**משפט וטכנולוגיה – רועי צרפתי**

נהלים:

מבחן – 100%, חומר סגור.

מטיב – עד 5 נק', השתתפות פעילה ותורמת ללמידה.

מתווה הקורס:

1. רקע ומסגרת אנליטית
2. גורמי הביניים והשאלות שהם מעוררים ברשת האינטרנט
3. אסדרה ואכיפה באמצעות גורמי ביניים – ניטור תוכן ברשת, זכויות יוצרים ברשת
4. יישוב סכסוכים במרחב המקוון
5. בתי משפט מקוונים, המהפכה הטכנולוגית בבתי המשפט בתקופת הקורונה
6. כלים אלגוריתמיים בפעולות אסדרה ואכיפה
7. כלים אלגוריתמים בהחלטות שיפוטיות, מנהליות
8. הגינות אלגוריתמית
9. פרטיות והגנת מידע בעידן הדיגיטלי
10. שירותים משפטיים מקוונים, ליגל – טק (טכנולוגיות משפטיות).

# מבוא

מטרת הקורס הינה לספק מבט-על שחוצה את גבולותיהם של תחומי משפט מובחנים או דוקטרינות ספציפיות. נעסוק בהסדרה ההדדית של משפט וטכנולוגיה.

עידן של מהפכות טכנולוגיות (אמצע שנות ה-80 ועד ימים אלו):

כיום אנו נמצאים בעידן, בו פעולות שעד מס' שנים התבצעו באופן אוף-ליין, מול ימים אלו, בהם רוב הפעולות מבוצעות במרחב המקוון, ברשתות. טכנולוגיות מידע חדרו לכל תחומי החיים שלנו. האינטרנט הפך לזירת פעילות חברתית, מסחרית-כלכלית, מקצועית, ציבורית, פוליטית ולעיתים אף עבריינית / טרוריסטית.

ישנו קושי מובנה עם סוגיות טכנולוגיות משום שטכנולוגיה מתפתחת בקצב מהיר ודינמי, שרק הולך וגדל. בתקופת הקורונה הפיתוח החל להיות מהיר עוד ועוד. בעוד שחקיקה ופסיקה לוקחות שנים ארוכות. (ביג דאטה, אלגוריתמים, מכונות אוטונומיות וכו'). הצורך הוא אבי ההמצאה.

טענה אפשרית היא כי הממשק בין משפט וטכנולוגיה נוגע בעיקר ליישום ע"י החלת כללים משפטיים קיימים על טכנולוגיה חדשה או עיצוב כללים חדשים. למשל – התאמת דיני הגנת הצרכן למסחר אלקטרוני. אבל? יש טכנולוגיות פרסונליזציה, מאפייני עסקאות, C2C? מתווכים?

## הפער הדיגיטלי:

הפער הדיגיטלי מתייחס לעובדה שעדיין עם כל החדירה הזאת של הרשת ושל המידע, עדיין קיימים סקטורים קיימים בעולם בהם אין להם כלל גישה לאינטרנט, או שמא גישה לטלפון חכם. בנוסף, אין להם אפשרות להחיל ולהפעיל את הטכנולוגיה באופן אפקטיבי.

פער דיגיטלי = תופעה חברתית וכלכלית הקשורה להתפתחויות הטכנולוגיות הדיגיטליות של [עידן המידע](https://he.wikipedia.org/wiki/%D7%A2%D7%99%D7%93%D7%9F_%D7%94%D7%9E%D7%99%D7%93%D7%A2). המונח שמתאר פער בין אוכלוסיות המתגוררות באזור מוגדר, קהילה או מדינה, שיש להן גישה, כישורים, התקנים, תקשורת או מיומנויות לעשות שימוש בטכנולוגיות החדשות, לבין אוכלוסיות אחרות ללא כל אלה. מדובר באי-שוויון כלכלי וחברתי בין קבוצות של בני אדם בנגישות ובשימוש בטכנולוגיה דיגיטלית.

# התפתחות המרחב הדיגיטלי וטכנולוגיות המידע

האינטרנט כפלטפורמה לתקשורת בין אישית:

1. הפצת מסרים: דוא"ל, מודעות, פורומים וכו'.
2. שירותים: מתווכים, מנועי חיפוש, מדיה חברתית וכו'.

דיגיטציה של מוצרים:

1. האינטרנט כרשת להפצה של מוצרים.
2. התרחבות של הכלכלה השיתופית (Uber, Airbnb וכו').
3. ביזור באחסון ובעיבוד של מידע.

האינטרנט כרשת של תקשורת עם "דברים":

1. מכשירים חכמים (שעון חכם, מקרר חכם וכו').
2. טכנולוגיות מידע (ICT) מתרחבות לכלל תחומי החיים.
3. חיישנים מתקדמים, תקשורת סלולרית 5G וכו'.

אלגוריתמים, מערכות אוטונומיות, רובוטים:

1. Big data analytics
2. אינטליגנציה מלאכותית (AI), למידת מכונה ולמידה עמוקה
3. אינטראקציה בין תוכנה לחומרה, רובוטים שמחליפים פעולות של בני אדם בעולם הפיזי – המכונית האוטונומית, הבית החכם, שליח רחפן...

יישומיים רחבים:

1. מד טק
2. ליגל טק
3. פינטק (Fintech)

מודלים טכנולוגיים ביזוריים, מסחור:

1. בלוקצ'יין (Blockchain)
2. ביטקוין (Bitcoin)
3. NFT
4. DAO וכו'.

כיצד משנה הטכנולוגיה את העבודה המשפטית עצמה?

"מי יכתוב חוזים חכמים – עו"ד או שמא מתכנת?"

בימים אלה, עם עליית החוזים החכמים המבוססים על טכנולוגיית בלוקצ'יין, נדמה שהשאלה שהוכרעה – עבודתו של עו"ד תחייב מיומנויות ריאליות מובהקות לכל הפחות ואולי אף הבנה מעמיקה בתכנות.

ישנו קושי מובנה עם סוגיות טכנולוגיות משום שטכנולוגיה מתפתחת בקצב מהיר ודינמי, בעוד שחקיקה ופסיקה לוקחות שנים ארוכות (ביג דאטה, אלגוריתמים, מכונות אוטונומיות וכו').

## טענה אפשרית – הממשק בין משפט וטכנולוגיה נוגע בעיקר ליישום:

1. החלת כללים משפטיים קיימים על טכנולוגיה חדשה או עיצוב כללים חדשים.
2. כיצד מערכת המשפט מתמודדת עם הצורך בשינוי והתאמה? עם עקרונות משפטיים, מושגי שסתום, פרשנות משפטית וכו'.. בנוסף גם בעזרת חקיקת משנה, הנחיות מנהליות, סמכויות רגולטוריות, פסיקה וכו'...

כיצד מערכת המשפט מתמודדת עם הצורך בשינוי והתאמה?

לדוג' – התאמת דיני הגנת הצרכן למסחר אלקטרוני, או שמא לעסקאות C2C.

C2C = צרכן מול צרכן (Consumer 2 Consumer).

לדוג' – התאמת דיני התעבורה והאחריות למכוניות אוטונומיות. מהו נהג סביר בתנאי הדרך? האם ישנה יכולת לצפות נזק?

לדוג' – מערכות אלגוריתמיות שמקבלות החלטות מנהליות? מה לגבי חובת הנמקה? לגבי החלטה סבירה? תשתית עובדתית? האם ישנה זכות ערעור?

דוגמאות אלו למעשה מעלות כי ישנו צורך בפיתוח פרדיגמה לבחינת סוגיות המערבות משפט וטכנולוגיה.

## טענה חלופית – קצב התפתחות המשפט אינו תואם את קצב ההתפתחות הטכנולוגית:

חוק מור (Moore) – לפיו כוח המחשוב מכפיל את עצמו בכל 18 חודשים לערך. אציין כי חוקי המשחק השתנו עם המחשוב הקוונטי.

טכנולוגיות מידע מחוללות תהליכי שינוי בקצב, בעוצמה וברוחב יריעה חסרי תקדים.

טענה אפשרית היא שכאשר נתקלים במצב חדש אנחנו לוקחים את המסגרת הנורמטיבית הקיימת, מבינים איך היא חלה במקרה הנדון ומיישמים אותה. עושים זאת בעזרת היקש, פרשנות, מושגי שסתום אליהם יוצרים תוכן. הקושי עם זה הוא שישנן טכנולוגיות המאתגרות הנחות יסוד של המצב המשפטי הקיים. למשל – רובוט הוא ילד? חיית מחמד? תאגיד? לכן, יש לפתח מערך כולל חדש של תפיסות על מנת להתמודד עם אותם מקרים.

טכנולוגיות מידע המחוללות תהליכי שינוי בקצב, בעוצמה וברוחב היריעה חסרי תקדים הופכים את המשפט לדי חסר אונים.

אם הגישה שלנו היא להגיב בצורה אד-הוק לכל התפתחות והתפתחות – הפתרון אינו יכול להיות תגובה משפטית נקודתית!

נקודה מרכזית – שינוי במעמד המשפט כמערכת המסדירה התנהגות בעזרת כללים שנאכפים ע"י רשויות אכיפה ובתי משפט:

סדרי גודל חסרי תקדים של מידע ושל פעילות. שינוי במעמד המשפט כמערכת שמסדירה התנהגות באמצעות כללים שנאכפים בבתי המשפט ע"י רשויות אכיפת החוק. שוק גלובאלי, פעילות החוצה גבולות, מכאן גם סמכויות שיפוט. משמע:

1. הפרטת האכיפה, אוטומציה, שקיפות, פיקוח, פיתוח נורמות וכללים, גיבוש וערכים.
2. סדרי גודל חסרי תקדים של מידע ושל פעילות.
3. שינוי בהתנהגות ובתפישות החברתיות.
4. תובנות כלליות בנוגע למהות המשפט, צדק, הגינות וערכים.

# מודל ההסדרה של לורנס לסיג – Code Is Law

אל מול שינויים אלו מצא עצמו לורנס לסיג.

אנחנו רואים שינוי במעמדו של המשפט כמערכת שמסדירה את ההתנהגות של האנשים במרחב הטכנולוגי, בעזרת כללים שנאכפים ע"י רשויות אכיפה ובתי משפט.

הסיבה לכך היא סדרי הגודל חסרי התקדים של מידע ושל פעילות שיש להסדיר. עקב המאפיינים של הפעילות הטכנולוגית הזו, ועקב המאפיינים של השוק החדש חסר הגבולות (=הגלובלי), אנו נמצאים בעולם בו ישנה יותר ויותר הפרטה של פעולות אכיפה ורגולציה, ושלצד ההפרטה הזו ישנה הישענות הולכת וגוברת על אמצעים טכנולוגיים, אשר חלק ניכר מהם הם אוטומטיים הפועלים ללא יד אדם בהפעלתם.

שני מאפיינים אלו (שוק גלובלי ואוטומציה של התהליכים) מציבים לנו אתגרים מובנים, אשר ניתקל בהם במקרי המבחן השונים.

* כיצד נייצר שקיפות, פיקוח, גיבוש ערכים ופיתוח נורמות וכללים בפעילות של גורם פרטי בכדי שנוכל לפקח שאיזון הערכים שקיים בהם הוא איזון שמקובל עלינו כחברה?
* כיצד כאשר נדבר על פעילות אוטומטית נוכל להבטיח ולפקח גם על הפרוצדורה וגם על התוצאות שלה, כאשר זירות הפעולה והאכיפה הופכות יותר ויותר להיות דיגיטליות?
* כיצד נתאים כחברה את המסגרת הנורמטיבית אל מול האתגרים הללו?

שינוי מאפיינים אלו מוביל גם לשינוי בתפיסות החברתיות של האנשים ובהתנהגות שלהם. לדוג' אם דיברנו על הגנת הפרטיות והמסגרת הנורמטיבית שאנו רגילים לדבר עליה בהקשר זה, אנו רואים תפיסות שונות בין אנשים בגילאים שונים. אנו נוטים לראות כי אנשים מבוגרים רואים בפעולות מסוימות ככאלו הפוגעות בצורה קשה בפרטיות שלהם וכי מדובר בתשלום מחיר גבוה מידי באשר לתמורה המתקבלת, בעוד הדור הצעיר רואה בכך את ההתנהלות הרגילה של העולם כיום.

מכל אלו ננסה להסיק תובנות כלליות בנוגע למהות המשפט, הצדק, ההגינות והערכים שלנו.

במערכת המשפט העמימות אינה באג אלא פיצ'ר.

מודל ההסדרה של לסיג:

המשפט

הנורמות החברתיות

השוק

הטכנולוגיה - CODE

* רגולציה עקיפה -
* רגולציה ישירה -
* הפעילות המוסדרת (ההתנהגות האנושית) –

לסיג מציג מודל הסדרת התנהגות חדש, אליו הכניס את הטכנולוגיה. מה מסדיר את הפעילות האנושית?

אנחנו כבר יודעים שלצד כללי המשפט הקובעים את המותר והאסור, באמצעות כללים משפטיים, יש עוד גורמים שקובעים מה אפשרי או לא אפשרי. כגון:

1. נורמות חברתיות – יכול להיות שלא יהיה חוק אבל נורמות חברתיות יגרמו לכך שלא יעשו את זה או שיהיה חוק אבל נורמה חברתית תגרום לכך שהוא לא ייאכף.
2. שוק – שיקולים של תחרות, של מחיר, אינטרסים של חברות – משפיע על ההתנהגות של אנשים בפועל.
3. לתוך כל אלו לסיג הציג גורם נוסף שהוא הטכנולוגיה. ממש כמו שאר הגורמים האחרים, ה-code שהוא הטכנולוגיה, מסדירה התנהגות כמו כל הגורמים האחרים וקובעת מה אפשרי ולא אפשרי.

לדוג' – אלגוריתם תכנון מחירים מציג לי מחיר שונה בהתאם להתנהלות שלי ברשת אז הוא מסדיר את ההתנהגות שלי.

לא רק שכל הגורמים האלה משפיעים על ההתנהגות האנושית, אלא גם יש קשרי גומלין ביניהם – הם משפיעים אחד על השני. המשפט יכול לקבוע כללים שאומרים איזה טכנולוגיה אסור או מותר לפתח.

## משמעות המודל:

שאנחנו נתקלים בפעילות אנושית יש סל כלים עשיר לעיצוב מדיניות ולהכוונת התנהגות. לדוג': נורמה חוקית האוסרת על הפצת תכנים פורנוגרפיים לילדים. מצד שני, כל ילד בן 10 יש טלפון חכם והוא יכול לגשת להרבה תכנים. יכול להיות מנגנון טכנולוגי שמסנן תכנים והוא יכול להיות יותר יעיל מאשר איסור חוקי.

כך ניתן להבין שתפיסה אינסטרומנטלית היא מיושנת – הטכנולוגיה היא לא רק פונקציונלית. אלא היא גם מקדמת ערכים.

לפי הגישה המהותית – ערכית: הטכנולוגיה מגלמת בתוכה ערכים בין אם באופן עקיף ובין אם באופן ישיר (מתוכננת מלכתחילה כדי לקדם ערכים מסוימים). לפעמים המשמעות שניתנת לטכנולוגיה היא הערכים שאנחנו חושבים שהיא מקדמת. היא לפעמים מחוץ לכוונות המפתחים שלה – לדוג': cookies נוצר כדי שהבראוזר יזכור את הסיסמאות שלו, כיום הטכנולוגיה משמשת למטרות שונות לחלוטין.

מהצד השני של המטבע: אם מדברים על המשפט כמעצב טכנולוגיה, אזי התערבות משפטית יכולה להשפיע על סוג הטכנולוגיות שמותרות בשימוש, על אופן יישומן, על עלות הפעלתן ועל היתכנותן של טכנולוגיות חלופיות.

## Code Is Law (לסיג):

המודל של לסיג מניח כי כל פעילות אנושים שהמתבקשת להסדרה, פועלות ארבע מערכות הסדרה שונות המשפיעות עליה ישירות (מידת ההשפעה יכולה להשתנות לפי ההקשר):

1. מערכת המשפט:

כולל כללים משפטיים המסדירים באופן ישיר את הפעילות ומשפיעים עליה (הנורמה – מה מותר ומה אסור). לדוג': המשפט יכול להגיד שאנו לא יכולים להגביל את חופש הביטוי הפוליטי בפוסטים בפייסבוק. בנוסף המשפט משפיע על הפעילות האנושית באופן עקיף מכיוון שהוא משפיע גם על השוק, הטכנולוגיה והנורמות החברתיות שגם הן כאמור משפיעות על הפעילות האנושית (למשל: שהמשפט קבע שמשכב זכר זו עבירה הייתה לכך השפעה גם על הנורמות החברתיות).

1. כוחות השוק:

שפועלים ומשפיעים על הפעילות האנושית, למשל יכולת כלכלית שקובעת אם דבר הינו אפשרי או לא בסיטואציה נתונה.

1. נורמות חברתיות:

נורמות חברתיות שמסדירות את מה שמקובל בהתנהלות האנושית, ומשפיעות על המשפט.

1. הטכנולוגיה:

הטכנולוגיה עצמה משפיעה על הפעילות האנושית, לדוג': זה שבפייסבוק ניתן לעשות או לייק, או שייר, או לכתוב תגובה, ולא יותר מכך זו קביעה של הטכנולוגיה עצמה לאפשריות הנתונות לפעילות האנושית.

בכל פעולה או כל תחום שנתייחס אליו בקורס, נראה כיצד קיימים קשרי גומלין של כל אחד מהגורמים הללו. אנו נראה כי לעיתים הקשרים וההשפעות יהיו בלתי-ישירים.

השאלה שתלווה אותנו לאורך כל הקורס היא האם ראוי שהפתרון לבעיה שנגרמת מפעילות האנושית צריך שיבוא בהכרח מהמשפט?

הרעיון הוא שלמשפטנים כמעצבי המדיניות ולמפתחי תוכנה יש סל כלים עשיר ביד כשאנו מעצבים מדיניות טכנולוגית,והפתרון המשפטי לסוגיות הטכנולוגיות הללו הוא לא בהכרח הפתרון המיטבי, ולפעמים כוחות השוק או הטכנולוגיה או הנורמות החברתיות ישחקו תפקיד משמעותי יותר.

## הגישה האינסטרומנטלית לטכנולוגיה:

אנו יכולים לחשוב שברגע שאנו מגייסים איזו שהיא טכנולוגיה, אנו נראה בה כלי אינסטרומנטלי בלבד. משמע מטרתה היא רק ליישם איזה שהן הנחיות וכו'. לסיג טען כי לא נכון לראות בטכנולוגיה רק ככלי אינסטרומנטלי, קרי מעין ציבור מקשר המהווה הפלטפורמה לביצוע ההתנהגות, אלא בטכנולוגיה עצמה יש השפעות על אופי ההתנהגות האנושית. גישה זו היום היא כבר נחשבת מיושנת מאוד, כי אנו כבר לא תופסים בטכנולוגיה רק ככלי בידי המשתמש, אלא הטכנולוגיה עצמה נושאת בתוכה ומגלמת ערכים. הטכנולוגיה מתפתחת במענה לצרכים של החברה ומעוצבת בהתאם להם. על-כן אנו רואים שינוי תפיסתי מהגישה האינסטרומנטלית אל עבר הגישה "המהותית - ערכית".

## הגישה המהותית-ערכית לטכנולוגיה:

הטכנולוגיה מגלמת בתוכה ערכים, ובאופן עקיף הטכנולוגיה מתפתחת במענה לצרכים של החברה, ומעוצבת בהתאם להם. סוציולוגים ופילוסופים של טכנולוגיה מצביעים על כך שהטכנולוגיה אינה ניטרלית, קרי אינה מכשיר וכלי יישומי בלבד, אלא מגלמת בתוכה בחירות ערכיות נורמטיביות של המתכננים שלה, באופן עקיף וישיר. באופן עקיף, הטכנולוגיה מתפתחת בהתאם לצרכי החברה, ומתוך הסוגיות והתכנים שמעסיקים את החברה. באופן ישיר היא מכוונת לגלם ערכים מסוימים (למשל, תוכנות סינון שמאפשרות בקרה הורית על תכנים פוגעניים באינטרנט, או פלאפונים כשרים לצורך בקרה הלכתית).

## הצד השני של המטבע – המשפט כמעצב טכנולוגיה:

התערבות משפטית יכולה להשפיע על סוג הטכנולוגיות שמותרות בשימוש, על אופן יישומן, על עלות הפעלתן ועל היתכנותן של טכנולוגיות חלופיות.

גם המשפט מרים ראשו ומנסה להשפיע על עיצוב הטכנולוגיה. אנו נראה הכיצד התערבות משפטית (חקיקת חוק, תקנות, פסיקת ביהמ"ש וכו') משפיעה על סוג הטכנולוגיות המותרות בשימוש, על אופן יישומן, על עלות הפעלתן (לאור מגבלות חוקיות כלאה ואחרות שיכולות להיות מושתות) ועל היתכנותן של טכנולוגיות חלופיות.

למשל:

* מגבלות בחוק על פיתוח ייצור וייצוא טכנולוגיות. לדוג' בישראל יש הגבלות מסוימות על שיטות שונות של הצפנה.
* תמריצים לפיתוח טכנולוגיות מסוג מסוים. לדוג' תקנות הגנת הפרטיות (אבטחת מידע), הנדסת פרטיות;
* הטלת אחריות משפטית בגין שימוש בטכנולוגיה אחת עשויה לעודד פיתוח של טכנולוגיה אחרת (תוכנות שיתוף קבצים למשל). לדוג' חברת נפסטר שהייתה החלוצה של יצירת פלטפורמה לשיתוף קבצים – בעלי זכויות היוצרים של אותם קבצים תבעו את חברת נפסטר בטענה של הפרת זכויות יוצרים, זאת מכיוון שחברת נפסטר יודעת שמשתמשיה הפרו זכויות יוצרים והיא מאפשרת להם זאת. כאן עולה השאלה האם ניתן להטיל אחריות על בעלי הפלטפורמה הטכנולוגית שלא מפרה את זכויות היוצרים בעצמה אך מהווה רק פלטפורמה המאפשרת זאת. לאחר תביעת חברת נפסטר עלתה לאוויר חברה חדשה בשם "איימסטר". איימסטר אפשרה למשתמשיה לשתף קבצים מוצפנים, אך גם כאן קבעו בתי המשפט שניתן להטיל אחריות אל מי שמפעיל את פלטפורמת השיתוף כמפר זכויות יוצרים. במהלך תביעות אלה הייתה הן התפתחות טכנולוגית והן התפתחות משפטית כדי לפתור עניין זה. כך שנוצרה תוכנה חדשה שאפשרה לשתף קבצים באופן פרטני בין משתמשים, שיתוף קבצים מבוזר. תוכנה זו לא מנעה את הפרת זכויות היוצרים, אך אפשרה לתבוע את מפיץ התוכן שמפר את זכויות היוצרים באופן ישיר ולא את האתר.

דוגמה לעניין – תעמולת בחירות באינטרנט:

חוק הבחירות (דרכי תעמולה) מסדיר את שידורי תעמולה באמצעות אמצעי התקשורת (רדיו, טלוויזיה, עיתונות). החוק מבוסס על הקצאת זמני שידור (כל מפלגה מקבלת זמן שידורי תעמולה לפי החוק) ועולה השאלה כיצד זה יותאם באינטרנט. האם החוק חל על תעמולה באינטרנט? עד היום לא. למה?

מצד אחד לאינטרנט אין הגבלה של ערוצי שידור. באינטרנט אין מחסור בערוצי שידור ובזמן שידור.

מצד שני באינטרנט קיימים חסמים אחרים: כמו עיצוב תוצאות חיפוש / עיצוב ה"פיד" או עמוד החדשות, העדפה לתכנים ממקור מסוים, שימוש בתוכנות סינון, גישה למידע אישי על הבוחרים (הצלבה ועיבוד לצורך השגת יתרון בתעמולת הבחירות), פייק ניוז, בוטים, הודעות שאין מזוהות כתעמולה, טוקבקים בתשלום.

שאלת התעמולה באינטרנט עולה לפני ועדת הבחירות.

פס"ד ש"ס נ' פינס: עתירה כנגד צ'אט של גולשי אתר של עיתון בטענה שזה תעמולת בחירות באינטרנט. השופט חשין קבע שזוהי לא תעמולת בחירות.

פס"ד בן מאיר נ' מפלגת הליכוד: האם פרסום באינטרנט וברשת חברתית חייב לכלול את שם המפלגה שמטעמה פורסם? האם יש לאסור על רשימות לשלם לגורמים שונים תמורת פרסומים שמתחזים לאישיים? השופט מלצר החליט שהוראות החוק יחולו גם על פרסומים באינטרנט.

בפועל המשמעות היא שבכל פרסום שיעשה על ידי מפלגות ורשימות לכנסת, או ביוזמתם יש לפרט:

1. זהותו, שמו ומענו של מזמין המודעה (הרשימה המתמודדת לבחירות הרלבנטית).
2. פרטים מקבילים לגבי האחראי להזמנת המודעה.
3. למסור את דרכי ההתקשרות עמם (מען, כתובת אלקטרונית, טלפון).

מכאן כי יש לציין מי מזמין ההודעה ופרטי ההתקשרות איתם. אם זה לא קורה, ניתן לדווח לרשת החברתית והיא צריכה להוריד את הפוסט. אם לא תעשה את זה, תהא גם היא אחראית בדבר.

מה ניתן ללמוד מהחלטת יו"ר ועדת הבחירות (נשענת על פרשנות תכליתית)?

יש פה פרשנות תכליתית של מטרת דיני התעמולה.

1. התאמת תכליות חוק דרכי תעמולה לביטוי הפוליטי בעת הנוכחית.
2. מטרת החוק למנוע הולכת שולל של קהל הבוחרים, ולהגביר שקיפות וגילוי למען הסדר הטוב של הליך הבחירות.
3. זאת אף במחיר של הגבלה מסוימת של חופש הביטוי הפוליטי האנונימי ברשת.

# חזון האינטרנט ככיכר העיר החדשה

חזון שהתחיל בראשית ימי האינטרנט והשתרש עם התפתחות הטכנולוגיה למצב כיום. בזכות הביזוריות והנגישות הגדולה של האינטרנט, נוצר סדר יום חדש של שוק חופשי – של דעות בפרט וחופשי בכלל – של רבים וטובים להציע את הסחורה שלהם בצורה ציבורית. כל אדם יכול להציע את שירותיו לאחרים. חזון זה ביקש לקחת את האפשרות הזו ולהרחיב אותה בסדרי גודל גלובליים, לכולם.

חזון זה נשען על מאפיין האינטרנט כרשת מבוזרת – רשת של רשתות מבוזרות. היעדר סמכות ריכוזית יחידה שאמונה על ניהול האינטרנט, ניהול מבוזר ושיתופי במודל של "בעלי עניין מרובים". אין מנהל יחיד שמחליט על האינטרנט. ביזור הרשת הוא למעשה אנטי-תזה לריכוז השליטה בידי אמצעי תקשורת מועטים. אפיון זה של האינטרנט מקושר קידום ערכים חברתיים: חופש מידע, חופש ביטוי, חירות אישית, חדשנות.

מבנה זה אף קשור למושג "ניטרליות רשת" כאשר לא נשאיר גורם ריכוזי נוכל לקדם את חזון כיכר העיר וכל אחד יוכל לומר מה שירצה ברשת האינטרנט.

# אופייה המבוזר של רשת האינטרנט

ביזור האינטרנט:

האינטרנט = רשת של רשתות מבוזרות.

כיום מתקיים היעדר סמכות מרכזית יחידה שאמונה על ניהול על האינטרנט.

ניהול מבוזר ושיתופי במודל של "בעלי עניין מרובים".

ביזור הרשת:

ביזור הרשת = אנטי-תזה לריכוז השליטה בידי אמצעי תקשורת מעטים.

ביזור זה מאפשר קידום של ערכים חברתיים – חופש מידע, חופש ביטוי, חירות אישית, חדשנות.

מבנה זה קשור גם למושג "ניטרליות רשת".

הרעיון של ניטרליות רשת נשאר רלוונטי עד ימינו.

ICANN – הגוף האחראי על משילות רשת האינטרנט.

