**שיעור 1 - 5.3.18**

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

עידן של מהפכות טכנולוגיות

טכנולוגיות מידע חדרו לכל תחומי החיים שלנו. האינטרנט הפך לזירת פעילות חברתית, מסחרית-כלכלית, מקצועית, ציבורית, פוליטית ולעיתים גם עבריינית/טרוריסטית.

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

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

התפתחות המשפט אינה תואמת את קצב ההתפתחות הטכנולוגיות:

* חוק מור אומר שכוח המחשוב מכפיל עצמו כל 18 חודשים.

תהליכי השינוי שמחוללות טכנולוגיות המידע הם דינמיים ומתרחשים בקצב ובעוצמה חסרי תקדים. לא מדובר באירוע חד פעמי ועל כן **הפתרון אינו תגובה משפטית נקודתית.**

כיצד, אם כן, מערכת המשפט מתמודדת עם הצורך בשינוי והתאמה?

1. **פרשנות משפטית -** שימוש בעקרונות משפטיים ומושגי שסתום שלתוכם ניתן לצקת משמעויות חדשות שיתאימו לקצב השינויים הדינמי.
	* **חקיקת משנה, הנחיות מנהליות, סמכויות רגולטוריות, פסיקה (פעם ב.**.. חקיקה ראשית)
	* **פיתוח פרדיגמה לבחינת סוגיות שמערבות משפט וטכנולוגיה**
2. הבנה של הקשר המורכב בין משפט וטכנולוגיה משפרת את היכולת **לפתח כלים משפטיים מתאימים.**

**בקורס נפתח חשיבה פרדיגמטית על משפט וטכנולוגיה?**

* מסגרת אנליטית לבחינה יחסי גומלין בין משפט וטכנולוגיה
	+ טכנולוגיות שמאתגרות את ההסדר המשפטי הקיים או את אופן פעולת המשפט
* התמקדות בשאלות שנוגעות לרגולציה של טכנולוגיה ובאמצעות טכנולוגיה

נקודה מרכזית: שינוי במעמד המשפט כמערכת שמסדירה התנהגות באמצעות כללים שנאכפים בבתי המשפט ע"י רשויות אכיפת החוק.

1. הפרטת האכיפה, אוטומציה, שקיפות, פיקוח, פיתוח נורמות וכללים, גיבוש וערכים
2. סדרי גודל חסרי תקדים של מידע ושל פעילות
3. שינוי בהתנהגות ובתפישות החברתיות?

האם יש צורך בפרדיגמה של משפט וטכנולוגיה?

כשמתמודדים עם טכנולוגיה חדשה לא מדובר רק ב - (1) **התאמה של הכללים הקיימים לטכנולוגיה חדשה** אלא מערכת חדשה של שיקולים שלא מאפשרת ליישם את הדין הקיים בסיטואציה חדשה, ולפיכך מחייבת (2) **עיצוב כללים משפטיים חדשים.**

* פרדיגמה = המערך הכולל של העמדות, התפיסות והשיטות המגדירים את החשיבה המדעית בתקופה נתונה בתחום מסוים.

אחד הדברים המרכזיים שנדון בהם בקורס הוא מוגבלות המשפט במתן מענה לאתגרים שהעולם הטכנולוגי מציב. הצורך של משפטנים לפתח הבנה של המרחב והשיקולים הסובבים אותו משמעותי. אם חושבים על מטרות המשפט (הכוונת התנהגות, קידום וביסוס ערכי היסוד של השיטה, צדק, יעילות ונגישות וכו') צריך לשאול איך ניתן להגשים אותן נוכח האתגרים החדשים?

מדובר במערכת מורכבת של יחסי גומלין, ובכל סיטואציה יש למצוא את הכלים המחשבתיים שמאפשרים לגשת אליה.

מתי עולה הצורך בחשיבה כזו אצל משפטן? ניסוח חוזים ותקנונים לאתרי אינטרנט; קבלת החלטות מנהליות ושיפוטיות; חקיקה של תקינה טכנולוגית ומדיניות טכנולוגית ; עיצוב מדיניות בכל תחום עם ממשק טכנולוגי; מעורכות תומכת בעיצוב טכנולוגיה ועיצוב מוצר וכו'.

כיצד המשפט מגיב לשינויים טכנולוגיים?

התפתחויות טכנולוגיות מאלצות את מערכת המשפט לבחון את התאמתם של כללים משפטיים קיימים למציאות חדשה. התשובה מחייבת בחינה של תכלית החקיקה והבנה של הסביבה הטכנולוגית.

 דוגמה – תעמולת בחירות באינטרנט.

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

עם זאת, המשפט אינו חסר אונים ומסדיר משמעותית התפתחויות טכנולוגיות. התערבות משפטית יכולה להשפיע על טכנולוגיות המותרות לשימוש, על אופן יישומן, על עלות הפעלתן ועל היתכנותן של טכנולוגיות חלופיות. דוגמאות:

**א. מגבלות בחוק על פיתוח וייצור טכנולוגיות** (סוגים שונים של הצפנה; פריצת מנעולים טכנולוגיים שנועדו להגן על זכויות יוצרים).

**ב. מתן תמריצים לפיתוח טכנולוגיות מסוג** מסוים (תקנות הגנת הפרטיות (אבטחת מידע) 201 – תמריץ לפיתוח מערכות אבטחה.

**ג. הטלת אחריות משפטית בגין שימוש בטכנולוגיה אחת יכולה לעודד פיתוח של טכנולוגיות אחרות** (נפסטר, תוכנה לשיתוף קבצים, נמצאה אחראית להפרת זכויות יוצרים; איימסטר, חברה שהצפינה את התקשורת שלה כדי לטעון שלא יכולה להיות לה ידיעה על הפרות זכויות יוצרים - אך הפרקטיקה נפסלה ע"י ביהמ"ש; כך נולדה פטפורמה של שיתוף קבצים מבוזר (מלקוח אחד לאחר) + תוכנה חופשית + creative commons). 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.

המודל של לורנס לסיג - CODE IS LAW

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

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

גישה מהותנית-ערכית למשפט וטכנולוגיה

הטכנולוגיה מגלמת בתוכה ערכים. באופן עקיף: הטכנולוגיה מתפתחת המענה לרכים של החברה ומעוצבת בהתאם להם. האופן ישיר: טכנולוגיה שמתוכננת בכוונת מכוון לגלם ערך מסוים (תכונות סינון – בקרה הורית/ עצמית/הלכתית על תכנים באינטרנט; ארכיטקטורת האינטרנט כרשת נטולת שליטה מרכזית – אוסף של צינורות, תקשורת נתונים מקצה לקצה מגלמת ערכים של ביזור.

לעיתים משמעות הטכנולוגיה נקבעת בדיעבד, לא רק ע"י המתכנתים והמפתחים אלא גם ע"י המשתמשים.

המשמעות של ההשפעה המרובעת הזו על הפעילות האנושית היא שמי שרוצה להסדיר את המדיניות נהנה מסל כלים עשיר. למשל, כדי למנוע חשיפה של ילדים לתכנים פוגעניים באינטרנט ניתן לקבוע כללים משפטיים פליליים או כללים חוזיים כלפי המשתמשים באתר. אולם, הפתרונות המשפטיים כשלעצמם מציעים מענה חלקי בלבד. ישנם פתרונות שוקיים או טכנולוגיים שיכולים להתפתח (למשל תוכנות סינון שמונעות מילדים גישה לתכנים מסוימים).

**החוק הוא לא תמיד הפתרון המיטבי או ההכרחי לסוגיה.** לעיתים די בטכנולוגיה, בכוחות השוק או בנורמות חברתיות.

האם זה בסדר שמערכת המשפט תיתן לגורמים פרטיים לבצע אכיפה ושיטור? האם הערכים שמוטמעים בקוד התוכנה משקפים באמת את הערכים החברתיים? איך ניתן לפקח על כך?

המודל של ניבה אלקין קורן ומיכאל בירנהק

ניבה אלקין קורן ומיכאל בירנהק הציעו משולש של משפט-טכנולוגיה-ערכים. בעוד שהקשר בין הטכנולוגיה למשפט הוא אינסטרומנטלי ומהותני, הקשר בין ערכים למשפט הוא פרשני ותורת משפטי.

**גורמי ביניים ברשת האינטרנט**

החלום והחזון של רשת האינטרנט: ביל גייטס טבע את המונח "האינטרנט הוא כיכר העיר החדשה". כל מה שנמצא בכיכר העיר נגיש לכולם וכולם יכולים להגיע אליו, כמו כן האינטרנט הוא המרכז.

האינטרנט ככיכר העיר החדשה

* מרחב ציבורי וירטואלי בו כל אדם יכול לקחת חלק פעיל בשיח הציבורי.
* אנטי-תזה לריכוז השליטה בידי אמצעי תקשורת מעטים. היחלשות העיתון והטלוויזיה.
* התפישה: אופייה המבוזר (לא ריכוזי) של רשת האינטרנט מקדם ערכים חברתיים (מאפשר אופנים חדשים שבהם ערכים חברתיים יכולים לבוא לידי ביטוי).חופש המידע, חופש הביטוי, החירות האישית של כל אדם ובגלל הורדת החסמים ויכולות השיתוף הגדילו את החדשנות – יכולות להגדיל את סוגי המודלים.

(האנונימיות – יכולות לבצע פעולות ולומר דברים בלי לדעת מי אמר אותם, אפשרויות מסחר ושירותים גדולות יותר.)

**חזון האינטרנט ככיכר העיר החדשה נשען על אופיה המבוזר**

1. האינטרנט = רשת של רשתות מבוזרות
* אין סמוכת מרכזית יחידה שממונה על ניהול האינטרנט
* ניהול מבוזר ושיתופי במודל של "בעלי עניין מרובים"
* נחזור לנושא כשנלמד על ניטרלית רשת.
1. חסמי כניסה נמוכים לאינטרנט => גיוון במשתתפים ובשיח
* אין צורך בהקצאת ערוצי שידור (ולכן גם לא ברישוי ובפיקוח הנלווים לכך)
* עלות מינימלית להפצת תוכן ברשת. אם בעבר כדי לפרסם תוכן היה צריך לקנות את האפשרות הזו, היום העלות היא מינימלית.
1. המדיום – אמצעי התקשורת מאפשר תקשורת ישירה בין משתמשים=> הגדלת מגוון התכנים
* ביטול התלות במסננת העריכה של אמצעי התקשורת המסורתיים
* לגולשים ברשת נתונה אוטונומיה להגדיר את סדר היום בעצמם
1. התפתחות מאגר עשיר ודינמי של תוכן חופשי ממקורות מגוונים
2. החלשת כוחם של מוקדי השליטה בשוק התקשורת והתוכן

**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.

גורמי ביניים ברשת האינטרנט – מתווכים ברשת

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

**סוגים של גורמי ביניים:**

* ספקיות הגישה לאינטרנט
	+ מקצה לכל משתמש שם וכתובת המאפשרים לו להיות מחבור לרשת (אינטרנט זהב, בזק)
* ספק תוכן ושירותים
	+ מציג תוכן באתר לשם הפצתו בין משתמשים (למשל: וואלה, ווינט)
	+ פלטפורמות מסחר ושירותים (איביי, אמזון)

שלושה דורות של גורמי ביניים ברשת

הדור הראשון: שיתוף וקישור למידע

* תכלית מרכזית : שיתוף וקישור למידע וידע (גוגל)

הדור השני: מסחר ושירותים

* זירות מסחר כמו איביי, אמזון ושירותים שונים כמו החלפת קבצים (נאבסטר).
* הובילו לשינויים משמעותיים בתעשיית ההוצאה לאור, חדשות ומדיה, מוזיקה וקמעונאות.

**שיעור 2 - 12.3.18**

ישנן שתי גישות מרכזיות להבן הקשר בין משפט וטכנולוגיה:

1. הגישה הדטרמניסטית-אינסטרומנטלית להבנת צלע הקשר בין משפט וטכנולוגיה

כופרת בקיומו של קשר בין משפט לטכנולוגיה. **לטכנולוגיה אין ערכים מוסריים או נורמטיביים והיא פונקציונלית בלבד -** שיטה ניטרלית ליישום והטמעה של ידע בתוך מכשיר. תפקיד הטכנולוגיה לאפשר למשתמש להגשים מטרה, וכשלעצמה **חסרת טבע מוסרי** ואדישה למטרות השונות שניתן להשיג באמצעותה (חיוביות או שליליות).

אי אפשר, בהתאם, לעצב טכנולוגיה כמכשיר משפטי כי היא מתפתחת בהתאם לכלליה שלה, ללא אינטראקציה עם גורמים אחרים. גישה זו מיושנת וכיום קשה למצוא לה תומכים.

1. גישה מהותנית-ערכית להבנת צלע הקשר בין משפט וטכנולוגיה

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

לעיתים משמעות הטכנולוגיה נקבעת בדיעבד, לא רק ע"י המפתחים אלא גם ע"י המשתמשים.

שלבים בהתפתחות הטכנולוגיות הדיגיטליות

* האינטרנט כפלטפורמה לתקשורת בין-אישית (הפצת מסרים במייל ובפורומים; מתן שירותי תיווך, מנועי חיפוש, מדיה חברתית וכלכלה שיתופית).
* האינטרנט כרשת להפצה של מוצרים (הורדת קבצים כתחליף לעותקים מוחשיים; התרחבות הכלכלה השיתופית [UBBER]; ביזור באחסון ובעיבוד של מידע)

השלב האחרון הוא **האינטרנט של הדברים וכלכלת המידע:**

* האינטרנט כרשת של תקשורת עם "דברים" (מכשירים חכמים; טכנולוגיות מידע ICT מתרחבות לכלל תחומי החיים (חיישנים מתקדמים, סטנדרט תקשורת סלולרית)
* יכולות עיבוד מפותחות שהולידו אלגוריתמים לתמיכה בהחלטות/קבלת החלטות (טכנולוגיות אלו הולכות ונעשות מורכבות יותר עם התקדמות בכוח המחשוב והידע שלנו בתחומים כמו ביג דאטה, אינטליגנציה מלאכותית, למידת מכונה, אינטראקציה בין מכונה לתוכנה [רובוטים יכולים להחליף פעולות של בנ"א ולבצע פעולות בעולם הפיזי]).

יישוב סכסוכים בעידן הדיגיטלי - ממסחר מקוון לבתי המשפט

בקורס נעסוק בשתי זוויות: הראשונה היא **האתגרים של הטכנולוגיה והעולם המקובל,** כיצד מתמודדות איתם מערכת המשפט או מערכת חלופיות אחרות שלוקחות חלק ברגולציה שלהם; השנייה היא **הכלים שהטכנולוגיה נותנת לעולם המשפט כדי להגשים את תכליותיו** (הכוונת התנהגות, הסדרת מערכות היחסים של הפרטים).

ODR יישוב סכסוכים מקוון

מערכות ליישוב סכסוכים שמאפשרות להשלים את ההליך במלואו \_מהגשת התביעה/ התלונה/ הערר ועד לסיום הכרעה או הסכם) על גבי לפט]ורמה מקוונת. לעיתים מתאפשרת גם אכיפה באופן מקוון.

מונח גג: מקורות וסוגים של סכסוכים, שיטות יישוב סכסוכים, טכנולוגיות שונות ותהליכים שהם שילוב של שיטות ויישוב והטכנולוגיה שמתאפשרים במרחב המקוון.

שני מכונני מהפכת הODR:

**קולין רול:** מייסד תחום יישוב הסכסוכים של איביי. בחברת איביי היו קונים ומוכרים רבים שרצו לבצע עסקאות באמצעות המערכת, אך נתקלו בבעיה רצינית אם משהו השתבש במהלכה (החבילה איחרה להגיע או אם המוצר היה תקול). האתגר היה בכמות הרבה של הסכסוכים (60 מיליון בשנה!), היו להם מאפיינים דומים (מוכר וקונה ממדינות שונות, על סכומים יחסית נמוכים בממוצע מאה דולר), כאשר לא היה ברור מה סמכות השיפוט הרלוונטית ביחס אליהם (כי מדובר בפלטפורמה מקוונת, שבה המוכר ממדינה אחת והקונה ממדינה אחרת). בהיעדר פתרון יעיל למשתמשים במערכת לא היה ביטחון ואמון בה, והיה חשש גדולה שהם יינטשו את הפלטפורמה ויפסיקו לבצע דרכה עסקאות. היה ברור שלא שווה לפנות לבימ"ש או אפילו למגשר/בורר באופן פרטי נוכח הכמות הגדולה של העסקאות, ושווין הנמוך יחסית (100 דולר). כל אלה הובילו ליצירת המערכת ה-ODR הפרדיגמטית.

**מייקל בריגס:** לורד צדק ושופט בביהמ"ש העליון באנגליה, שהופקד על הרפורמה במערכת המשפט האזרחית שתתמודד עם כמה בעיות יסוד של מערכת המשפט. בשנת 2016 הוא הוציא דו"ח על שמו, שהמלצתו העיקרית הייתה הקמת תיקים מקוונים עבור הליכים אזרחיים במערכת בתי המשפט באנגליה. הבעיה של בריגס הייתה שבמערכת המשפט האנגלית הייתה כמות עצומה של מייצגים עצמיים (אנשים שפועלים ללא עורך דין נוכח העלויות היקרות של השירותים המשפטיים, כי גם עבור מי שידו משגת העלות של הליכים היא מאוד גבוהה),בעיה נוספת היתה הנגישות, יש להגיע פיזית לבית המשפט ולא תמיד נוח להגיע כי הם לא מפוזרים בצורה נוחה בעולם, וגם המורכבות של החוק עצמו וחוסר הנגישות של אנשים לייצג את עצמם, מה שהוביל לעומס תיקים גדול ועיכוב בניהול התיקים, שגרר ביקורת גדולה על הנגישות למערכת המשפט. הלורד בריגס חשב שהפתרון לכך טמון בהקמת בתי משפט מקוונים, שגבול הסמכות שלהם יהיה ב-25 אלף פאונד (בעוד שתביעה קטנה באנגליה שווה 10 אלף פאונד). כלומר, זהו פתרון ממשי עבור כמות גדולה מהתיקים האזרחיים.

ODR יישוב סכסוכים מקוון (עובד מסיכומים של שיר ואור)

תופעת ה-ODR נבעה מהעלייה השימוש בשירותים המקוונים באופן כללי, זירה חדשה של מערכות יחסים עסקיות, אישיות ואחרות, והזירה הולידה סוג חדש של סכסוכים וצורך בהבטחת אמון המשתמשים והצורך בפתרון יעיל ואפקטיבית ליישור סכסוכים. שירותים רבים מסופקים באופן מקוון, נגישות ומסוגלות טכנולוגית, ואפילו ציפייה לשירותים מקוונים – "ממשל זמין". זה הוביל ליזמות, חדשנות גם בעולם של היישוב הסכסוכים. ועדיין קיימים פערים בנגישות טכנולוגית.

יישוב סכסוכים מקוון כחלק מהמגמה ליישב סכסוכים בדרכים חלופיות

תנועת הנגישות לצדק +תנועת הADR – יישוב סכסוכים בדרכים חלופיות. למשל, גישור, בוררות, הערכת מומחה מקדמית, מו"מ, והם קיימות גם בתוך מערכת המשפט.

הרעיון שעמד בבסיס תנועת ה נמצאה התפיסה שע"י כך שנציג דרכים שונות אנו נרחיב את הנגישות לצדק, היתה גם שאיפה להתאמת ההליך לבעלי העניין: צרכים יכולות, אינטרסים, מטרות ושאיפה ליישוב סכסוכים באופן מהיר, זול, נגיש, יעיל, פשוט–פרוצדורלית.

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 הODR כ"צד רביעי" בסכסוך

מקרה פרטי של code is law .

בעולם הXDR יש צד רביעי שיש לו תפקיד בעיצוב הממשק והמערכת הטכנולוגית משפיעים על הליך יישוב הסכסוך. השפעה זו אינה ניטרלית בהכרה וע"פ רוב אינה שקופה למשתמש.

תפקיד אינסטרומנטלי: מערכת הODR מופעלת ע"י אדם למשל אמצעי תקשורת, כלי לביצוע משימות קונקרטיות שמופעל בהנחיית המגשר.

מערכת הODR כ"צד שלישי" בסכסוך

כל המאפיינים של מערכת ODR כצד ריביע ובנוסף: תפקיד אוטונומי (הצד הרביעי + הצד השלישי) מערכת הODR מנהלת באופן עצמאי את הליך יישוב הסכסוך, מציעה פתרונות ואף מכירעה בסכסוך ללא צורך המעורבות של צד שלישי אנושי (מגשר, בורר, שופט). ניתן לעשות זאת ע"י הסתמכות על עצי החלטה (אשף יישוב סכסוכים), הליכים מונחי בינה מלאכותית וחישוביות.

מודלים טכנולוגיים בהליכי יישוב סכסוכים

מודלים חדשים – עיצוב מחדש – העברה לסביבה מקוונת שכוללת הרחבת נגישות: מיקום וזמן, ניטרול רגשות, סכסוכים בלעי מרכיב הירככי, למשל עובד-מעביד = כשיש יחסי כוחות / היררכיה.

**עיצוב מחדש - תפישה צרכנית: מתוכנן לשימוש "אדם מן הישוב"**

* פישוט פרצידורלי
* מתן סיוע/ מידע נחוץ לאורך ההליך
* אבחון אוטומטי של בעיות ופתרונות
* שפה יום יומית
* אימות מידע בשדות למניעת טעויות
* חוויות משתמש מותאמות
* הפקת מסמכים אוטומטית

היות והתהליך מותאם גם למשתמש החד פעמי וגם לשופט, היא יכולה להציע לכל אחד מהם חווית משתמש אחרת שתהיה נגישה יותר עבורו (עו"ד מעוניין בנגישות למידע רב, משתמש חבר ידע משפטי יקבל מיגע נגיש וכו'..)

מודלים חדשים – חישוביות, מערכות לומדות – שלומדות את הפעולות המבוצעות ומשנות על בסין את פתרוכנות הסכסוכים שיבוא אחריהם

רשתות חברתיות

בלוקציין - חוזים חכמים וכו'.

כמובן שהבחנות אלו הם לא מחייבות, קיימים גם תהליכים היברדיים (יכולות להתחיל כהליך פיזי ולעבור להליך מקוון ולהפך).

