משפט וטכנולוגיה – אור כהן – מחברת מקוצרת

[**מבוא** 2](#_Toc518787746)

**[יישוב סכסוכים בעידן הדיגיטלי: ממסחר מקוון לבתי המשפט](#_Toc518787747)** [2](#_Toc518787747)

**[רפורמת ההליכים האזרחיים באנגליה – ביהמ"ש המקוון של הלורד בריגס](#_Toc518787748)** [3](#_Toc518787748)

[**מבוא למתווכים ברשת** 4](#_Toc518787749)

[**הרצאת אורח – מערך הסייבר הלאומי – עמית אשכנזי** 5](#_Toc518787750)

[**זכויות יוצרים ברשת האינטרנט: אסדרה באמצעות גורמי הביניים ושימוש באכיפה טכנולוגית** 6](#_Toc518787751)

[**אכיפה באמצעות גורמי הביניים – המקרה של סעדים טכנולוגיים** 8](#_Toc518787752)

[**פרטיות בעידן הדיגיטלי - מבוא** 9](#_Toc518787753)

[**רגולציית הגנת המידע באירופה GDPR – חיים רביה – מהפכת הפרטיות באירופה** 10](#_Toc518787754)

[**הגנת הפרטיות בעידן הדיגיטלי בישראל** 11](#_Toc518787756)

[**החובות המוטלות על מנהל המאגר** 12](#_Toc518787757)

[**הרצאת אורח – ההיבטים הרגולטורים של שוק התקשורת** 12](#_Toc518787758)

[**חובות הסודיות ואבטחת המידע** 13](#_Toc518787759)

[**הזכות להישכח – מה קורה עם המידע האישי הדיגיטלי שלנו לאחר המוות** 14](#_Toc518787760)

[**שירותים משפטיים מקוונים** 15](#_Toc518787761)

**מבוא**

**המודל של לורנס לסיג: Code is Law**

המודל שלו מניח כי כל פעילות אנושית שאנו מעוניינים להסדיר, פועלות עליה 4 מערכות שונות של הסדרה, שיש להן השפעה באופן ישיר, ומידת ההשפעה יכולה להשתנות בכל הקשר, והן קובעות את מה שמותר ואסור, מקובל ולא מקובל ביחס לאותה פעילות אנושית.

1. **מערכת המשפט**
2. **כוחות השוק**
3. **נורמות חברתיות**
4. **הטכנולוגיה עצמה (Code)**

המשמעות של הפעולה המרובעת הזאת על הפעילות האנושית – **מי שרוצה להסדיר ולעצב את המדיניות האנושית – יש לו סל כלים עשיר.**

**המודל של ניבה-אלקין קורן ומיכאל בירנהק**

**גישה מהותנית** – הקשר בין משפט וטכנולוגיה. הטכנולוגיה עצמה, העיצוב שלה והתמלולים שעומדים בבסיסה הם לא ניטרליים. הטכנולוגיה מגלמת בחירות ערכיות נורמטיביות של המתכננים שלה. יש לה השפעה ממשית (גם אם בלתי צפויה).

**יישוב סכסוכים בעידן הדיגיטלי: ממסחר מקוון לבתי המשפט**

**Colin**: המנהל המייסד של פלטפורמת יישוב הסכסוכים באיביי. הבעיה - הפניה לבית משפט/מגשר/בורר זה לא ישים.

**Michael**: שופט בבית המשפט העליון באנגליה, מופקד על הרפורמה ומערכת המשפט האזרחי באנגליה. בשנת 2016 הוא הוציא את **דו"ח בריגס** (על שמו) שבעצם, ההמלצה המהפכנית ביותר שלו, היא להקים הליכים מקוונים עבור תיקים מקוונים במערכת בתי המשפט באנגליה. **הביקורת הגדולה של מערכת המשפט היא ביקורת על הנגישות שלה.**

**הרקע להתפתחות תחום יישוב הסכסוכים באופן מקוון (ODR)**

* **העידן הדיגיטלי**
* **תנועת הנגישות לצדק ותנועת ה-ADR (דרכים חלופיות ליישוב סכסוכים)**

**מאפיינים שמשפיעים/מתארים מערכות ODR**

* חשיבות רבה להקשר של הסכסוך, לתהליך ולסוג הטכנולוגיה.

|  |  |  |  |
| --- | --- | --- | --- |
|  | גבול תחתון | 🡨--------------------🡪 | גבול עליון |
| סכסוך | מסחר מקוון, משפחה, עבודה, עסקי | מורכבות | היכן נולד |
| תהליך | שיטת יישוב הסכסוך | עושר הערוץ התקשורתי | סינכרוניות, אוטונומיות |
| הקשר | פרטי או ציבורי | מדינתי או בינ"ל | ספק שירות – עצמאי, מתווך, מוסדי |

* המוקד שלנו: השפעת הטכנולוגיה על ההליך.

**מערכת הODR כצד רביעי וכצד שלישי בסכסוך**

**תפקיד אינסטרומנטלי** – **מערכת ODR כצד הרביעי בלבד** – מופעלת על ידי אדם

**תפקיד אוטונומי** – **הצד הרביעי + הצד השלישי** – המערכת המקוונת מפעילה בעצמה את הליך יישוב הסכסוך ללא צורך במעורבות של צד שלישי אנושי.

**מודלים טכנולוגיים בהליכי יישוב סכסוכים (מהמאמר)**

* **העברתה לסביבה מקוונת**
* **עיצוב מחדש (תפישה צרכנית)**
* **חווית משתמש מותאמת**
* **חידוש**
* **הליכים היברידיים שמשלבים בין השיטות**.

**מערכת ישוב הסכסוכים של איביי**

**איביי** – פיתחה את המערכת הODR (Online Dispute Resolution). **קולין רול** תכנן את המערכת המקורית שלאיביי.

**הסיבה לפיתוח המערכת –**

* יש לנו כמות מאוד גדולה של סכסוכים (60 מיליון), ושווי ממוצע נמוך של עסקאות (100 דולר).
* יחס עלות תועלת של פתרון על ידי מגשר בורר אנושי – בלתי סביר כלכלית.
* ריחוק פיזי בין מוכרים לקונים: קושי מעשי + ספק לגבי סמכות שיפוט.
* צורך בהבטחת סביבה מסחרית בטוחה ואמינה כדי לעודד עסקאות.

**איך זה קורה? איך המערכת האוטומטית עובדת?**

**מערכת רב שלבית:**

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

**90% מהסכסוכים נפתרים ללא מעורבות גורם אנושי!**

**חששות וסיכונים**

* **Code is Law** – הטכנולוגיה אינה ניטרלית (המודל של לסיג)
* **חשש להטיות** – הכרעה בלתי שוויונית על סמך שיקולים חיצוניים לסכסוך.
* סיפוק המשתמשים מהתהליך אינו מבטיח שהמערכת הוגנת/צודקת.

