מחברת בחינה

״דיני מחשבים״

מרצה: ד״ר שרונה אהרוני גולדברג

כתיבת המחברת: שלי משה

פקולטה למשפטים

האקדמית נתניה

דיני מחשבים

הבחינה מורכבת משני חלקים(חומר סגור).
א. אמריקאי
ב. שאלה פתוחה

פרשה 1 – **פרשת קליסקוב(?):**

גב' עובדת במשרד ושמה טלי איסקוב. היא מקבלת מהמעסיק שלה מחשב ששייך למעסיק. היא כתבה במחשב מייל לחברת כוח אדם דרך הכתובת שלה. יש כאן הבדל בין קניין מוחשי(Tangiable) במחשב לבין קניין ערטילאי(Intagable - שלא ניתן לנגוע בו).
המעסיק נכנס למייל של העובדת ורצה להגיש את המייל כראיה בבית המשפט. השאלה היא האם ניתן להגיש את זה כראיה או לא?

פרשה 2 – בארה"ב: עובד במשרד רוצה להיות שותף במשרד. מתנהל מו"מ שבמהלכו הוא לוקח חומרים של המעסיק(כל מיני נתונים, מאגרי מידע של המעסיק וכו'...) ושולח אותם אל המחשב הפרטי שלו בבית. השאלה: האם הוא עובר עוולה של חדירה למחשב?
ההבדל בין עבירה לעוולה -
עבירה: מתחום המשפט הפלילי, לעומת עוולה – מהתחום הנזיקי.

שאלה נוספת שמתעוררת נוגעת להעברת סיסמאות.
דוג' 1 – מזכירה שיש לה גישה למאגר המידע של מחשב המעסיק. היא נכנסת אל מאגר המידע של המעסיק ואומרת למישהו שעזב את המשרד את הסיסמא ושיכנס הוא למאגר המידע.
האם מדובר בחדירה למחשב?

דוג' 2 – פייסבוק: אדם ישב בבית שלו, התחבר לפייסבוק, העביר את הסיסמא של הפייסבוק שלו לחברה בשם "דאבל קליק". החברה נכנסת לדף הפייסבוק שלו ושמה בדף פרסומות.
חברת פייסבוק טענה שהיא לא רוצה לתת לדאבל קליק רשות להיכנס לפייסבוק שלו.
האם יש כאן פגיעה בזכויות האדם שלו? חופש הביטוי? פגיעה בזכויות של חברת הפרסום?

<u>מהפכת המחשבים:</u>
החיים בחברה המודרנית הם תלויי מחשב ולצד מהפכת המחשבים יש היבטים שליליים שונים, זוהי "תופעת המחשוב הפולשני"\"סייבר".
תופעת המחשוב הפולשני – אנשים שנכנסים או למחשב המוחשי ששייך למישהו אחר, או למידע הממוחשב ששייך למישהו אחר. תופעה זו נמצאת בעלייה מתמדת.

<u>הגדרה פונקציונאלית של מערכות מחשב(תפקידים):</u>
1. כלי אחסון של מידע – מידע, מצלמות, מאגרי מידע, מידע רפואי, "המשאב" – כסף.
2. כלי למדידות, תכנון וחישוב

3. כלי בקרה ושליטה במערכות ממרחק
4. כלי חברתי ובידורי. לדוגמא: פייסבוק, אינסטגרם
5. כלי לתקשורת פרטית(לדוגמא whatsapp) והמונים(לדוגמא רדיו, טלוויזיה, עיתון).
- לתקשר בין מחשבים
- חיפוש מידע
- במה להבעת דעות (ספקי תוכן – אתרים, צ'אט, קבוצות דיון, טוקבק, פרסומות, בלוגים...)
- ביטוי חופשי.

IOT – "Internet of things"

חלק ניכר מהמחשבים מחוברים לרשת, ומכשיר שהפונקציה שלו היא אחרת(למשל, מקרר או מצלמה) אבל הוא מחובר לרשת, נקרא לו "Internet of thing".

איך מחשב משמש פלטפורמה(במה) לתקשורת פרטית?
דרך אימיילים.
איך מחשב משמש פלטפורמה(במה) לתקשורת המונית?
דרך פייסבוק (פוסטים ציבוריים, רוטרנט, בלוגים).

האינטרנט מאפשר לכולם לפתוח אתר מאוד בקלות, באפס כסף, ולהגיע לכל העולם.
היתרון: חשיפה, במה, נגיש, פתוח לכולם, חינמי כמעט...
מכיוון שהאינטרנט הוא זול, נגיש ומהיר, משמש פלטפורמה לתקשורת המונים מבלי צנזורה בעבר, בכדי לקבל גישה לפלטפורמה המונית היה צריך לעבור את המסננים של הצנזורה המערכתית, התאגידית, לדוג': עורכי העיתונים.
צנזורה תאגידית: עורך העיתון. בעבר, בכדי שאדם יוכל היה להביע את דעתו על נושאים בעלי עניין ציבורי, הוא היה צריך לעבור את "מערכות הסינון" של עורכי העיתונים, עורכי החדשות, הבעלים...

דוגמא של צנזורה תאגידית -

הנשיא עזר ויצמן היה אהוב על רוב חלקי העם. יום אחד עיתונאי בשם יואב יצחק גילה שעזר ויצמן קיבל משכורת חודשית מהמדינה ומחברו. העיתונאי רצה לפרסם את זה בעיתונים בתמורה לכסף. אך אף עורך עיתון לא הסכים לפרסם את הכתבה.

האינטרנט מאפשר פלטפורמה שעוקפת את הצנזורה התאגידית ומאפשרת לכל אחד מאיתנו במה להביע בה את דעתנו. כלי לביטוי חופשי. כלי מן "המעלה הראשונה" (חשוב ביותר).
"hyde park" – באנגליה היה פארק שאנשים פרטיים היו לוקחים כיסא, עומדים עליו, ואומרים את דעתם על כל נושא שבעולם ובאים להקשיב להם.

<u>"מנגנוני סינון של חומר"</u>

גם הכלי הזה כפוף לגורמי סינון. יכולה להיות רגולציה(אסדרה) חקיקתית. כשחוק עושה אסדרה של תחום מסוים, הוא אומר מה צריך לעשות באותו התחום.

למשל יש אסדרה ברשת בנוגע לכך שמחייבים היום ספקי גישה ברשת לעשות איזשהו סינון על תכנים פורנוגראפיים.

"רגולציה שיפוטית" – בית המשפט יפרש בצורה רחבה מידי חוקים מסוימים או ייתן צווים שיורו למחוק משהו מהרשת.
"רגולציה עצמית".

בפרשת RINO – היה ניסיון בארה"ב לאמץ רגולציה שתסדיר את התוכן הפורנוגראפי באינטרנט. הממשל האמריקאי אימץ חוק שאסר על פורנוגרפיה ברשת. בית המשפט האמריקאי לערעורים ביטל את החוק הזה, שכן הוא פוגע ב"חופש הביטוי הפרונו גרפי". כל מה שמאפיין את רשת האינטרנט הוא שהיא במה לחופש הביטוי ולכן לא יתאפשר חוק הפוגע בחופש הביטוי ברשת.

"הזכות להישכח" – בית המשפט באירופה אמר לGOOGLE למחוק את מה שמפורסם באתר שלה על 'פלוני אלמוני' כי עברו הרבה שנים מאז שפורסם שהוא פשט את הרגל, ולכן יש לו "זכות להישכח". בית המשפט נכנס למעשה לתכנים המפורסמים ברשת באמצעות החלטות שיפוטיות.

"שרת" – SERVER מחשב גדול המשרת מחשבים אחרים.

TOR – רשת אנונימית, מה שמאפיין אותה זה שקשה לאתר את מי שמשתמש בה לפי כתובת הI.P שלו.

ברשת ה"DARK NET" אי אפשר לאתר אנשים דרך כתובת הI.P שלו.

סיכום: המחשב הפך לכלי בעל עוצמות אדירות בחברה המודרנית. בית המשפט בפרשת דביר נ' מדינת ישראל מייחס למחשב חשיבות אדירה וקובע שהוא הפך ל"ידידו הטוב שלא האדם", כך אומר בית המשפט על הסמארט פון. בית המשפט מוסיף בפרשה זו שיש היום אפילו תופעה של "נומופוביה", כלומר, למי שאין סמארט פון אז אנשים יהפכו לעצבניים. אנחנו תלויים במחשב, גם כאנשים פרטיים וגם החברה כולה תלויה במערכות ממוחשבות. לכן, המחשב מקדם מאוד את החברה משום שהוא מאפשר לנו מסחר מהיר, חישובים מדויקים, מאפשר להגיע לקצה העולם מבלי לזוז מהכיסא שלנו, מאפשר לנו להביע את דעתנו.
אך "עליה וקוץ בה" – תופעת הסייבר: "תופעת המחשוב הפולשני".

<u>ארבעה היבטים למחשוב פולשני(סייבר):</u>

1) חדירה למחשב או למידע ממוחשב מבלי לפגוע במידע – למשל, פרשת טלי איסקוב, מעסיק שנכנס למחשב, מעתיק את המייל, ומבקש להגיש אותו כראיה בבית המשפט. מדובר בחדירה למידע במחשב. המידע הוא Intagiable.

Traffic Data Analysis – חדירה למחשב מבלי לפגוע במידע:

Non Data information : למשל, פירוט השיחות שלי בבזק. אבל לא יודעים את תוכן השיחה. המשמעות היא לדעת למשל באילו אתרים גלשתי ברשת. זה יכול להעיד מי הבן אדם, מתי הוא עשה את זה, מה הוא מחפש. לא מכיל את התוכן.
איפה בן אדם מסוים נמצא?

Event Log – באיזה שעה המחשב התחבר עם האינטרנט. מקרה של מישהו שחדר לאיוונט לוג. יש מדינות(גם בארץ) שהרגולציה שלהם בנוגע לחשיפת Non Data Information היא הרבה יותר קלה. בארצות הברית למשל התברר שהמשטר של בוש השיג Non Data Information על אזרחים שלא היו חשודים בדבר ללא שום צו.

המאפיין המרכזי לתחום זה הוא שמדובר בתחום ערטילאי. לבתי המשפט מאוד קשה להתמודד עם דברים שהם ערטילאיים, לא מוחשיים.

פרשת עזרא- היה מדובר בהאקר שחדר לחשבונות בנק, העביר כספים לחשבון הבנק שלו, והוא מזוכה מעבירת החדירה למחשב בערכאה הראשונה. גם בערעור שוב זיכו את עזרא מעבירת החדירה למחשב. השופט אליקים רובינשטיין הרשיע לראשונה את ניר עזרא בהסתמך על מאמרים בהלכה העברית בדיני המחשבים.
לבתי המשפט קשה לקבוע כי לא מדובר במשהו פיזי.

2) שינוי, שיבוש והפרעה למחשב: יש על כך חקיקה. מכניסים וירוס או תוכנה זדונית למחשב.

3) גניבת משאבים הנשלטים על ידי מחשב: המשאב הכי חשוב שאפשר לגנוב באמצעות המחשב הוא כסף (למשל, בפרשת אתי אלון, פרשת ניר עזרא). למשפט מאוד קשה להתמודד עם זה כי הם מאוד ערטילאיים.

4) "דואר זבל" – ההיבט הכי בעייתי של דואר זבל הוא הפגיעה בזכות של הפרט להיעזב לנפשו, "הטרדה". מדובר בפעולה טכנית של שליחת אימייל שיכולה להיות לגיטימית ויכולה להיות לא לגיטימית. צריך להבין מה הופך את ההודעה ל"לא לגיטימית".

מאפייני העוסקים במחשוב פולשני – מי הם האנשים שעוסקים בסייבר ופריצות למחשב?

א) גורמי שלטון או טרור : כאשר יש חשד שבן אדם רוצה לפגוע בשלום הציבור.
למשל יחידת הסייבר, שב"כ, גופי מודיעין (מוסד, 8200).
לגורמי השלטון יש מטרה לאתר פושעים, להגן על שלום הציבור, למנוע טרור.
מצד שני, מטרת הטרוריסטים היא לזרוע פחד.
"מלחמת סייבר"\"לוחמה אלקטרונית" – בשנת 2007 התפתחה לראשונה "לוחמת מחשבים" כאשר רוסיה, עפ"י פרסומים, חדרה למחשבים של מדינת אסטוניה בניסיון למוטט את אסטוניה. כמו כן, מהפנטגון בארצות הברית נגנבו אלפי מסמכים ויש החושדים שזה נעשה על ידי סין. כמו

כן, "לוחמה אלקטרונית" אומצה על ידי רוסיה במלחמתה מול רוסיה. בנוסף, לאיראן הוכנסה תולעת למחשבים שהאטה את פיתוח האטום.
הטורקים הפילו מטוס רוסי ובתגובה הרוסים השביתו הרבה אתרים של ממשלת טורקיה. **הסייבר מאומץ על ידי רשויות המדינה** מטעמי שיפור, מניעת מלחמה, הגנה על שלום הציבור, איסוף מודיעין. הסייבר מאומץ גם על ידי מדינות במלחמות וכן גם על ידי גורמי טרור.

גורם נוסף שעוסק בסייבר הוא **אזרחים פרטיים – ההאקרים.** "האקר" = פצחן.
בעבר ייחסו להאקרים חדירה למחשבים **ממניעים אידיאולוגיים**. לאנשים שחדרו למחשבים ממניעים אלו קראו גם "White Hats".
ההאקרים פרצו בכדי להרתיע מפני פרצות מחשבים. לדוגמא: האקר בשם איתן טען שהוא מגלה פרצות אבטחה במחשבים של גופי שלטון בארצות הברית. איתן נכנס לאתר של הגופים הללו וכתב "שימו לב, יש כאן פרצת אבטחה מסוג כזה וכזה..."

אידיאולוגיה נוספת – **"עיקרון פתיחות הרשת ונגישות המידע לציבור".**
אדם הנקרא קווין מיטניק היה "פרקר" – כלומר, אדם שפורץ למערכות טלפוניות ממוחשבות.
מיטניק חשב שמערכות הטלפוניה מאוד יקרות והן צריכות להיות משאב ציבורי לא יקר.
הוא היה פורץ למרכזיות טלפון ומתקשר על חשבונן לכל מיני מקומות.
החוקרת תורג'מן-גולדשמיט מציינת שפעמים רבות גם האקרים שהם "כובעים לבנים" מונעים משיקולים שהם לא בהכרח אידיאולוגיים או **אלטרואיסטים****"זולתנות"** – אלטר(זולת) ארואיזים(דאגה לזולת). גולדשמיט ראיינה עשרות האקרים והיא מספרת שבחלק מן המקרים ההאקרים פועלים מתוך נקמה אישית או מתוך רצון לחסוך כסף, כמו כן פועלים מתוך הנאה, הגשמה עצמית ורצון לצבור ידע במחשבים.

דוגמא לפון האקר: האחים בדיר -
האחים בדיר פרצו למערכות טלפונים ממוחשבות, שמעו הודעות קוליות שהושארו בהם והקימו מרכזיית טלפון בין לאומית על חשבון הטלפון של גלי צה"ל ביפו.
האקרים פועלים בכדי לדלות מידע אישי ממחשבים (לדוגמא: **אוהד טננבאום** היה מאוהב בבחורה וניסה לפרוץ למייל שלה בכדי לדעת עם מי היא מתכתבת).
תא"ל במילואים אלי בן מאיר אומר ש40% מתקיפות הסייבר בעולם מבוצעות על ידי עובדים מתוך הארגון, לעובדים יש גישה כדין למערות מחשבים. הם עובדים במשרד המעסיק שלהם, הוא נותן להם מחשב או שהם עובדים עם הלפטופ שלהם, ויש להם גישה למאגרי המידע של המעסיק ולמסמכיו הסודיים. לעיתים, הם גם מעבירים לעצמם או לאנשים אחרים מידע זה ולפעמים נכנסים למאגרים שאין להם גישה אליהם.
חלק ניכר מהפסיקה בישראל עוסקת גם במקרים הפוכים בהם המעסיק נותן לעובד שלו מחשב ואז המעסיק חודר למחשב הנ"ל.

גם **תאגידים מסחריים וחברות**, תרים אחרי סודות מסחריים, למשל: פרשת הסוס הטרויאני.
בפרשה זו דובר במהנדס מחשבים שתכנת תוכנת ריגול מתקדמת והיא אפשרה למי שמפעיל אותה

להפעיל את המחשב שחודרים אליו. המהנדס הועסק על ידי חוקרים פרטיים שהשולחים שלהם ביקשו מהם לדלות מידע על הנעשה במחשבים של המתחרים שלהם. Spyware : תוכנות ריגול.

סטודנטים, מעסיקים, האקרים, גורמים ממשלתיים, עובדים...
מי שעוסק עוד בתחום של מחשוב פולשני הם גם אנשים שפועלים מתוך מניעים כלכליים לצורך גניבת משאבים, השתלטות על המחשב בכדי לקבל כופר...

"קראקרים" – פרצנים. אנשים אשר המניע שלהם הוא וונדליזם, הרס.
המניע שלהם שהם הורסים מערכות מחשבים הוא בכדי ללמוד איך המערכת פועלת.

מאפייני תופעת המחשוב הפולשני:

1. קלות וזמינות החדירה למחשב – **בפס"ד עזרא** בית המשפט אומר שזה לא היה כל כך קשה לחדור למחשב ולכן זיכו את עזרא בגלגול הראשון של פסק הדין.
מאוד קל לפרוץ למחשבים ולא צריך להיות גאון מחשבים בכדי לפרוץ למערכות מחשבים. אפשר בקלות רבה להוריד תוכנות פריצה מהאינטרנט ולפרוץ למחשבים.
הסייבר **"נשלט מרחוק"**, ההאקר יכול לשבת בביתו ולהפיץ תוכנת וירוס שתפגע במחשבים ברחבי העולם. די במחשב אחד מחובר או בטלפון חכם אחד בשביל לחדור למחשבים. יש מוצרים שהם **IOT** – למשל, מצלמות אבטחה. האקרים מתחברים למצלמות אלו ודרכן הם תוקפים חברות אחרות.
2. פיתוי – זה מפתה לחדור למחשבים. האינטרנט הוא כלי אחסון של מידע וחדירה למחשב יכולה למלא את הסקרנות של האנשים. פוטנציאל הניצול האדיר הוא עניין מפתה.
3. חוסר המודעות לעצם הפלישה – במחשבים הרבה פעמים, ולרוב, אין מודעות לעצם הפלישה.
רק 5% מכלל התקיפות והפריצות למחשבים מזוהות. בפרשת הסוס הטרויאני היה מדובר בפריצה למערכות המחשבים החשובות ביותר במשק של התאגידים הכי חשובים במשק, של המנכ"לים של אותם תאגידים, ואיש מאותם מנכ"לים שהוחדר למחשב שלהם תוכנת ריגול לא היה מודע לעצם החדירה למחשב שלו. **"אי נראות"** של הסייבר, בדרך כלל לא יודעים שיש חדירה למחשב.

קבצי Cookies : אנחנו לא יודעים מה אותם קבצים עושים למחשב שלנו. קבצי העוגיות נמצאים באתרים שאנחנו נכנסים אליהם. על פי רוב, לא מיידעים את האנשים על קבצי הקוקיז (אלא אם שינינו את ההגדרות שלנו במחשב). מדובר על קובץ מידע ששומר במחשב שלנו את **ה"Where - "About**, כלומר, איפה היינו באתר בדיוק באיזו שעה, באילו נושאים עיינתי באתר וכדומה... וזה יוצר פרסומות מתעוררות.
Defaults – ברירת מחדל. "Allow Cookies" ← צריך להתיר את הכניסה של הקוקיז מבלי שישאלו אותי. הקבצים האלו יכולים להישאר במחשב שלנו עד עשרות שנים.

4. כשל מידע – חוסר מודעות לנזקי התופעה ולדרכי ההתגוננות:
בפס"ד בדיר אמר בית המשפט שהבעיה העיקרית היא **Social Engineering** – "הנדסת אנוש",

הכוונה היא שכל הטעויות הן טעויות אנוש, אפשר לרמות בקלות מאוד את האנשים ולגרום להם לתת את הקוד הסודי שלהם.

5. קושי באיתור המזיק והעבריין – קשה מאוד לאתר את ההאקרים. ההאקרים פעמים רבות יכולים לפעול גם ממחשב של מישהו אחר, כלומר הם יכולים לפרוץ למחשב של אדם אחר ומשם לפעול. **DOS** – מתקפה שבה פורצים למחשב של מישהו אחד ומהמחשב הזה פורצים למחשב של איש אחר כך שקשה מאוד לאתר את ההאקר.

6. גלובאליות וקושי בהבאת המזיקים לדין – תופעת הסייבר היא עולמית ונפרסת על פני כל הגלובוס. מכיוון שכך, גם כאשר אנחנו מצליחים לתפוס את ההאקר, קשה להביא אותו לדין.

7. היעדר כיס עמוק – לרוב המזיקים, עברייני הסייבר, אין להם כיס עמוק. 40% מכלל האנשים שעוסקים בסייבר הם עובדים, מעסיקים קטנים, האקרים, קראקרים, אנשים צעירים. אולם הנזקים שהם גורמים להם הם אדירים. אין להם כסף לשלם על הנזק שהם גרמו לו ולכן הם אינם יכולים לפצות את הניזוקים במישור הנזיקי.

8. הקושי בהוכחת העבירה ובניהול הדיון המשפטי – בשביל להוכיח הליך פלילי בכל הנוגע לסייבר, צריך להביא לבית המשפט את המחשב. בהיבט הפלילי, אנחנו לא רוצים לתת לשוטר לראות מה קורה לנו במחשב. מצד שני, בהיבט הנזיקי אנחנו צריכים לתת למומחה של ההאקר להיכנס לנו למחשב. הקושי בהוכחת העבירה ובניהול הדיון המשפטי מתייחס לכך שכשצריך לנהל תיק הוכחות בעבירות סייבר צריך לחשוף את המחשב שלנו בפני שוטר או עד מומחה של הצד השני, ולא הרבה רוצים לעשות את זה ולהראות את האינפורמציה שיש להם במחשב.

9. יחס סלחני של החברה - גלוריפיקציה(תהילה): בכל הנושא של סייבר מי שעושים לו גלוריפיקציה הוא ההאקר, מוותרים לו. מכיוון שההאקרים נתפסים בחברה המודרנית כאנשים חכמים, מתוחכמים, לא רק שיש כלפיהם יחס סלחני אלא שגם מהללים אותם, יש האדרה של ההאקרים. מעסיקים האקרים בשביל לבדוק שהמערכת חפה מתקלות. תורג'מן אומרת כי בשנים האחרונות משתנה היחס ומתחילים להתייחס אל ההאקרים כאל עבריינים, מה גם, שלתחום הסייבר נכנסים בשנים האחרונות גורמים פליליים כמו משפחות פשע...

10. רתיעה מנקיטה בהליכים משפטיים – באינטל למשל, מסופר בפרשת בדיר שחברת אינטל שילמה דמי שתיקה לאחים בדיר בכדי שהם לא יפיצו את העובדה שהם פרצו למערכות המידע שלה. כלומר, לא נוקטים בהליכים משפטיים משום שהדבר יהווה **הודאה** בכישלון מערכת האבטחה הממוחשבת.

סיבה נוספת לרתיעה מנקיטה בהליכים משפטיים היא חשש **מהסגות גבול זדוניות** ומרושעות אשר תבואנה כנקמה על עצם נקיטה בהליכים משפטיים.

סיבה נוספת, מדובר **באנשים נורמטיביים**. ההאקרים הם אנשים נורמטיביים: עובדים, מעסיקים, ומעדיפים לסגור איתם העניין.

התוצאה של כל המאפיינים הללו היא שיש **"תת הרתעה"** כלומר, יש פחות מידי הרתעה.

ההאקרים אינם נרתעים, והניזוקים ממשיכים לסבול בשקט, הם לא פונים לאפיק הפלילי וגם לא לאפיק הנזיקי, הם לא פונים למשטרה, ואכן – מתוך 5% מכלל עבירות המחשב שמתגלות רק 5% מדווחות למשטרה. כך גם בהליך הנזיקי. ההליך הנזיקי דורש משאבים כלכליים מאוד גבוהים ולכן אנשים נרתעים מהגשת תביעות נזיקיות.

יש **"כשל שוק"** בתחום הזה. כלומר, מצד אחד יש תופעה מאוד נרחבת אבל מצד שני לא עושים כנגדה כלום. למרות תת ההרתעה וכשל השוק הזה אנחנו נראה תיקים(כמו בפרשת ניר עזרא) שבהם בתי המשפט מזכים, ובתחום העוולות המסחריות המצב יותר גרוע: עובדים שגונבים סודות מסחריים, בתי המשפט לא עושים עם זה הרבה.

סיכום: הנזקים הם **נזקים פיזיים וכלכליים**, הריסה של מחשבים ומערכות מחשבים, גונבים כספים. ישנה **פגיעה באינטרסים תועלתניים**: אם מערכות המחשבים לא פועלות אז הפונקציות של המחשב לא מתאפשרות – כלי שליטה ובקרה, כלי בידור, במה לכלי תקשורת ועוד...

נזק נוסף – **פגיעה בזכויות אדם** הנגרמת כתוצאה מהמחשוב הפולשני: זכות לפרטיות, ביטחון הציבור...

שאלה:

א' חודר לאתר "הבלוגיה". א' משנה את מראה פני האתר(defacing) בבלוג של בנימינה. במקום הציור היפה עכשיו מופיעה שם גולגולת. הקיפו בעיגול את התשובה הנכונה:

1. א' פגע בפונקציה של הרשת ככלי אחסון ומשאב.
2. א' פגע בפונקציה של הרשת ככלי לגלוריפיקציה של הגולשים(שרובם ככולם נורמטיביים).
3. א' פגע בפונקציה של הרשת ככלי אחסון של המשאב

4. א' פגע בפונקציה של הרשת כפלטפורמה לחופש ביטוי ובמקרה זה גם ככלי לתקשורת המונים.

זכויות האדם שנפגעות בחדירה למחשב: הזכות לקניין, הזכות לכבוד(אוטונומיה), חופש הביטוי (עליהם נרחיב את הדיבור בהמשך).

1. הזכות לפרטיות – הזכות לפרטיות במשפט המערבי היא זכות חדשה מאוד. באנגליה למשל כמעט לא מדברים עליה עד עצם היום הזה.

רקע היסטורי בהתפתחות הזכות לפרטיות: במאה ה17 (1,600 ו...) היה נהוג לפתוח מכתבים של אזרחים ע"י השלטונות. כלומר, השלטונות נהגו לקחת מכתבים של נתינים(אזרחים) שלהם, מכיוון שהמכתבים היו סגורים בחותם שעווה לקחו את המכתבים למשקע אפלה בעזרת אדים היו פותחים את החותם, קוראים את המכתבים וככה היו אוספים מידע על המתנגדים של השליט, על אשתו וכדומה.

"Black Chambal's"("הלשכות האפלות"): פענוח אגרות לאיסוף מודיעין ולפענוח אגרות מותפלות. הם היו נפוצים בכל רחבי אירופה. השלטון הרגיש חופשי להיכנס לאגרות של אנשים, ולכן לא הייתה באותה התקופה הגנה על הפרטיות. הם התרחבו מאוד ונפוצו בכל אירופה עד לאמצע המאה ה19 (1,850). באנגליה רשות הדואר הפכה לזרוע של סוכנות הביון(הריגול) הלאומית. היה חריג אחד, במאה ה-18 (1782) – בארה"ב הומצאה פקודה שאסרה על רשות הדואר

לפתוח מכתבים של אזרחים ללא צו. לפקודה הזו לא היה באמת ביטוי בשטח משום שעדיין רשות הדואר נהגה לפתוח מכתבים של אזרחים.
במחצית השנייה של המאה ה-19 (1850) החלו לנשב רוחות ליברליות. פתאום אנשים הבינו שיש להם זכויות אדם: זכות לקניין... אבל אף אחד לא דיבר על הזכות לפרטיות. התושבים רצו חוקה שתעניק להם זכויות בכתב.
ביוני 1884 החלו הפגנות בבריטניה כנגד הנוהג של פתיחת מכתבים על ידי הרשויות והופסק בבריטניה הנוהג השלטוני ליירד תכתובת של אזרחים.
נקבע שפתיחת אגרות מחייבת צו שיפוטי ולאט לאט סגרו את הלשכות האפלות, זה היה תהליך מתפשט עד תחילת המאה שעברה. למרות זאת – בשום חוקה לא הייתה התייחסות לזכות לפרטיות. כלומר, התחילו להגן על חדירה לדואר מפני חדירה שרירותית.

