עומר טנא*

הסתכל בקנקן וראה מה יש בו: נתוני תקשורת ומידע אישי במאה העשרים ואחת

א. מבוא

המשפט מנהל מערכת יחסים מורכבת עם הטכנולוגיה. מצד אחד ידו של המשפט על העליונה, שכן הוא יכול לכפות על הטכנולוגיה להתאים את עצמה למידותיו או אף לאסור כליל את השימוש בה. כך, למשל, הצליחה תעשיית המוזיקה לחסל את שירות שיתוף הקבצים "נפסטר" ("Napster") בעקבות החלטה של בית משפט בקליפורניה, שלפיה "נפסטר" אפשר למשתמשיו להפר זכויות יוצרים;[1] ולהבדיל, כך הפך המשפט את הטכנולוגיה לייצור נשק גרעיני לסוד שמור שהפצתו היא עבירה חמורה בעולם כולו.[2] מן הצד האחר, הטכנולוגיה זריזה ודינמית מהמשפט; המשפט זקוק לדיונים מייגעים של מומחים, של פוליטיקאים ושל שופטים כדי להתקדם, ואילו הטכנולוגיה מזנקת על רגליהם הצעירות של נערים זריזים המפצחים אלגוריתמים במחשב האישי בחדר שבביתם.[3]

כדי לשמור על רלוונטיות בעולם טכנולוגי, על המשפט לסגל לעצמו את הדינמיות ואת הגמישות הנחוצות כדי להתמודד עם קצב ההתקדמות המסחרר של הטכנולוגיה. ואכן, ניצחונה של תעשיית המוזיקה על "נפסטר" התגלה כניצחון פירוס, שכן לא חלפו ארבע שנים והיא נאלצה להגיע שוב לבית המשפט העליון של ארצות הברית כדי "להכחיד" שירות חדש, "גרוקסטר" ("Grokster"), שאפשר אף הוא לגולשים לשתף קבצים באמצעות שימוש בטכנולוגיה חדשה.[4] ואילו כיום, חמש שנים – ועשרות אלפי תביעות – לאחר פסק הדין בעניין *Grokster*, מתמודדת תעשיית המוזיקה עם שיטפון של טכנולוגיות

* מרצה בכיר, בית הספר למשפטים, המסלול האקדמי המכללה למינהל. ברצוני להודות לפרופסור ניבה אלקין־קורן ולפרופסור מיכאל בירנהק על הערותיהם המועילות ועל ההזדמנות לפרסם בספר זה. תודתי נתונה גם לד"ר תמר גדרון ולעו"ד עמית אשכנזי על הערותיהם. כל האתרים הנזכרים במאמר נבדקו לאחרונה בינואר 2011.

1 A&M Records v. Napster, 114 F. Supp.2d 896 (N.D. Cal. 2000), *aff'd*, 239 F.3d 1004 (9th Cir. 2001).

2 International Atomic Energy Agency, Treaty on the Non-Proliferation of Nuclear Weapons, Apr. 22 1970, 21 U.S.T. 483, 729 U.N.T.S. 161, *available at* www.iaea.org/Publications/Documents/Infcircs/Others/infcirc140.pdf.

3 לעניין זה אין דוגמה מאלפת מהקמתה של "גוגל" בחדרם של לארי פייג' וסרגיי ברין במעונות הסטודנטים באוניברסיטת סטנפורד. ראו: John Battelle, The Search: How Google and its Rivals Rewrote the Rules of Business and Transformed our Culture 65–93 (2005).

4 Metro-Goldwyn-Mayer Studios v. Grokster Ltd., 545 U.S. 913 (2005) (להלן: עניין *Grokster*).

המאפשרות שיתוף קבצים מבוזר ללא גורם מרכזי מתאם, ובראשן פרוקוטול הרשת "ביטורנט" ("BitTorrent").[5] לעתים מתברר שהמשפט לחוד והמציאות לחוד. כידוע, גם האמנה למניעת הפצה של נשק גרעיני מתגלה כמשענת קנה רצוץ בהתמודדות עם תופעת ההפצה של טכנולוגיות גרעין.[6]

בפרק זה אציג מקרה מבחן להתגוששות בין המשפט לבין הטכנולוגיה באחד התחומים הנמצאים על קו שבר ידוע בין שתי הדיסציפלינות – הגנת הפרטיות.[7] הגנת הפרטיות בתקשורת, בתכתובת ובמידע מבוססת על שתי הבחנות יסודיות: האחת – הבחנה בין תוכן לבין נתוני תקשורת: תוכן של תקשורת זוכה להגנה רבה, בחוק ובחוקה, ואילו נתוני תקשורת מוגנים פחות; והאחרת – הבחנה בין מידע אישי לבין מידע שאינו אישי: מידע אישי כפוף למסגרת רגולטורית מקיפה, המסדירה את אופן איסוף המידע, את השימוש בו ואת העברתו הלאה, ואילו מידע שאינו אישי אינו כפוף לכללים אלה.

עם התפתחותן של טכנולוגיות תקשורת ושל מערכות מידע חדשות, הטשטשו ההבדלים בין תוכן לבין נתוני תקשורת ובין מידע אישי לבין מידע שאינו אישי. האם, למשל, רשימת כתובות של אתרי אינטרנט שבהם ביקר אדם היא בגדר תוכן או בגדר נתוני תקשורת? האם פרופיל מדויק של גולש באינטרנט, המסווג על פי מספר קוד אקראי, הוא בגדר מידע אישי אם לאו? הבחנות פורמליות אלה שוחקות את ההיגיון שביסוד המסגרת החוקית הקיימת והתוצאה היא שפרטיותם של יחידים נשחקת.

---

5 ראו: EFF, Electronic Frontier Foundation, RIAA v. The People (2008), *available at* www.eff.org/riaa-v-people.

6 Vejay Lalla, *The Effectiveness of the Comprehensive Test Ban Treaty on Nuclear Weapons Proliferation: A Review of the Nuclear Non-Proliferation Treaties and the Impact of the Indian and Pakistani Nuclear Tests on the Non-Proliferation Regime*, 8 Cardozo J. Int'l & Comp. L. 103 (2000); Richard Falk, Mary Kaldor, Randall C. Forsberg & George Perkovich, *Gone Nuclear: How the World Lost Its Way*, The Nation, Oct. 10 2006, *available at* www.thenation.com/article/gone-nuclear-how-world-lost-its-way.

7 חלוצי הגנת הפרטיות בעידן המודרני, סמואל וורן ולואיס ברנדייס, תלו את הצורך בהכרה בזכות המשפטית לפרטיות בהתפתחויות טכנולוגיות המאיימות על המרחב הפרטי:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops"; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, at note 10 (1890).

ראו גם: Omer Tene, *Privacy: The New Generations*, 1 Int'l Data Priv. L. 15 (2011); A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461 (2000).

בחלק הראשון בפרק זה אסקור את המסגרת המשפטית של הגנת הפרטיות בתקשורת ובתכתובת. אתאר את שני הצירים המרכזיים שסביבם התפתח הדיון: ההבחנה בין תוכן לבין נתוני תקשורת וההבחנה בין מידע אישי לבין מידע שאינו מוגדר ככזה. בחלק השני אבחן את המסגרת המשפטית לאור ההתפתחויות הטכנולוגיות. אראה כי ההבחנה בין תוכן לבין נתוני תקשורת היא תלויית טכנולוגיה: בעת משלוח מכתבים בדואר רגיל קל להבחין בין הכתוב במכתב לבין הכתוב על המעטפה, אולם במשלוח דואר אלקטרוני, בגלישה באינטרנט או בשימוש בטלפון סלולרי הבחנות אלה מִטשטשות. גם ההבחנה בין מידע אישי לבין מידע שאינו מוגדר ככזה מתערערת לנוכח יכולות כריית מידע (data mining) ויצירת פרופילים על סמך מידע "פסידונימי", מידע שאינו ניתן אולי לזיהוי אישי אך עלול להשפיע על ההתייחסות לאדם ספציפי.

טענתי היא כי שמירה על דינמיות ועל גמישות של המשפט מחייבת להימנע מכללים דיכוטומיים שאינם מתאימים למגוון המצבים המתקיים במציאות. דינם של כללים שאינם מתאימים למציאות הטכנולוגית הוא לא להיאכף, או להתפרש על ידי שופטים ורגולטורים בהתאם לנטיות לבם האישיות. התאמתם של הכללים לשלל גווניה של הסביבה הטכנולוגית היא היבט אחד של הניסיון ליצור הסדרים משפטיים ניטרליים לטכנולוגיה (technology neutral), בהתבסס על התובנה שלפיה דינם של כללים המותאמים לטכנולוגיות מסוימות לעבור מן העולם עם התפתחותן של טכנולוגיות חדשות.[8] מסגרת חוקית דינמית תושתת על עקרונות מהותיים של העצמת הפרט, להבדיל מהבחנות פורמליות שהן יסוד לכללים ביורוקרטיים הנאכפים על ידי רגולטורים.

ב. המסגרת המשפטית: הגנת הפרטיות בתקשורת ובתכתובת

אחד ההיבטים המסורתיים של הזכות לפרטיות הוא פרטיותו של אדם בתקשורת ובתכתובת. עוד בשנת 1000 לספירה (לערך) פסק רבנו גרשום כי אין לקרוא מכתב שנועד לאדם אחר.[9] בית המשפט העליון של ארצות הברית פסק ב־1877 כי החוקה אוסרת על רשויות המדינה לפתוח מכתבים וחבילות שנשלחו בדואר.[10] עם השנים השתכללו אמצעי התקשורת ונוספו כלי תקשורת כגון טלפון, טלפון סלולרי ואינטרנט. גם לאחר התפתחויות אלה, הגנת פרטיותו של אדם באמצעי התקשורת ממשיכה להיות מוכרת כזכות יסוד בכל שיטת משפט דמוקרטית,[11] והעדרה הוא מסימני ההיכר המובהקים של משטר טוטליטרי.[12]

8 ראו למשל: Lyria B. Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. Ill. J.L. Tech. & Pol'y 239.

9 נחום רקובר **ההגנה על צנעת הפרט** פרק 3 (2006).

10 *Ex Parte* Jackson, 96 U.S. 727 (1877).

11 ראו: Convention for the Protection of Human Rights and Fundamental Freedoms (להלן: ECHR) art.8, Nov. 4, 1950, 213 U.N.T.S. 221; התיקון הרביעי לחוקת ארצות הברית: U.S. Const. amend. IV; ס' 7 לחוק יסוד: כבוד האדם וחירותו, התשנ"ב-1992, ס"ח התשנ"ב 1391.

12 ראו, למשל, הסרט הגרמני "חיים של אחרים": Das Leben der Anderen (2006). בסרט תועדו החיים בצל עינה הפקוחה ואוזנה הכרויה של המשטרה החשאית של מזרח גרמניה,

כאמור, הזכות המשפטית לפרטיות בתקשורת ובתכתובת נסבה סביב שני צירים מרכזיים: הבחנה בין תוכן לבין נתוני תקשורת והבחנה בין מידע אישי לבין מידע שאינו כזה. מכוח ההבחנה בין תוכן לבין נתוני תקשורת (traffic data), הידועים גם כנתוני מעטפת, מוענקת לתוכן הגנה חזקה יותר בחוק, ולעתים גם בחוקה. התוכן הוא הטקסט המופיע במכתב או המושמע במהלך שיחת הטלפון; נתוני התקשורת הם כתובתו של הנמען או מספר הטלפון ומשך השיחה. אינטואיטיבית, נראה כי לא בכדי מסתיר אדם את תוכנו של מכתב באמצעות מעטפה אך חושף את כתובת הנמען שעליה – עניינו של אדם בפרטיות התוכן חזק מעניינו בפרטיות נתוני התקשורת. התוכן שמור לנמען או לבן השיח בלבד, ואילו נתוני התקשורת חשופים בפני הדוור ובפני חברת הטלפון.

מכוח ההבחנה האחרת שבה עסקינן מוענקת למידע אישי (Personal Data) הגנה חוקית, ולעתים גם חוקתית. בשיטת המשפט האירופית מידע אישי, המוגדר ככל מידע על אודות אדם מזוהה או הניתן לזיהוי באמצעים סבירים, מוגן הגנה חוקתית, בחוק וברגולציה.[13] אף על פי שבארצות הברית מסגרת החוק המגנה על מידע אישי "רזה" יותר מאשר באירופה, מעוגנת ההגנה על מידע אישי (Personally Identifiable Information או PII) בהסדרים חוקיים מגזריים[14] או בדרך של הסדרה פרטית, כלומר באמצעות חוזים וכללי התנהגות מוסכמים (Code of Practice) של ארגוני תעשייה שונים. ההגנה על מידע אישי מתבטאת לאו דווקא בחובה לשמור על סודיות המידע אלא בכללים לאיסוף הוגן של מידע אישי, לאגירתו, לשימוש בו ולהעברתו.[15] בחלק זה אעמוד על שתי ההבחנות שביסוד ההגנה על פרטיות בתקשורת ובתכתובת בישראל, בארצות הברית ובאנגליה.

1. הבחנה בין תוכן לבין נתוני תקשורת

(א) *הדין הישראלי*

ההבחנה בין הגנת הפרטיות החלה על תוכן שיחה לבין פרטיות נתוני התקשורת באה לידי ביטוי בפער שבין הוראות חוק האזנת סתר[16] לבין הוראות חוק סדר הדין הפלילי (סמכויות

השטאזי. ראו גם דו"ח ארגון "Privacy International" על מצב הפרטיות בסין: Privacy International, *PHR2006 - People's Republic of China* (Dec. 18, 2007), *available at* www.privacyinternational.org/article.shtml?cmd[347]=x-347-559508.

13 ECHR, לעיל ה"ש 11; Council Directive 95/46, Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (EC) (להלן: "דירקטיבת 95/46"); Council Directive 2002/58, Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) (EU), (להלן: "דירקטיבת 2002/58").

14 מאגרי מידע של חברות המספקות שירותים פיננסיים: Gramm-Leach-Bliley Act of 1999, Pub. L. No. 102–106, 113 Stat. 1338 (1999); מידע רפואי: Health Insurance Portability and Accountability Act, Pub. L. 104–191, 110 Stat. 1936 (1996) (להלן: HIPAA); שירות נתוני אשראי: Fair Credit Reporting Act, Pub. L. No. 90–321, 15 U.S.C. § 1681 et seq. (2000) (להלן: FCRA).

15 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006).

16 חוק האזנת סתר, התשל"ט-1979, ס"ח 938 (להלן: "חוק האזנת סתר").

אכיפה – נתוני תקשורת).[17] חוק האזנת סתר עוסק בתוכנן של שיחות; חוק נתוני תקשורת, כשמו כן הוא, עוסק בנתוני תקשורת המוגדרים כ"נתוני מיקום, נתוני מנוי או נתוני תעבורה, והכל **למעט תוכנו** של מסר בזק".[18] חוק האזנת סתר קובע כי האזנה שלא כדין לשיח הזולת היא עבירה פלילית שהעונש בגינה הוא חמש שנות מאסר; העונש המרבי בגין הפרת הוראותיו של חוק נתוני תקשורת הוא שלוש שנות מאסר. חוק האזנת סתר מחייב צו של נשיא בית משפט מחוזי כדי להתיר למשטרה לבצע האזנת סתר, וצו כזה יינתן רק אם הדבר "דרוש לגילוי, לחקירה או למניעה של עבירות מסוג פשע";[19] חוק נתוני תקשורת מסמיך שופט שלום להתיר למשטרה לקבל נתוני תקשורת מספקית שירותי תקשורת למטרת גילוי עבירות מסוג פשע או עוון, חקירתן או מניעתן.[20] חוק האזנת סתר כולל הוראת פסלות ראיות, שלפיה "דברים שנקלטו בדרך של האזנת סתר בניגוד להוראות [ה]חוק [...] לא יהיו קבילים כראיה בבית משפט";[21] חוק נתוני תקשורת אינו כולל הוראה דומה.

