
האוניברסיטה העברית בירושלים

סילבוס

דיני סייבר - 67398

תאריך עדכון אחרון 12-09-2019

נקודות זכות באוניברסיטה העברית: 2

תואר: בוגר

היחידה האקדמית שאחראית על הקורס: מדעי המחשב

השנה הראשונה בתואר בה ניתן ללמוד את הקורס: 0

סמסטר: סמסטר ב'

שפת ההוראה: עברית

קמפוס: קרית א"י ספרא

מורה אחראי על הקורס (רכז): השופט בדימוס ד"ר אברהם טננבוים

דוא"ל של המורה האחראי על הקורס: avi3333@gmail.com

שעות קבלה של רכז הקורס:

מורי הקורס:

תאור כללי של הקורס:

השתלבות המחשב בחברה המודרנית גורמת לשינויים טכנולוגיים וחברתיים שסופם איננו ברור עדיין. יש שהגדירו זאת כמהפכה החשובה ביותר מאז מעבר האנושות מחיי נוודות לחקלאות.

לכך יש להוסיף את ההתפתחות האחרונה של רשתות המחשבים שבראשם אם כל הרשתות - האינטרנט. אלו מחוברים גם למכשירים בעלי כוח המחשוב שאינם מוגדרים כמחשבים כגון טלפונים סלולאריים, טלוויזיות אינטראקטיביות, שלא לדבר על ה - 'אינטרנט של הדברים'.

שילוב האינטרנט בחיי המסחר והחברה עורר בעיות משפטיות שדורות קודמים לא שיערום. שאלות של סמכות שיפוט, אנונימיות, כריתת חוזים והפרתם, פרטיות, נזקים, לשון הרע, ורבות אחרות. יום יום מתמודדים בתי המשפט ברחבי העולם עם שאלות חדשניות אלו, והפתרונות שונים, משתנים, וחלוקים.

בעתיד הלא כל כך רחוק נצטרך כנראה לדון בשאלות שכיום נראות במדע בדיוני אך כבר עכשיו יש בהן שיח משפטי ער כגון זכויות אזרח לרובוטים, מעמדם המשפטי של מחשבי על, אחריות על מכונת ללא נהג ועוד.

גם למשפטנים מנוסים וותיקים קשה להתנהל במרחב הסייבר המשפטי, ובוודאי לכאלה שאינם משפטנים. לצערנו, אי הבהירות הקיימת כיום יכולה לגרום לאיש מחשבים לבצע פעולות שרק בדיעבד יתברר לו כי היו אסורות לביצוע. ניתן כמה דוגמאות:

- - איש מחשבים מבקש לאחסן את אתרו על מחשבי חברת אחסון כלשהי. אולם היות והוא חושש הוא רוצה לבדוק בעצמו את אמצעי האבטחה של אתרי החברה על ידי שימוש בכמה תוכנות תקיפה/בדיקה. האם מותר לו הדבר? האם הוא צריך לקבל אישור ממישהו? האם בכלל מותרת האחזקה של תוכנות שיכולות לשמש לבדיקה תקיפה?

- - איש מחשבים הצליח לפתח אפליקציית הצפנה זולה שיכולה לעזור להצפין מסמכים/מסרים. האם מותר לו לשווק זאת דרך האינטרנט לכל דכפין? האם הוא צריך לקבל אישורים ממישהו לכך? האם הדבר תלוי ברמת ההצפנה ו/או בגורמים אחרים?

- - חוקר אקדמי מבקש ללמוד על פעולות תוכנות כופר ועל העבריינים העוסקים בכך. לשם כך החליט לפנות דרך ה- web dark למוכרי התכנות ולהציע לקנות אותן, לברר את מחיריהן ואת רמת פעולתם, להתמקח על המחיר, לבדוק אותן טרם קנייתן, ואולי אף לרכוש אותן בסופו של דבר. כל זאת כדי ללמוד על יוצריהן ועליהן. האם מותרות לו פעולות אלה? או שייחשב כמי שרוכש סמים בשוק העברייני על מנת ללמוד על שוק הסמים?

אלו הן רק דוגמאות וקיימות רבות כאלו. מטרת הקורס היא לתת מעין מפה ובסיס לסטודנטים למחשבים על המצב המשפטי הקיים, על הפעולות שמהן צריכים הם להיזהר, ועל הדרכים לברר את המותר והאסור.

