



הכנסת
הלשכה המשפטית
תחום חקיקה ומחקר משפטי

חשיפת זהותו של מעוול אנונימי ברשת האינטרנט

– רקע תיאורטי וסקירה משווה –

כ' באב התשע"ה

5 באוגוסט 2015

עדכון: 13 ביוני 2018

כתיבה: ד"ר ירון אונגר, עו"ד

אישור: עו"ד הודיה קין, ממונה בכירה (חקיקה ומחקר משפטי)

מסמך זה הוא סקירה משפטית משווה ואינו חוות דעת

תוכן העניינים

2	תמצית	תמצית
6	1. הקדמה מושגית	1. הקדמה מושגית
7	2. תמורות במשקלם של ערכים בעידן המידע	2. תמורות במשקלם של ערכים בעידן המידע
7	2.1 מן "המערב הפרוע" לדין האינטרנט	2.1 מן "המערב הפרוע" לדין האינטרנט
8	2.2 חופש הביטוי ברשת	2.2 חופש הביטוי ברשת
9	2.3 אנונימיות	2.3 אנונימיות
10	2.4 הזכות לפרטיות בעידן המידע	2.4 הזכות לפרטיות בעידן המידע
11	3. מודלים מוסדיים	3. מודלים מוסדיים
12	3.1 חקיקה שיפוטית	3.1 חקיקה שיפוטית
13	3.2 חקיקה	3.2 חקיקה
14	3.3 הסדרה עצמית	3.3 הסדרה עצמית
17	4. רקע נורמטיבי	4. רקע נורמטיבי
17	4.1 חקיקה	4.1 חקיקה
19	4.2 פסיקות בתי המשפט	4.2 פסיקות בתי המשפט
20	5. סקירה משווה	5. סקירה משווה
20	5.1 משפט בינלאומי	5.1 משפט בינלאומי
24	5.2 ארה"ב	5.2 ארה"ב
29	5.3 בריטניה	5.3 בריטניה
31	5.4 קנדה	5.4 קנדה
35	5.5 הונג קונג	5.5 הונג קונג
36	5.6 גרמניה	5.6 גרמניה
37	5.7 שבדיה	5.7 שבדיה
37	6. משפט עברי	6. משפט עברי
37	6.1 חופש הביטוי	6.1 חופש הביטוי
38	6.2 הזכות לפרטיות וחובת הסודיות	6.2 הזכות לפרטיות וחובת הסודיות
39	6.3 אנונימיות ולשון הרע	6.3 אנונימיות ולשון הרע
40	6.4 חשיפת זהות המעוול	6.4 חשיפת זהות המעוול
40	7. סוגיות נוספות לדיון	7. סוגיות נוספות לדיון
41	7.1 חשיפת זהות בידי ספקי גישה למחשבים, מנהלי אתרים ואחרים	7.1 חשיפת זהות בידי ספקי גישה למחשבים, מנהלי אתרים ואחרים
41	7.2 עילות החשיפה	7.2 עילות החשיפה
42	7.3 שמירת מידע ותוכנות המספקות אנונימיזציה	7.3 שמירת מידע ותוכנות המספקות אנונימיזציה
42	7.4 סוג המידע שייחשף	7.4 סוג המידע שייחשף
43	7.5 חובת סודיות, פרטיות וחיסיון	7.5 חובת סודיות, פרטיות וחיסיון
43	7.6 השימוש במידע שנחשף	7.6 השימוש במידע שנחשף
43	7.7 חשיפה ביוזמת ספקי השירות	7.7 חשיפה ביוזמת ספקי השירות
44	7.8 שיהוי והתיישנות	7.8 שיהוי והתיישנות



תמצית

מסמך זה נכתב לבקשתה של עוה"ד נירה לאמעאי, היועצת המשפטית של ועדת המדע והטכנולוגיה, כרקע לדיון מקיף בהצעות חוק שעלו לאחרונה על סדר יומה של הוועדה, שעניינן הסדרת ההליכים לחשיפת פרטי מעוול אנונימי ברשת האינטרנט.

רשת האינטרנט מאפשרת לכל אדם להביע את עצמו, להגיב לדברי אחרים ולפרסם כל שתוכן שירצה בו, בעילום שם. יש המנצלים מצב זה על מנת לפגוע באחרים באמצעות הפצת דיבה, הטרדה, פגיעה בזכויות קניין רוחני וכדומה, מבלי להיות חשופים לתביעה אזרחית, שקיומה מותנה בהכרת זהותו של הפוגע - המעוול.

לעיתים ניתן לחשוף את זהותו של המעוול, באמצעות התחקות אחר המחשב שדרכו הופץ המידע ואיתור זהותו של בעל המחשב, דרך שימוש בפרטים מזהים שמסר המשתמש לחברה המספקת לו שירותי גישה לאינטרנט.

עד לפני כשנתיים, דנו בתי המשפט בישראל בבקשות להורות לספקי שירותי הגישה לאינטרנט לחשוף את זהותו של משתמש מעוול כדבר שבשגרה. לפני כשנה פורסם פסק דינו של בית המשפט העליון בפרשת מור,¹ שקבע למעשה שבהעדר הסדר דיוני הקבוע בחוק לחשיפת זהותו של מעוול ברשת האינטרנט, אין בתי המשפט בישראל מוסמכים להורות לספקי שירותי הגישה לחשוף את זהותו של מעוול.

בעקבות פסיקה זו, נעשו במהלך השנתיים האחרונות ניסיונות חקיקתיים שונים, שיתוארו במסמך זה, לעגן בחוק את סמכות בתי המשפט להורות על חשיפת זהותו של מעוול ברשת האינטרנט.

במסמך זה מוצג הרקע הטכנולוגי, העיוני והנורמטיבי בנושא זה, האופן שבו בחרו מדינות שונות בעולם להתמודד עם הסוגיה ועמדת המשפט העברי בנושא. בסיומו של המסמך יוצגו 'על קצה המזלג' סוגיות שונות הכרוכות בהצעת החוק שעלו אגב בחינת המצב בעולם והשיח האקדמי בנושא, אשר יש לתת עליהן את הדעת בדיון בהצעות החוק שעל הפרק.

מן המסמך עולים הממצאים העיקריים הבאים:

- חשיפת זהותו של מעוול אנונימי מבוצעת באמצעות זיהוי ספק שירותי הגישה לאינטרנט של המשתמש, דרך חשיפת ה"כתובת" של המחשב (IP) שנשלחה אל האתר שבאמצעותו בוצעה העוולה וחשיפת זהותו של בעל ה"כתובת" בידי ספק שירותי הגישה.
- הזיהוי מותנה בשמירת פרטיו המזהים של הגולש בידי ספקי שירותי הגישה לאינטרנט.
- קיימות כיום דרכים טכנולוגיות להבטיח אנונימיות מוחלטת בגלישה, שאינה מאפשרת לחשוף את זהותו של הגולש.
- התפיסה המקובלת כיום היא, שרשת האינטרנט אינה "מערב פרוע" שכללי המשפט בעולם הממשי לא חלים עליה, אך יש לעצב את הכללים בדרך שתאמים למציאות המורכבת והמיוחדת של האינטרנט.
- הנימוקים להצדקת השמירה על האנונימיות של הגולש מבוססים על טיעונים שיסודם בעיקרון חופש הביטוי והתרומה המשמעותית שיש לרשת האינטרנט לקידומו של עיקרון זה, או על הזכות

¹ רע"א 4447/07 רמי מור נ' ברק אי. טי.סי [1995] החברה לשירותי בזק בינלאומיים בע"מ (25.3.2010), פורסם ב"נבו". להלן: פרשת מור).



לפרטיות, ובכללה, הזכות לשמור על האנונימיות.

- יש הגורסים שהאנונימיות תורמת לקידומו של השיח הדמוקרטי, ויש החולקים על הנחה זו וטוענים שהאנונימיות עלולה לעוות את השיח הדמוקרטי.
- יש הטוענים שבעידן המידע יש להעניק הגנה פחותה לזכות לפרטיות, אך מנגד רבים מצביעים על כך שדווקא בעידן זה נדרשת הגנה חזקה יותר על פרטיות הגולש מבעבר.
- רבים מעלים את החשש שחשיפת זהותו של הגולש תיצור 'אפקט מצנן' שיוביל לצמצום היקף השימוש ברשת האינטרנט. טענה זו לא הוכחה עד כה בצורה אמפירית.
- ישנם חמישה מודלים מוסדיים להסדרת דין האינטרנט: מודל החקיקה הסגורה, המבקש להשיג הסדר שלם וממצה באמצעות החקיקה; מודל החקיקה הפתוחה, המבקש לקבוע כללים להסדרת הסוגיה, שיפותחו בידי בית המשפט; מודל החקיקה השיפוטית, המותיר את מלאכת ההסדרה באופן בלעדי בידי בתי המשפט; מודל ההסדרה העצמית המלאה, המניח את כל ההסדרה בידי המשתמשים וספקי הגישה לאינטרנט, ומודל ההסדרה העצמית החלקית המשלב הסדרה עצמית עם תמריצים שנקבעים בחוק לאימוצה של הסדרה שכזו.
- כאמור, בפרשת מור הכריע בית המשפט העליון שאין להסדיר את הנושא של חשיפת זהותו של מעוול אנונימי ברשת האינטרנט באמצעות חקיקה שיפוטית.
- **בישראל**, הנושא של חשיפת פרטי מעוול ברשת האינטרנט נדון במספר הצעות חוק ובבתי המשפט. ההסדרים שהוצעו הן בהצעות החוק והן בחקיקה השיפוטית היו שונים ומגוונים, אך מכולם עלתה ההכרה בכך שאין לאפשר לרשת האינטרנט לשמש עיר מקלט לביצוע עוולות.
- ברמה הבינלאומית, לא קיימים הסדרים **המחייבים** באופן מפורש את המדינות לאמץ חקיקה המאפשרת את זיהויו של מעוול אנונימי, אם כי, ישנן אמנות ודירקטיבות **המכירות בסמכותן** של המדינות לאמץ חקיקה שכזו מבלי להפר את עקרונות ההגנה על הפרטיות המקובלים במדינות נאורות.
- **בארה"ב** קיימת הבחנה בין סוגיית החשיפה של מעוול אנונימי בעולת לשון הרע, שאותו ניתן לחשוף באמצעות צו מיוחד בהתאם לכללי סדר הדין הפדראליים, לסוגיית החשיפה של מפר זכויות קניין רוחני שהוסדרה בצורה מפורשת בחוק פדראלי.
- התנאים המהותיים למסירת הצו בעולת לשון הרע פותחו בפסיקה אמריקאית מגוונת וענפה, ולא אחידה. ככלל, בתי המשפט נוהגים לייחס משקל רב לשלושה גורמים: תום לבו של המבקש, קיומה של עילת תביעה לכאורה ואיזון בין הערכים המתחרים – חופש הביטוי, הזכות לפרטיות והזכות לשם טוב, בהתאם לנסיבות המקרה.
- בנוגע לחשיפת זהותו של מעוול שהפר זכויות קניין רוחני, החוק מאפשר מסירת צו לחשיפת פרטים בידי פקיד בית המשפט, ורק אם מקבל הצו מתנגד לצו, הנושא יגיע לפתחו של בית המשפט. ואולם, על פי הפסיקה, ניתן למסור צו זה לספקי שירותי אירוח אך לא לספקי שירותי גישה לאינטרנט.²
- גם במקרה זה, התנאים המהותיים לאישורו של הצו לא נקבעו בחוק. השאלה, האם אותם תנאים שנקבעו בפסיקה בנוגע לחשיפת זהותו של מעוול אנונימי בעולת לשון הרע תקפים גם בנוגע לחשיפת זהותו של מפר זכויות קניין רוחני אנונימי, לא הוכרעה.

² על ההבחנה שבין ספק שירותי גישה לאינטרנט וספק שירותי אירוח, ראו להלן, בהקדמה המושגית.



- **בבריטניה**, סמכות בתי המשפט להורות על חשיפת פרטי מעוול הוכרה לראשונה בפסיקה של בית הלורדים בפרשת *Norwich pharmacal*. סמכות זו עוגנה מאוחר יותר בחוק.
- התנאים שנקבעו בפסיקה למתן הצו עוסקים בסיכויי התביעה כנגד המעוול, בטיב היחסים שבין המשיב לצו (ספק שירותי הגישה) ובין המעוול, בשאלת היכולת להשיג את המידע המבוקש מבלי לערב את המשיב, בשאלת הנזקים הצפויים למשיב כתוצאה מן החשיפה ויכולתו של המבקש לפצותו עליהם, למידת מעורבותו של המשיב בביצוע העוולה ובאופיו של הביטוי שבגיניו התבקשה החשיפה.
- **בקנדה**, סמכות בתי המשפט להורות על חשיפת פרטי מעוול מעוגנת בחוקים העוסקים בהגנת המידע האישי, בכללי הפרוצדורה האזרחית העוסקים בחשיפת זהות מעוול במהלך הליך משפטי שכבר החל, ובכללי המשפט המקובל באמצעות צווי *Norwich pharmacal*, בהם ניתן להשתמש לפני תחילתו של הליך משפטי.
- התנאים הקבועים בחוק למתן צו כאמור בהתאם לכללי הפרוצדורה האזרחית מסתפקים בכך שיוכח כי חשיפת זהותו של המעוול חיונית לשם המשך קיומו של ההליך. ואולם, בתי המשפט פירשו סמכותם בצמצום, וקבעו שבית המשפט לא ייתן צו כאמור אלא אם השתכנע שישנה עילת תביעה לכאורה, ושהחשיפה מוצדקת לאור מבחן האיזון בין הערכים המתנגשים.
- הפסיקה בנוגע לתנאים למתן צו *Norwich pharmacal* אינה אחידה, אך ככלל ניתן לומר שכדי שבית המשפט ייעתר לבקשה, יש להוכיח עילת תביעה לכאורה, שהתביעה נעשית בתום לב, שספק שירותי הגישה יהיה מעורב בעקיפין בביצוע העוולה, שנקטו אמצעים סבירים לשם חשיפת זהות המעוול שלא באמצעות הצו, שניתן לפצות את ספק השירות על הנזקים או ההפסדים שייגרמו לו עקב מתן הצו, שהמידע חיוני לשם הגשת התביעה, שלגולשים אין ציפייה סבירה לפרטיות בנסיבות העניין ושהחשיפה נועדה לשם קיומו של הליך משפטי.
- גם **בהונג קונג**, סמכות בתי המשפט להורות על חשיפת פרטי המעוול מעוגנת בכללי הנוגעים להגנה על פרטיות המידע. בתי המשפט מעניקים צווים לשם מטרה זו במתכונת דומה ביותר לזו של צווי *Norwich pharmacal* כאשר הגורמים שהם בעלי משקל בהחלטת בית המשפט אם להעניק את הצו הם: הצורך בחשיפה כדי למנוע שימוש לרעה ברשת, העדר מקור אחר שניתן להפיק ממנו את המידע המבוקש, הצורך בפעולה מהירה, קיומה של חובת סודיות בנוגע לחשיפת המידע בנסיבות שהובאו בפני בית המשפט, היקף המידע שהתבקש אינו רחב יתר על המידה והוא יכול לשמש אך ורק לשם ההגנה על זכויות המבקשים.
- **בגרמניה**, באתרים בעלי אופי ציבורי נדרש מי שמבקש להעלות תוכן לאתר, להירשם ולמסור בעת הרישום פרטים מזהים (שם, כתובת וכדומה), דבר המקל במידה רבה על חשיפת זהותו של המעוול, ואמנם, התופעה של הגשת תביעות דיבה כנגד מגיבים, בלוגרים וכדומה היא תופעה נפוצה למדי בגרמניה.
- בנוגע לחשיפת פרטי מעוול שהפר זכויות יוצרים, קובע החוק הגרמני שניתן יהיה לתבוע את חשיפת זהותו של המעוול, ובלבד שהפרת הזכויות תהיה ברמה מסחרית. פירושו של המושג "רמה מסחרית" מושפע מאופייה של ההפרה, גודלה, השפעתה על רווחי הנפגע וכדומה.
- **בשבדיה**, ניתן לפנות לבית המשפט על מנת שיורה לספק גישה לאינטרנט לחשוף את זהותו של מפר זכויות קניין רוחני, ובלבד שהמבקש יראה עילה לכאורה לתביעה על הפרת זכות שכזו, על ניסיון להפר



את הזכות או על ביצוע פעולה המאפשרת הפרה של הזכות. לא מצאנו בדין השבדי הוראות העוסקות בחשיפת פרטי מעוול בעוולות נוספות.

- המשפט העברי מייחס ערך רב לעיקרון חופש הביטוי, אם כי, נראה כי משקלו של העיקרון פחות מזה שניתן לו בהגות הליברלית.
- המשפט העברי מייחס ערך רב להגנה על פרטיות האדם, ושולל חשיפת זהותו של משתמש על ידי ספקי הגישה, זולת אם החשיפה נועדה להגן על גופו או רכושו של אדם.



1. הקדמה מושגית³

על מנת להבין היטב את הדיון בכל נושא הקשור להסדרת הגלישה ברשת האינטרנט, יש להבין הן את הרקע הטכנולוגי הקשור לנושא, והן את מושגי היסוד הרווחים בתחום:

רשת האינטרנט הינה רשת המחברת בין רשתות רבות של משתמשים, המחוברים לרשת הגלובאלית באמצעות ציוד קצה. ציוד הקצה הינו כל אמצעי המאפשר חיבור לרשת האינטרנט, כמחשב, טלפון סלולארי, מחשב לוח וכדומה.

המשתמש הוא מי שמעלה תוכן, צופה או אף מוריד תוכן מאתרי האינטרנט, למחשבו האישי.

ספק שירותי גישה לאינטרנט (ISP): החיבור של ציוד הקצה לרשת מתאפשר רק לאחר שהמשתמש יוצר קשר עם ספק שירותי גישה, שהוא זה שלמעשה יוצר את החיבור בין המחשב לרשת האינטרנט.

ספק שירותי אירוח הוא למעשה גוף שמחזיק במחשבים בעלי נפח זיכרון עצום, המאפשר לאנשים או גופים המבקשים להעלות תוכן לרשת האינטרנט, לאחסן את התוכן במחשבי הספק.

ספק שירותי גישה למחשבים הוא כל גוף המאפשר לאנשים רבים לעשות שימוש במחשביו כדי להתחבר לרשת האינטרנט, כגון: קפה אינטרנט, אוניברסיטה או בית ספר.

ספקי תוכן הם אלו אשר ממלאים את האתרים בתוכן, כגון: *NRG, Ynet*, 'נענע' וכדומה.

כדי לחבר את המחשב לרשת, על המשתמש להתקשר עם ספק שירותי גישה לרשת. בעת ההתקשרות עם המשתמש, מבקש הספק מהמשתמש שימסור לו פרטים מזהים, והוא נותן למשתמש מספר מזהה (*IP*), שמעתה ואילך ישמש לשם זיהויו של המחשב ברשת.

בעיקרון, יכול ספק שירותי הגישה להחליף מעת לעת את המספר המזהה, אך לרוב נהוג שהמספר המזהה נותר קבוע.

כאשר המשתמש מבצע פעולה כלשהי הקשורה לרשת (גלישה, רכישה מחנות מקוונת, העלאת תכנים וכדומה), ציוד הקצה של המשתמש יוצר קשר עם ספק שירותי הגישה, באמצעות פרוטוקול המכונה *TCP/IP*, המחייב החלפת כתובות ה-*IP* בין מחשבי הספק למחשב של המשתמש, כדי שתיווצר תקשורת ביניהם.⁴

מאחר שלכל ספקית גישה ברשת מוקצה מרחב כתובות *IP*, זיהוי כתובת ה-*IP* מאפשר לאתר את ספק הגישה לאינטרנט, שבידיו מצויים הפרטים המזהים של המשתמש שהוא בעל כתובת ה-*IP*.

לאחר זיהויו של ספק הגישה, ניתן לבקש ממנו לחשוף את הפרטים המזהים שמסר בידיו המשתמש, וכך לזהותו. אמנם, כאשר המשתמש התחבר לרשת דרך מחשב שהוא בבעלות ספק שירותי גישה למחשבים, לא יהיה די בזיהויו של בעל כתובת ה-*IP* לשם חשיפת זהות המשתמש, משום שהזיהוי יוביל רק לזהותו של ספק שירותי הגישה למחשב, ולא לזהותו של המשתמש הספציפי.

³ לרקע טכנולוגי נרחב יותר, ראו: מיכאל בירנהק "חשיפת גולשים אנונימיים ברשת" חוקים ב, 51, 59 – 62 (2010) להלן: בירנהק, חשיפת גולשים).

⁴ זוהי 'ברירת המחדל', אם כי, ישנם אתרים הדורשים הזדהות לפני הגלישה בהם.



במקרה זה יהיה צורך בשיתוף פעולה גם מצידו של ספק שירותי הגישה למחשבים, כדי שינסה לסייע באיתור המשתמש הספציפי בשעה מסוימת. **זיהוי שכזה הוא בעייתי**, משום שקשה מאוד לאתר באופן וודאי את המשתמש המסוים בשעה מסוימת, וייתכן זיהוי מוטעה.

חשוב להדגיש שכיום **קיימים שרתים ותוכנות המאפשרים אנונימיות מוחלטת**, באמצעות שימוש בטכנולוגיות מתקדמות שלא כאן המקום לפרטן.⁵ גולש שביצע עוולה באמצעות שימוש בטכנולוגיה מסוג זה, ייהנה מחסינות טכנולוגית מפני חשיפת זהותו.

2. תמורות במשקלם של ערכים בעידן המידע

לדעת רבים, המשמעות של יצירתה ופיתוחה של רשת האינטרנט היא יותר מאשר מהפכה טכנולוגית. לדבריהם, הרשת יצרה למעשה מהפכה תרבותית,⁶ עידן חדש, שיש המכנים אותו בשם 'עידן המידע'. עידן זה מחייב בחינה מחודשת בדבר תקפותם של הערכים שלאורם התנהלה החברה לפני עידן המידע.

2.1. מן "המערב הפרוע" לדין האינטרנט

בשנים הראשונות לקיומה של רשת האינטרנט, אופייה הגלובלי של הרשת, זמינותה לכל אדם והאפשרות להעביר מסרים ומידע באופן אנונימי ומייד, הובילו רבים למסקנה **שרשת האינטרנט יצרה למעשה עולם חדש, נטול גבולות, המשוחרר מכבלי העולם הישן**. לפי תפיסה זו, ששבתה את לבם של רבים, רשת האינטרנט הינה מעין "מערב פרוע", **מרחב וירטואלי שבו אין תחולה לכללי המשפט החלים על העולם הממשי**.⁷

אחרים הציגו תפיסה דומה אך פחות רדיקלית, ולפיה, **רשת האינטרנט אולי לא צריכה להיות "מערב פרוע", אך בפועל, בשל אופייה היא בהכרח תביא להיעלמותן של חלק מהזכויות שהיו מוכרות בעולם המשפט שלפני עידן האינטרנט**. כך למשל, סקוט מקנילי, מנכ"ל חברת "סאן מיקרוסיסטמס" יצא בהכרזה מפורסמת ש"באינטרנט אין לנו פרטיות", ולמעשה "עלינו לחיות עם זה".⁸

באופן דומה, ג'ון פרי ברלו⁹ קבע ש"דיני זכויות היוצרים הגיעו אל קצם", משום שחוק המקנה ליוצר זכויות לשלוט בביטוי הפיזי של היצירה איננו מתאים עוד לסביבה הווירטואלית של הרשת.

ואולם, בחלוף השנים גילו רבים את הסכנות הטמונות ברשת האינטרנט, ואת הפגיעות שיש בכוחה לגרום לאנשים בעולם הממשי, ובעקבות זאת התפתחה תפיסה הפוכה, שלפיה **רשת האינטרנט כפופה לאותם כללים משפטיים החלים על העולם הממשי**.¹⁰

⁵ ראו למשל, **כאן**. לדיון נרחב בנושא ראו, מסמך מרכז המחקר והמידע של הכנסת בנושא "שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה" (כתיבה: רועי גולדשמידט, 1 בינואר 2012).