חסמי כניסה נמוכים לאינטרנט:

הרעיון היה שאם נסיר את החסמים הללו יהיה יותר גיוון, יהיה יותר אנשים שיציגו את דעותיהם. ככל שיהיו יותר משתתפים בשיח, כך יהיה יותר מגוון.

המדיום למעשה מאפשר תקשורת ישירה בין המשתמשים => הגדלת מגוון התכנים.

ביטול התלות במסננת העריכה של אמצעי התקשורת המסורתיים.

גולשים ברשת בעלי אוטונומיה להגדיר את סדר היום בעצמם => מודלים חדשים לייצור והפצה של תוכן.

התוצאה:

1. התפתחות מאגר עשיר ודינמי של תוכן חופשי ממקורות מגוונים.
2. החלשת כוחם של מוקדי השליטה בשוק התקשורת והתוכן.
3. מכאן גם נולדו שאלות משפטיות חדשות.

החזון הוא שהאינטרנט יהיה כיכר העיר החדשה.

# גורמי ביניים (מתווכים) ברשת האינטרנט

הגדרה – גופים (ברובם למטרות רווח) אשר מאפשרים לבצע התקשרויות או עסקאות בין צדדים שלישיים באינטרנט, על דרך של מתן גישה לרשת, אחסון, שידור או אינדוקס של תוכן, או אספקת שירותים ומוצרים מקוונים שמקורם בצדדים שלישיים נוספים.

לדוג': מנועי חיפוש, חיבור לאינטרנט (ספק גישה לרשת), פורטלים, מדיה חברתית, שירותי אחסון ועיבוד מידע, מרשמים של שמות מתחם וכו'.

למעשה, גורמי ביניים הם כל הפלטפורמות המאפשרות תקשורת בין כל אותם צדדים שלישיים מבלי לקחת צד בעניין.

גורמי הביניים בהם נתמקד:

1. ספקי גישה לאינטרנט (ISP) – ספקי הגישה מקצים לכל משתמש שם וכתובת המאפשרים לו להיות מחובר לרשת.
2. ספקי תוכן ושירותים – מציגים תוכן באתר לשם הפצתו בין משתמשים, פלטפורמות מסחר ושירותים ורשתות חברתיות.

לגורמים הביניים כוח משמעותי להבנות, להגביל ולשלוט על הפעילות ברשת, ולעצב ולהתוות את דעת הקהל ברשת. חלק מגורמי הביניים, בתור גופים פרטיים הינם תאגידים עם אינטרסים כלכליים / פוליטיים ואחרים. מכאן עולה השאלה האם עלינו להסתכל על אותם גופים פרטיים כעל גופים דו מהותיים בעלי חובות מתוקף פעילותם?

שאלה זו עולה מאחר וגורמי הביניים מאתגרים משמעותית את התפיסה של האינטרנט כמקדם אבסולוטי של חופש מידע, חופש ביטוי, חופש יצירה וחופש עיסוק.

נקודות מפתח:

* לגורמי הביניים כוח משמעותי להבנות, להגביל ולשלוט על הפעילות ברשת.
* גורמי הביניים הם תאגידים פרטיים, תאגידים עם אינטרסים כלכליים, פוליטיים ואחרים.

מכאן, האם מדובר בגופים דו מהותיים?

גוף דו מהותי = גוף דו מהותי הוא יצור כלאיים בין הציבורי והפרטי ולכן למרות שבמהותו אינו גוף ממשלתי חלים עליו גם חובות מכוח המשפט המנהלי. לדוג': חברות ביטוח, בנקים וכו'.

גורמי הביניים מאתגרים משמעותית את התפיסה של האינטרנט כמקדם אבסולוטי של חופש מידע, חופש ביטוי, חופש יצירה, חופש עיסוק... בפועל גורמי הביניים נכנסים בנעליים של רשויות ציבוריות, כגון חקיקה, אכיפה, שפיטה ועוד.

## עקרון "ניטרליות רשת":

לפיו ספקיות גישה לרשת מחויבות להתייחס לכל סוגי תעבורת האינטרנט באופן שוויוני, ללא אפליה.

המטרה של עקרון זה היא יצירת מגרש משחקים שוויוני בין כל מי שרוצה להיכנס למשחק ולהשתמש ברשת.

מונח זה נקבע ע"י טים וו, והוא כולל כמה עקרונות משנה:

1. אסור לחסום – ספק רשת לא יכול לחסום את הגישה לאתר / תוכן מסוים ללא צו שיפוטי, למניעת מצבים בהם רשתות מסוימות חוסמות / משלמות כדי שיחסמו גישה לגופים אחרים.
2. אסור להאט – אסור להאט את הגישה לתוכן / גישה מסוימים, כדי למנוע מעבר של הגולשים בשל חווית שירות לא טובה.
3. אסור לתעדף – אין לתת עדיפות לתוכן / אתר מסוימים. הדבר מהווה התערבות בשוק, שכן לא ניתן לשלם עבור מתן עדיפות למקורות מסוימים.
4. איסור תמחור 0 – איסור על תמחור 0, מתן גלישה חינמית לתכנים מסוימים. אחרי הכול מה זה גורם לעשות? גורם לנו להעדיף את התוכן החינמי על פני הזה שאיננו.

המשמעות היא: איסור על אפליה בתעבורת הרשת על בסיס תכנים, כתובת מקור / יעד, ציוד קצה, אמצעי תקשורת, זהות משתמשים, פלטפורמה / אפליקציה.

## בעד ונגד ניטרליות רשת:

בעד:

1. קידום חופש הביטוי
2. קידום חופש העיסוק
3. עידוד חדשנות ויזמות עקב קיומם של שחקנים רבים המעוניינים להיכנס לשוק ולספק תחרות
4. עלויות נמוכות

נגד:

1. זכות הקניין – האם ניתן להתערב לאנשים באופן בו הם מממשים את זכותם לקניין.
2. חדשנות ויזמות – ללא מגבלות נוכל לאפשר צמיחה של חדשנות ויזמות.
3. שדרוג תשתיות – התערבות ברשתות יכולה להביא לשדרוג התשתיות בצורה המאזנת את הצריכה ביניהן וגובה בהתאם.
4. עלויות נמוכות – ברגע שמוטלות מגבלות רגולטוריות נוצרת פגיעה ביעילות הכלכלית.

## ניטרליות רשת בישראל:

עד שנת 2009 לא היה הסדר ניטרליות רשת בישראל. זה עד שהסקייפ הגיע לישראל אשר אפשר שיחות אינטרנט ללא הגבלה וללא תשלום פר דקות בשיחה (בניגוד לשאר חברות הפלאפון אשר דרשו תשלום חודשי ותשלום עבור כל דקת שיחה). כתוצאה מכך, סלקום חסמה ללקוחותיה את האפשרות להשתמש בסקייפ.

מכאן ב-2011 נחקק: תיקון לסעיף 51(ג) בחוק התקשורת (בזק ושידורים) התשמ"ב-1982 – אשר כלל כללי ניטרליות רשת במסגרת חברות סלולר בשנת 2011.

בשנת 2014, לאחר ההכרה בצורך, הורחב תחולת החוק גם על ספקי גישה לאינטרנט.

סעיף 51(ג) – סייפא ב':

ספק מורשה, מי שעוסק בסחר בציוד קצה שהוא ציוד רדיו טלפון נייד (בסעיף זה – ציוד קצה רט"ן) ומי שעוסק בסחר בציוד תקשורת, לא יגרום להגבלה או לחסימה של המפורטים להלן, בעצמו או באמצעות אחר, לרבות בדרך של קביעת תעריפים;

\*המשפט המסומן בקו - הנ"ל מהווה כסעיף איסור תמחור 0.

## ניטרליות רשת בארה"ב:

דרמה פוליטית-כלכלית אשר תלויה בנשיא המכהן.

1. ב-2005 ה-FCC קובעת עקרונות ניטרליות רשת.
2. בשנים 2007-2014 בתי המשפט מתבקשים להכריע במאבקים בין ספקיות הרשת ל FCC, וקובעים כי ל FCC אין סמכות לאכוף כללי ניטרליות רשת.
3. בשנים 2015-2016 ה FCC קובעת כללי ניטרליות חדשים אשר זוכים לאישור ביהמ"ש (שלושת האיסורים: חסימה, האטה, מתן עדיפות).
4. ב-2017 (ממשל טראמפ) ה FCC מבטלת את כללי ניטרליות הרשת, ספקיות ראשיות לחסום, להאט ולהעדיף תכנים מסוימים.
5. ב-2019 ביהמ"ש מאשר את חוקיות הביטול של כללי הניטרליות ברשת, אך מאפשר לכל מדינה לקבוע את כללי ניטרליות הרשת שלה.
6. ב-2021 הנשיא ביידן ממנה יו"ר FCC חדשה בעלת דעות פרו-ניטרליות רשת, ומנחה את ה FCC בצו נשיאותי לפעול להשבת כללי ניטרליות רשת.

האם חזון הביזור, החופש וניטרליות הרשת מוגשם בפועל?

כיום ישנה שליטה של תאגידים פרטיים על סביבת התוכן המהווה סוג חדש של ריכוזיות, איומים חדשים על האוטונומיה של הפרט וחופש הביטוי. בנוסף, ארכיטקטורת הרשת וקוד התוכנה אינם ניטרליים, התשתית הטכנולוגית מבנה את הפעילות האנושית המתקיימת על גביה (לדוג' שיח, מסחר, מערכות יחסים, שירותים, קהילות וכו').

חמשת הגדולות (החברות):

1. מיקרוסופט
2. מטא
3. אפל
4. גוגל
5. אמזון

## מודלים חדשים, איומים חדשים, שלטון הפלטפורמות:

השיח של הכנסת משווה את המדיניות של רשתות חברתיות שונות. יש כל מיני פרקטיקות להפעיל את הכוח הזה ורואים בהרבה מובנים את קור היד של מחוקקים מדינתיים עם הכוח העולה. האדם החזק ביותר בעולם הוא נשיא ארה"ב. עם זאת, הכוח לא עזר – כשטוויטר חשבו שלא מגיע לו חופש הביטוי הם חסמו את הפוסטים ואת המשתמש שלו. יש כאן החלטה של שיקול דעת: יכול להיות שזה נכון אבל מי שקיבלה את ההחלטה היא חברה מסחרית.

הכוח של אותן חברות בזירה הבינ"ל: כשהאקרים תקפו את אוקראינה יום קודם לתקיפה, צוות מייקרוסופט תקף חזרה נגד התקיפה הזאת. עכשיו כשיש פייק ניוז רוסי בתודעה בניגוד לתגובה האיטית יחסית בקורונה, הרשתות נכנסו לפעולה כדי לנטר את הפעילות הזאת והסרה של משתמשים לא אותנטיים.

שאלות משפטיות שמעוררים גורמי הביניים:

* האם גורמי ביניים אחראיים לפעילות של המשתמשים שלהם? האם לצד אחריות של המזיק הישיר (המשתמש) יש להטיל אחריות גם על גורם הביניים? זה מכוח דיני הנזיקין (לשון הרע, פגיעה בפרטיות), דיני הקניין (זכויות יוצרים), דיני עשיית עושר (רווח מפרסומות על בסיס תוכן לא חוקי), הדין הפלילי (הטרדה מינית, פרסום תועבה, פגיעה בפרטיות, לשון הרע וכו').
* האם יש לגבש משטר אחריות אחיד לכל סוגי גורמי הביניים? כלפי ספק הגישה לאינטרנט, בעל פורום, רשת חברתית, פלטפורמת מסחר / שירותים – דוגמת תוכן שמפר קניין רוחני, לשון הרע, תוכן פוגעני / לא חוקי. שאלת מתן סמכות ואחריות לאותם גורמים נועדה להבטיח אמון משתמשים בפלטפורמה שלהם. האם כל גורמי הביניים נולדו שווים?
* האם ראוי להפקיד בידי גורמי ביניים סמכויות משפטיות לפיקוח, רגולציה, יישוב סכסוכים ואכיפה? מבחינה מסורתית, מדובר בסמכויות שמצויות בידיהן של רשויות ציבוריות, לא אצל חברות פרטיות. כיום גורמי ביניים מפעילים סמכויות אלה באופן נרחב במרחב המקוון. מדוע? מכיוון שעליהן לקיים את הוראות הדין. בנוסף הן מעוניינות להימנע מחשיפה משפטית (בעקבות הטלת אחריות לפעולות משתמשיהם). שלישית כך מבטיחים את אמון המשתמשים בפלטפורמה.

היעדר האסדרה כיום:

הפעלת תפקידי האסדרה נעשית פעמים רבות בוואקום חקיקתי (היעדר אסדרה של פעילות האסדרה). למשל, ניטור תכנים והסרת תכנים ע"י רשתות חברתיות. נקודת המוצא בישראל היא היעדר אסרה חקיקתית על הסרה של תכנים אסורים / בעייתיים מרשתות חברתיות (למעט באמצעות הליך משפטי אזרחי – כדוג' לשון הרע, זכויות יוצרים). בנוסף, תנאי השימוש וכללי הקהילה של רשתות חברתיות שמכוחם מבוצעת האסדרה.

אפשרויות אסדרה:

1. מנגנון הודעה והסרה (+ ביקורת שיפוטית)
2. הסרה או הגבלת גישה לבקשת גורם אכיפה ממשלתי (+ ביקורת שיפוטית)
3. הסרה מכוח צו שיפוטי
4. הסרה לבקשת הנפגע (די חופף לאפשרות מס'1)
5. אסדרה בחוק של פעילות ניטור התוכן והסרת התכנים (+ אכיפה וביקורת שיפוטית)

האתגרים:

1. הפרטה – בסוף מדובר בחברה פרטית בעלת אינטרסים מסחריים להשיא את רווחי הקהילה, והיא הקובעת את כללי הקהילה, האם התוכן פוגעני או לא ומהם התנאים להסרת תוכן.
2. אוטומציה – הניטור והאכיפה משלבים כלים אלגוריתמיים, מה שמשלב עולם של קבלת החלטות אלגוריתמיות והבעיות העולות מכך.

## כיצד מערכת האסדרה העצמית של גורמי הביניים משפיעה על עיצוב נורמות והתנהגות?

1. תנאי השימוש והפרטיות – חוזים אחידים שמסדירים את מערכת היחסים בין הפלטפורמה למשתמשים שלה. כאשר הפלטפורמה קובעת מהם תנאי השימוש שלה, לציבור מוגדר מהו חופש הביטוי בשימוש בפלטפורמה המדוברת – נורמות שמתקבעות עם הזמן והתודעה מעוצבת לאורו.
2. כללי קהילה – מסדירים התנהלות בתוך הפלטפורמה, לדוג' קביעת גבולות השיח, משמעותם של מושגים.
3. מבנה הפלטפורמה עצמה ועיצוב ממשק המשתמש – הינדים דיגיטליים. לדוג' ישנם שני כפתורים: אחד גדול אדום ואחד קטן לבן, רוב הסיכויים שנבחר בכפתור האדום והבולט. משמע בדרך זו ניתן להשפיע גם כן.

דוג' לכך היא קביעת מגדר חשבון המשתמש. האפשרויות המוצגות מהוות הצהרה חברתית-נורמטיבית. בנוסף, תיתכן השפעה פנימית וחיצונית על יישומים המבוססים על פרסונליזציה – המידע שהפלטפורמות אוספות על המשתמשים ע"פ פעילותיהן מגדירה את המשך השימוש בפלטפורמה.

דוג' נוספת היא עיצוב גבולות חופש הביטוי הפוליטי. אקטיביסטית בארה"ב רצתה לעודד נשים להצביע בבחירות ועשתה זאת ע"י פוסטר המציג עירום נשי המבוסס על הקלטה של טראמפ. מה גובר על מה – האיסור על שימוש בעירום בבחירות או חופש הביטוי הפוליטי? התקבלו תלונות של משתמשים ובקשות להסרת התוכן, מה שהביא להסרת התוכן וחסימת אותה משתמשת. פעולה זו קבעה את גבולות השיח ומנעה את האפשרות של משתמשים מסוימים להשתתף בשיח.

## הקשיים מתגברים כאשר ניטור התוכן מבוצע באמצעות כלים אלגוריתמיים אוטומטיים:

כאשר יש תכנים הנחשדים כאסורים ונחסמים אוטומטית, ללא הצדקה. כאשר אלגוריתם מבצע את הסריקה, ישנן טעויות טכניות בשל דמיון כזה או אחר. הפעלת הכוח של הפלטפורמה מגיע גם לביהמ"ש, כאשר יש תלונות של משתמשים על האופן בו הפלטפורמה התייחסה אליהם. לדוג': כאשר אמיר חצרוני תבע את פייסבוק על שחסמו את החשבון שלו, השופט רחמים כהן במחוזי קבע כי תנאי השימוש של פייסבוק מהווים הסכם מחייב – ועל כן הסרת המשתמש של אמיר חצרוני הייתה מוצדקת, במיוחד לאור העובדה כי פייסבוק נתנה לו מספר הזדמנויות ואזהרות בנוגע לשימוש.

פס"ד פרופ' חצרוני נ' פייסבוק אירלנד: "התובע מעלה את השאלה – האם פייסבוק רשאית לקבוע כללי חופש ביטוי משלה והגבלות שימוש בפלטפורמה שהיא מספקת אשר פוגעות (לשיטתו) בחופש הביטוי. ייתכן שיש מקום לבחון שאלה זו על רקע מעמדה של פייסבוק והיותה פלטפורמת רשת בעלת היקף של למעלה משני מיליארד משתמשים באופן שיש בו פוטנציאל לנווט את השיח החברתי והפוליטי... פסק דין זה אינו האכסניה המתאימה לכך... עניינה של תובענה זו בסוגיה חוזית.. התובע עצמו הפר את החוזה עם פייסבוק... התובע לא השכיל להוכיח, שהליך האכיפה של פייסבוק בעניינו לא היה נאות או שנפל בו פגם שאינו עולה בקנה אחד עם הוראות החוזה שבין הצדדים."

גם החלטה שלא להסיר תוכן עשויה להיות בעייתית:

לינוי בר גפן ניצחה את טוויטר שלא הסירה ציוץ בוטה במיוחד. בר גפן תבעה את טוויטר לאחר שפנתה פעמיים לחברה, ולא קיבלה מענה. השופט מתח ביקורת על טוויטר וחייבת אותה בהוצאות כבדות.

אציין כי לא רק רשתות חברתיות הן משפיעות ומשנות, אלא גם תוצאות חיפוש לדוג' – אם סיני מחפש את כיכר "דיי מן" בגוגל תמונות – אזי יוצגו בפניו תוצאות חיפוש בהן נראה הכיכר ביופיו ושליו. אך אילו אם אדם ממדינה מערבית יחפש את אותו חיפוש בדיוק – אזי יוצגו בפניו תוצאות חיפוש בהן ניתן לראות גם טנקים בכיכר, ולא רק את יופיו. כך תוצאות החיפוש משפיעות.

מה המשמעות המשפטית של פעולות משתמשים על גבי פלטפורמות? האם ההגדרות המשפטיות הקיימות רלוונטיות?

לדוג' האם משתמש מבצע לייק או שיתוף לפוסט על גבי פלטפורמת תוכן הדבר מטיל עליו אחריות לתוכן האמור (שכן אותו פרסם משתמש אחר)?

פס"ד שאול ואח' נ' ניידלי תקשורת בעמ: נקבע כי לייק ותגובה לפוסט פוגעני לא מהווים עילה לנסיבה באחריות, זאת לעומת שיתוף פוסט בעל תוכן פוגעני – אשר אכן מהווה עילה לנשיאה באחריות, מאחר וישנו בסיס לפרסום התוכן הפוגעני. שיתוף לעומת לייק או תגובה, למעשה יוצר העתק של הפוסט וכך נעשה פרסום שלילי אקטיבי האסור בדיני לשון הרע.

האם גורמי ביניים צריכים להיות כפופים לרגולציה דומה לזו של שירותים בעולם הפיזי?

* לדוג' האם Airbnb צריך לקבל היתרים עמו של בתי מלון? או כמו של אכסניה?
* דוג' נוספת האם Uber צריכה להיות כפופה לרגולציה כאמצעי תחבורה ציבורית?

הסוגיה הנפוצה ביותר היא שאלת הטלת האחריות על גורמי ביניים בגין פעולות שביצעו המשתמשים שלהם – זכויות יוצרים, לשון הרע, פורנוגרפיה, דברי שטנה והסתה ועוד.

# מודלים אפשריים להסדרת אחריות גורמי הביניים

1. מודל אחריות מוחלטת:

גורמי הביניים אחראים לתכנים שפרסמו המשתמשים בהם, ולכן מחויבים לפקח על פעילות המשתמשים כדי לוודא שאין בה הפרת חוק. הדבר יביא לפיקוח הדוק יותר, יהיה צנזורים בכמות גדולה יותר.

1. מודל המפרץ הבטוח:

לגורמי הביניים ניתנת חסינות מאחריות לתכנים שלא הם יצרו (שהמשתמשים פרסמו באמצעותם), בתנאי שהם עומדים בתנאים שנקבעו לכך בחוק.

1. מודל החסינות המוחלטת:

גורמי הביניים הם בבחינת צינורות שאינם נושאים באחריות לתוכן שמופץ דרכם.

1. מודל רישיון בתחום הקניין הרוחני:

מתחלק לשניים:

1. כשבעל הזכויות ידוע, גורם הביניים נדרש לקבל רישיון להצגת התוכן ולפצותו כנדרש במידה והיה שימוש לא כדין, משמע ללא רישיון.
2. כשבעל הזכויות אינו ידוע, גורמי הביניים נדרשים לעשות מאמץ מיטבי לאתרם.

## הכללים המשפטיים משפיעים על התנהלות גורמי הביניים (מתוך מחקר של UNESCO שנת 2014):

המודל שמדינה בוחרת ליישם הוא משמעותי! המחקר מראה כי בפועל ככל שכללי האחריות במערכת המשפט המדינתית ביחס לגורמי הביניים חמורים יותר, כך גובר הסיכוי כי גורמי הביניים יסירו תכנים באופן יזום / על רקע בקשה להסרה. הדבר אף משפיע על העובדה שבפועל מתפתחת טכנולוגיה המבצעת אכיפה ופיקוח על גורמי הביניים.

DSA – Digital Services Act (EU) – ניטור תוכן משתמשים:

* הסדרת פטור מאחריות של פלטפורמות לתוכן משתמשים
* הקמת מנגנוני הודעה ופעולה לדיווח על תוכן בלתי חוקי / בניגוד להסכם השימוש
* קביעת תנאי מינימום מנגנונים, אפשרות לדיווח אנונימי

לעניין "הליך הוגן":

* הקצאת משאבים מספקים לטיפול בדיווחי משתמשים.
* פירוט ברור של הטעמים למניעת שירות / הסרת תוכן.
* יידוע המשתמשים על הטעם להסרת תוכן ומנגנוני השגה פנימיים + ביהמ"ש.
* בהתאם לגודלה של הפלטפורמה, חובת דו"ח שקיפות שנתי בעניין הסרת התוכן.

# זכויות יוצרים ברשת האינטרנט – אסדרה באמצעות גורמי ביניים ושימוש באכיפה טכנולוגית

## זכויות יוצרים – רקע בסיסי:

דיני הקניין הרוחני כוללים מנגנונים משפטיים המאפשרים להפוך ידע מופשט לנכס שניתן לרכוש בו בעלות ולסחור בו. ישנן זכויות רבות בתחום הקניין הרוחני ומנגנונים שונים. במקרה זה, נתמקד בזכויות יוצרים.

זכות היוצרים מקנה ליוצר בעלות ביצירה, המפקיעה אותה מנחלת הכלל לפרק זמן מוגבל ע"פ חוק. שימוש ביצירה מצריך הרשאה מבעליה.

בבעלות הניתנת לבעל הזכות גלום מתח מובנה:

מצד אחד רוצים לעודד חדשנות ויצירה, ועל כן יש רצון לתת תמריץ ע"י מתן בעלות. מצד שני, יש רצון כי בחברה יהיה קיים חופש מידע, שניתן יהיה להשתמש ביצירות באופן במרחיב אותם כדי לאפשר חופש ביטוי וחופש יצירה עתידית.

בדין הישראלי:

הגישה התוצאתנית של הדין הישראלי היא שהגנה על זכויות יוצרים מוצדקת ככל שהיא מקדמת תוצאה רצויה. תוצאה רצויה היא קידום הרווחה החברתית הכוללת באמצעות תמריצים (גישה כלכלית). מתן תגמול ליוצרים יעודד השקעה ביצירה וחדשנות, זאת תוך איזון מול הפגיעה בחופש המידע ובחופש הביטוי.

חוק זכויות יוצרים – התסש"ח (2007):

הכלי המשפטי המעגן זכות זו הוא חוק זכויות יוצרים התשס"ח-2007.

## סעיף 47 לחוק – מהי הפרת זכויות יוצרים:

הפרת זכויות יוצרים – ביצוע אחת מהפעולות שיוחדו לבעל הזכות היוצרים לפי ס'11 לחוק, ללא קבלת רשותו של בעל זכות היוצרים.

## סעיף 11 לחוק – מהי זכות יוצרים:

זכות יוצרים מהי – זכות יוצרים ביצירה היא הזכות הבלעדית לעשות ביצירה, או בחלק מהותי ממנה, פעולה, אחת או יותר, כמפורט להלן, בהתאם לסוג היצירה:

1. העתקה כאמור בסעיף 12 – לגבי כל סוגי היצירות;
2. פרסום – לגבי יצירה שלא פורסמה;
3. ביצוע פומבי כאמור בסעיף 13 – לגבי יצירה ספרותית, יצירה דרמטית, יצירה מוסיקלית ותקליט;
4. שידור כאמור בסעיף 14 – לגבי כל סוגי היצירות;
5. העמדת היצירה לרשות הציבור כאמור בסעיף 15 – לגבי כל סוגי היצירות;
6. עשיית יצירה נגזרת כאמור בסעיף 16, ועשיית הפעולות המנויות בפסקאות (1) עד (5) ביצירה הנגזרת כאמור – לגבי יצירה ספרותית, יצירה אמנותית שאינה גופן, יצירה דרמטית ויצירה מוסיקלית;
7. השכרה כאמור בסעיף 17 – לגבי תקליט, יצירה קולנועית ותוכנת מחשב.

הגנה זו אינה מוחלטת – ישנם חריגים באמצעותם ניתן לעשות שימוש הוגן ביצירה של בעל זכות אחר, לדוג' למטרות חינוך, מחקר, דיווח עיתונאי. ישנם שימושים המותרים ללא רישיון, כגון הליכים משפטיים, ספריות וארכיונים ועוד.

## סעיף 19 – שימוש הוגן:

(א) שימוש הוגן ביצירה מותר למטרות כגון אלה: לימוד עצמי, מחקר, ביקורת, סקירה, דיווח עיתונאי, הבאת מובאות, או הוראה ובחינה על ידי מוסד חינוך.

(ב) לצורך בחינה של הוגנות השימוש ביצירה לעניין סעיף זה, יישקלו, בין השאר, כל אלה:

(1) מטרת השימוש ואופיו;

(2) אופי היצירה שבה נעשה השימוש;

(3) היקף השימוש, מבחינה איכותית וכמותית, ביחס ליצירה בשלמותה;

(4) השפעת השימוש על ערכה של היצירה ועל השוק הפוטנציאלי שלה.

(ג) השר רשאי לקבוע תנאים שבהתקיימם ייחשב שימוש לשימוש הוגן.

\*לדוג' למטרות חינוך, מחקר, דיווח עיתונאי וכו'.

פרק ד' סעיפים 20 – 30 , 32 – שימושים המותרים ללא רישיון:

\*לדוג' בהליכים משפטיים, ספריות וארכיונים (סתם הרחבה).

תביעה בגין הפרת זכות יוצרים:

התובע צריך להוכיח לביהמ"ש:

(1) הוא בעל זכות היוצרים ביצירה בגינה הוא תובע

(2) הנתבע הפר את זכותו.

בחוק קבועים תנאים נוספים לקבלת הגנה על זכויות יוצרים ביצירה (שלצערנו לא זה הקורס בו נלמד אותם).