חריגים:
בשנת 1980, שניים מהוגי הדעה המשפטית בארצות הברית: וורן ובראנדס כתבו מאמר ששמו "The right to privacy" – הם אמרו שלכל אדם יש זכות לפרטיות אפילו אם היא לא כתובה על ספר. כלומר, לא חקוקה. זה מאמר בעל חשיבות גדולה.

בשנת 1948, לאחר מלחמת העולם השנייה התחילו המדינות לאמץ הצהרות, אמנות בין לאומיות שמתייחסות לזכות לפרטיות. למשל: ההכרזה האוניברסאלית על זכויות האדם מתייחסת לזכות של אדם לפרטיות בביתו ובתכתובות שלו (יומן, מכתבים)...

עדיין פסיקת בתי המשפט לא מכירה בקיומה של הזכות לפרטיות. גם החקיקה הלאומית(שבתוך מדינות) לא מתייחסת לזכות לפרטיות.

אחד מפסקי הדין הראשונים בעולם שהכיר בקיומה של הזכות לפרטיות הוא פס"ד **גריזוולד נ' קונטיקט (1985)** – בפס"ד זה היה מדובר בחוק של מדינת קונטיקט שעסק בתחום של אמצעי מניעה. הייתה עתירה ששל גריזוולד לבית המשפט, תחילה לבית המשפט הקהילתי ולאחר מכן לבית המשפט הפדראלי.
האם חוק שאוסר שימוש באמצעי מניעה פוגע בפרטיות?
בית המשפט אמר שיש כאן בעיה מכיוון שאם אנחנו מסתכלים על החוקה האמריקאית לא מוזכרת בה הזכות לפרטיות בשום מקום. למרות שהחוקה האמריקאית אינה מתייחסת מפורשות לזכות לפרטיות, בית המשפט קבע שהחוק המדינתי הזה פוגע בזכות לפרטיות. שניים מהשופטים בהרכב הדיון אמרו הזכות לפרטיות עולה מזכויות אחרות שכן מפורשות בחוקה, למשל: חופש המצפון. אם לכל אחד יש זכות להחליט מה שהוא רוצה אז יש לו גם זכות לפרטיות להחליט גם בנוגע לחיי המשפחה שלו מה שהוא רוצה. גם פסיקה מאוחרת יותר הלכה בעקבות פסק הדין הזה וקבעה שיש זכות חוקתית לפרטיות למרות שזכות זו אינה מפורשת בחוקה.

התפתחות הגנת הפרטיות בישראל:

במשפט הישראלי קיימת עבירה של "הסגת גבול במיטלטלין" וזה גם אמצעי לשמור על הרכוש של האדם. בכל זאת בית המשפט קובע בשנות ה-50 וה60 שאין הגנה על הזכות לפרטיות של האדם.
"איסור פתיחה של דבר דואר ללא צו", בשנות ה-80 אסור היה להטריד אדם באמצעות הטלפון\הטלגרף.
החל מ1979 מאומצת בישראל חקיקה שמגנה על הזכות לפרטיות באמצעות חוקים.
חוק האזנת סתם שאסר על האזנה לשיחה של הזולת באמצעות מכשיר האזנה.
1981 חוקק חוק הגנת הפרטיות, ומאוחר יותר חוקק חוק יסוד : כבוד האדם וחירותו שהגן על הזכות לכבוד ופרטיות.
בשנת 1995 חוקק "חוק המחשבים".
בשנת 2001 חוקק "החוק למניעת הטרדה מאיימת" המתייחס למצב שמישהו הולך ברחוב ומישהו עוקב אחריו בגלוי.

חוק הגנת הפרטיות ותקנות הגנת הפרטיות:

סעיף 8 לחוק - הגנה על מאגרי מידע. חובת רישום.
סעיף 13 לחוק – כל אדם זכאי לעיין במידע שמוחזק עליו במאגר מידע.
סעיף 17 לחוק – בעל מאגר מידע אחראי לאבטחת המידע. חברות במחזיקות במאגר מידע הן כמו בנק, המידע שמוחזק על אנשים צריך להיות מאובטח.

בשנת 2017 התקינו את תקנות הגנת הפרטיות(אבטחת מידע) שבהן חייבו בעל מאגר מידע לדווח על רשם מאגרי המידע על אירועי אבטחה במאגר המידע (אם פרצו למישהו לתוך המערכת).
הם חייבים לדווח, ולפעמים 'רשם מאגרי המידע' יכול לחייב אותם לדווח על אירועי אבטחה לנושאי המידע שפרטיהם כלולים במאגר.
חובה מעין זו קיימת גם בארה"ב במקומות מסוימים וגם באירופה.

תקנה 7 לתקנות הגנת הפרטיות קובעת – "לא ייתן בעל מאגר מידע גישה למידע המצוי במאגר אלא אם כן נקט אמצעים סבירים בהליכי מיון עובדים". המעסיק צריך למעשה לבדוק את מי הוא מקבל לעבוד אצלו בתור אחראי מידע ולסנן בעלי הגישה למאגר מידע.

תקנה 9(א) – בעל מאגר המידע יבדוק שהגישה למאגר המידע תהיה ע"י מורשה כניסה למאגר המידע.

תקנה 10 – תיעוד של זהות משתמש במאגר המידע, תאריך, שעה... ולשמור זאת במשך שנתיים.

תקנה 11 – חייבים לתעד אירוע אבטחה.

חוק מניעת הטרדה מאיימת, התשס"ב – 2001.

סעיף 30א לחוק התקשורת – שיגור דבר פרסומת באמצעות מיתקן בזק (תקשורת ממרחק):
Opt – in: בשביל שיעשו לך משהו, שישלחו לך פרסומות, ידווחו על מבצעים וכו'... אתה צריך לבקש להיכנס לזה ושישלחו לך. **חייב את הרשות\הסכמה\שיחה מוקלטת\אישור** בכתב שלי.

קיימים שני חריגים:
א. פניה חד פעמית מטעם מפרסם לנמען שהוא בית עסק פעם אחת לא תיחשב.
ב. רשאי מפרסם לשגר דבר פרסומת כאמור אף אם לא התקבלה הסכמת הנמען(מי ששולחים לו את דבר הפרסומת). הנמען מסר את פרטיו למפרסם במהלך רכישה של מוצר... והמפרסם הודיע לו כי הפרטים שמסר ישמשו לצורך משלוח דבר פרסומת, למשל: חתימה על כרטיס מועדון.

Opt – out: אני רוצה שלא ישלחו לי דברי פרסומת בכלל. **מי שמבקש לצאת מזה** מחייבים את בעל מאגר המידע שיוציא את אותו אדם מזה.
נתנו את הפרטים שלנו למשל לצורך כרטיס מועדון והמפרסם הודיע לנו שישלח לנו דברי דואר בעקבות המנוי, תמיד יש לנו אפשרות לOpt out (יציאה ממאגר המידע).
המפר הוראה זו דינו קנס, והפרת סעיף זה מהווה עוולה אזרחית(נזיקית). אם שוגר דבר פרסומת ביודעין, הפרסום יהיה עד 1,000 ₪ ובתי המשפט כיום מתחילים אט אט להבין את החשיבות של הפיצוי הזה משום שכולם מקבלים הודעות כאלה וזה פוגע בזכותינו לא להיות מוטרדים.

מה קרה ב70 השנה האחרונות שגרם להגנה כל כך מאסיבית על הזכות לפרטיות?

למה פתאום יש מבול של חקיקה בכל הנוגע בזכות לפרטיות?
התפתחות חקיקה שמגנה על הזכות לפרטיות + התפתחויות חקיקתיות אירופאיות:

* **הגורם הראשון** – <u>התרחבות עוצמתם של אמצעי התקשורת ההמוניים</u> בסוף המאה ה19 (1890) (למשל התפתחות הרדיו, טלוויזיה, עיתון). במקביל, התפתחה ה"עיתונאות הצהובה".
וורן וברנדס אומרים שהטריגר שגרם להם לכתוב את המאמר שלהם היה שפירסמו הודעה רכילותית באחד העיתונים. פגיעה בפרטיות מורידה את הסטנדרטים המוסריים של החברה משום שהיא רכילותית. רכילות הייתה טריגר למאמר החשוב ביותר בנושא הזכות לפרטיות. זה הוביל לחקיקה בנוגע ללשון הרע וגם לאסדרה=(רגולציה: מה מותר ומה אסור לעשות) של כלי התקשורת.
גם האינטרנט ככלי תקשורת המוני גרם לניסיון לבדוק מהי האחריות של פייסבוק לגבי המידע שמתפרסם בו? נדבר על כך בהמשך, עדיין אין לכך חוק מסודר.
פרשת רמי לוי: דובר באדם שהוא מטפל הוליסטי והוא גילה שמישהו כתב עליו פוסט קשה ברשת. הוא ביקש מהאתר למחוק את הטוקבק ורצה לתבוע בנזיקין את מי שפרסם עליו את הטוקבק הזה.
הטוקבקיסט היה אנונימי ובית המשפט לא רצה לחשוף את הכתובת של הטוקבקיסט.
מצד אחד רצו לשמור על הזכות לפרטיות של הטוקבקיסט, ומצד שני לא הגנו על הזכות לשם טוב של רמי לוי.

בתזכיר חוק מסחר אלקטרוני (לפני הצעת חוק) – נקבע מה האחריות של אתרי אינטרנט?

*** הגורם השני** – <u>פיתוח טכנולוגיות אחסון ואיסוף(מאגרי מידע)</u>:

הטכנולוגיות מאפשרות לנו לאגור מידע על אנשים אחרים, וגם לעבד את המידע הזה, להצליב מידע במידע אחר... ולבנות פרופיל מחודש לגולש.

פרופ' האצ'ר אומר: במאגרי המידע יש סכנת פריצה. צד שלישי יכול לפרוץ למאגר המידע. יש סכנה של דליפת מידע לצד שלישי, הפורץ, הגונב, הקונה, או המקבל של המידע... חברות סוחרות במידע הזה. בעיה נוספת היא, שלילת הפיקוח על דיוק הנתונים. ולכן תקנות הגנת המידע אומרות שלכל אדם יש את הזכות לקבל את האינפורמציה שיש לחברה עליו על מנת שיוכל לתקן את המידע הנ"ל בין היתר.

סעיף 2(9) לחוק הגנת הפרטיות קובע: "אין לעשות שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה שלשמה היא נמסרה".

באירופה, ה- "EU DATA PROTECTION DIRECTI" קבע שניתן להעביר מידע פרטי למדינת צד שלישי (שלא באיחוד האירופי) רק אם אותה מדינת צד שלישי מחזיקה ברמה נאותה של אבטחת מידע.

פייסבוק באירופה רצתה להעביר מידע לפייסבוק ארה"ב על כל נתוני הגולשים. בכדי שתאגידים באירופה יוכלו להעביר מאגרי מידע אישיים לתאגידים בארצות הברית התפתחה פרוצדורה שנקראה "SAFE HARBOR". אם התאגיד שמקבל את המידע לוקח על עצמו לשמור על כל מיני הוראות של פרטיות, אבטחת מידע וכו', אז מותר להעביר לו את המידע מהאיחוד האירופי לארצות הברית.

בפרשת SCHREMS, היה מדובר בסטודנט אוסטרי שנחשף לגילויים של סנואודן.

סנואודן היה עובד של אחת מסוכנויות הביון האמריקאיות והוא העתיק על דיסק מידע שחשף איך החברות פוגעות בין היתר בזכות לפרטיות של ראשי מדינות אחרות, איך הן מצותתות לראשי מדינות אחרות, מקבלים מפייסבוק את הDATA על הגולשים שלה בלי צווים. שריימס הסטודנט פונה לבית המשפט האירופי לצדק (ECG) ואומר להם שהוא העביר את המידע שלו לפייסבוק אנגליה, פייסבוק אנגליה שומרת כראוי על הפרטיות שלי, אך היא מעבירה את המידע שלו לפייסבוק ארצות הברית שמחויבת לכללי ה"סייף הארבור".

כללי הסייף הארבור אינם רלוונטיים בכל הנוגע לכך שהתאגיד האמריקאי מעביר את המידע לא לתאגיד שלישי, אלא לסוכנות ביון ממשלתית והסייף הארבור לא מגן על הפרטים במקרה הזה.

בית המשפט האירופי קבע: "הסייף הארבור הוא לא חוקתי: "הסדר הסייף הארבור איננו מספיק שכן הוא לא מחייב את הרשויות הממשלתיות האמריקאיות אלא רק את התאגידים האמריקאיים. לפיכך, רשויות הביון האמריקאיות משוחררות מהוראותיו. כך נגרמת פגיעה גורפת ובלתי מידתית בפרטיות של נשואי המידע" (שריימס). החקיקה האמריקאית לא מאפשרת לנשואי המידע לעתור לקבלת סעדים משפטיים בקשר לפגיעה בפרטיותם, למשל, החקיקה האמריקאית לא מאפשרת גישה למידע שנאסף על הפרט, היא לא מאפשרת לדרוש את תיקון המידע, היא לא מאפשרת למחוק מידע לא נכון שנמצא במאגר המידע ולכן אין הגנה מספקת על הפרטיות, המידע

מועבר לגופי הביון בלי שום סינון – ולכן, הסייף הארבור הוא לא חוקתי והוא בטל.
אומץ כלי חדש שנקרא "EU-US PRIVACY SHILD": מגן פרטיות שיאפשר לתושבי האיחוד האירופי לפנות לבתי המשפט בארצות הברית בכדי להגן על המידע שלהם.

בעבר, הרגולציה על הData משנת 2006 מחויבת לאחסן נתונים עד שנתיים במאגרי מידע. זה חייב חברות כמו פייסבוק לשמור מידע שנתיים אחורנית בכדי שלרשויות השלטון תהיה גישה למידע (גם אם הפרטים לא חשודים בכלום).
בשנת 2014 קבע בית המשפט **בפס"ד אירלנד** שהחוק הזה קובע בצורה לא פרופורציונאלית בזכות לפרטיות, שכן, מחייבים לאסוף מידע על אנשים שאינם חשודים.

* **הגורם השלישי** – הכניסה לתחום הפרט באמצעים טכנולוגיים.
למשל, שליחת SMS שיווקי המוני. סעיף 30א לחוק התקשורת בא להגן על כך.

* **הגורם הרביעי** – ההכרה האנושית בחשיבות ערך הפרטיות.
פרופ' רות גביזון: מה קרה שפתאום יש מבול של אמנות שמגנות על הזכות לפרטיות?
לדעתה, בשלות חברתית היא שהובילה להכרה האנושית בחשיבות ערך הפרטיות. הייתה תחושה של אנשים שהגענו לרגע בהיסטוריה שבו אנחנו יכולים להרשות לעצמנו להכיר בחשיבות של הערך שבפרטיות. **הפגיעה בפרטיות אפשרה את הפגיעה החמורה יותר בזכויות אדם כמו הזכות לחירות והזכות לחיים.** לדוגמא: הנאצים ביררו דרך מרשם האוכלוסין פרטים על יהודים(מקום מגוריהם) בשואה על מנת לרצוח אותם.
במלחמת העולם השנייה הופקע חופש הפרט בעזרת הפצת נתוני אמת אובייקטיבים ובסיסיים.
האם יש בשלות חברתית גם בכל הנוגע לפרטיות שלנו ברשת? האם יש מודעות לכך שיש לנו זכות לפרטיות או שאנחנו מקבלים את הזכות לפרטיות כדבר מובן מאליו?
אנחנו מסכימים לפגיעה חמורה בפרטיות שלנו. אנחנו למעשה החזרנו את עצמנו 200 שנה אחורנית.

לפני 10 שנים כתב **האצ'ר** ש"יש הכרה חברתית בצורך לשמירה על פרטיות הגולש באינטרנט, שיש הבשלה מסוימת ושהיום יש מודעות לכך שצריך להגן על פרטיות הגולש מפני לקיחה של פרטיו האישיים". אבל, לדעת המרצה – אין באמת מודעות ואין באמת עמידה על זכותנו לפרטיות.

חשיבות ההגנה על הזכות לפרטיות ברשת

על ארבע הנקודות הבאות עמד **פרופ' ווסטין**, מלומד שחקר את נושא הפרטיות והראשון בשנת 1968 שכתב ספר בנושא שהסביר את חשיבות הזכות לפרטיות:

ארבע סיבות תועלתניות בצורך להגנה על הזכות לפרטיות:
הפילוסוף המשפטי בנטהאם אמר שיש זכות לקניין בגלל שאם המדינה תגן על הקניין שלנו זה יביא לתועלת ואושר למקסימום אנשים.

1) לכל אדם יש צורך להיות לבד כדי לבחון ולפתח רעיונות – ההתפתחות האישית של הפרט וגיבוש מחשבה עצמאית ושונה מצריכה זמן שבו הפרט יהיה לבדו ולא יחשוש מלגלוג או מעונש. כלומר, אדם לא יכתוב אם כל הזמן המרצה שלו ישב לו על הראש. הוא כל הזמן יפחד ממה שהמרצה יגיד. אם אנשים יפחדו מלהתפתח החברה תסבול.

2) הצורך של האדם להיות בלי מסכות ולהשיג מנוחה ממתחים מצטברים – החיים בחברה המודרנית גוררים מתחים רבים. בריאותו המנטאלית(השכלית) והפיזית של הפרט דורשת פריקת מסיכות\מתחים. בשביל לפרוק את הריגושים והלחץ, אדם צריך לשחרר קיטור ולסטות, אפילו אם זמנית, מנורמות ההתנהגות המקובלות בחברה. בשביל כך האדם צריך את ד אמותיו(ארבעת אמותיו – "המחרב הפרטי שלו").

3) הצורך בשמירה על הסודיות בתקשורת הבין אישית – לדעתו של ווסטין, התקשורת הבין אישית היא מוגבלת, הפרט אינו מגלה את כל העניינים הסודיים שלו. אבל צריך להגן על הפרטיות בכדי שיהיו איים של שמירה על הסודיות. האינטרנט צריך להגן על התקשורת האישית שלנו ברשת. אנחנו חייבים שפייסבוק לא תעביר בשוטף את המידע שלנו לגורמי ביון.

4) הצורך בזמן ללא התערבות חיצונית – כל אחד מאיתנו צריך זמן בכדי לעכל את המידע ואת החוויות שעברנו בכדי לתכנן את צעדינו העתידיים. אנחנו צריכים זמן להיעזב לנפשנו. טכנולוגיית המחשבים\הטכנולוגיה הדיגיטלית מאפשרת להטריד אותנו במרחב הפרטי שלנו. למשל, מסרונים שיווקיים, דואר זבל, שיחות טלפון שיווקיות...

5) מלומד אחר בשם פרייד אמר שהפרטיות הכרחית למערכת יחסים של אהבה, זוגיות ואמון להבעת רגשות.

6) פגיעה ברגשותיו של הפרט – עוצמת הפגיעה ברגשותיו של האדם תלויה בסוג הסגת הגבול, המחשב הוא קניין מכונן, בעל חשיבות בסיסית ביותר, לרבות הפלאפון שלנו. בחברה המודרנית אנחנו מאכסנים בו הכול ושאדם מגלה שצ'וטטו לשיחות שלו דרך המחשב זה מטלטל את נפשו.

7) הצורך באנונימיות – ההגנה על הפרטיות מאפשרת לאדם להביע דעה, עמדה שונה ומנוגדת להלך הרוח הכללי... הצורך בהגנה על חיסיון פרטיו של המפרסם. כמו כן, אנשים מפרסמים

פוסטים באמצעות פסידונים (שם שהוא לא נכון\שם מטעה). האנונימיות מאפשרת לגוון את השיח התרבותי ברשת.
פרשת **בורוכוב נ' פורן** – היה מדובר בפורום של חרשים שאחד הטוקבקיסטים פרסם משהו תחת הפסידונים שלו (הכינוי שלו\השם הלא אמיתי שלו). מנהל הפורום פרסם את הפסידונים והייתה כאן פגיעה קשה בזכות לפרטיות.

8) הפגיעה בקניין – כשנעשית חדירה למחשב היא מאפשרת לפגוע בקניין של האדם. כי במחשב יש לנו קודים סודיים, כסף, פרטים שונים.

9) מניעת סממנים שלטוניים טוטליטריים – שלטון טוטליטרי הינו שלטון במרכז כוח רב בכל הנוגע לאזרחים באותה החברה באמצעות ריכוז מידע רב על האזרחים.
בשלטון עריץ השלטון מבצע מעקב אחר הפרט לא רק במטרה למנוע טרור או למצוא חשודים בפשעים, אלא למשל להסיר מתנגדים או סיבות פרטיות, בשביל לסחוט יריבים פוליטיים (לדוג': יחידת ההאזנה בצה"ל שהאזינה לשיחות טלפונים של אלופים בצבא).
'תופעת האח הגדול' – חברה שבה השלטון עוקב כל הזמן אחרי הפרט, יודע איפה אנשים נמצאו בכל העת, ע"י מצלמות, מיקרופונים... גם אם הם לא עבריינים.
תופעת האח הקטן - תאגידים שמכרזים מידע על הפרט כמו ממשלים טוטליטריים. הפייסבוק זו דוגמא מובהקת לאח קטן.
הבעיה עם תופעת האח הגדול היא שאנשים ישרי דרך לא יביעו את דעתם גם בפורומים סגורים כנגד השלטון מכיוון שהם יפחדו שהנתונים על אודותם יירשמו ויענישו אותם לאחר מכן.
אנטגוניזם כנגד השלטון: גישת אנטי לשלטון כי כל הזמן יש תחושה שעוקבים אחרי הפרט.
לכאורה, הNSA קיבל מאגרי מידע של חברות הטלפון בארצות הברית לא לגבי חשודים ספציפיים ובלי צווי בית משפט.
בשנות ה90 ארה"ב הפעילה את תוכנת "קליפרט שיפט" אשר אפשרה לצ'וטט למחשבים מוצפנים.

10) סיבה הומניסטית – לאדם יש זכות שיגנו על הפרטיות שלו מבלי קשר שזה מועיל למדינה.

המלומד ריימן אומר שהפרטיות היא קניין מוסרי של הפרט, משהו ששייך לפרט, משהו שקשור לקיום של הפרט ובלעדיה קשה לקיים חיים נורמאליים.
השופט ברק פס"ד **פלונית נ' בית הדין הרבני** – "סביב כל אדם יש מרחב שבתוכו הוא זכאי להיות עם עצמו. מרחב זה נע עם האדם עצמו, על כן, הוא עשוי לחול גם במקום שבו אין לפרט כל קניין כגון בית חולים, תא טלפון או בית הוריו".

שאלה לדוגמא:

א' מקבל דבר דואר פרסומי שמציע לו הגנה משפטית מחברת "גיבורים בע"מ" למקרה שחזר שיק שלו. א' חושד שחברת "שיקים חוזרים לעד" מחזיקה במאגר המידע שלה מידע לא מדויק עליו שכן לפני שבוע חזר לו שיק שהוא שכח לכתוב עליו את התאריך.

א) לפי סעיף 30א לחוק התקשורת בזק ושידורים חברת "גיבורים בע"מ" יכולה לשלוח לו דברי דואר בהיותו אדם פרטי.

ב) חברת גיבורים יכולה לשלוח לו דבר דואר שיווקי אחד כמו שקרה במקרה זה

ג) בחוק הבזק יש מנגנון Opt-in ולכן החברה לא יכולה לשלוח לו דבר דואר – מבקשים ממנו להיכנס.

ד) תשובות א' ו-ב' נכונות.

שאלה שנייה:

א' חושד שחברת "שיקים חוזרים לעד" מחזיקה במאגר המידע שלה מידע לא מדויק עליו שכן לפני שבוע חזר לו שיק שהוא שכח לכתוב עליו את התאריך.

א) א' יוכל לפנות לחברת "צ'קים חוזרים" לפי תקנות הגנת הפרטיות ולבקש את המידע שהיא מחזיקה על אודותיו.

ב) לפי הדירקטיבה האירופית, החברה מחויבת להחזיק במאגר המידע הזה ולכן א' לא יוכל לבקש להימחק ממנו

ג) מכיוון שהזכות לפרטיות היא פועל יוצא של התפתחויות טכנולוגיות, המחוקק ביקש להגן על מאגרי מידע ולא מאפשר שינוי תוכן של מידע המוחזק בהם.

ד) אף תשובה אינה נכונה.

הקורס נחלק לשני חלקים: 1. החלק הנורמטיבי- פגיעה בזכויות האדם. 2. הדין הקיים-סעיפי חוק וכו'.

דוגמא לשאלה פתוחה לבחינה - אהרון מאוד אוהב את חברת הכבלים הדיגיטליים חברת "גלילה" כי היא זולה וטובה. אבל אהרון גילה לתדהמתו שחברת הכבלים הדיגיטלית "גלילה" (ממחושבת) שאליה הוא מחובר, מעבירה את רשימת הצפייה שלו לחברת הפרסומות "בואו נצפה" ולרשויות הביטחון במדינה. התייחסו להיבטים **הנורמטיביים** של הסוגיה:

א. התייחסו גם לסוגיה במובנה הרחב
ב. מהי זכות האדם העיקרית הנפגעת
ג. מדוע היא נפגעת
ד. מהו הדין הראוי לדעתכם

תשובה-

א. חשיבות המחשב, המחשב הוא כלי תקשורת, כלי בידור, זול, מהיר המקדם את העולם. פונקציות חיוביות. למחשב יש 5 פונקציות, במקרה דנן, חברה "גלילה" הוא גם כלי תקשורת, גם כלי בידור וגם זול ומהיר.

ב. הזכות הנפגעת היא הזכות לפרטיות. אמנם מדובר בנתוני אמת, שאינם בהכרח אישיים מאוד, אבל אדם צופה בזה בפרטיות. בנוסף יש העברה של אמת לצד שלישי, ללא הסכמתו. הבית כמקום מוגן גם באמנות. יכול להיות גם מידע רגיש (סרטים למבוגרים). הוא הסכים להעביר לחברת גלילה את הפרטים, אבל לא הייתה הסכמה להעביר לצד ג. למעשה גלילה היא מאגר מידע המחויבת בהגנה מפני העברה לצד שלישי.

ג. פגיעה בפרטיות עלולה להוביל לשלטון טוטליטארי שבו הרשויות מרכזות מידע רב על הפרט. בעצם צריך להסביר למה חשוב להגן על הפרטיות של אהרון, 10 סיבות של חשיבות ההגנה על הפרטיות, ליישם את הסיבות גם בהקשר של החברה הפרטית "בואו נצפה" וגם בהקשר של הרשויות.

ד. השאלה דורשת חשיבה ביקורתית, הפעלת המוח באופן עצמאי. לחשוב על הדין הקיים במהלך השיעורים, לרשום הערות בצד ולהכניס גם לסיכומים לקראת הבחינה.

