# פרטיות בעידן המודרני

מאת לירון ויניק

יוני 2020

# חשיבות הפרטיות, הבדלים בין פעם והיום

הזכות לפרטיות היא זכות יסוד ואחת מזכויות האדם החשובות בישראל. הזכות עוגנה בחוק יסוד: כבוד האדם וחירותו, הקובע כי כל אדם זכאי לפרטיות ולצנעת חייו, ובהסדרים בכמה חוקים אחרים.חוק הגנת הפרטיות, התשמ"א 1981 – (להלן -חוק הגנת הפרטיות או החוק) קובע את הכללים להגנה על פרטיותו של אדם. בדומה לזכויות יסוד אחרות, הזכות לפרטיות אינה מוחלטת וכשהיא מתנגשת עם זכויות אחרות או עם אינטרסים ציבוריים אחרים, נדרש איזון בין הזכויות

בעשורים האחרונים הפך המידע למשאב מרכזי ורב ערך, לרבות ערך כלכלי. גם הנורמות החברתיות המשתנות מרגילות את הציבור למסור מידע אישי, וזה נאגר במאגרי מידע, ברשתות החברתיות ובמאגרים ממשלתיים, הכוללים מידע רב ורגיש הנוגע לכל היבטי חייהם של בני האדם .לפיכך, לצד תועלתה העצומה של ההתפתחות הטכנולוגית לאדם ולחברה, עלולה להיפגע הזכות לפרטיות.

**מהי פרטיות?**

ד"ר מיכאל בירנהק, מחבר הספר "מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה", חושב שמדובר במונח שעובר שינוי. "הפרטיות היתה מאז ומעולם מושג דינמי, שמשתנה כל הזמן לפי שינויים חברתיים ,תרבותיים וטכנולוגיים - וכמובן משפטיים. הפרטיות לא מתה, אבל היא כן נתונה במתקפה חזיתית מכיוונים רבים, שמאיימים עליה בו-זמנית."

מעולם לא הייתה הגדרה מדויקת ושקופה למושג פרטיות. איך יתכן הדבר לאחד המושגים החשובים ביותר של זמננו ואחד היסודות ה"מקודשים" של המודרניות. יש לפרטיות מעמד מרכזי בכל תחום בחיינו כיום, אם זה בין אדם לעצמו ולסביבתו, או בין אדם למחשבותיו האישיות. אפילו מציינים לכבוד הפרטיות יום בשנה

– Data Privacy Day – החל בתאריך 28 בינואר.

**הפרה של פרטיות** היא מונח קצת יותר חד וצלול. הפרה של פרטיות לא חייבת להתבטא בחשיפה של מידע אישי בפני כל האנשים הקיימים בעולם – כל גישה לא רצויה למידע פרטי, גם אם מדובר באדם אחד בלבד ,היא כבר הפרה של פרטיות. ככל שיותר אנשים חשופים לאותו מידע פרטי ,כך ההפרה חמורה יותר.

למרות שיש אנשים אשר קנאים לפרטיותם, יש גם את אלה שאינם ממהרים להסתרר ואף חפצים לשתף את נחלת הכלל בפעולותיהם או מחשבותיהם האישיות.

**הצורך בחשיפה**

הצורך בחשיפה תמיד היה קיים בנו משחר הימים. אם בעבר האנשים אשר היו חושפים מידע על מעשיהם ומחשבותיהם היו שחקנים, סופרים ויוצרים אשר נתנו לחברה לעבור דרך ''דלתות התודעה'' הפרטיות שלהם, נראה שבעידן של היום עם ההתקדמות המטאורית של הטכנולוגיה, החשיפה גדלה מיום ליום ומאבדת פרופורציות בהיקפים חסרי תקדים. היום, בשונה מבעבר, אנשים החולקים מידע ברשתות החברתיות, מגיעים לכמות עצומה של אנשים תוך זמן קצר לכל הדעות.

