פגיעה בפרטיות באמצעות נוזקת מעקב

אחריות תורמת של היצרן

עיתונאים, פעילי זכויות אדם ומתנגדי משטר עשויים להיות תחת מעקב תמידי וחודרני שלא נראה כמותו בעבר. נוזקת מעקב מוחדרת בהיחבא למכשירי הטלפון שברשותם ומאפשרת למפעילה גישה לכל אורחות חייהם ומחשבותיהם: ללוח הזמנים שלהם ולמיקומם הגיאוגרפי, לתכתובת ההודעות האישיות שלהם, לתמונות ולסרטונים שצילמו במכשיר ואף לשיחות שניהלו בין באמצעות המכשיר ובין שלא. מעקבים אלו פוגעים בזכויות יסוד כגון הזכות לחופש ביטוי והזכות לפרטיות ומובילים לאפקט המצנן את חופש העיתונות.

רחל ארידור הרשקוביץ

מחקר
מדיניות
197

המכון הישראלי
לדמוקרטיה

המכון הישראלי
לדמוקרטיה

מחקר מדיניות 197

פגיעה בפרטיות באמצעות נוזקת מעקב

אחריות תורמת של היצרן

רחל ארידור הרשקוביץ

ספטמבר 2024

Violation of Privacy by Spyware:
The Manufacturer's Contributory Infringement

Rachel Aridor-Hershkovitz

עריכת הטקסט: חמוטל לרנר
עיצוב הסדרה והעטיפה: סטודיו Alfabees
ביצוע גרפי: אירית נחום
הדפסה: גרפוס פרינט, ירושלים

מסת"ב: 978-965-519-458-6

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר – כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו"ל.

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר), 2024

נדפס בישראל, תשפ"ד/2024

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים:
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800

כל פרסומי המכון ניתנים להורדה חינם, במלואם או בחלקם, מאתר האינטרנט.

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

הדברים המובאים במחקר מדיניות זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.

תוכן העניינים

תקציר	7
מבוא	11
פרק 1. דוקטרינת ההפרה התורמת	17
1.1. ארצות הברית: מסוני ועד גרוקסטר	17
1.2. האיחוד האירופי	26
1.3. ישראל	38
1.4. סיכום: דוקטרינת ההפרה התורמת – משפט משווה	47
פרק 2. הזכות לפרטיות וחשיבותה	51
פרק 3. תעשיית נוזקות המעקב והפגיעה בפרטיות	64
3.1. נוזקות מעקב, השימוש לרעה בהן ופגיעתן בפרטיות ובזכויות נוספות	64
3.2. סיכום	73
פרק 4. אוזלת היד של האסדרה החקיקתית הקיימת של השימוש בנוזקות מעקב – סקירת משפט משווה	76
4.1. המשפט הבינלאומי	76
4.2. האיחוד האירופי	91
4.3. ארצות הברית	106
4.4. ישראל	114
4.5. סיכום סקירת המשפט המשווה	121
פרק 5. אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות – הבסיס העיוני ושיקולי המדיניות	125
5.1. שיקולי מדיניות המצדיקים את אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכלל ובהקשר של נוזקות מעקב בפרט	127
5.2. שיקולי מדיניות השוללים את אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכלל, ובהקשר של נוזקות מעקב בפרט	134
5.3. סיכום	145

פרק 6. דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות – התנאים לתחולתה ויישומם בהקשר של נוזקות מעקב 149

6.1. קיומה של הפרה ישירה 150

6.2. מודעות המפר התורם 151

6.3. תרומה משמעותית, ניכרת וממשית 154

6.4. סיכום – יישום דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות בנסיבות של שימוש לא חוקי בנוזקת מעקב המוביל לפגיעה בפרטיות 155

פרק 7. סיכום 158

תקציר

בשנים האחרונות התרבו העדויות בדבר השימוש שעושים משטרים שונים, ברובם לא דמוקרטיים, בנוזקות מעקב לשם איסוף מידע על עיתונאים, פעילי זכויות אדם, עורכי דין ומתנגדי משטר. נוזקות מעקב אלו מוחדרות באופן חשאי לחלוטין למכשיר הטלפון הנייד של יעד המעקב, ומאפשרות למפעיליהן לשאוב מידע רב האגור על גבי המכשיר או זמין באמצעות החיישנים שבו: תמונות, הודעות טקסט, קובצי וידיאו ואודיו, יומן פגישות וכל תוכן אחר הזמין באמצעות המכשיר הנייד. כמו כן, מפעיל הנוזקה יכול לעקוב אחר נתוני המיקום של המכשיר, להפעיל מרחוק את המיקרופון והמצלמה המותקנים בו, להטמיע במכשיר קבצים ונתונים כרצונו ואף לעשות שימוש ביישומונים המותקנים במכשיר. מכאן שנוזקות המעקב מאפשרות לגבש תמונה מפורטת ומדויקת של חייו האישיים של יעד המעקב, לרבות קשריו החברתיים והמקצועיים, דעותיו ומחשבותיו. רמת החודרנות שלהן עשויה להוביל להשתקת כל ביקורת נגד המשטר ולפגיעה אנושה בחופש העיתונות ובזכויות אדם, ובראשן הזכות לחופש ביטוי ולפרטיות.

עם זאת, נוזקות מעקב הן טכנולוגיות דו־שימושיות: לצד השימוש לרעה בהן, הן יכולות גם לסייע לרשויות הביון ואכיפת החוק במאמצי הלוחמה בטרור ובפשיעה. למשל, באירופה סייעו נוזקות מעקב לחשיפתם ומעצרם של חשודים בפדופיליה בלמעלה מ־40 מדינות. התרת המשך השימושים החוקיים בנוזקות מעקב, לצד התמודדות עם השימושים הבלתי חוקיים בהן ומניעה או מזעור של הפגיעה בפרטיות שהן גורמות, היא אתגר גדול לחברה ולמשפט.

אף שהיצוא של נוזקות מעקב נתון לרגולציה מחמירה, האסדרה הקיימת במישור הבינלאומי אינה נותנת מענה מספק לצורך למנוע את הפגיעה החריפה והרחבה בזכות היסוד לפרטיות, שכן היא מתמקדת בעיקרה בשיקולי ביטחון המדינה ויחסי החוץ שלה. ארצות הברית וישראל מיישרות קו ומתמקדות גם הן בשיקולים הקשורים להגנה על ביטחון המדינה ויחסי החוץ שלה, ולא בהגנה על הזכות לפרטיות, בכל הנוגע למתן רישיונות ליצוא נוזקות מעקב. באיחוד האירופי התמונה שונה מעט, והרגולציה מביאה בחשבון שיקולים הקשורים להגנה על הזכות לפרטיות, וכן מכפיפה את הפגיעה בפרטיות הנגרמת בשל שימוש רשויות האכיפה והביון בנוזקות מעקב לדרישת הנחיצות ולמבחן מידתיות.

בהיעדר כלים יעילים להתמודד עם הפגיעה החמורה בפרטיות עקב השימוש לרעה בנוזקות מעקב, מחקר זה מציע לבחון את אימוצה של דוקטרינת ההפרה התורמת מדיני הקניין הרוחני כאמצעי חלופי להגנה על זכותו לפרטיות של מי שהיה נתון למעקב חודרני כל כך.

אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בישראל אפשרי מכוח צינור הקליטה שבסעיף 12 לפקודת הנזיקין. אימוץ הדוקטרינה יכול להוביל לחיזוק נחוץ של הזכות לפרטיות, ויש בו כדי להשיב את המשקל הראוי לערכים שבבסיס הזכות לפרטיות – אשר נגזרת מהזכות לכבוד, הכרחית לגיבוש זהותו ותפיסתו העצמית של הפרט ולקבלת החלטות עצמאית, וחיונית לשם הגנה על זכויות אחרות כגון הזכות לחופש ביטוי ולשוויון. כן תפתור דוקטרינת ההפרה התורמת את כשלי השוק המאפיינים שווקי מידע.

ואולם, אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי לעורר כשלי אכיפה משמעותיים. האחד נוגע להגדרת הזכות לפרטיות והתנאים להפרתה: כיצד יכול בית משפט בישראל לקבוע אם הופרה פרטיותו של עיתונאי ממקסיקו עקב השימוש בנוזקת מעקב פרי פיתוחה של חברה ישראלית? האם יבחן את הפגיעה בפרטיות לפי הדין בישראל או שמא לפי הדין במקסיקו? כיצד תקבע החברה המפתחת מהי פגיעה בפרטיות ומתי אין לעשות שימוש בטכנולוגיה פרי פיתוחה? האם עליה לבחון את דיני הפרטיות, העונשין והלוחמה בטרור בכל אחת מהמדינות שבהן פועלים לקוחותיה? עם זאת, כשל אכיפה זה עשוי להצטמצם עם התרחבות השפעת ה־GDPR, המביא עימו גם האחדה מסוימת בהגדרת הזכות לפרטיות והתנאים לפגיעה בה.

כשל האכיפה האפשרי השני נוגע לסמכות השיפוט: כיצד יכול בית משפט בישראל (או במדינה אחרת שבה תוגש תביעה) לדון בתביעה נגד חברה המפתחת נוזקת מעקב בגין שימוש שעשתה רשות שלטונית במדינה אחרת בנוזקת המעקב שפיתחה? זאת ועוד, אף בהנחה שאפשר להוכיח הפרה ישירה של הזכות לפרטיות, המפר הישיר עשוי ליהנות מטענות הגנה, בעיקר כאשר מדובר ברשות שלטונית.

נוסף על כך, שיקולים של צדק חלוקתי לא בהכרח תורמים לקביעה שמפתחי נוזקות מעקב הם מונע הנזק הזול. לטענת החברות המפתחות נוזקות מעקב, רישיונות השימוש בנוזקות המעקב שפיתחו מוגבלים רק לרשויות ביון ואכיפת חוק מדינתיות ולמטרות לגיטימיות של לוחמה בטרור ובפשיעה. כמו כן, החברות נתונות ממילא לרגולציית ייצוא מכבידה, ואימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי להטיל עליהם נטל כבד מנשוא ולהבריח אותן מחוץ לישראל כדי לפעול במדינות שבהן המשטר המשפטי מקל יותר.

כשלי אכיפה אלו מקבלים ביטוי בבחינת יישומם של שלושת התנאים להחלת דוקטרינת ההפרה התורמת: קיומה של הפרה ישירה, תרומה ממשית וקונקרטית של גורם ביניים להפרה, ומודעות בפועל של המפר התורם. באשר להוכחת הפרה ישירה, הקושי אינו נעוץ בשאלה אם הופרה הזכות לפרטיות אלא בשאלה של הטלת אחריות תורמת על גורם הביניים שעה שהמפר הישיר נהנה מחסינות מפני תביעה. עם זאת, העובדה שבתי המשפט המשיכו בבחינת אחריותו התורמת של גורם הביניים להפרת זכות יוצרים גם כאשר המפירים הישירים נהנו מטענת הגנה, מתוך רצון להעניק סעד כלשהו לנפגע לנוכח הנזק המשמעותי שנגרם לו, עשויה להיות רלוונטית גם כאן. באשר לדרישת המודעות, החברות המפתחות נוזקות מעקב מקפידות לפעול בהתאם למשטרי הייצוא המדינתיים וקהל הלקוחות המוצהר שלהן הוא רשויות ביון ואכיפת חוק במדינה, ועל כן טוענות כי לגיטימי מצידן להניח שלקוחות אלו יפעלו כדין לשם הגשמת תכליות לגיטימיות וחשובות, כגון ביטחון הציבור, הביטחון הלאומי, לוחמה בטרור ומניעת פשיעה. לא זו אף זו, לטענתן אין הן נחשפות כלל למידע האישי הנאסף באמצעות נוזקת המעקב אלא רק להיבטים הטכניים הקשורים בתפעולה. משום כך, לטענתן, אין להן מודעות בפועל, ממשית וקונקרטית, לפגיעה בפרטיות.

עם זאת, בנסיבות מסוימות אפשר להוכיח מודעות בכוח, או לפחות עצימת עיניים מכוונת העולה כדי מודעות בכוח. כך, למשל, החברות מפתחות נוזקות מעקב תוך ידיעה שאלו מאפשרות רמת חודרנות חסרת תקדים, אך למרות מודעותן לפגיעה אפשרית זו בזכות לפרטיות הן נמנעות מנקיטת אמצעים טכנולוגיים ומינהליים כדי למזער את הסיכון לשימוש לרעה בנוזקות המעקב.

הפרשנות הלא־אחידה של דרישת המודעות במסגרת דוקטרינת ההפרה התורמת בדיני זכויות יוצרים בארצות הברית, בצד ההכרה באיחוד האירופי במודעות בכוח באמצעות עצימת עיניים מכוונת במקרים מסוימים, השאירה פתח לקביעה כי מודעות בכוח עשויה להיות מספקת לשם הטלת אחריות תורמת על גורם הביניים.

זאת ועוד, לאור הערכים החשובים שבבסיס הזכות לפרטיות וחולשתה של הזכות נוכח התפתחויות טכנולוגיות והפריחה של תחום טכנולוגיות המעקב, יש לדעתי אינטרס ציבורי במתן תמריץ, באמצעות אימוץ דוקטרינת ההפרה התורמת, למפתחי נוזקות המעקב להגדיר באופן מדויק יותר את הפונקציונליות של הנוזקות ואת תנאי רישיון השימוש שלהן. האיזון בין חיזוק הזכות לפרטיות לבין אינטרס הציבור בביטחון ציבורי ולאומי, וההתמודדות עם כשלי האכיפה הנלווים לאימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות, צריכים להיעשות בהחלת הדוקטרינה בנסיבות כל מקרה ומקרה, ואינם צריכים להיות שיקול בהחלטה המקדמית אם נכון לאמץ את דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות. דוקטרינת ההפרה התורמת תהיה כלי נוסף בארגז הכלים הקיים לשם התמודדות עם פגיעות חמורות בזכות לפרטיות. אין זה הכלי העיקרי, והכוונה אינה להציבו כחלופה לאסדרת השימוש בנוזקות מעקב. עם זאת, דוקטרינת ההפרה התורמת היא כלי שיורי וחשוב, שאף שלצד יתרונותיו עשויים להיות לשימוש בו גם חסרונות, יש בידו כדי לסייע ולתרום לחיזוק הנחוץ וההכרחי של הזכות לפרטיות.

מבוא

חייה של חדיג׳ה איסמאילובה, עיתונאית מבאקו שבאזרבייג׳אן, הפכו לגיהינום. דיווחיה על השחיתות במדינתה עוררו עליה את זעם השלטונות. היא מצאה את עצמה נתונה למעקב תמידי אחר תנועותיה, חבריה ומשפחתה התבקשו פעמים רבות לרגל אחריה, ומצלמות שהותקנו בחשאי בביתה תיעדו אותה ברגעים אינטימיים. היא נעצרה והואשמה בסיוע להתאבדות של עמית ובהעלמת מס, ונשלחה לשבע שנות מאסר. כשנה וחצי לאחר כליאתה שוחררה למעצר בית ונאסר עליה לעזוב את המדינה למשך חמש שנים, שבמהלכן ביתה הפך עבורה לכלא. כשהותר לה לעזוב את המדינה היא היגרה לאנקרה שבטורקיה בתקווה להימלט מעיני המשטר, לחיות באופן חופשי וללא חשש ולהמשיך לדווח על מעשי השלטון ממקומה הבטוח בגלות. שלוש שנים מאוחר יותר המציאות טפחה על פניה כאשר התברר לה שהייתה נתונה למעקב חשאי וחודרני לאין שיעור: במכשיר הטלפון הנייד שברשותה הותקנה נוזקת המעקב ״פגסוס״, פרי פיתוחה של חברת NSO הישראלית. המידע שנאסף באמצעות נוזקת המעקב סיכן לא רק את חייה של איסמאילובה עצמה, אלא גם את חיי משפחתה, חבריה והמקורות שעליהם הסתמכה בדיווחיה החדשותיים.[1]

1 Phineas Rueckert, *Pegasus: The New Global Weapon for Silencing Journalists*, Forbidden Stories (July 18, 2021) (להלן: Rueckert, *Pegasus*).

איסמאילובה אינה היחידה. לפחות 180 עיתונאים, עורכי דין, פעילי זכויות אדם, מתנגדי משטר ואקטיביסטים פוליטיים היו נתונים בשנים האחרונות למעקב חודרני ביותר באמצעות נוזקות מעקב שהותקנו בחשאי במכשירי הטלפון הסלולריים שלהם – מעקב שמטרתו זריעת פחד, פגיעה חמורה בזכות היסוד לחופש ביטוי, השתקת ביקורת וחסימת התנגדות למשטר.[2]

נוזקות מעקב הן תוכנות מחשב אשר מנצלות חולשות במכשירי טלפון ניידים של משתמשים מזוהים מראש, והתקנתן אינה מחייבת מעורבות מצד חברות הטלפוניה והסלולר. משהותקנו הן מעניקות למפעיליהן גישה מלאה למכשיר הטלפון הנייד של הנעקב וכמעט אינן מותירות עקבות פורנזיים לפעילותן. נוזקות מעקב יכולות לאפשר למפעיליהן לשאוב מהמכשיר מידע מגוון: תמונות, הודעות טקסט, קובצי וידיאו ואודיו, כולל שיחות קוליות, סיסמאות ליישומונים אחרים המותקנים על גבי המכשיר ונתוני המיקום של המכשיר, והכול ללא מגבלה גיאוגרפית. כמו כן, מפעילי הנוזקה יכולים להפעיל מרחוק את המיקרופון והמצלמה של המכשיר הנעקב וכן יישומונים אחרים המותקנים בו.[3]

לשימוש בנוזקות מעקב עשויים להיות יתרונות והצדקות. השימוש יכול לסייע לרשויות הביון ואכיפת החוק במאמצי הלוחמה בטרור ובפשיעה. כך, למשל,

2 **שם**; Phineas Rueckert, *"Jaw-Dropping" Targeting: How Pegasus Was Used Against Critical Journalists in El Salvador*, Forbidden Stories (Jan. 13, 2022) (להלן: Rueckert, *"Jaw-Dropping" Targeting*); Ronen Farrow, *How Democracies Spy On Their Citizens*, The New Yorker (April 18, 2022)

3 Hendrik Mildebrath, Europe's PegasusGate: Countering Spyware Abuse 3 (European Parliamentary Research 2022); Marcin Rojszczak, *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses*, 29 Eur. J. Crime Crim. L. & Crim. Just. 290, 300 (2021); Ottavio Marzocchi & Martina Mazzini, Pegasus and Surveillance Spyware 4 (Policy Department for Citizens' Rights and Constitutional Affairs for the European Parliament's Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, 2022); European Data Protection Supervisor, Preliminary Remarks on Modern Spyware 3–5 (Feb. 2022)

נוזקת המעקב פגסוס של חברת NSO סייעה לרשויות במקסיקו לתפוס את ברון הסמים הידוע בכינוי אל צ'אפו. באירופה נעשה שימוש בנוזקת המעקב פגסוס כדי להביא לחשיפתם ולמעצרם של חשודים בפדופיליה ביותר מ־40 מדינות.[4]

אולם לצד השימושים החוקיים והמוצדקים בנוזקות מעקב, השימוש בהן יכול להוביל גם לפגיעה חמורה בזכות החוקתית לפרטיות. נוזקת מעקב היא כלי חודרני הרבה יותר מיירוט נתוני תקשורת מחברת הטלפוניה והסלולר. האחרון מאפשר איסוף נתונים דוגמת מספר הטלפון שיזם את השיחה, יעד השיחה, מיקום המכשיר, תא השטח שבו שהה מבצע השיחה או שממנו נשלחה הודעת טקסט והיסטוריית הגלישה באינטרנט, בדומה לפעילותו של "הכלי" של השב"כ.[5] נוזקת מעקב, מנגד, מאפשרת לגבש תמונה מפורטת ומדויקת של חייו האישיים של יעד המעקב, לרבות קשריו החברתיים והמקצועיים, דעותיו ומחשבותיו.[6] לפיכך לא בכדי מתייחסים לנוזקות מעקב כגורם שמשנה את כללי המשחק (game changer), שינוי פרדיגמה של ממש מבחינת הגישה לתקשורת פרטית, אשר משלב רמת פולשנות שאין שנייה לה עם מאפיינים שהופכים כל אמצעי אבטחה משפטי או טכני לחסר משמעות.[7]

נוזקות מעקב נחשבות אפוא "טכנולוגיות דו־שימושיות" (dual use technologies): לצד השימושים החוקיים, המוצדקים והמועילים בהן, יכולים להיות להן גם שימושים פוגעניים ובלתי חוקיים. החיסרון הבולט ביותר של טכנולוגיית המעקב הוא הפגיעה בזכות היסוד לפרטיות ובאמצעותה בזכויות יסוד אחרות, דוגמת הזכות לחופש ביטוי.

4 Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, The New York Times Magazine (Jan. 28, 2022)

5 רונן ברגמן ועידו שברצטוך "'הכלי', מאגר המידע הסודי של השב"כ, אוסף נתונים על כל אזרחי מדינת ישראל ויודע: איפה הייתם, עם מי דיברתם, ומתי עשיתם את כל זה" **ידיעות אחרונות: 7 ימים** 25.3.2020.

6 Farrow, **לעיל** ה"ש 2; Ron Deibert, *Protecting Society from Surveillance Spyware*, 38 (2) Issues Sci. Tech. 15 (2022)

7 European Data Protection Supervisor, **לעיל** ה"ש 3, בעמ' 2, 4–5.

ההתמודדות עם השימושים הבלתי חוקיים בנוזקות מעקב תוך מניעה או מזעור של הפגיעה בפרטיות, לצד התרת המשך השימושים החוקיים בהן, היא אתגר גדול המונח לפתחם של החברה והמשפט. תעשיית נוזקות המעקב נתונה לרגולציה בינלאומית ומדינתית מחמירה על בסיס הגדרת הנוזקות כטכנולוגיה דו־שימושית בהסדר ואסנאר.[8] עם זאת, הדו־שימושיות תחת הסדר ואסנאר היא בעלת משמעות שונה מהדו־שימושיות שבה עסקנו עד כה: אין הכוונה למוצר שיכול לשמש למטרות חוקיות לצד מטרות בלתי חוקיות, אלא למוצר המשמש למטרות אזרחיות לצד מטרות צבאיות. זאת ועוד, רגולציה בינלאומית ומדינתית זו כלל אינה מספקת מענה מתאים לפגיעה האפשרית בזכות החוקתית לפרטיות באמצעות נוזקות מעקב.

קושי נוסף הוא שדיני הגנת הפרטיות בארץ ובעולם אינם מעמידים סעד הולם או יעיל לרשות מי שפרטיותו נפגעה מהפעלת נוזקת מעקב. דינים אלו נשענים, רובם ככולם, על עקרונות ניהול מידע הוגן (fair information practices, FIPs) שגובשו בסוף שנות השבעים ובתחילת שנות השמונים של המאה הקודמת, תוך שילוב מצומצם של רעיונות חדשים כגון עיצוב לפרטיות (privacy by design) – אף שמידע אישי נעשה בשנים האחרונות נכס סחיר בעל ערך רב ובסיס לכלכלת המידע.[9] כמו כן, בעקבות עליית קרנו של מידע אישי כנכס סחיר בעל ערך רב, מעמדה של הזכות לפרטיות נשחק ונחלש, והכלים העומדים לרשותו של נפגע בודד מוגבלים ואינם יעילים. זאת ועוד, בכל הנוגע לנוזקת מעקב, פעמים רבות קשה עד בלתי אפשרי לאתר את המפר הישיר, הוא לקוח הקצה אשר הפעיל את נוזקת המעקב, לנהל נגדו הליך משפטי ולזכות בסעד אכיף ויעיל.

מחקר זה מעלה את האפשרות לעשות שימוש בכלי מהמשפט האזרחי – דוקטרינת ההפרה התורמת – כדי לבחון את אחריותו של מפתח נוזקת

8 הסדר בינלאומי שנחתם בדצמבר 1995, אשר מעגן את הכללים המנחים לאסדרת היצוא של כלי נשק ומוצרים שעשויים להיות להם שימושים צבאיים לצד שימושיים אזרחיים. למידע נוסף על ההסדר ראו בטקסט הנלווה לה"ש 185–190 **להלן**.

9 Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 Yale J. L. & Tech. 256, 260–261 (2020) (להלן: Lev-Aretz & Strandburg, *Privacy Regulation*).

מעקב לשימוש לרעה הנעשה בטכנולוגיה שלו לשם פגיעה בפרטיות. דוקטרינת ההפרה התורמת עשויה להיות אפיק חלופי שיעניק סעד משפטי למי שזכותו לפרטיות נפגעה בשל השימוש בנוזקת מעקב, ותוכל לתת בידי החברה והמשפט כלי לסימון קו הגבול שבין שימושים חוקיים בנוזקות מעקב לשימושים לא חוקיים או לא רצויים מבחינה חברתית, כמו גם להשפיע, ולו במעט, על אופני הפיתוח והשימוש העתידיים בנוזקת מעקב.

בבסיסה של דוקטרינת ההפרה התורמת מצויה השאלה אם יצרן טכנולוגיה דו־שימושית אחראי לשימוש שעושה משתמש הקצה ומוביל לפגיעה לא חוקית בזכותו של אדם. אין זו סוגיה חדשה: כבר לפני 40 שנים עסקו בתי המשפט בארצות הברית בשאלת אחריותו של יצרן טכנולוגיה דו־שימושית לשימוש לא חוקי הגורם לפגיעה בזכויות יוצרים הנעשה בטכנולוגיה שלו, בפסק הדין הנודע בפרשת **סוני**.[10] עם זאת, השאלה לא נבחנה בהקשר של נוזקת מעקב המאפשרת פגיעה בזכות היסוד לפרטיות. מחקר זה מבקש לבחון האם ובאילו תנאים אפשר לאמץ את דוקטרינת ההפרה התורמת גם לדיני הגנת הפרטיות, ומהם שיקולי המדיניות הרלוונטיים לאימוץ כזה.

בפרק הראשון של המחקר תוצג סקירה של התפתחות דוקטרינת ההפרה התורמת בדיני זכויות היוצרים ועיגונה בדין בארצות הברית, באיחוד האירופי ובישראל. בפרק השני אבחן את ההצדקות התיאורטיות לזכות לפרטיות ואצביע על חשיבות הערכים שבבסיסה. בפרק השלישי אסקור בהרחבה את כל הידוע על נוזקות מעקב והשימושים החוקיים והבלתי חוקיים שנעשו בהן, ובפרק הרביעי – את האסדרה באמצעות חקיקה של פיתוחן, יצואן והשימוש בהן במישור הבינלאומי, בארצות הברית, באיחוד האירופי ובישראל. בפרק החמישי אסקור את הבסיס העיוני לאימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות, ואבחן בהרחבה את שיקולי המדיניות בעד ונגד אימוץ הדוקטרינה תוך עמידה על הדומה והשונה בין הזכות לפרטיות לזכות היוצרים, והדגשת היתרונות והחסרונות הטמונים באימוץ שכזה. בפרק השישי אבחן, על בסיס שיקולי המדיניות הרלוונטיים, את יישומם של התנאים להחלתה של

10 Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984) (להלן: פרשת **סוני**).

דוקטרינת ההפרה התורמת מדיני זכויות היוצרים על פגיעה בזכות לפרטיות עקב שימוש בנוזקת מעקב. הפרק השביעי ייחד לסיכום ולמסקנות.

***

אני מודה להוצאה לאור של המכון הישראלי לדמוקרטיה ולעורכת חמוטל לרנר על העבודה המסורה. תודה לד"ר תהילה שוורץ אלטשולר, לעו"ד איה מרקביץ, לד"ר דנה בלאנדר ולפרופ' סוזי נבות על הערותיהן החשובות.

פרק 1

דוקטרינת ההפרה התורמת

האם יצרן של מוצר טכנולוגי דו־שימושי, כלומר מוצר שעשויים להיות לו שימושים חוקיים אך גם שימושים לא חוקיים, אחראי לשימושים הלא חוקיים במוצר? ואם כן, באילו תנאים?

שאלה זו התעוררה בארצות הברית בשנות השמונים של המאה הקודמת בהקשר של הפרת זכויות יוצרים. הקושי שהציבה שאלה זו מלכתחילה לפני בתי המשפט היה היעדר מערכת יחסים מתמשכת וישירה של פיקוח כלשהו בין יצרן הטכנולוגיה למשתמשי הקצה בה – בניגוד, למשל, למערכת היחסים בין משכיר אולם אירועים לשוכר, או בין מעסיק לעובד, אשר יוצרת מנגנוני פיקוח ושליטה של המשכיר או המעסיק על מעשיהם של השוכרים או העובדים. הדיונים בסוגיית אחריותו של יצרן טכנולוגיה להפרות זכויות היוצרים בידי המשתמשים בה הובילו לפיתוחה של דוקטרינת ההפרה התורמת, תחילה בארצות הברית ובהמשך באירופה ובישראל, כפי שיתואר להלן.

1.1. ארצות הברית: מסוני ועד גרוקסטר

דוקטרינת ההפרה התורמת (contributory liability) בדיני זכויות יוצרים היא הרחבה יציר המשפט המקובל של עקרון האחריות הקבוע בדיני זכויות היוצרים. שורשיה הנורמטיביים נעוצים בהיעדר איסור מפורש בדין על הטלת אחריות על מפר תורם, וכן בעובדה שעקרון האחריות התורמת מקובל בדיני הנזיקין ובדיני הפטנטים.[11] ראשיתה של הדוקטרינה בשנת 1911, אז פסק בית המשפט העליון בארצות הברית שחברה שהעסיקה עובד במטרה שיכתוב תסריט המבוסס על ספר אחראית להפרה הישירה שביצע העובד, וכן להפרה

11 39 U.S.C.A. §271(C) (1994); John M. Moye, *How Sony Survived: Peer-to-Peer Software, Grokster, and Contributory Copyright Liability in the Twenty-First Century*, 84 N.C. L. Rev. 646, 653 (2006)

הישירה שביצעה חברת הפקת הסרטים שרכשה ממנה את התסריט.[12] בפסקי הדין שניתנו בשנים הבאות התבססה הדוקטרינה כאפיק להטלת אחריות על מי שמספק לאחֵר אמצעים להפרה, מודע להפרה, שולט על השימוש ביצירות מוגנות בזכות יוצרים או מתיר שימוש כאמור ללא רשות בעל זכות היוצרים.[13] ההכרה במודעותו של גורם הביניים התבססה, רובה ככולה, על הקשר בינו לבין המפר הישיר, ההיכרות ביניהם ויכולתו של גורם הביניים לשלוט במעשיו של המפר הישיר.[14]

בשנת 1976 נחקק חוק זכויות יוצרים חדש בארצות הברית,[15] אולם אף שבית המשפט כבר פיתח את דוקטרינת ההפרה התורמת, המחוקק לא שילב בחוק הוראות המעגנות אותה. עם זאת, לפי היסטוריית החקיקה נראה שהמחוקקים ביקשו להכיר בדוקטרינת ההפרה התורמת באמצעות ההכרה המפורשת בזכות הבלעדית של בעל זכות היוצרים להתיר את השימוש ביצירתו.[16]

בפרשת **סוני** (1984) הכיר בית המשפט בקיומה של דוקטרינת ההפרה התורמת יצירת הפסיקה ובחיזוק שניתן לה בהיסטוריה החקיקתית של חוק זכויות היוצרים משנת 1976. ואולם, בית המשפט הבהיר שנסיבות המקרה שונות, משום שאין מדובר במערכת יחסים של מודעות, שליטה או פיקוח כמו במקרה של בעלי אולם קונצרטים, בעלי אולם אירועים או בעלי חנות המוכרת קלטות

12 ראו Connie Davis Powell, *The Saga Continues: Secondary Liability for Copyright Infringement: Theory, Practice and Predictions*, Akron Intell. Prop. J. 189, 191 (2016), המתאר את פסק הדין בפרשת Kalem Co. v. Harper Bros., 222 U.S. 55 (1911).

13 Powell, **לעיל** ה"ש 12, בעמ' 191–192.

14 Methaya Sirichit, *Catching the Conscience: An Analysis of the Knowledge Theory Under §512(c)'s Safe Harbor & The Role of Willful Blindness in the Finding of Red Flags*, 23 Alb. L.J. Sci. & Tech. 85, 99–100 (2013)

15 Copyright Act of 1976, 17 U.S.C. §§101–810 (1976)

16 ראו Powell, **לעיל** ה"ש 12, בעמ' 191–192.

ריקות ושירות הקלטה והעתקה.[17] בפרשת **סוני** דובר על יצרן של מכשיר טכנולוגי המאפשר העתקה, לצד שימושים אחרים חוקיים, ועלול להימצא אחראי תורם להפרת זכויות היוצרים בידי לקוחותיו אף אם אין ביניהם מערכת יחסים מתמשכת של פיקוח כלשהו.[18]

הטכנולוגיה שנדונה באותה פרשה הייתה מכשיר הווידיאו של חברת סוני, ה־Betamax. בשנות השמונים היה ה־Betamax למכשיר החדשני הראשון שאפשר למשתמשיו להחזיק בבתיהם ספריות וידיאו אישיות שלא היו מביישות ארכיון טלוויזיה עשיר. בעלי זכויות היוצרים של כמה תוכניות טלוויזיה ששודרו באותה העת בערוצי השידור הציבוריים עמדו לפני דילמה קשה: זכויות היוצרים שלהם הופרו בקנה מידה נרחב אולם בידי מפירים בודדים רבים, וניהול תביעה נגד כל אחד ואחת מהם לא היה מעשי או משתלם כלכלית. בעלי זכויות היוצרים החליטו אפוא לתבוע את חברת סוני.[19]

בית המשפט העליון בארצות הברית התבסס בפסק דינו על דוקטרינת ההפרה התורמת מדיני הפטנטים,[20] שלפיה כאשר אפשר לעשות בטכנולוגיה שימוש מסחרי חוקי משמעותי (commercially significant non-infringing use), הוכחת מודעותו בכוח של היצרן לאפשרות השימוש הבלתי חוקי בטכנולוגיה שייצר אינה מספקת לשם הטלת אחריות תורמת. באמצעות יצירת חריג השימוש החוקי המשמעותי ביקש בית המשפט לאזן בין הגנה על זכות היוצרים והאינטרס של יוצרים לשלוט בשימוש ביצירותיהם, לבין האינטרס

17 Moye, **לעיל** ה"ש 11, בעמ' 653; Jane C. Ginsburg, *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 Ariz. L. Rev. 577, 580 (2008)

18 David G. Post, Annemarie Bridy & Timothy Sandefur, *Nice Questions Unanswered: Grokster, Sony's Staple Article of Commerce Doctrine, and the Deferred Verdict on Internet File Sharing*, 2004 Cato Sup. Ct. Rev. 234, 240–241

19 פרשת **סוני**, **לעיל** ה"ש 10, בעמ' 442.

20 Patent Act of 1952, 35 U.S.C. §271; Charles W. Adams, *A Brief History of Indirect Liability for Patent Infringement*, 22(3) Santa Clara High Tech. L.J. 369 (2006)

של החברה לעודד חדשנות וזרימה חופשית של רעיונות, מידע ומסחר. יישום דוקטרינת ההפרה התורמת והחריג לה בנסיבות המקרה הוביל את בית המשפט למסקנה שמכשיר הווידיאו של סוני, שתכליתו המרכזית היא לאפשר שימוש הוגן משמעותי בדמות הקלטה וצפייה מאוחרת (time shifting), אינו יכול להוות בסיס להטלת אחריות תורמת על סוני בגין השימושים המפירים הנעשים באמצעותו.[21] פסק הדין בפרשה אותת לציבור שבית המשפט מבקש לעודד חדשנות כל עוד מטרתה היחידה והבלעדית של הטכנולוגיה החדשנית היא שימוש לגיטימי ולא הפרת זכויות יוצרים.[22]

עם זאת, בית המשפט לא הגדיר קנה מידה ברור ל"שימוש חוקי משמעותי" או לנסיבות שבהן יהיה אפשר להישען על מודעותו בכוח של היצרן לשימושים מפירים כבסיס להטלת אחריות תורמת עליו.[23] כך נוצרה עמימות באשר לתנאיה של דוקטרינת ההפרה התורמת.[24]

התפתחות האינטרנט וטכנולוגיות שאפשרו הצגת תמונות וקישוריות לחומרים המוגנים בזכות יוצרים הובילו לחקיקת ה־Digital Millennium Copyright Act

21 פרשת **סוני**, **לעיל** ה"ש 10, בעמ' 423, 428, 441.

22 Moye, **לעיל** ה"ש 11, בעמ' 659; Diane Leenheer Zimmerman, *Daddy, Are We There Yet – Lost in Grokster-Land*, 9 N.Y.U. J. Legis. & Pub. Pol'y 75, 78 (2005). נציין שבדין הישראלי, החריג שנקבע בפרשת **סוני** (**לעיל** ה"ש 10) אינו מקובל, לכאורה, כפי שמעידה אמירתו של השופט ריבלין בפרשת **שוקן**, שלפיה אפשר להטיל אחריות תורמת גם כאשר ההפרה הישירה חוסה תחת חריג השימוש ההוגן. ראו ע"א 5977/07 **האוניברסיטה העברית בירושלים נ' בית שוקן להוצאת ספרים בע"מ** (נבו 15.11.2010), פס' 24 לפסק דינו של השופט ריבלין (להלן: פרשת **שוקן**). לביקורת על עמדה זו ראו אורית פישמן אפורי "אחריות תורמת להפרת זכויות יוצרים בישראל: מהפורום בהר הצופים לפורום המקוון" **הפרקליט** נב 3, 47–48 (התשע"ג).

23 Elizabeth Miles, *In re Aimster & MGM, Inc. v. Grokster, Ltd.: Peer-to-Peer and the Sony Doctrine*, 19 Berkeley Tech. L.J. 21, 22 (2004); Craig A. Grossman, *From Sony to Grokster, The Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War between Content and Destructive Technologies*, 53 Buff. L. Rev. 141, 164 (2005); Moye, **לעיל** ה"ש 11, בעמ' 657–656.

24 Post, Bridy & Sandefur, **לעיל** ה"ש 18, בעמ' 244–246.

(DMCA) בשנת 1998.[25] ה־DMCA כולל, בין השאר, הוראות המכונות "נמלי ביטחון" (safe harbors), הקובעות באילו תנאים יהיו ספקי שירותי אינטרנט הנמנים עם אחת מארבע קטגוריות המוגדרות בחוק[26] פטורים מאחריות ישירה, עקיפה או תורמת להפרת זכויות יוצרים המבוצעת באמצעות השירותים שהם מספקים.[27] כדי ליהנות מהחסינות שמספקים נמלי הביטחון, ספקי שירותי האינטרנט למיניהם נדרשים, בין השאר, להטמיע מנגנון "הודעה והסרה", להוכיח שהם אינם מודעים בפועל לשימוש המפר, אינם שולטים עליו ואינם מפיקים רווח ישיר ממנו, וכן שהם מסירים כל שימוש מפר מייד עם היוודע להם דבר קיומו.[28] בתי המשפט פירשו את דרישת המודעות בפועל כמתקיימת רק בעקבות קבלת הודעה מבעל זכות היוצרים על השימוש המפר במסגרת מנגנון הודעה והסרה. בספרות הוצע להכיר במודעות בכוח של הספק כאשר אפשר להוכיח שפעל באופן לא אחראי או ציני, אולם עמדה זו לא התקבלה בפסיקה. נפסק שאין די בהוכחת מודעות כללית לכך שהשירות עשוי לשמש גם להפרת זכויות יוצרים או שיש בשרתיו של הספק גם תכנים המפירים זכויות יוצרים. עוד נקבע שעצימת עיניים יכולה להקים מודעות בכוח מצד ספק השירותים רק אם אפשר להוכיח שהיא הייתה מכוונת, ולשם כך נדרש כי יחזיק במידע על הפרה ספציפית שממנה הוא מעלים עין.[29] לפיכך ניתן לומר שדרישת המודעות לפי ה־DMCA מצומצמת למודעות בפועל בלבד.[30]

עם העלייה בהיקף השימוש באינטרנט, בעלי זכויות היוצרים התקשו יותר ויותר לנטר תכנים המפירים את זכויותיהם ולהודיע על הימצאם לכל אחד

25 Digital Millenium Copyright Act (DMCA), Pub. L. N. 105-304, 112 Stat. 2860 (1998)

26 **שם**, בסעיף 512.

27 **שם**.

28 **שם**, בסעיף 512(i)(1).

29 UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1108 (C.D. Cal 2009); Sirichit, **לעיל** ה"ש 14, בעמ' 186-187.

30 **שם**, בעמ' 125-144.

מספקי השירותים האינטרנטיים, ופנו לערכאות המשפטיות.[31] כ־17 שנים אחרי פסיקת ביהמ"ש העליון בפרשת **סוני** דן בית המשפט לערעורים במחוז התשיעי בארצות הברית בתוכנת שיתוף הקבצים נאפסטר. נאספטר אפשרה שיתוף מבוזר של קבצים, בין השאר קובצי שירים מוגנים בזכויות יוצרים, בין משתמשי הקצה שלה. נאפסטר עקבה אחר כלל משתמשיה, ידעה מי מהם מחובר לפלטפורמה בכל רגע נתון ומהם קובצי המוזיקה הזמינים במחשבו האישי, וכן תחזקה אינדקס של קובצי השירים הזמינים לשיתוף ומיקומם. האינדקס שיצרה שימש כמנוע חיפוש נוח למציאת קובצי מוזיקה ולהורדתם המהירה ממחשבי משתמשי נאפסטר האחרים. נפסק שאפשר לעשות שימוש חוקי משמעותי בטכנולוגיה של נאפסטר, אף שהחברה לא הוכיחה שבאמת נעשה שימוש כאמור. אולם בית המשפט לערעורים במחוז התשיעי מצא שנאפסטר הייתה מודעת לשימושים המפירים ויכלה לפקח עליהם באמצעות האינדקס שניהלה. נפסק שכאשר גורם הביניים מחזיק במודעות בפועל להפרה ספציפית של זכות היוצרים, העובדה שהטכנולוגיה היא דו־שימושית ועשויים להיעשות באמצעותה שימושים חוקיים משמעותיים אינה רלוונטית. לפיכך נפסק כי נאפסטר אחראית תורמת להפרת זכויות היוצרים בידי משתמשיה.[32]

הפרשה הבאה שהגיעה לפתחו של בית המשפט לערעורים במחוז התשיעי עסקה בפלטפורמה נוספת לשיתוף קבצים – גרוקסטר. גרוקסטר החזיקה בשרת מרכזי ששמר את פרטי משתמשי הקצה וסייע במציאת משתמשים אחרים, אך לא אספה כל מידע בנוגע לתעבורת קבצים. מרגע הורדתה למחשב של משתמש הקצה, למפתחיה של גרוקסטר לא הייתה כל שליטה על הקונפיגורציה שלה או על אופן השימוש בה. במובן זה גרוקסטר דומה למכשיר

31 Michael Harrigan, *Beyond a Reasonable Doubt: How Blockchain Technology Can Shift the DMCA's Burden of Notification away from Copyright Owners*, 39 Ent. & Sports Law. 145, 146–147 (2023)

32 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020–1022 (9th Cir. 2001) (להלן: פרשת **נאפסטר**); Bryan H. Choi, *The Grokster Dead-End*, 19(2) Harv. J.L. & Tech 393, 395 (2006); Grossman, **לעיל** ה"ש 23, בעמ' 200–198; Ginsburg, **לעיל** ה"ש 17, בעמ' 582.

הווידיאו Betamax של סוני, שעם רכישתו על ידי משתמש הקצה איבדה סוני כל יכולת לשלוט על השימושים הנעשים בו.[33]

בית המשפט לערעורים במחוז התשיעי פסק שאם מוכח שימוש חוקי משמעותי, אזי נדרשת מודעות ממשית להפרה ספציפית בשלב שבו גורם הביניים יכול להפסיק, למנוע או למזער את ההפרה הישירה. עוד נפסק שגם שיעור נמוך של שימושים חוקיים (בפסק הדין דובר על 10%) מספיק להכרה בקיומו של שימוש חוקי משמעותי. לפיכך נפסק שמפתחיה של גרוקסטר אינם נושאים באחריות תורמת להפרות הנעשות באמצעות התוכנה.[34] בית המשפט לא ייחס כל חשיבות לכך שמפתחיה של גרוקסטר בחרו במכוון לעצבה באופן המונע מודעות מצידם, כדי לצלוח את הפרשנות של בית המשפט לדוקטרינת ההפרה התורמת בפרשת **נאפסטר**.[35]

באותן שנים שבהן פרשות **נאפסטר** ו**גרוקסטר** נדונו בבית המשפט לערעורים במחוז התשיעי נדונה פרשת **איימסטר**, גם היא פלטפורמת שיתוף קבצים, בבית המשפט לערעורים במחוז השביעי. איימסטר הצפינה את הקבצים המועברים על גבי הפלטפורמה שלה, כך שלא יהיה אפשר לדעת אילו קבצים מועברים בין משתמשיה. על אף הצפנת הקבצים, בית המשפט לערעורים במחוז השביעי פסק כי התקיים יסוד המודעות החיוני להוכחת אחריות להפרה תורמת, משום שאיימסטר נקטה "עצימת עיניים" כלפי הפרות אפשריות (willful blindness).[36] לפי פסק הדין, הכוונה הרעה של איימסטר מלכתחילה ליצור מערכת שהארכיטקטורה שלה אינה מאפשרת לחברה המפתחת ומפעילה אותה לקבל מידע בנוגע לשימושים הנעשים בה מהווה עצימת עיניים מכוונת,

33 Miles, **לעיל** ה"ש 23, בעמ' 42; Choi, **לעיל** ה"ש 32, בעמ' 395–396.

34 MGM Studios Inc. v. Grokster, Ltd., 380 F.3d 1154, 1160–1161 (9th Cir. 2004)

35 Moye, **לעיל** ה"ש 11, בעמ' 666; Miles, **לעיל** ה"ש 23, בעמ' 27; Choi, **לעיל** ה"ש 32, בעמ' 395.

36 In re Aimster Copyright Litigation, 334 F.3d 643, 655 (7th Cir. 2003), *cert. denied*, 540 U.S. 1107 (2004) (להלן: פרשת **איימסטר**).

ומלמדת על מודעות גורם הביניים להפרה.[37] בכך חרג בית המשפט במחוז השביעי מהפרשנות המקובלת עד אז לדוקטרינת ההפרה התורמת, שלפיה נדרשת מודעות בפועל להפרה הישירה לשם הטלת אחריות תורמת.[38]

גם באשר לחריג לאחריות להפרה תורמת שנקבע בפרשת **סוני** בחר בית המשפט במחוז השביעי בפרשנות שונה מזו שנתן בית המשפט במחוז התשיעי בפרשות **נאפסטר** ו**גרוקסטר**. נפסק שאין די בהוכחת היכולת של המוצר או הטכנולוגיה לאפשר שימוש חוקי משמעותי, אלא יש להוכיח שהמוצר או הטכנולוגיה אכן שימשו בפועל לשימושים חוקיים משמעותיים ושאי־אפשר באמצעים סבירים כלכלית למנוע או להפחית במידה ניכרת את השימושים המפירים. בהתאם לפרשנות זו נפסק שאיימסטר לא הצליחה להוכיח שימוש חוקי כלשהו בפלטפורמה שלה.[39]

ההתדיינות המשפטית בנוגע לאחריות התורמת של גרוקסטר להפרת זכויות היוצרים הגיעה לפתחו של בית המשפט העליון האמריקני בשנת 2004, והוא התבקש לחוות דעתו באשר לתנאים ולנסיבות שבמסגרתם מפיץ של מוצר דו־שימושי ייחשב אחראי להפרת זכות יוצרים המבוצעת על ידי צד שלישי העושה שימוש במוצר. משהסכים לדון בפרשה ציפו רבים שבית המשפט העליון יישב אחת ולתמיד את המחלוקת הפרשנית בין הערכאות הנמוכות באשר לסטנדרט המודעות הנדרש להטלת אחריות תורמת, וכן באשר לרף השימוש החוקי המשמעותי הפוטר מאחריות תורמת לפי החריג שנקבע בפרשת **סוני**. לצד ציפייה זו גבר החשש שבית המשפט יצמצם את החריג אשר נקבע בפרשת **סוני** וכך תיגרם פגיעה של ממש בחדשנות.[40]

אולם בפסיקתו לא הכריע בית המשפט העליון בין הפרשנויות השונות שהוצעו בבתי המשפט במחוז השביעי ובמחוז התשיעי, והמחלוקת באשר למהותה

37 Sirichit, **לעיל** ה"ש 14, בעמ' 107–108.

38 ראו Powell, **לעיל** ה"ש 12, בעמ' 194–195.

39 פרשת **איימסטר**, **לעיל** ה"ש 36, בעמ' 648.

40 Moye, **לעיל** ה"ש 11, בעמ' 673; Zimmerman, **לעיל** ה"ש 22, בעמ' 84; Alfred C. Yen, *Third Party Copyright Liability after Grokster*, 91 Minn L. Rev. 184, 188 (2005)

של דרישת המודעות ולרוח הוכחת השימוש החוקי המשמעותי הנדרש נותרה בעינה.

השופט סוטֶר, אשר כתב את פסק הדין בשם כלל שופטי ההרכב, מתח ביקורת על הפרשנות שנתן בית המשפט במחוז התשיעי בפרשת **גרוקסטר** לדרישת המודעות בפועל, וקבע כי הדרישה להוכיח מודעות בפועל להפרה ספציפית כתנאי להחלת אחריות תורמת היא שגויה. עם זאת, השופט סוטר נמנע מלקבוע אמת מידה כמותית ל"שימוש חוקי משמעותי" הפוטר מאחריות תורמת לפי החריג שנקבע בפרשת **סוני**, וכתב כי סוגיה זו תזכה להתייחסותו בעתיד אם זו תידרש. השופטת גינסבורג, שלעמדתה הצטרף גם השופט קנדי, הסכימה עם תוצאת פסק הדין, אך התייחסה באופן ספציפי לשאלת היקף השימוש החוקי המשמעותי הנדרש כדי ליהנות מהחריג שאומץ בפרשת **סוני**. לעמדתה יש להעניק פרשנות מחמירה יותר מזו שהייתה מקובלת עד אז לחריג פרשת **סוני**, ולחייב הוכחה ממשית לקיומו של שימוש חוקי משמעותי במוצר. לשיטתה, בפרשת **גרוקסטר** לא הוכח באופן סביר שימוש חוקי משמעותי. ובכל מקרה, אף אם תוכנות שיתוף הקבצים שימשו גם למטרות חוקיות, מספר השימושים החוקיים מתגמד לעומת הכמות העצומה של ההפרות שתוכנות אלה אפשרו. השופט בְּרֶייֶר, שלעמדתו הצטרפו השופטים אוקונור וסטיבנס, הסכים גם הוא עם תוצאת פסק הדין, אולם חלק על ניסיונה של גינסבורג להציע פרשנות מחמירה יותר לחריג פרשת **סוני**. לשיטתו של ברייר, גם בפרשת **סוני** עצמה היקף השימושים החוקיים, אשר בית המשפט העליון דאז הכיר בהם כמקיימים את חריג השימוש החוקי המשמעותי, היה נמוך ועמד על 10% לערך. משום כך, לדעתו גרוקסטר עמדה בדרישת קיומו של שימוש חוקי משמעותי, ואין מקום להחמרת הפרשנות המוענקת לחריג זה שכן הוא עדיין משקף את האיזון הנכון והראוי בין האינטרס של בעל זכות היוצרים בהגנה על זכותו לבין אינטרס הציבור בקידום חדשנות.[41]

במקום להכריע בשאלות הקשורות לתנאים להחלתה של דוקטרינת ההפרה התורמת במקרה של יצרן טכנולוגיה דו־שימושית, בחר בית המשפט לפתח

41 MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 936–937 (2005) (להלן: פסק דין **גרוקסטר** בעליון); Yen, **לעיל** ה"ש 40, בעמ' 188, 223.

בסיס חלופי להטלת אחריות תורמת להפרת זכות יוצרים – "תיאוריית השידול". לפי תיאוריית השידול, כאשר קיימות ראיות ברורות לכך שהמניע העיקרי ליצירת הטכנולוגיה והפצתה הוא עידוד השימוש בה לשם הפרת זכות יוצרים, יוצר הטכנולוגיה חב באחריות תורמת להפרת זכות היוצרים בידי המשתמשים בה. אם כן, תיאוריית השידול מחייבת את בתי המשפט לצלול לבחינה סובייקטיבית של השאלה האם מפתחי הטכנולוגיה שידלו את המשתמשים להפר זכויות יוצרים. לפי פסק הדין של בית המשפט העליון בפרשת **גרוקסטר**, אפשר ללמוד על הכוונה מהארכיטקטורה של הטכנולוגיה, דהיינו מהתקנה או אי־התקנה של מסננים לסינון תוכן בלתי חוקי, או מהמודל העסקי של החברה שמפיצה את הטכנולוגיה. הבחינה, בסופו של דבר, תהיה כנראה כמותית: אם יוצר טכנולוגיה לא התקין מסננים לסינון תוכן בלתי חוקי, אם הטכנולוגיה שלו מאפשרת שימושים מפירים בהיקפים גבוהים ואם לפי המודל העסקי שלו רווחיו גדלים ככל שגדל היקף הפעילות המפירה, אזי סביר שבית המשפט ימצא בכך שידול והוא יימצא אחראי להפרה תורמת לפי תיאוריית השידול. אם יוצר הטכנולוגיה לא התקין מסננים אך המודל העסקי שלו אינו נשען על פעילות מפירה לשם הגדלת הרווחים, סביר שבית המשפט לא יטיל עליו אחריות תורמת להפרת זכות יוצרים, גם אם בפועל הטכנולוגיה שלו מאפשרת גם שימושים לא חוקיים בהיקף ניכר. אם כן, תיאוריית השידול מאפשרת למפתחי טכנולוגיה להמשיך להישען על החריג שנקבע בפרשת **סוני** כדי לפתח טכנולוגיות חדשניות, ובית המשפט שומר בכך על מסגרת המעודדת חדשנות.[42]

1.2. האיחוד האירופי

דוקטרינת ההפרה התורמת באיחוד האירופי אינה יציר הפסיקה, אך היא גם אינה קבועה בדבר חקיקה יחיד וסדור. מדובר בדוקטרינה העשויה טלאים

42 Pamela Samuelson, *Three Reactions to MGM v. Grokster*, 13 Mich. Telecomm. & Tech. L. Rev. 177, 186 (2006); Ginsburg, **לעיל** ה"ש 17, בעמ' 586–590.

