

דיני סייבר

מרצה אבי טננבאום, מסכם נמרוד רק

הרצאה 1 | מבוא למשפט בכללי

המשפט מחולק לשני סוגים – המשפט הציבורי, בו המדינה היא צד (מנהלי - נגד רשות מבצעת, חוקתי - נגד רשות מחוקקת וכיוצ"ב) ופרטי, בו המדינה אינה צד (נזיקין, קניין, תאגידים, חוזים, ממקרקעין וכד').

שיטות המשפט במדינות שונות ניתנות לסיווג לשתי קטגוריות מרכזיות – הקונטיננטלי, שנמצא בכל מקום שצרפת/ספרד כבשו, והמקובל שנמצא בכל מקום שאנגליה כבשה (לרבות בישראל מכוח המנדט).

במשפט **קונטיננטלי** השופט חוקר ומאוד אקטיבי בדיון, רשויות נזהרות הרבה יותר מהתערבות בפועלה של רשות אחרת, ואין שימוש בתקדימים אלא כל מקרה לגופו. במשפט **מקובל** כל הנ"ל הפוך: השופט פסיבי ואין בעיה לבטל/לשנות פעולה של רשות אחרת, ותקדימים נמצאים בשימוש נרחב.

בהקשר של טכנולוגיה, השופט רודף את הטכנולוגיה ומנסה להסדיר אותה עם כלים קיימים, ובהתאם לאפקט הסטטוס קוו (שמרנות בכל הנוגע להמצאת קונספטים חדשים). אעפ"כ, החלטות ביהמ"ש לא ניתנות לניבוא תמיד ומשתנות מעת לעת בנושאים שלא מוסדרים עד הסוף בחוק. בארץ קשה מאוד להעביר חוק ולכן הרבה עניינים טכנולוגיים מוצאים עצמם נקבעים לפי פסיקה של ביהמ"ש. אם החוק לא מתייחס למשהו (לקונה), שופטים צריכים להכריע לפי עקרונות החירות והצדק של המשפט העברי ומורשת ישראל.

הרצאה II | חוזים באינטרנט

שני עקרונות יסודי בדיני חוזים

אוטונומיה – אפשר לכתוב בחוזה מה שרוצים, אלא אם הוא מכיל סעיפים לא חוקיים, או שבאים בניגוד לתקנת הציבור (נורמות, עקרונות וערכים בסיסיים בחברה), או שנכתבו שלא בתום לב.

יחסי הכוחות בין הצדדים – חוזים אחידים מכילים מגבלות נוספות, משום שצד אחד יותר חזק באופן משמעותי מהאחר, ואלו מעוגנות בחוק החוזים האחידים וחוק הגנת הצרכן.

חוזה נכרת ע"י הצעה של הצד המציע וקיבול של הצד הניצע, האינטרקציה הזו נקראת מפגש רצונות. כשדנים בשאלה אם אינטרקציה באינטרנט היא חוזה (לחיצה על קישור, הצגת פרסומת, קבלת מייל), בודקים אם הייתה כוונה של הצדדים, ואם היה מפגש רצונות. למעט חוזים שדורשים כתב יד פיזי כמו צוואות, כל חוזה אחר אפשר לחתום באינטרנט (בעזרת חתימה דיגיטלית אם צריך).

ביהמ"ש החיל את כל החוקים של חוזים רגילים על חוזים אינטרנטיים, ובפרט חוקים הנוגעים לחוזים אחידים על האינטרנט, בטענה שאתרים זמינים לכולם ולכן החוזה הוא אחיד. כמה דוגמאות לחוזים כאלה הן חוזה גלישה (כניסה לאתר) וחוזה הקלקה (קבלת עוגיות).

פס"ד נ' פייסבוק מ-2015: פייסבוק סגרה דף באתר לה כי רצתה, ושופט פסק שאסור היה לה כי בחוזה השימוש באתר נכתב שכל הסעיפים הם סעיפים יסודיים (כלומר שאם אינם מתקיימים אז כל החוזה בטל), וחזקה שזה סעיף מקפח, ולכן התניה לפיה פייסבוק טענה שסגרה את דף המשתמש לא חלה בכלל.

ישנו בית דין לחוזים אחידים שיכול לקבוע שחוזה הוא חוקי ואז אף בימ"ש לא יכול לטעון שהוא מכיל סעיפים מקפחים או לא חוקי וכד', אבל מעט גורמים משתמשים בשירות הזה מפני שרבים מהם יודעים שהחוזים שלהם מכילים בעייתיות כלשהי שלא הייתה מתקבלת ע"י ביה"ד.

פס"ד נ' פייסבוק מ-2019: NSO הסתכסכה עם פייסבוק אז פייסבוק מחקה את כל המשתמשים של עובדים של NSO. אלו תבעו אותה וניצחו בביהמ"ש, בטענה שהפגיעה שרירותית כי העובדים לא מייצגים או אשמים במעשי החברה, בדיוק כמו שזה היה שרירותי אם זה היה נגד יהודים או ערבים ככלל.

הרבה מהפסיקות בעניין נושאים באינטרנט ניתנות כתוצאה מתובענות ייצוגיות – תביעה של קבוצה/אדם שמייצגים קבוצה גדולה של אנשים שטוענים לעוול מתאגיד כלשהו, שלמדינה אין את המשאבים לעסוק בה בשל המספר העצום של מקרים כאלה. תובענות ייצוגיות לא קיימות באירופה, אלא בעיקר בישראל, ארה"ב וכמה מדינות נוספות.

הגדרות בתחום ברירת הדין

- סדר דין – איך מנהלים תביעה (אזרחית או פלילית), רכיב מהותי במשפט שנקבע לפי ערכים וסדרי עדיפויות בכל חברה.
- סמכות מקומית – באיזה מחוז (בארץ) דנים בתביעה.

- סמכות עניינית – באיזה סוג בי"ד דנים (תביעות קטנות, השלום, מחוז).
- מחיקה/דחייה על הסף – מחיקה היא פסילת עתירה בשביל הגשה מחדש לתיקון טעות טכנית ודחייה לא מאפשר הגשה מחדש.
- תנאי/תנייה – תנאי הוא חלק מהותי בחוק/חזזה ואילו תנייה היא חלק יותר שולי.
- תניית שיפוט זר – תנייה בחזזה שקובעת איפה ידונו בתביעות על החזזה.
- תניית דין זר – תנייה בחזזה שקובעת לפי דין של איזו מדינה ידונו (אורתוגונולי לתניית שיפוט זר).
- חזקת שוויון הדינים – חזקה לפיה אם אין שופט שיכול לשפוט לפי דין זר, נניח שהדין הזר מספיק דומה לדין בארץ כך שניתן לשפוט לפי הדין הישראלי.

אפשר לבחור לדון בחזזה בבוררות, כלומר מחוץ לביהמ"ש עם בורר חיצוני, וכך להגיע להחלטה יותר מהר ובחשאיות. עד האינטרנט, עקרון הטריטוריה ו"קיר הברזל" הנחו את קביעת סמכות השיפוט, לפיהם כל מדינה שופטת לפי עצמה, בהצדקה שלמדינות שונות חוקים שונים שמתאימים לחברות השונות שלהן.

תאוריית שלושת השלבים להערכת סמכות שיפוט בתביעה בינ"ל

- סמכות שיפוט – יש לקבוע איפה דנים בתביעה.
- ברירת דין – יש לקבוע באמצעות איזה דין דנים בתביעה.
- אכיפת פסק הדין – יש לבקש מביהמ"ש במדינה שבה נמצא הנתבע לאכוף את קביעת ביה"ד (ייתכנו שאלה שניים שונים).

פס"ד חברה אנגלית הציעה לחברה ישראלית הצעה בלתי חוזרת (מה שזה נשמע) וחזרה בה לפני שהחברה הישראלית הסכימה. האם הפרה את החוק? אנגליה לא חתומה על אמנת וינה ולכן אם לא הייתה תמורה לא הייתה עבירה על החוק האנגלי, אבל ישראל כן אז לפי החוק הישראלי כן הייתה. זה מקרה שבו סמכות השיפוט קובעת חח"ע את תוצאת המשפט עוד לפני שהתחיל ולכן היא מהותית.

פס"ד שוויצרי ידוע בציבור בישראל לישראלית, מת בשווייץ והשאיר צוואה באנגליה. לפי סמכות השיפוט של כל מדינה, היא עצמה זוכה לדון בתביעה – מה עושים? אם האזרח היה ישראלי והיה מת בשווייץ כל מדינה הייתה משליכה על המדינה האחרת את סמכות השיפוט – מה אז עושים?

בחוזים, אם יש תניית שיפוט/דין זר הבעיה נפתרה, ואחרת השופט נבחר המקום עם הזיקה המינימלית (קרובה ביותר).

פס"ד Voyeur Dorm v. Tampa: אתר פורנוגרפיה תיעד את המתרחש בוילה סגורה בשכונת מגורים בעיר. חוקק חוק שאוסר על עסקי מין בטווח שני ק"מ משכונת מגורים. האתר עתר לביהמ"ש בטענה שאילו לא היה מתגלה שהווילה בלב שכונת המגורים, לא הייתה שום בעיה, וניצח, כשנקבע שעסקי מין כוללים רק בתי עסק שלקוח פיזית באים אליהם. השופט הפריד כאן בין העולם הווירטואלי (האתר קיים) לבין העולם הפיזי (האתר לצורך העניין לא באמת בוילה).

פס"ד The Dow Jones v. Gutnick: למו"ל ה-WSJ יש 3% לקוחות באוסטרליה ולכן גוטניק תבע תביעת לשון הרע את DJ על פרסומים שלהם עליו באוסטרליה, בטענה שדיבתו הוצאה באוסטרליה (הסיבה האמיתית היא שבאוסטרליה חופש

הביטוי יותר מוגבל מבארה"ב ולכן היה לו סיכוי יותר טוב שם). ביהמ"ש דחה את העתירה באוסטרליה בטענה שלא ייתכן שהמו"ל יתרוצץ בכל העולם לכל מקום שיש לו מנויים, וגוטניק עדיין ניצח בסוף.

פס"ד נ' Yahoo France: באתר של Yahoo נמכרו מזכרות נאציות, שאסורות לפי החוק הצרפתי, לכן אגודת הסטודנטים היהודים בצרפת תבעה את Yahoo France. בסופו של דבר דנו בזה גם בצרפת וגם בארה"ב וניתנו פסקי דין סותרים. מה שחשוב כאן הוא של-Yahoo יש נכסים בצרפת ולכן גם אם בארה"ב נדחתה העתירה, ביהמ"ש בצרפת יכול לאכוף על הרכוש הזה את פסק הדין ככל שיהיה.

מבחן קהל היעד

המבחן לסמכות השיפוט באינטרנט היה בהתחלה מבחן Zippo שקבע לפי רמת הפעילות של אתר במדינות שונות אבל זה עתה הוחלף. מבחן קהל היעד הוא המבחן הקובע מאז, שקובע שאם קהל היעד של אתר כלשהו כלל אזרחים ממדינה כלשהי, אותם אזרחים יכולים לתבוע בארצם את האתר. איך קובעים אם אתה פונה לקהל יעד כלשהו? אם יש לבעלי האתר מידע על מיקום המשתמשים או אם בבדיקת כתובת IP (שנכונה בסבירות גבוהה) אפשר לזהות משתמשים ממדינה כלשהי, בעלי האתר לא יכול להכחיש שהוא פונה לאזרחים ממדינה זו. בנוסף אם ישנם מאפיינים באתר שמבטאים פנייה לקהל יעד מסוים, כמו שפת האתר (בעברית - כנראה פונה לישראלים).

פס"ד מלכא: מלכא תבע חברת תוכנה ישראלית שהתקינה לו תוכנת סחר במט"ח שפגעה בו בדרך כלשהי, וחווה השימוש בה כלל תניית שיפוט זר באנגליה, אבל ביהמ"ש פסק שסמכות השיפוט בישראל.

פס"ד איסכור נ' אקליפס: איסכור קנתה מגנטים תעשייתיים מאקליפס, טענה להפרת חוזה ותבעה בארץ, בטענה שהאינטרנט הוא בכל מקום ובפרט בארץ. ביהמ"ש פסק שבגלל שאין לנתבעת שום ייצוג או פעילות פיזית בארץ אין סיבה שזה יהיה בארץ ולכן זה נדון באנגליה. זו דוגמה לסמכות שיפוט בחוזה לא אחיד.

