בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: **כב' השופט כ. סעב** **תאריך:** **28/02/2006**

בעניין: **מדינת ישראל** **המאשימה**

נ ג ד

לרמן מיכאל, ת.ז. 05747027 **הנאשם**

הכרעת דין

רקע כללי

האם בפנינו נאשם שערך והכין "סוס טוריאני" ולאחר מכן פעל להשתלתו במחשבים מרוחקים, השתלה שאפשרה לו השתלטות מרחוק, שליפת קבצים אישיים או שמא בפנינו גולש אינטרנט תמים, שפורץ מחשבים מתוחכם השתלט על מחשבו האישי והשתמש בו כבסיס לביצוע עבירות כלפי מחשבים אחרים.

העבירות שמיוחסות לנאשם

המאשימה מייחסת לנאשם את העבירות הבאות:

א. שיבוש או הפרעה למחשב או לחומר מחשב, עבירה על סעיף 2 לחוק המחשבים, התשנ"ה-1995. (להלן: "**חוק המחשבים**").

ב. חדירה לחומר מחשב כדי לעבור עבירה אחרת - עבירה על סעיף 5 לחוק המחשבים.

ג. עריכת והחדרת נגיף מחשב, עבירה על סעיף 6 לחוק המחשבים.

ד. פגיעה בפרטיות, עבירה על סעיף 5 לחוק הגנת הפרטיות, התשמ"א- 1981 (להלן: "**חוק הגנת הפרטיות**").

עובדות כתב האישום

א. החל מיום 13.4.00 ובעת הרלבנטית לאישום זה, היה הנאשם מנוי לקבלת שירותי אינטרנט בחברת "**בזק בינלאומי**", ושם המנוי שלו היה "**mirlan**", בנוסף היה הנאשם רשום כמשתמש בתוכנת "**ICQ**", ומספר המשתמש שלו היה 17581504. מספר הטלפון בביתו של הנאשם, ממנו בוצעה ההתחברות לרשת האינטרנט היה: 8212028 – 04.

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

ב. במהלך חודש דצמבר 2000, במספר הזדמנויות (ביניהן בתאריך 23.12.00 ופעמיים בתאריך 29.12.00), פרסם הנאשם הודעות בפורום אליהן צירף קובץ מחשב שהכיל וירוס מחשב מסוג "**סוס טרויאני**", וזאת בכוונה שיוכל לחדור, באופן לא חוקי, למחשביהם של הגולשים שיורידו את הקובץ.

ג. בהזדמנויות אחרות (ביניהן בתאריך 20.01.01 בשיחה עם משתמשת בכינוי "**Daniella**") הפיץ הנאשם את וירוס המחשב הנ"ל גם באמצעות תוכנת "**ICQ**", וזאת באמתלה שמדובר בקובץ "**תמים**".

ד. הנאשם ביצע את הפעולות האמורות מהמחשב שבביתו, ובאמצעות קו הטלפון המחובר לדירתו. בהמשך, חדר הנאשם באופן לא חוקי תוך שניצל את הפירצה, שנפתחה לעיניו במחשבים בהם השתיל את הוירוס הנ"ל, על מנת לעיין במסמכים אישיים של בעלי אותם מחשבים, ולהעתיק את תוכנם למחשבו האישי. בין יתר המחשבים אליהם חדר, באופן המתואר לעיל, היו מחשביהם של כוכבי שמש וקרן איינזברג.

ה. עוד נאמר בכתב האישום, שהנאשם איים על משתתפי הפורום בחשיפת פרטיהם האישיים, ובהמשך לאיומיו חשף מספר פרטים, עליהם למד מהמסמכים האישיים אותם העתיק, באופן המתואר לעיל.

ו. הנאשם השתמש בתוכנת "ICQ" והתחבר גם תחת מספר מנוי, שאינם שלו, והשייכים לבעלי המחשבים, אליהם חדר. פעולה זו אף גרמה לתקלות שונות במחשבים שנפגעו.

ז. במעשיו המתוארים לעיל, חדר הנאשם לחומר מחשב שלא כדין, שיבש פעולתם של מחשבים, ערך נגיף מחשב והחדירו למחשבים אחרים ופגע בפרטיותם של בעלי המחשבים, אליהם חדר.

