המלצות לאיסוף מידע גלוי ברשת (OSINT) תוך צמצום חשיפה משפטית

מהדורה 1.0 - 24.10.23

מטרת המסמך היא להציג דגשים משפטיים מרכזיים רלוונטיים לפעילות של איסוף מידע ממקורות גלויים – Open Source Intelligence, או בקיצור OSINT.[1]

הדגש במסמך הוא על צמצום חשיפה משפטית בעת ביצוע פעילות OSINT בהיבטים של דיני מחשבים (הפעלת כלים ממוחשבים ואיסוף מידע בהיבט המחשובי), דיני פרטיות (היבטים של איסוף ושימוש במידע אישי), דיני חוזים (בכל הקשור לתנאי שימוש של אתרים ופלטפורמות), ודיני קניין רוחני.

מומלץ לעיין גם במסמכים משלימים, העוסקים בהיבטים נוספים מעבר לאיסוף בנושא שרשרת ראייתית, בנושא שימוש הוגן, ובנושא היבטי פרטיות של שימוש בחומרים בהם מתועדים נפגעים.

מסמך זה נועד לידע והדרכה כלליים בלבד. הוא עוסק בסוגיות מורכבות, שחלקן לא קיבלו מענה בפסיקה או בהנחיות רגולטוריות, ואינו מיועד להיות עצה משפטית. המסמך מתמקד בדין הישראלי בלבד. מחבריו אינם נושאים באחריות להסתמכות על האמור בו בלא לקבל ייעוץ מקצועי מעורך-דין מיומן בתחום.

מי אנחנו

אנחנו קבוצה של כשלושים משפטנים ומשפטניות שעוסקים בתחומי הקניין הרוחני, פרטיות, אינטרנט, מהאקדמיה ומהפרקטיקה, שפועלים כדי לסייע בייעוץ משפטי ראשוני למיזמים חברתיים, לא מסחריים, שמבקשים לקדם פעולות חברתיות בזמן המלחמה, לטובת אזרחי ישראל. אנו פועלים בהתנדבות. פירוט חברי וחברות הקבוצה נמצא כאן.

פנו אלינו

אנו זמינים לשאלות בנוגע למסמך זה בפניה בדואר אלקטרוני – 101@law.co.il.

[1] להרחבה כללית על פעילות OSINT בהקשר הנוכחי ראו את המסגרת שפותחה ב"פרוטוקול ברקלי" – מסמך שגובש בידי נציב זכויות האדם של האו"ם ואוניברסיטת ברקלי, והוא נועד לסייע באיסוף ראיות על פשעים בזירה הבין-לאומית, כולל בידי ארגוני חברה אזרחית: Berkely Protocol on Digital Open Source Investigations: Human Rights Center at UC Berkely School of law, United Nations Human Rights Office of the High Commissioner, Berkely Protocol on Digital Open Source Investigations, https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

הנחות עובדתיות

הדיון כאן מניח פעילות שמקיימת את המאפיינים הבאים:

1. פעילות ה-OSINT מוגבלת לאיסוף ותיעוד מידע על אודות פעילות עוינת הקשורה במלחמת חרבות ברזל ותגובות לה בעולם;

2. מטרת הפעילות היא לצורכי מודיעין, תיעוד, והליכים משפטיים עתידים, וכן פעילות הסברה, חינוך, התמודדות, ופעילות חברתית הכרוכות בכך;

3. אופי הפעילות הוא ציבורי, לא מסחרי. הפעילות לא נועדה להפקת רווח או תועלת אישית או מסחרית כלשהי.

4. ככל שאיסוף המידע נעשה באמצעות טכנולוגיית Data Scraping, היא אינה מצריכה עקיפה של הגנות טכנולוגיות, שימוש לא מורשה בסיסמאות, פענוח הצפנה או קוד, יירוט ופענוח של תעבורה מוצפנת, יירוט של תכתובות דואר אלקטרוני, חדירה למאגרי מידע או למרשמים ארגוניים פנימיים או פעולות דומות.

5. על פעילות הכוללת גם הפצה של תוצרים האיסוף יש לבחון היבטים נוספים (ראו: מסמך בנושא פרטיות).

אם הפעילות <u>אינה</u> מקיימת תנאים אלה ניתן לפנות אלינו להבהרות והשלמות.