כשמדובר בפלילים, כל המדינות מרחיבות את סמכות השיפוט שלהן בלי התנגדות, במיוחד מאז המלחמה על הטרור שהכריזה ארה"ב.

הרצאה III | סמכות שיפוט ומטאפורות עומק

פס"ד בן חמו נ' פייסבוק מ-2019: עו"ד גיא אופיר ייצג את בן חמו בתביעה על סך 400 מיליון דולר נגד פייסבוק. שם ביהמ"ש העליון קבע שתניית השיפוט הזר (בקליפורניה) מקפחת, לא כל שבן משום שהנתבעת היא פייסבוק אירלנד ולא ארה"ב (מסיבות מס).

פס"ד טרויס נ' פייסבוק מ-2022: פייסבוק שינתה את המדיניות שלה מאז בן חמו ועבשיו כולם דנים בארץ אבל צרכנים לפי הדין הישראלי ומפרסמים לפי הקליפורני. ביהמ"ש העליון פסל גם את זה, וקבע שבכל תביעה שאינה תובענה ייצוגית באינטרנט, סמכות השיפוט וברירת הדין יהיו הישראליים. בעניין התובענה הייצוגית לא שונה דבר (סמכות שיפוט לפי מבחן קהל היעד בארץ אבל ברירת דין יכולה להיות קליפורנית).

הסכנה בהרחבת סמכות השיפוט יתר על המידה היא שבתי משפט במדינות אחרות לא יהיו מוכנים לאכוף פסיקות ישראליות. בכל מקרה מבחן קהל היעד הוא הקובע מבחינת סמכות השיפוט בכל המדינות (למעט עסקים קטנים שייטבעו במדינתם).

סמכות מקומית בתביעות בעניין האינטרנט

חוק סדר הדין האזרחי שונה לפני שנתיים ועתה מגדיר היטב את הסמכות המקומית בתביעות באינטרנט.

- תובענה ייצוגית תישפט במחוז מקום מגוריו או עסקו של הנתבע (2 אפשרויות).
- כתב תביעה יישפט במחוז מקום מגוריו או עסקו של הנתבע או תובע (4 אפשרויות).

מטאפורות עומק כמעצב תפישת עולם

משפטים משתמשים במטאפורות שהם מכירים בניסיון להסדיר את האינטרנט (וטכנולוגיות אחרות) אך בהיעדר ידע והבנה מתאימים, עושים נזק באמצעות התבססות על מטאפורות שגויות/לא רלוונטיות.

ברמה העקרונית, למטאפורות יש השלכות הרת גורל על צורת המחשבה שלנו. לדוגמה, התייחסות לוויכוח כאל מלחמה (באמצעות ביטויים מתאימים) תגרום להתנהגות שונה מהתייחסות אליו כריקוד, או כמשחק. ברמת המדיניות מטאפורת העונש כתשלום חוב לחברה שגויה כי אסירים עולים הרבה כסף, ועוד דוגמאות רבות אחרות.

מטאפורות להבניית נקודת מבט על האינטרנט

- אוטוסטרדת המידע – דרושה "מהירות מותרת", אכיפה, חוקים והסדרה להתנהלות אינטרנט.
- הספר (frontier) האלקטרוני – כל אחד רשאי לעשות מה שירצה ואין צורך בחיקוק והסדרת האינטרנט.

פס"ד חברת משולחים קטנה אחת תבעה אחרת על פריצה וגניבת מספרי הטלפון של הלקוחות שלה. השלום טען שהייתה פה הסגת גבול (לא מטאפורה נכונה) והמחוזי הסתכל על מספרי הטלפון כספר טלפונים (גם שגוי).

מטאפורות ספרותיות בהקשר הזכות לפרטיות

אם נסתכל על פגיעה בזכות לפרטיות כמו שהיא קורת ב-"1984" של ג'ורג אורוול, הרי שכל איסוף מידע, במיוחד של השלטון על האזרחים, הוא פגיעה בפרטיות שמין הראוי למזער.

פס"ד ג'יימס סידס היה ילד פלא שהתפרסם בחוכמות בגיל מאוד צעיר, ואז בחר להיעלם מן הבמה העולמית. לאחר עשרים שנה, עיתון עקב אחר עקבותיו ומצא שהוא פועל בבית חרושת. סידס תבע את העיתון בטענה שהופרה הזכות שלו לפרטיות (הזכות להיות לבד), אבל ביהמ"ש קיבל את טענת המו"ל לפיה זכות הציבור לדעת, כי כזכור חופש הביטוי בארה"ב מאוד חזק בחקיקה ושפיטה.

הסיבה שבגללה מטאפורות נדרשות, בפרט בתחום הפרטיות, היא שבעקבות ההתקדמות בטכנולוגיה והיכולת לפגוע בחומרה גבוהה הרבה יותר בפרטיות, גם החקיקה מנסים להצמיד את הפער ולהגן על הזכות לפרטיות, שלפניכן (בוודאי לפני 100 שנה) לא הייתה רלוונטית.

הרצאה IV | המשך מטאפורות ועבירות מחשב

שתי מאפורות עומק לזכות לפרטיות

- מצב קפקאי – אדם קם בבוקר ומתברר שהוא מואשם במשפט, והוא חסר אונים כי אין לו מושג במה הוא מואשם ועל בסיס מה, וכולם חושבים שאם יש נגדו משפט אז הוא כנראה עשה את העבירה. לפי מטאפורה זו, מותר לאסוף מידע, רק שכל אחד יוכל לשלוט ולדעת איזה מידע נאסף עליו.
- האח הגדול – אסור ששום מידע יאסף עלינו, פחות רלוונטי כיום כי מי שאוספים את המידע הן חברות ולא השלטון, ומעבר לכך יש גם יתרונות (ביטחון לאומי, מניעת גניבת זהות עם ת"ז ביומטרי...) להפרת הפרטיות מצד השלטון.

פס"ד האגודה לזכויות האזרח תבעה את רשות האוכלוסין כי לבנקים יש גישה ישירה למרשם האוכלוסין כדי לבדוק אם לקוחות חדשים הם אנשים קיימים. זה מפר את הזכות לפרטיות כי לא ידוע לנו שמשתמשים במידע עלינו, אבל הבנקים טענו שאחרת לקוחות היו צריכים להגיע פעמיים לבנק כדי לפתוח חשבון וניצחו. כאן מטאפורה האח הגדול אוסר על כל שימוש במידע, ואילו לפי קפקא רק חשוב שהלקוח ידע שמשתמשים במידע הזה שלו. במציאות הרבה מידע מסתובב חופשי ולכן קפקא יותר רלוונטי (אגרון וכיוצ"ב).

פס"ד מזרחי (יש כמה בשם זה) תבע את עיריית תל אביב על דו"ח חניה שקיבל בו נכתב שמצלמה תיעדה אותו יוצא עם מישהי מרכב וחונה איפה שאסור. מזרחי טען שהייתה פגיעה בפרטיות. השלום אסר שימוש במצלמות כאלה, והמחוזי הפך את ההחלטה בטענה שהפרת הפרטיות מינורית כאן – עדיין לא הוכרעה הסוגייה בעליון.

כיום הנחיית הרשות להגנת הפרטיות במשרד המשפטים היא לאפשר צילום אזרחים לצורך אכיפת החוק בתנאי שמיידיעים אותם שמצלמים אותם ומאפשרים להם גישה לתוכן. בנושא זה, המשטרה משתמשת במערכת "עין הנץ" שיכולה לא רק לזהות לוחית רישוי בכביש אלא גם את הנהג בתוכה, וכך לפתור מקרי פגע וברח ועבירות תנועה אחרות ביעילות רבה. לאחר תביעות ושינוי חקיקה הנוהל הנוכחי דורש אישור תנ"צ ומעלה לשימוש במערכת.

מטאפורה העומק של האינטרנט כ"מרחב וירטואלי" שגויה וגורמת נזק – מחשב הוא לא בית (ולכן מחשב אינו מבצרי), לא באמת "נכנסים" לאתר אלא מתחברים/מתקשרים עם מחשב אחר. בגלל הבנה שגויה זו נפסק בעבר על פריצה לאתר בדומה לפריצה לבניין.

בעיות עם מטאפורות במשפט

לרוב משתמשים במטאפורות כשאינו הסבר טוב לעמדה כלשהי בנושא חדש – עדיף להימנע מהן כי פעמים רבות משתמשים במטאפורה לא רלוונטית שעושה עוול לאיך שהטכנולוגיה עובדת במציאות.

מטאפורות לרוב מכניסות השקפת עולם בדלת האחורית – מציב בסיס עובדתי שכבר מוטה לעמדה אחת.

חוק המחשבים

חוק המחשבים חוקק ב-1995 לאחר 13 שנות דיונים, כשהוא לא כולל בכלל אזכור לאינטרנט כי לא חשבו שזה יהיה רלוונטי. החוק קצר מאוד ובקושי מתייחסים אליו בפסיקה, והוא כולל התייחסות נזיקין ועוולות כתוצאה מעבירות מחשב.

אין התייחסות לטלפונים אבל ישנו פס"ד שמכיל דיני מחשבים על טלפונים. החוק מקנה למשטרה את הזכות לקחת מידע מטלפון בחקירה, ולא לחשוף לנתבע באיזה חומר משתמשים כי יש יותר מדי מידע שזה לא אפשרי. למשטרה יש את היכולת לתפוס כל נכס לחקירה, אבל בגלל שטלפונים ומחשבים הם בין היתר כלי עבודה והיעדרם מהווה שיבוש בלתי מידתי לאורח החיים שלנו, נדרש צו כדי שהמשטרה תוכל לקחת אותו לחקירה.

אמנת בודפשט

האמנה נחתמה ב-2004 וחוקקה בכנסת ב-2005 (רק החל מהחיקוק מחייבת). האמנה דורשת מכל מדינה לחוקק חוקים נגד עבירות מחשב, ולאפשר למשטרה להיכנס למחשבים ממדינה אחרת ולקחת ראיות מהם, ולשם כך יש להקים מכרז שירות 24/7 לבקשות ממשטרות של מדינות אחרות. בעקבות האמנה, הורחבה הגדרת "וירוס מחשב" לכל תוכנה שמונעת שליטה, קוראת, כותבת, או אוספת מידע שלא כדין, ולא רק כזו שמוחקת, כמו שהיה עד אז.

פסקי דין בעניין חדירה למחשב

בחוק העונשין, חדירה למחשב היא התחברות או שימוש במחשב ללא אישור.

- פס"ד רפאלי (ישן) ופסיקתו אינה רלוונטית כיום): רפאלי עזב את מקום העבודה שלו אבל נשארה לו גישה למערכות המידע של מקום העבודה שלו, ולכן הוא התעדכן מעת לעת במתרחש בחברה, וכשזו גילתה שזה מה שהוא עושה – תבעה אותו על חדירה למחשב שלא כדין. הוא טען שהוא לא עשה נזק ולכן זו לא חדירה, אבל לא כתוב בחוק שצריך להיעשות נזק ולכן הורשע.
- פס"ד מזרחי (3): מזרחי בדק אם אתר דרושים של המוסד מאובטח באמצעות כלי שסורק פרצות אבטחה באתר. המוסד תבע אותו על חדירה למחשב, אך הראשון זוכה כי הוכיח שרק חיפש פרצות אבטחה, והשופט הסכים שזה לא נופל תחת "חדירה שלא כדין". בהקשר הזה, תפיסת Kerre קובעת שחדירה למחשב דורשת עקיפה של מחסום טכנולוגי כלשהו, ולא רק הפרת חוזה.
- הלמו (מבין רבים): הלמו הסתכסך עם עופר שדות. הלמו רצה להראות לצורך משהו שיש לשדות חובות, ולכן נכנס לאתר לגביית קנסות ושילם שקל בשם שדות, וכך גילה שאכן יש לו חובות. בגלל שהאתר נכתב גרוע – זה פרע את כל החוב (שהיה על סך 8 מיליון שקל). שדות טען שהלמו עשה זאת בידיעה שהחוב יפרע ויגרום לו להראות עבריו. הוא זוכה (ע"י המרצה) כי אפשר היה לגרום לנזק הזה גם בלי הבנה במחשבים בכלל.
- פרשת הלמו: הלמו הצליח בקלות להיכנס לפסקי דין חשאיים באתר הרשות השופטת. בסופו של דבר זוכה לאחר שהפרקליטות הבינה את גודל המחדל.
- יועץ בחוות מחשבים באוני' העברית קיבל גישה לחשבונות מייל של מרצים, ניצל זאת לרעה והורשע בחדירה שלא כדין (אפילו שלא פרץ מחסום טכנולוגי).
- רון עזרא: עזרא השיג באופן לא חוקי סיסמה לחשבון בנק של מישהו, והעביר לעצמו כסף דרך אתר הנזק. הפרקליטות האימשה אותו בחדירה למחשב. האם אכן הייתה חדירה?

