**5/3/18**

המטרה שלנו בקורס תהיה לספק מבט על שחוצה את גבולותיהם של תחומי משפט מובחנים או דוקטרינות משפטיות ספציפיות. נעסוק באופן ההסדרה ההדדי בין התחומים משפט וטכנולוגיה.

האינטרנט חדר לכל תחומי החיים, טכנולוגיות המידע בכלל חדרו גם הן והתפתחו זירות חדשות שתופסות נתח משמעותי בפעילות הכלכלית, החברתית, הפוליטית, המשפטית, המקצועית ולעיתים גם העבריינית או טרוריסטית.

**אוצר מילים:** ביג דאטה, חישוביות, אלגוריתמים, למידת מכונה, למידה עמוקה, רובוטים, מכונות אוטונומיות. האופן בו אותן מילים מגולמות למערכות שונות ומה ההיבטים המשפטיים, הנורמטיביים הכרוכים בהן.

יש קושי מובנה בהתמודדות עם סוגיות טכנולוגיות, משום שהקצב שבו הטכנולוגיה מתפתחת הוא מהיר ודינמי ביותר.

**\*חוק מור MOORE -** כוח המחשוב מכפיל עצמו כל 18 חודשים ויחד עם ההכפלה של כוח החישוב מגיעים ליכולות גבוהות של טכנולוגיה.

תהליכי השינוי שמחוללות טכנולוגיות המידע: דינמיים, מתרחשים בקצב ובעוצמה חסרי תקדים ואינם חד פעמיים. הפתרון לא נובע מתוך תגובה משפטית נקודתית לשינוי הטכנולוגי, אלא מתוך הבנה רחבה יותר מתוך עקרונות יסוד בסיסיים יותר:

1. עקרונות משפטיים ומושגי שסתום – פרשנות משפטית

2. הבנה של הקשר המורכב בין משפט וטכנולוגיה מאפשרת לפתח כלים משפטיים מתאימים

**האם יש צורך בפרדיגמה של משפט וטכנולוגיה?**

**\*פרדיגמה -** המערך הכולל של העמדות, התפיסות והשיטות שמגדירים את החשיבה המדעית בתקופה נתונה בתחום מסוים.

טענה אפשרית: הממשק בין משפט וטכנולוגיה נוגע בעיקר ליישום:

- החלת כללים משפטיים קיימים על טכנולוגיה חדשה

- עיצוב כללים משפטיים חדשים

למשל: דיני הגנת הצרכן ולהחיל אותם על מסחר אלקטרוני – זה דבר מורכב, ואין החלה אוטומטית זה לא מאפשר פשוט ליישם את הדין הקיים על הסיטואציה החדשה.

המוגבלות של המשפט כמענה אקסלוסיבי לאתגרים שהעולם הטכנולוגי מציב, ולכן לצורך של משפטנים לפתח הבנה של המרחב הזה ושל השיקולים הסובבים אותו.

**המטרה בקורס:** לפתח חשיבה פרדיגמטית על משפט וטכנולוגיה - מסגרת אנליטית לבחינת יחסי הגומלין בין משפט וטכנולוגיה ובכל סיטואציה מרגע שיש את הכלים הנכונים אנחנו יכולים לפתח את התגובה הראויה בסיטואציה הספציפית.

**מתי עולה צורך בחשיבה מסוג זה בעבודת המשפטן?**

- ניסוח חוזים ותקנונים לאתרי אינטרנט (הסכמה מדעת, חוזה אחיד, נגישות בינלאומית וכו')

- קבלת החלטות מינהליות ושיפוטיות

- הבנה ופרשנות של סטנדרטים משפטיים (ואחרים)

- חקיקה של תקינה טכנולוגית

- עיצוב מדיניות בכל תחום שכולל ממשק טכנולוגי

- מעורבות תומכת בעיצוב טכנולוגיה

מעורבות של עורכי דין עצמם בעיצוב של טכנולוגיות חדשות, אמצעים טכנולוגיים ובליווי של פיתוח טכנולוגיות חדשות.

האופן שבו המשפט מגיב לשינויים טכנולוגיים:

התפתחויות טכנולוגיות מאלצות את מערכת המשפט לבחון את התאמתם של כללים משפטיים קיימים למציאות חדשה.

למשל: תעמולת בחירות – שנת 2001 האם העובדה שחבר כנסת עונה לשאלות של גולשים באתר של עיתון האם זה מהווה תעמולה לפי ס' 17ב לחוק הבחירות (דרכי תעמולה). המתווה הכללי הוא ערוצי תקשורת מחויבים להקצות לכל מפלגה זמן שידור לתשדירי תעמולה. מדובר על אמצעי התקשורת המסורתיים: טלוויזיה, רדיו ועיתונות. נשאלת השאלה במה האינטרנט שונה מהם: מצד אחד – באינטרנט אין מחסור בערוצי שידור ובזמן שידור, אבל מצד שני – קיימים חסמים אחרים: עיצוב תוצאות החיפוש של מנועי החיפוש, העדפה של ספקי שירות לתכנים ממקור מסוים/שימוש בתוכנות סינון וגישה למידע אישי על הבוחרים: הצלבה ועיבוד לצורך השגת יתרון בתעמולת הבחירות. תעמולה בעולם האינטרנט מצריכה שיקולים אחרים. השופט חשין התייחס לסוגיה הזו.

המשפט כמעצב טכנולוגיה

המשפט מסדיר התפתחויות טכנולוגיות בצורה משמעותית – התערבות משפטית יכולה להשפיע על סוג הטכנולוגיות המותרות בשימוש, על האופן שבו יישמו אותם, על עלות הפעלתן ועל היתכנותן של טכנולוגיות חלופיות. לדוגמה:

- מגבלות בחוק על פיתוח וייצור טכנולוגיות: סוגים שונים של הצפנה או פריצת מנעולים טכנולוגיים שנועדו להגן על זכויות יוצרים.

- מתן תמריצים לפיתוח טכנולוגיות מסוג מסוים: החובה לאבטח מידע שמוטלת על מאגרי מידע שיש בהם מידע פרטי (ס' 17 לחוק הגנת הפרטיות) – תמריץ לפיתוח מערכות הגנה.

- הטלת אחריות משפטית בגין שימוש בטכנולוגיה אחת יכולה לעודד פיתוח של טכנולוגיות אחרות:

א. נפסטר – חברה לתוכנה לשיתוף קבצים – החברה נמצאה אחראית שהייתה צריכה להיות לה ידיעה על הפרות זכויות יוצרים של הקבצים)

ב. איימסטר - חברה שהצפינה את כל התקשורת בתוך המערכת שלה כדי לטעון שלא יכולה להיות לה ידיעה על הפרות זכויות יוצרים שמתרחשות, ביהמ"ש פסל את הפרקטיקה הזו.

ג. כך נולדה פלטפורמה של שיתוף קבצים מבוזר – מלקוח אחד ללקוח אחר + תוכנה חופשית + Creative commons גם המשפט תורם להתפתחות הטכנולוגיה והתמורה אינה רק שלילית, אלא גם חיובית וזו גם התפחתות של מודלים כלכליים חדשים כמו תוכנות Open Source ו Creative commons רשיונות של זכויות קניין רוחני כדי שלא יהיה ניתן לעקוף את דיני זכויות היוצרים.

**שינויים במשפט כמוסד בעידן טכנולוגיות המידע:**

המשפט ככלי להסדרת התנהגות ואכיפה משתנה בעידן הטכנולוגיה וקמים לו מתחרים פרטיים. ההסדרה ע"י גופים פרטיים ובאמצעות טכנולוגיה יהיה נושאים מרכזיים שנדון בהם בקורס. למשל: EBAY מסחר אינטרנטי. הבעיה שנתקלו בה מוכרים וקונים שביצעו עסקאות על גבי מסחר מקוון היא שאם היה סכסוך לא היה אמצעי אמיתי לפתרון הבעיה, וזה הוליד תעשייה של יישוב סכסוכים מקוון (כמו עלי אקספרס). ממנה הגיעה זליגה לקמת מערכות מקוונות ליישוב סכסוכים שלא משרתות רק פעילויות אינטרנטיות, אלא גם פעילויות פיזיות לחלוטין. למשל: מערכות לגירושים, מיסים, תביעות קטנות, תשלומים, עבירות תנועה, הגנת הצרכן ועוד.

- 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 ובין הסדרה ציבורית

- דוגמה: 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 IN LAW:

1) מערת המשפט, כללים משפטיים שמסדירים באופן ישיר את הפעילות ומשפיעים עליה גם באמצעות השפעתם העקיפה על השוק, הטגנולוכיה והנורמות החברתיות.

2) כוחות השוק, שפועלים ומשפיעים על הפעילות האנושית – למשל: יכולת כלכלית שקובעת אפ דבר הינו אפשרי או לא בסיטואציה נתונה.

3) נורמות חברתיות שמסדירות את מה שמקובל בהתנהלות האנושית, למשל: הנורמה של פרסום תמונה של חבר בפייסבוק.

4) הטכנולוגיה עצמה CODE - בשנת 1999 לסיג דיבר על הקוד של התוכנה, היום אנחנו יכולים לדבר על האינטרקציה של הקוד של התוכנה: רובוטים, רחפנים, מכוניות אוטונומיות ועוד. ה

משמעות של הפעולה המרובעת על הפעילות האנושית – מי שרוצה להסדיר ולעצב את המדיניות האנושית יש לו סל כלים עשיר. הפתרונות המשפטיים האלה לכשעצמם מציעים מענה חלקי ביותר בסיטואציה הספציפית. למשל: המקרה של חשיפת ילדים לתכנים פוגעניים באינטרנט. יש פתרונות שוקיים שיכולים להתפתח, למשל: תוכנות סינון שמונעות מילדים גישה לתכנים מסוימים (בביה"ס או בבית), היכולת של הטכנולוגיה לזהות מראש את טיב התוכן היא מוגבלת ולא מדויקת.

- החוק הוא לא תמיד פתרון המיטבי או ההכרחי לסוגיה.

- לעיתים די בכוחות השוק או בנורמות החברתיות או בטכנולוגיה.

עד כמה זה בסדר שמערכת המשפט תיתן אכיפה ושיטור לגורמים פרטיים (ספקית האינטרנט)? האם הערכים שמשקפים את קוד התוכנה משקפים את הערכים החברתיים ואיך אפשר לפקח על זה? רואים באינטרנט לא רק כלי יישום ניטרלי בידי המשפט, אלא כלי שמגלם בתוכו ערכים שלרוב הם סמויים מן העין.

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

משולש של המשפט, הטכנולוגיה והערכים – בין הטכנולוגיה וערכים יש קשר לא אינסטרומנטלי נטו, כל קשר מגללם ערכים מסויימים ואותה מערכת יחסים בין המשפט לטכנולוגיה.

גישה אינסטרומנטלית, גישה מהותנית ותורת המשפט והפרשנות.

**שלבים בהתפתחות הטכנולוגיות הדיגיטליות:**

- האינטרנט של הדברים וכלכלת המידע

- מכוניות אוטונומיות

**דרישות הקורס:**

- בחינה – 100% ציון

- מקרי מבחן של טכנולוגיות שונות

- מרצים אורחים

- מיטיב (השתתפות)

**12/3/18**

**יש שתי גישות של המשפט:**

1. הגישה הדטרמינסטית-אינסטרומנטלית – כופרת בקיומו של קשר בין משפט וטכנולוגיה, הטכנולוגיה לא מגלמת ערכים מוסריים או בחירות נורמטיביות, אלא היא פונקציונליות ומכשירנית ומגשימה את רצונותיו של המשתמש. תפקיד הטכנולוגיה הוא לאפשר למשתמש להגשים מטרה כשלעצמה היא חסרת טבע מוסרי והיא אדישה למטרות השונות שניתן להשיג באמצעותה. אדם יכול להשתמש בה באופן חיובי או שלילי. אין אפשרות לעצב את הטכנולוגיה כמכשיר משפטי, היא מתפתחת בהתאם לכללים משל עצמה, ללא אינטראקציה עם גורמים אחרים. זו גישה מיושנת שקשה למצוא לה תומכים בדורנו.

הגישה המקובלת כיום היא הגישה המהותנית שמסתכלת על הטכנולוגיה באופן מהותי.

2. הגישה המהותנית-ערכית – הטכנולוגיה עצמה, העיצוב והמנגנונים שעומדים בבסיסה הם לא נייטרלים, הם כשלעצמם אינם רק מכשיר וכלי יישומי, אלא מגלמת בתוכה בחירות ערכיות נורמטיביות של המתכננים שלה ואולי גם כאלה שלא תוכננו במכוון, נמצאים בה ויש להם השפעה ממשית גם אם היא בלתי צפויה. סומיולוגים ופילוסופים של טכנולוגיה מצביעים על כך שהטכנולוגיה מגלמת בתוכה ערכים באופן עקיף וישיר:

- באופן עקיף – הטכנולוגיה מתפתחת במענה לצרכים של החברה מתוך התכנית והסוגיות שמעסיקים את חבריה.

- באופן ישיר – טכנולוגיה שמתוכננת בכוונת מכוון לגלם ערך מסוים. למשל: תוכנות סינון שנועדו לאפשר בקרה הורית להגן מפני תכנים פוגעניים או לאפשר למשתמשים שימושים קהלתניי בטכנולוגיה. ארכיטקטורת האינטרנט כרשת נטולת מרכז אחד – אוסף של "צינורות" תקשורת נתונים מקצה לקצה מגלמת ערכים של ביזור – היעדר שליטה מרכזית.

לעיתים המשמעות של הטכנולוגיה נקבעת בדיעבד, לא רק על ידי המתכנתים והמפתחים, אלא גם ע"י המשתמשים.

**שלבים בהתפתחות הטכנולוגית הדיגיטליות:**

- תחילה ראינו את האינטרנט כפלטפורמה לתקשורת בינאישית – הפצה של מסרים: דוא"ל, לוחות מודעות ופורומים, מתן שירותים: מתווכים, מנועי חיפוש, מדיה חברתית וכלכלה שיתופית.

- בהמשך ראינו את ההתפתחות הטכנולוגית, הדיגיטציה, של המוצרים עצמם – האינטרנט כרשת להפצה של מוצרים: הורדת קבצים כתחליף לעותקים מוחשיים (מוזיקה, וידאו, תוכנות, ספרים וחדשות), התרחבות של הכלכלה השיתופית (UBBER – מאפשרת לכל אדם להפוך לנהג מונית ולהשתמש ברכבו הפרטי לצורך כך) וביזור באיחסון ובעיבוד של מידע.

- השלב האחרון הוא האינטרנט של הדברים וכלכלת המידע –

1. האינטרנט כרשת של תקשורת עם "דברים": מכשירים חכמים, טכנולוגיית מידע ICT מתרחבות לכלל תחומי החיים (חיישנים מתקדמים, סטנדרט תקשורת סלולרית).

2. יכולות עיבוד שהתפתחו מאוד והביאו לאלגוריתמים לתמיכה בהחלטות/לקבלת החלטות, הטכנולוגיות הללו הולכות ונעשות מורכבות יותר עם התקדמות בכוח המחשוב והידע שלנו בתחומים כמו: ביג דאטה (ביצוע תחזיות על סמך כמויות עתירות מידע), אינטיליגנציה מלאכותית, למידת מכונה, ולמידה עמוקה, אינטראקציה בין תוכנה לחומרה - רובוטים ומערכות אוטונומיות יכולים להחליף פעולות של בני אדם (פעולות בעולם הפיזי). חזון הבית החכם שהוצג עד לא מזמן כמשהו עתידני קורם עור וגידים. הדבר משפיע גם על מקצועות מסוימים כמו אפסנאות, נהגים, גם מקצוע עריכת הדין.

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

סיפור על שני אנשים שמגלם את שתי הזוויות שאנו נרצה לעסוק בהם בקורס. מצד אחד, האתגרים של הטכנולוגיה והעולם המקובל, ההתמודדות של מערכת המשפט או של מערכות חלופיות אחרות שמשתתפות ברגולציה שלהם ומצד שני מהם הכלים שהטכנולוגיה מאפשרת לעולם המשפט כדי לבצע את אותן פעולות ולהגשים את אותן תכליות של עולם המשפט (להכווין התנהגות, להסביר את מערכות היחסים של פרטים).

**\*קולין רול –** הוא מייסד של תחום יישוב הסכסוכים של איביי. האתגר של קולין בחברת איביי היה קונים ומוכרים רבים שרצו לבצע עסקאות רבות במערכת שנתקלו בבעיה רצינית אם משהו השתבש (החבילה איחרה להגיע, אם המוצר היה שבור או בצבע הלא נכון). הקושי היה שהיו **60 מיליון סכסוכים** בשנה, וכיאה לפלטפורמה מקוונת שהמוכר ממדינה אחת והקונה ממדינה אחרת לא היה ברור מה **סכמות השיפוט** ובהיעדר פתרון משמעותי למשתמשים במערכת לא היה **אמון** והיה חשש עסקי שהם ינטשו את הפלטפורמה ולא יחזרו לבצע עסקאות. נוכח כמות הסכסוכים הגדולה ו**השווי הנמוך** שלהם 100 דולר היה ברור שהפתרון של פניה לבימ"ש או אפילו למגשר/בורר באופן פרטי הוא לא ישים.

**\*מייקל בריגס -** הוא לורד צדק ושופט בבימ"ש העליון באנגליה שהופקד על הרפורמה במערכת המשפט האזרחית באנגליה וב2016 הוציא דו"ח על שמו שהמלצתו המרכזית הייתה הקמת תיקים מקוונים עבור הליכים אזרחיים במערכת בתי המשפט באנגליה. הבעיה של בריגס הייתה העובדה שבמעררכת המשפט האנגלית יש כמות עצומה של מייצגים עצמיים – אנשים שניגשים למערכת המשפט ללא עורך דין משום שהשירותים המשפטיים מאוד יקרים, והמערכת עצמה מתמודדת עם עומס תיקים גדול כך שיש עיכובים בניהול התיקים והביקורת הגדולה על מערכת המשפט היא הנגישות אליה. הלורד בריגס חשב שהפתרון של הבעיה הוא בהקמת בתי משפט מקוונים – גבול הסמכות של ביהמ"ש המקוון יהיה 25 אלף פאונד, תביעה קטנה באנגליה זה 10 אלף פאונד. כלומר, מדובר בפתרון ממשי עבור כמות גדולה מהתיקים האזרחיים במדינה,

**ODR יישוב סכסוכים מקוון –** העלייה בשימוש בשירותים מקוונים באופן כללי והצורך בפתרון יעיל ואפקטיבי ליישוב סכסוכים. המערכת של איביי והמערכת של לורד בריגס אלו רק שתי דוגמאות מתוך שורה של מערכות שמאפשרות להשלים את כל הליך הסכסוך מפתיחת ההליך (הגשת תביעה/תלונה) ועד להכרעה בעניין של צד שלישי או הסכמה של הצדדים במו"מ על התוצאה. לעיתים מתאפשרת גם אכיפה באופן מקוון.

מדובר במונח מסגרת רחב שמתייחס לסכסוכים שמקורם לא רק בסביבה המקוונת, למשל: תביעות צרכניות, תביעות אזרחיות עד סכום מסוים, גיבוש הסכם גירושין, ערעורי מיסים, תיקי תנועה, סכסוכים קניינים, הסכמי עבודה. גם שיטות יישוב סכסוכים הן שיטות מגוונות: מו"מ, גישור, בורוות, הכרעה שיפוטית ומודלים חדשים של מושבעים (מיקור המון של החלטות). הטכנולוגיות הן מגוונות ותכנון התהליכים הוא מגוון לכשעצמו (ההליך הפרוצדורלי מגוון).

**רקע להתפתחות תחום יישוב הסכסוכים באופן מקוון:**

- העידן הדיגיטלי – שירותים רבים מסופקים באופן מקוון, נגישות ומסוגלות טכנולוגית ואפילו ציפייה לשירותים מקוונים (ממשל זמין – היכולת להשלים פעולות מול הממשל באינטרנט), זירה חדשה של מערכות יחסים עסקיות, אישיות ואחרות – סוג חדש של סכסוכים. יזמות ביזור מוקדי הכוח, ועדיין קיימים פערים בנגישות טכנולוגית.

הפנייה לעידן הדיגיטלי הולידה סכסוכים חדשים שהפתרון להם נוצר באותה מערכת יחסים שבו הסכסוך נוצר.

- תנועת הנגישות לצדק ותנועת הADR (דרכים חלופיות ליישוב סכסוכים) – הגמישות התהליכית והנגישות והעלות המופחתת שמלווה את ההליך פגשה את עולם הסכסוכים המקוונים התחברה עם כוח חברתי חזק – תנועת הנגישות לצדק והתנועה ליישוב סכסוכים בדרכים חלופיות כאשר הרעיון היה לאפשר להשתמש בטכנולוגיה כדי להנגיש תהליכים להתאים אותם למה שמעניין וחשוב לצדדים לסכסוך ולאפשר להם דרך מהירה, זולה ונגישה לפתרון סכסוכים. הדבר המעניין הוא שתנועת הADR שהחלה בשנות ה-60 נכנסה למערכת המשפט בשנות ה-80 בתהליך הדרגתי גם הגישור והבוררות חדרו למערכת המשפט ונעשים בחסות בתי המשפט. באופן דומה גם מערכות הODR שהחלו כמענה לצרכים עסקיים מצאו את דרכם בתוך מערכת המשפט.

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

- חשיבות רבה להקשר של הסכסוך, לתהליך ולסוג הטכנולוגיה:

1. סכסוך: מסחר מקוון, משפחה, עבודה, עסקי?| מורכבות|היכן נולד?

2. הקשר: פרטי או ציבורי?| מדינתי או בינ"ל| ספק שירות- עצמאי, מתווך, מוסדי?

3. תהליך: שיטת יישוב הסכסוך | עושר הערוץ התקשורתי | סינכרוניות | אוטונומיות?

המוקד שלנו - השפעת הטכנולוגיה על ההליך.

**מערכת הODR כצד רביעי וכצד שלישי בסכסוך:**

**\*Ethan Katsh & Janet Rifkin (2000) -**

מאמר שבו טבעו את המושג "הצד הרביעי", הטכנולוגיה משמשת כצד הנוסף והמרכזי שמשפיע על הסכסוך לצד הבורר/שופט שמסייע לצדדים. מקרה פרטי של המונח שטבע לסיג CODE IS LAW. עיצוב הממשק והמערכת הטכנולוגית משפיעים על הליך יישוב הסכסוך, ההשפעה אינה ניטרלית בהכרח ולרוב אינה שקופה למשתמש.

תפקיד אינסטרומנטלי - מערכת ODR כצד רביעי בלבד – מופעלת ע"י אדם, למשל: אמצעי תקשורת, כלי לביצוע משימות קונקטריות.

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

**מודלים טכנולוגיים בהליכי יישוב סכסוכים:**

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

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

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

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

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

**19/3/18**

איביי פיתחה את המערכת שנחשבת ע"י רבים בתחום כמערכת הOBR הפרדיגמטית כי זה איזשהו מקרה מבחן שמדגים את ההיווצרות של צרכים חדשים בגלל הפעילות ברשת ובמקביל את הפתרונות שטכנולוגיית המידע יכולה לספק לבעיות האלה. פלטפורמה למסחר מקוון, מוכרים וקונים מכל העולם שמשתמשים בזירת התיווך של איביי כדי לערוך עסקאות. בתחילת שנות ה-2000 יש בבת אחת כמות גדולה מאוד של אינטראקציות וסכסוכים, אין הרבה ניסיון לחברות, למשתמשים שלה. היה אינטרס לייצר סביבה עסקית בטוחה שיהיה ניתן לתת בה אמון. הם מתמודדים עם:

- 60 מיליון סכסוכים בשנה

- השווי שלהם היה נמוך 100$ ולכן לא היה פתרון באוף ליין

- יחסי עלות תועלת של פתרון ע"י מגשר/בורר אנושי – בלתי סביר כלכלית

- ריחוק פיזי בין מוכרים לקונים: קושי מעשי + ספק לגבי סמכות שיפוט

- צורך בהטחת סביבה מסחרית בטוחה ואמינה כדי לעודד עסקאות

\*יש בעיה מרכזית של סמכות שיפוט שנכונה לכל הרשת, האם איפה שנמצא השרת? האם איפה שאיביי רשומה? האם במדינת הנתבע/תובע?

\*רייטינג/פידבק למוכרים מסייע בהרתעה והכוונת התנהגות – האם ניתן לסמוך על אותו מוכר או לא, בשיטת הרייטינג היה ניתן להתגבר על הפער של היעדר המידע והמוניטין. בתוך איביי יש מערכת ליישוב סכסוכים על פידבקים – מוכרים שחושים שניתן להם פידבק שלילי יכולים לבקש הליך יישוב סכסוך כדי להסיר את הפידבק השלילי ולא לפגוע במוניטין שלהם. מערכת הפידבק לא נתנה פתרון ממצה ולא יצרה סביבה מספיק בטוחה ומכאן הגיעה מערכת יישוב סכסוכים.

**מה מייחד את איביי כצד שלישי ליישוב סכסוך?**

- שיקולים עסקיים, מסחריים

יש לאיביי נראות לכל שלבי התהליך של היווצרות העסקה וכריתת החוזה, של התנאים שהוסכמו, של תנאי התשלום וגם ידיעה מאוד טובה לגבי הסכסוך עצמו, פתרונות ואמצעי אכיפה. בגלל שלאיביי יש מסד נתונים עצום של כל הליכי הסכסוך במשך השנים במערכת שלה, יש לה כמות נתונים שמאפשרת ללמוד את דפוסי הסכסוך ולבנות תהליכים שמונעים היווצרות של סכסוכים ופותרים בהצלחה באופן אוטומטי שיעור גדול מאוד מהסכסוכים.

**מערכת יישוב הסכסוכים של איביי:**

1. אבחון הסכסוך

2. מו"מ/גישור מתווך טכנולוגית

3. גישור/בוררות ע"י נציג החברה

4. 90% מהסכסוכים פותרים ללא מעורבות גורם אנושי מטעם החברה

**מערכת לומדת, מבוססת נתונים:**

- ניתוח הנתונים לצורך זיהוי דפוסי מחלוקת, המידע הנחוץ לפתרונם, ופתרונות שיש סבירות גבוהה לקבלתם > עצי החלטה לתהליך המו"מ.

- פרסונליזציה סטטיסטית – גם על סמך מידע שלא נמסר ע"י הצדדים לסכסוך הספציפי, על סמך הידיעה שאני פיתחתי כמערכת לומדת מאינספור סכסוכים קודמים שהיו להם מאפיינים דומים.

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

יש למערכות הללו חסרונות ויש חששות בתור מי שאמונים על האינטרס הציבורי, למשל: פגיעה בפרטיות ע"י חשיפת פרטים אישיים, הפרטת האכיפה, חוסר אובייקטיביות של הגוף הפרטי (אינטרסים כלכליים והעדפה של צד מסוים), צדק הוא לא בהכרח צדק פוזיטיבי (אין מענה למקרים חריגים).

**חששות וסיכונים:**

- Code is Law המודל של לסיג לגבי השפעות של המערכת על ההתנהגות האנושית. טכנולוגיה אינה ניטרלית: היעדר שקיפות לגבי אופן פעולת המערכת (ניתוב הסכסוכים, הצעות פשרה), היעדר שקיפות ביחס לתוצאות.

- 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 פרוצדורלי, בדומה לתווי תקן בתחום התשלום/אבטחה. לא יכולים לאמוד את אופן הפעילות, המודל של תו הוא מודל מקובל.

- רגולציה עצמית – סטנדרטים אתיים שיפותחו ע"י התעשייה עצמה.

- סטנדרטים מומלצים – למשל, הABA התווה עקרונות לנתוני שירותי ODR.

- מודל מסלקה – גורם מרכזי ינתב סכסוכים למערכות ODR שאושרו (לנותן השירות הספציפי).