⁶ ראו יצחק זמיר, "חופש הביטוי באינטרנט" **משפט וממשל** ו (תשס"ג) 353.

⁷ ראו: מיכאל בירנהק, "חורים ברשת: פורנוגרפיה, מידע ועיצוב מדיניות בסביבה דיגיטלית" **פוליטיקה**, גיליון 13 (2005) 101 ("התקופה הראשונה של פריצת האינטרנט הציגה את דמיונם של רבים: הרשת יוצרת אפשרויות ביטוי חדשות: יותר דוברים יוכלו לפנות ליותר נמענים, בעלות נמוכה מאי-פעם... הרשת נתפסה כדמוקרטיה במיטבה... היותה של הרשת חוצת-גבולות פיזיים הועלתה אף היא על נס... חומות וגדרות אינם מטרידים אותה, וגם לא גרלים, ממשלות, צנזורים, מחוקקים או בתי משפט... הרשת הוצגה כ"מקום אחר", שאיננו כפוף לשום מגבלה... מקום של חופש מוחלט. לפי עמדה זאת, המשפט הקיים איננו חל ברשת"). (המאמר זמין גם **באתר האינטרנט של איגוד האינטרנט הישראלי**).

⁸ Polly Sprenger, Sun on Privacy 'Get Over It' (1999), www.wired.com/politics/law/news/1999/01/17538

⁹ J.P. Barlow "The Economy of Ideas: A framework for Patents and Copyrights in the Digital Age" **WIRED**, 2.03: March, 1994.

¹⁰ ראו למשל, יובל קרניאל, "אנונימיות ולשון הרע באינטרנט - בין חופש ביטוי להפקרות", בתוך: **עיתונות דוט.קום: העיתונות המקוונת בישראל** (בעריכת תהילה שוורץ-אלטשולר, הוצאת המכון הישראלי לדמוקרטיה, ירושלים תשס"ז) 85, בעמ' 87 ("אין היום רבים המחזיקים בעמדה הרומנטית שהרשת היא מעין מערב פרוע, מקום חופשי, שאין להחיל



בשנים האחרונות ניכרת התפתחות של מגמת ביניים, הגורסת שכללי המשפט החלים על העולם הממשי אינם מתאימים לרשת האינטרנט, אך מאידך גיסא, אין להותיר את הרשת כשדה פרוץ, נטול גבולות משפטיים. לפיכך, יש לעצב עבור הרשת דין מיוחד – דין האינטרנט. דין זה יעוצב בהתאם לצרכים ולאחרים שמציבה הרשת בפני האדם.¹¹

2.2. חופש הביטוי ברשת

”עוצמת ההגנה על חופש הביטוי תולה עצמה, בין השאר, באמצעי התקשורת שבו נעשה השימוש”.¹² עיקרון זה, המכונה גם - עיקרון ייחודיות המדיום, מחייב לבחון את מאפייני השימוש ברשת האינטרנט, לפני כל ניסיון לשרטט את קווי המתאר לגבולותיו של חופש הביטוי באינטרנט.¹³

לפני כ-15 שנים נקבע בארה"ב חוק פדראלי האוסר הצגתם של מסרים לא צנועים הפוגעים בטעם הטוב ברשת האינטרנט. ארגון זכויות האדם האמריקני עתר לבית המשפט העליון הפדראלי בתביעה שיכריז על בטלותו של החוק, בהיותו פוגע בחופש הביטוי. בית המשפט, בפסק דין תקדימי,¹⁴ קיבל את העתירה בהתבססו על ההיקף שיש להעניק לעיקרון חופש הביטוי ברשת האינטרנט. בית המשפט סקר את ההבדלים שבין השימוש ברשת האינטרנט לבין השימוש באמצעי תקשורת אחרים, וקבע שלאור הבדלים אלו יש לקבוע שיש להעניק הגנה מרבית לחופש הביטוי באינטרנט, שהיא רחבה בהיקפה מן ההגנה הניתנת לביטוי בכלי תקשורת אחרים.

בהסתמך על פסק דין זה, דחה השופט מישאל חשין, בתפקידו כיו"ר ועדת הבחירות לכנסת ה-16, עתירה של סיעת ש"ס בכנסת לאסור על חבר הכנסת (דאז) אופיר פינס, להפיץ תעמולת בחירות באינטרנט, על פי היקש מחוק התעמולה, שאסר את שידור התעמולה ברדיו או בטלוויזיה. בהחלטתו, הציג השופט חשין את ההבדלים המרכזיים שבין אמצעי התקשורת:

אם נתבונן ברשת האינטרנט ונעמיד בצדה את הרדיו והטלוויזיה, וידענו כי השניים שונים הם באורח מהותי... תדרי הרדיו והטלוויזיה מוגבלים הם במספרם (כהיום הזה) ואילו במרחב האינטרנט אין מחסור במשאב הערוצים; הרדיו והטלוויזיה, כל אחד מהם, הינו מדיום שיכולת ברירת התכנים בו מעטה עד-לאין-שיעור מן היכולת לברור תכנים באינטרנט. יתר-על-כן, המאזין לרדיו והצופה בטלוויזיה הינם מאזין וצופה פסיביים – השניים הם בבחינת "מאזין שבוי" ו"צופה שבוי" – בעוד אשר המשתמש באינטרנט הינו, במובן מסוים, גם שחקן על הבימה... האינטרנט שונה מאחיו ומאחותו הבכירים גם במהירות התעבורה, בזמינות השירות, בפשטות ובעלות. מאפיינים אלה, השונים באינטרנט מזה, וברדיו ובטלוויזיה מזה,

עליו את הנורמות והכללים של החברה האנושית המאורגנת ושל המדינה. אין חולק כי יש להחיל את החוק גם על פרסומים באינטרנט; רע"א 4447/07 רמי מור נ' ברק אי. טי.סי [1995] החברה לשירותי בזק בינלאומיים בע"מ (25.3.2010, פורסם ב"נבו". להלן: פרשת מור), פסקה 17 לפסק הדין של כב' השופט ריבלין ("האינטרנט אינו "מערב פרועי" ואין לראות בו מסגרת שבה אין דין ואין דיין").

¹¹ ראו למשל, יובל קרניאל וחיים ויסמונסקי, "חופש הביטוי, פורנוגרפיה וקהילה באינטרנט", מחקרי משפט כג(1), תשס"ז-2006, 259, בעמ' 282 (להלן: קרניאל וויסמונסקי, קהילה באינטרנט).

¹² תב"מ 16/2001 ש"ס התאחדות ספרדים עולמית שומרי תורה נ' פינס ואח' (להלן: פרשת ש"ס)

¹³ ראו יובל קרניאל, "חופש הביטוי באינטרנט" עלי משפט א (תש"ס) 163, בעמ' 181-183.

¹⁴ Reno v. American Civil Liberties Union (1997) 521 U.S. (להלן: פרשת רנו).



מצדיקים אף יחס שונה לאינטרנט מכאן ולרדיו ולטלוויזיה מכאן.¹⁵

בהתאם לשיקולים אלה, קבע השופט חשין שיש להעניק לחופש הביטוי באינטרנט משקל רב מכפי שניתן לו בכלי תקשורת אחרים, ועל כן דחה את העתירה.

שיקול נוסף שרבים מעלים בהקשר זה הוא, שיש להעניק הגנה רחבה יותר לחופש הביטוי ברשת האינטרנט מכפי שניתן לו באמצעי תקשורת אחרים, משום שרשת האינטרנט מגשימה את הרעיון הדמוקרטי של "ככר העיר", שבה מתנהל שוק חופשי של רעיונות, בו יכול כל אחד להשמיע את קולו ולהתרשם מקולותיהם של אחרים. "הרשת היא אפוא זירה טבעית להתפתחות שיח מבוזר, המאפשר למשתתפים רבים להתבטא באופן עצמאי וישיר במעין "הייד פארק" וירטואלי... וכעת יכול אדם לממש בפועל את חופש הביטוי, שבעידן הטרור אינטרנט, היה נתון לו כמעט באופן תיאורטי בלבד".¹⁶

ואולם, להבדלים שבין הביטוי ברשת האינטרנט לביטוי בכלי תקשורת אחרים יכולה להיות גם השפעה הפוכה. ככל שהמידע נגיש יותר, תפוצתו רחבה יותר והיכולת לשמור אותו גבוהה יותר, הרי שפוטנציאל הפגיעה שלו עולה, ודבר זה יכול להצדיק הגבלה רחבה יותר של הביטוי מן ההגבלה הקיימת על הביטוי בכלי תקשורת אחרים.¹⁷

2.3. אנונימיות

תנאי מרכזי לקיומה של "ככר העיר" הוא האפשרות להתבטא באנונימיות, המאפשרת לגולש לבטא דברים שלא היה מעז לבטא אילו היה נדרש לחשוף את זהותו,¹⁸ להסיר מעליו מסכות שבדרך כלל הוא עוטה על עצמו ולבטא את אישיותו בצורה מהימנה וגלויה.¹⁹

יש הטוענים שהאנונימיות חשובה גם כדי להגן על חופש ההתאגדות. לפי טיעון זה, רבים מבין הגולשים באינטרנט לא היו מסוגלים ליצור לעצמם תא חברתי אילו היה הדבר כרוך בחשיפת זהותם. לכן, השמירה על האנונימיות חיונית לשם שמירת זכותם להתאגד.²⁰

ואולם, יש הטוענים שהתפיסה הגורסת שלאנונימיות יש תרומה ממשית לשיח הדמוקרטי היא לא יותר מאשר מיתוס, מכמה סיבות. ראשית, בשל מבנה הרשת, אין בה מוקדים ריכוזיים המהווים מעין "צוואר בקבוק" לכל הביטויים ברשת. לפיכך, הרשת יוצרת מעין "בימות רבות ומבוזרות, באופן שייתכן מצב שיש

¹⁵ דברי יו"ר ועדת הבחירות דאז, השופט מישאל חשין, בפרשת ש"ס.

¹⁶ בש"א 4995/05 (שלום – י-ם) פלונית נ' בזק בינלאומי בע"מ (טרם פורסם, 28.2.2006); פרשת מור, סעיף 14 לפסק דינו של כב' השופט ריבלין. וראו גם, ניבה אלקין-קורן, "המתווכים החדשים בכיכר השוק הוירטואלית" משפט וממשל ו(2), ניסן תשס"ג עמ' 381-382 (להלן: אלקין קורן, המתווכים החדשים); יובל קרניאל, "חופש הביטוי באינטרנט" עלי משפט (1) (תש"ס, 1999), עמ' 186 (להלן: קרניאל, חופש הביטוי); Victoria Smith Ekstrand, "Unmasking Jane and John Doe: Online Anonymity and the First Amendment", 8 Comm. L. & Pol'y 405, at 407.

¹⁷ "הלכה פסוקה היא כי לעיתים היקף הפגיעה ישפיע אף על חומרת הפגיעה" – ע"א (ת"א) 2319/08 פלוני נ' פלונית (פורסם במאגר המשפטי 'נבו'), סעיף 28 לפסק דינו של השופט שנלר. הדיון עסק בפרסום פסק דין ברשת האינטרנט שפרטיו עלולים לפגוע בפרטיות המתדיינים.

¹⁸ "היכולת לשמור על עילום-שם היא לעיתים תנאי לעצם האפשרות או הנכונות להתבטא. יש מצבים שבהם אדם שלא יוכל לדבוק באלמוניותו – לא יתבטא כלל. כך, למשל, בשל תחושות אישיות כמו בושה או מבוכה, או בשל לחצים חיצוניים וחששות מפני תגובת הסביבה" (פרשת מור, סעיף 11 לפסק דינו של כב' השופט ריבלין).

¹⁹ "האנונימיות והאפשרות למצבים מרובים באינטרנט נותנות למשתמש אפשרויות ייחודיות לשחק עם זהותו שלו, לחקור את "האני האמיתי" שלו, ולתת ל"אני האמיתי" שלו ביטוי. "האני האמיתי" הן אותן איכויות פנימיות שיש לפרט. אלו תכונות שהפרט לא מבטא בחיים היום יומיים, במפגשים פיזיים שיש לו" (שרית הכהן דרוקמן, "ההשלכות החברתיות לחברות קבועה בפרומים באינטרנט", חיבור לשם קבלת התואר מוסמך למדעי הרוח והחברה באוניברסיטת בן גוריון, ינואר 2008, עמ' 14).

²⁰ Minjeong Kim, "The Right to Anonymous Association in Cyberspace us Legal Protection for Anonymity in Name, in Face and in Action", Scripted Volume 7, Issue 1, 51 (April 2010).



למתבטא קהל מצומצם בלבד, אם בכלל".²¹ שנית, מאחר שאין סינון לתוכן המידע המועלה לרשת, אמינותו של המידע מוטלת בספק. שלישית, שליטה של גופים פרטיים רבי עצמה ברשת מאפשרת להם לתמרן את המשתמש בכל הנוגע לאופן החיפוש, תוצאותיו וסוג המידע שאליו הוא ייחשף.²² גופים אלו מסוגלים גם להציף את הרשת במידע התואם את תפיסת עולמם, ובדרך זו לעוות את השיח הדמוקרטי באמצעות יצירת מצג שווא של ריבוי דוברים האוחזים בעמדה אחת, בעוד שלמעשה מדובר בדובר אחד המעסיק "טוקבקיסטים בתשלום".²³ ולבסוף, בשל כמות המידע העצומה הקיימת ברשת, סובל המשתמש מ"ערפיח המידע" המקשה עליו לבור את המוץ מן התבן, דבר המפחית במידה ניכרת את עצמת הביטוי.²⁴ כמו כן, יש הסבורים שאין להגן על האנונימיות, משום שהיא עלולה לשמש 'עיר מקלט' לביצוע עוולות ופשעים.²⁵

2.4. הזכות לפרטיות בעידן המידע

בעידן המידע, ישנה הכרה חברתית בערכו של המידע לשם קידומן של תועלות חברתיות. בעקבות זאת יש שטענו שהזכות לפרטיות היא תוצר מלאכותי של התרבות הליברלית המבכרת את האינטרס של הפרט על פני האינטרס החברתי, ומאפשרת הסתרת מידע שהוא חיוני להבטחת שלום הציבור, רווחתו וביטחונו.²⁶

טענה דומה מקדמים אנשי הניתוח הכלכלי של המשפט ולפיה ניתוח כלכלי של הזכות לפרטיות מגלה שזוהי זכות שאינה יעילה, משום שהיא מעכבת זרימת מידע שהוא חיוני ליצירת תנאים מיטביים של שוק חופשי, היא מאפשרת הטעייה של לקוחות, והיא מונעת סחר במידע, שהוא משאב שניתן וראוי לסחור בו.²⁷ בהתאם לכך קובע פוזנר, שהגנה על הפרטיות תהיה מוצדקת רק כאשר היא תעודד יצירת מידע נוסף, כגון כאשר ההגנה נחוצה לשם שמירת סודות מסחריים, פטנטים וכדומה.

ביקורות אלו, בצידן של ההערכות שמאפיינה של רשת האינטרנט אינם מאפשרים עוד הגנה על הפרטיות,²⁸ מעידות על ערעור מעמדה של הזכות לפרטיות בעידן המידע.

מנגד, רבים סבורים שדווקא בעידן המידע נדרשת הגנה רחבה ויעילה יותר על הפרטיות מכפי שהיה מקובל בעבר, מן הסיבות שלהלן.

²¹ ראו, אלקין-קורן, המתווכים החדשים, עמ' 382.

²² שם, עמ' 383.

²³ ראו, מסמך מרכז המחקר והמידע של הכנסת בעניין "מקומם של ה"טוקבקים" בשיח הציבורי בישראל", כ"ח בתמוז תשס"ו, 22 באוגוסט 2006 (כתיבה: רועי גולדשמידט), עמ' 5-6.

²⁴ אלקין-קורן, המתווכים החדשים, עמ' 406.

²⁵ על הקשר שבין האנונימיות לביצוע עוולות עמד כבר אפלטון, בספר השני של חיבורו – 'הרפובליקה'. בספר, מספר גלאוקון-אחיו של אפלטון, על רועה צאן המוצא טבעת עם כוחות קסמים הגורמת למי שעונד אותה להיות בלתי נראה. הרועה עונד את הטבעת ותחת מעטה האנונימיות מבצע פשעים חמורים. לעניין זה ראו לעניין זה יצחק כהן ואמל ג'ברין, "חשיפת זהותם של משתמשים אנונימיים באינטרנט- נקודת מבט מוסדית", מחקרי משפט כח (2012), 7. (להלן: כהן וג'ברין, חשיפת זהותם). וראו גם כתבה בכתב העת העין השביעית מן ה-13 לאפריל 2011, בה צוטט פרופ' אסא כשר כמי שאמר בכנס אקדמי באריאל, ש"צריך לצמצם את חופש הביטוי לשם שמירה על כבוד האדם. היום ההגנה היא על כבודו של הטוקבקיסט האנונימי, שיושב לו בסתר בתא החשוך שלו, ומפעיל את המקלדת שלו כדי להשמיץ, כדי להכפיש, כדי לזרוק לחלל טענות שלא היו ולא נבראו, ובית-המשפט יגן עליו בשם חופש הדיבור וכבוד האדם. ומה עם שמו הטוב של האדם שהאיש הזה מקלקל? עליו צריך להגן".

²⁶ Amitai Etzioni, *The Limits of Privacy* 183-184 (New York, Basic Books, 1999), at pp. 185.

²⁷ נספח לדן וחשבונו הצוות לבחינת החקיקה בתחום מאגרי המידע, ינואר 2007, עמ' 83-84 (להלן: דו"ח מאגרי מידע). Richard A. Posner, "An Economic Theory of Privacy", in *Philosophical Dimensions of Privacy: An Anthology* 333, at pp. 336-339 (Ferdinand Davis Schoeman ed., Cambridge, Cambridge University Press, 1984). עמ' 84-85.

²⁸ ראו לעיל, ליד הציון להערה 9; ניב אחיטוב, עולם ללא סודות – על חברת המידע הפתוח (תל אביב, עם עובד תשס"ב), עמ' 118-123.



בעבר, ההגנה על הפרטיות דרשה הגנה מצומצמת ביותר, על פרטי מידע "רגישים", כמצב בריאותי, נטיות מיניות, מראה, הרגלי צריכה, מצב כלכלי וכדומה. ואולם, טכנולוגיית איסוף המידע מן הגולשים מאפשרת הצלבת מידע משוכללת, המאפשרת חשיפת מידע זה מפיסות מידע "תמימות", שלכאורה אין להן קשר לאותו מידע "רגיש". מצב זה מגביר את הצורך בהגנה על הפרטיות, ודורש את החלת ההגנה גם על פרטי מידע שבעבר לא היה נהוג להגן עליהם.²⁹

היבט נוסף קשור לקלות היחסית של החזירה למרחב הפרטי. אם בעבר חזירה זו הייתה דורשת כוח, תחכום והקצאת משאבים מיוחדים, כיום, "חזירה לפרטיות מתאפשרת בלחיצת כפתור".³⁰ מצב זה מעורר את הצורך להגביר את ההגנה, כדי שתוכל להתמודד עם האתגרים החדשים.

כמו כן, אם בעבר מי שפרטיותו נפגעה היה מודע לפגיעה ומסוגל להתמודד עמה באופן מידי בכלים משפטיים, כיום, בשל ההתפתחות הטכנולוגית המואצת, רוב המשתמשים ברשת אינם מודעים לפוטנציאל הרב של הפגיעה בפרטיותם, ובשל כך, על פי רוב, אינם מזהים את הפגיעה כאשר היא מתרחשת. בהנחה שהפרטיות עדיין נחשבת כערך חברתי שמן הראוי להגן עליו, יש הטוענים שמצב זה דורש הגנה רחבה יותר מבעבר, כדי למנוע מצב של העדר פרטיות ברשת.³¹

ולבסוף, **רבים טוענים, שכל פגיעה בפרטיותם של הגולשים עלולה ליצור 'אפקט מצנן', שיוביל להפחתת השימוש ברשת.** בהנחה שזרימה חופשית של מידע ברשת האינטרנט היא אינטרס חברתי שמן הראוי להגן עליו, טיעון זה עשוי להצדיק שמירה קפדנית על פרטיות הגולש ברשת האינטרנט.³² ברם, הטענה האמורה מעולם לא הוכחה מבחינה אמפירית,³³ הגם שבתי המשפט בישראל ובעולם נוטים לייחס לה משקל רב.³⁴

3. מודלים מוסדיים

השאלה המרכזית שעמדה בייסוד פסיקת בית המשפט העליון בפרשת מור הייתה, מיהו הגוף השלטוני שאמור להסדיר את הנושא של חשיפת זהותו של מעוול ברשת האינטרנט:

בעניין זה ישנם חמישה מודלים: **מודל החקיקה הסגורה; מודל החקיקה הפתוחה; מודל החקיקה השיפוטית; מודל ההסדרה העצמית המלאה ומודל ההסדרה העצמית החלקית.**

עד לפסיקת בית המשפט העליון בפרשת מור, הוסדר נושא זה בדרך של חקיקה שיפוטית, אך בית המשפט העליון דחה דרך זו וקבע שבתי המשפט אינם מוסמכים להסדיר את הנושא כל עוד לא נקבע בחוק הליך מסודר לחשיפת זהותו של המעוול. בשורות שלהלן יוצג כל אחד מן המודלים האמורים, וייסקרו יתרונותיו וחסרונותיו.

²⁹ ראו, **פרטיות בסביבה דיגיטלית** (סדרת פרסומי המרכז למשפט וטכנולוגיה, חוברת מס' 7, מאת תלמידי הסדנה הרב-תחומית במשפט וטכנולוגיה בפקולטה למשפטים, אוניברסיטת חיפה), עמ' 18 (להלן: פרטיות בסביבה דיגיטלית).

³⁰ ראו, **לוחמה בטרור בזירת המידע**, (מאת תלמידי הסדנה הרב-תחומית במשפט וטכנולוגיה בפקולטה למשפטים, אוניברסיטת חיפה), עמ' 61.

³¹ ראו, **פרטיות בסביבה דיגיטלית** עמ' 20.

³² ראו **פרשת מור**, סעיף 4 לפסק דינו של כב' השופט ריבלין, וכן סעיף, נ"א לפסק דינו של כב' השופט רובינשטיין.

³³ ראו **כהן וג'ברין, חשיפת זהותם**, עמ' 36. על דבריהם יש להוסיף, שלדברי העיתונאי יואב יצחק, מנהל האתר NFC, פגיעה חלקית באנונימיות של המגיבים באתר הובילה אמנם לירידה במספר התגובות באתר, "בשלב הראשון של התהליך", אך "הוא שב ועולה בהדרגה", ו"ניתן לראות שינוי חיובי באופיין ובאיכותן של התגובות מאז חשיפת כתובות ה-IP של המגיבים". ראו מסמך מרכז המחקר והמידע בעניין "תוכן גולשים ואחריות מנהלי אתרי אינטרנט" (כתיבה: רועי גולדשמידט, 11 במאי 2008), עמ' 5.

³⁴ **פרשת מור**, שם.



3.1. חקיקה שיפוטית

מודל החקיקה השיפוטית מבוסס על פיתוח ההסדרים לחשיפת זהותו של מעוול אנונימי באמצעות הפסיקה. מודל זה התפתח בעיקר בבריטניה, כפי שיפורט בהמשך.

דומה כי אין חולק כיום על סמכותו **הפורמאלית** של בית המשפט להסדיר סוגיה משפטית הטעונה הכרעה בדרך של חקיקה שיפוטית.³⁵ לפיכך, כל אימת שקיימת סוגיה משפטית שלה אין מענה בחוק, נשאלת השאלה האם **מן הראוי** שבית המשפט הוא יהיה הגוף השלטוני שיוביל את ההסדרה?