בטרם הבאת הראיות, יש להבהיר מספר מושגים ולהביא מספר הגדרות שכן, בתיק שזורים מושגים טכניים רבים, שאין מנוס אלא מלהבהירם.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

הגדרת מושגים ועבירות ברשת האינטרנט

בכתב האישום הובאו מספר הגדרות שחשובות לענייננו, להלן אביא אותן, אך תחילה אקדים מספר מילים על אופי העבירות, שמתבצעות ברשת האינטרנט, יפים לענייננו הדברים שנאמרו ע"י השופטת רוטלוי בתפ 40250/99 (תל אביב) **מדינת ישראל נ' מונדיר בן קאסם בדיר**:

> **"בעידן המחשב והאינטרנט, שוב אין העבריין נזקק לגעת באופן פיזי במושא העבירה. עבריין המחשב, בדומה לעבריין ה"צוארון הלבן" פועל בדרכים מתוחכמות, לעתים במסגרות חובקות עולם, תוך התעלמות מגבולות גיאוגרפיים, ובכך מנסה להסוות את פעילותו העבריינית. כפועל יוצא, ברי, כי ראיות ישירות אך לעתים רחוקות יכריעו את הכף לחובתו. בהקשרים אלו, בכוחן של ראיות נסיבתיות להוות משקל מכריע בהוכחת אחריותם של עברייני המחשב לביצוע העבירות המיוחסות להם."**

כתובת ה- I.P

לכל מחשב שמחובר לרשת האינטרנט יש מספר ייחודי בכל רגע נתון, מספר זה הנו בבחינת כתובת של המחשב, הכתובת הזו נקראת I.P (Internet protocol) (להלן: "**כתובת I.P**") בת"פ (י-ם) 3047/03 **מדינת ישראל נ' מזרחי אבי** (ניתן ביום 29.2.04) (להלן: "**פרשת מזרחי**") ניתנה סקירה מקיפה ע"י כבוד השופט אברהם טננבוים ביחס לרשת האינטרנט, ובין היתר גם על כתובת ה- I.P שם נאמר:

> **"... כבר בשלב התפתחות מוקדם של רשת האינטרנט התברר כי קל הרבה יותר לזכור שמות מאשר 4 מספרים אקראיים. לצורך כך קיימים מספר "שרתי שמות" ... כאשר אנו מקישים את שם האתר שאליו ברצוננו לגלוש ישנם שרתי שמות שאליהם שולח המחשב שלנו את כתובת האתר והם מחזירים לו את המספר. אשר על כן, ישנו מעין "תרגום" של השמות הידועים למספרים. כך למשל מספרו של אתר המוסד הוא 147.237.72.43, ושל אתר בית המשפט 10.1.1.48**

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

> **23..... כל ספק אינטרנט מקבל מלאי כלשהו של מספרים. כאשר אחד המנויים מתחבר אל הספק הוא מקבל באופן זמני את אחד המספרים המוקצים לספק האינטרנט שלו ומספר זה משמש אותו במשך גלישתו. כאשר הוא מתנתק מהספק הופך מספר זה להיות חופשי ומשתמש אחר שמתחבר דרך הספק מקבל את המספר שהתפנה. בניגוד למשתמשים ביתיים, הרי לשרתים מוקצה כתובת קבועה. זאת משום שלשרתים אלו ניגשים הרבה יותר וכתובת קבועה תחסוך רבות."**

"**סוס טרויאני**" – תוכנת וירוס מוסווית, שניתן להחדירה למחשבים באמצעות רשת האינטרנט והמאפשרת, בין היתר, כניסה סמויה עתידית למחשב בו הושתלה. השימוש בתוכנה זו יכול לתת למי שמשתילה במחשב גישה מלאה לכל החומר האגור במחשב הנגוע. כך ניתן, לערוך, למחוק ולשנות את הקבצים השונים שבמחשב, וכן לצפות בכל הקבצים השונים. פעולות אלו יכולות להתבצע בלי שבעל המחשב יהיה מודע כלל לפריצה למחשבו.

"**ICQ**" – תוכנת מחשב שנועדה לשימוש גולשי האינטרנט. התוכנה מאפשרת לגולש למצוא את חבריו ברשת האינטרנט ו"להתרועע" עימם בזמן אמת. הגולש יוצר רשימת קשר (contact list), אשר מכילה את אותם האנשים שעימם הוא רוצה לתקשר, להם הוא יכול לשלוח הודעות (message), לשוחח עימם בזמן אמת (chat), לשלוח קבצי מחשב ועוד. לכל משתמש בתוכנה יש מספר מנוי אישי. באפשרות המשתמש לקבל מספר רב של מספרי מנוי, ולהשתמש באותה תוכנה בכל אחד ממספרי המנוי, ללא שיהיה צורך בתוכנה נפרדת לכל מנוי.

