

סדרת פרסומי המרכז למשפט וטכנולוגיה

חוברת מס' 4

דואר או זבל?

ההסדרה של

דואר אלקטרוני לא-רצוי

מאת

תלמידי הסדנה הרב-תחומית במשפט וטכנולוגיה
הפקולטה למשפטים, אוניברסיטת חיפה

Haifa Center of Law & Technology
University of Haifa, Faculty of Law
Mail or Junk? The Regulation of Spam

© כל הזכויות שמורות למרכז למשפט וטכנולוגיה.
חיפה, תשס"ה-2004.

שימוש הוגן בנייר העמדה מבורך.

נא לצטט את המסמך כך :

יניב דרוקמן ואח', **דואר זבל – ההסדרה של דואר אלקטרוני לא-רצוי** (המרכז למשפט וטכנולוגיה, עורכים :
ניבה אלקין-קורן, מיכאל בירנהק, 2004).

ליצירת קשר :

טל' 04-8288569, פקס : 04-8240681

דוא"ל : techlaw@law.haifa.ac.il

אתר הבית : <http://techlaw.haifa.ac.il>

ISSN 1565-5741

Printed in Israel

צוות הכותבים

יניב דרוקמן יניב סימסולו סער סיקלאי

תלמידי הסדנה למשפט וטכנולוגיה – תשס"ד

יעל און	מיכאל גבע
יניב דרוקמן	אריאל זיסמן
רום טימור	ענבל לב
ארז מארון	תמר מרון
יוסי נחמני	יניב סימסולו
סער סיקלאי	עדי פוקס
מאור פישמן	שי פקר
לטם פרי	

מנחים ועורכים

ד"ר ניבה אלקין-קורן ד"ר מיכאל בירנהק

בשיתוף המכון ליישומים בינתחומיים של מדעי המחשב
ע"ש קרן קיסריה אדמונד בנימין דה-רוטשילד

הקדמה ודברי תודה

הפרסום שלפניכם הוא פרק מקדים מתוך נייר עמדה בנושא פרטיות בסביבה הדיגיטאלית, שיתפרסם בחודשים הקרובים. פרק זה הופרד משאר הפרקים הן כדי שישמש חומר רקע לכנס המרכז למשפט וטכנולוגיה "דואר או זבל?" המתוכנן ליום 16 בדצמבר 2004, באוניברסיטת חיפה, והן, כפי שיוסבר בהמשך, משום שבמהלך עבודת הסדנה למשפט וטכנולוגיה שחקרה את הנושא, התברר לנו כי הקשר בין דואר זבל לפרטיות הוא עקיף בלבד.

הסביבה הדיגיטאלית מאפשרת שימושים חדשים במידע: בדרכי איסוף, עיבודו, שמירתו והפצתו. השינויים הטכנולוגיים האלו יוצרים מחד גיסא הזדמנויות עיסקיות חדשות, ומאידך גיסא, איומים חדשים על הפרטיות. הפרטיות נתפסת כזכות יסוד, היא מהווה מרכיב חיוני ביצירת סביבה בטוחה לסחר האלקטרוני, ובו בזמן מהווה מסווה לפעילות פלילית וטרוריסטית, ולכן היא עניין גם לגורמי אכיפת החוק.

הסדנה למשפט וטכנולוגיה בשנת הלימודים תשס"ד התמקדה בשאלת הפרטיות ברשת בכלל ובישראל בפרט. ביקשנו להבין את הצרכים של התעשייה, השחקנים בזירת הסחר האלקטרוני, המדינה וגורמי אכיפת החוק, וכמובן גם של הגולשים. בדקנו את האפשרויות הטכנולוגיות השונות למעקב, איסוף מידע, עיבודו והשימוש בו. את האפשרויות הטכנולוגיות מיקמנו במסגרת המשפטית הישראלית, תוך היעזרות במשפט משווה, ושאלנו האם המשפט צריך להתערב, ואם כן כיצד ובאילו מקרים, ומהם הפתרונות החלופיים שמציע השוק ומציעה הטכנולוגיה.

בסדנה השתתפו חמישה עשר סטודנטים מצטיינים מן הפקולטה למשפטים באוניברסיטת חיפה אשר נבחרו בתהליך מיון קפדני. הסדנה למשפט וטכנולוגיה מהווה מסגרת מחקר ייחודית העוסקת בשאלות מעשיות מתחום מדיניות המידע. עיצוב המדיניות בתחום המשפט וטכנולוגיה מתרחש לא רק בבתי המשפט, אלא גם – ובמידה רבה – בכנסת וברשויות המדינה השונות. מעצבי המדיניות אשר זקוקים למידע, נתונים, הערכות, ניתוח המשמעות וההשלכות של המדיניות על מנת שיוכלו לקבוע את דרכי פעולתם, ניזונים בעיקר מקבוצות אינטרסים המספקות נתונים אשר כמובן מקדמים את ענייניהם. הקול הציבורי כמעט שאינו נשמע בדיונים האלה. גם חברות רבות, ובעיקר חברות סטארט-אפ חדשות, זקוקות להדרכה משפטית בנושאים בעלי נגיעה ציבורית. הסדנה למשפט וטכנולוגיה נועדה למלא את החלל הזה.

עבודת המחקר והכתיבה בסדנה התנהלה במספר שלבים. לאחר סיעור מוחות ראשוני וגיבוש נושאי המחקר, צוותו המשתתפים לצוותי עבודה, על-פי נושאים שונים. המשך המחקר התנהל במפגשים פנים-אל-פנים ובדיונים קבוצתיים באמצעות פורום אינטרנטי, בהם לובנו השאלות והנושאים שעל הפרק. עם השלמת המחקר והשלמת הטיוטא הראשונית של נייר העמדה, סברנו כי יש מקום ללמוד מה עמדתם של מומחים ובעלי מקצוע בתחומים שבהם עסקנו. כך בא לעולם כנס נווה אילן (19-17 לדצמבר, 2003). במשך שלושה ימים מרוכזים דנו בסוגיות שעל הפרק עם עשרות מומחים מתחומי מחקר ועיסוק שונים, ובעיקר מדעי המחשב ומשפטים. המשפטנים באו מהאקדמיה, מהשוק הפרטי ומהמגזר הציבורי. הדינמיקה שנוצרה במהלך שלושת ימי הסדנה, ההרצאות המאלפות והדיונים הפוריים הבהירו יותר מכל את הצורך בדיון בלתי תלוי ובעבודת מחקר עצמאית ורב תחומית בנושאים הקשורים למשפט וטכנולוגיה.

הנייר הוא פרי עבודתם של הסטודנטים בסדנה ומייצג את עמדתם הקולקטיבית, ואינו משקף בהכרח את עמדת מקום עבודתם הנוכחי או את עמדתם של העורכים.

לקחי המחקר וכנס נווה-אילן בכל הנוגע לסוגיית דואר הזבל מסוכמים בנייר העמדה שלפניכם. בסוגיות רבות משקף נייר העמדה ניסיון ראשון מסוגו להתמודד עם סוגיות אשר טרם זכו לדיון ציבורי בישראל. אנו תיקווה שנייר העמדה יהיה בסיס לדיון רציני בסוגיות הטעונות הכרעה ויסייע בעיצובה של מדיניות מושכלת.

פעילות הסדנה התאפשרה הודות לתמיכתו הנדיבה של **המכון ליישומים בין-תחומיים של מדעי המחשב ע"ש קרן קיסריה, אדמונד דה-רוטשילד**. אנו מבקשים להודות לראשי המכון ליישומים בינתחומיים של מדעי המחשב, פרופסור **מרטין גולומביק** וד"ר **אירית הרטמן**, שסיפקו לא רק את האמצעים, אלא הפגינו התלהבות לאורך הפרוייקט כולו, ותרמו באופן פעיל למפגש עצמו. אנו מבקשים להודות גם לגבי **ליבי עודד**, מזכירת המכון.

אנו מבקשים להודות גם לאנשי הפקולטה למשפטים באוניברסיטת חיפה שסייעו לנו: הדיקן פרופסור **אריאל בנדור**; ממלא מקום הדיקן, פרופסור **עלי זלצברגר**; ראש מינהל הפקולטה, **משה סייג**, ומתאמי התיקשוב, **יותם ורד וסער בן משה**.

שורת מומחים נכבדה הקדישה זמן ומאמץ לסדנה, ותרומתם של אורחי הסדנה כולם הייתה רבה. האורחים מיקדו את השאלות העומדות לדיון, הציגו זוויות רבות ומגוונות לסוגיות שעל סדר היום, חידדו נקודות עמומות, ואנו מבקשים להודות לכולם (לפי סדר א"ב):

שלומי אונגר, מנכ"ל "מחשבה"; עו"ד **דן אור-חוף**, רביה ושות' עורכי דין; ד"ר **יובל אלוביץ'**, החוג להנדסת מערכות מידע, אוניברסיטת בן-גוריון בנגב; עו"ד **שלי בן-ארי**, tmicha.net; פרופסור **אריאל בנדור**, דיקן הקולטה למשפטים, אוניברסיטת חיפה; ד"ר **יוסי ברג**, היועץ המשפטי של המועצה הישראלית לצרכנות; **אמיר גנס**, מנהל עסקי, New Approach; עו"ד **ריבקי דב"ש**, מחלקת ייעוץ וחקיקה במשרד המשפטים; ד"ר **גיא דוידוב**, הפקולטה למשפטים, אוניברסיטת חיפה; עו"ד **יעקב וילון**, מחלקת ייעוץ וחקיקה, משרד המשפטים; עו"ד **יוספה טפיירו**, רשמת מאגרי המידע, משרד המשפטים; ד"ר **משה כהן-אליה**, המכללה האקדמית למשפטים, רמת-גן; ד"ר **נעמה כרמי**, אוניברסיטת חיפה והמרכז הבינתחומי הרצליה; **אמיר לב**, נשיא Commtouch; **אלון מוליאן**, סמנכ"ל MRM; **רן נטף**, סמנכ"ל מידע וניהול ידע, DataSafe; עו"ד **חיים קלוגמן**, יו"ר המועצה הציבורית להגנת הפרטיות; השופט **גבריאל קלינג**, סגן נשיא בית המשפט המחוזי בתל-אביב (בדימוס); ד"ר **יובל קרניאל**, בית הספר למשפטים ובית הספר לתקשורת, המסלול האקדמי, המכללה למינהל; ד"ר **רבקה ריב"ק**, החוג לתקשורת, אוניברסיטת חיפה; עו"ד **יהושע שופמן**, המשנה ליועץ המשפטי לממשלה לענייני חקיקה; **אמיר שור**, אחראי פתרונות לקוח, ברק 013; **איל שיף**, קצין פרטיות dotomi; ד"ר **ברכה שפירא**, החוג להנדסת מערכות מידע, אוניברסיטת בן-גוריון בנגב.

כמו כן, אנו מבקשים להודות למשתתפים נוספים שהצטרפו אלינו לסדנה ותרמו רבות לדיונים ולמי שהקדישו לנו מזמנם ויעצו: עו"ד **ערן ברקת**; עו"ד **גיל גרנות-מאיר**; עו"ד **דלית דרור**; **רונן האוסירר**; **אלעד וידר**; ד"ר **אמיר חורי**; **נחמן ליס**; פרופסור **מוטי מירוני**; **רן קמיל**; עו"ד **חיים רביה**; **אורלי רייכמן**; **אריאל שוורץ**.

הפקת האירוע התאפשרה בזכות **ענבל לב**, מתאמת המרכז למשפט וטכנולוגיה בתשס"ד. הפקת נייר העמדה התאפשרה בזכות **אלעד וידר**, המתאם הנוכחי של המרכז.

ניבה אלקין-קורן, מיכאל בירנהק
חיפה, דצמבר 2004.

הערה:

כל האמור בלשון נקבה או בלשון זכר מתייחס גם ללשון האחרת.
כל הקישורים המופיעים במסמך זה נבדקו לאחרונה ביום 16.11.04.

תוכן עניינים

i.....	הקדמה ודברי תודה
1	1. מבוא
1.....	א. מהו דואר זבל אלקטרוני?
3.....	ב. שורש הבעיה
7.....	ג. היקף הבעיה
8.....	ד. דואר זבל והגנת הפרטיות
11.....	ה. דואר זבל פוגעות וחופש הביטוי
12	2. טכנולוגיות בשימוש הספאמרים
12.....	א. טכנולוגיות ואמצעים להפצת הודעות דואר זבל אלקטרוני
15.....	ב. דרכים להשגת כתובות דואר אלקטרוני לשם שליחת דואר זבל
19	3. הסדרה פרטית של דואר זבל
19.....	א. תוכנות סינון
23.....	ב. מחלקת ה-Abuse של ספקית האינטרנט
24.....	ג. מאגרי מידע על שולחי דואר זבל
24.....	ד. שינוי הארכיטקטורה של האינטרנט על מנת לצמצם את היקף דואר הזבל
28.....	ה. חזרה לעידן בולי הדואר
30	4. מודלים משפטיים: ארצות הברית, האיחוד האירופי ונטיקט
30.....	א. ארצות הברית
36.....	ב. האיחוד האירופאי
37.....	ג. כללי האתיקה של הרשת
38	5. דואר זבל כחול-לבן: המצב המשפטי
38.....	א. החקיקה הקיימת
40.....	ב. הפסיקה
40.....	ג. הצעות החוק
45	6. הסדרה ציבורית: פתרונות משפטיים אפשריים
45.....	א. שיתוף פעולה בין לאומי
45.....	ב. חובת תיוג דואר זבל פרסומי
45.....	ג. ביטול בדיעבד (Opt Out)
46.....	ד. מתן הסכמה מראש (Opt-In)
48	7. סיכום והמלצות

1. מבוא

נייר עמדה זה מבקש לחקור וללמוד את תופעת דואר הזבל, את התנאים הטכנולוגיים, הכלכליים והחברתיים שאפשרו אותה, ולבחון דרכים שונות להתמודדות עם דואר הזבל. במהלך הדברים נבחן גם את מידת הקשר שבין הסוגיה הספציפית להגנת הפרטיות ולחופש הביטוי. המחקר מסכם בהמלצות, שתמציתן מופיע גם לעיל. סוגית דואר הזבל היא חשובה ומעניינת לכשעצמה, כפי שיובהר בעמודים הבאים, אולם היא משמשת מקרה מבחן לשאלות רחבות יותר, בדבר היחס שבין משפט לטכנולוגיה.

בפרק זה נגדיר את התופעה בה מדובר. נעמוד על הקושי בהגדרה, ומתוך כך כבר נאבחן בין דואר זבל לדיוור ישיר, ומכאן נפריד בין שאלת הגנת פרטיות לבעיית דואר זבל. נעמוד על הארכיטקטורה של הרשת שאפשרה את התופעה, כמו גם התנאים הכלכליים שלה, ונסה לאמוד, בהתבסס על מחקרים שונים, את היקף הבעיה. לאחר מכן נבחן במישרין את הקשר שבין דואר זבל לשאלות הגנת הפרטיות וחופש הביטוי.

דואר הזבל אינו תופעה חדשה. הודעת דואר הזבל הראשונה נשלחה לראשונה כבר ב-1978 ברשת ה-ArpaNet (שלימים הפכה להיות האינטרנט). אותו דואר זבל ראשון נשלח כמעט לכל מנויי הרשת בחוף המערבי של ארצות הברית. במקרה זה סוכנות ה-DCA האמריקנית (מפעילת רשת ה-ArpaNet) התלוננה בפני שולח דואר הזבל והבהירה לו כי השימוש ברשת הוא לצרכי מחקר ולימוד בלבד. בניגוד לדואר הזבל כיום, דווקא באותם ימים התלוננו המנויים שלא קיבלו את אותו דואר זבל, מפני שהרגישו כאילו הם נשכחו מחוץ למעגל הפרסום החדש.¹ אך כיום דואר זבל, היא מילת גנאי באינטרנט.

א. מהו דואר זבל אלקטרוני?

הקושי בהגדרה

ניתן להניח, כי כל אדם אשר עושה שימוש פעיל בכתובת דואר אלקטרונית חשוף לתופעת דואר הזבל ואף מבין אינטואיטיבית את משמעות המושג "דואר זבל". יחד עם זאת, אין זה פשוט להגדיר את המושג מבחינה משפטית באופן ממצה שיתאים ויתאר כל תכתובת לא מוזמנת, לא רצויה, לא מועילה באופן ישיר,² או שקרית ומוטעית,³ המוצאת את דרכה אל תא הדואר האלקטרוני של נמען.

הקושי בהגדרה אינו רק עניין טכני. הוא משקף את האינטרסים היריבים בשאלת ההסדרה של הדואר האלקטרוני שלא נתבקש על-ידי הנמען. לנמענים אינטרס שלא להיות מוטרדים,

¹ Brad Templeton, "Reflections on the 25th Anniversary of Spam", **Templetons.com** (2003), <http://www.templetons.com/brad/spam/spam25.html>. כל הקישורים המופיעים במסמך זה נבדקו לאחרונה ביום 16.11.04.

² ראו את הצעת המועצה הישראלית לצרכנות, **הצעה לתיקון חוק הגנת הפרטיות (מניעת פניות בלתי מוזמנות)**, תשס"ג-2003, בסעיף 17(א).

³ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, §5(a)(1) (CAN SPAM Act, 2003).

וייתכן אף שניתן לתאר אינטרס זה בלבוש של זכות קניין או זכות לפרטיות (על כך נרחיב בהמשך). לשולח דבר הדואר, מנגד, יש זכות לחופש הביטוי (בין המסחרי ובין שאינו מסחרי), כמו גם זכות לחופש העיסוק (וגם על כך נרחיב בהמשך). ההגדרות השונות ערות לשיקולים אילו, ומבקשות – במידה זו או אחרת של הצלחה – להפנימן לתוך ההגדרה. כדי להמחיש את הקושי, הנה מספר דוגמאות:

- הצעה להשתתף "במבצע" שבמסגרתו מחולקת מתנת חינם ללא כל התחייבות של הלקוח. נניח כי ההצעה אמיתית ואינה בגדר הונאה. הגם שהודעת הדואר לא נתבקשה, רבים ישמחו לקבלה.
- פנייה פוליטית: אין בה פן של התעשרות, ניצול או הונאה מסחרית, ומדובר בביטוי הנמצא ב"גרעין" חופש הביטוי.
- פנייה לתרומה (שאינה תרגיל "עוקץ").

כיצד נבחין בין פניות הנהנות מהגנה גבוהה של חופש הביטוי לבין פניות מסחריות לא רצויות? בתקופה האחרונה הוצעו מספר הצעות חוק בעניין, שנקטו גישות שונות. בהמשך נבחן את הצעת החוק של משרד התקשורת, וכן את הצעת חוק פרטית שהוגשה על-ידי חבר הכנסת רומן ברונפמן. הצעה ראשונה שפורסמה בשנה החולפת היא של המועצה הישראלית לצרכנות,⁴ ואנו מבקשים לעיין בה בקצרה, לשם בירור המושג – דואר זבל. הצעת החוק מתייחסת לדואר זבל בעל אופי מסחרי פרסומי ותכליתה לאסור על חברות מסחריות להפיץ דואר אלקטרוני אשר לא קיבל את אישור הנמען. ההצעה מבקשת לשנות את חוק הגנת הפרטיות ולהוסיף בו סעיף שיקבע כי מפיץ דואר אלקטרוני בעל אוריינטציה פרסומית יהיה רשאי לשלוח דואר רק מכוח חוזה בינו לבין הנמען, על-פי חוק, או על-פי דרישתו של הנמען. בהצעה מופיע הסייג, לפיו מפיץ הדואר יהיה רשאי להפיצו ללא רשות מצד הנמען כאשר מדובר בדואר אשר הנמען מפיק ממנו תועלת ישירה.

נדמה כי המציעים הגדירו במודע או שלא במודע, על דרך השלילה את המושג דואר זבל, כ- "כל דואר שאינו מביא תועלת ישירה לנמען". הגדרה כזו טומנת בחובה קשיים פרשניים לא מבוטלים, בהיותה רחבה מדי ומצריכה פרשנות אובייקטיבית, וכידוע, מה שמועיל לאחד אינו מועיל בהכרח לאחר. לפיכך, אנו סבורים שבסבך הפרשנות עלול להיווצר מצב שבו הצעת חוק זו, גם אם תחוקק, תעמוד כאבן שאין לה הופכין ולא תשיג את תכליתה.

דואר זבל מול דיוור ישיר

ראוי גם לאבחן את דואר הזבל מהמושג של דיוור ישיר. מושג אחרון זה מוגדר ומוסדר בחוק הגנת הפרטיות. סימן ב' לחוק חל על העוסקים בדיוור ישיר: עליהם לרשום את מאגר המידע המשמש לדיוור ישיר בפנקס מאגרי המידע, בפנייה לנמען עליהם לציין את מקור המידע, לציין כי דבר הפרסום הוא דיוור ישיר, להודיע לנמענים על זכותם להימחק מהרשימה ולציין את זהותו וכתובתו של בעל רשימת הדיוור. דיוור ישיר מוגדר כ"פניה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על-פי איפיון אחד או

⁴ ראו לעיל, הערה 2.

יותר של בני אדם ששמותיהם כלולים במאגר מידע".⁵ כלומר כדי שהוראות הסימן יחולו, דבר הדואר צריך להיות פניה אישית על-פי איפיון אחד או יותר. בכך נבדל הדיוור הישיר מדואר הזבל בו אנו עוסקים כאן: דואר זבל אלקטרוני איננו פניה אישית והאיפיון היחיד עליו הוא מסתמך, הוא הימצאותה של כתובת הדואר האלקטרוני של הנמען ברשימת הכתובות של מפיץ דואר הזבל (להלן: הספאמר). יצוין כבר עתה, כי אם בידי הספאמר רשימה הכוללת רק "שם, מען ודרכי התקשרות" – ולענייננו – כתובות דואר אלקטרוני – הרי אין מדובר כלל ב"מאגר מידע", כפי שהוא מוגדר בחוק הגנת הפרטיות, והחובות השונות המוטלות על מחזיקי מאגרים כלל אינן מופעלות.⁶

ב. שורש הבעיה

את שורש הבעיה של ריבוי הודעות דואר שאינן רצויות ניתן לאתר בשני יסודות: כלכלי וטכנולוגי.

1. הטכנולוגיה של דואר זבל

הסיבה שכל כך קל, זול ופשוט לשלוח דואר זבל אלקטרוני טמונה בפרוטוקול המשמש לשליחת רוב הדואר האלקטרוני בעולם – פרוטוקול SMTP.⁷ כאשר פורסם ב-1982 פרוטוקול SMTP על-ידי ה-IETF,⁸ הייתה רשת האינטרנט פתוחה ואמינה, והגולשים בה היו אנשי מחקר ואקדמיה, כך שמפתחי הפרוטוקול לא ראו צורך לשלב בו אמצעים נגד ניצולו לשליחת דואר אלקטרוני בלתי רצוי. לרוע מזלנו, כאשר האינטרנט התפתח והפך נגיש לציבור רחב מאוד, התחילו שולחי דואר הזבל האלקטרוני (המכונים גם: ספאמרים) לנצל את פשטותו של הפרוטוקול על מנת לשלוח באופן מהיר ובעלויות אפסיות דואר זבל אלקטרוני למיליוני נמענים.⁹ בנוסף פרוטוקול SMTP איננו כולל אמצעים לאימות זהותו של השולח, דבר המאפשר לשולחי דואר הזבל להסתיר את מקורו של הדואר.