בהעדר חקיקה בנושא החשיפה של מעוול אנונימי ברשת האינטרנט, מודל החקיקה השיפוטית שימש את בתי המשפט לשם פיתוח כללים בנוגע לחשיפת זהותו של מעוול אנונימי, עד לפסיקת בית המשפט העליון בפרשת מור, ששללה (בדעת הרוב) את המשך השימוש במודל זה.³⁶

יתרונה המרכזי של החקיקה השיפוטית הוא, **שיש בה כדי לתת מענה למגוון רחב של מצבים שבהם עשויה להידרש חשיפת זהותו של המעוול, מצבים שקשה למחוקק לחזותם מראש.**³⁷ בשל כך, חקיקה ראשית עלולה להיכשל באחת משתיים: או שהיא תעצב הסדר כולל עבור קשת רחבה של מצבים תוך התעלמות מאופיין הייחודי של הזכויות המתנגשות בכל אחד מן המצבים, המצדיק לעיתים שוני בעיצובו של ההסדר המשפטי,³⁸ או שהיא תסדיר רק את המצבים השכיחים שבהם נדרשת החשיפה, ותותיר מצבים אחרים ללא מענה משפטי. במצב זה, עלולה שתיקת המחוקק להתפרש כהסדר שלילי, המונע לחלוטין חשיפה של פרטי מעוול, בנסיבות שבהן לא עסק החוק.³⁹

יתרון נוסף של החקיקה השיפוטית, נובע מהעדר הוודאות לגבי תוכנו הראוי של ההסדר המשפטי. קביעת ההסדר המשפטי בעניין החשיפה של זהות המעוול מושפעת רבות הן משינויים טכנולוגיים שאת חלקם קשה עדיין לצפות והן מהערכה אמפירית בנוגע להשפעתו של ההסדר על רמת הגלישה באינטרנט ("האפקט המצנן"), שאף היא איננה זמינה כעת. במצב זה, **יש הסוברים שיש להעדיף חקיקה שיפוטית, על פני הסדר המעוגן בחקיקה ראשית, שמטבע הדברים חקיקה כזו קשיחה יותר וקשה יותר לשינוי.**

ואולם, לחקיקה השיפוטית יש גם חסרונות לא מבוטלים. חקיקה שכזו מבוססת בהכרח על מתן מענה לסכסוך נתון. **מאחר שבית המשפט אינו יכול לזוז חקיקה, פתרונה המלא של סוגיה תלוי במידה רבה בנכונותם של צדדים פוטנציאליים להביא סכסוך בפניו.** בשל כך, על מנת להגיע להסדר שלם וממצה יידרשו לעיתים שנות דור.⁴⁰

חקיקה שיפוטית מבוססת על הליך שיפוטי, שבמסגרתו מוצגות עמדותיהם של הצדדים. במסגרתו של הליך זה **לא מובאות בפני בית המשפט עמדותיהם של צדדים שלישיים, לרוב אין בית המשפט מסוגל לדון**

³⁵ סמכות זו קבועה למשל, בסעיף 1 לחוק יסודות המשפט, התש"ס-1980, וראו בהרחבה, ברק, חקיקה שיפוטית, עמ' 33-36; **כהן וג'ברין, חשיפת זהותם**, עמ' 20-21.

³⁶ ראו להלן, בפרק העוסק בפסיקת בתי המשפט בישראל.

³⁷ ראו בהרחבה, **כהן וג'ברין, חשיפת זהותם** עמ' 28-31.

³⁸ ראו שם, עמ' 29.

³⁹ ראו שם, עמ' 30.

⁴⁰ ראו אהרון ברק, "חקיקה שיפוטית" **משפטים** יג (תשמ"ג) 25, בעמ' 50 (להלן: ברק, חקיקה שיפוטית). וראו גם:

J. Woodford Howard, Jr., *Adjudication Considered As a Process of Conflict Resolution: A Variation on Separation of Power*, 18 **J. PUB. L.** 339, 343 (1969).

ברק (שם, עמ' 52, הערה 148) מעיר, שגם הרשות המחוקקת "צריכה נענוע לפני שתנוע, אך בעוד שהשופט משהוז חייב ליתן פסק דין, הרי המחוקק יכול להימנע מחקיקה בעצם הימנעותו מלדון בעניין".



בשאלות מדיניות החורגות מגבולותיו של הסכסוך (למשל, עלויות כלכליות של ההסדר המוצע) וכללי דיני הראיות מגבילים את סוג המידע שיובא בפניו. מסיבה זו, יש הטוענים שהשופט הוא "מחוקק בעל מום".⁴¹

החקיקה השיפוטית אף עלולה לפגוע בתדמיתו הניטראלית של השופט.⁴²

כמו כן, כל עוד לא נקבע תקדים מחייב בידי בית המשפט העליון, חקיקה שכזו עלולה ליצור מספר הסדרים המתקיימים במקביל בערכאות שונות.⁴³ דבר זה עלול לפגוע בוודאות המשפטית ואף ליצור "אפקט מצנן" שירתיע רבים מהתבטאות חופשית ברשת האינטרנט.⁴⁴

ולבסוף, חקיקה שיפוטית קובעת את תוכנו של ההסדר בדיעבד, ואיננה מאפשרת לגולש להכיר את ההסדר מראש, ולהיזהר מפני התבטאות שעלולה בסופו של דבר להביא לחשיפת זהותו.⁴⁵ יתר על כן, אף לאחר שנקבעה ההלכה, היא "מכוסה" על פי רוב במלל רב של עובדות, טיעונים ודיון משפטי, המקשה על האזרח הקטן להכיר את הכלל המשפטי שנקבע בפסיקה.⁴⁶

יש הסוברים שאין לתת לשני השיקולים האחרונים משקל רב, משום שההיסטוריה השיפוטית בנוגע לחשיפת זהותו של מעוול אנונימי מגלה שלמרות הגישות השונות, בתי המשפט בישראל מאוחדים בדעה שאין לאפשר לאנונימיות לשמש מחסה לביצוע עוולות, ועד לפסיקת בית המשפט בעניין מור האמורה, ניכרה מגמה של התכנסות להסדר אחיד. לכן, אין להניח שלמעוול אנונימי תהיה ציפייה לגיטימית וסבירה לכך שיוכל לבצע עבירות ועוולות תחת מעטה האנונימיות, מבלי להיחשף,⁴⁷ ואף אין לחשוש שמא חוסר הוודאות יצנן את נכונותם של גולשים לעשות שימוש ברשת.⁴⁸

בשל מגבלותיה, מקובל שחקיקה שיפוטית ראויה לשם עריכת רפורמה "מוגבלת וקומפקטית", אך אין היא ראויה לשם עריכת "רפורמה מקיפה בענף משפטי שלם".⁴⁹

3.2. חקיקה

במסגרת מודל החקיקה יש להבחין בין שני סוגים של חקיקה: חקיקה סגורה וחקיקה פתוחה, כפי שיבואר להלן.

3.2.1. חקיקה סגורה

מודל החקיקה הסגורה מותיר למעשה את כל מלאכת ההסדרה בידי המחוקק. על פי מודל זה, כל היבטיה של הסוגיה יידונו על ידי בית המחוקקים, והסדר מפורט וממצה ייקבע בחוק שעל פיו יפעלו בתי המשפט מיום כניסתו של החוק לתוקף ואילך.

יתרונותיו וחסרונותיו של מודל זה הינם "תמונת ראי" של יתרונותיו וחסרונותיו של מודל החקיקה

⁴¹ ראו ברק, חקיקה שיפוטית עמ' 50. עם זאת, מעיר ברק (שם, עמ' 52, הערה 148), ש"לא פעם נעשה דבר חקיקה – בעיקר אצל הרשות המבצעת – בלא התייעצות מוקדמת עם בעלי האינטרסים הרלוונטיים, ובלא שתינתן להם ההזדמנות להשמיע את דעתם".

⁴² ברק, חקיקה שיפוטית, עמ' 51.

⁴³ כהן וג'ברין, חשיפת זהותם.

⁴⁴ שם.

⁴⁵ ברק, חקיקה שיפוטית, עמ' 51; כהן וג'ברין, חשיפת זהותם.

⁴⁶ ברק, חקיקה שיפוטית, עמ' 51.

⁴⁷ כהן וג'ברין, חשיפת זהותם.

⁴⁸ שם.

⁴⁹ ברק, חקיקה שיפוטית, עמ' 66.



השיפוטית. מודל החקיקה הסגורה מקדם ודאות משפטית, מגן על ציפיותיהם הסבירות של הצדדים, מאפשר לכוון מראש את התנהגות האזרח ומשקף בצורה נאמנה את ערכיה של החברה, בהיותו תוצר של הליך דמוקרטי שבו שותפים כל נבחרים הציבור.⁵⁰

מנגד, כאמור לעיל, בשל קוצר ידו של המחוקק והעדר יכולת לצפות מראש את מכלול המצבים ושינויי הטכנולוגיה שידרשו הסדרה, החלתו של מודל זה על סוגיית חשיפתם של מעוולים אנונימיים ברשת האינטרנט עלולה ליצור הסדרים חלקיים או פגומים. בשל אופיו של הליך החקיקה, שינויי חקיקה בעקבות מידע חדש העולה מן המחקר או משינויי טכנולוגיה אינם דבר של מה בכך, ובשל כך, הדבר עלול להביא להיקבעותו של הסדר שאינו נותן מענה ראוי לנושא.

3.2.2. חקיקה פתוחה

חקיקה פתוחה הינה חקיקה הקובעת אמת מידה כללית (סטנדרט) לחשיפת זהותו של המעוול, מבלי לקבוע באופן מפורט את מכלול השיקולים ומבחני העזר אשר ישמשו את בית המשפט בבואו להכריע בסכסוך מסוים. חקיקה שכזו מותירה את "עיקר העבודה" לבתי המשפט,⁵¹ אך משדרת מסר חברתי שלפיו האנונימיות של המשתמש ברשת לא תשמש לו כעיר מקלט מפני תביעה אזרחית.

מודל זה מכיר בכוחו של בית המשפט לקיים הליך לחשיפת זהותו של מעוול אנונימי, יתרונותיו הם יתרונותיה של החקיקה השיפוטית, וחסרונותיה הם חסרונותיו, באשר הוא מותיר את ההכרעה הערכית בסוגיה זו בידי בית המשפט.⁵²

3.2.3. הסדרה עצמית

מודל ההסדרה העצמית מבקש להותיר במידה רבה את הכללים הנוגעים לחשיפת זהותם של גולשים אנונימיים בידי "קהילה הוירטואלית".

על אף שחסידי ההסדרה העצמית נוהגים להצדיק הסדרה שכזו בנימוקים תועלתניים, יש הסוברים שביסודה של ההסדרה העצמית מונחת תפיסת עולם שנדונה לעיל, ולפיה, קהילה הוירטואלית איננה חופפת את קהילה הממשית.⁵³ זוהי קהילה שלה מערכת ערכים משל עצמה, ובהתאם לכך, מן הראוי שיהיה לה משפט משל עצמה.⁵⁴ החברים בקהילה הוירטואלית, לפי תפיסה זו, עשויים אמנם להיות גם שותפים בקהילות ממשיות, אך ערכיהם כחברים בקהילה הוירטואלית אינם בהכרח חופפים את ערכיהם כחברים בקהילה הממשית.

לפיכך, הסדרה מדינתית, בהתאם לתפיסה זו אינה מתאימה לניהול קהילה הוירטואלית, ולו בשל כך שהסדרה שכזו מבקשת להשליט את ערכיה של קהילה אחת על קהילה אחרת, שאינה בהכרח מזדהה עם ערכים אלו.

באופן טבעי, אימוצה של תפיסה זו יכול להוביל לאימוצו של מודל שלפיו הסדרת הגלישה באינטרנט תימסר באופן בלעדי בידיה של קהילה הוירטואלית. מודל זה יכונה להלן בשם – "הסדרה עצמית מלאה".

⁵⁰ כהן וג'ברין, חשיפת זהותם.

⁵¹ ראו כהן וג'ברין, חשיפת זהותם.

⁵² שם.

⁵³ לעניין זה ראו בהרחבה, קרניאל וויסמונסקי, קהילה באינטרנט עמ' 281-284.

⁵⁴ ראו קרניאל וויסמונסקי, קהילה באינטרנט עמ' 282, ועמ' 284, הערה 88, המדגישים שתתכן תפיסה שלפיה האינטרנט מכונן קהילות רבות, ותפיסה שלפיה כל הגולשים נחשבים כקהילה וירטואלית אחת. לפי התפיסה הראשונה, כל קהילה תידרש לגבש לעצמה כללי התנהגות באינטרנט, בעוד שלפי התפיסה השנייה, לא יהיה מנוס מרגולציה עצמית בינלאומית על מנת להסדיר את הגלישה ברשת האינטרנט.



ואולם, ישנה גם תפיסה מרוככת יותר. לפי תפיסה זו, האינטרנט אינו יוצר קהילות השונות באופן מהותי מן הקהילות הממשיות, ולכן אין הצדקה לקיומה של מערכת ערכים ייחודית לאינטרנט.⁵⁵ יחד עם זאת, בשל שיקולים תועלתניים שיוצגו להלן, יש טעם בדרישה שהסדרת נהלי הגלישה באינטרנט תימסר בידיהם של ה"שחקנים" המרכזיים בזירת האינטרנט. בהתאם לתפיסה זו, למדינה תהיה מעורבות מינימאלית בהסדרת דין האינטרנט (שתכליתה לפקח על כך שההסדרה העצמית תשקף את ערכיה של החברה), בעוד שתוכנם של ההסדרים ופרטיהם ייקבעו בידי הגולשים, ספקי שירותי הגלישה ומנהלי האתרים. מודל זה יכונה להלן בשם – "הסדרה עצמית חלקית".

3.2.4. הסדרה עצמית מלאה

מודל ההסדרה העצמית מבקש להוציא את נושא ההסדרה מידי רשויות השלטון ולהעבירו לידיהם של מפעילי האתרים וספקי התשתית לרשת האינטרנט.⁵⁶ בהתאם למודל זה, כל הנושאים הכרוכים בהסרת תוכן, פיקוח, חשיפת מעוולים וכדומה, יוסדרו בכללים שייקבעו בידי הגולשים, ספקי השירות ומנהלי האתרים.

חסידי מודל זה עומדים על כך שהוא משקף את הערך הליבראלי של **הסכמת הנמשל לממשל** ואת הערך של **עצמאות הקהילה**,⁵⁷ ונראה כי ביסודה של השקפה זו עומדת התפיסה שלפיה המרחב הווירטואלי הינו מרחב עצמאי המנותק מן המרחב הממשי מבחינה פיזית, תרבותית ומשפטית,⁵⁸ ובשל כך, מן הראוי שיחולו עליו הסדרים עצמאיים שהינם פרי של הסכמת החברים בקהילה הווירטואלית.⁵⁹

בדומה למודל החקיקה השיפוטית, **מודל זה מאפשר גמישות וערנות לשינויים טכנולוגיים, חברתיים או כלכליים, שעשויים להשפיע על דמותו של ההסדר.** יתרון זה מועצם במודל ההסדרה העצמית לנוכח העובדה שההסדר נקבע על ידי אנשי מקצוע שערנותם לשינויים טכנולוגיים ולהשפעותיו של ההסדר על השימוש ברשת גבוהה מזו של השופטים.⁶⁰

בין אנשי האסכולה של כלכלה ומשפט יש הטוענים ש**מודל ההסדרה העצמית הינו המודל היעיל ביותר מבחינה כלכלית**, משום שכל הסדר שקובעת המדינה משפיע על מדינות אחרות. הסדר המשפיע על צדדים שלישיים, שלהם אין חלק בעיצובו, יוצר החצנה לא רצויה הפוגעת ברווחה המצרפית שניתן להפיק ממנו. לעומת זאת, הסדר שמבוסס על הסדרה עצמית מקטין את החצנה, משום שכל הקהילה הווירטואלית שותפה בעיצובו, ובכך מעצים את הרווחה המצרפית שניתן להפיק ממנו.⁶¹

ברמה הפוליטית, יש הטוענים ש"ההסדרה העצמית נמנעת מכשלים המאפיינים הליכי חקיקה במדינות דמוקרטיות כמו השפעות של קבוצות אינטרסים, פשרות פוליטיות וכדומה".⁶²

ואולם, בצידם של יתרונות אלה יש למודל ההסדרה העצמית חסרונות לא מבוטלים. ניתוח של הנזקים הצפויים לחברות המספקות שירותי גלישה אל מול התועלת שעשויה לצמוח להן כתוצאה מחשיפת

⁵⁵ ראו קרניאל וויסמונסקי, קהילה באינטרנט עמ' 282.

⁵⁶ להגדרה מפורטת של מודל זה ואופיו, ראו מיכאל בירנהק, [הסדרה עצמית, מסמך עקרוני](#). (להלן: בירנהק, הסדרה עצמית).

⁵⁷ ראו רפעת עזאם, "על הצעת חוק מסחר אלקטרוני ומודל ההתאמה האינטגרטיבי להסדרתו ולמיסויו של המסחר האלקטרוני" משפט ועסקים יג, התש"ע (ספטמבר 2010) 191, עמ' 217-219 להלן: עזאם, מסחר אלקטרוני.

⁵⁸ ראו לעיל, אחר הציון להערה 7

⁵⁹ עזאם, מסחר אלקטרוני, שם.

⁶⁰ ראו עזאם, מסחר אלקטרוני, עמ' 217; בירנהק, הסדרה עצמית, פרק א, סעיף 7, ופרק ב סעיף 4.

⁶¹ ראו בהרחבה, עזאם, מסחר אלקטרוני, עמ' 221-223; בירנהק, הסדרה עצמית, פרק א, סעיף 6.

⁶² ראו בירנהק, הסדרה עצמית, שם.



זהותו של גולש מעוול מגלה, ש"העלות הכרוכה במסירת פרטים מזהים אודות המשתמשים עולה על התועלת הצומחת להן מכך",⁶³ ובשל כך, בהיעדר תמריץ לחשיפת פרטי המעוול, קשה להניח שספקי השירות ייצאו מגדרם (בלשון המעטה) כדי לסייע לנפגע לתבוע את המעוול.

כמו כן, ההסדרה העצמית עלולה "להיות אמצעי כוח נוסף בידי גורמים חזקים במגזר הפעילות הרלוונטי לנסות ולכפות את עמדתם ואת האינטרסים שלהם, תוך התעלמות או רמיסה של אינטרסים וזכויות של המיעוט או של גורמים חלשים".⁶⁴

ולבסוף, מאחר שהאפקטיביות של ההסדרה העצמית מותנית בהסכמה מלאה של כל השחקנים,⁶⁵ קשה להעריך את הזמן שיידרש עד להשגת הסדרה מלאה של הנושא, ובזמן שיחלוף עד להסדרה המלאה, עלולים גולשים רבים להיפגע. לפיכך, גם אם מקבלים את כל הטיעונים בעד קיומה של הסדרה עצמית בנושא חשיפת זהותם של מעוולים אנונימיים, אין בכך כדי ליתר הסדרה ציבורית של הנושא, עד לגיבושה של הסדרה עצמית.⁶⁶

3.2.5. הסדרה עצמית חלקית

מודל ההסדרה העצמית החלקית מבקש להתגבר על היעדר התמריץ מצידם של "השחקנים" הרלוונטיים ליצור הסדרה עצמית באמצעות יצירת מנגנון סטטוטורי שייצור תמריץ שיניע אותם לייצר הסדרה שכזו.

כך למשל נהגו בארה"ב בנוגע להסדרת האכיפה של דיני זכויות היוצרים ברשת האינטרנט. במקום ליצור משטר של פיקוח ואכיפה בחוק, קבע המחוקק שספקי שירות אשר ייטלו חלק בפעולות אכיפה ומניעה של הפרת זכויות יוצרים ברשת האינטרנט יזכו ל"חוף מבטחים" (*Safe Harbor*) שיעניק להם חסינות מפני אחריות להפרת זכויות יוצרים ברשת.⁶⁷ מאחר שהספקים יבקשו להגיע אל חוף המבטחים, יש להניח שהם לא יתעצלו לנקוט אמצעי פיקוח ואכיפה אשר יובילום אל חוף זה.

חסרונו של מודל זה הוא, שהניסיון מלמד שלעיתים, על מנת להגיע אל חוף המבטחים יאמצו ספקי השירות הסדרים בלתי מידתיים, אשר יפגעו באינטרס הציבורי,⁶⁸ או שיימנעו מלפקח על התכנים העוברים דרכם, על מנת שלא ייתפסו כמעורבים במעשי העוולה, ולא תוטל עליהם אחריות למעשים אלו.⁶⁹

⁶³ כהן וג'ורין, חשיפת זהותם, עמ' 9.

⁶⁴ בירנהק, הסדרה עצמית, פרק ג, סעיף 2; בהקשר זה ראוי להביא גם את דעתה של ד"ר קרן ברזילי-נהון, שחקרה את הנושא ומצאה ש"הסדרה עצמית מקדמת לרוב את קולו של הרוב, לא את קול המיעוט". ראו קרן ברזילי נהון, "מי שולט בקהילות וירטואליות?" פנים 30, 70-76.

⁶⁵ ראו בירנהק, הסדרה עצמית פרק ד, סעיפים 1, 2.

⁶⁶ דברים ברוח זו כותב גם כבי' השופט יצחק עמית בסעיף 52 לפסק דינו בבר"ע 850/06 (מחוזי חיפה) רמי מור נ' ידיעות אינטרנט מערכות אתר YNET.

⁶⁷ ראו ניבה אלקין-קורן, "הסדרה עצמית של זכויות יוצרים בעידן המידע" עלי משפט ב (תשס"ב) 319, בעמ' 322. מדיניות דומה אומצה אף בנוגע לאחריות ספקי השירות לתכנים פוגעניים המופצים ברשת. לעניין זה ראו אלקין-קורן, המתווכחים החדשים, עמ' 394.

⁶⁸ עו"ד חיים רביה מציין שמחקר שנערך לאחרונה באוניברסיטת ברקלי גילה שבארה"ב כ-30% מהדרישות להסרת תכנים אינן עומדות בדרישות החוק. בנוגע למנגנון דומה שהונהג בהולנד, מציג עו"ד רביה בדיקה שנעשתה על ידי אגודה הולנדית, שהעלתה לשרתי המחשב של עשרה ספקי שירותים הולנדים קטע ספרותי שנכתב על-ידי סופר בן המאה ה-19, שזכויות היוצרים בו פקעו מזמן. לאחר זמן מה פנתה האגודה בדרישה לעשרה ספקים להסיר את התוכן מפר זכויות היוצרים בטענה שהיא בעלת הזכויות ביצירה. לטענה זו לא היה כל שחר, עורך הדין שפעל לכאורה בשמה של האגודה לא היה ולא נברא, ובטקסט נאמר במפורש שהיצירה נכתבה ב-1871, והסופר נפטר בשנת 1877. למרות כל אלה, שבעה מבין עשרה הספקים מחקו את "היצירה המפרה". ראו חיים רביה, "בדיחה רעה" Law.co.il הפורטל המשפטי לאינטרנט, סייבר וטכנולוגיית מידע.

⁶⁹ "נראה כי ספקי שירות ייקחו על עצמם תפקידי פיקוח, וידאגו להסיר מיידית ובאופן עצמאי כל פרסום פוגעני, אם לא יחששו כי באם יפקחו, תוטל עליהם אחריות" – פרשת סבו, עמ' 26.



4. רקע נורמטיבי

בשנים האחרונות נעשו ניסיונות אחדים להסדיר את סוגיית חשיפת זהותו של מעוול אנונימי ברשת האינטרנט בדרך של חקיקה, ואולם עד כה, אף לא אחת מן ההצעות עברה את כל שלבי החקיקה. להלן נסקור את ההצעות המרכזיות בעניין זה. בהמשך, נסקור את פסיקות בתי המשפט בנושא.

4.1. חקיקה

עד היום, הוגשו מספר הצעות חוק להסדרת הנושא של חשיפת זהות מעוול ברשת האינטרנט, אך אף אחת מהן לא עברה את כל שלבי החקיקה.

4.1.1. הצעת חוק מסחר אלקטרוני, התשס"ח-2008

הצעת חוק מסחר אלקטרוני, התשס"ח-2008 (להלן: הצעת חוק מסחר אלקטרוני) הינה פרי עבודתה של ועדה בינמשרדית שבראשה עמדה עוה"ד טנה שפניץ, ואשר דנה בבעיות המשפטיות הכרוכות במסחר האלקטרוני, והגישה את המלצותיה בחודש מאי 2004 (להלן: ועדת שפניץ).⁷⁰

המודל שהוצע בהצעת חוק מסחר אלקטרוני להסדרת הטיפול בעוולות הנגרמות בידי גולש אנונימי מבוסס על שתי רגליים: חסינות מוגבלת לספק השירות, והסדרת הליך לחשיפת זהות המעוול לשם הגשת תביעה כנגדו.