# דרכי פעולה – תקיפה

סיפור רקע קטן:

אחת מפרשות האבטחה הגדולות ביותר של השנים האחרונות הגיעה לסיומה עם מאסרו של היו מין נגו – האקר וייטנאמי בן 25 שלפי האישומים נגדו, הצליח לגנוב ולאסוף מידע אישי של כ 200 מיליון אמריקאים, ולמכור אותם בפורומים מחתרתיים באינטרנט. ההאקר הצעיר נעצר על ידי השירות החשאי האמריקאי והובא למשפט – שם נגזרו עליו לא פחות משלוש עשרה שנות מאסר.

בין הפרטים שנגנבו על ידי היו מין נגו היו כתובות, מספרי טלפון, מספרי ביטוח לאומי ואף נתונים פיננסיים כמו מספרי כרטיסי האשראי וחשבונות בנק – ששימשו למשיכה של כ 60 מיליון דולר מאזרחים אמריקאים בין השנים 2007 ל- 2013.

חתיכת סיפור אה?

גניבת זהות לא אומרת שאותו אדם המבצע את העבירה הופך בין לילה למותקף שלו – הגניבה יכולה להתבטא גם בפעולות קטנות המשרתות את אותו התוקף – ברוב המקרים מדובר בפעולות הקשורות בתחום הכלכלי.

גניבת זהות יכולה גם לבוא לידי ביטוי בדרכים שונות – אדם יכול להשתלט על חשבון הפייסבוק שלנו כדי להפיץ הונאות או פרסומים זדוניים, הוא יכול להשתמש בכרטיס האשראי שלנו או לעשות העברות כספים בשמנו לגורמים כאלה ואחרים. ישנם מקרים נדירים יותר בהם הצליחו התוקפים להשתלט על זהויות של אנשים שנפטרו על מנת להתחמק מלתת דין וחשבון על פשעים בשמו של התוקף.

תחום כלכלי הזכרנו?

גניבת זהות מבוצעת עבור אחת או יותר מהסיבות הבאות:

משיכת כספים מחשבון הבנק של הקורבן. השתלטות על חשבונות או קבצים של הקורבן למטרת כופר. הפצת הונאות ברשתות החברתיות או בדואר האלקטרוני - השגת מידע אישי או רגיש על ידי השתלטות על חשבון הדואר האלקטרוני האישי או העסקי של הקורבן.

לא די בכך, אפילו המקום שאמור להיות ''חוף המבטחים'' שלנו, מבצרנו האישי, הלא הוא ביתנו שלנו, מדליף אודותינו מידע מבלי שאנו בכלל שמים לב, במכוון או לא במכוון. מכשירים טכנולוגיים שאנו מכניסים בצורה תמימה אל ביתנו, משמשים לעיתים לרעתנו.

אם אלה הטלויזיות החכמות אשר עוקבות אחרי התוכן בו אנו צופים, אם אלה מערכות הבית החכם IOT (internet of things) אשר מקשרות בין כלל מכשירי הבית, והופכים אותו למטרה קלה ונוחה להאקרים מנוסים לנסות ולפגוע בנו, ואפילו מצלמות האבטחה אשר אמורות להגן עלינו מפני פורצים או איומים – מתעדות את הפעולות שלנו יום ביומו. ואם כבר חשבנו שראינו הכל, אפילו הרמקולים החכמים של ענקיות הטכנולוגיה, מאזינים בחוכמה לכל המתרחש בבית

כמעט ואין כיום פעולה שאנו עושים, שלא משאירה אחריה עקבות של מידע שעובר לגוף מסויים בסופו של דבר, בין אם בהסכמה ובין שלא בהסכמה, במודע ושלא במודע. כל המידע שאנו מעבירים יוצר מאגר גדול מאוד של מידע כזה או אחר אשר מאפשר לארגונים עסקיים לנצל זאת לטובתם, או לממשלים ומשטרים (לרוב דקטטורים כמו מדינות הרב או סין לדוגמא), למנוע מאיתנו חופש תנועה, הבעת דעה ולעקוב אחר פעולותינו.