מסמך זה עוסק בהיבטים של דיני מחשבים, היבטים של דיני פרטיות, תנאי שימוש, והיבטי קניין רוחני. בכל אחד מתחומים אלה, המסמך מציג את ההמלצות בצורה ממוקדת, ולאחר מכן, סוקר את ההיבטים המשפטיים הרלוונטיים.

דיני מחשבים

בקיצור

- פעילות **OSINT** כוללת איסוף מידע ממחשבים ושרתים מרוחקים.
- דיני המחשבים בישראל וברוב העולם אוסרים על חדירה למחשב של אחר שלא כדין.
- הכללים שלהלן מוצעים להכוונת פעילות **OSINT** שנעשית בידי יחידים וארגונים לא מסחריים, שאינם גורמי אכיפה, למטרות של הסברה, תיעוד, ומיזמים חברתיים-ציבוריים שונים בקשר למלחמה.
- הכללים המוצעים נועדו לצמצם סיכונים משפטיים:
  - באופן כללי, יש לאסוף מידע שזמין לכלל הגולשים, כלומר, לא לבצע פריצה או מניפולציה כדי להגיע למידע.
  - מותר לאסוף מידע פומבי שזמין לכל ברשת ללא רישום או סיסמה, בהתאם לפרוטוקולי תקשורת מקובלים;
  - יש להימנע מהפעלת תוכנה על גבי השרתים מהם נאסף המידע;
  - יש לצמצם את ההשפעה של פעילות האיסוף על פעולת השרתים מהם נאסף המידע, ולהימנע מהכבדה לא סבירה עליהם, כגון פניות מרובות בפרק זמן מצומצם;
  - אין לפרוץ מנגנון טכנולוגי שמגן על אתר או פלטפורמה;
  - ניתן לעשות שימוש בשם בדוי לצרכי הגנה על פעילות החוקר, אולם לא בזהות של אדם אחר.

בהרחבה

1. סעיף 4 לחוק המחשבים, התשנ"ה-1995, קובע כך:

> "החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו מאסר שלוש שנים; לעניין זה, 'חדירה לחומר מחשב' חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר, תשל"ט."

2. מטרת הסעיף היא למנוע "פריצה" למחשבים, כלומר גישה למחשב ללא רשות.

3. רשת האינטרנט מבוססות על קשר בין שרת מחשב שעליו פועל אתר אינטרנט או רשת חברתית, לבין המחשב של המשתמש. על רקע זה, עולה השאלה באילו נסיבות כאשר המחשב של המשתמש מתחבר לשרת המחשב שמפרסם את המידע לצורך פעילות איסוף, ידנית או ממוכנת של המידע, הפעילות עלולה להיות "התחברות שלא כדין".

4. לצורך כך נציג בקצרה את פרשנות הסעיף בישראל, ולאחר מכן את ההנחיות של משרד המשפטים האמריקני לגבי סעיף דומה בקשר ל-OSINT.

הדין בישראל והנחיית פרקליט המדינה לגבי מדיניות העמדה לדין ביחס לעבירה

5. בפסק הדין בעניין *מדינת ישראל נ' עזרא* שניתן בדצמבר 2015, קבע בית המשפט העליון כללי פרשנות להוראות חוק המחשבים:[2]

- "חדירה" למחשב תפורש באופן מרחיב וכללי, כך שכל מידע "שנכנס" למחשב, בין שנוצר על ידי מחשב אחר ובין שנוצר כתוצאה מפעילות המשתמש במחשב מקימה את הדרישה ההתנהגותית לביצוע העבירה.

- "חדירה שלא כדין" מתייחסת לכל חדירה שבוצעה ללא הסכמת בעל המחשב.

- עקיפה או פריצה של מנעול טכנולוגי היא פעולה חמורה יותר מאשר חדירה "פשוטה", ולבן מצדיקה את החמרת הדין כלפי מבצע העבירה, וזאת לעומת חדירה שבוצעה ללא עקיפה או פריצה כאמור.

6. באוגוסט 2018 פורסמה הנחיית פרקליט המדינה, שקובעת את מדיניות ההעמדה לדין והענישה בעבירה של חדירה שלא כדין לחומר מחשב.[3]

- ההנחיה עוסקת בשיקולים שמנחים את התביעה לגבי העמדה לדין בעבירה זו.

