן, משתמשי הקצה, שהם גם הנמענים של המסרים השיווקיים.
- בדיון המשפטי המפורט נשוב ונבחן את הכללים המשפטיים שחלים על השחקנים השונים, וננסה לאתר נקודות חולשה שראוי לחזק או לתקן. פרק זה משמש תשתית להבנת הפרקים הבאים, שיעסקו בהתאמה במשפט הספאם ובטכנולוגיות ספאם ואנטי ספאם. השחקנים שמופיעים בפרק זה ישובו ויופיעו בפרקים הבאים, שם נוכל לנתח לעומק את אופני פעולתם בהסתמך על הניתוח והמסקנות שבפרק זה.

פרק ג
דיני הספאם

1. **מבוא** 45
2. **דיני הספאם בישראל: תמונת מצב עכשווית** 46
   א. הגדרות החוק ותחולתו 46
   ב. תיקוני החקיקה 47
   ג. מגמות בפסיקה 49
3. **מנגנוני אכיפה: תמונת מצב בשטח** 51
   א. מנגנון ראשון: תביעה אישית ותביעות בהליכים מקוצרים 51
   ב. מנגנון שני: תובענה ייצוגית 52
   ג. מנגנוני הסדרה נוספים 53
4. **פתרונות משפטיים בעולם ומידת התאמתם לישראל** 54
5. **ניתוח: הישגים, כשלים ופתרונות** 59
6. **סיכום** 62

1. מבוא

פרק זה עוסק בצד המשפטי של תופעת הספאם. במארס 1996 התקבל תיקון 4 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות"), שעוסק בדיוור ישיר.[1] הייתה זו הפעם הראשונה בה התמודדו החוק הישראלי, גם אם באופן עקיף, עם תופעת הספאם.[2] ההתמודדות הישירה עם התופעה הגיעה לפרקה עם חקיקת תיקון 40 לחוק התקשורת (להלן: "חוק הספאם"), במאי 2008.[3] משרד התקשורת יזם הצעת חוק בשנת 2005.[4] החוק שהתקבל בסופו של דבר אימץ את המודל האירופי להסדרת ספאם, שאוסר על שליחת תוכן שיווקי ללא הסכמה מפורשת מראש של הנמען. בדברי ההסבר להצעת חוק הספאם נומקה הבחירה במודל האירופי בכך שהוא מגלם איזון ראוי בין פרטיות המשתמש ומניעת מטרדים מצד אחד, לבין שימוש לגיטימי במתקן בזק לטובת פרסום, מצד שני.[5] ואכן, דיונים רבים לקראת חקיקת חוק הספאם עסקו בצורך למצוא איזון ראוי בין חופש הביטוי של מפרסמים ובעלי עסקים, אל מול זכותו של הפרט לפרטיות.[6]

יש מספר הבדלים בין האיסור על משלוח ספאם לבין ההסדרה של "דיוור ישיר" בחוק הגנת הפרטיות.[7] סעיף 17ג לחוק הגנת הפרטיות מגדיר "דיוור ישיר" כ"פניה אישית לאדם, בהתבסס על השתייכות לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע." לעומת זאת, ספאם (או דואר זבל) בדרך כלל אינו מופנה באופן אישי לנמען, והוא אינו מבוסס בהכרח על מאפייני הנמען או על השתייכותו לקבוצה. להיפך. דואר זבל נשלח בכמות גדולה, באופן גורף, ללא אבחנה בין הנמענים (bulk). בנוסף לכך, במקרים רבים שיגור ספאם אינו מסתמך על רשימות נמענים העונות להגדרת "מאגר מידע" שבחוק הגנת הפרטיות, אלא נשלח באופן גורף.[8] אולם, העידן הדיגיטלי, על ריבוי גורמי הביניים שמעורבים בשרשרת ההפצה של הספאם, שאותם הצגנו בהרחבה בפרק ב, מטשטש במקרים רבים את הגבולות בין שיווק ישיר לגיטימי לבין ספאם, ולכן לקושי ממשי להבחין בין השניים.

פרק זה ממפה ומנתח את מסלולי האכיפה המשפטיים הקיימים בקשר לספאם, ומנסה להעריך את יעילותם בפועל. שיטת האכיפה הישראלית המרכזית להתמודדות עם הספאם היא הפרטת האכיפה, בדרך של יצירת אפשרות של תביעה אישית (בדרך כלל תביעה קטנה) עם פיצוי סטטוטורי – כלומר פיצוי ללא הוכחת נזק, ובצידה מסלול של תובענה ייצוגית. לצד ניתוח החוק ובחינת מגמות בפסיקה, נעזרנו בשיחות עם שחקנים בזירה המשפטית, וכן בממצאי דוח איגוד האינטרנט הישראלי, שבנה מאגר נתוני עתק המבוסס על כל תביעות הספאם שהוגשו בישראל בשבע השנים האחרונות (2022-2016), כולל תביעות קטנות, הליכים בסדר דין מהיר ותובענות ייצוגיות.[9] דוח האיגוד מסייע לנתח מגמות בהתפתחות מסלולי האכיפה השונים.

בחלקים הבאים נציג את הדין הישראלי הקיים ואת הדרך שעבר עד היום. נפתח בסקירת תמונת המצב העכשווית של דיני הספאם בישראל, לאחר מכן נפנה לסקירת תמונת המצב בשטח. זו כוללת את מנגנוני האכיפה המשפטיים המרכזיים של חוק הספאם, שהם מסלול התביעה האישית ומסלול התובענה הייצוגית, וכן את ההתפתחויות המרכזיות בפסיקה בנוגע לספאם. הניתוח כולל בחינה של התפתחות החקיקה, כדי לחלץ מתוך זה את השיקולים השונים,

1 התיקון הוסיף לחוק את סימן ב בפרק ב.

2 ראו דן חי **תורת המסר: בין דיוור ישיר לספאם** 8-7 (2012).

3 חוק התקשורת (בזק ושידורים) (תיקון מס' 40), התשס"ח-2008 (החוק, להלן: "חוק התקשורת"; תיקון 40 – להלן" חוק הספאם").

4 הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 33), התשס"ה-2005, ה"ח 182.

5 דברי הסבר להצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 33), התשס"ה-2005, ה"ח 182, 886.

6 ראו לדוגמה בפרוטוקול ישיבה 2 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 15 (31.1.2007).

7 להרחבה, ראו חי **תורת המסר**, לעיל ה"ש 2, בעמ' 27-21.

8 ס' 7 לחוק הגנת הפרטיות, התשמ"א-1981, מגדיר מאגר מידע כך: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –(1) אוסף לשימוש אישי שאינו למטרות עסק; או(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".

9 ראו איגוד האינטרנט הישראלי, ניתוח נתוני עתק של תביעות דואר זבל אלקטרוני (ספאם) בישראל (להלן: **דוח איגוד האינטרנט**). נמצא ב: https://www.isoc.org.il/research/spam-data-analysis. מאגר האיגוד כולל למעלה מעשרים פריטי מידע על כל תיק, כמו למשל שם השופט או הרשם, שמות התובע והנתבע, בית המשפט בו התנהלה התביעה, סכום התביעה, סטטוס ההליך ותוצאתו. על אף שחוק הספאם נחקק בשנת 2008, הנתונים עליהם נשען דוח האיגוד כוללים מידע רק עבור הליכים משנת 2016, משום שרק אז החל סיווג שיטתי של תביעות מכוח חוק הספאם במערכת נט-המשפט. ראו שם, בפרק "מתודולוגיה".

לעיתים הסותרים, שהביאו לעיצוב הדין במתכונתו הנוכחית, והאופן בו השפיעו אינטרסים שונים של שחקנים שונים, כפי שהוצגו בפרק ב, על עיצובו של הדין. בהמשך נסקור התפתחויות של מנגנוני הסדרה בזירת הספאם, ופתרונות משפטיים נוספים שהוצעו או שנבחנו במדינות אחרות, וננתח אותם ואת מידת התאמתם למצב המשפטי הקיים בישראל. בחלק האחרון של פרק זה ננתח את ההישגים ואת הכשלים של חוק הספאם הישראלי ומנגנוני האכיפה שלו, ונציע פתרונות טנטטיביים.

2. דיני הספאם בישראל: תמונת מצב עכשווית

א. הגדרות החוק ותחולתו

הגדרת הספאם בדין הישראלי מופיעה בסעיף 30א(ב) לחוק התקשורת:

> "לא ישגר מפרסם דבר פרסומת באמצעות פקסימיליה, מערכת חיוג אוטומטי, הודעה אלקטרונית או הודעת מסר קצר, בלא קבלת הסכמה מפורשת מראש של הנמען, בכתב, לרבות בהודעה אלקטרונית או בשיחה מוקלטת; חיוג לנמען באמצעות מערכת חיוג אוטומטי בלא הסכמת הנמען כאמור ייחשב הפרה של הוראות סעיף זה, גם אם החיוג הופסק בטרם נענתה השיחה ובחיוג של הנמען למספר שממנו בוצע החיוג מושמע לו דבר פרסומת; פנייה חד-פעמית מטעם מפרסם לנמען שהוא בית עסק או לנמען לשם קבלת תרומה או תעמולה, באחת הדרכים האמורות בסעיף קטן זה, המהווה הצעה להסכים לקבל דברי פרסומת מטעמו, לא תיחשב הפרה של הוראות סעיף זה."

נעיין בכמה מרכיבים מרכזיים בהסדר הזה: מהו "דבר פרסומת", מה כוחו של הנמען, מי נחשב ל"מפרסם" – ומה החריגים, על מה חל האיסור – ומה החריגים.

באופן כללי, הסעיף אוסר על שיגור "**דבר פרסומת**" ללא הסכמה מפורשת, מראש ובכתב, של הנמען. הסכמה יכולה להיעשות גם בשיחה מוקלטת ובהודעה אלקטרונית. עם זאת, החוק מונה חריגים: פנייה חד-פעמית של מפרסם לבית עסק, ובה הצעה להסכים לקבל דברי פרסומת מטעמו; פנייה חד-פעמית של מפרסם שכוללת הצעה להסכים לקבל דברי תרומה או תעמולה; וכן שליחת דבר פרסומת באמצעות דוא"ל על ידי חברה לתועלת הציבור או עמותה, כל עוד הנמען לא הודיע על סירוב. בנוסף, בהתקיים מספר תנאים מצטברים, מפרסם יוכל לשגר דבר פרסומת ללא הסכמתו מראש של הנמען.[10] על מפרסם שעמד בסייגי החוק והותר לו לשלוח מסרים שיווקיים, לעמוד בתנאי סעיף 30א(ה), לפיהם עליו לציין את סוג המסר (פרסומת, תעמולה, תרומה) בתחילתו של המסר, לציין את פרטי המפרסם, ולהצביע בפני הנמען באופן ברור על דרכי הסירוב העומדות בפניו.

מושא האיסור בחוק הוא "דבר פרסומת." בהגדרת החוק, דבר פרסומת הוא מסר מסחרי שמטרתו לעודד את הנמען לרכוש דבר מה. הגדרת "דבר פרסומת" היא רחבה, ומסייגת רק מסרים פוליטיים. אמצעי שיגור המסר עליהם חל החוק הישראלי הם פקס, מערכת חיוג אוטומטית, הודעה אלקטרונית (כלומר דוא"ל) או הודעת מסר קצר (SMS, מסרון). החוק חל גם על "צנתוק", כלומר חיוג שהופסק בטרם נענתה השיחה ("צנתוק" הוא הלחמה של צלצול-ניתוק), ובהמשך לכך מחייג הנמען בחזרה למספר ממנו התקבלה השיחה ונענה בהשמעה של פרסומת.

בצד הנמענים, החוק מבקש להקל ככל האפשר על הנמען להביע סירוב לקבלת המסרים הפרסומיים, בכך שהוא מאפשר לו להודיע על סירובו לקבלת דבר הפרסומת בכל עת; לעשות זאת בכתב או בדרך בה הועבר המסר, לפי בחירת הנמען, וללא עלות (למעט בהודעת סמס); וכן לראות במועד סיומה של התקשרות ממושכת כאילו הייתה מתן הודעת סירוב של הנמען.[11]

10 ראו ס' 30א(ג) לחוק התקשורת. התנאים הם: 1. הנמען מסר את פרטיו למפרסם בזמן רכישת מוצר או שירות, והמפרסם הודיע לו על כוונתו להשתמש בפרטים אלה לטובת משלוח דברי פרסומת; 2. המפרסם נתן לנמען הזדמנות להודיע על סירוב, והנמען לא מימש אותה; 3. דבר הפרסומת קשור למוצר או שירות מתחום דומה לזה שסביבו הנמען התקשר עם המפרסם מלכתחילה. למשל, התנאי לא יתקיים במקרה שבו חברה למכירת רכבים שהתקשרה בעבר עם נמען לשם רכישת רכב – עסקה שלטובתה מסר הנמען את פרטיו – תשלח לנמען פרסומת לאבקת כביסה.

11 ראו ס' 30א(ד) לחוק התקשורת.

בצד השולח, "מפרסם", בהגדרת החוק, הוא מי שייהנה מפירות הפרסום, ואשר שמו מופיע בדבר הפרסומת. החוק מחריג את המדינה ומוסדותיה מהגדרת "מפרסם". בנוסף, כפי שראינו בפרק ב, החוק מחריג מהגדרת "מפרסם" את חברות התקשורת, על אף שהן אלה שמפיצות את דבר הפרסומת עבור אחרים, והפצת מסרים היא עסקן ומקור רווחיהן. לעומת זאת, מי שמשווק "דבר פרסומת" עבור אחר, כלומר חברות ההפצה - ייחשב כמפרסם.

החרגת חברות התקשורת מהגדרת "מפרסם" בחוק אחראית לחלק מהקשיים באכיפת חוק הספאם. בנוסף, בפועל הגבולות בין גורם שמשווק את עסקיו של השולח לבין מפיץ המסרים מטושטשים. כך, למרות שהחוק הישראלי מחריג את חברות התקשורת מאחריות על הפצת תכנים שיווקיים באופן לא חוקי, במקרים רבים, נראה שבתי המשפט תופסים את ההגנה המוחלטת על חברות התקשורת ככזו שחלה גם על חברות ההפצה. דוגמה בולטת לכך היא במקרים בהם חברת ההפצה היא גם חברת תקשורת, כמו חברת "טלזר" שאוחזת בשני הכובעים.[12] חברה גדולה נוספת כזו היא "שמיר". חברות אלה מספקות לבעלי עסקים פלטפורמה להפצת מסרים, והן מצהירות במסמכיהן שהאחריות על המסרים המופצים מוטלת על הלקוח שלהן ולא עליהן. על מנת שחברת הפצה תחשוף את זהות לקוחותיה יש צורך בצו שיפוטי. מכיוון שחברות אלה אחראיות להפצת תכנים ותו לא, לכאורה אין להן ידיעה לגבי תוכן המסרים. כך, הן פטורות מאחריות כאשר התוכן המופץ אינו לגיטימי (כמו תוכן הנוגע למכירת סמים, או הלוואות בשוק האפור) וגם בשאר המקרים, שבהם התוכן חוקי, שכן קיימת אפשרות שהתוכן המופץ חוסה תחת הגנת החוק (למשל במקרה של מסרים פוליטיים). בחלקו הבא של הפרק, נזכיר את הצעת החוק לעניין החרגת חברות התקשורת, המונחת כעת על שולחן הכנסת.

החוק מונה מספר **סנקציות** בגין הפרתו. הפרת סעיפי החוק היא עוולה אזרחית עליה חלות הוראות פקודת הנזיקין. מנגנוני האכיפה המרכזיים העומדים בפני נפגעי הספאם הם הגשת תביעה קטנה, כאשר החוק קובע פיצויים ללא הוכחת נזק בגובה של עד 1000 ש"ח לכל דבר פרסומת שנשלח בניגוד להוראות הסעיף; והגשת בקשה לאישור תובענה ייצוגית, לפי התוספת השנייה לחוק תובענות ייצוגיות שהכיר בחוק הספאם כעילת תביעה.[13] בנוסף, שליחת דבר פרסומת באופן אסור היא גם עבירה פלילית, והחוק קובע קנס של עד 226,000 ש"ח, לפי סעיף 61(א)(4) לחוק העונשין. על שליחה של מסר שאינה עומדת בתנאי סעיף 30א(ה), קובע החוק קנס של עד 75,300 ש"ח, לפי סעיף 61(א)(3) לחוק העונשין.

בחוק יש מספר חזקות לעניין החבות ולעניין **זהות החייבים** בגין הפרת סעיף 30א לחוק התקשורת. ראשית, סעיף 30א(ח) קובע כי כאשר מדובר בתאגיד, חובה על מנהל התאגיד ועל מי שאחראי בו לתחומי השיווק והפרסום לדאוג לכך שהוראות הסעיף לא יופרו. מקום בו הפר התאגיד או מי מעובדיו את הוראות הסעיף, יראו בכך הפרת חובה של נושא המשרה בתאגיד, אלא אם עשה כל שביכולתו כדי לעמוד בחובה שהטיל עליו החוק. כך, גם מנהלי תאגידים יתקשו להסיר מעצמם אחריות בטענה שלא היו אחראים להפרה. בנוסף, חזקה שמפרסם ששיגר דבר פרסומת בניגוד להוראות חוק הספאם - עשה כך ביודעין.

ב. תיקוני החקיקה

במהלך 15 השנים שחלפו מעת חקיקת חוק הספאם במאי 2008, הוא תוקן והורחב מספר פעמים במהלך השנים, כך שהוא חל גם על חומרי תעמולה, על בקשות תרומה, ועל מסרים הכוללים הצעה ליצירת תקשורת עם המפרסם לקבלת מסר מסוים.[14]

בשנת 2016 חוקק תיקון 63 לחוק התקשורת,[15] שכלל גם תיקון להסדר הספאם. תיקון זה הרחיב את הגדרת "דבר פרסומת" ואת הגדרת "מפרסם" באופן שכלל גם הפצת מסרים של תרומות ושל תעמולה. התיקון החריג מפורשות

12 ראו למשל ת"א (שלום ת"א) 332-12-17 **אופנר נ' פלאפון תקשורת בע"מ** (נבו 24.6.2020).

13 ראו סעיפים 30א(ו) ו-30א(י) לחוק התקשורת.

14 החוק תוקן באוגוסט 2016 באופן שיאפשר את תחולתו על בקשות תרומה ועל תעמולה (בסייגים מסוימים). ראו חוק התקשורת (בזק ושידורים) (תיקון מס' 63), התשע"ו-2016. במאי 2018 תוקן החוק באופן שמרחיב את הגדרת המושג "דבר פרסומת", כך שיכלול גם את תופעת ה"צנתוק", כלומר משלוח מסרים חלקיים לנמען תוך עידודו להתקשר למספר ממנו התקבלה ההודעה, ובכך לאלצו לקבל מסרים פרסומיים. חוק התקשורת (בזק ושידורים) (תיקון מס' 72), התשע"ח-2018.

15 חוק התקשורת (בזק ושידורים) (תיקון מס' 63), התשע"ו-2016.

תעמולה פוליטית מהגדרת "דבר פרסומת". בנוסף, התיקון חייב מפרסמים שמשתמשים בחיוג אוטומטי, להודיע לנמען בתחילת ההודעה שהוא יכול להיות מוסר מרשימת התפוצה וזאת על ידי לחיצה על חייגן.[16]

כשנתיים מאוחר יותר הגיע תיקון 66,[17] שקבע שמועד סיומה של התקשרות ממושכת בין נמען לבין עסק ייחשב כמועד בו התקבלה הודעת סירוב של הנמען להוסיף ולקבל מסרים שיווקיים מהעסק. התיקון נועד למנוע מצבים בהם מכוח ההיתר הקבוע בסעיף 30א(ג)(1), שמתיר למפרסם להוסיף ולשלוח דברי פרסומת למי שמסר את פרטי הקשר שלו, ושנמסר לו שפרטים אלה ישמשו לשם משלוח דברי פרסומת – יוסיף המפרסם לשלוח דברי פרסומת לנמען גם כאשר הנמען סיים את ההתקשרות עמו. במילים אחרות, אם אדם נרשם לאתר היכרויות, והסכים בעת ההרשמה לקבל דברי פרסומת מבעל האתר, הרי שמרגע שהחליט אותו אדם לסיים את ההתקשרות עם בעל האתר והודיע לו על כך, מסתיימת גם ההרשאה שנתן בנוגע לקבלת דברי פרסומת מאתר ההיכרויות, ועל בעל האתר נאסר להוסיף ולשלוח לו דברי פרסומת.

באותה שנה חוקק גם תיקון 72 לחוק התקשורת,[18] שנועד להתמודד עם תופעות חדשות שהביאו איתן מערכות חיוג אוטומטיות, כמו תופעה חדשה יחסית באותה העת: חיוג לנמען והשמעת מסרים חדשותיים או רכילותיים עם פרטי מידע חלקי, במטרה לגרום לו לחייג למספר אחר שהופיע בהקלטה ששמע. התיקון הרחיב את הגדרת "דבר פרסומת" כך שתכלול מסר שמציע לנמען להתקשר למספר מסוים לשם קבלת מסר פרסומי. תופעה נוספת עמה התמודד התיקון הייתה תופעת ה"צנתוק": חיוג לנמען באמצעות מערכת חיוג אוטומטי וניתוק השיחה בטרם נענתה, כדי לגרום לנמען לחייג בחזרה את אותו המספר, כך שהמפרסם יוכל להשמיע לנמען את דבר הפרסומת או את המסר. התיקון קבע שחיוג לנמען באמצעות מערכת חיוג אוטומטי, בלא קבלת הסכמתו המפורשת של הנמען מראש ובכתב, יהיה אסור אף אם החיוג הופסק בטרם נענתה השיחה, במקרים בהם בחיוג חוזר של המספר שממנו בוצע החיוג לנמען - מושמע לו דבר פרסומת.

בשנת 2022 חוקק תיקון 76 לחוק התקשורת,[19] שנכון להיום הוא התיקון האחרון לחוק הספאם. התיקון נוגע בעיקר לעניינים תשתיתיים בתחום שירותי הבזק, ולעניינים טרמינולוגיים הנוגעים להם. נכון לזמן כתיבת דוח זה, מונחת על שולחן הכנסת הצעת חוק פרטית שנועדה להתמודד עם הפטור ממנו נהנים כיום גורמי השיגור שנחשבים ל"צינור" בלבד, אך בפועל מאפשרים הגנה על ספאמרים, בכך שאינם חושפים את זהותם.[20] הקושי מתגבר לנוכח ריבוי ספאם בפלטפורמות המסרונים, כאשר שליחת המסרונים נעשית ממספרים פיקטיביים או שהיא נעדרת פרטים מספקים לשם קביעת זהות השולח. לפי ההצעה, מי ששלח הודעה עבור אחר יחויב לחשוף את פרטי השולח במקרה הצורך. אם יבחר שלא לחשוף את פרטי השולח הוא יחשב כמפרסם, ובהתאם - יחויב לשאת באחריות על שליחת המסרים. הצעות חוק זהות הונחו על שולחן הכנסת בשלוש הכנסות הקודמות. הצעה זו למעשה מנסחת קריאות קודמות מצד שחקנים בזירת הספאם, לשינוי מצב העניינים הנוכחי בנוגע לאחריות מפיץ המסרים. כך למשל, בדיונים שנערכו לקראת החקיקה, הציג נציג עמותת "אל ספאם" יוגב עזרא את עמדת העמותה ביחס למצב הבעייתי שיצר החוק הקיים בנוגע לחברות ההפצה והדיוור הישיר. חברות אלה שולחות מצד אחד הודעות בצורה אנונימית עבור לקוחותיהן, כאשר לפי הלכת **רמי מור** לא ניתן להגיש תביעה אזרחית נגד גורם אלמוני,[21] והחברות מסרבות לחשוף את שמות לקוחותיהן.[22] ובנוסף, החוק החריג את החברות מאחריות, כך שאי אפשר לתבוע אותן ישירות. עמדת "אל ספאם" הייתה שיש להתיר למי שמוחרג מהחוק לשמור על ההגנות הנתונות לו אם ימסור את פרטי הלקוח שמפיץ דואר זבל, ללא צו בית משפט, אלא בעקבות בקשה של הנפגע. במקרה של סירוב למסירת פרטים, לא ייהנה עוד המוחרג מהגנת החוק, ואפשר יהיה לתבוע אותו באופן אישי. לפי שעה, ההצעה לא התקבלה. נשוב לסוגיית האחריות גם בפרק ה, שבו נפרט המלצות שונות.

לסיכום, תיקוני החקיקה הגיבו לשינויים בדפוסי המשלוח של ספאם, להתנהגויות שונות של המפרסמים, וכן לשינויים טכנולוגיים מסוימים. חלק ניכר מהתיקונים פעלו לצד האזרח הנמען - כמו התיקון בדבר המשמעות של סיום התקשרות

16 ראו ס' 30אה(1)(ג)(2) לחוק התקשורת. הוועדה בכנסת שאחראית על החקיקה הייתה ועדת הכלכלה, וזאת בשונה מהוועדה האחראית על חקיקת חוק הספאם, שהייתה ועדה משותפת שכללה נציגים ממשרדי ממשלה נוספים.

17 חוק התקשורת (בזק ושידורים) (תיקון מס' 66), התשע"ח-2018.

18 חוק התקשורת (בזק ושידורים) (תיקון מס' 72), התשע"ח-2018.

19 חוק התקשורת (בזק ושידורים) (תיקון מס' 76), התשפ"ב-2022.

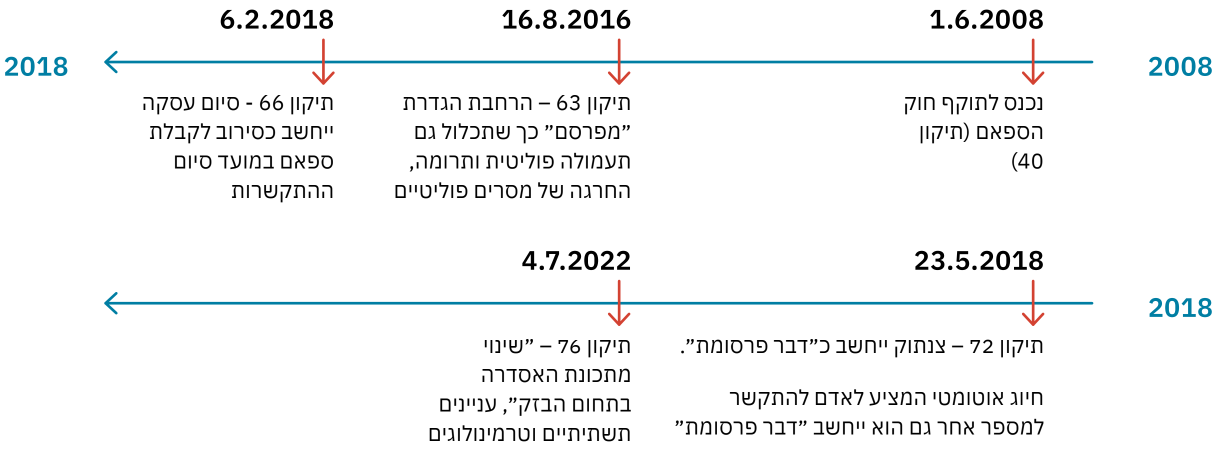
20 הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התשפ"ג-2022 (פ/276/25). ההצעה היא מהכנסת הנוכחית (ה-25).

21 רע"א 4447/07 **מור נ' ברק אי. טי. סי.** (1995) החברה לשירותי בזק בינלאומיים בע"מ, פ"ד סג(3) 664 (2010).

22 פרוטוקול ישיבה 138 של ועדת הכלכלה (4.1.2022), בעמ' 42-45.

ממושכת, או התיקון שהגיב ל"צנתוק". חלק מהתיקונים פעל דווקא לטובת מפרסמים מסוימים – כמו החרגת תעמולה פוליטית. עד כה, המחוקק נמנע מלהגיב לשינויים בדפוסי הפצת המסרים ולתופעה של ריבוי השחקנים השונים בצד ההפצה.

תרשים ג.1: ציר הזמן של חקיקת חוק הספאם ותיקוניו



ג. מגמות בפסיקה

בחמש עשרה השנים שחלפו מעת חקיקת חוק הספאם, הוגשו עשרות אלפי תביעות לערכאות השונות בבתי המשפט בארץ,[23] ולאורך השנים תרמו בתי המשפט את חלקם בפרשנות ובעיצוב החוק. בתי המשפט קבעו שורת קביעות עקרוניות, חלקן הרחיב וחלקן צמצם את תחולת החוק.

בצד המרחיב, ראוי לציין פסקי דין שהרחיבו את ההגדרה של "דבר פרסומת" – למשל, שההגדרה חלה גם על הודעות שמציעות הטבות שונות במטרה למשוך את הנמען להתקשר עם המפרסם שלא באמצעות מסר מפורש וישיר, אלא בדרכים עקיפות ו"תמימות", כמו למשל הזמנה לקבלת "הטבה".[24] במקרה נוסף קבע בית המשפט כי גם הודעה שיווקית באמצעות הצ'אט של פייסבוק היא "הודעה אלקטרונית" עליה חל חוק הספאם, שכן מדובר במסר המועבר ברשת האינטרנט, שאותו ניתן לשמור באופן ממוחשב.[25] לעניין הצנתוק, עוד בשנת 2011 קבעה השופטת אגמון-גונן כי שיטת הצנתוק מפרה את הוראות סעיף 30א לחוק התקשורת.[26]

בצד המצמצם, קבע בית המשפט בעניין **קסטרו** כי גם מסירת מספר טלפון נייח ולא נייד מאפשרת לבעל עסק לחסות תחת החריג לסעיף 30א(ג) ולשלוח מסר פרסומי למי שאישר קבלת מידע פרסומי בטופס הצטרפות. במסגרת זו קבע בית המשפט לגבי התנאי הראשון של החריג לפיו "הנמען מסר את פרטיו למפרסם במהלך רכישה של מוצר או שירות, או במהלך משא ומתן לרכישה כאמור", שאין זה משנה אם הפרטים נמסרו לטובת מטרה אחרת מקבלת מידע פרסומי.[27] בעניין **בזק** נקבע שמסרון שמטרתו אינה פרסומית אלא הוא נועד למתן שירות, אינו 'דבר פרסומת' כהגדרתו בחוק התקשורת.[28] בעניין **טויסטר** קבע בית המשפט שיש לפרש את המונח "הודעה אלקטרונית" בצמצום.[29]

23 ראו דוח איגוד האינטרנט, לעיל ה"ש 9, בפרק המבוא.

24 ת"צ (ת"א) 10591-05-15 **גלסברג נ' פסגות בית השקעות בע"מ** (נבו 9.5.2017).

25 ת"צ (מחוזי חי') 24822-02-20 **לב נ' דאבלטק בע"מ** (נבו 24.2.2021).

26 ת"א (מחוזי ת"א) 1586/09 **חיות נ' טלרן מסרים מיידים בע"מ** (נבו 5.4.2011), בעמ' 16-19.

27 ראו ע"א (מחוזי י-ם) 2526-12-17 **קסטרו מודל בע"מ נ' רגב** (נבו 8.4.2018), בפס' 10-14.

28 המסרון נועד ליידע את הנמענים בנוגע לשירות אינטרנט של בזק ללא תשלום וללא תוכן פרסומי. ראו רע"א 1154/18 **בזק החברה הישראלית לתקשורת בע"מ נ' זינגר** (נבו 6.6.2019), בפס' 3.

29 פסק הדין עסק במערכת ה- Remarketingשל גוגל, שמאפשרת למפרסם לכוון את הפרסומות שלו למשתמשים שגלשו באתר שלו בעבר. בית המשפט דן בשאלה האם מדובר ב"הודעה אלקטרונית" שהיא אחת מדרכי השיגור של פרסומת המנויות בס' 30א(ב). השופט גרוסקופף פירט את ארבעת המרכיבים בהגדרה של הודעה אלקטרונית (המופיעה בס' 30א(א) לחוק התקשורת), שהם: (1) מסר בזק מקודד, (2) המועבר ברשת האינטרנט, (3) אל נמען או קבוצה של נמענים, (4) וניתן לשמירה ולאחזור בדרך ממוחשבת. השופט גרוסקופף קבע שיש לפרש את המונח

נקודת ציון משמעותית בפסיקת בתי המשפט בנושאי ספאם הייתה שני פסקי דין שניתנו בבית המשפט העליון בשנת 2014, שניהם עסקו בשאלת הפיצוי. הרקע לפסקי הדין הוא עלייה במספר התביעות שהוגשו, ואי נחת של בתי המשפט מהעיסוק הגובר בסוגייה. פסק הדין הראשון, **גלסברג נ' קלאב רמון**, עסק בגובה הפיצויים שיש לפסוק בתביעה לפי סעיף 30א לחוק התקשורת. בית המשפט הטעים כי המחוקק רואה בפיצוי לדוגמה הקבוע בסעיף 30א(י) לחוק את האמצעי היעיל ביותר להגשמת תכלית הסעיף, שהיא בלימת תופעת הספאם.[30] הפיצוי לדוגמה נועד לעודד אכיפה פרטית, שהיא היא, בעיני המחוקק, הכלי האפקטיבי ביותר ליישום החוק ואכיפתו. בית המשפט קבע כנקודת מוצא סכום תקרה של 1000 ש"ח להודעת ספאם אחת, כאשר מסכום זה ניתן יהיה להפחית בנסיבות המתאימות, לדוגמה כאשר הנפגע לא לחץ על כפתור "הסר" מרשימת תפוצה ובכך לא פעל מספיק לשם הקטנת הנזק.

פסק הדין השני, **חזני נ' הנגבי**, עסק באמת המידה לפסיקת פיצוי ללא הוכחת נזק בגין הפצת ספאם.[31] בית המשפט העליון למעשה חזר בו מהקביעה בעניין **גלסברג** לעניין חובת הקטנת הנזק, וקבע שבמקרה שבו דבר פרסומת כולל אפשרות של הסרה מרשימת תפוצה, הדבר יהיה שיקול להפחתת הפיצוי שייפסק. בית המשפט העליון בעניין **חזני** הבהיר שהשיקולים שיש לשקול לשם קביעת סכום הפיצוי הם בין היתר: (1) אכיפת החוק והרתעה מפני הפרתו; (2) עידוד הנמען למימוש זכויותיו; ו-(3) היקף ההפרה. מטרת הפיצוי, לפי בית המשפט, אינה להשיב את מצבו של התובע לקדמותו, כי אם לאכוף את החוק, להרתיע את הנתבע ולתמרץ הגשת תביעות יעילות. מול השיקולים שנועדו להשיג את המטרות הללו, בית המשפט גם צריך לוודא שהפיצוי לא יעלה על הנדרש לשם השגתן. בית המשפט קבע שאין חובה על הנמען ללחוץ על כפתור "הסרה" מרשימת תפוצה על מנת לזכות במלוא הפיצוי, כלומר לא חלה עליו חובת הקטנת הנזק.[32]

ההבדל החשוב לענייננו הוא שבניגוד לעניין **גלסברג**, שם בית המשפט ראה באור חיובי את מתן האפשרות לנמענים ללחוץ על כפתור "הסר" מרשימת תפוצה, בעניין **חזני** בית המשפט הביא בחשבון את השיקול הטכנולוגי, בהתחשבו בכך שלחיצה על קישור (לינק) עשויה דווקא להגדיל את הנזק של הנמען ולחשוף אותו לסכנות כמו גניבת מידע או השתלת רוגלות במכשירו. בית המשפט הטעים כי אם תוטל חובת הקטנת נזק על הנמען עשויה להביא לכך שמפרסמים יוסיפו בקלות רבה כפתור הסרה מה שיהפוך שליחת פרסומות לנמענים ללא הסכמתם למשתלמת עוד יותר, בעוד שעבור הנמענים אפשרות הסרה עשויה להפוך את הטרחה שבתביעה ללא משתלמת.

במחקר שערכה הנהלת בתי המשפט עלה שבשנת 2014, 1.2% מכלל התביעות בבתי המשפט לתביעות קטנות היו תביעות ספאם.[33] אולם עורכות המחקר ציינו שלמרות הנתונים הללו, מראיונות שערכו עם גורמים שיפוטיים לקראת תום המחקר בשנת 2016, עלה שקיימת עלייה בכמות תיקי הספאם וכן שנראה שהצדדים "מגיעים מוכנים מאד לדיון, כיוון שיש אתרי אינטרנט ייעודיים לעניין המכוונים אותם בכתיבת כתב התביעה וההערכות לדיון עם פסיקה רלוונטית בנושא.[34] ייתכן שעדויות אלה משקפות את השלב הנוסף במשחק "חתול ועכבר" זה, שהגיע לשיא עם כניסתה לתמונה של חברת "ספאם אוף", אותה הצגנו בפרק הקודם,[35] והסתיים מרגע שקבע בית המשפט העליון את הלכת **ארד**, עליה נרחיב בהמשך פרק זה, בחלק 3, שעוסק בתביעות קטנות.