בנוגע לחשיפת זהותו של גולש אנונימי נקבע ש"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)."⁷¹

בית המשפט יהיה רשאי להורות על חשיפת זהותו של המעוול, אם נוכח שקיים חשש ממשי שהמידע או התוכן שהופץ מהווה עוולה אזרחית או הפרה של זכות קניין רוחני.

על פי ההצעה, הסדרים מפורטים לעניין אופן הגשת הבקשה האמורה והליך בחינתה, ייקבעו על ידי השר הממונה.

ההצעה עברה בקריאה ראשונה בכנסת ה-17, אך לא הוחל עליה דין רציפות. במהלך כהונתה של הכנסת ה-18, הונחה הצעת חוק דומה על שולחן הכנסת, בחודש יולי 2011, אך הפעם לא כהצעת חוק ממשלתית אלא כהצעת חוק פרטית של חבר הכנסת מאיר שטרית, שפרטיה, בכל הנוגע לעניינו של מסמך זה, זהים לפרטי הצעת החוק הממשלתית.

הצעה זו לא עברה קריאה ראשונה, ולא הועברה עדיין לטיפול של ועדה מועדות הכנסת.

4.1.2. הצעת חוק איסור לשון הרע (תיקון – חשיפת פרטי מעוול), התש"ע-2010

הצעת חוק זו, שהונחה על שולחן הכנסת בידי חבר הכנסת זבולון אורלב, מתמקדת בחשיפת פרטי מי שהפיץ לשון הרע על הזולת ברשת האינטרנט. על פי ההצעה, מי שחש עצמו נפגע יוכל להביא לחשיפת

⁷⁰ הוועדה לבדיקת בעיות משפטיות הכרוכות במסחר אלקטרוני, דו"ח חלקי, ירושלים, אייר תשס"ד, מאי 2004.
⁷¹ סעיף 13(א).



זהותו של המעוול באמצעות פניה לבית המשפט כדי שיורה לספק האינטרנט לחשוף את זהותו של המעוול. בנוגע למבחני הסף לחשיפת פרטי המעוול, נקבע בהצעת החוק שדי בכך ש"קיים חשש של ממש שתוכנו של המידע שהופץ מכיל לשון הרע".

נקודה נוספת שמן הראוי לתת אליה את הדעת היא, שלפי ההצעה, שיקול דעתו של בית המשפט מוגבל ביותר. משעה שהוכח קיומו של חשש ממשי לכך שתוכנו של המידע שהופץ מכיל לשון הרע, נדרש בית המשפט להורות על חשיפת פרטי המעוול, והוא רשאי לחמוק מחובה זו רק "מטעמים מיוחדים שיירשמו".

בנייר עמדה שהוגש לוועדה מטעם איגוד האינטרנט הישראלי,⁷² הובעה הסתייגות מהתמקדות בעולה אחת בלבד, ומאי הסדרתו של הליך המאפשר למפיץ המידע להתגונן בפני הבקשה לחשוף את זהותו.

הצעה זו עברה קריאה ראשונה, ובימים אלה דנה בה וועדת המדע של הכנסת, לשם הכנתה לקריאה שנייה ושלישית.

4.1.3. תזכיר הצעת חוק חשיפת פרטי מידע של משתמש ברשת תקשורת אלקטרונית, התשע"א-2011

בין המלצותיה של ועדת שפניץ הייתה גם ההמלצה להסדיר בחוק את נושא ההליך המשפטי הראוי לשם חשיפת זהותו של מעוול אנונימי ברשת האינטרנט.

המלצה זו קיבלה משנה תוקף לאחר פסיקת בית המשפט העליון בפרשת מור, בה נקבע שבהעדר מסגרת דיונית הקבועה בחוק לשם פנייה לחשוף את פרטי המעוול, אין בית המשפט מוסמך לעסוק בפנייה מסוג זה.⁷³ בהתאם לכך הוכן במשרד המשפטים והופץ תזכיר להצעת חוק חשיפת פרטי מידע של משתמש ברשת תקשורת אלקטרונית, התשע"א-2011,⁷⁴ העוסק בכל העוולות או ההפרות של זכויות.

עיקרו של ההסדר הוא ביצירת שני מסלולים לחשיפת זהותו של המעוול. **מסלול אחד הוא מהיר, ולא דורש קיום הליכים בבית המשפט, אך מאידך גיסא, אין הוא מאפשר זיהוי ממשי של המעוול, אלא רק לקבל עליו "נתון מזהה", שהוא "נתון טכנולוגי שהינו חלק מפרוטוקול התקשורת בין מחשבים, המסייע לאיתור של מחשב או רשת מחשבים שמהם הועלה תוכן לרשת תקשורת אלקטרונית".** על פי ההצעה, **אם "פנה מבקש לספק השירות שבאמצעותו הועלה או הופץ התוכן האמור לשם קבלת הנתון המזהה במועד הפצת התוכן האמור, ימסור לו הספק את הנתון המזהה, ככל שהוא מצוי ברשותו".**

לעומת זאת, **אם מבקש אדם לקבל "פרטי מידע", כגון שמו המלא של הפוגע, מענו, מספר תעודת הזהות שלו, שם חברה ומספר הרישום של חברה, עליו "לפנות לבית המשפט בבקשה שיורה לספק השירות לחשוף את פרטי המידע של המנוי", והמנוי יוכל להתנגד לבקשה זו.** בית המשפט יכריע בבקשה, בהתחשב בשלושה גורמים:

- א. **תום לב** – על בית המשפט להשתכנע שהבקשה הוגשה "כדי לאפשר למבקש להגיש תביעה";
- ב. **עילה לכאורה** – על בית המשפט להשתכנע ש"קיים חשש ממשי, בהתבסס על ראיות לכאורה שהציג המבקש, שהתוכן שלגביו הוגשה הבקשה מהווה עוולה כלפי המבקש או הפרת זכות

⁷² לבנייר העמדה, ראו [כאן](#).

⁷³ פרשת רמי מור עסקה כאמור בעולת לשון הרע, אך הלכה זו אושרה מאוחר יותר גם בפרשת גוגל, בנוגע להפרת זכות הקניין הרוחני. ראו: ע"א 1622/09 **גוגל ישראל בע"מ נ' חברת ברוקרטוב** (1.7.2010, פורסם ב"נבו").

⁷⁴ לנוסח התזכיר ודברי ההסבר ראו [כאן](#).



קניין רוחני שלו";

ג. **סיכויי התביעה** – על בית המשפט להשתכנע שקיימים סיכויים שהתביעה תוכרע לטובת המבקש.

איגוד האינטרנט הישראלי הגיב למסלול המהיר המוצע בתזכיר לחשיפת "נתון מזהה"⁷⁵, בטענה שלאור ההתפתחות הטכנולוגית, לעיתים חשיפתו של נתון מזהה יכולה להוביל לזיהוי ממשי של מי שהעלה את המידע שבשלו הוגשה הבקשה. בהתאם לעמדה זו, מציע האיגוד שאף ההליך לחשיפת "נתון מזהה" יהיה כפוף לשיקול דעת שיפוטי.⁷⁶

4.2. פסיקות בתי המשפט

בהעדר הסדר בחוק, פנו נפגעים רבים אל בתי המשפט בישראל על מנת שיוורו לספקי תשתיות האינטרנט לחשוף את פרטיהם של גולשים שלטענתם עוולו כלפיהם. בהקשר זה התפתחו בפסיקה הישראלית שלוש גישות, כדלהלן.

הגישה המחמירה ביותר היא זו שנקבעה בפרשת בזק,⁷⁷ ולפיה, **על מנת שייעתר בית המשפט לבקשה לחשוף את זהותו של גולש אנונימי, יש להוכיח קיומו של חשש ממשי לכך שהפרסום מגיע לרף הפלילי הדרוש לשם הרשעה בעבירה של לשון הרע**. רף זה מחייב הוכחת כוונה לפגוע, ורמת הוכחה שהיא מעבר לספק סביר, כמקובל בדין הפלילי.⁷⁸

גישה מקלה יותר נקבעה על ידי השופט עמית בדיון בפרשת מור, בבית המשפט המחוזי.⁷⁹ פרשה זו עסקה בבקשה של מטפל אלטרנטיבי בבעיות עור להורות לחברת ברק אי.טי.סי, ספקית גישה לאינטרנט, לחשוף את זהותו של מי שלטענת המבקש, הפיץ עליו לשון הרע בפורום אינטרנטי. בדיון בבקשה בבית משפט השלום נדחתה הבקשה, ובבקשת רשות הערעור לבית המשפט המחוזי בחיפה, קבע השופט עמית שדרישה זו בדין יסודה, והתווה לעניין זה אמות-מידה מנחות, אך "החליט... לייחס לפסיקתו תוקף פרוספקטיבי ולא להחילה על עניינו של המבקש".

השופט עמית קבע, **שכדי שתיחשף כתובתו של גולש יש להראות, בראש ובראשונה, כי למבקש הייתה עומדת זכות תביעה כנגד המפרסם לו זהותו הייתה ידועה לו, אולם לגישתו יש להוסיף "דבר מה נוסף"**, כדי להתמודד עם החשש מ"אפקט מצנן" שעלול לנבוע מחשיפת זהותו של הגולש.

כמו כן, השופט עמית הציע כמה **מבחנים לקיומו של אותו "דבר מה נוסף"**, כדלהלן: **מידת תום הלב של המבקש; סיכויי תביעה טובים** (האם הביטוי הפוגע חרג מגדר הבעת דעה מותרת ועשוי להוות לשון הרע?); **זהות הנפגע** (אדם פרטי או דמות ציבורית); **עוצמת הביטוי הפוגע; משך הפרסום; טיב האתר בו**

⁷⁵ ראו כאן.

⁷⁶ לא למותר לציין בהקשר זה, שהשאלה, האם כתובת IP נחשבת מידע אישי שנויה במחלוקת, והיא נושא לדיון ער ברמה הבינלאומית. כך למשל, בית המשפט בגרמניה פסק שכתובת IP אינה בגדר "מידע אישי" (ראו דיווח, כאן), וכך פסק גם בית המשפט בצרפת (ראו דיווח, כאן). מנגד, בית המשפט האירופי לצדק פסק שכתובת IP נחשבת כ"מידע אישי" לכל דבר ועניין (ראו דיווח, כאן). למחקר תמציתי של העמדה המקובלת במדינות שונות באיחוד האירופי בשאלה זו, ראו כאן.

⁷⁷ בש"א 4995/05 פלונית נ' בזק בינלאומי בע"מ, (פורסם בנבו, 28.2.06). לדיון בגישה זו, ראו בירנהק, חשיפת גולשים, עמ' 74-75.

⁷⁸ בגישה זו הלכו גם ההחלטות שניתנו בבש"א (חי') 5478/06 ק.א.ס.פי מחשבים בע"מ נ' ברק אי.טי.סי. (1995) החברה לשירותי בזק בינלאומיים בע"מ (פורסם בנבו, 13.8.06); בש"א (חי') 1238/07 מור נ' ברק 013 שירותי אינטרנט בע"מ (פורסם בנבו, 12.2.07), וכן פסק הדין של השופטת גונן בפרשת סבו. וראו גם, ת"א (תי"א) 61825/07, בש"א 178590/07 מנסור נ' חלבי, (פורסם בנבו, 14.1.08); ת"א (תי"א) 14303/08, בש"א 152863/08 "רבקה פלח-חנות בייבי פלוס" נ' דוקטורס-אתר אינטרנט, (פורסם בנבו, 12.2.08); ת"א (ראשלי"צ) 4470/07 ברלומנפלד נ' GOOGLE INC (פורסם בנבו, 25.11.07).

⁷⁹ בר"ע 850/06, 1632/07 מור נ' ידיעות אינטרנט מערכות אתר YNET-מערכת הפורומים, (פורסם בנבו, 22.4.07).



פורסם הביטוי הפוגע; המשקל שקורא סביר ייתן לפרסום הפוגע; התועלת שתצמח מחשיפת פרטי הגולש לעומת הנזק שעלול להיגרם מהחשיפה.

בצידם של מבחנים אלו, הציע השופט עמית מספר תנאים מקדמיים לכך שבית המשפט יורה על חשיפת זהות גולש, ובין היתר: **על המבקש לנקוט צעדים מטעמו לחשיפת זהותו של אותו אנונימי**, ולכל הפחות קריאה באותו פורום או אתר לגולש להזדהות בשמו תוך ציון העובדה שהמבקש עומד להגיש בקשה לעניין זה; **צירוף טיוטת כתב תביעה בעילה הנטענת**, כדי להוכיח את תום ליבו בבקשת הגילוי.

הגישה המקלה ביותר אומצה על ידי כב' השופטת פלפל בפרשת מזמור.⁸⁰ גישה זו נסמכת על נוסח הצעת חוק מסחר אלקטרוני, שהיא "ליברלית יותר מהפסיקה הקיימת עד היום", ותכליתה "לגרום לכך שהשיח הציבורי יהיה ענייני, תכליתי, בוטה אולי, אבל נקי ללא ביצוע עבירות או עוולות".

השופטת פלפל סבורה שבהצעה זו ביקש המחוקק לקבוע את "נקודת האיזון בין זרימת מידע חופשית לבין הגנה על הכבוד, הקניין הרוחני והפרטיות בס' 13(ב) להצעה", וזאת באמצעות קביעת אמת המידה של "חשש של ממש" לביצוע עוולה או פגיעה בקניין הרוחני.

"חשש של ממש" הוגדר על ידי השופטת פלפל כחשש ש"אינו בגדר הוודאות הקרובה, והוא גבוה יותר, מבחינה ראייתית, מהחשש הסביר". לפיכך, "בדיקת עילת התביעה צריכה לעבור את הסף של ה"חשש הסביר", אך אינה נדרשת לענות על קריטריונים מחמירים של רמת וודאות קרובה".

לפי גישה זו, **משעה שנוכח בית המשפט שקיים "חשש של ממש" לביצוע עוולה אזרחית, רשאי הוא להורות על חשיפת פרטי המעוול, ואין הוא כבול בקיומם של תנאים מקדמיים כלשהם**. מבחני ה"דבר מה נוסף" שהוצעו על ידי השופט עמית בפרשת מור, ייושמו לפי גישה זו במסגרת בחינת קיומה של "עילת תביעה לכאורה", אך **השופטת פלפל אינה מקבלת את מבחן תום הלב** שהוצע על ידו משום ש"גם אדם שאינו תם לב, זכאי שלא יפגעו בכבודו, וזכאי להחליט בסופו של יום, מה הוא עושה עם המידע שהגיע לידי אודות שמו של הפוגע לכאורה".

בערעור על פסיקתו של כב' השופט עמית לבית המשפט העליון, דחה בית המשפט את הכרעתו של השופט עמית וקבע שבהעדר הסדר חוקי המאפשר את הדבר בצורה מפורשת, אין לבתי המשפט בישראל סמכות להורות לספקי שירותי הגישה לחשוף את זהותו של מעוול.

5. סקירה משווה

5.1. משפט בינלאומי

סוגיית החשיפה של פרטי מעוול ברשת האינטרנט, על אף אופייה הגלובלי, טרם הוסדרה ברמה הבינלאומית,⁸¹ אם כי, הזכויות המתנגשות בכל הכרעה הנוגעת לסוגיה זו, מוכרות ומעוגנות בדן הבינלאומי.⁸²

⁸⁰ הפ (ת"א) 1244/07 **מזמור הפקות בע"מ נ' מעריב הוצאת מודיעין בע"מ (אתר האינטרנט NRG)**. וראו גם: ה"פ (ת"א) 250/08 **חברת ברוקר טוב בע"מ נ' חברת גוגל ישראל בע"מ** (פורסם בינוי, 7.1.09).

⁸¹ אם כי, "מתפתחת הכרה בינלאומית, שיש להגן על המרחב הקיברנטי לטובת הכלל ולהסדיר את הפעילות בו, בדומה להסדרת הפעילות במרחבים האחרים; וזאת באמצעות שיתוף פעולה בין מדינות, התאמת כללי הדין הבינלאומי וגיבוש אמנה בינלאומית מחייבת" (שמואל אבן ודוד סימן טוב, "**לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**"), המכון למחקרי ביטחון לאומי, מזכר, יוני 2011, עמ' 8).

⁸² ראו למשל, הסעיפים הבאים מן ההכרזה לכל באי עולם בדבר זכויות האדם: סעיף 12 (הזכות לפרטיות, כבוד ושם טוב); סעיף 17 (זכות הקניין); סעיף 19 (חופש הדעה והביטוי); סעיף 8 (הזכות לסעד מבית המשפט בשל הפרה של זכויות האדם). כמו כן ראו: מגילת זכויות



בשנת 2008 התבקש בית המשפט האירופי לזכויות אדם לחוות דעתו באשר לזכותם של בתי המשפט במדינות האיחוד האירופי, להורות לספקי שירותי הגישה לחשוף את פרטיהם של מפרי זכויות קניין רוחני ברשת האינטרנט (להלן: פרשת טלפוניקה).⁸³

פסק הדין עוסק בבקשה של חברת תקליטים ספרדית מבית המשפט בספרד, להורות לחברה שהיא ספקית שירותי גישה לאינטרנט בספרד לחשוף את זהותם של מפירי זכויות יוצרים שהורידו יצירות מוסיקליות באמצעות התוכנה לשיתוף קבצים KaZaA. ספקית שירותי הגישה, חברת Telefónica, טענה בפני בית המשפט שבהתאם לחוק בספרד, חשיפת זהותם של משתמשים ברשת האינטרנט מותרת רק לשם חקירה משטרתית, הגנה על שלום הציבור, שמירה על הביטחון הלאומי וכדומה, אך לא לשם הגנה על אינטרס אזרחי בלבד. בית המשפט הספרדי נתן את הצו המבוקש, אך בערעור על פסק דין זה הוקפא הדיון ונשלחה בקשה לפסק דין הצהרתי מאת בית המשפט של האיחוד האירופי בשאלה, האם משפט האיחוד מאפשר את חשיפת זהותם של מפירי זכויות קניין, ואם כן, באלו תנאים.

בפסיקה זו נסקרו מספר מסמכים בינלאומיים, ובהם: אמנה בינלאומית ודירקטיבות של הפרלמנט האירופי שיש להם נגיעה ישירה לנושא שבנדון, והם יוצגו להלן.⁸⁴

בית המשפט האירופאי הכריע שאין במקורות האמורים כדי לחייב את המדינות החברות לאמץ הסדרים שיאפשרו לבתי המשפט להורות לספקי הגישה לחשוף את זהות המעוול, אולם הם מאפשרים למדינות החברות לאמץ הסדרים שכאלו, והסדרים אלו אף עולים בקנה אחד עם העקרונות העולים מהם.

5.1.1. אמנת T.R.I.P.S.

אמנת T.R.I.P.S (*Agreement on Trade-Related Aspects of Intellectual Property Rights*) הינה אחת מן האמנות שנחתמו בידי מדינות מפותחות רבות, וישראל בכללן, עם הקמתו של ארגון הסחר העולמי, בשנת 1994.

האמנה מתמקדת בהגנה על הקניין הרוחני, ולעניינו של מסמך זה ניתן לציין את ההוראות הבאות של האמנה:

סעיף 41(1) לאמנה קובע שהמדינות החברות יבטיחו בחקיקה את קיומן של הפרוצדורות המפורטות בפרק השלישי של האמנה, שיאפשרו הגנה אפקטיבית נגד הפרה של זכויות קניין רוחני, כולל סעדים מיידיים לשם מניעת ההפרה וסעדים שנועדו לשם הרתעת מפריים.

סעיף 41(2) לאמנה קובע שעל הפרוצדורות האמורות להיות הוגנות וקלות ליישום.

סעיף 42 לאמנה קובע שעל המדינות החברות לאמנה לאפשר קיומן של פרוצדורות לקיום הליכים אזרחיים כנגד מפרי זכויות קניין רוחני.

היסוד של האיחוד האירופי (Charter of Fundamental Rights of The European Union, 2000/C 364/01), סעיפים 1 (ההגנה על כבוד האדם); 7 (ההגנה על הזכות לפרטיות); 8 (הגנת המידע האישי); 11 (ההגנה על חופש הביטוי); 17 (ההגנה על זכות הקניין והקניין הרוחני); 47 (תרופות שיש להעניק לאדם על הפרת הזכויות שנקבעו במגילה).

⁸³ [Productores de Música de España \(Promusic\) v. Telefónica de España SAU, C-275/06](#).

לדיון בפסק הדין ובמשמעויותיו, ראו:

Christopher Kuner, "[Data Protection and Rights Protection on the Internet: The Promusic Judgment of the European Court of Justice](#)", *European Intellectual Property Review*, Issue 5, 2008, pp. 199.

⁸⁴ ההצגה, לפי סדר הופעת המקורות בפסק הדין, ולא לפי הסדר הכרונולוגי.



סעיף 47 לאמנה קובע שהמדינות החברות יסמיכו את בתי המשפט להורות למפר זכויות הקניין להודיע לבעל הזכות את זהותו של צד שלישי שמעורב בייצוא או בהפצה של סחורה, בדרך של פגיעה בזכויות קניין רוחני.

הסעיף האמור אמנם אינו עוסק בספקי שירותי גישה לאינטרנט אלא באלו שהפרו בעצמם את זכויות הקניין הרוחני, באמצעות צד ג', אך בפרשת טלפוניקה, ציין בית המשפט האירופי לזכויות אדם את הסעיף הזה, כאחת מן ההוראות הבינלאומיות שעל בית המשפט להתחשב בהן בבואו להכריע בבקשה לחשיפת זהותו של מעוול שהפר זכויות קניין רוחני ברשת האינטרנט.

5.1.2. הדירקטיבה בעניין היבטים חוקיים של קהילת המידע (DIRECTIVE 2000/31/EC)⁸⁵

הדירקטיבה בעניין היבטים חוקיים של קהילת המידע מתמקדת באחריות ספקי השירות לתוכן שמועלה לאתרים על ידי הגולשים.

הדירקטיבה אוסרת על המדינות החברות להטיל חובה כללית על ספקי השירות לפקח על המידע העובר דרכם או על המידע המאוחסן באתרים, או לחפש מידע שיגלה פעילות בלתי חוקית.⁸⁶ יחד עם זאת, הדירקטיבה מאפשרת למדינות להטיל על ספקי השירות את החובה ליידיע את הרשויות המוסמכות על פעילות בלתי חוקית הידועה להם, או להעביר לרשויות המתאימות, לפי בקשתן, מידע שיאפשר את זיהוי לקוחותיהם.⁸⁷

כמו כן, הדירקטיבה קובעת שעל המדינות החברות להבטיח את זמינותו של הליך משפטי על פי חוק המדינה, שיאפשר אימוץ מהיר של אמצעים שנועדו להילחם בהפרה של זכויות או למנוע פגיעה בזכויות.⁸⁸

ואולם, בית המשפט האירופי לזכויות אדם קבע שאין בהוראות האמורות, לפי נוסחן, כדי לחייב את המדינות לאמץ חקיקה המחייבת ספקי שירותי גישה לאינטרנט לחשוף את זהותו של מעוול אשר הפר זכויות קניין רוחני.⁸⁹

5.1.3. הדירקטיבה לאיחוד היבטים של זכויות יוצרים בקהילת המידע (DIRECTIVE 2001/29/EC)⁹⁰

דירקטיבה זו עוסקת בחובת המדינות החברות לנקוט באמצעים משפטיים כדי להגן על זכויות קניין רוחני.

סעיף 8 של הדירקטיבה קובע שעל המדינות לקבוע סנקציות ותרופות יעילות ומידתיות כנגד הפרות של זכויות קניין רוחני, שעליהן לאפשר למחזיק בזכויות היוצרים לתבוע את אכיפתן של סנקציות או תרופות אלה, וכן, לתבוע כל גוף שצד שלישי עושה שימוש בשירותיו לשם הפרה של זכויות קניין רוחני.