- הסדרה ציבורית באמנות/הסכמים/חקיקה – הדירקטיבה האירופאית, בנושא ADR והתקנה בנושא ODR. בין מדינות האיחוד השונות יצרו הוראה שמחייבת יצירה של פורטלי גישור מקוונים להליך יישוב הסכסוך – זה רק להגשת התלונה, אבל לא לכל ההליך. כללי מודל לODR של UNCITRAL של האו"ם – תקינה למסחר בינאלומי מייצר נוסח כללי שניתן להתחייב אליו חוזית, 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 – בתי המשפט לא נגישים מספיק עבור צדדים בהליכים אזרחיים מסיבות רבות, בעיקרן העלות הגבוה מאוד של ייצוג משפטי באנגליה ושל ניהול הליכים והקושי של מייצגים עצמיים, תובעים או כנתבעים ללא ייצוג של עורך דין. הלורד בריגס פרסם דו"ח ב2016 שבו המלצות למערכת המשפט כשהעיקרית שבהן הייתה המלצה להקמת בימ"ש מקוון לכל ההליכים האזרחיים עד גבול סמכות של 25,000 פאונד. הרעיון היה לקחת את התפיסות הצרכניות של איביי ולהשתמש בהליכים האזרחיים.

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

בסוגים שונים של הליכים משפטיים, בעיקר באנגליה ובארה"ב, יש אחוזים מאוד גדולים של מייצגים עצמיים. הסיבות לכך מגוונות: אנשים שרגילים לתרבות "עשה זאת בעצמך", עלות הייצוג, מיעוט משאבים לסיוע משפטי, חוסר אמון בעו"ד, צרכנות, אינדיבידואליזם וטלוויזיה.

אחד מהשיקולים של היעילות והנגישות הטכניים היא שאדם מן השורה לא יודע לנסח את טיעוניו בבית המשפט באופן שמצופה ממנו. מערכת המשפט סדרי הדין והדין המהותי עוצבו ונוסחו באופן שנועד להפעלה ע"י 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- בחלק מהמקרים יותר מ50% נמחקים על הסך- שיעור הצלחה נמוכים יותר מאשר למיוצגים משפטית |
| אתיקה:- הללים 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 ביהמ"ש – השתקה- תחושות בלבלול, הצפה, תסכול, חששות |

חסמי גישה כלליים: זמן, מקום ומשאבים.

**השופט בריגס הציע דרך להתמודד עם הבעיות הללו ע"י מודל ביהמ"ש המקוון:**

שלב 1: (אוטונומי)

- סיוע בניסוח התיק באופן סדור כך שיובן ע"י בעלי הדין שכנגד וביהמ"ש

- הוספת כלל המסמכים והראיות הרלוונטיים בתיק

שלב 2: ניהול תיק וניסיונות פישור (אינסטרומנטלי)

- ע"י תפקידן בביהמ"ש – יתחיל באופן מקוון ובמידת הצורך פנים אל פנים

שלב 3: הכרעה ע"י שופט (אינסטרומנטלי)

- באופן מקוון: על סמך המסמכים בלבד או לאחר דיון אודיו/וידאו - בטלפון

- במידת הצורך לאחר דיון פנים אל פנים באולם ביהמ"ש

**המודל של בריגס מתבסס על מערכת שעובדת בקנדה במחוז בריטיש קולומביה – מודל הטריבונל האזרחי:**

- המערכת של בריגס היא חסרת תקדים בהיקף שלה – תביעות אזרחיות עד 25 אלף פאונד ואילו המערכת בקנדה מוגבלת לתביעות קטנות, עבירות תנועה וסכסוכים מסוימים קנייניים.

- למערכת בקנדה יש שלב נוסף של אבחון סכסוך ופתרונות מחוץ לביהמ"ש – לפני שמגישים תביעה לביהמ"ש ייתכן שקיים פתרון אחר, במיוחד כשמדובר בצדדים בלתי מיוצגים, ניתן לפנות לגורם ממשלתי או להציג מכתב דרישה לנתבע.

- בקנדה יש אבחון אוטומטי לפי שאלות החלטה, ביחס לפעולות משפטיות או אחרות שאותו פונה יכול לנקוט בהן כדי לפתור את הבעיה שבגללה הגיע לביהמ"ש.

**יתרונות המודלים המקוונים להליכים שיפוטיים:**

1. יתרונות הליכים אסינכרוניים:

- עבור בעלי הדין: חסמים פיזיים – גישה 24/7 מכל מקום, איכות ההשתתפות בהליך

- עבור המערכת המשפטית – ניהול משאבי מקום וזמן שיפוטי, עלות תשתית נמוכה

2. יתרונות בניית התהליך המחודשת:

- פישוט והדרכה, מניעת טעויות, ניהול המידע

- ניהול תיקים יעיל

3. מתן סיוע משפטי בזמן אמת

4. 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:

- תיאוריית עושר המידע Daft & Langel 1984– להעברת מסר מורכב דרוש אמצעי תקשורת "עשיר", להעברת מסר פשוט די באמצעי "דל". תקשורת פנים אל פנים, וידאו, אודיו, כתב.

- האם ניתן להפיק צדק באופן ממוכן?

- האם השימוש באוטומציה שונה בהליכים מחייבים לעומת מייעצים?

- שמירה על ליגיטימיות 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 ופונקציית תומכת החלטה ולא מחליטה, ממשק המשתמש ואופן עיבוד המידע הם כולם יוצרים ארכיטקטורות בחירה, זה מבנה 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.מרחב ציבורי וירטואלי בו כל אדם יכול לקחת חלק פעיל בשיח הציבורי.

התפישה של האינטרנט כמקדם חופש מידע וביטוי נשענה על ההנחה שאופייה המבוזר של רשת האינטרנט הוא אנטיתזה לריכוז השליטה בידי אמצעי תקשורת מעטים.

- חסמי הכניסה לאינטרנט נמוכים: אין צורך בהקצאת ערוצי שידור, ולכן גם לא ברישוי ובפיקוח הנלווים לכך. עלות מינימלית להפצת תוכן ברשת. ביטול התלות במסננת העריכה של אמצעי התקשורת המסורתיים: יותר משתתפים בשיח.

- בניגוד לעיתונות, הטלוויזיה והרדיו המגדירים עבור הקורא את סדר היום, לגולש באינטרנט נתונה האוטונומיה 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 הרשת היה שלא יהיו חסמים על אופן זרימת המידע ושכוחות השוק לא יכתיבו איזה מידע אני אראה קודם או בכלל. בפועל, כמות המידע באינטרנט ואפשרויות הפעולה הן כל כך גדולות כך שאין נגישות אמיתית לכולו. התוצאות שמופיעות במנוע החיפוש בדף הראשון, בדף השני – מכתיבות את האופן שבו ניגש למידע שקיים ברשת. המתווך הוא מנוע החיפוש בו אנו תלויים כדי לדלות את המידע, ההחלטות שהמתווך הזה מקבל משפיעות על תמונת העולם שאני כמחפש מקבל – שיטת קידום האתרים של מנועי החיפוש.

העובדה שמתווכים שונים כמו זירות המסחר, מנועי החיפוש ומפיצי התוכן הם תאגידים פרטיים שפועלים באופן שלא שקוף למשתמש מעצבת בפועל את סביבת הפעילות עבור המשתמשים ברשת. אחת הסוגיות בעולם המקוון היא גם להבין וגם לפקח בצורה הנכונה על האופן שבו המתווכים ברשת מבנים את הפעילות בה.

**מתווכים ברשת האינטרנט:**

- הגדרה: 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, למשל: בזק, נט ויז'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/המוצר בעצמה)

- מערכות תשלום מקוונות

- פלטפורמות להפצת תוכן אשר לא יוצרות את התכנים המופצים בעצמן

- מדיה חברתית

**\*מאמר של אורלי לובל:** היא מדברת על שלושה דורות -

1. הדור הראשון: מתווכים שמאפשרים שיתוף וקישור למידע וידע, למשל: מנועי חיפוש כמו גוגל ויאהו.

2. הדור השני: זירות מסחר ושירותים כמו איביי ואמזון, שירותי החלפת קבצים כמו נאפסטר. חברות אלו הובילו לשינויים משמעותיים בתעשייה ההוצאה לאור, ערוצי חדשות ומדיה, מוזיקה וקמעונאות.

3. הדור השלישי: חברות פלטפורמה – מתן גישה לשירותים במרחב הלא מקוון, במחיר נמוך משמעותית ותוך התאמה אישית גדולה יותר > הטכנולוגיה משנה את האופן שבו ניתנים שירותים ונערכות עסקאות בעולם הפיזי. דוגמאות: BNB AIR לתעשיית המלונאות, UBBER לתעשיית המוניות, EAT WITH למכור ארוחות בבית כמו מסעדות.

**שאלות משפטיות מרכזיות ביחס למתווכים:**

- באיזו מידה מתווכים 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. האם לאדם יש אחריות אם הוצאה לשון הרע בפרסום שלו, האם מעבר לכך הפלטפורמה שאיפשרה את הפרסום הזה תהיה אחראית.

- באיזו 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? אורלי לובל The Law of the Platform בעולם של תעשיות קיימות כמו תיירות או תחבורה, למשל UBER או AIR BNB.

**9/4/18**

**עו"ד עמית אשכנזי, היועץ המשפטי של מערך הסייבר הלאומי:**

מה עושה הממשלה בנושא סייבר? בצד המשפטי מה עושים בתחום הגנת הסייבר?

מטה הסייבר הלאומי הוקם במשרד רוה"מ ב2011, ואוחד לגוף חדש של מערך הסייבר הלאומי, מונה כ200 איש.

**הגדרות:**

\*הגנת סייבר – פעילות לצורך שמירה על תפקודן התקין של מערכות מחשב, המידע בהן והתקשורת ביניהן בארגונים, במגזרי המשק ובמדינה. ללא עיסוק בתוכן.

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

**סייבר אינטרנט – הפעילות בממד התוכן "דיני מידע":**

דינים שמסדירים מידע כמו דיני לשון הרע וזכויות יוצרים, דיני פרטיות התאימו אותם לעידן המידע שהמידע נוסע ברשתות התקשורת והמחשבים. זה התחיל בשאלות עקרוניות כמו לסיג, האם למרחב האינטרנט צריך דינים חדשים או להתאים את הדין הקיים (יש התייחסות בחוק הפרטיות, חוק זכויות יוצרים וחוק לשון הרע).

חוק המחשבים – חוקק לעידן המידע, נשאלת השאלה למה המחוקק הסדיר זאת בחוק מיוחד. המעשים שהוא מסדיר כמעשים אסורים הם קשורים ללא קשר למחשב, אלא הערך המוגן של המחשב והתפקיד החברתי שלו הוא מיוחד ולכן צריך לחוקק חוק ייעודי לכך.

חוק הסרטונים – חוק חדש שחוקקו לגבי סרטונים שמופצים ברשתות החברתיות, בחקיקה של חוק מיוחד סימנו שזה חשוב כאינטרס ציבורי.

אחריות המתווכים – דילמת האכיפה של האינטרנט היכולת של אדם לקבל מידע או להפיצו ולגרום לעבירות אנונימיות, גרמה לזה שיהיה יותר יעיל לאכוף באמצעות המתווכים (מעבירי המידע) ואז עולה שאלת אחריות המתווכים (יו טיוב, גוגל, פייסבוק). אז אני יכול לתבוע דרכם. מצד שניף בשלב מוקדם של המשחק כדי לאפשר את התנועה של חופש הביטוי, הארגונים האלה קיבלו חסינות כזו או אחרת בחלק מהשיטו בעולם כדי לאפשר הפצת מידע. הנרטיב המשפטי שליווה את התקופה הזו היה אופטימי שבו התפקיד של המשפט בהסדרת האינטרנט הוא תפקיד פסיבי, גם בפן של המשפט החוקתי. צריך להשאיר את זה להסדרה פרטית. זה תקופת דיני תנאי השימוש (עד לאחרונה).

היה דיבור על זה ש"המשפט הוא גרוע" וצריך לתת לשוק לפתח את התעשייה ממנה אנחנו נהנים, של פיתוח אפליקציות ותוכנות, שכולן יציר השוק פרטי והמשפט הפרטי. ואז קרו שני דברים:

1. התפיסה הטובה על האינטרנט התפוגגה בעקבות אדוארד סנודן עובד של סוכנות האמריקנית NSA איך הממשל האמריקני אוסף מידע מודיעיני דרך האינטרנט. הדבר הזה הביא למשבר אמון שהאינטרנט הוא מקום פתוח וחופשי שהממשלה לא נמצאת בו.

2. איומי הסייבר – האינטרנט הפך למקום פחות בטוח ונשאלה שאלה עקרונית כמו שאנחנו מצפים מהמדינה להגן עלינו במרחב הפיזי, מה לגבי הגנה במרחב הסייבר?

למה מדינות מתעניינות במה שקורה באינטרנט?

כשאנחנו גולשים באינטרנט אתם חיברתם את המחשב לעולם והעולם "גולש" אלינו למכשירים. התקשורת הזו היא דו צדדית: אם אתם קוראים ידיעות אחרונות בעיתון לעומת באתר – יש את חווית הקריאה האנושית שפעם אחת היא חופשית מניטור ובפעם השנייה היא רוויית ניטור של גופים שרוצים לדעת מה מעניין אותנו ולהשתמש בזה לצורך מסחרי.

\*פס"ד גונזלס – ביה"ד האירופי לזכויות אדם התערב בנושא של גוגל – תנאי שימוש, לממשלות זה כר פורה למידע. בנוגע לאפל, באמצעות המידע שנצבר בטלפון ניתן להרשיע ולהפליל.

המדינה מבינה שאם היא הייתה צריכה סוכנים בשטח מה שפעם היא הייתה צריכה לעשות עם יחידת קומדנו ומכשור מיוחד היום ניתן לעשות זו בדרכים זולות ומתוחכמות. יש דילמות בין אינטרסים של אכיפת חוק ובטחון אל מול פגיעה בפרטיות.

ישראל היא מעצמת סייבר גם בהגנת סייבר ובהשקעות. לשמור על התפקוד התקין של המחשב ושל המידע שיש לו, ככל הניתן ללא עיסוק בתוכן. "ככל הניתן" זה שיח בין הטכנולוגים לבין המשפטנים, ההנחייה המשפטית של המרצה היא ללא עיסוק בתוכן (אלא אם הוא קשור ספציפית לתקיפה).

מערך הסייבר הלאומי:

1. קידום ההיערכות הלאומית להגנת הסייבר (החלטות ממשלה 2443, 2444)

2. קידום עוצמה ביטחונית אזרחית

3. הובלה ישראלית במרחב הסייבר

4. פיתוח תעשייה, אקדמיה והון אנושי - יעד מאוד משמעותי כתוצאה מזה שיש לנו עוצמה גדולה בסייבר רוצים לוודא שיש לנו עוצמה באזורים אחרים

5. קידום היציבה הבינלאומית של ישראל - הקמנו חמישה מרכזי מחקר שתפקידם לגרום לאקדמאים להתעסק בסייבר, כחלק מהמעוצמה הישראלית.

תקיפת סייבר זה אירוע שבו מישהו משתמש בחולשה במערכת מחשב, למשל: באג או תקלת תכנות שמאפשרת למחשב לתפקד לא כפי שהוא תוכנת. החולשה הזו מאפשרת להשתיל קוד זדוני או להתגבר על מנגנוני ההגנה ולעשות את מה שהתוקף רוצה לעשות. תקיפת סייבר נעשית למטרות שונות: גניבת מידע, גרימת נזק ותקיפה שמטרתה שיבוש פעילות. גופי המודיעין משתמשים בסייבר לצורך גניבת מידע או תקיפת מידע. בעולם המעשי המשמעות הוא שבכל מקרה שיש מחשב שבו יש מידע חשוב אנחנו חשופים לתקיפה באופן שיגרום לנו נזק. למשל: מחשבי חברת חשמל – היא מספקת חשמל למפעלים, משקי בית, בתי חולים, לצבא – בעבר היינו צריכים לתקוף מבנים או לשלוח איש קומנדו לבצע פעילות חבלנית. כיום בעידן הסייבר, מה שצריך לעשות הוא למצוא חולשה ברשת של חברת החשמל ולתת הוראות שונות: לטורבינות להפסיק לעבוד, להשמיד את כל המידע התפעולי. ראינו דוגמה לכך באוקראינה.

יש פעולת בידול – לבדל אותם מהאינטרנט.

חברת חשמל מוגנת בעולם הקינטי אבל בעולם הדיגטילי יש אתגר משמעותי, הגבול שצריך להגן עליו הוא גלובלי כי לא מדובר בנקודות שאפשר למקום לפי מכ"מ אלא מדובר בכל מי שמחובר לאינטרנט בעולם כולו: החל מהאקר שרוצה להוכיח את עצמו וזה עובר לארגוני פשע וטרור וירטואליים (מתקפות השבעה באפריל) ועד מדינות. ב2002 בגלל שישראל מדינה מתקדמת היא הבינה שגופים המשמעותים למשק ויש להם מחשבים עלולים לספוג נזק בעקבות תקיפות סייבר ולפגוע באינטרס הלאומי. בהחלטת ממשלה ב1984 נקבע שיש תשתיות קריטיות והם גופים שבאמצעות תקיפת מידע אפשר לגרום לנזק חמור לביטחון הלאומי. הטיפול באותן תשתיות הוטל על יחידה בשב"כ – לאתר ולהגן. המססגרת המשפטית היא החוק להסדרת הביטחון בגופים ציבוריים העוסק בביטחון פיזי והתאימו אותו לסייבר. הגופים שנכנסו הם חברת חשמל, בנק הדם, רשות האוכלוסין, גופי תקשורות וכו'. העיסוק בישראל הוא פר גוף ולא פר ענף, במדינות אחרות מדובר על ענפים: פיננסים, בריאות וכו'. במקביל לזה רגולטוריים מגזריין במשק הישראלי, התחילו להבין שיש אפשרות לתקוף את הגופים שלהם באמצעות בעיות באבטחת מידע והגופים הללו הוציאו רגולציות להתמודד עם בעיית הסייבר. מדובר בתפיסה סקטוריאלית – תשיות קריטיות מטופלות ע"י השב"כ וכל רגולטור צריך היה לבחון אם צריך. תפיסת הבוטיק הזו שנכנסה לתוקף ב2002 והייתה די מתקדמת ביחס לעולם ועמדה בסימן שאלה – האם ניתן להגן על מרחב הסייבר הישראלי בתפיסת הבוטיק? האם ניתן להגן על מרחב הסייבר על כל המשק?

**Wanna Cry** הרכיבו שני סוגי מחלות, תולעת וירטואלית שמתפשטת ולשכפל את עצמה עם תוכנת כופר שנועלת את המחשב ודורשת כסף תמורת שחרורו. באנגליה מערכת הבריאות כל המקומות בהם היו מחשבים לא מעודכנים ננעלו ולא היה ניתן לעשות שום דבר במחשבים הללו. התפסיה שמאפשרת להגן על מבצר אחד לא תופסת כי כחברה אנו חשופים במקרים רבים ושנים. רואים שככל שהמחשב והנייד מחוברים זה לזה יותר נפוץ ונכנסי ליותר יישומים במשק. ניתן לשות בהם שימוש לרעה ולגרום לזה להתפשט לכן להגן רק על 30 גופים במשק זה לא מספיק טוב, כדי להגן על כולם. בעיית המדיניות היא מורכבת מאוד, ישראל היא בין הראשונות שהצליחה להציע תפיסה וגם לממש אותה במידה רבה.

1. זירת ההגנה היא במערכות הארגון – התקיפה בסייבר מתרחשת בתוך המערכת הארגונית, וכל מי שרגיל לפעול במערכת הזו. תקיפת הסייבר מתרחשת בתוך "הבית שלנו" ולמדינה אין שום יתרון יחסי.

2. זירת ההגנה מבוססת טכנולוגיות אזרחיות – מה שמאפיין את הטכנולוגיות האלה הוא שכל הזמן יוצאים מוצרים חדשים ולא בודקים לעומק את העדכונים של הטכנולוגיה.

3. משרעת רחבה של איומים, תוקפים, ופוטנציאל נזק – ככל שיש יותר מחשבים ניתן לעשות שימוש יותר לרעה.

4. קישוריות והשפעות רוחב – תוכנות פגע, כמו התולעת הזו שמתוכנתת להתפשט ולהתרחב להרבה מחשבים.

5. זמני תגובה קצרים – זה מהיר.

6. מרחב גלובלי שאינו מצוי בריבונות "אחת" – היכולת שלנו לשלוט ולהשפיע ולהפעיל כוח במרחב הסייבר היא מוגנת משום שחלק מהסייבר הוא מחוץ לטריטוריה שלנו, למרחב שלנו.

7. תפקיד ואופן המערבות של המדינה בהגנה תוך איזון מול:

א. מרחב הסייבר כיכר לחדשנות ויזמות – האם לא צריך לבקש אישור מהמדינה לעשות דברים והמדינה לא משפיעה על כניסה של טכנולוגיות.

ב. מרחב הסייבר כבעל השפעה משמעותית על זכויות יסוד – פרטיות וחופש הביטוי. הדילמה היא גם מצד האתגר הביטחוני תפעולי וגם מבחינת החששות של תופעות לוואי. צריך שהיא תהיה חוקתית ובתוך זה מידתיות וחלופה של מידתיות במובן הצר ושם אנחנו בוחנים את תופעות הלוואי.

ב2015 התקבלו שתי החלטות ממשלה:

א. 2443 הסדרה והובלה ממשלתית –

1. מערך הסייבר כגורם לאומי מנחה

2. רגולציה אחידה באמצעות רשויות האסדרה –

3. מנגנון "ניהול תקין" של הממשלה ומשרדיה לטיפול בהגנת הסייבר

סטנדרט או נורמה אחידים לא משנה מה מהות הגוף. שיטת הבוטיק נותרה כי ישנם גופים מסוימים שצריכים טיפול ספציפי, אבל יש פתרון גם לכל יתר הגופים. מערך הסייבר לא עושה את הרגולצה במישרים, אלא באמצעות הרגולטורים – אנחנו נותנים להם את הסטנדרט ואיך ליישם והם מתאימים זאת אליהם ולארגונים בהם הם עובדים. הרעיון שעומד מאחורי זה: קודם כל שאותם רגולטורים מופקדים על אינטרס ציבורי וסיכוני הסייבר הוא מחולל נזק פוטנציאלי שיכול לגרופ נזק לאותו אינטרס ציבורי. לכן מי שצריך לתח את הדבר הזה אלה רשויות האסדרה המגזריות. שנית, זה יותר ייעיל חברתית שבמקום שיהיה גוף אחד ענק שיטפל בכל המשק הדבר יעבור דרך מי שמול היום בכל אחד מהמגזרים של המשק בעצמו. ??

התפיסה שהמדינה צריכה להשקיע יותר בהגנה מפני סייבר נמצאת גם במדינות אחרות, למשל: באיחוד האירופי חוקקו דירקטיבה שתיכנס לתוקף במאי והיא עוסקת בזה גם – גופים צריכים תמריץ חיצוני להשקיע יותר בהגנת סייבר והממשלה צריכה לגרום להם לעשות זאת. המשמעות היא שאנחנו מנסים לגרום לארגונים להיות יותר מוגנים באמצעותת השקעה שיטתית באבטחה ובהבנה של מה זה אבטחה בדומה לביטחון הפיזי, יש תחומים בהם האיום בסייבר הוא יותר גבוה ולכן יש התערבות רגולטורית.

נשאלת השאלה מה קורה כאשר יש סממנים של תקיפה?

ב. 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

?? יש הבחנה בין התקיפה לתוקף וזה אחד הדברים הרלוונטים בין התוקף לנתקף. אנחנו לא יודעים מי עומד מאחוריה וגם אם אנחנו יודעים מי זה אני לא בטוח יודעים איך לעצור את זה. לכן, אחנו רוצים למצוא את הדרך להתמודד עם התקיפה ללא קשר לטיפול בתוקף. האנלוגיה פה היא שריפות וחקירה של אירוע הגרימה לשריפה. קודם כל לפני שמחקים אחר מי הצית אותה כי השריפה עצמה יכולה להתפשט וליצור עוד נזק, לכן למדינה יש תפקיד שעד ההחלטה הזו לא ישב אצל אף אחד. הרעיון שיש מוקד 100 שמטפל בתקיפות הוא רעיון שמסתובב בעולם, אבל ישראל הייתה בין הראשונות ליישם אותו בעוצמה. שם הגופים הללו הוא CERT ותפקידם לחלוק מידע עם המרחב האזרחי ויכולת לטפל באירועים.

**Wanna Cry** ב14 למרץ פורסמה חולשה בתוכנה של מייקרוסופט. ה CERT מפרסם התראה לציבור באתר שלו וסיפר על פירצה ב14 באפריל נוצר כלי תקיפה שמנצל את החולשה, ותוך זמן קצר ב12 למאי התפרסמו ידיעות על כך שנוצר כלי שיודע להשתמש לרעה בחולשה הזו. מייקרוסופט פירסמה את הכלי שכנגד, ויום אחרי פרסום ה CERT. באנגליה לא עידכנו את התוכנות של מייקרוסופט, מתחילים להינעל המחשבים בבתי החולים הבריטיים ובמערכת הבריאות כולה. ראש הממשלה ראה את הדיווחים בBBC והוא שאל את עצמו למי אפשר להתקשר, בישראל זה ראש מערך הסייבר. במדינות אחרות זה כל מיני פונקציונרים שיש להם תפקיד לפעול באירועי חירום, אבל לא תפקיד ייעודי. מערך הסייבר התכנס כדי לחשוב איך מתמודדים עם האירוע הזה ואיך מכילים אותו. החל מלגרום למייקרוסופט ישראל לפרסם את העדכון הזה בעוד אתר, כי האתר קרס. היה ניתוח של האירוע, לפוגען היו מאפיינים ייחודיים שהיה צריך להכיר ולנסות להבין מה קורה. וזה החידוש של גוף סייבר לאומי וזה בכלל לא קשור לתוקף. כעבור זמן מה ממשלת ארה"ב כינסה מסיבת עיתונאים והיועץ לביטחון פנים אמר שהוא מאשים את צ' קוריאה בתקיפה. הנתון לא היה רלוונטי בזמן התקיפה כי אין מה לעשות איתה תוך כדי. צריך להכיל את האירוע תוך כדי שהוא קורה ולא לחפש אחרים.

ג. החוק להסדרת הבטחון בגופים הציבוריים

**איך כל האופרציה של איסוף מידע ושיתופו של הCERT עם קרונות עניין הפרטיות?**

כדי לבצע את משימת הגנת הסייבר בצורה טובה יש חשיבות לאסוף מידע על דברים מוזרים שקורים באינטרנט וברשת ולחלוק אותו מיד עם כולם כמו וייז גם כאן יש חשיבות מאוד גדולה לשיתוף מידע. הדבר השני הוא כשמטפלים באירועים במחשבים בעצם נוגעים במחשב ותקשורת וזה מעורר שאלות בנוגע לנגישות של המדינה למידע.

מהקמת אותם CERTים קם אותו ארגון שנקרא FIRST ומטרתו היא שיתוף מידע בין כל ארגוני הCERT באותו סופ"ש של האירוע והרבה מידע עבר שם. בזמן העברת החטות הממשלה השאלה שהתעוררה היא איך מסדירים את המתחש בין הכניסה המחודשת של המדינה למרחב הזה לבין הגנה על זכויות יסוד.

ישנו מסמך "עקרונות הפרטיות של הCERT הלאומי" – יישום של עקרונות דיני הפרטיות לתהליכי העבודה של המרכז. זה ניסיון לייצר מדיניות םרטיות קצרה, ברורה ושקופה לגבי מה אנחנו עושים ומה לא תבתחום הגנת הסייבר. גם כאן, נעשה ניסייון לשמור על ההבחנה בין תוכן לבין מידע שרלוונטי לסייבר. יש שם מונחים חדשים רבים כמו מידע בעל ערך אבטחתי שמטרתו לכוון לזה שאנחנו אוספים מידע על תקיפות ודרכי טיפול בהן, ולא על תוכן.