⁵ סעיף 17 לחוק הגנת הפרטיות, תשמ"א-1981 (להלן: חוק הגנת הפרטיות).

⁶ סעיף 7 לחוק הגנת הפרטיות.

⁷ SMTP הם ראשי תיבות של Simple Mail Transfer Protocol. פרוטוקול זה שהוצג ב-1982, הוא הפרוטוקול הנפוץ בעולם לשליחת דואר אלקטרוני: <http://www.ietf.org/rfc/rfc0821.txt>.

⁸ The Internet Engineering Task Force - IETF – הארגון שמפתח תקנים להעברת מידע באינטרנט: <http://www.ietf.org>.

⁹ רויטרס, "הסכנה: חומות לדואר האלקטרוני", ynet (11.06.2003), <http://www.ynet.co.il/articles/0,7340,L-2654034,00.html>.

שליחת דואר אלקטרוני באמצעות שרת SMTP ללא אימות זהותו של השולח:¹⁰

1. תחילה, מתחבר השולח לשרת SMTP (דרך שער 25).¹¹ זה יכול להיות שרת הדואר היוצא של ספקית האינטרנט שלנו, למשל:

OPEN smtp.dr-vb.co.il 25

2. השולח ממתין ל"ברכת השלום" (greeting) של שרת ה-SMTP, ברכת השלום נראית למשל כך:

220 msg2s.dr-vb.co.il -- Server ESMTP (MSG)

חלק מהשרתים מוסיפים להודעה שבשורה למעלה את המילים "NO UCE", המציינות כי דרך שרת זה אין להעביר דואר שלא נתבקש (UCE = Unsolicited Commercial Email), אך שולחי דואר זבל בדרך כלל מתעלמים מדרישה זו (שרת ה-SMTP אינו בודק בעצמו, אם הדואר הנשלח הוא דואר זבל מסחרי).

3. השולח משגר בקשת HELO לשרת ה-SMTP, בה הוא מזדהה (בחלק משרתי ה-SMTP אין צורך לבצע בקשה זו ובחלק מהשרתים אין צורך לזהות את השולח):

HELO spammer.noreply.org

שרת ה-SMTP אינו מאמת שאכן שם המתחם שהועבר הוא אכן שם המתחם ממנו נשלח הדואר. אם השרת קיבל את בקשתנו אז יוחזר קוד 250 (OK):

250 msg2s.dr-vb.co.il OK.

4. השולח משגר לשרת את כתובת הדואר האלקטרוני ממנה נשלחת ההודעה:

MAIL FROM: spammer@noreply.org

שימו לב, כי כל כתובת דואר אלקטרוני שהיא חוקית מבחינה תחבירית (לפי כללי התחביר של כתובות דואר אלקטרוני), הייתה מתקבלת על-ידי השרת. השרת אינו מאמת אם אכן כתובת הדואר הזו שייכת לשולח או האם היא בכלל קיימת. כעת השרת יקבל את הבקשה:

250 2.5.0 Address Ok.

השרת קיבל את הבקשה משום שכתובת הדואר האלקטרוני הייתה חוקית מבחינה תחבירית.

5. כעת נשלחת כתובת הנמען:

RCPT TO: ydruk01@study.haifa.ac.il

והשרת מקבל את הבקשה:

250 2.1.5 ydruk01@study.haifa.ac.il OK.

6. כעת נשלחת בקשה לשליחת מידע באמצעות השרת:

DATA

והשרת משיב לנו בחיוב:

354 Please start mail input; end with .

7. כעת נשלחת הודעת הדואר עצמה:

Date: 5 Dec 2003 10:00:00 +0200

From: spammer.noreply.org

To: ydruk01@study.haifa.ac.il

Subject: Spam check

¹⁰ הסבר זה מבוסס על התיאור הרשמי של פרוטוקול SMTP מהמסמך הבא: Jonathan B. Postel, "RFC 821 - Simple Mail Transfer Protocol", IETF (1982), 4-33. המסמך זמין לצפייה בכתובת הבאה: <http://www.ietf.org/rfc/rfc821.txt>.

¹¹ ניתן לנסות את ההדגמה המתוארת כאן (לצורכי מחקר בלבד) באמצעות כל תוכנת Telnet תוך שימוש בשרת הדואר היוצא של ספקית האינטרנט שלכם.

X-Mailer: Workshop spam sender v0.01

I can send spam using this SMTP server.

השרת יקבל כל מידע שנשלח אליו (כתובת השולח, זמן המשלוח והתוכנה שבעזרתה נשלחה ההודעה) ולא יבדוק כלל את נכונותו. לאחר כתיבת ההודעה ושליחתה (על-ידי כתיבת שורה שבה מופיעה '!), תתקבל מהשרת ההודעה שהמסר עומד בתור למשלוח:

250 Mail queued for delivery.

8. אם השולח מעוניין לשגר עוד הודעות (ושולח דואר זבל בוודאי ירצה לעשות כן) אז נשלחת לשרת בקשת RSET.

לסיום המשלוח, נשלחת לשרת בקשת QUIT ואז השרת ישלח את ההודעה או ההודעות שביקשנו לשלוח:

QUIT

221 Closing connection. Good bye.

בהדגמה זו, ראינו עד כמה קל לנצל שרת SMTP על מנת לשלוח דואר, מבלי שזהותנו אומתה.¹²

שולחי דואר הזבל משתמשים בנוסף בדרך כלל גם בשרתי Proxy, על מנת להסתיר את כתובת ה-IP ממנה נשלח דואר הזבל, וכך הם מקשים על איתורם.

כמו כן חשוב להדגיש כי ההליך המתואר כאן מתבצע בין המחשבים המתקשרים במהירות רבה (בדרך כלל הרבה פחות מעשירית שניה – אך הדבר תלוי במהירות העיבוד של המחשבים ובמהירות התקשורת בין המחשבים), דבר המאפשר לשולחי דואר הזבל לשלוח כ-100,000 הודעות דואר בשעה.

2. הכלכלה של דואר זבל

הטעם השני שבגללו הדואר הלא-רצוי הפך לבעיה, נעוץ בחלוקת העלויות של משלוח הדואר וקבלתו. בשונה מעלות שיחת טלפון, משלוח SMS, פקס או דואר רגיל, הרי בדואר אלקטרוני עיקר עלויות המשלוח מועברות מהשולח אל ספקיות האינטרנט ואל הנמען. עבור ספקית האינטרנט, "זמן" (שכידוע שווה לכסף) כולל גם את העומס על המעבד בשרתי הדואר האלקטרוני שלה. הבעיה מורכבת גם מן העובדה, שהעברת דואר הזבל גוזלת רוחב פס, שרכישתו היא העלות העיקרית עבור ספקיות אינטרנט בינוניות וקטנות, מה שמותיר לספקיות האינטרנט שלוש ברירות: א. לספק ללקוחותיהן חיבור אינטרנט איטי יותר. ב. לספוג את העלויות הנוספות הכרוכות ברוחב הפס הנוסף שצורכת העברת דואר הזבל. ג. להעלות את תעריפי הגלישה באינטרנט ללקוחותיהן.¹³

¹² אמנם קיימת הרחבה לפרוטוקול SMTP המאפשרת לאמת את זהותו של השולח, אך רוב שרתי ה-SMTP אינם מממשים אותה. ההרחבה מתוארת ב-RFC2554 בדף הבא: <http://www.ietf.org/rfc/rfc2554.txt>

¹³ CAUCE, "Unsolicited Commercial Email - The Problem", [cauce.org](http://www.cauce.org), <http://www.cauce.org/about/problem.shtml>

כלכלנים קוראים לתופעה זו "החצנה שלילית". הכלכלן זוכה פרס נובל, Ronald Coase, כתב על הקושי שבהחצנה שלילית: כאשר עסק לא יעיל (עסק שלא יכול לעמוד בעלויות הפעילות שלו – שזהו עסק שליחת דואר הזבל במקרה שלנו), מפזר את העלויות שלו על פני "קורבנות" רבים, שלמרות שיש להם נזק, הוא לרוב לא משמעותי כל כך על מנת שהם יפעלו במישור המשפטי וישכרו את שירותיו של עורך דין. מצב כזה במונחים כלכליים, הוא מתכון לאסון, בגלל שמרשים לאי-היעילות להמשיך להתקיים, דבר שגורם לשוק החופשי להיכשל. כך ש"היד הנעלמה" שמאזנת את השוק ושומרת על כך שהוא יהיה יעיל, מנוצחת על-ידי אי-היעילות שמוציאה אותה משיווי משקלה.¹⁴

כיוון ששולחי דואר הזבל מודעים למאמצי המשתמשים והספקים להימנע מהעברה, קבלה וקריאה של הודעות הזבל, התפתח מערך של אמצעים של המפיצים להתחמקות מאמצעי הסינון. שולחי דואר הזבל המנסים לחמוק מתוכנות סינון, מעבירים את ההודעות שלהם דרך שרת דואר של צד שלישי תמים. הטקטיקה הזו מכפילה את הנזק הנגרם, על-ידי כך שגם המערכת המקבלת וגם המערכת המעבירה מוצפות בדואר זבל המעלה את עלויות תפעולן.

שולחי דואר הזבל מסווים, לרוב, את הודעותיהם מתוכנות הסינון על-ידי הצגה של הטקסט כקלט גרפי. קלט כזה חומק לעתים מידי תוכנות הסינון. ההשפעה של אמצעי התחמקות אלה על המשתמשים היא שהספק נאלץ להפעיל אמצעי סינון יעילים ומורכבים יותר כל הזמן. לאמצעים אלה עלות גבוהה במונחי תוכנה. כלומר – אמצעי פענוח הודעות הזבל וסילוקן מהמערכת דורש משאבי עיבוד וזיכרון גדולים במחשבי הספק. לכך יש השפעה על כוח המחשוב אותו נאלץ הספק להפעיל, ועל זמן ההמתנה של דברי הדואר אותם אנו מעוניינים לקבל בתור הדואר הנכנס של הספק. בנוסף, הודעות הזבל שהצליחו לחמוק ממסנני הספק מאוחסנות על מחשביו – ושוב מגולגלת הוצאת האחסון המוגדלת אל הלקוח.

ניתן לראות כי שליחת דואר זבל כמוה כזריקת אבן לאגם. לפעולה הפשוטה יש מעגלי השפעה רבים, שבסופם הלקוח משלם. החשש הוא שדואר הזבל יהפוך את שרות הדואר האלקטרוני לכלי לא שימושי לתקשורת עסקית. אם כמויות דואר הזבל לא יוקטנו באופן משמעותי יהפוך הדואר האלקטרוני לכלי שאינו שימושי אף לצרכים פרטיים.

¹⁴ Ronald Coase, "The Problem of Social Cost", *J. of L. & Econ.* 1, 42-44 (1960)

ג. היקף הבעיה

חברת Brightmail, העוסקת בסינון דואר עבור ספקיות אינטרנט וחברות גדולות בארצות הברית,¹⁵ דיווחה בפברואר 2003 על כך שכ-40% מכל תעבורת הדואר האלקטרוני שהיא סרקה הייתה של הודעות דואר לא מוזמנות ולא רצויות – ובקיצור של דואר זבל.¹⁶ כאשר כל גולש מקבל בממוצע כ-2000 הודעות דואר זבל בשנה. בנוסף, חברת Commtouch זיהתה עליה של 60% בכמויות דואר הזבל במהלך ארבעת החודשים הראשונים של שנת 2003 בלבד.¹⁷ גם על-פי נתוני Tmicha.net האוספת מידע על היקף תופעת דואר הזבל בישראל, ישנה עליה מחודש לחודש בהיקף שליחת דואר זבל אלקטרוני בישראל.¹⁸

מרבית הדואר הלא-רצוי הנשלח הינו פרסומי-מסחרי, ועל כן הגופים הנלחמים בדואר זבל (כמו CAUCE)¹⁹ מפנים את מאמציהם כנגד סוג זה של דואר זבל. אך חשוב לזכור כי קיים גם דואר המציג עמדות אידיאולוגיות או דתיות. כאשר סוגי מכתבי הדואר הנפוצים ביותר הם:

- מכתבי שרשרת.
- תרמיות פירמידה (כולל שיווק רב שכבתי MLM - Multi Level Marketing).
- תרמיות "התעשר מהר" (Make Money Fast – MMF) אחרות.
- הצעות לשיחות סקס טלפוני או לאתרים פורנוגרפיים.
- הצעות לתוכנות לאיסוף כתובות דואר אלקטרוני ושליחה של דואר זבל (המפרסמים, כמובן מציגים, לרוב, את התוכנות הללו כתוכנות לדיוור ישיר).
- הצעות לשליחה של דואר זבל במסות.
- הצעות לרכישת מניות של חברות הזנק (start-up) אנונימיות.
- הצעות ל"תרופות אלילי".
- תוכנות פיראטיות או פרוצות (WAREZ).²⁰

¹⁵ כמו: Cisco, AT&T, Microsoft, Verizon, Earthlink.

¹⁶ קייד מץ, "הזבלן לסל- וחסל", PC מגזין ישראל 117 (מרץ 2003), 74, 76-78.

¹⁷ מתוך דף המידע של חברת Commtouch על מוצר הסינון ASAP: http://www.commtouch.com/news/english/2004/pr_040401.shtml

¹⁸ גל מור, "דו"ח: דואר הזבל בישראל גדל", ynet (18.2.2004), <http://www.ynet.co.il/articles/0,7340,L-2795055,00.html>

¹⁹ CAUCE - The Coalition Against Unsolicited Commercial Email – הוא ארגון הפועל כנגד דואר זבל מסחרי, בעיקר במטרה לשכנע את המחוקקים לחוקק חוקים הקובעים מדיניות של הסכמה מראש (Opt-In) לשליחת דואר מסחרי בלתי מוזמן. ל-CAUCE יש סניפים בארצות הברית, האיחוד האירופאי, הודו, אוסטרליה וקנדה. אתר הארגון: <http://www.cauce.org>

²⁰ WAREZ – הוא כינוי לתוכנות המופצות באופן בלתי חוקי, דרך רשת האינטרנט, או דרך BBS.

ד. דואר זבל והגנת הפרטיות

בעבר קבלת דואר חילזון (דואר מסורתית), הייתה מלווה בהילה רומנטית. אנו אוהבים לקבל מכתבים והודעות שנכתבו במיוחד בשבילנו, כאשר אנו יודעים כי כותב המכתב הקדיש זמן ומאמץ במיוחד בשבילנו בכתיבת המכתב. כיום ההתלהבות הזו מקבלת דואר כמעט ונעלמה, מפני שרוב הדואר שאנו מקבלים כיום מורכב מחשבונות, עלוני פרסומת ומכתבי שרשרת. אך עדיין יש תקווה קלושה, שיום אחד נקבל מכתב אישי שנכתב במיוחד בשבילנו. הדואר האלקטרוני, עבר תהליך דומה לדואר החילזון. בתחילה הוא שימש להעברת מסרים אישיים, שהיו במיוחד בשבילנו ואותם באמת רצינו לקרוא. אך די מהר הופיעו הסימנים שבישרו על סוף העידן הרומנטי של הדואר האלקטרוני ותחילתו של העידן המסחרי. ד"ר John Suler כותב על כך, כי רוב האנשים מתייחסים לדואר האלקטרוני, כמרחב פרטי שלהם, בו הם מתקשרים עם משפחה, חברים ועמיתים לעבודה.²¹ האם דואר זבל הוא עניין של פרטיות? גם חלק מהצעות החוק שעל הפרק ממקומות את הפתרון המשפטי במסגרת דיני הגנת הפרטיות. האומנם זה המקום הראוי? אנו סבורים שעיקר הנוק שגורם דואר זבל אינו בפגיעה בפרטיות, אלא לכל היותר, בפגיעה עקיפה בה.

לפי המלומד William Prosser, הזכות לפרטיות מורכבת מארבע עילות נזיקיות, שאחת מהן היא "חדירה למרחב הפרטי של אחר".²² האם קבלת דואר אלקטרוני בניגוד לרצון הנמען מהווה פגיעה בפרטיות? נראה שהתשובה שלילית. אם נפנה לערכים היסודיים של הזכות לפרטיות, הרי שתיבת הדואר הרגיל הפיסית אינה שונה מתיבת דואר אלקטרוני. כשם שקבלת דבר דואר פרסומי פיסית לתיבת הדואר של אדם אינה מהווה פגיעה בפרטיותו, כך גם קבלת דבר דואר פרסומי לתיבת הדואר האלקטרוני שלו.

הגדרת המרחב הפרטי של אדם אינה כוללת את תיבת הדואר הפיסית שלו שבביתו, לכן אינה צריכה לכלול את תיבת הדואר האלקטרוני. נוסף על כך, רשת האינטרנט מאפשרת לאנשים מנגנון אינהרנטי של אנונימיות. הרשת מתוכננת כך שגולש נשאר אנונימי אלא אם הוא בוחר לחשוף פרטים על עצמו. בהיבט זה, הרי שפרטיות תיבת הדואר האלקטרוני האישית של משתמש מובטחת עוד יותר מאשר פרטיות תיבת הדואר הפיסית של המשתמש. אנונימיות זו מבטיחה שדברי הדואר האלקטרוני שאנו מקבלים מהמפרסמים אינם אישיים. ביסודות הזכות לפרטיות נמצא האדם האינדיבידואלי. הזכות לפרטיות מוגדרת עבור אדם נתון, ולא עבור אישיות אלמונית כלשהי שלה יש מתאר במדיום כלשהו. תכונות רשת האינטרנט הן כאלו, המקנות אנונימיות אינהרנטית למשתמש. כלומר, אלא אם כן בחר המשתמש לחשוף פרטים על עצמו, או שמפיץ הדואר השיג בדרכים אחרות פרטים אישיים של המשתמש,²³ אזי דברי הדואר שיקבל המשתמש יהיו, בהגדרה, דברי דואר שאינם אישיים. מכאן נובע שפרטיות תיבת הדואר האלקטרוני של המשתמש מוגנת יותר מאשר פרטיות תיבת הדואר הפיסית שלו. לכן, עצם קבלת דואר לא רצוי לתיבת

²¹ John Suler, "E-Mail Communication and Relationships", *Psychology of Cyberspace* (3.6.1998), <http://www.rider.edu/~suler/psycyber/emailrel.html>

²² William L. Prosser, "Privacy", 48 *Cal L.Rev.* 383, 389-392 (1960)

²³ בכך נרחיב בנייר העמדה הסופי "הזכות לפרטיות באינטרנט".

הדואר האלקטרוני של המשתמש אינה יכולה לשמש כפגיעה בפרטיות המשתמש כשלעצמה.

בנוסף, ראוי לבחון את השאלה גם לאור עמדתה של פרופסור רות גביוזן, כי הזכות לפרטיות כוללת את יכולתו של הפרט להגביל את הגישה אליו.²⁴ ניתן לומר כי קבלת דברי דואר בניגוד לרצוננו ניתנת לשליחה. כלומר – הפרט יכול להגביל קבלת דברי דואר אלקטרוני שאינם רצויים באמצעים שונים בעלי רמות יעילות שונות. מכאן נובע שכל עוד רשת הדואר האלקטרוני ורשת האינטרנט מאפשרות למשתמש להגביל קבלה של דואר לא רצוי, אזי אין הפרה של פרטיותו. כאמור, חלק מהפטרונות כנגד דואר זבל מחייבים שימוש בטכנולוגיות שונות ובעלי דרגות יעילות שונות. אולם אם משתמשת עושה שימוש מושכל בפתרונות קיימים בשוק כנגד דואר זבל, הרי שכמות דברי הדואר הלא רצויים שיגיעו לתיבת הדואר האלקטרוני שלה אינה שונה משמעותית מכמות דברי הדואר הלא רצויים המגיעים לתיבת הדואר הפיסית שלה. רשת האינטרנט ורשת הדואר האלקטרוני מפקדה בידי הגולשת יכולת סבירה לקבוע אילו דברי דואר תקבל ולכן תוכל לשמור על פרטיותו לפי התפיסה הקלאסית.

בית המשפט העליון של קליפורניה סבור כי תיבת הדואר של המשתמשים אינה פרטית. בפרשת *Hamidi v. Intel*²⁵ תבעה חברת אינטל עובד שפוטר ושלה אלפי מכתבים לתיבות הדואר האלקטרוניים של עובדי החברה. במכתבו הסביר חמידי את סיבת הפיטורין הלא מוצדקת לשיטתו. אינטל תבעה את חמידי בעוולה של הסגת גבול במיטלטלין (trespass to chattels) באמצעות דואר אלקטרוני, ובית המשפט התבקש לקבוע את גבולות חופש הביטוי באינטרנט - האם, כפי שאינטל טענה, לחברה יש הזכות "לגדר" את שרתי הדואר שלה, או כפי שחמידי טען, כי כל כתובת באינטרנט חייבת לקבל מידע לגיטימי, כמו דעה, מכל כתובת אינטרנט. נדמה כי טענתו של חמידי היא במידה רבה טענה לפיה תיבת הדואר שלנו היא ציבורית (במקרים בהם התכתובת היא בעלת חשיבות ציבורית).²⁶ את טענתו של חמידי גיבו פעילי האגודה לזכויות האזרח בארצות הברית וארגון החזית האלקטרונית (EFF),²⁷ שלוחם למען זכויות הפרט באינטרנט. אלו טענו כי התביעה של אינטל מאיימת על עתיד התקשורת החופשית באינטרנט. בית המשפט העליון בקליפורניה אימץ את גישתו של חמידי וקבע כי לא רק שחמידי אינו אחראי בעוולת הסגת גבול במיטלטלין, אלא שהפסיקות (ההפוכות) של הערכאות הנמוכות הפרו קשות את התיקון הראשון לחוקה. He (Hamidi) no more invaded Intel's property than does a protester holding a "

²⁴ Ruth Gavison, "Privacy and Limits of Law", 89 *Yale L.J.* 421, 428 (1980)

²⁵ *Intel Corporation v. Hamidi*, 1 Cal. Rptr. 3d 32 (Cal. 2003)

²⁶ טענה זו מתיישבת עם הרציונל של המועצה הישראלית לצרכנות, המותירה פתח למשלוח דואר ללא אישור הנמען כאשר המדובר בתכתובת אשר הנמען "מפיק ממנה תועלת ישירה". אין המדובר בדואר בעל אופי פרסומי או שיווקי. ראו סעיף 17(א) להצעת תיקון חוק הגנת הפרטיות (מניעת פניות בלתי מוזמנות), התשס"ג - 2003.