**מודלים להסדרה של מערכות ישוב סכסוכים מקוונות:**

* **אקרדיטציה**
* **רגולציה עצמית**
* **סטנדרטים מומלצים**
* **מודל מסלקה**
* **הסדרה באמנות/הסכמים/חקיקה**:

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

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

**האתגרים הכרוכים בייצוג עצמי**

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

**חסמי גישה כלליים:**

**זמן, מקום, משאבים**

**מודל בית המשפט המקוון בדו"ח בריגס**

**שלב 1 (אוטונומי)**

**שלב 2: ניהול תיק וניסיונות פישור (אינסטרומנטלי)**

**שלב 3: הכרעה על ידי שופט (אינסטרומנטלי)**

**מודל הטריבונל האזרחי במחוז בריטיש קולומביה בקנדה - Civil Resolution Tribunal.**

* המערכת של בריגס חסרת תקדים מבחינת היקף – עד 25,000 פאונד
* דווקא למערכת הוותיקה בקנדה יש שלב נוסף – **Self Help**

**יתרונות המודלים המקוונים להליכים שיפוטיים**

* יתרונות הליכים א-סינכרוניים
* יתרונות בניית התהליך המחודשת
* מתן סיוע משפטי בזמן אמת
* חוויות משתמש שונות – האופן שבו המידע נאסף מהתובע/נתבע, המידע שמוצע לו יהיה שונה מאשר מה שהשופט רואה.

**חששות מתקשורת מקוונת ומאוטומציה**

* תיאוריית עושר המידע
* 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. ארכיטקטורת בחירה.

**מבוא למתווכים ברשת**

**המאמר של ניבה-אלקין קורן**

בראשית ימיה, היא הגיעה עם הבטחה מאוד גדולה של ביזור הכוח – כיכר העיר החדשה והשוק החופשי. **אבל** אנו בעצם יודעים שהאינטרנט והמודלים של השימוש באינטרנט הם לא באמת חופשיים לחלוטין משליטה/פיקוח/הגבלה.

**מודלים חדשים – איומים חדשים – שליטת התאגידים**

**מתווכים ברשת האינטרנט – Internet Intermediaries -** גופים, לרוב למטרות רווח שמאפשרים ביצוע התקשרויות/עסקאות בין צדדים שלישיים באינטרנט.

**המאמר של אורלי**

אורלי מדברת על 3 דורות של מתווכים ברשת:

* **דור ראשון** - אותם מתווכים שמאפשרים שיתוף/קישור למידע.
* **דור שני** - מאפשרים אינטראקציה/טרנזקציה כמו איביי, אמזון, העברת קבצים peer to peer
* **דור שלישי** - כניסה למרחב הפיזי, חברות הפלטפורמה (platform Economy).

**למה בעצם גורמי הביניים מהווים כתובת אטרקטיבית בכלל לתביעות משפטיות ולהפקדה של סמכויות אכיפה?**

* קל יותר לזהות אותם
* יהיה זול יותר לתבוע את YNET מאשר הטוקבקיסט.
* כיס עמוק
* מדובר גם במונע הנזק היעיל ביותר

**NAPSTER** לדוגמא.

**קשיים וסכנות בהטלת אחריות משפטית על גורמי הביניים**

* עמימות ביחס לכללים המשפטיים שחלים על המתווך (הפעילות ברשת).
* הרעיון הבסיסי - החשיפה המשפטית עלולה לייקר משמעותית את עלות הפעלתם של שירותים ברשת (הקמת מנגנוני סינון, ייעוץ משפטי, התדיינות משפטית) => צמצום מספר השירותים + התייקרות גישה למידע ולאמצעי ביטוי => ריכוזיות (גם עולה **בפס"ד רוטר**)

**הרצאת אורח – מערך הסייבר הלאומי – עמית אשכנזי**

הנרטיב המשפטי שליווה את התקופה הראשונית של האינטרנט, היה כזה שאמר שתפקיד המשפט בהסדרת האינטרנט הוא תפקיד יותר **פסיבי**, והמדינה לא צריכה להתערב באזור זה, וצריך להשאיר זאת להסדרה חוקתית. זאת התקופה שהמרצה קורא לה "**דיני תנאי השימוש**" אז קרו 2 דברים:

1. כל התפיסה הנורא יפה על האינטרנט התפוגגה עקב גילויים של אנואר סנודן שסיפר לעולם איך באמצעות האינטרנט ה-NSA יכול לאסוף מודיעין בצורה יעילה לממשלה האמריקאית. זה גרם למהלך שנמשך עד היום – **משבר אמון**.
2. **התגברות איומי הסייבר**. האינטרנט הפך להיות קצת פחות בטוח.

**מערך הסייבר הלאומי**

זה הגוף שהוקם. משימותיו:

* קידום ההיערכות הלאומית להגנת הסייבר (החלטת ממשלה 2442 ו2444).
* קידום עוצמה ביטחונית-אזרחית.
* הובלה ישראלית במרחב הסייבר.
* פיתוח תעשייה, אקדמיה והון אנושי.
* קידום היציבה הבינלאומית של ישראל.

**תקיפת סייבר:**

* תקיפות שנועדו לגנוב מידע.
* תקיפות שנועדו לגרום לנזק.
* תקיפות שנועדו לשבש את הפעילות.

**החלטת ב-84** - ב2002 המדינה הבינה שהנושא של רגישות גופים אלו דורשת טיפול – היא קיבלה את החלטת ב-84 (החלטה היסטורית) שבה נקבע כי יש גופים שהם תשתיות קריטיות – גופים שניתן באמצעות תקיפתם לגרום לנזק חמור מאוד לתשתית הבינלאומית. הטיפול בכך הוטל על השב"כ.

**יתרון נוסף של ישראל** – העיסוק בתשתיות קריטיות הוא פר גוף ולא פר ענף. (גישת הבוטיק ולא גישת הסופרמרקט) – מדובר בחליפה ייחודית לכל גוף ותשומת לב מדינתית.

**אירוע Wanna cry** – דוגמא ללמה גישת הבוטיק לא מספיקה.

**הבעיות בגיבוש תפיסת הגנה לאומית בסייבר:**

1. "זירת ההגנה" היא במערכות הארגון .
2. זירת ההגנה מבוססת טכנולוגיות אזרחיות.
3. משרעת רחבה של איומים, תוקפים ופוטנציאל נזק.
4. קישוריות והשפעות רוחב.
5. זמני תגובה קצרים.
6. מרחב גלובלי שאינו מצוי בריבונות "אחת".
7. תפקיד ואופן המעורבות של המדינה בהגנה תוך איזון מול:

**מדיניות הגנת הסייבר**

ב2014 המדינה קיבלה 2 החלטות – 2443 ו2444.

* 2443 – אסדרה והובלה ממשלתית
* **תפיסה מרכזית שבה יש לנו שפה אחת**
* **רגולציה אחידה באמצעות רשויות האסדרה**.
* **מנגנון "ניהול תקין" של הממשלה ומשרדיה לטיפול בהגנת הסייבר**.
* 2444 – מערך הסייבר הלאומי – גוף ייעודי להגנת הסייבר
* שיתוף מידע וטיפול באירועים בזמן אמת.
* הגנה בשילוב כלל הגורמים הממשלתיים.
* הגנה על זכויות יסוד.

הגוף בישראל נקרא C-SIRT (CERT) וגופים אלו בעלי מספר תפקידים.

**איך כל האופרציה של איסוף המידע מתיישב עם עקרונות הגנת הפרטיות?**

"עקרונות הפרטיות של הCERT הלאומי" – זה ניסיון לייצר מדיניות פרטיות קצרה, ברורה ושקופה לגבי מה אנו עושים ומה לא. גם כאן נעשה ניסיון לשמור על ההבחנה בין תוכן לבין מידע שרלוונטי לסייבר, ויש המצאה של מונחים חדשים לטובת הדבר הזה.