של הודעה אלקטרונית "בצמצום... כך שלא תחול על כל דבר פרסומת המוצג באתר תוכן", בהתאם הוא השווה בין הפרסומות המוצגות באתרים לבין דוא"ל (ה"גרעין" של המונח "הודעה אלקטרונית") והגיע למסקנה כי: "בשונה מפרסומת בה נתקל משתמש באתר תוכן, אשר נעלמת מעולמו מיד כשהוא עוזב את האתר... פרסומת הנשלחת למערכת דואר אלקטרוני מטילה על המשתמש את הנטל לקבל החלטה מה יעשה בה... מניעת הכבדה נוספת זו היא שמצדיקה, מבחינת תכלית ההסדר בעניין דואר זבל, את האיסור על העברת פרסומת באמצעות דואר אלקטרוני ללא קבלת הסכמת המשתמש". מאחר שהפרסומות המופיעות באתרים אינן "מטילות על המשתמש את הנטל לטפל בהן לאחר שיעזוב את אתר התוכן אליו גלש.. מכאן ששירות ה- Remarketing איננו מביא ליצירת ההכבדה שההסדר בעניין דואר זבל ביקש למנוע." ראו ת"צ (מחוזי מרכז) 1862-11-12 **טויסטר נ' Google Inc.** (נבו 18.9.2014), בפס' 24-20.

30 רע"א 2904/14 **גלסברג נ' קלאב רמון בע"מ** (נבו 27.7.2014).

31 רע"א 1954/14 **חזני נ' הנגבי (סיתונית מועדון דאיה ורחיפה במצנחים)** (נבו 4.8.2014).

32 עם זאת, במסגרת פסיקת הפיצוי יוכל בית המשפט לשקול את העובדה שלחיצה על כפתור ההסרה הייתה קלה יחסית.

33 גלי אביב וענבל גלון "בית המשפט לתביעות קטנות" (מחלקת המחקר של הרשות השופטת, 1.9.2016), בעמ' 16.

34 שם, בעמ' 18-17.

35 ראו שם, בעמ' 39-38.

3. מנגנוני אכיפה: תמונת מצב בשטח

כאמור, החוק מאפשר אפיק של תביעה אישית ללא הוכחת נזק, ואפיק של תובענה ייצוגית, כאשר הנתבעים הפוטנציאליים האפשריים הם המפרסם או חברת ההפצה. בחלק זה, נתאר את המצב בשטח, על בסיס הפסיקה ונתונים אמפיריים.

א. מנגנון ראשון: תביעה אישית ותביעות בהליכים מקוצרים

מרבית התביעות בענייני ספאם מוגשות בבתי המשפט לתביעות קטנות. בין השנים 2022-2016 הוגשו בארץ לכל הפחות 13,133 תביעות ספאם.[36] 93% מהן היו תביעות קטנות (12,228) לעומת 7% תביעות מסוג סדר דין מהיר (905). בנוסף, בשנים אלה הוגשו 232 בקשות לאישור תובענות ייצוגיות בנושא ספאם,[37] פחות ממחצית מתביעות הספאם (43%) שהוגשו לבתי המשפט בשנים אלה התקבלו, כאשר הסיבה לכך עשויה להיות לעיתים הסדר פשרה.[38] בנוגע לסיכויי ההצלחה של תביעה קטנה בתיקי ספאם, לפי נתוני המחקר שערך איגוד האינטרנט בנושא, המשתנה שמסייע לנבא את סיכויי ההצלחה באופן מיטבי הוא זהות הגוף הנתבע. עוד עלה מנתוני הדוח כי מאפיינים לא מהותיים, כמו אזור השיפוט, זהות השופט, או סכום התביעה אינם מספקים פתרון טוב לחיזוי תוצאות התיק.[39]

לבית המשפט לתביעות קטנות יש סמכות לדון בתביעות אזרחיות שהגיש יחיד עד סכום של 36,400 ש"ח (נכון למועד זה).[40] בתי המשפט לתביעות קטנות יכולים לקבל ראיות שאינן קבילות בבית משפט אחר, ובנוסף הם אינם כפופים לסדרי הדין הנהוגים בבתי משפט אחרים. כל זאת לטובת העיקרון שמנחה את פעילות בתי המשפט לתביעות קטנות, שעל בית המשפט לפעול "בדרך הנראית לו מועילה ביותר להכרעה צודקת ומהירה".[41] לדברי השופט רובינשטיין, כוונת המחוקק הייתה לייסד הליך שיפוטי שמטרתו "הליך חסכוני שאינו מטיל הוצאות גדולות על הצדדים, ומהיר, שאינו גוזל מזמנם יתר על המידה".[42]

מאפיין מרכזי ומהותי של הליכי תביעות קטנות הוא שהתובע אינו מיוצג באופן מקצועי על ידי עורך דין. שאלה זו הפכה מהותית סביב תביעות בנושאי ספאם לאחר כניסתה של חברת "ספאם אוף" לזירה, שאת פעילותה תיארנו בפרק הקודם. כאן נדגיש מספר היבטים משפטיים של התופעה. במהלך תקופת הפעילות של החברה, היקף הגשת תביעות הספאם תפח והגיע בממוצע לפי-שבעה יותר תיקים שנפתחו בכל חודש.[43] תרשים עומס של איגוד האינטרנט מגלה עומס גדול של תיקים פתוחים שהגיע עד כדי ארבעת אלפים תיקים פתוחים בחודש אפריל 2017 (רובם תיקי תביעות קטנות).[44] עומס התביעות הביא לעוינות גלויה כלפי פעילות החברה, אולם ריבוי התביעות בעת פעילות החברה עשוי להעיד על כך שפעילותה עזרה לקדם נגישות להליכים משפטיים, וזאת בעזרת אוטומציה של שירותים משפטיים.

כך סבר גם בית המשפט העליון בעניין **ארד**. עיקר הפרשה סבבה סביב שאלת הייצוג בתיקי תביעות קטנות. סעיף 63(א) לחוק בתי המשפט (נוסח משולב), התשמ"ד-1984 מסדיר את נושא הייצוג בתביעה קטנה, ולפיו ייצוג על ידי עורך דין יינתן רק בנסיבות מיוחדות, ורק באישור בית המשפט. הסעיף גם קובע את האפשרות להיות מיוצג על ידי

36 הנתונים מתבססים על דוח האיגוד, ראו דוח האיגוד בעמ' 9. אנו מציינים "לכל הפחות", משום שלעיתים סיווג פסקי הדין במערכות השונות חסר.

37 ראו דוח האיגוד האינטרנט, לעיל ה"ש 9, בפרק "ממצאים ודיון", תת הפרק "היקף תביעות הספאם והטיפול בהן".

38 דוח האיגוד בעמ' 22: "מתוך כלל תביעות הספאם שנסגרו בין השנים 2016-2022 (12,797), 43% מהתביעות (5,491) התקבלו, 25.7% (3,292) נדחו, 31% (3,966) נמחקו וב-1.7% (48) חלה תוצאה אחרת (סגירה טכנית, עיכוב בוררות, פשרה, מחיקת/דחיית התיק ע"י מגישו או אחר). בהשוואה לת"ק ותא"ם אחרות, תביעות ספאם נדחות יותר, ההסבר שהוצע הוא "אי היכרות מספקת של האזרחים עם תוכן חוק הספאם ו/או תפיסה מקלה של השופטים בתופעה" (עמ' 25). הדוח אינו מספק מידע בנוגע לפשרות בתיקי ספאם.

39 דוח איגוד האינטרנט, לעיל ה"ש 9, בפרק "סיכום ויכולת ניבוי".

40 ס' 60(א)(1) לחוק בתי המשפט (נוסח משולב), התשמ"ד-1984.

41 ס' 62(ב), שם.

42 רע"א 6892/13 **חיימוביץ' נ' אוריון** (נבו 23.2.2014).

43 "בין ספטמבר 2016 לאפריל 2017 הייתה עמוסה במיוחד בהיקף הגשת תביעות הספאם, כשבכל חודש למעט אוקטובר 2016 נפתחו בין כ- 500 ל- 1000 ספאם תביעות חדשות. זאת לעומת96 תיקי ספאם חדשים בממוצע לחודש החל ממאי 2017." ראו דוח האיגוד האינטרנט, לעיל ה"ש 9, בפרק "ממצאים ודיון", תת הפרק "היקף תביעות הספאם והטיפול בהן".

44 שם.

ארגון שקבע שר המשפטים ובאישור בית המשפט, כאשר במצב כזה גם הצד שכנגד יוכל להיות מיוצג, ברשות בית המשפט. סעיף 63(ב) לחוק מציג חריג לסעיף הייצוג, וקובע שאדם יכול לייצג אחר, אם בית המשפט אישר זאת וגם בעל הדין נתן ייפוי כוח לאותו אדם לעניין זה. ההחרגה לא תחול בשלושה מקרים: 1. אם המייצג עוסק בכך דרך קבע; 2. אם הייצוג נעשה במהלך הרגיל של עסקיו של המייצג; 3. אם הייצוג נעשה בתמורה.

במהלך תקופת הפעילות של "ספאם אוף", החברה העלתה עליה את קצפם של עורכי דין שסברו שהיא עוקפת את הגבלות הייצוג בתיקי תביעות קטנות בניגוד לחוק, ובכך מסיגה את גבולות מקצוע עריכת הדין. החברה גם העלתה את כעסם של שופטים, שסברו שהחברה מבקשת להתעשר באמצעות נגיסה בתשלומי הפיצויים של תובעים בהליך שאוסר על ייצוג מקצועי. אכן, בעניין **גלסברג** קבע השופט רובינשטיין בנוגע לתום הלב של התובע הסדרתי, כי "ברי שסעיף 30א לחוק התקשורת מעודד הלכה למעשה הגשת תביעות רבות מכוחו בקלות יחסית, ואין זה פלא כי יש אשר אולי יראו בכך מקור הכנסה נאה בטרחה מועטה... סבורני כי מיטיב היה המחוקק לעשות אילו נתן לכך דעתו ואיפשר לבתי המשפט במקרים המתאימים, ומבלי לאיין את התמריץ שיש לשמר לעניין הגשת תביעות מעין אלה, לפסוק חלק מן הסכומים לטובת מטרות ציבוריות כגון עמותות – שבהן כמובן אין כוונת רווח – אשר שמו להן למטרה להילחם בתופעת ה-spam באופן קונקרטי, או למען הגנת הפרטיות".[45] ככל שמנגנון זה אינו בנמצא, קבע השופט, נתון לבית המשפט שיקול דעת, לקבוע למשל, כי תובע מסוים מייצר תביעות חדשות לבקרים, מה שעל פניו עלול להחשיד ב"תאוות רווח אישי". בנוסף לכך, סברו בתי המשפט כי מעורבותה של החברה יוצרת "כשל שוק" המפר את האיזון שביקשו המחוקק ובתי המשפט לערוך, בין הרתעת חברות ועסקים מלשלוח הודעות ספאם מפרות לבין מיטוט עסקים קטנים אשר מעדו באופן נקודתי או ממוקד.[46] עוד סברו בתי המשפט שפעילות החברה מייצרת עומס חריג – ומיותר – על בתי המשפט לתביעות קטנות, מה שמקשה עליהם למלא את ייעודם, ופוגע בציבור בכללותו, וכן שהיא פוגעת בלקוחותיה המגיעים תכופות לא מוכנים לבית המשפט.[47]

הדיון בעניין הייצוג הגיע כאמור לפתחו של בית המשפט העליון, בעניין **ארד**. עוד בעניין **רז נ' האפרתי** דן בית המשפט העליון בשאלת הייצוג על ידי מייצג מקצועי, כלומר עורך דין, בבית המשפט לתביעות קטנות, סביב תביעת ספאם.[48] בית המשפט בעניין **רז** אמנם סבר שבמקרה זה היה חשש שאכן הייצוג לא עמד בתנאי סעיף 63(א), אך לא מצא לנכון להתערב בפסק הדין בשל כך. במקרה "ספאם אוף", בית המשפט קבע שלמרות שכביכול החברה לא עמדה בתנאים שהחוק הגדיר, שכן היא אינה ארגון שהוכר מטעם משרד המשפטים, וכן היא מקבלת תמורה בעבור הייצוג (החברה גבתה מכל תובע תעריף הצלחה בגובה 20% מסכום הפיצוי), הרי שפעילותה עומדת בדרישות החוק.[49] זאת בשל העובדה שהתכלית של פעילות החברה עלתה בקנה אחד עם מהות מוסד התביעות הקטנות, שהיא פתיחת שערי המשפט בפני האזרח הקטן, וזאת בכדי לאפשר לו כלי מהיר, זול וזמין לבירור תביעות בהיקף כספי מצומצם לשם מיצוי זכויותיו. אולם, כפי שהזכרנו בפרק ב, עד שניתן פסק הדין בעניינה, החברה כבר הפסיקה את פעילותה.

ב. מנגנון שני: תובענה ייצוגית

בין השנים 2022-2016 הוגשו בישראל 232 בקשות לאישור תובענות ייצוגיות בעניין ספאם.[50] בקשות אלה האלה הביאו, לדברי עורכי דין שעוסקים בתחום, לעלייה בנכונות המפרסמים הלגיטימיים לכבד את הוראות חוק הספאם.[51] עם זאת, מכיוון שבמנגנון התביעה הייצוגית לא קיים פיצוי לדוגמה, קשה להעריך מהו הסכום שיש לדרוש כפיצוי על הודעת ספאם אחת, וקשה לקבוע מהו הסכום שייצר הרתעה יעילה. בעוד שכאשר מדובר בספקי לידים, סכומי התביעה יכולים להגיע למיליוני שקלים, הרי שבמקרים של חברות קטנות יותר מדובר בסכומי גמול להפרה שלא

45 רע"א 2904/14 **גלסברג נ' קלאב רמון בע"מ** (נבו 27.7.2014), בפס' יד לפסק דינו של השופט רובינשטיין.

46 ת"ק (כ"ס) 2809-05-16 **פנחס נ' טוטוקרד 5 בע"מ** (נבו 15.8.2016), בפס' 29-31.

47 ראו ת"ק (חד') 42711-03-17 **זיסו נ' המרכז הישראלי ל.ע. ברשת בע"מ** (נבו 19.8.2017), בפס' 13; ת"ק (עכו) 48592-12-16 **יעקובוב נ' אל.טי. - פאוור טכנולוג'יס בע"מ** (נבו 5.4.2017), בפס' 3-4.

48 רע"א 1868/16 **רז נ' האפרתי** (נבו 19.6.2016).

49 רע"א 7064/17 **ארד נ' מנקס אונליין טריידינג בע"מ** (נבו 11.12.2018).

50 ראו דוח האיגוד האינטרנט, לעיל ה"ש 9, בפרק "ממצאים ודיון", תת הפרק "היקף תביעות הספאם והטיפול בהן".

51 הדברים עלו בשיחה עם עו"ד זיו גלסברג, שנערכה ביום 30.4.2023.

בהכרח ייצרו תמריצים מספקים לשם הגשת תביעה. בנוסף, בניגוד לתביעות קטנות ולתביעות בסדר דין מהיר בענייני ספאם, מטבע הדברים לתובענה ייצוגית לוקח זמן רב יותר להתברר ולהיסגר.[52]

ההיגיון הכלכלי של התובענה הייצוגית וההיגיון הכלכלי של הספאם מתנגשים.

בצד התובענה הייצוגית, מנגנון משפטי זה מבקש להתגבר על כשל משפטי ידוע: כאשר גורם אחד מזיק לאנשים רבים, ושיעור הנזק שנגרם לכל אחד קטן, הסיכוי שמי מהם יתבע – קטן, וזאת במיוחד כאשר מדובר בתובענות מורכבות מבחינה משפטית וטכנולוגית, כלומר בתביעות שיש עלויות יחסית גבוהות להכנתן.[53] כאן נכנס מנגנון התובענות הייצוגיות לתמונה: התביעה הייצוגית מאפשרת לאחד לתבוע בשם הקבוצה, כאשר מדובר בשאלה עובדתית ומשפטית שמשותפת לחברי הקבוצה.[54] התמריץ של האחד הוא הגמול שיינתן לתובע – ולא פחות חושב מכך – לעורכי הדין – עם ההליך יסתיים בהצלחה.

בצד הספאם (להרחבה ראו פרק ב): כאשר מדובר בחברות גדולות, ההנחה העומדת מאחורי הפצת מסרים המוניים ללא הסכמת הנמענים היא שמתוך מאות אלפים של נמענים שקיבלו מסר כזה, רק בודדים ישלחו מסרון ביטול, ואם בקשתם לא תכובד, רק נמענים ספורים מתוך האחרונים עשויים לטרוח ולהגיש תביעה. במילים אחרות, הרווח הצפוי לשולח המסרים גבוה, והסיכון קטן. עם זאת, הסיכון קיים, כפי שמעידות התביעות שכן הוגשו בנושא. תובענה ייצוגית עשויה להתגבר על המאזן הכלכלי הקיים, לפיו הנזק הכלכלי שנגרם לשולח הספאם הוא אפסי, ולעומתו הרווח הכלכלי שלו עשוי להיות גדול מאוד.

מנגד, נמצאים התובעים. כפי שהסביר לנו עו"ד גלסברג, רוב התובעים הסדרתיים עושים זאת מתוך אידיאולוגיה.[55] עבור עורכי הדין העוסקים בתחום, הגשת תובענה ייצוגית בעניין ספאם אינה עסק משתלם במיוחד מבחינה כלכלית, ונוסף על כך הקושי הנובע מהפיכת סוגיית תום הלב של התובע לעיתים קרובות לשאלה מרכזית.

ג. מנגנוני הסדרה נוספים

בחודש אפריל 2023 נכנסו לתוקף הנחיות חדשות של משרד התקשורת לעניין הסדרת הפצת מסרונים.[56] הנחיות אלה נולדו בעקבות הבנה שמערכות הדיוור וההפצה הישירה מנוצלות לרעה, למשל על ידי מפיצי קנאביס. מפיצים של מסרים שתוכנם אינו חוקי משתמשים במערכות הדיוור – הם מציגים למנהלי המערכות כרטיסי אשראי מזויפים שמאפשרים להם לעבור את מערכות האבטחה של המפיצים, ולייצר סליקה מקוונת, ובהמשך רוכשים חבילות של הודעות טקסט ומשתמשים בשירותי המערכת כדי להפיצם. לחברות ההפצה יש אינטרס ברור לסכל את הפעילות הזו – הן משום שהיא אינה חוקית, והן, ובעיקר, משום שפעילות המפיצים הלא חוקיים עלולה להשפיע על סיווג חברות ההפצה עצמן: אם הן תיכנסנה לרשימה שחורה, הדבר יפגע בעסקים הלגיטימיים שלהן. למרות שחברות ההפצה מנסות לברר את זהות ואמינות לקוחותיהן, לא תמיד הן הצליחו לזהות זיופים.

הנחיות 2023 מחייבות את חברות ההפצה לאמת את זהות לקוחותיהן, וכן, הן מגבילות את כמות ההודעות שניתן לשגר בו זמנית בתשלום מראש. ההנחיות מבקשות להתמודד עם העובדה שהפרוטוקול של הודעות סמס פרוץ יחסית, וקל לתמרן אותו. הפרוטוקול מכיל ארבעה שדות כאשר פרט לכתובת הנמען ולתוכן ההודעה, ישנו בנוסף שדה ה-CLI (Command-Line Interface), שבו ניתן לכתוב מספר טלפון או טקסט ללא מגבלה; וכן שדה ה-SMSC (Short Mes-sage Service Center), כלומר שרת המסרונים, המכיל את המספר ממנו באמת נשלחה ההודעה, שאותו הנמענים לא תמיד רואים, ובנוסף הגישה אליו אינה פשוטה. בהתאם, הנחיות משרד התקשורת קובעות שאם ב-CLI מופיע מספר טלפון, יש לוודא שהוא מתאים למספר שמופיע בשדה ה-SMSC, כלומר שהוא תואם לזהות השולח. אם ה-CLI מכיל טקסט, על חברת ההפצה לזהות במי מדובר ולבקש מסמכים לאימות.

52 על כך ראו גם בדוח האיגוד האינטרנט, לעיל ה"ש 9, בפרק "ממצאים ודיון", תת הפרק "היקף תביעות הספאם והטיפול בהן".

53 ראו אלון קלמנט "קווים מנחים לפרשנות חוק התובענות הייצוגיות, התשס"ו-2006" **הפרקליט** מט 131 (2007).

54 ראו ס' 4(א)(1) לחוק התובענות הייצוגיות, התשס"ו-2006.

55 הדברים נאמרו בשיחה שנערכה ביום 30.4.2023.

56 הוראת מנהל של משרד התקשורת "שירות שליחת מסר קצר ('מסרון')" (13.2.2023). ראו באתר משרד התקשורת: https://www.gov.il/he/departments/policies/14022023_1.

לעת עתה, נראה שהרגולציה החדשה מצליחה להתמודד עם הבעיה המרכזית אותה היא נועדה לפתור, שהיא בעיקר מסרים שמבקשים לשווק עסקים לא חוקיים, אולם היא אינה מבטיחה צמצום של ספאם שיווקי "רגיל". מנקודת המבט של חברות ההפצה, הרגולציה החדשה נתפסת כבעייתית. כדברי אחד מבעלי החברות, "זה בא להרוג עשבים שוטים, אבל הורג הרבה מעבר. זה חונק הרבה לקוחות."[57] תחת הרגולציה החדשה, על חברות הדיוור הישיר לבצע עם כל לקוח שיחת וידאו בה עליו להציג תעודות, וכן לבצע סריקה שדורשת אימות מול חברת האשראי. תהליך וידוא זה מייקר את ההליכים הנדרשים על מנת לאמת לקוחות חדשים, מאריך אותם עד כדי הכפלת כמות העבודה לעסקה, וכך מצמצם את מספר הלקוחות הפונים לבקש שירותים מהחברות – וכל זה, מייקר את העלויות של החברות האלה. בנוסף, משרד התקשורת דורש מחברות הדיוור לבצע את ההליכים האלה גם מול לקוחות קיימים.

תוצאה אחת של ייקור העלויות למפיצים היא ניסיון לעקוף את ההנחיות. אחד האפיקים החדשים אליהם פונות חברות ההפצה, ועמם לקוחות שיכולים להרשות לעצמם, הוא סוגי מסר שהרגולציה אינה חלה עליהם, כמו הודעות וואטסאפ שבבעלות חברת מטא. מכיוון שמדובר בחבילות יקרות בהרבה, עסקים קטנים נפגעים יותר: גם אם יש להניח שרבים מהם יפסיקו להשתמש בשרותי הודעות טקסט, הם לא בהכרח ירכשו במקום זאת חבילות וואטסאפ.

כאמור, ההנחיות עדיין חדשות. הן עוסקות בסוגיה נקודתית – אבל חשובה – של משלוח הודעות לא חוקיות באמצעות חברות ההפצה, בצד הודעות חוקיות, ומנסות ליצור מנגנון שיבדל בין החוקי ללא-חוקי. בשלב זה, נראה שהשוק עדיין לומד את ההנחיות, אבל כבר מחפש דרכים לעקוף אותן. השפעת ההנחיות על שוק הספאם הלא-חוקי והחוקי גם יחד, ראויה לבחינה נוספת בעתיד, לאחר שיצטבר ניסיון מעשי בשטח.

4. פתרונות משפטיים בעולם ומידת התאמתם לישראל

אך מובן שישראל אינה היחידה שמתמודדת עם סוגיית הספאם. מדינות שונות ניסו ומנסות פתרונות שונים. חלק זה סוקר את הפתרונות המרכזיים, ובוחן את מידת התאמתם לישראל. נציג תחילה את השיטות השונות באופן כללי, ולאחר מכן את הגישות בקשר לפלטפורמה שכפופה לחוק, את הגדרות הדינים לעניין המסרים ושולחיהם, את מודל ההסכמה, והיבטים של אכיפה.

החוק והשיטה

בעולם המערבי יש שתי שיטות מרכזיות להתמודדות עם ספאם. לפי **השיטה האירופית**, שהחוק הישראלי הלך בעקבותיה עד כה, אסור לשלוח ספאם לנמען, אלא אם הנמען הביע הסכמה מפורשת מראש וניתנה לו אפשרות לסרב בכל עת לקבלת ספאם. כלומר, שיטה של opt in. לפי **השיטה האמריקנית**, מותר לשלוח ספאם לכל נמען שלא נרשם אקטיבית ברשימת המסרבים לקבלת ספאם. כלומר, opt out. הביקורת המרכזית נגד שיטה זו נוגעת לסכנות שבפריצה למאגר שמרכז בתוכו מיליוני כתובות דוא"ל ומספרי טלפון.

החקיקה הרלוונטית באירופה היא Directive on Privacy and Electronic Communications, שנכנסה לתוקף באוקטובר 2003. הדירקטיבה עוסקת בהגנת פרטיות, והסדרת ספאם היא רק מטרה נלווית. בארצות הברית קיימת חקיקה פדרלית לעניין ספאם טלפוני (TCPA -Telephone Consumer Protection Act) עוד משנת 1991,[58] שעברה תיקונים לאורך השנים, בניסיון להתאימה לשינויים טכנולוגיים.[59] כמו כן, בשנת 2003 נכנסה לתוקפה חקיקה פדרלית נוספת, הנוגעת לספאם המופץ באמצעות דואר אלקטרוני.[60]

57 מתוך שיחה עם נאור מן, שנערכה ביום 1.6.2023.

58 Telephone Consumer Protection Act, ראו: https://www.fcc.gov/sites/default/files/tcpa-rules.pdf.

59 לדיון בעובדה שהחוק אינו מתאים למציאות הטכנולוגית העכשווית, ראו: Marissa J. Blasing, *The Telephone Consumer Protection Act of 1991: Adapting an "Odd" Law*, 62 Santa Clara L. Rev. 411 (2022). לסקירת החוק על השינויים הרבים שחלו בו עד שנת 2013, ראו: Spencer Weber Waller, Daniel B. Heidtke, and Jessica Stewart, *The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology*, 26 Loy. Consumer L. Rev. 343 (2013).

60 Controlling the Assault of Non-Solicited Pornography and Marketing Act, ראו: https://www.govinfo.gov/content/pkg/PLAW-108publ187/pdf/PLAW-108publ187.pdf.

<u>פלטפורמות עליהן חל החוק</u>

חוק התקשורת הישראלי והדירקטיבה האירופית, חלים שניהם על הודעות שנשלחות באמצעות פקס, מערכות חיוג אוטומטיות, מסרונים, והודעות דוא"ל.[61] לעומת זאת, החוק האמריקני מפוצל: בעוד שה-TCPA חל על שיחות טלפון אוטומטיות (רובוקולס - robocalls), מסרונים ופקס, ומעורר בעיות רבות בעניין התאמתו לשינויים טכנולוגיים, הרי שהחוק משנת 2003 נוגע לדוא"ל ומבהיר מפורשות שאין כוונה להחילו על פלטפורמות נוספות וזאת על מנת למנוע התנגשות עם ה-TCPA, המסדיר תקשורת סלולרית.[62] עם זאת, בעשור האחרון, עם כניסת הרשתות החברתיות לתמונה, קיימת תנועה לכיוון הרחבת ההגדרה הצרה של פלטפורמת ההפצה בחוק.[63]

טבלה ג.1: מושא ההסדרה של חוקי ספאם

	האיחוד האירופי	ארה"ב	ישראל
פקס	✓	✓	✓
מערכות חיוג אוטומטיות	✓[64]	✓	✓
מסרונים בטלפון	✓	✓	✓
דוא"ל	✓	✓	✓
צ'אטים ברשת חברתית	אין התייחסות מפורשת	התייחסות בפסיקה[65]	
מסרונים ברשת חברתית	אין התייחסות מפורשת	אין התייחסות מפורשת	התייחסות בפסיקה (כאל הודעה אלקטרונית, ולא הודעת מסר קצר)[66]
שיחות טלפון אנושיות	לפי שיקול דעת של כל מדינה ומדינה[67]	יש התייחסות אך ללא הסדרים מפורשים[68]	✗

61 הדירקטיבה האירופית מציינת כך: "unsolicited communications for direct marketing purposes in particular by means of au-tomated calling machines, telefaxes, and e-mails, including SMS messages". ראו: Directive 2002/58/EC Directive on Privacy and Electronic Communications of 12, July 2002, Official Journal of 31 July 2002, L 201, page 37: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&qid=1688385791762.

62 Controlling the Assault of Non-Solicited Pornography and Marketing Act, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§7701-7713 (2003)), §14(a).

63 ראו למשל: Krishna Jayakar, *Can We Can Spam? A Comparison of National Spam Regulations.* A Comparison of National Spam Regulations). TPRC 41, 12-13 (August 15, 2013).

64 נראה שהנוסח של ס' 40 לדירקטיבה, "unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS message", מאפשר פרשנות רחבה של מערכת חיוג אוטומטית.

65 המונח e-mail פורש בפסיקה כך שיכלול גם הודעות ברשתות חברתיות (myspace). ראו: MySpace, Inc. v. The Globe.com, Inc., 2007 WL 1686966 (C.D. Cal., 2007).

66 ראו לדוגמה לעיל בה"ש 25.

67 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), §42.

68 ה-TCPA מתייחס לאפשרות של שיחות מאוישות, תחת המונח "telephone solicitation". הוא אינו קובע הסדרים מפורשים, אבל מורה על הסדרה עתידית של הנושא, כולל אפשרות של הקמת מאגר מידע ובו מספרים של נושאי מידע שאינם מעוניינים לקבל שיחות טלמרקטינג (Telephone Consumer Protection Act, 47 U.S.C. § 227(c) (2011)).

הגדרות החוק

לעניין המסרים: גם כאן, יש דמיון ניכר בין הגדרת ספאם בחוק הישראלי להגדרתו בדירקטיבה האירופית, כאשר שתי ההגדרות רחבות מאשר ההגדרות בחוק האמריקני.[69] את הגדרת הדין הישראלי ל"דבר פרסומת" ראינו לעיל; הדין האירופי מתייחס ל-"unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages".[70] ההגדרה רחבה, בדומה לחוק הישראלי. לעומת זאת, בחוק האמריקני ההגדרה ב-TCPA היא "unsolicited advertisement to a telephone facsimile machine.", ובחוק עצמו לא מופיעה המילה "ספאם". הגדרה זו הורחבה כאמור וכוללת גם שליחת מסרונים. לגבי דואר אלקטרוני, ההגדרה האמריקנית היא "unsolicited commercial electronic mail" ונכללים בה הודעות דוא"ל בעלי תוכן שיווקי, שנשלחו מבלי שניתנה הסכמה מראש, או שהנמען לא היה מוכן שישתפו את כתובת הדוא"ל שלו.

טבלה ג.2: הגדרת הספאם בחוק: המסר

	האיחוד האירופי	ארה"ב	ישראל
הגדרת הספאם: מסר	unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages	**דוא"ל:** unsolicited commercial electronic mail. מיילים שנשלחו ללא הסכמה לפני שליחתם, או שהנמען לא היה מוכן שישתפו את כתובת המייל שלו. **טלפון:** unsolicited advertisement to a telephone facsimile machine. בחוק עצמו לא מופיעה המילה ספאם. ההגדרה הורחבה גם לשליחת מסרונים.	"דבר פרסומת" - מסר מסחרי שנועד לעודד רכישה של מוצר, כולל תעמולה ותרומה (מסרים פוליטיים – לא יחשבו כתעמולה). גם מסר המופץ באופן רחב, הכולל בתוכו הצעה להתקשר למספר טלפון לשם קבלת מסר ייחשב כ"דבר פרסומת".

לעניין שולח המסר: גם כאן, יש דמיון גדול בין ההגדרות הישראלית והאירופית. החוק הישראלי מגדיר "מפרסם" כמי שנהנה מהפרסום, המשווק, מי שכתובתו מופיעה במען.[71] החוק מחריג את חברות הפצה לפי רישיון בזק, ואת המדינה ומוסדותיה.[72] בחוק האירופי, מי שנושא באחריות הוא מי שהמסר נשלח עבורו, כלומר מי שייהנה מפירות הפרסום.[73] לעומת זאת, ה-TCPA האמריקני אינו מגדיר במפורש מיהו מפרסם או שולח, ומאפשר להטיל אחריות על חברות שמתירות לצדדים שלישיים לשלוח מסרים בשמן.[74] החוק שנוגע לדוא"ל חל על שני גורמים: על מי שנהנה מפירות הפרסום, ועל שולח המסר.[75] במקרה זה, דווקא החוק האמריקני ער לבעייתיות שבהפרדה בין מי שמפרסם את עסקו

69 למעשה, גם החוק האמריקני וגם האירופי אינם מגדירים "מסר" כפי שעושה החוק הישראלי. עם זאת, התחולה של ההגדרה האירופית רחבה מזו האמריקנית, וזאת בדומה לחוק הישראלי.

70 דירקטיבה EC/2002/58, לעיל ה"ש 67, בס' 40.

71 ס' 30א(א) לחוק התקשורת.

72 ס' 30א(א) לחוק התקשורת.

73 הדירקטיבה אוסרת משלוח דברי פרסומת תוך הסתרת הגורם שיזם את המשלוח, ראו דירקטיבה EC/2002/58, לעיל ה"ש 67, ס' 13(4).

74 ראו במדריך למשתמש של החוק בס' 3 של ה"dos": https://www.mondaq.com/advicecentre/content/2158/The-Dos-and-Donts-of-TCPA-Lawsuit-Defense.

75 "'sender', when used with respect to a commercial electronic mail message, means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message." ראו:

למי שמפיץ בפועל את המסר עבורו, מבטל אותה, ומתייחס לכל חוליות ההפצה בשרשרת הספאם באופן אחיד.[76] נראה שהדין האמריקני בחר דרך שעשויה להתמודד עם חלק מהקשיים שציינו בעניין החרגת חברות התקשורת מאחריות.

טבלה ג.3: הגדרת הספאם בחוק: שולח המסר

	האיחוד האירופי	**ארה"ב**	**ישראל**
הגדרת הספאם: שולח המסר	מי שייהנה מפירות הפרסום	**דוא"ל:** מי ששלח את המסר בפועל, ומי שייהנה מפירות הפרסום **טלפון:** אין הגדרה חד משמעית; אפשר להטיל אחריות על חברות המאפשרות לשלוח מסרים בשמן	מי שנהנה מהפרסום, המשווק, מי שכתובתו מופיעה במען, למעט חברות הפצה ברישיון והמדינה

<u>מודל ההסכמה</u>

כמו המודל האירופי, גם המודל הישראלי להסכמה לעניין קבלת דואר שיווקי הוא מודל של opt-in: יש להסכים מראש באופן מפורש (בכתב) לקבלת דברי פרסומת.[77] החריגים המרכזיים הם משלוח כחלק ממערכת יחסים עסקית בין המפרסם לנמען כאשר הפרסומת קשורה למערכת היחסים; פנייה חד-פעמית לבית עסק; וכן פניה חד-פעמית לקבלת תרומה או תעמולה. המודל האירופי אף הוא דורש את הסכמתו המפורשת של הנמען מראש לקבלת מסרים שיווקיים,[78] כאשר החוק האירופי מפורש יותר בנוגע לדרכים למתן הסכמה, למשל, החוק מזכיר במפורש שסימון אקטיבי של תיבת בחירה באתר אינטרנט היא הסכמה מספקת.[79] מכך יוצא, שבלי סימון כזה של המשתמש, אין הסכמה למשלוח הודעות.

לעומת זאת, מודל ההסכמה בחוק הדוא"ל האמריקני הוא opt-out, אולם החוק מפרט תנאים שנדרשים על מנת שמסר שיווקי לא ייחשב לספאם.[80] בנוגע ל-TCPA, מלשון החוק עולה כי נדרשת הסכמה מראש לפני ביצוע כל שליחת פקס או ביצוע שיחה אוטומטית או מוקלטת.[81] אולם בפועל המצב מורכב בהרבה, משום שהדרישות משתנות בהתאם

Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 3(16).

76 ראו אצל ג'איאקר, לעיל ה"ש 63, בעמ' 19.

77 ס' 30א(ב) לחוק התקשורת.

78 "For such forms of unsolicited communication for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them." ראו: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), §40.

79 "Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website", שם, בס' 17.