בית המשפט האירופאי פסק, שאין בהוראותיה של דירקטיבה זו כדי לחייב את המדינות לחוקק חוקים אשר יאפשרו לבתי המשפט להורות לספקי שירותי הגישה לאינטרנט לחשוף את זהותם של מעוולים.⁹¹

⁸⁵ [DIRECTIVE 2000/31/EC](#) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

⁸⁶ סעיף 15(1).

⁸⁷ סעיף 15(2).

⁸⁸ סעיף 18.

⁸⁹ פרשת טלפוניקה, סעיף 59 לפסק הדין.

⁹⁰ [DIRECTIVE 2001/29/EC](#) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

⁹¹ פרשת טלפוניקה, סעיף 59 לפסק הדין.



5.1.4. הדיקטיבה בעניין אכיפת זכויות קניין רוחני (DIRECTIVE 2004/48/EC) 92

דיקטיבה זו עוסקת באמצעים הדרושים לשם אכיפת זכויות קניין רוחני. סעיף 3(1) של הדיקטיבה קובע שעל המדינות החברות לספק אמצעים, הליכים ותרופות לשם ההגנה על זכויות קניין רוחני, וכי על אמצעים אלו להיות זמינים, פשוטים וללא כל מגבלות זמן שעלולות להכשיל את יישומם של האמצעים האמורים.

סעיף 8(1) של הדיקטיבה קובע, שעל המדינות החברות להבטיח שבמסגרת ההליכים להגנה על הזכויות האמורות, בתי המשפט יוכלו להורות על מסירת מידע בדבר מקורות ההפרה או ההפצה של חומר הפוגע בזכויות קניין רוחני על ידי מפר הזכויות או על ידי אדם או גוף אחר השולט בחומר הפוגע ברמה מסחרית, עושה שימוש בשירותים המפרים את הזכויות באופן מסחרי, מעניק שירות שמסייע לפעילות המפרה את זכויות הקניין הרוחני, ברמה מסחרית. כמו כן, הדיקטיבה מאפשרת לדרוש מידע גם מאדם אחר, שצוין על ידי אדם או גוף כאמור, כמי שהיה מעורב בייצור או הפצה של חומר שיש בו הפרה של זכויות קניין רוחני.

כדי להסיר ספק, מובהר בסעיף 8(2) שהמידע יכיל, בהתאם לצורך, פרטים אודות השמות והכתובות של מפרי זכויות הקניין הרוחני. ואולם, גם הוראות אלו לא פורשו על ידי בית המשפט האירופאי לזכויות אדם כמחייבות את המדינות לקבוע בחקיקה את חובתם של ספקי שירותי גישה לאינטרנט לחשוף את זהותו של גולש שהפר זכויות קניין רוחני.⁹³

5.1.5. הדיקטיבה בעניין שמירת המידע (Directive 95/46/EC)⁹⁴

הדיקטיבה בעניין שמירת המידע עוסקת בהגנה על המידע האישי, המוגדר בסעיף 2 לדיקטיבה כ**מידע שיכול להוביל לזיהויו של אדם**. הדיקטיבה אוסרת עיבוד של מידע אישי (*processing of personal data*), ובכלל זה גם **חשיפה של המידע באמצעות העברתו (disclosure by transmission)** ומאפשרת העברה של מידע בנסיבות חריגות, שאינן נוגעות למסמך זה.⁹⁵

סעיף 13 של הדיקטיבה קובע שהמדינות החברות רשאיות לאמץ חקיקה המגבילה את היקף החובות והזכויות שנקבעו בדיקטיבה, כאשר ההגבלה היא מידתית ונחוצה לשם שמירת הביטחון הלאומי, שלום הציבור, מלחמה בפשיעה או בהפרות של כללי אתיקה מקצועית, הגנה על עניין כלכלי חשוב של המדינות החברות **ולשם הגנה על זכויותיו של נושא המידע או של אחרים**.

בית המשפט קבע, שסעיף זה מכשיר חקיקה המגבילה את חובת המחזיק במידע לשמור על סודיות המידע, כאשר המידע נחוץ לשם הגנה על זכויות קניין רוחני.⁹⁶

5.1.6. הדיקטיבה בעניין הפרטיות והתקשורת האלקטרונית (Directive 2002/58/EC)⁹⁷

גם הדיקטיבה בעניין הפרטיות והתקשורת האלקטרונית עוסקת בהגנה על המידע האישי, אך בניגוד

⁹² [Directive 2004/48/EC](#) of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

⁹³ שם, סעיף 70 לפסק הדין.

⁹⁴ of the European Parliament and of the Council of 24 October 1995 on the protection of [Directive 95/46/EC](#) individuals with regard to the processing of personal data and on the free movement of such data.

⁹⁵ ראו סעיפים 7, 8(2)(c).

⁹⁶ שם, סעיף 53 לפסק הדין.

⁹⁷ [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector



לקודמתה היא מתמקדת בהגנה על פרטיות המידע בסביבה הדיגיטאלית.

סעיף 5 של הדירקטיבה מחייב את המדינות החברות להבטיח את סודיות התקשורת והעברת המידע ברשתות התקשורת באמצעות חקיקה מדינתית.

יחד עם זאת, סעיף 15 של הדירקטיבה קובע, שהמדינות החברות רשאיות לאמץ בחקיקה אמצעים להגבלת היקף החובות והזכויות לפי הדירקטיבה, כאשר הגבלות אלו נחוצות במידה הראויה לחברה דמוקרטית. זאת, כדי להגן על הביטחון הלאומי, שלום הציבור ומלחמה בפשיעה או למנוע שימוש אסור ברשת התקשורת האלקטרונית, בהתאם להוראה שבסעיף 13 לעיל של הדירקטיבה בעניין שמירת המידע.

סעיף 6 קובע שיש לעשות במידע המצוי בחזקת ספקי שירות שימוש אך ורק למטרה שלשמה הועבר המידע ובידי האנשים שהוסמכו לכך על ידי ספקי השירות, ויש למחוק מידע זה או להפכו לאנונימי כאשר אין עוד צורך בו, אך הוראה זו בוטלה למעשה בדירקטיבה מאוחרת של האיחוד משנת 2006⁹⁸ בית המשפט האירופי קבע, שההפניה לסעיף 13 של הדירקטיבה בעניין שמירת המידע שהוזכרה לעיל מאפשרת למדינות לחוקק חוקים המגבילים את סודיות המידע כדי להגן על אינטרסים אזרחיים שאינם ציבוריים, אך לפי נוסח הסעיף אין המדינות מחויבות לעשות כן.

5.2. ארה"ב

בתי המשפט בארה"ב קבעו לא אחת, שהתיקון הראשון לחוקת ארה"ב (חופש הביטוי) מגן אף על הביטוי האנונימי,⁹⁹ וכי הגנה זו נפרשת גם על ביטוי ברשת האינטרנט.¹⁰⁰ בשנת 1997, בית המשפט העליון במדינת ג'ורג'יה אף ביטל חוק של המדינה, שאסר התקשורת אנונימית דרך האינטרנט.¹⁰¹ יחד עם זאת, בתי המשפט קבעו שחופש הביטוי האנונימי אינו מוחלט, ואין הוא מעניק הגנה לביטוי פוגעני.¹⁰² החקיקה הפדראלית יוצרת למעשה הבחנה בין חשיפת פרטי מעוול, כאשר העוולה היא עבירת של לשון הרע, לבין חשיפת פרטי מעוול כאשר העוולה היא פגיעה בקניין רוחני, כפי שיבואר להלן.

5.2.1. חשיפת פרטי מפרסם לשון הרע

בארה"ב קיים הסדר דיוני המאפשר לבית המשפט להורות בצו מיוחד (Subpoena) על הצגת מידע המצוי

⁹⁸ ראו סעיף 5 של הדירקטיבה בעניין שמירת המידע, המחייב את ספקי הגישה לשמור מידע אישי על מפרסם תוכן באינטרנט, למשך תקופה של שנה מיום הפרסום. לנוסח האנגלי של הדירקטיבה, ראו: DIRECTIVE 2006/24/EC Of The European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

⁹⁹ *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 ("an author's decision to remain anonymous... is an aspect of the freedom of speech protected by the First Amendment")
¹⁰⁰ M. Froomkin, "Anonymity and the Law" לסקירה רחבה יותר בעניין זה ראו: *Reno v. ACLU*, 521 U.S. at 870. University of Miami Legal Studies Research Paper No 2008-42 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1309225 (last accessed 21 Jan 2010).

¹⁰¹ *ACLU of Georgia v Miller*, [1997] 977 F Supp 1228 (ND GA) ואולם, יש להעיר שחלק מן המלומדים בארה"ב סברו שהחוק לא עמד במבחן החוקתי משום ניסוחו הכוללני, אך אם הניסוח היה מכוון רק לשם מניעת שימוש לרעה באנונימיות שמקנה הרשת, הוא היה עומד במבחן זה. ראו למשל: D. Karl, "State Regulation of Anonymous Internet Use after *ACLU of Georgia v Miller*" (1998) 30 *Arizona State Law Journal* 513-540; P Weston, "III First Amendment: 2 Internet Crime Statutes: b) Fraud: American Civil Liberties Union of George v Miller" (1999) 14 *Berkeley Technology Law Journal* 403-418.

¹⁰² See *Mobilisa, Inc. v. Doe*, 170 P.3d 712, 717 (Ariz. Ct. App. 2007). *Mobilisa* פרשת: להלן.



ברשותו של אדם או בשליטתו, לשם חשיפת מידע הנוגע לזהותו של מעוול. הוראות פרטניות לגבי צו זה נקבעו בכללי סדר הדין האזרחי הפדראליים.¹⁰³ על פי כללים אלה, כאשר הנמען לצו מתנגד לו, מופנים הצדדים לבית המשפט לשם קיום הליך שיכריע האם מן הראוי לבטל את הצו או שמא יש לכבדו.¹⁰⁴ מכוחו של הסדר דיוני זה, הוגשו לבתי המשפט עתירות רבות שנועדו לחשוף את זהותם של גולשים אנונימיים ברשת האינטרנט, ובפסיקה גובשו מבחנים שונים לנכונותו של בית המשפט להיעתר לעתירות מסוג זה, כדלהלן¹⁰⁵:

מבחן תום הלב

מבחן תום הלב, שנקבע על ידי בית המשפט בוירג'יניה בפרשת AOL¹⁰⁶ מבוסס על שלושה מבחני עזר.¹⁰⁷ הראשון שבהם הוא המבחן הראייתי, לפיו, על התובע לשכנע את בית המשפט בקיומה של עילת תביעה.¹⁰⁸ השני שבהם הוא, מבחן תום הלב, לפיו, על התובע לשכנע את בית המשפט שיש לו יסוד לגיטימי לטעון בתום לב שהוא הקרבן של ההתנהגות שבגינה הוגשה התביעה,¹⁰⁹ והאחרון הוא מבחן הצורך, לפיו על התובע לשכנע את בית המשפט שחשיפת זהותו של הפוגע הכרחית לשם קידום התביעה.¹¹⁰

החיסרון הבולט של מבחן תום הלב הוא בהעדרו של מנגנון שיכול להבטיח מניעת שימוש לרעה בזכות לחשוף את זהות הגולש האנונימי. ג'ונס¹¹¹ מצביע על כך שחברה המעוניינת להשתיק ביקורת לגיטימית, ולא לקבל פיצוי על נזק שנגרם, יכולה בקלות די רבה לצלוח את שלושת מבחני העזר האמורים, להביא לחשיפת המבקרים, ובדרך זו, להשתיק את הביקורת.¹¹²

מבחן ההליך המהיר

מבחן ההליך המהיר מבוסס על הליך ייחודי לסדר הדין המקובל בארה"ב, ולפיו, על מנת שבית המשפט ייעתר לבקשה לחשוף את זהותו של הגולש האנונימי, יש לייצע את הפוגע על הכוונה לפתוח בהליך לחשיפתו ולתת לו הזדמנות נאותה להתגונן בפני הליך זה, וכן להוכיח את קיומן של נסיבות המצדיקות קיומו של הליך

¹⁰³ Federal Rules of Civil Procedure, Rule 45.

¹⁰⁴ שם, סעיף (c)(2)(B) 45. יש לציין את קיומו של הסדר מקל יותר על החשיפה מצוי בחוק העוסק בספקי גישה לאינטרנט שהם חברה של תשתית כבלים. כאן נקבע שכעיקרון, ספק הגישה חייב לשמור על האנונימיות של הגולשים, זולת אם קיבל הוראה לחשוף את זהותם על ידי בית המשפט (47 U.S.C. §551(c)(2)(B)). אולם, הוראה זו נוגעת אך ורק לחשיפת זהותו של גולש שחשוד שהיה מעורב בפעילות פלילית (ראו שם, סעיף (h) 551).

¹⁰⁵ לשם השלמת התמונה יש להזכיר, שבחלק מן המדינות בארה"ב נקבעו כללי סדר דין מיוחדים, המאפשרים אף הם את חשיפת זהותו של מעוול אנונימי. ראו למשל, במדינת ניו יורק: New York Civil Procedure rule 3102(c). בית המשפט עשה שימוש בכלל זה כדי לחייב ספקיות אינטרנט לחשוף פרטי גולשים מעוולים. ראו: **Matter of Greenbaum v. Google, Inc.**, 845 N.Y.S. 2d 695 (Sup. Ct. 2007); **Matter of Ottinger v. Non-Party The Journal News**, 2008 N.Y. Misc. LEXIS 4579 (Sup. Ct. 2008); **Matter of Cohen v. Google Inc.**, 2009 N.Y. Misc. LEXIS 2302 (Sup. Ct. 2009).

¹⁰⁶ **America Online, Inc. v. Anonymous Publicly Traded Co.**, 261 Va. 350 (Va. 2001) at 37. ()

¹⁰⁷ See Jonathan D. Jones, Note, *Cybersmears and John Doe: How far Should First Amendment Protection of Anonymous Internet Speakers Extend?*, 7 **FIRST AMEND. L. REV.** 421 (2009), at pp. 425-426.

¹⁰⁸ שם.

¹⁰⁹ שם.

¹¹⁰ שם.

¹¹¹ Jones, Jonathan D., "Cybersmears and John Doe: How Far Should First Amendment Protection of Anonymous Speakers Extend?" 7 **First Amend. L. Rev.** 421, 426 (2008-2009). (להלן: ג'ונס, השמעות מקוונות).

¹¹² ביקורת נוספת שהושמעה בקרב מלומדים כנגד מבחן זה היא, שבהנחה שהמבחן נועד להוסיף הגנה על חופש הביטוי באינטרנט, הרי שלמעשה, הוא כמעט ולא מוסיף הגנה על הביטוי האנונימי. לעניין זה ראו:

Ryan M. Martin, "Comment and Casenote: Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits" 75 **U. Cin. L. Rev.** 1217 at 1240-1241.



מהיר בעניין.¹¹³ הליך מהיר מנוהל כאשר לא קיימת מחלוקת בין הצדדים על העובדות הנוגעות לדין, ואף לא קיימת מחלוקת בנוגע לדין שיש להחיל על העובדות (במידה ותיחשף זהותו של הפוגע).

גיוס מציין שלא כל בתי המשפט עושים שימוש במבחן זה.¹¹⁴ לדבריו, מבחן זה לא יכול להחליף את מבחן איזון הערכים משום שלעיתים יישומו עלול להוביל לחשיפת זהותו של גולש אנונימי גם בנסיבות שהפגיעה נעשתה בטעות, אגב ביטוי פוליטי, שלו מן הראוי להעניק הגנה גבוהה מאשר לביטוי שאיננו כזה.¹¹⁵ תוצאה זו עשויה להימנע לדברי גיוס, אם יעשה בית המשפט שימוש במבחן איזון הערכים, שיידון להלן.

מבחן איזון הערכים

מבחן איזון הערכים, שמקורו בפסיקת בית המשפט לערעורים במדינת ניו ג'רזי בפרשת *Dendrite*,¹¹⁶ נועד למעשה למצוא את הנוסחה שתעניק את המשקל הראוי לחופש הביטוי מחד גיסא, ולזכותו של אדם לשם טוב, מאידך גיסא.¹¹⁷ מבחן זה מורכב למעשה מארבעה שלבים, כדלהלן:

ראשית, על הנפגע לפעול כדי ליידע את הפוגע על כך שהוא עתיד להיחשף להליכים שתכליתם גלות את זהותו. היידוע חייב להתפרסם באותו מקום ובאותה הבלטה שבה התפרסמה הפגיעה, כדי להעניק לפוגע הזדמנות נאותה להתנגד לחשיפת זהותו.

שנית, על הנפגע להבהיר בדיוק מהו הביטוי שבשלו הוא מעוניין בחשיפת זהותו של הפוגע.

שלישית, על הנפגע לשכנע את בית המשפט בראיות לקיומה של עילה לכאורית לפעולה כנגד הפוגע האנונימי.

לבסוף, במידה והצליח הנפגע לעבור את שלוש המשוכות הקודמות, **על בית המשפט לאזן בין חופש הביטוי האנונימי לזכותו של הנפגע לקבל פיצוי על הפגיעה בו.**

מבחן ארבע-שלבי זה אומץ גם על ידי בית המשפט לערעורים במדינת מרילנד בפרשת *Brodie*,¹¹⁸ ששכלל במידת מה את המבחן הראשון בקובעו שיש להעניק לפוגע זמן סביר כדי להגיב לאזהרה שפרסם הנפגע.

בפרשת *Mobilisa*,¹¹⁹ בית המשפט הבהיר שמבחן איזון הערכים יתחשב בין השאר בסוג הביטוי הפוגע, בצפייתו של הפוגע לפרטיות ובהשלכות הצפויות שיהיו לחשיפת זהותו של הפוגע, על הפוגע עצמו ועל גולשים אחרים במצבו.

בפרשת *Anonymous*¹²⁰ נקבע בפסק דין תקדימי, שהמבחנים המחמירים שנקבעו בפסיקת בתי המשפט בפרשות *Dendrite* ו-*Cahill* ייושמו בבקשות לחשיפת זהות מעוול שהביטוי שבגיניו נדרשת החשיפה הינו פוליטי במהותו, ולא על חשיפת זהותו של מעוול שהביטוי שבגיניו נדרשת החשיפה איננו כזה.

¹¹³ *Doe v. Cahill*, 884 A.2d 451, at 460-461.

¹¹⁴ גיוס, השמצות מקוונות, עמ' 428.

¹¹⁵ גיוס, השמצות מקוונות, עמ' 429-430.

¹¹⁶ *Dendrite International Inc. v. Doe*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001), at 760.

¹¹⁷ פסק דין זה עסק בגולש אנונימי שפרסם נתונים על מצבה הכלכלי של חברה ציבורית.

¹¹⁸ [Indep. Newspapers, Inc. v. Brodie](#), 2009 Md. LEXIS 18 (Md. Feb. 27, 2009)

¹¹⁹ פרשת *Mobilisa*, עמ' 720.

¹²⁰ [Anonymous Online Speakers v. Unites States district court](#), 611 F.3d at 661 (9th Cir. 2010) – "The nature of the speech should be a driving force in choosing a standard by which to balance the rights of



המלומד Mazzota¹²¹ ניתח פסקי דין שדנו במבחן זה, ומסקנתו היא שרוב בתי המשפט דוחים את המבחן משתי סיבות, שבמידה מסוימת סותרות זו את זו: חלק מבתי המשפט סברו שהמבחן מיותר, משום שלמעשה הוא כלול ב'מבחן ההליך המהיר' שבמסגרתו ייבחנו ממילא שיקולים הנוגעים לאיזון הערכים. חלק אחר של בתי המשפט סברו שהמבחן אכן מוסיף על 'מבחן ההליך המהיר', אך הוא אינו מוצדק משום שבמידה והשתכנע בית המשפט בכך שלמבקש יש עילת תביעה לכאורה כנגד המעוול האנונימי, וזאת לאחר ששקל כבר את המגבלות החוקתיות הנוגעות לבקשה, הטלת מגבלה נוספת על זכותו של המבקש לקבל סעד מבית המשפט תהיה בלתי חוקתית בעליל.

5.2.2. חשיפת פרטי מפר זכויות קניין רוחני

התנאים לחשיפתו של מפר אנונימי של זכויות קניין רוחני קלים מן התנאים הדרושים, לפי פסיקות בתי המשפט, לשם חשיפת פרטי מעוול בעוולת לשון הרע. תנאים אלו נקבעו ב- *Digital Millennium Copyright Act*, או בכינויו המקוצר – ה-*DMCA*.

סעיף 512(h) של חוק זה קובע¹²² שהליך לזיהוי מפר זכויות קניין אנונימי ייפתח בבקשה מצידו של הנפגע, שתועבר לידי פקיד בית המשפט, על מנת שהפקיד יורה לספק השירות למסור פרטים מזהים אודות המפר. הבקשה תכיל העתק של ההודעה בדבר הכוונה לפתוח בהליך לזיהוי המפר, נוסח מוצע לצו והצהרה בשבועה שהמידע שיימסר אודות זהותו של המפר ישמש אך ורק לשם ההגנה על זכויות הנפגע. על פי הצו, יהא על נותן השירות לספק באופן מיידי מידע שיש בו כדי לזהות את המפר, במידה שמידע שכזה מצוי ברשותו.

במידה והצו נערך כראוי, פקיד בית המשפט יחתום על הצו וימסור אותו לידי הנפגע, על מנת שיעבירו לידי ספק השירות, ואם הספק מתנגד לצו, יופנו הצדדים לדיון אודותיו בבית המשפט.¹²³ הוראות דומות נקבעו גם בחוק בעניין טלגרף, טלפוניה ורדיו-טלגרף, בנוגע לחשיפת זהותו של גולש ברשת אינטרנט של חברת תשתית לכבלים.¹²⁴

בפסק דין תקדימי משנת 2004, קבע בית המשפט הפדראלי¹²⁵ ש ה-*DMCA* חל רק על ספק של שירותי אירוח, ולא על ספק של שירותי גישה.¹²⁶

לדברי בירנהק,¹²⁷ פסיקות בתי המשפט באמריקה מלמדת שבהגנה על זכות הגולש לאנונימיות התמקדו בתי המשפט, כמעט באופן בלעדי, בעיקרון חופש הביטוי, ולא בזכות לפרטיות. לתפיסה זו יכול להיות משקל רב

anonymous speakers in discovery disputes".

¹²¹ See, Mathew Mazzota Note: Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers 51 B.C. L. Rev 833 at 858-859.

¹²² 17 U.S.C. sec. 512(h).

¹²³ ראו בירנהק, הזכות לפרטיות, עמ' 362.

¹²⁴ 47 U.S.C. sec. 551 (c)(2)(B).

¹²⁵ **Recording Industry Association of America v. Verizon Internet Services** 351 F.3d 1229, Case No. 03-7015 (D.C. Cir., December 19, 2003) cert denied 125 S.Ct. 309 (2004).

¹²⁶ ברוח זו פסק גם בית המשפט הפדראלי בפסק הדין בעניין *Recording Industry Association*, ראו:

Recording Industry Association of America v. Charter Communications Inc. 393 F.3d 771 (8th Cir., January 18, 2005)

¹²⁷ ראו בירנהק, הזכות לפרטיות, עמ' 360.



בכל הנוגע להגנה על התבטאויות שערכן, מבחינת הצורך להגן על חופש הביטוי, הוא קל יחסית.¹²⁸

בירנהק מציון,¹²⁹ שהמבחן המקובל בפסיקה האמריקנית בנוגע לפרטיות הראויה להגנה הוא מבחן הציפיות הסובייקטיביות הסבירות. מבחן זה הוא מבחן אובייקטיבי-סובייקטיבי שנועד לבחון האם לאדם הייתה צפייה ראויה וסבירה לפרטיות. רק אם הייתה לאדם צפייה שכזו, פרטיותו ראויה להגנה.¹³⁰ הפסיקה האמריקנית אינה רואה בעצם הפקדתו של מידע בידי צד שלישי מעשה הגורר אחריו קיום צפייה סבירה לפרטיות.

