**מחברת משולבת במשפט וטכנולוגיה**

**שיעור 1, 25.02.19**

**נושא 1 לסילבוס: מבוא**

**התפתחות המשפט אל מול ההתפתחות הטכנולוגית**

**1.**     **התפתחות המשפט אינה תואמת את קצב ההתפתחות הטכנולוגית:**

**a.**   **חוק מור -** כוח המחשוב מכפיל את עצמו על 18 חודשים

**b.**   טכנולוגיות מידע מחוללות תהליכי שינוי בקצב ובעוצמה חסרי תקדים

**c.**      הפתרון אינו יכול להיות תגובה משפטית נקודתית

**2.**    **כיצד מערכת המשפט מתמודדת עם הצורך בשינוי והתאמה?** עקרונות משפטיים, מושגי שסתום, פרשנות משפטית, וחקיקת משנה, הנחיות מנהליות, סמכויות רגולטוריות פסיקה, ולעיתים גם חקיקה ראשית. **בנוסף, פיתוח פרדיגמה לבחינת סוגיות שמערבות משפט וטכנולוגיה.**

* **בקורס נפתח חשיבה פרדיגמטית על משפט וטכנולוגיה:**
* מסגרת אנליטית לבחינה יחסי הגומלין בין משפט וטכנולוגיה (טכנולוגית שמאתגרות את ההסדר המשפטי הקיים או את אופן פעולת המשפט)
* התמקדות בשאלות שנוגעות לרגולציה של טכנולוגיה ובאמצעות טכנולוגיה.
* **נקודה מרכזית:** שינוי במעמד המשפט כמערת שמסדירה התנהגות באמצעות כללים שנאכפים בבתי המשפט ע"י רשויות אכיפת החוק.
  + הפרטת האכיפה, אוטומציה, שקיפות, פיקוח, פיתוח נורמות וכללים, גיבוש ערכים
  + סדרי גודל חסרי תקדים של מידע ושל פעילות
  + שינוי בהתנהגות ובתפישות החברתיות?

**3.**    עידן הטכנולוגיה מביא לשינוי במעמד המשפט בתור מערכת מרכזית שמסדירה התנהגות, באמצעות כללים שנאכפים בבתי המשפט ע"י רשויות אכיפת החוק. (הפרטת האכיפה, אוטומציה ואכיפה?)

**4.**    אם כן, כיצד המשפט מגיב לשינויים טכנולוגיים? **התפתחויות טכנולוגיות מאלצות את מערכת המשפט לבחון את התאמתם של כללים משפטיים קיימים למציאות חדשה**

**a.**   האם הגלישה באתר האינטרנט היא בגדר הסכמה לחוזה?

**b.**   האם צעצועים חכמים פוגעים בפרטיותם של ילדים שמשחקים עם בעל הצעצוע?

**c.**   האם לרובוטים בעלי בינה מלאכותית יש אישיות משפטית?

**d.**   האם גם חופש הביטוי חל על בוטים שמייצרים פייק ניוז?

**e.**    התשובות לכל אלה, מחייבות בחינה של תכלית החקיקה והבנה של הסביבה הטכנולוגית.

**דוגמה - תעמולת בחירות באינטרנט (השלמה מעדי לובוצקי)**

חוק הבחירות (דרכי תעמולה) המסדיר את שידורי תעמולה באמצעות אמצעי תקשורת (רדיו, טלוויזיה, עיתונות).  האם החוק חל על תעמולה באינטרנט? עד היום לא. למה?

בשנת 2001 השופט חשין נדרש לשאלה האם חבר כנסת שעונה לשאלות של גולשים בצ'ט כפוף לחוק הבחירה (דרכי תעמולה). כלומר, האם מה שנוגע לשידורי תעמולה ברדיו ובטלוויזיה חל גם באינטרנט? החוק קובע שערוצי תקשורת מחויבים להקצות לכל מפלגה (בהתאם למפתח שנקבע) זמן שידור לתשדירי תעמולה. באינטרנט אין מחסור באמצעי שידור או זמן שידור, אבל קיימים היבטים (חסמים) אחרים שיכולים לנהל ולהשפיע על תשומת ליבם של צרכני התוכן. למשל, האופן שבו מעוצבות תוצאות החיפוש במנועי החיפוש; העדפה של ספקי שירות לתכנים ממקור מסוים; שימוש בתוכנות סינון; גישה למידע אישי על בוחרים לצורך הצלבה ועיבוד לצורך השגת יתרון בתעמולת הבחירות. פייק ניוז, בוטים, הודעות שאינן מזוהות כתעמולה; חשין קבע שלא מדובר בתעמולה פסולה והתייחס לכך שבתעמולה בעולם האינטרנט יש לשקול שיקולים אחרים.

בשנת 2019 השופט מלצר נדרש לשאלה האם פרסום באינטרנט וברשת חברתית חייב לכלול את שם המפלגה שמטעמה פורסם? האם יש לאסור על רשימות לשלם לגורמים שונים תמורת פרשומים שמתחזים לאישיים? עמדת היועמ"ש  - מסכימים שהקירות הורטואלים לא שונים מכל מודעה אחרת.

**המשפט כמעצב טכנולוגיה**

**1.**   המשפט יכול להשפיע על סוג הטכנולוגיות המותרות לשימוש, על אופן יישומן, על עלות הפעלתן ועל היתכנותן של טכנולוגיות חלופיות.

**2.**   מגבלות בחוק על פיתוח וייצור טכנולוגיות - סוגים שונים של הצפנה או פריצת מנעולים טכנולוגיים שנועדו להגן על זכויות אדם

**3.**   תמריצים לפיתוח טכנולוגיות מסוג מסוים

**4.**   הטלת אחריות משפטית בגין שימוש בטכנולוגיה אחת עשוי לעודד פיתוח של טכנולוגי אחרת: כלומר, המשפט יכול לתרום להתפתחות הטכנולוגיה גם באופן חיובי, באמצעות התפתחות מודלים כלכליים חדשים כגון תוכנות Open Source או רשיונות של קניין רוחני כדי שלא ניתן יהיה לעקוף את דיני זכויות היוצרים.

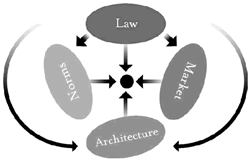
**שינויים במשפט כמוסד בעידן טכנולוגיות המידע**

למשפט - ככלי להסדרת התנהגות ואכיפה - קמים מתחרים פרטיים בעידן הטכנולוגיה. אחד הנושאים המרכזיים שבהם נדון בקורס הוא הסדרה ע"י גופים פרטיים ובאמצעות טכנולוגיה. למשל, ב-Ebay (אתר שעוסק במסחר אינטרנטי) מוכרים וקונים נתקלו בבעיה שסכסוכים על רקע סחר מקוון לא באמת היו ניתנים לפתרון ריאלי. מכך נולדה תעשייה שלמה של יישוב סכסוכים מקוון (כמו בעלי אקספרס), שאף הובילה לזליגה והקמת מערכות מקוונות ליישוב סכסוכים שלא משרתות רק פעילויות אינטרנטיות אלא גם פעילויות פיזיות של ממש (כגון מערכות לגירושין, מיסים, תביעות קטנות, תשלומים, עבירות תנועה, הגנת הצרכן וכו').

* האפקטיביות והלגיטימיות של חקיקה מדינתית ברשת גלובלית
* אכיפה
* יישוב סכסוכים מקוון
* הסדרה של טכנולוגיה, הסדרה באמצעות טכנולוגיה
* השלכות טכנולוגיה על תפקוד המשפט (למשל, הנגשת חקיקה ופסיקה)
* התגברות ההסדרה הפרטית והיחס בינה לבין הסדרה ציבורית
* **לדוגמה:** גיוס ספקיות אינטרנט לחסימת הגישה של גולשים לכתובות IP של חברות מחוץ לישראל כדי למנוע פעילות בלתי חוקית כמו הימורים.

**אילו מנגנוני הסדרה של טכנולוגיה פועלים לצד המשפט:**

* חוזים
* תקנות שימוש
* קודים של ארגון או ענף
* כללי תקינה
* כללי אתיקה
* נורמות חברתיות
* הטכנולוגיה עצמה

**המודל של לסינג**

אחד המלומדים פורצי הדרך בתחום המשפט וטכנולוגיה הינו לורנס לסיג, שטבע את הביטוי CODE IS LAW. המודל שלו מניח שעל כל פעילות אנושית שמבקשים להסדיר פועלות **ארבע מערכות הסדרה שונות שמשפיעות עליה ישירות** (מידת ההשפעה יכולה להשתנות לפי הקשר):

**(1)** **מערכת המשפט**, כללים משפטיים שמסדירים באופן ישיר את הפעילות ומשפיעים עליה גם באמצעות השפעתם העקיפה על השוק, הטכנולוגיה והנורמות החברתיות.

**(2)** **כוחות השוק**, שפועלים ומשפיעים על הפעילות האנושית - למשל יכולת כלכלית שקובעת אם דבר הינו אפשרי או לא בסיטואציה נתונה.

**(3)** **נורמות חברתיות** שמסדירות את מה שמקובל בהתנהלות האנושית, ומשפיעות על המשפט (כמו ערך הפרטיות).

**(4)** **הטכנולוגיה** עצמה.

**הגישה האינסטרומנטלית למשפט וטכנולוגיה:**

1. לטכנולוגיה אין ערכים, היא פונקציונאלית בלבד: מיישמת ומטמיעה ידע בתוך הכלי הטכנולוגי ופועלת בהתאם למטרות של משתמשיה.
2. גישה מיושנת שקשה למצוא לה תומכים בדורנו.

**גישה מהותנית-ערכית למשפט וטכנולוגיה:**

1. הטכנולוגיה מגלמת בתוכה ערכים
   1. **באופן עקיף**: הטכנולוגיה מתפתחת במענה לצרכים של החברה, ומעוצבת בתנאים להם.
   2. **באופן ישיר**: טכנולוגיה שמתוכננת בכוונת מכוון לגלם ערך מסוים
2. תוכנות סינון (בקרה הורית/עצמית/הלכתית על תכנים באינטרנט)
3. ארכיטקטורת האינטרנט כרשת נטולת שליטה מרכזית – אוסף של "צינורות" תקשורת נתונים מקצה לקצה.
   1. לעיתים משמעות הטכנולוגיה נקבעת בדיעבד, לא רק ע"י המתכנתים והמפתחים אלא גם ע"י המשתמשים.

**שיעור 2, 04.03.19**

**נושא 2 לסילבוס: גורמי ביניים ברשת האינטרנט  - (מתווכים - intermediates)**

**המאמר של ניוה-אלקין קורן (מהמחברת של אור כהן)**

בראשית ימיה, היא הגיעה עם הבטחה מאוד גדולה של ביזור הכוח - כיכר העיר החדשה והשוק החופשי שבה כל אדם יכול לגשת למידע בצורה חופשית, וחופשי לפעול. מרחב האנושות כולה יכולים לשגשג באין מפריע, כאנטי-תזה לריכוזיות שמאפיינת את ההפצה של מידע ודעות במדיות המסורתיות.

הסיבה היא, שאם אנו משווים את האינטרנט לאמצעים מסורתיים של הפצה (עיתונים, טלוויזיה, רדיו, ספרים...) – לא נצטרך הקצאה של ערוצי שידור, לא נצטרך משאב ציבורי. יש מרחב שכל אחד יכול לגשת ובעלות מאוד מינימלית להפיץ תוכן, והוא יכול לעשות זאת בצורה כמעט חופשית – אני פשוט אפרסם את מכתבי. יש לי יותר משתתפים בשיח ויותר חופש דעה. ההיבט של הביזור כאן מתבטא בכך שאין שליטה על קביעת סדר היום בשיח. אני כבר לא תלוי בבחירת העורך, אני יכול לגלוש לכל בלוג או אתר שאני רוצה. אם אני ארצה לצרוך מידע של מישהו שיושב באלסקה 30 שנה בבונקר, אין לי שום בעיה לעשות כן.

יש לנו יותר פלורליזם, תקשורת ישירה בין אנשים, דינמיות, מהירות תגובה והפצה של מידע. זה נראה נהדר וחופשי, מאושר ומקדם את חופש הביטוי, חופש הדעה, המידע, החירות האישית והאוטונומיה של הפרט...

**אבל** אנו בעצם יודעים שהאינטרנט והמודלים של השימוש באינטרנט הם לא באמת חופשיים לחלוטין משליטה/פיקוח/הגבלה. אחד העקרונות הבסיסיים של הרשת מראשיתה היה ניטרליות – שכוחות השוק לא יכתיבו איזה מידע אני אראה קודם/בכלל, אבל בפועל אפשרויות הפעולה באינטרנט הן כלכך עצומות, שאין לנו נגישות אמתית. פותחים מנוע חיפוש באינטרנט ודרכו אני ניגש למידע. יש רק 5%

**האם באמת האינטרנט מגשים את חזון הביזור והחופש?**

מודלים חדשים לייצור והפצה של תוכן. מה למשל?

* שליטה של תאגידים פרטיים על סביבת התוכן =>איומים חדשים על חופש הביטוי והאוטונומיה של הפרט
* הרשת עצמה אינה פלטפורמה ניטרלית - זו תשתית טכנולוגית שבכוחה להבנות את השיח ואת הפעילות האנושית בה. האתרים של האינטרנט יוצרים פרופיל רשת משלנו, יש חשיפה לכתבות בהתאם להעדפותינו. , יש השפעה ריכוזית על פעילות האתרים. ריכוזיות הזו יש אלמנטים טכנולוגים, שכן אלגוריתמים הם שקובעים זאת על סמך דפוסי התנהגות קודמים. (=>זכרו את מודל לסיג).
* לא רק שיח: מסחר, מערכות יחסים, שירותים, קהילות.

**מודלים חדשים - איומים חדשים- שלטון תאגידים**

לגורמי הביניים כוח משמעותי להבנות, להגביל ולשלוט על הפעילות ברשת.

התפישה של האינטרנט כמקדם אבסלוטי של חופש המידע, חופש ביטוי, חופש יצירה, חופש עיסוק -נדמית כיום כמיתוס.

מודלים חדשים יצרו איומים חדשים ואם בעבר היו מדברים על כוח המדינה או הצנזורה לשלוט על השיח ולעשות רגולציה לפעילויות ולהגביל ועצב את פעולות האזרחים, אז היום מדברים על הכוח המאוד חזק של התאגידים האינטרנטיים במיוחד שאלו צוברים כוח.

The big four – חברות טכנולוגיות הגדולות ששולטות בהיבטים נרחבים באינטראקציה באנושית כיום: גוגל, פייסבוק, אמזון, ואפל. לחברות אלו יש נתח שוק גדול מאוד והשפעה אדירה על כמות עצומה של אנשים בעולם.

**מתווכים ברשת האינטרנט – Internet Intermediaries**

גופים, לרוב למטרות רווח שמאפשרים ביצוע התקשרויות/עסקאות בין צדדים שלישיים באינטרנט. הם עושים זאת באמצעות סיפוק שירותי אינטרנט מקוונים. הם נותנים גישה לשירותים, מאחסנים מידע, משדרים אותו, מאנדקסים תוכן, או שמספקים מוצרים ושירותים מקוונים שהמקור שלהם הוא צד שלישי (תמיד מתווכים ברשת)

**לדוגמא:**

1. ספקיות הגישה - בזק, 012, נטויז'ן - ISP. גורם מתווך זה מאפשר לגשת לרשת.
2. שירות אחסון אתרים.
3. מנועי חיפוש/פורטלים
4. אתרי תיווך ומסחר.
5. מערכות תשלום מקוונות.
6. פלטפורמות להפצת תוכן אשר לא יוצרות את התכנים המופצים בעצמן.
7. המדיה החברתית (פייסבוק, טוויטר).

**סוגים של גורמי ביניים:**

1.   **ספקיות הגישה לאינטרנט:**  מקצה לכל משתמש שם וכתובת המאפשרים לו להיות מחבור לרשת (אינטרנט זהב, בזק)

2**. ספק תוכן ושירותים:**

א. מציג תוכן באתר לשם הפצתו בין משתמשים  (למשל: וואלה, ווינט)

ב. פלטפורמות מסחר ושירותים (איביי, אמזון)

**המאמר של אורלי**

1. אורלי מדברת על 3 דורות של מתווכים ברשת:
2. **דור ראשון** - אותם מתווכים שמאפשרים שיתוף/קישור למידע.
3. **דור שני** - מאפשרים אינטראקציה/טרנזקציה כמו איביי, אמזון, העברת קבצים peer to peer - הייתה להם השפעה משמעותית על שווקים גדולים.
4. **דור שלישי** - כניסה למרחב הפיזי, חברות הפלטפורמה (platform Economy) - החיבור בין המתווכים המקוונים לבין פעילויות בעולם הפיזי - שירותים שניתנים בעולם הפיזי. AIRBNB מאפשרת לתווך בין השוכר והמשכיר ומאפשרת לגשת למידע ולפנטז איזה נכס אני בדיוק רוצה, באיזה עיר ובאיזה תנאי תשלום, אבל בסוף השירות הוא פיזי לחלוטין - מחליף מלונות. Uber - תעשיית המוניות. היכולת להשתמש בנהגים פרטיים כנהגי מונית. האפליקציה מתווכת בין הצרכן שרוצה לנסוע לנהג שמבקש להשתמש במשאב שלו כדי להפיק רווחים. Eat With - מאפשרת לאנשים למכור ארוחות, לאכול עם עוד אנשים, להכיר חברים.
5. **ביחס לכל מערכות אלו יש לנו אתגרים ושאלות משפטיות שעולות:**
6. באיזו מידה למתווכים יש אחריות על הפעילות של המתווכים והשירותים שלהם?
7. באיזו מידה ראוי להפקיד בידי מתווכים סמכויות משטור, רגולציה ואכיפה?
8. באיזו מידה מתווכים צריכים להיות כפופים לרגולציה דומה לזו של נותני שירותים בעולם הפיזי? האם זה רק שירות תיווך או יותר מזה?
9. **איזה תפקיד ממלאת מערכת הממשל העצמי של גורמי הביניים בעיצוב נורמות והתנהגות?**
10. תנאי השימוש ומדיניות הפרטיות ממלאים תפקיד רגולטורי משמעותי
    1. חוזים אחידים שמסדירים את מערכת היחסים בין הפלטפורמה למשתמשיה
    2. הגדרת חובות וזכויות, המותר והאסור לשני הצדדים לחוזה
    3. לעיתים כלי הסדרת התנהגות בלעדי (בהיעדר יכולת אכיפה של חוקי המדינה)
11. כללי התנהלות בתוך הפלטפורמה,   השלכות חיצוניות לפלטפורמה:
    1. שימוש במידע שנצבר בפלטפורמה לרבות מידע של משתמשים + העברה לצד ג'
    2. השפעות חברתיות-פוליטיות-נורמטיביות - עיצוב תפישות המשתמשים(ציפיות לגבי התנהגויות ראויות חוקיות?)
12. האם ובאיזו מידה מתווכים צריכים להיות כפופים לרגולציה דומה לזו של נותני שירותים בעולם הפיזי? (אורלי)

האם איירבינבי צריך לקבל היתרים כמו בית מלון או אכסנייה? מתי נחצים הקווים?

**מדוע גורמי הביניים ברשת מהווים כתובת אטרקטיבית לתביעות משפטיות?**

1. ניתנים לזיהוי ואיתור בקלות
2. בעוד שתהליך זיהויו של המשתמש היחיד עלול להיות יקר וממושך, במיוחד לנוכח השכיחות של פעילות אנונימית (היום קל יותר לחשוף זהות של משתמשים) – זול ליותר להגיש תביעה נגד המתווך
3. לרוב מדובר בבעלי "כיס עמוק"
4. סיכוי הנפגע להיפרע מהנזק גבוה יותר
5. פעמים רבות הם מונע הנזק היעיל ביותר
6. מצויים בעמדה שמאפשרת למנוע באופן אקטיבי את הישנות המקרה:
7. למשל ע"י חסימת גולשים או הטמעת אמצעי סינון ועריכה שיגבילו הפצת תכנים
8. התמריץ: צמצום חשיפתם המשפטית
9. דוגמה: תביעות אסטרטגיות של בעלי זויות יוצרים בשל אחריות תורמת (פרשת נפסטר)

**קשיים בהטלת אחריות משפטית על גורמי ביניים**

1. עמימות ביחס לכללים המשפטים שחלים על גורם הביניים (הפעילות ברשת)
2. במדינה שבה רשום גורם הביניים?
3. במידה שבה גורם ביניים נותן שירות?
4. במדינה שבה מצויים שרתיו?
5. במדינה שזה מצויים המשתמשים בשירות?

**השלכות שליליות של הטלת אחריות משפטית שעל גורמי הביניים**

1. חשיפה המשפטית עלולה לייקר משמעותית את עלות הפעלתם של שירותים ברשת  - הקמת מנגוני סינון, ייעוץ משפטי התיידינות משפטית
2. צמצום מספר השירותים
3. התייקרות גישה למידע ולאמצעי ביטוי
4. ריכוזיות,
5. חשש מיצירות מוקדי כוח ברשת שיכשילו את הביזור וחובליו ל"אפקט מצנן".
6. שוני איכותי בין גורמי הביניים לבין עורכים באמצעי תקשורת מסורתיים: הכמות והתדירות של התוכן המופק ברשת - תלות במערכות סינון ועריכה שלפחות בחלקן נשענות על טכנולוגיה ואכיפה אוטומטית.
7. כלל שכללי האחריות במערת המשפטית הרלוונטית חמורים יותר, כך גובר הסיכוי שתוכן יוסר ע"י המתווך באופן יזום או על רקע בקשה להסרתו. (עדי לוביצקי)

**שיעור 3, 11.03.19**

**נושא 3 לסילבוס: גורמי הביניים כגורמי אכיפה - המקרה של זכויות יוצרים ברשת**

**זכויות יוצרים כללי**

**רקע:** מנגנונים משפטיים בתחום הקניין הרוחני הם המכשיר המשפטי שמאפשר לנו להפוך ידע מופשט לנכס שניתן לסחור ולרכוש בו בעלות. הבעלות המוקנית ליוצר או לממציא מפקיעה את היצירה או ההמצאה מנחלת הכלל לפרק זמן מוגבל על פי חוק (שימוש ביצירה מחייב את הרשאתו).