והדובדבן שבקצפת - גם הדמוקרטיה הגדולה בעולם הלא היא ארה"ב הגדולה, מבצעת מעקב וניטור של מכשירי טלפון ותקשורת אינטרנטית בכל מקום בו היא יכולה באמצעות ארגוני ביון ובראשם ה NSA, -בתוך ומחוץ לארה"ב במטרה למנוע טרור, אך כפי שחשף ביוני 2013 בחור בשם אדוארד סנודן ל"הגארדיאן" ו-ל"וושינגטון פוסט" חומר מסווג על תוכניות סודיות ביותר של הסוכנות לביטחון לאומי, כולל תוכניות מעקב בשם PRISM ו – Muscular.
לאחר מכן נמלט סנודן לרוסיה לבקשת מקלט מדיני, ונכון ל2017 עדיין מתגורר ברוסיה במקום לא ידוע.

# דרכי פעולה – הגנה

הפעולות הבסיסיות שאנו מבצעים לרוב בקלילות דעת ולא מקדישים להן חשיבות בשימושינו במרחב הדיגיטלי, מאשרים לתוקפים לעשות רווח קל על חשבונינו, אך עם קצת רצון ויכולת, כל אחד יוכל להקשות ולהגן קצת יותר מפני איומים כאלה ואחרים בשימוש והקפדה על הכללים הבאים:

**שימוש בסיסמאות חזקות –** נכון, למי יש כוח לזכור סיסמא המורכבת מתווים מרובים, או שלרוב הסיסמא מודבקת על גבי פתק למסך המחשב, אך יש להימנע מההרגלים המגונים האלה ולהתייחס לחשיבות הסיסמא בכובד ראש. מומחי אבטחה רבים טוענים שזמנן של הסיסמאות עבר מזמן ויש לעבור להשתמש במנגנוני הגנה טובים יותר, אך עד שאותם מומחים ימציאו לנו מנגנון אבטחה יעיל ושימושי שיחליף את אותן סיסמאות אנחנו צריכים להקפיד על שימוש בסיסמאות חזקות שיקשו פושעי הרשת להשתלט על החשבונות שלנו. האקרים מיומנים יוכלו לפרוץ כל סיסמה – לא משנה עד כמה היא חזקה – בעזרת הכלים והמשאבים המתאימים, אבל לרוב הם יוותרו על השקעת זמן רב בפריצה לחשבון מאובטח כאשר ישנם מיליוני חשבונות שאינם מאובטחים.

כיום קיימים הרבה מאוד שירותים חינמיים או בתשלום ליצירת סיסמאות ושמירתן והם מסייעים לנו לאבטח את המידע שלנו בצורה טובה יותר. *נכון שתלוי בשירות, אך אציין שבכמה שירותים מצויינים מוציאים יותר כסף על תספורת במספרה מאשר על רישיון.

סיסמה חזקה היא כזו המורכבת משילוב רנדומלי של ספרות, סמלים ואותיות לועזיות "גדולות וקטנות" – כמה שיותר הרי זה משובח. סיסמאות כמו "123" או "Aa123456" הן סיסמאות כל כך חלשות עד שהן יפרצו תוך שניות והן לא יגנו על החשבונות או המידע שלכם – עם זאת הרבה מאוד גולשים עדיין משתמשים בהן.

**אימות כפול –** לאחר שהכנסתם שם משתמש וסיסמא לאותו אתר או שירות אשר חפץ בו ליבכם, תקבלו למכשירכם קוד אימות חד פעמי אשר אותו תצטרכו להזמין בנוסף לפרטים אשר מסרתם. מטרת הקוד היא לאמת את זהותכם. רוב החברות הגדולות משתמשות בקוד זה ואף מעודדות שימוש במנגנון זה.