²⁷ Electronic Frontier Foundation - EFF – ארגון לא ממשלתי בארצות הברית, הפועל להגנת "הזכויות הדיגיטליות" של הפרט: <http://www EFF.org>

sign or shouting through a bullhorn outside corporate headquarters, posting a letter through the mail, or telephoning to complain of a corporate practice”²⁸, כתבה השופטת Kathryn Werdegar, המשקפת את דעת הרוב. השופטת הוסיפה כי פסיקה זו אינה נותנת תוקף חוקי למעשים של אנשים השולחים דואר זבל או מטרודים באמצעות דואר אלקטרוני בדרכים אחרות. לדברי בית המשפט העליון בקליפורניה, שרתי הדואר של אינטל לא ניזוקו כלל כתוצאה מהמשלוח ואילו הנמענים להודעותיו של חמידי יכלו לבקש את הסרתם מרשימת הדיוור, ובקשה כזו נענתה בחיוב. אם שני התנאים האלה לא היו מתקיימים, ייתכן שחמידי היה מסיג גבול.

אם כן אנו רואים כי הנטייה האמריקנית היא לשמור על חופש הביטוי באינטרנט אפילו במחיר של פלישה לתיבת הדואר שלנו. נטייה זו במידה רבה מגדירה את תיבת הדואר האלקטרוני כאמצעי דואלי, מחד גיסא היא פרטית כאשר מדובר בדואר זבל, ומאידך גיסא היא ציבורית כאשר מדובר בדואר אלקטרוני אשר תוכנו לגיטימי וחוסה תחת חופש הביטוי.

דואר זבל אלקטרוני עלול לפגוע בפרטיות בעקיפין, בדרך שבה השולח מוצא את כתובת הדואר האלקטרוני שלנו. לעיתים משתמש מפיץ הדואר בשיטות לא ראויות על מנת לבנות מאגרי מידע לא מורשים (בניגוד לחוק מאגרי מידע) של משתמשים וכתובות דואר אלקטרוני של משתמשים.²⁹ בפסק הדין הראשון בישראל שנגע לדואר זבל,³⁰ הנתבע “קצר” כתובות דואר אלקטרוני של מנויים באתר אינטרנט, על-ידי תוכנה שסרקה את הדפים בפורום שבאתר ושמרה את כל כתובות הדואר האלקטרוני שהיא מצאה באותם דפים (כאשר הנתבע מאוחר יותר שלח לאותן הכתובות דואר זבל, המפרסם את אתרו שלו).

²⁸ עניין חמידי, לעיל הערה 25, בעמ' 27 לפסק הדין.

²⁹ בכך נרחיב בנייר העמדה הסופי “הזכות לפרטיות באינטרנט”.

³⁰ ת”ק (ת”א) 6000/03 אבן-חן אורי נ’ סוויסה ניר (לא פורסם).

ה. דואר זבל פוגעות וחופש הביטוי

חופש הביטוי בדין הישראלי הוא זכות יסוד בהיותו חלק מכבוד האדם,³¹ ולכן גם שולחי דואר הזבל **המסחרי** נהנים מזכות זו. אמנם מעמדו של הביטוי המסחרי נחות יותר מהביטוי הפוליטי, כדברי השופט חשין:³²

"הפרסומת המסחרית היא מעין דיירת בעלת זכויות נחותות בבית חופש הדיבור והביטוי, וניתן לחסמה בהגבלות אלו ואחרות, הגבלות שלא יעלה על הדעת כלל להעמידן בדרכו של חופש הביטוי הקלאסי".

אך גם חופש הביטוי המסחרי זוכה להגנה בהיותו מספק מידע לציבור, מבטיח תחרות בין המפרסמים והוא גם חלק מהיצירה האנושית בתקופה המודרנית.³³ למרות שאולי רבים יתקשו להסכים כי דואר הזבל האלקטרוני זוכה להגנה דומה תחת חופש הביטוי, ועוד פחות יסכימו שהוא מתיישב עם הרציונאלים העומדים בבסיס פסיקות בג"ץ בנושא,³⁴ אנו סבורים כי גם דואר הזבל הפרסומי נהנה מהגנות דומות. אך איננו סבורים שיש לכפות על אנשים להיחשף לאותם ביטויים בניגוד לרצונם. חופש הביטוי דן בחופש של הדובר להתבטא, אך לא בהכרח ב"חובתו" של הקהל להקשיב, ועל כן הגנה על הציבור שאינו מעוניין לקבל הודעות דואר פוגעות רק בעקיפין בחופש הביטוי של הדובר. בכל מקרה, ברור שהפתרון למתח הזה שבין הזכויות של השולח והנמענים מורכב יותר, ובלשון החוקתית, האיזון צריך להיות כזה שהפגיעה מידתית בכל אחת מהזכויות ו/או האינטרסים.

³¹ ראו למשל: בג"צ 4804/94 חברת סטיישן פילם בע"מ נ' המועצה לביקורת סרטים ומחזות, פ"ד (5) 661, 674-675.

³² בג"צ 606/93 קידום יזמות ומו"לות נ' רשות השידור, פ"ד מח(2) 1, 27-28.

³³ בג"צ 5118/95 מאיו סימון פרסום שיווק נ' הרשות השנייה, פ"ד מט(5) 751, 755-756.

³⁴ ראו גם לבג"ץ 4644/00 יפאורה תבורי בע"מ נ' הרשות השנייה לטלויזיה, פ"ד נד(4) 178, 181-182.

2. טכנולוגיות בשימוש הספאמרים

מפיצי דואר הזבל מודעים למעשיהם בדרך כלל, וכמו כן הם מודעים למאמצי הספקים והמשתמשים למנוע תעבורה וקריאה של דואר זבל. לכן משתמשים הספאמרים בטכניקות וטכנולוגיות שונות על מנת להפיץ הודעות ועל מנת לגרום למשתמשים לקרוא אותן. בפרק זה נסקור תחילה את האמצעים הטכנולוגיים המרכזיים שבאמצעותם משתמשים מפיצי דואר הזבל להפצת הדואר, ובתת-הפרק הבא, נסקור את האמצעים הטכנולוגיים להשגת כתובות דואר אלקטרוני.

א. טכנולוגיות ואמצעים להפצת הודעות דואר זבל אלקטרוני

כותרות מפתות

מפיצי דואר הזבל משתמשים בכותרות מפתות להודעותיהן כ"תמריץ" עבור המשתמש לקרוא אותן. למשל "הדרך הקלה והבטוחה להרוויח \$50,000" וכן הלאה. לעיתים קרובות תוכן ההודעה שונה לחלוטין מהתוכן עליו מרמזת הכותרת. אך ספק רב אם יש בכך עבירה על איסור ההטעיה בסעיף 2 לחוק הגנת הצרכן.³⁵

שליחת הודעות גרפיות

שליחה של הודעה גרפית מאפשרת למפיצים להתחמק מתוכנות לסינון דואר זבל. רוב תוכנות הסינון סורקות רק את התוכן הטקסטואלי של ההודעות ואינן יכולות לקרוא תוכן גרפי, וכך מצליח הספאמר להעביר את הודעותיו למשתמשים. התוכן הגרפי דורש משאבי אחסון ועיבוד רבים יותר, ומעמיס את התעבורה על הרשת יותר מאשר תוכן טקסטואלי. תוכן גרפי אף עשוי "לסתום" את תיבות הדואר של המשתמשים באופן מהיר ביותר. כך שהודעות זבל גרפיות מסבות נזק כבד ביותר לספקים ולמשתמשים, ושיעור התעבורה שלהן גדול ביותר עקב היכולת לחמוק מאמצעי הסינון.

זיוף של כתובת השולח

זיוף כתובת השולח מאפשר למפיץ לשלוח הודעות זבל ולהישאר אנונימי ביחס לחוק. הדבר מעניק אפקט מטריה לשולח דואר הזבל, בדיוק כמו השימוש בתא דואר תמים של צד ג'. ההבדל בין מקרה זה לבין שימוש בצד ג' הוא שבמקרה זה הרשויות מודעות לכך שהשולח אינו ידוע, ואילו כאשר הספאמר משתמש בצד ג' מופנה מאמץ האכיפה כנגד צד ג'. בכל מקרה – הספאמר אינו ניתן להשגה על-ידי הרשויות.

³⁵ סעיף 2 לחוק הגנת הצרכן, התשמ"א-1981, ס"ח 248. השופט שטרסברג-כהן סברה בע"א 1977/97 ברזני נ' בזק, פ"ד נה(4) 584, 602-603 כי הדרישה לפיה כל אחד מהתובעים בתביעה ייצוגית צריך להוכיח את הסתמכותו על הפרט המטעה איננה סבירה ועל כן יש ליצור חזקה כי צרכן שרכש את המוצר- נראה אותו כמי שנחשף למצג המטעה ופעל לפיו. השופט שטרסברג-כהן נותרה נדבעת מיעוט.

שימוש הפוך בהתניית "אנא מחק אותי מרשימת התפוצה"

הספאמרים עושים שימוש הפוך בפניות של משתמשים למחיקה מרשימות תפוצה. עבור הספאמר זהו אישור שמדובר בתא דואר פעיל, והדבר רק מדרבן את הספאמר לשמור על הכתובת ברשימת התפוצה, ואף להפיצה לאחרים. גם אם הספאמר מחק את המשתמש מרשימת תפוצה אחת, אזי הוא מעביר אותו לרשימות התפוצה האחרות למוצרים האחרים שברשותו. כלומר – עבור הלקוח שכבר השקיע מזמנו ומרצו על מנת להקטין את תופעת דואר הזבל ההישג יהיה הפוך.

הסבר התופעה: לכל שולח דואר זבל יש מספר רשימות תפוצה של משתמשים, ברמות איכות שונות. חלק מתיבות הדואר הרשומות אצלו הן תיבות דואר "מתות", חלק הן תיבות דואר שנקלטו בהטעיה של מנהלי אתרים,³⁶ חלק הן תיבות הנבחרות באופן אקראי,³⁷ חלק מהתיבות נקצרו על-ידי תוכנות קצירה, וחלקן נאספו בדרכים אחרות. בנוסף, קונים שולחי דואר זבל רשימות של כתובות דואר מספקים שונים. ברור כי כמות תיבות הדואר המתות או הפיקטיביות הנמצאת אצל הספאמר היא גבוהה. יתר על כן, חלק מתיבות דואר אלה נועדו במקור לשמש מנהלי אתרים על מנת לזהות שולחי דואר זבל. יוצא שמצד אחד הספאמר מעוניין לשלוח כמה שיותר דואר, ומצד שני מעוניין להקטין את חשיפתו לכלי איתור דואר זבל ככל שניתן. אינטרס נוסף של הספאמר הוא איכות כתובות הדואר האלקטרוני שברשותו. לכן, כאשר החוק מחייב את הספאמר לשים התניית "מחק אותי מרשימה", הספאמר נמצא במצב של ניגוד אינטרסים. הספאמר מבצע מאמצים רבים על מנת להשיג כתובות דואר של משתמשי אינטרנט, ובהינף עכבר יכולים המשתמשים למחוק את עצמם מרשימת הכתובות שלו. וכאילו לא די בכך, משתמש שהגיב למכתב וביקש שימחקו אותו מרשימה אימת את כתובת הדואר שלו הנמצאת ברשימת הכתובות של הספאמר. זו כתובת אמיתית, חיה, שאין הספאמר יכול להתעלם ממנה.

לכן, כאשר הספאמר מקבל פניה כזו ממשמש הוא עושה בה שימוש הפוך. הוא מוחק את כתובת הדואר מהרשימה בה היא מופיעה, אך אין הדבר מונע ממנו להוסיף אותה לרשימת הכתובות ה"איכותיות". אין גם מניעה ממנו מלמכור כתובת זו לספאמרים אחרים. אין מניעה ממנו להעביר כתובת זו לרשימות אחרות עבור מוצרים אחרים שברשותו. גם שליחת הדואר אינה גוררת עלויות משמעותיות על הספאמר. לכן, ספאמר אחד יכול לחלוש על כמות גדולה של רשימות כתובות דואר של משתמשים. אישור על זהות משתמש וכתובת דואר אלקטרוני הוא אחד הגורמים המדרבנים את הספאמר לשלוח דואר זבל. ייתכן אף שקיימים ספאמרים שאינם מחויבים על-פי חוק להוסיף התניית "מחק אותי מרשימה",³⁸ אך מוסיפים התניה כזו רק על מנת לאמת את כתובת הדואר שברשותם. המסקנה עבור המשתמש היא: לעולם לא להגיב להתניית "מחק אותי מרשימה". כל זאת בעצם נעשה

³⁶ מנהלי אתרים המבקשים להילחם בתופעה בונים דפים מיוחדים להתמודדות עם תוכנות קצירה. בדפים אלה ישנה כמות גדולה מאוד של תיבות דואר פיקטיביות שנועדו להוריד מאיכות תוצאות תוכנות הקצירה של שולח דואר הזבל.

³⁷ קיימים מוצרים הבונים כתובות דואר אלקטרוני עבור ספאמרים באופן אקראי, תוך שימוש בשמות נפוצים. ברור כי כלים אלו נותנים מעט מאוד כתובות אמיתיות ביחס לכמות הכתובות שאין מאחוריהן תיבות דואר פעילות.

³⁸ נמצאים מחוץ לגבולות ארצות הברית למשל.

בניגוד לאינטרס של המפרסם, הואיל ול"מפרסם סביר", אין אינטרס "להציק" לקהל שאינו מעוניין בפרסום. אך נראה, כי המטרה של רוב שולחי דואר הזבל, היא להגיע לקהל כמה שיותר גדול, אפילו אם הוא אינו מעוניין בפרסום, על מנת לנסות להגדיל את האחוז המזערי של העונים לפרסום באמצעות דואר הזבל (שהופך את דבר שליחת דואר הזבל לרווחי).³⁹

שימוש בתא דואר תמים של צד ג'

שולחי דואר זבל חשופים במדינות מסוימות לסנקציות מצד החוק או מצד ספקיות האינטרנט. אחת הדרכים בהן בוחרים הספאמרים לעקוף את החוק ולהתחמק מהסנקציות היא על-ידי שימוש בתא דואר תמים של צד ג'. באמצעים שונים משיגים הספאמרים שליטה על כתובת דואר אלקטרוני פעילה של צד ג'. הספאמרים "מתלבשים" על תא דואר תמים של צד ג', וממנו שולחים את דואר הזבל. כך, צד ג' עשוי לשלם יותר מהדרוש עבור שירותי הדואר, וכמו כן, כאשר יפעלו הרשויות או ספקיות הדואר כנגד הספאמר, היחיד להיפגע יהיה אותו צד ג'. כלומר, הספאמר מסב נזק כבד לצד ג' ויוצא נשכר. שיטה יעילה לביצוע יכולה להיות תוכנות מסוג תולעת או פריצה אחרת למחשב חשוף של צד ג'. כעת ישלחו הספאמרים את כל מכתביהם דרך כתובת הדואר שהשיגו ללא דאגות. גם כאשר יחליטו הרשויות או הספקים לפעול נגד ספק דואר הזבל, הם יגיעו לכל היותר אל צד ג' התמים, יפעילו עליו את הסנקציות, ויאפשרו לספאמר להתחמק מעונש. צד ג' יצטרך להוכיח את חפותו, על לא עוול בכפו, וכאשר ברור כי המכתבים נשלחו ממחשבו.

אין לרשויות החוק דרך קלה לתפוס את הספאמרים, או למנוע את התופעה כאשר משלוח דואר הזבל מגיע ממחשב תמים, ואדם שאינו הספאמר נאלץ להתמודד מול הרשויות. קיימת "מלחמת חימוש" בתחום דואר הזבל, והספאמרים משתכללים כל הזמן. ללא יכולת איתור מדויקת של הספאמרים, לא יוכלו סנקציות בחוק לעצור את התופעה.

שימוש במדינות "נוחות"

כפי שקורה בענף הספנות או מיסוי בינלאומי, כך משתמשים הספאמרים בכתובות דואר ושרותי דואר במדינות בהן אין פעילות או איסורים נגד מפיצי דואר זבל. כך יכולים הספאמרים לפעול באין מפריע ובעיית דואר הזבל אינה נעלמת.

³⁹ מחקר שנערך על-ידי ה-Wall Street Journal הראה שאחוז היענות של 0.001%, מספיק על מנת להפוך את שליחת דואר הזבל לרווחית. מקור: Mylene Mangalindan, "For Bulk E-Mailer, Pestering Millions Offers Path to Profit", *The Wall Street Journal Online* (13.11.2002), <http://online.wsj.com/article/0,,SB1037138679220447148,00.html>

ב. דרכים להשגת כתובות דואר אלקטרוני לשם שליחת דואר זבל

"קצירה" של כתובות דואר

הספאמרים משתמשים במנועי קצירה (תוכנות הדומות באופי פעולתן למנוע חיפוש) על מנת להשיג כתובות דואר אלקטרוני של גולשים. לעיתים תוכנות אלה חודרות למאגרים חסויים או ללא הרשאה. בחדירה למאגרים אלו, יש משום חדירה לפרטיות (פרטיו האלקטרוניים של המשתמש) וכן יש בכך עבירה על סעיף 4 לחוק המחשבים, האוסר על חדירה לחומר מחשב שלא כדין.⁴⁰ בנוסף יש בכך לגרום נזק למחשבי הספק.⁴¹

השימוש בתוכנות הקצירה נועד להשיג רשימות של כתובות למשלוח דואר זבל. ישנם מקומות רבים (כגון פורומים) ואתרים רבים בהם מפורסמות כתובות דואר אלקטרוני של משתמשים. כתובות אלה הן מוצר מובחר עבור הספאמרים. מדובר בכתובות אמיתיות, של תיבות דואר פעילות, של משתמשים אמיתיים, שניתן להשיגן בעלות מזערית, וללא מאמץ רב. חלק מכתובות אלה אף מפולחות מעצם הופעתן באתר שתוכנו מפולח. אתרי פורומים או קהילות מקוונות אחרות (שאינן חדרי צ'אט למיניהם) בהם מפורסמים פרטים של המשתמשים הם בבחינת מטמון עבור הספאמרים: מאות ואלפי כתובות פעילות, חשופות לכל דורש. כך גם אתרים של רשימות דואר שאינן מקוונות,⁴² אך מתעדות את תכתובות הרשימה באינטרנט מעת לעת.

תוכנות הקצירה עובדות כמנוע חיפוש. תוכנת הקצירה מורכבת מרובוט הנכנס באופן אוטומטי לדפי האתר הנסרק ומחפש את התוכן הרצוי בתוך הדפים, וכן מאינדקס – בסיס נתונים אליו מוכנסות הכתובות אותן איתר הרובוט. כשם שניתן לחפש תוכן של דף או אתר באינטרנט על-ידי שימוש במנוע חיפוש, כך ניתן לבדוק האם בתוכן של דף מופיע הסימן "@" . מנועי חיפוש מובילים חוסמים חיפוש המכיל את הסימן "@"⁴³. אולם ניתן לבנות בקלות, תוך שימוש במוצרי מדף מנועי חיפוש אשר סורקים את הרשת ומחפשים אחר מחרוזות המכילות את הסימן כרוכית (@) בתוכן הדפים. מנועים אלה שומרים רק את המחרוזות המכילות את הסימן "@" ומתעלמים משאר התכנים.

⁴⁰ סעיף 4 לחוק המחשבים, התשנ"ה-1995, ס"ח 366.

⁴¹ עניין אבן-חן, לעיל הערה 30.

⁴² רשימות דואר אלקטרוני שאינן קיימות במצב מקוון – list groups. למשל: MC-CHASSIS-DESIGN.

⁴³ מנוע החיפוש Google מחזיר תוצאות זבל אחרי חיפוש מלה המכילה כרוכית. מנועי החיפוש Lycos, Yahoo, Altavista מחזירים תוצאות ריקות.

תוכנות קצירה הן בעצם מנועי חיפוש, בעלי אפשרויות בקרה וכיוון.⁴⁴ הספאמרים מפעילים תוכנות אלה כלפי אתר מסוים. התוכנה סורקת דפים מהאתר בקצב גבוה ושומרת את כתובות הדואר האלקטרוני המופיעות באתר. תוכנות אלה יעילות ביותר, יתכן אף שיעילות מדי.⁴⁵

תוכנות הקצירה הן מהירות ויעילות ביותר. מרבית המגבלות הטכניות החלות על מנועי חיפוש רגילים באינטרנט אינן חלות על תוכנות הקצירה.⁴⁶ תוכנות הקצירה אף מתעלמות מהנחיות מנהלי האתרים לגבי האזורים אליהם מותרת הכניסה והאזורים אליהם הכניסה אסורה לרובטי סריקה.⁴⁷ כך מבצעות תוכנות הקצירה פעולות שאינן ראויות. תוכנות אלה פולשות לתחומי אתרים שהם אסורים, אוספות חומר עליו התכוון בעל האתר לשמור, וכן אוספות כתובות דואר פרטיות של משתמשים.

אולם לתוכנות הקצירה תכונה מזיקה נוספת. עקב יעילותן הרבה הן מסוגלות לשלוח אלפי שאילתות בדקה לשרתי האתר הנסרק. האתר הנסרק אינו מסוגל לטפל בתעבורה למענה הוא משמש, ומטפל אך ורק בפניות של תוכנת הקצירה. האתר אף יכול לקרוס אם תוכנת הקצירה אגרסיבית מספיק. פעילות זו של תוכנת הקצירה זהה להתקפת תוכנה שמטרתה להפיל מחשבים ושרתים, ובלבד שבביצוע הפעולה תוכנת הקצירה גם מושכת משהו מהאתר לעצמה. דחייה של השאילתות או מענה ריק עליהן – גם היא גוזלת משאבי מחשב וגורמת נזק חמור לבעלי האתר.⁴⁸

קנייה של רשימות תפוצה

המפיצים קונים רשימות תפוצה של משתמשים מחברות בעלות מוסר אחסון נתונים ירוד, או "ספאמרים" אחרים. יש בכך סחר בפרטים אישיים של משתמשים. יתכן שיש בכך הפרה של הודעת אוסף המידע הראשוני כלפי האזרח, כי לא יעשה שימוש אחר במידע מעבר למטרה המיידית של איסופו, ואולי אף הפרה של סעיף 2(9) לחוק הגנת הפרטיות. יתכן גם שיש בכך הפרה של חובת מאגר מידע שלא לעשות במידע שימוש אחר. אם כך, הרי יש כאן פגיעה בזכות לפרטיות.

מכירות כאלה מגבירות את המוטיבציה של הספאמרים לעשות שימוש שלילי בנתוני המשתמשים בכלל, ובנתוני משתמשים שהפעילו את התניית "מחק אותי מרשימה" בפרט.

⁴⁴ היכולת לסרוק רק שם מתחם (domain) נתון, חשובה ביותר לשולחי דואר זבל למשל. כך גם יכולות מיקוד נוספות של תוכנת הסריקה.