"**פורום**" – אתר אינטרנט או חלק מאתר אינטרנט, המיועד להעברת מסרים בין גולשים. פורום יכול שיהיה כללי או לנושא מוגדר, כגון חדשות. גולש אינטרנט, המבקש להשאיר הודעה בפורום, עושה זאת תחת כינוי, אשר הוא בוחר לעצמו, לשם כתיבת ההודעה בלבד. במידה ויחפוץ בכך, יכול הגולש לכתוב הודעות שונות תחת כינויים שונים. במסגרת הפורום ניתן גם להעביר קבצי מחשב בין הגולשים השונים.

"**העלאת קובץ**" – העתקה של קובץ מחשב, הנמצא במחשב פרטי, אל רשת האינטרנט – למשל כחלק מהודעה בפורום.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

"**הורדת קובץ**" – העתקה של קובץ מחשב, מרשת האינטרנט אל מחשבו הפרטי של הגולש ברשת.

תשובת הנאשם

הנאשם הודיע שהוא איננו מודה בעובדות המפורטות בכתב האישום.

מהלך העניינים

שתי טענות מרכזיות בפי הנאשם: **האחת**, שלא הוכח מעל לכל ספק סביר שהוא ביצע את העבירה של הפצת הווירוס. **והשנייה**, אדם אחר השתלט על מחשבו, והשתמש בו בתור פלטפורמה או בסיס לביצוע עבירות כלפי קורבנות שונים.

לאור דברים אלו אדון תחילה בעבירה של החדרת הווירוס למחשבי הקורבנות, שכן רק אם נגיע למסקנה שהנאשם ביצע מעשה זה, יהיה מקום לדון בעבירות האחרות, שהן תלויות ונגזרות מהעבירה של הפצת הווירוס. במקרה דנן, החדירה לחומר המחשב, הפגיעה בפרטיות, ושיבוש העבודה במחשב אפשריים רק בהנחה ויוכח שהנאשם כן החדיר את הווירוס. לאחר מכן, אתייחס לטענה השנייה לפיה מישהו אחר ביצע את העבירות.

הרקע לפתיחת החקירה

חקירת המשטרה נפתחה לאור מידע מודיעיני שהגיע למפלג עבירות מחשב ביאח"ה, לפיו במהלך חודש דצמבר 2000, גולש שכינה את עצמו "משה-גרוס", פרסם בפורום האקטואליה של "**IOL**" הודעות, שאליהן צירף קבצים שהכילו וירוס מסוג סוס טוריאני.

מבדיקה שנערכה במשטרה, התברר שאכן קבצים אלו נגועים בסוס טרויאני מסוג "**SUB7**" **(ראה, ת/52)**. כמו כן, התברר שמקור הקבצים הנו ביתו של הנאשם, למסקנה זו הגיעה המשטרה באמצעות בדיקת דיסקיט שהכיל את הוירוסים וכן בעזרת צו ביהמ"ש שהורה לבזק בינלאומי לגלות מי בעל כתובת ה- "**I.P**" שממנה נשלח הקובץ.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

בדיקה זו העלתה שבעל הכתובת השתמש בחשבון אינטרנט בשם "**MILRAN**", והוא שייך לנאשם, כמו כן, העלתה הבדיקה שהחשבון היה פעיל בזמנים הרלבאנטיים שבהם הופץ הוירוס, וששההתקשרות בוצעה ממספר הטלפון שבבית הנאשם.

הערה מקדמית: קבילות המסמכים שהכין החוקר נסר

במהלך החקירה חלה החוקר נסר, אחד החוקרים בצוות החקריה, במחלה קשה ולאחר מכן למרבה הצער נפטר. הצדדים הסכימו על הגשת המסמכים, תוך שההגנה שומרת לעצמה את הזכות לתקוף את קבילותם. בסיכומה בעמוד 29 הבחינה ההגנה בין מסמכים מהותיים לבין מסמכים טכניים, וטענה שרק הסוג האחרון קביל.

לאור עמדה זו יש להכריע בשאלה האם המסמכים **ת/42 ות/43 א-יג**, קבילים הם.

המאשימה בסכיומיה (עמודים 2-9) סקרה בהרחבה את הפסיקה בסוגיה זו ולטעמה לאור עובדות המקרה והמבחנים שנקבעו בפסיקה, כל המסמכים קבילים.

לטעמי הצדק בעניין זה הנו עם המאשימה. אני מפנה לפסיקה הרבה שהובאה בסיכומיה וכן לספרו של המלומד קדמי **על הראיות**, חלק ראשון, מהדורה משולבת ומעודכנת תשס"ד 2003 עמ' 507, שם סוכמו התנאים שדרושים לשם קבלת אימרה של נפטר שניתנה במהלך מילוי תפקידו: **הראשון**, האימרה נעשתה על ידי העובד במסגרת מילוי תפקידו. **השני**, האימרה מתייחסת לפעילות שכבר בוצעה להבדיל מפעילות עתידית. **השלישי**, לא קיים ספק באשר לאמיתות תוכנה. **הרביעי**, קרבת זמן הרישום למועד הפעילות- יש הרואים בו שיקול לעניין המשקל בלבד.