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)
* מידע על הסכסוך
* 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
* היסטוריית פתרונות
* 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 תפרים 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**

* Code is law - הטכנולוגיה אינה ניטרלית – לא ניתן להניח שהיא לא משפיעה על החלטות המשתמשים :
	+ היעדר שקיפות לגבי אופן פעולת המערכת (ניתוב הסכסוכים, הצעות פשרה)
	+ היעדר שקיפות ביחס לתוצאות
* חשש להטיה (היות ומדובר בגורם ביניים פרטי בעל שיקולים נוספים)– הכרעה בלתי שוויוניות על סמך שיקולים חיצוניים -איביי למשל יכולה לפצות משתמש מסוים מכספה ומשתמש אחר לא.
	+ חשש לפגיעה בשוויון ובצדק
* סיפוק המשתמשים מהתהליך אינו מבטיח שהמערכת הוגנת

רפורמת ההליכים האזרחיים באנגליה (ביהמ"ש המקוון של הלורד בריגס). זוהי דוגמא לשימוש בטכנולוגיה לצורך שיפור מערכת המשפט הציבורית. היו מספר בעיות שהיה צורך לטפל בהם: מייצגים עצמיים (פונים ללא עו"ד), עומס ניהול הליך, עומס ומשך חיי תיקים, נגישותבתי המשפט -אולמות, זמן(שעות הפעילות) וגם מבחינת המורכבות של סדרי הדין והדין המהותי שלא תואמת את העובדה שיש מייצגים עצמיים שלא יכולים להתמודד עם המורכבות הזו. צמצום משאבים: בתי משפט + סיוע משפטי.

הלורד עשה צעד אמיץ ואמר שיש להישען בצורה יותר מסיבית על טכנווגיה במע' המשפט. משרד המשפטים באנגליה מובילה רפורמה עם 50 פרוייקטי דיגיטיציה של מע' המשפט האנגלית, נתמקד באחד מהם:

הבעיה הגדולה של מערכות המשפט שמתמודדות עם מייצגים עצמיים. באנגליה ובארה"ביש תיקים רבים בהם מעורבים מייצגים עצמיים (30%-75%)

האתגר: מערכת המשפט תוכננה ע"י עורכי דין ועבורם מתוך הנחה של בקיאות של עורך דין. ולכן יש בעיה של נגישות לצדק. ולפעמים יש חסם כניסה (דחיה על הסף) +טעויות בדין מהותי ופרוצידוראלי.

בנוסף : מערכת המשפט מאופיינת בחמי גישה כלליים – זמן, משאבים.

Online solutions court

מעבר לניהול ההליך על פלטפורמה טכנולוגית. ובנוסף, ההליך מכוון כך שהצדדים יגיעו לפתרון בעצמם ולא הכרעה בידי שופט.

שלב 1 (מונחה תוכנה) : זהו השלב הקשה ביותר.

* אבחון הבעיה ובחינת קיומה של עילת תביעה, הצגת אפשרויות פעולה (לרבות ADR).
* סיוע בניסוח סדור של התביעה / כתב התביעה כך שתובן ע"י בעלי הדין ובית המשפט
* הוספת כלל המסמכים והראיות הרלוונטים לתיק

שלב 2 : ניהול הליך וניסיונות פשרה (מונחה תוכנה + מנהל תיק).

* פעולות ניהול תיק וקידומו לפשרה.
* באופן מקוון בכתב, ולפי הצורך: בשיחת ועידהף היוועדות חזותית או פנים אל פנים.

שלב 3: ניהול הליך והכרעה ע"י שופט – אם לא הצלחנו להגיע לפשרה

* הכרעה על סמך המסמכים (במערכת המקוונת)
* במידת הצורך: ניהול הליך או דיון בשיחת ועידה, היוועדות חזותית או באולם בית המשפט.
* המערכת הזו מיועד לתביעות אזרחיות לגבי תביעות קטנות.

האב הרוחני של המערכת הזו הוא למעשה הרחבה של מודל קודם – Civil resolution tribunal

היא מיועדת לשימוש בסכסוכים קטנים בין שכנים וכו'.

**סיכום: יתרונות הליכים שיפוטיים מקוונים**

* דגש על הליכים אסינכורניים
* התגברות על חסמים פיזיים – גישה 24/7 מכל מקום
* איכות ההשתתפות בהליך
* ניהול משאבי מקום וזמן שיפוטי, עלות תשתית נמוכה

תכנון מחודש של ההליך

* פישוט לגבי תביעות קטנות ופשוטות, מניעת טעויות
* ביצירת טפסים כאלו למעשה מבצעים ניהול של המידע => פתח לניתוב + ניהול תיקים אוטומטי, ייעול עבודת ביהמ"ש

סיוע משפטי בזמן אמת

חוויות משתמש שונות

סיכונים שכרוכים המערכת יישוב סכסוכי מקוונות

אבטחת מידע , אותנטיקציה

נגישות לחיבור אינטרנט ןנגישות טכנולוגית כלל(יכולת להתשמש בטופס כזה בתורה אםקטיבית)

ניטרליות / מניפוציה בתכנון הליכים. גם כאן כמו באייבי יש אתגר בטכנולוגיה ובייצור עצי ההחלטה ובאבחון הבעיה. וזה עלול ליצור בעיות של מניפולציה.

* Code is law סייג
* מניפולציה בתכנון ארכיטקטורות בחירה (ממשק המשתמש)

צדק פרוצדוראלי ואמו ןהציבור המערכת המשפט

פומביות הדיון וגם את כמות ההכרעות שמתקבלות ומייצרות תקדימים ומעצבות את מע' המשפט.

לכן נשאלת השאלה האם מדובר בצדק סוג ב'? שאלת ה-bench mark : למה אנחנו משווים את ההליך המקוון? ב"כ חושבים על הליך משפטי ראייתי מלא שבסופו הכרעה מנומקת ע"י שופט.

ODR בהליכים שיפוטיין בישראל :

נט המשפט היא תשתיתי טכנולוגית ותרבותית. יש תרבות של ישראל דיגיטלית, הטמעת טפסים מקוונים במשרד המפשטים באופן מקוון לחלויטן.

היתה רפורמה בתקנות סד"א התשע"ח +תפיסת ניהול ההליך.

העומס בבית המשפט וכן השאלה של דפוסי ניהול וסיום תיקים ושאלת הבנצ' מרק.

בעיית העומס - יש גידול 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
	+ הנחיות להגשת כתב תביעה
	+ טפסים כמו "שאלון לתבוע בתביעה לנזקי גוף"
* מיסוד של שימוש בכלים טכנולוגי בניהול ההליך
	+ 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)

המערכת של איביי והמערכת של לורד בריגס הן רק שתי דוגמאות מתוך שורה ארוכה של מערכות שמאפשרות להשלים את כל הליך הסכסוך החל מפתיחת ההליך (הגשת תביעה או תלונה) ועד להכרעה של צד שלישי או הסכמת הצדדים במו"מ על התוצאה. לעיתים מתאפשרת גם אכיפה מקוונת.

ה-ODR הוא מונח מסגרת רחב שמתייחס לסכסוכים שמקורם לאו דווקא בסביבה מקוונת. למשל, תביעות צרכניות; תביעות אזרחיות עד סכום מסוים; גיבוש הסכם גירושין; ערעורי מס; תיקי תנועה; סכסוכים קנייניים; הסכמי עבודה וכו'. גם השיטות ליישוב סכסוכים מגוונות, ונעות בין מו"מ, גישור, בוררות, הכרעה שיפוטית ואף מודלים חדשים של מושבעים. הטכנולוגיות שמפעילים לשם כך הן מגוונות, וכך גם תכנון התהליכים (הליכים פרוצדורליים מגוונים).

רקע להתפתחות תחום יישוב הסכסוכים באופן מקוון

* העידן הדיגיטלי: שירותים רבים כיום מסופקים באופן מקוון, באופן שיוצר נגישות ואף ציפייה לשירותים מקוונים (ממשל זמין – היכולת להשלים פעולות מול הממשל באינטרנט). האינטרנט כזירה חדשה של מערכות יחסים עסקיות, אישיות ואחרות, שבתורן יוצרות סוג חדש של סכסוכים. המעבר לעידן הדיגיטלי הוליד סכסוכים חדשים שהפתרון עבורם נוצר באותה סביבה-מערכת יחסים שבה הם נוצרו.
* תנועת הנגישות לצדק ותנועת ה-ADR (דרכים חלופיות ליישוב סכסוכים) - הגמישות התהליכית והנגישות והעלות המופחתת שמלווה את ההליך פגשה את עולם הסכסוכים המקוונים והתחברה עם כוח חברתי חזק (תנועת הנגישות לצדק וה-ADR). הרעיון היה לאפשר להשתמש בטכנולוגיה כדי להנגיש תהליכים ולהתאים אותם למה שמעניין וחשוב לצדדים לסכסוך, באופן שיאפשר להם דרך מהירה, זולה ונגישה לפתרון סכסוכים. תנועת ה-ADR, שהחלה בשנות ה-60, נכנסה למערכת המשפט בשנות ה-80 בתהליך הדרגתי. גם הגישור והבוררות חדרו למערכת המשפט והפכו לבני חסותה. באופן דומה, גם מערכות ה-ODR שהחלו כמענה לצרכים עסקיים מצאו את דרכן לתוך מערכת המשפט "הרגילה".

מאפיינים שמשפיעים/מתארים מערכות ODR (הטבלה בעמ' 648-647)

 חשיבות רבה להקשר של הסכסוך, לתהליך ולסוג הטכנולוגיה:

1. סכסוך: מסחר מקוון, משפחה, עבודה, עסקי? היכן הוא נולד?
2. הקשר: פרטי או ציבורי? מדינתי או בינ"ל? ספק שירות עצמאי, מתווך או מוסדי?
3. תהליך: שיטת יישוב הסכסוך, עושר הערוץ התקשורתי, סינכרוניות, אוטונומיות?

המוקד שלנו הוא בהשפעת הטכנולוגיה על ההליך.

מערכת ה-ODR כצד רביעי ושלישי בסכסוך

Ethan Katsh & Janet Rifkin כתבו בשנת 2000 מאמר שבו טבעו את המושג "הצד הרביעי" - הטכנולוגיה משמשת כצד נוסף ומרכזי שמשפיע על הסכסוך, לצד הבורר/שופט שמסייע לצדדים. זהו מקרה פרטי למונח שטבע לסיג, Code is Law. עיצוב הממשק והמערכת הטכנולוגית משפיעים על הליך יישוב והסכסוך, ההשפעה אינה ניטרלית בהכרח ולרוב אינה שקופה למשתמש.

1. **תפקיד אינסטרומנטלי:** מערכת ODR כצד רביעי בלבד - מופעלת ע"י אדם, למשל כאמצעי תקשורת או כלי לביצוע משימות קונקרטיות.
2. **תפקיד אוטונומי:** מערכת ה-ODR כצד רביעי ושלישי - המערכת המקוונת מפעילה בעצמה את הליך יישוב הסכסוך ללא צורך במעורבות של צד שלישי אנושי.

מודלים טכנולוגיים בהליכי יישוב סכסוכים:

1. העברה לסביבה מקוונת (העתקת התהליך כמו שהוא מתקיים בעולם הפיזי אל הסביבה המקוונת): המקום להגיע למשרד או לאולם ביהמ"ש נתקשר באמצעות וידאו, אודיו וסביבה מקוונת. היתרון הוא הרחבת הנגישות להליך, ומחקרים אף מצאו יתרונות כמו שליטה על רגשות בסכסוכים אמוציונליים (דוגמת גירושין), לצד אפשרות רבה יותר לליטיגציה גם בסיטואציה של פערי כוחות (לצד החלש קל יותר להשתתף בהליך כשהוא לא מול הגורם עצמו).
* הרחבת נגישות מיקום וזמן; רגשות; יחסי כוחות/היררכיה.
1. עיצוב מחדש - תפיסה צרכנית - מתוכנן לשימוש עבור אדם מן היישוב: עיצוב מחדש של אבני הבניין של יישוב הסכסוכים מתוך תפיסה צרכנית שלפיה מי שיבצע את ההליך הוא אדם מן היישוב ולא עורך דין. כך, כמו שכל אדם יכול להשלים רישום לאתר או להזמין כרטיסים לסרט באינטרנט, כך כל אדם יוכל לפתור את הסכסוך הצרכני (או אחר) באמצעות אתר שינחה אותו בשפה פשוטה ויומיומית, עם חווית משתמש מותאמת.
* פישוט פרוצדורלי: מתן סיוע ומידע נחוץ לאור ההליך; אבחון אוטומטי של בעיות ופתרונות; שפה יומיומית; אימות מידע בשדות למניעת טעויות; חוויית משתמש מותאמת; הפקת מסמכים אוטומטית.
1. חידוש: היכולת להציע לעולם יישוב הסכסוכים הליכים חדשים לחלוטין, כגון יכולות חישוביות מתקדמות; מערכות לומדות; שימוש ברשתות חברתיות ובמוניטין; שימוש במיקור חוץ; חבר מושבעים (חוסר המקצועיות של ההמון מהווה בעייתיות מסוימת). בנוסף, קיימים הליכים היברידיים המשלבים שיטות אלו עם השיטה הקלאסית של "פנים מול פנים".

**שיעור 3 (עובד מסיכומים של שיר ואור) - 19.3.18**

איביי פיתחה את מה שנחשב ע"י רבים למערכת ה-ODR הפרדיגמטית כי היא היוותה מקרה בוחן שהדגים את היווצרות הצרכים החדשים בגלל הפעילות ברשת, ובמקביל את הפתרונות שטכנולוגיית המידע יכולה לספק לבעיות אלו.

כאמור, באיביי היו ה-60 מיליון סכסוכים בשנה בשווי נמוך (100$), שהפכו פתרונות כמו מגשר או בורר אנושי ללא סבירים כלכלית. בנוסף, היה ריחוק פיזי בין הקונים למוכרים. עם זאת, היה צורך בהבטחת סביבה מסחרית בטוחה ואמינה כדי לעודד עסקאות.

* רייטינג או פידבק שניתן למוכרים מסייע בהרתעה והכוונת התנהגות – האם ניתן לסמוך על המוכר או לא? בתוך איביי יש מערכת ליישוב סכסוכים על פידבקים. אם מוכר רואה שניתן לו פידבק שלילי הוא יכול לבקש הליך יישוב סכסוך כדי להסיר את הפידבק השלילי, באופן שלא יפגע במוניטין שלו. אולם, מערכת הפידבקים כשלעצמה לא נתנה פתרון ממצה או סביבה בטוחה דיה ומכאן הגיע מערכת יישוב הסכסוכים.

מה מייחד את איביי כצד שלישי ליישוב סכסוך? שיקולים עסקיים ומסחריים. לאיביי יש אפשרות לראות את כל שלבי התהליך של היווצרות העסקה וכריתת הוזה, החלק מהתנאים שהוסכמו וכלה בסכסוך עצמו ופתרונות עבורו. בגלל שלאיביי יש מסד נתונים עצום של כל הליכי הסכסוך במשך השנים, היא יכולה ללמוד את דפוסי הסכסוכים ולבנות תהליכים במונעים מלכתחילה היווצרות סכסוכים, ובכך לפתור אוטומטית חלק גדולה מאוד מהסכסוכים.

מערכת יישוב הסכסוכים של איביי:

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

\*90% מהסכסוכים נפתרים ללא מעורבות גורם אנושי מטעם החברה.

מערכת לומדת, מבוססת נתונים:

* ניתוח הנתונים לצורך זיהוי דפוסי מחלוקת, המידע הנחוץ לפתרונם ופתרונות עם סבירות גבוהה לקבלתם.
* פרסונליזציה סטטיסטית: גם על סמך מידע שלא נמסר ע"י הצדדים לסכסוך הספציפי, מידע שהמערכת הלומדת פיתחה מאינספור סכסוכים קודמים עם מאפיינים דומים).
* בירור עובדתי ישיר מתוך נתוני המערכת (העסקה מבוצעת על הפלטפורמה)

למערכות אלו יש חסרונות, והן מעלות חששות מצד מי שאמון על האינטרס הציבורי. למשל, פגיעה בפרטיות ע"י חשיפת פרטים אישיים, הפרטת האכיפה, חוסר אובייקטיביות של הגוף הפרטי (אינטרסים כלכליים והעדפה של צד מסוים בסכסוך), צדק אינו בהכרח פוזיטיבי (כלומר אין מענה למקרים חריגים).

חששות וסיכונים:

* המודל של לסיג (CODE IS LAW) מתייחס להשפעות של המערכת על ההתנהגות האנושית. טכנולוגיה אינה ניטרלית: היעדר שקיפות לגבי אופן פעולת המערכת (ניתוב סכסוכים, הצעות פשרה), היעדר שקיפות ביחס לתוצאות וכו'.
* חשש להטיות: הכרעה בלתי שוויונית על סמך שיקולים חיצוניים לסכסוך, חשש לפגיעה בשוויון ובצדק - האם מובאים בחשבון נתונים דוגמת "השווי" העסקי של המשתמש עבור איביי או הרקורד שלו במערכת?
* סיפוק המשתמשים מהתהליך אינו מבטיח שהמערכת הוגנת/צודקת, יש סבירות רצון שאפשר להגיע אליה באופן מניפולטיבי.

כיצד ניתן להסדיר מערכות ליישוב סכסוכים כמו איביי? מערכות פרטיות שפועלות בצורה ראויה?

* **אקרדיטציה:** גוף מרכזי יעניק תו תקן פדרלי, בדומה לתווי תקן בתחום התשלום/אבטחה. לא יכולים לאמוד את אופן הפעילות, המודל הוא של תו תקן מקובל.
* **רגולציה עצמית:** סטנדרטים אתיים שיפותחו ע"י התעשייה עצמה.
* **סטנדרטים מומלצים:** למשל, ה-ABA התווה עקרונות לנותני שירותי ODR.
* מודל מסלקה: גורם מרכזי ינתב סכסוכים למערכות ODR שאושרו (לנותן השירותים הספציפי).
* **הסדרה ציבורית באמנות/הסכמים/חקיקה:** הדירקטיבה האירופית בנושא ADR והתקנה בנושא ODR. בין מדינות האיחוד השונות יצרו הוראה שמחייבת יצירת פורטלי גישור מקוונים להליך יישוב הסכסוך (רק לצורך הגשת התלונה, לא לכלל ההליך); כללי מודל ל-ODR של UNCITRAL של האו"ם - תקינה למסחר בינ"ל מייצג נוסח כללי שניתן להתחייב אליו חוזית, מעין סטנדרט שיהיה ניתן לאמץ לתוך ההליך.

רפורמת ההליכים האזרחיים באנגליה - ביהמ"ש המקוון של הלורד בריגס

דוגמה לשימוש בטכנולוגיה כדי לשפר את מנגנוני יישוב הסכסוכים הקיימים במערכת המשפט הציבורית. מערכת המשפט האזרחית באנגליה מתמודדת עם בעיה חריפה של נגישות עקב העלות הגבוהה של ייצוג משפטי באנגליה והקושי של מייצגים עצמיים (תובעים או נתבעים) לנהל הליכים ללא עו"ד. הלורד בריגס פרסם דו"ח בשנת 2016 שהמליץ להקים בימ"ש מקוון לכל ההליכים האזרחיים עד גבול סמכות של 25 אלף פאונד, כאשר הרעיון היה לאמץ את התפיסה הצרכנית של איביי לתוך ההליכים האזרחיים.

**המערכת המשפטית לא תוכננה עבור מייצגים עצמיים:**

בסוגים שונים של הליכים משפטיים, בעיקר בארה"ב ובאנגליה, יש אחוזים גדולים מאוד של מייצגים עצמיים. זה נובע מסיבות רבות ומגוונות, כגון תרבות "עשה זאת בעצמך", עלויות הייצוג, מיעוט משאבים לסיוע משפטי, חוסר אמון בעו"ד, צרכנות, אינדיבידואליזם וטלוויזיה.

אחד מהשיקולים של היעילות הנגישות הטכניים הם שאדם מן השורה לא יודע לנסח את טיעוניו בביהמ"ש באופן המצופה ממנו. מערכת המשפט, סדרי הדין והדין המהותי עוצבו ונוסחו באופן שנועד להפעלה ע"י אנשי מקצוע, עורכי דין.

האתגרים הכרוכים בייצוג עצמי:

|  |  |
| --- | --- |
| גופים שיפוטיים | בעלי הדין המייצגים עצמם |
| **תפעול:**- עלויות מניעה וטיפול וטעויות בניהול ההליך- עיכוב בטיפול בתיקים, סיבוך פרוצדורלי מיותר | **ידע:**- טעויות בדין המהותי והפרוצדורלי- יותר מ-50% מהמקרים נמחקים על הסף- שיעור הצלחה נמוכך יותר מלמיוצגים משפטית |
| **אתיקה:**- מתירים מתן מידע, אך לא מתן סיוע משפטי- מתח בין ניטרליות לנגישות לצדק | **השתתפות:**- טענות משפטיות לעומת דיבור יומיומי (רגשי)- הדינמיקה של השיח באולם ביהמ"ש - השתקה- תחושות בלבול, הצפה, תסכול, חששות |

* חסמי גישה כלליים: זמן, מקום ומשאבים.

הדרך שבריגס הציע להתמודד עם הבעיות הללו היא מודל ביהמ"ש המקוון:

שלב 1 (אוטונומי)

* סיוע בניסוח התיק באופן סדור כך שיובן ע"י בעלי הדין שכנגד ובית המשפט
* הוספת כלל המסמכים והראיות הרלוונטיים בתיק

שלב 2: ניהול תיק וניסיונות פישור (אינסטרומנטלי)

* תפקידן בביהמ"ש יתחיל באופן מקוון בתהליך, ובמידת הצורך אף פנים מול פנים

שלב 3: הכרעה ע"י שופט (אינסטרומנטלי)

* באופן מקוון: על סמך המסמכים בלבד או לאחר דיון אודיו/וידאו בטלפון
* במידת הצורך ההכרעה תתקבל לאחר דיון פנים מול פנים באולם ביהמ"ש

**המודל של בריגס מתבסס על מודל הטריבונל האזרחי שעובד בקולומביה הבריטית שבקנדה:**

* המערכת של בריגס חסרת תקדים בהיקפה - תביעות אזרחיות עד 25 אלף פאונד, בעוד שהמערכת בקנדה מוגבלת לתביעות קטנות, עבירות תנועה וסכסוכים קנייניים מסוימים.
* למערכת בקנדה יש שלב נוסף של אבחון סכסוך ופתרונות מחוץ לביהמ"ש (לפני הגשת תביעה, ייתכן שקיים פתרון אחר - במיוחד כאשר מדובר בצדדים בלתי מיוצגים). ניתן לפנות לגורם ממשלתי או להציג מכתב דרישה לנתבע.
* בקנדה יש אבחון אוטומטי לפי שאלות החלטה, ביחס לפעולות משפטיות או אחרות שהפונה יכול לנקוט בהן כדי לפתור את הבעיה שבגללה הגיע לביהמ"ש.