**איפה אנחנו כיום?**

אנחנו נמצאים באריזה של כל המדיניות הזו לשלב של תזכיר חוק. התזכיר אמור לעסוק בצד הרגולטורי וגם בצד האופרטיבי. בתוך זה, בגלל שהוא חוק שאמור לתת סמכויות למציאות ??

רוב התקיפות מתחילות עם פישינג – הלינק מעניין אותנו כי הוא מקשר לקובץ הזדוני.

**הרצאתו של עו"ד עמית אשכנזי שהוא היועץ המשפטי של מערך הסייבר**

ההרצאה תנוע בין הפוזיטיבי לתיאורטי- בין מה עושה הממשלה עם כספי המיסים בעניין סייבר, לבין מה עומד מאחורי הדבר הזה ובצד המשפטי מה עושים בתחום הגנת הסייבר.

מערך הסייבר הלאומי הוקם במשרד רוה"מ, מטה הסייבר הוקם ב2011 והוא המליץ על הצורך בגוף נוסף שיתעסק בסייבר- הרשות הלאומית להגנת הסייבר. שני אלה אוחדו לגוף חדש שנקרא מערך הסייבר הלאומי. המערך מונה כ200 אנשים בערך.

הגדרות

**הגנת סייבר-** פעילות לצורך שמירה על תפקודן התיקן של מערכות מחשב, המידע בהן, והתקשורת ביניהן בארגונים במגזרי המשק והמדינה ללא עיסוק בתוכן.

**סייבר אינטרנט**- הפעילות במימד התוכן, דיני מידע. חוק המחשבים חוקק במיוחד לזה, שם הוא מסביר את האובייקט שנקרא מחשב וחוק. למה המחוקק הסדיר את זה בחוק מיוחד? כי הדברים שהוא מסדיר כמעשים אסורים הם אסורים לא רק מבחינת מחשב. החוק מיוחד כי הערך המוגן של המחשב והתפקיד החברתי שלו הוא כזה שצריך לייחד לו חוק מיוחד. זה הסדרה ייעודית לנושא של מחשבים.

גם לשון הרע באינטרנט ואחריות עליה מסדירה חקיקה מיוחדת או שניתן לפרש את הדינים הקיימים באותו האופן. הפסיקה פיתחה את הדברים האלה. לפעמים המחוקק רוצה לייחד תופעות כמו חוק הסרטונים. החקיקה של החוק המיוחד והענישה המיוחדת סימנו שזה חשוב כאינטרס ציבורי.

בתוך הנושא הזה יש את שאלת האחריות המתווכים. דילמת האכיפה של האינטרנט, היכולת של כל אחד מכל מקום להפיץ או לקבל מידע או לבצע הפרות ועבירות, ואנונימיות, גרמה לזה שיהיה יותר יעיל לאכוף באמצעות המתווכים (מעבירי המידע) ואז עולה שאלת אחריותם (יו טיוב, גוגל, פייסבוק, וכו'.) משמעות אחריות המתווכים היא שאם מישהו לא מצליח לאכוף הפרות זכויות יוצרים שלי אבל כולם משתפים דרך פייסבוק או יוטיוב- אז אני יכול לתבוע דרכם. מצד שני, בשלב מוקדם של המשחק כדי לאפשר את התנועה של חופש הביטוי, הארגונים האלה קיבלו חסינות כזו או אחרת בחלק מהשיטות בעולם כדי לאפשר הפצת מידע. הנרטיב המשפטי שליווה את התקופה הזו היה אופטימי שבו התפקיד של המשפט בהסדרת האינטרנט הוא תפקיד פסיבי, גם בפן של המשפט החוקתי. צריך להשאיר את זה להסדרה פרטית. זה תקופת דיני תנאיי השימוש (עד לאחרונה). התקופה הזו היה בה דיבור לרעתו של המשפט שהוא מכביד ומייצר נטלים. לדעתם לא צריך יותר מדי חוקים, וצריך לתת לשוק לפתח את כל התעשייה שאנחנו נהנים ממנה של אפליקציות וחדשות שכולם יציר השוק הפרטי והמשפט הפרטי.

ואז קרו 2 דברים: ראשית התפיסה על האינטרנט קצת התפוגגה בגלל גילויים של עובד NSA שסיפר לעולם איך באמצעות האינטרנט ניתן לאסוף מידע מודיעיני על ידי הממשלה. זה גרם למהלך שנמשך עד היום- משבר אמון בעובדה שאינטרנט אמור להיות מקום פתוח שהממשלה לא נמצאת בו. שנית, התגברות איומי הסייבר, האינטרנט הפך להיות מקום קצת פחות בטוח. נשאלה שאלה עקרונית- כמו שאנחנו מצפים מהמדינה להגן עלינו במרחב הפיזי, מה תפקידה בהגנה עלינו במרחב הסייבר?

למה מדינות כלכך מתעניינות במה שקורה באינטרנט? כשגולשים באינטרנט לא באמת גולשים באינטרנט, אלא באינטרנט נמצא אצלנו. התחברנו לעולם והוא גולש אלינו למחשב. התקשורת הזו היא דו צידית- אם קוראים את ידיעות, אבל אם גולשים באותה כתבה בוואינט, האתר שולח כל הזמן אותות כדי להבין במה אנחנו מתעניינים כדי להציע לנו פרסומות. הדבר הזה נותן הרבה מידע על אנשים. אפילו מידע כמו כמה זמן לקח לקורא את הכתבה, כמה זמן לקח להזיז את העכבר, וכו'.

**סייבר-** שימוש של גורמי המדינה השונים במרחב זה לאיסוף מידע ולפעילות בטחונית או אכיפת חוק. המדינה מבינה שאם פעם היא הייתה צריכה לעשות דברים עם יחידות קומנדו וטלסקופים- היום אפשר לעשות את זה בדרכים יותר זולות ומתוחכמות. יש דילמות בין אינטרסים של אכיפת חוק ובטחון אל מול פגיעה בפרטיות. ישראל היא מעצמת סייבר שעוסקת בהגנת הסייבר- לשמור על התפקוד התקין של המחשב והמידע שיש בו, ככל הניתן ללא עיסוק בתוכן. זה שיח בין המשפטנים לטכנולוגיים- אפשר אל מול אי אפשר מבחינה מוסרית. ההנחייה המשפטית העקרונית היא שאסור לעסוק בתוכן אלא אם הוא קשור ספציפית לתקיפה.

מערך הסייבר הלאומי

מהם משימותיו?

-       קידום ההערכות הלאומית להגנת סייבר- החלטות הממשלה 2443 2444

-       קידום עוצמה ביטחונית אזרחית

-       הובלה ישראלית במרחב הסייבר

-       פיתוח תעשייה אקדמיה והון אנושי

-       קידום היציבה הבינלאומית של ישראל

מה קרה בישראל בטיפול בהגנת סייבר? תקיפת סייבר זה אירוע שבו מישהו משתמש בחולשה במערכת מחשב (באג או תקלת תכנות שמאפשרת לגרום למחשב הזה לתפקד לא כפי שהוא תוכנן). החולשה הזו מאפשרת להשתיל קוד זדוני ולהתגבר על מנגנוני הגנה ולפעול בדרך אחרת וכתוצאה מזה לעשות את מה שרוצה התוקף לעשות. תקיפות הסייבר נחלקות לתקיפה שמטרתה גניבת מידע, תקיפה שמטרתה גרימת נזק, ותקיפה שמטרתה שיבוש הפעילות. גופי המודיעין אוהבים להשתמש בזה כדי לגנוב או להדליף מידע נגיד.
מה המשמעות של זה בעולם המעשי? בכל מקרום שיש לנו מחשב ששולט על תהליך או מידע חשוב- אנחנו מוצאים את עצמנו חשופים לתקיפה כנגד המחשב הזה בצורה שיגרום לנו נזק. אם נסתכל על משהו כמו חברת חשמל- שהוא סופר חשוב לנו- אם יריב שלנו ירצה לגרום לה נזק הוא היה צריך או להפציץ אותו עם מטוס ולעבור את ההגנה אווירית. זה מסובך. היום בעידן הסייבר הוא צריך פשוט למצוא חולשה ברמת המחשב כחברה חשמל ולמצוא דרך למצוא לאותה רשת מחשבת ולתת הוראות לטורבינות דרך המחשב לסגור את עצמן לדוגמא או להשמיד מידע תפעולי. באמצעות תקיפת מחשב אנחנו מסוגלים לגרום לנזק. האתגר הזה גדול כי הגבול שאנחנו צריכים להגן עליו עכשיו הוא גבול גלובלי- אפשר לתקוף אותנו לא רק מהמדינות הקרובות אלינו פיזית, ומי שיכול לתקוף אותנו זה לא רק בעל הצבא החזק, אלא כל מי שמחובר לאינטרנט יכול לנסות.

ב2002 המדינה הבינה שהנושא של גופים מאוד משמעותיים למשק באמצעות לוחמת מידע וניתן לגרום לה נזק. יש תשתיות קריטיות שהם גופים שבאמצעות תקיפת מידע שלהם יכול להגרם נזק לאומי. על השב"כ הוטל לאתר את הגופים האלה ולהגן. המסגרת המשפטית שנקבעה היא חוק להסדרת בטחון בגופים ציבוריים שעוסק בבטחון פיזי והתאימו אותו גם לסייבר. הגופים שאותרו הם חברת חשמל, מקורות, בנק הדם, הלשכה המרכזית לסטטיסטיקה וכו. בעולם היום יש עיסוק גדול בתשתיות קריטיות. ישראל התחילה עם זה מוקדם ב2002. לישראל יש יתרון כי העיסוק שלנו בתשתיות קריטיות הוא פר גוף ולא פר ענף. זה מאפשר טיפול בוטיק.

במקביל לטיפול בתשתיות קריטיות, רגולטורים נגזרים על התשתיות הקריטיות (כמו המפקח על הבנקים) הבינו שיש אפשרות לתקוף את הגופים שלהם באמצעות בעיות באבטחת מידע, והם הוציאו רגולציות במסגרת הסמכויות שלהם להתמודד עם סיכוני הסייבר. התפיסה היא סקטוריאלית- תשתיות קריטיות מטופלות ע"י שב"כ, וכל רגולטור הסתכל האם הוא צריך. תפיסת הבוטיק הזו מ2002 הועמדה בסימן השאלה האם ניתן להגן על מרחב הסייבר הישראלי בתפיסה תרבותית. מה קורה עם יתר המשק? הבעיה בתפיסה התרבותית הוא שמרחב הסייבר הרבה יותר רחב וגדול מאשר אותו מספר מצומצם של תשתיות קריטיות. לדוגמא- אירוע שנקרא wanna cry שבו הרכיבו 2 חולירות שכל אחת מהם יכלה להתקיים בנפרד- 1) תולעת- משהו שיודע לשכפל את עצמו ולהתפשט, 2) תוכנת כופר. ואז היה שילוב של 2 תוכנות שונות שמנצלות חולשה בווינדווז, ופתאום כל המחשבים באנגליה שהיו קשורים בווינדווז ננעלו.  ככל שהמחשב והסמארטפון יותר נפוץ, והמחשבים נכנסים ליותר ויותר יישומים בכלכלה, בחברה, וכו', אז ניתן לתקוף אותם ולעשות בהם שימוש לרעה דרך האינטרנט.

כשרצו לעצב את המדיניות בארץ בהתאם לדברים הללו, ישראל היא בין הראשונות שהצליחה להציע תפיסה ואפילו לממש אותה במידה רבה. מה הם הבעיות בגיבוש תפיסת הגנה לאומית בסייבר?

1.     זירת ההגנה היא במערכות הארגון- התקיפה בסייבר מתרחשת בתוך הרשת הארגונית. בסייבר אנחנו חיים בתוך הרשת הארגונית ושם מתנהל הקרב. בתוך הבית שלנו. למדינה אין שם שום יתרון יחסי, כי אם עכשיו צריך לטפל ברשת של בר אילן, אין יתרון לכל הגאונים של 8200, למדינה יש אתגר משמעותי לנסות ולפענח שנים של עבודה שם.

2.     זירת ההגנה מבוססת טכנולוגיות אזרחיות- מה שמאפיין אותם זה שכל הזמן רוצים להוציא מוצר חדש ואין זמן לבחון אותו מול כל הבאגים האפשריים שלו.

3.     משרעת רחבה של איומים תוקפים ופוטנציאל נזק- ככל שיש מחשבים ביותר מקומות במשק אפשר לעשות בהם יותר שימוש לדברים הללו בדיוק

4.     קישוריות והשפעות רוחב- נובע מזה שהכל מחובר. התולעת נגיד מתוכנתת להתפשט.

5.     זמני תגובה קצרים- המרחב הוירטואלי הוא לא כולו בישראל, וזה מעלה את אתגר הריבונות. היכולת לשנות לשלוט ולהשפיע במרחב הסייבר מוגבלת בגלל שחלק מהמרחב הזה הוא לא בטריטוריה שלנו אלא במרחבים אחרים

6.     מרחב גלובלי שאינו מצוי בריבונות אחת

7.     תפקיד ואופן המעורבות של המדינה בהגנה תוך איזון מול מרחב הסייבר ככר לחדשנות ויזמות, ומרחב הסייבר כבעל השפעה משמעותית על זכויות יסוד (בעיקר פרטיות וחופש הביטוי). הדילמה היא גם מצד האתגר הביטחוני התפעולי, וגם מצד החששות לתופעות לוואי (בכל המקומות בהם המעורבות הממשלתית יותר מזיקה מאשר מועילה). אנחנו רוצים מסגרת משפטית חוקתית ושם אנחנו מודדים את תופעות הלוואי.

ב2015 הממשלה קיבלה 2 החלטות ממשלה עיקריות:

1.     2443 הסדרה והובלה ממשלתית. דרכו אנחנו עוברים מרגולציה מגזרית כל אחד לפי איך שהוא מבין אותה, לתפיסה מרכזית בו יש שפה אחת ומיישרים את מגדל הבבל לגבי מה זה הגנת סייבר. שלכולם יהיה נורמה וסטנדרט קצת יותר אחידה. הרעיון של החלק הרגולטורי הוא שמערך הסייבר לא עושה את הרגולציה במישרין אלא באמצעות הרגולטורים. כמדברים על תשתיות קריטיות אנחנו מטפלים בהם בעצמו. התפיסה של רגולציה באמצעות רשויות ההסדרה אומרת שאנחנו נותנים להם את הסטנדרט ואת ההנחיות איך ליישם, והם לוקחים את זה ומתאימים את זה למגזר שלהם בו הם פועלים. מערך הסייבר הלאומי לא עובד ישירות מול הגורמים האלה אלא מול הרשות. מה הרעיון שעומד מאחורי זה? קודם כל שאותם רגולטורים מופקדים על איזה שהוא אינטרס ציבורי, וסיכוני הסייבר הוא מחולל נזק פוטנציאלי שיכול לגרום נזק לאותו אינטרס ציבורי. לכן מי שצריך לנתח את הדבר הזה אלה רשויות ההסדרה המגזריות. שנית, זה יותר יעיל חברתית שבמקום שיהיה גוף אחד ענק שיטפל בכל המשק, הדבר יעבוד דרך מי שמטפל היום בכל אחד מהמגזרים של המשק בעצמו.
הדבר השני שיש בהחלטה הזו זה ההבנה שגם הממשלה עצמה כגוף לא מספיק טובה בהגנת סייבר. יש הוראות שעוסקות בניהול תקין אל הממשלה ומשרדיה לטיפול בהגנת סייבר. הממשלה צריכה לבחון האם הם חשופים להגנת סייבר, להקים ועדות, ולהשקיע לפחות 8% מתקציב המחשוב בהגנת סייבר. הרעיון היה לגרום למשרדים להיות מחויבים. התפיסה שהמדינה צריכה לגרום לארגונים להשקיע יותר בהגנה מפני סייבר, נמצאת גם במדינות אחרות. באיחוד האירופי חוקקו דירקטיבה שתכנס לתוקף במאי והיא עוסקת בזה גם. גופים צריכים תמריץ חיצוני להשקיע יותר בהגנת סייבר. זה אומר שאנחנו מנסים בעצם לגרום לארגונים להיות יותר מוגנים באמצעות השקעה שיטתית באבטחה, הבנה של מה נדרש לאבטחה, בדיוק כמו טיפול בבטחון פיזי. בשונה מבטחון פיזי, יש תחומים בהם האיום בסייבר הוא יותר גבוה ולכן יש התערבות רגולציה.

2.     2444 מערך הסייבר הלאומי כגוף ייעודי להגנת הסייבר. זהו גוף הטיפול בתקיפות סייבר. עוסקת בתפקיד המדינה בטיפול בתקיפות. יש הבחנה בין התקיפה לתוקף. כשרואים תקיפת סייבר רואים משהו מוזר קורה ברשת ואנחנו לא יודעים מי עומד מאחוריה. גם אם אנחנו יודעים אנחנו לא בטוח יודעים איך לעצור את זה. לכן אנחנו רוצים למצוא את הדרך להתמודד עם התקיפה ללא קשר לטיפול בתוקף. האנלוגיה פה היא שריפות, וחקירה של חוקר השריפות. צריך לטפל בשריפה לפני שמתחקים אחרי מי הצית אותה, כי השריפה עצמה יכולה להתפשט וליצור עוד נזק. לכן למדינה יש תפקיד, שעד ההחלטה הזו לא ישב אצל אף אחד. הרעיון שיש סוג של מוקד לסייבר שיש לו תפקיד בלשתף מידע ולטפל בתקיפות הוא רעיון בין לאומי. הגופים שעוסקים בנושא הזה הם cert או see-cert.

3.     החוק להסדרת הבטחון בגופים ציבוריים.

אירוע wanna cry

ב14 למרץ פורסמה חולשה בתוכנה של מייקרוסופט. הcert מפרסם התראה לציבור באתר שלו ומספר על כך שיש חולשה וצריך להתקין עדכון דרך האתר כדי לחסום את הפרצה. תוך חודש נוצר כלי תקיפה שמנצל את החולשה. באותו יום מייקרוסופט פרסמה את הכלי שכנגד, ויום אחרי פרסם הcert אזהרה לתושבים גם בישראל. המדינה מתריעה בעצם על חולשות במערכות מחשב- משהו שלא היה קודם וזה חלק מהחידוש של ההחלטות. חודש אחרי, מתפרסמות הידיעות על הכלי הזה שהוא שילוב של תולעת עם פוגען כופר. זה מתפשט מאוד מהר במערכת הבריאות הבריטית כי הם לא אירגנו את הווינדווז. מתחילים להינעל מחשבים בבתי חולים. רוה"מ מסתכל ולא מבין למי הוא צריך להתקשר עכשיו- זה לא צבאי זה לא שב"כ, אז הוא התקשר לראש מערך הסייבר. במדינות אחרות לא היה למי להתקשר וזה נפל בין כל מיני אנשים שיש להם אולי תפקיד לאירועי חירום אבל לא היה מישהו שיוכל להתסכל על כל התמונה. ואז מערך הסייבר הלאומי של ישראל ושאל את עצמו איך מכילים את האירוע הזה. גרמו למייקרוסופט ישראל לפרסם את הכלי שכנגד בעוד אתר כדי שיוכלו במקביל אנשים רבים לעשות את הדברים. זה החידוש של גוף סייבר לאומי- וזה בכלל לא קשור לתוקף.
בארה"ב כינסו בנתיים מסיבת עיתונאים ויועץ הנשיא לבטחון פנים אמר שהוא מאשים את צפון קוריאה בתקיפה הזו. אבל הנתון לא היה רלוונטי בזמן התקיפה כי אין מה לעשות איתה תוך כדי. צריך להכיל את האירוע תוך כדי שהוא קורה ולא לחפש אשמים.

איך כל האופרציה של איסוף מידע ושיתופו של הcert עם עקרונות עניין הפרטיות?

כדי לבצע את משימת הגנת הסייבר בצורה טובה יש חשיבות לאסוף מידע על דברים מוזרים בקורים באינטרנט ולחלוק אותו מיד עם כולם (כמו וואיז). גם כאן יש חשיבות מאוד גדולה לשיתוף מידע. הדבר השני הוא שכשמטפלים באירועים במחשבים בעצם נוגעים במחשב ותקשורת וזה מעורר שאלות בנוגע לנגישות של המדינה למידע.
מהקמת אותם certים, קם ארגון גם שנקרא first שמשתף מידע בין כל ארגוני הcertים. באותו סופ"ש של wanna cry הרבה מידע עבר שם. בזמן העברת החלטות הממשלה השאלה שהתעוררה היא איך מסדירים את המתח שבין הכניסה המחודשת של המדינה למרחב הזה לבין ההגנה על זכויות יסוד. ישנו מסמך ליישום עקרונות דיני הפרטיות לתהליכי העבודה של המרכז. "עקרונות הפרטיות של הCert הלאומי". זה נסיון לייצר מדיניות פרטיות קצרה, ברורה, ושקופה לגבי מה אנחנו עושים ומה לא בתחום הגנת הסייבר. גם כאן, נעשה נסיון לשמור על ההבחנה בין תוכן לבין מידע שרלוונטי לסייבר. יש שם מונחים חדשים רבים כמו מידע בעל ערך אבטחתי- שמטרתו לכוון לזה שאנחנו אוספים מידע על תקיפות ודרכי טיפול בהם, ולא על תוכן.

איפה אנחנו נמצאים היום?

אנחנו נמצאים באריזה של כל המדיניות הזו לשלב של תזכיר חוק. התזכיר אמור לעסוק בצד הרגולטורי וגם בצד האופרטיבי. בתוך זה, בגלל שהוא חוק שאמור לתת סמכויות למציאות טכנולוגית משתנה, מצד אחד הוא נותן סמכויות בלשון יחסית פתוחה, ומצד שני על מנת שיהיה מידתי יש בתוכו שורה של איזונים ובלמים שנועדו להבטיח שהפעלת הסמכות תהיה מידתית. האלמנטים האלה כוללים את התכלית- הגנת סייבר בלבד.

**16/4/18**

גורמי הביניים מהווים כתובת אטרקטיבית לתביעות משפטיות ולהפקדה של סמכויות אכיפה. החשיפה הגדולה שנוצרה לביטוי ברשת בהיבטים של הגנה על השם הטוב.

מדוע גורמי ביניים ברשת מהווים כתובת אטרקטיבית לתביעות משפטיות?

1. ניתנים לזיהוי ואיתור בקלות – בעוד שתהליך זיהויו של המשתמש היחיד עלול להיות יקר וממושך, במיוחד לנוכח השכיחות של פעילות אנונימית. זול יותר להגיש תביעה נגד המתווך.

2. לרוב בעלי "כיס עמוק" – סיכוי הנפגע להיפרע מהנזק גבוה יותר. המתווך הוא כיס עמוק וזה מושך לפנות אליהם.

3. פעמים רבות הם מונע הנזק היעיל ביותר – מצויים בעמדה שמאפשרת למנוע באופן אקטיבי את הישנות המקרה: הם יכולים לנטר את הפעילות, להפעיל עריכה, לחסום משתמשים, לצנזר תכנים ואמירות פוגעניות. ככל שנגדיל את החשיפה המשפטית שלהם הם יתומרצו לפעול כך, הם ימנעו את הסיכון מראש. למשל: תביעות אסטרטגיות של בעלי זכויות יוצרים בשל אחריות תורמת (פרשת נפטסר – נפטסר היה שירות שאיפשר למשתמשים להחליף קבצים ושם הוצעה הדוקטרינה של "אחריות תורמת" עם הקביעה שהאתר למרות שהוא לא אחראי ישיר סיפק את הטכנולוגיה שמאפשרת לבצע את הפרת זכויות היוצרים והייתה לו יכולת לפקח על פעילות המשתמשים. בנוסף, האתר הפיק תועלת כלכלית מהפעילות הזו שכללה הפרה של זכויות יוצרים).

הצורך להסיר את החסינות של האנונימיות ברשת כי אנחנו לא רוצים לעודד את המשך ההגנה על פעילות עבריינית. העיקרון של איך אנחנו מפעילים את גורמי הביניים לשיפור יכולת האכיפה – תובעים זיהו אותה מהר.

קשיים וסכנות בהטלת אחריות משפטית על גורמי ביניים:

1. עמימות ביחס לכללים המשפטים שחלים על המתווך (הפעילות ברשת)

- במדינה שבה רשום המתווך?

- במדינה שבה פועל המתווך?

- במדינה שבה מצויים המשתמשים בשירות?

למשל: פייסבוק בישראל, AIR B&B

2. החשש הוא שהחשיפה המשפטית עלולה לייקר משמעותית את עלות הפעלתם של שירותים ברשת – הקמת מנגנוני סינון וניור של פעילות משתמשים, ייעוץ משפטי והתדיינות משפטית. זה יוביל לצמצום מספר השירותים, והתייקרות גישה למידה ואנחנו כחברה נפסיד אמצעי ביטוי, זירות לפעילות מסחרית וגישה לידע ונחזור למצב ריכוזי (פס"ד רוטר ובדיונים על אחריות של מתווכחים ברשת).

יש הנחה בסיסית שקיים שוני איכותי בין גורמי הביניים ברשת במיוחד בכל הקשור להפצת מידע ולחופש ביטוי, לבין אמצעי התקשורת המסורתיים. הכמות של המידע שעובר ברשת היא בלתי ניתנת בהשוואה למה שקורה בעיתונות/אמצעי התקשורת האחרים בכלל ומכאן התפיסה של הצורך להשתמש באמצעים טכנולוגיים כדי להתמודד עם היקף הפעילות הגדול. נשאלת גם השאלה - האם הרשת מצדיקה חשיבה אחרת מהכללים המשפטיים שאנחנו מכירים.

**הכללים המשפטיים משפיעים על התהלות גורמי הביניים (מחקר של UNESCO 2014):**

המדיניות והפרקטיקות של גורמי ביניים ברשת בכל הנוגע להגבלת מידע מובנות ע"י הכללים המשפטים במדינת האם (ובמידה פחותה – במדינות שבהן הם פועלים). יש חשיבות גדולה לדיון בשאלות האלה – הם מצאו שיש קשר בין כללי האחריות במערכת המשפטית הרלוונטית, כך שככל שהאחריות חמורה יותר הסיכוי שתוכן יוסר על ידי המתווך באופן יזום או על רקע בקשה להסרתו.

הרצון לקדם את חופש הביטוי, המסחר, העיסוק, ההתאגדות ושאר זכויות שאינטרנט מגביר, אל מול הרצון לצמצם את הסיכוי לפגוע בשם הטוב, בקניין הרוחני, לבצע עבירות פליליות וכו'.

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

מקרה שמראה לנו את המתחים בהטלת אחריות על גורמי ביניים מחד ומנגד את הפוטנציאל של הסדרה ורגולציה ואכיפה באמצעים טכנולוגיים.

רקע:

מנגנונים משפטיים בתחום הקניין הרוחני מאפשרים להפוך ידע מופשט לנכס שניתן לרכוש בו בעלות ולסחור בו. הבעלות המוקנית ליוצר או לממציא מפקיעה את היצירה או ההמצאה מנחלת הכלל לפרק זמן מוגבל עפ"י חוק (שימוש ביצירה מחייב הרשאתו). המחוקק יצר זכויות שונות בקניין רוחני. בשיעור זה נתמקד בזכויות יוצרים. כלומר, מי שרוצה להשתמש ביצירה צריך לקבל הרשאה מבעל הזכות ואם לא נעשה כן יש הפרה של זכות ובגינה תרופה.