טלאים מדברי חקיקה שונים, שכל אחד מהם עוסק בהיבט אחר של אחריות תורמת להפרת זכויות קניין רוחני.[43] המקור הראשון הוא דירקטיבת האכיפה, אשר קובעת כי על המדינות החברות באיחוד האירופי לקבוע בחקיקה אמצעים יעילים לאכיפת זכויות קניין רוחני, ובהם סעדים, לרבות צווי ביניים, נגד מתווכים שהשירות שלהם משמש צדדים שלישיים להפרה של זכויות קניין רוחני, למעט זכויות יוצרים.[44] דירקטיבת חברת המידע מספקת מקור נוסף לדוקטרינת ההפרה התורמת באמצעות הוראה המתייחסת אל מתווכים כאל מונע הנזק הזול, ועל כן מחייבת את המדינות החברות באיחוד האירופי לקבוע בחקיקה סעדים נגד מתווכים שהשירות שלהם משמש צדדים שלישיים להפרת זכויות יוצרים.[45] דומה שזהו סטנדרט המינימום לאחריות תורמת להפרת זכויות קניין רוחני. עם זאת, מתווכים המספקים תשתית פיזית להעמדה לרשות הציבור של יצירות מוגנות מוחרגים מגדרי האחריות התורמת.[46] מקור חקיקתי נוסף המלמד על היקפה של דוקטרינת ההפרה התורמת באיחוד האירופי הוא דירקטיבת ה־E-Commerce, אשר קובעת "נמלי ביטחון" המגבילים את יכולתן של המדינות החברות להטיל אחריות תורמת על ספקי שירותי אינטרנט. לפי הוראות אלה, ספק שירותי אחסון (host provider) לא יישא באחריות תורמת להפרה שמבצע משתמש הקצה באמצעות שירות האחסון בהתקיים שני תנאים: (1) הספק לא היה מודע בפועל להפרה, או לעובדות או לנסיבות שמהן עולה ההפרה בבירור; (2) עם היוודע דבר ההפרה או העובדות או הנסיבות

43 Christina Angelopoulos, *Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe*, Inter'l Rev. Intell. Prop. & Competition L. 253 (2013)

44 Directive 2004/48, of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, pmbl. 3, 9–10, arts. 9, 11, 2004 O.J. (L 157) 45 (הדירקטיבה להלן: דירקטיבת האכיפה).

45 Directive 2001/29, 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, pmbl. 59., art. 8(3), 2001 O.J. (L 167) 10 (הדירקטיבה להלן: דירקטיבת חברת המידע).

46 World Intellectual Property Organization Copyright Treaty, art. 8, Dec. 20, 1996, 36 I.L.M. 65

שמהן היא עולה הסיר הספק מייד את התוכן המפר או מנע גישה אליו.[47] עוד אוסרת דירקטיבת ה־E-Commerce על המדינות החברות באיחוד האירופי להטיל על ספק שירות אינטרנט חובה לנטר את התוכן המאוחסן או המועבר על גבי התשתית שהוא מספק.[48] עם זאת, נמלי הביטחון מוגבלים רק למקרים שבהם פעילות ספק השירות היא טכנית, אוטומטית ופסיבית מטבעה. ספק אקטיבי שהמודל העסקי שלו מבוסס על האינטרסים שלו באחסון תוכן מפר, הנותן העדפה לאחסון או העברה של תוכן מפר, או שאפילו מפרסם שימוש לא חוקי שכזה בפלטפורמה שלו, אינו זכאי ליהנות מחריג האחריות שכן הוא אינו ניטרלי באשר לתוכן המועבר או המאוחסן.[49] עמדה זו קיבלה חיזוק גם בפרשנות של בית הדין לצדק של האיחוד האירופי (CJEU) לסעיף 14 לדירקטיבת ה־E-commerce.[50] כמו כן, דירקטיבת ה־E-commerce מאפשרת למדינות החברות להגביל את יישומם של נמלי הביטחון במקרה של סעד של צו מניעה – כלומר אפשר לקבוע בחוק מדינתי כי על ספק שירות אינטרנט לסיים או למנוע הפרה מרגע שהוא מקבל עליה הודעה.[51]

ביוני 2021 נכנסה לתוקף דירקטיבת ה־DSM, שחוללה שינוי מסוים בדוקטרינת ההפרה התורמת באיחוד האירופי משום שהיא מגדירה מחדש את היקף האחריות הישירה של ספק תוכן שיתופי באינטרנט (online content-sharing

47 Directive 2000/31, 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"), art. 14, 2000 O.J. (L 178) 1 (הדירקטיבה להלן: דירקטיבת ה־E-commerce).

48 **שם**, בסעיף 15.

49 **שם**, בסעיף הקדמה 42 ובסעיף 15.

50 Opinion of Advocate General Poiares Maduro, Joined Cases C-236/08, C-237/08 & C-238/08, Google France SARL v. Louis Vuitton Malletier SA, 2010 E.C.R. I-2417, ¶¶ 137 et seq. (Sept. 22, 2009)

51 סעיף הקדמה 45 וסעיפים 12(3), 13(3) ו־14(3) לדירקטיבת ה־E-commerce, **לעיל** ה"ש 47.

service providers).[52] זהו ספק שירותי מידע חברתיים שמטרתו העיקרית, או אחת ממטרותיו העיקריות, היא לאחסן ולהעניק לציבור גישה לכמות גדולה של תכנים המוגנים בזכות יוצרים,[53] המועלים בידי משתמשיו ומאורגנים ומקודמים על ידי הספק עצמו במטרה להפיק רווח מהנגשתם לציבור המשתמשים. ההגדרה של ספק תוכן שיתופי באינטרנט אינה כוללת ספקים אשר מטרתם העיקרית אינה זו – למשל ספקים של פלטפורמות המאחסנות ומעניקות גישה לחומרים חינוכיים ומדעיים שלא למטרות רווח; ספקים של שירותי תקשורת מסורתיים, כגון חברות המספקות שירותי חיבור לרשת האינטרנט; ספקי שירותי ענן, כגון DropBox או Google Drive; ספקי פלטפורמות שוק מקוון שמטרתן העיקרית היא לאפשר מסחר מקוון בין המשתמשים ולא מתן גישה ליצירות המוגנות בזכות יוצרים; ספקי פלטפורמה לפיתוח תוכנות קוד פתוח, כמו למשל GitHub; וספקי פלטפורמות לאנציקלופדיה מקוונת שלא למטרות רווח.[54]

לפי דירקטיבת ה־DSM, הנגשה לציבור של תוכן המוגן בזכויות יוצרים על גבי פלטפורמה של ספק תוכן שיתופי באינטרנט מהווה העמדה לרשות הציבור על ידי הספק, ומחייבת אותו לקבל רישיון לשם כך מבעל זכות היוצרים.[55] בהיעדר רישיון מבעל זכות היוצרים יהא ספק תוכן שיתופי אחראי להפרת זכות היוצרים, אלא אם מתקיימים התנאים שלהלן:

(**1**) הספק נקט פעולות סבירות לקבלת רישיון מבעל זכות היוצרים;[56]

52 ראו Directive 2019/790, of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directive 96/9/EC and 2001/29/EC, art. 17, 2019 O.J. (L 130) 92 (הדירקטיבה להלן: דירקטיבת ה־DSM).

53 השאלה אם זהו ספק המעניק גישה לכמות גדולה של תכנים תיבחן באופן כמותי בכל מקרה ומקרה, תוך הערכה של כמות התוכן המוגן בזכויות יוצרים שהספק מאחסן ומנגיש ושל מספר המשתמשים בשירות שהוא מספק. ראו **שם**, בסעיף הקדמה 63.

54 **שם**, בסעיפי הקדמה 61–62.

55 **שם**, בסעיף הקדמה 64 ובסעיף 17(1).

56 **שם**, בסעיף 17(4)(a).

(**2**) הספק נקט מאמצים סבירים, בהתאם לסטנדרטים גבוהים של חריצות מקצועית המקובלים בתעשייה, כדי להבטיח את אי־זמינותן של יצירות שבעל זכויות היוצרים בהן הודיע לו על הימצאותן בשירות ללא אישורו;[57]

(**3**) ובכל מקרה, הספק פעל מייד עם קבלת הודעה מפורטת מבעל זכות היוצרים להסרתם של התכנים המפירים או לחסימת הגישה אליהם, וכן נקט מאמצים סבירים למניעת העלאה חוזרת של התכנים המפירים לשירות שלו.[58]

עמידתו של הספק בכל אחד מתנאים אלו תיבחן בהתאם לעקרון המידתיות ולאור שיקולים נוספים המנויים בדירקטיבת ה־DSM, כגון סוג השירות המסופק, קהל היעד שלו והיקפו, סוג היצירות המועלות לשירות על ידי משתמשיו, והזמינות והעלות של אמצעים יעילים שיאפשרו לספק התוכן השיתופי לעמוד בדרישות אלו.[59]

בחקיקת דירקטיבת ה־DSM ביקשה נציבות האיחוד האירופי להחמיר את כללי האחריות החלים על ספקים של תוכן שיתופי באינטרנט, כדי לתמרץ אותם לפנות לקבלת רישיון מבעל זכות היוצרים ולהטמיע בשירות שהם מספקים כלים טכנולוגיים לזיהוי אוטומטי של תוכן, וכך להקטין את היקף התוכן המפר זכויות יוצרים שמשתמשי הקצה מעלים לרשת האינטרנט.[60] על משטר האחריות שנקבע בדירקטיבה זאת נמתחה ביקורת רבה בטענה שהוא לא ברור, מעורפל ועשוי להתפרש כמטיל חובת ניטור כוללני ומתמיד של התכנים על ידי ספק השירות באופן הפוגע בזכויות יסוד של המשתמשים, כגון הזכות לחופש ביטוי והזכות לפרטיות.[61]

למרות הביקורת, באפריל 2022 דחה ה־CJEU את טענת פולין שלפיה יש לבטל את משטר האחריות הקבוע בדירקטיבת ה־DSM בנימוק שהוא מטיל חובת

57 **שם**, בסעיף 17(4)(b).

58 **שם**, בסעיף 17(4)(c).

59 **שם**, בסעיף 17(5).

60 Pamela Samuelson, *Pushing Back on Stricter Copyright ISP Liability Rules*, 27 Mich. Tech. L. Rev. 299, 302–303 (2021)

61 **שם**, בעמ' 313–330.

ניטור תוכן ולכן פוגע בזכות לחופש ביטוי. אומנם ה־CJEU הכיר בכך שהחובה לנקוט פעולות סבירות כדי להבטיח שיצירות המוגנות בזכות יוצרים יהיו זמינות לציבור רק באישור בעלי הזכויות מחייבת למעשה ספקי תוכן שיתופי באינטרנט לנטר תוכן לפני שהמשתמשים מעלים אותו לשירות שלהם, וכך מגבילה את זכות היסוד של משתמשי הפלטפורמה לחופש ביטוי. עם זאת, הזכות לחופש ביטוי אינה זכות מוחלטת אלא יש לבחון את הפגיעה בה בהתאם לעקרון המידתיות. כן הבהיר ה־CJEU שכל פתרון טכנולוגי ליישום החובה לנקוט אמצעים סבירים חייב להבחין בבירור בין תוכן חוקי לתוכן שאינו חוקי. נוסף על כך, ה־CJEU מצא שהדירקטיבה כוללת אמצעי הגנה מספקים על הזכות לחופש ביטוי, וכן שפגיעתה בזכות לחופש ביטוי היא נחוצה ומידתית לשם הגנה על זכויות קניין רוחני.[62] כך, למשל, לפי דירקטיבת ה־DSM עמידתו של הספק בדרישות לפטור מאחריות תיבחן בהתאם לעקרון המידתיות ותוך התחשבות בשיקולים נוספים, כגון סוג השירות, קהל היעד שלו והיקפו.[63] כן מונחות המדינות החברות להתייחס באופן שונה לספק תוכן שיתופי אשר פועל באיחוד האירופי פחות משלוש שנים ושהרווח השנתי שלו קטן מ־10 מיליון אירו – ספק כזה יחויב אך ורק בנקיטת פעולות סבירות לקבלת רישיון מבעלי זכויות היוצרים כדי לזכות בפטור מאחריות להפרת זכויות יוצרים בידי משתמשיו.[64] זאת ועוד, דירקטיבת ה־DSM מבהירה שעל המדינות החברות להבטיח שכל שיתוף פעולה בין בעלי זכויות יוצרים לספקי תוכן שיתופי לא יפגע בזמינותן של יצירות המוגנות בזכויות יוצרים, אם השימוש בהן נעשה למטרות ציטוט, ביקורת, סקירה, קריקטורה או פרודיה.[65] עוד נדרשים ספקי תוכן שיתופי להחזיק במנגנון לבירור תלונות ויישוב סכסוכים בכל הקשור להסרת תוכני משתמשים על ידם, ולהבטיח שכל החלטה בדבר הסרת תוכן או חסימת הגישה אליו מאושרת בידי גורם אנושי. על המדינות החברות להבטיח שמשתמשים הסבורים כי זכויותיהם נפגעו עקב הסרת תכנים שהעלו או

62 Case C-401/19, Republic of Poland v. European Parliament & Council of the European Union, ECLI:EU:C:2022:297 (Apr. 26, 2022)

63 דירקטיבת ה־DSM, **לעיל** ה"ש 52, בסעיף 17(5)(a).

64 **שם**, בסעיף 17(6).

65 **שם**, בסעיף 17(7).

חסימת הגישה אליהם יקבלו את יומם בבית המשפט.[66] לצד אלה, הדירקטיבה קובעת גם כי על נציבות האיחוד לקיים מפגשים בהשתתפות ספקי תוכן שיתופי ובעלי זכויות יוצרים כדי לגבש קווים מנחים באשר לסטנדרט הפעולות הסבירות שעל ספקי תוכן שיתופי לנקוט לשם קבלת פטור מאחריות להפרת זכויות יוצרים.[67]

מאחר שמשטר האחריות והחריג לאחריות הקבוע בדירקטיבת ה־DSM מוגבלים רק לספקי תוכן שיתופי באינטרנט, על שאר ספקי השירות שאינם נכללים בהגדרת ספקי תוכן שיתופי חל משטר האחריות המורכב מהוראות דירקטיבת חברת המידע, דירקטיבת האכיפה ונמלי הביטחון שבדירקטיבת ה־E-commerce. היקפה של אחריות זו והחריגים לה נידונו ביולי 2021 בפסק הדין של ה־CJEU בשתי פרשות שהדיון בהן אוחד: פרשות *YouTube* ו־*Cyando*. בשתי הפרשות תבעו בעלי זכויות יוצרים את הבעלים והמפעילים של פלטפורמות שיתוף קבצים, YouTube של גוגל ו־Uploaded של חברת Cyando, בגין הפרת זכויות יוצרים שביצעו לטענתם משתמשי הקצה של הפלטפורמות. בעניין *Youtube* טענו בעלי זכויות היוצרים כי יצירות מוגנות הועלו לשירות והועמדו בו לרשות הציבור ללא אישורם. בעניין *Cyando* נטען כי שירות אחסון הקבצים שלה, Uploaded, אפשר הפרת זכויות יוצרים בידי משתמשי קצה אשר אחסנו קבצים המוגנים בזכויות יוצרים על השירות ושיתפו באתרי אינטרנט שונים (בלוגים ופורומים) קישוריות לקבצים אלו, ללא אישור מבעלי זכויות היוצרים. בעלי זכויות היוצרים פנו לבתי המשפט האזוריים במחוז המבורג ובמחוז מינכן לאחר שהיצירות המוגנות שבבעלותם הוסרו מהפלטפורמות בעקבות פנייתם אך שבו והועלו בידי משתמשי הקצה. לפיכך בעלי זכויות היוצרים ביקשו מבית המשפט להוציא צו האוסר על החברה להעמיד לרשות ציבור את היצירות המוגנות, להורות לכל אחת מהחברות להעביר לידיהם מידע על ההפרות וכן על רווחים שהפיקה בגינן, וכן לשלם להם פיצוי כספי בגין הנזקים שנגרמו להם עקב הפרת זכויות היוצרים. בעלי זכויות היוצרים ערערו על החלטת בית המשפט המחוזי לערכאת בית המשפט המחוזי הגבוה, ובהמשך ערערו

66 **שם**, בסעיף 17(9).

67 **שם**, בסעיף 17(10).

התובעים והנתבעים לבית המשפט הפדרלי לצדק בגרמניה. זה האחרון השהה את הדיון בערעור, ופנה בבקשה ל־CJEU לפרש את היקף האחריות התורמת של ספק שירות בהתאם להוראות דירקטיבת ה־E-commerce, דירקטיבת חברת המידע ודירקטיבת האכיפה.[68]

ה־CJEU בחן את אופן פעולתן של הפלטפורמות YouTube ו־Uploaded, והכיר בכך שהן יכולות לשמש לשימושים חוקיים אך גם לשימושים בלתי חוקיים: קובצי וידיאו המשותפים באמצעות YouTube עשויים לכלול יצירות המוגנות בזכויות יוצרים, והיכולת לאחסן ולשתף קבצים גדולים באמצעות פלטפורמת Uploaded הופכת אותה לכלי פרקטי לשיתוף קבצים המוגנים בזכויות יוצרים.[69]

לפיכך נפסק שמשתמשי הפלטפורמות מפירים את זכות ההעמדה לציבור, שהיא אחת מהזכויות באגד זכויות היוצרים ביצירות המוגנות, כאשר הם מעלים אל הפלטפורמה תכנים המוגנים בזכויות יוצרים ללא רשות בעלי הזכויות, ובוחרים לשתף יצירה זו עם ציבור המשתמשים האחרים – במקרה של YouTube באמצעות מתן הרשאות צפייה ציבוריות, ובמקרה של Uploaded באמצעות העתקת הקישור לקבצים והצגתו בבלוגים ובפורומים. עוד נקבע שתרומתם של ספקי השירות להפרה הישירה שהמשתמשים מבצעים היא חיונית שכן בהיעדרה ההפרה אינה יכולה להתבצע. ואולם, בית המשפט קבע כי ספק שירות ייחשב אף הוא כאחראי להפרת זכות ההעמדה לציבור רק אם יוכח כי תרומתו לא הייתה רק חיונית אלא גם מכוונת.[70] לפי פסק הדין, בבחינת כוונתו של ספק השירות לתרום תרומה חיונית להפרה הישירה בית המשפט צריך לשקול כמה שיקולים:

(**1**) ספק השירות ידע או היה עליו לדעת באופן כללי שמשתמשי הפלטפורמה מעמידים באמצעותה לרשות הציבור יצירות המוגנות בזכות יוצרים שלא כחוק. אולם אין די במודעות בפועל או בכוח, אלא נדרש שלמרות ידיעה זאת

68 Joined Cases C-682/18 & C-683/18, Peterson v. Google LLC, ECLI:EU:C:2021:503 (להלן: עניין *Youtube* ו־*Cyando*).

69 **שם**, בפס' 45 לחוות דעתו של ה־Advocate General.

70 **שם**, בפס' 60–83 לפסק הדין.

נמנע ספק השירות מלספק אמצעים טכנולוגיים מתאימים כדי למנוע הפרת זכות יוצרים, כמצופה ממפעיל זהיר.[71] ה־CJEU פסק ש־Youtube נקטה אמצעים אמינים ויעילים כדי להתמודד עם הפרת זכויות יצרים, כמו יידוע המשתמשים כמה פעמים בכך שהעלאת תכנים המפירים זכויות יוצרים היא אסורה, וכן ש־Youtube אימצה מגוון אמצעים טכנולוגיים כדי למנוע הפרת זכויות יוצרים על גבי הפלטפורמה שלה, כמו הליכי יידוע והתראה שונים לדיווח על תכנים מפירים, כמו גם תוכנות לאימות ולהכרת תוכן.[72]

(**2**) ספק השירות סיפק למשתמשים כלים לשיתוף לא חוקי של התכנים המפירים או עודד במודע שיתוף כאמור, כפי שאפשר ללמוד מהמודל הכלכלי של ספק השירות.[73] ה־CJEU בחן את אופן פעולתה של פלטפורמת Uploaded ופסק כי מפעילת הפלטפורמה Cyando כלל לא יצרה, בחרה או בדקה את התכנים שהמשתמשים שלה מעלים, ואף לא צפתה בהם, ועל כן לא סיפקה להם כלים להפרת זכות יוצרים. יתרה מזו, Cyando סיפקה רק למשתמש הקצה עצמו קישור לתוכן שהעלה, ולא נתנה בידו כלים המאפשרים לו לשתף את התוכן עם הציבור.[74]

אם נמצא שספק השירות תרם תרומה חיונית ומכוונת להפרה הישירה של זכות היוצרים, על בית המשפט לבחון את תחולת החריג לאחריות התורמת – נמל הביטחון הקבוע בסעיף 14 לדירקטיבת ה־E-Commerce. בפרשות *YouTube* ו־*Cyando* נפסק שספק שירות יוכל ליהנות מהחריג לאחריות תורמת להפרת זכות יוצרים בידי משתמש הקצה רק בהתקיים אחד מהתנאים האלה:

(**1**) הוא אינו מודע בפועל להפרת זכות יוצרים ספציפית ואין ביכולתו לשלוט על התכנים המועברים באמצעות השירות שהוא מספק;

71 **שם**, בפס' 84.

72 **שם**, בפס' 90–96.

73 **שם**, בפס' 60–83.

74 **שם**, בפס' 98–99.

(2) הוא אינו מודע לעובדות או לנסיבות שהובילו להפרת זכות היוצרים, או פעל להסרת התכנים המפירים או למניעת גישה אליהם מייד כאשר למד עליהם.[75]

היעדר מודעות בפועל או בכוח או שליטה כאמור ייתכנו רק כאשר ספק שירות הוא ניטרלי לתכנים, כלומר פועל באופן טכני גרידא, אוטומטי ופסיבי. העובדה שספק השירות מפעיל כלים טכנולוגיים לאיתור תכנים מפירים, מקטלג באופן אוטומטי את התכנים שהמשתמשים מעלים ומאפשר חיפוש ואיתור תכנים, כפי שעושה YouTube, או מודע לאופייה הדו־שימושי של הטכנולוגיה שמספק, אינה מלמדת על מודעות של ספק השירות לתכנים המפירים או על שליטתו בהם. לצד זאת, כדי ליהנות מנמל הביטחון ולהוכיח היעדר מודעות או שליטה, ספק השירות אינו נדרש לנטר באופן תמידי את התוכן שהמשתמשים מעלים לפלטפורמה שהוא מספק.[76] בפרשת *eBay*, למשל, נפסק שהחברה אינה יכולה ליהנות מנמל הביטחון הקבוע בסעיף 14 לדירקטיבת ה־E-commerce שכן היא פועלת למיטוב מודעות הפרסומת של לקוחותיה, וכך יכולה להיחשף למידע הנוגע להצעה למכירה של מוצר המפר זכויות קניין רוחני, או להשיג שליטה במידע כזה.[77]

עם זאת, משטר האחריות החל על ספקי שירות לפי דירקטיבת ה־E-commerce ולפי פסיקת ה־CJEU בפרשות *YouTube* ו־*Cyando* עומד להשתנות בעקבות הוראות ה־Digital Service Act (DSA), שאושרו בפרלמנט האירופי באוקטובר 2022 ונכנסו לתוקף בינואר 2024.[78] ה־DSA נועד להתאים את המשטר המשפטי בתחום הקניין הרוחני להתקדמויות הטכנולוגיות שהתרחשו מאז כניסתה לתוקף של דירקטיבת ה־E-commerce לפני עשרים שנה, ובראשן הופעת הפלטפורמות האינטרנטיות, המשמשות כיום כמתווכות העיקריות, כמקור

75 שם, בפס' 103–118.

76 שם, בפס' 104–111.

77 Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-6011

78 Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Service Act), art. 93, 2022 O.J. (L 277) 1

מידע וכמעצבות השיח. ה־DSA הוא נדבך נוסף בניסיון להתאים את אירופה לעידן הדיגיטלי, להגן על הצרכנים ברשת האינטרנט, להבטיח את זכויות היסוד שלהם וליצור מרחב סייבר פתוח ושקוף שבו החדשנות תשגשג. הוראות ה־DSA מחליפות את הוראת נמלי הביטחון שבדירקטיבת ה־E-Commerce,[79] ומטרתן ליצור אחידות במשטר האחריות של מתווכים[80] – ספקי שירות המוגדרים כ"צינורות העברה" (mere conduit), ספקי שירות העברה או מטמון (caching services) או ספקי שירות אחסון (hosting service). מתווכים עשויים לכלול ספקי רשת אלחוטית מקומית, ספקי שמות מתחם, ספקי רשתות וירטואליות פרטיות, מנועי חיפוש, ספקי שירותי ענן, ספקי שירותי דוא"ל וספקי שירותי Voice Over IP.[81] ה־DSA משמר את עקרונות דירקטיבת ה־E-commerce באשר להחרגת ספק שירות ניטרלי מאחריות תורמת וכן בכל הנוגע לאחריות המפר הישיר.

ה־DSA מדגיש שהכתובת הראשונה והמרכזית להתמודדות עם תכנים ופעולות בלתי חוקיות צריכה להיות משתמשי הקצה המבצעים את הפעולה הבלתי חוקית, ולא ספקי השירות המשמשים כמתווכים.[82] כן משמר ה־DSA את העיקרון שלפיו לא חלה על מתווכים חובת ניטור אקטיבית, ומובהר שפעולותיו הוולונטריות של הספק לאיתור וזיהוי תוכן בלתי חוקי, וכן פעולות שהספק נוקט משנתגלה תוכן כזה, המבוצעות בתום לב ובאופן זהיר, אובייקטיבי ומידתי, תוך התחשבות בזכויותיהם של כלל הצדדים ונקיטת אמצעי זהירות למניעת טעויות והסרה בלתי מוצדקת של תכנים חוקיים, אינן מלמדות כשלעצמן על מודעותו של הספק לתוכן או על שליטה בתוכן המועבר או המועלה בידי המשתמשים לשירות שהוא מספק.[83]

79 **שם**, בסעיף 89.

80 **שם**, בסעיף 2(a).

81 **שם**, בסעיפי הקדמה 28–29 ובהגדרת "intermediary service" בסעיף 3.

82 **שם**, בסעיף הקדמה 27.

83 **שם**, בסעיפים 7–8 ובסעיפי הקדמה 26 ו־30.

כך, נקבע שלא תוטל אחריות תורמת להפרת זכות יוצרים על ספק המשמש צינור העברה בלבד בהתקיים התנאים שלהלן: (1) הספק אינו יוזם את העברת התוכן; (2) הספק אינו בוחר את מקבל התוכן; (3) הספק אינו בוחר או משנה את התוכן המועבר. כלומר ספק הממלא תפקיד אקטיבי המאפשר לו שליטה על המידע או מודעות לתוכנו, או ספק שירות המשתף פעולה במכוון עם המשתמש לשם פעילות בלתי חוקית, לא יוכל ליהנות מהחריג לאחריות תורמת בכל הנוגע לתוכן בלתי חוקי שהמשתמשים מעלים. לדוגמה, חריג האחריות לא יחול על ספק שירות שהמטרה העיקרית של השירות שהוא מציע היא לאפשר פעילות בלתי חוקית, בין שהספק מציג זאת במפורש ובין שהשירות מתאים למטרה זו. עם זאת, ה־DSA מבהיר שהעובדה שהשירות מאפשר הצפנה של התכנים המועברים או שאפשר לעשות בו שימוש אנונימי אינה מלמדת, כשלעצמה, על כך שהשירות מכוון לאפשר פעולות בלתי חוקיות.[84]

ספק המספק שירותי מטמון (caching) לא יישא באחריות להעברה, לתיווך ולאחסון זמני של תוכן מפר, אשר בוצעה רק למטרה של העברת מידע באופן יעיל ובטוח למשתמשים אחרים של השירות לפי בקשתם, ובלבד שהספק (1) אינו משנה את התוכן המועבר; (2) מציית להוראות ה־DSA בנוגע למתן גישה לתוכן; (3) אינו מפריע לשימוש חוקי בטכנולוגיה המוכרת בתעשייה לשם השגת מידע על השימוש בתוכן; (4) פועל להסרת התוכן המפר או לחסימת הגישה אליו מייד כאשר נודע לו שהמידע הוסר ממקור ההעברה או שהגישה אליו נחסמה, או אם רשות משפטית הורתה על הסרתו או על חסימת הגישה אליו.[85]

על ספק שירותי אחסון (hosting) לא תוטל אחריות תורמת לאחסון תוכן מפר אם לא היה מודע לפעילות הבלתי חוקית או לתוכן המפר, או אם לא היה מודע לנסיבות שברור מהן שמתרחשת התנהגות הלא חוקית או שהתוכן אינו חוקי, כלומר היעדר מודעות בפועל או בכוח, או אם פעל להסרת התוכן הבלתי חוקי או למניעת הגישה אליו מייד כשנודע לו על קיומו. מודעותו של הספק יכולה לנבוע מפעולות שהוא מבצע בעצמו או מהודעה ממי שנפגע מהתוכן

84 **שם**, בסעיף 4 ובסעיפי הקדמה 18, 20–21.

85 **שם**, בסעיף 5.

הבלתי חוקי. ואולם, עצם העובדה שהספק יודע שהשירות שהוא מציע משמש לאחסון תוכן בלתי חוקי, שהספק מקטלג באופן אוטומטי את התכנים המועלים לפלטפורמה שלו או שהוא מאפשר חיפוש בתוכן ומספק המלצות לתוכן על בסיס הפרופיל האישי שהוא מגבש על כל אחד ממשתמשיו, אינה מלמדת על מודעותו בפועל לקיומו של תוכן בלתי חוקי. כמו כן, הסרת התוכן או חסימת הגישה אליו בידי הספק צריכות להיעשות תוך התחשבות בזכויות בסיסיות של המשתמשים, לרבות הזכות לחופש ביטוי.[86]

1.3. ישראל

הבסיס לדוקטרינת ההפרה התורמת בדין הישראלי מצוי בסעיף 12 לפקודת הנזיקין, אשר מאפשר הטלת אחריות משפטית על המייעץ או המשדל למפר הישיר.[87] כלומר לשם הטלת אחריות משפטית לא נדרשת מערכת יחסים הדוקה בין המפר הישיר למפר התורם, כמו למשל במקרה של עובד ומעסיק או מרשה ושלוח; די בהוכחת קיומה של מערכת יחסים רחוקה יותר המקיימת קשר כלשהו בין המפר הישיר למפר התורם. להטלת אחריות תורמת לעוולה נזיקית שתי הצדקות מרכזיות: האחת – הטלת אחריות על מונע הנזק הזול, והשנייה – הרצון לפצות את הניזוק בהתבסס על עקרון הכיס העמוק, כלומר האחריות מוטלת על מי שיש בידו האמצעים לעמוד בפיצוי הנדרש לניזוק. עם זאת, המשקל שניתן להצדקה זו הצטמצם לאורך השנים נוכח המשמעות של הטלת אחריות משפטית בהתאם ליכולת הכלכלית.[88]

חדירתה של דוקטרינת ההפרה התורמת לדיני הקניין הרוחני בישראל הייתה הדרגתית. תחילה נסקרה דוקטרינת ההפרה התורמת בפרשת **רגבה** באשר

86 **שם**, בסעיף 6 ובסעיף הקדמה 22.

87 סעיף 12 לפקודת הנזיקין [נוסח חדש], נ"ח התשכ"ח 266: "לענין פקודה זו, המשתף עצמו, מסייע, מייעץ או מפתה למעשה או למחדל, שנעשו או שעומדים להיעשות על ידי זולתו, או מצווה, מרשה או מאשרר אותם, יהא חב עליהם".

88 פישמן אפורי, **לעיל** ה"ש 22, בעמ' 41–42.

לשאלת האחריות להפרת פטנט. השופטים באותה פרשה חיוו דעתם שאימוצה של הדוקטרינה בדיני הפטנטים בישראל, תוך קביעת תנאים מגבילים להוכחתה, עשוי להיות התפתחות חיובית. עם זאת, הם נמנעו מלהכריע בסוגיה.[89]

בתחילת שנות האלפיים חל שינוי בעמדת בית המשפט העליון והוא הכיר בקיומה של דוקטרינת ההפרה התורמת בדיני הפטנטים בפסק דינו בפרשת **רב בריח**. בית המשפט העליון אזכר בפסיקתו את סעיף 12 לפקודת הנזיקין, הקובע את עקרונות האחריות התורמת במקרה של עוולה נזיקית, והציג את האפשרות לייבא את הדוקטרינה לחוק הפטנטים באמצעות הקביעה כי הפרת פטנט היא בבחינת הפרת חובה חקוקה לפי סעיף 63 לפקודת הנזיקין.[90] אולם ההכרה בקיומה של דוקטרינת ההפרה התורמת בפסק הדין בפרשת **רב בריח** התבססה בעיקרה על התפתחותה בפסיקה בארצות הברית ובגרמניה.[91] נפסק כי לשם הטלת אחריות תורמת להפרת פטנט יש להוכיח את קיומם של התנאים שלהלן: (1) קיומה של הפרה ישירה; (2) הרכיבים שבגינם הוגשה התביעה מהווים חלק מהותי מהאמצאה המוגנת בפטנט; (3) קיום יסוד נפשי – הנתבע ידע בפועל, או שהיה עליו לדעת לפי הנסיבות ובהתאם למבחן האדם הסביר, על ההפרה הישירה; (4) אין שימוש משמעותי אחר מהשימוש המוגדר בפטנט.[92]

דוקטרינת ההפרה התורמת יובאה לדיני זכויות היוצרים בישראל רק כעבור עשור, בפסק דינו של בית המשפט העליון בפרשת **שוקן**.[93] באותה פרשה נבחנה

89 ע"א 7614/96 **צחורי ובניו תעשיות בע"מ נ' רגבה – מושב שיתופי חקלאי**, פ"ד נד(3) 721, 741–742 (2000).

90 ע"א 1636/98 **רב בריח בע"מ נ' בית מסחר לאביזרי רכב חבשוש (1987) בע"מ**, פ"ד נה(5) 337 (2001), פס' 23 לפסק דינו של השופט אנגלרד (להלן: פרשת **רב בריח**); מיכאל ד' בירנהק "לידתה של עוולה: הפרה תורמת בדיני פטנטים" **טכנולוגיות של צדק: משפט, מדע וחברה** 169, 173 (שי לביא עורך 2003) (להלן: בירנהק "לידתה של עוולה").

91 פרשת **רב בריח**, **לעיל** ה"ש 90, בפס' 25–30 לפסק דינו של השופט אנגלרד; פישמן אפורי, **לעיל** ה"ש 22, בעמ' 12.

92 פרשת **רב בריח**, **לעיל** ה"ש 90, בפס' 31–35 לפסק דינו של השופט אנגלרד.

93 פרשת **שוקן**, **לעיל** ה"ש 22.

אחריותה של האוניברסיטה העברית לשכפול והפצה של יצירה ללא אישור בעל זכויות היוצרים בה – הוצאת שוקן – בידי נציג תא סטודנטיאלי באוניברסיטה תוך שימוש במשאבים שהאוניברסיטה העמידה לרשותו. השופט ריבלין עמד על כך שחוק זכויות היוצרים מכיר בהפרה תורמת באופן מוגבל בהקשר של בעל מקום בידור, כגון תיאטרון או אולם שמחות, וכן מכיר בהפרת הזכות לביצוע פומבי; אולם אין החוק מכיר באפשרות העקרונית להטלת אחריות מכוח דוקטרינת ההפרה התורמת.[94]

בבוחנו את יתרונותיה של דוקטרינת ההפרה התורמת ציין השופט ריבלין כי אימוצה לדיני זכויות היוצרים יאפשר לבעל זכות היוצרים להרחיב את מעגל הנתבעים האפשריים ו"להיפרע ממי שהייתה לו יד בהפרת זכותו", גם כשמדובר במי ש"אינו מבצע את ההפרה בעצמו, אך הוא מאפשר ומתיר את פעילותו המפירה של גורם אחר, או אף מסייע ומעודד את אותה הפעילות. הוא משמש מעין 'גורם ביניים', בשרשרת ההפרה – בטווח שבין המפר הישיר (מפר 'הקצה'), לבין בעל הזכות".[95]

בהמשך פנה השופט ריבלין לסקור את ההצדקות לעיגונה החוקי של זכות היוצרים ואת הרלוונטיות שלהן להכרה בדוקטרינת ההפרה התורמת. ראשית, השאיפה לתגמל את היוצר ולהגן על האינטרסים הקניינים הלגיטימיים שלו מצדיקה גם הטלת אחריות על גורמי ביניים שפעולתם מביאה לפגיעה בזכויותיו של היוצר. כך יוכל היוצר להיפרע מכל מי שהיה מעורב בהפרת זכויותיו. שנית, החשש מפני פגיעה בתמריציו של היוצר ליצור וההשלכות של פגיעה זו על החברה והחדשנות עומדים בבסיס ההכרה בזכות היוצרים וההגנה עליה, ורלוונטיים גם להצדקת ההכרה במפר תורם. זאת נוכח כשל השוק, שהופך את אכיפת זכות היוצרים נגד כל אחד מהמפירים הישירים ליקרה ובלתי יעילה כלכלית ומוביל לאכיפת חסר העלולה לפגוע בתמריץ של היוצר להמשיך וליצור. מתן כלי בידיו של בעל זכות היוצרים לתבוע את המפר התורם, שהוא גוף יחיד ומוכר, פותר כשל שוק זה ומבטיח גמול ראוי ליוצר והמשך ההגנה על

94 סעיף 49 לחוק זכות יוצרים, התשס"ח-2007; פרשת **שוקן, לעיל** ה"ש 22, בפס' 12 לפסק דינו של השופט ריבלין.

95 **שם**, בפס' 11-12.

תמריצו. הצדקה נוספת להטלת אחריות על המפר התורם נעוצה בהיותו מונע הנזק הזול, דהיינו הגורם שיכול לפקח ביעילות ובאופן פשוט וזמין יחסית על המפירים הישירים.[96]

עוד נשען השופט ריבלין על ההכרה בדוקטרינת ההפרה התורמת בפסיקה בארצות הברית ובפסיקת בית המשפט העליון בפרשת **רב בריח**. דיני הפטנטים ודיני זכויות יוצרים משתייכים לאותה "משפחת" דינים, ועל כן הם עשויים להשפיע זה על זה, תוך התאמה למאפייניו הייחודיים של כל משטר. כן מציין השופט ריבלין את הוראת סעיף 12 לפקודת הנזקין כצינור הקליטה של הדוקטרינה לדיני זכויות היוצרים, שכן הפרת זכות יוצרים נחשבת עוולה אזרחית שפקודת הנזיקין חלה עליה, בשינויים המתחייבים נוכח תכלית חוק זכויות יוצרים – המשקף איזון עדין בין גמול ליוצר על השקעתו והבטחת תמריצים להמשך היצירה, לבין הגנה על זכויות המשתמשים ועידוד פלורליזם במרחב הציבורי.[97] לפיכך נקבעו בפסק הדין בפרשת **שוקן** שלושה תנאים מצטברים לתחולתה של אחריות תורמת להפרת זכות יוצרים. תנאים אלו מבטאים יישום זהיר של דוקטרינת ההפרה התורמת ומזעור הפגיעה במשתמשים ובמרחב הציבורי:[98]

(**1**) קיומה בפועל של הפרה ישירה. משמעות דרישה זו היא שהטלת אחריות על מפר תורם תתאפשר רק כאשר אכן מופרת זכות היוצרים. עם זאת, תנאי זה עשוי להתקיים אף אם פעולתו של המפר הישיר חוסה תחת אחד מהחריגים הקבועים בחוק זכות יוצרים, כגון חריג השימוש ההוגן, משום שהגנות אלו מונעות מהמפר לשאת באחריות להפרה, אך אינן מאיינות את עצם ההפרה. נוסף על כך, ייתכן שהנזק הנגרם מפעולתו של כל אחד מהמפירים הישירים אינו גדול, ואף עשוי לחסות תחת אחת מן ההגנות הקבועות בחוק זכות יוצרים,

96 **שם**, בפס' 13–15.

97 פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 18, 20–23 לפסק דינו של השופט ריבלין, ובפס' 3 לפסק דינו של השופט דנציגר; סעיף 52 לחוק זכות יוצרים: "הפרה של זכות יוצרים או זכות מוסרית היא עוולה אזרחית, והוראות פקודת הנזיקין [נוסח חדש] יחולו עליה, בשינויים המחוייבים ובכפוף להוראות חוק זה".

98 פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 18, 20–23 לפסק דינו של השופט ריבלין; פישמן אפורי, **לעיל** ה"ש 22, בעמ' 8–10.

אולם הנזק המצטבר הנגרם מההפרה על ידי כל המפירים הישירים הוא גדול, וחוסר היכולת של בעל זכות היוצרים לקבל פיצוי בגינו הוא כשל אכיפה שדוקטרינת ההפרה התורמת באה לפתור.[99]

(**2**) מודעותו של המפר התורם להפרה הישירה. לדרישת המודעות מספר הצדקות. ראשית, היא עולה בקנה אחד עם הדרישות שנקבעו בפסיקה להוכחת אחריות מכוח סעיף 12 לפקודת הנזיקין. שנית, מנקודת מבטה של החברה בכללותה, הטלת אחריות על מונע הנזק הזול תיתכן רק כאשר היה ביכולתו למנוע את ההפרה. יכולת זו מותנית במודעותו של המפר התורם לעצם ביצועה של ההפרה על ידי המפר הישיר. הצדקות אלו מחייבות ידיעה ממשית וקונקרטית כחלק מדרישת המודעות, ואין די בידיעה קונסטרוקטיבית כללית. זאת משום שהסתפקות בידיעה בכוח בלבד עשויה להטיל נטל כבד מדי על כתפי גורמי הביניים, להצר את פעולתם החופשית בשוק ולהטלת אחריות רבה מדי עליהם. ואולם, אין צורך בהוכחת ידיעת המפר התורם על כל אחת ואחת מההפרות הספציפיות, שכן דרישה שכזו הייתה יוצרת את אותו כשל אכיפה שבו נתקל בעל הזכות למול המפירים הישירים הרבים: גם גורם הביניים אינו מודע לפעילותו של כל אחד ואחד מהמפירים הישירים. לפיכך נפסק שדי במודעות בפועל לקיומה של פעילות מפירה.[100]

(**3**) קיומה של תרומה משמעותית, ניכרת וממשית לביצוע ההפרה.[101] דרישה זו נשענת על לשון סעיף 12 לפקודת הנזיקין, המציג כמה פעולות אשר עשויות ללמד על תרומה משמעותית של גורם הביניים להפרה: שיתוף, סיוע, ייעוץ, פיתוי, ציווי, הרשאה או אשרור של ההפרה הישירה.

קיומו של תנאי זה ייבחן לפי נסיבות המקרה, ובית המשפט יביא בחשבון את מכלול פעולותיו של גורם הביניים, את מעורבותו בשרשרת האירועים שהביאה להפרה ואת יכולתו למנוע אותה בנקיטת אמצעים סבירים. אם המפר התורם

99 פרק ד' לחוק זכות יוצרים; פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 24 לפסק דינו של השופט ריבלין.

100 **שם**, בפס' 25.

101 **שם**, בפס' 23.

יכול למנוע את ההפרה במאמצים סבירים אך נמנע מכך, הרי שמתקיים תנאי זה והימנעותו מפעולה נחשבת תרומה משמעותית. בחינה זו תואמת את תיאוריית מונע הנזק הזול: אם המפר התורם נדרש לנקוט אמצעים יקרים ובלתי סבירים כדי למנוע את ההפרה, לא עומדת עוד ההצדקה הכלכלית להטיל עליו אחריות תורמת שכן הוא אינו מונע הנזק הזול. לפיכך סבירות האמצעים נמדדת במונחים כלכליים של עלותה של פעולת מניעת הנזק. אם העלות אינה זניחה, אין הצדקה להטילה דווקא על גורם הביניים.[102] בספרות הוצע כי בבחינת סבירות האמצעים שגורם הביניים נקט יש לתת משקל לקוד הפעולה המקובל בענף הרלוונטי. לשם הגברת הוודאות המשפטית בהחלת דוקטרינת ההפרה התורמת, יש לצאת מנקודת הנחה שציות לסטנדרט הפעולה המקובל בתעשייה מלמד על סבירות האמצעים הננקטים על ידי גורם הביניים.[103]

עוד הבהיר השופט ריבלין בפרשת **שוקן** שאין צורך בהוכחת קשר סיבתי במובנו הצר, כלומר בהוכחה שפעילות המפר התורם הייתה תנאי הכרחי לקיומה של ההפרה הישירה, אלא די בהיותה חלק אינטגרלי ומשמעותי בשרשרת הפעולות שהובילו להפרה הישירה.[104] על פרשנות זו נמתחה ביקורת בנימוק שהיא עלולה לפגוע בוודאות המשפטית ולהביא לתחולה רחבה מדי של דוקטרינת ההפרה התורמת. למשל, יהיה אפשר לטעון שיש להטיל על חברת החשמל אחריות תורמת להפרת זכות יוצרים, שכן ללא חשמל לא היה אפשר להפעיל את המחשבים שבאמצעותם בוצעה ההפרה. מנגד, גם דרישה שמעורבותו של המפר התורם תהיה ישירה עד כדי הגדרתו כמעוול במשותף אינה רצויה, שכן היא עלולה לרוקן מתוכן את דוקטרינת ההפרה התורמת. הוצע שדרישת התרומה המשמעותית תפורש כדרישה להוכחת מעורבות גבוהה מאוד עד כדי הפרה ישירה על ידי גורם הביניים – כלומר להבחין בין גורם ביניים המספק אמצעים היקפיים בלבד ותרומתו פסיבית לבין גורם ביניים הפועל באופן אקטיבי לשם ביצוע הפעולות המפירות. לצד זאת הוצע שאם נעשה בשירות שגורם הביניים מספק גם שימוש חוקי משמעותי, אזי

102 **שם**, בפס' 26–27.

103 פישמן אפורי, **לעיל** ה"ש 22, בעמ' 50–61.

104 פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 26–27 לפסק דינו של השופט ריבלין.

לא מתקיים קשר סיבתי בין מעשה ההפרה לפעולותיו של גורם הביניים ולא מתקיים תנאי התרומה המשמעותית.[105]

בפרשת **שוקן** נפסק שתנאי התרומה המשמעותית, הממשית והניכרת לא התקיים באשר לאוניברסיטה העברית. אומנם תרומתה של האוניברסיטה להפרת זכויות היוצרים הייתה תרומה שבמחדל, והיא לא פעלה כלל למניעת ההפרה. עם זאת, האוניברסיטה אינה מונע הנזק הזול; היא אינה יכולה לפקח באמצעים סבירים על פעולותיהם של התאים הסטודנטיאליים או של כל סטודנט וסטודנט, ולמנוע את הפרות זכויות היוצרים שנגרמות בשל מעשיהם.[106]

בפרשת **א.ל.י.ס.** (2011) יישם בית המשפט המחוזי מרכְּז את דוקטרינת ההפרה התורמת בעניין הפרת זכות יוצרים. באותה פרשה הגישה חברה העוסקת בהגנה על זכויות יוצרים בסרטים תביעה נגד מפעילי אתר אינטרנט שבו מתנהלים פורומים מקוונים, בהם שני פורומים שהכניסה אליהם מותנית ברישום ובתשלום דמי חבר – פורום אחד שכותרתו "הורדות" ופורום שני שנקרא "סרטים וטלוויזיה". בתביעה נטען כי משתמשי הפורומים, ובעיקר הפורומים שבתשלום, מציבים בהם קישורים לאתרי אינטרנט שמהם אפשר להוריד באופן בלתי חוקי סרטי קולנוע המוגנים בזכויות יוצרים, ועל מפעילי האתר לשאת באחריות תורמת להפרה הישירה. בפסק דינו עמד בית המשפט המחוזי על הצורך באיזון בין היותו של גורם הביניים מונע הנזק הזול ורצונו של בעל הזכות להגן על זכויותיו באופן אפקטיבי ויעיל, לבין האינטרס הפרטי של גורם הביניים לספק את השירות שבו בחר מבלי לשאת בעול של ניטור וסינון התכנים לשם מניעת פגיעה בבעל הזכות, והאינטרס החברתי בהגנה על חופש הביטוי ובהימנעות מצינון פעילות חברתית רצויה באמצעות יצירת מנגנוני אחריות ופיקוח יקרים. עוד הצביע בית המשפט על היעדר הסדר הולם בחוק לאחריות ספק שירות, שבעטיו בית המשפט נאלץ להפעיל כללים מהמשפט הפרטי תוך התאמתם לנסיבות המקרה ולטכנולוגיה הרלוונטית.[107]

105 פישמן אפוריי, **לעיל** ה"ש 22, בעמ' 50–61.

106 פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 28 לפסק דינו של השופט ריבלין.

107 ת"א (מחוזי מר') 09-08-567 **א.ל.י.ס. אגודה להגנת יצירות סינמטוגרפיות (1993) בע"מ נ' רוטר. נט בע"מ** (נבו 8.8.2011), פס' 18–19, 21 לפסק הדין (להלן: פרשת **א.ל.י.ס.**).

בפסיקתו בפרשת **א.ל.י.ס.** הדגיש בית המשפט המחוזי כי הבסיס הסטטוטורי להחלת דוקטרינת ההפרה התורמת בדיני זכויות היוצרים בישראל הוא סעיף 12 לפקודת הנזיקין באמצעות "צינור הקליטה" הקבוע בסעיף 52 לחוק זכויות היוצרים, אשר מבהיר שהפרת זכות יוצרים היא עוולה אזרחית שפקודת הנזיקין חלה עליה – זאת לצד הצדקות נורמטיביות נוספות, לרבות פתרון לכשל השוק הפוגע בהגנה על זכות היוצרים ובתמריץ היוצר להמשיך וליצור וכן עקרון מונע הנזק הזול.[108]

בבחינת קיומם של התנאים להחלת דוקטרינת ההפרה התורמת, כפי שנקבעו בפרשת **שוקן**, הגיע המשפט המחוזי למסקנה כי בנסיבות המקרה בפרשת **א.ל.י.ס.** דרישת המודעות של גורם הביניים תתקיים רק אם בעל זכות היוצרים הודיע לו על קיומה של יצירה מפירה. הנימוק לצמצומה של דרישת המודעות באופן זה היה שבנסיבות המקרה, הטלת אחריות תורמת ללא הודעה קודמת מבעל זכות היוצרים משמעה החלת חובה רחבה של ניטור תכנים על גורם הביניים. החלת חובת ניטור כזו אינה עולה בקנה אחד עם פסיקת בית המשפט העליון בפרשת **שוקן**, שהדגישה שנדרשת מודעות בפועל ולא בכוח. חובת ניטור אף אינה רצויה מבחינה חברתית, שכן היא הופכת את גורם הביניים לעורך תוכן ובכך מגבירה את החשש לצנזורה ולפגיעה בחופש הביטוי של ציבור המשתמשים באתר.[109] בקביעה זו אימץ בית המשפט לדין הישראלי ולהחלתה של דוקטרינת ההפרה התורמת את פרשנות דרישת המודעות שבה דגל בית המשפט במחוז התשיעי בפרשת **גרוקסטר**. פרשנות זו נדחתה במפורש בידי בית המשפט העליון האמריקני בפסק הדין בראשותו של השופט סוטר.[110]

בפסק דינו בפרשת **א.ל.י.ס.** הבהיר בית המשפט המחוזי גם את המבחנים הראויים לקביעה אם הנתבע הוא מונע הנזק הזול, כלומר את סבירות האמצעים שעל הנתבע לנקוט כדי למנוע את ההפרה. המבחן הראוי, לפי פסק הדין, הוא מבחן דו־ראשי: בחלקו האחד זהו מבחן יעילות הבוחן אם עלויות הפיקוח המצטברות שבעל זכות היוצרים צריך לשאת בהן כדי להגן על זכויותיו גבוהות

108 **שם**, בפס' 45–47.

109 **שם**, בפס' 43, 45–46.

110 ראו דיון בטקסט הנלווה להע"ש 41 **לעיל**.