הבה נבחן את המסמכים שבעניינינו לאור הלכה זו: **בת/42** כותב החוקר נסר ז"ל שהוא ביקר במשרדי בזק בנילאומי וקיבל תדפיס שכלל פרטים ביחס לשם המשתמש של הנאשם ולטלפון ממנו בוצעו השיחות. כל התנאים שסקרתי לעיל מתקיימים בעניינינו באופן מובהק וברור. ועל כן, אני קובע שמסמך זה קביל לגבי תוכנו.

לעניין **ת/43 א-יג** המדובר במסמכים שהדפיס החוקר נסר ז"ל, לאחר שביצע חיפוש במחשב הנאשם, המסמכים מתארים את הקבצים שנמצאו במחשב הנאשם. גם כאן המבחנים מתקיימים, המדובר בעובדת, להבדיל ממסקנות, הדו"ח נכתב במהלך מילוי תפקידו, הפעילות כבר בוצעה,

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

אין ספק לגבי העובדת, ואם יש ספק הרי המחשב של הנאשם עדיין קיים ואפשר לבדוק עובדת אלו, כמו כן היתה סמיכות זמנים. מכאן, אני קובע שגם מסמכים אלו קבילים.

עבירת עריכת והפצת הוירוס

סעיף 6 לחוק המחשבים קובע:

> **"(א) העורך תוכנה באופן שהוא מסגלה לגרום נזק או שיבוש למחשב או לחומר מחשב בלתי מסויימים, כדי לגרום שלא כדין נזק או שיבוש למחשב או לחומר מחשב, מסויימים או בלתי מסויימים, דינו - מאסר שלוש שנים.**
>
> **(ב) המעביר לאחר או המחדיר למחשב של אחר תוכנה אשר סוגלה לגרום נזק או שיבוש כאמור בסעיף קטן (א), כדי לגרום שלא כדין נזק או שיבוש כאמור, דינו - מאסר חמש שנים."**

עריכת הוירוס

סעיף זה מבחין בין עורך הוירוס לבין מפיצו, לטעמי המאשימה לא הרימה את נטל ההוכחה בכל הקשור לעבירה של עריכת וירוס, שכן בכדי להרשיע בעבירה זו, יש להוכיח שהנאשם יצר ותכנת את הוירוס בעצמו, ולא העתיק אותו ממקום אחר.

הפירוש למילה עריכה בהקשר לסעיף 6 (א) הנו, יצירת הוריוס, אני למד זאת מהצעת חוק המחשבים בה נאמר: **"מוצע לאסור על שני סוגים של פעילות מזיקה ולקבוע אותם כעבירות: האחד,.....יצירתו של חומר מסוכן זה, במטרה לגרום בכך נזק לקבוצה...."**. (ההדגשות הוספו כ.ס).

ומכאן, אם הוירוס נוצר על ידי אדם מסוים והתוכנה כוללת תפריטים שניתנים להתאמה, והמשתמש משנה תפריטים אלו, אזי אין לראות בו כיוצר הוריוס. ועל כן, עצם הכנסת הסימסה והמצאות קבצי עריכה במחשב הנאשם אינם מלמדים על ביצוע העבירה של עריכת וירוס.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

בעניין זה אני אף מפנה לעדותו של המומחה מר שמעון שהעיד **(עמוד 87, לפרוטוקול הישיבה מיום 31/3/05)**:

> **"בזמנו כבר משנת 1998, אם אני זוכר נכון, היו קיימים מספר סוסים טורייינים כדוגמאת** SUB 7 **ונטבס. בעצם נוצרה תוכנה עם תפריטים נוחים מאוד עם כפתורים שבעצם כל אחד יכול בלי שום ידע מוקדם לתפעלו."**

לאור התוצאה שהגעתי אליה, לא ארחיב את הדיבור שכן השאלה איזו פעולות צריכות להתבצע בכדי לראות בפעולה כעריכת ווירוס, שאלה נכבדה היא וראוי שתינתן עליה את הדעת בבוא המקרה המתאים, שבו יונחו בפני ביהמ"ש גם ראיות ועובדות ולא רק טיעון משפטי ערטלאי.

<u>העברת והחדרת הווירוס</u>

בפנינו עבירה התנהגותית שלא קשורה בהתרחשות נזק. היסוד העובדתי של העבירה כולל שני יסודות: **הראשון**, הימצאות תוכנה מזיקה (הווירוס), **השני**, העברת או החדרת התוכנה. נוסף על כך, נדרש יסוד נפשי של כוונה לגרימת נזק.