הדין הישראלי, בדומה לאמריקני, נוקט גישה תוצאנית – הגנה על זכויות יוצרים מוצדקת ככל שהיא מקדמת תוצאה רצויה. זו גישה כלכלית: קידום הרווחה החברתית הכוללת באמצעות מתן תמריצים. מצד אחד אנחנו רוצים לתת תגמול ליוצרים וממציאים כדי לעודד השקעות ביצירה וחדשנות (זכות למנוע את השימוש). מצד שני, הרווחה החברתית הכוללת מכילה בתוכה את הרצון לקדם את חופש המידע והביטוי - איזון מול הפגיעה בחופש המידע (גישה לידע ושיתוף ידע) וחופשי הביטוי. נשאלת השאלה באיזה אופן הקידום של ערכים אלה במסגרת המכשיר של זכויות יוצרים הוא שונה/מושפע מהזירה החדשה הזו.

**חוק זכויות יוצרים התשס"ח-2007:**

**\*ס' 47:**

(א) העושה ביצירה פעולה מהפעולות המפורטות בסעיף 11, או מרשה לאחר לעשות פעולה כאמור, בלא רשותו של בעל זכות היוצרים, מפר את זכות היוצרים, אלא אם כן עשיית הפעולה מותרת לפי הוראות פרק ד׳.

(ב) החל מיום 07/08/2018): בבחינת טענה להפרה כאמור בסעיף קטן (א) לגבי יצירה שהיא גופן יובא בחשבון, בין היתר, מגוון האפשרויות הקיים לעיצוב אותיות, ספרות וסימני שפה אחרים.

**\*ס' 11:** זכות יוצרים ביצירה היא הזכות הבלעדית לעשות ביצירה, או בחלק מהותי ממנה, פעולה, אחת או יותר, כמפורט להלן, בהתאם לסוג היצירה:

(1)העתקה כאמור [בסעיף 12](https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%96%D7%9B%D7%95%D7%AA_%D7%99%D7%95%D7%A6%D7%A8%D7%99%D7%9D#%D7%A1%D7%A2%D7%99%D7%A3_12) – לגבי כל סוגי היצירות;

(2)פרסום – לגבי יצירה שלא פורסמה;

(3)ביצוע פומבי כאמור [בסעיף 13](https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%96%D7%9B%D7%95%D7%AA_%D7%99%D7%95%D7%A6%D7%A8%D7%99%D7%9D#%D7%A1%D7%A2%D7%99%D7%A3_13) – לגבי יצירה ספרותית, יצירה דרמטית, יצירה מוסיקלית ותקליט;

(4)שידור כאמור [בסעיף 14](https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%96%D7%9B%D7%95%D7%AA_%D7%99%D7%95%D7%A6%D7%A8%D7%99%D7%9D#%D7%A1%D7%A2%D7%99%D7%A3_14) – לגבי כל סוגי היצירות;

(5)העמדת היצירה לרשות הציבור כאמור [בסעיף 15](https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%96%D7%9B%D7%95%D7%AA_%D7%99%D7%95%D7%A6%D7%A8%D7%99%D7%9D#%D7%A1%D7%A2%D7%99%D7%A3_15) – לגבי כל סוגי היצירות;

(6)עשיית יצירה נגזרת כאמור [בסעיף 16](https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%96%D7%9B%D7%95%D7%AA_%D7%99%D7%95%D7%A6%D7%A8%D7%99%D7%9D#%D7%A1%D7%A2%D7%99%D7%A3_16), ועשיית הפעולות המנויות בפסקאות (1) עד (5) ביצירה הנגזרת כאמור – לגבי יצירה ספרותית, יצירה אמנותית (החל מיום 07/08/2018: שאינה גופן), יצירה דרמטית ויצירה מוסיקלית;

(7)השכרה כאמור [בסעיף 17](https://he.wikisource.org/wiki/%D7%97%D7%95%D7%A7_%D7%96%D7%9B%D7%95%D7%AA_%D7%99%D7%95%D7%A6%D7%A8%D7%99%D7%9D#%D7%A1%D7%A2%D7%99%D7%A3_17) – לגבי תקליט, יצירה קולנועית ותוכנת מחשב.

ס' 47 ו-11 יחד מראים הבנה שהפרה של זכויות יוצרים היא ביצוע של פעולה שיוחדה לבעל זכויות היוצרים (שימוש ביצירה שיוחד לבעל זכות היוצרים) בלי לקבל את הרשות של בעל הזכות. השימושים שיוחדו מפורטים בס' 11: העתקה, פרסום, שידור וכו' – חל על שימוש ביצירה או חלק מהותי ממנה. ההגנה היא לא הגנה מוחלטת, במסגרת האיזונים יש התרה של שימושים **ללא רישיון:**

1. ס' 19 שימוש הוגן (למטרת חינוכיות, מחקריות ודיווח עיתונאי)

2. שימושים שהינם מותרים ללא רישיון (פרק ד', ס' 20-30, 32) (שימוש אגבי, בהליכים משפטיים, בספריות וארכיונים).

**תביעה בגין הפרת זכות יוצרים:**

על הובע מוטל נטל ההוכחה - התובע צריך להוכיח שהוא בעל זכות היוצרים ביצירה שבגינה הוא תובע והנתבע הפר את זכותו. החוק קובע תנאים נוספים לקבלת הגנה על זכויות יוצרים ביצירה (קיימים תנאים נוספים שלא רלוונטיים לענייננו).

**מה האתגר באכיפת זכויות יוצרים בעידן הדיגיטלי?**

- בחינה של האם מתקיימים התנאים בחוק לאכיפת הזכות, איך נבצע בדיקה בהיקף גדול של פעילות

- העידן הדיגיטלי ומהפכת המידע שינו את האופן שבו יוצריפ, מעבדים, משתמשים, משתפים ומפיצים יצירות (כולל העתקה, שינוי, שילוב פורמטים). ניתן לשכפל יצירות או חלקי יצירות, להוריד קבצים ולשתפם בקלות רבה. דרך שימוש ברשתות חברתיות, אפליקציות – מתאפשרת הפרה של זכויות יוצרים בקנה מידה נרחב מאוד.

- האמצעים לכך מצויים בידי על משתמש – הרחבת מעגל המשתתפים וזה מביא לציבור גדול של מפירים פוטנציאליים. התוצאה: אכיפת זכויות יוצרים ברשת מחייבת נקיטת פעולות אכיפה רבות.

למשל: אנחנו רוצים כחברה שמייקרוסופט יפיצו את הגרסה החדשה שלהם או שאומן ישחרר את השיר שלו ברשת.

- קושי נוסף: זיהוי משתמשים הפועלים ברשת האינטרנט באופן אנונימי וזה מביא לקושי בהטלת אחריות ישירה על משתמשים שהפרו זכויות יוצרים. נשאלת השאלה עד כמה באמת יש היום אנונימיות ברשת? בהתחשב ביכולת הטכנולוגית להצליב מידע על משתמשים ברשת ובאפליקציות. טוענים במאמר שהנחת האנונימיות הזו צריכה שקילה מחדש לפחות בהיבטים מסוימים כי הטכנולוגיה עצמה מאפשרת לזהות בצורה יותר טובה את המשתמשים.

הפתרון של אכיפה באמצעות בית המפשט בעייתי:

1. עלות גבוה בפנייה לביהמ"ש

2. ספק לגבי יעילותה בהתחשב בהיקף ההפרות

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

- כדי לקבל את פרטי הזיהוי של המשתמש בעל הזכות צריך לפנות לספק שירותי הגישה ולקבל את פרטי הזיהוי של המשתמש (כתובת הIP של המנוי שבאמצעותו בוצעה הפעילות).

- ביהמ"ש קבעו שלא יימת סמכות בחוק המאפשרת להם להורות לספק לחשוף את זהותו של משתמש שלכאורה ביצע עוולה אזרחית, ולרוב דחו בקשות שכאלו. דוגמה: **The Football Association Premier League** **Limited נ' פלוני -** אתר שאיפשר למשתמשים ישראלים לצפות במשחקים של הליגה האנגלית בתשלום חלקי, הליגה הנאגלית ביקשה לחשוף את זהות המשתמשים כדי שתוכל לתבוע אותם וביהמ"ש קבע שאין סמכות להורות על חשיפת פרטי המשתמשים. בפסק הדין דובר על דוקטרינות אחרות לחייב את גורם הביניים באחריות תורמת, אך לא שיש לביהמ"ש סמכות להורות לגורם הביניים לחשוף את זהות המשתמש.

- ההצעה לתיקון מס' 5 לחוק זכויות יוצרים מבקשת ליצור מקור סמכות זו. פרק ח1: חשיפת זהותו של עושה פעולה בתוכן ברשת תקשורת אלקטרונית. הצעה ליצור מקור חוקי לסמכות האמורה מעלה. לביהמ"ש, כך מוצע, תהא אפשרות להורות לגורמי הביניים את זהות מבצעי הפעולה.

**התוצאה:**

תוצאת המגבלות הללו של אכיפה באמצעות בתי המשפט הייתה באופן לא מפתיע שבעלי זכויות יוצרים נדרשו לפתח אסטרטגיות חדשות, המרכזית: אכיפה ע"י גורמי ביניים ברשת.

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

- המטרה: לחזק את האכיפה ברשת מחוץ לבתי המשפט ולייצר פעולות שיטור, מניעה והרתעה מבלי להזדקק להליכים נגד מפרי חוק בבית המשפט.

- האמצעים: בעיקר אמצעי אסדרה טכנולוגיים.

- הקושי: מדובר ביצירת מנגנוני אכיפה באמצעות גורמי ביניים פרטיים, לרוב גופים מסחריים שפועלים בהיעדר שקיפות וללא כל בקרה משפטית.

רואים יותר אכיפה אצל גורמי הביניים מאשר בבתי המשפט.

סוגי אמצעי אסדרה טכנולוגיים:

- הגבלת הגישה למוצר בו מאוחסן התוכן המוגן בזכויות יוצרים, למשל: מנעולים דיגיטליים.

- הגבלה על העברת מידע ברשת, מוטלת באופן טיפוסי בעיקר על: ספקיות גישה, ספקיות מארחות, מנועי חיפוש, בעלי אתרים, פלטפורמות שיתוף קבצים – כל אלה אמצעים טכנולוגיים שונים מבוססי IP/DNS/URL ועוד.

כיצד ניתן לקדם אסדרה באמצעות גורמי הביניים? האם הם אחראים להפרות שבוצעו ע"י משתמשים?

- לא מטילים אחריות ישירה

- אחריות עקיפה – בישראל נעשית בעיקר על בסיס דוקטרינת ההפרה התורמת והבסיס לה הוא "נוהל הודעה והסרה" (הסדר שאומץ מארה"ב).

**\*פרשת "על השולחן"**

**היעדר אחריות ישירה של גורמי הביניים בגין הפרות זכויות יוצרים שבוצעו בידי המשתמשים:**

- בתי המשפט לא הטילו על גורמי ביניים אחריות ישירה בגין פעולות שבוצעו בידי המשתמשים באמצעות המערכת (בכפוף לנוהל הודעה והסרה).

- אם מקור היצירה המפירה הוא בגורם הביניים ולא במשתמשים תחול אחריות ישירה להפרה, למשל: פורום, עיתון אינטרנטי המפרסם בעצמו עותקים של יצירות ללא רישיון.

- המצב המשפטי בישראל דומה למצב המשפטי בארה"ב ובאירופה.

**החלת דוקטרינת ההפרה התורמת בזכויות יוצרים על גורמי ביניים ברשת:**

**\*פרשת שוקן -** גורמי ביניים בעולם הפיזי הציגה את הדוקטרינה של ההפרה התורמת. התעוררה השאלה מה היו התנאים לאחריות של גורמי ביניים – תא סטודנטיאלי באוניברסיטה העברית שיכפל יצירה שלהוצאת שוקן היו זכויות יוצרים בה, הדפיס וכרך אותה במסגרת מקראה, ללא אישור האוניברסיטה, אך בשטחה. התנאים שנקבעו ע"י ביהמ"ש הם: שתהיה הפרה ישירה בפועל, ידיעה ממשית של הגורם על ההפרה (האוניברסיטה במקרה זה) ושלגורם הביניים תהיה ידיעה משמעותית לביצוע ההפרה. התוצאה הייתה שהאוניברסיטה לא חויבה, לא נמצא שהיא עמדה בתנאים כי לא הייתה לה ידיעה וגם לא תרומה משמעותית.

התנאים להחלת דוקטרינת האחריות התורמת בדיני זכויות היוצרים:

1. הפרה ישירה בפעול

2. ידיעה ממשית וקונקרטית של המפר התורם על ההפרה הישירה שקרתה. לא די בידיעה קונטרוקטיבית כללית.

3. תרומה משמעותית, ניכרת וממשית לביצוע ההפרה.

בסמכוך ליציאת אותו פסק דין נפלה הכרעה בידי השופט גרוסקופף שנדרש להכריע במקרה של אתר רוטר.נט.

**\*פרשת רוטר -** הדוקטרינה של הפרה תורמת חלה גם על מתווכים ברשת – משתמשים וגולשים ברוטר שפירסמו קישורים לאתרים אחרים שבאתרים אלו הועלו יצירות ללא הרשאה (הפרת זכויות יוצרים). העיקרון שנקבע בפסק הדין הוא שאין להטיל אחריות להפרת זכויות יוצרים על בעל אתר שלא ידע עליה, ובתנאי שכאשר נודע לו עליה הסיר את הפרסום המפר סמוך להודעה. המשמעות של קביעת דוקטרינת האחריות התורמת בנושא זה, בכפוף לנוהל הודעה והסרה היא שכל עוד גורמי הביניים מקיימים מנגנונים של הסרה של תכנים מפרים תהיה להם חסינות מפני אחריות להפרת זכויות יוצרים בידי משתמשים. כדי לממש את המנגנון הזה הם הופכים לזרוע אכיפה אחראית בתחום זכויות היוצרים.

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

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

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

3. חשש מהטלת עלויות כבדות על גורמי הביניים שיצטרכו לנקוט בפעולות של ניטור וסינון תכנים.

4. סכנה ליצירת אפקט מצנן על פעולות רצויות בשל הטלת אחריות על גורמי ביניים (**פס"ד א.ל.י.ס. בע"מ נ' רוטר.נט בע"מ**).

5. ה"מחיר" הערכי של הפיכת ספקיות האינרנט למעין צנזור ברשות ביהמ"ש הוא מחיר שקול לפחות, אם לא כבד יותר, לפגיעה בזכות הקניין הרוחני של המבקשות (**פס"ד זיר"ה נ' פלוני**).

**חריגים לכלל של "הודעה והסרה":**

הכלל: משתמשים שמעלים תוכן מפר לא יגררו אחריות של הפרת זכויות יוצרים על גורמי הביניים אם לא ידעו עליה וכשידעו עליה הסירו את התוכן המפר סמוך להודעה. למשל: קובץ או קישור לאתר מפר.

מצבים חריגים בהם תוטל אחריות על האתר בגין פעולות משתמשים:

1. עידוד – האתר מעודד פרסום קישורים מפרים. נלמד מאופי שיווק האתר ושמו, 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.

- יחסי: אחוז הקישורים המפרים ביחס לכלל ההודעות בפורום

**כללי אצבע היוצרים חשד לפורום פסול (פרשת רוטר):**

ב**פס"ד רוטר** השופט גרוסקופף עושה הבחנה בין פורום שהכניסה אליו מוגבלת (ע"י תשלום למשל) לבין פורום פתוח.

1. פורום סגור: הכניסה אליו מוגבלת בתשלום או באופן אחר. קשה יותר לבעלי זכויות היוצרים לבצע את הפיקוח. מאפיינים: 10 קישורים מפרים והודעות הכוללות קישורים מפרים מהוות יותר מרבע מההודעות המהותיות בפורום.

2. פורום פתוח: לפחות מחצית מהתוכן המהותיש ל הפורום יהיו הודעו הכוללות קישורים לאתרים מפרים.

**המשמעות של הוכחת "פורום פסול":**

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

2. על בעל האתר מוטל הנטל להוכיח אחד משניים:

א. להמשך קיומו של הפורום יש ערך לגיטימי (למשל, קידום ערכים חינוכיים או סיוע לאוכלוסיות מוחלשות).

ב. הוא לא ידע על היקף הפעילות הפסול (ולכן, לא ייש באחריות אלא לאחר שנמסרה לו הודעה על כך שמדובר ב"פורום פסול").

מקרים נוספים בהם יצא האתר אחראי:

\*פס"ד גולצמן – במקרה זה 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 השימוש הראוי בנוהל "הודעה והסרה" משום שעובדי המשרד הם אלו שהעלו את החומר המפר (שיר) לא היו משמתמשים פרטיים שאינם בשליטת בעלי האתר, אלא עובדי המשרד.

בישראל הנוהל הוא יציר הפסיקה כאמור (הודעה והסרה). בארה"ב: דיגיטל מיליניום אקט. באירופה: ??

**ממצאי מחקר שערכו בר זיו ואלקין-קורן:** מחקר אמפירי על האופן בו אוכפים זכויות יוצרים בביהמ"ש ובקרב גורמי הביניים- דפוסי השימוש. המחקר השווה שתי זירות:

ביהמ"ש: אליהם פונים בעלי זכויות יוצרים על מנת לתבוע בגין הפרה.

גורמי ביניים: הנדרשים לנקוט אמצעי הסרה, חסימה, מניעה וסינון (ניתוח בקשות שהוגשו לגוגל להסרה מתוצאות החיפוש של דפים ואתרים בגין הפרת זכויות יוצרים לכאורה).

99 תביעות משפטיות מול 2556 בקשות הסרה: רק על סמך חצי שנה.

ממצאים מרכזיים אכיפה בבתי המשפט:

הליכים בבתי המשפט משרתים מגוון מצומצם של תובעים ונותנים מענה לסוג מצומצם של יצירות.

??

ממצאים מרכזיים:

ביהמ"ש נותן שירות למגוון מצומצם של תובעים והפרות, בעיקר הפרות של זכויות יוצרים בצילומים ורוב המקרים מסתיימים בפשרה שכוללת פיצוי כספי בסכום נמוך מזה שנתבע במקור. כלומר הסעד של אכיפה וצו המסיר תוכן מפר היה פחות משמעותי. אחרת ממה שרואים אצל גורמי הביניים, אצלם הסרת התוכן המפר, האכיפה, גדולה יותר. הרבה פעמים הפשרות משקפות את זה שעצם הגשת התביעה הפעילה לחץ על הנתבע להסיר את התוכן המפר.

מה משמעות הפרטת האכיפה והעברת הפעילות הזו לגורמי הביניים? אם ממילא מה שיש לנו זה בעיקר פשרות ולא נוצר כלל משפטי מחייב וביהמ"ש לא עוסק באופן משמעותי בפרשנות החוק/היקף ההגנה על הזכויות, אלא נותן יותר תוקף להסכמות שהצדדים הגיעו אליהן בנוגע לאיזושהי הפרה פרטנית.

מה ביחס למנועי החיפוש?

הסיבה שמנוע החיפוש הוא זירה משמעותית לאכיפת זכויות יוצרים היא שמה שלא נגיש באמצעותם כמעט לא נגיש כלל. הדחקת תוצאות בהחלט מקשה על גישה לתוכן ובעלי זכויות מצאו שזה גורם ביניים שמשיג את התוצאה גם מבלי להגיע לאתרים ספציפיים בהם התוכן מפורסם. אזי כשמגישים בקשת הסרה לגוגל, היא חסימת קישורים לתוכן המפר. שהקישורים לא יעלו במנוע החיפוש (חלק מנוהל הודעה והסרה).

גוגל מפרסמת נתונים גולמיים ביחס לבקשות הסרה שהתקבלו אצלה בדו"חות שקיפות תקופתיים.

**23/4/18**

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

מנוע החיפוש של גוגל הפך לכלי משמעותי לאכיפה זכויות יורים ברשת בשל תפקידו המרכזי בגישה לתכנים ברשת. תכנים שאינם נגישים באמצעות מנוע החיפוש או שנדחקים לתחתית תוצאות החיפוש, מאוד קשים לאיתור. הדרה מתוצאות חיפוש יכולה להקטין משמעותית תעבורה באתר.

בגלל עושר המידע הקיים באינטרנט, כגורם ביניים מנועי חיפוש וגוגל בפרט, אם אינך ממוקם במקום גבוה דיו בתוצאות החיפוש – מידת החשיפה של האתר קטנה באופן משמעותי כי קשה למצוא אותו. מבחינת בעלי זכויות יוצרים, הפנייה לגוגל כאתר צד שלישי, זה מקטין משמעותית את הפגיעה בזכויותיהם.

\***בקשות הסרה –** בעלי זכויות יוצרים לכאורה מבקשים מגוגל לאכוף את זכותם ע"י הסרה של קישורים לחומרים מפרים לכאורה מתוצאות מנגנון החיפוש של החברה. אנחנו מבינים שבהשוואה לביצוע מבחנים משפטיים משמעותיים יותר, כאן יש רק טענות, רק כתב תביעה (ללא כתב הגנה).

גוגל מפרסמת נתונים גולמיים ביחס לבבקשות הסרה שהתקבלו אצלה בדו"חות שקיפות תקופתיים.

**ממצאים נוספים:**

בתקופת המחקר, נשלחו 7091 תלונות על הפרת זכויות יוצרים לכאורה המתבצעת ב219 שמות מתחם ישראליים. בכל התקופה שנבדקה בביהמ"ש בין 2010-2012 נדונו בבית המשפט בישראל 190 תיקים שעניינים הפרת זכויות יוצרים באינטרנט.

קיים מספר בולט של שחקנים חוזרים הפעילים בהגשת בקשות הסרה, בעיקר חברות רב לאומיות בתחום התוכנה וחברות סרטים. חברת מיקרוסופט הגישה את מספר התלונות הגבוה ביותר.

בקשות הסרה של אתרים מתוצאות נחיפוד הכוכל מתוך: דו"ח השקיפות של החברה:

**כיצד פועל המנגנון?** מציגים את זה בגוגל כמנגנון פשוט ויעיל לבעל זכויות היוצרים. מדובר בטופס אינטרנטי פשוט למדי, שולחים הודעה לגבי התוכן המפר לכאורה, יש התייחסות לבדיקת הצוותים בקפידה (צוותים אלגוריתמיים כמובן) ואם אין בעיה – מסירים.

איזון ערכים חברתיים באכיפה ע"י גורמי הביניים: הרשת איננה רק זירה להפצת תוכן מפר. לצד הגנה על קניין רוחני והאינטרסים הלגיטימיים של בעלי זכויות היוצרים, חשוב להבטיח הגנה על הערכים שטמונים ברשת כזירת יצירה ומסחר:

- כזירת מסחר: חופש העיסוק, התחרות החופשית וזכויות הצרכן.

- כסביבת יצירה, תרבות, שיח וחיברות: הגנה על האוטונומיה של הפרט, הזכות לפרטיות, חופש הביטוי, חופש הגישה למידע וחופש ההתאגדות (הוכר ב**פס"ד מור נ' ברק אי.טי.סי. החברה לשירותי בזק בינלאומיים בע"מ**).

כיום אין ביקורת שיפוטית או פיקוח ציבורי שמבטיחים כי האיזון שמושג באכיפה ע"י גורמי הביניים הוא ראוי.

נשאלת השאלה באיזו מידה גורמי הביניים מגנים גם על האינטרסים הללו? אם חושבים כמה הגנות מגולמות בפעילות ההסרה של גוגל, התשובה לא ברורה וגם אין יכולת לפקח. לא לציבור, לא לביהמ"ש או לרגולטור שההליך אכן משיג איזון ראוי בין הערכים המתנגשים הללו. חשוב לציין שזו לא רק תפיסה תיאורטית, אלא היא הוכרה גם ע"י ביהמ"ש העליון בפרשת מור. חשיבות האיזון בין אינטרסים שונים הגלומים ברשת.

**המציאות המשפטית עלולה לעודד גורמי ביניים לפעול לניטור וחסימת יתר של תכנים ומשתמשים, גם מראש:**

- באמצעות חיוב גורמי ביניים לפעולות ניטור וחסימת תכנים או משתמשים.

- באמצעות עיצוב מציאות טכנולוגית שמאפשרת שליטה, ניטור ומעקב. כך גם ייתכן ניצול לרעה של מנגנון ההודעה וההסרה (תלונות שווא).

החשש הוא שבגלל המציאות הזו והמנגנונים היקרים לתפעול הללו וכל תקיפה בביהמ"ש של הפרת זכויות יוצרים ע"י גורם ביניים כרוכה בעלויות משפטיות רבות, כך שיש חשש כאמור שמתמרצים במציאות שנוצרה את גורמי הביניים לפעול יותר מדי ולחסום תכנים ומשתמשים כדי לנהל סיכונים משפטיים, גם מראש. אף לא להגיע למצב של ההסרה, אלא למנוע פרסום. כך גם ייתכן ניצול לרעה של מגנון ההודעה וההסרה ושליחת תלונות שווא, זה מעבר לפעולה שאינה הוגנת מצד גורמי הביניים. יש כאן פתח לאנשים שאינם בהכרח בעלי זכות היוצרים, להגיש תלונות שווא ולחסום תכנים לגיטמיים.

**דרכים לצמצום או מניעת הסיכונים:**

מבחינת פיקוח חיצוני ולא רק פנימי מבחינת ערעור, לא רק באמצעות יישום של טכנולוגיות מתקדמות יותר, אנחנו יכולים לדאוג מבחוץ כרגולטור ליצור כללים ברורים ביחס לטיפול בתלונות, למשל: ניתן להפחית תלונות שווא אם נחייב את המתלונן להזדהות או אם נחייב אותו לספק מידע ונפעיל אמצעים מינימליים כלשהם כדי לברר את הזכות.

- יצירת כללים ברורים בדבר טיפול בתלונות, למשל: ההזדהות המתלונן, נקיטת אמצעים מינמליים לבירור זכויותיו.

- שקיפות לגבי היקף שיתוף הפעולה בין גורמי ביניים לבעלי זכויות.

- שקיפות לגבי אופן הפעולה של מנגוני האכיפה של גורמי הביניים.

\*מה הם מבקשים מהם כדי להוכיח? האם יש מסלול מהיר וישיר אם סומכים על חברה כמו מיקרוסופט או איזו בדיקה נוקטים בה כדי להשתכנע אם התלונה מוצדקת לצורך הסרה?

כוחות השוק פיתחו במצב המשפטי סביב נוהל הודעה והסרה ודוקטרינת ההפרה התורמת, נעבור לדבר על סעדים טכנולוגיים באופן כללי ועל השלב הבא שמערב את מערכת המשפט – צווי הגבלה. במקום לבקש מכל אתר/גורם ביניים לחסום גישה לתוכן מפר. עולים רמה אחת מעלה ומבקשים מספקית הגישה לאינטרנט לחסום גישה לתכנים מסוימים בצורה גורפת. התיקון לחוק (הצעת חוק שטרם עברה) מציע לקבוע את הסכמות הזו כסטטורית ועד היום מרבית בתי המשפט קבעו שאין סמכות להוציא צווי הגבלת גישה בהיעדר מקור בחוק.

**סעדים שנפסקים במסרת הליך שיפוטי "מסורתי":**

פסיקת סעדים ע"י ביהמ"ש שדורשת את ההכרעה בשאלה האם התקיימה הפרה או לא. היישום של צו כזה שמורה לחברה מסוימת להסיר שלט פרסומת כי הוא מפר זכויות יוצרים, הוא קורה בעולם הגשמי והוא חד פעמי באופן שביהמ"ש מורה עליו.

**מאפייני סעדים טכנולוגיים (כמו צווי הגבלת גישה):**

- כפופים להליך משפטי מקוצר ופשוט ללא הכרעה מהותית בשאלת ההפרה. מאפשרים לבעלי הזכויות להפסיק בקלות ובאופן מידי את הפעילות המפרה.

- מיושמים ע"י אמצעים טכנולוגיים דינמיים ובלתי שקופים (מוכוונים לעולם דיגיטלי שמשתנה אף הוא).