- ההנחיה אימצה את קביעות בית המשפט בעניין עזרא, אך הדגישה שהנטל להוכיח שהחדירה בוצעה ללא הרשאה מוטל על התובע. כאשר קיימת עמימות בשאלת ההרשאה לגישה למחשב ועולה ספק סביר לעניין גבולות ההרשאה – יפעל הספק לטובת החשוד.

---

[2] רע"פ 8464/14 **מדינת ישראל נ' עזרא** (נבו 15.12.2015).

[3] הנחיות פרקליט המדינה הנחיה 2.38 – מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב (אוגוסט 2018).

- ההנחיה קובעת כי בשל תחולתה הרחב יחסית של העבירה, יש להימנע מהעמדה לדין בשל מעשים של מה בכך.

- ההנחיה מפרטת נסיבות לחומרה המגבירות את הנטייה להעמיד לדין בגין העבירה, וביניהן, כשהעבירה נעשתה כדי לעבור עבירה אחרת, כשנגרם נזק ישיר או עקיף בעקבות החדירה לחומר המחשב, כשהחדירה הביאה לפגיעה בצנעת הפרט (כדוגמת חשיפת תמונות אינטימיות), כשהופק רווח כלכלי כתוצאה מהחדירה וכשבוצעו פעולות להתגברות על מנעולים טכנולוגיים.

- בהתאם להנחיה כל עוד אין הפרה של הוראות בעל המחשב בנושא "הרשאת גישה", אין הפרה של הוראות חוק המחשבים. ההנחיה מבחינה בין הפרה של הרשאת גישה (שהיא הפרה של חוק המחשבים), לבין הפרה של "הרשאת שימוש", שאינה הפרה של חוק המחשבים, אולם עלולה להיות הפרה של דינים אחרים כמו דיני החוזים או דיני הפרטיות. (על דיני החוזים ודיני הפרטיות ראו להלן).

- כך למשל אדם שאינו מורשה לגשת לחומר מחשב (למשל תיקיה של עובד אחר), וניגש אליו, יחשב כמפר את חוק המחשבים. לעומת זאת אם אדם מורשה לגשת לחומר (למשל לתיקיית עבודה), אולם הוא ביצע בחומר שימוש שאינו מורשה, אז כפי הנראה לא תהא הפרה של איסור החדירה.

חשיפה גלובלית וההנחיה האמריקנית

7. הוראה דומה לסעיף 4 לחוק המחשבים הישראלי בדבר איסור על "חדירה שלא כדין" מופיעה באמנת בודפשט להתמודדות עם פשיעת סייבר,[4] ולכן זו נורמה כמעט אוניברסלית, שהחשיפה אליה היא מעבר לדין הישראלי בלבד.

8. עקב כך, להשלמת התמונה ומבלי להתיימר לכסות את הדין הבין-לאומי, נזכיר שני מסמכים רלוונטיים של משרד המשפטים האמריקני: מדיניות אכיפה לגבי הסעיף המקביל לעבירת החדירה לחומר מחשב, ומסמך לגבי המלצות לגבי רכישת מודיעין שנאסף במרחב הסייבר.[5]

---

[4] Counsel of Europe, Convention on Cybercrime, Budapest 23.11.2001, No. 185, Article 2, available at https://rm.coe.int/1680081561. Counsel of Europe, Convention on Cybercrime, Explanatory report to the convention on cybercrime, ss. 44-50, p 9-10, available at https://rm.coe.int/16800cce5b.