⁴⁵ עניין אבן-מן, לעיל הערה 30: אחת מהטענות נגד הנתבע הייתה שהשתמש בתוכנה שנכנסה מספר רב של פעמים בזמן קצר מאוד לאתרו של התובע, ועל-ידי כך גרמה להפלת שרתי האינטרנט שלו.

⁴⁶ לדוגמה: תוכנות הקצירה אינן זקוקות למחשבים יקרים וחזקים מאוד, כיוון שעומק הרקורסיה (הסריקה הנסיגתית) וגודלה במהלך סריקת אתר נתון, קטן משמעותית מאשר עומק הרקורסיה של מנוע חיפוש העובר על חלק גדול יותר מהאינטרנט.

⁴⁷ מרבית תוכנות הקצירה מתעלמות מהנחיות לרובוטים כגון, ההנחיות הנמצאות בקובץ "robots.txt".

⁴⁸ קיימים אתרים עבורם עלות הנוכחות באינטרנט גבוהה ביותר. נפילת שרתים באתרים כאלה עשויה להתבטא באלפי דולרים לשעה. באופן לא מקרי אלו אתרים המשרתים אלפי משתמשים בו זמנית. אתרים כאלה הם גם המטרות העדיפות של הספאמר, הואיל והוא מעוניין בכתובות של אותם אלפי משתמשים, וכאן המקום להשיגן.

מניין הספאמרים משיגים את כתובות הדואר האלקטרוני?

מחקר שנערך בנושא על-ידי ה-The Center For Democracy & Technology (להלן: CDT) במשך שישה חודשים, ניסה לבדוק מהיכן משיגים הספאמרים את כתובות הדואר האלקטרוני שברשותם, וכיצד ניתן להקשות עליהם להשיג את אותן כתובות.⁴⁹ המחקר מצא כי כתובות דואר אלקטרוני, שנקצרו מאתרי אינטרנט פומביים הם המקור העיקרי לכתובות הדואר האלקטרוני שברשות הספאמרים, כאשר ככל שהתעבורה באתר, בו נמצאת כתובת דואר אלקטרוני מסוימת, גדולה יותר, כך היא תקבל יותר דואר זבל. בנוסף המחקר גילה, כי ישנה חשיבות לעובדה, האם כתובת דואר אלקטרוני מסוימת עדיין מופיעה באתר אינטרנט. נתגלה כי אם מסירים כתובת דואר אלקטרוני שפורסמה באתר אינטרנט, אז ככל שיעבור יותר זמן, היא תקבל פחות ופחות דואר זבל. מכאן שהספאמרים מעדכנים לעתים קרובות את רשימות הכתובות שברשותם, כך שהן יהיו יותר עדכניות (הואיל ובניגוד למספרי טלפון, למשל, לכתובות דואר אלקטרוני יש לרוב "אורך חיים" קצר יותר והן נוטות להתעדכן ולהשתנות לעתים קרובות יחסית). גם כתובות דואר אלקטרוני שפורסמו ב-Usenet זכו לקבל כמות נכבדה של דואר זבל אלקטרוני,⁵⁰ אך פחות מאשר כתובות המפורסמות באתרי אינטרנט. כאשר גם כאן הספאמרים משתמשים בתוכנות קצירה, על מנת לדלות את הכתובות מתוך קבוצות דיון ב-Usenet.

בנוסף, המחקר בדק, האם כתובת דואר אלקטרוני המסופקת לאתרים עסקיים בעלי מדיניות פרטיות, תגיע לידי הספאמרים (כלומר האם אתרים אלו מוכרים את כתובות הדואר של המשתמשים לספאמרים)? כאשר המחקר מצא, כי כמעט כל הכתובות שסופקו לאתרים אלו (וליהם בלבד) לא זכו כלל לקבל ספאם (כלומר, אתרים אלו אכן שומרים על מדיניות הפרטיות המוצהרת שלהם, לפחות בכל הנוגע להעברת כתובות הדואר האלקטרוני לצדדים שלישיים).

המחקר ניסה לבדוק האם כתובות דואר אלקטרוני, המסופקות בעת רישום שמות מתחם (domain name), זוכות לקבל דואר זבל? התוצאה הייתה די מפתיעה – למרות שכתובות אלו נוטות להישאר עדכניות לזמן רב, ולמרות שניתן בקלות לבצע WHOIS על כל שם מתחם ולקצור מרשומת ה-WHOIS את כתובות הדואר האלקטרוני, הספאמרים (משום מה) לא עושים זאת וכתובות אלו בדרך כלל לא זכו כלל לקבל ספאם.

CDT, "Why Am I Getting All This Spam?", CDT (19.3.2003), ⁴⁹
<http://www.cdt.org/speech/spam/030319spamreport.pdf>

⁵⁰ Usenet היא רשת המספק שירותי קבוצת דיון דרך האינטרנט.

תוצאה מעניינת נוספת של המחקר, היא שכתובות דואר אלקטרוני שכלל לא פורסמו, עדיין זכו לקבל כמות גדולה של דואר זבל אלקטרוני. מעיון בקבצי ה-log של השרתים הרלוונטיים, נתגלה כי הדבר קרה על-ידי התקפות "דואר אלקטרוני" המנסות לנחש את כתובת הדואר האלקטרוני. התקפות אלו מנסות לשלוח דואר זבל, לכתובות שהן מנחשות, כאשר הניחושים מבוססים על:

- א. צירופים של שמות פרטיים ושם המתחם, כמו למשל: john@haifa.ac.il.
- ב. צירופים של שמות פרטיים ושמות משפחה נפוצים עם שם המתחם, כמו למשל: johndoe@haifa.ac.il, john_doe@haifa.ac.il, doejohn@haifa.ac.il וכך הלאה.
- ג. התקפות מילון ("dictionary attack"), ששולחות דואר אלקטרוני למילים מהמילון עם שם המתחם, כמו למשל: technology@haifa.ac.il.
- ד. ניחוש ברוטאלי של כתובות דואר אלקטרוני ("brute force attacks"), כאשר בהתקפות אלו מנסה הספאמר לשלוח דואר זבל לכתובות דואר המורכבות מכל צירוף אותיות אפשרי, למשל: ab@haifa.ac.il ... aa@haifa.ac.il, a@haifa.ac.il וכך הלאה. התקפות מסוג זה גוזלות בדרך כלל משאבי עיבוד רבים משרת הדואר המותקף.

שרתים של ספקיות אינטרנט, וספקיות דואר אלקטרוני גדולות, מכירים את התופעה ויש להם כלים לזהות את ההתקפה ולמנוע אותה.

אם כן, לעיתים יש שמפיצי דואר הזבל משתמשים בשיטות שאינן חוקיות על מנת להפיץ את הודעותיהם. שיטות אלו מסבות נזק רב למשתמשים ולספקים. שיטות פעולה נלוות אלו מהוות גורם מדרבן לרשויות לפעול כנגד דואר הזבל. לדעתנו, אין להתעלם מדרכי הפעולה של המפיצים במתן פתרון לבעיית דואר הזבל. הפתרון צריך להתמקד הן בהודעות לא רצויות, והן באיסוף ואחסון נתונים של משתמשים ללא רצונם.

3. הסדרה פרטית של דואר זבל

בפרק זה נסקור אפשרויות שונות - טכנולוגיות ועסקיות - להסדרה פרטית של בעיית דואר הזבל האלקטרוני, וכן ננסה לבדוק האם הפתרונות הללו אכן עשויים לפתור את בעיית דואר הזבל האלקטרוני. במונח "הסדרה פרטית" הכוונה היא לכללים משפטיים שאינם "מונחתיים" על הציבור מלמעלה, על-ידי המחוקק או בתי המשפט, אלא לכללים הצומחים "מלמטה", בין על-ידי השחקנים הרלוונטיים בשדה הפעילות בו מדובר, ובין על-ידי ארגונים ששמו להם למטרה לגבש כללים בתחום מסוים.⁵¹ ההסדרה הפרטית יכולה לבוא בדמות כללים אתיים, כללי התנהגות אחרים של ארגונים ותאגידים, או באמצעות טכנולוגיה. נפתח בתוכנות סינון, נמשיך בציון פעולתן של ספקיות השירות, נבחן את המשמעות של שינוי אפשרי בארכיטקטורה של הרשת, ונסיים בבחינת מודל כלכלי של בולי דואר.

א. תוכנות סינון

ישנם פתרונות טכנולוגיים רבים המנסים להתמודד עם בעיית דואר הזבל. הפתרון הנפוץ ביותר הוא תוכנות הסינון, כאשר חלק מתוכנות הסינון מסננות את דואר הזבל רק לאחר שהוא כבר הורד למחשב הנמען וחלק מתוכנות הסינון מסננות את דואר הזבל עוד כשהוא נמצא על שרת הדואר של ספקית האינטרנט, ובכך חוסכות את צריכת רוחב הפס והזמן שהיה כרוך בהורדת הדואר למחשבו של הנמען.

כיצד מזהות תוכנות הסינון את דואר הזבל?

רוב תוכנות הסינון משתמשות ביותר משיטה אחת על מנת לזהות את דואר הזבל. כאשר זיהוי דואר הזבל נעשה: א. לפי השוואה של ההודעה הנסרקה עם "רשימה שחורה" של הודעות הידועות כדואר זבל. ב. לפי זיהוי מקור ההודעה – בדיקה האם ההודעה נשלחה משרת SMTP הידוע כמשמש שולחי דואר זבל. ג. זיהוי כותרות וצירופי מילים האופייניות לדואר זבל. ד. בדיקה האם ההודעה עברה מסלול סיבובי (כלומר עברה שרתי דואר רבים עד להגעתה לנמען) – דבר המאפיין הודעות דואר זבל לעתים קרובות. ה. זיהוי דואר שנשלח מתיבות דואר פיקטיביות – שזה דבר המאפיין (לפי חברת Brightmail) את יותר ממחצית הודעות דואר הזבל.⁵²

סוגי תוכנות הסינון

תוכנות הסינון מתחלקות באופן כללי לשני סוגים: 1. תוכנות המותקנות על מחשב הלקוח (הנמען). 2. תוכנות המותקנות על שרת הדואר האלקטרוני של ספקית האינטרנט (כמו תוכנות SpamAssassin⁵³ או Anti-Spam). אך גם בין התוכנות המותקנות על מחשב הלקוח יש מספר סוגים של תוכנות:

⁵¹ ראו "עקרונות ההסדרה הפרטית", איגוד האינטרנט הישראלי: <http://www.isoc.org.il/hasdara/mavo.html>

⁵² מץ, לעיל הערה 16, בע' 76-83.

⁵³ אתר התוכנה <http://eu.spamassassin.org>

1. תוכנות הבדקות את ההודעה, עוד כאשר היא נמצאת על שרת הדואר הנכנס (שרת POP בדרך כלל),⁵⁴ ובכך מונעות את הצורך להוריד את הודעות דואר הזבל למחשב הנמען וחוסכות את הזמן, משאבי הרשת וזמן העיבוד של המחשב שהיה כרוך בהעברת הודעת דואר הזבל. תוכנת הסינון מבצעת את כל השלבים הללו באופן אוטומטי בלי התערבות המשתמש.

בדיקת הודעת דואר זבל על שרת הדואר הנכנס (שרת POP) מבלי להוריד את הודעת הדואר

תחילה, מתחבר הגולש לשרת הדואר הנכנס (זה בדרך כלל יהיה שרת POP או IMAP), למשל לשרת דואר נכנס הפועל לפי פרוטוקול POP3:⁵⁵

+OK POP3 service

הגולש נדרש בהתחלה להכניס שם משתמש:

USER yanivdr

+OK password required for user yanivdr

וסיסמה:

PASS mypassword

אם הוקלדו שם וסיסמה נכונים, תתקבל ההודעה הבאה:

+OK Maildrop ready

כעת מופעלת הפקודה STAT המחזירה את מספר ההודעות הנמצאות בתיבת הדואר שלנו על השרת ואת גודלן הכולל:

STAT

+OK 5 68483

במקרה זה ניתן לראות כי יש חמש הודעות דואר בתיבת הדואר שגודלן הכולל הוא 68,483 בייטים. כעת נכתבת הפקודה:

TOP 1 0

המורה לשרת להציג רק את ה-header (הכותרת) של ההודעה הראשונה (הודעה 1).

+OK

כעת השרת יראה לגולש את ה-header של ההודעה הראשונה:

Return-Path: <yaniv@zahav.net.il>

Received: from www02.dr-vb.co.il (yanivdr@localhost)

by dr-vb.co.il (8.11.6/8.11.6) with ESMTP id hB5GWbp09156

for <ydr@dr-vb.co.il>; Fri, 5 Dec 2003 12:32:37 +0200

X-ClientAddr: 192.110.186.95

Received: from balder.inter.net.il (balder.inter.net.il [192.110.186.15])

by www02.dr-vb.co.il (8.11.6/8.11.6) with ESMTP id hB5GWbJ09151

for <ydr@dr-vb.co.il>; Fri, 5 Dec 2003 12:32:37 +0200

⁵⁴ Post Office Protocol – הפרוטוקול הנפוץ ביותר לקבלת דואר אלקטרוני.

⁵⁵ IETF Network Working Group, "Post Office Protocol - Version 3 (POP3)", IETF (1996). <http://www.ietf.org/rfc/rfc1939.txt>

Received: from hever (tony06-83-249.inter.net.il [80.230.83.249])

by balder.inter.net.il (Mirapoint Messaging Server MOS 3.3.7-GR)

with SMTP id DCM77812;

Fri, 5 Dec 2003 12:33:35 +0200 (IST)

Message-ID: <000901c3bb4d\$e03d5e60\$0d00000a@hever>

From: "Yaniv Simsolo" <yaniv@zahav.net.il>

To: "Yaniv Drukman" <yd@dr-vb.co.il>

References: <0HPF000R249HJJ@mxout3.netvision.net.il>

Subject: Spam group – notes for second draft

Date: Fri, 5 Dec 2003 12:36:02 +0200

MIME-Version: 1.0

Content-Type: TEXT/PLAIN

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2800.1158

X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2800.1165

בשיטה זו, תוכנות הסינון יכולות לבדוק את ה-header (כותרת) של ההודעה, ולראות האם הוא מצביע על כך שההודעה נשלחה ממקור האופייני לדואר זבל (למשל), ואם כן – ניתן יהיה למחוק את ההודעה מהשרת באמצעות הפקודה:

DELE 1

מבלי שיהיה צורך להוריד את כל ההודעה מהשרת למחשב הלקוח.

2. תוכנות המורידות את ההודעה למחשב הלקוח ורק אז בודקות האם ההודעה היא הודעת דואר זבל, על-ידי חיפוש אחר מילים האופייניות להודעות דואר זבל, בדיקה האם מקור ההודעה ידוע כמקור להודעות דואר זבל וכדומה.

המגבלות של תוכנות הסינון

אף תוכנת סינון עדיין אינה מושלמת, ואצל רובן חלק מדואר הזבל הצליח לחמוק ולהגיע לתיבת הדואר הנכנס של המשתמש. אך הבעיה העיקרית עם התוכנות, היא סינון בטעות של הודעות דואר לגיטימיות (הודעות שאינן דואר זבל). על מנת להימנע ממחיקת הודעות לגיטימיות, יש להוריד את רמת האגרסיביות של פעולת התוכנה, דבר המביא לכך שיותר ויותר דואר זבל יצליח להסתגל לתוך תיבת הדואר האלקטרוני שלנו.⁵⁶ חלק מהתוכנות מאפשרות לקבל דואר ממקורות ידועים בלבד ("רשימות לבנות"), הקושי בשיטה זו הוא, שכל מי שלא נמצא ברשימת המקורות הידועים – ייחסם, על אף שהודעתו לגיטימית ועל אף שאנו היינו מעוניינים לקבל את הודעתו.

⁵⁶ מץ, לעיל הערה 16, בע' 76-83.

בעיה נוספת היא שיש יותר מדי דואר זבל, דבר המאלץ את ספקיות האינטרנט ואותנו להקדיש משאבי עיבוד לסינון דואר הזבל ולהוציא כסף לרכישת תוכנות הסינון. איננו רואים הגיון בכך שאנו וספקיות האינטרנט צריכים לשלם עבור פרסומת של מישהו אחר. אמנם אנו משלמים עבור פרסומת בטלוויזיה בכך שאנו משקיעים זמן ותשומת לב, אך הדבר שונה, הואיל ועלות הפרסומות בטלוויזיה אינה מגולגלת על המשתמשים. הן בפרסומות באינטרנט והן בפרסומות בטלוויזיה, המפרסם הוא המשקיע בהפקת הפרסומת. הצופה, מצידה, משקיעה תשומת לב. בפרסומות בטלוויזיה המפרסם משלם לערוץ המשדר עבור זמן השידור. עלות התשלום נמדדת לפי משך שידור הפרסומת והרייטינג לו זוכים שידורי הערוץ בזמן הצפייה בו משודרת הפרסומת. מפיץ דואר זבל אינו משלם דבר לספק האינטרנט עבור הפצת הפרסומת (שידור הפרסומת ברחבי האינטרנט אל הצופים). כל עלות הפצת הפרסומת נופלת על ספק האינטרנט. על ספק האינטרנט לכסות עלות זו, ולכן הוא גובה תעריף יותר גבוה מלקוחותיו.

נוסף על כך, בפרסומות בערוצי המדיה השונים – טלוויזיה או רדיו, יש לצופים יכולת מסוימת להימנע מהפרסומות על-ידי מעבר לערוץ תקשורת אחר בזמן שידור הפרסומות. הפרסומות משודרות במקבצים, דבר המקל על המשתמש להימנע מקבלת הפרסומות. דואר הזבל מכיל פרסומות באופן כזה שהמשתמשים אינם יכולים להימנע מהן. בכל רגע נתון בו ניגשת המשתמשת לערוץ התקשורת בו היא מנהלת את הדואר האלקטרוני – היא חשופה לפרסומות. אין יכולת ניטרול של הפרסומות – בשונה מזו ששקיימת בערוצי המדיה הקלאסיים. דואר זבל מונע מהמשתמש את היכולת ליישם מנגנון בקרה כלשהו על כמות הפרסומות אליהן הוא חשוף. כך למשל, אם אני צופה בשידורי ערוץ 2, אני יודע שעבור כל שעת שידור אהיה חשוף למספר סופי של דקות פרסומת. כלומר – ככל שאצפה בשידורי הערוץ יותר זמן, כך אצפה בכמות פרופורציונאלית של שידורי פרסומת. מנגד, תיבת הדואר שלי חשופה תמיד לשידורי פרסומת, ולא מתקיימת פרופורציה בין כמות השימוש בתיבת הדואר לבין כמות הפרסומות. כך, נוצר מצב בו תיבת הדואר כל כך עמוסה בפרסומות עד שהשימוש בה אינו מעשי יותר – משך הזמן שמושקע בטיפול בדואר הזבל גדול בסדר גודל ממשך הזמן המושקע בטיפול בדואר האמיתי אותו מתכוון המשתמש לנהל.

אם נניח לשידורי הטלוויזיה לאפשר פרסומות כשם שאנו מקבלים דואר זבל, הרי שמשך כל זמן השידור נקבל פרסומות אל המסך, כך שאפשרות שינוי הערוץ הופכת ללא יעילה, וכן עבור כל פרסומת משודרת, נחויב בתשלום על זמן השידור. במצב זה, העלות העיקרית של הפרסומות בטלוויזיה תרד מכתפי המפרסמים עצמם, כך שלמפרסמים יהיו הן יכולת והן אינטרס להפיק כמה שיותר פרסומות. הצופים יאלצו לשלם מחיר הרבה יותר גבוה עבור שידורי הטלוויזיה, והמצב הקיים היום של ערוצים שקליטתם אינה עולה כסף עשוי להיעלם. ניתן לראות כי מפיצי דואר הזבל נהנים מבעית הרוכב החופשי. כל הגורמים האחרים מעורבים בתשלום עבור שירותי דואר האינטרנט השונים, למעט מפיץ דואר הזבל. זהו למעשה מצב של כשל שוק.

ניתן לראות שבכמה מובנים, אילו היו שידורי רדיו וטלוויזיה מאפשרים פרסומת באותה צורה בה מופץ כיום דואר זבל, הרי הם היו נכשלים. לאור שיקולים אלה, איננו רואים הגיון בכך שאנו וספקיות האינטרנט צריכים לשלם עבור פרסומת של מישהו אחר, ובכך לאפשר קיום של ערוץ תקשורת המעודד מצב של כשל שוק – המפרסם הוא רוכב חופשי.

טכנולוגיה חדשה - איתור וסינון דואר זבל לפי אפיוני תפוצה

חברת Commtouch מפעילה פתרון חדשני של איתור וגילוי הודעות דואר זבל שאינן תלויה כלל בתוכן הודעת הזבל, אלא רק באופן ההפצה שלה. כך התוכנה אינה תלויה בטקסט של ההודעה, או בתוכנה הגראפי. על-ידי דגימה של מידע מלמעלה מ-30 מיליון תיבות דואר על שרתי ספקי דואר אלקטרוני בכל העולם, ותוך זיהוי אופני התפוצה בעולם של דואר זבל, מצליח המוצר הנקרא ASAP לסנן למעלה מ-90% מהודעות הזבל, לדברי החברה.

העלויות לחברה כתוצאה מדואר הזבל נעצרות בתהליך המעבר של הדואר בצמתי הרשת. לא כל העלות נחסכת לחברה, אולם עיקר הנזק הכלכלי כתוצאה מתעבורת יתר ועיבוד יתר ברמת ספקי הדואר נמנע. אם מוצרים כמו זה יאומצו על-ידי ספקי הדואר, יתכן כי יימצא איזון לשוק דואר הזבל. עם הזמן יבינו המפיצים כי אינם משיגים תפוצה נאותה למכתביהם, ולבסוף תרד כמות דואר הזבל המציפה את הרשת. מוצרים כגון זה מאפשרים לשוק למצוא נקודת שווי משקל, גם אם זו אינה אופטימלית.

ב. מחלקת ה-Abuse של ספקית האינטרנט

דרך נוספת להתמודדות עם דואר הזבל היא באמצעות מחלקת ה-Abuse שמופעלות אצל רוב ספקיות האינטרנט. תפקידה של מערכת זו הוא לטפל בתלונות גולשים שנפגעו כתוצאה מניצול שירותיה של ספקית האינטרנט. מחלקה זו מטפלת גם בתלונות על קבלת ושליחת דואר זבל באמצעות שרתי החברה.⁵⁷ הבעיה היא ששולחי דואר זבל, לרוב מסתירים ומטשטשים את זהותם, כך שדואר הזבל יכול להיראות כנשלח דרך אותה ספקית אינטרנט – למרות שהדבר אינו כך.⁵⁸

⁵⁷ האתר הישראלי Tmicha.net אסף מידע על התלונות על דואר זבל שהגיעו לספקיות האינטרנט הישראליות, אולם בינתיים נסגר.

⁵⁸ גדי שמעון, "דע את המזבל", *netמגזין* 35 (אוגוסט 2003), 51, 52-53.