- פרטיה הטכניים של טכנולוגיית הגבלת הגישה (החסימה) שמשמשת ליישום הצו מגדירים את היקף התחולה והאפקטיביות של צווי ההגבלה, ולכן: מגדירים את היקף ההגנה שניתנת בפועל לזכויותיהם של בעלי זכות היוצרים. מגדירים את האיזון בין זכויות בעלי זכות היוצרים וזכויות בעלי תכנים, ספקי גישה וציבור המשתמשים כמו חופש הביטוי והזכות לפרטיות.

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

הרעיון של סעדים טכנולוגיים קיים באופן כללי ויש אכיפה שקורית ע"י גורמי הביניים כל העת ויש צווים של ביהמ"ש שמחייבים לקיים סעד שנקבע בביהמ"ש ואופן היישום הוא טכנולוגי.

מעשית, יש טכנולוגיות שונות כדי לחסום/להגביל גישה, הטכנולוגיה שבה גורם הביניים יבחר תגדיר מעשית את התחולה והאפקטיביות של צו ההגבלה. למשל: אם בהליך שמתקיים בבימ"ש הוא מגדיר את היקף ההגנה על זכות היוצרים מול אינטרסים/קובע איזון מסוים ביניהם. כאן, האמצעי שגורם הביניים יבחר לקיום הצו/הסעד הטכנולוגי, הוא שיעשה את האיזון הזה בטכנולוגיה מסוימת – אם יש טכנולוגיה זולה המייצרת הגבלה גדולה יותר, קשה לראות את הצעת החוק וביהמ"ש לפנים האיזון הנכון. שיקול הדעת נתון לספק הגישה.

**מאפיינים טכנולוגיים של צווי הגבלת גישה:**

- הוצאת הצו אל הפועל נעשית באמצעות אלגוריתם או קוד שמונע תעבורה לאתר החסום. ההגדרות הטכניות שבסיס האלגוריתם או הקוד קובעות למעשה את היקף תחולתו, יעילותו והשלכותיו של סעד החסימה. קיימות טכנולוגיות חסימת תכנים שונות, הנדבלות זו מזו מבחינת עלות, אפקטיביות ופגיעה אפשרית בתכנים לגיטמיים.

- האמצעים הטכנולוגיים הספציפיים שיינקטו יקבעו בסופו של דבר את גבולות חופש הביטוי וישיפיעו על ניטרליות הרשת לתחרות ולחדשנות.

**הקשיים שמתעוררים בשימוש בצווי הגבלת גישה:**

- מאפייניהם הייחודיים מקשים להכפיפם לביקורת משפטית ופיקוח ציבורי.

- הליך הוצאת הצווים כפוף לפיקוח שיוטי מראש, אך יישומם, ??

- חשש שהמשטר המשפטי יתמרץ אכיפת יתר: כדי להימנע מאחריות משפטית ליישום הצווים (+ העלויות הכרוכות בכך), גורמי הביניים עשויים ליצור תשתית טכנולוגית פרטית שתימנע את אחריותם שלא באמצעות ביהמ"ש וללא פיקוח משפטי או ציבורי. הגבלת גישה לאתרים המארחים חומרים מפרים.

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

הרעה בדירוגן של תוצאות חיפוש הקשורות להפרת זכויות יוצרים ברשת

הסרה אוטומטית מראש של תכנים מפרים לכאורה.

מה יש לנו בהצעת חוק זכויות יוצרים?

הצעה זו מציעה 4 הסדרים חדשים, לא רק צווי הגבלת גישה, בין היתר הסדר פרטים וחשיפתם של גולש אנונימי. נתמקד בצווי הגבלת גישה. לפי הצ"ח זו, הסיבה שהיא מעלה הסדרים חדשים היא שיש בעיות אכיפה שבעלי זכויות יוצרים נתקלים בהם בצל טכנולוגיות חדשות (שהן כשלעצמן רצויות). כלומר, מוטמעים שני היבטים שונים בתפיסת מנסחי העת החוק והם שרשת האינטרנט מקשה על אכיפת זכויות יוצרים ושצריך הסדרים חדשים להתמודד עם זה. האם זה נכון? האם צריך הסדרים מיוחדים?

פרל ואלקין קורן אומרים שהנחות אלה היו רלוונטיות בשנות ה-90 ואינן רלוונטיות כיום. גם משום שיש יותר שירותים חוקיים לרכישת יצירות דיגיטליות ואז יש פחות הפרות וגם למעשה כי יש שליטה פיקוח מובנים בזכות הטכנולוגיות החדשות: המעבר לשירותי ענן, אינטרנט סלולרי ושירותי סטרימינג שמאפשרים שליטה רבה יותר על שימוש ביצירות. ניתן למנוע הפרה בשלב מוקדם ויחד אלה מצטרפים לירידה בהיקף הפיראטיות - הגידול בהיצע השירותים החוקיים לרכישת גישה ליצירות דיגיטליות.

יש מחלוקת כיום בבתי המשפט המחוזיים לגבי סמכות הוצאת צווי הגבלת גישה. מדברים על הגבלת גישה נגד ספקית אינטרנט שאינה צד להליך משפטי של הפרה, היא לא המפר עצמו ולא הפלטפורמה עליה מתרחשת ההפרה. העמדה המקובלת יותר היא זו שהופיעה ב**פס"ד 012 סמייל** – שם חברת צ'רלטון ביקשה מביהמ"ש לאשר את פנייתה ל012 בדיעבד, כשצ'רלטון ביקשה שתיחסם גישת לקוחותיה של 012 לאתרים פיראטיים שמשדרים שידורי ספורט בהם יש לצ'ארלוטן לכאורה זכויות שידור בלעדיות. היא ביקשה שיפסקו לה פיצויים בגין סירוב ספקית הגישה לקיים את הבקשה. קודם כל ביהמ"ש קבע שלספקי הגישה אין אחריות תורמת (הדוקטרינה לא חלה עליהם כי אינם חלק אינטגרלי ומשמעותי מהשרשרת שמובילה להפרה) והדבר החשוב הוא שבהיעדר מקור סמכות בחוק, לביהמ"ש אין סמכות להוציא צו הגבלת גישה/חסימת גישה. העמדה הזו זכתה להדהוד בפסקי דין אחרים. הייתה גם עמדה אחרת בפסיקה, לפיה יש סמכות – ב**פרשת בלומברג (אן.אם.סי יונייטד אנטרטיינמנט בע"מ נ' Bloomberg Inc)** היה אתר בשם יונידאון שמאפשר לגולשים להאזין ליצירות ישירות מאתר יוטיוב ועלתה שאלה האם יש הפרה תורמת של האתר וגם התבקש שביהמ"ש יוציא צו לספקיות גישה לחסום את הגישה לאתר. דווקא לאן.אם.סי היתה הצלחה נקבע שהייתה הפרה תורמת של האתר והם גם קיבלו צו חסימת גישה. כלומר קבעו שלביהמ"ש יש סמכות מכוח חקיקה שיפוטית להוציא צו כזה.

כאמור יש מחלוקת בביהמ"ש מבקש המחוקק לתת סמכות לביהמ"ש להורות על חסימת גישה ולפי ס' 53 להצעת החוק ביהמ"ש יוסמך לתת צו מניעה כנגד צדדים שלישיים לשם הגבלת גישה לאתר אינטרנט כולו/חלקו אבל באתר האינטרנט הזה עיקר תוכנו של האתר מהווה זכויות יוצרים. במקום לנקוט הליך פרטי נגד מפר/בעל אתר, חלק מהאתרים הללו יפעלו מחוץ לטריטוריה של מ"י ואין סמכות שיפוט ואין אפשרות להורות באופן אפקטיבי על הסרת התוכן המפר, מדובר על צו הגבלה שיכוון כלפי ספק הגישה ויחייב חסימת גישה לאתרים המפרים/התכנים המפרים.

**ס' 53א(ג)** להצעת החוק אומר שהספקיות יידרשו לנקוט אמצעים סבירים להגבלת גישה, נשאלת השאלה מהם אמצעים סבירים. אם ביהמ"ש לא ייתן הנחיה ברורה/קווים ליישום, ההכרעה הערכית לגבי המשקל היחסי של אינטרסים/הזכויות המתנגשות תיארך כ"י ספק הגישה. כמה חשוב לתת עדיפות לאפקטיביות של החסימה? כמה לעלות? כמה נוודא שהאכיפה מדויקה? כמה נבחן את ההשפעה על זכויות של משתמשים/בעלי אתרים? מתי תהא הצדקה להשתמש באמצעי יקר המשיג תוצאות ראויות ומדויקות יותר? האם לביהמ"ש יש יכולות לפקח על כך?

**ס' 53א(ד)** מראה רשימת סל:

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 הצו או מהחלטת ביהמ"ש שלא לתת צו.

\*כל אלו קורים בשלב הוצאת הצו ולא בשלב יישום הצו - ביהמ"ש שוקל אותם כדי להכריע אם יש מקום להוציא את צו הגבלת הגישה, אבל הוא לא (מכוח הצ"ח) מנחה לפיהם את אופן יישום הצו ע"י ספק הגישה.

לפי **ס' 53א(ב)** צו הגבלת גישה מכוון לאתר אשר עיקר התוכן שבו מפר: "בית המשפט רשאי, על פי בקשה של בעל זכות יוצרים או בעל רישיון ייחודי (בסעיף זה – המבקש), לתת צו מניעה המופנה כלפי ספק גישה ומורה לו להגביל את הגישה לאתר אינטרנט, כולו או חלקו (בסעיף זה - צו הגבלת גישה לאתר). אם שוכנע כי מתקיים לגבי עיקר התוכן שבאותו אתר אחד מאלה..." נשאלת השאלה מה זה אומר עיקר ואיך בוחנים זאת? מה לגבי פגיעה בתכנים לגיטימיים? בפועל בעלי התכנים הלגיטימיים לא יהיו צד להליך ולא תהא להם אפשרות להגן על זכויותיהם במסכרת הצואת הצו. הם יוכלו בדיעבד לשנות את הצו, אך לא במעמד הוצאתו.

גם תכנים לגיטמיים צפויים להיחסם = לפגוע בזכויות בעליהם: זכויות יסוד כמו חופש הביטוי וחופש העיסוק, ראוי שיתווסף באופן מפורש השיקול של הגנה על בעלי תכנים לגיטמיים.

בדברי ההסבר מצוין כי הדרישה לעניין "עיקר התוכן" משמעה מבחן מהותי ולא מבחן טכני כמותי, אך לא ברור כיצד יש לאומדה. ביחס לכלל התכנים באתר? רק ביחס לתכנים המוגנים בזכויות יוצרים?

מבחינה פורמלית צו הגבלת גישה הוא סעד זמני, אבל מבחינה מהותית הוא בעצם הסעד העיקרי בהליך (הוא היחיד שמתנהל בהליך) ולדבר הזה יש מספר השלכות:

אם יש סעד זמני ניתן לשנות את הקביעה הזאת בסוף ההליך, אם אנחנו רוצים לשנות את הצו בעלי זכויות תכנים לגיטמיים צריכים לפנות לביהמ"ש ולבקש ביטול/שינוי הצו. לעומת מתן סעד זמני במסגרת החוק אנחנו צריכים לשקול שיקולים בין הנזק שייגרם אם לא יוצע הצו לכל אחד מהצדדים, בהקשר של זכויות יוצרים באינטרנט נדבר על הנזק הציבורי בחסימה של תכנים, במקרה הזה אין לנו בהצעת החוק ביטוי אמיתי שמבטיח שיינתן משקל לכל השיקולים והצדדים במערכת היחסים. ההליך יכול להמשיך גם אם לא איתרנו בעלי זכויות נוספים שייפגעו מהצו.

ההליך למתן צו הגבלת גישה הוא ההליך העיקרי, היחיד והסופי המתנהל בנוגע לשאלת ההפרה – שונה מסעד זמני שעפ"י טיבו נלווה להליך עיקרי. כשניתן סעד זמני הקביעה יכול להשתנות בסוף ההליך (ביטול/שינוי של הצו אפשריים רק בעקבות פנייה חדשה לביהמ"ש של כל אדם מעוניין). כשניתן סעד זמני, יש מקום לערוך בחינה השוואתית בין הנזק שייגרם למבקש הצו אם לא יינתן הסעד הזמני עומת הנזק שייגרם לבעל האתר, מפעילו והמפר וכן הנזק שייגרם לציבור בגין חסימת התכנים (הצעת החוק אינה נותנת באופן מפורש משקל לכלל האינטרסים הרלוונטיים ולמכלול הזכויות שבסכנה, במיוחד שעה שבעלי הזכויות אינם נוכחים בהליך).

יש מספר לקחים לגבי הDMCA שיצר את נוהל הודעה והסרה והיה חלוץ עירוב גורמי הביניים בפעולות אכיפה והתמריץ המשפטי לחברות ענק אינטרנטיות לפתח מנגנוני אכיפה אוטומטיים, וניתן לקבל מושג מה קורה כשניתנים כוח ואחריות לגורמי הביניים. נוהל הועה והסרה על כבר לפני 20 שנה, מה שהוא עשה זה הפך את נטל ההוכחה בדיני זכויות יוצרים. במקום שההנחה תהא שתוכן הוא לגיטימי, הנוהל הפך את נקודת המוצא קודם מסירים כדי להימנע מאחריות, כל הלכאורה, נהיה בפועל, ללא בחינה משפטית. הבעיה היא התמריץ של גורמי הביניים. אנו לא מטילים אחריות על הספקים אם הסירו בתו"ל חומר לגיטימי. אבל, אם הספק ידע, גם אם לכאורה, על הפרת זכות – די בכך שאם בדיעבד באמת הייתה הפרת זכויות יוצרים – כדי שהוא ימצא אחראי. סיכון משפטי עצום. אין בעיה להסיר מטעות ויש בעיה לא להסיר. מי שמשלם את המחיר הם שאר בעלי הזכויות. לנו הציבור יש פחות חופש מידע באינטרנט, יש לנו משטר אכיפה אוטומטי גם במובן הזה שהרבה מבעלי הזכויות מנהלים את זכויותיהם באופן אוטומטי ובקשות ההסרה נעשות באופן אוטומטי וגם גורמי הביניים שמקבלים הכרעות באופן אוטומטי ביחס להגנה על זכויות יוצרים מכורח המציאות והופכים זאת לפעולה וולנטרית (ללא בקשת הסרה, נוקטים בזהירות מראש). למשל: מערכת הcontent ID של יוטיוב שהפכה למודל עסקי מצליח למסחור יצירות מוגנות בזכויות יוצרים - המערכת מסירה תוכן חשוד, גם אם לא היה עומד במבחן משפטי כתוכן מפר.

**30/4/18**

**פרטיות ברשת האינטרנט ושימושים שונים שניתן לעשות במידע ברשת:**

נוגע למגוון תחומים לא רק גלישה באינטרנט, אלא בכלל לחיים הדיגיטליים שלנו: מצלמות אבטחה, מאגרים ביומטריים, עולם רחב של פריטי מידע. השאלה מה המעמד של המידע הזה ומה המעמד שלנו ביחס למידע שקשור בנו ואילו כלים משפטיים יש לנו כדי להתמודד עם הגנה על המידע הזה.

"אנו מפזרים את רסיסי המידע שלנו בכל מקום ובכל פעולה אגב פעולות אחרות, וברוב המקרים בלי לדעת ככל שאנחנו משאירים אחרינו שובל של מידע ובלי להבין את משמעותו של השובל הזה... מי שילקט את רסיסי המידע יוכל לשחזר את דמותנו במידה רבה..." - מיכאל בירנהק.

בעידן הדיגיטלי כיום כל פעולה שאנחנו עושים מייצרת מידע, ולצד האפשרות הזו של ייצור מידע בהתנהלות שלנו יש אפשרויות טכנולוגיות שונות לאסוף את המידע, לתעד אותו, לעבד אותו ולהפיץ אותו הלאה. הטכנולוגיה הפכה את היכולות האלה לפשוטות ונגישות ואת העלות לעלות נמוכה יותר. אנחנו נמצאים בעולם שבו יש גורמים רבים שיכולים לבצע את פעולות האיסוף, העיבוד וכו'.

המחשבה על הגנת הפרטיות, החלה בחשיבה של האדם מול השלטון, "האח הגדול". 1984, ג'ורג' אורוול שלטו דיקטטורי או הבטחת ביטחון וסדר ציבורי. אחד הדברים שקרו עם המעבר לעידן האינטרנט, אנחנו כבר לא מסתכלים על איך השלטון מסתכל עלינו ואוסף עלינו מידע, אלא גם מה תאגידים פרטיים עושים.

כמו שני חזירים שמקבלים אוכל בחינם בדיר שהם מתכוננים לשחיטתם, כך גם תאגידים מנצלים את הלקוחות. הם לא לקוחות באופן מובהק של האתרים כמו פייסבוק, אלא הם המוצר עצמו – הם עושים שימוש במידע של המשתמשים ואת הכסף הם מרווחים מזה שהם מוכרים את המידע של המשתמשים לשימושים מסחריים.

יש משמעות בנוגע לשימוש בנתונים לפילוחים פוליטיים או חברתיים על סמך המידע האישי שנחלק ברשת. הרובד הנוסף של הגנה על הפרטיות מפני תאגידים ושימושים מסחריים שוקיים לצרכי השאת רווחים, צרכי השוק. כך יוצא שבכל מקום שבו אנחנו הולכים יש סיכונים שונים לפרטיותנו. למשל: מצלמות אבטחה, היסטוריית גלישה, מידע ביומטרי, זירות חדשות שבהן המידע נאסף, למשל: בית חכם – המכשירים בבית מדווחים על חוסרים לחברות שונות לשימושים רבים. מדובר במידע שהוא לכאורה מידע טריוויאלי, אך יש בזה גם סכנות ושימושים לרעה. מידע שרואים בו כשלנו ובוחרים מה לספר ומה לא, הרגלי החיים מאפשרים לבנות פרופיל לגבינו ללא שיהיה לנו כוח לעצב את הדמות שנוצרה – הסקה מתוך פריטי מידע של חיינו. הדברים האלה התפתחו גם כיוון שיש לכך תועלות שונות, השלטון יקבל החלטות על בסיס מידע מקיף כמה שיותר ויש תועלת רבה בכך שנראה פרסומות על מבצעים ומוצרים שמתאימים לרווחה האישית שלי. השאלה איפה נמצא האיזון הראוי ומהם הכללים המשפטיים.

יש הרבה טכנולוגיות חדשות שהשימוש בהן מייצר פטנציאל לפגיעה בפרטיות:

- שימוש בטלפון סלולרי: תחומי עניין, פעולות שבוצעו, תוכן בשיחה ופרטי ההתקשרות (עם מי אנחנו בקשר), שימוש במצלמה ובמיקרופון לציתות, באמצעות תמונות שצילמנו אנחנו מוסרים מידע על המקום.

- נסיעה ברכב עם מכשיר ניווט לוייני

- גלישה באינטרנט

- משלוח דוא"ל

- שימוש בכרטיס אשראי

- יצירת אלבום צילומים דיגיטלי

- שימוש במכשיר חכם לביש

- בית חכם – מספרים פרטים על שגרת החיים שלנו, למשל: הרגלי אכילה, הרגלי היגיינה, מה מבשלים, כמה זמן נמצאים בבית.

במציאות הזאת קורה משהו מעניין – מעקב השלטון אחר אזרחים ושליטה של התאגידים בנתוני מידע והפיכתם למקור לרווח. שני העולמות האלה גם נפגשים ואנחנו נמצאים במציאות של מעקב מידע ומעקב המונים. המידע יכול להגיע חזרה לממשלה, מידע פרטי יכול לחבור יחד עם מידע ממשלתי – יכולות להיות לכך השלכות נהדרות, למשל: ידיעה על כך שבארה"ב נעצר גבר בן 73 בחשד שביצע עשרות מעשי אונס ורצח של נשים בשנות ה-80, הגיעו אליו באמצעות ממצאים שהיו בידי המשטרה ומידע שמסרו קרובי משפחה של אותו אדם לאתרי פרופיל גנטי (שירות מסחרי שנותנים חומר גנטי). המשטרה עשתה חיבור בין המידע שהיה במאגרים שלה ובין המידע ממאגרים פרטיים שחשוד לא בהכרח התכוון למסור, ותאגידים פרטיים אוספים. למרות שאנו יודעים את הדברים האלה, בהתנהלות היומיומית של אנשים יש אשליה של פרטיות, הן בסביבה הדיגיטלית והן בסביבה הפיזית. כשעוברים ליד מצלמת אבטחה, אנחנו לא חושבים על האפשרות הסבירה של באמצעות טכניקות ניתוח תמונה נזוהה ויהיה ידוע שהיינו במקום מסוים ומה מעשינו באותו מקום. דוגמה נוספת, כשאנחנו משתמשים בכרטיס של הסופר אנחנו נהנים מהנחות שמתאימות לנו, אך אנחנו לא חושבים על ההשלכות של מה עושים עם פרופיל הרגלי האכילה שלנו, למשל: אוכל דל שומן או ללא גלוטן.

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

הגדרת פנאופטיקון:

"בניין היקפי בצורת טבעת. במרכזו מגדל המנוקב חלונות גדולים הפונים אל פנים הטבעת. המבנה החיצוני מחולק לתאים, רוחבו של כל אחד מהם כעוביו של הבניין. לתאים הללו יש שני חלונות, האחד פונה פנימה כלפי חלונות המגדל המרכזי, ואילו השני פונה החוצה ומאפשר לאור היום למלא את התא. כל שנותר לעשות הוא להציב משגיח במגדל ולאכלס כל תא במטופל, אסיר, פועל או תלמיד. תאורת הגב מאפשרת לעקוב מהמגדל המרכזי אחר הצלליות הקטנות הלכודות בטבעת התאים. בקצרה, זהו היפוך של עקרון הצינוק; אור היום ומבטו של המשגיח לוכדים את האסיר ביעילות גבוהה יותר מאשר החשכה, שסיפקה בסופו של דבר מידה של הגנה".

הכוח הממשמע והממשטר של "המבט" הננעץ בנו: שוכני הפנאופטיקון אינם יכולים להביט אל מגדל ההשמירה המרכזי, ולכן אינם יכולים לדעת מתי צופים בה. אי לכך, עליהם להניח שהם נצפים באופן תמידי.

הרעיון המרכזי הוא שמי שנמצא בתוך הפנאופטיקון לא יכול לדעת מתי צופים בו וממשטרים אותו, לכן אין לו ברירה להניח שצופים בו כל הזמן או אין לנו ברירה לשנות את ההתנהגות שלו בהתאם. הרעיון הוא שבעידן שלנו אנחנו מותירים אחרינו שובל של מידע שנאסף ונאגר והיחס אלינו יכול להשתנות על בסיס, אנחנו נמצאים בסוג של פנאופטיקון. בשאלה האם בני אדם משנים את ההתנהגות בגלל שזה המצב, זה ניתן למחלוקת – ההתנגשות בין המחשבה על פרטיות שנוצרה בעולם אנלוגי לבין החיים המודרנים הדיגיטליים וחלק מהמושגים האלה צריכים לעבור התאמה.

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

זיכרו את מודל לסיג – השפעה הדדית:

- תפישות ונורמות חברתיות של פרטיות

- הזכות המשפטית לפרטיות

- הטכנולוגיה

- השוק

ההגדרה של מהי הזכות לפרטיות בעידן הדיגיטלי, אנחנו לא מדברים רק על מהן הטכנולוגיות או איך צריך לעצב טכנולוגיות כך שלא יפגעו בפרטיות, אלא אנחנו מדברים על שיח ערכי וחברתי על המשמעות של פרטיות בעידן הזה. ייתכן שכבר אין חשיבות לפרטיות, שצריך לתת לכוחות השוק לפעול באופן חופשי ללא חסמים. השיח הזה יעזור לנו לחשוב יחד אילו כלים משפטיים אנחנו צריכים לעצב. בנוסף, איך צריך לעצב את הטכנולוגיה – האם צריכות להיות מגבלות או תכונות מסוימות בטכנולוגיה לנוכח התפיסה שלנו את הפרטיות.

**טכנולוגיה היא לא בהכרח טובה או רעה:**

1. טכנולוגיות מעקב - טכנולוגיות שמאפשרות לאתר עקבות דיגיטליות או לזהות באופן ביומטרי, זה יכול להיות מאוד נוח שאתר שאנחנו מבקרים בהם בתדירות גבוהה עושים פרסונליזציה לתכנים שאנחנו רוצים לקרוא, למשל: כתבות בתחומים שמעניינים אותנו. אמצעי ציתות מתוחכמים, אמצעי מעקב והעברת מידע לאחרים, אמצעים לעיבוד מידע ולתיעוד. איכון גיאוגרפי – כשמאבדים טלפון זה דבר שחוסך משאבים אם מאתרים אותו.

2. טכנולוגיות של פרטיות – טכנולוגיות הצפנה, אבטחת מידע, מנעולים דיגיטליים, אמצעי טשטוש עקבות – מאפשרות שליטה על המידע שלנו ועל התוכן שאנחנו מייצרים.

לאורך זמן יכול לחול שינוי במהות של טכנולוגיה מסוימת, למשל: עוגיות – הדפדפן זוכר מידע/אתרים מסוימים. הטכנולוגיה של "עוגיות" הומצאה ע"י איש מחשבים שרצה להקל על הגלישה בכך שלא צריך לזכור את כל הסיסמאות. מצד שני הטכנולוגיה הזו מאפשר מעקב אחרינו ואיסוף מידע. כך כשאנחנו חושבים על המשמעות של הטכנולוגיה נקבע המארג בין כוונת מפתח הטכנולוגיה, למאפיינים של הטכנולוגיה עצמה והשימושים שלה בפועל. כמשתמש ניתן לגלוש בסתר – כך עוקפים את הבעייתיות של איסוף המידע באמצעות הגלישה ברשת.

**צירים לדיון בפרטיות בעידן הדיגיטלי:**

- הבנת הזכות לפרטיות כמושג משפטי שנמצא במשא ומתן רצציף עם נורמות חברתיות ועם הטכנולוגיה וזה גורר השתנות.

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

- קריסת הנחות אנלוגיות שאינן מתאימות לסביבה הדיגיטלית ולחיים הפוסט מודרניים של דורנו. החיים שלנו נטועים בסביבת המידע. למשל: הייתה הנחה בהגנת הפרטיות לגבי הקשר בין פרטי ההתקשרות לבין תוכן ההתקשרות - בעבר כל מי שהיית שולחת לו מכתב היה רואה את הפרטים האישיים, ההבחנה שהתאימה למכתבים מתאימה פחות להודעות דואר אלקטרוני.

- הגנת מידע ביחסים מול המדינה ומול השוק (תאגידים פרטיים, אנשים פרטיים). הכוח שיש לכל מי שנמצא ברשת החברתית לתייג אותנו בתמונות, מפקיע מאיתנו חלק מהשליטה על המידע שלנו.

**מהי פרטיות?**

- הפרטיות כנורמה חברתית - מה אנשים בחברה רואים כפגיעה בפרטיות, למשל: להגיד באיזה קורס אני משתתף זה לא פגיעה בפרטיות, אבל לעומת זאת איזה ציון קיבלתי בקורס זו עלולה להיות פגיעה בפרטיות.

- פרטיות כזכות משפטית – הזכות לפרטיות מוגנת בחוק ובפסיקה, מדובר על יצירת כללי משחק ביחסים בינינו לבין אחרים ביחס להגנה על הפרטיות. אנחנו יכולים לדבר על הזכות שמכוחה יש איסור על אחרים לפגוע בנו ע"י האזנה לשיחות שלנו, קריאת מכתבים שלנו, צילום ברשות היחיד, הגנה על סוגים שונים של מידע כמו מידע רפואי שהוא רגיש, מידע רגיל כמו הרכלי צריכה או גלישה באינטרנט. ברגע שיש זכות משפטית היא מקנה לנו אמצעים למנוע את הפגיעה, ההטרדה או מסחור של דמותנו ומאפשרת לקבל פיצוי בשל כך. יש גם עבירה פלילית בגין פגיעה בפרטיות.