**זכויות יוצרים ברשת האינטרנט – אסדרה באמצעות גורמי הביניים ושימוש באכיפה טכנולוגית**

**רקע בסיסי**

הדין הישראלי בדומה לדין האמריקאי מונחה על ידי **גישה תוצאתנית** – הגנה על זכויות יוצרים היא מוצדקת אם היא מקדמת **תוצאה רצויה**. התמריצים שהחוק נותן כדי לקדם את **הרווחה המצרפית הכוללת**, כשהרווחה החברתית מוגדרת מאגד של ערכים שאנו רוצים לקדם.

**מצד אחד**, אנו רוצים לעודד השקעות ביצירה וחדשנות

**מצד שני**, הרווחה החברתית הכוללת, כוללת את הרצון לקדם את חופש המידע, הגישה אליו, שיתופו, ואת חופש הביטוי.

**חוק זכויות יוצרים**. לא נדבר על כל החוק.

**הרעיון הבסיסי**: יחד עם **ס' 47 וס' 11** אנו מגיעים להבנה שהפרה של זכויות יוצרים היא ביצוע של פעולה שיוחדה לבעל זכות היוצרים (שימוש ביצירה שייוחד לבעל זכות היוצרים) בלי לקבל את הרשות של בעל הזכות.

ס' 11 – "פעולות אלו ששימושיהם יוחדו": העתקה, פרסום, ביצוע פומבי, שידור, יצירת יצירה נגזרת, והשכרה לצורכי מסחר.

**ההגנה לא חלה רק על היצירה כולה אלא גם על חלקים ממנה**.

במסגרת איזון הערכים יש לנו כבר בחוק **הכרה לשימושים מותרים שלא ברישיון** – כמו שימוש אגבי או להליכים משפטיים (ס' 20-30 ו32) ושימוש הוגן.

כדי להוכיח תביעה בזכויות יוצרים/או בגין הפרה, התובע צריך להוכיח **שהוא בעל הזכות, ושהנתבע הפר את הזכות**.

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

כדי להיות יכול לאכוף את זכויות היוצרים, בעלי הזכויות צריכים לנקוט **בפעולות אכיפה מרובות** כדי להבטיח את האינטרס שלהם.

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

\*במאמר של פרל ואלקין-קורן – עד כמה באמת יש אנונימיות ברשת? האם באמת קיים קושי גדול להצליב מידע של משתמשים? בטלפון הסלולרי בכלל.

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

* זה יקר.
* ספק אם זה בכלל יעיל.
* יש קושי בזיהוי המשתמשים לצורך הטלת אחריות.
* צריך לפנות לספק הגישה ולקבל את הIP של המפר.
* ביהמ"ש קבעו שלא קיימת סמכות בחוק המאפשרת להם להורות לספק לחשוף את זהותו של משתמש שלכאורה ביצע עוולה אזרחית ולרוב דחו בקשות שכאלו. –Primer League .
* ההצעה לתיקון מס' 5 לחוק זכויות יוצרים מבקשת ליצור מקור לסמכות זו: בפרק ח'1: חשיפת זהותו של עושה פעולה בתוכן ברשת תקשורת אלקטרונית.

**התוצאה – פנייה לגורמי הביניים**

גורמי הביניים: מנהלי אתרים, מנועי חיפוש, רשתות חברתיות וספקי אינטרנט.

המטרה: פנייה זו קיימת מראשית רשת האינטרנט.

האמצעים: בעיקר אמצעי אסדרה טכנולוגיים. **סוגי אמצעי אסדרה טכנולוגיים**:

* **מנעולים דיגיטליים על היצירה עצמה**
* **הגבלת העברת מידע ברשת**

**כיצד ניתן לקדם אסדרה באמצעות גורמי ביניים?**

* **אחריות ישירה** (לא עושים).
* **אחריות עקיפה** – נעשית היום בדין הישראלי בעיקר על בסיס **דוקטרינת ההפרה התורמת**. הבסיס לה הוא **נוהל הודעה והסרה** (כמו שיש בארה"ב). פרשת על השולחן, פרשת שוקן, פרשת רוטר.

**מה מהצב המשפטי הזה אומר?**

* אין אחריות ישירה על גורמי הביניים בגין פעולות שבוצעו על ידי המשתמשים (בכפוף לנוהל הודעה והסרה).
* חשוב להבחין את המקרה הזה לבין מקרה שבו גורם הביניים הוא אחראי בעצמו להפרה.

**אז מה כן?**

**אחריות משפטית עקיפה**. **פשרת שוקן** (תא סטודנטיאלי באוניברסיטה העברית) בית המשפט דן בשאלה מה היו התנאים באחריות של גורם הביניים במקרה הזה? התנאים שנקבעו הם:

1. הפרה ישירה בפועל
2. ידיעה ממשית של המפר התורם (האוניברסיטה) על ההפרה – לא מספיק ידיעה קונסטרוקטיבית
3. שלגורם הביניים תהיה תרומה משמעותית, ניכרת וממשית לביצוע ההפרה.

פרשת **רוטר** (פרסום קישורי סרטים ללא הרשאה)

**העיקרון שנקבע בפסק הדין הוא שלא תוטל אחריות להפרת זכויות היוצרים על בעל האתר אם הוא לא ידע עליה, ובתנאי שכשנודע לו עליה, הוא הסיר את הפרסום המפר.**

**שיקולי מדיניות בהחלת דוקטרינת ההפרה התורמת על גורמי ביניים ברשת וקיום נוהל "הודעה והסרה"**

1. הכרה בכך שהיקף ההפרות והחומרה שלהם גדולים יותר ברשת עקב הקלות, הנגישות וקהל המשתמשים הרב (לוין נ' קניבסקי).
2. חשיבות בהגנה על זרימת המידע, זכות הציבור לדעת, חופש הביטוי (עלה ברוטר)
3. חשש מהטלה של עלויות על גורמי ביניים שיצטרכו לנקוט בפעולות של שיטור, ניטור וסינון\*
4. חשש שהפעילות תצטמצם יותר מידי עד שייווצר אפקט מסנן.
5. זיר"ה נ' פלוני - המחיר שהחברה משלמת מהפיכה של גורמי הביניים לצנזורים

**החריגים לכלל של הודעה והסרה:** משתמשים שמעלים תוכן מפר לא יעלו אחריות של גורם הביניים כל עוד הוא הסיר את הפרסום ברגע שנודע לו שהוא מפר.

**בפס"ד רוטר** נזכרים חריגים שבהם כן תוטל אחריות על האתר בגין פעולות שהמשתמשים ביצעו:

* אם האתר מעודד את המשתמשים לבצע פעילות
* אם אנו מזהים שכל מטרת האתר היא פסולה

**כללי האצבע החדשים היוצרים "פורום פסול" (פרשת רוטר)**

השופט גרוסקוב עושה הפרדה בין **פורום סגור** מול **פורום פתוח**.