מקרה מבחן לשימוש בהוראה החשיפה לפי ה-DMCA הוא פרשת *LE (Landmark education)*. היא חברה בינלאומית ה"מציעה תוכניות המאתגרות פרספקטיבות שגרתיות ודפוסי קבלת החלטות. תוכניות אלו מספקות כלים חדשים... על מנת להביא לשינוי משמעותי ולחולל מפנה בעצם טבעו של מה שאפשרי".¹³¹ במסגרת התוכניות האמורות, מפעילה LE פורום, שהוא למעשה מעין קורס אינטנסיבי, שבו רוכשים המשתתפים כלים שאמורים לשפר את חייהם.

בשנת 2006 פרסם ערוץ טלוויזיה בצרפת (*France 3*) כתבת תחקיר על החברה, שהציגה אותה כמעין כת בעלת מאפיינים דתיים. הכתבה התבססה, בין השאר, על קטעי וידאו שצולמו במצלמה נסתרת, במהלך הקורס של LE. קטעים אלו הועלו לרשת האינטרנט על ידי חברות המספקות שירותי אירוח לקטעים מסוג זה, כגון *youtube, google* ועוד.

LE תבעה מן האתרים האמורים להסיר את קטעי הוידאו המדוברים, אך נענתה בשלילה. לפיכך, הגישה LE בקשה לחשיפת זהותו של מי שהעלה את הסרטונים לרשת לפי סעיף 512(h) ל-DMCA, בטענה שהסרטונים הכילו חלקים מקורסים של החברה, המוגנים בזכויות יוצרים.¹³²

המקרה האמור מעניין, משום שברור היה שהבקשה לא נועדה לחשוף את מפירי זכויות היוצרים, אלא להביא להסרת הסרטונים מהרשת, ולא להגן על זכויות היוצרים של LE אלא על שמה הטוב של החברה.

בפרשה זו, יוצג מפר הזכויות האנונימי על ידי ארגון ה-*EFF (Electronic Frontier Foundation)*. בתגובה לבקשה האמורה, העלה ה-*EFF* טיעונים אחדים הנוגעים לערכה של הזכות לאנונימיות בדיון האמריקאי ולצורך להגן על פרטיות הגולש.¹³³ עניין מיוחד מעוררים הטיעונים הנוגעים לאופן יישומה של ההוראה שבסעיף 512(h) ל-DMCA.

ראשית, ה-*EFF* טען שבהתאם להלכה שנקבעה בפרשת *Highfields*,¹³⁴ שעסקה בהפרה של הזכות לשם טוב ופגיעה בסימן מסחר, נקבע שלשם חשיפת זיהויו של המעוול נדרש המבקש את החשיפה להביא בפני בית המשפט ראיות המוכיחות את קיום יסודות העוולה מעבר לספק סביר.

¹²⁸ ראו לעיל, אחר הציון להערה 31, וכן בירנהק, הזכות לפרטיות, שם ("יוצא שפרטיותו של גולש שאינו דובר חלשה מאוד, בייחוד לעומת גורמים אחרים (להבדיל ממדינתיים), אולם "גולש דובר" יזכה להגנה חזקה יותר") שם.

¹²⁹ ראו בירנהק, הזכות לפרטיות, עמ' 361.

¹³⁰ מתוך אתר לנדמרק אדינקיישן ישראל.

¹³¹ לנוסח הבקשה, ראו כאן.

¹³² לטיעונים אלו בהרחבה, ראו כאן.

¹³³ *Highfields*, 385 F. Supp. 2d at 975-76



שנית, במידה ועמד המבקש בתנאי האמור, על בית המשפט לאזן בין זכות הפוגע לפרטיות אל מול הפגיעה הצפויה במבקש, אם תידחה בקשתו.

לטענת ה-*EFF*, אמות המידה לקבלת בקשות לחשיפת מעוול בעוולה של הפרת זכויות יוצרים לא צריכות להיות שונות מאמות המידה המקובלות בבקשות דומות, כאשר העוולה היא עוולת לשון הרע או הפרה של סימן מסחר. בטענה זו נסמך ה-*EFF* על פסיקת בית המשפט בפרשת *Sony*,¹³⁵ שאף היא עסקה בחשיפת פרטי מעוול שהפר זכויות קניין רוחני, על פי כלל 45 לכללי סדר הדין האזרחי הפדראליים. בפסיקה זו קבע בית המשפט חמישה תנאים שבהתקיימם ייעתר בית המשפט לבקשה: (1) קיומן של ראיות לכאורה לפגיעה הנטענת; (2) ייחוד הבקשה כלפי עוולה מסוימת; (3) העדר אמצעים אחרים להביא לחשיפת פרטי המעוול; (4) קיומו של צורך חיוני בחשיפת פרטי המעוול כדי לקדם הליך משפטי; (5) בחינה של צפיית הצדדים לפרטיות. תנאים אלו דומים לתנאים שנקבעו על ידי בתי המשפט בכל הנוגע לחשיפת זהות המעוול בעוולת לשון הרע.

אמנם, ה-*EFF* הכיר בכך שתנאים אלו לא נקבעו בחוק, בנוגע לבקשה לחשיפת פרטי מעוול לפי ה-*DMCA*, אך לטענתו, מן הראוי שהחלטות פקיד בית המשפט לפי הוראות ה-*DMCA* תהיינה חשופות לביקורת שיפוטית הדומה לזו שהתגבשה בפסיקה הנוגעת לחשיפת פרטי מעוול בעוולת לשון הרע.

הלכה למעשה, טענות אלו לא נדונו בבית המשפט, מאחר שהצדדים הגיעו לידי הסכם פשרה שלפיו הסרטונים יוסרו מהרשת ו-*LE* תמשוך את בקשת החשיפה.¹³⁶ לא למותר לציין, שהסכם זה מוכיח את יעילותה של בקשת החשיפה כאמצעי להשתקת ביקורת.¹³⁷

אפשר שנכוונתה של *EFF* לחתום על הסכם הפשרה ובכך להגן על האנונימיות במחיר השתקתה של הביקורת נגד *LE* מעידה שבאי כוחה של *EFF* לא היו משוכנעים שבית המשפט יקבל את טיעוניהם, וחששו מפני תקדים שיקבע שהתנאים לחשיפת פרטי מעוול בעוולה של פגיעה בזכויות יוצרים קלים מן התנאים הדרושים לשם חשיפת פרטי מעוול בעוולה של לשון הרע.

5.3. בריטניה

בבריטניה, הנושא של חשיפת פרטי מעוול מוסדר באמצעות צווי *Norwich Pharmacal*. צווים אלו הינם יציר פסיקה של בית הלורדים משנת 1974,¹³⁸ שאפשרה באופן עקרוני למי שנפגע מעוולה, להוציא כנגד צד שלישי צו המורה לו לחשוף פרטים שיביאו לזיהויו של המעוול, על מנת שניתן יהיה לתובעו.¹³⁹

בפסיקה זו אף נקבעו מספר גורמים שיש להתחשב בהם בעת מתן הצו, כגון: סיכויי התביעה כנגד המעוול; טיב היחסים שבין המשיב לצו ובין המעוול; השאלה האם ניתן להשיג את המידע המבוקש

¹³⁵ Sony v Does, 326 F. Supp. 2d at 564-65

¹³⁶ לנוסח ההסכם, ראו כאן.

¹³⁷ על השימוש בבקשות מסוג זה לשם השתקת ביקורת, ראו בהרחבה:

Lyrissa Barnett Lidsky, Anonymity in Cyberspace: What Can We Learn from John Doe?, 50 B.C. L. REV. 1373 (2009); Lyrissa Barnett Lidsky, "Silencing John Doe: Defamation & Discourse in Cyberspace", 49 Duke L. J. 855, at pp. 881.

¹³⁸ Norwich Pharmacal Co. v. Customs and Excise Commissioners, [1974] A.C. 133 (H.L.)

¹³⁹ על צו זה ראו גם, בירנהק, הזכות לפרטיות עמ' 358



בדרך אחרת (מבלי לערב את המשיב); האם חשיפת זהות המעוול עלולה להסב למשיב נזק שלא יהיה בכוחו של המבקש לפצות עליו?

לפי בירנהק, פסיקת בתי המשפט בבריטניה מלמדת, שכאשר בתי המשפט בבריטניה מעניקים הגנה לאנונימיות של הגולש, הם מסתמכים בעיקר על הזכות לפרטיות, ופחות על עיקרון חופש הביטוי. זאת, בניגוד לעולה מפסיקת בתי המשפט בישראל, לפיה ההגנה על האנונימיות של הגולש מבוססת בעיקר על חופש הביטוי, ופחות על הזכות לפרטיות.¹⁴⁰ לתפיסה זו יכול להיות משקל רב בכל הנוגע להגנה על התבטאויות שערכן, מבחינת הצורך להגן על חופש הביטוי הוא קל יחסית.¹⁴¹

הפרקטיקה של חשיפת זהותו של מעוול באמצעות צו *Norwich Pharmacal* עוגנה בשנת 1998 בסעיף 35 של ה- (*Data Protection Act (DPA)*),¹⁴² הקובע שניתן לחשוף מידע אישי כאשר הדבר דרוש על פי חוק או על פי צו של בית המשפט. זאת, כאשר המידע נחוץ לשם או בקשר לכל הליך משפטי (קיים או צפוי), כאשר המידע נחוץ לשם קבלת ייעוץ משפטי או כאשר הוא נחוץ לשם ביסוס, מימוש או הגנה על זכויות משפטיות.

כמו כן, סעיף 31.18 של כללי הפרוצדורה האזרחית¹⁴³ קובע, שההוראות הנוגעות לחשיפתם של מסמכים לפני שהמשפט החל ולחשיפת פרטים המצויים בידי צד שלישי, לא נועדו להגביל כל כוח שיש בידי בית המשפט להורות על חשיפת פרטים לפני שהמשפט החל או על חשיפת פרטים המצויים בידי צד שלישי, שאינו צד לדיון. הוראה זו נועדה לשמר בידי בתי המשפט את הסמכויות שהיו להם כבר מאז שנות השבעים של המאה העשרים, למסור צווי *Norwich Pharmacal*.¹⁴⁴

בפרשת *Totalise*¹⁴⁵ הדגיש בית הלורדים שעיקרון סמכותם של בתי המשפט להעניק צווי *Norwich Pharmacal* בחוק, לא נועד לגרוע מאמות המידה שנקבעו בפסיקה הנוגעת לצווים מסוג זה, והיו תקפות ערב כניסתו של החוק לתוקף. באותה פסיקה נקבע, שבעניין זה יתחשב בית המשפט, בין השאר, בסיכויי התביעה ובקיומה או העדרה של מדיניות פרטיות לאתר שבמסגרתו התרחשה הפגיעה.¹⁴⁶

בהתאם לפסיקה זו, בתי המשפט החילו את אותן אמות מידה שהיו מקובלות בפסיקה ערב כניסתו של החוק האמור לתוקף, אף על צווי *Norwich Pharmacal* שניתנו בהתאם לסעיף 35 של ה- *DPA*, ואף הרחיבו והבהירו תנאים אלה.

כך למשל, בפסק הדין בעניין *Mitsui*¹⁴⁷ נקבעו ארבעה תנאים שבהתקיימם ייעתר בית המשפט לבקשה להעניק לתובע צו *Norwich Pharmacal*: (1) העוולה בוצעה על ידי המעוול או שהמעוול היה שותף לביצועה; (2) חשיפת זהות המעוול חיונית לשם קיומו של הליך נגדו; (3) האדם שכנגדו מופנה הצו חייב להיות שותף במידת מה לביצוע העוולה, ולו בכך שאפשר את קיומה; (4) בידי האדם שכנגדו מופנה הצו

¹⁴⁰ ראו בירנהק, הזכות לפרטיות, עמ' 359.

¹⁴¹ ראו לעיל, אחר הציון להערה 31.

¹⁴² לנוסח הסעיף באנגלית, ראו כאן.

¹⁴³ [Civil Procedures Rules 31.18](#)

¹⁴⁴ Silke Weiss, "[Is an Internet Service Provider authorized to disclose my personal details to \(1\) third parties or \(2\) courts in the case of copyright infringement?](#)" (Detailed Answer for United Kingdom), Knowledge Base Copyright Law (KB:Law|©), Answer No. 156, Version: 16/07/2009

¹⁴⁵ *Totalise plc v. Motley Fool L.td*, [2001] 2 EWCA Civ 1897.

¹⁴⁶ על פסיקה זו ראו גם, בירנהק, הזכות לפרטיות, עמ' 358-359.

¹⁴⁷ *Mitsui Limited v Nexen Petroleum UK Limited* [2005] EWHC 625 (Ch).



ישנו מידע שבעזרתו ניתן, או צפוי שיהיה ניתן לתבוע את המעוול.

צווי *Norwich Pharmacal* משמשים כיום ככלי המרכזי לחשיפת פרטי מעוול ברשת האינטרנט.¹⁴⁸ בהקשר זה מן הראוי לציין פסיקה מעניינת שניתנה ממש לאחרונה,¹⁴⁹ ולפיה בבואו להורות על חשיפת פרטי המעוול, על בית המשפט לקחת בחשבון את אופיו של הביטוי וכן את ההקשר שבו הוא מופיע. פסיקה זו עסקה בתביעת דיבה כנגד מגיבים לידיעה באתר חדשותי, שבו דווח שהגב' *Jane Clift* זכתה בתביעה נגד הוועד המקומי של העיירה בה היא התגוררה. חלק מהמגיבים השמיצו אותה וגב' *Clift* הגישה לבית המשפט בקשה להורות למנהל האתר *Mail Online*¹⁵⁰ לחשוף את זהותם של המגיבים. בית המשפט דחה את התביעה הן בשל כך שלדעת בית המשפט התגובה אינה בהכרח בגדר לשון הרע, והן בשל כך שלפי אופייה של התגובה יש להניח שרוב הקוראים יראו בה "שיחת פאב" בלבד, בייחוד לאור הכתבה האוהדת ועמדתם של רוב המגיבים.

5.4. קנדה

הבסיס החוקי לסמכות בתי המשפט להורות על חשיפת פרטי מעוול, מצוי בדרך כלל, בהוראות ברמה הפדראלית או המדינתית הקובעות חריגים לכלל הקובע שספקי השירות מחויבים להגן על המידע האישי שנמסר בידיהם.

כך למשל, במדינת בריטיש קולומביה, קובע סעיף 18 של החוק להגנה על המידע האישי משנת 2003¹⁵¹ שארגון יהיה רשאי לחשוף מידע אישי על אדם מבלי לקבל את הסכמתו, אם החשיפה היא לשם ציוד לצו בית המשפט, או לצו של כל אדם או גוף המוסמך להורות על חשיפה שכזו.

הוראה דומה קיימת גם ברמה הפדראלית, בסעיף 7(3)(c) של החוק להגנת המידע האישי והמסמכים האלקטרוניים משנת 2000.¹⁵² כך, אף בהעדר הסדרה מדינתית של הזכות לדרוש חשיפה של מידע אישי לשם ניהולו של הליך משפטי, יוכלו בתי המשפט להורות על חשיפה שכזו, בהסתמך על החוק הפדראלי. לשם השגת צו שיפוטי המורה לספקי השירות לחשוף את זהותו של מעוול, ניתן לעשות שימוש באחת משתי דרכים: באמצעות יישום כללי הפרוצדורה האזרחית, או באמצעות צווי *Norwich Pharmacal*.¹⁵³ ההבדל המרכזי שבין שני המסלולים נוגע לשלב שבו מוגשת הבקשה לחשיפת זהותו של המעוול: בעוד שההליך החוקי מאפשר להגיש את הבקשה רק לאחר שהוחל כבר בקיומו, המסלול השיפוטי מאפשר להגיש בקשה שכזו גם לפני שנפתח הליך משפטי.

¹⁴⁸ ראו פסקי הדין הנוכחים בהערות 145, ו-147, וכן: *Sheffield Wednesday Football Club Ltd v. Hargreaves*, [2007] EWHC 2375 (Q.B.); *G & G v. Wikimedia Found. Inc.*, [2009] EWHC 3148.

¹⁴⁹ [Jane Clift v Martin Clarke](#) [2011] (QBD) (Judgment 18.02.11)

¹⁵⁰ אתר חדשותי של העיתון Daily Mail.

¹⁵¹ Personal Information Protection Act, S.B.C. 2003 c.63, sec. 18(1)(i).

¹⁵² Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5.

¹⁵³ אמנם, יש הקוראים לאיחוד שני המסלולים, בשל הקשיים הנוצרים כתוצאה מקיומם של שני מסלולים לקיומו של אותו הליך, שבכל אחד מהם נקבעים כללים שונים. לעניין זה ראו למשל: Matthew Nied, "Unmasking Anonymous Defendants in Internet Defamation Cases: Recent Developments and Unresolved Issues", *Canadian Privacy Law Review*, Vol. 8, No. 3, p. 31, 2011 at 34.



5.4.1. כללי הפרוצדורה האזרחית

השימוש בכללי הפרוצדורה האזרחית הוא הדרך הנפוצה יותר לחשיפת פרטי המעוול. מסלול זה מבוסס על הוראות חוק הקובעות את סדר הדין האזרחי במחוזות השונים של קנדה. כך למשל, סעיף 30.10 של כללי סדר הדין האזרחי במדינת אונטריו¹⁵⁴ מסמך את בית המשפט להורות לצד שלישי שאינו מעורב בתביעה שלפניו, להציג מסמך שהוא רלוונטי לתביעה ולא ניתן לקיים דיון הוגן בלעדיו.¹⁵⁵ לחילופין, בית המשפט מוסמך להורות לצד שלישי להכין מסמך שיובא לעיונו, על מנת שיוכל להכריע האם יש לגלות מסמך זה במשפט או לא.¹⁵⁶

בתי המשפט פירשו הוראה זו כמקנה להם גם את הסמכות להורות לצד שלישי לחשוף את זהותו של מעוול אנונימי, כאשר הדבר דרוש לשם המשך קיומו של ההליך המשפטי.

תנאי הסף הקבועים בכללי סדר הדין לשם מתן הוראה למסור מידע שהוא רלוונטי לקיומו של ההליך הינם מקילים באופן יחסי. די בכך שיוכח כי חשיפת זהותו של המעוול חיונית לשם המשך קיומו של ההליך, על מנת שבית המשפט יהיה מוסמך להורות לצד שלישי לחשוף את זהותו של המעוול.

ואולם, בתי המשפט פירשו סמכות זו בצמצום, מתוך תפיסה שכללים אלו כפופים להוראותיה של מגילת זכויות האדם הקנדית, ובשל כך, על בית המשפט להתחשב בעקרונות חוקתיים כחופש הביטוי, הזכות לפרטיות וכדומה, בבוא ליישם.

בהתאם לתפישה זו קבע בית המשפט של מחוז אונטריו בפרשת *Warman*¹⁵⁷ שעל בית המשפט להתחשב בשלושה גורמים בטרם יורה על חשיפת המידע המבוקש:

1. על בית המשפט להשתכנע שהמבקש הציג ראיות המספיקות כדי להקים עילת תביעה לכאורה.
2. על בית המשפט להשתכנע בחיוניות הליך החשיפה להמשך קיומו של ההליך שבפניו.
3. על בית המשפט להורות על חשיפה רק לאחר שאיזון בין הערכים המתנגשים, ומצא שהכף נוטה לטובת החשיפה.

בנוגע לעריכת האיזון בין הערכים, הציע בית המשפט ארבעה מבחני עזר, כדלהלן:

1. האם המעוול היה אמור לצפות לכך שזהותו לא תיחשף בנסיבות הקיימות?
2. האם המבקש הקים עילת תביעה לכאורה כנגד המעוול והוא נוהג בתום לב?
3. האם המבקש נקט באמצעים סבירים כדי לחשוף את זהות המעוול אך כשל בכך?
4. האם העניין הציבורי שבחשיפת זהותו של המעוול גובר על זכות המעוול לפרטיות ולחופש ביטוי?

פסיקה זו יושמה גם בתביעות לחשיפת פרטי מעוולים אנונימיים ברשת האינטרנט במחוזות אחרים של קנדה.¹⁵⁸

¹⁵⁴ Rules of Civil Procedure, RRO 1990, Reg 194 (להלן כללי סדר הדין, אונטריו).

¹⁵⁵ הוראה דומה קיימת אמנם גם בסעיף 183 לתקנות סדר הדין האזרחי, התשמ"ד-1984 (אם כי היא הרבה פחות מפורטת), אולם תקנות סדר הדין האזרחי בישראל אינן מאפשרות הגשת תביעה כנגד נתבע אנונימי (ראו פרשת מור, סעיף 24 לפסק דינו של השופט ריבלין).

¹⁵⁶ וראו גם כללי סדר הדין, אונטריו, סעיף 76.03, כללי סדר הדין האזרחי בבית המשפט העליון של מחוז בריטיש קולמביה (B.C Reg. [Supreme Court Civil Rules](#) 168/2009), סעיפים 7-1 ס"ק (18), וכן סעיף 7-5, כללי סדר הדין במדינת נובה סקוטיה (Nova Scotia Annotated Civil Procedure Rules), סעיפים 14.12, ו-18.12, וכללי סדר הדין בבתי המשפט של מדינת ניו בرونסוויק (New Brunswick Rules of Court), סעיף 32.12.

¹⁵⁷ *Warman v. Wilkins Fournier*, [2010] O.J. No. 1846, 2010 ONSC 2126 at para. 24 (Div. Ct.)



5.4.2. צווי Norwich Pharmacal

הפרקטיקה של חשיפת פרטי מעוול באמצעות הענקת צווי *Norwich Pharmacal*, שהורתה בבריטניה, אומצה למעשה גם על ידי בתי המשפט בקנדה, אם כי, בשינויים קלים.

צו *Norwich Pharmacal* ניתן לראשונה על ידי בית המשפט הפדראלי בפרשת *Glaxo* משנת 1998.¹⁵⁹ בפסק דין זה קבע בית המשפט ארבעה עקרונות, שבהתקיימם ייעתר בית המשפט לבקשה למסור את הצו, כדלהלן:

1. על המבקש להוכיח שיש בידיו טענה תמת לב כנגד המעוול;
2. על המבקש להראות קיום סוג מסוים של יחסים בינו לבין המשיב;
3. על המבקש להוכיח שלא יוכל לחשוף את זהות המעוול מבלי להידרש לעזרתו של המשיב;
4. על בית המשפט להתחשב במכלול השיקולים, בעד ונגד החשיפה.

דרישת הטענה בתום לב קיבלה פרשנות רחבה על ידי בית המשפט לערעורים במדינת אונטריו בפרשת *Straka*.¹⁶⁰ בפרשה זו התברר שהמבקש את חשיפת הזהות עדיין לא גיבש תביעה כנגד המעוול, אלא רק רצה לבחון את סיכוייו להגיש תביעה שכזו. למרות זאת, בית המשפט פסק שאין לראות במבקש כמי שאין בידיו טענה תמת לב כנגד המעוול, ואין בכך כדי לשלול את זכותו לדרוש את חשיפת זהותו של המעוול.

בפרשת *Leahy*¹⁶¹ קבע בית המשפט של מדינת אלברטה שלא יינתן צו, אלא כאשר המידע המבוקש חיוני לשם זיהוי המעוול; המידע חיוני כדי לסייע בתביעה כנגד המעוול או למצער, לסייע בהכרעה האם ניתן לתבוע את המעוול; המידע חיוני כדי לעקוב או להגן על רכוש.

בבקשת רשות הערעור קבע בית המשפט חמישה מבחנים למתן הצו, כדלהלן:

1. האם המבקש סיפק ראיה שיש בה די להקים עילת תביעה סבירה, תקפה ותמת לב?
2. האם התקיימו יחסים בין המשיב למעוול, העושים את המשיב למעורב בצורה כלשהיא במעשים שפגעו במבקש?
3. האם המשיב הינו הגורם היחידי שניתן להיעזר בו לשם חשיפת זהות המעוול?
4. האם ניתן יהיה לפצות את המשיב על נזקים או הוצאות שייגרמו לו כתוצאה מן הציות לצו?
5. האם שיקולי צדק מטים לטובת מתן הצו?