1. בדיון בשלום נקבע שהפגיעה הייתה במחשב ולכן אכן הייתה החדירה.

2. בדיון נוסף בשלום נקבע שלא נעקף מחסום טכנולוגי ולכן זו אינה חדירה.

3. במחוזי נקבע שזו חדירה רק אם יש פגיעה בשפת מכונה (Assembly) – מה שמעיד על חוסר הבנה של איך מחשב עובד וגורם נזק למקרים אחרים כי אפשר לחדור למחשב בלי להגיע לרמת שפת המכונה.
4. בעליון נקבע שכל שימוש במחשב בלי הסכמת בעליו היא חדירה – קביעה גורפת שמזיקה גם היא. עם זאת הוסיפה חזקה שהפרקליטות לא תגיש כתבי אישום על מקרים שאינם עבירות באמת.

הרצאה V | דילמות בהגדרת חדירה שלא כדין למחשב

הקביעה של העליון, תוך שימוש במטאפורה שגויה (השוואה לבית), גרמה נזק לניסיון לאבטחת הרשת: Bug Bounty הוא כרגע לא חוקי! כך גם האקרים אתיים אינם מוגנים. נוסף על כך, crawler-ים באשר הם (כמו אלו של גוגל) אינם חוקיים כי לא הושג אישור של בעלי האתר.

שתי חזקות שיפתרו את הבעיה (לדעת המרצה)

שתי החזקות הבאות הן כרגע בגדר הלכה לא מחייבת בפסיקה.

- שימוש במידע שהושג כדין לחדירה למחשב היא חוקית.
- להתקשר עם אתר באופן סביר מנוגד לרצון בעל האתר היא חדירה, אלא אם הודיעו לבעל האתר על כך.

פסקי דין העוסקים בהגדרת חדירה למחשב

- בתקנון הבלוג "המזבלה" נכתב שלעובדי פייסבוק אסור להיכנס לאתר. הם נכנסים אליו כי הוא זמין לכולם – האם כולם חוזרים שלא כדין למחשב? במקרה הזה ביהמ"ש זיכה את המואשמים מסיבה אחרת במקרה הזה.
- פס"ד איסקוב: האם למעסיק מותר לחדור לדוא"ל של עובד? פס"ד מפריד בין מייל מהעבודה, שמותר לו להיכנס, לבין מייל מעורב או פרטי, שלו הוא לא יכול להיכנס. מאז מעסיקים לרוב מחתימים עובדים בחוזה על סעיף שמאפשר להם לגשת לדוא"ל העבודה.
- המשטרה ביקשה מיונתן אוריך גישה לטלפון שלו, הוא לא ידע שהוא יכול לסרב והסכים. הוא גילה בדיעבד שלא היה צו ושיכל לסרב. בינתיים המשטרה מצאה חומרים מפלילים בטלפון שלו, וביקשה צו בדיעבד. העליון קבע שהמשטרה לא יכולה להשתמש בראיות האלה במשפט, אבל קבע הלכה, לפיה המשטרה יכולה להלבין חומר שהושג לא כדין אם יש לה מספיק חומר שהושג כן כדין.
- יו"ר לשכת עורכי הדין לשעבר אפי נווה הסתכסך והתגרש מאשתו. גרושתו לקחה לו את הטלפון, העבירה לעיתונאית, זו העבירה למומחה שמצא חומרים מפלילים עליו. במקרה הזה המשטרה לא יכלה להלבין את הראיות כי לא היה לה אף ראיה מלבד תוכן הטלפון.
- נאמן רודף אחר נכסיו של פושט רגל ומבקש צו לקבלת גישה לכל המחשבים שלו כדי לראות אילו נכסים הוא מנסה להבריח. השופט לא איפשר צו שכזה.
- גבר לקח את הטלפון של אקסית שלו ומחק משם מידע, ונתבע בין היתר על חדירה למחשב והורשע.
- חדירה למצלמות אבטחה ופגיעה בזכות לפרטיות (בסיטואציות עירום לדוגמה), היא פגיעה בפרטיות, כלומר חדירה למחשב לצורך ביצוע עבירה אחרת.
- ראש עיר מחק חומר מיומנו הדיגיטלי שהראה על חשד לשחיתות בטרם העביר אותו הלאה לבקשת חופש מידע. הוא הורשע במחיקת חומר מחשב, אע"פ שלטענתו זה יומן שלו והוא רשאי לעשות מה שרוצה בו, כי בחוק המחשבים מחיקה היא עבירה אם תוצאתה היא מידע/פלט כוזב, וכאן אכן היה פלט כוזב – הטעיית הציבור. בנוסף היומן שייך בכלל לעירייה ולא לו.
- השתלטות על חשבון פייסבוק ודוא"ל לאחר השגת הסיסמה באופן לא חוקי – לא הורשע בחדירה.

- עבירות מין באינטרנט – החדרת כל דבר לאיבר מינה של קטינה מתחת לגיל 14 היא אונס. אדם קיים שיחות מיניות עם בנות באינטרנט וכתוצאה מכך הכניסה קטינה חפץ לאיבר מינה והואשם באונס, והורשע. כדי למנוע דיסוננסים קוגניטיביים כאלה, יש צורך בחיקוק עבירות ספציפיות לעבירות מין באינטרנט.

אכיפת חוק כוללת ארבעה שלבים: קביעת נורמה (חוק); התנהגות בהתאם לנורמה; תגובה למפירים את הנורמה; השפעה של תגובה זו.

תזה מרכזית - הרבה יותר קל לאכוף עבירות רגילות שקורות באינטרנט מאשר מחוצה לו. עם זאת, הנזק מעבירות אלו גבוה הרבה יותר (אי אפשר לדעות אפילו). האכיפה קלה יותר משום שאפשר לבצע אותה בכלים טכנולוגיים שלא דורשים את המשפט בכלל, כמו לחסום אתרים, לא לכבד סליקה מעסקי הימורים לא חוקיים וכיוצ"ב.

בדומה, בגלל שהכל דיגיטלי ונתון למערכות ניתור ו-logging, קשה הרבה יותר להעלים דברים כמו לא לשלם מע"מ או מכס. אף חברה לא תעז לא לשלם את כל המיסים הנדרשים בעסקאות אינטרנטיות, ואילו במציאות רבות לא יחששו לא לשלם מכס או לעבוד בשחור.

הרצאה VI | אכיפת החוק באינטרנט ומכונות אוטונומיות

העבירות שקשה לאכוף באינטרנט הן עבירות שקשורות לתשתית האינטרנט, כלומר שמנצלות או לא-נבלמות בגלל שהאינטרנט לא עוצב באופן שמונע וממגר עוולות ועבירות.

לדוגמה, בשנות ה-90 וה-00 היו אתרי הימורים בעברית באינטרנט ופרסומות בכל מקום בשבילים. בשלב כלשהו המשטרה פשטה על משרד החברות שפרסמו אותם, ושל חברות האשראי שאישרו את העסקאות שלהם, וכך כולם סירבו לשתף עם אתרי ההימורים פעולה מיוחדת מהמשטרה.

פס"ד ב-2010 המשטרה הוציאה צו שהורה לספקיות לחסום את אתרי ההימורים, ואיגוד האינטרנט הישראלי עתר מנהלית נגד צו זה. הצו הוצא מכוח פקודת המשטרה, המאפשרת להוציא צו סגירה לחצרי בית עסק שלא חוקי לפי קריטריונים שונים. השופטת במחוזי התייחסה לכמה סוגיות, הרלוונטיות שבהן היא שאלת הסמכות של המשטרה להוציא את הצו. השופטת קבעה שאין פרשנות לפיה האתר הוא בית עסק, וכדרך אגב שהספקיות הן צד שלישי שלא ברור איך המשטרה מערבת אותם בכלל. העליון קבע שהחוק לא מקנה סמכות לסגור אתרים, ובפרט אין סמכות לערב ספקיות בעניין לא להן, והורה את המחוקק לפתור את הבעיה.

חוקק חוק שמסדיר סגירת אתרים, והוא מטפל באתרי טרור, מין, סמים והימורים. הוא מאפשר להסיר, להגביל גישה, או להגביל גישה חפזית לאתר, ומאפשר לתת לספקיות צווים לחסום ברמת ה-DNS.

ביקורת נגד סגירת אתרים במתכונתה הנוכחית

האגודה לזכויות האזרח טוענת שחסימה של אתרים באמצעות המשטרה (בפרט עם רשימות ארוכות שמגיעות מחו"ל) יכולה להוביל לצנזורה שלטונית.

איגוד האינטרנט טוען שהחסימה לא יעילה (יעילה בעיקר למי שאין אוריינות דיגיטלית) ומה שבן חוסמת הוא יותר מדי.

בעולם משטרים אפלים חוסמים (לא באפקטיביות) אתרים עם חופש ביטוי רחב מדי ושל מתנגדים, אך אלו לעתים אינן פופולריות במקרים של אתרים גדולים בשימוש נרחב של הציבור.

בפועל החסימה הכי יעילה היא צנזורה של מוסדות פיננסיים באמצעות אי-מתן שירותי סליקה לאתרים לא חוקיים. זה גורם למצב שבו מי שקובע מי מצונזר ומי לא הן חברות פרטיות, שאין להן בהכרח שיקול דעת הוגן או את טובת הציבור בראש סדר העדיפויות.

לפרקליטות יש מאז 2015 יחידת סייבר שאחראית על ניהול תיקים פליליים שדורשים מומחיות טכנית וכן על אכיפה אלטרנטיבית בהסכמה עם החברות הרלוונטיות, בצורת חסימת אתרים והגבלת גישה חפזית של האתרים. יש כאן בעייתיות כי השת"פ הזה בין הרשויות לתאגידים עם כוח גדול נשמעת כמו הקשר האדוק בין חברות סיניות לממשל בסין.

פס"ד פוליטיקאית תבעה את פייסבוק ב-2019 בבית הדין האירופי לאחר שהאחרונה סירבה להסיר פוסטים שקוראים לה בוגדת פשיסטית. ביה"ד פסק לטובת הפוליטיקאית וקבע תקדים שמחייב כל מדינה חברה בביה"ד.

את העתיד אפשר לשאול מומחים, שכולם מסכימים שטועים הרבה, או באמצעות חיזוי לוגי. כך או כך אף אחד לא יכול לחזות טכנולוגיה ששוברת את כלי המשחק, כמו שלא חזו את האינטרנט. זו גם הסיבה שהחקיקה מפגרת אחר הטכנולוגיה. יש יתרונות לאיחור של החקיקה, לדוגמה שאפשר להתקדם מהר יותר בלי דיונים משפטיים ענפים.

המכונית האוטונומית מתחלקת לשני חלקים מהותיים – הרכיב האוטונומי (היכולת לנהוג ללא אדם) והרכיב המקושר (היכולת לתקשר עם מכוניות אחרות ומערכות מידע חיצוניות). הראשון קיים חלקית כיום בטסלה, והאחרון קיים אפילו בוויז, אבל אף אחד מהם לא יושם בהצלחה עד כה. עניין שלא מקבלת התייחסות רבה הוא שברמה העקרונית, רכב יהפוך לשירות ולא למוצר.

הסיבה שאין עדיין מכוניות אוטונומיות בכל מקום הוא מחיר (יקר מאוד להחליף את כל המכוניות); תשתיות (לא כל מקום מאפשר נסיעה אוטונומית); בטיחות (אין הבטחות מהימנות לרכב אוטונומי עדיין); וטכנולוגיה (כרגע היא לא מספקת תוצאות טובות מספיק). ברמה הרגולטורית, ה-NHTSA קבע 5 רמות של אוטונומיה, שצריכות כל אחת לקבל יחס רגולטורי שונה: עזרה לנהג; אוטומציה חלקית; אוטומציה מלאה בתנאים מגבילים; אוטומציה מלאה עם החזרת שליטה בחריגים; ואוטומציה מלאה.