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

**בפורום פתוח** שם אין הגבלת גישה, **מחצית** המתוכן המהותי של הפורום יהיו הודעות הכוללות קישורים לאתרים מפרים.

אם הוכחתי שהפורום פסול, יש חזקה שבעל האתר מודע לכך שהוא מסייע לקיומן של הפרות ישירות וכי סיוע זה הוא בגדר תרומה ממשית ומשמעותית להפרות. הנטל עכשיו עובר אליו להוכיח:

1. להמשך קיומו של הפורום יש ערך לגיטימי,
2. או שהוא לא ידע על היקף הפעילות הפסולה

בנוסף, אם הפעילות המפרה בוצעה על ידי מישהו שהוא בעל האתר/נציגיו הוא יהיה אחרי לכך

**המעמד שמשפטי של נוהל "הודעה והסרה"**

**בישראל** הנוהל הזה הוא יציר הפסיקה.

**ארה"ב** – Digital Millennium Act.

**אירופה** – הדירקטיבה האירופאית בנושא סחר אלקטרוני (Directive 2000/31/ec).

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

**באיזו מידה גורמי הביניים מגנים גם על זכויות המשתמשים?** אם אנו חושבים שיש הגנות על האוטונומיה של הפרט במנגנונים של גוגל – התשובה לא מאוד ברורה. **בנוסף**, אין לנו כלכך יכולת לפקח. החשש הוא שבגלל המציאות הזאת, אנו נתמרץ במציאות המשפטית שנוצרה את גורמי הביניים לפעול **יותר מדי**

**דרכים לצמצום או מניעת הסיכונים**

* בשלב הזה, באמצעות פיקוח חיצוני (ולא רק פנימי) אנו יכולים לדאוג מבחוץ ליצירת כללים ברורים בדבר טיפול בתלונות
* שקיפות לגבי היקף שיתוף הפעולה בין גורמי ביניים לבעלי זכויות
* שקיפות לגבי אופן הפעולה של מנגנוני האכיפה של גורמי הביניים

**אכיפה באמצעות גורמי הביניים – המקרה של סעדים טכנולוגיים**

**סעדים מסורתיים**

* פסיקת סעדים על ידי ביהמ"ש אשר כוללת הכרעה.
* סעד פיזי.

**סעדים טכנולוגיים**

* יהיו כפופים בד"כ להליך משפטי מקוצר, ולא בהכרח תהיה הכרעה מהותית בשאלת ההפרה.
* מי שמיישם את הצו הזה יהיה אמצעי טכנולוגי, שלרוב יהיה אמצעי דינמי ובלתי שקוף.
* ההגדרה הטכנולוגית של יישום צווי החסימה נותרת בידי ספק הגישה, בהתאם לשיקול דעתו.

**הקשיים שמתעוררים בשימוש בצווי הגבלת גישה**

* אין לנו פיקוח שיפוטי, הפרטים הטכניים מוגבלים על ידי גורמי הביניים, וכשאנו מעבירים את השליטה לספקי גישה פרטיים, יש חשש שהמנגנונים יהיו בלתי צודקים ויפגעו בזכויות יוצרים.
* יש לנו חשש מאכיפת יתר שמתומרצת על ידי המשפט.

**הנחות היסוד בבסיס הצעת החוק -** חוק זכויות יוצרים שפורסמה בנוב' 2017

מציעה 4 הסדרים חדשים (שלא נדון בכולם), בין היתר את הליך חשיפת הפרטים של גולש אנונימי. אנו נתמקד בעניין של **צווי הגבלת גישה**.

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

**האם הנחות יסוד אלו נותרו רלוונטיות כיום?**

העמדה של אלקין-קורן וחברתה (למרות שהיא לא המקובלת ביותר) היא שהנחות אלו אולי היו רלוונטיות בשנות ה90 אבל **לא כיום**.

**התמריץ להצעת החוק** - יש מחלוקת כיום בבתי המשפט לגבי הסמכות להוציא צווי הגבלת גישה על ספק האינטרנט על ידי ביהמ"ש. **צ'רלטון נ' 012**. **ביהמ"ש** קבע קודם כל שלספקי הגישה אין אחריות תורמת, **ובהעדר מקור סמכות בחוק, לביהמ"ש אין סמכות להוציא צו הגבלת גישה**

**עם זאת**, הייתה גם עמדה אחרת – **שיש סמכות**. **פרשת בלומברג**.

**הצעת החוק: אמצעים סבירים להגבלת גישה - בהצעת החוק לפי ס' 53** נקבע, כי בעצם יהיה צו הגבלה שיכוון כלפי ספק הגישה ויחייב אותם לחסום את הגישה לתכנים מפרים.

**מה זה אמצעים סבירים?** אנו נשארים בסוף עם "אמצעים סבירים".(נתון לפרשנות ביהמ"ש).

מה שביהמ"ש כן מקבל בס' 53 א' ד' זה רשימת סל של השיקולים שביהמ"ש ישקול:

1. *חומרת ההפרה הנטענת.*
2. *נחיצות הצו למניעת הפרתה של זכות יוצרים.*
3. *יעילותם של סעדים אחרים העומדים לרשות בעל זכות היוצרים או בעל הרישיון הייחודי.*
4. *מידת הפגיעה הצפויה בגישה לאתרי אינטרנט אחרים.*
5. *מידת הפגיעה הצפויה בפרטיות של משתמשי האינטרנט.*
6. *ההשפעה על הציבור כתוצאה מהגבלת הגישה לאתר לפי צו או מהחלטת בית המשפט שלא לתת צו.*

**איך נבחן את התוכן?** הצעת החוק מדברת על **מבחן מהותי**, אבל לא ברור איך זה ייושם. האם זה מתייחס לחלק מהתכנים או כל התכנים באתר?

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

מבחינה מהותית, למרות שההגדרה הפורמלית של הצו "סעד זמני", צו הגבלת גישה זה בעצם **סעד עיקרי**.

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

יש לנו כמה לקחים – **הDMCA האמריקאי.**

מנגנון הודעה והסרה **הפך** את נטל ההוכחה המסורתי בדיני זכויות היוצרים. השיקול העסקי הברור הוא **להסיר**, ומי שמשלם את המחיר זה שאר הזכויות. לנו כציבור יש **פחות חופש מידע באינטרנט.**

**בפועל** – הרבה מבעלי הזכויות מנהלים את הזכויות באופן אוטומטי.

**פרטיות בעידן הדיגיטלי - מבוא**

**מיכאל בירנהק, מרחב פרטי** (מחומרי הקריאה)

יש לנו הרבה טכנולוגיות חדשות, שעצם השימוש בהן והפעולות שהן מאפשרות, מייצרות פוטנציאל לפגיעה בפרטיות.

**במציאות הזאת קורה משהו מעניין** – יש מעקב של השלטון, כניסת התאגידים (המידע הופך להיות מוצר שכיר), ושני עולמות אלו נפגשים – ואנו נמצאים בעולם של **Dataveillance** (מעקב מידע) ומעקב המונים.

למרות שאנו בעצם "סוג של" יודעים את כל הדברים האלה, בהתנהגות היום-יומית של אנשים קיימת **אשליה של פרטיות**.

**מצד שני**, קיים מושג שנקרא **פאנופטיקון** על ידי **ג'רמי בנת'הם ומישל פוקו**.

**הרעיון המרכזי של הפאנופטיקון**: מי שנמצא בפנים לא יכול לדעת מתי צופים בו או לא, ולכן אילן לו ברירה להניח שצופים בו כל הזמן

שיח ערכי על **משמעות הפרטיות בעידן זה**

הנחת מוצא - **הטכנולוגיה היא לא בהכרח רעה או בהכרח טובה.**

לאורך זמן, יכול לחול שינוי בטכנולוגיה מסוימת/במשמעות שאנו מייחסים לה. (Cookies)

**המודל של לסיג**: משמעות הטכנולוגיה נקבעת בידי המפתח למטרה שלמה הוא מפתח, למאפייני הטכנולוגיה עצמה והשימושים שנעשים בה בפעול.