80 התנאים הם: 1. אין להשתמש במידע שקרי או מטעה בכותרת. מידע ה"from", "to", "to reply", מידע הניתוב, שם הדומיין וכתובת הדואר האלקטרוני חייבים להיות מדויקים ולזהות את האדם או העסק שיזמו את ההודעה; 2. אין להשתמש בכותרות מטעות. שורת הנושא חייבת לשקף במדויק את תוכן ההודעה; 3. יש לחשוף בצורה ברורה ובולטת שהמסר הוא פרסומת; 4. על ההודעה לכלול את כתובת הדואר הפיזית של השולח; 5. יש לכלול באופן בולט וברור כיצד ניתן לבטל הסכמה לקבלת דוא"ל מהשולח בעתיד (out-opt); 6. אסור לשלוח לאדם דוא"ל אם ביטל את הסכמתו. יש לכבד את בקשת הביטול של נמען בתוך 10 ימי עסקים. לא ניתן לגבות עמלה על הביטול, או לדרוש מהנמען למסור מידע אישי מזהה מעבר לכתובת הדוא"ל שלו. לא ניתן למכור כתובת דוא"ל, אפילו בצורה של רשימת תפוצה; 7. החוק מבהיר שהעסקת חברה אחרת שתטפל בשיווק הדוא"ל, אינה מסירה אחריות משפטית מהמפרסם. הן החברה שהמוצר שלה מקודם בהודעה והן החברה ששולחת את ההודעה בפועל עשויות לשאת באחריות משפטית. על כך ראו במדריך לעסקים כיצד לעמוד בחוק הספאם, אותו פרסם ה-FTC: https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business.

81 "It shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States— to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party)." ראו: 47 U.S.C. § 227(b)(1).

לאמצעים השונים, וכן, קיומו של מאגר "אל תתקשר אליי", המכיל רישום מרוכז של סרבני ספאם לצד מספרי הטלפון והדוא"ל שלהם, ונועד לתת מענה לעסקים ולחברות, מתאים דווקא למודל הסכמה של opt-out.

ביקורת רבה על השיטה האמריקנית נשמעה במהלך הדיונים לקראת חוק הספאם הישראלי, שבחר בסופו של דבר במודל הסכמה ברוח האירופית ולא האמריקנית. עם זאת, לאחרונה הוקם בישראל מאגר דומה,[82] בו נדון בהרחבה בפרק הבא העוסק בטכנולוגיות ספאם.

לעניין ההשוואה, בקנדה הושקה בספטמבר 2008 רשימת 'אל תתקשר אליי'. חודש לאחר מכן מסרו ארגוני צרכנות בקנדה כי מצב הנרשמים למאגר גרוע משהיה קודם להרשמה, שכן הם מקבלים שיחות פרסומיות רבות מכפי שקיבלו בטרם נרשמו, כנראה בשל דליפת תוכן המאגר.[83] במאי 2023 הגישו התובעים הכלליים של 48 מדינות בארצות הברית ומחוז קולומביה תביעת ענק נגד חברת Avid Telecom, המספקת שירותי VOIP (Voice Over Internet Protocol) בטענה שאפשרה לקיים שיחות למספרים שנמצאים במרשם ה"אל תתקשר אליי" האמריקני.[84] התובעים טוענים שבתקופה שבין דצמבר 2018 לינואר 2023 החברה אפשרה לקיים יותר מ-24.5 מיליארד שיחות קצרות למספרים אלה, תוך התעלמות מ-329 התראות בנידון. עוד נטען שהחברה מכרה מספרי טלפון, נתונים ותוכנות חיוג שאפשרו ללקוחותיה לבצע שיחות אוטומטיות בהיקפים עצומים. באמצעות השירות, לקוחותיה יכלו לזייף את אזורי החיוג של שיחותיהם כדי להתאים לקהל היעד אליו כיוונו. השיחות כללו לכאורה הונאות של, בין השאר, ביטוח לאומי, שירותים רפואיים, או שירותי ריבית בכרטיסי אשראי.[85] במועד זה, התביעה תלויה ועומדת.

<u>אכיפה</u>

העיקרון של הפרטת האכיפה מנחה גם את ה-TCPA האמריקני, שעוצב מלכתחילה באופן המסתמך על אכיפה בידי יחידים.[86] יחידים יכולים לתבוע ולקבל פיצויי של 500 דולר לכל הפרה או בגובה של ההפסד הכספי, לפי הגבוה מהחלופות. במקרה שהמפר הפיץ ספאם מרצון ותוך ידיעה, ניתן לפצות את הנפגע בסכום של עד 1500 דולר.[87] בחוק הישראלי, התובע יכול להיות אדם פרטי או המדינה, וכן ניתן לתבוע בדרך של תובענות ייצוגיות. ב-TCPA האמריקני, התובע יכול להיות אדם פרטי, או פרקליט המדינה שאף הוא יכול להגיש תביעה במקרה שהוא מזהה הפרות חוזרות (מפר סידרתי). בנוסף, לרשות הסחר הפדרלית, ה-FTC, יש סמכות לאכוף קנסות כספיים נגד אנשים פרטיים וישויות. לעומת זאת, בחוק הדוא"ל האמריקני אנשים פרטיים לא יכולים לתבוע, והסמכות לתביעה נתונה לשני גורמים: לפרקליט המדינה ול-FTC. פרט לשני הגורמים הללו הגורם הפרטי היחיד שיכול לתבוע הוא ה-Internet Access Service (IAP). בעשור האחרון קיימת מגמת הרחבה לעניין הגורמים הפרטיים שיוכלו לתבוע.[88] האכיפה באירופה אינה אחידה, והיא משתנה ממדינה למדינה. הדירקטיבה האירופית מורה לכל מדינה לקבוע בחקיקה מה תהיינה התרופות המשפטיות במקרה של הפרה.[89]

82 על כך, ראו למשל: אור כהן "ההרשמה למאגר 'אל תתקשר אליי' נפתחה; חשש מניצול לרעה" **הפורטל המשפטי לאינטרנט, סייבר וטכנולוגיית מידע** (14.12.2022): https://www.law.co.il/news/2022/12/14/registration-do-not-call-me-database-opened-fear-of-abuse/.

83 ראו טל קפלן "קנדה: רשימת 'אל תתקשרו אליי' מזיקה יותר ממועילה" **הפורטל המשפטי לאינטרנט, סייבר וטכנולוגיית מידע** (22.1.2009): https://www.law.co.il/news/2009/01/22/canadian-do-not-call-list-made-situation-worse.

84 לכתב התביעה, ראו: https://oag.dc.gov/sites/default/files/2023-05/COMPLAINT_49%20AGs%20v%20Lansky%20dba%20Avid%20et%20al%20%281%29.pdf.

85 ראו אור כהן "ארה"ב: תביעת ענק בגין שיחות ספאם", **הפורטל המשפטי לאינטרנט, סייבר וטכנולוגיית מידע** (28.5.2023), לקריאה: https://www.law.co.il/news/2023/05/28/usa-lawsuit-against-a-telecom-company-for-spam-calls.

86 על כך, ראו בהרחבה אצל וולה, היידטקה וסטיוארט, לעיל ה"ש 59, בעמ' 358.

87 Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3) (2011).

88 ראו למשל אצל ג'יאיקר, לעיל ה"ש 63, בתת הפרק 4.6.

89 דירקטיבה EC/2002/58, לעיל ה"ש 67, ס' 47.

טבלה ג.4: אכיפה

	האיחוד האירופי	**ארה”ב**	**ישראל**
אכיפה	משתנה ממדינה למדינה	**דוא"ל:** רק פרקליט המדינה או ה-FTC יכולים לתבוע **טלפון:** בנוסף, גם יחידים יכולים לתבוע	הפרטת אכיפה; התובע יכול להיות אדם פרטי, המדינה + תובענות ייצוגיות

5. ניתוח: הישגים, כשלים ופתרונות

חקיקת הספאם במדינות השונות, ובכלל בישראל, נועדה לצמצם את תופעת הספאם בדרך של הפרטת האכיפה. החוק ביקש להקל על נפגעי הספאם בכך שפתח עבורם אפיק מרכזי של הגשת תביעות בהליכים פשוטים וזולים, וכן אפשרות נוספת של הגשת תובענה ייצוגית. ואכן, לפחות לתקופות מסוימות נראה שהיקף התופעה הצטמצם, יש להניח שבין השאר בשל החוק, וכן שהפסיקה בענייני ספאם הביאה לסגירה של חלק מהעסקים שעסקו באופן סדרתי בשליחת מסרים באופן לא חוקי. גם ההנחיות החדשות של משרד התקשורת משנת 2023 מתמודדות עם בעיית המסרונים הנשלחים על ידי חברות ההפצה, ואף אם עדיין קשה לאמוד את מידת הצלחתן בשטח, נראה שהמגמה הכללית חיובית.

עם זאת, וכפי שעלה גם מהניתוח בפרק ב, ריבוי השחקנים והאינטרסים הסותרים שלהם בזירת הספאם, הציבו אתגרים שונים. בפרק הקודם הצגנו את השחקנים השונים בשרשרת הספאם, ובפרק זה את הניתוח המשפטי. כעת, אפשר להקביל ביניהם:

תרשים ג.2: שחקנים בשרשרת הערך – מצב משפטי

בעלי המסר

↓

גורמים מסייעים *לפני* ההפצה

ספק לִידִים | בעל מאגר מידע

↓

גורמים מסייעים *בשלב* ההפצה

רשתות שותפים | חברות הפצה | חברות התקשורת

↓

נמענים

”מפרסם“

החוק חל על מי שנהנה מפירות הפרסום, ומי ששמו מופיע בדבר הפרסומת. בעלי המסר נושאים באחריות משפטית להפצת ספאם

מסייעים לפני הפצה

כמי שנהנים מפירות הפרסום, החוק חל גם ספקי לידים וגם על בעלי מאגרים. עם זאת, מעשית קשה לזהות את מקור מאגרי המידע המשמשים לשליחת ספאם, ואת ספקי הלידים.

מסייעים בשלב ההפצה

החוק מחריג את חברות התקשורת ברישיון בזק מאחריות על שליחת ספאם; חברות ההפצה האחרות לא נהנות תמיד מהפטור.

נמענים

מוגנים בחוק מפני "דבר פרסומת" שנשלח אליהם ללא הסכמתם המפורשת, מראש ובכתב. הנמען יכול לבקש סעד משפטי בכוחות עצמו

דיון זה חושף את הנקודות החלשות בשרשרת הספאם, ומזמין הסדרה שלהן. אחד האתגרים המרכזיים נוגע ליכולת ההתמודדות עם ספקיות התקשורת ועם שאלת אחריותן להפצת ספאם, שכן ספקיות התקשורת הן שחקן מרכזי בזירה, שמשרת שחקנים בעלי אינטרסים סותרים. בעניין זה כאמור, הונחה הצעת חוק על שולחן הכנסת.[90] אולם, פרדיגמת המחקר של משפט וטכנולוגיה שאותה הצגנו בפרק המבוא, מלמדת אותנו שהמשפט אינו בהכרח הפתרון היחיד או הראשון במעלה. בצד המשפט, יש גורמים מאסדרים אפשריים נוספים: נורמות חברתיות, נורמות שוק, והטכנולוגיה.

הנורמות החברתיות מתאימות פחות להסדרת יחסים בין גורמים מסחריים לבין צרכנים. הנורמות שחלות במרחב הזה הן נורמות שוק שונות. הנורמות הכלכליות משולבות בנורמות המשפטיות. כפי שראינו, לספאם יש הגיון כלכלי משלו, והכללים המשפטיים מנסים לעקוב אחרי הכללים האלה, לשבש את התמריצים של הספאמרים להפיץ דברי פרסו־מת לא רצויים, וליתן בידי הצרכנים תמריצים לתבוע, ולאכוף את הדין בעצמו. הכלי האחרון הוא הטכנולוגיה. מטבע הדברים, הטכנולוגיה היא זו שיוצרת את הבעיה מלכתחילה, בכך שהיא מאפשרת הפצה מהירה, זולה ופשוטה של הודעות, שלא כולן רצויות; והקושי הוא לבדל בין הודעה רצויה להודעה לא רצויה, וזאת, לאורך החוליות השונות של שרשרת הספאם. בהתאם, הפרק הבא בוחן את המרכיב הטכנולוגי.

סוגיות נוספות אותן נמנה בסמוך אף הן ממתינות לפתרון.

א. זהות המפר

חסם מרכזי מפני מימוש זכות התביעה הוא זיהוי המפר. למרות שחוק הספאם הישראלי מאפשר לנפגעים לתבוע את שולח הספאם, לנפגעים רבים אין כל דרך מעשית לברר את זהות השולח, ודאי כאשר מדובר בהפרות שבוצעו על ידי ספאמרים מקצועיים, וקל וחומר כאשר תכני המסרים אינם חוקיים. חברות רבות מערימות קשיים מכוונים על הנמענים ומקשות עליהם את האפשרות לזהות את מקור ההודעות המפרות. מעשית, עבור תובע פוטנציאלי, יש קושי גדול להגיש תביעה: ראשית יש לזהות חברת הפצה, להוכיח שאינה חברת תקשורת (שכאמור, מוחרגת מאחריות בדין הספאם הישראלי), להתריע בפניה, ואז יש "לתפוס" הודעה נוספת שנשלחת לאחר ההתראה.

עוד לעניין זהות המפרסם, הרי שבעוד שהחוק עוזר אולי להילחם ב"מפרסם המוסדר", לא כל הספאמרים הם תאגידים לגיטימיים, ויש גורמים עלומים ששולחים הודעות ספאם מבלי להזדהות, מבלי לתת אפשרות להסרה מרשימת התפוצה, ושהתחקות אחריהם מסובכת ביותר. גם כאשר מתקבל פסק דין נגדם, הסיכוי לקבלת הפיצוי קלוש. בנוסף, לא כל הספאמרים מגיעים מישראל, עניין שמקשה עוד יותר את מלאכת האיתור והאכיפה.

באשר לאפשרות זיהוי השולח והעלויות הנלוות לצורך הגשת תביעה – חברת "ספאם אוף" נתנה מענה לנפגעי ספאם רבים. דרך נוספת עשויה להימצא בהצעת החוק שהזכרנו לעניין חיוב חברות הפצה לחשוף שמות של לקוחות מפרים. מענה מסוג זה יצטרך להביא בחשבון את האתגר שבחשיפת שמות לקוחות. לדוגמה, חברה ששמה ייחשף למרות שלא הייתה אחראית להפצת ספאם, תוכל לתבוע את חברת ההפצה בגין לשון הרע.[91] פתרון אפשרי נוסף לבעיה זו עשוי להיות יצירת מנגנון פשוט להגשת תביעה לקבלת צו, כלומר של פניה לחברת הפצה או לספקית תקשורת כדי לקבל את נתוני השולח. כיום, רק למשטרה סמכות לעשות כך, או שיש לפנות לקבלת צו באמצעות בית המשפט.[92] בנוסף, החוק היום אינו מחייב את חברות התקשורת להפעיל מנגנוני סינון אוטומטיים שיזהו מבעוד מועד שולחי ספאם ויסננו אותם. מנגנונים מעין אלה אמנם קיימים בשירותי דוא"ל כמו Gmail, אך הבחירה להפעילם נתונה בידי מפעיל השירות. לגבי מסרונים, יש קושי טכנולוגי להשתמש במסננים אוטומטיים, כפי שנראה בפרק הבא, העוסק בטכנולוגיות ספאם.

ב. בעיית עלויות – התחשיב הכלכלי

חסם שני להגשת תביעות – למרות המספר הגבוה לכאורה של תביעות – הוא התחשיב הכלכלי של התביעה, והצד המשלים – היעדר הרתעה מספקת למפיצים שמפרים את החוק.

---

90 הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התשפ"ג-2022 (פ/25/276).

91 נעיר שלפי הדין הישראלי, לתאגידים אין זכות לפרטיות, כך שעילת התביעה שעומדת לתאגיד ששמו שורבב באופן שגוי לפרסום היא עילת לשון הרע, שכן עומדת לתאגידים. לעניין היעדר הגנת הפרטיות לתאגידים, ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 126-132 (2023). לזכות התביעה של תאגיד במקרה של פגיעה בשמו הטוב, ראו ס' 4 לחוק איסור לשון הרע, התשכ"ה-1965.

92 חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007.

הפרטת האכיפה האזרחית והפיצוי הסטטוטורי, שנועדו להפוך את התביעה לקלה יותר ואת שליחת הספאם ללא משתלמת – אינם מספקים פתרון לבעיה באותם המקרים, שאינם מעטים, בהם התחשיב הכלכלי עדיין משתלם למפיצי ספאם ולספקי לידים. ראשית, סכום הפיצוי בתביעה קטנה (1000 ש"ח) נותר כשהיה במהלך חמש עשרה השנים האחרונות, ולא הוצמד למדד המחירים. הדבר מביא להרתעת חסר של שולחי הספאם, ביחס למה שסבר המחוקק כהרתעה יעילה בעת החקיקה.

בנוסף, בהתאם להלכת **חזני**, לבית המשפט שיקול דעת בקביעת הפיצוי, והכלל שהתקבע הוא שבית המשפט לא יפסוק פיצויים בסכום העולה על הסכום המגלם הרתעה אופטימלית. בית המשפט ציין שייתכן שאדם אליו נשלחו 1000 הודעות יקבל פיצוי שווה לאדם אליו נשלחו 100 הודעות, כך שאף אם תקרת הפיצוי האפשרי עלתה יש לעצור בסכום המהווה הרתעה אופטימלית.[93] משכך, ריבוי הודעות ספאם לא מבטיח בהכרח שהנפגע יפוצה באופן שיהווה תמריץ להגשת תביעה.

כמו כן, משיחות שערכנו עם שחקנים בזירה המשפטית עולה שכאשר בית המשפט דורש מחברות ההפצה לחשוף פרטי תקשורת, הן דורשות לעיתים קרובות תשלום גבוה עבור התהליך – כלומר מבקשות תשלום עבור כל פריט מידע שמבקשים מהן לגלות - בטענה שהדבר כרוך בניתוח מסובך.[94] בכך חברות הפצה מייצרות עלויות משמעותיות עבור תובעים, בעיקר כאשר מדובר באזרח מן השורה ולא בבעל עסק. במקרה שהעלות של בירור הנתונים הנדרשים לשם הגשת התביעה היא גבוהה, התמריץ הכלכלי להגשת תביעה, שהוא הפיצוי בגובה 1000 ש"ח, עשוי להיפגע.

ג. אוריינות טכנולוגית ומשפטית

חסם שלישי מפני הגשת תביעות בקשר לספאם הוא היעדר אוריינות טכנולוגית ומשפטית מתאימה. כאשר מבקשים מהציבור להיות אוכף החוק, כלומר במקרה של אכיפה אזרחית – הציבור זקוק לכלים מתאימים. לא כולם מומחים מתוחכמים למחשוב, ואוריינות טכנולוגית נחוצה במקרים רבים, כאשר מקור הספאם, אופן שליחתו, והדרך לאיתור המקור, אינם מובנים מאליהם. בנוסף, אוריינות משפטית אף היא חיונית כאשר מדובר באכיפה על ידי יחידים. לדוגמה, העובדה שחברה היא נתבעת סדרתית אין משמעה שהחברה פועלת באופן לא לגיטימי; מדוח איגוד האינטרנט עולה גם שיש חברות שהן אמנם נתבעות סדרתיות, אך בתי המשפט מוצאים אותן חייבות לעיתים רחוקות.[95] השערת מחברי הדוח היא כי "ישנם מקרים שבהם קיים בציבור **פער ידע ביחס להגדרת הודעת ספאם**, מה שגורם לבזבוז משאבי תביעה במקרים ללא עילה."[96]

לפי דוח האיגוד, נראה כי לבתי משפט השלום במרכז הארץ מוגשות תביעות רבות יותר בנושאי ספאם, לעומת בתי המשפט בצפון הארץ ובדרומה.[97] קשה לקבוע בוודאות האם הסיבה לכך היא מודעות גבוהה יותר של אזרחים באזורי המרכז לנושא הספאם, יכולת גבוהה יותר להשתמש בכלים משפטיים והבנת ההליכים, או שמדובר באוכלוסייה שכלפיה מבוצעות עבירות רבות יותר.[98] כך או כך, אנו סבורים שהדבר מעיד על הצורך בהסברה משופרת, הן בעניין הספאם לגופו, והן בעניין המנגנונים המשפטיים העומדים לרשות האזרח הנפגע. הפקדת מנגנון האכיפה בידי האזרח אינה שלמה מבלי שיינתנו בידיו הכלים המתאימים להשתמש בו כהלכה.[99]

93 ראו עניין **חזני**, לעיל ה"ש 31, בפס' 10.

94 ראו למשל את הודעתה של חברת טלזר בתיק ת"צ 47554-07-20 מיום 28.2.2022, שם ציינה החברה כי היא גובה תשלום של 250 ₪ על מסירת פרטי הודעה אחת, ובמקרה זה, בו נתבקשה למסור נתונים בנוגע לחמישה מספרים לאורך תקופה, היא דורשת סכום של 8000 ₪ תמורת המידע. בהמשך, עבור רשימת מספרי הטלפון אליהם נשלחו ההודעות, ביקשה טלזר סכום של 10,000 ₪. ראו תגובת טלזר לבקשה למתן צו להשלמת נתונים, ת"צ 47554-07-20 מיום 4.6.2023.

95 עמ' 31-32. הדוגמאות בדוח הן "למשל רק 1% מ- 216 התביעות שהוגשו נגד משרד הפנים נמצאו מוצדקות ורק 2% מתוך 135 התביעות שהוגשו נגד חברת "גלוגובר" נמצאו מוצדקות".

96 שם.

97 ראו דוח האיגוד האינטרנט, לעיל ה"ש 9, בפרק "ממצאים ודיון", תת הפרק "היקף תביעות הספאם והטיפול בהן".

98 שם.

99 ארגוני חברה אזרחית כמו למשל עמותת אל ספאם פועלים לקידום ההבנה בענייני ספאם, הן הטכנולוגית והן המשפטית, באמצעות מאמצי הסברה. ראו למשל את סדרת סרטוני בהדרכה בעניין ספאם לתובעים שהפיקה העמותה: https://www.youtube.com/watch?v=7ZAN-JGUaWOE&t=27s.

ד. עוינות מצד המערכת המשפטית

חסם רביעי למימוש זכות התביעה הוא עמדה עוינת מצד חלק מבתי המשפט שעסקו בספאם. עורכי דין פעילים בתחום הספאם הצביעו על עוינות מסוימת מצד חלק מהמערכת המשפטית לתביעות ספאם, המתבטאת באופנים שונים. כך למשל, לדברי עורכי הדין עימם שוחחנו, יש שופטים שמזלזלים בראיות להוכחת הסכמה לקבלת פרסומת, כאלה הדוחים תביעות מוצדקות תוך חיוב בהוצאות, מה שמרתיע תובעים עתידיים, ובעיקר שופטים שאינם מתייחסים להכרעה כפיצוי ללא הוכחת נזק אלא "מנסים ללכת אימים על הנמען ולהטיל ספק בתום ליבו ושוכחים שהוא הנפגע".[100]

פרשת "ספאם אוף" היא תזכורת לכך שאהדת המערכת המשפטית לסוגיה נחוצה לשם הצלחת החוק. נראה שהחברה הקדימה את זמנה בשימוש בכלים אוטומטיים בהליכים משפטיים. יש להניח שכיום כלים כאלה זמינים עוד יותר.

ה. תחולה צרה של החוק מבחינת הגדרת "דבר פרסומת" והגדרת "מפרסם"

קושי אחרון הוא תחולתו של החוק, והתאמת הגדרותיו למצב העניינים בפועל. ראשית, החוק אינו חל על ספאם פוליטי ועל כן אינו מטפל בכל המטרדים בפועל. לפי החוק, תוכן "אידיאולוגי" יכול להישלח אלינו בכל עת ובאין מפריע. כמובן, כפי שציינו לעיל, למסרים פוליטיים יש פן משמעותי של חופש הביטוי הפוליטי, ופן מסחרי מופחת. בנוסף, החוק אינו חל על שיחות טלפון אנושיות, שבמקרים רבים הפכו למטרד של ממש, כאשר מבול של טלפנים אנושיים עוסקים בהפצת אותו מסר שיווקי לרשימות ארוכות של נמענים שלא הסכימו לכך – יש לשאול האם מדובר בספאם לכל דבר ועניין.[101]

6. סיכום

הדיון בפרק זה הציג את ההסדר המשפטי הנוכחי בישראל בקשר לספאם, על תיקוניו לאורך השנים. ההסדר מרחיב מבחינת סוגי הטכנולוגיות שאליהן הוא מתייחס, מנסה לבדל בין מסרים פרסומיים למסרים שאינם כאלה כמו מסרים פוליטיים, ומטיל אחריות בעיקר על מועני המסר, תוך שהוא מחריג את מי שעוסק בהפצת מסרים. מנגנון האכיפה העיקרי הוא של הפרטת האכיפה, כלומר מתן אפשרות ליחידים שנפגעים לתבוע בעצמם. החוק מאפשר פיצוי סטטוטורי, ובצידו, אפיק של תובענה ייצוגית. ואכן, לאורך השנים הוגשו עשרות אלפי תביעות קטנות וכמה מאות תביעות בסדר דין מקוצר, וכן מאות אחדות של בקשות לאישור תובענה ייצוגית.

עם זאת, ההסדר הקיים מצליח להתמודד רק עם חלק מהסוגיות. מצד אחד, ההסדר נותן כלי משפטי אפקטיבי למדי בידי הנפגעים מול בעלי עסקים לגיטימיים שמשווקים את עסקיהם. מצד שני, עדיין מתעוררים קשיים ואתגרים ניכרים, ויש חסמים לא מעטים בפני מימוש זכות התביעה. הדיון מצביע על החסמים הבאים כאתגרים עיקריים:

- התמודדות עם ספקיות התקשורת ועם שאלת אחריותן להפצת ספאם, על רקע העובדה שספקיות משרתות שחקנים בעלי אינטרסים סותרים. כרגע הן נהנות מחסינות בקשר להפצה, בשל אי-ידיעתן על התכנים המועברים וחוקיותם;
- קושי בזיהוי ואיתור גורמים מפרים, שמוביל לשימוש-חסר בכלים משפטיים;
- חסמים כלכליים מתביעה, בשל מורכבותה, עלויות קשורות, וזאת מול תמריצים כלכליים יעילים של שולחי הספאם;
- שונות במידת האוריינות המשפטית והטכנולוגית של נפגעים;

100 לילך דניאל "עשור לחוק הספאם: האם החוק היה הצלחה או כישלון ומה צופה העתיד?" **תקדין** (13.12.2018): https://portal.takdin.co.il/Article/Article/6169706. עורכי הדין שהתראיינו לכתבה היו דורון תמיר, עמית זילברג ואופיר לב.

101 עם זאת, שיחות כאלה עשויות להיות בגדר "דיוור ישיר", ובכל מקרה, ככל שהן מבוססות על מאגר מידע כהגדרתו בחוק הגנת הפרטיות, הגורם המתקשר צריך לעמוד בדרישות החוק – רישום מאגר המידע כחוק (ס' 8 לחוק), הודעה מתאימה לאדם בדבר איסוף מידע (ס' 11), וכדומה. לנמען יש זכות לדרוש גישה למידע שמוחזק במאגר מידע (ס' 13), אך כיום, אין זכות מלאה לדרוש את מחיקת הרישום (למעט כאשר המידע שגוי, ס' 14).

- עוינות מסוימת מצד חלק מהמערכת המשפטית לתביעות ספאם;
- תחולה צרה מדי של החוק לעניין הגדרת "מפרסם" ו"דבר פרסומת".

מהדיון בפרק זה עולות כמה מסקנות ביניים:

- לספאם יש הגיון כלכלי משלו. את הכללים המשפטיים יש לעצב כך שיעקבו אחרי ההיגיון הכלכלי של מערכת הספאם, ויפצחו אותו.
- ההסדר המשפטי המפורט בנוגע לספאם מספק כלי משפטי אפקטיבי למדי בידי הנפגעים מול משווקים לגיטימיים; אך למרות זאת קיימים חסמים בפני תביעה, ואתגרים ניכרים. כלים אלה אפקטיביים פחות מול משווקים לא לגיטימיים, כלומר מי שמציעים תכנים או שירותים לא חוקיים.
- האתגרים המשפטיים העיקריים כיום הם שאלת אחריות ספקיות תקשורת להפצת ספאם; חסמים מפני תביעה של קושי בזיהוי ואיתור גורמים מפרים; עלויות התביעה מול תמריצים כלכליים יעילים של המפרים; שונות באוריינות משפטית וטכנולוגית מצד הנפגעים; עוינות מסוימת מצד המערכת המשפטית לתביעות ספאם; ותחולה צרה מדי של החוק לעניין הגדרת "מפרסם" ו"דבר פרסומת".

פרק ד
טכנולוגיות אנטי-ספאם

1. **מבוא: מרוץ חימוש אינסופי** **65**
2. **טכנולוגיות מרכזיות בשימוש** **66**
   א. ספאם ואנטי ספאם בדוא"ל 67
   ב. ספאם ואנטי ספאם בהודעות טקסט למכשירי הטלפון 70
   ג. ספאם ואנטי ספאם בהודעות קוליות 71
   ד. ספאם ואנטי ספאם בפלטפורמות חברתיות 75
   ה. פתרונות טכנולוגיים: הדור הבא 76
3. **סיכום** **77**

1. מבוא: מרוץ חימוש אינסופי

בפרקים הקודמים תיארנו היבטים כלכליים ומשפטיים של ספאם. אולם, ספאם הוא גם תופעה טכנולוגית. השחקנים השונים שמעורבים בשרשרת הערך של הספאם אותם הצגנו בפרק ב, משתמשים בכלים, בתשתיות ובפרקטיקות טכנולוגיות על מנת להוציא לפועל את מבוקשם, שהוא ייצור והפצת מסרים שיווקיים – שחלקם הוא בגדר ספאם. גם נמעני הספאם נחשפים אליו כחלק מהשימוש היומיומי שלהם בכלים ובפרקטיקות טכנולוגיות. בפרק הקודם בחנו וניתחנו את המנגנונים והכלים **המשפטיים** שמנסים למגר את תופעת הספאם. פרק זה סוקר ומנתח את מנגנוני האכיפה **הטכנולוגיים** המרכזיים בתחום הספאם, ומתאר את מרוץ החימוש האינסופי במאבק בין טכנולוגיות ספאם וטכנולוגיות אנטי-ספאם.

בשנת 2006 כתב ברוס שנאייר (Schneier), קריפטוגרף ומומחה אבטחת-מידע מוביל, את הדברים הבאים בנוגע לתופעת הספאם: "הדרך הטובה ביותר לחשוב על זה היא מרוץ חימוש. מוצרי אנטי-ספאם חוסמים סוג מסוים של ספאם. ספאמרים ממציאים טקטיקה שעוקפת את המוצרים האלה. ואז, המוצרים חוסמים את הספאם הזה. ואז הספאמרים ממציאים סוג נוסף של ספאם. וכך הלאה."[1] Schneier תיאר למשל כיצד הכנסתם של אתרי ספאם לרשימות שחורות, שעל יצירתן נרחיב בהמשך הפרק, אילצה את הספאמרים להסוות את מקורו של הספאם, או כיצד סריקת מיליוני הודעות דוא"ל בחיפוש אחר ספאם המוני שמקורו זהה, אילצה ספאמרים להפוך כל הודעת ספאם לייחודית. בהמשך, בתגובה לזיהוי סמנטי של ספאם החלו ספאמרים להטמיע את ההודעות שלהם בתוך תמונות. כך, כל הגנה נתקלת בהתקפה נוספת, ומול כל התקפה חדשה מפתחים אמצעי הגנה נוספים, וכך הלאה.

מצד שני, ספאמרים מקצועיים חושבים על עיסוקם באופן דומה, כפי שמשתקף מספרו של ספאמר אנונימי שיצא לאור בשנת 2004: "הכל מרוץ נגד הזמן – ספאמרים מול קבוצות אנטי-ספאם. קבוצות אנטי-ספאם ימצאו דרך לחסום כל טכניקה לשליחת ספאם שספאמרים ממציאים. וספאמרים ימצאו דרך לעקוף כל טכניקה שקבוצות אנטי-ספאם יוצרות כדי לחסום ספאם... ספאמרים משתמשים באינטרנט בכמה מהדרכים היצירתיות והמדהימות ביותר; חשבו עלינו כעל המק'גאייבר של הסייברספייס."[2]

שני הצדדים מגיעים למסקנות דומות. כל צד מאמין שגם אם המלחמה היא אינסופית, הסטטוס קוו מעיד על סיפור הצלחה מצדו. כך מתאר זאת Schneier: "בכנות, אין סוף באופק הנראה לעין... אבל למרות זאת, ספאם הוא אחד מסיפורי ההצלחה של אבטחת מחשבים; מוצרי אנטי-ספאם נוכחיים עובדים די טוב. אני מקבל רק כמה הודעות ספאם ביום, ומעט מאוד הודעות דוא"ל לגיטימיות מגיעות לפח האשפה שלי."[3] בדומה לכך, כותב הספאמר האנונימי: "בסופו של דבר אף אחד לא באמת מנצח. כל כך הרבה ספאם נשלח מדי יום, וגם אם מסננים יחסמו 99 אחוזים ממנו, עדיין אחוז אחד של ספאם שיגיע ליעדו יספיק ליצירת מיליוני דולרים... ספאם הפך לגז חסר ריח וחסר טעם – בלתי ניתן לזיהוי, בלתי ניתן לאיתור, וחודר לכל סנטימטר בעולם המקושר בסייבר."[4]

בתווך נמצאים הנמענים, אנחנו, משתמשים רגילים של מערכות תקשורת. לא תמיד קל לשכנע אותנו באמונת אנשי האבטחה הרואים בפתרונות שלהם סיפור הצלחה, וגם לא באמונתם של הספאמרים, המשוכנעים שספאם הוא חלק בלתי נפרד ובלתי נמנע מחיי היומיום המקוונים שלנו. אחרי הכל, אנחנו לא רק מספרים, ואחוז אחד של ספאם "מוצלח" יכול לפגוע באנשים רבים. יתר על כן, כפי שנראה בפרק זה, בעוד שמרוץ החימוש סביב הספאם בדוא"ל אכן הגיע לסטטוס קוו בעת הזו, באפיקי ספאם נוספים, כמו שיחות טלפוניות או הודעות טקסט, המצב רחוק מלהיות מאוזן.

בהתאם, פרק זה בוחן ומנתח במשקפיים טכנולוגיים את שלושת אפיקי הספאם העיקריים שרלוונטיים למקרה הישראלי, שהם דוא"ל, מסרונים למכשירי הטלפון, ושיחות קוליות. נציג את האופן שבו פועלת טכנולוגית הספאם ואת הפתרונות הטכנולוגיים שמבקשים להגיב לספאם. נדגיש את ההשלכות והאתגרים המשפטיים של הטכנולוגיות השונות. בשינויים המתחייבים, הדיון ניתן ליישום לטכנולוגיות נוספות ולאפיקי ספאם נוספים אליהם נתייחס לשם

1 Bruce Schneier, *Why Spam Won't Go Away*, Forbes, (12.12.2006), נמצא ב: https://www.forbes.com/2006/12/11/spam-se-curity-email-tech-security-cz_bs_1212spam.html?sh=58fea4c54626.

2 Spammer-X, Inside the Spam Cartel: Trade Secrets from the Dark Side 30 (2004) (התרגום שלנו).

3 Schneier, לעיל ה"ש 1.

4 ספאמר X, לעיל ה"ש 2, בעמ' 30.

השוואה נקודתית לפי הצורך. במיוחד נציג את אפיק הספאם ברשתות חברתיות, שטרם זכה להתייחסות נפרדת בחוק הישראלי.[5] כמו כן, כאשר עוסקים בעיצוב מדיניות יש להביא בחשבון טכנולוגיות חדשות שטרם זכו להתייחסות מצד המחוקק וטרם נדונו בבתי המשפט, אך השפעתן כבר ניכרת, כמו השימוש בכלי בינה מלאכותית (Artificial Intelligence – AI), בהם משתמשים גם בטכנולוגיות ספאם וגם בטכנולוגיות אנטי-ספאם.

לאחר הסקירה והניתוח של הטכנולוגיות המרכזיות, נפנה לדיון וניתוח של פתרונות טכנולוגיים אפשריים נוספים, ונכין את הקרקע לפרק הבא, שיתכלל את הדיון.

2. טכנולוגיות מרכזיות בשימוש

הטכנולוגיות שנסקור וננתח בסמוך נחלקות בהתאם לאפיקי הספאם בהם מכיר החוק הישראלי במפורש: דוא"ל, הודעות טקסט, ושיחות קוליות.[6] נוסיף על אלה גם ספאם ברשתות חברתיות. מגוון טכנולוגיות האנטי-ספאם המרכזיות שנמצאות בשימוש נחלקות לקטגוריות רבות, וכאן אנחנו מתמקדים בקטגוריות הרלוונטיות ביותר להבנת הממשק שבין הטכנולוגיה למשפט. למרות שהטכנולוגיות שאותן נסקור וננתח בסמוך הן טכנולוגיות אנטי-ספאם, טכנולוגיות הספאם, כלומר הטכנולוגיות בהן משתמשים ספאמרים ושאותן מנסות לבלום טכנולוגיות האנטי-ספאם, יוזכרו בהתאמה במקומות הרלוונטיים. זאת בשל העובדה שמדובר במרוץ חימוש מתמשך, בו כל טכנולוגית אנטי-ספאם מאלצת ספאמרים לחפש דרכים לעקוף אותה, ואף למצוא אותן. נפתח בהשוואה הכללית, ולאחר מכן נפרט.