רכבים אוטונומיים מעלים הרבה שאלות חוקיות ומסריות, ביניהן מי אשם אם יש תאונה, המפתח, היצרן, הנהג? מה אם רכב מותקף ופורץ גורם לדריסה? כמה לאפשר פגיעה בפרטיות בכל המידע שנאסף מהמכונית? מה המכונית צריכה לבחור בסיטואציות דוגמת בעיית הקרניות? 40 מיליון אנשים נדרשו להכריע בבעיית הקרניות וניכרות שלוש העדפות מרכזיות רווחות: בני אדם על חיות; צעירים על מבוגרים; ורבים על מעטים.

בשל כך שבינה מלאכותית אינה דטרמיניסטית, בעיית הקרניות ונגזרותיה פחות בשיח המשפטי והסוגייה המרכזית כרגע היא הפרת הזכות לפרטיות.

ישנן מגמות חקיקה עולמיות, ביניהן איסור מוחלט על שימוש ברכים אוטונומיים חופשיים, מתן היתר לרכבי מבחן. בנוסף ברוב המדינות יש חובה להגנה ובלמים שנשלטים בידי אדם במקרים חריגים. לאחרונה ה-NHTSA אשרו רכב בלי הגה ובלמים, ובלבד שאין בו בני אדם. בישראלי המפקח על התעבורה יכול לתת היתר לניסויים ברכבים עצמאיים, ויש תזכיר חוק שנותן יד חופשית לביצוע ניסויים עם רכב עצמי, ככל הנראה בהשפעה משמעותית של לוביסטים מטעם מובילאיי ושות'.

הרצאה VII | מדיניות בעניין בינה מלאכותית וקניין רוחני

הרגולציה שמאפשרת ניסויים ברכבים אוטונומיים בעייתית, כי חברות שרוצות להסיר כל אחריות פלילית מעצמן מפעילות לחצים שכך יחוקק. מצד אחד לא יכול להיות שהחברה לא תהיה אחראית בכלל, מצד שני הפחד שמנכ"ל חברה יואשם בגרימת מוות ברשלנות כי הרכב האוטונומי שלו עשה תאונה מונעת מהתקדמות בפרויקטים כאלה. המצב תקוע.

בינה מלאכותית מוגדרת ע"י כמה מבחנים שונים, ביניהם מבחן טיורינג ותחרות לובנר, אבל בכל מקרה אין לאדם יכולת לשלוט באיך היא תתנהג. התחום מאופיין בהרבה קפיצות טכנולוגיות והשגת מה שנחשב לבלתי אפשרי באופן תדיר. ישנן כמה סכנות בשימוש ב-AI, לדוגמה מה קורה אם אלג' נותן דיאגנוזה ואז טועה, מי אשם? האם חישוב ערבות אוטומטי מוסרי (מוטה גזעית בגלל ההיסטוריה)? האם כלי עזר לשופטים שמחשב אחוזי פשיעה מוסרי?

רחפנים אוטונומיים זוכים לרגולציה יותר משוחררת, בין היתר בשל הסכנה הפחותה במקרה של תאונות, וזאת בניגוד ללוויינים, שעליה יש ליצרן אחרית מוחלטת (לא משנה מה קרה כתוצאה מהתנהגות הלוויין, גם אם לא באשמתו, הוא אשם) מכוח חוק משנות ה-60.

האיחוד האירופי מציע שלוש רמות סיכון לשימוש ב-AI, החמורה שבהן היא התנהגויות השקולות ל"אשראי חברתי" ואלו אסורות, אבל כך או כך ההגדרות די עמומות ולא ישימות כל כך. בארץ ישנה טיוטת מדיניות בתחום הבינה המלאכותית, היא באורך 115 עמודים וכוללת דרישות מהמכונה כמו "האדם במרכז", "שקיפות והסברתיות" ו"איסור אפליה פסולה", שהם דברים חשובים אבל בלתי ישימים בפועל. כרגע המגמה בישראל היא שלא יהיה חוק AI יחיד אלא שכל שר יתקין תקנות בתחומי העיסוק שלו.

לסיכום, העולם מתקרב לרכב אוטונומי ושימושי AI שנויים מחלוקת אחרים, אבל ייקח הרבה זמן עד שיאופשר שימוש רחב ללא הגבלות וזה יקרה בצעדים קטנים, כשבסופו של דבר הציבור וביהמ"ש לא ימצא עניין רב בתאונות שנעשו ספציפית ע"י רכבים אוטונומיים וכד'.

מבוא לקניין רוחני

קניין רוחני נוצר כדי להוות תמריץ ליצר, באיזון עם האינטרס הציבורי להימצאות יצירות ברשות הציבור. קניין רוחני מכל סוג מותנה בכך שייחשף לציבור ומוגבל בזמן (לרוב 70 שנה ממות היוצר). ההגנה על קניין רוחני היא שאחרים לא יכולים להשתמש בקניין, בצורה כזו או אחרת כפי שתפורט בהמשך בסוגים השונים.

סוגי קניין רוחני

- זכויות יוצרים – מגנות על תוצר כלשהו ולא צריך לרשום אותם, אבל דורשות מקוריות ויצירתיות. מזכויות יוצרים יש זכויות נלוות, כמו זכות מבצעים, זכות משדרים וזכות התקליט.
- פטנטים – מגנים על תהליך ולא על תוצר, נדרש רישום של הפטנט (שעולה כסף) והוא חל למשך 20 שנה, בטענה שהפגיעה בציבור יותר חזקה כאן מאשר בזכויות יוצרים. התנאי לפטנט הוא חדשנות וצעד אמצאתי (משהו שניתן לתעד כפטנט, שיהיה שונה ממה שיש עד עכשיו...). תביעות פטנטים לרוב עושים בארה"ב, ואפשר או לשלם לעו"ד לפי אחוזים (קשה להשיג ייצוג לתביעות לא ענקיות) או לפי שעות (העו"ד יכול למשוך את התביעה שנים).

- עיצובים – ניתן לרשום פטנט על הצורה של המצאה, אם יש מקוריות וחדשנות. מעגלים אלקטרוניים משולבים זו דוגמה לא טריוויאלית לעיצוב (מדגם).
- סימני מסחר – נשמרים לנצח כל עוד משתמשים בהם, חובה לרשום אותם והתנאי שלהם הוא שיהיה אופי מבחין שניתן לזיהוי (חזותית). שמפניה היא דוגמה לסימן מסחר שיכול להיות מאופיין נטו לפי אזור גאוגרפי.
- מידע חסוי – בשולי הקניין הרוחני, מגן על סודות מסחריות ונלווה ממנו הגנה מפני תחרות לא הוגנת. לדוגמה אדיס תבעה חברה שייצרה נעליים עם ארבעה פסים, אבל הפסידה כי ניתן להבחין בין 3 ו-4 פסים. בדומה החברה שייצרה את "לחם עיניים" תבעה את לחם ברמן שייצרה "לחם לעניין" והפסידה, כי ניתן להבחין.

סוגיות שעולות מקניין רוחני

- כלכלי – תביעות פטנטים הן מאוד יקרות, ויש טרולים שתובעים חברות סתם וזוכים בדמי השתקעה כדי לא להיכנס לתביעה מיותרת ויקרה.
 - פוליטי-מדיני – סין לא הגנה על קניין רוחני שנים, ולאחרונה החלה לאכוף כדי שיאכפו את שלה. במדינות בלי הרבה קניין רוחני כמו הודו אין כמעט אכיפה על קניין רוחני. ארה"ב הפעילה לחצים על ישראל שתאכוף יותר טוב פטנטים שלה, ולשם כך נפתחה יחידת הקניין הרוחני במשטרה. לישראל כאומת היי-טק יש עניין באכיפת פטנטים כי בלעדי זה לחברות אין מוצר ייחודי שהן יכולות למכור.
 - פילוסופי – בארה"ב אין מושג של קניין רוחני, אלא הכל נופל תחת זכויות יוצרים, כלומר ההגדרה אינה "זה שלי" אלא "זה לא שלך". יש תנועות שקוראות לשחרר את כל המידע לחופש, ויש חברות כמו אקו"ם שעוברות בין בתי קפה ובזדקות שהן לא משמיעות מוזיקה של הלקוחות שלה.
- האם קניין רוחני קיים בכלל? אם הוא קניין הוא נכס פיזי, ואם הוא רוחני אז הוא לא קניין – זו מטאפורה שגויה! חוק יסוד – כבוד האדם וחירותו מעגן את הזכות לקניין, וגם בהצהרה הבינ"ל לזכויות אדם של האו"ם הזכות לקניין מוכרת כזכות אדם.

ארגונים בינ"ל שאחראיים על קניין רוחני

- WTO – ארגון הסחר העולמי, שמכיל בתוכו יחידות שאחראיות להסדרת פטנטים, בהתאם לאמנת GATT, ורוב המדינות חברות בו.
 - WIPO – ארגון הקניין הרוחני העולמי, שאחראי רק על זה, בו גם רוב המדינות חברות ותחתיו ישנן אמנות רבות, בראשן TRIPS הנוגעת לאכיפת פטנטים בינ"ל.
- בעזרת הארגונים הנ"ל נאכפת הגנה על פטנטים בכל העולם, כאשר כל פטנט זוכה לשנה הגנה בינ"ל חינם, ולאחריה צריך לשלם (די הרבה) כדי לקבל הגנה. הרעיון המרכזי של האמנות הוא שההגנה על פטנטים היא שווה ליוצרים אזרחי המדינה בה הופר הפטנט ליוצרים שאינם אזרחי המדינה.

זכויות יוצרים בשמות מתחם (domain names)

בראשית האינטרנט, ארגון בשם IANA שלא הוסדר חוקית, הקצה כתובות IP ושמות מתחם בשיטת כל הקודם זוכה. זה גרם להרבה תביעות מצד חברות שנלקח להן שם המתחם עם השם שלהן, ואלו העמיסו על בתי המשפט במשך שנים. הפתרון שנמצא הוא בוררים בשלל ארגונים שזול ומהיר לגשת אליה ואכיפתם יעילה וחד משמעית. הם מעבירים בעלות של שם מתחם אם מתקיימים שלושה תנאים:

- שם המתחם מטעה.
- אין לנתבע זכויות לגיטימיות לשם.
- התובע פעל בתום לב.

לדוגמה, אדם קנה את carrefour.co.il, הרשת הצרפתית ביקשה את הכתובת, ובגלל שלא סיפק סיבות טובות, ניצחה. בכל הנוגע לשמות מתחם פוגעניים, יש דיון אידיאולוגי האם צריך לאפשר אותם בכלל, בדומה לשמות רחוב פוגעניים. יש ועדה שמתכנסת אחת לארבע שנים שקובעת האם שמות פוגעניים יכולים להיות שמות מתחם, בהתאם לחוקיותם, פגיעתם ברגשות הציבור וקריטריונים נוספים.

קניין רוחני במקום העבודה

לפי החוק, כל קניין רוחני של עובד שנעשה למטרות העבודה הוא של המעסיק. בגלל שלעיתים מגלים דברים כדרך אגב במהלך מחקר, לכל אונ' יש חברה שרושמת פטנטים על דברים שהיא חושבת שיכולים להצליח ולא כדאי לפספס (כל פרופ' מגיש עשרות פטנטים ורישום פטנט הוא יקר ולכן עליהן לסנן). לעתים הסינון מפספס, כמו את מובילאיי.

בישראל אם חוזה לא מסדיר את עניין הפטנטים, יש וועדת תמלוגים ופיצויים שמכריעה בסוגיות כאלה. כתוצאה מכך חברות רבות מוסיפות סעיפים שקובעים שכל מה שהעובד עושה גם אם לא ישירות למטרת העבודה הוא שייך לחברה, וזה גורם לתופעה של עובדים שמנסים להבריא או להלבין פטנטים שעלו עליהם בזמן העבודה.

פס"ד עובד בתכנית "הצינור" יצר אתר אינטרנט, וכשעבר לתחנה אחרת לקח איתו את האתר. התכנית תבעה אותו על שימוש לא חוקי בקניין רוחני (שם המתחם), ובגלל שהעניין הזה לא הוסדר עד כה, השופטת הציעה מגוון שאלות אחרות שבאמצעותן יכריעו את הנושא.

