© חוקים ב 2010, 51-131

חשיפת גולשים אנונימיים ברשת

מיכאל בירנהק*

מה צריך להיות הכלל המשפטי בנוגע לחשיפת גולשים אנונימיים ברשת האינטרנט? מתי על בית משפט להורות לספקי שירות לחשוף את זהותו של גולש אנונימי? מאמר זה עוסק בשאלות אלה. הדיון מתנהל בשלוש מסגרות: הראשונה מבקשת לאתר את הבסיס הנורמטיבי והמשפטי של האנונימיות. אטען כי האנונימיות היא זכות הראויה להגנה כנגזרת של חופש הביטוי ושל הזכות החוקתית לפרטיות גם יחד; המסגרת השנייה עניינה חופש הביטוי בסביבה המקוונת. אטען כי זהו עיקרון מרכזי שצריך להנחות את העוסקים בעיצוב המשפט לסביבה זו. רשת האינטרנט מציעה זירת שיח ייחודית ויש לאתר מראש את ההשפעות האפשריות של כלל משפטי כזה או אחר על אפשרויות הביטוי והשיח בזירה זו; המסגרת השלישית עניינה עיצוב מדיניות לסביבה המקוונת בכלל והסוגיה של חשיפת גולשים היא מקרה מבחן שלה. בכך המאמר מבקש להמחיש את גורל האנונימיות בסביבה דינמית של טכנולוגיית מידע. המשפט, הטכנולוגיה, הנורמות החברתיות המתעצבות לנגד עינינו וגורמים נוספים כמו כוחות השוק פועלים פה בערבוביה ובאינטנסיביות רבה.

אציג את ההסדר שהוצע בהצעת חוק מסחר אלקטרוני, את הגישות השונות שנדונו בפסיקה ובכלל זה בפסק הדין האחרון של בית המשפט העליון בסוגיה, ואת מערך הזכויות והאינטרסים שעל הפרק. אטען כי נוסף על הנפגע המבקש את חשיפת הזהות ונוסף על הפוגע האנונימי יש לתת את הדעת לתפקידם של ספקי השירות. בצד זה אציג טכנולוגיות שונות שמציעות פתרונות ואסכם בהצעת מודל שבו ספק השירות משמש מתווך ראשון בין הצדדים ובית המשפט – מתווך שני במידת הצורך.

---

* מרצה בכיר, הפקולטה למשפטים, אוניברסיטת תל־אביב. תודה לאלעד אורג, לטל ז׳רסקי, לאבנר פינצ׳וק, לבני פנקס ולאיסי רוזן־צבי על הערות מועילות, וללירון דר, לגיא לוטם ולמורן קליינפלד על עזרה במחקר. אני מבקש להודות לאיגוד האינטרנט הישראלי על תמיכתו הנדיבה במימון של מחקר זה ולמערכת **חוקים** על הערותיה המצוינות. האחריות לתוכן היא שלי בלבד.

א. הקדמה

תגובה אנונימית לכתבה שמתפרסמת באתר אינטרנט פופולרי משמיצה אדם מזוהה. הנפגע טוען שהתוכן משפיל ומבזה אותו או שהוא שקרי ומבקש לתבוע בתביעת לשון הרע – אולם אינו יודע את מי לתבוע, שכן התגובה האנונימית אינה כוללת את שם הכותב אלא מסתפקת בכינוי שאינו מזהה. אתר האינטרנט שאליו הנפגע פונה בבקשת עזרה באיתור הגולש משיב את פניו ריקם. האם המשפט צריך לסייע לנפגע לאתר את הפוגע ולהורות – לאתר האינטרנט תחילה ולספק שירותי הגישה לאינטרנט בהמשך – לחשוף את זהות הגולש האנונימי? בשאלה זו עוסק המאמר.[1]

השאלה טרם הוכרעה במשפט הישראלי. חוק מפורש שמסדיר את חשיפת הגולשים – עדיין אין; הצעת חוק – הייתה והוקפאה בינתיים; פסקי דין – יש כמה עשרות, של בתי משפט שלום ומחוזיים, אולם הם חלוקים באשר למבחן שיש להחיל במצבים מעין אלה. בחלק מפסקי הדין וההחלטות הורו בתי המשפט על חשיפת הזהות ובחלקם הורו שלא לחשוף אותה. במרס 2010 טרף בית המשפט העליון את הקלפים וקבע, בעניין **מור נ' ברק**

---

1 הדיון מתמקד בהיבטים האזרחיים של הסוגיה. בהקשר של אכיפת החוק, עולה שאלת האנונימיות בעיקר בקשר לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007 (להלן: חוק נתוני תקשורת). בבג"ץ תלויות ועומדות עתירות כנגד חוקתיות חלק מסעיפי החוק. ראו בג"ץ 3809/08 **האגודה לזכויות האזרח נ' משטרת ישראל**; בג"ץ 9995/08 **לשכת עורכי הדין נ' שר המשפטים**. לדיון קצר בחוק ראו מיכאל בירנהק "חוק נתוני תקשורת והפגיעה בזכות לפרטיות" **הסניגור** 130 4 (2008). את ההיבטים הפליליים, הביטחוניים והמדינתיים אשאיר לדיון נפרד.

אי.טי.סי,[2] כי בהיעדר מסגרת דיונית מתאימה אי־אפשר לחשוף את הגולשים האנונימיים. מלאכת עיצוב ההסדר, קבע בית המשפט ברוב דעות, היא בידי המחוקק ולא בידיו של בית המשפט.

הצעת חוק מסחר אלקטרוני, התשס״ח-2008 כללה הצעה להסדר של חשיפת זהות. הוצע לקבוע כלל של אנונימיות ולו חריג, שיאפשר את חשיפת הזהות באמצעות פנייה לבית משפט בהתקיים ״חשש של ממש״ שתוכן המידע המופץ ברשת הוא עוולה או הפרה של זכות קניין רוחני.[3] אף על פי שטרם התקבלה שימשה הצעת החוק את בתי המשפט כאמת־מידה, גם אם כללית.[4]

מאמר זה בוחן את השיקולים שיש להביא בחשבון בעת עיצוב חקיקתי או שיפוטי של הכלל המשפטי. הדיון מתנהל בשלוש מסגרות. הראשונה מבקשת לאתר את הבסיס הנורמטיבי והמשפטי של האנונימיות. אטען כי האנונימיות היא זכות הראויה להגנה כנגזרת של חופש הביטוי ושל הזכות החוקתית לפרטיות גם יחד; המסגרת השנייה עניינה חופש הביטוי בסביבה המקוונת. אטען כי זהו עיקרון מרכזי שצריך להנחות את העוסקים בעיצוב המשפט. רשת האינטרנט מציעה זירת שיח ייחודית ויש לאתר מראש את ההשפעות האפשריות של כלל משפטי כזה או אחר על אפשרויות הביטוי והשיח בזירה זו; המסגרת השלישית עניינה עיצוב מדיניות לסביבה המקוונת בכלל והסוגיה של חשיפת גולשים היא מקרה מבחן שלה.

המאמר מבקש להמחיש את גורל האנונימיות בסביבה דינמית של טכנולוגיית מידע. הסוגיה היא המחשה ליחס המורכב שבין הפרטיות (והמשפט בכלל) לבין הטכנולוגיה, כשגם הנורמות החברתיות טרם עוצבו. המשפט, הטכנולוגיה, הנורמות החברתיות

---

2 רע״א 4447/07 **מור נ׳ ברק אי.טי.סי. [1995] החברה לשרותי בזק בינלאומיים בע״מ** (פורסם בנבו, 25.3.2010).

3 סעיף 13 להצעת חוק מסחר אלקטרוני, התשס״ח-2008, ה״ח 356. הצעת החוק מבוססת במידה רבה על המלצות הוועדה לבדיקת בעיות משפטיות הכרוכות במסחר אלקטרוני דו״ח **ביניים** (2004) (בראשות עו״ד טנה שפניץ). הדו״ח דן בשאלה של חשיפת הגולשים בקצרה; ראו שם, בעמ׳ 77-78. הצעת החוק אושרה בקריאה ראשונה בכנסת השבע־עשרה ואף התקיימו כמה דיונים בוועדת־משנה לנושא אינטרנט וטכנולוגיית מידע של ועדת המדע והטכנולוגיה של הכנסת, אולם בשלב מסוים החליט משרד המשפטים שלא לקדם עוד את ההצעה. הוועדה בכנסת לא הגיעה לדון בסעיף שמבקש להסדיר את סוגיית החשיפה.

4 בחלק מהמקרים התייחסו בתי המשפט להצעת החוק כאילו היא משקפת את כוונת המחוקק. ראו ה״פ (מחוזי ת״א) 1244/07 **מזמור הפקות בע״מ נ׳ מעריב הוצאת מודיעין בע״מ**, פסקה ג (פורסם בנבו, 20.3.2008, השופטת דרורה פלפל). לפני פרסום הצעת החוק הפנו חלק מבתי המשפט לתזכיר שחיבר משרד המשפטים, שקבע עיקרון דומה בניסוח שונה מעט מזה שבהצעה.

המתעצבות לנגד עינינו וגורמים נוספים כמו כוחות השוק פועלים בערבוביה ובאינטנסיביות רבה.[5] אנו עדים למאבק על הבכורה בין הגורמים המסדירים, תוך שהם משפיעים זה על זה ומנסים לגייס זה את זה לטובתם או להכפיף את האחר אליהם. אנו רחוקים מהכרעה. לפיכך, אני סבור שגם אם וכאשר יהיה כלל משפטי ברור, בין שייקבע בחקיקה ובין שייקבע בפסיקה, אין זה צפוי להיות סופו של המאבק אלא רק שלב נוסף בו. יהא אשר יהא הכלל המשפטי – הטכנולוגיה, השוק והנורמות החברתיות יגיבו לו, ולא מובטח כי ישלימו עמו.

בחלק השני אציג את הרקע הטכנולוגי המכתיב את ההליכים המשפטיים. החלק השלישי בוחן את הכללים המשפטיים שהתגבשו בבתי המשפט בערכאות הנמוכות בישראל, את העמדות שהובעו בדעת הרוב ובדעת המיעוט בעניין מור, אל מול הצעת חוק מסחר אלקטרוני ואל מול הכללים המתגבשים במדינות אחרות. בתי המשפט בישראל נחלקו בעמדתם בסוגיה, מחלוקת שבאה לידי ביטוי גם בעניין מור. הדיון בהתמודדות המשפטית עם הסוגיה במדינות אחרות מעלה כי בין שהדגש הוא על הפרטיות ובין שהוא על חופש הביטוי, המסקנה בפועל דומה למדי.

החלק הרביעי פורש את מערך השחקנים בשדה ומתרגם את האינטרסים השונים לשפה המשפטית של שיח הזכויות. בצד הזכות המהותית של הנפגע המבקש את חשיפת הזהות עומדת לו זכותו לגישה לערכאות. מולו ניצב הגולש האנונימי. הדיון מברר את מהותה המשפטית של האנונימיות ומציע לגזור אותה הן מהזכות לפרטיות והן מחופש הביטוי. בצד הנפגע והגולש האנונימי פועלים ספקי שירות מסוגים שונים (שירותי אירוח או שירותי גישה)[6] והציבור כולו. הדיון המשפטי הקיים התמקד עד כה בשני השחקנים הראשיים: הנפגע והגולש האנונימי. בתי המשפט עסקו במידה מסוימת וחלקית בציבור והקדישו רק מעט תשומת לב, אם בכלל, לשחקנים האחרים – בעיקר הכוונה לספקי השירות השונים. בתי המשפט התייחסו אליהם כאל נתון קיים. אטען שלספקי השירות יש תפקיד מרכזי בהרבה בהבנת הסוגיה ותפקיד מסוים בפתרונה.

עיצוב כללי התנהגות בסביבה טכנולוגית דינמית אינו מצומצם לתחום המשפטי. החלק החמישי בוחן היבטים טכנולוגיים של הסוגיה. תחילה יידון הקשר שבין טכנולוגיה לערכים ותיטען הטענה שהטכנולוגיה מגלמת סל ערכים שאינו בהכרח קוהרנטי. לאחר מכן אסקור טכנולוגיות שונות המנסות לאפשר לגולשים כלים של אנונימיות. דיון זה ממחיש את התזזית שבה נמצאת הסוגיה, את היעדר הבלעדיות של המשפט ובמידה מסוימת את קוצר

---

5 לגורמים השונים שמשפיעים על עיצוב הסביבה הדיגיטלית ראו LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

6 אשתמש במונחים אלה בעקבות ההגדרות שבסעיף 7 להצעת חוק מסחר אלקטרוני, הצועדת בתורה בעקבות הדין האמריקני והאירופי בקשר לסיווג.

ידו. כלל משפטי נבון צריך לנבוע מדיון אנליטי סדור, אבל גם לפעול עם גורמים אחרים המעצבים את ההתנהגות שלנו בזירה הנתונה.

החלק השישי קושר את הקצוות ומציע מתווה נורמטיבי־משפטי לדיון בבקשה לחשיפת זהות. לאור עמדתו של בית המשפט העליון, הכתובת להסדר כזה היא המחוקק (הראשי או המשני). האמצעי הראשון שאציע, ברוח הערות בפסיקה האנגלית וברוח הסדר אחר, הכלול בהצעת חוק מסחר אלקטרוני בדבר חסינותם של ספקי שירות, הוא שספק השירות ישמש מתווך בין המבקש לבין הגולש האנונימי בלי לחשוף את זהותו של האחרון. המודל הוא של הודעה־הודעה־והפניה לבית המשפט: עם קבלת תלונה מהמבקש יעביר הספק את התלונה לגולש, ככל שיש ביכולתו לעשות כן. אם לא ייפתר הסכסוך באותו שלב – בין מחמת היעדר יכולת טכנית להגיע לגולש ובין משום שהגולש לא יסכים להיחשף – יוכל המתלונן לפנות לבית המשפט. אם השלב המקדמי לא יועיל לפתרון והמתלונן יפנה לבית משפט בבקשת חשיפה, ייתכן שהגולש יהיה מיוצג כשזהותו נשמרת חסויה. ברוח הצעותיו של השופט עמית בבית המשפט המחוזי, בעניין **מור נ' ידיעות אינטרנט**,[7] (שהיא ההחלטה שעמדה למבחן בבית המשפט העליון בעניין מור), אציע שבהיעדר ייצוג כזה יוכל בית המשפט לשמש מתווך בין הצדדים ויאפשר לגולש ייצוג תוך שמירת האנונימיות שלו.

אם גם ההליכים המקדמיים האלה לא יועילו יצטרך בית המשפט לבחון את הבקשה לגופה במעמד צד אחד – המבקש בלבד. בית המשפט יוודא תחילה שהבקשה היא בקשת־אמת שנועדה לממש זכות מהותית שנפגעה ושאין בה ניסיון להשיג יתרונות אחרים, שהדרך להשיגם, אם בכלל, היא מחוץ לכתליו של בית המשפט. לאחר מכן יעריך בית המשפט את סיכויי התביעה על סמך מרב הראיות שיש, מתוך הפעלה של עקרונות מבוססים בענף המשפטי הרלוונטי. בקשה שתצלח את המשוכות האלה תיבחן לפי שלושת מבחני המידתיות המקובלים. הראשון הוא מבחן הקשר בין התביעה לבקשה, כלומר: בין הזכות המהותית שנפגעה לבקשת החשיפה; המבחן השני בודק את קיומם של אמצעים חלופיים שפגיעתם פחותה. לשם כך יש לפתח סל יצירתי של סדרי דין – למשל כמו זה שהוצע, שעל פיו ישמש בית המשפט מתווך ויאפשר לגולש להשמיע את דברו בלי להיחשף; המבחן השלישי הוא "מידתיות צרה", כלומר: הערכה של היתרון מול החיסרון. במסגרת זו על בתי המשפט להקפיד שלא להדיר את האינטרס הציבורי. בדרך כלל תיטה הכף לטובת האינטרס הציבורי וזכות הגולש ורק במקרים קיצוניים תיטה לטובת המבקש. בכל מקרה עלינו

---

7 בר"ע (מחוזי חי') 850/06 **מור נ' ידיעות אינטרנט מערכות אתר YNET – מערכת הפורומים** (פורסם בנבו, 22.4.2007, השופט יצחק עמית) (להלן: **עניין מור מחוזי**).

להפנים את המחיר שאנו, הציבור הרחב, משלמים בעיצוב הכלל המשפטי והתוצאה הקונקרטית.

ב. עקבות דיגיטליים ושיחות מקוונות

חלק זה מציג תחילה את התשתית הטכנולוגית של רשת האינטרנט שיוצרת את המצב הנדון, שבו גולשים יכולים להשתתף בזירה הציבורית הפומבית באופן אנונימי ראשוני (ex ante) אבל האנונימיות ניתנת להסרה בדיעבד (ex post). לאחר מכן אשאל מונחים מתחום מדעי המחשב, המבחינים בין סוגים שונים של שיחות. המשגה זו מסייעת למפות את המגוון האפשרי של סוגי התקשרויות, את השחקנים השונים ואת "האיומים" על התקשורת.

1. מבנה הרשת

רשת האינטרנט בנויה כיום כך שאין בה זיהוי מובנה. גולשת המתחברת לרשת אינה נדרשת להזדהות על ידי גורם שנמצא במרכז הרשת משום שכידוע אין גורם כזה. אין צורך בהרשמה מוקדמת אלא רק בשער כניסה. את שער הכניסה יכול לספק גורם שדורש זיהוי כמו ספק של שירות גישה לאינטרנט או גורם פיזי כמו מעסיק, ספרייה ציבורית או מוסד חינוכי שיכולים לדרוש הרשמה מוקדמת וזיהוי של הגולשים. ברשת עצמה הזיהוי איננו תנאי לגלישה. שליחת דוא"ל, כתיבה בפורום, שיחה בצ'אט או פעילות אחרת – כולן אפשריות ללא זיהוי מראש. נהוג לתאר את הארכיטקטורה של הרשת כ"קצה לקצה" (end to end – e2e), כלומר: הרשת עצמה היא אוסף של "צינורות" שבהם כשלעצמם אין תבונה; זו נמצאת בקצוות, כלומר: ביישומים שמשתמשי הקצה מפעילים. מבנה "טיפש" זה של הרשת הוא אחד הגורמים להצלחתה.[8] קל יותר לעדכן, לשדרג ולחדש יישומים בקצוות מאשר להחליף ולעדכן את התשתית עצמה.

---

8 לדיון בחשיבות העיקרון הטכנולוגי הזה ראו Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001).

התשתית הקיימת של רשת האינטרנט מבוססת על זיהוי "מיקומם" של המחשבים המחוברים לרשת באמצעות מספרים.[9] המספר שמתאר את מיקום המחשבים ברשת הוא כתובת IP (Internet Protocol). כתובת זו מורכבת מארבעה שדות וטווח המספרים של כל שדה הוא בין 0 ל־255.[10] ככל שמדובר באתרי אינטרנט, ומאחר ששימוש במספרים בינאריים או במספרים ארוכים בכלל אינו נוח לבני אדם, המספרים שמזהים את מיקום אתרי אינטרנט מתורגמים לשפה מילולית, כלומר: לצירוף של אותיות ולעתים גם ספרות שמובן בדרך כלל לבני אדם. זהו שם המתחם.[11] כאשר אנו מבקשים לגלוש באתר פלוני, למשל: nytimes.com, המילה מתורגמת לספרות המתאימות שהן 192.239.136.200. התרגום נעשה באמצעות מערכת של שמות מתחם (Domain Name System – DNS).[12] אתרי אינטרנט נוטים להיות בעלי כתובות IP קבועות אולם הדבר אינו הכרחי.

כל פעולת גלישה פשוטה כרוכה בחיבור בין שני מחשבים. כך, למשל, כאשר גולשת "מתחברת לאינטרנט" ומבקשת לגלוש באתר פלוני, היא שולחת לספק שירות הגישה שלה בקשה "למצוא את האתר". הספק מתרגם את בקשת הגולשת (כתובת אתר האינטרנט המבוקש) לכתובת IP של האתר באמצעות שרת DNS ומקשר בין הגולשת לאתר. האתר שולח עותק של תוכנו כפי שהוא קיים באותו רגע למחשב הגולשת; לעתים ספק השירות יוצר עותק של האתר, הנשמר אצלו, כדי להקל על תעבורת המידע ברשת.[13] כאשר הגולשת ממשיכה ומבקשת לראות עמוד פנימי בתוך האתר המבוקש, לכתוב בו מסר כלשהו או לבצע כל פעולה אחרת שהאתר מאפשר, נוצר ערוץ תקשורת בין מחשב הגולשת למחשב האתר. כל אחד מהמחשבים צריך "לדעת" את "מיקומו" של המחשב האחר. כך גם כששני גולשים משוחחים זה עם זה בתוכנה ישירה כמו תוכנה למסרים מידיים (IM), צ'אט או שיחה קולית מקוונת (VoIP): כל אחד מהמחשבים צריך "לדעת" היכן נמצא המחשב השני ברשת כדי שהמחשבים יוכלו "לשוחח", כלומר: להעביר ביניהם מידע בפורמט דיגיטלי –

---

9 לסקירה טכנולוגית תמציתית של מבנה הרשת ראו Vinton G. Cerf, *Computer Networking: Global Infrastructure for the 21st Century*, www.cs.washington.edu/homes/lazowska/cra/networks.html (1995).

10 כתובת IP טיפוסית נראית כך: 132.66.234.228. מספר זה מתורגם לשפה בינארית, שאותה המחשבים "מבינים". המספר הנ"ל מתורגם למספר הבינארי 10000100001000010111010101 1100100. ראו, למשל, באתר זה: ip-lookup.net.

11 לסקירה טכנולוגית ראו ICANN, Internet Domain Name System Structure and Delegation, www.icann.org/en/icp/icp-1.htm.

12 ראו את ההסבר של איגוד האינטרנט הישראלי www.isoc.org.il/domain_heb/faq.html.

13 זהו שירות "מטמון" (cache), המעורר שאלות משפטיות בדבר זכויות יוצרים, החורגות מהדיון.

אותות חשמליים – שמתורגמים לשפה אנושית בכתב, בקול או בתמונה. התיאור הזה עמוס, כמובן, מטאפורות אנושיות ופיזיות שנועדו להסביר; יש להיזהר שלא ליפול שבי בפרדיגמות הפיזיות והאנושיות שהן מייצגות.[14]

התוצאה של מבנה רשת זה, המכונה IPv4, היא שמספר כתובות ה־IP הוא גדול מאוד אולם מוגבל וכבר היום יש מחסור בכתובות כאלה בגלל ריבוי המחשבים המחוברים לרשת בכל רגע נתון. לבעיה זו יש כמה פתרונות ובהם מעבר לתשתית רשת חדשה (IPv6).[15] פתרון אחר הוא הקצאה חוזרת של כתובות IP. ספקי שירות הגישה הם בעלי קבוצת כתובות שרכשו ממרשם שמות מתחם אזורי, שבתורו קיבל את הכתובות מארגון בין־לאומי (IANA) הפועל שלא למטרות רווח ומקצה את הכתובות.[16] ספקי השירות מקצים את הכתובות ללקוחותיהם על בסיס דינמי. ההקצאה נעשית בעצם ההתחברות לרשת האינטרנט באמצעות הספק ולכן אין צורך שהגולש ידע על קיומה של ההקצאה או על מספר ה־IP עצמו. מחשב שמחובר ברגע מסוים לרשת האינטרנט באמצעות ספק הגישה יקבל כתובת IP למשך הגלישה. כאשר יתנתק תחזור הכתובת לספק השירות ותהיה פנויה להקצאה לגולש חדש. זו כתובת IP דינמית. כאשר מדובר בכתובת IP קבועה כל העת, המיועדת רק לשימושו של גולש מסוים, היא נקראת כתובת סטטית.

מבנה זה של הרשת מאפשר גלישה בלי שאתר האינטרנט, גולשים אחרים או צדדים שלישיים יודעים את זהותנו אלא אם הזדהינו בעצמנו או הסגרנו פרטים מזהים.[17] לשם גלישה נדרש שהאתר יידע את כתובת ה־IP של המחשב שממנו אנו גולשים ואין ידיעה על אודות זהות המשתמש.

---

14 לסכנה של שימוש במטפורות בניתוח משפטי של הסביבה הדיגיטלית ראו Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); אברהם נ' טננבוים "על המטאפורות בדיני המחשבים והאינטרנט" **שערי משפט** ד 359 (2006).

15 ראו www.ipv6.org. IPV4, IPV6 הם פרוטוקולים של הרשת, כלומר: "השפה" שבה מתנהלת התעבורה ברשת. הפרוטוקולים מפותחים על ידי Internet Engineering Task Force (IETF), שהיא רשת בין־לאומית של מתכנתים; ראו www.ietf.org.

16 IANA הוא Internet Assigned Numbers Authority. ראו www.iana.org, הפועל במסגרת Internet Corporation for Assigned Names and Numbers – ICANN, ראו www.icann.org.

17 גולשים החוזרים ופוקדים אתר עשויים להגיע בכל פעם מכתובת IP אחרת בגלל שיטת ההקצאה הדינמית. אתר המבקש לזהות את גולשיו החוזרים לא יוכל, לפיכך, לזהותם לפי כתובת ה־IP שלהם (אלא לכל היותר יוכל לזהות את ספק שירות הגישה שלהם ואת המקום הגאוגרפי של הגלישה). כדי להתגבר על קושי זה נוהגים אתרים ליצור קובץ מידע קטן שנשמר במחשבו של הגולש ומזהה אותו כלפי האתר. זו העוגייה (cookie). בגלישה הבאה יבדוק האתר אם כבר קיימת במחשבו של הגולש עוגייה; אם תמצא כזו, יוכל לזהות את הגולש בקלות גם אם השתמש בכתובת IP שונה.

2. חשיפת זהות בשלוש תחנות

יש כמה דרכים לזיהוי הגולש. המקרה הטיפוסי, שבו נפתח מאמר זה, כולל "שלוש תחנות" לזיהוי. מישהי נתקלת באתר אינטרנט בתגובית (טוק־בק; talk back) המשמיצה אותה. התגובית עצמה אינה מזהה את הכותב/ת, ואין בה מידע על כתובת ה־IP שלו/ה. לפיכך, התחנה הראשונה של הנפגעת המבקשת לחשוף את הגולש היא האתר המארח. בעת שהגולש גלש באתר וכתב את שכתב הייתה בינו לבין האתר התקשרות ישירה (טכנולוגית, לאו דווקא התקשרות חוזית). לכן, בידי האתר היה מידע על כתובת ה־IP של המגיב. מידע זה נאסף כחלק בלתי־נפרד מהארכיטקטורה של הרשת כפי שהיא בנויה כיום, כתוצאה מהתקשורת הישירה בין האתר לגולש כפי שהוסבר לעיל. עם זאת, אין הכרח שהמידע יישמר. מבחינה טכנולוגית האתר בהחלט יכול למחוק את המידע (אם כי עשויים להיות לו שימושים מועילים גם עבור האתר כמו ספירת הגולשים בו). אם המידע נשמר, בעל האתר יכול לבדוק ברשימותיו (log) את כתובת ה־IP של המחשב שממנו גלש המגיב. אם כן, התחנה הראשונה היא האתר המארח שבידו כתובת ה־IP של הגולש. בלי תחנה זו אין טעם בהמשך הפענוח ולפחות לא בדרך הזו.

את כתובת ה־IP של הגולש אפשר כעת לבחון בדרך של בירור ההקצאה. הפענוח פשוט. אינספור אתרים מציעים שירות פענוח של כתובות IP או של שמות מתחם. המידע שיש בהם מבוסס על שרתי השורש (root servers) של רשת האינטרנט שהם מעין לוח תמסורת לרשת. באמצעות שימוש במאגרי מידע אלה אפשר לקשר בין כתובת IP לבין אתר ולהפך. בדומה אפשר לבצע שיוך של כתובות IP המוקצות לגולשים. שחזור כתובת IP יביא אותנו ברוב המקרים לספק השירות. למשל, בדיקה של כתובת IP 132.66.234.228 תעלה שהכתובת שייכת לספק השירות Tel Aviv University Network, אולם לא תזהה את הגולש המסוים.

מצוידת בכתובת IP ובפענוח חלקי שלה יכולה המבקשת לשים פעמיה לספק של שירות הגישה ולבקש בדיקה במאגר הנתונים שלו, ככל שהמידע נשמר שם. אם המידע נשמר אצל הספק הוא יכול לבדוק למי מגולשיו הקצה את הכתובת הנדונה. ההצלבה אפשרית אם ספק השירות יודע את פרטי לקוחותיו – נתון קיים בדרך כלל מטבעו של השירות – ואם הוא שמר את נתוני ההקצאה של כתובות IP. מאחר שכיום ההקצאה היא ברובה דינמית, המידע צריך להיות מדויק ברמה גבוהה. לא די לשאול למי הוקצתה כתובת IP ביום מסוים ויש לבחון את ההקצאה בדיוק של שעה ודקה. אם כן, התחנה השנייה היא הספק של שירות הגישה.

לעתים די בתחנה אחת, למשל כשנמצאים בידי האתר המארח לא רק כתובת IP של הגולש אלא גם פרטים מזהים ישירים שלו. באתרים שבהם נדרשים חובת זיהוי של הגולש ורישום מוקדם, והמידע בהם אמין,[18] די בתחנה הראשונה ואין צורך בתחנה השנייה.[19]

מצב שני שבו די בתחנה אחת הוא כשהאתר המארח מפרסם את כתובת ה־IP של המגיבים אצלו. כך, למשל, נוהג האתר "מחלקה ראשונה" מאז פברואר 2008.[20] לדוגמה, גולשים המעיינים בתגוביות לכתבה בכותרת "ממשלת ביבי תיפול תוך חצי שנה"[21] ייתקלו בין היתר בתגובית מס' 20 שכותרתה "צריך לחשוף את הבלוף 'ביבי'". כינויו של הכותב הוא "אפרסק רקוב" וכתובת ה־IP שלו, כפי שמתפרסמת באתר, היא 84.95.22.157. כן מצוינת שם השעה המדויקת שבה הועלתה התגובית לאתר (09:34). בדיקה של כתובת זו באחד מאתרי הפענוח מעלה כי ספק שירות הגישה של "אפרסק רקוב" הוא חברת ערוצי זהב 012 בע"מ. אם יבקש ראש הממשלה נתניהו לחשוף את "אפרסק רקוב", הפרקטיקה שננקטה באתר זה "תחסוך" לו תחנה אחת והוא יוכל לפנות במישרין לספק השירות.

מצב שלישי של תחנה אחת הוא כשהנפגע היה בקשר ישיר עם הגולש האנונימי. מחשבו של המבקש "שוחח" עם המחשב האחר וכך נמסרה כתובת ה־IP של הגולש ישירות למבקש. הנדסה חוזרת תגלה את ספק השירות. זה המקרה של שימוש בתוכנות לשיתוף

---

18 מחקר אמפירי של אתרי אינטרנט ישראלים, הדורשים מגולשיהם להזדהות כתנאי לגלישה באתר או בחלקים ממנו, העלה כי ביותר ממחצית מהאתרים שנבדקו, יכול הגולש למסור פרטים כוזבים ולמרות זאת גישתו לאתר תתאפשר. ראו Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance* (2009), ssrn.com/abstract=1456968.

19 בשני מקרים שהתעוררו לא ברור כיצד השיגו המבקשים את כתובת ה־IP של הגולש. ראו ת"א (מחוזי מרכז) 2223-04-08 **סי. אנ. אימיגריישן בע"מ נ' ווינשטיין** (פורסם בנבו, 3.7.2008, השופט אברהם יעקב). המשיבים ביקשו לפסול את הראיה, כלומר, את זיהוי כתובת ה־IP, מחמת שהושגה תוך פגיעה בפרטיות, אולם בית המשפט קבע כי לא עמדו בנטל הראיה הנדרש. במקרה אחר נחשף בלוגר שכינה עצמו "ייגר מאייסטר" וחיבר בלוג בשם "עומדים בשער" ובו ביקורת על עיתונות הספורט. הבלוגר, העיתונאי שלמה מן, פוטר בעקבות החשיפה ממשרתו כעורך ספורט בעיתון מעריב והוגשה כנגדו תביעת לשון הרע. מן תבע את תובעיו ואת ספק שירות הגישה וטען כי כתובת ה־IP שלו נחשפה שלא כדין. ראו ת"א (שלום) 151582/09 **אסייג נ' מן**. ספק שירות הגישה הכחיש בכתב ההגנה כי מסר את פרטיו. התביעה עודנה תלויה ועומדת.

20 ראו את הודעתו של מו"ל האתר ועורכו הראשי, יואב יצחק "אתר NFC: נפרסם כתובת IP" **מחלקה ראשונה** (2.2.2008) www.news1.co.il/Archive/003-D-27553-00.html?tag=22-02-34.

21 עידן יוסף "ממשלת ביבי תיפול תוך חצי שנה" **מחלקה ראשונה** (15.2.2009) www.news1.co.il/Archive/001-D-190768-00.html?tag=16-41-38.

קבצים. כידוע, בתוכנות כאלה נעשה שימוש ניכר של הפרת זכויות יוצרים. העברת הקבצים נעשית במישרין בין הגולשים: הקובץ מועבר מגולש שבמחשבו נמצא הקובץ לגולש אחר. חברות המוזיקה בעלות זכויות יוצרים יכולות – ובארצות־הברית אף נהגו כך – לגלוש בעצמן ברשת של משתפי הקבצים ובגלישה סמויה כזו לזהות מי מפיץ קבצים של יצירות מוגנות שבבעלותן.[22] מטבע הארכיטקטורה של הרשת והטכנולוגיה של התוכנות הנ״ל, הזיהוי מלווה במידע של כתובת IP של הגולש האחר. מצוידות במידע זה, בעלות הזכויות יכולות לפנות במישרין לספק של שירות הגישה.

לעתים לא די בשתי תחנות שכן במקום הגלישה יש משתמשים רבים. לכן, גם אם אפשר לאתר את המחשב שממנו גלש הגולש אין פירוש הדבר בהכרח שהגולש זוהה; לכל היותר זוהה המחשב. במקרים מסוימים זיהוי המחשב לבדו לא יועיל כלל, למשל כשמדובר במחשב שנמצא במקום ציבורי ונגיש למשתמשים רבים כמו מחשב בספרייה ציבורית או בקפה אינטרנט, או כשמדובר ברשת גלישה אלחוטית פתוחה לציבור. בהחלט ייתכן שהגולש המבוקש אינו בעל הרשת אלא אחד משכניו או עובר אורח שהשתמש בשירותי הרשת האלחוטית הפתוחה. כדי להוכיח את זהות האדם יידרש מידע נוסף, חיצוני לגלישה עצמה.[23] מובן שהמקומות הפיזיים שבהם אנו נמצאים בעת הגלישה יכולים ליצור פרקטיקות של זיהוי. במקרה כזה, מלאכת הבילוש תכלול תחנה נוספת. כך, למשל, מפעילים של קפה אינטרנט באיטליה דורשים מאז שנת 2005 תעודה מזהה של המשתמשים. הדרישה נובעת מחוק למניעת טרור שנחקק שבועות ספורים לאחר פיגועי הטרור בלונדון, ביולי 2005.[24] אם מלאכת השחזור תעלה שהתגובה נכתבה מקפה אינטרנט

---

22 לתיאור חשיפה באמצעות גלישה סמויה ראו London Sire Records, Inc. v. Doe 1, 542 F. Supp.2d 153, 160 (D. Mass. 2008).