[5] U.S. Department of Justice, Prosecution Policy 9-48.000, Computer Fraud and Abuse Act (19.05.2022), available at https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act להלן: "Prosecution Policy".
U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Division, Cybersecurity Unit, Legal Considerations when Gathering Online Cyber Threat Intelligence and

❖ מדיניות האכיפה של משרד המשפטים האמריקני מציינת כי בכלל, לא תהיה העמדה לדין בגין חדירה שלא כדין לחומר מחשב בגין חריגה מהרשאה חוזית בלבד, הקבועה בתנאי שימוש למשל.[6]

❖ במסמך לגבי מודיעין שנאסף במרחב הסייבר, נאמר כי אין מניעה לבצע את הפעילות כל עוד מתקיימים התנאים הבאים:

i. איסוף המידע מאתרים או מפורומים הזמינים באינטרנט, הוא פסיבי;

ii. הוא נערך בהתאם לכללי הנגישות הרגילים למידע;

iii. איסוף המידע נעשה בדרך של "צילומי מסך" או בטכניקה דומה;

iv. אפילו האיסוף נעשה תוך שימוש בשם בדוי - כל עוד השם הבדוי איננו שמו של אדם אמיתי.[7]

לעומת זאת, אם נעשה שימוש בסיסמאות או בזהויות שנגנבו, או שהייתה עקיפה של מנעולים טכנולוגיים, הסיכון להפרת הוראות החוק גבוה יותר.[8]

דיני פרטיות במידע

בקיצור

❖ דיני הגנת הפרטיות מתירים איסוף ועיבוד של מידע אישי (personal data), בהתאם לכללים שמטרתם צמצום הסיכון לפרטיות. מידע אישי הוא כל מידע על אודות אדם מזוהה, או כאשר האדם ניתן לזיהוי.[9] האדם הוא נושא המידע (data subject).

❖ הכללים המוצעים לצמצום סיכונים משפטיים:

- איסוף מידע שאיננו על בני אדם - למשל על פעילות של מדינות, ארגונים, תאגידים וכדומה - אינו מוסדר בדיני הגנת הפרטיות.

Legal considerations, :להלן ,Purchasing Data from Illicit Sources, Version 1, February 2020 available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

6 ראו Prosecution Policy, בעמ' 4.

7 Legal Considerations, בעמ' 3.

8 Legal considerations, בעמ' 4-5.

9 הגם שהחוק הישראלי מגדיר "מידע" ו"מידע רגיש", נשתמש פה במונח "מידע אישי", ברוח הדין האירופי (כמו גם המלצות ה-OECD ומסמכים משפטיים בין-לאומיים אחרים).

- איסוף מידע על אדם מזוהה, או על מי שניתן לזיהוי (הנחת העבודה היא שבדרך כלל מידע שנחזה להיות לא מזוהה ניתן בכל זאת לזיהוי, בהינתן משאבים מספקים), צריך להיעשות לפי דיני הגנת הפרטיות.

- איסוף מידע אישי ממקורות גלויים ברשת (כפי שתואר לעיל בהיבטי מחשבים) אינו מייצר סיכון גבוה כשהוא נעשה לצורך תיעוד ושימור ראיות, מודיעין או לשם ביסוס טענות משפטיות בנוגע למלחמה הנוכחית, תוך שמירה על המידע שנאסף מפני שימוש שלא למטרות אלה.

- איסוף מידע על בסיס הנחיה או הוראה חוקית מפורשת של גופי ביטחון עשוי להיות פטור מאחריות משפטית.

- אם הפעילות כוללת שימוש במידע שנאסף למטרות אחרות (כגון לפרסם את המידע ברבים), יש לבחון את היבטי הפרטיות בנפרד, לדיון ראו במסמך זה.

בהרחבה

הגנת הפרטיות ו-OSINT - כללי

1. חוק הגנת הפרטיות אוסר על פגיעה בזכותו של אדם לפרטיות ללא הסכמתו (סעיף 1 לחוק). סעיף 2 לחוק מגדיר פעולות שונות שעולות לכדי פגיעה בפרטיות.[10] פעולות אלה מחייבות "הסכמה מדעת, במפורש או מכללא" של האדם שפרטיותו נפגעת (סעיף 3 לחוק). בנוסף, גם אם אדם נותן הסכמה מדעת, במפורש או מכללא, עיקרון יסודי של דיני הפרטיות הוא עקרון "צמידות המטרה" האוסר שימוש במידע שנמסר למטרה אחת, למטרה אחרת.[11]

2. בהתאם לכך, השאלה הראשונה היא האם ניתן לומר שהמידע שאותו אוספים במסגרת ה-OSINT פורסם בהסכמה מדעת, מפורשת או מכללא של האדם. בנוסף, גם אם ניתן לומר שהאדם הסכים לפרסום המידע, למשל פרסום רגיל ברשת חברתית, האם ניתן לומר שאיסופו בידי גורם אחר, למטרה אחרת, מקיים את עיקרון צמידות המטרה. זו שאלה תלוית הקשר משפטי