**הקפדה על כללים בסיסיים של גלישה בטוחה – <u>חשוד</u>** היא המילה המרכזית - הימנעות מלחיצה על קישורים חשודים או פתיחת קבצים חשודים או כאלו שמגיעים ממקור לא ידוע או מפוקפק, לא לספק פרטים אישיים לאתרים מפוקפקים או כאלה שתומכים בדפדפן אקפלורר (חה חה) וכו'. אחת מהפעולות הנפוצות ביותר של האקרים ברשת היא להתחזות לגופים מוכרים או אפילו אנשים שאתם מכירים מרשימת אנשי הקשר שלכם, כדי לנסות לגרום לכם להיענות לדרישתם ולהשרות תחושת היכרות וביטחון – **עליכם להיות חשדניים גם אם הכל נראה תמים.**

**הגנו על חשבונות המדיה החברתית שלכם –** פה יש אבסורד מאוד גדול – מטרת הדגל של כלל הרשתות החברתיות של היום היא לעודד אותנו המשתמשים לשתף כמה שיותר מידע על עצמינו, חברינו, הורינו, סבינו, דודינו וכל מי שיש לו בעצם דופק. האקרים יודעים זאת היטב ומשקיעים משאבים רבים כדי לחטוף חשבונות מדיה חברתית וזהויות.

אז אמרנו לחזק את הסיסמא, אמרנו להגביל את מסירת הפרטים האישיים ברשת, ואמרנו לחשוד בכל אתר או מייל שנראה חשוד, אך הדבר הטוב ביותר שיעזור לכולנו להתמודד עם איומי הרשת הגדולה והמסוכנת, הוא לסגל לעצמינו דפוסי התנהגות חדשים. אחת הפעולות הפשוטות והראשוניות היא להגביל את המידע שאנחנו חושפים ברשתות החברתיות לחברים שלנו בלבד (ע"י שינוי בהגדרות הפרופיל) או מחיקת המידע הרגיש לחלוטין. **<u>לא</u>** לשתף מידע אישי כמו כתובת מגורים, מספר טלפון או פרטי זיהוי כמו מספר תעודת זהות, מספר דרכון או מספר רישיון נהיגה – **<u>וכמובן שלא</u>** נתונים פיננסיים כמו מספרי חשבון בנק וכרטיסי אשראי.

**הקפידו לעדכן תוכנות במחשב** – תוכנות המחשב שלנו חשופות לפרצות דרכן יכולים האקרים לחדור לנו למחשב, לכן מומלץ להשתמש בתוכנות חוקיות ועדכניות, על אחת כמה וכמה מערכת האנטי וירוס. אלפי וירוסים חדשים מיוצרים יום יום ולכן חשוב לעדכן את מערכת האנטי וירוס שתתעדכן באותם האיומים החדשים הקיימים ותדע להוסיף אותם למאגר האישי שלה. מערכות נוספות שיש להקפיד לעדכן הן מערכת ההפעלה, דפדפנים ואת תוכנת הג'אווה.

# OSINT

**מהו אותו המונח OSINT?**

OSINT הם ראשי התיבות ל- **O**pen **S**ource **Int**elligence

התקדמות הטכנולוגיה של ימינו הובילה עמה בין היתר הרבה מאוד שינויים שנעשו ברמת הנגישות הציבורית למידע. בעקבות העובדה שהטכנולוגיה נמצאת בכל מקום, נגישה בכל שעה ויותר מזאת, נגישה כמעט לכל יד, אנו רואים שינויים אדירים במרכזי המודיעין הגלוי , (OSINT) בתחומים רבים.

בזכות קיומו של תחום ה-OSINT אנחנו חשופים לכמויות מידע אדירות, אשר לרוב באות לידי שימוש על ידי קבוצה הנקראת אנליסטים מודיעיניים (מודיעין עסקי, כלכלי, חברתי, צבאי בטחוני וכו') ,לזיהוי סיכונים פוטנציאליים חבויים, או בהמלצות לקבלת החלטות אסטרטגיות.