## האתגר של אכיפת זכויות יוצרים בעידן הדיגיטלי:

בעידן הדיגיטלי הפרת זכויות יוצרים נעשית בצורה קלה יותר, זאת מאחר והכל נגיש – ישנם אמצעים רבים יותר באמצעותם ניתן להפר זכויות יוצרים, אז ההפרה הפוטנציאלית היא בקנה מידה רחב מאוד. ההפרה אף קלה לביצוע, שכן השימוש ביצירות כאלו ואחרות (תמונות, סרטונים) הוא יומיומי ואינו נושא אשר אנשים מעמיקים את המחשבה לגביו – קל להשתמש, קל להפיץ (רשתות חברתיות), מה שמביא לכך שההפרה יכולה להגיע לכמה שיותר גורמים. ציבור המפרים הפוטנציאלים הוא גדול, מה שאומר שבעל זכות יוצרים אשר רוצה להגן על הזכות שלו – צריך לנקוט בפעולות אכיפה רבות.

* יותר אמצעים, יותר משתמשים = הפרת זכויות יוצרים בקנה מידה רחב
* גידול באופן ובהיקף שבו יוצרים, מעבדים, משתמשים משתפים ומפיצים יצירות
* האמצעים מצויים בידי כל משתמש קצה ברשת, ובנוסף ישנו ציבור גדול של מפירים פוטנציאליים

מודל האכיפה המסורתי:

מודל האכיפה המסורתי בתחום זכויות היוצרים מטיל אחריות אישית על האדם שפרסם את הפרסום המפר. התביעה לביהמ"ש תוגש כתביעה פרטנית, ביהמ"ש יבחן עניינית את שאלת ההפרה, וכאשר התביעה תוכח יינתן סעד משפטי כזה או אחר. מודל זה אינו מתאים לעידן הדיגיטלי בשל מספר קשיים:

1. בשל גידול בריבוי ההפרות ובזירות ההפרה, קיים קושי מעשי לאתר את מקרי ההפרה. איתור כל מקרי ההפרה ואכיפת ההפרה נגדם מצריכים עלות גדולה (ויקרה) וספק אם מדובר במודל יעיל. עם זאת, בהיעדר הגנה טובה על זכות היוצרים – הדבר יפגע ביצירת יצירות חדשות, לאנשים לא יהיה תמריץ ליצור.
2. הרחבת המשתמשים המפרים (והאנונימיים שבהם). קיים קושי בזיהוי משתמשים ספציפיים לצורך הטלת אחריות, קל וחומר בפעילות אנונימית של משתמשים אשר קיים קושי לחשוף את זהותם. כיום, הנחת היסוד של אנונימיות אינה תקפה עוד בהכרח. קיים קושי לשמור על אנונימיות ברשת. בנוסף, תיקון מס' 5 לחוק זכויות יוצרים מקל על חשיפת זהות מפרים פוטנציאלים.
3. העלות גדולה מן התועלת.
4. ספק בנוגע לתפקידם של גורמי הביניים בקשר להפרות שביצעו המשתמשים שלהם, וחלקם בהפרה.

במקרה זה ישנן שתי שאלות יסוד:

1. האם גורמי הביניים אחראיים להפרות של המשתמשים, בין באופן ישיר בין באופן עקיף, מאחר והם מספקים את הפלטפורמה לכך?
2. האם אנו מעוניינים שגורמי הביניים יהוו בפועל תפקיד באסדרת זכויות יוצרים ברשת?

## שיקולים התומכים בהטלת אחריות על גורמי ביניים:

1. ניתנים לזיהוי ואיתור בקלות:

ראשית, גורמי הביניים ניתנים לזיהוי ואיתור בקלות. תהליך זיהויו של המשתמש ביחיד עלול להיות יקר וממושך, במיוחד בפעילות אנונימית, ועל כן זול וקל יותר להגיש תביעה נגד המתווך.

1. פעמים רבות הן מהוות למונע הנזק הזול:

בנוסף, פעמים רבות גורמי הביניים הם מונע הנזק ביעיל ביותר – הם מצויים בעמדה המאפשרת למנוע באופן אקטיבי את הישנות המקרה. ניתן לראות כי טענות אלו התקבלו במהלך השנים בביהמ"ש (בפרשת נפסטר). התמריץ הוא צמצום חשיפתם המשפטית של אותם גורמי ביניים. בהמשך ניתן לראות כי תמריץ זה הינו אליה וקוץ בה – לעיתים הרצון לצמצם חשיפה משפטית עלול להביא להשלכות שליליות.

1. לרוב בעלי כיס עמוק והם יכולים לפזר את עלויות הנזק:

לרוב גורמי הביניים הללו מהווים כיס עמוק, כך שביכולתם לפזר את עלויות הנזק. סיכויי הנפגע להיפרע מהנזק יהיו גבוהים יותר, ובנוסף גורמי הביניים מפזרים את עלות הפגיעה אל אחרים באופן טוב יותר מהמעוול / הנפגע.

1. הוגנות:

במקביל, ישנו שיקול בסיסי של הוגנות – אם גורם ביניים מרוויח מהתכנים המפורסמים בו, עליו גם לשלם על העוול הנגרם מהשימוש בו. שכן כמעט כל רווחי החברות הנ"ל נולד מתוך התכנים, אזי מתוך הוגנות עליהם לקחת אחריות עליהם.

1. אינטרס ציבורי:

זאת ועוד, ישנו אינטרס ציבורי לשמירת ההתנהלות ברשת תחת שליטה, למנוע פגיעה בכבוד, אוטונומיה, קניין, פרטיות וכיוצא בזה של משתמשים.

## ההשלכות השליליות של הטלת אחריות על גורמי ביניים:

1. החשיפה המשפטית עלולה לייקר משמעותית את עלות הפעלתם של שירותים ברשת, זאת בשל הצורך להקים מנגנוני פיקוח וסינון, ייעוץ משפטי והתדיינות משפטית. הדבר יוביל לצמצום מספר השירותים ולמניעת כניסה לשוק של גופים קטנים/חדשים, מה שיוביל לריכוזיות וליצירת מוקדי כוח שיכשילו את הביזוריות. הפועל היוצא לכל פרט הוא התייקרות עלות השימוש ברשת, לרבות גישה ולאמצעי ביטוי.
2. אפקט מצנן: תמרוץ גורמי הביניים להפעיל פיקוח יתר באמצעות מערכות סינון ועריכה, מה שיביא לצמצום בפרסום ותוכנית וצנזורה עצמית של משתמשים.
3. צמצום מרחב השיח ופגיעה בחופש הביטוי: בנוסף, ייגרם צמצום במרחב השיח תוך פגיעה בחופש הביטוי. כאשר האסדרה נתונה בידיים פרטיות מתעוררים קשיים שונים. בשלך הקושי לעשות זאת ע"י בני אדם, נוצרת הישענות על מערכות אלגוריתמיות לניטור תוכן ואכיפה – האלגוריתם למעשה מבצע איזון בין הערכים, דבר המביא למורכבויות שונות ולקשיים סביב איך מתקבלת ההחלטה והאפשרות להעביר ביקורת על החלטות כאלה.

האתגר: כיצד נאזן בין המטרות החברתיות השונות?

מצד אחד, יש חיפוש אחר מנגנון שיוכל להגשים ולתמרץ הגנה על זכויות יוצרים, מנגנון שיהווה מנגנון הפרה יעיל, כאשר מצד שני יש רצון למנוע את הבעייתיות שבהטלת חובת ניטור וסינון על גורמי הביניים – הטלת אחריות על גורמי הביניים לפעולות המבוצעות ע"י המשתמשים עליהם תוביל להטלת חובת לנטר ולסנן תכנים, חובה המהווה נטל מאוד גבוה לגורמי הביניים – מה שיביא לפגיעה בחזון כיכר העיר החדשה.

## מסגרות רגולטוריות שונות מצאו נקודות איזון שונות ביחס לחובה שתוטל על גורמי הביניים:

1. נוהל הודעה והסרה (אומץ בארה"ב ובישראל) – המשטר שנתמקד בו בקורס
2. אחריות גורמי ביניים להשגת רישיון לשימוש בתוכן מלכתחילה (אומץ ע"י האיחוד האירופי) – נדרשים לקבל רישיון שימוש.

בפועל:

בפועל, לא משנה מה המשטר שאומץ – אכיפה באמצעות גורמי ביניים ברשת היא אסטרטגיית אכיפה מרכזית בזירה הדיגיטלית. יש תמרוץ משמעותי של גורמי הביניים לנקוט באותן פעולות שיטור, ויש הרתעה משמעותית המתרחשת בפועל וגורמת לגורמי הביניים לקחת על עצמם את התפקיד הזה. התמרוץ הזה נובע מעקרון מונע הנזק הזול – גורמי הביניים נמצאים בפוזיציה ייחודית למנוע את ההפרות הללו באופן יעיל ומהיר, זאת מבלי להזדקק להליכים נגד מפרי חוק בבית המשפט.

אמצעי האכיפה של גורמי הביניים הם בעיקר אמצעי הסדרה טכנולוגיים:

1. פיקוח על השימוש ביצירות שהופצו באופן דיגיטלי וזיהוי הפרות
2. אפשרות למנוע מראש גישה / הפצה לא מורשית של יצירות
3. בפועל, אמצעים אלו משמשים לא רק לזיהוי ולמניעה מראש אלא גם לנקיטת פעולות לאחר זיהוי ההפרה.

דוגמאות לאמצעי אסדרה טכנולוגיים:

1. הגבלת הגישה למוצר בו מאוחסן התוכן המוגן בזכויות יוצרים, לדוג' מנעול דיגיטלי על זכויות יוצרים בתוכנה.
2. הגבלה על העברת מידע ברשת, חסימת גישה: ספקיות גישה, ספקיות מארחות, מנועי חיפוש, בעלי אתרים, פלטפורמות שיתוף קבצים, אמצעים טכנולוגיים שונים. הבחירה באמצעי ספציפי משמעותה איזון שונה בין הערכים האמורים (חופש הביטוי וכו').

גורם ביניים = שהוא מתווך, שהוא גורם המחבר בין צדדים.

# הדין בישראל

האם גורמי ביניים אחראים להפרטות שביצעו המשתמשים שלהם?

אחריות ישירה:

גורמי הביניים בישראל לא אחראיים באחריות ישירה לפעולות שהמשתמשים שלהם ביצעו באמצעות הפלטפורמה שלהם (כן באחריות תורמת בכפוף לנוהל הודעה והסרה).

עם זאת, כאשר מדובר על גורם ביניים אשר מפרסם תכנים בעצמו, האחריות יכולה לחול עליו לא כגורם ביניים אלא כגורם מפרסם בעצמו.

אם מקור היצירה המפירה הוא בגורם הביניים ולא במשתמשים, תחול אחריות ישירה להפרה. אחריות זו תוטל מאחר ובמקרה כזה הוא לא מתפקד כמתווך אלא כגורם בפני עצמו.

אחריות תורמת:

פס"ד שוקן: האם גורם ביניים מתווך העל אחריות על פגיעה בזכויות יוצרים של הדפסת יצירה בבעלות הוצאות שוקן ומכירתה כמקראה ע"י תא סטודנטיאלי שמקושר למפלגת העבודה. התעוררה השאלה האם האוניברסיטה (ואיתה המפלגה) אחראיים להפרת זכויות היוצרים שביצע התא הסטודנטיאלי. בפס"ד זה נקבעו התנאים להחלת דוקטרינת האחריות התורמת בדיני זכויות יוצרים:

1. התבצעה הפרה ישירה בפועל
2. למפר התורם הייתה ידיעה ממשית וקונקרטית על ההפרה הישירה, לא מספיקה ידיעה קונסטרוקטיבית כללית
3. המפר התורם תרם תרומה משמעותית, ניכרת וממשית לביצוע ההפרה

בפועל היה ספק האם האוניברסיטה העברית הייתה מודעה להפרה בפועל להפרת הזכויות של שוקן, ונראה כי היא לא תרמה באופן ניכר וממשי לביצוע ההפרה, ולכן לא החילו על האוניברסיטה אחריות כמפרה תורמת לפעילות התא הסטודנטיאלי – בניגוד למפלגת העבודה, אשר עליה הוחלה אחריות זו.

פס"ד רוטר: פורום שקיים באינטרנט, בתוכו נמצאים קישורים המכילים תוכן פיראטי. אלי"ס ושורה של בעלי זכויות יוצרים פנו לביהמ"ש וביקשו שרוטר תצפה אותם על הפרת זכויות יוצרים שהתאפשרה באמצעותה. התובעים עצמם הצדיקו את הפנייה לביהמ"ש תוך הפניה לעקרון מונע הנזק הזול – הטיפול היעיל ביותר אינו טיפול בגורם המפר אלא הטלת אחריות על גורם הביניים האחראי לכך. זו הייתה הזדמנות לבחון את דוקטרינת האחריות התורמת.

גרוסקופף: קובע כי בעל אתר שלא ידע על הפרת זכויות יוצרים לא יישא באחריות להפרה, כל עוד כאשר נודע לו על הפרת זכויות היוצרים דאג להסיר את הפרסום המפר סמוך לקבלת ההודעה עליו.

הלכה למעשה, ישנה חסינות לגורמי הביניים מפני אחריות תורמת כאשר המחיר לחסינות זו אינה גבוה, מחיר של ניהול מנגנון הודעה והסרה.

גרוסקופף החליט לנקוט במודל זה כדי לא לגרום לאפקט מצנן, וכדי למנוע את העלויות הכרוכות בהטלת אחריות לקיום מנגנוני ניטור וסינון. משכך, אין חובה משפטית לקיים מנגנוני ניטור וסינון, אלא החובה היא רק בעניין מנגנון הודעה והסרה.

לדעת המרצה, מערכת המשפט צריכה להתעשת ולהסדיר בצורה ברורה יותר את האכיפה ע"י גורמי הביניים. התוצאה היא שגורמי הביניים ברשת הפכו לזרוע אכיפה בתחום זכויות היוצרים.

מצבים חריגים בהם תוטל אחריות על גורם הביניים בגין פעולות משתמשים:

1. עידוד, האתר מעודד פרסום קישורים מפרים: נלמד משמו של האתר, אופן שיווקו, תקנון האתר והמסר הכולל לגולשים.
2. הפורום הפסול, הפורום משמש, רובו ככולו, להצבת קישורים לאתרים מפרים. הקביעה נעשית בשני אופנים:
3. מבחן אבסולוטי: מספר הקישורים המפרים לאתרים מפרים.
4. מבחן יחסי: אחוז הקישורים המפרים ביחס לכלל ההודעות בפורום.

המשמעות של פורום פסול:

1. חזקה שבעל האתר מודע לכך שהוא מסייע לקיומן של הפרות ישירות וכי סיוע זה הוא בגדר תרומה ממשית ומשמעותית להפרות
2. כדי להימנע מהטלת אחריות, על בעל האתר מוטל להוכיח אחד משניים:
3. להמשך קיומו של הפורום יש ערך לגיטימי;
4. היעדר ידיעה על היקף הפעילות הפסולה – ומכאן חזרה לנוהל "הודעה והסרה".

כללי אצבע היוצרים חשד לפורום פסול (נוסחו ב-2011, בפס"ד רוטר):

1. בפורום סגור:

פורום אשר הכניסה אליו מוגבלת בתשלום או באופן אחר, מה שמקשה על בעלי זכויות היוצרים לבצע את הפיקוח.

יש להוכיח כי באתר יש 10 קישורים מפרים וכי ההודעות הכוללות קישורים מפרים מהוות יותר מרבע מההודעות המהותיות בפורום – אזי ייווצר חשד לפורום פסול.

1. בפורום פתוח:

קל יותר לפיקוח. על כן כאשר לפחות מחצית מהתוכן המהותי של הפורום הן הודעות הכוללות קישורים לאתרים מפרים ייווצר חשד לפורום פסול.

שיקולי המדיניות מאחורי דוקטרינת ההפרה התורמת וקיום נוהל הודעה והסרה ע"י גורמי הביניים ברשת (גרוסקופף):

1. היקף וחומרת ההפרות גדולים יותר בשל הקלות של הפרת הזכויות ברשת.
2. חשיבות בהגנה על זרימת המידע, זכות הציבור לדעת וחופש הביטוי.
3. המורכבות באלטרנטיבה (הטלת אחריות על גורמי הביניים): חשש מהטלת עלויות כבדות של ניטור וסינון על גורמי הביניים הפרטיים, ומנגד חשש מאכיפת יתר כדי למנוע סיכונים משפטיים. בנוסף, ישנו חשש לאפקט מצנן על פעולות רצויות, חדשנות, ביזור וחזון כיכר העיר החדשה.

נוהל הודעה והסרה הינו יציר פסיקה אמריקאית שאומץ בחוק. בישראל, נוהל זה יציר פסיקתי אשר הופיעה בפרשת רוטר ובפרשות אחרות שקדמו לה והפנו למודל האמריקאי.

כדי להבחין בין הטלת אחריות ישירה מול אחריות תורמת, אזי נשאל עצמנו – מי מפרסם? עלינו תמיד לבחון האם הפלטפורמה בכובע של "המפרסמת" או שמא בכובע של "המתווכת".

הפרה שבוצעה ע"י גורם הביניים עצמו:

משמע כאשר ההפרה מבוצעת ע"י הגורם עצמו, לא על ידי המשתמשים. במקרים כאלו גורם הביניים יהיה אחראי להפרה.

* פס"ד גולצמן:

ההפרה בוצעה ע"י כתב ששותף בניהול האתר ולא ע"י גולש אנונימי, ולכן גורם הביניים נמצא אחראי בגין הפרת זכות יוצרים.

* פס"ד ברזל:

משרד החינוך חויב בתשלום פיצויים למרות השימוש הראוי בנוהל הודעה והסרה, משום שעובדי המשרד הם אלו שהעלו לאתר את החומר המפר (שיר) – זאת בניגוד למשתמשים פרטיים באינם נמצאים בשליטת בעלי האתר.

השוואת פעילות אכיפת זכויות יוצרים ברשת בבית המשפט ובקרב גורמי הביניים (מחקר של אלקין-קורן ובר-זיו):

בעוד בביהמ"ש הוגשו פחות ממאה תביעות, מנגד לגוגל הוגשו מעל 2550 בקשות! לכאורה גורמי הביניים החליפו את בתי המשפט בנושא.

1. בתי המשפט: כמה תביעות של בעלי זכויות יוצרים בגין הפרת זכויות ברשת הוגשו לביהמ"ש (99 תביעות).
2. גורמי ביניים: כמה בקשות של בעלי זכויות יוצרים לנקוט אמצעי הסרה, חסימה וסינון בגין הפרת זכויות יוצרים הוגשו לגורמי הביניים. במחקר: בקשות מגוגל להסיר דפים ותארים מתוצאות החיפוש. במנוע החיפוש של גוגל סירץ' בלבד – 2,556 בקשות הסרה. היקף אכיפה עצום באמצעות גורמי הביניים בהשוואה לבתי המשפט. משכך, ניתן לראות כי בפועל זירת האכיפה המשמעותית עזבה את ביהמ"ש ועברה לגורמי הביניים. המצב מאתגר אף יותר כאשר מסתכלים על מה קורה בפועל בשתי זירות האכיפה:

ממצאים מרכזיים: אכיפה בבתי המשפט:

* משרתת מגוון מצומצם של תובעים, במענה לסוג מצומצם של יצירות
* תובעים ביקשו בעיקר סעד כספי (60%), אך גם צווים שונים ופיצויים (38%)
* הליכים רבים מסתיימים בפשרה (ולא בהכרעה) – דבר המהווה עדות ללחץ על הנתבעים להפסיק את פעילות ההפרה => מכאן לנו לא נוצר הכלל המשפטי
* שחקנים חוזרים עושים שימוש אפקטיבי בהליך משפטי. למשל ארגון זיר"ה (זכויות יוצרים ברשת)

ממצאים מרכזיים: בקשות הסרה מגוגל:

* מספר רב של בקשות הסרה – בתקופת המחקר (14.6.11 – 12.1.14) היו כ-7091 תלונות על הפרת זכויות יוצרים לכאורה. התייחסו להפרות ב-219 שמות מתחם ישראליים.
* מספר שחקנים חוזרים בולטים הפעילים בהגשות בקשות הסרה (בעיקר חברות רב לאומיות בתחום התוכנה וחברות סרטים, כאשר מייקרוסופט הגישה את מספר התלונות הגבוה ביותר).
* גוגל מפרסמת נתונים גולמיים (עולמיים) ביחס לבקשות הסרה שהתקבלו אצלה בדו"חות שקיפות תקופתיים – 5,098,780,527 בקשות הסרה של אתרים.

## אכיפה באמצעות מנגנון הודעה והסרה מתוצאות מנוע החיפוש של גוגל:

בפועל מנוע החיפוש של גוגל הפך לכלי משמעותי לאכיפת זכויות יוצרים ברשת, שכן על מנת להגן על זכויות היוצרים נפנה ל"שוטר התנועה" אשר מכוון את האנשים לשם.

בקשות הסרה: בעלי זכויות יוצרים (לכאורה) מבקשים מגוגל לאכוף את זכותם ע"י הסרה של קישורים מפרים (לכאורה) מתוצאות מנגנון החיפוש של החברה.

הליך בקשת ההסרה כמתואר בגוגל (מצוטט מהתקנון):

1. אם הודעת הסרה מתבררת כחוקית, חוק זכויות היוצרים דורש מאיתנו להסיר את התוכן מהשירותים. במקרה זה, להסיר כתובת אתר מתוצאות החיפוש.
2. כאשר אנו נוקטים פעולה בתגובה להודעת הסרה בגין הפרת זכויות יוצרים, אנו מיידים את מנהל האתר המושפע מפעולה זו דרך search console של גוגל.
3. אם מנהל האתר הרלוונטי או ספק התוכן המדובר סבור שהתוכן אינו מפר זכויות יוצרים או שההודעה הוגשה בטעות, הוא יכול להגיש הודעה נגדית.
4. אנחנו בודקים את כל ההודעות הנגדיות ומחליטים האם להחזיר את התוכן.

## "נוהל הודעה והסרה" – היפוך נטל הראייה?

הודעה = ככלל, הסרה – למרות שמדובר רק בטענה להפרה ולבעלות בזכות, פעמים רבות ההודעה מבוצעת אף היא באמצעים טכנולוגיים.

בהליך של גוגל נעשה מעין היפוך של נטל הראיה**.** הודעה מביאה להסרה, למרות שמדובר רק בטענה להפרה ולבעלות בזכות. פעמים רבות, ההודעה מבוצעת אף היא באמצעים טכנולוגיים. עקרונית, מפרסם התוכן המפר יכול לערער על החלטת ההסרה, זאת ע"י פנייה לגורמי הביניים ולבקש לבחון מחדש את ההחלטה. בהליך משפטי בבתי המשפט תוכן מוחזק כלגיטימי אלא אם כן הוכח כי הוא מפר זכות יוצרים. במנגנון הודעה והסרה, תוכן שנטען (אך לא הוכח) שהוא מפר זכות יוצרים (שנטענה אך לא הוכחה) מוסר מיידית, כאשר החזרת התוכן מותנית בהגשת ערעור לגורם הביניים ע"י בעל התוכן. מנגנון זה מקשה על הגורמים הקטנים כאשר החליטו להסיר תוכן כזה או אחר שהעלו.

מדוע היפוך נטל הראייה:

בהליך משפטי – תוכן מוחזק כלגיטימי אלא אם הוכח כי הוא מפר זכות יוצרים.

בהליך מנגנון "הודעה והסרה" – תוכן שנטען (אך לא הוכח) שהוא מפר זכות יוצרים (שנטענה אך לא הוכחה) מוסר מיידית. החזרת התוכן מותנת בהגשת "ערעור" לגורם הביניים על ידי בעל התוכן.

האם רצוי להפקיד בידי גורמי הביניים את תפקיד קביעת קיומה של הפרת זכות יוצרים?

מצד אחד, הגנה על זכות יוצרים ויצירת מנגנון אכיפה יעיל מובילות לצורך בהטלת אחיות על גורמי ביניים ושילובם בפעולות אכיפה.

מצד שני, מודל אכיפה שנשען על גורמי ביניים פרטיים באמצעים טכנולוגיים מעורר קשיים רבים.

לקחים מיישום נוהל הודעה והסרה בארה"ב – The Digital Millennium Copyright Act (DMCA):

1. גורמי הביניים תומרצו לתת משקל יתר להגנה על זכויות יוצרים, גם במחיר פגיעה בזכויות אחרות, בין היתר כי לא מוטלת אחריות בגין הסרה בתום לב של חומרים שנחשדו כמפרים אך בפועל הינם לגיטימיים – כאשר אם נודע להם על ההפרה אך החומר לא הוסר מיד, כן תוטל עליהם אחריות.
2. גורמי הביניים פיתחו מדיניות וולונטרית של סינון אקטיבי מראש של תכנים מפרים לכאורה. בפועל נעשתה העברת נטל השיטור נגד הפרת זכויות יוצרים מבעלי הזכויות לגורמי הביניים – שיטור שנעשה באופן אלגוריתמי. משכך, לא ניתן להיות בטוחים ב100% מה עומד מאחורי פעולת הסינון, האם היא מושפעת מאינטרסים מסחריים המפעילים טכנולוגיות סינון פרטיות. עם זאת, הדבר יצר מודל מסחור מצליח – השגת רישיון לשימוש בתוכן מוגן בזכויות יוצרים. למשל: מערכת Content ID של יוטיוב (אבל – גם הוא מודל מסחור מצליח).
3. משטר אכיפה אוטומטי-אלגוריתמי : עיבוד וטיפול אוטומטי בבקשות ההסרה (מענה הכרחי גם בשל האוטומציה של בקשות ההסרה). הישענות על טכנולוגיות סינון ושיטור פרטיות – שיקול דעת אלגוריתמי. אינטרסים פרטיים, כלכליים – מסחריים בעיקרם. היעדר שקיפות (סוד מסחרי) – בעיית "הקופסא השחורה". מעורבות אנושית מינימלית בהחלטות על איזון הזכויות.

למעשה משטר האכיפה האוטומטי – אלגוריתמי: נוצר כדי לעמוד בהיקפים הרבים של הפעילות, בעיקר בגורמי הביניים הדומיננטיים אשר בפועל מיישמים את מנגנון הודעה והסרה אליו הם מחויבים, באמצעות מערכת טכנולוגית המעבדת ומטפלת באופן אוטומטי בבקשות הסרה. הקושי המרכזי הוא שישנה הישענות על טכנולוגיות סינון ושיטור פרטיות, כאשר הפלטפורמות מפעילות שיקול דעת אלגוריתמי שלא נודע כיצד עוצב וגם אין שקיפות לגבי האופן בו עוצב. על כן למסתכלים מבחוץ אין יכולת אמיתית להסתכל ולראות מה נעשה.

בעיית הקופסא השחורה:

אין שום מידע על כיצד מיושם בפועל מערך האיזונים הרלוונטי להחלטה. משכך, ישנה מעורבות אנושית מינימלית בהחלטות על איזון הזכויות.

שילוב טכנולוגיה בפעילות האכיפה של בעלי הזכויות:

טכנולוגיה המזהה אוטומטית של הפרות זכויות יוצרים, ע"י משלוח אוטומטי של בקשות הסרה של תוכן.

החשש הוא טעות בזיהוי הפרות ובקשות המבוססות על דרישות לא לגיטימיות.

לדוג' – בקשה להסיר תוכן מוגן כאשר השימוש מותר ע"פ חוק.