[10] הפעולות שהן פגיעה בפרטיות כוללות בין היתר מעקב, האזנת סתר, צילום אדם ברשות היחיד או פרסום של צילום מביך, פתיחת מכתבים (כולל דיגיטליים), שימוש בשמו של אדם למטרת רווח, הפרת חובת סודיות שנקבעה בדין או בהסכם, פרסום מידע אישי מסוים, ועוד. לפי הפסיקה, זו אינה רשימה סגורה.

[11] ראו סעיף 2(9) לחוק הגנת הפרטיות: "שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה" – הוא פגיעה בפרטיות. כלומר, פעולה הפוגעת בפרטיות, בהקשר זה, מתממשת בהתקיימם של שני תנאים מצטברים: (1) שימוש בידיעה על ענייניו הפרטיים של אדם; (2) שימוש בידיעה שלא למטרה שלשמה נמסרה.

וטכנולוגי. לעיתים ברור מהנסיבות שאדם מעוניין לפרסם מידע, ולכן אין מניעה משפטית ומותר לאסוף ולהשתמש במידע - ולעיתים הדברים מורכבים יותר.[12]

פרטיות – OSINT ואיסוף מידע לצרכי מודיעין, ביטחון, תיעוד או שימור ראיות בהקשר המלחמה

3. בהקשר להיבטי הפרטיות, יש להבחין בין שלושה סוגים של בעלי זכויות פוטנציאלים:

   - ❖ קורבנות של פעילות מלחמתית שמידע על אודותיהם כלול במידע שנאסף;
   - ❖ צדדים שלישיים שאינם קורבנות ואינם קשורים לביצוע הפעילות;
   - ❖ מחבלים וגורמים עווינים שהפעילות אודותם מתועדת במידע שנאסף.

4. הנחת העבודה היא כי לגבי הקבוצה האחרונה, של מחבלים וגורמים עוינים אחרים, מאחר שמדובר במידע פומבי שלא הושג תוך הפרה של דיני המחשבים, יש אינטרס ציבורי לגיטימי מובהק באיסוף התיעוד, ולכן אין צורך לבחון היבטי פרטיות נוספים.

5. לגבי קורבנות וצדדים נוספים, העובדה שהמידע פורסם ברבים אינו מסיר ממנו את הגנת דיני הפרטיות. בהקשר שלפנינו, נראה כי המטרה של "תיעוד או שימור ראיות" היא מטרה שניתן להניח לגביה הסכמה מכללא של מי שמתועד במידע. יודגש כי לעניין הפצה נוספת לא בהכרח ניתן להניח כך, ולכן יש לבחון את הדברים בנפרד. (ראו כאן). בנוסף, סעיפים 18(2) ו -18(3) לחוק הגנת הפרטיות מקנים הגנה בגין פגיעה לכאורה בפרטיות, כאשר הפגיעה נעשתה בתום לב למשל, בשל חובה מוסרית או חוקית או תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל. ככל שפעולת האיסוף והעיבוד מתבצעת לפי הנחיה של רשות ביטחון, ייתכן שהפעולה פטורה לפי סעיף 19(ב) לחוק.

6. נדגיש, כי לאחר איסוף המידע יש להקפיד כי המשך העיבוד והשימוש במידע נעשים בהתאם לכללי שימוש ששומרים שהשימוש במידע הוא למטרות הנדרשות בלבד, ומונעים שימוש למטרה אחרת. שיטה מקובלת לעשות זאת היא על ידי החלת מעטפת אבטחת מידע על אופן