<u>מאמר "חדירה למחשב בפריזמה הלכתית":</u>

מהפכת המחשבים מקדמת את העולם, מאפשרת להשיג מידע בקלות, להרחיב את האופקים, לאחסן מסמכים, אבל למהפכת המחשבים יש תופעת לוואי והיא תופעת המחשוב הפולשני, או כפי שנהוג לכנות אותה "סייבר". יש חדירה למחשב הזולת באמצעות תוכנה נסתרת. במשפט המערבי המענה להגנה על הפרטיות של האדם בכלל והפרטיות של האדם במערכות המחשבים, המענה הוא חדש, למעשה עד לפני 30 שנה, בתי המשפט בישראל ובעולם כולו לא הכירו בזכות לפרטיות כזכות בת הגנה במשפט. לפיכך, מפליא לגלות שבמשפט העברי יש מענה ברור ומאוזן בכל הנוגע להגנת הפרטיות. המענה הזה מקורו אלפי שנים אחורה. במהלך היחידה הזאת נראה הלכות שמתייחסות לסוגיות של פגיעה בפרטיות של האדם, פגיעה בתכתובת של האדם, שניתן ליישם אותן על כל הנוגע לסוגית המחשוב הפולשני.

חרם דרבנו גרשום- רבנו גרשום מאור הגולה חי לפני כאלף שנים, בימי הביניים. הוא נקרא מאור הגולה משום שהוא הביא אור ליהודים בעולם כולו. הוא קבע שורה ארוכה של חרמים, שורה ארוכה של כללים שמי שיפר אותם הסנקציה נגדו היא סנקציה חברתית (חרם). אחד החרמים שהוא **הטיל הוא חרם על פתיחת דבר דואר השייך לזולת**.

"חרם שלא לראות בכתב חברו ששולח לחברו בלא ידיעתו אסור, ואם זרקו מותר".

הדגש הוא הסכמה של כותב המכתב.

הגאון פלאג'י מסביר: אסור לגלות דברי האיגרת לאחרים, אפילו בסתם. שום סוד ודבר מגונה ונזק לכותב האיגרת. איסור לגלות. אסור לגלות גם אם לא מדובר במידע רגיש/חשוב.

לדעת המרצה, מבחינה תכליתית ופונקציונאלית גם המטרה וגם השימוש של הכתב האלקטרוני דומה לכתב הממשי. אימייל/אסמס וכו' הוא כמו מכתב. בכל מקרה גם האסאמס שהוא לכאורה בלתי ניתן למגע/לא מוחשי, הוא מגולם בחפץ מוחשי (מחשב/פלאפון).

רואים יישום כזה **בפרשת אפיקי מים**: היה מדובר במהנדס שעובד בחברה התובעת. יום אחד המעסיק חשד שהוא גונב סועד מסחריים מהעסק, הוא סוחר בלש פרטי והחוקר הפרטי מגלה שהוא באמת גנב, הוא מגלה שהמהנדס שולח אימיילים עם סוד מסחרי למישהו מחוץ לחברה,

למעשה המהנדס הקים חברה מתחרה באמצעות סודות המסחר במקביל לעבודתו אצל המעסיק. הוא גם זרק לפח סוד מסחרי כלשהו. בית המשפט פונה לדין העברי בשביל לדעת אם הוא עשה משהו לא בסדר, השופט ארמון מיישם את העקרונות המשפטיים העולים מהחרם, וקובע שמה שהמעסיק עשה בשני המקרים הוא שהוא הפר את שני הכללים של חרם דרבנו גרשום. יישמו את החרם גם על אימיילים וגם על האזנת סתר. הסיבות הנורמטיביות למה לא להעביר משהו שאי כתב לב'.חרם דרבנו גרשום אוסר פתיחת מכתבים של אנשים אחרים, האם ההגנה על הפרטיות בהלכה העברית מתייחסת רק למקרים של פתיחת מכתבים של אחרים, והאם היא לא מגנה גם על קובץ/מכתב שלא תוקשר לזולת, השאלה הזאת מובילה אותנו לרמב"ם אשר מתייחס לפסוק שמופיע בתורה בספר ויקרא י"ט, הפסוק הזה אומר "לא תלך רכיל בעמך, לא תעמוד אדם רעך". הרמב"ם מפרש ואומר שרכיל זה שהוא טוען דברים והולך מזה לזה ואומר "כך וכך אמר פלוני, כך וכך שמעתי על פלוני", רכילות זה א' הולך לב' רואה מה ב' עושה והולך לג' ואסור לו להגיד לג' שהוא ראה את א' עושה משהו. הקיצור בשולחן ערוך: איזהו רכיל, זה שטוען דברים והולך מזה לזה ואומר: כך אמר פלוני, כל וכך שמעתי על פלוני. אך על פי שהוא אמת וגם אין בו גנות הרי זה עובר בלאו. הפרשנות המצמצמת יותר של הרמב"ם מדברת על כך שאסור להעביר מידע רק אם המידע עלול לגרום לסכסוכים או שפיכות דמים. הגישה המרחיבה של הרמב"ם מתייחסת גם למקרה של הפצת מרשם האוכלוסין של משרד הפנים (מדובר באדם שעבד כקבלן במשרד הפנים, הכניס דיסק און קין למחשב של משרד הפנים והפיץ את זה ברשת). הפצה של מידע סודי שעלול לגרום לשפיכות דמים וכו' זה הפצה של מרשם האוכלוסין בשואה. הגישה הצרה שמדברת על הפצה של מידע שניתן בסתר, כל מה שמאוחסן לנו במחשב זה סוג של סוד (מה שלא הפצנו). מידע ממוחשב הנמצא באתר ציבורי הוא לא סוד, כי אפשר לצאת מנק' הנחה של הסכמה מכללא. גישת הביניים הסובייקטיבית, ר' יוסף קארו(לא הספקתי לכתוב). קובץ וורד שלא פרסמת לדעת המרצה הוא סוד, לעומת זאת לדעת המרצה מה שמופיע על צג המחשב לדוגמא זה לא סוד מכיוון שזה נמצא ברשות הרבים. אבל תמיד יש מקום לדיין לכאן או לכאן. ניתן לפנות להלכה העברית על מנת לדעת אם מישהו חודר לקובץ וורד של מישהו אחר עושה משהו לא בסדר.

יש כמה בעיות עם פסוק י"ט מספר ויקרא:

1. האם מידע ממוחשב הנמצא במחשב/אמצעי אחסון אחר של מידע שאינו מאובטח באמצעי טכנולוגי הוא בבחינת סוד, כלומר, דבר שאדם מעלימו מאחרים? מנגד - יש הרואים בסוד רק דבר מאובטח וחתום. הגנת הפרטיות היא הגנה על דברים סתומים וחתומים, זו גישה צרה. בשביל שכתב על פי ספר מנורת המאור יהיה משהו שאסור לגשת **<u>אליו צריך 2 דברים:</u>** 1. היעדר הסכמה 2. שיהיה חתום וסתום. על פי גישה זו רק הצפנה של מידע הופכת אותו לסוד, ברם הבעייתיות עם הגישה הזאת שהיא איננה מגנה על החלשים טכנולוגית. בנוסף, היא איננה מגנה מפני אנשים שקיבלו את הקוד הסודי, למשל **בפרשת נתן אשל** שהיה עובד בלשכת ראש הממשלה, הוא מסר את הפלאפון החכם שלו לסמנכ"ל משרד ראש הממשלה, על מנת שידאג לתיקון הפלאפון, לצורך התיקון מר אשל נתן את הסיסמא לפלאפון, הסמנכ"ל השתמש בקוד הסודי בשביל לבדוק את הקבצים של התמונות שיש בפלאפון. הביקורת של המרצה היא שהגישה הצרה הזאת אינה מגנה מפני אנשים שקיבלו את הקוד הסודי. עוד ביקורת היא שהגישה הצרה הזאת היא עלולה להוביל

למדרון חלקלק שבו בתי המשפט יגיד שלמרות שהמחשב מוגן בקוד, הקוד לא מספיק חזק. עדיין מנסים להבין האם מותר לחדור למחשב של מישהו ומתי זה יהיה אסור. הרמב"ם אומר שאיסור רכילות זה איסור של הפצת מידע, אבל ההצדקות שהוא מביא לאיסור הפצת מידע הן דרמטיות: "מחריב את העולם וגורם להרוג נפשות רמת מישראל, לכן נסמך 'לא תעמוד על דם רעך'. צא ולמד מה אירע לדואג האדומי", בעקבות הפצת המידע של דואג האדומים על כך שהכהן הגדול עזר לדוד המלך במשכן בנוב שאול המלך כל כך התרגז שהרג את כל הכהנים חוץ מכהן אחד. האם פגיעה בפרטיות יכולה לגרום להרוג נפשות רבות גם בימנו? בסין ספקית שירות אינטרנט נתנה לממשל את כתובת האינטרנט (IP) של מישהו ששלח מכתב והממשל גילה שאותו סיני שלח דיווח לאתר אינטרנט בארה"ב על מה שהתרחש בוועידת המפלגה הקומוניסטית בסין ובהסתמך על הדיווח הזה הכניסו אותו לכלא ל20 שנה, אולי לא נשפך פה דם אבל בהחלט נפגעה החירות של אנשים. לדעת המרצה גם בימנו אי הגנה מספקת על המידע יכולה להוביל לשפיכות דמים.

איסור רכילות כאיסור חדירה למידע:

שלוש גישות פרשניות-

1. יש איסור לבקש ולחפש מסתוריו של חברו, ומה לי לא תלך רכיל לאחרים או לעצמי. א' מגלה סוד לג', הרב חגיזכמו שאסור לג' לגלות סוד לד' (סוד של א') אסור לג' לגלות את הסוד לעצמו כי א' לא מסכים. לא תלך רכיל לעצמו ולאחרים. יש הנחה שהמידע במכתב הוא סוד, ההסתרה היא מאוד רחבה (כל מה שבתוך המכתב הוא סוד) והאיסור רכילות מתייחס לכך שאסור לגלות סוד של א' לצד שלישי, ואסור לגלות סוד של א' לעצמו (להאקר/חודר) בדיוק באותה צורה. בהסתמך על התשובה של הרב חגיז, בימנו הרב חגי כהן גרוס אסר להשתמש במכשיר האזנת סתר לשיחות טלפון של הזולת, שכן שיחת הטלפון בין א' לב' היא סוד ואסור לג' להפיץ את אותו סוד לעצמו. את התפיסה הזאת ניתן ליישם על דיני המחשבים ולומר שכאשר א' כותב קובץ וורד במחשב של עצמו זהו סוד, ואת הסוד הזה אסור להאקר לגלות לעצמו.
2. פרשנות על דרך ההיקש - מספר מקומות בתנ"ך שמופיע המונח רכילות: "הולך רכיל מגלה סוד" משלי יא 13. "סוד אחר אל תגל" משלי כה 9 "גולה סוד הולך רכיל" משלי כ 19.

איסור רכילות מתייחס לגילוי סוד, את הפועל גילוי ניתן לפרש ב2 דרכים: 1. הפצה ברבים. דואג האדומים גילה לשאול המלך מה קרה במשכן (גילה זה הפצה של המידע לזולת). 2. המשמעות השנייה של הפועל גילה, גילה זה גם לגלות איזשהו משהו שהתחבא, גילוי של משהו. בהקשר הזה גילה זה לחשוף דבר מוסתר, להסיר את הכיסוי.

האקר שחודר למחשב מגלה קודם כל מה יש במחשב, מגלה את עבודת הסמינריון ואחר כך הוא יכול להפיץ את העבודה ובכך הוא מגלה לעולם.

איסור רכילות פירושו איסור גילוי סודות, איסור גילוי סודות פירושו לא רק איסור לגלות את הסוד לצד שלישי, אלא גם פירושו איסור לתור אחרי הסוד של הזולת.

3. איסור רכילות כאיסור ריגול וחיפוש- בעברית כ' וג' מתחלפות, לכן איסור רכילות זה איסור רגילות. אסור לרכל זה אסור לרגל. לפי גישה זו איסור הרכילות מתייחס למי שעושה חיפוש במרחבו של הזולת, מי שמרגל, למשל מי שחודר למחשב של הזולת.

אם כך חרם דרבנו גרשום זה רק מקרה אחד שהוא חלק מאיסור רחב יותר, והאיסור הוא איסור כניסה למחשב/מיילים וכו' של הזולת ללא הסכמתו. על איסור רכילות אין סנקציה. הוא איסור נורמטיבי (מוסרי) שממנו נבע החרם. לאיסור הזה יש חריג מאוד גדול הרמב"ם מסביר שכל היכול להציל ולא הציל עובר על לא תעמוד על דם רעך. אדם רואה מישהו טובע בים או לסטים באים עליו ולא יכול להצילו הוא בעצמו שישכור אחרים. הכלל הוא שחייבים להציל, לא תעמוד על דם רעך כלומר צריך להציל לא רק את האדם הפיזי (קדושת החיים) אלא דם מפורש בצורה מאוד רחבה, גם בתור המילה דמים (כסף). לגבי הפגיעה בפרטיות, כל הפרשנים מסבירים כי הקרבה בין לא תלך רכיל ללא תעמוד על דם רעך, הופכת את לא תעמוד על דם רעך לחריג. מותר להפיץ מידע על זולת על מנת למנוע נזק לזולת. ספר התשובות אומר: לפיכך נסמך לא תלך רכיל בעמך ל- לא תעמוד על דם רעך, שפעמים שחייבים להודיע מום וכו' בשידוכין, שאלת שאם לא כן, עוברים על "לא תעמוד".

עקרון הסודיות בהלכה איננו חזות הכול, יש לאזנו מול אינטרסים וצרכים מנוגדים. כך גם בדיני מחשבים. בפרשת אילן כהן היה מדובר באדם נכה שיצא עם רכבו ביום קפוא ולא שב לביתו עד השעות הקטנות של הלילה. משפחתו של אילן פנתה לחברת איתורן וביקשה ממנה למסור מידע על היכן נמצא הרכב. החברה הגנה על פרטיותו של אילן כהן וסירבה למסור את המידע. הרכב של אילן כהן נתקע על פסי רכבת, ניסה לצאת מהרכב נפל וקפא למוות. הסיפור ממחיש עד כמה הגנה על הפרטיות יכולה להוביל לשפיכות דמים ומתי צריך לאזן. גם על הסייג של לא תעמוד על דם רעך.

א הוא סוחר בטורקיה יש לו מכתב שהוא אמר שהוא סודי, א נתן לב את המכתב על מנת שיעביר אותו לג'. ב פונה לרב חיים פאלג'י ואומר שהוא חושש שיש במכתב הוראות ל-ב על מנת שיעשה לג' משהו רע. גם א וגם ב הם גויים ולא תלך רכיל זה רק ליהודים. הרב אוסר עליו לפתוח את המכתב, אומר שמקור האיסור הוא לא בחרם אלא בלא תלך רכיל בעמך אבל שבמקרה זה יש חשש לנזק, בכל מקרה כזה יש לפנות לבית דין לקבל היתר לפתוח. במקרה דנן התיקון בכדי להציל את עצמו להיות מציל מידם, התיקון הוא פורר וזורה לרוח או מטיל לים. הוא משמיד את המכתב. לא תמיד חייבים להגיע למצבי הקיצון (צריך לקבל צו שיפוטי גם על מנת להרוס את המכתב). בפרשת אפיקי מים דובר על מקרה של נזקים (המהנדס גנב סודות פגע בדמים של המעסיק), בית המשפט לא מתיר לקחת את מה שנזרק. במקרה אז היה מצב של לא תעמוד על דם רעך, הבלש היה יכול לצלם באותו הרגע כי לא היה לו זמן לגשת לערכאה לקבל אישור (זה לדעת המרצה). פרשת איסקוב דובר באישה שעבדה אצל המעסיק, ביום השני הוא מפטר אותה וביום השלישי היא מגלה שהיא בהריון וביום הרביעי היא תובעת שהוא פיטר אותה בגלל ההיריון, הוא אומר שהוא פיטר לפני שהוא והיא ידעו שהם בהריון. הוא רצה להביא מכתב כראיה שהוא מצא שהיא חיפשה ראיון לאותו יום שהוא פיטר אותה. ביהמ"ש לא מוכן לקבל את המכתב כראיה בגלל הפרטיות.

מאז ומעולם המידע הוא בעל משאב חשוב. בעידן המחשב ערכו של המידע הוא אף בעל ערך רב יותר, זאת בשל היותו ניתן להעתקה/שינוי/הפצה מהירים וזולים. התעצמותם של פיתוחים טכנולוגים שונים המאפשרים הסגת גבול לא מוחשית (האקר פורץ למחשב ממרחק) לגבולו

הממוחשב של היחיד, הותירה במידה רבה את דלת אמותיו של היחיד פרוצות לכל. להלכה היהודית יש מקום רב בבואנו לבחון את הדין הראוי בכל הנוגע לפרטיות, הן מהפן הפרשני (פירוש הדין הקיים) והן מהפן הפילוסופי מוסרי. היופי שבהלכה העברית בעניין הזה היא שהלכה להגן על הפרטיות לפני הרבה שנים עוד לפני עידן המחשב וההתפתחות הטכנולוגית, והמענה שההלכה נותנת הוא גאוני ומאוזן, מצד אחד מגנה על האינטרס של היחיד לפרטיות אבל מצד שני מגנה על קדושת החיים ואינטרסים כלכלים. לכן ראוי ללמוד מההלכה העברית ולעשות בה שימוש.

שאלה לדוגמא:

לא' יש קובץ וורד בפלאפון החכם. ב' מצליח לנחש את הסיסמא הקלה של הפלאפון ופותח את הפלאפון, קורא את קובץ הוורד ואת האסאמאס שא' שלח לג' ובו הוא כותב שבכוונתו להתאבד.

על פי ההלכה העברית:

1. אין להלכה העברית נפקות שכן ההלכה העברית אינה רלוונטית לימים כיום.
2. על פי הרמב"ם איסור רכילות רלוונטי רק להפצת מידע (פלוני עשה כך וכך) ולפיכך אין להלכה העברית רלוונטיות לכניסה לקובץ וורד על פי כל הפרשנים
3. בפתיחת קובץ הוורד אין משום איסור רכילות או גילוי סוד שכן לא מדובר בכתב חתום וסגור (מנורת המאור).
4. מדובר בקובץ סגור על ידי סיסמא שאסור לפתוח אותו (סוד אחר אל תגלה גם לעצמו- הרב חגיז).
5. איסור לא תעמוד על דם רעך מצדיק את קריאת האסמס, אבל לא את פתיחת קובץ הוורד (לא תלך רכיל לאחרים ולעצמו).

6. תשובות 4 ו5 נכונות.

הפגיעה בחופש הביטוי

למה צריך להגן על חופש הביטוי?

סעיף 19 להכרזת האו"ם האוניברסאלית על זכויות האדם מגן על חופש הביטוי, הוא כולל בחופש הביטוי גם את הזכות לקבל מידע, "חופש המידע".

הכותב ג'ון סטיוארט מיל כתב ספר על החירות. הנימוקים שהוא מביא בספרו הם נימוקים תועלתניים (זכויות האדם יביאו תועלת לכלל). מי שפיתח את התיאוריה התועלתנית הוא בנטהאם ובעקבותיו נכתב הספר.

אחת הסיבות שג'ון סטיוארט מונה לצורך בהגנה על חופש הביטוי היא:

* **<u>ההפסד שבהשתקת האמת והדעה הנכונה – מגוון דעות:</u>** לאנשים קשה לקבל דעה שהיא שונה משלהם. למשל, פיתגורס חי בקומונה עם עוד מתמטיקאית שחיה איתו בקומונה והיא פיתחה תפיסה מתמטית חדשנית לחלוטין. פיתגורס אמר לחבריו בקומונה לזרוק אותה לנהר ולהטביע אותה. קשה לאנשים לקבל דעה חדשנית ושונה משלהם.

ג'ון סטיוארט מיל קורא לזה **"עריצות הדעה הציבורית והעריצות המדינית".** השלטון הוא עריץ, קשה לו לשמוע ביקורות ולקבל דעות שונות.

ג'ון סטיוארט אומר – תתנו לאנשים לבטא את עצמם משום שאולי הם צודקים, אולי הם אלה המחזיקים בדעה הנכונה. גם לאנשים חכמים קשה מאוד להשיג את האמת ולהבין אותה, ולכן, הם צריכים להיות פתוחים לקבל פרשנות חדשה, ביקורת, וטענות נוגדות שונות.

"השתקת דעה גורמת רעה מיוחדת במינה שעל ידי כך מקפחים את המין האנושי כולו, לא רק את הדור הקיים, אלא גם את הדורות שיבואו. ולא רק במחזיקים באותו הדעה, אלא גם במי שכופר באותו דעה(מתנגד לה)... כי אם הדעה נכונה אז שוללים מהציבור בכללותו להחליף טעות באמת. ואם הדעה מוטעית – כי אז שוללים מהם טובת הנאה השקולה כמעט כנגד זו, והיא הכרת אמת בהירה יותר ותפיסת אמת ערה יותר הנובעת מתוך התנגשות האמת בטעות".

יש שתי דרכים להגיע לאמת: 1. על ידי דיבור 2. על ידי שמיעה.

סיבה ראשונה: גילוי האמת.

בזמננו, אומר פרופ' קאן – אם נפגע יתר על המידה חופש הביטוי ונפגע גם בדברים שהם לא פופולאריים, אז אנשים יחששו מלחשוב, מלהרהר, מלהתנסות בדברים בגלל עריצות דעת הרוב והתוצאה תהיה קו מחשבה שהוא לא מקורי. כולם יחשבו את אותו הדבר כי הם יפחדו ממה שיגידו להם.

אם כך, השתקה של דעה לא מקובלת פוגעת בחקר האמת, בפיתוח האמת ובמחשבה.

<u>סיבה שנייה: רווחה אישית של הפרט.</u>

ג'ון סטיוארט מיל רוצה להביא תועלת גם לחברה וגם לפרט. כי אם אנשים יוכלו לדבר, תהיה

חברה של אנשים מאושרים וכך תהיה רווחה מצרפית בחברה(״מקסימום אושר״). ג׳ון סטיוארט מיל אומר שהתפתחותה החופשית של האישיות היא אחת מסודות האושר ההכרחיים ולצורך התפתחותה נדרשים לה חופש דעה וחופש הבעה.
בספרו של ווסטין הוא כותב שקיים צורך אישי וחברתי בתקשורת. אנשים צריכים לדבר אחד עם השני כי זה הצורך האנושי שלהם. ולכן אנחנו צריכים להגן על חופש הביטוי של האנשים בכדי שיוכלו להגיד את מה שמפריע להם ללא חשש...

<u>סיבה שלישית: הביטוי כסוג של יצירה אישית (טעם הומניסטי).</u>
יש תפיסה הומניסטית שאומרת שלכל אדם יש זכויות אדם מכוח היותו אדם ולא מתוך כך שזה עוזר לרווחה המצרפית בחברה. לבן אנוש יש זכות לחופש ביטוי כי הוא בן אנוש. התפיסה ההומניסטית שבאה להצדיק את חופש הביטוי אומרת שני דברים:
1. הביטוי של האדם הוא סוג של קניין שלו. אם אני כותבת טור דעה, טור הדעה הזה הוא הקניין שלי, ולכן לא יכול להיות שיבוא מישהו ולא ייתן לי לתלות את טור הדעה בלוח מודעות כי הוא שלי! ואני מחליטה מה לעשות איתו.
פרייד אומר – ״הביטוי החופשי של האדם הוא פועל יוצא מהזכות לאוטונומיה של הפרט״, הזכות להחליט מה אנחנו עושים במהלך חיינו ולבחור החלטות שונות.

<u>הסיבה הרביעית: החשש משלטונות טוטליטריים.</u>
בשלטון טוטליטרי, בשלטון עריץ יש פגיעה בחופש הביטוי משום שהשלטון אינו מעוניין בביקורת של נתינים. בשלטון מסוג זה לא נותנים מקום לביקורת, ואנחנו חוששים גם משלטון עריץ של ״חברת המידע״.

מתי יוגבל חופש הביטוי?
ג׳ון סטיוארט מיל עומד על כך שאנחנו לא נפגע בחופש הביטוי בשביל להגן על הפרט שמתבטא אלא רק לצורך הגנה עצמית.
העיקרון היחיד שעל פיו צריכה חברה להתנהג עם היחיד בענייני כפייה ופיקוח הוא הגנה עצמית ולא טובתו של הפרט. אנחנו נשתיק מישהו לצורך הגנה עצמית - חברתית מהסיבה של ״שלום הציבור״ ופגיעה בציבור למשל.

בפרשת כל העם - בית המשפט העליון אמר שהפגיעה בחופש הביטוי תהיה רק אם יש ״וודאות קרובה״ לפגיעה בשלום הציבור.

מה הקשר בין חופש הביטוי לבין מחשוב פולשני?

אחת מהפונקציות החשובות ביותר של המחשב היא היותו כלי תקשורת המוני או פרטי המאפשר לנו גישה למאגרי מידע והכול ללא עלות, במהירות ובצורה בת קיימא.
עוד מאפיין הוא שהרשת איננה כפופה למנגנוני רישוי.

הדרכים שבהם מחשוב פולשני עלול להוביל לפגיעה בחופש הביטוי:

1. חדירה למחשב וצ'ילינג אפקט:

צ'ילינג אפקט זה תופעת הצינון והתפיסה היא שחדירה למחשב, למרות שהיא לא פוגעת בחירות הביטוי באופן ישיר, בעקיפין, היא גורמת לצנזורה עצמית ולתופעת הצינון.
סנאטור מקרת'י יצר רשימות שחורות של אנשים שחשודים בפעילות קומוניסטית. אותם אנשים שהוכנסו לרשימות השחורות הללו, אנשים אחרים התחילו להחרים אותם, להתעלם מהם, לפטר אותם מהמשרות שלהם. אחד האנשים שעזר לפתח את פצצת האטום בארה"ב, ברגע שהשם שלו נכנס לרשימה השחורה, לא שיתפו אותו בכלום.
בעתירה לבית המשפט העליון בארה"ב עלתה הטענה שהרשימות השחורות האלו פוגעות בחופש ההתאגדות ובחופש הביטוי של האזרחים. ובית המשפט קיבל את הטענה הזאת וקבע שהרשימות השחורות הן לא חוקתיות.
בית המשפט העליון אסר על קיומן של הרשימות השחורות שכן הן פוגעות בפעילות פוליטית חוקית ושוחרת שלום. התפיסה היא שאדם לא יירשם למפלגה הקומוניסטית שכן הוא מפחד שהשם שלו יכנס לרשימות השחורות אפילו שהחברות במפלגה הקומוניסטית היא חוקית.

פרייד אומר – "אם נדע שכל פעולותינו נרשמות וכי כל מה שנעשה או נאמר יוודע לכולם, הדבר עלול להשפיע על פעולות שננקוט". לכן, אם אני אדע שחברת נטפליקס תעביר את המידע (במה שאני צופה) לצד שלישי, זה יגרום לי לצנזורה עצמית (אפילו שמותר לי לראות את כל מה שאני רוצה בשרת).
הצ'ילינג אפקט הוא תועלתני.

סקר מלפני 10 שנים הוכיח ש78% מהגולשים באינטרנט היו מגבירים את השימוש שלהם אם מדיניותם של אתרים בסוגיית הפרטיות הייתה נחשפת לפני כן. כלומר, אנשים מפחיתים את השימוש ברשת בגלל החשש שהרשת היא לא מוגנת כמו שצריך.

כיום, למרות שאנחנו יודעים שיש עוגיות, אנחנו מקבלים את זה על עצמנו.

<u>צ'ילינג אפקט וקוקיז:</u>

צריך לעשות הבחנה בין "צפייה אקראית"(במקרה) לבין "מעקב". הסכנה במעקב היא שזה יגרום לצנזור עצמי ולפגיעה בכבוד האדם. בעולם האמיתי, כאשר אנשים מסתכלים על אנשים אחרים זה נורמטיבי. אבל כאשר המעקב הוא פרטני, זה מוביל ל"צנזורה עצמית" שיכולים למנוע מהאדם מלבצע פעולות כלשהן...

במרחב הסיברקינטי(באינטרנט), איסוף המידע הוא סוג של מעקב בלא צפייה אקראית וזה גורם לצ׳ילינג אפקט כי אנשים יחששו מלעסוק בפעילות שהיא לא פופולארית או שהיא לא בזרם המרכזי של ההתנהגות.