ג. מאגרי מידע על שולחי דואר זבל

הסובלות העיקריות מדואר הזבל הן ספקיות האינטרנט (ואנחנו בסופו של דבר כלקוחותיהן, כי העלויות שלהן מגולגלות בסופו של דבר עלינו), שנאלצות להוסיף משאבי אחסון ועיבוד נוספים, כדי לאפשר את תעבורת דואר הזבל. לכן על מנת להילחם בתופעה, ספקיות האינטרנט נעזרות במאגרי מידע על שולחי דואר זבל, שהידוע מכולם הוא Spam-Cop.⁵⁹ מאגרי מידע אלו כוללים ריכוז של כתובות דואר אלקטרוני, כתובות IP ומאפיינים מזהים אחרים של שולחי דואר זבל. שיטה זו מתגלה כאפקטיבית מאוד, כי כאשר שם של ספקית אינטרנט נכנס לאחת הרשימות הללו מיד הודעות הדואר של לקוחותיה נחסמות, דבר הגורם ללקוחות להתקשר באופן מיידי לתמיכה הטכנית של ספקית האינטרנט, דבר שגורם לה לפעול באופן נחרץ ומהיר נגד שולחי דואר הזבל המשתמשים בשירותיה על מנת שהיא תצא מאותן רשימות שחורות.

ד. שינוי הארכיטקטורה של האינטרנט על מנת לצמצם את היקף דואר הזבל

כפי שצוין במבוא לנייר עמדה זה, הסיבה שכל כך קל וזול לשלוח דואר זבל טמונה בפרוטוקול ה-SMTP המשמש לשליחת רוב הדואר בעולם. לכן ב- Internet Research Task Force (ה-IRTF), שפיתח במקור את פרוטוקול ה-SMTP, הוקמה קבוצה הבודקת אילו שינויים יש לבצע בטכנולוגיית האינטרנט, על מנת לצמצם את היקף דואר הזבל.⁶⁰ חברי הקבוצה דנים כיום בדרכי שדרוג פרוטוקול ה-SMTP ובשינוי סטנדרטים אחרים באינטרנט, בדרך כזו שתקשה על הפצת דואר זבל. נכון לזמן כתיבת שורות אלו, עדיין לא פורסמו המלצותיה של קבוצה זו.

לפני מספר שנים פורסמו הצעותיה של קבוצה אחרת, שעבדה במסגרת ה- Internet Engineering Task Force (IETF),⁶¹ לשינויים בפרוטוקול ה-SMTP, העשויים להקשות באופן ניכר על שליחת ספאם. כאשר עיקר התיקונים לפרוטוקול ה-SMTP, שהוצעו על-ידי ה-IETF הם:⁶²

⁵⁹ אתר Spam-Cop : <http://www.spamcop.net>

⁶⁰ קבוצה זו נקראת ASRG (Anti-Spam Research Group) ופעילותה מתוארת בדף הבא: <http://asrg.sp.am>

⁶¹ ה-IRTF וה-IETF עוסקים בתחומים משותפים תוך כדי שיתוף פעולה, כאשר קבוצות העבודה של ה-IRTF עוסקות במציאת פתרונות לטווח ארוך, וקבוצות העבודה של ה-IETF עוסקות במציאת פתרונות לטווח הקצר.

⁶² IETF Network Working Group, "RFC 2505: Anti-Spam Recommendations for SMTP MTAs", IETF (1999), <http://www.ietf.org/rfc/rfc2505.txt>

1. אימות זהות השולח, הנשלחת ב-"MAIL From" באמצעות שרת ה-DNS,⁶³ כדי לוודא שאכן אותו דואר אלקטרוני שייך לשם מתחם קיים. הבעיה ביישום פתרון זה, הוא העומס העלול להיווצר על שרתי ה-DNS אם כל שליחת דואר אלקטרוני תצטרך לעבור אימות מול שרת ה-DNS. אך, ניתן לפתור את הבעיה הזו על-ידי יצירת מטמון (cache) שישמור את המידע על שמות המתחם בשרת ה-SMTP עצמו, דבר שיגדיל את העומס (ויגדיל את זמן העיבוד) על שרת הדואר, אך ימנע עומס על שרת ה-DNS.⁶⁴ חברת AOL, ספקית האינטרנט הגדולה בארצות הברית, אף הציעה פתרון דומה בשם Sender Policy Framework (SPF),⁶⁵ שמוסיף רשומה לשרת ה-DNS, בה מוגדרים מאילו שרתים ניתן יהיה לשלוח דואר אלקטרוני תוך שימוש בשם מתחם מסוים.⁶⁶

דרך פעולת SPF:⁶⁷

נניח שהספאמר מנסה לזייף את כתובת המקור, ככתובת השייכת לשם המתחם haifa.ac.il. כאשר הוא מצהיר שמקור הדואר הוא בכתובת: forged@haifa.ac.il, אין צורך להאמין לו, אלא ניתן יהיה לבדוק ברשומת ה-DNS של שם המתחם haifa.ac.il (שמישם את SPF), האם ה-IP ממנו נשלח הדואר, אכן שייך לרשת שלו. למשל רשומת ה-DNS הבאה:

```
haifa.ac.il IN TXT "v=spf1 mx ptr -all"
```

אומרת ב-"mx", כי אם לשם המתחם haifa.ac.il יש רשומת MX, התואמת לכתובת IP של השולח, אז יש לאפשר את שליחתה (כי הדואר מגיע מאחד משרתי הדואר של שם המתחם haifa.ac.il).

כמו כן הרשומה אומרת ב-"ptr", כי אם מצאנו שה-Hostname (שם המחשב המארח), של השולח הוא haifa.ac.il, אז יש לאפשר את שליחת הדואר (הואיל והדואר נשלח ממחשב ששייך לרשת של haifa.ac.il).

ה-"all" אומר, כי אם אחת מסוגי ההתאמות (mx או ptr) לא עבדו, אז יש לדחות בכל מקרה אחר את הדואר ולא לאפשר את העברתו הלאה (הערה: v=spf1 מצייין את גרסת ה-SPF).

⁶³ תפקידו של שרת ה-DNS (קיצור של Domain Name Service) הוא לתרגם שמות מתחם למספרי IP. שרת ה-DNS מעדכן כל פרק זמן מסוים את רשימת שמות המתחם מול שרתי ה-Root (שרתי ה-DNS הראשיים), כך שהוא כולל מידע די עדכני על כל שמות המתחם הרשומים. שרת ה-DNS גם יכול לבדוק האם שם מתחם מסוים קיים.

⁶⁴ ראו לעיל, הערה 62, בע' 3-4, 14.

⁶⁵ פתרון זה הוכר בעבר (עד 11.2.2004) בשם "Sender Permitted From" (SPF). כמו כן, חשוב לציין כי SPF הוא סטנדרט פתוח. באוקטובר 2003, קבוצת המחקר ASRG שהוזכרה לעיל הערה 60, נתנה את חסותה לפרויקט זה.

⁶⁶ Paul Roberts, "AOL testing new antispam technology", **InfoWorld** (22.1.2004), http://www.infoworld.com/article/04/01/22/HNaolantispam_1.html

⁶⁷ SMTP+SPF team, "SPF: Frequently Asked Questions", **SMTP+SPF Project** (13.2.2004), <http://spf.pobox.com/faq.html>

אך תיקון מסוג זה, על אף שהוא נראה כאפקטיבי מאוד בפתרון בעיית דואר הזבל, עשוי לעורר בעיות בשני מישורים (לפחות): א. הדבר יגרום לכך שתנועת הדואר האלקטרוני, תפסיק להיות ברובה אונימיית, והדבר יקל על "חטטנים אלקטרוניים", לעקוב ביתר קלות אחר הדואר האלקטרוני שלנו, ולבדוק בדיוק מי שלח הודעה למי ומתי.⁶⁸ ב. יישום פתרון מעין זה, מחייב שינוי של שירותי קידום הדואר (email forwarding),⁶⁹ אחרת לא יהיה ניתן לקבל דואר משרת המקדם דואר אלקטרוני שנשלח במקור משרת אחר (הואיל וכתובת ה-IP של השרת המקדם, איננה שייכת לרשת, שלה שייכת כתובת הדואר האלקטרוני ממנה מקדמים את הדואר).

2. סירוב לקבל דואר משולח המזהה את עצמו בבקשת ה-HELO בשם מתחם מזויף.⁷⁰
3. סינון דואר הזבל ברמת שרת ה-SMTP, דבר החוסך את עיבודו של הדואר אם הוא מזוהה כדואר זבל. הדבר חוסך גם את השימוש בתוכנות סינון, הואיל ותוכנות הסינון מטפלות בדואר הזבל, רק לאחר שהוא כבר נתקבל בשרת ה-SMTP. הדבר יעשה על-ידי בדיקה עם רשומת ה-MX⁷¹ של שם המתחם המסוים, שתכלול גם רשימת כתובות (refuse-list) מהן או להן יש לסרב לקבל דואר אלקטרוני.⁷²
4. להרחיב את פרוטוקול SMTP בפקודות סינון דואר שמקורו בשמות מתחם, או טווח כתובות IP מסוים.⁷³
5. אפשרות ליצירת רשימת כתובות (שנשלחו בבקשת MAIL From), או שמות מתחם (המזוהים בבקשת HELO), מהם יש לסרב לקבל דואר אלקטרוני. המטרה בדבר זה, היא לאפשר ליצור רשימות של כתובות ושמות מתחם הידועים כנמצאים בשימוש על-ידי ספאמרים, וכך שרת ה-SMTP עצמו יסרב לקבל את הודעות הדואר, מבלי שהוא יצטרך (כמעט בכלל) לעבד אותן.⁷⁴

⁶⁸ Michael J. Miller, "Technology and Politics: The Choices for 2004", **PC Magazine** (15.1.2004), <http://www.pcmag.com/article2/0,4149,1437815,00.asp>

⁶⁹ Email forwarding – שירות נפוץ לקידום הודעות דואר אלקטרוני, מכתובת דואר אלקטרוני אחת או יותר לכתובת דואר אלקטרוני אחרת. שירות זה מקל (למשל) על קיבוץ כל הודעות הדואר לתיבת דואר אחת, עבור אנשים המחזיקים מספר כתובות דואר אלקטרוני. גם האתר Tmicha.net, מספק למעשה (גם) שירות של העברת דואר אלקטרוני נקי מספאם, דרך שרתי האתר לתיבת הדואר האלקטרוני של המנוי.

⁷⁰ ראו לעיל, הערה 62, בע' 6.

⁷¹ קיצור של mail exchange record – רשומה זו (הנמצאת בשרת ה-DNS) קובעת איזה שרת דואר יטפל בכתובות דואר השייכות לשם מתחם מסוים.

⁷² ראו לעיל, הערה 62, בע' 8-9.

⁷³ שם, בע' 3, 6-7.

⁷⁴ שם, בע' 6.

6. להקטין את קצב שליחת ההודעות ממקור השולח הודעות רבות (Bulk mail) ליעדים רבים. מכיוון שדואר זבל בדרך כלל נשלח במסות, הדבר יקטין את קצב השליחה שלו ויאפשר לדואר לגיטימי להישלח מבלי להתעכב (כמעט) על-ידי דואר הזבל. דואר הנשלח בכמויות אינו נחסם לחלוטין, מפני שהוא עשוי להיות דואר לגיטימי, ולכן ההצעה היא רק להקטין את קצב השליחה שלו, כדי לא לפגוע בשליחת שאר הודעות הדואר שנתקבלו בשרת.⁷⁵

7. אי קבלת הודעות דואר מכתובת IP שאיננה נמצאת בשימוש לפי נתוני ICANN.⁷⁶ מכיוון שספאמרים רבים מעוניינים להסתיר את מקור שליחת דואר הזבל, הם מזייפים את כתובת ה-IP ממנה נשלח הדואר האלקטרוני, דבר זה ימנע קבלת דואר אלקטרוני מכתובות IP שאינן קיימות, ובכך יקטין את היקף דואר הזבל המועבר, מכיוון שלאחר אימוץ פתרון זה, הספאמרים יאלצו לחשוף את כתובת ה-IP שלהם (אך הספאמרים עדיין יוכלו להשתמש בשרתי Proxy שיסתירו את כתובות ה-IP שלהם. אפשר לפתור די בקלות בעיה זאת, על-ידי אי-קבלת דואר שעבר דרך שרת Proxy המאפשר תעבורת מידע אנונימית).⁷⁷

תיקונים אלו, אם וכאשר ייושמו באופן נרחב (במרבית שרתי ה-SMTP), עשויים להפחית באופן ניכר את תעבורת דואר הזבל בעולם, בעיקר בגלל שיגרמו לשולחי דואר הזבל להיות חשופים יותר (הם יצטרכו להעביר כתובת IP אמיתית ושם מתחם אמיתי), דבר שיקל על איתורם. בנוסף אמצעים שידחו את דואר הזבל ברמת שרת ה-SMTP, עשויים להוריד באופן ניכר את המוטיבציה של שולחי דואר הזבל, שיקלעו למצב בו רוב הדואר שלהם נחסם ברמת השרת, מבלי שהוא מגיע כלל לנמען הסופי. עם זאת, שולחי דואר הזבל עשויים לגלות "יצירתיות" בעקיפת המגבלות הללו – אך יש מחיר ליצירתיות הזו (הזמן והמשאבים הדרושים לפיתוח האמצעי לעקיפת המגבלות), דבר שיגרום לכך ששליחת דואר זבל תהיה פחות כדאית.

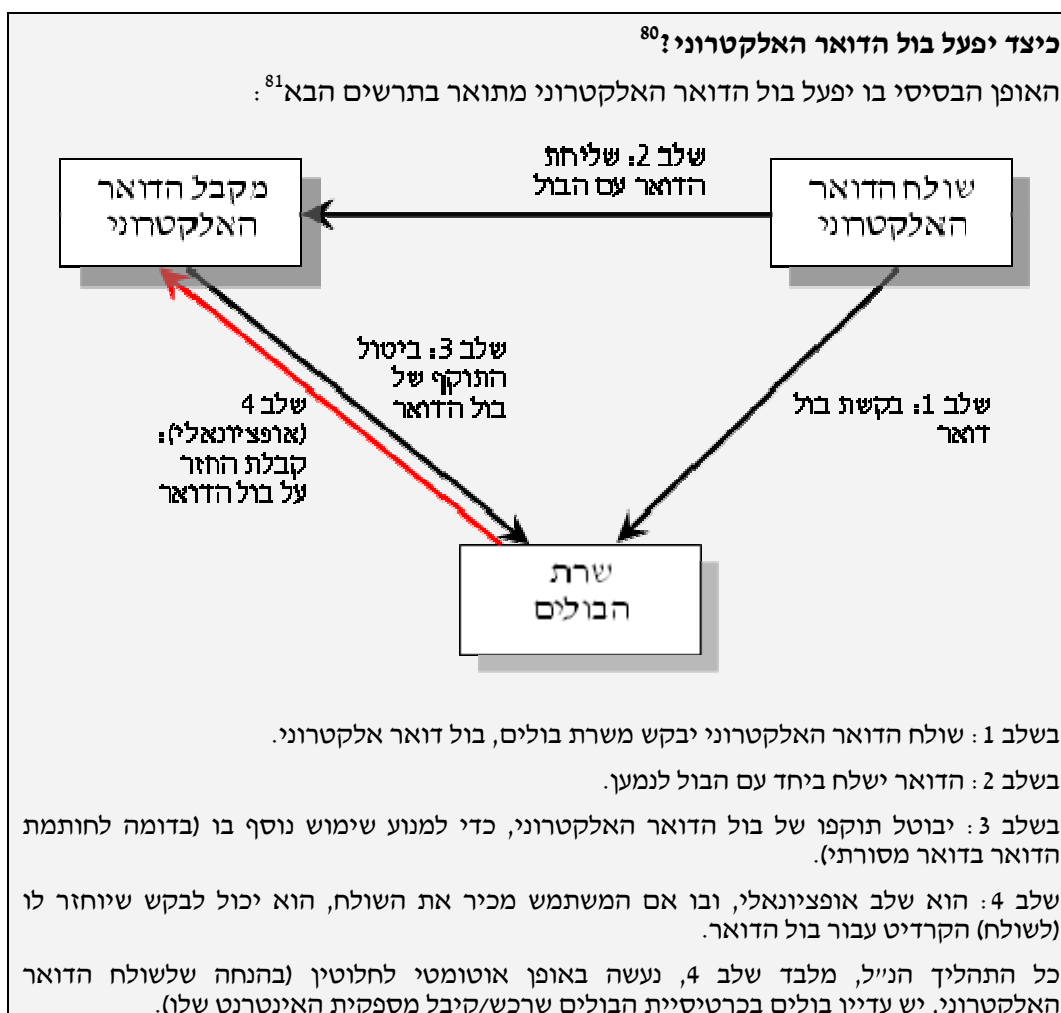
⁷⁵ שם, בע' 14.

⁷⁶ Internet Corporation for Assigned Names and Numbers - ICANN - הגוף המפקח והמקצה כתובות IP ו-TLDs באינטרנט. ICANN האצילה את סמכותה לרשמי אינטרנט אזוריים (RIR), כמו ARIN בצפון אמריקה, RIPE באירופה, APNIC באסיה, אוסטרליה ובאיים באוקיאנוס השקט, LACNIC באמריקה הלטינית ובאיים הקריביים ו-AfriNIC באפריקה.

⁷⁷ ראו לעיל, הערה 62, בע' 7-8.

ה. חזרה לעידן בולי הדואר

בתחילת שנת 2003, הכריזה חברת Microsoft על פרויקט נגד דואר זבל – בשם " Penny Black".⁷⁸ הפרויקט מציע לבייל כל הודעת דואר אלקטרוני בבול אלקטרוני, בעלות נמוכה מאוד, שלא תמנע משולחי דואר לגיטימי משלוח אותו, אך תגרום לכך ששליחת דואר אלקטרוני במסות גדולות על-ידי שולחי דואר הזבל לא תהיה כדאית, מפני שהם יאלצו לשלם סכומי כסף גדולים.⁷⁹ על מנת ליישם את הפרויקט, נדרש שיתוף הפעולה של ספקיות האינטרנט, שמצד אחד מעוניינות להקל את עומס דואר הזבל העובר דרכן, אך מצד שני הן חוששות מיצירת "אפקט צינון" אצל לקוחותיהן, שיירתעו משליחת דואר זבל בגלל עצם העובדה שהוא אינו בחינם יותר. התשלום עבור בולי הדואר אמור להתבצע באמצעות ספקיות האינטרנט עצמן, או באמצעות אמצעי תשלום אלקטרוניים אחרים.



⁷⁸ על שם בול הדואר הראשון שהונפק באנגליה בשנות ה-30 של המאה ה-19.

⁷⁹ Microsoft, "The Penny Black Project", **Microsoft.com** (2003), <http://www.research.microsoft.com/research/sv/PennyBlack>

⁸⁰ Martín Abadi, Andrew Birrell, Mike Burrows, Frank Dabek, Ted Wobber, "Bankable Postage for Network Services", Proceedings of the 8th Asian Computing Science Conference (Mumbai, India, December 2003), 76-79. ניתן לעיין בגרסה אלקטרונית של המאמר בכתובת הבאה: <http://research.microsoft.com/research/sv/pennyblack/demo/ticketserver.pdf>

הבעיה העיקרית במודל זה, היא שעדיין לא ברור מי יפעיל את אותם שרתי בולי דואר אלקטרוני (Ticket Server). ישנם כאלו המביעים חשש, שרעיון זה מבטא ניסיון של Microsoft ליצור שוק חדש, ואז להשתלט על נתח השוק של שליחת הדואר האלקטרוני.⁸²

⁸¹ שם, בע' 77 (התרשים תורגם על ידנו מאנגלית).

⁸² "בחזרה לעידן הבוליס", ynet (17.2.2003), <http://www.ynet.co.il/articles/1.7340.L-2441016.00.html>

4. מודלים משפטיים: ארצות הברית, האיחוד האירופי

ונטיקט

בפרק זה נסקור את שני המודלים המשפטיים העיקריים הקיימים להתמודדות עם בעיית דואר הזבל האלקטרוני. המודל המשפטי האמריקני, הנוקט מדיניות של Opt-Out, המחייבת מתן אפשרות ליציאה בדיעבד מרשימת הדיוור של שולח הדואר (שכלל לא ביקשנו להיות מנויים בה) והמודל המשפטי האירופאי, הנוקט מדיניות Opt-In, המחייבת הסכמה מראש למשלוח דואר אלקטרוני פרסומי. בנוסף נבדוק האם ניתן להשתמש בכללי האתיקה של הרשת, על מנת לטפל בבעיה.

א. ארצות הברית

ב-2004.1.1 נכנס לתוקפו החוק האמריקני (CAN-SPAM Act, 2003) לטיפול בתופעת דואר הזבל האלקטרוני.⁸³ החוק אוסר על משלוח דואר אלקטרוני אשר לא קיבל את אישורו מראש של הנמען שתוכנו הוא "שקרי או מטעה". החוק החדש גם אוסר על שולחי דואר זבל:⁸⁴ א. להסוות את זהותם על-ידי שימוש בכתובות דואר אלקטרוניות מזויפות. ב. להשתמש בכותרות מטעות להודעות הדואר האלקטרוני. ג. לקצור כתובות דואר אלקטרוני מאתרי אינטרנט. הפרת איסורים אלו, עשויה להביא לקנסות כבדים ואף למאסר בפועל. החוק האמריקני נוקט מדיניות של Opt-Out, כאשר הוא מחייב את השולח לתת לנמענים אפשרות להסיר את עצמם מרשימת הדיוור שלו. יישום החוק האמריקני על מדיניות ה opt out שבו היא בדרך של הקמת מאגר מידע, בו יירשמו לקוחות או בתי אב אשר אינם מעוניינים לקבל דואר זבל אלקטרוני (Do-Not-E-Mail registry). כאשר משלוח דואר זבל לכתובת דואר אלקטרוני המופיעה במאגר, תוך התעלמות מרצונו המפורש של הנמען, עלולה להביא לחיובו של המפר בפיצויים עד גובה מיליון דולר, ואף להוביל להליך פלילי שבצידו עונש היכול להגיע עד כדי מאסר.

נדמה שהוראות החוק שנתקבלו נובעות בעיקר (ולא במפתיע בהתחשב בתרבות האמריקנית), מתוך תפיסה שדואר זבל אינו משרת מטרות כלכליות, כאשר בוחנים את התופעה במונחים של תועלת חברתית מצרפית. מחקרים שנעשו בארצות הברית מראים כי כמחצית מתעבורת הדואר האלקטרוני היא דואר זבל. בתרגום למונחים כלכליים התופעה עולה לכלכלה האמריקנית כ-10 מיליארד דולר בשנה, כאשר הכימות נעשה על-פי ממוצע שעות העבודה המבוזבזות של הנמען הטורח למחוק את התכתובת חסרת הערך מבחינתו.

⁸³ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act).