<u>הימצאות התוכנה המזיקה</u>

לשם הקביעה האם מדובר בתוכנה שנועדה לגרום נזק, ביהמ"ש מסתייע בעדות מומחים, שבודקים את מאפייני התוכנה, הגדרה זו הנה רחבה וכבר בפסק הדין הראשון במדינת ישראל שדן בעבירת החדרת ווירוס, ת"פ 8243/97 (חיפה) **מדינת ישראל נ' גיל פז**, העיר כבוד השופט כהן:

> **"הגם שכותרת סעיף 6 לחוק המחשבים היא "נגיף מחשב", הרי שהסעיף נועד לחול על סוגים שונים של "תוכנות מרושעות" (**Malicious Softwares**), ובכללן כאלה המכונות "** Trojan Viruses" , "Logic Bombs","Worms", "horses" **ו-** "Stealth viruses""

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

כיום סביר להניח שרשימה זו התארכה עד מאוד.

לאחר שהוכח שמדובר בתוכנה מזיקה עפ"י מכלול הראיות שהובאו בפני, יש כמובן להוכיח את היסוד השני, דהיינו ההעברה או ההחדרה של הווירוס למחשב אחר, וכאן יש להבחין בין שני מצבים: **הראשון**, העברה שמתבצעת בצורה פיזית, כגון החדרת וירוס באמצעות דיסקט **והשני,** העברה דרך רשתות תקשורת ובראשן האינטרנט.

אין ספק שהסוג השני הוא המשמעותי והנפוץ ביותר, לפיכך הדיון בהמשך יתייחס לסוג העברה זה.

עולה השאלה, מה צריך להראות בכדי להוכיח שהיתה העברה דרך רשת האינטרנט?

הסיטואציה האופטימלית תכלול ראיות לגבי שלושת היסודות הבאים:

א. הימצאות הוירוס במחשב התוקף- הנאשם.

ב. הימצאות הוירוס במחשב הקורבן.

ג. ראיות דיגיטליות בעניין מסלול העברת הווירוס ברשת האינטרנט, שמוכיחות שהוירוס נשלח מכתובת "**I.P**" ששייכת לנאשם.

במצבים רבים, בדומה לענייננו, הראיות שקיימות אינן עונות על שלושת הדרישות הללו, כך למשל, ייתכן והוירוס לא ימצא במחשב הקורבן משום שהמחשב תוקן ותוכנו נמחק, ייתכן והקובץ לא יימצא במחשב הנאשם, היות והנאשם מחק אותו וניסה לטשטש עקבות ולהעלים ראיות, או אף ייתכן מצב בו הווירוס יימצא הן במחשב הקורבן והן במחשב הנאשם, אך לא נמצא את כתובת ה I.P של הנאשם בגלל אובדן מאגר הנתונים של הכתובות.

שאלות אלו אינן פשוטות כלל וכלל, שכן עסקנין בראיות מחשב, שמאפייניהן שונים מהראיות הרגילות הן מבחינת איתורן, והן מבחינתם דיוקן, ועל כן, בבואנו לדון בעבירות כגון אלו, עלינו לקחת בחשבון את מכלול הראיות הדיגיטליות, והראיות הנסיבתיות האחרות שמקשרות בין המעשה של ההפצה לבין הנאשם עצמו.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

מסקנתי היא שבכדי להרשיע אדם בעבירה של הפצת וירוס, חייבים להתקיים לפחות שניים מהיסודות של ההפצה או ההחדרה, וזאת בנוסף לראיות נסיבתיות אחרות וכן קיומו של הסבר סביר להיעדרות היסוד השלישי החסר.

דומני, שהמקרה הבעייתי ביותר הנו מקום בו מוצאים את אותו וירוס אצל הנאשם והקורבן, אך לא מצליחים להצביע על כתובת ה- "**I.P**", במקרה זה, נדרוש ראיות חזקות בצורה משמעותית, שכן מטבעם של וירוסים הן נשלחים בכמויות, ולפעמים הם מתוכנתים כך שהם יישלחו הלאה, במקרים כאלו עצם ההימצאות של הווירוס אינה יכולה לבסס הרשעה, אלא כאמור יש לדרוש ראיות חיצוניות, למשל אם שמעון מתקשר לראובן ומאיים עליו בשליחת וירוס ולאחר מספר ימים מתגלה אותו וירוס עם אותם מאפיינים בשני המחשבים ומוכח שבאותם זמנים שני המחשבים היו מחוברים לאינטרנט, אזי ייתכן וכן יהיה מקום להרשעה.