המחוקק יצר זכויות שונות בקניין רוחני. בשיעור זה נתמקד בזכויות יוצרים.

הדין הישראלי, בדומה לדין האמריקני, נוקט בגישה תוצאנית: **הגנה על זכויות יוצרים מוצדקת ככל שהיא מקדמת תוצאה רצויה.** זוהי גישה כלכלית במהותה, הפועלת לקידום הרווחה החברתית הכולל באמצעות מתן תמריצים. למשל, תגמול ליוצרים וממציאים כדי לעודד השקעות ביצירה וחדשנות (זכות למנוע את השימוש) וכן איזון בין הפגיעה בחופש המידע (גישה לידע ושיתוף ידע) וחופש הביטוי. נשאל מי ראוי שיבצע את האיזון? בית המשפט וכן המחוקק. באיזה אופן אכיפת הזכויות ברשת האינטרנט היא בעלת מאפיינים מיוחדים ואילו אתגרים יש לה.

**זכויות יוצרים רקע בסיסי:**

1. מנגנונים משפטיים בתחום הקניין הרוחני, מאפשרים להפוך ידע מופשט לנכס שניתן לרכוש בו בעלות ולסחור בו, להפיק ממנו רווח וכן הלאה.
2. הבעלות שמוקנית ליוצר מפקיעה את היצירה מנחלת הכלל לפרק זמן מוגבלת ע"פ חוק (שימוש ביצירה מחייב את קבלת הרשאתו). כל מי שרוצה לעשות שימוש ביצירה צריך לקבל הרשאה מבעל הזכות באותה יצירה.
3. בשיטת המשפט הישראלית בדומה לדין האמריקאי מנגנון זה של הגנת זכויות יוצרים מוצדק בדוק' בשיטה המשפטית שלנו ע"ב תוצאתי – ככל שמקדם תוצאה רצויה. גישה כלכלית: קידום הרווחה החברתית הכוללת באמצעות מתן תמריצים (עידוד השקעה ביצירה וחדשנות ואיזון מול הפגיעה בחופש המידע וחופש הביטוי). נשאל מי ראוי שיבצע את איזון זה היום.
4. **חוק זכויות יוצרים:**
5. **ס' 47:** הפרת זכויות יוצרים = ביצוע אחת מהפעולות שיוחדו לבעל זכות היוצרים לפי סעיף 11 לחוק, ללא קבלת רשותו של בעל זכות היוצרים.
6. **ס' 11:** מעשה של העתקה, פרסום, ביצוע פומבי, שידור, העמדה לרשות הציבור, יצירת יצירה נגזרת או השכרה לצרכי מסחר. חל על שימוש ביצירה או בחלק מהותי ממני.
7. **למעט**: שימוש הוגן (ס' 19), למשל למטרות חינוך, מחקר, דיווח עיתונאי.

* שימושים שמותרים ללא רישיון (פרק ג', ס' 20-30, 32) למשל: הליכים משפטיים, ספריות.

**תביעה בגין הפרת זכות יוצרים**

1. על התובע מוטל הנטל להוכיח כי:
2. הוא בעל זכות היוצרים ביצירה שבגינה הוא תובע
3. הנתבע הפר את זכותו
4. בחוק קבועים תנאים נוספים לקבלת הגנה על זכויות יוצרים ביצירה.

**מה האתגר באמת באכיפה של זכויות יוצרים בעידן הדיגיטלי?**

המהפכה הדיגיטלית והנגישות של כלים ליצור, להפיץ, לשתף, לחלוק, לשמוע... הפכו את היכולת לשכפל ולהשתמש ביצירות לכל-כך קלה וכל-כך מהירה ונגישה, שההפרה של זכויות יוצרים יכולה וגם בפועל מתבצעת בקנה מידה מאוד רחב, ובאמת כמעט כל אחד שעושה שימוש באינטרנט וברשתות חברתיות באיזשהו שלב הפר זכויות יוצרים. יש ציבור מאוד גדול של מפרים פוטנציאלים. מעגל המשתתפים הוא פשוט עצום. כתוצאה מכך, כדי להיות יכול לאכוף את זכויות היוצרים, בעלי הזכויות צריכים לנקוט **בפעולות אכיפה מרובות** כדי להבטיח את האינטרס שלהם. חברת מייקרוסופט משקיעה שנות עבודה במערכת ההפעלה של וינדוס כשהיא יודעת שהיא תהיה זכאית להגנה של חוקי הקניין הרוחני, ובסוף מורידים פרוץ. התגמול הכלכלי על ההשקעה לא בהכרח מגיע, ואנו כחברה רוצים שמייקרוסופט תיתן את מערכת ההפעלה החדשה שלה.

**קושי נוסף** - הזיהוי של המשתמשים הפועלים ברשת באופן אנונימי\* והיכולת להטיל עליהם אחריות ישירה על הפרת זכויות היוצרים.

* **במאמר של פרל ואלקין-קורן** - עד כמה באמת יש אנונימיות ברשת? האם באמת קיים קושי גדול להצליב מידע של משתמשים? בטלפון הסלולרי בכלל. כשאנו עושים LOGIN יש יכולת להצליב את המידע עם אמצעים מזהים, ובמאמר נטען כי הנחת האנונימיות צריכה להישקל מחדש בהיבטים מסוימים, משום שהטכנולוגיה עצמה מאפשרת כבר היום לזהות בצורה טובה יותר את המשתמשים. נדבר על כך כשנדבר על הגנת הפרטיות (הצד השני של המטבע).

**למה הפתרון של אכיפה באמצעות ביהמ"ש הוא בעייתי?**

1. זה יקר.
2. ספק אם זה בכלל יעיל.
3. יש קושי בזיהוי המשתמשים לצורך הטלת אחריות.
4. כדי לקבל את הפרטים של המשתמש שהפר, בעל הזכות צריך לפנות לספק הגישה ולקבל את הIP של המפר.

* ביהמ"ש קבעו שלא קיימת סמכות בחוק המאפשרת להם להורות לספק לחשוף את זהותו של משתמש שלכאורה ביצע עוולה אזרחית ולרוב דחו בקשות שכאלו.
* **לדוגמא** - ע"א 9183/09 The Football Association Premier League Limited נ' פלוני ואחרים (2012). בפרשה זו, אתר אפשר לצפות בליגה ללא תשלום. Primer League ביקשה לזהות את המשתמשים שיהיה ניתן לתבוע אותם, וביהמ"ש אמר כי אין לו סמכות לחשוף את פרטי המשתמשים. באותו פסק דין כבר ציינו דוקטרינות שיכולו לחייב את הספק עצמו, אבל לא סמכות של ביהמ"ש להורות על חשיפת המשתמשים.
* **ההצעה לתיקון מס' 5 לחוק זכויות יוצרים** מבקשת ליצור מקור לסמכות זו: בפרק ח'1: חשיפת זהותו של עושה פעולה בתוכן ברשת תקשורת אלקטרונית.

**התוצאה - פנייה לגורמי הביניים**

1. התוצאה של המגבלות האלה של האכיפה באמצעות בתי המשפט הייתה באופן לא מפתיע, שבעלי זכויות היוצרים חיפשו אסטרטגיות אחרות. מאותם שיקולים הם פנו לגורמי הביניים.
   1. **גורמי הביניים:** מונע הנזק הזול - מנהלי אתרים, מנועי חיפוש, רשתות חברתיות וספקי אינטרנט.
   2. **המטרה:** פנייה זו קיימת מראשית רשת האינטרנט. בשנים האחרונות עקב ההתפתחות הטכנולוגיות ועוצמת ההפרות מצד משתמשים יש התעצמות באמצעים שהם נוקטים. היקף פעילות האכיפה באמצעות גורמי ביניים גדולה משמעותית מהאכיפה שמבוצעת על ידי בתי המשפט.
   3. **האמצעים:** בעיקר אמצעי אסדרה טכנולוגיים:
      1. פיקוח על השימוש ביצירות שהופצו באופן דיגיטלי וזיהוי הפרות
      2. כמו כן יש אמצעים טכנולוגיים שמונעים מראש העלאת והפצת תכנים שפוגעים בזכויות יוצרים אפשרות למניעה מראש של גישה/הפצה לא מורשית של יצירות.
      3. נקיטת פעולות לאחר זיהוי ההפרה - יכולים להסיר באופן אוטומטי ע"י רובוטים וכו'.

**אילו קשיים מעורר מודל אכיפה שנשען על גורמי ביניים פרטיים, באמצעים טכנולוגיים:**

1. הפרטת אכיפה - איזון זכויות (נעשה ע"י גורמים פרטיים ולא ע"י מחוקק/בימ"ש)
2. בעלי אינטרסים מסחריים
3. היעדר שקיפות, קושי בפיקוח, היעדר בקרה שיפוטית, וזאת בניגוד לגורמים מנהליים

* **"הקופסה השחורה"** של מנגנוני האכיפה הטכנולוגיים – האופן שבו החברה פרטה את מדיניותה, את האיזון שהיא עושה על הגנה על זכויות יוצרים והזכויות המתחרות לתוך שורות קוד שמזהות את התכנים המפרים, לתוך מנגנונים מסוימים שהיא בוחרת להפעיל של חסימה לגישה לתכנים, וכל מנגנון כזה שנבחר פוגע באיזון הזכויות במידה כזו או אחרת (הזכויות הן חופש הביטוי, חופש למידע, חופש העיסוק וכו'). (עדי לובוצקי)

**סוגי אמצעי אסדרה טכנולוגיים**

1. **מנעולים דיגיטליים על היצירה עצמה (דוג') -** הגבלת הגישה למוצר בו מאוחסן התוכן המוגן בזכויות יוצרים.
2. הגבלת העברת מידע ברשת (חסימת גישה) - מוטלת באופן טיפוסי בעיקר על ספקיות גישה, ספקיות מארחות, מנועי חיפוש, בעלי אתרים, פלטפורמות שיתוף קבצים, אמצעים טכנולוגיים שונים מבוססי IP, DNS, URL וכו'...

**אחריות גורמי ביניים להפרות שביצעו משתמשיהם**

1. **אחריות ישירה** (לא עושים).
2. **אחריות עקיפה** - נעשית היום בדין הישראלי בעיקר על בסיס **דוקטרינת ההפרה התורמת**. הבסיס לה הוא **נוהל הודעה והסרה** (כמו שיש בארה"ב).
3. **בפרשת על השולחן** ראינו את העימות של נוהל הודעה והסרה מצד דיני זכויות היוצרים (שקשור ללשון הרע).
4. **פרשת שוקן** התעסקה בגורמי ביניים בעולם הפיזי שם הוצגה הדוקטרינה.
5. **פרשת רוטר** - הדוקטרינה הזאת הוחלה גם על מתווכים גורמי ביניים ברשת.

מה המצב המשפטי הזה אומר?

* אין אחריות ישירה על גורמי הביניים בגין פעולות שבוצעו על ידי המשתמשים (בכפוף לנוהל הודעה והסרה).
* חשוב להבחין את המקרה הזה לבין מקרה שבו גורם הביניים הוא אחראי בעצמו להפרה -לדוגמא, כאשר האתר עצמו מפרסם הודעה/לינק/קובץ שהוא מפר. הוא כן יהיה אחראי במקרה הזה והוא לא גורם ביניים. המצב המשפטי הזה דומה למצב שקיים בארה"ב ובאירופה.

אז מה כן?

* אחריות משפטית עקיפה. **בפשרת שוקן** התעוררה השאלה הזאת. היה תא סטודנטיאלי באוניברסיטה העברית - הוא שכפל יצירה שהוצאת שוקן היו יוצרים בה, והוא כרך ומכר אותה ללא אישור האוניברסיטה. בית המשפט דן בשאלה מה היו התנאים באחריות של גורם הביניים במקרה הזה? התנאים שנקבעו הם:

1. הפרה ישירה בפועל

2. ידיעה ממשית של המפר התורם (האוניברסיטה) על ההפרה - לא מספיק ידיעה קונסטרוקטיבית

3. שלגורם הביניים תהיה תרומה משמעותית, ניכרת וממשית לביצוע ההפרה.

השורה התחתונה - האוניברסיטה לא חויבה. לא הייתה לה ידיעה ולא תרומה משמעותית.

* בסמוך ליציאת פסק הדין הזה, היה **המקרה של רוטר:** **הרקע -** גולשים פרסמו באתר קישורים לאתרים אחרים ששם הועלו יצירות ללא הרשאה (סרטים, סדרות...) העיקרון שנקבע בפסק הדין הוא שלא תוטל אחריות להפרת זכויות היוצרים על בעל האתר אם הוא לא ידע עליה, ובתנאי שכשנודע לו עליה, הוא הסיר את הפרסום המפר. **המשמעות:** מתן חסינות לגורמי הביניים מפני אחריות להפרה תמורת ניהול מנגנוני הסרה של תכנים מפרי זכויות יוצרים. בנוסף, גורמי הביניים ברשת הפכו לזרוע אכיפה בתחום זכויות היוצרים.

מצבים חריגים בהם תוטל אחריות על גורם הביניים בגין פעולות משתמשים - כותרת

**"עידוד":** האתר מעודד פרסום קישורים מפרים - נלמד מאופי השיווק האתר ושמו, תקנון הפורום והאמירה הכוללת לגולשים.

**"הפורום הפסול"**: הפורום משמש, רובו ככולו, להצבת קישורים לאתרים מפרים (גם אם יש לו נוהל הודעה והסרה - זה לא יתן לו הגנה). הקביעה נעשית בשני אופנים:

1.    **מבחן אבסטולוי -** מספר הקישורים לאתרים מפרים

2.     **מבחן יחסי -** אחוז הקישורים המפרים ביחס לכלל ההודעות בפורום

כללי אצבע היוצרים חשד "לפורום פסול" (רוטר)

**בפורום סגור**

* הכניסה אליו מוגבלת בתשלום או באופן אחר
* קשה יותר לבעלי זכויות היוצרים לבצע את הפיקוח
* 10 קישורים מפרים
* הודעות הכוללות קישורים מפרים מהוות יותר מרבע מההודעות המהותיות בפורום.

**בפורום פתוח**

* לפחות מחצית מהתוכן המהותי של הפורום יהיו הודעות הכוללות קישורים לאתרים מפרים
* ההנחה שיש לנו פורום פסול אומרת שיש איזשהי חזקה שבעל האתר מודע לכך שהוא מסייע לקיו של הפרות ישירות ואנו מבינים שבגלל שגורמי הביניים והבמה שהם מספקים וכי סיוע זה הוא בגדר תרומה ממשית ומשעותית להפרות על בעל האתר הנטל הוכיח אחד משנים: להמשך קיומו של הפורום יש ערך לגיטימי או הוא לא ידע על היקף הפעילות הפסולה (ולכן, לא יישא באחריות אלא לאחר שנמסרה ו הודעה על כך שמדובר ב"פורום פסול").

**שיעור 4, 18.03.19**

**נושא 4 לסילבוס: אכיפה אלגוריתמית וסעדים טכנולוגיים -זכויות יוצרים ברשת האינטרנט:**

נושא זה הוא נושא פרדיגמטי-מרכזי שמסביר את הקשר בין המשפט והטכנולוגיה, איך מתפתחים כלים טכנולוגיים שמשפיעים על המשפט. בשבוע שעבר למדנו רקע בסיסי על זכויות היוצרים. **השוואת פעילות אכיפת זכויות יוצרים ברשת בבתי המשפט ובקרב גורמי הביניים (אלקין-קורן ובר-זיו):**

* + - 1. **בתי המשפט -** תביעות של בעלי זכויות יוצרים בגין הפרת זכויות יוצרים ברשת
      2. **גורמי ביניים -** בקשות של בעלי זכויות יוצרים לנקוט אמצעי הסרה, חסימה וסינון בגין הפרת זכויות יוצרים. במחקר: בקשות מגוגל להסיר דפים ואתרים מתוצאות החיפוש.
      3. **בתי משפט -** 99 תביעות.
      4. **לגוגל בלבד** הוגשו 2,556 בקשות הסרה (ממנוע החיפוש של גוגל בלבד). מבחינת היקף האכיפה גורמי הביניים משחקים תפקיד הרבה יותר משמעותי מבית המשפט.

**ממצאים מרכזיים: אכיפה בבתי המשפט:**

1. **משרתת מגוון מצומצם של תובעים, במענה לסוג מצומם של יצירות:**
2. **61**% מהתביעות לאכיפת זכויות יוצרים - בצילומים
3. פחות מ-3% מהתביעות לאכיפת זכויות יוצרים - בתוכנה.
4. **הסעדים המבוקשים:**
5. 60% מהתובעים ביקשו סעד כספי בלבד
6. 38% מהתובעים ביקשו צווים שונים ופיצויים (לרבות ללא הוכחת נזק)
7. **הליכים רבים מסתיימים בפשרה ללא הכרעת ביהמ"ש:**
8. עדות לניסיון להפעיל לחץ על הנתבעים להפסיק את פעילות ההפרה
9. לא נוצר כלל משפטי (תקדימים, הנחיות לפרשנות החוק או היקף ההגנה על הזכויות)
10. **שחקנים חוזרים**
11. למשל, ארגון זיר"ה (זכויות יוצרים ברשת האינטרנט) עושה שימוש אפקטיבי בהליך המשפטי.

**בקשות הסרה מגוגל**

אז הגענו לדבר על הממצאים ביחס להסרה ממנוע החיפוש של גוגל. מנוע זה הפך למנגנון כלכך מרכזי, כך שכגורמי ביניים, מנועי חיפוש כוללים את כל מה שנגיש לעולם. אם אתה לא נמצא בתוצאות החיפוש - יהיה קשה מאוד למצוא אותך והחשיפה לאתר תהיה מינימלית. לכן מבחינת העותרים, הפנייה לגוגל (כצד שלישי) מקטינה משמעותית את הפגיעה בזכויותיהן.

**בקשות הסרה** - מישהו בעל זכויות יוצרים "לכאורה" מבקש מגוגל לאכוף את הזכות הזו "לכאורה" על ידי הסרה של קישורים שמפרים "לכאורה" מתוצאות מנגנון החיפוש של החברה. בהשוואה לביצוע של מבחנים משפטיים יותר משמעותיים, כאן יש לנו רק טענות (רק כתב תביעה). בפועל, כשגוגל מקבלת בקשת הסרה, כדי שתהנה מנוהל בקשה והסרה – היא מסירה. לפחות יש לנו שקיפות לגבי הנתונים ביחס לבקשות ההסרה שהתקבלו אצלה.

בישראל, בתקופת המחקר החוקרות מצאו שנשלחו 7091 תלונות על הפרת זכויות יוצרים ב219 שמות מתחם ישראליים ([www.biu.ac.il/XXXX](http://www.biu.ac.il/XXXX)). המספר הקומפרבילי שניתן להשוות אותו - הוא שבאותה תקופה הוגשו 190 תיקים שעניינם הוא הפרת זכויות יוצרים באינטרנט. בבקשות הסרה חברות תוכנה הגישו את מספר התלונות הגבוה ביותר, והדרך היעילה ביותר להסיר הייתה באמצעות מנועי החיפוש.

**מספר שחקנים חוזרים בולטים שפעילים בהגשת בקשות הסרה**

1. בעיקר חברות רב לאומיות בתחום התוכנה וחברות סרטים
2. חברת מייקרוסופט הגישה את מספר התלונות הגבוה ביותר - חברת מייקרוסופט יכולה להפעיל אלגוריתם כדי לאכוף.
3. גוגל מפרסמת נתונים גולמיים (עולמיים) ביחס לבקשות הסרה שהתקבלו אצלה בדו"חות שקיפות תקופתיים.

**איך עובד המנגנון הזה?**

המנגנון מוצג כמנגנון פשוט ויעיל לבעלי זכויות היוצרים. יש טופס אינטרנטי פשוט למדי = בעל זכויות היוצרים שולח בקשה להסרת התוכן המפר, יש משפט על כך שהצוותים (האלגוריתמים) בודקים את הבקשה בקפידה, ואם לא חסרים פרטים ולא מוצאים בעיה – כתובת האתר מוסרת. כתובות אתרים שהמדווח ביקש להסיר - 3,373,005,572. דומיינים שצוינו - 1,689,765, בעלים של זכויות יוצרים - 135,891, ארגונים שדיווחו - 121,212. רואים שיש כאן שחקנים חוזרים.

**הליך בקשת ההסרה כמתואר בגוגל**:

1. "אם הודעת הסרה שאנחנו מקבלים מתבררת כחוקית, חוק זכויות היוצרים דורש מאיתנו להסיר את התוכן מהשירותים שלנו – במקרה זה, להסיר כתובת אתר מתוצאות החיפוש.
2. כאשר אנחנו נוקטים פעולה בתגובה להודעת הסרה בגין הפרת זכויות יוצרים אנחנו מיידעים את מנהל האתר המשופע מפעולה זו
3. אם מנהל האתר הרלוונטי או ספר התוכן המדובר סבור שהתוכן אינו מפר ז"י או שההודעה הוגשה בטעות, הוא יכול להגיש הודעה נגדית.
4. אנחנו בודקים את כל ההודעות הנגדיות ומחליטים אם להחזיר את התוכן".

**נוהל הודעה והסרה = היפוך נטל הראייה?**

המוציא מחברו עליו הראיה?

• הודעה  = ככלל, היא מובילה להסרה – למרות שמדובר רק בטנה להפרה ולבעלות בזכות.

• פעמים רבות – ההודעה מבוצעת אף היא באמצעים טכנולוגיים.

• עקרונית, מפרסם התוכן המפר יכול ל"ערער" על החלטת ההסרה

• לפנות לגורם הביניים ולבקש לבחון מחדש את ההחלטה.