מטרות הקורס:

לתת לסטודנטים למחשבים רקע משפטי קצר שיוכל להבהיר להם את המותר והאסור ואת הבעיות

המשפטיות שיוכלו להיתקל בהם בעתיד בבואם ליישם את אשר למדו.

תוצרי למידה

בסיומו של קורס זה, סטודנטים יהיו מסוגלים:

להכיר את מושגי היסוד במשפטים היכולים להיות רלוונטיים לעבודתו של איש המחשבים

דרישות נוכחות (%) :

על פי נוהלי החוג

שיטת ההוראה בקורס: הרצאות מלוות בחומרי קריאה ודין בכיתה

רשימת נושאים / תכנית הלימודים בקורס:

רשימת הנושאים:

א. מבוא למשפטים

היות ואין מדובר במשפטים, מבוא קצר למשפטים יהיה הכרחי (כשיעור-שניים מקסימום). נתאר בקצרה את שיטות המשפט השולטות כיום בעולם (קונטיננטלי והמקובל), את מקורות המשפט הישראלי, דרכי החקיקה, וכמה מונחי יסוד הכרחיים במשפט פלילי.

ב. סמכות שיפוט וברירת הדין

דיני העונשין, ככלל, חלים על התנהגות המתרחשת בגבולות המדינה. מהם גבולות האינטרנט? האם לאינטרנט יש גבולות? איך מתייחס לכך החוק? האם יכולה מדינה אחת לנסות להסדיר את האינטרנט? מה הדין כשאותה פעולה ברשת אסורה במדינה אחת ומותרת במדינה אחרת? (למשל, כאשר חופש הביטוי רחב יותר במדינה אחת מאשר אחרת?) איזה חוק יחול על מפתח התכנה הישראלי? מהן הוראות החוק הישראלי? ואלו אמנות בינלאומיות אם בכלל חלות על כך?

ג. חוק המחשבים הישראלי ומגבלותיו

חוק המחשבים הישראלי חוקק בשנת 1995 לאחר עשר שנות מעבר בוועדות שונות וכבר בזמן חקיקתו לא היה לגמרי מעודכן. רשת האינטרנט כלל לא מופיעה בו ואין בו התייחסות אליה. אך בכל מקרה הוא החוק הרלוונטי ביותר לעבירות מחשבים ונעבור עליו בקצרה.

ד. רגולציה ותקינה של הגנת הסייבר

מיהו/מיהי 'מומחה' לצורך הגנת הרשת? באיזה אמצעים הוא יכול לנקוט? למי מותר לו להעביר את אמצעי ההצפנה/פענוח? האם הגנה 'פרו-אקטיבית' מותרת? ואיך יוגדר הגבול הדק בין הגנה להתקפה? יש בעולם (ובישראל) ניסיון לרגולציה ותקינה של העוסקים בהגנת סייבר ונעסוק בו. בישראל ישנה בעיה נוספת של ייצוא אמצעי הצפנה/פענוח היכולים להיחשב כ - 'נשק' ובשל כך יש עליהם רגולציה מיוחדת.

ה. מטאפורות בדיני הסייבר - וההשלכות על החקיקה והפסיקה

משפטים אינם מתיימרים להיות אנשי מחשבים וטכנולוגיה. אשר על כן, פעמים רבות מוסברות תופעות בעולם הסייבר בהסתמכות על חוקים קיימים בעולם הפיזי (למשל, 'אתר' אינטרנט מושווה לבית, והשתלטות על אתר נחשבת כ 'פריצה לבית'). הסתמכות זאת מעוותת את החקיקה והפסיקה

ודוגמאות יובאו לגבי מספר מושגים כדי להיזהר מכשלים אלו.

ו. חדירה למחשב

מהי עבירת החדירה למחשב? באלו ערכי חברה פוגעת החדירה? האם מדובר בעבירה טכנולוגית או משפטית? האם בכלל ניתן לדבר על התקשרות למחשב כעל 'חדירה'? האם כל חדירה אסורה? איך פורשה זו בארץ ובעולם?

ז. הדין המשפט של נזקקות למיניהן

מה דינם של וירוסים, סוסים טרויאנים, תוכנות DDoS, וכיוצא בזה? מתי תוגדרנה תוכנות כנזקקות? האם מותר לפתח נזקקות מעין אלו? באלו תנאים? למי מותר להחזיק בהם? מה אומרים על כך החוק והפסיקה בעולם ובישראל?