יותר מעלויות הפיקוח המצטברות שעל הנתבע לשאת בהן, במקרה זה מפעיל אתר הפורומים. בחלקו השני זהו מבחן של צדק חלוקתי, אשר בודק אם הסטת עלויות הפיקוח המצטברות מבעל זכות היוצרים לנתבע או לגורמים כמותו, במקרה של פסק הדין – בעלי אתרים שבהם מתנהלים פורומים שהגולשים מפרסמים בהם קישורים לאתרים המאפשרים העתקה ללא רשות של יצירות מוגנות, היא הסטה מוצדקת. במסגרת מבחן הצדק החלוקתי בית המשפט מביא בחשבון את אינטרס הציבור ואת הערך החברתי שבפעילותו של הנתבע, כפי שבא לידי ביטוי בחריג השימוש החוקי שנקבע בפרשת **סוני**.[111]

בדומה להתפתחות דוקטרינת ההפרה התורמת בארצות הברית ובאיחוד האירופי, וכן ברוח פסיקת בית המשפט העליון בפרשת **שוקן**, בית המשפט המחוזי מבהיר בפסק דינו בפרשת **א.ל.י.ס.** שתיתכן הטלת אחריות תורמת על גורם ביניים גם כאשר לא ניתנה לו הודעה כנדרש, בשני מצבי קיצון או חריגים מרכזיים:[112]

הראשון הוא "חריג העידוד": בדומה לפסיקת בית המשפט העליון בארצות הברית בפרשת **גרוקסטר**, כאשר גורם הביניים מעודד באופן אקטיבי את הפרת זכות היוצרים, הרי שהוא מודע להפרה וגם תורם לה תרומה משמעותית, ולכן עליו לשאת באחריות תורמת להפרה. בבחינת העידוד מצד גורם הביניים יביא בית המשפט בחשבון, בין השאר, את שם השירות שגורם הביניים מספק, את אופן שיווקו בציבור ואת הנחיות השימוש בו.[113] השני הוא "חריג הפורום הפסול": כאשר פורום מסוים מבין הפורומים המופעלים באתר משמש רובו ככולו להצבת קישורים לאתרים מפירים, ובעל האתר מודע לכך, אף אם לא עודד זאת, עליו לחסום את הגישה לפורום. אם לא עשה כן, עליו לשאת באחריות תורמת להפרת זכות היוצרים. הקביעה אם פורום משמש רובו ככולו להצבת קישורים לאתרים מפירים תישען על בחינת היקף הקישורים לאתרים המפירים בהשוואה להיקף שאר הפעילות בפורום, וכן על בחינה אבסולוטית – מספר הקישורים המפירים שפורסמו בפורום. עוד ישקול בית

111 פרשת **א.ל.י.ס.**, **לעיל** ה"ש 107, בפס' 48, 50–51.

112 **שם**, בפס' 55.

113 **שם**, בפס' 56.

המשפט את שאלת הגישה לפורום: אם מדובר בפורום סגור, שהגישה אליו מוגבלת למשתמש רשום או למשתמש המשלם דמי שימוש, יקשה על בעל זכויות היוצרים לפקח ביעילות על פעילותו ולנטר את הצגת התכנים המפירים. משום כך, פורום סגור שמתקיים בו כלל האצבע שהציג בית המשפט, שלפיו בפורום יש יותר מ־10 קישורים לאתרים מפירים וההודעות הכוללות קישורים כאמור הן יותר מרבע מהתוכן המהותי בפורום, חשוד כפורום פסול, וקמה חזקה שלפיה מפעיל הפורום מודע להפרות ותורם להן משמעותית. לפיכך הוא עלול לשאת באחריות תורמת אם לא יצליח להפריך את החזקה. כאשר הכניסה לפורום פתוחה לכלל הגולשים, בית המשפט מחמיר יותר בקביעה אם זהו פורום פסול, וכלל האצבע שנקבע הוא שמחצית מהתוכן המהותי בפורום כולל קישורים לאתרים מפירים.[114] בפרשת **א.ל.י.ס.** התייחס בית המשפט רק לנסיבות המקרה שלפניו, אולם אפשר להבחין כי חריג זה הוא תמונת מראה של חריג השימוש החוקי המשמעותי מפרשת **סוני**: שם דובר על קיומו של שימוש חוקי משמעותי ושופטי בית המשפט העליון בפרשת **גרוקסטר** נמנעו מלקבוע אמות מידה כמותיות ברורות לקיומו של החריג,[115] ואילו כאן ההתמקדות היא במרכזיותו של השימוש הבלתי חוקי תוך ניסיון להגדירו באופן כמותי.

1.4. סיכום: דוקטרינת ההפרה התורמת – משפט משווה

טכנולוגיות דו־שימושיות, המאפשרות שימושים לא חוקיים בהן לצד שימושים חוקיים, מציבות זה כמה עשורים אתגרים משפטיים לפני בעלי זכויות היוצרים. אלו ביקשו להיתלות ביצרני הטכנולוגיה לשם אכיפת זכויותיהם, תוך התמודדות עם כשל האכיפה שנבע מקיומם של מפירים ישירים רבים ומפוזרים, וניצול היותם של יצרני הטכנולוגיה הדו־שימושית מונע הנזק הזול.

114 **שם**, בפס' 57.

115 ראו הטקסט הנלווה להע"ש 41 **לעיל**.

הטלת אחריות תורמת על יצרני הטכנולוגיה סיפקה את האפיק המתאים להפיכתם לזרוע האכיפה הארוכה של בעלי זכות היוצרים, תוך איזון בין ההגנה על זכות היוצרים ובין אינטרס הציבור בעידוד חדשנות וזרימה חופשית של רעיונות, מידע ומסחר.

כפי שמתומצת בלוח 1 להלן, בשלושת המשטרים המשפטיים שנבדקו – בארצות הברית, באיחוד האירופי ובישראל – אומצו הסדרים דומים, בפסיקה או בחקיקה, בנוגע להיקפה של האחריות התורמת של גורם הביניים להפרת זכות יוצרים בידי המשתמשים בשירותים. עם זאת, המגמה הברורה העולה מסקירת המשפט המשווה היא קיומו של משחק "חתול ועכבר" בין המשפט ובעלי זכויות היוצרים לבין מפתחי הטכנולוגיה: האחרונים למדו בכל שלב מהו הכלל המשפטי ופיתחו דרכים יצירתיות כדי לעקוף אותו ולהמשיך לאפשר למשתמשים להפר זכויות יוצרים מבלי לשאת באחריות תורמת לכך.

ואולם, לאחר האימוץ של דוקטרינת ההפרה התורמת ושל מדיניות ההודעה וההסרה בחקיקה ובפסיקה בערכאות הגבוהות בסוף שנות התשעים ובתחילת שנות האלפיים, פחתו מאוד תביעות מצד בעלי זכויות יוצרים נגד מפעילים של טכנולוגיות דו־שימושיות המאפשרות הפרת זכות יוצרים, ונדמה גם שהצטמצם פיתוחן של טכנולוגיות המזלזלות באופן בוטה בזכויות יוצרים. גם בגזרת החקיקה נרשמת יציבות, ויוזמות החקיקה האחרונות באיחוד האירופי נוגעות בעיקר לאחריות של פלטפורמות אינטרנטיות להבטחת מרחב סייבר בטוח והוגן עבור הצרכנים, ואינן מתמקדות דווקא בהפרת זכויות יוצרים. במקביל התפתחו מודלים טכנולוגיים ועסקיים המאפשרים צריכת יצירות מוגנות בזכויות יוצרים בקלות ובעלות נמוכה בכל רחבי העולם תוך כיבוד זכויות היוצרים לצד עידוד חדשנות ותחרות בשוק – למשל באמצעות שירותי מוזיקה בתשלום דוגמת ספוטיפיי, דיזר ואפל מיוזיק או שירותי טלוויזיה דוגמת נטפליקס ודיסני+.

אומנם הזכות לפרטיות אינה זוכה ללובי חזק כמו זכות היוצרים. אנשים פרטיים, עובדים, עיתונאים ואקטיביסטים שפרטיותם נפגעת טרם התאגדו

לשם פעולה משותפת נגד הפגיעה החמורה בזכותם החוקתית,[116] כפי שעשו בעלי זכויות היוצרים לפני כ־30 שנה עם הופעת תוכנות שיתוף הקבצים. אולם התהליך שהתרחש במשפט ובטכנולוגיה בתחום זכויות היוצרים עשוי דווקא לחזק את העמדה שלפיה יש לתת בידי בעלי הזכויות כלים משפטיים נוספים, בדמות הכרה בדוקטרינת ההפרה התורמת ואימוצה בפסיקה ובחקיקה, כדי לחזק את ההגנה על הזכות לפרטיות ולהביא, בסופו של דבר, להתפתחויות טכנולוגיות אשר יכבדו את הזכות ובה בעת ייתנו מענה לצרכים העסקיים של המעסיקים ולצורך של החברה בקִדמה וביעילות כלכלית.

לוח 1
דוקטרינת ההפרה התורמת – סקירת משפט משווה

דוקטרינת ההפרה התורמת

ארצות הברית

יציר המשפט המקובל. התנאים להחלתה:

1. הוכחת הפרה ישירה.

2. מודעות גורם הביניים:

כאשר קיים שימוש מסחרי חוקי משמעותי נדרשת הוכחת מודעותו להפרה. עם זאת, לא ברור אם יש צורך בהוכחת שימוש מסחרי חוקי משמעותי בפועל או די בהוכחת היתכנות טכנולוגית לשימוש חוקי כאמור.

בהיעדר שימוש מסחרי חוקי משמעותי, די בהוכחת מודעות בכוח להפרה ספציפית. אין די בהוכחת מודעות כללית לקיומם של שימושים מפירים.

כמו כן, לא ברור אם עצימת עיניים מכוונת מספיקה לשם הוכחת מודעות של גורם הביניים לשימושים המפירים.

3. תרומה משמעותית: אין די בהוכחה שגורם הביניים שימש כצינור פסיבי לפעילות מפירה או הפיק תועלת מהפעילות המפירה. מנגד, מתן המשאבים או התשתית לפעילות מפירה מספיקים להוכחת תרומה משמעותית.

116 לאחרונה הגיש ארגון העיתונאים העצמאי אל פארו מאל סלבדור תביעה נגד NSO בגין המעקבים שנוהלו נגד עיתונאים משורותיו, אולם נכון לעכשיו מדובר בתביעה יחידה מסוג זה והיא מצויה בשלבי בירור ראשוניים. ראו הטקסט הנלווה לה"ש 281 **להלן**.

דוקטרינת ההפרה התורמת

ארצות הברית (המשך)

בשנת 1998 נחקק ה־DMCA, הכולל "נמלי ביטחון" להחרגת ספקי שירות אינטרנטיים מאחריות ישירה, עקיפה או תורמת להפרת זכויות יוצרים שמבצעים משתמשים בשירות. ספקי השירות נדרשים לעמוד בכמה תנאים כדי ליהנות מהגנת נמל הביטחון הרלוונטי לעיסוקם. בין השאר, הם נדרשים להפעיל מנגנון "הודעה והסרה" ולהוכיח היעדר מודעות בפועל או בכוח להפרה. בפסיקה פורשה מודעות בכוח כמתקיימת בנסיבות מצומצמות שבהן ההפרה ברורה, כפי שאפשר לרוב להוכיח בהתבסס על הודעה מטעם בעל זכות היוצרים, ונקבע כי ספק השירותים האינטרנטיים אינו נדרש לבצע בחינה נוספת כדי לאשש את דבר קיומה של ההפרה. למעשה, פרשנות זו מובילה להקבלה כמעט מלאה בין מודעות בכוח למודעות בפועל. עוד נפסק כי עצימת עיניים מכוונת נוכח מידע על הפרה ספציפית תוכר כמודעות בכוח.

האיחוד האירופי

דירקטיבת ה־DSM מטילה סטנדרט אחריות מחמיר על ספק תוכן שיתופי באינטרנט: עליו לפעול מראש לקבלת רישיון מבעל זכות היוצרים ולהטמיע אמצעים טכנולוגיים, בהתאם למבחני סבירות ומידתיות, למזעור הפרות. נוסף על כך, הספק יימצא אחראי להפרה בכפוף למודעות בפועל בעקבות הודעה מתאימה מבעל זכות היוצרים. ספקי תוכן שיתופי באינטרנט שמטרתם העיקרית היא לאפשר הפרת זכויות יוצרים לא יוכלו ליהנות מהגנת הדירקטיבה.

לפי ה־DSA, ספק שירותי אחסון לא יישא באחריות תורמת להפרת זכויות יוצרים בידי המשתמשים בשירותיו אם יוכיח היעדר מודעות בכוח או בפועל או יוכיח שביצע פעולה להסרת התוכן מייד עם רכישת מודעות בפועל. מודעות כללית לכך שהשירות שהוא מספק יכול לשמש להפרת זכות יוצרים אינה מספקת לשם הכרה במודעות בכוח.

ישראל

דוקטרינת ההפרה התורמת נשענת על סעיף 12 לפקודת הנזיקין. התנאים להחלתה לפי פסק הדין של בית המשפט העליון בפרשת **שוקן**: (1) קיומה של הפרה ישירה; (2) מודעות ממשית וקונקרטית לקיומה של פעילות מפירה – לא נדרשת מודעות ממשית לכל הפרה ספציפית; (3) תרומה משמעותית, ניכרת וממשית לביצוע ההפרה.

בפרשת **א.ל.י.ס.** פירש בית המשפט המחוזי את דרישת המודעות כמחייבת הודעה בדבר קיומה של הפרה, ופסק כי בהיעדר מודעות תוטל אחריות תורמת רק בנסיבות קיצון מוגבלות: המפר התורם שידל או עודד את ההפרה הישירה; או התקיים חריג "הפורום הפסול", שהגדרתו מבטאת ניסיון של בית המשפט המחוזי לקבוע קנה מידה כמותי לשימוש בלתי חוקי, כתמונת ראי של חריג השימוש המסחרי החוקי המשמעותי מדוקטרינת ההפרה התורמת בארצות הברית.

פרק 2
הזכות לפרטיות וחשיבותה

בפרק הקודם עסקנו בדוקטרינת ההפרה התורמת בדיני זכויות היוצרים, בהתפתחותה לאורך השנים בארצות הברית ובאיחוד האירופי ובאימוצה לבסוף לדיני זכויות היוצרים בישראל. עתה הגיע הזמן לפנות לבחינת אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות, ולבדוק אם יצרן נוזקת מעקב עשוי לחוב באחריות תורמת לפגיעה בפרטיותו של אדם שנוזקת מעקב כאמור הותקנה במכשיר הסלולרי האישי שלו. אולם בטרם נצלול לשאלות אלו יש להציג ביתר פירוט את הזכות לפרטיות, את הערכים שבבסיסה ואת חשיבותה. דיון זה הכרחי וחשוב כדי לבחון את מידת הפגיעה בזכות ואת הפתרונות האפשריים לפגיעה זו. בכך יעסוק בקצרה פרק זה.

הזכות לפרטיות מעוגנת במפורש במשפט הישראלי כזכות יסוד חוקתית, בסעיף 7 לחוק־יסוד: כבוד האדם וחירותו, וכזכות סטטוטורית, בחוק הגנת הפרטיות, התשמ"א–1981. עם זאת, מדובר בזכות המתאפיינת בעמימות רבה, שטיבה אמורפי וגבולותיה מושפעים ממערכת היחסים הדינמית שבין החברה (נורמות חברתיות מקובלות) למשפט ולטכנולוגיה.[117]

הצורך בהבנת הערכים שבבסיסה של הזכות לפרטיות ובעמידה על חשיבותה הוליד גישות תיאורטיות שונות להגדרתה לאורך השנים. אף שגישות אלו לא הובילו לאימוצה של הגדרה ברורה, אחידה ומקיפה לזכות לפרטיות, יש בהן כדי לשפוך אור על הערכים שבבסיסה של הזכות ועל חשיבותה.

עורך הדין האמריקני לואיס ברנדס, לימים שופט בית המשפט העליון בארצות הברית, ועמיתו עורך הדין סמואל וורן הגדירו בשנת 1890 את הזכות לפרטיות כ"זכות להיעזב במנוחה" (the right to be left alone). השניים, שסלדו מכתבות רכילות שפורסמו בעיתונות המקומית עליהם ועל חבריהם, ביקשו ליצור

117 מיכאל בירנהק **פרטיות חוקתית** 25–26 (2023) (להלן: בירנהק **פרטיות חוקתית**).

באמצעות הזכות לפרטיות כלי למניעת חשיפה זו.[118] לפי הגישה התיאורטית שלהם, שכונתה "הגישה המושגית הצרה", הזכות לפרטיות היא אגד של אינטרסים המוגן כבר בדינים אחרים, דוגמת דיני הנזקין או דיני הקניין, ועתה מומשג בנפרד תחת הזכות לפרטיות.[119] אומנם גישה זו מציגה לכאורה גמישות ומכירה באפשרות החפיפה בין מושגים משפטיים מדינים שונים. אולם בד בבד גישה זו אינה רואה כל ערך נוסף בזכות לפרטיות מעבר לאינטרסים המוגנים הפזורים בדינים אחרים, ולפיכך הטעם ביצירת זכות חדשה אינו ברור.[120]

לאימוץ הגישה המושגית הצרה במשפט הישראלי היו תוצאות בעייתיות בכל הנוגע להגנה על הזכות לפרטיות. כך, בפרשת **ועקנין** נבחנה קבילותן של ראיות שהושגו לאחר שנכפה על אסיר לשתות מי מלח, והם גרמו לו להקיא ולפלוט שקיות סמים שבלע קודם לכן. בית המשפט העליון קבע שפעולת הסוהרים הייתה בלתי חוקית לפי דיני העונשין ודיני הנזקין, ועל כן אין צורך לפסוק גם שהיא מפירה את חוק הגנת הפרטיות.[121] בפרשת **ביטון נ' סולטן** בחן בית המשפט אם פרסום תמונתה של גננת בצמוד לכתבה המעלה טענות קשות באשר ליחסה לילדי הגן הוא בגדר פגיעה בפרטיות. בית המשפט העליון קבע שחוק הגנת הפרטיות אינו מגן על השם הטוב, שכן אינטרס זה מוגן במסגרת חוק איסור לשון הרע, ואין מקום ליצור חפיפה העשויה להביא לעקיפה של ההסדרים והאיזונים הקבועים בו. משום כך, השאלה אם פרסום התמונה הוא פגיעה בפרטיות צריכה להיבחן במנותק מתוכן הכתבה עצמה.[122]

118 Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 Ariz. L. Rev. 1 (1979)

119 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 5 Harv. L. Rev. 193 (1890)

120 מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 62 (2010) (להלן: בירנהק **מרחב פרטי**).

121 ד"נ 9/83 **בית הדין הצבאי לערעורים נ' ועקנין**, פ"ד מב(3) 837 (1988); פרופ' בירנהק דן בפרשה בספרו, וראו בירנהק **מרחב פרטי**, **לעיל** ה"ש 120, בעמ' 62–63.

122 רע"פ 9818/01 **ביטון נ' סולטן**, פ"ד נט(6) 554 (2005); פרופ' בירנהק דן בפרשה בספרו, וראו בירנהק **מרחב פרטי**, **לעיל** ה"ש 120, בעמ' 65–66.

גישת הפרטיות כשְׁליטה היא גישה תיאורטית נוספת ומרכזית להמשגתה של הזכות לפרטיות, והיא מכשירה פגיעה בפרטיות במקרה של קבלת הסכמת נושא המידע לפגיעה.[123] לפי גישה זו הזכות לפרטיות משמעה בפועל שליטה אקטיבית של נושא המידע בזרימת המידע עליו בכל שלב בשרשרת הפעולות הקשורות באיסוף המידע ובעיבודו. מאחר שהמידע האישי רב כל כך הוא משקף את נושא המידע עצמו, ועל כן השליטה במידע מעניקה בפועל שליטה בנושא המידע. יתרה מכך, הסיווג והתיוג של האדם לקבוצות אוכלוסייה (למשל קבוצות סיכון או קבוצות צרכניות לפי סגנון חיים) על בסיס המידע הנאסף ומבלי שהאדם יכול להשפיע על הסיווג או לערער על ההחלטה פוגעים באוטונומיה של האדם וביכולתו להחליט עבור עצמו. משום כך נטען כי הבנת הזכות לפרטיות כשליטתו המשפטית של האדם במידע עליו עולה בקנה אחד עם ראיית הזכות לפרטיות כמבוססת על עקרון־העל של כבוד האדם.[124]

העולם המודרני, ובעיקר העובדה שמרביתנו מסכימים לפגיעות בזכותנו לפרטיות מבלי להקדיש לכך כלל מחשבה ותשומת לב, מאתגרים את גישת הפרטיות כשליטה. נטען שהגישה אינה אפקטיבית, שכן על פי רוב קשה מאוד לנושא המידע לשלוט בפעולות הנעשות במידע לאחר איסופו הראשוני, ולעיתים אף קשה לו לשלוט על האיסוף הראשוני של מידע אישי עליו, בעיקר בסביבה דיגיטלית. לעיתים מקור המידע האישי אינו נושא המידע עצמו אלא גורמים אחרים, כגון המדינה או נושאי מידע אחרים. כמו כן, בסביבה דיגיטלית

123 יובל גולדפוס "הפילוסופיה של הפרטיות" 83 **פרלמנט** (2019); סעיף 1 לחוק הגנת הפרטיות, התשמ"א–1981; סעיף 6(a) ל־Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), art 6(a), 2016 O.J. (L 119) 1 (הרגולציה להלן: GDPR). עמדת הפרטיות כשליטה אומצה גם בידי ועדת שופמן, שהסבירה כי "החלטה להגן על המידע היא הכרעה ערכית בה החברה מאפשרת למושא המידע, גם אם אינו בעל החזקה במידע, לבקר את השימושים במידע אודותיו ואף לשלוט בהם"; ראו הצוות לבחינת החקיקה בתחום מאגרי המידע **דין וחשבון** 8 (2007).

124 Alan F. Westin, Privacy And Freedom (1967); בירנהק **מרחב פרטי, לעיל** ה"ש 120, בעמ' 89–99.

פעמים רבות נושא המידע אינו מודע לאיסוף המידע עליו וליכולת לעבד אותו, להצליב אותו ולכרות מתוכו מידע חדש נוסף. עם זאת, נטען כי קושי זה במימוש אפקטיבי של גישת הפרטיות כשליטה נעוץ באופן יישומה הפרקטי של הגישה על ידי מעצבי המדיניות, ואינו מלמד על אי־התאמתה להמשגת הזכות לפרטיות.[125]

ביקורת נוספת על גישת הפרטיות כשליטה מתמקדת בטענה שהגישה ממשיגה את הזכות לפרטיות כזכות קניינית, והקבלה זו מעודדת בפועל את מסחור המידע האישי של נושא המידע, ומכאן את מסחורו של נושא המידע עצמו.[126]

פרופ׳ רות גביזון הייתה מההוגים המרכזיים של תפיסת הפרטיות כגישה. לפי תפיסתה הזכות לפרטיות היא זכות עצמאית המבוססת על יכולתו של אדם למנוע גישה של אחרים אליו בשלושה מישורים: (1) סודיות – הנגישות של אחרים לנושא המידע מבחינתם מודעותם אליו ועליו; (2) הנגישות הפיזית של אחרים לנושא המידע; (3) אנונימיות – המידה שבה נושא המידע מהווה מושא לתשומת ליבם של אחרים.[127] תפיסת הפרטיות כגישה באה לידי ביטוי בחקיקה ובפסיקה בישראל בראיית הזכות לפרטיות כזכותו של הפרט למנוע את הגישה אליו באמצעות האזנה, צילום, פרסום ואמצעים דומים.[128]

גישה תיאורטית נוספת לזכות לפרטיות מכונה "הטענה המושגית המרחיבה". לפי גישה זו יש ערך מוסף בהמשגת הזכות לפרטיות כזכות נפרדת, ואין היא זהה באופן מוחלט לאגד האינטרסים העשוי להיות מוגן בדינים אחרים.

125 ראו הצוות לבחינת החקיקה בתחום מאגרי המידע, **לעיל** ה"ש 123, בעמ' 8–9; בירנהק **מרחב פרטי**, **לעיל** ה"ש 120, בעמ' 89–99.

126 Julie E. Cohen, *Turning Privacy Inside Out*, 20(1) Theoretical Inquiries L. (2019)

127 Ruth Gavison, *Privacy and the Limits of Law*, 89(3) Yale L.J. 421 (1980); רות גביזון "הזכות לפרטיות ולכבוד" **בלי הבדל... זכויות האדם בישראל: קובץ מאמרים לזכרו של ד"ר חמן שלח ז"ל** 61, 68 (1988).

128 הלל סומר, אלעד שרף ותמר שוויצר **הזכות החוקתית לפרטיות** 34 (הכנסת, מרכז מחקר ומידע 2004).

יש לבחון כל מקרה לגופו ובמסגרת זו להתייחס לבסיס העיוני של כל זכות, להצדקות, לתכלית, לערך החברתי המוגן על ידה ולנסיבות המשפטיות, כדי לקבוע את טיב היחס בין שני המושגים המשפטיים – הזכות לפרטיות ואינטרסים העשויים להיות מוגנים תחת דינים אחרים; האם מדובר בחפיפה, ביחס של עיקר וטפל או במקרה של בלעדיות של אחד המושגים? הגישה המושגית המרחיבה אינה חפה מביקורת. ראשית, ההכרה באפשרות קיומה של חפיפה בין מושגים משפטיים מדינים שונים בעייתית כשלעצמה, שכן לעיתים כפילות המונחים המשפטיים עלולה לבלבל ולפגוע בעקרון החוקיות אם מדובר במושגים מתחום המשפט הפלילי. שנית, כאשר מייבאים מושג משפטי מדין אחד לאחר נפגעים האיזון והריסון של הזכות. למשל, עוצמתה של זכות היוצרים מוגבלת מכוח ההגנות הניתנות למשתמשים, דוגמת הגנת שימוש הוגן. כאשר מייבאים את אינטרס שליטת הפרט ביצירותיו לפני פרסומן מדיני זכויות היוצרים אל דיני הפרטיות לא מייבאים את המנגנון הנלווה והמרסן של עוצמת הזכות. בדיני הפרטיות זכות הפרט לשלוט במידע אישי עליו אינה מאוזנת למול אינטרסים מנוגדים, כגון לשון הרע או כבוד האדם.[129]

גישה תיאורטית נוספת מציעה להגדיר את הזכות לפרטיות בהתבסס על זיהוי מצבים הנחשבים לפגיעה בפרטיות וסיווגם לקטגוריות. מקובל להכיר בארבע קטגוריות של פרטיות, בהתאם לסוג הפעילות שבה מדובר: (1) פרטיות במקומות (בבחינת "ביתו של אדם מבצרו"); (2) פרטיות בתקשורת; (3) פרטיות במידע; (4) פרטיות בהחלטות. חוק הגנת הפרטיות מאמץ את גישת הקטגוריות באופן חלקי בהגדירו מקרים של פגיעה בפרטיות, אם כי אלו אינם חופפים לארבע הקטגוריות המקובלות.[130] גם על גישת הקטגוריות של הפרטיות נמתחה ביקורת. למשל, נטען שהגדרת פרטיות במקומות אינה מדויקת, שכן מושא ההגנה של הזכות לפרטיות הוא האדם ולא מקום פיזי, ואין זהות או חפיפה בין זכות הקניין לזכות לפרטיות. כמו כן, ההתמקדות במיקום הפיזי מקשה על בחינת קיומה והיקפה של הזכות לפרטיות מבחינה מהותית במצבי ביניים, למשל פרטיותם של ילדים מול הוריהם, פרטיותה של

129 בירנהק **מרחב פרטי, לעיל** ה"ש 120, בעמ' 65–66.

130 סעיף 2 לחוק הגנת הפרטיות.

מטפלת בילדים או מנקה במקום עבודתה שהוא גם בית מגוריהם הפרטי של מעסיקיה, פרטיותו של אדם בביתו כאשר הבית משמש גם כמקום העבודה או מידת הפרטיות במרחב הציבורי, למשל בזמן שיחה עם הרוקח בבית המרקחת או במלתחה בחדר הכושר.[131]

גם ההבחנה הנהוגה בקטגורית הפרטיות בתקשורת בין תוכן השיחה לנתוני התקשורת שלה, כפי שבאה לידי ביטוי בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ז-2007, ספגה ביקורת לא מעטה בנימוק שהיא אינה תקפה עוד בעידן המידע. יכולות עיבוד וכריית המידע הקיימות כבר כיום מאפשרות להפוך מידע לא מזוהה למזוהה וכך ללמוד על תוכן השיחה והמעורבים בה לפי נתוני התקשורת.[132]

דניאל סולוב הציע בשנת 2008 להגדיר את הזכות לפרטיות בהתאם למענה המשפטי למצבים שונים של פגיעה בפרטיות. הצעתו התבססה על ההבנה שאי־אפשר להעניק לזכות לפרטיות הגדרה אחת אחידה שתספק מענה מתאים לכל פגיעה אפשרית בזכות. יש חפיפה מסוימת בין הצעתו של סולוב לגישת קטגוריות הפרטיות.[133] סולוב מונה ארבע קבוצות של בעיות שעימן הזכות לפרטיות מבקשת להתמודד: איסוף מידע, עיבוד מידע, הפצת מידע וחדירה לחייו האישיים של אדם. בכל אחת מן הקבוצות הוא מונה כמה מצבים: בקטגוריה של איסוף מידע נמנים מעקב וחקירה; בקטגוריה של עיבוד מידע – צבירת מידע, זיהוי על בסיס מידע, אבטחת מידע, היעדר שקיפות כלפי נושא המידע ושימושים אחרים במידע; הקטגוריה של הפצת מידע מורכבת מהפרת אמון, גילוי מידע, חשיפה, הגברת תפוצה של מידע, סחיטה, נטילת זהות ועיוות מידע; ובקטגוריה האחרונה של חדירה לחייו האישיים של אדם נכללים המצבים של פלישה לחייו של אדם או התערבות בהחלטותיו.[134] ככלי משלים להגדרת הזכות לפרטיות בהתבסס על רשימת מצבים של פגיעה בפרטיות,

131 בירנהק **מרחב פרטי, לעיל** ה"ש 120, בעמ' 67-73.

132 **שם**, בעמ' 74-77.

133 **שם**, בעמ' 83-85.

134 Daniel Solove, Understanding Privacy (2008)

הוסיפו סולוב ודניאל סיטרון רשימת נזקים הנגרמים עקב פגיעה בזכות לפרטיות.[135]

הלן ניסנבאום הציעה בשנת 2010 תיאוריה נוספת להמשגת הזכות לפרטיות. לשיטתה, הזכות לפרטיות נלמדת מההקשר: כאשר הפרט מבקש לממש את זכותו לפרטיות אין הוא מעוניין בהגבלת זרימת המידע העוסק בו או בשליטה על מידע זה, כי אם בהבטחה שהמידע המועבר עליו יועבר בצורה ראויה ותואמת להקשר הרלוונטי. לפיכך ניסנבאום מציעה מנגנון שהיא מכנה contextual integrity (להלן: פרטיות הקשרית) אשר יבטיח זרימת מידע ראויה על הפרט בכל תחום מתחומי החיים מבלי להיות תלוי בטכנולוגיה ספציפית, בזמן או במקום. לשיטתה תפיסת הפרטיות ההקשרית תאפשר גם לבחון ולהעריך טכנולוגיות חדשות ולקבוע את המדיניות הנאותה כלפיהן.[136]

לפי גישת הפרטיות ההקשרית, זרימת המידע על הפרט תיבחן ותיעשה לפי הנורמות הנהוגות בתחום שבו מתרחשת זרימת המידע, ואין תחום שבו אין כלל נורמות התנהגות רלוונטיות להעברת מידע. נורמות ההתנהגות הן משני סוגים:

הסוג הראשון הוא נורמות התנהגות של גילוי מידע אישי בהתאם לתוכן המידע. למשל, בביקור אצל רופא נורמת ההתנהגות היא העברת מידע מהחולה לרופא לגבי מצבו הרפואי של המטופל; לפקיד הבנק או לנותן הלוואה נהוג לגלות מידע על מצבנו הפיננסי; לעומת זאת, נורמות ההתנהגות גם קובעות שלא מצופה מעובד לשתף מעביד במידע על נטייתו המינית.

הסוג השני הוא נורמות התנהגות של גילוי מידע אישי בהתאם לקהל היעד. למשל, בהקשר של חברות הנורמה השלטת היא סודיות – חברים מצפים שהמידע שהם מגלים איש לרעהו לא יועבר לצדדים שלישיים ללא אישורם.[137]

135 Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793 (2022)

136 Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010)

137 **שם**, בעמ' 129–131; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79(1) Wash. L. Rev. 119, 138–140 (2004)

כדי להכריע מהי הנורמה השלטת בנסיבות מסוימות, ניסנבאום מציעה להעדיף את הנורמות המשקפות את הסטטוס קוו.[138] אולם הצעה זו היא המוקד לביקורת על תפיסת הפרטיות ההקשרית של ניסנבאום, משום שמשמעותה היא הישענות על מבחן הציפייה הסבירה בקביעת היקפה של הזכות לפרטיות, ומבחן זה אינו מספק מענה במקרה של פרקטיקה חברתית או טכנולוגית חדשה. יתרה מכך, ציפייה סבירה עלולה להיות מוטה כאשר צד חזק, כגון המדינה או מעסיק, יכול לשנות באופן חד־צדדי את הנורמות המכתיבות אותה.[139]

שלל הגישות התיאורטיות לזכות לפרטיות והיעדרה של הגדרה אחידה או קוהרנטית מעידים שמדובר בזכות עמומה ומשתנה, שקשה להמשיגה באופן אחיד וברור.[140] זאת ועוד, בכל אחת מהגישות טמונים קשיים מסוימים. כך, למשל, הגדרת הזכות לפרטיות לפי החלוקה לקטגוריות, כפי שנהוג היום בחוק הגנת הפרטיות,[141] בעייתית נוכח טשטוש הגבולות בין המרחב הפרטי למרחב הציבורי. אף ההתמקדות בפרטיות כגישה, כהצעתה של גביזון, נתקלת בקשיים נוכח התפתחויות טכנולוגיות המאפשרות פגיעה ברמה זו או אחרת באוטונומיה ובמרחב הפרטי של האדם מבלי לחדור פיזית לגוף או למרחב הפיזי, ואף חשיפה של זהות נושא המידע מבלי לעבד מידע אישי שנאסף ממנו עצמו, או אף ללא פרטי מידע מזהים כשלעצמם. גם גישת הפרטיות ההקשרית של ניסנבאום עלולה לרוקן את הזכות לפרטיות מתוכן ככל שהיא נשענת על הסטטוס קוו ועל מבחן הציפייה הסבירה. ואף אימוץ גישת הפרטיות כשליטה נתקל בקשיים אמיתיים נוכח הקושי האופרטיבי בקבלת הסכמה מדעת לכל איסוף, עיבוד או שימוש במידע.

138 **שם**, בעמ' 140–143; Nissenbaum, **לעיל** ה"ש 136, בעמ' 129–131; Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, *in* Privacy, Bid Data, and the Public Good: Frameworks for Engagement 44, 47–49 (Julia Lane et al. eds., 2014)

139 בירנהק **מרחב פרטי**, **לעיל** ה"ש 120, בעמ' 86.

140 בירנהק **פרטיות חוקתית**, **לעיל** ה"ש 117, בעמ' 68.

141 סעיף 2 לחוק הגנת הפרטיות.

עם זאת, עצם הניסיונות הרבים לספק הגנה לזכות לפרטיות יש בו כדי ללמד על חשיבותה. יובל גולדפוס מציע תרגיל מחשבתי המסייע בהבנת חשיבותה ועוצמתה של הזכות לפרטיות. לשיטתו, מידע אישי על אדם אינו נפרד מתודעתו של האדם על עצמו. האדם הוא יצור שהגדרתו אינה ניתנת להפרדה מההקשר הפיזי, החברתי, ההיסטורי או הפוליטי שבו הוא מצוי או נבחן. האדם הוא חלק מהסביבה, והווייתו מכוננת ומשתנה בהתאם לאינטראקציה שלו עם הסביבה. משכך, מידע אישי על אדם אינו פריט לבוש שאפשר לסחור בו. מדובר בחלק אינטגרלי מהאופן שבו האדם מבין את עצמו. לכן, מסחר במידע אישי אינו דומה למסחר בקניין או בטובין אלא מזכיר יותר במאפייניו סחר באיברים, מבחינת חשיבות המידע האישי והשפעתו על הסביבה והאדם – נושא המידע עצמו.[142]

מיכאל בירנהק מציע לבחון את ההצדקות לזכות לפרטיות כדי להבין את מהותה וחשיבותה של הזכות. הוא ממשיג זאת כאוסף מעגלים קונצנטריים, שהפנימי בהם הוא מעגל נושא המידע עצמו – מעגל האדם, וההגנה על הזכות לפרטיות נגזרת מהיחס שבין נושא המידע לאנשים אחרים או לגורמים אחרים במעגלים האחרים. במעגל השני מדובר על ההצדקות לזכות לפרטיות בכל הקשור ביחסים שבין נושא המידע לפרטים אחרים במעגלי קשרים בין־אישיים ומקצועיים. במעגל השלישי מדובר על ההצדקות לפרטיותו של נושא המידע במערכת היחסים שלו עם הקהילה, ובמעגל החיצוני והאחרון מדובר על ההצדקות לפרטיותו של נושא המידע למול המדינה. כל אחד ממעגלי ההצדקות נשען על קודמו ומכיל אותו, והציר המשותף לכל המעגלים הוא תפיסת הפרטיות כשליטה – כיכולתו של נושא המידע לקבוע מה ייעשה במידע האישי עליו.[143]

במעגל הראשון, מעגל האדם, מצויות ההצדקות הקושרות בין הזכות לפרטיות לזכותו של אדם לכבוד, ובין פגיעה בפרטיות לפגיעה בכבוד.[144] הצדקה נוספת

142 גולדפוס, **לעיל** ה"ש 123.

143 בירנהק **פרטיות חוקתית**, **לעיל** ה"ש 117, בעמ' 69–70.

144 Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 1000 (1964)

היא זו הרואה בזכות לפרטיות כלי משפטי וחברתי ליצירת מרחב פרטי פיזי, וירטואלי, אינטלקטואלי ונפשי לכל אדם בהתאם לרצונו והחלטתו. מרחב פרטי זה מבוסס על האדם עצמו, ולא על מקום פיזי שבו הוא נמצא, והוא הכרחי להתפתחות העצמי של האדם ולגיבוש זהותו ותפיסתו העצמית, מבלי שאחרים יפריעו לו לעשות זאת, יבקרו אותו ויהיו שיפוטיים לגביו. כן מוצדקת הפרטיות כאמצעי הגנה על היחיד מפני מבטו החודר והממשטר של האחר.[145]

במעגל השני של הקשרים הבין־אישיים, האינטימיים והמקצועיים, ההצדקה לזכות לפרטיות נובעת מכך שהיא חיונית ליצירת יחידה זוגית, למשל בין בני זוג, בין עורכת דין ללקוח, בין רופאה למטופל או בין פסיכולוגית למטופלת. ביחידה זוגית שכזו יש אינטימיות וחופש משיפוטיות, והיא מוגנת מפני גורמים אחרים (אנשים, תאגידים, תקשורת או רשויות המדינה). כך מכשירה הזכות לפרטיות את הקרקע להבניית אמון בין הצדדים, החיוני ליצירת קשרים אלו ולתחזוקתם, ובה בעת משמרת את המרחב הפרטי של כל אחד מהפרטים ביחידה הזוגית.[146]

ההצדקה לפרטיות במעגל השלישי, מעגל הקהילה, היא כפולה. מחד גיסא, פרטיות היא כלי המסייע בכינונה של קהילה, משום שאדם יכול להחליט באיזו מידה הוא מוותר על פרטיותו ומשתף את הקהילה במידע עליו, כתנאי להצטרפותו לקהילה. מאידך גיסא, פרטיות היא גם ערך חברתי המשותף לכל אחד מהפרטים המרכיבים את הקהילה. כל אחד מהפרטים בקהילה מעוניין במידה כזו או אחרת של פרטיות, ומידת פרטיותו של יחיד בקהילה תלויה במידה רבה בהקשר החברתי שבו הוא נתון ובפרטיותם של אחרים. למשל,

145 Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, *in* Philosophical Dimensions of Privacy: An Anthology 300 (David F. Schoeman ed., 1984); Charles Fried, An Anatomy of Values: Problems of Personal And Social Choice (1970); Robert S. Gerstein, *Intimacy and Privacy*, 89(1) Ethics 76 (1978); Thomas Nagel, *Concealment and Exposure*, 27(1) Phil. & Pub. Affs. 3 (1998); בירנהק **פרטיות חוקתית**, **לעיל** ה"ש 117, בעמ' 70–71.

146 **שם**, בעמ' 75–78.

יחיד המפרסם את תוצאות בדיקת ה־DNA שביצע עשוי לחשוף תוך כדי כך גם מידע אישי על אחיו וילדיו.[147]

מעגל ההצדקות הרביעי והאחרון, מעגל המדינה, מתייחס לתפקידה החשוב של הזכות לפרטיות בהבטחת חשאיות הבחירות וההשתייכות המפלגתית, שהיא הכרחית למשטר דמוקרטי. כמו כן, הזכות לפרטיות כשלעצמה היא אמצעי להגנה על זכויות יסוד אחרות, ובעיקר על הזכות לשוויון ולחופש ביטוי. האנונימיות שמאפשרת הזכות לפרטיות מבטיחה חופש ביטוי גם למי שחושש מלומר את דבריו או מבקש להימנע מדיון וחיטוט בחייו הפרטיים אשר עלול להסיט את הדיון מדבריו לגופם. מידע אישי רגיש כגון נטייה מינית, השתייכות דתית או עמדה פוליטית אינו יכול לשמש בסיס לאפליה, למשל בעת קבלה לעבודה. לבסוף, הזכות לפרטיות מאפשרת לאדם לקבוע, בגבולות החוק, את מידת החודרנות של המדינה למרחב הפרטי שלו, וכך להבטיח את חירותו האישית במדינה.[148]

מעגלי ההצדקות לפרטיות רק מעצימים את הבנת חשיבותה של הזכות לפרטיות למשטר דמוקרטי, לאוטונומיה האישית של כל אחד ואחד, שהיא קריטית לגיבוש הזהות האינדיבידואלית וליכולת להחליט החלטות עצמאיות, ולמימוש זכויות יסוד אחרות, ובראשן הזכות לחופש ביטוי ולשוויון. הבנה זו של חשיבותה של הזכות לפרטיות היא שצריכה להיות בבסיס בחינת הפגיעה בפרטיות בידי המשתמשים בטכנולוגיות דו־שימושיות.

אומנם, בעשור השלישי של המאה ה־21 נחשב השימוש בטכנולוגיות כהכרח חיובי המזוהה עם קִדמה, חדשנות ויעילות. מרבית האזרחים אף מצפים שייעשה שימוש גובר בטכנולוגיות, לרבות טכנולוגיות המבוססות על איסוף ועיבוד מידע אישי בהיקפים גדולים, כדי לייעל את השירות שרשויות השלטון נותנות לאזרח, להקל את התניידותו במרחב הפיזי ולשפר את חוויית הקנייה שלו. במצב זה נתפסת הזכות לפרטיות כחסם מפני חדשנות וקִדמה.[149]

147 **שם**, בעמ' 80.

148 **שם**, בעמ' 80–86.

149 Tal Z. Zarsky, *The Privacy–Innovation Conundrum*, 19 Lewis & Clark L. Rev. 115 (2015)

אולם תפיסה זו היא תפיסה פשטנית המתעלמת מיתרונותיה של הפרטיות כמאפשרת מרחב אישי מוגן להתנסויות והתלבטויות החיוניות כל כך לשגשוגה של חדשנות, כפי שבא לידי ביטוי לעיל בנוגע להצדקות של הזכות לפרטיות.[150] כמו כן, כפי שנסקור בסעיף 5.2.1 להלן, ההתנגשות לכאורה בין טכנולוגיה לפרטיות היא בפועל התנגשות בין זכות חוקתית לאינטרס ציבורי מנוגד שיש לאזן ביניהם, תוך מתן ביטוי לחשיבותו של כל אחד מהם. אין מקום לבטל את הזכות לפרטיות ואת הערכים שבבסיסה בשם החדשנות הטכנולוגית.[151]

חיזוק לטענה שהזכות לפרטיות לא נסוגה או נעלמה כדי לפנות מקום לחדשנות אפשר למצוא בהתנהלותו של מארק צוקרברג, מייסד הרשת החברתית פייסבוק. בשנת 2010 הכריז צוקרברג כי פרטיות אינה נורמה חברתית יותר. לדבריו אז, אנשים מעדיפים את הנורמה החברתית של פתיחות ושיתוף במידע אישי עם אחרים על פני הנורמה החברתית הדועכת של פרטיות.[152] במרץ 2019, לאחר חשיפתם של כמה סקנדלים הנוגעים לזכות לפרטיות, ובראשם קיימברידג' אנליטיקס, שינה צוקרברג את עמדתו. ברשומה שפרסם ברשת החברתית הבהיר צוקרברג שמעתה תדאג פייסבוק לפרטיות משתמשיה. אומנם לשיטתו מדובר בפרטיות מצומצמת בין משתמשים, ולא בין המשתמש לפייסבוק עצמה, אולם ניתן לראות בכך את תחילתה של ההבנה שהזכות לפרטיות אינה נורמה חברתית שחלפה מהעולם.[153]

זאת ועוד, בעולם דיגיטלי נאספות על כל אחד ואחת מאיתנו כמויות בלתי נתפסות של מידע אישי אשר משמשות גופים מדינתיים ומסחריים לבניית פרופילים אישיותיים, פסיכולוגיים והתנהגותיים מדויקים למדי. פרופילים אלה משמשים ליצירת "מלכודות אוטונומיה" המציעות לנושא המידע מגוון

150 Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904 (2013) (להלן: Cohen, *What Privacy*).

151 בירנהק **פרטיות חוקתית**, **לעיל** ה"ש 117, בעמ' 36–37.

152 Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, The Guardian (Jan. 11, 2010)

153 Alex Hern, *Mark Zuckerberg's Privacy Blogpost: What He Did and Didn't Say*, The Guardian (March 7, 2019)

מצומצם של אפשרויות פעולה, כגון האוכל שכדאי להזמין, נתיב הנסיעה שבו מוצע לו לנסוע או הסרט שבו כדאי לו לצפות. אפשרויות פעולה אלו נוצרו בידי מערכת ממוחשבת המנתחת את מאפייני האישיות של נושא המידע בהתבסס על המידע האישי שנאסף עליו, ובפועל הן בגדר ויתור מודע מצד נושא המידע על חלק מתהליכי קבלת ההחלטות האישיים שבעבר היה מבצע בעצמו. אולם אם לא נדע או לא נוכל להציב גבולות, מערכות אלו ימליצו לנו גם מה לחשוב, למי להצביע ובמי להאמין. הסכנה לדמוקרטיה בנסיבות אלו ברורה. ההחלטות מהותיות כבר לא יהיו נתונות באמת בידי הפרט האוטונומי אלא יוכתבו לו, אף מבלי שנתן על כך את הדעת, בידי תאגידים מסחריים או המדינה. תהילה שוורץ אלטשולר סבורה כי כדי למנוע הידרדרות שכזו יש להתייחס לזכות לפרטיות כאל זכות קבוצתית המגינה מפני מלכודות אוטונומיה ומבטיחה שיח ציבורי עשיר ומתפקד החיוני להליך דמוקרטי תקין.[154]

סקירת ההצדקות התיאורטיות לזכות לפרטיות והאיומים החדשים עליה בעקבות המהפכה הדיגיטלית מדגימה ביתר שאת את חשיבותה של הזכות גם כיום, ואת ההכרח להגן עליה כדי להגן על ערכים חשובים וזכויות חשובות אחרות המושפעים ממנה, כגון זכות היסוד לחופש ביטוי, האוטונומיה של הפרט ויכולתו לקבל החלטות באופן עצמאי, וכפועל יוצא – המשטר הדמוקרטי עצמו. סקירה זו תשמש כבסיס לבחינה בפרק הבא של הפגיעה החריפה בזכות לפרטיות עקב השימוש בנוזקות מעקב והשלכותיה על זכויות יסוד, ואף על חוזקתו ועוצמתו של המשטר הדמוקרטי.

154 תהילה שוורץ אלטשולר "פרטיות – מלכת זכויות האדם בעולם דיגיטלי" 83 **פרלמנט** (2019).

פרק 3

תעשיית נוזקות המעקב והפגיעה בפרטיות

בפרק הקודם התחלנו את המסע לבדיקת אפשרות אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות באמצעות סקירה של התיאוריות השונות הממשיגות את הזכות לפרטיות, וכן באמצעות הצגת חשיבותה של הזכות לחופש הביטוי ולהתפתחות האישית, וביתר שאת בעידן הדיגיטלי – לאוטונומיה של הפרט ולהגנה מפני מלכודות אוטונומיה בהקשרים של בחירות והשפעה על תודעה. הצעד הבא בבחינת אימוצה של הדוקטרינה לדיני הגנת הפרטיות, ולנסיבות של נוזקות מעקב באופן פרטני, הוא הבנה של השימושים הנעשים בנוזקות מעקב ושל הפגיעה בפרטיות המתאפשרת באמצעותן. בכך עוסק פרק זה.

3.1. נוזקות מעקב, השימוש לרעה בהן ופגיעתן בפרטיות ובזכויות נוספות

תעשיית נוזקות המעקב המוחדרות למחשב האישי של המשתמש, או ברוב המקרים למכשיר הטלפון הנייד שלו, היא תעשייה גלובלית משגשגת בשווי מוערך של 12 מיליארד דולר שפועלות בה חברות רבות, מרביתן לא מוכרות או ידועות. היא התפתחה כחלק מניצול היתרונות הרבים הטמונים בכך שמרביתנו מחוברים לרשת האינטרנט דרך קבע באמצעות מכשיר הטלפון הנייד. כך הופך המכשיר הנייד לא רק לחלון לעולם עבור המשתמש בו, אלא גם לחלון נוח ביותר לחייו הפרטיים של המשתמש עבור מי שיש להם היכולת והמשאבים לנצל חלון זה.[155]

155 Deibert, **לעיל** ה"ש 6.

בניגוד ליירוט נתוני תקשורת מחברת הטלפוניה והסלולר, המאפשר איסוף נתונים דוגמת מספר הטלפון שיזם את השיחה, יעד השיחה, מיקום המכשיר, תא השטח שבו שהה מבצע השיחה או שממנו נשלחה הודעת טקסט והיסטוריית הגלישה באינטרנט – בדומה לפעילותו של "הכלי" של השב"כ[156] – נוזקות מעקב מנצלות חולשות במכשירי טלפון ניידים של משתמשים מזוהים מראש, אינן מחייבות מעורבות מצד חברות הטלפוניה והסלולר, מאפשרות מעקב אחר מגוון סוגי מידע, מעניקות למפעיליהן גישה מלאה למכשיר הטלפון הנייד של הנעקב וכמעט אינן מותירות עקבות פורנזיים לפעילותן. למשל, נוזקת מעקב יכולה לאפשר למפעילה לשאוב מהמכשיר תמונות, הודעות טקסט, קובצי וידיאו ואודיו, כולל שיחות קוליות, סיסמאות ליישומונים אחרים המותקנים על גבי המכשיר ונתוני מיקום של המכשיר, והכול ללא מגבלה גיאוגרפית. נוזקת מעקב אף מאפשרת להפעיל מרחוק את המיקרופון והמצלמה של המכשיר וכן יישומונים אחרים המותקנים בו.[157]

לכאורה, איסוף המידע האישי באמצעות נוזקת מעקב המותקנת על הטלפון הנייד אינו ייחודי, שכן חברות רבות נשענות כיום על איסוף מידע אישי ושימוש בו לצרכים מסחריים. איסוף המידע האישי מאפשר להן ללמוד על חייו האישיים של המשתמש, קשריו החברתיים, תחביביו ומיקומו הגיאוגרפי, ולהציג לו פרסומות ותכנים מותאמים אישית. שימושים אלו בעייתיים ביותר ובעלי השלכות מרחיקות לכת, שאין להקל בהן ראש, על האוטונומיה של הפרט, על מידת הקשב שלו ואף על עוצמתו של המשטר הדמוקרטי.[158]

156 מעטים האנשים בישראל שיודעים במדויק כיצד פועל ה"כלי" של השב"כ – איזה מידע הוא אוסף, באיזו תדירות וכיצד. אולם לפי תחקיר עיתונאי שבחן את פעולתו של ה"כלי" בתקופת הקורונה, ה"כלי" של השב"כ אוסף נתוני תקשורת מחברות הטלפוניה והסלולר – מספר הטלפון שיזם את השיחה, יעד השיחה, מספר הטלפון שאליו מיועדת השיחה, מיקום המכשיר ותא השטח שבו שהה אחד מהצדדים לשיחה או שממנו נשלחה הודעת טקסט. כמו כן, ה"כלי" אוסף גם את היסטוריית הגלישה באינטרנט של כל אדם בישראל. ראו ברגמן ושברצטור, **לעיל** ה"ש 5.

157 ראו ה"ש 3 **לעיל**.

158 להרחבה בסוגיות אלו ראו, למשל, Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019); מיכה גודמן **מהפכת הקשב** (2021).