**מתי הOSINT בא לידי ביטוי?**

אם תחשבו על זה, כמעט כל שימוש שלנו באינטרנט הוא שימוש בOSINT – אם אלו תוצאות חיפוש כלשהו, צפיה בחדשות או קבלת מידע על רכישת מוצר אשר אנו מתעניינים בו – כל זה הוא OSINT. כולנו חשופים למידע הגלוי הזה.

עד עכשיו נראה שתחום הOSINT הוא מאוד חיובי מה שהופך אותו לכלי מאוד שימושי, אז איפה בעצם הבעיה?

הבעיה היא בעצם ריבוי המידע שהולך וגדל כל יום, יוצר "הצפה" של מידע באינטרנט, ובחסות בעיה זאת נוצרה בעצם מערכת ריכוז וניהול הידע בצורה טובה יותר, כי כיום אף אחד לא אוהב לא לקבל את התוצאה שהוא מבקש במרחק כמה קליקים אחדים וכמה שיותר מהר.

על מנת לכרות (to mine) או למצוא את את המידע הרלוונטי לנו בכל מאגר המידע העצום כיום , נכון להשתמש בכלי ניהול ידע - באופן ספציפי בכלי כריית מידע (נקרא בשפה המקצועית text mining\data mining)

**ערכו של המודיעין הגלוי**

המטרה העיקרית של מודיעין גלוי אפקטיבי, הוא כריית המידע הנכון והטוב ביותר עבורנו.
**ההצלחה העיקרית שלו היא השילוב בין מידע איכותי וכמותי**, הרי אם נוכל למצוא את המידע הרלוונטי והאיכותי ביותר עבורנו, הרי זה הופך אותנו לאפקטיביים יותר. דוגמה טובה לכך היא סקרי שוק והשוואות בין שווקים לצורך שיווק מוצר חדש כלשהו.

על מנת לשווק מוצר חדש בצורה טובה, עלינו לבדוק מספר קריטריונים, בהם הבולט ביותר הוא האם ישנה דרישה בשוק למוצר. במידה ויש דרישה השאלה מתרחבת כמו עץ יוחסין לתתי שאלות - איזה גילאים צורכים הכי הרבה ממנו? באיזה אזור יקנו ממנו יותר? התפלגות קלות התפעול של המוצר על ידי אוכלוסיות שונות, תלות המוצר במגדר, גיל, יכולות מוטוריות, ועוד.

לאחר מענה על שאלות אלו וניתוח שוק מוצלח, נקבל יותר נתונים סטטיסטיים (**כמות**) וככל שנדע יותר את דעת קהל היעד שלנו (**איכות**), כך המוצר/שירות/פתרון שלנו יצליח יותר ויניב לנו יותר אחוזי הצלחה.

**ה OSINT קיים ברשתות החברתיות**

ניטור המידע והידע ברשתות החברתיות היא התחלה טובה כדי להתחיל לשווק את המוצר שלך ולגלות מה אנשים שונים בקהילות השונות חושבים על כך. השימוש ברשתות החברתיות הוא מאוד נוח מכיוון שמדובר בפריסה רחבה מאוד של מרחב הציבור - כלומר מעבר לכך שהרשת החברתית היא כלי חברתי למען שיתוף אספקטים שונים בחיי היומיום של כולנו –הוא ציבורי, ונגיש לכל החפץ בכך. כלומר אחוז מאוד גבוה מהמידע הזה הוא לא פרטי (על סמך העובדה שאותו אדם בוחר לשתף את המידע שלו או לא בצורה ציבורית) אך כמובן שיש גם מידע פרטי, אבל הוא לא נחשב כחלק מהמידע הגלוי.
גם בעולם המודיעיני בטחוני הרשתות החברתיות מספקות מודיעין גלוי. לדוגמה - במידה והצבא מחפש אדם מסוים אשר מסית בדעותיו הפוליטיות או סביר להניח שמתכנן פעולת טרור כלשהי, הצבא יכול להשתמש ברשת החברתית בכדי לאתר אותו, לראות מה הוא כותב בפרופיל הפייסבוק שלו ,לחפש נקודות "צ'ק אין" שלו, תמונות שמעידות על מיקומו, מי הם חבריו בפייסבוק, באיזה מקומות הוא נוהג להסתובב ועוד.
משמע - **רשתות חברתיות בשילוב עם OSINT מאיצות את התהליך של גילוי ושיתוף של מידע וידע.**