5 להתייחסות בפסיקה ראו רע"א 3599/18 **שפירא נ' עופרי** (נבו 30.5.2018); תא"מ (הרצ') 15909-04-16 **לב נ' ממון** (נבו 29.9.2017); ת"ק (ת"א) 32611-12-15 **רדזינר נ' סלקום ישראל בע"מ** (נבו 24.7.2016); תא"מ (רח') 32289-06-19 **ריטרסקי נ' קוד נדל"ן בע"מ** (נבו 14.7.2020).

6 לפי ס' 30א(ב) לחוק התקשורת (בזק ושידורים), התשמ"ב-(1982), שמגדיר: "לא ישגר מפרסם דבר פרסומת באמצעות פקסימיליה, מערכת חיוג אוטומטי, הודעה אלקטרונית או הודעת מסר קצר, בלא קבלת הסכמה מפורשת מראש של הנמען, בכתב, לרבות בהודעה אלקטרונית או בשיחה מוקלטת...".

טבלה ד.1 מאפיינים של טכנולוגיות אנטי-ספאם לפי אפיק המשלוח

אופי הסינון	דוא"ל	הודעות טקסט (SMS)	הודעות קוליות	מסרים ברשתות חברתיות
מבוסס מקור (נתוני התוכן)	במכשיר המשתמש או אצל ספק השירות	על ידי משתמשים (סינון תוכן שיתופי. תלוי בהשתתפות משתמשים) או אצל ספק השירות	במכשירי משתמשים: • יישומים לחסימת מספרים לא מזוהים או לא מוכרים • חסימה מובנית במכשיר עצמו אצל ספק השירות: שירות של זיהוי מתקשר הניתן להתאמה אישית	✕
מבוסס-תוכן	במכשיר המשתמש (דורשה אוריינות דיגיטלית) או אצל ספק השירות	במכשיר המשתמש או אצל ספק השירות. בשל מאפייני המדיום, סינון כזה אינו אפקטיבי כמו בדוא"ל (מגבלות טכניות כמו כוח עיבוד זמין, צורך במכשיר ידידותי לתוכנת הסינון, צורך באוריינות דיגיטלית)	לא קיים	✕
מסנני נפח		בשימוש חלקי, לא מספיק אפקטיבי	לא קיים	✕
רשימות שחורות או סינון על בסיס אופי המוען	אצל ספק השירות	אצל משתמשים (שיתופי) או אצל ספק השירות	יישומים שפועלים במכשירי משתמשים. מבוססים על סינון תוכן שיתופי	שימוש במאפיינים של משתמשים כגון מספר החברים, העוקבים, והתנהגות סביב הפרסום.
רשימות לבנות			שירות "אל תתקשר אלי"	✕

א. ספאם ואנטי ספאם בדוא"ל

ספאם בדוא"ל לא "מת". מדבריו של מנכ"ל חברת הפצה מקומית בשיחה איתנו, עולה ששיווק באמצעות דוא"ל הוא עדיין ערוץ רווחי מאוד, ורשימת לקוחות בדוא"ל היא נכס ממשי עבור חברות.[7] מסרים באמצעות דוא"ל אינם מידיים, ולפיכך פוטנציאל ההטרדה שלהם קטן מאשר הודעות טקסט ועוד פחות מאשר שיחות קוליות. לטענת אותו מנכ"ל, הרגולציה בתחום הדוא"ל סייעה דווקא להגדיל ולהרחיב את עסקיהן של חברות הפצה.

הפתרונות שהוצעו עד היום למלחמה בספאם בדוא"ל נחלקים לשלושה סוגים עיקריים. הראשון כולל פתרונות משפטיים, בעיקר של חקיקה ושל תביעות אזרחיות נגד ספאמרים. בכך דנו בפרק ג. השני, שבו נעסוק בפרק זה, הוא

7 שיחה שנערכה עם נאור מן ביום 1.6.2023.

סינון.[8] הסוג השלישי נוגע לשינויים בפרוטוקול הטכני, כלומר "פתרונות מבוססי תשתית":[9] למשל, שינוי האופן בה אנו נוהגים לשלוח דוא"ל באמצעות דרישת אימות מהשולח או תשלום מאומת. לכך נשוב בחלקו האחרון של פרק זה.

בעשורים האחרונים, מסנני דוא"ל הוכיחו את עצמם ככלי יעיל ביותר למניעת ספאם.[10] **מסנן ספאם** הוא כלי אוטומטי שבוחן דואר לפני העברתו לנמען, ומזהה דוא"ל זבל, כלומר ספאם. המסנן מתבסס על תוכן ההודעה, על מאפייני השולח, על "ידיעה" של הנמען, כלומר האם הנמען מחשיב הודעות דומות כספאם או את המוען כספאמר, ועוד. לשם כך משתמש המסנן בידע מובנה, באלגוריתמים שונים, במשובי משתמשים ובמשאבים חיצוניים כגון רשימות שחורות או דוחות ממשתמשים אחרים. מכיוון שלא קיים "ידע מושלם", יש צורך להגביל את המסנן למקורות מידע מוגדרים היטב.[11] מסננים כאלה מבוססים על עדכון רציף.

מסננים יכולים כאמור לבחון רכיבים שונים של הודעת דוא"ל. כך למשל, מסננים **מבוססי מקור** או כתובת משתמשים בדרך כלל בעל התוכן, כלומר בנתוני התוכן בלבד (מטא דאטה), כמו למשל כתובת IP, כתובת דוא"ל או כותרת דוא"ל, כדי לזהות ספאם.[12] לעומת זאת, מסננים **מבוססי תוכן** בוחנים, כשמם, את תוכנה של הודעת הדוא"ל.[13] התוצאה הרצויה היא קבלת איתות האם מדובר בהודעת ספאם. התוצאה הפשוטה ביותר היא סינון בינארי: ספאם או לא ספאם. התוצאה הנפוצה יותר היא תוצאה יחסית, שמתקבלת מפעולת מסננים שמספקים איתות לגבי מידת הסבירות שההודעה היא אכן ספאם.[14]

הבדל חשוב נוסף בין מסננים נוגע לזרימת המידע: מסננים ניתן להתקין **במכשירו של המשתמש**, או ב**שרתים של ספקי תשתיות ושירותים**, כלומר במקום בו הם מבצעים שירות דומה עבור משתמשים רבים.[15] כאשר המסנן פועל בשרת הדוא"ל, הוא מסנן את הדוא"ל הנכנס על סמך כללים אוניברסליים, עבור כלל המשתמשים. כך ניתן למחוק דוא"ל בטרם יצא מתיבת הדואר הנכנס של השרת אל המשתמש, ומשם לתיבת הספאם אצל משתמש הקצה. בתרשים ד.2, זהו האפיק התחתון. כאשר המסנן פועל כחלק מתוכנית הדוא"ל של המשתמש עצמו, יכול המשתמש להתאים את הכללים לדרישותיו, והסינון מתבצע כאשר הדוא"ל מגיע מהשרת אל תיבת הדוא"ל של המשתמש.[16]

---

8 ראו James Carpinter & Ray Hunt, *Tightening the Net: A Review of Current and Next Generation Spam Filtering Tools*, 25 Comp. & Sec. 566, 567 (2006).

9 על פתרונות אלה, ראו Gordon V. Cormack, *Email Spam Filtering: A Systematic Review*, 1.4 Foundations and Trends® in Information Retrieval, 11 (2008).

10 הדבר נכון ביחס למצב העניינים הגלובלי בתקופה בה נחקק חוק הספאם הישראלי, ראו קורמאק, שם. ביחס למצב העניינים העכשווי, ראו: Tushaar Gangavarapu, Jaidhar C.D., Bhabesh Chanduka, *Applicability of Machine Learning in Spam and Phishing Email Filtering: Review and Approaches*, 53(1) AI Rev. 5019-5081, 5060-5078 (2020); Isra'a AbdulNabi, Qussai Yaseen, *Spam Email Detection Using Deep Learning Techniques*, 184(2) Procedia Computer Science 853-858 (2021).

11 אלה יכולים לכלול את תוכן ההודעה עצמה, כללים מוגדרים ידנית אותם מטמיעים במסנן, מידע סטטיסטי הנגזר ממשובי משתמשים לפעולת המסנן, ועוד. ראו קורמאק, לעיל ה"ש 9, בעמ' 11.

12 שלושת הסוגים העיקריים של מסננים מבוססי מקור הם רשימות שחורות, רשימות לבנות ומערכות אתגר/תגובה (challenge/response systems). בנוסף, גם מערכות אימות (sender authentication systems), ניתוח רשתות חברתיות (social network analysis) וסינון מבוסס מוניטין נכללים תחת מסנני המקור. מערכות אלה שמות דגש על אימות זהות המוען או אימות כתובת הדומיין שלו, ועל מנת שתהיינה יעילות הן דורשות התאמה של מערכת הדוא"ל עצמה. הדבר נכון גם למערכות לסינון הודעות טקסט; ראו: Sarah Jane Delany, Mark Buckley and Derek Greene, *SMS Spam filtering: Methods and Data*, 39.10 Expert Systems with Applications 9899-9908, 9907 (2012).

13 Duncan Francis Cook et al., *Catching Spam Before It Arrives: Domain Specific Dynamic Blacklists*, 54 Proceedings of the 2006 Australasian Workshops on Grid Computing & E-Research 2 (2006).

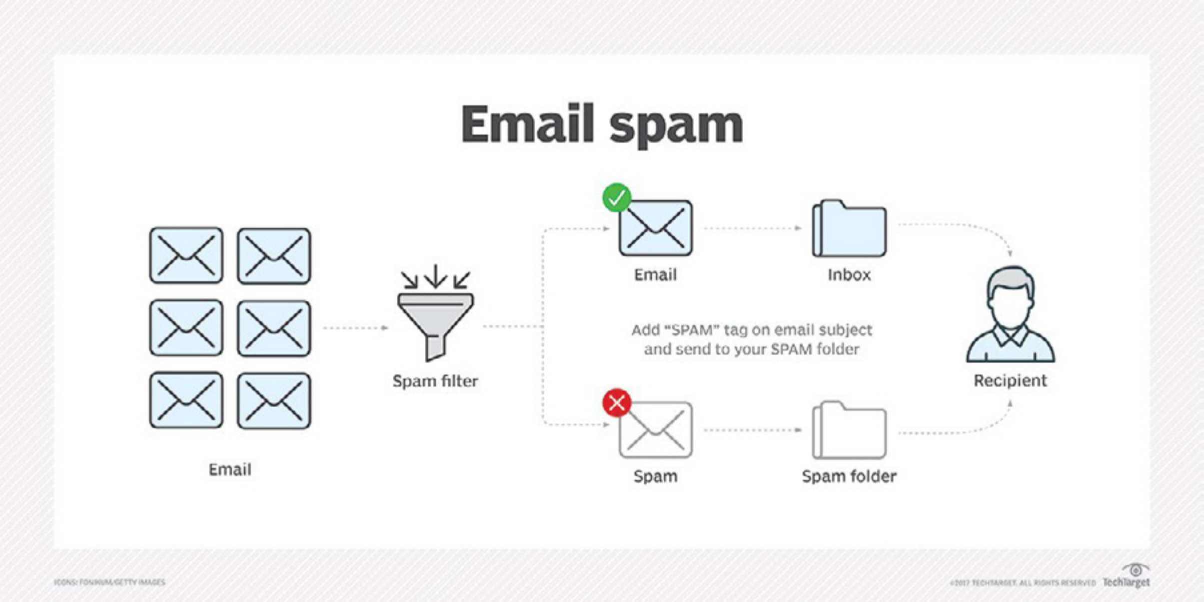
14 מסנן מהסוג הראשון, המספק תוצאה בינארית, נקרא "מסנן קשה" ("Hard Classifier"). מסנן מהסוג השני, המספק תוצאה יחסית, נקרא "מסנן רך" ("Soft classifier"). מסננים רכים רבים משווים את התוצאה היחסית שלהם מול תוצאה שמפיק מסנן קשה, "רגיש" יותר. ישנם מסננים שמאפשרים למשתמש להגדיר את רמת הרגישות בהתאם להעדפותיו (כמה הוא "סלחן" ביחס לספאם, או כמה הוא חושש מאובדן הודעות לגיטימיות). ראו למשל קורמאק, לעיל ה"ש 9, בעמ' 11. בנוסף, אפשר למיין את טכנולוגיות הסינון לכאלה המבוססות על כלי למידת מכונה (ML) וכאלה שאינן מתבססות על כלי למידת מכונה. אולם נראה שלרוב גם טכנולוגיות שהחלו ככאלה שאינן מבוססות ML, השתכללו עם הזמן והחלו לעשות שימוש בכלים אלה. ראו קרפינטר, לעיל ה"ש 8, בעמ' 568. הבחנה נוספת היא בין טכנולוגיות המספקות פתרונות מלאים לאלה המספקות פתרונות משלימים. פתרונות מלאים בונים בסיס ידע מקיף המאפשר להם לסווג את כלל הדואר הנכנס באופן עצמאי, בעוד פתרונות משלימים פועלים כמרכיב של מערכת סינון גדולה ומציעים תמיכה למסנן הראשי; שם. לדרכים נוספות לסיווג טכנולוגיות סינון, ראו: Bhowmick Alexy & Shyamanta M. Hazarika, *E-mail Spam Filtering: A Review of Techniques and Trends*, Advances in Electronics, Communication and Computing: ETAEERE-2016, 583 (2018).

15 קורמאק, לעיל ה"ש 9 בעמ' 13.

16 קרפינטר, לעיל ה"ש 8 בעמ' 568.

במקרה כזה, הביצוע נופל על כתפי המשתמש. בתרשים ד.2, זהו האפיק העליון. שני מסלולי הפעולה הללו אינם חפים מקשיים.

תרשים ד.2. מסנני ספאם ברמת השרת[17]



לגבי **מסננים ברמת השרת**, ספקי אינטרנט (ISPs), ספקי שירות דוא"ל חינמי (כמו גוגל ומיקרוסופט) ועסקים, משתמשים במסנני הספאם. תאגידי המידע הגדולים וספקיות תשתיות ושירותים משתמשים במסננים גם כלפי דוא"ל נכנס וגם כלפי דוא"ל יוצא, בעוד שארגונים קטנים עד בינוניים בדרך כלל מסננים דוא"ל נכנס בלבד, על מנת להגן על הרשת שלהם.[18] לחברות הגדולות המספקות שירותי תקשורת יש אינטרס בסינון ספאם, משום שכך הן מספקות שירותים טובים יותר ללקוחותיהן, אולם הן אינן מחויבות משפטית לספק שירות כזה; משכך, ההגנה על המשתמשים תלויה ברצון הטוב (כלומר באינטרס העסקי) של ספקיות השירות. בנוסף, בהנחה שמשתמשים יבחרו בשירותים שמספקים הגנה טובה יותר מפני ספאם, הרי כל עוד שירותי הגנה כאלה אינם ממומנים על ידי המדינה, התחרות בשוק נוטה לטובת החברות הגדולות ומעלה את רף הכניסה לשוק. ההשפעה היא על כניסת מתחרות קטנות לשוק, שמתקשות לספק למשתמשיהן הגנה ברמה זהה לזו שמספקים תאגידי הענק.

מסננים ברמת המשתמש מעלים שוב את סוגיית הפערים באוריינות הדיגיטלית בין משתמשים שונים.[19] למעשה, הפערים הללו קיימים גם כאשר משתמשים בסינון שמספקות החברות, מכיוון שהתאמה אישית של השירות להרגליו וצרכיו של משתמש ספציפי, למשל בחירה בסינון מחמיר יותר או פחות, דורשת אוריינות דיגיטלית בסיסית. כאשר המשתמש עצמו אחראי להתקנה ושימוש במסנן ספאם, הפערים בין משתמשים בעלי מידה שונה של אוריינות דיגיטלית ניכרים אף יותר. על כך יש להוסיף את העובדה שחלק משירותי הסינון שמציעות חברות למשתמשים אינם חינמיים.[20]

---

17 התרשים מתוך: Andrew Zola, *Definition: Spam Filter*, Techtarget (2021), נמצא ב: https://www.techtarget.com/searchsecurity/definition/spam-filter.

18 שם.

19 ראו דיון קודם שלנו בסוגיה זו בפרק ב, ס' 3(ב), בעמ' 36.

20 למשל, מסנן Mailwasher Pro של Firetrust, בעלות של כ-$50 לשנה, ראו: https://www.firetrust.com; מסנן "אנטי ספאם" של בזק, בעלות של 15.90 ש"ח לחודש (11.90 ש"ח במבצע): https://selfservice.bezeqint.net/safe-surfing/anti-spam. לדיווח על שירות "Smart Call" של פלאפון: אופיר ארצי "פלאפון משיקה שירות חסימה של שיחות ספאם" **TGSPOT** (9.2.2015): https://www.tgspot.co.il/pelephone-smart-call-filter/. השירות הוצע במחיר של 2.90 ש"ח לחודש. גם נטוויז'ן הציעה בעבר (2004) שירות סינון לדואר זבל במחיר של 9.90 ש"ח לחודש: "נטוויז'ן משיקה שירות אנטי ספאם" **ynet** (22.2.2004), ראו: https://www.ynet.co.il/articles/0,7340,L-2878368,00.html. שירות ה"אנטי ספאם" שמציעה חברת פרטנר, בעלות של 4.96 ש"ח לחודש, פועל על בסיס רשימות שחורות שמתעדכנות כל 24 שעות, ראו באתר החברה: https://www.partner.co.il/-2/pms3/internetservices/anti_spam. Zerospam, מציעה שירותי סינון במספר חבילות שהעלות שלהן נעה בין 5 ל-20 יורו לחודש: https://www.zerospam.eu/en/.

ב. ספאם ואנטי ספאם בהודעות טקסט למכשירי הטלפון

לעומת ספאם בדוא"ל, שהפך למטרד ש"אפשר לחיות איתו" כל עוד נשמר הסטטוס קוו בין ספאמרים לבין אלה הנלחמים בהם, זירת המאבק בתחום הודעות הטקסט שנשלחות למכשירי הטלפון והשיחות הקוליות רחוקה מרגיעה. עוד בשנת 2008, במהלך הדיונים לקראת חקיקת חוק הספאם מצב העניינים היה דומה. כך, כאשר הציע ח"כ בנימין אֱלון, אז יו"ר ועדת מדע וטכנולוגיה של הכנסת, להחיל את החוק רק על הודעות פקסימיליה ודוא"ל, התנגד לכך בתוקף חיים גרון, סמנכ"ל במשרד התקשורת דאז, בטענה שמוקד הבעיה אינה שני האפיקים האלה, אלא שיחות טלפון והודעות טקסט (SMS). גרון טען שההטרדה בשיחות ובהודעות טקסט פוגענית יותר משום שבפנייה לטלפון פרטי של אדם אין אפשרות לנמען לבחור האם להיות מוטרד או לא, בשונה מהטרדה בדוא"ל, שם אדם יכול לבחור האם להיכנס לתיבת הדואר שלו ומתי לעשות כן.[21]

מערכת התקשורת הסלולרית של שירות ההודעות הקצרות הפכה לאטרקטיבית במיוחד לספאמרים בשל הזמינות של חבילות סמס ללא הגבלה או תשלום מראש במדינות מסוימות כמו הודו, פקיסטן וסין.[22] בנוגע לישראל, ההנחה היא שמרבית הספאם בהודעות טקסט הוא מקומי, גם משום שקהל היעד של הפרסומים המסחריים הוא במקרים רבים מקומי (מה שנכון גם לסוגים אחרים של ספאם) אבל בעיקר משום שעלות משלוח מסרון בארץ היא אגורה, ואילו עלות השליחה של אותו מסרון מחוץ לארץ היא 30-40 אגורות להודעה. מכיוון שהסיכוי לרווח קטן באופן משמעותי, קשה להניח שלחברות דיוור גלובליות יש אחריות משמעותית למשלוח ספאם בהודעות טקסט לנמענים בישראל.

בעבר, ננקטו שיטות סינון פשוטות שניתחו את התעבורה ברשת, כדי לזהות נפחים גבוהים של הודעות ממנויים בודדים. אלה הם מסנני נפח. כלומר, כאשר מנוי אחד שלח את אותה הודעה (לפי מאפייניה החיצוניים – סוג ההודעה ומשקלה בזיכרון) לנמענים רבים, פעולה זו הייתה סימן לכך שמדובר בהודעת ספאם. שיטות כאלה מבוססות על מאפיינים חיצוניים, ולא על תוכן ההודעה. אבל, השיטות האלה איבדו מיעילותן, לאחר שספאמרים החלו להשתמש בנפחים נמוכים על מנת לחמוק ממסנני נפח.[23] ספאמרים עשו זאת באמצעות שליחת כמויות קטנות של מסרים כדי לבחון את תגובתה של תשתית הסמס של המפעיל, ובהמשך להגדיר את הנפח הרצוי לשליחה. זו גם המחשה למרוץ החימוש הטכנולוגי בתחום. דרך פעולה זו יצרה צורך בסינון מבוסס-תוכן.[24]

קיימות טכנולוגיות לסינון ספאם בדוא"ל שהוכחו כיעילות לסינון ספאם גם בהודעות טקסט, למרות שבשונה מסינון בדוא"ל, קשה יותר ליצור מסננים "חכמים" שיתגברו על הקושי בפרוטוקול פחות מתוחכם. כלומר, הודעות טקסט מספקות פחות "תוכן" לעבוד איתו עבור מסננים מתוחכמים. טכנולוגיות סינון תכנים המשמשות גם לסינון ספאם בהודעות טקסט כוללות טכניקות **סינון תוכן ישיר** וטכניקות **סינון תוכן שיתופי**.[25] טכנולוגיות סינון תוכן ישיר משתמשות בתוכן הטקסטואלי של ההודעה.[26] כלומר, הן מנתחות את נתוני ההודעה ואת התכנים המועברים בה. לעומתן, טכניקות סינון תוכן שיתופי מאפשרות לקבוצות משתמשים לשתף מידע על הודעות ספאם, והן נשענות במידה רבה על איכות וכמות דיווחי משתמשים על ספאם.[27] כלומר, טכניקות אלה הן מעין יצירה שיתופית של "רשימה שחורה" הנבנית מדיווחי משתמשים. אלא שלא לכל הטלפונים הניידים יש פונקציות כמו תיקיית ספאם או דיווח על ספאם. היבט זה הופך מסנני תוכן שיתופיים המסתמכים על משוב משתמשים לפחות שוויוניים מבחינה חלוקתית – מה שמדגיש את ההיבטים החלוקתיים של שאלת הסינון.

עם זאת, מאפייניה הייחודיים של הודעת טקסט מאתגרים מסננים מבוססי תוכן. כיום, הודעות אלה מוגבלות ל-160 תווים, ולכן מספקות חומר מועט יחסית למסננים כאלה. בנוסף, ספאמרים מרבים להשתמש בשפה ייחודית רוויה

21 ראו פרוטוקול ישיבה 6 של הוועדה המשותפת לוועדת הכלכלה ולוועדת המדע והטכנולוגיה, בעמ' 15-16 (1.4.2008).

22 Sarah Jane Delany, Mark Buckley, Derek Greene, *SMS Spam Filtering: Methods and Data*, 39.10 Expert Systems with Appl - cations 9899-9908, 9899 (2012).

23 דלאני, לעיל ה"ש 11, בעמ' 9900.

24 דלאני, שם, בעמ' 9899.

25 Sarah Jane Delany, Mark Buckley, Derek Greene, *SMS Spam filtering: Methods and Data*, 39.10 Expert Systems with Appl - cations 9899-9908, 9900 (2012). טכנולוגיות נוספות בוחנות את זהות השולח ולא את ההודעה עצמה, כמו למשל טכנולוגיית ניתוח רשתות (Network Analysis), המבוססת על ניתוח כתובות; שם.

26 טכנולוגיות אלה משתנות מסינון פשטני של מילות מפתח, ועד לגישות סיווג טקסט אלגוריתמיות מורכבות יותר.

27 ראו דלאני, לעיל ה"ש 11, בעמ' 9900.

בקיצורים וסימנים, המקשים על מסננים המבוססים על שפות טבעיות מוכרות לפענח את התכנים.[28] גם כותרת ההודעה (header) כוללת פחות מידע מכפי שכוללת כותרת בדוא"ל, שם היא משמשת רכיב חשוב בסינון ספאם.[29] כך, שלוש הבעיות העיקריות שמעכבות פיתוח אלגוריתמים בתחום הספאם בהודעות טקסט הן היעדר מערכי נתונים ציבוריים ואמיתיים לחוקרים בתחום, מספר נמוך של תכונות אותן ניתן לחלץ מכל הודעה, והעובדה שהטקסט שופע ניבים ייחודיים וקיצורים.[30]

בדומה לספאם בדוא"ל, סביר להניח שסוגים מסוימים של ספאם בהודעות טקסט ניתנים לסינון טוב יותר בשיטות מסוימות, כך שהדרך המבטיחה היא פתרונות היברידיים.[31] בהתחשב בכך שסינון הודעות טקסט חייב להתרחש תחת מגבלות קפדניות מאוד של זמן עיבוד, ניתן להגדיל באופן משמעותי את האפקטיביות של מסננים מבוססי תוכן ושיתופיות באמצעות שיטות סינון פשוטות ופחות עתירות משאבים כגון רשימות שחורות או פרופיל תנועה.[32]

הפתרונות לזיהוי ולסינון ספאם מתוכננים לפעול בשכבת הגישה (Access Layer, AL) כלומר ברמת **המשתמש**, או בשכבת **ספק השירות** (Service Provider Layer, SPL).[33] יתרונותיו של סינון במכשיר המשתמש הם שהוא בלתי תלוי ברשת ובמדיניות הספאם של מפעיל הרשת, והוא יכול לפעול על סמך הגדרות אישיות של המשתמש. עם זאת, סינון כזה כפוף למגבלות טכניות כמו כוח עיבוד זמין, והנחיצות במכשיר שהוא ידידותי לתוכנה (למשל, מכשיר של אנדרואיד בו אפשר לדווח על ספאם). בנוסף, כמו בנוגע לדוא"ל, סינון במכשיר המשתמש דורש אוריינות דיגיטלית של משתמשים. ניתן גם לשלב בין סינון בצד השרת וצד הלקוח.[34]

לקשיים אלה יש להוסיף את האינטרס של ספקיות שירות ההודעות. בניגוד לדוא"ל, שהוא שירות חינמי, שליחת הודעות כרוכה בתשלום וסינון שולחים עשוי לעלות לספקית השירות בהפסד כלכלי. במילים אחרות, לספקית שירות הודעות טקסט אינטרס כלכלי בשליחת כמה שיותר הודעות, בשונה מהאינטרס של ספקית שירות דוא"ל לעניין חסימת ספאם.

אם כך, יש מספר שיטות סינון עיקריות עם אפקטיביות מוגבלת:

- **מסנני נפח**, שהאפקטיביות שלהם ירדה מעת שספאמרים למדו לעקוף אותם;
- **מסנני תוכן ישיר**, שמנתחים את נתוני ההודעה ואת תוכנה. מסננים אלה מתקשים להתמודד עם מיעוט המידע בהודעות טקסט, עם סימנים מיוחדים וקיצורים שמאפיינים הודעות כאלה, ועם מיעוט התוכן בכותרת ההודעות;
- **מסנני תוכן שיתופי**, שמבוססים על דיווחי משתמשים. אפקטיביות של מסנן כזה תלויה בכמות המשתתפים ובאיכות הדיווח.

נזכיר, שלספקיות השירות יש אינטרסים סותרים: מצד אחד הן מבקשות להגן על לקוחותיהן מפני ספאם, אך מהצד השני כל חסימה של מקור ממנו נשלחות הודעות רבות תעלה להן בהפסד כלכלי.

ג. ספאם ואנטי ספאם בהודעות קוליות

בהשוואה לספאם בדוא"ל, שיחות קוליות מאתגרות אף יותר מהודעות טקסט. קשה ליישם טכניקות פשוטות נגד ספאם בשיחות קוליות, ואתגרי המערכת האקולוגית הטלפונית דורשים היערכות מסוג שונה מההיערכות שנדרשה

28 למשל, שימוש בסימן U כדי להחליף את המילה "you", שימוש באימוג'יז, וכדומה.

29 שם, בעמ' 9902.

30 ראו: Tiago A. Almeida, José María G. Hidalgo, Akebo Yamakami, *Contributions to the Study of SMS Spam Filtering: New Collection and Results*, Proceedings of the 11th ACM symposium on Document engineering 8 (2011).

31 שם.

32 דלאני, לעיל ה"ש 11, בעמ' 9907.

33 Muhammad Abdulhamid Shafi'I et al., *A Review on Mobile SMS Spam Filtering Techniques*, 5 IEEE Access 15653-4 (2017), וכן: Olusola Abayomi-Alli et al., A Review of Soft Techniques for SMS Spam Classification: Methods, Approaches and Applications, 86 Engineering Applications of Artificial Intelligence 197, 207 (2019).

34 דלאני, לעיל ה"ש 11, בעמ' 9906.

לקראת ספאם בדוא"ל או בהודעות טקסט.[35] רשת טלפון ציבורית (Public Switched Telephone Network, PSTN) היא אוסף רשתות טלפון מחוברות זו לזו העומדות בתקני הליבה של איגוד הטלקומוניקציה הבין-לאומי. ספאם טלפוני פועל בדרך כלל באופן הבא:

- שולח הספאם מתחבר דרך האינטרנט לספק שירותי הטלפון;
- השיחה מנותבת על ידי ספק חילופין (Interexchange Carrier);
- משם, השיחה עוברת לספק הסופי (Termination Carrier) והוא שמנתב את השיחה לנמען.

שולח הספאם יכול להיות חלק מארגון או שהוא פועל כקבלן עצמאי שמציע את הספאם כשירות. השיחות מתבצעות באמצעות חייגן אוטומטי, המחובר לספק שירותי טלפוניה.[36] כדי להפיץ שיחות באופן המוני לנמענים ברשת PSTN משתמשים בשירות VoIP (Voice Over Internet Protocol),[37] שדרכו אפשר להפיץ כמות גדולה של תכנים בעלות נמוכה בהשוואה לשירותי טלפון מסורתיים.[38]

ספאם באמצעות טלפון מציב אתגרים ייחודיים, חלקם טכני וחלקם רגולטורי:

- אילוצי מידיות – מערכת אנטי-ספאם בטלפון צריכה להשלים את ניתוח הנתונים באופן מידי, בחלון זמן מצומצם (כשהשיחה נכנסת).[39]
- קושי עם עיבוד שמע – מסיבות טכניות, ניתוח גל רדיו שונה מניתוח טקסט ומורכב יותר. יתר על כן, התוכן נחשף רק בשעה שהנמען ענה לשיחה.[40]
- היעדר נתוני כותרת (header) – בשונה מדוא"ל, שם נתוני הכותרת עשירים יחסית, נתוני הכותרת בשיחות קוליות הם זעומים. בנוסף, השמטת כתובת IP ושם הדומיין מכותרת שיחה קולית היא פשוטה למדי.[41] זאת גם בהשוואה לנתוני הכותרת בהודעות טקסט.
- קושי בהשגת הסכמה של משתמשים לשימוש במערכת אנטי-ספאם – לצרכנים יש סובלנות נמוכה מאוד לחסימת מוטעית של שיחות לגיטימיות (false positives). שיחות טלפון נוטות להיות דחופות יותר וחשובות יותר מדוא"ל או מהודעת טקסט, ולחסימה שגויה של שיחת טלפון עשויות להיות תוצאות הרות אסון.[42]
- זיוף זהות המתקשר – שירותי זיהוי מתקשר מספקים לנמען מידע על המתקשר בטרם המענה לטלפון. עם זאת, בהיעדר מנגנון אימות, קל למדי לזייף את זהות המתקשר.[43]
- קושי במעקב אחר שיחות ספאם – אחת הדרכים להילחם בספאם היא הפיכתו לבלתי חוקי. בעבר, מספר קטן של שחקנים היה אחראי למרבית הספאם, כך שנקיטת צעדים נגד שחקנים מרכזיים הביאה לצמצום בנפח התופעה. כיום, האתגרים הטכניים והרגולטוריים של ניטור תעבורת PSTN והשכיחות של זיוף זיהוי מתקשר מקשים על זיהוי מפיצי ספאם. הקושי במעקב אחר ספאם גדל מפני שניתן ליזום שיחות ספאם דרך האינטרנט, מה שמאפשר לספאמר להתחבא מאחורי פרוקסי, VPNs, רשתות Tor, או להפיץ שיחות יוצאות דרך רשת בוטים.[44]

---

35 Huahong Tu et al., *SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam*, 2016 IEEE Symposium on Security and Privacy (SP), 320 (2016).

36 שם, בעמ' 321-320.

37 טכנולוגיות שונות להעברת דיבור ברשתות IP.

38 טו ואח', לעיל ה"ש 35, בעמ' 322.

39 שם, בעמ' 323.

40 שם, בעמ' 324-323.

41 שם, בעמ' 324.

42 שם.

43 שם, בעמ' 325. מנגנון האבטחה היחיד נובע מכך שה-TSP שולח את זיהוי המתקשר בשמו. אך הזיהוי הזה נשחק כאשר שולח הספאם נרשם לשירות TSP המאפשר התאמה אישית של זיהוי המתקשר. פעם היה מדובר על תהליך יקר מאוד, אך עם עליית שירותי VoIP המספקים תכונות כגון התאמה אישית של זיהוי מתקשר דרך האינטרנט, ניתן לזייף את זהות המתקשר בזול ובמהירות.

44 שם, בעמ' 325.

- מערכת PSTN קיימת כבר כמה עשורים ומאפשרת לכל טלפון להגיע לטלפון אחר באמצעות חיבור עצום של מרכזי מיתוג. בעוד שרתות הליבה התפתחו להיות נישאות כמעט במלואן על ידי תשתית מבוססת IP – פרוטוקולי האיתות לא השתנו (כדי להבטיח תאימות מדור קודם). למרות שה VoIP נחשבת כמהפכה גדולה של התקשורת הקולית, המורשת הטכנולוגית של פרוטוקולי PSTN תישאר לעוד שנים רבות. הדבר מאפשר לשולחי ספאם לנצל את נקודות התורפה של המערכת הישנה, למשל היעדר היכולת לאמת את זהותו של המתקשר.[45]
- היעדר רגולציה אפקטיבית – מחסור בתמריצים לתעשייה להשתתף במאמץ נגד הספאם, בין השאר משום שספקי שירותי טלפון נהנים מנפחי תעבורה גדולים אותם מייצרים ספאמרים.[46]

משתמשי "טלפון חכם" יכולים להשתמש **ביישומים ייעודיים** לחסימת שיחות ממספרים לא מזוהים או לא מוכרים, למשל Trucaller, אם כי לשימושים כאלה יש מחיר של פגיעה בפרטיות המשתמשים ברשת הטלפונית, ובכלל זה הנמענים. דרך שנייה היא **חסימה מובנית** – רוב הטלפונים היום כוללים הגדרה בסיסית המאפשרת לחסום ממתקשרים לא רצויים באופן אוטומטי.