אמנם, בעניין תוכנו של חוק נתוני תקשורת ניטשה מחלוקת עזה; מחלוקת זו הגיעה לכלל עתירה לבג"ץ כנגד חוקתיותו של החוק, עתירה שהגישה האגודה לזכויות האזרח ואליה הצטרפה לשכת עורכי הדין.[22] אולם גם מבקרי החוק נוטים להסכים כי ההגנה שיש להבטיח לנתוני תקשורת צריכה להיות פחותה ברמתה מן ההגנה המוענקת לתוכן שיחות.[23]

17 חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007, ס"ח 2122 (להלן: "חוק נתוני תקשורת").

18 ס' 1 לחוק נתוני תקשורת (ההדגשה שלי – ע' ט').

19 ס' 6 לחוק האזנת סתר; תיתכן גם האזנת סתר למטרת בטחון המדינה: ס' 4–5 לחוק האזנת סתר.

20 ס' 2–3 לחוק נתוני תקשורת.

21 ס' 13 לחוק האזנת סתר.

22 בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (להלן: עניין **האגודה לזכויות האזרח**; במועד כתיבת פרק זה הועברה העתירה לדיון בפני הרכב שופטים מורחב אך טרם ניתן פסק דין). חוק נתוני תקשורת כונה בתקשורת "חוק האח הגדול"; ראו למשל שחר אילן "אושר 'חוק האח הגדול' – המשטרה תקים מאגר מידע הגדול במערב" **הארץ** Online **20.12.2007 משפט ופלילים** www.haaretz.co.il/hasite/pages/ShArtPE.jhtml?ite mNo=935772&contrassID=2&subContrassID=. ראו עוד מכתב מיכאל בירנהק, יו"ר הוועדה המשפטית, המועצה הציבורית להגנת הפרטיות, ועומר טנא, בית הספר למשפטים, המסלול האקדמי המכללה למינהל, לוועדת החוקה, חוק ומשפט של הכנסת (13.8.2007) (בנושא הערות המועצה הציבורית להגנת הפרטיות להצעת החוק לתיקון פקודת סדר הדין הפלילי [מעצר וחיפוש] [מס' 13] [קבלת נתוני תקשורת וקבצי נתונים ממאגר מידע של בעל רישיון בזק], תשס"ו–**2006**), www.knesset.gov.il/committees/heb/material/data/H13-08-2007_9-11-23_birenhak.doc.

23 כך, למשל, דורשות העותרות בעניין **האגודה לזכויות האזרח** "להדק" את התנאים המאפשרים את קבלתם של נתוני תקשורת של מנוי, להבטיח הגנה על שיחות חסויות על פי דין ולמנוע את הקמתו של מאגר נתוני תקשורת שיוחזק בידי המשטרה, אך הן אינן דורשות להכפיף את ההליך לקבלת נתוני תקשורת להוראותיו של חוק האזנת סתר. ואולם ראו מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 34–36 (2007).

(ב) *הדין האמריקני*

הפער בין ההגנה המוענקת לתוכן תקשורת לבין ההגנה על נתוני תקשורת בולט גם בארצות הברית, הן במישור החוקתי הן במישור החוקי. במישור החוקתי מעוגנת ההגנה על פרטיות בתקשורת ובתכתובת בתיקון הרביעי לחוקה.[24] לפי הדוקטרינה החוקתית שהתפתחה במשך עשרות שנים בארצות הברית ובאה לידי ביטוי מובהק בפסק הדין הידוע בעניין *Katz*, יש להגן על פרטיותו של אדם במקום שבו הוא עשוי לפתח "ציפייה סבירה לפרטיות".[25] מבחן "הציפייה הסבירה לפרטיות" הוא מבחן מעורב, סובייקטיבי (פוזיטיבי) ואובייקטיבי (נורמטיבי). סובייקטיבי, שכן יש לבדוק אם האדם אכן פיתח "ציפייה לפרטיות" בנסיבות העניין; אובייקטיבי, שכן אין די בציפייה לפרטיות – היא חייבת להיות ציפייה "סבירה", וסבירות הוא כידוע מונח שסתום שמצריך הפעלת שיקול דעת שיפוטי.[26]

בית המשפט העליון האמריקני קבע בסדרת הלכות חשובות כי אף שלאדם יש "ציפייה סבירה לפרטיות" בתוכן של תקשורת, נתוני תקשורת אינם מקימים ציפייה סבירה כזאת. אם כן, ההגנה החוקתית על פרטיות תקשורת אינה משתרעת על נתוני תקשורת והיא מוגבלת לתוכן בלבד.[27] ההנמקה העיקרית בבסיסן של החלטות אלה היא כי מאחר שנתוני התקשורת נמסרים לידי ספקית שירותי התקשורת וחשופים לעיני עובדיה, אין לאדם ציפייה סבירה לפרטיות בכל הנוגע למידע זה.[28] אדם שמוסר מידע לידיה של חברת תקשורת המעסיקה עשרות אלפי עובדים "נוטל על עצמו את הסיכון" כי החברה או מי מעובדיה יעבירו את המידע הלאה, אולי גם לחוקרי משטרה. הנמקה זאת מבוססת על האמרה המיוחסת לבנג'מין פרנקלין, שלפיה "שלושה יכולים לשמור סוד רק אם שניים

24 בתיקון הרביעי לחוקת ארצות הברית נקבע כך:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized ;U.S. Const. amend. IV.

25 Katz v. United States, 389 U.S. 347, 360–361 (1967) (Harlan, J., concurring).

26 ראו למשל: רונן שמיר "הפוליטיקה של הסבירות: שיקול דעת ככוח שיפוטי" **תיאוריה וביקורת** 5, 7 (1994).

27 ראו בעיקר: United States v. Miller, 425 U.S. 435 (1976) (להלן: עניין *Miller*);Smith v. Maryland, 442 U.S. 735 (1979) (להלן: עניין *Smith*).

28 בעניין *Miller* (לעיל ה"ש 27, בעמ' 443) קבע בית המשפט העליון כך:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

מהם מתים";[29] אולם היא מתעלמת מכך שהמידע נמסר לחברת התקשורת מתוך אמונה וציפייה כי זו לא תעשה בו שימוש אלא למטרות מתן השירות.[30] מכתב נמסר לדוור כדי שזה ישגרו ליעדו, ולא כדי שיעשה כל שימוש אחר בנתוני המעטפה. באופן דומה, לפחות מבחינה סובייקטיבית רובנו איננו מעוניינים או צופים שחברת הטלפון תשתמש באופן כלשהו בנתוני החיוג שלנו למעט למטרות גבייה, או ש"גוגל" תמכור למפרסמים ניתוחים של שאילתות החיפוש שלנו. אנו מוסרים את המידע לדוור, לחברת הטלפון או ל"גוגל" מתוך ציפייה והנחה ש"יישאר בינינו". מסירת המידע לצד שלישי למטרות שיווק, חקירה פרטית[31] או אכיפת חוק היא בגדר הפרת אמון על ידי מוסר המידע.[32]

גם במישור החוקי בולטת בארצות הברית ההבחנה בין תוכן לבין נתוני תקשורת. בחוק האזנת סתר האמריקני, ה־Wiretap Act, הנכלל בהוראותיו של ה־Electronic Communications Privacy Act (ECPA), נקבעו דרישות מחמירות במיוחד לקבלת היתר להאזין לתוכן של שיחה.[33] צו האזנת סתר ניתן רק על ידי שופט בית משפט פדרלי מחוזי או בית משפט לערעורים, לאחר שנוכח לדעת שקיימת עילה סבירה לכך:

> [T]here is probable cause [to believe] that an individual is committing, has committed, or is about to commit a particular offense [… and that] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

מבחן "העילה הסבירה" ("Probable Cause") הוא מבחן דווקני וצר, במיוחד בהשוואה למבחן המופעל לקבלת צו לחשיפת נתוני תקשורת, שלפיו די אם הנתונים "רלוונטיים לחקירה מתנהלת".[34]

---

29 www.quotationspage.com/quote/27739.html.

30 לביקורות על עניין *Miller* ועל עניין *Smith* (לעיל ה"ש 27), ראו: Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1135 (2002); Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1397–1412 (2004); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 Mich. Telecomm. Tech. L. Rev. 61, 78 (2000); Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 Hastings L.J. 1303 (2002); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 Minn. L. Rev. 1325 (2002).

31 ראו למשל ע"פ 9893/06 **אלון־לאופר נ' מדינת ישראל** (טרם פורסם, 31.12.2007).

32 Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 Utah L. Rev. 1433 (2008); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L.J. 123 (2007).

33 Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2520 [2000 & Supp. II 2002]) (להלן: ECPA).

34 18 U.S.C. § 3122(b)(2)(1986).

בדומה לחוק האזנת סתר הישראלי, נקבע ב־Wiretap Act כלל פסלות ראיות להאזנות שבוצעו שלא כדין;[35] לעומת זאת, חוק נתוני תקשורת האמריקני, ה־Pen Register Act, שנכלל אף הוא בהוראות ה־ECPA, אינו כולל הוראה דומה.[36] דינו של מפר ה־Wiretap Act הוא חמש שנות מאסר; עונש המאסר המרבי מכוח ה־Pen Register Act הוא שנת מאסר אחת.[37] בעקבות אירועי 11 בספטמבר נחקק בארצות הברית ה־USA PATRIOT Act,[38] המרחיב את תחולתו של ה־Pen Register Act ומחיל אותו על נתונים המכונים "DRAS" ("dialing, routing, addressing, or signaling information").[39] מטרת החוק היא להתאים את הגדרת "נתוני תקשורת" שנקבעה ב־1986 (לפני עידן האינטרנט) לטכנולוגיות תקשורת חדשות, מבלי להרחיבה לתוכן שנותר בתחום ה־Wiretap Act.

(ג) *הדין האנגלי*

ההבחנה בין ההגנה המוענקת לתוכן לבין ההגנה על נתוני תקשורת באה לידי ביטוי גם בדין האירופי. באנגליה, למשל, מוסדר נושא האזנות הסתר ב־Regulation of Investigatory Powers Act (RIPA).[40] סעיף 1 ל־RIPA אוסר על "יירוט" תוכנה של תקשורת ללא צו ומטיל עונש מאסר של שנתיים על המפר הוראה זאת. שר הפנים מוסמך להוציא צו להאזנת סתר אם הדבר נחוץ לצורך מניעה של "פשע חמור", לשם חקירתו או מטעמים של הגנה על ביטחון המדינה או על יציבותה הכלכלית.[41] הביקורת על סמכותו של שר הפנים מסורה לנציב ההאזנות, ועל החלטותיו קיימת זכות ערעור לבית דין מיוחד. תוכנה של האזנת סתר, אף אם הותרה כדין, אינו קביל בבית משפט[42] – לא מטעמים של הגנה על פרטיות הנאשם, אלא לשם שמירה על ביטחון המדינה והבטחת סודיותם של אמצעי החקירה.[43] עם זאת, בנסיבות מיוחדות יוכלו גורמי החקירה להעביר תוכן של האזנת סתר לידי התביעה או אף לעיונו של שופט.[44] הגישה לנתוני תקשורת מוסדרת בפרק נפרד

35 18 U.S.C. § 2518 (1968).

36 18 U.S.C. §§ 3121–3127 (1986) (2000 & Supp. II 2002).

37 18 U.S.C. § 3121(d) (1986).

38 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272.

39 18 U.S.C. § 3127(3)–(4) (2001).

40 Regulation of Investigatory Powers Act, 2000, c. 23 (Eng.) (להלן: RIPA).

41 שם, בס' 5.

42 שם, בס' 17.

43 לאחרונה המליצה ועדה ממשלתית לבטל כלל זה; ראו: Privy Council Review of Intercept as Evidence, Report, 2008, Cm 7324.

44 RIPA, לעיל ה"ש 40, בס' 18(7). מעניין לציין כי בשלוש הזדמנויות שונות קבע בית הדין האירופי לזכויות אדם כי דיני האזנת הסתר האנגליים מפרים את הזכות החוקתית לפרטיות המעוגנת בדין האירופי. ראו: Malone v. United Kingdom, A95 Eur. Ct. H.R. 5 (1985); Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997); ולאחרונה: Liberty v. United Kingdom, App. No. 58243/00, 48 Eur. H.R. Rep. 1 (2008).

ב־RIPA. על פי סעיפים 21–25 לחוק, שורה ארוכה של פקידי ממשל (מרכזי ומקומי), לרבות חוקרי משטרה, רשויות מס ורשויות ביטחון שונות,[45] מוסמכת לדרוש מספקיות שירותי תקשורת נתונים על אודות לקוחותיהן בהתקיים מגוון רחב יחסית של נסיבות.[46] אירועי 11 בספטמבר הותירו את חותמם גם על הדין האנגלי בהקשר זה. בפרק 11 של ה־Anti-Terrorism, Crime and Security Act 2001 (ATCSA) נקבעו הסדרים המטילים על ספקיות השירות חובה לאגור נתוני תקשורת לצורך שימוש אפשרי בידי רשויות אכיפת החוק.[47] בשנת 2006 אימץ האיחוד האירופי הסדר מקביל ל־ATCSA, המחייב את ספקיות שירותי התקשורת בכל מדינות אירופה ליצור מאגר נתוני תקשורת ולהחזיקו לתקופה של בין שישה לעשרים וארבעה חודשים.[48] הסדר זה אומץ אל הדין האנגלי ב־The Data Retention (EC Directive) Regulations 2007.[49]

הנה כי כן, במשפט הישראלי כמו גם בדין האמריקני והאירופי, ניכר פער בין ההגנה הרבה שמעניקים חוקי האזנות הסתר לתוכנה של תקשורת לבין ההגנה הפחותה המוענקת לנתוני תקשורת. ראשית, הדרישות שיש לעמוד בהן כדי לקבל צו להאזנת סתר מחמירות לעומת אלה הנחוצות לשם קבלת גישה לנתוני תקשורת. שנית, העונש בגין עבירה על חוקי האזנות הסתר חמור מזה המוטל בחוקי נתוני התקשורת. לבסוף, תוכן של האזנת סתר שהושג שלא כדין פסול בדרך כלל מלשמש ראיה בבית משפט, ואילו חוקי נתוני התקשורת אינם קובעים כלל פסלות דומה.

---

45 The Regulation of Investigatory Powers (Communications Data) Order, 2003, S.I 2003/3172 (U.K.), as amended by the Regulation of Investigatory Powers (Communications Data) (Amendment) Order, 2005, S.I 2005/1083 (U.K.) and the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order, 2006, S.I 2006/1878 (U.K.). בדוח שהגיש ב־2004 קבע נציב ההאזנות כך: "In addition to the agencies covered by Chapter I of Part 1 of RIPA, and the prisons (138 in number) there are 52 police forces in England, Wales, Scotland and Northern Ireland and 510 public authorities who are authorised to obtain communications data"; HC 549 93 Nov. 2005) at 5.

46 RIPA, לעיל ה"ש 40, בס' 22(2); החוק מאפשר לדרוש נתוני תקשורת אם אלה נחוצים לצורך הגנה על אינטרסים כגון ביטחון לאומי, שלום הציבור או בריאותו או טובתה הכלכלית של המדינה, וכן לשם מניעת פשע או לשם איתורו של עבריין.