ח. דינו של מידע אישי לאחר המוות

אין לך כמעט אדם שאין לו חשבונות ברשתות חברתיות, חשבונות דוא"ל, אתרי קניות, ועוד? המחזיק מות לאחר אלו חשבונות של דינם מה. (שבהם הידועים הם Facebook, Gmail, Amazon) האם החוק מטפל בכך? אמור לטפל בכך? מה צריך להיות ההסדר הראוי? מה הדין הנוהג בארץ ובעולם.

ט. פגיעה בפרטיות ומאגרי מידע.

מושג הפרטיות הוא מורכב וכנראה משתנה מחברה לחברה ומתקופה לתקופה. כיצד נחיל את חוקי הפרטיות בעידן האינטרנט? האם אותם חוקים נאכפים גם לגבי השחקנים 'הגדולים' ברשת? (גוגל, פייסבוק, אמאזון). כיצד ישפיעו תקנות הפרטיות החדשות באירופה (GDPR) על ישראל? וכיצד ישפיעו התקנות הישראליות החדשות של אבטחת מידע?

י. מדריך טאלין ודיני מלחמה במרחב הסייבר.

אין כיום ספק שכל מלחמה עתידית תכלול בתוכה גם מלחמה במרחב הסייבר. מה מותר ומה אסור במלחמת סייבר? האם תקיפת סייבר נחשבת כמעשה מלחמתי המצדיק תגובה מלחמתית? האם מדריך טאלין שנכתב לצורך כך מיושם בפועל? מה מקומה של ישראל בלוחמת סייבר?

יא. קניין רוחני, ההגנה עליו והפגיעה בו

מהו קניין רוחני? איך התפתחה ההיסטוריה ההגנה עליו עד היום? האם קיימת הגנת קניין רוחני על תוכנה וחומרה? כיצד יכול איש מחשבים להגן על פיתוחיו? והאם דיני הקניין הרוחני מתאימים למציאות הטכנולוגית כיום? דגש יינתן על הצד הפלילי בקניין הרוחני הקשור להפרתו.

יב. שאלות משפטיות של ביטקוין וכסף וירטואלי

ישנם לא מעט מומחי מחשבים העושים שימוש בביטקוין. אבל האם הביטקוין הוא מטבע או סחורה? האם הוא הילך חוקי בישראל? האם המשתמשים בו עוברים עבירה? האם כורי הביטקוין חייבים לשלם מס הכנסה? האם עסקת ביטקוין איננה חייבת במע"מ? לכל אחת מהתשובות ישנה השלכות משפטיות משלה, וחלקן אף פליליות.

יג. שאלות משפטיות של מכונית ללא נהג

מהן המכונית האוטונומית והמכונית המקושרת? מה כבר קיים ומה מתוכנן לגבי מכונית ללא נהג? מי יהיה אחראי למקרה של תאונות דרכים? מי אחראי על מניעת פריצה לתכנות המכוניות ללא נהג? מה הרגולציה שכבר קיימת בארץ ובחול?

יד. פסיקה עדכנית ואחרונה

יובאו דוגמאות למקרים אמיתיים ועדכניים שבהם דנו בתי המשפט בארץ ובחו"ל בדיני סייבר בשנים 2017-2018 והשלכותיהם על פעולות חברות ואנשי המחשבים.

חומר חובה לקריאה:

מאמרים ופסקי דין שיהיו נגישים על אתר הבית של המרצה

חומר לקריאה נוספת:

אין

הערכת הקורס - הרכב הציון הסופי :

מבחן מסכם בכתב/בחינה בעל פה 100 %

הרצאה 0 %

השתתפות 0 %

הגשת עבודה 0 %

הגשת תרגילים 0 %

הגשת דו"חות 0 %

פרויקט מחקר 0 %

בחנים 0 %

אחר 0 %

מידע נוסף / הערות:

חלק מהמבחן המסכם יהיה מבחן ביניים שיערך באמצע הקורס (על החומר שנלמד עד אז). בסוף הקורס יהיה מבחן סופי (על כל החומר).

אם ציון מבחן הביניים יהיה גבוה מציון המבחן הסופי, ערכו יהיו 40%.

אם ציון מבחן האמצע יהיה נמוך מציון המבחן המסכם, ערכו יהיה 20%.

תהיה אפשרות לקבלת עד עשר נקודות בonus על השתתפות והגשת מטלות רשות