**צירים לדיון בפרטיות בעידן הדיגיטלי (סיכום של הדברים)**

* ההבנה של **הזכות לפרטיות** כמושג משפטי שנמצא **במו"מ מתמיד** עם נורמות חברתיות והטכנולוגיה.
* הבנה של מושג הפרטיות במונחים של **שליטה של האדם על עצמו** (על מה ששלו, ומהותו).
* **חוסר התאמה של הנחות של עולם אנלוגי**
* **הגנת מידע ביחסים מול המדינה ומול השוק**.

**מהי פרטיות?**

* **נורמה חברתית**
* **זכות משפטית**

**ס' 7 לחוק יסוד כבוד האדם וחירותו**:

*(א) כל אדם זכאי לפרטיות ולצנעת חייו.*

*(ב) אין נכנסים 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.*

בחוק הישראלי, הזכות לפרטיות היא נגזרת של חוק יסוד כבוד האדם. היא מגיעה מתפיסות שמדובר בכבוד האדם ולא תפיסה קניינית/חירות (כמו הדין האמריקאי)

**חוק הגנת הפרטיות 1981** – קובע איסור על פגיעה בפרטיות ומונה 12 תתי סעיפים שונים על מעשים שיהוו פגיעה בפרטיות.

גם חוק היסוד וגם חוק ההגנה על הפרטיות **לא כוללים** **הגדרה של מהי הזכות לפרטיות**.

**אז מאיפה הגיעה הזכות לפרטיות?**

**וורן וברנדייס, 1890** – הזכות לפרטיות כזכות להיעזב למנוחה.

**ב1967 אלן ווסטין** - היכולת של אדם לקבוע בעצמו ולמען עצמו איזה מידע על אודותיו לשתף עם אחרים ובאיזה אופן ותנאים מידע זה ישותף.

1. הבחנה זו קושרת את עצמה יותר **לכבוד האדם**
2. הזכות להיעזב במנוחה היא **זכות פסיבית לפרטיות**

מדובר בהבחנה קונספטואלית שעוזרת לנו להבין איך אנו מגיעים לכלים קונקרטיים כמו **עקרון ההסכמה**, או **עקרון צמידות המטרה** (לא ניתן לעשות שימוש במידע למטרות אחרות).

**קטגוריות של פרטיות:**

1. **פרטיות במקומות** – "ביתו של אדם מבצרו"
2. **פרטיות בתקשורת (שבין בני אדם)** - **בתיקון מס' 9 לחוק**, תוכן של מכתב **כולל גם מסר אלקטרוני**. היום יש לנו **הגנה פחותה** על נתוני התקשורת בהשוואה לתוכן התקשורת.
3. **פרטיות במידע** – קיימות 2 גישות מרכזיות לגבי השאלה **מהו מידע אישי**:

**גישה סקטוריאלית (ארה"ב)** - אם לא הגבלתי את הגישה לשימוש, ואם הציבור מעוניין, הוא יכול לסחור בו.גישה זו מנוגדת לגישה האירופאית**.**

**גישה אירופאית (הגישה המרחיבה)** – כל מידע ייחשב לפרטי אם הוא קשור לאדם מזוהה או אדם שניתן לזהותו. אם אני יכול לעשות דה-אנונימיזציה למידע, אז הוא יהיה זכאי להגנה

**הגישה בישראל** יותר קרובה לאירופאית, אבל כן יש בה אמת מידה תכנית.

**רגולציית הגנת המידע באירופה – GDPR – מרצה אורח – חיים רביה**

**מהפכת הפרטיות באירופה**

**General Data Protection Regulation – תקנות הGDPR**

1. **דירקטיבה** – דבר חקיקה של האיחוד, שכל אחת מחברות האיחוד חייבת להתאים את דיניה הלאומיים לדירקטיבה.
2. **תקנות** – המילה תקנות מטעה מפני שהן כופות עצמן הר כגיגית, הן מבחינת הדין המחייב. תקנות אלו לוו במערך מרשים של **קנסות**.

ה**GDPR** הוא דבר חקיקה מקיף מאוד. הוא עוסק בעיבוד מידע אישי.

**על מה ומי תקנות הGDPR- חלות?**

**חלה על כל עיבוד של מידע**, גם אם לא מבוצע באמצעות מחשב.

**המידע צריך להיות אישי**. מידע אישי = כל דבר שהוא מזהה אדם או מאפשר לזהות אדם.

**תקנות הגנת הפרטיות** חלות על כל מי שמצוי בתחום הטריטוריאלי של ישראל. **הכלל הוא משפט לעולם טריטוריאלי**, גם כדרך של מדינות לכבד זו את מדיניותה של זו.

**באו התקנות האירופאיות (הGDPR) וסטו מהכלל הזה**:

1. חלות על מי שיש לו Establishment בEU – **כמעט כל דבר**.
2. חלות על מי שמעבדים מידע אישי של יחידים באיחוד האירופאי, גם אם הארגונים נמצאים **מחוץ לתחום הטריטוריאלי של האיחוד**, ב2 תנאים:
3. הם מעבדים את המידע כי הם מציעים שירותים או מוצרים באיחוד האירופאי
4. אם אתה מנטר התנהגות של יחידים בזמן שהם נמצאים באירופה.

**הדין לא דבוק לאזרח** – כשאזרח צרפתי עובר למדינה אחרת אין לו זכויות מכוח הGDPR.

**IP Address:** זהו מידע אישי לפי הGDPR/

**עיבוד מידע אישי** – איסוף, אחסנה, השמדה... **פעולת השמדת מידע באה לכדי עיבוד**.

**הבחנה בין Controller לProcessor-:**

**קונטרולר** – מי שקובע את מטרות עיבוד המידע ואת האמצעים שישמשו לעיבוד המידע.

**פרוססור** – מי שמספק בפועל את השירות של עיבוד המידע.

**ייתכן למעשה שיהיה יותר מקונטרולר אחד!** ((Joined Controller. הוא יכול להיות גם אותו גורם.

**לפי הGDPR-, עיבוד המידע חייב להיות:**

* **חוקי, הוגן ושקוף**.
* **למטרה מוגדרת**
* **תואם, רלבנטי ומוגבל למטרה**
* **מדויק ועדכני**
* **מוגבל בזמן**
* **מאובטח**.

**מה ייחשב לעיבוד חוקי?**

1. אם הוא מבוסס על הסכמה.
2. עיבוד המידע הוא חיוני לעיבוד החוזה.
3. חיוני לציות לחוק.
4. חיוני לאינטרס האישי של נושא המידע או צד שלישי.
5. חיוני לאינטרס ציבורי.
6. חיוני לאינטרס לגיטימי של הקונטרולר או צד שלישי.

**הסכמה**

* חייבת להיות חופשית, מוגדרת ומדעת.
* חובת ההוכחה על הקונטרולר.
* היא חייבת להיות נפרדת בבירור מעניינים אחרים.

**מהן הזכויות של נושא המידע?**

1. לקבל מידע (שקיפות)
2. איסור על העברת מידע למדינות בעלות רמת אבטחת מידע נמוכה (יחד עם עקרון התאימות)
3. זכות העיון והתיקון
4. הזכות להישכח (גונזלס נ' גוגל)

**הגנת הפרטיות בעידן הדיגיטלי בישראל**

**הגישה הישראלית: זכות כללית לפרטיות**

**ס' 7 לחוק יסוד כבוד האדם וחירותו**

קובע זכות כללית לפרטיות, כל אדם זכאי לפרטיות ולצנעת חייו.