יתרונות המודלים המקוונים להליכים שיפוטיים:

1. **הליכים א-סינכורניים:**
* עבור בעלי הדין: הסרת חסמים פיזיים (גישה 24/7 מכל מקום, איכות השתתפות בהליך)
* עבור המערכת המשפטית: ניהול משאבי מקום וזמן שיפוטי, עלות תשתית נמוכה
1. **יתרונות בניית התהליך המחודש:**
* פישוט והדרכה, מניעת טעויות, ניהול המידע
* ניהול תיקים יעיל
1. **מתן סיוע משפטי בזמן אמת**
2. **חוויות משתמש שונות:** האופן שבו המידע נאסף מהתובע/נתבע או האופן שבו מוצג לו המידע יהיה שונה מהאופן שבו השופט רואה.

חששות מתקשורת מקוונת ומאוטומציה:

* תיאורית עושר המידע של Daft & Langel מ-1984, שלפיה להעברת מסר מורכב דרוש אמצעי תקשורת "עשיר", בעוד שלצורך העברת מסר פשוט די באמצעי "דל".
* האם ניתן להפיק צדק באופן ממוכן?
* האם השימוש באוטומציה שונה בהליכים מחייבים לעומת מייעצים?
* שמירה על לגיטימיות מוסדית, צדק פרוצדורלי, צדק מהותי
* CODE IS LAW: יש להבטיח שממשק המשתמש ותכנון התהליך אינם יוצרים הטיות בבחירות המשפטיות של המתדיינים – גם כשאנחנו נותנים לצדדים בחירה ומדובר בהליך הסכמי ופונקציה תומכת החלטה (ולא מחליטה), ממשק המשתמש ואופן עיבוד המידע יוצרים ארכיטקטורות בחירה ומשנים את האופן שבו אני בוחר.

**מתווכים ברשת האינטרנט**

מאמר של ניבה אלקין קורן: "כיכר העיר החדשה". בראשית ימיה של רשת האינטרנט הודגש אופייה המבוזר כמקדם של חירות אישית, חופש מידע וחופש ביטוי, מעין מרחב ציבורי וירטואלי שבו כל אדם יכול לקחת חלק פעיל בשיח הציבורי. התפישה של האינטרנט כמקדם חופש מידע וביטוי נשענה על ההנחה **שאופיו המבוזר של האינטרנט הוא אנטיתזה לריכוז השליטה בידי אמצעי תקשורת מעטים.**

* **חסמי הכניסה לאינטרנט נמוכים:** אין צורך בהקצאת ערוצי שידור, ובהתאם גם לא צריך רישוי ופיקוח הנלווים לכך; ישנה עלות מינימלית להפצת תוכן ברשת; ביטול התלות המסננת העריכה של אמצעי התקשורת המסורתיים, יותר משתתפים בשיח.
* בניגוד לעיתונות, הטלוויזיה והרדיו, המגדירים עבור הקורא את סדר היום, לגולש באינטרנט יש **אוטונומיה להגדיר את סדר היום בעצמו.**
* המדיום מאפשר תקשורת ישירה ובלתי אמצעית בין משתמשים.
* התפתחות מאגר עשיר ודינמי של תוכן חופשי ממקורות מגוונים.
* יותר פלורליזם ומגוון בתוכן המיוצר והמופץ.
* החלשת כוחם של מוקדי השליטה בשוק התקשורת והתוכן.

**נייטרליות רשת:** אחד העקרונות הראשוניים של רשת האינטרנט היה שלא יהיו חסמים על אופן זרימת המידע, ושכוחו השוק לא יכתיבו איזה מידע נראה קודם או בכלל. בפועל, כמות המידע באינטרנט ואפשרויות הפעולה הן כל כך גדולות עד שאין נגישות אמיתית לכולו. התוצאות שמופיעות במנוע החיפוש בדף הראשון מכתיבות את האופן שבו ניגש למידע שקיים ברשת. המתווך הוא מנוע החיפוש שבו אנו תלויים כדי לדלות את המידע, ההחלטות שהמתווך מקבל משפיעות על תמונת העולם שאנחנו כמחפשים מקבלים - שיטת קידום האתרים של מנועי החיפוש.

העובדה שמתווכים שונים כמו זירות המסחר, מנועי החיפוש ומפיצי התוכן הם תאגידים פרטיים שפועלים שאופן שלא שקוף למשתמש מעצבת בפועל את סביבת הפעילות עבור משתמשים ברשת. חשוב להבין וגם לפקח בצורה נכונה על האופן שבו המתווכים ברשת מבנים את הפעילות בה.

הגדרת מתווכים ברשת האינטרנט: גופים (לרוב למטרות רווח) אשר מאפשרים ביצוע התקשרויות או עסקאות בין צדדים שלישיים באינטרנט, על דרך של אספקת שירותים אינטרנטיים לצדדים שלישיים או מתן גישה, אחסון, שידור או אינדוקס של תוכן, מוצרים ושירותים מקוונים שמקורם בצדדים שלישיים.

דוגמאות:

* ספקיות הגישה ושירות לרשת האינטרנט (בזק, נטוויז'ן, הוט)
* שירותי אחסון אתרים ועיבוד מידע, לרבות מרשמים של שמות מתחם.
* מנועי חיפוש ופורטלים
* אתרי תיווך מסחר ושירותים מקוונים (הפלטפורמה אינה מוכרת את השירות או המוצר בעצמה)
* מערכות תשלום מקוונות
* פלטפורמות להפצת תוכן אשר לא יוצרות את התכנים המופצים בעצמן
* מדיה חברתית

**סוגים של גורמי ביניים:**

**במאמרה של אורלי לובל** היא מדברת על שלושה דורות:

1. הדור הראשון - **מתווכים שמאפשרים שיתוף וקישור למידע וידע,** כגון מנועי חיפוש כמו גוגל ויאהו.
2. הדור השני - **זירות מסחר ושירותים** כמו איביי ואמזון, שירותי החלפת קבצים כמו נאפסטר. חברות אלו הובילו לשינויים משמעותיים בתעשיית ההוצאה לאור, ערוצי חדשות ומדיה, מוזיקה וקמעונאות.
3. הדור השלישי - חברות פלטפורמה שנותנות **גישה לשירותים במרחב הלא מקוון במחיר נמוך משמעותית, תוך התאמה אישית גדולה יותר** (למשל גט טקסי)

הטכנולוגיה משנה את האופן שבו ניתנים שירותים ונערכות עסקאות בעולם הפיזי. למשל, AIR BNB לתעשיית המלונאות, UBBER לתעשיית המוניות, EAT WITH למכירת ארוחות בבית כמו מסעדות.

שאלות משפטיות מרכזיות ביחס לגורמי הביניים - המתווכים:

* באיזו מידה מתווכים אחראים לפעילות של המשתמשים?
* האם לצד אחריותו של המזיק הישיר יש להטיל אחריות גם על המתווך - גורם הביניים (ספק הגישה לאינטרנט, בעל הפורום, נותן שירות התיווך באשר הוא)? האם, כאשר אדם נושא באחריות על הוצאת לשון הרע, גם הפלטפורמה שאפשרה את הפרסום הזה נושאת באחריות?
* האם ראוי ובאיזו מידה ראוי להפקיד בידי מתווכים סמכויות משטור, רגולציה ואכיפה משפטית?
	+ נוהל הודעה והסרה להגנה של זכויות יוצרים
	+ צווי הגבלת גישה / חסימת תכנים (זכויות יוצרים, תכנים פוגעניים, פורנוגרפיה, טרור ופלילים).

איזה תפקיד ממלאת מערכת הממשל העצמי של גורמי הביניים בעיצוב נורמות והתנהגות?

* תנאי השימוש ומדיניות הפרטיות ממלאים תפקיד רגולטורי משמעותי
* חוזים אחידים שמסדירים את מערכת היחסים בין הפלטפורמה למשתמשיה
* הגדרת חובות וזכויות, המותר והאסור לשני הצדדים לחוזה
* לעיתים – כלי הסדרת התנהגות בלעדי (בהיעדר יכולת אכיפה של חוקי המדינה)
* כללי התנהלות בתוך הפלטפורמה
* השלכות חיצוניות לפלטפורמה:
* שימוש במידע שנצבר בפלטפורמה לרבות מידע של משתמשים + העברה לצד ג'

השפעות חברתיות-פוליטיות-נורמטיביות – עיצוב תפישות המשתמשים(ציפיות לגבי התנהגויות ראויות חוקיות?)

* האם ובאיזו מידה מתווכים צריכים להיות כפופים לרגולציה דומה לזו של נותני שירותים בעולם הפיזי? (אורלי לובל)

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

מדוע גורמי הביניים ברשמת מהווים כתובת אטרקטיבית לתביעות משפטיות?

ניתני לזיהוי ואיתור בקלות

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.

* לרוב מדובר בבעלי "כיס עמוק"

סיכוי הנפגע להיפרע מהנזק גבוה יותר

פעמים רבות הם מונע הנזק היעיל ביותר

מצויים בעמדה שמאפשרת למנוע באופן אקטיבי את הישנות המקרה:

למשל ע"י חסימת גולשין או הטמעת אמצעי סינון ועריכה שיגבילו הפצת תכנים

התמריץ: צמצופ חשיפתם המשפטית

דוגמה: תביעות אסטרטגיות של בעלי זויות יוצרים בשל אחריות תורמת (פרשתנפסטר)

קשיים בהטלת אחריות משפטית על גורמי ביניים

עמימות ביחס לכללים המשפטים שחלים על גורם הביניים (הפעילות ברשת)

במדינה שבה רשום גורם הביניים?

במידה שבה גורם ביניים נותן שירות?

במידנה שבה מצויים שרתיו?

במדינה שזה מצויים המשתמשים בשירות?

השלכות שליליות של הטלת אחריות משפטית שעל גורמי הביניים

חשיפה המשפטית עלולה לייקר משמעותית את עלות הפעלתם של שירותים ברשת - הקמת מנגוני סינון, ייעוץ משפטיף התיידינות משפטית

צמצום מספר השירותים

התייקרות גישה למידע ולאמצעי ביטוי

ריכוזיות,

חשש מיצירות מוקדי כוח ברשת שיכשילו את הביזור וחובליו ל"אפקט מצנן".

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.

כלל שכללי האחירות במערת המשפטית הרלוונטית חמורים יותרף כך גובר הסיכוי שתוכן יוסר ע"י המתווך באופן יזו ם או על רקע בקשה להסרתו.

**שיעור 4 (עו"ד עמית אשכנזי) - 9.4.18**

הגדרות

**"סייבר-אינטרנט": הפעילות הממד התוכן - "דיני מידע".**

"חוק המחשבים" הסדיר את תופעת המחשבים. המחוקק ראה לנכון להסדיר את המעשים הללו, על אף שחלקם אסורים גם ללא "סביבת המחשב". זוהי **הסדרה ייעודית לסביבת המחשב.**

"חוק הסרטונים" הפך את הפצת הסרטונים המיניים ברשתות חברתיות לפלילית. חקיקתו סימלה את האינטרס הציבורי בנוגע לעניין.

נושא מאוד מרכזי בסייבר-אינטרנט הוא אחריות המתווכים. היכולת של כל אחד לבצע עבירות באנונימיות הפכה את אחריות המתווכים למשמעותית יותר לצורך טיפול בתופעה.

אחריות המתווכים: בעייתיות האכיפה של הפצת מידע ועבירות אנונימיות הובילה לתפיסה שיותר יעיל לאכוף באמצעות מתווכים (כגון יוטיוב, גוגל ופייסבוק). עם זאת, בשלב מוקדם יחסית קיבלו המתווכים חסינות כזו או אחרת כדי לאפשר את הפצת המידע והמשך חופש הביטוי. הנרטיב המשפטי שליווה את התקופה הזו היה **נרטיב אופטימי וליברטריאני שאמר שתפקיד המשפט באסדרת האינטרנט הוא פסיבי,** והמדינה לא צריכה להתערב באזור הזה (אסדרה פרטית בלבד). מה שקובע את זכויות וחובות הצדדים הם תנאי השימוש של הצדדים. לא רצו שהמשפט יתערב בחקיקה מיוחדת לאינטרנט וייצור נטלים מיותרים.

אולם, תפיסה "טובה" זו של האינטרנט התפוגגה בעקבות חשיפותיו של **סנודאן,** שגילה לעולם כיצד הממשלה האמריקנית (באמצעות סוכנות הביון NSA) אוספת מידע על אזרחים. זה הוביל למשבר אמון לגבי היותו של האינטרנט מקום פתוח וחופשי שהממשלה לא נמצאת בו. בנוסף, **איומי הסייבר** הפכו את האינטרנט למקום פחות בטוח (והעלו את השאלה העקרונית, האם ניתן לצפות מהמדינה להגן עלינו במרחב הסייבר כפי שהיא מחויבת להגן עלינו בממד הפיזי?).

**למה מדינות כל כך מתעניינות במה שקורה באינטרנט?** כשאנחנו גולשים באינטרנט אנחנו בעצם מחברים את המחשב שלנו לעולם. התקשורת הזו היא דו צדדית - דברים מבחוץ נכנסים פנימה ודברים מבפנים יוצאים החוצה. ההעדפות שלנו והפעילויות שלנו מנוטרות כל הזמן. למשל, באמצעות המידע שנצבר בטלפון של אדם ניתן להרשיע ולהפליל אותו בעבירות שביצע.

המדינה הבינה שאת מה שהייתה צריכה לעשות בעבר עם סוכני קומנדו בשטח ומכשור מיוחד, היום ניתן לבצע בדרכים זולות ומתוחכמות. קיימות לא מעט דילמות בין אינטרסים של אכיפת החוק והביטחון מול פגיעה בפרטיות ובחופש הביטוי של האזרחים.

* נקודת המעבר מתנאי שימוש "פרטיים" לאסדרה רשמית נעשתה **בפס"ד גונזלס,** שבו ביה"ד האירופי לזכויות אדם התערב בתנאי השימוש של גוגל.

**"סייבר" -** **שימוש של גורמי המדינה השונים במרחב זה לאיסוף מידע ולפעילות ביטחונית או אכיפת חוק.**

**הגנת הסייבר -** **פעילות לצורך שמירה על תפקודן התקין של מערכות מחשב, המידע בהן והתקשורת ביניהן בארגונים, במגזרי המשק ובמדינה** (ללא עיסוק בתוכן).

ישראל היא מעצמת סייבר. עיקר הדגש בהגנת סייבר הינו "במעטפת" ולא בתוכן המהותי.

מערך הסייבר הלאומי - משימות

1. קידום ההיערכות הלאומית להגנת הסייבר

2. קידום עוצמה ביטחונית-אזרחית

3. הובלה ישראלית במרחב הסייבר

4. פיתוח תעשייה, אקדמיה והון אנושי

5. קידום היציבה הבינ"ל של ישראל

**תקיפת סייבר הינה אירוע שבו מישהו מנצל חולשה** **במערכת** (באג, תקלת תכנות וכו') **כדי לגרום למחשב לתפקד לא כמתוכנן.** ישנן תקיפות שמטרתן גניבת מידע, תקיפות שמטרתן לגרום נזק ותקיפות שמטרתן שיבוש הפעילות או השתלטות חיצונית. בעולם המעשי, המשמעות של זה היא שבכל מקום שבו יש מחשב אנחנו חשופים לתקיפה שיכולה לגרום לנו נזק. למשל, אם מישהו יתקוף את מחשבי חברת החשמל, יהיו לכך השלכות מזיקות בעולם הפיזי (טורבינות יפסיקו לעבוד, מידע תפעולי יושמד וכו').

למרות שחברת החשמל מוגנת "פיזית", האתגר משמעותי יותר **בעולם הדיגיטלי שבו הגבול הוא גלובלי -** לא רק המדינות הקרובות יכולות לתקוף אותנו אלא כל העולם, ומי שיכול לתקוף הוא לא רק בעל חיל האוויר החזק ביותר אלא כל האקר שרוצה להוכיח את עצמו.

בשת 2002 המדינה קיבלה החלטה היסטורית בשם ב-84, שמכריזה על תשתיות מסוימות **כתשתיות קריטיות** שהפגיעה בהן תגרום לנזק חמור לביטחון הלאומי. על השב"כ הוטל לאתר ולהגן על התשתיות הללו. המסגרת המשפטית שנקבעה לכך מעוגנת בחוק להסדרת הביטחון בגופים ציבוריים, בחלק העוסק בביטחון פיזי (שהותאם לסייבר).

הגופים שזכאים להגנה הזו כתשתיות קריטיות הם חברת החשמל, מקורות, בנק הדם, רשות האוכלוסין, גופי התקשורת וכו'. גם במדינות אחרות בעולם מגנים על גופים כאלו, אבל בישראל ההגנה החלה מוקדם מאוד (כבר ב-2002) וגם פועלת פר גוף ולא פר ענף (בעוד שבמדינות אחרות הולכים לפי ענף הבריאות, הפיננסים וכו'). ככה **כל תשתית מקבלת חליפת הגנה מיוחדת התפורה למידותיה.** במקביל לטיפול בתשתיות קריטיות, רגולטורים מגזריים (כמו המפקח על הבנקים) החלו להבין שגם עליהם להתגונן בהתאם. **התפיסה היא סקטוריאלית:** תשתיות קריטיות מטופלות ע"י שב"כ וכל רגולטור דואג למגזר שלו.

תפיסת הבוטיק הזו, שפעלה מאז 2002, הועמדה בסימן שאלה - מרחב הסייבר גדול יותר מאותן תשתיות מצומצמות שנכללו בהגנה. האם די בתפיסת הבוטיק כדי להגן על כל המשק?

אירוע שמדגים למה לא די בתפיסת הבוטיק הוא WannaCry, שהייתה שילוב בין תולעת וירטואלית שמשכפלת את עצמה ומתפשטת עם נוזקת כופר שניצלה חולשה של ווינדוס. היא גרמה לכך שכל המחשבים הלא מעודכנים במערכת הבריאות באנגליה ננעלו, ואח"כ זה התפשט הלאה. זה מראה שהתפיסה שלפיה "ניתן להגן רק על מבצר אחד" לא תופסת, כי הכל מחובר זה לזה ווירוסים יכולים להתפשט. לא די להגן על 30% מהתשתיות בלבד. וכאן אנו חוזרים לשאלה מהו תפקיד הממשלה במרחב בסייבר. מדינת ישראל היא בין הראשונות שהצליחה להציע תפיסה בנושא וגם לממש אותה במידה רבה.

 מעצבי המדיניות בישראל ניתחו מהן הבעיות בגיבוש תפיסת הגנה לאומית בסייבר:

1**. "זירת ההגנה" היא במערכות** **הארגון -** בסופו של דבר התקיפה בסייבר מתרחשת בתוך הרשת הארגונית. ביטחוניסטים רגילים לפעול בגבול העוין, כאשר "הקרב" בסייבר מתרחש בארגון, "בבית שלנו". אין למדינה יתרון יחסי על האויב כשהיא מנסה להבין רשת ארגונית.

**2. זירת ההגנה מבוססת טכנולוגיות אזרחיות -** טכנולוגיות אזרחיות רוצות להוציא מוצרים חדשים כמה שיותר מהר, בלי לבדוק לעומק את כל הבאגים האפשריים.

3. משרעת רחבה של איומים, תוקפים ופוטנציאל נזק.

**4. קישוריות והשפעות רוחב -** הכל מחובר כיום, וחלק מהתוכנות (כמו התולעים) מתוכנתות להתפשט ולפגוע בכמה שיותר מחשבים.

**5. זמני תגובה קצרים -** הכל קורה מיד.

**6.** **מרחב גלובלי שאינו מצוי בריבונות "אחת" -** היכולת שלנו לשלוט, להשפיע ולהפעיל כוח במרחב הסייבר מוגבלת, כי אנחנו חלק ממרחב אקס-טריטוריאלי.

7**. איזון בין תפקיד המדינה להגן לבין היותו של מרחב הסייבר כר לחדשנות ויזמות ובעל השפעה משמעותית על זכויות יסוד** (פרטיות וחופש ביטוי). הדילמה היא גם מצד האתגר הביטחוני התפעולי וגם מבחינת החשש לתופעות לוואי.

בשנת 2015 הממשלה קיבלה שתי החלטות -

2443: הסדרה והובלה ממשלתית

1. מערך הסייבר כגורם לאומי מנחה: **מרגולציה מגזרית,** שבה כל אחד עושה לעצמו הגנת סייבר כפי שהוא מבין אותה, **עוברים לתפיסה מרכזית שבה יש שפה אחת לגבי הגנת סייבר, כך שלארגונים יהיה תקן/סטנדרט אחיד.** שיטת הבוטיק נשארה עבור גופים קריטיים, אבל יש פתרון לכל היתר.
2. **רגולציה אחידה באמצעות רשויות האסדרה:** לא עובדים ישירות מול מערך הסייבר הלאומי אלא באמצעות רשות הרגולציה המגזרית, שמקבלת את הסטנדרט הרצוי אבל מבצעת לו התאמה בהתאם לסקטור שלה. כל אחד מהסקטורים הללו אמון על אינטרס ציבורי, והרגולטור הרלוונטי צריך לנתח את סיכון הסייבר באותו הקשר (יעיל יותר מגוף מפלצתי שצריך לטפל בגופים שונים משונים).
3. **מנגנון "ניהול תקין" של הממשלה ומשרדיה** להגנת הסייבר: ההבנה שגם הממשלה לא חסינה מפני תקיפות סייבר, ועליה להקדיש אחוזים מתקציבה להגנה בסייבר.

עם זאת, לא כל גוף יכול להגן על עצמו. כאן נכנס תפקידו של מערך הסייבר הלאומי.

2444: מערך הסייבר הלאומי - גוף ייעודי להגנת הסייבר

1. שיתוף מידע וטיפול באירועים בזמן אמת
2. הגנה בשילוב כלל הגורמים הממשלתיים
3. הגנה על זכויות יסוד

החלטה זו עוסקת בתפקיד המדינה כאשר ישנו אירוע של תקיפת סייבר. לא תמיד ברור מי התוקף ולכן **צריך להתמודד עם התקיפה ללא קשר לטיפול בתוקף** (לטפל בשריפה עוד לפני שמתחקים אחרי המצית). תפקיד זה לא ישב אצל אף גוף לאומי עד החלטה 2444.

* **גופי CERT** (CYBER EVENT RESPONSE TEAM) **כל הזמן מחפשים מידע כל סיכונים ומתריעים איך להתגונן מפניהם.** זהו תפקיד חדש של המדינה שלא היה קודם.