23 במקרה אחד חשף הספק של שירותי הגישה, לפי צו בית המשפט, את פרטי המנוי, שהיו למעשה שני מנויים נשואים באותה עת. התביעה הוגשה נגד אחד מהם שטען כי לא הוכח שהוא מחבר התוכן השנוי במחלוקת. בית המשפט התבסס על הימנעות הנתבע מלהעיד כראיה שפעלה כנגדו. ראו ת״א (שלום י-ם) 7667/03 **נבות נ׳ גור** (פורסם בנבו, 11.2.2008, השופטת עירית כהן). במקרה אחר חשפה חברת גוגל את פרטיו של בלוגר לפי צו בית משפט, אולם הבלוגר הכחיש כל קשר לתוכן הפוגעני. נדרשה החלטה נוספת ובה הורה בית המשפט על חשיפת פרטיהם של כל בעלי כתובת ה־IP הדינמית. ראו בש״א (שלום ראשל״צ) 567/08 **בלומנפלד נ׳ Google, Inc.** (פורסם בנבו, 21.9.2008, השופט אורן שוורץ). לדיון בקשיים ובכך שלעתים יידרשו עוד תחנות ראו עניין מור, לעיל ה״ש 2, בפסקה 10 לחוות דעתו של המשנה לנשיאה ריבלין.

24 ראו סעיף 7 לחוק האיטלקי, La Legislazione Antiterrorismo, Law No. 155/2005. החוק מכונה חוק פיזאנו על שם שר הפנים האיטלקי דאז ג׳וזפה פיזאנו (Pisanu). www.parlamento.it/parlam/leggi/05155l.htm (איטלקית).

אזי בתחנה השלישית – מפעיל הקפה – אפשר יהיה לבדוק מי השתמש במחשב המבוקש במועד מסוים. במילים אחרות, הפענוח אפשרי אבל כרוך בתחנות נוספות; לכן יש לו עלויות שונות ותוצאתו אינה מובטחת.

הסקירה מעלה כמה מסקנות חשובות לדיון: הארכיטקטורה של רשת האינטרנט איננה כוללת זיהוי מובנה אך היא מותירה עקבות דיגיטליים בדמות כתובת IP של הגולשים. הכתובות ניתנות לפענוח בתחנה אחת או בשתיים וכן באמצעות שימוש בתוכנות זמינות ברשת. במובן זה, זהותם של הגולשים אפשרית למעקב (traceable),[25] אולם הזיהוי אינו ודאי: הוא מחייב איסוף של המידע הרלוונטי, אי־מחיקתו בשלב הראשון (באתר, "התחנה הראשונה") ואפשרות לאחזר את המידע מתוך המאגרים שמתעדים את הגלישה אצל ספק שירות הגישה ("התחנה השנייה"). השחקנים השונים המעורבים בתהליך יכולים לחשוף מראש את הנתון של כתובת IP, כבדוגמת האתר "מחלקה ראשונה". גם במקרים שבהם המידע נאסף ונשמר עלולים להתעורר קשיים באיתור הגולש, למשל אם נעזר בתוכנה שמספקת לו אנונימיזציה.[26] במקרים אחרים, התחנה השנייה (ספק השירות) והתחנה השלישית (מקום הגלישה) הם אותו ארגון כגון אוניברסיטאות שמספקות שירותי גישה לאינטרנט ומקום גישה פיזי לאינטרנט.

3. שיחות מקוונות ונתוני תקשורת

הזכות לפרטיות עוסקת בכמה קטגוריות משפטיות ובהן פרטיות בתקשורת.[27] ההגנה היא בראש ובראשונה לתוכן השיחות.[28] חשיפת הזהות שבה דן מאמר זה איננה עוסקת

---

25 ראו A. Michael Froomkin, *Anonymity and Its Enmities*, 1995 J. ONLINE L. art. 4, par. 11, 14; Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity and Pseudonimity as Overall Solutions to the Troubles of Information Privacy*, 58 U. MIAMI L. REV. 1301 (2004).

26 ראו להלן, חלק ה(2).

27 ראו מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 27-38 (2007) (להלן: בירנהק "שליטה והסכמה").

28 חוק־יסוד: כבוד האדם וחירותו קובע בסעיף 7(ד): "אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו". חוק האזנת סתר, התשל"ט-1979 אוסר האזנות סתר ומסדיר האזנות של גורמי אכיפת החוק. חוק הגנת הפרטיות, התשמ"א-1981 קובע כמה מצבים של פגיעה בפרטיות שעניינם תקשורת: סעיף 2(2) קובע כי האזנה שאסורה על פי החוק היא פגיעה בפרטיות; סעיף 2(5) קובע כי העתקת תוכן של מכתב שלא נועד לפרסום היא פגיעה בפרטיות, כאשר כתב מוגדר מאז תיקון מס' 9 לחוק ככולל גם מסר אלקטרוני. ראו חוק הגנת הפרטיות (תיקון מס' 9), התשס"ז-2007, ס"ח 2101, 368.

במישרין בתוכן השיחה אלא במעטפת. במקרה של תגובית אנונימית, התוכן גלוי והשאלה היא מי חיבר אותו. ההבחנה בין מעטפת לתוכן קיימת בסביבה הפיזית ולכן רב הפיתוי להשליך אותה על הסביבה הדיגיטלית;[29] אולם כגודל הפיתוי הקוגניטיבי כך הסכנה המשפטית.[30] סעיף זה מציג את ההבחנה הקיימת בעולם שאינו מקוון בין תוכן לבין נתוני תקשורת ואת מדרג הפרטיות המשפטי שנלווה לה. זהו מדרג אנלוגי; הטענה היא שההבחנה של מעטפת־תוכן, ובעקבותיה המדרג המשפטי האנלוגי, אינם מתאימים לסביבה דיגיטלית.[31]

"מכתב" כולל תוכן ומעטפה. מה שנמצא בתוך המעטפה הסגורה מוגן על ידי הדין. הפרטים שנמצאים בחוץ, על גבי המעטפה, הם נתוני המכתב המכוונים לספקי השירות, כלומר: שירותי הדואר. כתובת הנמען הכרחית לשם שיגור המכתב ליעדו ואילו כתובת השולח תאפשר את החזרת המכתב במקרה שהנמען לא יימצא. ההבחנה בין התוכן למעטפת מכתיבה לכאורה הבחנה משפטית: התוכן שבפנים הוא פרטי ואילו המידע שבחוץ, על גבי המעטפה, הוא מכשירני; הוא איננו חלק מתוכן ולכן איננו "סוד שיחו" של אדם. ההבחנה בין התוכן למעטפת מולידה מדרג אינטואיטיבי של הגנת פרטיות גבוהה יותר לתוכן והגנה פחותה לנתוני התקשורת.[32]

לא בכדי רשויות אכיפת החוק מגלות עניין בנתוני התקשורת וקידמו את הרחבת סמכויותיהן בנושא.[33] ניתוח הנתונים (traffic analysis) יכול לקשר בין אדם לבין פעילות מסוימת. חוקרים פרטיים עשויים להתעניין בכך כדי לקשר בין פעולה ידועה לבין אדם שזהותו אינה ידועה. גם גורמים מסחריים מתעניינים בנתוני התקשורת שלנו. הנתונים

---

29 יש מצבים עובדתיים מגוונים אחרים, למשל כאלה שבהם התוכן גלוי ונתוני התקשורת, כולל זהות המחבר, סמויים, למשל: כתובת גרפיטי או כרוז אנונימי שהודבק על לוח המודעות.

30 ראו Hunter, לעיל ה"ש 14; טננבוים, לעיל ה"ש 14.

31 לתיאור היחס המשפטי השונה לתוכן לעומת נתוני תקשורת ולביקורת על ההבחנה בהקשר הדיגיטלי ראו גם עומר טנא "תסתכל בקנקן ותראה מה שיש בו: נתוני תקשורת ומידע אישי במאה ה־21" **משפט וטכנולוגית מידע** (ניבה אלקין־קורן ומיכאל בירנהק עורכים, צפוי להתפרסם בשנת 2010) (הספר להלן: **משפט וטכנולוגית מידע**).

32 ראו ביקורתו של טנא כלפי ההבחנה, שם. השוו לעמדה שמצדדת בהבחנה ובתחולתה בסביבה הדיגיטלית: Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 611-616 (2003).

33 חוק נתוני תקשורת מסדיר שלושה אפיקים לקבלת נתוני תקשורת מספקיות הבזק השונות. דרך המלך היא פנייה לבית משפט בבקשה לצו, אפיק שני הוא פנייה ישירה לספקיות השירות במקרים דחופים והאפיק השלישי מפקיד בידי המשטרה מאגר מידע על בעלות בקווי טלפון ועל מיקום אנטנות סלולריות. חשוב להדגיש כי דרכים אלו מקלות מאוד בהשוואה לדרך לקבלת גישה לשיחה מספקיות הבזק השונות באמצעות צו לפי חוק האזנת סתר.

מעידים על הרגלים, על העדפות ועל הקשרים החברתיים שלנו. במובן הזה, רשתות חברתיות מהסוג שנפוץ בעשור הראשון של המאה העשרים ואחת הן מכרה זהב לבעלי אתרים, למפרסמים ולרשויות חקירה: מפת ההקשרים החברתיים של אנשים פרושה לעין כל.[34] לנתוני התקשורת יש יתרון נוסף על פני התוכן: קל יותר לשמור אותם ולעבד אותם. כריית מידע בתוך נתוני תקשורת עשויה להניב הקשרים מעניינים שעין אנושית לא בהכרח הייתה מבחינה בהם.[35]

כל תקשורת דיגיטלית היא שיחה: הגולשת "משוחחת" עם אתרי אינטרנט או עם גולשים אחרים. התקשורת הדיגיטלית כרוכה בהעברת מידע בין המחשבים ובכלל זה נתונים על אודות מקום הימצאם של המחשבים ברשת. יש להבחין בין סוגים שונים של "שיחות" שמכתיבים התייחסות שונה.[36] מדעני מחשבים מבחינים בין סוגי שיחות שונים לפי ה"איומים" על השיחה.[37] בהתאם, הם ממשיגים את האינטרסים של הצדדים לשיחה: סודיות (confidentiality), המתייחסת לתוכן השיחה; וידוא זהות (authentication), שהוא האינטרס של הצדדים לדעת שהם משוחחים עם מי שהם חושבים שהם משוחחים איתו; אנונימיות, שהיא הסתרת הזהות של המשוחחים זה כלפי זה או כלפי צדדים שלישיים.[38]

---

34 Lilian Edwards & Ian Brown, *Data Control and Social Networks: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION 202 (Andrea M. Matwyshyn ed., 2009). לדיון באפשרויות השונות של מעקב אחרי רשתות כאלה באמצעות לימוד נתוני התקשורת ראו George Danezis & Bettina Wittneben, *The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications*, *in* PROCEEDINGS OF THE 5TH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2006).

35 על כריית מידע בכלל ראו Tal Z. Zarsky, *Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J. L. & TECH. 1 (2002). לדיון בהקשר של איסוף מידע על גולשים, ראו Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 270-273 (2008).

36 על הצורך בהתאמה של כללי משפט שונים לפי סוגי התקשורת ברשת עמד השופט מישאל חשין בהחלטה בכובעו כיו"ר ועדת הבחירות המרכזית. ראו תב"מ (יושב ראש ועדת הבחירות המרכזית לכנסת ה-16) 16/01 **סיעת ש"ס נ' פינס**, פ"ד נה(3) 159, 164 (2001).

37 ראו, למשל, את ההגדרות המקובלות, כפי שהוגדרו תחילה על ידי Andreas Pfitzmann & Marit Köhntopp-Hansen ועודכנו על-ידי אחרים בין השנים 2000 ל-2005: *Anonymity, Unobservability, and Pseudonimity: A Proposal for Terminology*, www.freehaven.net/anonbib/cache/terminology.pdf.

38 ראו, למשל, Danezis & Wittneben, לעיל ה"ש 34.

לפי מושגים אלה, אמות־המידה הרלוונטיות לדיון בחשיפת הגולשים הן שתיים: (1) האם תוכן השיחה גלוי – ולמי? האם רק למשוחחים או גם לצדדים שלישיים? (2) האם זהות המשוחחים ידועה – ולמי? לכולי עלמא, לכל המשוחחים או רק לאחד מהם?

במונחים אלה, למשל, גלישה ברשת היא שיחה בין גולשת אנונימית לבין אתר ידוע שתכניו גלויים; אבל עצם ההתקשרות – כלומר: העובדה שגולשת מסוימת גלשה באתר – ידועה רק לגולשת ואילו האתר יודע רק את פרטי ההתקשרות הטכניים של הגולשת, דוגמת כתובת IP, אלא אם ביקש וקיבל זיהוי מלא. הגלישה ברשת היא תקשורת בין מחשבים ולכן דומה לשיחה בעולם שאיננו מקוון, בהבדל משמעותי: התוכן ונתוני התקשורת מתמזגים. גלישה באתר רפואי מצביעה על העניין שיש לגולש במידע הרפואי. אין משמעות הדבר בהכרח שהגולשת סובלת ממחלה מסוימת: אולי היא חוקרת את המחלה, אולי היא מתעניינת בסימפטומים שונים שהתגלו אצלה או אצל אחר או ששמעה עליהם בתקשורת והיא מבקשת להרחיב את אופקיה. גלישה באתר לייעוץ פסיכולוגי מלמדת על העניין של הגולשת באתר. אין הדבר מעיד בהכרח שהגולשת סובלת מבעיה פסיכולוגית, אבל האפשרות קיימת. כך גם בקשר לאתרים הומו־לסביים, אתרים פיננסיים, אתרי היכרויות, ובעצם כל אתר: גלישה מעידה על עניין. האפשרות הטכנולוגית לאסוף את המידע על הרגלי הגלישה שלנו – קיימת. איסוף הנתונים יוצר את הפרופיל שלנו. נתוני התקשורת – כלומר: הנתונים בדבר זהות הגולשים, מחוזות גלישתם, יעדי מכתביהם המקוונים ובכלל זה שיחות מקוונות מסוגים שונים – כל אלה מעידים במקרים רבים על תוכנה של התקשורת, ולכן ההבחנה בין תוכן למעטפת קורסת.

את המצב הנדון כאן – התגובית האנונימית המתפרסמת באתר – אפשר להמשיג כשיחה בין גולשת לבין ציבור הגולשים באתר, כשתוכן השיחה גלוי ואילו זהות הגולשת אינה ידועה לכול. כמו כן, ספק שירותי האירוח יודע פרטים מסוימים על אודות הגולשת האנונימית, כלומר: את כתובת ה־IP שלה.

אפיון זה מתבסס על הבחנה בין תוכן לבין זהות, אבל – כבדוגמת הגלישה – זהות הכותב עשויה להיות מרכיב חשוב בתוכן.[39] גם בשיחות מהסוגים האחרים, האפשרות שזהותו של אחד מבני השיחה אינה ידועה היא חלק מתוכן השיחה. המסר מועבר בצורה שונה כאשר הכותב גלוי, משתמש בפסבדונים, מוסר פרטים מסוימים על אודותיו (אזכור מקום מגורים, למשל, נפוץ בתגוביות באתרי חדשות) או נותר אנונימי. הקוראים עשויים לייחס משקל שונה לכתוב בהתאם לזהות הכותב, וכשזו אינה ידועה – לפי היעדרו של

---

39 לטיעון משכנע בקשר לכך ראו Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1559-1568 (2007).

הזיהוי. במובן זה, זיהוי המחבר הוא חלק מהמדיום, שהוא, כאמרתו הידועה של מרשל מקלוהן, המסר, כלומר: התוכן.[40]

סיווג השיחות לפי אמות־מידה של תוכן (גלוי או פרטי) ושל זהות המשוחחים (גלויה, סמויה וכלפי מי) מעלה שבגלישה באינטרנט קורסת ההבחנה בין התוכן לבין נתוני התקשורת ובעקבותיה קורס "מדרג הפרטיות" האינטואיטיבי שמגן על התוכן יותר מאשר על נתוני השיחה. כאשר התוכן גלוי והזהות סמויה, המדרג מתהפך. מידע על נתוני השיחה חושף את זהות הכותבת. במקרים אחדים, עצם העובדה שפלונית שוחחה עם אלמוני חשובה יותר מתוכן השיחה משום שהיא מעידה על קשר ביניהם: העובדה שאדם שוחח עם עיתונאית יכולה להעיד כי הוא המקור של אותה עיתונאית. זהותה של מי שתרמה תרומה אנונימית באמצעות אתר תרומות היא חלק בלתי־נפרד מהפעולה.

מסקנת ביניים של הדיון היא שגם התקשרויות מקוונות שנחזות להיות אנונימיות, ובכלל זה פרסום תגובית אנונימית, ניתנות לאיום של חשיפה בדיעבד של זהות הגולשים. במקרים מסוימים הזהות היא חלק בלתי־נפרד מתוכן השיחה ולעתים אף חשובה ממנו. מדרג משפטי שמייחס יתר חשיבות לתוכן הוא כלל משפטי תלוי טכנולוגיה אנלוגית, שמומחש בפרדיגמה של המכתב והמעטפה. כלל אנלוגי כזה אינו מתאים כמות שהוא לסביבה הדיגיטלית.

בהקשר החשיפה של שמות הגולשים לא עמדו בתי המשפט על הבחנות אלה וחלקם הניחו את תחולתו של מדרג הפרטיות האינטואיטיבי. החלק הבא בוחן את עמדתם של בתי המשפט; זה שאחריו צולל לעומק השיקולים הנורמטיביים.

ג. גיבוש כללים משפטיים תוך כדי תנועה

רשת האינטרנט שזורה ברשת משפטית. השאלה המשפטית בעניינו היא אימתי יש לאפשר את חשיפת זהותו של הגולש האנונימי. אנו נמצאים בעיצומו של תהליך שיפוטי לגיבוש כללים, המתרחש לנגד עינינו במהירות גבוהה תוך ניסיון להתאים כללים משפטיים לטכנולוגיה דינמית. חלק זה מציג את ההתייחסות המשפטית המתגבשת בפסיקה הישראלית, בהצעת חוק מסחר אלקטרוני ובשיטות משפט אחרות. המטרה היא לדלות את

---

40 MARSHAL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 7 (1964). השופט ריבלין ציין זאת אף הוא וכתב "האנונימיות היא לעתים חלק מהמסר עצמו" – ואף הדגים בשימוש בפסבדונים ספרותי. ראו עמדתו בעניין מור, לעיל ה"ש 2, בפסקה 12.

השיקולים שיש להביא בחשבון ואת השיקולים שהוחמצו, ולחשוף את הנחות הרקע הסמויות הפועלות בזירה.

1. חובת סודיות

שאלה מקדמית היא אם מותר לספק השירות למסור את המידע שיש בידו, אם בכלל, על פי רצונו או שמא הוא כפוף לחובה למסור את המידע. התשובה נמצאת בעיקר בדיני הגנת הפרטיות ובמידה פחותה בדיני החוזים.

מה טיבה המשפטי של כתובת IP? המסגרת המשפטית המתאימה היא של חוק הגנת הפרטיות ושל הביטוי "ענייניו הפרטיים של אדם" המופיע בו בכמה הקשרים. בתי המשפט פירשו מונח זה בצורה מרחיבה, ככולל גם שם, כתובת או מספר טלפון,[41] אם כי נשמעו גם עמדות מצמצמות יותר.[42] באיחוד האירופי דיני הגנת המידע (data protection) מגדירים "מידע אישי" כמידע שמזהה אדם או כמידע שממנו אפשר לזהות אדם.[43] ועדת מומחים בישראל המליצה לאמץ הגדרה דומה בדין הישראלי.[44] לפי ההגדרה האירופית, המידע על כתובות IP מוגן ומוסדר בדין וכך אף קבע הגורם המקצועי באיחוד, בחריג של מקרים שבהם אין דרך לדעת מי הגולש שקיבל את כתובת ה־IP כגון בקפה אינטרנט.[45]

---

41 ראו ע"א 439/88 **רשם מאגרי המידע נ' ונטורה**, פ"ד מח(3) 808, פסקה 7 לפסק דינו של השופט גבריאל בך (1994). במקרים מהעת האחרונה נפסק, למשל, שצילום אדם הוא "ענייניו הפרטיים" של אדם; ראו רע"א 6902/06 **צדיק נ' הוצאת עיתון הארץ בע"מ**, פסקה 9 לפסק דינו של השופט אליעזר ריבלין (פורסם בנבו, 13.8.2008). עוד נפסק כי מידע על הכנסות הוא "ענייניו הפרטיים" של אדם; ראו עע"ם 398/07 **התנועה לחופש המידע נ' מדינת ישראל**, פסקה 41 לפסק דינה של השופטת עדנה ארבל (פורסם בנבו, 23.9.2008).

42 ראו עניין **ונטורה**, לעיל ה"ש 41, בעמ' 835. לעמדה מצמצמת מהעת האחרונה ראו בג"ץ 844/06 **אוניברסיטת חיפה נ' עוז**, פסקה 20 לפסק דינה של השופטת אסתר חיות (פורסם בנבו, 14.5.2008).

43 סעיף 2(a) לדירקטיבה להגנת מידע משנת 1995, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 (1995).

44 ראו משרד המשפטים – הוועדה לבחינת החקיקה בתחום מאגרי המידע **דין וחשבון** 20 (2007) (בראשות המשנה ליועץ המשפטי לממשלה יהושע שופמן). המחבר היה חבר בוועדה.

45 ראו Article 29 Data Protection Working Party, WP 136, Opinion 04/2007 on the concept of personal data 16-17 (20.6.2007) www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

ככל שכתובת IP נשמרת עם מידע נוסף על אודות הגולש, יוצא שבידי ספק השירות נמצא "מאגר מידע" כהגדרתו בחוק – ואז חייב הספק בשמירת סודיות לגבי המידע.[46] כאשר מדובר בספקים של שירות גישה הפועלים לפי רישיון של המדינה, חל עליהם איסור לגלות מידע המתייחס למסר בזק.[47] במקרים אחרים ייתכן שספק השירות כפוף לחובה של שמירת המידע מכוח דין ספציפי או מכוח הסכם.[48] בכל מקרה שבו אין חובה ספציפית אני סבור שיש לגזור את חובת הסודיות מתוך עקרונות יסוד של דיני הגנת הפרטיות. יסוד מרכזי הוא העיקרון של צמידות המטרה, שלפיו מידע שנאסף למטרה אחת אינו יכול לשמש למטרה אחרת. חובת הסודיות נגזרת מעיקרון יסודי זה.[49]

לאור חובת הסודיות, מסירת המידע מותרת בהסכמת הגולש. לפי חוק הגנת הפרטיות, הסכמה כזו צריכה להיות הסכמה מדעת.[50] ספק רב אם תקנוני השימוש השונים והצהרות הפרטיות של האתרים הם חוזים תקפים ומחייבים שאפשר להסיק מהם הסכמה מדעת כזו.[51] אכן, עד כה לא הסתמכו בתי המשפט על הבסיס החוזי כדי לקבוע שמסירת הפרטים מותרת.[52] לאור חובת הסודיות, דרך שנייה לחשוף את הזהות היא צו של בית משפט.[53] אם כן, מרכז הכובד עובר לשאלה המהותית: מתי יורה בית משפט על חשיפת זהות?

---

46 סעיף 16 לחוק הגנת הפרטיות.

47 סעיף 32 לחוק התקשורת (בזק ושידורים), התשמ"ב-1982.

48 אם נקבעה חובת סודיות בדין או בהסכם, וככל שנקבעה חובה כזו, הרי גם סעיפים 2(7) ו־2(8) לחוק הגנת הפרטיות קובעים כי מסירת מידע על ענייניו הפרטיים של אדם בנסיבות כאלה היא פגיעה בפרטיות.

49 לעקרון של צמידות המטרה ראו בירנהק "שליטה והסכמה", לעיל ה"ש 27, בעמ' 54-57.

50 ראו סעיפים 1 ו־3 לחוק הגנת הפרטיות. המונח "הסכמה מדעת" נוסף בחוק לתיקון הגנת הפרטיות (תיקון מס' 9), התשס"ז-2007. המונח אינו מפורש בחוק. אני סבור שיש לפרשו ברוח מקורו, בהקשר של זכויות החולה. ראו בירנהק "שליטה והסכמה", לעיל ה"ש 27, בעמ' 50.

51 כדי לקבוע כך יש להשיב על כמה שאלות: האם בכלל נכרת חוזה? האם החוזה תקף (במיוחד נוכח דיני החוזים האחידים)? האם תניות ספציפיות בחוזה תקפות? האם התוכן מספק את דרישת ההסכמה מדעת?

52 השאלה עשויה לעלות אם הספק מסר מידע מרצונו והגולש שנחשף תובע את הספק בגין הפרת הסודיות או החוזה.

53 בעניין מור, לעיל ה"ש 2, ציין השופט רובינשטיין בדעת מיעוט כי גם אם יש חובת סודיות בין ספקית השירות ללקוחותיה, הרי אין בדין הקיים חיסיון שפוטר את הספקית ממסירה של פרטי הגולשים על דוכן העדים. מכאן סבר השופט כי אין מניעה לקבוע חובה של הספקית למסור את המידע ובכך ליצור עילת תביעה פסיקתית שהיא "אך הרחבת הנסיבות בהן ייחשף המידע". שם, בפסקאות יא, יג.

2. מדואר הצבי למהירות האור

מעניין לפתוח דווקא בפסק דין שעסק בחשיפה של דובר אנונימי בסביבה הפיזית, **דואק נ' רשות הדואר**, שנפסק בבית המשפט המחוזי בחיפה.[54] עלון אנונימי שהופץ באמצעות רשות הדואר כלל ביטויים כנגד דואק, חבר מועצת העיר בקרית ביאליק, ביטויים שלטענתו היו משפילים ומבזים. דואק פנה לסניף הדואר וביקש מידע על זהותו של שולח העלון. רשות הדואר סירבה לבקשה ודואק פנה לבית המשפט.[55] בית המשפט קבע כי פרטיות השולח כוללת גם את שמו ולא רק את תוכן מכתביו,[56] אולם לאחר מכאן ציין את הקביעה הנפוצה בפסיקה כי הזכות לפרטיות – ולכן גם הזכות לאנונימיות – אינה מוחלטת. את היקפה של האנונימיות ביקש בית המשפט לגזור מתוך ההצדקה של הזכות לפרטיות, אולם קבע כי אנונימיות הקרובה לרצון להתחמק מאחריות אינה באה בשעריה של הזכות לפרטיות.[57] בהמשך קבע בית המשפט קביעה נוספת שלפיה כאשר תוכן המכתב גלוי לעין כל, כפי שהיה במקרה זה, טענת הפרטיות לא יכולה לעמוד.[58] האיזון של הזכות לפרטיות, לאחר שתוחמה בצורה צרה, עם זכותו של המבקש לשם טוב וכדי שיוכל לממש את זכויותיו, הכתיב את חשיפת זהותו של השולח.[59]

הבקשות לחשיפת זהותם של גולשים אנונימיים ברשת הן מעין גרסה מקוונת של עניין **דואק**: הפרסום גלוי לעין כל, זהות הגולש – או פרטים מזהים שלו – ידועים לגורם הביניים

---

54 ה"פ (מחוזי חי') 231/04 **דואק נ' רשות הדואר** (פורסם בנבו, 19.7.2005, השופטת אסתר שטמר).

55 הבסיס המשפטי לסירוב הוא הזכות לפרטיות של השולח לפי חוק הגנת הפרטיות, לפי חוק-יסוד: כבוד האדם וחירותו ולפי חובת הסודיות המוטלת על רשות הדואר לפי סעיף 91 לחוק הדואר, התשמ"ו-1986. העוגן לסמכותו של בית המשפט נמצא בסעיף 16 לחוק הגנת הפרטיות, הקובע חובת סודיות על מחזיק של מאגר מידע כהגדרתו של "מאגר מידע" בסעיף 7 לאותו חוק, אבל מתיר שיקול דעת לבית המשפט להורות על הגילוי. הוראה כללית זו אכן קובעת להליך החשיפה וו שניתן להיתלות בו, לפחות ככל שמדובר במאגר מידע.

56 עניין **דואק**, לעיל ה"ש 54, בפסקה 7. השופטת שטמר פירשה את סעיף 2(5) לחוק הגנת הפרטיות, הקובע כי "העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתוכנו, בלי רשות מאת הנמען או הכותב [...]" הוא פגיעה בפרטיות.

57 שם, בפסקה 9.

58 שם, בפסקה 10.

59 כפי שאסביר בחלק הבא, אכן נכון לגזור את האנונימיות מתוך הזכות לפרטיות אולם לא ברור מקור התיחום המצר שננקט בפסק הדין. הקביעה שכאשר מדובר בפרסום גלוי אין מקום לאנונימיות מבטלת למעשה את הגנת האנונימיות בפרסום פומבי. הבקשה העלתה שמחבר העלון היה יריב פוליטי של דואק. בעקבות חשיפת השם הוגשה נגדו תביעת לשון הרע, שהסתיימה בפשרה בראשית 2009. כך עודכנתי בשיחת טלפון עם יוסי דואק (10.3.2009).

המתווך, אולם אינם מתפרסמים ברבים, ויש מי שנפגע ומבקש להורות על חשיפת הזהות כדי לממש זכות מהותית שנפגעה.

מאז שנת 2000 הוגשו לבתי המשפט כמה עשרות בקשות לחשיפה של שמות גולשים; הזרם התגבר מאז שנת 2006. רוב הבקשות עוסקות בלשון הרע. בית המשפט העליון נדרש לסוגיה וכאמור קבע כי אין כלל מסגרת דיונית לבקשות החשיפה.[60] בתי המשפט הזכירו בהחלטותיהם שורה של שיקולים, ובהם זכותו המהותית של המבקש לשם טוב וזכות הגולש האנונימי לאנונימיות. הזכות לאנונימיות הומשגה בכמה מקרים כחלק מחופש הביטוי,[61] כנגזרת של הזכות לפרטיות[62] ולפעמים כנתון בשיח המקוון[63] – בדרך כלל ללא הנמקה יתרה. השאלה בדבר הבסיס העיוני של האנונימיות ומעמדה המשפטי עלתה באופן ישיר במחלוקת שנפלה בבית המשפט העליון בעניין **מור**. דעת הרוב של המשנה לנשיאה ריבלין המשיגה את האנונימיות הן כנגזרת של חופש הביטוי והן כנגזרת של הזכות לפרטיות. מסקנתו הייתה ש"האנונימיות מבטאת זכויות יסוד חשובות – זכות לחופש ביטוי וזכות לפרטיות – ויש לה מעמד חוקתי".[64] לעומת זאת, דעת המיעוט של השופט רובינשטיין המשיגה את האנונימיות רק במסגרת של חופש הביטוי, תוך הכפפת האנונימיות לחופש הביטוי ותיאורה כעובדה בלבד: "לפי פרספקטיבה זו, אין זכות לאנונימיות מעבר לזכות לחופש הביטוי – ואין לראות באנונימיות 'זכות' אלא עובדה, מציאות חיים שהפכה קלה יותר עם התפתחות רשת האינטרנט".[65] במקרים ספורים העירו בתי המשפט כי למבקש

---

60 עניין **מור**, לעיל ה"ש 2. בבית המשפט העליון תלויים ועומדים בעת כתיבת שורות אלה, למיטב בדיקתי, ע"א 256/08 **סבו נ' ידיעות**; וע"א 1502/09 **עיריית אריאל נ' וואלה תקשורת בע"מ**.

61 ראו בש"א (שלום י-ם) 4995/05 **פלונית נ' בזק בינלאומי בע"מ** (פורסם בנבו, 28.2.2006, השופטת מיכל אגמון-גונן) (להלן: עניין **בזק בינלאומי**); עניין **מור מחוזי**, לעיל ה"ש 7, בפסקאות 27, 29, 31 ו-34.

62 ראו, למשל, עניין **בזק בינלאומי**, לעיל ה"ש 61; עניין **מור מחוזי**, לעיל ה"ש 7, בפסקה 27.

63 זו עמדתה של השופטת פלפל בעניין **מזמור**, לעיל ה"ש 4, ובה"פ (מחוזי ת"א) 250/08 **חברת ברוקרטוב בע"מ נ' חברת גוגל ישראל בע"מ** (פורסם בנבו, 7.1.2009). השופטת פלפל מתארת בפסקי דינה את האנונימיות באינטרנט בצורה ספקנית ואף עוינת משהו ("הטבע האנושי הוכיח את עצמו, שאנונימיות מוחלטת עלולה לגרום גם לזרימתו של רוע, רצון להזיק, וניסיון להחליף את הדיון מגופו של עניין, לדיון בגוף או בגופה עצמם" – עניין **מזמור**, לעיל ה"ש 4, בפסקה ד).

64 ראו עניין **מור**, לעיל ה"ש 2, בפסקת הסיום של פסק דינו של השופט ריבלין.

65 שם, בפסקה מו לפסק דינו של השופט רובינשטיין.

יש גם זכות גישה לערכאות.[66] בחלק מהמקרים התייחסו בתי המשפט לתוכן הדברים שנאמרו וקבעו כי על פניהם אין בהם משום לשון הרע ובכך תם הדיון בבקשה.[67] בחלק אחר של המקרים לא חסכו בתי המשפט את מורת רוחם מרמתו הירודה של השיח המקוון והפנו אצבע מאשימה, בין היתר, לאנונימיות;[68] חלקם אף גזר מכך מסקנה מעשית: הנחיה לחשיפת הגולשים.[69]

3. עמדתם של בתי המשפט

בפסיקה הישראלית שעד עניין **מור** אפשר היה לאתר שלוש גישות לשאלת החשיפה של הגולשים האנונימיים, אלא שעניין **מור** סתם לפי שעה את הגולל על אפשרות החשיפה בבתי המשפט – לפחות עד שהמחוקק יתערב או עד שבית המשפט העליון יאמץ עמדה אחרת.

(א) עמדתו של בית המשפט העליון בעניין מור

בעניין **מור** דובר בתגובות אנונימיות שהופיעו באתר אינטרנט המוקדש לבריאות. מור הוא מטפל אלטרנטיבי במחלות עור. בתגובות נכתבה ביקורת בוטה וקצרה על מור ובין

---

66 ראו, למשל, עניין **בזק בינלאומי**, לעיל ה"ש 61, בפסקה 7(ג); עניין **מור מחוזי**, לעיל ה"ש 7, בפסקה 33 לחוות דעתו של המשנה לנשיאה ריבלין; בש"א (שלום חי') 1238/07 **מור נ' ברק 013 שירותי אינטרנט בע"מ**, בפסקאות 14-15 (פורסם בנבו, 15.4.2007, השופטת בטינה טאובר) (להלן: עניין **ברק 013**); בש"א (שלום ת"א) 173201/06 **לוי נ' בזק בינלאומי בע"מ**, פסקה 15(ב)(3) (פורסם בנבו, 25.10.2006, השופט מאיר יפרח) שם תואר האינטרס ב"מיצוי זכויות חוקיות"; בש"א (שלום י-ם) 2403/09 **אריאל נ' גוגל ישראל בע"מ** (פורסם בנבו, 2.7.2009, השופט עודד שחם).