ראיות הצדדים

זה העת לבחון האם לאור המבחן שהצעתי לעיל, המאשימה הצליחה להוכיח מעל לכל ספק סביר שהנאשם החדיר ווירוסים במספר הזדמנויות ולמספר קורבנות.

המאשימה טוענת בסיכומיה שהיא הוכיחה מעל לכל ספק סביר את העבירה של הפצת הווריוס וזאת על סמך הראיות הבאות: הידיעה המודיעינית שהובילה לנאשם, הקבצים שנמצאו במחשבו, התאמת זמני גלישתו באינטרנט לזמן הפצת הוירוס, הימצאות ראיות מקשרות בין הוירוס לבין הנאשם ובראשם הסיסמה, ההיכרות בינו לבין חלק מהקורבנות, חוסר שיתוף הפעולה עם החוקרים והעדרם של הסברים סבירים מטעמו.

מנגד טוען הנאשם, שהמאשימה לא הצליחה להוכיח את העבירות שמיוחסות לו או לכל הפחות, נותר ספק סביר באשר לביצוע העבירות. ההגנה בחרה בסיכומיה להתייחס לאירועים הספציפיים ולסקור את הראיות ביחס אליהם.

קורבנות הנאשם

מכתב האישום עולה כי הנאשם פגע במחשביהם של שלושת קורבנות: מר כוכבי שמש, הגב' קרן אייזנברג ומישהי בשם דניאלה. להלן, אפרט את הראיות שהובאו ביחס לכל קורבן:

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

<u>החדירה למחשבו של מר כוכבי</u>

הטבלה הבאה מסכמת את תמצית טענותיה של ההגנה לגבי האירועים שקשורים בחדירה למחשבו של מר כוכבי שמש:

תאריך ושעת האירוע	**האירוע הראשון 23/12/00 22:54**	**האירוע השני 29/12/00 21:22**	**האירוע השלישי 29/12/00 23:11**
האם הקובץ נגוע בוירוס	אין הוכחה, מדובר בעדותו של כוכבי. **(עמ' 32 לסיכומיה)**	לא הוכח מקור הקובץ שהביא קצין המודיעין.	לא הוכח מקור הקובץ שהביא קצין המודיעין
כתובת ה- I.P ממנה נשלח הקובץ	ע"פ תדפיסי בזק בינלאומי יש קשר בין הקובץ ל – I.P.	אין כל מסמך של ספק שירות שמקשר בין הקובץ ל I.P. (עמ' 37 לסיכומיה)	אין כל מסמך של ספק שירות שמקשר בין הקובץ ל I.P. (מ' 31 לסיכומיה)
האם כתובת ה- I.P שייכת לנאשם	כן, ע"פ בדיקת בזק בינלאומי. **(ת/71 ג')**	לא הוכח שבאותה עת הנאשם היה מחובר לרשת. (30)	כן, ע"פ התדפיסים של בזק בינלאומי. **(ת/67 ב)**

<u>האירוע הראשון</u>

המאשימה טוענת שביום 23.12.00, שלח הנאשם שהשתמש בשם המשתמש "**משה_גרוס**", הודעה למר כוכבי, בפורום "**IOL**", ההודעה כללה קובץ שהכיל וירוס **(ראה ת/ 2א)**. בחקירתו במשטרה מסר מר כוכבי שני קבצים שהוריד מהפורום, "**אילו קבצים שהורדתי למחשב שלי מדובר ביום 23.12.00 והשני 29.12.00.**" **(פרוטוקול 14).**

להוכחת אישום זה המאשימה מבססת את דבריה על הראיות הבאות: **ראשית,** ההודעה והקובץ שמסר מר כוכבי לחוקרים, הובילו לכתבות "**I.P**" ששייכת לנאשם. **שנית,** השיחות בפורמים שהתקיימו בין מר כוכבי לשם המשתמש "**שרול**", מוכיחות ששרול, פרץ למחשבו של מר כוכבי

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

ושלף משם קבצים. **שלישית,** הנאשם השתמש במספר שמות משתמש והם: "**משה_גרוס**" ו-"**שרול**" ו"**שפלן**". ומכאן שהוא זה אשר פרסם את הפרטים לגבי מר כוכבי.

ההגנה מסכימה שההודעה אכן נשלחה מביתו של הנאשם (**ראה סיכומיה עמוד 32 פסקה 121**), אך לטענתה לא הוכח שההודעה כללה וירוס.