צ׳ילינג אפקט ומעקב תעבורתי:

מעקב תעבורתי: בודקים לאן הלכנו, למי כתבנו, באיזה שעה, ממי קיבלנו מיילים ובאיזה שעה... גם מעקב תעבורתי יכול להוביל לצ׳ילינג אפקט.

לפי תופעת הצינון – אנחנו נחשוש להתכתב עם גורמים מסוימים או לגלוש באתרים מסוימים אם נדע שיש מעקב על נתוני האיכון שלנו. זה יפגע גם בצורה עקיפה בזכות שלנו לא רק להתבטא, אלא גם להתאגד. סולובה אומר שמעקב פוגע בחופש הביטוי ובחופש ההתאגדות, הוא פוגע בפעילות רגילה ולגיטימית של האנשים.

2. רגולציה(אסדרה) עצמית של תכנים:

הרגולציה גורמת לפגיעה בחופש הביטוי. למשל: מצב בו מנהל פורום מצנזר תוכן של תגובות וכך מונע מאנשים מלהביע את דעתם. כך למשל קרה בפרשת ״בורוכוב״. הצנזורה הזו יכולה להיעשות מכל מיני שיקולים.

יכול להיות גם רגולציה של תכנים במקרים שבהם אנשים רוכשים אתר של מישהו אחר בכדי לסנן את המידע שלו, או למשל בגוגל: הם רצו לקדם אתרים ששילמו להם אז הם שמו את האתרים בראש רשימת החיפוש, ואת האתרים שלא שילמו להם בתחתית הרשימה במנוע החיפוש.

על מנת לקבל רישיון לפעול בסין, גוגל הסכימה לצנזר את תוצאות החיפוש באתר הסיני וכך לא יתגלו כל האתרים. בדומה, מיקרוסופט מחקה מהאינדקסים של האתרים שלה דעות שלא מצאו חן בשלטון הסיני.

בארץ נעשתה פניה לחברת גוגל מטעם הנהלת בתי המשפט והנהלת בתי המשפט ביקשה מחברת גוגל שלא לאפשר גישה לאחד האתרים בארץ ״למען עתיד ילדינו״ שכן הוא ביקר את מערכת המשפט בישראל ללא צו. גוגל סירבה לכך.

3. מחשוב פולשני המונע גישה לאתרים:

יכולה להיות התקפה על אתר אינטרנט מסוים כדי שהוא לא יוכל לפרסם את המידע שיש לו. זאת אומרת, מניעה גישה טכנולוגית לאתר אינטרנט בכדי למנוע את פעילותו. מניעת הגישה הזו יכולה להיעשות על ידי האקרים\ע״י ארגונים או על ידי השלטון. למשל, ארגון ״אנונימוס״ פגע באתרי אינטרנט בארץ. האקרים פגעו באתרי אינטרנט מסוימים. במצריים, השלטון השבית את הרשת ואת היכולת לשלוח מסרונים כדי שלא תהיינה התקוממויות כנגד השלטון. ובסין, נמנעה הגישה של גולשי גוגל לאתר ״גוגל״.

4. צווי חיפוש, צווי הסרה, וצווים שיפוטיים:

גם צווים שונים מסוג זה יכולים לפגוע בחופש הביטוי של אנשים ברשת. למשל, אתר אינטרנט שמכר מזכרות נאציות קיבל צו מניעה מביהמ״ש מלמכור את המזכרות הנאציות.

הממשל בסין דרש מחברת ״יאהוו״ למסור את פרטי המייל של עיתונאי סיני שדיווח על פילוג של

המפלגה הקומוניסטי.
במחשוב הפולשני יכול להיעשות ברשות ע"י הרשויות בעזרת צווים משפטיים\צווי חיפוש.
על פי מסמכים שפרסם סנואודן - לממשל האמריקאי יש גישה לכל המידע שמוחזק על ידי גוגל ועל ידי גורמים אחרים במחשוב בענן.
בפרשת **רמי מור**, היה מקרה של אדם, מטפל הוליסטי, שעתר לבית המשפט וביקש לקבל צו לחשוף את כתובת האיי פי על מישהו שפרסם עליו ברשתות דברים מכוערים ברשת ודברי שקר. בית המשפט העליון בעמדת רוב קבע שחשיפת כתובת האיי פי של הגולש תפגע בחופש הביטוי שלו. השופט ריבלין אמר שברירת המחדל היא שאין אפשרות ליתן סעד של חשיפה בשיטת המשפט המקובל. אין סמכות לבית המשפט לתת צו שיורה לחשוף את כתובת האיי פי. יש חוק בארץ המאפשר לקבל כתובת איי פי (בתקנות סדר הדין האזרחי יש אפשרות לאשר חיפוש במחשבים).
דוגמא נוספת היא פסיקה חדשנית של **בית המשפט האירופי** – ("הזכות להישכח"):
בפס"ד גוגל ספיין: בפרשה זו היה מדובר באדם שהיה חייב כסף לביטוח לאומי בספרד. מכרו את רכושו בכדי לפרוע את חובו לביטוח הלאומי והדבר פורסם באתר אינטרנט של עיתון כלשהו. לאחר 10 שנים, אותו אדם פנה לעיתון ואמר שעדיין כל מי שכותב את שמו ברשת הוא רואה שיש לו חוב לביטוח הלאומי, והוא ביקש להישכח ושלא יזכרו אותו בגלל החוב הזה, אין שום סיבה שהשם שלו יופיע כבעל חוב כי החוב שלו נפרע.
בית המשפט אמר שלכל אדם יש זכות להישכח ואפשר למחוק את המידע מהרשת. כלומר, בהינתן שחלף זמן רב – אפשר למחוק מידע מסוג זה.
The right to be forgotten.
אנחנו רואים פה שבית המשפט התערב במה שקורה ברשת בשביל לשמור על שמו הטוב של האדם.
אולם **בפרשת רינו** קרה מקרה הפוך. בית המשפט סירב להתערב במה שקרה ברשת. היה מדובר בחוק פדראלי שאסר פרסום פורנוגראפי ברשת מהחשש שילדים קטנים יכולים להיחשף למידע הזה ולהיפגע ממנו. בית המשפט קבע שחוק כזה יפגע בחופש הביטוי הפורנוגראפי וחופש הביטוי הרשת הוא בעל מעמד מאוד גבוה, כמדיניות, יש להעניק חופש הביטוי באינטרנט את ההגנה המקסימאלית מהתערבות ממשלתית יותר מאשר לרדיו ולטלוויזיה. כל המאפיין של הרשת שלה זה הברדק, הכאוס, הבלגן.
בית המשפט העליון פסל את החוק שאוסר על אתרים פורנוגראפיים ברשת בהיותו "לא פרופורציונאלי" כי הוא עלול להוביל לאפקט המסנן שבמסגרתו יירתעו אנשים מביטוי מוגן.
מקרה דומה היה **בפרשת שס נ' פינס**, היה מדובר בפרסומים ברשת לפני תקופת הבחירות לכנסת. החוק אמר שאסור לפרסם פרסומים מסוג זה לפני בחירות. מפלגת ש"ס עתרה כנגד המערך לכנסת ואמרה שאסור לפרסם ברשת לפני בחירות. מפלגת פינס(המפרסמת ברשת) טענה מנגד שהחוק לא אוסר פרסום באינטרנט ויש לפרש את החוק בצמצום. השופט חשין קבע שמפאת חשיבות עיקרון חופש הביטוי אין להרחיב את לשון החוק שעה שבאים לצמצם את חופש הביטוי ושלא נאסרה תעמולת בחירות בכנסת.

בפרשת רמי מור נאמר שהרשת היא כיכר העיר החדשה שהכול שותפים לה ושהמרחב הווירטואלי מצוי בכל. הרשת היא אמצעי דמוקרטי מובהק המקדם את עיקרון השוויון ומציב מחסום מפני התערבות שלטונית. לכן, במישור החוקתי כשאדם מבקש לשמור על האנונימיות שלו עומדות בפניו שני זכויות חשובות:
1. חופש הביטוי 2. הזכות לפרטיות

לטענת המרצה, **תקנה 387(ה) - "חיפוש בחומר מחשב"**, כן מאפשרת להוציא צו שיורה לחשוף כתובת איי פי.

5. רגולציה חקיקתית:
חוק התקשורת קובע שאסור לחברות הפועלות בשוק הסלולר להתערב בתוכן של המידע הרץ בסלולר. ההתייחסות אליו תהיה כאל צינור העברה ותו לא, וזה נקרא במילים אחרות "הניטרליות של הרשת". בניגוד לכך שיש אסדרה עצמית של אתרים, בכל הנוגע לשוק הסלולר(אבל לא לרשת בכלל), יש התערבות חקיקתית שנועדה להגן על חופש הביטוי ברשת ולשמור על עיקרון הניטרליות של הרשת.
בסין יש איסור על תשתית אינטרנט חיצונית. בארץ ובמדינות אחרות יש צנזורה ביטחונית ברשת. בארץ יש את החוק של הגנה על הציבור מפני עבירות מין וסעיף 13 מגביל את השימוש של עבריין מין באינטרנט.
דרך אחרת לרגולציה חקיקתית היא צנזורה על תכנים. למשל: איסור קיום תעמולת בחירות, מניעת שידור פורנוגרפיה(פס"ד רינו).

האם יש מקום להגביל גם את הפרסומות ברשת?
דוגמא להתערבות שלטונית ברשת הוא חוק התקשורת(בזק ושדורים) סעיף 51ג. קובע איסור על גורמים הפועלים בשוק הסלולר לחסום תכנים ברשת.
חוק התקשורת אוסר התערבות ברשת לבצע הגבלות או חסימות שונות כדי לשמור על עיקרון הניטרליות של הרשת.

האם נחייב חברות אחרות לשמור על הניטרליות של הרשת? (למשל, פייסבוק\גוגל), איפה האיזון?
– כיום יש הצעת חוק לתיקון נוסף בחוק התקשורת המבקש להרחיב את הכלל הזה על כל הגורמים שפועלים בתקשורת ולא רק על חברות הסלולר.
החל ממאי 2018 תכנס לתוקף מבחינה חוקתית "הזכות להישכח" והיא תהיה קבועה **בחוק האירופי.**

EU GENRAL DATA PROTECTION REGOLATION בסעיף 71 -
הזכות להישכח – מידע צריך להימחק ללא דיחוי אם הוא כבר לא נדרש ואם ההסכמה לפרסומו נלקחה וזו למעשה קודיפיקציה של פס"ד גוגל ספיין.

שאלה לדוגמא:

אם נדע כי כל פעולותינו נרשמות וכי כל מה שנאמר או נעשה יוודע לכולם הדבר עלול להשפיע על פעולות שננקוט. הסבירו את כוונתו של פרייד ויישמו את הדברים על כל הנוגע לדיני סייבר. הביאו גם דוגמאות מהפסיקה ומספרים.

יש לציין את פס"ד רינו + סולובה וקאנג

הזכות לקניין שנפגעת כתוצאה ממחשוב פולשני:

כאשר מבוצעת חדירה למחשב של הזולת, יש פגיעה בזכות לקניין של בעל המחשב. בהקשר זה, הזכות לקניין נחלקת לשני פנים:

1. הזכות **לקניין המוחשי** במחשב הפיזי שלו
2. הזכות **לקניין הערטילאי.**

לפעמים התמונה היא יותר מורכבת. למשל, אדם שנמצא במחשב של המעסיק שלו ומעביר את המידע ששייך למעסיק לחזקתו של צד שלישי.
למי יש בעלות, ובאיזה קניין?

הזכות לקניין מוחשי עוגנה מקדמת דנא על ידי המשפט. בכל משפט כמעט תהיה הגנה על קניין מפני גניבה וכו'. לעומת זאת, ההגנה על הזכות לקניין הערטילאי היא חדשה ביותר במשפט המערבי והיא פועל יוצא של צורך שנבע מהתפתחויות טכנולוגיות ופחות פועל יוצא של תפיסה פילוסופית-מוסרית.

* הגורמים להתפתחות ההגנה המשפטית על הקניין הרוחני:

אפשר לעמוד על ההתפתחות הטכנולוגית, כלומר התפתחות הנייר והדפוס.
עד לפני כ500 שנה הנייר היה מאוד יקר ורק בשנת 1400 לערך, התפתח תיעוש של הנייר והנייר הפך ליותר זמין. מאוחר יותר התפתח גם הדפוס שאפשר לשכפל נייר מודפס בכמויות גדולות.
בעקבות התפתחות הדפוס והנייר נוצר מצב קשה:
בהתחלה התפתח העיתון אבל אז באו אנשים שהעתיקו את מה שכתב X על העיתון, שכפלו אותו, הדפיסו אותו מחדש, ו Y מכר את העיתון החדש. לא הייתה ליוצר המודעה בעיתון הגנה מכיוון שהייתה הגנה רק על הקניין המוחשי.
נעשתה פניה למלכת אנגליה וביקשו ממנה להגן על העיתונאים המקוריים ומלכת אנגליה הוציאה פריבילגיות למוציאים לאור שאסרו על העתקת העיתונים שלהם.
מאוחר יותר החלו גם התפתחויות חברתיות שהובילו להגנה על הקניין הערטילאי אבל רק מאות שנים לאחר מכן.

הוגה דעה בשם ג'ון לוק אמר שלכל אדם יש זכות לחירות וזכות לקניין בלי קשר לעובדה שהמלך או השלטון מעניק לו את הזכויות הללו. לכל אדם יש זכות לקניין מטבע בריאותו.

לדעתו של ג׳ון לוק, הזכות לקניין המוחשי נוצרת מהעבודה של האדם ← ״תיאוריית העבודה״.
העבודה של האדם היא זו שיצרה את הזכות שלו בקניין.

מאות שנים לאחר תיאוריית העבודה בא הוגה דעה אחר בשם וונדי גורדון שאמר שיש את תיאוריית העבודה ויש את ״תיאוריית זיעת אפיך״ ← זאת אומרת, אדם שמשקיע, מתאמץ, אוסף מידע על כל הצבעים של החולצות שאנשים לבשו במכללה ביום ראשון ומתאמץ בחשיבה שלו בשביל ליצור מאגר מידע, אז יהיה לו בעלות על הקניין הערטילאי שלו! מה ששלו שייך לו.

ג׳ון לוק נפטר. הוא קרא לזכות לחיים ולרכוש זכויות טבעיות של כל אדם המוקנות לו מבלי להיות תלוי בכוחות השלטון, זוהי למעשה תיאוריה הומניסטית.
לגבי הזכות לקניין אומר ג׳ון לוק, הואיל ולכל אדם זכות על גופו הרי שיש לו גם זכות טבעית למלאכת כפיו ולפרי עמלו.

1. תיאוריית העבודה: ג׳ון לוק.
2. תיאוריית זיעת אפיך: וונדי גורדון
3. תיאוריית התועלתנות: בנטהאם.

״תיאוריית התועלתנות״ – בנטהאם:
לפי תיאוריית התועלתנות: הקניין הפרטי נחוץ שכן הוא מועיל להשגת התכלית שהחברה מעוניינת בה והיא הבטחת רווחתו של הכלל. אנשים יהיו מאושרים יותר אם הם ידעו שהחוק מגן על הקניין שלהם. אנשים לא יהיו מאושרים בחברה שאין בה הגנה על הקניין.
התיאוריה התועלתנית קנתה חזקה בכל מה שנוגע לדיני הקניין הרוחני.
למשל – המשפט המערבי מגן על יצירה ספרותית בעלת ערך אומנותי ונותן ליוצר מונופול על היצירה מפני העתקתה. אנחנו נותנים תמריץ ליוצר של יצירה אומנותית בכך שאנחנו נותנים לו מונופול על היצירה שלו. כלומר, אף אחד לא יכול להעתיק את היצירה שלו מבלי לקבל את הסכמתו. אנחנו נותנים תמריץ כי לחברה יש אינטרס שאנשים יכתבו סיפורים, זה מקדם את החברה, את התרבות וכדומה...
תחימת המונופול: מותר להעתיק יצירה אומנותית בשימוש הוגן, ההעתקה מוגבלת בזמן. מנסים למצוא איזון לטובת החברה בכללותה.

ראינו שהזכות לקניין הערטילאי התפתחה הרבה יותר מאוחר כתוצאה מהתפתחויות טכנולוגיות (בשונה מהזכות לקניין מוחשי).
המלכה מרי נתנה בשנת 1556 פריבילגיות למדפיסים כדי שלא יבוא מישהו אחר וידפיס את מה שהם כבר ידפיסו. ב1774, **בפס״ד דונלדסון** ניתנה למחבר של יצירה אומנותית זכות להחליט אם לפרסם את יצירתו... ובחל מ1842 נחקקו במדינות המערב חוקים בתחום זכויות היוצרים, והחל מ1886 נחקקה אמנה להגנת יצירות ספרותיות.

מה היא הזכות לקניין?

ישנן הגדרות שונות לזכות לקניין. יש המגדירים את הזכות לקניין כ"זכות **לשלוט** בקניין שלנו".
יש המפרשים ומגדירים את הזכות לקניין בצורה מצומצמת יותר, "הזכות למנוע הסגות גבול".
השאלה היא – מה היא ההגדרה הראויה של הזכות לקניין ערטילאי במחשב?
ככלל, הבעלות בקניין המוחשי(כלומר בקושחה) ובמידע הממוחשב(כלומר בחומרה) נותנים לבעלים את הזכות למנוע את גניבת המחשב, למנוע הסגת גבול למידע הממוחשב, ובכלל זה, למנוע כל העתקה של המידע הממוחשב הסגור(קבצים שהם בתוך המחשב).
המידע המוגן כולל גם את הNon data information שנמצא במחשב הסגור. הזכות לקניין כוללת גם את הזכות למנוע מאחרים שימוש במשאבים ממוחשבים.

ההגדרה הרצויה של הזכות לקניין ערטילאי ממוחשב:
עצם החדירה למחשב הזולת באה לידי ביטוי כפגיעה לזכות לקניין. הפגיעה בזכות לקניין אינה פונקציה של נזק למידע והיא גם לא פונקציה של פיצוח מנגנון הגנה טכנולוגי.
זו הגדרה מאוד רחבה ולא כל כך מקובלת בקרב המלומדים בדיני המחשבים.
האם התפיסה הזאת מוצדקת או לא?
ישנם מספר טעמים הבאים להצדיק את ההגדרה הרחבה לזכות לקניין:
- עצם הבעלות בקניין המוחשי וההשקעה בקניין הערטילאי מובילה להגרה רחבה של הזכות הזאת (גישה ליברטריאנית, פס"ד מזרחי).
- הביטוי הממוחשב הוא סוג של יצירה אישית שהושקע בה מאמץ
- הקבלה בין מידע ממוחשב לבין שיחת היחיד
- המידע הממוחשב כביטוי למשאב מוחשי שניתן לגנוב(כסף, דלק).

בחברה שלנו יש נטייה יותר להגן על הקניין המוחשי. לשופטים ולמחוקקים עדיין קשה להגן על הקניין הערטילאי. בחברה המודרנית חייבים להגן על המידע בצורה רחבה.

<u>הצדקות תועלתניות לגישה המוצעת:</u>

בחברה המודרנית, שמושתת במידה רבה על מחשבים, יש אינטרס מובהק להגן על המידע הממוחשב מפני חשיפתו הלא מורשית, העתקתו ושימוש במשאביו מכמה סיבות:

- עידוד שימוש במחשב.

- רווח אישית ופסיכולוגית לבעל המידע הממוחשב

- מניעת צ'ילינג אפקט

- הערכים הממוחשבים\ערטילאיים מייצגים משאבים כלכליים ששימוש בהם כמובן כגניבה או מרמה (צדק וסדר חברתי).

הדין המוצע – מה החוק צריך להגיד בכל הנוגע לדיני מחשבים?
כדי שאנשים ישתמשו במחשב ויצרו במחשב צריך שהוא ישמש מעין דלת אמות סגורות מפני חדירה, העתקה, ופרסום לא מורשים. צריך שהדין יאסור חדירה למחשב, העתקה של המידע שמופיע בו ופרסום לא מורשה של אותו מידע.

תוכן המידע יכול להיות ברף הנמוך ביותר, לא צריך המידע הממוחשב יהיה יצירה ספרותית.
יחד עם זאת, יש לכך חריגים: החוק לא צריך לאסור הצצה בצג מחשב שנמצא במקום ציבורי, הוא לא צריך לאסור לקיחה של מידע שנזרק לפח הזבל (בניגוד לפרשת אפיקי מים).

עוד שני חריגים שנוגעים למחשב מעורב ולאתר אינטרנט:

מחשב מעורב

מחשב מעורב מתייחס למצב שהבעלות במידע שונה מהבעלות בקושחה. למשל, המידע שלנו על ביקורים אצל הרופא בקופת חולים היא שייכת לי. אבל המחשב(הקושחה) שייך לקופת החולים.
במקרים כאלה של קניין מעורב מופחתת השליטה של בעל המחשב הפיזי ושל המידע הממוחשב שנמצא בו. כל אחד משניהם, גם בעל המחשב וגם בעל המידע, השליטה הקניינית שלהם במידע פוחתת.
בפרשת איסקוב היה מדובר בעובדת שפוטרה. היא חיפשה עבודה חדשה מהמחשב של המעסיק, היא שלחה אימייל לחברת כוח אדם, נכנסה להיריון ותבעה את המעסיק שלה על כך שהוא פיטר אותה בקשר לראיון. המעסיק טען שהוא פיטר את העובדת לפני הראיון ולראיה עמדה לו הודעת האימייל שלה.
הייתה כאן התנגשות בין הבעלות הקניינית של המעסיק במחשב שלו לבין הבעלות הקניינית של איסקוב(העובדת) באימייל שלה.

למה מגנים על הקניין?
דגן מביא 4 סיבות להגנה על הקניין וכל אחת מהן מתקיימת גם על מחשבים:

1. הקניין מגלם ערך של אישיות, קל וחומר שהמחשב כי הוא קניין מכונן של הפרט.
2. במגלם ערך של פרטיות במיוחד המחשב כי יש לו מידע רגיש. יש למחשב מידע אישי, מסחרי וכו'. המחשב מקדם ערכים לא רק של פרטיות אלא גם של קונפידנציאליות (סודי), יש בו גם את הקוד לכניסה לחשבון בנק, טיוטות וכו' (דברים שהם לא בהכרח פרטיים במובן הצר של המילה).
3. הקניין מגלם גם ערכים של קהילה באמצעות יצירת תשתית ארגונית תומכת ליחסים בין אישיים ארוכי טווח. איך הקניין מגלם ערך של קהילה?
4. מגנים על הרווחה המצרפית. מביאים תועלת לא רק לפרט אלא לעולם בכלל. המחשב מקדם את החברה הוא מאפשר לחשב מהר, לעשות עסקים וכו'.

שלושה מצבי צבירה של קניין:

1. קניין פרטי
2. קניין משותף/מעורב
3. קניין ציבורי

<u>הקניין כציפייה על פי בנטהאם-</u>
בנטהאם אומר: הרעיון של הקניין בא לידי ביטוי בציפייה, מאמינים שאפשר להשיג יתרון ממה שאני הבעלים שלו בהתאים לאופי של הקניין. בנטהאם מגדיר קניין כסוג של ציפייה/אמונה שאפשר להשיג יתרון מסוים מהרכוש שבו מדובר.
הציפיות מהקניינים השונים:
הכלל הוא שהציפייה להשיג יתרון מהקניין שלנו היא בהתאם למצב הצבירה של הקניין.
דוגמאות:
קניין פרטי- עט, מכונית.
קניין משותף- חניה משותפת לבעלי הבניין, שטח משותף.
קניין ציבורי- בית קברות, חניון ציבורי, אוטובוס, מסעדה
במחשבים אותו מחשב (המידע הממוחשב) יכול להיות במצב צבירה שונה בכל רגע נתון:

- קניין פרטי - המידע הממוחשב הוא פרטי שלו
- קניין משותף - כשכותבים ביחד עם עוד אדם סיכום, הקובץ של הוורד הוא משותף. קבוצה בפייסבוק של דיני מחשבים שמשתפים שם מידע, כאשר מעלים פוסט לקבוצה אפשר לראות בזה קניין משותף עם פייסבוק, משום שלמארק צוקרברג יש גישה לזה. לתפיסת המרצה כשמשתפים בפייסבוק יש קניין משותף עם חברת פייסבוק. כשגולשים באתר של חברה מסוימת (ASOS) יש קניין משותף, חברת ASOS נכנסת לנו למחשב היא מעבירה מידע, אנחנו בחרנו להכניס אותם למחשב.
- קניין ציבורי - כאשר מעלים פוסט ציבורי.

קניין פרטי - סודיות המידע (שלא יופץ). אקסלוסיביות בגישה. שלמות פונקציונאלית.
קניין מעורב - אקסלוסיביות בגישה גם למורשה בגישה.
פרשתBREKKA - עובד שעבד בחברה,הייתה לו גישה למאגרי המידע והוא שלח לעצמו במייל את המידע (לא היה לו הסכם סודיות). לדעת המרצה הציפייה של המעסיק היא שלא ייקחו לו את הקניין הזה.
בפרשת איסקוב הציפייה של העובדת היא שלא יכנסו לה לאימיילים.
קיימת ציפייה לגיטימית שהמשתמש הפנימי יכבד את הציפייה של זולתו ולא יחרוג מהגישה שניתנה לו בין אם מפורשות ובין אם מכללא. אותו הדבר לגבי אדם שגולש באתר אינטרנט, הגולש למעשה מזמין את האתר לשלוח לו מידע אבל הציפייה היא שהגישה של האתר יוגבל.
קניין ציבורי- באתרים פתוחים שהגישה אליהם אינם כפופה לקוד וגישה אין ציפייה לאקסלוסיביות, המידע נחשף בכוונה. הציפייה היא שקהל הגולשים באתרים הללו ייחשף למידע באתר ישירות באתר ולא באתר מראה או באתר ששואב מהם את המידע.

לבעלי מחשבים יש ציפייה לגיטימית להפיק מהם רווחים, ואופייה של הציפייה והרמה שלה משתנה בהתאם למצב הצבירה של המחשב שבו מדובר. לרמת והאופי של הציפייה יש השלכה על האופן שבו אנו נגן על המחשב.

הפסול שבהשגת גבול:
* פגיעה בסדר החברת
* צדק/מוסר ("זה שלי")

בנטהאם מציין שלבסיס הפגיעה ברכוש הזולת עומד פסול מוסרי, זה הרצון האוניברסלי ליהנות בקלות ובמהירות מפרי עמלו של הזולת. כלומר, הרצון האוניברסלי הברור מאליו של כולם זה להשיג דברים בקלות ובמהירות. הרצון האנושי הוא להשיג קניין בקלות ובמהירות. בנטהאם ממשיך ואומר דיני הקניין שמרסנים את הרצון הזה מבטאים את ניצחון האנושות על עצמה. לדעת המרצה הדברים מתאימים גם לזירת הסייבר. השגת גבול היא סוג של פגיעה ברכוש הזולת, הפגיעה ברכוש הזולת יכולה להתבטא בכניסה לא מורשת למחשב, בהעתקה של המידע, בהפצה שלו, בעצם ניצב הרצון להשיג מידע ממוחשב במהירות ובלי המאמץ הכרוך, זה בעצם חמדנות.
העובדות **בפרשת ניר עזרא** – ניר עזרא קיבל סיסמאות כניסה לכרטיסי אשראי, הוא נכנס עם אחת הסיסמאות לחשבון בנק מכוון והעביר כספים מהחשבון של בעלת החשבון לחשבון של עצמו (3000 ₪). דוגמא מובהקת למקרה של חמדנות.
לדעת המרצה, הפסול המוסרי שבהשגת גבול במחשב הוא רחב יותר מחמדנות, לפעמים הוא כרוך בצרות עין, רצון להרע(סייבר טרור), הוא יכול גם לגרום לסקרנות, רכילות ומציצנות, האזנה לשיחות המתבצעות בסמוך למחשב, בנוסף עריצות ושתלטנות (לאסוף מידע פוליטי וכו').