**העיגון המשפטי של הזכות לפרטיות, חוק יסוד: כבוה"א וחירותו:**

1. ס' 7 לחו"י כבוה"א וחירותו – פרטיות וצנעת הפרט:

(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.

הזכות לפרטיות בחוק הישראלי היא נגזרת של כבוד האדם, לא מתוך תפיסות קנייניות או חירות כמו בדין האמריקני, אלא קשור באוטונומיה של הפרט.

2. חוק הגנת הפרטיות, תשמ"א -1981 – קדם לחוקי היסוד וקובע איסור על פגיעה בפרטיות ומונה 12 תתי סעיפים שונים על מעשים שיהוו פגיעה בפרטיות. החוק כולל פרקים על מאגרי מידע עליהם נדבר בנפרד. החוק כולל בתוכו הגנות ומקרים של פטור מאחריות. מכיל גם עוולה וגם עבירה.

שני אלה לא כוללים הגדרה למונח פרטיות, יש רק פירוט מצבים שיהוו פגיעה בפרטיות, אך לא מגדירים מהי. ניתן לפנות לפסיקה ולדין הישראלי בכללותו, אך אין הגדרה ברורה בחוק.

**מהיכן הגיעה הזכות לפרטיות?**

מאמר - הזכות לפרטיות כ"זכות להיעזב במנוחה", וורן וברנדייס 1890 – עורכי דין שהושפעו משינויים בעולם באותה עת, שינויים בעיתונות החלו להופיע צהובונים וגם מצלמות הפכו לפופולריות יותר וניתן היה לצלם אנשים במקומות פרטיים ולתעד אותם. המניעים של וורן ברנדייס היו חברתיים וטכנולוגיים: שינויים בעיתונות (מדורי רכילות) וטכנולוגיים (פופולריות גוברת של המצלמה).

הם טענו שלמרותש הזכות לפרטיות לא מנויה בחוקה האמריקנית למעשה הזכות לפרטיות קיימת בדין האמריקני. הם הגדירו את הזכות לפרטיות: הזכות לפרטיות קיימת בדין במובן של זכותו של אדם לשלוט על פרטין על אודותיו ובאישיותו (אך קיימים גורמים שיכולים להגבילה, למשל: אינטרסים ציבוריים מסוימים).

ההגדרה הזו איננה מספקת לעידן הדיגיטלי משום שהיא לא חלה על פרטי מידע שהיינו חושבים שהם פרטי מידע טריוויאליים כמו הרגלי צריכה שלנו או הגלישה שלנו באינטרנט.

**הזכות לפרטיות כשליטה:**

בשנת 1967 הסוציולוג אלן ווסטין על סמך מחקר אנתרופולוגי הגיע למסקנה שלאנשים חשוב לשלוט במידע הפרטי שלהם. הפרטיות כשליטה: היכולת של אדם לקבוע עצמו, למען עצמו, איזה מידע על אודותיו לשתף עם אחרים, מתי, באילו תנאים ולאילו מטרות.

ההגדרות הללו לא סותרות זו את זו, אבל יש מספר הבחנות:

1. הגדרה זו קושרת את המושג של פרטיות עם האוטונומיה של האדם, הזכות הבסיסית שיש לאדם על עצמו.

2. הגדרה של הזכות להיעזב מגדירה תנאי סביל לפרטיות, כלומר למנוע התערבות של אחרים במרחב האוטונומי של הפרט. לעומת זאת, הפרטיות כשליטה מניחה שלאדם יש כלים פעילים שמאפשרים לו לשלוט על היחידה האוטונומית שלו.

זה עוזר לנו להבין איך אנחנו מגיעים לכלים קונקרטיים הניתנים לאדם כדי לשלוט על המידע שלו, למשל: עיקרון ההסכמה (מתן הסכמה מודעת לשימוש במידע) או עיקרון צמידות המטרה (הסכמה לשימוש במידע למטרה מסוימת). יכולה לחול על סוגים רחבים יותר של מידע.

**אנחנו יכולים לדבר על פרטיות במקומות:**

- ביתו של אדם, מבצרו

- בעלות על מרחב פיזי או במטלטלין שבהם יש לנו פרטיות. אם מישהו חודר למרחב האישי שלנו ללא אישור הוא פוגע בפרטיות.

- כניסה לא מורשית אליהם היא פגיעה בפרטיות: אין עורכים חיפוש ברשות היחיד ללא הסכמתו וכו'. יש הבחנות בחוק הפרטיות, למשל: החוק אוסר צילום ברשות היחיד אבל פרסום של תמונה של אדם ברשות הרבים יהיה אסור רק אם הוא עלול להשפילו או לבזותו. ישנה הבחנה בין כניסה למעמד רשות היחיד לבין כניסה למעמד ברשות הציבור.

**פרטיות בתקשורת שבין בני אדם:**

- סוגיות התקשורת מוגנת, ומי שחודר לתוכה – מאזין לה או מתעד אותה – מעשים שפוגעים בפרטיות (לאחר תיקון מס' 9 "כתב" כולל גם מסר אלקטרוני).

- ביטוי בחוק ההזנות סתר בחוק היסוד, בחוק הגנת הפרטיות:

ס' 2(2) האזנה אסורה היא פגיעה בפרטיות, ס' 2(5) העתקת תוכן של מכתב היא פגיעה בפרטיות.

- יש הגנה פחותה על נתוני התקשורת בהשוואה לתוכן התקשורת, למשל: מי שוחח עם מי, מתי, כמה זמן נמשכה השיחה. אפשר להבין מדוע יש הגנה פחותה – עבור גורמי אכיפת החוק זה כלי חשוב מאוד לחשיפת התנהגות עבריינית או רשתות עברייניות. בעידן שלנו של עיבוד והצלבת נתונים בכמויוית גדולות הן יכולות כמעט בסיסיות זה בעייתי לעשות את ההבחנה הזו כי ניתן ללמוד הרבה על אדם גם מתוך נתוני התקשורת, למשל: מבלי לדעת מה תוכן השיחה, אם אדם התקשר למספר הטלפון של מוקד תמיכה נפשי או אם אדם גולש באתר אינטרנט שדן בבעיה רפואית מסוימת זה ברור שיש לאדם עניין בבעיה הרפואית הספציפית.

**נתוני תקשורת בעידן של כריית מידע ואמצעי תקשורת חדשים:**

- טכנולוגיות של כריית מידע מאפשרות: להפוך מידע לא מזוהה למזוהה, להסיק מנתונים טריוויאליים דברים משמעותיים הרבה יותר. כלומר, ניתן לאסוף את כל הפרופיל של החיים הדיגיטליים שלי: באילו שעות אני פעילה, לאילו תכנים אני נחשפת, מי הקשרים העסקיים שלי, מה מצבי מבחינה רפואית/חברתית/תעסוקתית.

- סוגי שיחות חדשים מעוררים בעיות ואתגרים חדשים: דוא"ל, שירותי טלפוניית רשת, תוכנות צ'אט, שיחות שמעורב בהן גורם ביניים (לעיתים כצינור בלבד ולעיתים מעורב יותר).

**פרטיות במידע:**

- מידע הוא תוצר מרכזי של פעילותנו. עצם העובדה שעשינו פעילות כזו או אחר הוא נתון מידע.

- מידע הוא "סם החיים" של הכלכלה החדשה וגם בסיס חשוב לפעולות השלטון – המידע הוא יעד אטרקטיבי.

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

ניתן לחבר שתי גישות מרכזיות לשאלה מהו מידע אישי:

א. הגישה בארה"ב – גישה סקטוריאלית – הדין הפדראלי מגדיר שמידע בעניינים מסוימים הוא מידע פרטי, מוסכמות חברתיותש באות לידי ביטוי בהצהרת המחוקק, למשל: מידע פיננסי, בריאותי, גנטי, מידע שנאסף על ילדים מתחת לגיל 13 באינטרנט, מידע על תלמידי ביה"ס (ציונים), מידע על קלטות וידיאו או סרטים שמזמינים בשירותי צפייה.

כל מה שלא הגדרתי בחוק כפרטי לא ייחשב פרטי ולא יזכה להגנה מכוח הזכות לפרטיות. בדין הפדרלי מידע שאינו מוסדר בחוק מסוים לא ייחש פרטי ולא יזכה להגנה תחת הזכות לפרטיות. ככל שיש לשוק עניין במידע זה ניתן לסחור בו.

ב. הגישה האירופית – גישה מרחיבה – כל מידע ייחשב לפרטי אם הוא קשור לאדם מזוהה או לאדם שאפשר לזהותו. מתייחסת לפרטיות כנגזרת של ענף "הגנת המידע" וזו תפיסה שקשורה לכבוד האדם. היא גישה מרחיבה מאוד משום שגם מידע טריוויאלי, למשל: הרגלי הצריכה על אדם הוא עניין של פרטיות. פעולות שקשורות לאיסוף מידע ולעיבודו כפופות למשטר של הגנת מידע – חובות שמוטלות על אוסף המידע ועל המחזיק בו ולמושאי המידע יש זכויות.

**הגדרת מידע אישי בGDPR (ס' 4(1)):**

מגדירה פרטיות ?? נדבר על זה בשבוע הבא

**מהו מידע שמזהה את האדם לפי הגישה האירופית?**

- מידע שמזהה את האדם – אבל זיהוי האדם אינו מרכיב הכרחי לצורך מתן הגנה משפטית למידע, שכן היעדר זיהוי כלשעצמו אינו מפחית בהכרח מחשיבותו של המידע.

- מידע אנונימי/סטטיסטי אם אינו מנותק מהאדם: יכול להתאפשר זיהויו באמצעות פעולה של דה אנונימיזציה, אפשרי יותר ויותר עם התפתחות טכניקות סטטיסטיות וטכנולוגיות עיבוד מידע.

אנונימיות אינה תרופת קסם להגנה על מידע, דרושים אמצעים נוספים כמו: סנקציות פליליות, אזרחיות ומשמעתיותב מקרה של הפפרה, פסילת החלטות שהתקבלו על בסיס מידע כזה או אחר.

גם אם הוא לא מזהה אותו באופן ישיר, אלא מידע אנונימי, סטטיסטי אם ניתן באמצעותו לזהותו אדם. גם האדם הזה יהיה בר הגנה. כלומר, אם ניתן לעשות דה אנונימיזציה לאדם ולזהות למי המידע שייך הוא יהיה זכאי להגנה. בפועל, יכולים יותר ויותר לזהות אנשים באמצעות טכניקות של ניתוח סטטיסטי/כריית מידע ממקורות רחבים.

הגישה בישראל קרובה יותר לגישה האירופאית, אבל כן יש זכות כללית לפרטיות והיא משתרעת על הפרטיות במידע במובן הזה שלא הגדרנו תחומים מסוימים שבהם הזכות תחול, אבל יש אמת מידה תוכנית מסוימת – זה לא מספיק שהמידע מזהה את האדם, סוגי מידע מסוימים יזכו להגנה אבל יש מרחב פרשנות שיפוטי רחב בנושא.

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

יתרונות:

- תאגידים מסחריים, מעסיקים או בעלי כוח אחר, וכן מצד פרטים אחרים מתבססים על מידע כדי להבין את לקוחותיהם, רצונותיהם, ונכונותם לרכוש מוצרים ושירותים.

חסרונות:

- באמצעות המידע מנסים לנווט אותנו לרכוש עוד, סוחרים במידע ולפעמים מעבירים אותו גם לממשלה.

- אוספי המידע מסווגים אותנו לתבניות ופועלים על בסיס האפיון שאפיינו אותנו.

- טכנולוגיות מידע מעבירות כוח רב לידי אנשים פרטייםם אחרים, למשל: בתיוג אנשים אחרים ברשת חברתית.

**7/5/18**

**שיעור הרצאה: עו"ד חיים רביה**

**מהפכת הפרטיות באירופה:**

בסוף החודש ייכנסו לתוקף התקנות האירופאיות בנושא עיבוד מידע אישי שמשקפות מהפכה שאירופה הצליחה להכניס להרבה ארגונים עסקיים מעבר לתחום הטריטוריאלי של אירופה בשנתיים האחרונות. מחר ייכנסו לתוקף תקנות הגנת הפרטיות 2017, שיחליפו את התקנות משנת 1986. חברת קיימברידג' אנליטיקה קרסה (פייסבוק נקלעה לצרה רגולטורית כי חברה הצליחה לאגור מידע על מיליוני משתמשים שלה, לצורך השפעה על הצבעה.

חברה נותנת קוד חופשי כי היא רוצה ליצור גמישות למפתחים ולתת אמון בקרב המשתמשים.

**תקנות:**

האיחוד האירופי פועל בשתי צורות חקיקה:

- דיריקטיבה – דבר חקיקה של האיחוד שכל אחת מהמדינות החברות בו חייבת להתאים את דיניה הלאומיים לאמות המידה האירופאיות. העקרונות של הדירקטיבה חייבים לבוא לידי ביטוי בו.

- תקנות - עד היום ישנן תקנות משנת 1996, אירופה חוקקה לפני שנתיים את התקנות הללו, הן כופות עצמן על כל המדינות החברות באיחוד, ולא צריכות לאמץ אותן בחוק פנימי ולא יכולות לסטות מהן בחוקים לאומיים. עדיין התקנות מתירות אפשרות להסדיר עניינים באופן פרטיקולרי. מעין "גבינה עם חורים".

התקנות לוו במערך קנסות – מערך הקנסות מתחיל מ2% או 10 מיליון דולר (הגבוה מביניהם), במדרג הנמוך של הקנסות. הגבוה - 4% או 20 מיליון יורו. אשר על כן, חברות נערכות במרץ שנתיים ומתאימות את עצמן לדרישות של הGDPR.

GDPR עוסק בעיבוד של מידע אישי, הגדרותיו רחבות מאוד, הוא מטפל באינספור היבטים: החל מעקרונות עיבוד מידע אישי, יחסים בין האדם לבין נותן שירות עיבוד המידע האישי, האם מותר להעביר מידע ממדינה אחת לאחרת ובאילו תנאים.

השואה היא הגורם להקפדה על זכויות באירופה – השואה התבססה על מידע על דתם של אנשים, השתייכות קהילתית ומידע זה נועד לייצר מדיניות גזענית. הטראומה הולידה באירופה דיני הגנת פרטיות שונים לחלוטין. למשל: אם באירופה יש דין שעוסק בפרטיות והוחל על כל ארגון מכל סוג שהוא בארה"ב אין דין כזה, יש איים של פרטיות בתחומים מסוימים כמו עיבוד מידע רפואי או פרטיות של ילדים בשירותים מקוונים, פרטיות בשירותים פיננסיים.

למשל: אם אתה מפתח בארה"ב אפליקציה להיכרויות שלוקחת מידע רב על אנשים, אתה לא כפוף לשום חקיקה פרטנית. הדבר היחיד שפועל נגדך הוא סעיף שאומר שאסור להטעות בעיסוק במסחר. אם אתה פועל לפי הצהרתך, עשוי לקבל מידע רב מאוד על כל אחד.

הרגולציה האירופאית חלה על כל עיבוד של מידע, גם אם לא מתבצע באמצעות מחשב. לפני שנים אחדות יצאה בישראל הנחייה שעסקה בזכותם של אנשים לקבל את המידע שנאסף אודותם כשהם מגישים בקשה לעבודה במקום מסוים. חברות כוח אדם רצו להימנע מהחובות שיש על בעלי מאגרי מידע בישראל (מאגרים ממוחשבים) והדפיסו את המידע האישי ומחקו את הקובץ.

המידע צריך להיות מידע אישי, כלומר, אם יש מידע על פרל כהן, אז אין מידע אישי. זה יכול להיות מידע טריוויאלי כמו שם וטלפון, התקנות חלות עליו. יכול להיות שהתקנות יחולו לא רק על טלפון גם מידע שלא נוקב בשם האדם כמו שירותי WEB מי נכנס לשרת וידיעת הIP נחשב למידע אישי. ההגדרה של מידע אישי הוא כל דבר שמזהה אדם או מאפשר לזהות אדם.

התקנות חלות על כל מי שנמצא בשטח הטריטוריאלי של מדינת ישראל, אך לא על ישראלים שנמצאים מחוץ לתחום השיפוט של המדינה. הדין המאפיין שלו הוא שהוא טריטוריאלי. נעשה גם כדרך של מדינות לכבד זו את זו.

**על מה ומי תקנות ה-GDPR חלות:**

- עיבוד אוטומטי ואחר של מידע אישי

- יחידים

- חברות בEU: עיבוד מידע אישי של יחידים באיחוד לצורך: מסחר ושירותים, ניטור התנהגות.

הGDPR באו וסטו מהכלל, והן חלות על ארגונים שמעבדים מידע אישי של יחידים (גם מחוץ לתחום הטריטוריאלי של האיחוד האירופי). בתנאי שהם מייצאים מוצרים או שירותים לאזרחים באיחוד האירופי. כיוצא בזה, אם אתה מנטר התנהגות של יחדים הנמצאים באירופה, עניין רגיש. החברה המבצעת את זה כפופה לדין האירופי. מעורר קושי במוסדות אקדמאיים – תחומים רבים במחקר נוגעים לניטור התנהגות ואם הוא בוחן עיבוד נתונים של אנשים באירופה זה כפוף לGDPR.

הדין לא דבוק לאזרח, לכן כשאזרח צרפתי נוסע לנמיביה לעבוד בחברה נמיבית - אין לו זכויות מטעם התקנות. פליט סורי עובד בחברה גרמנית - התקנות חלות עליו. אזרח צרפתי נוסע לעבוד בחברה אירופאית - הזכויות עדיין נתונות לו.

**למה אנחנו מתכוונים?**

- מידע אישי – מזוהה או בר זיהוי, לא משנה אם לארגון יש את השם או לא. העובדה שאפשר להצליב בין הנתונים שיש בידי ארגון אחד לבין נתונים שיש בידי ארגון אחר הופכת את זה למידע אישי.

- עיבוד – ההגדרה מרחיקת לכת ורחבה, היא מקיפה כמעט כל פעולה: איסוף מידע, אחזור של מידע, הפצה של מידע, מחיקה של מידע והשמדה של מידע. אין דבר שדיני פרטיות יעדיפו מהשמדת מידע לכאורה, ועדיין פעולת השמדה באה בגדר עיבוד שכפוף להוראות התקנות. הסיבה היא שאמנם תופסים את זה כפרטיות, אך תחולתו רחבה יותר. זכויות בעיבוד מידע אישי, לא רק הגנת הפרטיות כפשוטה. כל יחיד זכאי לקבל מידע אודותיו מארגון שמעבד מידע בתבנית שמאפשרת להעבירו לארגונים אחרים.

הזכות להיעזב the right to be let alone – הגישה של וורן וברנדס לזכות לפרטיות. גישות מאוחרות יותר מתמקדות בזכות לשלוט במידע שלך.

- CONTROLLER – אותו גוף שקובע את מטרות עיבוד המידע והאמצעים לעיבוד המידע.

- PROCESSOR – מי שמספק בפועל את השירות של עיבוד המידע.

הבנק הוא קובע את המטרות שלשמן המידע יעובד, לצורך סיפוק שירותים בנקאיים והוא יבצע את עיבוד המידע במחשבים שלו (הבנק משמש גם CONTROLLER וגם PROCESSOR). ארגון רוצה לבצע ניסויים רפואיים בבני אדם – פיתחו תרופה, רוצים לנסות, לאסוף מידע ולעבד אותו - הארגון יהיה CONTROLLER, אך הניסוי יתבצע במסגרת מרכז רפואי כמו ביה"ח שיש לו את המידע הזה והרופאים מטפלים בחולה באמצעות התרופה הניסויית. ביה"ח יהיה גם הוא ה CONTROLLER – שניהם יחד יהיו JOINT CONTROLLER על כל אחד מהם יחולו מלוא החובות ביחס לעיבוד המידע. ניסויים רפואיים מתבצעים גם באמצעות חברות שבוחרות פציינטים, למשל מנהלות את הניסוי – החברות האלה הן PROCESSOR.

- SOFTWARE AS A SERVICE – הצעת תוכנות שמתבצעות לרוב ע"י אינטרנט, ונצרכות באמצעות דפדפן האינטרנט. ספקים מספקים לחברות הצעות שונות, ניהול מערכת בענן. יכול להיות שהחברה המעבדת תרצה להשתמש במידע על הלקוחות לצרכים אחרים – שימושים לצרכים עסקיים משלה, היא תהפוך מ PROCESSOR ל- CONTROLLER.

**לפי התקנות עיבוד מידע חייב להיות:**

- חוקי, הוגן ושקוף

- למטרה מוגדרת – יש ניסוחים כגון "ולכל דבר אחר" – מאפיים העידן הוא שאיננו יודעים מה נוכל/נרצה לעשות במידע בעוד חצי שנה, למשל, והמידע קריטי להצלחה עסקית ולכן מותיר מרחב פעולה ע"י ניסוחים עמומים. הGDPR מבקש להילחם בזה ומבקש מטרה מוגדרת. היחידים צריכים להסכים למטרות.

- תואם, רלבנטי ומוגבל למטרה – למשל: AIR BNB צריכה לדעת שם, אשראי, מייל, טלפון – אבל היא לא יכולה לבקש לדעת מה המין או מה סוג הרכב של אדם כיוון שהמידע לא תואם את מטרת העיבוד.

- מדויק ועדכני – איזה מאמץ דרוש לארגון לשמור מידע על עשרות מיליוני בני אדם, באופן מדויק ועדכני.

- מוגבל בזמן – נשמור את המידע לנצח כי זה זול יחסית, מרבית המידע לא צורך נפח אחסון גדול ויש מטרות דחופות יותר מאשר לקבוע מנגנונים למחיקה ואנחנו לא יודעים אם בעתיד נזדקק למידע. למשל: יש ערך לזה שנצבור מידע ונוכל להריץ על המידע ההיסטורי עיבודים. הGDPR אומר שאפשר לשמור את המידע רק לצורך מימוש המטרה, אלא אם כן יש חריגים (למשל: החוק מחייב דיני מס הכנסה או לצורך תביעה).

- מאובטח – לא חל על ביטחון חוץ וחקירת מניעת פשעים. היו דינים כאלה שנפסלו באירופה.

**מה ייחשב לעיבוד חוקי?**

1. מבוסס הסכמה: להסכמה שני חסרונות: הסכמה תמיד אפשר לבטל ולא תמיד אפשר לקבל הסכמה. בכל מקום שיש ממשק עם הלקוח, קשר בלתי אמצעי עם הלקוח, יש אפשרות לבקש הסכמה. צריך לבקש הסכמה לכל מטרה בעיבוד המידע.

2. חיוני לביצוע חוזה: אם אני מעסיק אני חייב לעבד מידע אודות עובדים בחברה לצורך עריכת חוזה העסקה (שם, כתובת, מצב משפחתי, קרנות פנסיה וכו'). האם אני חייב לקבל הסכמה מהעובד? לא לפי הGDPR באירופה. בישראל נחוצה מדיניות פרטיות בקשר לשימוש במערכות הטכנולוגיות של המעסיק.

3. חיוני לציות לחוק: גם לצורך ציות לחוק, למשל: צווים שקיבלתי מבית משפט או דיני מס הכנסה.

4. חיוני לאינטרס אישי של נושא המידע או צד שלישי (טיפול רפואי)

5. חיוני לאינטרס הציבורי (מחקר סוציולוגי, המאגר הביומטרי)

6. חיוני לאינטרס לגיטימי של ה CONTROLLERאו צד שלישי (מעבד מידע כדי ללמוד לשפר את האפליקציה שבאמצעותה הוא אוסף את המידע)

**הסכמה:**

 - חופשית, מוגדרת ומודעת

- חובת ההוכחה על הCONTROLLER

- נפרדת מעניינים אחרים

- שפה נגישה וברורה – שיהיה ברור למה הסכמנו

**שקיפות:**

- על הCONTROLLER למסור מידע תמציתח, שקוף, מובן, נגיש בקלות בשפה ברורה ופשוטה

- בחינם

- מתי למסור: בעת קבלת המידע מנושא המידע, אם לא התקבל מנושא המידע – לפי המוקדם: תוך חודש/בתקשורת עם נושא המידע/במסירה לאחר.

מה למסור: זהות הCONTROLLER, פרטי הקשר והמייצג, מטרת העיבוד, מי יקבל המידע, העבברה בין מדינתית, תקופת האחסנה, זכות הגישה והתיקון, זכות הביטול, זכות התלונה, האם האספקת המידע נדרשת בחוק או בחוזה, מערכות אוטומטיות לקבלת החלטות, מקור המידע (כשלא נמסר מנושא המידע).

מה שיעשו במידע קשור למדיניות הפרטיות שלהם, ושל עוד ארגונים רבים – המשתמש לא ייקרא את המדיניות של חברות רבות.

בGDPR יש עיקרון יסוד שאוסר להעביר מידע מהאיחוד האירופי למדינות שאינן באיחוד ושרמת ההגנה בהן אינה כרמת ההגנה באיחוד. העיקרון הזה "תאימות" משתקף בדירקטיבה שהGDPR מחליף. האיחוד האירופי הכריז על 13 מדינות כתואמות – ישראל אחת מהן, כלומר הדינים הישראליים תואמים את הדינים האירופאיים בכל מה שנוגע לעיבוד מידע. אין להעביר מידע אלא למדינה תואמת, אם אינה תואמת – צריך להצהיר על כך ולומר מהן ההשלכות או דרך הסדרים חוזיים. בעולם של אינטרנט העברת מידע עוברת במהירות, אנחנו לא יודעים איפה המידע נמצא – העברת מידע בין מדינתית מתרחשת כהרף עין.

**זכות העיון והתיקון:**

- גישה למידע – יחיד תמיד יכול לדרוש מארגון לראות את המידע עליו.

- תיקון מידע לא מדויק - יחיד תמיד יכול לבקש מארגון לתקן את המידע.

- השלמת מידע חסר – יחיד בעל הזכות להשלים את המידע.

**הזכות להישכח The right to be forgotten:**

- על מי החל החובה לשכוח - הזכות של היחיד לבקש למחוק אותו ולא להיות קיים במאגרים של חברה. המידע עליי נכון/רלוונטי אך הפסקתי להסכים שתעבד את המידע עליי. הזכות הזו הוכרה לפני 3 שנים בפס"ד בעניין גונזלס נ' גוגל – אדם מספרד שבשנת 1998 נקלע לצרה כלכלית ועיקלו את ביתו. המידע הופיע במודעה באתר חדשות ספרדי, הוא פנה לגוגל ואמר שזה לא רלוונטי. 20 שנה לאחר מכן, הוא אדם אחר. גוגל לא הסכימה, וביהמ"ש האירופי חייב למחוק את המידע אודותיו למרות שהוא נכון. זה הניב מיליוני פניות והליכים רגולוטוריים שניסו לכפות על גוגל למחוק את המידע מהכל ולא רק ממנועים אירופים. הזכות הזו הורחבה בGDPR מחייבת גם את האתרים עצמם ולא רק את מנועי החיפוש.

זכות זו לא מוכרת בישראל, חוק הפרטיות תוקן ב1981 – לפני האינטרנט, טכנולוגיות שאיפשרו פיענוח מצב רוח ובריאות בהתאם לקול/תמונה. כלומר העולם המודרני של עיבוד מידע לא היה מוכר. אירופה לעומתנו חוקקה דירקטיבה ב1996 ומחליפה אותה, החוק הישראלי מיושן לא מתאים לימינו דינו להתחלף.