ואולם, נוזקות מעקב נבדלות מטכנולוגיות המידע המסחריות במאפיין אחד קריטי – הן עושות זאת ללא ידיעת משתמש הקצה, במחשכים ובהיעדר שקיפות, ומבלי להותיר כמעט עקבות פורנזיים, מה שמקשה על איתורן גם בדיעבד. משום כך, הן ניצבות בצד הקיצוני והחודרני ביותר של סקאלת הפגיעה בפרטיות. פגיעתן בפרטיות היא בוטה וברורה לפי כל אחת ואחת מהגישות התיאורטיות לזכות לפרטיות שנסקרו בפרק הקודם: מדובר בחדירה החותרת תחת שליטתו של נושא המידע במידע האישי עליו, ובכך פוגעת בזכות לפרטיות במובנה כשליטה; היא מאפשרת לאחרים גישה למידע אישי ורגיש ללא ידיעת נושא המידע, תוך פגיעה בסודיות ובאנונימיות, וכך נפגעת הזכות לפרטיות במשמעותה כגישה; באמצעות הפגיעה בזכות לפרטיות מתאפשרת גם פגיעה בזכויות נוספות, כמו הזכות לחופש ביטוי ואף הזכות לחיים; ולבסוף, פגיעתה מתקיימת גם במצבים ובהקשרים הנחשבים מבחינה נורמטיבית כפרטיים.[159]

במחקר זה נתמקד רק בשימוש הנעשה בנוזקות מעקב לשם הגשמת אינטרסים ביטחוניים או פוליטיים. זה שנים יש לסוכנויות ביטחון מדינתיות אינטרס גובר במעקב דיגיטלי. תחילה רק רשויות ביטחון שהיה בידיהן משאבים מספיקים, כמו הסוכנות לביטחון לאומי של ארצות הברית (NSA), יכלו לפתח כלי מעקב מתוחכמים שכאלו. אולם כיום תעשיית נוזקות המעקב מאפשרת גם למדינות שאין בידיהן המשאבים או היכולת הטכנולוגית לפתח נוזקות מעקב מתוחכמות לרכוש רישיון שימוש בכאלו. במשך שנים החזיקה חברת NSO הישראלית בבכורה בשוק נוזקות המעקב, אך בשנים האחרונות ספגה מכה קשה וירדה מגדולתה. פגסוס, מוצר הדגל שלה, הוא נוזקה שאפשר להתקינה מרחוק ובאופן חשאי, במה שמכונה zero click attack, על מכשיר טלפון חכם של יעד המעקב, מבלי שהאחרון ידע או יידרש לבצע כל פעולה לשם כך. הנוזקה מעניקה למפעילה גישה לתכתובת טקסט, תמונות, תכתובת דוא"ל, קובצי וידיאו ורשימת אנשי קשר, וכן גישה לכלל חיישני המכשיר, לרבות

159 Deibert, **לעיל** ה"ש 6.

הפעלה מרחוק של מיקרופון המכשיר והמצלמה שלו, ואף מאפשרת גישה למידע המצוי ביישומונים מוצפנים, כגון תוכנת המסרים המיידיים Signal.[160]

מחקרים שפורמו בשנים האחרונות חשפו שהנוזקה פגסוס שימשה למעקב אחר עיתונאים, פעילי זכויות אדם, מתנגדי משטר, דיפלומטים ופוליטיקאים במדינות שנות במטרה להשתיק כל ביקורת נגד המשטרים במדינות הללו. לאור פרסומים אלה הכניסה מחלקת המסחר האמריקנית (U.S. Department of Commerce) את NSO לרשימה השחורה של חברות שאין לספק להן מוצרים של חברות אמריקניות, ואף הוגשו נגדה כמה תביעות משפטיות בארצות הברית.[161] אולם NSO אינה החברה היחידה בשוק, וידוע כיום על מספר לא מבוטל של חברות המפתחות ומשווקות נוזקות מעקב דומות. קבוצת ניתוח האיומים של גוגל איתרה במאי 2022 כ־30 ספקי נוזקות מעקב למכירה שמוצריהם תקפו מכשירי טלפון ניידים שמותקנת עליהם מערכת הפעלה מסוג אנדרואיד.[162]

בישראל ידוע על פעילותן של חברות נוספות, אם כי לפי דיווחים בתקשורת שוק הסייבר ההתקפי בישראל הולך ומצטמצם בעקבות שינוי במדיניות רישוי

160 Audrey Travere, *The Rise and Fall of NSO Group*, Forbidden Stories (July 19, 2021); Fred Guterl, *Special Report: When Spyware Turns Phones Into Weapons*, Committee to Protect Journalists (Oct. 12, 2022); Rueckert, *Pegasus* **לעיל** ה"ש 1;

161 קונסורציום של 17 ארגוני תקשורת בעשר מדינות שונות, המנוהל על ידי הארגון Forbidden Stories בסיוע תמיכה טכנית של מעבדות האבטחה של ארגון אמנסטי הבינלאומי, הציג מחקרים שלפיהם פגסוס שימשה למעקב אחר עיתונאים, פעילי זכויות אדם, דיפלומטים ופוליטיקאים, בין השאר במקסיקו, אזרבייג'ן, מרוקו, סעודיה והונגריה, למטרות ריגול והשתקת כל ביקורת המאיימת על יציבות המשטרים במדינות אלו. הכנסתה של NSO לרשימה השחורה של חברות שאין לספק להן מוצרים של חברות אמריקניות היא מכה קשה לחברה, שזקוקה בפעילותה השגרתית למעבדי מחשבים, טלפונים וכלי פיתוח המשווקים פעמים רבות על ידי חברות אמריקניות. להרחבה ראו Travere **לעיל** ה"ש 160; Guterl **לעיל** ה"ש 160; Stephen Shankland, *Pegasus Spyware and Citizen Surveillance: Here's What You Should Know*, CNET (July 19, 2022). וכן ראו הדיון בסעיף 4.3.2 **להלן**.

162 Lily Hay Newman, *Spyware Vendors Target Android With Zero-Day Exploits*, Wired (May 19, 2022)

היצוא בשנים האחרונות, וכן בשל הגילויים בתקשורת בנוגע לשימוש פוגעני בנוזקות מעקב בידי משטרים לא דמוקרטיים. כמה מהחברות המוכרות בשוק הישראלי הן Candiru, שהקימו בשנת 2014 שני עובדי NSO לשעבר, ערן שורר ויעקב ויצמן, אך לפי הדיווחים סובלת מקשיים כלכליים; חברת QuaDream, שהוקמה בשנת 2016 בידי קבוצה הכוללת שני עובדי NSO לשעבר, גיא גבע ונמרוד רזניק, והתמקדה בפיתוח ושיווק נוזקת מעקב בשם Reign המוטמעת במכשירי טלפון ניידים. החברה נסגרה באפריל 2023 ולפי פרסומים בתקשורת נוזקת המעקב שלה הייתה בשימוש המשטר בסעודיה; וחברת Paragon, שהוקמה בשנת 2018 בידי יוצאי יחידת מודיעין בצה"ל ושראש הממשלה והרמטכ"ל לשעבר אהוד ברק הוא חבר בדירקטוריון שלה. החברה מפתחת ומשווקת נוזקת מעקב שאינה מיועדת להשגת שליטה מלאה מרחוק במכשיר טלפון נייד אלא לפריצה לתוכנות מסרים מיידיים מוצפנות, ולפי הפרסומים מוכרת את מוצריה לממשל האמריקני.[163] חברות מוכרות אחרות ברחבי העולם הן חברת הסייבר Cytrox מהונגריה, אשר מפתחת ומשווקת את נוזקת המעקב Predator שהוחדרה למכשירי טלפון ניידים מבוססי אנדרואיד במצרים, ארמניה, יוון, מדגסקר, חוף השנהב, סרביה, ספרד ואינדונזיה;[164] חברת הסייבר האיטלקי Hacking Team, שפיתחה ושיווקה את נוזקת המעקב Remote Control System, שלפי הדיווחים שימשה למעקב אחר פעילים למען זכויות אדם ועיתונאים ממדינות שונות. חברת Memento Labs פיתחה על בסיס הטכנולוגיה של Hacking Team את הנוזקות Krait ו־RCS X, המאפשרות חדירה למכשיר הטלפון הנייד של יעד המעקב ללא כל פעולה אקטיבית מצידו, ומעניקות למפעיליהן גישה למגוון הסיסמאות של יעד המעקב, למכלול חיישני

163 ל־Candiru, QuaDream ו־Paragon אין אתרי אינטרנט וכל הידוע עליהן נלמד מפרסומים בתקשורת. ראו Farrow, **לעיל** ה"ש 2; עומר כביר "הסייבר הישראלי מצטמק: מ־18 ל־6 יצרניות רוגלה בתוך שנה" **כלכליסט** (19.4.2023).

164 Newman, **לעיל** ה"ש 162. ביולי 2023 הודיעה מחלקת המסחר האמריקנית על הוספתה של החברה לרשימה השחורה של החברות שאין לסחור עימן, וראו Jarrett Renshaw, David Shepardson & Karen Freifeld, *U.S Adds Two European Surveillance Firms to Export Control List*, Reuters (July 18, 2023)

המכשיר החכם ולכלל המידע המאוחסן בו;[165] וחברת הסייבר האיטלקית RCS Lab,[166] המפתחת ומשווקת את נוזקת המעקב Hermit, שלפי הדיווחים שימשה את ממשלת קזחסטאן, את רשויות אכיפת החוק באיטליה ולדיכוי המיעוט הכורדי בצפון־מזרח סוריה. הנוזקה אינה יכולה לחדור למכשיר הטלפון הנייד של המשתמש ללא כל פעולה אקטיבית מצידו אלא מתחזה ליישומון לגיטימי, אולם מרגע חדירתה למכשיר היא מעניקה למפעיליה גישה מלאה מרחוק לתוכן המכשיר, לחיישניו וליישומונים המותקנים בו.[167]

נוזקת מעקב היא טכנולוגיה דו־שימושית: אפשר לעשות בה שימוש חוקי ולגיטימי, למשל כאשר רשויות אכיפה משתמשות בה למטרות לוחמה בטרור ומניעת פשיעה בהתאם לחוק. עם זאת, שגשוגה של תעשיית נוזקות המעקב, אשר שיפר מאוד את יכולתם של גורמים שונים לעשות שימוש בנוזקות מעקב מתוחכמות, טומן בחובו סכנה לשימוש לרעה בהן תוך פגיעה של ממש בזכויות פרט – ובראש ובראשונה בזכות לפרטיות. הפגיעה בזכות לפרטיות מאפשרת פגיעה חמורה בחופש הביטוי ובזכויות פרט נוספות.[168] ואכן, בשנים האחרונות הצטברו עדויות רבות לשימוש בנוזקות לשם מעקב אחר עיתונאים, פעילי זכויות אדם, מתנגדי משטר, אנשי עסקים וראשי מדינות, על ידי ממשלות בכ־20 מדינות, כגון בחריין, מרוקו, סעודיה, הודו, מקסיקו, הונגריה, אזרבייג'ן, טוגו ורואנדה, חלקן מדינות דיקטטוריות וחלקן דמוקרטיות.

165 בשנת 2015 נחשפה Hacking Team למחקפת סייבר שהובילה לחשיפת השימוש שנעשה בנוזקת המעקב שבפיתוחה בידי משטרים דיקטטוריים בסודן, ערב הסעודית ומצרים באופן הפוגע שלא כדין בזכויות אדם. החשיפה הובילה לנפילתה של החברה, שהצטיירה כמי שמאפשרת למשטרים לדכא את אזרחיהם. בשנת 2016 אף ביטלה רשות היצוא האיטלקית את רישיון היצוא שניתן לחברה ומנעה ממנה למכור את טכנולוגיית המעקב שלה ללקוחות זרים. אולם בשנת 2019 נרכשה החברה על ידי איש הייטק ויזם איטלקי, והוא עשה שימוש בקניינה הרוחני לפיתוח נוזקת מעקב מתוחכמת בחברה שבבעלותו, Memento Labs. ראו Patrick Howell O'Neill, *The Fall and Rise of a Spyware Empire*, MIT Technology Review (Nov. 29, 2019)

166 אתר האינטרנט של RCS Lab.

167 Tera Seals, *Sophisticated Hermit Mobile Spyware Heralds Wave of Government Surveillance*, Dark Reading (Sep. 21, 2022); Guterl, **לעיל** ה"ש 160.

168 Deibert, **לעיל** ה"ש 6; Newman, **לעיל** ה"ש 162.

כך, למשל, קיימות עדויות לכך שהמשטר במרוקו השתמש בנוזקות מעקב נגד עיתונאים ומבקרי המשטר החל משנת 2015. ארגון אמנסטי הבינלאומי מצא שהנוזקה פגסוס הותקנה והופעלה במשך כשנה במכשיר הטלפון הנייד של העיתונאי העצמאי עומר ראדי, ממתנגדיו של מלך מרוקו. ראדי עסק בחקירת הפקעת קרקעות בבעלותו של שבט סביטה לטובת בניית אתרי בידור ווילות יוקרתיות לאליטה הפוליטית והכלכלית במרוקו. בשנת 2022 הוא נעצר, הואשם והורשע בעבירות פגיעה בביטחון הלאומי ואונס ונידון לשש שנות מאסר. ראדי הכחיש כל מעורבות בעבירות, וארגוני זכויות אדם טוענים שהמשטר במרוקו עושה שימוש בעבירות אינוס ובעבירות כלליות של פגיעה בביטחון המדינה ככלי להשתקת ביקורת. אמנסטי מצא שהנוזקה פגסוס גם הוחדרה בשנת 2017 למכשיר הטלפון הנייד של עורך הדין המרוקני עבד אלצאדק אלבושתאוי, שייצג פעילים מתנועת ההתנגדות למשטר ופעילי זכויות אדם. הוא נידון ל־20 חודשי מאסר בגין כמה עבירות, לרבות העלבת עובד ציבור, איום והעלבת מוסדות ציבוריים ותרומה לארגון הפגנות לא חוקיות.[169] גם העיתונאי המרוקני הישאם מנצורי, שברח ממרוקו בשנת 2016 לנוכח איומים משפטיים ואלימות פיזית כלפיו, היה נתון למעקב באמצעות פגסוס במהלך שנת 2021 בעת שחקר את המסחר בסמים בלתי חוקיים בבתי הכלא במרוקו.[170]

השימוש בנוזקת פגסוס אינו ייחודי למשטר במרוקו. בינואר 2016 קיבלה העיתונאית המקסיקנית כרמן אריסטגואי למעלה מ־20 הודעות טקסט הכוללות קישוריות חשודות שהובילו לתוכנת פגסוס, לאחר שפרסמה תחקיר בנוגע לרכושו של נשיא מקסיקו אנריקה נייטו. גם חבריה ובני משפחתה קיבלו הודעות דומות באותה התקופה. עדויות לשימוש בנוזקת המעקב פגסוס נמצאו גם במכשיר הטלפון של העיתונאית מבקרת המשטר חדיג'ה איסמאילובה מבאקו, אזרבייג'ן, לאחר שזו עזבה את מדינתה והיגרה לטורקיה. גם סבולץ' פני (Panyi), עיתונאי הונגרי, היה נתון למעקב במשך 9 חודשים במהלך שנת 2019 באמצעות נוזקת פגסוס שהוחדרה למכשיר הטלפון הנייד שלו. העיתונאי ההודי פאראנג'וי גוהא תקורטה (Thakurta) היה

169 *Morocco: Human Rights Defenders Targeted with NSO Group's Spyware*, Amnesty International (Oct. 10, 2019)

170 Rueckert, *Pegasus*, **לעיל** ה"ש 1.

אף הוא נתון למעקב באמצעות הנוזקה פגסוס במהלך שנת 2018, בעת שחקר את עסקיו של האיש העשיר ביותר בהודו בזמנו, דהירובהאי אמבאני המנוח.[171]

גם צמד עיתונאים עצמאים באל סלבדור, קרלוס ואוסקר מרטינז, אשר ערכו תחקירים ופרסמו דיווחים על כנופיות פושעים הפועלות במדינה וקשריהם עם פוליטיקאים מושחתים, בהם נשיא אל סלבדור נאיב בוקלה, היו נתונים למעקב באמצעות הנוזקה פגסוס. המעקב כלל הקלטה של שיחות שקיימו השניים בנוגע לחקירה ולפרסומה. האחים מרטינז לא היו העיתונאים היחידים שהנשיא עקב אחריהם באמצעות החדרת הנוזקה פגסוס למכשיר הטלפון שלהם. מרכז המחקר הקנדי The Citizen Lab מצא שהמשטר באל סלבדור עשה שימוש בפגסוס נגד מספר רב של אנשי תקשורת ופעילים מהמגזר השלישי בעת שאלו היו מעורבים בחקירות הנוגעות לשחיתות המשטר, לקשריו עם כנופיות פושעים ולשימוש לא ראוי שעשה בקרנות הסעד בתקופת הקורונה.[172]

בספרד, למעלה מ־60 מכשירי טלפון ניידים בבעלותם של אזרחי חבל קטלוניה, בהם פוליטיקאים, עורכי דין ואקטיביסטים הפעילים למען עצמאות החבל, היו מטרות למעקב באמצעות פגסוס. שלושה מהמכשירים שנמצא כי הודבקו בנוזקה פגסוס היו בבעלותם של חברי פרלמנט האיחוד האירופי. הקטלונים סוברים שממשלת ספרד היא שעומדת מאחורי המעקב, וכך גם הציע The Citizen Lab, אשר אישר את דבר המעקב באמצעות פגסוס במכשירים אלו. עובד לשעבר של NSO אף אישר שלחברה יש התקשרות עם ספרד. שיחות עם למעלה מ־40 מהאנשים שהיו נתונים למעקב זה מגלות אווירה של פרנויה וחוסר אמון. יתרה מכך, מרביתם היו המומים לגלות רמה כזו של מעקב במדינה דמוקרטית החברה באיחוד האירופי.[173]

The Citizen Lab חשף עוד שביולי 2020, מכשיר טלפון המחובר לרשת של ביתו הרשמי של ראש ממשלת בריטניה דאז, בוריס ג'ונסון, היה יעד להדבקה באמצעות פגסוס. זהות המכשיר המסוים שהודבק לא נמצאה ועל כן לא ברור

171 **שם.**

172 Rueckert, *"Jaw-Dropping" Targeting*, **לעיל** ה"ש 2.

173 Farrow, **לעיל** ה"ש 2.

כלל מהו המידע שנחשף באמצעות נוזקת המעקב. כן נמצא שמכשירים שהיו מחוברים לרשת של משרד החוץ היו יעד למתקפות מצד פגסוס בחמישה מועדים שונים בין יולי 2020 ליוני 2021. נציגי ממשלת בריטניה אישרו שאכן אותרה מתקפת סייבר באמצעות פגסוס על מכשירים המקושרים לרשת משרד ראש הממשלה ומשרד החוץ. חוקרי The Citizen Lab חושדים שאיחוד האמירויות היא שעומדת מאחורי ההדבקה. מידע זה הבהיר לכול שהשימוש בפגסוס מאיים על הביטחון הלאומי של מדינות דמוקרטיות כגון ארצות הברית ואנגליה. NSO מצידה הצהירה שמדובר במידע שקרי.[174] עוד נחשף בבית משפט בבריטניה שפגסוס שימשה למעקב אחר הנסיכה האיה, אשתו לשעבר של אמיר דובאי מוחמד בן ראשד, שברחה עם שני ילדיה לאנגליה, וכן למעקב אחר עורך דינה.[175]

נמצא גם שהרפובליקה האפריקנית ג׳יבוטי רכשה רישיון שימוש בפגסוס במימון ה־CIA האמריקני למטרת לחימה בטרור, אולם בחקירה שביצעה חברת וואטסאפ נמצא שפגסוס שימשה למעקב אחר חברי ממשלה בג׳יבוטי, לרבות אחרי ראש הממשלה ושר הפנים שלו. אפל מצאה שפגסוס הוחדרה למכשירי אייפון ושימשה למעקב אחר שמונה אנשי ממשל אמריקנים שעבדו בשגרירות ארצות הברית באוגנדה.[176] מייקרוסופט מצאה שחברת Canidru הישראלית הצליחה לחדור למערכת ההפעלה שלה ולהחדיר נוזקת מעקב לתוך מחשביהם האישיים של עיתונאים ואקטיביסטים.[177]

כשנה לאחר פרסום הגילויים על ידי *Forbidden Stories* אישרו חמש מדינות – גרמניה, הונגריה, פולין, ספרד וישראל – שרכשו רישיון שימוש בתוכנת פגסוס. ממשלת בלגיה נמנעה מלאשר זאת אך יש ראיות רבות לכך שגם רשויות אכיפת החוק שלה עושות שימוש בנוזקה. בארצות הברית, ה־NSA וסוכנות הביון המרכזית (CIA) עושות שימוש בנוזקות מעקב משלהן, אך משרד המשפטים ויחידות שונות בצבא רכשו טכנולוגיות מעקב מתוצרת חברות פרטיות. לשכת

174 שם.

175 שם.

176 שם.

177 שם.

החקירות הפדרלית (FBI) אישרה כי נרכש רישיון לשימוש בנוזקה, אך מסרה כי מדובר ברישיון מוגבל ולא נעשה בו שימוש לתמיכה בשום חקירה אלא רק למטרות בחינת מוצרים והערכה.[178]

3.2. סיכום

נוזקות מעקב הן טכנולוגיות דו־שימושיות העשויות לשמש למטרות חוקיות וחשובות, כגון מניעת פשיעה ולוחמה בטרור. כך למשל, נוזקת המעקב פגסוס של חברת NSO סייעה לרשויות במקסיקו לתפוס את ברון הסמים הידוע בכינוי אל צ'אפו, ובאירופה נעשה שימוש בנוזקת המעקב כדי להביא לחשיפתם ומעצרם של חשודים בפדופיליה ביותר מ־40 מדינות.[179] אולם קיימות גם עדויות רבות לשימוש לרעה בנוזקות מעקב המוביל לפגיעה חמורה בזכות לפרטיות ובחופש הביטוי.

אכן, מעקב של ממשלות וארגוני פשיעה אחרי עיתונאים מחשש שאלו יפרסמו תחקירים על שחיתויות ופעולות בלתי חוקיות שלהם אינו דבר חדש. אולם השימוש בנוזקות למעקב אחר טלפונים ניידים הוא עליית מדרגה של ממש ביכולות המעקב, במידת החודרנות של המעקב ובפגיעה בפרטיות שהוא גורם, וכן בהשלכותיו. היכולת לגבש תמונה מפורטת ומדויקת של חייו האישיים של יעד המעקב, לרבות קשריו החברתיים והמקצועיים, דעותיו ומחשבותיו, באמצעות איסוף המידע האישי הרגיש באופן קבוע וחודרני יוצרת אקלים של פחד, פרנויה וצנזורה עצמית, ומהווה איום קיומי על עתיד העיתונות וחופש הביטוי.[180] מקורות חוששים להעביר מידע לעיתונאים, ועיתונאים עצמם חוששים מביצוע תחקירים מסוכנים מחשש לא רק לשלומם הם אלא גם לשלום המקורות שלהם, משפחותיהם וחבריהם. הידיעה שהעיתונאי עשוי

178 Karine Pfenniger, *Pegasus Project: What Has Happened Since the Revelations?* Forbidden Stories (July 18, 2022)

179 Bergman & Mazzetti, **לעיל** ה"ש 4.

180 Farrow, **לעיל** ה"ש 2; Deibert, **לעיל** ה"ש 6.

להיות במעקב גם ללא פעולה אקטיבית מצידו, וללא ידיעתו, באמצעות נוזקה העושה שימוש בחולשת יום אפס כמו פגסוס, יוצרת רמות פרנויה גבוהות בחדרי החדשות ובקרב עיתונאים. העיתונאים חשים חסרי אונים שכן אין בידם כלים להתמודד עם המעקב וההדבקה בנוזקה או למנוע אותם. אין הם יכולים לנקוט משנה זהירות, לעשות שימוש בתוכנות אנטי וירוס או הגנת סייבר שונות או לתקשר באמצעות תוכנות מסרים מוצפנות, שכן הנוזקה עושה שימוש בחולשת יום אפס, אשר במועד ניצולה על ידי הנוזקה ידועה למפתחי הנוזקה בלבד. כמו כן, מרגע החדרתה הנוזקה מקבלת גישה מרחוק לכל תוכני המכשיר, לרבות התכנים מתוכנות מסרים מיידיים מוצפנות, כאשר אלו מופיעים ללא הצפנה במכשיר היעד – בדומה לאדם הקורא את מכתבו של האחר מעבר לכתפו לפני שהאחרון סוגר את המעטפה.[181]

מרבית חברות הטכנולוגיה המפתחות נוזקות מעקב הגיבו באופן דומה לגילויים בדבר שימוש לרעה בנוזקות אשר מוביל לפגיעה חמורה בזכות לפרטיות המאפשרת פגיעות חמורות גם בזכויות יסוד אחרות. לטענתן, הן מוכרות רישיונות שימוש לנוזקות המעקב לרשויות אכיפת חוק מדינתיות בלבד ולמטרות לגיטימיות הקשורות בהגנה על הביטחון הלאומי ומניעת טרור, ואין ביכולתן לדעת מהו השימוש שעושים הלקוחות בפועל בנוזקת המעקב או לפקח עליו.[182] יתרה מזו, חלק מהחברות התרעמו על עצם הפנייה אליהן כנושאות באחריות כלשהי למעשיהם של המשתמשים. כך, למשל, איש ההייטק והיזם האיטלקי פאולו לאזי, שרכש את חברת Hacking Team ופיתח על בסיס קניינה הרוחני את נוזקות המעקב המשווקות בחברת Memento Labs, התרעם מאוד כאשר נשאל כיצד יעלה בידו להבטיח שלקוחותיו לא יעשו שימוש לרעה בטכנולוגיות המעקב. הוא השיב שאיש אינו מפנה תהייה דומה כלפי יצרני אקדחים ורובים, והדגיש שהחברה מפתחת טכנולוגיה מתקדמת לסיוע לרשויות אכיפת חוק.[183] חברות אחרות, ובראשן NSO הישראלית, הוסיפו

181 Guterl, **לעיל** ה"ש 160.

182 ראו, למשל, תגובת חברת הסייבר האיטלקית RCS Lab *Apple and Android Phones Hacked by Italian Spyware, Says Google,* Reuters (June 23, 2022); וכן תגובת NSO הישראלית כמצוטט אצל Farrow, **לעיל** ה"ש 2.

183 O'Neill, **לעיל** ה"ש 165.

והסבירו שהן מוכרות רישיונות לנוזקת המעקב אך ורק לממשלות, למטרות לגיטימיות של לחימה בפשיעה ובטרור, ולא זו בלבד אלא שכל מכירת רישיון נבדקת ומאושרת על ידי המדינה שבה הן רשומות. נוסף על כך, NSO הצהירה כי היא מבצעת מיוזמתה, ומבלי שנדרשה לכך בחוק, בדיקה מקיפה של הלקוח הפוטנציאלי וכן פועלת לפי מדיניות זכויות האדם שאימצה.[184] טענותיה של NSO מדגישות כי נוזקות מעקב הן דו־שימושיות, בדומה למכשיר הווידיאו של סוני: חברת הטכנולוגיה אשר פיתחה את נוזקת המעקב ייעדה אותה לשימוש חוקי, אולם כפי שסקרנו לעיל, בהחלט עשוי להתבצע בה גם שימוש בלתי חוקי.

184 Phineas Rueckert, Cecile Schilis-Gallego, *Hacked: The Story Behind the Israeli Spyware Targeting Moroccan Journalists*, Forbidden Stories (June 22, 2020); Cecile Andrzejewski & Hicham Mansouri, *The Moroccan Cash Machine: Pursuing Omar Radi's Investigation*, Forbidden Stories (Sep. 19, 2022); *Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools*, Amnesty International (June 22, 2020)

פרק 4

אוזלת היד של האסדרה החקיקתית הקיימת של השימוש בנוזקות מעקב – סקירת משפט משווה

בפרק הקודם סקרנו את השימושים לרעה שנעשו בנוזקות מעקב ואת הפגיעה בפרטיות שמתאפשרת באמצעותן. בפרק זה נבחן אם האסדרה הקיימת במשפט הבינלאומי, בארצות הברית, באיחוד האירופי ובישראל נותנת מענה מספק לפגיעה זו בפרטיות. בחינת המענה המשפטי הקיים חשובה לשם הבנת הצורך באימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות ולנסיבות של שימוש לרעה בנוזקות מעקב.

4.1. המשפט הבינלאומי

לקראת סוף המלחמה הקרה הבינו מדינות רבות שיש צורך לפקח על הפיתוח, ההפצה והיצוא של נשק קונבנציונלי ושל טכנולוגיות דו־שימושיות במטרה להתמודד עם הסכנות לביטחון במישור המדינתי והבינלאומי ולהגביר את היציבות בעולם. בהקשר של משטר הפיקוח על יצוא ביטחוני, טכנולוגיות דו־שימושיות הן טכנולוגיות שיש להן שימושים אזרחיים אך בה בעת גם שימושים צבאיים, שעשויים לאיים על השלום העולמי ולעמוד בניגוד לכללי המלחמה הבינלאומיים. הגדרה זאת שונה מזו שעשינו בה שימוש עד כה במחקר זה – עד כה התייחסנו לטכנולוגיות המאפשרות שימושים חוקיים לצד שימושים לא חוקיים, כגון time shifting לצד הפרת זכויות יוצרים בהקשר של דיני זכויות יוצרים, או לוחמה בטרור או בפשיעה לצד פגיעה חמורה בפרטיות בהקשר של נוזקות מעקב ודיני הגנת הפרטיות.

בדצמבר 1995 נחתם הסדר ואסנאר. בתחילה אישרו את ההסדר 33 מדינות, וכיום חתומות עליו 42 מדינות, שבחתימתן הסכימו לשקף בחקיקה המדינתית שלהן את הקווים המנחים שבהסדר לאסדרת היצוא של כלי נשק ומוצרים דו־שימושיים.[185] ההסדר הוא וולונטרי ואינו כולל סנקציות בגין אי־אכיפתו על ידי

185 המדינות המייסדות של ההסדר הן ארגנטינה, אוסטרליה, אוסטריה, בלגיה, בולגריה, קנדה, צ'כיה, דנמרק, פינלנד, צרפת, גרמניה, יוון, הונגריה, אירלנד,

המדינות החברות בו. מטרת ההגבלות הקבועות בהסדר היא לקדם שקיפות ולהגביר את האחריות הנלווית לכל העברה של נשק קונבנציונלי, טכנולוגיות ומוצרים דו־שימושיים. במסגרת זו המדינות הכירו בזכותה של כל מדינה לרכוש אמצעים לגיטימיים להגנתה, אולם אסרו לחלוטין רכישה של נשק קונבנציונלי, מוצרים דו־שימושיים וטכנולוגיות על ידי ארגוני טרור.[186]

הסדר ואסנאר הוא הסדר דינמי. נציגי המדינות החברות נפגשים מדי שנה במה שמכונה המליאה (Wassenaar Arrangement Plenary), המוסמכת להחליט החלטות בנושאים הקשורים להסדר. יו"ר המליאה מתחלף מדי שנה והחלטותיה מתקבלות בהסכמת המשתתפים. המליאה הקימה לאורך השנים גופי משנה האחראים להכנת חומרי רקע והמלצות לקראת הדיונים, וכן לכנס דיונים אד הוק בנושאים הקשורים לתפקוד ההסדר.[187]

בשנת 2013 הוספו לרשימת הטכנולוגיות הדו־שימושיות שבהסכם ואסנאר גם "תוכנות חודרניות" (intrusion software), המוגדרות כתוכנות המיועדות לחמוק מגילוי על ידי כלי ניטור או לעקוף אמצעי הגנה המוטמעים במערכות מחשוב, במטרה לשאוב מידע אישי ממערכות מחשוב, לשנות מידע אישי כאמור או לשנות את פעולותיהן של מערכות מחשוב ולאפשר את הפעלתן מרחוק. לרשימה הוספו גם מערכות מעקב מבוססות פרוטוקול אינטרנט לרשתות תקשורת.[188] מאחר שנוזקות מעקב עונות להגדרה זו של תוכנות

איטליה, יפן, לוקסמבורג, הולנד, ניו זילנד, נורווגיה, פולין, פורטוגל, דרום קוריאה, רומניה, רוסיה, סלובקיה, ספרד, שוודיה, שווייץ, טורקיה, אוקראינה, אנגליה וארצות הברית. בהמשך הצטרפו גם קרואטיה, אסטוניה, הודו, לטביה, ליטא, מלטה, מקסיקו, סלובקיה ודרום אפריקה. ראו *How Many Countries Participate in the Wassenaar Arrangement and When did They Join?* The Wassenaar Arrangement

186 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Guidelines & Procedures, including the Initial Elements, Initial Elements II, Sec. 1 (Dec. 19, 1995) (ההסדר להלן: הסדר ואסנאר).

187 *About Us*, The Wassenaar Arrangement

188 ראו הסדר ואסנאר, **לעיל** ה"ש 186, בחלק Public Document, Volume II, List of Dual-Use Goods and Technologies and Munitions List

חודרניות, מגבלות היצוא הקבועות בהסדר חלות גם עליהן, בהתאם ליישום הקווים המנחים בכל מדינה החברה בהסדר. בין השאר, יצוא של תוכנות חודרניות מחייב קבלת רישיון יצוא מהמדינה, והמדינה בוחנת את מתן הרישיון לפי העקרונות המנחים הקבועים בהסדר.[189] כמו כן, על המדינות לדווח על העברה או סירוב להעברה של מוצרים מהרשימה למדינות יעד שאינן חברות בהסדר. סירובה של מדינה להעניק רישיון יצוא אינו מחייב את שאר המדינות לסרב ליצוא של מוצר זהה מתחומן, אולם מדינה המעניקה רישיון יצוא למוצר הזהה לזה שמדינה אחרת דיווחה כי אסרה על יצואו מחויבת לדווח על כך.[190]

הביקורת המרכזית על הסדר ואסנאר היא שהמגבלות הקבועות בו אינן באות לשרת הגנה על הזכות לפרטיות או על זכויות אדם אחרות, אלא מכוונות כאמור להגברת שקיפות ואחריות בשם היציבות הביטחונית בעולם.[191] הנציב העליון של האו"ם לעניין זכויות אדם אף התייחס בהרחבה בכמה הזדמנויות לחסרונותיו של ההסדר בהקשר של הפגיעה בפרטיות המבוצעת באמצעות נוזקות המעקב והשלכותיה החמורות על חופש העיתונות וחופש הביטוי.[192]

(amended 2013); Elaine Kozark, *Export Controls: The Wassenaar Experience and Its Lessons for International Regulation of Cyber Tools*, *in* Routledge Handbook of International Cybersecurity (Eneken Tikk & Mika Kerttunen eds., 2020)

189 למשל, Best Practice Guidelines for the Licensing of Items on the Basic List and Sensitive List of Dual-Use Goods and Technologies (Agreed at the 2006 Plenary)

190 הסדר ואסנאר, **לעיל** ה"ש 186, בסעיף 4.

191 Collin Anderson, Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies (Access 2015)

192 Rep. of the Office of the U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, at 6–7, U.N. Doc. A/HRC/27/37 (June 30, 2014) (להלן: דוח הנציב העליון 2014); Rep. of the Office of the U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29 (Aug. 3, 2018) (להלן: דוח הנציב העליון 2018); Rep. of the Office of the U.N. High Comm'r for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including Peaceful Protests, U.N. Doc. A/HRC/44/24 (June 24, 2020); Rep. of the Office of the U.N.

אומנם למסקנות הנציב והמלצותיו אין תוקף מחייב, אך יש בהן כדי לשפוך אור על חומרת הפגיעה בפרטיות, הסכנות הטמונות בה לזכויות נוספות, ואוזלת היד הנוכחית של המשפט הבינלאומי בסוגיה.

בשנת 2014 הכיר הנציב העליון של האו"ם לענייני פרטיות בכך שכל איסוף של מידע מתקשורת, לרבות מטא־דאטה (metadata), כלומר כל שימוש באמצעי מעקב אחר תקשורת דיגיטלית, מהווה פגיעה בפרטיות. ואולם, לעיתים תותר פגיעה כאמור בפרטיות כל עוד המעקב אחר תקשורת דיגיטלית נחוץ ויעיל לשם אכיפת חוק או למטרות מודיעין, ונעשה בהתאם לדרישות הדין המקומי והבינלאומי, לרבות האמנה הבינלאומית להגנה על זכויות אדם. כלומר מעקב אחר תקשורת דיגיטלית מותר כל עוד אינו מביא לפגיעה בלתי חוקית או שרירותית בזכות לפרטיות. המבחן הוא מבחן מידתיות ונחיצות: על הפגיעה להיות מידתית לשם השגת מטרתה וכן נחוצה בנסיבות המקרה.[193]

בדוח משנת 2018 התייחס הנציב העליון של האו"ם לענייני פרטיות להחדרת נוזקת מעקב למחשבים אישיים ולטלפונים ניידים, וקבע שחדירה כזו מאפשרת האזנת סתר ואיסוף של כל סוגי התקשורת והמידע, מוצפנים ושאינם מוצפנים, וכן מאפשרת גישה חסויה ומרחוק למכשירים אישיים ולמידע המאוחסן בהם. באופן זה מתאפשר מעקב בזמן אמת על בעל המכשיר וביצוע מניפולציית במידע האגור במכשיר. לשיטתו, פעולות אלו מסכנות לא רק את הזכות לפרטיות אלא גם את הזכות למשפט הוגן, נוכח החשש לפגיעה באמיתות הראיות שיוצגו בפני בית המשפט.[194]

כשנה לאחר מכן, במאי 2019, בחן גם הבודק המיוחד מטעם האו"ם לנושא עידוד הזכות לחופש דעה וביטוי וההגנה עליה את השימוש שעושות מדינות שונות בנוזקות מעקב. לשיטתו, שימוש בנוזקות מעקב עלול להוביל לפגיעה

High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022) (להלן: דוח הנציב העליון 2022).

193 דוח הנציב העליון 2014, **לעיל** ה"ש 192, בעמ' 6–7; International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 (להלן: האמנה הבינלאומית להגנה על זכויות אדם).

194 דוח הנציב העליון 2018, **לעיל** ה"ש 192, בעמ' 6.

של ממש בחופש הביטוי, משום שמדינה העושה שימוש בנוזקה למעקב אחר אדם מסוים עלולה להשתמש במידע שהנוזקה חשפה לשם השתקה והענשה של מבקרי המשטר ומתנגדיו. במדינה שבה שוררת אווירה של מעקב לא חוקי נרחב, לחשש מפני מעקב כאמור עשוי להיות אפקט מצנן על חופש הביטוי. בכך מתח הבודק המיוחד מטעם האו"ם קו ברור בין פרטיות לחופש ביטוי בעידן הדיגיטלי: שמירה על הזכות לפרטיות היא תנאי לחופש ביטוי.[195]

אכן אסדרת השליטה על יצוא טכנולוגיות דו־שימושיות במסגרת הסדר ואסנאר, שעליו חתומות 42 מדינות, הייתה עשויה לספק פתרון יעיל להגנה על זכויות אדם באמצעות מניעה של מכירת נוזקות מעקב למדינות אשר יעשו בהן שימוש לא חוקי ופוגעני בזכויות אדם. אולם הבודק מצא כי בפועל ההסדר אינו מספק פתרון אסדרתי מתאים. ראשית, ההסכם אינו מחייב: על המדינות החתומות להטמיע אותו בחקיקה המדינתית, אך אין בו מנגנון מחייב או אמצעים לאכיפת חובה זו. השימוש הנרחב בנוזקות מעקב אף מוכיח שהמגבלות על היצוא הקבועות בהסדר ואסאנר אינן יעילות. שנית, מטרת ההסדר היא למזער את האיומים על הביטחון המקומי והבינלאומי, והוא אינו מתאים להתמודדות עם הפגיעה של נוזקות מעקב ממוקדות אישית בזכויות אדם. שלישית, אין בהסכם כללים מנחים או אמצעי אכיפה אשר יספקו מענה ישיר לפגיעה בזכויות אדם עקב יצוא של נוזקות מעקב. רביעית, התמודדות עם הפגיעה בזכויות אדם שגורמות נוזקות מעקב באמצעות פיקוח על היצוא מתעלמת מהבעיה המרכזית, שהיא השימוש בנוזקות מעקב לשם דיכוי של ביטוי חוקי ושל מתנגדים או עיתונאים המממשים את זכותם לפרטיות ולחופש ביטוי.[196]

195 Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, at 7–9, U.N. Doc. A/HRC/41/35 (May 28, 2019) (להלן: דוח הבודק המיוחד 2019).

196 **שם**, בעמ' 10.

בדוח משנת 2019 בחן הבודק המיוחד גם אם הכללים המנחים של האו"ם לחברות פרטיות[197] נותנים מענה לסוגיה. לדבריו, כללים אלה אומנם מתווים קווים מנחים לבחינת השאלה אם חברות מתעשיית נוזקות המעקב מכבדות את זכויות האדם של אלו המושפעים מהמוצרים והשירותים שהן מוכרות, אולם בפועל אין הם מספקים הגנה אמיתית לזכות לפרטיות. לפי הכללים, על חברות להטמיע מדיניות המכבדת זכויות אדם; לבצע בדיקת נאותות כדי לזהות, למנוע ולמזער פגיעה של המוצרים והשירותים שהן מוכרות בזכויות אדם, וכן לשאת באחריות לפגיעה כזאת; להיוועץ בקבוצות המושפעות ממוצריהן; לבצע הערכה מתמשכת של יעילות מדיניות הגנת זכויות האדם שלהן; ולהפעיל מנגנון למתן סעד יעיל למי שזכויותיו נפגעו. ואולם, לדעת הבודק, בהתחשב באופייה החשאי של תעשיית נוזקות המעקב והשימוש הנרחב במוצריה למטרות שאינן עולות בקנה אחד עם הדין הבינלאומי להגנה על זכויות אדם, קשה להאמין שהחברות הפרטיות בתעשייה זו באמת נותנות את הדעת להשפעת השימוש במוצריהן על זכויות אדם או עומדות בדרישות המינימום המפורטות בכללים המנחים, ואין לקבל את טענותיהן כי הן אינן יכולות לדעת על השימוש הפוגעני במוצריהן. למשל, חברת Hacking Team אומנם טוענת שלפני כל התקשרות עם לקוח פוטנציאלי היא בוחנת אם קיימות ראיות אובייקטיביות או חששות אמינים לכך שמוצריה ישמשו את הלקוח לפגיעה בזכויות אדם. אולם הבודק המיוחד מטעם האו"ם מצביע על כך שהחברה אינה מסבירה כיצד היא מטפלת במידע שמתקבל אצלה במסגרת בחינת לקוחות שכזו, וכן אינה מזהה באילו זכויות אדם עשויה הנוזקה שלה לפגוע. הבודק המיוחד דחה גם את טענותיה של NSO, שלפיהן היא פועלת לפי המלצותיה של ועדת אתיקה מטעמה הכוללת מומחים חיצוניים מתחומים שונים, לרבות משפטים ויחסים בינלאומיים, ושהיא עשויה לסיים התקשרות עם לקוח אם תמצא שמוצריה משמשים אותו באופן בלתי חוקי. לשיטתו, אף

197 Rep. of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (להלן: הכללים המנחים של האו"ם 2011).

ש־NSO מצהירה שתחקור כל טענה אמינה לשימוש לרעה במוצריה, אין כל אינדיקציה לכך שלראייתה שימוש לרעה כולל גם פגיעה בזכויות אדם.[198]

יתרה מכך, באותו דוח טען הבודק מטעם האו"ם כי גם האמנה הבינלאומית לזכויות אזרחיות ופוליטיות, אשר מחייבת את המדינות לספק לנפגע סעד יעיל ונגיש בגין פגיעה בזכות אדם שלו, לרבות חקירה מיידית מטעם רשויות אכיפת החוק של הטענות לפגיעה בזכות, אינה מספקת הגנה אמיתית ויעילה נגד הפגיעה בזכויות אדם באמצעות נוזקות מעקב.[199] זאת משום שבמרבית המקרים אין פיקוח משפטי על יצוא נוזקת מעקב ולא נפתחת חקירה מקיפה מטעם המדינה בנוגע לשימוש בנוזקת מעקב על ידי ממשלות אחרות. משום כך, מי שפרטיותו נפגעה עקב שימוש בנוזקת מעקב יתקשה להוכיח עילת תביעה נגד החברה המפתחת אותה. במרבית המקרים, בהיעדר לחץ מדינתי ובינלאומי ונוכח מדיניות סודיות המוצדקת מנימוקים של ביטחון הציבור, גם לא יעמוד לרשותו סעד מכוח הדין הבינלאומי. כך, למשל, ארגון אמנסטי פנה למשרד הביטחון בישראל בבקשה לבטל את רישיון היצוא שניתן לחברת NSO, לאחר שאחד מעובדי אמנסטי נפל קורבן לניסיון מעקב באמצעות תוכנת פגסוס. בתגובה סירב משרד הביטחון הישראלי לספק מידע כלשהו על מדיניות מתן רישיונות יצוא או שלילתם, או על רישיון היצוא שבידי NSO, אך ציין שרישיון היצוא שניתן ל־NSO עומד בדרישות הדין הבינלאומי. ארגון Privacy International הגיש לאנשי הקשר הלאומיים של ה־OECD בגרמניה ובאנגליה תלונה בנוגע להפרת כללי ה־OECD בידי חברת Gamma בגין מכירת רישיון שימוש לתוכנת FinSpy לשלטון בבחריין. בגרמניה נדחתה התלונה בנימוק שאין ראיות מספיקות להוכחת מעורבותה של Gamma בבחריין, ואילו באנגליה התקבלה התלונה, נקבע שהראיות מצביעות על כך שנעשה שימוש בנוזקת המעקב של החברה נגד אקטיביסטים בבחריין והוצעו מספר המלצות שמטרתן הגנה על זכויות אדם בהקשר של נוזקת מעקב. אולם אין כל ראיות לכך שחברת Gamma הכירה בהמלצות אלו או יישמה אותן.[200]

198 דוח הבודק המיוחד 2019, **לעיל** ה"ש 195, בעמ' 10.

199 האמנה הבינלאומית להגנה על זכויות אדם, **לעיל** ה"ש 193, בסעיף 2(3).

200 דוח הבודק המיוחד 2019, **לעיל** ה"ש 195, בעמ' 12–13.

עוד מצביע הבודק על נקודה חשובה ובעייתית מבחינת אחריות החברות המפתחות את נוזקות המעקב. לדבריו מתקיים שיתוף פעולה בין גופים ציבוריים לגופים פרטיים בכל הנוגע לתכנון, פיתוח, הטמעה ותפעול של נוזקות מעקב: יחידות פנים־ממשלתיות אינן מצליחות לפתח נוזקות מעקב הממלאות אחר כלל הדרישות הפונקציונליות של ממשלותיהן, ומנגד, לחברות במגזר הפרטי יש תמריץ לפתח טכנולוגיות מעקב העומדות בדרישות אלו ולמכור לממשלות המעוניינות בכך רישיונות שימוש בהן, והממשלות מסייעות בתמורה לחברות בשיפור הנוזקה ושדרוגה בהתאם ללקחי השימוש בה. כמו כן, קיים קשר הדוק בין חברות פרטיות המפתחות נוזקות מעקב לבין הממשלות במדינות שבהן הן פועלות, ואף קיימת תופעה של "דלתות מסתובבות" שבמסגרתה מומחי טכנולוגיה ומעקב מדלגים מהשוק הפרטי למגזר הציבורי ולהפך. במרבית המדינות אין כל אסדרה של תופעה זו.[201]

לפיכך הבודק המיוחד הציע להפסיק באופן מיידי וגלובלי כל מתן של רישיונות יצוא לחברות המפתחות נוזקות מעקב, כל מכירה של נוזקות מעקב המפותחות על ידי חברות פרטיות ומדינות וכן כל מתן רישיונות שימוש או שירותי תמיכה למשתמשים בנוזקות. ההפסקה תעמוד בתוקפה עד שהחברות המפתחות יציגו ראיות משכנעות (1) לכך שהטמיעו אמצעים מספיקים לביצוע בדיקת נאותות טרם התקשרות למתן רישיון שימוש בנוזקת מעקב; (2) לשקיפות במערכת היחסים החוזית עם לקוחותיהן; (3) לאחריותיות שלהן למניעה או למזעור של השימוש בנוזקות המעקב הממוקדות אישית פרי פיתוחן לשם פגיעה בזכויות אדם; (4) ליכולת טכנית להגביל את השימוש בנוזקות המעקב פרי פיתוחן למטרות חוקיות בלבד בהתאם לנורמות ההגנה המקובלות על זכויות אדם, או להגבלת היצוא של נוזקות מעקב רק למדינות שבהן השימוש בטכנולוגיות יהיה מותנה באישור של גוף שיפוט עצמאי וחיצוני לפי חוק ובכפוף להוכחת דרישת הנחיצות והמידתיות. הדרך הטובה ביותר לעמוד בדרישות אלו תהא, לדעת הבודק המיוחד, גיבוש מסגרת להגנה על זכויות יסוד שאותה כינה "עיצוב להגנה על זכויות אדם" (Human Rights by Design) שתוטמע בעת התכנון והפיתוח של נוזקת מעקב. את המסגרת יש לגבש באמצעות רגולציה

201 **שם**, בעמ' 6–7.

שיתופית (co-regulation) תוך התייעצות עם המגזר הפרטי, האקדמיה וארגוני זכויות אדם.[202]

הבודק המיוחד גם המליץ לחייב את החברות המפתחות נוזקות מעקב ליישם את הכללים המנחים של האו"ם להגנה על זכויות אדם על ידי עסקים[203] כתנאי לקבלת רישיון יצוא. במסגרת הכללים הללו על החברות לנקוט את הפעולות שלהלן:

(**1**) לאשר באופן חד־משמעי את אחריותן לכיבוד הזכות לחופש ביטוי, הזכות לפרטיות וזכויות אדם אחרות בעת השימוש בטכנולוגיות שהן מפתחות ומוכרות, ולהתנות כל מכירה, מתן רישיון שימוש או העברה של נוזקת המעקב, וכן מתן שירותי תמיכה בנוזקת מעקב, בציות הלקוח לדין הבינלאומי בנוגע להגנה על זכויות אדם;

(**2**) לבצע בדיקת נאותות לבחינת השפעתה של נוזקת המעקב על זכויות אדם;

(**3**) לאסור במדיניות פנימית של החברה וכן במסגרת חוזי ההתקשרות שלה מתן רישיון שימוש בנוזקת המעקב, העברה שלה או מתן שירותי תמיכה בתפעול ובשימוש בה באופן המפר את החוקים הנוגעים להגנה על זכויות אדם;

(**4**) להטמיע אמצעים ארגוניים או טכנולוגיים המבטיחים הגנה על זכויות אדם – לדוגמה מערכת המזהירה בעת גילוי שימוש לרעה בטכנולוגיה וכפתור הרג (kill switch) שאפשר להפעילו במקרה שמתגלה שימוש לרעה בנוזקת המעקב;

(**5**) לקיים ביקורות שגרתיות המבטיחות שהשימוש במוצרים עומד בדרישות ההגנה על זכויות אדם לפי הדין הבינלאומי, לרבות התחייבות לגלות לציבור ממצאים מרכזיים של הביקורת;

202 **שם**, בעמ' 18–19.

203 הכללים המנחים של האו"ם 2011, **לעיל** ה"ש 197.

(6) ליידע באופן מיידי את הנציג הממשלתי או הבינלאומי הרלוונטי ברגע שמתגלה שימוש לרעה בנוזקת המעקב;

(7) לנהוג בשקיפות באשר ליכולות נוזקת המעקב שהן מפתחות והשירות שהן נותנות, וכן באשר למקרים של שימוש לרעה בנוזקה, ולספק מידע על נתוני המכירה של נוזקת המעקב לרשויות אכיפת חוק או ביון;

(8) להתייעץ כעניין שבשגרה עם מומחי זכויות אדם בנוגע להשפעה האפשרית של נוזקת המעקב על זכויות אדם ובאשר לאמצעים שאפשר להטמיע כדי למנוע או למזער פגיעה בזכויות אדם באמצעותה;

(9) להפעיל מנגנון של תלונות ציבור שבמסגרתו יכול כל מי שרואה עצמו נפגע מנוזקת המעקב לפנות בתלונה בנוגע לפגיעה בזכויותיו, ולהפנות את התלונה לבחינתו של גורם חיצוני לחברה;

(10) להפעיל מנגנון של מתן סעד פיצוי או אחר לנפגע שהבודק החיצוני מצא את תלונתו נכונה.[204]

עוד הציע הבודק לחייב את המדינות להבטיח שיאסדרו את השימוש בנוזקות מעקב בחוק המקומי באופן התואם את דרישות הגנת זכויות האדם בדין הבינלאומי. לשם כך על הדין המקומי לקבוע הוראות ברורות ומפורשות אשר ימנעו פגיעה שרירותית או בלתי חוקית בזכות לפרטיות, בזכות לחופש דעה וביכולת לחפש אחר ידע ומידע ללא גבולות ובאמצעות כל אמצעי תקשורת. בה בעת, הוראות החוק המקומי יאפשרו שימוש בנוזקות מעקב רק ביחס לאדם מסוים וידוע, למטרות חוקיות, כגון מניעה, חקירה או הענשה בגין עבירות פליליות חמורות, ובהתאם לדרישות הנחיצות והמידתיות. כמו כן, בהוראות החוק המקומי ייקבע כי היקף השימוש יהיה מוגבל מבחינת משך הזמן ועומק המעקב, וכפוף לקבלת אישור מראש על ידי גוף עצמאי שיפוטי בהתאם למנגנון ברור וידוע ולתיעוד הליך האישור. עוד נדרש שהחוק המקומי יחייב מתן הודעה למושא המעקב בתנאי שהודעה כאמור לא תסכן את מטרת

204 שם.