67 ראו ת"א (מחוזי ת"א) 2433/07 **עיריית אריאל נ' וואלה תקשורת בע"מ** (פורסם בנבו, 18.1.2009, השופט אבי זמיר).

68 בעניין **מור מחוזי**, לעיל ה"ש 7, שיבח השופט עמית את האנונימיות אך לצד זה עמד גם על חסרונותיה, למשל בפסקה 30: "אם אור השמש הוא המחטא הטוב ביותר, אזי העלטה האנונימית מעודדת הפקרות ואנרכיה".

69 זו עמדתה של השופטת פלפל. ראו עניין **מזמור**, לעיל ה"ש 4, בפסקה ד: "השיח הציבורי יכול להיות שוטף ואנונימי, כל אימת שהוא ענייני; ברגע שהבמה האלקטרונית הופכת לזירת אגרוף בבוץ, צריך המתפלש בבוץ להבין ולהפנים שאם זרק בוץ על מאן דהוא ובכך לכאורה יש עבירה או עילת תביעה בנזיקין או בקניין רוחני, זכאי אותו נפגע לדעת מיהו זורק הבוץ [...]". בעניין **ברוקרטוב**, לעיל ה"ש 63, בפסקה ד, כתבה השופטת כך: "החיסרון אולי 'הים־תיכוני' של מכשיר מעין זה [שיח אנונימי; מ' ב'] הוא שלעתים במקום לדון לגופו של עניין, נסחפים הגולשים לדון לגופו של מגיב, לעתים בצורה בוטה, גסה, ולהעיר הערות מכוערות גם לגולשים אחרים, שאינם בדעתם".

היתר הוא כונה "שרלטן". בהליכים קודמים השיג מור את כתובת ה־IP של הגולשים המגיבים (מה שכונה לעיל "התחנה הראשונה לחשיפה") ושם פעמיו לספק שירות הגישה לאינטרנט ("התחנה השנייה"). בית המשפט המחוזי אימץ גישת ביניים, לעומת גישות אחרות שנקבעו בפסיקה המחוזית, שלפיה אפשר להורות על חשיפת פרטיו של הגולש האנונימי בהתקיים "דבר מה נוסף". בצד זה קבע בית המשפט המחוזי שורה של אמצעים דיוניים לקיומו של הליך החשיפה, בין היתר שבית המשפט ישמש כמעין מתווך בין הצדדים במקרים המתאימים.[70]

בבית המשפט העליון נחלקו הדעות.[71] דעת הרוב, מפי השופט ריבלין ובהסכמת השופט לוי, מצאה כי אין כלל מסגרת דיונית מתאימה וכי אין זה מתפקידו של בית המשפט ליצור כזו יש מאין. השופט ריבלין בחן אפיקים שונים שבהם צעדו בתי המשפט בערכאות הנמוכות, כמו הסמכות הכללית של בתי המשפט ליתן סעד (סעיף 75 לחוק בתי המשפט [נוסח משולב], התשמ"ד-1984) או פקודת הנזיקין, ומצא כי אינם מקימים סמכות מתאימה לתביעות נגד נתבעים אנונימיים (אלה המכונים בפסיקה האמריקנית John Doe, ובתרגומו של בית המשפט – "רן דן"). מעניין כי בשולי פסק הדין הזכיר השופט את סעיף 16 לחוק הגנת הפרטיות, הקובע חובת סודיות של בעל מאגר מידע, כמקור סמכות, אולם הותיר את השאלה לעיון אחר. השופט רובינשטיין, בדעת מיעוט, דווקא מצא מסגרת משפטית מתאימה וסעד: חובת העדות של ספק האינטרנט בבית המשפט, שאותה ביקש להרחיב לנסיבות של חשיפת פרטי הגולשים.

אולם המחלוקת בין השופטים איננה רק עניין של סדרי הדין. כפי שציינתי לעיל, בלב המחלוקת עמדה הבנתם את מקורותיה העיוניים של האנונימיות (כנגזרת של חופש הביטוי והזכות לפרטיות גם יחד מחד גיסא או כמקרה מצומצם של חופש הביטוי מאידך גיסא), ולפיכך את מעמדה של האנונימיות (כזכות בעלת מעמד חוקתי מחד גיסא או כ"נסיבה אקראית" מאידך גיסא), ויותר מכך: הבנתם את היחס שבין המשפט לטכנולוגיה של האינטרנט.

השופט ריבלין הציג הבנה עשירה ורחבה של יחס זה. לאחר שעמד על החשיבות החוקתית של האנונימיות כמאפשרת ביטוי ושמירה על הפרטיות, הוא זיהה את תפקידה של האנונימיות ביצירת "תרבות הגלישה באינטרנט"; את מרחב הגלישה הוא זיהה כתחום של חופש: "בגבולות ראויים ראוי לשמר את מקלטי האנונימיות כחלק מתרבות הגלישה באינטרנט. ניתן לומר כי במידה רבה האנונימיות עושה את האינטרנט למה שהוא, ובלעדיה

---

70 עניין מור מחוזי, לעיל ה"ש 7.
71 עניין מור, לעיל ה"ש 2.

ייגרע מן החופש במרחב הווירטואלי״. לפי עמדה זו, הגולשים מגיבים לטכנולוגיה ומפתחים ציפייה מסוימת – במקרה זה, לאנונימיות. מאחר שהשופט מצא שהאנונימיות ראויה, מסקנתו היא ש״ניפוץ ׳אשליית האנונימיות׳, במציאות שבה תחושת הפרטיות של הגולש היא מיתוס, עלול לעורר אסוציאציות של ׳אח גדול׳. פגיעה זו ראוי למזער.״ יתרה מכך: השופט הבין כי כל התערבות משפטית תשפיע על התנהגות הגולשים: ״ככל שתתרחב האפשרות לעלות על העקבות הנותרים בחלל הווירטואלי, יש לצפות לשינוי מהותי בדפוסי ההתנהגות של המשתמשים״.[72]

השופט רובינשטיין הציג בדעת המיעוט עמדה צרה יותר, לאחר שבחן את טיבה של האנונימיות ואפיין אותה כנתון אקראי בלבד, תוך דחיית המעמד החוקתי שעליו הצביעה דעת הרוב. גם הוא זיהה את קיומה של ציפייה אפשרית לאנונימיות אולם הוא ביקש לנפץ אותה: ״במובן זה, אין – ולא יכולה להיות – לספקית האינטרנט ציפיה מוגנת, כי לעולם לא תיאלץ למסור את פרטי לקוחותיה, וללקוחות אין ציפיה מוגנת שפרטיהם לעולם לא יימסרו. לפי המצב המשפטי הנוכחי, גם הספקית וגם הלקוחות צריכים להיות מודעים לכך, שמעל דוכן העדים תהיה הספקית חייבת למסור את המידע שברשותה״.[73]

במונחיו של לורנס לסיג,[74] דעת הרוב המשיגה את הדיון במרחב שבין הטכנולוגיה (שמאפשרת אנונימיות אך גם את הסרתה), הנורמות החברתיות (תרבות הגלישה) והמשפט (המעמד החוקתי של האנונימיות), תוך הבנה שהנורמות החברתיות (התנהגות המשתמשים) יגיבו לכלל המשפטי. דעת המיעוט המשיגה את הדיון במרחב שבין הטכנולוגיה (שמאפשרת אנונימיות באופן אקראי) למשפט (שמקנה רק מעמד מצומצם של האנונימיות כאגבית לחופש הביטוי בלבד), תוך הכפפה של הטכנולוגיה והנורמות החברתיות לכלל המשפטי (הקביעה שאין ציפייה מוגנת לאנונימיות).

המשגה זו של דעת הרוב מול דעת המיעוט במסגרת שהציע לסיג מחדדת את הדמיון והשוני ביניהן. שתי העמדות יוצאות מנקודת מבט ערכית: השיקול המרכזי שמניע את שתי העמדות הוא הבנת האנונימיות באופן ערכי (כאשר לגופה של העמדה הערכית, דעת הרוב ודעת המיעוט משקפות מחלוקת עמוקה ובלתי ניתנת לגישור בקשר למהות האנונימיות). עוד בצד המשותף, שתי העמדות אינן מבטלות את תפקיד המשפט בסביבה הטכנולוגית ולפיכך שתיהן דוחות במשתמע תפיסות טכנולוגיות דטרמיניסטיות. אולם הדעות מחזיקות בעמדות שונות בדבר כוחו של המשפט ביחס לטכנולוגיה. בעוד שדעת הרוב הייתה ערה

---

72 שם, בפסקה 16 לפסק דינו.
73 שם, בפסקה יג לפסק דינו.
74 לעיל ה״ש 5.

לדינמיות של יחסי הגומלין שבין המשפט לטכנולוגיה ולהשפעה של שני אלה על הנורמות החברתיות, דעת המיעוט התייחסה לקשרים אלה כחד־סטריים, שבהם המשפט גובר על הטכנולוגיה. דעת המיעוט גם החמיצה את האפשרות של תגובה של הנורמות החברתיות לכלל המשפטי. יצוין כי גם דעת הרוב וגם דעת המיעוט התעלמו מהאפשרות של תגובה טכנולוגית לכלל המשפטי (ובכך אדון בהמשך המאמר); עוד יצוין כי במסגרת של לסיג יש קודקוד נוסף – הנורמות של השוק – שלא נדון בפסק הדין.

(ב) הגישה בפסיקה שקדמה לעניין מור

המחלוקת בבית המשפט העליון בשאלת האנונימיות משקפת במידה מסוימת את המחלוקות בערכאות הנמוכות, שגיבשו – עד שנסתם הגולל על אפשרות החשיפה – שלוש עמדות יריבות.

הראשונה, פרי עטה של השופטת ד"ר מיכל אגמון־גונן בעניין **בזק בינלאומי**,[75] קבעה רף גבוה במיוחד, שרק בהתקיימו יורה בית המשפט על חשיפת הזהות. דובר שם בבקשה של עובדת מדינה בכירה לחשוף את זהותם של גולשים אנונימיים שכתבו דברי בלע עליה ועל בִּתָּה, כלשון בית המשפט, בתגוביות לכתבה באחד האתרים. התגוביות עסקו בהרגליה המיניים של האישה, בזהות של אבי־בִּתָּה ובטענות בדבר גניבת כספים. בית המשפט דן בהרחבה בזכויות הצדדים, בשאלה של חופש הביטוי ברשת וכן בתפקיד של ספקי השירות במערך זה. האנונימיות הומשגה שם כנגזרת של חופש הביטוי ובמידה מסוימת כנגזרת של הזכות לפרטיות, וכן נזכרה זכותם של הנפגעים לנגישות לערכאות משפטיות.[76] לפיכך, קבעה השופטת רף גבוה, שלפיו (בהליך האזרחי) יש להראות חשש של ממש כי לשון הרע מגיעה לרף פלילי. רף זה מחייב הוכחת כוונה לפגוע וזו יכולה להילמד מתוכן הפרסום ומהנסיבות.[77] למרות הרף הגבוה, הורתה השופטת על חשיפת הזהות בשל נסיבות המקרה

---

75 עניין **בזק בינלאומי**, לעיל ה"ש 61. עמדה זו אומצה בשורה של החלטות ופסקי דין: בש"א (שלום חי') 5478/06 **קי.אס.פי. מחשבים בע"מ נ' ברק אי.טי.סי. 1995 והחברה לשירותי בזק בינלאומיים בע"מ** (פורסם בנבו, 13.8.2008); עניין **ברק 013**, לעיל ה"ש 66; בש"א (שלום ראשל"צ) 4470/07 **ברלומנפלד נ' Google, Inc.** (פורסם בנבו, 25.11.2007, השופט אורן שוורץ); בש"א (שלום ת"א) 61825/07 **מנסור נ' חלבי** (פורסם בנבו, 14.1.2008, השופטת זהבה אגי); בש"א (שלום ת"א) 152863/08 **פלח נ' דוקטורס** (פורסם בנבו, 12.2.2008, השופטת בלהה טולקובסקי) (עניין **פלח** נהפך בערעור בבית המשפט המחוזי: ע"א 1806/09 **פלח נ' שירותי בריאות כללית** (פורסם בנבו, 16.3.2010, השופט זאב המר)).

76 עניין **בזק בינלאומי**, לעיל ה"ש 61, בפסקה 5 (חופש הביטוי והזכות לפרטיות) ובפסקה 7(ג) (נגישות לערכאות).

77 שם, בפסקה 8(א).

ובעיקר בשל חומרת הפרסומים ובשל העובדה שנכתבו שלושים ואחת תגוביות – אולם התברר שכולן נכתב על ידי גולשים יחידים (כלומר מאותה כתובת IP) ובחלקן השתמשו בשמה של הנפגעת.

במקרה נוסף, **סבו נ' ידיעות תקשורת**, שנפסק גם הוא על ידי השופטת אגמון־גונן, הפעם בבית המשפט המחוזי, דובר בטענות אנונימיות שהועלו כנגד מתמודד לראשות עיריית קרית אונו בפורום מקוון לתושבי העיר באתר ynet.[78] הגולש, שכינה עצמו "צחי200", העלה טענות שונות על התנהלותו של סבו; זה האחרון ראה בהן פגיעה בשמו הטוב וביקש לחשוף את זהותו של "צחי200". השופטת חזרה על עמדתה העקרונית אבל התוצאה הפעם הייתה שונה עקב השוני בנסיבות: בעוד שבעניין **בזק בינלאומי** דובר בהשמצה של עובדת מדינה בעניינים פרטיים, בעניין **סבו** דובר באיש ציבור ובטענות בעניינים ציבוריים, שקשורות לזירה המקומית (סגירת פרגולה ללא רישיון, הפעלת קשרים ברשות המקומית וכדומה – עניינים שסבו כופר בהם ונפגע מהם). משום שמדובר בביטוי פוליטי בהקשר ציבורי, תוך התבססות על הלכות יציבות של בית המשפט העליון, קבעה השופטת כי אין להורות על חשיפת פרטיו של הגולש. עם זאת אימצה השופטת אגמון־גונן מקצת מההסדרים הדיוניים שהציעו בתי המשפט האחרים שדנו בסוגיה ובעיקר מיצוי אפשרויות, כלומר: שהמבקש יפנה קודם לתובע בפורום שבו מדובר בבקשה שיחשוף את זהותו.[79]

גישה שנייה, בעניין **מור נ' ידיעות אינטרנט**, שהיה מושא הערעור בעניין **מור**, פרי עטו של השופט יצחק עמית בבית המשפט המחוזי בחיפה, קבעה רף מהותי נמוך יותר מזה שנקבע בעניין **בזק בינלאומי** ובעניין **סבו**, אולם הציעה שורה של אמצעים דיוניים חשובים.[80] בצד המהותי הנחה השופט עמית כי על המבקש להראות "דבר מה נוסף", והציע כמה מבחנים: הגשת התביעה בתום לב, הוכחת סיכויי זכייה טובים (ולא רק סיכוי לשרוד בקשה למחיקה על הסף שנענית רק לעתים רחוקות), התייחסות לסוג הביטוי – פוליטי,

---

78 ה"פ (מחוזי ת"א) 541/07 **סבו נ' ידיעות אינטרנט (שותפות רשומה)** (פורסם בנבו, 11.11.2007, השופטת מיכל אגמון־גונן).

79 **שם**, בעמ' 41.

80 עניין **מור מחוזי**, לעיל ה"ש 7. טרם פסק הדין בבית המשפט העליון, אומצה גישה זו בכמה החלטות ופסקי דין. ראו בש"א (שלום ת"א) 151638/07 **לוי נ' בזק בינלאומי בע"מ** (פורסם בנבו, 26.3.2008, השופטת אביגיל כהן); בש"א (שלום ת"א) 180513/08 **ערב ערב באילת נ' פלוני/ת** (פורסם בנבו, 25.12.2008, השופטת בלהה טולקובסקי); בש"א (שלום ת"א) 178523/08 **פריד נ' פלוני אלמוני** (פורסם בנבו, 23.12.2008, השופטת בלהה טולקובסקי); ת"א (שלום ת"א) 22992-09-09 **מכון התקנים הישראלי נ' אלמוני** (פורסם בנבו, 15.11.2009, השופטת חדוה וינבאום וולצקי).

פוליטי, מסחרי או פרטי, זהותו של המבקש הנפגע (אם מדובר באיש ציבור או באדם פרטי), עוצמת הביטוי הפוגעני, נסיבות הפרסום (חד־פעמי או שיטתי, משך הפרסום וכדומה), טיב הזירה המקוונת (מתוך הנחה שהציבור מייחס משקל שונה לתוכן לפי זירת הפרסום) והמשקל המשוער שנותנים הקוראים לתוכן. על כל אלה, הוסיף השופט עמית את מבחן המידתיות הבוחן תועלת מול נזק.[81] המרכיב הדיוני שהציע השופט עמית כולל מיצוי של אפשרויות חשיפה מרצון, כלומר: פניה של הנפגע לגולש האנונימי בזירה המקוונת שבה מדובר, פרסום דבר התביעה, מתן אפשרות לגולש האנונימי לפנות לבית המשפט בלי שזהותו תיחשף כדי להתנגד לחשיפה ולבסוף נשיאה בעלויות מצד המבקש.[82]

גישה שלישית, פרי עטה של השופטת דרורה פלפל בבית המשפט המחוזי בתל־אביב, קבעה רף נמוך עוד יותר. בעניין **מזמור הפקות בע"מ נ' מעריב הוצאת מודיעין בע"מ**, שעסק בתגובית אנונימית נגד המבקשת, חברת הפקות שסיפקה שירותים לערוץ ספורט,[83] ובהמשך בעניין **חברת ברוקרטוב בע"מ נ' חברת גוגל ישראל בע"מ**, שעסק בבקשה לחשיפת זהותו של מי ששלח דואר אלקטרוני ששמח לאידם של המבקשת ומנהלהּ בסמיכות לעוולות מסחריות שבוצעו כנגד אתר אינטרנט של המבקשת, הקלה השופטת פלפל עם מבקשי החשיפה.[84] פרשנותה אחזה בביטוי "חשש של ממש" שבהצעת חוק מסחר אלקטרוני.[85] יישום המבחן המקל הביא להורות על חשיפת זהות הגולשים.[86]

---

81 עניין **מור מחוזי**, לעיל ה"ש 7, בפסקה 38.

82 שם, בפסקה 40.

83 עניין **מזמור**, לעיל ה"ש 4.

84 עניין **ברוקרטוב**, לעיל ה"ש 63. מפסק הדין לא ברור הקשר בין שולח הדוא"ל לבין העוולות; ראו בייחוד פסקה ח לפסק הדין. גישה זו אומצה בפסיקה נוספת, ראו עניין **אריאל**, לעיל ה"ש 66, שם הורה בית המשפט על חשיפת פרטיו של מחזיק בכתובת דוא"ל. באותו מקרה דובר בתביעת לשון הרע נגד מוציא לאור של עיתון מודפס ששמר על אנונימיות; ת"א (מחוזי חי') 914/07 **כהן נ' נטוויז'ן 013 ברק בע"מ** (פורסם בנבו, 12.5.2009, השופט אלכסנדר קיסרי), אם כי שם העלה השופט את הרף הנדרש להוכחת לשון הרע, דבר שהביא לדחיית הבקשה למרות אימוץ גישתה של השופטת פלפל.

85 עניין **מזמור**, לעיל ה"ש 4, בפסקה ד; מצוטט גם בעניין **ברוקרטוב**, לעיל ה"ש 63, בפסקה ט. ראו בדומה גם עניין **עיריית אריאל**, לעיל ה"ש 67.

86 מאחר ששלוש הגישות יוצרות מדרג, היו בתי משפט שדחו בקשות לחשיפת זהות, שהזכירו את העמדות שמקלות יותר על חשיפת הזהות, ונימקו כי אפילו לפי גישות אלה אין לחשוף את הפרטים המתבקשים. כך למשל, בבש"א (שלום ת"א) 160133/08 **הרודס בניה ופיתוח (1990) בע"מ נ' מעריב הוצאת מודיעין בע"מ** (פורסם בנבו, 11.5.2008, השופטת ריבה ריב) קבעה השופטת כי אפילו לפי הגישה המקלה בעניין מזמור, לעיל ה"ש 4, אין מקום להורות על החשיפה. בעניין **עיריית אריאל**, לעיל ה"ש 67, אומץ המבחן המקל, אולם נקבע כי הודעות דוא"ל אנונימיות שנשלחו לראש העירייה אינן בגדר לשון הרע.

4. הצעת חוק מסחר אלקטרוני

סעיף 13 להצעת חוק מסחר אלקטרוני הציע כך:

(א) ספק שירותי אינטרנט המספק שירות גישה או שירות אירוח לא יגלה כל פרט, ידיעה או מסמך שהגיעו אליו ושיש בהם כדי לזהות מפיץ מידע, אלא אם כן הסכים לכך מפיץ המידע, במפורש ובכתב, או אם נדרש לכך לפי הוראות כל דין או לפי צו של בית משפט כאמור בסעיף קטן (ב).

(ב) הוכח להנחת דעתו של בית משפט כי קיים חשש של ממש שתוכנו של מידע שהועלה לרשת תקשורת אלקטרונית או הפצתו ברשת כאמור, מהווים עוולה כלפי אדם או הפרת זכות קניין רוחני שלו, רשאי הוא, על פי בקשת אותו אדם, להורות לספק שירותי אינטרנט המספק שירות גישה או שירות אירוח, למסור למבקש פרטים שברשותו שיש בהם כדי לזהות את מפיץ המידע.

(ג) השר יקבע הוראות לעניין הפרטים שיש לציין בבקשה כאמור בסעיף קטן (ב), המסמכים שיש לצרף לה, סדרי הדיון בבקשה והתנאים שבהם ייתן בית המשפט את הסעד המבוקש.

ההצעה ביקשה לעגן את הזכות לאנונימיות ובו־זמנית לסייגה. ייתכן כי הפגיעה באנונימיות – ולכן הפגיעה בזכות לפרטיות – עולה על הנדרש, אולם כאן אני מתמקד בסייג שבס"ק (ב). קל לראות כי נוסח זה כולל שיקול דעת נרחב, תוך שימוש במושג שסתום של "חשש של ממש".[87] ההסדר המוצע כללי למדי והוא חסר (לפי שעה) את התקנות הנלוות של סדרי הדין. מכל זה יוצא כי הצעת החוק – אם וכאשר תתקבל, גם אם ייעשו בה שינויים – טעונה פרשנות ככל חוק וודאי חוק חדש, אבל גם אז מרחב שיקול הדעת השיפוטי שמובנה בה רחב למדי. את ההסדר לחשיפה של זהות הגולשים יש לקרוא עם חלק קודם בהצעת החוק, המקנה לספקי השירות חסינות מפני תביעות בהתקיים תנאים מסוימים.[88]

---

87 למרות שהצעת החוק טרם הפכה לחוק התייחסו בתי המשפט למבחן הסתברותי זה, ועוד קודם פרסום ההצעה, התייחסו לתזכיר החוק של משרד המשפטים. השופטת אגמון־גונן העירה כי זהו מבחן של רמת הסתברות גבוהה יחסית, אולם הטילה ספק ביכולתו של ההסדר המוצע להגן על הגולש. ראו עניין **בזק בינלאומי**, לעיל ה"ש 61, בעמ' 22.

88 לדיון ראו בחלק ד(3) במאמר זה.

כפי שאטען בחלק הבא, קלות התביעה או קושי התביעה נגד ספקי השירות משליכים במישרין על התביעה נגד הגולשים האנונימיים.

5. חשיפת גולשים במדינות אחרות

ההתלבטות בשאלת החשיפה של גולשים אנונימיים איננה ייחודית לישראל. גם שיטות משפט אחרות מתחבטות בשאלת הסטנדרט המשפטי הראוי לחשיפה. בדיקת העמדות המתגבשות בכמה מדינות מעלה שיש דמיון רב במבחנים המשפטיים, הגם שהבסיס הרעיוני לסוגיה מומשג בצורות שונות. אפתח באנגליה ובקנדה, שבהן משטר ההגנה על הפרטיות ועל המידע האישי קרוב יותר לזה הישראלי; אמשיך במשפט האמריקני.

באנגליה, הבסיס המשפטי לפיתוח הסטנדרט המשפטי הוא צו לחשיפת זהותו של אדם אנונימי שניתן בקשר לסביבה פיזית לפני יותר משלושים וחמש שנים בעניין *Norwich Pharmacal*, שעל שמו מכונה צו החשיפה ברשת כיום.[89] באותו מקרה טען בעל פטנט כי יבואן אנונימי מפר את זכויותיו וקיבל צו שחייב את רשויות המכס לחשוף את זהות היבואן המפר. אם כן, באותו מקרה דובר בפעולה פיזית (ייבוא של מוצר מפר), בצו חשיפה שהופנה לגוף ציבורי (רשות המכס) ובפעילות שאין בה היבט של חופש ביטוי. למרות הבדלים משמעותיים אלה החילו בתי המשפט את הצו גם בזירה המקוונת.

פסק הדין המרכזי בעניין חשיפת גולשים נפסק בשנת 2001.[90] בערכאה הראשונה הורה בית המשפט לספק של שירות אינטרנט לחשוף את פרטי הגולשים שהיו בידיו וחייב אותו בהוצאות ההליך. הערעור נסב סביב החיוב בהוצאות אולם בית המשפט לערעורים העיר הערות אגב משמעותיות. השופטים עמדו על טיבו החד־צדדי של ההליך ועל המלכוד שבו נתון ספק השירות (בין הגולש האנונימי לבין מי שמבקש את חשיפת הזהות), והבהירו כי הספק רשאי שלא למסור את המידע מרצונו.[91] עוד נכתב בפסק הדין כי לפני שייתן צו חשיפה בית המשפט חייב לברר את זכויותיו של מושא המידע (data subject), כלומר: הגולש האנונימי.[92] הערה מעניינת נוספת של בית המשפט היא שספק השירות יכול לשמש מתווך בין המבקש לבין הגולש האנונימי.[93]

---

89 Norwich Pharmacal Co v. Customs & Excise Commissioners [1974] AC 133 (H.L. 1973).

90 Totalise Plc v. The Motley Fool Ltd. [2001] EWCA Civ. 1897.

91 לטיב ההליך ראו שם, בפסקה 22; למלכוד הספק ראו שם, בפסקה 17; להיעדרה של חובת הספק ראו שם, בפסקה 28.

92 שם, בפסקה 24.

93 שם, בפסקה 26.

בהמשך נשמרו בפסיקה העקרונות האלה. כך, למשל, בתביעה של בעלי קבוצת כדורגל לחשוף את זהותם של גולשים אנונימיים שכתבו נגדם מסרים שונים באתר האוהדים של הקבוצה,[94] בית המשפט מנה שיקולים מהותיים שיש לשקול בבקשה מעין זו. בין השאר ציין כי עליו להשתכנע שאכן בוצעה עוולה על ידי הגולש האנונימי, שיש קשר בין בקשת החשיפה לבין מימוש התביעה כנגד המעוול ושספק השירות יכול לספק את המידע הדרוש. בית המשפט מנה שיקולים נוספים ובהם עוצמת התביעה הלכאורית, עוצמת הביטוי הפוגעני, בדיקה אם המעוול לכאורה ניהל "קמפיין" נגד המבקש ואם ניצל את האנונימיות שהאתר מאפשר, אם היו למבקש אפיקים חלופיים לזהות את הגולש ומה המדיניות של האתר בנושא.[95] בית המשפט הבהיר כי הוא מאזן בין הזכות לשם טוב של המבקש לבין האנונימיות והביטוי של הגולשים.[96] יישום המבחנים באותו מקרה הביא לצו לחשיפה של חלק מהגולשים ולדחיית הבקשה לחשיפה נגד רוב הגולשים האנונימיים.

השיקולים והמבחנים דומים לאלה שמתגבשים בפסיקה הישראלית. מעניין לשים לב לדרך ההמשגה של זכויות הגולש: הן מוצגות גם כזכות לביטוי – בדרך כלל בהערות אגב, אך בעיקר הן מוצגות כזכות לפרטיות. בתי המשפט דנו בזכויותיו של הגולש במשקפיים של חוק הגנת המידע (Data Protection Act) ובמשקפיים של הזכות לפרטיות הקבועה בחוק זכויות האדם (Human Rights Act משנת 1998), המגן על פרטיותם של מושאי המידע בכל הנוגע לחשיפת מידע על אודותיהם. המשגה זו מצרפת את הפרטיות וחופש הביטוי יחדיו, אולם המשקל העיקרי ניתן לפרטיות והמשקל הטפל ניתן לחופש הביטוי. גישה זו באה לידי ביטוי גם בפסק דין מהעת האחרונה, שבו התיר בית משפט אנגלי לחשוף את זהותו של בלוגר אנונימי שמתח ביקורת על המשטרה.[97] האינטרס של הבלוגר באנונימיות הומשג שם במסגרת של הזכות לפרטיות. בית המשפט החיל את מבחן "הציפייה הסבירה" וקבע כי כתיבת בלוגים היא פעולה פומבית במהותה ולכן לא יכולה להיות לבלוגר ציפייה סבירה לאנונימיות. בית המשפט הוסיף וקבע כי גם אילו הייתה הפעולה פרטית יש לציבור אינטרס לדעת מיהו המבקר. אני סבור ששתי הקביעות שגויות מיסודן, אולם לענייננו חשובה המשגת האנונימיות במסגרת הזכות לפרטיות כדבר מובן מאליו.

בקנדה הגיעו בתי המשפט למסקנות דומות. הדין הקנדי אימץ את הגישה האנגלית לחשיפת זהות מתחום הפטנטים (צו Norwich Pharmacal) ויישם אותו בקשר לחשיפת גולשים אנונימיים באינטרנט, אם כי היישום היה זהיר מזה האנגלי והתמקד בהקשר של

---

94 Sheffield Wednesday Football Club Ltd. v. Hargreaves [2007] EWHC 2375 (Q.B.D).

95 שם, בפסקאות 11-12.

96 שם, בפסקה 18.

97 The Author of a Blog v. Times Newspapers Ltd. [2009] EWHC 1358 (Q.B.D).

הפרת זכויות יוצרים באמצעות תוכנות לשיתוף קבצים.[98] בפסק הדין המרכזי בסוגיה הבהיר בית המשפט הפדרלי לערעורים כי שיקולי הפרטיות נסוגים מפני ההגנה על הקניין הרוחני במקרים שבהם הפעולה המפרה מאיימת לשחוק את זכות היוצרים.[99] האיזון הזה תורגם לדרישה שלפיה מבקש החשיפה יראה לבית המשפט כי בידו עילת תביעה תמת־לב. הובהר כי הרף הגבוה יותר של הוכחת עילה לכאורה אינו נדרש בשלב של בקשת החשיפה מאחר שבשלב זה אין בידיו של בית המשפט די ראיות לבחון זאת.[100] לבחירה עקרונית זו נלוותה אזהרה משמעותית: מחמת חלוף הזמן יש חשש משמעותי לזיהוי שגוי של הגולשים, דבר העלול להוביל לפגיעה בפרטיות ולתביעות נגד מי שאינם קשורים כלל להפרה.[101]

גם המשפט האמריקני הגיע למבחנים דומים למדי לאלו שמתגבשים בישראל ובאנגליה, אולם ההמשגה שם של זכות הגולש לאנונימיות היא כמעט רק במונחים של חופש הביטוי. את הדין האמריקני יש לקרוא על רקע ההגנה החזקה שניתנת בו לספקי השירות: הדין האמריקני מעניק לספקי השירות חסינות כמעט מוחלטת מפני אחריות לפעולות פוגעניות של צדדים שלישיים, למעט במקרה של קניין רוחני שאז יש מנגנון של הודעה והסרה.[102] בצד זה, פעולות ביטוי אנונימיות נהנות מהגנה חזקה מאוד של התיקון הראשון, המגן על חופש הביטוי, אולם האנונימיות איננה נגזרת שם מהזכות לפרטיות. יוצא שפרטיותו של גולש שאינו דובר חלשה מאוד בהשוואה למידת ההגנה שהוא מקבל בישראל, במיוחד מול גורמים אזרחיים (להבדיל ממדינתיים); אולם "גולש־דובר" יזכה להגנה חזקה יותר.

הדין האמריקני אינו כולל הסדר דיוני אחיד לעניין חשיפת זהותם של גולשים. יש כמה הליכים אפשריים – חלקם במישור הפדרלי וחלקם במישור המדינתי, חלקם כולל הוראות מיוחדות לפי סוג ההפרה (זכות יוצרים) או לפי סוג הספק (חברת שידורי כבלים) וחלקם מבוסס על הוראות כלליות (כללי סדר הדין האזרחי).

---

98 לדיון כללי ראו Ian Kerr & Alex Cameron, *Nymity, P2P & ISPs: Lessons from BMG Canada Inc. v. John Doe*, *in* PRIVACY AND TECHNOLOGY OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 269 (Katherine Strandburg & Daniela Stan Raicu eds., 2005).

99 BMG Canada Inc. v. John Doe [2005] FCA 193.

100 שם, בפסקאות 32-34, 40-41. בית המשפט הוסיף שיקולים אחרים – מיצוי חלופות לחשיפה ושיפוי של ספק השירות בגין הוצאותיו בקשר להליך ולחשיפה, שם, בפסקה 34.

101 שם, בפסקאות 21, 42-43.

102 להסדר הכללי ראו 47 U.S.C. §230 (1996); ראו גם פרשנותו בעניין Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), והשוו להסדר הנקוט שם בקשר לזכויות יוצרים – 17 U.S.C. §512 (1998).

ההסדר הדיוני הכללי שנקבע בכללי סדר הדין האזרחי הוא של צו משפטי מעין־שיפוטי – subpoena.[103] הצו מוצא לבקשת תובע, על ידי פקיד בית המשפט ולא על ידי שופט. אם נמען הצו מתנגד לו הצדדים מופנים לדיון שיפוטי, בין לפי בקשה של המבקש לאכוף את הצו ובין לפי התנגדות של הנמען או של צד שלישי.[104] בעניינו, הצו מופנה לספק השירות, שיכול לציית לו או להתנגד לו ובכלל זה לבקש את ביטולו, וגם מושאי הצו – כלומר: הגולשים – יכולים לבקש את ביטולו, בין מטעמים טכניים ובין מטעמים מהותיים.[105]

הסדרים סטטוטוריים אחרים חלים כשספק שירות הגישה לאינטרנט הוא חברה של תשתית כבלים. החוק המסדיר קובע חובת סודיות שחלה על הספק, בחריגים מסוימים. אחד החריגים הוא צו בית משפט המורה על גילוי המידע, תוך שיש להודיע ללקוח על כך.[106]

כאשר מדובר בהפרה של זכויות יוצרים, החוק האמריקני קובע הסדר מפורט יחסית לחשיפת זהותו של גולש, הסדר הנשען גם על כללי סדר הדין האזרחי הכלליים.[107] לפי ההסדר בעל זכות יוצרים יכול לפנות לפקיד בית המשפט בבקשה להוציא צו (subpoena) שיורה לספק שירות לחשוף גולש שהפר לכאורה זכויות. את הבקשה יש ללוות בתצהיר

---

103 Federal Rules of Civil Procedure, Rule 45.

104 שם, Rule 45(c)(2)(B).