לדוגמה, באירועי WannaCry נחשפה ב-14 באפריל חולשה במערכת של מייקרוסופט. חודש לפני ההדלפה של החולשה מייקרוסופט הוציאו עדכון גרסה דחוף במענה לחולשה, אבל לא כל המשתמשים היו על מצב עדכון אוטומטי – כך שחלקם נותרו פגיעים. ב-16 באפריל הוציא ה-CERT הלאומי בישראל הודעה לציבור לגבי קיומה של הפרצה והמליץ מה לעשות (להוריד עדכון מהאתר של מייקרוסופט). בינתיים הפוגען כבר החל להתפשט במערכת הבריאות הבריטית, שלא עדכנה את המחשבים שלה, וב-12 במאי כולם כבר שמעו על התולעת הזדונית WannaCry, שנעלה את מערכת הבריאות באנגליה. בעוד שבישראל ה-CERT הפיץ התראות בזמן אמת, מדינות אחרות "לא היה עם מי לדבר". לא היו פונקציונרים ייעודיים לאירועי חירום בסייבר.

כדי לבצע את משימת הגנת הסייבר בצורה טובה, יש חשיבות לאיסוף מידע על מה שקורה במרחב הסייבר הישראלי כל הזמן ולדווח לכולם. **שיתופיות המידע** משמעותית מאוד. בנוסף, כשמטפלים באירועים מחשוביים עולות שאלות לגבי נגישות המדינה למידע. איך מסדירים את המתח בין הכניסה המחודשת של המדינה למרחב הסייבר לבין ההגנה על זכויות היסוד?

ישנו מסמך בשם "עקרונות הפרטיות של ה-CERT הלאומי", כיצד מיישמים את עקרונות הפרטיות בתהליכי העבודה של המרכז. בכך מנסים להציג מדיניות פרטיות קצרה, ברורה ושקופה לגבי מה המדינה עושה ומה לא בתחום הגנת הסייבר. גם כאן ישנו ניסיון לשמור על ההבחנה בין תוכן לא רלוונטי ותוכן רלוונטי להגנה בסייבר ("מידע בעל ערך אבטחתי").

**שיעור 5 - 16.4.18**

שאלות משפטיות מרכזיות ביחס לגורמי ביניים ברשת (מתווכים)

גורמי ביניים מהווים כתובת אטרקטיבית לתביעות משפטיות ולהפקדה של סמכויות האכיפה. אולם, **באיזו מידה גורמי ביניים באמת אחראיים לפעילות של המשתמשים?** האם לצד אחריותו של המזיק הישיר יש להטיל אחריות גם על המתווך (ספק הגישה לאינטרנט, בעל הפורום, נותן שירות התיווך באשר הוא)? **ובאיזו מידה ראוי להפקיד בידי מתווכים סמכויות משטור, רגולציה ואכיפה?** (נוהל הודעה והסרה להגנה על זכויות יוצרים, אחריות תורמת לפגיעה וכו') **באיזו מידה מתווכים צריכים להיות כפופים לרגולציה דומה לזו של נותני שירותים בעולם הפיזי?** (Orly Lobel, The Law of the Platform)

מה הופך את גורמי הביניים לכתובת אטרקטיבית לתביעות משפטיות?

1. **ניתנים לזיהוי ואיתור בקלות** - בעוד שתהליך זיהויו של המשתמש היחיד עלול להיות יקר וממושך (במיוחד לנוכח שכיחותה של פעילות אנונימית); זול יותר לתבוע את המתווך.
2. **לרוב בעלי "כיס עמוק"** - סיכוי הנפגע להיפרע מהנזק גבוה יותר.
* **פעמים רבות המתווכים הם מונע הנזק הזול היעיל ביותר** - מצויים בעמדה המאפשרת למנוע באופן אקטיבי את הישנות המקרה, למשל ע"י חסימת גולשים והטמעת אמצעי סינון ועריכה שיגבילו הפצת תכנים. ככל שנגדיל את החשיפה המשפטית שלהם יותר הם יתומרצו לפעול כך, כדי למנוע את הסיכון מראש. לדוגמה, תביעות אסטרטגיות של בעלי זכויות יוצר בשל אחריות תורמת (פרשת נפסטר).

קשיים וסכנות בהטלת אחריות משפטית על גורמי ביניים

**1. עמימות ביחס לכללים המשפטיים שחלים על המתווך (הפעילות ברשת):**

1. הכללים במדינה שבה רשום המתווך?
2. הכללים במדינה שבה פועל המתווך?
3. הכללים במדינה שבה מצויים המשתמשים?

> למשל, פייסבוק בישראל.

2. החשיפה המשפטית עלולה לייקר משמעותית את עלות הפעלתם של שירותים ברשת (הקמת מנגנוני סינון, ייעוץ משפטי, התדיינות משפטית), באופן שיביא לצמצום במספר השירותים והתייקרות בגישה למידע, לאמצעי ביטוי ולזירות מסחר ויביא לריכוזיות (עלה בפס"ד רוטר).

ישנה הנחה בסיסית שלפיה קיים שוני איכותי בין גורמי הביניים ברשת, במיוחד בכל הקשור להפצת מידע וחופש ביטוי, לבין אמצעי התקשורת המסורתיים. כמות המידע שעוברת ברשת בלתי ניתנת להשוואה ביחס לעיתונות ואמצעי התקשורת האחרים המסורתיים. מכאן נובעת התפיסה שיש לעשות שימוש באמצעים טכנולוגיים כדי להתמודד עם היקף הפעילות הגדול ברשת (והאם הרשת מצריכה חשיבה אחרת מהכללים המשפטיים שאנו מכירים?).

מחקר של UNESCO משנת 2014 מראה שהמדיניות והפרקטיקטות של גורמי ביניים ברשת בכל הנוגע להגבלת מידע מובנות ע"י הכללים המשפטיים במדינת האם (ובמידה פחות - במדינות שבהן הם פועלים). כלומר, **שהכללים המשפטיים משפיעים על התנהלות גורמי הביניים.** ככל שכללי האחריות במערכת המשפטית הרלוונטית חמורים יותר, כך גובר הסיכוי שתוכן יוסר ע"י המתווך באופן יזום או על רקע בקשה להסרתו.

**זכויות יוצרים ברשת האינטרנט: אסדרה באמצעות גורמי ביניים ושימוש באכיפה טכנולוגית**

השוואת פעילת אעכיפת זכויות יוצרים ברשת בבתי המשפט

בתי המשפט – תביעות של בעלי זכויות יוצרים בגין הפרת זכויות יוצרים ברשת.

גורמי ביינים (גוגל) -בקשות של בעלי הזכויות יוצרים לנקוט אמצעי הסרה, חסימה וסינון בגין הפרת זכויות יוצרים. במחקר: בקשות מגוגל להסיר דפים ואתרים מתוצאות חיפוש.

בתקופה שבין יולי ודצמבר 2012 – בעוד שלביהמ"ש הוגשו 99 תביעות לגוגל הוגשו 2556 בקשות הסרה (מגוגל בלבד).

מבחינת היקף האכיפה גורמי הביניים משחקים תפקיד משמעותי יותר מבתי המשפט.

ממצאים מרכזיים: אכיפה בבתי המשפט

* משרתת מגוון מצומצם של תובעים, במענה לסוג מצומצם של יצירות
	+ 61% מהתביעות לאכיפת זכויות יוצרים- בצילומים. פחות מ-3% מהתביעות לאכיפת זכויות יוצרים – בתוכנה.
	+ הסעדים המבוקשים – יותר מחצי מהתובעים ביקשו סעד כספי בלבד ופחות מארבעים ביקשו צווים שונים ופיצויים (לרבות ללא הוכחת נזק).

הליכים רבים מסתיימים בפשרה ולא בהכרעה

עדות לניסיון להפעיל לחץ על הנתבעים להפסיק את פעילות ההפרה

לא נוצר כלל משפטי (תקדימים הנחיות לפרשנות החוק או היקף ההגנה על הזכויות)

שחקנים חוזרים – למשל, ארגון זיר"ה (זכויות יוצרים ברשת האינטרנט) עושה שימוש אפקטיבי בהליך המשפטי.

ממצאים בקשות הסרה מגוגל

* בתקופת המחקר (כשנתיים וחצי)
	+ נשלחו 7091 תלונות על הפרת זכויות יוצרים לכאורה
	+ התייחסו להפרות ב-219 שמות מתחם ישראליים
	+ בכל התקופה שנבדקה בביהמ"ש נמצאו 190 תיקי הפרת זכויות יוצרים ברשת
* מספר שחקנים חוזרים בולטים שפעילים בהגשת בקשות הסרה
	+ בעיקר חברות רב לאומיות בתחום התוכנה וחברות סרטים
	+ חברת מיקרוסופט הגישה את מספר התלונות הגבוה ביותר ככל הנראה בגלל שהשימוש הוא חוזר על עצמו וחברות גדולות יכולות לבנות אלגוריתמים כדי לאתר הפרות ולהגיש תלונות ישר.
* גוגל מפרסמת נתונים גולמיים (עולמיים) ביחס לבקשות הסרה שהתקבלו אצלה בדו"חות שקיפות תקופתיים.

**אכיפה באמצעות מנגנון הודעה והסרה מתוצאות מנוע החיפוש של גוגל**

* מנוע החיפוש של גוגל הפך לכלי משמעותי לאיפה זכויות יוצרים ברשת.
	+ מדוע? היא ממלאה תפקיד מרכזי בהנגשת תכנים
* בקשות הסרה
* בעלי זכויות יוצרים (לכאורה) מבקשים מגוגל לאכוף את זכותם ע"י הסרה של קישורים לחומרים מפרים (לכאורה) מתוצאות מנגנון החיפוש של החברה. מה גוגל יכול לעשות?

הליך בקשת ההסרה כמתואר בגוגל

העובדה שמתקיים הליך מול גוגל לא מאיינת את הזכות של בעל זכות היוצרים ממשיכה לעמוד הזכות להגיש תביעה בבית המשפט.

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 מיישום נוהל הודעה והסרה בארצות הברית –

היפוך נטל ההוכחה המסורתי בדיני זכויות יוצרים

בהליך המשפטי: תוכן מוחזק כלגיטימי אלא אם הוכח אחרת – שהוא כן מר זכויות יוצרים

במנגנון הודעה וההסרה: תוכן שנטען (אך לא הוכח) שהוא מפר זכויות יוצרים מוסר במידית, כאשר החזרת התוכן מותנית בהגשת ערעור ע"י בעל התוכן

גורמי הביניים מתומרצים לתת משקל יתר להגנה על זכויות יוצרים במחיר כרסום בחופש הביטו ובזכויות יסוד אחרות

לא מוטלת אחריות בגין הסרה בתום לב של חומרים לגיטימיים

מוטלת אחריות אם נודע להם על ההפרה אך החומר לא הוסר מיידית – כפי שהוזכר "אחריות מוחלטת"

* מדיניות וולנטרית של סינון אקטיבי מראש של תכנים מפרים לכאורה
	+ העברת נטל השיטור נגד הפרת זכויות יוצרים מבעלי הזכויות לגורמי הביניים.
* משטר אכיפה אוטומטי-אלגרותמי
* בגלל היקפן הגודל של ההפרות העיבוד והטיפול אוטומטי בבקשות הסרה
* כדי להתמודד עם מיליוני הודעות הסרה בחודש
* הישענות על טכנולוגיות סינון ושיטור פרטיות
* שיקול דעת אלגוריתמי
* מושפע מאינטרסים פרטיים, כלכליים בעיקרם, של הפלטפורמות המפעילות.
* העדר שקיפות (סוד מסחרי)
* דוגמא לאכיפה אלגוריתמית: 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:

* טעות בזיהוי הפרות
* 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)

האתגר: אכיפת זכויות יוצרים מצריכה איזון ערכים

* לצד הגנה על קניין רוחני והאינטרסים הלגיטימיים של בעלי זכויות יוצרים

נדרשת הגנה על הרשת כזירת יצירה, תרבות, שיח ומסחר

האוטונמציה של הפרט

הזכות לפרטיות

חופש הביטוי, חופש הגישה למידע

חופש ההתאגדות, חופש העיסוק, תחרות חופשית

זכויות יוצרים

האם ראוי שגורמי הביניים יופקדו על האכיפה?

* הפרטה: הפקת האחריות לביצוע איזון הערכים בידי גורמי ביניים פרטיים
* טכנולוגיה: איזון הערכים מבוצע בכלים טכנולוגיים – אכיפה אלגוריתמית
* היעדר פיקוח: בפועל, לא קיימים ביקורת שיפוטית או פיקוח ציבורי (רגולטורי) אפקטיביים על אופן הפעולה של גורמי הביניים
	+ היעדר שקיפות
	+ קושי טכני – הבנת המשמעויות של קוד התוכנה

אמצעים לצמצום או מניעה של הסיכונים

* יצירת כללים ברורים בדבר טיפול ה=בתלונות – למשל, הזדהות המתלונן, נקיטת אמצעים מינימליים לבירור זכויותיו.
* שקיפות לגבי היקף שיתוף הפעולה בין גורמי ביניים לבעלי זכויות
* שקיפות לגבי אופן הפעולה של מנגנוני האכיפה של גורמי הביניים
	+ לצורך כך נצטרך סטנדרטיים בבחינת בקשות הסרה
	+ כיצד נעשית בחינת הבקשות
	+ דוחות מפורטים לגבי דפוס בקשות והחלטות הסרה

אכיפה באמצעות גורמי הביניים וסעדים טכנולוגיים: המקרה של צווי הגבלת הגישה

אכיפה של צווי בית המשפט באמצעות גורמי הביניים (למשל, מו הגבלת גישה לאתרים מפרים)

אכיפה טכנולוגיית עצמאית מצד גורמי הביניים (זיהוי והסרה אוטומטיים של תכנים)

סעדים שנפסקים במסגרת הליך משפטי "מסורתי"

בית המשפט נדרש להכריע הכרעה מהותית בשאלת ההפרה. הסעדים מכוונים לעולם הגשמי – ישומם הוא שקוף, ודאי וחד-פעמי.

בניגוד לכך, סעדים טכנולוגים (למשל, צווי הגבלת גישה)

כפופים להליך משפטי מקוצר, ללא הכרעה מהותית בשאלת ההפרה

מאפשרים לבעלי הזכויות להפסיק בקלות ובאופן מידי את הפעילות המפרה

כאן הצו מוצא אל הפועל באמצעים טכנולוגיים :ספקית הגישה מכינה קוד תוכנה שמגביל גישה לאתר.

מגוון טכנולוגיות חסימת תכנים

נבדלות בעלות, מידת האפקטיביות ומידת הפגיעה בתכנים לגיטימיים

באמצעים הטכנולוגיים הם דינמיים, היעדר שקיפות לגבי אופן פעולתם

ההגדרה הטכנולוגיות של יישום צווי ההסרה נותרת בידי ספק הגישה.

מהם צווי הגבלת גישה?

צווי ההגבלה = סעד טכנולוגי שעניינו הגבלת גישה לאתר אינטרנט, המשך מגמת פיתוח של אמצעי אכיפה טכנולוגיים כנגד הפרת זכויות יוצרים

המשמעות:

במקום לנקוט הליכים משפטיים מסורתיים כנגד משתמשי קצה או בעלי אתרים רבים( שחלקם עשויים לפעול הטריטוריות מחוץ לסמכות השיפוט).

צווי הגבלה מכוונים כלפי ספקי הגישה ויחויבו אותם לחסום גישה לאתרים או לתכנים מפרים

המצב המשפטי : לפני תיקון מס' 5 לחוק זכות יוצרים

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

הקושי: ספק הגישה איננו צד להליך משפטי בין בעל הזכות למפר

בפרשת צ'רלטון נ' 012 – ביהמ"ש דחה את תחולת דוק האחריות התורמת על ספקי הגישה.

המצב המשפטי: בעקבות תיקון מס ' 5 לחוק זכויות היוצרים

* לפי דברי ההסבר, ההסדרים החדשים נועדו לתת מענה ל"קשיי האכיפה שבהם נתקלים בעלי זכויות יוצרים בצל הטכנולוגיות החדשות(אשר הן לעצמן רצויות)".
* יצירת מקור חוקי לסמכות בית המשפט להוציא צווי הגבלת גישה שיחייבו ספקי דישה לרשת לחסום גישה למקור תוכן שמפר זכות יוצרים.

ס' 53 א "צו הגבלת גישה למקור תוכן"

סעיף הגדרות (א): מקור תוכן, בת המשפט המחוזי , ספק גישה, ספק שירותי אחסון ובעל רישיון ייחודי

מקור הסמכות(ב): לבקשת בעל זכות יוצרים או בעל רישיון....

מתווה צו הגבלת הגישה (ג)

בית המשפט יורה לספק הגישה:

לנקוט באמצעים סבירים להגבלת הגישה למקור התוכן, כולו או חלקו

בתנאים ובמידה שאינה עולה על הנדרש

שיקולים שעל בית המשפט לשקול במתן צו ההגבלה וקביעת תנאיו:

ההשפעה על הציבור..

**ביהמ"ש מחוייב לשקול שיקולים אלה גם אם לא הוגשה התנגדות ממי שהפר את זכות היוצרים.**

מה המשמעות כשמדובר בסעד טכנולוגי (אמצעי אכיפה טכנולוגיה שמיושם ע"י ספק הגישה?

אין הנחיות ברורות לביהמ"ש איך לקבוע את

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

במקום : תיתן הוראה להסרת תכון מהשרת בתנאים שייקבע

אלו קשיים מעורר השימוש הגבלת גישה?

מאפיינים מקשים להכפיפם לביקורת משפטית ופיקוח ציבורי:

הוצאת צווים כפופה לפיקוח שיפוטי מראש

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

גם לפני תיקון מס' 5 ף ביהמ"ש נדרש לשקול שיקולים שונים קביעת תנאי הצו, אך אינו נדרש לקבוע מהם אמצעי ההגבלה מידתיים ביותר בנסיבות.

העברת השליטה על האכיפה לספקי גישה פרטיים

חשש שיפעלו למקום רווחים ובהתאם לשיקולים עסקיים

חשש שיעוצבו מנגנונים בתי צוקים ומוטים,

פגיעה באיזון בין הגנה על זכויות יוצרים

חשש שמהשטר המשפטי יתמרץ אכיפת יתר וייצור אפקט מצנן

כדי להימנע מאחריות משפטית ביחס ליישום הצווים (העלויות הכרוכות בכך )גורמי ביניים עשויים ליצור תשתית טכנולגיות פרטית שתימנע את אחריותם שלא באמצעות בית המשפט וללא פיקוח משפטי או ציבורי

הגבלת גישה לאתרים המאחרים חומרים מפרים

זו סכנה כללית שטבועה בסעדים טכנולוגים שמיושמים ע"י גורמי ביניים

הרעה בדירוגן של תוצאות חיפוש הקשורות להפרת זכויות יוצרים ברשת

הסרה אוטומטית מראש של תכנים מפרים לכאורה

* הכלים של אכיפה אלגוריתימית הם רלוונטים לכלל הקשר (למשל גם בפייסבוק ולא רק בגוגל).

רקע בסיסי על זכויות יוצרים

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.

התחום מוסדר בחוק זכויות יוצרים התשס"ח-2007:

ס' 47: הפרת זכות יוצרים הינה ביצוע אחת מהפעולות אשר יוחדו לבעל זכות היוצרים לפי ס' 11 לחוק, ללא קבלת רשותו של בעל הזכות.

ס' 11: זכות יוצרים היא **הזכות הבלעדית לעשות שימוש ביצירה או בחלק מהותי ממנה פעולה** מתוך רשימה ארוכה (מעשה של העתקה, פרסום, ביצוע פומבי, שידור, העמדה לרשות הציבור, יצירת יצירה נגזרת או השכרה לצרכי מסחר).

השילוב בין ס' 47 וס' 11 מציגים תפיסה שלפיה **הפרת זכויות יוצרים היא ביצוע פעולה שיוחדה לבעל זכויות היוצרים מבלי לקבל את רשות בעל הזכות.** זו אינה הגנה מוחלטת, ובמסגרת האיזונים שנוקטים ישנה התרה של מספר שימושים:

* **ס' 19 מתיר "שימוש הוגן",** כגון מטרות חינוכיות, מחקריות ודיווחים עיתונאיים.
* **שימושים שמותרים ללא רישיון** (פרק ד', ס' 30-20, 32) כגון שימוש במסגרת הליכים משפטיים, בספריות ובארכיונים.

תביעה בגין הפרת זכות יוצרים

על התובע מוטל הנטל להוכיח כי:

1. הוא בעל זכות היוצרים ביצירה שבגינה הוא תובע
2. הנתבע הפר את זכותו

החוק קובע תנאים נוספים לקבלת הגנה על זכויות יוצרים ביצירה (לא רלוונטיים לענייננו).

האתגר של אכיפת זכויות יוצרים בעידן הדיגיטלי

* העידן הדיגיטלי ומהפיכת המידע שינו את האופן שבו יוצרים ומשתמשים משתפים ומפיצים יצירות (כולל העתקה, שינוי ושילוב פורמטים). **ניתן לשכפל יצירות, להוריד קבצים ולשתפם בקלות רבה,** מה שמאפשר הפרת זכויות יוצרים בקנה מידה נרחב מאוד.
* האמצעים לכך מצויים בידי כל משתמש קצה ברשת - באופן המרחיב את מעגל המשתתפים ויצירת **ציבור גדול מאוד של מפרים פוטנציאליים.** כתוצאה מכך, אכיפת זכויות יוצרים ברשת מחייבת נקיטת פעולות אכיפה רבות.
* **קושי נוסף הינו זיהוי משתמשים הפועלים ברשת האינטרנט באופן אנונימי**, מה שיוצר קושי בהטלת אחריות ישירה על משתמשים שהפרו זכויות יוצרים.
* יש יותר אמצעים ויותר משתמשים שיכולים להפר את זכויות היוצרים בצורה נגישה גורמת להפרת זכויות יוצרים בקנה מידה רחב. והעניין הזה נוגע גם לגידול באופן ובהיקף שבו יוצרים, מעבדים, משתמשים משתפים ומפיצים יצירות ע"י:
	+ העתקה, שינוי, שילוב פורמטים ועוד
	+ רשתות חברתיות, שיתוף קבצים, סטרימינג ועוד
	+ האמצעים מצויים בידי כל משתמש קצה ברשת (ציבור גדול של מפירים פוטנציאליים)

הפתרון של אכיפה באמצעות ביהמ"ש בעייתי

א. עלות גבוהה בפניה לביהמ"ש

ב. ספק לגבי יעילותה בהתחשב בהיקף ההפרות

ג. קושי בזיהוי משתמשים שהפרו זכויות יוצרים לצורך הטלת אחריות אישית (משתמשים רבים פועלים ברשת באופן אנונימי)

מודל האכיפה במסורתי בתחום זכויות היוצרים

* הטלת אחריות אישית על גורמים מפירים

התהליך:

* הגשת תביעות פרטניות לבית המשפט
* בחינה עניינית של שאלת ההפרה
* קבלת סעד משפטי כאשר התביעה הוכחה

מדוע בעידן הדיגיטלי קיים קושי במודל האכיפה המסורתי?