סיכום:

## החששות מהפקדת האכיפה בידי גורמי ביניים:

1. הפרטת האכיפה: הפקדת האחריות לביצוע איזון הערכים בידי גורמי ביניים פרטיים. גורמי הביניים מתומרצים לנקוט אמצעים להפחתת הסיכון המשפטי. הדבר מוביל לחשש מניטור וחסימת יתר של תכנים או של משתמשים, גם מראש (לשם מניעה). מעבר לשיקולים אינטרסים מסחריים-כלכליים המעורבים בסינון התוכן, יש חשש מפתח לניצול לרעה של מנגנון הודעה והסרה (הודעות שווא). זה בהשוואה לביהמ"ש, אשר אמון על האינטרס הציבורי בכללותו – ההגנה על הקניין הרוחני של היוצרים והאוטונומיה של הפרט, הזכות לפרטיות, חופש הביטוי חופש הגישה – הם הערכים הדורשים איזון במקרים כאלו. אין שום הבטחה כי במנגנון סינון פרטי, האיזון אכן מתקיים באופן הזה, כפי שהוא מתקיים בביהמ"ש.
2. אסדרה באמצעים טכנולוגיים: איזון הערכים מבוצע בכלים טכנולוגיים, אכיפה אלגוריתמית.
3. היעדר פיקוח: בפועל, לא קיימים פיקוח ציבורי או ביקורת שיפוטית אפקטיביים על אופן הפעולה של גורמי הביניים, זאת בנוסף להיעדר השקיפות (סוד מסחרי) ולקושי הטכני של הבנת המשמעות של קוד התוכנה.
4. אפקט מצנן: פגיעה בחופש הביטוי של משתמשים ובפעולות רצויות ברשת.
5. ריכוזיות ופגיעה בחדשנות: הפחתה בהיצע השירותים בשל עלויות משפטיות ותפעוליות. זה מכיוון שעל מנת להיכנס לשוק, על שחקנים חדשים עכשיו לפתח מנגנונים יקרים ומורכבים בדומה למנגנונים שגוגל כבר פיתחה ומשתמש בהם.

## אמצעים לצמצום/מניעה של סיכונים:

1. יצירת כללים ברורים בדבר טיפול בתלונות (הזדהות המתלונן, נקיטת אמצעים מינימליים לבירור זכויותיו).
2. שקיפות לגבי היקף שיתוף הפעולה בין גורמי הביניים לבין בעלי הזכויות.
3. שקיפות לגבי אופן הפעולה של מגנוני האכיפה של גורמי הביניים (סטנדרטים בבחינת בקשות הסרה, כיצד נעשית בחינת הבקשות, דו"חות מפורטים לגבי דפוסי בקשות והחלטות הסרה).

ריכוזיות לעומת ביזוריות בניטור תוכן?

האם רצוי ליצור שיתוף פעולה בין פלטפורמות בניטור תוכן או אפילו גורם אחד שיעסוק בניטור תכנים (פרטי, ללא מטרות רווח, ציבורי)?

"קרטלים של תוכן" – אוולין דואק:

האם בתחום למעשה נוצרו קרטלים של תוכן? שרק מס' חברות בודדות שולטות בניטור וסינון התוכן. קרטלים אלו למעשה חותרים תחת כל מה שרצינו להשיג ברשת האינטרנט. לדוג' פורנוגרפיה, הסתה לטרור, השפעה על בחירות, ספאם. האם ההתנגדות פוחתת בעניין זכויות יוצרים? למעשה יכולים להיות שיקולים לכאן ולכאן – ישנה חשיבות לתחום התוכן שבו אנו עוסקים.

**המצב המשפטי באיחוד האירופי:**

ההסדר הקודם – "המפרץ הבטוח":

בהיעדר ידיעה, היעדר אחריות; ניתן לדרוש שיורידו תוכן מפר, ללא חובת ניטור או סינון תוכן.

## ההסדר החדש באירופה – סעיף 17 ל-CDSM (יוני 2021):

חל על גורמי ביניים המאפשרים שיתוף תוכן.

חבים באחריות ישירה לתוכן המפר שפרסמו משתמשיהם ולכן נדרשים:

* לעשות את מרב המאמצים לקבל מבעל זכות היוצרים אישור לפרסום התוכן.
* להבטיח שיצירות שאין אישור לפרסמן לא יועלו לשירותיהם.

השינוי בחקיקה האירופית:

יש כאן שינוי, מפאסיביות לאקטיביות – במקום להמתין לקבלת הודעת ההסרה, יש לנקוט בפעולות על מנת להבטיח שהתוכן המפר לא יעלה. באופן מעשי – ישנה חובת ניטור תוכן אקטיבית בכלים אוטומטיים.

ביהמ"ש האירופי נקט בפרשנות מצמצת:

לפיו ההסדר בסעיף 17 מאזן כראוי בין חופש הביטוי והזכות לקניין רוחני.

פרשנות מצמצמת: התמקדות בפעולות לאחר העלאת התוכן + הגנות פרוצדורליות שונות בהליך ניטור והסרת התוכן.

חריג: סינון תוכן "אקס אנטה" ייעשה רק במקרים שבהם לא נדרשת בדיקה עצמאית בנוגע להחרגות.

סיכום:

בארץ – גורמי ביניים נושאים באחריות תורמת להפרת זכויות יוצרים שביצעו משתמשיהם, בכפוף ל-"נוהל הודעה והסרה" (פס"ד רוטר).

* גורמי הביניים ברשת הפכו לזרוע אכיפה מרכזית בתחום זכויות היוצרים.
* היקף פעולות האכיפה בבתי המשפט מזערי בהשוואה לגורמי הביניים.
* היפוך נטל הראייה המסורתי בתחום של אכיפת זכויות יוצרים ברשת.
* קשיים משמעותיים בהפרטת האכיפה ובשילוב אמצעי אכיפה טכנולוגיים.

# סעדים טכנולוגיים: המקרה של צווי הגבלת גישה

להשליםםםםםם

אסטרטגיית אכיפה באמצעות צווי הגבלת גישה:

צווי הגבלת גישה = סעד טכנולוגי.

רקע: סעדים במסגרת הליך משפטי "מסורתי":

* ביהמ"ש מכריע הכרעה מהותית בשאלת ההפרה ולאחריה מוצא צו אכיפה.
* הסעדים מכוונים לעולם הגשמי (קנס, צו עיקול...)
* יישום הצו (אכיפת הסעד) שקוף, וודאי וחד פעמי. לדוג' צו עיקול, אנו רואים בפועל את העיקול. לדוג' צו יציאה מהארץ, אנו רואים בפועל את ביצוע הצו (פלוני למעשה לא יוצא מהארץ).

סעדים טכנולוגיים (לדוג' צווי הגבלת גישה):

* כפופים להליך משפטי מקוצר, ללא הכרעה מהותית בשאלת ההפרה. הם מאפשרים לבעלי הזכויות להפסיק את בקלות ובאופן מידי את הפעילות המפרה.
* הצו מוצא אל הפועל באמצעים טכנולוגיים: קוד תוכנה שמגביל גישה לאתר. ישנם מגוון אמצעי חסימה טכנולוגיים. נבדלים בעלות, מידת האפקטיביות ומידת הפגיעה בתכנים לגיטימיים. פעולת אמצעי החסימה דינאמית (גם אם האתר משנה את מיקומו, עדיין ניתן לרדוף אחריו ולהמשיך לחסום אותו). היעדר שקיפות לגבי אופן הפעולה.

האכיפה בפועל:

האמצעי הטכנולוגי הספציפי שספק הגישה ינקוט יגדיר אץ היקף תחולתו, יעילותו והשלכותיו של סעד החסימה.

עלינו לשים לב כי ביהמ"ש הוא זה שמוציא את הצו, אך יישומו בפועל מוגדר על ידי ספק הגישה לרשת, שמעצב את פעולתו:

1. קביעת היקף ההגנה שניתנת בפועל לזכויותיהם של בעלי זכות היוצרים.
2. ביצוע האיזון בין זכויות בעלי זכות היוצרים וזכויות בעלי תוכנים, ספקי גישה וציבור המשתמשים כמו חופש הביטוי, חופש העיסוק והזכות לפרטיות.
3. התערבות בניטרליות הרשת.

## סעיף 53(א') – צו הגבלת גישה למקור תוכן:

סעיף א': מהווה כסעיף הגדרות.

סעיף ב': בית המשפט רשאי, על פי בקשה של בעל זכות יוצרים או בעל רישיון ייחודי (בסעיף זה – המבקש), לתת צו המופנה כלפי ספק גישה ומורה לו להגביל את הגישה למקור תוכן, כולו או חלקו (בסעיף זה – צו הגבלת גישה), אם שוכנע כי מתקיים לגבי עיקר התוכן שבאותו מקור תוכן אחד מאלה...

סעיף ג' – מתווה זו הגבלת הגישה: בצו הגבלת גישה יורה בית המשפט לספק הגישה לנקוט אמצעים סבירים להגבלת הגישה למקור התוכן, כולו או חלקו, והכול בתנאים ובמידה שאינה עולה על הנדרש, כפי שיורה בית המשפט, כדי למנוע, ככל האפשר בנסיבות העניין, את הפגיעה בבעל זכות היוצרים או בבעל הרישיון הייחודי; בצו כאמור ייכללו בין השאר כל אלה:

1. פרטי מקור התוכן שהגישה אליו תוגבל
2. הוראות לעניין היקף הגבלת הגישה למקור התוכן
3. התקופה שבה תוגבל הגישה למקור התוכן

סעיף ד' – שיקולים שעל ביהמ"ש לשקול במתן צו ההגבלה וקביעת תנאיו: במתן צו הגבלת גישה ובכלל זה בקביעת תנאיו ישקול בית המשפט, בין השאר, את כל אלה, אף אם לא הוגשה התנגדות לבקשה:

1. ההשפעה על הציבור כתוצאה מהגבלת הגישה לפי הצו או מהחלטת בית המשפט שלא לתת צו;
2. חומרת ההפרה הנטענת;
3. חיוניות הצו למניעת הפרה, ככל האפשר, של זכות יוצרים;
4. יעילותם של סעדים אחרים העומדים לרשות בעל זכות היוצרים או בעל הרישיון הייחודי, ובכלל זה פנייה למפר או למשיב, אם זהותו ידועה או אם ניתן לאתרו בשקידה סבירה;
5. מידת הפגיעה הצפויה בגישה למקורות תוכן אחרים;
6. מידת הפגיעה הצפויה בפרטיות של משתמשי האינטרנט.

הבהרה: ביהמ"ש מחויב לשקול שיקולים אלה גם אם לא הוגשה התנגדות.

היחס בין צו הגבלת גישה להסרת תוכן:

ככל שהשרת עליו מאוחסן התוכן או מקור התוכן נמצא בישראל או שהוא בשליטת אדם / תאגיד הנמצא בישראל לא יינתן צו הגבלת גישה.

במקום זאת: תינתן הוראה להסרת התוכן מהשרת בתנאים שיקבע ביהמ"ש (אלא אם הסרת התוכן או מקור התוכן מהשרת אינה אפשרית בנסיבות או שיש טעמים מיוחדים אחרים להימנע מהסרה).

הבעיה המרכזית העולה היא ששיקול האינטרסים לא מתבצע בפועל ע"י ביהמ"ש, אלא מתבצע ע"י גורמי הביניים.

אלו קשיים מעורר השימוש בצווי הגבלת גישה?

העברת השליטה על האכיפה לספקי גישה פרטיים.

חשש שהמשטר המשפטי יתמרץ אכיפת יתר וייצור אפקט מצנן: תמרוץ להסרה אוטומטית מראש של תכנים מפרים לכאורה.

הפקדת גורמי ביניים על העיצוב הטכנולוגי של החסימה (במילים אחרות – על איזון הזכויות).

מאפייניהם מקשים להכפיפם לביקורת משפטית ופיקוח ציבורי:

1. הוצאת הצווים כפופה לפיקוח שיפוטי מראש
2. יישום הצווים, לרבות הגדרת פרטיהם הטכניים, נתון בידי גורמי ביניים פרטיים.

למבחן: יש לחזור על הקשיים האמורים ולפתח יכולת לנתח כל הצעה טכנולוגית, או הסדר טכנולוגי, ואותם לראות בראי הקשיים הנ"ל. חלקם חוזרים שוב ושוב, חלקם ייחודיים.

הסעיף המאפשר "חופש ביטוי" לכאורה ברשת בארה"ב - 47 US Code 230(c):

(c) Protection for “Good Samaritan” blocking and screening of offensive material

(1)Treatment of publisher or speaker

No provider or user of an [interactive computer service](https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=47-USC-1900800046-1237841278&term_occur=999&term_src=title:47:chapter:5:subchapter:II:part:I:section:230) shall be treated as the publisher or speaker of any information provided by another[information content provider.](https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=47-USC-10252844-1237841279&term_occur=999&term_src=title:47:chapter:5:subchapter:II:part:I:section:230)

(2)Civil liability No provider or user of an [interactive computer service](https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=47-USC-1900800046-1237841278&term_occur=999&term_src=title:47:chapter:5:subchapter:II:part:I:section:230) shall be held liable on account of —

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to [information content providers](https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=47-USC-10252844-1237841279&term_occur=999&term_src=title:47:chapter:5:subchapter:II:part:I:section:230) or others the technical means to restrict access to material described in paragraph (1).

הביקורת נגד הסעיף:

הביקורת היא שלאחרונה סעיף זה יצא משליטה, ככל שהמודל הזה עבר, החל ניצול לרעה של החסינות הנ"ל (של הסעיף).

בפועל ישנו חשש כי מרוב שרצינו לתמוך בחופש הביטוי, הגענו למצב שלא בטוח שאנו מעוניינים בחסינות שכזו.

# יישוב סכסוכים בעידן הדיגיטלי: ממסחר מקוון לבתי משפט מקוונים

המרצה מציגה את קולין רול, המנהל המייסד של מחלקת יישוב הסכסוכים של Ebay ואת השופט מייקל בריגס אשר עמד בראש ועדה שהציעה רפורמה במערכת בתי המשפט בבריטניה. שניהם נולדו מתוך הצורך המקוון של הזירה הדיגיטלית בכל הקשור ליישוב סכסוכים.

הנתונים הרשמיים של החברה מפרטים כי ב-Ebay יש כ-60 מיליון סכסוכים בשנה הנוגעים להגעת המוצר ולחוסר שביעות רצון ממנו, והם בשווי ממוצע של 100 דולרים – שווי די נמוך של תביעה אשר אינו מצדיק בהכרח פעולות משפטיות קלאסיות בעלות עלות כלכלית גבוהה. בנוסף, גם ישנו קושי כיוון שמדובר בגורם ביניים, כך שלא ברור מה סמכות השיפוט הרלוונטית לסכסוך (פעמים רבות הלקוח והמוכר מגיעים ממדינות שונות ומשיטות משפטיות שונות), וגם אם היה ברור, לא סביר כי סכסוך בין-יבשתי בשווי של 100 דולרים לערך שווה וראוי את המאמץ.

עם זאת, Ebay חייבת להעניק פתרון לבעיה כדי ליצור אמון ביניהם לבין המשתמשים. נדרש לעשות זאת באופן יעיל וזול, ללא שימוש בעורכי דין, על מנת לתת מענה ראוי למשתמשים תוך שימוש בעלויות סבירות. המערכת שרול יצר, "מערכת ה-ODR הפרדיגמטית", מהווה כיום דגם שהרבה חברות אימצו לאחר מכן, וזה גם השפיע על האופן בו בתי משפט, כמה עשורים לאחר מכן, עשו בו שימוש.

השופט בריגס, שבאותו הזמן קיבל מנדט למצוא פתרון למשבר של מערכת המשפט האנגלית, מצא כי השיטה שפיתח רול יכולה להתאים לו לצורך שהתעורר באותו הזמן. מערכת המשפט האנגלית מאופיינית בשיעור גבוה של בעלי דין שמייצגים את עצמם. משכך, המערכת הבריטית מתאפיינת בעלויות מאוד גבוהות של ליטיגציה (דבר המהווה חסם עבור חלק מהאנשים), המערכת מתמודדת עם עומס מאוד גדול של תיקים, וכתוצאה מכך משך חיי התיקים הוא מאוד ארוך. בנוסף, ישנה גם בעיה של נגישות במרחק (בריטניה הינה מדינה גדולה יחסית עם אוכלוסייה מפורזת), נגישות של זמן (לא היה מספיק זמן בפועל, הן למערכת המשפט, הן לאדם הפרטי) ונגישות של חוק.

עם זאת, החסם המרכזי מכל היה מורכבות הדין הפרוצדורלי ומורכבות הדין המהותי, שכן השפה המשפטית וכלליה אינם נגישים לרוב הציבור. אלו הבעיות שהתבקש השופט בריגס לפתור, תוך כדי שנדרש במקביל לצמצם את התקציב שניתן למערכת המשפט ולגופי הסיוע המשפטי – זאת לאור המשבר הכלכלי בשנת 2008.

במקביל, עם העלייה בשימוש והתגברות היכולות של טכנולוגיות מתקדמות יותר, החלו להיכנס גם מערכות חכמות אחרות ומתוחכמות יותר למערכות משפט שונות המתקשרות לנושא של קבלת החלטות אלגוריתמיות והישענות על אוטומציה במערכות המשפט.

תפנית בעלילה – הגעתה של הקורונה:

התפנית בעלילה התרחשה בעת מגפת הקורונה, אשר לא השאירה למערכת המשפט ברירה אלא לאמץ כלים טכנולוגיים בשל הריחוק החברתי שנכפה עליהם, זאת במקביל לצורך הממשיך בהליכים המשפטיים. משכך, הושקו הליכים מרחוק ובבת אחת אפשרו להגיש באופן מקוון מסמכים וניהול תיק בצורה מקוונת. בתי משפט החלו בעשרות מדינות לנהל הליכים באופן מקוון, זאת לאחר התנגדות ארוכת שנים לשנות את התצורה המסורתית של המשפט שלא השתנתה כבר מאות שנים באופן בו היא מתנהלת. בישראל דיוני מעצר עברו לדיון מרחוק בהיוועדות חזותית, נערך פיילוט של היוועדות חזותית בהליך אזרחי בהסכמה והליכים רבים התנהלו בצורה מקוונת כזו או אחרת.

בהמשך, בגין הצורך לקיום הליכי יישוב סכסוכים אשר היו נעשים בטריבונלים כאלה ואחרים, הוקם בית הדין המקוון הראשון בישראל, כאשר מיום הקמתו כל הליכיו נעשים בצורה מקוונת.

:ODR – Online Dispute Resolution:

מערכת של יישוב סכסוכים מקוון במסגרתה מאפשרים לצדדים להשלים את כל ההליך במלואו, החל מהגשת התביעה ועד לסיום בהכרעה או הסכם, כולל ערעור, על גבי פלטפורמה מקוונת. הליך המהווה יותר מאשר היוועדות חזותית בלבד. פלטפורמה זאת מהווה שילוב של שני כוחות מהותיים:

1. יישוב סכסוכים בדרכים חלופיות (ADR) והתוצר של חיים בעידן הדיגיטלי.
2. הציפייה של אנשים כי שירותים שבעבר ניתנו פנים אל פנים יינתנו כעת באופן מקוון.

זהו מונח גג הכולל בתוכו מקורות וסוגים שונים של סכסוכים, שיטות שונות של יישוב סכסוכים, טכנולוגיות והליכים.

יישוב סכסוכים מקוון כתוצר של העידן הדיגיטלי:

ככל שיש מגוון רב יותר של מערכות שונות במרחב הדיגיטלי, נוצרת זירה חדשה של מערכות יחסים עסקיות ואינטראקציות אשר מולידות סכסוכים. מערכת זו יוצרת סוג חדש של סכסוכים ואת הצורך להבטיח את אמון המשתמשים. בנוסף, ישנה ציפייה מצד המשתמשים כי יישוב הסכסוך ייעשה בצורה מקוונת, זאת לאור העובדה כי שירותים רבים כיום מסופקים באופן מקוון – קל וחומר לאור הנגישות והמסוגלות הטכנולוגית ("ממשל זמין"). הדבר מתעצם לאור הגדילה ביזמות ובחדשנות במרחב הדיגיטלי. עם זאת, ישנו חלק באוכלוסייה בעל פערים בנגישות טכנולוגית אשר יש להביא בחשבון בעת החשיבה על ניהול המערכת המקוונת.

יישוב סכסוכים מקוון כחלק מהמגמה ליישוב סכסוכים בדרכים חלופיות (ADR):

תנועת הנגישות לצדק ותנועת ה-ADR דרשו ליצור דרכים אחרות לפתרון סכסוכים על מנת להגביר את הנגישות לצדק לחתכים רחבים באוכלוסייה – הן מבחינת צרכים, יכולות, אינטרסים ומטרות. הם טענו כי ההליך החד צדדי שביהמ"ש מציע אינו מגשים את מטרות הצדדים בצורה מלאה, ועל כן יש צורך לפתרון אחר אשר יתאים, זאת תוך שאיפה ליישוב סכסוכים באופן מהיר, זול, יעיל, נגיש, ופשוט פרוצדורלית. החזון שעמד לנגד עיניהם הוא של "בית משפט מרובה דלתות", כך שאנשים יוכלו לפנות ליותר מדלת אחת במקרים של סכסוך: הליך אזרחי, גישור, בוררות, גישור קהילתי. הדבר בגדר חזון מאחר ואין אפשרות להגשים אותו במלואו.

היבטים המתארים מערכות ODR:

1. בתחום הסכסוך ישנם מערכות שונות המיישבות סכסוכים בתחומי מסחר, צרכנות, משפחה, עבודה – זאת ברמת מורכבות גדולה באופן הכוללת עילות ונושאים רבים, סכסוכים שנולדו ברשת ומחוצה לה.
2. המערכות מיישבות סכסוכים בהקשר פרטי או ציבורי, מדינתי או בינ"ל, ובהקשר סוגים שונים של ספק השירות (עצמאי, מתווך, מוסדי).
3. התהליך עצמו של שיטת יישוב הסכסוך נעשה בדרכים שונות: גישור, בוררות, שיפוט, מושבעים, הערכת מומחה.
4. הטכנולוגיה: עושר הערוץ התקשורתי, סינכרוניות, אוטונומיות המערכת: האם היא כלי המופעל ע"י הצדדים או מערכת אוטונומית בפני עצמה.

מערכת ה ODR כצד רביעי בסכסוך:

היות הפלטפורמה מופעלת ע"י בנאדם ומאפשרת לצדדים לבצע פעולות כאלה ואחרות בהליך מגדירה מערכת ה ODR כצד הרביעי לסכסוך, שכן ישנם שני הצדדים וישנו הגורם המגשר. אית'ן קאש וג'נט ריפקין טמעו את המושג הזה ע"י מאמר אקדמי. התפיסה גורסת כי לא מדובר בצד ניטרלי לסכסוך, וכי עיצוב הממשק והמערכת הטכנולוגית משפיעים על הליך יישוב הסכסוך, דבר שאינו יהיה שקוף ואינו ייחשף בהכרח בעיני הצדדים לסכסוך. לטכנולוגיה יכול להיות תפקיד שיותר אינסטרומנטלי, בעיקר במצבים בהם המערכת עוברת שימוש על ידי האדם ומקבלת הוראה מאחד הצדדים.

מערכת ה ODR כצד שלישי לסכסוך:

המערכות המאתגרות יותר הן כאשר מערכת ה-ODR היא "הצד השלישי" בסכסוך, במסגרתה מערכת ה-ODR מנהלת באופן עצמאי את הליך יישוב הסכסוך, ללא צורך במעורבת של צד שלישי אנושי. מדובר על מערכת שמסתמכת על עצי החלטה (אשף יישוב סכסוכים) על הליכי בינה מלאכותית ובשימוש כלים חישוביים מתקדמים יותר.

מודלים טכנולוגיים בהליכי יישוב סכסוכים – 3 קטגוריות:

1. העברת יישוב הסכסוך כפי שהוא לסביבה מקוונת: הרחבת נגישות של מקום וזמן, כשאר עצם ההפרדה והריחוק מאפשר לנהל רגשות ולשלוט על פערים ביחסי הכוחות באופן שמייצר תחושת השתתפות מוגברת מכל הצדדים.
2. עיצוב מחדש של ההליך: אנו לוקחים את ההליך כפי שאנו מכירים אותו ומסדרים אותם מחדש בכדי לתת הליך חדש ונגיש יותר באופן המתוכנן לשימוש "אדם מן היישוב", זאת ע"י: פישוט פרוצדורלי, מתן סיוע/מידע נחוץ לאורך ההליך, אבחון אוטומטי של בעיות ופתרונות, שפה יומיומית ולא בטרמינולוגיה משפטית, אימות מידע בשדות למניעת טעויות, חוויות משתמש מותאמות, הפקת מסמכים אוטומטית.
3. מודלים חדשים: חישוביות, מערכות לומדות, רשתות חברתיות, CROWD SOURCING, בלוקצ'יין.

הרבה פעמים נראה מערכות היברידיות, בהן נראה שילוב של כלים שונים ממודלים שונים.

מספר דוגמאות:

1. הראשונה מראה ניהול מקוון של ההליך (העברת יישוב הסכסוך לסביבה מקוונת) ע"י תקשורת סמויה בין עו"ד ללקוחה, מתן אפשרות להציג מסמכים וראיות וניסוח הסכם משותף על גבי הפלטפורמה עצמה.
2. השנייה מראה מודל של עיצוב מחדש של ההליך, ע"י ניהול מידע, זיהוי הסכמות ומחלוקות בין הצדדים תוך הבנייה ומיקוד של ההליך.
3. דוגמא נוספת להבניה מחדש של ההליך היא מודל המבוסס על עץ החלטה (אשף פתרון סכסוך) כאשר ישנה סטנדרטיזציה של בעיות ופתרונות אבחון עצמאי, קידום ההליך לפתרון באופן עצמאי – בצורה המותאמת לצרכנים חסרי השכלה משפטית.

מערכת יישוב הסכסוכים של חברת Ebay (דוגמה למנגנון):

כפי שצוין קודם, מדובר במעלה משישים מיליון סכסוכים בשנה בין מוכרים לקונים, עם שווי ממוצע של 100 דולרים לסכסוך. מיותר לציין כי לשם כך ניתן לראות את הצרכים של EBAY כגורם ביניים, במסגרתם ניתן למנות:

1. הבטחת סביבה מסחרית בטוחה ואמינה בכדי לעודד עסקות: צורך בגיבוש פתרון אמין, הוגן, פרקטי ואכיף עבור המשתמשים. בנוסף, דירוג/משוב למוכרים המסייע בהתרעה והכוונת התנהגות – לפני שמערכת יישוב סכסוכים זו פותחה, היה ניסיון של EBAY להסתמך על דירוג של מוכרים וקונים, דבר שיעודד או ירתיע מרקימת עסקות. וכפי שצוין, הייתה קיימת בעיה במחשבה של יתרון סכסוך מסורתי בידי בני אדם, עקב היקף סכסוכים אדיר.
2. קושי בפתרון הסכסוך בעזרת מגשר / בורר אנושי – בהתאם למספרים שצוינו, ברור כי חברה כמו EBAY תצטרך למצוא פתרונות מקוונים עקב יחסי עלות-תועלת בלתי אפשריים בהיקף של 60 מיליון סכסוכים בשנה.
3. עדיפות לגיבוש פתרון הסכמי פנימי, כמעין פתרון לבעיית תחולת ערכאות שיפוט של מדינות שונות.

היתרונות של Ebay כגורם ביניים:

הם השליטה בזירת המסחר והתשלום (PayPal) ומסד הנתונים העצום.

העובדה שיש ל-Ebay שליטה בזירת המסחר והתשלום מקנה לה יכולת אכיפה ובמידה ואדם לא מתנהל לפי הוראותיה ומסרב לפעול לפי דרך יישוב הסכסוכים שלה, הוא פשוט יהיה מנוע מלהמשיך להשתמש בשירותיה.

בנוסף, יש לחברה מסד נתונים עצום על כל הסכסוכים שנולדים במסגרתה, וכך היא יכולה ללמוד על ההיסטוריה של איך נולדים ואיך נפתרים סכסוכים – מה המוכר/הקונה היו צריכים לדעת בכדי להגיע למסקנה. ברגע שיש לחברה מסד נתונים עצום כזה, המערכת יכולה ללמוד על פי לקחי העבר ולפתח תובנות ושיפורים מתמידים.

להליך יישוב הסכסוך ישנם 3 שלבים:

1. אבחון הסכסוך
2. מו"מ / גישור מתווך טכנולוגית
3. גישור / בוררות ע"י נציג החברה

90% מהסכסוכים בEbay- נפתרים ללא מעורבות גורם אנושי מצד החברה (שלב 2).

לאור העובדה כי מדובר במערכת לומדת לאור יתרונותיה של Ebay, הבירור העובדתי נעשה באופן ישיר מתוך המערכת (שכן העסקה מבוצעת על הפלטפורמה), זיהוי דפוסי המחלוקת והמידע הנחוץ לפתרונן ופתרונות שיש סבירות גבוהה לקבלתן – מוכנסים בצורה מותאמת לעצי ההחלטה בתהליך המו"מ.