מצד הספאמרים, שתי הדרכים הנפוצות לעקוף אמצעי הגנה אלה הן: 1. שימוש בדואר קולי, כלומר בהודעות קוליות מוקלטות מראש המגיעות לתא הקולי של הנמענים, באמצעות טכניקות המעבירות ישירות את השיחה המוקלטת אל התא הקולי, ללא המתנה למענה; 2. זיוף זהות המתקשר (Caller ID spoofing). מדובר בדרך יעילה להערים על היישומונים חוסמי השיחות, משום שניתן לזייף בקלות את מספר המתקשר בשל היעדר מנגנון אימות מובנה, וכן מפני שהנמען אינו יכול לאמת את המספר בזמן אמת. כמו כן, על ספק השירות של המתקשר לא חלה חובה חוקית לוודא שמספר זיהוי המתקשר בכותרת בקשת השיחה אכן נמצא בבעלות המתקשר בטרם בוצעה השיחה. חלק מספקי שירותי טלפוניה מספקים שירות של זיהוי מתקשר הניתן להתאמה אישית.[47]

מאגר "אל תתקשר אליי"

ביום 1.1.2023 נכנס לתוקף המאגר הלאומי "אל תתקשר אליי", בעקבות תיקון 61 לחוק הגנת הצרכן, התשמ"א-1981, שקובע, בין היתר, מגבלות על שיחות שיווק טלפוניות ומחייב עוסק המבצע שיחת שיווק באמצעות הטלפון או בדרך אלקטרונית לברר האם מספר הטלפון שאליו מתבצעת השיחה רשום במאגר ייעודי.[48] לצורך כך, הרשות להגנת הצרכן ולסחר הוגן הקימה ומנהלת מאגר שבו נרשמים מספרי טלפון של צרכנים שאינם מעוניינים שיבוצעו למספר הטלפון שלהם שיחות שיווק. לפי החוק, עוסקים שמבצעים פנייה שיווקית לא אמורים לפנות לצרכנים שנרשמו במאגר. עוסק שמבקש להתקשר לצרכן יצטרך לבדוק האם הצרכן רשום במאגר, ורק אם מספרו של הצרכן אינו חלק מהמאגר הוא יוכל להתקשר אליו. הרשות להגנת הצרכן מאפשרת לבעלי עסקים לבדוק האם מספרי טלפון של צרכנים נמצאים במאגר באמצעות ממשק API למאגר. בעל העסק מבצע שאילתה לגבי מספר מסוים ומקבל מידית תשובה חיובית או שלילית.[49]

הצורך בתקנות נבע מכך שבארץ התפתחה פרקטיקה של שיווק אגרסיבי דרך שיחות טלפון, במיוחד כלפי אזרחים ותיקים, עולים חדשים ואוכלוסיות מוחלשות. שיחות אלו הובילו לא אחת לעסקאות בשווי של מאות אלפי שקלים תוך הטעיית הצרכן. התופעה התגברה בתקופת הקורונה, כאשר במהלכה גברה הישנותם של מקרי העושק באמצעות

45 H. Tu, A. Doupé, Z. Zhao, G. -J. Ahn, *SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam*, 2016 IEEE Symposium on Security and Privacy (SP) 320, 324 (2016).

46 טו ואח', לעיל ה"ש 35, בעמ' 325.

47 שם, בעמ' 323.

48 חוק הגנת הצרכן (תיקון מס' 61), התשפ"א-2020.

49 כמו כן, מוחזרת מספר הטרנסאקציה לפנייה. מספר זה מהווה אסמכתא לבעל העסק, שאכן התבצעה בדיקה, לפני ביצוע שיחת טלמרקטינג ללקוח. ראו הרשות להגנת הצרכן ולסחר הוגן, "אל תתקשרו אליי – מסמכים לעוסקים" (12.12.2022), נמצא ב: https://www.gov.il/he/departments/news/cpfta_dncapi. עסקים שיתעלמו מהמאגר יהיו חשופים לעיצומים כספיים של 45 אלף ש"ח לתאגיד ו-25 אלף ש"ח לעוסק פרטי. בשונה מחוק הספאם, המאפשר הגשת תביעות לפיצויים ללא הוכחת נזק בגין מסרון שנשלח ללא הסכמה – לא קיימת הוראה דומה בקשר עם שיחות טלפון למספר שמופיע במאגר.

שיחות הטלפון.[50] לאור הקושי להוכיח התנהלות מטעה כלפי צרכנים, שממנו נבע גם הקושי לבצע אכיפה כנגדה, החליט המחוקק להטיל מגבלות על היכולת לבצע פניות שיווקיות בטלפון.[51]

המאגר הוא שירות חינמי המיועד לצרכנים המעוניינים לרשום מספר טלפון (נייד או נייח) ישראלים. נתונים במאגר מאובטחים והמאגר אינו דורש או אוסף כל מידע נוסף מהצרכן מלבד מספר הטלפון שנרשם למאגר. ניתן להסיר מספר טלפון מהמאגר בכל שלב. עם זאת, התקנות אינן חלות על מסרונים או הודעות מידיות דומות כמו וואטסאפ.[52] הקמת המאגר היא חלק ממגמה עולמית במדינות רבות בעולם, לרבות ארצות הברית, קנדה, אנגליה, סינגפור והודו. לפי סקר שנערך בארצות הברית בשנת 2009, לאחר הקמת מאגר דומה שם, פחת מספר שיחות הטלמרקטינג הממוצע שהתקבלו בחודש מ-30 ל-6 בלבד.[53]

עם זאת, מומחי אבטחת מידע מתריעים מפני דליפת מידע מהמאגר בשל האופן בו הוא בנוי, וכן מציינים שארגונים רבים מוחרגים מהמאגר, וחלקם ישמחו לקבל רשימות של מספרי טלפון פעילים בהם יוכלו להשתמש לפי ראות עיניהם.[54] למעשה, מכיוון שאין מגבלה על השאילתות שעסק יכול להגיש למאגר, בעלי עסקים יכולים לייצר רשימות של מיליוני מספרי טלפון באופן זה. בשיחה שערכנו עם עו"ד זיו גלסברג שפעיל בתחום הספאם, עלו חששות נוספים פרט לסכנת ההדלפה או השימוש לרעה בנתוני המאגר. עו"ד גלסברג הוסיף על אלה את העובדה שמכיוון שהתקנות לפיהן הוקם המאגר אינן חלות על הודעות טקסט, ספאמרים יוכלו להתחיל לשלוח הודעות טקסט למספרים שמופיעים במאגר. בנוסף הביע גלסברג את החשש שהמאגר מטיל נטל על שחקנים מוחלשים באוכלוסייה, בתקווה שהם אלה שיאספו ראיות – מה שממילא קשה לעשות - ויפנו תלונות לרשות להגנת הצרכן. בהמשך לכך ציין גלסברג כי הקושי הראייתי הגדול ביותר נוגע לבעיית התיעוד. בכדי להגיש תלונה, על הנמען להקליט את השיחה, ולרוב, בשל העובדה שמדובר בשיחות קצרות יחסית, בכדי שיוכל להקליט שיחה זו, עליו להקליט כל שיחה נכנסת. גם לאנשים עם ידע טכנולוגי יש קושי בהקלטת שיחות, לא כל שכן כל השיחות הנכנסות. כך, למשל, אפל אינה מאפשרת הקלטת שיחות במכשיריה,[55] וגם במכשירי אנדרואיד קיימות לעיתים מגבלות ביכולת ההקלטה, כתוצאה מניסיון לעמוד בדיני האזנות סתר בטריטוריות שונות.

בעיה נוספת נובעת מכך שלמרות שהשירות נוצר בתגובה להיעדר יכולת ההגנה של אזרחים ותיקים, עולים חדשים ואוכלוסיות מוחלשות נוספות מפני פרקטיקות של שיווק אגרסיבי, סביר להניח שאוכלוסיות אלה בדיוק יהיו אלה שיתקשו לרשום את עצמם בכוחות עצמם במאגר. על מנת להתגבר על קושי זה נדרש מערך הסברה מקיף שיידע את האוכלוסיות הרלוונטיות בדבר קיומו של השירות, וכן יסייע להן להירשם אליו.

מלבד החשש מדליפת מידע, שיקול פרטיות נוסף נוגע לפשטות שבה אפשר לאפיין אנשים לפי מספרי הטלפון שלהם. דוגמה מייצגת היא האופן בו אפשר להסיק שאדם הוא דתי מכך שמספר הטלפון שלו שייך למספרים "כשרים". למרות שדוגמה זו מצביעה על כך שמספר טלפון עשוי להיות מידע אישי רגיש, אין עדיין התייחסות מפורשת לכך מצד החוק.[56]

---

50 אסף הראל ואביטל חייטוביץ "המדריך המלא לסיום שיחות הספאם: מה-1 בינואר תוכלו להימנע משיחות שיווקיות" **מאקו דיגיטל** (30.9.2022), צפו: https://www.mako.co.il/nexter-guide/Article-d307477a7598381027.htm.

51 שם.

52 שם.

53 סיון חילאי "מאגר 'אל תתקשר אליי' החל לפעול: כך תוכלו להירשם", **Ynet** (12.12.2022): https://www.ynet.co.il/economy/article/s1l7yundo.

54 רן בר זיק "רוצים להירשם למאגר 'אל תתקשר אליי'? כדאי שתחשבו פעמיים", **דה-מרקר** (13.12.2022): https://www.themarker.com/captain-internet/2022-12-13/ty-article/.premium/00000185-0ada-d43f-afc7-bbde11840000.

55 המכשיר אינו מגיע, כברירת מחדל, עם האפשרות להקליט שיחות, אך מחיפוש בחנות היישומונים של אפל, נראה שיש כמה יישומונים שמאפשרים את הפונקציה הזאת, ראו: https://www.apple.com/us/search/call-recorder?src=globalnav.

56 ראו גילוי דעת של הרשות להגנת הפרטיות "האם אוסף של שמות וכתובות דואר אלקטרוני מהווה "מאגר מידע"? (28.11.2018) וגם, גילוי דעת של הרשות להגנת הפרטיות בנושא פרשנות המושגים "מידע" ו"ידיעה על ענייניו הפרטיים של אדם" בחוק הגנת הפרטיות (21.12.2022). משני המסמכים עולה שהרשות מתייחסת לדוא"ל כאל מידע אישי.

יישומוני צד שלישי לחסימת שיחות

מדובר בפתרון שפועל בצד הנמען, שמוריד אל מכשירו יישומון לסינון ולזיהוי של שיחות ספאם, וזאת בשונה ממאגר "אל תתקשרו אליי". במקום שהמאגר יכלול את פרטי הנמענים, הוא כולל את פרטי המוענים הלא רצויים. יישומונים אלה מבוססים על מאגר זיהוי שיחות שמתעדכן וגדל ככל שיותר אנשים משתמשים ומסמנים ביישומון מספרים מהם התקבלו שיחות מטרידות.[57] בעלי מכשיר אייפון (מגרסה 13 של iOS) יכולים להפעיל תכונה בשם 'השתקת שיחות ממוענים לא מוכרים'. הפעולה חוסמת מספרי טלפון שבעל המכשיר לא קיבל מהם שיחות קודם לכן או שלא שמר ברשימת אנשי הקשר.[58] המספרים המושתקים עדיין יכולים להשאיר הודעות בתא הקולי (אם יש כזה), והשיחות יופיעו ברשימת השיחות האחרונות. כך אפשר לעשות גם בנוגע להודעות טקסט.[59] גם בעלי מכשיר אנדרואיד יוכלו לחסום ידנית מספרים ספציפיים. הדבר מצריך זיהוי השיחה כשיחת ספאם (מענה לשיחה או דרך התקנה של אפליקציית לזיהוי שיחות), וחסימה ידנית של כל מספר בנפרד. מהרגע שהשולח חסום, לא יתקבלו התראות כשהוא מתקשר או שולח הודעות, והוא כמובן לא יוכל לדעת שהוא נחסם.[60] עם זאת, יש לזכור שהודעות עשויות להתקבל ממשתמש שמזדהה באמצעות טקסט ולא באמצעות מספר, וכן שספאמרים רבים נוהגים להחליף מספרים בתדירות גבוהה.[61]

ד. ספאם ואנטי ספאם בפלטפורמות חברתיות

בשנות ה-90 המאוחרות של המאה הקודמת, הגיע הספאם לפלטפורמות של הודעות מהירות (instant messag-ing), ובהמשך התפתח למערכות הודעות מהירות מודרניות כמו וואטסאפ, X (לשעבר טוויטר), פייסבוק ומסנג'ר.[62] במערכות כמו וואטסאפ אנשים פותחים את מרבית ההודעות הנשלחות אליהם, ובניגוד להודעות סמס, שם אחוזי הפתיחה הם 90% ונמצאים כנראה במגמת ירידה (מכיוון שאנשים משתמשים בערוץ זה פחות ופחות לצורך העברת הודעות פרטיות), משתמשי וואטסאפ משתמשים בערוץ זה להעברת כל סוגי המסרים, אישיים, חברתיים, ומקצועיים.[63]

מבחינה משפטית, לעניין שליחת ספאם, אין הבדל מהותי בין פלטפורמות חברתיות לבין אמצעי תקשורת אחרים. החוק רואה במסרים הנשלחים באמצעות הפלטפורמות הודעות אלקטרוניות (להבדיל מ"הודעות מסר קצר") ולכן חל עליהם הדין שחל על הודעות דוא"ל. בתי המשפט התמודדו עם סוגיות שונות הנוגעות לשאלה מהי הודעה אלקטרונית.[64] עם זאת, בפלטפורמות החברתיות יש גורם מרכזי המחזיק בידיו גישה לכלל המידע, ויש להניח שבכוחו לזהות בקלות יחסית חשבונות של ספאמרים.

---

57 ראו למשל בנוגע לאחד היישומונים הללו: דורון פרידמן "נמאס לכם משיחות ספאם של פוליטיקאים? Truecaller משיקה אפליקציה שמזהה חצי מיליון מספרים" **ישראל היום** (30.8.2022): https://www.israelhayom.co.il/tech/tech-news/article/13017513.

58 המספרים "המושתקים" יכולים להשאיר הודעות בתא הקולי, והשיחות יופיעו ברשימת השיחות האחרונות שלכם. הדבר נכון גם במקרה של הודעות. במקרה של ביצוע שיחת חירום, התכונה תושבת זמנית למשך 24 שעות כדי לאפשר קבלת שיחות. ראו בדף התמיכה של חברת אפל: https://support.apple.com/he-il/HT207099.

59 במקרה של ביצוע שיחת חירום, התכונה 'השתקת שיחות ממטלפנים לא מוכרים' תושבת זמנית למשך 24 השעות הבאות כדי לאפשר קבלת שיחות; שם.

60 נבו טרבלסי "הסוף לספאם הבחירות: כך תחסמו הודעות ושיחות לא רצויות" **גלובס** (27.10.2022): https://www.globes.co.il/news/article.aspx?did=1001428007.

61 שם.

62 ראו: Emilio Ferrara, *The History of Digital Spam*, 62.8 Communications of the ACM 84-5 (2019).

63 נראה שבשנים האחרונות הודעות סמס משמשות יותר ויותר לצרכי שיווק, סיסמאות חד פעמיות ושחזור חשבונות, ופחות לצורך הודעות פרטיות. ראו למשל דיווח של חברה מסחרית בנושא: MAUSUMI, SMS is dying, WhatsApp is taking over, **kommunicate** (4.3.2022), נמצא ב: https://www.kommunicate.io/blog/sms-vs-whatsapp-which-is-best-for-your-business.

64 בית המשפט המחוזי בתל אביב קבע כי לשון החוק מאפשרת להתאים את הגדרת הספאם לאמצעי תקשורת שונים, בעלי מאפיינים דומים, שהחוק לא מנה במפורש, אך יש לעשות כך תוך שימת לב לאיזון העדין שבין החלה דווקנית של לשון החוק לבין החלתו על אמצעי טכנולוגי שהמחוקק לא נתן עליו את דעתו בעת החקיקה. בהמשך לכך קבע בית המשפט כי אין מקום להבחין בין רשת האינטרנט לרשת הלווין ככל שהדבר נוגע לתחולת חוק הספאם. ראו ת"צ (מחוזי ת"א) 3468-09-14 **רודד נ' די.בי.אס. שרותי לווין (1998) בע"מ** (נבו 26.06.2019), בעמ' 31-21. בהמשך, בת"צ (מחוזי מרכז) 1862-11-12 **טויסטר נ' Google Inc** (נבו 18.09.2014), קבע השופט גרוסקופף שיש לפרש את המונח של הודעה אלקטרונית "בצמצום... כך שלא תחול על כל דבר פרסומת המוצג באתר תוכן". לקביעה לפיה הודעת מסר בפייסבוק עונה על הגדרת "הודעה אלקטרונית" בחוק הספאם, ראו תק (ת"א) 32611-12-15 **רדזינר נ' סלקום ישראל בע"מ** (נבו 24.07.2016), וכן תא"מ (שלום הרצ') 15909-04-16 **לב נ' ממון** (נבו 29.09.2017). בשנת 2018 קבע בית המשפט לתביעות קטנות שהודעות פרטיות בפייסבוק שעניינן פרסום

בעוד שלפני שנות האלפיים מרבית פעילות הספאם נעשתה על ידי מפעילים אנושיים, השימוש הגובר בבוטים איפשר ספאם בקנה מידה חסר תקדים ברשתות חברתיות, כאשר ספאמרים מייצרים פרסונות אונליין עם עוקבים מזויפים.[65] חשבונות מזויפים או בוטים משמשים לשליחה אוטומטית של הודעות או ציוצים שמכילים קישורים שניתן להשתמש בהם או כדי לאסוף מידע שיווקי או למטרות זדוניות. לכן פתרונות סינון מתמקדים בניסיון לאפיין ולזהות את השולח ולא בתוכן ההודעה. המאפיינים המשמשים לזיהוי ספאם מבוססים בדרך כלל על **התנהגות המשתמש** מתוך הנחה שהבוטים יתנהגו בצורה שונה משמעותית ממשתמשים אנושיים. בתוכן הטקסט של הודעה נעשה שימוש מצומצם, בעוד עיקר השימוש של מסננים מתקדמים הוא במאפיינים מבוססי משתמשים כגון מספר החברים ברשת החברתית, העוקבים, והתנהגות סביב הפרסום. תכונות נוספות שנבחנות הן מספר האשטאגים, אזכורים, וכתובות אתרים בהודעה.[66]

גם בספאם ברשתות חברתיות, מרוץ החימוש בעיצומו. התפתחויות חדשות בתחום הבינה המלאכותית מאפשרות ייצור בוטים שמסוגלים ליצור שפה טבעית המדמה שפה אנושית, וליצור אינטראקציה עם בני אדם כמעט בזמן אמת.[67] הדבר מאפשר ליצור סוכנים מזויפים שיסייעו לספאמרים בהפצת מרכולתם. ספאם באמצעות סוכני בינה מלאכותית, גם אם ברובו הוא עדיין ספקולטיבי, מייצר אתגר משמעותי עבור טכנולוגיות אנטי-ספאם קיימות, ומומחי אבטחת סייבר וחוקרי למידת מכונה התאחדו על מנת לפתח טכניקות שיאתרו את החתימה המלאכותית של בוטים ברשתות חברתיות.[68]

ה. פתרונות טכנולוגיים: הדור הבא

מתוך התבוננות במנגנוני האכיפה הטכנולוגיים המרכזיים המצויים בשימוש היום בישראל וניתוח שלהם, עולות מספר אפשרויות לפתרונות שטרם נוסו, או לדרכי חשיבה רצויות על פתרונות כאלה. כאן נמנה מספר מנגנוני פעולה טכנולוגיים או משולבים, טכנולוגיים-משפטיים, שאינם בשימוש היום אך הם מציעים מענה לבעיות קיימות. אלה עלו מניתוח הנתונים והחומרים עד כה ומשיחות עם העוסקים בתחום:

- יכולת טובה להתחקות אחר מחזיקי שמות מתחם של אתרי אינטרנט וכתובות דוא"ל, עשויה לשפר את היכולת לזהות ספאמרים חוזרים. אולם שיפור ביכולת הזו מהווה גם שיפור ביכולת הפגיעה בפרטיותם של מחזיקי שמות מתחם. מכיוון שרבים מהספאמרים הקבועים הם תאגידים, ולתאגידים אין פרטיות,[69] פיתוח יכולת כזו כלפי תאגידים בלבד עשויה להתגבר על הקושי. כך למשל החזקה של יותר משם מתחם אחד על ידי אותה ישות עשוי להוות אינדיקציה לכך שלא מדובר באדם פרטי.
- כדאי לשים לב שטכנולוגיות סינון מתקדמות מבוססות תוכן, כמו למשל טכנולוגיות NLP (Natural Language Processing), נועדו בעיקר לזהות ספאם זדוני למטרות הונאה או מטרות פליליות אחרות. תוכן שיווקי שטכנולוגיות כאלה לא סיננו משום שהוא לגיטימי, לא מבטיח עדיין שהתגברנו על בעיית ההסכמה. מסננים מבוססי מקור יכולים אמנם לזהות כתובת לא רצויה, אך זאת רק כאשר הנמען ציין כתובות כאלה, למשל כאשר הוא סימן הודעה שהגיעה לתיבת הדואר שלו כהודעת ספאם. קושי זה הוא אחד מיני רבים המעידים על כך שפתרונות טכנולוגיים בלבד אינם מספיקים על מנת להילחם בספאם. ללא השתתפות פעילה של נמענים בסינון, קשה להניח שמסנן יוכל לזהות בכוחות עצמו מי הנמען שאינו מעוניין בקבלת מסר פרסומי מסוים ולא הסכים לכך, ומי הנמען שדווקא מבקש לקבל בדיוק את המסר השיווקי הזה.
- כפי שהזכרנו בראשית הדיון בספאם בדוא"ל, הפתרונות שהוצעו עד היום למלחמה בספאם בדוא"ל נחלקים לשלוש קטגוריות עיקריות. מלבד פתרונות משפטיים ופתרונות בדמות טכנולוגיות סינון, הקטגוריה השלישית היא פתרונות המבוססים על תשתיות. פתרונות כאלה מבקשים לשנות את האופן בו אנו נוהגים לשלוח דוא"ל

מסיבות הן הודעות פרסומת וחל עליהן חוק הספאם, ובית המשפט העליון לא מצא לנכון להתערב בקביעה אם כי הטעים שהסוגיה טרם מוצתה, ראו רע"א 3599/18 **שפירא נ' עופרי** (נבו 30.5.2018).

65 פררה, לעיל ה"ש 62, בעמ' 88.

66 דלאני, לעיל ה"ש 35, בעמ' 9902.

67 פררה, לעיל ה"ש 62, בעמ' 89.

68 שם.

69 ראו ס' 3 לחוק הגנת הפרטיות, ודיון אצל מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט וטכנולוגיה** 126-132 (2010).

למשל באמצעות דרישת אימות מהשולח או תשלום מאומת. לדוגמה, אפיק טכנולוגי מבטיח שיאפשר להתגבר על בעיית האימות היא שימוש בטכנולוגיות בלוקצ'יין.[70] טכנולוגיות אלה יכולות להתגבר על הבעיה הנוצרת בשל היעדר אמצעי אימות ווידוא זהות (authentication) שיבטיחו את זהות המוענים ואת הלגיטימציה של שליחת מסרי תקשורת. טכנולוגיות בלוקצ'יין עשויות לסייע גם בווידוא זהות מהימן יותר של פרסונות דיגיטליות, ובכך למנוע חלק מצורות הספאם ולמתן את השפעתן ואת קנה המידה של טכנולוגיות אחרות.[71]

- עו"ד גלסברג, ממייסדי עמותת "אל ספאם", סיפר על שירות שהעמותה שוקלת לספק למפרסמים ולנמענים, ושנועד לפתור מספר בעיות עם מודל ההסכמה הקיים. למרות שהמודל הקיים הוא opt-in, לעיתים אנשים נרשמים אך אינם זוכרים שעשו כך, או שאדם אחר רושם אותם. המודל המוצע מבקש לאמת את ההסכמה, כלומר הוא שירות של "double opt-in". כך, כאשר אדם יירשם לשירות חדש, הוא יקבל קוד או קישור בדוא"ל, ורק אז יוכל להשלים את תהליך ההרשמה. תהליך כזה מוודא שלאדם שהזין פרטים לשירות מסוים תהיה גישה לאמצעי התקשורת שהוא מסר וכי הוא אכן מעוניין בהרשמה. כך גדלה הוודאות שמדובר בהסכמה של ממש, מדעת ומרצון. בנוסף, השירות המוצע ישלח הודעה לשני הצדדים כאשר תהליך ההרשמה יושלם, וכן תשלח הודעה לצדדים כאשר משתמש מבקש להיות מוסר מרשימת תפוצה; בכך יספק השירות ראייה מצד שלישי אובייקטיבי שבמקרים רבים אינה קיימת."

3. סיכום

בפרק זה עמדנו על פתרונות טכנולוגיים שונים המבקשים להתמודד עם ספאם באפיקי התקשורת עליהם חל החוק הישראלי. לצד הצלחות טכנולוגיות לא מבוטלות, עולה ההבנה שכל עוד ספאם הוא עסק רווחי מספיק, איננו עומדים לחזות בקץ התופעה בקרוב.

הגישה המחקרית שמנחה דוח זה היא פרדיגמת המחקר של "משפט וטכנולוגיה", כלומר היא ערה לקשר המורכב שבין משפט לטכנולוגיה וגורסת כי המשפט לבדו, או הטכנולוגיה לבדה, אינם יכולים לפתור בעיות סוציו-טכנולוגיות בכוחות עצמם. פרק זה הוסיף על הניתוח המשפטי של הפרק הקודם את לימוד הטכנולוגיות הרלוונטיות, המבקשות לחסום את הספאם בשלבים שונים של זרימת המידע. אכן, ספאם הוא אמנם תופעה הנטועה בטכנולוגי, אבל כמו כל תופעה טכנולוגית אחרת, ספאם מושפע מגורמים רבים בעולם החברתי, הכלכלי והפוליטי, ומשפיע עליהם. גם בספרות המחקרית העוסקת בספאם, צמחה ההבנה שעל מנת להתמודד עם התופעה באופן אפקטיבי נדרש שילוב של כלים טכנולוגיים עם חוקים ומדיניות משפטית עדכניים.[72] בכך יעסוק הפרק הבא.

מסקנות ביניים

- כל עוד ספאם הוא עסק רווחי מספיק, איננו עומדים לחזות בקץ התופעה בקרוב.
- בעוד שמרוץ החימוש סביב הספאם בדוא"ל אכן הגיע לסטטוס קוו בעת הזו, באפיקי ספאם נוספים, כמו שיחות טלפוניות או הודעות טקסט, המצב רחוק מלהיות מאוזן.
- בנוגע לספאם בדוא"ל, בעשורים האחרונים, מסנני דוא"ל הוכיחו את עצמם ככלי יעיל ביותר למניעת ספאם. עם זאת, בנוגע למסנני ספאם **ברמת השרת**, ההגנה על המשתמשים תלויה ברצון הטוב (כלומר באינטרס העסקי) של ספקיות השירות. בנוסף, כל עוד שירותי הגנה כאלה אינם ממומנים על ידי המדינה, התחרות בשוק נוטה לטובת החברות הגדולות ומעלה את רף הכניסה לשוק. בנוגע למסנני ספאם **ברמת המשתמש**, פערים משמעותיים באוריינות דיגיטלית בין משתמשים שונים מצביעים על כך שפתרונות כאלו אפקטיביים רק עבור פלח קטן של האוכלוסייה.

---

70 ראו פררה, לעיל ה"ש 62, בעמ' 90-91.

71 שם.

72 Roderic Broadhurst & Mamoun Alazab, *Spam and Crime, in* Regulatory Theory, Foundations and Applications 517, 527 (Peter Drahos, ed., 2017).

- בנוגע לספאם בהודעות טקסט, קיימות מספר שיטות סינון עיקריות עם אפקטיביות מוגבלת: **מסנני נפח**, שהאפקטיביות שלהם ירדה מעת שספאמרים למדו לעקוף אותם; **מסנני תוכן ישיר**, שמנתחים את נתוני ההודעה ואת תוכנה. מסננים אלה מתקשים להתמודד עם מיעוט המידע בהודעות טקסט, עם סימנים מיוחדים וקיצורים שמאפיינים הודעות כאלה, ועם מיעוט התוכן בכותרת ההודעות; **מסנני תוכן שיתופי**, שמבוססים על דיווחי משתמשים. אפקטיביות של מסנן כזה תלויה בכמות המשתתפים ובאיכות הדיווח. בנוסף לקשיים אלה, לספקיות השירות יש אינטרסים סותרים: מצד אחד הן מבקשות להגן על לקוחותיהן מפני ספאם, אך מהצד השני כל חסימה של מקור ממנו נשלחות הודעות רבות תעלה להן בהפסד כלכלי.
- שיחות קוליות מאתגרות אף יותר מהודעות טקסט. קשה ליישם טכניקות פשוטות נגד ספאם בשיחות קוליות, ואתגרי המערכת האקולוגית הטלפונית דורשים היערכות מסוג שונה מההיערכות שנדרשה לקראת ספאם בדוא"ל או בהודעות טקסט. האתגרים הייחודיים, טכנית ורגולטורית, של ספאם באמצעות טלפון אותם מנינו הם: אילוצי מידיות; קושי טכני עם עיבוד שמע; היעדר נתוני כותרת (header); קושי בהשגת הסכמה של משתמשים לשימוש במערכת אנטי-ספאם; זיוף זהות המתקשר; קושי טכנולוגי במעקב אחר שיחות ספאם ומקורן; ניצול נקודות תורפה של מערכת ישנה, כמו למשל היעדר יכולת לאמת את זהות המתקשר. בנוסף, הרגולציה אינה אפקטיבית בשל מחסור בתמריצים כלכליים לתעשייה להשתתף במאמץ נגד הספאם. פתרונות חדשים כמו מאגר "אל תתקשר אליי" או יישומוני צד שלישי לחסימת תכנים, אף הם אינם חפים מקשיים.
- בנוגע לספאם ברשתות חברתיות, מרוץ החימוש הטכנולוגי בעיצומו. פתרונות סינון עכשוויים מתמקדים בניסיון לאפיין ולזהות את השולח ולא בתוכן ההודעה.

פרק ה

ספאם, זבל, והנדסת ניקיון

1. **מבוא: משפט וטכנולוגיה בזירת הספאם** **80**
2. **התערבות משולבת: לפני ואחרי מעשה** **80**
   א. פתרונות לפני מעשה (*ex ante*): הנדסת ניקיון 80
   (1) הנדסה ערכית 81
   (2) מטפורת הניקיון 81
   ב. פתרונות לאחר מעשה (*ex post*): "ספאם אוף" כמשל 85
3. **הטלת חבות משפטית: שחקנים אפשריים** **86**
   א. שחקנים בשרשרת הערך 87
   (1) שלב ראשון – בעלי המסר 87
   (2) שלב שני: גורמים מסייעים לפני ההפצה 88
   (3) שלב שלישי: גורמים מסייעים בשלב ההפצה 90
   (4) שלב רביעי: הנמענים והשחקנים שאמונים על הגנתם 93
5. **סיכום** **95**

1. מבוא: משפט וטכנולוגיה בזירת הספאם

בפרקים הקודמים בחנו באופן פרטני את סל הכלים המשפטי להתמודדות עם ספאם ואת סל הכלים הטכנולוגי להתמודדות עם התופעה. ההפרדה המכשירנית שנקטנו בין הפן המשפטי לפן הטכנולוגי מאפשרת לבחון בפירוט כל אחד מהאפיקים הללו, אך היא אינה מספרת את כל הסיפור. הפן המשפטי והפן הטכנולוגי קשורים זה בזה ומשפיעים אחד על השני באופנים שונים. כעת הגיעה העת לחבר ביניהם. הבנת הממשק בין שני הגורמים הללו תאפשר הבנה טובה ומלאה יותר של המערכת האקולוגית של הספאם. בחינה זו נועדה לאפשר לקובעי מדיניות לשקול באופן מעמיק את הפתרונות השונים, הקיימים והמוצעים. בכך עוסק פרק זה.

הדיון בדוח בכלל ובפרק זה במיוחד מסתמך על מסגרת רעיונית שפיתחנו בדוח מדיניות קודם, שם טענו שכדי להבין את ההיבטים המשפטיים של מערכות מבוססות-מידע, יש ללמוד אותן בתוך ההקשר הרחב שבו הן פועלות.[1] גישה מחקרית זו ממוסגרת בתוך השיח ובתוך פרדיגמת המחקר של "משפט וטכנולוגיה". מדובר בגישה מחקרית שעֵרה לקשר המורכב שבין משפט לטכנולוגיה, והגורסת שהמשפט לבדו, או הטכנולוגיה לבדה, אינם יכולים למגר את תופעת הספאם בכוחות עצמם. גם בספרות המחקרית העוסקת בספאם משתרשת ההבנה שעל מנת להתמודד עם התופעה באופן אפקטיבי נדרש שילוב של כלים טכנולוגיים עם חוקים ומדיניות משפטית עדכניים.[2]

סביבות המידע בהן מועברים מסרים אלקטרוניים הן סביבות מורכבות, מרובות זרמי מידע ומרובות שחקנים המעורבים בזירת הספאם. בפרקים הקודמים מיפינו את השחקנים השונים ואת האינטרסים שלהם, וניתחנו את המפה המשפטית והטכנולוגית. כל אלה הניחו תשתית לאיתור נקודות במערכת בהן התערבות רגולטורית, טכנולוגית, או משולבת – תהיה מיטבית. כמו כן, התשתית שהונחה בפרקים הקודמים נועדה להקל על ניתוח של פתרונות אפשריים, ולהצביע על יתרונות וחסרונות באופן מושכל.

פרק זה קושר בין כל המרכיבים שנדונו עד כה: הבנת שרשרת הספאם בכלל, הפנים הטכנולוגי והכלכלי שלה, מיפוי השחקנים השונים בזירת הספאם, וההיבט המשפטי של הפעילות בזירה וההיבט הטכנולוגי שלה, ומציע דרכי פעולה למעצבי המדיניות ומקבלי ההחלטות. נפתח בהסבר וניתוח הממשק שבין המשפט לטכנולוגיה בזירת הספאם. בהמשך, הפרק בוחן ומנתח את הצמתים הטכנולוגיים האפשריים בהם לא קיימת עדיין התערבות משפטית, אך התערבות כזו עשויה להיות יעילה. באופן משלים, הפרק דן בהטלת חבות משפטית על שחקנים בשרשרת הספאם שפעילותם הנוכחית אינה מוסדרת. מכאן עולות המלצות מדיניות קונקרטיות.

2. התערבות משולבת: לפני ואחרי מעשה

א. פתרונות לפני מעשה (*ex ante*): הנדסת ניקיון

חלק זה מתמקד בבחינת פתרונות שמשלבים חשיבה משפטית וטכנולוגית ומבקשים להתערב בנעשה בזירה בטרם מעשה (*ex ante*). אנו מכנים פתרונות אלה בשם "הנדסת ניקיון": הטמעה מראש של עקרונות וערכים רצויים בטכנולוגיה שנועדה להתמודד עם ספאם, עוד בשלבי העיצוב הטכנולוגי. תכנון מוקדם של טכנולוגיה על מנת לסייע בשמירה על "ניקיון" המערכת האקולוגית התקשורתית, כדי לצמצם פעילות של דואר זבל לא חוקי, הוא התוצאה המתבקשת של תובנות הגישה המחקרית של "משפט וטכנולוגיה" המקדמת הטמעת ערכים רצויים בטכנולוגיות עוד בשלב העיצוב שלהן.[3] להנדסת הניקיון שני מרכיבים, האחד, הוא הרעיון של השפעה משפטית על תכנון המערכות (וזה

1 ראו מיכאל בירנהק ומיקי זר "עקרונות פעולה משפטיים לפיתוח טכנולוגיות לאיתור מגעים" (דוח מדיניות עבור משרד המדע והטכנולוגיה, 2020), נמצא ב: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3683166.

2 Roderic Broadhurst & Mamoun Alazab, *Spam and Crime*, *in* Regulatory Theory, Foundations and Applications 517, 527 (Peter Drahos, ed., 2017).

3 ראו Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (2011) וגם Mickey Zar & Niva Elkin-Koren, *The By-Design Approach Revisited: Lessons from COVID-19 Contact Tracing Apps*, 33 Intell. Prop., Media & Ent. L.J. 635, 640-645 (2023).

מרכיב ה"הנדסה"), והשני, הוא מרכיב "הניקיון". זו מטפורה מארגנת, שמסייעת לנו להאיר היבטים שנותרו סמויים עד כה.

(1) הנדסה ערכית

פתרונות משפטיים פועלים בדרך כלל באופן של איסור או היתר מראש להתנהג באופן מסוים, כלומר באופן שמבקש להתערב לפני מעשה, ובאופן של הטלת סנקציה על פעולה שלא בהתאם לחוק, כלומר באופן שמבקש להתערב לאחר מעשה (*ex post*). בתחום הגנת הפרטיות, גישה זו נקראת "הנדסת פרטיות" (Privacy by-Design) וכבר הפכה מקובלת, גם אם לא תמיד קלה ליישום. גישה זו מבקשת לשלב את ההגנה על הפרטיות בתוך מערכת טכנולוגית כלשהי כבר בשלב בו מפתחים את המערכת, ולא רק בדיעבד. הרעיון של הנדסת פרטיות הוא גיוס הטכנולוגיה להסדרת ההתנהגות בה מדובר, ושילוב והטמעה של הגנת הפרטיות בטכנולוגיה, כבר בשלב התכנון והעיצוב שלה, ולא בניסיון בדיעבד, שהוא בדרך כלל מסורבל, יקר ולעיתים קרובות נכשל.[4]

הרעיון של הנדסת פרטיות התגבש ובהדרגה זכה להכרה בין-לאומית ומשפטית.[5] דוח של רשות הסחר האמריקנית (Federal Trade Commission – FTC) משנת 2012 בנושא הגנת הפרטיות במידע, המליץ לתאגידים לאמץ את הגישה של הנדסת פרטיות.[6] דיני האיחוד האירופי אימצו את הנדסת פרטיות, והפכו אותה לחובה משפטית ב-GD-PR.[7] גם בישראל יש ניצנים להטלת חובה כזו, בפסיקה של בית המשפט לעניינים מנהליים, לפחות בקשר לרשויות המנהל.[8] בפועל, הנדסת הפרטיות נתקלת בקשיים שונים, למשל הקושי לתרגם מונחים ורעיונות משפטיים לשפה הנדסית,[9] והאתגר לשכנע את התאגידים תאבי המידע להטמיע גישה כזו, שעלותה בצידה.