* גידול בהיקף ההפרות, ריבוי זירות הפרה ->
	+ עלות גבוהה – איתור הפרות ונקיטת פעולה
	+ ספק לגבי יעילות
* הרחבת מעגל המשתמשים המפרים, הפרות בזירה הדיגיטלית ->
	+ קושי בזיהוי משתמשים ספציפיים שהפרו זכויות יוצרים לצורך הטלת אחריות
	+ משתמשים רבים פועלים ברשת באופן אנונימי\*->קושי בחשיפתם זהותם\*\*
		- פניה לספק שירותי הגישה כדי לקבל את פרטי הזיהוי של המשתמש (כתובת IP של בעל המנוי)
		- \*בחינה מחדש של הנחת היסוד של אנונימיות \*\*שינוי במצב המשפטי בעקבות תיקון מס' 5 לחוק זכויות יוצרים – מעניק סמכות לביהמ"ש להוציא צו שמורה לספקיות הרשת לחשוף את זהות המשתמשים.

מדוע בעידן הדיגיטלי קיים קושי במודל האכיפה המסורתי? (המשך)

ספק לגבי תפיקדם של גורמי הביניים בקשר להפרות שביצעו משתמשיהם

גורמי ביניים: מנהלי אתרים, מנועי חיפוש, רשתות חברתיות וספקי אינטרנט

שתי שאלות יסוד:

האם גורמי הביניים אחראים להפרות שביצעו משתמשים באמצעות הפלטפורמה?

באופן ישיר או עקיף

האם גורמי הביניים צריכים למלא תפקיד באסדרת תחום זכויות היוצרים ברשת?

בעייתיות בהטלת אחריות/ תפקיד על גורמי הביניים בקשר להפרות שביצעו משתמשיהם->

* **יצירת חובת ניטור וסינון->**
* **עלויול כלכליות גבוהות** : פגיעה בחדשנות ובהיצע השירותים->ריכוזיות
* **מחיר חברתי: אפקט מצנן**
* פגיעה בחופש היבטוי של המתשמשים, אסדרה ע"י גורמי פרטיים
* פגיעה בפעולות רצויות ברשת

נדרש איזון בין המטרות החברתיות השונות:

* מצד אחד: הגנה על זכות יוצרים, יצירת מנגנון אכיפה יעיל
* מצד שני: החסרונות הנ"ל שבהטלת חובת ניטור וסינון על גורמי הביניים

**אסטרטגיות אכיפה חדשות בזירה הדיגיטלית המרכזית: אכיפה באמצעות גורמי ביניים ברשת**

* תמרוץ פעולות שיטור, מניעה והרתעה של גורמי הביניים
	+ עיקרון מונע הנזק הזול: איתור, מניעה והרתעה של מפירים באופן יעיל ומהיר
* מבלי להיזקק להליכים נגד מפרי חוק בבית המשפט

בזכות התמרוץ, בעל הזכויות היוצרים שאינו קשור לגורם הביניים מפחיתים את הצורך לנקוט בפעולות אכיפה נגד המפר הספציפי.

* אמצעי אכיפה: בעיקר אמצעי אסדרה טכנולוגיים
	+ פיקוח על השימוש ביצירות שהופצו באופן דיגיטלי וזיהוי הפרות
	+ אפשרות למניעה מראש של גישה / הפצה לא מורשית של יצירות
	+ נקיטת פעולות לאחר זיהוי הפרה
* אילו קשיים מעורר מודל אכיפה שנשען על גורמי ביניים פרטיים, באמצעים טכנולוגיים
	+ הפרטת האכיפה – איזון זכויות
	+ בעלי אינטרסים מסחריים
	+ היעדר שקיפות, קושי בפיקוח, היעדר בקרה שיפוטית על אופן הפעלת שיקול הדעת
	+ "הקופסא השחורה") של מנגנוני האכיפה הטכנולוגיים - האופן שבו החברה פרטה את המדיניות שלהף את האיזון שהיא עושה על הגנה על זכויות יוצרים וזכויות המתחרות לתוך שורות קוד שמזהות את התכנים המפרים, לתוך מנגונים מסוימים שהיא בוחרת להפעיל של חסימה לגישה לכתניםף וכל מנגון כזה שנבחר פוגע באיזון הזכויות במידה כזו או אחרת (זכויות הן חופש היבטוי, חופש המידע וכו'.

סוגי אמצעי אסדרה טכנולוגיים

הגבלת הגישה מוצר בו מאוחסן התוכן המוגן בזכויות יוצרים

הגבלה על העברת מידע ברשת (חסימת גישה): ספקיות גישה, מנועי חיפוש, בעלי אתרים, אמצעים טכנולוגיים שונים מבוססי IP וכו'.

אחריות גורמי הביניים להפרות שביצעו משתמשיהם

אחריות ישירה, אחריות עקיפה שכוללת דוקרטינת ההפרה התורמת ובכפוף לנוהל הודעה והסרה.

פרשת על השולחן

פרשת שוקן

פרשת רוטר

היעדר אחריות ישירה של גורמי הביניים (בגין הפרות זכויות יוצרים שביצעו משתמשיהם)

גורמי הביניים אינם חבים באחירות ישירה בגין פעולות שביצעו משתמשיהם באמצעות המערכת ובכפוף לנוהל הודעה והסרה

עם זאת: אם מקור היצירה המפירה הוא בגורם הביניים ולא במשתמשים תחול אחריות ישירה

**פרשת שוקן** – הדפסת יצירה בבעלות הוצאת שוקן ומכירתה כמקראה ע"י תא סטודנטיאלי ובפרשה הזו נקבעו התנאים להחלת דוקטרינת האחריות התורמת בדיני זכויות יוצרים:

1. התבצעה הפרה ישירה בפועל
2. למפר-התורם היתה ידיעה ממשית וקונקרטית על ההפרה הישירה (לא מהפסיקה ידיעה קונסטרוקטיבית כללית).
3. המפר -תורם תרם תרומה משמעותית ניכרת וממשית לביצוע ההפרה

\*המפר הוא גורם הביניים

עפ"י מבחנים אלה, האם סרטון שמפר זכויות יוצרים שעולה ליוטיוב, האם פעולת העלאת סרטון ניתן להאשים את יוטיוב בהפרת זכויות יוצרים? ס' 3 - עצם היותה פלטפורמה להעלאת סרטונים - היא תורמת וכלי לביצוע ההפרה. ס'2 – לא בטוח.

החלת דוקטרינת ההפרה התורמת בזכויות יוצרים על גורמי ביניים ברשת, בכפוף לנוהל "הודעה והסרה" (פרשת רוטר)

אומצה הדוקטרינה הזו במשפט הישראלי.

הרקע: גולשי האתר פרסמו בפורומים קישורים לאתרים אליהם הועלו יצירות ללא הרשאה (=הפרת זכויות יוצרים) .

העיקרון שנקבע: אין להטיל אחריות להפרת זכות היוצרים על בעל אתר שלא ידע עליה, כל עוד כאשר נודע לו עליה הסיר את הפרסום המפר סמוך להודעה. אם הוכחנו שהוא ידע כבר אין צורך בהודעה.

המשמעות:

* חסינות לגורמי הביניים מפני אחריות-תורמת להפרה ב"מחיר" של ניהול מנגנון הודעה והסרה
* גורמי הביניים ברשת הפכו לגרוע אכיפה בתחום זכויות היוצרים

מצבים חריגים בהם תוטל אחריות על גורם הביניים בגין פעולות משתמשים

**"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 לקיומן 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").

**זכויות יוצרים ברשת האינטרנט: אסדרה באמצעות גורמי ביניים ושימוש באכיפה טכנולוגית**

* במאמר של ניבה אלקין קורן ופרל נשאלת השאלה עד כמה באמת יש אנונימיות ברשת? האם באמת ישנו קושי גדול בהצלבת מידע של משתמשים? (למשל, בגלישה בפלאפון ניתן להצליב את המידע ב-LOGIN עם אמצעים מזהים). במאמר נטען כי הנחת האנונימיות צריכה להישקל מחדש בהיבטים מסוימים, כי הטכנולוגיה עצמה מאפשרת כיום לזהות בצורה טובה יותר את המשתמשים. נעסוק בכך בהגנת הפרטיות (הצד השני של המטבע).

כדי לקבל את פרטי הזיהוי של המשתמש המפר (כתובת IP של בעל המנוי שבאמצעותו בוצעה הפעילות), בעל הזכויות נדרש לפנות לספק שירותי הגישה. ביהמ"ש קבעו שלא קיימת סמכות בחוק המאפשרת להם להורות לספק לחשוף את זהותו של משתמש שלכאורה ביצע עוולה אזרחית, ולרוב דחו בקשות שכאלו.

דוגמה - **ע"א 9183/09 the football association premier league limited נ' פלוני ואח':** הליגה האנגלית ביקשה לחשוף את זהות המשתמשים באתר שאפשר לישראלים לצפות במשחקי הליגה האנגלית בתשלום חלקי כדי לתבוע אותם, וביהמ"ש קבע שאין סמכות להורות על חשיפת פרטיהם. בפסק הדין הוזכרו דוקטרינות אחרות שבגינן ניתן לחייב את גורם הביניים באחריות תורמת, אבל לא שיש לביהמ"ש סמכות להורות לגורם הביניים לחשוף את זהות המשתמש.

ישנה **הצעה לתיקון מס' 5 לחוק זכויות יוצרים, המבקשת ליצור מקור לסמכות זו:** בפרק ח1 מדובר על חשיפת זהותו של עושה פעולה בתוכן ברשת תקשורת אלקטרונית. לפי הצעה זו, לביהמ"ש תהיה אפשרות להורות לגורמי הביניים לחשוף את זהות מבצעי הפעולה.

התוצאה של מגבלות האכיפה באמצעות בתי המשפט היא **שבעלי זכויות יוצרים נדרשו לפתח אסטרטגיות אכיפה חדשות, כאשר המרכזית שבהן היא אכיפה ע"י גורמי ביניים ברשת** (אתרים, מנועי חיפוש, ספקיות גישה, רשתות חברתיות וכו').

זאת, במטרה **לחזק את האכיפה ברשת מחוץ לבתי המשפט ולייצר פעולות שיטור, מניעה והרתעה** מבלי להזדקק להליכים נגד מפרי חוק בבית המשפט.

האמצעים הננקטים לשם כך הינם בעיקר אמצעי אסדרה טכנולוגיים, והקושי הטמון בכך הינו שמדובר ביצירת מנגנוני אכיפה פרטיים, לרוב גופים מסחריים, שפועלים בהיעדר שקיפות וללא כל בקרה משפטית. עם זאת, ניתן לראות יותר אכיפה בפועל דרך אותם גורמי ביניים.

סוגי אמצעי אסדרה טכנולוגיים

א. הגבלת הגישה למוצר שבו מאוחסן התוכן המוגן בזכויות יוצרים (למשל, מנעולים דיגיטליים).

ב. הגבלת על העברת מידע ברשת. מוטלת באופן טיפוסי על ספקיות גישה, ספקיות מארחות, מנועי חיפוש, בעלי אתרים, פלטפורמות שיתוף קבצים - אמצעים טכנולוגיים שונים מבוססי IP, DNS, URL ועוד.

כיצד ניתן לקדם אסדרה באמצעות גורמי ביניים?

1. **אחריות ישירה -**

ביהמ"ש לא הטילו על גורמי ביניים אחריות ישירה בגין פעולות שבוצעו בידי משתמשים באמצעות המערכת. אולם, אם מקור היצירה המפירה הינו בגורם הביניים עצמו - תחול אחריות ישירה להפרה (פורום/מגזין אינטרנטי המפרסם עותקים של יצירות ללא רישיון).

1. אחריות עקיפה (הדרך המרכזית) - בעיקר באמצעות **דוקטרינת ההפרה התורמת**, שהבסיס לה הוא "נוהל הודעה והסרה" (הסדר שאומץ מארה"ב).

אחריות תורמת להפרת זכויות יוצרים (גורמי ביניים בעולם הפיזי) - פרשת שוקן

**ע"א 5977/07 האוניברסיטה העברית נ' בית שוקן להוצאת ספרים בע"מ:** סטודנטים באוניברסיטה הדפיסו, כרכו ומכרו יצירה שהייתה בבעלות שוקן בשטח האוניברסיטה (אך לא באישורה). ביהמ"ש דן בשאלת האחריות של האוניברסיטה, וקבע תנאים להחלת דוקטרינת ההפרה התורמת בדיני זכויות יוצרים:

1. קיומה בפועל של הפרה ישירה

2. ידיעה ממשית וקונקרטית של המפר-התורם על ההפרה (לא די בידיעה קונסטרוקטיבית כללית)

3. תרומה ממשית, ניכרת וממשית לביצוע ההפרה

בשורה התחתונה, **גורמי הביניים יישאו באחריות אם הם תרמו בידיעה לביצוע הפרה ישירה של זכות היוצרים בידי משתמשי קצה או עודדו אותה.** האוניברסיטה באותו מקרה לא חויבה באחריות, כי לא עמדה בתנאי הדוקטרינה (לא הייתה לה ידיעה ממשית או תרומה משמעותית).

החלת דוקטרינת ההפרה התורמת בזכויות יוצרים על גורמי ביניים ברשת - פרשת רוטר

**ת"א (מחוזי מר') 567-08-09 א.ל.י.ס בע"מ נ' רוטר.נט בע"מ:** גולשי האתר רוטר פרסמו בפורומים שלו קישורים לאתרים שאליהם הועלו יצירות ללא הרשאה (הפרת זכויות יוצרים). העיקרון שנקבע בפסק הדין הוא **שאין להטיל אחריות להפרת זכות יוצרים על בעל אתר שלא ידע עליה, כל עוד כאשר נודע לו עליה הסיר את הפרסום המפר סמוך להודעה.**

המשמעות של קביעת דוקטרינת האחריות התורמת הנושא זה בכפוף לנוהל "הודעה והסרה" היא **שכל עוד גורמי הביניים מקיימים מנגנוני הסרה של תכנים מפרים, תהיה להם חסינות מפני אחריות להפרת זכויות יוצרים בידי משתמשים.** בנוסף, כדי לממש את המנגנון הזה **גורמי הביניים ברשת הופכים לזרוע אכיפה בתחום זכויות היוצרים.**

שיקולי מדיניות בהחלת דוקטרינת ההפרה התורמת על מתווכים ברשת וקיום נוהל הודעה והסרה

1. היקף וחומרת ההפרות גדולים יותר בשל הקלות להפר זכויות ברשת (**פס"ד לוין נ' קניבסקי**).

2. חשיבות בהגנה על זרימת המידע, זכות הציבור לדעת וחופש הביטוי.

3. חשש מהטלת עלויות כבדות של ניטור וסינון על גורמי הביניים הפרטיים.

4. סכנה ליצירת אפקט מצנן על פעולות רצויות בשל הטלת אחריות על גורמי ביניים (**פס"ד רוטר**).

5. "המחיר הערכי" של הפיכת ספקיות האינטרנט למעין צנזור ברשות ביהמ"ש שקול לפחות (אם לא כבד יותר) לפגיעה בזכות הקניין הרוחני (**ת"א (מחוזי ת"א) 37039-05-15 זיר"ה נ' פלוני**).

**משטר "הודעה והסרה"** קובע כי אין להטיל אחריות להפרת זכות יוצרים על בעל אתר שלא ידע עליה, וכאשר נודע לו עליה הסיר את הפרסום המפר (קובץ או קישור לאתר מפר) סמוך להודעה.

חריגים לכלל "הודעה והסרה", שבהם כן תוטל אחריות על האתר בגין פעולות משתמשים -

1. **"עידוד":** אם האתר עצמו מעודד פרסום קישורים מפרים (נלמד מאופי שיווק האתר ומשמו, תקנון הפורום והאמירה הכוללת לגולשים).
2. "**הפורום הפסול":** הפורום משמש, רובו ככולו, להצבת קישורים לאתרים מפרים. הקביעה נעשית בשני אופנים: אבסולוטי (מספר הקישורים לאתרים מפרים) ויחסי (אחוז הקישורים המפרים ביחס לכלל ההודעות בפורום).

כללי אצבע היוצרים חשד לפורום פסול

בפרשת רוטר השופט גרוסקופף מספק כמה **כללי אצבע היוצרים חשד ל"פורום פסול",** תוך הבחנה בין פורום סגור (שהכניסה אליו מוגבלת בתשלום או באופן אחר, ולכן קשה יותר לבעלי זכויות היוצרים לבצע פיקוח) לבי פורום פתוח.

**בפורום סגור צריכים להיות 10 קישורים מפרים,** והודעות הכוללות קישורים מפרים מהוות **יותר מרבע מההודעות המהותיות** בפורום.

**בפורום פתוח צריך שלפחות מחצית מהתוכן המהותי של הפורום** יהיה הודעות הכוללות קישורים לאתרים מפרים.

המשמעות של הוכחת "פורום פסול"

 **חזקה שבעל האתר מודע לכך שהוא מסייע לקיומן של הפרות ישירות וכי סיוע זה הוא בגדר תרומה ממשית ומשמעותית להפרות.**

במצב כזה הנטל עובר לבעל האתר, שעליו להוכיח אחד משניים:

1. יש **ערך לגיטימי להמשך קיומו של הפורום** (כגון קידום ערכים חינוכיים או סיוע לאוכלוסיות חלשות).
2. הוא **לא ידע על היקף הפעילות האסורה** (ולכן לא יישא באחריות אלא לאחר שנמסרה לו הודעה על כך שמדובר ב"פורום פסול")

מקרים נוספים שבהם האתר יצא אחראי:

פס"ד גולצמן: נפסק פיצוי כי גורם הביניים נמצא אחראי בגין תכנים מפרי זכויות יוצרים שהועלו לאתר, משום שההפרה לא בוצעה ע"י גולש אנונימי אלא ע"י כתב השותף בניהול האתר.

פס"ד ברזל: משרד החינוך חויב בתשלום פיצויים למרות שימוש הראוי בנוהל "הודעה והסרה", משום שעובדי המשרד הם אלו שהעלו את החומר המפר.

המעמד המשפטי של נוהל "הודעה והסרה"

במשפט המשווה - מעוגן בחוק. בארה"ב יש את ה-Digital millennium copyright Act; באירופה ישנה הדירקטיבה האירופית בנושא סחר אלקטרוני.

בישראל נוהל "הודעה והסרה" הינו יציר הפסיקה (פס"ד "על השולחן"; גלעד נ' נטוויז'ן; רוטר).

אלקין קורן ובר זיו ערכו מחקר אמפירי שבו השוו את היקף פעולות האכיפה בביהמ"ש לעומת גורמי הביניים. 99 תביעות משפטיות מול 2,556 בקשות הסרה (רק ממנוע החיפוש של גוגל).

ממצאים מרכזיים: אכיפה בבתי המשפט

נראה שההליכים ביהמ"ש משרתים מגוון מצומצם של תובעים ונותנים מענה לסוג מצומצם של יצירות (יותר ממחצית מהתביעות קשורות לצילומים, פחות מ-3% מהתביעות קשורות בתוכנה). הליכים רבים מסתיימים בפשרה (ולא בהכרעה), הכוללת פיצוי נמוך מזה שנתבע במקור. כלומר, סעד האכיפה והסרת התוכן המפר היה פחות משמעותי בהשוואה לגורמי הביניים - מה שמשקף שלעיתים קרובות **עצם הגשת התביעה נועדה להפעיל לחץ על הנתבע להסיר את התוכן המפר.** בנוסף, **היעדר הכרעה בביהמ"ש מוביל לכך שלא נוצר כלל משפטי** (תקדים מחייב, הנחייה לפרשנות החוק או היקף ההגנה על הזכויות)

ממצאים מרכזיים: אכיפה באמצעות מנגנון הודעה והסרה מתוצאות מנוע החיפוש של גוגל

מנוע החיפוש של גוגל הפך לכלי משמעותי לאכיפת זכויות יוצרים ברשת בשל תפקידו המרכזי בגישה לתכנים ברשת. תכנים שאינם נגישים באמצעות מנוע החיפוש, או נדחקים לתחתית התוצאות, מאוד קשים לאיתור. כשמגישים בקשת הסרה לגוגל, בעצם מבצעים "הדרה" מתוצאות החיפוש, שיכולה להקטין משמעותית את התעבורה באתר. גוגל מפרסמת דוחות שקיפות תקופתיים שמאפשרים לראות כמה מתוך בקשות ההסרה היא מקבלת בפועל.

* "בקשות הסרה": בעלי זכויות יוצרים (לכאורה) מבקשים מגוגל לאכוף את זכותם על ידי הסרה של קישורים לחומרים מפרים (לכאורה) מתוצאות מנגנון החיפוש של החברה.

**שיעור 6 (עובד מסיכומים של שיר ואור) - 23.4.18**

ישנו מספר בולט של שחקנים חוזרים הפעילים בהגשת בקשות הסרה (בעיקר חברות בינ"ל בתחום התוכנה וחברות סרטים). חברת מייקרוסופט הגישה את מספר התלונות הגבוה ביותר.

כיצד פועל מנגנון בקשות ההסרה? גוגל מציגה אותו כמנגנון פשוט ויעיל עבור בעל זכויות היוצרים. טופס אינטרנטי פשוט, הנשלח לגבי התוכן המפר לכאורה. הבקשה נבדקת בקפידה ע"י צוותים אלגוריתמיים ואם אין עמה בעיה - התוכן מוסר.

איזון ערכים חברתיים באכיפה ע"י גורמי ביניים

הרשת אינה רק זירה להפצת תוכן מפר (המצריכה הגנה על קניינם של היוצרים) אלא גם זירה חשובה לחופש הביטוי, המידע, התפתחות המסחר והשוק החופשי. חשוב להבטיח הגנה על הערכים שטמונים ברשת כזירת יצירה ומסחר.