חששות וסיכונים:

1. הטכנולוגיה אינה ניטרלית. מערכות אלגוריתמיות לוקות בהיעדר שקיפות לגפי אופן פעולת המערכת (ניתוב הסכסוכים, הצעות פשרה) ובהיעדר שקיפות ביחס לתוצאות.
2. בנוסף, ישנו חשש להטיה – הכרעה בלתי שוויונית על סמך שיקולים חיצוניים לסכסוך (כגון שיקולים עסקיים להשאת רווחי החברה), מה שגורם לחשש לפגיעה בשוויון ובצדק.
3. סיפוק המשתמשים מהתהליך אינו מבטיח שהמערכת הוגנת – הנתונים מראים כי גם צדדים שהפסידו בהליך יישוב הסכסוך המערכת יצאו מסופקים מההליך ואמונם במערכת גבר, זאת מבלי לדעת מהם השיקולים שהניעו את המערכת לפעול בצורה שפעלה.

רפורמת ההליכים האזרחיים באנגליה (ביהמ"ש המקוון של הלורד בריגס):

במקביל לצורך להתמודד עם אתגרים משפטיים במערכות המשפט המקובל, עלה הצורך המקוון של הזירה הדיגיטלית לתת מענה מתאים לתחום יישוב הסכסוכים. אחת ההחלטות שהתקבלו הייתה לסגור בתי משפט פיזיים קיימים וליצור מערכת דיגיטלית שתחליף אותם – זאת כמענה לעלויות ליטיגציה רבות, עומס ומשך חיי תיקים ואי נגישות של מערכת המשפט.

קולין רול עוזב את Ebay ומייסד חברת סטאראפ בשם Modria אשר הייתה מעוניינת לקחת את הרעיון שעמד בבסיס חברת Ebay ולהפוך אותו למודל רלוונטי למערכת המשפט. כיום יש שורה של מערכות ומשפט ושל חברות מסחריות, אשר פועלות בצורה של מערכת משפט – בין אם חברות שפועלות בפני עצמן, ובי אם חברות אשר מוכרות את המודל עצמו לבתי המשפט.

המיקוד יהיה ברפורמה של בריגס משום רוחב היריעה שלה, שהוא רחב מאוד. היא היוותה קפיצת מדרגה, אמירה לפיה מעבירים את כל מערכת המשפט האחראית על סכסוכים אזרחיים – לניהול מקוון.

מ-ODR במסחר קוון לנגישות לצדק במערכת המשפט הציבורית:

כיום בישראל יש צוותים רבים בהנהלת בתי המשפט אשר תפקידם לנסות להביא את המודלים הללו למערכת המשפט בישראל. קיימים מספר פתרונות המנגישים את מערכת המשפט הציבורית:

* פתרון עצמאי או באמצעות כלים לשימוש עצמי
* מקורות מידע חיצוניים או סיוע שאינו משפטי
* שוק השירותים המשפטיים הדיגיטליים
* צריכת דירות של גופים ממשלתיים (יחידות משרד המשפטים)
* מנגנונים אלטרנטיביים ליישוב סכסוכים
* שוק עריכת הדין הקלאסי
* מערכת בתי המשפט

בפועל: בסופו של דבר רוב הצרכים המשפטיים של אנשים בחברה לא נפתרים באופן משפטי. אם כך, כיצד יש לפעול מבלי למוטט את מערכת המשפט? לדעת המרצה, יש לחשוב באיזה אופן ניתן לשמן את הגלגלים של המערכת כדי שהחסמים הפרוצדורליים לא יהוו מחסום, תוך מתן מענה תוך זמן סביר ובאיכות גבוהה.

חסמי גישה כלליים למערכת המשפט:

ישנם חסמי גישה כלליים למערכת המשפט, הן מנקודת מבט של המתדיינים ומיצגיהם והן מנקודת המבט של המערכת. גם ללא טכנולוגיה, ישנם חסמים ביניהם חסמים כגון זמן, מקום ומשאבים. נערכת המשפט לא תוכננה עבור בעלי דין שמייצגים את עצמם – בעלי דין לא יודעים לספר את הסיפור שלהם בצורה משפטית. המערכת תוכננה ע"י עורכי דין ועבור עורכי דין – הדין המהותי וסדרי הדין מנוסחים בצורה משפטית, תוך הנחה כי מיש שישתמש בהם יהיו בעלי השכלה משפטית. בפועל, ישנו שיעור גבוה של בעלי דין בלתי מיוצגים. בארה"ב ובאנגליה ישנם סוגי תיקים רבים בהם מעורבים בעיקר מייצגים עצמאיים – תוצאה שנובעת בעיקר מהכלים הרבים שמנסים להנגיש את מערכת המשפט לאזרחים. בישראל אין מספיק נתונים בנושא.

האתגר – בעיית נגישות לצדק:

הן בשל חסמי כניסה, קשיי התמצאות וטעויות בדין מהותי ופרוצדוראלי. בארה"ב ניתן לראות כי בסוגי הליכים מסוימים יותר מ-50% מהתביעות נמחקות על הסף.

שיעורי בית לשבוע הבא:

בהמשך להסבר היום בשיעור, לקראת השיעור הבא אנא השלימו תרגיל קצר להתנסות בשימוש ב-civil resolution tribunal solution explorer. באתר הקורס, תחת יחידת הלימוד של 2.5.2023 תמצאו שני קישורים – הסיפור של סוניה (Sonia's Story) שבוא תיאור מקרה משפטי. בהמשך, היכנסו לקישור "Solution Explore" והשתמשו בממשק האבחון כדי למצוא את הפתרון: כיצד סוניה צריכה לפעול כעת? כתבו לעצמכם את הפתרון אליו הגעתם באמצעות המערכת.

הסיפור של סוניה, civil resolution tribunal:

דמות פיקטיבית שפרסם ביהמ"ש המקוון המצליח הראשון, בקנדה. בסרטון מוצגת פלטפורמה שמראה לה מהן הזכויות שלה וכיצד היא יכולה לדרוש אותן. העזרה ניתנת בניסוח עילת התביעה (/ניסוח עילת ההגנה, במקרים בהם מוגשת תביעה כזו נגד מישהו), באופן ההגשה ובהליך הפרוצדוראלי הנדרש על מנת להשלים את ההליך המשפטי, זאת תוך צירוף ראיות. לאחר מכן, מתנהל משא ומתן ע"י התוכנה, זאת במטרה להגיע להסכמה. הפלטפורמה מאפשרת לדעת האם יש טעם להגיש תביעה והאם קיימת עילה לתבוע בגינה. הצגה של תפיסה אחרת, מערכת משפט אחרת ושונה מהמערכת האזרחית. ההנחה היא כי ניתן לטפל בדברים עוד לפני הגשת התביעה, רק באמצעות מתן מידע והנגשת ההליך לאזרחים.

הייחוד של המודל שלקח את הפעולות של גוגל ותרגם אותם למערכת משפטית הוא הטיפול הנרחב בסוגי תיקים שונים, זאת ללא צמצום לתחום/נושא מסוים. סוג הסכסוכים הכי משמעותי מבחינת היקף אשר מטופל בפלטפורמה הוא תביעות הדומות לתביעות פלת"ד, שהן עד 50,000$ קנדי.

סיכום:

## יתרונות הליכים שיפוטיים מקוונים:

1. דגש על הליכים א-סינכרוניים: מה שמאפשר התגברות על חסמים פיזיים תוך מתן גישה למידע של 24/7 מכל מקום, משפר את איכות ההשתתפות בהליך ומאפשר ניהול משאבי מקום וזמן שיפוטי כאשר העלות התשתית נמוכה.
2. תכנון מחודש של ההליך: ע"י פישוט ומניעת טעויות תוך סיוע בניווט בהליך. ניהול המידע פותח פתח לניתוב ומאפשר ניהול תיקים אוטומטי, מה שמייעל את עבודת בתי המשפט.
3. סיוע משפטי בזמן אמת: מה שמאפשר לאזרח לקבל סיוע בזמן בו הוא זקוק לו ולא לאחר פרק הזמן שדרוש להליכים הפרוצדוראליים.
4. חוויות משתמש שונות: האזרח יכול לחוות דברים בצורה שונה מזו שהיה חווה אם היה פועל באמצעות עו"ד, זאת במקביל לעובדה כי השופט יכול לראות את הדברים אחרת – זאת לאור הצגתם בצורה שונה וללא "תיווך".
5. שילוב כלים אנליטיים אוטומטיים: מה שמתאפשר בזכות הבניית טפסים ושילוב כלי כריית מידע וניתוח נתונים. הצגת סטטיסטיקה תיאורית (התפלגות תוצאות של הליכים בעלי מאפיינים דומים), חיזוי באמצעות AI.
6. כרוך בקושי משמעותי: יצירת הטיות בקבלת החלטות וקושי בביקורת.

שימוש בבינה מלאכותית בבית משפט וזה יתחבר לנושא של שירותים משפטיים מקוונים ונדבר על טכנולוגיות בשימוש בשוק הפרטי וטרם נכנסו למערכות הציבוריות. בכל מקרה של שימוש בבינה מלאכותית זה כרוך בהטיות מסוימות- החלטות בעלי הדין, עורכי הדין, שופטים (שמשתמשים במערכות האלו). בדומה לניתוח שעשינו בקבלת החלטות אלגוריתמיות בנושא של קניין רוחני, גורמי ביניים עושים ניטור- יש פה קושי מובנה בביקורת ובטיפוח, כשאנו מדברים על גורמים ציבוריים, על רשויות מנהל וכו'.

## סיכונים בהליכים שיפוטיים מקוונים:

1. אבטחת מידע, אותנטיקציה ועוד: לדוג' כיצד נוכל לזהות באמת שאותו אדם שמזדהה במרשתת הוא באמת אותו אדם.
2. נגישות לחיבור אינטרנט ונגישות טכנולוגית ככלל: לדוג' מה לגבי אנשים שאין להם אינטרנט בבית? הכיצד יוכלו להגיש תביעות?
3. ניטרליות / מניפולציות בתכנון הליכים (מניפולציה בתכנון ארכיטקטורות בחירה, ממשק המשתמש)
4. צדק פרוצדורלי ואמון הציבור במערכת המשפט: האם ניתן להבטיח צדק בדרך שכזו? האם הליכים שכאלו מכבדים ומעניקים אמון לציבור בדומה לאופן בו בתי המשפט הפיזיים מעניקים?
5. הבטחת פומביות הדיון, עקרון בסיסי במערכת המשפט (נעשו התנסויות בעניין זה בזמן משבר הקורונה): אנו רוצים להבטיח את ביקורת הציבור. יש נושאים רבים שיכולים להעלם אילו יפתרו אך ורק בדי אלגוריתם.
6. צד סוג ב'? האם בשל אי היכולת לקבל את שירות ה"פרימיום" של המערכת מתקבל צדק סוג ב', פחות איכותי? צדק סוג ב' לאנשים הכי מוחלשים, שכן הם אלו שלרוב יפנו להליכים שכאלו.

# חזון ODR בהליכים שיפוטיים בישראל

כיצד ישתלבו הפלטפורמות המקוונות בהליכים השיפוטיים בישראל?

קיימת מערכת נט המשפט, אשר מהווה תשתית טכנולוגית ותרבותית של הגשת טפסים שיפוטיים באופן מקוון, כולל החלטות שופטים שניתנות בצורה מקוונת.

ישראל דיגיטלית – הטמעת טפסים מקוונים במשרד המשפטים.

בנוסף, תקנות סדר הדין האזרחי שונו בשנת 2018, מה שהביא למהפכה בכל הנוגע להסדרים ניהול הליכים אזרחיים בישראל. חלק משמעותי מהתקנות הוא תפיסת ניהול הליך מובנית יותר מאשר בעבר.

כל זאת במקביל לעומס בבתי המשפט ובמטרה להפחית אותו. הדבר מביא לדפוסי ניהול וסיום תיקים, תוך חשיבה לטווח הרחוק ולהמשך.

כל זאת נעשה תוך מחויבות לנגישות הצדק לאזרחים.

## בעיית העומס בבתי המשפט:

ככל שחולפות השנים נפתחים יותר ויותר הליכים בבתי המשפט, זאת ללא שינוי משמעותי בכמות השופטים ובאולמות המשפט – מה שיוצר עיכוב משמעותי בבירור ובהכרעה בתביעות המוגשות לביהמ"ש. בעיה זו קשורה לתופעות נוספות:

1. ריבוי פשרות, רצון של הצדדים לסיים את ההליך מוקדם יותר.
2. המשפט הנמוג, שיעור הולך וקטן של תיקים המגיעים מביהמ"ש לשלב ההוכחות וההכרעה של שופט – קיימים תיקים שנפתחים בביהמ"ש אך הם אינם מבשילים לכדי הליך משפטי מלא.
3. השופט כמנהל, מושג שבארה"ב נטמע קודם לכן ועוסק בשופטים העוסקים בניהול ההליך – החלפת המידע בין הצדדים, ניהול בקשות ביניים של הצדדים. שופטים החלו למלא תפקיד בניהול ההליך ובקידום פשרות במקום להכריע בתיק, זאת במטרה להפחית את כמות התיקים שיבשילו לכדי הליך משפטי מלא וידרשו הכרעה מוחלטת של השופט.

תופעות אלו הן הגדרת הבעיה מחד, ומהוות את הסטנדרט להשוואה מאידך. על רקע דברים אלו, הגיעה הרפורמה בסדר הדין האזרחי – במטרה לפשט את ההליך.

הרפורמה בסדר הדין האזרחי ותפיסת ניהול ההליך:

המטרות המרכזיות:

1. צמצום מספר ההוראות, מניעת עומס קוגניטיבי, הקלה בהתמצאות
2. הסרת חסמים הגורמים להתארכות הדיונים, צמצום השימוש המרובה בניירת
3. לקדם את הגישה לערכאות שיפוטיות, למנוע בזבוז זמן שיפוטי יקר

המטרות המרכזיות שמשרד המשפטים הציב: התמקדות בליבת המחלוקת, ייעול ופישוט ההליכים המשפטיים, קיצור זמנים, מקסימום שקיפות בין הצדדים.. תוך התחשבות בשכבות מוחלשות ובמתדיינים בלתי מיוצגים, עבורם הותאמו כלים מיוחדים".

ניתן לראות כי התקנות סד"א 2018 קיים עידוד החלפת מידע, עידוד גיבוש הסכמות, הבניית פעולות רבות בהליך בטפסים או בהנחיות (הנחיות להגשת כתב תביעה, שאלון לתבוע בגין נזקי גוף), מיסוד של שימוש בכלים טכנולוגיים בניהול ההליך (מסמכים אלקטרוניים, ראיות אלקטרוניות, היוועדות חזותית), שיקול דעת שיפוטי לאפשר שמיעת ראיות בכתב. כל זה מהווה התאמה ליישום באמצעות מערכת מקוונת לניהול ההליך בביהמ"ש.

בתרשים המדגים את אופן סיום הליכים אזרחיים של ביהמ"ש השלום בשנים 2008-2011, ניתן לראות כי רוב התיקים מסתיימים בפשרה (כמעט 50%), בין אם פשרה באישור ביהמ"ש ובין אם פשרה מחוץ לביהמ"ש מה שהוביל למחיקת התביעה. ניתן לראות שיעור לא מבוטל של פסקי דין בהיעדר הגנה – הנתבע לא התגונן. 8% של מחיקה בשל חוסר מעש, 8% של מחיקת הליך לבקשת התובע, ועוד.

מבחינת ההליך והפרוצדורה עצמה, ניתן לראות כי יוצר ממחצית מהתיקים מסתיימים לאחר שהוגש כתב תביעה – זאת מבלי שהוגש כתב הגנה. בערך ב1/3 מהתיקים הצדדים רואים שופט, כאשר בשאר התיקים לא. ניתן לראות כי 40% מהתיקים נערכו בהיעדר מעורבות שיפוטית לאורך כל ההליך.

## הקשר בין מעורבות השופט לבין אופן סיום ההליך:

Chart

Description automatically generated

ניתן לראות כי לו הייתה מעורבות שיפוטית במספר גדול יותר של תיקים, תיקים רבים יותר היו מגיעים לכדי הבשלה/פשרה, ולא היו נסגרים בהיעדר הגנה או במחיקה מחוסר מעש. ההנחה היא לא שיש להפחית במעורבות השיפוטית אלא כיצד יש להשתמד במשאב השיפוטי על פני תיקים רבים יותר ובצורה מועילה יותר.

בהתאם לשאלת צדק סוג ב' – ניתן לראות כי קיימת אפשרות, בשילוב הכלים הטכנולוגיים, לשפר את מה שמערכת המשפט מעניקה לאזרחים שלה, ויש לדעת איך לעשות את זה נכון. אם כך, כיצד תיערך ההבחנה בין תיקים בהם יש צורך בשילוב ODR לבין תיקים בהם עדיפה מעורבות שיפוטית נוכחת?

שיקולים בבחירת הליכים בהם ישולב ODR:

כמות, מורכבות (משפטית, ראייתית, בין-אישית), דפוס ניהול הליך, אופני סיום, בעלי דין טיפוסיים (יחידים / תאגידים / מדינה או לחלופין עצירים / קטינים), ייצוג ופערי כוחות, תחום משפטי ואינטרס ציבורי בקיום דיון פומבי.

## היוועדות חזותית בהליכי המעצר בישראל – מעצרים בזמן הקורונה:

התרת קיום דיונים בהיוועדות חזותית במצב של סגר מלא או הגבלות חלקיות. במרץ עד אוגוסט היו שורה של הסדרים זמניים בתקנות שעת חירום. מחודש אוגוסט ואילך חוק קיום דיונים בהיוועדות חזותית בהשתתפות עצורים, אסירים וכלואים בתקופת התפשטות נגיף הקורונה (הוראת שעה).

מדרג דיונים שיקוימו באופן פיזי ולא בהיוועדות חזותית:

ניתנה עדיפות גבוהה לדיון מעצר ראשון. זה למעט אם העצור ביקש לקיים את הדיון בדרך של היוועדות חזותית או שהדבר לא אפשרי משיקולי מניעת הידבקות / העצור היה בבידוד. עדיפות נמוכה להארכת מעצר ומעצרים עד תום ההליכים שאין בהם טענה מהותית.

מדובר על פיילוט בין השנים 2007 – 2011. מדובר על היוועדות חזותית בהסכמת החשוד / הנאשם, לאחר שנועץ בסנגורו. הפיילוט לא התמשמש כראוי, מכאן בזמן הקורונה הדבר עלה במהירות.

בתקופת הקורונה נושא המעצרים נידון בזום כאלה ואחרים ולא בהליך רגיל. בעניין שכזה עלתה הדילמה – זכות הנוכחות מול נגישות ההליך וצדק פרוצדורלי.

דיון מרחוק משמעותו פגיעה באיכות ההליך (ותוצאותיו) לטובת גישה להליך.

משמע:

הזכות להליך הוגן (כבוד האדם), חסד"פ (מעצרים), אינטרס ציבורי ולגיטימיות.

אלו נגד:

גישה לצדק, כבוד האדם (בגישה לביהמ"ש) – ויתור על נוכחות, עלויות ושיקולי בריאות.

"הסנגוריה ציינה בדוח שהליך הליווי יוצר לעיתים אפקט מצנן אצל העצורים עד כי הם מעדיפים לוותר על זכותם להיות נוכחים בדיון המשפטי בעניינם".

הכיצד עצור יכול לוודא שסנגורו פועל לטובתו ובמיטב המאמצים בעוד איננו נוכח כלל בדיון?

## זכות הנוכחות:

משמעותה של זכות הנוכחות הינה הזדמנות ממשית להשתתף בהליך.

מכאן במקום לשאול ולהתעסק ב"סוג הנוכחות" (פיזית / מקוונת), עלינו להתעסק ב"איכות הנוכחות" (השתתפות).

איכות הנוכחות משמעותה:

1. יכולת העצור להבין את המתרחש בהליך. קשור לעניין הייצוג.
2. יכולת העצור להשפיע על ההליך. קשור לעניין התוצאה.
3. צדק פרוצדורלי (איכות הטיפול מביאה לאיכות ההחלטה). קשור לאמון, ללגיטימיות.

אם העצור נוכח פחות בדיון (משמע בהליך מקוון) אזי העצור מדבר עם סנגורו הרבה פחות. מהן הסיבות?

1. חוסר מודעות לרצון של העצור לתקשר
2. קושי מעשי לתקשר
3. רתיעה מלתקשר בהיעדר פרטיות – שכן אין אפשרות להיוועצות חסויה בין הנאשם לעורך דינו, אם ידברו אז כל ביהמ"ש ישמע את השיחה...

כך גם באינטרקציה בין העצור לשופטת. נשווה:

בדיון מעצר ימים – בנוכחות פיזית 29%, בנוכחות מקוונת 33%.

אך בדיון עד תום ההליכים – בנוכחות פיזית 65%, בנוכחות מקוונת 34%.

## הטענה הסופית:

זה חשוב כיצד ביהמ"ש מעוצב! לעיצוב המרחב תפקיד אינטרינזי בהליך עשיית הצדק וביסוס מראית פני הצדק. האם העצור ממוקם בשולי ההתרחשות או במרכזה? האם קולו מועצם או מושתק?

לטענת המרצה אנחנו צריכים לשנות את עיצוב ההליך לא רק באופן המקוון, אלא גם באופן הפיזי.

## הצעה – בית משפט מבוזר, נוכחות משותפת במרחב המקוון:

כניסת הטכנולוגיה היא הזדמנות לדמיין מחדש את הליך המעצר. מאידאה של נוכחות כ-co location לאידאה של נוכחות כ- co presence. חוויה הדדית ומסוכרנת של תשומת לב, הרגש וההתנהגות של המשתתפים.

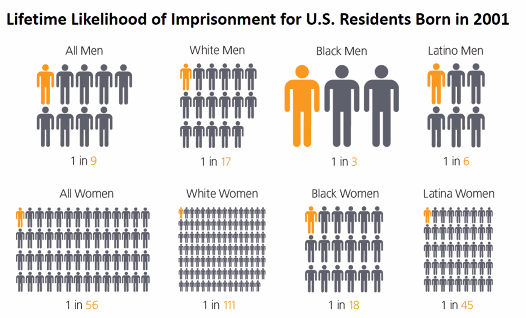
כלל משתתפי הדיון נוכחים במרחב אינטרקציה מקוון משותף, שאליו הם מתחברים ממיקומים פיזיים שונים. כך למעשה נשיג:

1. חוויה הליכית משותפת
2. שוויון בגישה
3. אותות ויזואליים וקוליים עשירים

מדלים אפשריים לבית משפט מבוזר:

1. חיבור מרחוק למערכת היוועדות חזותית – עיצוב ממשק המשתמש משקף תפקידים ומיקומים, מידע על ההליך הזמין, היוועצות חסויה.
2. עמדת מסכים המשקפת את המיקום במרחב וצירי האינטרקציה – מסך עבור כל מששתף.
3. מציאות רבודה (VR) – המשתתפים "נוכחים" כאווטרים בבית משפט וירטואלי באמצעות משקפי VR.

# הגינות אלגוריתמית: מערכות תומכות החלטה בבית המשפט

המרצה מראה תמונה של ג'ורג' פלויד, אדם שחור שנעצר ע"י המשטרה, אשר תוך כדי המעצר השוטר שעצר אותו נתפס במצלמה כשהוא חונק אותו למוות באמצעות הברך שלו. באותה התקופה, נערים ממוצא אפרו-אמריקאי נעצרו פעמים רבות – מה שהביא להקמת תנועת black lives matter, תנועה שקמה נגד הגזענות והיחס המפלה כנגד אוכלוסיות אלו. החשש העומד מאחורי הסיפור הזה או החשש מהטיות שיטתי במערכת המשפט הפלילית – גזענות שיטתית ושלילית של המערכת.

סטטיסטיקה זו מציגה את הפערים בין הקבוצות השונות בעניין מעצרם.

עניין זה אינו קשור רק בנוגע למעצר אלא בנוגע לכל שרשרת האכיפה הפלילית. השאלה האם אלגוריתמים יכולים לפתור את הבעיה היא שאלה בעלת שתי פנים.

אתגר המדיניות: נטרלו הטיות במערכת אכיפת החוק

* נקודת המוצא – היא כי קיימות הטיות גזעניות המשפיעות על פעולות האכיפה ועל החלטות בתי המשפט בתחום הפלילי.
* הנחת העבודה – היא כי מקור ההטיות היא בבני האדם המעורבים בקבלת ההחלטות.
* הפתרון המוצע – הוא ביסוס החלטות על ניתוח אלגוריתמי של המשתנים הרלוונטיים, תוך הוצאת נתונים הקשורים למוצא.
* מקרה הבוחן – שיילקח הוא הערכת הסיכוי שחשוד / נאשם בפלילים יבצע שוב עבירה, על בסיס נתונים נקיים.

בעקבות כך נולדו מערכות שונות, אשר עובדות על מנגנון בו בעל שורה של הטיות אנושיות אפשריות שנכנסות לתוך העיבוד האלגוריתמי, שהן לא בהכרח אובייקטיביות (מתוך ההתבססות על נתונים מהחלטות אנושיות).

תמונה שמכילה טקסט, גופן, לוגו, גרפיקה

התיאור נוצר באופן אוטומטי

אלגוריתם = תהליך המורכב ממערכת הוראות וחוקים, המעבד קלט (נתונים, input) ומוציא פלט (מסקנות / החלטות, output) במטרה לפתור בעיה או קבוצת בעיות.

COMPAS – CORRECTIONAL OFFENDER MANAGEMENT PROFILING FOR ALTERNATIVE SANCTIONS:  
קומפאס זוהי מערכת תומכת החלטה מבוססת חיזוי אלגוריתמי: חיזוי הסיכון הפלילי.

הסיכון שמנסים לחזות הוא בחינת ביצוע עבירה נוספת – המערכת בוחנת מהי ההסתברות שחשוד / נאשם בפלילים ייעצר שוב בחשד שביצע פשע נוסף (בתוך פרק זמן של שנתיים). מערכת זו נמצאת בשימוש בבתי משפט בארה"ב. המערכת נועד לתמוך בהחלטות שופט אם לשחרר נאשם עד להכרעה במשפטו / הגשת כתב אישום או לחילופין לשחררו בערבות / למעצר בית.

## The black box: הקופסה השחורה של מנגנון החיזוי

קומפס היא מערכת המבוססת על מנגנון של קופסא שחורה, העובדת על מנגנוני קלט ופלט:

* קלט – בתוך המערכת קיימים 137 משתנים בנוגע לנאשם, בתוכם תשובות אשר מולאו ע"י הנאשם בשאלון ייעודי ומידע מהתיק הפלילי של הנאשם.
* פלט – הערכת רמת הסיכון של הנאשם, כאשר ההסתברות שייעצר שוב נפלטת בצורה של ציון, בין 1 (נמוך) ל-10 (גבוה).

לחברה היה מאגר מאוד גדול של נתוני עבר, אשר כללו בין היתר פרטים על מה התרחש במידה ואותם החשודים השתחררו ממעצר. האלגוריתם "לומד" / "מתאמן" על נתונים היסטוריים ומזהה מתאם בין גורמים מסוימים לבין ההסתברות שנאשם ייעצר או לא ייעצר שוב; על בסיס נתונים אלו ניתן לבנות מערכת שתבנה דפוסים ותיתן ציון סיכון.

תמונה שמכילה גופן, לוגו, גרפיקה, טקסט

התיאור נוצר באופן אוטומטי

על בסיס המתאם, חוזה האלגוריתם את הסיכוי שנאשם חדש (שלא נכלל בנתונים שנלמדו) ייעצר שוב בגין עבירה בתקופת ההמתנה למשפטו. המודל רץ על הנתונים החדשים של החשוד / נאשם, והמערכת חוזה ביחס לאדם הזה מהו הסיכוי שהדבר יקרה – ומכאן נפלט ציון הסיכון שלו. למשתנים שונים ניתן משקל שונה בציון הכללי.