שילוב שכזה הופך את התהליך לקל יותר, מהיר יותר ויעיל יותר ופותח בפנינו עולם שלם של מידע וידע, שהיה ככל הנראה בלתי נראה בשימוש בכלים מסורתיים ושגרתיים יותר.

# הבדלים בגישה ביחס לפרטיות וחיסיון מידע

בעקבות התפתחות הטכנולוגיה בשנים האחרונות והזרמת המידע ההולך וגדל כל יום ביומו, הועלו גם דעות רבות על המושג פרטיות בעידן של היום. בזירת הפרטיות לכאורה, עומדים אחד מול השני שני גורמים אינטרסנטים שנלחמים זה בזה בתוך מלחמה כוללת שניטשת כבר כמה שנים: המעצמות החדשות מצד אחד, והממשלות, המעצמות הישנות, מנגד.

**האדם בלב מאבק הפרטיות**

בלב המערכה נמצא, כרגיל, האדם – שעבור צד הממשלות הוא נחשב אזרח, ועבור הצד של המעצמות החדשות הוא נחשב לצרכן. רוב האנשים כלל לא מבינים על מה המהומה ומדוע שני הצדדים נאבקים על משהו שנתפש כלא חשוב או עקרוני. מי שקובע את הטון הדברים והתוכן מספקות מעצמות הדיגיטל, שמושכות את העולם לכיוון פתיחות, הסרת הגבלות ועיצוב מחדש של דעת הקהל. מולן עומדים הגופים הריבוניים והממשלות, שנוטעים את העקרונות של העולם הישן, ובשם זכויות האזרחים מנסים לעצור את אוקינוס המידע הזורם ברשת.

**האם פרטיות קיימת ביום?**

בכל יום ביומו כיום מתבצעת חדירה לפרטיות שלנו, במודעות או בעקיפין. לכל מקום שאנו הולכים או בכל מקום שאנו עוברים בו, אנו משאירים ''עקבות דיגיטליות'' של עצמינו – המידע הזה נאגר ומצטבר ויש האומרים שלעולם לא יעלם.

כמעט כל פעולה, אפילו אם נראית הכי תמימה, מעידה על מעשינו, רצונותינו וכיוונינו – אם זה ניתור הטלפון שלנו דרך אפליקציות ניווט כגון וויז ומוב-איט, התחברנו לרשת אלחוטית בבית קפה אקראי – ניתור למיקומינו והאתרים אליהם אנו גולשים בעזרת הסלולרי או האפליקציות בהן אנו משתמשים

שימושים בשירותים כגון נטפליקס, ספוטיפיי, העברנו כספים לחברים דרך ביט – כל המידע נאגר, נצבר, מעובד, מפוצל ומשפיע על מהלך חיינו.

במקרים טובים - כל המידע שנאסף יציע לנו תכנים מותאמים אישית להעדפותינו, תכונה חיובית לכל הדעות, אך במקרים הפחות טובים - כל המידע שנאסף ומועבד, יציג לנו הצעות ופירסומות מציקות לרכישת מוצרים או שירותים אשר אמורים לשפר את רמת איכות החיים שלנו, ימכר לצדדים שלישיים דרך ענקיות הטכנולוגיה או יפתח אצל חלקינו תכונות סכיזופרניות כמו תהייה מסויימת על הפעם האחרונה אשר שקלנו לקנות מכסחת דשא בעלת התקן Bluetooth.