**חוק הגנת הפרטיות (1981)**

קובע איסור מפורש על פגיעה בפרטיות. פירוט מצבים שמהווים פגיעה בפרטיות:

1. **פגיעה בפרטיות פיזית**
2. **פגיעה בפרטיות מידע** (יכולה להיות עילת תביעה פלילית).

**אמת המידה להגנה המשפטית על המידע היא תכנית** אבל עדיין רחבה יותר מארה"ב.

**מהו עניינו הפרטי של אדם?**

**פס"ד ונטורה**. (מאגר כרטיסי אשרי) - סותר את ס' 9 לחוק ואת **עקרון צמידות המטרה**.

עמדה מרחיבה, בך – **כל מידע** שקשור לחייו הפרטיים של אותו אדם, **לרבות** שמו, כתובתו, מספר..

עמדה מצמצמת, שטרסברג כהן – ההגדרה לענייניו הפרטיים של אדם צריכה להיות זהירה...

תובנה צופה פני עתיד הגנת המידע בעידן הדיגיטלי, שטרסברג כהן.

**הסדר ספציפי למאגרי מידע – פרק ב' לחוק הגנת הפרטיות**

בהסדר הספציפי כן ניתנת הבחנה (התיקון נחקק בשנת 96) בין **מידע למידע רגיש**.

בס' 7 לחוק: יש עמדה של המחוקק ש**הכשרתו המקצועיות ומעמד אישי זה לא מידע רגיש**.

**מאגר מידע**

הרעיון הוא להפריד בין אוסף שנועד לשימוש פרטי ואוסף שנועד לשימוש מסחרי/מכירה לצד שלישי.

**מאגר ידני -** **הגישה הישראלית בחוק הגנת הפרטיות שונה מהגישה האירופאית והיא מחריגה את המאגרים האנלוגיים** – יוצרת הבחנה בין המאמרים הדיגיטליים לאנלוגיים. יש הנחה כי הסיכון הוא פחות בהשוואה למאגר דיגיטלי.

צריך לשים לב בחוק את הייחוס ל**נתוני מידע** לעומת משהו שחובר **על בסיס הנתונים הללו**.

**החובות המוטלות על מנהל המאגר**

**מנהל מאגר**

**1. רישום מאגר**

**ס' 8(א)**: חובת רישום מאגר אצל רשם מאגרי המידע, במקרים המנויים בס' 8(ג):

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

*(2) יש במאגר מידע רגיש;*

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

*למאגר זה;*

*(4) המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;*

*(5) המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.*

*(ד) הוראת סעיף קטן (ג) לא תחול על מאגר שאין בו אלא מידע שפורסם לרבים על פי סמכות כדין או שהועמד לעיון הרבים על-פי סמכות כדין.*

**מדוע יש חובת רישום מאגר?**

* **פיקוח מהותי** – יכולת לסרב לרשום, מטרת המאגר המוצהרת, מתן תשובה על הבעייתיות של הטקסטים הסבוכים.
* **פיקוח על הפעילות** – מופנה למגזרים, ולא רק למאגרים ספציפיים.
* **הנחה התנהגותית** – חובת הרישום גוררת בדיקה ופיקוח פנימיים אצל מנהלי המאגרים

הרעיון הוא שתיווצר תרבות של בעל המאגר לציית לחוק.

**2. חובת ההודעה** –

ס' 11: מי שפונה לאדם לקבלת מידע לשם החזקתו במאגר צריך לתת לו הודעה שעומדת בתנאים האלה:

1. האם על האדם חלה חובה חוקית למסור את המידע או שדרושה הסכמתו?
2. מהי המטרה אשר לשמה מבוקש המידע?
3. למי יימסר המידע ומהן מטרות המסירה?

**חשיבות חובת ההודעה**

* ההודעה היא בסיס לקבלת **הסכמה מדעת**.
* היא מהווה בסיס להפעלת **עיקרון צמידות המטרה**.

הבעייתיות היא, שאין לנו דרישות אמיתיות לצורת ההודעה.

**עקרון צמידות המידע** – המידע שלך יכול להימצא אצל מישהו אחר אבל לך יש זכות לשלוט במה שקורה למידע זה.

**צמידות המטרה** – כשאתה מוסר את המידע, זה לצורך **מטרה ספציפית/מסוימת**.

**3. חובת סודיות ואבטחת מידע**

שתי חובות שמטרתן לצמצם את הסיכון גם מדליפה מגורם פנימי (ס' 16) והסיכון שמישהו יפרוץ למאגר (ס' 17) שמכוחו מוטלת החובה לאבטח.

חשוב לשים לב שיש כאן **עקרון בסיסי** – אנו קובעים **סטנדרט ולא את האמצעים**.

**שיעור 10** **– הרצאת אורח – ההיבטים הרגולטורים של שוק התקשורת**

**משרד התקשורת וטכנולוגיה**

**עקרונות האסדרה**

1. **שירותים מתקדמים**
2. **מחיר סביר**
3. **עידוד תחרות**

**תקשורת וטכנולוגיה מבחינת משרד ממשלתי**

**במקרה הבוחן**, היחס של משרד התקשורת לטכנולוגיה הוא מורכב. **מצד אחד** אנו מאוד מעודדים טכנולוגיה חדשה, **אבל** אנו צריכים להיות זהירים.

**הממשק עם שוק התקשורת** - **שלב גיבוש הרגולציה** – זמן חשיבה לרגולציה חדשה. פשוט עושים שיחות עם חברות, לפעמים מזמינים אותן אלינו.

**מקרי הבוחן**:

1. אינטרנט מהיר.
2. אוניברסליות (סיבים אופטיים והפריפריה).
3. IOT.
4. ניטרליות הרשת.

**אינטרנט מהיר**

**טכנולוגיה חדשה ואתגריה**

**Dial UP** - עם בזק לא הייתה בעיה, אבל חברות הכבלים הוקמו כחברות כבלים! משרד התקשורת אמר שיש כאן בעיה **בעיקרון החוקיות**. אז כרגולטורים ניתן **לתקן את החוק**. הפתרון התחיל **במהלך מדורג** – בהתחלה נקפיא את הכניסה לטכנולוגיה, ובינתיים ננסה לחוקק כמה שיותר מהר חקיקה..**.**

**אוניברסליות רשת**

**טכנולוגיה חדשה ואתגריה**

**תשתיות מתקדמות** - לא רגולציה כופה אלא ניסיון של המשרד לעודד הנחת סיבים אופטיים.

**שירות לפריפריה** – פיזור אוכלוסייה ותעסוקה, מוביליות חברתית. החברות מקבלות פחות כסף מהפריפריה.**Beatty, Nevada, USA .**

**פתרונות** - הפתרון הוא להעדיף את **חובת האוניברסליות**, להטיל חובת אוניברסליות על הוט ובזק, אבל לתת הקלות

**IOT – האינטרנט של הדברים**

**4 המהפכות הטכנולוגיות:**

1. **המצאת הרכבת והקטר**.
2. **המצאת החשמל**.
3. **מהפכת המחשוב**.

עד כאן, מדובר בטכנולוגיית P2P – אני מעביר מידע מאדם לאדם.

1. **שליחת דברים באינטרנט של הדברים Machine to Machine.**

**יישום** - בית חכם (**מכונות כביסה חכמות**) יש גם **IMT** (**שירות רפואי אינטרנטי בזמן אמת**) (מהמאמר)

**האתגרים** - פריצות (Hacking), פרטיות, אחריות משפטית, מיסוי, עומס על התשתיות וספקטרום.

**פתרונות** - משרד התקשורת אישר ביצוע ניסויים בIOT-. בנוסף, (המרצה נתן לקרוא) – הרבה יותר קל לייבא עכשיו מוצרים שיכולים להוות בעיה מבחינת הספקטרום.