(2) מטפורת הניקיון

נקדים כמה מילים על מטפורת ה"ניקיון" בהקשר של ספאם. נזכיר ש"ספאם" הוא הכינוי הרווח והמקובל לדואר "זבל". השימוש שנעשה במטפורות של זבל ואשפה ביחס למסרים לא רצויים, כבר מימיה הראשונים של התקשורת האלקטרונית, מזמין את השימוש במטפורה המקבילה, של ניקיון, כתגובה הראויה. ניקיון מצביע על סביבה שאין בה מסרים לא רצויים כאלה. מטפורת ה"ניקיון" היא כלי מארגן שנועד להאיר היבטים שונים של תופעת הספאם (מהו "זבל" לא רצוי, מהו פרסום לגיטימי שאינו "זבל", מה נדרש על מנת "לנקות" את המערכת, וכדומה). ככל מטפורה, מטפורת ה"זבל" ומקבילתה, מטפורת ה"ניקיון", עשויות לאפשר השוואות ולהבין היבטים חדשים של תופעה, אך ככל מטפורה יש להן מגבלות.[10] למשל, לעיתים הן משרתות אינטרסים מסוימים אך מטשטשות אינטרסים אחרים. לעיתים הן משכיחות היבטים חשובים של התופעה שאותה הן מנסות להאיר.

למקרים ספציפיים של הנדסת פרטיות ראו מיכאל בירנהק "הנדסת פרטיות ציבורית: המקרה של העברת מידע ממרשם האוכלוסין למפלגות" **דין ודברים** יב 15 (2019); מיכאל בירנהק "פרטיות במשבר: הנדסה חוקתית והנדסת פרטיות" **משפט וממשל** כד 149, 172-176 (2022).

4 הפסקאות הבאות מבוססות על דיון אצל מיכאל בירנהק "פרטיות בעיר הדיגיטלית", **מחקרי משפט** לד 911 (2022).

5 תפקיד מרכזי בקידום הרעיון של הנדסת הפרטיות מילאה נציבת הגנת המידע והפרטיות של אונטריו, קנדה, אן קאבוקיאן (Cavoukian). במשך שנים רבות פעלה לקדם את הרעיון, ומאמציה זכו להצלחה. ההצהרה המסכמת של הכנס הבין-לאומי השנתי של נציבי הגנת הפרטיות בעולם שנערך בירושלים בשנת 2010, הוקדשה להנדסת הפרטיות, והכריזה על הנדסת הפרטיות כמרכיב חיוני בהגנת הפרטיות. הפורום הכריז ש "Privacy by Design [ ] an essential component of fundamental privacy protection". ראו: 32nd International Conference of Data Protection and Privacy Commissioners (Jerusalem, 29 October 2010).

6 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012), בעמ' 22. נמצא ב: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

7 ס' 25 ל-GDPR מטיל חובה על הגורם ששולט במידע (data controller) להטמיע אמצעים טכנולוגיים וארגוניים מתאימים ואפקטיביים הן בשלב תכנון המערכת והן בשלב עיבוד המידע.

8 הרעיון של הנדסת פרטיות אומץ כעיקרון משפטי מחייב בפסק דין של בית המשפט המחוזי בתל אביב שניתן ביולי 2019, ראו עת"מ (מנהלי ת"א) 28857-06-17 **עמותת חברות הסיעוד נ' משרד הביטחון** (1.7.2019).

9 לדיון, ראו למשל: Michael Birnhack, Eran Toch, Irit Hadar) Privacy Mindset, Technological Mindset, 55 Jurimetrics 55 (2014); Irit Hadar, et al, Privacy by Designers: Software Developers' Privacy Mindset, 23 Empirical Software Engineering 259 (2018).

10 לדיון עשיר ופורץ דרך על תפקידן של מטפורות ככלי מארגן המאפשר לנו להמשיג ולהבין חוויות מופשטות, וכן על מוגבלותן של מטפורות לעניין זה, ראו: George Lakoff & Mark Johnson, Metaphors We Live By (1980).

האופן שבו אנו מתייחסים לפסולת חושף במידה רבה את האופן בו אנו חיים ואת הערכים הרווחים בחברה לרבות בנוגע לכלכלה האחראית על ייצור הפסולת.[11] צריכה ופסולת הצריכה הולכות יד ביד; פסולת כ"בעיה" היא תולדה ישירה של חברה שבה מתקיימים ייצור וצריכה בקנה מידה גדול.[12] היבט חשוב של תופעת הספאם הוא שהיא חלק ממערכת גדולה יותר של כלכלת ייצור מסרים המוניים, ולכן אי אפשר להתייחס אליה כאל בעיה שיש להיפטר ממנה אחת ולתמיד, אלא להבין שבכלכלת מידע המבוססת על הצפת מידע, ספאם הוא חלק בלתי נמנע מהמערכת כולה. אין פירושו של דבר שאין מה לעשות, או שכדאי לוותר על התמודדות עם ספאם; פירוש הדבר הוא שמוטב לאמץ הבנה ולפיה מדובר בתופעה שלא ניתן למגר כליל כל עוד לא מתמודדים עם תופעת הצפת המידע עצמה – התמודדות שחורגת מתחומו של דוח זה – ולכן, לעת עתה, כדאי להתמקד בפתרונות ארוכי טווח שיצמצמו את התופעה ואת השלכותיה מתוך ידיעה שתופעת הספאם תישאר איתנו. לשם כך, יש לאמץ גישות המשלבות בין הפוליטי, הכלכלי, הטכנולוגי והמשפטי. לשם השוואה, בדיון על האתיקה של פסולת בהקשר האקולוגי, טענה חוקרת המדע והטכנולוגיה הלנה מתאוס ג'ירונימו (Mateus Jerónimo) ש"האמונה לפי אפשר לתקן את 'בעיית' הפסולת באמצעים טכניים בלבד היא אשליה טהורה", והוסיפה שהתמודדות יעילה עם הבעיה תלויה, בנוסף להיבט הטכנולוגי, בגישות המשלבות את החברתי, הכלכלי והפוליטי.[13]

בספר "טוהר וסכנה" שהתפרסם בשנת 1966 ניתחה האנתרופולוגית מרי דגלס (Douglas) את מושגי הטומאה והלכלוך ואת יסודותיהם התרבותיים.[14] לטענת דגלס, מה שנחשב לכלוך בחברה נתונה הוא כל מה שאינו במקומו, והפרשנות לכך תלויה בהקשר תרבותי: "טומאה אף פעם אינה אירוע מבודד. היא אינה יכולה להתרחש אלא לאור סידור שיטתי של מושגים. לפיכך, כל פרשנות חלקית לחוקי זיהום של תרבות אחרת נדונה מראש לכישלון, שהרי הדרך היחידה להבין את ההיגיון של מושגי זיהום היא מתוך התייחסות למבנה חשיבה כולל, שהיחסים בין אבני היסוד שלו, גבולותיו, תחומיו ומתחמיו הפנימיים לבין עצמם מוגדרים על-ידי טקסי הפרדה."[15]

תפיסות לגבי לכלוך וניקיון נבנות בתוך הקשר תרבותי והיסטורי. לכלוך, לטענת דגלס, הוא תוצאה של חריגה מגבולות הסדר, של יציאה מגבולותיו של הארגון החברתי. מן הצד השני, הימצאותו של לכלוך מעידה על קיומה של שיטה, משום שהלכלוך הוא תוצר הלוואי של סדר ושל סיווג שיטתי של חומר, כאשר סדר משמעו דחייה של אלמנטים לא הולמים. לפי חוקר הספרות ג'ונתן קאלר (Culler), דגלס מראה שלכלוך הוא ראיה חיונית למבנה הכולל של החשיבה בתרבות. זאת משום שלכלוך היא קטגוריה כוללנית, המכילה כל דבר שאינו במקומו. לפיכך, לחקור מה נחשב ללכלוך בחברה נתונה מסייע לזהות את הקטגוריות של המערכת.[16] כך, לטענת קאלר, מה שנחשב שולי או טאבו הופך לחיוני ללימוד המערכת שמחריגה אותו.[17]

זבל הוא תופעת לוואי בלתי נמנעת של חברת הצריכה. אנו חיים בחברה צרכנית שצדה האחר הוא פסולת הצריכה. ככל שמתרבה הייצור, מתרבה גם הזבל. בעוד שניקיון מקביל לסדר וצורה, הלכלוך משול לחוסר סדר והיעדר צורה. כאשר לכלוך ואשפה מתרבים ונוכחותם הופכת לדומיננטית, נוצר איום על הסדר במערכות החיים השונות, לרבות על הסדר של מערכות מידע.[18] במילים אחרות, כאשר המערכת מבקשת לדחות מתוכה את היסודות הלא "ראויים", היא מכנה אותם לכלוך או אשפה. פסולת – וניקיון, הם חלק בלתי נפרד ממעגל החיים המודרני. אנו מבקשים לחיות בסביבה נקייה וטורחים על כך מראש, כדי לשמור על היגיינה אישית בה אנו רואים גורם חשוב במניעת מחלות, ועל היגיינה של סביבת החיים שלנו בכלל, אותה למדנו לראות כאסתטית יותר ככל שהיא נקייה יותר. אנחנו מבקשים להימנע מלכלוך וגם לנקות לכלוך לאחר שנוצר, ולשם כך פיתחנו תעשיות שלמות סביב ניקיון: מוצרי ניקיון, שירותי ניקיון, הפרדה ומחזור סוגים שונים של זבל, שינוע של הזבל, מתקנים למחזור, הפקת אנרגיה מזבל, ועוד שיטות שונות

---

11 ראו באופן כללי על הקשר בין טכנולוגיה לבין ערכים אקולוגיים: Helena Mateus Jerónimo, *Technology and Ecological Values: Confronting Normal Waste as Unavoidable Matter in Modern Society, in* New Perspectives on Technology, Values and Ethics 183 (Wenceslao J. Gonzalez ed., 2015).

12 שם, בעמ' 184.

13 שם.

14 מרי דגלס **טוהר וסכנה: ניתוח של המושגים זיהום וטאבו** (יעל סלע מתרגמת, 2004).

15 שם, בעמ' 67.

16 Jonathan Culler, *Rubbish Theory, in* Framing the Sign: Criticism and its Institutions, 168, 168 (1988).

17 Culler, שם, בעמ' 169.

18 ראו דוד גורביץ', דן ערב "זבל, טראש" **אנציקלופדיה של הרעיונות**, נמצא ב: https://haraayonot.com/idea/junk.

לטיפול בו. יש לנו מסגרת חשיבה שלמה שמזהה ניקיון, עם היגיינה, עם אורח חיים בריא, מודרני, "נכון", מתקדם, שמבדל אותנו מכל מה שאינו נקי – חפצים, חומרים, חיות ובני אדם לא נקיים. כחלק ממסגרת החשיבה הזו, המלוכלך הוא "רע", והנקי – "טוב".

גם המשפט מתגייס לטפח את הניקיון, לעיתים במישרין, בנוגע לבריאות הציבור,[19] לעיתים בדרך של הסדרת כללים בקשר לניקיון,[20] נקיטת אמצעים למזעור הזבל מלכתחילה,[21] ולעיתים בדרך עקיפה, באמצעות דיני המטרדים.[22] בדומה, גם הטכנולוגיה מתגייסת להתמודד עם נושא הזבל. פתרונות שונים של מחזור (למשל, של נייר, זכוכית, פלסטיק) הם התגובה הטכנולוגית הבולטת לבעיה, כמו גם פתרונות של הפקת אנרגיה מזבל, או פיתוח מוצרים שמלכתחילה מייצרים פחות זבל, כמו שקיות מחומר מתכלה.

כפי שלכלוך, לטענת קאלה, מעיד על קיומה של השיטה בה הוא החריג, ולכן חקירה של לכלוך מאפשרת לימוד של המערכת בכללותה, אנו סבורים שלימוד תופעת הספאם, שהוא סוג מרכזי של פסולת שנוצרת כתוצאה מפעילותנו הווירטואלית, חיוני ללימוד ולהבנת המערכת הכוללת של זירת המידע. האם הפסולת הפיזית דומה לפסולת הווירטואלית? או במילים אחרות, האם הידע והתובנות שנצברו בקשר לניקיון פיזי יכולים לשמש מטפורה מתאימה לסביבה שבה אין חומר שמזהם את האוויר או הקרקע, שאין לו ריח, ואינו מהווה מכשול בדרך?

הדמיון העיקרי הוא בנזק. למרות שפסולת וירטואלית אינה נערמת לנגד עינינו ומפיצה ריחות רעים, פוטנציאל הנזק שלה רב: עבור הפרט, מדובר באובדן של זמן בטיפול בפסולת כזו, אובדן של שקט נפשי בהתמודדות עם תכניה, וגם בסכנה ממשית של נפילה בפח שטמנו נוכלים או גורמים עוינים. הזבל נתפס חברתית ותרבותית כיסוד לא יצרני ואפילו כיסוד החותר תחת יצרנות, ולכן חברה שמאורגנת סביב ייצור קפיטליסטי תחתור למזער את השפעת הזבל עליה ואם אפשר להקיא את הזבל מקרבה. לחילופין, היא תנסה להעניק לזבל ערך מחודש. לפי חוקר התרבות מייקל תומפסון (Thompson), קיימת זיקה בין מושג הזבל למושג הערך, כאשר לזבל אין ערך הן מבחינה כלכלית טהורה והן מבחינה סימבולית.[23] בהתאם, מחזור זבל הוא פעולה שנועדה להשיב לזבל "ערך". אלא בשונה מפסולת "פיזית", אין רווח במחזור פסולת וירטואלית. זאת משום שבעוד שפסולת פיזית נוצרת כחלק ממחזור החיים והבלאי הבלתי נמנע של תוצריהם, ולכן סימנים של חומר חיוני עדיין יכולים להימצא בה, הפסולת הווירטואלית נוצרת במכוון ומראש כפסולת. לכן, ההטיה המוסרית לרעת הפסולת ומי שמייצר אותה מוצדקת יותר במקרה של פסולת וירטואלית.

המטפורה של הנדסת ניקיון מסייעת לנו לזהות אתגרים שיש בספאם, ואפילו אפיקי פעולה. למשל, אחד הקשיים שעמדנו עליהם בנוגע להגנה מפני ספאם, הוא הפערים המשמעותיים במידת האוריינות הדיגיטלית בין משתמשי קצה של הטכנולוגיה. פערים אלה מייצרים גם פערים משמעותיים בין משתמשים בנוגע למידת ההגנה מפני ספאם שכל משתמש יכול לדאוג לה עבור עצמו. כפי שהזכרנו כבר בפרק המבוא, לכל שימוש בטכנולוגיה יש היבטים חלוקתיים, והבדלים בין אזרחים ואוכלוסיות עלולים להיות משועתקים מהסביבה הפיזית לסביבה המקוונת. בענייננו, חשוב לזכור שלא לכל האוכלוסייה יש מכשיר סלולרי או מחשב, ולאלו שיש – לא לכולם אוריינות טכנולוגית מספקת לשם הבנת פתרונות שונים ויישומם. בהתאם, מטפורת הניקיון יכולה לסייע בשלבי ההקניה של אוריינות טכנולוגית בנוגע לספאם, באמצעות "גיוס" עולם הקונוטציות המוכר הנוגע להיגיינה ולרווחים החיוביים למי ששומר עליה – לטובת הבנה של נזקי הספאם ולמידת דרכי התגוננות מפניהם. מטפורת הניקיון גם מסייעת להבין את החשש הגדול של חלק מבעלי מסרים מפני תיוג שלילי כספאמר: מה שנחשב למלכלך מתויג כשלילי וכזר למערכת הנקייה וה"בריאה". תיוג שלילי הנובע למשל מאסדרת יתר של פעילות בעלי המסרים, יפגע בפעילותם התקינה וכמו כל סטיגמה, הוא כתם קשה להסרה.

19 ראו ס' 16 לפקודת בריאות העם מס' 40 לשנת 1940 ("המנהל או רופא ממשלתי או מפקח רשאי בכל עת מתאמת להכנס לכל בית או מקום שבו אירע מקרה של מחלה מידבקת ורשאי הוא להוציא לפועל או לצוות להוציא לפועל כל פעולת חיטוי או כל פעולה להשמדת עכברים או משחיתים אחרים אשר, לדעתו, יש צורך בה."), וכן חלק ו ("הוראות בדבר מפגעים"), ובפרט ס' 57 ("הנחת כל זבל, בין זבל בהמות, ובין זבל מינרלי או זבל צמחים או כל פרש בכל רחוב, או שפיכת מים או נוזל מכל בית לכל רחוב, תהא עבירה עפ"י פקודה זו ותהיה בכך גרימת מפגע לענין חלק זה.")

20 ראו חוק איסוף ופינוי פסולת למיחזור, התשנ"ג-1993; חוק שמירת הנקיון, התשמ"ד-1984.

21 למשל המס שמוטל על שקיות ניילון, שנועד לעודד שימוש בסלים רב פעמיים. ראו החוק לצמצום השימוש בשקיות נשיאה חד-פעמיות, התשע"ו-2016.

22 ראו החוק למניעת מפגעים סביבתיים (תביעות אזרחיות), התשנ"ב-1992.

23 Michael Thompson, Rubbish Theory: The Creation and Destruction of Value (1979).

בנוסף, בעיצוב מדיניות כוללת יש להביא בחשבון את הפריסה הלא אחידה של טכנולוגיות חסימה שונות, את הרמות השונות של פגיעות אצל אוכלוסיות יעד שונות, את הפערים באוריינות הטכנולוגית של משתמשי הטכנולוגיות, ולשקול שיקולים אלה במכלול השיקולים בהתמודדות עם בעיית הספאם. טכנולוגיות להגנה מפני ספאם קיימות. אמצעים טכנולוגיים שונים מוצעים למשתמשים, שיכולים לבחור האם לאמצם ולהשתמש בהם כדי להתגונן מפני ספאם. השימוש בטכנולוגיות כאלה תלוי במשתמשים: עליהם לדעת מהו ספאם וממה עליהם להתגונן, עליהם לדעת שיש פתרונות טכנולוגיים, לאתרם, ולהשתמש בהם. כלומר, טכנולוגיות אנטי-ספאם כאלה מתאימות לקבוצה מיודעת ומתוחכמת יחסית של משתמשים. האחרים נותרים חשופים.[24]

לעומת זאת, "הנדסת-ניקיון", או הנדסה-מראש של פתרונות טכנולוגיים המתמודדים עם ספאם, מסיטה את כובד המשקל ממשתמשת-הקצה אל המפתחת. במקום שהמשתמשת תנסה לאתר פתרונות בעצמה, הטכנולוגיה תעוצב מראש כך שהפגיעה תמוזער. באופן זה, ההגנה מפני ספאם אינה תלויה באוריינות הדיגיטלית של המשתמשת, וכך גם נמנעים קשיים בדיעבד. הדבר דומה לניקיון: כל אדם דואג לניקיון ביתו שלו, אבל יש לנו מערכות ציבוריות שנועדו לדאוג לניקיון המרחב הציבורי והשירותים הציבוריים השונים – בין היתר לדאוג לניקיון המים שאנחנו שותים, המזון שאנחנו אוכלים מחוץ לבית או שנמכר בחנויות. כשם שהאחריות על הניקיון איננה מופרטת במלואה לאזרחים, וחלק גדול ממנה מאורגן באופן ציבורי, כך גם ניקיון הרשת מספאם.

לכן, אי אפשר להסתמך רק על פעולה עצמאית של משתמשי הקצה למיגור הספאם. על תעשיית המחשוב בפרט, אבל גם על המדינה, לכונן מדיניות ותכניות מחקר שיתמודדו עם תופעת הספאם. על תכנון מדיניות בתחום הספאם להביא בחשבון את העובדה שמדובר במרוץ חימוש אינסופי, בו כל טכנולוגיית אנטי-ספאם חדשה מביאה ספאמרים לחפש – ובדרך כלל גם למצוא – דרכים חדשות לעקוף אותה ולהוסיף להפיץ ספאם. אכן, טכנולוגיות אנטי-ספאם הם פתרונות שבדיעבד, והם חלק ממרוץ החימוש הטכנולוגי. לעומת זאת, פתרונות מקדימים יבקשו לתכנן טכנולוגיה במחשבה מראש על שימושים לרעה, ובכך לבנות מראש הגנה לתוך הטכנולוגיה עצמה.[25] הדבר נכון הן בנוגע לפרקטיקות חדשות של העברת מסרים (כמו הודעות מהירות ברשתות חברתיות כמו וואטסאפ, וכדומה) והן בנוגע לכלים חדשים לשליחה וקבלה של מסרים (כמו "טלפון חכם", מחשב נישא וכדומה).

אחד האפיקים המבטיחים עליהם הצבענו בפרק ד הוא הטמעת טכנולוגיות בלוקצ'יין במערכות טכנולוגיות, באופן שיתגבר על הקושי באמצעים מהימנים לאימות זהות (אותנטיקציה) של שחקנים ושל פעולות במערכות המידע. טכנולוגיות בלוקצ'יין עשויות לאפשר זיהוי ואימות אמין של זהויות, לרבות זהויות וירטואליות, ובאופן זה למנוע צורות שונות של ספאם או לכל הפחות למתן את היקפיו.[26] עם זאת, אנו סבורים שבדומה לזירות טכנולוגיות נוספות, להנדסת ניקיון יש סיכוי טוב יותר להצליח במגזר הציבורי. בדוח קודם, בקשר לטכנולוגיות לאיתור מגעים של נשאי קורונה, עמדנו על כך שבתחום הגנת הפרטיות, ל"הנדסת פרטיות" יש יתרונות וסיכויי הצלחה טובים במיוחד במגזר הציבורי. הצבענו על כך ש"הרעיון של הנדסת פרטיות נתקל בקשיים ביישומו במגזר הפרטי, מטעמים שונים: קושי להגדיר את הפרטיות בקונקרטיזציה מספקת; התנגדות של עסקים מבוססי-מידע; פערי שיח בין עולם המשפט לעולם ההנדסה, ואתגרים טכנולוגיים של יישום. עם זאת, במגזר הציבורי יש לרעיון הנדסת הפרטיות סיכוי טוב יותר להצליח..."[27]

לפיכך, אנו ממליצים לפעול ראשית במגזר הציבורי, באמצעות הטמעת עקרונות של הנדסת ניקיון במערכות המידע המשמשות במגזר הציבורי. לאחר שייצבר ידע מספיק בנוגע להטמעה, כדאי יהיה לנסות ולהטמיע את המסקנות בבנייה מוקדמת של טכנולוגיות במגזר הפרטי.

---

24 ההשוואה כאן מבוססת על השוואה דומה שערכנו בדוח איתור מגעים, בין טכנולוגיות מגבירות פרטיות להנדסת פרטיות; ראו בירנהק וזר, "עקרונות פעולה משפטיים לפיתוח טכנולוגיות לאיתור מגעים", לעיל ה"ש 1, בעמ' 20-21.

25 להמלצה ברוח דומה אך ללא ההסבר הטרמינולוגי, ראו Emilio Ferrara, *The History of Digital Spam*, 62.8 Communications of the ACM 90-91 (2019).

26 על כך, ראו שם, בעמ' 90-91.

27 הסיבות שמנינו הן: "המדינה ורשויותיה כפופות לחובות שלפי חוק היסוד, ובכלל זה, כפי שראינו, החובה לכבד את הזכות לפרטיות. לכן, סוגית הפרטיות אינה זרה למדינה, ואמורה להיכלל כשיקול רלוונטי בעת עיצוב מדיניות וקבלת החלטות. במדינה יש מומחיות בקשר להגנת הפרטיות, ובישראל, הרשות להגנת הפרטיות שפיתחה מומחיות וניסיון בקשר להנדסת פרטיות. בנוסף, החסמים של השיקולים העסקיים אינם קיימים במדינה. אמנם, שיקול תקציבי הוא חשוב, אבל אין מטרת רווח כמו בגוף פרטי." ראו בירנהק וזר, "עקרונות פעולה משפטיים לפיתוח טכנולוגיות לאיתור מגעים", לעיל ה"ש 1, בעמ' 22.

ב. פתרונות לאחר מעשה (ex post): "ספאם אוף" כמשל

על פתרונות נוספים שמשלבים חשיבה משפטית וטכנולוגית – הפעם בדיעבד – אפשר ללמוד מהדוגמה של חברת "ספאם אוף". כאשר דנו בפעילותה של החברה בפרק ב, ציינו שהמיזם היה שילוב של כלים משפטיים וטכנולוגיים, שנועד לתת מענה לכשל שוק בתחום תביעות הספאם. במונחיה של המטפורה המארגנת של הניקיון, חברת "ספאם אוף" הייתה קבלן פרטי שביקש להילחם במזהמים ולרפא כשל במערך האכיפה נגדם, בכך שסייע לנפגעים למצות את הדין עם מפיצי הפסולת.

למרות שהחוק קובע פיצוי סטטוטורי לנפגעי הספאם בתקווה שנפגעים יתבעו ובכך תיווצר הרתעה, ולמרות שלאורך השנים הוגשו רבבות תביעות, עדיין, רוב נפגעי הספאם אינם משתמשים בכלי המשפטי ואינם תובעים. הליך התביעות הקטנות אמור להיות נגיש, פשוט וזול, ואכן, הוגשו רבבות תביעות במהלך השנים, אולם עדיין, ההליך אינו נגיש לנפגעי ספאם רבים. השלב הראשון בתביעת ספאם הוא איתור מקור ההודעה. לא כל המפרסמים הם חברות לגיטימיות שניתן בקלות לאתר את זהותן, וחלקן לדוגמה משתמשות במספרי טלפון לא מקומיים כדי לעקוף את איום התביעה. חברת "ספאם אוף" איפשרה שליחת צילום מסך של הודעת הספאם, בדקה את מקור השולח והסיקה האם המקרה עמד באמות המידה שעל פיהן ניתן לתבוע פיצוי. לחברה היה מאגר מידע של פרטי ספאמרים, ובסופו של תהליך הבירור הוכן (באופן אוטומטי) כתב תביעה להגשה לבית המשפט לתביעות קטנות. בקצרה, חברת "ספאם אוף" סייעה לנפגעי ספאם להתגבר על חלק מהמכשולים בפני הגשת תביעה בשני אופנים עיקריים: 1. בכך שסייעה לאתר את מקור ההודעות המְפֵרות, שאחרת הנפגע לא יכול היה לממש את זכותו ולתבוע; 2. בכך שהפכה את התהליך לאוטומטי בחלקו. זאת למרות שהחברה לא הביאה פיתוח טכנולוגי פורץ דרך, אלא השתמשה בטכנולוגיות פשוטות ומוכרות באותה עת, כמו צילומי מסך או טפסים ממוחשבים, על מנת לייעל את התהליך.

אנו סבורים שחברת "ספאם אוף" הכניסה מספר חידושים ראויים שהיטו את המאזן לטובת נפגעי הספאם. החידושים העיקריים היו, ראשית, אוטומציה של הליך התביעה; שנית, אסטרטגיית פעולה שחילקה תביעת ספאם להרבה מאוד תביעות קטנות ש"הציקו" לגורם השולח (בתמונת ראי של הספאם עצמו); ושלישית, תביעה נגד נושאי משרה בחברות שהפיצו ספאם. בשילוב כל אלה יחדיו, "ספאם אוף" הדגימה פתרון שמשלב את ההיבטים המשפטיים עם ההיבטים הטכנולוגיים של ההתמודדות עם ספאם.

באשר לאפשרות זיהוי השולח והעלויות הנלוות לצורך הגשת תביעה – חברת "ספאם אוף" נתנה מענה לנפגעי ספאם רבים. דרך נוספת, כפי שציינו בפרק ג, עשויה להימצא בהצעת החוק שהזכרנו לעניין חיוב חברות הפצה לחשוף שמות של לקוחות מפרים.[28] מענה מסוג זה יצטרך להביא בחשבון את האתגר שבחשיפת שמות לקוחות. לדוגמה, חברה ששמה ייחשף למרות שלא הייתה אחראית להפצת ספאם, תוכל לתבוע את חברת ההפצה בגין לשון הרע.

כפי שתיארנו בפרק ב בדיון בפעילותה של חברת "ספאם אוף", במהלך תקופת הפעילות של החברה היא העלתה עליה את קצפם של עורכי דין שסברו שהיא מסיגה את גבולות מקצוע עריכת הדין. החברה גם העלתה את כעסם של שופטים שסברו שהיא מבקשת להתעשר באמצעות נגיסה בתשלומי הפיצויים של תובעים, וכן שמעורבותה של החברה יוצרת "כשל שוק" המפר את האיזון שביקשו המחוקק ובתי המשפט לערוך, בין הרתעת חברות ועסקים מלשלוח הודעות ספאם מפרות לבין מיטוט עסקים קטנים אשר מעדו באופן נקודתי או ממוקד. עוד סברו בתי המשפט שפעילות החברה מייצרת עומס חריג – ומיותר - על בתי המשפט לתביעות קטנות, מה שמקשה עליהם למלא את ייעודם, ופוגע בציבור בכללותו, ובלקוחות החברה המגיעים תכופות לא מוכנים לבית המשפט.[29] אלא שריבוי התביעות בעת פעילות החברה עשוי להעיד על כך שפעילותה עזרה לקדם נגישות להליכים משפטיים, וזאת בעזרת אוטומציה של שירותים משפטיים. כך סבר גם בית המשפט העליון בפרשת **ארד**, כאשר קבע כי פעילותה של ספאם אוף עומדת בדרישות החוק,[30] משום שהתכלית של החברה עלתה בקנה אחד עם מהות מוסד התביעות הקטנות, שהיא פתיחת שערי המשפט בפני האזרח הקטן, כדי לאפשר כלי מהיר, זול וזמין לבירור תביעות בהיקף כספי מצומצם לשם מיצוי זכויות. כאמור, עד שניתן פסק הדין בעניינה, החברה כבר הפסיקה את פעילותה. על כך יש להצר.

28 הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התשפ"ג-2022 (פ/25/276).

29 ראו ת"ק (חד') 42711-03-17 **זיסו נ' המרכז הישראלי ל.ע. ברשת בע"מ** (נבו 19.8.2017), בפס' 13; ת"ק (עכו) 48592-12-16 **יעקובוב נ' אל.טי. - פאוור טכנולוג'יס בע"מ** (נבו 5.4.2017), בפס' 3-4.

30 רע"א 7064/17 **ארד נ' מנקס אונליין טריידינג בע"מ** (נבו 11.12.2018).

חשוב להדגיש כי מכיוון שפסולת היא חלק בלתי נפרד ממעגל הייצור והצריכה, פתרונות של הנדסת ניקיון יוכלו לשפר את ניקיון המערכת באופן כללי, אך לא להביא למיגור סופי ומוחלט של פסולת. לכן, אנו סבורים שיש חשיבות גדולה גם ליצירה של פתרונות ניקיון שבדיעבד, באמצעות שיפור כלי האכיפה של החוק וסיוע לנפגעי ספאם לממש את זכויותיהם.

בהתאם, אנו סבורים שלא היה מקום ליחס העוין של בתי המשפט לחברה ולמי שנעזרו בשירותיה.[31] החברה זיהתה כשל שוק מסוים בנגישות לערכאות, הציעה פתרונות, ובכך פעלה לממש את תכלית החוק. אכן, לפעילות הזו היו השלכות, ובין היתר הכבדה של העומס על בתי המשפט. עומס זה נובע מהבחירה של המחוקק, להפריט את האכיפה. למעשה, פעילות החברה הקדימה את התחום של Legal Tech, של שימוש בטכנולוגיות לפתרונות משפטיים.[32] מובן שפעילות של "קבלן ניקיון" מסוג זה צריכה להיעשות ביעילות, להגיב לטכנולוגיות ספאם חדשות, להיזהר לא לפגוע בפעילות פרסום לגיטימית וחוקית, ולפעול בתוך מסגרת החוק.

3. הטלת חבות משפטית: שחקנים אפשריים

בפרק ב הצגנו ניתוח של שרשרת הערך של הספאם. ניתוחים כלכליים מקובלים של מערכת הספאם רואים בשרשרת הערך יחידת ניתוח נפרדת, שניתנת ללימוד ולהבנה במנותק מהכוחות שפועלים נגדה. בשונה מכך, הניתוח שהצענו יצא מתוך עמדה הוליסטית, שרואה בתופעת הספאם מערכת אקולוגית שמורכבת הן משרשרת הערך של הספאם והן מהכוחות שפועלים נגדה. מערכת זו כוללת, בנוסף לשחקנים האחראים על הפצת ספאם, גם את הצד השני של המטבע – את השחקנים המעורבים במלחמה בספאם. מערכת הספאם היא זירה רבת-משתתפים, בנוסף לשחקני הקצה – המוען והנמענים – יש שורה של גורמי ביניים שמעורבים בשלבים שלפני ההפצה, בהפצה, ובמאבק בספאם. בכל אחת מהחוליות האלה יש סוגים שונים של שחקנים – חלקם מעורב באופן ישיר וחלקם באופן עקיף, חלקם פועל בצורה חוקית ולגיטימית וחלקם פועל בצורה לא חוקית.

ניתוח המערכת שהצגנו נשען על ההנחה שללא הבנה מלאה של המערכת ושל השחקנים שמעורבים בה, מרבית ההתערבויות נגד ספאם עלולות להתמקד בהיבטים מסוימים בלבד, למשל סינון דוא"ל או רשימות שחורות של כתובות אתרים, ולהתעלם מהיבטים אחרים, כמו השלב המקדמי של קצירת כתובות דוא"ל ומספרי טלפון, או שלבי ביניים כמו שימוש בשירותי תיווך לשם הפצת מסרים. בהמשך לכך, טענו שבבחינת פתרונות חדשים במסגרת המאבק למיגור הספאם, יש לזנוח את הגישה הבינארית, שבוחנת רק את המשווק כמוען ואת משתמשי האינטרנט והטלפון כנמענים, ולראות את התמונה הרחבה יותר, שבה שחקנים רבים.

בהמשך, בפרק ג, ניתחנו את ההיבטים המשפטיים של תופעת הספאם, לרבות מערך הזכויות והחבויות המשפטיות של שחקנים שונים בזירה. הצבענו על כך שתיקוני החקיקה מגיבים לשינויים בדפוסי המשלוח של ספאם, להתנהגויות שונות של המפרסמים, וכן לשינויים טכנולוגיים מסוימים. חלק ניכר מהתיקונים פעלו לצד האזרח הנמען - כמו התיקון בדבר המשמעות של סיום התקשרות ממושכת, או התיקון בדבר תופעת ה"צנתוק". חלק מהתיקונים פעלו דווקא לטובת מפרסמים מסוימים – כמו החרגת תעמולה פוליטית. עד כה, המחוקק נמנע מלהגיב לשינויים בדפוסי הפצת המסרים ולתופעה של ריבוי השחקנים השונים בצד ההפצה.

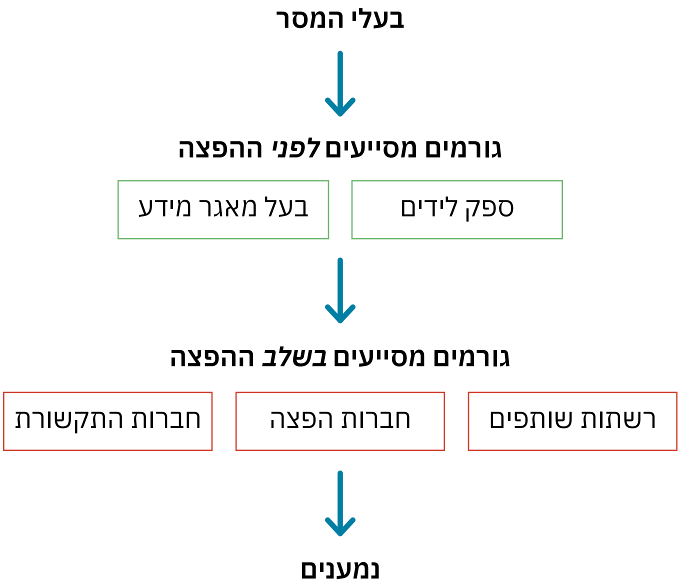
כאשר משלבים בין מסקנות פרק ב שעסק בשחקנים במערכת האקולוגית של הספאם, לבין מסקנות פרק ג שעסק בניתוח המשפטי של המערכת, עולות מספר תובנות והמלצות.