המדינה יכולה לחייב שימוש בפטנט רשום רק במקרים של תרופות (ואז תשלם אחוזים לחברה עם הפטנט).

תוכנה כקניין רוחני

מה מעמדה של תוכנה בהקשר של קניין רוחני? ברוב העולם חלים עליה דיני זכויות יוצרים ולא פטנטים, בטענה שזה טקסט, ולכן דינה כדין יצירות ספרותיות ודומיהן. בזכויות יוצרים לרוב קל הרבה יותר להוכיח הפרה מאשר בפטנטים, אבל בתוכנות זה דווקא הפוך – מאוד קשה להוכיח שתוכנה אחת העתיקה מאחרת. תוכנה שמשולבת בחומרה, לעומת זאת, לרוב רשומה יחד עם הפטנט של החומרה אבל לעתים קשה להבחין ביניהן. יש דוגמאות לכאן ולכן, אבל לרוב אם יש חומרה איפשהו ברעיון זה פטנטבילי.

ישנה הבחנה אחת חשובה בזכויות היוצרים החלים על תוכנה – לרוב בזכויות יוצרים, חוץ מהזכות לקניין ישנה גם הזכות המוסרית (הזכות של ישתמשו ביצירה או יגזרו מהיצירה), אבל לא כך בתוכנה. לדוגמה, אדריכל יכול למנוע שיפוצים שישנו את הבניין שעיצב בגלל זכותו המוסרית על היצירה, אבל טיעון זה **לא** עובד בתוכנה!

הרצאה VIII | דיני מלחמה, מדריך טאלין וחוק הסייבר

מלחמות יש כבר אלפי שנים, וכמעט תמיד יש מלחמה איפשהו בעולם ויש למלחמות גם השפעות "חיוביות", בראשון התפתחויות טכנולוגיות. בגלל כל אלו המשפט החל לעסוק במלחמות כבר לפני למעלה ממאה שנה ואכן יש התקדמות – כבר למעלה מחמישים שנה שלא הייתה מלחמה בין ממשלות נבחרות.

לדוגמה, יש עיקרון לפיו לחייל שנשבה יש הרבה זכויות, אבל אם מקבל חנינה, נלחם בשנית ושוב נשבה, מאבד את הזכויות האלה. לאחר מלחמת העולם השנייה, בין היתר בעקבות רצח העם הארמני (בו העותמאנים טענו שהם רשאים לעשות כל מה שחוקי בשטחם), נקבעו זכויות האדם שיש לכל אדם באשר הוא אדם, ואת הרעיון של ג'נוסייד.

משפט בינלאומי פומבי (בין מדינות) מתחלק להסכמי (אמנות שמדינות חותמות עליהן) ומנהגי (מה שמקובל לעשות). משב"ל מנהגי מחייב את כל המדינות אלה אם הן מחוקקות ספציפית אחרת, ואילו הסכמי מחייב רק אם הוא מחוקק בפרלמנט של המדינה. אין שום אכיפה (אפקטיבית, יש בתי דין בינ"ל עם השפעה מינורית) של משב"ל, אבל בגלל שכל מדינה לא יוצא מן הכלל טוענת שהיא הולכת לפי הדין הבינלאומי, עצם הקיום שלו משפיע על איך מדינות מתנהגות.

דיני מלחמה עוסקים בהכרזות והצדקות למלחמה; קבלת כניעה; טיפול בשבויי מלחמה; איסור על כלי נשק מסוימים; והכי שנוי במחלוקת – הצורך הצבאי בתקיפה, והבחנה ומידתיות במתקפות.

עקרונות בסיסיים בדיני מלחמה מודרנית

- צורך צבאי – לכל מתקפה חייב להיות צורך צבאי מובהק.
- הבחנה – אסור לפגוע בתשתיות אזרחים ויש להבחין בין מעורבים לבלתי-מעורבים.
- מידתיות – ההתקפה צריכה להיות מידתית (אי אפשר להטיל פצצת אטום על יריה).
- הימנעות מנזק מיותר – עד כמה שאפשר.

אין שום אמנה שקובעת שאסור להרוג שבויי מלחמה, אבל זה משפט מנהגי ולכן כולם מחוייבים לזה.

קשיים בדיני מלחמה בסייבר

- תגובת נגד – בדיני לחימה אפשר להגיב למתקפה "קינטית" (קלאסית), האם אפשר להגיב למתקפת סייבר?
- אחריות מדינית – לפי דיני מלחמה כל מתקפה קינטית משטח מדינה הוא באחריותה, האם כך גם במתקפות סייבר? האם מתקפת סייבר ממחשבים ממדינה מצדיקה מתקפה (מה אם לא ברור שהגורם הוא מאותה מדינה)?
- הבחנה – האם ניתן להפריד בין מתקפות סייבר על גופים אזרחיים וצבאיים?

עקרונות מדריך טאלין

מסמך החוסה תחת משב"ל מנהגי, גרסתו הראשונה (2013) שנויה במחלוקת, השנייה ב-2017 וממתינים לשלישית. המדריך היה אמור לשקף את החוק הבינ"ל הקיים, אבל מדינות המערב מתנגדות לו.

- מתקפות סייבר זהות למתקפות פיזיות. המתנגדים טוענים שמהותית מתקפת סייבר שונה מקינטית.

- החוק הבינ"ל חל על מתקפות סייבר.
 - הפרת הריבונות במתקפת סייבר זהה להפרה פיזית.
 - התקפת מחשבים מתוך מדינה כן נחשבת שימוש בכוח, ומדינה אחראית על מתקפות של אנשים פרטיים בשטחה. המתנגדים טוענים שמדינה לא יכולה ולכן לא צריכה כלהיות אחראית לכל מה שקורה בתוכן.
- אף מדינה אף פעם לא הודתה שתקפה בסייבר, או שתקפו אותה ולא הצליחה להתגונן, ובפרט מדינות עם היכולת לתקוף שומרות על עמימות.

מוטיבים במתקפות סייבר מהעולם

- לא כל מתקפות הסייבר הן כחלק ממלחמה, בניגוד למתקפות קינטיות שכולן כן. לדוגמה מתקפות לריגול אינן למלחמה.
- גניבה – צפון קוריאה וסין תוקפות וגונבות כסף, בלי לפגוע בתשתיות.
 - גרימת נזק – התולעת בכור האיראני הושתלה ע"י המוסד כדי לפגוע בכור.
 - פוליטיקה – רוסיה התערבה בבחירות בארה"ב.
 - מלחמה – מתקפות בסייבר כחלק מלחמה היברידית.

תגובות נגד נהפכו במובן מסוים למתקפות, לדוגמה ע"י הצבת מלכודת לתוקפים, שליחת דוא"ל שמאיים להפסיק להתקוף. המלחמה נהייה מתמדת. כרגע האכיפה היחידה שיש על מתקפות היא חשיפה לפומבי של המתקפות וסנקציות אישיות על האחראים לכאורה על המתקפה (אף אחד אף פעם לא לוקח אחריות).

כלי נשק אוטונומיים

כלי נשק אוטונומיים כמו מזל"טים נהיים חלק גדול יותר ויותר מהלחימה כיום. ישנן שלוש רמות של אוטונומיה לכלי נשק:

1. In-the-loop – אדם שולח, שולט ופוגע מרחוק באמצעות כלי נשק.
2. On-the-loop – אדם שולח, כלי הנשק שולט ופוגע והאדם מנטר יכול לבטל את המתקפה.
3. Out-of-the-loop – אדם שולח, כלי הנשק שולט ופוגע ולא ניתן לבטל או לשלוט בו.

האז"ם ומומחים מסכימים שכדי שכלי נשק אוטונומי יהיה חוקי, הוא צריך להיות לפחות On-the-loop, כך שיהיה עדיין שיקול דעת אנושי. הבעייתיות ב-Out-of-the-loop קורת כשמטרה נמצאת בבי"ח, ומזל"ט לא יפעיל שיקול דעת ויפגע בהרבה בלתי-מעורבים בניגוד למשב"ל. תמיד יש כלי נשק כאלה תקלות כך שניתן להניח שתמיד יפגעו רבים שלא לצורך במהלך שימוש בו (מה עם מזל"ט שמזהה לפי DNA)?

לוחמת חלל

במהלך המלחמה הקרה היה מאזן אימה – ארה"ב ובר"מ הציבו צוללות אטומיות ליד האחרת למקרה שהיא תתחיל מלחמה אטומית, אז תוכל להחזיר מהר. רייגן הציע ליירט טילים אטומיים מהחלל (לא אפשרי טכנית) וכך התחילה מלחמת הכוכבים. בגלל שבר"מ לא היו משאבים להתחרות בארה"ב, יש אמנות שאוסרות על הצבת כלי נשק בחלל.

הבעיה כיום היא שלא תמיד ברורה ההבחנה בין ציוד צבאי לאזרחי בחלל (לווין סיני שמחסל לווינים זר לדוגמה). כיום האמריקאים מובילים בטכנולוגיה צבאית בחלל וכל השאר (לעומתה) לרבות סין, קוראות לאסור על לוחמת חלל מכל סוג.

תובנות מהמלחמה באוקראינה בסייבר

- המתקפה הראשונית תוכננה שנה מראש (קינטית) אבל לא תכננו שום המשך בגלל הקונספציה שינצחו מיד.
- לוחמת סייבר דורשת הרבה הכנה מראש, ורוסיה לא הכינה מראש ולא ציפתה לסיוע מארה"ב ובריטניה ולכן נכשלה. לכן לוחמת הסייבר נהייתה יותר משלימה מאשר מהותית (הרבה יותר קל להמית טיל מאשר לפרוץ לרשת החשמל).
- כנופיות האקרים שפגעו באזרחי המדינה שלהם התגייסו לטובת המאבק הלאומי.
- רחפנים וכלי נשק אוטונומיים תופסים חלק מרכזי בלחימה (בלי יותר מדי שימת לב לפגיעה והבעייתיות).

הגנה מפני מתקפות סייבר בישראל

חוק הסדרת הביטחון בגופיים ציבוריים מ-1998 מסדיר היררכיות של ארגונים, כל אחת מחוייבת לרמת שמירה שונה: שמירה פיזית (אוניברסיטאות); שמירה על מערכות ממוחשבות; שמירה לאבטחת מידע ועוד.

בישראל יש כמה גופים שאחראיים על יישום ההגנה בסייבר:

- יחידה 443 במשטרה (יחידה די קטנה).
- המוסד והשב"כ.
- אגף התקשוב (מגן) וחיל המודיעין (תוקף) בצה"ל.
- חברות תקיפה והגנה פרטיות.

ב-2011 הוקם מטה הסייבר הלאומי (להגנה על תשתיות לאומיות) וב-2016 הוקמה הרשות הלאומית להגנת הסייבר (במרחב האזרחי). ב-2018 אוחדו השניים למערך הסייבר הלאומי, שכרגע משתף פעולה עם הארגונים האלה ולא מפקח עליהם.

תזכיר חוק הסייבר

כבר שנים שהחוק, שאמור להיחקק בהוראת שעה לשנתיים, הוא תזכיר בשל אי-יציבות פוליטית, ויש לו התנגדות גדולה מצד "הגופים המיוחדים" (צה"ל, שב"כ, המוסד והמשטרה) כי הוא מכפיף אותם למערך הסייבר הלאומי בכל הנוגע להגנה בסייבר. בדומה לישראל, גם בשאר העולם יש הרבה גופים שאחראיים על הגנה בסייבר.

החוק מחולק לשלושה חלקים:

1. פרק ארגוני – מגדיר את מערך הסייבר הלאומי כגוף בטחוני-מבצעי הכפוף לרה"מ.
2. פרק אופרטיבי – מקנה למערך הסייבר סמכויות לאתר ולהתמודד עם מתקפות.
3. פרק רגולטורי – מסדיר סמכויות של המערך לצורכי העלאת החוסן במשק האזרחי בהתאם לתקינה הבינ"ל. הפרק מחריג רשויות מסוימות מהישג ידו של המערך, לרבות ועדת הבחירות, נשיא המדינה ומבקר המדינה (כדי למנוע את דריסת המשטר הדמוקרטי) והגופים המיוחדים.

בפרק זה מוכרז גם כי המערך מאסדר רישוי והסמכות שונות להגנה בסייבר (כך ארגון יוכל לשכור את שירותיו של מומחה סייבר בתנאי שיש לו הסמכה כלשהי שהכרחית לעבודה).