פרשת פייסבוק וחברת קיימברידג׳ אנליטיקה- לכאורה עולה שחברת פייסבוק העבירה את המידע של הגולשים לחברת צד שלישית, ואמר לצד השלישי תלמדו את העמדות הפוליטיות של האנשים הללו ולאחר מכן תשלחו להם פרסומות ממוקדות. זה יכול לבוא מרצון לשתלטנות (להשתלט על קהל הגולשים ולהשפיע עליהם בבחירות).

בפרשת ניר עזרא בית המשפט מתייחס לביטוי בלטינית יש שני היבטים: מאלום פרויביטום- רע רק בגלל שהחוק אמר שהוא רק. מאלום אינסה- החוק רגע בגלל שהחוק כשלעצמו הוא כולל משהו רע.

לפי תפיסת המרצה חדירה למחשב (חוק שאוסר השגת גבול למחשב) הוא מאלום אינסה מגן על משהו רק כשלעצמו.

בית המשפט בפרשת ניר עזרא הש׳ רובינשטיין אומר שעבירה שאוסרת חדירה למחשב אוסרת מאלום פרויביטום, אוסר משהו לא בסדר כי החוק אומר שהוא לא בסדר.

עמדת המרצה נוגדת את עמדת בית המשפט בפרשת ניר עזרא. פרופ׳ מיגלדויטש ניסח את חוק המחשב, אמר שחדירה למחשב היא לא דבר נורא, אבל בגלל שכאשר חודרים למחשב אפשר לעשות כל מיני דברים ולכן זה לא בסדר רק כי החוק אומר שזה לא בסדר (גם גישתו היא מאלום פרויביטום).

על דיני השגת גבול לדעת המרצה להגן על המידע ובכך להגן על שלמות המידע ואקסלוסיביות הגישה אליו. אם כך הבעלות בקניין הממוחשב מתייחסת לפעמים לקניין מוחשי ולפעמים קניין ערטילאי. היא כוללת את הזכות למנוע את גניבת המחשב, את הזכות למנוע השגת גבול, את הזכות למנוע להעתיק מידע סגור (גם אם הוא לא מגיע למידע שמוגן בזכויות יוצרים), כוללת את הזכות לשלוט על האופן שבו יוצג המידע.

שאלות שנותרו פתוחות:

יש זכות לקניין, אך מתי תהיה הסגת גבול? מהו קו הגבול המשפטי שכאשר חוצים אותו החוק צריך להגיד שיש הסגת גבול למחשב. איך החוק צריך להגדיר הסגת גבול למחשב.

שלושה מצבי צבירה שונים, מתי תהיה השגת גבול לאתר פתוח? איך נגיד הסגת גבול בכל אחד ממצבי הצבירה השונים.

שאלה לדוגמא:

א׳ קנה מחשב ויש לו במחשב רק תוכנות ואפליקציות שונות. ב׳ הוא טכנאי מחשבים שהתבקש להתקין לא׳ את התוכנה שמאפשרת לתקשר מהמחשב של א׳ באימיילים. ב׳ פותח את הקובץ שבודק באיזה אתרים א׳ גלש. דונו בהיבטים הקניינים של הסוגיה.

פתרון:

מתחילים עם הערכים ולמה מגנים על הקניין, מיישמים ואומרים שהערך שנפגע הוא הפרטיות ומגנים עליו. א׳ הוא הבעלים. קניין מוחשי, היבט תועלתני והיבט הומניסטי. התאוריה התועלתנית אומרת שהקניין שייך לא׳ כי רוצים לקדם את הרווחה וכו׳. יש קניין ערטילאי שהוא שלו. מדובר במצב צבירה של קניין מעורב, משום שא׳ נתן לב׳ אישור. הציפייה בקניין מעורב היא שלא׳ אין ציפייה אקסלוסיבית מלאה, אלא רק אקלוסיביות חלקית. שהטכנאי לא יכנס למקומות

שא׳ לא נתן לו רשות להיכנס אליהם. הפלוס המוסרי בהשגת הגבול של ב׳ זה המציצנות, לדעת באיזה אתרים א׳ גולש. המסקנה היא שיש פגיעה בזכות לפרטיות, יש לו פרטיות גם למידע שהוא לא כלכלי וכו׳. יש סוג של השגת גבול.

<u>הזכות לאוטונומיה-</u>

מתי הופכת הגישה של א׳ למחשב של ב׳ להשגת גבול. מתי החוק צריך להגיד שכאשר א׳ נכנס למחשב של ב׳ יש השגת גבול. אין ספק שכאשר א׳ גורם לנזק למחשב של ב׳, או כשב׳ פורץ מנגנון הגנה טכנולוגי שמגן על המחשב של א׳ אין ספק שיש השגת גבול. השאלה היא אם א׳ נכנס למחשב של ב׳ בלי הסכמה של א׳ צריכה להיות השגת גבול. יש שלושה מנגנונים שונים שגורמים לכניסה להשגת גבול: 1. פיצוח מנגנון הגנה טכנולוגי 2. פריצה/נזק 3. אי הרשאה.

מתי יש הסגת גבול:

חוק יסוד כבוד האדם וחירותו: ס׳ 3 מגן על הקניין.
גדרת הזכות לקניין בכתבי המלומדים - הזכות להוציא אחרים מהקניין.
כל אלה לא עוזרים להבין מתי יש השגת גבול.
כמעט כל העבירות והעוולות, קו הגבול שלהן שונה. עוולת השגת גבול במטלטלין מתייחסת למשהו שגורם לנזק. ס׳ 2 לחוק המחשבים מדבר גם על נזק, ס׳ 7 לחוק המחשבים מדבר על הפרעה למחשב. פריצה מדברת על כניסה. חלק מדברים על יסוד נפשי. גם הפנייה לדין הכללי/העולם המוחשי על מנת להיקש לעולם המחשבים לא עוזרת.
קיים דיון מאוד סוער בכל הנוגע לשאלה הזאת בדיני המחשבים. בחוק האמריקאי ס׳ 1030 מתייחס לגישה לא מורשת ולכניסה שהיא בחריגה מההרשאה. חוק המחשבים בישראל מדבר על חדירה שלא כדין למחשב (לא מתייחס אם ללא הסכמה). השאלה שאלתה לדיון בפס״ד ניר עזרא מה זה ללא כדין, האם זה ללא הסכמה.
היחידה בוחנת האם ראוי שללא הסכמה ישמש קו הגבול בהשגה למחשב, וכיצד ראוי לפרש את יסוד ההסכמה:
גישת ההסכמה- לכל אדם יש הזכות לאוטונומיה אישית, הזכות לבחור את מהלך חייו. הזכות להחליט על מהלך חיינו. פרופ׳ דבורקין- הזכות לאוטונומיה היא היכולת של האדם להעדיף דברים, לרצות דברים. לזכות לאוטונומיה משקל רב בחברה המודרנית.
הזכות לאוטונומיה באה לידי ביטוי בזכות לכבוד. הנשיא ברק אומר שביסוד כבוד האדם עומדת האוטונומיה של הרצון הפרטי, חופש הבחירה וחופש הפעולה. כבוד האדם הוא החירות של האדם לעצב את חייו. כבוד האדם מתמקד ביחיד ובחופש הרצון שלו. הפס״ד החשוב ביותר המתייחס לזכות לאוטונומיה וכבוד האדם הוא פס״ד אלי דאקה. שמים דגש רב על האוטונומיה של הפרט. הנשיאה ביניש אומרת שיש שינוי תפיסתי תרבותי וחברתי בכל הנוגע לזכות לאוטונומיה, את השינוי החברתי הזה מיישמים גם בזירת הסייבר.
לתפיסת המרצה, הזכות לאוטונומיה אומרת שאפשר לעשות מה שרוצים בקניין שלך האישי. הרצון שלי הוא שיקבע מה יגע בקניין שלי. אותו הדבר גם בזירת הסייבר. מכוח הזכות

לאוטונומיה רשאי אדם לשלוט על הגישה לרכושו הווירטואלי ולהחליט מי ייגש למחשב שלו, מי יאזין לתקשורת וכו׳. אם יש לי זכות להחליט מי ייגש למחשב שלי, ראוי גם שדיני השגת גבול למחשב יוכפפו למשטר של הרשאה, כלומר, על פי גישה זאת ההרשאה היא שצריכה לסמן את קו הגבול בין כניסה תקנית לאסורה למחשב הזולת. זו גישה הומניסטית, לאדם יש זכות לאוטונומיה אז אסור לפגוע בזה. ההכפפה למחשבים היא גם תועלתנית. התועלת אם זה לא יהיה כפוף להרשאה אנשים יפחדו. האוטונומיה מגבירה את תחושת הרווחה של הבעלים ומחזקת את ביטחוניים לגבי נכסיהם. שהרי בהיעדר הגנה משפטית הבעלים יצטרכו להשתמש בטכנולוגיה על מנת להגן על רכושם ויחששו שמשיגי גבול יגעו בזה. כך גם לגבי המחשב.
קו הגבול הוא ההרשאה. האלטרנטיבה היא הפריצה/נזק, פיצוח מנגנון הגנה טכנולוגי.

לסיכום, ככלל יש שלוש גישות אפשריות: (מהו הדין הראוי לגבי השגת גבול)

1. **גישת ההרשאה**
2. **גישת הנזק**
3. **פיצוח מנגנון הגנה טכנולוגי**

לדעת המרצה קו הגבול הוא הסכמה.

ביקורות אפשריות על גישת ההסכמה:

1. לא תמיד אפשר לקבל הסכמה- פרופ׳ קר אומר שהחוק האמריקאי תלוי בהרשאה הוא רחב מדי, כי המונחים ללא הרשאה ובחריגה מהרשאה הם לא ברורים והם עלולים להפוך את החוק ללא חוקתי.

לדעת המרצה הצורך בבירור כוונת המסכים, והתחקות אחרי המצב שבו ניתנה הסכמה הוא לא נדרש רק בדיני מחשבים, הוא נדרש בכל מצבי השגת גבול שבהם אחד היסודות הוא הסכמה (אונס, תקיפה, גניבה וכו׳). לא הופך את העבירות הללו ללא חוקתיות.
בפרשת ניר עזרא בית המשפט מפרש את יסוד שלא כדין (יסוד ההסכמה). העמימות של המונח ללא הסכמה הוא פועל יוצא של כל עבירה או עוולה.

2. החשש מריבוי תביעות- בפרשת ניר עזרא, השופט רובינשטיין מדבר על ס׳ 34 לחוק העונשין. גם בפקודת הנזיקין יש הגנה מקבילה, של מעשה של מה בכך בס׳ 4 לפקודה. גם ס׳ 64 לפקודת הנזיקין.

הפגיעה בזכות לאוטונומיה

כניסה למחשב הזולת ללא הסכמה
כשיש הפצה של המידע – לא מספיק שהוא הסתכל, אלא שהוא גם הפיץ את המידע.

מה הבעיה עם גישת ההסכמה? למה זה לא טוב?
אולי הגישה הזו רחבה מידיי וצריך גישה מצומצמת יותר שתגרום גם נזק לרכוש.

כניסה למחשב הזולת תוך פיצוח מנגנון הגנה טכנולוגי -

מהו קו הגבול בחדירה למחשב? מתי החוק צריך לקבוע שזה לא בסדר שנכנסתי למחשב הזולת?

ישנן שלוש גישות:

1. גישת ההסכמה

2. גישת הנזק

3. גישת פיצוח מנגנון הגנה טכנולוגי

בחוקים שונים ובמדינות שונות יהיו קווים שונים.
בארצות הברית למשל חלה "גישת ההסכמה". באמריקה, קו הגבול הוא ההסכמה.
בישראל, חוק המחשבים קובע על פי **פרשת ניר עזרא** שחלה "גישת ההסכמה".

מה היתרונות של גישת ההסכמה?
היא מגנה על **זכות יסוד: כבוד האדם וחירותו**, על זכות האוטונומיה. לכל בן אדם יש זכות להחליט על מהלך חיו, מי יכנס לטלפון שלו ומי לא כחלק מהזכות לכבוד.
ככלל, עבירות המחשבים צריכות להיות בינאריות – אם הסכמנו, מותר למישהו להיכנס. אם לא הסכמנו, אסור לו להיכנס.

* ישנן בעיות עם מושג ההסכמה:

1. ההסכמה היא מושג עמום: בפרשת ברקה, בית המשפט אומר שבגלל שהמונח "הרשאה" הוא לא ברור, יש לפרש אותו בצמצום. המלומד קר אומר שבגלל שהמושג "הרשאה" הוא לא ברור - הוא לא חוקתי. צריך להבהיר את הדין בכל מה שנוגע ל"הרשאה".
לדעת המרצה – המונח "יסוד ההסכמה" מופיע בהמון עבירות של הסגת גבול, למשל בעוולת התקיפה\עבירת האינוס. צריך להבהיר את יסוד ההסכמה.

2. חשש מריבוי תביעות: טענה זו הועלתה **בפס"ד בני עזרא**: בחור ביקש ברשת מספרי כרטיסי אשראי של אנשים, הוא קיבל אותם, נכנס לחשבונות הבנק של אנשים, באחד המקרים גם העביר לעצמו כספים והוא מזוכה מעבירת החדירה למחשב בשתי ערכאות.
השופט אליקים רובינשטיין קרא לדברים האלה "מעשים של מה בכך". טענת החשש מריבוי תביעות נדחתה בפרשת ניר עזרא ע"י השופט אליקים רובינשטיין בהתבסס על **הגנת "זוטי דברים"**. בפרשת ניר עזרא נאמר בבית המשפט כי "פוטנציאל הנזק העצום הכרוך בעבירות מחשב

מחייב לדבוק בפרשנות המרחיבה של המושג ש"לא כדין" ולצמצם את הבעיה באמצעות שימוש בשכל הישר ו**בסייג "זוטי דברים"** שקבוע בסעיף 34יז לחוק העונשין".
האם באמת יש עומס על בתי המשפט בדיני מחשבים? – לא. יש כשל שוק בעניין זה:
אין כמעט תביעות המבוססות על חוק המחשבים, יש כשל שוק בכל הנוגע לעבירות הסייבר, שכן, אין מודעות לעצם הפריצה, אין כמעט אפשרות לתפוס את הפורצים. לכן אין מקום לחשש מריבוי תביעות כי בפועל אין הרבה תביעות בבתי המשפט הנוגעות לפריצה למחשב.

3. גישת הנזק כאלטרנטיבה לגישת ההסכמה: פרופ' ניבה אלקין קורן אומרת שקו הגבול לא צריך להיות הסכמה, אלא קו הגבול צריך להיות נזק. לדעתה, גישת הנזק איננה ראויה שכן היא מגבילה תחרות במשק.
גישת הנזק מחלישה את השליטה הקניינית של בעל המחשב בקניינו, היא לא נותנת מענה להשקעה של הפרט באתר שלו.

4. גישת הפיצוח כאלטרנטיבה לגישת ההסכמה בדיני מחשבים:
רק כשהמחשב שעליו מדובר הוא **מוגן באמצעי הגנה טכנולוגי**, צריך שהחוק יאסור חדירה למחשב. כלומר, <u>רק אם המחשב של דניאל מוגן בקוד וסיסמא רק אז החוק יגיד שאסור לחדור למחשב שלו.</u>
מה היתרון של הגישה הזו?
אם לכולנו יהיה קוד וסיסמא אז מערכת האינטרנט בכלל תהיה הרבה יותר בטוחה. למשל, יש מתקפה שקוראים לה "דידוס" – התקפת מחשבים בשרשרת. אם המחשב הראשון יהיה מוגן, שאר המחשבים האחרים לא ייפרצו.
יתרון נוסף, אנחנו יודעים שזה מבהיר לנו שמשהו לא בסדר, קו הגבול הוא הרבה יותר ברור.
מה החיסרון של הגישה הזאת?
קודם כל זה פוגע באוטונומיה שלי. העובדה שמישהו לא שם סיסמא זה לא אומר שהוא הסכים לפריצה למחשב.
בנטהאם אומר שכאשר יש חוק שמגן על הקניין של האדם זה מעלה את תחושת הרווחה של בעל הקניין, משום שהוא לא כל הזמן צריך לדאוג לשמור על הקניין שלו. אותו דבר במחשבים, תעלה תחושת הרווחה של האנשים גם אם הם לא שומרים על האמצעי הטכנולוגי שלהם באמצעות סיסמאות וקודים.
גישת הפיצוח מגנה רק על מי שיש לו ידע במחשבים, על החזק הטכנולוגי. היא לא מגנה על החלשים ולכן זה לא הוגן.
בעיה נוספת היא **"טענת המדרון החלקלק"** - בפרשת הלמו דובר על אדם בשם הלמו אשר נכנס לחשבון של אדם בשם שדות בביטוח הלאומי. שדות היה חייב כסף לביטוח לאומי, יש לו דף באתר הביטוח הלאומי בו כתוב כמה כסף הוא חייב. הדף היה מוגן בקוד, אולם הקוד היה מאוד חלש והיו יכולים לפרוץ לחשבון שלו בקלות.
הלמו פתח את הדף של שדות באתר של הביטוח הלאומי, שילם בשבילו שקל אחד כנגד חוב של מליון ₪. באתר של ביטוח לאומי היה באג שגרם לכך שהחוב של שדות התאפס ושדות קיבל לביתו

מכתב שהוא כבר לא חייב חוב לביטוח הלאומי.
כנגד הלמו הוגש כתב אישום על כך שהוא חדר למחשב ללא הסכמתו של שדות.
בבית המשפט זיכו את הלמו. טענת הזיכוי הייתה שהקוד של המחשב היה חלש מידיי. כל אתר שניתן להיכנס אליו בקלות כה רבה אי אפשר לטעון שהיה אסור להיכנס אליו. בהיעדר מחסום אבטחה, אין לומר שיש חדירה למחשב. גישת הפיצוח כאן מפורשת בצורה מאוד רחבה על ידי השופט. לא מספיק שיש קוד, אלא מנגנון ההגנה צריך להיות חזק.

הביקורת על גישתו המרחיבה של השופט טננבוים **בפסק דין הלמו:**
גישת הפיצוח עלולה להוביל ל"מדרון חלקלק", כלומר, היא יכולה להוביל לכך שבתי המשפט יגידו שמנגנון ההגנה הטכנולוגי צריך להיות חזק ולא מספיק שהוא קיים.

אין לתת חסינות גורפת למי שחודר למחשב הפרט ללא הסכמתו.

סיכום:
המחשב הוא אבן הפינה בחברה הדיגיטלית וראוי להגן עליו באמצעים משפטיים, ובכלל זה, להגן על האקסקלוסיביות של הגישה למידע הממוחשב, רק לי מותר להיכנס למחשב.
לדעת המרצה, בכדי לתת תוקף לריבונות הזאת, יש להפוך את ההסכמה הנובעת מזכות היסוד לאוטונומיה לקו הגבול בין גישה ראויה למחשב הזולת לבין הסגת גבול.
הצבת ההסכמה כקו הגבול בחדירה למחשב היא ביטוי להכרה בכך שלבעלים של המחשב יש שליטה מלאה בקניין שלהם וזכות לסרב לכניסת הזולת למרחב שלהם.

ג. כלים לפרשנות הרכיב "ללא הסכמה":

1. מצבי צבירה קניינים שונים בקניין המוחשי וניתוח העוצמות המשתנות של הזכות לאוטונומיה במרחב הווירטואלי -
מצבי הצבירה הם: קניין פרטי, קניין מעורב\משותף, קניין ציבורי\מעין ציבורי.
הפסיקה והחקיקה מפחיתה את הזכות לשלוט בקניין, את האחיזה הקניינית כשהוא הופך להיות "קניין משותף" וכשהוא הופך להיות "קניין ציבורי\מעין ציבורי". אם בקניין הפרטי בתי המשפט אומרים שהבעלים יכול להיות קפריזי(לעשות מה שבא לו), אז בקניין המשותף הוא כבר לא יכול לעשות מה שבא לו בדומה לקניין הציבורי\מעין ציבורי.
* מי צריך לקבל או לבקש את ההסכמה כשהוא רוצה להיכנס לקניין של הזולת?
על מי חל נטל בקשת ההרשאה ונטל ההתנגדות לגישה למחשב?
יש להתייחס למצבי הצבירה הקניינים השונים:
- קניין פרטי\אישי:
בקניין הפרטי יש מקסימום אוטונומיה לבעלים. השופט חשין אומר שזכות הקניין משמעה כעיקרון זכותו של האדם לעשות או לא לעשות בקניין שלו מה שהוא רוצה. נטל ההסכמה חל על מי שרוצה להיכנס לקניין, על האדם הזר.

- קניין מעורב:

הפסיקה מפחיתה את האוטונומיה של הבעלים בקניין. בפרשת סולברג השופט חשין אומר, כי זכות הקניין הקלאסית דוחה מעליה כעיקרון את יסוד הסבירות. אבל, מנגנון הסבירות במשפט נועד לוויסות של חיים יחדיו. בקניין משותף כן בודקים את הסבירות של המעשים של הפרט כי הוא תלוי בגורם נוסף.

- קניין ציבורי\מעין ציבורי:

גם כאן בתי המשפט נוטים לפרש את הזכות לאוטונומיה בצורה מצמצמת. פרופ' דגן אומר שבקניין הציבורי לערך הקהילה יש חשיבות גדולה. כדי שנוכל לפעול לכינון של חברה אחת, בקניין הציבורי צריכה לצמוח זכות כניסה לקניין באתרים שאליהם מורשים אחרים להיכנס (בפס"ד תעדן דיברו על "זכות הכניסה").

* איך מבססים את כל מצבי הצבירה למחשבים? *

1) בקניין פרטי – "חזקת אי ההסכמה לגישת הזולת" - יש לבקש הסכמה.

בקניין הפרטי ראוי ליתן משקל מוגדל לאוטונומיה של הבעלים בכל הנוגע לגישת הזולת למרחבו.
כאן, לקניין הפרטי כאתר של אישיות ושל חירות ופרטיות יש חשיבות רבה.
הקבצים של הפרט, התמונות שלו מבטאים את הפרטיות שלו. ההגנה הקניינית מגנה על הפרטיות של הפרט ולכן במחשב שלו קיימת חזקת אי ההסכמה לגישה למחשב, יש לקבל הסכמה על מנת להיכנס אל המחשב אחרת מדובר בהסגת גבול(וזה לא משנה אם הפריצה נעשתה בקלות או בקושי, אם יש סיסמא או אין סיסמא) מה שמשנה זה חוסר ההסכמה בכניסה לקניין פרטי.

2) בקניין מעורב – לדוגמא, מחשב של מעסיק, פלאפון ששמתי לתיקון אצל טכנאי, מחשב אישי הנמצא בשימוש משפחתי, אדם זר ברחוב שהשאלתי לו את הפלאפון בכדי שיתקשר לבית שלו.
לדעתה של המרצה, קניין מעורב קיים גם כשאני גולשת באתר של מישהו. המחשב שלי באותו רגע הופך לקניין מעורב.
בשביל שהוא יוכל להעביר לי את המידע, אני נותנת לו לגיטימציה להיכנס אליי למחשב, ברגע שאני נכנסת לאתר של מישהו אחר נתתי לו אישור להיכנס גם למחשב שלי.
בקניין מעורב אנחנו מדברים על "מורשי גישה" שהגישה שלהם מוגבלת.
בקניין משותף, לערך הקהילה יש משקל רב ולכן העדנות של הבעלים בקניין שלהם מצומצמת באופן יחסי. בקניין מעורב נחלשת הזכות לאוטונומיה ויש לאזן בין הזכויות המנוגדות. ככלל, בקניין מעורב, נטל קבלת הרשות לגישה מוטל על מי שיש לו אחיזה קניינית חלשה יותר באופן יחסי.
למשל, במחשב של מעסיק, לעובד מותר לעבוד על המחשב הזה, האם למעסיק מותר להיכנס למיילים האישיים של העובד?
תשובה: העובד הוא בעצם הבעלים של המיילים האישיים ולכן המעסיק במקרה הזה צריך לקבל את ההסכמה של העובד להיכנס למיילים שלו.

לדעתה של המרצה, בקניין המשותף צריכים לבחון את **הסבירות** של המעשים שנעשו, וצריך לבדוק את המדרג: למי יש יותר כוח, מי הבעלים, מי בעל הרשות ועוד.

בקניין מעין ציבורי – יוצאים מנקודת הנחה שניתנה הסכמה, חזקת הסכמה.
משקל האוטונומיה של הגולש במחשבו: מה מותר לאתר שנכנס לי למחשב לעשות?
במהלך גלישה באינטרנט ניתנת לאתר הרשאת גישה למחשב הגולש. יש לבחון את אופי האתר שבו דובר: באתרי אינטרנט פתוחים כמו פורומים וצ'טים, כשאדם גולש באתר אינטרנט פתוח, כמוהו כמי שנמצא ברשות הרבים, וכאילו שהוא נתן **הסכמה מכללא** לצפות במה שהוא עושה. אם הגולש מפרסם פוסטים אז האוטונומיה שלו היא אפסית כי הוא כאילו נתן הסכמה מכללא לצפות בו.
לעומת זאת, באתרי אינטרנט סגורים שאינם מהווים חלק מרשות הרבים, הציפייה של הגולש היא לגישה ללא עין בוחנת של גורם חיצוני, ולכן כאן אין הסכמה להפצה של המידע.
לעומת זאת, הגלישה ברשת איננה מהווה כרטיס כניסה חופשי למחשב של הגולש ואין בה משום הסכמה להחדרת תוכנות או קבצים כמו קוקיס למחשב. אם המחשב רוצה לעשות משהו הוא צריך, לדעת המרצה, לקבל הסכמה מבעל המחשב.

למה אני יוצאת מנקודת הנחה שיש "הסכמה מכללא" להיכנס למחשב?
אנחנו בתור חברה רוצים שיהיה חופש לכולם, לחברה יש אינטרסים להרשות לאנשים לגלוש באתרים פתוחים:
- קיים **אינטרס ציבורי** בחופש מידע ובשיתוף מידע, ובהנגשת מידע מקוון.
- גם אתר פרטי מבוסס על **קניין ציבורי**(שרתים ציבוריים). ג'ון סטיוארט אומר כי מי שנהנה מהגנת החברה חייב לגמול על טובה זו,לכוף את עצמו לכללי החברה, ולהקריב מהריבונות שלו.
כיום נוצרה נורמה מקובלת של גישה חופשית לאתרים פתוחים ברשת.

חזרה על שיעור שעבר:

הזכות לאוטונומיה –
א' עובד בחברה, הוא עוזב את מקום העבודה והוא מבקש מהמזכירה(ב') לתת לו להיכנס לאחד ממאגרי המידע של החברה. המזכירה מסכימה לכך, והוא נכנס.
האם יש כאן עבירה של חדירה למחשב?

כניסה למחשב בניגוד למשהו שכתוב בתנאי השימוש:
אנחנו גולשים באתר אינטרנט, ובאתר כתוב ש"בחורות עם חולצה לבנה לא יכולות לגלוש באתר שלנו"?

בשביל לענות על השאלות האלו, יש שאלה מקדימה שצריך לענות עליה:
מהו קו הגבול שראוי להציב בין כניסה תקינה למחשב הזולת לבין כניסה אסורה?
לפי **פרשת ניר עזרא** קו הגבול הוא "ללא הסכמה" - זאת אומרת, **כניסה ללא הסכמה של בעל המחשב היא כניסה אסורה.**

ההסכמה של בעל המחשב יסודה בזכותו לחוק יסוד: כבוד האדם וחירותו בתוך הזכות לכבוד. לכל אדם יש זכות לכבוד, ולכל אדם יש זכות להסכים או לסרב למה שייעשה בקניין שלו. לכן, כשקו הגבול הוא יסוד ההסכמה, אנחנו נותנים משמעות לזכות לכבודו של האדם וזכותו לאוטונומיה.