המערכת למעשה נותנת מספר המשקף הסתברות סטטיסטית לפיה החשוד להיעצר בשנית, בטווח בין 1-10. לעומת זאת, החלטת השופטת היא החלטה בינארית – מעצר / לא מעצר. המשמעות היא שהציון הערכת הסיכון נועד לסייע לשופטת להגיע להחלטה, הוא אינו מחליף את החלטת השופט. קיים חשש לכבילת שיקול הדעת השיפוטי ע"י הציון, שכן השופט יצטרך להצדיק את החלטתו בהתאם לציון הסיכון שניתן / למרות ציון הסיכון שניתן.

המטרה בהכנסת אלגוריתמים הייתה להגביר את הוגנות מערכת המשפט ולשפר את אובייקטיביות מערכת המשפט – החלפת הליך שמושפע מהטיות ואינטואיציות של שופטים / שוטרים (במיוחד הטיות על בסיס גזע / מוצא) בהליך הערכה מדעי אובייקטיבי (לכאורה), זאת ע"י הפחתת אפליה בהליך השחרור בערבות.

האסטרטגיה היא אי הכנסת משתנה של גזע או מוצא לתוך מערכת הקומפס, אלא הזנת נתונים רלוונטיים בלבד.

## שאלות מדיניות העולות משימוש במערכות אלגוריתמיות לצורת הערכת סיכויי פשיעה:

1. המערכת לא מספקת נימוקים להערכת הסיכון המופק, מה שמביא ליכולת פיקוח מוגבלת מאוד על המלצות המערכת.
2. יש צורך לדעת כמה החלטת המערכת מדויקת יותר מהחלטה שהייתה מתקבל ע"י גורמים אנושיים בלבד.
3. יש רצון לדעת האם בסופו של דבר החלטה / המלצה של אלגוריתם הוגנת יותר מהחלטה / המלצה שהייתה ניתנת ע"י שופט אנושי – האם המערכת אכן אינה מוטית נגד שחורים, על אף שעניין גזע / מוצא לא מוזן המערכת.

## כיצד ניתן לדעת האם האלגוריתם הוגן?

על מנת לדעת האם האלגוריתם הוגן יש לדעת מספר דברים: אלו נתונים מותר לאלגוריתם להביא בחשבון, איזו מטרה אנו מעוניינים להשיג באמצעות שימוש באלגוריתם, כיצד ניתן לתכנן / למדוד את מידת ההגינות של אלגוריתם.

נולד מכך אתגר מעשי ורגולטורי – כיצד ניתן לכמת הגינות? מערכות אלו משפיעות על מגוון מאוד גדול של תחומים (מתן קצבאות, זימון לראיונות עבודה, קבלת משכנתא, ועוד). ביחס להרבה מהן, יש רצון לדעת האם הן עובדות באופן הוגן.

השאלה הבסיסית היא האם הערכת הסיכון מדויקת, כאשר שאלת ההמשך היא האם הערכת הסיכון מדויקת עבור כלל הנאשמים / חשודים? קומפס עונה על אלות אלו:

תמונה שמכילה טקסט, עלילה, קו, תרשים

התיאור נוצר באופן אוטומטי

תמונה שמכילה טקסט, צילום מסך, גופן, מספר

התיאור נוצר באופן אוטומטיניתן לראות ע"פ נתונים רשמיים של החברה (בגרף), כי ההתאמה והחיזוי של המערכות כלפי שחורים ולבנים הייתה כמעט מלאה לחלוטין. לפיכך, מתקבל הרושם כי המערכת עובדת וחוזה באופן נכון. הנקודה המרכזית של מבקרי המערכת הזו היא כי לא ניתן להסתכל רק על המדד לפיו מה הסיכוי שאדם ייעצר שוב, אלא עלינו לבדוק את רמת הדיון על פני עוד קטגוריות ולרדת לרזולוציות יותר נמוכות.

## מדידת רמת דיוק של חיזוי רצידיביזם על בסיס ציון הסיכון:

כמובן שכחברה אנו מוטרדים מהזיהוי השגוי, אך אנו לא מוטרדים משתי הקבוצות השמאליות של המעגל באותה הצורה. הקבוצה שתטריד אותנו יותר כחברה היא הקבוצה שקיבלה חיזוי סיכון נמוך מוטעה ונעצר שוב, מאחר ומדובר באדם שחזר לעבריינות והציון לא תאם את מה שעתיד היה לקרות – מה ש"מסכן" את החברה בצורה מסוימת.

למעשה, מה שמגביר את הדיוק הן שתי הטעויות – הטעות שמסכנת את הציבור והטעות שמשאירה אנשים במעצר לשווא. בנוגע לאנשים קיבלו ציון סיכון גבוה מוטעה ונשארו במעצר לשווא – הנושא הטריד אנשים מסוימים ועניין אותם מי האנשים שנשארים באותה משבצת, על מנת לבחון האם אכן מתבצעת הגינות משפטית. עד כמה קומפס טועה אותו הדבר בנוגע לאנשים שחורים ולבנים.

אז מה קרה בפועל?

תמונה שמכילה טקסט, גופן, צילום מסך, לוגו

התיאור נוצר באופן אוטומטיבמחקר שנערך ב-2016 ובדק האם חברת קומפס מוטית גזעית, הממצא האמפירי היה כי מבין הנאשמים שלא נעצרו שוב, ההסתברות של נאשמים שחורים לקבל ציון סיכון גבוה הייתה גבוהה פי 2 מזו של נאשמים לבנים – נאשמים שחורים סובלים מטעות מסוג "זיהוי חיובי שגוי" בשיעור גבוה משל נאשמים לבנים. בקרב נבדקים שבסופו של דבר לא חזרו לפשוע, לנבדקים שחורים היה סיכוי כמעט כפול (42%) מאשר לנבדקים לבנים (22%) לקבל הערכת סיכון בטווח בינוני-גבוה. מכאן יצא, שחברת קומפס אכן מוטית וכי קיימים הבדלים על רקע גזעי.

נציג ויזואלית את המחקר בכדי להבין את המשמעות של "הגינות" בהחלטה האלגוריתמית:

אוכלוסיית המחקר הייתה כל הנאשמים שקיבלו ציון במערכת COMPAS בין השנים 2013-2014 במחוז במדינת פלורידה, ובסך הכול 7,200 נאשמים. נבצע מדגם של 500 נאשמים שנעצרו, אך טרם הורשעו. מהו ציון סיכון גבוה, ומהו הרף הראוי להשארת נאשם במעצר? הרי המערכת מעניקה ציון ולא החלטה בינארית.

הגדרה אפשרית להגינות: מיקום את הרף במקום בו יש לנו 100 אחוזי דיוק.

תמונה שמכילה טקסט, צילום מסך, תרשים, גופן

התיאור נוצר באופן אוטומטי

כיצד נבחר היכן למקד את הרף, בהינתן בו אין לנו נקודת חיזוי מושלמת?

חברת COMPAS הסתפקה ב-93% דיוק והחליטה למקם את הרף בין ציון 6 ל-7. הרף אינו מושלם אף פעם מבחינת דיוק.

* לא ניתן להימנע מהגבלת חירות שלא לצורך: אנשים שנשארו במעצר ולא היו נעצרים שוב בפועל לו היו משוחררים (נקודות ריקות מימין לרף).
* תמונה שמכילה טקסט, צילום מסך, גופן, מקביל

  התיאור נוצר באופן אוטומטילא ניתן להימנע מסיכון הציבור שלא לצורך: נאשמים ששוחררו ובסופו של דבר נעצרו שוב (נקודות מלאות מימין לרף).

אם כך, לאיזה ערך חברתי רצוי לתת יותר משקל (מה עדיף)? ניתן אולי להיעזר באמרתו של השופט וויליאם בלקסטון, משנת 1760, שאמר כי עדיף 10 פושעים משוחררים מאשר חף מפשע אחד שנאסר. הרמב"ם בעצמו אמר כי יותר טוב ויותר רצוי לפטור אלף חוטאים מלהרוג נקי אחד ביום מן הימים.

## מהו אלגוריתם חיזוי הוגן?

1. דין שווה: אותו רף לכל הנאשמים, התייחסות לנאשמים עם אות וציון באופן זהה.
2. מידת דיוק שווה באכיפה: התאמה של שיעור הטעות בין קבוצות – שיעור השגיאות שיעור השגיאות מסוג I (false positive); שיעור השגיאות מסוג II (false negative).

בנוגע לשיעור השגיאות משני הסוגים – שתי ההגדרות אינן יכולות להתממש באותו הזמן.

אם רוצים לתקן גזענות שיטתית במערכת – קומפס לא יספיק, פתרונות המדיניות צריכים להתחיל בשלב מוקדם יותר של התהליך ובצורה רחבה, מאחר ו (1) כרגע קיימת הטיה גם במידע שנכנס למערכת (2) אכיפה משטרתית לא עובדת ע"פ קומפס אך היא כן מכניסה נתונים למערכת.

פעמים רבות הבעיה היא לא בעיה אלגוריתמית אלא בעיה בנציגות, ועל כן יש להבחין מה האלגוריתם יכול לשפר ומה לא – ומה אנחנו צריכים לדעת כדי שנוכל להשתמש בכלים האלו ולהסתמך עליהם.

שיקולים נוספים:

1. הטייה בנתוני בסיס (קלט) => הטייה בחיזוי (פלט).
2. תחת גישת "דין שווה לכל" – בפועל חשודים ונאשמים שחורים נעצרים בשיעור גבוה יותר. שיעור גבוהה יותר בחיזוי מעצר גם. ציון סיכון גבוה יותר (בממוצע), הן מדויק והן שגוי. זו לא בעיה אלגוריתמית אלא זוהי המציאות.

אבל, קשה לבקר ולהשיג על החלטות שהתקבלו ב"קופסא השחורה". מתח זה מתקיים בכל מערכת אוטומטית המקצה משאבים או קובעת עונשים בין קבוצות ש"בחיים האמיתיים" יש ביניהן הבדלים בתוצאות.

# פרטיות בעידן הדיגיטלי

מבוא:

"אנו מפזרים את רסיסי המידע שלנו בכל מקום ובכל פעולה אגב פעולות אחרות, וברוב המקרים בלי לדעת כלל שאנו משאירים אחרינו שובל של מידע ובלי להבין את משמעותו של השובל הזה.. מי שילקט את רסיסי המידע יוכל לשחזר את דמותנו במידה רבה של הצלחה.. אין מדובר בחזון אפוקליפטי רחוק, אלא במציאות חיינו במאה העשרים ואחת" (מיכאל בירנהק, "מרחב פרטי: הזכאות לפרטיות בין משפט וטכנולוגיה").

בעידן הדיגיטלי, כל פעולה במרחב הדיגיטלי מייצרת מידע. קיימות אפשרויות טכנולוגיות רבות לאיסוף, עיבוד והפצה של מידע על אנשים – בקלות ובמחיר נמוך יחסית, ויכול להתבצע ע"י שחקנים רבים שמעורבים בפעילות.

חוק הגנת הפרטיות:

בתחילת הדרך המחשבה על הגנת הפרטיות החלה כמגננה של האזרחים מפני שלטון, ממחשבה על גורמים פנים -מדינתיים שאוספים מידע על האזרחים בכדי לשמר את השלטון, תוך מניעת ביטוי של האזרחים.

כיום המידע הפך להיות משאב כלכלי משמעותי ומרכזי, מעין מודל עסקי חדש – כאשר המוצר הוא המשתמשים (אם אינך משלם, אתה המוצר). כל פעולה מייצרת מידע שניתן לאגור ולעבד, לא רק ע"י הרשתות החברתיות וזירות המסחר אל ע"י כל נתון אישי שמוזן לרשת. מחקרים מראים כי ניתוח לייקים ושיתופים בפייסבוק מביאים ליצירת פרופיל אישי ברמה גבוהה יותר מאשר תיאור ע"י המעגלים הקרובים שלנו.

הנטייה היא לחשוב כי שובל המידע מסתכם במחשב ובפלאפון, כאשר למעשה שובל המידע רחב הרבה יותר – מערכות אבטחה, זיהוי ביומטרי בכניסה למקומות, קנייה בכרטיסי אשראי/מועדון, הזדהות בצ'יפ – כל אלו מהווים חלק מאיסוף המידע הכולל.

הטענה היא שכיום המציאות היא מציאות של מעקב מידע ומעקב המונים:

* מעקב רב ממדי – חזותי, גיאוגרפי, ביומטרי, מדעי
* המעקב נעשה לעיתים ע"י המדינה או ע"י תאגידים
* המידע שנאסף הוא סחיר
* ישנו חיבור של המידע הנמצא בידי המדינה לבין המידע הנמצא בידי גורמים פרטיים. לדוג' וויז הייתה מערבת את המשטרה על כל נהג שמשתמש באפליקציה שעובר את המהירות.

## דוגמאות להשלכות וסיכונים משמעותיים:

1. פרופיילינג לצרכי שיווק ברשת:

TARGET , אחת האוכלוסיות הרוכשות עם פוטנציאל רכישה גבוה הן נשים בהיריון. עם זאת, מדובר במידע רגיש ופרטי. מחלקת השיווק של רשת TARGET ניסתה לבחון כיצד ניתן לגלות במועד מוקדם את היותן של הנשים בהיריון והחליטו לבחון את היסטוריית הרכישה של נשים שהתברר לבסוף שהן בהיריון, והחלו לנתח מידע זה. לבסוף, הם זיהו מוצרים מסוימים ודפוסי רכישה בקרב נשים אלו. כך הם הגיעו לאיזה שהוא מודל לפיו ניתן לאבחן האם אישה בהיריון או לא, כל זאת בכדי לשווק עבורן מוצרים שייתכן שהן היו רוכשות גם כן. הדבר התגלה כאשר יום אחד אב הגיע הביתה וראה מכתב מרשת TARGET הממוען לביתו הנערה שהכיל מבצעים על היריון. האב הזועם ניגש אל הרשת הקרובה ומחלקת השיווק אמרה כי היא הבינה כי מדובר באישה בהיריון, וכך האב גילה כי ביתו בהיריון, לפני שהיא סיפרה לו בעצמה. מדובר בדוגמה אחת, אך זו ממחישה תופעות רחבות בהרבה.

1. ביטוח מבוסס פרופיילינג:

האפשרות כי ביטוח אדם יתבסס על ההתנהלות, הצרכנות וסגנון החיים שלו. ניתן לראות דוגמה לכך גם בחיפוש אחר עבודה, שכן מראיינים רבים היו מבצעים מעקב אחרי עובדים פוטנציאליים ברשתות החברתיות. הבנה זו הובילה לכך שאנשים רבים, בעיקר סטודנטים לקראת סוף התואר וחיפוש עבודה החלו לשנות את הרגלי השימוש שלהם ברשתות החברתיות בכדי לא לפגוע בסיכוייהם למצוא עבודה.

1. דירוג/אשראי חברתי בסין:

איסוף סך הפעולות שאדם עושה במרחב הציבורי והפרטי מול החברות ומול המדינה ולייצר פרופיל אודות האדם ולהתנות את הזכאות של אותו אדם לשירותים מהמדינה או להתקדמות בחייו על בסיס ההתנהגות שלו. איסוף המידע נעשה בתחומים רבים – מעבר חצייה באור אדום, רכישת אלכוהול רבה וכו'.

1. עוד ועוד ועוד:

הבית החכם, טכנולוגיה לבישה, האינטרנט של הדברים - איסוף מידע מהמרחב הפיזי הפרטי – כל אלה מסייעים לחיינו מאוד אך במקביל אוספים מידע אודות שגרת חיינו במרחב הפרטי ביותר שלנו- המבצר הפרטי שלנו, אשר בדרך כלל נותן לנו את התחושה של ההגנה המירבית. הטכנולוגיה יודעת מה קצב הלב שלנו, כמה פעמים ישנו עם מזגן דולק, מקרר חכם יכול לפגוע בפרטיות שלנו כי הוא רואה איזה מוצרים אנו קונים- למשל אם המקרר רואה שקנינו דברים בכשרות בד"ץ, אז יידעו עליי שאני דתיה. אם אני קונה הרבה יין, אז חברות הביטוח יידעו על זה ויעדכנו את המחיר של פרמיות ביטוח הבריאות שלי.

נניח אני מועמד לעבודה ולא רשאים לשאול אותי אם יש לי בבית ילדים קטנים רבים שעשויים להפריע לשגרת העבודה שלי, אך ניתן לאסוף מידע זה על בסיס הרכישות שלי – מזון לתינוקות, טיטולים ואפשר לראות לפי הכמויות כמה ילדים יש לי – כל אלו יוצרים את הפרופיל המשפחתי שלי.

## פנאופטיקון – ג'רמי בנת'הם ומישל פוקו:

מישל פוקו וג'רמי בנת'הם יצרו את המושג פנאופטיקון, כאשר ניסו ליצור מעין בית כלא אולטימטיבי. בית הכלא הינו מבנה מעגלי הכולל חלון כלפי פנים וחלון כלפי חוץ, ומאפשר לסוהר אחד בכל קומה לצפות על כולם ולתת לכל האסירים את התחושה שהם תמיד במעקב. טענתם היא כי התנהגותם של האסירים תושפע מתוך ידיעה זו, הם ניסו להוכיח את הכוח "הממשמע והממשטר", לפיו הידיעה כי יש מי שצופה בהתנהגות מהווה מעין גורם ממשמע.

מה אנחנו עושים בנושא?

חרף כל המידע שהצגנו עד כה בכל זאת אנו משתמשים בטכנולוגיה- וויז, רשתות חברתיות וכו'. האם קיימת אצלנו אשליה של פרטיות, או שאולי כבר לא אכפת לנו? ייתכן כי אנשים מסכימים לעסקה הזו – אנו נהנה מכל האפשרויות וההטבות של החיים הדיגיטליים ואנו מוכנים תמורת זה לוותר על הפרטיות. עם זאת, עדיין קיימת מעין אשליה של פרטיות. ייתכן כי הנורמות החברתיות השתנו, הן בסביבה הדיגיטלית והן בסביבה הפיזית, בכל הנוגע לתפיסת הפרטיות. ההטבות הניתנות בעולם הדיגיטלית הן גורם משמעותי בשינוי תפיסת הפרטיות.

"כל אחת מאיתנו זקוקה למרחב פרטי, וכל אחד צריך מקום פרטי שבו אפשר לתהות, להתנסות, לחשוב ולהתבטא, וגם לטעות, בלי מעקב ממשטר וממשמע... ללא צורך להצטדק ולהסביר את עצמנו... מרחב שבו אנחנו יכולים להיות עצמנו..." (מיכאל בירנהק, "פרטיות: תמונת מצב")

היחס בין פרטיות לטכנולוגיה: מקרה פרטי של הקשר בין משפט, טכנולוגיה, השוק והנורמות החברתיות:

תמונה שמכילה טקסט, צילום מסך, תרשים, תוכנה

התיאור נוצר באופן אוטומטיזכרו את מודל לסיג – השפעה הדדית. תפישות חברתית של פרטיות הן חלק מהעניין. כך גם הזכות המשפטית לפרטיות, הטכנולוגיה והשוק.

למבחן! עליי להכיר היטב את מודל זה. לטענתה יהיה נתון מקרה, ועלינו יהיה לנתח הכיצד המשפט יכול להשפיע, כיצד השוק יכול להשפיע, כיצד הנורמות וכו'.

טכנולוגיה היא איננה בהכרח רעה או טובה.

טכנולוגיות "לא טובות" של מעקב:

* + עקבות דיגיטליות, אמצעי זיהוי ביומטריים, איכון גיאוגרפי, אמצעי ציתות מתוחכמים;
  + אמצעי מעקב והעברת מידע לאחרים, אמצעים לעיבוד מידע ולתיעוד.

גם זאת, יש גם טכנולוגיות "טובות" של פרטיות (PET- PRIVACY ENHANCING TECHNOLOGIES):

* + טכנולוגיות הצפנה, אבטחת מידע, מנעולים דיגיטליים, אמצעי טשטוש עקבות (טכנולוגיות אנונימיות – למשל);
  + מבטיחות שליטה של בעל התוכן על הגישה אליו.

## צירים לדיון בפרטיות בעידן הדיגיטלי:

* הזכות לפרטיות כמושג משפטי שנמצא במשא ומתן מתמשך עם נורמות חברתיות ועם הטכנולוגיה.
* הגנת מידע ביחסים מול המדינה, מול השוק, ומול שניהם גם יחד.
* קריסת הנחות אנלוגיות שאינן מתאימות לסביבה הדיגיטלית ולחיים בימים אלו.
* הבנת הפרטיות במונחים של שליטת האדם על האוטונומיה האישית. הכוח של אדם לקבוע מתי יימסר מידע אודותיו, למי ובאילו תנאים?
* הקשר בין פרטיות לבין זכויות אחרות.

המידע שלנו הוא למעשה אנחנו עצמנו!

## מהי פרטיות?

פרטיות הינה גם זכות משפטית, אך לא רק, היא גם נורמה חברתית.

הזכות המשפטית למעשה אוסרת על האחר לפגוע בצנעת חייו של אחר. לדוג' קריאת מכתבים סגורים, האזנה לשיחות, צילום ברשות היחיד.

בנוסף היא מגנה על סוגים שונים של מידע – כגון מידע רגיש (לדוג' מסמכים רפואיים) ומידע "רגיל" (לדוג' הרגלי צריכה או גלישה באינטרנט).

מקנה לנו אמצעים למנוע הטרדה, עוגמת נפש, או מסחור של דמותנו.

## הזכות לפרטיות כ-"זכות להיעזב במנוחה" (וורן ובנדייס, 1890 – "The right to be let alone"):

למעשה שם טענו כי החוקה האמריקאית איננה מזכירה את הזכות לפרטיות. סעיפים שונים בחוקה פורשו ע"י ביהמ"ש העליון כמגנים על הפרטיות.

וורן וברנדיס – הזכות לפרטיות קיימת בדין, במובן של זכותו של אדם לשלוט על פרטים על אודותיו ובאישיותו (אך ישנם גורמים שיכולים להגבילה).

למעשה היא יוצרת תנאי "סביל" לפרטיות – אי התערבות במרחב האוטונומי של הפרט.

האם הגדרה זו מתאימה לעידן הדיגיטלי? לא! אין זה מספיק שלא יתערבו.

## הזכות לפרטיות כיכולת שליטה (אלן ווינשטיין 1967):

לפיו היכולת של אדם לקבוע בעצמו, ולמען עצמו, איזה מידע על אודותיו לשתף עם אחרים, מתי, באילו תנאים ולאילו מטרות.

גישה פעילה – שכן היא מהווה ליצירת כלים שיאפשרו לאדם לשלוט ב-"יחידה האוטונומית" שלו, למעשה במידע שלו. למעשה כללים קונקרטיים לדוג' "עקרון ההסכמה" ו-"עקרון צמידות המטרה".

גישה רחבה – תחולה אפשרית על סוגים רחבים יותר של מידע.

משבר הגנת המידע (והפרטיות) בעידן הדיגיטלי:

המהפכה הדיגיטלית, ועמה גם מהפכת הסלולר הביאו ליצירת מידע תוצר של הפעילות האנושית. משמע איסוף מידע בכמויות עצומות, ממגוון מקורות וסוגים. מידע זה נשמר לזמן רב מאוד. ניתן בעזרתו ועמו לבצע כריית, ניתוח והצלבת מידע מובילה למידע מזהה ומהותי.

## האם ניתן לפעול באנונימיות "אמיתית"?

הנחת האנונימיות המאותגרת, היא הבסיס של לערעור עקרונות הגנת המידע.

בפועל, כיום ניתן לשחזר זהות גם מתוך מידע אנונימי.

ישנו מקום לשקול מחדש הבחנות בין סוגים שונים מידע:

* מזוהה / אנונימי
* פרטי / פומבי
* רגיש / לא רגיש

להיפרד מרעיון ההגנה על מידע מזהה ופרטי בלבד.

"מידע אישי" – personal data, private information, private facts.

לפני כן אמרנו כי עקרון הפרטיות הינו שליטה של אדם במידע לגביו. העניין מעורר קושי, שכן קשה להצהיר מראש מה ייעשה עם המידע הזה בעתיד. גורמי איסוף המידע לא יודעים מה יעשו איתו ולמי בסוף ימכרו אותו. מכאן הם לרוב ישתמשו בניסוח מעורפל ("אנו חולקים את המידע עם שותפינו העסקיים").

קשה לבחון "צמידות מטרה" (העברת מידע לצורך מטרה מסוימת).

## האם אנחנו שולטים במידע שלנו?

למרות הרצון שנשלוט במידע, משטר ההגנה נשען על הסכמה, ובפועל היא רוקנה מתוכן – מרבית האנשים לא קוראים את מדיניות הפרטיות שנלווית ליישומים באינטרנט. ממצאי מחקרים מראים חד משמעית שההסכמה הניתנת אינה מספקת את תכלית השליטה של הפרט והאוטונומיה שלו.

אל מול אתגרים אלו מגיע המחוקק הישראלי.

# מאגרי מידע בדין הישראלי

הגישה הישראלית היא גישה שמצהירה על זכות לפרטיות שמשתרעת גם על פרטיות במידע + הגישה מצרפת לזכות זו איזשהו מבחן תוכני שאומר על איזה מידע יש הגנה.

אבל, ההגנה המשפטית על מידע תלויה בשני תנאים:

1. המידע מזהה את האדם.
2. המידע משתייך לסוגי מידע מסוימים שהוגדרו כפרטיים (אמת מידה תוכנית).

נותר לתנאים אלו מרחב לפרשנות והרחבה פסיקתית.

ההסדר המשפטי:

## זכות חוקתית לפרטיות – ס'7 לחוק יסוד כבוד האדם וחירותו:

(א) כל אדם זכאי לפרטיות ולצנעת חייו. => ללא הגדרה

(ב) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו. => פרטיות במקומות

(ג) אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו. => פרטיות בגוף

(ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו. => פרטיות בתקשורת

הגנה רחבה על פרטיות – ס'2 לחוק הגנת הפרטיות:

פגיעה בפרטיות היא אחת מאלה:

(1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת;

(2) האזנה האסורה על פי חוק;

(3) צילום אדם כשהוא ברשות היחיד:

(4) פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו;

ועוד ועוד...

אנחנו יותר נתמקד בסעיפים 2(9) ו-2(11):

(9) שימוש בידיעה על עניניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;

(11) פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד.

כפי שניתן לראות, החוק נותן הגנה לתוכן של התקשורת (אסור להאזין לשיחה), אך אין התייחסות לנתוני התקשורת.

כלומר, כאשר לא מדובר במה נכתב באימייל ששלחתי, אלא מה כתובת האימייל שלי. למה בעידן הדיגיטלי הגנה על אמצעי תקשורת חשובה? כי ניתן ללמוד עלינו אפילו מלהסתכל לטלפון של איזה רופא התקשרתי. זה כבר חושף מידע רגיש עליי.

הגנה רחבה למדי על פרטיות במידע:

* פרק ב' לחוק הגנת הפרטיות (הסדר מפורש של מאגרי מידע).
* פרק ד' לחוק הגנת הפרטיות (הסדר להעברת מידע בין גופים ציבוריים).
* תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (חובות אבטחת מידע על בעלים / מנהלים / מעבדים של מאגרי מידע אישי).

כפי שניתן לראות, אין אמירה מפורשת של זכות לפרטיות במידע. אך הפרשנות היא לאור מגמות במשפט הישראלי. יש פעולות של הרשות המבצעת – הרשות להגנת הפרטיות, רשם מאגרי המידע, שדרכם ניתן להבין שיש סוג של זכות לפרטיות במידע.

פגיעה בפרטיות "מידע" באשר הוא (דיגיטלי או אחר):

סעיף 2 מתייחס לפגיעה בפרטיות ב"מידע" בכל מיני אופנים:

* הפרת חובת סודיות בנוגע ל"ענייניו הפרטיים של אדם", בין אם נקבעה בדין (סיפא 7) או בין אם בהסכם (סיפא 8).
* שימוש / מסירה לאחר של ידיעה על ענייניו הפרטיים של אדם למטרה אחרת מזו שלשמה נמסרה (סיפא 9).
* פרסום מידע ביחס ל"צנעת חייו האישיים של אדם", עברו הרפואי או המיני, התנהגותו ברשות היחיד (סיפא 11).

כיצד נקבע אם מידע מסוים זכאי להגנה משפטית כמידע פרטי של אדם?

המונח "ענייניו הפרטיים של אדם" איננו מוגדר בחוק.