**28/5/18**

**הגנת הפרטיות בעידן הדיגיטלי בישראל:**

היכולת שלנו לצרף פרטים על הפרט השתפרה פלאים. בשיעור המבוא דיברנו על שתי גישות שונות להגנת הפרטיות: האירופאית והאמריקנית. הגישה האמריקנית היא גישה סקטוריאלית (אין זכות רחבה להגנת הפרטיות אלא הפרטיות מוגנת במקום שבו יש הסדר ספציפי בחוק). ע"פ גישה זו, מה שלא אסור – מותר. הגישה האירופאית היא גישה רחבה יותר הנותנת הגנה על זכות כללית בפרטיות. גישה זו הופיעה כבר בדירקטיבה שקדמה ל-GDPR. היא רחבה בהרבה מאוד מובנים – גם בתחולה שלה, גם בהגדרה שלה למידע רגיש (כל מידע שמזהה את האדם).

הגישה הישראלית היא גישה שקרובה יותר לגישה האירופית: זכות כללית לפרטיות.

* זכות חוקתית לפרטיות מתוקף ס' 7 לחוק יסוד: כבוד האדם וחירותו
* הגנה רחבה למדי על פרטיות במידע מכוח פרק ב לחוק הגנת הפרטיות, התשמ"א-1981 (הסדר מפורט של מאגרי מידע); פרק ד' לחוק הגנת הפרטיות התשמ"א-1981 (הסדר להעברת מידע בין גופים ציבוריים); תקנות הגדרת הפרטיות

חוק יסוד כבוד האדם וחירותו קובע שכל אדם זכאי לפרטיות ולצנעת חייו וגם מפרט שלושה מצבים שבהם זכאי האדם לפרטיות: רשות היחיד של האדם, גופו והתקשורת שהוא מנהל.

על כך נוסף חוק הגנת הפרטיות התשמ"א-1981 שקובע איסור מפורט לפגיעה בפרטיות. החוק לא מגדיר מהי בדיוק הזכות לפרטיות אבל הוא קובע שיש זכות לפרטיות ומפרט מצבים שמהווים פגיעה בפרטיות, שהם בחלקם מצבים שמתייחסים לפגיעה ב**פרטיות פיזית**, האזנות סתר, צילום, בילוש, וגם למצבים שאפשר להתייחס אליהם כ**פרטיות במידע** כמו הפרת חובת סודיות בנוגע לענייניו הפרטיים של אדם, פרסום מידע ביחס ל"צנעת חייו האישיים של אדם" ועוד.

פסק הדין המרכזי שעסק בסוגיה זו הייתה פס"ד ונטורה. באותו מקרה רשם מאגרי המידע סירב לרשום מאגר מידע שביקש להירשם מהטעם של אי חוקיות. היו אלה יזמים שביקשו להקים שירות ששומר מידע על נתוני אשראי של משתמשים. הרשם סבר שקיום מאגר מידע שכזה, שעושה שימוש שלא במטרה לשמה מושאי המידע מסרו אותו, נוגד את עיקרון "צמידות המטרה" (אפשר לעשות שימוש במידע רק למטרה לשמה הוא נועד). ונטורה פנו לביהמ"ש אשר אישר את העמדה של 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, זהןת חבריו, יחסיו עם אשתו ויתר חברי משפחתו וכדומה".

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

תוכנה צופת פני עתיד הגנת המידע בעידן הדיגיטלי (שטרסברג-כהן): יתכנו מקרים בהם כל פרט בנפרד אינו בהכרח "ענייו פרטי" אולם צירוף פרטים יחד עשוי להיות עניין פרטי מוגן.

הסדר ספציפי למאגרי מידע – פרק ב' לחוק הגנת הפרטיות

הגדרות – ס' 7 לחוק.

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

**"מידע רגיש"** – (1) נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו (2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה 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 איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

מה המעמד של מאגר ידני לפי החוק? הגישה הישראלית שונה מהגישה האירופאית ומחריגה את המאגרים האנלוגיים (בשונה מדיגיטליים) כי ההנחה היא שהסיכון הוא פחות.

החוק מתייחס ל**"נתוני מידע",** ולא לנתונים שעובדו. אם יש המלצה שנכתבה על סטודנט על סמך הנתונים במערכת המחושב של האוניברסיטה שכוללת את הציונים שלו, עומס הקורסים, מוסר התשלומים שלו לאוני', הקורסים שביצע וכו' – נפריד את הדו"ח שהוא תוצר של עיבוד הנתונים מהנתונים עצמם.

הדבר רלוונטי כאשר מדברים על הזכויות של מושאי המידע. אם יש למושא המידע זכות לעיון בנתונים, היא לא תחול על אותו דו"ח אלא על נתוני המידע בלבד.

מאגרים יכולים לשנות את טבעם ולצאת מגדרי ההחרגה ולהפוך למאגר מידע במונחי החוק.

בישראל יש כ-15,000 מאגרי מידע.

**חובות מנהל מאגר מידע – רישום מאגר**

          "מנהל מאגר" - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;

**רישום מאגר מידע והשימוש בו (תיקון מס' 4)  תשנ"ו-1996**

8.    (א)  לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:

(1)   המאגר נרשם בפנקס;

(2)   הוגשה בקשה לרישום המאגר והתקיימו הוראות סעיף 10(ב1);

(3)   המאגר חייב ברישום לפי סעיף קטן (ה) והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו.

          (ב)  לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

          (ג)   בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

(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.

קשה להגיד שהמאגר ממלא את הייעוד שלו בהרגעת החשש של אנשים לגבי איזה מידע נאסף עליהם. בעיה נוספת היא שההערכות הזהירות הן שרק כ-2% ממאגרי המידע במדינה רשומים.

**מדוע יש חובת רישום מאגר?**

* פיקוח מהותי
	+ סירוב לרשום מאגר למטרה בלתי חוקית (ס' 10(א)(1))
	+ שינוי מטרת המאגר המוצהרת לפי בדיקה של פעילות המאגר בפועל (ס' 10(א)(2))
* פיקוח על הפעילות – פונה למגזרים, לא רק למאגרים ספציפיים
* הנחה התנהגותית – חובת הרישום גוררת בדיקה ופיקוח פנימיים אצל מנהלי המאגרים->הגברת הציות לחוק.

**חובות מנהל המאגר – הודעה**

**חובת מבקש מידע**

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

(1)   אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו;

(2)   המטרה אשר לשמה מבוקש המידע;

(3)   למי יימסר המידע ומטרות המסירה.

החובה הזאת חלה גם על מי שכבר מנהל מאגר מידע בפועל, וגם על מי שפועל כדי להקים מאגר מידע.

חשיבות חובת ההודעה היא בכך שהיא מהווה בסיס לקבלת הסכמה מדעת של מושא המידע. ההודעה היא בסיס להפעלת עיקרון צמידות המטרה (ס' 2(9), ס' 8(ב).

היעדר דרישות צורה להודעה היא בעייתית. בנוסף, החובה לא מתייחסת לזכויות מושאי המידע – הזכות לגשת למידע, לעיין בו, לדרוש את תיקונו.

**חובת הסודיות ואבטחת מידע** הן שתי חובות שקשורות לסיכון ודליפה של המידע במאגר. הרצון הוא להקטין את הסיכון שבדליפת המידע.

          "אבטחת מידע" - הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;

אנו קובעים סטנדרט ולא אמצעים מתוך הבנה שקצב השתנות הטכנולוגיה הוא מהיר, וכן על בסיס עיקרון של ניטראליות טכנולוגית – אנחנו לא מעדיפים טכנולוגיה כזו או אחרת.

**בשיעור הבא – אורח ממשרד התקשורת שידבר על ניטראליות רשת והאתגרים שיש ביצירת מכשירים רגולטוריים מהסוג שדיברנו עליו.**

**4/6/18**

**אורנן שטיינברג – היועץ הבכיר של היועמ"ש למשרד התקשורת:**

steinbergo@moc.gov.il

במשרד התקשורת יוצרים את הנורמות, החוקים בתחום התקשורת.

ההיבטים הרגולטוריים בשוק עתיר טכנולוגיה - נקודת מבט מתוך משרד התקשורת על הנגישות לתשתיות תקשורת, האינטרנט של הדברים וניטרליות רשת.

הנושאים: סייבר במובן של תקשורת, אינטרנט, משפט וחירום, תדרי רדיו.

שוק התקשורת דינמי ועתיר פיתוחים טכנולוגיים, השוק מגלגל 20 מיליארד בשנה והמשרד שאחראי על הפיקוח של השוק זה משרד התקשורת. נושאים שמשפיעים על כלל הציבור, למשל: רפורמת הסלולר, פיצול בערוצים, מיזם הסיבים האופטיים (חברת החשמל תסייע בפריסת סיבים אופטיים), השוק הסיטונאי (ספק ותשתית רשת), תאגיד השידור הציבורי, פיצול ערוץ 2, העברת שידורים מחו"ל כמו נטפליקס.

משרד התקשורת עוסק בתחומי טלקום - טלקום זו תקשורת נייחת קווי טלפון, סלולרי, אינטרנט, כבל תת ימי, שיחות בינלאומיות ולוויינים, דואר, שידורים. העיסוק של משרד התקשורת הוא ברמת המאקרו, רמת העל. יש תחומים שקשורים לעולם התקשורת, אבל אינם כפופים למשרד התקשורת: שלום הציבור מבחינה בריאותית (הממונה על הקרינה הסלולרית במשרד להגנת הסביבה). מי שנותן תוקף משפטי הוא המשפטנים שמצביעים על הקשיים במדיניות. השלב של קביעת הנורמות – אורזים את ההחלטה/מדיניות בחליפה של כללי התנהגות והצ"ח. כדי לעשות זאת צריך שהלשכה המשפטית תהיה מעורבת מתחילת התהליך, מלווים את כל התהליך עד סופו. ההחלטות במשרד נקבעות בצוותי חשיבה: מהנדסים, משפטנים וכלכלנים. הלשכה המשפטית עוסקת בניסוח הצ"ח, ייצוג המשרד בוועדות הכנסת השונות ובוועדת השרים לענייני חקיקה. הלשכה מלווה את המשרד בהליכים משפטיים: בג"צים, ביהמ"ש לעניינים מינהליים, ביה"ד לענייני עבודה וביה"ד לתביעות קטנות. החברות בשוק התקשורת בעלות אינטרס רציני לעשות מה שמתאים למודל העסקי שלהן. לכן, כאשר יש משהו שמפריע להם הם שוכרים את עורכי הדין הטובים ביותר במדינה מה שמוסיף לאתגר במשרד התקשורת.

סוגי התחומים הם מגוונים: משפט ציבורי, משפט מסחרי, משפט וכלכלה, דיני רגולציה, צרכנות ומשפט וכלכלה. במשרד יש כ-15 עורכי דין ו2 מתמחים.

**משרד התקשורת והטכנולוגיה:**

**עקרונות האסדרה –** עקרונות על שיש למשרד, לשר – תכליות שאנו רוצים להשיג כדי ששוק התקשורת יהיה טוב:

א. שירותים מתקדמים – שהציבור יקבל שירותים מתקדמים, מהירים ואמינים. זה קשור לשדרוג מתמיד של המערכות האלה. לא רק משפיע על האזרח הקטן, אלא זה משפיע על המגזר העסקי כולו – תשתיות ושירותים מתקדמים מהווים מנוע צמיחה שמשפיע על המשק כולו.

ב. כל השירותים יינתנו במחיר סביר – תהיה נגישות לציבור לקבל את השירותים האלה.

לשוק יש דרכים משלו, לכן הדרך הנכונה היא באמצעות עידוד התחרות: מגרש משחקים שמאפשר לחברות לעשות זאת. ב1984 היה מונופול סטטוטורי, חברת בזק, הבינו שזה כבר לא יעיל לחברות להתמודד באמצעות תשתיות שונות כי הן שמות דגש רב מדי על המחיר.

**הקשר בין תקשורת וטכנולוגיה –** המשפט מפגר אחר הטכנולוגיה, הדבר הזה נכון גם לעניין המדינה ומשרד התקשורת. הסיבה לכך היא טבעית כיוון שהטכנולוגיה מגיעה מתוך השוק. סיבה אחת היא ההון האנושי – המשפטנים מגיעים ללא הידע הטכנולוגי. גם מומחים שמגיעים מהשוק לאחר שנים הם לא מעורים בטכנולוגיה. שולחים להשתלמויות את אנשי המשרד, זה מספק פתרון חלקי. מעודדים טכנולוגיה חדשה באמצעות השוק, לעיתים לפעמים נותנים הוראות כופות לסוגים שונים של טכנולוגיה. לעיתים יש החלטת מדינות מסוימת ומגיעות חברות עצמן ומציגות שיקולים שלא חשבו עליהן במשרד התקשורת. כפי שנראה במקרי הבוחן היחס של משרד התקשורת לטכנולוגיה הוא מורכב: מצד אחד, אנחנו מעודדים טכנולוגיה חדשה, אבל מצד שני כשמגיעה טכנולוגיה חדשה משרד התקשורת הוא "שומר הסף" שצריך לבחון אותה. כמשפטנים, הממשק שלהם עם טכנולוגיה – כדי לארוז את הטכנולוגיות כנורמות מחייבות צריך להבין אותן, המשפטנים מציעים את הפתרון הטכנולוגי המתאים כדי שהדבר הזה יהיה כמה שיותר חף מקשיים משפטיים.

**הממשק עם השוק –** משרד התקשורת הוא הרגולטור, אך יחד עם זאת הוא מעדיף לפעול בשיתוף פעולה. שלב גיבוש הרגולוציה ושלב אכיפת הרגולציה: בשלבי הגיבוש הממשק עם החברות הוא דרך פגישות עם החברות כדי להציף את הקשיים הטכנולוגיים, כלכליים וכו' ובשלבי האכיפה חלה חובה מכללי המשפט המינהלי להעניק לחברות זכות שימוע, סיורים בחברות עצמן. חברות מגיעות אל משרד התקשורת כדי לאשר טכנולוגיה חדשה. לגבי רגולציה קיימת, יש הוראות לגבי טכנולוגיה מסוימת, אבל החברות לא עומדות בהן. ישנן הפרות והטלת עיצומים כספיים (8 וחצי מיליון ש"ח עיצום כספי על בזק בגין השוק הסיטונאי).

**ממשק עם הציבור –** הציבור פונה ומעלה צורך מסוים שאותו מקדמים. תחקירים וכתבות שהיו בתקשורת.

1. אינטרנט מהיר – ?? בעבר הייתה טכנולוגיה ששמה DIA טכנולוגיה איטית מאוד. לפני 2000 נכנס לשוק טכנולוגיה חדשה בשם ADSL אינטרנט יותר מהיר, בזק וחברות הכבלים אמרו שהן רצו לספק את השירות הזה, הלכו למשרד התקשורת ושאלו אם הן יכולות לספק את זה. הבעיה הייתה שהחברות האלה היו חברות כבלים בלבד. הייתה בעיה בעיקרון החוקיות – המדינה יכולה לעשות אך ורק מה שהחוק מאפשר לה. מה שלא קבוע בחוק הוא האפשרות של המדינה לתת לכבלים אפשרות למתן שירותי ADSL. משרד התקשורת רצה ליזום מהלך של תיקון החוק כדי שהציבור יוכל ליהנות מהשירות המהיר של בזק. התחרות נפגעה בצורה משמעותית – אם היו נותנים לבזק להתחיל עם מתן השירות זה היה מביא ליצירת מונופול, פגיעה קשה בשוק. תחרות מצמיחה שירותים מתקדמים ומחיר סביר – השיפור הוא בטווח הקצר, אבל בטווח הארוך לא תהיה תחרות כי חברות הכבלים ובזק יתחרו כל הזמן אלה באלה.

הפתרון: מהלך מדורג -

א. נקפיא את הכניסה של טכנולוגיה ונחוקק כמה שיותר מהר חקיקה כזו. בזק לא רוצה עוד שחקן בשוק, וייתכן שהיו כוחות חזקים מצידה לעצור את המהלך הזה.

ב. אחרי שנה וחצי משרד התקשורת הבין שיש צורך באיזון כי השירותים המתקדמים נמנעי מהציבור זמן רב מדי ואיפשרו לבזק להיכנס לפני חברת הכבלים. החוק תוקן לבסוף וניתנה סמכות למתן השירות.

2. פריסה אוניברסלית – סיב אופטי נותן 10,000 מגה, הנתונים עוברים מהר מאוד (אוטוסטרדת מידע), שריד מפני מים ואש, פחות גניב (סוחרי מתכת בדרום). חברות פרטיות מבצעות את הנחת התשתיות.

שירות לפריפריה – הנגשת שירותי תקשורת מתקדמים, הזכות לשוויון לתשתיות מתקדמות נפגעת. פיזור אוכלוסיה ותעסוקה, אינטגרציה בין שכבות שונות של האוכלוסייה ומוביליות חברתית. המתח הוא: הוט אמרו שמיליארד השקלים לשירות לפריפריה יבואו על חשבון פיתוח תשתיות מתקדמות. המודל העסקי שלהם אומר שהם יקבלו יותר כסף מהמרכז, ולכן ישקיעו שם. BEATTY בנאוודה הצליחו להביא סיבים אופטיים על גבי חברת החשמל ליישוב.

פתרון:

להעדיף את חובת האוניברסליות של פריסת תשתיות על הוט ובזק, אבל לתת הקלות: הגעה דחויה ליישוב מסוים אם יש מניעה טכנולוגית מסוימת/סיבה ביטחונית, שיקולי עלות ותועלת, חלופה זמינה יותר (לוויינים). זה פתרון שמתכנסת ועדה ציבורית שדנה בכל בקשה של יישוב. על כל הקלה (מוצדקת) ה100 אלף ש"ח יכולים ללכת לסיבים אופטיים.

שוק התקשורת מופרט ועצמאי וכל מה שהושג – הושג באמצעות תחרות. בארה"ב אין חובת אוניברסליות, אבל יש קרן אם משלמים לחברת האינטרנט/סלולר יש חובה לשלם סכום סמלי לצורך השקעה בתשתיות.

3. IOT – "אינטרנט של הדברים": המהפכה הטכנולוגית הראשונה הייתה במאה ה-18 מפעולות של בני אדם לפעולות ממוכנות, שימוש טכנולוגי על בסיס מים וקיטור וההמצאה הייתה הרכבת. המהפכה הטכנולוגית השנייה הייתה המצאת החשמל, נורה, טלגרף. המהפכה הטכנולוגית השלישית טכנולוגיית מידע באמצעות אמצעים ממוחשבים. עד כה זו טכנולוגיית PTP – אדם לאדם. שליחת דברים באינטרנט של הדברים MTM. טשטוש בין הפיזי לבין הדיגיטלי הטכנולוגי – מדובר על 8 מיליארד מכשירי IOT בעולם, התחזיות שזה יעלה לעשרות מיליארדים. באנגליה יש תשתיות חכמות – מד אנרגיה של גז וחשמל שמשדר לחברות חזרה את הצריכה. מכוניות אוטונומיות ומשאיות אוטונומיות, רמזורים (VTV), בתים חכמים, תעשייה חכמה (BTB) מפעל חכם למכוניות - המכונית משדרת שיש לה פגם והמפעל יודע לתקן את הפגם בפס הייצור. טכנולוגיה לבישה – נעליים.

בעיות:

- פריצות

- פרטיות

- אחריות משפטית

- מיסוי

- עומס על תשתיות

- ספקטרום – תדרי הרדיו – המשרד התחיל לבצע ניסויים בטכנולוגיית IOT ובנוסף יותר קל לייבא ציוד אלחוטי.

- תשיתיות

- מספור – SIM להוסיף עוד מספרי טלפון

4. ניטרליות רשת

- חופש הביטוי

- עלויות נמוכות

- חדשנות יזומות

בישראל יש ניטרליות רשת - איסור להגביל תכנים, חברות התקשורת לא יכולות להגביל תכנים. בארה"ב נכנסה החלטה חדשה שהרשות עצמה ביטלה את ניטרליות הרשת.

**סיכום:**

יש אתגרים וסוגיות משפטיות, שיקולים רבים שיש לשקול כדי להגיע לפתרון מאוזן יותר.

**11/6/18**

דיברנו על הפרטיות במשפט הישראלי ועל הזכות הכללית לפרטיות שבחוק היסוד ובחוק הגנת הפרטיות. דיברנו על השאלה האם קיימת זכות יסוד להגנת מידע דיגיטלי ועל האפשרויות לכך וההבחנה של חוק הגנת הפרטיות בין הגנה על פרטיות פיזית לבין הגנה על פרטיות מידע. על דרך ההשוואה בין מידע ככלל לבין מידע רגיש. דיברנו על מה זה מאגר מידע והחריגים לו – מאגר מידע לא לשימוש עסקי לא נחשב כמאגר מידע לצרכי החוק. החוק הישראלי מתייחס רק למאגרי מידע שנמצאים בשליטתו של אותו עסק, לא מתייחסים ליכולת להצליב מידע – ההתייחסות בGDPR רחבה יותר. רישום של המאגר, הקושי שקיים בפועל ביישום של החובה של רישום מאגר. מנהל המאגר צריך להודיע למי שנכלל במאגר על כך – הבסיס של היכולת לקבל הסכמה מדעת, היכולת להשתמש במידע פרטי היא רק לשם המטרה שלשמה הוקם המאגר. עד כמה זה ישים לאכוף דרישות הסכמה מחמירות כמו של הGDPR – יומיים לאחר כניסתה של הGDPR הונחו תביעות כנגד חברות. מתח בין התפיסה הטהרנית של הזכות לפרטיות ועיקרון ההסכמה לבין הדינמיות של עולם המידע הדיגיטלי. חובת סודיות של מי שנחשף למידע בקרב העובדים של החברות וגם חובות אבטחת מידע כלפי העולם החיצון מפני צדדים שלישיים שעלולים לפרוץ למאגר - ההגדרה בחוק היא הגנה על שלמות המידה או הגנה על המידע מפני חשיפה, שימוש או העתקה. החוק לא מפרט כיצד זה ייעשה כיוון ש:

1. זה לא פרקטי – קצב ההשתנות של הטכנולוגיה הוא מהיר ודינמי, לכן הנטייה בדרך כלל לקבוע עקרון ולהותיר את אופני ההגשמה הטכנולוגיים שלו לשוק שמתחרה. הבחינה האם האמצעים שננקטו הם אמצעים סבירים ביחד למידע הספציפי נעשית בדיעבד ולא מראש.

2. נייטרליות טכנולוגית – עמדה נפוצה בנוגע לאסדרת טכנולוגיה. נייטרליות של ספקיות האינטרנט – האינטרנט פועל באופן שספקיות השירות לא יכולות להעדיף תעבורה לאתרים מסוימים או של משתמשים מסוימים, כלומר כולם שווים בפני החוק. לספקיות השונות יש אינטרס שלא לשמר את עיקרון הנייטרליות כי הם יכולות למכור בכסף העדפה של תעבורה מסוימת, למשל: אם לאתר מאקו היה הסדר מסוים עם ספקיות האינטרנט. אם פוגעים בנייטרליות אנחנו מתערבים באיזשהו אופן בשוק – אם המחוקק היה קובע טכנולוגיה ספציפית היו נותנים העדפה לטכנולוגיה מסוימת.

לקרוא: נייטרליות טכנולוגית בשוק הסלולרי

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 שכבו כאבן שאין לה הופכין במשך שנים רבות עד חודש מאי האחרון. מחליפות את תקנות הגנת הפרטיות משנת 1986. חוק הגנת הפרטיות מטיל בס' 17 חובת אבטחת מידע על כל גורם המנהל או מעבד מאגר של מידע אישי. התקנות מפרטות את אופן יישומה של החובה.

אנחנו לא יודעים הרבה על מאגרי מידע בעולם משום שיש הרבה גופים שמנהלים אותם עבור משתמשים שונים, למטרות שונות. נותר צורך להגדיר איזשהו רף מינימום או שיטת פעולה כדי שמנהלי מאגרי המידע יצטרכו לעמוד בה כדי להגן על הפרטיות של מידע המשתמשים. התקנות נכתבו בעולם שהשתנה ויוצרות חובות שלא היה ברור שהיו קיימות בחוק.

**\*למבחן:** לדעת מה ההבחנה בין קטגוריות שונות של מאגרים ולמה זה נעשה – המתודולוגיה.

**3 רבדים להסדרים בתקנות:**

- בעל המאגר נדרש לקבוע מהו המידע המוגן במאגר ומה הסיכונים הקשורים אליו

- הארגון נדרש לקבוע נהלים מפורטים וברורים לאבטחת המידע

- הוראות מהותיות בניהול אבטחת מידע

התפיסה שמשתקפת בתקנות היא תפיסה מודולורית – לא כל מאגרי המידע הם זהים, ולכן נחיל חובות ברמה הולכת וגוברת ככל שהפעילות של עיבוד המידע במאגר (כמות האנשים שנכללים במאגר) היא משמעותית יותר, ככל שמדובר במידע רגיש יותר וככל שיש יותר אנשים בארגון שחשופים למידע.

הרעיון הוא שייפחת הסיכון לפגיעה בפרטיות ואם תהיה אכן פגיעה בפרטיות יידעו כיצד לטפל בסוגיה.

הרשות להגנת הפרטיות במשרד המשפטים אמונה על הנושא.

**התקנות קובעות הסדרים ביחס ל4 סוגי מאגרי מידע:**

- מרבית החובות החלות לפי התקנות על בעל המאגר, יחולו גם על מנהל המאגר ועל המחזיק במאגר, למשל: בעל עסק שמשתמש בשירותי "ענן" לצורך שימור מידע.

- ס' 21 קובע אילו חובות יחולו על כל סוג מאגר.

- ס' 21: מעניק לרשם מאגרי המידע סמכויות המאפשרות גמישות בהחלת החובות:

(1) להחריג מתחולת התקנות (או לחייב בתחולת התקנות), באופן מלא או חלקי, מאגרים מסויימים "בהתחשב בגדל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר או מספר בעלי ההרשאות בו".

(2) לקבוע שמי שעומד בהוראות רגולציה אחרת יראו אותו כעמוד בתקנות כולן או חלקן.

התקנות משקפות עיקרון של ניטרליות טכנולוגית: דינמיות ומניעת פגיעה בתחרות.

**1. מאגר מידע המנוהל ע"י יחיד:**

מאגרים המנוהלים בידי יחיד לרבות תאגיד בבעלות יחיד כאשר הגישה למידע שבמאגר הינה לבעלים ולכל היותר שני מורשי גישה נוספים. לרוב מדובר בעסקים קטנים, כמו קוסמטיקאית או חנות שכונתית. החובות בהקשר הזה הינן המצומצמות ביותר.

א. הכנת מסמך הגדרות המאגר – חיוב שחל על כל בעלי המאגרים, לחשוב על מה שיש לו במאגר, ובהתאם לכך להיערך מראש לסיכונים של פגיעה בפרטיות. מטרות ואופן האיסוף, השימוש והעיבוד המידע, סוגי המידע, סיכוני אבטחת מידע ואופן התמודדות, פרטי מנהל המאגר, מחזיק המאגר וממונה אבטחת המידע.

ב. אבטחה פיזית

ג. ניהול הרשאות הגישה והיקפן

ד. תיעוד אירועי אבטחה

ה. הגבלת שימוש בהתקנים ניידים

ו. הפרדת מערכות ושימוש בתקשורת מאובטחת

\*מאגרים שבהם יש מידע על יותר מ10 אלף איש הוא לא יוגדר כמאגר המנוהל ע"י יחיד.

**2. מאגרים שחלה עליהם רמת האבטחה הבסיסית:**

מוגדרים על דרך השלילה - מאגרים שאינם מנוהלים בידי יחיד ואשר אינם מאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה.

**3. מאגרים שחלה עליהם רמת האבטחה הבינונית:**

- מפורטים בתוספת הראשונה לתקנות

- כל אחד מהמאגרים הבאים, ככל שיש להם לפחות 10 מורשי גישה:

א. מטרתם היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק – עסק ממש

ב. הם בבעלות גוף ציבורי

ג. הם מכילים מידע כגון: מצב רפואי/נפשי של אדם, מידע גנטי/ביומטרי של אדם, דעותיו הפוליטיות ואמונויות ודתו של אדם, הרשעות בפלילים, נתוני תקשורת לפי חוק סדר הדין הפלילי, מצבו הכלכלי של אדם, הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע כנ"ל או על אישיותו, אמונתו או דעותיו.