אם קו הגבול הוא יסוד ההסכמה, זה הופך את עבירת החדירה למחשב לעבירה דואלית:
יש לה שתי פנים – כלומר, אותו אקט של כניסה למחשב של מישהו תלוי ביסוד ההסכמה.
בעוד חוקים של "הסגת גבול וירטואלית" – חוק הגנת הפרטיות, חוק האזנת סתר, חוק המחשבים.
המון מלומדים לא מסכימים עם הגישה הזו שיסוד ההסכמה הוא היסוד שראוי לשמש קו הגבול בין חדירה ראויה ונאותה למחשב הזולת.
הביקורות:
1. הסכמה היא מושג עמום מידי: פרופ' קר אומר שזה הופך את כל העבירה ללא חוקתית. אדם שמאשימים אותו בחדירה למחשב הוא לא מבין אם כן הייתה הסכמה או לא הייתה הסכמה, למה מתכוונים שאומרים הסכמה בכלל? המושג הוא לא ברור.
בית המשפט העליון קבע כי יסוד ההסכמה צריך להיות מפורש בצמצום. יסוד ההסכמה הוא קו גבול הכרחי בדיני הסגת גבול. למשל: בעבירת האינוס – כשבחורה אומרת לא למה היא מתכוונת? אפשר לטעון שלא הבינו אותה.
בית המשפט והמלומדים צריכים להתוות ארגז כלים פרשני.
2. חשש מריבוי תביעות: הטענה הזאת הועלתה בפרשת ניר עזרא. גיל שווד מספר ש200 חברי"ה מחברת צ'ק פוינט(חברת אבטחת מידע) החליטו לבדוק את האיי רובוט של חברת אל ג'י. הם גילו שלאיי רובוט יש מצלמה ואפשר לפרוץ אליו. יש פרצת אבטחה באיי רובוט. אפשר לראות באמצעותו מה קורה בבית של האדם.
עו"ד של ניר עזרא אמר בתיק שלו שיהיו יותר מידיי תביעות.
המרצה אומרת: צריך להגן גם מפני חדירה למחשב מסוג "איי רובוט".
השופט רובינשטיין בפרשת ניר עזרא: הגנת "זוטי דברים".
תשובה נוספת לריבוי תביעות: בפועל, יש "כשל שוק" בכל מה שנוגע לעבירות מחשבים כי אין כמעט תביעות בכל מה שנוגע לעבירות מחשבים ובטח לכל מה שקשור לעוולות מחשבים.

ביקורת נוספת על גישת ההסכמה:
3. גישת הנזק: יש שופטים, מלומדים ומחוקקים שאומרים שרק שיש נזק למחשב הנחדר תהיה עבירה או עוולה. זה קו גבול יותר ברור מהסכמה.
בארץ, סעיף 2 וסעיף 7 לחוק המחשבים אומרים שאם נגרם נזק למחשב עשית עבירה או עוולה.
האם זה צריך להיות כאלטרנטיבה לחדירה למחשב ללא הסכמה?
גישת הנזק לא מגנה מפני פגיעה בפרטיות, זו "חדירת סתם". היא גם לא מגנה מפני חופש הביטוי, כי חדירה למחשב היא "מלום פרסה"(???) – דבר רע כשלעצמו.
בית המשפט בפרשת ניר עזרא אומר שזה לא טוב לחדור למחשב כי אחר כך אפשר לגנוב מהמחשב

הזה. המרצה אומרת בניגוד לשופט רובינשטיין שעצם החדירה למחשב היא דבר רע כשלעצמו.

גישה נוספת כקו גבול בעבירת החדירה למחשב:
4. גישת הפיצוח: לפי גישה זו, רק מחשב שמוגן בסיסמא וקוד או בחומת אבטחה יש לפצח מנגנון הגנה טכנולוגי.
יתרונות: הגישה הזו גורמת לנו להגן על המחשב שלנו, ומחשבים מוגנים עוזרים לכל החברה.
חסרונות: הגישה הזו לא מגנה על החלשים טכנולוגית, יש חשש למדרון חלקלק.
פס"ד הלמו.

ארגז כלים לפרשנות הרכיב "ללא הסכמה":

1) מצבי צבירה קניינים שונים בקניין המוחשי וניתוח העוצמות המשתנות של הזכות לאוטונומיה במרחב הווירטואלי – מחשב פרטי(המחשב שלי), מחשב ציבורי(אתר אינטרנט פתוח – למשל פייסבוק), מחשב מעורב(המחשב של המכללה):
* מתי הפייסבוק יהיה מחשב מעורב?
פייסבוק היא תמיד קניין מעורב כי יש את בעל הדף הפייסבוק, ויש את פייסבוק שהיא בעלת התוכנה\האפליקציה. יש לה תמיד קניין מעורב, לכן אי אפשר לעשות כל מה שאני רוצה בפייסבוק.

מה היוצא מן הכלל של שלושת מצבי הצבירה האלה?
- בקניין ממוחשב פרטי(למשל :פלאפון נייד) יש חזקת אי הסכמה לכניסה\לגישה.
נקודת המוצא היא שאין הסכמה. אם אני נכנסתי לפלאפון נייד של מישהו אחר אני צריכה להוכיח שהוא לא הסכים לכך.
- בקניין מעורב: הבעלים של האי מייל הוא העובד. בקניין מעורב, העובד הוא הבעלים של האימייל ולכן אם המעסיק רוצה להיכנס אז הוא צריך את ההסכמה של העובד לכך (בפסק דין איסקוב).
בקניין מעורב נחלשת החזקה הקניינית של שני הצדדים, גם של המעסיק וגם של העובד.
- בקניין ציבורי או מעין ציבורי(=כמו ציבורי, למשל האתר של המכללה. זה לא "כיכר העיר" אבל זה כמו "כיכר העיר"): במקום שהוא מעין ציבורי או ציבורי נחלשת החזקה הקניינית של המכללה ולכן יש "חזקת הסכמה לגישה"\"הסכמה מכללא" לקניין הזה. זאת אומרת, יוצאים מנקודת הנחה שהמכללה הסכימה שכולם יכנסו לאתר שלה. אין צורך להוכיח שקיבלנו הסכמה לגלוש באתר של המכללה בניגוד לפלאפון פרטי.
מכיוון שלדעת המרצה יש הסכמה מכללא לכניסה לאתר אז כל מיני הוראות שכתובות בתנאי השימוש – אין להם כמעט תוקף גם מבחינת דיני החוזים האחידים וגם מבחינת דיני הנזיקין.

לדעת המרצה ופרופ' קר, ... להסכמת בעל האתר המסתתרת בתנאי השימוש שאליהם איש כמעט אינו נכנס והנפרשים לעיתים ל... נוגדת את האינטרס הציבורי מכיוון שזו פלטפורמה למידע, זה יאט את הגלישה ברשת, זה יפגע בפונקציונאליות של הרשת ולכן אומר קר שהפרת תנאי השימוש

היא הנורמה המקובלת ולא להפך.
זה בא לידי ביטוי **בפרשת דרו(מייספייס):** היו שתי חברות והייתה ביניהן תחרות ואמא של חברה א' התעצבנה על חברה ב', לכן האימא פתחה דף במייספייס, התחזתה לבחור חתיך שהתחיל עם בחורה ב'. היא התאהבה בו ואז הוא "נפנף" אותה והיא התאבדה.
הגישו כנגד האמא כתב אישום בגין כך שהיא הפרה את תנאי השימוש של מייספייס אשר אסר התחזות.
בית המשפט אמר: אין לבסס הרשאה בגין תנאי שימוש, זה לא ברור שכל הפרה מכוונת של הוראה בTOU...
בקיצור נקבע: אין פה חדירה ללא הסכמה. למרות זאת, במקרים רבים בתי המשפט בארצות הברית אוכפים זכויות קנייניות בהסתמך על ההוראות שכתובות בTOU. (Terms of use).

יש מקרים שבהם יהיה ניתן לסתור את חזקת ההסכמה לגישת TOU -
בארצות הברית מסתמכים על "הודעה סבירה" על אי הרשאה. בארץ פחות מתייחסים לזה.

דרך שנייה: הגנה טכנולוגית. יש לשים מנגנון הגנה טכנולוגי באתר שקובע שחלק הזה והזה אתה לא יכול להיכנס. או אין כניסה לרובוט\מכונה.
בפרשת פייסבוק נ' פאוורריינג'רס: הפאוורריינג'רס רצו לפרסם משהו בפייסבוק של מישהו, ופייסבוק חסמה אותם. אז פאוורריינגרס טענו שמותר להם כי בעל הדף הסכים.
בית המשפט קבע שמי שצריך להסכים זו פייסבוק. פייסבוק הקימה מנגנון הגנה טכנולוגי ולכן זה תקף.

נזק: אם מי שחדר למחשב או לאתר גרם לו נזק סתרנו את ההסכמה מכללא.

שאלה לדוגמא:
באתר איי פרילנס יש חלקים הפתוחים לציבור כולו וישנם חלקים שיש לפתוח באמצעות קוד וסיסמא. משה מעוניין לאסוף את הפרטים של הגולשים הנמצאים במאגר הסגור של האתר. הוא מפעיל תוכנה שיודעת לזהות את הסיסמא של המשתמשים וכך אוסף את כל הפרטים של המשתמשים לרבות נתוני הדיווחים למס הכנסה.
הקף את התשובה הנכונה:
א. מכיוון שמדובר במצב צבירה פרטי בלבד, אין חדירה למחשב על פי גישת הפיצוח.
ב. מכיוון שמדובר באתר מעין ציבורי(שכן הוא בבעלות חברת איי.פרילנס) הרי שהכניסה אליו היא בהסכמה מכללא לפי גישתו של קר.
ג. מכיוון שמדובר באתר מעין ציבורי עם חלקים סגורים על פי גישת המרצה נסתרת חזקת ההסכמה(פיצוח) ויש עבירה גם בהיעדר נזק.
ד. על פי גישתו של קר ושל בית המשפט העליון בפרשת ניר עזרא, מכיוון שמנגנון ההגנה הטכנולוגי אשר הגן על האתר המעורב היה חלש – אין כאן חדירה למחשב.

מצב הצבירה: ציבורי\מעין ציבורי אבל יש בו גם חלקים סגורים+קוד(מנגנון הגנה טכנולוגי).
ככלל, באתר מעין ציבורי, החזקה היא חזקת הסכמה מכללא והיא נסתרת ע"י מנגנון הגנה(קוד).

מבחן תחולת ההסכמה – על מה חלה ההסכמה?
יש להבחין בין הסכמה מפורשת, מכללא וחוזית.
- בין הסכמה מפורשת להסכמה מכללא
- הסכמה חוזית
- הגישה המחוזית בארה"ב

במצב האידיאלי(שלא קיים תמיד) ניתנת הסכמה מפורשת לגישה למחשב וגם גבולותיה של ההסכמה מפורשים.
המצב הזה הוא נדיר. חיי היום יום מחייבים להסיק מכללא במשתמע את קיומה של ההסכמה לחדירה אל מחשב הזולת ואף את תיחומה, את הגבול של ההסכמה.
הדברים האלו דורשים התחקות אחר הנסיבות שבהן ניתנה ההסכמה.
* לדעתה של המרצה, היעדר אמירה בנוגע למה שאסור לעשות במחשב אין פירושו הסכמה לגישה לכל מקום למחשב.
* הסכמה חוזית:
מכיוון שהסכמה מפורשת לא תמיד מכסה כל פעולה שניתן לעשות במחשב ומכיוון שלעיתים קשה להגדיר את גבולות ההסכמה מכללא, המוצא הראוי הוא לפנות אל החוזה שבין הצדדים בכדי לברר מה הוסכם ביניהם.
אולם, נכון שזה הדבר האידיאלי(שיהיה חוזה בין הצדדים).
האם זה פרקטי? לא. מכיוון שזה כרוך בזמן, במאמץ.
במחשב הפך לאבן הפינה בחיינו וצריך שנושא הכניסה או הגישה למחשב יובהר על ידי בתי המשפט ולא יושאר לטיפול בלעדי של בעלי המחשב באמצעות חוזים. החוזה מגן רק על הצדדים החזקים לחוזה ולא על אנשים חלשים. יש להנגיש את מערכות המחשבים כך שניתנו מענה להתנהגויות שגרתיות בסביבה ממוחשבת, ולא תמיד ניתן להתייחס לכל היבט של ההרשאה. הרי לא נחתים טכנאי מחשבים על חוזה שאומר לאיזה קבצים הוא יכול להיכנס ולאיזה לא.

בארצות הברית, הלכו עם הגישה החוזית יותר מידי רחוק. בארצות הברית בחלק מפסקי הדין הושם דגש על ההיבט החוזי של ההסכמה לגישה למחשב תוך התעלמות מאי הסכמה משתמעת.
בפרשת ברקה: היה עובד שיש לו גישה למחשב המעסיק. הוא מנהל עם המעסיק שלו הסכם שותפות בעסק. ברקה שלח לעצמו מהמחשב של המעסיק אימיילים עם מסמכים סודיים של המעסיק. לפי גישת המרצה, זה לא בסדר. אבל בית המשפט אמר שהמעסיק לא תחם בחוזה את מה שאסור היה לברקה העובד לעשות ולכן לא הייתה כאן חריגה מהרשאה, מותר היה לו לעשות את זה.
האם הגישה הזו שתוחמת את גבולות ההסכמה בחוזה בין הצדדים היא גישה ראויה?
בית המשפט בארצות הברית קובע: מה שלא נאסר בחוזה – מותר.

מה הטענות כנגד התפיסה הזאת?
דרכי החיים המודרניות מבוססות על מחשבים ואי אפשר שעל כל פעולה פשוטה תהיה חוזה.
בפרשת ברקה - בית המשפט הסיק הסכמה מכללא אך לא הסיק את גבולות ההסכמה מכללא.
דיני החוזים צריכים להגן גם על החלשים, גם על מי שאין לו עורכי דין, ולכן אנחנו לא יכולים להתבסס רק על הגישה החוזית על פי דיני החוזים.

לדעתה של המרצה - הרשאה לגישה למחשב אינה מכשירה כל מעשה שנעשה במחשב על ידי מורשה הגישה, אלא רק את המעשים שלגביהם ניתנה הרשאה.
<u>חריגה מהרשאה</u> יכולה להתייחס למספר מימדים:
<u>1) לאיזה קבצים מותר להיכנס.</u>
<u>2) סוג השימוש המותר – להתקשר אל רשימת אנשי הקשר</u>
<u>3) אישיות מקבל ההרשאה</u>
אישיות מקבל ההרשאה הכוונה היא שאנחנו צריכים לשאול <u>למי ניתנה ההרשאה</u>?
אם נתנו הרשאה למשל למזכירה במשרד שלנו להיכנס למאגר מסוים, לא נתנו הרשאה לעובד לשעבר להשתמש במאגר הזה.
בפרשת נוזל: היה מדובר בעובד לשעבר שקיבל הרשאה מהמזכירה להיכנס למאגר המידע של העבודה.
נוזל 2: עובד לשעבר הפעיל עובדת מורשה להיכנס למחשב ותדלה ממנו מידע בעברו.
בית המשפט קבע כי פעולה באמצעות צד שלישי מורשה מהווה חדירה ללא הרשאה.
אותו דבר לגבי מתחזה. התחזות לטכנאי מורשה.
אם הטכנאי מתחזה למנכ"ל(פרשת בדיר), למי ההרשאה? יש כאן חריגה מהרשאה וחדירה למחשב. אם ההסכמה ניתנה למתחזה אין לה תוקף.
בפרשת ברקה דיברו על חריגה מההרשאה. בית המשפט אומר שחריגה מההרשאה זה גישה למחשב שלא הייתה רשות לגשת אליו.

<u>4) מתי מסתיימת ההרשאה?</u>
בפרשת ברקה דובר בעובד לשעבר. כל עוד ברקה היה עובד של המעסיק הייתה לו הרשאה. **אך ברגע שהוא פוטר הסתיימה ההרשאה.**
בפרשת קומפיוסרב: דובר על משלוח דואר זבל ללקוחות\לעובדים של התובעת. חברת קומפיוסורב שלחה הודעת "חדל". ברגע שהחברה שלחה למי ששלחה את הדואר זבל הודעה שיפסיקו – הסתיימה ההרשאה לשליחת אימיילים.
בפרשת סיטרים: דובר בעובד שעמד לפתוח עסק מתחרה במעסיק שלו כשהוא היה עובד אצל המעסיק הוא מחק את המידע שהיה במחשב הנייד של המעסיק. נקבע שההרשאה הסתיימה כאשר העובד פעל בניגוד לאינטרסים של המעסיק ובניגוד לחובת האמון שלו.
אם נייבא את ה"כלל" הזה לארץ אז היינו אומרים שברגע שיש פעולה בחוסר תום לב יש הפסקה של ההרשאה. חדירה לצורך תחרות היא מפסיקה את ההרשאה לחדירה למחשב.

5) למה ניתנה ההסכמה?

זו השאלה החשובה ביותר. בפרשת **רבקה צדוק** : רבקה היא עובדת ברשות המיסים. היא הייתה צריכה כסף לצורך טיפולי הפריה, וגיסה היה חוקר פרטי. הוא אמר שהוא ישלם לה כסף בשביל שהיא תיתן לו מידע ממאגר המידע של רשות המיסים(מי הנישומים). היא הוציאה את המידע שהוא ביקש והעבירה לו אותו.

האם מה שרבקה עשתה במחשב הולם להרשאה שניתנה לרבקה?

ההסכמה צריכה להיבחן בפריזמה אובייקטיבית סובייקטיבית

גם אם אין חוזה בין הצדדים אנחנו צריכים להסיק את גבולות ההסכמה מכללא.

איך נדע למה הוסכם?

בפרשת ברקה היה עובד ומעביד. אין חוזה בין הצדדים, וברקה שולח לעצמו אימייל עם מידע קונפידנציאלי של המעסיק. בית המשפט אומר כי **הגבולות של ההסכמה לא הוגדרו בחוזה ולכן אין כאן עוולה של חדירה למחשב ואין חריגה מהרשאה.**

לתפיסת המרצה, צריך לבדוק את ההסכמה מבחינה סובייקטיבית ואובייקטיבית.

איך אני בודקת למה המעסיק הסכים מבחינה סובייקטיבית?

צריך לבדוק על פי מה שהוא אומר בדוכן העדים למה הוא התכוון ולמה הוא לא התכוון בהסכמה שלו.

צריך גם מבחן אובייקטיבי שיבדוק את ההסכמה של המעסיק. יש לבחון בנוסף למבחן הסובייקטיבי איך **עובד סביר** היה מפרש את ההסכמה של המעסיק? או לחלופין מה **מעסיק סביר** היה מתיר לעובד לעשות בנסיבות?

האם מעסיק סביר היה מסכים שעובד יעביר מידע סודי שלו לעצמו?

הגישה של המרצה מסתמכת על **סקר שעשה פרופ' קוגלר**. קוגלר שאל אנשים מתי לדעתם יש הרשאה, למה יש הרשאה וכדומה?

מהסקר עולה שככלל, עובד מורשה גישה למחשב המעסיק שהשתמש בו לצרכים פרטיים. אבל כאשר הוא מעביר מידע ממוחשב על לקוחות החברה למתחרה או לחבר, הוא נתפס כמישהו שלא הייתה לו הסכמה. גם מישהו שהייתה לו הרשאה לגישה למחשב, נתפס כפועל ללא הרשאה כאשר הוא מעביר מידע למתחרה או לחבר.

לעומת זאת,

אותם נסקרים אמרו שכשעובד מורשה נכנס למחשב של המעסיק בשביל **לבדוק מה מזג האוויר – יש לו הרשאה לכך.**

ההסכמה צריכה להיות חופשית

הסכמה שניתנה תחת לחץ\כפיה\אינוס היא לא הסכמה חופשית.

כדי שלהסכמה יהיה תוקף היא **צריכה להינתן שלא מתוך כפייה**. רובינשטיין מוסיף ואומר שכדי שלהסכמה תהיה תוקף היא צריכה להינתן גם **לא מתוך "לחץ חברתי".**

לחץ חברתי פוסל הסכמה שניתנה.

יש להוסיף ולציין כי רק במקרים בודדים הסכמה תינתן תחת איומי אקדח.

אפשר להגיד שההסכמה היא לא חופשית כאשר היא ניתנת ללא אלטרנטיבות אחרות.

רז אומר שכדי להסכמה יהיה תוקף משפטי מחייב היא צריכה להינתן מתוך אפשרויות אחרות, **כאשר למישהו יש אפשרות לבחור בין אופציות שונות.**

ברשת אין אלטרנטיבות לפגיעה בפרטיות. אם כל האתרים הם כאלה שפוגעים בפרטיות, מכניסים קוקיז, אם ווינדוס לא שומרת על הפרטיות שלנו, אין באמת יכולת בחירה. אין במרחב הסיברקנטי(הרשתי) יכולת בחירה, שכן על פי רוב – הרשת בנויה בצורה שהיא פוגעת בפרטיות.

פרופ' לסיג אומר – החוק באינטרנט הוא "החוק הטכנולוגי".

פרופ' שוורץ אומר – קיימת א-סימטריה ביחסי הכוחות של הגולשים ברשת. לאתרים יש יותר כוח מאשר לגולשים. האתר הוא זה שקובע מה הטכנולוגיה, והטכנולוגיה היא לאסוף מקסימום מידע על הגולשים. הרשת מוטה כנגד הגנת הפרטיות של הגולשים ולכן לדעת המרצה, גם כמישהו לוחץ על "אני מסכים" אין באמת תוקף משפטי מחייב להסכמת הגולשים כשהם גולשים על I agree כי אין אלטרנטיבה.

יחסים בלתי שוויוניים – פערי כוחות

בזירת העבודה יש פערי כוחות ← המעסיק מול העובד שלו. למעסיק יש הרבה יותר כוח לעומת העובד. חופשיות הסכמת עובד לחדירת מעסיקו לאימיילים פרטיים שלו מוגבלת, שכן לרוב מדובר על יחסי כוחות בלתי שוויוניים ואין בידי העובד ברירה כי אם להסכים לפגיעה בפרטיותו.

בפרשת איסקוב(לפני הערעור) בהחלטה של בית הדין האזורי לעבודה אמרה השופטת: שהעובדת, איסקוב, יכלה שלא להשתמש במחשב של המעסיק ואז לא היו פוגעים לה בפרטיות. המרצה אומרת שאין לה אלטרנטיבה. הימנעות מגלישה באתרים מסוימים או ממשלוח דואר אישי איננה ברירה מתקבלת שכן היא מציבה את העובד בפני החליטה של "תיפגע או תפסיק" ואינה מעמידה לרשותו מבחר אפשרויות ראוי.

הסכמה מוסמכת:

כדי שההסכמה שניתנה תהיה ברת תוקף, היא **צריכה להינתן על ידי הגורם המוסמך.**

מתחזה לבעלים לא יכול להיות הגורם המוסמך! בפרשת נוזל 2, המזכירה הייתה נותנת הרשות, ובית המשפט קבע כי המזכירה לא הייתה מוסמכת לאפשר לעובד לשעבר כניסה אל מחשבי המעסיק. בניגוד לכך, שופט המיעוט לא הסכים עם הגישה הזו. הוא אמר שאין רע במה שהמזכירה עשתה. שיתוף של סיסמא הוא מקובל ולגיטימי. זה כמו שאני אעביר את הסיסמא של המחשב לאח שלי.

<u>עמדת שופט המיעוט בפרשת נוזל:</u>

מה אנחנו חושבים על עמדתו של שופט המיעוט?

שיתוף סיסמא הוא בסדר כל עוד הוא לא סותר מדיניות סבירה של הבעלים.

למשל, בפרשת **פייסבוק נ' פווריינג'ר** היה "שיתוף סיסמא" של דפי פייסבוק של לקוחות על מנת שחברת פווריינג'ר תוכל לפרסם בדפים שלהם פרסומות של החברה.

פייסבוק חסמה את הגישה של פאווריינג'ר בגלל שהיא לא קיבלה מהפעילות העסקית הזאת כסף ובבית המשפט נקבע ש: גולשים רשאים להרשות גישה לדף שלהם <u>אבל</u> חברת פייסבוק **רשאית לבטל** הרשאה זאת.

שורה תחתונה: "שיתוף סיסמא"(=Password sharing) חייב לעמוד במבחן של סבירות.

הסכמה מדעת

הסכמה שנתתי למישהו להיכנס אליי למחשב יהיה לה תוקף משפטי מחייב רק כשהיא הסכמה מדעת.

פס"ד עלי דקה: פ' אמנון רובינשטיין אומר כי הסכמה מדעת נגזרת מההכרה בזכותו של אדם לאוטונומיה. את התפיסה הזאת שבשביל שלהסכמה יהיה תוקף משפטי מחייב היא צריכה להיות מבוססת על מידע, ראוי ליישם גם ברשת.

לדעת המרצה, על המסכים לקבל מידע על אופייה של הכניסה, על מהותה, ועל הסיכונים הנובעים ממנה.

בית הדין הארצי לעבודה בפרשת איסקוב אומר שכאשר מעסיק רוצה לקבל הסכמה מדעת לחדירה למחשב של העובד, צריך שיהיה **גילוי מוחלט ושקיפות מלאה מצד המעסיק**, לאחר שהובאו לידיעת העובד טכנולוגיות איסוף המידע ומהותן, הנסיבות בהן ישתמש המעסיק בטכנולוגיות אלה ולאחר שהעובד הבין את השימוש שיעשה במידע.

בכדי שהסכמת עובד תהיה מדעת – המעסיק צריך לפרט בפניו פרטים רבים בקשר לחדירה אל המחשב.

לסיכום: ביחידה זו בדקנו מהו הקו הראוי בכל הנוגע לכניסה אל מחשב הזולת ואמרנו שקו הגבול הוא **"יסוד ההסכמה"** שמקורו בזכות היסוד לכבוד, ובזכות היסוד לאוטונומיה.

יחד עם זאת, המשקל שאנחנו נותנים להסכמה או לאי ההסכמה משתנה בהתאם למצב הצבירה של הקניין הממוחשב שעליו אנחנו דנים(פרטי\מעורב\מעין ציבורי).

* בקניין ממוחשב פרטי – קיימת חזקת אי הסכמה וזאת לעומת
* קניין ציבורי – אשר בו קיימת חזקת הסכמה לכניסה.

יכולה להיות הסכמה מכללא: הרשאה לגישה אך גם לגבולות הגישה למחשב. אמרנו שגם כשיש הסכמה צריך לבדוק האם יש הלימה, התאמה, בין ההסכמה שניתנה לבין מה שנעשה בפועל(חריגה מן ההסכמה) ואמרנו שבכדי שההסכמה תהיה תקפה היא צריכה להיות חופשית, מדעת, מוסמכת, וצריך לבחון אותה בעין אובייקטיבית וסובייקטיבית.

שאלה לדוגמא:

אהרון קיבל אישור כניסה למחשב של בנימין. בנימין אמר לו: "עשה טובה תבדוק לי למה הג'ימייל לא עובד לי. אהרון נכנס לקובץ התמונות של בנימין וצילם את המסך ושלח לעצמו את הצילום.

א) יש כאן חריגה מהכלל ב"Terms of use".

ב) מכיוון שמדובר בקניין "מעין ציבורי" יש כאן פעולה בחוסר סבירות

ג) להסכמה של אהרון אין תוקף משפטי מחייב שכן יש כאן יחסים בלתי שוויוניים ולא הייתה הסכמה מדעת.

ד) בנימין פעל בחריגה מהרשאה(הסכמה למה?) ולכן אין הלימה בין מה שנעשה במחשב לבין ההסכמה שניתנה וההסכמה אינה בת תוקף.

ה) תשובות א' וב' נכונות.

בפרשת **רמי מור** מבקשים צו מבית המשפט לאתר את כתובת ה IP של מישהו שפרסם לשון הרע על רמי מור.

עד כה במהלך השיעורים דיברנו על כך שיש שתי קבוצות עיקריות שעוסקות במחשוב פולשני:

קבוצה ראשונה: קבוצות פרטיות (האקרים מעסיקים, עובדים)

קבוצה שנייה: גורמים שלטוניים (משטרה, מוסד שב"כ).