בחוק לא מוגדר המושג סייבר והוא מטיל על המערך אחריות ומטרות עמומות.

סמכויות מערך הסייבר תחת חוק הסייבר

החוק מקנה ל"עובדים מוסמכים" של המערך כל סמכות אפשרית, ככל הנראה בשיטת העז (יורידו הרבה דברים לפני שהחוק יועבר ולכן מציעים דברים מופרכים שיודעים שהם מופרכים מלכתחילה). עובד מוסמך יכול:

- לדרוש כל קובץ או מסמך הנדרשים לחקירת מתקפה;
- להיכנס לכל מקום שיש בו מחשב עם מידע אבטחתי רגיש רלוונטי לחקירת מתקפה;
- להיכנס לבית פרטי או כל מקום אחר עם צו, ובשעת חירום בלי צו;
- לתפוס כל דבר (גם אם בעלי המחשב צד ג' ולא מואשם בדבר) ולהחזיר אחרי 15 ימים;
- לתת הוראות לביצוע פעולות לצורך הגנת סייבר ואלו מחייבות (גם גופים פרטיים).

בחוק יש מתח חריף וברור בין הסמכויות המוקנות, לבין חריות הפרט והזכות לפרטיות. לטענת המערך, הפגיעה בפרטיות מהסמכויות קלה בהרבה מזו הנגרמת מהמתקפות שהוא בא להגן מפניהן, ולכן סה"כ הפרטיות תיפגע דווקא פחות. קשה יהיה לפקח על הסמכויות הללו, אבל לדעת המרצה ניתן לתת כל סמכות (בשל אמונו הגבוה ברשויות), בתנאי שאיתה באה גם האחריות.

הרצאה IX | רכיב הסייבר ואיומיו (מרצה אורח – יגאל אונא)

הרשת מעצבת את תפיסת המציאות בכל תחום בחיים. היא נשלטת ע"י הגמוניה של מספר שחקנים מצומצם, והחקיקה בפיגור חמור מאחורי הטכנולוגיה. בהקשר המסחרי, דאטה הוא הדבר הכי חשוב – חברות עושות מזה הון תועפות – ואין כללי משחק או פיקוח בכלל.

בהקשר הביטחוני, המרחק בין מודיעין שנאסף לאמל"ח ברשת הוא מאוד קטן. תחת האיומים החדשים ברשת, המשטר הדמוקרטי והליברלי פגיעים הרבה יותר, וכאן נכנס הטריידוף בין פרטיות לביטחון לאומי. סייבר הוא "הצד האפל" של תקשורת/טכנולוגיה ממוחשבת לא רק אינטרנטית.

מתקפת סייבר יכולה להיות השגת שליטה למערכת מידע ללא אישור, או מניעת שליטה של בעלי סמכות לאותה מערכת מידע, וכל זאת בדדון. בעבר תקיפות סייבר אספו מידע וגנבו ריכוש אבל עכשיו הן גם גורמות נזק ומשפיעות על התודעה הציבורית.

המלחמות כיום הן מלחמות היברידיות – מלבד המאבק המזוין בלחימה בינ"ל (לדוגמה באוקראינה), ישנן מתקפות DDoS רבות, מוחקני מידע, הפלת תשתיות אזרחיות ועוד מתקפות שנהפכו חלק מהותי מהלחימה עצמה.

כדי להשפיע על תודעת הציבור, תוקפים מפילים תשתיות אזרחיות שנתפסות כגורמים אמינים (מוסדות פיננסיים, ממשל בריאות) ומערערים בקלות יתרה את אמון הציבור, הלא הוא הבסיס של החברה הדמוקרטית.

מאפייני המתקפות בסייבר

- א-סימטריה - מאוד קשה להיתפס וקל מאוד לפגוע.
 - קשה מאוד להוכיח שמתקפה הגיעה ממדינה כלשהי, וגם אם פיזית הגיעה ממדינה כלשהי להוכיח קשר של קבוצת האקרים לממשלה קשה אפילו יותר, כך שענישה נעשית בלתי אפשרי. בנוסף, יש אינטרפול נפרד לארגוני הגנה על גופים אזרחיים בסייבר, כך שאכיפה והרשעה בינ"ל מאתגרות מאוד.
 - המטרות הן בין היתר מטרות אזרחיות פגיעות הרבה יותר ממוצב צבאי פיזי שלא פעלו עד כה למגן.
- שבירת כללי המשחק – אם תקפו אותך, תוכל לגנוב את המתפקה ולהשתמש בה כנגד אחרים; לתוקפים אין גורמים מרסנים כמו שיש בלוחמה קלאסית; כאמור קל לתקוף קשה להגן.
 - גורמים מותקפים, בפרט בכופר, גורמים נזק חברתי-כלכלי כל כך גדול שהממשל נוטה להאשים את הקורבן על שלא התגונן דיו או צימצם את הנזק.

פס"ד מערכת הגבייה צינור הדלק של קולוניאל הושבת לכמה שעות בשלב מתקפת סייבר. הנזק התודעתי והכלכלי שנעשה מתחנות דלק ריקות לפרק זמן קצר היה כל כך גדול שביהמ"ש בארה"ב פסק שקולוניאל אשמה בנזקים שנגרמו מהמתקפה עליה.

מודל האבטחה בישראל מורכב משלושה רבדים – תשתיות מדינה קריטיות כגון חשמל, מים, תקשורת צבאית; שירותים חיוניים כגון משטרה, כיבוי אש (גופי A); והמשק והציבור. בסדר הזה גם רמת המגננה של כל רובד. לגופי A יש רגולטור,

יחידות סייבר שמעוגנות בחוק, שמחויב לבצע ולאכוף את מאמצי ההגנה מפני מתקפות של הארגון. חוק הסדרת הביטחון וטיוטת חוק הסייבר (שהוא שנים טיוטה) הם אלו שמעגנים את הנ"ל.

עולות כמה שאלות מוסריות/חוקיות בכל הנוגע לאחריות של ארגונים על הגנה מפני מתקפות. האם צריך לחייב סגירת חולשה ברגע שנמצאת? האם יש חובת דיווח (כרגע חברות מפחדות לדווח על חולשות מחשש לחקירה פלילית)? מה אם מישהו מת בבית חולים כתוצאה ממתקפה? האם צריך לתת חסינו למותקפים במקרים מסוימים? כרגע האחריות לכל ההגנה על ארגון כלשהו היא על ממונה האבטחה של החברה, גם אם המתקפה מגיעה ממדינה עוינת.

הרצאה X | זכויות יוצרים והליך הוגן (מרצה אורח – עו"ד גיא אופיר)

בעת פיתוח כשכירים בחברה כלשהי, ישנה חזקה שלמעסיק יש זכויות יוצרים על כל מה שהעובד כותב. בעניין זה ביה"ד האזרחי לעבודה מבחין בין הידע איך לעשות משהו (שייך לעובד), לבין הביטוי המעשי של הידע הזה (שייך למעסיק).

כדי לאפשר יצירתיות וקידמה במדע ותרבות, החוק (הישראלי ואחרים) מכיר ביצירה נגזרת – הגנה על זכויות היוצרים של יצירה שמכילה חלק מיצירה מקורית (גם אם רק 5%). פרודיה לדוגמה היא טכנית העתקה, אבל יש עניין בלאפשר אותה, והיא נחשבת יצירה נגזרת. מעבר לכך ניתן לעשות ביצירה שימוש הוגן ביצירה אחרת, גם הוא מוגן בחוק, כלומר העתקה מיצירה מקורית שאינה יצירה נגזרת, שבה הערך המוסף מספיק גבוה שהוא "שווה את הפגיעה" בזכויות יוצרים.

מצד שני יש לשמור על זכויות יוצרים ברמה העקרונית כי בלי הגנה על קניין רוחני לא יהיה אינטרס כלכלי לקידמה במדע וכו', לרבות מקרים בהם מדינות מלאימות פטנטים לתרופות כדי להציל מיליוני בני אדם וכו'. בעיה זו ניכרת אצל עובדי מדינה, שם כל הפטנטים שייכים למדינה ולא היה דירבון להמצאות חדשניות, ומאז עובדי מדינה מקבלים חלק מהתמלוגים.

פס"ד Oracle תבעו את גוגל על הרחבת Java על זכויות יוצרים, ועד היום הם דנים בזה.

בכל הנוגע ל-AI, בדומה לכלבים וקופים, אין להם זכויות משפטיות לצורכי זכויות יוצרים ולא יכולים להיות להם יצירות מקוריות. אם לתוצר של בינה מלאכותית יש תרומה מהותית, היא יכולה להיחשב יצירה נגזרת מהדאטה שלמד עליה. ככלל מי שנתן את התרומה המהותית לרוב זוכה בטענותיו בביהמ"ש בתביעות זכויות יוצרים. בישראלי כרגע חו"ד היועמ"שית מתירה למידת מכונה ומגנה עליה מפני תביעות זכויות יוצרים.

פס"ד דפי זהב עשו crawling ל-144 ובזק תבעו אותם. בגלל שדפי זהב סיווגו מחדש את מספרי הטלפון (תרמו תרומה מהותית לסידור המספרים), על זה היה להם זכויות יוצרים ולכן בזק הפסידו.

היעדר רגולציה כטכנולוגיות חדשות

- קביעת מדיניות קריטית ללא הסדרה – מפתחי אייבוס פיתחו מערכת התראה לטייס אוטומטי למטוסים שלהם, וקבעו פרוטוקול שגרם לנפילת מטוס כתוצאה מאי שימת לב להזדקרות, רק בגלל שהפרוטוקול היה רופף.
- היעדר הליך הוגן – כל פלטפורמה יכולה לחסום מי שהיא רוצה מתי שהיא רוצה בלי הגנה על "האזרח הקטן".
- הזכות להישמע בפלטפורמות חיוניות - התפתחה בשנים האחרונות בפסיקה בגלל החלק הכל כך מרכזי שפלטפורמות אלה תופסות בחברה כיום. מצד אחד יש לחברות את הזכות לעשות מה שבא להן והציבור לכאורה יכול לעבור לאתרים אחרים, אבל המציאות מראה שצרכנים לא מאוגדים והשוק לא רציונלי ולכן נדרשת הגנה על הצרכנים.
- כוח מאסיבי לתאגידי ענק – תאגידים יכולים לעשות נזק הרבה יותר חמור לאזרחים, שאפילו המשטרה ושב"כ לא יכולים לעשות, כי הם דווקא כן כפופים לחוק. את תקנון השימוש אף אחד לא קורא ואפשר לכלול שם סעיפים מקפחים שפוגעים באזרח הקטן.

הרצאה XI | קניין רוחני באינטרנט ופרטיות

פס"ד Sega v. Accolade: סאגה הגנו על פיתוח משחקים לקונסולה שלהם. מישהו פרץ להגנה והפיץ משחקים משל עצמו לקונסולה. החברה תבעה אותו על הפרת זכויות יוצרים והפסידו, מרצון לאפשר תחרות, ומכך שאין באמת זכות יוצרים שהופרה.

בכל הנוגע להגנה על מסדי נתונים, באירופה מסד הנתונים עצמו מוגן כיצירה מקורית מבחינת זכויות יוצרים, ואילו בארה"ב אין שום הגנה ובישראל יש הגנה רק על תוכן מקורי במאגר (לקט או להעתיק מסד נתונים אחר לא מוגן). בלי קשר, פריצה והפצת מאגר מידע ללא רשות היא לא חוקית מהיותה עבירת מחשב (פלילית).

פס"ד אחיטוב נ' הפרד: שניים פיתחו תוכנת הנהלת חשבונות ולשניהם יצא באופן ב"ת את אותן הדרישות ולכן אחד תבע את השני על הפרת זכויות יוצרים. המחוזי פירק לשלושה חלקים בפיתוח שכולם מוגנים בזכויות יוצרים בנפרד: אפיון; עיצוב; ותכנות. הבעיה כאן היא שהגנו על הרבה מעבר לתכנות עצמו (אפיון הוא לעתים נפרד).

בנאפסטר כל מי שנרשם תרם את כל הקבצים שלו (אולי פיראטיים) במחשב לשירות, וכתובתו עם שם הקובץ הועלתה לאתר, כך שמשמשים אחרים יכלו לבקש ממנו את הקובץ באופן ישיר (לא דרך השרת). האם נאפסטר מפרה זכויות יוצרים? היא הסתמכה על סוני נ' יוניברסל אבל בסופו של דבר הופלה משפטית.