* חשוב להגן על זכויות היוצרים כדי לעודד חופש ביטוי, ושיח אך יש דילמה כי בעולם האינטרנטי

**לקחים מיישומו האלגוריתמי של נוהל הודעה והסרה בארה"ב**

יש לנו כמה לקחים - **הDMCA האמריקאי.** אנו יכולים לקבל Fast Forward למה שקורה כשניתן כוח אכיפה ואחריות לגורמי הביניים. אף אחד מהמסקנות הללו לא יפתיעו אותנו - זה הסיכום והסגירה של הנושא, לא ניפגש בו עד שניקח את הקורס בקניין רוחני. הDMCA קובע נוהל הודעה והסרה לפני 20 שנה. מנגנון הודעה והסרה **הפך** את נטל ההוכחה המסורתי בדיני זכויות היוצרים - קודם כל מסירים כדי להימנע מאחריות, וכל ה-לכאורה הופך להיות בפועל בלי שנעשתה בחינה משפטית.

הבעיה שלנו, היא התמריץ של גורמי הביניים - אנו לא מטילים אחריות על הספקים אם הם הסירו בתו"ל חומר לגיטימי. אבל אם הספק ידע "לכאורה" שיש הפרה של זכויות יוצרים, די בכך שהייתה זכות יוצרים כדי שהוא ימצא אחראי באחריות תורמת להפרה. הסיכון המשפטי עצום אם לא הורדתי את התוכן שלכאורה מפר, בהשוואה ללהוריד תוכן בכל מקרה. לכן השיקול העסקי הברור הוא **להסיר**, ומי שמשלם את המחיר זה שאר הזכויות. לנו כציבור יש **פחות חופש מידע באינטרנט.** **בפועל** - הרבה מבעלי הזכויות מנהלים את הזכויות באופן אוטומטי. בקשות ההסרה נעשות באופן אוטומטי. גם גורמי הביניים שמעבדים ומטפלים באופן אוטומטי מקבלים הכרעות באופן אוטומטי לגבי זכויות היוצרים מכורח המציאות, וגם הופכים את זה למשהו שקורה באופן וולנטרי - אפילו בלי שבעל זכות ביקש שנסיר, אנחנו אקסטרה זהירים - אנו פשוט מונעים מראש. **לדוגמא** - מערכת הContent ID שמסירה תוכן חשוד (גם אם הוא לא היה עומד במבחן המשפטי כתוכן מפר)

**הישענות על טכנולוגיות סינון ושיטור פרטיות**

גורמי הביניים הם אלה שיפתחו את הטכנולוגיה ע"מ לזהות תוכן מפר ולפעול בהתאם. המשמעות היא אם כך, היא שחברה פרטית (בעלת אינטרסים משל עצמה, ואינה גוף ציבורי שאמור לאזן ואמון על האינטרס הכללי) היא זו שתעצב את השיקולים הנוגעים להגנה על זכויות יוצרים מול אינטרסים אחרים, תוך שלמעשה היא מתרגמת את שיקול הדעת הזה, לתוך אלגוריתם (שמהווה סוד מסחרי, לכן לא ניתן לדעת באיזו מידה משפיעים האינטרסים על האלגוריתם. כך לסיכום:

o       שיקול דעת אלגוריתמי

o       מושפע מאינטרסים פרטיים, כלכליים בעיקרם, של הפלטפורמות המפעילות.

o       העדר שקיפות (סוד מסחרי)

o       דוגמא לאכיפה אלגוריתמית (שיש בה גם יתרונות) : מערכת ה – Content ID של יוטיוב שהפכה למודל עסקי מצליח למיסחור יצירות מוגנות בזכויות יוצרים. מערכת זו יצרה מודל חדש בו בעל זכות היוצרים יכול לגבות את התשלום על התוכן שלהם, גוגל יכולה להציע למי שהפר את זכות היוצרים פשוט לשלם את התמלוגים לבעל הז"י.

גם בעלי הזכויות נעזרים בטכנולוגיה כדי לזהות הפרות ולשלוח אוטומטי של בקשות הסרה של תוכן.

החשש:

o       טעות בזיהוי הפרות

o       בקשות שמבוססות על דרישות לא לגיטימיות

דוגמא: בקשה להסיר תוכן מוגן, כאשר השימוש מותר על פי החוק  (למשל – שימוש הוגן).

החשש הוא שהמציאות המשפטית מעודדת ניטור וחסימת יתר, כשלציבור אין יכולות לשלוט על כך גם ללא פיקוח שיפוטי וגם ללא ציבורי אפקטיבי.

גורמי הביניים מתומרצים לנקוט אמצעים להפחתת הסיכון המשפטי

חסימה רחבה של תכנים או משתמשים

גם מראש (לטובת מניעה)

באמצעים טכנולוגיים לצורך התמודדות עם היקף הפעילות הנרחב (אך במחיר...)

התוצאה היא עיצוב מציאות טכנולוגיות שמאפשרת שליטה, ניטור ומעקב

פתח לניצול לרעה של מנגנון ההודעה וההסרה (תלונות שווא)

**איזון ערכים חברתיים באכיפה על ידי גורמי הביניים**

נדרשת מעורבות טכנולוגית על ידי גורמי הביניים, אבל אנו צריכים לזכור שכאשר אנו מבצעים אכיפה על ידי גורמי הביניים אנו צריכים לאזן ערכים נוספים. אין לנו כאן הגנה על הקניין של זכויות היוצרים בלבד - יש את חופש הביטוי, חופש המידע, התפתחות זירת המסחר, השוק החופשי... גם האינטרסים הללו עדיין כאן. יש לנו שאלה מהותית - באיזו מידה גורמי הביניים מגנים גם על האינטרסים האלה? אם אנו חושבים שיש הגנות על האוטונומיה של הפרט במנגנונים של גוגל – התשובה לא מאוד ברורה. בנוסף, אין לנו כל כך יכולת לפקח - לא לנו כציבור, לא לבתי המשפט ולא לרגולטורים שההליך המופעל אכן משיג איזון ראוי בין ערכים אלו. לא מדובר בתפיסה תיאורטית - היא הוכרה גם על ידי ביהמ"ש העליון שלנו בפרשת מור - החשיבות של שמירה/איזון בין האינטרסים השונים הגלומים ברשת. החשש הוא שבגלל המציאות הזאת, אנו נתמרץ במציאות המשפטית שנוצרה את גורמי הביניים לפעול יותר מדי. לחסום תכנים ומשתמשים כדי לנהל את הסיכונים המשפטיים שלהם, וגם מראש! (פשוט למנוע פרסום). יש לנו קושי שבאמת קשה להתמודד איתו בהתחשב במציאות הטכנולוגית - מדובר במנועים אוטומטיים ששולחים הודעת הסרה באופן אוטומטי. גם לבעלי זכויות היוצרים ואפילו מי שאינם בעלי זכויות היוצרים יש פתח להגיש תלונות שב – כי הביקורת לגבי עד כמה התלונה מוצדקת היא יחסית מועטה.

**דרכים לצמצום או מניעת הסיכונים**

דרך אחת היא להציע מנגנון ערעור, הקושי הוא שההליך מטופל באופן אוטומטי. הבעיה תוכל להיפתר באמצעות הטכנולוגיה – אבל זה יהיה בעתיד (FAIR USE אוטומטי).

1. בשלב הזה, באמצעות פיקוח חיצוני (ולא רק פנימי) אנו יכולים לדאוג מבחוץ ליצירת כללים ברורים בדבר טיפול בתלונות. למשל - לחייב את המתלונן להזדהות, או לנקוט באמצעים מינימליים לבירור זכויותיו.
2. שקיפות לגבי היקף שיתוף הפעולה בין גורמי ביניים לבעלי זכויות – אנו לא יודעים בדיוק איך עובד מנגנון ההתממשקות בין מיקרוסופט לגוגל, כמו מה הם נדרשים להוכיח?
3. שקיפות לגבי אופן הפעולה של מנגנוני האכיפה של גורמי הביניים - זה גם היה עוזר אם היה לנו קצת יותר מידע לגבי אופן הפעולה בנוגע לתהליך הפעולה וההסרה.

מדובר בסעדים שגורמי הביניים פתחו סביב נושא הDMCA, הודעה והסרה והסדרים דומים בעולם המערבי.

**האם ראוי שגורמי ביניים יופקדו על האכיפה?**

1. הפרטה: הפקדת האחריות לביצוע איזון ערכים בידי גורמי ביניים פרטיים
2. טכנולוגיה: איזון הערכים מבוצע בכלים טכנולוגיים - אכיפה אלגוריתמית
3. העדר פיקוח: הפועל, לא קיימים ביקורת שיפוטית או פיקוח ציבורי (רגולטורי) אפקטיביים על אופן הפעולה של גורמי הביניים
   1. העדר שקיפות
   2. קושי טכני - הבנת המשמעויות של קוד התוכנה

**אמצעים לצמצום או מניעה של הסיכונים**:

1. יצירת כללים ברורים בדבר טיפול בתלונות
   1. **למשל:** הזדהות המתלונן, נקיטת אמצעים מינימליים לבירות זכויותיו.
   2. שקיפות לגבי היקף שיתוף הפעולה בין גורמי ביניים לבעלי זכויות.
2. שקיפות לגבי אופן הפעולה של מנגנוני האכיפה של גורמי הביניים.
   1. סטנדרטים לבקשות ההסרה, כיצד נעשית בחינת הבקשות ודוחות מפורטים לגבי דפוסי בקשות והחלטות ההסרה.

עד כאן היינו בעולם הפרטי בין בתי המשפט לגורמי הביניים. **מעתה גורמי המשפט עובדים באמצעות גורמי הביניים:**

**אכיפה באמצעות גורמי ביניים וסעדים טכנולוגיים: המקרה של צווי הגבלה גישה**

1. אכיפה של צווי ביהמ"ש באמצעות גורמי הביניים, למשל: צו הגבלת גישה לאתרים מפרים
2. אכיפה טכנולוגית עצמאית מצד גורמי הביניים, למשל: זיהוי והסרה אוטומטיים של תכנים

**סעדים מסורתיים**

1. תמונת העולם שנגדה אנו פועלים היא תמונה של פסיקת סעדים על ידי ביהמ"ש שבעצם דורשת הכרעה בשאלה האם התקיימה הפרה או לא.
2. היישום של צו כזה שדורש להסיר שלט פרסומת שמפר זכויות יוצרים. זהו יישום שקוף בעולם הגשמי שקורה פעם אחת באופן שבו ביהמ"ש מורה עליו.

**סעדים טכנולוגיים**

1. יהיו כפופים בד"כ להליך משפטי מקוצר, ולא בהכרח תהיה הכרעה מהותית בשאלת ההפרה (החובה של ביהמ"ש לשקול את כל ההיבטים שהיה שוקל בצו רגיל).
2. מי שמיישם את הצו הזה יהיה אמצעי טכנולוגי, שלרוב יהיה אמצעי דינמי ובלתי שקוף. **למשל** – אם יש לנו צורך לחסום גישה לתוכן מפר מסוים, והתוכן המפר הזה משנה את מיקומו/אופן הגישה אליו, אז גם היישום של הצו באופן טכנולוגי ישתנה כדי להתאים את עצמו למציאות (שגם היא משתנה) על ידי שינוי הקוד.

3.  פרטיה הטכניים של טכנולוגיית הגבלת הגישה (החסימה) שמשמשת ליישום הצו מגדירים את היקף התחולה והאפקטיביות של צווי ההגבלה, ולכן:

1)   מגדירים את היקף ההגנה שניתנת בפועל לזכויותיהם של בעלי זכויות היוצרים.

2)   מגדירים את האיזון בין זכויות בעלי זכויות היוצרים וזכויות בעלי התכנים, ספקי גישה וציבור המשתמשים כמו חופש הביטוי והזכות לפרטיות.

4. ההגדרה הטכנולוגית של יישום צווי החסימה נותרת בידי ספק הגישה, בהתאם לשיקול דעתו.

**מאפיינים טכנולוגיים של צווי הגבלת הגישה**

ההגדרות הטכנולוגיות קובעות את היעילות של הסעד, והטכנולוגיות השונות זו מזו לגבי היעלות, הדיוק והיכולת לעקוף אותן. חשוב לנו כציבור להתחשב גם במידת הפגיעה שלהם בתכנים לגיטימיים שלא היינו רוצים שתחסם להם הגישה. לכן לגורמי הביניים ניתן **כוח מאוד גדול**. באמצעות הבחירות הטכנולוגיות שלהם הם מייצרים הכרעות לגבי חופש הביטוי, חופש העיסוק... בעצם כל המסגרת הזו מהותית הופכת להיות נתונה תחת ההחלטות של גורם הביניים.

המצב המשפטי: **לפני** תיקון מס' 5 לחוק זכויות יוצרים:

1. מחלוקת בין בתי המשפט המחוזיים: האם נתונה להם סמכות להוציא צווי הגבלת גישה לאתר אינטרנט כנגד ספק גישה?

* **הקושי:** ספק הגישה איינו צד להליך המשפטי בין בעל הזכות למפר.

המצב המשפטי: **בעקבות** תיקון מס' 5 לחוק זכויות יוצרים:

1. התקבל בינואר 19'
2. לפי דברי ההסבר, ההסדרים החדשים נועדו לתת מענה ל"קשיי האכיפה שבהם נתקלים בעלי ז"י בצל הטכנולוגיות החדשות (אשר הן כשלעצמן רצויות)".
3. יצירת מקור חוקי לסמכות ביהמ"ש להוציא צווי הגבלת גישה שיחייבו ספקי גישה לרשת לחסום גישה למקור תוכן שמפר ז"י.

ס' 53א - "צו הגבלת גישה למקור תוכן" - סעיף הגדרות (א) ומקור הסמכות (ב), **מתווה צו הגבלת הגישה (ג).**

**מהם "אמצעים סבירים"?** **"בתנאים ובמידה שאינה עולה על הנדרש."** אין בתיקון מס' 5 איך לקבוע את הדבר הזה, מה שכן יש שיקולים שבית המשפט צריך לשקול במתן הצו ובמתן תנאיו. החוק מפרט שורה של שיקולים (ההשפעה על הציבור כתוצאה מההגבלה, חומרת ההפרה, חיוניות הצו, יעילות סעדים אחרים, מידת הפגיעה בגישה למקורות תוכן אחרים, פגיעה בפרטיות וכו'). **מה המשמעות של שקילת שיקולים אלה כשמדובר בסעד טכנולוגי (אמצעי אכיפה טכנולוגי) שמיושם ע"י ספר הגישה?** צו חסימת גישה יינתן רק כאשר אין יכולת לעשות את נוהל הודעה והסרה (ס' קטן ח). **ביהמ"ש מחויב לשקול שיקולים אלה גם אם לא הוגשה התנגדות**.

**אילו קשיים מעורר השימוש בצווי הגבלת גישה?**

·         מאפייניהם מקשים להכפיפם לביקורת משפטית ופיקוח ציבורי:

·         **הוצאת הצווים** כפופה לפיקוח שיפוטי מראש

·         **יישום הצווים**, לרבות הגדרת פרטיהם הטכניים, נתון בידי גורמי ביניים פרטיים

o       גלם פני תיקום מס' 5: ביהמ"ש נדרש לשקול שיקולים שונים בקביעת תנאי הצו, אך אינו נדרש לקבוע מהם אמצעי ההגבלה המידתיים ביותר בנסיבות.

·         **העברת השליטה על האכיפה לספקי גישה פרטיים**

o       חשש שיפעלו למקסום רווחים ובהתאם לשיקולים עסקיים

o       חשש שיעוצבו מנגנונים בלתי צודקים ומוטים

·         **חשש שהמשטר המשפטי יתמרץ אכיפת יתר וייצור אפקט מצנן:**

o       כדי להימנע מאחריות משפטית ביחס ליישום הצווים (+העלויות הכרוכות בכך) גורמי הביניים עשויים ליצור תשתית וטכנולוגית פרטית שתימנע את אחריותם שלא באמצעות ביהמ"ש, וללא פיקוח משפטי או ציבורי

§         = הגבלת גישה לאתרים המארחים חומרים מפרים

·         זו סכנה כללית שטבועה בסעדים טכנולוגיים שמיושמים ע"י גורמי ביניים:

o       הרעה בדירוגן של תוצאות חיפוש בקשורות להפרת ז"י ברשת

o       הסרה אוטומטית מראש של תכנים מפרים לכאורה

**שיעור 5 25.03.19**

**נושא 5 לסילבוס: יישוב סכסוכים בעידן הדיגיטלי: ממסחר מקוון לבהמ"ש נגישים**

ODR-Online Dispute Resolution - יישוב סכסוכים מקוון:

·        מונח זה  נולד כתוצר משתי מגמות בעלות:

o       מגמת הדיגיטציה - יצירת מרחב חדש של פעילויות בזירה המקוונת

o       מגמת החשיבה המחודשת על האופן שבו אנחנו פותרים סכסוכים בחברה, תנועה של פתרונות סכסוכים חלופיות שטוענת שלא כל סכסוך צריך ליישב בביהמ"ש.

·         ODR הוא תוצר של שתי מגמות אלה – מערכות ליישוב סכסוכים שמאפשרות להשלים את ההליך במלואו (מהגשת התביעה/תלונה/הערר ועד לסיום בהכרעה או הסכם) על גבי פלטפורמה מקוונת.

o       לעיתים מתאפשרת גם אכיפה באופן מקוון

·         זהו מונח גג - מקורות וסוגים של סכסוך; שיטות יישוב סכסוכים; טכנולוגיות; תהליכים

·         **קולין רול** היה מנהל יישוב הסכסוכים הראשון בחברת "איביי" והחברה נתקלה בבעיה - השירות שלה היה מאוד פופולארי, בשלבים מוקדמים התמודדה עם 60,000,000 סכסוכים בין מוכרים לקונים, על סכומים של 100 דולר בממוצע, המוכר והקונה הגיעו ממדינות שונות ß סמכות שיפוט שונה, ללא עו"ד, אמון מול עלויות. כשעלות הסכסוך לא מצדיקה פנייה לביהמ"ש איביי נדרשה להעלות את האמון בה תוך צמצום עלויות.

o       כל זה הוביל למערת ה-ODR הפרדיגמטית. קולין רול יצר פתרון עבור החברה.

·         30 שנה קדימה, שנת 2015, השופט בריגס (אנגליה) נקרא לדגל להוציא דוח לרפורמה שתתמודד עם כמה בעיות היסוד של מערכת המשפט:

o       באנגליה יש שיעור גבוה מאוד של מייצגים עצמיים במערכת המשפט (ללא שימוש בעו"ד) כי הסיוע המשפטי היה יקר; עלויות ניהול ההליכים הייתה גבוה; עומס ומשך חיי התיקים, משך זמן רב; בעיית נגישות הציבור לבתי המשפט – הגעה פיזית, חיסור יום עבודה; מורכבות של סדרי הדין ויכולת הציבור לגשת ללא תיווך של עו"ד.

o       כל הבעיות האלה השופט בריגס נאלץ לפתור בזמן של צמצום משאבים וקיצוצים.

·         בשיעור נראה איך התמודד כל אחד מהשניים עם הבעיות.

**מה הוביל להולדתו של ה-ODR**

יישוב סכסוכים מקוון כתוצר של העידן הדיגיטלי

·         זירה חדשה של מערכות יחסים עסקיות, אישיות ואחרות - סוג חדש של סכסוכים, צורך בהבטחת אמון המשתמשים.

·         שירותים רבים מסופקים באופן מקוון - דוגמת סוכן נסיעות פעם ותכנון עצמאי היום באינטרנט

·         נגישות ומסוגלות טכנולוגית, ואפילו ציפייה לשירותים מקוונים - "ממשל זמין"

·         יזמות, חדשנות

·         ועדיין - יש פערים בנגישות טכנולוגית (Digital Divide)

יישוב סכסוכים מקוון כחלק מהמגמה ליישב סכסוכים בדרכים חלופיות (ADR – Alternative Dispute Resolution)

·         תנועת הנגישות לצדק + תנועת ה-ADR (יישוב סכסוכים בדרכים חלופיות)

o       גישור, בוררות, הערכת מומחה מקדמית, מו"מ ועוד

o       גם בתוך מערכת המשפט

·         שאיפה להגברת הנגישות לצדק

·         שאיפה להתאמת ההליך לבעלי העניין: צרכים יכולות, אינטרסים, מטרות

·         שאיפה ליישוב סכסוכים באופן מהיר, זול, נגיש, יעיל, פשוט-פרוצדורלית

·         תנועה זו רצתה להרחיב את הנגישות לצדק בכך שתרחיב את הדרכים לפתור סכסוכים בדרכים טובות יותר מאשר בדרך המקובלת - בביהמ"ש (קשה רגשית, עלויות נוספות, אות קין וכו').

היבטים שמגדירים מערכות ODR:

קיימות מערכות ששונות אחת מהשנייה בהיבטי:

·         **הסכסוך** - מסחר מקוון, משפחה (גירושין), עבודה, משפחה, עסקי? מורכבות? היכן הסכוך נולד? בעולם המקוון או הפיזי.

·         **ההקשר** - פרטי או ציבורי? מדינתי או בינ"ל? ספק השירות - עצמאי שפתח חברה לגישור, מתווך (למשל איביי), מוסדי?

·         **התהליך -** שיטות יישוב סכסוך שונות - גישור, בוררות

·         **הטכנולוגיה** - עושר הערוץ התקשורתי, סינכרוניות (בלייב עם השופט/ המגשר? או לא באותו זמן? למשל באמצעות הודעות מייל), אוטונומיות - האם המערכת עצמה היא בתפקיד המגשר או הבורר בסכסוך? ועוד.