כל סוג של מחשוב פולשני עלול לפגוע ב 4 זכויות אדם:

1) הזכות לפרטיות

2) הזכות לאוטונומיה

3) חופש הביטוי

4) הזכות לקניין

את המחשוב הפולשני הזה ניתן לעשות באמצעות צו, למשל המשטרה מבקשת צו חיפוש או האזנת סתר, או אדם פרטי מבקש צו לחשיפת כתובת ה IP של טוקבקיסט אנונימי כמו בפרשת רמי מור.

הפגיעה הקשה בזכויות האדם שנובעת ממחשוב פולשני, העיקרון שעולה שהחוק צריך לאסור מחשוב פולשני, החוק צריך להגן על הסודיות של המחשב של הפרט.

מחשוב פולשני יכול להיעשות ע"י הסרת מידע, כי המחשב הוא פלטפורמה לחופש הביטוי ולכן אם המשטר מתערב בתכנים יהיה פה משטר טוטליטארי. מצד שני, אם יש אתר פדופיליה, מחשוב פולשני ע"י גורמים שלטוניים יכול להיעשות במספר דרכים: צנזורה ברשת (הסרת מידע פוגעני), מניעת גלישה, מעקב אחרי פרטים.

היחידה הזאת עוסקת בשאלה: מתי צריך לאפשר לגורמים שלטוניים ולגורמים פרטיים להיכנס למחשב?

מתי נאפשר לגורמים שלטוניים לחדור למחשבים כדי למנוע פגיעה בחיי אדם?

Ex post factum (אחרי שקרה המקרה), לדוגמה: אחרי שחדרו לפייסבוק של ראש הממשלה, המשטרה רוצה לחפש מי עשה את זה.
Ex ante (לפני שקרה המקרה).

לפעמים יש צורך בחדירה למחשבים כדי למנוע פשיעה, כדי להביא עבריינים לדין וכדי להגן על ביטחון המדינה ולהציל חיי אדם. השאלה היא, איך צריך לעשות את זה?

איך עושים את האיזון, לשמור על 4 הזכויות ומצד שני מניעת פגיעה בחיי אדם?

עד למלחמת העולם השנייה עדיין היו לשכות אפלות כדי לגלות סודות, ובמלחמת העולם השנייה השלטון האמריקאי מפאת ההגנה על הפרטיות לא פתח אפילו מכתבים שהיו מיועדים לשגרירות יפן. והם הגנו על הזכות לפרטיות ופספסו מידע חשוב על ההתקפה המיועדת של יפן על הבסיס הצבא האמריקאי. וכאן רואים כי ההגנה גרמה לפגיעה בחיי אדם.

האיזון צריך להיות עדין בין מה שצריך לעשות לבין מה שהופך אותו למדינת האח הגדול. איך אנחנו מוודאים שמצילים חיי אדם בלי צווים ומצד שני איך אנחנו מונעים מצב של מדינת משטרה? ישנו אינטרס חברתי בשמירה על הסדר ובמניעת הסתה, המרדה שעלולה להוביל למוות באי פרסום מידע סודי, ישנו אינטרס ציבורי בשמירת חיי אדם, בשמירה על הסדר החברתי, בהבאה לדין.

המחשב עשוי לסייע בהכרה על כל האינטרסים הלגיטימיים הללו, שכן הוא אוצר גלום של ראיות מפלילות, יכו לספק מוצרי איכון. אבל בשביל להוביל לשימוש נכון במידע הזה ולמנוע פגיעה מיותרת בזכויות אדם, המחשוב הפולשני חייב להיעשות תוך הפעלה של מנגנוני ריסון ובקרה על הגורמים הממשלתיים. **ראשית לדעתי ראוי להתנות הליך חיפוש במחשב בצו שיפוטי גם שהחדירה ל non data information . לכלל הזה של צורך בבקרה משפטית יש *יוצא מן הכלל* והוא במצבים של ex ante כאשר יש *סכנה מיידית* וחמורה לחיי אדם ואולי גם לרכושו של אדם, הרי שלדעתי *אין צורך בקבלת צו חיפוש* , אלא גורם שלטוני יכול לחדור למחשב הזולת וזאת כאשר הסכנה היא ברורה.**
כמו לדוגמה בפרשת **אופיר נחום**, היה מדובר על בחור שיצר קשר עם בחורה באינטרנט, קבע להיפגש עמה במקום ולא חזר, המשטרה פתחה את המחשב ואיתרה את העניין. הבעיה בגישה הזאת נובעת מכך שמתברר שהבקרה השיפוטית היא חלשה מדי, משום ש99% מכלל הבקשות להאזנות סתר נענות בחיוב. לכן לדעתי לא צריך להסתפק בצו ראיות מינימאלי, אלא ביהמ"ש צריך לדרוש מהמשטרה **ראיה לכאורה** שנעברה עבירה (סף ראיות גבוה).

צריך להעביר את בקשת צו החיפוש לתגובת צד שלישי אובייקטיבי מעין סנגור ממונה מבית המשפט.

<u>הכלל</u>: ראוי להתנות הליך חיפוש במחשב בצו שיפוטי.
<u>החריג</u>: במצבים של סכנה מיידית לחיי אדם ולרכושו – אין צורך בקבלת צו חיפוש וגורם שלטוני יכול לחדור אל מחשב הזולת כאשר הסכנה היא ברורה.

מה שקורה היום שיש שופט ממונה שמביאים לו ערמה של תיקים והוא חותם עליהם?
לכן לדעת המרצה צריך להיות עו"ד לא מבית המשפט, שהוא מייצג את הצד השני.

Ex parte (צד), במעמד צד אחד. רוב הבקשות להאזנות סתר מתקבלות בחיוב היות ויש רק צד אחד.

לדעת המרצה, יש צורך לחשוף תיקים שלא הוגשו כתבי אישום בגינם לאחר 5 שנים וזאת כדי ליצור הרתעה על המשטרה, במיוחד כלפי פוליטיקאים. יש מערכת שנקראת **אשלון**, צלחת לווינית ענקית והיא מחפשת רשימה של אנשים חשודים לפי מילות מפתח. לדעת המרצה, **צו האזנה צריך להיעשות ע"י מומחה מטעם ביהמ"ש. ע"י צד שלישי אובייקטיבי** וזאת כדי לוודא שזכויות הפרט נאכפות כמו שצריך. אם הצו חיפוש מורחב יתר על המידה הוא אינו תקף וזאת עקב פרי העץ המורעל. זה לא קיים היום בחוק המחשבים, ונותרת שאלה פתוחה, מה לגבי אתרי אינטרנט? עד לאיפה נרשה התערבות של גורמי האכיפה בכל הקשור לאתרים.

הצעת חוק התקשורת בזק ושידורים (סינון אתרים המציגים דברי תועבה באינטרנט 2016), שמציעה שספק גישה לאינטרנט יספק למינויו כברירת מחדל שירות סינון תכנים. מצד אחד זה מגן על קטינים, מצד שני זה יוצר רשימות שחורות על אנשים שרוצים מידע על תועבה וזה עלול לפגוע בפרטיות שלהם.

תזכיר חוק הסרת תוכן המהווה עבירה מרשת האינטרנט 2016, קובע כי כל תובע ואדם פרטי יכול לפנות לביהמ"ש לבקש להסיר תוכן מאתר אינטרנט אם הפרסום מהווה עבירה פלילית ועלול לסכן באופן ממשי את ביטחונו של אדם או המדינה.

הצעת חוק נוספת: **הצעת חוק הסרת פרסום הסתה שהתפרסם ברשת החברתית המכוונת 2016.**
פורסמה הסתה לטרור ברשת החברתית, יסיר מפעיל הרשת החברתית תוך 48 שעות, ואם לא יקבל קנס של 300,000 דולר.

מתי ניתן לאפשר לגורמים שלטוניים למנוע גישה לאתרים פוגעניים או להסיר מידע פוגעני?

בפרשת reno ביהמ"ש אמר לא, אני אוסר על חוק שאוסר הקמת אתרים פונוגרפים ברשת וצריך לאשר את חופש הביטוי הפורנוגרפי.

שאלה לדוגמה:

הנכם חברי ועדת הטכנולוגיה של הכנסת, חברת הכנסת כהן העלתה לדיון בוועדה את הצעת החוק הבאה: "כל פוסט שמועלה לרשת החברתית והמבטא כנגד הדת של אזרחי ישראל יגרור קנס של מיליון ₪, אלה אם כן הנהלת הרשת החברתית תסיר אותו בתוך 3 ימים".

א. מהם מאפייניה הייחודיים של הרשת בכלל ושל הרשתות החברתיות כדוגמת פייסבוק בפרט?(מבוא ופרק חופש הביטוי)
ב. במה הן שונות מכלי שונות רגילים?
ג. על אליו ערכים באה להגן הצעת החוק?
ד. באילו ערכים היא פוגעת?
ה. הציעו הצעת חוק משלכם.
ו. נמקו את היתרונות שבהצעת החוק ופרטו מדוע היא ראויה.

<u>תשובה:</u>

א. כלי חופש הביטוי לאנשים פרטיים, תפוצה גדולה, פס"ד reno, אפשרות לבחור את התוכן שאליו נחשפים.
ב. הרשת תמיד זמינה, אין כמעט צנזורה (רגולציה=אסדרה, חוק רשות השידור, רישוי פיחת אמצעי תקשורת), כל אחד אומר מה שהוא רוצה.
ג. זה בא להגן על הזכות לשוויון, אולי זה בא למנוע הסתה וקדושת החיים.
ד. חופש ביטוי (שופכים פה את כל היחידה של חופש הביטוי- פס"ד reno, ש"ס, רמי מור).

*****(אם יש שאלה פתוחה של נמקו או פרטו/הביעו את דעתכם, צריך תמיד ללכת לשיעור המבוא ואחר כך לעמוד על היתרונות והחסרונות בהתאם ליחידות שנלמדו ואחר כך צריך להביע את דעתנו ולנמק אותה).**

באירופה הייתה פרקטיקה שנקראה "**data retention directive**" שחייבה את ספקי התקשורת לשמור נתונים של הלקוחות שלהם.
יתרונות: שמירת ראיות. **חסרונות:** פגיעה בפרטיות.

בית הדין לצדק של האיחוד האירופי קבע שמכלול נתוני התקשורת של הפרט מספק מידע מדויק ומפורט על חייו האישיים של הפרט, הרגלים ואורח חיים, פעילויות ויחסים חבריים, לפיכך אגירת נתוני התקשורת באופן המאפשר לשלטונות לקבלם פוגעת באופן משמעותי לזכות היסוד לפרטיות והגנת המידע. זוהי פגיעה חמורה בזכות יסוד. פגיעה זו אומנם נועדה לשרת תכלית ראויה שהיא **מניעת פשיעה וטרור והגנה על שלום הציבור**. אך עדיין על הפגיעה להיות מידתית.
נקבע שהדירקטיבה גורפת מידיי ואינה מידתית, שכן היא מחייבת לשמור על נתוני התקשורת של כולם, ללא חשד כלשהו כנגדם, ללא יוצאים מן הכלל, ללא הבחנה בין סוג המידע (למשל בין נתוני מקום ופירוט שיחות) וללא קביעת ערובות אפקטיביות להגנת המידע מפני ניצול. לאור זאת בית הדין ביטול את הדירקטיבה וזה נקבע בפרשת**digital rights data retention case.**

עיקרון סודיות המידע:

ההצדקות ל-למה לא להיכנס למחשב הזולת ללא הסכמתו:

א. פרטיות

ב. קניין

ג. חופש ביטוי

ד. אוטונומיה

הסייגים לעיקרון סוגיות המידע:

למה שהחוק יאפשר גישה למחשב הזולת ללא הסכמתו\ידיעתו?

א. ביטחון המדינה ואזרחיה, אכיפת החוק.

באיזה אופן משיגים את האינטרסים הראויים להגנה?

ראיות, אופן, פרוצדורה...

פרופורציונאלי, התגוננות, פיקוח על גורמי אבטחת סייבר(לא קיים כיום), וועדות אתיקה, צו ביהמ"ש זמני.

אינטרסים הראויים להגנה:

אינטרס קנייני, חיי אדם, חינוך, פגיעה בחברה בכללותה, זליגה לחברות פשע, היבטים כלכליים, הפרה של זכויות יוצרים והגנה על השם הטוב.

פס"ד גיל שוויד(דוגמא לאינטרס של "אבטחת מידע") –

בעלים של חברת אבטחת מחשבים לכל החברות הגדולות. הוא העסיק 500 מהעובדים שלו בשביל לבדוק האם אפשר לחדור אל ה"איי רובוט" ומה הם כשלי האבטחה שלו. הם גילו שניתן לחדור אל ה"איי רובוט" ממרחק.

יש גם דרכים חוקיות\לגיטימיות אחרות לעבוד בהן – למשל, הפעיל אנשים שמנסים לחדור לאתרי אינטרנט בשביל לראות האם פרטי הלקוחות שנמצאים באותם אתרי אינטרנט מוגנים.

בשאלה במבחן יש להתייחס אל היסודות האלה:

1. חשיבות המחשב: מבוא – כלי אחסון של מידע, כלי שליטה ובקרה...
2. למה לא לחדור למחשבים
3. למה לאפשר לגיל שוויד לחדור למחשבים
4. מה האינטרס שראוי להגנה? – קנייני, חיי אדם, חינוך...
5. באיזה אופן נאפשר את החדירה למחשבים?

פרשת מזרחי –

בפרשת מזרחי דובר בבחור שנתקל במודעת דרושים של המוסד. הבחור רצה לשלוח את קורות החיים שלו לאתר המוסד והוא חשש שמא אתר המוסד אינו מאובטח כנדרש. לכן הוא החליט לבדוק האם אתר המוסד מאובטח כנדרש, הוא נכנס לאתר של האקרים והוריד תוכנה שבודקת אמידות של אתרים מפני מתקפת "דוס". מה קורה אם תוקפים את האתר, איך האתר מגיב?

כעבור יומיים המוסד עצר את הבחור. במשפט, השופט דר׳ אבי טטנבויים מזכה אותו מכיוון שעיקר הטענות הן שהבחור עשה ׳משהו טוב׳, השופט מתייחס לכך שהאקרים שהם ב״כובעים לבנים״ באים להתריע מפני כשלי אבטחה. מלומדים רבים בארץ מסכימים עם השופט טננבויים.

המשך אינטרסים הראויים להגנה: **הזכות לשם טוב.**
בפרשת רמי מור דובר במטפל הוליסטי שראה שאחד הטוקבקיסטים השחיר את שמו באינטרנט. הטוקבקיסט כתב את הביקורת שלו בצורה אנונימית, בעילום שם.
רמי מור עותר לבית המשפט בשביל לקבל את כתובת ה-IP של הטוקבקיסט (זה סוג של חדירה למחשב).
מצד אחד כשאנחנו מבקשים צו חיפוש למצוא טוקבקיסט אנונימי שכתב דעה, אנחנו פוגעים בחופש הביטוי שלו ובזכות שלו לפרטיות. מהצד השני עומדת זכותו של רמי מור לשם טוב.
השופט ריבלין בדעת רוב מבצע איזון בין שתי זכויות אלו בית המשפט העדיף את הזכות לחופש הביטוי.
שופט המיעוט אליקים רובינשטיין כותב בפסק דינו כי נהפך האינטרנט למקום שבו ״כל דאלים כבר״(????), כלומר, ידו של הבריון עליונה. כל אחד יעשה מה שהוא רוצה.

מצד אחד עומדת ״הזכות להישכח״(שהוכרה באירופה) ומנגד עומדת הזכות ל״חופש המידע״.

ראוי שהדין יאסור חדירה לא מורשית למחשב הזולת שכן חדירה שכזו פוגעת ב4 זכויות אדם: פרטיות, קניין, חופש ביטוי ואוטונומיה.
גם בעיקרון סודיות המידע יש יוצאים מן הכלל, למשל לאתר אינטרנט פתוח מותר להיכנס גם בהיעדר הסכמה.

הסייגים לעיקרון סודיות המידע
1. מתי גורמים ממשלתיים כמו המשטרה יכולים לחדור למערכות מחשבים?
2. צידוקים לחדירה אזרחית למערכות מחשבים, כלומר, מתי אדם א׳ יכול לחדור למחשב של אדם ב׳?
מנינו שורה ארוכה של אינטרסים לגיטימיים של הפרט אשר מצדיקים חדירה למחשב הזולת ללא הסכמתו ולעיתים גם ללא ידיעתו, והם:
הזכות לשם טוב, פגיעה בקניין, פגיעה בפרטיות, הזכות להישכח, הזכות לתיקון מידע לא מדויק שנמצא באתרים.
בכלל הזכות לשם טוב ניתן להתייחס גם לביטויים פוגעניים שיכול להיות שהם נכונים, כמו במקרה של **אריאל רוניס**, מנהל מרשם האוכלוסין בת״א שהואשם בגזענות בפוסט בפייסבוק אשר הפך לפוסט ויראלי. אריאל רוניס כל כך נפגע מהפוסט הזה ולכן התאבד.
אם אין אפשרות לבקש צו הסרה מגיעים למצבי קיצון. גם מקרים של הצלת חיים, חשש מאדם

שכותב שהוא רוצה להתאבד, או חשש לחיו של אדם שלא חזר הביתה מצדיקים לפעמים חדירה למחשב וגם את הצורך למנוע פירצות אבטחה במחשבים(גיל שוויד).

כלומר, "הזכות לסודיות המידע הממוחשב" איננה זכות מוחלטת אלא זכות יחסית.
גישה מעין זו עולה בפרשת **אייל שגב נ' ויז מגי'ק**, שם אומר בית המשפט שלעיתים למעסיק יש זכות לחדור למחשב של העובד שלו. במקרה הזה, המעסיק ביקש להגיש כראיה דואר אלקטרוני שתראה שהעובד הקים מידע מתחרה והשמיד מידע מוחשב של המעסיק. בית המשפט קבע שהזכות לפרטיות של העובד איננה מוחלטת אלא יחסית.
בפרשת רמי מור לעומת זאת, העדיף בית המשפט את הזכות לפרטיות וחופש הביטוי של הגולש האנונימי על פני הזכות לשם טוב של רמי מור. השופט ריבלין בדעת רוב קבע כי אומנם האנונימיות ברשת איננה חזות הכול והאינטרנט הינו מערב פרוע שאין דין ואין דיין בו, אולם, אין בחוק בישראל פרוצדורה המאפשרת חדירה למחשב לצורך איתור כתובת הIP של הגולש האנונימי.

המרצה אומרת כי היא איננה מסכימה בכל הכבוד עם עמדתו של השופט ריבלין שכן תקנה 8(7)ה לתקנות סדר הדין האזרחי בחיפוש חומר מחשב מאפשרת פנייה לבית המשפט לצורך קבלת צו חיפוש למחשב.
המרצה מצדדת בעמדת המיעוט של השופט רובינשטיין הקובע שאין בדין הישראלי חיסיון הפוטר ספקיות אינטרנט מחשיפת פרטי משתמשים על דוכן העדים. בייחוד שעה שהאנונימיות מאפשרת מחסה לעושי עוולה(מי שהפיץ לשון הרע). בית המשפט אומר כי "העלאתה של האנונימיות לדרגת 'מעין קדושה' בגדרי כיכר השוק המודרנית איננה יכולה להפוך אותה למפלטו ומקלטו של הנוול".

עלתה הצעת חוק שתורה לספקי שירות לחשוף שם גולש אך היא עדיין לא הפכה לחוק.
כיום, **התיקון לחוק יסודות המשפט משמש מקור השראה <u>בענייני לאקונה</u>**, התיקון אומר כי **חייב לפנות אל הדין העברי במקרה של לאקונה. והדין העברי אומר שאסור לחדור למחשב, אבל במקרה מסוים הדין במקרה של הצלת חיי אדם או הצלת רכושו של אדם מותר לחדור אל המחשב.**
רבי חיים פלג'י אמר שאפשר לחדור למחשב הזולת לצורך הצלת החיים או הצלת הרכוש, אבל יש לפנות גם **לבית הדין** על מנת לקבל אישור לכך.

ישנם אינטרסים לגיטימיים המצריכים לפעמים חדירה למחשב הזולת(גם לאזרחים).
מה הן הדרכים הראויות לאיזון בין האינטרסים השונים?
1) באמצעות צו בית משפט וחקיקה מתאימה: אם רוצים לחדור למחשב הזולת צריך לעשות זאת באמצעות צו בית משפט.
באירופה יש את ההתייחסות ל"זכות להישכח" המורה כי מידע צריך להימחק ללא דיחוי אם אין בו כבר צורך או אם חזרו מהסכמה לפרסומו.
2) אסדרה של אתרים שיתנו מקום לנפגעים: למשל, בפיסבוק יש אפשרות לדווח על פוסט פוגעני(גם ביוטיוב).

3) ועדות אתיקה על האקרים או חברות אבטחה(גם באוניברסיטאות) שלא ישבו בהן בהכרח גורמים שלטוניים. – זו שאלה פתוחה.

כיום ישנם מספר הצעות חוק שמבקשות לקבוע שניתן יהיה לעצור או לחשוף אתרים שונים שיש בהם פגיעה בתוכן. למשל, הצעת חוק "חשיפת זהותו של מפרסם תוכן ברשת תקשורת אלקטרונית"(2012).

לדעת המרצה, כאשר אנחנו מדברים על אסדרה של גופים שמפרסמים בהם מידע פוגעני, **יש מקום לאמץ נוהל של הודעה לספק הגישה שיעביר הודעה למחבר הידיעה שיש בקשה למחוק את הפוסט שלו**, ומחבר הידיעה יוכל לעתור לבית המשפט בשביל לקבל צו מניעה. כל זאת יתאפשר רק כאשר ישנה **"ראייה לכאורה"** לעוולה.
המרצה חושבת שהחוק כן צריך לחייב איזשהו מנגנון פניה לאתרים שמכילים מידע פוגעני או עוולתי.

סעד עצמי

מה ניתן לעשות אם אין זמן לפנות אל בית המשפט במקרים כאלו?
"סעד עצמי" – ניתן לפעול על דעת עצמך ללא דיחוי.
גם בדיני המחשבים ראוי לאפשר סעד של עשיית דין עצמי או "עזרת גומלין"\"עזרה לזולת".

תנאים לחדירה אל מחשב הזולת גם בהיעדר חוק ספציפי בנושא:
הדין הזה לא כתוב עלי ספר, הם נכנסו דרך הפסיקה לדין הישראלי, וגם דרך סעיף 18 לחוק המקרקעין + חוק המיטלטלין המאפשרים לחדור אל מחשב הזולת בתנאים שלהלן:

<u>ראשית</u>, מדובר בהגנה מיידית מפני פגיעה, כלומר, אין אפשרות לדחות את הפעולה עד לפנייה בבקשה להתערבות שיפוטית או משטרתית. חייבים לפעול מיד.
<u>שנית</u>, הפניה לרשויות איננה אפשרית, יעילה, או מעשית.
<u>שלישית</u>, מדובר במצבי הגנה ולא התקפה – "מגן ולא חרב".
רביעית, הפעולה נעשית לא מתוך זדון או רצון להציק או לנקום.
<u>חמישית</u>, סבירות הצעדים שננקטו
<u>שישית</u>, סיכויי ההצלחה של ההתערבות העצמית. אם הסיכוי הוא אפסי זה לא מצדיק.
<u>שביעית</u>, הרלוונטיות של המידע שנאסף.
<u>שמינית</u>, מדובר בפגיעה נקודתית בזולת ולא בהפרה שיטתית של חירויות הזולת.

שיעור של ברק

ישנם שלושה חוקים עיקריים שמתייחסים לסוגיה של סייבר:

1. חוק הגנת הפרטיות.
2. חוק האזנת סתר.
3. חוק המחשבים.

סעיף 3 לחוק הגנת הפרטיות קובע שהחוק הו אזרחי ופלילי.
היסודות העובדתיים של חוק הגנת הפרטיות:
סעיף שלוש קובע **יסוד נפשי(זדון) - מודעות לעובדות ולנסיבות.**

סעיף 1 לחוק, קובע שאין לפגוע בפרטיותו של אדם ללא הסכמתו.

חשוב מאוד!!

המבנה של חוק הגנת הפרטיות:

סעיף 1- איסור פגיעה בפרטיות

סעיף 2- מחולק לסעיפים קטנים מסביר מהי פגיעה בפרטיות.

סעיף 18- לחוק הגנת הפרטיות נותן הגנה, כלומר אדם פגע בפרטיות יש לו הגנה בסעיף זה.

סעיף 32- קובע מתי אסור להגיש ראיה שהושגה תוך פגיעה בפרטיות.

בפרשת פלוני נגד מדינת ישראל, היה מדובר על אדם שחדר למחשב לטובת הדואר של המתלוננת וקרא את המיילים שלה. בית המשפט אומר כי העובדה שהיא לא הגנה על המיילים זה לא משנה את רמת האבטחה.

סעיף 2 לחוק קובע <u>שפגיעה בפרטיות היא אחת מאלה</u>:

1- **"בילוש או התחקות אחרי אדם העלולים להטרידו או הטרדה אחרת"**
בפרשת וקנין היה מדובר בעציר שהשקו אותו במי מלח בשביל שיפלוט מגופו סמים שחשדו שהוא שתה. עו"ד של העציר רצו לאסור את הראיה כי הם טענו שהייתה פגיעה בפרטיות שלו. אומר ביהמ"ש שהסעיף מתייחס לפגיעה בפרטיות במבנה הייחודי ואין כולל פגיעה פיזית באדם מכיוון שזה נדון בחוק העונשין. הסעיף אינו מוכן לכלול מעשה תקיפה שיש בו אלימות. ביהמ"ש אומר שבילוש כוללים גם מעשים שנעשים בפרהסיה (ללכת אחריו ברחוב).
גישה רחבה- לא הוגבלה לחדירה פיזית.
הגנה מפני טכנולוגיה מודרנית, המאפשרת חדירה לפרטיותו של אדם ממרחק.

הגנה אקסטריטוריאלית- אינה קשורה למרווח קנייני ספציפי. שאלת המקום והקניין אינה רלוונטית.

*מקורה מחוץ לטריטוריה שלו בתנאי שיש לה נפקות על הפרט.

לדעת המרצה- כוללים גם חדירה למחשב של אדם, הם כוללים ניטור ואן-אק, מכל מחשב נובעת קרינה אלקטרו-מגנטית, את הקרינה ניתן לאסוף ע״י מכשיר שניתן לבנות בבית, ועל צג הטלוויזיה ממקום אחר ניתן לראות את כל הנעשה במחשב.

מה ההבדל בין לחדור למחשב לבין לקלוט את המחשב- אין פה פלישה, השגת גבול.

סעיף 2(1) הוא מאוד רחב כי הוא אינו דורש חדירה למחשב, שאלת המקום והקניין אינה רלוונטית ולכן זהו סעיף רחב מאוד והוא נותן גם מענה לבעיית החדירה למחשב.

שמישהו נכנס לאתר סתמי האם יש פה בילוש או התחקות? - מספיק שצופים לאדם במחשב כל היום זה מטריד אותו. אך הנושא עדיין פתוח וגדול האם בוחנים זאת אובייקטיבי או סובייקטיבי.

ניתן לצמצם את **סעיף 2**- נניח שא׳ צופה באתר ספורט, וב׳ צופה לו במחשב אך הוא לא התכוון לצפות לא׳ הוא מתכוון לצפות לב׳.

הכוונה היא לשורה של מעשים, מגמה של מעקב, ואילו במקרה הזה מדובר במעשה אקראי ולדעת המרצה **<u>סעיף 2(1) לא חל על מעשה אקראי.</u>**

בפרשת מדינת ישראל נגד שפירא: היה מדובר בסמנכ״ל תקשורת לשעבר של חברת תקשורת גדולה, הסמנכ״ל ישב בבית חצי שנה והשתעמם, נכנס למחשבי החברה עם הסיסמה שלו הישנה וביהמ״ש האשים אותו כי זה הטריד את האנשים אשר הפרטים שלהם מאוחסנים במחשב.