---

[12] רשויות הגנת הפרטיות האירופיות פרסמו הודעה משותפת בנושא "איסוף נרחב" (data scraping), שמדגישה את המשך התחולה של דיני הפרטיות גם על מידע שפורסם ברבים, באופן שאיסוף נרחב עלול להיות הפרה של הדין, ואת האחריות של הפלטפורמות לעיצוב מנגנונים טכנולוגים להסדרת נושא זה. המטרות השליליות שמצביעות עליהן הרשויות באיסוף מידע גלוי נרחב הן: איסוף מידע מקדים לצורך תקיפת סייבר, גניבת זהות, מעקב אחר משתמשים ועריכת פרופילים שלהם, מעקב פוליטי ומודיעיני לא חוקי בידי רשויות ביטחון ממשלתיות, הצעת פרסומות וספאם. ראו Information Commissioner's Office, Joint Statement on data scraping and the protection of privacy (August 24, 2023), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/08/joint-statement-on-data-scraping-and-data-protection/.
במסמך זה, הנחת העבודה היא שמטרת האיסוף והשימוש אינה למטרות אלה, ולכן, הדברים רלוונטיים במידה פחותה.

השמירה והשימוש במידע. להיבטים אלה יש השלכה גם על שימור השרשרת הראייתית, כפי שמפורט במסמך נפרד בנושא.

חוזים - הפרת תנאי שימוש

בקיצור

- "תנאי השימוש" של אתרים, יישומונים (אפליקציות) ורשתות חברתיות קובעים לעיתים מגבלות על היכולת לאסוף מידע באופן נרחב.
- הכלל המוצע לצמצום סיכונים משפטיים הוא לפעול למטרות שתוארו מעלה (תיעוד ושימור ראיות, מודיעין או לשם ביסוס טענות משפטיות בנוגע למלחמה הנוכחית), בלי להפר את חוק המחשבים כפי שתואר לעיל, וכל עוד הפעילות אינה מביאה לשיבוש או האטה בפעילות האתר.

בהרחבה

1. השימוש במידע הנכלל באתר אינטרנט או ברשת חברתית כפוף לתנאי השימוש של האתר. במסגרת שימוש בטכנולוגיית Data Scraping, שמפעילה תוכנות רובוטיות שמבצעות חיפוש באתרי אינטרנט (שלא במנוע החיפוש הפנימי של האתר עצמו), העמידה בדרישות החוזיות תיבחן באופן נקודתי בהתאם לתנאי השימוש של האתר שממנו נשאב המידע.

2. במקרים רבים תנאי השימוש אוסרים על הפעלת תוכנות מחשב אוטומטיות לסריקה והעתקה של מידע או לאחזור מידע מהאתר. כמו כן, תנאי שימוש עשויים לאסור על פתיחת חשבון באתר תחת שם פיקטיבי או התחזות לאדם אחר (התחזות לאדם מסוים אחר היא גם עבירה פלילית לפי חוק העונשין הישראלי). כאשר מדובר בפלטפורמות, כמו רשתות חברתיות שונות, עשוית להיות הוראות נוספות שיש לבחון.[13] תוקפם החוזי של תנאי השימוש של אתרי אינטרנט נדון פעמים ספורות בבתי המשפט בישראל, ומהפסיקות עולה שהגישה המקובלת היא שהסכם מקוון תקף, ככל שהוא משקף את ההסכמה המשוערת של הצדדים לאור הנסיבות הכוללות של העניין ובהתחשב בכך שיש לראות את החוזה המקוון כחוזה אחיד.[14] נעיר, שנטייתם של בתי המשפט בישראל להכיר בתוקפו של הסכם מקוון גדולה יותר כאשר המשתמש מסכים לו באופן אקטיבי (clickwrap agreements), זאת לעומת הסכמים שההסכמה עליהם ניתנה

---

[13] ראו את המידע באתר איגוד האינטרנט: https://www.isoc.org.il/netica/question-and-answers/online-scams/imposter-profile.

[14] ת"א (מחוזי תל אביב) 1963-05-11 **מלכה נ' אווא פיננסי בע"מ** (נבו 25.6.2014). ראו גם ת"צ (מחוזי תל אביב-יפו) 64880-02-18 **הראל נ' פאנקו גרופ בע"מ** (נבו 25.7.2021). לסקירה מקיפה ראו ת"א 18763-04-15 **ויוה מדיה בע"מ נ' Google Ireland Ltd.,** (נבו 26.8.2019).

באופן פסיבי, כדוגמת תנאי שימוש שהגולש מסכים להם מעצם גלישתו באתר (browsewrap agreements).