מערכת ה-ODR כ"צד הרביעי" בסכסוך

·         **Eithan Katsh & Janet Rifkin**

o       The Fourth Party

o       מקרה פרטי של Code is Law  (לורנס לסיג)

o       עיצוב הממשק והמערכת הטכנולוגית משפיעים על הליך יישוב הסכסוך.

o       השפעה זו אינה ניטרלית בהכרח, וע"פ רוב אינה שקופה למשתמש.

·         **תפקיד אינסטרומנטלי בלבד**: מערכת ה-ODR מופעלת על ידי אדם, למשל: אמצעי תקשורת, כלי לביצוע משימות קונקרטיות שמופעל בהנחיית המגשר.

·         כל המאפיינים של מערכת ה-ODR כצד הרביעי ובנוסף:

o       **תפקיד אוטונומי** - הצד הרביעי + הצד השלישי - מערכת ה-ODR מנהלת באופן עצמאי את הליך יישוב הסכסוך, ללא צורך במעורבות של צד שלישי אנושי. במקרה זה המערכת ממלאת גם תפקיד של ניהול התקשורת והידע (החלפת המסמכים וכו' בין הצדדים) וגם מנהלת את הליך יישוב הסכסוך עצמו, אולי מכריע בסכסוך מבלי שיש צורך לצד שלישי (שם כולל למגשר, שופט וכו').

§         הסתמכות על עצי החלטה (אשף יישוב סכסוכים), הליכים מונחי בינה מלאכותית וחישוביות.

שלושה מודלים טכנולוגיים בהליכי יישוב סכסוכים (צריך לכתוב מחדש **יותר יפה**)

·         הפשוט ביותר - **העברה לסביבה מקוונת:**

o       **הרחבת הנגישות:** מיקום וזמן (מהבית, ב-21 בער. העברה לסביבה מקוונת - להעביר את התהליך כמו שהוא מתקיים בעולם הפיזי אל הסביבה המקוונת: במקום להגיע למשרד או לאולם ביהמ"ש נתקשר באמצעות וידאו, אודיו וסביבה מקוונת. היתרון הוא שמרחיבים את הנגישות להליך. במחקר נמצאו גם יתרונות כמו שליטה על רגשות בסכסוכים אמוציונליים כמו בגירושים וגם מאפשר עשיית ליטיגציה לפערי כוחות כלומר לפעמים יותר קל לצד החלש יותר בהליך להשתתף יותר כשהוא לא מול הגורם עצמו.

הרחבת נגישות מיקום וזמן; רגשות; יחסי כוחות/היררכיה.

1. עיצוב מחדש - תפיסה צרכנית - מתוכנן לשימוש עבור האדם מן היישוב: לקיחה של אבני הבניין של הליך היישוב ועיצובן מחדש מתוך תפיסה צרכנית שמי שיבצע את ההליך הוא אדם מן היישוב ולא עורך דין. כך, כמו שכל אחד יכול להשלים הליך רישום לאתר או להזמין כרטיסים לסרט באינרנט כך הוא יוכל לפתור את הסכסוך הצרכני או האחר באמצעות אתר שינחה אותו לעשות זאת בהליכים פשוטים ובשפה יומיומית. בעולם שבו אנו מפרידים את האינטראקציה כל אחד למסך שלו, ויכולים לעצב את התהליך של איסוף המידע והתקשורת של המידע לאבני בניין, לחתיכות של מידע מאפשרים חוויית משתמש שונה ומותאמת.

פישוט פרוצדורלי; מתן סיוע ומידע נחוץ לאור ההליך; אבחון אוטומטי של בעיות ופתרונות; שפה יומיומית; אימות מידע בשדות למניעת טעויות; חוויות משתמש מותאומת; הפקת מסמכים אוטומטית.

3. חידוש - היכולת להציע לעולם יישוב הסכסוכים הליכים חדשים לחלוטין, בין אם זה יכולות חישוביות מתקדמות, מערכות לומדות, שימוש ברשתות חברתיות ובמוניטין, שימוש במיקור חוץ, חבר מושבעים (בעייתיות היא חוסר המקצועיות של ההמון) ובלוקצ'יין דרכים לחשוב על פתרון סכסוכים באמצעים טכנולוגיים. בנוסף, קיימים הליכים היברידיים שמשלבים את השיטות הללו עם השיטה הקלאסית של "פנים אל פנים".

**ב אחרי שהילדים ישנים ללא הפסד יום עבודה)**

o       רגשות (נטרול סכסוכים רגשיים)

* יחסי כוחות/היררכיה (סכסוכים בעלי צד חזק וצד חלש).

**דוגמאות למערכות קיימות כאלה:**

1. **דוג' למודל ההעברה לסביבה מקוונת:** חברת MODRIA מאפשרת ניהול מקוון של הליך יישוב סכסוכים: מסמכים וראיות, תקשורת, ניסוח הסכם ועוד.
2. **דוג' להליך היברידי של מודל ההעברה לסביבה מקוונת ומודל העיצוב מחדש של ההליך:**  חברת JURIPAX -מערכת ליישוב סכסוכים בתחומי המשפחה והעבודה. המערכת עובדת עם אשף זהה ליישוב סכסוך, הצדדים מכניס את התשובות לאותו השאלון, וכך המגשר מקבל טבלה בה מסומן היכן הצדדים מסכמים והיכן לא. כך, המגשר מפנה את הצדדים למקומות בהם אין הסכמה ולהתדיין איתם שם. (גם בחברה זו יש מערכת הכוללת ניסוח שיתופי של ההסכם.)
3. **YOUSTICE:**  מודל מבוסס עץ החלטה. מותאם לצרכנים שאינם משפטנים. כולל סטנדרטיזציה של בעיות ופתרונות.
4. **LEGAL SELF HELP** - נותנת אפשרות להיעזר בטכנולוגיה גם להפקת מסמכים משפטיים סטנדרטיים.
5. **ACCESS TO JUSTICE AITHOR**  - תוכנה המאפשרת את הרחבת הסיוע המשפטי באופן קל ביותר. התוכנה מאפשרת לבעלי ידע משפטי ליצר תהליך שבסופו ניתן יהיה להפיק מסמך משפטי/פעולה משפטית. ביחס לכל שאלה שעולה באתר, עולה הסבר בשפה ופשוטה להבנה, ומדמה שיחה עם עו"ד. תוכנה המסייעת במקומות בהם יש בעיית נגישות לעורכי הדין (שלא כמו בישראל:)
6. **SMARTSETTLE מו"מ וגישור -** משתמשת באמצעים חישוביים כדי להגביר את היכולות להסדיר את הסכסוך. הפתרונות גלויים ל-2 הצדדים, אולם דירוג העדיפות לפתרונות חסוי לכל צד. המערכת מאפשרת התגברות על התנהגות לא רציונלית וניצול ההפרדה בניהול המידע. כך, הצדדים מציעים פתרונות, והמערכת יכולה לחשב את העדיפות לסכסוכים ולהציע את הפתרון באמצעותו יוכלו הצדדים להסדיר את הסכסוך מבלי לייצר מריבות ביניהם.

**קולין רול - דוגמה לפיתוח של מנגנון יישוב סכסוכים שנועד להתמודד עם סכסוכים יחודיים:**

הצרכים של איביי בתור גורם ביניים:

-          הבטחת סביבה מסחרית בטוחה ואמינה כדי לעודד עסקאות

-          צורך בגיבוש פתרון אמין, הוגן, פרטי ואכיף עבור המשתמשים

-          רייטניג / פידבק למוכרים מסייע בהרתעה והכוונת התנהגות אך אינו פתרון ממצה

-          קושי בפתרון הסכסוך בעזרת מגשר/בורר אנושי

-          יחסי עלות- תועלת בלתי אפשרי בהיקף של 60 M סכסוכים בשנה

-          עדיפות לגיבוש פתרון הסכמי פנימי ולא לשלוח לצד שלישי ויש לזכור שיש הסכם שימוש בחתימה על השימוש בה.

היתרונות של איביי כגורם ביניים:

·         שליטה בזירת המסחר והתשלום (פייפל)

o       מידע על הסכסוך

o       יכולת אכיפה

·         מסד נתונים עצום על העסקאות והסכסוכים שקרו בפלטפורמה עד אז – כך ניתן להציע פתרונות לצדדים ללא מעורבת יד אדם אנושית (חוץ מהצדדים עצמם). המערכת  לומדת מתוך ההיסטוריה של עצמה ולומדת מטעויות

o       היסטוריית פתרונות

o       מערכת לומדת שמאפשרת תובנות ושיפור מתמידים

מערכת יישוב הסכסוכים הרב- שלבית של איביי

1.    אבחון הסכסוך

2.    מו"מ / גישור מתווך טכנולוגית

3.    גישור / בוררות ע"י נציג החברה

וכך נפתרים מרבית הסכוסכים ללא מעורבות של גורם אנושי מטעם החברה.

**מערכת לומדת מבוססת נתונים, מה זה אומר?**

·         בירור עובדתי ישיר מתוך נתוני המערכת (העסקה מבוצעת על הפלטפורמה)

·         זיהוי דפוסי מחלוקת, המידע הנחוץ לפתרונן, ופתרונות שיש סבירות גבוהה לקבלתם =>עצי החלטה לתהליך המו"מ

·    **"פרסונליזציה סטטיסטית" -** כאשר מגיעים לסכסוך מסוג מסוים, אנו יודעים מה קרה בסכסוכים אחרים עם מאפיינים דומים וניתן להציע פתרונות מותאמים לסכסוך הזה ע"ב הידיעה שלנו שהיא כוללת את מה שאספנו במהלך השנים של פעילות המערכת עם הנתונים הדומים. גם על סמך מידע שלא נמסר ע"י הצדדים לסכסוך הספציפי.

**חששות וסיכונים**

**1.**      Code is Law (לארי לסיג) - הטכנולוגיה אינה ניטרלית: היעדר שקיפות לגבי אופן פעולת המערכת (ניתוב סכסוכים, הצעות פשרה), היעדר שקיפות ביחס לתוצאות.

**2.**      חשש להטיה - הכרעה בלתי שוויונית על סמך שיקולים חיצוניים לסכסוך: חשש לפגיעה בשוויון ובצדק. איביי לדוגמה יכולה לפצות משתמש מסוים מכספה ומשתמש אחר לא.

**3.**      סיפוק המשתמשים מהתהליך אינו מבטיח שהמערכת הוגנת.

**שיעור 6, 01/04/2019**

**נושא 6 לסילבוס: רגולציה בשוק עתיר טכנולוגיה - המקרה של האינטרנט של הדברים וסיבים אופטיים (עו"ד אורנן שטינברג, משרד התקשורת)**

משרד התקשורת

שוק התקשורת הוא דינאמי ועתיר פיתוחים טכנולוגיים, הרגולטור של השוק הזה הוא משרד התקשורת.

הנושאים המרכזיים של המשרד הם הדור החמישי, מיזם הסיבים האופטיים, מהפכת הסלולר, פיצול ערוץ 2 וכו'.

תחומי טלקום - תקשורת נייחת, תקשורת ניידת (פלאפונים), סלולר, גישה לאינטרנט (ולא התכנים) – יש משחק עדין בין לא לגעת בתכנים לבין איסור על תכנים, הכבל התת-ימי וכו'.

דימוי שעוזר לסייע: הרגולטור הוא אדם שרוצה לחצות כביש סואן, המשפטן הוא המסייע לרגולטור לחצות את הכביש ולמעשה לגרום לו להגיע ליעדו.

עיסוקים של הלשכה המשפטית במשרד התקשורת - משפט מנהלי, דיני רגולציה, דיני תאגידים, משפט חוקתי, משפט בין-לאומי, דיני עבודה, משפט וכלכלה, משפט מסחרי, משפט וצרכנות, דיני תקשורת ודיני תאגידים.

**משרד התקשורת וטכנולוגיה**

1.      עקרונות העל של האסדרה (מרכז התקשורת) - 2 מטרות על מרכזיות:

א. **שירותים מתקדמים מגוונים ואמינים**

ב. **מחיר סביר**

שתי מטרות העל האלה מתבססות על **תחרות**

2.      תקשורת וטכנולוגיה

יש יחס מורכב בין חדשנות טכנולוגים לבין אינטרסים של המשרד, הגדולה של המשפטנים היא לנסות להגיע לנק' האיזון הזו שבה בסופו של דבר יש הישג לשני הצדדים.

3.      הממשק עם השוק - אפשר לפנות למשרד לגבי החלטותיו.

**שני מקרי בוחן - העיקר**

1.      סיבים אופטיים

**הטכנולוגיה הקיימת/ישנה**

מבחינת הסיבים האופטיים היו פעם סיבים מיושנים, והעתיד הוא סיב אופטי – במקום כבל נחושת, מדובר בצינור זכוכית בקוטר של שערה שדרכו עובר אור.

יתרונות הסיב - צינוק קטן יכול להעביר G10 לשנייה מול M150 של צינור נחושת. אור עובר מהר יותר מאשר חשמל שעובר בחוטי הנחושת, שרידות למול חום, לחות ואש ופחות גונבים אותה. כדי שזה יוכל לתמוך ב-IOT, צריך שהנתונים יעברו במהירות.

**הטכנולוגיה החדשה**

ב-2016 בזק פרסה 60% מהארץ בסיבים אופטיים. הפריסה עצמה, שזה החסם הרציני, כבר פרוס, אך עדיין לא דולק.

**חדשנות ורגולציה**

השתלטות על הבניין מבחינת רישות סיבים אופטיים. יש מתח בין חדשנות לתחרות. הפתרון הוא **שימוש הדדי**: חברה פורסת סיבים אופטימיים בבניין מסוים, הרגולטור יחייב את החברה לתת את התשתית לחברות אחרות – אם מחייבים את סלקום לעשות את זה יחייבו כל חברה אחרת לעשות כן, גם כן. החברה מקבלת כסף...

\*שדרוג רשת בזק ל-200 מגה הוקפא עקב התערבות משרד התקשורת: טכנולוגיה קצרת טווח למול טכנולוגיה ארוכת טווח. הוחלט שבזק ישדרגו רק איפה שלא הותקנו הסיבים האופטיים – ב-40%.

**חדשנות ומשפט**

אחד הפתרונות הוא לחייב את בזק להשכיר את הטכנולוגיה לחברות נוספות כמו סלקום וכו' (**על חשבונם**)... נבחנת השאלה האם לחייב את בזק לתת לחברות אחרות להשתמש ב-60% שהיא פרסה: המתח – חדשנות למול זכות הקניין. בזק טוענת שמפקיעים לה את הקניין וזו פעולה לא מידתית. מצד אחד החברות ישלמו לבזק אך זה לא המטרה שבזק כיוונה אליה בהנחת התשתית המתקדמת.

2.      IOT (האינטרנט של הדברים)

**4 המהפכות הטכנולוגיות**

א. המהפכה הטכנולוגית באמצע המאה ה-18, מעבר ממעשה ידי אדם למכונות. שימוש בקיטור ומים.

ב. המהפכה השנייה הייתה המצאת החשמל, המצאת הנורה.

ג. המהפכה השלישית זו מהפכת המחשוב - עבודות שנעשו בצורה מכנית עברה למחשב.

ד. המהפכה הרביעית זו המהפכה הטכנולוגית - קשורה ל-M2M (משין טו משין) מאפשרת למחשב לדבר עם פלאפון, עם מקרר... היום יש כ-8 מיליארד מכשירי IOT והתחזית שה-2032 יהיו 50 מיליון מכשירים כאלה.

**חדשנות טכנולוגית**

**תשתיות חכמות -** לדוגמה שעון שנמצא על השיש במטבח, שמנתח את הנתונים וצריכת החשמל שנותן לצרכן נתונים אודות הצריכה שלו.

**תחבורה חכמה -** הכביש הופך להיות רגיש לתנועה, רמזורים חכמים, תאורה אוטומטית.

**בתים חכמים, תעשייה חכמה -** תקלה במכונית, המכונית שולחת למפעל את התקלה והמפעל עצמו

משנה את המפרט וכבר משנה את התקלה. רפואה חכמה, טכנולוגיה לבושה וכו'.

**חדשנות ורגולציה**

כל מכשירי IOT מבוססים על הספקטרום האלקטרומגנטי: ה-WIFI עובד על ספקטרום זה, לכל תחום וסוג מכשיר (משתנה בכל מדינה) יש תדרים מסוימים. הבעיה היא שהספקטרום אינו מוגבל אבל הידע שלנו בשימוש בו – מוגבל. המין האנושי לא יודע לעשות שימוש מיטבי בספקטרום, הולכים להיות הרבה מכשירים IOT כאמור, והולך להיות כאוס ספקטרלי ועומס תדרים. **המתח: חדשנות למול שלום הציבור** – ולכן הפתרונות הם הקצאת תדרים, פינוי תדרים וספקטרום לבן.

**חדשנות ומשפט**

יהיו מכשירים חכמים בעתיד בטכנולוגית IOT, הבעיה היא שזה יוצר סוג של פרופיל פיננסי, רפואי שמלווים אותנו לכל מקום - הזכות לפרטיות עולה פה בצורה משמעותית. **המתח: חדשנות למול הזכות לפרטיות**. כדי שחברה תעמוד בחובות הפרטיות צריך להשקיע ונדרשים משאבי מחשוב רבים.

תאונה של מכונית אוטונומית – הולכת רגל נדרסה ע"י מכונית אוטונומית של אובר. השאלה המשפטים שעולה פה היא: **חדשנות למול אחריות משפטית** - פעם זה היה הנהג או יצרן הרכב, כיום זה הרבה יותר מסובך - מי הנהג? נקבע שמי שמפעיל את הרכב.

**חדשנות רגולציה ומשפט**

מישהו מפעיל את הטכנולוגיה, ישנה חברית סינית שמתקדמת עם פיתו חדור 5 בסלולר, ארה"ב אמרה: "לא להשתמש בהם" אחרת ינתקו קשר עם ארה"ב – יש פחד שבעולם של דור 5, הסינים יגיעו לתשתיות המדינה מבחינה ביטחונית למשל או פרטיות.

**סיכום**

נחשפנו למבט של הרגולטור בעולם התקשורת, דיברנו על שני מקרי בוחן: סיבים אופטיים ו-IOT.

**שיעור 7,  08/04/2019**

**המשך נושא 5 לסילבוס: יישוב סכסוכים בעידן הדיגיטלי בין מסחר מקוון לבתי משפט נגישים**

**רפורמת ההליכים האזרחיים באנגליה – ביהמ"ש המקוון של הלורד בריגס**

**לורד בריגס** פרסם דוח ב2016 בו מפורטות המלצות למערכת בתי המשפט האנגלית, כשהעיקרית שבהם הייתה הקמת **בית משפט מקוון** לכל ההליכים האזרחיים עד לגבול של 25 אלף פאונד (הרחבה – לא רק לתביעות קטנות).

**האתגרים הכרוכים בייצוג עצמי**

|  |  |
| --- | --- |
| **גופים שיפוטיים** | **בעלי הדין המייצגים את עצמם** |
| **תפעול**  ·         עלויות מניעה וטיפול בטעויות בניהול ההליך  ·         עיכוב בטיפול בתיקים, סיבוך פרוצדורלי מיותר | **ידע**  ·         טעיות בדין המהותי והפרוצדורלי  ·         בחלק מהמקרים, יותר מ-50% נמחקים על הסף  ·         שיעורי הצלחה נמוכים יותר מאשר למיוצגים משפטית |
| **אתיקה**  ·         הליכים מתירים מתן מידע, אך לא מתן סיוע משפטי  ·         מתח בין ניטרליות לנגישות לצדק | **השתתפות**  ·         הצגת טיעונים משפטיים לעומת דיבור יומיומי (רגשי)  ·         הדינמיקה של השיח באולם בית המשפט - השתקה  ·         תחושות בלבול, הצפה, תסכול, חששות |

**חסמי גישה כלליים: זמן, מקום, משאבים**

דיברנו על שורה של בעיות שהלורד בריגס ביקש לפתור: שיעור גבוהה של מייצגים עצמיים (ללא עו"ד), עלויות ניהול הליך, עומס של מערכת וחיי המשפט ארוכים, נגישות – סדרי דין מורכבים שקשה לעסוק בהם, צמצום משאבים: בתי המשפט + סיוע משפטי - המערכות הציבוריות תמיד נמצאות במשבר ודורשים קיצוץ.

הלורד בריגס עשה צעד אמיץ והציע לפתור את הבעיות תוך הישענות על טכנולוגיה במערכת המשפט. הוא הוביל רפורמה (ברוחו, לא הוא) בשווי 1.2 מיליארד פאונד אנגלי עם 50 פרויקטי דיגיטציה של מערכת המשפט האנגלית, נתמקד באחד מהם.

**הבעיה הגדולה** של מערכות משפטיות ציבוריות - לא תוכננה עבור מייצגים עצמיים.

שיעור גבוה של מייצגים עצמיים - בארה"ב ובאנגליה סוגי תיקים רבים מערבים בעיקר מייצגים עצמיים (30%-75%). הסיבות לכך (לא למבחן) - עלות הייצוג, מיעוט משאבים לסיוע משפטי, חוסר אמון בעו"ד, צרכנות אינדיבידואליסטית וכו'...

**האתגר** ß מערכת המשפט - הדין המהותי וסדרי הדין - עוצבו ונוסחו ע"י עו"ד, עבור עו"ד

·         בעיית נגישות לצדק

·         חסם כניסה + טעויות בדין מהותי ופרוצדורלי

·         במהלכים מסוימים יותר מ-50% נמחקים על הסף

**Online Solutions Court**

בלב הרפורמה ישנו תהליך למעבר פלטפורמה מקוונת ושנית שהצדדים מגיעים לפיתרון בעצמם ולא בהכרעת השופט.