הפסיקה קבעה אמת מידה תוכנית, שהוא קובע אם מדובר במידע שפוגע בפרטיות או שאינו.

בארץ ישנה גישה צרה יותר מאשר באירופה, ורחבה יותר מאשר בארה"ב.

בחינת האם מדובר ב"ענייניו הפרטיים של אדם":

מדובר במבחן תוכני.

פס"ד התנועה לחופש המידע נ' רשות החברות הממשלתיות: נפסק כי "את תוכנו של הביטוי 'ענייניו הפרטיים של אדם' יש לצקת בכל מקרה בהתאם למכלול הנתונים הרלוונטיים, ותוך מחויבות להגנה על יכולתו של האדם לקיים את האוטונומיה שלו ואת המרחב הפרטי הנתון לו".

פס"ד רשם מאגרי המידע נ' ונטורה (השופטת שטרסברג – כהן): מציפה תובנה הצופה פני עתיד. לפיה יתכנו מקרים בהם כל פרט בנפרד אינו בהכרח "עניין פרטי" אולם צירוף פרטים יחד עשוי להיות עניין פרטי מוגן.

עניינים פרטיים של אדם מהפסיקה:

* כתובתו של אדם (פס"ד רוזנברג נ' רשות האכיפה והגבייה).
* מס' הטלפון הנייד של אדם (פס"ד הר שמש נ' הממונה על חוק חופש המידע ברשות המיסים).
* מס' כרטיס האשראי של אדם (פס"ד ינוסוב נ' פלאפון תקשורת בע"מ).
* יומן שיחות פרטיות של אדם (פס"ד דרוקר נ' הממונה על יישום חוק חופש המידע במשרד ראש הממשלה).
* פסילת מועמדותו של אדם כמועמד למשרה (פס"ד התנועה לחופש המידע נ' רשות החברות הממשלתיות).

הסדר ספציפי למאגרי מידע – פרק ב' ו-ד' לחוק הגנת הפרטיות:

מידע ששמור באופן ממוחשב הינו מאגר מידע.

מטרות העל של ההסדרים הללו:

1. להגן על פרטיות נושאי המידע.
2. לצמצם את הסיכונים לפרטיות הנובעים מאיסוף ועיבוד מידע אישי.
3. להעניק הגנות ספציפיות לנתוני מידע ולמידע רגיש.

האמצעים:

1. הטלת חובות על בעל מאגר מידע.
2. הטלת חובות על מי שמנהל / מחזיק / מעבד מאגר מידע.
3. הענקת זכויות לנושא המידע ש"המידע" אודותיו מוחזק במאגר.

היבטים נוספים להן לא נתייחס:

1. דיוור ישיר
2. הגבלת מסירת מידע מגופים ציבוריים וביניהם

ועוד..

הגדרת "מאגר מידע" – סעיף 7 לחוק:

"מאגר מידע" – אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –

(1) אוסף לשימוש אישי שאינו למטרות עסק; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

נתוני מידע – כל עוד לא מדובר על נתון מידע, לא חל החובות שבפרק. חובות אלו חלים על נתוני מידע.

המשך הגדרות – סעיף 7:

"מידע":

נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמנותיו.

"מידע רגיש":

1. נתונים על אישיותו של אדם, צנעת אישיותו, מצבו הבריאותי, מצבו הכלכלי, דעותיו ואמונותיו;
2. מידע ששר המשפטים קבע בצו, באישור ועדת החוקה, חוק ומשפט של הכנסת, שהוא מידע רגיש;

מידע VS מידע רגיש:

ניתן לראות כי מידע על "מעמדו האישי" ו-"הכשרתו המקצועית" אינם מוגדרים כ-"מידע רגיש".

על פי הפסיקה, כל מידע מהווה גם ידיעה על ענייניו הפרטיים של אדם כמובנה בחוק. אבל לא כל ידיעה על ענייניו הפרטיים של אדם היא מידע כמובנו בחוק.

דוגמאות לתוכן שיצקו בתי המשפט למונח "מידע":

* מעמדו האישי – נשוי, רווק, אלמן, יתום מהוריו.
* צנעת אישיותו – התנהגות הרשות היחיד, נטייה מינית.
* מצבו הבריאותי – מידע גנטי, מידע רפואי, מידע על מצבו הנפשי של אדם.
* מצבו הכלכלי – נכסים, חובות, התחייבויות כלכליות (בנוסף גם מידת העמידה בהן), ירושה, צו, צו עיקול, השתכרות, מידע בנקאי..
* דעותיו ואמונותיו – תפיסת עולם, דעה פוליטית או אמונה דתית של אדם.
* אישיותו של אדם – מונח סל, פרט אישי מסוים שאינו נכלל בקטגוריות הנ"ל. לדוג' עבר פלילי, מוצא, מידע שמקורו במבחני ההתאמה לעבודה.
* וגם: נתוני מיקום, נתוני תקשורת, נתוני הרגלי צריכה – שיש בהם כדי ללמד על הנ"ל.

לא רק מידע מזוהה ומידע שניתן לזיהוי באמצעים סבירים, אלא גם "מידע אנונימי" עשוי להיחשב "מידע" המוגן בפרק ב' לחוק הגנת הפרטיות.

מידע שמוצג באופן אנונימי אך מאפשר לבסס קשר לאדם ספציפי:

פס"ד גוטסמן אדריכלות בע"מ נ' ורדי: "די בכך שניתן לקשור, באמצעים כלשהם, בין המידע לבין אדם ספציפי על דרך ביצוע של 'הנדסה חוזרת'".

פס"ד עמותת חברות הסיעוד נ' משרד הבטחון: "באמצעות ממצאים ונתונים אחרים המאפשרים להסיק מיהו [האדם]... יש לומר כי המידע היה מזוהה מלכתחילה".

נתון מידע שיכול לשמש "מפתח" לזיהוי אדם או לגישה למידע אודותיו:

1. מספר ת"ז (בג"ץ מנאע נ' רשות המיסים).
2. אפיון ביומטרי (פס"ד הסתדרות העובדים נ' עיריית קלנסווה).

# חובות שחלות על מנהל מאגר מידע

# רישום מאגר

"מנהל מאגר" – הינו מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע, או מי שמנהל כאמור הסמיכו לעניין זה (מתוך סעיף 7).

סעיף 8(א): קובע כי הדבר הראשון שעל מנהל מאגר לעשות הוא חובת רישום מאגר אצל רשם מאגרי המידע, באחד מהמקרים המנויים בסעיף 8(ג):

1. מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;
2. יש במאגר "מידע רגיש";
3. המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;
4. המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;
5. המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17(ג).

\*כיום ההערכה היא כי רק 2% ממאגרי המידע הקיימים רשומים.

הרעיון שעמד מאחורי חובת הרישום, הוא שפקח מאגרי המידע יוכל לפקח עליהם.

מדוע יש חובת רישום מאגר?

פיקוח מהותי:

* + סירוב לרשום מאגר למטרה בלתי חוקית (סעיף 10(א)(1)).
  + שינוי מטרת המאגר המוצהרת לפי בדיקה של פעילות המאגר בפועל (סעיף 10(א)(2)).

פיקוח על הפעילות – מופנה למגזרים, לא רק למאגרים ספציפיים.

הנחה התנהגותית – חובת הרישום גוררת בדיקה ופיקוח פנימיים אצל מנהלי המאגרים שמוביל להגברת הציות לחוק.

סעיף 11- חובת מבקש מידע: (חובת מנהל מאגר-הודעה):

11. פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצויינו בה-

1. אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו והסכמתו (עקרון ההסכמה);
2. המטרה שלמשה מבוקש המידע (עקרון צמידות המטרה);
3. למי יימסר המידע ומטרות המסירה (עקרון צמידות המטרה).

גילוי דעת הרשות להגנת הפרטיות – הסכמה מדעת כאשר עיבוד המידע נערך באמצעות מערכות אוטומטיות: "על הליך היידוע לפרט על אופן פעולת המערכות האמורות, ככל שהדבר רלוונטי לגיבוש ההסכמה וככל שפירוט זה אפשרי מבחינה משפטית, טכנולוגית ומסחרית".

מהי חשיבות "חובת ההודעה"? (תפישת "הפרטיות כשליטה"):

* בסיס לקבלת הסכמה מדעת של מושא המידע;
* סעיף 3 מגדיר הסכמה "מדעת, במפורש או מכללא".
* בסיס להפעלת עיקרון צמידות המטרה:
  + סעיף 2(9)- "שימוש ביודעין על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה";
  + סעיף 8(ב)- "לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר".
  + סעיף 11(2): "המטרה אשר לשמה מבוקש המידע".

עם זאת, לא מדובר בנוהל מושלם:

* היעדר דרישות צורה ל"הודעה" (לעומת פרשנות חוזה צרכני, דיני הגנת הצרכן וכו').
* החובה לא מתייחסת לכל זכויות מושאי המידע (לעומת ה-GDPR):
  + הזכות לגשת למידע, לעיין בו, לדרוש את תיקונו.

גילוי דעת הרשות להגנת הפרטיות – "היידוע צריך להיות בשפה ברורה, פשוטה ונגישה, להינתן בד בבד עם הפניה לאדם".

הסכמי פרטיות והסכמי שימוש ממלאים תפקיד הסדרה:

* קובעים את פרקטיקות האיסוף, העיבוד והשיתוף הנתונים של היישומים;
* מממשים "על הנייר" את פרדיגמת ההסכמה, כאשר המשתמשים מאשרים את:
  + סוג המידע שייאסף;
  + השימושים במידע;
  + חלוקת המידע;
  + שמירת/אחסנת המידע.
* ישנה חשיבות גדולה מאוד לתוכן, למבנה ולשפה של הסכמים אלו- המצב כיום בעייתי!

מה ההבדל בין מנהל מאגר מידע לעומת מי שמעבד מידע ללא שמירתו?

הבעייתיות בהסדר:

ישנו היעדר דרישות צורה להודעה. בנוסף, החובה לא מתייחסת לכל זכויות מושאי המידע (הזכות לגשת למידע, לעיין בו, לדרוש את תיקונו).

הסכמי פרטיות והסכמי שימוש ממלאים תפקיד אסדרה:

הסכמים אלו קובעים פרקטיקות איסוף, עיבוד, שיתוף הנתונים של אפליקציות. בנוסף, הם מממשים על הנייר את פרדיגמת ההסכמה, כאשר המשתמשים את סוג המידע שנאסף, השימושים במידע, חלוקת המידע, שמירת/אחסון המידע. קיימת חשיבות גודלה לתוכן, למבנה ושלפה של ההסכמים הללו.

בפועל: משתמשים חותמים מבלי לקרוא.

משתמשים נותנים הסכמתם באופן כמעט אוטומטי. מדובר על כמות רבה מאוד של הסדרים – ארוכים, מורכבים ונכתבים בשפה משפטית. אסטרטגיות לפישוט הטקסט לא הובילו לשינוי משמעותי. בטלפונים ניידים תשומת הלב של משתמשים נמוכה עוד יותר. מכאן האם "מותה של פרדיגמת ההסכמה" הגיע?

כלים / זכויות שמקנה החוק למושא המידע:

כלים המאפשרים את המשך שליטת המושא במידע.

* סעיף 13: זכות לעיין במידע שמוחזק אצל אחרים. עם זאת, חובת ההודעה אינה כוללת יידוע בדבר הזכות לעיין במידע. תוצרי עיבוד המידע (פרופיילינג) אינם כלולים בזכות העיון או התיקון.
* סעיף 14: זכות לדרוש את תיקון המידע. כאשר מידע אינו נכון, שלום או מעודכן, אם בעל המאגר מסרב לתקן – קמה זכות תביעה (ס'15).
* סמכויות אכיפה: לאזרחים סעיף 31 לחוק הגנת הפרטיות; לרשות ייעודית סעיף 10 לחוק הגנת הפרטיות. הרשות היא רשם מאגרי המידע במשרד המשפטים.

פגיעה בפרטיות: עוולה אזרחית, עבירה פלילית

שימוש בידיעה על ענייניו האישיים של אדם, שלא למטרה לשמה נסמר המידע מאת נושא המידע – הפרה של סעיף 2(9) לחוק הגנת הפרטיות.

עבירה על ס'4 תהווה עוולה אזרחית, ומשכך יחולו הוראות פקודת הנזיקין;

עבירה על ס'5 תהווה עבירה פלילית – הפוגע במזיד בפרטי זולתו, באחת הדרכים האמורות בסעיף 2(1), (3) עד (7) ו-(9) עד (11) – דינו מאסר 5 שנים (חוק העונשין).

פיצוי נזיקי למושאי המידע בגין הפרת הוראות החוק:

עוולה בנזיקין, ס'31ב: מעשה או מחדל בניגוד להוראות פרקים ב' או ד' או בניגוד לתקנות יהווה עוולה לפי פקודת הנזיקין. למשל, מנהל מאגר מיגע שהתרשל בחובת סודיות או באבטחת מידע, חב בנזיקין כלפי מושא מידע שנפגע. הקושי הוא שלפי דיני הנזיקין נדרש להוכיח נזק, רף שקשה לעמוד בו, מה שיכול להקשות על ההליך.

ביהמ"ש אף מוסמך לפסוק פיצוי ללא הוכחת נזק (עד 50,000 ₪), ס'29א, הן במקרה של הרשעה בעבירה לפי ס'5 (סעיף קטן א) והן במקרה של עוולה אזרחית ע"פ ס'4. אך זה חל על פרק א' לחוק ולא על פרק ב'.

חובות סודיות ואבטחת מידע:

סעיף 16 – חובת סודיות:

לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי.

סעיף 17 – חובת אבטחת מידע:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017:

תקנות אלו נכנסו לתוקף בשנת 2018. תקנות אלה מפרטות את אופן יישום חובת בטחת מידע שבסעיף 17 לחוק הגנת הפרקטיות.

הרעיון הכללי הוא שתקנות אלו מודולריות, ויוצרות ארבעה סוגים של מאגרי מידע, המשתנות בהתאם לרמת הסיכון שהמאגר משקף.

תקנות מודולריות – הסדרים ביחס לארבעה סוגי מאגרי מידע:

חובות ברמה הולכת וגוברת על ארבעה סוגי מאגרים – ככל שפעילות עיבוד המידע בארגון משמעותית יותר. לדוג' כאשר המאגר מכיל מידע רגיש / מידע על אנשים רבים ומטרת המאגר היא מסירת מידע לאחרים.

ככל שמדובר במידע רגיש יותר – לדוג' מידע רפואי, עמדות פוליטיות, אמונה דתית, מידע כלכלי וכו'. בפועל גם הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע כנ"ל או אישיותו של אדם.

ככל שיותר אנשים בארגון חשופים למידע, משמע מס' מורשי הגישה.

סעיף 21 לחוק קובע אילו חובות יחולו על כל סוג מאגר. מרבית החובות שחלות על בעל המאגר, יחולו גם על המנהל וגם על מחזיק המאגר.

# תקנות הגנת המידע האירופאיות – **GDPR: General Data Protection Regulation**

הסדר זה אינו הסדר הגנת הפרטיות גרידא, אלא הסדר הכולל ניהול נבון במידע ובהשלכות שיכולות להיות לניהול במידע.

תקנות אלו מהוות דין מחייב עבור כל המדינות באיחוד האירופאי, והן אינן יכולות לסטות מהוראות אלו. ישנם כל מיני תחומים שהתקנות מאפשרות למדינות לקבוע הסדרים לעצמם, הליבה של התקנות מחייבת את כל המדינות באיחוד האירופאי.

יש אינטרס גדול של המדינות להסדיר את הנושא, על מנת שיוכלו לשגשג כלכלית על בסיס כלכלת המידע – באופן ההולם את ההוראות להגנה על המידע.

הגישה האירופאית הינה גישה מרחיבה, הן בהשוואה לחקיקה הסקטוריאלית האמריקאית והן בהשוואה לחקיקה הישראלית הנוכחית.

נקודה המוצא של גישה זו היא:

1. לכל אדם קיימת זכות יסוד לחירות ולפרטיות.
2. לכל לאדם יש זכות להתגונן מפני עיבוד של מידע פרטי אודותיו.

ניתן לשייך גישה זו מרחיבה לטראומה של אירופה ממלחמת העולם השנייה, בה נעשה שימוש במידע על מוצא אתני של אנשים למטרות מזעזעות כפי שקרה אז (הומואים, יהודים, צוענים וכו').

ניסיון להתאים את הגנת הפרטיות לעידן טכנולוגיות המידע והגלובליזציה.

תקנות אלו לא חלות (או חלות אחרת) על סוגיות של בטחון פנים, בטחון חוץ ועוד.

GDPR יוצרת סל זכויות וכלים למושאי המידע, בצירוף חימוש רגולטורים.

רגולטורים – רשויות הגנת הפרטיות השונות באיחוד האירופאי. הכלים בהם הם מחמשות אותן הם הליכים מנהליים, קנסות כספיים, ובמקרים מסוימים – נקיטה בהליכים פליליים.

טרמינולוגיה של:

data subjects 🡨 מושאי מידע 🡨 נושאי המידע 🡨 נשואי המידע.

מושא מידע = אדם מזוהה או ניתן לזיהוי שעל אודותיו נאסף / מעובד מידע אישי.

חיזוק שליטתם של מושאי המידע במידע האישי שלהם:

עיבוד מידע יכול להיעשות רק אם יש לו בסיס חוקי או אם ניתנה הסכמה של מושא המידע.

סל זכויות וכלים למושא המידע – ניוד מידע, גישה למידע, הזכויות להישכח ועוד.

יש לדעת! ה-GDPR מסדירה זכויות במידע ככלל, לא עוסקת רק בהגנה על הפרטיות.

הסיבות בגינן GDPR גרמה למהפכה:

1. הרחיבה את ההגדרה של מידע אישי (personal information / personal data)
2. הגדרה מרחיבה של עיבוד מידע + דרישת בסיס חוקי לעיבוד מידע.
3. מדובר על ניסיון אמיתי לצקת תוכן משמעותי להסכמה של מושאי המידע לשימוש במידע אודותיו.
4. תחולה פרסונלית רחבה (סיבת חסרת תקדים לפי דברי המרצה). מדובר על חריג מאוד נדיר..
5. מערך קנסות חסר תקדים (ס'83): במדרג הנמוך: עד 2% מהמחזור השנתי או 10 מיליון אירו לפי הגבוה מבין השניים; במדרג הגבוה: עד 4% מהמחזור השנתי או 20 מיליון אירו לפי הגבוה מבין השניים.

סיבה מס' 5 למעשה חלה גם על קבוצת חברות. משמעה אם יוטיוב מפרה ונקנסת, אז למעשה מחשבים את העונש על פי הנתונים של חברת האם שלה, בעניינו לדוג' אלפאבט.

**סעיפי GDPR**

סעיף 4(1) – הגדרת GDPR למידע אישי:

ס'1 נוקט בגישה מרחיבה – הכרה ביכולת הצלבת נתונים שמתקבלים מקורות מידע שונים באופן המאפשר זיהוי של האדם וחשיפת מידע אישי אודותיו.

משכך, מידע היא הוא כל מידע שקשור לאדם מזוהה או לאדם שניתן לזיהוי – אם באופן ישיר או בלתי ישיר (מידע שלא נוקב בשם האדם אבל מאפשר לזהותו). מידע מזהה, מידע ספציפי הנוגע לזהות, כתוב IP וכו'.

אם מדובר על מידע שהותמם (עבר אנונימיזציה, שהפכו את המידע לאנונימי), אם סביר ששילובו עם מידע נוסף יביא לזיהוי של מושא המידע אז גם הוא מהווה למידע אישי.

סעיף 9 – קטגוריות מיוחדות של מידע אישי (רגיש במיוחד):

גזע, מוצא אתני, דעה פוליטית, אמונה דתית או פילוסופית, חברות ארגון עובדים, מידע רפואי, חיי מין / נטייה מינית, נתונים ביומטריים, מידע גנטי. הסעיף פורט שלל קטגוריות נוספות.

עיבוד מידע מסוג זה יותר רק בכפוף לעמידה בדרישות מחמירות, יותר מאשר הדרישות בנוגע למידע אישי "רגיל".

הגדרה רחבה לעיבוד מידע:

סעיף 4(2) ל-GDPR קובע שעיבוד מידע הוא כל עיבוד מידע, גם אם הוא לא מתבצע באופן אוטומטי / באמצעי ממוחשב, כולל איסוף, אחסנה, אחזור, הפצה, מחיקה, השמדה ועוד.

ההגדרה הרחבה של עיבוד המידע היא פועל יוצא של ההתמקדות בהגנת מידע, ולא רק בפרטיות.

הצעות החוק בישראל הקיימות הולכות בדרכה של ה GDPR ומנסות להרחיב את ההגדרה לעיבוד מידע, כאשר בישראל הדבר ייעשה באמצעים ממוחשבים בלבד.

הבחנה בין Processor ל-Controller:

הבחנה חשובה שה GDPR עושה, היא האבחנה בין processor לבין controller.

* קונטרולר – הגוף שקובע את מטרות עיבוד המידע ואת האמצעים לעיבוד המידע.
* פרוססור – מי שמספק בפועל את שירות עיבוד המידע.

לדוג': בנק שאוסף ומעבד מידע בנוגע ללקוחות שמנהלים אצלו חשבונות. הבנק הוא הגוף שקובע את מטרות עיבוד המידע בעוד שהמערכת היא שמספקת בפועל את המידע. דוג' נוספת: חברת טכנולוגיה שמפתחת טכנולוגיית זיהוי רגשות על פי צילום פנים, שוכרת את שירותיו של צד שלישי – מעבדת ניסוי, כדי לבצע ניסויים ביכולת הזיהוי בתנאי אור שונים. החברה היא הגוף שקובע את המטרות, בעוד שהמעבדה היא זו שמעבדת את המידע ומספקת אותו בפועל.

במצב שבו שני גופים מהווים לתפקיד, למעשה שניהם חבים לשני התפקידים, מצב שכזה נקרא Joint Controller.

מתי עיבוד מידע ייחשב לחוקי על פי ה-GDPR?

כל GDPR חייב שיהיה לו בסיס חוקי לעיבוד המידע.

ישנן 6 אופציות המגדירות עיבוד מידע כחוקי:

1. עיבוד מידע שמבוסס על הסכמה של מושא המידע. על ההסכמה להיות חופשית, מפושרת ולצורך ספציפי.
2. עיבוד ידע חיוני לביצוע חוזה שנכרת עם מושא המידע או לצורך כריתתו, כגון חוזה ביטוח / הצעה לחוזה ביטוח.
3. חיוני לקיום הוראות חוק.
4. חיוני לצורך אינטרס אישי של מושא המידע, כגון הגנה על החיים / שלמות הגוף, טיפול רפואי וכו'.
5. חיוני למטרה ציבורית (המטרה צריכה להיות מעוגנת בדין), כגון מחקר של המדינה.
6. חיוני לאינטרס לגיטימי של בעל השליטה במידע או צד שלישי, לרבות אינטרסים מסחריים, אישיים או חברתיים. אופציה זו תחול רק אם זכותו של מושא המידע להגנה על הפרטיות לא גוברת על האינטרס הלגיטימי.

בסופו של דבר, הבסיס החוקי בו מתמקדת ה GDPR הוא עיבוד מידע המבוסס על הסכמה של מושא המידע, זאת לאור הקלות שדורשת בסיס זה (הסכמה) לעומת שאר הבסיסים הדורשים אובייקטיביות.

דגשים:

* הדרישה היא שהעיבוד יהיה חיוני (necessary). אם ניתן להשיג את אותה מטרה באופן סביר וללא ביצוע של עיבוד מידע אישי 🡨 העיבוד אינו נחוץ ונשלל הבסיס החוקי לעיבוד המידע. דרישה זו רלוונטית לאפשרויות 2-6, להוציא את בסיס ההסכמה.
* יש לקבוע את הבסיס החוקי לעיבוד המידע ולהודיע עליו למושא המידע לפני תחילת עיבוד המידע. לא ניתן להשתמש במידע שהושג על יסוד בסיס חוקי אחד, כדי לבצע עיבוד של המידע על יסוד בסיס חוקי אחר. במקרה של עיבוד מידע רגיש במיוחד, ישנן קריטריונים של פירוט ויידוע מחמירים בהתאם.

העמדת מושא המידע במרכז לעניין פעולות במידע שלו:

ה-GDPR מעמידה במרכז את ההסכמה של מושא המידע לפעולות במידע שלו (ס'4(11) + ס'7).

ההסכמה צריכה להיות:

1. חופשית, מדעת, פעילה (ס'4(11)).
2. בשפה פשוטה, מפורשת וספציפית (ס'4(11)).
3. מופרדת ומובדלת מתניות הסכמיות אחרות (ס'7(2)).

יש לקבל הסכמה עבור כל סוג מידע וכל סוג עיבוד מידע (תוך הצהרה על צמידות מטרה).

בנוסף, למושא המידע צריכה להיות אפשרות ממשית שלא להסכים.

הסכמה באמצעות גלישה באתר אינה חוקית משום שהיא אינה פעילה ואינה מאפשרת משיכת הסכמה באופן פשוט (הנחיות EDPB) 🡨 נדרשת הסכמה אקטיבית.

דגשים נוספים:

* יש לציין מפורשות את זהות בעל השליטה במידע ומעבד המידע.
* חובת ההוכחה לקבלת ההסכמה מוטלת על בעל השליטה במידע (סעיף 7(1)). משמע יש לתעד את ההסכמה.
* למושא המידע יש זכות לבטל את הסכמתו – סעיף 7(3). בעת קבלת ההסכמה יש להציג באופן גלוי וברור את האפשרות לבטל את ההסכמה.
* ברירת מחדל של אישור עוגיות מהווה לאסור. על ההסכמה להיות "פעילה", שאתה צריך לסמן או ללחוץ שאתה מסכים, ולא כמו בדוגמה שראינו בכיתה (כל הוי היו מסומנים שאושרו, ועל הגולש להוריד את הוי שאליהם הוא לא מסכים).

מערך הקנסות: הקנסות הכי גבוהים שהושתו (יוני 2023):

* מטא – 1.2 מיליארד יורו (אירלנד). עיבוד מידע ללא בסיס חוקי (העברת מידע לארה"ב).
* מטא + וואצפ – שורת החלטות באירלנד. היעדר ציות להוראות עיבוד המידע. על סך מיליארדי יורו.
* אמאזון – 746 מיליון אירו (לוקסמבורג). נקנסו על אופן עיבוד נתוני המשתמשים.
* H&M – 35 מיליון אירו (גרמניה). ניטור עובדים באמצעות הקלטת מפגשים.

**תחולתו הרחבה של ה-GDPR:**

1. תחולה טריטוריאלית - סעיף 3:

נקודת המוצא היא שדינים הם טריטוריאליים, ו GDPR מותחת את הגבול הזה – תחולת ה GDPR היא על כל בעל מאגר או גורם שמעבד מידע אישי שיש להם establishment באיחוד האירופי.

גם אם עיבוד המידע לא נעשה בשטח האירופי, עדיין ה GDPR יחול!

הדבר כולל גורמים אשר מרכז ניהול העסקים שלהם או המקום שבו מתקבלות ההחלטות על מטרות עיבוד המידע והאמצעים הנדרשים לעיבוד נמצאים בתחומי האיחוד.

כמו כן, גם אם מדובר בגוף שיש להם רק נציג באיחוד, תחולת התקנות תתקיים.

1. תחולה אקס-טריטוריאלית – סעיף 3:

ה GDPR יחול על גורמים שאין להם establishment באיחוד האירופי אם הם:

1. מעבדים מידע אישי של מושאי מידע מהאיחוד האירופי וגם העיבוד קשור להצעה של מוצרים או שירותים לאותם אנשים, בתמורה או ללא תמורה;
2. גורמים המעבדים בידע באופן שקשור לניטור התנהגות אשר מתרחשת בתחומי האיחוד האירופי (אנשים שנמצאים באירופה).

מושא המידע הוא מי שנמצא בתחומי האיחוד האירופי, לא בהכרח אזרח.

אציין שמדובר בתנאים מצטברים.

עקרון הנאותות (adequacy) – סעיף 45:

מידע עובר כל הזמן בין מדינות.