המעקב. לבסוף המליץ הבודק המיוחד ששימוש בנוזקות מעקב ממוקדות נגד אנשי תקשורת ייאסר במפורש גם בחוק המקומי.[205]

צעד נוסף שעל המדינות לנקוט, לדעת הבודק המיוחד, הוא הקמה של מנגנון ציבורי בניהול הגוף המדינתי האחראי להגנה על זכויות אדם, אשר יפעל לצד המנגנון המשפטי, לשם אישור השימוש בנוזקות מעקב ופיקוח עליו. בעוד המנגנון המשפטי יעניק אישור פרטני לשימוש בנוזקות מעקב בנסיבות ספציפיות, המנגנון הציבורי יעסוק בבחינה ואישור של רכישת נוזקות מעקב על ידי רשות מרשויות המדינה באמצעות שיתוף הציבור.[206]

הצעד השלישי שעל מדינות לנקוט במסגרת הצעתו של הבודק המיוחד מטעם האו"ם הוא לספק למי שזכותו לפרטיות או לחופש ביטוי נפגעה עקב שימוש בנוזקת מעקב אפשרות אמיתית לתבוע את נזקו מהמדינה, משחקנים שאינם מדינתיים, ובמקרים מסוימים ממדינות זרות בבתי המשפט במדינתו של הנפגע.[207]

כמו כן, הבודק המיוחד הציע לחייב מדינות המעניקות רישיונות יצוא לנוזקות מעקב להצטרף להסדר ואסנאר, וכן למלא את החוסרים שבהסדר בכל הנוגע להגנה על זכויות אדם, באמצעות נקיטת הפעולות שלהלן:

(**1**) היוועצות בקבוצות עבודה אשר יציעו סטנדרטים ליצוא של נוזקות מעקב המביאים בחשבון שיקולים הנוגעים להגנה על זכויות אדם;

(**2**) התניית כל רישיון ליצוא נוזקות מעקב בבחינת הגוף המדינתי האחראי להגנה על זכויות אדם במדינה המייבאת, וכן בציות של החברה מקבלת הרישיון לקווים המנחים של האו"ם להגנה על זכויות אדם;

(**3**) אי־מתן רישיון יצוא אם קיים סיכון ממשי שנוזקות המעקב ישמשו לפגיעה בזכויות אדם, או אם אין במדינה שאליה מתבקש היצוא מסגרת משפטית

205 דוח הבודק המיוחד 2019, **לעיל** ה"ש 195, בעמ' 15.

206 **שם**, בעמ' 16.

207 **שם**, בעמ' 16–17.

לאסדרת השימוש בנוזקות המעקב התואמת את הדין הבינלאומי להגנה על זכויות אדם;

(**4**) הקפדה על שקיפות במתן רישיון היצוא כדי להבטיח פיקוח וביקורת ציבורית.[208]

גם בשנת 2020 פרסם האו"ם דוח על השימוש בנוזקות מעקב. הפעם בחן הנציב העליון של האו"ם לענייני זכויות אדם את הפגיעה בזכות ההתארגנות וההפגנה בעקבות השימוש שעושות מדינות בנוזקות אלה למעקב אחר תקשורת דיגיטלית. הנציב העליון קבע שעל החברות הפרטיות המפתחות נוזקות מעקב להגן על זכויות אדם כחלק מהמדיניות המוצהרת שלהן. במסגרת זו עליהן לבצע בדיקת נאותות כדי לזהות, למנוע ולמזער את הפגיעה של הטכנולוגיה שפיתחו בזכויות אדם, וכן לספק הסבר על האופן שבו הן עושות זאת. נוסף על כך, מצופה מהחברות לגבש מדיניות לטיפול בהשלכות השליליות על זכויות אדם הנגרמות על ידן או שהן תורמות להן, ולפעול לפי מדיניות זו. בה בעת, על המדינות להבטיח שהשימוש שהן עושות בנוזקות מעקב מותאם לחוק הבינלאומי ועומד בדרישות הנחיצות והמידתיות. עוד קרא הנציב העליון למדינות להטיל מגבלות יצוא ולמנוע מכירת נוזקות מעקב כאשר יש אינדיקציה לכך שהן תשמשנה למעקב באופן הפוגע בזכויות אדם.[209]

בשנת 2022 פרסם הנציב העליון לענייני זכויות אדם של האו"ם דוח נוסף אשר עסק במפורש בנוזקות מעקב דוגמת פגסוס של חברת NSO. הנציב העליון קבע שהחודרנות של נוזקה כזו מאפשרת לגבש תמונה מפורטת על חיי קורבן המעקב, מחשבותיו, העדפותיו, פעילותו המקצועית, השקפותיו הפוליטיות, מצבו הכלכלי, הבריאותי והחברתי ויחסיו האינטימיים. לשיטתו, בכך פוגעת הנוזקה פגיעה אנושה בזכות לפרטיות ובזכויות נוספות, כגון הזכות לחופש דעה ומחשבה. החדרת הנוזקה למכשירי טלפון ניידים של עיתונאים גם פוגעת בחופש העיתונות ויוצרת אפקט מצנן על חופש הביטוי, ובסופו של דבר פוגעת במשטר הדמוקרטי. כמו כן, מאחר שנוזקת מעקב מאפשרת גם שתילה או

208 **שם**.

209 **שם**, בעמ' 11.

שינוי של ראיות באמצעות החדרת מידע או שינוי מידע המאוחסן במכשיר הנייד, יש בשימוש בה משום פגיעה אפשרית בזכות למשפט הוגן. הפגיעה אינה מוגבלת לזכויותיו של יעד המעקב בלבד אלא עשויה להוביל לפגיעה באנשים שעימם היה בקשר ואף באנשים שהיו בסביבתו הפיזית, אם נעשה שימוש במצלמת המכשיר או במיקרופון שלו. זאת ועוד, מאחר שנוזקה דוגמת פגסוס מותקנת במכשיר הנייד ללא צורך בפעולה אקטיבית כלשהי מצד קורבן המעקב, במה שמכונה zero click attack, מרגע שהוחלט כי אדם מסוים יהיה יעד למעקב הוא אינו יכול למנוע את חדירתה למכשיר הנייד שלו.[210]

הסכנה הברורה לפגיעה בבסיסה של הזכות לפרטיות ופוטנציאל הפגיעה בחופש הביטוי והמחשבה הובילו את הנציב העליון להמליץ, בדוח משנת 2022, כי השימוש בנוזקות מעקב יוגבל רק למטרה לגיטימית ויעמוד בדרישות החוק הבינלאומי בנוגע לזכויות אדם, לרבות עקרונות החוקיות, הנחיצות, המידתיות והאי־אפליה. עמידה בדרישות אלו מחייבת שהשימוש בנוזקת מעקב ייעשה אך ורק לשם מניעה או חקירה של פשע רציני מסוים או של פעולה המאיימת איום חמור על הביטחון הלאומי, יתמקד במעקב אחר החשודים בביצוע ובתכנון מעשה כאמור, בהיקף ולתקופה מוגדרים ומוגבלים, ויינקט כמוצא אחרון – כלומר השימוש בנוזקת מעקב ייעשה רק לאחר שכל שאר האמצעים העומדים לרשות רשויות אכיפת החוק במדינה נוסו ונכשלו. כמו כן, הנציב המליץ שהשימוש בנוזקת מעקב יהיה מותנה באישור מקדים של רשות שיפוטית, שרשויות אכיפת החוק ייחשפו רק למידע הרלוונטי עבורן מתוך שפע המידע שנוזקת מעקב מנגישה, ושהשימוש בפועל בנוזקה יהיה כפוף לפיקוח חיצוני עצמאי. המלצה נוספת היא שכל מדינה תאמץ מדיניות יצוא קפדנית ושקופה המונעת מכירת רישיונות שימוש בנוזקת מעקב כאשר קיימות אינדיקציות לכך שייעשה בהן שימוש הפוגע בזכויות אדם, ושכל מדינה תבצע בדיקת נאותות מערכתית ותקופתית שבמסגרתה תיבדק ההשפעה של הטכנולוגיה המתוכננת, המפותחת, הנרכשת או המיושמת בתחומיה על זכויות אדם. בעת בדיקת הנאותות יש להביא בחשבון את המצב המשפטי שבו הטכנולוגיה אמורה להיות מיושמת, לרבות הסיכון של שימוש לרעה בה אם המשטר הפוליטי יוחלף. עוד המליץ הנציב על הטמעת חקיקה מקיפה להגנה על הזכות

210 דוח הנציב העליון 2022, **לעיל** ה"ש 192, בעמ' 17–18.

לפרטיות על ידי רשות עצמאית וחזקה, על הגברת שקיפות השימוש בנוזקות מעקב ועל עידוד שיח ציבורי בנוגע ליתרונות ולחסרונות שבשימוש בנוזקות מעקב בידי רשויות הביון ואכיפת החוק במדינה. כן המליץ הנציב להבטיח מתן סעדים מתאימים למי שזכויותיהם נפגעו עקב השימוש בנוזקות מעקב. לבסוף חזר הנציב העליון לזכויות אדם של האו"ם על המלצתו של המבקר המיוחד של האו"ם[211] להימנע מכל מכירה או העברה של נוזקות מעקב וכן מכל שימוש בהן עד לחקיקתו של משטר המגן על זכויות אדם.[212]

בדצמבר 2021 השיקו אוסטרליה, דנמרק ונורווגיה, בהנהגת ארצות הברית, יוזמה חדשה בשם Export Controls and Human Rights Initiative.[213] במסגרת יוזמה זו גיבשו המדינות במשותף קוד התנהגות וולונטרי להטמעת שיקולי זכויות אדם במדיניות מתן רישיונות יצוא. אלבניה, בולגריה, קנדה, קוסטה ריקה, קרואטיה, צ'כיה, אקוודור, אסטוניה, פינלנד, צרפת, גרמניה, יפן, קוסובו, לטביה, הולנד, ניו זילנד, צפון מקדוניה, נורווגיה, דרום קוריאה, סלובקיה, ספרד ואנגליה הביעו גם הן תמיכה בקוד ההתנהגות.[214] קוד ההתנהגות הוא תוספת למשטר הפיקוח על היצוא הבינלאומי הקיים, ומטרתו להתוות מחויבות פוליטית ליישום הגבלות על היצוא שיבטיחו שהשימוש שייעשה בטובין ובטכנולוגיות מעקב יעמוד בדרישות הדין הבינלאומי בכל הקשור להגנת זכויות אדם, ושלא ייעשה בהם שימוש לרעה כדי לפגוע שלא כחוק או בשרירותיות בזכות לפרטיות או להפר משמעותית זכות אדם אחרת.

המדינות החתומות על קוד ההתנהגות התחייבו לבצע את הפעולות שלהלן:

211 Press Release, Office of the High Commissioner for Human Rights, Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Techn (Aug. 12, 2021)

212 דוח הנציב העליון 2022, **לעיל** ה"ש 192, בעמ' 3-6.

213 Press Release, The White House, Joint Statement on the Export Controls and Human Rights Initiative (Dec. 10, 2021)

214 Press Release, U.S. Department of State, Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy (March 30, 2023)

(**1**) לנקוט מאמצים כדי להבטיח שהחוק המקומי מתאים ומעודכן לשם שליטה על יצוא של טכנולוגיות דו־שימושיות אשר עשויות לשמש לרעה למטרות של הפרה חמורה של זכויות אדם;

(**2**) ליצור שיתופי פעולה עם המגזר הפרטי, האקדמיה, חוקרים, אנשי טכנולוגיה וארגוני חברה אזרחית לשם התייעצות בנושאים הקשורים ביישום יעיל של אמצעי פיקוח על היצוא;

(**3**) לשתף את המדינות האחרות במידע על איומים וסיכונים הטמונים בטכנולוגיות דו־שימושיות;

(**4**) לשתף, לפתח וליישם שיטות עבודה מומלצות (best practices) בנוגע להיבטים שלהלן: שליטה על היצוא של טכנולוגיות דו־שימושיות העשויות לפגוע בזכויות אדם למדינות ולשחקנים שאינם מדינתיים; קבלת אישור מהגורמים שאליהם מיוצאות הטכנולוגיות שלפיו לא ייעשה בהן שימוש לרעה; יצוא מחדש או העברה באופן העשוי לאפשר הפרה של זכויות אדם; ושיתוף במידע הרלוונטי לרשויות הפיקוח על היצוא כדי להעריך את הסיכון שהטכנולוגיות המיוצאות ישמשו להפרת זכויות אדם;

(**5**) להתייעץ עם התעשייה ולקדם יישום של מדיניות הגנה על זכויות אדם בהתאם לקווים המנחים של האו"ם לעסקים בנושא גם על ידי שחקנים שאינם מדינתיים;

(**6**) לעודד מדינות נוספות להצטרף לקוד ההתנהגות או לפעול לפיו.[215]

יוזמת קוד ההתנהגות היא יוזמה חדשה, וקשה להעריך כבר עכשיו את יעילותה והשלכותיה. עם זאת, העובדה שמדובר בקוד התנהגות וולונטרי שיישומו תלוי ברצונן הטוב של המדינות ושאין כל אמצעים לאכיפת החובות הקבועות בו עשויה להעיד שהשפעתו תהיה מוגבלת.

215 Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights (2023)

4.2. האיחוד האירופי

4.2.1. חקיקה

המענה המשפטי של האיחוד האירופי לפגיעה האפשרית של נוזקות המעקב בזכויות אדם מורכב מכמה דברי חקיקה העוסקים בהיבטים שונים הנוגעים להן: יצואן ממדינות החברות באיחוד האירופי למדינות אחרות, הגנה על אזרחי האיחוד מפני נוזקות אלה והשימוש האפשרי בנוזקות מעקב בידי רשויות אכיפת חוק באירופה.

4.2.1.1. יצוא: רגולציית המוצרים הדו־שימושיים

רגולציית המוצרים הדו־שימושיים באיחוד האירופי מחייבת קבלת רישיון ליצוא של מוצרים דו־שימושיים המנויים ברגולציה, ובהם נוזקות מעקב.[216] בבחינת הענקת הרישיון על המדינות החברות לתת את הדעת לכיבוד זכויות אדם לפי הדין הבינלאומי במדינות היעד, וכאשר קיים סיכון ברור לדיכוי פנימי במדינת היעד יש להימנע ממתן רישיון יצוא.[217]

בנובמבר 2020 עודכנה רגולציית המוצרים הדו־שימושיים וגם נוזקות מעקב חויבו בקבלת אישור ליצוא. וכך, יצוא של מוצרי סייבר המשמשים למעקב, שסביר שייעשה בהם שימוש לדיכוי פנים־מדינתי או להפרה של זכויות אדם ושל הדין ההומניטרי הבינלאומי, חייב בקבלת אישור בהתאם לרגולציה.[218] בבחינת

216 Council Regulation 428/2009, Annex I, art. 3(1) juncto category 4A005, 4D004, 4E001(c), 2009 O.J. (L 134) 1 (EC); Amnesty International et al., Operating from the Shadows: Inside NSO Group's Corporate Structure 20 (31 May 2021); O.L. van Daalen et al., The New Rules for Export Control of Cyber-Surveillance Items in the EU 48-50 (Institute for Information Law 2021); Anderson, **לעיל** ה"ש 191.

217 Council Common Position 2008/944/CFSP, art. 2(2), 2008 O.J. (L 335) 99 (EU); למידע נוסף ראו Council of the European Union, User's Guide to Council Common Position 2008/944/CFSP, Council Doc. 10858/15 (July 20, 2015)

218 Council Regulation 2021/821, 2021 O.J. (L 206) 1 (EU).)

מתן אישור היצוא על הרשות האחראית לבחון את השפעת נוזקת המעקב הנדונה על זכויות אדם. במסגרת עדכון הרגולציה הורחבו גם דרישות הגילוי באופן העשוי להביא לחשיפת מכירת נוזקות מעקב על ידי חברות המבוססות במדינות האיחוד למשטרים דיקטטוריים ברחבי העולם.[219] עם זאת, הרגולציה על מוצרים דו־שימושיים יושמה באופן חלקי בשל הקושי להעריך את ההתייחסות לזכויות אדם במדינת היעד, עקב העדפת אינטרסים לאומיים, כלכליים וביטחוניים, או לנוכח שליטה מוגבלת על השימוש הנעשה בפועל בתוכנות שניתן לגביהן רישיון יצוא.[220]

4.2.1.2. הגנה על משתמש הקצה: הצעת חוק חוסן הסייבר

בספטמבר 2022, כשנתיים לאחר עדכון רגולציית המוצרים הדו־שימושיים, הוצגה הצעת חוק חוסן הסייבר. ההצעה אושרה בפרלמנט האירופי במרץ 2024 ועתה ממתינה לאישורה הסופי במועצת האיחוד האירופי.[221] ההצעה נועדה לשפר את הגנת הסייבר ולהעלות את מודעות הצרכנים לאיומי סייבר ולרמת הגנת הסייבר של המוצרים שהם רוכשים,[222] וכן ליצור מסגרת מקיפה ואחידה להגנת סייבר על מוצרים חכמים באיחוד האירופי,[223] וכך למזער את הסיכון שמכשירים חכמים יותקפו ותתוקן עליהם נוזקת מעקב.

219 Milderbrath, **לעיל** ה"ש 3, בעמ' 26.

220 **שם**.

221 *Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirement for Products with Digital Elements and Amending Regulation*, COM (2022) 454 final (Sep. 15, 2022) (להלן: הצעת חוק חוסן הסייבר); European Parliament Resolution of 12 Mar. 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements, Eur. Parl. Doc. P9_TA(2024)0130 (2024)

222 הצעת חוק חוסן הסייבר, **לעיל** ה"ש 221, בסעיף הקדמה 1.

223 **שם**, בסעיפי הקדמה 3–4.

לשם הגשמת מטרות אלו, הצעת החוק מגדירה קריטריונים אובייקטיבים וניטרליים מבחינה טכנולוגית להגנת הסייבר ב"מוצרים בעלי רכיבים דיגיטליים",[224] שהשימוש המיועד שלהם, והצפוי באופן סביר, כולל תקשורת לצורך העברת מידע באופן ישיר או עקיף, פיזי או אלחוטי, למכשיר אחר או לרשת. הצעת חוק החוסן אינה חלה על מוצרים שהגנת הסייבר בהם מאוסדרת בחקיקה ספציפית, כמו מוצרים רפואיים, מוצרי תעופה או כלי רכב. כן מוחרגים מתחולת הצעת החוק מוצרים חכמים המפותחים באופן בלעדי למטרות ביטחון לאומי או למטרות צבאיות, ומוצרים שמתוכננים באופן ייחודי להעברת מידע חסוי.[225]

במסגרת תנאים אובייקטיבים וניטרליים טכנולוגית אלו, הצעת חוק חוסן הסייבר כוללת, בין השאר, דרישות סף להגנת סייבר לאורך כל חיי המוצר – בשלבי העיצוב, התכנון, הפיתוח והייצור של המוצר, בעת שיווק לצרכנים וכן לאורך כל חיי המוצר בשוק או חמש שנים מהחדרתו לשוק, המוקדם בהם. דרישות סף אלו כוללות חובת ביצוע סקר סיכוני סייבר והתחשבות בתוצאות הסקר לאורך כל שלבי הפיתוח, הייצור, השיווק והתמיכה במוצר בשוק, חובות הנוגעות לפיתוח עדכוני תוכנה למוצר עם גילוי וזיהוי חולשות בו, וחובות דיווח בנוגע לחשיפת חולשות ולמתקפות סייבר. חשיפת החולשות תדווח הן לרשויות המתאימות, כדי שאלה יעריכו אם נדרשים צעדים מדינתיים ואם יש להגביר את רמת הגנת הסייבר בקרב מגזרים קריטיים, והן למשתמשים, כדי שיוכלו להתנהל באופן המגן על ביטחונם וזכויותיהם.[226] הצעת חוק החוסן מבהירה גם שהגנה על מידע אישי באמצעות עיצוב לפרטיות כבר משלב העיצוב והתכנון של המוצר ולאורך כל חייו היא רכיב חשוב בהגנת סייבר ובמניעת סיכוני סייבר.[227]

224 "מוצר בעל רכיבים דיגיטליים" (product with digital elements) מוגדר ככל מוצר תוכנה או חומרה ופתרונות עיבוד מידע מרחוק המוטמעים בו, לרבות רכיבי תוכנה או חומרה המשווקים בשוק בנפרד. ראו **שם**, בסעיף 3(1).

225 **שם**, בסעיף 2.

226 **שם**, בסעיף הקדמה 35.

227 **שם**, בסעיף הקדמה 17.

עוד כוללת הצעת חוק חוסן הסייבר כללים בנוגע למעקב אחר הציות של גורמי השוק להוראות הצעת החוק וכן כללים לאכיפת ההוראות.[228] על יצרן לבצע, בעצמו או באמצעות חברה חיצונית, הערכת ציות לדרישות הקבועות בהצעת החוק ולקבל אישור הגנת סייבר. בכך מטילה הצעת חוק החוסן על יצרני המוצרים, בכל שלבי שרשרת האספקה, החל מהיצרן ועד למשווק, את האחריות להבטיח ציות לדרישות האבטחה של מוצריהם, בהתאם לתפקיד שלהם בשרשרת האספקה. הגברת נטל האחריות על היצרנים תועיל לציבור המשתמשים, לאזרחים ולעסקים משום שהיא תוביל להגברת השקיפות בנוגע להיבטי הגנת סייבר, תעודד אמון במוצרים חכמים ותבטיח הגנה טובה יותר על זכויות יסוד, לרבות הזכות לפרטיות. יבואן של מוצרים בעלי רכיבים דיגיטליים מחויב גם כן להוכיח שהיצרן ציית לכלל הדרישות הקבועות בהצעת חוק החוסן טרם החדרת המוצר לשוק. חברה המוכיחה ציות לדרישות החיוניות הקבועות בהצעת חוק החוסן תזכה לאישור בדמות סימון האותיות CE על גבי המוצר. סימון זה הוא תנאי לשיווקו של המוצר בשוק האירופי,[229] ועל מפיץ מוצרים בעלי רכיבים דיגיטליים לוודא שהמוצרים קיבלו את האישור הנדרש לשם הצגת סימון זה.[230] כך יוצרת הצעת חוק החוסן מתווה אשר יאפשר לצרכנים לשקול שיקולים הנוגעים לרמת הגנת הסייבר במוצר בעת רכישת מוצר בעל רכיבים דיגיטליים.[231]

מוצרים המנויים בתוספת השלישית להצעת חוק החוסן יהיו כפופים לדרישות הגנת סייבר מחמירות יותר. מדובר במוצרים בעלי מאפיינים דיגיטליים שנחשבים מוצרים קריטיים מבחינת הנזק שחולשת סייבר בהם עלולה לגרום, בהינתן התעשייה שבה הם פועלים. יצרניהם של מוצרים אלו יהיו כפופים להערכת ציות מחמירה יותר, ונציבות האיחוד האירופי אף מוסמכת להתקין תקנות ייעודיות אשר יפרטו קטגוריות של מוצרים קריטיים ביותר, בהתאם לסוג הלקוחות העושים שימוש במוצרים אלו ולהערכת הסיכון הצפוי

228 **שם**, בסעיף 1.

229 **שם**, בעמ' 1–2, 9, ובסעיף הקדמה 20.

230 **שם**, בסעיפי הקדמה 1–6, 17–20, 35–37, 43–44, 65, ובסעיפים 10–11, 13–14.

231 **שם**, בסעיפי הקדמה 2, 6.

לאינטרסים חיוניים בשל מתקפת סייבר עליהם. למשל, אם תשתית חיונית נשענת על קטגוריות מוצרים מסוימת, מוצרים מקטגוריה זו ייחשבו קריטיים במיוחד ויצרניהם יחויבו בדרישות המחמירות הקבועות בתוספת הראשונה להצעת החוק כתנאי לקבלת אישור להגנת הסייבר שלהם.[232]

אי־עמידה בדרישות הסף הקבועות בהצעת חוק החוסן חושפת את היצרן, היבואן או המפיץ לקנסות מינהליים, אך גם לתביעות מצד צרכנים שנגרם להם נזק עקב מתקפת סייבר על המוצר. זאת משום שהצעת חוק החוסן מגדירה את דירקטיבת האחריות למוצרים פגומים, המטילה על היצרן אחריות מוחלטת לכל נזק שנגרם למשתמש במוצר לא בטוח,[233] כדירקטיבה משלימה מבחינת אחריות היצרן. בשל שילוב זה של הצעת חוק חוסן הסייבר עם דירקטיבת האחריות למוצרים פגומים יהיה אפשר, למשל, להטיל אחריות מוחלטת על יצרן שלא ביצע עדכוני אבטחה למוצר חכם לאחר החדרתו לשוק, כנדרש לפי הצעת חוק חוסן הסייבר, ומשום כך המשתמשים במוצר נפלו קורבן למתקפת סייבר ונגרם להם נזק.[234]

הצעת חוק החוסן מתייחסת גם למקרים שבהם יש לרשויות אכיפת החוק המדינתיות בסיס סביר לחשד כי מוצר חכם מציב איום סייבר משמעותי, לרבות באופן התמודדותו עם חולשות. במקרה כזה יש לרשות המדינתית סמכות לבצע הערכה של מידת הציות של המוצר לדרישות הצעת חוק החוסן, ויצרן המוצר מחויב לשתף פעולה עם בחינה שכזו. אם במהלך ביצוע ההערכה הרשות המדינתית מגלה שהמוצר החכם אינו עומד בדרישות הצעת חוק חוסן הסייבר, בסמכותה לדרוש מיצרן המוצר לנקוט ללא דיחוי את כל הצעדים המתקנים המתאימים כדי לעמוד בדרישות, להוציא את המוצר מהשוק או לדרוש את החזרתו מהמשתמשים והמפיצים בתוך תקופת זמן סבירה, בהתאם למידת

232 **שם**, בעמ' 9–10.

233 Directive 85/374 of the European Parliament and of the Council of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products, 1985 O.J. (L 210) 29

234 הצעת חוק חוסן הסייבר, **לעיל** ה"ש 221, בסעיפי הקדמה 1–6, 17–20, 35–37, 43–44, 65.

הסיכון הגלום בו, להערכתה. על רשות האכיפה המדינתית ליידע את נציבות האיחוד בנוגע לקיומו של מוצר שלהערכתה אינו עומד בדרישות הצעת חוק חוסן הסייבר. אם בתוך שלושה חודשים הנציבות או מדינה אחרת מהאיחוד אינן מעלות כל טענה נגד האמצעים שנקטה רשות האכיפה המדינתית שדיווחה על היעדר הציות לראשונה, כל רשויות האכיפה בכל מדינות האיחוד יוודאו נקיטת צעדים דומים כלפי אותו המוצר, ללא דיחוי.[235]

אם הרשות המדינתית מוצאת בבדיקתה שיצרן המוצר עומד בדרישות הצעת חוק החוסן, אך לדעתה עדיין גלום במוצר איום סייבר משמעותי, ונוסף על כך הוא מסכן את בריאותם או בטיחותם של אנשים, או אינו עומד בדרישות של האיחוד או של המדינה בכל הקשור להגנה על זכויות יסוד, לזמינות ולמהימנות או לסודיות של שירותים שגופים חיוניים חיצוניים מציעים או להיבטים אחרים של הגנה על אינטרס ציבורי – היא מוסמכת לדרוש מהיצרן לנקוט את כל הצעדים המתאימים כדי להבטיח שבעת החדרת המוצר החכם לשוק הוא אינו מציב עוד כל סיכון, או להוציא את המוצר מהשוק או לאסוף אותו מהלקוחות בתוך זמן סביר, בהתאם לאופי הסיכון. על הרשות המדינתית להודיע על הצעדים שנקטה ללא דיחוי לנציבות האיחוד. על הנציבות להתייעץ עם כל המדינות החברות ועם יצרן המוצר הרלוונטי, לבחון את הצעדים שנקטה רשות האכיפה המדינתית ובמידת הצורך להציע צעדים מתאימים נוספים.[236]

הצעת חוק חוסן הסייבר מעניקה גם לנציבות האיחוד האירופי כלים לחיוב הרשויות המדינתיות לבצע הערכת ציות אם הנציבות חוששת שבמוצר מסוים גלום סיכון סייבר משמעותי והוא אינו עומד בדרישות הצעת חוק החוסן. בנסיבות חריגות המצדיקות היערכות מיידית לשם שמירה על תפקודו התקין של השוק החופשי, וכאשר לנציבות יש סיבות מספיקות לחשוד שבמוצר כלשהו טמון סיכון סייבר משמעותי, או סיכון לפגיעה בבריאותם או בביטחונם של אנשים או בזכויות היסוד שלהם, בין שהמוצר עומד בדרישות הצעת חוק החוסן ורשויות האכיפה המדינתיות לא נקטו צעדים יעילים ובין שלא, הנציבות מוסמכת לבקש מסוכנות הגנת הסייבר האירופית (European Union Agency

235 **שם**, בסעיף 43.

236 **שם**, בסעיף 46.

(for Cybersecurity, ENISA) לבצע הערכה של מידת הציות של המוצר החכם לדרישות הצעת חוק חוסן. על יצרן המוצר לשתף פעולה עם ENISA. על בסיס הערכת ENSIA תאמץ הנציבות האירופית, לאחר שתתייעץ ללא דיחוי עם המדינות החברות ועם יצרן המוצר הרלוונטי, אמצעים מגבילים או מתקנים ברמת האיחוד, לרבות הוראה להוציא את המוצר מהשוק או לאסוף את כל המוצרים ששווקו כבר בתוך תקופה סבירה.[237]

לסיכום, סקירת הצעת חוק החוסן מעידה כי חקיקת החוק יכולה להיות צעד משמעותי וחשוב לחיזוק הגנת הסייבר במוצרי צריכה דיגיטליים, וייתכן שהוא אף יקשה על חברות המפתחות נוזקות מעקב להחדיר את הנוזקה למכשיר הטלפון הסלולרי. אולם כבר היום ידוע שהחברות המפתחות נוזקות מעקב משקיעות מאמצים רבים באיתור חולשות המכונות "חולשות יום אפס", כלומר חולשות שטרם התגלו על ידי היצרן ואין בנמצא עדכון אבטחה לתיקונן. למשל, נטען שחברת NSO ניצלה שלוש חולשות אבטחה שגילתה במערכות של מכשירי הטלפון של חברת אפל, אף שזו מקפידה על אמצעי הגנת סייבר מחמירים.[238] הצעת חוק החוסן מתמקדת בהטלת חובות ציות והגנת סייבר מחמירות יותר על היצרנים, אך יעילותה בחסימת פעולתן של נוזקות מעקב, בהתחשב באופני הפעולה של תעשייה זו, עלולה להתגלות כנמוכה.

4.2.1.3. אסדרת השימוש של רשויות אכיפת חוק באירופה בנוזקות מעקב

4.2.1.3.1. צ'רטר זכויות היסוד[239]

הצ'רטר הוא חלק מאמנת ליסבון,[240] ועל כן מחייב את כל המדינות החברות

237 **שם**, בסעיפי הקדמה 58–59 ובסעיפים 45–46.

238 Bill Marczak et al., *NSO Group iMessage Zero-Click Exploit Captured in the Wild*, CITIZENLAB (Sep. 13, 2021)

239 Charter of Fundamental Rights of the European Union, 2016 O.J. C 202) 389) (להלן: צ'רטר זכויות היסוד).

240 Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 Dec. 2007, 2007 O.J. C 306) 1) (להלן: אמנת ליסבון).

באיחוד האירופי[241] ובעל תוקף משפטי כשל אמנה. כלומר על כל מוסדות האיחוד האירופי ועל כל המדינות החברות באיחוד, כאשר הן מיישמות חקיקה של האיחוד, לכבד את הזכויות המעוגנות בצ'רטר. אחת מן הזכויות המעוגנות בצ'רטר היא הזכות להגנה על מידע אישי.[242] פגיעה מותרת בזכות לפרטיות חייבת לעמוד בתנאי הצ'רטר, ומכאן ששימוש של רשות אכיפת חוק אירופית בנוזקת מעקב חייב לעמוד בכמה תנאים:

(**1**) השימוש נעשה בהתאם לחוק. על החוק המתיר את הפגיעה בפרטיות להיות נגיש, צפוי, מדויק וברור דיו בכל הנוגע לכללים, לנסיבות ולתנאים שבמסגרתם מעקב ופגיעה בפרטיות יכולים להתבצע. חוק כאמור גם צריך לכלול מנגנון פיקוח, כדי למנוע שימוש לרעה באמצעי מעקב, וכן סעדים יעילים למי שנפגע מהפרה שלא כחוק של זכותו לפרטיות;

(**2**) הפגיעה בזכות לפרטיות נעשית לאחת מהתכליות הלגיטימיות המנויות בסעיף 8.1 לצ'רטר: ביטחון לאומי, ביטחון הציבור, מניעת אי־סדר או מניעת פשע. החוק המדינתי חייב להגדיר במפורש את המונח "ביטחון לאומי" ואת היקף העבירות שייחשבו כאיום על הביטחון הלאומי או שמניעתן או חקירתן מצדיקות פגיעה בזכות לפרטיות;

(**3**) הפגיעה בזכות לפרטיות היא נחוצה ומידתית בחברה דמוקרטית כדי להשיג מטרות לגיטימיות. המידתיות והנחיצות צריכות להיבחן בכל אחד משלבי ההפעלה של נוזקת המעקב. על המדינות להקים ולהפעיל מנגנונים יעילים, לרבות בתי משפט, מנגנוני פיקוח וניטור וביקורת ציבורית, כדי למנוע פגיעה שרירותית ולהבטיח איזון הוגן בין הזכות לפרטיות לבין התכלית

241 פולין וצ'כיה מחויבות לצ'רטר במתכונת מצומצמת יותר במסגרת הסדר מיוחד שנחתם עימן בנושא. ראו Agnieszka Kastelik-Smaza, *The Application of the Charter of Fundamental Rights of the EU in Poland*, 4 Acta Universitatis Carolinae 101 (2018); Martin Madej, *The Charter of Fundamental Rights of the EU in the Czech Judicial Decisions: Falling Short of Expectations?* 9(3) The Lawyer Quarterly 228 (2019)

242 צ'רטר זכויות היסוד, **לעיל** ה"ש 239, בסעיף 8.

שהפגיעה בפרטיות נועדה להשיג.[243] בפסיקה אף נקבע שכאשר רשות עושה שימוש בהיחבא בסמכויות שניתנו לה לפגיעה בזכות לפרטיות, קיים סיכון ברור לפגיעה שרירותית מעבר לנחוץ. לפיכך נדרש שהכללים המאפשרים לרשות לעשות שימוש בכלי מעקב חשאיים יהיו ברורים וגלויים, יכללו פירוט של העבירות המצדיקות מעקב חשאי, קטגוריות של האנשים שאפשר לעקוב אחריהם באופן חשאי, מגבלה על משך זמן המעקב המותר, מנגנון לבחינה, שימוש ואחסון של המידע שנצבר עקב המעקב, אמצעי הזהירות שיש לנקוט כאשר המעקב מוביל למידע על אנשים נוספים לבד מיעד המעקב, והנסיבות שבהן חובה למחוק מידע שהושג במעקב אחר תקשורת דיגיטלית.[244]

4.2.1.3.2. האמנה האירופית לזכויות אדם[245] ואמנה 108+[246]

כאשר רשויות אכיפה מדינתיות משתמשות בנוזקות מעקב למטרות ביטחון לאומי הן כפופות לחוקים המדינתיים הרלוונטיים וכן לשתי אמנות אירופיות מרכזיות: האמנה האירופית לזכויות אדם, אשר מגינה על זכויות יסוד של אזרחי 47 מדינות האיחוד ואנגליה החתומות עליה, לרבות הזכות להגנה על מידע אישי;[247] ואמנה 108+, העוסקת בעיבוד אוטומטי של מידע אישי ומחייבת את המדינות החתומות עליה ואת מוסדות האיחוד האירופי. מכוח שתי אמנות אלו, שימוש בנוזקות מעקב למטרות ביטחון לאומי חייב לעמוד

243 Tamar Kaldani & Zeev Prokopets, Pegasus Spyware and Its Impacts on Human Rights 10–13 (Council of Europe Information Society Department 2022)

244 Roman Zakharov v. Russia [GC], App. No. 47143/06 (Eur. Ct. H.R. Dec. 4, 2015); Szabó & Vissy v. Hungary, App. No. 37138/14 (Eur. Ct. H.R. Jan. 12, 2016)

245 European Convention on Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 (as Amended by Protocols Nos. 11, 14 and 15) (להלן: האמנה האירופית לזכויות אדם).

246 Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 (להלן: אמנה 108+).

247 האמנה האירופית לזכויות אדם, **לעיל** ה"ש 245, בסעיף 8.

בדרישת הנחיצות והמידתיות: עליו להיות האמצעי הנחוץ והמידתי להגשמת המטרה. כמו כן, אמנה 108+ מחייבת רשויות ציבור וחברות פרטיות להטמיע עקרונות של עיצוב לפרטיות, להעניק הגנה מוגברת על מידע רגיש, וליישם אבטחת מידע מוגברת, שקיפות ואחריותיות. האמנה אף מחייבת מפתחים וספקי שירות להוכיח ציות לכללי הגנת מידע.[248]

4.2.1.3.3. הדירקטיבה להגנה על מידע אישי בידי רשויות אכיפת חוק

דירקטיבה זו מסדירה את ההגנה על מידע אישי שנאסף ומעובד בידי רשויות אכיפת חוק, ואת השימוש במידע זה.[249] מכאן שיש בדירקטיבה כדי להסדיר את השימוש שיעשו רשויות אכיפת החוק האירופיות במידע אישי שיאספו בעת השימוש בנוזקת מעקב. הדירקטיבה מבוססת על הבנה שהטכנולוגיה הקיימת היום מאפשרת עיבוד מידע אישי בהיקפים בלתי נתפסים, ואפשר באמצעותה למנוע, לחקור ולגלות עבירות פליליות ולהעמיד את מבצעיהן לדין; ואולם, יש להבטיח שהשימוש של רשויות אכיפת חוק במידע אישי למטרות אלו, כולל למטרות הגנה מפני איומים על ביטחון הציבור ומניעתם, ייעשה תוך הגנה ברמה הגבוהה ביותר האפשרית על המידע האישי. לפיכך נדרש שעיבוד מידע ייעשה באופן חוקי, הוגן ושקוף כלפי נושא המידע, ושהטכנולוגיות שבעזרתן המידע יעובד יעוצבו בהתאם לעקרון העיצוב לפרטיות, תוך הטמעת אמצעים טכנולוגיים וארגוניים להגנה על מידע אישי.[250] חריגה מדרישות אלו מותרת רק אם היא נעשית לפי חוק ספציפי המתיר זאת ואם היא האמצעי הנחוץ והמידתי

248 European Data Protection Supervisor, **לעיל** ה"ש 3, בעמ' 6–9; Kaldani & Prokopets, **לעיל** ה"ש 243, בעמ' 13–14.

249 Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of their Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89 (להלן: הדירקטיבה להגנה על מידע אישי בידי רשויות אכיפת חוק).

250 **שם**, בסעיפים 19–20.

בחברה דמוקרטית, ועליה להיעשות תוך התחשבות באינטרסים הלגיטימיים של נושא המידע.[251]

כאשר סביר שפעולות עיבוד מידע אישי, בייחוד אם הן נעשות באמצעות טכנולוגיות חדישות, ובהתחשב באופיין, היקפן או מטרותיהן, יסכנו מאוד את זכויותיו וחירויותיו של נושא המידע, על רשויות האכיפה לערוך סקר סיכונים. סקר זה צריך לכלול גם בחינה של האמצעים והמנגנונים שרשויות אכיפת החוק מבקשות להטמיע כדי להבטיח מתן הגנה למידע אישי ולהוכיח ציות לדרישות הדירקטיבה.[252] כן מחויבות רשויות אכיפת החוק להתייעץ עם הרשות המדינתית להגנת הפרטיות טרם עיבוד המידע.[253]

עוד מחייבת הדירקטיבה את רשויות האכיפה לספק לנושא המידע פרטי מידע שונים על עיבוד המידע האישי עליו, לרבות מידע בנוגע לזהות בעל השליטה במידע ודרכי יצירת הקשר עימו, מטרת עיבוד המידע, זכותו של נושא המידע לפנות בתלונה לרשות להגנת הפרטיות וכן זכותו לגשת למידע האישי עליו, לעיין בו ולדרוש את תיקונו. הדירקטיבה גם מחייבת את רשויות האכיפה לכבד את זכויותיו אלו של נושא המידע. גם כאן מאפשרת הדירקטיבה למדינות החברות לחרוג מדרישת מסירת המידע לנושא המידע או מכיבוד זכויות נושא המידע כל עוד הדבר נחוץ ומידתי במדינה דמוקרטית, בהתחשב בזכויות היסוד והאינטרסים הלגיטימיים של האנשים הנוגעים בדבר, ולמטרות אלו בלבד: (1) כדי למנוע הפרעה לחקירה או להליך רשמי או משפטי; (2) כדי למנוע שיבוש של פעולות שמטרתן מניעה, חקירה או גילוי של עבירה פלילית או תביעה בגינה, או כדי למנוע שיבוש של ענישה פלילית; (3) להגנה על ביטחון הציבור; (4) להגנה על הביטחון הלאומי; (5) להגנה על זכויות וחירויות של אחרים.[254]

251 **שם**, בסעיף הקדמה 26.

252 **שם**, בסעיף הקדמה 58 ובסעיף 27.

253 **שם**, בסעיף הקדמה 59 ובסעיף 28.

254 **שם**, בסעיף הקדמה 44 ובסעיפים 13–15.

כל שימוש במידע אישי בידי רשויות אכיפת החוק למטרות אחרות פרט למניעה, גילוי וחקירה של עבירות פליליות והבאת מבצעיהן לדין מוסדר במסגרת ה־GDPR.[255]

4.2.2. פסיקה ודוחות

באוקטובר 2020 פסק ה־CJEU שמדינה החברה באיחוד אינה פטורה מדרישות החוק האירופי, ובעיקר מדרישות הצ'רטר לזכויות יסוד, גם כאשר היא נוקטת פעולות להגנה על הביטחון הלאומי שלה. במילים אחרות, המדינה אינה יכולה להשתמש בהגנה על הביטחון הלאומי כבמילת קסם המאפשרת פגיעה בזכויות אדם. אכן, כל מדינה החברה באיחוד חופשייה לקבוע את היקף האינטרס של הגנה על הביטחון הלאומי שלה בהתאם לערכיה ולצורכי התקופה, ופגיעה בזכויות אדם מותרת בנימוק של ביטחון הציבור או של אינטרסים ביטחוניים חיוניים.[256] אולם כל אמצעי מדינתי שננקט בשם ההגנה על הביטחון הלאומי חייב לעמוד בדרישות החוק האירופי.[257]

במחקר שערך שירות המחקר של הפרלמנט האירופי בנוגע לשימוש של מדינות החברות באיחוד בנוזקת המעקב פגסוס נקבע ששימוש בנוזקות מעקב עשוי להיות מוצדק כאשר יש חשש ממשי לביטחון הלאומי או לביטחון הציבור.[258] כדי למזער את הסכנה שבשימוש לרעה בנוזקות מעקב הציעו החוקרים, בין השאר, לחייב את מפתחי הנוזקה וספקיה להטמיע אמצעים טכניים, ארגוניים ומשפטיים כדי להבטיח ציות לדרישות ההגנה על זכויות אדם האירופיות והבינלאומיות. אמצעים כאלה יכולים להיות, למשל, מגבלות

255 **שם**, בסעיפי הקדמה 3–4, 11, 15.

256 Consolidated Version of the Treaty on the Functioning of the European Union, arts. 36, 45(3), 51(1), 62, 65(1)(b), 346(1), 2016 O.J. (C 202) 47

257 Joined Cases C-511/18, C-512/18 & C-520/18, La Quadrature du Net v. Premier ministre, ECLI:EU:C:2020:791, ¶ 99; Milderbrath, **לעיל** ה"ש 3, בעמ' 45, 71, 74–77.

258 **שם**, בעמ' 1.

טכניות על השימוש בנוזקות מעקב מבחינת זמן המעקב ומיקומו הגיאוגרפי, סעיפים חוזיים האוסרים על שימוש הפוגע בזכויות יסוד, אמצעים טכניים שיזהירו מפני שימוש לרעה בנוזקת המעקב, ואפשרות להפסיק את השימוש בנוזקה מרחוק במקרה של הפרת זכויות אדם וללא צורך בביטול החוזה קודם לפעולה זו (kill switch). עוד הוצע לאפשר ליצרניות של נוזקות מעקב לדרוש מלקוחותיהן הפקדת סכומי כסף כעירבון לשימוש תקין בנוזקה, והוצע שאם יוכח שלקוח עשה שימוש לרעה בתוכנה יועבר הפיקדון לקרן לפיצוי מי שניזוקו מהשימוש לרעה. אפשרות נוספת היא לחייב יצרניות או ספקיות של נוזקות מעקב בביצוע תסקיר השפעה על זכויות אדם בטרם השלמת עסקה למתן רישיון שימוש בנוזקה. כן מוצע שמשקיעים ובעלי מניות יבצעו בדיקת נאותות לחברה המייצרת נוזקת מעקב לפני השקעה בה, כדי להיווכח באיזו מידה מוטמעת במוצריה הגנה על זכויות אדם.[259]

במחקר נוסף שבוצע לבקשת הפרלמנט האירופי הוסבר שחריג "הביטחון הלאומי" הוא עקב אכילס של ההגנה על הזכות לפרטיות ועל הזכות לחופש ביטוי, ההכרחיות במשטר דמוקרטי, משום שהוא מעניק פטור נרחב מחובת ציות להוראות המגינות על הזכות לפרטיות, דוגמת אלו הקבועות ב־GDPR או בדירקטיבת ה־ePrivacy.[260] לפיכך הוצע שחריג הביטחון הלאומי יפורש בצמצום כך שיחול רק על איומים הממוקדים בכלל הקהילה הפוליטית במדינה. במקביל הובהר מהן הפעולות שבשום אופן אינן פעולות מטעמי ביטחון המדינה: (1) השפעה לרעה על יריב פוליטי; (2) השפעה על ההליך הדמוקרטי, למשל על מערכת הבחירות או מערכת המשפט; (3) הפרעה

259 **שם**, בעמ' 68–69.

260 Directive 2009/136/EC, of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector and Regulation (EC) No. 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 (להלן: דירקטיבת ה־ePrivacy).

לתקשורת; (4) מעקב אחר אקטיביסטים למען זכויות אדם; (5) דיכוי התנגדות או ביקורת; (6) מתן יתרון מיוחד לחברות או לתעשיות; או (7) העדפה של חברי קבוצות שונות המקוטלגות לפי דת, דעה פוליטית, מוצא אתני, מגדר, או הבחנות אחרות שיש בהן כדי להפלות, או פגיעה בחברי קבוצות כמתואר. מדינה הטוענת שפעולותיה נעשות לשם שמירה על ביטחון המדינה אולם הן נופלות לגדרי אחת מהפעולות הללו, תצטרך לשכנע שפעולותיה נעשו למען ביטחון המדינה ושנקטה את כל האמצעים הסבירים למזעור ההשלכות השליליות שלהן. עוד הוצע שלא להוציא מעקב מטעמי ביטחון לאומי מתחולת הוראות ה־GDPR ודירקטיבת ה־ePrivacy, כלומר שמדינות חברות המבקשות לעשות שימוש בנוזקת מעקב למטרות ביטחון לאומי, במובנו הצר, יצטרכו לעמוד גם בהוראות ה־GDPR.[261]

המפקח על הגנת מידע באיחוד האירופי (European Data Protection Supervisor, EDPS), שהוא רשות הגנת המידע העצמאית של האיחוד, בחן אף הוא את השימוש שעשו מדינות החברות באיחוד האירופי בנוזקת המעקב פגסוס של חברת NSO. לשיטתו, מאחר שכיום אנו נשענים על הטלפון החכם לביצוע פעולות רבות בחיי היום־יום שלנו, אגור בטלפון מידע רב מאוד. הטלפון בעצם יודע הכול על המשתמש בו, הוא יכול להאזין למשתמש, לראות אותו, לאתר את המיקום הגיאוגרפי שלו ולדעת עם מי הוא נפגש ומשוחח. משום כך, נוזקת מעקב דוגמת פגסוס, אשר מעניקה למפעילה גישה מלאה ובלתי מוגבלת למידע אישי, לרבות מידע רגיש, מאפשרת הפרעה להיבטים האינטימיים ביותר של חיי היום־יום, עשויה להוביל לרמת פולשנות חסרת תקדים השקולה לנישול נושא המידע מזכותו לפרטיות, ומאיימת בכך על מהות הזכות לפרטיות. הפגיעה אינה רק בפרטיותו של נושא המידע המשתמש בטלפון החכם שאליו הוחדרה נוזקת המעקב, אלא גם בפרטיותם של כל מי שנמצא עימו בקשר או מצוי בסביבתו.[262]

261 Giovanni Sartor & Andrea Loreggia, The Impact of Pegasus on Fundamental Rights and Democratic Processes 55–60 (Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies 2023)

262 European Data Protection Supervisor, **לעיל** ה"ש 3, בעמ' 2, 4–5.

המפקח על הגנת מידע באיחוד האירופי הסיק אפוא שנוזקת מעקב דוגמת פגסוס היא בגדר שינוי של כללי המשחק (game changer), שינוי פרדיגמה של ממש מבחינת הגישה לתקשורת פרטית; נוזקת מעקב משלבת רמת פולשנות שאין שנייה לה עם מאפיינים שהופכים כל אמצעי אבטחה משפטי או טכני לחסר משמעות.[263]

במצב זה, קבע המפקח, יש סבירות נמוכה שנוזקת מעקב עומדת בדרישת המידתיות הקבועה באמנה האירופית לזכויות אדם ובאמנה 108+, ושאלת נחיצותה להשגת מטרה לגיטימית במדינה דמוקרטית כלל אינה רלוונטית. לפי המפקח, שימוש בנוזקת מעקב דוגמת פגסוס אינו עומד בדרישות הדין האירופי, אלא בנסיבות חריגות שבהן קיים איום מיידי של מתקפת טרור ובלבד שאפשר להשבית חלק מהיכולות של נוזקת מעקב דוגמת פגסוס ולהימנע מלהשתמש בהן.[264]

המפקח על הגנת מידע באיחוד האירופי הצביע על בעיה נוספת הכרוכה בשימוש בנוזקות מעקב דוגמת פגסוס: מאחר שהנוזקה מעניקה למפעיליה שליטה מלאה ובלתי מוגבלת בטלפון הנתון למעקב, ומאחר שהיא כמעט אינה מותירה עקבות דיגיטליים לפעילותה, ספק אם המידע הנאסף באמצעותה יכול בכלל לשמש כראיה בהליך פלילי – מנקודת המבט המינהלית ומבחינת אמיתות הראיה. מרבית המומחים לנושא אינם יכולים לוודא את אמיתות הראיה ולהבטיח שאין מדובר בראיה שנשתלה בטלפון הנייד בידי מי שהפעיל את הנוזקה. במובן זה השימוש בנוזקה עשוי לפגוע בזכותו של אדם למשפט הוגן.[265]

המדיניות הראויה והנכונה, לדעת המפקח על הגנת מידע באיחוד האירופי, היא איסור על השימוש בנוזקות מעקב דוגמת פגסוס בכל מדינות האיחוד, ואם בכל זאת נעשה שימוש בנוזקה שכזו יש לנקוט צעדים כדי למנוע שימוש בלתי חוקי בה. המפקח מציע לחזק את הפיקוח הדמוקרטי היעיל על השימוש

263 שם.

264 שם.

265 שם, בעמ' 6–9.

בנוזקות מעקב באמצעות רשות הגנת מידע, ביקורת שיפוטית מראש ובדיעבד וצורות אחרות של ביקורת דמוקרטית; להבטיח ציות לדרישות החקיקה האירופית, ובעיקר לדירקטיבה להגנה על מידע אישי בידי רשויות אכיפת חוק; לחזק את הזכות למשפט הוגן של נאשם בהליך פלילי; להעניק פרשנות מצומצמת ודווקנית לחריג הביטחון הלאומי המשמש להצדקת השימוש בנוזקות מעקב דוגמת פגסוס; להבטיח עצמאות שיפוטית ותקשורת חופשית ולחזק את השיח הציבורי בנוגע לשימוש בנוזקות שכאלו.[266]

4.3. ארצות הברית

4.3.1. פיקוח על היצוא

בארצות הברית קיים משטר פיקוח על יצוא מוצרים וטכנולוגיות דו־שימושיים על בסיס הסדר ואסנאר. משטר זה מחייב יצואנים של מוצרים המנויים בתקנות, כמו גם יצואנים של טכנולוגיות חדשניות ורגישות שמחלקת המסחר האמריקנית החליטה שיש לפקח על יצואן ולא נכללו עד כה ברשימת הטכנולוגיות הקריטיות,[267] בקבלת רישיון יצוא מסוכנות התעשייה והביטחון (Bureau of Industry and Security) שבמחלקת המסחר האמריקנית. משטר פיקוח זה עודכן בשנת 2019 מתוך הבנת הקשר בין טכנולוגיות חדשניות וקריטיות לבין ביטחונה הלאומי של המדינה ויחסי החוץ שלה.[268] מטרת משטר

266 **שם**, בעמ' 9–11.