יש כאן שאלה מהותית: באיזו מידה גורמי הביניים מגנים גם על האינטרסים הללו? לא ברור אם יש הגנות על האוטונומיה של הפרט במנגנונים של גוגל, ואין יכולת ממש לפקח על כך שההליך משיג איזון ראוי בין הערכים. חשיבות האיזון בין האינטרסים המגולמים ברשת (הגנה על זכויות היוצרים מול הגנה על זירת היצירה, השיח והמסחר) הוכרה ע"י ביהמ"ש העליון **בפרשת מור.**

החשש הוא **שהמציאות המשפטית עלולה לעודד גורמי ביניים לפעול לניטור וחסימת יתר של תכנים ומשתמשים** כדי לנהל את הסיכונים המשפטיים שלהם, ואפילו מראש! (מניעת פרסום). קיים גם חשש מפני ניצול לרעה של מנגנון ההודעה וההסרה (תלונות שווא, מנועים ששולחים הודעות הסרה ב אופן אוטומטי וכו'). גם למי שאינו בעל זכויות היוצרים יש אפשרות טכנית להגיש תלונות, ויכול להיווצר מצב שבו נחסמים תכנים לגיטימיים.

דרכים לצמצום או מניעת הסיכונים

* באמצעות **פיקוח חיצוני, ניתן כרגולטור ליצור כללים ברורים לטיפול בתלונות** (למשל, הפחתת תלונות שווא באמצעות חיוב המתלונן להזדהות; בירור מינימלי של זכויותיו).
* שקיפות לגבי **היקף שיתוף הפעולה בין גורמי ביניים לבעלי זכויות** (איך עובד מנגנון ההתממשקות בין מייקרוסופט לגוגל? מה הם נדרשים להוכיח?).
* **שקיפות לגבי אופן פעולת מנגנוני האכיפה של גורמי הביניים** (מידע על תהליך ההסרה).

כוחות השוק הובילו להתפתחות סעדים כמו הודעה והסרה בקרב גורמי ביניים. למשל, במקום לבקש מכל אתר או גורם ביניים לחסום גישה לתוכן מפר, ניתן לעלות שלב ולערב את מערכת המשפט באמצעות **צווי הגבלה - לבקש מספקית האינטרנט** **לחסום גישה לתכנים מסוימים בצורה גורפת.** ישנו תיקון לחוק (שטרם התקבל) המציע לקבוע זאת כסמכות סטטוטורית, משום שמרבית ביהמ"ש פסקו עד כה שאין סמכות להוצאת צווי הגבלת גישה ברשת בהיעדר מקור חוקי.

סעדים מסורתיים

פסיקת סעדים "מסורתית" ע"י בית משפט דורשת הכרעה בשאלה האם התקיימה הפרה או לא. היישום של צו בימ"ש הדורש להסיר שלט פרסומת המפר זכויות יוצרים הינו **חד פעמי, רלוונטי למקרה הקונקרטי, חל בעולם הגשמי** ושמור לחברה מסוימת.

סעדים טכנולוגיים

**סעדים טכנולוגיים** (כמו צווי הגבלת גישה) **כפופים להליך משפטי מקוצר ופשוט,** אף ללא הכרעה מהותית בשאלת ההפרה. הם מאפשרים לבעל הזכויות להפסיק בקלות ובאופן מידי את הפעילות המפרה. **יישום הצווים יעשה באמצעים טכנולוגיים דינמיים ובלתי שקופים** (למשל, אם יש צורך לחסום גישה לתוכן מפר, שמשנה את מיקומו ואופן הגישה אליו, אז גם היישום הטכנולוגי של הצו ישתנה כדי להתאים את עצמו למציאות המשנה).

**פרטיה הטכניים של טכנולוגיית הגבלת הגישה** (החסימה) שמשמשת ליישום הצו הם שמגדירים את אפקט התחולה והאפקטיביות של צווי ההגבלה, ולפיכך:

1. **מגדירים את היקף ההגנה שניתנת בפועל לזכויות היוצרים.**
2. מגדירים את **האיזון בין זכויות היוצרים וזכויות בעלי התכנים, ספקי הגישה וציבור המשתמשים** (כמו חופש הביטוי והזכות לפרטיות).

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

מאפיינים טכנולוגיים של צווי הגבלת גישה

הוצאת הצו אל הפועל נעשית באמצעות אלגוריתם או קוד שמונע תעבורה לאתר החסום. ההגדרות הטכניות שבבסיס האלגוריתם הן אלו שקובעות למעשה את היקף תחולתו, יעילותו והשלכותיו של סעד החסימה. קיימות טכנולוגיות חסימת תכנים שונות הנבדלות זו מזו מבחינת עלות, אפקטיביות ופגיעה אפשרית בתכנים לגיטימיים. האמצעים הספציפיים שייבחרו יקבעו בסופו של דבר את גבולות חופש הביטוי, וישפיעו על ניטרליות הרשת לתחרות ולחדשנות.

הקשיים שמתעוררים בשימוש בצווי הגבלת גישה

* מאפייניהם הייחודיים מקשים להכפיפם לביקורת שיפוטית ופיקוח ציבורי
* חשש מאכיפת יתר מצד גורמי הביניים כדי להימנע מאחריות משפטית
* הסרה אוטומטית מראש של תכנים מפרים לכאורה

הצעת חוק זכויות יוצרים

הצעת חוק זכויות יוצרים פורסמה בנובמבר 2017 ומציעה ארבעה הסדרים חדשים, וביניהם את חשיפת פרטיו של הגולש האנונימי. נתמקד בנושא של צווי הגבלת גישה. לפי הצעת החוק, הסיבה להצעת הסדרים חדשים היא התפיסה שלפיה בעלי זכויות יוצרים נתקלים בקשיי אכיפה בשל הטכנולוגיות החדשות שממשיכות להתפתח (שהן כשלעצמן רצויות). כלומר, בתפיסת מנסחי הצעת החוק מוטמעים שני היבטים:

1. רשת האינטרנט מקשה על אכיפת זכויות יוצרים.
2. דרושים הסדרים משפטיים נוספים כדי להתמודד עם המצב.

האם הנחות יסוד אלו נותרו רלוונטיות כיום?

לדעתן של אלקין קורן ופרל, הנחות אלו היו רלוונטיות בשנות ה-90 אבל לא עוד, גם משום שיש יותר שירותים חוקיים לרכישת יצירות דיגיטליות (ולפיכך פחות הפרות), וגם כי ישנם שליטה ופיקוח מובנים על השימוש ביצירות הגנובות הזכות הטכנולוגיות החדשות (המעבר לשירותי ענן, אינטרנט סלולרי ושירותי סטרימינג מאפשרים שליטה רבה יותר על שימוש ביצירות). העובדה שניתן למנוע הפרה בשלב מוקדם, עוד לפני ההתרחשות עצמה מצטרפת לירידה בהיקף הפיראטיות ברשת נוכח הגידול בהיצע השירותים החוקיים.

התמריץ להצעת החוק נובע **ממחלוקת שקיימת בבתי המשפט לגבי הסמכות להוציא צווי הגבלת גישה לספקיות האינטרנט.** ספקית הגישה אינה המפר עצמו, הפלטפורמה שעליה מתרחשת ההפרה או צד להליך משפטי של הפרה.

העמדה המקובלת יותר הופיעה **בפס"ד צ'רלטון בע"מ נ' 012 סמייל:** חברת צ'רלטון ביקשה מביהמ"ש לאשר את פנייתה לספקית האינטרנט 012 בדיעבד, כשצ'רלטון ביקשה שתיחסם גישת לקוחותיה של 012 לאתרים פיראטיים ששידרו שידורי ספורט שבהם יש לצ'רלטון זכויות שידור בלעדיות. צ'רלטון ביקשה שייפסקו לה פיצויים בגין סירוב ספקית הגישה לקיים את הבקשה. ראשית ביהמ"ש רבע שלספקית הגישה אין אחריות תורמת להפרה (הדוקטרינה לא חלה עליה כי אינה חלק אינטגרלי ומשמעותי מהשרשרת שהובילה להפרה), **ובהיעדר סמכות בחוק, לביהמ"ש אין סמכות להוציא לה צו הגבלת או חסימת גישה.** עמדה זו זכתה להדהוד בפסקי דין נוספים.

עמדה אחרת בפסיקה, שגורסת כי לביהמ"ש דווקא יש סמכות בנושא, הופיעה **בפרשת בלומברג:** אתר בשם Unidown אפשר להאזין ליצירות ישירות מיוטיוב וגם להוריד אותן. התעוררה השאלה האם ישנה הפרה תורמת של האתר? כמו כן התבקש ביהמ"ש להוציא צו הגבלת גישה לספקיות האינטרנט. דווקא ל-MBC הייתה הצלחה וביהמ"ש קבע שהייתה הפרה תורמת מצד האתר, והושג צו חסימת גישה לספקית. כלומר, **שם נקבע שלביהמ"ש יש סמכות להוציא צו כזה.**

הצעת החוק: אמצעים סבירים להגבלת גישה

בהצעת החוק נקבע כי ביהמ"ש יוסמך לתת צו מניעה כנגד צדדים שלישיים לשם הגבלת גישה בגין הפרת זכויות יוצרים, לכולו או לחלקו, כאשר עיקר אתר האינטרנט הינה הפרת זכויות יוצרים. כך, במקום לנקוט בהליכים אינדיבידואלים נגד מפרים או בעלי אתרים (כאשר חלק מהאתרים בכלל פועלים מחו"ל ואין לביהמ"ש סמכות שיפוט כלפיהם), ניתן יהיה להורות על צו הגבלה שיכוון כלפי ספק הגישה, ויחייבו לחסום את הגישה לתכנים/האתרים המפרים.

 **ס' 53א(ג) להצעת החוק אומר שהספקיות יידרשו לנקוט אמצעים סבירים להגבלת הגישה.** מהם אמצעים סבירים? אם ביהמ"ש לא ייתן הנחיה ברורה או קווים ליישום, ההכרעה הערכית לגבי המשקל היחסי של הזכויות המתנגשות תהיה נתונה להערכת ספק הגישה. כמה חשוב לתת עדיפות לאפקטיביות החסימה? כמה לעלות החסימה? עד כמה נוודא שהאכיפה מדויקת? עד כמה נבחן את השפעתה על זכויותיהם של משתמשים או בעלי אתרים?

ס' 53א(ד) מספק רשימת סל של שיקולים שביהמ"ש ישקול:

* חומרת ההפרה הנטענת
* נחיצות הצו למניעת הפרת זכויות היוצרים
* יעילותם של סעדים אחרים העומדים לרשות בעל זכויות היוצרים/בעל הרישיון הייחודי
* מידת הפגיעה הצפויה בגישה לאתרי אינטרנט אחרים
* מידת הפגיעה הצפויה בפרטיות של משתמשי האינטרנט
* ההשפעה על הציבור כתוצאה מהגבלת הגישה לפי הצו/מהחלטת ביהמ"ש שלא לתת צו

**שיקולים אלו מנחים את ביהמ"ש בשלב הוצאת הצו** (האם בכלל להוציא צו?), ולא בשלב היישום. אין הנחיה של ביהמ"ש ביחס לביצוע הצו ע"י הספק. מידת הפגיעה הצפויה, יעילות הצו והשפעתו על הציבור - כל אלו עשויים להשתנות בהתאם לטכנולוגיית החסימה שהספק ינקוט.

לפי ס' 53א(ב) צו הגבלת גישה מכוון לאתר אשר עיקר התוכו שבו מפר. כיצד בוחנים מה זה "עיקר"? ומה לגבי פגיעה בתכנים לגיטימיים? זה חשוב, כי בעלי התכנים הלגיטימיים לא יהיו צד להליך ולא תהיה להם אפשרות להגן על זכויותיהם במסגרת הוצאת הצו (רק לאחר מכן יוכלו לערער לשינוי או ביטול הצו).

 הדרישה לעניין "עיקר התוכן" בהצעת החוק מדברת על מבחן מהותי ולא טכני-כמותי, אולם לא ברור כיצד יש לאומדה. ביחס לכלל התכנים באתר? רק ביחס לתכנים המוגנים בזכויות יוצרים?

חשש לאכיפת יתר בשל מעמדם הדיוני המיוחד של צווי הגבלת הגישה (חסימה טכנולוגית)

למרות שההגדרה הפורמלית של הצו הינה "סעד זמני", מבחינה מהותית מדובר בסעד העיקרי בהליך ויש לכך מספר השלכות:

* כדי לשנות את הצו בעלי זכויות תכנים לגיטימיים יצטרכו לפנות מחדש לביהמ"ש בבקשת ביטול או שינוי. זאת, לעומת מתן סעד זמני שבמסגרתו החוק מחייב איזון בין הנזק שייגרם אם יוצא הצו או לא יצא ביחס לכל אחד מהצדדים המעורבים. במקרה הזה אין בהצעת החוק הסדרה מהותית שמבטיחה שיינתן משקל לכל אחד מהצדדים במערכת היחסים הזו, וההליך יכול להמשיך גם אם לא אותרו בעלי זכויות נוספות שעלולים להיפגע ממתו הצו.
* ההליך למתן צו הגבלת גישה הוא ההליך העיקרי, היחיד והסופי המתנהל בנוגע לשאלת ההפרה (בשונה מסעד זמני, שמטבעו נלוו להליך עיקרי אחר).

לקחים מיישומו של "נוהל הודעה והסרה" בארה"ב

ה-DMCA האמריקני היה החלוף בעירוב גורמי הביניים באכיפה ויצירת תמריץ לחברות ענק אינטרנטיות לפתח מנגנוני אכיפה אוטומטיים. כבר לפני 20 שנה הוא קבע את נוהל ההודעה וההסרה, שבעצם **הפך את נטל ההוכחה בדיני זכויות היוצרים.** במקום שנקודת המוצא תהיה שהתוכן הינו לגיטימי, הנוהל הוא שקודם מסירים את התוכן כדי להימנע מאחריות. זה בעייתי כי זה נותן מתמרץ גורמי ביניים להסיר תכנים. זאת, משום **שאם תכנים לגיטימיים הוסרו בתו"ל, לא תוטל עליהם אחריות - בעוד שידיעה לכאורה על הפרת זכויות יוצרים תטיל עליו אחריות תורמת להפרה.** הסיכון המשפטי שטמון בלא להסיר את התוכן המפר לכאורה גדול בהרבה מהסיכון שבהורדת תוכן בכל מקרה. השיקול העסקי הברור הוא להסיר - ומי שמשלם על כך את המחיר הם בעלי התוכן הלגיטימי והציבור, שסובל **מפחות חופש מידע ברשת.**

במקביל, גם הרבה מבעלי זכויות היוצרים מנהלים את זכויותיהם באופן אוטומטי (בקשות ההסרה נעשות באופן אוטומטי). גם גורמי הביניים שמכריעים בנוגע להגנה על זכויות היוצרים עובד "על אוטומט" - למשל, מערכת ה-Content ID של יוטיוב, שמסירה תוכן חשוד גם אם לא היה עומד במבחן משפטי כתוכן מפר.

**שיעור 7 – 29.4.19**

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?

* 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?

1. *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.**

1. *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.

General Data Protection Regulation

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

מהו מידע אישי לפי הגישה האירופאית?

* 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.
* מידע אנונימי/ סטטיסטי, אם אינו מנותק מהאדם
* יכול להתאפשר זיהויו באמצעות פעולה של דה-אנונימיזציה
* 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 והאירופה, 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 איסוך 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.
* להבין לקוחות ולנתח את נכונותם לרכוש מומרים ושירותים.
* לסנן מועמדים לעבודה ולבחון את התאמתם
* לנווט ולהשפיע על התנהגותנו

המידע עשוי לבוביל לאפלייה 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
	+ ס' 7 לחו"י כבוד האדם וחירותו.
* הגנה רחבה על פרטיות
	+ ס' 2 לחוק הגנת הפרטיות – התשמ"א- 1981.
* הגנה רחבה למדי 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), 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.

מהו "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).

**שיעור 8 (עו"ד חיים רביה)**

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.

* **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?

1. עיבוד מידע **המבוסס על הסכמה.** להסכמה יש יתרונות וחסרונות (קל מאוד לתת הסכמה אולם יש תחומים שאין בהם תחולה להסכמה, והסכמה תמיד ניתן לבטל).
2. 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).
3. עיבוד מידע **החיוני לציות לחוק** (דיני מס הכנסה, צווים של בימ"ש).
4. עיבוד מידע **החיוני לאינטרס אישי של נושא המידע או צד שלישי** (רופא מטפל).
5. עיבוד מידע **החיוני לאינטרס הציבורי** (מחקר סוציולוגי).
6. 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.

**שיעור 9 - 28.5.18**

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.**

* אמת המידה להגנה המשפטית על מידע היא תוכנית. 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.

* **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?

1. 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)).
1. פיקוח על פעילות המאגר.
2. 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 יהיה זכות עיון, אם זה עלול לגרום נזק חמור לביראתו הגופנית או הנפשית של המבקש או לסכן את חייו.

ס' 13:

1. וכל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.
2. 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.
3. 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:

* יש לקבוע מהו המידע המוגן והסיכונים הקשורים אליו
* יש לקבוע נהלים מפורטים וברורים לאבטחת מידע
* קביעת הוראות מהותיות בניהול אבטחת מידע

תקנות מודולריות: הסדרים ביחס לארבעה סוגי מאגרי מידע

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

* ככל שפעילות עיבוד המידע בארגון משמעותית יותר. למשל: כשהמאגר מכיל מידע רגיש / מידע על אנשים רבים ומטרת המאגר היא מסירת מידע לאחרים
* 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
* 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").

מהפכת הפרטיות באירופה: General Data Protection Regulation (27/05/19)

האתגרים של חדירה לפרטיות והסכנה של הפרופיילינג, ושיכולות להיות לה תוצאות חמורות על החיים שלנו. הGDPR מנסה להתמודד עם האתגרים האלו.

Data protection regulation: מציגה גישה מרחיבה יותר להגנת הפרטיות והיא נובעת מתוך הגנת המידע. בהשוואה לגישה של ארה"ב (הסקטוריאלית) שקובעים חוקים מאוד ספציפיים – נק' המוצא של הGDPR:

* לכל אדם יש זכות יסוד לחירות ופרטיות
* לכל אדם יש זכות להתגונן מפני עיבוד של מידע פרטי אודותיו ללא קשר ללאום שלו או למקום מגוריו.

אחת הסיבות לכך שבאירופה ההגנות יותר מחריבה היא בגלל מלחמת העולם השנייה בה נאסף מידע על נטיות מיניות, על מוצא וכו'.

שימו לב: ה GDPR **לא חלות** על סוגיות של בטחון פנים וחוץ, פעולות למניעת פשעים ולחקירתם, מידע של הרשות השופטת עצמה (לא על מה שנאמר במסגרת פס"ד).

הGDPR נותנת סל של זכויות וכלים למושאי המידע וסמכויות רבות לרגולטורים במדינות האיחוד השונות. הכוונה ברגולטורים = רשויות להגנת הפרטיות במדינות האיחוד האירופי.

* כלים: הליכים מנהליים, קנסות כספיים משמעותיים על מי שמפר את ההוראות השונות, במקרים מסוימים – נקיטה בהליכים פליליים.
* הGDPR שמות במרכז את מושאי המידע = נושאי המידע = נשואי המידע (DATA SUBJECTS) כאשר הם כל אדם מזוהה או ניתן לזיהוי שעל אודותיו נאסף / מעובד מידע אישי.
* המטרה – לחזק את השליטה של מושאי המידע במידע האישי שלהם.
* האמצעי להשגת המטרה - היא או הבטחה שהעיבוד נעשה בהסכמה או באופן חוקי + סל זכויות וכלים.
* בסה"כ יש 6 דרכים שבאמצעות אפשר לאשר עיבוד/ העתרה וכו' של מידע אישי.
* הGDPR מסדירות זכויות במידע ככלל ולא רק הגנה על הפרטיות. כמו למשל ניוד מידע, גישה למידע, הזכות להישכח ועוד. הGDPR אומרות שניתן להעביר את המידע עליי – למשל אם אני מנויה לנטפליקס ואני רוצה לעבור ל"הולו" אבל אני לא רוצה לחכות שהם ילמדו מה העדפות שלי.

הGDPR נכנסו לתוקף ב-28.5.18. קדמה להן דירקטיבת הגנת פרטיות האירופאית משנת 1996. דירקטיבה (DIRECTIVE) המשמעות שהמדיניות החברות צריכות לבצע חקיקה פנימית כדי להתאים את עצמן להראות של הדירקטיבה. לעומת זאת, תקנות (REGULATION) מהוות דין מחייב עבור המדינות (אין צורך באימות לדין הפנימי) וזה אומר שהמדינות אינן רשאיות לסטות מהוראותיה בדין הפנימי. אך הן מותירות נושאים מסוימים שלגביהם המדינות רשאיות לקבוע הסדרים פרטיקולריים (recitals זה הנושאים שהמדינות יכולות לקבוע ).

מדוע GDFR גרמה למהפכה?

* היא נתנה בוסט למה שמושא המידע יכולה לעשות - לתת חתימה בעלת משמעות וכן הזכות להישכח שהיו מוגבלות או הוכרו רק בפסיקה.
* הרחבה של מה שנחשב מידע אישי (personal data / personal information) – יש הגנה על יותר דברים.
* הגדרה מרחיבה של עיבוד מידע
* ניסיון לצקת תוכן משמעותי להסמכ השל מושא המידע לשימוש במידע אודותיו
* תחולה פרסונאלית רחבה – אם חברה ישראלית ותנת שירות למישהו באירופה היא חשופה לסנקציות של ה הGDPR.
* מערך קנסות חסר תקדים בהיקף שלו יש מדרגים שונים להפרות שונות :
	+ במדרג הנמוך: עד 2% מהמחזור השנתי או 10 מיליון אירו לפי הגבוה מבין השניים – התמריץ של החברות לוודא שהן עומדות בהנחיות האלו הוא גבוה מאוד, והרגולטורים האירפואים הוכיחו את הנכונות שלהם להפעיל את הסנקציות של מי שמפר את ההוראות של הGDPR.
	+ במדרג הנמוך: עד4% מהמחזור השנתי או 20 מיליון אירו לפי הגבוה מבין השניים.

**הגדרת הGDPR למידע אישי – ס' 4(1)**

* **מידע אישי** = כל מידע שקשור לאדם מזווה או אדם שניתן לזיהוי.
* **ה**GDPR מתייחסת באופן מובהק לכך שלא ינקבו בשם של האדם, אלא ינו מידע יעזור לזהות את האדם. בין אם באופן ישיר או בלתי-ישיר (מידע שלא נוקב בשם האדם אבל מאפשר לזהותו) למשל: מס' זהות, כתובת IP , מזהה של טלפון נייד מידע ביומטרי, מידע מיקום. מידע בנוגע לזהות הפיזיולוגי, הגנטית, הנפשית, הכלכלית, התרבותית של אדם.

השאלה הלרוונטית היא לא האם המידע הזה מזהה אותי באופן ברור אלא אם ניתן לשחזר את המידע הזה ומתוכו את הזהות שלי.