**ניטרליות הרשת** – לא נספיק לדבר (יש להשלים מחומרי הקריאה).

יש מלחמה מאוד קשה בארה"ב ויש דעות לכאן ולכן. בישראל **יש ניטרליות רשת**. בארה"ב היה בהתחלה, ואז ביהמ"ש ביטל את ההחלטה הזו, ואז הרשות לתקשורת האמריקאית החזירה זאת עם תיקונים, ביהמ"ש תיקן זאת, ואז ביהמ"ש אישר זאת. למעשה לפני חודש נכנסה ההחלטה שהרשות עצמה ביטלה את ניטרליות הרשת בארה"ב.

**שיעור 11 - חובות הסודיות ואבטחת המידע**

החוק **בס' 7** מגדיר אבטחת מידע בסעיף ההגדרות: *"כהגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה ללא רשות כדין".* בעצם מדובר על **החובה לצמצם את הסיכון שהמידע ידלוף**.

החוק לא מפרט בדיוק איך הדבר הזה ייעשה ממספר טעמים:

1. **לא כלכך פרקטי** - הבחינה האם האמצעים היו סבירים נעשית **בדיעבד ולא מראש**.
2. **ניטרליות טכנולוגית -** יש לה גם מאתגרים תמידיים (במיוחד בארה"ב - ניטרליות הרשת)

**מושג ניטרליות הרשת** כולל מספר שימושים: השימוש הנפוץ ביותר בשיח לגביו זה ניטרליות של ספקיות האינטרנט. היום האינטרנט פועל באופן של ניטרליות רשת – ספקיות השירות לא יכולות להעדיף תעבורה של אתרים או משתמשים מסוימים, וכולם שווים בפני חוק ניתוב המידע ברשת **עם זאת**, לספקיות יש אינטרס לא לשמר אותו, כי הן יכולות למכור בכסף גישה מהירה יותר והעדפה של תעבורה מסוימת (Mako)עמדה של ניטרליות רשת משקפת מבט על הרשת כ**תשתית חיונית** ולא רק כשירות עסקי. **הצד השני של זה** – אם נפגום בניטרליות נפגום בשוק.

**חוק הגנת הפרטיות**

**תקנות הגנת הפרטיות – אבטחת מידע**, החליפו תקנות קודמות שלא היו רלוונטיות לחלוטין לעידן הדיגיטלי ומאגרי מידע ממוחשבים, והקושיה הזו של איך ליישם את חובת הגנת הפרטיות שחוק הגנת הפרטיות מטיל ב**ס' 17**, קיבלה איזשהו תוכן קונקרטי לגבי האופן שבו החובה הזו תיושם.

**התקנות בעצם מסדירות את חובת אבטחת המידע במאגרי המידע ב3 רבדים:**

1. בעל מאגר המידע צריך לקבוע איזה מידע מוגן יש לו במאגר ומהם הסיכונים שקשורים אליו.
2. בעל מאגר המידע צריך לקבוע מה יהיו נהלי העבודה שבהם הוא ינקוט כדי לאבטח את המידע.
3. בעל מאגר המידע צריך לקבוע מה יהיו ההוראות המהותיות בניהול אירוע אבטחת מידע.

**תפיסה מודולרית** **אנו נחיל חובות ברמה הולכת וגוברת ככל שהפעילות של עיבוד המידע המאגר היא משמעותית יותר, ככל שהמידע רגיש יותר ,וככל שיש יותר אנשים בארגון שחשופים למידע**.

מרבית החובות חלות **גם על בעל המאגר וגם על מנהל המאגר** (ס' 21)

**4 סוגי מאגרי המידע**:

1. **מאגר יחיד** - מאגר שמנוהל על ידי יחיד (יכול להיות גם תאגיד בבעלות של יחיד) כל עוד הגישה למאגרים היא לבעלים של המאגר ולכל היותר 2 מורשי גישה נוספים. חשוב לציין, שאם יש מידע על יותר מ10,000 איש, גם אם יש גישה לאדם אחד – הוא לא יכלל תחת גדרי מאגר שמנוהל על ידי יחיד(וזה יעלה לכדי בסיסי).
2. **מאגרים שחלה עליהם רמת האבטחה הבסיסית** – מוגדרים על דרך השלילה, מאגרים שלא מנוהלים על ידי יחיד ולא חלה עליהם רמת האבטחה הבינונית או הגבוהה.
3. **מאגרים שחלה עליהם רמת האבטחה הבינונית** – יש להם קודם כל לפחות **10 מורשי גישה** מאגרים אלו, מטרתם איסוף מידע לצורך מסירתו לאחר, או שהם בבעלות גוף ציבורי ויש הפניה לגופים ציבוריים, או שהם מכילים מידע רגיש, כמו מידע ביחס למצב רפואי, נפשי, מידע גנטי/ביומטרי על האדם, מידע על הדעות/אמונות של האדם.

ניצנים של **התפיסה על החיבוריות** – היכולת לבנות פרופיל של האדם מתוך מאגרים נוספים

1. **מאגרים שחלה עליהם רמת האבטחה הגבוהה ביותר** – מאגרים של יותר ממאה אלף אנשים, או שמספר המורשים לגשת למידע הזה הוא לפחות 100 או עולה על 100, וההנחה גם כאן היא שהמטרה של המידע היא איסוף לצורך מסירתו לאחר או שיש כאן מידע רגיש.

בעצם, מה שמבחין בין הבינונית לגבוהה זה כמה אנשים יש במאגר.

**ככל שרמת הסיכון גבוהה יותר, יש דרישות גבוהות יותר ממנהל המאגר**.

**מה בעצם אנחנו, מושאי המידע, יכולים לעשות?**

למושא המידע יש כל מני זכויות שמוקנות לו. ההנחה שלמושא המידע יש זכות במידע האישי עליו.

* **החוק בס' 13 מאפשר למושא המידע זכות לעיין במידע** (ואפשר להרשות לאחר לעיין).
* **הזכות לתקן את המידע/לדרוש את התיקון של המידע**.
* **פגיעה בפרטיות עלולה להקים גם עוולה אזרחית** ויכולה להוות יסוד לעבירה פלילית אם נעשתה במזיד.
* **חוק הפרטיות קובע בס' 31 עוולה בנזיקין**

**הזכות להישכח – מה קורה עם המידע האישי הדיגיטלי שלנו לאחר המוות**

**שובל המידע הדיגיטלי** מהפרק של בירנהק. במחקר של בירנהיים – יש מגוון רצונות של משתמשים שהם שונים, של משתמשים שרוצים לעשות דברים עם המידע שלהם אחרי מותם.

**אילו זכויות ואינטרסים במידע לאחר המוות קיימים? איזה מן התנגשויות אנו יכולים לראות ביניהם?**

הטכנולוגיה פתחה דרך להתמודד עם אובדן ולהנציח את המנוח בדרך שמשאירה משהו ממנו נוכח. אבל היא גם מעלה שאלות מאוד מאתגרות לגבי השליטה במידע וגם היכולת לעצב את הזיכרון – איזו דמות נותרת מאחור, ועד כמה לאדם יש שליטה על הזכרות שנותר ממנו? חלק מהמאפיינים המיוחדים האלה מעוררים שאלה על היכולת שלנו להחיל מסגרות משפטיות קיימות שעוצבו בסביבה לא דיגיטלית.