4. מאגרים שחלה עליהם רמת האבטחה הגבוהה:

- מפורטים בתוספת השניה לתקנות

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

א. מטרתם איסוף מידע לצורך מסירתו לאחר

ב. יש בהם מידע רגיש כמתואר לעיל

\*מה שמבחין בין הרמה הבינונית לגבוהה הוא מספר האנשים במאגר/מספר האנשים שחשופים לו.

\*ככל שרמת הסיכון שהמאגר מציב היא גבוהה יותר יש דרישות גבוהות יותר ממנהל המאגר, ניתן לראות שמחייבים דרישות שהעלות שלהן ומורכבותן גדולות יותר. יש הנחה שמי שמנהל מאגרים ברמת סיכון גבוהה יותר ייצטרך להשקיע יותר באבטחת המידע.

**החובות על שלושת סוגי המאגרים האחרונים:**

- הכנת מסמך הגדרות מאגר

- עריכת נוהל אבטחת מידע

- מיפוי המערכות (ולרמת האבטחה הגבוהה גם ביצוע סקר סיכונים)

- אבטחה פיזית

- ניהול הרשאות גישה, זיהוי ואימות ובקרה

- תיעוד אירועי אבטחה

- הגבלת שימוש בהתקנים ניידים

- הפרדת מערכות (ככל הניתן, בין המאגר למערכות מחשוב אחרות של בעל המאגר)

- אבטחת תקשורת

- חובות נוספות כמפורט בתקנות

אם מפרים את מדיניות הגנת הפרטיות בהסכם השימוש ניתן לפנות בכלים חוזיים, לרוב תובענות ייצוגיות.

ס' 13 זכות עיון במידע – עיקרון השליטה במידע - למושא המידע יש זכות פרטיות למידע עליו.

(א) כל אדם זכאי לעיין בעצמו, או ע"י בא כוחו שהרשהו בכתב או ע"י אפוטרופסו, במידע שעליו המוחזק במאגר מידע.

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

+(ה) החרגת תחולת ס' 13(א) על מאגרים שונים

כשבעל מאגר מידע מחזיק אותו אצל אחר עליו להורות למחזיק לאפשר למבקש את העיון (ס' 13א(1))

הבעייתיות היא:

מחייב את בעל מאגר המידע בס' 13 א(1) להפנות את מושא המידע - יש קשיים במימוש הזכות: לא הרבה אנשים יודעים שהזכות הזו קיימת. החובה של בעל מאגר המידע להודיע למושא המידע על המידע לא כוללת הודאה על הזכויות שיש לו.

אפשר לחשוב על המעבדה שבה בוצעה בדיקת דם ונמצא שאדם חולה באיידס ויש חובה להעביר זאת לאדם החולה, אבל יעדיפו שהמידע יימסר ע"י הרופא האישי ולא ע"י הטלפנית.

ס' 14 זכות מושא המידע לדרוש תיקון מידע – ניתן לפנות לבעל המאגר ולבקש לתקן את המידע או למחוק אותו. נדרשת הסכמה של בעל המאגר לבקשה.

ס' 15 במקרה של סירוב לבקשת מושא המידע - אם בעל המאגר סירב לכל אחת מהבקשות של מושא המידע, קמה למושא המידע עילה להגיש תובענה לביהמ"ש על הסירוב על מנת שיורה על בעל המאגר לתקן את המידע.

חוץ מהעניינים הקשורים במאגר המידע, חשוב לציין שפגיעה בפרטיות יכולה להקים עוולה אזרחית (ס' 4), להקים יסוד לעבירה פלילית אם נעשתה במזיד (ס' 5 פגיעה בפרטיות - עבירה) או עוולה בניזיקין (ס' 31ב), למשל: אם מנהל המאגר התרשל בחובה שלו להבטיח את המידע/סודיות כלפי פנים. הקושי של ס' 31ב הוא הוכחת הנזק כדי לקבל פיצוי נזיקי. לפחות בנוגע לפגיעות הנזיקיות לפי פרק א' לחוק, ס' 1-11, יש אפשרות לתבוע פיצוי ללא הוכחת נזק (ס' 29א).

**הזכות להישכח – מידע אישי דיגיטלי לאחר המוות:**

מה גורל השיירים של המידע האישי שאנו מותירים לאחר מותנו?

האם יש זכות חוזית ואפשר להתנות עליה והאם יש קניין במידע זו זכות קניינית שעוברת או האם מדובר בזכות לפרטיות כמו זו שבחיים?

המחוקק הישראלי טרם הכריע איך לסווג את המידע הזה, מה ששולט כיום אלו תנאי השימוש וכלים שונים שהפלטפורמות הטכנולוגיות השונות מציעות למשתמשים שלהם.

- לאחר מותנו, אנו מותירים עקבות דיגיטליים: תכנים שיצרנו ברשת, חשבונות אישיים שנותרים "חיים".

- למי צריכה להיות גישה למידע ושליטה בו?

- מהם הישקולים שראוי לשקול ומה המדיניות המתאימה להסדרת הסוגיה?

- התשובות מורכבות ותלויות הקשר כי יש סוגים שונים של מידע, של פלטפורומות שבהם מאוחסן המידע ומגוון רצונות של משתמשים ביחס לניהול הגישה למידע לאחר המוות.

כמו בנושאים רבים את הפעילות הזו מסדירים המשפט, הנורמות החברתיות, השוק והטכנולוגיה - מקום שיש חלל משפטי הכוחות האחרים תופסים נתח גדול יותר.

**התנגשות בין זכויות ואינטרסים במידע לאחר המוות:**

- זכויות קניין במידע: זכויות יוצרים, מידע כקניין בר הורשה

- זכות לפרטיות של המשתמשים החיים בקשר לגורל המידע שלהם (אם זכות זו שורדת את המוות)

- אינטרסים של בני משפחה וחברים אבלים – גישה או שליטה במידע של המנוח לצורכי זיכרון, אבל והנצחה

- זכות לפריות של משתמשים חיים שהיו בקשר דיגיטלי עם המנוח

- חובת סודיות של מי שהעניקו למנוח שירותים רפואיים, פסיכולוגיים או משפטיים

- אינטרסים עסקיים של ספקי השירות, בפועל כיום הם אלו שמכתיבים את גורל המידע והתכנים של משתמשים שמתו.

**שיקולים ביחס לגישה למידע דיגיטלי אישי לאחר המוות:**

הטכנולוגיה מאפשרת דרכים חדשות להתמודדות עם האובדן:

• מרחבי התאבלות וירטואליים, הנצחה ותיעוד (פרופילים וקבוצות רשת קיימים/פורומים שנפתחו לאחר המוות).

• יחסי הכוח בשליטה במידע ובעיצוב הזיכרון - בשליטת המנוח? בשליטת מעגלים שסובבים אותו (משפחתי, מקצועי, חברתי – מי ספציפית?)

• מאפייניו הייחודיים של המידע הדיגיטלי => מעוררים שאלות לגבי היכולת להחיל ישירות את המסגרת המשפטית הקיימת, אשר עוצבה עבור סביבה לא דיגיטלית

**מאפייניהם הייחודיים של זיכרונות דיגיטליים:**

- המידע אינו מתכלה

- המידע ניתן לעיבוד בקלות

- המידע כולל תוכן + נתונים על תוכן META DATA

- השליטה האפקטיבית במידע, בעולם הפיזי: מי שיש להם גישה לניירת ושאר חפצים שהותיר אחריו המנוח. זירה הדיגיטלית, גורמי הביניים (ספקי שירות כמו דוא"ל ואחסון בענן או פלטפורמות תוכן כמו רשתות חברתיות או אתרי היכרויות) מכילים את המידע ושולטים בו פיזית. מי שמותיר אחריו את הגישה לאתרים/רשתות מאפשר גישה במחדל.

פתרונות טכנולוגיים לניהול מידע אישי לאחר המוות:

1. פייסבוק מאפשרת למשתמשים לקבוע אם לאחר מותם חשבונם ייסגר או יהפוך לחשבון מונצח שבו תינתן גישה למידע ולביצוע פעולות לגורם מסוים. חשבון מונח דורש מינוי של LEGACY CONTACT, אדם שיוכל לבצע פעולות מסוימות בחשבון, אך לא לגשת לשיחות אישיות.

2. גוגל מציעה כלי בשם GOOGLE INACTIVE ACCOUNT MANAGER – משתמש יכול לקבוע מה יקרה לחשבונותיו לאחר תקופת אי פעילות שהגדיר מראש (מוות) – האם ייסגרו או שתינתן גישה לגורמים ספציפיים שהוא קבע. יש היבטים פיננסיים: בני משפחה של משתמש מנוח יכולים לבקש לסגור את החשבון, לקבל כספים שיש בחשבונות, ולקבל נתונים מהחשבונות.

3. חברות רבות אינן מציעות פתרון מובנה לטיפול במידע דיגיטלי לאחר המוות.

**18/6/18**

**שירותים משפטיים מקוונים:**

האפשרות לספק חלק משירותים המשפטיים מעוררת שאלות שונות לגבי השוק המשפטי ככלל ומקצוע עריכת הדין וייחודיותו בפרט.

המודל של לסיג – איך השוק, הטכנולוגיה, הערכים וההסדרה שמפטית משפיעות על כל ההתנהגות וברמחב המקוון בעיקרו, זו התפתחת מעניינת.

**מתן שירות משפטי באופן מקוון:**

שירות מקוון חלקי/היברידי – ממשק מקוון שמקשר לשירותים אנושיים

שירות מקוון מלא – השירות ניתן באמצעים טכנולוגיים בלבד.

חידוש – AL+NLP עיבוד שפה טבעית, עיבוד טקסט וטכנולוגיה של בינה מלאכותית – ניתוח טקסטים רגילים.

הבנייה מחדש/עיצוב – פישוט פרוצדורלי, שפה; אבחון אוטומטי, אימות מידע; הדרכה משפטית צמודה. באמצעות עיצוב טפסים בעלות נמוכה אפשר לספק שירותים לקהל רחב של משתמשים.

העברה לסביבה מקוונת – הרחבת נגישות: מקום, זמן; רגשות

הרכיב הטכנולוגי בתוך התהליך מחליף היבט של פעולות שעורכי דין, עוזרים משפטיים ביצעו בעבר. גם דברים שעורכי דין מנוסים וותיקים עושים יש תוכנות שעושות זאת אף בצורה טובה יותר מהם.

**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, AL, למידת מכונה.

4. אופני תקשורת שונים – טופס-טקסט סטטי, ממשק צ'ט בוט, הנחיות קוליות.

מגוון הפעולות המשפטיות שניתן לבצע באמצעות היישומים האלה הוא רחב: הסכמי שכירות, מכר, הסכמי שימוש בנכס, ייפוי כוח, צוואות, הסכמי עבודה, הסכמי גירושין, מסמכי התאגדות חברה, שותפות ועמותה, רישום פטנטים, סימן מסחר וזכויות יוצרים, הסכמי סודיות, אי תחרות ושירותים, הגשת מסמכים לבתי משפט ולרשויות.

דוגמה: רישום חברה באמצעות חברת "LegalZoom" – החברה התאגדה ב1999 והתחילה להציעה את השירותים שלה ב2001, יש לה 1000 עובדים והכנסות של מיליוני דולרים. העלות של ביצוע שירותים משפטיים דרך האתר של החברה נעה בין 15$ לכמה מאות דולרים לעריכת מסמכים משפטיים כאלה. יש רמות שונות של המסמכים – חבילה בסיסית או חבילה מורחבת.

דוגמה: עריכת הסכם גירושין באמצעות WEVORCE -

- שילוב של טכנולוגיה ותפישה תהליכית של גירושין בשיתוף פעולה.

- הדגמת שימוש מצד הלקוח

- הדגמת שימוש ע"י עו"ד ככלי גישורי/ניהולי

החברה מציעה לזוגות המתגרשים מודל של גירושין בהסכמה, גם להם יש מודלים ממילוי הטפסים לבד, שימוש בעורך דין מטעמם שינהל את תהליך הגישור. הם מציעים חבילות שונות בין 300-900 דולר. חינוך משפטי ומתן המידע הכללי, טפסים משפטיים שבצידם יש דברי הסבר.

כמה אינטואיטיבי קל להשלים הליך גירושין בצורה מקוונת, מעבר לממשק המשתמש כל אחת מהחברות האלה מציעות חוברות הדרכה עם הסבר – מקום שבו הדבר מתאפשר ע"י המשטר המשפטי יש נתח שוק רחב ומשמעותי שיוצא מחזקתם של עורכי הדין ועובר לתוכנות האלה.

**סטודנטים למשפטים בחזית:**

- תוכנה שפותחה בבוסטון AUTHOR – לאנשים בעלי ידע משפטי, לרוב בבתי ספר למשפטים שחוברים לעמותות, בתי משפט ומשרדים ממשלתיים, עובדים יחד איתם כדי לייצר שאלונים אינטראקטיביים לאנשים מעוטי יכולת.

- תוכנה המשמשת גורמים בעלי ידע משפטי לצורך עיצוב שאלון/ראיון משפטי מקוון לאבחון ואיסוף מידע + הפקת מסמך משפטי רשמי.

- השירות עצמו ניתן ללקוחות כשירות ענן SaaS

מערכת דומה במחוז אורנג' בקליפורניה שיפרה פלאים את מצבם של המיוצגים העצמאיים וגם השופטים העידו שזמן הקריאה של הבקשות התקצר.

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

- הינד דיגיטלי

- הינד: קבלת ההחלטות של משתמשים מושפעת מהאופן שבו בחירות מוצגות: התוכן וההצגה החזותית מפעילים הטיות קוגנטיביות, רציונליות מוגבלת.

דוגמאות: עוגן, ברירת מחדל, סדר הצגה, אפקט מחסור, אפקט הסחה.

\*הספר של ריצ'רד טלר וקאס סאנסטיין NUDGE

\*הספר של שלמה בן ארצי THE SMARTER SCREEN – הממשק המקוון משפיע על אופן קבלת החלטות של אנשים.

אלו ספרים שמתייחסים לשאלות הללו ואיך חוויתה משתמש והאופן בו הממשק המקוון מעוצב משפיע על קבלת ההחלטות. הרעיון הוא שבסביבה הדיגיטלית – החזות מטה קוגניטיבית וגורמת לאנשים לקבל החלטות מסוימות. יש חשיבות לבחירה של עיצוב ממשק המשתמש.

אתר שמאפשר ליצור כתב תביעה – יודעים מהמחקר שכאשר יש ברירת מחדל שנבחרה, קשה לאנשים להחליפה. אנחנו מדברים על השאלה איך אדם הטווה את הזכות המשפטית שלו - מחקרים מראים שקיימת הטייה לאפשרות הראשונה והאחרונה.

**עו"ד צ'ט בוט – ROBOLAWYER:**

- חוויית משתמש של שיחה אינטראקטיבית

- עיבוד שפה טבעית

- התאמה של מסמכים

- הגשה מקוונת לרשות

<https://www.youtube.com/watch?v=PHZobnM2wlw>

אחד התחומים שהתפתחו הוא **שימוש בטכנולוגיה לצורך גילוי מסמכים מוקדם:**

- בעידן הדיגיטלי – כמות המסמכים גדלה ואיתה שעות האדם הדרושות כדי להעריך את הרלוונטיות של כל מסמך להתדיינות המשפטית.

- אלגוריתמים ייעודיים שתוכנתו לכך עורכים חיפוש בכמויות גדולות של מסמכים באופן שמחקה את תהליך האיתור והמיון שמבצע אדם בעל הכשרה בתחום.

- התוצר: ניבוי בדרגת ודאות גבוהה יחסית אם מסמך כלשהו רלוונטי להליך ספציפי.

תעשיית הליגל טק בישראל פורחת בשנים האחרונות, למשל: חברתLawGeex עובדת עם יועצים משפטיים, המייסדים הם עורכי דין. להעריך באיזו מידה הסכמים/חוזים שהחברה חותמת עליהם תואמים את עקרונות המדיניות של החברה, ועל סמך קריטריונים שכל חברה מגדירה מראש המערכת הזאת עושה עבור המחלקה המשפטית את ההערכה של הסיכונים המשפטיים של כל חוזה/הסכם. סיכון זו פסקה בחוזה/הסכם שלא תואמת את הקריטריונים שהוגדרו מראש. אם מזהים סיכון כזה מעבירים לעורך דין במחלקה לצורך בחינת העניין. החברה הזו עשתה ניסיון לפני מספר חודשים – לקחה 20 עורכי דין בעלי ניסיון בבחינת חוזים אשר התבקשו לבחון 5 הסכמי סודיות והוקצבו להם 4 שעות למשימה. במקביל, החברה ביקשה מהתוכנה לאתר את הסיכונים המשפטיים בהסכמי הסודיות הללו. התוצאות היו עוה"ד (ממוצע + טווח) לעומת התוכנה:

משך זמן להשלמת המשימה – 92 דקות לעומת 26 שניות

אחוז הדיוק: 85% בקרב עורכי הדין לעומת 94% בקרב התוכנה

ההשלכות על עבודת עו"ד:

- טפסים משפטיים: שימוש נפוץ, חתך נתח מסוים מעבודת עוה"ד; מודלים משולבים – קיטוע/תיחום של עבודה עוה"ד באופן משלים

- תוכנות ה”E-DISCOVERY” הן אמצעי מקובל ונפוץ שהתקבל כלגיטימי בבתי המשפט. תחילה: שימוש בתוך משרד עו"ד = החלפת עובדתם של מזכירות משפטיות, מתמחים ועו"ד צעירים. בהמשך: קמו חברות שהתמקצעו בתחום, שיכללו את המודלים והן מציעות שירותים למשרדי עו"ד במודל של מיקור חוץ.

- תוכנות הערכת מסמכים: קפיצת מדרגה טכנולוגית בשנה האחרונה.

כרגע יותר מדובר על תוכנות שמשמשות כלי עזר לעורכי דין, לאו דווקא מחליפות אותם עדיין.

**דוגמאות למערכות תומכות החלטה:**

- חישוב פיצויים

- חישוב גזרי דין

- חישוב סיכויי תביעה

- חישוב סכום לפשרה

- סטטיסטיקה תיאורית של הליכים, שופטים ועורכי דין. ניתן להכניס את שם השופט ולקבל תובנות על סמך המערכת ותיקים שהתקיימו בעבר. בעצם כלים שנועדו לתמוך בהחלטת עורך הדין תוך שהוא מייצג את הלקוח שלו.

- נזיקליק – באתר תקדין. לפי פרטים מסויימים ניתן לקבל הערכה לאן עורך הדין צריך לכוון את התביעה שלו.

- דיספוטק – ביה"ד לענייני עבודה.

התמריצים שהביאו להתפתחות של התחום:

הנגישות משחקת תפקיד משמעותי – השירותים נגישים בכל מקום בו יש גישה לאינטרנט, בעלות נמוכה משמעותית, בקצב מהיר יותר. הפירוק של סוגיות משפטיות לשלבים שונים שניתן לעשות בנפרד פותח את הפתח גם לשינוי תפיסתי על המקצוע של עורכי הדין, כל פעולה משפטית מסוימת ניתנת לפירוק לרכיביה השונים.

**קשיים בפיתוח מיזמים משפטיים טכנולוגיים:**

- 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.

- ייחוד פעולות המקצוע.

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

עורכי הדין קיבלו אוטונומיה מהמחוקק, זו גילדה סגורה, נזקק רישיון מקצועי, יש בחינות של לשכת עורכי הדין. תמורת ההכפפה של עורכי הדין להסדרה ולמחויבויות אתיות, מקצועיות משמעותיות – עורכי דין קיבלו הגנה בדמות ייחוד המקצוע, פעולות שמותרות רק לעורכי דין ואנשים אחרים לא יכולים לבצע.

הנורמות הללו והכללים לגבי השאלה מהי פעולה משפטית שנמצאת תחת ייחוד המקצוע נקבעו הרבה לפני עידן הטכנולוגיות המשפטיות שדנו בהן היום. למשל: ייצוג בהליכים, איסור שיתוף בהכנסות או קבלת הפנייה של לקוח שנעשתה למטרות רווח (כדי להבטיח שירות של ייצוג משפטי ללא ניגוד עניינים).

**ס' 20 לחוק לשכת עורכי הדין: ייחוד פעולות המקצוע:**

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

 (2)  ייצוג אדם אחר וכל פעולה אחרת בשמו לפני גופים שונים בהם:

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

(4)  ייעוץ וחיווי דעת משפטיים.

שירותים משפטיים מקוונין: הסגת גבול המקצוע?

- מתן מידע משפטי באמצעות אתר מקוון אינו אסור כשלעצמו.

- לעומת זאת, ייעוץ משפטי או מתן חוות דעת משפטית ע"י מיש אינו עורך דין אסורים. ככל שהמידע כללי יותר ואינו מתייחס למקרה העובדתי הקונקרטי = מידע. ככל שהמידע נשען על נסיבותיו הפרטניות של הפונה = ייעוץ.

- בנוסף, יש לבחון אם המידע/השירות/הייצוג בנסיבות המקרה הם משפטיים > אמות המידעה נקבעו בהלכת "המרכז למימוש זכויות רפואיות" - "מידע" ו"ייעוץ" אלו מונחים שלא הוגדרו באופן ברור בחוק. ופסק הדין הזה מנחה כיצד להכריע בקו הגבול בשאלה האם שאלה היא כללית או פרטנית - התשובה לא תמיד ברורה. למשל: אישה עובדת שיוצאת לחופשת לידה לפני שסיימה שנת עבודה מלאה, האם מחויב לשמור לה את מקום עבודתה?

**הלכת המרכז למימוש זכויות רפואיות – ייעוץ וחיווי דעת משפטיים:**

לבנת פורן ערערה על קביעת המחוזי שהשירותים שהיא מציעה מסיגים את גבול המקצוע.

נקודות המוצא:

- הגדרה טעונה פרשנות: לא נית להגדיר מראש באופן ממצה את המונחים הכלולים בסעיף 20, כגון: ייצוג, אופי משפטי וכו'.

- תכלית ס' 20: להבטיח שלא ייגרם לציבור נזק כתוצאה משירות משפטי לקוי (רק בעלי הידע וההכשרה המתאימים יעניקו שירותי משפט).

**אמות המידה שיש לשקול בהכרעה אם פעולה/שירות הם ייחודיים למקצוע עורך הדין:**

היקף שיקול הדעת הכרוך בביצוע השירו או הפעולה הניתנים לציבור. האם השירות או הפעולה "כרוכים בהפעלת שיקול דעת רחב תוך שקלול של משתנים רבים או שמא מדובר בפעולה טכנית בעיקרה שאינה מצריכה בחירה בין דרכי פעולה רבות.

פוטנציאל הנזק לציבור עקב שירות לקוי: ככל שמדובר בפוטנציאל משמעותי יותר ובנזק בלתי הפיך השירות יוקצה לעורכי דין בלבד.

החלופה העומדת לציבור במימוש זכויותיו, אם ייאסר מתן השירות ע"י מיש אינו עו"ד (בשים לב למחיר).

ככל שזו לא פעולה טכנית וצריך לשקלל יותר משתנים נחשוב על כך שמדובר בפעולה משפטית. בנוסף, נבחן כתנאי שני מה פוטנציאל הנזק שעלול להיגרם לציבור במידה שהוא יקבל שירות משפטי לקוי – ככל שפוטנציאל הנזק יהיה גדול יותר נייחד את השירות הזה לעורכי דין בלבד. בנוסף, נשקול מה החלופה העומדת לציבור במימוש זכויותיו אם ייאסר על מי שאינו עורך דין לספק את השירות הזה.

**יישום אמות המידה בהקשר של שירותים משפטיים מקוונים:**

- בשולי פסק הדין מציינת השופטת ארבל כי במבט צופה פני עתיד, ייתכן ששירותים משפטיים מסוימים ונקודתיים יסופקו לציבור הרחב אף עח ידי מי שאינם עורכי דין.

- לצורך כך נדרשת הסדרה של גופים אלה – יצירת מנגנוני פיקוח ובקרה אשר יבטיחו כי השירות ניתן לאחר הגשרה מתאימה, בוכפוף לכללי התנהגות מחייבים.

- מלאכת יצירת ההסדרים נתונה למחוקק

בהליך נגד חברה שמספקת שירותים שונים בתחום השכר והפנסיה ובין היתר, מציעה מרכז מומחים ולשאול שאלות שונות גם שאלות משפטיות ולקבל מענה והפנייה לחומרי עזר ומאמרים שעוסקים בשאלות האמורות. ביהמ"ש בהחילו את אמות המידה שקבעה השופטת ארבל, נעתר לבקשת עורכי הדין ונתן צו מניעה שהפסיק את פעולת מרכז המומחים, אך אפשר לחברה ששמה דטה פקס להמשיך ולהפנות משתמשים למאמרים בנושאים רלוונטיים לשאלות שלהם. כך המשיך האתר לפעול במהלך ההתדיינות המשפטית ולשכת עורכי הדין המשיכה להתנגד. הקו הדק בין מידע לייעוץ – כאן עושה ביהמ"ש שימוש בפסק דינה של ארבל בפרשת המרכז לזכויות רפואיות וקיבל את תביעת הלשגה, בקובעו כי הייעוץ היה סביב מסכת עובדתית קונקרטית ודרש הפעלת שיקול דעת רחב. נקבע שההפניה למאמרים ספציפיים עולה כדי ייעוץ משפטי.

על סמך החלת אמות המידה שבפסק הדין, ביהמ"ש קבע שלמרות שלא מכנים זאת באתר כייעוץ משפטי – בפועל זה כן ייעוץ משפטי. אותם עובדים עלומים של החברה צריכים להתאים את המאמר לשאלה הקונקרטית של הלקוח, עבודה זו מצריכה הבנה משפטית רחבה בבחירה ובהצגה של הסוגיה המשפטית שמתעוררת במקרה הספציפי, ועל כן חברת דטה פקס כבר לא מספקת את השירות הזה ללקוחותיה.

מה היה קורה לו אלגוריתם ואל עובד עלום היה מבצע את ההפניה?

האם במקרה שבו עורך דין מיפה מראש את כל הסוגיות המשפטיות האפשריות בנושא מסוים (וכל ההסתעפויות לשאלות ההמשך הנגזרות מהתשובות המתקבלות) וחבר למתכנת שיצר תוכנה המעניקה את השירות, מדובר בהפרה של ס' 20?

האם זה ייעוץ? (לא מופעל שיקול דעת במקרה הספציפי)

אם זה ייעוץ – עו"ד נתן אותו לכתחילה > נראה שלא ידובר בהפרה.

המרצה לא מכירה מקרה שהגיע לפתחו של ביהמ"ש בארץ ובחו"ל.

**הבחינה:**

- הנושאים שנלמדו מראייה רוחבית: איך מסתכלים על סוגיה בראי המודל של לסיג, העיצוב המשפטי השפיע, מה ההיבט הטכנולוגי עשה, שיקולים של נורמות חברתיות שהשפיעו. למשל: הגנת הפרטיות או אכיפת זכויות יוצרים ע"י גורמי ביניים ברשת ולנתח את הסוגיה לאור זה.

- 5 שאלות אינפורמטיביות ממוקדות + קייס קצר שהוא יישום של נושא משפטי

- תהיה דוגמה עם פתרון

- חומרי הקריאה הם רלוונטיים בשיעורים של מרצים אורחים: הגנת סייבר (מסמכי עקרונות הממשלה והסרט), אורנן שטיינברג (נטיירליות רשת). חומרים לשיעורים שלנו לא מחייבים – מה שדיברנו בכיתה מחייב.