105 לשם כך בידי הגולשים לשגר עורכי־דין מטעמם בלי שפרטיהם שלהם ייחשפו. ראו, למשל, בעניין Doe. v. 2TheMart.com Inc., 140 F. Supp.2d 1088 (W.D. Washington, 2001), שעסק בהודעות אנונימיות בפורום בקשר לתביעה נגזרת של בעלי מניות נגד תאגיד. הגולשים האנונימיים לא היו נתבעים אלא עדים פוטנציאליים בתביעה.

106 ראו 47 U.S.C. §551(c)(2)(B) (1996).

107 בתביעות בגין זכויות יוצרים, נזקק בעל הזכויות בדרך כלל ל"תחנה אחת" בלבד לשם איתור הגולש האנונימי, שכן הוא יכול להתחזות לגולש בעצמו ברשת לשיתוף קבצים וכך להשיג ללא קושי את כתובת ה־IP של המחשב שבו נעשה שימוש (אם כמה אנשים השתמשו במחשב יש צורך בתחנות נוספות). גם ראיות מושגות בדרך זו: עצם העברת הקובץ היא העתקה וכאשר הקובץ כולל יצירה בבעלות התובע, הגולש יוכל לטעון לכל היותר כי מתקיימת הגנה כלשהי בעניינו. הגנת השימוש ההוגן למצב של העתקת קבצים היא אפשרית אך תהיה דחוקה למדי ברוב המקרים. הפעולה של שיתוף קבצים אולי חוסכת לגולש את רכישת הקובץ החוקי, אולם ההיבטים הביטויים שיש בפעולה כזו מצומצמים מאוד. ראו Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535, 545 (2004), וכן עניין *London Sire*, לעיל ה"ש 22, בעמ' 163, שהיה מוכן לקבל טענה זו. גישה זו חריגה, שכן בתי המשפט בארצות־הברית מתקשים לקבל את הטענה בדבר קונפליקט בין חופש הביטוי לזכויות יוצרים. לדיון ראו Michael D. Birnhack, *The Copyright Law and Free Speech Affair: Making-Up and Breaking-Up*, 43 IDEA 233 (2003) (להלן: Birnhack, *Copyright*).

ובהודעה על ההפרה שהופנתה לספק השירות עצמו.[108] בית המשפט בערכאת ערעור פדרלית פירש את הסעיף כך שהוא מכוון רק לספקים של שירות אירוח אך לא לספק שירותי גישה.[109] בין השנים 2003-2008 הגיש ארגון בעלי הזכויות במוסיקה (Recording Industry Association of America – RIAA) לא פחות מ־35 אלף תביעות נגד גולשים. ברוב המקרים הסתיימו ההליכים בפשרה או בזכייה של התובעים. למרות זאת, בשלהי שנת 2008 הודיע הארגון כי יפסיק לתבוע גולשים אנונימיים וכי במקום זאת גיבש תכנית אכיפה בשיתוף של ספקי השירות, שישמשו זרוע ארוכה של בעלי הזכויות, יודיעו לגולשים על דבר ההפרה וינקטו סנקציות מסוימות – תוך שמירה על אנונימיות הגולשים כלפי בעלי הזכויות.[110]

בתי המשפט המדינתיים מתחבטים בשנים האחרונות בהסדר הראוי בתוך המסגרת הדיונית הכללית הזו, ובתי המשפט הפדרליים מתחבטים בה בקשר לזכויות יוצרים.[111] השיקולים שנזכרו בפסיקה שם הם זכותו של המבקש לאכוף את זכותו מול חופש הביטוי של הגולשים האנונימיים וחופש הביטוי כלל; תשומת לב רבה ניתנה לחשש מאפקט מצנן שעלול להיות לחשיפת זהות גולשים. בתי המשפט מנסים לתרגם את השיקולים השונים לאמות־מידה משפטיות: עוצמתה של עילת התביעה (המבחנים שהוצעו נעים בין סף נמוך יחסית של עמידה בבקשת מחיקה מחוסר עילה לבין סף גבוה יותר של הוכחת תביעה לכאורה); דרישת תום לב; דרישת רלוונטיות של החשיפה המבוקשת לליבת התביעה וכן היעדר מקור חלופי לגיטימי להשגת המידע.[112] בחלק מהמקרים דרשו בתי המשפט גם הוכחת נזק (בתביעות לשון הרע), ובכל מקרה הציעו הסדרים דיוניים שונים ובמיוחד דרישה החוזרת ומופיעה – יידוע הגולש האנונימי.[113] בתי המשפט חלוקים ביניהם במידה מסוימת

---

108 ראו 17 U.S.C. §512(h) (1998).

109 Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003) (להלן: עניין *Verizon*).

110 ראו Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J. (19.12.2008) www.online.wsj.com/article/SB122966038836021137.html.

111 דיני זכויות יוצרים בארצות־הברית מוסדרים באופן בלעדי במישור הפדרלי (ראו 17 U.S.C. §301 (1998)) ואילו דיני איסור לשון הרע מוסדרים בכל מדינה בנפרד. העיקרון החוקתי הפדרלי של חופש הביטוי מחייב את כל בתי המשפט.

112 ראו, למשל, *In Re Subpoena Dues Tecum to America Online, Inc.*, 52 Va. Cir. 26 (2000); עניין *2TheMart.com*, לעיל ה"ש 105; Dendrite International, Inc. v. John Doe, No. 3, 342 N.J. Super. 134 (2001) (להלן: עניין *Dendrite*); John Doe No. 1 v. Cahill, 884 A.2d 451 (S.Ct. Delaware, 2005); Independent Newspapers, Inc. v. Brodie, 2009 WL ולאחרונה 484956 (Md. App., 2009).

113 ראו, למשל, עניין *Dendrite*, לעיל ה"ש 112.

מסוימת בקשר לפירוט הדרישות האלה ובקשר להרכב השיקולים.[114] גם שם ההלכה טרם התייצבה והמחוקק הסתפק בהצעת המסגרת הדיונית ולא התערב בשיקולים המהותיים, למעט במקרה של זכות יוצרים.

מדינות נוספות מתחבטות בסוגיה וגם בהן האנונימיות מומשגת כחלק מחופש הביטוי או כחלק מהזכות לפרטיות, וגם בהן יש התלבטות בקשר לסוג ההליך, למבחנים המתאימים לחשיפה ולמשמעות שלה.[115] בסיכום ביניים אפשר לומר שהגישה האמריקנית ממשיגה את זכויות הגולש כחלק מחופש הביטוי וכוללת כמה מסגרות דיוניות לחשיפה, לפי הנושא; הגישה האנגלית והגישה הקנדית ממשיגות את הסוגיה תחת הגג של הזכות לפרטיות ומאפשרות חשיפת זהות ביתר קלות, ברוח צו Norwich Pharmacal, כאשר גם בהן – ובעיקר בקנדה – יש התלבטות בדבר הדרך לפיתוח מבחני־המשנה של צו זה. על רקע כל אלה יש מקום לצלול לעומק השדה, להכיר את השחקנים השונים ולעמוד על קשיים שונים של המציאות הטכנולוגית־משפטית. לאחר זיהוי האינטרסים והקשיים אפשר יהיה לפנות לגיבוש פתרון מושכל.

ד. מיפוי השדה המשפטי

לאור פסק הדין בעניין מור ולאחר שתיבחר המסגרת הדיונית המתאימה, מהי הגישה המהותית הראויה? במבט ראשון נראה שהמשפט הישראלי מצויד בכלים שדי בהם כדי לקבוע אם ומתי ראוי לחשוף את זהות הגולש האנונימי. המשגה מתבקשת היא העמדת הזכויות של הנפגע מול זכויותיו של הפוגע, ככל שיש כאלה, ואיזון ביניהן. אכן, שיח הזכויות ושפת האיזונים מושרשים היטב במשפט הישראלי. אנו רגילים להמשיג עימותים

---

114 לסקירת ההתפתחות בפסיקה האמריקנית ראו Nathaniel Gleicher, *John Doe Subpoenas: Toward A Consistent Legal Standard*, 118 YALE L.J. 320 (2008). המחבר מזכיר שיקול ייחודי שלפיו לעתים חלק מהדוברים האנונימיים משתיקים בפועל דוברים אחרים, למשל במקרה של מתקפות מקוונות על רקע שוביניסטי, גזעני או הומופובי. ראו שם, בעמ׳ 324. במקרים כאלה הוא סבור שיש להגן על הביטוי האנונימי של הגולשים במידה פחותה משום שהוא דווקא פוגע בחופש הביטוי ולא מקדם אותו.

115 לסקירה השוואתית של המצב המשפטי באנגליה, בארצות־הברית, בקנדה ובאירלנד ראו T.J. McIntyre, *Online Anonymity: Some Legal Issues*, 10 COMMERCIAL L. PRACTITIONER 1 (2004); לסקירה השוואתית של ארצות־הברית, אנגליה, קנדה, אוסטרליה וניו־זילנד ראו Alexandra Sims, *Court Assisted Means of Revealing Identity on the Internet*, *in* DIGITAL ANONYMITY AND THE LAW – TENSIONS AND DIMENSIONS 271 (C. Nicoll, J.E.J. Prins & M.J.M. van Dellen eds., 2003).

וקשיים שונים כהתנגשות בין זכויות לזכויות אחרות, בין זכויות לאינטרסים או בין אינטרסים מסוג אחד לאינטרסים אחרים; עומד לרשותנו מערך מרשים של נוסחאות שמתאימות למצבי ההתנגשות השונים: איזון אופקי להתנגשות בין זכויות שוות מעמד; איזון אנכי להתנגשויות בין זכויות לאינטרסים בעלי מעמד שונה;[116] וכיום גם פסקת ההגבלה, המעגנת את האיזון האנכי – לפחות ככל שמדובר בזכויות חוקתיות.[117] לפיכך מתבקש שנזהה את הזכויות והאינטרסים שעל הפרק – ודרכנו לפתרון סלולה.

אלא מאי? הסביבה הטכנולוגית הדינמית, טיב האינטראקציות שבהן מדובר, היחס המורכב שבין המשפט לטכנולוגיה וטיבן המורכב של הזכויות שעל הפרק – כל אלה מבהירים כי שפת האיזונים אינה מספקת. זהו מקרה (נוסף) שבו שפה זו משטיחה את הדיון ומזרזת את המשפטנים לפתרון לפני שירדו לעומקה של הסוגיה.[118] אני סבור שיש הכרח להתעכב ולבחון את מכלול הבעיה ואת מורכבותה לפני שאפשר להגיע למסקנות. האיזון יבוא – אולם יש להגיע אליו מצוידים בהבנה עשירה ככל האפשר של השדה הנדון.

חלק זה בוחן את השדה המשפטי המורכב משחקנים שונים בעלי אינטרסים וזכויות. התמונה מורכבת בהרבה מאשר זכות הנפגע לשמו הטוב וזכות הגולש לאנונימיות. כפי שראינו בחלק הקודם, הדיון המשפטי עד כה התמקד בנפגע ובפוגע; כפי שאטען כעת, הדיון הזניח יחסית את תפקידם של ספקי השירות בסוגיה. אני סבור שהבנת תפקידו של ספק השירות היא חיונית לדיון – וכמוה גם לציבור, בין זה שקורא את הדברים ובין זה שהוא דובר פוטנציאלי.

1. הנפגע: התובע

(א) זכות מהותית

לנפגע עומדת בדרך כלל זכות מהותית והוא טוען שזכותו נפגעה. ברוב המקרים שנדונו עד כה בפסיקה הישראלית דובר בזכות לשם טוב; המצב הנפוץ הוא שהפוגע האנונימי פגע בשמו הטוב של הנפגע. במצב זה אתמקד בדברים שלהלן. במקרה אחד הטענה הייתה

---

116 ראו בג"ץ 953/87 **פורז נ' ראש עירית תל-אביב יפו**, פ"ד מב(2) 309 (1988).

117 ראו בג"ץ 10203/03 **המפקד הלאומי בע"מ נ' היועץ המשפטי לממשלה**, בפסקה 29 לפסק דינה של השופטת מרים נאור ובפסקה 7 לפסק דינה של הנשיאה דורית ביניש (פורסם בנבו, 20.8.2008); מיכאל בירנהק "השיח על אודות השיח" **שקט, מדברים! התרבות המשפטית של חופש הביטוי בישראל** 11 (מיכאל בירנהק עורך, 2006) (הספר להלן: **שקט, מדברים!**).

118 לביקורת שפת האיזונים ראו מיכאל בירנהק "הנדסה חוקתית: המתודולוגיה של בית המשפט העליון בהכרעות ערכיות" **מחקרי משפט** יט 591 (2003).

לפגיעה בזכות יוצרים[119] ובמקרה אחר הטענה הייתה לפגיעה באינטרסים מסחריים.[120] במצב רגיל, שבו זהות הפוגע ידועה, תובעים התובעים את כאבם בבית המשפט; ברגיל מוטל עליהם הנטל להוכיח את יסודות העוולה והנתבע, אם יבקש, יטען לטענות הגנה ואז הנטל להוכיחן מוטל עליו.

דיני לשון הרע הם דינים מורכבים ויש בהם שורה של שאלות מפתח שבהן נדרש בית משפט להכריע, בכל מקרה לגופו: האם הדברים "פורסמו"?[121] האם הדברים משפילים או מבזים את האדם?[122] מהו המבחן הראוי – פגיעה סובייקטיבית של התובע או מבחן אובייקטיבי כלשהו?[123] האם חלה אחת ההגנות הקבועות בחוק איסור לשון הרע, כמו הגנת "אמת דיברתי" (פרסום אמת שיש בו עניין ציבורי), או שהפרסום נעשה בתום לב באחת הנסיבות המנויות בחוק?[124] דיני לשון הרע פיתחו שורה של כללים משפטיים המבקשים לגלם את ההגנה על שמו הטוב של האדם, נורמות חברתיות, סיבולת חברתית לביטויים שאינם נעימים או אף שקריים ושיקולים בדבר חופש ביטוי וחופש עיתונות.[125]

חלק מהראיות זמינות ונגישות, ובייחוד במקרה של פרסום ברשת האינטרנט. יש ראיות בדבר הפרסום והטקסט הפוגע לכאורה נמצא גם הוא לפני בית המשפט. גם זהות התובע ידועה ובדיני לשון הרע יש לה חשיבות: מאחר שדיני לשון הרע מגלמים איזון מורכב בין שמו הטוב של האדם לבין חופש הביטוי, ומאחר שהביטוי הפוליטי נהנה מהגנה משפטית מוגברת, פותח בפסיקה מדרג של נפגעים: אין דינו של איש הציבור כדינו של אדם רגיל מן הישוב.[126] לעומת זאת, ראיות בדבר מטרותיו של הפוגע, בדבר אמיתות או שקריות התוכן או בדבר תום לבו או נסיבות ספציפיות שעשויות להקים לנתבע הגנה – כל אלה אינן

---

119 ת"א (מחוזי ת"א) 1636/08 **The Football Association Premier League נ' פלוני** (פורסם בנבו, 2.9.2009, השופטת מיכל אגמון־גונן).

120 עניין **ברוקרטוב**, לעיל ה"ש 63.

121 ראו הגדרת "פרסום" בסעיף 2 לחוק איסור לשון הרע.

122 סעיף 1 לחוק איסור לשון הרע.

123 תשובת הדין הנוכחי היא שהמבחן הוא אובייקטיבי, לפי קבוצת ההשתייכות של הנפגע. השוו ע"א 466/83 **שאהה נ' דרדריאן**, פ"ד לט(4) 734 (1986); ע"א 809/89 **משעור נ' חביבי**, פ"ד מז(1) 1 (1992); וכן ראו ע"א 89/04 **נודלמן נ' שרנסקי**, בפסקה 18 לפסק דינה של השופטת איילה פרוקצ'יה (פורסם בנבו, 4.8.2008).

124 ראו סעיפים 14-15 לחוק איסור לשון הרע.

125 על הערכים החברתיים המוגנים בדיני איסור לשון הרע ראו חאלד גנאים, מרדכי קרמניצר ובועז שנור **לשון הרע: הדין המצוי והרצוי** (2005).

126 ראו ע"א 214/89 **אבנרי נ' שפירא**, פ"ד מג(3) 840 (1989); עניין **נודלמן**, לעיל ה"ש 123, בפסקה 51; ע"א 10281/03 **קורן נ' ארגוב**, בפסקה 18 לפסק דינה של השופטת ארבל (פורסם בנבו, 12.12.2006); גנאים, קרמניצר ושנור, לעיל ה"ש 125, בעמ' 144-152.

נמצאות לפני בית המשפט כשמדובר בהליך חד־צדדי, שבו רק התובע נמצא באולם והנתבע אינו ידוע.

מכאן הקושי המרכזי שבהליך חשיפתו של הגולש האנונימי. האתר המארח וספק השירות בתחילה, ובית המשפט לאחר מכן, מתבקשים לחשוף את זהות הגולש האנונימי על סמך טענות של צד אחד בלבד, הכוללות ראיות רק על חלק מסיפור המעשה. במצב כזה לא תמיד קל להעריך אם אכן נפגעה זכותו של התובע ומה עוצמת הפגיעה.

(ב) זכות לסעד

בצד הזכות המהותית עומדת לתובע זכות נספחת שהוא יכול לאחוז בה – זכות לסעד. זו זכות מסדר שני, מכשירנית באופייה, שנועדה לאפשר לאדם לממש זכות מהותית בבית המשפט. מה טעם יש בזכותו של אדם לשם טוב אם אין הוא יכול לממש את הזכות כשהיא נפגעת? הגם שהזכות נספחת לזכות מהותית היא יכולה להיגזר גם מכבוד האדם. האם אפשר להפעיל את הזכות לסעד כדי לחייב ספק שירות למכור מידע שבידיו?

עוגן אפשרי אחד של הזכות לסעד נמצא בזכות הגישה לערכאות, שנמצאת עדיין בחיתוליה במשפט הישראלי[127] (למעט המקרה של זכות העמידה בבג״ץ, שפותח בהרחבה). הזכות עוגנה, לפחות בספרות, כזכות חוקתית, בין שסווגה כחלק מזכות הקניין או כחלק מכבוד האדם ובין שסווגה כזכות נספחת לזכות מהותית אחרת.[128] הזכות הוכרה בהקשרים דיוניים: חסמים המוצבים בדרכם של תובעים פוטנציאליים ומונעים מהם לממש את זכותם נתפסים כפגיעה בזכות הגישה לערכאות. כך נקבע, למשל, לגבי אגרה גבוהה במיוחד או כללים בדבר התיישנות.[129] במובן זה, זכות הגישה לערכאות היא זכות שלילית המכוונת כלפי המדינה: תוכנה הוא איסור על המדינה להערים קשיים על מי שמבקש לפנות לבית המשפט.

מובן אפשרי אחר של הזכות הוא חיובי – הטלה של חובת עשה לסייע לאדם להגיע לבית משפט. אנו מכירים שורה של מנגנונים שנועדו להנגיש את בתי המשפט לאזרחים על

---

127 לדיון ראשון ראו שלמה לוין ״חוק יסוד: כבוד האדם וחירותו וסדרי הדין האזרחיים״ **הפרקליט** מב 451 (1996) (להלן: לוין ״חוק יסוד״). לדיון מעודכן ראו שלמה לוין **תורת הפרוצדורה האזרחית – מבוא ועקרונות יסוד** 30-37 (מהדורה שנייה, 2008). כן ראו יורם רבין **זכות הגישה לערכאות כזכות חוקתית** (1998).

128 ראו לוין ״חוק יסוד״, לעיל ה״ש 127, בעמ׳ 452-455; רבין, לעיל ה״ש 127, בעמ׳ 139, 148.

129 לדיון בשאלת האגרה ראו לוין ״חוק יסוד״, לעיל ה״ש 127, בעמ׳ 456-457; לשאלת ההתיישנות ראו ע״א 6805/99 **תלמוד תורה הכללי והישיבה הגדולה עץ חיים בירושלים נ׳ הוועדה המקומית לתכנון ובנייה, ירושלים**, פ״ד נז(5) 433, 444 (2003).

ידי סיוע שמוענק להם,[130] אולם לא ברור מה עוצמתו של הפן החיובי הזה של הזכות. אם, למשל, תסגור המדינה את הלשכה לסיוע משפטי, ברור שהדבר יפגע בפועל בגישה של רבים לערכאות, אולם האם אפשר יהיה לטעון שלמדינה יש **חובה** לספק שירות כזה, שאחרת יש פגיעה **בזכות** הגישה לערכאות? שאלות אלה טרם נענו בפסיקה ואין צורך להשיב עליהן כאן.[131] בצד המשפט הציבורי הוזכרה זכות הגישה לערכאות גם בתחומי המשפט הפרטי, למשל כשצד אחד מנסה להגביל את זכות הגישה לערכאות של אחר בהסכם[132] או בהכבדה יתרה.[133]

במקרה הנדון כאן המצב מורכב עוד יותר: טענה בדבר זכות לסעד בגדר הזכות לגישה לערכאות, המכוונת כלפי ספק שירות, היא טענה קשה מבחינה אנליטית שכן משמעותה היא הטלה של חובת עשה חיובית על גורם פרטי. אם לא ברור שחלה חובה כזו במשפט הציבורי קל וחומר שיש ספק באשר לתחולתה במשפט הפרטי. כדי שבית המשפט יפתח את זכות הגישה לערכאות כך שתטיל על הספק חובה לסייע לתובע לממש את זכויותיו המהותיות, נדרשים כמה צעדים בדרך שטרם נסללה.[134] כמו כן, קביעה כזו תעמוד בסתירה לחובת הסודיות המוטלת על הספק בקשר למידע ותסתור את העיקרון של צמידות המטרה.

האם ספק השירות כפוף לחובה מעין זו? מקור אחד של חובה כזו יכול להיות חוזי: במקרה שספק של שירות גישה או אתר אינטרנט מתחייב כלפי הגולשים בו או הציבור בכלל לעשות כל שביכולתו כדי לשמור על שמם הטוב, אפשר יהיה, למשל, לגזור מהתחייבות כזו חובה לסייע לתובע לממש את זכויותיו. אולם ספקי שירות אינם מתחייבים בהתחייבויות מעין אלו, להפך: הם מקפידים לפטור את עצמם מאחריות לנזקים שנגרמים לגולשים או לצדדים שלישיים על ידי גולשים אחרים או צדדים שלישיים. מקור אחר לחובת סיוע יכול להיות בדין ספציפי קיים. חוק איסור לשון הרע עצמו (וגם חוק הגנת הפרטיות) כולל הטלת אחריות עקיפה על עורך של אמצעי תקשורת.[135] אולם, גם אם ימצא בית משפט שאתר אינטרנט או ספק של שירות גישה חב חובה כלפי הנפגע (שמבקש את חשיפת זהות

---

130 ראו, למשל, את חוק הסיוע המשפטי, התשל"ב-1972.

131 לדיון ראו רבין, לעיל ה"ש 127, במיוחד בעמ' 168-171, הטוען כי הזכות היא נגטיבית ופוזיטיבית גם יחד.

132 ראו ע"א 3833/93 **לוין נ' לוין**, פ"ד מח(2) 862, 874 (1994).

133 ראו, למשל, עב' (אזורי ת"א) 5646/03 **בוסי נ' הנהלת רשת גני אגודת ישראל** (פורסם בנבו, 26.2.2009).

134 אם כי כך מקובל באנגליה, במסגרת צו Norwich Pharmacal, ראו לעיל ה"ש 89. הקושי הוא שמבחן זה פותח בקשר לרשויות ציבוריות אולם הוחל על גופים פרטיים כאילו אין הבדל ביניהם.

135 ראו דיון להלן, בטקסט ליד ה"ש 160.

זהות הגולש הפוגע), תהא לנפגע עילת תביעה ישירה נגד ספק השירות בגין הפגיעה שפגע הוא בתובע. כדי לגזור מכאן חובת סיוע שתוטל על ספק השירות לסייע לתובע לממש את זכות התביעה המהותית שיש לו, ככל שיש לו, כלפי צד שלישי – נדרש ביסוס משמעותי יותר. ייתכן שאפשר לאתר חובת סיוע בדיני הנזיקין. אפשר להציע טענת תביעה כנגד הספק במבנה הבא: ספק שירות שאינו מסייע לנפגע לממש את זכותו המהותית מפר את חובת הזהירות המושגית והקונקרטית שהוא חב כלפי התובע או גורם לו נזק ראייתי.[136] נראה כי האפיק הנזיקי אינו מועיל לנו בבירור השאלה המהותית: האם ספק השירות כפוף לחובה של חשיפת זהות הגולשים, לטובת התובע? המסגרת הנזיקית תשאל את אותה שאלה בדיוק: האם יש להחיל חובת עשה על ספק של שירות פרטי לסייע לנפגע?

אכן, למי שיש זכות מהותית שבגינה הוא זכאי לתבוע צריך שתהיה אפשרות ממשית לתבוע. מצוקתו של מי שנפגע מהשמצה אנונימית היא מובנת: שמו נפגע ואין הוא יודע את מי לתבוע ואינו יכול לתבוע את עלבונו. זכות זו כשלעצמה אינה מטילה חובה על ספק השירות לחשוף את הגולשים כל עוד אין הוא כפוף לחובה כזו ממקור אחר. אפשר כמובן לקבוע חובה כזו בדין,[137] אולם כפי שיוסבר בהמשך אני סבור שאין זה רצוי. לפיכך, כל

---

136 בית משפט שלום שדן בתביעה של גולש נגד מנהל פורום מקוון פנה לאפיק הנזיקי לבחון את אחריותו הישירה של הספק כלפי הנפגע והיה מוכן לקבל אותה בכפוף לתנאים מסוימים. ראו ת"א (שלום כפ"ס) 7830/00 **בורוכוב נ' פורן** (פורסם בנבו, 14.7.2002, השופט רמי אמיר). גם בת"א (שלום ת"א) 37692/03 **סודרי נ' שטלריד**, בפסקאות 25-29 (פורסם בנבו, 1.8.2005, השופטת רות רונן) נבחנה האפשרות לחייב את מפעיל הפורום בנזיקין. בית המשפט דחה אותה תוך שהביא בחשבון את העלות החברתית הכוללת לתוך המשוואה הנזיקית של תוחלת הנזק מול עלות המניעה של הנזק. ראו בדומה גם ת"א (שלום ת"א) 51859/06 **דיסקין נ' הוצאת עיתון הארץ בע"מ**, פסקאות 124-130 (פורסם בנבו, 28.10.2008, השופטת תמר אברהמי). מקרים אלה לא עסקו בחשיפת זהות הגולשים.

137 ראו, למשל, את הצעת החוק של ח"כ ישראל חסון, הצעת חוק התקשורת (בזק ושידורים) (תיקון – זיהוי המגיבים באתרי אינטרנט), התשס"ז-2006, ה"ח 1637, שבה הוצע לתקן את חוק התקשורת כך: "בלי לגרוע מסמכויות השר לפי סעיף זה, השר יקבע, בתקנות או ברשיון, הוראות לעניין חובתו של בעל רשיון מיוחד למתן שירותי גישה לאינטרנט, להבטיח כי באתרי אינטרנט שבהם ניתנת לגולשים האפשרות להגיב על תוכן הידיעות המפורסמות באתר, יידרשו הגולשים להזדהות בדרך שניתנת לאימות באמצעים סבירים כתנאי למתן אפשרות להגיב לתוכן כאמור". ביקורת רבה נמתחה על ההצעה; ח"כ חסון משך אותה ובמקומה הציע את הצעת חוק אחריותן המשפטית של הנהלות אתרי האינטרנט על דברי הגולשים המגיבים באתריהן (תיקוני חקיקה), התשס"ח-2007, ה"ח 3171. גם הצעה זו לא צלחה.

עוד אין חוק שמטיל חובה כזו, הטענה בדבר זכות גישה לערכאות יכולה לחזק – בעיקר רטורית – את כוחו של התובע. נוסף על כך יש להיזהר פן תנוצל הגישה לערכאות לרעה.[138]

2. הפוגע: הגולש האנונימי

הגולש האנונימי אינו מתייצב בבית המשפט, אולם דווקא מחמת היעדרו – כלומר: מאחר שהליך הבקשה לחשיפה הוא חד־צדדי – מוטלת על בית המשפט המלאכה לאתר את הזכויות והאינטרסים של הגולש האנונימי. החשיפה היא חד־סטרית: מרגע שגולש נחשף אין הוא יכול עוד להיות אנונימי. האנונימיות בהקשר הזה איננה יחסית אלא בינארית: היא קיימת או שאינה קיימת.

מה טיבה של האנונימיות? האנונימיות היא קטגוריה תרבותית שנויה במחלוקת. בחיי היום־יום יש לא מעט מצבי אנונימיות ואנחנו נהנים מהם באופן ישיר או כקהילה כגון מתן בסתר, תרומת זרע, בחינות אקדמיות, שיפוט אקדמי, שימוש בכסף מזומן, בדיקות רפואיות מסוימות, תלונה למשטרה, חשיפת שחיתות, מקור עיתונאי, כתיבה ספרותית, גלישה ברשת ועוד. בצד אלה האנונימיות נתונה לביקורת: יש מי שרואים בה מסתור של פחדנים שמתחמקים מאחריות, "מפלטו ומקלטו של הנבל", כלשונו של השופט רובינשטיין בדעת המיעוט שלו בעניין מור.[139] היא מאפשרת להיות "דני דין", הרואה ואינו נראה, אבל אולי בניגוד לדני דין היא גם מאפשרת לנצל את התכונה הזו לרעה.

האנונימיות אינה מוגנת במפורש בדין ולכן יש לברר אם היא כלולה בזכויות יסוד אחרות. שתי הזכויות המרכזיות המועמדות הן חופש הביטוי והזכות לפרטיות.[140] המשפט האמריקני ממשיג את האנונימיות כחלק מחופש הביטוי.[141] להמשגה הזו יתרון בכך שהגנת

---

138 ליחס שבין זכות הגישה לערכאות לניצול הליך לרעה ראו: משה בר־עם "הליכי סרק אזרחיים" **עלי משפט** ו 135 (2007).

139 עניין מור, לעיל ה"ש 2, בפסקה יא לפסק דינו של השופט רובינשטיין.

140 אפשר לגזור את האנונימיות גם מהזכות ליחס שווה ומחופש ההתאגדות. ראו למשל, National Association for Advancement of Colored People v. State of Alabama, 357 U.S. 449 (1958). ספק עד כמה עקרונות אלה יכולים לשמש וו איתן לתלות עליו את האנונימיות במשפט הישראלי.

141 פסק הדין המרכזי הוא McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995), שעסק בחלוקת מנשרים פוליטיים אנונימיים. ראו גם Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton, 536 U.S. 150, 166-167 (2002), שעסק בחלוקת מנשרים דתיים אנונימיים. בהקשר המקוון ראו American Civil Liberties Union of Georgia v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997), שבו פסל בית משפט פדרלי חוק במדינת ג'ורג'יה שקבע עברה פלילית של שימוש בפסבדונים באינטרנט.

חופש הביטוי האמריקנית חזקה מאוד, אולם בצדה חסרון: הפעולה האנונימית תוגן רק ככל שהיא נכללת בתחום הכיסוי של חופש הביטוי.[142] ביטוי אנונימי יוגן מפני התנכלות של המדינה אולם פעולה שאין בה ממד של ביטוי (למשל תרומות, בדיקות רפואיות או מסחר), או פעולה שהגורם הפוגע באנונימיות אינו מדינתי – לא תזכה להגנה.

המשפט האירופי ממשיג את האנונימיות כחלק מהזכות לפרטיות, בכך שהוא מגדיר מידע אישי (personal data) כמידע מזהה או ניתן לזיהוי.[143] אני סבור שזו גם המסגרת הראויה בישראל, בצד ונוסף על המסגרת של חופש הביטוי. חופש הביטוי כלול בכבוד האדם וככל שמדובר בביטוי או בפעולה ביטויית (ובכלל זה גלישה פסיבית ללא כתיבה פעילה)[144] הרי המסגרת של חופש הביטוי חלה. כמו כן, ככל שמדובר בפעולות שאינן בתחום הכיסוי של עקרון חופש הביטוי, הזכות לפרטיות יכולה וצריכה לשמש גג משפטי לאנונימיות.

הזכות לפרטיות מוגנת הן בחוק היסוד והן בחוק מיוחד. הפגיעה באנונימיות אינה נזכרת במפורש ברשימה של אחד־עשר מצבי הפגיעה בפרטיות המפורטים בחוק הגנת הפרטיות או בארבעת המצבים המנויים בחוק היסוד.[145] אפשר לקרוא אותה לתוך המצבים האלה בנסיבות מסוימות, למשל: כשיש הסכם המחייב אנונימיות הפרתו היא גם פגיעה בפרטיות;[146] אולם החוק עצמו – וחוק היסוד בוודאי – כוללים מונחי שסתום שיש לפרשם כמו "ענייניו הפרטיים של אדם" ומושג ה"פרטיות" עצמו. במדרג הנורמטיבי הישראלי אין מניעה לפרש את חוק היסוד בדרך שמרחיבה מעבר לרשימה (הסגורה) של החוק. אם כן,

---

142 לחשש זה ראו Froomkin, לעיל ה"ש 25, בפסקאות 60, 69. כמו כן, ההגנה לביטוי שאינו פוליטי חלשה יותר ומתקיימת בעיקר כשהביטוי מכוון לגורם פוליטי או ציבורי. בישראל הגנת חופש הביטוי חלשה מאשר בארצות־הברית. בתי המשפט כאן נכונים לאזן את חופש הביטוי ביתר קלות אל מול זכויות ואינטרסים אחרים בהשוואה לבתי המשפט מעבר לים. ראו אמנון רייכמן "קול אמריקה בעברית? פנייתו של בית המשפט הישראלי אל הדין האמריקני בסוגיית חופש הביטוי" **שקט, מדברים!**, לעיל ה"ש 117, בעמ' 185.

143 ראו לעיל ה"ש 43, וכן את חוות הדעת של הגוף המופקד על נושא הפרטיות באיחוד האירופי, לעיל ה"ש 45, בעמ' 21.

144 לגלישה כפעולה החוסה תחת חופש הביטוי ראו מיכאל בירנהק "החופש לגלוש בספריות ציבוריות" **משפט וממשל** ו 421 (2003); לגלישה אנונימית, ראו Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace*, 28 CONN. L. REV. 981 (1996).

145 ראו סעיף 2 לחוק הגנת הפרטיות; סעיף 7 לחוק־יסוד: כבוד האדם וחירותו. קריאה דווקנית של החוק הביאה את בית משפט השלום בעניין **בורוכוב**, לעיל ה"ש 136, לקבוע שהאנונימיות אינה מוגנת במשפט הישראלי. כמוסבר בטקסט, אני סבור שקביעה זו מוטעית.