47 Anti-Terrorism, Crime and Security Act, 2001, c.24, §§ 102–103 (Eng.) (להלן: ATCSA); חוק זה מאפשר לספקיות שירותי התקשורת להתקשר בהסדרים מוסכמים עם המדינה. ראו: The Retention of Communications Data (Code of Practice) Order 2003, S.I 2003/3175); ס' 104 לחוק מאפשר למדינה לאכוף חובות אגירת מידע גם ללא הסכמה.

48 Council Directive 2006/24, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) (EU) (להלן: "דירקטיבת 2006/24").

49 SI 2007/2199.

2. הבחנה בין מידע אישי לבין מידע שאינו אישי

מידע אישי על אודות בני אדם יחידים זוכה במשפט האירופי להגנה חוקתית.[50] מקורה של התפיסה האירופית בשיעור הקשה שנלמד במהלך המאה העשרים, כאשר משטרים אירופיים טוטליטריים בגרמניה, בגוש הסובייטי וברפובליקות שהרכיבו את יוגוסלביה השתמשו במאגרי מידע לצורך הטלת שלטון אימים על אזרחיהם, למטרות רדיפה של מיעוטים ולעתים אף להשמדתם.[51] ב־1995 נתקבלה באיחוד האירופי דירקטיבת הגנת המידע (95/46/EC),[52] דירקטיבה שהחילה הן על המגזר הפרטי הן על המדינה כללים לאיסוף של מידע אישי, לאגירתו, לשימוש בו ולהעברתו באופן הוגן, שהבטיחו את שמירת פרטיותם של "נושאי המידע" (data subjects). דירקטיבה 95/46 חייבה את מדינות האיחוד האירופי להקים נציבויות הגנת מידע עצמאיות (DPAs – Data Protection Authorities) שיופקדו על אכיפת החוק,[53] ואומצה בחקיקה בכל 27 מדינות האיחוד.[54]

בשנת 2002 נתקבלה באיחוד האירופי דירקטיבת הגנת הפרטיות באמצעי תקשורת אלקטרוניים, דירקטיבה המפרטת ומרחיבה את דירקטיבת הגנת המידע בכל הנוגע לספקיות שירותי תקשורת, אינטרנט וסלולר.[55] הנקודה הארכימדית של משטר הגנת המידע האירופי היא המונח "מידע אישי". דיני הגנת מידע חלים אך ורק על מידע אישי, המוגדר בסעיף 2 לדירקטיבה כך:

---

50 בס' 8 לחוקת האיחוד האירופי (הטעונה עדיין אשרור של המדינות החברות) נקבע כדלקמן:
(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority; Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1, *available at* www.europarl.europa.eu/charter/pdf/text_en.pdf.

51 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151, 1165–66 (2004); James Q. Whitman, *On Nazi 'Honor' and the New European 'Dignity'*, *in* Darker Legacies of Law in Europe: The Shadow of National Socialism and Fascism Over Europe and its Legal Traditions 243 (Christian Joerges & Navraj S. Ghaleigh eds., 2003).

52 דירקטיבת 95/46, לעיל ה"ש 13.

53 ראו למשל את אתר נציבות הגנת המידע הבריטית (ICO – Information Commissioner's Office): www.ico.gov.uk.

54 ראו: Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm. ראו למשל באנגליה: Data Protection Act, 1998, c. 29 (Eng.).

55 דירקטיבת 2002/58, לעיל ה"ש 13.

> [A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[56]

ההגדרה כוללת שני רכיבים: ראשית, מידע אישי הוא מידע **הקשור לאדם מזוהה או שניתן לזיהוי**. מידע אנונימי, שאי אפשר לקשרו לאדם מסוים, אינו כפוף למשטר הגנת המידע האירופי. כך, למשל, מידע טריוויאלי כגון מספר טלפון או מספר תעודת זהות הוא מידע אישי הזוכה להגנה, שכן הוא קשור בדרך כלל לאדם מסוים הניתן לזיהוי. לעומת זאת, מידע כגון "פלוני אלמוני הוא נרקומן חולה איידס עם נטייה גנטית לסרטן בלוטת הערמונית, הוא מקבל דמי אבטלה בסך 2,000 אירו בחודש ונוהג לרכוש בהם סמים" – אינו מידע אישי, כל עוד "פלוני אלמוני" אינו ניתן לזיהוי באמצעים סבירים. שנית, מידע אישי הוא מידע **על אודות אדם**. לצורך הגדרת המידע כמידע אישי חייב האדם להיות במרכז. בפסק הדין החשוב שניתן בבית המשפט לערעורים באנגליה בעניין *Durant*, קבע בית המשפט כי מסמכים שהכילו מידע על אודות עסקאות פיננסיות, שהוחזקו בידי רשות ניירות הערך האנגלית (ה־FSA) ואזכרו את מר דורנט, לא היו בגדר "מידע אישי" שלו,[57] אף על פי שלכל הדעות היה דורנט "אדם מזוהה או ניתן לזיהוי" באותם מסמכים. לגישתו של בית המשפט, המידע לא היה "על אודות מר דורנט" אלא על אודות עסקאות שערך מר דורנט עם בנק ברקליס ועל תלונות שהוגשו בהקשר זה לרשות ניירות ערך. בית המשפט קבע כי מידע אישי יוגדר כך: "[I]nformation that affects [a person's] privacy, whether in his personal or family life, business or professional capacity".[58] לדברי בית המשפט יראו מידע כמידע אישי על אודות אדם רק אם המידע הוא "ביוגרפי באופן משמעותי" (ולשם כך לא די במידע המאזכר את מעורבותו של אדם בעניין או באירוע ללא הקשר אישי משמעותי), או אם האדם נמצא במוקד (focus) המידע.[59]

לא בכדי ממשיכה סוגיית ההגדרה של "מידע אישי" להיות אבן שואבת לפרשנויות ולדיונים משפטיים־פילוסופיים על פי הדירקטיבה גם כיום, שלוש־עשרה שנים לאחר חקיקתה. במהלך שנת 2007 פרסמו "ועדת סעיף 29" האירופית (Article 29 Data Protection Working Party), המורכבת מנציבי הגנת המידע במדינות האיחוד ומופקדת על פרשנות החקיקה, ונציבות הגנת המידע הבריטית, ניירות עמדה מקיפים בדבר פרשנות המונח "מידע אישי", מונח הניצב בבסיס הפירמידה של דיני הגנת המידע.[60] חשיבות

56 דירקטיבת 95/46, לעיל ה"ש 13.

57 Durant v. Financial Services Authority, [2003] F.S.R. 28, [2003] EWCA Civ 1746.

58 שם, בס' 28 להחלטה.

59 שם, בס' 29 להחלטה.

60 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, Jun. 20, 2007, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (להלן: Article 29, WP 136); Information Commissioner's Office, Data Protection Technical Guidance: Determining what is personal data (Aug. 16, 2007), *available at* http://www.ico.gov.uk/upload/documents/

הגדרתו של מידע כמידע אישי, או אי־הגדרתו ככזה, רבה מאוד. איסוף מידע אישי מחייב להודיע על כך לנושאי המידע ולקיים הליך מסורבל של יידוע נציבי הגנת המידע;[61] מידע אישי חייב להישמר סודי ומאובטח;[62] מידע אישי חייב להימחק לאחר שסיים לשרת את המטרה שלשמה נאסף;[63] חלה חובה לאפשר לנושא המידע האישי לעיין בו ולדרוש לתקנו;[64] אין להעביר מידע אישי מאירופה לארצות הברית, למשל, מבלי להעמיד לשם כך מנגנונים חוזיים מורכבים בין הגורם המעביר לגורם המקבל, שמטרתם להבטיח את ההגנה על פרטיות האזרחים האירופים כפי שהם נהנים ממנה באירופה.[65] הוראות דומות אינן

library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf.

61 ס׳ 10 וס׳ 18–19 לדירקטיבת 95/46, לעיל ה״ש 13.

62 ס׳ 16–17 לדירקטיבת 95/46, לעיל ה״ש 13.

63 ס׳ 6(1)(e) לדירקטיבת 95/46, לעיל ה״ש 13. לאחרונה דרשה הנציבות האירופית (The European Commission) מ״גוגל״ למחוק את מאגר המידע שבידיה על אודות שאילתות החיפוש של הגולשים לאחר תקופה של לא יותר משישה חודשים; לעניין זה ראו: Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, Apr. 4, 2008, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

64 ס׳ 12 לדירקטיבת 95/46, לעיל ה״ש 13.

65 ס׳ 25–26 לדירקטיבת 95/46, לעיל ה״ש 13. ס׳ 25 לדירקטיבת 95/46 אוסר על יצוא מידע אישי מאירופה אלא אם דיני המדינה המייבאת מבטיחים ״רמה הולמת של הגנה״ למידע, בהתאם לעקרונות הדירקטיבה. הנציבות האירופית מוסמכת להכריז על מדינות כבעלות ״רמה הולמת של הגנה״. עד כה הוכרזו רק קנדה, שוויץ וארגנטינה, וכן כמה איים בתעלה הבריטית, כמדינות המקיימות את דרישת הסעיף. בינואר 2011 החליטה נציבות האיחוד האירופי להכיר גם בישראל כמדינה בעלת רמה הולמת של הגנה על פרטיות. ראו Commission Decision (2011/61/EU), on the adequate protection of personal data by the State of Israel (2011). יצוא מידע אישי למדינות אחרות הוא אסור, אלא אם מתקשרות מייצאת המידע ומייבאת המידע בהסכם התואם את הנחיות הנציבות, שלפיו מתחייבת מייבאת המידע לקיים את עקרונות הדירקטיבה ולהכפיף עצמה לסמכות השיפוט ולדין האירופי. לתנאי ההסכם העיקרי שאושר על ידי הנציבות ראו: Commission Decision 2004/915/EC, Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standardcontractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74 *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF; מאחר שארצות הברית אינה מוכרת כמדינה בעלת ״רמה הולמת של הגנה״, אך כוחה הכלכלי גדול מכדי להציב לה מגבלות סחר, הגיעו הנציבות האירופית ומשרד המסחר האמריקני להסדר מיוחד, המכונה הסדר ״Safe Harbor״ – במסגרתו יכולות חברות אמריקניות המעוניינות בכך להצהיר על התחייבותן לקיים את עקרונות הגנת המידע שבדירקטיבה, ורשות הסחר הפדרלית (ה־FTC) מוסמכת לאכוף על החברות את העמידה בהתחייבויותן, מכוח סמכותה למנוע מצגי שווא (misrepresentation) כלפי הצרכנים. להסדר ה־״Safe Harbor״ ראו: www.export.gov/safeHarbor. ל״יצוא״ הדין האירופי מכוח ס׳ 25–26 לדירקטיבת 95/46, ראו: Michael D. Birnhack, *The EU*

חלות על מידע שאינו בגדר "מידע אישי". כך, למשל, אם חברה אוספת מידע על הרגליהם של הגולשים באינטרנט והמידע נשמר כך שאפשר לייחסו בחזרה לנושאיו, מדובר במאגר של מידע אישי הכפוף לדיני הגנת המידע האירופיים. אם, לעומת זאת, תצליח החברה להראות שהמידע הנשמר במאגריה אינו ניתן לייחוס ל"אדם מזוהה או ניתן לזיהוי", לא יטילו הוראות הדין את משקלן הכבד על המאגר. כפי שאראה בהמשך, עם התפתחות הטכנולוגיה הופכת ההבחנה בין מידע אישי לבין מידע שאינו כזה לקשה, ולעתים אף לחסרת פשר.

(א) *הדין הישראלי*

גם הדין הישראלי מבחין בין מידע אישי למידע שאינו כזה. בישראל, כמו במדינות אירופה, ובניגוד לארצות הברית, נחקק חוק מקיף המסדיר את הגנת הפרטיות ואת ההגנה על המידע האישי, הן ביחס למדינה הן ביחס למגזר הפרטי. יתר על כן, חוק הגנת הפרטיות, המייחד פרק לטיפול במאגרי מידע,[66] הוא אחד מדברי החקיקה הראשונים בעולם שעסקו בנושא זה.[67] בכנסת ה־16 אף נדונה הצעה שלפיה לסעיף 7 לחוק יסוד: כבוד האדם וחירותו, המכריז על הזכות לפרטיות כעל זכות יסוד חוקתית, יוסף סעיף הגנת מידע שלפיו "אין אוספים מידע על פרטיותו של אדם ואין מחזיקים או מעבדים מידע כזה שלא בהסכמתו".[68] חוק הגנת הפרטיות מגביל בחלקו הכללי את השימושים המותרים ב"ידיעה על עניניו הפרטיים של אדם".[69] פרק ב לחוק, שדן במאגרי המידע, מגדיר "מידע" כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".[70]

Data Protection Directive: An Engine of a Global Regime, 24(6) Comp. L. & Sec. Rep. 508 (2008).

66 פרק ב לחוק הגנת הפרטיות, התשמ"א-1981, ס"ח 1011 (להלן: חוק הגנת הפרטיות). פרק ד, שהוסף לחוק הגנת הפרטיות בתיקון מס' 1 בשנת 1985, עוסק בהעברת מידע בין גופים ציבוריים.

67 לאמנה הבין־לאומית הראשונה בתחום זה, ראו: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Strasbourg, Jan. 1, 1981); חוק הגנת המידע הראשון בעולם נחקק במדינת הסה בגרמניה, ב־1970: Hessisches Datenschutzgesetz (HDSG), Oct. 7, 1970 GVBI. I, p. 625; החוק הגרמני הפדרלי נחקק ב־27 ינואר 1977: Bundesdatenschutzgesetz 1977 (BDSG), BGBI. I 1978, p. 201.

68 **נוסח מבואר של הצעות לחוקה** (ועדת החוקה, חוק ומשפט, הכנסת ה־16, בשבתה כוועדה להכנת חוקה בהסכמה רחבה, 2006).

69 בס' 2(9) לחוק הגנת הפרטיות נקבע כי "שימוש בידיעה על עניניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה" הוא פגיעה בפרטיות. בס' 4 נקבע כי פגיעה בפרטיות היא עוולה בנזיקין, ובס' 5 נקבע כי דינו של הפוגע במזיד בפרטיות זולתו הוא חמש שנות מאסר.

70 בס' 7 לחוק הגנת הפרטיות מוגדר "מידע רגיש" כך: "נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו".