⁸⁴ 47 U.S.C. §1037 (2003)

על אף האמור נדמה שקיימת גם תכלית נוספת העומדת מאחורי המהלך. האמריקנים רואים בתופעת דואר זבל כגורם בעל אופי מטריד ללא קשר ישיר להשלכותיו הכלכליות. הסנאטור Tom Daschle מציין כי "ספאמרים מטרידים לקוחות ומשפחות כבר יותר מדי זמן".⁸⁵ לעניות דעתנו, מאמירה זו ניתן ללמוד כי העם האמריקני אינו סובלני כלפי חדירה פולשנית לא קרואה אל תוך התא המשפחתי.

הערכת החוק האמריקני

על אף שנדמה כי האמריקנים החליטו לשים קץ לתופעת דואר הזבל ונעשות פעולות ברמה החקיקתית, יש לציין כי החוק אינו אוסר על משלוח דואר זבל מכל סוג, אלא רק דואר זבל העונה להגדרה "שקרי או מטעה".⁸⁶ אנו סבורים כי בהגדרה זו מנסה המחוקק האמריקני להימנע מהדילמה הפרשנית אשר עשויה להתעורר בהקשר של הצעת החוק הישראלית (הכשל שבהגדרה הרחבה לפיה דואר זבל, הוא דואר שאינו מביא תועלת ישירה לנמען).

בנוסף, מדיניות ה-Opt-Out אותה נוקט החוק, מכשירה למעשה שליחת דואר זבל אלקטרוני, בתנאי שהספאמרים אינם מזייפים או מסווים את כתובת הדואר האלקטרוני שלהם, אינם שולחים הודעות פורנוגרפיות ובתנאי שהם נותנים אפשרות לנמענים להסיר את עצמם.

החוק הפדראלי בנוגע לדואר זבל, גובר על כל חקיקה מדינתית בנושא דואר הזבל במידה שהם מתנגשים, כולל החוק של מדינת קליפורניה,⁸⁶ שנכנס גם הוא לתוקף ב-1 לינואר 2004. החוק הקליפורני קובע מדיניות מחמירה יותר כלפי דואר הזבל האלקטרוני: א. הוא אוסר על משלוח דואר אלקטרוני פרסומי, ללא הסכמה מפורשת או בלא קשר עסקי קודם. ב. הוא מאפשר לספקית האינטרנט של שולח דואר הזבל, המפר את הוראות החוק, לתבוע אותו (את הספאמר) בגין הפרת מדיניות הדואר האלקטרוני שלה. ג. החוק מאפשר לאנשים פרטיים, לתבוע בהליך אזרחי את הספאמרים. ד. החוק מטיל קנסות, גם כאשר מדובר על משלוח הודעה פרסומית בודדת בניגוד לחוק, ולא רק במקרה של שליחה מסיבית של הודעות דואר זבל (שאינן עשויות היו להיות מוטלים על הספאמר קנסות כבדים מאוד). ה. החוק חל לא רק על הודעת דואר הנשלחת מקליפורניה, אלא גם על כל הודעת דואר אלקטרוני הנשלחת לקליפורניה, מכל מקום בעולם.

כאמור, בכל מקום בו יש סתירה בין החוק הפדראלי (ה-CAN-SPAM) לחוק הקליפורני, החוק הפדראלי יגבר, וחבל שכך, הואיל והחוק הקליפורני נחקק בעקבות לקחים שהופקו מחקיקה מדינתית קודמת (שלא הצליחה במלחמתה בדואר הזבל). פרופסור Lawrence Lessig אמר בעניין, כי החוק הפדראלי הוא נקודת ציון חשובה במלחמה בת שמונה השנים

⁸⁵ רויטרס, "הסנאט האמריקני חוקק חוק אנטי ספאם", ynet (23.12.03), <http://www.ynet.co.il/articles/1,7340,L-2803215,00.html>

⁸⁶ California Business and Professions Code §17529-17529.9, 17538.45, Restrictions on Unsolicited Commercial E-mail Advertisers

בדואר הזבל האלקטרוני, אך הוא גם "כשלון מוחלט", מפני שהוא לא הפיק את הלקחים מחקיקה דומה, שלא הצליחה לבלום את התפשטותו של דואר הזבל.⁸⁷

מגבלות על דואר זבל אלקטרוני וחופש הביטוי בארצות הברית⁸⁸

מאחר שהטלת מגבלות על משלוח דואר זבל עשויה להיתקל בטענה כי יש בכך פגיעה בחופש הביטוי, ראינו לנכון לבחון את השאלה בקצרה. חופש הביטוי בארצות הברית מוגן בתיקון הראשון לחוקה האמריקנית,⁸⁹ הקובע:

"Congress shall make no law ... abridging the freedom of speech, or the press...".

הזכות לחופש הביטוי מקיפה גם ביטוי כתוב כמו דואר אלקטרוני. אפילו, ודווקא סוגי ביטוי, שאינם פופולאריים – זכאים להגנה תחת התיקון, למרות שמגבלות מסוימות על חופש הביטוי עשויות להיות חוקתיות. מגבלות על חופש הביטוי בארצות הברית ניתן לסווג לשתי קטגוריות: א. מגבלות המבוססות על תוכן הביטוי. ב. מגבלות המבוססות על אפקט "העוינות" המיוחס לביטוי, מבלי להתחשב בתוכנו. מגבלה שאינה נופלת לאחת מן הקטגוריות האלו – הינה בלתי חוקתית, ותיפסל על-ידי בתי המשפט.

א. מגבלות המבוססות על תוכן הביטוי

התנאי הבסיסי, לפיו מגבלה על חופש הביטוי תהיה חוקתית, הוא שהמגבלה צריכה להיות ניטרלית לתוכן של הביטוי המסוים. כאשר הממשל מטיל מגבלה המבוססת על תוכן הביטוי, הוא חייב להראות שהמגבלה היא הכרחית, על-מנת לשרת אינטרס ציבורי משכנע והיא מידתית ביחס למטרתה. כאשר ביטוי מסחרי, הוא יוצא דופן לכלל זה, כך שניתן להטיל עליו מגבלות, ללא צורך לעבור את מבחן הבדיקה הקפדנית.⁹⁰

בפרשת *Central Hudson*,⁹¹ קבע בית המשפט העליון האמריקני, כי הגבלה על ביטוי מסחרי תהיה חוקתית במידה שהיא עומדת במבחן הכולל ארבעה תנאים: 1. הביטוי המסחרי אינו מוגן מסיבה אחרת, כמו במקרים בהם מדובר בביטוי מטעה, או בביטוי הנוגע לפעילות בלתי חוקית. 2. חייב להיות אינטרס ממשלתי חשוב, המצדיק את המגבלה. 3. המגבלה חייבת לקדם דווקא את אותו האינטרס ממשלתי החשוב. 4. המגבלה חייבת שלא לעלות על הנדרש (מידתיות), כלומר היא חייבת שלא להיות רחבה מהמינימום ההכרחי הנדרש על מנת לקדם את האינטרס הציבורי החשוב.

⁸⁷ Stefanie Olsen, "California 'disempowered' by federal spam law", CNet (22.1.2004), <http://news.com.com/2100-1028-5145849.html>

⁸⁸ R. Jonas Geissler, "Whether Anti-Spam Laws Violate : בכתיבת חלק זה על נעזרנו רבות במאמר: The First Amendment", 8 *J. Online L.* 1 (2001).

⁸⁹ U.S. Const. Amend. 1

⁹⁰ ראו: *Virginia Pharmacy Bd v. Virginia Consumer Council*, 425 U.S. 748 (1976), שקבע כי ביטוי מסחרי אינו זוכה לאותה רמת ההגנה כמו ביטוי שאינו מסחרי.

⁹¹ *Central Hudson v. Public Service Commission*, 447 U.S. 557 (1980)

ב. מגבלות שאינן נוגעות לתוכן הביטוי

הסוג השני של המגבלות על חופש הביטוי, כולל מגבלות שאינן נוגעות לתוכנו של הביטוי, אלא לזמן, למקום ולאופן בו הביטוי מבוטא. כאשר הממשל מטיל מגבלה על ביטוי ללא קשר לתוכנו, אזי, בית המשפט יפעיל מבחן דו-שלבי: א. בחינה האם המגבלה אכן ניטרלית לתוכן הביטוי. כאשר במידה שבית המשפט מוצא שהמגבלה מופנית לתוכן הביטוי, אז המגבלה אינה ניטרלית לתוכן ולכן צריכה לעבור את המבחן הקפדני שצריכות לעבור מגבלות המגבילות את תוכנם של ביטויים. ב. אפילו במקרה שעל פניו, נראה שהמגבלה ניטרלית לתוכן הביטוי, בית המשפט יבחן בשלב השני, האם המגבלה מיועדת לסוגים מסוימים של ביטויים. במידה שהמגבלה עוברת את שני שלבי המבחן, אזי היא נחשבת כניטרלית לתוכן הביטוי.

כאשר מגבלות ניטרליות לתוכן מוערכות בהתייחס לפרום ספציפי: א. אם המגבלה מתייחסת לפרום ציבורי, אז האינטרס הממשלתי החשוב המגולם במגבלה, חייב לעלות על האינטרס הגלום בחופש הביטוי של הדובר בפרום הציבורי. בנוסף המגבלה חייבת להיות מידתית ומצומצמת ככל האפשר. ב. אם המגבלה מתייחסת לפרום שאינו ציבורי, אז הממשלה צריכה רק להראות כי המגבלה קשורה באופן הגיוני לאינטרס ממשלתי חשוב וכי יש לדובר דרכים אלטרנטיביות אחרות להגיע לאותו קהל. אם אין לדובר דרכים אלטרנטיביות כדי להגיע לאותו קהל המטרה, אז הממשל צריך להראות שהמגבלה על חופש הביטוי במקרה זה אינה עולה על הנדרש.⁹² מבלי להתייחס לפרום אליו מתייחסת המגבלה, בית המשפט עדיין יכול לפסול את המגבלה על חופש הביטוי במידה שהיא רחבה מדי או מנוסחת בצורה מעורפלת.

כאשר מדובר במגבלה על ביטוי פוליטי, בית המשפט יבחן את המגבלה בצורה קפדנית יותר, למרות שעדיין ביטוי פוליטי עשוי להיות כפוף למגבלות ניטרליות לתוכן, כמו מגבלות הנוגעות לזמן למקום ולצורה שהוא מבוטא וכל זאת הואיל וביטוי זוכה להגנה המרבית תחת התיקון הראשון לחוקה, מתוך הכרה בחשיבותו הרבה של חופש הביטוי הפוליטי.

מגבלות על דואר זבל וחופש הביטוי

כדי לבחון האם הטלת מגבלות על דואר זבל בחוק פוגעת בחופש הביטוי בארצות הברית, יש קודם לאפיין את דואר הזבל והמגבלות האפשריות שניתן להטיל עליו:

1. **הפורום של דואר הזבל אינו פורום ציבורי** – הואיל ודואר הזבל מופנה לפרטים המשתמשים בתיבות הדואר האלקטרוני אליהן הוא נשלח. הפורום ייחשב כציבורי במידה שהוא ידוע כזה, או במידה שוהוא עונה לשני התנאים (המצטברים) הבאים: א. הפורום באופן מסורתי לאסיפות ציבוריות. ב. המטרה הבסיסית של הפורום היא לאפשר החלפת דעות חופשית. תיבת הדואר האלקטרוני, אינה ידועה כפורום ציבורי, מכיוון שלרוב, כל תיבת דואר אלקטרוני היא בשימוש של אדם יחיד. בנוסף תיבת הדואר האלקטרוני אינה עונה לשני התנאים המצטברים הנ"ל לקיומו של פורום ציבורי: א. ברור כי תיבת הדואר האלקטרוני אינה משמשת לאסיפות ציבוריות (בעוד

- פורומים וחדרי צ'אט ברשת, עשויים להיות כאלו).
 ב. אמנם תיבת הדואר האלקטרוני מאפשרת החלפת מידע בין השולח לנמען או הנמענים, אך אין היא מאפשרת החלפת מידע חופשית, הואיל וקהל המטרה מוגדר מראש, על-ידי בחירת כתובות הדואר האלקטרוני, אליהן נשלחות הדעות.
2. **המגבלות הן, לרוב, על ביטוי מסחרי:** רוב המגבלות, שהוצעו בחקיקה בארצות הברית, כמו בחוק הפדראלי שנכנס לתוקף ב-1 לינואר 2004,⁹³ מתייחסות לדואר זבל מסחרי, וכאמור ביטוי מסחרי זוכה להגנה פחותה תחת התיקון הראשון לחוקה האמריקנית. למרות שהסיבה לכך שהחקיקה הפדראלית מתייחסת רק לדואר אלקטרוני מסחרי ("unsolicited commercial electronic mail"), וברור שההגדרה נועדה לעמוד בדרישה החוקתית בהטלת מגבלות על ביטוי שאינו מסחרי, אין זה תמיד פשוט להבחין בין דואר אלקטרוני מסחרי לבין דואר אלקטרוני שאינו מסחרי. לדוגמה: האם דואר אלקטרוני הכולל קישור לאתר בו נמכרת סחורה הוא ביטוי מסחרי?⁹⁴ החוק הפדראלי האמריקני דווקא מתייחס לבעייתיות זו, וקבע כי גם דואר אלקטרוני המפנה לתוכן מסחרי באינטרנט נחשב להודעת דואר אלקטרונית מסחרית.⁹⁵ הבעייתיות עשויה עדיין להתעורר במסרים המכילים ביטויים פוליטיים לצד ביטויים מסחריים. למשל, ארגון עובדים המביע בהודעות דואר אלקטרוני ששלח עמדות פוליטיות פרו-סוציאליסטיות, שהן ביטוי פוליטי, לצד המלצה לקוראים לקנות רק תוצרת אמריקנית, על מנת לתמוך בעובדים האמריקנים.
3. **המגבלות הן מסוג מניעה מוקדמת (prior restraint):** כלומר הן מונעות את עצם הגעת דואר הזבל לנמענים (לפי דוקטרינת המניעה המוקדמת, לא ניתן למנוע את הביטוי מראש, אלא רק במקרים מסוימים, להטיל עליו סנקציה לאחר שהביטוי כבר יצא).⁹⁶

האם המגבלות בחוק ה-CAN SPAM סותרות את התיקון הראשון לחוקה האמריקנית?
 החוק האמריקני הפדראלי, מתייחס לדואר אלקטרוני מסחרי, ולכן צריך לעבור את המבחן שקבע בית המשפט העליון האמריקני בפרשת *Central Hudson*: 1. החוק האמריקני אוסר על כותרות מטעות להודעות וכן על זיוף המידע על מקור ההודעה (header information). ולכן, במידה שלהודעה יש כותרת מטעה, היא עשויה ליפול על התנאי הראשון של המבחן ולכן מגבלה כזו תהיה חוקתית. 2. האינטרס החשוב המצדיק את המגבלה הוא ההגנה על הנמענים מפני תוכן מטעה או לא רצוי והגנה על הדואר האלקטרוני ככלי תקשורת יעיל. 3. החוק הפדראלי האמריקני בחר במודל Opt-out, המאפשר לנמענים דרך לבחור לא לקבל יותר דואר אלקטרוני מהשולח, כאשר כל מה שהשולח נדרש לעשות, הוא לאפשר לנמענים

⁹² *Ward v. Rock Against Racism*, 491 U.S. 781 (1989).

⁹³ CAN-SPAM, לעיל הערה 83.

⁹⁴ שאלה נוספת שיכולה להישאל בהקשר זה, היא האם קישור כשלעצמו הוא ביטוי?

⁹⁵ §3(2) ל-CAN-SPAM, לעיל הערה 83.

⁹⁶ להרחבה בנושא דוקטרינת המניעה המוקדמת: Ariel Bendor, "Prior Restraint, Incommensurability, and the Constitutionalism of Means", 68 *Fordham L.Rev.* 289 (1999).

דרך להסיר את עצמם מרשימת התפוצה שלו. פתרון כזה נראה שמקדם את האינטרס החשוב המצדיק את המגבלות שמטיל החוק הפדראלי. 4. בחירה במודל Opt-out שאינה אוסרת מראש את שליחת הדואר האלקטרוני, אלא אם כן הנמען בחר שלא לקבלו – נראה שעומדת בדרישת המידתיות.

נראה כי החוק הפדראלי עומד בתנאים שקבע בית המשפט העליון, בהם ניתן להטיל מגבלות על חופש הביטוי המסחרי. מכיוון שכאמור, הפורום של הדואר האלקטרוני אינו פורום ציבורי, וקיים אינטרס ציבורי חשוב בהגבלת דואר הזבל, נראה כי המגבלות בחוק עומדות גם בתנאים להטלת מגבלות הניטרליות לתוכן הביטוי ועל כן נראה כי החוק הפדראלי נגד דואר הינו חוקתי.

דרישת התיג (Labeling)

החוק הפדראלי מטיל גם חובה על שולחי הדואר המסחרי, לציין בצורה בולטת וברורה כי מדובר בהודעה מסחרית. כמו כן, חקיקה במדינות שונות בארצות הברית מחייבת את סימון של כותרות הודעות הדואר האלקטרוני המסחרי בתגיות "ADV" (לתוכן מסחרי) או "ADV:ADULT" (לתוכן מסחרי המיועד למבוגרים בלבד).⁹⁷ דרישת התיג, למעשה מתייחסת לתוכן הביטוי, ועל כן צריכה להיות מצומצמת ככל האפשר על מנת להשיג את האינטרס החשוב לשמו היא נועדה. לדעתנו, סימון "ADV" או סימון דומה לו בכותרת ההודעה, הינו מידתי וכל כן דרישה זו היא חוקתית.

עם זאת, יש שרואים בדרישת התיג כביטוי כפוי ("forced speech"), שהוא חמור כמו "שתיקה כפויה". לכן, לדעתם, דרישת התיג עומדת, בסתירה לתיקון הראשון לחוקה, במיוחד לאור קביעת בית המשפט העליון האמריקני בפרשת *Reno*,⁹⁸ כי האינטרנט הוא הצורה הזוכה להגנה הרבה ביותר של התיקון הראשון לחוקה.⁹⁹

⁹⁷ למשל: קליפורניה, אינדיאנה, קנטס, ניו-מכסיקו, אוקלהומה, מינסוטה, דקוטה הדרומית, טנסי ויוטה – מחייבות סימון "ADV" בכותרות של הודעות מסחריות ו-"ADV:ADULT" בכותרות של הודעות המכילות תוכן למבוגרים בלבד. קולורדו ונבדה למשל מחייבות סימון הודעות מסחריות בלבד ב-"ADV" ללא קשר האם ההודעה מופנית למבוגרים בלבד. מדינות נוספות בארצות הברית, כמו למשל, ויסקונסין ואלסקה – מחייבות סימון הודעות למבוגרים בלבד. כאמור החוק הפדראלי בעניין הסימון יגבר על החוקים המדינתיים ויחייב סימון מתאים (כאשר החוקים המדינתיים שכבר מחייבים סימון הודעות מסחריות, עומדים למעשה בדרישות החוק הפדראלי).

⁹⁸ *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

⁹⁹ CDT, "Labeling Mandates In Anti-spam Legislation Threaten Free Speech", CDT (1.6.2001), http://www.cdt.org/publications/pp_7.04.shtml (ביקור אחרון 14.11.2004).

ב. האיחוד האירופאי

בשנת 2002 ניסחו המועצה האירופית והפרלמנט של האיחוד האירופי את הדירקטיבה האחרונה הנוגעת ל- "עיבוד מידע אישי והגנה על פרטיות".¹⁰⁰ בין היתר מתייחסת הדירקטיבה גם לנושא דואר הזבל ומנחה את המדינות החברות להסדיר בחקיקה עד סוף שנת 2003, הוראה אשר תאסור על חברות מסחריות להפיץ הצעות מסחריות בדואר אלקטרוני טרם קיבלו את אישור הנמען (מדיניות של Opt-In – הסכמה מראש):¹⁰¹

"13(3). Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2 (automatic calling machines, fax and email), are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation."

עו"ד חיים רביה מבהיר: "במקום מתן זכות לנמען לדרוש שלא לקבל יותר דואר זבל אלקטרוני (opt-out), נאסר לשלוח לכל אדם מסר אלקטרוני שלא התבקש מפורשות מראש (opt-in – מדיניות של מתן הסכמה מראש)".¹⁰²

הערכת הדירקטיבה האירופאית

א. הפתרון האירופאי מניח כהנחת המוצא שדואר מסחרי המתקבל ללא רשות מצד הנמען מפר את פרטיותו. האירופאים אינם מסתבכים בהגדרה אשר כוללת בתוכה את הסייגים, אלא מציעים נוסחה פרקטית יחסית, שלפיה הפרט הוא שיקבע מה רצוי לו (בניגוד להצעה של המועצה הישראלית לצרכנות, אשר לשיטתנו תוביל לכך שבית המשפט הוא שייאלץ להכריע ולגבש נוסחה אובייקטיבית אשר תקבע מה יעיל לנמען ומה לא).

¹⁰⁰ 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).

¹⁰¹ שם, בסעיף 13(3) לדירקטיבה.

¹⁰² חיים רביה, "רגולציה של תקשורת ואינטרנט מהיר באירופה", law.co.il (2.8.2000), במאמרו מתייחס עו"ד רביה לדירקטיבה 97/66/EC, שבוטלה עם כניסתה לתוקף של הדירקטיבה החדשה - 2002/58/EC. הערה: [14.11.2002] <http://law.co.il/showarticles.php?d=h&article=144>.

ב. על אף האמור גם הצעה זו אינה כה פרקטית, בהתחשב בעובדה שהאיחוד יכול לכפות רצונו רק על המדינות החברות בו, בעוד שדואר הזבל מגיע בחלקו הגדול מארצות הברית ומדינות נוספות.¹⁰³ מכאן שפיתרון אמיתי יושג רק על-ידי שיתוף פעולה בין האיחוד האירופאי לארצות הברית. יש לציין כי רבות הן המדינות בעולם אשר מעוניינות להסדיר את סוגיית דואר הזבל, ישנן כאלו אשר עדיין נמצאות בשלב ההצעות וישנן כאלו שכבר חוקקו חוקים בעניין.¹⁰⁴

ג. כללי האתיקה של הרשת

בשני פסקי דין שניתנו אחד באונטריו שבקנדה ואחד במדינת טנסי שבארצות הברית, ניתן תוקף מחייב לכללי האתיקה הבלתי כתובים של הרשת (Netiquette), הכוללים גם איסור על משלוח דואר אלקטרוני בלתי רצוי.

פסק הדין הראשון שניתן בעניין היה בבית המשפט העליון של מדינת טנסי בארצות הברית.¹⁰⁵ בפסק הדין אישר בית המשפט את השעייתם של שני עורכי דין, שפרסמו את שירותיהם, באמצעות שליחת דואר זבל לכתובות דואר אלקטרוני של קבוצות דיון (Usenet) באינטרנט. בית המשפט ייחד בפסק הדין פרק לעבירות האתיות של פרסומת בלתי מבוקשת באמצעות הדואר האלקטרוני. בית המשפט קבע כי הפרסום בדרך זו גרם נזק למוניטין של מקצוע עריכת הדין ולשיטה המשפטית כולה.