146 ראו סעיף 2(8) לחוק הגנת הפרטיות.

השאלה היא מהותית: מהי תכליתה של האנונימיות והאם לפי פרשנות תכליתית היא נכללת בזכות לפרטיות?

בראש ובראשונה, האנונימיות מספקת חירות ממעקב. מעקב משתק את פעילותו של מי שחושש מהעוקבים: המדינה, המעסיק, החברה בכלל. האנונימיות מאפשרת פעולה תוך יצירת מגן בין הפועל לבין מי שמבקשים את רעתו. במקרים מסוימים, בלעדי האנונימיות לא תתקיים פרקטיקה רצויה מבחינה חברתית כמו בדיקות רפואיות, דיווח לעיתונאי, תלונה למשטרה, ביטוי או גלישה באינטרנט. בלי האנונימיות לא יושגו ההגינות והשוויון הרצויים במקרים של בחינות או שיפוט אקדמי. הנהנה מהפעולות האלו הוא הציבור כולו. האנונימיות מאפשרת את פעולות אלה בכך שהיא מונעת מהגורמים העוינים להתנכל (בצדק או שלא בצדק מבחינתם) או לסכל את הפעילות של השחקן האנונימי. האנונימיות מסיטה את מבטם המקפיא של גורמים שונים למקום אחר ומאפשרת לשחקן לפעול בלי שתשומת הלב מרתיעה אותו. הטעמים המכשירניים בעד האנונימיות חוזרים ומופיעים בספרות המשפטית.[147]

ההצדקות של האנונימיות כרוכות ושלובות בהצדקות של הזכות לפרטיות, שעליהן הרחבתי במקום אחר.[148] לזכות לפרטיות יש הצדקות רבות. שתי גישות מרכזיות הן **הפרטיות כגישה**, המזוהה עם עמדתה של רות גביזון, **והפרטיות כשליטה**, שמקורה בכתיבה סוציולוגית.[149] גביזון מתארת שלושה מצבים של פרטיות, שאחד מהם הוא תשומת לב אל האדם.[150] לשיטתה, כל תשומת לב שמופנית לאדם פוגעת בפרטיותו, בין שהיא מכוונת ובין שלא. גביזון מתרגמת תשומת לב זו לאנונימיות ומסבירה שההיטמעות בהמון – מצב שבו אין האדם מושא לתשומת לב מיוחדת – היא אנונימיות; עם זאת גביזון עצמה מודה שהתרגום של הגנה מפני תשומת לב לאנונימיות אינו מדויק ומלא.[151] לפי עמדת הפרטיות

---

147 ראו, למשל, Lidsky & Cotter, לעיל ה"ש 39, בעמ' 1556-1559; Gary T. Marx, *What's in a Concept? Some Reflections on the Complications and Complexities of Personal Information and Anonymity*, 3 U. OTTAWA L. & TECH. J. 1, 19 (2006).

148 ראו בירנהק "שליטה והסכמה", לעיל ה"ש 27.

149 ראו, בהתאמה, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980) (להלן: גביזון); ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

150 גביזון, לעיל ה"ש 149, בעמ' 432. שני המצבים האחרים הם מידע על האדם וגישה אליו.

151 שם, בעמ' 433-434, בה"ש 40 למאמרה כתבה גביזון כך: "I may stare hard, focusing all my attention on an individual, without knowing who he is. The subject of my attention is therefore anonymous. On the other hand, even the President has times when he is not the subject of anyone's attention, but we would not call him an anonymous individual. Nevertheless, the aspect of anonymity that relates to attention and privacy is that of

כגישה, גזירת האנונימיות מתוך הזכות לפרטיות היא מלאכה אנליטית פשוטה, שכן הגדרת הפרטיות מבוססת בין היתר על מצב של אנונימיות. מי שמאמץ גישה זו יכול לגזור את האנונימיות מתוך הזכות לפרטיות.[152]

לפי עמדת הפרטיות כשליטה יש קשר הדוק בין הפרטיות לבין המושג של כבוד האדם ולכן היא משתרעת גם על הזיהוי של האדם. ברצותו יחשוף אדם את זהותו וברצותו לא יחשוף אותה. הנתון שלפיו ביצע אדם פעולה מסוימת הוא מידע על אודות אותו אדם, על התנהגותו. הנתון מעיד על האדם – בין שהוא מעיד על התנהגות חריגה ובין שהוא מעיד על התנהגות שגרתית. בדרך זו, הבנת הפרטיות כשליטה מגנה על זהותו של האדם ללא בחינה של תוכן הפעולה.

גזירת האנונימיות מתוך גישת הפרטיות כשליטה מתיישבת היטב עם ההצדקות הפרטיקולריות של הזכות לפרטיות במעגלים השונים, במיוחד עם "מעגל האדם".[153] המפתח לזהותו של אדם – כלומר: לגילויה או לשמירתה, המלאה או היחסית, המותנית או שאינה מותנית – יופקד בידי האדם עצמו. כאשר גורם חיצוני מקבל החלטה עבור אדם אחר הוא מבטל את האוטונומיה של אותו אדם, את היותו אדון או גברת לגורלו/ה. כמו כן, ההצדקה המדגישה את הצורך של האדם במרחב אישי שבו יוכל להתנסות, ללמוד ולתהות, ללא צורך לבקש רשות מראש או לספק הסברים בדיעבד, גם היא מכתיבה את הפקדת המפתח בדבר זהותו של האדם בידיו הוא ובידיו בלבד.

הצדקות אלה חשובות בקשר לפעולות אקטיביות שספק אם היו מי שמשתתפים בהן אלמלא האנונימיות. כך, למשל, השתתפות בקבוצת תמיכה לגמילה מסמים. הקבוצה יוצרת מרחב מוגן שבו האדם יכול לבקש ולקבל סיוע ולטפל בעצמו. בדיקות רפואיות אנונימיות גם הן מאפשרות פעילות רצויה, תוך יצירת תנאי רקע שמאפשרים לאדם ליטול אחריות אישית לגורלו ולהיבדק. כך גם בקשר לפרסום יצירה באופן אנונימי במקרה של יוצרת צעירה החוששת מהתגובה ליצירתה או במקרה של יוצרת המבקשת שיצירתה תישפט ותוערך לפי תוכנה ולא לפי דמותה שלה. כך גם בקשר לפרסום דעה, למשל בתגובית ברשת. האנונימיות מאפשרת השתתפות בשיח הציבורי ובקהילה בכלל תוך שמירה על אמצעי הגנה; היא מאפשרת פעולה "בחוץ" תוך שמירת מרחב פנימי.

---

being lost in the crowd. If the President could ever be lost in a crowd, he would be anonymous in this context. To draw attention to him in such a case will cost him his anonymity – and his privacy".

152 ליישום של עמדת הפרטיות כגישה לסביבה המקוונת ראו Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 INFO. SOC'Y 141 (1999).

153 ראו בירנהק "שליטה והסכמה", לעיל ה"ש 27, בעמ' 57-68.

ההצדקות האלה של הזכות לפרטיות מסבירות גם מדוע יש לנו צורך באנונימיות בפעולות פסיביות של לימוד, תהייה ובדיקה כמו גלישה באינטרנט ושימוש במנועי חיפוש. היכולת שלנו לגלוש באינטרנט באופן אנונימי, בלי שיש מי שיודע את זהותנו, מאפשרת לנו להיעזר במידע הרב שיש ברשת כדי ללמוד על עצמנו. זה המקרה, למשל, של נער מתבגר התוהה בקשר למיניותו ונבוך או חושש לשאול את מי שסביבו. עבורו, האנונימיות שבגלישה מאפשרת לו להגיע למידע בלי לחשוש (כמובן, כל עוד יש לו אנונימיות בפועל). בכלל, בכל מצב שבו אדם מבקש לפעול בדרך שאינה מקובלת בסביבה המיידית שלו – ואין הכוונה לפעולות בלתי חוקיות אלא לפעולות החורגות מנורמות קשיחות של הקהילה – האנונימיות מאפשרת לו לפעול בלי לסכן את חברותו בקהילה. זה המקרה, למשל, של אדם דתי החי בקהילה דתית שמרנית. פעולות מסוימות נתפסות על ידי הקהילה כחריגות והן מגונות. האנונימיות מאפשרת לו לממש את אישיותו ולפתח את עצמיותו ללא מורא חברתי. האנונימיות מאפשרת לנו גם להתגונן מפני המבט הננעץ בנו. המבט החודרני עלול לצנן ולהקפיא את פעילויותינו; אך טבעי שכבני אדם החיים במסגרות חברתיות נחשוש מתגובת החברה לכל מה שייחשב לחריג בעיניה. האנונימיות היא מגן מפני המבט הנוקב, הביקורתי, המצמית.

עיגון האנונימיות בזכות לפרטיות הוא חשוב. הוא מעלה שהאנונימיות איננה רק מסכה של מי שיש לו משהו להסתיר אלא אף מגן לחלש מפני עריצות ומפני התנכלות. האנונימיות היא גם כוח מאפשר שבזכותו הגולש האנונימי יכול להתבטא, להשתתף בשיח ולתרום לחברה בכללותה. אם כן, האנונימיות משמשת גם כוח מניע חיובי. בלעדיה אנו עלולים להחמיץ את יתרונותיה האמורים. בלעדיה נקבל ביטויים גלויים אולם אלה יחסרו את הכוח הנשכני, החושף, החיוני כל כך שיש בביטויים אנונימיים. בלעדי האנונימיות לא נדע מה נחמיץ.

יתרונות האנונימיות מלמדים גם על הסכנה שיש בחשיפה מהירה מדי של גולשים אנונימיים. סכנה אחת היא קונקרטית לגולש שבו מדובר וטמונה בכך שיש מי שיבקשו לנצל את החשיפה לרעה. החשש הוא שבקשת החשיפה לא נועדה תמיד לממש זכויות מהותיות לגיטימיות כמו הגנה על שם טוב או זכות יוצרים אלא כדי לאפשר ל"נפגע" להתנכל למי שביקר אותו, להשתיק ביקורת לגיטימית, לדכא תחרות ובכלל להעביר מסר פשוט: "איתי לא מתעסקים".[154] החשש למסע נקם גדול יותר כשמדובר בתביעת לשון הרע, שבה תיתכן היכרות בין הנפגע לפוגע, לעומת תביעה על הפרת זכות יוצרים ששם בעל הזכויות מבקש

---

154 ראו בדומה ת"א (שלום בית־שאן) 7832-10-08 **מושקוביץ נ' וואלה! תקשורת בע"מ**, בפסקאות 14-15 (פורסם בנבו, 31.5.2009, השופטת עיריה מרדכי), על בסיס טיוטה של מאמר זה. בקשת רשות ערעור נדחתה. ראו בר"ע (מחוזי נצ') 213/09 **מושקוביץ נ' וואלה! תקשורת בע"מ** (פורסם בנבו, 19.1.2010, השופט אברהם אברהם).

להיפרע את נזקיו ולהעביר מסר כללי ולא בהכרח להתנכל למפר מסוים דווקא. כאשר הנפגע הוא תאגיד או מנהל בכיר בחברה, לא מן הנמנע שהתגובית האנונימית שחושפת שחיתות או מאשימה את המנכ״ל בשחיתות ובאי־סדרים נכתבה על ידי עובד. כאשר הנפגע הוא פוליטיקאי או איש ציבור שנטען נגדו על היעדר יושר או על היעדר יושרה, לא מן הנמנע שהתגובית האנונימית נכתבה על ידי מתנגדים פוליטיים מבית או מחוץ. כאשר התגובית כוללת מידע שהיה רק בידיעת ״אנשי שלומו״ של הנפגע ייתכן שמדובר בסוג של הדלפה ששקולה למסירת מידע לעיתונאי.

בהמשך לדברים אלה, הסכנה השנייה היא כללית. הגנה פחותה על האנונימיות משדרת מסר מרתיע ומצנן לגולשים שמבקשים לכתוב, להתבטא ולפעול – אולם אינם בטוחים אם פעולתם מותרת ואין ביכולתם לברר את החוקיות, או שהבירור המשפטי יסתיים גם הוא בסימן שאלה ולא בסימן קריאה. ביטויים ביקורתיים (בקשר לעוולות של לשון הרע) ושימושים מותרים (בקשר לדיני זכויות יוצרים) זקוקים למרחב נשימה ללא איום. חשיפה קלה מדי עלולה לצנן פעולות וביטויים אנונימיים רצויים וחשובים.

בכל אלה חשוב לעמוד על קיומה של האנונימיות ולהקפיד לגזור אותה משני מקורותיה העיקריים – חופש הביטוי והזכות לפרטיות גם יחד. בדרך זו צעדה דעת הרוב בעניין מור, בניגוד לדעת המיעוט שהסתפקה בתיאור האנונימיות כעובדה אקראית הנמצאת, לכל היותר, במסגרת המשפטית של חופש הביטוי. במיוחד יש להגן על האנונימיות מפני מי שמבקש להסירה כדי לסכל את מטרותיה ואילו מימוש זכותו המהותית, אם בכלל נפגעה, אינו בראש מעייניו.

3. ספק השירות

ספקים של שירות אירוח (אתרי האינטרנט) וספקים של שירות גישה לאינטרנט נמצאים בין הנפגע לבין הגולש האנונימי. במצב האופייני שנדון כאן – תוכן פוגעני שנכתב על ידי גולש אנונימי – הספקים מחזיקים את המפתח לחשיפת הזהות. הספקים אינם צד ישיר לסכסוך אולם עדיין יש להם עניין רב בו והאינטרסים הישירים שלהם כרוכים בתסבוכת שנוצרת. הספקים נמצאים במלכוד כפול: הראשון הוא ברירה בין סיכון משפטי ישיר של הספק לבין אינטרסים של צדדים אחרים – ולא מפתיע שהספקים מבכרים את עצמם; המלכוד השני הוא שגם אחרי שחיסנו הספקים את עצמם מסכנה ישירה הם נתונים בסד שבין הנפגע לגולש. העדפת האחד מהאחר עלולה להשליך על סוג השירות שהספקים מציעים ועל איכותו.

(א) מלכוד ראשון: הספק או כל השאר?

אדם שמגלה כי שמו הטוב נפגע בתגובית המופיעה באתר חדשות, בבלוג שמתארח אצל ספק פלטפורמות בלוגים או בפורום מקוון מבקש תחילה לעצור את הפגיעה, כלומר: להסיר

את החומר הפוגעני; בהמשך יבקש פיצוי על נזקיו. הכתובת הטבעית לבקשה הראשונה היא הספק של שירות האירוח – האתר המארח, פלטפורמת הבלוגים, מנהל הפורום המקוון וכדומה. בפועל, ספקי שירות שונים נוהגים באופן שונה בבקשות הסרה כאלה. חלקם יסירו מיד את הדברים הפוגעניים ללא היסוס, חלקם יסרב להסרה או יפנה את המבקש למשטרה או לבית המשפט. ההחלטה של כל ספק מונַעת משיקולים מסחריים – והיא תוצאה של הכללים המשפטיים שיש בקשר לאחריות הספק עצמו. אך מובן הוא שהספק מבקש להימנע מחשיפה לאחריות משפטית.

כשלי אכיפה

במצב הרגיל, כאשר אדם נפגע מפעולתו של אחר, מתבקש כי יפנה אל הפוגע. מאפיינים טכנולוגיים, כלכליים ומשפטיים של הסביבה הדיגיטלית מקשים עליו לתבוע את המעוול הישיר. כאן אפשר להבחין בין שני סוגי תביעות או עוולות: סוג אחד הוא כשיש מעוול אחד – וזה המצב האופייני בתביעות לשון הרע; סוג אחר הוא כשיש מספר מעוולים גדול – וזה המצב האופייני בתביעות בגין הפרה של זכויות יוצרים.

במקרה של מעוול אחד, הנפגע שמבקש לתבוע ניצב לפני שורת קשיים שעליו להתגבר עליהם. הראשון הוא איסוף הראיות. חלק מהראיות הן גלויות, כמו ההודעה הפוגענית, אבל חלקן – כמו כוונותיו של הפוגע, שעשויות להיות רלוונטיות כדי להתמודד עם טענות הגנה אפשריות – אינו ידוע; גם זהות הפוגע אינה ידועה כמובן. קושי שני הוא עלות התביעה. הפעולות המקדימות שנדרשות לשם הגשת התביעה – כלומר: חשיפת הזהות – אינן בהכרח זולות. כמו כן, כל עוד לא ידוע מי הנפגע קשה להעריך אם הוא בעל כיס עמוק. ייתכן שאחרי תהליך ארוך של בירור יתברר שמדובר בקטין חסר כל שאין טעם כלכלי לתבוע אותו. הקושי השלישי כרוך בסיכונים הרגילים בהגשת תביעה: קשיי הוכחה, הסיכוי שבית המשפט לא יקבל את גרסת התובע או חלילה יטעה בפסיקתו.

במקרה של מעוולים רבים יש קושי רב יותר באיסוף הראיות מאחר שחלק מהפעולות מתרחש בביתו של הגולש ולאו דווקא בפומבי. כך בקשר להעברת קבצים באמצעות רשתות ותוכנות לשיתוף קבצים. בחלק מהמקרים יש קושי משפטי, שכן ייתכן שפעולתם של חלק מהגולשים מוגנת ומותרת.[155] לקושי הראייתי נוסף קושי עסקי. משתמשי הקצה – המפרים לכאורה – הם לקוחות של בעלות הזכויות, חברות המוזיקה. בעלי עסקים יהססו בדרך כלל

---

155 בתי המשפט בארצות־הברית, שדנו בתביעות נגד שירותים של שיתוף קבצים התחבטו בשאלה זו, שכן אם ספק השירות מסייע לגולשים לבצע פעולה מותרת אין הוא חב באחריות להפרה תורמת. למרות זאת בתי המשפט שם דחו את טענות ההגנה של הגולשים. ראו בייחוד A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

לתבוע את לקוחותיהם, במיוחד כשמדובר ביחסים עסקיים נמשכים ולא חד־פעמיים.[156] בדומה למקרה של מעוול אחד, עלויות התביעה גבוהות; אולם בשונה ממנו, כאן יש יתרון לעצם הגשת התביעה: היא משדרת מסר הרתעה לכלל הגולשים כך שתועלתה של התביעה עשויה להיות גבוהה מעלותה.

לעומת הקושי לתבוע את הגולשים האנונימיים, ספק השירות ניצב מואר באור בהיר וחזק "מתחת לפנס".[157] הספק ידוע, נגיש וזמין; בדרך כלל הוא בעל כיס עמוק – או לפחות עמוק מזה של הגולשים; קל יותר להשיג ראיות נגדו וגם החשש מיחסי הציבור השליליים של תביעה נגד לקוחות קטן יותר. לפיכך, לא מפתיע שהספק הוא יעד מועדף על הנפגעים/התובעים. אולם, למרות היתרונות בתביעה כנגד הספק, הבסיס המשפטי של התביעה כנגדו אינו חד ויש בו קשיים משפטיים לא מבוטלים. לשם כך עלינו לבחון את סוגי האחריות המשפטית– אחריות ישירה ואחריות עקיפה, וכן הסדרים המקנים לספקי השירות חסינות מפני תביעות.

אחריות ישירה ואחריות עקיפה

אחריותו של הספק במצב הנדון כאן איננה אחריות ישירה. דיני הנזיקין, ובכלל זה העוולות של פגיעה בשם הטוב, הפרת פרטיות, עוולות מסחריות ודיני הקניין הרוחני מבחינים בין אחריות ישירה של מעוול לבין אחריות עקיפה של גורם אחר. מי שביצע את העוולה בעצמו – אחראי, בכפוף להוכחת היסודות הנדרשים של העוולה, ובכפוף לקיומם של חריגים והגנות לפי החוק הספציפי שמסדיר את ההתנהגות הנדונה. מי שפעל ברקע הדברים, אינו אחראי בהפרה ישירה.[158] כך, מי שפגע בשמו הטוב של אדם או בפרטיותו, או הפר את זכויות היוצרים של אחר – אחראי למעשיו, שוב, בכפוף להוכחה של יסודות העוולה ולקיומן של הגנות אפשריות הקבועות בדינים השונים (למשל: הגנת אמת דיברתי

---

156 אכן, חברות המוזיקה בארצות־הברית נכוו כשהתברר שכמה תביעות נגד גולשים הופנו לכתובת שגויה ויחסי הציבור השליליים לא איחרו להגיע. ראו, למשל, את הדיווח על תביעות שגויות: John Schwartz, *She Says She's No Music Pirate. No Snoop Fan, Either*, NEW YORK TIMES (25.9.2003).

157 לדיון ראו ניבה אלקין־קורן "המתווכים החדשים ב'כיכר השוק' הווירטואלית" **משפט וממשל** ו 365, 372-373 (2003).

158 כך נפסק, למשל, בארצות־הברית בקשר לזכויות יוצרים. ראו Religious Technology Center v. Netcom Online Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). בארץ, בקשר ללשון הרע, ראו עניין **סודרי**, לעיל ה"ש 136.

בלשון הרע, הגנת העניין הציבורי בדיני הגנת הפרטיות או הגנת השימוש ההוגן בדיני זכויות יוצרים).

בצד זה, הדינים הספציפיים מתייחסים בחלקם למצב של אחריות עקיפה, כלומר: לשאלת אחריותו של מי שלא היה מעוול בעצמו אבל היה מעורב בדרך כלשהי. אתר אינטרנט שמאפשר תגוביות אינו זה שמשמיץ את הנפגע. פלטפורמת הבלוגים אינה זו שחשפה פרטים אישיים על אודות הנפגע. אתר שמאפשר לגולשים להציג תוכן שהגולשים מעלים לאתר (אתרי Web 2.0 דוגמת Flickr או YouTube) אינו מפר את הזכויות (כל שיש הפרה) של בעלי זכויות. הדינים השונים קובעים את אחריותם של גורמים שונים לפגיעות העקיפות; הם מאפשרים את הפעילות הפוגענית מראש ותורמים לה בכך – או משום שאינם מונעים את התמשכותו של הנזק, בדיעבד, לאחר שכבר התרחש.

סעיף 7 לחוק איסור לשון הרע אוסר על פגיעה ישירה. זו איננה תלויה במדיום שבו פורסמו הדברים הפוגעניים.[159] אם הדברים פוגעים, הרי שלשם הטלת האחריות אין זה משנה אם נאמרו בשיחה על פה, במכתב, באמצעי תקשורת המונים או ביישום מקוון. צורת הפרסום עשויה להשליך על היקף הנזק ועל גובה הפיצוי. מי שהוכפש בשיחה על פה שהתנהלה בין שניים בלבד נפגע בצורה שונה ממי ששמו הטוב הוכפש בשידור חדשות בטלוויזיה. בצד זה, חוק איסור לשון הרע מטיל אחריות משפטית (אזרחית) גם על "עורך אמצעי התקשורת" ועל "אחראי לאמצעי תקשורת";[160] כלומר: לשון הסעיף מצביעה על כך שבמקרה של האחריות העקיפה, המדיום שבו מדובר הוא רלוונטי. הגדרת "אמצעי תקשורת" שם מתבססת על "עיתון" תוך הפניה לפקודת העיתונות. בתי משפט בערכאות הנמוכות התלבטו בפרשנות המושג "עיתון" וביישומו על יישומים מקוונים שונים. במקרה מוקדם אחד נקבע שאתר אינטרנט או פורום מקוון הם בגדר "עיתון": באותו מקרה דובר באתר אינטרנט שבבעלות עיתון שהיה זהה בתכניו למהדורה המודפסת של העיתון;[161] לפי שעה, בכל שאר המקרים נקבע אחרת. כך במקרה אחר, שבו המהדורה המקוונת הייתה דומה לעיתון מודפס;[162] כך כשדובר בפורום מקוון[163] ובאתר היכרויות[164] – בכל אלה

---

159 החוק מגדיר פרסום לעניין זה בצורה שמקיפה כל אמצעי תקשורת "בין בעל פה ובין בכתב או בדפוס, לרבות ציור, דמות, תנועה צליל וכל אמצעי אחר".

160 סעיף 11 לחוק איסור לשון הרע.

161 ק"פ (שלום ת"א) 145/00 **ויסמן נ' גולן** (פורסם בנבו, 2.9.2002, השופטת דורית רייך-שפירא).

162 עניין **דיסקין**, לעיל ה"ש 136, בפסקאות 66-77.

163 עניין **בורוכוב**, לעיל ה"ש 136; ת"א (שלום ת"א) 32986/03 **בושמיץ נ' אהרונוביץ** (פורסם בנבו, 6.5.2007, השופטת שושנה אלמגור).

סירבו בתי המשפט לראות אתרים כ״עיתון״. במקרה אחר ניתנה תשובה מסויגת, שהציעה לבחון את מהות הפעילות של האתר ועד כמה היא דומה למערכת של עיתון.[165]

גם חוק הגנת הפרטיות אוסר על פגיעה בפרטיות, כפי שזו מוגדרת בסעיף 2 לחוק. זו הפגיעה הישירה; בצדה קובע החוק הסדר זהה כמעט לזה שקבוע בחוק איסור לשון הרע ומטיל אחריות עקיפה על עורך העיתון ועל המוציא לאור שלו, ובתנאים מסוימים גם על המדפיס והמפיץ.[166]

חוק זכות יוצרים, התשס״ח-2007 אוסר על הפרת זכות מזכויותיו של בעל הזכויות ביצירה המקורית המוגנת.[167] האיסור הוא על מי שמבצע את המעשים המתוארים בחוק או מי שמרשה לאחרים לעשות זאת. הרשאה לאחר לבצע פעולה מפרה אינה ממצה את מלוא המצבים העובדתיים. לעתים יש מי שאינו מאפשר באופן פעיל לאחרים להפר, אבל עצם פעילותו תורמת להתרחשותה של ההפרה. זהו המצב של ״הפרה תורמת״ (contributory infringement). דיני הקניין הרוחני החקוקים בישראל אינם מתייחסים למצב זה אולם את החסר משלימה הפסיקה. תחילה קבע בית המשפט העליון את הדוקטרינה בדיני הפטנטים, ומשם היא זלגה לדיני זכויות יוצרים.[168] הדוקטרינה עדיין נמצאת בחיתוליה ואינה נקייה מקשיים.[169]

בצד הדינים הפרטיקולריים יש בדין עקרונות כלליים של הטלת אחריות על מי שסייעו לאחרים או שידלו אותם לפגוע בזכויות של צד שלישי. כאלה הם העיקרון של אחריות שילוחית והעיקרון הכללי בדיני הנזיקין בדבר אחריות של ״משתף ומשדל״.[170]

---

164 ת״ק (שלום ת״א) 8796-06-08 **דוביצקי נ׳ שפירא** (פורסם בנבו, 26.10.2008, השופט בני שגיא). באותו עניין קבע בית המשפט כי האתר אחראי כלפי התובע לפי עוולת הרשלנות.

165 עניין **סודרי**, לעיל ה״ש 129.

166 ראו סעיפים 30-31 לחוק הגנת הפרטיות. יש להניח שהפסיקה שפירשה מהו ״עיתון״ בקשר ללשון הרע תחול גם כאן.

167 סעיף 11 לחוק זכות יוצרים קובע את אגד הזכויות וסעיף 47 קובע כי עשיית פעולה מאלו המפורטות בסעיף 11 היא הפרה. ראו גם סעיף 50 בקשר לזכויות המוסריות.

168 בדיני הפטנטים ראו ע״א 1636/98 **רב בריח בע״מ נ׳ בית מסחר לאביזרי רכב חבשוש בע״מ**, פ״ד נה(5) 337 (2001); בדיני זכויות יוצרים ראו בש״א (מחוזי י-ם) 2184/02 **Microsoft Corp. נ׳ אגמה מחשוב 1999 בע״מ** (פורסם בנבו, 22.11.2002, השופט יהונתן עדיאל); ת״א (מחוזי י-ם) 6306/04 **בית שוקן להוצאת ספרים נ׳ מפלגת העבודה הישראלית** (פורסם בנבו, 16.5.2007, השופט יוסף שפירא).

169 לביקורת על עניין **רב בריח**, לעיל ה״ש 168, ראו מיכאל בירנהק ״לידתה של עוולה: הפרה תורמת בדיני פטנטים״ **טכנולוגיות של צדק: משפט מדע וחברה** 169 (שי לביא עורך, 2003).

170 ראו סעיפים 12, 14 לפקודת הנזיקין [נוסח חדש], נ״ח התשכ״ח 266 (לעניין אחריות שילוחית ושיתוף ושידול בהתאמה).

מחירה של העמימות המשפטית

מהאמור עולה כי ספק שירות אינו יכול להסתפק בכך שהוא אינו המעוול הישיר ואינו יכול להיות בטוח שלא ייתבע. הדין מטיל אחריות גם על מי שתרמו לפגיעות או אפשרו אותן; אבל כאן יש אי־ודאות משפטית כמעט בכל רכיב של האחריות העקיפה. במקרים של לשון הרע והגנת הפרטיות יש לשאול אם ספק שירות מסוים הוא "עיתון", מה מידת הידיעה הנדרשת כדי להטיל אחריות ואם יש הגנה כלשהי שקמה למעוול הישיר, שהרי בהיעדר עוולה ישירה אין בפעולתו של המסייע־התורם דבר פסול כלשהו. כך, למשל, אם השימוש שעשה משתמש בזכויות יוצרים של אחר ללא רשות הוא בגדר שימוש הוגן (עניין שאינו ודאי כלל וקשה לצפייה מראש גם הוא), הרי פעולתו של משתמש הקצה מותרת – וסיוע לפעולה לגיטימית אינו פסול; להפך, הוא מבורך. כמו כן, גם אם לא מתקיימים תנאיה של עוולה מסוימת ייתכן שתוטל אחריות מכוח דין אחר. כך, למשל, בצדה של עוולת לשון הרע בתי המשפט בוחנים אם יש בהתנהגות הספק משום רשלנות לפי דיני הנזיקין. המבחנים להטלת אחריות שם גם הם אינם ברורים.

לעמימות המשפטית יש מחיר: ספק שירות שיטעה בהפעלה של שיקול דעתו יצטרך לשלם על טעותו. מאחר שספקי השירות מבקשים להימנע, כמובן, מאחריות כזו, החשש הוא לאפקט מצנן: בכל מקרה של ספֵק, הספק לא יהסס וימחק את התוכן שבו מדובר. התגובית כוללת טענה עובדתית שלא ברור על מה היא נסמכת? – תימחק. התגובית כוללת ביקורת? – היא תימחק. יש חשש קל שבקלים שקובץ שהועלה על ידי גולש מפר זכויות של אחר? – יוסר הקובץ. לאפקט המצנן יש השלכות כלכליות: ספק השירות צריך לנטר את האתר שלו השכם והערב, מראש, או להגיב לבקשות מחיקה בדיעבד. לפעולה כזו יש עלויות ישירות. כך, למשל, באתר ynet נכתבות רבבות תגוביות מדי יום. סינון מוקדם של התגוביות מצריך שעות עבודה רבות. לא כל ספק שירות יכול לעמוד בנטל הכלכלי הזה. אתרי אינטרנט קטנים יתקשו לעמוד בכך. יוצא, שלכלל משפטי תמים שעניינו לשון הרע יש השלכות עקיפות שאינן רצויות על תחרות בשוק הרלוונטי.

לאצבע הקלה על מקש המחיקה יש השלכות נוספות, חשובות יותר, על השיח המקוון ועל איכותו.[171] מאחר שאין לספק השירות כלים לבחון את חוקיותם של כל ביטוי או פעולה של גולש, יש להניח שהמחיקה תהיה בעיקר של ביטויים שנויים במחלוקת, ביטויים מתוחכמים מצד אחד שאולי יש בהם רמיזות וכפל לשון או ביטויים רדודים ובוטים. בדרך כזו, השיח המקוון יתרכז ויתמרכז – אבל חופש הביטוי נועד להגן דווקא על הביטויים

171 לדיון ראו אלקין־קורן, לעיל ה"ש 157, בעמ' 372-377.

הביקורתיים, החתרניים, מטילי הספק ומעוררי הביקורת. העיקרון של חופש הביטוי שואף לאפשר למרב הדעות להישמע ולמרב הדוברים להשתתף בשיח. האפקט המצנן יפעל בצורה לא אחידה לגבי סוגי ביטויים שונים. אם כן, הפגיעה היא בחופש הביטוי.

להטלת אחריות משפטית על ספקי השירות בסביבה הדיגיטלית יש משמעות מעשית: היא שקולה להאצלה של שיקול דעת ערכי לספקי השירות הפרטיים. ספקי השירות אינם נבחרים בבחירות דמוקרטיות אלא הם "נבחרים" על ידי כוחות השוק. ספקי השירות אינם חייבים בדין וחשבון ובאחריותיות הציבורית (accountability). הם גופים פרטיים שפועלים במשפט הפרטי. אמנם אפשר לכפוף אותם לנורמות מסוימות מן המשפט הציבורי – בין לפי "מודל התחולה העקיפה", שלפיו הנורמות הציבוריות מחלחלות לתוך המשפט הפרטי באמצעות מושגי שסתום כמו "תום לב" או "תקנת הציבור", ובין באמצעות ראייתם במקרים המתאימים כ"גופים דו־מהותיים" הפועלים גם בשדה המשפט הפרטי וגם בשדה הציבורי[172] – אולם הדרך לשם אינה קלה.[173]

חסינות?

מדינות שונות התמודדו עם הקשיים האלה על ידי הענקת חסינות לספקי השירות, בין שירותי אירוח תוכן ובין שירותי גישה. יש מודלים משפטיים שונים של הענקת חסינות וכאן די בסקירה קצרה.[174] מודל אחד שננקט בארצות־הברית בקשר לשורה של עוולות, ובהן לשון הרע, מקנה חסינות כמעט מלאה לספקי השירות.[175] "הגנת השומרוני הטוב" נועדה לאפשר לספקי השירות מרחב תמרון בין נפגעים פוטנציאליים מצד אחד לבין גולשים מצד שני, ולקבוע מדיניות לפרסום תוכן של גולשים ובכללה מדיניות להסרת התוכן כרצונו של מפעיל האתר או השירות המקוון. ספק שירות שינהג בדרך האמורה יזכה בחסינות מפני תביעות אפשריות משני צדי המתרס. בתי המשפט בארצות־הברית הדגישו כי ההסדר נועד

---

172 למודל התחולה העקיפה ראו אהרן ברק "זכויות אדם מוגנות והמשפט הפרטי" **ספר קלינגהופר** 163 (יצחק זמיר עורך, 1993); ע"א 294/91 **חברת קדישא גחש"א "קהילת ירושלים" נ' קסטנבאום**, פ"ד מו(2) 464 (1992). לגופים דו־מהותיים ראו בג"ץ 731/86 **מיקרו דף נ' חברת החשמל לישראל בע"מ**, פ"ד מא(2) 449 (1987); ע"א 3414/93 **און נ' מפעלי בורסת היהלומים (1965) בע"מ**, פ"ד מט(3) 196 (1995).