מבחנים אלו אומצו במספר פסקי דין נוספים שעסקו בסוגיה זו.¹⁶²

לכאורה, המבחנים שנקבעו בפרשת *Leahy* אינם כוללים את מבחן חיוניות החשיפה המוכר מן הפסיקה הבריטית. ואולם, בפסיקה של בית המשפט לערעורים במדינת אלברטה משנת 2008 נדחתה בקשה

¹⁵⁸ See: *A.B v. Bragg Communication Inc.*, [2010] N.S.J. No. 360, 2010 NSSC 215; *Doucette v. Brunswick News* [2010] N.B.J. No. 235, 2010 NBQB 233;

¹⁵⁹ *Glaxo Wellcome PLC v. Canada* (1998), 162 D.L.R. (4th) 433 (F.C.A.)

¹⁶⁰ *Straka v. Humber River Regional Hospital* (2000), 51 O.R. (3d) 1 (C.A.).

¹⁶¹ *Alberta v. Leahy* (2000), 270 A.R. 1 (Q.B.), aff'd (2002), 303 A.R. 63 (C.A.), leave to appeal denied [2002] S.C.C.A. No. 235 (QL)

¹⁶² ראו למשל: *Dynasty Furniture Manufacturing Ltd. v. Toronto-Dominion Bank*, 2009 ABQB 388 at para. 14; *Isoton S.A. v. Toronto Dominion Bank*



למסירת צו *Norwich Pharmacal* ללא דיון של ממש במבחנים האמורים, רק בשל העובדה שהמבקש לא הציג בפני בית המשפט סיבה משכנעת לכך שהליך הזיהוי המקובל לפי סדרי הדין האזרחיים, במהלך קיומו של משפט, לא יועיל לו. יש המסיקים מכך, שמבחן חיוניות החשיפה תקף גם במדינת אלברטה.¹⁶³ גם במדינת אונטריו, בפסק הדין בעניין *Ventra*¹⁶⁴ עמד בית המשפט על חשיבותו של מבחן חיוניות החשיפה כאחד מן השיקולים החשובים שעל בית המשפט לשקול בבואו לתת את הצו.

בשנת 2009 אומצו מבחנים אלו ואף הורחבו בפסק הדין בעניין *York University*¹⁶⁵ שעסק בחשיפת זהותו של מעוול שהפיץ שמועה ברשת האינטרנט נגד נשיא אוניברסיטת יורק, לפיהן הוא נהג במרמה במינויים אקדמיים באוניברסיטה. בית המשפט קבע שעל מנת שיוורה על חשיפת זהות המעוול יש לקיים את התנאים הבאים:

1. **תום לב** – על המבקש להוכיח עילה לכאורה לתביעה כנגד המעוול, ושהתביעה היא סבירה ותמת לב.
2. **מעורבות** - על המבקש להוכיח שספק השירות היה מעורב בעקיפין בביצוע העוולה, שכן הוא הגורם שהפיץ את ההשמעות.
3. **הכרחיות ההליך** - על המבקש להוכיח שננקטו על ידו אמצעים סבירים לשם חשיפת זהות המעוול שלא באמצעות פתיחת ההליך כנגד ספק השירות, ושההליך הינו הדרך היחידה האפשרית לחשיפת זהותו של המעוול.
4. **פיצוי ספק השירות** - על המבקש להוכיח שניתן לפצות את ספק השירות על הנזקים או ההפסדים שייגרמו לו כתוצאה מן החשיפה.
5. **חיוניות המידע** – על המבקש להוכיח שהמידע המבוקש חיוני למבקש.
6. **ציפייה סבירה לפרטיות** - על המבקש להוכיח שלגולשים אין ציפייה סבירה לפרטיות.
7. **מטרת החשיפה** - על המבקש לשכנע את בית המשפט שהחשיפה נועדה אך ורק לשם קיומו של הליך משפטי.

בקרב המלומדים הובעו דעות שונות בנוגע לפרשנות הראויה של כל אחד מן המבחנים שנקבעו בפסיקה הקנדית למתן צו *Norwich Pharmacal*.

בנוגע לדרישת תום הלב, יש שסברו שדי בהצגת עילה המבוססת על אמונה סובייקטיבית של המבקש שיש לו עילת תביעה.¹⁶⁶ ואולם, הדעה הרווחת כיום היא שמשמעות הדרישה האמורה היא, שהתביעה שבשלה מוגשת הבקשה לצו לא תהיה למטרה שאינה ראויה, וניתן יהיה לתמוך בה בראיה מסוימת, שהיא מעבר לאמונתו הסובייקטיבית של המבקש.¹⁶⁷

בנוגע לדרישת המעורבות, הגישה הרווחת בקרב המלומדים היא, שכאשר ניתן להצביע על רווח מכל סוג

¹⁶³ D. Lynne Watt, "The Law and Policy of Norwich Pharmacal Orders", at pp. 7.

¹⁶⁴ GEA Group AG v. Ventra Group 2009 ONCA 619.

¹⁶⁵ York University v. Bell Canada Enterprises 2009 CanLII 46447 (Ont. S.C.J.).

¹⁶⁶ BMG Canada Inc. v. John Doe, 2004 FC 488 at para. 13, rev'd 2005 FCA 193 at 21 [BMG]; 34ff

¹⁶⁷ Randall W. Block, Michael A. Marion and R.J. Gilborn, "Sealed Ex Parte Norwich Orders: Safeguarding Against Abuse of the Pre-Action Disclosure Remedy" (2003) *Annual Review of Civil Litigation* 225 at para. 34. (להלן: בלוק מריון וגילבורן, 2003).



שהוא שצומח למשיב כתוצאה מפרסום המידע האנונימי, די בכך כדי לקשור בינו לבין העוולה.¹⁶⁸

אחרים הציעו את ההבחנה בין משקיף (*bystanders*) למסייע (*facilitators*), וטענו שצד שלישי שהוא רק "משקיף" אינו חשוף לצו. רק צד שלישי שהוא גם מסייע לעוולה במידה מסוימת, אף אם הוא עושה זאת בתום לב או אף שלא במודע, חשוף לצו.¹⁶⁹

בנוגע להכרחיות ההליך, שעל המבקש להוכיח שההליך הוא הדרך ההגיונית והסבירה ביותר לחשיפת זהותו של המעוול, אך אין צורך שיוכיח שזוהי הדרך הבלעדית לשם כך.¹⁷⁰

הדרישה של **חיוניות המידע** היא עמומה. בפרשת *Ventra*¹⁷¹ קבע בית המשפט שגבולותיה של דרישה זו ייקבעו בהתאם לכל מקרה נתון. לעיתים המידע חיוני כדי להעריך את סיכויי התביעה, לעיתים כדי לקבל סעד מן המעוול, לעיתים כדי לשמר עדויות ולעיתים כדי להגן על רכוש. חשוב גם לציין, שלפי פסק הדין אין צורך להוכיח קיומו של הליך בפועל, שזיהוי המעוול חיוני לשם קיומו, אלא די בכך שהמבקש ישכנע את בית המשפט שהוא שוקל ברצינות לפתוח בהליך שכזה.¹⁷²

5.5. הונג קונג

ברמה הסטטוטורית, נקבעו בסעיף 58 לתקנות ההגנה על פרטיות המידע¹⁷³ חריגים אחדים, שבהתקיימם, ניתן לחשוף מידע אישי. לעניינו של מסמך זה, חשוב להפנות לס"ק (2), הקובע שמידע אישי יוחרג מן ההוראות בעניין ההגנה על המידע האישי, בכל מקרה שהמידע דרוש לשם אחת מן המטרות המנויות בס"ק (1), וההגנה על המידע עלולה לפגוע באחת מן הזכויות המנויות בס"ק זה.

בין המטרות המנויות בס"ק (1), ניתן למצוא בס"ק (d): "מניעה, עצירה או הבטחת פיצוי בשל התנהגות לא חוקית, לא הוגנת, לא מוסרית או רשלנית".

צירופן של ההוראות מוביל למסקנה, שניתן לפגוע בפרטיות המידע לשם חשיפת זהותו של מעוול, וזאת כדי שניתן יהיה לתבוע ממנו פיצוי או למנוע ממנו לבצע עוולות.

בפרשת *Cinepoly Records*¹⁷⁴ עשה בית המשפט העליון של הונג קונג שימוש בסעיף האמור כדי להורות על חשיפת פרטיהם של מפירי זכויות קניין רוחני ברשת האינטרנט, בהתבסס על התנאים שנקבעו בבריטניה, בנוגע למסירת צווי *Norwich Pharmacal*.

בית המשפט קבע שלפי נוסח סעיף (2) של התקנות האמורות, אין להגן על מידע אישי אם חשיפתו נועדה להגן מפני עוולות. ואולם, על המבקש את חשיפת המידע לשכנע את בית המשפט שהחשיפה אכן תשרת את המטרה האמורה.

בפסיקתו, התחשב בית המשפט בשישה גורמים רלוונטיים:

¹⁶⁸ בלוק מריון וגילבורן, 2003 עמ' 243.

¹⁶⁹ יו, 2007 סעיף 18ff.

¹⁷⁰ ראו: בלוק מריון וגילבורן, 2003. כמו כן ראו [D. Lynne Watt, "The Law and Policy of Norwich Pharmacal Orders"](#), pp. 12. (להלן: וואט, חוק ומדיניות)

¹⁷¹ לעיל, הערה 164, פסקאות 91-90.

¹⁷² שם, פסקה 87.

¹⁷³ לנוסח הסעיף באנגלית, ראו בכתובת http://www.privacy.com.hk/pt_viii.html#58 (כניסה אחרונה: 31 בינואר, 2012).

¹⁷⁴ *Cinepoly Records Co. Ltd. et al, v. Hong Kong Broadband et al.*, HCMP2487, 2005



1. אין מקור אחר שניתן להפיק ממנו את המידע המבוקש.
2. הקלות, המהירות וההיקף של ההפרה מחייבים פעולה מהירה.
3. סירוב לבקשה יוביל לתוצאה הבלתי נסבלת שהמעוולים יוכלו להמשיך ולהפר את זכויותיהם של אחרים, תוך שימוש במעטה האנונימיות שמספקת רשת האינטרנט.
4. לפי תנאי ההתקשרות שבין ספקי השירות למשתמשים, אין החשיפה מנוגדת הן לתקנות בעניין ההגנה על פרטיות המידע והן לחובת הסודיות המוטלת על הספקים בהתאם לחוזה ההתקשרות שבינם לבין המשתמשים.
5. היקף המידע שהתבקש אינו רחב יתר על המידה.
6. המידע יכול לשמש אך ורק לשם ההגנה על זכויות המבקשים.

5.6. גרמניה

בגרמניה, האיזון החוקתי שבין חופש הביטוי לכבוד האדם שונה באופן משמעותי מהאיזון המקובל בארה"ב, בקנדה ובבריטניה. החוקה הגרמנית רואה אמנם בחופש הביטוי ערך יסודי, אך היא קובעת בצורה מפורשת שהערך של השמירה על כבוד האדם ויכולתו לפתח את אישיותו גובר על הערך של חופש הביטוי. החוקה אף קובעת שעל המדינה לדאוג לכך שכבודם של האזרחים וזכותם לפתח את אישיותם יישמרו.¹⁷⁵ שוני זה באיזון החוקתי בא לידי ביטוי בפסיקות בתי המשפט בגרמניה בהקשרים שונים שאינם מעניינו של מסמך זה, אך גם בכל הנוגע לחשיפת פרטי מעוול אנונימי.

בהתאם לתפיסה החוקתית האמורה, קובע החוק הגרמני¹⁷⁶ שבאתרים בעלי אופי ציבורי, כאתרים מסחריים, רשתות חברתיות וכדומה, על כל מי שמבקש להעלות תוכן לאתר, להירשם ולמסור בעת הרישום פרטים מזהים (שם, כתובת וכדומה). הוראות אלו מצמצמות במידה ניכרת את הצורך לחשוף את זהותו של המעוול, משום שעל פי רוב, זהותו חשופה ממילא, ולא נדרש מאמץ רב כדי להביאו לדין.

ואמנם, התופעה של הגשת תביעות דיבה כנגד מגיבים, בלוגרים וכדומה היא תופעה נפוצה למדי בגרמניה. בנוגע לחשיפת פרטי מעוול שהפר זכויות יוצרים, אימץ חוק זכויות היוצרים הגרמני את הדירקטיבה האירופית בעניין אכיפת זכויות קניין רוחני (וראו פרק 5.1.4 לעיל),¹⁷⁷ המכירה בזכותו של הנפגע להגיש לבית המשפט תביעה לחשיפת זהותו של המעוול.¹⁷⁸ החוק הגרמני קובע, שניתן יהיה לתבוע את חשיפת זהותו של המעוול, ובלבד שהפרת הזכויות תהיה ברמה מסחרית. הפירוש המדויק של הרמה המסחרית המצדיקה פתיחתו של הליך מסוג זה שנוי במחלוקת בין בתי המשפט בגרמניה, אך ככלל, ניתן לומר שפירושו של המושג מושפע מאופייה של ההפרה, גודלה, השפעתה על רווחי הנפגע וכדומה (למשל, הורדת שיר בודד מתוך דיסק, לא תחשב הפרה של זכויות יוצרים ברמה מסחרית).

¹⁷⁵ ראו: Ronald Krotoszynski, Jr., Defamation in the Digital Age: Some Comparative Observations on the Difficulty of Reconciling Free Speech and Reputation in the Emerging Global Village, 62 **WASH. & LEE L. REV.** 339 (2004) at 350-349; Allison Hayward. 2007, "Regulation of Blog Campaign Advocacy On the Internet: Comparing U.S., German and EU Approaches" ExpressO. Available at: http://works.bepress.com/allison_hayward/2_at_pp_10-11 (להלן: אליסון, 2007).

¹⁷⁶ Impresum Law, § 5 TMG & § 55 RstV וראו בהרחבה אליסון, 2007 בעמ' 13-14.

¹⁷⁷ IP Enforcement Directive (2004/48/EC)

¹⁷⁸ ראו Urheberrechtsgesetz, UrhG סעיף 101a. להרחבה בעניין זה ראו [European Commission Study on Online Copyright Enforcement and Data Protection in Selected Member States](#), November 2009, pp. 37-35.



5.7. שבדיה

שבדיה אימצה אף היא בחוק זכויות היוצרים שלה¹⁷⁹ את הוראות הדיקטיבה האירופית האמורה בעניין אכיפת זכויות קניין רוחני משנת 2004, המאפשרות חשיפת פרטי מעוול שהפר זכויות יוצרים.¹⁸⁰ התנאי היחיד לחשיפה הוא, שהמבקש יראה עילה לכאורה לתביעה בשל הפרת זכות יוצרים. החוק אף קובע שהוראותיו יחולו לא רק בנוגע להפרה ממשית של זכויות יוצרים, אלא גם בנוגע לניסיונות להפר זכויות יוצרים או למבצעי פעולות המאפשרות את ההפרה.¹⁸¹

ואולם, בשנת 2006 אימץ הפרלמנט האירופי דיקטיבה חדשה, העוסקת בין השאר, בחובתם של ספקי גישה לאינטרנט להגן על מידע המגיע לידיהם, ובכלל זה להימנע מהעברת כתובות IP וכדומה.¹⁸² דיקטיבה זו לא אומצה אמנם בחוק השבדי, אך בתביעה לחשוף זהותו של מעוול אשר הפר לכאורה זכויות יוצרים שנידונה לאחרונה בבית המשפט העליון בשבדיה, הפנה בית המשפט שאלה לבית המשפט האירופי לצדק (ECJ), על מנת שיחווה דעתו בשאלה, האם לאור הוראותיה של הדיקטיבה החדשה ניתן עדיין לחשוף את פרטי המעוול.¹⁸³ לא מצאנו בדין השבדי הוראות העוסקות בחשיפת פרטי מעוול בעוולות נוספות.

6. משפט עברי

6.1. חופש הביטוי

בספר בראשית (ב, ז), מתואר האדם הראשון עלי אדמות כ"נפש חיה", ומתרגם אונקלוס - "רוח ממללא", כי "אף בהמה וחיה נקראו נפש, אך זו של אדם חיה שבכולן, שנתוסף בה דעה ודיבור".¹⁸⁴ מכאן, שיכולתו של האדם לבטא את שעל ליבו היא תמצית האנושיות, והיא המשקפת את יתרונו של האדם על החיה.

רבי אליעזר אשכנזי, מקובל ופוסק בן המאה ה-17 הדגיש את הערך של השמירה על חופש הביטוי בשל תרומת הביטוי לחקר האמת, כי "מתוך הויכוח יתבאר האמת... שמתוך היות אמונות נבדלות ונפרדות זו מזו ימשך התעוררות ויתברר האמת".¹⁸⁵

באופן דומה, רבי ישראל סלנטר, מייסד 'תנועת המוסר' במאה ה-19, לומד מן הפסוק "בקרוב אלי מרעים תשמענה אוזני" (תהלים כז, ב), ש"צריך לשמוע אף לדברי מרעים, שמא יש בדבריהם שמץ או גרעין של אמת, וחז"ל אמרו: 'איזהו חכם הלומד מכל אדם' (אבות ד, א)".¹⁸⁶

ACT ON COPYRIGHT IN LITERARY AND ARTISTIC WORKS (Act 1960:729, of December 30, 1960,¹⁷⁹ as amended up to April 1, 2009), section 53c

OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April [DIRECTIVE 2004/48/EC](#)¹⁸⁰ 2004 on the enforcement of intellectual property rights, section 8.

¹⁸¹ חקיקה זו הובילה לכך שספקי גישה לאינטרנט החלו למחוק מידע הנוגע לזהות הגולשים. לדיווח על כך, ראו [כאן](#).
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March [DIRECTIVE 2006/24/EC](#)¹⁸² 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, section 5.

¹⁸³ לדיווח על פסיקה זו ראו [כאן](#).

¹⁸⁴ פירוש רש"י על התורה, בראשית ב, ז.

¹⁸⁵ מעשי ה' מעשה בראשית, פרק לא, נו ע"ב.

¹⁸⁶ מובא בחידושי בעל 'שרידי אש' הקדמה, פרקי חיים, עמ' 5, הערה 11.



המהר"ל מפראג רואה בסתימת פיות ביטוי לחולשה. לכן, "אף אם הדברים הם נגד אמונתנו ודתו, אין לומר אליו: 'אל תדבר ותסתום דברי פיך', שאם-כן לא יהיה בירור הדת... כי העלם דברי המתנגד בדת, אין זה רק [=אלא] בטול וחולשת הדת..."¹⁸⁷

אמנם, כאשר בוחנים לעומק את משקלו היחסי של חופש הביטוי, לעומת המשקל הניתן לעיקרון זה בהגות המערבית, ניתן להיווכח בכך שהעמדה העקרונית העולה ממקורות רבים תומכת דווקא בגישה שלעיתים יש להמעט בדיבור. "סייג לחכמה שתיקה"¹⁸⁸ אמרו חכמים, ואם ערכה של "מילה בסלע - שתיקה בשניים"¹⁸⁹ רבן שמעון בן גמליאל העיד על עצמו, "כל ימי גדלתי בין החכמים, ולא מצאתי לגוף טוב משתיקה... וכל המרבה דברים מביא חטא"¹⁹⁰.

הרמב"ם¹⁹¹ דן בהרחבה בתפיסה זו ומעמת אותה עם גישת הפילוסופים היוונים. מסקנתו של הרמב"ם היא ש"רוב הדיבור מותרות וחטאים", ולכן "מסימני החכמים מיעוט הדברים... וריבוי הדברים מסימני הסכלים".

הרמב"ם סיווג את הביטוי לחמש קטגוריות: "מצווה, ואסור, ומאוס, ואהוב, ומותר". דיבור אסור הוא "עדות שקר וכזב ורכילות ומלשינות וקללה... נבלות פה ולשון הרע", והדיבור המאוס הוא "הדיבור אשר אין תועלת בו לאדם בנפשו ולא משמעת ולא מרי, כרוב סיפורי ההמון במה שארע ומה שהיה, ואיך מנהג מלך פלוני בארמונו, ומה הייתה סיבת מות פלוני או עושר פלוני".

מסיווג זה עולה, שהביטויים הנדונים במסמך זה יוגדרו על ידי הרמב"ם כביטוי אסור או מאוס, שאינו ראוי להגנה. ואכן, מדברי הרמב"ם הסיק ד"ר אביעד הכהן שקיים פער בין המשקל שניתן לחופש הביטוי במשפט המודרני לבין המשקל שניתן לו במשפט העברי.¹⁹²

6.2. הזכות לפרטיות וחובת הסודיות

ביטוי לערך הרב המיוחס להגנה על צנעת הפרט במסורת היהודית ישנו בברכתו של בלעם בן בעור לבני ישראל: "מה טובו אהליך יעקב, משכנותיך ישראל" (במדבר כד, ה), ברכה שנבעה מן הרושם העז שהותיר המבנה של מחנה ישראל במדבר על בלעם, "שראה פתחיהם שאינן מכוונין זה מול זה"¹⁹³.

עיקרון זה של השמירה על פרטיות הזולת ועל צנעת חייו היה יסוד מוצק להלכות רבות, החל מהלכות הנוגעות לשמירת סוד שיחו של אדם, סודותיו המסחריים ומסמכיו הפרטיים מפני עין זרה, וכלה בדיני התכנון והבניה.¹⁹⁴

על הפסוק שבראש ספר ויקרא (ויקרא א, א): "וידבר ה' אליו מאהל מועד לאמור" נאמר בתלמוד: "מנין לאומר דבר לחברו שהוא ב"בל יאמר", עד שיאמר לו: "לך אמור"? שנאמר: "וידבר ה' אליו מאהל מועד

¹⁸⁷ באר הגולה ירושלים תשל"א, באר שביעי, קנ-קנא

¹⁸⁸ משנה אבות פרק ג, משנה יג.

¹⁸⁹ ע"פ מדרש רבה (וילנא) ויקרא פרשה טז, אות ה'.

¹⁹⁰ משנה אבות פרק א, משנה יז.

¹⁹¹ פירוש המשניות אבות, פרק א, משנה טז.

¹⁹² אביעד הכהן, "המשפט העברי וחירות הביטוי - על עקרונות חופש הביטוי ומגבלותיו במשפט העברי", פרשת השבוע (הוצאת משרד המשפטים ומכללת שערי משפט) גיליון מס' 205.

¹⁹³ פירוש רש"י במדבר כד, ה.

¹⁹⁴ להרחבת העיון בנושאים אלו, ראו נחום רקובר, ההגנה על צנעת הפרט, ירושלים תשס"ו (להלן: רקובר, צנעת הפרט); איתמר ורפהטיג, צנעת אדם משפטי ארץ, עפרה תשס"ט.



לאמור¹⁹⁵. מדברים אלה עולה עיקרון כללי שלפיו, 'ברירת המחדל' בכל הנוגע למידע הנמסר מאדם לחברו היא, שעל המידע חלה חובת סודיות, ומקבל המידע אינו רשאי להפיצו לאחרים.

אכן, יש הסוברים שזוהי הוראה מוסרית בלבד, שאין לה מעמד של הלכה מחייבת, ויש הסוברים שזוהי אמנם הלכה מחייבת, אך היא חלה רק כאשר לפי נסיבות העניין יש להניח שמוסר המידע מקפיד על כך שהמידע לא יימסר לאחרים.¹⁹⁶

כך או אחרת, ברור מן המקורות שמסירת מידע אישי שהופקד בידיו של אדם היא אסורה לפי המשפט העברי, אף אם חובה זו לא צוינה במפורש בהסכם ההתקשרות שבין הספק למשתמש.