החוק הישראלי מורכב למעשה מחיבור של שני "חוקים" נפרדים – חוק להגנת הפרטיות בהגדרתה "המסורתית", הכולל את עוולות הנזיקין של הפגיעה בפרטיות ואת איסור המעקב (פרקים א ו־ג לחוק להגנת הפרטיות);[71] וחוק מאגרי מידע, הכולל רגולציה של מאגרי מידע והעברות מידע בין גופים ציבוריים (פרקים ב ו־ד לחוק להגנת הפרטיות). לכל אחד מה"חוקים" המרכיבים את חוק הגנת הפרטיות סעיף הגדרות משלו – סעיף 3 בפרק א וסעיף 7 בפרק ב. מצב זה יוצר חוסר הרמוניה בביטויים המשמשים להגדרת "מידע אישי" בתוך החוק עצמו. כך, למשל, מגן פרק א לחוק על "ידיעה על עניניו הפרטיים של אדם" ועל "ענין הנוגע לצנעת חייו האישיים של אדם", ואילו פרק ב לחוק מגן על "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו" (הגדרת המונח "מידע") ועל "נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו" (הגדרת המונח "מידע רגיש", הזהה כמעט לחלוטין להגדרתו של המונח "מידע"). ואמנם, בינואר 2007 המליץ צוות בין־תחומי במשרד המשפטים, בראשות המשנה ליועץ המשפטי לממשלה יהושע שופמן, לשנות את ההגדרה הבסיסית בפרק ב לחוק הגנת הפרטיות, הגדרת "מידע", להגדרה "אירופית" שלפיה "מידע אישי" הוא "כל מידע אודות אדם מזוהה או הניתן לזיהוי באמצעים סבירים".[72]

מכל מקום החוק הישראלי, בדומה לדין האירופי, מגן על "מידע" ועל "ידיעה על עניניו הפרטיים של אדם". התיבה האחרונה זכתה לפרשנות מרחיבה בפסק הדין החשוב של בית המשפט העליון בעניין **ונטורה**.[73] באותו עניין קבע השופט בך כי גם מידע טריוויאלי לכאורה, כגון כתובת, מספר טלפון, מספר תעודת זהות או מספר חשבון בנק, הוא "ידיעה על עניניו הפרטיים של אדם" הראויה להגנה על פי החוק.[74] בכך פסע השופט בך במסלול שהתווה המשפט האירופי, המגן על מידע על אודות אדם מזוהה או שניתן לזיהוי מבלי לדון בשאלת חשיבותו של המידע או בשאלת אופיו האינטימי או ה"אישי"

71 ראו בעיקר ס' 2(1), (2), (3), (4), (6) ו־(11) לחוק הגנת הפרטיות. עוולות הפגיעה בפרטיות קוטלגו על ידי ויליאם פרוסר: William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960). פרוסר אף ניסח את העוולות כסעיפים במסגרת ה־Restatement; ראו: Restatement (Second) of Torts §§ 652A–652E (1997).

72 הצוות לבחינת החקיקה בתחום מאגרי המידע **דין וחשבון 20**, המלצה 3.1.4 (2007) (להלן: **דוח שופמן**). הצוות ציין שם כך: "החוק נוקט מונחים שונים בהקשרים דומים, דבר הגורם לאי אחידות בדברי החקיקה [...] השימוש במונחים שונים לכוונות דומות גורם לאי בהירות משפטית".

73 ע"א 439/88 **רשם מאגרי מידע נ' ונטורה**, פ"ד מח(3) 808 (1994).

74 שם, בעמ' 821. שאלה אחרת היא אם אפשר להסיק הסכמה מכללא לשימוש בידיעות מסוג זה. ואכן, השופט בך "מווסת" את היקף ההגנה למידע אישי באמצעות שסתום ההסכמה מכללא. הגנה זו זוכה מידיו לפרשנות מרחיבה מאוד. ובלשונו של השופט בך, שם: "מאחר שפירסומם של כל אותם פרטים, אשר לגביהם ניתנת הסכמה כאמור, במפורש או מכללא, לא יהווה פגיעה אסורה בפרטיות ולא יגרום אפו לכל סנקציה לגבי המפיץ או המפרסם, הרי עולה מכאן, כי אין חשש שהפירוש הרחב המוצע יביא לתוצאה קשה או אבסורדית".

(בלשון בלתי מקצועית). גם ההנמקה של השופט בך דמתה להנמקה שביסוד משטר הגנת המידע האירופי:

> חייבת להיות מודעות להשפעה הגוברת והולכת של המחשבים למיניהם ושל שילוב המידע של מחשבים שונים, במישור הלאומי ואף הבין־לאומי. כך, פירסום שמו ויתר פרטיו של אדם במאגר מידע, בגין שיק מסוים שלא כובד, עשוי לגרום להכללתו בעשרות רשימות שונות בארצות רבות ולהסב לו נזק בלתי משוער. הוא עשוי למצוא עצמו ברשימות שחורות לרוב, והדבר עלול לגרום לאיבוד אפשרות לגיוס כספים ולהרס כלכלי שלו ושל החברות המצויות בשליטתו.[75]

הגברת היכולות הטכנולוגיות המאפשרות לאגור מידע בהיקף אדיר ובעלויות שוליות על שבבים דקים משערה, להצליב את המידע עם מידע ממאגרים שונים, לחפש במידע ולמצוא פרטי־פרטים בתוך שבירי שנייה באמצעות טכנולוגיות הזמינות לכל אדם המחובר לאינטרנט (analytics) – כל אלה הופכים כל מידע, לרבות מידע שנראה טריוויאלי, לבעל פוטנציאל לפגוע בפרטיות. הראה לי את אזור החיוג שלך, את רשימת הקניות שלך בסופרמרקט ואת תדפיס שיחות הסלולר שלך – ואומר לך מי אתה, לעתים בצורה מדויקת יותר משתוכל אתה לומר בעצמך.

גם הרכיב הנוסף בהגדרה של מידע אישי – היותו של המידע מידע **על אודות אדם**, כלומר מידע שאדם מסוים נמצא ב"מוקדו", במובן של עניין *Durant* – קנה לו אחיזה בדין הישראלי, בפסק דינו של בית המשפט העליון בעניין **עוז**.[76] באותו עניין עלתה השאלה אם עדויות של מתלוננים בוועדת בדיקה אוניברסיטאית ראויות להגנת דיני הפרטיות כמידע אישי של אותם מתלוננים או כידיעות על ענייניהם הפרטיים. בהתבסס על הלכת ונטורה, קובעת השופטת חיות כך:

> ברמה הבסיסית ניתן לומר כי הזכות לפרטיות יכול שתתייחס למידע או לנתונים הנוגעים באופן מובהק לפרט ולו בלבד (עם מידע או נתונים כאלה נמנים למשל מצבו הרפואי, רמת הכנסותיו, גילו, משקלו, העדפותיו המיניות וכדומה), ויכול שתתייחס למידע או נתונים הנוגעים לפרט במגעיו עם אחרים (עם מידע או נתונים כאלה נמנים למשל תוכן של שיחה או התכתבות שקיים עם אחר, קשר בין־אישי שקיים עם אחר, אירוע טראומטי שחווה הקשור לאדם אחר ועוד). על פי גישה מרחיבה ניתן לומר כי כמעט כל נתון הנוגע לפרט ולו בלבד יכול להיחשב כמופע של הזכות לפרטיות.[77]

אולם השופטת חיות מוסיפה וקובעת, בתוך סטייה מהלכת ונטורה, את הדברים הללו:

---

75 שם, בעמ' 830.

76 בג"ץ 844/06 **אוניברסיטת חיפה נ' עוז** (טרם פורסם, 14.5.2008) (להלן: עניין **עוז**); לדיון בבית הדין הארצי לעבודה ראו ע"ע (ארצי) 371/05 **עוז – אוניברסיטת חיפה** (טרם פורסם, 19.12.2005).

77 עניין **עוז**, שם, בעמ' 28 לתדפיס ההחלטה.

> עם זאת, וככל שבנורמה המשפטית עסקינן, נראה לי כי הגדרה כה רחבה של הזכות לפרטיות אין לה הצדקה. כך לפחות **מקום שבו במוקד המידע או הנתונים אשר לגביהם מתבקשת הגנה עומדים אותם אחרים ואילו חלקו של הפרט המבקש הגנה לגביהם הוא שולי ביותר ומעמדו אינו עולה על זה של משקיף או צופה מן הצד** (אלא אם כן חשיפת עצם נוכחותו באירוע יש בה בנסיבות העניין כדי לפגוע בפרטיותו).[78]

כלומר, השופטת חיות אינה מסתפקת בנדבך הראשון של הגדרת מידע אישי – היות המידע קשור לאדם מזוהה או ניתן לזיהוי, שהרי אין ספק שהמתלוננים בעניין **עוז** היו אנשים מזוהים. בדומה לבית המשפט האנגלי לערעורים בעניין *Durant*, דורשת השופטת חיות לראות כי אותם אנשים המבקשים להגן על פרטיותם נמצאים **במוקד** המידע המוגן. במקרה דנן סברה השופטת כי מי שנמצא "במוקד המידע" הוא דווקא המרצה הנילון, ואילו המתלוננים נמצאים בשוליים, במעמד של "משקיף או צופה מן הצד". במילים אחרות, המידע על אודות נוכחותם של המתלוננים בהליך ועל אודות עדויותיהם הוא מידע אישי השייך לנילון ולא למתלוננים. בין אם תפיסתה של השופטת חיות מתאימה למצב העובדתי בנסיבות העניין ובין אם לאו, מדובר בעמדה מגובשת ומשמעותית בעניין פרשנות המושג הבסיסי בדיני הגנת הפרטיות הישראליים.

(ב) *הדין האמריקני*

רק בתחומי משפט מעטים עמדתה של ארצות הברית קוטבית לעמדה הנהוגה באירופה. דיני החוזים, דיני הקניין ודיני הנזיקין אינם שונים באופן מהותי משני עברי האוקיאנוס. אולם בכל הנוגע לפרטיות ולהגנה על מידע הפערים גדולים, והם גורמים להתנגשויות פוליטיות חוזרות ונשנות בין שני גושי הסחר הגדולים בעולם.[79] נקודת המוצא של דיני

78 שם, בעמ' 29 לתדפיס ההחלטה (ההדגשה שלי – ע' ט').

79 שתי פרשות הגיעו לכלל התנגשות דיפלומטית. בעניין אחד דרש המשרד האמריקני לביטחון פנים (DHS – Department of Homeland Security) מחברות תעופה אירופיות לספק פרטים אישיים של הנוסעים בטיסותיהן (PNR – Passenger Name Records) כתנאי לנחיתתן בשדות התעופה בארצות הברית. נציבי הגנת המידע האירופים הבהירו כי קיום דרישתו של המשרד האמריקני לביטחון פנים יגרום להפרה של דיני הגנת המידע האירופיים; ראו: Article 29 Data Protection Working Party, Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities, WP 132, Feb. 2007, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp132_en.pdf. הפרשה אף הגיעה לבית הדין האירופי העליון (ECJ) לאחר שהפרלמנט האירופי תקף הסדר פשרה שאליו הגיעו הנציבות האירופית והמשרד האמריקני לביטחון פנים; ראו: Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, 2006 E.C.J, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/judgement_ecj_30_05_06_pnr_en.pdf. בעניין אחר התגלה כי מסלקת הבנקים המובילה בעולם, "SWIFT", שהיא חברה בלגית, מעבירה מידע לרשויות הביטחון האמריקניות משרתי החברה הממוקמים בארצות הברית. ראו: Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data

הגנת המידע האירופיים היא כי מידע אישי הוא נחלת הפרט וכי השליטה בשימוש במידע ובהעברתו צריכה להישמר בידיו של הפרט. לעומת זאת, ההנחה ביסוד הדין האמריקני היא כי מידע אישי הנאסף במאגרי מידע הוא רכושו של בעל המאגר, נכס עובר לסוחר,[80] והוא כשמן בגלגלי כלכלת השוק, המבוססת על תנועה חופשית של מידע.[81] זאת ועוד; עצם המחשבה על הפקדת פרטיותו של האזרח בידי רגולטורים, מפקחי פרטיות והגנת מידע[82] מטעם המדינה (ה־DPAs),[83] מעוררת תמיהה בקרב משפטנים אמריקנים, האמונים על הגנת הפרטיות **מפני** המדינה ולא באמצעותה. בארצות הברית המדינה היא שנתפסת כאויבת הגדולה של הפרטיות, ואילו מנגנוני השוק ואמצעים טכנולוגיים נתפסים כפועלים להבטחת מידה רצויה (ויעילה) של פרטיות לאזרח.

עם זאת, גם בארצות הברית יש נפקות משפטית למונח "מידע אישי", או בגרסתו האמריקנית "מידע מזוהה אישית" (PII – Personally Identifiable Information). בתחומים מסוימים, המוסדרים בחקיקה ענפית, כלומר חוקים המסדירים רק ענף או מגזר מסוים ואין להם תחולה כללית,[84] מוענקת ל־PII הגנה חוקית הדומה להגנה הרחבה, הכלל־משקית, הקיימת באירופה. זה, למשל, המצב בעניין מידע רפואי, המוסדר ב־ Health Information Portability and Accountability Act (HIPAA) מ־1996.[85] HIPAA מבחין בין מידע מזוהה אישית, המכונה בחוק "protected health information" (PHI), לבין מידע שאינו מזוהה אישית, המכונה "identified health information".[86] PHI מוגן

---

by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, Nov. 22, 2006, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf. בעקבות פרשה זאת נאלצה "SWIFT" להעביר את מרכז העסקים שלה מארצות הברית לשווייץ; ראו: Out-Law.com, *Swift to Stop Processing EU Banking Data in the US*, The Register, Oct. 15, 2007, *available at* www.theregister.co.uk/2007/10/15/swift_processing_halt.

80 Lawrence Lessig, Code – Version 2.0, 228–229 (2006); Judith J. Thomson, The Realm of Rights 285–288 (1990). השוו: Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1377–1391 (2000); Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055 (2004).

81 Richard A. Posner, *The Right to Privacy*, 12 Ga. L. Rev. 393 (1978).

82 כותרת תפקידו של הרגולטור הבריטי, "נציב המידע", דומה כאילו נלקחה מספר של ג'ורג' אורוול. כותרת זאת נובעת מהיותו של הנציב הבריטי ממונה לא רק על הפרטיות ועל הגנת המידע, אלא גם על חופש המידע (Freedom of Information). לעניין זה ראו את אתר הנציבות, לעיל ה"ש 53.

83 למען הדיוק יש לציין כי דירקטיבת 95/46 מחייבת את הקמתן של הנציבויות כגופים **עצמאיים** שאינם כפופים למדינה, אלא לחוק בלבד. ראו ס' 28(1) לדירקטיבה, לעיל ה"ש 13, שבו נקבע: "These authorities shall act with complete independence in exercising the functions entrusted to them".

84 לעיל ה"ש 14.

85 שם.

86 לצורך הפיכת PHI למידע שאינו מזוהה אישית יש להסיר מהמידע לא פחות מאשר את כל הפרטים הללו:

באמצעות שורה של כללים, כגון הגבלת השימושים וההעברות המותרים במידע,[87] צמצום המידע למינימום הנחוץ[88] וחובת יידוע נושאי המידע.[89] גם במגזר הממשלתי הפדרלי מוגן מידע אישי, באמצעות ה־Privacy Act of 1974; חוק זה נחקק חודשים אחדים לאחר התפטרותו של הנשיא ניקסון בעקבות פרשה של חדירות לפרטיות. ה־Privacy Act חל על רשומה (record) של מידע, המוגדרת כפריט או אוסף של מידע על אודות אדם המזוהה בשמו או באמצעות מספר זיהוי או פרט אחר, כגון טביעת אצבע.[90] גם בחוק זה

(A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses: (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information; 45 C.F.R. § 164.514(b) (1996).

87 45 C.F.R. §§ 164.502–164.514 (1996).

88 45 C.F.R. §§ 164.502(b), 164.514 (d) (1996).

89 45 C.F.R. §§ 164.520(a), 164.520(b) (1996).