כדי שנגיע למידע שיסייע לנו כבני אנוש, בעלי רצונות ודפוסי התנהגות הייחודיים לנו, אנו נדרשים להפקיד בידי "מתווכים טכנולוגיים" (כגון חברות ענק כמו גוגל ופייסבוק), חלק מהמידע אודותינו. כלומר, בכדי להבדיל את עצמנו ואת הייחודיות שלנו משאר האנשים הסובבים אותנו, אנו נאלצים להסכים למידה מסוימת של פגיעה וחדירה בפרטיות שלנו ע''י שימוש בשירותים אלה ומסירת פרטים אשר נשארים בשרתים של אותן החברות. אנו מניחים כי המידע שאנו מפקידים בידם יסייע להם להנגיש לנו את המידע המועדף והרלוונטי ביותר עבורנו, וכך - אנו מקווים - נצליח להשיג את מבוקשנו ולממש את האישיות הייחודית שלנו.

**פרטי כנורמליזציה**

יש גישה האומרת שאין יותר דבר כזה, 'פרטי', כיוון שהפרטי שאנחנו מתייחסים אליו כרגע הוא תוצאה של נורמות חברתיות. העולם הטכנולוגי התפתח והגבולות למידע בו תושתשו, וכל המידע זמין בלחיצת כפתור - אין במה לאיים על הפרט. הוא יכול לעשות מה שבא לו, איך שבא לו ומתי שבא לו. מתרחש תהליך של התרוקנות ה'אני' מהמשמעות הסמנטית ההיסטורית שלו, והתהליך הזה נמצא עכשיו בשיאו, לא מעט בזכות הקפיצה הטכנולוגית.

**המאבק על שליטה במידע**

עקרונית אם מסתכלים טוב, אפשר לראות ששני הצדדים בכלל לא מנוגדים בדעותיהם, והמאבק ביניהם הוא לא על זכויות הפרט – אלא על שליטה במידע. מי שמחזיק במידע על הצרכנים/ אזרחים הוא זה שיוכל לשלוט בהם, ובצורה זאת לחלוש על כל העולם. מידע על האזרחים או מידע בכללי הוא אחד הנכסים החשובים ביותר כיום, והממשלות נחרדות מהאפשרות שלנגד עיניהן קמים גופים אחרים, עוצמתיים, ששואבים את כוחם מאותו מידע שעד היום אפשר להן בלבד לשלוט באזרחים. הגופים המסחריים, מנגד, הרבה יותר מהירים ובעלי משאבים מהממשלות, מה שהופך אותם ליעילים יותר מולם, והם משתמשים בדרכם במידע על הצרכנים ורותמים אותו לצרכיהם. האינטרס הבסיסי שלהם הוא לחלץ כמה שיותר מידע על המשתמשים, ובכך למקסם מהם את הרווחים.

# בבליוגרפיה


OSINT applications against criminality

https://expertsystem.com/osint-applications-3-examples/

Open Source Intelligence from a Knowledge Management perspective

http://www.kmrom.com/Site-En/Articles/ViewArticle.aspx?ArticleID=467

Privacy remains a big issue in today's smart home

https://venturebeat.com/2019/05/15/privacy-remains-a-big-issue-in-todays-smart-home/

How to Turn Off Smart TV Snooping Features

https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/

גניבת זהות

https://he.wikipedia.org/wiki/%D7%92%D7%A0%D7%91%D7%AA_%D7%96%D7%94%D7%95%D7%AA

הזכות לפרטיות

https://he.wikipedia.org/wiki/%D7%94%D7%96%D7%9B%D7%95%D7%AA_%D7%9C%D7%A4%D7%A8%D7%98%D7%99%D7%95%D7%AA

כל מה שרציתם לדעת על גניבת זהות, ואיך להתגונן מפניה

https://www.haaretz.co.il/captain/net/1.2268533

זהות בדויה

https://www.globes.co.il/news/article.aspx?did=719093