267 The United States Munitions List, או ה־Commerce Control List (CCL) שהייתה נהוגה תחת ה־Export Administration Act of 1979, 50 U.S.C. §§4601–4623 (2018) (repealed 2018)

268 החוק הראשון אשר הסדיר יצוא של מוצרים מסוג זה היה ה־Export Administration Act of 1979 (**שם**). עם פקיעתו בשנת 1994 הוארכו הוראותיו בצווים נשיאותיים במסגרת ה־International Emergency Economic Powers Act, 50 U.S.C. §1702. בשנת 2018 הוטמעו מגבלות הייצוא שנקבעו בו ב־Export Control Act of 2018, 50 U.S.C. §§4801–4852, אשר נחקק כחלק מה־National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, 132 Stat. 1636 (2018) (להלן: NDAA 2019).

הפיקוח המעודכן היא לשפר את ההגנה על משאביה הטכנולוגיים של ארצות הברית באמצעות הטלת מגבלות מחמירות יותר על העברה לידיים זרות של טכנולוגיות מפתח חדשניות ושל טכנולוגיות להגנת סייבר הנחשבות קריטיות לביטחון המדינה.[269] המגבלות חלות גם על העברת יכולות טכנולוגיות וידע, בין השאר באמצעות מיזמים משותפים. בבחינת מתן הרישיון נשקלים שיקולי ביטחון לאומי לצד שיקולים הנוגעים למדיניות החוץ של ארצות הברית.[270] כדי לקבוע אם יש להטיל על טכנולוגיה פיקוח מוגבר יש לבחון את הפיתוח של טכנולוגיות דומות במדינות זרות, את ההשפעה של מגבלות היצוא על פיתוח טכנולוגיות אלו בארצות הברית ואת היעילות של מגבלות היצוא בהגבלת השגשוג של טכנולוגיות חדשניות דומות במדינות זרות. לאחר ההכרזה על טכנולוגיה כנתונה לפיקוח מוגבר, מחלקת המסחר האמריקנית רשאית להביא בחשבון גם את משתמשי הקצה של הטכנולוגיה ואת מדינות היעד האפשריות בקביעת המגבלות הספציפיות שיחולו עליה. בכל מקרה תוטל חובת רישוי על יצוא טכנולוגיות שיוכרזו כמפוקחות למדינות שארצות הברית הטילה עליהן אמברגו, לרבות סין. בבחינת בקשות רישיון יצוא ספציפיות יובאו בחשבון הערכות מודיעיניות בדבר השפעת יצוא הטכנולוגיה המבוקשת על ביטחונה הלאומי של ארצות הברית, והשפעת היצוא על הגנת התעשיות הביטחוניות בארצות הברית.[271]

4.3.2. פסיקה

חוקיות השימוש בנוזקות מעקב מצויה בימים אלו בדיונים בבתי משפט בארצות הברית. באוקטובר 2019 הגישו חברת מטא וחברת בת שלה, וואטסאפ, תביעה נגד NSO לבית המשפט המחוזי בקליפורניה. בכתב התביעה נטען שבמהלך החודשים אפריל–מאי 2019 יצרה NSO כמה חשבונות וואטסאפ והסכימה במסגרתם לתנאי השימוש ביישומון, אולם בפעולותיה הפרה את

269 **שם**, בסעיף 1758.

270 Burt Braverman, *Congress Enacts the Export Controls Act of 2018, Extending Controls to Emerging and Foundational Technologies*, Davis Wright Tremaine LLP (Sep. 26, 2018)

271 NDAA 2019, **לעיל** ה"ש 268, בסעיף 1758.

הסכם השימוש משום שבאמצעות החשבונות האלה הצליחה NSO לעקוף את מנגנוני ההצפנה והאבטחה של היישומון. כך עלה בידי NSO להחדיר את הנוזקה פגסוס לכ־1,400 מכשירי טלפון ניידים ומכשירים ניידים אחרים ב־20 מדינות שונות, מתוכם 100 מכשירים השייכים לעיתונאים או פעילי זכויות אדם, מבלי שמשתמשי המכשיר נדרשו לנקוט לשם כך פעולה אקטיבית כלשהי כמו לחיצה על הודעה או קישורית. עוד נטען ש־NSO שלטה מרחוק בתפעול הנוזקה ובשימוש שעשו בה לקוחותיה באמצעות רשת מחשבים. כך יכלה NSO לעדכן את הנוזקה מרחוק, להורות לנוזקה לבצע פעולות שונות במכשיר הנייד של יעד המעקב, לנטר את פעולותיה של הנוזקה במכשיר ולהעביר מידע ממנו ללקוחותיה.[272]

בתביעה נטען גם ש־NSO הפיקה רווח פיננסי ישיר ממכירת רישיונות שימוש בנוזקה וממתן שירותי תמיכה ללקוחותיה, שכללו התקנת הנוזקה, תוך עקיפת האבטחה של היישומון והפרת הסכם השימוש בו, ניטור השימוש בנוזקה והכשרת הלקוחות לשימוש בה. כמו כן, NSO העניקה ללקוחותיה תמיכה טכנית באמצעות דוא"ל, תקשורת טלפונית ופתרון בעיות על ידי גישה מרחוק לנוזקה על גבי רשת פרטית.[273]

בקשתה של NSO למחיקת התביעה על הסף נדחתה. בית המשפט המחוזי במחוז הצפוני בקליפורניה פסק שאף ש־NSO פועלת כסוכנת של המדינה שלה מכרה את רישיון השימוש בנוזקה בכל מקרה ומקרה, היא אינה יכולה ליהנות מהחסינות יציר המשפט המקובל המוענקת לסוכנים הפועלים מטעם או בשם מדינה זרה, משום שפסיקה נגד NSO לא תחייב את המדינה הזרה ש־NSO פעלה בשמה או מטעמה.[274] בית המשפט לערעורים במחוז התשיעי בארצות הברית אישר את החלטת בית המשפט המחוזי ודחה את בקשת NSO לסילוק

272 Complaint and Demand for Jury Trial, WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 3:19-cv-07123 (N.D. Cal. filed Oct. 29, 2019)

273 **שם**; Plaintiffs' Opposition to Defendants' Motion to Dismiss, WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 4:19-cv-07123-PJH (N.D. Cal. May 27, 2020)

274 WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020)

התביעה על הסף בנימוק שונה: הוא פסק שה־Foreign Sovereign Immunities Act (FSIA)[275] הוא המקור החקיקתי היחיד לחסינות מפני אחריות של מדינה זרה ושל סוכניה, והוא מאיין את החסינות יציר המשפט המקובל. מאחר ש־NSO אינה נופלת בגדר הגופים שלהם מוענקת חסינות לפי ה־FISA, בקשתה למחיקה על הסף בנימוק זה נדחתה.[276]

באפריל 2022 הגישה NSO לבית המשפט העליון בארצות הברית בקשה לערעור על החלטת בית המשפט לערעורים במחוז התשיעי בטענה כי יש להכיר בה כסוכנת מטעמה של מדינה זרה הזכאית ליהנות מהחסינות יציר המשפט המקובל המוענקת לגופים כמותה.[277] טרם החלטה פנו שופטי בית המשפט העליון למשרד המשפטים האמריקני בבקשה לחוות את דעתו בסוגיה.[278] ממשל ביידן ביקש, במסמך שהוגש מטעמו לבית המשפט, שבקשת הערעור תידחה, אם כי לא שלל את האפשרות העקרונית לקיומה של חסינות יציר המשפט המקובל לצד זו המוענקת לפי ה־FSIA. בינואר 2023 דחה בית המשפט העליון בארצות הברית את בקשת רשות הערעור של NSO, והתיק הוחזר להמשך דיון לבית המשפט המחוזי בקליפורניה.[279]

תביעה נוספת נגד NSO הוגשה על ידי חברת אפל בבית המשפט המחוזי במחוז הצפוני של קליפורניה. בכתב התביעה נטען שנוזקת המעקב פגסוס הותקנה מרחוק במכשירי אפל באמצעות רמייה והתחזות, ושלא בהסכמת

275 Foreign Sovereign Immunities Act of 1976 (FSIA), U.S.C 28, §§ 1330, 1332, 1391(f), 1441(d), 1602–1611.

276 WhatsApp LLC v. NSO Grp. Techs Ltd., No. 20-16408 (9th Cir., Jan. 6, 2022) (rehearing denied)

277 Petition for Writ of Certiorari, NSO Grp. Techs. Ltd. v. WhatsApp Inc., No. 21-1338 (U.S. Apr. 6, 2022)

278 Lawrence Hurley, *U.S Supreme Court Seeks Biden's View on WhatsApp 'Pegasus' Spyware Dispute*, Reuters (June 6, 2022)

279 *US Supreme Court Lets WhatsApp Pursue Pegasus Spyware Lawsuit*, Reuters (Jan. 9, 2023); Tonya Riley, *Supreme Court Clears Way for WhatsApp Case Against NSO Group, Opening Spyware Firm to More Lawsuits*, Cyberscoop (Jan. 9, 2023)

בעל המכשיר או בידיעתו. הנוזקה הוחדרה באמצעות יצירת חשבונות זיהוי באפל (Apple ID), הסכמה לתנאי השימוש של iCloud וניצול חולשה שהתגלתה במערכותיה של אפל. בכך עשתה NSO שימוש לרעה במכשירי אפל והפרה את תנאי השימוש שלהם הסכימה. מרגע התקנתה אפשרה פגסוס ל־NSO וללקוחותיה לעקוב מרחוק אחר המשתמש במכשיר שבו הותקנה, לרבות אחר פקידי ממשל, עיתונאים, אנשי עסקים, פעילים חברתיים, אנשי אקדמיה ואזרחי ארצות הברית. NSO פיתחה, מכרה ותפעלה את הנוזקה, וכן תמכה מרחוק בשימוש שעשו בה לקוחותיה, לרבות באמצעות מתן שירותי ייעוץ, ועל כן הפיקה מהשימוש שעשו לקוחותיה בתוכנת פגסוס רווח כלכלי. עוד טענה אפל בכתב בתביעה כי היא מצויה במרוץ חימוש עם NSO: אפילו כאשר אפל מפתחת פתרונות אבטחה משופרים למכשיריה, NSO ממשיכה לעדכן את הנוזקה שלה ולחפש חולשות שהיא מנצלת כדי להתגבר על שיפורי האבטחה שאפל מתקינה.[280]

תביעה נוספת נגד NSO הוגשה לאותו בית משפט בנובמבר 2022 בשם עיתונאים מארגון העיתונאים העצמאי אל פארו (El Faro) מאל סלבדור. לטענתם הם היו נתונים למעקבים באמצעות תוכנת פגסוס של NSO אשר התרחשו כל אימת שהעיתונאים עמדו לפרסם תחקיר חשוב. לפיכך בכתב התביעה דרשו העיתונאים ש־NSO תזהה, תשיב ותמחק כל מידע שהושג באמצעות מעקבים אלו, ותצביע על הלקוחות שהורו על כל אחד ואחד מהמעקבים. NSO הגישה בקשה למחיקת התביעה על הסף, והדיון בבקשה טרם התקיים.[281]

4.3.3. שימוש רשויות הביון והאכיפה בנוזקות מעקב

ככלל, לפי צו נשיאותי של הנשיא ביידן מאוקטובר 2022, רשות ביון אמריקנית רשאית לבצע פעילות מודיעינית של איסוף מודיעין אותות (סיגינט), ובכלל זה שימוש בנוזקת מעקב, רק מכוח הרשאה בחוק או בהוראה נשיאותית, ובכפוף

280 Complaint, Apple Inc. v. NSO Grp. Techs. Ltd., No. 3:21-cv-09078 (N.D. Cal. filed Nov. 23, 2021)

281 Dada v. NSO Grp. Techs. Ltd., No. 3:22-cv-07513 (N.D. Cal. filed Nov. 29, 2002)

לאמצעי הגנה מתאימים שיבטיחו ששיקולים הקשורים לזכות לפרטיות ולחירויות אזרחיות של כל אדם יובאו בחשבון בעת ביצועה, כך שהפעילות המודיעינית תבוצע בתנאים האלה: (1) לאחר קביעה, המבוססת על הערכה סבירה של כל ההיבטים הרלוונטיים, שהפעילות נחוצה לשם השגת מטרה מודיעינית מאומתת (validated intelligence priority) ולגיטימית, אף אם אין מדובר באמצעי היחיד האפשרי לקידום היבטים הקשורים במטרה זו. הצו הנשיאותי מונה כמה מטרות לגיטימיות אפשריות, לרבות הבנה או הערכה של היכולות, הכוונות או הפעילות של מדינה או ארגון זרים, הבנה או הערכה של איום גלובלי, הגנה מפני פעילות צבא זר והגנה מפני פעילות טרור; (2) בהיקף מידתי לאותה מטרה, תוך הקפדה על איזון ראוי בין החשיבות של השגת המטרה המודיעינית המאומתת ובין השפעתה של הפעילות על הזכות לפרטיות וחירויות אחרות של כל אדם, ללא קשר ללאום שאליו הוא משתייך או למקום מגוריו; (3) תחת פיקוח קפדני שמטרתו להבטיח התאמה לתנאים שלעיל.[282]

שנה קודם לכן, בנובמבר 2021, הוסיפה מחלקת המסחר האמריקנית את NSO לרשימה השחורה של חברות שאסור למכור להן מוצרי חומרה ותוכנה של חברות אמריקניות אלא ברישיון מיוחד מרשויות ארצות הברית, שהסבירות לקבלתו נמוכה. צעד זה נבע מהטענה ש־NSO סיפקה נוזקה לממשלות זרות שעשו בה שימוש למעקב בזדון אחר עיתונאים, עובדי שגרירות, אנשי עסקים ואקדמיה ופעילים חברתיים.[283] ביולי 2023 הוסיפה מחלקת המסחר האמריקנית לרשימה שתי חברות נוספות המייצרות נוזקות מעקב: חברת Cytrox מהונגריה וחברת Intellexa מקפריסין.[284]

282 Exec. Order No. 14086, Enhancing Safeguards for United States Signals Intelligence Activities, §2, 87 Fed. Reg. 62283 (Oct. 7, 2022)

283 Press Release, U.S. Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021)

284 Renshaw, Shepardson, & Freifeld, **לעיל** ה"ש 164. חברת Intellexa הוקמה על ידי יוצא מערכת הביטחון אל"מ טל דיליאן בקפריסין. ראו שוקי שדה "השותפות נחשפת: איש העסקים שמקשר בין תוכנת ריגול טורפנית לבין הפנסיה שלכם" **שומרים** (23.6.2023).

הכללת חברה ברשימה השחורה משמעה שהחברה לא תוכל לרכוש מערכות הפעלה של חברת מייקרוסופט, שירותי ענן של אמזון או מכשירי אייפון – מוצרים וטכנולוגיות שהיא עושה בהם שימוש כחלק מפעילותה הרגילה. משום כך, חברה הנכללת ברשימה השחורה צפויה להתמודד עם קשיים ניכרים בהמשך פעילותה השגרתית. מנכ"ל NSO דאז, שלֵו חוליו, התרעם על ההחלטה וטען שכל התקשרויותיה של NSO מאושרות על ידי ממשלת ישראל במסגרת משטר הפיקוח על היצוא הקיים במדינה, ולכן NSO מעולם לא מכרה את נוזקת המעקב שפיתחה למדינות שאינן בעלות בריתה של ארצות הברית או ישראל. כהוכחה לדבריו סיפר שממשלת ישראל מנעה מכירת רישיון שימוש בנוזקה לממשלת אוקראינה מפני שחששה מתגובת ממשלת רוסיה לעסקה.[285]

הגילויים בדבר השימוש שעשו מדינות שונות בנוזקת המעקב פגסוס של NSO הובילו לדיונים גם בבית הנבחרים האמריקני. באחד הדיונים אישר ראש ה־FBI כריסטופר ריי שבשנת 2019 רכשה ה־FBI רישיון שימוש מוגבל בנוזקת פגסוס למטרות בחינה והערכה של הנוזקה, בין השאר כדי לשפר את יכולתה להתמודד עם הנוזקה אם ייעשה בה שימוש לרעה בידי גופים זרים. לדבריו לא נעשה בנוזקה כל שימוש למטרות חקירה.[286] עם זאת, בעיתונות נחשף שלקראת סוף 2020 ובמחצית הראשונה של שנת 2021 נעשה מאמץ ב־FBI להכשיר את השימוש בנוזקת המעקב פגסוס כדי להשתמש בה בחקירות פליליות, ונוסחו כללים מנחים עבור תובעים פדרליים לגבי חשיפת השימוש בנוזקה במהלך הליכים פליליים. אולם ביולי 2021, כנראה בעקבות החשיפות בתקשורת בנוגע לשימוש לרעה שעשו ממשלות זרות בנוזקה, הוחלט ב־FBI להימנע משימוש בה בחקירות פליליות. עם זאת, ה־FBI לא הכחישה שייתכן שתעשה בעתיד שימוש בנוזקות למעקב דיגיטלי במהלך חקירות פליליות.[287] יתרה מכך, לפי דיווחים שפורסמו בתקשורת בנובמבר 2021 נחתם חוזה סודי

285 Farrow, **לעיל** ה"ש 2.

286 Stephanie Kirchgaessner, *FBI Confirms It Obtained NSO's Pegasus Spyware*, The Guardian (Feb. 2, 2022)

287 Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I Came to Deploying Spyware*, The New York Times (Nov. 12, 2022)

בין NSO לרשות ממשלתית אמריקנית לקבלת רישיון לשימוש במקסיקו בנוזקת מעקב המאפשרת מעקב אחר נתוני מיקום של מכשיר הסלולר של יעד המעקב ללא ידיעתו. פרטים בדבר זהותה של הרשות הממשלתית החתומה על החוזה, השימוש שנעשה בנוזקת המעקב בפועל והאופן שבו חוזה זה נחתם על אף איסור מפורש מצד הממשל אינם ידועים.[288]

במרץ 2023 הוציא ממשל ביידן צו מינהלי נשיאותי האוסר על רשויות פדרליות להשתמש בנוזקות מעקב מסחריות שייתכן שנעשה בהן שימוש לרעה בידי מדינות זרות, בנוזקות שעשויות לשמש למעקב אחר אזרחי ארצות הברית מחוץ למדינה או בנוזקות שעשויות להוות סיכון אם יותקנו ברשתות הממשל. איסור השימוש מוגבל אך ורק לנוזקות מעקב מסחריות, אך אינו חל במקרים מסוימים שבהם איש ממשל קובע שנוזקת המעקב אינה מציבה סיכון ביטחוני או מודיעיני משמעותי לממשל בארצות הברית, או שאין סיכוי גבוה לשימוש לרעה בנוזקה בידי ממשלה זרה או אזרח זר.[289]

בשנת 2022 התקבל ה־National Defense Authorization Act לשנת 2022, אשר חייב את מחלקת המדינה להכין רשימה של ספקי ציוד תקשורת, ספקי טכנולוגיית מידע – לרבות תוכנה וחומרה – וספקי שירותים, שסייעו או אפשרו לבצע מתקפת סייבר או מעקב דיגיטלי נגד ארצות הברית בשם או מטעם ממשלה זרה המנויה ברשימת השחקנים המהווים איום סייבר משנת 2017, או נגד יחידים – לרבות אקטיביסטים, עיתונאים, מתנגדים פוליטיים או אחרים – למטרות דיכוי התנגדות או הרתעה מפני ביקורת, בשם מדינה המנויה ברשימת המדינות הפוגעות בזכויות אדם כחלק מדיכוי פוליטי. על מחלקת המסחר להימנע ככל האפשר מהתקשרות חוזית עם גוף המנוי ברשימה זו.[290] עוד

288 Mark Mazzetti & Ronen Bergman, *A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill*, The New York Times (April 2, 2023)

289 Exec. Order No. 14093, Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 88 Fed. Reg. 18957 (March 27, 2023)

290 National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, §5502, 135 Stat. 2048 (2021)

הטיל החוק מגבלות על תעסוקת עובדי מערכת המודיעין האמריקנית לאחר סיום העסקתם בגוף הממשלתי, לרבות תקופת צינון, חובות דיווח ומגבלות על העסקתם בחברות או בממשלות זרות.[291]

4.4. ישראל

4.4.1. פיקוח על היצוא

ישראל אינה חברה בהסדר ואסנאר. עם זאת, משנת 2014 קיים בה משטר פיקוח דה יורה על יצוא מוצרים וידע סייבר התואם את עיקרי הסדר ואסנאר, והוא מזכה אותה במעמד של "מדינה נאמנה" (adherent state).[292] חוק הפיקוח על יצוא ביטחוני, התשס"ז–2007 (להלן: חוק הפיקוח), מסדיר את הפיקוח המדינתי על יצוא מוצרים ביטחוניים, על העברה של ידע בתחום ועל מתן שירותי ביטחון, בהתבסס על שיקולי ביטחון ויחסי החוץ של המדינה. לפי חוק הפיקוח, יצוא של ציוד ביטחוני, לרבות השיווק שלו הכולל גם את המשא ומתן המקדמי בטרם חתימה על חוזה, מחייב קבלת רישיון מאגף הפיקוח על היצוא הביטחוני (אפ"י) במשרד הביטחון. לפי החוק, "ציוד ביטחוני" כולל בין השאר גם "ציוד דו־שימושי מפוקח": ציוד שנועד מעיקרו לשימוש אזרחי ומתאים גם לשימוש ביטחוני אשר נכלל ברשימת טובין וטכנולוגיות דו־שימושיים שנקבעה בהסדר ואסנאר, כפי שמתעדכנת מעת לעת,[293] ואשר נועד לשימוש ביטחוני, או כל ציוד דו־שימושי אחר שקבע שר הביטחון בצו.[294]

291 **שם**, בעמ' 308.

292 **אסדרת יצוא טכנולוגיות סייבר ממדינת ישראל: ההסדר הראוי** 30–31 (סדנת סייבר, הפקולטה למשפטים באוניברסיטת חיפה, יוני הר כרמל עורך, ינואר 2018) (להלן: אסדרת יצוא טכנולוגיות).

293 המשמעות היא שכל עדכון של רשימת הטכנולוגיות הדו־שימושיות בהסדר ואסנאר חל אוטומטית גם בישראל.

294 סעיף 2 לחוק הפיקוח.

אם הציוד שעבורו מבוקש רישיון היצוא מיועד לשימוש ביטחוני, יש להגיש את בקשת הרישיון לאפ"י. אם הציוד מיועד לשימוש אזרחי, יש להגיש את בקשת הרישיון למשרד הכלכלה והתעשייה בהתאם להוראות צו היבוא והיצוא (פיקוח על יצוא טובין, שירותים וטכנולוגיה דו־שימושיים), התשס"ח-2006. במקרים מסוימים, בהתאם למוגדר בחוק, על משרד הכלכלה והתעשייה לפנות למשרד הביטחון ולמשרד החוץ כדי לבחון השלכות ביטחוניות של מתן הרישיון המבוקש או השלכות אפשריות על יחסי החוץ של המדינה. מתן רישיון יצוא לשימוש אזרחי הוא בסמכות משרד הכלכלה והתעשייה, אולם עליו להביא בחשבון את עמדת משרד הביטחון ומשרד החוץ. אם משרדים אלו מתנגדים למתן הרישיון ומשרד הכלכלה והתעשייה חולק על עמדתם, יכריעו בבקשה מנכ"לי שלושת המשרדים. אם המנכ"לים אינם מצליחים להגיע להסכמה תועבר ההכרעה בבקשה לראש הממשלה.[295]

אם השימוש המיועד הוא ביטחוני חלות על בקשת הרישיון הוראות חוק הפיקוח ותקנות הפיקוח על יצוא ביטחוני (רישיונות), התשס"ח-2008. בהתאם למסגרת רגולטורית זו על המבקש להירשם תחילה כיצואן במאגר הרישום של אפ"י, לפרט את המוצרים שהוא מעוניין לייצא ולהגיש לאפ"י בקשה לרישיון שיווק בטחוני לשם שיווקו של הציוד הביטחוני. רק לאחר קבלת רישיון השיווק, ולאחר שנחתמה עסקה עם לקוח מסוים, על היצואן לפנות לאפ"י בבקשה לקבל רישיון ליצוא הציוד המסוים ללקוח ספציפי. בקשת רישיון לשיווק או ליצוא נבחנת תחילה בידי ועדה מייעצת שחברים בה נציגים ממשרד הביטחון, ממשרד החוץ וממשרד התעשייה, וכן עובדי כוחות הביטחון. אם נציג משרד החוץ מסתייג ממתן רישיון אך הוועדה המייעצת שוקלת שלא לקבל את הסתייגותו, או אם אפ"י שוקלת להיענות לבקשת רישיון על אף המלצת הוועדה המייעצת לסרב לבקשה, ההכרעה מועברת לדיון משותף של ראש אפ"י וראש האגף לעניינים אסטרטגיים במשרד החוץ. אם בעלי תפקידים אלו אינם מצליחים להגיע להחלטה, תועבר ההכרעה למנכ"לי משרד הביטחון והחוץ, ואם אלו לא הגיעו להחלטה תועבר בקשת הרישיון להכרעת ועדת

295 סעיפים 4–7 לצו היבוא והיצוא (פיקוח על יצוא טובין, שירותים וטכנולוגיה דו־שימושיים), התשס"ו–2006.

המשנה של ועדת השרים לביטחון לאומי.[296] לאחר קבלת הרישיון חב היצואן בדיווח שנתי לאפ"י על הפעילות שביצע במסגרת הרישיון.[297]

על משטר הפיקוח על היצוא של מדינת ישראל נמתחה ביקורת במישור הבינלאומי, בעיקר לאחר חשיפת השימוש של משטרים לא דמוקרטיים בנוזקות מעקב שפיתחו חברות ישראליות. נטען שמשטר הפיקוח על היצוא בישראל לוט בערפל ואינו מאפשר ביקורת ציבורית יעילה, שכן מתן הרישיונות, מספרם, מדינות היעד ליצוא ונושאים נוספים הקשורים ברישוי מוצרי ביטחון הם חסויים.[298] נוסף על כך, לפי הפרסומים מדינת ישראל הייתה מודעת לשימוש לרעה שעושות מדינות בנוזקת המעקב פרי פיתוחה של חברת NSO, תוך פגיעה בזכויות אדם. נטען אף שישראל השתמשה בסחר בנוזקה כבסיס לשיפור יחסיה הדיפלומטיים עם מדינות אחרות. עם זאת, בהצהרה רשמית מטעם שר הביטחון נאמר שהשיקולים במתן רישיונות יצוא כוללים שיקולי ביטחון, שיקולי מדיניות חוץ ובחינת יחסה של המדינה המבקשת לרכוש רישיון שימוש במוצר לזכויות אדם.[299]

לא זו אף זו, עצם העמידה בתנאי משטר הפיקוח הובילה חברות המפתחות נוזקות מעקב להניח שאין צורך בבחינת השלכות הטכנולוגיה שפיתחו על זכויות אדם. כך עולה מדבריו של מנכ"ל NSO לשעבר שלֵו חוליו. לשיטתו העובדה ש־NSO פעלה הלכה למעשה לפי הוראותיה של ממשלת ישראל בכל אחת מהתקשרויותיה מלמדת כי אין לממשל האמריקני סיבה לכלול אותה ברשימה השחורה של מחלקת המסחר.[300]

מדיווחים בתקשורת עולה שעקב חשיפת השימוש שעשו משטרים לא דמוקרטיים בנוזקות מעקב מתוצרת ישראל הקשיח משרד הביטחון בסוף

296 תקנות הפיקוח על יצוא ביטחוני (התייעצות עם משרד החוץ בנוגע למתן רישיון יצוא ביטחוני), התשס"ח–2008, ק"ת 463; סעיפים 23–27 לחוק הפיקוח.

297 סעיף 28 לחוק הפיקוח.

298 דוח הבודק המיוחד 2019, **לעיל** ה"ש 195, בעמ' 11–12, 17.

299 Farrow, **לעיל** ה"ש 2.

300 **שם**.

שנת 2021 ותחילת שנת 2022 את מדיניות הפיקוח ומתן רישיונות היצוא לטכנולוגיות סייבר התקפי, ובהן נוזקות מעקב. ישראל צמצמה את רשימת המדינות שאליהן מותר לייצא מוצרי סייבר מ־102 ל־37 מדינות, וביטלה את רישיונות השיווק והיצוא שניתנו ליצוא למדינות שהוצאו מהרשימה. החברות נדרשו להגיש מחדש בקשה לרישיון שיווק ולרישיון יצוא גם באשר לחוזים שכבר נחתמו ויצאו אל הפועל.[301] לטענת בכירים בתעשיית הסייבר ההתקפי צעד זה יקשה מאוד על חברות הסייבר ההתקפי בישראל, שכן מדינות המערב המנויות ברשימת 37 המדינות שמותר לייצא אליהן רוכשות נוזקות מעקב במשורה ובאופן מפוקח ואינן קהל הלקוחות השגרתי של חברות הסייבר ההתקפי – אלו התבססו בעיקר על משטרים לא דמוקרטיים אשר היו מוכנים לשלם סכומי עתק בעבור נוזקות מעקב. התוצאה, כך סוברים בכירי התעשייה, תהא עזיבה של חברות הסייבר ההתקפי את ישראל ופתיחת חברות זהות במדינות שאינן מפקחות באופן מחמיר כל כך על יצוא טכנולוגיות ביטחון דו־שימושיות.[302]

תביעות משפטיות שניסו לגרום למשרד הביטחון לשקול את השפעתן של טכנולוגיות דו־שימושיות על זכויות אדם בעת בחינת מתן רישיון יצוא לטכנולוגיות אלו לא צלחו עד כה. בשנת 2020 דחה בית המשפט המחוזי בתל אביב את תביעתם של שלושים פעילי ארגון אמנסטי הבינלאומי להורות למשרד הביטחון לבטל את רישיון היצוא שניתן לחברת NSO.[303] בעתירה שהוגשה בשנת 2021 נגד משרד הביטחון בבקשה למנוע יצוא של נוזקות מעקב של חברת Cellebrite לגוף הכפוף לנשיא רוסיה, פסק בג"ץ כי ביקורת שיפוטית מטעמו תופעל רק במקרים חריגים. שופטי בית המשפט העליון שטיין, ברון ומינץ פסקו כי "כבשאר העניינים של יחסי חוץ וביטחון,

301 מאיר אורבך "משרד הביטחון קיצץ בשני שליש את מספר המדינות שחברות הסייבר יכולות למכור להן" **כלכליסט** (25.11.2021); אודי עציון "משרד הביטחון ביטל רישיונות יצוא לחברות בתחום הסייבר ההתקפי" **כלכליסט** (16.6.2022).

302 טל שחף "תקנות הייצוא החדשות חונקות את חברות הסייבר ההתקפי הישראלי" **Tech12** (16.6.2022).

303 עת"מ (מנהליים ת"א) 28312-05-19 **מלקאר נ' ראשת אגף הפיקוח על הייצוא הביטחוני** (12.7.2020).

שיקול הדעת המצוי בידי רשויות המדינה הינו רחב במיוחד".[304] שתי תביעות משפטיות נוספות הוגשו נגד חברת NSO בגין פגיעה בזכויות אדם שבוצעה באמצעות נוזקת המעקב פגסוס שפיתחה, ועודן מתנהלות בבית המשפט המחוזי בתל אביב: האחת הוגשה בידי חמישה עיתונאים ממקסיקו והשנייה בידי עומר עבד אלעזיז אלזהרני, סעודי תושב קנדה וחברו של העיתונאי המנוח ג'מאל חשוקג'י. על שתיהן הטיל בית המשפט צו איסור פרסום.[305]

4.4.2. שימוש רשויות הביון והאכיפה בנוזקות מעקב

לרשויות אכיפת החוק והביון בישראל פטור רחב מאחריות בגין פגיעה בזכות לפרטיות. כך, סעיף 19(ב) לחוק הגנת הפרטיות, התשמ"א-1981 קובע שאם רשות ביטחון, עובדיה או הפועל מטעמה פגעו בזכות לפרטיות לפי החוק, אך הפגיעה בפרטיות נעשתה במסגרת תפקידו של הפוגע או לשם מילויו ועומדת במבחן סבירות, אזי הפגיעה מותרת.[306]

חוק שירות הביטחון הכללי, התשס"ב-2002, קובע בסעיף 8(א)(1) שלצורך מילוי תפקידו השב"כ, באמצעות עובדיו, מוסמך לקבל ולאסוף מידע. סעיף 18 לחוק קובע סייג כללי לאחריות פלילית או אזרחית, שאינו מתייחס במפורש

304 בג"ץ 1942/21 **אגמון נ' מנכ"ל משרד הביטחון** (אר"ש 27.6.2021).

305 Siena Anstis, *Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry*, The Citizen Lab (Dec. 12, 2018); Raphael Satter, *Lawsuit Lays Bare Israel-Made Hack Tools in Mideast, Mexico*, Associated Press (Sep. 1, 2018); David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, The New York Times (Dec. 2, 2018); ביני אשכנזי "האם מערכת המשפט מגוננת על NSO?" **וואלה!** (8.2.2022).

306 בדיון הראשון בפרשת **ועקנין** (בג"ץ 249/82 **ועקנין נ' בית הדין הצבאי לערעורים**, פ"ד לז(2) 393 (1983)), פסק השופט בך בדעת הרוב כי השקיית המערער במי מלח מהווה הטרדה אחרת לפי סעיף 2(1) לחוק הגנת הפרטיות ויכולה להתבצע רק מכוח הסמכה מפורשת בחוק, וסעח, 19(ב) לחוק הגנת הפרטיות אינו מהווה הסמכה שכזו. נוסף על כך, ולמעלה מן הצורך, קבע השופט בך שהפעולה אינה עומדת במבחן הסבירות הנדרש בסעיף 19(ב). לבד מפסק דין זה בתי המשפט לא עסקו בפרשנות שיש לתת לסעיף 19(ב).

לפגיעה בפרטיות, שלפיו עובד השב"כ או הפועל מטעמו לא יישאו באחריות פלילית או אזרחית למעשה או מחדל שנעשה בתום לב, במסגרת תפקידם או לשם מילויו ועומד במבחן סבירות.

בינואר 2022 דווח בתקשורת הישראלית שמשטרת ישראל מבצעת פעולות אקטיביות עצמאיות למעקב טכנולוגי אחר אזרחים, לעיתים ללא קשר לחקירה מתנהלת או לבירור חשדות לביצוע עבירות פליליות ומבלי שהתקבל צו שיפוטי, באמצעות תוכנת פגסוס של חברת NSO. בתגובה לפרסומים מונה בסוף אותו חודש צוות בדיקה בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי) עו"ד עמית מררי. צוות הבדיקה בחן, באופן מדגמי ובסיוע NSO וחברה נוספת שהמשטרה השתמשה במוצריה, כ־25 מקרים שבהם המשטרה השתמשה במערכות מיום הפעלתן הראשונית ועד מועד הבדיקה. נמצא שבמקרים שנבדקו פעלה משטרת ישראל כאשר ברשותה היתר כדין, למעט בארבעה מקרים: בשני מקרים ניתן צו להאזנת סתר, אך לא מסוג של האזנה לתקשורת בין מחשבים לטלפון נייד; במקרה אחד ניסיון ההדבקה נעשה בסמיכות למועד פקיעת הצו; ובמקרה נוסף לא אותר היתר כדין. בכל ארבעת המקרים הללו לא צלח ניסיון ההדבקה בנוזקת המעקב. לפיכך הסיק צוות הבדיקה שאין כל אינדיקציה לכך שמשטרת ישראל הדביקה או ניסתה להדביק בנוזקת מעקב, ללא צו משפטי, מכשיר טלפון של מי מבין רשימת האנשים שפורסמה בתקשורת. כן נמצא שאין אינדיקציה להדבקה או לניסיונות הדבקה של מי מרשימת אנשים אלו באמצעות המערכת הנוספת שבידי משטרת ישראל.[307]

עם זאת, צוות הבדיקה מצא שנוזקת המעקב פגסוס אפשרה איסוף ועיבוד מידע מעבר למידע המותר לפי חוק האזנת סתר, בשתי דרכים: ראשית, המערכת מאפשרת איסוף וגישה למידע שנוצר קודם למתן הצו; שנית, המערכת מאפשרת איסוף מידע שאינו תקשורת – למשל פרטי יומן, אנשי קשר ופתקים האגורים במכשיר הטלפון הנייד. רק באפריל 2020 הוטמעו בנוזקה חסימות טכנולוגיות שמונעות איסוף מידע עודף ושאיבה של מידע שנצבר קודם למועד המותר בצו. קודם לכן, אי־השימוש במידע עודף ואיסור

307 הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים **דין וחשבון** 6 (2022).

איסוף מידע קודם למועד הצו נשענו על נהלים פנימיים בלבד. מסקנת צוות הבדיקה הייתה ש"המשמעות הדרמטית של הכנסה לשימוש של מערכת בעל יכולות טכנולוגיות רחבות היקף המהווה נקודת מפנה מבחינת עולם האזנות הסתר, לא הובנה לאשורה על ידי גורמי המשטרה הרלוונטיים".[308]

בדיון בנושא בוועדת החוקה, חוק ומשפט של הכנסת התגלתה תמונה מטרידה העולה כדי כשל רב־מערכתי של שומרי הסף בהבנת הטכנולוגיה ויכולותיה בעת שאישרו למשטרה לעשות בה שימוש. כך, עו"ד מררי אישרה כי מנגנוני הפיקוח כלל לא נתנו דעתם לתכונותיה של נוזקת המעקב פגסוס אשר אפשרו חדירה לתכנים מעבר לאלו המותרים לפי חוק האזנת סתר. אף בתי המשפט, אשר נדרשו לאשר את צווי האזנת הסתר, לא בחנו אם נוזקת המעקב פגסוס יכולה לאפשר למשטרה חדירה למידע מעבר למבוקש בצו לפי חוק האזנת סתר. גם ראש מחלקת הסייבר בפרקליטות המדינה, ד"ר חיים ויסמונסקי, אשר בשנת 2018 התבקש על ידי המשטרה לחוות דעתו על השימוש שהיא עושה בנוזקת המעקב פגסוס, העיד כי בעת כתיבת חוות דעתו לא ידע שהמערכת מאפשרת גם חיפוש סמוי, כלומר העתקה של תכנים האגורים במכשיר הסלולר. עם זאת, בחוות דעתו משנת 2018 הזהיר ויסמונסקי את המשטרה לבל תבצע חיפוש סמוי שאינו בסמכותה החוקית. רק לאחר חשיפת הפרשה בתקשורת החלו בפרקליטות לבחון אם השימוש שעשתה המשטרה בנוזקת המעקב פגסוס חרג מגבולות המותר לפי חוק האזנת סתר. עוד ציינה עו"ד מררי כי צוות הבדיקה ערך בדיקה מדגמית בלבד ואין בה כדי להבטיח שבאף אחד מלמעלה מ־1,000 המקרים שבהם נעשה שימוש בנוזקה לא אירעה זליגת מידע ולא נעשו שימושים בלתי חוקיים בו.[309] ביולי 2023 מתח שר המשפטים לוין ביקורת על ועדת מררי, שלדבריו לא הייתה בלתי תלויה, נעדרה סמכויות חקירה וביצעה בדיקות מדגמיות בלבד. לפיכך החליט שר המשפטים להקים ועדת בדיקה ממשלתית לבדיקת השימוש בנוזקות מעקב בשירות המשטרה. לפי הפרסומים בתקשורת, הוועדה תבדוק את השימוש בכמה תוכנות, בהן

308 שם.

309 תומר גנון "מררי: 'התגלה כשל מערכתי, למדנו עליו מהפרסום ב'כלכליסט'" **כלכליסט** (1.5.2023); "בניגוד להכחשות, כבר ב־2018 הוזהרה המשטרה משימוש בפגסוס" **כלכליסט** (3.4.2023).

מערכת "סייפן" ונוזקת המעקב פגסוס, שגרסה מוחלשת שלה פותחה עבור המשטרה, וכן תבחן את התנהלות המשטרה, הפרקליטות ומערכות הפיקוח עליהן, בכל הקשור לרכש של כלי סייבר אזרחיים ומעקב ואיסוף באמצעותם.[310]

4.5. סיכום סקירת המשפט המשווה

תעשיית נוזקות המעקב נתונה לרגולציה ולפיקוח קפדני בכל הנוגע ליצוא הטכנולוגיה. אולם על אף החודרנות הגבוהה שמאפשרות נוזקות המעקב והסכנה הממשית הנלווית לשימוש בהן בידי גורמי קיצון ובהיעדר פיקוח, הפעילות בתעשיית נוזקות המעקב אינה מאוסדרת במלואה בהיבט של הפגיעה בזכות לפרטיות, לא במישור הבינלאומי ולרוב גם לא במישור המקומי.[311]

במישור הבינלאומי, הסדר ואסנאר הוא הסדר וולונטרי, חסר כלים לאכיפת הוראותיו, וממילא מתמקד אך ורק בשיקולים של ביטחון המדינה ויחסי החוץ שלה. גם הכללים המנחים של האו"ם לחברות פרטיות אינם נותנים מענה מספק לאסדרת ההגנה על הזכות לפרטיות בתעשיית נוזקות המעקב, שכן מדובר בכללים וולונטריים הנעדרים מנגנון יעיל לבחינת הציות להם או לאכיפתם. בהתאם, גם יישום הסדר ואסנאר ברמה המדינתית בארצות הברית ובישראל אינו מספק. באיחוד האירופי, לעומת זאת, רגולציית המוצרים הדו־שימושיים מסמיכה את המדינות החברות באיחוד לאסור או להטיל דרישות רישוי על יצוא מוצרים דו־שימושיים, שאינם מנויים ברגולציה, מטעמי הגנה על זכויות אדם.

310 חן מענית "פרשת פגסוס: לוין מקים ועדת בדיקה ממשלתית לשימוש ברוגלות בידי המשטרה" **הארץ** (20.7.2023).

311 Farrow, **לעיל** ה"ש 2; Deibert, **לעיל** ה"ש 6.

יתרה מכך, יש לתת את הדעת לחסרונות משטר הפיקוח על היצוא בכל הנוגע לנוזקות מעקב. הצבת שיקולי ביטחון המדינה ויחסי החוץ שלה בראש סדר העדיפויות תוך התעלמות מפגיעה אפשרית של הטכנולוגיה המיוצאת בזכויות אדם, ובראשן הזכות לפרטיות, העניקה מעטה חוקיות, לכאורה, למוצריהן של חברות פרטיות. כמו כן, מסגרת אסדרתית זו לא יצרה כל תמריץ לחברות הפרטיות לבחון את השלכות הטכנולוגיות שהן מפתחות על זכויות אדם במדינה שהיא יעד היצוא. כמו כן, מדינות רבות כלל אינן מקיימות משטר פיקוח על יצוא טכנולוגיות דו־שימושיות, ועל כן הן מהוות בפועל מדינות מקלט לחברות המבקשות לפתח נוזקות מעקב ללא ביקורת ציבורית ומבלי שייאלצו לציית לדרישות המחמירות של מדינות המערב הדמוקרטיות.[312]

לצד הסדר ואסנאר ואסדרת הפיקוח על היצוא של נוזקות מעקב, בכל משטר משפטי מהמשטרים שנבדקו קיימות הוראות בנוגע לשימוש של רשויות ביון ואכיפת חוק בנוזקות מעקב, אם כי נראה שגם הן אינן נותנות מענה מספק לפגיעה החמורה בזכות לפרטיות המתאפשרת עקב שימוש לא חוקי בנוזקות מעקב. כך, בארצות הברית השימוש של רשויות ביון ואכיפה בנוזקות מעקב מותר אף אם הוא יוביל לפגיעה חמורה בזכות לפרטיות, כל עוד זו תהיה מוצדקת מטעמים של ביטחון המדינה או אכיפת החוק, בכפוף למבחן המידתיות ולדרישת הנחיצות. יוזמות החקיקה של הקונגרס ושל ממשל ביידן בנושא מתמקדות בעיקר במניעת דריסת רגל של חברות מסחריות זרות בקרב רשויות האכיפה והביון האמריקניות. בישראל נהנות רשויות אכיפת החוק והביון מפטור רחב יחסית המתיר פגיעה בזכות לפרטיות כל עוד היא עומדת במבחן הסבירות ונעשית במסגרת התפקיד או למענו. עם זאת, ועדת מררי, אשר קבעה כי עיקר השימוש שעשתה המשטרה בנוזקות מעקב היה כדין, הצביעה על כך שהמשטרה לא הביאה בחשבון את המשמעות הדרמטית של השימוש בנוזקת מעקב מבחינת רמת החודרנות שהיא מאפשרת. אי־הבנה של חודרנות השימוש בנוזקת מעקב הייתה גם מנת חלקם של שומרי הסף בפרקליטות. באיחוד האירופי רשאיות רשויות האכיפה והביון בכל מדינה לעשות שימוש בנוזקות מעקב בכפוף לצ'רטר זכויות האדם האירופי, האמנה

312 אסף גלעד "כולן רוצות להיות NSO: למרות הביקורת, תעשיית הסייבר ההתקפי מתפוצצת ובכירי אמ"ן מתברגים בצמרתה" **גלובס** (13.8.2021).

האירופית לזכויות אדם, אמנה 108+ והדירקטיבה להגנה על מידע אישי בידי רשויות אכיפת חוק. במסגרת זו מותרת פגיעה בפרטיותו של אדם רק אם היא נעשית למטרה מוגדרת של שמירה על ביטחון לאומי, שמירה על ביטחון הציבור או מניעה, גילוי וחקירה של עבירות פליליות והבאת מבצעיהן לדין, בהתאם לחוק מדינתי ספציפי ובהתאם לדרישת הנחיצות ולמבחן מידתיות.

האיחוד האירופי מציג מענה מסוים להגנה על פרטיותו של משתמש הקצה מפני חדירתה של נוזקת מעקב בדמות הצעת חוק חוסן הסייבר, המחייבת הטמעת שיקולי הגנת פרטיות כבר בשלב פיתוח נוזקת מעקב, אך יש להמתין לאישור ההצעה ולעקוב אחר הטמעת החוק בכל אחת מהמדינות החברות באיחוד. יתרה מכך, אף שהצעת חוק החוסן היא צעד חשוב לחיזוק הגנת הסייבר במוצרי צריכה דיגיטליים, תעשיית נוזקות המעקב משקיעה מאמצים כבירים באיתור חולשות יום אפס במוצרי צריכה העומדים בתקני הגנת סייבר מחמירים, ועל כן החוק עשוי שלא להיות יעיל דיו בחסימת פעולתן של נוזקות מעקב. כן ייתכן שחיזוק ההגנה על פרטיותו של משתמש הקצה למול תעשיית נוזקות המעקב יגיע דווקא מהכרעות בתי המשפט בארצות הברית בתביעות התלויות ועומדות כיום נגד חברת NSO בגין השימוש שעשו לקוחותיה בנוזקת המעקב פגסוס, אולם יש להמתין לשם כך לבירורן של התביעות.

גם הפתרונות שהוצעו במישור הבינלאומי אינם מספקים. כך, למשל, סביר שמדינות רבות יסרבו לשתף פעולה עם הפסקה מלאה של מכירה וקנייה של נוזקות מעקב. גם סגירתה של חברה המפתחת נוזקת מעקב, או חשיפת החולשה שבה היא משתמשת ופרסום עדכון אבטחה מתאים, לא יובילו לפתרון ממשי לפגיעה החמורה בזכות לפרטיות. פעולות אלו אולי יועילו בהקשר של נוזקת מעקב מסוימת, אולם תעשיית נוזקות המעקב היא תעשייה משגשגת ובה חברות אחרות רבות שממשיכות וימשיכו לפעול, ויש להן תמריץ לאתר חולשות ולאפשר את המשך ההפעלה של נוזקות המעקב שבפיתוחן. כל עוד השוק אינו מאוסדר וכל עוד ניתנת עדיפות לחדשנות על פני אבטחה ועל פני הגנה על הפרטיות, מצב זה יימשך.[313]

313 Deibert, **לעיל** ה"ש 6.

במישור זה נדמה שפתרונות אפשריים ראויים הם דרישה ממדינות הרוכשות רישיונות שימוש בנוזקות מעקב לעשות כן בשקיפות ורק לאחר שווידאו שהחברה שממנה הן רוכשות עומדת בדרישות הבינלאומיות להגנה על זכויות אדם. כמו כן, מדינות יכולות להחמיר את המגבלות שהן מטילות על יצוא טכנולוגיות דו־שימושיות למעקב כדי למזער את הסיכון שאלו יימכרו למשטרים שיעשו בהם שימוש המפר זכויות אדם. צעד אפשרי נוסף הוא הענשת חברות טכנולוגיות המעקב ישירות, בדומה לצעד שנקטה ארה"ב נגד NSO, Cytrox ו־Intellexa, בהכנסתן לרשימה השחורה של החברות שאין לספק להן מוצרים תוצרת ארצות הברית אלא באישור מחלקת המסחר האמריקנית. זהו צעד חמור שעשוי להקשות על חברות אלו להמשיך להתקיים. לבסוף, מדינות יכולות לחוקק חוק הקובע שהנפגעים מנוזקות מעקב יכולים לתבוע את החברות המפתחות את הטכנולוגיה.[314] עם זאת, בחינת מסגרת משפטית מדינתית ובינלאומית מתאימה לפיקוח על פיתוח, שיווק ויצוא של טכנולוגיות מעקב, וכן לפיקוח על השימוש בהן, אינה מעניינו של מחקר זה. מחקר זה מבקש לבחון כיצד מי שפרטיותו נפגעה בשל שימוש בנוזקת מעקב יכול לקבל סעד לנזקיו, למשל באמצעות אימוץ דוקטרינת ההפרה התורמת מדיני זכויות היוצרים.

314 שם.

פרק 5

אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות – הבסיס העיוני ושיקולי המדיניות

בפרקים הקודמים עסקנו בהתפתחותה ובתנאיה של דוקטרינת ההפרה התורמת בדיני זכויות היוצרים ובמהותה וחשיבותה של הזכות לפרטיות. בחנו את תעשיית נוזקות המעקב ואת הפגיעה החמורה בזכות לפרטיות המתאפשרת באמצעות שימוש בלתי חוקי בהן, ועמדנו על הלקונה בדין הקיים בכל הנוגע לסעדים העומדים לרשותו של מי שזכותו לפרטיות נפגעה עקב שימוש כאמור בנוזקת מעקב. עתה הגיעה העת לבחון את אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכל הקשור לשימוש לא חוקי בנוזקות מעקב.

אימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים בישראל נשען על סעיף 12 לפקודת הנזיקין,[315] שדיני זכויות היוצרים נחשבים חוקי לוויין שלה.[316] בישראל, פגיעה בפרטיות היא עוולה אזרחית והוראות פקודת הנזיקין חלות עליה.[317] לפיכך אפשר, לכאורה, לאמץ את דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות תוך שימוש באותו בסיס נורמטיבי – צינור הקליטה הקבוע בסעיף 12 לפקודת הנזיקין, שלשונו: "לעניין פקודה זו, המשתף עצמו, מסייע, מייעץ או מפתה למעשה או למחדל, שנעשו או שעומדים להיעשות על ידי זולתו, או מצווה, מרשה או מאשרר אותם, יהא חב עליהם".

דוקטרינת ההפרה התורמת בדיני זכויות יוצרים היא כלי משפטי להרחבת מעגל האחראים בנזיקין. בעזרתה עשויים גורמי הביניים – למשל יצרני מוצר טכנולוגי, ספקי גישה לאינטרנט, בעלי אתרים שונים שבהם מועבר מידע, מפעילי פלטפורמות של רשתות חברתיות ומנועי חיפוש – לשאת באחריות תורמת להפרת זכות היוצרים בידי משתמשי הקצה. ההכרעה בשאלת הטלתה

315 סעיפים 11 ו־12 לפקודת הנזיקין.

316 פישמן אפורי, **לעיל** ה"ש 22, בעמ' 10; בירנהק "לידתה של עוולה", **לעיל** ה"ש 90, בעמ' 173.

317 סעיף 4 לחוק הגנת הפרטיות.