חשוב לומר שגם אם מעבירים מידע אישי ש"הותמם" (עבר להיות אנונימי – ע"י הסרת הפרטים המזהים) גם הוא בכלל המידע אסור, אם סביר ששילובו עם מידע נוסף יביא לזיהויו של המושא המידע. אנחנו מטילים על כל החברות את ההגבלות – אין להבחין בין חברה מפותחת לזו שפחות . משום שכל חברה יכולה לשחזר ולעבד מידע באופן זהה באמצעות "מיקור חוץ" – רכישה של שירותי חברה אחרת שתעבד את המידע עבורה.

**גישה מרחיבה:**

הכרה ביכולת הצלבת נתונים שמתקבלים ממקורות מידע שונים באופן שמאפשר זיהוי של האדם וחשיפת מידע אישי אודותיו.

הגדרת הGDPR לעיבוד מידע (data processing) ס' 4(2)

כל עיבוד מידע, גםאם לא מתבצע באופן אוטומטי (באמצעי ממוחשב). הגדרה אחבה שכוללת איסוף, אחסנה, איחזור, הפצה, מחיקה , השמדה ועוד כי מדובר בניהול מידע באופן כללי ולא רק הגנה על המדיניות.

הGDPR עוסקות בכל הזכויות שקשורות במידע אישי, לא רק הגנת הפרטיות – ולכן למושא המידע יש את הזכות לקחת את המידע האישי שלי ולעשות איתו מה שאני רוצה. לדוג': זכות לניוד מידע – מושא מידע יכול לקבל מארגון א' קובץ עם המידע הישי שנאגר עליו ולהעבירו לארגון ב'. למה זה טוב?

ההבחנה בין processor ל- controller

Controller: גוף שמספק את מטרות עיבוד המידע והאמצעים לעיבוד המידע.

processor : מי שמספק בפועל את שירות עיבוד המידע

דוגמא: בנק שאוסף את ומעבד מידע בנוגע ללקוחות שמנהלים אצלו חשבונות:

* כשהבנק מעבד את המידע בעזרת מערכותיו הפנימיות, אז הוא משמש בשני הכובעים.
* כשהבנק מעבד את המידע בעזרת צד שלישי – הבנק הוא בעל השליטה במאגר והחברה החיצונית היא מעבדת המידע.

בפועל יש קצת יותר חובות לבעל השליטה במאגר, הניגוד להסדרים שונים שבהם חובות של מעבד המידע ביו רק חוזיות (הסדרים רגולטורים שקבעו בעל השליטה במידע הוא האחראי הבלעדי, ו וא חייב לאכוף על מעבד המידע את החובות שמוטלות עליו בנוגע לשליטה במידע). ואילו ה GDPRקובע כי לבעל השליטה במאגר צריך לאכוף בחוזה ולקבוע כי מעבד המידע שעובד תחתיו יצטרך לשמור על ההוראות בתקנות, אך בנוסף לכך – החברה שמעבדת את המידע חייבת ..(לבקש משני הילביץ).

דוגמא: מעבדת תרופות שוכרת את שירותיו של צד שלישי כדי לבצע ניסויים קליניים בחולים. במקרה הזה יש מעמד של שולטים כפולים, הם שניהם חייבין כבעלי שליטה במידע – כי הוא קיבל בחוזה (יש התקשרות ישירה) ממעבדת התרופות את המסכות לבצע ניסויים שבמסגרתם אוספים הרבה מידע, ומידע רגיש. (joint controller

אם למעבד המידע נמצא בקשר ישיר מול מושאי המידע, ולא רק מקבל מבעל השליטה ומעבד אותו, אז גם הוא עצמו הופך לבעל השליטה.

מתי עיבוד מידע ייחשב לחוקי לפי הGDPR?

1. מבוסס על הסכמה חופשית, מפורשת ובאופן ספציפי (מצטברות).
2. חיוני לביצוע חוזה שנכרת עם מושא המידע או לצורך כריתתו, למשל חוזה ביטוח, הצעה לחוזה ביטוח – צריך למסור הצהרה רפואית.
3. חיוני לקיום הוראות חוק – כדי לשמור על החוק אני צריך למסור מידע אישי למשל מס הכנסה.
4. חיוני לצורך אינטרס אישי של מושא המידע - (הגנה על החיים או שלמות הגוף) למשל – טיפול רפואי.
5. חיוני למטרה ציבורית - (המטרה צריכה להיות מעוגנת בדין) למשל – מחקר של המדינה.
6. חיוני לאינטרס לגיטימי של בעל השליטה או צד שלישי - לרבות אינטרסים מסחריים, אישיים או חברתיים, רק אם זכותו של מושא המידע להגנה על הפרטיות **לא גוברת** על האינטרס הלגיטימי. למשל, לצורך קבלת השקעה מקרן השקעות סינית היא רוצה לדעת איזה משתמש עושה שירות לחברה שלו. הרגולטור של הגנת הפרטיות הוא קבוע האם האינטרס הוא לגיטימי או לא.

תמיד מדובר באינטרסים המתנגשים עם הגנת הפרטיות של מושאי המידע אבל גם רוצים לקדם מטרות נוספות כמו סחר עם מדינות אחרות, פיתוח כלכלי.

דגשים:

הדרישה שהעיבוד יהיה חיוני= necessary, ולכן חוץ מהסכמה, אם יש אפשרות להשיג את המטרה ללא עיבוד מידע אישי זה לא חיוני ואז יאן בסיס חוקי לעיבוד המידע.

אם ניתן להשיג את אותה המטרה באופן סביר ללא ביצוע עיבוד מידע אישי => העיבוד אינו נחוץ ונשלל הבסיס החוקי לעיבוד המידע - רלוונטית לאפשרויות 2-6 הנ"ל (להוציא הסכמה)

יש לקבוע את הביססי החוקי לעיבוד המידע בכתב + להודיע עליו למושא המידע לפני תחילת עיבוד המידע. לא ניתן להשתמש במידע שהושג על יסוד בסיס חוקי אחד, כדי לבצע עיבוד של המידע על עיבוד בסיס חוקי אחר. צריך לדבוק באותו בסיס חוקי, ואם כן, יש להודיע עליו מחדש למושא המידע. הבסיס החוקי הוא חשוב. אם העילה שלי היא לצורך הוראה חוקית למושא המידע אין זכות לבקש את מחיקת המידע לעומת מקרה בו אני נותן הסכמה.

 > GDPR מנסה להתאים את מדיניות הגנת המידע למציאות שלנו. בגל ההיקף והקלות של הפקת המידע ואיסוף המידע של ימינו. וכן התפתחות טכנולוגית מבוססות מידע אישי (שירותי מחשוב ענן, שירותים מבוססי מיקום, רשתות חברתיות). ולכן הGDPR נכתב מתוך התפיסה שיש לנו כלכלת המידע שמובילה לכך שיש מידע השווה לנכס סחיר וגלובליות ושקיים מתח כחברה בין שגשוג כלכלי שיכול לנבוע מזה במקומות שניתן לקנות את הפרטיות שלנו במקום לוות רעליו תמורת שירות בחינם לצד סיכוני הפרטיות.

**שיעור 10 (עו"ד אורנן שטיינברג) - 4.6.18**

שוק התקשורת הוא שוק דינמי ועתיר פיתוחים ומגלגל כ-20 מיליארד ₪ בשנה. הוא עוסק בנושאים שמשפיעים על כלל הציבור: רפורמת הסלולר, דור חמש בסלולר, סיבים אופטיים, השוק הסיטונאי (תשתיות אינטרנט), תאגיד השידור הציבורי, פיצול ערוץ 2, נטפליקס וכו'.

**התחומים שמשרד התקשורת מתעסק בהם הם תחומי טלקום** (תקשורת נייחת, תקשורת ניידת, אינטרנט, כבל תת ימי, שיחות בינ"ל, לוויינים וכו'). משרד התקשורת לא מפקח יום יום על השידורים אלא **ברמת המאקרו, של מדיניות וחקיקת על.**

* ישנם תחומים שנראה שהם תחת משרד התקשורת, אבל לא. **משרד התקשורת הוא הצינור ולא מתעסק בתכנים.** עוד נושא תקשורתי שהמשרד לא מתעסק בו הוא קרינה סלולרית, שעל זה אמון המשרד להגנת הסביבה.

הלשכה המשפטית מצביעה על קשיים משפטיים במדיניות ובהחלטות של משרד התקשורת. בנוסף, היא "אורזת" את ההחלטה ב"חליפה" של כללי התנהגות, החלטות והצעות חוק מחייבות. לשם כך הלשכה המשפטית צריכה להיות מעורבת מתחילת התהליך, שלרוב מתנהל בצורת צוותי חשיבה. היא כם מלווה את המשרד בהליכים בערכאות כגון בג"ץ, ביהמ"ש לעניינים מנהליים וכו'.

המשרד מתעסק במשפט ציבורי, רגולציה, צרכנות ומשפט וטכנולוגיה.

הממשק בין משרד התקשורת לטכנולוגיה

כדי ששוק התקשורת בישראל יהיה השוק הטוב ביותר שיכול להיות, ישנם מספר עקרונות על:

1. סיפוק **שירותים מתקדמים.** שדרוג מתמיד של המערכות. מדובר במנוע עסקי שמשפיע על המשק כולו. סטארט-אפים, חינוך אונליין, רפואה מהירה - כולם מושפעים מאיכות השירותים הקיימים.
2. כדי שתהיה נגישות לציבור, השירותים הללו צריכים להינתן **במחיר סביר.**
3. **תחרות.** משרד התקשורת יוצר מגרש משחקים רב משתתפים.

משרד התקשורת עוסק בתקשורת וטכנולוגיה. המשפט תמיד מפגר אחרי הטכנולוגיה, וזה נכון גם לגבי המדינה ומשרד התקשורת באופן ספציפי. **טכנולוגיה מגיעה מתוך השוק, שנמצא עם היד על הדופק.** הרבה מהאנשים שמאיישים את המשרד לא מגיעים מתוך השוק ולכן נטולי ידע טכנולוגי מוקדם. גם מי שמגיע מחברות פרטיות מאבד את היתרון שלו אחרי כמה שנים, כי הטכנולוגיה משתכללת. דרך אחת להתמודד עם זה היא הבאת אנשים מהשוק הפרטי או לחלופין, שליחת עובדי המשרד להשתלמויות, כנסים ואירועים. **במשרד לא כופים טכנולוגיה חדשה אלא מעודדים אותה באמצעות השוק** (רק לעיתים רחוקות עושים שימוש בהוראות כופות).

כפי שנראה, היחס של משרד התקשורת לטכנולוגיה הוא מורכב. מצד אחד מעודדים טכנולוגיה חדשה, ומצד שני מתייחסים אליה בזהירות. **המשרד מהווה "שומר הסף"** וצריך לשקול סוגיות שונות ואתגרים שאותה טכנולוגיה מציפה.

מה הממשק של הלשכה המשפטית במשרד התקשורת עם הטכנולוגיה? ניסוחים של חוקים, למשל, יכולים להשפיע על סוג הטכנולוגיה. ישנן גם שאלות משפטיות שעוזרות למהנדסים לעצב את הטכנולוגיה. לפעמים דווקא המשפטנים מציעים את הפתרון "הטכנולוגי".

הממשק עם השוק אינו פשוט. **משרד המשפטים הוא הרגולטור, אבל הוא מעדיף לפעול בשיתוף פעולה עם השחקניות בשוק.** בשלב הראשון ישנו גיבוש רגולציה, ואז הממשק עם החברות נעשה באמצעות שיחות ודיונים כדי לקבל את חוות דעתן. כך ניתן להציף קשיים טכנולוגיים, כלכליים ומשפטיים. לפעמים נדרש מהחברות לספק מידע. כשהרגולציה מתגבשת המשפט המנהלי מחייב מתן אפשרות ערעור לחברות. בשלב השני כשכבר יש רגולציה, לפעמים חברות מבצעות הפרות שגוררות הטלת עיצומים כספיים גבוהים. לפעמים גם מגיעים לערכאות משפטיות בנושא.

* ישנו גם ממשק קטן עם הציבור - למשרד יש מחלקה של פניות ציבור. אם נעשה לאזרח "הקטן" עוול, הוא יכול לפנות למשרד התקשורת.

מקרי הבוחן:

1. **אינטרנט מהיר**

ה-ADSL החליף את טכנולוגיית ה-dial-up המיושנת. בזק וחברות הכבלים רצו לספק את השירות הזה ללקוחות בארץ. אולם, החוק הישראלי לא אפשר לחברות כבלים לעשות כן (הוט, למשל, הוקמה כחברת כבלים - וזה ממש לא מובן מאליו שכיום היא מספקת שירותים סלולריים ואינטרנט). עקרון החוקיות במשפט המנהלי אומר שהמדינה יכולה לעשות רק מה שקבוע בחוק שמותר לה לעשות, ולכן היא לא יכולה לתת רישיון אינטרנט לחברת כבלים. אין סמכות בחוק לעשות כן. איך מתגברים על זה? תיקון החוק, ובינתיים הוצע שבזק לבדה תספק את הטכנולוגיה הזו. הבעיה בכך היא שבזמן שיתקנו את החוק (לוקח זמן רב) בזק יהפכו למונופול בתחום, והחדירה של הוט לשוק תהפוך לקשה עד בלתי אפשרית. התחרות נפגעת.

לחלופין, אפשר להגיד שהשיפור בטווח הקצר הוא שירותים מתקדמים. ברגע שיש שני שחקנים (גם הוט וגם בזק), כל אחת תנסה להתחרות בשנייה כדי להגדיל את התחרות ביניהן. אם לא יאפשרו להוט לספק אינטרנט מהיר בזק תוכל לעשות מכה מבלי שיהיה לה תמריץ להשתדרג.

הפתרון הוא **מהלך מדורג.** נקפיא את כניסתה של הטכנולוגיה ובינתיים ננסה לחוקק כמה שיותר מהר חקיקה שתאפשר כניסה של שחקניות נוספות לשוק. אחרי זמן מה משרד התקשורת הבין שיש צורך לעשות איזון, כי השירותים המתקדמים נמנעו מהציבור יותר מדי זמן. אחרי כשנה וחצי אפשרו לבזק להיכנס לשוק האינטרנט המהיר (לפני חברת הכבלים).

1. **אוניברסליות**

בעבר עשו שימוש בכבלי נחושת שיכלו להעלות ולהוריד כ-150 מגה. כיום יש סיבים אופטיים שיכולים להעביר מידע על בסיס אור במהירות אדירה. אחד הדברים שמשרד התקשורת רוצה לעודד הוא הנחת סיבים אופטיים. עם זאת, משרד התקשורת רוצה גם לשמור על שוויון ולא להגיע למצב שבו ימנעו מלפרוס טכנולוגיות מתקדמות בפריפריה. נוצר מצב שצריך **לאזן בין השקעה בטכנולוגיות מתקדמות במיוחד לבין סיפוק שירותים לפריפריה.** החברות מעדיפות להשקיע בשירותים מתקדמים במרכז ולא בפריפריה.

דוגמה חריגה: ישנו יישוב בעמק המוות בנבאדה, ארה"ב. התשתיות שם איטיות מאוד כי הספקיות הגדולות לא רוצות להגיע לשם. אותו יישוב הפך לסיפור הצלחה כי היה שם מהלך גדול מאוד מבחינה פוליטית, כלכלית וטכנולוגית והצליחו להביא סיבים אופטיים לאותו יישוב.

**הפתרון היה להטיל חובת אוניברסליות של פריסת תשתיות, אבל לתת הקלות** (אפשרות לא להגיע ליישוב מסוים/להגיע במועד דחוי). זהו פתרון מאוזן. הקלות אלו נובעות מסיבות ביטחוניות, כשלים טכנולוגיים במקומות מסוימים, חלופות טכנולוגיות ואף שיקולי עלות-תועלת.

* על כל הקלה ביישוב אפשר לדרוש מהחברות לשפר את איכות השירותים שהיא מציעה.

ישנה ועדה שדנה באופן פרטני בכל יישוב. כיום בזק פרושה ב-98% מהיישובים והוט ב-92%.

בארה"ב אין חובת אוניברסליות וכל יישוב צריך לדאוג לעצמו אך ישנה קרן להשקעה בתשתיות).

1. **IOT**

המהפכה הטכנולוגית הראשונה הייתה באמצע המאה ה-18, עם מעבר לפעולות ממוכנות (באמצעות מים וקיטור). המהפכה הטכנולוגית השנייה באמצע המאה ה-19 הייתה החשמל, שכללה את הנורה והטלגרף. המהפכה השלישית הייתה מהפיכת המחשוב. המהפכה הרביעית היא מהפיכת ה-IOT (Internet of Things). **שילוב בין הפיזי לדיגיטלי** (כמו בית חכם), ניסיון לייעל ולהפוך את החיים לנוחים יותר למשתמש. היום ישנם כ-8 מיליארד מכשירי IOT בעולם.

דוגמאות ליישום של ה-IOT:

* באנגליה ישנן תשתיות חכמות. מד אנרגיה של גז או חשמל שנותן מידע אונליין של מה שקורה בבית, הן לצרכן והן לחברה - באופן שמייעל את הצריכה.
* תעשייה חכמה (B2B, Business to Business). מכונית שיוצאת ממפעל חכם יכולה לשדר למפעל שיש בה פגם והוא מתקן בפס הייצור את הפגם באופן אוטומטי.

אלו אתגרים דבר כזה יכול להעלות? פריצות של האקרים; פגיעה בפרטיות; אחריות משפטית (מי אחראי על תאונת דרכים שמבצע רכב חכם?); עומס על תשתיות; מיסוי וכו'.

1. **ניטרליות רשת**

לא הספקנו לעסוק בזה בהרחבה. בישראל יש ניטרליות רשת - לחברות התקשורת (ספקיות השירות) לא יכולות להעדיף תעבורה לאתרים מסוימים או להגביל משתמשים מסוימים. כולם שוויום בפני החוק. לספקיות יש אינטרס שלא לשמר את עקרון הניטרליות כי הן יכולות למכור בכסף העדפה של תעבורה. למשל, מאקו היו יכולים לקנות הסדר העדפה עם ספקיות האינטרנט.

פגיעה בניטרליות הרשת מהווה התערבות בשוק - אם המחוקק היה קובע טכנולוגיה מסוימת על פני אחרת, הוא היה דה פקטו מעניק לה העדפה. אסור להגביל תכנים (לקרוא מאמר מהסילבוס).

* לסיכום, צריך להתחשב במגוון שיקולים כשמכניסים טכנולוגיות חדשות לשוק בישראל.

**שיעור 11 (עובד מסיכומים של שיר ואור) - 11.6.18**

חובת הסודיות ואבטחת המידע

דיברנו על כך שמנהלי מאגר מידע ובעל מאגר מידע צריכים לשמור על פרטיות המידע שבמאגר גם כלפי פנים וגם כלפי חוץ (מצדדים שלישיים).

תקנות הגנת הפרטיות (אבטחת מידע) משנת 2017 החליפו את תקנות הגנת הפרטיות משנת 1986, ומפרטות את אופן יישומה של החובה לסודיות ואבטחת המידע. תקנות אלו עומדות מול אתגר – אנו לא יודעים הרבה על מאגרי מידע, כי יש כל כך הרבה סוגים של מאגרים וגופים שמנהלים אותם, למטרות שונים, עם סוגי מידע שונים וכו'. למרות השוני ביניהם, ישנו צורך להגדיר **רף מינימום או סטנדרט פעולה שמנהלי מאגרי המידע צריכים לעמוד בו** כדי להגן על פרטיות מושאי המידע. נידרש לדעת למבחן את עקרון ההבחנה בין מאגרים ומדוע הוא נעשה.

התקנות מסדירות את חובת אבטחת המידע בשלושה רבדים:

1. בעל מאגר המידע נדרש לקבוע איזה מידע מוגן יש במאגר ומה הסיכונים הקשורים אליו.
2. בעל מאגר המידע נדרש לקבוע נהלי עבודה מפורטים וברורים לאבטחת המידע.
3. בעל המידע נדרש לקבוע מה יהיו ההוראות המהותיות בניהול אירוע אבטחת מידע.

התפיסה שמשתקפת בתקנות הינה מודולרית - לא כל מאגרי המידע זהים, ולכן נחיל חובות ברמה הולכת וגוברת ככל **שפעילות עיבוד המידע במאגר** (כמות האנשים שנכללים במאגר) **משמעותית יותר,** ככל שמדובר **במידע רגיש יותר** וככל שיש **יותר אנשים בארגון שחשופים למידע.**

הרעיון הוא הפחתת הסיכון לפגיעה בפרטיות, ואם תהיה פגיעה בפרטיות ידעו כיצד להתמודד ולצמצם אותה. הגורם שאמון על הנושא הוא הרשות להגנת הפרטיות במשרד המשפטים.

התקנות קובעות הסדרים ביחס לארבעה סוגים של מאגרי מידע/קטגוריות מדורגות של חובות

מרבית החובות חלות גם על בעל המאגר וגם על מנהל המאגר (למשל, בעל עסק שמשתמש בשירותי "ענן" לצורך שימור מידע).

ס' 21 קובע אילו חובות יחולו על כל סוג מאגר, ומעניק לרשם מאגרי המידע סמכויות המאפשרות גמישות בהחלת החובות:

1. החרגה מתחולת התקנות (או חיוב בתחולת התקנות) באופן מלא או חלקי של מאגרים מסוימים, בהתחשב **בגודל המאגר,** **סוג המידע שנמצא בו, היקף פעילות המאגר** או **מספר בעלי ההרשאות בו.**
2. לקבוע שמי שעומד בהוראות רגולציה אחרת יראו אותו כעומד בתקנות כולן או חלקן.

התקנות משקפות עקרון של ניטרליות טכנולוגית: דינמיות ומניעת פגיעה בתחרות. לא כתוב כיצד ליישם כל אחת מהוראות החוק.

1. מאגר מידע המנוהל ע"י יחיד

מאגר המנוהל ע"י יחיד (יכול להיות גם תאגיד בבעלות יחיד), כאשר הגישה למידע שבמאגר הינה בעלים ולכל היותר שני מורשי גישה נוספים. לרוב מדובר בבעלי עסקים קטנים עם מאגר לקוחות מצומצם (כמו קוסמטיקאית או חנות שכונתית). על מאגר זה מוטלות החובות הכי מצומצמות:

1. **הכנת מסמך הגדרות המאגר -** חיוב שחל על כל בעלי המאגרים מכוח התקנות. מחייב את בעל המאגר לחשוב על מה שיש לו במאגר ובהתאם לכך להיערך מראש לסיכונים של פגיעה בפרטיות; מטרות ואופן האיסוף, השימוש והעיבוד של המידע וכו'.