90 החוק מקודד ב־5 U.S.C. §552a (1974). בס"ק (4)(a) מוגדרת "רשומה" כך:

[A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying

נקבעו שורה של כללים המגנים על פרטיות המידע, מסדירים את איסופו, את אגירתו, את השימוש בו ואת העברתו,[91] מקנים לנושא המידע זכות לעיין בו ולתקנו[92] ומקנים זכות תביעה לאזרח שנפגע.[93]

עיקר העיסוק בהגנה על מידע אישי בארצות הברית אינו מתרכז בחקיקה או ברגולציה אלא בהסדרה פרטית המעוצבת על ידי כוחות השוק ומתבטאת במסמכים הידועים כ"מדיניות פרטיות" (privacy policy).[94] מדיניות הפרטיות הפכה להסדר הדומיננטי בתחום זה בארצות הברית בעקבות שילוב כוחות בין דרישת הצרכנים (בעיקר באתרי אינטרנט) לדעת מה נעשה במידע אישי על אודותיהם, לבין לחץ של רשות הסחר הפדרלית על חברות לגבש וליישם מדיניות פרטיות ולא לסטות מהוראותיה.[95] ב־2003 נחקק חוק ראשון מסוגו בקליפורניה, ה־Online Privacy Protection Act (OPPA); חוק זה חייב אתרי אינטרנט האוספים מידע אישי על אודות תושבי המדינה לפרסם את מדיניות הפרטיות במקום בולט באתר.[96] החוק חל רק על מי שאוסף "מידע אישי" על אודות הגולשים – מידע על אודות אדם מזוהה או ניתן לזיהוי, לרבות שם ושם משפחה, כתובת, כתובת דואר אלקטרוני, מספר טלפון, מספר זהות (social security number), או כל מאפיין אחר המאפשר גישה פיזית או מקוונת אל אדם מסוים. ואכן, אתרים רבים מבחינים במסגרת מדיניות הפרטיות שלהם בין מידע אישי הנאסף על אודות הגולשים לבין מידע אחר שאינו מסווג כמידע אישי, כגון סוג הדפדפן של הגולש, מערכת ההפעלה שלו וכתובת ה־IP,[97] וקובעים כללים נוקשים יותר לשימוש במידע אישי ולהעברתו.[98] ביקורת רבה

number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

91 5 U.S.C. §552a(b) (1974).

92 5 U.S.C. §552a(d) (1974).

93 5 U.S.C. §552a(g) (1974).

94 Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 Am. Bus. L.J. 55 (2007); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 Penn St. L. Rev. 587 (2007).

95 לפעולות אכיפה בהקשר זה ראו למשל: Eli Lilly & Co., 133 F.T.C. 20 (2002), *available at* www.ftc.gov/os/caselist/0123214/0123214.shtm; Microsoft Corp., 2002 WL 1836831 (F.T.C.), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm.

96 The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004) (להלן: OPPA).

97 בעניין כתובת ה־IP ניטשת מחלוקת עזה בין הגורסים כי מדובר במידע אישי, שכן יש לספקית שירותי האינטרנט (בדרך כלל) האמצעים לקשרו לאדם מסוים, לבין הגורסים כי מדובר במידע שאינו אישי, מאחר שהוא אנונימי ולא תמיד ניתן לזיהוי אפילו באמצעות ספקית השירות. ראו: Article 29, WP 136, לעיל ה"ש 60; לעומת זאת, ראו: Peter Fleischer, *Are IP addresses Personal Data?*, Peter Fleischer Privacy…? (Feb. 5 2007), http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html.

98 ראו, למשל, את מדיניות הפרטיות של "פייסבוק" (www.facebook.com/policy.php); של "גוגל" (www.google.com/privacypolicy.html); של "יאהו" (http://info.yahoo.com/

נשמעה כנגד ביסוס ההגנה על הזכות לפרטיות על חוזה אחיד; את החוזה מנסחים יועציהן המשפטיים של חברות, שעניינם אינו בהגנה על פרטיות הצרכנים אלא בפטירת החברות מכל אחריות משפטית.[99] לעומת זאת, יש הסבורים כי מסירת אכיפתה של הזכות לפרטיות לידיהם של נושאי המידע עצמם, להבדיל מהרגולטורים הממונים על זכויותיהם באירופה, מקנה בסופו של יום הגנה משפטית יעילה יותר.

ג. המסגרת הטכנולוגית: הסוסים בורחים מהאורווה

במאמרו הידוע *"Cyberspace and the Law of the Horse"*, הסביר השופט פרנק איסטרברוק לפני יותר מעשור מדוע אין מקום ליצירת ענף משפט חדש לשם הסדרת העולם המקוון.[100] לדבריו, כפי שאין תחום מיוחד במשפט ל"דיני סוסים", אף על פי שסוסים מעוררים שאלות מעניינות בדיני קניין, בדיני חוזים ובדיני נזיקין, כך אין מקום לייסד "דיני אינטרנט" או "משפט וטכנולוגיה". העולם הטכנולוגי בכלל והאינטרנט בפרט אינם אלא זירות נוספות שבמסגרתן יחולו הדוקטרינות המוכרות מדיני החוזים, דיני הקניין, דיני הקניין הרוחני וזכויות היוצרים ודיני הגנת הפרטיות וחופש הביטוי. טענה קשורה היא כי על המשפט להישאר "ניטרלי" לטכנולוגיה, כלומר לקבוע ערכים, עקרונות וכללים שיחולו ללא קשר לטכנולוגיה שנמצאת בשימוש בעת מסוימת.[101] אחת הסיבות לכך היא הכרה מפוכחת בכך שגם המחוקקים הזריזים ביותר לא יצליחו להדביק את קצב ההתפתחויות הטכנולוגיות, ולכן כל חוק שאינו "ניטרלי" לטכנולוגיה נועד להישכח ולהפוך לבלתי רלוונטי, לעתים אף טרם חקיקתו.

השופט איסטרברוק נשען, אפוא, על הביטחון שמעניקה המסורת המשפטית ובעיקר על המשפט המקובל, שהוכיח יכולת הסתגלות מרשימה לשינויים פוליטיים, כלכליים

---

www.8hands.com/content/privacy-) "8hands" ושל ;(privacy/us/yahoo/details.html policy).

99 Tene, לעיל ה"ש 32; לביקורת על חוזים ברשת ראו: Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002); Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up To Be?*, 9 Tul. J. Tech. & Intell. Prop. 173 (2007); Christina L. Kunz, John Ottaviani, Elaine Ziff, Juliet M. Moringiello, Kathleen Porter & Jennifer Debrow, *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 Bus. L. 279 (2003); Sharon K. Sandeen, *The Sense and Nonsense of Web Site Terms of Use Agreements*, 26 Hamline L. Rev. 499 (2003); Robert A. Hillman & Jeffery J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. Rev. 429 (2002).

100 Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207; ראו גם: Joseph H. Sommer, *Against Cyberlaw*, 15 Berkeley Tech. L.J. 1145 (2000). לטיעון הנגדי ראו: David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996); Lawrence Lessig, *The Path of Cyberlaw*, 104 Yale L.J. 1743 (1995).

101 ראו למשל: Open Source Initiative, *The Open Source Definition (Annotated)*, www.opensource.org/docs/definition.php.

וחברתיים כבירים – החל מן המהפכה הצרפתית, עבור דרך המהפכה התעשייתית ועד בכלל. אי אפשר היה לצפות לגישה אחרת משופט שמרן. גישתו מחייבת התאמה של הדוקטרינות המסורתיות של הגנת הפרטיות, המבוססות על ההבחנה בין תוכן לבין נתוני תקשורת ובין מידע אישי למידע שאינו כזה, למציאות הטכנולוגית הנוכחית. אלא שכפי שנראה להלן, ההתפתחויות הטכנולוגיות מן השנים האחרונות, הבולטות יותר מכול בשוק התקשורת האלקטרונית, מותחות עד קצה גבול היכולת את הדוקטרינות המקובלות ומקשות על יישומן. ייתכן שהסוסים של איסטרבורוק ברחו הפעם מאורוות המשפט המקובל וכי יש להעניק להם טיפול מיוחד, פן תסוכל ההגנה על הפרטיות המוכרת לנו.

1. הבחנה בין תוכן לבין נתוני תקשורת

ההבחנה בין תוכן לבין נתוני תקשורת היא הבחנה תלויית טכנולוגיה. כאשר מדובר במשלוח מכתבים בדואר רגיל (המכונה כיום "דואר חלזונות" – snail mail), קל להבחין כי התוכן הוא הכתוב במכתב המקופל בתוך המעטפה, ואילו נתוני התקשורת הם כתובת הנמען, כתובת השולח והבול שעל המעטפה. גם באשר לשיחת טלפון הנערכת בטלפון קווי ההבחנה ברורה: התוכן הוא הנאמר בין הצדדים לשיחה, ואילו נתוני התקשורת הם מספר הטלפון של מקבל השיחה, מספר הטלפון של המתקשר ומשך השיחה. בניגוד למשלוח מכתב בדואר, בידי ספקית שירותי הטלפון מצוי גם מידע נוסף על אודות המשתתפים בשיחה, הכולל פרטים אישיים של בעל הקו כגון: כתובתו, מספר כרטיס האשראי שלו, מספר תעודת הזהות שלו, שירותים אחרים שאותם הוא מקבל והרגלי השימוש שלו בשירותי החברה.[102] אלה נתונים משמעותיים ואפשר להסיק מהם מסקנות שונות בעניין השתייכותו הדמוגרפית של המתקשר, גילו, זהות חבריו הקרובים או שותפיו העסקיים ועוד. נתונים אלה משליכים ישירות על זכותו של המתקשר לפרטיות, אך הם אינם חודרים אל ה"ליבה" של ההגנה על תוכן השיחה. מעטים יחלקו על הטענה כי לא מדובר בתוכן אלא בנתוני תקשורת. כלומר, ייתכן שספקית שירותי הטלפון יודעת שאני מתקשר פעמים רבות ביום למספר טלפון מסוים וכי אותו מספר אינו בבעלותה של אשתי; אך היא אינה יודעת על מה אני משוחח עם בעלת המספר – שמא מדובר בענייני עבודה, בהחלפת מתכוני בישול או, רחמנא ליצלן, בעניינים שבינו לבינה.

דא עקא, כשמדובר בטכנולוגיות תקשורת חדשות כגון דואר אלקטרוני, טלפון סלולרי, שירותי מסרים מידיים וגלישה באינטרנט, ההבחנה בין תוכן לבין נתוני תקשורת מטשטשת.[103] הדוגמה הפשוטה היא הדואר האלקטרוני. הכול יסכימו כי גוף ההודעה הוא

102 נתונים אלה מוגדרים בס' 1 לחוק נתוני תקשורת כ"נתוני מנוי", הכלולים במסגרת ההגדרה של "נתוני תקשורת" המופיעה באותו סעיף.

103 ראו בירנהק, לעיל ה"ש 23, בעמ' 34:

> בעידן שבו יכולות עיבוד מידע ממוחשבות אינן בדיוניות, אלא כלי יומיומי זמין וקל לשימוש, ניתן ללמוד מנתוני התקשורת על תוכן השיחה ועל המשוחחים. למשל, שיחות טלפון יומיומיות בין אדם לבין מוקד תמיכה נפשית מעידות על תוכן השיחה; גלישה באתר באינטרנט שעוסק בבעיה רפואית מסוימת מלמד רבות על הגולש; נתוני שיחה של עיתונאית חושפים את מקורותיה; מנתוני התקשורת

בגדר תוכן, וכי נתונים בדבר "משקלה" (למשל, שני מגה־בייט) או אורכה (למשל שתים־עשרה שורות טקסט) הם בגדר נתוני תקשורת. אולם, מה בדבר כתובת השולח וכתובת הנמען? בדואר אלקטרוני, להבדיל מדואר רגיל או משיחת טלפון, יכולה כתובת המשתמש להעיד על מקום לימודיו (למשל omer.tene@nyu.edu), על מקום עבודתו (omer.tene@ibm.com) או על שמה של אשתו (daphna.omer@gmail.com).

שאלה מעניינת אף יותר היא האם שורת הנושא של הודעת הדואר האלקטרוני היא בגדר תוכן או בגדר נתוני תקשורת? מבחינה טכנית, כל הודעת דואר אלקטרוני מחולקת ל"כותרת" ול"גוף ההודעה". הכותרת כוללת את כתובת השולח, את כתובת הנמען (לרבות נמענים בשדות ההעתק הגלוי, Cc, או ההעתק הסמוי, Bcc), את מועד ההודעה ואת שורת הנושא; גוף ההודעה כולל טקסט וקבצים מצורפים. אם כן, שורת הנושא שייכת לכאורה לנתוני התקשורת. האומנם? מבחינה מהותית עלולה שורת הנושא לחשוף את התוכן שבגוף ההודעה בצורה שאין מקבילה לה בשיחות טלפון או בדואר רגיל. יתר על כן, לגופים מתעניינים רבים עשויה שורת הנושא להספיק כדי לאפיין את התכתובת, מבלי שיתעורר צורך או עניין לבחון את גוף ההודעה. כך, למשל, עשויים מפרסמים שונים לבקש לצרף פרסומות לתכתובת על סמך ניתוח שורת הנושא.[104]

בתי המשפט בארץ התחבטו לאחרונה בשאלה דומה: האם הודעת דואר אלקטרוני הנשמרת על השרת של ספקית השירות דומה למכתב שנפתח, שתפיסתו על ידי המשטרה מחייבת צו חיפוש רגיל, או שמא לשיחת טלפון, שהאזנה לה מחייבת צו האזנת סתר?[105] בעניין **פילוסוף** סקר השופט חאלד כבוב את עמדת המדינה בנושא; עמדה זו "התהפכה" ארבע או חמש פעמים במהלך תקופה של שנים אחדות, כתלות בשאלה אם המדינה הייתה המאשימה בתיק (כלומר, הגישה כתב אישום נגד אדם ש"יירט" הודעת דואר אלקטרוני) או הנתבעת (על ידי מי שטען שהודעותיו "יורטו" ללא צו שיפוטי כנדרש).[106] בניסיון להטמיע את הטכנולוגיה החדשה במסגרת חוקית מוכרת, נעזר השופט כבוב באנלוגיה מתחום אחר:

> יוצא כי מסעה של הודעת הדוא"ל בדרכה לנמען כוללת עצירות ביניים. דומה הדבר לרכב הנוסע מתל אביב לחיפה ובדרכו עוצר בתחנת דלק לשם תדלוק, האם ניתן לומר כי עצירה זו קוטעת את מסעו של האדם הנוהג ברכב מתל אביב לחיפה? האם ניתן לומר כי העצירה בתחנת הדלק משמעה סיום המסע ותחילת מסע חדש? אמנם מבחינה טכנית בוצעה עצירה אך מדובר בעצירה

של אדם אפשר ללמוד על קשריו החברתיים, העסקיים והאחרים, ומהם ללמוד על האדם עצמו.

104 ראו למשל ע"ב (אזורי ת"א) 10121/06 **איסקוב ענבר – הממונה על חוק עבודת נשים** (טרם פורסם, 15.7.2007). באותו מקרה יכול היה המעביד להסיק משורת הנושא של הודעות דואר אלקטרוני ששלחה העובדת, כי היא מחפשת עבודה חדשה. הודעות אלה הוגשו לבית הדין כראיה לכך שהעובדת פוטרה עוד לפני מועד כניסתה להיריון. בית הדין הארצי לעבודה קיבל את הערעור על פסק הדין. ראו ע"ע 90/08 **איסקוב־ענבר נ' מדינת ישראל – הממונה על חוק עבודת נשים** (טרם פורסם, 8.2.2011).

105 ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף** (טרם פורסם, 5.2.2007).

106 שם, בס' 3 לתדפיס ההחלטה.

> הכרחית לשם המשך המסע והגעה ליעד הסופי, כל עת שהרכב לא הגיע לחיפה נאמר כי האדם נמצא בדרכו ליעד שלשמו יצא.[107]

כלומר, תפיסתה של ההודעה על השרת של ספקית השירות דומה ל"יירוט תנועה" של שיחת טלפון ולא לתפיסה של מכתב, שהוא חפץ נייח.