·         שלב 1 (מונחה תוכנה)

o       אבחון הבעיה ובחינת קיומה לש עילת תביעה, הצגת אפשרויות פעולה

o       סיוע בניסוח של התביעה/כתב התשובה כך שתובן ע"י בעלי הדין ובית המשפט

o       הוספת כלל המסמכים והראיות הרלוונטיים לתיק

·         שלב 2 ניהול הליך וניסיונות פישור (מונחה תוכנה + "מנהל תיק")

o       פעולות ניהול תיק וקידומו לפשרה

o       באופן מקוון בכתב, ולפי הצורך: בשיחת ועידה, היוועדות חזותית או פנים-אל-פנים

·         שלב 3 ניהול הליך והכרעה ע"י שופט

o       הכרעה על סמך המסמכים (במערכת המקוונת)

o       במידת הצורך: ניהול הליך או דיון בשיחת ועידה, היוועדות חזותית או באולם ביהמ"ש

האב הרוחני של הרפורמה של בריגס זהו ה-civil resolution tribunal שעשו בו שימוש בסכסוכים קטנים, בין שכנים וכו'.

**מודל הטריבונל האזרחי במחוז בריטיש קולומביה בקנדה (הרחבה על המודל הקודם) - Civil Resolution Tribunal.**

* + 1. המערכת של בריגס חסרת תקדים מבחינת היקף - עד 25,000 פאונד
    2. דווקא למערכת הוותיקה בקנדה יש שלב נוסף - **Self Help**

**יתרונות המודלים המקוונים להליכים שיפוטיים**

1. יתרונות הליכים א-סינכרוניים
   1. עבוד בעלי הדין - ללא חסמים פיזיים. יש אפשרות לבצע את ההליך מכל מקום ובכל זמן, מבלי שיהיה צורך להגיע אל בית המשפט.
   2. עבור המערכת המשפטית - עלות נמוכה יותר, ניהול משאבים של זמן, מקום, וזמן שיפוטי נכונים יותר.
2. יתרונות בניית התהליך המחודשת - פישוט, הדרכה, ייעול עבודת בתי המשפט: מניעת טעויות, ניהול מידע ותיקים יעיל.
3. מתן סיוע משפטי בזמן אמת
4. חוויות משתמש שונות - האופן שבו המידע נאסף מהתובע/נתבע, המידע שמוצע לו יהיה שונה מאשר מה שהשופט רואה.

**סיכונים שכרועים במערכת יישוב סכסוכים מקוונות**

* + 1. אבטחת מידע, אותנטיקציה וכיו"ב
    2. נגישות לחיבור אינטרנט ונגישות טכנולוגית ככלל
    3. ניטרליות/מניפולציה בתכנון הליכים

o       Code Is law - לסיג

o       מניפולציה בתכנון ארכיטקטורות בחירה (ממש המשתמש)

* + 1. צדק פרוצדורלי ואמון הציבור במערכת המשפט - הגינות באופן ניהול ההליך
    2. פומביות הדיון
    3. צדק סוג ב'?

o       **שאלת ה-bench mark:** למה אנחנו משווים את ההליך המקוון? רוב האנשים חושבים שמדברים על תהליך משפטי מלא שבסופו הכרעה מנומקת ע"י שופט.

o       רוב עורכי הדין והשופטים יגידו שזה צדק סוג ב' ושהיא לא נותנת מענה זהה למערכת המשפט כיום.

* + 1. **Code Is Law:** יש להבטיח שממשק המשתמש ותכנון התהליך אינם יוצרים **הטיות** בבחירות המשפטיות של המתדיינים. ארכיטקטורת בחירה.

**ODR בהליכים שיפוטיים בישראל**

1. נט המשפט היא תשתיתי טכנולוגית ותרבותית. יש תרבות של ישראל דיגיטלית, הטמעת טפסים מקוונים במשרד המפשטים באופן מקוון לחלויטן.
2. היתה רפורמה בתקנות סד"א התשע"ח +תפיסת ניהול ההליך.
3. העומס בבית המשפט וכן השאלה של דפוסי ניהול וסיום תיקים  ושאלת הבנצ' מרק.
4. בעיית העומס בבתי המשפט  - יש גידול משמעותי במספר התיקים שנפתחים בבית המשפט בלא שהוספו די תקני שופטים ואולמות משפט =>עיכוב  בבירור ובהכרעה בתביעות זה מוביל לריבוי פשרות, ולכך שהמפשט נמוג וכן, לכך שהשופט הופך למנהל פרוצידוארלי שמבצע פעולות שנועדו לקדם את סגירת התיק.

**הרפורמה בסדר הדין האזרחי ותפישת ניהול ההליך -** מהווה פלטפורמה של כניסת תהליכים טכנולוגים גם בישראל.

תקנות סדר הדין האזרחי, תשע"ט 2018

-          עידוד החלפת מידע

-          עידוד גיבוש הסכמות

-          הבניית פעולות רבות בהליך בטפסים או בהנחיות

o       הנחיות להגשת כתב תביעה

o       טפסים כמו "שאלון לתבוע בתביעה לנזקי גוף"

-          מיסוד של שימוש בכלים טכנולוגי בניהול ההליך

o       מסמכים אלקטרוניים, ראיות אלקטרוניות, התקנות מאפשרות לבצע להיוועדות חזותית

-          שיקול דעת שיפוטי לאפשר שמיעת ראיות בכתב (כאשר בד"כ שומעים ראיות במהלך דיון)

כל אלו לצורך התאמה ליישום באמצעות מערכת מקוונת לניהול ההליך בבית המשפט.

גם המע' המשפט של ישראל האידיאל שאנו משווים אליו רלוונטי רק לתיקים קטנים, תיקים הגדולים השאלה צריכה להיות איך אנו משפרים את המע' השיפוטית כדי לסייע ביישוב סכוסכים ע"י האמצעים הטכנולוגיים (כלים מקוונים – לתת שירות טוב יותר ונגישות לצדק וכו'). (8/04)

בשורה התחתונה, רפורמה זו משמשת כפלטפורמה לכניסת תהליכים מקוונים לבית המשפט בישראל. הרפורמה מעודדת בין היתר גיבוש הסכמות, עידוד החלפת מידע, ומאפשרת את קידום ההליך המשפטי, הכוללת ראיות אלקטרוניות, משמכים אלקטרוניים ואף מגדירות את אופן האיסוף שלהם.

**שיעור 8, 29.04.2019**

**נושא 7 לסילבוס: פרטיות בעידן הדיגיטלי - מבוא**

המרצה מצטטת מהספר של **מיכאל בירנהק, מרחב פרטי** (מחומרי הקריאה)

הטענה שעולה בספר, בעצם מדברת על כך שבעידן הדיגיטלי כיום, **כל פעולה שאנו מבצעים מייצרת מידע**. לצד האפשרות הזו, יש גם **אפשרויות טכנולוגיות רבות לאסוף את המידע הזה**, לתעד אותו, לעבד אותו, להפיצו הלאה, לחלוק אותו עם גורמים אחרים **בקלות**, והטכנולוגיה הפכה את המידע נגיש לגורמים רבים **בעלות נמוכה**, כך שבעולם זה יש גם **גורמים (שחקנים) רבים שיכולים לבצע את פעולות האיסוף וההפצה של המידע כך.**

מחשבה על הגנת הפרטיות החלה מהרצון **להגן על האדם מפני "האח הגדול", השלטון.** אולם, עם התפתחות הטכנולוגיה והאינטרנט, הרצון להגן על פרטיותנו לא מופנה רק כלפי השלטון אלא גם כלפי תאגידים פרטיים ש"מבלשים" אחרינו ואוספים עלינו מידע. אתרים חינמיים עושים שימוש במידע של המשתמשים, ואת הכסף הם מרוויחים ממכירת המידע של המשתמשים, מהיותו משאב כלכלי מרכזי (בין השאר ע"י פרסומות). כך נכנס גם רעיון **הגנת הפרטיות מפני תאגידים מסחריים.**

בשנים האחרונות המידע הפך למשאב כלכלי מרכזי, ולא קיים רק חשש של הגנת הפרטיות מפני השלטון אלא גם הגנת מפני תאגידים שפועלים למטרות רווח. יש מעקב מתמיד מסביבנו ואיסוף המיע הוא לא רק במכשירים הפרטיים שלנו, אלא גם במרחב הציבורי (כמו למשל מצלמות ברחוב)

בכל מקום שאליו אנו הולכים, ישנם סיכונים שונים לפרטיותנו: מצלמות אבטחה, היסטוריית גלישה, מידע ביומטרי וכן זירות חדשות שבהן המידע נאסף - הבית החכם. אפילו לחץ דם, מיקום.

הכניסה של איסוף נתונים דיגיטליים אל המרחב הפרטי, מייצרת פלטפורמה של מידע עצומה על חיינו.

כל אלו חושפים הרבה פרטים על שגרת החיים שלנו. דיברנו על השלטון שמנהל אחרינו מעקב ועל התאגידים שהופכים את המידע שלנו למוצר סחיר - שני העולמות הללו נפגשים **למציאות של מעקב מידע** (Dataveillance) **ומעקב המונים** (mass surveillance). מעקב של המדינה, מעקב של תאגידים, מסחר במידע, חיבור המידע שנמצא בידי המדינה ובידי גורמים פרטיים.

קיימים לכך השלכות וסיכונים משמעותיים - מערך דירוג / "אשראי חברתי" בסין נותן ציונים ונקודות ע"י פעולות שונות שמתבצעות במרחב ציבורי והפרטי. החשש הזה בא לידי ביטוי גם ברשתות מסחריות – פרופיילינג לצרכי שיווק ברשת טארגט. כך לחברות מסחריות יש גישה למידע רגיש מאוד על חיינו, ויש לכך השלכות חברתיות לתרבות איסוף ועיבוד המידע על חיינו.

מה קורה כשהכוח לבחור מה לחלוק ומה לא נלקח מאיתנו?

טכנולוגיות רבות מאפשרות פעולות שיש בהן פגיעה מובנית בפרטיות: שימוש בטלפון סלולרי (שיחות, מיקום, גלישה באינטרנט, עם מי אנחנו בקשר וכו'); נסיעה ברכב עם מכשיר ניווט לווייני; גלישה  באינטרנט; שליחת דוא"ל; שימוש בכרטיסי אשראי; יצירת אלבום תמונות דיגיטלי; שימוש במכשיר חכם לביש; בית חכם; רשתות חברתיות וכו'.

למרות שאנחנו יודעים את הדברים הללו, בהתנהגות היום יומית של אנשים קיימת **אשליה של פרטיות -** הן בסביבה הדיגיטלית והן בסביבה הפיזית. כשאנחנו הולכים ברחוב ליד מצלמת אבטחה אנחנו לא חושבים על האמצעות הסבירה שנזוהה בכל מקום שבו נצולם. כשאנחנו משתמשים בכרטיס מועדון בסופר אנחנו לא חושבים על מה שאפשר לעשות עם המידע בדבר הרגלי האכילה שלנו.

פנאופטיקון: מושג שהמציא ג'רמי בנת'הם והגיע לפרסום באמצעות מישל פוקו, הפילוסוף הצרפתי. פנאופטיקון מוגדר כבניין היקפי בצורת טבעת שבמרכזו מגדל עם חלונות המופנים לתוך הטבעת. הכוח הממשמע והממשטר של "המבט" הננעץ בנו. שוכני הפנאופטיקון אינם יכולים להביט אל מגדל השמירה ולכן אינם יכולים לדעת מתי צופים בהם. לפיכך, **עליהם להניח שהם נצפים תמיד וכך ההתנהגות שלך תשתנה.**

בעידן שלנו, שאנו מותירים אחרינו שובל של מידע שנאסף ונאגר, והיחס אלינו עשוי להשתנות על בסיסו - אנחנו מצויים במעין פנאופטיקון של משטר ותאגידים. האם בני אדם משנים את התנהגותם בגלל שזה המצב? ניתן לומר שערך הפרטיות כבר לא רלוונטי / שהטכונולגיה חושפת מה מתקיים שנים רבות.

היחס בין פרטיות לטכנולוגיה:

מקרה פרטי של הקשר בין משפט, טכנולוגיה, השוק והנורמות החברתיות

כשמדברים על מהי הזכות לפרטיות בעידן הדיגיטלי לא מדברים רק על מהן הטכנולוגיות או איך צריך לעצב אותן כך שלא יפגעו בפרטיות, אלא על שיח ערכי במשמעות של פרטיות בעידן הזה. האם כבר אין חשיבות לפרטיות? האם צריך לתת לכוחות השוק לפעול באופן חופשי וללא חסמים?

Ø   מודל לסיג - השפעה הדדית בין הזכות המשפטית לפרטיות , היכולות הטכנולוגית של איסוף ועיבוד מידע, שוק ותפישות חברתיות של פרטיות.

השיח הזה אמור לעזור לנו לחשוב אילו כלים משפטיים צריך לעצב ואיך לעצב את הטכנולוגיה - האם להגבילה בדרכים שונות? האם צריכות להיות לה תכונות מסוימות נוכח תפיסתנו את הפרטיות?

טכנולוגיה אינה בהכרח רעה או טובה

-          **טכנולוגיות מעקב** מאפשרות לנו לאתר עקבות דיגיטליות, לזהות ביומטרית, לאכן גיאוגרפית, לצותת, להעביר מידע לאחרים, לעבד מידע ולתעד. זה יכול להיות מאוד נוח כשאנחנו מאבדים פלאפון או כשאתר שאנו מבקרים בו לעיתים קרובות עושה פרסונליזציה לתכנים שאנחנו רוצים לקרוא.

-          **טכנולוגיות של פרטיות** מאפשרות לנו הצפנה, אבטחת מידע, מנעולים דיגיטליים, טשטוש עקבות (אנונימיות) ובמידה מסוימת **מחזירות לנו שליטה על הגישה לתוכן שלנו.**

לאורך זמן יכול לחול שינוי במהותה של טכנולוגיה מסוימת או במשמעות שאנו מייחסים לה. המשמעות הערכית, החברתית והאתית של טכנולוגיה נתונה נקבעה ביחס שבין כוונת המפתח, מאפייני הטכנולוגיה, והשימושים שנעשים פה בפועל. למשל, טכנולוגיית ה-cookies נועדה לעזור בניהול סיסמאות לאתרים. עם זאת, זו טכנולוגיה שמאפשרת איסוף מידע ומעקב אחרינו, כך **שמשמעותה נקבעת איפשהו במארג היחסים בין כוונת המפתח, מאפייני הטכנולוגיה עצמה והשימושים שנעשים בה. עם השנים יש התחדשות והתפתחות טכנולוגית אז ניתן לבצע גלישה פרטית באופן שלא שומר את ההיסטוריה. כך נולדים אתגרים חברתים ומשפטיים חדשים ופתרונות חדשים.**

צירים לדיון הפרטיות בעידן הדיגיטלי

-          הבנת הזכות לפרטיות **כמושג משפטי שנמצא במשא ומתן רציף עם נורמות חברתיות ועם הטכנולוגיה.** זה גורר השתנות.

-          מושג הפרטיות במונחים של **שליטת האדם על עצמו -** הכוח של אדם לקבוע מתי יימסר מידע אודותיו, איזה למי ובאילו תנאים.

-          **קריסת הנחות אנלוגיות** שמקורן בעולם טרום-הטכנולוגיה הרווחת, וכבר לא מתאימות לסביבה הדיגיטלית ולחיים הפוסט-מודרניים של דורנו. חיינו נטועים בסביבת המידע.

-          **הגנת מידע ביחסים מול המדינה ומול השוק** (תאגידים פרטיים, אנשים פרטיים). מי שיכול לתייג אותי בתמונות מפקיע ממני חלק מהשליטה על המידע שלי.

מהי פרטיות?

**א. נורמה חברתית -** מה אנשים בחברה רואים כפגיעה בפרטיות (למשל, חשיפת ציונים בקורס).

**ב. נורמה משפטית -** הזכות לפרטיות מעוגנת בחוק ובפסיקה, ויוצרת כללי משחק ביחסים בינינו לבין אחרים. למשל, זכות זו **אוסרת על אחרים לפגוע בנו** באמצעות קריאת מכתבים סגורים, האזנה לשיחותינו עם אחרים או לצלם אותנו ברשור/ת היחיד; **מגנה על סוגים שונים של מידע** (מידע רגיש כמו מידע רפואי; מידע "רגיל" כמו הרגלי צריכה או גלישה באינטרנט); **ומקנה לנו אמצעים למנוע הטרדה שלנו או מסחור של דמותנו.**

הזכות לפרטיות מעוגנת בחוק יסוד כבוד האדם וחירותו, ס' 7:

א. כל אדם זכאי לפרטיות ולצנעת חייו.

ב. אין להיכנס לרשות היחיד של אדם שלא בהסכמתו.

ג. אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו.

ד. אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו.

עוד לפני חוקי היסוד נקבע **חוק הגנת הפרטיות, תשמ"א-1981,** שכולל 12 סעיפים שונים של מעשים שיהוו פגיעה בפרטיות. חוק זה כולל בתוכו הגנות ומקרים של פטור מאחריות.

שני חוקים אלו לא כוללים הגדרה של הזכות לפרטיות – הם קובעים את קיומה ושורה של מצבים שיהוו פגיעה בפרטיות.

**מקור הזכות לפרטיות**

הזכות לפרטיות כ"זכות להיעזב במנוחה" (וורן וברנדייס, 1890)

מאמר שכתבו שני מלומדים עקב שינויים חברתיים וטכנולוגיים (שינויים בעיתונות עם הקמת מדורי הרכילות; שינויים טכנולוגיים נוכח הפופולריות הגוברת של המצלמות). הם הגדירו את הזכות לפרטיות כזכות שקיימת בדין (על אף שאינה מנויה בחוקה האמריקנית), במובן של **זכותו של אדם לשלוט על פרטים אודותיו ובאישיותו.** הגדרה זו אינה מספיקה לעידן הדיגיטלי משום שהיא לא חלה על פרטי מידע שהיינו חושבים שהם טריוויאליים, כמו הרגלי הצריכה שלנו או גלישה באינטרנט. המניעים של וורן וברנדייס היו חברתיים וטכולגים – שינויים ביונות (מדורי הרכילות) שינויים טכנולוגיים (הפופולאריות של המצלמה).

עולה השאלה האם הגדרה זו של פרטיות מתאימה לעידן הדגיטאלי?

הזכות לפרטיות כשליטה

גישה זו הוצעה ע"י הסוציולוג אלן וסטין (1967), שהגיע למסקנה שלאנשים חשוב לשלוט על המידע הפרטי שלהם. הוא ראה את **הזכות לפרטיות כשליטה - היכולת של אדם לקבוע בעצמו ולמען עצמו איזה מידע על אודותיו לשתף עם אחרים,** מתי ובאיזה אופן ועבור אילו מטרות.

הגדרות אלו אינן סותרות זו את זו, אך יש ביניהן מספר הבחנות:

-          הזכות להיעזב במנוחה היא **זכות צרה יחסית, היא סבילה, פסיבית** (מניעת התערבות של אחרים באוטונומיה של הפרט).

-          גישתו של וסטין רחבה יותר ופעילה. במקום אי התערבות במרחב האוטונומי של הפרט, "הפרטיות כשליטה" דורשת **הפעלת כלי פעיל בידי האדם שיאפשר לו לשלוט ב"יחידה האוטונומית" שלו.** גישה זו מכתיבה כללים קונקרטיים דוגמת "עקרון ההסכמה" ו"עקרון צמידות המטרה" (מידע ניתן לשימוש רק למטרה שלשמה מסרנו את המידע), **ויכולה לחול על סוגים רחבים יותר של מידע.**

בדין הישראלי ניתן לסווג קטגוריות של פרטיות

**א. פרטיות במקומות**

-          "ביתו של אדם - מבצרו"

-          בעלות במרחב פיזי או במיטלטלין מסוימים קובעת פרטיות בהם, כך שכניסה אליהם ללא אישור תהווה פגיעה בפרטיות. החוק הישראלי מגן על רשות היחיד יותר מעל רשות הרבים. (למשל, אסור לפרסם תמונה של אדם ברשות היחיד ללא הסכמתו לעומת פרסום של תמונה של אדם ברשות הרבים אם הוא עלול להשפילו או לבזותו).

**ב. פרטיות בתקשורת (שבין בני אדם)**

-          סודיות התקשורת מוגנת, ומי שחודר לתוכה - בהאזנה או בתיעוד - פוגע בפרטיות.

-          מקבלת ביטוי בחוק האזנות סתר, בחוק היסוד ובחוק הגנת הפרטיות – לאחר תיקון מס' 9 גם מסר אלקטרוני.

-          ישנה הגנה פחותה לנתוני תקשורת (מי שוחח עם מי, מתי וכמה זמן נמשכה השיחה) בהשוואה לתוכן התקשורת (לאיזה מספר התקשרתי, איזו שעה, מאיזה טלפון). זה בעייתי בעידן של יכולות עיבוד והצלבת מידע מתקדמות, כי ניתן ללמוד הרבה על אדם מנתוני התקשורת שלו (למשל, אם התקשר לער"ן / גלישה לאתרים של בעיות רפואיות).

-          למשרדי הביטחון יש אינטרס שמשפיע על החקיקה הישראלית.

נתוני תקשורת בעידן של כריית מידע ואמצעי תקשורת חדשים (6/05)

טכנולוגיות של כריית מידע (data minining) טכנולוגיית עיבוד מידע – Data science מאפשרות **להפוך מידע לא מזוהה למזוהה ולהסיק מנתונים טריוויאליים דברים משמעותיים.** לשלב נתוני מידע ופרטי מידע "טכניים" נוספים כדי ליצור תובנות משמעותיות. ניתן להסיק מנתונים טריוויאלים פרטים משמעותיים יותר תוך זיהוי בני אדם ספציפיים.

פניתן לאסוף את כל הפרופיל של החיים הדיגיטליים של אדם, כגון באילו שעות הוא פעיל, לאילו תכנים הוא נחשף, מיהם הקשרים העסקיים שלו וכו'.

ישנם סוגי שיחות חדשים שמעוררים בעיות חדשות - דוא"ל, טלפוניית רשת, תוכנות צ'אט וקיימים תפקידים שונים של גורמי ביניים בשיחות.