גם כאן מופעל שיקול דעת - גם אם פסיכיאטרית עומדת בתנאים של מאגר יחיד, לפי תכליות החוק יחולו עליה חובות מוגברים יותר עקב טבעו הרגיש של המידע שברשותה. עוד נקודה חשובה: **אם יש מידע במאגר על יותר מ-10,000 אנשים, גם אם יש גישה לאדם אחד - לא נכלול זאת תחת מאגר יחי**ד (אלא בסיסי).

1. אבטחה פיזית
2. ניהול הרשאות הגישה והיקפן
3. תיעוד אירועי אבטחה
4. הגבלת שימוש בהתקנים ניידים
5. הפרדת מערכות ושימוש בתקשורת מאובטחת
6. מאגרים שחלה עליהם רמת אבטחה בסיסית

מוגדרים על דרך השלילה – אלו מאגרים שאינם מנוהלים על ידי יחיד ואינם מאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה.

1. מאגרים שחלה עליהם רמת אבטחה בינונית

כל אחד מהמאגרים הבאים, שיש להם לפחות 10 מורשי גישה (לפי הרציונלים והסיכונים שבחשיפת מידע, ככל שיש יותר מורשי גישה הסיכון גובר):

* מטרתם הינה איסוף מידע לצורף מסירתו לאחר (עסק ממש)
* או שהם בבעלות גוף ציבורי עם הפניה לגופים ציבוריים
* או מכילים מידע רגיש, כמו מידע ביחס למצב רפואי, נפשי, גנטי, ביומטרי על האדם, או לגבי דעותיו הפוליטיות, אמונותיו, רישום פלילי, מצב כלכלי וכו'.

כאן רואים תפיסה מתקדמת יותר שמשקפת תובנות שהשפיעו על עיצוב ה-GDPR, ניצנים של תפיסת החיבוריות (היכולת לבנות פרופיל של אדם מתוך מאגרים נוספים כמו הרגלי צריכה).

1. מאגרים שחלה עליהם רמת אבטחה גבוהה:

יש בהם מידע על אודות לפחות 100 אלף איש או שמספר מורשי הגישה למידע עולה על 100, וכן:

* מטרתם איסוף מידע לצורך מסירתו לאחר
* יש בהם מידע רגיש במתואר לעיל

מה שמבחין בין הרמה הבינונית לגבוהה הינה מספר האנשים במאגר/מספר מורשי הגישה.

החובות המוטלות על שלושת סוגי המאגר האחרונים גבוהים יותר ככל שרמת הסיכון עולה. הדרישות מפורטות בתקנות, וישנן דרישות שעלותן ומורכבותן גבוהה יותר (כגון ביצוע סקר סיכונים, אבטחת תקשורת מחמירה, הפרדת מאגרים, הפרדה בין מערכות מחשוב וכו').

מה מושאי המידע יכולים לעשות?

למושא המידע מוקנות כל מני זכויות, כאשר ההנחה היא שלמושא המידע יש זכות במידע עליו.

* ס' 13 מעניק זכות עיון במידע. הבעיה היא שלא הרבה אנשים יודעים שזכות זו קיימת (חובת ההודעה של בעל המאגר לא כולל הודעה בדבר הזכויות שיש למושא המידע).
* ס' 14 מעניק זכות לדרוש תיקון של המידע (אם נמצא לא נכון, שלם או מעודכן). נדרשת הסכמה של בעל מאגר המידע לבקשה. אם סירב, קמה עילה לתובענה בביהמ"ש (ס' 15).
* פגיעה בפרטיות יכולה להקים עוולה אזרחית (ס' 4) ואם נעשתה במזיד להוות יסוד לעבירה פלילית (ס' 5).
* ס' 31 קובע עוולה נזיקית - למשל, אם מנהל המאגר התרשל בחובתו לאבטח את המידע. הקושי בסעיף הוא הצורך להוכיח נזק כדי לקבל פיצוי.

הזכות להישכח - מידע אישי דיגיטלי לאחר המוות

מה קורה עם שובל המידע הדיגיטלי שאנו משאירים אחרינו לאחר מותנו?

המחוקק הישראלי טרם הכריע בשאלה כיצד לסווג מידע אישי דיגיטלי שנותן לאחר המוות (האם קניין במידע, שעובר בירושה? או זכות לפרטיות שנותרת עם המוות? או זכות חוזית שניתן להתנות עליה?). מה ששולט כיום הינם תנאי השימוש והסדרים שונים שפלטפורמות מציעות למשתמשים שלהן.

לאחר מותנו אנו מותרים עקבות דיגיטליים שונים – תכנים שיצרנו ברשת וחשבונות אישיים. נשאלת השאלה מי יכול לראות את מה שהעלנו ולשלוט במידע הזה? מהם השיקולים שראוי לקחת בחשבון בעת עיצוב המדיניות המתאימה להסדרת הסוגיה? זוהי שאלה מורכבת ותלויות פלטפורמה ומידע.

כפי שמסתמן במחקר של בירנהיים, למשתמשים יש רצונות שונים (חלקם רוצים לעשות דברים עם המידע שלהם לאחר מותם).

התנגשות בין זכויות ואינטרסים במידע לאחר המוות

* זכויות קניין במידע (זכויות יוצרים, מידע כקניין בר הורשה).
* הזכות לפרטיות כזכות אישית שפוקעת עם המוות.
* אינטרסים של בני משפחה וחברים (גישה/שליטה במידע על המנוח לצורכי הנצחה ואבל).
* זכות לפרטיות של משתמשים חיים שהיו בקשר עם המנוח.
* חובת סודיות של מי שהעניק למנוח שירותים רפואיים, פסיכולוגיים או משפטיים.
* אינטרסים עסקיים של ספקי שירות, שבפועל כיום מכתיבים את גורל המידע והתכנים של המשתמשים שמתו (מדיניות הספקיות, גורמי הביניים ברשת וכו').

הטכנולוגיה מאפשרת דרכים חדשות להתמודד עם האובדן (מרחבי התאבלות וירטואליים, הנצחה ותיעוד). עם זאת, היא מעלה שאלות מאוד מאתגרות ביחס לשליטה במידע והיכולת לעצב את הזיכרון - איזו דמות נותרת מאחור? עד כמה לאדם יש שליטה על הזיכרון שנותר ממנו?

למידע הדיגיטלי יש מאפיינים ייחודיים שמעוררים שאלות לגבי היכולת להחיל מסגרות משפטיות קיימות (שעוצבו עבור סביבה לא דיגיטלית).

המאפיינים הייחודיים של זיכרונות דיגיטליים

* המידע הדיגיטלי אינו מתכלה
* ניתן לעיבוד בקלות
* כולל תוכן וסוגים נוספים של מידע (META DATA)
* שאלות שלא היו קיימות בעבר בנוגע לשליטה האפקטיבית במידע. אם בעבר שליטה במידע הייתה כרוכה בגישה פיזית אליו, ולרוב הייתה נתונה בידי הקרובים למנוח – בזירה הדיגיטלית ישנם גורמים נוספים (גורמי ביניים כמו ספקי שירות) שמחזיקים במידע ושולטים בו באופן אפקטיבי.

פתרונות טכנולוגיים לניהול מידע אישי לאחר המוות

**רוב ספקי השירותים לא הסדירו את הנושא ואין להם פתרון** (אולי ס' בתנאי השירות אבל לא כלי של ממש בידי המשתמשים לעיצוב המידע שלאחר המוות).

* פייסבוק מאפשרת למשתמשים לקבוע האם חשבונם ייסגר או יהפוך לחשבון הנצחה שבו תינתן גישה למידע ולביצוע פעולות לגורם מסוים, ה-LEGACY CONTACT.
* גוגל מציעה כלי בשם GOOGLE INACTIVE ACCOUNT MANAGER. משתמש יכול לקבוע מה יקרה לחשבונותיו לאחר תקופת אי פעילות שהגדיר מראש – האם ייסגרו או שתינתן גישה לגורמים ספציפיים שיקבע מראש. יש לכך היבטים פיננסיים – בני משפחתו של המנוח יכולים לבקש לסגור את החשבון, לקבל כספים שמוחזקים בגוגל וכן לקבל נתונים מהחשבונות.

**שיעור 12 - 18.6.18**

**שירותים משפטיים מקוונים**

האפשרות לספק חלק מהשירותים המשפטיים באופן מקוון מעוררת שאלות לגבי השוק המשפטי ככלל ומקצוע עריכת הדין וייחודיותו בפרט. זוהי התפתחות מעניינת מבחינת המודל של לסיג.

מתן שירות משפטי באופן מקוון

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

יכולה להיות העברה לסביבה מקוונת (אותה עבודה אבל בסקייפ); עיצוב/הבנייה מחדש (אבחון אוטומטי, הדרכה משפטית אוטומטית למי שממלא טופס).

טפסים משפטיים מקוונים

1. הבסיס: טפסים סטנדרטיים (תבנית קבועה מראש, המשתמש ממלא בעצמו את הנתונים אשר נשתלים במסמך).
2. טפסים מותאמים אישית (התוכנה מייצרת מסמך מותאם אישית לפי מידע והנחיות שהמשתמש מספק; כל משתמש מקבל מסמך עם תוכן ומבנה שהותאמו למידע שסיפק).
3. "ממשקים חכמים" (שילוב עיבוד טקסט ושפה טבעית, AI, למידת מכונה)
4. אופני תקשורת שונים (טופס-טקסט סטטי, ממשק צ'ט-בוט, הנחיות קוליות).

ישנו מגוון רב של פעולות משפטיות שניתן לבצע באמצעות היישום הללו: חוזים שונים (הסכמי שכירות, מכר, שימוש בנכס); ייפויי כוח; צוואות; הסכמי עבודה, גירושין; מסמכי התאגדות חברה, שותפות, עמותה; רישום פטנטים, סימן מסחר, זכויות יוצרים; הסכמי סודיות, אי-תחרות, שירותים; הגשת מסמכים לבתי משפט ולרשויות בקשה לשינוי דמי מזונות, פש"ר.

דוגמאות:

* חברת Legalzoom מציעה מגוון שירותים משפטיים מקוונים כגון עריכת צוואה תמורת 369-69$, רישום חברה וכו'.
* חברת Wevorce עוזרת לערוך הסכם גירושין באמצעות שילוב של טכנולוגיה ותפיסה של גירושין בהסכמה (תמחור של 900-300$).
* תוכנת Access to Justice Author משמשת גורמים בעלי ידע משפטי (כמו סטודנטים) כדי לייצר שאלונים משפטיים מקוונים לאבחון ואיסוף מידע והפקת מסמכים רשמיים.

כיצד הממשק המקוון עשוי להשפיע על "בחירות משפטיות" (תהליכיות ומהותיות) של משתמשים?

האם אנשים היו מקבלים החלטה אחרת לו היו מבצעים את הפעולות באופן לא מקוון? האם סביבת קבלת ההחלטות משפיעה על ההחלטות שמתקבלות?

* הינד: קבלת ההחלטות של משתמשים מושפעות מהאופן שבו הבחירות מוצגות. התוכן וההצגה החזותית מפעילים הטיות קוגניטיביות.

בסביבה הדיגיטלית התוכן ואופן ההצגה החזותית משפיעים על קבלת ההחלטות של אנשים, ויש חשיבות לעיצוב ממשק המשתמש (אפשרויות ברירת המחדל; סדר הצגה; מילוי ערך עצמאי וכו').

עו"ד צ'ט בוט – ROBOLAWYER

1. חוויית משתמש של שיחה אינטראקטיבית
2. עיבוד שפה טבעית
3. התאמה של מסמכים
4. הגשה מקוונת לרשות

שימוש בטכנולוגיה לצורך גילוי מסמכים מוקדם (e-discovery)

בעידן הדיגיטלי כמות המסמכים גדלה (paper trail) ואיתה שעות האדם הדרושות כדי להעריך את הרלוונטיות של כל מסמך להתדיינות המשפטית. לפיכך חברות שונות פתחו מערכות אלגוריתמים ייעודיות שתוכנתו לבצע את הסריקה עבור עורכי הדין. הן מחקות את תהליך האיתור והמיון שמבצע אדם בעל הכשרה בתחום (למידת מכונה). התוצר הינו ניבוי בדרגת ודאות גבוהה יחסית אם מסמך כלשהו רלוונטי להליך ספציפי.

ההשלכות על עבודת עו"ד

**טפסים משפטיים -**

* שימוש נפוץ, חתך נתח מסוים מעבודת עורכי הדין
* מודלים משולבים: קיטוע/תיחום של עבודת עוה"ד באופן משלים

**תוכנות e-discovery הן אמצעי מקובל ונפוץ שהתקבל כלגיטימי בבתי המשפט -**

* תחילה: שימוש בתוך משרד עו"ד = עבודת מזכירות משפטיות, מתמחים ועו"ד צעירים.
* בהמשך: קמו חברות שהתמקצעו בתחום, שכללו את המודלים ומציעות שירותים למשרדי עו"ד במודל של מיקור חוץ.

**תוכנות הערכת מסמכים -**

* קפיצת מדרגה טכנולוגית בשנה האחרונה.

כרגע מדובר בעיקר בתוכנות שמשמשות ככלי עזר לעורכי דין ולא באמת מהוות תחליף (עדיין...).

דוגמאות למערכות תומכות החלטה: חישוב פיצויים; חישוב גזרי דין; חישוב סיכויי תביעה; חישוב סכומי פשרה; סטטיסטיקה תיאורית של הליכים, שופטים ועורכי דין (ניתן להכניס שם של שופט ולקבל תובנות על סמך המערכת ותיקי עבר). כלים שתומכים בהחלטת עו"ד בייצוג הלקוח.

קשיים בפיתוח מיזמים משפטיים טכנולוגיים

1. **כללי ההסדרה המקצועיים של עורכי דין**
* חוק לשכת עורכי הדין תשכ"א-1961
* כללי לשכת עורכי הדין (אתיקה מקצועית) התשמ"ו-1986

הנורמות האתיות והמקצועיות התפתחו והתקבעו בעידן שבו הטכנולוגיות הנוכחיות לא היו קיימות, וכך גם לא היישומים שלהן בתחום המשפט.

1. **ייחוד פעולות המקצוע (ס' 20 לחוק לשכת עוה"ד)**
* עריכת מסמכים בעלי אופי משפטי/ייעוץ וחיווי דעת משפטיים מותרים רק למורשים

עורכי הדין קיבלו אוטונומיה מהמחוקק - זוהי גילדה זקוקה שהכניסה אליה הינה רק באמצעות רישיון מקצועי, שמתקבל ע"י מעבר בחינות לשכת עורכי הדין. תמורת הכפפת עורכי הדין להסדרה ולמחויבויות אתיות ומקצועיות משמעותיות עורכי הדין קיבלו הגנה בדמות "ייחוד המקצוע", פעולות שמותרות רק לעורכי דין ואנשים אחרים לא יכולים לבצע. הנורמות והכללים הללו נקבעו הרבה לפני עידן הטכנולוגיות המשפטיות.

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

שירותים משפטיים מקוונים: הסגת גבול המקצוע?

מתן מידע משפטי באמצעות אתר מקוון אינו אסור כשלעצמו. לעומת זאת, ייעוץ משפטי או מתן חוו"ד משפטי ע"י מי שאינו עו"ד אסורים.

* ככל שהמידע **כללי** יותר ואינו מתייחס למקרה העובדתי והקונקרטי - הוא מידע.
* ככל שהמידע נשען על **נסיבותיו הפרטניות** של הפונה - ייעוץ.

בנוסף יש לבחון **האם המידע/השירות/הייצוג בנסיבות המקרה הם משפטיים**.

אמות המידה לכך נקבעו בפס"ד המרכז למימוש זכויות רפואיות נ' לשכת עורכי הדין - לא ניתן להגדיר מראש באופן ממצה את המונחים הכלולים בס' 20 ("ייצוג", "אופי משפטי" וכו'), ההגדרה טעונת פרשנות. **תכלית הסעיף היא להבטיח שלא ייגרם לציבור נזק כתוצאה משירות משפטי לקוי** (רק בעלי הידע המתאים יעניקו שירות). השופטת ארבל קובעת את אמות המידה הבאות שלפיהן נכריע אם פעולה/שירות הוא ייחודי למקצוע עורך הדין:

1. **היקף שיקול הדעת הכרוך בביצוע השירות או הפעולה הניתנים לציבור**
* האם השירות/הפעולה כרוכים בהפעלת שיקול דעת רחב, תוך שקלול של משתנים רבים או שמא מדובר בפעולה טכנית בעיקרה, שאינה מצריכה בחירה בין דרכי פעולה רבות?
1. **פוטנציאל הנזק לציבור עקב שירות לקוי**
* ככל שהפוטנציאל משמעותי יותר והנזק בלתי הפיך השירות יוקצה לעורכי דין בלבד
1. **החלופה העומדת לציבור במימוש זכויות, אם ייאסר מתן השירות ע"י מי שאינו עו"ד** (בשים לב למחיר)

היא מציינת בשולי פסק הדין כי במבט צופה פני עתיד, ייתכן ששירותים משפטיים מסוימים ונקודתיים יסופקו לציבור הרחב אף ע"י מי שאינם עורכי דין. לשם כך יהיה בצורך **בהסדרה של גופים אלו באמצעות מנגנוני פיקוח ובקרה** (שיבטיחו כי השירות יינתן לאחר הכשרה מתאימה ובכפוף לכללי התנהגות מחייבים). מלאכת יצירת ההסדרים נתונה למחוקק.

בפס"ד דטהפקס הייתה חברה שהפנתה לקוחות למאמרים ודפי מידע בנושאים רלוונטיים לבעיות שלהם. לשכת עורכי הדין תבעה אותם בטענה ש"עובדים עלומים" נטולי הכשרה מבצעים את ההפניה ללא הכשרה מתאימה. ביהמ"ש השתמש באמות המידה שנקבעו בפס"ד של השופטת ארבל, וקבע כי ההפניה למאמרים, שאולי לא מכונה ייעוץ משפטי, מהווה ייעוץ משפטי בפועל. נציגי החברה נדרים להתאים את המאמרים ללקוחות, ועצם ההתאמה מצריכה ידע משפטי רב כך שיתאים מקרה הספציפי. על כן נאסר על חברת דטהפקס לספק את השירות הזה ללקוחותיה.

מה היה קורה לו השירות היה מבוצע ע"י אלגוריתם, ולא עובד רנדומלי? כרגע זו שאלה תיאורטית לחלוטין, שכנראה נידרש לה בעתיד עם התקדמות הטכנולוגיה.

המבחן ידרוש להכיר את הנושאים שלמדנו עליהם בקורס וגם להסתכל בראייה רוחבית על הנושאים ששבו ועלו כתמות במהלך הקורס (למשל, איך מסתכלים על סוגיות בראי המודל של לסיג? איך עיצוב המשטר המשפטי/כוחות השוק השפיעו על סוגיה? נורמות חברתיות?). אפשר לקחת סוגיה כמו הגנת הפרטיות ואכיפת זכויות יוצרים ע"י גורמי ביניים ברשת ולנתח אותה.

חומרי הקריאה רלוונטיים למבחן, ובמיוחד מהרצאות האורח. מומלץ להסתכל בשיעור בנושא הגנת הסייבר (**מהי תפיסת הגנת הסייבר בישראל** כפי שהיא משתקפת בהחלטות הממשלה ובמסמך ה-CERT? אילו הסדרים ספציפיים קובעות תקנות ה-GDPR ביחס לחובות ולזכויות של מי ששולטים במידע או מעבדים אותו, וכן של מושאי המידע? להכיר את **מהות ההסדרים** כגון זכות העיון והתיקון). המקורות מהשיעור של אורנן, בעיקר המאמר של **ניטרליות רשת.** שאר החומרים לא מחייבים מעבר למה שדובר בכיתה.

המודל של לסיג מספק **מסגרת לניתוח והבנה של מערך הכוחות שמשפיעים על התנהגויות בסביבה טכנולוגית.** במרכזו של המודל נמצאת פעילות אנושית שאותה מעוניינים לבחון, והמודל מצביע על ארבעה גורמים שמשפיעים עליה: המשפט, השוק, הנורמות החברתיות והטכנולוגיה.

לפיכך, כאשר נבחן מה משפיע על/מסדיר פעילות נתונה, לצד הבחינה המובנת מאליה של המסגרת המשפטית נבחן כיצד שיקולים כלכליים, מסחריים ושוקיים (כמו מחיר או תחרותיות) משפיעים עליה ועל אפשרויות האסדרה שלה (כיצד הם מגבילים/מאפשרים/מעודדים/מעצבים את ההתנהגות). בדומה לכך נבחן כיצד המאפיינים הטכנולוגיים של אותה פעילות וכלים טכנולוגיים קיימים משפיעים עליה, ואיזה תפקיד הנורמות החברתיות (תפיסות לגבי מה שמקובל, ראוי או רצוי) משפיעות על התנהגותם בפועל של השחקנים. המשמעות היא **שבעיצוב המדיניות ביחס להתנהגויות בסביבה טכנולוגית יש בידינו מגוון כלים שצריך לקחת את השפעתם בחשבון.**

במקרים מסוימים הטכנולוגיה והשוק יהיו הראשונים להציע פתרון מעשי (עוד לפני הסדרה משפטית ישירה), ולעיתים, **במקרים שבהם ידו של המשפט קצרה מלהושיע - גורמי האסדרה העיקריים יהיו הנורמות החברתיות, הטכנולוגיה והשוק.** כיוון שהשוק והטכנולוגיה אינם ניטרליים בפעולתם, קיימת חשיבות עליונה לבחינת השפעתם על אסדרת פעילויות בסביבה טכנולוגית. בנוסף, יש להביא בחשבון **שבין ארבעת הגורמים מתקיימים קשרי גומלין של השפעה הדדית.**

למשל, על אף שקיים חוק האוסר על הצגת תכנים פורנוגרפיים לילדים, אפשרויות צריכתם ברשת מקשה על אכיפה אפקטיבית של הפתרון המשפטי. בתוך החלל הזה פועלות נורמות חברתיות (כמו חינוך), טכנולוגיות שונות (כמו חסימת תכנים) ופתרונות שוקיים (תמריצים כלכליים לספקיות תוכן וטכנולוגיה להציע שירותים רלוונטיים). כמובן שדרישות השוק והמענה להן מושפעים מהנורמות החברתיות, הרלוונטיות של פתרונות אסדרה מושפעת מעלותם ויעילותם, וזו מושפעת בתורה גם מהטכנולוגיה שמבצעת בפועל וכן הלאה. כלומר, יש חשיבות גם לבחינת קשרי הגומלין בין ארבעת הגורמים. זוהי נקודה שאלקין קורן ובינהק מדגישים, אך היא אינה מייתרת את המודל של לסיג אלא **מרחיבה את האפשרויות של יישומו.**