היה ניתן לטעון כי **לא החליפו לו את הסיסמה ולכן הייתה כאן הסכמה.**

טענה נוספת שיכולה לעזור לשפירא- סעיף 2(1) מדבר על בילוש או התחקות אחרי אדם העלולים להטרידו או הטרדה אחרת, **סעיף 3** לחוק הגנת הפרטיות, מגדיר אדם למעט תאגיד. אחרי אדם ולא תאגיד. אך ניתן לטעון כי אומנם מדובר בתאגיד אולם באתר החברה יש פרטים של אדם, ניתן לגשת לחוק כבוד האדם וחירותו שם **מוגדר אדם לרבות תאגיד.**

יש בפסיקה מספר גישות לשאלה: מה נחשב ל- ״תאגיד״?

גישה ראשונה:

מתעלמת מכל הנושא הזה, מתעלמת מאי תכולתו על תאגיד. **בפס״ד צדוק** ביהמ״ש התעלם מהשאלה האם מדובר בפריצה לרשות המיסים של התאגיד.

גישה שנייה:

באה לידי ביטוי **בפרשת נוואי נגד יושב ראש הכנסת**: אדם לא כולל תאגיד כמושא לפגיעה בפרטיות.

גישה שלישית:

פרשת סקולר נגד ג'רבי, הזכות לפרטיות מוגנת גם בכבוד האדם וחירותו ואנחנו נפרש אותה בהרחבה לפי חוק יסוד: כא"ח שבו הזכות לפרטיות מגנה גם על תאגידים.

גישה רביעית:

עמדת המיעוט של השופט חשין (**בפרשת סקולר**): כאשר תאגיד מחזיק מידע של אנשים פרטיים ויש חדירה למחשב של התאגיד וגילוי פרטים על אנשים פרטיים, אדם בשר ודם הוא זה שנפגע.

לכן יש מקרים שבהם לא תהיה תחולה של חוק הגנת הפרטיות על חדירה לפרטיות למחשב כמו בפרשת **ד"ר רום:**

פס"ד ד"ר רום -

היה מדובר על רופאה שעבדה במשרד הבריאות וביקשו ממנה לתרגם את המבחן לעברית לרוסית, היא העתיקה את הבחינה ונתנה את הדיסקט לבעלה והוא תרגם את הבחינה לרוסית ומכר את הבחינה לנבחנים רוסים, הוא מחק את המבחן ובמהלך הבחינה גילו העתק בתיק של אחד הנבחנים ולאחר חיפוש בבית שיחזרו את הבחינה ואיתרו את זה. אך לא הגישו כתב אישום כי היה מדובר בתאגיד.

סעיף 2(2) - הוא סעיף נזיקי, אי אפשר להגיש בגין הפרתו כתב אישום.

סעיף 2(5) - העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו; לענין זה, "כתב" – לרבות מסר אלקטרוני כהגדרתו בחוק חתימה אלקטרונית, התשס"א-2001;

<u>מחלקים סעיף זה ליסודות:</u>

כתב: <u>האם ווטסאפ נחשב לכתב? כן!!</u>

להבנת המרצה: גם ניטור קרינה אלקטרו מגנטית היא סוג של כתב, כי מישהו יכול לקלוט את זה ולפענח את זה. לא שמים בסעיף דגש על התוכן של הכתב, לא משנה מה התוכן אך שלא נועד לפרסום.

העתקת תוכן של מכתב או כתב אחר:

העתקה זה למשל באמצעות הרוגלה, צילום מסך. אם אדם היה ניגש לכתובת פותח וקורא זה לא נקרא העתקה. גם הכנסת (התקנת) הרוגלה היא לא העתקה, רק ברגע שהרוגלה העבירה לו מסר לפלאפון שלו יש העתקה.

למרות שהמונח אדם כ-"בשר ודם" לא מופיע בסעיף 2(5) בתי המשפט קבעו:

בפס"ד חוגלה היה עובד שנכנס למחשב של המעסיק ובמחשב שלו מופיעים המיילים של המעסיק, הוא קרא אותם וסיפר למישהו אחר. עו"ד של פריאל טען כי זה תאגיד ולא אדם. ביהמ"ש מקבל את זה אף שהמילה אדם לא חל בסעיף 2(5) לא צוין אדם.

בפס"ד בנק מזרחי נ' שאולי לא מכיל את **סעיף 2(5)** על מסמך של מנכ"ל בבנק.

שבהם בית המשפט מסרב להכיל סעיף זה על חדירה למיילים עסקיים.

אך מנגד יש **פס"ד מולטילוק, וקייסרית נגד ערערת** שבהם כן ניתנה הגנה למיילים של תאגיד.

אם א' שולח לב' מייל וב' מעביר לג'- האם יש העתקה? כן!
האם יש פה העבירה? התקיים היסוד של כתב אחר, התקיים היסוד של ללא הסכמה, התקיים היסוד של העתקה, אבל יש פה הגנה – "ללא רשות של הנמען או הכתוב".
ב' הוא הנמען ולכן הוא יכול להעביר את המייל.

בדין העברי ההעברה היא אסורה
אך במשפט הישראלי אמרו שזה קשה מדי ולכן מתירים.

סעיף 18- במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(2) הנתבע או הנאשם עשה את הפגיעה **בתום לב** באחת הנסיבות האלה:

מה זה תום לב?
בפרשת גילת דעת הרוב קבעה שיש לבחון את עיקרון תום הלב באמצעות מבחן אובייקטיבי סובייקטיבי. הייתה פריצה לבית, הלכו מכות, צילמו אותם בחדרי חדרים ונקבע שלא היה תום לב.

בפרשת פלונית נגד בית הדין הרבני האזורי היה מדובר על סיפור דומה, האישה עם הידיד שלה במרתף של בית המגורים המשותף, הבעל כבר לא גר שם ונכנס לבית למרתף ומצלם אותם וטוען לתום לב. הנשיא ברק אומר, תום הלב הוא סובייקטיבי. אבל הוא אומר שזה צריך להיות מידתי.

פרשת צוקרמן ביהמ"ש אומר שכשהוא בודק את יסוד תום הלב, הוא בודק האם הם היו **מודעים** לאלטרנטיביות חוקיות ומידתיות, המובילות **למינימום פגיעה בפרטיות**?
האזנת סתר לפעיל בוועד עובדים, המעסיקים טוענים לטענתם שהם עושים את זה בחשד שהוא גנב ולכן הם אומרים שהם פעלו בתום לב, **ביהמ"ש אומר שהיו אלטרנטיביות חוקיות והיו יכולים לפנות למשטרה.** וזה מזכיר סעד עצמי והוא לא מתקיים כשאפשר לפנות למשטרה ולרשויות.

(2) הנתבע או הנאשם עשה את הפגיעה בתום לב באחת הנסיבות האלה:

(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות- לא מתקיים אצל אהרון

(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה- להציל אנשים כמו עם החיילת שכתבה שהיא הולכת להתאבד.

(ג) הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע;

(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה) הפגיעה הייתה בדרך של צילום, או בדרך של פרסום תצלום, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע, תשכ"ה-1965;

מה למדנו:

א- מבוא

ב- הרקע הנורמטיבי:

1- פגיעה בפרטיות

2- בקניין.

3- מחופש הביטוי.

4- האוטונומיה.

5- מתי לאפשר חדירה = הסייג ללא הסכמה למחשב.

ג- הדין הקיים:

1- חוק הגנת הפרטיות סעיפים: 1, 2(1), 2(5), 3.

2- סייגים להגנות הפרטיות ס' 18 לחוק הגנת הפרטיות.

ד- חוק המחשבים.

ה- חוק האזנת סתר.

סעיף 18 לחוק הגנת הפרטיות אומר:

במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(1) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, תשכ"ה-1965;

(2) הנתבע או הנאשם עשה את הפגיעה בתום לב באחת הנסיבות האלה:

(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;

(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה;

(ג) הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע;

(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה) הפגיעה היתה בדרך של צילום, או בדרך של פרסום תצלום, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע, תשכ"ה-1965;

(3) בפגיעה היה ענין ציבורי המצדיק אותה בנסיבות הענין, ובלבד שאם היתה הפגיעה בדרך של פרסום - הפרסום לא היה כוזב.

<u>שני מקרים:</u>

1- מעסיק פותח את המחשב של העובד שלו, ורואה שהוא מעביר סודות מסחריים.
2- איתוראן.

הסעיף אומר שיש מקרים בהם מותר לפגוע בפרטיות של הזולת, אך מתי?

התנאי הראשון הוא תום לב - בפרשת גיל עם, היה מדובר בבעל ואישה שנמצאו בהליכי גירושין, האישה רוצה להוכיח שהבעל בוגד בה והיא רואה שוטר... ביהמ"ש אומר שיש עבירה על החוק אין כאן משהו שנעשה בתום לב.

בצוקרמן- אומר בית המשפט אין עילות בתום לב אם היו אלטרנטיבות פוגעות פחות.

בפלונית נ' בית הדין הרבני האזורי בנתניה - היה מדובר בבעל ואישה שהיו בהליכים, האישה נשארה בבית והבעל עזב, הבעל נכנס לבית המשתף שהוא לא גר בו ומצלם את האישה במרתף,

הוא רוצה להגיש את זה כראייה בבית המשפט. ביהמ"ש אומר שאין פה תום לב (בג"צ), יש פה פגיעה חריפה וקיצונית בפרטיות. בג"צ קובע שהתמונות לא כבילות.

ביהמ"ש קורא לתום הלב דרישה סובייקטיבית- זאת פעולה מתוך אמונה כי הפגיעה היא במסגרת ההגנה שאותה מעלה הפוגע, לכאורה זה סובייקטיבי. אך בית המשפט מוסיף שמקום שבוא הפגיעה בפרטיות אינו מידתית יש הנחה של חוסר תום לב, אך הוא אומר זאת לפי סעיף 20 לחוק הגנת הפרטיות מדובר על פעולה החורגת מגבול הסביר, מה שחורג מתחום הסביר לא נעשה בתום לב.

פרשת איסקוב - היה מדובר בעובדת מפטרים אותה ואז נודע לה שהיא בהריון, היא מחפשת עבודה אחרת באימייל ואז היא תובעת המעסיק כי הוא פיטר אותה כי הוא בהריון ואז הוא אומר שהוא לא ידע וכראייה הוא מוציא מייל שמראה שהיא חיפשה עבודה אחרת לפני שידעה שהיא בהריון.

סעיף 18 לחוק הגנת הפרטיות: הוא פעל בתום לב, ופעל כדי להגן על האינטרסים של עצמו. בית הדין אומר כי יחולו בדווקנות וצמצום. אומר בית הדין כי הגנת תום הלב עמומה ולכן הוא מחליט לפרש את זה בצמצום.

בית הדין מצמצם את תום הלב בגלל עמימותה, בית הדין קובע שלוש הנחות מוצא בהם מותר למעסיק לחדור למחשב של עובד שלו:
1- למעסיק יש זכות לקבוע האם לעובדים יש את האפשרות להשתמש באינטרנט צרכים פרטיים.
2- השימוש באמצעים אלקטרוניים, ניתנים לשימוש למטרות עבודה ולא לצרכים אישיים. 3- חדירת מעסיק מהווה פגיעה בפרטיות.

מתי מעסיק יכול לנטר את התיבה המקצועית של העובד? – להשלים-

העובד צריך להסכים לכל פעולה שנעשתה ולהיות נוכח. הסכמה מדעת, חופשית וכו'.

אבל אם בתיבה המקצועית נעשה שימוש גם לצרכים פרטיים, המעסיק לא רשאי להיכנס למייל. ובתכתובת אישית אי אפשר להיכנס לנתנוניתוכוואסור לחדור לתיבה פרטית אלא בבקשת צו במעמד צד אחד אנחנו מבקשים להיכנס לעובד. אם זאת תיבה מעורבת אי אפשר לנת

(להשלים את התיבות)

בפרשת יהודה זינגר - היה מדובר במעסיק שמעביר את המחשב למישהו אחר ורואה מייל מחשיד, אדם שנחשף באופן מקרי ופסי להודעת דואר אלקטרוני של הזולת כנראה שמגיעה לו הגנה של סעיף 18, הדבר תלוי כל מקרה לגופו, אומר בית המשפט בשביל ליזום חיפוש וחיטוט בתיבת דואר האלקטרוני צריך לקבל צו שיפוטי כולל. אבל לפעמים שלא מדובר על מעקב יזום שעורך מעביד אחרי עובד, אלא כמו במקרה הנ"ל החשיפה מקרית די בעצם החשיפה כדי לבסס את הצורך בהגנה על עניין אישי כשר ללא צורך לצו שיפוטי, ומי שנחשף להודעות יהיה רשאי להעתיקם ולהשתמש בהם לראייה, הדבר נתון בכל מקרה לגופו ובמידת הדחיפות.

אם אדם נחשף להודעה שיש בה כדי לעורר חשד בעניין אישי קשר אין די בכך כדי לבסס את ההגנה בסעיף 18 ועליו לפנות לקבל צו, ... להשלים

בית המשפט אומר- (תום לב) אני מבדיל בין המקרה של איסקוב למקרה זה, פה לא היה מעקב יזום. דבר שני,

לא מספיק כדי להפעיל את סעיף 18 כדי שיהיה פה תום לב, אפשר להפעיל אותו בתום לב (אובייקטיבי סובייקטי, מיעוט- סובייקטיבי).

<u>סעיף 32 לחוק הגנת הפרטיות:</u>

חומר פסול לראיה

32. חומר שהושג תוך פגיעה בפרטיות יהיה פסול לשמש ראיה בבית משפט, ללא הסכמת הנפגע, זולת אם בית המשפט התיר מטעמים שיירשמו להשתמש בחומר, או אם היו לפוגע, שהיה צד להליך, הגנה או פטור לפי חוק זה.

הסעיף אומר: אם אתם רוצים להגיש את הראייה בפרשת נחמיאס, יש לבדוק האם הייתה פה פגיעה סעיף 32 2(1), 2(5), אחר כך צריך לבדוק האם עמדו לו הגנות ס' 18.

ואז בסעיף 32 אנחנו צריכים להוכיח כדי שלא יאפשרו, אין הסכמה של הצד השני להגיש את זה אך זולת אם בית המשפט מאשר מטעמים שירשמו.

פסקי דין על סעיף 32- פרשת יהב חמיאס (לקרוא בבית).

בפרשת גורלניק- בחורה שדיברה עם חברה בקיר של הפייסבוק והמעסיק לקח לה את הטלפון הסלולרי- בית הדין לעבודה אומר כי גם שפונים לקבלת צו אנטון פילר, בית הדין ייתן את זה רק במקרים ממש מצומצמים ובנסיבות חריגות.

מתעלמים לגמרי מכל מה שכוב בסעיף 8 לחוק הגנת הפרטיות.

חוק המחשבים:

סעיף 4-

חדירה לחומר מחשב שלא כדין

4. החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו - מאסר שלוש שנים; לענין זה, "חדירה לחומר מחשב" - חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר, תשל"ט-1979.

היסודות של סעיף 4:

1- חומר מחשב.
2- מה זה מחשב?
3- חדירה למחשב- למעט חוק להאזנת סתר.
4- המונח שלא כדין.
5- יסוד נפשי.
6- אין צורך בהוכחת נזק.

למה צריך עבירה חדירה למחשב- קשה לאתר עבריינים של מחשבים ולכן אנחנו תופסים אותם רק בשלב הראשוני.

היסוד הנפשי לא מצויין ברכיבי העבירה ולכן שמדובר בעבירה שותקת היסוד הנפשי הוא מסוג **מחשבה פלילית,** וזאת עפ"י סעיף 19-20 לחוק העונשין.

בתי המשפט לפעמים מתבלבלים ברכיב הזה

בפרשת מזרחי- היה מדובר באדם שהכניס והפעיל תוכנה שבודקת עמידות של אתרים, בית המשפט אומר הוא לא באמת הרס את המחשב ואני חושב שמה שהוא עשה זה דבר טוב, הוא רצה לבדוק המחשב עמיד בפני התקפות וזה טוב שאקרים יבדקו אתרים לפני התקפות.

1- **חומר מחשב-** מידע או תוכנה, מידע- נתונים, סימנים, מושגים או הוראות, למעט תוכנה, המובעים בשפה קריאת מחשב, והמאוחסנים במחשב או באמצעי אחסון אחר, ובלבד שהנתוניםהבימנים, המושגים או ההוראות אינם מיועדים לשימוש במחשב עזר בלבד. מגינה על כל סוג של מידע ממוחשב לא משנה מה הוא, הסעיף מדבר על חומר מחשב הנמצא במחשב, מכאן אנו למדים כי על החומר צריך להיות בתוך המחשב, במצב נייח.
2- **מה זה מחשב-**
3- **חדירה למחשב-** יכולה להתבצע בשלוש דרכים: 1- התקשרות עם המחשב (תקשורת עם נתונים, טלפון).

מה היא חדירה למחשב – סעיף 4 לחוק הגנת המחשבים:

דרכי החדירה למחשב

- התקשרות
- התחברות
- הפעלה

למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר.

פרשת פילוסוף: החדרה של סוס טרויאני למחשב שמאפשר לצפות בכל הקבצים של המחשב הנגוע.
ברגע ששני החוקים יכולים להיות, גם חוק המחשבים וגם חוק האזנת סתר – לא יחול חוק המחשבים. חוק האזנת סתר גובר.
בחוק המחשבים אין כלל של "פסלות ראיה" (פרשת יהב נחמיאס).
בפרשת בדיר הייתה האזנה להודעה קולית, בית המשפט מתעלם מהסיפא של סעיף 4 לחוק המחשבים בהסכמה, והרשיע גם לפי חוק המחשבים וגם לפי חוק האזנת סתר.

האם וואצפ זה חומר מחשב?
"חומר מחשב" הוא: סימנים, חומרים ואותות המאוחסנים במחשב.

קרינה אלקטרומגנטית לא נכנסת תחת סעיף 4 לחוק המחשבים אלא לחוק הגנת הפרטיות.
אין חדירה למחשב כשמדובר על ניטור קרינה אלקטרומגנטית.
לא' יש בית. בתוך הבית יש מחשב, בתוך המחשב יש אימייל פתוח שכתובים בו דברים. בני נמצא במכונית בחניון ליד הבית של א', יש לו מכשיר וולק(?). המכשיר הזה קולט את הקרינה האלקטרומגנטית היוצאת מהמחשב של א', והוא רואה את מה שמופיע על צג המחשב שלו. זה לא חדירה למחשב – זו קליטה.
אין כאן יסוד של חדירה, אין כאן יסוד של מחשב, הקליטה היא באוויר, והמידע הוא לא מאוחסן.

מה היא "חדירה שלא כדין"?

בפסק דין סלע נקבע כי "חדירה שלא כדין" היא חדירה למחשב ללא היתר שבדין חיצוני.
אפשר להפוך את המונח שלא כדין לטענת הגנה.
על פי המרצה, אפשר לייבא את סעיף 18 לחוק הגנת הפרטיות הוא הדין החיצוני.
פעילות שבתום לב + למען צורך אישי כשר

אין בחוק המחשבים הגנות בניגוד לחוק האזנת סתר. פרשנות אחרת של המונח "שלא כדין" יכולה להיות: **"ללא הסכמה או ללא הרשאה".** אפשר להבין זאת מתוך הצעת החוק ומפרשת בדיר + פרשת ניר עזרא.
<u>קו הגבול הוא יסוד ההסכמה.</u>

אין דרישת פיצוח של מנגנון הגנה טכנולוגי ואין דרישה של נזק בחוק המחשבים, אבל למשל ד"ר בירנהאק במאמרו אומר שיש לפרשם בצמצום את המונח שלא כדין על חריגה, כך שלא יחול על חריגה מהרשאה. שלא כדין זה לא "ללא הרשאה" אלא 'פיצוח מנגנון הגנה טכנולוגי'.
לדעת המרצה אם יש אתר אינטרנט שכתוב בו "לא מרשים למרצות דתיות להיכנס" מכיוון שאתר האינטרנט הוא אתר ציבורי קיימת הסכמה מכללא להיכנס.

בפרשת בדיר בית המשפט מפרש בצורה רחבה את יסוד ההסכמה. אותו דבר נקבע גם בפרשת איסקוב.

חוק האזנת סתר:

סעיף 2(א) לחוק האזנת סתר קובע שדינו של מאזין שלא כדין הוא 5 שנים. (עונש יותר חמור מחוק המחשבים – 3 שנים).

מה היא האזנה?
בית המשפט אומר בפרשת צוברי שלפי סעיף 2(א) לחוק האזנת סתר, חייבים שהאזנה תהיה באמצעות מכשיר. באימרת אגב בפרשת צוברי נאמר גם כי יש עוד חוק שאוסר על האזנת סתר, והוא סעיף 2(2) לחוק הגנת הפרטיות. הסעיף הזה לא מצריך מכשיר לצורך האזנת סתר.
אם מישהו מתחבא מתחת השולחן יכול להיות שנגיד שזוהי האזנת סתר בניגוד לסעיף 2(א) לחוק האזנת סתר.

האם שימוש במחשב הנחדר זה "מכשיר"?
בפרשת **זינגר נ' יהב חמיאס** אומר בית המשפט שאם מוצאים על המחשב הנחדר אימייל זה לא באמצעות מכשיר. כאשר מדובר בחשיפה מקראית להודעת דוא"ל פתוחה המצויה על מסך המחשב, לא ניתן לראות בכך האזנה באמצעות מכשיר.
בית המשפט רואה האזנה באמצעות מכשיר כהאזנה באמצעות חיבור של מכשיר האזנה כלשהו.
בפס"ד זינגר נאמר באימרת אגב כי:
שימוש במחשב של האדם של המיילים שלו חודרים זה לא האזנה באמצעות מכשיר.

שיחה מוגדרת ב"דיבור או בבזק, לרבות בטלפון, בפקסימיליה, הוא בתקשורת בין מחשבים....
האזנת סתר היא גם תקשורת בין מחשבים וגם האזנה לשיחת הזולת.
בסעיף 1 יש הגדרה של המונח 'בזק' – טלקומוניקציה. ← תקשורת ממרחק.
האזנת סתר מתייחסת לשיחת הזולת, תקשורת בדיבור, וגם תקשורת ממרחק ולרבות בתקשורת בין מחשבים. (גם טלפון שהוא לא מחשב עם טלפון שהוא מחשב).
בזק – סימנים, אותות וכו' המועברים באמצעות תיל.
מהביטוי 'המועברים' אנו למדים שהסימנים והאותות צריכים להיות במצב נייד(נד).
המונח 'בזק' מתייחס למידע שזז. לדוג': דואר, הודעה במזכירה הדיגיטלית.

2(א) לחוק האזנת סתר: "האזנה".
2(ב) לחוק האזנת סתר: שימוש בשיחה שנקלטה.
2(ג): התקנת מכשיר האזנה.

פרשת פילוסוף: הבזק\השימוש במחשב חייב להיות חומר נייד ולא נייח.
ההלכה - דרישת הסימולטניות בחוק האזנת סתר היא שרירה וקיימת.
פרשת בדיר(מנוגדת לגישה של פרשת פילוסוף): דרישת הסימולטניות היא לא רלוונטית.
המרצה מסכימה עם מה שנקבע **בפרשת פילוסוף.**

פרשת צוברי: מה שמפריד בין השימוש בדיעבד לבין האזנת סתר זו העובדה שזה סימולטנית לרגע שבו מתקיימת השיחה(=מקביל, בו זמנית). הקליטה היא במקביל ברגע שבה נעשתה השיחה.

הודעה\מייל תקוע.

ניתן לטעון שמדובר באימייל נייד, אפילו שהוא תקוע עכשיו במחשב של הISP.
בשביל להבין זאת אנחנו נשתמש במטאפורת הרמזור,
א' הוא שליח, א' קיבל חבילה, הוא רוצה להעביר לשלי חבילה ליום הולדתה. א' נוסע בדרך – כשהוא נוסע, האם החבילה שלו ניידת או נייחת?
תשובה: החבילה היא ניידת.
כשא' עוצר ברמזור באור אדום, החבילה שלו לכאורה נייחת כי הוא נח ברמזור, אבל החבילה היא ניידת כי רמזורים ועצירות בהם, הם חלק מתהליך המשלוח של המתנה.
כך גם בכל הנוגע לשליחת מיילים והודעות ברשת. כשאנו שולחים הודעה ברשת, חלק מ"המסע" של המייל הוא מעבר בתחנות ביניים כמו המחשב של הISP.
לכן, ההודעה היא עדיין ניידת כל עוד היא לא הגיעה אל היעד שלה.
בפרשת USA בארה"ב נקבע שיירוד(קליטה) של אימייל באיחסון זמני כמו בISP, זה סוג של האזנת סתר. כך נקבע גם **בפרשת פילוסוף** בארץ ישראל:
העתקת דואר אלקטרוני הנמצא אצל ספק השירות שטרם נמשך על ידי מחשב היעד מהווה האזנת סתר!
לעומת זאת,
בפרשת בדיר: בית המשפט קובע שהאזנה להודעה שנקלטה במכשיר קולן היא גם חדירה למחשב וגם האזנת סתר.
מכשיר קולן(=מרכזיה דיגיטלית המשמשת כמזכירה, השארת הודעה בתא קולי).
המרצה לא מסכימה עם הקביעה של בית המשפט בפרשת בדיר.

* מה קורה אם ספק השירות שומר אצלו עותק של המייל והאקר חודר למחשב של ה-ISP ומעתיק משם את המייל הזה? האם יש כאן חדירה למחשב או האזנת סתר?
תשובה: המידע כבר הגיע אל ייעדו, הוא לא "מועבר". ולכן – יש כאן חדירה למחשב כי חומר המחשב נמצא במחשב והגיע כבר אל ייעדו. מייל שכבר מאוחסן במחשב יחול עליו חוק המחשבים.

על פי סעיף 13 לחוק האזנת סתר: יש פסילת ראיות שהושגו שלא כדין על פי דוקטרינת "פרי העץ המורעל".
בפס"ד יהודה זינגר(נאמר בהערת אגב): הכלל של פסילת ראיות לא חל על חוק המחשבים אלא רק על חוק האזנת סתר.

בחוק סדר הדין הפלילי(סמכויות אכיפה-נתוני תקשורת) המשטרה צריכה לקבל צו שיפוטי לצורך קבלת נתוני תקשורת ממאגר מידע של בעל רישיון.
אבל, סעיף 4 קובע שבמקרים דחופים כגון מקרים של הצלת חיי אדם, מותר לקבל מידע גם ללא קבלת צו.

שאלה לבחינה:

אהרון מאוהב בבתיה, הוא רוצה לדעת עם מי היא מתכתבת. הוא נכנס למחשב שלה ולוחץ על "PAGE DOWN" כשהיא הולכת למטבח, והוא רואה לתדהמתו שהיא קיבלה לפני שתי דק' הודעה במסנג'ר מגבריאל החבר שלה לשעבר.

א. אין כאן חדירה למחשב (על פי סעיף 4 לחוק המחשבים) כי אין כאן "מכשיר".
**** לא נכון: אין דרישה ל"מכשיר" בחוק המחשבים!!! רק בחוק האזנת סתר ****
ב. אין כאן האזנת סתר כי המכשיר שבו מדובר הוא מחשב נייח (פרשת בדיר).
זה לא אומר שום דבר שהמחשב הוא נייח.
ג. יש כאן האזנת סתר בשל יסוד הסימולטניות (פס"ד בדיר+סעיף 2(ג) לחוק האזנת סתר)
ד. יש כאן חדירה למחשב (סימנים, אותות... המאוחסנים במחשב)

אם במבחן יש שאלה על ההיבטים הנורמטיביים של חדירה למחשב
= צריך לציין את המבוא, הפגיעה בזכות לפרטיות, בחופש הביטוי,
באוטונומיה ופגיעה לקניין והסייגים. ולא את הדין הקיים!!!