ברי כי התאמתן של הדוקטרינות המסורתיות להתפתחויות הטכנולוגיות מחייבת הפקדת שיקול דעת נרחב בידי השופטים, והם נאלצים להחליט "מה דומה למה". משימה זאת נראית אולי סבירה כשמשווים בין הודעת דואר אלקטרוני לשיחת טלפון; אך עם התפתחותן של טכנולוגיות חדשות וההתרחקות מהמסגרת החוקית המקורית, היא עלולה להפוך לתרגיל מעניין מבחינה אינטלקטואלית אך חסר מִשְמעת פרשנית. כך, למשל, יהיה המצב אם שופט ייאלץ להחליט אם קידוד מולקולות דנ"א בתאי גזע עובריים דומה לנסיעה על אופניים בכביש בין־עירוני או להנפקת אגרות חוב ניתנות להמרה בשוק יורד. במילים אחרות: מגיע השלב שבו ראוי להתאים את המסגרת החוקית, המיועדת ליישום על טכנולוגיות שעברו מן העולם או שפחתה חשיבותן, לסביבה טכנולוגית דינמית המתפתחת במהירות רבה ממהירות התקדמותו של החוק.

גם טכנולוגיית הטלפון הסלולרי מציבה קשיים בפני ההבחנות המקובלות. הטלפון הסלולרי מאפשר לקבוע את מיקומו הגאוגרפי של מחזיקו גם בשעה שהוא אינו משוחח בו. לכאורה, מעקב גאוגרפי צמוד כזה הוא בגדר פגיעה חמורה בפרטיות, ועד לפני שנים אחדות קשה היה לדמיינו.[108] על אף האמור, "נתוני המיקום" נחשבים לנתוני תקשורת ולא לתוכן.[109] סיווג זה נכון אולי מבחינה אנליטית (שכן מיקומו של אדם אינו מעיד על תוכן שיחתו עם הזולת), אך מעורר קושי אינטואיטיבי, לנוכח ההסדרים המשפטיים המקלים החלים על קטגוריית מידע זו. נוסף לכך, מכשיר הטלפון הסלולרי כולל את הרשימה המקיפה ביותר מן הנמצא של בני משפחתו של אדם, של חבריו, של מכריו ושל שותפיו לעבודה. מדובר בנכס מידע רב ערך; אף שדומה שרק מי שחווה את אבדנו יודע לאמדו במדויק, נכס זה הוא ללא ספק נכס מוערך בשוק ההון. כך, למשל, באוקטובר 2007 רכשה "מיקרוסופט" 1.6 אחוזים ממניותיה של הרשת החברתית המקוונת "פייסבוק", לפי שווי שוק של 15 מיליארד דולר.[110] אף ש"פייסבוק" לא הרוויחה באותה תקופה ולו דולר אחד, עֶרְכָּהּ עבור ענקית התכנה "מיקרוסופט" התבטא במאגר המידע העצום שנאגר ברשת על אודות קשריהם החברתיים של 50 מיליון משתמשיה.[111] מידע כזה בדיוק, בהיקף רחב יותר

---

107 שם, בס' 8(5) לתדפיס ההחלטה.

108 בס' 2(1) לחוק הגנת הפרטיות נקבע: "פגיעה בפרטיות היא אחת מאלה: (1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת".

109 ס' 1 לחוק נתוני תקשורת, לעיל ה"ש 17; ס' 2 ו־9 לדירקטיבת 2002/58, לעיל ה"ש 13; ס' 1, 2 ו־5(1)(f) לדירקטיבת 2006/24, לעיל ה"ש 48; וראו ת"א (ת"א) 06-1994 **אמיר לירן, עו"ד נ' פלאפון תקשורת** בע"מ (החלטתה של השופטת ברון מיום 30.11.2010).

110 Brad Stone, *Microsoft Buys Stake in Facebook*, N.Y. Times, Oct. 25, 2007, *available at* www.nytimes.com/2007/10/25/technology/25facebook.html?ref=technology.

111 הנתונים נכונים למועד העסקה; בחודש ינואר 2011 היו לאתר כבר יותר מ־600 מיליון משתמשים. לאחרונה השקיע בנק ההשקעות "גולדמן סאקס" ב"פייסבוק" סכום של 500

ובאיכות גבוהה יותר, מוחזק בידי ספקיות שירותי הסלולר. חשבו בעצמכם: איזו רשימה משקפת באופן מדויק יותר את קשריכם החברתיים והעסקיים, רשימת החברים ב"פייסבוק" (הכוללת מן הסתם מכרים מן התיכון ו"חברים של חברים של חברים" שמעולם לא ראיתם את פניהם במציאות) או רשימת אנשי הקשר במכשיר הטלפון הסלולרי שלכם?

ההבחנה בין תוכן לבין נתוני תקשורת מאבדת כל אחיזה כשמדובר בהרגלי גלישה באינטרנט. אפשר אמנם לטעון כי הבחנה זו אינה ממין העניין בהקשר זה, שכן לא מדובר בתקשורת דו־צדדית. שיחת טלפון, מכתב רגיל והודעת דואר אלקטרוני הם אמצעים לתקשורת בין שני בני אדם (או יותר), ואילו גלישה באינטרנט היא תקשורת בין אדם לבין מחשב. אולם בהקשר של הזכות לפרטיות, הבחנה זו בין שיחה בין בני אדם לבין "שיחה" בין אדם לבין מחשב אינה משמעותית. אמצעי התקשורת הנמצאים ברשותנו כיום מורכבים ממסרים המועברים מאדם לאדם (שיחת טלפון, הודעת דואר אלקטרוני, מסרון – הודעת SMS), מאדם למחשב (הודעה בתא קולי, חיפוש ב"גוגל", גלישה באינטרנט), ממחשב לאדם (שיחות טלפון אוטומטיות, הודעות דואר אלקטרוני ומסרונים אוטומטיים) וממחשב למחשב (תקשורת בין שבבי RFID לקורא).[112] אנו מפתחים ציפייה סבירה לשמירת פרטיותנו בכל אחד מאמצעי התקשורת הללו. ההגדרות בדיני האזנת הסתר גמישות מספיק כדי להכיל תקשורת בין אדם לבין מחשב. חוק האזנת סתר מגדיר "'שיחה' [...] לרבות [...] בתקשורת בין מחשבים". ואילו ה־ECPA חל על "תקשורת אלקטרונית", המוגדרת כך: "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system". נראה, אם כן, כי תקשורת בין אדם לבין מחשב באינטרנט כפופה לדיני האזנת הסתר ולהגנת הפרטיות.

האינטרנט הוא רשת מיתוג מנות (Packet Switched Network); כל תשדורת מחולקת למנות (חבילות), ואלה מנותבות ביחד או לחוד בין נתבים שונים אל מחשב היעד, בהתאם לעומס היחסי ברחבי הרשת. אמנם מבחינה טכנית אפשר להבחין בין "מנת מעטפת" (Packet Header) לבין "מנת תוכן" ("payload" או "body"): מנת תוכן כוללת את המידע המועבר בין המחשבים; מנת מעטפת כוללת את הנתונים הנחוצים לניתוב ההודעה, כגון כתובת ה־IP של המחשב השולח (השרת) ושל המחשב הנמען, וכן את הפרוטוקול השולט במנות התוכן. כתובת ה־IP של השרת (למשל, 72.3.133.152) ניתנת לתרגום באמצעות ה־DNS (Domain Name System) ל־URL (Uniform Resource Locator), רצף של אותיות ומספרים המשמש לזיהוי תכנים באינטרנט (למשל: http://www.nytimes.com/pages/technology/index.html). אולם מבחינה מהותית עשויים נתוני מעטפת (כגון כתובת ה־IP או ה־URL של השרת) להסגיר ללא כל קושי את תוכן הדף.

מיליון דולר, בעסקה שלפיה מוערך כיום שוויה של החברה (הפרטית עדיין, אם כי כבר רווחית) ב־50 מיליארד דולר. Barbara Ortutay, *Goldman Invests in Facebook at $50 Billion Valuation*, The Huffington Post, Jan. 3, 2011, *available at* http://www.huffingtonpost.com/2011/01/03/facebook-valuation-goldman_n_803447.html.

112 לטכנולוגיית RFID ראו להלן ה"ש 135–137 והטקסט המפנה אליהן.

כך, למשל, כוללת כתובת ה־URL של שאילתות החיפוש ב"גוגל" את מילות החיפוש שהקליד הגולש. למשל, אם הגולש מחפש את המילה "apple", יהיה ה־URL של החיפוש כזה: http://www.google.com/search?source=ig&hl=en&rlz=&=&q=apple&btnG=Google+Search. ה־URL כולל את הפרוטוקול (http), את שם המתחם (google.com) ואת הדף המבוקש (search?source=ig&hl=en&rlz=&=&q=apple&btnG=Google+Search, במקרה זה).[113] אמנם, המביט במידע לא יֵדע אם הגולש מעוניין בתפוחי עץ או ב־"iPhone". אך בדרך כלל אפשר לדלות מידע זה על פי ניתוח של כמה שאילתות חיפוש רצופות (למשל, האם החיפוש הבא הוא ל"מחשבי כף יד" או ל"חופשה בגולן"?), אף מבלי להיזקק לניתוח "תוכן" הדף (ה־payload). ואכן, באוגוסט 2005 דרשה ממשלת ארצות הברית ממנועי החיפוש הגדולים בארצות הברית להעביר לידיה את יומן שאילתות החיפוש שהציגו הגולשים במשך חודשיים,[114] כדי להוכיח כי שיעור ניכר מהתנועה ברשת מיוחד לפורנוגרפיה.[115] נקל לראות כי לשם הוכחת אופיו של התוכן שמחפשים הגולשים אין צורך להידרש לדבר פרט לרשימת כתובות ה־URL. אך דא עקא שאלה עשויים להיתפס כנתוני תקשורת, מאחר שהם אינם התוכן שמחפש הגולש אלא רק הפניה של הדפדפן אל אותו תוכן במחשבו האישי של הגולש. ברור גם כי ממשלת ארצות הברית כלל לא שקלה להתייחס אל דרישתה כאל בקשה לצו האזנת סתר.[116] תוכן לחוד ונתוני תקשורת לחוד.

שנה לאחר פרשה זו, זכה הציבור להצצה מביכה אל רשימות כדוגמת אלה שביקשה ממשלת ארצות הברית, כאשר "AOL" החליטה לפרסם באתר ה"מחקר" של החברה את שאילתות החיפוש שהציגו 658,000 גולשים במשך תקופה של שלושה חודשים.[117] רשימת

---

113 ההדגשה שלי – ע' ט'.

114 Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. Times, Jan. 20, 2006, *available at* http://stono.cs.cofc.edu/~bowring/docs/Google%20Resists%20U.S.pdf.

115 לכאורה מדובר בקביעה טריוויאלית, אך ממשלת ארצות הברית נדרשה להוכיחה במסגרת מאבקה המשפטי המתמשך לתמוך בחוקתיותו של חוק ה־Child Online Protection (COPA), מאבק להגנה על ילדים מפני חשיפה לתכנים פורנוגרפיים ברשת. בית המשפט העליון האמריקני פסל פעמיים כבלתי חוקתי את החוק בגלגוליו השונים. ראו: Reno v. ACLU, 521 U.S. 844 (1997); ACLU v. Ashcroft, 124 S. Ct 2783 (2004).

116 ראו בקשת המדינה בעניין *Gonzales* Reply Memorandum in Support of the Motion to Compel Compliance With Subpoena Duces Tecum, Gonzales v. Google Inc., 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW), 2006 WL 733758; בית המשפט דחה את בקשת המדינה בעניין זה: Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D.Cal. 2006).

117 Saul Hansell, *AOL Removes Search Data on Vast Group of Web Users*, N.Y. Times, Aug. 8, 2006, *available at* http://tinyurl.com/38rzpq; J. Nicholas Hoover, *AOL Search-Term Data was Anonymous but not Innocuous*, InformationWeek, Aug. 14, 2006, *available at* http://tinyurl.com/2wr2ue; אף שכלל לא ברור אם החשיפה גרמה להפרתן של זכויות משפטיות כלשהן, שילם מנהל הטכנולוגיה הראשי של החברה על טעות יחסי הציבור במשרתו; ראו: Elinor Mills & Anne Broache, *AOL Axes Staff Over Privacy Breach*, ZDNET,

השאילתות, שאינה אלא רשימה של כתובות URL, חשפה מידע אישי מאוד, חשיפה שהשלכותיה על זכותם לפרטיות של הגולשים היו מרחיקות לכת. הרשימה כללה מידע על תחומי העניין של כל גולש, על מכלול תקוותיו, שאיפותיו, פחדיו, תאוותיו, תחביביו ותכניותיו, על טיולים שערך, על עבודות שחיפש ועל עניינים פיננסיים שהעסיקו אותו. למעשה, שרטטה רשימת כתובות ה־URL מפה מדויקת ביותר של כל מה שחלף במוחו של הגולש ביושבו מול המחשב, מעין "שיקוף רנטגן" של מכלול מחשבותיו.[118] לא זו בלבד שרשימת כתובות ה־URL כללה מידע אישי ורגיש ביותר, בין אם נסווגו כתוכן ובין אם נסווגו כנתוני תקשורת, אלא שאף אם המידע עבר תהליך מכוון של אנונימיזציה – דובר במידע מזוהה אישית. במקרה הנדון "הצפינה" "AOL" את המידע מאחורי שמות־משתמש אקראיים; שמות אלה החליפו את כתובות ה־IP של הגולשים, שלפיהן נשמר המידע בדרך כלל.[119] למרות זאת, עיתונאי של "הניו־יורק טיימס" הראה כיצד הצליח לזהות גולשת שהוסתרה מאחורי מספר אקראי של "AOL" באמצעות ניתוח חובבני של שאילתות החיפוש שלה.[120]

לא רק רשימה של כתובות URL של שאילתות חיפוש חושפת את התוכן המבוקש, אלא גם רשימה של כתובות URL של דפי אינטרנט אחרים. למשל, כתובת ה־URL של הספר "החטא ועונשו" מאת פיודור דוסטוייבסקי באתר "אמזון" היא: http://www.amazon.com/Crime-Punishment-Fyodor-Dostoevsky/dp/0679734503/ref=sr; כתובת ה־URL של סדרת "ThinkPad X" של מחשבי "לנובו" היא: http://shop.lenovo.com/us/notebooks/thinkpad/x-series; ולא קשה לנחש במה עוסק הדף המיוחס לכתובת ה־URL הזו: http://www.twilightsex.com/celebs-thumbs.html.

מעקב של המשטרה אחר רשימת כתובות URL שבהן גלש אדם, כמו גם רשימת כתובות ה־IP של האתרים שבהם ביקר, או איסוף של רשימה כזו, שקולות לגישה לתוכן שצרך אותו אדם. מסקנה זו אינה משתנה גם מקום שהתוכן "מסתתר" מאחורי כתובת מספרית (במקרה של כתובות IP) או מילולית־מספרית (במקרה של כתובות URL). הדבר דומה למסירת מידע מוצפן למאן דהוא בצירוף מפתח ההצפנה – כל שאותו אדם נדרש לעשות כדי לחשוף את המידע הוא להשתמש במפתח ההצפנה המצוי בידיו. בדיוק באותו אופן יכול שוטר המקבל רשימת כתובות IP שבהן ביקר אדם לגלות את תוכן האתרים, באמצעות הקלדה פשוטה של הכתובות בדפדפן. כפי שהוסבר לעיל, אם אותו שוטר מקבל רשימת כתובות URL, במקרים רבים הוא כלל לא יידרש לבקר באתרים כדי לזהות את תוכנם. כמו כן, לא זו בלבד שהשוטר יוכל לצפות בתוכן באמצעות שימוש בכתובות ה־IP, אלא שהוא יוכל לצפות בתוכן שבו צפה הגולש **במועד שבו גלש**, כיוון שאתרים

Aug. 22, 2006, http://news.zdnet.co.uk/communications/0,1000000085,39281482,00.htm.