173 אהרן ברק הציע בכתיבה אקדמית לכפוף את העיתונות הפרטית לנורמות מן המשפט הציבורי. ראו אהרן ברק "על העיתונות הפרטית" **עלי משפט** ב 293 (2002). לגישה ביקורתית להצעה זו ראו, למשל, גיא פסח "הבסיס העיוני של עיקרון חופש הביטוי ומעמדה המשפטי של העיתונות" **משפטים** לא 895 (2001).

174 להרחבה ראו אלקין־קורן, לעיל ה"ש 157, בעמ' 377-386.

175 47 U.S.C. §230 (1998).

להגן על חופש הביטוי ולכן פירשו את ההגנה בצורה מרחיבה, מעבר ללשון המשתמעת של החוק.[176] כמה בתי משפט אמנם הביעו אי־נוחות מהכלל הזה אולם החסינות הרחבה עדיין חזקה.[177]

בכל הנוגע לקניין רוחני נבחרה בארצות־הברית גישה שונה – "הודעה והסרה".[178] מדיניות דומה ננקטת באיחוד האירופי בכל סוגי העוולות והפגיעות, ללא התייחסות ייחודית לקניין הרוחני.[179] לפי מדיניות זו, ספק שירות העומד בתנאים שונים יזכה בחסינות. לבם של התנאים הוא מדיניות של הסרת חומר פוגעני לאחר קבלת הודעה מצד הנפגע. מכך יוצא שהספק אינו חייב בניטור מוקדם של התכנים שמעלים הגולשים לאתר, אולם עם קבלת הודעה על תכנים פוגעניים עליו להסירם בהקדם. ההסדרים קובעים גם כללים פרטניים בדבר צורת ההודעה, התחייבות של המודיע לאמיתות ההודעה, צורת קבלת ההודעה ושאר פרטים נלווים.

---

176 עניין *Zeran*, לעיל ה"ש 102. החוק האמריקני [47 U.S.C. §230] קובע, תחת הכותרת "הגנת השומרוני הטוב", כי: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". נוסח פתלתל זה יש לקרוא על רקע ההבחנה במשפט המקובל בקשר ללשון הרע בין דובר, מו"ל ומפיץ: יש מדרג של אחריות ביניהם ותנאים שונים להטלת האחריות עליהם. לפי המשפט המקובל מפיץ חב באחריות רק כשקמה ידיעה שלו בדבר הפגיעה ואף על פי כן הוא ממשיך בהפצה. לכלל זה ביטוי גם בדין הישראלי וראו סעיף 12 לחוק איסור לשון הרע. על רקע הבחנה זו נראה היה שיש לקרוא את החוק האמריקני כך שהוא רואה בספק השירות משום מפיץ ולכן שהספק יהיה אחראי בהתקיים התנאים הקבועים בדין לאחריות מפיץ. אולם, בית המשפט בעניין *Zeran*, לעיל ה"ש 102, קבע כי יש לראות במפיץ משום קטגוריית־משנה שנכללת בתוך הקטגוריה המשפטית של מו"ל, ולכן גם הוא נהנה מחסינות בהתקיים תנאי הסף.

177 ראו, למשל, דעת המיעוט של השופט Lewis בעניין Doe v. America Online, Inc., 783 So.2d 1010 (Fla. 2001); Batzel v. Smith, 333 F.3d 1081 (9th Cir. 2003); ואבחונים שונים בעניין Fair Housing Council of San Fernando Valley v. Roommates.com, LL.C., 521 F.3d 1157 (9th Cir. 2008).

178 ראו 17 U.S.C. §512 (1999).

179 ראו סעיפים 12-15 לדירקטיבת המסחר האלקטרוני: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. נראה שהטעם להבחנה האמריקנית בין סוגי הפגיעות השונים – קניין רוחני מצד אחד וכל שאר הפגיעות מצד שני – נובע בעיקר מלחצים פוליטיים מוצלחים של תעשיות התוכן שביקשו וזכו ביחס מועדף. אני סבור שיש טעם נוסף, והוא הקושי של המשפט האמריקני להודות בקיומו של קונפליקט בין חופש הביטוי לבין דיני הקניין הרוחני ובעיקר זכויות יוצרים. לדיון ראו Birnhack, *Copyright*, לעיל ה"ש 107.

גרסה נוספת של מדיניות חסינות היא של "הודעה, הודעה והפניה לבית משפט" – גישה שהוצעה בקנדה[180] וגם בישראל, בהצעת חוק מסחר אלקטרוני.[181] גם לפי הסדר זה ספק השירות אינו צריך לנטר את התוכן של הגולשים מראש, אבל גם אינו צריך למהר ולהסיר את התוכן עם קבלת הודעה: תפקידו הוא לשמש מעין מתווך בין המתלונן לבין הגולש הפוגע. לאחר שנתקבלה הודעת תלונה מצד הנפגע לכאורה הספק נדרש להעביר את התלונה לידי הפוגע לכאורה. אם "הפוגע" מסכים להסרה או אינו מגיב יוסר החומר; בשאר המקרים, כך לפי ההצעה בישראל, יישאר החומר על כנו באתר.[182]

חשוב להדגיש כי ההסדרים השונים עוסקים בהענקת חסינות ואין בהם משום הטלת אחריות. כאשר מתקיימים התנאים – קמה חסינות; כאשר התנאים אינם מתקיימים – אין מוענקת חסינות, אולם התובע עדיין צריך להוכיח את אחריותו של ספק השירות לפי הדין הרלוונטי – לשון הרע, הגנת הפרטיות, דיני קניין רוחני או דיני הנזיקין הכלליים.

המלכוד

לאור כל זאת, ספק השירות ניצב לפני סיכון שייתבע בעצמו. אם נלווית לאיום התביעה כנגד הספק בקשה לחשיפה של שמות הגולשים, רב הפיתוי של הספק להסיר את איום התביעה הישיר כנגדו במחיר של מסירת פרטי הגולשים. הניסיון הישראלי שנצבר בשנים האחרונות מעלה שחלק מספקי השירות דווקא הגנו על גולשיהם, אולם לא בכל המקרים.[183] זהו מלכוד משפטי: הרצון להימנע מאחריות משפטית עלול להוביל את הספקים לפגוע בגולשיהם.

---

180 ראו סעיף 40.1 להצעת חוק C-60, An Act to amend the Copyright Act, www.parl.gc.ca/PDF/38/1/parlbus/chambus/house/bills/government/C-60_1.PDF. הצעת החוק נתקלה בביקורת ציבורית והוצעה שוב (C-61), אולם טרם התקבלה.

181 ראו סעיפים 7-12 להצעת חוק מסחר אלקטרוני.

182 שם, בסעיף 10(א)(3).

183 למשל: העיתון הנתבע התנגד לחשיפת זהותו של הגולש וטענתו בדבר חוסר סמכות עניינית התקבלה; ראו עניין **דיסקין**, לעיל ה"ש 136, בפסקאות 24, 135. בעניין **סבו**, לעיל ה"ש 78, הגן האתר המארח על הגולש וסירב לחשוף את פרטיו. בעניין **מור מחוזי**, לעיל ה"ש 7, הגנה ספקית שירות הגישה על האנונימיות של הגולשים (וכדברי בית המשפט בפסקה 45, "נלחמה כארי"). לעומת זאת, בעניין **מזמור**, לעיל ה"ש 4, הגישה תחילה התובעת תביעה נגד אתר האינטרנט שאירח את התוכן הפוגעני. תביעה זו הסתיימה בהסדר גישור, שבמסגרתו פרסם האתר הודעה מטעמו כי האתר אינו קשור לתוכן הפוגע. לפי הסדר הגישור הסכימו הצדדים שהתובעת תפנה לבית המשפט בבקשה להורות על חשיפת פרטיו של הגולש האנונימי והאתר יוכל לטעון לחשיבות האנונימיות אולם ישאיר את ההחלטה בבקשה בידי בית המשפט. בבש"א (שלום ת"א) 173154/07 **פרסיקו נ' שידורי קשת בע"מ** (פורסם בנבו, 20.11.2007)

אפשר לראות את המצוקה והקושי שבו נתון הנפגע. לכאורה קל יותר לנפגע לתבוע את הספק של שירות האירוח משום שזהותו ידועה ואילו זהות הגולש עלומה, אולם הקשיים המשפטיים בתביעה כזו וההסדרים המתרבים להענקת חסינות לספקים מצמצמים את אפשרויותיו. סיכוייו לזכות בתביעה נגד הספק קטֵנים ולכן הוא מחפש יעדים חדשים־ישנים לתביעה. לכן אין זה מפתיע שככל שהתבררו ונקבעו ההגנות שיש לספקי השירות בישראל מפני תביעות של נפגעים, גדל מספר התביעות כנגד הגולשים האנונימיים.[184] כעת, לאחר שעניין מור חסם את האפשרות של חשיפת גולשים – לפחות עד שיחוקק חוק או עד שתשונה ההלכה – יהיה מעניין לראות אם יש גידול במספר התביעות נגד ספקי השירות.

(ב) מלכוד שני: בין הנפגעים לגולשים

בצד זה הספק נתון בצבת שיקולים אחרים, עסקיים, שגם להם יש השלכה על התנהגות הצדדים. בתמצית, הספַּק "הסביר" אינו מעוניין לפגוע במבקשי החשיפה מצד אחד, אבל גם אינו מעוניין לפגוע בגולשים המשתמשים בשירות שלו, מהצד האחר. אך טבעי שספק יבקש לעצב את סביבת הפעילות שהוא מפעיל בצורה מיטבית, לפי המודל העסקי שלו. בקצה אחד נמצא ספק שירות שבוחר להקים אתר איכותי, שמאפשר שיח ותגוביות – אולם ברמה גבוהה, שיח הכולל טענות מושכלות ואין בו ניבולי פה, שגיאות כתיב והקלדה או קלישאות נבובות. זו בחירה בשיח איכותי ואולי אף אליטיסטי. שיח המבקש להימנע מפגיעות שווא בצדדים שלישיים ייאלץ לעשות זאת במחיר של בקרה על התכנים (מראש או בדיעבד) או במחיר שיידרשו הגולשים לשלם כגון הרשמה מזוהה מראש, שמאפשרת רק למי שנרשם להגיב, פרסום מראש של כתובת IP של הגולשים המגיבים או מדיניות של מסירה פשוטה ומהירה של פרטים מזהים בדיעבד, לכל דורש, ללא הערמת קשיים. בשונה מסעיפים חוזיים־משפטיים בתקנוני שימוש שאיש אינו קורא ואינו מבין, הסיכויים שהגולשים יבחינו

השאירה ספקית השירות את ההחלטה בידי בית המשפט בלי שטענה בשם הגולשים. באותו מקרה היה המבקש עובד של המשיבה, שהפעילה את האתר שבו נכתבו התגובות האנונימיות הפוגעניות. באחת הפרשיות שאוחדו בעניין מור מחוזי, לעיל ה"ש 7, הפנה האתר המארח (אתר "דוקטורס", שבבעלות חברה בשם קומרקס בע"מ) את המבקש לבית המשפט, ושם לא נקטה החברה עמדה לגוף העניין ואף לא התייצבה לדיון. ראו תיאור ההליכים שם, בפסקה 9. הדיון בבקשת רשות הערעור (עניין מור, לעיל ה"ש 2) כוון נגד ספקית שירות הגישה.

184 לטענה דומה בהקשר האמריקני ראו Shaun B. Spencer, *CyberSlapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMP. & INFO. L. 493, 494-495 (2001); Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 871-872 (2000). ראו גם את הערות השופטים בעניין *Verizon*, לעיל ה"ש 109, בעמ' 1231-1232.

באמצעים האלה רבים יותר – במיוחד בסינון התכנים ובוודאי בדרישת הרשמה מוקדמת – ויכלכלו צעדיהם בהתאם. מי שלא יקבל את כללי המשחק לא יגיב שם. מובן כי טענה זו מניחה שהגולשים מבינים את משמעות הפרסום של פרטיהם המזהים, וככל שמדובר בכתובת IP – שהם יודעים מהי ומה כוחה.

בקצה שני נמצא ספק שירות שמעדיף כמות מגיבים וגולשים על פני איכות. ספק כזה יבקש לפנות למכנה משותף רחב ככל האפשר, שבמקרים רבים הוא גם מכנה משותף נמוך ורדוד. במקרה כזה אין סינון, בקרה או עריכה. שיח פופולרי יבקש להציב משוכות מעטות ככל האפשר בדרכם של הגולשים המבקשים להגיב, מתוך מחשבה סבירה בהחלט שמגבלות ימנעו ביטויים ביקורתיים רצויים, דעות מקוריות ולא קונבנציונליות, חשיפת שחיתויות וכדומה. המחיר של מדיניות ליברלית בקשר להשתתפות בשיח הוא חשש מוגבר לפגיעה בצדדים שלישיים.

שתי הבחירות האלה וכל הנקודות האפשריות שביניהן הן לגיטימיות וחוקיות כשלעצמן. אלה הן בחירות ערכיות ועסקיות. כל נקודה על פני הספקטרום משפיעה על השחקנים האחרים המעורבים בשיח: הגולשים שמשתתפים בו ישירות ומי שאינם בהכרח משתתפים בו, כלומר: מושאי הכתיבה, שהם הנפגעים הפוטנציאליים.

האפשרויות שיש לספק השירות לעצב את הזירה שהוא מפעיל מגלמות עסקת חליפין (trade off) בין האינטרסים של הגולשים מצד אחד לאלה של צדדים שלישיים שעלולים להיפגע מצד שני, והספק בתווך. האם זהו תפקידו של המשפט להתערב ולקבוע כי מודל אחד עדיף מרעהו? אני סבור שלא. לספק יש זכות קניין וחופש עיסוק לנהל את עסקו כרצונו, בכפוף למגבלות בדין, כמובן. כאשר מדובר בזירת שיח, לספק יש גם זכות לחופש ביטוי, ככל שהוא גם דובר, ולא רק "במה". לספק יש זכות לעצב את ההתקשרות בינו לבין גולשיו, במסגרת חופש החוזים ובכפוף למגבלות דיני החוזים. מובן שיש עוד שחקנים בזירה הזו, למשל מפרסמים. שיקולי הסדרה אחרים עשויים להביא להתערבות משפטית מטעמים אחרים אלה.

האינטרסים והזכויות של הספק אינם רק עניינו. הם מעניינו כולנו, שכן הדרך שבה השיח המקוון מעוצב משפיעה על השיח הציבורי בכלל ועל המטרות שביסודו של חופש הביטוי. ככל שחיינו נהפכים דיגיטליים יותר, ואנו מקיימים יותר ויותר פעילויות ובכלל זה פעילויות תקשורת ושיח בסביבה המקוונת, יש לציבור ככלל עניין בצורה שבה מעוצבת זירת השיח, ובמונחי חופש הביטוי: בשוק הדעות. חלק מההצדקות המקובלות של חופש הביטוי מכתיבות העדפה של סוג שיח אליטיסטי או עממי וחלק אחר אדיש לכך.[185]

185 לדיון בהצדקות של חופש הביטוי ראו פסח, לעיל ה"ש 173.

ההצדקה המדגישה את חשיבותו של חופש הביטוי לפרט הדובר כאמצעי למימוש עצמי ולבניית זהותו של האדם תבכר זירת שיח שבה יש מגבלות מעטות ככל האפשר על הביטוי. ההצדקה שמדגישה את התפקיד המכשירני של חופש הביטוי בעיצוב של שוק הדעות, שנועד להוציא מתוכו את האמת, תבכר גם היא זירה שבה אין מגבלות וחסמים על הכניסה לשוק. ההצדקה שמדגישה את התפקיד של חופש הביטוי כאמצעי לשלטון עצמי של הריבון הדמוקרטי – כלומר: העם – עשויה להעדיף שיח איכותי על פני כמותי.[186] ההצדקה שמדגישה את מרכיב ההשתתפות השוויונית בשיח תעדיף את הכמות (של הדוברים) על האיכות.[187]

המשפט הישראלי לא העדיף הצדקה אחת של חופש הביטוי על פני האחרות והוא מקבל את כולן.[188] הסביבה הדיגיטלית מאפשרת לנו לקיים בו־זמנית זירות שיח מסוגים שונים. אפשר לקיים שיח פופולרי ורדוד ובצדו שיח איכותי ואליטיסטי – וגם את כל סוגי השיח שביניהם. העיקרון בדבר חופש הביטוי מגן על כל סוגי השיח, ללא התייחסות לאיכותם. הריבוי חשוב בפני עצמו. הוא מאפשר את ההפעלה של זכות הקניין, של חופש הביטוי ושל חופש העיסוק של מפעיל הזירה, והוא מאפשר ליחידי הציבור לבחור את הזירה המועדפת עליהם.

השיקול בדבר איכות השיח לא נעלם מעיניהם של בתי המשפט, אולם נראה שלחלקם יש העדפה ברורה לשיח איכותי. מהעדפה זו הם גזרו כללים משפטיים שאינם עולים בקנה אחד עם הניטרליות של המשפט לאיכות השיח.[189] הדברים צפים בדיון השיפוטי בנושא אמינותם של המסרים האנונימיים. בתי המשפט תהו בקשר לאמינות שמייחסים הגולשים

---

186 אבי התאוריה הזו הוא איש החינוך האמריקני אלכסנדר מייקלג׳ון. ראו ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1948), reprinted in POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE (1965). עמדה זו השפיעה רבות על המשפט האמריקני. ראו את פסק הדין הידוע בעניין New York Times v. Sullivan, 376 U.S. 254, 270-271 (1964); ראו גם דבריו של השופט ברנן במאמר שחיבר: William J. Brennan, *The Supreme Court and the Meiklejohn Interpretation of the First Amendment*, 79 HARV. L. REV. 1, 18 (1965).

187 לדיון בהעדפות הסמויות והגלויות של ההצדקות השונות של חופש הביטוי ביחס לכמות של ביטוי, של דוברים או של איכות השיח ראו Michael D. Birnhack, *More or Better? Shaping the Public Domain, in* THE PUBLIC DOMAIN OF INFORMATION 59 (Lucie Guibault & P. Bernt Hugenholtz eds., 2006).

188 לדיון ביקורתי ראו אילנה דיין־אורבך ״המודל הדמוקרטי של חופש הביטוי״ **עיוני משפט** כ 377 (1996).

189 לגישה שיפוטית שזיהתה – בהקשר הנדון כאן – כי גם השיח הירוד זכאי להגנה משפטית ראו עניין **מושקוביץ**, לעיל ה״ש 154.

לביטויים האנונימיים הפוגעניים. הערות השופטים בנקודה זו מתבססות על הנחות והשערות, תוך שניכר כי הם משליכים מניסיונם האישי. כך, למשל, בהחלטה של בית משפט שלום נכתב: "על רקע האנונימיות של הכותבים, חוסר הזדהותם והיותם דמויות פיקטיביות אין הציבור ממילא מייחס לפרסום משקל רב והתכנים המפורסמים אינם נתפסים בהכרח כאמינים בעיני הציבור הרחב",[190] ובערעור בבית המשפט המחוזי באותו עניין הסכים השופט עמית וקבע כי "הביטוי האנונימי הוא 'ביטוי מוחלש' שהקורא הסביר אינו נותן לו משקל של ממש".[191]

נתונים רלוונטיים להערכת אמינותו של הביטוי האנונימי שנזכרו בפסיקה הם זירת הביטוי, כלומר: סוג האתר (שהוא אחד השיקולים באיתור "דבר מה נוסף", לפי עניין **מור מחוזי**), רהיטות הטקסט ותוכנו. ככל שמדובר באתר מכובד, שתפוצתו רחבה וההודעה רהוטה ונטולת שגיאות כתיב – משקלה בעיני השופטים רב. כך, למשל, בעניין **מזמור** העירה השופטת בקשר לתגובית הפוגענית שכתב גולש שכינה את עצמו "יודע דבר": "הפרסום עצמו אינו מנומק, אך הכותב מתבטא בנחרצות, שחורג לכאורה מהבעת דעה, עמדה, או העלאת חשדות למעשים שבוצעו לכאורה. הקורא מקבל רושם ברור שמדובר בקביעת עובדות ובממצאים בדוקים ממקור 'יודע דבר'".[192] הפרסום באתר מוכר ורחב תפוצה, השפה שאינה מתלהמת או קיצונית, לשונו שאינה עילגת ושאין בה שגיאות כתיב – כל אלה הביאו למסקנה שהקורא הסביר ייחס לתגובית משקל רב. בתי משפט אחרים הנהיגו כללים דומים[193] וכך גם בתי המשפט בארצות־הברית.[194] יובל קרניאל הניח גם הוא כי המשקל של ביטוי אנונימי ברשת הוא נמוך, וכותב כי "פרסום אנונימי ברשת הוא חסר משקל וחסר כוח השפעה. אין ביכולתו לעשות דבר מעבר ליכולת להעיד על כותבו המתוסכל והחלש, המתחבא מאחורי הכינוי האנונימי. אין הכותבים יכולים לבטא עמדה או מידע רציני ואמין".[195] מכאן גזר קרניאל מסקנה משפטית שלפיה יש לקבוע דין נפרד

---

190 עניין **ברק 013**, לעיל ה"ש 66, בפסקה 10.

191 עניין **מור מחוזי**, לעיל ה"ש 7, בפסקה 34.

192 עניין **מזמור**, לעיל ה"ש 4, בפסקה ה.

193 ראו, למשל, עניין **מור מחוזי**, לעיל ה"ש 7, בפסקה 38.

194 ראו עניין *Cahill*, לעיל ה"ש 112, בעמ' 37.

195 יובל קרניאל "אנונימיות ולשון הרע באינטרנט – בין חופש ביטוי להפקרות" **עיתונות דוט.קום – העיתונות המקוונת בישראל** 85, 102 (תהילה שוורץ אלטשולר עורכת, 2007) (הספר להלן: **עיתונות דוט.קום**).

לביטוי ברשת, ובהמשך לכך – שהפרסום האנונימי לא יכול לשמש בסיס לתביעה בלשון הרע, ונגזר מכך כי אין לאפשר חשיפת זהות אלא רק במקרים חריגים.[196]

הגם שאני שותף למסקנה האחרונה בדבר חשיפה של זהות הגולשים, היא נסמכת על הנחות הטעונות הוכחה אמפירית. השערותיהם של השופטים (ושל קרניאל) סבירות אולם הן השערות בלבד וטעונות הוכחה לפני שאפשר יהיה להסתמך עליהן לצורך קביעת אמינותו של אתר, ולפני שאפשר יהיה לגזור מכך מסקנה משפטית כללית או פרקטיקולרית. מחקרים שונים שבדקו אמינות של אתרי אינטרנט (לא נמצא מחקר שבחן אמינות של תגובות או אמינות של ביטויים אנונימיים) מצאו שגורמים נוספים משפיעים על האמינות שמייחסים הגולשים לנאמר, בסדר הבא: עיצוב האתר, מבנה המידע שבאתר, מיקוד המידע, התועלת שבמידע המובא באתר, המוניטין שמיוחס לאתר, מידת הדיוק של המידע, פרסום, דעה מוקדמת על האתר, ורק אז נזכר – כשיקול נוסף על הקודמים – סגנון הכתיבה באתר, ולאחריו שיקולים נוספים.[197]

אכן, השיח בתגובות נוטה להתלהמות,[198] לעתים קרובות שפתו משובשת, קלוקלת וסרת טעם; אבל לביטוי האנונימי בכלל ולטוקבקים יש ערך חיובי רב לשיח הציבורי ולתרבות הדיגיטלית.[199] משום כך אני סבור כי בתי משפט שמעדיפים שיח איכותי אבל מתרגמים את ההעדפה הזו להתערבות בבחירה הערכית־מסחרית של ספק השירות, חוטאים להבנת העיקרון של חופש הביטוי ובדרך גם פוגעים בזכויות האמורות של הספק. לפיכך, המסקנה היא כלשונו של השופט ריבלין בעניין מור: "עצם העובדה שיש מבין התגובות שטעמן רע וניסוחן עילג בוודאי אינו מוציא אותן מתחולת הזכות החוקתית לחופש ביטוי".[200]

---

196 שם, בעמ' 98. עמדתו אומצה בעניין כהן, לעיל ה"ש 84.

197 ראו, למשל, B.J. Fogg, Leslie Marable, Cathy Soohoo, Julianne Stanford, David R. Danielson & Ellen R. Tauber, *How do Users Evaluate the Credibility of Web Sites? A Study with over 2500 Participants*, *in* PROCEEDINGS OF THE 2003 CONFERENCE ON DESIGNING FOR USER EXPERIENCES 1 (2003), *available at* tinyurl.com/bb6lgh.

198 ראו איילת כהן ומוטי נייגר "To Talk and to Talkback: ניתוח הרטוריקה של השיח־תגובה (talkback) בעיתונות המקוונת" **עיתונות דוט.קום**, לעיל ה"ש 195, בעמ' 321.

199 לכתב הגנה מרתק על התגובות ראו יעקב הכט "המאבק על ההגמוניה בשוק התוכן המקוון – המקרה של הטוקבק" **מגזין איגוד האינטרנט** (2003) www.isoc.org.il/magazine/magazine4_3.html.

200 עניין מור, לעיל ה"ש 2, בפסקה 15 לפסק דינו של השופט ריבלין.

4. הציבור

מסקנת הדברים עד כה היא שחשוב לזהות את תפקידו של ספק השירות במערך המשפטי, העסקי והחברתי. המשגת הסכסוך בצורה בינארית, בין הנפגע לבין הגולש האנונימי, מחמיצה את מקומו החשוב של ספק השירות. מצד אחד, העמימות בקשר לאחריות הספק לתכנים פוגעניים והמגמה להקנות לספקים חסינות, מטעמים של חופש ביטוי, דוחקת את הנפגעים לתבוע את הגולשים האנונימיים. מצד שני, הספק זכאי לבחור את צורת השיח בזירה שהוא מנהל ויש חשיבות ציבורית כללית שתהיה לספק אפשרות לבחור בין סוגים שונים של זירות שיח. כלל משפטי שקובע את התנאים שבהתקיימם תיחשף זהותו של גולש אנונימי צריך להביא בחשבון גם את האינטרסים והזכויות של הספק, על רקע יחסי הגומלין המורכבים בין השחקנים השונים ובין השיקולים השונים, כפי שתוארו כאן. גם כלל שיפוטי צריך להביא בחשבון את ההשלכות הרחבות שיש למתן צו חשיפה או להימנעות ממתן צו כזה על השיח הציבורי.[201]

הדיון העלה שהשדה כולל עוד שחקנים, מעבר לשני הצדדים הישירים ולספק. השחקן המרכזי הנוסף הוא הציבור: הן הציבור שקורא את התכנים באופן סביל והן זה שעשוי להשתתף בשיח באופן פעיל. כלל משפטי שקובע את אחריותו (או את חסינותו) של ספק השירות משליך על הדרך שבה ינהלו ספקי השירות את זירות השיח. כלל משפטי שיחשוף את פרטי הגולשים בקלות יחסית ישפר אולי את איכות השיח אבל ידיר סוגי שיח פשוטים ועממיים יותר, שגם להם יש מקום וגם הם משרתים את אותן תכליות שמשרת העיקרון בדבר חופש הביטוי. "כלל משפטי חושפני" ידיר גם משתתפים שהאנונימיות הכרחית להשתתפותם בשיח, מחמת האפשרויות החיוביות שיש לאנונימיות ולביטוי האנונימי. מובן שיש לציבור אינטרסים נוספים ובהם שמירת הסדר הציבורי, מימוש זכויות של יחידים ושמירת שלטון החוק בכלל.

מי מייצג את הציבור בבית המשפט? טיבו החד־צדדי של הליך בקשת החשיפה מעלה חשש שהאינטרס הציבורי לא יזכה לייצוג הולם על ידי הצדדים לבקשה. ספק השירות הוא המשיב לבקשה, אולם כפי שהוצג לעיל יש לספק אינטרסים משל עצמו, ובמלכוד הראשון שבו הוא נתון הספק עלול להציל את עורו גם במחיר פגיעה בגולשים. הניסיון מעלה שחלק מספקי השירות מתייצבים בבית המשפט ללא טענה מהותית ומסתפקים בהודעה שלפיה יקבלו את עמדת בית המשפט, תהא אשר תהא.[202] עמדה כזו זולה יותר מבחינת העלויות המשפטיות ויש לה מחיר עסקי נמוך, שכן אם יטענו גולשים כנגד האתר על כך שחשף את

201 ראו ברוח זו עניין **אריאל**, לעיל ה"ש 66.
202 ראו לעיל ה"ש 183.

זהותם יוכל הספק להשיב, ובצדק, כי פעל לפי צו בית משפט. את המחיר של עמדה כזו משלם הציבור בכך שהאינטרס שלו אינו מיוצג כראוי בבית המשפט. גם אם החשש מהמלכוד הראשון אינו מתקיים, הספק עדיין נתון במלכוד השני: שיתוף פעולה של הספק בחשיפת גולשים (בין מראש ובין בדיעבד) יהיה איתות ברור לגולשים ועלול לפגוע בבחירה הערכית ובמודל העסקי של הספק.

כיצד אפשר להתגבר על קושי זה? דרך אחת, והיא דרך המלך, היא הפנמה שיפוטית של המשמעות הרחבה יותר של ההחלטה הקונקרטית, כלומר: בית המשפט הוא נציג הציבור. מובן שטענה זו נכונה לגבי הפסיקה בכלל, אבל כאן סוג ההליך עלול להביא להחמצת ההיבט הציבורי. חוק ברור יכול לסייע לשופטים ולהבטיח שהשיקול הציבורי לא ייעלם מעיניהם. טכניקה חקיקתית אפשרית היא של "הבניית שיקול הדעת" השיפוטי, בכך שהחוק יפרט את השיקולים שעל בית המשפט לשקול ובכלל זה את ההשלכה של המקרה על האינטרס הציבורי של קיום זירות שיח חופשיות, מגוונות ורבות, ללא העדפה א־פריורית של סוג שיח אחד מהאחר. כאשר החוק מונה את השיקולים שיש לשקול, יש להניח שבית המשפט יבחן את השיקולים האלה. דרך שנייה, יצירתית אך יקרה יותר, יכולה **לחייב** התייצבות של גורם ניטרלי, שאינו קשור לצדדים הישירים לסכסוך או לספק, כדי לייצג את העמדה הציבורית.[203] דרך שלישית, נספחת לקודמתה, יכולה להיות **מתן רשות** לגורמים שלישיים להתייצב בהליך המתאים, בבחינת ידידי בית המשפט.

יהא אשר יהא הכלל המשפטי, הוא אינו פועל בחלל ריק ואין לו כוחות־על להתיר את הסבך. כללים משפטיים נתקלים בתגובות טכנולוגיות, חברתיות ועסקיות. כלל משפטי אינו סוף פסוק אלא שלב נוסף במאבק בשדה עתיר־כוחות. לכן ראוי לבחון אותו, ובעיקר את הטכנולוגיה.

ה. עיצוב מדיניות בסביבה טכנולוגית

עיצוב כללים משפטיים לסביבה טכנולוגית בכלל ולטכנולוגיית מידע בפרט צריך לבוא תוך דיאלוג עם הטכנולוגיה. הדיון עד כה הניח שהטכנולוגיה קבועה ונתונה וכי המשפט יכול לחול לגביה. הדיון הציג את המשפט בעמדת תגובה לנסיבות טכנולוגיות חדשות שהן רשת האינטרנט כפי שהיא בנויה כיום, כלומר: שהתקשורת בין המחשבים מבוססת על איתורם לפי כתובות IP. מהניסיונות החקיקתיים והשיפוטיים בישראל ובמקומות אחרים

---

203 למשל: בעניין **בזק בינלאומי**, לעיל ה"ש 61, הוצגה גם עמדת היועץ המשפטי לממשלה בבית המשפט.

עולה עוד שהמשפט אינו חושש לכפות את עמדתו על הטכנולוגיה. בחלק זה אטען, ראשית, שעמדה כזו עלולה להחמיץ פן מרכזי של הטכנולוגיה והוא שהיא מגלמת ערכים. אטען שראוי ללמוד את הטכנולוגיה, לחלץ ממנה את הערכים הגלומים בה ולבחון אותם בבדיקה ערכית. הדיון עד כה כלל הנחה מובלעת כזו וכעת יש להציפה. שנית, אטען שהעמדה המשפטית הנוכחית היא תלוית־טכנולוגיה וככל שהיא מניחה שהכלל המשפטי שיוחל על הטכנולוגיה יביא סוף פסוק לבעיה המוסדרת – הרי היא שגויה. לשם כך אראה כי הטכנולוגיה מגיבה לכללים המשפטיים המתגבשים באמצעות פיתוח טכנולוגיות של אנונימיות. כלל משפטי נבון צריך לצפות את האפשרות הזו ולהתמודד איתה.

1. טכנולוגיה של ערכים

ההנחה שהטכנולוגיה היא נתון נפוצה בחשיבה המשפטית. כשם שדיני הקניין מניחים את קיומם של מקרקעין ומיטלטלין ומסדירים אותם בלי לתהות בדרך כלל אחר טיבו הפיזי של המשאב, כך גם הסדרה משפטית של טכנולוגיה נוטה להתייחס לטכנולוגיה כמות שהיא, לזהות את הבעיות שמתעוררות ולהציע להן פתרון. כך, למשל, דיני הקניין מזהים את חשיבותו של משאב המקרקעין לבני אדם ואת הקשיים שמתעוררים בקשר לניהול המשאב, ולכן הם מבקשים להציע משטר קנייני שקובע את הבעלות במשאב, את אפשרויות השימוש בו והסדרים פרטניים יותר.[204] אולם דיני המקרקעין אינם סבורים שיש במקרקעין "ערכים" שמגולמים בהם; המקרקעין הם נתון בחשיבה המשפטית ומה שנבדק הוא היחס שלנו, בני האדם, אליהם.

ההסדרה המשפטית של טכנולוגיה נוטה להתייחס לעתים לטכנולוגיה באופן דומה: דיני הטכנולוגיה כמוהם כדיני הסוס, כפי שהכריז השופט האמריקני פרנק איסטרברוק (Easterbrook).[205] אולם, הטכנולוגיה שונה מהמקרקעין ומהסוסים שהם יציר הטבע: הטכנולוגיה היא יציר האדם. האדם מפתח את הטכנולוגיות השונות בתוך סביבה אנושית, חברתית־קהילתית או תאגידית־עסקית. בין בכוונת מכוון ובין ללא כוונה או אפילו הבנה,

---

204 לחשיבות המקרקעין לבני אדם ראו חנוך דגן **קניין על פרשת דרכים** (2005). דגן מקדם עמדה של הכרה ב"ערכים קנייניים", אולם אלה הם ערכים שמשויכים לדין, לאו דווקא למשאב המוסדר. לשיטתו, לטיבו של המשאב יש חשיבות רבה, שכן היחס שלנו משתנה לפי החפץ שבו מדובר. היחס למקרקעין שונה מהיחס לטבעת נישואין, למשל.