**ג. פרטיות במידע**

-          מידע הוא **תוצר מרכזי של פעילותנו.** דוגמאות לתוצרי מידע של חיינו – איך קוראים לנו, איפה אנחנו גרים וכו'. עצם זה שעשינו פעילות כלשהי מהווה נתון מידע.

-          מידע הוא **"סם החיים" של הכלכלה החדשה ובסיס חשוב לפעולות השלטון,** מה שהופך אותו **ליעד אטרקטיבי.**

-          המידע גורם לנו לבקר מחדש את ההבחנות בין סוגים שונים של מידע: מזוהה/ אנונימי, פרטי/ פומבי, רגיש/לא רגיש ומידע אישי – Personal data, private information ,private facts.

-          ס' 2(7)-2(9) ו-2(11) לחוק הגנת הפרטיות מתייחסים לפרטיות במידע שניתן להגדירו כמידע אישי או מידע פרטי.

מהו מידע אישי?

*א.*   *הגישה בארה"ב (גישה סקטוריאלית)*

החוק מצביר על המוסכמות החברתיות – עניינים מסויימים שהמידע לגביהם פרטי. מידע זכאי להגנת החוק אם המחוקק קבע אותו כקטגוריות מידע שזוכה להגנה -  כל מה שלא הוסדר לא ניתן להגנה עליהם. ישנן מוסכמות חברתיות כי מידע פיננסי, בריאותי, גנטי, על תלמידי בי"ס, מידע שבידי המדינה, מידע שנאסף מילדים בני 13 ומטה בעת גלישה באינטרנט, מידע על קלטות וידאו שאדם שכר בחנות או סרטים שהזמין בשירות צפייה וכו' מהווה עניין פרטי.

·         בדין הפדרלי, מידע נחשב פרטי וזוכה להגנה תחת הזכות לפרטיות רק אם הוא מוסדר בחוק מסוים. וזה אומר שאם הגנת המידע לא הוסדרה ולשוק יש עניין במידע, ניתן לסחור בו.

המחוקק מצהיר שזה מה שהחברה רואה כמידע פרטי, **וכל מה שלא הוסדר בחוק לא ייחשב כפרטי ולא יזכה להגנה תחת הזכות לפרטיות.**

*ב.*   *הגישה באיחוד האירופי (גישה מרחיבה)*

**כל סוג של מידע נחשב פרטי אם הוא קשור לאדם מזוהה או לאדם שאפשר לזהותו – גם אם אין שם נתונים כמו ת.ז. אלא לפי נתונים אחרים ניתן לזהותו.** גישה זו מתייחסת לפרטיות כנגזרת של ענף "הגנת המידע" (data protection), תפיסה הקשורה לכבוד האדם. כך, גם מידע טריוויאלי (למשל, על הרגלי הצריכה של האדם) הוא עניין של פרטיות.

זה אומר שכל הפעולות שקשורות לאיסוף מידע ולעיבודו כפופות למשטר הגנת המידע מוטלות חובות על מי שאוסף מידע, מחזיק במידע או מעבד מידע. ונתונות זכויות למושאי המידע (data subjects) –למשל לבקש תיקון של המידע, ואם הזכויות מופרות ניתן לתבוע פיצויים.

**שיעור 9, 06.05.2019**

**נושא 8 בסילבוס: הגנת הפרטיות בעידן הדיגיטלי - הדין הישראלי**

**הגנת הפרטיות בעידן הדיגיטלי בישראל**

בישראל ישנה **זכות חוקתית לפרטיות,** הקבועה בס' 7 לחוק יסוד: כבוד האדם וחירותו. כמו כן יש **הגנה די רחבה על פרטיות במידע -** פרק ב' לחוק הגנת הפרטיות (הסדר מפורט של מאגרי מידע); פרק ד' לחוק הגנת הפרטיות (הסדר להעברת מידע בין גופים ציבוריים); תקנות הגנת הפרטיות (אבטחת מידע)(חובות אבטחת מידע של בעלים/מנהלים/מעבדים של מאגרי מידע אישי)).

חוק יסוד: כבוד האדם וחירותו קובע בס' 7 **זכות כללית לפרטיות,** ומפרט **שלושה מצבים ספציפיים של פרטיות: פרטיות במקומות, בגוף האדם ובתקשורת.**

Ø   אמת המידה להגנה המשפטית על מידע היא תכנית. זוהי גישה צרה יותר מאירופה אך רחבה יותר מארה"ב.

פגישה בפרטיות "פיזית" ובפרטיות "מידע"

מצבים המנויים בס' 2 שמתייחסים לפגיעה בפרטיות "פיזית" הם **הטרדה ובילוש** (ס"ק 1); **האזנת סתר** (ס"ק 2); **צילום ברשות הרבים** (ס"ק 3).

מצבים המנויים בס' 2 שמתייחסים לפגיעה בפרטיות "מידע" הם **הפרת חובת סודיות בנוגע ל"ענייניו הפרטיים של אדם"** שנקבע בדין (ס"ק 7) או בהסכם (ס"ק 8); **פרסום דבר שהושג תוך פגיעה בפרטיות** (ס"ק 10); **פרסום מידע ביחס ל"צנעת חייו האישיים של אדם", עברו הרפואי או המיני, התנהגותו ברשות היחיד** (ס"ק 11).

"ענייניו הפרטיים של אדם"

**ע"א 439/88 רשם מאגרי המידע נ' ונטורה:** ונטורה רצה להקים מאגר מידע ששמר נתוני אשראי של משתמשים והרשם סבר שקיומו של מאגר מידע שכזה נוגד את ס' 2(9) לחוק (עקרון צמידות המטרה - ניתן לעשות שימוש במידע רק למטרה שלשמע הוא נאסף). ונטורה פנה לביהמ"ש, שאישר את עמדת הרשם ותוך כדי הדיון התייחס להגדרה של "ענייניו הפרטיים של אדם":

עמדה מרחיבה (השופט בך): **כל מידע הקשור לחייו הפרטיים של אותו אדם,** לרבות שמו, כתובתו, מספר הטלפון שלו, מקום עבודתו, זהות חבריו, יחסיו עם אשתו ומשפחתו וכדומה".

עמדה מצמצמת (שטרסברג-כהן): "ראוי שלא ליצור רשימה סגורה או פרטנית אלא לאפשר **בדיקת הנושא על פי ההקשר...** המטרה שלשלמה נדרשת פרשנות.. בבואנו להגדיר 'ענייניו הפרטיים של אדם' הגדרה שתהפוך כל הפוגע בהם למפר חוק, **עלינו להיות זהירים ודווקניים**".

תובנה צופת פני עתיד הגנת המידע בעידן הדיגיטלי (שטרסברג-כהן): ייתכנו מקרים שבהם כל פרט בנפרד אינו בהכרח "עניינו הפרטי של אדם", אולם **צירוף פרטים יחד יהווה עניין פרטי מוגן.**

הסדר ספציפי למאגרי מידע - פרק ב' לחוק הגנת הפרטיות, הגדרות:

הגדרות (ס' 7):

**"מידע":** נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

**"מידע רגיש":** (1) נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו. (2) מידע ששר המשפטים קבע בצו, באישור ועדת חוקה חוק ומשפט של הכנסת, שהוא מידע רגיש (טרם נקבע ע"י השר).

**"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 אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד שבשליטתו אין אוסף נוסף.

Ø   **הגישה הישראלית בחוק הגנת הפרטיות** שונה מהגישה האירופית **ומחריגה מאגרים ידניים** (אנלוגיים). ההנחה היא שהסיכון לפרטיות פחות במאגרים ידניים.

**החוק מתייחס ל"נתוני מידע" ולא לנתונים שעובדו.** כלומר, אם יש המלצה שנכתבה על סטודנט על סמך הנתונים במערכת המחשוב של האוניברסיטה (שכוללים את הציונים שלו, עומס הקורסים, התשלומים לאוניברסיטה וכו') - נפריד את הדו"ח (תוצר של עיבוד נתונים) מהנתונים עצמם. זה רלוונטי גם לעניין זכויותיהם של מושאי המידע. אם יש להם זכות גישה לנתונים, היא לא תחול על הדו"ח המעבד אלא על הנתונים הגולמיים בלבד.

מאגרים יכולים לשנות את טיבם עם הזמן ולצאת מגדרי ההחרגה (ולהפוך למאגר מידע במונחי החוק). בישראל יש כיום כ-15,000 מאגרים רשומים (לא הרבה יחסית). המספרים נמוכים כי כנראה אין סנקציה חזקה על אי-רישום.

חובות מנהל מאגר מידע - רישום מאגר

על מנהל מאגר מידע מוטלת חובה בחוק לרשום את המאגר. מדוע? מהי תכלית הרישום?

**א.**   פיקוח מהותי

-          פקח יכול לסרב לרשום מאגר למטרה בלתי חוקית (ס' 10(א)(1)).

-          שינוי מטרת המאגר המוצהרת לפי בדיקה של פעילות המאגר בפועל (ס' 10(א)(2)).

**ב.**   פיקוח על פעילות המאגר.

**ג.**        הנחה התנהגותית (חובת הרישום גוררת בדיקה ופיקוח פנימיים אצל מנהלי המאגרים, שיגבירו את הציות לחוק).

הרעיון הוא שתיווצר תרבות של בעלי מאגרים לציית לחוק.

קפיצה מעמוד 43  מנהל מאגר לעומת מי שמעבד מדע ללא שמירתו.

חובות מנהל מאגר מידע - חובת ההודעה

מי שפונה לאדם לקבלת מידע לשם החזקתו במאגר צריך לתת לו הודעה שעומדת בתנאים הללו:

(1)   האם חלה על האדם חובה חוקית למסור את המידע, או שמסירתו תלויה ברצונו והסכמתו?

(2)   מהי המטרה אשר לשמה מבוקש המידע?

(3)   למי יימסר המידע ומהן מטרות המסירה?

מדוע ההודעה חשובה?

חובת ההודעה חשובה בכך שהיא מהווה בסיס לקבלת הסכמה מדעת של מושא המידע. ההודעה היא הבסיס להפעלת עקרון צמידות המידע (איזו מטרות ולמי יימסר המידע)- ס' 2(9), ס' 8(ב) - שאומר שהמידע שלך יכול להימצא אצל מישהו אחר, אבל יש לך זכות לשלוט במה שקורה למידע הזה – יש לך אוטונומיה על המידע, ומנהל המאגר יכול להשתמש בו רק בגבולות ההסמכות.

עם זאת, היעדר דרישה צורנית להודעה בעייתית (בהשוואה לפרשנות חוזה צרכני, דיני הגנת הצרכן). כמו כן, החובה לא מתייחסת לזכויות מושאי המידע (הזכות לגשת למידע, לעיין בו או לדרוש את תיקונו).

**דרישת ההסמכה ועקרון צמידות המטרה סיכום -**

**1.**    הסכמה היא מדעת במפורש ו מכללא וס' 11 נדרש הסכמה של אדם כדי להכניס אותו למאגר מידע

**2.**    צמידות המטרה -ס'2 (9), ס' 8(ב) ס' 11 ולצורך הסכמתו של האדם לשימוש במידע שלו - הוא צריך לדעת מה המטרה של איסוף המידע.

·         אוסף המידע ראשי להשתמש במידע אך ורק למטרה שלשמה נאסף.

·       הבטחת המשך השליטה של מושא המידע במידע: מותר להשתמש המידע רק בהסכמתו ורק באופנים שלגביהם הוא נתן את ההסכמה רק ע"י מי שהוא נתן לו את ההסכמה ואלו האדנים של דרישת ההסכמה ועקרון צמידות המטרה.

ב2008,כשנערך מחקר, עלה כי כדי לקרוא את כל ההסכמים שאנו מאשרים במהלך שנה, ידרשו 40 דק' ביום, ולכן עלו פתרונות של עיצוב ויזואלי או לפשט את השפה, או לעשות כותרות - ואחרי שבדקו את זה, גילו שלא היה שינוי בכלל של ההבנה של הגולשים.

יש מרכזיות גדולה להסכמה והיא נותרת גם הGPR ויש קושי בהתבססות הזו על ההסכמה ככלי, כי היא ניתנת כלאחר יד. והיה ניסיון לפשט את הסכם הפרטיות ואת תנאי השימוש, זה לא סייע למושאי ההסכמה להבין על מה הם מסכימים. לכן יש בעייתיות להתבסס על הסכמה כאמצעי הסדרה של הגנת הפרטיות. הדין הישראלי וגם דינים אחרים, משקפים את התפיסה של שליטת תפיסת המידע גם בזכויות אחרות שהם נותנים.

המשך שליטת מושא המידע במידע

* זכות לעיין במידע שמוחזק אצל אחרים (ס' 13)
* זכות לדרוש את תיקון במידע (ס' 14)
* מוגבלות בהשוואה לדין האירופאי  - יוסבר בשיעור הבא
* למושא המידע קיימות סמכויות אכיפה:
* **לאזרחים -** ס' 31 ב לחוק הגנת הפרטיות (זו עוולה אזרחית)
* **לרשות ייעודית (ס' 10 לחוק הגנת הפרטיות).** הרשות = רשם מאגרי המידע במשרד המשפטים. (זו עבירה פלילית)

**בפתרון קייס - תמיד לבדוק לפי ס' 7 לחוק הגנת הפרטיות מהו מידע.**

זכות העיון במידע -

לא תמיד תהיה זכות עיון, אם זה עלול לגרום נזק חמור לביראתו הגופנית או הנפשית של המבקש או לסכן את חייו.

ס' 13:

(א)     וכל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.

(ג)    בעל המאגר רשאי שלא למסור למבקש מידע המתייחס למצבו הרפואי או הנפשי אם לדעתו עלול המידע לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור בעל המאגר את המידע לרופא או לפסיכולוג מטעמו של המבקש.

(ה)   החרגת תחולה על מאגרים רשויות היבטחון, שב"ס, רשות המיסים ועוד.

קשיים במימוש זכות העיון -

חובת ההודעה כפי שהיא מוגדרת בחוק לא כוללת יידוע של מושא המישע בדבר הזכות לעיין במידע.

המימוש בפועל מאתגר:

1.    למי לפנות?

2.       מקרים של היעדר זהות בין בעל המאגר למחזיק המאגר (מחזיק המידע ומנהלו)

ס' 13 א(1): במקרה שבו בעל מאגר מידע מחזיק אותו אצל אחר - עליו להורות למחזיק לאפשר למושא המידע לממש את זכות העיון.

זכרו כיצד "מידע" מוגדר בחוק: תוצרי עיבוד המידע (למשל – פרופיילינג.9 אינם כלולים בזכות העיון (או התיקון)

תיקון המידע -

ס' 14:

(א)  אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע, ואם הוא תושב חוץ - למחזיק מאגר המידע, בבקשה לתקן את המידע או למוחקו.

         (ב) הסכים בעל מאגר המידע לבקשה כאמור בסעיף קטן (א), יבצע את השינויים הנדרשים במידע שברשותו ויודיע עליהם לכל מי שקיבל ממנו את המידע בתקופה שנקבעה בתקנות.

        (ג) סירב בעל מאגר המידע למלא בקשה כאמור בסעיף קטן (א), **יודיע על כך למבקש,** באופן ובדרך שנקבעו בתקנות.

במקרה של סירוב לבקשת מושא המידע -

ס' 15 : על סירובו של בעל מאגר מידע לאפשר עיון כאמור בסעיף 13 או בסעיף 13א ועל הודעת סירוב כאמור בסעיף 14(ג), רשאי מבקש המידע להגיש תובענה לבית המשפט באופן ובדרך שנקבעו בתקנות.

אם בעל המאגר מסרב לזכות העיון או התיקון, אז מושא המידע יכול לפנות לבית המשפט בנושא.

רשם מאגרי המידע הוציא הנחיות על מקרה בו בעל המאגר המידע מעביר את חלק מהפעולות במאגר (למשל עיבוד) – יש לזכור כי יש חובה לצמידות מטרה גם כשעוסקים במיקור חוץ:

כבעל מאגר מידע עובר עם מקור חוץ - בין אם הוא נותן לו גישה או מעביר לו את הכל או חלק מהמידע - ממשיך לחול עליהם ההנחה של צמידות המטרה. בעל מאגר המידע צריך לכתוב מה המטרה.

·         יש להגדיר את אופי השירות שיבוצע + היקף המידע  האישי שנחוץ להעבירו לשם כך.

·         יש להעדיף העברת מידע / הרשאות גישה רק בהיקף שדרוש למתן השירות - לא להעביר את המאגר בכללותו.

**פגיעה בפרטיות: עוולה אזרחית, עבירה פלילית**

החוק מבחין הבין פרק א' דרכים שונות של פגיעה בפרטיות, בהפרתם לפי סע' 4 יש עוולה אזרחית (ניתן לבקש פיצוי ללא הוכחת נזק (עד 50 אלף ₪) או תביעה נזיקית רגילה על מלוא הנזק שנגרם אך נדרשת הוכחת נזק בלי תקרה של סכום כספי. ואם התבצעו במזיד- מדובר בעבירה פלילית (עד 5 שנות מאסר) ולפי ס' 29 א' - פיצוי ללא הוכחת נזק. לבין פרק ב' הפרות של החובות מנהלי / בעל המאגר וכל מה שקשור לניהול המידע. הפיצוי יהיה לםי פק' הנזיקין - ס' 31 ב' לחוק הגנת הפרטיות – נדרשת הוכחת נזק.

שימוש בידיעה על ענייניו האישים של אדם, שלא למטרה לשמה נמסר המידע מאת נושא המידע= הפרת סע' 2 (9)לחוק הגנת הפרטיות.

ס' 4 : פגיעה בפרטיות – עוולה אזרחית, יחולו הורואת פקודת הנזיקין.

ס' 5: פגיעה בפרטיות – עבירה – הפוגע במזיד בפרטיות זולתו באחת הדרכים האמורות בסע' 2(1),(3) עד (7) ו-(9)עד 11, דינו מאסר חמש שנים.

פיצוי נזיקי למושאי המידע בגין הפרת הוראות החוק

עוולה בנזיקין  - ס' 31 ב: מעשה או מחדל בניגוד להוראות פרקים ב' או ד' או בניגוד לתקנות יהווה עוולה לפי פקודת הנזיקין. למשל: מנהל מאגר שהתרשל בחובת סודיות או אבטחת מידע חב בנזיקין כלפי מושא המידע שנפגע.

ביהמ"ש מוסמך לפסוק פיצוי ללא הוכחת נזק (עד 50,000 ₪) – ס' 29 א'

במקרה של הרשעה בעבירה לפי ס' 5 (ס"ק א)

חובת הסודיות ואבטחת מידע

בעלי מאגר מידע חייבים בחובות נוספות כדוגמת:

חובת סודיות – ס' 16: 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; אם הוגשה הבקשה לפני תחילת ההליך תידון הבקשה בבית משפט השלום. המפר הוראות סעיף זה, דינו - מאסר 5 שנים.

חובות אבטחת מידע – ס' 17: בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.

ס' 7 מגדיר מהי אבטחת מידע = הגנה על שלמות המידע או הגנה על המידע מפני חשיפה שימוש או העתקה שלא כדין (ס' 7)

תקנות הגנת הפרטיות (2017) פורטות אתה חובה לפרטיות בחוק להוראות ספציפיות קונקרטיות והן קובעות סטנדרטים ולא הוראות טכנולוגיות ברורות שקובעות איך לאבטח את המידע בפועל, לא קובעים כלים ופעולות הכרחיות אלא רק סטנדרט כללי.

נכנסו לתוקף ב - 8.5.2018 מפרטות את אופן יישום חובת אבטחת המידע שבסע' 17 לחוק הגנת הפרטיות

**3 רבדים עיקריים להסדר שבתקנות:**

1. יש לקבוע מהו המידע המוגן והסיכונים הקשורים אליו
2. יש לקבוע נהלים מפורטים וברורים לאבטחת מידע
3. קביעת הוראות מהותיות בניהול אבטחת מידע

**תקנות מודולריות:** הסדרים ביחס לארבעה סוגי מאגרי מידע

**חובות ברמה הולכת וגוברת על ארבעה סוגי מאגרים**

1. ככל שפעילות עיבוד המידע בארגון משמעותית יותר. למשל: כשהמאגר מכיל מידע רגיש / מידע על אנשים רבים ומטרת המאגר היא מסירת מידע לאחרים
2. כלל שמדובר במידע רגיש יותר למשל מידע ר]ואי, עמדות פוליטיות, אמונה דתית, מידע כלכלי אבל גם : הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע כנ"ל או אישותיו של אדם
3. ככל שיותר אנשים בארגון חשופים למידע – מס' מורשי הגישה

ס' 20 קובע אילו חובות יחולו על כל סוג מאגר. מרבית החובות שחלות על בעל המאגר, יחולו גם על מנהל + מחזיק המאגר.

שתי חובות שמטרתן לצמצם את הסיכון לדליפה של המידע במאמר, הן מגורם פנימי (ס' 16) והן מגורם חיצוני (ס' 17).

"אבטחת מידע": הגנה על שלמות המידע או הגנה עליו מפני חשיפה/שימוש/העתקה שלא כדין.

חשוב לשים לב שנקבע כאן עקרון בסיסי, סטנדרט - ולא האמצעים, מתוך ההבנה שקצב השתנות הטכנולוגיה מהיר והיכולת לפרוץ משתנה כל הזמן (ועל כן נוקטים "ניטרליות טכנולוגית").

**שיעור 10  20.05.2019**

**שיעור 11, 27.05.2019 + שיעור 12, 03.06.19**

**נושא 9 בסילבוס: מהפכת ה-GDPR בהגנת הפרטיות**

**General Data Protection Regulation**

מידע ביחס לאדם מזוהה או שניתן לזהותו, זיהוי ישיר או עקיף - התייחסות לשם וכו'.

מהו מידע אישי לפי הגישה האירופאית?