118 Tene, **לעיל ה"ש 32**.

119 **לעיל ה"ש 97**.

120 Michael Barbaro & Tom Zeller, *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, *available at* www.nytimes.com/2006/08/09/technology/09aol.html.

רבים שומרים בארכיב גרסאות היסטוריות של דפי האינטרנט שהציגו בעבר, וגרסאות אלה מאפשרות צפייה באותם דפים כפי שהופיעו במועד הרלוונטי.[121] ראוי לציין עוד כי למשטרה אין עניין ברשימת כתובות ה־URL שבהן ביקר אדם אלא למטרת חשיפה של תוכן האתרים. לעומת נתוני חיוג של אדם, שעשוי להיות להם ערך חקירתי גם בלא תוכן השיחות (למשל, הם עשויים לספק מידע בשאלה אם החשוד שוחח עם קורבן העבירה בסמוך להתרחשותה או אם נהג לדבר עם שותפיו לקשירת הקשר), לרשימת כתובות URL אין כל ערך אלא כמפתח לחשיפה של תוכן.

אפשר לטעון כי מסקנת הניתוח צריכה להיות שבשונה מנתוני תקשורת, נתוני גלישה ברשת יש לסווג כתוכן, וכי אין כל קושי לעשות כן על פי ההבחנות הקיימות. במונחים של השופט איסטרברוק – אין צורך ביצירתם של "דיני סוסים", שכן המסגרת המשפטית הקיימת מתאימה להחלה על התוכן. אולם פתרון זה אינו נקי מספקות, שכן אף על פי שהרגלי הגלישה ברשת כוללים מאפייני תוכן, קשה להקבילם לתוכן של שיחה. גולשים רבים מודעים לכך שהרגלי הגלישה שלהם מנוטרים לא רק על ידי ספקיות שירותי האינטרנט, אלא גם על ידי רשתות מפרסמים המציבות "עוגיות" (cookies) באתרים שונים[122] ועל ידי האתרים עצמם. קל מאוד להסיר "עוגיות" או לחסום את הצבתן מלכתחילה, אלא שרק מתי מעט מהגולשים נוהגים לעשות כן. אם כן, נראה כי מבחינת ציפייתם לפרטיות של הגולשים עצמם לא הרי גלישה באינטרנט כהרי תוכנה של שיחת טלפון.

תופעה נוספת המשליכה על הגנת הפרטיות בתקשורת ובתכתובת היא הטשטשות קו הגבול – הלכידות (convergence) – בין אמצעי התקשורת השונים. מצד אחד, נוהגים גולשים רבים באינטרנט להתחבר כיום לרשת באמצעות מכשיר הטלפון הסלולרי, ותופעה זאת צפויה עוד להתרחב עד כדי כך שמכשיר הטלפון יהפוך לפלטפורמת הגלישה המובילה, אף יותר מהמחשב האישי.[123] מן הצד האחר, רשת האינטרנט הופכת אט אט למתחרה משמעותית של חברות התקשורת המסורתיות להעברת שיחות טלפון, באמצעות טכנולוגיית VoIP (Voice-over-Internet Protocol).[124] הלכידות בין אמצעי התקשורת וקריסת ההבחנה בין תוכן לבין נתוני תקשורת מחייבות מסגרת חוקית חדשה להגנת הפרטיות, מסגרת שלא תבוסס על דיכוטומיה כקודמתה אלא על רצף של מצבים שיסווגו בהתאם למידת הסכנה שהם מציבים לפרטיות.

---

121 Beryl A. Howell, *Proving Web History: How to Use the Internet Archive*, 9 J. Internet L. 3 (2006).

122 "קוקי" (עוגיה) היא קובץ טקסט קטן הנשלח מאתר אינטרנט לדפדפן של הגולש למטרת איסוף מידע, אימות זיהוי ומעקב. ראו: Jessica J. Thill, *The Cookie Monster: From Sesame Street to Your Hard Drive*, 52 S.C. L. Rev. 921 (2001).

123 Adam Wright, *Mobile Phones Could Soon Rival the PC as World's Dominant Internet Platform*, Ipsos News Center, Apr. 18, 2006, www.ipsos-na.com/news/pressrelease.cfm?id=3049.

124 שירותי VoIP, שהידוע שביניהם הוא שירות "סקייפ" ("Skype"), מאפשרים לנהל שיחות טלפון באמצעות רשת האינטרנט בדרך של דחיסת שבריר שניות של דגימות קול על פני פרוטוקול אינטרנט ושיגורן אל המחשב הנמען.

2. הבחנה בין מידע אישי לבין מידע שאינו אישי

גם ההבחנה בין מידע אישי לבין מידע שאינו אישי נשחקה עם התפתחותן של טכנולוגיות חדשות (כגון כריית מידע או שבבי RFID). במהלך שנת 2008 התעוררה סערה משני עברי האוקיאנוס בשל כוונתן של ספקיות שירותי אינטרנט (כגון ענקית הכבלים "צ'רטר" בארצות הברית וחברת הטלקום "BT" באנגליה) להשתמש בשירותיהן של חברות כריית מידע כדי לאפיין את הרגלי הגלישה של המשתמשים.[125] עד אותה עת נאלצו ספקיות שירותי האינטרנט להסתפק במעמד של "צינור" להעברת מידע והתקנאו בחברות שנהנו מנתח מהשוק אדיר הממדים של הפרסום המקוון. שוק זה מתחלק בין חברות כגון "גוגל", המספקות שירותי ניתוח קונטקסטואלי (Contextual Targeting) של דפים לשם הצבת פרסומות מתאימות,[126] לבין חברות כגון "DoubleClick" ו"טאקודה", המספקות שירותי ניתוח התנהגותי (Behavioral Targeting) של הרגלי הגולשים במסגרת קבוצת אתרים נתונה (Advertising Networks).[127] "שם המשחק" בשוק הפרסום המקוון הוא הצבה של הפרסומות המתאימות ביותר לצורכי הגולש ולרצונותיו כדי למקסם את מדד הרווחיות העיקרי – שיעור ה־Click-through (CTR), וכפועל יוצא מכך את ההכנסות מפרסום.

ספקיות שירותי האינטרנט מחזיקות בפוטנציאל ניתוח מידע אדיר, שכן הן מסוגלות לעקוב אחר כל תנועה ותנועה של לקוחותיהן ברשת ללא הגבלה לאתר או לשירות מסוימים. כדי לממש את פוטנציאל כריית המידע התקשרו ספקיות שירותי האינטרנט בהסכמים עם חברות שונות, בעיקר עם חברת "Phorm" באנגליה ועם חברות "NebuAd" ו־"Front Porch" בארצות הברית. חברות אלה השתמשו בטכניקה הידועה כ־"deep packet inspection", טכניקה שיוחדה בעבר לסוכנויות ביון כגון סוכנות "NSA" (National Security Agency) האמריקנית או "GCHQ" (Government Communications Headquarters) הבריטית, כדי לנתח את תוכן דפי האינטרנט שבהם צופים הגולשים (כלומר, לא רק את המידע במעטפת אלא גם את התוכן).

כאמור, הידיעות על השירות החדש עוררו סערה ציבורית. פעילי הגנת הפרטיות והגנת הצרכן טענו כי פרט להפרה של רישיונות התקשורת ושל אמון הצרכנים, עם הפעלת שירות זה הפרו ספקיות שירותי האינטרנט את דיני האזנת הסתר ופגעו בפרטיותם של

125 Louise Story, *A Company Promises the Deepest Data Mining Yet*, N.Y. Times, Mar. 20, 2008, *available at* www.nytimes.com/2008/03/20/business/media/20adcoside.html?scp=1&sq=phorm&st=nyt; Saul Hansell, *The Mother of All Privacy Battles*, N.Y. Times, Mar. 20, 2008, *available at* http://bits.blogs.nytimes.com/2008/03/20/the-mother-of-all-privacy-battles/?pagemode=print.

126 כך, למשל, אם אדם צופה באתר האינטרנט של מוזאון הלובר, יוצגו לפניו פרסומות של בתי מלון בפריז.

127 כך, למשל, אם אדם צופה באתר האינטרנט של מוזאון הלובר לאחר שצפה בדפים העוסקים בגני ילדים בפריז, בחנויות לממכר דברי סדקית ובשירות התשלומים של רשות מס ההכנסה הצרפתית, יוצגו בפניו פרסומות של קורסים לאמנות או של תערוכות במוזאונים אחרים בפריז ולא של בתי מלון, מתוך הנחה שהוא תושב העיר.

הגולשים.[128] כדי למנוע גל של רגולציה או מרד צרכנים, פירסמו חברות "Phorm" ו־"NebuAd" הסברים מפורטים על אופי פעילותן וטענו כי הן אינן פוגעות בפרטיות המידע. על פי הנטען, "Phorm" ו־"NebuAd" כלל לא אספו "מידע אישי" של גולשים, שכן פרופיל הגלישה של כל משתמש נשמר וקוטלג (באמצעות "עוגייה") על פי מספר קוד אקראי, שאינו ניתן לקישור לאדם מסוים.[129] במילים אחרות, ספקית שירותי האינטרנט, היכולה (בדרך כלל) לחבר כתובת IP של משתמש לשמו ולפרטיו האישיים, לא קיבלה לידיה את פרופיל הגולש; ואילו "Phorm" ו־"NebuAd", שהחזיקו בפרופיל מפורט של כל גולש, לא קיבלו לידיהן את כתובת ה־IP שלו או את פרטיו האישיים. פרופיל המשתמש נמצא ב"קופסה שחורה", שהעבירה לספקית שירותי האינטרנט רק את התוצר סופי, קרי: המלצה להציב בפני גולש מסוים פרסומת שתוכנה מתאים לאותו משתמש (או את הפרסומת עצמה). ארכיטקטורת השירות בנויה כך שמספר הקוד האקראי לעולם אינו מוצלב עם כתובת ה־IP או עם כל מידע אחר המזוהה אישית עם הגולש.[130] ואכן, נציב הגנת המידע הבריטי נאלץ לאשר את הפעלת השירות. לדבריו: "BT has also stated that the system *does not store personally identifiable information*, URLs, IP addresses or retain browsing histories and that search information is deleted almost immediately, and is not retrievable".[131]

מקרה זה זורה אור על הקושי שמעוררת ההבחנה בין "מידע אישי" לבין מידע שאינו כזה. אינטואיטיבית, נראה כי השירות שמספקות "Phorm" ו־"NebuAd" פוגע בפרטיות הגולשים ללא קשר לשאלה אם החברות יכולות לזהות כל אחד מן הגולשים בשמו, בכתובתו או אף בכתובת ה־IP שלו. גם אם נניח שאין לחברות כל דרך לזהות את הגולש המסתתר מאחורי מספר הקוד האקראי שהעניק לו המחשב (למשל 12345), כלומר שהמידע "פסידונימי" גם אם הוא אינו אנונימי ושהפרופיל המדוקדק שבידי החברות אינו "מידע אודות אדם מזוהה או ניתן לזיהוי" (ובמקרה זה מדובר בהנחה שכלל אינה נקייה

128 Center for Democracy & Technology, *An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising*, Jul. 8, 2008, www.cdt.org/privacy/20080708ISPtraffic.pdf.

129 80/20 Thinking Ltd., *First Stage (Interim) Privacy Impact Assessment*, Phorm, Feb. 10, 2008, http://privacy.phorm.com/Phorm_PIA_interim.pdf.

130 השירות גם מוחק באופן אוטומטי קטגוריות מסוימות של מידע, כגון מידע רגיש במיוחד (למשל מידע רפואי או מידע על העדפות מיניות), מספרים ארוכים משלוש ספרות (כגון מספרי טלפון ומספרי כרטיסי אשראי), או מידע מאתרי Webmail כגון "ג'ימייל" או "הוטמיילי".

131 Information Commissioner's Office, Phorm Advertising – ICO Statement, Apr. 4, 2008, *available at* www.ico.gov.uk/upload/documents/pressreleases/2008/new_phorm_statement_040408.pdf (ההדגשה שלי – ע' ט').

מספקות), אזי עדיין מדובר בפגיעה בפרטיות.[132] בעקבות האפיון יקבל הגולש 12345 יחס מיוחד, מותאם אישית, המבוסס על צפייה בלתי מתפשרת בהרגליו, ברצונותיו, בתאוותיו, בפחדיו ובתחומי העניין שלו. מבחינת החברות המעורבות בפרויקט הגולש 12345 הוא אדם שקוף, אובייקט שנועד לפילוח ולשימוש לצורך הגברת הרווחיות. במובן מסוים, "תלישת" שמו של גולש 12345 והפיכתו למספר, למוצר, פוגעת יותר בכבודו האישי מאשר יצירת פרופיל אישי שלו המקושר לשמו. אותו מספר, אותו "no name" המופרד מהקהל ומיוחד לטיפול פרטני, הוא בדיוק התוצאה שדיני הגנת הפרטיות בכלל ודיני הגנת המידע בפרט נועדו למנוע[133] – שכן מי שעל יסוד פרופיל אישי מופרד היום מהכלל למטרות פרסום, עלול בעתיד להיות מופרד מהכלל לשם ביזוי או אפליה.

אפשר לטעון כי הבעיה ניתנת לפתרון בדרך של סיווג המידע שבידי חברות כמו "Phorm" ו־"NebuAd" כ"מידע אישי". אדרבה, הבה נקבע כי גם מידע "פסידונימי", כלומר מידע על אודות אדם מזוהה או ניתן לזיהוי לא רק בשמו אלא גם בתכונותיו ובהרגליו הייחודיים, הוא בגדר "מידע אישי". אמנם איננו יודעים מיהו הגולש 12345, אך אנו יודעים בדיוק "מהו" או "ממה הוא עשוי". אולם גם פתרון זה אינו נקי מספקות. דיני הגנת המידע מחייבים, למשל, להבטיח לנושא המידע זכות עיון במידע הנשמר על אודותיו וזכות לתקן מידע שנמצא שגוי ושעלול להטעות; אולם כיצד נבטיח לגולש 12345 זכות לעיין במידע על אודותיו אם איננו יודעים מיהו או יכולים לברר זאת? באופן כללי יותר, הזכות לפרטיות היא זכות יסוד חוקתית; כיצד יוכל הגולש 12345 לאכוף את זכויותיו אם אינו יודע ואינו יכול לדעת שהוא הוא?