של אחריות תורמת על גורמי הביניים, כלומר בשאלה אם הם צריכים לשמש שומרי סף ולשאת באחריות להתנהגות פסולה שלא הם ביצעו, תלויה בשיקולי מדיניות ויעילות אכיפה.[318] האימוץ של דוקטרינת ההפרה התורמת לדיני זכויות יוצרים סימן את האיזון הראוי, לפי שיקולי מדיניות, בין חדשנות טכנולוגית לבין הזכות הקניינית של יוצרים.[319] הקביעה אם נתבע חב באחריות תורמת להפרת זכות יוצרים מבוססת בסופו של דבר על איזון בין המחיר החברתי והכלכלי שבפגיעה בזכות יוצרים, המחיר הכלכלי והחברתי שבהפיכת צדדים שלישיים לזרוע האכיפה הארוכה של בעל זכות היוצרים והפגיעה בחדשנות ובשימושים מותרים אפשריים.[320]

אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יוביל לתוצאה זהה של הרחבת מעגל האחראים להפרת הזכות לפרטיות מעבר למפר הישיר. מבחינה זו האימוץ מחזק את הזכות לפרטיות באמצעות יצירת עוולה חדשה המשנה את האיזון הקיים בין אינטרס הציבור לבין הזכות לפרטיות. משום כך, קודם להחלטה בדבר אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יש לבחון את הבסיס העיוני להצדקת אימוצה ואת שיקולי המדיניות ויעילות האכיפה הרלוונטיים, ולהתמודד עם הקשיים המרכזיים שאימוצה עשוי לעורר.[321] בחינה זו תביא בחשבון גם את ההבדלים ונקודות הדמיון בין זכות היוצרים, שהיא זכות קניינית במהותה, לבין הזכות לפרטיות.

318 פישמן אפורי, **לעיל** ה"ש 22, בעמ' 4.

319 Moye, **לעיל** ה"ש 11, בעמ' 653.

320 Yen, **לעיל** ה"ש 40, בעמ' 214.

321 בדומה למה שהתרחש עם אימוצה של העוולה לדיני הפטנטים ומאוחר יותר לדיני זכות היוצרים. ראו בירנהק "לידתה של עוולה", **לעיל** ה"ש 90, בעמ' 186–196.

5.1. שיקולי מדיניות המצדיקים את אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכלל, ובהקשר של נוזקות מעקב בפרט

5.1.1. חיזוק הזכות לפרטיות והערכים שבבסיסה

בדומה לדוקטרינת ההפרה התורמת בדיני זכויות היוצרים, שהביאה להרחבת זכות הקניין הרוחני בפטנט או ביצירה,[322] אימוצה של דוקטרינת הפרה תורמת לדיני הגנת הפרטיות יוביל לחיזוקה של הזכות לפרטיות על ידי הרחבת מעגל האחראים להפרתה. לאחר שנים של התפתחויות טכנולוגיות שהובילו לשחיקתה של הזכות לפרטיות,[323] חיזוק הזכות לפרטיות הוא הכרחי. מדובר בזכות שיש לה חשיבות ניכרת לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו וללא התערבות זרה.[324]

כמו כן, שוקי המידע מאופיינים בכמה כשלי שוק המונעים הגנה ראויה על הזכות לפרטיות ומצדיקים התערבות חיצונית שנועדה לחזקה. ראשית, לפגיעה בזכות לפרטיות מגוון החצנות שליליות שלחברות המסחריות אין תמריץ למנוע אותן. כך, עיבוד מידע אישי על אדם עשוי להשפיע על צד שלישי. לדוגמה, מודלים של ניתוח תחזיתי המשתמשים בנתונים כדי לחזות אירועים או התנהגויות עתידיות עשויים להצביע על מאפיינים ולעיתים על אשמה של צד שלישי בהתבסס על מידע אישי על חברים או משפחה. החצנה שלילית נוספת, הבאה לידי ביטוי חריף במקרה של נוזקות מעקב, היא היכולת לאסוף ולנתח מידע אישי לא רק על בעל המכשיר שאליו הוחדרה נוזקת המעקב, אלא גם על כל מי שבסביבתו או מתקשר עימו.

322 **שם**, בעמ' 193–195.

323 ראו, למשל, Zuboff, **לעיל** ה"ש 158.

324 להרחבה בנוגע לחשיבותה של הזכות לפרטיות ראו הדיון בסעיף 2 **לעיל**.

כשל שוק חמור נוסף המצדיק רגולציה לחיזוק הזכות לפרטיות הוא מידע א־סימטרי. בהקשר של נוזקות מעקב הכשל ברור, שכן הנוזקה מותקנת בחשאי, ללא ידיעתו של נושא המידע וממילא מבלי שיבין מהו השימוש הצפוי במידע האישי עליו. אולם כשל שוק זה מתקיים גם בהקשרים מסחריים שגרתיים. לרוב מנוסחת מדיניות הפרטיות של החברות המסחריות בהרחבה ובצורה מעורפלת. מאחר שעיקר מטרתן של החברות במתן השירות או המוצר היא איסוף מידע אישי על הצרכנים, אין להן תמריץ ליצור מדיניות פרטיות ברורה וקצרה שתאפשר לצרכנים ללמוד בקלות ובבהירות איזה מידע נאסף עליהם ולאילו מטרות. משום כך, התעמקות במדיניות הפרטיות והבנת היקף המידע האישי שייאסף והשימוש הצפוי בו כרוכות בעלויות עסקה גבוהות, וצרכנים נמנעים בדרך כלל מלשאת בהן ומסכימים לאיסוף מידע עליהם ולשימוש בו באופן עיוור מבלי להביע את עמדותיהם האמיתיות, ואף מבלי לדעת או להבין את השלכות איסוף זה. כמו כן, קשה עד בלתי אפשרי לאתר בדיעבד מי החברה האחראית לשימוש מזיק במידע אישי, ולכן בדרך כלל השוק אינו מצליח להזהיר צרכנים מפני חברות שנהגו בעבר בחוסר הוגנות.[325]

כשל שוק חשוב נוסף המאפיין שוקי מידע אישי הוא כשל השוק המוכר של פעולה קולקטיבית: כדי להגן על הזכות לפרטיות, למשל, באמצעות מאבק בחברה מסחרית בדרישה שזו תשנה את מדיניות הפרטיות שלה, או באמצעות מעבר לשירות רשת חברתית מתחרה המגן יותר על הזכות לפרטיות תוך שימור יתרונותיו של אפקט הרשת (network effect), יש צורך בפעולה משותפת של יחידים רבים. אולם פעולה זו אינה אפשרית כאשר מדובר ביחידים מבוזרים. וכך, בעוד להצלתה של זכות היוצרים נרתמו תאגידי ענק בעלי כוח וממון שהיה בכוחם לנהל מאבקים משפטיים ארוכים ולהפעיל שדלנים בבתי המחוקקים בארצות הברית, כל אחד ואחד מאיתנו, המחזיק בזכות החוקתית לפרטיות, אינו משופע במשאבים כספיים ואנושיים, ברצון או במודעות לנזק שעשוי להיגרם לו, הדרושים כדי לצאת להגנת פרטיותו. המאבק להגנתה של הזכות

325 Lev-Aretz & Strandburg, *Privacy Regulation* **לעיל** ה"ש 9, בעמ' 285–287, 289–290.

לפרטיות נותר אפוא נחלתם של מעטים, ארגוני החברה האזרחית ופעילי זכויות אדם.[326]

ההחצנות השליליות ושלל כשלי השוק שתוארו לעיל מובילים למסקנה שכוחות השוק אינם יכולים ללמד על העדפותיהם האמיתיות של הצרכנים בנוגע לשימוש במידע אישי עליהם ואף אינם יכולים לספק הגנה ראויה על הפרטיות. כמו כן, היכולת לאסוף, לעבד ולנתח מידע אישי באופן ממוחשב מתוך כמויות עצומות של מידע ממקורות שונים, מאפשרת לחברות להסיק מידע אישי ממקורות שאין לנושא המידע כלל שליטה עליהם. התוצאה היא החרפת כשלי השוק שתוארו לעיל והפיכת תיקונם על ידי השוק עצמו לבלתי אפשרי. למשל, אף אם חברות יפעלו בשקיפות מלאה באשר למידע שהן אוספות מנושא המידע ובאשר למידע שהן משלבות ממקורות אחרים, ללא הבנת האלגוריתם אשר משמש אותן לעיבוד המידע ולהסקת מסקנות ממנו לא יוכל הצרכן להעריך מראש את המחיר שייגבה ממנו בפועל עקב השימוש באותו מידע אישי. משום כך, בחירותיו של הצרכן לא ישקפו את העדפותיו האמיתיות בשאלת ההגנה על פרטיותו. זאת ועוד, האיסוף והעיבוד של נתוני עתק ממקורות שונים מקשים על איתור האחראי לפגיעה בפרטיות. כן מוחמרת ההחצנה השלילית של פגיעה בצדדים שלישיים – אלו יהיו נושאי מידע שכלל לא הסכימו לאיסוף ועיבוד מידע אישי עליהם, אולם אפשר להסיק מידע אישי עליהם מאגרגציה ועיבוד של מידע אישי של אנשים דומים להם, קרובים אליהם או נמצאים באותה קבוצה או אזור גיאוגרפי.[327]

יתרה מזו, כוחות השוק מתייחסים למידע אישי כאל כל סחורה אחרת ולכן מתעלמים מערכים חשובים שבבסיסה של הזכות לפרטיות, אשר נפגעים בשל שימוש לא ראוי במידע אישי. הזכות לפרטיות אינה זכות קניינית כזכות היוצרים אלא זכות יסוד חוקתית הנגזרת מזכותו של אדם לכבוד ולאוטונומיה. שלל הגישות התיאורטיות מצביעות על כך שמדובר בזכות החיונית למימוש

326 ראו, למשל, Zuboff, **לעיל** ה"ש 158; Yafit Lev-Aretz & Katherine J. Strandburg, *Regulation and Innovation: Approaching Market Failure from Both Sides*, 38:1 Yale J. on Regul. Bull. (2020)

327 Lev-Aretz & Strandburg, *Privacy Regulation* **לעיל** ה"ש 9, בעמ' 291–296.

כבודו של האדם, והכרחית לגיבוש זהותו ותפיסתו העצמית, לקבלת החלטות עצמאית ולהגנה מפני מבטו הממשטר של האחר. זוהי גם זכות החיונית לשם הגנה על זכויות אחרות כגון הזכות לחופש ביטוי ולשוויון.[328] הסמנים שהשוק מספק בנוגע להגנת הפרטיות המבוקשת על ידי הצרכנים או הרצויה מבחינה חברתית מטעים ומעודדים דווקא טכנולוגיות של מעקב ואיסוף מידע, ובה בעת – התמריצים לפיתוח תחומי חדשנות אחרים ויעילים חברתית, שלשם פיתוחם דווקא נדרשת הגנת פרטיות המאפשרת חשיבה יצירתית ועצמאית, מצויים בחסר.[329] לפיכך כוחות השוק אינם מסוגלים להתוות הגנה ראויה לזכות לפרטיות. בכך יש כדי להצדיק יוזמות רגולטוריות לחיזוק ההגנה על פרטיות במידע.

חיזוק הזכות לפרטיות הוא בעל משמעות יתרה דווקא בישראל. הזכות לפרטיות מעוגנת אומנם כזכות יסוד חוקתית בחוק־יסוד: כבוד האדם וחירותו,[330] אולם היקפה ואכיפתה מוגדרים באמצעות חוק הגנת הפרטיות, שהוא חוק מיושן שאינו מותאם למציאות הדיגיטלית. עדכונו האחרון של חוק הגנת הפרטיות אומנם משמעותי, אך הוא מוגבל בעיקרו לחיזוק סמכויות האכיפה של הרשות להגנת הפרטיות וחסר הוראות הנוגעות להגנה מהותית על הזכות לפרטיות.[331]

זאת ועוד, בשנים האחרונות נדמה שישראל הופכת ל"חצר האחורית" של מדינות המערב הדמוקרטיות בכל הקשור להגנת הפרטיות. התקנתן של תקנות הגנת הפרטיות לשימור מעמד הנאותות בחודש מאי 2023[332] רק מדגישה את חולשתה של הזכות לפרטיות בישראל ומגבירה את החשש ממיצובה של ישראל כ"חצר אחורית". מטרת תקנות אלה היא לעמוד בדרישות

328 Westin, **לעיל** ה"ש 124; בירנהק **מרחב פרטי**, **לעיל** ה"ש 120, בעמ' 89–99; כן ראו הדיון בפרק 2 **לעיל**.

329 Cohen, *What Privacy* **לעיל** ה"ש 150, בעמ' 1918–1927.

330 סעיף 7 לחוק־יסוד: כבוד האדם וחירותו.

331 חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד–2024, ס"ח 3287, עמ' 1430.

332 תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג–2023, ק"ת 1720 (להלן: תקנות הגישור).

האיחוד האירופי כדי לקבל להכרה בתאימות של דיני הגנת הפרטיות בישראל לאלו הנהוגים באיחוד. אולם לשם מטרה זו הן מעניקות זכויות יתר רק לנושאי מידע שהמידע עליהם מגיע לישראל מהאזור הכלכלי האירופי.[333] נושאי מידע שמידע עליהם מגיע מישראל, קרי כל נושאי המידע הנמצאים במדינת ישראל, אינם זכאים לאותן הזכויות ונשארים נתונים להגנה מצומצמת, ארכאית ובסופו של דבר חלשה של חוק הגנת הפרטיות הקיים.[334] במצב זה יהיה אפשר, למשל, לבצע בישראל מחקרי נתונים תוך שימוש במידע אישי על אזרחיה, בתנאים מקילים בהרבה מאלו הנדרשים במדינות אחרות, ואולי אף לבצע ניסויים כאמור שאסור לבצעם במדינות דמוקרטיות מערביות אחרות.

אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יעניק לנושא המידע כלי אזרחי שבאמצעותו יוכל לתבוע את נזקו מהגורמים אשר תרמו לפגיעה בפרטיותו ולקבל סעד אפקטיבי שיהיה בו גם כדי להרתיע מפני סיוע דומה לפגיעה בפרטיות בעתיד. כך, עקב בצד אגודל, יהיה אפשר לחזק את הזכות לפרטיות למול ההתפתחויות הטכנולוגיות, ובישראל גם למול חולשתו וכישלונו של המחוקק בנושא. אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות אף עולה בקנה אחד עם מגמת החקיקה הבינלאומית, שהאיחוד האירופי הוא ממוביליה,[335] של חיזוק הזכות לפרטיות במידע נוכח הדיגיטציה הגוברת של חיי היום־יום והפיכתו של מידע אישי למטבע סחיר רב ערך.

333 האזור הכלכלי האירופי מוגדר ככולל את המדינות החברות באיחוד וכן את איסלנד, נורווגיה וליכטנשטיין. ראו **שם**, בסעיף 1.

334 להרחבה ראו רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר "טיוטת תקנות הגנת הפרטיות עלולה לפגוע בעיקרון השוויון ולהביא לזעם בציבור" **המכון הישראלי לדמוקרטיה** (19.4.2023). עם זאת, יש לציין שהחל מ־1 בינואר 2025, הוראות תקנות הגישור יחולו גם על מידע אישי על נושאי מידע מישראל המצוי באותו מאגר מידע עם מידע אישי על נושאי מידע שהועבר מהאזור הכלכלי האירופי, למעט מידע אישי שהועבר במישרין מנושא המידע. ראו סעיף 2(2) ו־9 לתקנות הגישור, **לעיל** ה"ש 332.

335 עם חקיקת ה־GDPR (**לעיל** ה"ש 123) בשנת 2016 וכניסתן לתוקף במאי 2018.

5.1.2. מונע הנזק הזול

אחת ההצדקות לאימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים הייתה היותו של הנתבע, יצרן הטכנולוגיה, מונע הנזק הזול. עקרון מונע הנזק הזול נשען על שני מבחנים. המבחן הראשון בוחן אם גורם הביניים אשר פיתח את הטכנולוגיה שבה נעשה שימוש לרעה לשם הפרת זכויות היוצרים ההמונית והחמורה הוא גם הגורם שסביר להטיל עליו את האחריות לעצירתה או למניעתה של ההפרה. סבירות הטלת האחריות נבחנת לפי יכולתו של גורם הביניים, מבחינה כלכלית, לעצור את ההפרה או למנוע אותה מראש. אם גורם הביניים הוא צוואר הבקבוק או החוליה בשרשרת הפעולות המובילות להפרת זכות הקניין הרוחני, וביכולתו לפקח ביעילות ובאופן פשוט וזמין יחסית על המפירים הישירים, להפסיק את שיווק הטכנולוגיה או לשנותה באופן אשר ימנע את המשך השימוש לרעה בה, סביר לראות בו מונע הנזק הזול.[336] המבחן השני נשען על שיקולים של צדק חלוקתי ובוחן אם קיים אינטרס ציבורי המצדיק את הסטת עלויות הפיקוח המצטברות מבעל זכות היוצרים לגורם הביניים.[337]

יישום מבחנים אלו לדיני הגנת הפרטיות בהקשר של נוזקות מעקב מציג תמונה מורכבת. נדמה שאכן מפתחי נוזקות המעקב עונים להגדרת מונע הנזק הזול במונחי יעילות כלכלית, כיוון שהם צוואר הבקבוק או החוליה בשרשרת הפעולות המובילות לפגיעה החמורה בזכות לפרטיות. כמו כן, איתור הפוגע הישיר במקרה של נוזקת מעקב קשה – אף אם זהות הפוגע הישיר ידועה, סביר מאוד שמדובר בשליט המדינה או ברשות שלטונית, ואז יתקשה הנפגע, שאותו גורם רודף אותו במדינתו ואולי אף מחוצה לה, להגיש נגדו תביעה ולנהלה. בנסיבות אלו, מרגע הזיהוי והאיתור של נוזקת המעקב במכשיר הטלפון הנייד, האיתור והזיהוי של מפתחיה הם משימה אפשרית וקלה יחסית.

336 פישמן אפורי, **לעיל** ה"ש 22, בעמ' 41–42, 50–61; פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 13–15 לפסק דינו של השופט ריבלין.

337 פרשת **א.ל.י.ס.**, **לעיל** ה"ש 107, בפס' 48, 50–51.

עם זאת, בבחינת שאלת הצדק החלוקתי התשובה אינה חדה וברורה. החברות המפתחות נוזקות מעקב חוזרות ומבהירות כי הן נועדו לשימוש למטרות אכיפת חוק ולוחמה בטרור. הן נותנות בידי רשויות אכיפת החוק כלים נוחים למעקב נקודתי אחר אדם ספציפי שמייתר את הצורך של רשויות אלו במעקב רחב יותר, למשל באמצעות כפיית "דלת אחורית", דוגמת תוכנת Prism שחשף אדוארד סנודן,[338] על חברות טכנולוגיה כגון גוגל, פייסבוק ואפל.[339] לפיכך לכאורה, קיים אינטרס ציבורי דווקא בהקלה על פעילותם של גורמי הביניים המפתחים נוזקות מעקב המשמשות למטרות המשרתות אינטרס ציבורי ברור, כגון אכיפת החוק ולוחמה בטרור. הכרה בדוקטרינת הפרה תורמת בנסיבות אלו עלולה להקשות עוד יותר על מפתחות נוזקות המעקב, הנתונות ממילא למשטר רגולטורי מורכב,[340] לפגוע בתחרות החופשית ולדחוף אותן לפעול דווקא במדינות אחרות שמשטרן המשפטי לא יכביד עליהן.[341] מנגד, יש לתת את הדעת לכך שככל טכנולוגיה דו־שימושית, גם לנוזקות מעקב שימושים ראויים ורצויים לצד שימושים פוגעניים. אימוץ דוקטרינת ההפרה התורמת עשוי דווקא לתמרץ את החברות המפתחות נוזקות מעקב לפעול למזעור הפגיעה האפשרית בזכות לפרטיות, למשל באמצעות צמצום הפונקציונליות של נוזקת המעקב בהתאם לנסיבות שונות, או הגברת הפיקוח על השימושים הנעשים בה במסגרת רישיון השימוש לשם הבטחת שימוש ראוי, מבלי לפגוע במימוש האינטרס הציבורי של שימוש בהן למטרות לוחמה בטרור והתמודדות עם פשיעה. משום כך, לדעתי קיים אינטרס לציבור בתמרוץ מפתחי נוזקות המעקב להגדיר ביתר דיוק את הפונקציונליות של הנוזקות שהן מפתחות ואת תנאי רישיון השימוש בהן.

338 Timothy B. Lee, *Here's Everything We Know About Prism to Date*, The Washington Post (June 12, 2013)

339 Farrow, **לעיל** ה"ש 2.

340 ראו דיון בפרק 4 **לעיל**.

341 להרחבה בנושא הפגיעה בתחרות החופשית ראו הדיון בטקסט הנלווה לה"ש 355–356 **להלן**.

5.1.3. גורם הביניים כבעל הכיס העמוק

העובדה כי גורם הביניים, מפתח הטכנולוגיה שאפשרה הפרת זכות היוצרים, הוא בעל כיס עמוק שימשה כדי להצדיק את אימוצה של דוקטרינת ההפרה התורמת לעולם זכויות היוצרים. לעומת המפירים הבודדים הרבים ניצב גורם הביניים – חברת סוני, נאפסטר או גרוקסטר – כבעל האמצעים לעמוד בפיצוי בעל זכות היוצרים בגין הפגיעה בזכותו.[342]

בהקשר של פגיעה בפרטיות עקב שימוש לא חוקי בנוזקת מעקב, לגורם הביניים, מפתח נוזקת המעקב, אין בהכרח כיס עמוק יותר מאשר לפוגע הישיר בזכות לפרטיות, יהיה זה שליט, מעסיק או רשות שלטונית. עם זאת, המשקל שניתן להצדקה זו הלך ופחת לאורך השנים נוכח המשמעות שבהטלת אחריות משפטית בהתאם ליכולת הכלכלית,[343] ולכן להצדקה זו עשוי להינתן משקל מועט במכלול השיקולים הנבחנים בעת אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות.

5.2. שיקולי מדיניות השוללים את אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בכלל, ובהקשר של נוזקות מעקב בפרט

5.2.1. פגיעה בחדשנות

בתחום דיני הקניין הרוחני בכלל וההגנה על זכות היוצרים בפרט מקובל לדבר על איזון בין חדשנות לזכות היוצרים. מחד גיסא, חדשנות נתפסת כמאיימת על זכות היוצרים. כך, למשל, תוכנות שיתוף הקבצים פגעו ביכולתם של בעלי זכויות היוצרים לקבל תגמול עבור השקעתם ועל כן איימו לפגוע פגיעה

342 בירנהק "לידתה של עוולה", **לעיל** ה"ש 90, בעמ' 200–201.

343 פישמן אפורי, **לעיל** ה"ש 22, בעמ' 41–42.

חמורה בתמריצים להמשיך וליצור. מאידך גיסא, ההצדקות התיאורטיות לזכות היוצרים הלקוחות מעולם הניתוח הכלכלי של המשפט מדגישות את חיוניותה של זכות היוצרים, מבחינה כלכלית ותועלתנית, להשגתה של חדשנות. זכות היוצרים מספקת את התמריצים הנחוצים להשקעה בחדשנות. תובנות מנוגדות אלו משקפות את האיזון המוטמע בזכות היוצרים בין הגנה על האינטרס הפרטי הקנייני של היוצר, הממציא או מפתח התוכנה, לבין האינטרס הציבורי שבחדשנות, התקדמות טכנולוגית והתפתחות חברתית ותרבותית. כמעט כל פיתוח חדש, מכל סוג, נשען על פיתוחים קודמים שהם נחלת הכלל, וההגנה המוענקת בזכות היוצרים לאינטרס הפרטי מכרסמת ביכולת להגיע לפיתוח הבא ובהתקדמות חברתית ותרבותית. מנגד, ההגנה על האינטרס הפרטי חיונית לשם שמירה על תמריצי היוצרים והמפתחים להשקיע מלכתחילה בפיתוחים חדשים.[344]

אימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים התבסס מלכתחילה על ההבנה שטכנולוגיות דו־שימושיות מאתגרות את האיזון הראוי שהמחוקק ביקש לקיים בין אינטרס הציבור בעידוד חדשנות, זרימה חופשית של רעיונות, מידע ומסחר והימנעות מפגיעה במנוע המוביל של הכלכלה המודרנית, לבין הזכות הקניינית של היוצרים לשלוט בניצול יצירותיהם. במובן זה דוקטרינת ההפרה התורמת היא כלי חשוב להשבת האיזון הראוי המגולם בזכות היוצרים.[345]

כפי שבסוף שנות התשעים של המאה ה־20 טענו בעלי זכויות היוצרים כי ההתפתחויות הטכנולוגיות מובילות לפגיעה חמורה בזכות היוצרים עד כדי הפרת האיזון הראוי בינה לבין חדשנות, נדמה שהחדשנות בתחום איסוף מידע ועיבודו מפירה את האיזון הראוי בינה לבין הזכות לפרטיות ואף מאיימת על

344 מיגל דויטש **עוולות מסחריות וסודות מסחר** (2002).

345 Moye, **לעיל** ה"ש 11, בעמ' 659; Zimmerman, **לעיל** ה"ש 22, בעמ' 78. נציין שבדין הישראלי החריג שנקבע בפרשת **סוני** (**לעיל** ה"ש 10) אינו מקובל, לכאורה, כפי שמעידה אמירתו של השופט ריבלין בפרשת **שוקן** שלפיה אפשר להטיל אחריות תורמת גם כאשר ההפרה הישירה חוסה תחת חריג השימוש ההוגן. ראו פס' 24 לפסק דינו של השופט ריבלין בפרשת **שוקן**, **לעיל** ה"ש 22. לביקורת על עמדה זו ראו פישמן אפורי, **לעיל** ה"ש 22, בעמ' 47–48.

עצם קיומה של הזכות לפרטיות.[346] מנגד, הרחבת מעגל האחראים להפרת הזכות לפרטיות, עם אימוץ דוקטרינת ההפרה התורמת, יוביל לחיזוק הזכות לפרטיות ולכן מעורר את החשש כי האיזון בין חדשנות לפרטיות יופר דווקא בעקבות הפגיעה הצפויה בחדשנות. הרחבת היקפה של הזכות לפרטיות, כך נטען, אינה תואמת את הציפייה הסבירה של נושא המידע לפרטיות, תפגע בזרימה החופשית של מידע, שהוא חומר הגלם הבסיסי לחדשנות הטכנולוגית כיום, ולפיכך תוביל לפגיעה אנושה בחדשנות שהיא בעלת ערך ורצויה מבחינה חברתית.[347]

לפי עמדה זו, כדי למנוע פגיעה חמורה בחדשנות, מוצדק להתעלם באופן מוחלט מהפרות הזכות לפרטיות ולתמוך ברגולציה חלשה להגנה על הזכות לפרטיות בשווקי מידע.[348] התומכים בעמדה זו מביאים כדוגמה את הפער בחדשנות בתחום טכנולוגיית המידע בין ארצות הברית לאיחוד האירופי. לשיטתם, הסיבה לכך שבארצות הברית מופיעים חידושים רבים יותר בתחום זה מאשר באיחוד האירופי היא חולשתה של חקיקת הגנת הפרטיות בארצות הברית לעומת זו הקיימת באיחוד האירופי. עם זאת, לעמדה זו אין סימוכין במחקרים, והמחקרים הקיימים מצביעים דווקא על מגוון סיבות אפשריות אחרות לפער זה. זאת ועוד, הפער בחדשנות בשוקי המידע בין ארצות הברית למדינות האיחוד האירופי עשוי דווקא ללמד על הצורך בסטנדרט פרטיות גלובלי אחיד, בדומה לזה הקיים באשר לזכות היוצרים. סטנדרט אחיד כאמור יאפשר חדשנות רצויה וראויה חברתית מבחינת הגנת הפרטיות, מבלי להעניק

346 Zarsky, **לעיל** ה"ש 149, בעמ' 117–118.

347 Avi Goldfarb & Catherine Tucker, Privacy and Innovation (NBER Working Paper Series, Working Paper 17124, 2011); Ashley Johnson, Balancing Privacy and Innovation in Smart Cities and Communities (Information Technology & Innovation Foundation 2023); Zarsky, **לעיל** ה"ש 149, בעמ' 140–141; Lev-Aretz & Strandburg, *Privacy Regulation*, **לעיל** ה"ש 9.

348 Cohen, *What Privacy*, **לעיל** ה"ש 150, בעמ' 1918–1927.

יתרון בתחום ליזמים ממדינות שאינן מעניקות הגנה מתאימה לזכות יסוד חשובה זו.[349]

זאת ועוד, לעומת זכות היוצרים, הזכות לפרטיות אינה נגזרת רק מהזכות החוקתית לקניין, וההצדקות לה אינן לקוחות מעולם הניתוח הכלכלי של המשפט ומתפיסת התועלתנות. לפיכך ניתוח כלכלי תועלתני אינו מתייחס לזכות לפרטיות כאל אמצעי חיוני להשגת חדשנות, וטיעונים בדבר קשר חיובי בין חדשנות לפרטיות נדחים בדרך כלל. כך, נטען שפגיעה בפרטיות וחיים תחת מעקב, רציף או לא רציף, מובילים לתחושת משטור ולחשש מפני חשיפה, ותחושות אלו פוגעות ביצירתיות. מאחר שחדשנות היא תוצר של יצירתיות, הגנה על הפרטיות חיונית גם כשלעצמה לשם עידוד החדשנות. עם זאת, על טיעון זה נמתחה ביקורת בנימוק שמדובר בטיעון ספקולטיבי שאינו מגובה בנתונים אמפיריים ונשען על התפיסה הרומנטית של היוצר או הממציא הבודד. כלל לא ברור שהיצירתיות הנדרשת לחדשנות מקורה בעיקר ביחיד ובהגנה על פרטיותו, ולא בהשקעה בחינוך ובהשכלה גבוהה של חלק גדול מהציבור וביצירת מרחב אשר יאפשר שיח פתוח בין עמיתים במקום העבודה.[350]

עוד נטען שקשר חיובי אפשרי נוסף בין חדשנות להגנה על הזכות לפרטיות בא לידי ביטוי בחיוניותה של האחרונה לשם יצירת יחסי אמון, הסכמה ושקיפות בין נושא המידע, המשתמש או הצרכן, לבין החברה המסחרית המספקת את הטכנולוגיה החדשנית. ההנחה היא שכאשר לקוחות ידעו שמידע אישי עליהם נחשף שלא כדין, הם יימנעו מלתת אמון בחברות המסחריות המפתחות ומפעילות את הטכנולוגיות החדשניות. הימנעות שכזו תפחית את מספר

349 Goldfarb & Tucker, **לעיל** ה"ש 347; Johnson, **לעיל** ה"ש 347; Zarsky, **לעיל** ה"ש 149, בעמ' 140–141; Lev-Aretz & Strandburg, *Privacy Regulation*, **לעיל** ה"ש 9.

350 Margaret Steen, *Privacy and Innovation*, Markkula Center for Applied Ethics at Santa Clara University (Feb. 1, 2023); M. Ryan Calo, The Unknown Unknowns: The Role of Innovation in Privacy (Yale ISP Symposium 2010–2011); Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of Participatory Turn*, *in* The Participatory Condition in the Digital Age 207 (Darin Barney et al. eds., 2016); Cohen, *What Privacy*, **לעיל** ה"ש 150, בעמ' 1918–1927.

המשתמשים או הצרכנים המתעניינים בטכנולוגיות חדשניות וכך יקטן התמריץ ליצור טכנולוגיות חדשניות והחדשנות ככלל תפגע. גם על טיעון זה נמתחה ביקורת בנימוק שאין בנמצא הוכחות להשפעה של הגנה על פרטיות המשתמש או של היעדרה על אמון המשתמשים באופן המוביל להימנעות משימוש במוצר טכנולוגי וכך לפגיעה בחדשנות.[351]

עם זאת, כשלי השוק המאפיינים שוקי מידע אישי רלוונטיים גם להצדקת אימוצה של דוקטרינת ההפרה התורמת תוך חיזוק הזכות להגנת הפרטיות ויצירת איזון ראוי מחודש בינה לבין אינטרס הציבור בחדשנות.[352] יתרה מכך, השפעתה של רגולציה על החדשנות תלויה במתווה ובדרישות של אותה רגולציה. רגולציה המתוכננת נכון תביא בחשבון את עלויות הציות ואת חשיבות ההגנה על התמריצים הכלכליים לחדשנות, ועל כן פגיעתה הצפויה בחדשנות יעילה חברתית אמורה להיות מזערית, אם בכלל.[353]

זאת ועוד, בניגוד לזכות היוצרים, שמעצם טבעה אמורה לעודד קדמה וחדשנות ומהווה כלי להשגת חדשנות, הזכות לפרטיות אינה מבוססת על אינטרסים תועלתניים כלכליים אלא על תפיסת כבוד האדם, האוטונומיה האישית שלו והגנה מפני חדירה פוגענית מדי מצד המדינה ומצד האחרים. האינטרסים הציבוריים הכלכליים שהחדשנות מגינה עליהם הם משניים בחשיבותם לערכים אלו. משום כך, האיזון בין הזכות לפרטיות אינו יכול לצאת מנקודת הנחה שמדובר בזכות ואינטרס במשקל זהה. נקודת האיזון בין הזכות לפרטיות לחדשנות צריכה להיות שונה מזו המקובלת ביחס שבין זכות היוצרים וחדשנות.[354]

351 Zarsky, **לעיל** ה"ש 149, בעמ' 132.

352 להרחבה בעניין כשלי השוק המאפיינים שוקי מידע ראו הדיון בסעיף 5.1.1 **לעיל**.

353 Lev-Aretz & Strandburg, *Privacy Regulation* **לעיל** ה"ש 9, בעמ' 275–276, 291–296.

354 Zarsky, **לעיל** ה"ש 149, בעמ' 143–146.

5.2.2. פגיעה בתחרות

יש הסבורים כי אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יפגע בתחרות החופשית, בעיקר בשוק נוזקות המעקב. כפי שעולה מסקירת האסדרה החקיקתית, המכירה של רישיונות שימוש בנוזקות מעקב כפופה לאסדרה בינלאומית ומדינתית מחמירה שתפקידה לפקח על יצוא נוזקות מעקב ולמזער את הסכנה הביטחונית שבנפילת טכנולוגיות כאלו לידיים בלתי מורשות. הטלת אחריות על החברות המפתחות נוזקות מעקב לפגיעה בפרטיות מכוח דוקטרינת ההפרה התורמת עשויה דווקא להכביד עוד יותר על תעשיית נוזקות המעקב, הנתונה גם כך לרגולציה מחמירה, להקשות מאוד על חברות ישראליות מתעשייה זו להתחרות בשוק החופשי, ואף להוביל אותן לסגור את עסקיהן בישראל ולבחור לפעול ממדינות שבהן אין רגולציה כלל, אף לא מגבלות על היצוא מטעמי ביטחון המדינה, כמו למשל סינגפור, קפריסין, רוסיה או סין.[355]

אומנם יש הטוענים שהגנה על הזכות לפרטיות חיונית לשם הגברת התחרות בשוק. מעמדה זו משתמע שכוח השוק המונופוליסטי של חברות הטכנולוגיה הגדולות מבוסס על איסוף, החזקה ועיבוד של כמויות עצומות של מידע אישי. חקיקה המגינה על מידע אישי ומסדירה את השימוש בו עשויה לפיכך לצמצם את יכולתן של החברות הגדולות לאסוף, להחזיק או לעבד כמויות עצומות של מידע אישי, וכך להקטין את חסמי הכניסה לשוק ולאפשר השתתפות של חברות אחרות, קטנות יותר וחדשניות. עם זאת, גם על עמדה זו נמתחה ביקורת בנימוק שייתכן שדווקא החלשת ההגנה על הזכות לפרטיות תקל על חברות חדשניות וקטנות לסחור במידע אישי וכך להשיג כוח שוק אשר יאפשר להן להתחרות בחברות הגדולות.[356] יתרה מזו, בשוק נוזקות המעקב כניסתה של חברה צעירה לשוק אינה תלויה בכמות המידע האישי שהיא כבר מחזיקה בידה, אלא ביכולת של נוזקת המעקב שפיתחה לחדור למערכות ממוחשבות ולאסוף מהן מידע ביעילות ובחשאיות.

355 Farrow, **לעיל** ה"ש 2.

356 Zarsky, **לעיל** ה"ש 149, בעמ' 135–136.

5.2.3. כשל אכיפה

ההצדקה המרכזית לאימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים או הפטנטים הייתה קיומו של כשל אכיפה. כשל זה בא לידי ביטוי בקיומם של מפירים יחידים רבים, שאת חלקם היה קשה לאתר, ושתביעת כל אחד מהם בנפרד יקרה ועלולה לסכן את תוקף הזכות, והתועלת הצפויה ממנה נמוכה משום שכלל לא ברור מהו הפיצוי שייפסק לטובת בעל הזכות. לפיכך תביעת כל אחד ואחד מהמפירים הייתה קשה לביצוע וגם לא כדאית מבחינה כלכלית עבור בעל זכות היוצרים או הפטנט. אימוצה של דוקטרינת ההפרה התורמת אִפשר לבעל זכות היוצרים או הפטנט לפנות בתביעה לקבלת סעד מהגורם שסיפק את הכלים שאפשרו את ההפרה ההמונית של זכויותיו – יצרן הטכנולוגיה.[357]

במקרה של פגיעה בפרטיות בעלי הזכויות הנפגעים הם רבים, מבודדים וחלשים כלכלית אל מול הפוגעים ומפתחי הטכנולוגיות המשמשות לפגיעה בפרטיות. מדובר בכשל השוק של היעדר יכולת לפעול באופן קולקטיבי,[358] ולאו דווקא בכשל אכיפה.

עם זאת, דווקא אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי להוביל לכשל אכיפה מכמה בחינות. ראשית, מבחינת הדין הנוהג – אף אם נוזקת המעקב פותחה בידי חברה ישראלית, המפר הישיר עשוי להיות בן מדינה זרה (אולי אף רשות שלטונית במדינה זרה), ועוולת הפגיעה בפרטיות עצמה עשויה להתרחש במרחב הפיזי והדיגיטלי הזר בלבד או במרחב הפיזי והדיגיטלי הישראלי או בכל שילוב של השניים, שהרי מדובר בתוכנת מחשב שפעולתה אינה תלויה בגבולות גיאוגרפיים. כשל האכיפה נובע מכך שלזכות לפרטיות אין הגדרה אחידה ומקובלת בכל העולם. שלל הגישות התיאורטיות לזכות לפרטיות מצביע על כך שמדובר בזכות עמומה ומשתנה, שקשה להמשיגה באופן אחיד וברור.[359] זאת בניגוד לזכות היוצרים, שגבולותיה

357 בירנהק "לידתה של עוולה", **לעיל** ה"ש 90, בעמ' 200–201.

358 להרחבה ראו הדיון בטקסט הנלווה לה"ש 326 **לעיל**.

359 בירנהק **פרטיות חוקתית**, **לעיל** ה"ש 117, בעמ' 68.

והיקפה ברורים ומוסכמים במרבית מדינות העולם, ומשקפים את האיזון הראוי בין האינטרס הפרטי של היוצר לבין האינטרס הציבורי בחדשנות המבוססת על נחלת הכלל. בהיעדר הגדרה אחידה וברורה, מעשה שעשוי להיחשב פגיעה בזכות לפרטיות במדינה אחרת עשוי להיות מותר וחוקי במדינה אחרת.

היעדר הגדרה אחידה עשוי להטיל נטל כבד על החברות המפתחות נוזקות מעקב. יהא עליהן להחזיק מערך משפטי מורכב אשר יכיר את דיני הגנת הפרטיות לצד דיני העונשין, דיני הלוחמה בטרור והסמכויות של כל רשות שלטונית רלוונטית בכל המדינות שלהן הנוזקה נמכרת ובכל המדינות שבהן היא עשויה להיות מופעלת, להטמיע דרישות חוזיות מתאימות בכל עסקה לרכישת רישיון שימוש בנוזקה ולהפעיל מנגנון טכנולוגי וחוזי לאיתור פגיעות אפשריות בפרטיות בהתאם לשימוש המבוצע בנוזקת המעקב. אם נטל כזה אכן יוטל על החברות המפתחות, ספק אם הן אכן יהיו מונע הנזק הזול.

עם זאת, חקיקת ה־GDPR באיחוד האירופי הובילה להאחדה יחסית ומבורכת של סטנדרט ההגנה על הזכות לפרטיות בקרב מרבית המדינות.[360] בהנחה שמגמת ההאחדה של דיני הגנת הפרטיות ברוח ה־GDPR תימשך ותעמיק, כשל אכיפה זה, ביחס לדין הנוהג, עשוי להצטמצם.

כשל האכיפה האפשרי השני רלוונטי במיוחד למקרה שבו המפר הישיר הוא רשות שלטונית העשויה ליהנות מחסינות. כך, למשל, תביעתה של ארוסתו של העיתונאי הסעודי ג׳מאל חשוקג׳י נגד יורש העצר הסעודי, בגין חלקו לפי דיווחים בלכידתו ורציחתו של בן זוגה, נדחתה בידי בית המשפט הפדרלי בארצות הברית בנימוק שהנתבע זכאי לחסינות מפני תביעה בארצות הברית כראש מדינה.[361] אף בישראל חוק חסינות מדינות זרות, התשס״ט–2008 (להלן: חוק החסינות) מעניק למדינה זרה חסינות מפני סמכות השיפוט של בתי משפט בישראל, למעט בעניינים פליליים.[362] אולם החוק מונה גם חריגים

360 Cedric Ryngaert & Mistale Taylor, *The GDPR as Global Data Protection Regulation*, 114 Am. J. Int'l L. 5 (2020)

361 Edward Wong, *U.S. Court Dismisses Suit Against Saudi Ruler in Khashoggi Killing*, The New York Times (Dec. 6, 2022)

362 סעיף 2 לחוק החסינות.

לעקרון החסינות, למשל בתביעה בשל עוולה שהתרחשה בישראל וגרמה לנזק לגוף או לרכוש מוחשי, או בגין הפרת זכות בקניין רוחני בידי המדינה הזרה.[363]

כמו כן, בפרשת **רב בריח** נפסק שגם כאשר המפר הישיר חוסה תחת אחד מהחריגים הקבועים בחוק זכות יוצרים, כגון חריג השימוש ההוגן, עדיין אפשר לקבוע שתנאי קיומה של הפרה ישירה מתקיים בעת בחינת תחולתה של דוקטרינת ההפרה התורמת. הרציונל לקביעת בית המשפט היה רצונו להעניק סעד לתובע לנוכח הנזק המשמעותי שנגרם לו. בית המשפט הסביר שאף שהנזק הנגרם מפעולתו של כל אחד מהמפירים הישירים אינו גדול, ואף עשוי לחסות תחת אחת מן ההגנות הקבועות בחוק זכות יוצרים, הנזק המצטבר מההפרה על ידי כל המפירים הישירים הוא גדול, וחוסר היכולת של בעל זכות היוצרים לקבל פיצוי בגינו הוא כשל אכיפה שדוקטרינת ההפרה התורמת באה לפתור.[364] במקרה של פגיעה בפרטיות אין מדובר במפירים רבים שהנזק מההפרה הבודדת שביצעו אינו רב – השימוש בנוזקת מעקב מוביל לפגיעה אחת ומשמעותית בפרטיות על ידי מפר ישיר אחד. עם זאת, אם המפר הישיר זוכה לחסינות או להגנה מפני תביעה, התובע עשוי להיוותר ללא כל סעד, למרות הפגיעה המשמעותית בפרטיותו. לפיכך הרציונל לקביעת בית המשפט בפרשת **רב בריח** עשוי להתקיים גם בנסיבות של פגיעה בפרטיות עקב שימוש בנוזקת מעקב, ולהצדיק הטלת אחריות על גורם הביניים גם כאשר המפר הישיר זוכה לחסינות. קיומם של החריגים לחסינות המדינתית במקרה של עוולה נזיקית והפרת קניין רוחני בחוק החסינות,[365] ושיקולי מדיניות ואינטרס הציבור במתן תמריץ לחברות המפתחות נוזקות מעקב לדייק את הפונקציונליות של הנוזקות, תומכים גם הם בעמדה זו.

363 סעיפים 5 ו־7(ב) לחוק החסינות.

364 פרק ד' לחוק זכות יוצרים; פרשת **שוקן**, **לעיל** ה"ש 22, בפס' 24 לפסק דינו של השופט ריבלין.

365 סעיפים 5 ו־7(ב) לחוק החסינות.

5.2.4. אינטרסים ציבוריים נוספים

כאמור, בעת בחינת אימוצה של דוקטרינת ההפרה התורמת לדיני זכויות היוצרים התמקד הדיון בניתוח כלכלני תועלתני של השלכות אימוץ הדוקטרינה והסתיים בבחינת האיזון הראוי בין זכות היוצרים לבין אינטרס הציבור בחדשנות. לעומת זאת, הדיון באימוצה של הדוקטרינה לדיני הגנת הפרטיות אינו מתמצה בנקודה זו. הזכות לפרטיות היא זכות מורכבת החולשת על מגוון נרחב, ולעיתים אבסטרקטי, של פעולות, תופעות וחשיבויות. במובן הרחב ביותר ניתן לומר שפרטיות היא היכולת של הפרט להגדיר, בתנאיו הוא, את עצמו ואת זהותו כלפי העולם. היקפה הנרחב של הזכות לפרטיות אף הוביל להקבלת הפגיעה בה לתופעות כמו ההתחממות הגלובלית ושינוי האקלים, שהפילוסוף הבריטי טימות'י מורטון כינה "היפר־אובייקט": תופעות רחבות שקשה לאדם להגדיר במלואן ולהבין את הסכנה הטמונה בהן לטווח הארוך. לכן במקום לנקוט פעולות לשם הגנה על הזכות לפרטיות, מרבית הציבור בוחר בנוחות המיידית גם במחיר של פגיעה בה. למשל, אנשים ימשיכו לעשות שימוש במזגן בימים חמים, אף שהם יודעים ששימוש רב במכשירים צורכי חשמל גורם לפגיעה בשכבת האוזון המובילה להתחממות הגלובלית. באופן דומה, מרביתנו ימשיכו להשתמש ביישומון ניווט בטלפון הנייד, אף בידיעה שהיישומון אוסף עלינו מידע אישי ורגיש ומוכר אותו למרבה במחיר תוך פגיעה חמורה בפרטיותנו.[366]

בשל עומקה ורוחבה של הזכות לפרטיות, גם חיזוקה עשוי לפגוע בקשת רחבה של זכויות או אינטרסים. כך, למשל, אימוץ דוקטרינת ההפרה התורמת עשוי לפגוע באינטרס הציבור בביטחון הלאומי או בביטחון הציבור. יש לתת את הדעת לפגיעות אפשריות אלו בבואנו לבחון את הבסיס העיוני לאימוצה של דוקטרינת ההפרה התורמת ואת שיקולי המדיניות הנלווים לו.

אולם בכל הקשור לנוזקת מעקב, לצד הפגיעה האפשרית באינטרס הציבורי בביטחון לאומי או בביטחון הציבור יש לתת את הדעת גם לסכנה שבשימוש

366 Timothy Morton, Hyperobjects: Philosophy and Ecology after the End of the World (2013); Charlie Warzel, *Privacy Is Too Big to Understand*, The New York Times (April 16, 2019)

לרעה בנוזקות מעקב למטרות שאינן קשורות בהכרח לביטחון הלאומי או לביטחון הציבור – למשל לשם השתקת מתנגדים לשלטון או למעקב ללא צו שיפוטי מתאים אחר אזרחים. כמו כן, בשנים האחרונות נפתחות חברות סייבר התקפי המפתחות נוזקות מעקב במדינות מחוץ לישראל, כגון יוון וקפריסין. נראה כי מומחי סייבר התקפי ישראלים בוחרים לפתוח חברות אלו מחוץ לישראל בניסיון להימלט מהוראות הפיקוח על היצוא. אולם חלק מבעלי המניות בחברות אלו הן חברות ישראליות או אזרחים ישראלים. למשל, לפי דיווחים בתקשורת, חברת הסייבר ההתקפי המפתחת ומשווקת את נוזקת המעקב Intellexa (שלאחרונה הוכנסה לרשימה השחורה של מחלקת המסחר האמריקנית)[367] הוקמה בידי יוצא מערכת הביטחון אל"מ טל דיליאן בקפריסין, שם הוא גם מתגורר. אך אחד מבעלי המניות בחברה הוא חברת מבטח שמיר הישראלית. יש להניח שתופעה זו מוכרת במדינות נוספות חוץ מישראל. בעוד המדינה מתקשה להחיל פיקוח על חברות סייבר התקפי במדינות זרות מכוח רגולציית הפיקוח על היצוא, אף אם מקימיהן או בעלי המניות בהן הם ישראלים,[368] אם תאומץ דוקטרינת ההפרה התורמת, בעלי המניות בחברות אלו עשויים להבין את הסכנה שבמתן רישיונות שימוש בנוזקות המעקב במקרים של פגיעה חמורה בזכות לפרטיות ולמדינות הידועות באי־כיבוד זכויות אדם בסיסיות. הבנה זו מצד בעלי המניות עשויה להביא להגדרה מדויקת יותר של הפונקציונליות של נוזקות המעקב ולבחינה מדוקדקת של השפעת השימוש בהן על הזכות לפרטיות בעסקאות עתידיות.

זאת ועוד, נקודת המוצא בבחינת שיקולי מדיניות אלו היא שמדובר באינטרסים. משום כך, באיזון למול הזכות החוקתית לפרטיות יש לתת להם משקל נמוך יותר ממשקלה של הזכות לפרטיות, על אף חשיבותם הציבורית הגדולה. במסגרת זו פגיעה בזכות החוקתית לפרטיות לשם הגשמת אחד מאינטרסים חשובים אלו עדיין צריכה לעמוד בדרישת המידתיות. כלומר על הפגיעה בפרטיות להיות לא רק לתכלית ראויה, אלא גם יש להוכיח שהאמצעי שננקט ומוביל לפגיעה הוא האמצעי המתאים והיעיל להגשמת האינטרס, שאין אמצעי אחר

367 ראו הדיון בטקסט הנלווה לה"ש 284 **לעיל**.

368 שדה, **לעיל** ה"ש 284.

שיעילותו דומה אך פגיעתו בזכות לפרטיות פחותה, וכן שהתועלת השולית מהשימוש בו עולה על הנזק שבפגיעה בזכות לפרטיות.[369] עמידה במבחנים אלו תיבדק במסגרת יישום דוקטרינת ההפרה התורמת בנסיבות של נוזקת מעקב בפרק 6 להלן.

5.3. סיכום

אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בישראל אפשרי מכוח צינור הקליטה שבסעיף 12 לפקודת הנזיקין. אולם סקירת שיקולי המדיניות הרלוונטיים מצביעה על כך שאימוץ הדוקטרינה לדיני הגנת הפרטיות בהקשר של שימוש לא חוקי בנוזקות מעקב עשוי לעורר קשיים.

אומנם אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות יוביל לחיזוק הזכות לפרטיות. חיזוק זה נחוץ ביותר נוכח הפגיעה הניכרת בחשיבות הזכות ובהגנה עליה בשנים האחרונות עם הקִדמה הטכנולוגית. יש בו כדי להשיב את המשקל הראוי לערכים שבבסיס הזכות לפרטיות, הנגזרת מהזכות לכבוד ומרכזית לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו וללא התערבות זרה. כן תפתור דוקטרינת ההפרה התורמת את כשלי השוק המאפיינים שוקי מידע.

נוסף על כך, מפתחי נוזקות המעקב מצויים, לכאורה, בעמדת המפתח להפסקת הפגיעה בפרטיות או למניעתה, אולם לא ברור שדי בכך לשם הכרזתם כמונע הנזק הזול – שיקול אשר שימש להצדקת אימוץ דוקטרינת ההפרה התורמת לדיני זכויות היוצרים. זאת משום שמבחינת הצדק החלוקתי, דוקטרינת ההפרה התורמת עשויה להכביד מאוד על תעשיית נוזקות המעקב – על החברות יוטל לבחון את הדינים הרלוונטיים להגנת פרטיות ואת דיני הלוחמה בפשיעה ובטרור בכל מדינה, ולעיתים להסתכן באחריות לפגיעה בפרטיות במקום שבו

369 מרדכי קרמניצר ורענן סוליציאנו קינן **קבלת החלטות בימי הקורונה בראי הפסיקה: ההחלטה להשתמש באיכוני השב"כ כמקרה מבחן** 8 (המכון הישראלי לדמוקרטיה 2021).

פעולת הרשות המדינתית תיחשב חוקית לפי חוקי אותה מדינה. נטל זה עלול להוביל חברות אלו, הנתונות ממילא במשטר פיקוח קפדני על היצוא, לסגור את פעילותן בישראל ולפעול דווקא במדינות אחרות שמשטרן המשפטי לא יכביד עליהן.

באשר לטיעון בדבר הפגיעה בחדשנות, אף שיש הטוענים לקשר חיובי, במובנים מסוימים, בין פרטיות לחדשנות נוכח חיוניותה של הפרטיות למחשבה חופשית ויצירתית, ליצירת יחסי אמון בין המשתמש לחברה המפתחת ולהגברת התחרות בשווקי המידע האישי, נדמה שהזכות לפרטיות אינה נחשבת חיונית לחדשנות בבחינה תועלתנית כלכלית. עם זאת, כשלי השוק וההחצנות השליליות המאפיינים שוקי מידע אישי ומשמשים להצדקת רגולציה המחזקת את הזכות לפרטיות רלוונטיים גם להדיפת הטענות האפשריות לפגיעה בחדשנות עקב אימוץ דוקטרינת ההפרה התורמת. כוחות השוק אינם מאפשרים למשתמשים לשקף את העדפותיהם האמיתיות בנוגע לשימוש במידע אישי עליהם. יתרה מכך, טכנולוגיות לעיבוד נתוני עתק מחריפות את כשלי השוק והופכות את תיקונם בידי השוק עצמו לבלתי אפשרי. כמו כן, כוחות השוק מתייחסים למידע אישי כאל כל סחורה אחרת ולכן מתעלמים מהערכים החשובים שבבסיסה של הזכות לפרטיות, אשר נפגעים משימוש לא ראוי במידע אישי.