31 ליחס עוין זה, ראו לעיל, פרק ב, בעמ' 38-39.

32 להרחבה על LegalTech, ראו למשל נטע זיו "מי הזיז את העכבר שלי: על הסגת גבול מקצוע עריכת הדין" **עיוני משפט** לט 189 (2016).

א. שחקנים בשרשרת הערך

נזכיר בתמצית את השחקנים שמעורבים בשרשרת הערך של הספאם:



לפי הדין הישראלי הנוכחי, השחקנים העיקריים שנושאים בחבות משפטית הם בעלי המסר, כלומר בעלי עסקים שמבקשים לשווק את עסקיהם ("המפרסם", בלשון החוק),[33] וספקי הלידים, שהם מי שאוסף פרטי קשר – מספרי טלפון, כתובות דוא"ל, וכדומה – של אנשים שידוע או שאפשר לשער שהם מעוניינים בשירות מסוים, וסוחר במאגר המידע שיצר. במקרים בודדים, נוספים על אלה גם חברות ההפצה. זאת למרות שכפי שציינו, כל השחקנים השונים הפועלים בשרשרת הערך (פרט לנמענים) אחראים במידה כזו או אחרת להפצת ספאם.

(1) שלב ראשון – בעלי המסר

לגבי קבוצת בעלי המסרים, ראינו שהיא אינה עשויה מקשה אחת. כאשר בוחנים את זהותם של נתבעי ספאם סדרתיים, מסתבר שאבחנה חשובה בין עסקים היא גודל העסק. כך, בעוד שלתאגידי ענק יש אמצעים משפטיים, כלכליים וטכנולוגיים להתמודד עם תביעות ספאם, הרי שעסק קטן שנתבע בעילה של הפצת ספאם עלול לספוג מכה אנושה, עד כדי סגירה. במילים אחרות, לכלל המשפטי יש השלכה חלוקתית, ויש חשש שפעולתו האחידה של חוק הספאם על כלל בעלי המסר משפיעה באופן לא אחיד על התמריצים של שחקנים שונים.

כאשר הדין פועל באופן אחיד כלפי כל סוגי החברות, התוצאה עשויה להיות הרתעת-חסר כלפי השחקנים הגדולים, מצד אחד, והרתעת-יתר כלפי שחקנים קטנים, מצד שני. שחקן חזק לא יתקשה להתמודד עם תביעות משפטיות, גם אם ייאלץ לשלם מעת לעת. נזכיר את כלכלת הספאם: עלות משלוח הודעה אחידה למשתמשים רבים, נמוכה, ודי במשתמשים בודדים שייענו להצעה המסחרית, כדי לכסות את העלויות, וגם כדי לכסות פיצויים ועלויות משפטיות מעת לעת. במילים אחרות, שחקן חזק עלול לנקוט גישה של הפרה יעילה, כלומר, להפר את החוק במודע, משום שזה יעיל לו יותר לנהוג כך.[34] זו הרתעת החסר. לעומת זאת, שחקן קטן עלול להתמוטט. התוצאה היא הרתעת יתר, כלומר חשש ששחקנים כאלה יימנעו מפעילות שיווקית לגיטימית. תוצאה כזו מחזקת את כוחם של החזקים על חשבון החלשים.

דרך אחת להתמודד עם פער זה היא בשיקול הדעת של בית המשפט בעת קביעת הפיצויים. החוק מציין שיקולים שונים שעל בית המשפט לשקול בעת פסיקת הפיצוי. סעיף 30א(י)(3) לחוק התקשורת מציין את שיקול אכיפת החוק

33 ראו ס' 30א(א) לחוק התקשורת (בזק ושידורים), התשמ"ב-1982 (להלן: חוק הספאם).

34 המושג של הפרה יעילה צמח מתוך דיני החוזים, ראו למשל ד"נ 20/82 **אדרס חומרי בנין בע"מ נ' הרלו אנד ג'ונס ג.מ.ב.ה**, פ"ד מב(1) 221 (1988). להרחבה, ראו עמרי בן שחר ויובל פרוקצ'יה "פרק ד: חוזים" 153, **הגישה הכלכלית למשפט** (יובל פרוקצ'יה עורך, 2012), בעמ' 203-201; וגם אריאל פורת "מתי ירצו הצדדים לחוזה 'הפרות יעילות'?" **ספר דניאל – עיונים בהגותו של פרופסור דניאל פרידמן** 171 (עורכים נילי כהן ועופר גרוסקופף, 2008).

וההרתעה, את עידוד הנמען למימוש זכויותיו, ואת היקף ההפרה. אנו סבורים שתחת השיקול הראשון, של ההרתעה, יש לשקול גם את סוג הפעילות של הצד הפוגע ואת היקפה של הפעילות (בצד היקפה של ההפרה, לפי השיקול השלישי).

אבחנה נוספת שערכנו בתוך קבוצת בעלי המסרים היא מידת הלגיטימיות של פעולתם ומידת החוקיות של התוכן המופץ. הצבענו על כך שמרבית תביעות הספאם בארץ מוגשות נגד משווקים לגיטימיים, ולאו דווקא נגד ספאמרים "סדרתיים", וזאת בשל הקלות היחסית להגיע לראשונים והקשיים לאתר ולתבוע את האחרונים. בתוך קבוצת הספאמרים הסדרתיים, הבחנו בין שתי תת קבוצות: ספאמרים שביסודם הם שומרי חוק, ולכן יפסיקו להפר במצב בו תביעה תהפוך את הפרת החוק שלהם ללא יעילה, וכאלה שביסודם אינם שומרי חוק, שלא יושפעו מהחוק, ויוסיפו לפעול באופן לא חוקי. ספאמרים כאלה נוטים לחמוק מיד החוק, וגם אם ניתנו פסקי דין בעניינים – לא לקיימם.

בעניין זה, אנו ממליצים להפנות מאמצים לאכיפה פלילית בתחום הספאם, כאשר מדובר בגורמים שאינם "מתרגשים" מאכיפה אזרחית. אנו ערים לכך שעיסוק בנושא זה אינו בראש סדר העדיפויות של המשטרה, אולם יש להקצות לכך כלים מתאימים במקרים קיצוניים.

לפני שנחקק חוק הספאם, חל איסור רק על משלוח הודעת פרסומת בפקס, כאשר הפרת האיסור הייתה עבירה פלילית. בעת החקיקה הושמעו ביקורות על כך שאכיפה פלילית בעניין אינה אפקטיבית או שאינה ראויה ביחס לאופייה של העבירה, וביקורות אלה הפכו לסיבה המרכזית להכרה בכך שמוטב להסתמך על אכיפה אזרחית של חוק הספאם.[35] אכן, במישור הפלילי, אכיפתו של סעיף 30א לחוק התקשורת חלשה.[36] זאת למרות שפיצוי ללא הוכחת נזק הוא כלי שנמצא בתפר שבין הפלילי לאזרחי.[37] בשלב החקיקה הודגש שאכיפה פלילית תישמר לנסיבות "קיצוניות".[38] אנו סבורים שפעילותם של ספאמרים מקצועיים, שאכיפה אזרחית אינה מרתיעה אותם, עשויה לעלות לכדי נסיבות "קיצוניות" שמצדיקות שימוש בכלי אכיפה עונשיים. יש לקוות שאכיפה פלילית תייצר הרתעה יעילה יותר עבור ספאמרים שעבורם החוק הקיים אינו משחק תפקיד משמעותי בהחלטה האם להפיץ ספאם, וכן שהיא תסייע בפיצויים של נפגעים מספאמרים כאלה.

לעניין עיצומים כספיים מנהליים, על מנת לאפשר אפיק פעולה זה יש צורך להקים גוף שיטפל בכך, כחלק ממשרד התקשורת או כחלק מהרשות למידע וטכנולוגיה [שפועלת באופן זה בכל הנוגע לאכיפה מנהלית של חוק הגנת הפרטיות].[39]

לסיכום חלק זה, הצעותינו הן להביא את היקף הפעילות של החברה המפרסמת כשיקול מפורש במסגרת שיקולי בית המשפט בעת פסיקת פיצויים, כדי לצמצם הן את הרתעת-החסר והן את הרתעת-היתר שיש במבנה הדין האחיד הנוכחי; ולהפנות מאמצים של אכיפה פלילית במקרים המתאימים, שבהם הספאמרים אינם מורתעים מאכיפה אזרחית.

(2) שלב שני: גורמים מסייעים לפני ההפצה

בנוסף לספקי הלידים, בשלב שלפני ההפצה, מעורבים בעלי מאגרי המידע שמציעים את מרכולתם לכל המרבה במחיר. על בעל מאגר העונה לדרישות שבחוק הגנת הפרטיות, התשמ"א-1981 מוטלות חבויות מכוח החוק. בהנחה שברשות ספקי הלידים מאגרי מידע העונים על הגדרת "מאגר מידע" בסעיף 7 לחוק הגנת הפרטיות, עליהם לציית להוראות החוק בנוגע לניהול מאגר כזה ולשימושים בו. בין היתר, יש חובת הודעה לאנשים על כך שהמידע עליהם

35 דן חי **תורת המסר** 238 (2012).

36 שם, בעמ' 287. חיפוש עדכני שערכנו אחר הליכים משפטיים לפי ס' 30א(1), שקובע את העבירה הפלילית, העלה חרס. נראה שלא מתקיימת אכיפה באפיק זה.

37 לטענת חי, הדרישה שהפיצוי יוטל רק אם השליחה נעשתה ביודעין בניגוד לחוק, מעידה על כך כי מדובר בסעד עונשי; שם, בעמ' 244-245.

38 שם, בעמ' 229.

39 על הצעות לתיקון חוק הגנת הפרטיות כך שהרשות למשפט וטכנולוגיה תופקד גם על אכיפת ס' 30א, ראו אצל חי, שם, בעמ' 286, בה"ש 47.

נאסף, ולאיזו מטרה (סעיף 11 לחוק), חובת סודיות (סעיף 16), חובת אבטחת מידע (סעיף 17 וכן תקנות נלוות), וכן, עקרון צמידות המטרה (סעיף 8(ב)), שלפיו, אין להשתמש במידע שנאסף למטרה אחת, למטרה אחרת.

משתמע מכך, שבעל מאגר מידע צריך לדעת למי הוא מעביר את המידע ולאיזו מטרה, שהרי עליו ליידע על כך את נושאי המידע, מראש, בעת הבקשה לאיסוף המידע. לכן, בעל מאגר מידע שמעביר מידע ללא הודעה מתאימה, מפר הן את חובת ההודעה והן את עקרון צמידות המטרה. הוא נושא באחריות משפטית ישירה להפרות אלה, לפי פרק ב של חוק הגנת הפרטיות. גם אם בעל המאגר התנסח בטופס ההודעה שלו באופן כללי, הוא אינו יכול לעצום את עיניו כאשר המידע נמכר לגורם מפוקפק. חזקה על משתמשים שלא היו מסכימים להעברת המידע האישי שלהם שנאסף למטרה אחת, לידי גורם מפוקפק, למטרה שיהפכו ליעדים לשיווק של שירותים ומוצרים לא חוקיים.

במילים אחרות, התשתית המשפטית להטלת אחריות על בעלי המאגרים קיימת. האתגר הוא ביישום ובאכיפה, וכאן, יש כמה קשיים. ראשית, משתמש הקצה שמקבל מסרים לא רצויים אינו יודע בהכרח מה מקור המסרים, ומי סיפק את פרטי הקשר שלו למפרסם, ודרושה פה מלאכת בילוש מסוימת. שנית, חוק הגנת הפרטיות אינו כולל פיצוי סטטוטורי בגין הפרת הוראות פרק ב של החוק. יש בחוק פיצוי סטטוטורי להפרת הוראות פרק א של החוק, שמונה עוולות פרטיות קלאסיות, אבל אין שם התייחסות למידע, למעט עקרון צמידות המטרה שמופיע גם שם, בסעיף 2(9) לחוק. שלישית, עילות תביעה לפי חוק הגנת הפרטיות אינן מופיעות כיום בחוק התובענות הייצוגיות, ולכן מי שמבקש לנקוט אפיק תביעה כזה, צריך להשתחל לאחת העילות שמנויות שם.[40] לעיתים קרובות, הדבר אפשרי, אולם זהו עוד חסם מפני התביעה. רביעית, תקופת ההתיישנות לתביעה בגין הפרת חוק הגנת הפרטיות היא שנתיים בלבד. לעיתים, אין די בפרק הזמן הזה.

קושי משמעותי נוסף נוגע לבעלי מאגרים שכרו נתונים באופנים שונים, לאו דווקא לגיטימיים, ומוכרים אותם לכל דורש. מעבר לקושי שבזיהוי מקורו של מאגר המידע, גם בהנחה שמקור המאגר יאותר ופעילותו תופסק, הרי שמאגר מידע הוא למעשה קובץ ממוחשב, קל לשעתוק ולהפצה בכמות בלתי מוגבלת של עותקים. כך, גם אם יאותר מקורם הראשוני ויוגבל, מאגרי המידע יוכלו להוסיף לשרת גורמים אחרים שלרשותם הם הועברו בטרם נחסם המקור.

דרך נפוצה לבניית מאגר מידע היא באמצעות קצירת מידע (scraping) ממקורות שונים כמו רשתות חברתיות ורשימות תפוצה. עצם בניית המאגרים באופן הזה מטילה צל של לגיטימיות מפוקפקת על השימוש בהם מלכתחילה; פרטים אינם מודעים וודאי שאינם מסכימים להכללתם במאגרי מידע בכלל ולמטרות שיווקיות של גורמים אחרים בפרט, והם (אולי) מודעים לעצם קיום המאגר רק לאחר שהחלו לקבל הודעות שלא רצו בהם ממקורות שונים. איסור על קצירת מידע והקמת מאגרי מידע ללא הסכמת מושאי המידע עשוי להטות את העול מכתפי מושאי המידע אל כתפי מי שמקימים מאגרים שכאלה. התמודדות נוספת היא בדמות מאגר מדינתי של "אל תתקשר אלי", שמנסה להתמודד עם הבעיה אך מייצר בעיות חדשות – כאשר העיקרית שבהן לענייננו היא הטיפול בנושא שיחות קוליות, אך לא הודעות טקסט.[41] כך, מי שיטרח לאסוף את פרטי הנרשמים למאגר "אל תתקשר אלי" יזכה במאגר נתונים של פרטים אליהם אפשר לשלוח לו הודעות טקסט.

בנוסף, הטלת מגבלות על סחר במאגרי מידע תטה אף היא את הכף לטובת נפגעי ספאם. כך גם הטלת חבות על חברת ההפצה או חברת התקשורת, לחשיפת מקור מאגר המידע בו השתמש מפיץ הספאם. נתיב אפשרי נוסף הוא הטלת קנס שרירותי על מי שמוכר מאגר מידע כאילו שיתף פעולה בהפצת ספאם אלא אם הוכיח אחרת.

לסיכום חלק זה, כדי לקטוע את שרשרת הספאם באיבה, יש להתמודד עם סחר במאגרי מידע לא חוקיים שנוצרו למטרה של הפצת ספאם. הצעתנו היא לשפר את נגישות האכיפה של חוק הגנת הפרטיות, בדרך של הרחבת הפיצוי הסטטוטורי גם לעוולות לפי פרק ב של חוק זה שעוסק במאגרי מידע, הארכת תקופת ההתיישנות בחוק לשבע שנים, כמו בכל תביעה אזרחית, והוספת האפשרות לתבוע בגין הפרת חוק הגנת הפרטיות בדרך של תובענה ייצוגית.

40 תביעה ייצוגית אפשרית רק לפי התוספת השניה של חוק תובענות הייצוגיות, התשס"ו-2006. הרשימה כוללת 14 פרטים, אבל אין בה התייחסות ישירה לפרטיות. הפרט המתאים ביותר הוא פרט 1, שעוסק ביחסי עוסק-צרכן.

41 על המאגר ואתגריו, ראו בהרחבה בפרק ד, בעמ' 77-79.

(3) שלב שלישי: גורמים מסייעים בשלב ההפצה

רשתות שותפים

נזכיר, שרשתות שותפים הן פלטפורמות המקשרות בין גורמים העוסקים בפרסום בזירות טכנולוגיות שונות (השותפים), ובין בעלי עסק המעוניינים לפרסם את עסקיהם.[42] מכיוון שלתובעים אין בדרך כלל דרך להגיע לרשתות השותפים ללא אמצעי חקירה משמעותיים, אין זה פלא שרשתות השותפים אינן נתבעות בבתי המשפט. רשתות השותפים מציבות אתגר משמעותי בתחום האכיפה הנובע מקושי בזיהוי פעילות ואיתור מקורה. בנוסף לכך, רשתות שותפים גם מסייעות לטשטש את מקור הספאם, כך שנפגע בדרך כלל יתקשה לתבוע במקרה של הפצת ספאם שבה מעורבת רשת כזו גם את ספק הלידים או את בעל המסר.

המלצתנו היא להפנות מאמצי מחקר לכיוון נושא רשתות השותפים בישראל, שבעניינן רב הנסתר על הגלוי, והגלוי המועט מצביע על מרכזיותן בשרשרת הערך של הספאם. אנחנו סבורים שלפחות במקרים מסוימים, רשתות השותפים אחראיות להפצת ספאם - אם במודע, כמו במקרה בו הן "משדכות" בין ספאמר מקצועי לבין חברת הפצה, ואם באופן של עצימת עין, כאשר אינן מבקשות לתהות על קנקנם של המפרסמים. אלא שבתחום רשתות השותפים חסר מחקר אמפירי, כמותי ואיכותי, שיסייע להבין את תמונת המצב בישראל בנוגע לתרומתן לשרשרת הערך של הספאם. בהיעדר מחקר כזה, קשה להעריך את המצב המשפטי בנוגע להטלת אחריות משפטית על רשתות שותפים. מחקר זה יסייע להבנה כיצד יש להתמודד עם שחקן זה ועם האתגרים שהוא מציב בזירת הספאם. העמקת הידע בנושא תאפשר הכוונה יעילה ומדויקת של מאמצי הרגולציה לכיוונו של שחקן זה.

חברות ההפצה

מקומן של חברות ההפצה בזירה מורכב יותר ביחס לספאם מאשר רשתות השותפים, מכיוון שהן מציעות שירות שאינו בלתי חוקי כשלעצמו, אבל יש חשש שינוצל לרעה. במובן זה, השירות שלהן הוא דו-שימושי (dual use), כלומר ניתן לשימוש לטובה או לרעה. למעשה, שולחי ספאם מקצועיים מסכנים את עסקיהן של חברות ההפצה, וכפי שהסברנו בפרק ב, להן עצמן יש אינטרס לעמוד על המשמר בקשר לשימוש בשירות שלהן.

בניגוד לשחקנים אחרים בשרשרת הערך שבעניינים אנו סבורים שהאסדרה חסרה, בנוגע לחברות ההפצה זיהינו גם פוטנציאל לקיומה של **אסדרת-יתר**. כפי שתיארנו בפרק ג, בחודש אפריל 2023 נכנסו לתוקף הנחיות חדשות של משרד התקשורת לעניין הסדרת הפצת מסרונים.[43] ההנחיות מחייבות את חברות ההפצה לאמת את זהות לקוחותיהן, וכן מגבילות את כמות ההודעות שניתן לשגר בו זמנית בתשלום מראש. ההנחיות מבקשות להתמודד עם העובדה שהפרוטוקול של הודעות סמס פרוץ יחסית, וקל לתמרן אותו. לעת עתה, נראה שהרגולציה החדשה מצליחה להתמודד בעיקר עם בעיה של מסרים שמבקשים לשווק עסקים לא חוקיים, אך אינה מבטיחה צמצום של ספאם שיווקי "רגיל". מנקודת המבט של חברות ההפצה, הרגולציה החדשה מייקרת הליכים באופן שמכביד על פעילותן, כאשר התוצאה היא ניסיון לעקוף את ההנחיות. אחד האפיקים החדשים אליהם פונות חברות ההפצה, ועמם לקוחות שיכולים להרשות לעצמם, הוא סוגי מסר שהרגולציה אינה חלה עליהם, כמו הודעות וואטסאפ שבבעלות חברת מֶטָה. מכיוון שמדובר בחבילות יקרות בהרבה, עסקים קטנים נפגעים יותר: גם אם יש להניח שרבים מהם יפסיקו להשתמש בשרותי הודעות טקסט, הם לא בהכרח ירכשו במקום זאת חבילות וואטסאפ.

ההנחיות עוסקות בסוגיה נקודתית – אבל חשובה – של משלוח הודעות לא חוקיות באמצעות חברות ההפצה, בצד הודעות חוקיות, ומנסות ליצור מנגנון שיבדל בין החוקי ללא-חוקי. ההנחיות חדשות ובשלב זה נראה שהשוק עדיין לומד אותן, אבל כבר מחפש דרכים לעקוף אותן. השפעתן של ההנחיות על שוק הספאם הלא-חוקי והחוקי גם יחד, ראויה לבחינה נוספת בעתיד, לאחר שיצטבר ניסיון מעשי בשטח.

ספקיות תקשורת

בצד חברות ההפצה, האפשרות המבטיחה ביותר (בעיקר עקב בעיות אכיפה) לשינוי מפת החבויות בזירת הספאם נוגעת לספקיות התקשורת. מבחינה פונקציונלית, ההבדל בין חברות ההפצה לספקיות התקשורת אינו משמעותי בהקשר הנוכחי, שכן הן חברות ההפצה והן ספקיות התקשורת מספקות פלטפורמות להפצת מסרים בהיקף גדול.

42 להרחבה, ראו פרק ב לעיל.

43 הוראת מנהל של משרד התקשורת "שירות שליחת מסר קצר ('מסרון')" (13.2.2023). ראו באתר משרד התקשורת: https://www.gov.il/he/departments/policies/14022023_1.

ההבדל המהותי בין השחקנים הוא מוסדי: חברות התקשורת מחזיקות ברישיון בזק שפוטר אותן מאחריות לתכנים המשוגרים באמצעותן, בעוד שחברות ההפצה אינן זוכות להגנה כזו, לפחות לא באופן מפורש.

כפי שציינו, חברות התקשורת נמצאות בתווך, בין השחקנים בשרשרת הערך לבין השחקנים מהעבר השני, המבקשים להילחם בספאם. חברות התקשורת משרתות אינטרסים צולבים, והמורכבות הגדולה של תפקידן נובעת בעיקר מהעובדה שהן אוחזות בשני כובעים: הן מחזיקות ומפעילות תשתיות תקשורת (בדומה לחברות ההפצה והדיוור), ובנוסף הן מספקות ללקוחותיהן שירותי תקשורת שונים. כלומר, חברות התקשורת משרתות שני שחקנים מרכזיים שהאינטרסים הבסיסיים שלהם מנוגדים בתכלית: מחד גיסא, המשווקים והמפרסמים, ומאידך גיסא, לקוחותיהן, משתמשי הקצה, שהם גם הנמענים של המסרים השיווקיים. החברות משרתות הן את המפרסמים, ומרוויחות יותר כאשר חבילות המסרים גדולות יותר; והן את ציבור המשתמשים ושם הן מבקשות להציע שירותים נקיים ככל האפשר מהפרעות לא רצויות.

ההסדרה המשפטית של גורמי ביניים שהם בגדר צינור, ושירותיהם הם דו-שימושיים במובן שתואר, כלומר הם ניתנים לניצול לרעה או לטובה, היא סוגיה מורכבת בסביבה המקוונת. נעיר על שני היבטים מרכזיים שלה: הטלת אחריות / מתן חסינות לגורמי הביניים בקשר לתכנים פוגעניים ולשימושים מפרים שביצעו לקוחות, וחשיפת זהות של משתמשים מעוולים.

אחריות וחסינות

השאלה התעוררה בקשר לאחריות של גורמי ביניים כמו ספקי שירות, מנועי חיפוש, ופלטפורמות שונות כמו מדיה חברתיים, לתכנים פוגעניים של גולשים. האם מֶטָה (פייסבוק) אחראית לפוסט פוגעני שגולש פרסם? האם יו-טיוב אחראית להפרת זכויות יוצרים מצד גולש שהעלה תכנים מפרים? האם מנוע חיפוש אחראי לכך שבשאילתות החיפוש מופיעות גם תוצאות שהן עצמן בלתי חוקיות (למשל, אם תצוגת החיפוש כוללת לשון הרע), או שהן מפנות לאתרים פוגעניים או כאלה שמפרים זכויות קניין רוחני?

במדינות שונות יש גישות שונות לעניין, וגם שוני בקשר לסוגי ההפרות. בקשר לקניין רוחני, בארצות הברית ובאירופה, ההסדרים המשפטיים השונים הם של חסינות שמותנית בקיום הליך של "הודעה והסרה".[44] כלומר, פלטפורמות, מנועי חיפוש ואתרים אחרים אינם מחויבים בניטור מוקדם של תכנים לשם איתור הפרות זכויות יוצרים,[45] אולם אם הן מקבלות הודעה על הפרה נטענת, ומסירות את התוכן המפר לכאורה, הן יזכו בחסינות מפני תביעה. אם הן אינן מפעילות הליך כזה, או שהן אינן מסירות את התוכן – הרי אין להן חסינות, אולם יש לשים לב: היעדר חסינות אין פירושו אחריות. התובע יצטרך להוכיח את אחריותן לפי עקרונות של דיני זכויות יוצרים ודיני הנזיקין, למשל אחריות להפרה תורמת (contributory infringement).[46]

באיחוד האירופי, מודל חסינות מותנית זה קיים גם בקשר לכל תוכן פוגעני.[47] לעומת זאת, בארצות הברית, בקשר לכל סוגיה שאיננה זכויות יוצרים, נקבע מודל של חסינות מוחלטת. המטרה המקורית הייתה לעודד את ספקיות השירות להתערב, ללא חשש מתוצאות ההתערבות, אולם לאור החסינות המוחלטת ממנה נהנו, רבות מהן בחרו שלא להתערב כלל, והתוצאה הייתה כאוס וריבוי תכנים פוגעניים. במשך השנים כמה מהפלטפורמות המרכזיות, כמו מֶטה

44 בארצות הברית, ראו 17 U.S.C. §512. באיחוד האירופי, הנושא הוסדר תחילה בדירקטיבה בעניין סחר אלקטרוני משנת 2000, ראו Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), 2000 O.J. (L 178), בסעיפים 13-14, בדירקטיבה משנת 2019. ראו Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.), 2019 O.J.(L 130). Art. 89(2) של הרגולציה משנת 2022 מורה על מחיקת סעיפים 12-15 מהדירקטיבה משנת 2000, והחלה של סעיפים 4-6, 8 של הדירקטיבה משנת 2022. ראו Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277).

45 באיחוד האירופי הדברים נאמרו במפורש בס' 17(8) של הדירקטיבה משנת 2019. הוראה דומה קיימת גם בדירקטיבה משנת 2000, בס' 15(1), ביחס לס' 12-14.

46 דוקטרינה זו הוכרה גם בדין הישראלי, בפסיקה, תחילה בדיני הפטנטים (ראו ע"א 1636/98 **רב בריח נ' בית מסחר לאביזרי רכב חבשוש**, פ"ד נה(5) 337, 353ז-354ג (2001) ומשם זלגה לדיני זכויות יוצרים, תחילה בסביבה הפיסית (ע"א 5977/07 **האוניברסיטה העברית בירושלים נ' בית שוקן ספרים בע"מ**, פ"ד סד(3) 740, בפס' 18-19 (2011), ומשם לסביבה הדיגיטלית, ראו ת"א (מרכז) 567-08-09 **א.ל.י.ס. אגודה להגנת יצירות סינמטוגרפיות (1993) בע"מ נ' רוטר.נט בע"מ** (נבו 8.8.2011) (להלן: **עניין א.ל.י.ס**), בפס' 52.

47 ראו ס' 12-14 לדירקטיבה משנת 2000, כפי שתוקנו ב Digital Services Act משנת 2022, ס' 4-6, 8.

(פייסבוק), אימצו כללים פנימיים ("כללי קהילה") ומגנונים להסרת תכנים פוגעניים. עם זאת, אנו רואים שונות בנושא. למשל X (לשעבר טוויטר) צמצמה מאוד את התערבותה בהסרת תכנים פוגעניים מאז שנרכשה על ידי אֶלון מאסק, בשנת 2022.

השיקולים בעיצוב ההסדרים המשפטיים בנושא הם הרצון לעודד את הפעילות של גורמי הביניים למיניהם, בשל מרכזיותם וחשיבותם לפעילות הרשת, ומתוך חשש שאם תוטל עליהם אחריות משפטית למעשיהם של משתמשי הקצה, הם ינהגו בדרך של אצבע קלה על מקש המחיקה. במילים אחרות, שיקול מרכזי בעיצוב ההסדרים המשפטיים השונים הוא כיצד לעודד שיח וחופש ביטוי, ולצמצם חדירה של שיקולים מסחריים לשיח הזה.

אנו סבורים שניתן להקיש מההסדרים בדבר אחריות וחסינות של גורמי ביניים, לעניין הספאם. הגורמים בשרשרת הספאם שמספקים שירות דו-שימושי במובן שתואר לעיל, שהם בעיקר חברות ההפצה וספקיות התקשורת, מציעים שירות חשוב ולגיטימי, והאתגר הוא לבדל את השימושים הטובים מן הרעים. כיום, החברות עצמן פטורות מבירור מקדים כזה, האם השימוש המיועד הוא הפצה חוקית און שהיא בגדר ספאם, ולכן פטורות מאחריות.

אנו סבורים שיש לאמץ נוהל הודעה והסרה, בליווי חזקות בעניין הזה. למשל, ספק שירות הפצה שיודע, משום שקיבל הודעות ממשתמשים או מגורם אחר, שלקוחותיו מפיצים ספאם לא חוקי, ומתעלם מההודעות האלה, יכול להיות אחראי לספאם עצמו. ספק שירות שמשדל לקוחות להפיץ ספאם – בוודאי שצריך להיות אחראי.[48] בהיקש מעניין **א.ל.י.ס** שדן בפורומים מקוונים של שיתוף קבצים וקישורים לתכנים מפרי זכויות יוצרים – ניתן לקבוע חזקות: כאשר חלק ניכר מהלקוחות של חברת ההפצה מפרים את דיני הספאם, הדבר משליך לאחור על חברת ההפצה.[49] בעניין **א.ל.י.ס** מנה השופט גרוסקופף שני חריגים לכלל של היעדר חבות בהינתן מנגנון של "הודעה והסרה": חריג העידוד, החל כאשר בעל אתר מעודד באופן אקטיבי הצבת קישורים לאתרים מפרים באחד או יותר מהפורומים של האתר ובהתאם עלול למצוא עצמו אחראי להפרה תורמת;[50] וחריג ה"פורום הפסול", שחל כאשר "פורום מסוים הופך להיות מוקדש, רובו ככולו, להצבת קישורים לאתרים מפרים... ביחס לפורום החשוד כ'פורום פסול' החזקה היא כי בעל האתר מודע לכך שהוא מסייע לקיומן של הפרות ישירות, וכי סיוע זה הוא בגדר תרומה ממשית ומשמעותית להן."[51]

חשיפת זהות המעוולים

כפי שראינו בפרקים ב, ו-ג, אחד האתגרים בהתמודדות עם הספאם הוא שזהות הגורם המפרסם מוסתרת, וכך, משתמש הקצה אינו יודע מי בדיוק פוגע בו, ומתקשה לתבוע. עלויות הבירור עשויות להיות גבוהות. הדברים אמורים במיוחד בנוגע להודעות בעלות תוכן לא חוקי, ולהודעות המגיעות דרך חברת הפצה או חברת תקשורת, כאשר זהות הלקוח שהפיץ את המסרים דרכן אינה ידועה.

ניסיון אחד לאזן בין האינטרסים הסותרים הללו הוא ברוח הצעת החוק הפרטית שמונחת כעת על שולחן הכנסת, שנועדה להתמודד עם הפטור ממנו נהנים כיום גורמי השיגור שנחשבים ל"צינור" בלבד, אך בפועל מאפשרים הגנה על ספאמרים, בכך שאינם חושפים את זהותם.[52] לפי ההצעה, מי ששלח הודעה עבור אחר יחויב לחשוף את פרטי השולח במקרה הצורך. אם יבחר שלא לחשוף את פרטי השולח הוא יחשב כמפרסם, ובהתאם, יישא באחריות על שליחת המסרים. הצעה זו למעשה מנסחת קריאות קודמות מצד שחקנים בזירת הספאם, לשינוי מצב העניינים הנוכחי בנוגע לאחריות מפיץ המסרים.

בנוסף לשינוי הפטור המלא של חברות התקשורת, אנו ממליצים ליצור הליך פשוט לקבלת צו לחשיפת זהות של המפרסם, כלומר פנייה לחברת הפצה או לספקית תקשורת כדי לקבל את נתוני השולח. כיום, רק למשטרה יש סמכות

---

48 ראו בדומה, בקשר לשידול (inducement) להפרת זכויות יוצרים, בארצות הברית: MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

49 עניין **א.ל.י.ס.**, לעיל ה"ש 46, בפס' 55-57.

50 שם, בפס' 55-56.

51 שם, בפס' 57.

52 הצעת חוק התקשורת (בזק ושידורים) (תיקון - חובת מסירת פרטים של שולח פרסומת בניגוד לחוק), התשפ"ג-2022 (פ/25/276). ההצעה היא מהכנסת הנוכחית (ה-25).

לעשות כך, או שיש לפנות לקבלת צו באמצעות בית המשפט.[53] הליך כזה יאפשר לנפגעי ספאם להתגבר ביתר קלות על בעיית חשיפת זהות מפיץ הספאם, מכשול העומד בדרכם להגשת תביעה.

מנגנוני סינון

החוק כיום אינו מחייב את חברות התקשורת להפעיל מנגנוני סינון אוטומטיים שיזהו מבעוד מועד שולחי ספאם ויסננו אותם. מנגנונים מעין אלה אמנם קיימים בשירותי דוא"ל כמו Gmail, אך הבחירה להפעילם נתונה בידי מפעיל השירות. לגבי מסרונים, יש קושי טכנולוגי להשתמש במסננים אוטומטיים, כפי שנראה בפרק הבא, העוסק בטכנולוגיות ספאם.

בהתאם, אנו ממליצים לחייב את חברות התקשורת להתקין מסננים אוטומטיים כאלה. אמנם, יש לכך עלויות, והתערבות בקניין של החברות, אולם, חיוב כזה יעביר את הנטל מכתפי הנמענים אל כתפי החברות המספקות להם שירותי תקשורת. עדיין, חברות תוכלנה להציע שירותים נוספים מעבר להגנה הבסיסית שתספקנה, למי שמבקש לשפר את אמצעי האבטחה שלו. אולם ברירת המחדל עבור נמענים תהיה שירותים בעלי מנגנוני סינון בסיסיים. אנו מודעים לכך שחיוב כזה מטיל נטל גדול יותר על חברות קטנות ועשוי להכביד על כניסתן לשוק התקשורת ועל יכולתן להתחרות בו. עם זאת, אנו סבורים שמדובר בשירות בסיסי, ושבעניין זה אין להטיל את עול התחרות בשוק על כתפי הנמענים.

(4) שלב רביעי: הנמענים והשחקנים שאמונים על הגנתם

המדינה

בפרק ב ציינו את המתח המובנה בין חובת המדינה להגן על אזרחיה מפני הצפה של תקשורת לא רצויה, לבין חובתה להגן על שחקני שוק שונים. המדינה, כרגולטור המרכזי הן בתחום המשפטי והן בתחום הכלכלי, יכולה להשפיע באופן משמעותי על שינויים לטובה בתחום המאבק בספאם. בשלושת השלבים הקודמים ציינו אפשרויות שונות של שינוי מפת החבויות, בהתאם לניתוח מפת השחקנים הלוקחים חלק בשרשרת הערך. יש שינויי רגולציה נוספים שבכוחה של המדינה לחולל, ושיוכלו להשפיע על הזירה באופן חיובי:

א. **אכיפה פלילית**. בעוד שהאכיפה האזרחית של חוק הספאם רחבה, הרי האכיפה במישור הפלילי אינה משמעותית.[54] כך למשל בעוד שחוק הגנת הפרטיות מאפשר הטלת קנסות מנהליים בגין הפרתו, חוק הספאם אינו קובע עיצומים כספיים מנהליים. למרות שהצעה כזו הועלתה במהלך החקיקה, היא נדחתה מהטעם שבשונה לאכיפת הוראות בנוגע לדיוור ישיר בחוק הגנת הפרטיות, בחוק הספאם אין המדובר בגופים שכפופים לגורם רגולטורי מסוים.[55] כדי שתתאפשר הטלת קנסות מנהליים בגין הפצת ספאם, יש צורך בגוף שיטפל בקנסות כאלה, ויוכל בנוסף לכך גם לפעול להעלאת מודעות של פרטים לזכויותיהם ולנקוט יוזמות נוספות.[56]

ב. **קידום אוריינות דיגיטלית**. המדינה יכולה לעודד ולטפח במגוון דרכים שונות אוריינות דיגיטלית בכלל, ואוריינות דיגיטלית בכל הנוגע למערכת הספאם בפרט. מיזמים כמו מאגר "אל תתקשרו אלי" מעוררים קשיים שונים עליהם עמדנו בפרק ד. אולם גם אם היו חפים מכל קושי, לא תהיה בהם תועלת אם הציבור שעליו הם נועדו להגן אינו מודע לקיומם או שאינו יודע כיצד לרתום אותם לעזרתו. עידוד האוריינות הדיגיטלית נחוץ בעיקר כאשר מדובר באוכלוסיות חלשות – למשל קשישים או עולים חדשים, שהם בעיקר מי שעליו מיזמים כמו "אל תתקשרו אלי" נועד להגן מלכתחילה.