פתרון אפשרי נוסף הוא הענקת זכות בחירה חופשית ומודעת לנושאי המידע. כלומר אם ירצו – יאפשרו נושאי המידע לספקית השירות לנתח את הרגלי הגלישה שלהם, ואם לא ירצו – יוכלו לחסות בצל האנונימיות. ואכן, חלק משמעותי מהדיון הציבורי בעניין השירותים שמספקות חברות כמו "Phorm" ו־"NebuAd" נסב סביב סוגיית ההסכמה וסביב השאלה אם ההסכמה חייבת להיות מפורשת (opt in) או שמא די בהסכמה מכללא, הנלמדת מאי־התנגדותו של הלקוח לתנאי השירות (opt out).[134] פתרון זה מבוסס על תפיסתה של הפרטיות כשליטה של אדם במידע אישי על אודותיו,[135] והוא מעניק את הכוח לנושאי המידע, להבדיל מהפקדתו בידיו של רגולטור הממונה על אינטרס הציבור. ואכן, יש הטוענים כי מסגרת ההגנה על פרטיות ועל מידע אישי בארצות הברית, המבוססת

132 Richard Clayton, *The Phorm "Webwise" System*, Apr. 23, 2008, www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

133 Ruth Gavison, *Privacy*, 89 Yale L.J. 421 (1980); בירנהק, לעיל ה"ש 23, בעמ' 59.

134 Chris Williams, *Information Commissioner: Phorm Must Be Opt-in Only*, The Register, Apr. 9, 2008, *available at* www.theregister.co.uk/2008/04/09/ico_phorm_tougher/; Ryan Paul, *NebuAd's "Breakthrough Opt-out" Approach: Legal or No?*, ArsTechnica, July 8, 2008, http://arstechnica.com/news.ars/post/20080708-nebuads-breakthrough-opt-opt-approach-legal-or-no.html.

135 Alan F. Westin, Privacy and Freedom 7 (1967); ראו גם בירנהק, לעיל ה"ש 23, בעמ' 41–44.

על הסדרים חוזיים ועל אכיפה פרטית, יעילה יותר מהמסגרת הרגולטורית האירופית, המפקידה כוח רב בידי ביורוקרטים שכלל לא ברור אם הם עוסקים בעיקר או בטפל.[136]

התלבטות דומה מתעוררת נוכח השימוש ההולך וגובר בשבבי RFID (Radio Frequency Identification). שבבי RFID הם תגים זעירים הנושאים משדר רדיו, שבאמצעותם אפשר לאגור ולשדר מידע על אודות חפץ, תעודה או אדם. קיימים שבבי RFID פסיביים, שאינם כוללים מקור כוח עצמאי ומופעלים רק בעזרת קורא חיצוני המצוי בדרך כלל במרחק קצר (סנטימטרים אחדים) מהשבב; לעומתם קיימים שבבי RFID אקטיביים, שהם בעלי מקור כוח עצמאי, נושאים מידע רב ויכולים לשדרו למרחק של מטרים אחדים. שבבי RFID הוכנסו לשימוש נרחב על ידי ענקית הקמעונאות "וול־מארט" ("Wal Mart") כאמצעי לניהול מלאי המחליף ומשפר את קוד הקווים (ה"ברקוד"). בניגוד לקוד הקווים, המוענק לסדרה שלמה של מוצרים, מזוהה כל שבב RFID באמצעות מספר ייחודי ומאפשר לעקוב אחרי כל מוצר ומוצר במהלך המחזור העסקי: החל מקבלת המוצר במחסן, עבור דרך אחסונו והוצאתו לחנות, וכלה בעמדת הקופאי. כך אפשר למנוע גניבות, להסיר מוצרים ישנים מהמדף ובאמצעות סריקה אוטומטית של סל המוצרים של הלקוח – לחסוך זמן יקר בקופות.[137]

עם השנים התרחבו שימושיהם של שבבי RFID, וכיום הם משמשים לניהול מערכות תחבורה ציבוריות (באמצעות "כרטיסים חכמים" המנהלים את חשבון הלקוח, כגון כרטיס ה"אויסטר" בלונדון – "Oyster card"), לגבייה בכבישי אגרה (כגון מכשיר ה"פסקל" בכביש 6), לאגירת מידע (ביומטרי ואחר) בתעודות זיהוי ודרכונים (כגון הדרכונים החדשים שהחלה ארצות הברית להנפיק בשנת 2006),[138] למעקב אחרי בעלי חיים (באמצעות התקנת שבב)[139] ולעתים גם להשתלה בגופם של בני אדם (למשל, לצורך גישה לתיק רפואי בשעת חירום או למעקב אחרי ילדים, אסירים או חוסים).[140]

---

136 ראו למשל ביקורתם של פרד קייט ואדוארדו אוסטרן: Fred H. Cate, *The Failure of Fair Information Practice Principles, in* Consumer Protection in the Age of the "Information Economy" 341–78 (Jane K. Winn Ed., 2006); Eduardo Ustaran, Editorial, *Changing the Directive*, 5(7) Data Protection L. & Pol'y (2008). יש לציין כי קייט אינו מציע להגדיל את חופש הבחירה של הלקוחות, שכן לדעתו ברוב המקרים מדובר בחופש מדומה. עם זאת הוא מבקר בחריפות את המנגנון הקיים באירופה, מנגנון הנוטה לחובות רישום ביורוקרטיות על פני הגנה אמתית לזכויות נושאי המידע.

137 ראו באופן כללי: Gal Eschet, *FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification*, 45 Jurimetrics 301 (2005); Jonathan Weinberg, *Tracking RFID*, 3 J. L. & Pol'y Info. Soc'y 777 (2008).

138 Grant Gross, *United States to Require RFID Chips in Passports*, PCWorld, Oct. 26, 2005, www.pcworld.com/article/123246/united_states_to_require_rfid_chips_in_passports.html.

139 ראו תקנות להסדרת הפיקוח על כלבים, התשס"ה-2005, ק"ת 6365.

140 Thomas C Greene, *Feds approve human RFID implants*, The Register, Oct. 14, 2004, *available at* www.theregister.co.uk/2004/10/14/human_rfid_implants.

לא אתייחס כאן לשאלות המתעוררות, כמובן, נוכח היכולת לסמן בני אדם באמצעות השתלת שבב, וגם לא לבעיות הנוגעות בשבבים האוגרים "מידע אישי", כגון אלה המוטבעים בכרטיסי נסיעה חכמים או בכרטיסי מועדון ברשתות השיווק – אלה אינם מעוררים שאלות הנוגעות בעצם ההגדרה של המונח "מידע אישי". שאלות כאלה מתעוררות דווקא נוכח השימוש בשבבי RFID שאינם אוגרים "מידע אישי", כלומר מידע על אודות אדם מזוהה או ניתן לזיהוי, אך עלולים לשמש בכל זאת לצורכי מעקב וחדירה לפרטיות. קחו למשל אסימונים נושאי שבב RFID המחולקים ללקוחותיה של רשת שיווק לשם הפעלת עגלות קנייה. בכל פעם שלקוח מבקר בחנות, המידע על אודות הרכב המוצרים שבעגלתו נאסף ומוטבע על השבב. באופן זה אוספת הרשת מידע על אודות הרגלי הצריכה של הלקוח ועל המיקום הגאוגרפי והשעות שבהם בחר לבקר בחנויות. מידע זה יכול לשמש ליצירת פרופיל של הלקוח ולסיווגו בהתאם לרמת הכנסתו המשוערת, לבריאותו, להרגלי חייו וכדומה. באמצעות פרופיל זה עשויה רשת השיווק להתאים ללקוח פרסומות (למשל, במסכים הפרוסים ברחבי החנות) ומבצעים, או אף לתמחר את מוצריה תמחור דינמי ומותאם אישית. אמנם, רשת השיווק אינה יודעת את שמו של הלקוח או פרטי זיהוי אחרים על אודותיו, אך בדומה ל־"Phorm" ול־"NebuAd" היא יוצרת פרופיל אישי מדויק שלו, המאפשר לה להבחין בינו לבין שאר הצרכנים ולהעניק לו יחס מיוחד (לטוב או לרע).

דוגמה נוספת היא סריקה של שבבי RFID שהותקנו בחנות אחת על ידי קורא בחנות אחרת. אחת התלונות העיקריות של פעילי הגנת פרטיות והגנת הצרכן כנגד טכנולוגיית ה־RFID היא כי שבבים שהותקנו לכאורה למטרת ניהול מלאי אינם מנוטרלים בנקודת המכירה. כך יוצא שלקוח עוזב את החנות עם בגדים, עם שעון, או עם חפצים אחרים, הנושאים שבב המכיל מידע על אודות המוצר והניתן לקריאה מרחוק. ברי כי אדם שנכנס לחנות כלשהי ומזוהה כנושא שעון "רולקס", מכשיר "בלאקברי" ומפתחות של מכונית "ב.מ.וו" מודל 2010 עשוי לזכות ליחס שונה מלקוח המזוהה כנושא שעון "סווטש", מכשיר טלפון סלולרי "דור ראשון" ומפתחות של "טוסטוס" מודל 1985. בשני המקרים הלקוח אינו מזוהה בשמו או בכתובתו, אך הוא מאופיין על ידי פרופיל המתאים לו אישית ומובחן מן הכלל לצורך קבלת יחס מיוחד.

גם במקרה של שבבי RFID, כמו בדוגמה של ניתוח התנהגותי על ידי "Phorm" ו־"NebuAd", ההגדרה המסורתית של "מידע אישי" מחמיצה דבר מה ומאפשרת פגיעה בפרטיותו של אדם בחסות החוק. ההתפתחות הטכנולוגית מובילה לכך שההבחנה בין מידע אישי לבין מידע שאינו אישי, כמו ההבחנה בין תוכן לבין נתוני תקשורת, מאבדת מכוחה הנורמטיבי. הטכנולוגיה מאפשרת ליצור פרופיל מדויק של אדם לא מזוהה ושאינו ניתן לזיהוי, אך הכפוף ליחס מיוחד על סמך הנתונים שנאספו על אודותיו.

ד. הפתרון

השופט איסטרברוק היה טוען ודאי כי הקושי ליישם כללים מתחומי המשפט המקובלים לענייני טכנולוגיים אינו מחייב את יצירתם של דיני טכנולוגיה חדשים, אלא את פיתוח הדוקטרינות המסורתיות והתאמתן למצב העובדתי החדש. אולם נראה שנוכח ההתפתחות

הרבה והמהירה של טכנולוגיות התקשורת ומערכות המידע, ההבחנות בין תוכן לבין נתוני תקשורת ובין מידע אישי לבין מידע שאינו אישי התערערו מן היסוד.

לצורך קביעתה של מסגרת חוקית חדשה להגנת הפרטיות בתקשורת ובמאגרי מידע, יש לוודא שמירה על עקרונות אחדים.

ראשית, יש להימנע מהבחנות דיכוטומיות ולהתבסס על רצף של מצבים שיסווגו בהתאם למידת הסכנה שהם מציבים לפרטיות. אפשר להתווכח ארוכות אם רשימת כתובות URL היא בגדר נתוני תקשורת (הפניית דפדפן לאתר) או בגדר תוכן (מסגירה את תוכן האתר), אך קשה לטעון שחשיפה של רשימת כתובות URL שבהן גלש אדם או ניתוח שלה אינה פוגעת בפרטיותו במובן האינטימי והחודרני ביותר. באופן דומה, אפשר לטעון כי פרופיל גולש 12345 שנאגר על ידי חברות כמו "Phorm" ו־"NebuAd" אינו מידע על אודות אדם מזוהה או ניתן לזיהוי, אך קשה לטעון שפרופיל כזה הוא חסר משמעות מבחינת פרטיותו של גולש 12345, יהא שמו אשר יהא. היכולת להשפיע על אדם מסוים בהתאם לניתוח מדוקדק של התנהגותו, של צרכיו או של המאפיינים שלו היא התופעה שעמה על החוק להתמודד. השאלה אם אותו אדם מזוהה או ניתן לזיהוי היא שאלה משנית. באופן דומה, על הדין לבחון את מידת הפגיעה בפרטיות הנגרמת עקב מעקב אחר תקשורת או תכתובת של אדם, ללא קשר לשאלה אם מדובר במעקב אחרי תוכן או אחרי נתוני תקשורת. כך, למשל, עלולה חשיפה של תדפיס שיחות טלפון של אדם לגרום להרס משפחתו או מעמדו המקצועי, אף שמדובר לכל הדעות בנתוני תקשורת ולא בתוכן.[141]

שנית, יש להבטיח שמירה על עקרונות משפטיים ניטרליים מבחינה טכנולוגית, נוכח המיזוג בין טכנולוגיות תקשורת שונות והשינויים המהירים בתחום זה. כך, למשל, הניסיון להגדיר במסגרת דיני האזנת סתר מהי "שיחה" על פי קריטריונים טכנולוגיים (כגון סוג המכשיר, סוג האות או אופן החיבוריות) נועד לכישלון. הפיכת האינטרנט מפלטפורמת תקשורת לפלטפורמת המחשוב ואגירת המידע הבסיסית (Cloud Computing)[142] והגברת הקישוריות בין מכשירים שונים באמצעות שבבי RFID ליצירת "אינטרנט של חפצים" (Internet of Things),[143] מחייבות חשיבה חדשה המבוססת על עקרונות יציבים, להבדיל מהבחנות פורמליות הנסמכות על מאפיינים טכנולוגיים חולפים.

שלישית, יש לאתר פתרונות המעצימים את הפרט ולא פתרונות המבוססים על רגולציה. הענקת זכות בחירה אמיתית ללקוח מקהה את מידת הפגיעה בפרטיותו. סריקת תוכן הודעות הדואר האלקטרוני (שהוא ללא ספק תוכן של שיחה) על ידי "גוגל" במסגרת שירות "Gmail" והצבת פרסומות מותאמות אישית לצדן לא פגעה בהיקף השימוש בשירות, אף שהלקוחות ידעו על החדירה לתוכן שיחותיהם ולמרות הסערה הציבורית

141 **ראו למשל עניין אלון־לאופר**, לעיל ה"ש 31.

142 **ראו למשל:** Julian Sanchez, *Pew Study: Cloud Computing Popular, Privacy Worries Linger*, Ars Technica, Sept. 14, 2008, *available at* http://arstechnica.com/news.ars/post/20080914-pew-cloud-computing-study-debuts-at-google-event-in-progress.html; Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 Nw. U. L. Rev. Colloquy 1 (2008).

143 **ראו למשל:** L. Jean Camp, Kalpana Shankar & Kay Connelly, *Systematic Design for Privacy in Ubicomp* (Jan. 2006), *available at* http://ssrn.com/abstract=889444.

שהתעוררה בתחילה.[144] הלקוחות בחרו לשלם את "מחיר" השירות, הניתן ללא תשלום, בדרך של פגיעה בפרטיותם. אם לקוחותיהן של ספקיות שירותי האינטרנט יבחרו להצטרף לשירות האפיון של "Phorm" ו־"NebuAd" כדי להוזיל את מחיר המינוי החודשי או כדי לשפר את חוויית הגלישה, למשל, יש לכבד את בחירתם. פרטיות היא שליטה במידע; אם אדם מוותר על השליטה באופן רצוני ומודע – אין פסול בכך.[145] מערכות רגולטוריות ביורוקרטיות עלולות ליצור אשליה של הגנה מבלי לספק לאזרח הגנה משמעותית באמת, ולהדגיש היבטים פורמליסטיים של החוק על פני היבטים מהותיים.[146]

144 Kim Zetter, *Free E-Mail With a Steep Price?*, Wired News, Apr. 1, 2004, *available at* www.wired.com/news/business/0,1367,62917,00.html; Matthew A. Goldberg, *The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 Lewis & Clark L. Rev. 249, 250 (2005); Jason Isaac Miller, *Note, "Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights*, 33 Hofstra L. Rev. 1607 (2005).

145 בירנהק, לעיל ה"ש 23.

146 לעניין החובה לרשום מאגרי מידע ראו למשל דוח שופמן, לעיל ה"ש 72, בעמ' 26-27.