פס"ד סוני נ' יוניברסל: סוני ייצרה מכשיר שמאפשר להעתיק תוכן של קלטת, ויוניברסל תבעה אותה בטענה שמשמשים במכשיר שלה כדי להפר זכויות יוצרים. העליון בארה"ב קבע שבגלל שאפשר להשתמש במכשיר לצרכים חוקיים, גם המכשיר הזה חוקי (בדומה לכלל דומה מהמשנה).

נאפסטר לא הצליחו להגן על עצמם במקרה הזה כי 99% מהתוכן שהיה בשרת הפר זכויות יוצרים. גרוקסטר החליפה את נאפסטר עם פרוטוקול P2P ללא שרת מרכזי, אבל הופלו גם הם. כיום זה לא רלוונטי כי יש הכל פיראטי בטלגרם.

פס"ד רמי מור: באתר "הדוקטור" הושמץ רמי מור בטוקבק, והאחרון חשב שהוא יודע מי מאחורי האתר, אז ביקש מביהמ"ש לחייב את האתר לחשוף מי מאחורי התגובות. העליון קבע שאין הליך כזה.

פס"ד פלוני נ' Premier League: אדם שידר באלטרואיזם משחקי כדורגל, ותבעה אותו הליגה שלה זכויות היוצרים על השידורים. המחוזי קבע שמדובר בשימוש הוגן, והעליון הפך את ההחלטה וקרא למחוקק להתערב.

הסעיפים העיקריים בתיקון 5 לחוק זכויות היוצרים

1. הפרה עקיפה של זכות ההעמדה לרשות הציבור (הזכות הבלעדית של בעל זכויות היוצרים להפיץ את היצירה המוגנת), דוגמת קישור לאתר המפר, בתנאי שיש רווח מעשי (מסחרי) מההפרה, דינה מאסר.
2. צו לספקי אינטרנט המורה על הגבלת כניסה לאתר המפר זכויות יוצרים.
3. חשיפת זהות מפרי זכויות יוצרים אנונימיים.
4. סנקציות פליליות על הפרת זכויות יוצרים באינטרנט.

5. 100,000 שקל פיצוי ללא הוכחת נזק על הפרה, כשבפועל מקבלים הרבה פחות.

חשוב להבחין שמדובר בסנקציות וצווים רק בהקשר של זכויות יוצרים, ולא לשון הרע (ולכן לא עוזר לרמי מור). בנוסף אין התייחסות בחוק למנגנוני הגנה טכנולוגיים להגנה על זכויות יוצרים (בארה"ב ובאירופה יש חוקים המתייחסים אליהם).

הקלות בתיקון לחוק זכויות יוצרים

- במקרה שלא יודע מי בעל היצירה על אף מאמצי חיפוש (סעיף 27(א)) ואז נדרשים פרטי קשר למקרה שבעל היצירה יחשוף עצמו ויבקש תשלום.

- מוסדות מוחרגים כגון רשויות המדינה (אם נעשה במהלך מילוי תפקידן), מוזיאונים ומוסדות חינוך, מלכ"רים ועוד.

על אף כל החקיקה, כל המהלכים נכשלו כי הציבור תמיד מוצא דרכים לעקוף חסימות ומגבלות (לדוגמה סדרות). הוצע רעיון בעבר שכל מי שמתחבר לאינטרנט ישלם מס שיחולק בין בעלי זכויות היוצרים, אבל זה כמובן לא עבד, בין היתר כי אי אפשר לקבוע מחיר לדבר כזה. בתאוריית קביעת מחירים, המודל המקובל כיום הוא מחיר השוק (היצע וביקוש), ובלבד שהשוק הוא שוק משוכלל (אפשר להתחרות, אין קרטלים ומונופולים, אין חסימה לכניסה לשוק וכד'). במציאות השוק לא משוכלל והמחיר נקבע ע"י המוכר והציבור צריך "להצביע ברגליים".

האם כולם רמאים?

ניסוי המטריצות של דן אריאלי: נתנו לסטודנטים דפים עם בעיות מתמטיות שעליהם לפתור ולאחר מכן לזכות בתגמול. קבוצה אחת התבקשה להגיש את הפתרון לבוחנת שתחשב את התגמול; קבוצה שנייה התבקשה לחשב עצמאית את התגמול ולדווח לבוחנת; וקבוצה שלישית התבקשה לגרוס את הדפים ואז לדווח את התגמול לבוחנת. התוצאות הראו פער לא זניח אך קטן יחסית בין תגמולי הקבוצות, כאשר ההסבר הוא שאנשים מוכנים להיות רמאים, אבל עד גבול מסוים בו הם מרגישים עצמם רמאים (הפרזה בתגמול הראוי).

ניסוי המקרר המשותף של דן אריאלי: הניחו ליד מקרר משותף מכונת משקאות ובתוך המקרר פחיות קולה, וצלחת ועליה שטרות דולרים. מהר מאוד נעלמו כל הפחיות אבל אף אחד לא נגע בדולרים – המסקנה היא כמו בניסוי הקודם.

תזה מרכזית - כל המגבלות שמגנות על זכויות יוצרים, אינן טבעיות ולכן יתקלו בהתנגדות כבדה מצד הציבור.

לדוגמה, מודל השמלה: מוכרים שמלה במחיר מוזל, בתנאי שניתן ללבוש אותה רק בימי ראשון, או רק בימי שלישי. לעומת זאת, יש מודלים שכן מצליחים שמגנים על זכויות יוצרים, כמו מודל המנויים של ספוטיפיי.

אעפ"כ, נטפליקס לא מודל מוצלח בדיעבד לפחות, כי יש הרבה שירותים שמפצלים ביניהם את תוכני האיכות ואז שוב יש מגבלה לא טבעית על המשתמש אז הוא עובר לפיראטיות. ייסורי המצפון של ויקיפדיה והגרדיאן, שהם חנימיים עם תרומות יזומות, יהפכו בעתיד למודל עסקי פופולרי. חשוב בכל זאת להימנע מהמצב בבעיית הטרמפיסט – כולם משתמשים בשירות חינם על חשבון אחרים, ואז אף אחד לא מתווכח לתמוך בשירות והוא חודל מלפעול.

ירושה דיגיטלית

בדיני ירושה בכללי יש שתי גישות, כשבמציאות רוב הגישות הן איפשהו באמצע.

- אדם קובע למי עובר הקניין שלו לאחר מותו. לדוגמה גונתר הרביעי, כלב שהורש לו 400 מיליון דולר וחי חיי פאר.
- הציבור/החוק יקבע לחלוטין מה לעשות בדבר קניין של אדם מת.

במשפט המקובל הגישה הראשונה מאומצת במלואה, ואילו במשפט הקונט' אחוז מסוים מהירושה של אדם חייב ללכת לצאצאיו (גם אם ביקש במפורש שלא). במשפט העברי (מהמשנה) רק זכרים מקבלים ירושה ובכורות פי 2, ולכן ישנם מעקפים שונים כגון "שטר חצי זכר".

מס ירושה כאינטרס ציבורי

אינטרס הציבור בירושה (מס ירושה לדוגמה) נעשה ברור לאחר ש-Thomas Piketty הראה שקל יותר לעשות כסף מהון קיים מאשר מעבודה קשה, כלומר שירושה רק לצאצאים מונעת ניידות חברתית.

בישראל אין מס ירושה משתי סיבות:

- מס ירושה דורש מס מתנות עשר שנים לפני (כדי שאנשים לא ילבינו את נכסיהם לפני שימותו) וקשה ליישם מס שכזה פרקטית.
- רצו שיהודים עשירים יבואו לארץ ושהכסף שלהם יכנס וישאיר בכלכלה הישראלית, ומס ירושה היה מרתיע אותם.

מידע של אדם שנפטר

פס"ד עו"ד יוסופוף נחשב לאדם עשיר כשחי, וכשמת התגלה שהוא בחובות. נאמניו רצו לדעת אילו נכסים יש לו באמצעות גישה לדוא"ל שלו, אבל גוגל לא הסכימה. למי המידע שייך?

דין מידע של מנוח במציאות

יש שלוש אפשרויות שמתקיימות במציאות במדינות שונות. החריג הוא צרפת שם הגנת הפרטיות חזקה מאוד ולכן המידע של אדם מת לא שייך לאף אחד אחר.

1. חוקים שקובעים מפורשות מה דין המידע (בקרב בארה"ב יהיה "נאמן מידע").
2. הסכמים בין המשתמשים לפלטפורמות בתקנון השימוש (דגש בבריטניה אכן על הצד החוזי).
3. החלת דיני ירושה כלליים.

מחקר בירנהק-מורס

המחקר בדק את דעת הציבור על מתן גישה לשירותים שונים לאחר המוות לאחרים. שליש ביקשו לחסום גישה לגמרי; שליש ביקשו לאפשר גישה לגמרי; ושליש ביקשו לאפשר גישה חלקית. אתרי היכריות כשירות היו החריג בהן רוב מוחלט ביקש לחסום גישה לאחרים למידע שלהם שם.

התזה המרכזית – אין מספיק מודעות לעניין ובנוסף ישנה אי הסכמה בקרב הציבור. הפתרון המוצע הוא העלאת מודעות הטלת חובה על חברות לקבוע מדיניות ולהנגיש אותה, כשקביעה זו תגבר על כל חוק. לדעת המרצה עדיף שברירת המחדל תהיה לפי החוק, ושיש לשאול בעת ההרשמה את המשתמש.

במציאות לפלטפורמות שונות יש הסדרה עצמית בתקנון השימוש – בפייסבוק אפשר רק להנציח דפים, בגוגל אפשר לבקש גישה בתנאי שיש צו (כדי שלא יראה כאילו הם קובעים מדיניות), ובטוויטר נמחק חשבון המנוח.

כרגע אין בישראל פסיקה רבה בנושא ולכן דיני ירושה קלאסיים חלים, ובהם החוקים הרלוונטיים לקניין וירושה, ובפרט לפלטפורמות גם חוקי חוזים והגנת הפרטיות.

סוגיות בהגנת הפרטיות

מכירים בזכות לפרטיות בשלושה רבדים: חדירה פיזית (למקום פרטית, לרבות הגוף); שימוש במידע (ששייך לאדם); והזכות לאנונימיות (הזכות שלא ידעו מי אני). לתאגיד אין זכות לפרטיות.

הרוצח הסדרתי Joseph DeAngelo השאיר עקבות DNA אחריו אבל לא הופיע בשום מאגר. במרוצת השנים המשטרה השוותה את ה-DNA שלו במאגרים של חברות מסחריות של אנשים שמעלים את הריצוף שלהם, ועברה אחד אחד עד שמצאו אותו וכך הורשע – הופרה לו הזכות לפרטיות.

דוגמה נוספת היא ב"ח שאיבחו פרקינסון אצל אדם, אבל לא הראשון ולא האחרון סיפרו לבתו שלה אדם שהיא גם מועדת לפרקינסון. היא ילדה ילד ואובחנה לאחר כמה שנים, גילתה שהרופאים כבר ידעו שהיא מועדת ותבעה אותם על שלא סיפרו לה – האם מגיע לה שיספרו לה (על אבחון אביה)?

GDPR

תקנות (שמגדירות בדיוק מה צריך לעשות, לא דריקטיבה שהיא כללית) שמחייבות כל חברה בעיסוקיה עם אזרחים אירופיים (אחרת כל החברות היו פשוט יוצאות מהאיחוד והתקנות לא היו חלות עליהן). התקנות הן אותן תקנות בכל מדינה באיחוד ומחייבות את כולן. בגלל גודל השוק וההשפעה הפוליטית, התקנות נהיות לאט לאט התקינה הבינ"ל בעניין הגנת פרטיות במחשב. הסעיפים בתקנות נגרים משני עקרונות כלליים:

1. מידע שמתייחס לאדם שייך לו.

2. לכל מי שמתעסק במידע יש אחריות עליו.

ה-GDPR פותר את הבעיה במטאפורה של קפקא, כי הוא מתיר איסוף מידע אבל מחייב שנושא המידע יוכל לשלוט בו.