ג. **שיפור הגישה לערכאות**. הגישה למשפט בכלל ולערכאות דיוניות בפרט, אינה נחלקת באופן שוויוני בין אוכלוסיות שונות. בעיצוב מדיניות כוללת יש להביא בחשבון שמלבד פערים באוריינות הדיגיטלית קיימת פריסה לא אחידה של הגישה לערכאות, ולשקול שיקולים אלה במכלול השיקולים בהתמודדות עם בעיית הספאם. מיזמים כמו "ספאם אוף" סייעו לצמצם פערים בגישה לערכאות לנפגעי ספאם, ועל כן ראוי לעודדם. על המדינה לעודד את המערכת המשפטית לשיתוף פעולה עם גופים פרטיים שמטרתם מלחמה בספאם, למשל עמותות כאל ספאם

53 חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007.

54 ראו חי **תורת המסר**, לעיל ה"ש 35, בעמ' 287.

55 על כך, ראו חי, **תורת המסר**, שם, בעמ' 229-230.

56 חי, שם, בעמ' 285, מצביע על כך שהצעות להקמת גוף כזה עלו עוד לפני הליכי חקיקת חוק הספאם. בה"ש 47, בעמ' 286 חי הפנה להצעות לתיקון חוק הגנת הפרטיות באופן שיהפוך את רמו"ט (כיום הרשות להגנת הפרטיות) למופקדת גם על אכיפת ס' 30א.

או חברות פרטיות כמו "ספאם אוף". לכל הפחות, יש לפעול לשם מניעת הישנות מצבים בהם מערכת המשפט פועלת בעוינות דווקא כלפי גופים שמטרתם לסייע לאזרח במאבק בספאם.

ד. **חיזוק התמריצים לתבוע**. בפרק ג הצבענו על מכשולים שונים שעומדים בפני יצירת מערך תמריצים כלכליים יעילים בזירת הספאם. הכללים המשפטיים מנסים לעקוב אחר ההיגיון הכלכלי של הספאם, לשבש את התמריצים של הספאמרים להפיץ דברי פרסומת לא רצויים, וליתן בידי הצרכנים תמריצים לתבוע ולאכוף את הדין בעצמם. עם זאת, עדיין אחד החסמים המרכזיים להגשת תביעות – למרות המספר הגבוה לכאורה של תביעות – הוא התחשיב הכלכלי של התביעה, והצד המשלים – היעדר הרתעה מספקת למפיצים שמפרים את החוק. באופן כללי, על הגופים האמונים על כך לבחון מחדש את שאלת התמריצים הכלכליים ואת יעילות מערך התמריצים הקיים, ולבחון אפיקים לשינוי המפה הקיימת. הצענו נקודתית מספר דרכי פעולה אפשריות בכיוון זה, כמו למשל התאמה מחודשת למדד המחירים של הפיצוי הקיים היום; חשיפת זהות המפר על ידי חברות התקשורת; או הטלת קנסות מנהליים על מפרים "מקצועיים".

ה. **הרחבת תחולת החוק**. כמו כן, ציינו שתחולתו של החוק לעניין הגדרת "מפרסם" ו"דבר פרסומת" צרה מדי, ועמדנו על כך שיש להתאים את הגדרות החוק למצב העניינים בפועל. ראשית, החוק אינו חל על ספאם פוליטי ועל כן אינו מטפל בכל המטרדים בפועל. לפי החוק, תוכן "אידיאולוגי" יכול להישלח אלינו בכל עת ובאין מפריע. כמובן, כפי שציינו לעיל, למסרים פוליטיים יש פן משמעותי של חופש הביטוי הפוליטי, ופן מסחרי מופחת. בנוסף, החוק אינו חל על שיחות טלפון אנושיות, שבמקרים רבים הפכו למטרד של ממש, כאשר מבול של טלפנים אנושיים עוסקים בהפצת אותו מסר שיווקי לרשימות ארוכות של נמענים שלא הסכימו לכך – יש לשאול האם מדובר בספאם לכל דבר ועניין.[57]

הנמענים

כפי שעלה לא אחת במהלך הדוח, קשה להפריז בחשיבותה של אוריינות דיגיטלית למאבק בספאם. כמובן, בעוד שאנו סבורים שאין לגלגל אל הנמענים את האחריות להגן על עצמם מפני מסרים לא רצויים, ברור לנו שככל שפרטים ישתמשו באמצעי הגנה טכנולוגיים אפקטיביים שמטרתם מניעת ספאם, היקפי התופעה יצטמצמו. קראנו למדינה להשקיע מאמצים בהקניית אוריינות טכנולוגית לציבור, ובפרט לחלקים בציבור שחשופים במיוחד לנזקי הספאם: קשישים, עולים חדשים, מעוטי אמצעים. עד שהמדינה תרים את הכפפה, יש לקוות שיותר ויותר משתמשי קצה ילמדו להשתמש בעצמם באמצעי הגנה טכנולוגיים מפני ספאם.

חברות טכנולוגיה שמפתחות טכנולוגיות אנטי-ספאם

חברות הטכנולוגיה מעורבות במרוץ החימוש המתמשך בכל הנוגע לפיתוח אמצעי אבטחה טכנולוגיים, לרבות אמצעים למלחמה בספאם. מדובר בשחקן שהשוק מסדיר את פעולתו, ולכן יש להניח שתמריצים כלכליים יוכלו לתעדף שחקני שוק כאלה כאשר הם מספקים מוצר שהטמיע עקרונות של הנדסת ניקיון. דוגמה לתעדוף כזה תהיה העדפת מוצרים בהם הוטמעו ערכי הנדסת ניסיון בכל רכישת מוצרים כאלה במגזר הציבורי. במקרה שבו יחליט הרגולטור להפוך את הגישה של הנדסת ניקיון למחייבת עבור ספקיות השירותים, חברות הטכנולוגיה המספקות מוצרים לחברות אלה יתומרצו לפעול אף הן לפי כללים אלה ולהטמיע במוצריהן מראש ערכים של ניקיון המערכת ממסרים לא רצויים.

חברות התקשורת

בכובען כספקיות שירותים, חברות התקשורת אינן מחויבות להתקין מסנני ספאם עבור לקוחותיהן, ואספקה של שירות אנטי-ספאם הוא וולונטרי. למרות שהתקנת מסננים מתקדמים עשויה לייקר את עלות השירות עבור החברה, וכן להקשות על כניסתן של מתחרות קטנות יותר לשוק התקשורת, אנו סבורים שיש לקבוע בחקיקה או ברישיונות הבזק, רף מינימלי של שירות סינון שחברות אלה מחויבות לספק ללקוחותיהן.

בנוסף לכך, השימוש במסננים שמספקות החברות דורש התאמה אישית של השירות להרגליו וצרכיו של משתמש ספציפי, למשל בחירה בסינון מחמיר יותר או פחות, פעולה המצריכה אוריינות דיגיטלית בסיסית של המשתמש. אנו

57 עם זאת, שיחות כאלה עשויות להיות בגדר "דיוור ישיר", ובכל מקרה, ככל שהן מבוססות על מאגר מידע כהגדרתו בחוק הגנת הפרטיות, הגורם המתקשר צריך לעמוד בדרישות החוק – רישום מאגר המידע כחוק (ס' 8 לחוק), הודעה מתאימה לאדם בדבר איסוף מידע (ס' 11), וכדומה. לנמען יש זכות לדרוש גישה למידע שמוחזק במאגר מידע (ס' 13), אך כיום, אין זכות מלאה לדרוש את מחיקת הרישום (למעט כאשר המידע שגוי, ס' 14).

מציעים לפיכך לנסח וליצור פרוטוקול אחיד שיועבר לכל משתמשי חברות התקשורת כאשר אלו מבקשים להירשם לשירות, בדמות לומדה או סרטון הדרכה, שעניינו הקניית אוריינות דיגיטלית בסיסית בכל הנוגע לספאם ולדרכים להימנע ממנו. אכן, לא כל המשתמשים יבחרו לצפות בסרטון או בלומדה, אך גם במקרה שהתועלת אינה ברורה, אנו מאמינים שזהו אפיק שראוי לנסות.

חשוב להזכיר שהאינטרס של ספקית שירות דוא"ל, שהוא שירות חינמי, בחסימת ספאם, שונה מהאינטרס של ספקית שירות הודעות טקסט. לספקית שירותי טקסט יש אינטרס מובהק שלא לסנן שולחים של הודעות טקסט משום שסינון כזה עשוי לעלות לספקית השירות בהפסד כלכלי. במילים אחרות, לספקית שירות הודעות טקסט יש אינטרס כלכלי בשליחת כמה שיותר הודעות. התקנות החדשות שהוחלו על חברות ההפצה הן צעד לכיוון שינוי חיובי בעניין זה, משום שהן מחייבות את חברות ההפצה לתהות טוב יותר על קנקנם של מפיצי המסרים. עמדנו על כך שיעילות התקנות עדיין צריכה להיבחן בראי הזמן, אולם בהנחה שיעילותן תוכח, יש לשקול הרחבה שלהן כך שיחולו גם על ספקיות התקשורת באופן כללי. בנוסף, במקרה שתוטל על חברות התקשורת חבות לעניין חשיפת ספאמרים, כפי שהמלצנו, אנו מאמינים שהדבר יהווה תמריץ, מעבר לתמריצים כלכליים, שלא לפעול תוך עצימת עיניים לפעולתם של ספאמרים.

גם הרשתות החברתיות נמצאות בניגוד אינטרסים בשל המנגנון שמטרתו הפצת כמה שיותר מסרים לקהל גדול ככל האפשר, מה שמפריע לניסיונות להקטין הפצת ספאם למשתמשים. גם כאן, אנו סבורים שעל הרגולטור להציב רף מינימלי מחייב של הגנה על משתמשים מפני ספאם באמצעות מסננים ייעודיים, כאשר יוטל על החברות בנוסף לדאוג לכך שמשתמשים יידעו על מסננים אלה ועל האופן להפעילם. בנוסף, אנו סבורים שיש לעודד את המחקר המבקש לפתח טכניקות לאיתור חתימה מלאכותית של בוטים ברשתות, תוך שיתוף פעולה של מומחי אבטחת סייבר וחוקרי למידת מכונה.[58]

אינטרסים כלכליים דומים של חברות תקשורת וחברות טכנולוגיה, בראש ובראשונה שמירה על יתרון כלכלי בשוק, עשויים להביא לכך שהמחקר המתקדם ביותר בנוגע לזיהוי ספאם לא יהיה גלוי לכלל הציבור.[59] אמנם, הסודיות נדרשת לעיתים קרובות כאשר מדובר במרוץ חימוש, על מנת לא לחשוף בפני היריב את האופנים בהם אפשר לטרפד את פעולותיו. אלא שהתוצאה היא שהמלחמה בספאם נעשית באופנים שונים ועל ידי גופים שונים בהתאם לתמריצים כלכליים, בעוד ההיבטים החברתיים של התופעה אינם מטופלים כהלכה. למשל, פתרונות שוקיים בלבד מביאים להעמקת פערים בין בעלי אוריינות טכנולוגית לנעדרי אוריינות, ובין משתמשי שירות מבוסס יותר שמעניק הגנה טובה יותר למשתמשים, למשתמשי שירות שכלי האבטחה שלו משוכללים פחות. אחד הפתרונות לכך עשוי להיות השקעה במחקר ופיתוח מטעם המדינה של כלים טכנולוגיים למלחמה בספאם, שיוכלו לשמש את כלל האוכלוסייה, בדומה למשל לאפליקציית "המגן" שפותחה בעת המאבק של מדינת ישראל במגפת הקורונה.

4. סיכום

בפרק זה קשרנו בין כל המרכיבים שנדונו עד כה: מפת השחקנים השונים בזירת הספאם, ההיבט המשפטי של הפעילות בזירה, וההיבט הטכנולוגי שלה, והצענו דרכי פעולה עתידיות לקובעי מדיניות. ראשית, בחנו וניתחנו את הצמתים הטכנולוגיים האפשריים בהם לא קיימת עדיין התערבות משפטית, אך התערבות כזו עשויה להיות יעילה. באופן משלים, דנו בהטלת חבות משפטית על שחקנים בשרשרת הספאם שפעילותם הנוכחית אינה מוסדרת או שהסדרתה אינה מיטבית.

הפתרונות המשלבים חשיבה משפטית וטכנולוגית, שאותם הצענו בחלקו הראשון של הפרק, נחלקו לשניים: פתרונות שלפני מעשה ופתרונות שלאחר מעשה. אנו מכנים את הפתרונות שלפני מעשה בשם "הנדסת ניקיון": הטמעה מראש של עקרונות וערכים רצויים בטכנולוגיה שנועדה להתמודד עם ספאם, עוד בשלבי העיצוב הטכנולוגי. מדובר בתכנון מוקדם של טכנולוגיה על מנת לסייע בשמירה על "ניקיון" המערכת האקולוגית התקשורתית, כדי לצמצם פעילות של דואר זבל לא חוקי.

58 פררה, לעיל ה"ש 25, בעמ' 89.

59 על כך ראו למשל אצל פררה, שם, בעמ' 86, הטוען שלספקיות שירותים יש תמריצים להשתמש בפתרונות מוגנים בפטנט או בקוד סגור על מנת לשמר יתרון תחרותי.

לגבי **פתרונות שלפני מעשה**, המלצנו על הדברים הבאים:

1. תכנון מדיניות בתחום הספאם צריך להביא בחשבון את העובדה שזירת הספאם היא מרוץ חימוש אינסופי. כפועל יוצא מכך, יש להעדיף פתרונות מקדימים, שיבקשו לתכנן טכנולוגיה במחשבה מראש על שימושים לרעה, ובכך לבנות מראש הגנה לתוך הטכנולוגיה עצמה.
2. בהתאם, אנו מציעים לאמץ חשיבה של "הנדסת ניקיון", כלומר תכנון מוקדם של טכנולוגיות באופן שימזער את הפצת הספאם מראש.
3. למימוש הרעיון של הנדסת ניקיון דרושה הכוונת מדיניות מדינתית מצד אחד, ונכונות מצד התעשייה, מהצד המשלים. כל הגורמים המעורבים, כמו גם האקדמיה המדעית, צריכים לנסות ולפתח אמצעים טכנולוגיים טובים יותר שיאפשרו את הנדסת הניקיון.
4. אפיק מבטיח עליו הצבענו הוא שימוש בטכנולוגיות בלוקצ'יין שיאפשר להתגבר על הקושי באימות זהות של שחקנים ושל פעולות במערכות מידע.
5. בעקבות הניסיון שנצבר בנוגע ל"הנדסת פרטיות", אנו סבורים שלהנדסת ניקיון יש סיכוי טוב יותר להצליח במגזר הציבורי, ולכן המלצנו להפנות מאמצי פיתוח של הנדסת ניקיון בראש ובראשונה במגזר הציבורי.

לגבי **פתרונות שלאחר מעשה**, בחנו את המקרה של חברת "ספאם אוף", שמאפשר הפקת לקחים לעתיד. מסקנתנו והמלצתנו היא

6. לעודד מיזמים כמו "ספאם אוף", שהכניסה מספר חידושים שהיטו את המאזן לטובת נפגעי הספאם.
7. החידושים העיקריים היו אוטומציה של הליך התביעה; אסטרטגיית פעולה שחילקה תביעת ספאם להרבה מאוד תביעות קטנות, ש"הציקו" לגורם השולח (בתמונת ראי של הספאם עצמו); וכן תביעת נושאי משרה בחברות שהפיצו ספאם. שילוב של כל אלה יחדיו מדגים פתרון שמשלב את ההיבטים המשפטיים עם ההיבטים הטכנולוגיים של ההתמודדות עם ספאם.
8. פתרונות כאלה יכולים לשפר את הנגישות של אזרחים למערכת המשפט ולשפר את מאזן ההרתעה.

בחלקו השני של הפרק דנו ב**הטלת חבויות על שחקנים שונים** בזירת הספאם. המלצותינו, בתמצית, הן:

9. כאשר בית המשפט שוקל שיקולים בעת פסיקת פיצויים, עליו לשקול גם את סוג הפעילות של הצד הפוגע ואת היקפה, ולהתאים את הפיצויים כדי להתאים את ההרתעה לאיום. שיקול זה ישקף ויכיל את הפערים בתוך קבוצת בעלי המסרים, בין עסקים גדולים לקטנים, ואת התמריצים השונים שפועלים לגביהם.
10. אנחנו ממליצים להפנות מאמצים לאכיפה פלילית בתחום הספאם, כאשר האכיפה האזרחית אינה יעילה דייה.

לגבי **גורמים מסייעים בשלב שטרם ההפצה**, המלצותינו הן -

11. לאסור על קצירת מידע והקמת מאגרי מידע ללא הסכמת מושאי המידע, כך שהעול יעבור מכתפי מושאי המידע אל כתפי מקימי מאגרים שכאלה.
12. להטיל מגבלות על סחר במאגרי מידע;
13. להטיל חובה – וליצור הליך מתאים – לחשיפת מקור מאגר המידע בו השתמש מפיץ הספאם;
14. להטיל קנס עונשי שרירותי על מי שמוכר מאגר מידע כאילו שיתף פעולה בהפצת ספאם אלא אם הוכיח אחרת.

לגבי **גורמים מסייעים בשלב ההפצה**, המלצנו כך:

15. להפנות מאמצי מחקר לכיוון נושא רשתות השותפים בישראל. המידע על אודות אופן הפעולה של רשתות שותפים בישראל דל ביותר, עד כדי הצבת קושי ממשי בפני הערכה של חבויות משפטיות שניתן וראוי להטיל עליהן. מחקר אמפירי, כמותי ואיכותי, יסייע להבנה כיצד יש להתמודד עם שחקן זה ועם האתגרים שהוא מציב בזירת הספאם. העמקת הידע בנושא תאפשר הכוונה יעילה ומדויקת של מאמצי הרגולציה לכיוונו של שחקן זה.

16. בחודש אפריל 2023 נכנסו לתוקף הנחיות חדשות של משרד התקשורת לעניין הסדרת הפצת מסרונים. ציינו שקיים חשש מאסדרת יתר של פעילות חברות ההפצה, ושהשפעתן של ההנחיות על שוק הספאם הלא-חוקי והחוקי גם יחד, ראויה לבחינה נוספת בעתיד, לאחר שיצטבר ניסיון מעשי בשטח.

17. האפשרות המבטיחה ביותר (בעיקר עקב בעיות אכיפה) לשינוי מפת החבויות בזירת הספאם נוגעת לשני שחקנים: חברות ההפצה וספקיות התקשורת. הצעת החוק הפרטית המונחת כעת על שולחן הכנסת, נועדה להתמודד עם הפטור ממנו נהנים כיום גורמי השיגור שנחשבים ל"צינור" בלבד.

מנינו מספר **שינויים נוספים שבכוחה של המדינה לחולל בזירה:**

18. הרחבת האכיפה הפלילית בתחום באמצעות הטלת קנסות מנהליים.

19. עידוד אוריינות דיגיטלית בכלל, ואוריינות דיגיטלית בכל הנוגע למערכת הספאם בפרט.

20. שיפור הגישה לערכאות. בעיצוב מדיניות כוללת יש להביא בחשבון שמלבד פערים באוריינות הדיגיטלית קיימת פריסה לא אחידה של הגישה לערכאות, ולשקול שיקולים אלה במכלול השיקולים בהתמודדות עם בעיית הספאם. על המדינה לתמוך בשיתופי פעולה בין המערכת המשפטית לבין גופים פרטיים שמטרתם מלחמה בספאם, למשל עמותות כמו "אל ספאם" או חברות פרטיות כמו "ספאם אוף". לכל הפחות, יש לפעול לשם מניעת הישנות מצבים בהם מערכת המשפט פועלת בעוינות דווקא כלפי גופים שפועלים על מנת לסייע לאזרח במאבק בספאם.

21. על הגופים האמונים על יצירת מערך תמריצים כלכליים לבחון מחדש את שאלת התמריצים הכלכליים ואת יעילות מערך התמריצים הקיים, ולבחון אפיקים לשינוי המפה הקיימת. הצענו נקודתית מספר דרכי פעולה אפשריות בכיוון זה, כמו למשל התאמה מחודשת למדד המחירים של הפיצוי הקיים היום; חשיפת זהות המפר על ידי חברות התקשורת; או הטלת קנסות מנהליים על מפרים "מקצועיים".

22. בחינה מחודשת בנוגע להרחבה ראויה של תחולתו של החוק לעניין הגדרת "מפרסם" ו"דבר פרסומת". הדבר נחוץ בעיקר בנוגע לספאם פוליטי, ולשיחות טלפון אנושיות.

23. בעוד שאיננו סבורים שיש להטיל חבות משפטית על נמענים להגן על עצמם מפני מסרים לא רצויים, ברור לנו שככל שפרטים ישתמשו באמצעי הגנה טכנולוגיים אפקטיביים שמטרתם מניעת ספאם, היקפי התופעה יצטמצמו, ואנו ממליצים על כך.

24. המלצנו על תיעדוף של חברות טכנולוגיה שיספקו מוצרים שהוטמעו בהם מראש עקרונות וערכים של הנדסת ניקיון, למשל כאשר גופים במגזר הציבורי יונחו להעדיף רכישת מוצרים כאלה על פני רכישת מוצר זהה למעט שלא הוטמעו בו ערכי הנדסת ניקיון. במקרה שבו יחליט הרגולטור להפוך את הגישה של הנדסת ניקיון למחייבת עבור ספקיות השירותים, חברות הטכנולוגיה המספקות מוצרים לחברות אלה יתומרצו לפעול אף הן לפי כללים אלה ולהטמיע במוצריהן מראש ערכים של ניקיון המערכת ממסרים לא רצויים.

25. יש לקבוע רף מינימלי של שירות סינון שחברות אלה מחויבות לספק ללקוחותיהן. בנוסף, המלצנו ליצור פרוטוקול אחיד שיועבר לכל משתמשי חברות התקשורת, שעניינו הקניית אוריינות דיגיטלית בסיסית בכל הנוגע לספאם ולדרכים להימנע ממנו.. לעניין הפטור מאחריות ממנו נהנות ספקיות התקשורת ולעיתים גם חברות ההפצה, המלצנו להקיש מהסדרים קיימים בתחום אסדרת פעילות גורמי ביניים שונים כמו פלטפורמות של רשתות חברתיות, ולאמץ נוהל הודעה והסרה בליווי חזקות מתאימות לעניין הספאם.

26. גם בנוגע לרשתות חברתיות, המלצנו לרגולטור להציב רף מינימלי מחייב של הגנה על משתמשים מפני ספאם באמצעות מסננים ייעודיים, כאשר יוטל על החברות בנוסף לדאוג לכך שמשתמשים יידעו על מסננים אלה ועל האופן להפעילם. בנוסף, המלצנו על עידוד המחקר המבקש לפתח טכניקות לאיתור חתימה מלאכותית של בוטים ברשתות, תוך שיתוף פעולה של מומחי אבטחת סייבר וחוקרי למידת מכונה.

27. המלצנו בנוסף על השקעה במחקר ופיתוח מטעם המדינה של כלים טכנולוגיים למלחמה בספאם, שיוכלו לשמש את כלל האוכלוסייה, בדומה למשל לאפליקציית המגן שפותחה בעת המאבק של מדינת ישראל במגפת הקורונה. פיתוח כלים כאלה ייעשה תוך הטמעת עקרונות של הנדסת ניקיון.

היבט חשוב של תופעת הספאם הוא שהיא חלק ממערכת גדולה יותר של כלכלת ייצור מסרים המוניים, ולכן אי אפשר להתייחס אליה כאל בעיה שיש להיפטר ממנה אחת ולתמיד, אלא להבין שבכלכלת מידע המבוססת על הצפת מידע, ספאם הוא חלק בלתי נמנע מהמערכת כולה. לכן, המלצנו לאמץ הבנה ולפיה מדובר בתופעה שלא ניתן למגר כליל ולכן, לעת עתה, כדאי להתמקד בפתרונות ארוכי טווח שיצמצמו את התופעה ואת השלכותיה מתוך ידיעה שתופעת הספאם תישאר איתנו.

ספאם: מילון מונחים וקיצורים

אוריינות דיגיטלית

שליטה במגוון הולך וגדל של מיומנויות טכניות, קוגניטיביות וסוציולוגיות הנדרשות לשם ביצוע מטלות ולפתרון בעיות בסביבות דיגיטליות.

בוֹטנֶט – Botnet

מערך חיבור של מחשבים רבים זה לזה ברשת, שמאפשר הוצאה לפועל של משימות הזקוקות למשאבים חישוביים רבים. בדרך כלל, המונח מתייחס למערכת כזו המשמשת לביצוע משימות "זדוניות". לבוטנט יש בדרך כלל ערוץ "פיקוד ושליטה" שאחראי להעברת הוראות הפעלה לשאר המחשבים המחוברים לרשת שלו.

דבר פרסומת

הסדרת הספאם בדין הישראלי מתייחסת ל"דבר פרסומת". לפי ההגדרה בס' 30א(א) לחוק התקשורת, דבר פרסומת הוא מסר מסחרי שמטרתו לעודד את הנמען לרכוש דבר מה. הגדרת "דבר פרסומת" היא רחבה, ומסייגת רק מסרים פוליטיים. אמצעי שיגור המסר עליהם חל החוק הישראלי הם פקס, מערכת חיוג אוטומטית, הודעה אלקטרונית (כלומר דוא"ל) או הודעת מסר קצר (SMS, מסרון). החוק חל גם על "צנתוק", כלומר חיוג שהופסק בטרם נענתה השיחה ("צנתוק" הוא הלחמה של צלצול-ניתוק), ובהמשך לכך מחייג הנמען בחזרה למספר ממנו התקבלה השיחה ונענה בהשמעה של פרסומת.

דיוור ישיר

סעיף 17ג לחוק הגנת הפרטיות מגדיר "דיוור ישיר" כ"פניה אישית לאדם, בהתבסס על השתייכות לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע."

הנדסת ניקיון

ההיתכנות של תכנון מוקדם של טכנולוגיה על מנת לסייע בשמירה על "ניקיון" המערכת האקולוגית התקשורתית, כדי לצמצם פעילות של דואר זבל לא חוקי.

הנדסת פרטיות (Privacy by Design)

גישה שמבקשת לשלב את ההגנה על הפרטיות בתוך מערכת טכנולוגית כלשהי כבר בשלב בו מפתחים את המערכת, ולא רק בדיעבד. הרעיון של הנדסת פרטיות הוא גיוס הטכנולוגיה להסדרת ההתנהגות בה מדובר, ושילוב והטמעה של הגנת הפרטיות בטכנולוגיה, כבר בשלב התכנון והעיצוב שלה, ולא בשלבים שלאחר השימוש בטכנולוגיה, כאשר תיקון הוא בדרך כלל מסורבל, יקר ולעיתים קרובות נכשל.

הפרה יעילה

מושג שצמח מתוך דיני החוזים, והמצביע על התנהגות של צד לחוזה הבוחר להפר במודע את החוזה, משום שמשתלם עבורו יותר לנהוג כך. המושג יכול להצביע על כל הפרת חוק שנעשית במודע, כאשר המפר סבור שגם אם ייאלץ לשלם את מחיר ההפרה, עדיין משתלם לו יותר להפר.

כלכלת ספאם

שיווק מבוסס-ספאם הוא עסק, ותעשיית הספאם היא מפעל רווחי. כלכלת הספאם הדיגיטלית היא מערכת אקולוגית-טכנולוגית-עסקית סבוכה ומרובת שחקנים, שלכל אחד מהם אינטרסים שונים ומגוונים, שלעיתים מתלכדים זה עם זה ולעיתים הם סותרים. מערך מורכב של שחקנים ראשיים, שחקני ביניים ומשאבים משמש לייצור רווח משליחת ספאם.

בכלכלת הספאם הכמות היא שם המשחק, משום שהעליות הנמוכות של דיוור אלקטרוני המוני וזמינותו הגבוהה מביאים לכך שדי באחוז קטן של משתמשים שייענו להצעה שיווקית, כדי שהמהלך ישתלם. כלכלת הספאם מעודדת משלוח מסרים שיווקיים בהיקפים גדולים, תוך החצנת העלויות לנמענים ולספקי השירות, ולעיתים תוך ניצול לרעה על ידי גורמים עוינים למשתמשים.

מסנן ספאם

כלי אוטומטי שבוחן מסרים לפני העברתם לנמען, ומזהה ספאם. המסנן מתבסס על תוכן ההודעה (מסנן מבוסס תוכן), על מאפייני השולח (מסנן מבוסס מקור), על "ידיעה" של הנמען, כלומר האם הנמען מחשיב הודעות דומות כספאם או את המוען כספאמר, על נפח ההודעות שנשלחו ממקור מסוים (מסנן נפח) ועוד. לשם כך משתמש המסנן בידע מובנה, באלגוריתמים שונים, במשובי משתמשים ובמשאבים חיצוניים כגון רשימות שחורות או דוחות ממשתמשים אחרים. מסנן יכול להיות מותקן בשרתי ספקית התקשורת, או במכשיר הקצה של המשתמש.

"מפרסם"

חוק התקשורת ס' 30א(א) מגדיר "מפרסם" כך: "... מי ששמו או מענו מופיעים בדבר הפרסומת כמען להתקשרות לשם רכישתו של נושא דבר הפרסומת, מי שתוכנו של דבר הפרסומת עשוי לפרסם את עסקיו או לקדם את מטרותיו, ובכלל זה לקדם קבלת תרומות או תעמולה, או מי שמשווק את נושא דבר הפרסומת בעבור אחר; לעניין זה, לא יראו כמפרסם מי שביצע, בעבור אחר, פעולת שיגור של דבר פרסומת כשירות בזק לפי רישיון או תקנות ההיתר הכללי, לפי העניין."

ספק לִידִים

ספק לידים (מלשון lead), הוא מי שמספק למשווקים את רשימות התפוצה, אותן הוא אוסף או רוכש מבעלי מאגרי מידע. ספק הלידים הוא הגורם שמחפש נמענים שהם צרכנים פוטנציאליים, ויכול למצוא אותם בצורה לגיטימית (רשימות מאושרות, פרסומות, דפי נחיתה של אתרים שאליהם גולשים פונים מיוזמתם שלהם) או בדרכים לא חוקיות (למשל רכישת מאגרי מידע שנגנבו ונמכרו ברשת האפלה, ה-dark net).

פישינג

פישינג או דיוג (באנגלית: phishing) הוא ניסיון לגנוב מידע באינטרנט על ידי התחזות לגורם לגיטימי.

צנתוק

חיוג שהופסק בטרם נענתה השיחה (צנתוק הוא הלחמה של צלצול-ניתוק). מדובר בתופעה של חיוג לנמען באמצעות מערכת חיוג אוטומטי וניתוק השיחה בטרם נענתה, כדי לגרום לנמען לחייג בחזרה את אותו המספר, כך שהמפרסם יוכל להשמיע לנמען את דבר הפרסומת או את המסר.

רובוקולס - Robocalls

שיחות טלפון שמשתמשות בחייגן אוטומטי כדי להעביר הודעה מוקלטת מראש, לכמות נמענים גדולה.

(ה)רשות להגנת הפרטיות

הגוף המסדיר, המפקח והאוכף על פי חוק הגנת הפרטיות, התשמ"א-1981. במסגרת תפקידה כרגולטור של זכות היסוד לפרטיות ולהגנת מידע אישי בישראל, מופקדת הרשות על הגנת המידע האישי במאגרי מידע דיגיטליים מכוח חוק הגנת הפרטיות ועל ביצורה של הזכות לפרטיות. לתכלית זו הרשות מפעילה רגולציה, לרבות אכיפה מנהלית ופלילית, על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי דיגיטלי.[60] הרשות היא יחידה במשרד המשפטים, ולפנים נקראה הרשות למשפט וטכנולוגיה (רמו"ט).

60 ראו: https://www.gov.il/he/departments/about/about_ppa.

רשימה שחורה

רשימה שחורה היא מאגר כתובות שמהן נשלח ספאם, שמאפשר חסימת שירותים והטלת סנקציות על שחקנים "שסרחו". רשימות שחורות מורכבות על ידי גופים שונים, פרטיים (למטרת רווח) או ציבוריים (כמו עמותות שמטרתן לוחמה בספאם ובבעיות אבטחה). שרת דואר יכול לחפש את כתובת ה-IP ממנו מגיע מסר, ולדחות מסר שמגיע מכתובת שמופיעה ברשימה שחורה. מנהלי מערכות יכולים לבחור מתוך מגוון גדול של רשימות, כאשר כל רשימה משקפת סטנדרט עצמאי של סינון, בהתאם למדיניות הרשימה.

רשת אפילה (dark net)

רשת שפועלת על פני תשתית האינטרנט, ושהגישה אליה אפשרית רק באמצעות תוכנה, הגדרה או אישור ספציפיים לרשת. כל הרשתות האפלות דורשות שינוי הגדרות או התקנה של תוכנה מסוימת כדי שמשתמש יוכל להתחבר אליהן.

רשת שותפים

פלטפורמות המקשרות בין גורמים העוסקים בפרסום בזירות טכנולוגיות שונות (השותפים), ובין בעלי עסק המעוניינים לפרסם את עסקיהם.

שם מתחם

שם מתחם או שם תחום (domain name) הוא שמו הייחודי של אתר אינטרנט. לכל אתר אינטרנט שם מתחם משלו, המאפשר לזהותו. בישראל, איגוד האינטרנט הישראלי הוא הגוף היחיד המורשה לרשום שמות מתחם. שם המתחם מקושר לכתובת האתר במרחבי הרשת.

שרשרת הערך של הספאם

סך השחקנים והמשאבים שמעורבים במאמץ להפוך ספאם לרווחי בשרשרת שני שלבים מרכזיים: הראשון כולל את כל הפעילות המתרחשת לשם יצירת ספאם ושליחתו, עד לרגע שבו מגיע הספאם אל הנמען. השני כולל את כל הפעילות המתרחשת במידה שספאם "הצליח", והניע את הנמען לרכישה.

GDPR

General Data Protection Regulation. זו החקיקה המרכזית בתחום הגנת המידע באיחוד האירופי, משנת 2016, שנכנסה לתוקף בשנת 2018. ל-GDPR יש תחולה ישירה במדינות האיחוד. הרגולציה קובעת את המותר והאסור בקשר לאיסוף מידע, עיבודו, ושימושים אחרים בו, בדרך של קביעת זכויות לנושאי המידע (data subjects), הטלת חובות על אוספי ומעבדי המידע (data controllers), ואפשרויות אכיפה, וכן כללים מבוססי-תהליך, שנועדו להביא להטמעת הכללים המהותיים בתוך ארגונים, כמו הנדסת פרטיות, או מינוי ממונה הגנת פרטיות ארגוני.

רשימת קיצורים

AI	**A**rtificial **I**ntelligence
AL	**A**ccess **L**ayer
API	**A**pplication **P**rogramming **I**nterface
CLI	**C**ommand-**L**ine **I**nterface
FTC	**F**ederal **T**rade **C**ommission
GDPR	**G**eneral **D**ata **P**rotection **R**egulation
IP	**I**nternet **P**rotocol
ISP	**I**nternet **S**ervice **P**rovider
ML	**M**achine **L**earning
NLP	**N**atural **L**anguage **P**rocessing
PSTN	**P**ublic **S**witched **T**elephone **N**etwork
SMSC	**S**hort **M**essage **S**ervice **C**enter
SPL	**S**ervice **P**rovider **L**ayer
TCPA	**T**elephone **C**onsumer **P**rotection **A**ct
URL	**U**niform **R**esource **L**ocator
VoIP	**V**oice **O**ver **I**nternet **P**rotocol
VPN	**V**irtual **P**rivate **N**etwork