1. מידע שמזהה את האדם. אבל, זיהוי האדם אינו מרכיב הכרחי לצורך מתן הגנה משפטית למידע. התפישה היא היעדר זיהוי כשלעצמו אינו מפחית בהכרח מחשיבותו של המידע.
2. מידע אנונימי/ סטטיסטי, אם אינו מנותק מהאדם
   1. יכול להתאפשר זיהויו באמצעות פעולה של דה-אנונימיזציה
   2. אפשרי יותר ויורת עם התפתחות טכניקות סטטסטיות וטכנולוגיות עיבוד מידע אנונימיות אינה "תרופת קסם" להגנה על מידע, דרושים אמצעים נוספים למשל, סנקציות פליליות, אזרחיות ומשמעתיות במקרה של הפרה, פסילת החלטות שהתקבלו על בסיס מידע אישי שלא התקבל כדין.

**סיכום ביניים : משבר הגנת המידע והפרטיות בעידן הדיגיטלי**

**המהפכה הדיגטלית ומהפכת הסלולר -** איסוף מידע בכמויות עצומות, ממגוון מקורות וסוגים, משירת מידע לאורך זמן, כריית, ניתוח והצלבת מידע. כל זה אומר שהנחת האנונימיות מאותגרת וגם הבסיס של עקרונות הגנת המידע מתערער. בדין הישראלי והאירופאי, רק מידע מזהה זוכה להגנות מוגברות של הדין. בפועל, כיום, ניתן לשחזר זהות גם מתוך מידע אנונימי.

קיים קושי בהצהרה מראש לגבי מה ייעשה במידע, גורמי איסוף ועיבוד מידע מתקשים להצביע מראש על השימושים שייעשו בו. שימוש רווח בניסוח מעורפל "המידע ישמש בסיס לניתוח נוסף".

ההסכמה שניתנת אינה מספקת, כשהמטרה הראשונית מעורפלת, קשה לבחון צמידות מטרה בהמשך.

זה אומר שאנו מסתכלים על המידע הפרטי באדן של דרישת ההסכמה ושל צמידות המטרה - שתי הדרישות מאותגרות מאוד במציאות הזו - יש לומר שלא ברורה כמה שווה ההסכמה- מוביל לריקון ההסכמה מתוכן היות ומרבית האנשים אינם קוראים את מדיניות הפרטיות שנלווית ליישומים ברשת או בטלפון. ממצאי המחקרים שרוב הגולשים לא קוראים הם חד משמעיים ביחס לכך שדרישת ההסכמה מרוקנת מתוכן.

* **הזכות לפרטיות נתונה לאיום הן מצד המדינה, הן מצד שחקנים פרטיים.**

1.    תאגידים מסחריים, מעסיקים או בעלי כוח אחר, וכן מצד פרטים אחרים.

2.    על בסיס המידע: מסווגים אותו לתבניות.

3.    נוקטים בפעולות על בסיס האפיון שאפיינו אותנו.

o       להבין לקוחות ולנתח את נכונותם לרכוש מומרים ושירותים.

o       לסנן מועמדים לעבודה ולבחון את התאמתם

o       לנווט ולהשפיע על התנהגותנו

המידע עשוי לבוביל לאפליה והוא נותן אפשרות לסחור במידע / להעביר מידע בין הממשלה ובין גופים פרטיים.

לפי הגישה האירופית, מידע שמזהה את האדם הוא:

(1)   מידע שמזהה את האדם עצמו

(2)   מידע אנונימי/סטטיסטי אם אינו מנותק מהאדם (כך שניתן לבצע פעולת דה-אנונימיזציה - אפשרי יותר ויותר עם התפתחות טכניקות סטטיסטיות ויכולות עיבוד מידע).

**הגישה הישראלית דומה יותר לגישה האירופאית** (היא מצביעה זכות כללית לפרטיות שמשתרעת על פרטיות במידע ולא רק בתחומים מצומצמים) **אבל יש בה אמת מידה תוכנית מסוימת** - לא די בכך שהמידע מזהה את האדם אלא המידע צריך להשתייך לסוגי מידע מסוימים שהוכרו כפרטיים (=אמת מידה תוכנית) וזאת תוך הותרת מרחב פרשנות שיפוטי.

**ההסדר המשפטי -**

·         סמכות חוקתית לפרטיות

o       ס' 7 לחו"י כבוד האדם וחירותו.

·         הגנה רחבה על פרטיות

o       ס' 2 לחוק הגנת הפרטיות - התשמ"א- 1981.

·         הגנה רחבה למדי על פרטיות במידע

o       פרק ב' לחוק הגנת הפרטיות (הסדר מפורט של מאגרי מידע).

o       פרק ד' לחוק הגנת הפרטיות (הסדר להעברת מידע בין גופים ציבוריים)

o       תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז- 2017. חובות אבטחת מידע על בעלים/ מנהלים/מעבדים של מאגרי מידע אישי).

עיגון חוקתי של הזכות לפרטיות – חוק יסוד: כבוד האדם וחירותו בס' 7. כאן מוטלת חובה על רשויות המדינה לשמור על הפרטיות, פגיעה בפרטיות מותרת רק בתאני פסקת ההגבלה.

לכן יש צורך של הסמכה מפורת בחוק וכן שהפגיעה נועדה לתכלית ראויה, שהולמת את ערכי המדינה והיא מידתית.  דוג': בג"צ 8070/98 - האגודה לזכויות האזרח נ' משרד הפנים -המידע הועבר באופן רחב ולא היתה הסמכה מפורשת בחוק להעביר

מהסתכלות על החוק לא רואים הגנה חוקתית על פרטיות במידע – אבל זה מתאפשר באמצעות פרשנות לאור מגמות המשפט הישראלי ופעולות הרשות המבצעת (הרשות להגנת הפרטיות, רשם במאגרי המידע).

להבדיל מפגיעה פיזית (הטרדה ובילוש, האזנת סתר, צילום ברשות היחיד) יש פגיעה בפרטיות של מידע כאשר החובה לשמור על הסודיות קבועה בדין ס' 7 או בהסכם ס' 8 ופרסום מידע ביחס ל"צנעת חייו האישיםשל האדם", עברו הרפואי או המיני, התנהגותו ברשות היחיד (ס' 11).

כך ניתן לראות שזו אמת המידה להגנה המשפטית על מידע היא תוכנית, והיא נותנת עילות סל מאשר החוקים הספצייפים של הגישה הסקטוריאלית ויש בה אפשרות לפרשנות. גישה צרה יותר מאירופה, רחבה יותר מארה"ב.

מהם "ענייניו הפרטיים של אדם?"

* **"רשם מאגרי המידע נ' ונוטורה -** השופט בך נקט בעמדה מצמצמת ולעומתו שטרסברג-כהן נוקטת בעמדה מרחיבה - עדיף לא לנקוט בעמדה סגורה. מה שמעניים בתפיסה זו היא אמירת אגב צופה פני עתיד "יתכנו מקרים בהם כל פרט בנפרד אינו בהכרח עניין פרטי אולם צירוף פרטים יחד עשוי להיות עניין פרטי מוגן" – שזה מתאים לתפיסה של כל פרט בנפרד על מישהו לא מזהה אותו אבל מכלול הפרטים מסייע למצוא את האדם.

הסוד ספציי למאגרי מידע  - פרק ב' לחוק הגנת הפרטיות

הגדרות – ס'7 מגדיר מהו מידע לצרכי החוק הזה – נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו ומהו מידע רגיש – לא מופיעים מעמדו האישית והכשרתו המצקועית – כי לדעת המחוקק אלו לא מידע רגיש.

יש גם הגדרה לגבי מאגר מידע – אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב למעט  -

(1)   אוסף לשימוש אישי שיאנו למטרות עסק; או

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

מאגר ידני - בישראל, מאגר ידני אינו בבחינת מאגר מידע. בחוק האירופאי המצב שונה.

וכן חשוב להדגיש שההגדרה הזו מתייחס ל"נתוני מידע" – מה שאינו נתון מידע – לא יחולו עליו החובות שבפרק ב'.

חובות מנהל מאגר המידע 0 רישום מאגר

מנהל מאגר 0 מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מיש מנהל כאמור הסמיכו לענין זה (ס'7).

ס' 8: חובות רישום מאגר אצל רשם מאגרי המידע במקרים המנויים בסעיף 8 (ג):

(1)   מספר האנשים שמידע עליהם נמצא המאגר עולה על 10,000;

(2)   יש במאגר מיגע רגיש;

(3)   המאגר כולל מידע על אנשים והמידע לא נמסר של ידיהם, מטעמם או בהסכמתם למאגזר זה

נכון לשנת 2015: למעלה מ-15,000 מאגרים רשומים בישראל, הערכה היא כי רק כ-2% ממאגרי המידע קיימים כרשומים.

**מדוע יש חובת רישום מאגר?**

אנו יוצרים מעין מאגר על מאגרים שיש בו נתונים לגבי המאגר, לרשם המאגר יש אפשרות לפקח מבחינה מהותית והוא יכול לסרב לרשום מאגר למטרה בלתי חוקית (ס' 10 א' 1) ושינוי מטרת האתגר המוצהרת לפי בדיקה של פעילות המאגר בפועל (ס' 0 א 2).

פיקוח על הפעילות – מופנה למגזרים, לא רק למאגרים ספיצפיים

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

במאה ה-21 הזכות לפרטיות נתונה לאיום לא רק מצד השלטון אלא גם מצד השוק

-          תאגידים מסחריים, מעסיקים או בעלי כוח אחר מתבססים על מידע כדי להבין את לקוחותיהם, רצונותיהם ונכונותם לרכוש מוצרים ושירותים. באמצעות המידע מנווטים אותנו לרכוש עוד. **סוחרים במידע ואף מעבירים אותו לממשלה.**

-          אוספי המידע מסווגים אותנו לתבניות **ופועלים על בסיס האפיון שלנו.** סיווג זה יכול להתבסס על מידע חלקי, לא מדויק או שרירותי ולהשפיע מאוד על חיינו.

-          טכנולוגיות מידע מעבירות כוח רב לידי אנשים פרטיים אחרים (למשל בתיוג בפייסבוק).

**מהפכת הפרטיות באירופה: General Data Protection Regulation**

באיחוד האירופי יש שתי צורות חקיקה מרכזיות: דירקטיבה ותקנה. **תקנות אלו מהוות דין מחייב גם מבלי שעבר חוק מחייב בפרלמנט של כל מדינה.** תקנות הגנת המידע האירופיות לוו במהלך מרשים של קנסות, שמתחילים מ-2% ממחזור ההכנסות או מיליון יורו (לפי הגבוה בין השניים). המדרג הגבוה של הקנסות מדבר על 4% ממחזור ההכנסות או 20 מיליון יורו. לפיכך חברות נערכות במרץ כדי להתאים את עצמן לדרישות **ה-GDPR, דבר חקיקה מאוד מקיף שעוסק בעיבוד של מידע אישי.**

אחת הסיבות שאירופה מקפידה מאוד על פרטיות במידע אישי היא השואה, שבה נוצל מידע אישי כדי לבצע רצח עם. הטראומה הזו הולידה **דיני הגנת פרטיות חריפים** ושונים משמעותית מהדינים האמריקניים. הרגולציה האירופאית מתבצעת כלפי **כל סוג של מידע,** גם אם אינו נעשה באמצעות מחשב. המידע צריך להיות **מידע אישי** (כל דבר שמזהה/מאפשר לזהות אדם).

**תקנות ה-GDPR חורגות מהכלל הטריטוריאלי וחלות הן על חברות באיחוד האירופי והן על ארגונים שמעבדים מידע אישי של יחידים באיחוד האירופי,** גם אם אותם ארגונים נמצאים מחוץ לתחום הטריטוריאלי של האיחוד. זאת, בשני תנאים: אם הם מעבדים את המידע מפני שהם **מציעים מוצרים או שירותים** או אם הם **מנטרים התנהגות של יחידים באירופה** (Behavioral Data). זה מקשה מאוד על מוסדות אקדמיים שזקוקים לניטור לצורך מחקרים.

Ø   **הדין לא דבוק לאזרח,** אז אם אזרח צרפתי נוסע לעבוד בנמיביה בחברה מקומית - אין לו זכויות מכוח ה-GDPR. אבל אם פליט סורי עובד בחברה אירופאית הוא כפוף ל-GDPR.

**ההגדרה לעיבוד רחבה מאוד ומקיפה כל פעולה שניתן להעלות על הדעת בהקשר למידע** (איסוף, אחזרה, הפצה, מחיקה, השמדה וכו'). ה-GDPR אומנם עוסק ברובו בדברים שאנו תופסים כפרטיות אך גם עוסק **בזכויות בקשר לעיבוד מידע אישי.** למשל, כל יחיד זכאי לקבל את המידע עליו בפורמט שמאפשר להעביר אותו לארגון אחר.

CONTROLLER הוא הגוף שקובע את מטרות עיבוד המידע והאמצעים לעיבוד המידע.

PROCESSOR הוא מי שמספק בפועל את שירות עיבוד המידע.

לדוגמה, חברה שפיתחה תרופה ורוצה לנסות אותה על נסיינים אנושיים - היא הקונטרולר והמרכז הרפואי שבו מתבצע הניסוי הוא הוא הפרוססור והקונטרול במשותף. על כל אחד מהם יהיו מלוא החובות של ה-GDPR.

דוגמה נוספת: חברת ניהול פרטי לקוחות (פרוססור) יכולה למכור את כל המידע שיש לה על לקוחות שקונים רהיטים. ברגע שהיא לא משתמשת במידע עבור חנות הרהיטים אלא לצרכיה שלה היא הופכת לקונטרולר ביחס לאותו מידע.

ב-GDPR יש שורת עקרונות יסוד ביחס לעיבוד מידע:

-       **עיבוד מידע חייב להיות חוקי, הוגן ושקוף**.

-      **להיעשות למטרה מסוימת -** בעבר מסמכי privacy policy נוסחו בצורה עמומה מאוד ואפשרו לחברות להשתמש במידע למטרות עסקיות נוספות. ה-GDPR מנסה להילחם בכך, משום שבעידן הנוכחי לא תמיד יודעים מה אפשר לעשות עוד שנה עם המידע שנאסף היום. ה-data subject חייב להסכים למטרות עיבוד המידע.

-    **תואם, רלוונטי ומוגבל למטרה -** למשל, חברת AirBnB רוצה לדעת את שמנו, מספר כרטיס האשראי שלנו, דוא"ל וטלפון. אבל היא לא יכולה לדרוש מאתנו למסור את המין שלנו או את סוג כלי הרכב שלנו, כי מידע זה אינו תואם את מטרת העיבוד (שכירת דירה).

-     **המידע צריך להיות מדויק ועדכני -** לא טריוויאלי כשמדובר בארגון שאוסף מידע על עשרות מיליוני אנשים.

-     **החזקת המידע חייבת להיות מוגבלת בזמן -** קל מאוד לשמור מידע לנצח כי רובו טקסטואלי ולא תופס נפח רב. ה-GDPR מאשר שמירת מידע רק לצורך מימוש המטרה.

מה ייחשב לעיבוד מידע חוקי?

**א.**   עיבוד מידע **המבוסס על הסכמה.** להסכמה יש יתרונות וחסרונות (קל מאוד לתת הסכמה אולם יש תחומים שאין בהם תחולה להסכמה, והסכמה תמיד ניתן לבטל).

**ב.**   עיבוד מידע **חיוני לביצוע חוזה** (מעסיק שחייב לעבד מידע אודות עובדיו כדי לתת להם פנסיה, קרנות, אישורי מחלה וכו' גם ללא הסכמה, כי זה חיוני לביצוע החוזה).

**ג.**     עיבוד מידע **החיוני לציות לחוק** (דיני מס הכנסה, צווים של בימ"ש).

**ד.**   עיבוד מידע **החיוני לאינטרס אישי של נושא המידע או צד שלישי** (רופא מטפל).

**ה.**   עיבוד מידע **החיוני לאינטרס הציבורי** (מחקר סוציולוגי).

**ו.**   עיבוד מידע **החיוני לאינטרס לגיטימי של ה-Controller או צד שלישי** (מעבד מידע כדי לשפר את האפליקציה שבאמצעותה הוא אוסף מידע).

כאמור, ההסכמה לעיבוד המידע חייבת להיות חופשית, מוגדרת ומדעת. חובת ההוכחה היא על הקונטרול. כמו כן, ההסכמה חייבת להיות נפרדת בבירור מעניינים אחרים, מוחשית, נגישה בקלות, פשוטה וברורה. **ה-data subject צריך להבין למה הוא מסכים.**

זכויותיו של ה-data subject הן לקבל מידע תמציתי, שקוף, מובן, נגיש בקלות בשפה ברורה ופשוטה, ולקבלו בחינם. **לפי ה-GDPR, אחרי שמידע עובר לחברה עליה לפנות לבעל מידע תוך חודש כדי לוודא שהוא מסכים שתחזיק בו** (טרו קולר).

**ב-GDPR  יש** **עקרון יסוד ("עקרון התאימות") שאוסר על העברת מידע מהא"א למדינות שאינן חברות באיחוד, ורמת ההגנה בהן על מידע אישי אינה כרמת ההגנה על מידע כמו באיחוד.** הא"א הכריז על 13 מדינות כמקיימות רמה מספקת של תאימות. בשנת 2011 ישראל הוכרה כמתאימה (דהיינו, הדין הישראלי תואם את האירופי בכל הנוגע לעיבוד מידע). מותר להעביר מידע רק למדינה תואמת, ואם היא לא תואמת ישנן דרכים מיוחדות להעברה: יש להגיד למושא המידע על העברה והשלכותיה. לחלופין, ישנם הסדרים חוזיים מסובכים.

**בעולם של אינטרנט העברת מידע בין מדינות מתבצעת באופן אוטומטי לגמרי.** כשאנחנו רוכשים משהו באינטרנט המידע עלינו עובר בחלקיק שניה בין עשרים ארגונים. האם ריאלי לסבור שהיוזר יוכל להסכים להעברת מידע כזו, אפילו אם נציג זאת בפניו? גם אם נפרט לו, כדי שיקבל החלטה מושכלת, זה ייקח זמן רב ויהפוך את הקנייה ללא ריאלית.

**זכות העיון והתיקון:**

-          גישה למידע (יחיד תמיד רשאי לגשת למידע עליו)

-          תיקון מידע לא מדויק (יחיד תמיד רשאי לדרוש את תיקונו של מידע לא מדויק לגביו)

-          השלמת מידע חסר (יחיד בעל הזכות להשלים את המידע החסר לגביו)

**הזכות להישכח - The Right to Be Forgotten**

זכות זו אומרת שאדם יכול לבקש שימחקו אותו ממסד הנתונים גם אם המידע נכון, בגלל שהוא לא רלוונטי יותר או שההסכמה לעיבוד המידע כבר לא רלוונטית. זכות זו הוכרה לראשונה **בפס"ד גונזלס נ' גוגל.** בשנת 1998 גונזלס נקלע לצרה כלכלית שבעקבותיה ביתו עוקל, והידיעה על כך הופיעה בגוגל בכל פעם שחיפשו את שמו. עשרים שנה לאחר מכן הידיעה עדיין הופיעה. ביהמ"ש האירופי חייבה את גוגל למחוק את המידע הזה על אף שהיה נכון.

**זכות זו הורחבה מאוד ב-GDPR ומחייבת לא רק את מנועי החיפוש אלא גם את האתרים עצמם שאספו את המידע.** החוק הישראלי עדיין לא מכיר בזכות זו, כי החוק להגנת הפרטיות הוא משנת 1981, שבה עוד לא היה אינטרנט, מידע ביומטרי, גנטי, מצלמות במרחב הציבורי וכו'. במילים אחרות, העולם המודרני של עיבוד מידע לא היה קיים.

**נושא 10 לסילבוס: ניטרליות רשת בישראל ובעולם (עו"ד אורנן שטיינברג)**

**+ המשך נושא 9 לסילבוס**

**ניטרליות ברשת** -

מה המשמעות? עיקרון לפיו יש להתייחס לכל התכנים שמועברים ע"י האינטרנט באופן שוויוני, על הספק הרשת(בזק בינלאומי נניח) לנהוג באופן שוויוני [ולכן אסור להפלות בין תכנים].

1.    אסור לחסום את הגישה שלך לתוכן.

2.    אסור להאט את הגישה לאתרים או תוכן מסוימים.

3.    אסור לספק ולתעדף תכנים בתשלום.

4.    תמחור 0 - במקרה הזה כשספק אינטרנט מציע תוכן למנוי שלו בעלות נמוכה או בחינם.

**יתרונות וחסרונות:**

בעד ניטרליות:

1.  **חופש הביטוי -** ב-2007 היה מקרה מרתק שבארה"ב שידרו הופעה ב WEB של מחווה ללהקה Piny Floyd ואז הם אמרו שהם לא צריכים bosh , מספקי התוכן פשוט צנזרו את השיר כדי לא שאנשים מסוימים לא יפגעו - נפגע חופש הביטוי.

2.    **חדשנות ויזמות -** ברגע שחברות גדולות משלמות הון כדי שהתכנים שלהם יועברו ולא אחרים, זה מונע בחברות חדשות לנסות להצליח, סטרטאפים ימותו כי לא יוכלו להתחרות בחברות גדולות.

3.    **עלויות נמוכות -** אם החברות יצטרכו להוציא מכיסם כדי להשתלט על תכנים מסוימים בספקים בסופו של יום מי שיישא בנטל הכלכלי זה הצרכנים ויצטרכו לשלם יותר כסף על השירותים באפליקציות או אתרים כי נשלם גם על הפרסום והשליטה בספק.

**נגד ניטרליות:**

**1.    עלויות נמוכות -** לא משלמים על כל התוכן אלא רק על חלק ספציפי מכלל התוכן ולכן נוכל לחסוך בחבילת האינטרנט ולכן נוכל לקבוע מחיר על קצת ולא על חבילה שלמה.