בעניין זה, צודק הנאשם, שכן בעוד שלגבי ההודעות של האירועים השני והשלישי יש מסמך של פקד פטרבורג שקובע שהקבצים מכילים ווירוס, הרי שלגבי האירוע השלישי אין מסמך כזה. **האם במצב דברים זה ולאור נסיבות המקרה דנן, יש לזכות את הנאשם מהאירוע הראשון?**

דומני שלא, היכן שישנן ראיות נסיבתיות חזקות מאוד שמראות בבירור שהנאשם כן שלח קובץ שמכיל וירוס, קובץ שאפשר לו בהמשך לשלוף קבצים ממחשבו האישי של מר כוכבי ולפרסמם בפורום. יצויין, שהפרטים שפורסמו עסקו בנושאים אישיים רבים של מר כוכבי, כגון: מכתב שנשלח לביטוח לאומי (**ת/3**); מכתב שהכין לידידה בנושא עסקי (**ת/ 6א'-ב'**), כתובתו המדויקת (**ת/9**) וקורות חייו, ליתר פירוט עיינו **בעמוד 13 לסיכומי המאשימה.**

מר כוכבי העיד, שהוא שמר את המסמכים במחשבו ולא פרסם אותם ברשת בכל צורה שהיא, וברור מעדותו שהוא לא שלח אותם לנאשם או "**לשרול**". כאמור, הווירוס הופץ ע"י "**משה גרוס**", בעוד מי שמסר את הפרטים שפורטו לעיל, פעל תחת הכינוי "**שרול**", לפיכך נשאלת השאלה, האם "**משה גרוס**", ו"**שרול**" הם אותו אחד, ואם כן, האם מדובר בנאשם?

בעניין זה המאשימה טוענת שאכן מדובר בנאשם וזאת על סמך עדותו של מר כוכבי, לפיה הוא שמר את הלינקים של "שרול", ששייכים למי שהפיץ את הווירוס. המסמכים שמתעדים את הלינקים הוגשו וסומנו **ת/17 א'- ג'**.

אך הראיה החותכת לגישתם, היא ההתאמה בין הנתונים של הכינוי "**שרול**" ו"**משה_גרוס**" לבין חשבון האינטרנט של הנאשם, שכזכור הנו **mirlan**. התאמה זו נסמכת על בדיקת כתובת ה-"**I.P**" של הלינקים ששמר מר כוכבי וכן על ידי זיהוי מקור שיחת הטלפון. (הנתונים ששימשו בסיס לבדיקות, סומנו **ת/45 ו ת/47, וכן, ת/37 ות/38א'-ד'**).

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

הנאשם טוען, שהמסקנה של המאשימה בטעות יסודה, לגישתו המאשימה לא בדקה את ההתאמה בין כל כתובות ה- "**I.P**" שחברת "**WALLA**" העבירה לידה **(ת/46)** לבין שם המשתמש של הנאשם, אלא הסתפקה בבדיקת 4 כתובות בלבד, כאשר 3 כתובות מתייחסות לתאריכים מחודש נובמבר **(ת/ 38 א'-ג')** וכתובת אחת לדצמבר **(ת/38ד').**

אין דעתי כדעת ההגנה, שכן די בבדיקה מדגמית שתראה התאמה ואין צורך לבדוק את כל כתובות ה- "**I.P**" במשך כל התקופה, שכן מטרת הבדיקה בעניין זה אינה הוכחת מקור משלוח כל הודעה והודעה, אלא המטרה הנה בדיקת ההתאמה בין זהות מפרסם ההודעה "**שרול**" ו- "**משה גרוס**" לבין שם המשתמש של הנאשם "**mirlan**", וכיוון שהמאשימה הוכיחה זאת לגבי מספר הודעות, אזי היא הרימה את הנטל והוכיחה מעל לכל ספק סביר את העובדות הנטענות שיש בהן כדי להרשיע את הנאשם כפי שיפורט להלן.

אוסיף עוד, שכתובות ה- "**I.P**" הנוספות היו ידועות לנאשם, ואם הוא היה חפץ בהוכחת מקורם, הרי שהוא יכל לעשות כן.

על יסוד כל אלה, אני קובע שהנאשם הוא זה ששלח את ההודעות שפורטו לעיל למר כוכבי.

<u>האירועים השני והשליש</u>

<u>מקור הקבצים שבהודעה המודיעינית</u>

ההגנה טוענת שמקור הקבצים שבהודעה אינו ידוע ומכאן אין להם כוח ראייתי, עוד היא מציינת שאין אף דו"ח פעולה שמתאר את הורדת הקבצים מהרשת על ידי המשטרה.

צודק בא כוח הנאשם, לעניין תפקוד קצין המודיעין, לא כן, לגבי התוצאה המתבקשת, אמת, היה על קצין המודיעין, לכתוב דו"ח בעת קבלת הידיעה המודיעינית ובמיוחד דו"ח לגבי פעולת הורדת הקבצים מהאינטרנט, היה עליו לתאר, בין היתר מתי הורדו הקבצים, מאיזו אתר ובאילו אמצעים הוא נעזר בהורדתם מהרשת.