ישנן שתי גישות לאסדרה (רגולציה):

1. ממוקדת תוצאה – עשה מה שתמצא בתנאי שהזיהום במפעל יהיה מתחת לרף מסוים.

2. מנחה ומפורטת – עשה בדיוק כפי שנאמר לך, בלי קשר לתוצאה, שתגיע בכל מקרה אם תעקוב אחר ההנחיות.

האיחוד בחר בגישת ביניים (ממוקד תהליכים) – לא להכריז על תוצאה ולא לספק מפרט מדויק להתנהגות, וזה נעשה בצדק ובכוונה – אין תמיד תוצאה בפרטיות שאפשר לכוון אליה, אבל הנחיות מדויקות דורשות פיקוח שאינו פרקטי.

באמנה מבחינים בין ה-Data Subject, מי שהמידע עליו, לבין ה-Data Controller, מי שמקבל ושולט במידע (צד ב'), ו-Data Processor שהוא צד ג' שמקבל לידיו את המידע מ-Controller.

סעיפים מרכזיים ב-GDPR

- סעיף 5:
 - יש לעבד מידע לפי החוק ובצורה הוגנת ושקופה.
 - על האדם לדעת שהוא מעביר את המידע שנאסף.
 - יש לאסוף רק את המידע שנדרש לביצוע הפעולה המוצהרת.
 - על המידע להיות מדויק.
 - יש להחזיק את המידע רק לזמן שצריך.ניתן להפר את הנ"ל, ובלבד שניתן אישור מהמשתמש.
- סעיף 9: יש איסור גורף על איסוף נתונים הנוגעים לדעה פוליטית, גזע, דת, פילוסופיה אישית (סוגר מעקפים חוקיים לדת), נטייה מינית ועוד כדי למנוע אפליה פסולה. ישנן החרגות לנ"ל, לדוגמה דברים שהכרחיים לטיפולים רפואיים מונעים, עניין ציבורי ממשי ועוד.
- הסעיף לא אוסר על פרסום פוסטים העוסקים בעמדה פוליטית כי מדובר במידע שחברה אוספת מהמשתמש ושומרת בטבלאות אצלה, ולא דברים הנוגעים למהות המוצר.
- סעיף 13: לנושא המידע צריכה להיות האפשרות:
 - לקבל תיאור של המידע שנאסף עליו;
 - לקבל עותק של כל המידע.
 - לתקן את המידע.
 - למחוק אותו את המידע;
 - לדרוש שהמידע לא יעובד;
 - לבקש שהמידע לא יעבור עיבוד אוטומטי.
- סעיף 32: חובות ה-Controller:
 - הוא צריך להיות accountable.
 - צריך לאמץ פרטיות בעיצוב.
 - למנות ממונה פרטיות מהאיחוד.
 - "לעשות אבטחה היטב" ולהשתמש בהגנות State of the art.
 - לספר לרגולטור אם יש פרצת אבטחה.

הרצאה XII | פרטיות במאגרי מידע ובישראל

הועד האירופי לפרטיות מפרסם קווים מנחים (לא מחייבים) למימוש הכללים התאורטיים של ה-GDPR, שאם הולכים לפיהם ככל הנראה שמוגנים מפני תביעות. הפרה של ה-GDPR מביאה לקנס של 20 מיליון דולר או 4% מהמחזור השנתי של בית העסק (כולל מלכ"ר וכו'). כל חברה מנהלת את הסיכונים שתפר את התקנות לעומת ההוצאות הגדולות הכרוכות בקיום התקנות. התקנות גרמו ל"הנדסת מידע" עולמית, ושינתה את האופן בו חברות אוספות, מעבדות ומנגישות מידע.

עסק ישראלי צריך לבדוק האם התקנות האירופאיות חלות עליו (האם יש לו לקוחות אירופאיים)? אם כן, איזה מידע יש לו, מי מחזיק בו ולמי הוא עובר? האם יש הצדקה חוקית להחזקתו? האם הוא מונגש ללקוחות? עם זאת, עוד לא עמדה למבחן אכיפת ה-GDPR על עסק בארץ.

חוק הגנת הפרטיות

בחוק חמישה פרקים, הראשון מגדיר מהי פגיעה בפרטיות: בילוש, צילום אדם ברשות היחיד, האזנת סתר בה המקליט אינו צד לשיחה, שימוש בצילום/קול של אדם לריווח ועוד.

פרסום שממוקד במיניות אדם היא עבירה בחוק הטרדה מינית אבל מוכלת בהגנת הפרטיות, כשהרעיון הוא שתהיה סטיגמה סביב העבירה שהיא עבירת מין ולא "סתם" עבירת הפרת פרטיות.

חרדי שעובר במצעד הגאווה לא יכול לבקש שסיריו תמונה שלו מהעיתון (גם אם טוען שזה מזיק לו בקהילה שלו) כי ברגע שהשתתף באירוע ברשות הרבים, הוא אינו יכול לטעון לפגיעה בפרטיות.

פס"ד אמסלם היא כדורסלן, שהקבוצה היריבה היו צועקים עליו שהוא הומו. כשהתקיימה האולימפיאדה הגאה בלוס אנג'לס, "הארץ" דיווח שאמסלם "לא לבד", אז אמסלם תבע את העיתון על הפרת הפרטיות. העיתון אכן הפסיד, כי בית המשפט קבע שמה שמשנה הוא לא עמדת הארץ בנושא אלא עמדת הסביבה של אמסלם, ושם נפגעה לו הזכות לפרטיות.

מאגרי מידע בישראל

מאגרי מידע מוגדרים תקנות הגנת הפרטיות (אבטחת מידע) ככל אוסף נתוני מידע (גם אם לא על בני אדם, בניגוד ל-GDPR). שמוחזק למטרות עסק. התקנות שכל מאגר מידע שמקיים אחד מחמשת הבאים צריכים להירשם ברשם מאגרי המידע (עם אחריות קפידה, כלומר נחשב שביצע עבירה גם אם לא התכוון), ומי שמחזיק במאגר ללא רשות דינו עד שנת מאסר:

1. מספר האנשים שיש מידע עליהם הוא למעלה מ-10,000.
2. המאגר מכיל מידע רגיש (אישיותו או צניעותו של אדם, בריאותו, כלכלתו, דתו או אמונתו).
3. המאגר כולל מידע שלא נמסר בהסכמת או מטעם האדם.
4. המאגר שייך לגוף ציבורי.
5. המאגר משמש לדיוור ישיר (דוא"ל).

4 רמות משטרי מידע בתקנות

תקנות הגנת הפרטיות מגדירות 4 רמות "משטרי מידע" (מאגרי מידע), שהמחזיק בכל אחת מהן באחריותו לקיים את כל הכללים המצטברים (מהרמות מתחת) שמפורטים בחוק (חוץ מלהיות רשום אצל הרשם). הרשם רשאי לדרוש ממנהל המאגר יותר מהמפורט בתקנות, או פחות (לדוגמה מאגר מידע שמוסמך לפי תקינת ISO לא מחויב בתקנות) הרמות הן:

1. מאגר המנוהל ע"י יחיד: מאגר מידע כהגדרת החוק שבו יש מנהל יחיד, עם לכל היותר 2 נוספים עם הרשאה.

- המאגר צריך להיות במקום מוגן.
 - המנהל צריך לכתוב מסמך הגדרות על המאגר (אילו נתונים מוכלים בו, למה, באיזה פורמט וכו').
 - בכל שנה צריך לבדוק האם המאגר מכיל יותר נתונים משנדרש כדי לבצע את תפקידו.
2. רמת אבטחה בסיסית: מאגר שאינו מנוהל ע"י יחיד ואינו בינוני או גבוה.
- המנהל צריך לגבול ניהול אבטחת מידע.
 - צריך לכתוב מסמך טכני של הגדרות המאגר (מעבר למסמך ההגדרות, ולכלול את החומרה של המאגר).
 - לבדוק ולתדרך בעלי הרשאות.
 - לתעד אירועי אבטחה לשמור את התיעוד ל-24 חודשים.
3. רמת אבטחה בינונית: מאגרים של גופים ציבוריים או המכילים מידע רפואי, עבר פלילי, דעות או דת של אדם וכו'.
- נדרשת אבטחה פיזית למאגר.
 - תיעוד של כל בעלי ההרשאה.
 - יש להודיע לרשם על אירוע אבטחה חמור, שברמה זו הוא שימוש מהותי של אדם בלתי מורשה במאגר.
 - צריך לערוך ביקורת חיצונים אחת לשנתיים.
 - דיון באירועי אבטחה אחת לשנה.
4. רמת אבטחה גבוהה: מאגרים עם למעלה מ-100 בעלי הרשאה או מידע על למעלה מ-100,000 אנשים.
- יש להודיע לרשם על אירוע אבטחה חמור, שברמה זו הוא כל אירוע של גישה בלתי מורשת למאגר.
 - יש לבצע סקר סיכונים ומבדקי חדירות.
 - דיון באירועי אבטחה אחת לשלושה חודשים.

פס"ד כהן ואח': חוקרים פרטיים כיום משיגים מידע בעיקר דרך מאגרי מידע שאין להם גישה אליהם. במקרה זה לכמה מהחוקרים המואשמים היו אנשי קשר ברשויות המדינה והם סחרו במידע עם חוקרים אחרים – חלקים הורשעו וחלקם זוכו. ברמת העקרונית, חוקר פרטי כבר לא יכול לעשות את העבודה שלו בצורה חוקית.

ה-GDPR לעומת התקנות בישראל

אפשר לענות לתקנות הגנת הפרטיות בלי לקיים את ה-GDPR ולהפך, ולכן עסק ישראלי עם לקוחות אירופאים צריך לבצע את שניהם. ברמה העקרונית, הדגש ב-GDPR הוא על זכויותיו של האדם עליו המידע, ואילו בישראל הדגש הוא על אבטחת המידע.

דגשים ב-GDPR שלא מופיעים בתקנות הישראליות:

1. קיימת הזכות להישכח (The right to be forgotten) שלא קיימת בישראל - לכל עבירה יש מספר שנים שלאחריו ניתן לבקש למחוק את ידיעות על קיומה.
2. קיימת הזכות לקבל את המידע שנאסף ונדרש אישור גורף לאסוף אותו.
3. יש הגבלות על אוטומציה (עיבוד קו"ח אוטומטי לדוגמה).
4. מתעסק רק עם אנשים חיים, כשבבישראל חל על הכל (בפרט מתים).
5. כללים ותאוריה ללא הנחיות פרקטיות.

דגשים בתקנות הישראליות שאין ב-GDPR:

1. דרישות של מסמכי הגדרות ומיפוי מאגרים.

2. אכיפה אזרחית ופלילית ערה.

3. מעשי עם הגדרות ברורות.

תיקון 13 לחוק הגנת הפרטיות המתוכנן אמור להגביל את סמכויות הרשם כך שיוכל להטיל סנקציות כלכליות וענשים פליליים למפרי התקנות, לדרוש ערבויות ממנהלי המאגר למקרה של אירוע אבטחתי, וסמכויות חיפוש וחקירה.

ישנם הרבה מאוד פסקי דין המאזכרים את תקנות הגנת הפרטיות, רבים מהן תובענות ייצוגיות נגד חברות שדלף מהן מידע.

פס"ד אבישר נ' קריית מוצקין (עדיין בדיונים): ראש העיר תיחזק מאגר מידע על חשבון העירייה עם מידע על עמדות פוליטיות של תושביו. לא היה רשום והפר את הזכות לפרטיות.

האם פסקי דין צריכים להיות פומביים? יש טענות טובות שזה מרתיע תובעים צודקים שמפחדים להגיד דברים שיפגעו להם בפרטיות שחשובים לתביעה. כרגע בי"ד לענייני משפחה כברירת מחדל בדלתיים סגורות (מה שמעלה טענות טובות על פעילות בעייתית במחשכים) והשאר פומבי. ייתכן שישנו פתרון טכנולוגי כמו אנונימיזציה שיכול לפתור את הבעיה.

פס"ד הנהלת בתי המשפט מנעה חיפוש לפי שם של פסקי דין במטרה לשמור על פרטיות הנידונים (אפשר רק לפי מספר), זה הגיע לבג"ץ והנהלת בתי המשפט הפסידה ועבשיו אפשר לחפש לפי שם.

המגמה בעולם היא אכן לאפשר לאדם לשלוט על המידע שלו (המטאפורה של קפקא).

סוף.