**2.    חדשנות ויזמות -** היעדר רגולוציה שווה לחדשנות, יש שוק חופשי.

**3.    שדרוג תשתיות -** אם ניתן לחברות מסוימות להתקדם, והם צריכים המון תוכן (יוטיוב משתמשת ב-30% מהתעבורה), ולכן אם החברות האלו ירצו לשלם על כך יותר בשביל לקבל יותר תוכן, הספקים יסכימו לשדרג את התשתית שלהם כי החברה רוצה עוד נפח ולכן היא תשלם לספק כדי שירחיב את התשתית - כולם מרוויחים.

**4.    החזר על השקעה -** כאשר חברה תשלם כסף לספק הספק יחזיר את ההשקעה על התשתית שבנה.

**5.    זכות הקניין** - ?

**ניטרליות רשת בישראל**

בעבר סלקום הייתה מרוויחה כסף על כל שיחה בפני עצמה. ב-2009 הגיעה חברה קטנה בשם סקייפ, ומה שהם הציעו זה לבצע שיחות דרך אפליקציה בפלאפון בחינם. סלקום חסמה את הגישה לסקייפ.

ההסדר המשפטי - נקבע בחוק התקשורת 51ג שאסור לגרום להגבלה של שימוש בכל שירות או יישום המסופקים ע"י רשת האינטרנט, הסייג לא יכול מהדבר המתחייב על ניהול תקין והוגן של הרשת.

מה קורה במציאות הישראלית? - החברות לא ניטרליות, הם כן מספקות תוכן בצורה שונה וכן נותנות שירותים בתמחור 0.

**ניטרליות רשת בארה"ב**

המרצה הציג את השינויים שחל באמריקה לאורך תקופה מסוימות ברגולציה של הניטרליות. פעמיים זה נפסל למשרד התקשורת האמריקאי ע"י ביהמ"ש בגלל חוסר סמכות, רק בפעם השלישית זה הצליח אך כאשר משרד התקשורת התחלף הם פשוט ביטלו את זה.

לעומת זאת, בחלק מסוים של המדינות יש חוקים וניטרליות רשת למרות שאין חוק פדרלי והוגשה עתירה להחזיר את החוק הפדרלי.

**ניטרליות באירופה**

באירופה אין חובה לניטרליות אך הולנד קיבלה על עצמה את הניטרליות, היא השאיר את התמחור 0 , אך האיחוד האירופי ביטל להם את זה.

**בחזרה לישראל**

אנחנו לא יודעים מה המשמעות של האטה בארץ התוכן, אם בארה"ב יאטו את הגלישה בתוכן זה עלול להשפיע גם עלינו, תלוי מה הספק של התוכן עושה.

**מבט לעתיד**

יכול להיות שנרמה לתעדף, תלוי מה יהיה בעתיד, נניח אם זה לצורך רפואה חכמה נרצה לתת לו קדימה בספקים.

**שיעור 13, 17.06.19**

**נושא 11 לסילבוס: שירותים משפטיים מקוונים**

מתחברים לנושא של יישוב סכסוכים מקוון. היקף השירותים המשפטיים המקוונים גדול הרבה יותר מאלו שידברנו עליהם בתחום יישוב הסכסוכים.

* שירות מקוון חלקי/היברידי (ממשק מקוון שמקשר לשירותים אנושיים).
* שירות מקוון מלא (השירות ניתן באמצעים טכנולוגיים בלבד).

ניתן לדבר על ההבחנה בין ניהול התקשורת בסביבה מתוקשרת (סקייפ/מייל וכו'), קרי הרחבת הנגישות, לבין עיצוב/הבנייה מחדש - בניית אבני הבניין של השירות המשפטי, באמצעות טפסים משפטיים וניהול חכם יותר של המידע, דבר שמאפשר לעסוק בנושאים משפטיים כיחידות מידע, כנתונים של תשובות לשאלות שניתנות לעיבוד אוטומטי, והקטגוריה האחרונה היא **חידוש** - בינה מלאכותית ועיבוד שפה טבעית (al+nlp).

המערכות הללו מייצבות שורה של אתגרים. החל מאיך מתכננים מערכת כזו מקוונת, איך הבחירות בתכנון הטפסים מתבצעות, הממשק שאנו מייצרים (כפתור/סליידר/צבע), משפיעים על השירות וכלה בקופסה השחורה של האלגוריתמים (מכניסים קלט ויוצא פלט שיכול להיות מסמך משפטי, פעולה משפטים, גזר דין, פיצוי - לכל אלו משמעות רבה). מתחבר למה שלמדנו באשר לאכיפה האלגוריתמית בתחום זכויות היוצרים, איך זה עובד? איך מאזנים בין אינטרסים? מדובר בהכרעות משמעותיות וגורליות והפוטנציאל גדול.

מגוון רב של פעולות משפטיות

מגוון רב של פעולות משפטיות ( לאו דווקא פעולות בין 2 אנשים אלא אפילו פעולה של יחיד אל מול הרשות, התוכנה עוזרת לנו ומנחה אותנו).

1.       חוזים

2.       הסכמי עבודה וגריושין.

3.       ייפוי כח

4.       צוואות

5.       מסמכי התאגדות חברה, שותפות, עמותה

6.       רישום פטנט

7.       הסכמי סודיות, אי תחרות

8.       הגשת מסמכים לבית משפט ולרשויות.

המרצה מציגה רשימה של חברות שהתפקיד שלהם זה לעזור למשתמשים בפעולות משפטיות (כמו legalzoom).

ההבטחה הגדולה מעבר לכל השיקולים של יישוב סכסוכים והנגשה פיזית והזמנית/שפתית שהם חופפים לשיעורים הקודמים, זה התמחור שהוא חסר תקדים לעומת עו"ד רגיל. זה סכום מינימלי של כסף בשביל להבטיח נגישות גדולה הרבה יותר לפעולות משפטיות.

**Access to justice author**

התוכנה הזאת מאשרת סטודנטים לקליניקות משפטיות שעובדים בשת"פ עם גורמי חברה אזרחית ועוזרים להם לתרגם פעולות משפטיות בשירות עצמי וכלים לבצע את הפעולות הללו באופן עצמאי, כאשר כל הפעולות הללו נשענות על שאלון אל מול המשתמש.

מה האחריות שלנו בעיצוב מוצרים מהסוג הזה? כיצד אנחנו מנסחים את השאלות הללו? כיצד ממשק המשתמש משפיע על הבחירות שלנו

הדבר הזה נקרא הינדים דיגיטליים.

**הינד** - קבלת ההחלטות של המשתמשים מושפעת מאופן הצגת אפשרויות הבחירה:

1. התוכן וההצגה החזותית מפעילים הטיות קוגנטיביות.
2. רציונליות מוגבלת - הגם שאנו יכולים לחשוב שהבחירה מושקעת מחשבה רציונלית ומוסרית וכיו"ב. למעשה, נמצא במחקרים, כי השאלה המרכזית היא איך אנחנו רואים את הדברים ואיך בפועל האפשרות מוצגת לנו.

חשיבות יתירה לעיצוב ממשק המשתמש:

1. מיקום על המסך

2. צבעים

3. סוג כפתורים/אופן ביצוע פעולות/ חיווי החלטות

ההינד פועל בעת קבלת ההחלטה.

המרצה מציגה טופס שבו רואים שברירת המחדל של התשובה (שכבר מסומנת) בדר"כ לא משתנה. אם הבוחר משנה את הבחירה הוא לרוב ישנה לפי מה שמליצו לו בתצוגה (עוגן).

כשאנו מדברים על תכנון ממשקים וטכנולוגיות משפטיות, החלטות מנהלי המוצר הללו מאוד משפיעות על בחירות המשתמשים.

אם מבקשים ממישהו לסמן בסקאלה, מאוד משנה על מה הסמן עומד (0 או 50); גם סדר הצגת אפשרויות התשובה משנה ומשפיע.

שירות משפטי באמצעות צ'ט בוט - robotlawyer

דוגמה לשירות שכבר עובד.

* חוויית משתמש של שיחה אינטראקטיבית.
* עיבוד שפה טבעית.
* התאמה של מסמכים.
* הגשה מקוונת לרשות.
* הדגמה באתר הקורס - שירות DO NOT Pay.

עד כאן, נראה שזה בשוליים ובפריפריה של ביטול דוחות חנייה ועבירות תנועה מינוריות.

מערכות תומכות החלטה בעבודת המשפטנים! מערכות משפט אוטומטיות?

מערכות שמסייעות למשפטן לעשות עבודתו בצורה טובה יותר ע"י חיזוי או הפקה של טקסטים משפטיים. למשל:

1. חישוב פיצויים
2. חישוב גזרי דין
3. חישוב סיכויי תביעה
4. חישוב סכום לפשרה

* סטטיסטיקה תיאורית של הליכים שופטים עו"ד ועוד.

מערכות תומכות החלטה כבר קיימות והן בשימוש כיום, בעיקר בחו"ל. מקום בו השוק המשפטי מצדיק את הכסף הרב בפיתוחים מעין אלו.

בישראל, יש אפילו כסף ממשלתי שעוסק בפיתוח הטכנולוגיות לשירות עוה"ד מטעם המדינה.

**השאלה הגדולה היא שאלה של אתיקה**: מתי נאמר לשופט אתה לא רק צריך לשקול מהי התוכנה המיטבית עבורך אלא מתי נאציל את הסמכות לתוכנה הזו ואף נוותר על המעורבות האנושית?

חיזוי אלגוריתמי לצורך הליכי גילוי מסמכים מוקדם

* האתגר: בעידן הדיגיטלי - גידול בכמות המסמכים שמוביל לגידול בשעות האדם הדרושות כדי להעריך את הרלוונטיות של כל מסמך להליך המשפטי.
* הפתרון הטכנולוגי: תוכנות שמבצעות חיפוש אוטומטי במסמכים באופן שמחקה את תהליך האיתור והמיון של אדם בעל הכשרה בתחום (מחפשות את כל המסמכים הרלוונטיים בתיבות האימייל של התאגיד, בתיקיות וכיו"ב).
* התוצר: ניבוי בדרגת וודאות גבוהה יחסית ביחס לשאלה אם מסמך כלשהו רלוונטי להליך ספציפי שמוביל לפחות שעות אדם הדרושות להערכת מסמכים.
* הקושי: שגיאה מסוג 1 - זיהוי חיובי שגוי. שגיאה מסוג 2 - אי-זיהוי שגוי (האלגוריתם לא זיהה מסמך רלוונטי). ברי, כי השגיאה השנייה חמורה יותר, מאחר שהאדם עובר רק על התוצרים של התוכנה, ולכן על שגיאה מסוג 1 יעלה, אך על שגיאה מסוג 2 לא.

דוגמא למערכות:

מערכת compass שנמצאת בשימוש בארה"ב ושופטים משתמשים בה כדי לחזות את רמת המסוכנות של אדם ששוקלים אם לשחרר אותו בערבות או לא, היא לוקחת 137 משתנים את חלקם היא שואבת מתוך תשובות של החשוד לשאלות שהחשוד צריך למלא ועל בסיס 137 משתנים היא מוציאה פלט שאומר לשופט מה רמת המסוכנות. זה משווה כנגד מוסד נתונים שהיה בעבר.

מערכת hart היא מערכת מגבילה באנגליה שהיא מנסה להעריך סיכוי שנאשם יחזור לפשוע בתוך שנתיים על בסיס של 34 משתנים שהשוטרים מזינים באופן ידני והפעם התוצאה תשפיעה על האם הוא יקבל תכנית שיקומית כחלופה למעצר. המערכת מתוכננת להעדיף שגיאות מסוג 2 על פני שגיאות מסוג אחד.

ההשוואה תמיד נעשית על בסיס הנתונים מהעבר, שהמערכת למדה להעריך את רמת המסוכנות. לדוג': אם יש כמות רבה של נאשמים בעלי מאפייני אתני מסוים, השכונות מהם הגיעו בעלות ממוצע סוציו-אקונומי מסוים, והסיכוי להיעצר בהן גבוהה יותר בגלל נוכחות גבוהה יותר של המשטרה. המערכת משכפלת את אותן הטיות שהיו כנגד שחורים כשבני אדם קיבלו את ההחלטה בפלט הזה של האלגוריתם. **צריך לזכור שגם התוכנות הללו בעיות הטיות, מאחר שמה שנכנס לתוכן זה סך הגזענות מהעבר.** ככל שהמערכת לומדת יותר נתונים היא צריכה להשתפר ביכולות שלה.

הקושי המרכזי במערכות מהסוג הזה הוא שאנו לא יודעים בדיוק מה קורה בקופסות השחורות הללו. אותה בעיה שדיברנו עליה בהקשרי אכיפה אלגוריתמית בזכויות יוצרים, באשר לאינטרסים ולזכויות.

ייתכן שהמערכת הזו גם מביאה בחשבון כל מיני תכונות שלא היו נלקחות בחשבון ע"י שוטר למשל (כמו גובה של אנשים).

חיזוי אלגוריתמי: ביקורת והערכת סיכונים בחוזים

האם המערכות הללו עושות טעויות יותר או פחות מבני אדם?

אחת החברות שניסתה ליתן טעימה לעניין הזה היא חברת LAWGEEK. החברה יצרה תוכנה שמאפשרת לקחת חוזים, לסרוק אותם ולאתר בהם סיכונים משפטיים (סיכון משפטי-משהו שהלקוח/החברה הגדיר/ה כבעייתי, שהוא/היא לא רוצה בחוזים שלו/שלה).

החברה הזו עשתה תחרות וניסתה למדוד שני דברים: מי יעיל יותר (כמה זמן לוקח לביצוע המשימה)? ומי מדייק יותר? המשימה הייתה לקרוא 5 הסכמי NDA = הסכמי סודיות. השאלה הייתה: איזה שיעור של סיכונים משפטיים בחוזה הזה (עסקאות הסותרות מדיניות משפטית בארגון) התוכנה תזהה לעומת עוה"ד. היא נתנה זאת ל-20 עו"ד, בדרגות בכירות שונות, ובמומחיות המתאימה.

לעוה"ד לקח בממוצע 92 דקות בממוצע. לעומת התוכנה שלקח לה 26 שניות. ושיעור הדיוק אצל עוה"ד 85%, לעומת 94% אצל התוכנה.

חיזוי וניסוח: מערכות לניתוח וניסוח מסמכים משפטיים

**PROMETEA** - מערכת שנוצרה בשת"פ של אקדמאים ומשפטנים בבואנוס איירס. המערכת הזו מנסה לעשות אוטומטית 2 דברים:

1. הפקת מסמכים משפטיים: כתבי בי"ד שתוכל הפרקליטות להגיש לביהמ"ש.
2. ניבוי תוצאות משפטיות של הליכים.

הפרקליט מכניס למערכת את מס' התיק (קלט) ומה שהוא מקבל (פלט): שאלות מנחות רלוונטיות ומסמך משפטי של השלב הבא בהליך.

המערכת משתמשת על בסיס הנתונים: כ-10,000 פס"דים, כ-300,000 מסמכי פרקליטות וכ-1500 חוות דעת משפטיות.

המערכת הזו עדיין במסגרת פיילוט. אולם ישנן 3 סוגיות משפטיות(דיור; מוגבלויות; דיני עבודה) בהן היא נוסתה והטענה היא שהיא בעלת שיעורי הצלחה גבוהים (אם בהפקת המסמכים ואם בניבוי).

מה משמעות התוכנות הללו למקצוע

האם ישנה אפשרות בישראל להשתמש בתוכנות הללו?

בישראל מה שנפוץ כיום הוא ניתוח כמותי של פס"דים בביה"ד לעבודה (DISPUTEC); תוכנת נזיקליק (תקדין) מאפשרת להוציא סכום פשרה לתיק או כמה שווה תיק נזיקין.

מצד אחד, ישנה הבטחה גדולה של הגברת הנגישות של השירותים המשפטיים. לכל הפחות ישנה דרך להוזלת השירות שעוה"ד נותנים. ישנה אפשרות לחשוב על מודלים חדשים של עבודה משפטית, כזו שבחלקה נעשית באון עצמאי ע"י הלקוח. ישנו שק גדול מאוד של סכנות אתיות ומשפטיות שאנו כחברה צריכים לשקול באילו תנאים אנו מוכנים לקחת אותן, כאשר אנו נותנים לאלגוריתמים לבצע הפעולות הללו ולא לבני אדם. וכאן המקום לכללי הסדרה:

אתגרים לפיתוח מיזמים משפטיים טכנולוגיים בישראל

* כללי ההסדרה המקצועיים של עורכי הדין:

1. חוק לשכת עורכי הדין
2. כללי האתיקה המקצועית

* הנורמות האתיות והמקצועיות התפתחו בעידן שלפני טכנולוגיות המידע (ולפני יישומן בתחום המשפט).

אלו בשני עניינים עיקריים:

1. ייחוד פעולות המקצוע (הסגת גבולות המקצוע).

הס' המרכזי הוא ס' 20 לחוק לשכת עורכי הדין: ייחוד פעולות המקצוע - תת סעיפים (1)-(4).

1. איסור שיתוף בהכנסות או קבלת הפניה של לקוח שנעשתה למטרות רווח.

* האתגר: האם חברות טכנולוגיות שמבקשות לספק שירותים מקצועיים ע"י מי שאינו עו"ד מסיגות את גבול המקצוע.

שירותים משפטיים מקוונים: הסגת גבול המקצוע?

* מתן מידע משפטי באמצעות אתר מקוון אינו אסור כשלעצמו.
* ייעוץ משפטי או מתן חוו"ד משפטית ע"י מי שאינו עו"ד - אסורים.

מה האינדיקציות כדי להחליט האם מדובר במתן מידע או בייעוץ?

1. ככל שהמידע כללי יותר ולא מתייחס למקרה עובדתי קונקרטי זה מידע.
2. ככל שהמידע נשען על נסיבות פרטניות של הפונה ועל העובדות הקונקרטיות אנו נכנסים לגבול הייעוץ.

* השאלה הבסיסית היא האם המידע/השירות/הייצוג בנסיבות המקרה הם משפטיים?

אמות המידה נקבעו בהלכת "המרכז למימוש זכויות רפואיות" (לבנת פורן).

**ע"א 4223/12 המרכז למימוש זכויות רפואיות נ' לשכת עוה"ד**

השאלה: כיצד נפרש מונחים כמו "ייצוג" ו"אופי משפטי" בס' 20?

1. נק' המוצא: אין למונחים הגדרה ממצה שניתן לקבוע מראש.
2. תכלית הסעיף: להבטיח שלא ייגרם לציבור נזק כתוצאה משירות משפטי לקוי.

רק בעלי ידע והכשרה מתאימים יעניקו שירות משפטי.

הקושי: ייחוד המקצוע=מונופול שפוגע בזכויות ואינטרסים של אחרים: חופש העיסוק; אוטונומיה לבחור; נגישות.

אמות המידה שיש לשקול בהכרעה אם פעולה או שירות ייחודים למקצוע עורך הדין

1. היקף שיקול הדעת שכרוך בביצוע השירות או הפעולה הניתנים לציבור. (שיקול דעת רחב תוך שקלול משתנים רבים = ייחוד; פעולה טכנית בעיקרה שאינה מצריכה בחירה בין דרכי פעולות רבות = ללא ייחוד.
2. פוטנציאל הנזק לציבור עקב שירות לקוי - ככל שפוטנציאל הנזק משמעותי יותר והנזיק בלתי הפיך = ייחוד.
3. איזו חלופה עומדת לציבור במימוש זכויותיו אם ייאסר מתן השירות ע"י מי שאינו עו"ד (בשים לב למחיר).

**ת"א 50926-10-15 לשכת עורכי הדין בישראל נ' חשבים ה.פ.ב מידע עסקי בע"מ ח.פ - 5122799855**

ביהמ"ש (כשהיה צריך להכריע האם שירות של מחולל חוזים שמאפשר למעסיק להיכנס ולהרכיב חוזים דרך אלגוריתם כלשהו) קבע, כי מחולל חוזי העבוד, מחולל סיום יחסי העבודה הוא דבר טכני. נקבע כי לא מדובר בהפעלת שיקול דעת. השופטת התייחסה לפלטפורמה הזו כפלטפורמה של שירות עצמי, ועשתה הקבלה להורדת נוסחים מהאינטרנט ובחירת התניות המתאימות. היא הדגישה את העלות הנמוכה ואת פוטנציאל הנזק הנמוך.

הלשכה ערערה לעליון ובפרוטוקול נאמר ללשכה לחשוב טוב אם היא רוצה פסק-דין, והיא החליטה למשוך הערעור.

בהליכים קודמים, הסוגייה הזו לא זכתה לפרשנות זהה. יש לנו ניצני פסיקות ביחס לשירותים משפטיים מקוונים וימים יגידו איך עלינו לפרש את כלל ייחוד המקצוע והאם אלו ישתנו. נדגיש כי לא מדובר בבינה מלאכותית או באלגוריתם שעושה הדברים לגמרי מעצמו.

**באשר למבחן:**

המבחן יהיה במתכונת של 4 שאלות פתוחות. בחלקן יהיו סעיפי משנה. יחד עם המבחן, נקבל, ככל שנצטרך, נספח חקיקה רלוונטי ולכן לא צריך לזכור ס' בע"פ. סילבוס לא יצורף למבחן. השאלות בחלקן שאלות חשיבה ויישום מסוג הדיונים שנוהלו בכיתה (שיקולים או ניתוח סיטואציות); בחלקן שאלות שמחברות בין נושאים שונים שדיברנו עליהם בקורס. תמות: כמו מה מקום גורמי הביניים ברשת; 4 גורמי ההסדרה במודל לסיג בסיטואציות שונות; המתחים שעולים בשימוש באלגוריתמים; האתגרים שהעידן הטכנולוגי העלה. **המבחן בחומר סגור. 3 שעות. (**הרעיון הוא לגרות את המחשבה והחשיבה על מתחים/שיקולים/סוגיות שעולות; אין תשובה חד משמעית ברורה וקבוע וזה טבעו של התחום והקורס; יש לגשת לשאלות בצורה אינטליגנטית). **ייפתח פורום שאלות.**