6.3. אנונימיות ולשון הרע

פרסום לשון הרע בחסות האנונימיות לא נולד עם התפתחותה של רשת האינטרנט. במאה ה-19, היו שביקשו לפרסם השמצות תחת מעטה אנונימי באמצעות כתבי פלסטר שהודבקו על קירות הבתים. רבי ישראל מאיר הכהן מראדין, מן הבולטים שבפוסקי ההלכה ובעלי המוסר במאה ה-19, שזכה לכינוי "החפץ חיים" בזכות ספרו 'חפץ חיים' שבו ריכז את כל הלכות לשון הרע ורכילות, התייחס לתופעה זו בחריפות רבה. לדבריו הפסוק "ארור מכה רעהו בסתר" (דברים כז, כד) מכוון במיוחד אל "אותן כותבי עמל (שקורין פאשקווילין), שעליהם נאמר ארור מכה רעהו בסתר והכל הוא כדי שלא יוכל להישמר ממנו, ויוכל להזיקו".¹⁹⁷

הפגיעה בזולת היא חמורה, אך חמורה ממנה הפגיעה בסתר, שאינה מאפשרת לנפגע להתמודד מול הפוגע ולתבוע את עלבונו.

לאנונימיות יש משקל משמעותי בהלכות לשון הרע, גם בשל המשקל שניתן לביטוי האנונימי. אחד העקרונות המרכזיים בהלכות לשון הרע הוא, שכאשר הפגיעה בשמו הטוב של הזולת נועדה לתועלת, הדבר מותר.¹⁹⁸ בהקשר זה מסביר רבנו יונה גירונדי, בן המאה ה-13, שיש יתרון לפרסום הגלוי על פני הפרסום האנונימי. לדבריו, כאשר מספר אדם בגנותו של הזולת בפרהסיא, אם כוונתו היא לתועלת אין בכך משום לשון הרע, כי "הכל יודעים שאין אדם כשר מספר דבר שקר ברבים",¹⁹⁹ ומשום כך יאמינו לדברים ויידעו להיזהר מפני עושי עוולה. אולם, כאשר אדם מסתתר מאחורי מעטה האנונימיות, דבריו אינם נתפסים כמהימנים די הצורך כדי שיניעו את הציבור לפעולה, ובשל כך אין בכוחם להפיק את אותה התועלת שניתן להפיק מפרסום שאינו אנונימי.

היבט נוסף נוגע לכוונתו הסובייקטיבית של המפרסם. ההלכה היהודית אינה מתירה פרסום לשון הרע, אף שיש בו כדי להועיל, אם המפרסם אינו תם לב והפרסום לא נועד להגן על הציבור אלא לפגוע בזולת. בהקשר זה כותב רבנו יונה, שפרסום דבר בפרהסיא, בפני שלושה אנשים לפחות, מעיד על המפרסם שכוונתו היא "לקדם את העניין" ולהזהיר את הציבור, בעוד שפרסום בפני אדם אחד או שניים, ובוודאי שפרסום אנונימי, מעורר את החשד שהמספר "רוצה ליתן פגם לחבירו, ונהנה לספר לשון הרע".²⁰⁰

בהתאם לכך קובע הרב עזריאל אריאל, ש"המפרסם צריך לעמוד בגלוי מאחורי מה שהוא אומר, ולא

¹⁹⁵ תלמוד בבלי יומא ד ע"ב.

¹⁹⁶ ראו בהרחבה, רקובר, צנעת הפרט עמ' 66-74.

¹⁹⁷ שמירת הלשון, עמ' כח.

¹⁹⁸ ראו: חפץ חיים, הלכות לשון הרע, כלל ד, ס"ק לב; שם, כלל ט, סעיף ב; הלכות רכילות, כלל ט, סעיף ב.

¹⁹⁹ מובא בשיטה מקובצת בבא בתרא לט ע"ב, ד"ה 'כל'.

²⁰⁰ שם.



אכן, ישנם מצבים שבהם אין מנוס מן הפרסום האנונימי, כי ללא מעטה האנונימיות מי שמעוניין לפרסם מידע המזהיר מפני מעוול לא יאזור אומץ לפרסם את המידע. בנסיבות אלו, יש להניח שהפרסום האנונימי מותר, ואף ראוי. אולם, יש לבחון בזהירות רבה, האם יש בכוחו של הפרסום להניע את הציבור לפעולה שתגן עליו מפני עושי עוולה, או שמא יישאר הפרסום בגדר שמועה רעה ותו לא.

6.4. חשיפת זהות המעוול

שאלה בעניין חובתו של אדם לחשוף את זהותו של מעוול הופנתה לרב מנשה קליין, מפוסקי זמננו. השאלה עסקה בתלמיד שהזיק לרכוש של מוסד ציבורי וחברו יודע על כך. השואל ביקש לדעת, האם עליו לספר למנהלי המוסד את זהותו של המזיק לרכוש המוסד, או שמא, חשיפת זהותו של המעוול תיחשב כרכילות?²⁰²

בדבריו, דן הרב קליין בסוגיה התלמודית²⁰³ העוסקת בחובה למסור עדות בפני בית דין, חובה שמקורה בפסוק "אם לוא יגיד ונשא עונו" (ויקרא ה, א). הסוגיה קובעת שגם אדם יחיד היה עד לאירוע שבו עוסקת העדות, חייב להעיד על הידוע לו. זאת, על אף שבהתאם לדיני הראיות של המשפט העברי, אין בעדות של עד אחד בלבד כדי לחייב את הנתבע בדין. הסיבה לכך היא, שעדותו של עד אחד מספיקה כדי לחייב את מי שמעידים כנגדו לאמת את טענותיו בשבועה, ומאחר שייתכן שהנתבע יירתע מן השבועה ויעדיף להודות, הרי שיש תועלת בעדות זו, ולכן יש חובה למוסרה בפני בית הדין.

מסוגיה זו לומד הרב קליין עיקרון כללי, ולפיו, **כל אימת שניתן לעשות שימוש בעדות כדי להביא לפיצוי הנפגע, מוטלת על מי שיכול להעיד חובה למסור את עדותו בפני הערכאה המוסמכת לדון בדבר.**

בהתאם לעיקרון זה הוא הורה, שעל מי שידע את זהותו של המעוול מוטלת חובה למסור את המידע המצוי בידיו לערכאה המוסמכת על מנת לאפשר לנפגע להגן על זכויותיו, ואין בכך משום לשון הרע, רכילות או הפרה של חובת הסודיות.

יחד עם זאת, מן הראוי להעיר שהמשפט העברי מכיר בכך שלעיתים, מן הראוי להקריב את עניינו של היחיד לשם הגשמת יעדים חברתיים, ובהתאם לכך, לקבוע שראיות מסוימות ייחשבו כראיות חסויות, שלא ייחשפו בפני בית הדין, משום שחשיפתן עלולה לפגוע בערך חברתי.²⁰⁴

לפיכך, במידה ואמנם מוצאת החברה שהשמירה על פרטיות הגולש, בכל מצב ובכל תנאי הינה ערך חברתי שמן הראוי להגן עליו, ניתן לקבוע כלל הקובע שהמידע האישי על זהותו של הגולש ייחשב מידע חסוי, שאין לחשוף אותו, גם לא לשם הגנה על שמו הטוב או על קניינו של אדם אחר.

7. סוגיות נוספות לדין

מסמך זה מתמקד בליבתן של הצעות החוק הנוגעות לחשיפת פרטי מעוול: הזכות לפתוח בהליך לחשיפת פרטי המעוול והשיקולים שבית המשפט עשוי להתחשב בהם במסגרתו של הליך זה. בחקיקה, בפסיקה הזרה ובכתבי המלומדים בנושא זה עלו גם סוגיות משפטיות נוספות החורגות מהנושא העיקרי של מסמך זה ודורשות דיון נפרד. לשם השלמת התמונה, יוצגו סוגיות אלו בקצרה.

²⁰¹ הרב עזריאל אריאל, "לשון הרע במערכת ציבורית דמוקרטית (ב)", **צהר** ו' 23, בעמ' 40.

²⁰² **שו"ת משנה הלכות** חלק יב סימן שצה

²⁰³ **תלמוד בבלי** בבא קמא, נה ע"ב. וראו גם: **משנה תורה** הלכות עדות, פרק יז, הלכה ז; **שולחן ערוך**, חושן משפט כח, א.

²⁰⁴ להרחבה בעניין זה ראו: ירון אונגר, "האם לא יגיד? - על עדויות חסויות בדין התורה", **משפטי ארץ** ב (תשס"ה), עמ' 232.



7.1. חשיפת זהות בידי ספקי גישה למחשבים, מנהלי אתרים ואחרים

כפי שהוזכר לעיל,²⁰⁵ חשיפת זהותו של מעוול, כאשר העוולה בוצעה ממחשב של רשת מחשבים ציבורית, דורשת שיתוף פעולה לא רק מצד ספק שירותי הגישה לאינטרנט, אלא גם מצידו של ספק הגישה למחשבים (אוניברסיטה, אינטרנט קפה וכדומה). הצעות החוק שנדונו עד כה התייחסו אך ורק לספקי שירותי הגישה לאינטרנט. על כן עולה השאלה האם מן הראוי לעגן בחוק גם את חובתם של ספקי שירותי הגישה למחשבים לשתף פעולה עם הליך החשיפה, ואם לאו, האם אין בהסדרים המוצעים כדי להפוך את רשתות המחשבים הציבוריות למעין "ערי מקלט" לביצוע עוולות?

7.2. עילות החשיפה

הצעות החוק מתמקדות בחשיפת פרטי המעוול לשם קיום הליך אזרחי שבמסגרתו יוכל הנפגע לקבל סעד מהמעוול על הנזקים שנגרמו לו. עם זאת, יש לתת את הדעת לכך שישנן עילות נוספות שעשויות להצדיק את חשיפת פרטי המעוול. בראשן כמובן עומדת העילה של העמדה לדין פלילי, כאשר קיים חשד שגולש השתמש באנונימיות על מנת לבצע עבירה. ואולם, קיימות גם עילות שאינן קשורות בעוולה או עבירה, ובכל זאת, הן עשויות להצדיק חשיפת פרטי גולש אנונימי. להלן דוגמאות אחדות:

- גולש אנונימי כתב שידוע לו היכן נמצא רכוש של פלוני, שאבד ממנו. חשיפת פרטי הגולש עשויה לסייע במציאת האבידה.
 - פלונית גילתה שהיא מאומצת, אך היא מתקשה באיתור הוריה הביולוגיים. בפורום אינטרנטי מתכתב עמה אדם הטוען שהוא אביה, אך הוא מסרב לגלות את זהותו. האם תוכל פלונית לדרוש מספק השירות שימסור בידיה את פרטי הגולש?²⁰⁶
 - לעיתים, קיימות עילות חשיפה הקשורות בביצוע עוולה, אך המעוול אינו הגולש האנונימי, או שהעוולה לא בוצעה במסגרת הגלישה באינטרנט. למשל:
 - משתמש אנונימי מספר שהוא היה עד לתקיפת ראובן בידי צד שלישי, וראובן מעוניין לחשוף את זהותו, כדי לגלות דרכו את זהות התוקף.
 - משתמש אנונימי מספר בפורום שתקף את ראובן. ראובן, שהותקף מאחור, מעוניין לגלות את זהות התוקף כדי להגיש נגדו תביעה אזרחית, ולשם כך הוא מבקש לחשוף את זהות המשתמש.
- לאור זאת, יש מקום לדון בשאלה האם מן הראוי להסדיר הליך של זיהוי משתמש גם בנסיבות כאמור.²⁰⁷

²⁰⁵ ראו לעיל, לפני הציון להערה 6.

²⁰⁶ דוגמה נוספת נדונה לאחרונה בבית המשפט המחוזי בקליפורניה: בנק מקומי תבע את Google בשל סירובה לגלות זהותו של בעל כתובת Gmail, אשר בטעות קיבל הודעה שנשלחה על ידי עובד בנק. ההודעה האמורה כללה נספח ובו מידע חסוי של למעלה מ-1,000 מלקוחות הבנק, לרבות שמותיהם, כתובותיהם, מספר זיהוי לצורכי מס ומספר ביטוח לאומי. לא ידוע האם ההודעה הני"ל כלל נפתחה. הבנק תבע את Google כאמור, על מנת לקבל את המידע – ובכללו מענה לשאלה האם חשבון הדואר האלקטרוני פעיל אם לאו. ראו **Rocky Mountain Bank v. Google, Inc.**, Case No.: C 09-4385 PVT US District Court for the Northern District of California (September 18, 2009).

²⁰⁷ בהקשר זה, לא למותר להעיר, שהמלומדים Block, Gilborn, ו-Marion העירו שבקנדה, כפי שהודגם בפסקי הדין בעניין **Leahy** (לעיל, הערה 161) ו-Ventra (לעיל הערה 164), נעשה שימוש בצווי Norwich Pharmacal למטרות מגוונות בהרבה מאלו המוצעות בהצעת החוק, כגון: לשם מעקב אחר כספים ורכוש, לשם שמירה ושלטיה במסמכים בנקאיים, לשם שמירה או גילוי של ראיות ועוד. ראו: **Randall W. Block, Michael A. Marion and R.J. Gilborn**,



7.3. שמירת מידע ותוכנות המספקות אנונימיות

כפי שהוזכר לעיל, חשיפת זהותו של המעוול מותנית בכך שספקית האינטרנט תשמור מידע אודות זהותם של משתמשים אשר קיבלו ממנה כתובות IP. כיום, הספקיות אכן שומרות מידע שכזה, אך הן עושות זאת משיקוליהן, ולמעשה אין החוק מחייב אותן לנהוג כך.²⁰⁸ לפיכך, ייתכן שבעקבות אימוץ הצעת החוק, יבחרו ספקיות השירות למחוק נתונים מזהים של משתמשים. בהנחה שהמחוקק מעוניין לאפשר את חשיפת זהותו של מעוול אנונימי, מן הראוי לדון בשאלה, האם יש לחייב את ספקיות השירות לשמור את הנתונים בדבר זהות המשתמשים?²⁰⁹

שאלה קרובה נוגעת לשרתים ותוכנות הקיימים כבר היום, המאפשרים אנונימיות מלאה בגלישה באופן שימנע התחקות אחר זהותו של הגולש.²¹⁰ גם בעניין זה עשויה להתעורר השאלה, האם, לאור כוונת המחוקק לאפשר זיהוי של מעוול אנונימי, ראוי לאסור בחוק את השימוש באמצעים אלו או הצעתם של אמצעים לשמירה על האנונימיות המוחלטת?²¹¹

7.4. סוג המידע שייחשף

הצעת החוק מתמקדת במסירת פרטים שיכולים לסייע לחשיפת זהותו של המעוול. בהקשר זה יש להעיר, שבידי ספקיות השירות מצויים פרטים רבים על המעוול, החורגים מזיהוי הפורמאלי, כגון: כתובת מגורים, מספר תעודת זהות וכדומה. בארצות המשפט המקובל, נהגו בתי המשפט לצוות במסגרת מסירת צווי Norwich Pharmacal גם על מסירת פרטים מסוג זה, כל אימת שהדבר מוצדק ונחוץ לשם קידומה של התביעה כנגד המעוול.²¹² יש מקום לדון אפוא בשאלה, האם יש מקום לנהוג כך גם בישראל, או שמא יש לצמצם את גדרי החשיפה לזהותו של המעוול ותו לא?

"Sealed Ex Parte Norwich Orders: Safeguarding Against Abuse of the Pre-Action Disclosure Remedy"
Annual Review of Civil Litigation 225, at 230-233. (2003) (להלן: בלוק מריון וגילבורן, 2003)

²⁰⁸ בהקשר זה יש לציין את הדירקטיבה של האיחוד האירופי שהוזכרה לעיל משנת 2006, המחייבת את ספקי שירותי הגישה לאינטרנט לשמור מידע על זהות המשתמש לתקופה של 12 חודשים מיום שפרסם המשתמש תוכן מסוים (The Data Retention Directive 2006/24/EC). ביסודה, נועדה ההוראה להקל על המדינות החברות להילחם בטרור, אך למעשה, היא מאפשרת למשתמשים לדרוש מספקי הגישה לחשוף את זהותם של מעולים. לעניין זה ראו גם: [Silke Weiss, "Is an Internet Service Provider authorized to disclose my personal details to \(1\) third parties or \(2\) courts in the case of copyright infringement?"](#) (Detailed Answer for United Kingdom), Knowledge Base Copyright Law (KB:Law|©), Answer No. 156, Version: 16/07/2009 13:59

²⁰⁹ באופן עקרוני, ייתכן שבמידה וספק השירות מחק את נתוני המזהים של המעוול, יוכל הנפגע לתבוע את הספק במישרין, מכוח הדוקטרינה של נזק ראייתי (ראו א' פורת וא' שטיין, "דוקטרינת הנזק הראייתי: ההצדקות לאימוצה ויישומה למצבים טיפוסיים של אי-וודאות בגרימת נזקים", **עיוני משפט** כא(2) 191 (תשנ"ח) עמ' 191-211). ואולם, ספק רב אם בתי המשפט יקבלו את החלטה של דוקטרינה זו במקרים של מעשה שפגע בראיה, בשעה שעדיין לא היה בה כל צורך לשם ניהול הליך אזרחי.

²¹⁰ ראו למשל, **כאן**. לדין נרחב בנושא ראו, מסמך מרכז המחקר והמידע של הכנסת בנושא "שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה" (כתיבה: רועי גולדשמידט, 1 בינואר 2012)

²¹¹ לדין בשאלה זו, ראו למשל: Frances Brazier, Anja Oskamp, Corien Prins, Maurice Schellekens and Niek Wijngaards, "[Anonymity and Software Agents: an Interdisciplinary Challenge](#)", **Artificial Intelligence and Law**, Vol. 12, No. 1-2. (March 2004), pp. 137-157. (בגרסת האינטרנט, בעמ' 8. להלן: ברזיר ואחרים, אנונימיות וסוכני תוכנה)

וראו גם: **כהן וג'ברין, חשיפת זהותם**, עמ' 44; **בירנהק, הזכות לפרטיות**, עמ' 395-398.
²¹² כך המצב בקנדה, ראו: **בלוק מריון וגילבורן, 2003** בעמ' 231; **יו, 2007** בסעיף 50. כך גם המצב בבריטניה, ראו: Paul Matthews and Hodge M. Malek, **Discovery**, 2nd ed. (London: Sweet & Maxwell, 1992) at 22 ("It should be noted that disclosure of the wrongdoer's identity is not enough; the obligation extends to giving full information").
Straka (לעיל הערת שוליים 160), בסעיף 45 של פסק הדין.



הכנסת

תחום חקיקה ומחקר משפטי

7.5. חובת סודיות, פרטיות וחסיון

במסגרת הדיון בחשיפת פרטי המעוול מקובל להבחין בין שלוש דוקטרינות משפטיות קרובות אך שונות: חובת סודיות, פרטיות וחסיון.²¹³

חובת סודיות מקורה בחיוב חוזי שבין מוסר המידע למי שהמידע נמסר בידיו, והיקפה נקבע בהתאם לתוכנו של החיוב החוזי. חובה זו יכולה לקום מכוח פרסום מדיניות הפרטיות של האתרים ושל ספקי השירות, אם כי, כוחם החוקי של פרסומים מסוג זה מוטל לעיתים בספק. פרטיות היא זכותו של כל אזרח לכך שמידע אישי אודותיו לא יפורסם ברבים. בסיסה המשפטית של חובה זו הוא בחוק.

החסיון הוא קביעה סטטוטורית שלפיה אין למסור מידע מסוים, בשל כך שמסירת המידע פוגעת באינטרס ציבורי חשוב, כביטחון המדינה, שלום הציבור, רווחתו, בריאותו וכדומה. כאן חשוב להדגיש, שבניגוד לזכות לפרטיות, השוללת מסירת מידע בשל ההגנה על זכויות הפרט, החיסיון שולל את מסירת המידע בשל ההגנה על האינטרס הציבורי.

ההבחנות האמורות מעוררות את השאלה, האם דין אחד צריך להיות לספקי שירות שבינם לבין המשתמשים יש חיוב חוזי המקים חובת סודיות ולספקי שירות שבינם לבין המשתמשים לא קיימת חובה שכזו?²¹⁴ האם בנסיבות מסוימות יצדיקו שיקולים של חיסיון חריגה מהוראת החוק המאפשרת את חשיפת פרטיו של המעוול?

7.6. השימוש במידע שנחשף

מלומדים בארצות המשפט המקובל הביעו עמדה חד משמעית שלפיה אין לעשות במידע שנחשף שימוש, מחוץ לגבולותיו של ההליך שלטובתו התבקש המידע,²¹⁵ אך הוראה דומה לא קיימת בהצעת החוק. במצב דברים זה עשויות להתעורר השאלות: האם רשאי אדם לעשות שימוש במידע שנחשף בפניו למטרות שונות מאלו שלשמן הוא קיבל לידיו את המידע? האם בתי המשפט יוכלו לעשות שימוש במידע במסגרת הליך אחר?

7.7. חשיפה ביוזמת ספקי השירות

הצעת החוק מתמקדת בחשיפת פרטי המעוול על פי צו בית המשפט, ואימוצה יכול להוביל למסקנה המשפטית, שספקי שירותי הגישה לאינטרנט אינם רשאים למסור את המידע המצוי ברשותם מבלי שבית המשפט ציוה עליהם לעשות כן. עם זאת, יש לציין שבעולם קיים דיון ער בשאלה, האם יש לספקי הגישה זכות לחשוף את זהותו של מעוול מרצונם החופשי. בשל ההשלכות האפשריות של הצעת החוק לעניין זה, כאמור, נראה שיש לבחון, האם אכן מבקשים המציעים לשלול מספקי הגישה את הזכות לחשוף מרצונם את זהותו של המעוול,²¹⁶ ואם לאו, כיצד ניתן לעגן את סמכות בתי המשפט להורות

²¹³ להבחנות אלו ראו למשל: **בירנהק, הזכות לפרטיות**, עמ' 350; יו, 2003, סעיפים 60, 69.

²¹⁴ נושא זה נדון לא מעט בפסיקות בתי המשפט בארה"ב, והובעו בו דעות שונות ומגוונות. ראו לעניין זה: **Swartz v. Doe #1**, No. 08C-431 (Tenn. Cir. Ct., Davidson County, Oct. 8, 2009); **Sedersten v. Taylor**, No. 09-3031-CVS- GAF, 2009 WL 4802567 (W.D. Mo. Dec. 9, 2009); **McVicker v. King**, 266 F.R.D. 92 (W.D. Pa. 2010);

²¹⁵ **וואט, חוק ומדיניות**, עמ' 19.

²¹⁶ למשל, בבריטניה ספקי שירותי הגישה מנועים על פי חוק מלמסור את פרטיו המזהים של הגולש האנונימי מבלי שבית



לספקי הגישה לחשוף את זהותם של מעוולים, מבלי לפגוע בסמכותם לחשוף את המעוולים שלא על פי צו בית המשפט.

7.8. שיהוי והתיישנות

האם ניתן יהיה לדרוש חשיפה של פרטי מעוול גם לאחר שלוש שנים מיום פרסומו של תוכן פוגעני? יש הטוענים שמאחר שלכל התבטאות ברשת האינטרנט יש קיום משל עצמה, ומשעה שהועלה תוכן לאתר הוא זמין לכל וניתן להורידו בכל עת למחשב האישי של כל משתמש ולהעבירו ממשתמש למשתמש, יש להתאים את כללי השיהוי וההתיישנות למציאות זו ולאפשר לנפגע לדרוש חשיפה של פרטי המעוול גם זמן רב לאחר שהתוכן הפוגע הועלה לרשת. בעניין זה קיימות גישות שונות בפסיקת בתי המשפט במדינות השונות.²¹⁷

Silke Weiss, "[Is an Internet Service Provider authorized to disclose my personal details to \(1\) third parties or \(2\) courts in the case of copyright infringement?](#)" (Detailed Answer for United Kingdom), Knowledge Base Copyright Law (KB:Law|©), Answer No. 156, Version: 16/07/2009 13:59, בלגיה, צרפת, גרמניה, ספרד ושבדיה, ראו: prepared by Hunton & Williams, Brussels, November 2009, "Study on Online Copyright Enforcement and Data Protection", פולין ובריטניה, ראו: "Study on Online Copyright Enforcement and Data Protection in Selected Member States" (Netherlands, Poland, UK), prepared by Hunton & Williams, Brussels, April 2010.²¹⁷ לעניין זה ראו: DEFAMATION LAW, PAPER 3.1, "[The Modern-Day Soapbox: Defamation in the Age of the Internet](#)", Bryan G. Baynham, QC and Daniel J. Reid, pp. 3