בפסק הדין שנידון בבית המשפט העליון של אונטריו שבקנדה,¹⁰⁶ נתן בית המשפט תוקף לכללי האתיקה של הרשת, וקבע כי שליחת דואר זבל מהווה הפרה של כללי הרשת, אלא אם כן הדבר הותר מפורשות בהסכם עם ספקית האינטרנט (דרכה עובד דואר הזבל). חשוב לשים לב, כי באותו מקרה התוקף ניתן מכוח הסכם מפורש בין הצדדים, ולא בטוח אפילו שאותו בית משפט היה נותן לכללי האתיקה של הרשת - תוקף מכוח עצמם.¹⁰⁷ למרות שיש חשיבות רבה לכללי האתיקה של הרשת, קשה להחיל אותם, בגלל שהם אינם מגובשים דיים, על מנת שיהיה ניתן לתת להם תוקף מחייב. כמו כן לא ברור האם בתי משפט אחרים, יבחרו ללכת בדרך זו של החלת כללי האתיקה של הרשת במקרים של שליחת דואר זבל.

¹⁰³ על-פי נתוני האתר Spamhaus (אתר המנהל מעקב מקיף ושוטף אחר מקורות דואר הזבל האלקטרוני ברחבי העולם), מארצות הברית נשלחת כמות דואר הזבל הגדולה ביותר. כאשר מקורות דואר הזבל העיקריים אחרי ארצות הברית (נכון ל-18.2.2004) הם: סין, דרום קוריאה, ברזיל, טייוואן, קנדה, ארגנטינה, רוסיה, איטליה ובריטניה. <http://www.spamhaus.org>

¹⁰⁴ ראו למשל באתר: <http://www.spamlaws.com>

¹⁰⁵ *In Re Laurence A. Canter*, Superme Court of Tennessee 95-831-O-H (1997)

¹⁰⁶ *Ontario, Inc. v. Nexx Online Inc.*, [1999] O.J. No. 2246 (Court file no. C20546/99)

¹⁰⁷ חיים רביה, "מתן תוקף משפטי לכללי ההתנהגות המקובלים באינטרנט", (8.8.1999) law.co.il, <http://law.co.il/showarticles.php?d=h&article=174>

5. דואר זבל כחול-לבן: המצב המשפטי

בפרק זה נבחן את המצב המשפטי בישראל בכל הנוגע להסדרה ציבורית של דואר זבל. נבחן את מעט החקיקה שניתן, אולי, להחיל בהקשר הנדון כאן, ואת פסק הדין היחיד שדן בשאלה, וגם כן בהיבט צר שלה. לאחר מכן נסקור ונעריך את הצעות החוק הפרטיות שהועלו בשנה האחרונה, כמו גם את הצעת משרד התקשורת. הפרק הבא יבחן מודלים משפטיים נוספים.

א. החקיקה הקיימת

אין בישראל חקיקה המתייחסת במפורש לדואר הזבל האלקטרוני. כאמור לעיל, דואר זבל נבדל מדיוור ישיר (המוסדר בחוק הגנת הפרטיות). אך לדעת עו"ד חיים רביה ניתן למצוא בסיס לאיסור משלוח דואר זבל אלקטרוני, בסעיף 30 לחוק התקשורת הקובע: "המשתמש במיתקן בזק באופן שיש בו כדי לפגוע, להפחיד, להטרוד, ליצור חרדה או להרגיז שלא כדין, דינו - מאסר שלוש שנים"¹⁰⁸.

בהגדרת "מתקן בזק" נכלל גם דואר אלקטרוני, מפני שלפי סעיף ההגדרות בחוק הנ"ל,¹⁰⁹ מתקן בזק הוא מתקן הנועד ל"העברה או קליטה של סימנים, אותות, כתב, צורות חזותיות, קולות או מידע, באמצעות תיל, אלחוט..." וגם דואר אלקטרוני עובר באמצעים אלו ומכאן שיש איסור לשלוח בדואר אלקטרוני על מנת להטרוד שלא כדין.¹¹⁰

פרשנות זו לא התקבלה על-ידי השופטת ברלינר, שקבעה בפרשת *בן יוסף ברוך* (בבית המשפט המחוזי בתל-אביב),¹¹¹ כי הכוונה באיסור הקיים בסעיף 30 לחוק התקשורת היא לשימוש פיזי טכני במתקן בזק "באופן שיש בו כדי לפגוע, להפחיד, להטרוד..." ולא לתוכן הדברים המועברים באמצעותו. לדעתה: "לא יתכן, לשיטתי, כי אותן מילים עצמן, שאמירתן אינן מהווה עבירה על-פי אף אחת מהעבירות המנויות בספר החוקים של מדינת ישראל, בין משום שמלכתחילה תוכן אינו אסור, ובין משום שהפרשנות, ושימת הדגש על עקרון חופש הביטוי היו מקטלגות אותן כמרגיזות וכו' – אך לא מהוות סיכון לשלום הציבור וביטחונו – יהפכו את המשמיע אותן לעבריין, רק משום שהשמיען באמצעות הטלפון (למשל) ולא בשיחה פנים אל פנים".¹¹² השופטת ברלינר הגיעה למסקנה זו, על-ידי בחינת לשון סעיף 30 ובחינת "סביבתו החקיקתית" של הסעיף, המתמקדות בפן הטכני של השימוש במתקני בזק, ולא בתכנים המועברים באמצעותם.¹¹³ עם זאת, כתבה השופטת כי: "מספר שיחות (או התקשרויות בכל מיתקן אחר לרבות אינטרנט), תדירותן, אורכן וכו', הן בבחינת נסיבות שתיבחנה ותילקחנה בחשבון בכל מקרה ומקרה לגופו, לעניין הקביעה האם

¹⁰⁸ סעיף 30 לחוק התקשורת (בזק ושידורים), התשמ"ב-1982, ס"ח 218.

¹⁰⁹ שם, בסעיף 1 לחוק.

¹¹⁰ חיים רביה, "דואר זבל", <http://law.co.il/showarticles.php?d=h&article=130>, (1.3.1999), law.co.il.

¹¹¹ ע"פ (ת"א) 70868/00 מדינת ישראל נ' ברוך, תק-מח (2)2002, 1269.

¹¹² שם, בעמ' 12 לפסק הדין.

היה בשימוש כדי להטריד, ליצור חרדה וכו'".¹¹⁴ כלומר, עדיין ייתכן כי לפי פרשנות זו דואר זבל אלקטרוני, הנשלח במספר עותקים רב יבוא תחת האיסור הקבוע בסעיף 30 לחוק התקשורת.

בנוסף סעיף 30 לחוק הנ"ל קובע איסור על משלוח דבר פרסומת באמצעות פקסימיליה:

" (א) המשגר דבר פרסומת באמצעות פקסימיליה, ללא קבלת הסכמה מראש ובכתב, של הנמען, דינו - קנס כקבוע בסעיף 61(א)4 לחוק העונשין התשל"ז-1977; פניה חד-פעמית מטעם משגר לנמען שהינו בית עסק, הכוללת הצעה להסכים לקבלת דברי פרסומת מטעמו, באמצעות פקסימיליה, לא תהיה עבירה לפי סעיף זה".

המחוקק הישראלי קבע כאן מודל של הסכמה מראש (opt-in) ביחס לפקס פרסומי, הואיל ומשלוח הפקס הפרסומי מנצל את משאבי המקבל (הנייר והדיו המשמשים להדפסת הפקס), מבלי שזה בכלל ביקש לקבל אותו. בדומה דואר הזבל האלקטרוני, מנצל את זמן החיבור לאינטרנט ואת משאבי העיבוד של הנמען (שיכלו להיות מנוצלים לתכלית אחרת, מאשר לקבל את הודעת הזבל). לכן לדעתנו, רצוי לפרש את הסעיף כך שהוא חל גם על דואר אלקטרוני.¹¹⁵

בנוסף סעיף 2(9) לחוק הגנת הפרטיות,¹¹⁶ קובע כי פגיעה בפרטיות היא גם: "שימוש בידעיה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה". לעניין זה, קבעה הפסיקה, כי ב"ענייניו הפרטיים של אדם" נכללים גם פרטים טריוויאליים, כמו הכתובת ומספר הטלפון של אותו אדם.¹¹⁷ מכאן טוען עו"ד רביה כי השימוש בכתובת הדואר האלקטרוני (שהיא מ"ענייניו הפרטיים של אדם") לצרכים מסחריים, ללא הסכמה במפורש לכך – אסורה.¹¹⁸

¹¹³ שם, בעמ' 4-5 לפסק הדין.

¹¹⁴ שם, בעמ' 17 לפסק הדין.

¹¹⁵ חיים רביה, "הסכמה מראש או ביטול בדיעבד", law.co.il (29.12.2002), <http://law.co.il/showarticles.php?d=h&article=193>.

¹¹⁶ סעיף 2(9) לחוק הגנת הפרטיות, התשמ"א-1981, ס"ח 128.

¹¹⁷ ע"א 439/88 מדינת ישראל נ' ונטורה משה, פ"ד מח(3) 808, בפסקה 7 לפסק דינו של השופט בך.

¹¹⁸ ראו לעיל, הערה 115. בנוסף לדעת עורך דין רביה, הודעת דואר זבל בעל נפח גדול, העלולה לחסום את תיבת הדואר האלקטרוני של הנמען, או לדרוש מהנמען להורידה למחשבו במשך זמן רב, יכולה להיחשב כמשבשת את פעולתו התקינה של מחשב, לפי סעיף 2 לחוק המחשבים,¹¹⁸ ועל כן, לדעתנו, אסור לשגרה על-פי הדין הישראלי.

ב. הפסיקה

הפסיקה היחידה בארץ המתייחסת לדואר זבל היא בעניין *אבן-חן נ' סוויסה*.¹¹⁹ זהו פסק דין של בית משפט לתביעות קטנות, ולכן אין לו כמובן ערך תקדימי כלשהו. באותו מקרה הנתבע הפעיל תוכנה אוטומטית למציאת כתובות דואר אלקטרוני בפורום שבאתרו של התובע (תוכנה זו נקראת "תוכנת קצירה"), שגרמה לקריסתו של האתר. השופט דניאל ארנסט קבע כי פעולת הנתבע עולה לכדי העוולה של הסגת גבול במיטלטלין.¹²⁰ בנוסף השופט קבע כי סימן ב' לחוק הגנת הפרטיות רלוונטי לענייננו, כי שם נקבע שדיוור ישיר הוא גם פניה לאדם בדרך ממוחשבת ובנוסף ביצע הנתבע עוולה אזרחית, לפי סעיף 4 לחוק, מפני שהוא פגע בפרטיותם של הגולשים ללא הסכמתם, על-ידי קצירת כתובותיהם.¹²¹ עם זאת חשוב לשים לב, כי פסק הדין דן לא בעצם שליחת דואר הזבל לנמענים, אלא בקצירת הכתובות וכמו כן לפסק דין זה אין ערך תקדימי, בהיותו פסק דין של בית משפט לתביעות קטנות.¹²²

ג. הצעות החוק

1. הצעת המועצה הישראלית לצרכנות

בשנת 2003 הציעה המועצה הישראלית לצרכנות הצעת חוק שעניינה דואר זבל.¹²³ הצעת החוק מתייחסת לדואר זבל בעל אופי מסחרי-פרסומי ותכליתה לאסור על חברות מסחריות להפיץ דואר אלקטרוני אשר לא קיבל את אישור הנמען. ההצעה מבקשת לשנות את חוק הגנת הפרטיות ולהוסיף בו סעיף אשר יקבע כי מפיץ דואר אלקטרוני בעל אוריינטציה פרסומית יהיה רשאי לשלוח דואר רק מכוח חוזה בינו לבין הנמען, על-פי חוק, או על-פי דרישתו של הנמען. בהצעה מופיע הסייג לפיו משווק דואר יהיה רשאי להפיצו ללא רשות מצד הנמען כאשר מדובר בדואר אשר הנמען מפיק ממנו תועלת ישירה.

יישומו של החוק (על-פי ההצעה) עתיד להיות מופקד בידיה של רשמת מאגרי המידע, אשר תנהל מאגר מידע בו ירשמו אנשים אשר מבקשים שלא יפנו אליהם (בסגנון רשימת Do Not Call Me המונהגת לגבי טלמרקטינג בארצות הברית).¹²⁴ ההצעה המבוססת על מודל אמריקני, קובעת כי משווק אשר מפיץ דואר אלקטרוני לכתובת הרשומה במאגר מסתכן בכך שיוטל עליו קנס כספי דרקוני. בישראל ההצעה קובעת כי העובר על החוק יועמד לדין וצפוי לשלושה חודשי מאסר, בנוסף יהיה זכאי נמען שהופרה פרטיותו מצד המשווק לפיצוי כספי.

¹¹⁹ עניין *אבן-חן*, לעיל הערה 30.

¹²⁰ בקביעה זו הסתמך השופט (בטעות) על הלכת פסק הדין האמריקני *Intel v. Hamidi*, שנהפכה כבר על-ידי ערכאת הערעור.

¹²¹ עניין *אבן-חן*, לעיל הערה 30, בסעיפים 17-21 לפסק דינו של השופט ארנסט.

¹²² עו"ד רביה, כותב כי לדעתו העוולה המצויה בסעיף 2(9) לחוק הגנת הפרטיות האוסרת על שימוש בפרטים אישיים שלא לתכלית שלשמה הם נמסרו, הייתה יותר מתאימה במקרה הנדון. ראו חיים רביה, "בעלי בקר וסכסוכי מחשב", *law.co.il* (29.9.2003), <http://law.co.il/showarticles.php?d=h&article=222>.

¹²³ הצעת המועצה הישראלית לצרכנות, לעיל הערה 2.

ההצעה אינה חפה מקשיים וספק אם תתמודד עם הבעיה באופן יעיל וזאת לנוכח הכשלים הבאים:

א. ההצעה אינה יכולה להתמודד עם מפיצים זרים מחוץ לארץ. אפשר להניח כי מפיצים ישראלים יוכלו לנצל פרצה זו בנקל ולעקוף את החוק על-ידי שימוש בשרתים אשר ממוקמים מחוץ לתחום השיפוט הישראלי. כדי להתמודד עם בעיה זו, המועצה הישראלית לצרכנות, מתכוונת לתקן את נוסח ההצעה שלה, כך שיהיה ניתן לתפוס בחוק, גם את מי שדואר הזבל, **הגיע מטעמו**, ולא רק את מי ששלח בפועל את דבר דואר הזבל (כך שיהיה ניתן לתפוס מפרסמים ישראלים, ששולחים דואר זבל באמצעות שרתים הנמצאים מחוץ לישראל).

ב. ההגדרה של המועצה הישראלית לצרכנות, לוקה בחסר מפני שהיא מותירה כר נרחב לפרשנות ושיקול דעת בידי של המפרסם להחליט בעצמו האם יש בדואר שלו משום "תועלת ישירה לנמען". הקושי הנובע מכך הוא, שלא ברור מהו דואר אשר ייכלל בתחום ההגדרה הנ"ל. דוגמא אשר ניתנת בהקשר זה על-ידי המבקרים את הצעת החוק היא, האם דואר הקורא לגולשים להחרים מוצר מסוים הינו בחזקת דואר זבל, או דואר לגיטימי אשר הצרכן עשוי להפיק ממנו תועלת.¹²⁵ פתרון אפשרי לקושי העולה מן ההצעה של המועצה, הוא להשמיט את הסייג המתיר משלוח דואר אשר הנמען עשוי להפיק ממנו תועלת ישירה. בכך יימנע המחוקק מלנקוט גישה פטרנליסטית, שכן חזקה על אדם שהוא יודע מה מועיל לו. אם יבחר נמען להרשות תכתובת מצד משווק או כל גוף אחר שמורה לו הזכות לעשות זאת.

ג. שאלה נוספת העולה מההצעה, נוגעת לשאלה האם דואר זבל נתפש כתופעה אשר מפרה פרטיות? מחד גיסא הצעת החוק קושרת את דואר הזבל באופן טכני עם הפרת הפרטיות בכך שההצעה מבקשת להוסיף את ההגבלות על דואר הזבל דווקא כסעיף בחוק הגנת הפרטיות, אולם מאידך גיסא אם ננתח את ההגדרה שנתנו המציעים לדואר זבל, קרי "כל מה שאינו מביא תועלת ישירה לנמען", הרי שנגיע למסקנה כי אין בין דואר זבל לפרטיות דבר וחצי דבר, זאת משום שאין כל יסוד להניח כי מה שאינו מועיל בהכרח מפר פרטיות וההיפך. לשיטתנו אם השיקול התועלתני הוא השיקול העיקרי העומד לנגד עיניו של המחוקק הרי שאין לייחסו באופן ישיר לפרטיות.

¹²⁴ אתר The National Do Not Call Registry האמריקני: <https://www.donotcall.gov>

¹²⁵ גל מור, "המועצה לצרכנות מציעה: חוק נגד דואר זבל", *ynet* (5.11.2003), <http://www.ynet.co.il/articles/0,7340,L-2812715,00.html>

2. הצעת החוק של חבר הכנסת רומן ברונפמן

ביום 8.7.2004 הגיש חבר הכנסת רומן ברונפמן הצעה לתיקון חוק הגנת הפרטיות,¹²⁶ שגובשה יחד עם המועצה הישראלית לצרכנות, לפיה רשם מאגרי המידע ינהל "פנקס למניעת פניות בלתי מוזמנות". לפי הצעת החוק, ייאסר על מפרסמים לשלוח פניות בלתי מוזמנות לאדם שנרשם בפנקס הנ"ל. העובר על האיסור הזה יהיה חייב לפצות את הנפגע בפיצוי בסך עשירית הקנס הקבוע בסעיף 61(א)(1) לחוק העונשין.¹²⁷

המודל המוצע בהצעתו של ח"כ ברונפמן הוא מודל מסוג Opt-out, בו אדם בוחר האם לא לקבל את הפניות הבלתי מוזמנות. כאשר כל עוד אדם מסוים לא נרשם בפנקס למניעת פניות בלתי מוזמנות, ניתן יהיה לפנות אליו בפניות כאלו מבלי לעבור על התיקון לחוק המוצע. ח"כ ברונפמן מנמק בדברי ההסבר להצעת החוק, את הסיבה לבחירה במודל זה, בחשש לפגיעה בחופש הביטוי ובחופש העיסוק. לדעתו, מודל זה מהווה איזון בין הזכויות החוקתיות של המפרסמים לחופש הביטוי וחופש העיסוק לבין זכותו של אדם לבחור האם לקבל פניות אלו.

הצעת החוק מונה שני חריגים, לפיהם גם כאשר דוא"ל נשלח ללא הסכמה מראש, אין בכך הפרה של החוק המוצע: א. מידע אותו ביקש הנמען לקבל או מידע שהוא זכאי לקבל מכוח חוק או חוזה. ב. פניה שאינה פרסומת שמטרתה מסירת מוצר או שירות.

בעוד קביעת החריג הראשון היא נכונה ורצויה, קביעת החריג השני מכשירה למעשה דואר זבל המעביר מסרים פוליטיים, דתיים, בקשות לתרומות וכדומה, שכן הם אינם פניות למטרת מסירת מוצר או שירות.

בנוסף קיים חשש כי הקמת "פנקס למניעת פניות בלתי מוזמנות", תיתן למעשה לשולחי דואר הזבל רשימה של כתובות דואר אלקטרוני פעילות אליהן ניתן לשלוח דואר זבל. חשש זה נכון במיוחד לשולחי דואר זבל הפועלים מחוץ לתחום השיפוט של מדינת ישראל.

כמו כן, ההצעה אינה קובעת איסור כלשהו על זיוף או הסתרת מקור המסר, בעוד שולחי דואר זבל רבים מזייפים את הכתובת ממנה נשלחת ההודעה, דבר המקשה על איתורם ודבר הגורם להטעיית מקבלי דואר הזבל.

בנוסף, לא ברור האם הגדרת "פונה" לפי הצעת החוק, מתכוונת למי ששלח בפועל את הפרסום, או למי שמטעמו נשלח הפרסום, אף אם אינו שולח את הפרסום בפועל (אלא באמצעות קבלן משנה). לשון הצעת החוק, תשאיר את הדבר לפרשנותם של בתי המשפט, במקום לקבוע מפורשות כי גם השולח בפועל וגם מי שהפרסום הגיע מטעמו יהיו כפופים לאיסורים המוצעים בהצעת החוק. חשוב לציין כי הצעת חוק זו מתייחסת לכל פניה בלתי מוזמנת בדרך התקשרות כלשהי בבזק, ולא דווקא באמצעות דואר אלקטרוני.

¹²⁶ הצעת חוק הגנת הפרטיות (תיקון - מניעת פניות בלתי מוזמנות), התשס"ד-2004, פ/2757.

כאמור, הצעה זו היא בשיתוף עם המועצה הישראלית לצרכנות, וכנראה מחליפה את ההצעה שהציגה המועצה בשנת 2003.

3. תזכיר משרד התקשורת לתיקון מס' 31 לחוק התקשורת

משרד התקשורת פרסם תזכיר חוק, בו מוצע תיקון לסעיף 30א לחוק התקשורת (בזק ושידורים).¹²⁸ לפי ההצעה בתזכיר החוק, סעיף 30א לחוק התקשורת הקובע כיום איסור על משלוח דבר פרסומת באמצעות פקסימיליה ללא הסכמה מראש בכתב, יורחב כך שיכלול גם איסורים על משלוח דבר פרסומת באמצעות מערכת חיוג אוטומטית, דואר אלקטרוני והודעות מסר קצר (SMS) ללא הסכמה מפורשת מראש של הנמען (כלומר מוצע כאן מודל מסוג opt-in). לצד איסור זה נקבע סייג המאפשר פניה חד-פעמית מצד המפרסם – בה מציע המפרסם לנמען להסכים לקבלת דברי פרסומת מטעמו, המופצות באמצעות אמצעים אלו.

בנוסף, סעיף (א1) להצעה בתזכיר החוק מאפשר למשגר לשלוח דבר פרסומת, אף ללא קבלת הסכמתו של הנמען, כאשר קיימת התקשורת קודמת בין משגר ההודעה לנמען וכאשר מתקיימים התנאים המצטברים הבאים:

- (1) הנמען מסר את פרטיו למשגר ההודעה במהלך רכישה של מוצר או שירות, או במהלך משא ומתן לרכישה כאמור;
- (2) ניתנה לנמען הזדמנות להודיע כי הוא מסרב לקבל הודעות כאמור, דרך כלל או מסוג מסוים, והוא לא עשה כן;
- (3) דבר הפרסומת מתייחס למוצר או לשירות מסוג דומה למוצר או לשירות כאמור בפסקה (1).