עם זאת, אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי להוביל לכשל אכיפה הנוגע לדין הנוהג ולסמכות השיפוט. כשל זה יבוא לידי ביטוי במיוחד בנסיבות של שימוש לא חוקי של רשות שלטונית בנוזקות מעקב. אומנם כשל האכיפה הנוגע לדין הנוהג עשוי להיפתר בשנים הקרובות נוכח האחדה של הגדרת הזכות לפרטיות בעקבות "אפקט בריסל". אולם, כשל האכיפה הנוגע לסמכות השיפוט של בית המשפט במדינה שבה מוגשת התביעה על רשות שלטונית במדינה זרה, העשויה ליהנות מחסינות מפני תביעות, מקשה מאוד את הוכחתה של הפרה ישירה, ולפיכך את אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בישראל. לצד אלה, הצורך בחיזוקה של הזכות לפרטיות ובמזעור הפגיעה בה עקב שימוש בנוזקות מעקב, לצד הפסיקה הקיימת אשר התירה את החלת דוקטרינת ההפרה התורמת בדיני הקניין הרוחני גם כאשר המפר הישיר נהנה מטענת הגנה, עשויים להצדיק את אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות על

אף הקושי, ושאלת השפעת חסינותו של המפר הישיר, אם תהיה כזו, תיבחן בנסיבות כל מקרה ומקרה.

גורם נוסף העשוי להקשות את אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות קשור לטענה בדבר פגיעה בתחרות החופשית. תעשיית נוזקות המעקב נתונה לרגולציה כבדה בכל הקשור ליצוא טכנולוגיה דו־שימושית. אף שאסדרה זו אינה נותנת מענה מספק לפגיעה החמורה בפרטיות שמאפשרות נוזקות המעקב, הכבדה נוספת בדמות הסכנה שבנשיאה באחריות תורמת לפגיעה בפרטיות עשויה להקשות מאוד את התחרות בשוק החופשי עבור החברות הישראליות. ואכן, תעשיית הסייבר ההתקפי בישראל הולכת ומצטמצמת ומומחים אף מזהירים מ"בריחת מוחות" למדינות אחרות.[370]

זאת ועוד, בהקשר של נוזקות מעקב חיזוק הזכות לפרטיות עשוי להביא גם לפגיעה באינטרס הציבור בביטחון לאומי ובביטחון הציבור. אולם על אף חשיבותם הגדולה של אינטרסים אלו, יש לזכור שמדובר באינטרסים שמשקלם קטן מזה של הזכות החוקתית לפרטיות.

אכן, ניסיון העבר מלמד שהשימוש בדוקטרינת ההפרה התורמת בדיני זכויות היוצרים במטרה לשלוט בטכנולוגיות שיתוף קבצים היה בפועל משחק חתול ועכבר: בתי המשפט הרחיבו ביצירתיות את דוקטרינת ההפרה התורמת ומפתחי הטכנולוגיות מצאו דרכים לנצל את החורים בדוקטרינה כדי להתחמק מאחריות.[371] משחק חתול ועכבר דומה עשוי להתקיים, אם לא מתקיים כבר עתה, בין בית המשפט ליצרניות נוזקות המעקב: חברות המפתחות נוזקות מעקב עשויות לשכלל את הטכנולוגיה באופן אשר ימנע מהן כל מודעות בנוגע לשימוש הנעשה בהן או שליטה עליו. בסופו של דבר, משחק החתול והעכבר בין דיני זכויות היוצרים למפתחי הטכנולוגיה הוביל להכרה של תעשיית התוכן בכך שעליה להישען על טכנולוגיות חדשניות ולפתח מודלים עסקיים חדשים כדי להתגבר על חולשת הגנת זכויות היוצרים.[372] תוכנות שיתוף הקבצים איבדו

370 טל שחף "בסייבר מאשימים: 'הממשלה מתנערת מהסייבר ההתקפי – ויוצרת שכירי חרב מסוכנים'" **Tech12** (19.6.2023); כביר, **לעיל** ה"ש 163.

371 Choi, **לעיל** ה"ש 32, בעמ' 395.

372 Zimmerman, **לעיל** ה"ש 22, בעמ' 95.

מהפופולריות שלהן כי הופיעו חנויות המוזיקה, אבל האם יש לנו זמן לחכות לפתרון טכנולוגי שכזה בנוגע לפרטיות, והאם הזכות לפרטיות חזקה מספיק כדי שיתפתח פתרון כזה?

לכאורה, במצב דברים זה נדמה כי דווקא אסדרה בחוק של השימוש הנעשה בנוזקות מעקב, כפי שהציע הבודק המיוחד מטעם האו"ם, היא הכרח המציאות. אסדרה שכזו צריכה, לכל הפחות, לחייב את החברות המפתחות בשקיפות, בהטמעת מנגנונים טכנולוגיים לעיצוב לפרטיות ובביצוע בדיקה לפני כל התקשרות למתן רישיון שימוש, ולצד זאת עליה להתוות הליך פיקוח ובדיקה מטעם המדינה על פיתוח, שיווק ויצוא טכנולוגיות כאמור.[373] אולם הסיכוי לגיבוש אסדרה בינלאומית מקיפה שכזו שתהיה מקובלת על כל המדינות או אפילו רק על רובן הוא נמוך. מדובר בתהליך שעשוי לארוך שנים, ובמהלכו הפגיעה של נוזקות מעקב בפרטיות ובזכויות אחרות עשויה רק להתעצם. יש לתת את הדעת גם על כך שאף אם תגובש אסדרה בינלאומית כאמור, מדינות שאינן דמוקרטיות לא יצייתו לה כלל.

לא זו אף זו: יש לזכור שנוזקת מעקב היא טכנולוגיה דו־שימושית. לפיכך יש לתת את הדעת גם לסיכוי שאימוץ דוקטרינת ההפרה התורמת דווקא יתמרץ את החברות בתעשייה לפעול למזעור השימוש הלא חוקי במוצריהן, למשל באמצעות צמצום הפונקציונליות של נוזקת המעקב בהתאם לנסיבות שונות או הגדרה מדויקת יותר שלה, או באמצעות הגברת הפיקוח על השימושים הנעשים בה במסגרת רישיון השימוש לשם הבטחת שימוש ראוי. ייתכן גם שאימוץ דוקטרינת ההפרה התורמת יפעיל לחץ על בעלי מניות ישראלים של חברות מתעשיית נוזקות המעקב שאינן מצויות בישראל, ואלו ידרשו התחשבות בזכות לפרטיות באישור עסקאות למתן רישיונות שימוש בנוזקות מעקב.

לפיכך על אף הקשיים נראה שיש חשיבות לפיתוחה של דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות, וההתאמות הנדרשות נוכח הקשיים שעשויים להתעורר, בעיקר באשר לנוזקות מעקב, יבוצעו בעת יישומה של הדוקטרינה בפועל בנסיבות כל מקרה ומקרה.

373 דוח הבודק המיוחד 2019, **לעיל** ה"ש 195, בעמ' 14.

פרק 6

דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות – התנאים לתחולתה ויישומם בהקשר של נוזקות מעקב

בפרק הקודם בדקתי את הבסיס העיוני לאימוצה של הדוקטרינה ואת שיקולי המדיניות הנלווים לכך. נמצא שאף שאימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות אפשרי מכוח צינור הקליטה שבסעיף 12 לפקודת הנזיקין, הוא עשוי לעורר קשיים – בשל משטר הפיקוח הקפדני על היצוא המכביד כבר כיום על תעשיית נוזקות המעקב, כשלי האכיפה האפשריים והסכנה לעזיבת חברות מהתעשייה למדינות מקילות יותר. עם זאת, מכלול השיקולים הוביל למסקנה שהיתרונות הטמונים באימוצה של דוקטרינת ההפרה התורמת עולים על החסרונות, והתמודדות נכונה עם האחרונים ראוי שתיעשה בעת יישום הדוקטרינה בנסיבות כל מקרה ומקרה. לשם כך יש לבחון את התנאים להחלתה של הדוקטרינה ואת אופן יישומם בדיני הגנת הפרטיות. את זאת נפנה לעשות עתה.

מסקירת דוקטרינת ההפרה התורמת בדיני זכויות יוצרים בפרק 1 עולה שלשם החלתה נדרשת הוכחתם של שלושה תנאים מצטברים:

(**1**) קיומה של הפרה ישירה;

(**2**) מודעות גורם הביניים להפרה;

(**3**) תרומה משמעותית, ניכרת וממשית של גורם הביניים לביצוע ההפרה הישירה.

בעת בחינת אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בישראל יש לבדוק את האפשרות ליישם כל אחד מהתנאים המצטברים הללו ואת השלכות היישום.

6.1. קיומה של הפרה ישירה

ככלל, פגיעה בזכות לפרטיות, כבכל זכות חוקתית אחרת, צריכה לעמוד בתנאי פסקת ההגבלה שבחוק־יסוד: כבוד האדם וחירותו, כלומר עליה להיות לתכלית ראויה ובמידה שאינה עולה על הנדרש. מידתיות הפגיעה נקבעת לפי שלושה מבחנים:[374]

(**1**) **מבחן ההתאמה**: האם האמצעי שננקט עשוי להביא להשגת התכלית?

הנחת המוצא של בחינת הפגיעה בפרטיות באמצעות שימוש בנוזקות מעקב היא שתכלית השימוש בהן היא הגנה על ביטחון הציבור או על הביטחון הלאומי, ועל כן מדובר בתכלית ראויה ויש סבירות גבוהה שנוזקת המעקב היא אמצעי שעשוי להביא להשגתה. כל שימוש לתכלית אחרת, כגון השתקת יריבים פוליטיים או השתקת ביקורת על השלטון, אינו יכול להיחשב "תכלית ראויה" במדינה דמוקרטית המגינה על הזכות לפרטיות כזכות יסוד, ומשום כך מהווה הפרה ישירה של הזכות החוקתית לפרטיות.

(**2**) **מבחן הצורך**: האם האמצעי שנבחר הוא האמצעי היעיל שפגיעתו בזכות היא הקטנה ביותר, ואין אמצעי אחר שיעילותו דומה אך פגיעתו בזכות קטנה יותר?

(**3**) **מבחן המידתיות הצר**: האם התועלת השולית שתושג מהשימוש באמצעי עולה על הנזק שגורמת הפגיעה בזכות?

בחינת שתי שאלות אלו מובילה למסקנה שהפגיעה של נוזקות מעקב בזכות החוקתית לפרטיות אינה מידתית. מסקנה זו נסמכת על קביעותיהם של הנציב העליון לענייני זכויות אדם של האו"ם משנת 2022 ושל המפקח על הגנת מידע באיחוד האירופי.

בדוח הנציב העליון לענייני זכויות אדם של האו"ם משנת 2022 נקבע שנוזקת מעקב גורמת לפגיעה אנושה ומשמעותית בזכות לפרטיות, משום

374 קרמניצר וסוליציאנו קינן, **לעיל** ה"ש 369, בעמ' 8.

שבאמצעותה אפשר לגבש תמונה מפורטת על חיי מושא המעקב, מחשבותיו, העדפותיו, פעילותו המקצועית, השקפותיו הפוליטיות, מצבו הכלכלי, הבריאותי והחברתי ויחסיו האינטימיים.[375] גם המפקח על הגנת מידע באיחוד האירופי הציג עמדה דומה והסביר שנוזקת מעקב היא שינוי של כללי המשחק (game changer) ושינוי פרדיגמה של ממש מבחינת יכולות הגישה לתקשורת פרטית, משום שהיא עשויה להוביל לרמת פולשנות חסרת תקדים בשילוב מאפיינים שהופכים כל אמצעי אבטחה משפטי או טכני לחסר משמעות. לפיכך שימוש בנוזקת מעקב כמוהו כנישול נושא המידע מזכותו לפרטיות, תוך פגיעה חמורה גם בפרטיות הסובבים אותו. הפגיעה בזכות לפרטיות משימוש בנוזקת מעקב חמורה כל כך עד שלא סביר שהיא יכולה להיחשב מידתית.[376]

לפיכך הקושי בדרישת קיומה של הפרה ישירה אינו נוגע למידתיות הפגיעה בפרטיות אלא בשאלה אם המפר הישיר עשוי ליהנות מחסינות או מטענות הגנה כלשהן. כאמור, המשקל שיש לתת לשאלה זו תלוי בנסיבות כל מקרה ומקרה,[377] ויש לבחון את השאלה תוך שימת לב לעוצמת הפגיעה בפרטיות בנסיבות כל מקרה ולהשלכות של אי־מתן סעד על הנפגע הספציפי, כמו גם על פוטנציאל הפגיעות בנפגעים נוספים בעתיד.

6.2. מודעות המפר התורם

כבכל טכנולוגיה דו־שימושית, ההנחה בדבר מודעותה של חברה המפתחת נוזקת מעקב לפגיעה בזכות לפרטיות באמצעות הנוזקה אינה נקייה מספקות. לטענת החברות המפתחות נוזקות מעקב, רישיונות השימוש בנוזקות ניתנים לרשויות ביון ואכיפת חוק לשם השגת מטרות לגיטימיות של לוחמה בטרור ומניעת פשיעה. חיזוק לכך אנו מוצאים, למשל, בגילויים בדבר השימוש של רשויות אכיפת החוק והביון של כמה מדינות דמוקרטיות מערביות, כגון

375 ראו דיון בטקסט הנלווה להערות שוליים 210–212 **לעיל**.

376 ראו דיון בטקסט הנלווה להערות שוליים 262–266 **לעיל**.

377 ראו הדיון בטקסט הנלווה להערות שוליים 361–365 **לעיל**.

גרמניה, הולנד, בלגיה וספרד, בנוזקת המעקב פגסוס של חברת NSO – שימוש שלטענת אותן מדינות עומד בדרישות החוק האירופי.[378] כמו כן, בהנחה שמרבית החברות המפתחות נוזקות מעקב פועלות בדומה ל־NSO הישראלית, הרי שלכאורה אין להן גישה למידע הנאסף ונצבר באמצעות השימוש בנוזקות. כמו כן, טרם החתימה על הסכם רישיון שימוש בנוזקת המעקב פגסוס NSO עצמה אומדת את הסיכון לפגיעה בזכויות אדם, בין השאר לפי מטרת השימוש המבוקשת, היסטוריית ההגנה על זכויות אדם על ידי הממשלה המדוברת וסטנדרט ההגנה על זכויות אדם באותה המדינה. כן אוסר רישיון השימוש על שימוש לרעה בפגסוס באופן הפוגע בזכויות אדם שלא כדין.[379] NSO אף מחזיקה במנגנון לדיווח אנונימי על פגיעה בזכויות אדם או שימוש לרעה בנוזקה, בדומה למנגנון ההודעה וההסרה המקובל בדיני זכויות היוצרים.[380] כלומר NSO אינה יכולה לדעת אם נעשה בטכנולוגיה שלה שימוש מפר ומבקשת את עזרת הציבור לשם כך.

עם זאת, הבודק המיוחד של האו"ם דחה על הסף את טענות החברות המפתחות את נוזקות המעקב להיעדר מודעות מצידן. לשיטתו, אופייה החשאי של תעשיית טכנולוגיית המעקב והשימוש הנרחב במוצריה למטרות שאינן עולות בקנה אחד עם הדין הבינלאומי להגנה על זכויות אדם מלמד שהחברות הפרטיות בתעשייה אינן נותנות את הדעת להשפעת השימוש במוצריהן על זכויות אדם, או לדרישות המינימום המפורטות בכללים המנחים. לפיכך לדעתו אין לקבל את טענותיהן כי אין ביכולתן לדעת על השימוש הפוגעני במוצריהן.[381]

378 ראו דיון בסעיף 3.1 **לעיל**, וכן Mildebrath, **לעיל** ה"ש 3, בעמ' 20–28.

379 ראו דיון בסעיף 3.1 **לעיל**.

380 מנגנון ההודעה וההסרה הקבוע בסעיף 512 ל־DMCA האמריקני, ובסעיפים 12–15 לדירקטיבת ה־E-commerce האירופית, **לעיל** ה"ש 47, מעניק לספק שירות אינטרנט חסינות מאחריות להפרת זכות יוצרים שביצעו משתמשי השירות שלו, אם הוא מגיב במהירות להודעה העומדת בדרישות החוק מבעל זכות היוצרים וחוסם את הגישה לחומרים המפירים, ובלבד שספק השירות אינו מחזיק בידע בפועל או בכוח על ההפרה.

381 ראו הדיון בטקסט הנלווה לה"ש 194–210 **לעיל**.

מסקנה דומה אפשר להסיק גם מקביעתו של המפקח על הגנת מידע באיחוד האירופי, שלפיה נוזקות מעקב דוגמת פגסוס הן שינוי כללי המשחק מבחינת רמת החודרנות לתקשורת פרטית. תכנונן ופיתוחן מלכתחילה כמעניקות גישה מלאה ובלתי מוגבלת לכלל המידע האישי האגור בטלפון נייד או הזמין באמצעותו מאיימים על מהות הזכות לפרטיות.[382] מאחר שהחברות המפתחות הן שקבעו את הפונקציונליות של נוזקות המעקב ואת רמת הפולשנות הבלתי נתפסת שלהן, קשה להאמין שאין הן מודעות לשימוש הפוגעני האפשרי באמצעותן.

אם כן, לצד הקושי בהוכחת מודעות בפועל להפרה ישירה ספציפית של הזכות לפרטיות, כמה ממצאים עשויים להצביע על מודעות בכוח: מסקנותיהם של הבודק המיוחד מטעם האו"ם ושל המפקח על הגנת מידע באיחוד האירופי, כמו גם הימנעותן של מפתחות נוזקות מעקב מהטמעת אמצעים טכנולוגיים, כגון עיצוב לפרטיות, שיובילו ליציקת תוכן פרקטי להתחייבויות החוזיות וימנעו או ימזערו את הסיכון לשימוש לרעה בנוזקה.

בישראל יש קונצנזוס בפרשנות דרישת המודעות כמחייבת מודעות בפועל, אולם בארצות הברית קיימת מחלוקת בנושא. בהיעדר שימוש מסחרי חוקי משמעותי, כלומר כאשר אין מדובר בטכנולוגיה דו־שימושית, די בהוכחת מודעותו בכוח של גורם הביניים, אולם כאשר קיים שימוש מסחרי חוקי משמעותי נדרשת הוכחת מודעות בפועל. עם זאת, לא ברור מהו היקף השימוש החוקי שיש להוכיח. כמו כן, קיימת מחלוקת שטרם הוכרעה בין ערכאות הערעור בשאלה אם עצימת עיניים מכוונת מספיקה לשם הוכחת מודעותו של גורם הביניים לשימושים המפירים.[383] באיחוד האירופי, לעומת זאת, דרישת המודעות כוללת מודעות בפועל או מודעות בכוח העשויה להילמד מהנסיבות או מפעולות שנוקט ספק השירותים האינטרנטיים בעצמו. עם זאת, מודעות כללית לדו־שימושיות האפשרית של השירות אינה מספיקה לשם הקמת מודעות בכוח. במקרים מסוימים, למשל במקרה של ספק תוכן שיתופי באינטרנט, ניתן משקל גם לכוונת הספק כפי שמשתקפת

382 ראו הדיון בטקסט הנלווה לה"ש 262–265 **לעיל**.

383 ראו הדיון בסעיף 1.1 **לעיל**.

מהטכנולוגיה שבה הוא משתמש או משיווק השירות על ידו, וכן מהטמעה או הימנעות מהטמעה כאמור של אמצעים טכנולוגיים מידתיים וסבירים – בהשוואה לספקים אחרים של שירותי אינטרנט – לשם מניעת הפרה.[384] חוסר האחידות בפסיקה בארצות הברית לצד ההכרה האירופית במודעות בפועל בנסיבות מסוימות פותחים פתח להכרה במודעות בכוח כמספקת בהקשר של נוזקות מעקב, בהתבסס על שיקולי מדיניות הרלוונטיים להגנה על הזכות לפרטיות. כך, אפשר למשל לטעון כי החשאיות וחוסר השקיפות של הבדיקות האמיתיות שכל חברה עורכת באשר להשלכות מוצריה על זכויות אדם, לצד ההימנעות מהטמעת אמצעים טכנולוגיים להגנה על הזכות לפרטיות – אף כי הנסיבות מלמדות כי פגיעה שכזו אפשרית ואף מבוצעת במקרים מסוימים – עשויות דווקא ללמד, לכל הפחות, על עצימת עיניים מכוונת לאפשרות של שימוש הפוגע שלא כדין בזכות לפרטיות.

6.3. תרומה משמעותית, ניכרת וממשית

דרישת התרומה המשמעותית בדוקטרינת ההפרה התורמת בדיני זכויות יוצרים התמקדה בשאלה אם בידי גורם הביניים אמצעים סבירים מבחינה כלכלית למניעת ההפרה הישירה. מבחינת הנסיבות הנלוות לשימוש לא חוקי בנוזקת מעקב נמצא שחברה המפתחת נוזקת מעקב מעניקה בדרך כלל גם שירותי תמיכה טכנית והדרכה לשימוש בנוזקה לאורך חיי רישיון השימוש. כמו כן, סביר שביכולתה של החברה המפתחת להטמיע בנוזקה מנגנון kill switch, אשר יאפשר לה להשעות את רישיון השימוש עוד לפני פקיעת הרישיון. NSO, למשל, ציינה במדיניות זכויות האדם שלה שביכולתה להפסיק את השימוש בנוזקת המעקב פגסוס עוד לפני פקיעת הרישיון, אם היא מוצאת שנעשה בנוזקה שימוש המפר את תנאי הרישיון. כלומר בידי גורם הביניים, קרי החברה המפתחת נוזקת מעקב, אמצעים סבירים מבחינה כלכלית להפסקת שימוש

384 ראו הדיון בסעיף 1.2 **לעיל**.

בנוזקת המעקב שפיתחה אם היא מגלה שבוצע בה שימוש אשר מפר את הזכות לפרטיות.

כמו כן, מפתחת נוזקת המעקב יכולה, באמצעים סבירים מבחינה כלכלית, גם למנוע מראש פגיעה בזכות לפרטיות באמצעות חסימת חלק מיכולות המעקב של הנוזקה או התניית הפעלתן באישור מורשה גישה בכיר. למשל, לפי דיווחים בתקשורת, המשטרה הפדרלית בגרמניה רכשה רישיון שימוש בנוזקת המעקב פגסוס של חברת NSO, וחלק מהפונקציות הזמינות בנוזקת המעקב נחסמו כדי להבטיח שלא ייעשה בהן שימוש לרעה.[385]

6.4. סיכום: יישום דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות בנסיבות של שימוש לא חוקי בנוזקת מעקב המוביל לפגיעה בפרטיות

יישומם של התנאים המצטברים להוכחת עוולת ההפרה התורמת בדיני הגנת הפרטיות בנסיבות של שימוש לא חוקי בנוזקות מעקב מעורר מספר קשיים. ראשית, אף שאפשר להוכיח קיומה של הפרה ישירה יש לבחון אם תנאי זה ימשיך להתקיים אם המפר הישיר נהנה מטענות הגנה. בפסיקה בישראל בחן בית המשפט את אחריותו התורמת של גורם הביניים להפרת פטנט גם כאשר המפר הישיר נהנה מטענת הגנה. הרציונל לעמדה זו קיים גם במקרה של פגיעה בזכות לפרטיות עקב שימוש בנוזקת מעקב: פגיעה חמורה בזכות וההשלכות הקשות שעשויות להיות להותרתו של הנפגע חסר סעד.

שנית, ספקות רבים מתעוררים בנוגע לשאלת המודעות הנדרשת מצד גורם הביניים. בדיני זכויות היוצרים נדרשת על פי רוב מודעות ממשית וקונקרטית

385 *German Police Secretly Bought Pegasus Spyware*, Deutsche Welle (July 9, 2021)

לשם הוכחתה של הפרה תורמת. אולם הוכחת מודעות ממשית וקונקרטית מצד מפתחת נוזקת המעקב לשימוש בנוזקת מעקב המוביל לפגיעה בלתי חוקית בזכות לפרטיות אינה פשוטה. החברות המפתחות נוזקות מעקב משווקות אותן תחת מגבלות יצוא קפדניות ולאחר שקיבלו אישורים מהרשויות הרלוונטיות במדינותיהן, ומניחות שהן אינן נדרשות לבדוק בעצמן אם מבקש רישיון השימוש יעשה בנוזקה שימוש המפר את הזכות לפרטיות. נוסף על כך, הלקוחות העיקריים שלהן הם רשויות ביון ואכיפת חוק מדינתיות, ועל כן הן טוענות כי לגיטימי מצידן להניח שלקוחות אלו יפעלו כדין לשם הגשמת תכליות לגיטימיות וחשובות כגון שמירה על ביטחון הציבור, שמירה על הביטחון הלאומי, לוחמה בטרור ומניעת פשיעה. לא זו אף זו, לטענתן אין הן נחשפות כלל למידע האישי הנאסף באמצעות נוזקת המעקב אלא רק להיבטים הטכניים הקשורים בתפעולה. מסיבות אלה אין להן מודעות ממשית וקונקרטית לפגיעה בפרטיות.

מנגד, חברות אלה מפתחות נוזקות מעקב המאפשרות רמת חודרנות חסרת תקדים תוך איסוף מידע אישי המאפשר גיבוש תמונה מדויקת על חייו האישיים ומחשבותיו הכמוסות ביותר של האדם, ולמרות זאת נמנעות מלהטמיע אמצעים טכנולוגיים שימנעו או ימזערו את הסיכון לשימוש לרעה בנוזקה תוך פגיעה חמורה בפרטיות. השילוב של רמת החודרנות הגבוהה עם הימנעות מנקיטת אמצעים סבירים למניעה או למזעור הפגיעה עשוי ללמד לכל הפחות על מודעות בכוח לאפשרות הפגיעה בזכות לפרטיות בעת השימוש בנוזקת המעקב.

אומנם, השאלה אם אפשר להסתפק בהוכחת מודעות בכוח לשם החלת דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות בנסיבות של שימוש בנוזקת מעקב היא שאלה של מדיניות. גם ההכרעה בשאלה של הוכחת דרישת ההפרה הישירה כאשר המפר הישיר נהנה מחסינות מושפעת במידה רבה משיקולים אלו. מחד גיסא, אימוצה של דוקטרינת ההפרה התורמת בנסיבות אלו יוצר כשלי אכיפה חמורים ומכביד מאוד על תעשייה הנתונה גם כך למשטר רגולטורי קפדני. מאידך גיסא, אימוץ דוקטרינת ההפרה התורמת דווקא עשוי לתמרץ את החברות המפתחות נוזקות מעקב לפעול למזעור הפגיעה האפשרית בזכות לפרטיות, למשל באמצעות צמצום הפונקציונליות של נוזקת המעקב בהתאם לנסיבות שונות, או הגברת הפיקוח על השימושים הנעשים בה

במסגרת רישיון השימוש לשם הבטחת שימוש ראוי. זאת ועוד, חוסר האחידות בפרשנות לדרישת המודעות במשפט האמריקני, האפשרות כי מודעות בכוח הבאה לידי ביטוי בעצימת עיניים מכוונת תיחשב בנסיבות מסוימות כמספקת לשם הוכחת דרישת המודעות, והעובדה שבאיחוד האירופי הכיר המחוקק והסתפק, בתנאים מסוימים, בהוכחת מודעות בכוח באמצעות הוכחת עצימת עיניים מכוונת, משמעם כי הוכחת עצימת עיניים מכוונת עשויה להספיק גם במקרה של אימוץ דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות. גם הנימוק שאין להותיר את הנפגע ללא סעד נוכח הנזק שגורמים לו מפירים רבים ומבוזרים בהקשר של זכות קניין רוחני, רלוונטי גם במקרה של פגיעה אנושה בזכות לפרטיות עקב שימוש בנוזקת מעקב. נוסף על כך, לדעתי קיים אינטרס ציבורי במתן תמריץ למפתחי נוזקות המעקב להגדיר באופן מדויק יותר את הפונקציונליות של הנוזקות שהן מפתחות ואת תנאי רישיון השימוש שלהן – ואימוץ דוקטרינת ההפרה התורמת יכול להיות תמריץ כזה. האיזון בין חיזוק הזכות לפרטיות לבין אינטרס הציבור בביטחון ציבורי ולאומי, וההתמודדות עם כשלי האכיפה הנלווים לאימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות, צריכים להיעשות בנסיבות כל מקרה ומקרה, ואינם צריכים להשפיע על ההחלטה המקדמית אם נכון לאמץ את דוקטרינת ההפרה התורמת מלכתחילה לדיני הגנת הפרטיות.

פרק 7

סיכום

נוזקות מעקב הן טכנולוגיות דו־שימושיות שיכולות לשרת אינטרסים ציבוריים חשובים כמו הגנה על ביטחון הציבור וביטחון המדינה, ולוחמה בטרור ובפשיעה. כך, לפי דיווחים בתקשורת, השימוש בנוזקות מעקב סייע לתפיסתו של קרטל סמים ולחשיפת רשת פדופילים.

אולם לצד השימושים היעילים והחוקיים, נוזקות מעקב יכולות לשמש גם למטרות שאינן חוקיות, ובראשן פגיעה חמורה בזכות החוקתית לפרטיות. קיימים דיווחים רבים בדבר שימוש לא חוקי בנוזקות מעקב לשם השתקת ביקורת נגד המשטר, פגיעה בזכות לחופש ביטוי ואף העלמת מתנגדי משטר – מטרות שבינן לבין אינטרס הציבור בביטחון ציבורי או לאומי אין ולא כלום. יתרה מזו, גם אם התכלית המוצהרת של השימוש בנוזקת מעקב היא לגיטימית, למשל אינטרס הציבור בביטחון המדינה או ביטחון הציבור, ייתכן שהשימוש עצמו בלתי חוקי ופוגע בפרטיות. דוגמה לכך ניתן למצוא בהחלטתה של פרקליטות המדינה למשוך ראיות מתיק רצח, מכיוון שאלו הושגו באמצעות שימוש שלא כדין בנוזקת מעקב.[386] הנציב העליון לענייני זכויות אדם של האו"ם אף המליץ לחדול מכל מכירה של נוזקות מעקב, העברה שלהן או שימוש בהן עד לחקיקתו של משטר המגן על זכויות אדם, נוכח הסכנה המשמעותית לפגיעה בבסיסה של הזכות לפרטיות ופוטנציאל הפגיעה בחופש הביטוי והמחשבה, גם כאשר השימוש בנוזקת המעקב הוא למען תכלית לגיטימית.[387] עמדה דומה הביע המפקח על הגנת מידע באיחוד האירופי, שהסיק שנוזקת מעקב מאפשרת רמת פולשנות חסרת תקדים שכרגע אין כל דרך להתגונן מפניה, ומשום כך, אף אם השימוש בה הוא למטרה לגיטימית, לא סביר שפגיעתה בפרטיות תיחשב מידתית.[388]

386 עמיר קורץ "הפרקליטות משכה ראיות מתיק רצח משום שהושגו ע"י שימוש ברוגלות שלא כדין" **כלכליסט** (5.6.23).

387 ראו הטקסט הנלווה לה"ש 210–212 **לעיל**.

388 ראו הטקסט הנלווה לה"ש 261–264 **לעיל**.

האסדרה הקיימת אינה נותנת מענה מספק למניעת הפגיעה החריפה והרחבה בזכות היסוד לפרטיות הנגרמת משימוש בנוזקות מעקב. הדין הבינלאומי, אשר על בסיסו מוטלות מגבלות על היצוא של נוזקות מעקב ברמה המדינתית, אינו מחייב, ובכל מקרה אינו מתייחס כלל לפגיעה האפשרית בזכות לפרטיות משום שהשיקולים המרכזיים העומדים בבסיסו הם שיקולי ביטחון המדינה ויחסי החוץ שלה, ואילו לשיקולים הנוגעים לשמירה על הזכות לפרטיות לא ניתן משקל כלל. ארצות הברית וישראל מיישרות קו ומתמקדות בשיקולים הקשורים להגנה על ביטחון המדינה ויחסי החוץ שלה בעת בחינת רישיונות ליצוא של נוזקות מעקב, ולא בהגנה על הזכות לפרטיות. יוזמות חקיקה שונות בארצות הברית אינן משנות עמדה זו אלא בעיקר מבקשות למנוע דריסת רגל של חברות מסחריות זרות בקרב רשויות האכיפה והביון האמריקניות. בישראל נהנות רשויות הביון והאכיפה מפטור רחב המאפשר להן לעשות שימוש בנוזקות מעקב גם תוך פגיעה בזכות לפרטיות, כל עוד הן עומדות במבחן הסבירות והפגיעה נעשית במסגרת התפקיד או למענו. יתרה מכך, כפי שנחשף בדוח ועדת מררי ובדיונים שהתקיימו לאחריו בכנסת, שומרי הסף האמונים על אישור השימוש בנוזקות מעקב על ידי רשויות אכיפה וביון לא הבינו לאשורה את מידת החודרנות שמאפשרת נוזקת מעקב ואת השלכותיה. החקיקה באיחוד האירופי שונה מעט, והיא מביאה בחשבון שיקולים הקשורים להגנה על הזכות לפרטיות בכל הקשור ליצוא של נוזקות מעקב, וכן מכפיפה את הפגיעה בפרטיות באמצעות נוזקת מעקב שרשויות האכיפה והביון רשאיות לגרום לדרישת הנחיצות ולמבחן מידתיות. הבשורה הגדולה מבחינת משתמשי הקצה עשויה לבוא מהצעת חוק חוסן הסייבר, המחייבת הטמעת שיקולי הגנת פרטיות כבר בשלב פיתוח מוצר טכנולוגי, אך יש להמתין לאישורה ולעקוב אחר הטמעתה בחוק המקומי בכל אחת מהמדינות החברות באיחוד. עם זאת, גם אם תאושר לא ברור אם תוכל להשפיע השפעה של ממש על פיתוח נוזקות מעקב ושימוש לרעה בהן, משום שתעשיית נוזקות המעקב נשענת על גילוין של חולשות יום אפס וניצולן, גם כאשר יצרן המוצר הטכנולוגי נוקט את כל האמצעים הדרושים לפי חוק להגנת סייבר.

מאחר שנוזקות מעקב הן טכנולוגיות דו־שימושיות, ומאחר שהשימושים אשר פוגעים בזכות החוקתית לפרטיות נעשו על ידי המחזיקים ברישיונות שימוש בנוזקה, נטען, בעיקר על ידי החברות המפתחות נוזקות מעקב, כי

אין הן אחראיות בשום צורה לפגיעה זו בזכות לפרטיות – הן רק מפתחות כלי טכנולוגי שיכול לשמש למטרות לגיטימיות וחשובות, אך יכול להיעשות בו, לצערן ולכאורה לא בשליטתן, גם שימוש פוגעני ובלתי חוקי. טענות אלו נטענו לאורך שנים בתחום דיני זכויות היוצרים בידי מפתחיהן של טכנולוגיות שאפשרו למשתמשי הקצה להפר זכויות יוצרים ביצירות אודיו ווידיאו. על בסיסן התפתחה דוקטרינת ההפרה התורמת, תחילה בארצות הברית ובהמשך גם באיחוד האירופי ובישראל. הדמיון הרעיוני שבין מפתחי מכשיר וידיאו ותוכנות שיתוף קבצים למפתחיהן של נוזקות מעקב, לצד היעדר הגנה מספקת על הזכות לפרטיות בהקשרים של נוזקות מעקב, הופכים את שאלת אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות בישראל לחשובה עוד יותר.

לכאורה, אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות אפשרי מכוח צינור הקליטה שבסעיף 12 לפקודת הנזיקין. זאת ועוד, אימוצה יוביל לחיזוק הזכות לפרטיות, הנחוץ נוכח הפגיעה המשמעותית בחשיבות הזכות ובהגנה עליה בשנים האחרונות עם הקדמה הטכנולוגית. יש בו כדי להשיב את המשקל הראוי לערכים שבבסיס הזכות לפרטיות, הנגזרת מהזכות לכבוד ומשמעותית לאוטונומיה של הפרט, להגדרתו העצמית וליכולתו לקבל החלטות בעצמו וללא התערבות זרה. כן תפתור דוקטרינת ההפרה התורמת את כשלי השוק המאפיינים שווקי מידע. היא תאפשר להתגבר על ההחצנות השליליות של פגיעה בפרטיות, ובראשן הפגיעה בצדדים שלישיים. כמו כן, חיזוק הזכות לפרטיות באמצעות אימוצה של דוקטרינת ההפרה התורמת יפתור את כשל השוק של היעדר יכולת לפעול באופן קולקטיבי כנדרש לשם שינוי מדיניות פרטיות ולשם הפסקת פגיעה בפרטיות, שהיא שולית מבחינת הנפגע הבודד אולם מהותית כאשר מובאת בחשבון התמונה הכוללת.

חיזוקה של הזכות לפרטיות נחוץ גם משום שכוחות השוק מתייחסים למידע אישי כאל כל סחורה אחרת, ולכן מתעלמים מערכים חשובים שבבסיסה של הזכות לפרטיות ואינם מסוגלים לספק לה את ההגנה הדרושה. הזכות לפרטיות אינה זכות קניינית כזכות היוצרים, אלא זכות יסוד חוקתית הנגזרת מזכותו של אדם לכבוד. שלל הגישות התיאורטיות מצביעות על כך שמדובר בזכות החיונית למימוש כבודו של האדם, הכרחית לגיבוש זהותו ותפיסתו העצמית,

לקבלת החלטות עצמאית ולהגנה מפני מבטו הממשטר של האחר. זוהי אף זכות החיונית לשם הגנה על זכויות אחרות, כגון הזכות לחופש ביטוי ולשוויון.

יתרה מכך, לחיזוק הזכות לפרטיות חשיבות רבה דווקא בישראל, משום שחוק הגנת הפרטיות הוא מיושן ואינו מותאם למציאות הדיגיטלית. עדכונו האחרון אינו כולל הוראות מהותיות, ובינתיים נדמה שישראל הופכת ל"חצר האחורית" של מדינות המערב הדמוקרטיות בכל הקשור להגנת הפרטיות.

אני סבורה כי אין ממש בטענות לפגיעה אפשרית בחדשנות עקב אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות. ראשית, בשנים האחרונות שונה האיזון שבין הזכות לפרטיות לבין חדשנות באופן חד־צדדי וחריף, תוך התרת פגיעה חמורה בפרטיות. יתרה מכך, כשלי השוק וההחצנות השליליות המאפיינים שוקי מידע אישי ומשמשים להצדקת רגולציה המחזקת את הזכות לפרטיות רלוונטיים גם להדיפת הטענות האפשריות לפגיעה בחדשנות עקב אימוץ דוקטרינת ההפרה התורמת. כוחות השוק אינם מאפשרים למשתמשים לשקף את העדפותיהם האמיתיות בנוגע לשימוש במידע אישי עליהם. נוסף על כך, טכנולוגיות עיבוד נתוני עתק מחריפות את כשלי השוק והופכות את תיקונם על ידי השוק עצמו לבלתי אפשרי. זאת ועוד, הזכות לפרטיות אינה מבוססת על אינטרסים תועלתניים כלכליים אלא על תפיסת כבוד האדם והאוטונומיה האישית שלו. אינטרסים ציבוריים כלכליים, שאותם החדשנות משרתת, הם משניים בחשיבותם לערכים אלו. משום כך, האיזון בין הזכות לפרטיות לחדשנות אינו יכול לצאת מנקודת הנחה שמדובר בזכות ואינטרס במשקל זהה, ונקודת האיזון בין השתיים צריכה להיות שונה מזו המקובלת בין זכות היוצרים וחדשנות.

מנגד, אימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי לעורר כשלי אכיפה מהותיים. האחד נוגע לדין הנוהג, להגדרת הזכות לפרטיות ולתנאים להפרתה. עם זאת, כשל אכיפה זה עשוי להצטמצם עם התרחבות השפעת ה־GDPR, המביא עימו גם האחדה מסוימת בהגדרת הזכות לפרטיות וההצדקות לפגיעה בה.

כשל האכיפה האפשרי השני נוגע לסמכות של בית משפט בישראל לדון בפעולותיה של רשות שלטונית במדינה זרה, שעשויה להיות המפר הישיר

בהקשר של נוזקות מעקב וליהנות מחסינות מתביעה בישראל. אף שזהו כשל אכיפה משמעותי, ייתכן שאפשר למצוא תקדים למצב דומה בדיני הקניין הרוחני, שבהם נבחנת אחריותו התורמת של גורם ביניים להפרת זכות יוצרים גם כאשר המפר הישיר נהנה מטענת הגנה, בנימוק שאין להותיר את הנפגע ללא סעד לנוכח הנזק הרב שנגרם לו.

גם שיקולים של צדק חלוקתי לא בהכרח תורמים לקביעה שמפתחי נוזקות מעקב הם מונע הנזק הזול ועל כן אימוצה של דוקטרינת ההפרה התורמת מוצדק. לטענת החברות המפתחות נוזקות מעקב, רישיונות השימוש בנוזקות המעקב שפיתחו ניתנים רק לרשויות ביון ואכיפת חוק במדינה ורק למטרות לגיטימיות של לוחמה בטרור ובפשיעה. נוסף על כך, החברות נתונות ממילא לרגולציית יצוא מכבידה, ואימוצה של דוקטרינת ההפרה התורמת לדיני הגנת הפרטיות עשוי להטיל עליהן נטל כבד מנשוא ולהבריח אותן מחוץ לישראל כדי לפעול במדינות שבהן המשטר המשפטי מקל יותר.

שיקולי מדיניות אלו באים לידי ביטוי בבחינת החלתה של דוקטרינת ההפרה התורמת בהקשר של פגיעה בפרטיות בשל שימוש בנוזקות מעקב. עיקר הקושי ביישומה של דוקטרינת ההפרה התורמת בהקשר זה הוא בהוכחת קיומה של הפרה ישירה ושל דרישת המודעות בפועל. באשר להוכחת הפרה ישירה, הקושי אינו נעוץ בשאלה אם הופרה הזכות לפרטיות אלא בשאלת הטלת אחריות תורמת על גורם הביניים שעה שהמפר הישיר נהנה מחסינות מפני תביעה. אולם, כאמור, הפסיקה בנושא דוקטרינת ההפרה התורמת בדיני זכויות היוצרים מספקת תקדים לבחינת האחריות התורמת גם במקרים שבהם המפר נהנה מטענת הגנה.

לעניין דרישת המודעות, הפרשנות הלא־אחידה של מהות דרישת המודעות במסגרת דוקטרינת ההפרה התורמת בדיני זכויות יוצרים השאירה פתח לקביעה כי מודעות בכוח עשויה להיות מספקת לשם הטלת אחריות תורמת על גורם הביניים. עמדות אלו באשר לשאלת ההפרה הישירה ולדרישת המודעות מקבלות לדעתי משנה תוקף נוכח האינטרס הציבורי בחיזוק הזכות לפרטיות ובקביעת איזון חדש וראוי בינה לבין אינטרסים וזכויות אחרות.

אומנם, ניסיון העבר מלמד שהשימוש בדוקטרינת ההפרה התורמת בדיני זכויות היוצרים במטרה לשלוט בטכנולוגיות שיתוך קבצים היה בפועל משחק חתול ועכבר, שעשוי להתרחש, אם לא מתרחש כבר עתה, בין המשפט למפתחי נוזקות מעקב. בתחום זכויות היוצרים הוביל משחק זה לפיתוחם של פתרונות טכנולוגיים ומודלים עסקיים חדשים, כגון חנויות המוזיקה ושירותי צפייה דוגמת נטפליקס. אבל נוכח חומרת הפגיעה בפרטיות עקב השימוש בנוזקות מעקב והשלכותיה, ספק אם נוכל להמתין להתפתחות פתרון טכנולוגי דומה.

לצד זאת, אף שנדמה שהפתרון הראוי הוא אסדרה בחקיקה של שימוש בנוזקות מעקב, אין זה פתרון מעשי לעת עתה. חקיקה ברמה המדינתית, ועל אחת וכמה ברמה הבינלאומית הדרושה לשם יישור קו בכל הנוגע לשימוש בנוזקות מעקב, אורכת זמן רב. במהלך שנים אלו עשויה הפגיעה בפרטיות להתעצם ועימה גם הפגיעה בזכויות יסוד אחרות, כגון הזכות לחופש ביטוי. נוסף על כך, אף אם תגובש אסדרה בינלאומית, סביר שמדינות שאינן דמוקרטיות לא יצייתו לה כלל. לפיכך למרות הקשיים נראה שיש חשיבות בפיתוחה של דוקטרינת ההפרה התורמת בדיני הגנת הפרטיות, וההתאמות הנדרשות נוכח הקשיים שהיא עשויה לעורר יבוצעו בעת יישומה בפועל בנסיבות כל מקרה ומקרה. דוקטרינת ההפרה התורמת תהיה כלי נוסף בארגז הכלים הקיים לשם התמודדות עם פגיעות חמורות בזכות לפרטיות. אין זה הכלי העיקרי, ואין הכוונה להציבו כחלופה לאסדרת השימוש בנוזקות מעקב. עם זאת, דוקטרינת ההפרה התורמת היא כלי שיורי וחשוב, שאף שעשויים להיות לשימוש בו גם חסרונות, יש בידו כדי לסייע ולתרום לחיזוק הנחוץ והכרחי של הזכות לפרטיות.

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy Paper 197

VIOLATION OF PRIVACY BY SPYWARE

The Manufacturer's Contributory Infringement

Rachel Aridor-Hershkovitz

August 2024

Text Editor [Hebrew]: Hamutal Lerner

Series and Cover Design: Studio Alfabees

Typesetting: Irit Nachum

Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-458-6

No portion of this book may be reproduced, copied, photographed, recorded, translated, stored in a database, broadcast, or transmitted in any form or by any means, electronic, optical, mechanical, or otherwise. Commercial use in any form of the material contained in this book without the express written permission of the publisher is strictly forbidden.

Copyright © 2024 by the Israel Democracy Institute (RA)

Printed in Israel

The Israel Democracy Institute

4 Pinsker St., P.O.B. 4702, Jerusalem 9104602

Tel: (972)-2-5300-888

Website: en.idi.org.il

To order books:

Online Book Store: en.idi.org.il/publications

E-mail: orders@idi.org.il

Tel: (972)-2-5300-800

All IDI publications may be downloaded for free, in full or in part, from our website.

The views expressed in this policy paper do not necessarily reflect those of the Israel Democracy Institute.

ABSTRACT

The covert use of spyware by regimes—particularly non-democratic ones—has raised significant concerns regarding its impact on fundamental human rights. Journalists, human rights defenders, lawyers, and political dissidents are frequently targeted by this invasive technology, which, once installed on their devices, enables the comprehensive surveillance of their private and professional lives. Spyware can access personal communications, trace social connections, and monitor a target's activities and thoughts, leading to the suppression of dissent and stifling freedom of expression. This abuse poses a severe threat to press freedom, privacy, and other human rights.

However, spyware also serves lawful purposes. Intelligence agencies and law enforcement authorities worldwide employ spyware to combat terrorism and serious crime. Striking a balance between the legitimate use of spyware in the interest of public security and the need to curb its misuse to prevent human rights violations presents a significant challenge for both society and lawmakers. In Israel, these concerns are especially relevant, as both domestic and international spyware exports involve Israeli technology companies.

While international regulations exist to control the export of spyware, these frameworks, particularly in Israel and the United States, remain largely security-oriented, placing minimal emphasis on protecting privacy rights. By contrast, the European Union (EU) addresses privacy concerns more directly, mandating that any encroachment on privacy by law enforcement or intelligence agencies must adhere to strict principles of necessity and proportionality. This difference highlights the inadequacy

of current international regulations and underscores the need for more robust safeguards to protect against privacy violations caused by spyware abuse.

This policy paper critically examines Israel's current legal framework concerning spyware, analysing its limitations in addressing the growing threat to privacy posed by these surveillance technologies. In particular, the paper assesses the permissive regulatory approach that prioritizes national security and foreign relations over privacy protections, a stance that mirrors US policy. The study compares these frameworks with EU law, which offers a more privacy-focused regulatory approach. Through this comparative analysis, the paper aims to illuminate the gaps in Israeli law and provide a clearer path for its legislature to adopt a balanced approach to privacy and security.

One potential solution offered by this paper is the adoption of the contributory infringement doctrine, borrowed from intellectual property law, as a legal tool to hold spyware developers accountable for privacy violations. The doctrine of contributory infringement would enable courts to impose liability on developers who contribute to or facilitate the misuse of their spyware, even when direct offenders, such as government agencies, may be shielded by sovereign immunity or other defenses. This approach could enhance the protection of privacy rights by placing an additional burden on spyware developers to ensure their technology is not misused, while also reinforcing accountability mechanisms.

The paper delves into the practical challenges of applying the contributory infringement doctrine within Israel's legal system. Key issues include defining the scope of privacy violations, determining jurisdiction in transnational cases, and establishing the extent of spyware developers' knowledge about the illicit use of their technology. For example, how should an Israeli court assess whether the privacy of a foreign journalist, targeted by spyware developed in Israel, has been violated? Should Israeli law or the law of the victim's country apply in such cases? These

jurisdictional and enforcement challenges are further complicated by the fact that spyware developers often claim compliance with export regulations and limit their customer base to authorized governmental agencies.

Despite these difficulties, the paper argues that adopting the contributory infringement doctrine could incentivize developers to introduce stricter controls over the use of their technologies. By establishing clearer guidelines and definitions around spyware licensing and permissible usage, companies can help mitigate the risk of privacy violations and protect against the abuse of their products. The EU's General Data Protection Regulation (GDPR), which has promoted greater uniformity in defining privacy rights and violations, is explored as a potential model for guiding this approach.

Furthermore, the paper acknowledges potential enforcement failures, such as difficulties in proving the developer's knowledge of misuse or determining liability when spyware is used by foreign government authorities. Nevertheless, the paper argues that courts have long held intermediaries accountable in cases of copyright infringement, even when direct infringers have claimed legal defenses. This precedent supports the case for applying contributory liability in the context of privacy protection.

Finally, the paper proposes that the Israeli legislature consider integrating the contributory infringement doctrine as a supplementary tool to existing regulations. While not a comprehensive solution, the doctrine would serve as an essential residual mechanism to address grave violations of privacy, particularly when other avenues for enforcement are limited. This approach would enhance Israel's legal framework by offering a balanced response to the dual-use nature of spyware—protecting both national security and the fundamental right to privacy.

The conclusion emphasizes that while contributory liability may not be without its disadvantages, its adoption is necessary to ensure the proper functioning of privacy protection in the digital age. By aligning Israel's

legal framework with international standards and adopting a nuanced, case-by-case approach to spyware regulation, this paper provides a clear legislative path forward for Israeli lawmakers. The ultimate goal is to foster a legal environment that effectively balances national security with the protection of individual privacy, ensuring that spyware technologies are used responsibly and transparently.

עיתונאים, פעילי זכויות אדם ומתנגדי משטר עשויים להיות תחת מעקב תמידי וחודרני שלא נראה כמותו בעבר. נוזקת מעקב מוחדרת בהיחבא למכשירי הטלפון שברשותם ומאפשרת למפעילה גישה לכל אורחות חייהם ומחשבותיהם: ללוח הזמנים שלהם ולמיקומם הגיאוגרפי, לתכתובת ההודעות האישיות שלהם, לתמונות ולסרטונים שצילמו במכשיר ואף לשיחות שניהלו בין באמצעות המכשיר ובין שלא. מעקבים אלו פוגעים בזכויות יסוד כגון הזכות לחופש ביטוי והזכות לפרטיות ומובילים לאפקט המצנן את חופש העיתונות.

נפגעי המעקבים חסרי אונים. גם כאשר הצליחו להתחמק מהמעקב, אין בידם אפשרות מעשית לתבוע פיצוי בגין הפגיעה החמורה בזכויותיהם. המחקר המובא לפניכם מבקש לענות על השאלות האלה: האם יש אפשרות לתבוע את מי שנתן מלכתחילה בידי אותם משטרים אפלים את כלי המעקב החודרניים הללו? האם דינן של החברות המפתחות את נוזקות המעקב כדינן של תוכנות שיתוף הקבצים מתחילת שנות ה־2000? האם NSO צריכה לשאת באחריות תורמת לפגיעה המבוצעת באמצעות נוזקת המעקב פגסוס שפיתחה, בדומה לאחריות שהוטלה על נאפסטר או גרוקסטר להפרת זכויות היוצרים שביצעו משתמשיהן?

ד"ר רחל ארידור הרשקוביץ היא חוקרת בתוכנית "דמוקרטיה בעידן המידע" במכון הישראלי לדמוקרטיה; בעלת תואר שלישי במשפטים מהפקולטה למשפטים באוניברסיטת חיפה, בוגרת תואר ראשון במשפטים מאוניברסיטת חיפה ותואר שני במשפטים מאוניברסיטת ניו יורק. תחומי המחקר שלה הם פרטיות, הגנת סייבר, רשתות חברתיות ואתגרי המציאות הפיג'יטלית.

מחיר מומלץ: 45₪

ספטמבר 2024

מסת"ב:
978-965-519-458-6

0 4500001345 2
דאנאקוד 450-1345

www.idi.org.il