205 ראו Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

מפתחי הטכנולוגיה מטמיעים ערכים מסוימים בתוך יציר כפיהם.[206] כך, למשל, סכין יכולה לשמש להכנת סעודה ואז נאמר שהיא מגלמת ערך חיובי של יעילות, אבל אותה סכין יכולה לשמש גם לאיום, לשוד, לתקיפה ולרצח, ולחלופין להגנה עצמית. במקרה כזה נאמר שהסכין היא כלי נשק או אמצעי הגנה. היא מגלמת ערכים של אלימות או הגנה וקדושת החיים, בהתאמה. דוגמה זו ממחישה שאותה טכנולוגיה יכולה לגלם כמה ערכים סותרים בו־זמנית.

לעתים הוויכוח הוא על עצם קיומם של ערכים המוטמעים בטכנולוגיה. כזהו, למשל, הוויכוח הציבורי הנמשך בארצות־הברית בקשר להחזקת כלי נשק אצל אזרחים. המתנגדים מדגישים כי רובים וכלי נשק הם אמצעי הרג. הטכנולוגיה של הרובה מגלמת את הערך הזה ולכן המסקנה היא שיש לצמצם את אחזקת הנשק האזרחית ככל האפשר. התומכים בהחזקת נשק, ובמיוחד ארגון ה־NRA (National Rifle Association), מבקשים להסיט את הוויכוח מכלי הנשק אל המשתמשים בו. סיסמתם הידועה היא כי נשק אינו הורג אנשים – אנשים הורגים אנשים (guns don't kill people, people kill people).

הערכים המגולמים בטכנולוגיה אינם רק אלה שהוטמעו בה בעת הפיתוח אלא גם המשמעות שהחברה מעניקה לטכנולוגיה.[207] ההבניה החברתית של הטכנולוגיה יכולה להיות תהליך ממושך; במידה רבה אין לתהליך הזה קו סיום.[208] כך הדבר כאשר הטכנולוגיה שנויה במחלוקת כגון בקשר לאמצעי מניעה שהם פרי פיתוח מדעי וטכנולוגי. הם מאפשרים למשתמשים לקיים יחסי מין ולהימנע מהריון וכן הם משמשים אמצעי הגנה מפני העברה של מחלות מין. התומכים באמצעי המניעה רואים בהם טכנולוגיה של שליטה ברבייה ושל מין בטוח; אחרים, אנשי דת בעיקר, רואים בהם טכנולוגיה של פריצות שכן היא מצמצמת השלכות לא רצויות של קיום יחסי מין מזדמנים ובכך מעודדת אותם. הוויכוח הזה נסב על השאלה מהם הערכים שמגולמים בטכנולוגיה הזו. זהו ויכוח ערכי בין השקפות עולם שונות. לענייננו, בטכנולוגיה הדיגיטלית וברשת האינטרנט מוטמעים ערכים רבים.

---

206 ראו HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (Batya Friedman ed., 1997); יובל דרור **הפוליטיקה של הטכנולוגיה** (2006).

207 זו הגישה המכונה Social Construction of Technology – SCOT. לדיון ראו יובל דרור "חץ ההבניה – על הקשר שבין הסוכן האנושי לארטיפקט הטכנולוגי" **משפט וטכנולוגית מידע**, לעיל ה"ש 31 (להלן: דרור "חץ ההבניה"); אורן ברכה "הייל ופוקו במרחב הדיגיטלי: כח, טכנולוגיה, ומשפט בחברת המידע" **משפט וטכנולוגית מידע**, לעיל ה"ש 31.

208 ראו דרור "חץ ההבניה", לעיל ה"ש 207. דרור מבקר את גישת SCOT, שמניחה כי יש "סגירה" ערכית (closure) של המשמעות הערכית של טכנולוגיה.

ראוי לחלץ אותם ולבחון אותם: אלו מהם ראויים בעינינו? אלו מהם פסולים? קושי מרכזי בסביבה הטכנולוגית הוא להפריד את הרע מן הטוב.

רשת האינטרנט, כפי שהיא כיום, אינה כוללת אנונימיות מלאה אבל גם אין בה זיהוי מלא. הסיבה היא שימוש הרקע שנעשה ברשת בכתובות IP לשם יצירת התקשורת בין המחשבים וצורת ההקצאה של הכתובות (באמצעות ספקי שירות וכתובות דינמיות). כפי שציינו כמה מלומדים, מאפיין זה יוצר נורמה שבה הזהות אפשרית למעקב (traceable).[209] במובן זה, הטכנולוגיה מאפשרת מרחב ערכי לקבוע אם אנו רוצים לאפשר את החשיפה אם לאו. אילו הייתה הרשת בנויה כך שאין שום אפשרות לחשיפה השאלה המשפטית הייתה אחרת, אם בכלל: האם יש לאסור את הטכנולוגיה כמות שהיא או לדרוש את שינויה? אילו הייתה הרשת בנויה כך שיש בה זיהוי מלא, יש להניח שהיישומים והשימושים בה היו שונים מאלה שיש לנו כיום.

הרשת מגלמת ערכים נוספים, בין היתר ערך של אפשרות להשתתף בשיח הציבורי. השיח הציבורי מתנהל בכמה זירות – פיזיות ומקוונות, מקומיות וגלובליות, פתוחות או סגורות ועוד אינספור מאפיינים. בהשוואה לזירות השיח הפיזיות יש לסביבה הדיגיטלית פוטנציאל להגביר את הנגישות של דוברים רבים יותר לזירות האלה, הן כמאזינים והן כדוברים, תוך צמצום חסמי הכניסה ל"שוק הדעות" ותוך צמצום הכוח של מתווכים ושומרי סף שונים. בשנות התשעים של המאה הקודמת הועלתה תכונה זו על נס ונאמר כי הרשת היא "טכנולוגיה של חופש".[210] עד מהרה התברר כי המציאות מורכבת יותר:[211] במקום המתווכים הישנים באו מתווכים חדשים;[212] יש פער דיגיטלי שאינו יוצר הזדמנות שווה לכולם להשתתף בשיח הזה; פערים של שפה, אוריינות טכנולוגית, מוגבלות פיזית ופערים אחרים מקשים גם הם את ההשתתפות. אלה הם קשיים שיש להתמודד איתם והדיון בהם חורג ממסגרתו של מאמר זה; אולם מסקנה אחת אפשר לגזור מההבנה בדבר האפשרויות החיוביות שיש בטכנולוגיה לשיח הציבורי ולחופש הביטוי בכלל: המשפט צריך לעשות כל שביכולתו לעודד את השיח הזה מתוך הבנה שזהו עיקרון דמוקרטי בסיסי. ההצדקות הקלאסיות של חופש הביטוי זוכות לעדנה בסביבה הדיגיטלית. אפשרויות המימוש העצמי

---

209 ראו לעיל ה"ש 25.

210 Eugene Volokh, *Cheap Speech and What it Will Do*, 104 YALE L.J. 1805 (1995).

211 למבט מוקדם אך מפוכח, ראו Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1994).

212 לדיון ב"תקוות החופש" שתלו רבים ברשת האינטרנט וההתפכחות ממנה ראו אלקין־קורן, לעיל ה"ש 157.

התרחבו לאין שיעור; חסמי כניסה לשוק הדעות הצטמצמו (אם כי יש חסמים חדשים); השקיפות השלטונית וזרימת המידע הדו־סטרית בין העם הריבון לנציגיו בשלטון "עלתה כיתה"; האפשרות להשתתף בשיח נפתחה לפני דוברים רבים יותר (אם כי הפער הדיגיטלי, כאמור, טעון טיפול).

בצד זה, תכונת האנונימיות של הרשת אינה נתון קבוע. בתי המשפט צריכים לגבש את עמדתם הערכית באשר לאנונימיות. יש הרואים בה מסכה המאפשרת התחמקות מאחריות אישית וחברתית וכלי לניצול לרעה. אין ספק שיש המנצלים את האנונימיות לרעה; אולם הדיון במשמעות הנורמטיבית של האנונימיות העלה שיש לה פנים חיוניים וחיוביים רבים. שיוך האנונימיות לגג המשפטי הכפול של חופש הביטוי והזכות לפרטיות מדגיש זאת. לכן, אין להתייחס לאנונימיות כאל "רעה" או כאל "טובה": האתגר המשפטי הוא להבחין בין מצבי אנונימיות חיוביים לשליליים, בין המקרים שבהם היא מנוצלת לרעה לבין המקרים שבהם יש בה ערך ראוי.

2. טכנולוגיה של אנונימיות

(א) פיתוח מכוון

מפתחי הטכנולוגיה אינם אדישים לסוגיה הנדונה. יש מי שעסוקים באופן פעיל בפיתוח טכנולוגיות שיאפשרו גלישה אנונימית ברשת. טכנולוגיות של אנונימיות הן תת־קטגוריה של טכנולוגיות מקדמות פרטיות (PET; Privacy Enhancing Technology).[213] חוקרי מחשב רבים שוקדים זה קרוב לשלושה עשורים על פיתוח יישומים שונים לתקשורת שתאפשר לצדדים משוחחים להישאר אנונימיים זה כלפי זה, וכן על פיתוח יישומים שיאפשרו לגולשים לנהל שיחה אנונימית בלי שגורם חיצוני יידע על עצם קיומה או על זהות הצדדים.[214] כיום אפשר לזהות כמה סוגים מרכזיים של טכנולוגיות של אנונימיות. הסקירה

---

213 לסיווג הטכנולוגיות השונות של אנונימיות ראו Carlisle Adams, *A Classification for Privacy Techniques*, 3 U. OF OTTAWA L. & TECH. J. 35 (2006).

214 השיח של חוקרי מדעי המחשב ומערכות מידע הוא שיח מרתק. "השיח המחשבי" מניח בדרך כלל הנחת רקע סמויה למחצה, שלפיה צריכה להיות למשתמשים שליטה מוחלטת בסודיות המסר ו/או בזהותם. בגרסה הבוטה של השיח המחשבי הזה, כל התערבות חיצונית, גם אם מקורה בכללים משפטיים לגיטימיים, נתפסת כצנזורה. ראו, למשל, Andrei Serjantov, *Anonymizing Censorship Resistance Systems*, *in* REVISED PAPERS FROM THE FIRST INTERNATIONAL WORKSHOP ON PEER-TO-PEER SYSTEMS 111 (2002). הכותב מתייחס למגבלות משפטיות, שמקורן בדיני זכות יוצרים כאל צנזורה. ניכר כי גישתם של מדעני המחשב קרובה לעמדת המשפט האמריקני בכל הקשור לחופש הביטוי, שהגנתו קרובה

שלהלן אינה מתיימרת להיות כוללת אלא להציג את סוגי השאלות והפתרונות שהציעו מפתחי הטכנולוגיות ואת השאלות שאיתן צריך המשפט להתמודד – או אולי את השאלות שאיתן המשפט צריך שלא להתמודד.[215]

תיווך אנונימי

סוג נפוץ של טכנולוגיות אנונימיות מתבסס על תיווך של גורם ביניים, שתפקידו לטשטש את מקורו של המסר המקוון ובכך לשמור על חשאיותו של הגולש האנונימי. דוגמאות לכך הן שירות דיוור־חוזר (re-mailing), שרתי פרוקסי (proxy) שונים או שירותי אנונימיות ייעודיים כמו אנונימייזר (Anonymizer).

שירות הדיוור החוזר שהציע Johan Helsingius מפינלנד בשנות התשעים של המאה הקודמת ממחיש את פעולת התיווך כמו גם את סכנותיה. העיקרון פשוט: במקום שיגור ישיר של המסר מהמוען לנמען – צורת תקשורת שחושפת לפני הנמען את כתובת ה־IP של המוען – המוען משגר את המסר למתווך הדואר, שמעבירו הלאה ליעד תוך מחיקה של פרטי השולח. השירות לא האריך ימים; משטרת פינלנד נענתה לדרישה של נציגי הסיינטולוגיה ודרשה מהמפעיל לחשוף את זהותו של גולש אנונימי בקשר לטענות בדבר הפרה של זכויות יוצרים.[216]

בדומה לשירות זה של תיווך דואר, אתרי אינטרנט שונים מציעים שירותי גלישה אנונימית, חינם או בתשלום. הבולט שבהם הוא אנונימייזר. במקום לגלוש ישירות באתר המבוקש, הגולש פונה לאתר האנונימייזר ובאמצעותו גולש לאתר המבוקש. בדרך זו, התקשורת מתנהלת בשני שלבים: בין הגולש לבין המתווך ובין המתווך לבין אתר היעד. אתר היעד יזהה את כתובת ה־IP של המתווך אבל לא את זו של הגולש. בצד אתרים ייעודיים אפשר לגלוש באמצעות שרתי proxy.[217] שרתים אלה, בין בתשלום ובין חינם, מאפשרים לגולש להציג את גלישתו כלפי האתר הנמען כאילו הוא מגיע משרת הפרוקסי

למוחלטת. ראו, למשל, את הערותיהם של מפתחי מערכת TOR שתידון בהמשך. ניתוח מפורט של שיח זה חורג מגדרי המאמר.

215 לדיון בהקשר האמריקני ראו Rubinstein, Lee & Schwartz, לעיל ה״ש 35, בעמ׳ 274-280.

216 ראו Ron Newman, *The Church of Scientology vs. anon.penet.fi* (1996) www.spaink.net/cos/rnewman/anon/penet.html.

217 לסקירה בהירה של שרתי פרוקסי והאפשרויות שהם מספקים ראו whatismyipaddress.com/staticpages/index.php/how-do-i-hide-my-ip-address.

ולא ממחשבו שלו.[218] בצד שימושים כאלה, שרתי הפרוקסי מטשטשים את עקבותיו של הגולש.

אולם שירותי תיווך אינם מספקים הגנה מלאה לגולש האנונימי. גורלו המר של השירות הפיני חושף את החולשה של מודל זה: הוא נסמך על מתווך שממלא תפקיד של "חוליית אמון". כאשר האמון נשבר – בין משום שהמתווך מעל באמון הגולשים האנונימיים ובין משום שהוא עצמו נהפך יעד לגורמים חיצונים כמו האקרים, תובעים פוטנציאליים או רשויות אכיפת החוק –זהות הגולש עלולה להיחשף.[219] משמעות הדבר היא שהאנונימיות אינה מובטחת גם בשימוש בשירות תיווך, אבל בכל מקרה היא מעלה את מחיר החשיפה מצד התובע. תובע שיבקש לחשוף גולש שהשתמש בשירותי תיווך של אנונימיות כאמור, יגלה עד מהרה כי מדובר בשירות כזה, העשוי להימצא במדינה אחרת. תביעה כנגדו אפשרית אולם מחירה עולה וסיכוייה קטנים יותר.

מקור איום נוסף על האנונימיות של המשתמשים בשירותי תיווך הוא גורם־על שיכול לראות את התמונה כולה, כלומר: גם את השלב הראשון של גלישה או משלוח דואר מצד הגולש אל האתר המתווך וגם את השלב השני, של גלישה או משלוח דואר מצד המתווך. גורם חיצוני כזה יכול לחבר את שני הנתונים ולהסיק את הקשר שבין הגולש האנונימי לבין היעד. פעולה כזו היא מורכבת, יקרה, מסובכת וקשה לביצוע בגלל כמויות המידע האדירות שיש ברשת, אולם לגורם שתהיה מוטיבציה חזקה דיה – כמו, למשל, המדינה במצבי משבר ביטחוני – האפשרות קיימת.

---

218 לשירות כזה שימושים רבים כמו עקיפת מגבלות מקומיות על גלישה. כך, למשל, ממשלת סין חוסמת מאזרחיה גישה לאתרים רבים. גלישה באמצעות שרת פרוקסי יכולה לעקוף את המגבלה – אלא אם גם שרת זה, כמובן, חסום לגישה. שרת פרוקסי יכול לסייע גם לעקוף סינון שמבצע אתר היעד לפי כתובות IP. למשל, אתר שמבקש לפנות רק לאזרחי מדינה מסוימת – אולי מחמת רצון להימנע מחשיפה לאחריות משפטית במדינות אחרות – מזהה את גולשיו לפי כתובת IP ומאפשר רק למי שמגיע ממדינה מסוימת לגלוש באתר. בגלל מערך ההקצאה של כתובות IP ניתן לשייך כתובת וירטואלית לאזור גאוגרפי בשיעור דיוק ניכר. בפרשה ידועה טענה חברת Yahoo האמריקנית כי אינה יכולה לזהות מי מגולשיה מגיע מצרפת ולחסום לפניו אפשרויות של סחר במזכרות נאציות, האסור בצרפת. בית המשפט הצרפתי לא השתכנע, בין היתר בגלל אפשרות הזיהוי לפי כתובות IP. ראו League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc. (USA), Yahoo France (County Court, Paris, 2000).

219 המשתמש נמצא בדילמה: אם יהיה היחיד שישתמש בשירותי תיווך, או יטמיע אותם בתוך מערכת המחשוב שלו, קל יהיה לזהותו; אם ירצה לטשטש את עקבותיו בתוך ערב רב של משתמשים אחרים אין מנוס אלא לתת אמון בשירות תיווך חיצוני. לטענה זו ראו Alessandro Acquisti, Roger Dingledine & Paul Syverson, *On the Economics of Anonymity*, FINANCIAL CRYPTOGRAPHY – FC '03 (2003).

ערבול

פיתוח משמעותי שקדם לתיווך האנונימי, וקל יותר להבין את חשיבותו כעת, הוא של דיוויד צ׳אום (Chaum), במאמר שפרסם בשנת 1981.[220] צ׳אום הציע לערבל (MIX) מסרים שונים. התקשורת הישירה בין הגולש לאתר היעד מומרת בגלישה באמצעות מתווך, שצובר מסרים מוצפנים שונים ממקורות ואל מקורות שונים, כאשר לכל המסרים תכונות חיצוניות דומות (כגון נפח זהה); המתווך משנה את ההצפנה שלהם, משנה את סדר המסרים ומעביר אותם ליעדם בסדר שונה. כך, גורם שמצותת לגלישה יתקשה לזהות איזה מסר נשלח מאיזה גורם לאיזה גורם. כדי לשפר את המערכת ולמנוע ממתווך יחיד לדעת את הקישור בין שולחי המסרים למקבליהם הציע צ׳אום להעביר את המסרים דרך כמה מתווכים בזה אחר זה, כשכל אחד מהם משנה את הצפנת ההודעות ומערבל את הסדר ביניהן. בצורה זו רק קואליציה של כל המתווכים יחדיו יכולה לגלות איזה מקור שלח הודעה למקבל הודעה מסוים. הרעיון הזה הופעל במערכות רבות. מערכת כזו אמנם מגנה מפני גורם־על חיצוני שאלמלא המערכת יכול היה לקשר בין הגולשים ליעדי הגלישה שלהם, אבל אינה מציעה אנונימיות של הגולש כלפי גורם הביניים.

אנונימיות בהמון

פיתוח נוסף שמתגבר על הקשיים של מערכות התיווך האנונימי, ובעיקר על החשש שנובע מהתלות בחוליית־אמון יחידה, הוא טכנולוגיות שמתבססות על רעיון ההמון. כאשר אדם נמצא לבד במרחב גדול, קל יחסית לאתרו; כאשר האדם הוא חלק מההמון קשה לזהותו בקרב הרבים שסביבו והוא נהנה בפועל מאנונימיות רבה יותר. מערכת Crowds, למשל, פותחה בשנות התשעים של המאה הקודמת על בסיס רעיון זה: משתמשים ממקומות שונים קובצו יחדיו ל״המון וירטואלי״ והגלישה האינדיבידואלית של חברי הקבוצה שויכה לקבוצה ולא לגולש מסוים.[221] בדרך זו, חוליית האמון הבודדת של מערכות התיווך האנונימי השונות מתחלפת במערכת מבוזרת.

גם למערכת כזו יש חסרונות. ראשית, יש קושי בארגון קבוצה כזו. מובן שצריך שיהיו בה חברים רבים ככל האפשר. כמו כן, גם כאן גורם־על חיצוני עלול לזהות את מקור המסר. קשיים ספציפיים עשויים להתעורר, למשל, כשהמערכת מתקשה לתפקד בסביבה מאובטחת

---

220 ראו David L. Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, 24 COMMUNICATIONS OF THE ACM 84 (1981).

221 ראו Michael K. Reiter & Aviel D. Rubin, *Crowds: Anonymity for Web Transactions*, 1 ACM TRANSACTIONS ON INFORMATION & SYSTEM SECURITY 66 (1998).

כמו זו שיש בה, לדוגמה, חומת אש (firewall),[222] או שהמערכת יוצרת תעבורה עודפת ברשת.[223]

"ניתוב בצל"

סוג רביעי של טכנולוגיות של אנונימיות הוא "ניתוב בצל" (onion routing) או ניתוב רב־שכבתי, המשכלל את טכנולוגיות התיווך. בדומה לתיווך האנונימי, המסר מועבר ליעדו דרך גורם מתווך. בשונה ממערכות כמו אנונימייזר, ובדומה למערכות הערבול וההמון, המערכת בנויה מאוסף מתווכים. התיווך נעשה על ידי קהילה מבוזרת של מתווכים היוצרת רשת שמעבירה את המסר מיד ליד. מאחר שהקהילה מבוזרת אין לה מרכז: אין בה גורם שמנתב את התעבורה ברשת ושולט בה בדרך כלשהי. המסר עטוף באינספור שכבות ומכאן דימוי הבצל; כל חוליה במערכת מסירה שכבה אחת ומעבירה את המסר קדימה. חיסרון אפשרי של המערכת הוא פעולה של גורם עוין שמצליח להתברג למערכת, כמו מרגל, ויכול ללמוד את דפוסי התעבורה במערכת ולנסות לפי זה לשחזר את מקור המסר.

יישום ספציפי של רעיון ניתוב הבצל, המבקש להתגבר על הקושי הנ"ל, הוא TOR.[224] מערכת TOR מאפשרת למחבר המסר ליצור תחילה אפיק בטוח בתוך מערכת החברים[225] בדרך שגם חבר־מתווך אינו יודע מהיכן מגיע המסר. כך, גם אם יידרש החבר במערכת לחשוף את מקור המסר, הוא לא יידע לעשות זאת; גם הנדסה חוזרת תיכשל. אחד ממפתחי המערכת, רוג'ר דינגלדיין (Dingledine) תיאר זאת כ"אמון מבוזר".[226] המערכת תוכננה כך שהיא ידידותית למשתמשים ומטילה על גורמי הביניים עלויות נמוכות יותר משהטילו עליהם המערכות הקודמות. המערכת תוכננה להעברת מסרים פשוטים ולכן אינה מתאימה למערכות לשיתוף קבצים (P2P). גם למערכת TOR יש מגבלות וקשיים: היא אינה חסינה

---

222 שם, בעמ' 90. להשוואה של מערכת זו למערכת הערבול ראו שם, בעמ' 71.

223 למערכת שמבקשת להתגבר על הקושי הזה ראו Marc Rennhard, Sandro Rafaeli, Laurent Mathy, Bernhard Plattner & David Hutchison, *Analysis of an Anonymity Network for Web Browsing*, *in* PROCEEDINGS OF THE 11TH IEEE INTERNATIONAL WORKSHOPS ON ENABLING TECHNOLOGIES 49 (2002).

224 ראו www.torproject.org (להלן: אתר TOR). המערכת הוצגה לראשונה במאמר: Roger Dingledine, Nick Mathewson & Paul Syverson, *Tor: The Second-Generation Onion Router*, *in* PROCEEDINGS OF THE 13TH USENIX SECURITY SYMPOSIUM (2004).

225 ובכך היא שונה ממערכות קודמות, שיצרו את אפיק ההעברה עם העברת המסר. ראו שם, בפסקה 4.2.

226 Roger Dingledine, *TOR: An Anonymous Internet Communication System*, THE FREE HAVEN PROJECT (2005), *available at* www.idtrail.org/files/dingledine%20-%20Tor.pdf.

ממתקפה של גורם־על חיצוני[227] ומפני לימוד נמשך של אתרי היעד את המבקרים בהם, היכול להביא לחשיפתם.[228] קושי נוסף הוא שהגורם האחרון במערכת, שממנו יוצא המסר אל אתר היעד, ייחשב בטעות כמקור המסר. כתוצאה מכך, כאשר יתבצע הליך חשיפה יגיעו המשטרה או המתלוננים אל החוליה האחרונה ויראו אותה ככתובת לטענותיהם; חיסרון אחר הוא שאתרי היעד חוסמים את הגישה לכל משתמשי TOR.[229] מפתחי המערכת הגדירו סוגים שונים של חוליות שחלקן הוא "חוליות יציאה", והמנהלים של אותה חוליה יכולים להחליט על מדיניות השימוש בנקודת היציאה מהמערכת, למשל: לא לאפשר העברת קבצים מסוגים מסוימים.[230]

(ב) פתרון טכנולוגי?

הסקירה אינה ממצה ויש טכנולוגיות־של־אנונימיות רבות נוספות.[231] אולם לצורך הדיון המשפטי חשוב להכיר בקיומן של טכנולוגיות כאלה, המתפתחות על רקע צרכים שונים, או לפחות על פי ההשערה של מפתחיהן בדבר צורכי המשתמשים. הטכנולוגיות מאפשרות הגנה סבירה על זהות הגולשים מפני גורמים חיצוניים לתקשורת וגם זה כלפי זה. בקרב מפתחי המערכות השונות יש הסכמה כי אין מערכת החסינה לחלוטין מפני מתקפה של גורם שיבקש לגלות מי שוחח עם מי, ולענייננו – איזה גולש גלש היכן; אולם ברור שעלות החשיפה היא גורם משמעותי ושגם האינטראקציה בין האפשרות הטכנולוגית למגבלות הכלכליות היא נתון חשוב להכרעה בדבר עיצוב הכלל המשפטי.

לפי שעה נראה שהטכנולוגיות לא זכו להצלחה רחבה בקרב הגולשים. לא קשה לשער מדוע. כדי להשתמש בהן נדרש הגולש תחילה לדעת שיש בעיה, כלומר: שהאנונימיות שלו היא "על תנאי", שהיא יחסית וחלקית בלבד ושאפשר להסירה ללא קושי רב במיוחד. ספק

---

227 שם, בפסקה 3.1.

228 להצעה להתמודדות עם קושי זה ראו Nicholas Hopper, Eugene Y. Vasserman & Eric Chan-Tin, *How Much Anonymity Does Network Latency Leak?*, *in* PROCEEDINGS OF THE 14TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 82 (2007).

229 לדיון ולהצעת פתרון טכנולוגי ראו Peter C. Johnson, Apu Kapadia, Patrick P. Tsang & Sean W. Smith, *Nymble: Anonymous IP-Address Blocking*, *in* LECTURE NOTES IN COMPUTER SCIENCE 113 (2007). ההצעה מבוססת על יצירת "רשימה שחורה" של גולשים שגישתם לאתרי היעד תיחסם בלי שזהותם תיחשף לידיעת האתרים.

230 ראו שם, בפסקה 6.2.

231 לסקירה מקיפה ראו George Danezis & Claudia Diaz, *A Survey of Anonymous Communication Channels*, *in* MICROSOFT RESEARCH TECHNICAL REPORT (2008), *available at* ftp://ftp.research.microsoft.com/pub/tr/TR-2008-35.pdf.

כמה ועד כמה הגולשים מודעים לאפשרויות הטכניות של איסוף מידע עליהם. נושא זה אמנם טעון מחקר אמפירי ועשוי בהחלט להשתנות במשך השנים, אך נראה כי גולשים רבים סבורים שהם נהנים מאנונימיות באינטרנט, וכמו הקריקטורה המפורסמת של הניו־יורקר משנת 1993 – שאיש אינו יודע שהם כלב.[232] תנאי הגלישה (בבית, תוך שימוש במחשב אישי ובחירה בכינוי לא מזהה), היעדר היכרות טכנולוגית וניסיון אישי מחזקים את תחושת האנונימיות. גם גולש הער ליכולת החשיפה צריך להכיר את האפשרויות הטכנולוגיות לאנונימיות. היכרות כזו מחייבת רמת אוריינות טכנולוגית גבוהה למדי.

סקר נרחב שנערך באיחוד האירופי מאשש את ההנחות האלה.[233] הסקר מצא שאזרחים רבים מאוד (64%) מוטרדים מהגנת הפרטיות שלהם ובמיוחד באינטרנט (82%).[234] בה בעת, פחות ממחצית (42%) שמעו על קיומן של טכנולוגיות מקדמות פרטיות, ורק כמחצית מאלה (56%) השתמשו בטכנולוגיות כאלה.[235] הסיבות לאי־שימוש שנמנו היו ספקנות לגבי הטכנולוגיות (19%), חוסר ידיעה איך להשתמש (19%), חוסר ידיעה איך להתקין את הטכנולוגיה (17%) ושלל סיבות אחרות.[236] המחיר, אגב, היה גורם זניח יחסית (6%). עם זאת, יש ניצנים לשינוי: לפחות ב־15 מתוך 27 מדינות האיחוד נרשם גידול משמעותי במודעות לקיומן של טכנולוגיות מקדמות פרטיות בין השנים 2003 ל־2008.[237] הסקר עסק בטכנולוגיות מקדמות פרטיות בכלל ולאו דווקא בטכנולוגיות של אנונימיות, אולם אפשר לשער שהמגמות הכלליות דומות.

נראה שמפתחי TOR משקיעים מאמץ רב בהטמעת היישום שלהם, בהצגתו בצורה ידידותית למשתמשים ובשיפור חווית השימוש. מובן כי גולשים רבים אינם זקוקים לאנונימיות ביום־יום; בסופו של דבר לא כל עובד חושף שחיתויות מדי יום. עם זאת נראה כי מספר המשתמשים במערכת TOR גדל,[238] ולפי מפעילי היישום, מגוון השימושים רחב

---

232 ראו Peter Steiner, *On the Internet Nobody Knows You're a Dog*, 6 NEW YORKER 61 (5.7.1993), *available at* www.epatric.com/funstuff/dog.

233 ראו Flash Eurobarometer, *Data Protection in the European Union – Citizens' Perceptions*, Analytical Report (2008), *available at* ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

234 שם, בעמ' 21-22, 40.

235 שם, בעמ' 42.

236 שם, בעמ' 43.

237 שם, בעמ' 45.

238 לפי מחקר שפורסם בשנת 2008 נעשה שימוש במערכת TOR ביותר מ־120 מדינות, בראשן גרמניה, סין וארצות־הברית. נתבי TOR נמצאו בעיקר בגרמניה, בארצות־הברית, בצרפת ובהולנד. ראו Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno &

מאוד. המפעילים מדגישים שימושים דמוקרטיים כמו הגנה מפני הטרדות וגנבת זהות, פרטיות מפני גורמים מסחריים, הגנה על ילדים, פרטיות בקשר לחיפושי מידע, שימוש על ידי גורמי אכיפת החוק לצורך בילוש סמוי, שימוש על ידי עיתונאים במדינות שאין הן חופש עיתונות ועוד.[239]

כנגד טכנולוגיות של אנונימיות יש מי שעוסקים בטכנולוגיות של ציתות ומעקב, בין מטעמי ביטחון לאומי ואכיפת חוק ובין מטעמים פסולים.[240] זהו מעין מרוץ חימוש טכנולוגי. הגם שהוא אינו מספק הכרעה והגם שיש בו לעתים השקעה כפולה של משאבים, המרוץ עצמו ראוי. זו הדרך שבה התפתחו טכנולוגיות רבות מאז ומעולם, תוך דיאלוג פנים־טכנולוגי. זהו רעיון הקדמה (progress) שלפיו ההתקדמות האנושית באה נדבך על גבי נדבך, צעד אחרי צעד. תובנה זו מוכרת היטב בתחום של דיני הקניין הרוחני, המבוססים במידה רבה על רעיון הקדמה.[241]

3. תגובה משפטית?

האם הטכנולוגיות של האנונימיות ראויות וחוקיות? מצד אחד הן נועדו לסייע לגולשים לשמור את זהותם האנונימית שהיא, כפי שטענתי, זכות חוקתית שנגזרת הן מחופש הביטוי והן מהזכות לפרטיות. במובן זה הטכנולוגיה מקדמת את הפרטיות, ומאחר שהיא מסייעת לנו לקדם ערך חברתי ראוי היא ראויה גם כן. מצד שני, יש חשש שישתמשו בהן בדיוק אלה המבקשים לעשות שימוש לרעה באנונימיות. בצד זה, יש מצבים שבהם הגולשים דווקא יתעניינו בזיהוי – ויתרה מכך: יבקשו לוודא שהזיהוי שלהם אמין, כדי שיוכלו לקבל שירות כלשהו ואחרים לא יוכלו להתחזות להם ו"לגנוב" את זהותם.[242]

Douglas Sicker, *Shining Light in Dark Places: Understanding the TOR Network, in* PROCEEDINGS OF THE 8TH INTERNATIONAL SYMPOSIUM ON PRIVACY ENHANCING TECHNOLOGIES 63 (2008).

239 ראו אתר TOR, לעיל ה"ש 224.

240 ראו, למשל, הצעה לטכנולוגיה שמיועדת לאפשר האזנה לשיחות קוליות שמבוצעות ברשת (VoIP): Xinyuan Wang, Shiping Chen & Sushil Jajodia, *Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet, in* PROCEEDINGS OF THE 12TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 81 (2005).

241 ראו Michael D. Birnhack, *The Idea of Progress in Copyright Law*, 1 BUFF. IP L.J. 3 (2001). גם בדין הישראלי יש אמירות שיפוטיות מפורשות ברוח זו. ראו, למשל, ע"א 23/81 **הרשקו נ' אורבוך**, פ"ד מב(3) 749, 759 (1988).

242 לטענה כי ראוי להכיר בזכות לזהות אינפורמטיבית ראו אלעד אורג "זכות לזהות (מידע)" (צפוי להתפרסם בעיוני משפט לג, 2010). לדיון במתח שבין פרטיות לווידוא זהות

בצד השימושים הטובים והראויים אין לכחד כי הטכנולוגיות האלה מנוצלות לרעה ודווקא בידי חורשי הרעה והעבריינים המתוחכמים יותר. מי שמתכנן לפגוע בזדון באחר על ידי הכפשתו עשוי לאתר ולהשתמש בטכנולוגיות האמורות ואילו העובדת הזוטרה שמבקשת לחשוף שחיתות לא תדע להשתמש בהן. בעקבות המודל של לסיג, ראוי לבחון ארבעה גורמים מסדירים אפשריים: הטכנולוגיה (שנדונה בסעיף הקודם), השוק, נורמות חברתיות (שיידונו בסמוך) והמשפט (שידון בחלק הבא).[243]

בצד התגובה הטכנולוגית, ובכלל זה מאבק פנים־טכנולוגי, תגובה אפשרית אחרת היא להשאיר את המאבק לכוחות השוק.[244] הגם שעלותן של טכנולוגיות המעקב פוחתת, לגורם שמבקש חשיפה יש עלויות בחשיפה: בירור טכנולוגי, בירור משפטי, עלויות משפטיות לחשיפה וסיכון שהתהליך ייכשל. שימוש בטכנולוגיות של אנונימיות על ידי הגולש מייקר את עלות החשיפה. הכלכלנים יטענו כי אי־הוודאות בדבר המחיר תביא את הנפגעים להעריך את הנזק שנגרם להם מול תוחלת החשיפה – כלומר: הסיכוי שיצליחו בחשיפה – והעלויות. במקרים שבהם העלות גבוהה מתוחלת החשיפה יוותר המתלונן מראש על הבקשה. בדרך זו כוחות השוק מגנים על האנונימיות ללא צורך בהתערבות משפטית.