**מהם המאפיינים האלה?**

* מידע דיגיטלי אינו מתכלה וניתן לעבדו בקלות.
* הוא כולל עוד סוגים של מידע – נתוני התקשורת (ולא רק התוכן).
* יש כאן שאלות שלא היו קיימות בעבר בנוגע לשליטה האפקטיבית במידע

**מה הפלטפורמות הטכנולוגיות עשו? מה הן הפתרונות שסופקו?**

רוב ספקי השירותים לא הסדירו את הנושא ואין להם פתרון

**פייסבוק** מאפשרת למשתמשים לקבוע legacy contact

**לגוגל** יש כלי אחר שמאפשר לך להיכנס ולקבוע פרק זמן, שאם הוא חלף וגוגל לא איתרה פעילות מצדך, באופן אוטומטי אדם/אנשים מצדך יקבלו אימייל שיאפשר לאותו אדם לקבל גישה לחשבונות.

**שיעור 12 – שירותים משפטיים מקוונים**

**מתן שירות משפטי באופן מקוון** - שירותים משפטיים יכולים להינתן

1. באופן מקוון בצורה מלאה;
2. או בשילוב בו חלק מהתהליך קורה בצורה מקוונת, וחלק מהתהליך קורה בממשק עם אדם.

**הנקודה המרכזית שיש לחשוב עליה**, היא שכך או אחרת, הרכיב הטכנולוגי בתהליך מחליף איזשהו היבט של פעולות שעורכי דין, או לפעמים רק המזכיר המשפטי פעם ביצע.

**טפסים משפטיים מקוונים**

* **הבסיס – טפסים סטנדרטיים**.
* **טפסים מותאמים אישית**.
* **"ממשקים חכמים"** (סרטון על ממשק Checkbot).
* **אופני תקשורת שונים**.

**מגוון רב של פעילויות משפטיות**

חברת **LegalZoom**

חברת **Wevorce**

**A2J Author**.

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

**Richard** ו-**Cass** כתבו ספר שנקרא **Nudge** – בו הם פרצו את הדרך לשאלה כיצד אנו משפיעים על החלטות של החברה באמצעות עיצוב המקום בו הם מקבלים את ההחלטה. כמה שנים אחריהם שלמה בן ארצי הוציא את הספר **The Smarter Screen** (גם ספר מומלץ), שיש בו דוגמאות מאלפות על איך הסביבה הדיגיטלית והממשק המקוון והאופן שבו הוא מעוצב, איך הוא משפיע על קבלת ההחלטות של האנשים.

**עו"ד צ'ט בוט – RoboLawyer** (נקרא גם Do not pay) (היה בחומרי הקריאה).

* חווית משתמש של שיחה אינטראקטיבית.
* עיבוד שפה טבעית.
* התאמה של מסמכים.
* הגשה מקוונת לרשות.

**שימוש בטכנולוגיה לצורך גילוי מסמכים מוקדם (E-Discovery)**

**למידת מכונה** – לימדו את האלגוריתם איך לבצע את ההערכה, ועל סמך מדגם זה ייצרו כללי פעולה עבור האלגוריתם, שאותם הוא מחיל על כמות אין סופית.

**LawGeex** מישראל עובדת עם יועצים משפטיים. (**AI vs. Lawyers**)

**ההשלכות על עבודת עו"ד**

1. עתיד מקצוע עריכת הדין ישלב בתוכו יותר ויותר שירותים היברידיים
2. תוכנות הE-Discovery - היום יש חברות שמספקות את זה כשירות מיקוד חוץ לעורכי דין.
3. כל תחום הערכת המסמכים והסתכלות על תוכן הטקסט, זה תחום חם ומתפוצץ.

**מערכות תומכות החלטה**

**Disputec** – שנותנת סטטיסטיקות לבתי דין לעבודה, והיא מקבלת תובנות על סמך תיקים שהתנהלו.

**נזיקליק** – מאפשרת לראות את סכום הפיצויים שנתבעו לפי כל הפרטים שהוכנסו למערכת.

**לסיכום**, נגישות משחקת תפקיד מרכזי, והשירותים המרכזיים המשפטיים נגישים בכל זמן ובכל שעה. זה פותח את הפתח לשינוי תפיסתי לגבי השירות המשפטי – כל פעולה/צורך משפטי מסוים יוכל להתפרק לרכיביו, ולא אצטרך ללכת בהכרח לעורך דין אחד. אפשר יהיה להרכיב לעצמי מארג של מספר נותני שירותים, בין אם כולם עורכי דין, ובין אם זה נעשה על ידי תוכנה באופן חלקי.

**קשיים בפיתוח מיזמים משפטיים טכנולוגיים**

* כללי ההסדרה המקצועיים של עורכי הדין – חוק לשכת עורכי הדין (1961) וכללי לשכת עורכי הדין (אתיקה מקצועית) – 1986
* הנורמות האתיות והמקצועיות התפתחו והתקבעו בעידן שבו הטכנולוגיות לא היו קיימות.
* ייחוד פעולות המקצוע – דברים שעורך דין בישראל יכול לעשות אבל לא שירות מקוון.
* איסור שיתוף בהכנסות או קבלת הפנייה של לקוח שנעשתה למטרות רווח.

**ס' 20 לחוק לשכת עוה"ד: ייחוד פעולות המקצוע**

חברות שעושות שימוש בתוכנות שעורכות מסמכים באופן אוטומטי, מסתכנות בתביעה.

**שירותים משפטיים מקוונים: הסגת גבול המקצוע?**

* מתן מידע משפטי באמצעות אתר מקוון אינו אסור כשלעצמו.
* **לעומת זאת**: ייעוץ משפטי או מתן חוות דעת משפטית ע"י מי שאינו עורך דין אסורים.
* ככל שהמידע כללי יותר ואינו מתייחס למקרה העובדתי הקונקרטי זה יהיה מתן מידע.
* ככל שהמידע נשען על הנסיבות הפרטניות של הפונה – זה יהיה ייעוץ.
* בנוסף, יש לבחון האם המידע/השירות/הייצוג בנסיבות המקרה הם משפטיים

**בהלכת "המרכז למימוש זכויות רפואיות"** - כשאנו צריכים להכריע בקו הגבול, אנו צריכים לבדוק אם זה שאלה **כללית או פרטנית?**

**אמות המידה שהשופטת ארבל קובעת:**

* אנו נבדוק מהו היקף שיקול הדעת שכרוך בביצוע השירות/הפעולה.
* אנחנו נבחן כתנאי שני מהו פוטנציאל הנזק שעלול להיגרם לציבור אם הוא יקבל שירות משפטי לקוי.
* שיקול מדיניות שלישי – נשקול מה החלופה שיש לציבור לממש את הזכויות אם אנו נאסור על מי שאינו עורך דין לספק את השירות הזה.

השופטת ארבל כן מכירה בפסק הדין בכך שהמציאות משתנה, ושיכול להיות שיהיה שינוי ששירותים נקודתיים יינתנו לציבור הרחב, אבל זה דורש אסדרה. עכשיו נמתין למחוקק.

**פס"ד דטהפקס**

למרות שזה לא מכונה כייעוץ משפטי, בפועל זה **כן ייעוץ משפטי**. נציגי החברה צריכים להתאים את המאמרים ללקוח, ועצם פעולת ההתאמה מצריכה ידע משפטי רב, כדי שיתאים למקרה הספציפי.