כמו-כן, ההצעה קובעת חובה על המשגר דבר פרסומת (בסעיף א2 להצעה), המותר לפי ההצעה, לכלול בהודעה באופן בולט וברור את הפרטים הבאים:

- א. כי מדובר בדבר פרסומת.
- ב. שמו של משגר ההודעה, כתובתו ודרכי יצירת הקשר עימו.
- ג. הודעה כי הנמען רשאי להודיע למשגר על סירובו לקבל הודעות נוספות מהמשגר ללא תשלום (מלבד התשלום הכרוך במשלוח ההודעה).
- ד. אם מדובר בהודעת דואר אלקטרוני – חובה לציין: I. כתובת תקפה של משגר ההודעה, אליה ניתן יהיה לשלוח הודעת סירוב. II. פירוט בדבר אופן שליחת הודעת הסירוב. כלומר ניתן לראות כאן התייחסות לבעיית זיוף כתובת השולח, הנפוצה בשליחת דואר זבל. עם זאת, ההצעה אינה כוללת במפורש איסור על זיוף כתובת השולח, אלא רק חובה לכלול כתובת תקפה בגוף ההודעה. כמו כן אין ההצעה אינה אוסרת על שימוש בכותרות מטעות להודעות דואר אלקטרוני.

¹²⁷ נכון לכתובת שורות אלו – גובה הקנס יהיה 1,290 ₪ (לפי התיקון האחרון לסעיף 61 לחוק העונשין משנת תשס"ג).

¹²⁸ ראו לעיל, הערה 108, בסעיף 30א לחוק.

ההצעה קובעת כי עבירה על סעיף זה היא **הטרדה** לפי סעיף 2(1) לחוק הגנת הפרטיות, דבר המאפשר לנמען לתבוע פיצויים ללא הוכחת נזק בהליך אזרחי, כאשר הוא קיבל הודעת פרסומת בניגוד לחוק המוצע. בנוסף ההצעה קובעת שהפרת הוראות הסעיף תהווה עבירה פלילית שדינה קנס:

- א. מי שעובר על הכתוב בסעיף (א), כלומר שולח דבר פרסומת שלא נופל בגדר החרג הקבוע בסעיף (א1) ואינו רק פניה חד פעמית המציעה לקבל הודעות מטעם המפרסם, יהיה צפוי לקנס כקבוע בסעיף 61(א)(4) לחוק העונשין.¹²⁹
- ב. מי שיעבור על הכתוב בסעיף (א1) או (א2) להצעת החוק, יהיה צפוי לקנס כקבוע בסעיף 61(א)(3) לחוק העונשין.¹³⁰

דברי ההסבר צוין כי בכוונת משרד התקשורת להמליץ על קביעת העבירה הפלילית כעבירה מנהלית, שאכיפתה תימסר למערך האכיפה במשרד התעשייה המסחר והתעסוקה ולא לידי המשטרה. על מנת להפוך את העבירה לעבירה מנהלית שבגינה יהיה ניתן להטיל קנס מינהלי, על שר המשפטים יהיה להתקין תקנות לפי חוק עבירות מנהליות.¹³¹

הצעת זו אינה צפויה לפתור את בעיית דואר הזבל הנשלח מחוץ לתחום השיפוט של מדינת ישראל. אבל, הגדרת המונח "משגר" בהצעה, מאפשר לתפוס תחת האיסור, לא רק את מי ששלח בפועל את ההודעה (שעשוי להימצא מחוץ לישראל), אלא גם את מי שמטעמו נשלח הפרסום:

"משגר" – לרבות מי ששמו או מענו מופיעים בדבר הפרסומת כמען להתקשרות לשם רכישתו של נשוא דבר הפרסומת או מי שתכנו של דבר הפרסום עשוי לפרסם את עסקיו או לקדם את מטרותיו, זולת אם הוכיח כי נקט בכל האמצעים הסבירים כדי למנוע את שיגור דבר הפרסומת וכי דבר הפרסומת שוגר שלא בידיעתו; לעניין זה, לא יראו כמשגר את מי שביצע את הפעולה כשירות בזק לפי רשיון כללי או מיוחד שניתן לפי חוק זה;

כך, שבמקרה בו הודעת הדואר האלקטרוני האסורה על פי החוק המוצע, נשלחת משרת בחו"ל, אך מטעם מפרסם ישראלי, ניתן יהיה לחייב את המפרסם הישראלי שמטעמו נשלח דבר הפרסום.

הצעת חוק זו אף שאינה נטולת בעיות, יוצרת למעשה מנגנון opt-in, המחייב בהיעדר התקשרות קודמת, הסכמה מראש לשליחת ההודעות – שהוא לדעתנו המנגנון הרצוי לטיפול בבעיית דואר הזבל האלקטרוני.

¹²⁹ גובה הקנס נכון ליום כתיבת שורות אלו הוא 202,000 ₪, על פי התיקון לסעיף משנת תשס"ג.

¹³⁰ גובה הקנס נכון ליום כתיבת שורות אלו הוא 67,300 ₪, על פי התיקון לסעיף משנת תשס"ג.

¹³¹ חוק העבירות המינהליות, התשמ"ו-1985, ס"ח 31.

6. הסדרה ציבורית: פתרונות משפטיים אפשריים

בפרק זה נבחן פתרונות משפטיים אפשריים לבעיית דואר הזבל. הפתרונות נעים בין שיתוף פעולה בינלאומי, להטלת חובת תיוג – המתירה את משלוח הדואר, אך בתנאים. בעיקר נתמקד בשני המודלים המרכזיים: opt in ו opt out.

א. שיתוף פעולה בין לאומי

חברת הייעוץ גרטנר סוברת כי פתרון בעיית דואר הזבל, מחייב שיתוף פעולה בינלאומי, המשלב יוזמות ציבוריות ומסחריות.¹³² פתרון בינלאומי אפשרי הוא יצירת אמנה בינלאומית (במסגרת האו"ם או ה-WTO) שתפעל לצמצום התופעה. הבעיה עם פתרון זה, היא שיצירת אמנות אורכת זמן רב, שבזמן הזה עלולה להיפגע יכולת השימוש שלנו בדואר אלקטרוני לבלי הכר.

ב. חובת תיוג דואר זבל פרסומי

יש הטוענים כי ניתן לפתור את הבעיה על-ידי הטלת חובה לסמן דואר זבל פרסומי בצורה ברורה, למשל באותיות "ADV" (קיצור של advertisement) לפני כותרת ההודעה. תיוג כזה אמנם יקל עלינו בזיהוי וסינון דואר הזבל, אך אנו מעוניינים להפסיק לחלוטין את דואר הזבל ולא רק להקל את זיהויו. עדיין הקלות בזיהוי דואר הזבל לא מונעת את רוחב הפס הנצרך בהעברתו, עד שהוא מגיע לתוכנת הסינון. הצעה זו כלל אינה מבטיחה שדואר הזבל יפסק או אפילו יפחת. למשל במדינת קליפורניה, שבה נחקק עוד ב-1998 חוק המחייב סימון דואר זבל בתג "ADV", עדיין האזרחים מוצפים בדואר זבל ולא נראה כי שיטת התיוג עזרה כלל בפתרון הבעיה.

ג. ביטול בדיעבד (Opt Out)

פתרון המוצע (בעיקר בארצות הברית), שאף יושם במספר מדינות בארצות הברית, הוא לחייב את מפיצי דואר הזבל במתן אפשרות ליציאה מרשימת הדיוור שלהם (Opt-Out). אך ישנן בעיות רבות עם פתרון זה:

א. אפילו אם נסיר את עצמנו מרשימת דיוור של שולח ספאמר אחד, ישנם עוד אלפים כמוהו, שימשיכו לשלוח לנו דואר זבל ובלתי אפשרי להוציא את עצמנו מרשימות הדיוור של כל שולח דואר זבל בעולם.

ב. גם אם נבחר להסיר את עצמנו מרשימת הדיוור – הדבר עדיין לא מבטיח כי הספאמר יענה לבקשתנו, הואיל והדבר מנוגד לאינטרס שלו, שהוא שיותר אנשים יקראו את דואר הזבל. לא רק זאת, אלא כשאנו בוחרים להוריד את עצמנו מרשימת הדיוור, בדרך כלל נשלחת הודעה לשרת הדואר של הספאמר, שמאחורי כתובת הדואר שלנו, נמצא אדם אמיתי, שמקבל ואף קורא את הדואר – ועכשיו ניתן לשלוח אליו דואר זבל ביתר שאת.

¹³² ynet, "גרטנר: חקיקה נגד דואר זבל לא תפסיק את התופעה", ynet (26.5.2003), <http://www.ynet.co.il/articles/0,7340,L-2635374,00.html>

ג. מדוע עלי לבקש שיסירו אותי מרשימת דיוור שאף פעם לא ביקשתי להצטרף אליה? אני מעולם לא ביקשתי לקבל את הדואר, אז מדוע שאדרש להסיר את עצמי מכל רשימת דיוור שהוסיפה אותי בלי לשאול אותי.

ד. רוב דואר הזבל הנשלח, מסתיר את מקורו וכולל כתובת דואר אלקטרוני פיקטיבית לתגובות, כך ששליחת בקשה ליציאה מאותה רשימת דיוור, לרוב לא תגיע לשום מקום.

רשימות Opt-Out גלובליות

שכלול של רעיון ה-Opt-Out מצוי גם בחוק האמריקני החדש (CAN-SPAM) כנגד דואר זבל וגם בהצעה לחקיקה שהגישה המועצה הישראלית לצרכנות לוועדת המשנה לענייני אינטרנט של הכנסת. רעיון זה אומר ליצור רשימות Opt-Out גלובליות – שיכללו מאגר נתונים בו אנשים יוכלו לצאת בפעם אחת, מכל רשימות הדיוור של הספאמרים. במבט ראשון זה נראה רעיון טוב, אך הוא אינו עונה על השאלה מדובר מראש קיבלתי דואר זבל מבלי שנתתי את הסכמתי לכך. בנוסף אין דרך לגרום לכל ספאמר בעולם לכבד רשימה. כמו כן, יש הטוענים כי יצירת רשימות כאלו נותנות לגיטימציה מסוימת לספאמרים לפעול, על-ידי כך שהתופעה השלילית של שליחת דואר זבל – אינה נאסרת.¹³³

פתרונות מסוג זה, אינם חדשים כלל ועוד בשנת 1998 היה ניסיון של גופים פרטיים (יוזמת SAFEeps), ליצור מאגר דומה, של כתובות דואר אלקטרוני של אנשים שאינם מעוניינים לקבל ספאם.¹³⁴ ניסיון זה, על אף שיצא לפועל נכשל משתי סיבות: א. היה צורך לבצע פעולה אקטיבית של רישום למאגר עבור כל כתובת דואר אלקטרוני, דבר שגרם לכך שאנשים התעצלו לרשום את עצמם למאגר. ב. רוב הספאמרים לא כיבדו את רצונם של מי שנרשמו במאגר, על אף שארגון המשווקים באמצעות דיוור ישיר האמריקני, היה ממקימי המיזם.¹³⁵

ד. מתן הסכמה מראש (Opt-In)

גישה זו אומרת שלא ניתן לשלוח דואר זבל, ללא הסכמה מראש של הנמען (Opt-In). גישה זו היא הגישה הקיימת בהצעת הדירקטיבה האירופאית (לעיל). גישה זו קיימת גם בישראל ובמדינות רבות בעולם בנוגע לשליחת פקס-פרסומי ויש הטוענים שיש להרחיבה כך שתחול גם על דואר זבל פרסומי. מצדדי הגישה הזו, טוענים כי כשם שפקס פרסומי מנצל את משאביו של המקבל (נייר ודיו הדרושים להדפסת הפקס), כך גם דואר זבל אלקטרוני, מנצל את משאביו של המקבל (זמן חיבור לאינטרנט ומשאבי עיבוד) ועל כן יש מקום לחקיקה דומה.

¹³³ חיים רביה, "זבל אלקטרוני? לא בתיבת הדואר שלי", law.co.il (4.4.2001), <http://law.co.il/showarticles.php?d=h&article=129>

¹³⁴ Chris Oakes, "SAFEeps from Spam at Last?", *Wired* (9.10.1998), <http://www.wired.com/news/technology/0,1282,15511,00.html>

בארצות הברית אף ניתנו פסקי דין¹³⁶ שקבעו כי החקיקה נגד הפקס הפרסומי היא הגבלה סבירה על חופש הביטוי בנסיבות העניין, ועל כן חקיקה זו אינה עומדת בניגוד לחוקה האמריקנית. סביר להניח שחקיקה דומה בעניין דואר זבל פרסומי תזכה לאישור דומה מצד בתי המשפט.

אנו סבורים שפתרון זה הוא אף הפתרון המשפטי הראוי לבעיית דואר הזבל האלקטרוני. אמנם גם פיתרון זה אינו חף מבעיות, כמו אי התחולה על ספאמרים מחוץ לגבולות המדינה (חשוב לזכור כי הבעיה הטריטוריאלית קיימת בכל דבר חקיקה). אבל הוא לפחות אינו נותן לגיטימציה למשלוח דואר שאנו לא מעוניינים ולא מבקשים לקבלו.

אם פתרון זה יאומץ ברמה העולמית, אז הוא אולי יביא לסיום "המכה" העולמית של דואר הזבל.

אם לא ננקוט אמצעי זה, דואר הזבל עלול להרוס את היעילות והשימושיות של הדואר האלקטרוני ככלי תקשורת.

שילוב פתרונות טכנולוגיים

קיימים מספר פתרונות טכנולוגיים בשוק המאפשרים קיום פרסומות במסגרת שימוש בדואר אלקטרוני במנגנון של Opt-in.

חברת Deliverent.com פיתחה מנגנון במסגרתו מפרסמים מקימים פרסומות ודפי web חיים מסוגים שונים.¹³⁷ המערכת משתמשת ברשימת כתובות דואר אלקטרוני (CAN SPAM compliant opt-in email marketing and viral marketing service) של משתמשים שביצעו תהליך Opt-in לשרות. במסגרת הפתרון של חברת Deliverent.com מגיעות הפרסומות אל המשתמשים, במקום המצב הקיים כיום בו המפרסמים צריכים להביא את המשתמשים אל דפי הפרסומות או התארים שלהם.

סוג נוסף של פתרונות הקיימים בשוק אינו מחייב פיתוח טכנולוגיה ייחודית כמו בפתרון הקודם. במסגרת פתרון זה קיים ממשק אינטרנט רגיל ובסיס נתונים המקשר כתובות דואר של משתמשים לנושאים בהם מביעים המשתמשים עניין. המשתמשים ימשיכו לקבל דואר פרסומות בדיוק באותה המתכונת הקיימת כיום, אלא שהדואר אותו הם מקבלים יהיה ממוקד לפי הנושאים בהם הביעו עניין בלבד. פתרון כזה לדוגמא מפעילה חברת internet.com. החברה מפעילה שרות Opt-in לגולשים באינטרנט. גולש נכנס לדף של החברה, ובו רשימה גדולה של נושאים, בחלוקה לקטגוריות שונות. הנושאים אינם מסומנים מראש. הגולש בוחר את נושאי העניין שלו – המשתמש מעוניין לקבל דברי דואר ופרסומות בנושאים אלה. לאחר מכן המשתמש ממלא טופס ובו פרטיו – כתובת דואר אלקטרוני, מדינה, והפורמט בו הוא מעוניין לקבל את הדואר. לאחר שליחת הטופס המשתמש רשום לשרות, ויקבל דואר פרסומות ממוקד לפי דרישתו.

¹³⁵ Jim Sterne and Anthony Priore, *Email Marketing*, 45-46 (Wiley, New York, 2000)

¹³⁶ כמו פסק הדין הבא: *Destination Ventures, Ltd. v. FCC*, 46 F.3d 54 (9th Cir. 1995)

7. סיכום והמלצות

1. יש להבחין בין בעיית דואר הזבל לבין נושא הגנת הפרטיות. דואר הזבל עצמו אינו פוגע בפרטיות במישרין, הגם שהוא מטריד מאוד. עם זאת, ייתכן שהדרך בה הושגו כתובות הדואר האלקטרוני כללה פגיעה בפרטיות.
2. עיקר הפגיעה שיש בדואר זבל הוא במטרד לגולשים, בגזילת תשומת הלב שלהם, בהכבדה על משאבי ספקיות הגישה לאינטרנט, ובמקרים קיצוניים יש חשש לקריסה כוללת של מערכות דואר אלקטרוני.
3. אנו סבורים שהפתרון לבעיית דואר הזבל מצויה בשילוב של מספר גורמים ואפיקי הסדרה: הסדרה ציבורית בדמות חקיקה (ראו להלן); הסדרה פרטית בדמות אכיפה של ספקי השירות וגורמי ביניים אחרים במערכות הדואר האלקטרוניות, והסדרה טכנולוגית שיכולה להיות מופעלת הן ברמת המשתמש והן ברמת הרשת.
4. מודל ה-Opt-out שהונהג בארצות הברית עדיין לא הצליח לעצור את שטף הספאם. להיפך, נראה כי משנכנס החוק לתוקף גדל היקף הספאם בארצות הברית ובעולם.¹³⁸ דו"ח חדש שהוכן על-ידי OECD עבור הארגון האירופאי לשיתוף פעולה כלכלי ופיתוח, קבע כי דואר זבל אלקטרוני, הוא דבר מסוכן ויקר עבור עסקים ואנשים פרטיים. כמו כן הדו"ח קבע כי דואר הזבל האלקטרוני גורם לירידת אמון המשתמשים בסביבת התקשורת המקוונת ובמסחר האלקטרוני.¹³⁹
5. נראה כי אף המודל האירופאי שיישמו החל בכמה מדינות (שאר מדינות האיחוד עדיין בהליכי חקיקה), לא הצליח להוריד את היקף הספאם. אמנם מוקדם מדי לקבוע כי המודל נכשל, אך נראה כי הבעיה העיקרית במודל האירופאי היא, שהוא מתייחס לבעיית דואר הזבל כבעיה אירופאית בלבד ולא לכך שמדובר בבעיה בינלאומית. לכן נראה, כי יישום המודל המוצע בדירקטיבה האירופאית, חייב להיות מלווה באסטרטגיה בינלאומית משותפת, שתוכל להתמודד עם בעיית הספאם, החוצה גבולות.¹⁴⁰
6. המודל אותו אנו ממליצים לאמץ בישראל הוא מודל ה-Opt-In באמצעות חקיקה, בדומה למודל האירופאי. מודל זה הוא לא רק המודל הנכון להפחתת כמות דואר הזבל האלקטרוני, אלא הוא גם המודל הנכון עבור כל מי שמעוניין לפרסם באמצעות דואר אלקטרוני. פרסום בהסכמה מראש,¹⁴¹ יועיל למפרסם, בכך שרק

¹³⁷ אתר החברה: <http://www.deliverent.com> (ביקור אחרון 14.1.2004).

¹³⁸ Lance Ulanoff, "Spam: A Reality Check", *PC Magazine* (18.2.2004), <http://www.pcmag.com/article2/0,4149,1529243,00.asp>

¹³⁹ OECD, *Background Paper for The OECD Workshop on Spam* (OECD, Paris France, 2004), 4-5.

¹⁴⁰ שם, בע' 31.

¹⁴¹ בדומה למודל הפרסום של חברת Dotomi, שבו הגולש רואה רק פרסומות (באתרים העובדים בשיתוף פעולה עם Dotomi) מטעם מפרסמים שהוא בחר לקבל מהם פרסומות. למידע נוסף על המודל של חברת <http://www.dotomi.com/new/directmessaging/index.html>: Dotomi

מי שבאמת רוצה לשמוע את המסר שלו, אכן ישמע אותו, דבר שעשוי להעלות את מידת האפקטיביות של הפרסום.¹⁴²

7. כמו כן, יש להבטיח "אפשרות יציאה" מהמאגר, כך שמי שבחר באופן מודע לקבל פרסום מטעם מפרסם מסוים, יוכל לבחור גם להפסיק לקבל את הפרסום.
8. כדי שהחקיקה המוצעת תהיה אפקטיבית, יש להבטיח שהיא תחול לא רק על מפרסמים מהארץ אלא גם דואר זבל הנשלח מחו"ל מטעם מפרסמים ישראליים. יש אולי מקום לפעול בדומה לחוק הקליפורני, כך שהחוק יוחל על כל דואר המיועד לנמענים בישראל ולא משנה מה מקורו. אך הדבר עשוי להעלות מספר בעיות הנוגעות לסמכות שיפוט בינלאומית, ולעורר קשיי אכיפה.
9. שינוי עתידי של הארכיטקטורה של רשת האינטרנט עשוי להפחית במידה משמעותית את היקף דואר הזבל, ולהעלות את עלויות המשלוח של הספאמר, כך שלא יהיה כדאי לכללית לשלוח ספאם. אך יש להיזהר ביישום פתרונות אלו, כך שהם לא יפגעו בשירותי רשת קיימים, כמו Email Forwarding, וכן לא יחשפו יותר מדי את תעבורת הדואר האלקטרוני למעקב אפקטיבי, הואיל ומשיישומו הפתרונות הללו, ניתן יהיה לאמת את מקורו של כמעט כל דואר אלקטרוני שנשלח.
10. לאחרונה החל שיווקן של תוכנות סינון אפקטיביות במיוחד, שמונעות מדואר הזבל מלהגיע למשתמש, כמו תוכנת הסינון המשולבת ב-Microsoft Outlook 2003.¹⁴³ למרות שתוכנות אלו מונעות כמעט לחלוטין את הטרדה הנגרמת למשתמש מדואר זבל אלקטרוני, אין הן מונעות את רוחב הפס הכרוך בהעברת דואר הזבל, עד שהוא הגיע אל תוכנת הסינון.
11. תוכנת הסינון של Commtouch, ASAP, מצליחה למנוע לא רק את הגעת דואר הזבל לנמענים, אלא גם את רוחב הפס שהיה כרוך בהעברת הדואר. הבעיה היא שחשכון זה של רוחב הפס ומשאבי העיבוד, נעשה רק עבור שרתים המנויים לשירות של Commtouch, ולא לכלל השרתים דרכם עשוי להיות מועבר הדואר.
12. יישום מדיניות של Opt-In תוך שימוש בתוכנות סינון גם בצד השרת וגם בצד הלקוח, תוך שיתוף פעולה בינלאומי, עשוי בסופו של דבר להוריד את היקף דואר הזבל באופן ניכר, ואז אולי עשוי להתגשם חזונו של ביל גייטס על "עולם ללא ספאם".¹⁴⁴

¹⁴² Sterne & Priore, לעיל הערה 135, בע' 57-58.

¹⁴³ David Coursey, "Outlook 2003 fights the spam battle", ZDNet UK (22.10.2003), <http://comment.zdnet.co.uk/davidcoursey/0,39020667,39117284,00.htm>

¹⁴⁴ אי. פי., "ביל גייטס: דואר הזבל יעלם עד 2006", ynet (25.1.2004), <http://www.ynet.co.il/articles/0,7340,L-2864549,00.html>