9. כאמור, על בחינת ההפרה של תנאי השימוש במסגרת פעילות האיסוף המתבצעת באמצעות Data Scraping להיעשות באופן נקודתי מול הסכם תנאי השימוש בכל אתר אינטרנט שממנו נאסף המידע.

ככלל, הפרת תנאי השימוש עשויה להתקיים בעת פעילות האיסוף בשני מצבים עיקריים: (1) תנאי השימוש באתר דורשים פתיחת חשבון המחייב הזדהות בשם אדם אמיתי, אך פעילות האיסוף מתבצעת באמצעות חשבון פיקטיבי או מעקף טכנולוגי העוקף את דרישת פתיחת החשבון; (2) תנאי השימוש באתר אוסרים על העתקה של מידע, אחסון המידע במערכות אחזור מידע, שימוש בכלי סריקה והעתקה אוטומטיים או איסורים דומים, אך פעילות האיסוף מתבצעת תוך ביצוע פעולות כאמור.

10. ייתכן שככל שיימצא שפעילות האיסוף מנוגדת לתנאי השימוש, טענת הגנה אפשרית היא שבידיהם של בעלי האתר למנוע, באמצעים טכנולוגיים פשוטים, את פעילות ה-Crawlers או ה-Spiders על גבי האתר. משבחרו שלא לעשות כן, יש לראות אותם כמי שבחרו שלא לאכוף את תנאי השימוש שלהם ונתנו הסכמה משתמעת לפעילות איסוף כזו על גבי האתר.

11. אם תוגש תביעה לסעד בגין הפרת תנאי השימוש, התובע יידרש להוכיח, בין השאר, נזק שנגרם לו כתוצאה מההפרה. להערכתנו, גם אם בית המשפט ימצא שהופרו תנאי שימוש של האתר, הרי שמפעיל האתר יתקשה להוכיח נזק שנגרם לו כתוצאה מפעילות האיסוף, וזאת כל עוד איסוף המידע במסגרת פעילות ה-OSINT לא גרם למחיקת מידע, להאטה בפעילות האתר או הרשת, או לנזקים דומים אחרים. עם זאת, יודגש שהאתר עשוי להפעיל אמצעים טכנולוגיים למניעת פעילות האיסוף גם מבלי לנקוט הליכים משפטיים.

12. בתי המשפט בישראל טרם דנו בסוגייה של הפרה של תנאי השימוש כאשר המטרה היא ביצוע פעולה בעלת לגיטימציה חברתית גבוהה, כפי שמתואר במסמך זה. ניתן להניח כי במסגרת זאת יישקלו שיקולים הקשורים לאופי הפעילות, מידת ההפרעה שלה הטכנולוגית והמסחרית שלה לפעילות התקינה של האתר או הפלטפורמה, האם היא נעשית למטרת רווח, והיחס של הפלטפורמה עצמה לתכנים שנאספים.

קניין רוחני

1. צילומים, סרטים או טקסטים עשויים להיות מוגנים על ידי דיני זכות יוצרים, ולכן השימוש בהם מוסדר גם באמצעות דינים אלה.

2. אם מטרת הפעילות מושגת ללא שימוש ביצירה עצמה, אלא רק באיסוף נתונים עובדתיים או טכניים (למשל נתונים מספריים גולמיים ללא פרשנות עליהם, עיבודים שלהם, מבלי להעתיק סדר או ארגון ייחודי שלהם, וכדומה)– מוטב לפעול כך. עובדות כשלעצמן אינן מוגנות בדיני זכויות יוצרים.

3. אם הפעילות אוספת יצירות מוגנות, כגון תמונות, סרטונים או טקסטים, נדרש להתייחס לעקרונות השימוש המפורטים במסמך המלצות בנושא זה.

מסמך זה נכתב על ידי:

- עו"ד עמית אשכנזי
- עו"ד ד"ר עמרי רחום טוויג, משרד פישר; אוניברסיטת תל-אביב

העירו הערות:

- פרופסור מיכאל בירנהק, אוניברסיטת תל אביב
- עו"ד נועה דיאמונד, הקליניקה לפרטיות, אוניברסיטת תל אביב
- ד"ר דלית קן דרור פלדמן, הקליניקה למשפט וסייבר, אוניברסיטת חיפה
- עו"ד חיים רביה, משרד פרל כהן צדק לצר ברץ