תגובה אפשרית אחרת היא להשאיר את המאבק לזירה הציבורית. אנו נמצאים בראשיתו של תהליך טבעי של גיבוש נורמות חברתיות בקשר לגלישה האנונימית באינטרנט. אלא, שגיבוש המותר והאסור אינו פועל בחלל ריק. הוא נגזר מהאפשרויות הטכנולוגיות (המידה שבה יש בפועל אנונימיות והמידה שבה אפשר לחשוף את זהות הגולשים), הוא נגזר מהתחשיב הכלכלי שמכתיב את האפשרי והאי־אפשרי והוא נגזר מהתנהגות השחקנים השונים. המדיניות של אתר **מחלקה ראשונה** להציג תגובות עם כתובות IP של הגולשים נתקלה בתגובה של אתר **רוטר.נט** – של מחיקה אוטומטית של כתובות IP של גולשים.[245]

(authentication) ולטענה שאותן טכנולוגיות שאוספות מידע ופוגעות לכאורה בפרטיות יכולות דווקא לסייע בהגנה על המשתמשים ראו Stefan Brands, *Secure User Identification Without Privacy Erosion*, 3 U. OTTAWA L. & TECH. J. 205 (2006).

243 ראו LESSIG, לעיל ה"ש 5.

244 לניתוח כלכלי של מערכות טכנולוגיות לאנונימיות ראו Acquisti, Dingledine & Syverson, לעיל ה"ש 219.

245 ראו דיווח באתר www.law.co.il: "בעקבות NFC: רוטר.נט מצהירים כי לא ישמרו פרטי גולשים" 4.2.2008 law.co.il/news/free-speech/2008/02/04/4097. בתקנון הפורומים של רוטר.נט נכתב כי ככל שהמידע נמצא בידי האתר, מנהלי האתר רשאים למסור אותו לרשויות לפי דרישה מכוח החוק. ראו rotter.name/nor/takanon.htm. מנכ"ל רוטר.נט, הרב ד"ר ישעיהו רוטר, עדכן כי האתר אכן אינו שומר את המידע: "קטגורית אנחנו מוחקים אי.פי. אלא אם המשטרה מבקשת מאיתנו לאור חשש לפלילים מוחשיים ובאמצעות צו בית משפט, לעקוב

את הצעד של **מחלקה ראשונה** ואת התגובה של **רוטר.נט** אפשר להבין כחלק מהמאבק הציבורי על גיבוש הנורמות החברתיות. מובן שהנורמות החברתיות מתגבשות גם אל נוכח הכללים המשפטיים: המותר והאסור המשפטיים מכתיבים את הציפיות של הגולשים.

תגובה אפשרית אחרונה היא זו המשפטית. האם המשפט צריך להגיב? כמו במקרים רבים אחרים של הסדרה משפטית של טכנולוגיות מידע, הקושי נעוץ בכך שהטכנולוגיה היא דו־שימושית.[246] אפשר לעשות בה שימושים חוקיים וטובים ולצדם אפשר להשתמש בה לרעה. הטכנולוגיה מגלמת ערכים חיוביים בצד ערכים שליליים. לפי שעה נראה שאין דרך טכנולוגית או משפטית לזהות מראש איזה שימוש ראוי ואיזה פסול. מובן שכל בדיקה מראש כזו משמעותה היא כי יש גורם שבודק את התוכן ונחשף למקור ההודעה, ולכן כל יתרונותיה החיוביים של הטכנולוגיה יורדים לטמיון.

כלל משפטי שיאסור את השימוש בטכנולוגיות כאלה יפגע בשימושים החיוביים שיש בה, יתערב באופן גס בפיתוח טכנולוגי (שהוא אינטרס ציבורי, וניתן לתרגום לשפת זכויות משפטית: חופש העיסוק, חופש הביטוי וזכות הקניין של מפתח הטכנולוגיה). בהינתן האופי הגלובלי של רשת האינטרנט, הסדרה היפותטית כזו צפויה להיתקל בקשיים רבים. כלל משפטי שלא יתערב בטכנולוגיות האלה לא ייכשל באלה, אבל גם לא יועיל באיתור המקרים שבהם ראוי ורצוי היה לחשוף את הגולשים האנונימיים. במישור זה, המילה האחרונה רחוקה מלהיאמר.[247]

אחר גולש כדי ללכוד אותו. למשל סוחר סמים או מוכר טובין גנובים שפרסם הודעה לצורך מעשיו הפליליים. מצב 'ברירת המחדל' הוא אי שמירת אי.פי ונכון שזה גם מקל מאד על עומס ותחזוקת השרת אבל בעיקר נובע מחופש הביטוי הניתן לגולשים. חופש ביטוי אינו 'פלילי מוחשי' כנ"ל. כל גולש יכול לכתוב באתר את כל מה שהוא חושב. אם דבריו גולשים לחוסר טעם ברמת הבסיס ולא מטיעונים השקפתיים. כגון קללות וניבולי פה, מנהלי הפורום מוחקים את דבריו, הם גם נוגדים את התקנון" (דואר אלקטרוני מהרב רוטר, מנכ"ל רוטר.נט, למחבר, 11.3.2009).

246 בעיה זו אינה ייחודית לנושא הפרטיות. גם בהקשרים אחרים מתעוררת בעיה דומה. למשל, לתוכנות לשיתוף קבצים יש שימוש פסול נפוץ של העתקת יצירות מוזיקליות וקולנועיות תוך הפרה של זכויות יוצרים. לצד פעולות אלה להן יש גם שימושים ראויים של העברת קבצים שאינם מוגנים בזכויות, קבצים המועברים ברשות בעליהם כאמצעי הפצה ושיווק או קבצים שהשימוש בהם הוא הוגן לפי דיני זכויות יוצרים, שאחד ממרכיביה בוחן אם יש לגורם המפר ולפעילותו (ובמקרה זה לטכנולוגיה לשיתוף קבצים) שימושים מהותיים שאינם מפרים (substantial non-infringing uses). לדיון ראו, למשל, עניין *Napster*, לעיל ה"ש 155.

247 מחבר אמריקני מציע כי בהיעדר ידיעה בדבר השימוש במערכת יש להניח כי המסר זכאי להגנה מרבית. ראו Joshua A. Altman, *A Schrödinger's Onion Approach to the Problem of Secure Internet Communications*, 7 WASH. U. GLOBAL STUD. L. REV. 103 (2008).

בינתיים, פיתוח טכנולוגיות של אנונימיות קשור גם לכלל המשפטי המתגבש בנוגע לחשיפת גולשים. ככל שהמשפט יתערב יותר ויורה ביתר קלות על חשיפה, יגדל התמריץ לפתח ולהשתמש בטכנולוגיות של אנונימיות לשם עקיפת הכלל המשפטי. ככל שהמשפט יתערב פחות בחשיפת זהות יקטן התמריץ לשימוש טכנולוגי. בדרך זו יש דיאלוג בין המשפט לבין הטכנולוגיה. הטכנולוגיה מאפשרת פעילות רצויה (גלישה באינטרנט, בכלל זה באנונימיות) ובו־זמנית היא מאפשרת פעילות שאינה רצויה (ניצול לרעה של האנונימיות בדרך שפוגעת בצדדים שלישיים). המשפט, בין בחקיקה ובין בפסיקה, מנסה לגבש כללים להתמודדות עם הקשיים המתעוררים. הטכנולוגיה כבר מגיבה ותגובתה תלויה בכלל המשפטי. לפיכך, כל כלל משפטי בסוגיה היסודית צריך לבוא מתוך צניעות בכוחו של המשפט ומתוך הבנה שהמשפט אינו אדון לטכנולוגיה אלא גורם מסדיר בצדה. המשפט והטכנולוגיה יכולים לסייע זה לזה אבל יכולים גם להיאבק זה בזה. קשה להעריך כוחו של מי יגבר במקרה של התנגשות כזו.

ו. מתווה משפטי לחשיפת זהות

מיפוי השדה שבו השחקנים השונים פועלים וזיהוי הזכויות והאינטרסים שלהם אִפשר לנו לזהות את הכוחות המעורבים. מיקום הדיון במסגרת של משפט וטכנולוגיה אפשר לנו לעמוד על מגבלות הכוח של המשפט. הדיון זיהה קשיים שעמם יש להתמודד: ראשית, ככל שמדובר בתביעת־אמת, ראוי לסייע למי ששמו הטוב או זכות מהותית אחרת שלו נפגעו אולם ההליך החד־צדדי מקשה על בירור הבקשה. שנית, ספקי השירות עלולים להימצא במלכוד משפטי ומסחרי ולכן קושי מרכזי הוא ייצוג הגולש האנונימי. קושי שלישי הוא טכנולוגי: לעתים יש קושי להגיע לפוגע ואחת הסיבות היא שספק השירות מחק את המידע; לכן יש מקום להליך מהיר. קושי רביעי הוא החשש שהליך החשיפה ינוצל לרעה בדרך שלא נועדה לשרת את הזכויות המהותיות שנפגעו אלא כדי לספק אינטרסים פחותים בחשיבותם ואולי אף פסולים, שיפגעו באנונימיות של הגולשים. שיקול מרכזי שלא נשקל דיו הוא ההשלכה של החשיפה על גולשים אחרים: לחשיפה יש אפקט מצנן שעלול להרתיע גולשים אחרים מביטוי פוטנציאלי רצוי.

ההסדר המשפטי הקונקרטי צריך להביא בחשבון את כל אלה. חלק זה מציע מתווה משפטי לחשיפת זהות. לאור פסק הדין בעניין מור, המתווה מכוון כעת למחוקק. נקודת המוצא היא שיש מקום לאפשר את חשיפת הזהות במקרים מתאימים. אינני טוען שיש צורך באנונימיות מוחלטת בכל מצב; ודאי אינני טוען שיש לחשוף את הגולשים האנונימיים בכל מקרה. הדיון מעלה שיש מקום לקביעת מסגרת שיקולים כללית – אבל עדיין להותיר יישום אד־הוקי, למרות מחיר אי־הוודאות הכרוך בכך. המתווה המוצע הוא דו־שלבי: תחילה

מוצע מנגנון קדם־שיפוטי במתכונת של הסדרה פרטית בצל המשפט; בהמשך מוצע מתווה לתוכנו של הכלל המשפטי הראוי בבית המשפט.

1. ספקי השירות כמתווכים

אני סבור שתשובה אפשרית לרוב הקשיים האלה היא הליך מקדמי, שייערך בחסות המשפט אך לא בבית המשפט. ההשראה להליך המוצע היא הערות האגב של בתי המשפט באנגליה וההסדר שהוצע בהצעת חוק מסחר אלקטרוני בהקשר אחר, של חסינות ספקי שירות, ונורמות שקיימות בפועל אצל כמה ספקי שירות במדינות אחרות. בהליך מקדמי זה, ספק השירות (שירות אירוח או שירות גישה) ישמש מתווך בין הנפגע לגולש האנונימי.[248] תמצית ההליך המוצע היא: הודעה, הודעה נגדית ולפי הצורך – הפניה לבית משפט. את ההליך אפשר לעגן בחקיקה ולחלופין בהסדרה פרטית, כלומר: באימוץ מדיניות מעין זו של ספקי השירות.[249] בכל מקרה ההצעה נוספת על איסור שחל על הספק למסור מידע מרצונו החופשי ובכך תעוגן הזכות לאנונימיות.

הודעה

תחילת ההליך היא בתלונה. לשם כך על הספק (הן ספק של שירות אירוח והן ספק של שירות גישה) ליצור תשתית לקבלת הודעות. אם הספק מקיים מנגנון טיפול בהודעות כדי לזכות בחסינות מפני תביעות בכלל, אין עלויות נוספות מיוחדות בהקמת מנגנון כזה. אפשר לדרוש שההודעה תלווה בתצהיר, בהתחייבות לשיפוי של ספק השירות במקרה שייתבע בגין פעולותיו בנושא וכן החזר הוצאות הכרוכות בטיפול בבקשה. את שיעור ההוצאות אפשר לקבוע בתקנות כדי שלא ישמשו משוכה מלאכותית להכשיל בקשות־אמת.

הודעה נגדית

עם קבלת תלונה מהנפגעת ינסה ספק השירות ליצור קשר עם הגולש. כאשר הוא מחזיק בכתובת הדוא"ל או בפרטים מזהים אחרים של הגולש אין בכך קושי רב. כאשר מדובר

---

248 בדומה הצביע אלעד אורג על שורה של מתווכים פוטנציאליים ובין היתר ספק השירות, עורך־הדין של הגולש או בית המשפט. ראו אלעד אורג **אנונימיות משפט ואינטרנט – על חשיבה משפטית בנוגע לפעילות אנונימית באינטרנט ובכלל** 111 (עבודה מסכמת לצורך קבלת תואר מוסמך במשפטים, אוניברסיטת תל־אביב – הפקולטה למשפטים, 2002).

249 ראו, למשל, את המדיניות המוצעת על ידי כמה ארגונים לזכויות אדם, המופנית לספקי שירות: www.cyberslapp.org/about/page.cfm?pageid=6.

בספק של שירותי אירוח שבידיו רק כתובת IP, יוכל להעביר את הטיפול והתיווך לידי הספק של שירות הגישה. אם המידע אינו בידיהם של ספקי השירות – יוכלו להשיב כך למתלוננת ויחסכו ממנה הליכים משפטיים יקרים ומיותרים;[250] אם יתברר שהגולש אינו נמצא בישראל, יוכלו ליידע על כך את המתלוננת והיא תוכל לכלכל את המשך צעדיה המשפטיים. דרך נוספת ליידוע הגולש היא הודעה בפורום המקוון שבו בוצעה העוולה לכאורה, ככל שהדבר רלוונטי. מובן שהודעה פומבית כזו עשויה להיות לא רלוונטית ולכן יש מקום לשיקול דעת לפי נסיבות המקרה.

בירור ביניים

כאשר הבירור עד כה יַפנה לספק גלישה – בית קפה, ספרייה, תאגיד וכדומה – ככל שאינם ספקי גישה לאינטרנט בעצמם, יוכלו אלה לברר אם בכלל יש בידיהם דרך לאתר את הגולש הספציפי. אם אין – יידעו את המתלוננת ובכך תם אפיק החשיפה; אם הנתונים בידיהם, יתגלגל אליהם תפקיד התיווך והם יידעו את הגולש בדבר התלונה.

הפנייה לבית משפט

אם יאותר הגולש, הברירה בידיו להיחשף ולהתמודד עם הנפגעת במישרין או לסרב לחשיפה. במקרה הראשון תמה פרשת החשיפה והסכסוך יעבור לפסים רגילים של סכסוך משפטי בין הצדדים; במקרה השני יש לאפשר לגולש להעביר הודעה מטעמו – תוך שמירה על חשאיות זהותו, בין באמצעות נציג (עורך־דין) ובין באמצעות ספק השירות – אל הנפגעת המתלוננת. לאחר שירות תיווך אחד כזה ראוי שספק השירות ייצא מן התמונה וישאיר את הצדדים לכלכל את צעדיהם. לאור תגובת הגולש תוכל המבקשת לשקול שנית את בקשתה. יש להניח שבמקרים מסוימים, לאור מידע שיתקבל בהליך כזה או לאור טענות שיועלו לפניו תחליט המתלוננת לא להמשיך את ההליך. במקרים אחרים תוכל לפנות לבית המשפט.

ההליך המוצע זול מפנייה לבית המשפט. אם לא נשמר המידע או שהגולש האנונימי אינו נגיש בישראל, ההליך המוצע יאפשר את סיום הטיפול במהירות. ההליך מוציא את ספק השירות מן המלכוד הכפול שבו הוא נתון ויש בו ערובות פרוצדורליות שיבטיחו שהספק

---

250 למגבלות הכוח של המשפט מול הטכנולוגיה בהקשר זה ראו מיכל אגמון־גונן "האינטרנט כעיר מקלט?! הסדרה משפטית לאור אפשרויות העקיפה הטכנולוגיות וגלובליות" **משפט וטכנולוגית מידע**, לעיל ה"ש 31.

עצמו לא ייפגע מהתהליך וגם לא יחבל בו. בדרך זו יש סיוע לנפגעת לממש את זכותה המהותית שנפגעה במהירות גבוהה יותר ויש פתרון לבעיית הייצוג של הגולש האנונימי.

2. בית המשפט כמתווך

במקרה שההליך המקדמי על שלביו לא יועיל תוכל המבקשת לפנות לבית המשפט בבקשת חשיפה. הפעם יוכל בית המשפט לשמש מתווך בין הצדדים כך שספקי השירות יעבירו לבית המשפט את פרטי הגולש, ככל שאלה בידיהם, ויוכלו לצאת מן התמונה. בקשת החשיפה תועבר לידי הגולש. בדרך זו האנונימיות הכמעט־מלאה נהפכת לאנונימיות יחסית. רעיון התיווך השיפוטי אינו זר לדיון בישראל. הוא הוצע על ידי השופט עמית בשבתו בבית המשפט המחוזי בעניין **מור**, על ידי השופט אטדגי בעניין **וואלה נ' קולקר**,[251] ואפילו בבית המשפט העליון, בדעת המיעוט בעניין מור, אם כי שם הוצע לקבוע אפשרות כזו רק במקרים חריגים.[252] כך גם נהג בית המשפט המחוזי בתל־אביב בבקשה לחשיפת גולש אנונימי בתביעת בגין זכות יוצרים.[253] בדרך זו יזכה בית המשפט לשמוע גרסה אחרת לגרסת המבקש, שתוכל לסייע להעריך את השאלות המהותיות הראשוניות (האם מדובר בתביעת אמת תמת־לב? האם לפי דיני לשון הרע עצמם סיכויי התביעה גבוהים?) ואף לשמוע את עמדת הגולש בקשר לחשיפת זהותו.

בדיון בבקשת החשיפה לגופה על בית המשפט לשקול שיקולים שונים, בין ששני הצדדים מיוצגים בדרך כלשהי ובין שרק המבקש מיוצג. בתמצית, על בית המשפט לוודא שאין שימוש לרעה בהליך, שסיכויי התביעה גבוהים, שאין אמצעים חלופיים לפתרון הסכסוך בלעדי החשיפה ושהתועלת בחשיפה עבור הנפגע גבוהה מנזקיה לגולש האנונימי ולציבור בכלל, כשאת הנזק יש להבין כנזק חוקתי (ואת נזקו של התובע – לפי הדין המהותי הרלוונטי).

אי־ניצול לרעה

תחילה ראוי לוודא כי אין ניסיון להשתמש בהליך לרעה. יש להביא בחשבון את מכלול האינטרסים והזכויות שעל הפרק ובכלל זה את האינטרסים הציבוריים בקיומה של זירת שיח

---

251 ראו עניין **מור** מחוזי, לעיל ה"ש 7; ה"פ (שלום ת"א) 200357/07 **וואלה תקשורת בע"מ נ' קולקר** (פורסם בנבו, 9.9.2007, השופט יונה אטדגי).

252 עניין **מור**, לעיל ה"ש 2, בפסקאות סז-סט, לפסק דינו של השופט רובינשטיין.

253 עניין **The Football Association Premier League**, לעיל ה"ש 119. הנתבע שם שמר על אנונימיות, אולם יוצג על ידי עורך־דין.

אפקטיבית ודמוקרטית. חשוב לזכור כי למשפט אין ולא צריכה להיות העדפה לשיח איכותי, נקי ואליטיסטי על פני שיח עממי וצעקני יותר. אם הגולש אינו מיוצג יש להיזהר שלא למהר להורות על חשיפת זהותו רק משום שהצדדים לבקשת החשיפה – הנפגעת וספק השירות – מסכימים לחשיפת הזהות של הצד השלישי. הפתרון המשפטי הראוי צריך להתייחס בכובד ראש לזכויות של הגולש האנונימי, שהן זכויות חוקתיות של חופש ביטוי ופרטיות.

זהו שלב של הפרדת המוץ מן התבן. התבן, במקרה הזה, הוא שיקולים לא ענייניים שמוסווים בכסות לגיטימית של זכות מהותית שנפגעה. הנפגעת מַפנה לזכותה המהותית שנפגעה: שמה הטוב, פרטיותה, אינטרס קנייני מוגן שלה וכדומה; אולם יש מי מבין הנפגעים שמבקשים לנצל זאת כדי לדעת מי כתב את שכתב עליהם בלא שיש להם כוונת אמת לתבוע את הגולש. במקרים רבים עומדים לרשות המבקש אמצעים אחרים לפגוע במגיב ולהתנכל לו. כך, למשל, כשתגוביות מבקרות את התנהלותו של תאגיד ואת צורת הניהול של העומדים בראשו, מתבקש להניח כי התגובית נכתבה על ידי עובד בעל בטן מלאה או שהוא חושף שחיתויות, במיוחד כשמדובר בגוף ציבורי.[254] על סמך הפרטים המצוינים בתגובית גם המעסיק יכול לשער כי מדובר באחד מעובדיו. קשה לשער שהמעסיק יתבע את העובד, אבל קל יותר להניח שהמעסיק יבקש לפטר את העובד או להתנכל לו בדרך אחרת. כך ביחסי מרות בכלל; למשל: תגוביות על איכות ההוראה של מורים. לעתים בקשת החשיפה נועדה להעביר מסר ברור ובוטה למבקריו של המבקש, מסר שתוכנו "לא כדאי להתעסק איתי". בארצות־הברית ידועה תופעה של תביעות שנועדו להשתיק ביקורת (SLAPP; Strategic Litigation Against Public Participation). בכמה מדינות נחקקו חוקים שנועדו לסכל תביעות אסטרטגיות כאלה.[255] החשש הוא מהתנהגות אסטרטגית דומה גם בזירה המקוונת.[256]

המשפט צריך לחסום את אלה שמבקשים להשתמש בהליך החשיפה למטרות שאינן תביעה תמת־לב. ראשית, מי שאינו מבקש לתבוע מגלה בכך את דעתו שהפגיעה בזכותו המהותית – לשמו הטוב, למשל – לא הייתה משמעותית, אם בכלל; שנית, בהיעדר עילת

---

254 למקרה שבו הניח בית המשפט כי תגובית אנונימית שביקרה מעסיק נכתבה על ידי עובד ראו עניין **מכון התקנים**, לעיל ה"ש 80.

255 ראו, למשל, בקליפורניה California Code of Civil Procedure, sec. 425.16.

256 לדיון ראו Spencer, לעיל ה"ש 184. המחבר מביא דוגמאות למקרים שבהם לאחר שנחשפה זהות הגולשים לא נקטו המבקשים את החשיפה כל תביעה כנגדם אך התנכלו להם בדרכים אחרות. שם, בעמ' 495, 498. ראו עוד Lidsky, לעיל ה"ש 184, הדנה בתביעות של תאגידים נגד גולשים אנונימיים במטרה להשתיק ביקורת.

תביעה מהותית, גם הזכות הנספחת של גישה לערכאות אינה מתקיימת; שלישית, בקשות חשיפה שאינן מיועדות להגיע לתביעה חותרות תחת כל המטרות הרצויות שעליהן מגנה האנונימיות. לא בכדי גולש בוחר להגיב באופן אנונימי: כך הוא יכול לבקר ללא מורא, ללא חשש שיתנכלו לו, כך הוא יכול לחצות את הגבול החברתי של הקהילה אליה הוא משתייך (למשל אדם חרדי שמבקש להתבטא בשונה מהמקובל בסביבתו). בדיוק מפני מתנכלים למיניהם יש לגולש זכות לחופש ביטוי וזכות לפרטיות, שמהן נגזרת האנונימיות.

הקושי הוא כמובן להבחין בין בקשת אמת לבקשת סרק. פתרון אפשרי יכול להיות ראייתי ודיוני. ראייתי – בכך שהמבקש יצטרך להציג את מרב הראיות שבידו, כדי שאולי אפשר יהיה לעמוד על כוונותיו. אפשר להוסיף דרישה מפורשת לתום לב. פתרון דיוני יכול להיות ערבות שתופקד בבית המשפט. אם בסופו של דבר לא תוגש תביעה והגולש האנונימי יבקש פיצוי בגין חשיפת הסרק, הוא יוכל להיפרע את נזקיו במהירות.[257] דרישת ערבות תביא את המבקש להעריך ביתר תשומת לב את נזקו שנגרם כבר אל מול הנזק שעלול להיגרם לאחר. אמצעי דיוני נוסף הוא דרישה שהבקשה לחשיפת הזהות תוגש בד בבד עם הגשת תביעה עיקרית. פתרון זה מחייב הסדרה של תביעות נגד נתבעים אנונימיים – "רן דן", בלשונו של בית המשפט העליון. תחילה תופנה התביעה כנגד רן דן, ואם תתברר זהותו – תתוקן התביעה. לחלופין אפשר להסתפק בטיוטת התביעה, שתוגש עם הבקשה לחשיפה. בצורה כזו תיפרש לפני בית המשפט תמונה רחבה מעט יותר ויש בכך אינדיקציה לרצינות התובע. ייתכן, כמובן, שלאחר שתתברר זהות הגולש האנונימי יופתע המבקש ויחליט שלא לתבוע, למשל אם יתברר שהגולש הוא חבר (לשעבר) או קרוב משפחה.

סיכויי התביעה

שיקול מרכזי שני הוא סיכויי התביעה. כאשר בית המשפט סבור שמדובר בתביעת סרק או בכזו שסיכוייה נמוכים, יוכל לדחות את הבקשה כבר בשלב מוקדם, כפי שעשו כמה בתי משפט.[258]

הבדיקה צריכה להיעשות על רקע הכללים המהותיים שיש בענף המשפטי שלפיו מתבקשת הבקשה. כך, למשל, אם דיני לשון הרע מקנים הגנה פחותה לנבחר ציבור לעומת אדם שאינו נבחר, יש להביא זאת בחשבון גם בבקשת החשיפה. בתי משפט מורגלים

257 כך, למשל, נהג בית משפט השלום בעניין **פריד**, לעיל ה"ש 80.

258 ראו, למשל, עניין **עירית אריאל**, לעיל ה"ש 67, או עניין **סבו**, לעיל ה"ש 78; עניין **כהן**, לעיל ה"ש 84.

בהערכה כזו בשלבים של בקשות לצווי מניעה זמניים, למשל בתביעות של הפרת קניין רוחני; ההבדל המשמעותי הוא ששם הדיון מתקיים במעמד שני הצדדים ובכל מקרה צו המניעה הפיך וערבות יכולה לתקן את הנזק שגורם הצו, אם ניתן כזה ואם נגרם נזק. לעומת זאת, ההליך שבו מדובר הוא במעמד צד אחד בלבד ואינו הפיך. מרגע שנחשפה זהות הגולש אי־אפשר להשיב את הגלגל לאחור. לכן בית המשפט צריך לראות את מרב הראיות האפשריות ולהביא בחשבון את הכללים המגובשים שפותחו בדיני לשון הרע. כך, למשל, בדומה לדרך שנקט בית המשפט המחוזי בעניין **סבו**, יש לבחון אם המבקש הוא איש ציבור ואם ההקשר שבו הביטוי הפוגעני לכאורה נאמר אינו מסביר את הדברים ומוציא את עוקצם. ביטוי שנאמר במסגרת מערכת בחירות, מבחינת מושא הדברים ותוכנם, למשל, הוא ביטוי פוליטי מובהק.[259] גם אם אין בכך הצדקה לפגיעה בשמו הטוב של אדם, הקשר הדברים מחזק את הסיכוי שבתביעה גופה ימצא בית המשפט שהתקיימה הגנה מספקת לפי החוק. כך גם לגבי הגנות אפשריות אחרות הקבועות בדין. על בית המשפט להעריך אם תיתכן הגנה שמתבססת על מידע שנמצא רק בידי הגולש האנונימי.

בתי המשפט בארצות־הברית, באנגליה ובקנדה התחבטו ברף הנדרש בין דרישה שהתביעה תצלח בשלום בקשה למחיקה על הסף – בקשה שמתקבלת רק לעתים רחוקות, ולכן מדובר ברף נמוך יחסית – לבין רף גבוה של סיכויי זכייה גבוהים. אני סבור שהרף הגבוה יותר הוא המתאים. הוא מגלם את הזהירות הנדרשת בשל ההחצנות השליליות האפשריות שיש לחשיפה על הגולשים האנונימיים ועל הציבור בכלל.

איזון

המתווה המוצע כולו מגלם את האיזון החוקתי הכללי. כעת אנו מגיעים לאיזון הקונקרטי. לאחר כל הבדיקות המקדמיות שתוארו יש לאזן את מידת הפגיעה האמיתית שנפגע המבקש אל מול הזכויות של הגולש, תוך תשומת לב להשלכה הרחבה יותר של ההכרעה. גם כשנחה דעתו של בית המשפט שהבקשה היא בקשת אמת תמת־לב שנועדה לממש זכות מהותית שנפגעה, ושסיכוייה טובים, יש להיזהר בחשיפת הגולשים – שוב, מחמת שצעד זה אינו הפיך, מחמת שיש בו פגיעה קשה בזכויות הגולש ומחמת שיש לחשיפה השלכה על הצורה שבה אנחנו גולשים ברשת ומקיימים את זירת הביטוי הציבורית שלנו.

---

259 בולט במיוחד מספרם של המקרים בהקשר הפוליטי המקומי. ראו עניין **סבו**, לעיל ה״ש 78; עניין **ברלומנפלד**, לעיל ה״ש 75; עניין **עירית אריאל**, לעיל ה״ש 67; עניין **ערב ערב באילת**, לעיל ה״ש 80 וכן עניין **דואק**, לעיל ה״ש 54.

החלת מבחן של מידתיות יכולה לסייע כאן. המידתיות היא כיום הכלי המרכזי במשפט הישראלי שפורט את האיזון האנכי – כלומר: האיזון בין זכויות לאינטרסים מתנגשים – לבדיקה קונקרטית. ברוח מבחן "המידתיות הצרה", יש לבחון את התועלת שבחשיפת זהותו של הגולש האנונימי עבור המבקש אל מול המחיר שישלם הגולש האנונימי והציבור כולו. ההכרעה כאן היא במידה רבה ערכית ונוסחאות איזון כאילו־מדעיות ואובייקטיביות אינן יכולות לטשטש זאת. חשוב שבית המשפט יזכור את האינטרס הציבורי: אצבע שיפוטית קלה על חשיפת הזהות משדרת מסר ברור ומצנן לגולשים אנונימיים אחרים. משום כך אני סבור שיש לקבוע רף גבוה לחשיפה. רף גבוה יכול להיתרגם למבחן של עניין **בזק בינלאומי**, שנעזר ברף הפלילי, ויכול להתבטא בדרישה שבית המשפט ישתכנע שסיכויי התביעה להתקבל גבוהים מאוד ושהנזק שנגרם למבקש הוא נזק משמעותי.

בקביעת רף גבוה יש בחירה ערכית שמעדיפה במקרים רבים את האינטרס הציבורי הכללי ואת האנונימיות של הגולשים על פני נזקו של המבקש. המשמעות היא שלעתים ייצא הנפגע כמעט בלא כלום: את ספק השירות יתקשה לתבוע ואת הגולש האנונימי לא יוכל לתבוע. זהו מחיר כבד ויש בו אי־נוחות מכך שהנפגע משלם את מחיר הכלל. את נזקו של הנפגע אפשר למזער גם בלי פיצוי: הסרת החומר הפוגעני או הודעה מתקנת מטעמו או מטעם הספק.

ז. סיכום

כמה מסקנות כלליות עולות מהדיון. הראשונה היא שיש להיזהר מפני המשגה מהירה מדי של סכסוכים במסגרת המוכנה שמציעה לנו שפת האיזונים. המשגה כזו עלול לאבד את המורכבות של הזכויות שעל הפרק ולהחמיץ שחקנים נוספים בזירה. במיוחד הצביע הדיון על ספקי השירות באינטרנט, שהאינטרסים שלהם, מעמדם המשפטי והיקף חבותם לתכנים פוגעניים שחיברו צדדים שלישיים – הגולשים האנונימיים – הם גורם מרכזי בסוגיה.

מסקנה שנייה דנה בשאלה של עיצוב מדיניות בסביבה טכנולוגית. זו המחשה נוספת ליחסים המורכבים שבין המשפט לבין הטכנולוגיה בכלל ובקשר לדיון פה, זו המחשה לתלות של הזכות לפרטיות ושל חופש הביטוי בטכנולוגיה. הצעתי, כי את הכלל המשפטי יש לעצב תוך הבנת הדינמיות של הסביבה הדיגיטלית, המכירה בכך שהמשפט והטכנולוגיה נמצאים בדיאלוג נמשך.

מסקנה שלישית, ספציפית, היא הדרך לעיצוב הכלל המשפטי – מלאכה שצריכה להיעשות בזהירות ובדרך מחושבת. יש לנסות להתאים את הכלל המשפטי ולכיילו כך שפגיעתו בגולשים האנונימיים ובציבור בכלל תהיה מזערית. לשם כך הצעתי ליצור הסדרה פרטית, שבה ספק השירות ישמש מתווך בין הצדדים, תוך שמירה על אנונימיות הגולשים.

רק בהמשך, לפי הצורך, ידון בית המשפט בסוגיה – וגם אז הצעתי לנקוט תחילה הליך של תיווך על־ידי בית המשפט. אם כל זה לא יועיל יש לנקוט אמצעים לסינון בקשות חשיפה הנובעות מטעמים זרים, שאינם מבקשים להביא לכדי אכיפה של זכויות מהותיות. אמצעים דיוניים וראייתיים יכולים לסייע בכך. לאחר מכן יש להעריך את סיכוייה של התביעה העיקרית ולשם כך – לבחון מקרוב דוקטרינות מהותיות של הדין הרלוונטי. אם תשרוד בקשת החשיפה את המשוכות האלה, יש לבחון את הסוגיה במשקפיים של מבחן המידתיות, על שלושת מרכיביו; בין היתר יש לנסות ולאתר אמצעים שפגיעתם פחותה (התיווך של בית המשפט הוא אמצעי לכך). בסופו של דבר, אם כל אלו אינם מועילים, יש לאזן בין היתרון שיזכה בו המבקש אל מול הנזק שייגרם לגולש האנונימי ולציבור כולו.

לאחר עניין מור, גורל האנונימיות בעת הגלישה באינטרנט צפוי לשוב לשולחן הדיונים בכנסת. בצד המשפט, הטכנולוגיה אינה שוקטת על שמריה. טכנולוגיות חדשות מציעות לגולשים אמצעי אנונימיזציה. ככל שהכלל המשפטי יקל על חשיפת גולשים יש להניח שיגבר השימוש באפיקי הגנה טכנולוגיים. בצד המשפט והטכנולוגיה, גם ספקי השירות והגולשים מגיבים לאפשרויות הטכנולוגיות והמשפטיות, בין בטשטוש זהות מתוחכם יותר ובין בקבלת כללי המשחק החדשים והפנמתם.