הכלל אומר כי העברת מידע אישי של גורם מהאיחוד האירופי למדינה אחרת (מחוץ לאיחוד האירופי) תתאפשר רק לאחר קבלת הסכמה ישירה של מושא המידע או באופן חוזי. היישום של הכלל מאתגר בעולם שלנו הנשען על קישוריות מקוונת גלובלית – הדבר מוסיף נטל עצום על הצרכנים. לדוג' שירותים למניעת הונאות – הכיצד הם יוכלו לבדוק על גולשים שונים אילו כל פעם יצטרכו לבקש הסכמה?

ולכן, סעיף 45 מאפשר חריג – עקרון הנאותות:

ע"פ החריג, ניתן להעביר מידע מהאיחוד האירופי למדינות מחוץ לאיחוד האירופי, שחוקי הגנת המידע שלהם מספקים הגנה נאותה וראויה לעיבוד מידע אישי.

כיום 13 מדינות מוכרות ע"י המועצה האירופית כמקיימות רמת תאימות מספקת. ישראל הוכרה במעמד זה בשנת 2011 (תפיסה שהדינים הישראלים תואמים את הדינים האירופאים בכל הנוגע לעיבוד מידע תחת הדירקטיבה).

הנושא נתון לבחינה מחודשת בשל כניסה לתוקף של ה GDPR.

אפשרות נוספת:

היא הסכם בין האיחוד האירופי למדינה אחרת. בפועל הסכמים אלו קרסו, בין היתר בשל הצורך לאיסוף מידע לצרכי ביטחון. לדוג' הסכם ה-Privacy Shield שנערך עם ארה"ב, ההסכם קרס גם הוא (ביהמ"ש פסל את ההסדר).

כולנו תקווה שתיקון מס' 14 יעבור! (פה בארץ).

זכויות נוספות של מושא המידע:

* ס' 13-14: קבלת פרטים על המידע האישי שבמאגר.
* ס' 15: זכות גישה למידע האישי שבמאגר ולפרטים אודות אחזקתו ועיבודו.
* ס' 16: זכות לתיקון מידע אישי לא מדויק והשלמת מידע אישי שחסר.
* ס' 17: זכות למחיקת מידע אישי מהמאגר (הזכות להישכח) –

המקור: פרשת גונזלס נ' גוגל (2014)

1. אם המידע האישי אינו נדרש עוד למטרה שלשמה נאגר.
2. אם מבוטלת ההסכמה שמכוחה נאגר המידע האישי.
3. אם המידע הושג באופן בלתי חוקי.
4. אם המידע מעובד שלא כדין או שאין אינטרס לגיטימי בהחזקתו.
5. בזכות תיסוג בפני חובה חוקית לשמור את המידע ועשויה לסגת מול אינטרס ציבורי אחר, כמו חופש הביטוי או שלום הציבור.

הזכות להישכח אינה מעוגנת בישראל.

זכויות מושא המידע במידע (יותר מפרטיות) – זכות לניוד המידע:

אפשרות לנייד מידע אישי של מושא המידע בין פלטפורמות שירותי מידע.

אפשרות זו מקטינה את התלות בפלטפורמה עצמה, כך גם מעודדת תחרות.

זכות זו מוגבלת למידע אישי שמושא המידע סיפק בעצמו או שהגורם השולט במידע יצר עקב תצפית על התנהגותו ועל פעולותיו של מושא המידע.

הניוד כפוף לשמירה על זכויות צדדים שלישיים.

זכויות מושא המידע סעיף 22 – הזכות למעורבות אנושית בקבלת החלטות המבוססות על עיבוד אוטומטי של מידע אישי:

סעיף זה מקנה את הזכות, שהחלטה בעלת השלכות משפטיות או משמעותיות אחרות לא תתקבל רק על סמך עיבוד אוטומטי של מידע אישי או פרופיילינג, אלא תכלול מעורבות אנשית.

מושא המידע יכול להתנגד להחלטה, לערער עליה, ולדרוש בחינה אנושית של ההחלטה.

מהי החלטה בעלת השלכות משפטיות או משמעותיות בלבד? שאלה יפה מאוד.

מהי מידת המעורבות האנושית הנדרשת? גם שאלה יפה.

חריגים שבהם יותר עיבוד אוטומטי:

1. נדרש לכניסה לחוזה או ביצוע חוזה בין בעל השליטה במידע ומושא המידע
2. הדבר מותר בחוק
3. ניתנה הסכמתו של מושא המידע

הנדסת פרטיות – סעיף 25:

הגורם ששולט במידע מחויב להטמיע אמצעים טכנולוגיים וארגוניים לשמירה על הפרטיות הן בשלב תכנון המערכת והן בשלב עיבוד המידע.

* הרציונל: ראוי לעצב את הטכנולוגיה מראש כך שתמזער ככל שאפשר את הפגיעה בפרטיות.
* מעשית: קל יותר להטמיע הגנה על פרטיות במערכת טכנולוגית בשלב התכנון והעיצוב, מאשר להוסיף אמצעי הכנת פרטיות בדיעבד (כך התיקון יהיה יקר ומורכב יותר, ולעיתים גם מאוחר מדי).

**שירותים משפטיים מקוונים וטכנולוגיות משפטיות (Legal Tech)**

* היום נעסוק בשאלה האם טכנולוגיה יכולה למעשה לתת שירותים משפטיים?
* באיזה אופן עורכי דין יכולים להשתמש בטכנולוגיה לשם הענקת שירותים משפטיים?

התובנה איתה נלך השיעור היא לא "איך טכנולוגיה יכולה להחליף את עבודתם של עורכי הדין", אלא "איך אנשים יכולים לקבל את הדבר שלשמו הם פונים לעורך דין, אז רק באופן אחר".

עלות של עבודה משפטית, של ליטיגציה, הינה עלות אדירה. מדובר פה בשיקולים כלכליים. אך גם יש שיקולים כגון: צדק, מקסום הזמן האנושי וכו'.

ההתחלה: טפסים משפטיים מקוונים:

טפסים סטטיים – תבנית קבועה מראש. המשתמש ממלא נתונים אשר נשתלים במסמך.

טפסים מותאמים אישית – התוכנה מייצרת מסמך מותאם אישית לפי מידע והנחיות שהמשתמש מספק. המשתמש מקבל מסמך עם תוכן ומבנה שהותאמו למידע ספציפי שסיפק.

ממשקים חכמים – עיבד טקסט. למידת מכונה ועיבוד שפה טבעית (AI).

אופני תקשורת – להשליםםםםם

כיום ישנו מגוון שירותים משפטיים מקוונים, ליגל טק למשפטנים. שירותים אלו מאפשרים הפקת מסמכים משפטיים בעזרת טפסים מקוונים מותאמים אישית.

השירותים המשפטיים נעשים לעיתים באמצעות צ'אט בוט – אבחון הבעיה, הגשת תביעה. גם משפטנים משתמשים בטכנולוגיות האלו.

ישנן מערכות אלגוריתמיות תומכות החלטה, אשר משמשות בעיקר משפטנים, לשימושים שונים:

* אוטומציה של מחקר משפטי, אוטומציה בניסוח חוזים.
* חישובים פיצויים / גזרי דין; חישוב סיכויי תביעה / סכום פשרה.
* אנליזות של הליכים (סטטיסטיקה תיאורית וחיזוי).
* גילוי אוטומטי (בעייתיות אפשרית: זיהוי שלילי שגוי / אי זיהוי).
* איתור סיכונים בחוזים ותיקונם.
* ניסוח אוטומטי של מסמכים.

דוגמאות לחברות המציעות הפקה של מסמכים משפטיים:

* Legal zoom
* Rocket Lawyer
* I Can Legal
* Form Swift

שימוש בהם הוא זול משמעותית משימוש בעורך דין בשר ודם.

Access to Justice Author:

מדובר בתוכנה שנפעלת על ידי סטודנטים.

זוהי תוכנה שמשמשת גורמים בעלי ידע משפטי לצורך עיצוב שאלון / ראיון משפטי מקוון לאבחון ואיסוף מידע, בנוסף גם הפקת מסמך משפטי רשמי.

RoboLawyer:

* תוכנה המעבדת שפה טבעית.
* התאמה של מסמכים.
* הגשה מקוונת לרשות / לנתבע
* מספקת חווית משתמש של שיחה אינטראקטיבית.

מביטול דוחות חניה ועד דרישת פיצויים מגופים מוסדיים וכו'.

לא צריך בכלל להכיר את המונחים המשפטיים. אתה כותב בחיפוש – "חברת התעופה דפקה אותי", וישר הבוט מציג לך הגשת תביעת פיצויים מחברות תעופה.

אתגרים לפיתוח מיזמים משפטיים טכנולוגיים בישראל:

הסיבה המרכזית שהתחום לא התפתח היא ההתנגדות של לשכות עורכי הדין בשלל מדינות. עורכי הדין הם השחקן המרכזי שבשוק, והם מתנגדים נחרצות.

הנושא נקרא – ייחוד פעולות המקצוע, או מצדו השני – איסור שיתוף בהכנסות או קבלת הפנייה של לקוח שנעשתה למטרות רווח.

כללי ההסדרה המקצועיים של עורכי הדין הם חוק לשכת עורכי הדין תשכ"א-1961 וכללי לשכת עורכי הדין (אתי מקצועית, התשמ"ן-1986.

כללים אלו קובעים איסורים משני סוגים, אשר מקשים על פיתוח תעשיית השירותים המקוונים בישראל:

1. כללי ייחוד פעולות המקצוע (הסגת הגבולות המקצוע): ס' 20 קובע כי יש פעולות שרק עורכי דין יכולים לבצע
2. איסור שיתוף בהכנסות או קבלת הפנייה של לקוח שנעשתה למטרות רווח

הנורמות האתיות והמקצועיות התפתחו בעידן שלפני טכנולוגיות המידע ולפני היישומים שלהם בתחום המשפט.

נקודת המוצא היא ס'20 לחוק לשכת עורכי הדין: קביעת ייחוד פעולות מקצוע.

ייחוד פעולות המקצוע – סעיף 20 לחוק לשכת עורכי הדין:

הפעולות המנויות להלן, לא יעשה אותן דרך עיסוק, או בתמורה אף שלא דרך עיסוק, אלא עורך דין; ואלה הפעולות:

(1)  ייצוג אדם אחר וכל טיעון ופעולה אחרת בשמו לפני בתי משפט, בתי דין, בוררים וגופים ואנשים בעלי סמכות שיפוטית, או מעין שיפוטית;

(2)  ייצוג אדם אחר וכל פעולה אחרת בשמו לפני –

משרד ההוצאה לפועל;

לשכת רישום הקרקעות;

הפקיד המוסמך לענין חוק בתים משותפים, תשי"ג-1952;

רשם החברות;

רשם השותפויות;

רשם האגודות השיתופיות;

רשם הפטנטים והמדגמים;

הרשם כהגדרתו בחוק העיצובים, התשע"ז-2017;

רשם סימני המסחר;

(3) עריכת מסמכים בעלי אופי משפטי בשביל אדם אחר, לרבות ייצוג אדם אחר במשא ומתן משפטי לקראת עריכת מסמך כזה;

(4)  ייעוץ וחיווי דעת משפטיים.

למעשה המחוקק לעורכי הדין מונופול על הפרקטיקה המשפטית, בתמורה להגנה על הציבור. ייצוג משפטי קלוקל יכול לפגוע באינטרסים ובזכויות של המיוצגים, ועל כן המחוקק העדיף לתת לעורכי הדין את המונופול עבור הבטחת האיכות.

מכאן מתעוררת השאלה (אתגר): האם חברות טכנולוגיות המבקשות לספק שירותים משפטיים ע"י מי שאינו עו"ד מסיגות את גבול המקצוע? האם סיפוק שירותים אלו מהווה הפרה של ס' 20? לשם כך נדרשת הבחנה בין מתן מידע משפטי לבין ייעוץ משפטי.

מתן מידע משפטי באמצעות שירות מקוון אינו אסור כשלעצמו, בעוד שייעוץ משפטי או מתן חוות דעת שיפוטית ע"י מי שאינו עו"ד אסורים.

מתן מידע משפטי VS ייעוץ משפטי - אינדיקציות להבחנה:

ככל שהמידע כללי יותר ואינו מתייחס למקרה העובדתי הקונקרטי – ניטה לחשוב שמדובר במתן מידע; ככל שהמידע נשען על נסיבותיו הפרטניות של הפונה – ניטה לחשוב שמדובר בייעוץ.

בנוסף, יש לבחון את השאלה הבסיסית: האם המידע/השירות/הייצוג בנסיבות המקרה הם משפטיים? אמות המידה לשאלה זו נקבעו בפס"ד "המרכז למימוש זכויות רפואיות".

ייעוץ וחיווי דעה משפטיים:

פס"ד המרכז למימוש זכויות רפואיות נ' לשכת עורכי הדין: בחינה האם שירותי המרכז אכן מהווים שירות משפטי. בפס"ד נידונה השאלה כיצד לפרש מונחים כמו ייצוג ואופי משפטי בס'20, כאשר הקו המנחה של הפרשנות הוא תכלית הסעיף – להבטיח שלא ייגרם לציבור נזק כתוצאה משירות משפטי לקוי. הקושי בייחוד המקצוע הוא יצירת מונופול שפוגע בזכויות ואינטרסים אחרים – חופש העיסוק, האוטונומיה של הפרט לבחור לעצמו את האדם שייצג אותו, נגישות למערכת המשפט.

בפס"ד נקבעו אמות המידה שיש לשקול בהכרעה האם פעולה / שירות הם ייחודיים למקצוע ערכית הדין:

1. היקף שיקול הדעת שכרוך בביצוע השירות או הפעולה שניתנים לציבור. הפעלת שיקול דעת רחב, תוך שקלול משתנים רבים 🡨 ייפול בגדר ייחוד;

פעולה טכנית בעיקרה שאינה מצריכה בחירה בין דרכי פעולה רבות לא תחשב כייחודית.

1. פוטנציאל הנזק שייגרם לציבור עבור שירות לקוי. ככל שפוטנציאל הנזק משמעותי יותר והנזק בלתי הפיך 🡨 ייחשב כייחוד. ככל שהפוטנציאל יהיה מצומצם יותר כך ניטה לסווגו כלא ייחודי.
2. איזו חלופה עומדת לציבור במימוש זכויותיו? אם ייאסר מתן השירות על ידי מי שאינו עורך דין (בשים לב למחיר), שיקול של נגישות. לדוג' החלופה היחידה לניסוח צוואה היא רק תוך השכרת עו"ד, מדובר בחלופה יקרה, בכזה מצב לדוג' ביהמ"ש ייטה לאפשר שירות שכזה.

בפס"ד זה השופטת ארבל טוענת כי – בעתיד יתכן ששירותים משפטיים מסוימים ונקודתיים יסופקו לציבור הרחב אף על ידי מי שאינם עו"ד. "לא כל הכרוך במימוש זכויותיו של הציבור צריך להיות נחלתם הבלעדית של עורכי הדין".

נדרשת הסדרה על ידי המחוקק. בין היתר גם מנגנוני פיקוח שיבטיחו הכשרה מתאימה וכללי התנהגות במתן השירות.

שירותים משפטיים מקוונים: פסיקה בבתי המשפט המקוונים:

עם השנים, בתי המשפט החלו בהחלת מבחני המרכז למימוש זכויות רפואיות. מקרה מפורסם הוא פס"ד דטהפקס.

פס"ד לשכת עורכי הדין בישראל נ' דטהפקס בע"מ: השירות שניתן הוא שאלות ותשובות למרכז מומחים והתאמת מאמרים, כאשר חלק מהמומחים היו עורכי דין. השאלה הייתה מהו הקו המבחין בין מתן מידע לבין ייעוץ וחוות דעת? נקבע שהייעוץ ניתן סביב מסכת עובדתית קונקרטית ודרש הפעלת שיקול דעת רחב. התאמת המאמר לשאלת הלקוח מצריכה הבנה משפטית בדיני עבודה (ובתחומים משיקים), ודיוק בבחירת ובהצגת הסוגיות המשפטיות במקרה הספציפי. אך שמבחינה לשונית הדבר לא כונה כך, בפועל זהו ייעוץ משפטי ולכן הדבר נחשב כהפרת הסעיף.

שאלתי את המרצה – מדובר בעורכי דין שמעניקים את השירות, אז עצם כך לא מדובר בדבר חוקי? נענתי בכך שאילו היו עובדים בכובעם כעורכי דין, ולא בכובעם של עובדי דטהפקס, אז כנראה ולא הייתה בעיה. אך לא היה ידוע כי כל השירות שניתן הוא מעורכי דין בלבד. בנוסף אין מדובר פה בשירות משפטי, אלא בשירות החברה. אילו היו עובדים בפירמת עורכי דין זה היה תקין. דגש על פירמה.

פס"ד לשכת עורכי הדין בישראל נ' חשבים ה.פ.ב מידע עסקי בע"מ: שירות המחולל חוזה עבודה בהתאם לתנאים הספציפיים שהמעסיק מכניס לתוך המחולל. בנוסף מחולל של סיום יחסי העבודה משתמש באלגוריתם המחבר תניות בהסכם, כך הנושאים שצריכים להיות מוסדרים בסיום יחסי העבודה. ביהמ"ש פסק כי:

זהו חיבור טכני: שילוב נוסחים של חוזים בהתאמה לצרכי המשתמש.

למעשה, יש לראות זאת כפלטפורמה לשימוש עצמי המחליפה את הפרקטיקה הרווחת בשטח, למשתמש ניתנת אפשרות בחירה בין חלופות 🡨 לא ניתן ייעוץ משפטי קונקרטי אסור, זהו שירות למי שהחליט לפעול לבדו וללא ייעוץ משפטי. עלות השירות נמוכה, וספק אם ניתן היה לרכוש שירות מקצועי בעלות דומה. פוטנציאל הנזק נמוך יותר בהשוואה למציאות הטכנולוגית הקיימת של חיפוש-העתק-הדבק לפי בחירת המשתמש. למעשה נפסק כי אין מדובר בפעולה משפטית אסורה.

בנוסף השופטת ארבל מציעה שתהא הודעת פתיחת המודיעה כי השירות אינו ניתן ע"י עורך דין מקצועי (לא פרט מידע חשוב, סתם הוספתי).

הלשכה ערערה על פסק הדין. בעליון השופטים דוחקים בלשכה, וקובעים כי גם הלשכה צריכה להיות קשובה לשינויים שקורים ולהתפתחות עולמינו. מכאן שלשכת עורכי הדין משכה את הערעור.

בפס"ד יהונתן ארד נ' מנקס אונליין טריידינג בע"מ (2018) – ביהמ"ש אישר וקבע כי יש לקבל תביעות נגד ספאמרים המוגשות על ידי אזרחים בסיוע של חברות מסחריות, כמו חברת הסטארט אפ ספאם - אוף. בתכלס הוא אישר כי בכל מקרה מדובר בתביעות קטנות, עו"ד לא יכול להתעסק איתן בכל מקרה.

"פעילות של גופים כגון ספאם אוף מסייעת להגשים את התכלית ההרתעתית שבבסיס חוק התקשורת על ידי עידוד הגשת תביעות וטיובן; קיומן של תביעות רבות בגין הודעות ספאם אינו מעלה חשש להרתעת יתר, אלא תקווה לאכיפה אפקטיבית; אף אין לומר כי פעילות ספאם אוף נוגדת את תכליות הליך התביעה הקטנה. תכלית הליך התביעה הקטנה לאפשר לאזרח כלי מהיר, זול וזמין לבירור תביעות בהיקף כספי מצומצם לשם מיצוי זכויותיו. המחוקק הכיר בכך שלא ניתן להסתפק במאפייניו הגמישים והנגישים של הליך התביעה הקטנה אלא קיים צורך לאפשר לארגונים שיוכרו לשם כך להגיש סיוע משפטי וייצוג כדי להתגבר על מכשולים שונים. בענייננו אמנם אין מדובר בארגון ללא מטרת רווח שקיבל הכרה בצו של שר המשפטים אולם כל עוד פעילות ספאם אוף נעשית בצורה ראויה, אין בכך כל סתירה לתכליות הליך התביעה הקטנה; אין לקבל את השיקול בו נקטו הערכאות קמא לפיו ריבוי תביעות הספאם בסיוע ספאם אוף מוביל לעומס שיפוטי ודבר זה מצדיק לנקוט באמצעים שלא לעודד תביעות כאלה ואף לדחותן".

איסור שיתוף בהכנסות; איסור ייצוג של לקוחות שהופנו מגופים למטרות רווח

* סעיף 58 ו-59 לחוק לשכת עורכי הדין – איסור שותפות ושיתוף בהכנסות.
* כלל 11ב לכללי האתיקה – איסור ייצוג לקוח שהופנה על ידי מי שאינו עורך דין:

כלל 11ב(א) – כשהלקוח הופנה על ידי גורם שפועל למטרת רווח ולמטרה זו מפרסם ברבים מתן שירותים משפטיים;

כלל 11ב(ב)- אם עורך הדין מועסק על ידי מעסיק, אל לו להעניק שירות משפטי ללקוח שאינו המעסיק.

כללים אלה מקשים על פיתוח יוזמות עסקיות וטכנולוגיות של שירותים משפטיים.

הם מגבילים את עורכי הדין לשתף פעולה עם מי שאינם עורכי דין בעבודתם. מדובר על מגבלות שמגבילות מאוד את היכולת לפתח את התחום פה בישראל.

מודלים חדשים לשירות משפטי: קיטוע / תיחום:

פירוק הסוגיה המשפטית לרכיביה => אמצעי להגברת נגישות המשפט.

שירות נקודתי ומוגבל (לדוג' מתן מידע משפטי בעניין מוגדר, ניסוח מסמך).

התנסויות בפתרונות רגולטוריים חדשניים.

פתרונות רגולטוריים חדשניים?

1. ביוטה, ארה"ב – Regulatory Sandbox:

ביהמ"ש מעניק אישור מוגבל בזמן (שנתיים) למודלים עסקיים חדשניים ושירותים חדשניים בתחום המשפט שפועלים בתחומים מוגדרים.

על מנת להתקבל כחברה כזו ביוטה עליך לקבל אישורים כמובן.

אחד המודלים – Software provider with lawyer involvement.

1. באריזונה, ארה"ב:

שינוי הכלל שאוסר על מתן שירותים משפטיים על ידי מי שאינם עו"ד במקרים מסוימים באמצעות יצירת מתווה עבור יישות משפטית ייחודית – "Alternative business Structure". בין היתר עסק שמעניק שירותים משפטיים שנמצא בבעלות משותפת של עו"ד ומי שאינו עו"ד.

המודל שהיה ביוטה הוביל להרבה יותר התנסויות וקידמה. הוא זה שקידם את החדשנות במישור הזה בצורה המובהקת ביותר. אחרי כל הבאז המטורף שהיה על יצירת המסגרות הרגולטריות הללו – התברר כי השירותים שקמו בעקבות כך הם בעיקר נועדו לאדם הקטן, לחלשים, ולא לעשירים, לחזקים.

מערכות תומכות החלטה בעבודת המשפטנים:

מערכות משפטיות אוטומוטיות?

* אוטומציה של מחקר משפטי
* הבניה / אוטומציה בניסוח חוזים.

בנוסף יש עולם המספק:

* חישוב פיצויים
* חישוב גזרי דין
* חישוב סיכויי תביעה
* חישוב סכום לפשרה
* אנליזות של הליכים (סטטיסטיקה תיאורית וחיזוי) – לדוג' על פי הסטטיסטיקה מתי כדאי להגיש כך וכך.

אוטומציה במחקר המשפטי – Ravel View (Lexis). כלי לניתוח Data.

תחום נוסף הינו חיזוי אלגוריתמי.

חיזוי אלגוריטמי – גילוי מסמכים מוקדם (e-discovery):

* האתגר – בעידן הדיגיטלי ישנה גידול בכמות המסמכים, משמע גידול בשעות האדם שדרושות כדי להעריך את הרלוונטיות של כל מסמך להליך המשפטי.
* הפתרון הטכנולוגי – תוכנות המבצעות חיפוש אוטומטי במסמכים באופן שמחקה את תהליך האיתור והמיון של אדם בעל הכשרה בתחום.
* התוצר – ניבוי בדרגת ודאות גבוהה יחסית ביחס לשאלה אם מסמך כלשהו רלוונטי להליך ספציפי, מכאן פחות שעות אדם דרושות להערכת המסמכים.
* הקושי – שגיאות מסוג אחד (זיהוי חיובי שגוי) ושגיאות מסוג שני (אי זיהוי שגוי).

חיזוי אלגוריתמי – ביקורת והערכת סיכונים בחוזים (Lawgeex):

אחד מיועצי החברה הוא מהאוניברסיטה.

החברה בודקת עד כמה החוזה המסוים מתאים למדיניות המסוימת של החברה.

לדוג' אם ש חוזה שנראה מסוכן, שהוא לא עומד במדיניות החברה, אז התוכנה תסמן לייעוץ המשפטי של אותה חברה שישנה בעיה.

החברה ניסתה לבדוק מי יותר יעיל – עורכי דין או ה-AI?

המשימה הייתה איתור סיכונים בהסכמי סודיות. עורכי הדין (20 בכמותם) היו מומחים בנושא.

התוצאות:

|  |  |  |
| --- | --- | --- |
|  | עורכי הדין | תוכנת ה-Lawgeex |
| משך הזמן | 92 דק' בממוצע | 26 שניות |
| שיעור דיוק בסיכונים שאותרו | 85% (טווח של 67% עד 94%) | 94% |

אנליטיקה של הליכי ליטיגציה:

מה נוכל לבחון?

1. רמה נמוכה – מה קרה בעבר
2. רמה נמוכה פחות – מדוע זה קרה?
3. רמה בינונית – מה יקרה בעתיד?
4. רמה גבוהה – כיצד אנחנו יכולים לגרום לזה לקרות?

חיזוי וניסוח – מערכות לניתוח וניסוח מסמכים משפטיים:

חברת פרומטה:

הפקה אוטומטית של מסמכים משפטיים.

חיזוי של תוצאות משפטיות.

חברת לקס משינה:

כרייה ועיבוד של מידע קשור ליטגציה. חיזוי התנהגויות ותוצאות משפטיות.

לדוג' – באיזה אסטרטגיה עלי לנקוט?

בשנת 2019 בצרפת התקבל תיקון לחוק האוסר על ביצוע של אנליטיקה על החלטות השופטים באופן הנ"ל. זה בעקבות החשש שזה ישפיע על עצמאות החלטות השופטים. בנוסף מדובר בפגיעה בפרטיותם של השופטים. התוכנה מעבדת ממש את כלל פסיקותיהם ומכאן החשש לגביהם.

Litigate – היא תוכנה המייעלת מאוד את עבודתם של עורכי הדין.

מי יתלהבו מהרעיון? המדינה, הפרקליטות.

מנגד השאלה היא – כמה זה ראוי שלמדינה תהא גישה לכלי שכזה?

העתיד – רובוט ליטיגטור?

אין מדובר בחלום לא מציאותי. כבר נראו בעולמינו רובוטים שיודעים לפעול.

מכאן המרצה הראתה לנו סרטון של תחרות דיבייט בין בן אדם לרובוט. נקווה שלא נראה טכנולוגיה שכזו בבתי המשפט השונים (הוספה שלי – כותב המחברת).

מה העתיד?

* מומחיות
* יחסי אנוש – אין לבינה המלאכותית בינתיים...
* אתיקה
* יצירתיות – לדוג' היקש, עו"ד משתמש רבות בהיקשים, ואילו לבינה מלאכותית אין את האפשרות לבחון ולחשוב על היקשים.
* עבודה משולבת עם ה-AI – שליפה וארגון של מידע? הפעלת שיקול דעת ומסקנות?

דברים שלפני שנה נראו לא אפשריים, אז היום כבר אפשריים ובהחלט. מכאן שקשה מאוד לחזות מה יהיה בעתיד.

**המבחן**

1. דומה לשנים קודמות.
2. שילוב בין שאלות אמריקאיות ושאלות פתוחות.
3. שאלות ידע לחלוטין, ושאלות הדורשות לשלב שני תחומים שלמדנו.
4. השאלות הפתוחות הן או קייס, או שאלות שהן ככה של מחשבה או של יישום של דבר שלמדנו.
5. יהיו קבצי חקיקה רלוונטיים.