אך פגם חקירתי זה, אין בו בכדי לפגוע במשקל שיש לתת להודעה המודיענית, שכן קצין המודיעין בכל זאת כתב ידיעה **(עיין בס' 7)** כמו כן, הוא העיד בביהמ"ש, ועדותו נמצאה אמינה עלי, בעדותו

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

טען שמקור הידיעה הנו גב' בשם נורית, מנהלת הפורמים של "IOL". הגב' נורית מסרה בהודעתה במשטרה **(ראה ס' 9)**, כי היא לא זכרה אם היא העבירה את הידיעה לקצין המודיעין, אם כי היא אמרה שהיא העבירה לו בעבר מספר ידיעות עם מספרי "I.P". בעדותו בביהמ"ש מסר קצין המודיעין (עמוד 60 לפרוטוקול מיום 14/10/2004), פרטים לגבי דרך הטיפול בידיעה המודיענית, לטענתו: "**בדרך כלל אני נכנס לאינטרנט לאותו פורום מאתר את ההודעה שעליה מדובר מוריד את הקובץ המצורף אליי ובזה נגמר הסיפור. ומדפיס את ההודעה**". כמו כן, יש לציין שפקד נסר ז"ל בדק את הידיעה המודיענית, והוריד את אחד הקבצים מהאינטרנט **(ראה, ת/41 א')**.

לאור דברים אלו, נראה לי כי הוכח מקור הקבצים שהועברו לפקד פטרבורג, קבצים אלו נבדקו על ידו **ובת/52** הוא כותב: "**בדקתי את אחד הקבצים (שניהם זהים) באמצעות תוכנת אנטי וירוס ואכן נמצא ששני הקבצים נגועים ב-** "SUB SEVEN". ועל כן, יש לבדוק האם הקבצים הנגועים בוירוס הופצו באמצעות מחשב הנאשם. לשם כך, עלינו לבדוק האם כתובת ה- "I.P" שבידיעה המודיעינית מביאה אותנו למחשב הנאשם?

חברת בזק בינלאומי שהיא ספקית שירות האינטרנט, מסרה למשטרה את כתובות ה- "I.P" שהשתמש בהם הנאשם בתאריכים הרלבאנטיים לאישום. מסמכים אלו סומנו **ת/71 א' - כ'**, **ת/67 א' - ג'. מת/67 ב'** עולה שכתובת ה-"I.P" של האירוע השלישי אכן מקורה בבית הנאשם, ועל כן, אני קובע שהנאשם הפיץ את הוירוס בנוגע לאירוע השלישי, היכן שהוכח שהקובץ שמכיל וירוס, נשלח מכתובת ה-"I.P" ששייכת לנאשם.

לגבי האירוע השני, כתובת ה- "I.P" 212.179.134.104 שצוינה בדו"ח המודיעני לא מופיעה באף מסמך מהמסמכים הרבים שהוגשו על ידי בזק בינלאומי, ומכאן טוענת ההגנה שאין להרשיע את הנאשם באירוע זה.

דין טענתו זו להידחות, אנמק ואסביר: ייתכנו מקרים בהם תהיה הרשעה בהפצת וירוס על אף היעדר כתובת "I.P" שמובילה לנאשם. מקרים אלו יתקיימו כאשר ישנן ראיות חד משמעיות שמקשרות בין הנאשם לקורבן למשל, מציאת קבצים זהים שמכילים את הווירוס הן במחשב הנאשם והן במחשב הקורבן, כמו כן, מציאת ראיות חיצוניות נוספות שמקשרות בין הקורבן לנאשם כגון: היכרות מוקדמת, איום בשליחת ווירוס או ראיות אחרות שמקשרות בין הנאשם לקורבן.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

יצוין, שבמקרים כגון אלו, עלינו לנהוג במשנה זהירות, שכן כאמור, מטיבם של וירוסים הם מופצים למספר רב של מחשבים והסבירות שימצאו וירוסים זהים במחשבים שונים הנה גבוהה ומכאן החשיבות של ראיות נוספות שהן ספציפיות למועד האירוע.

במקרה דנן, וכמפורט לעיל, התקיימו ראיות נוספות, כגון היכרות של מר כוכבי עם הנאשם, פרסום פרטים אישיים של מר כוכבי בפורום ע"י שם המשתמש "**שרול**" שהוא בצעם הנאשם. אך לדעתי אין בכך די, הראיות שהביאו אותי להרשיע את הנאשם גם באירוע זה הנן, גילוי הסיסמה של הווירוס, וכן הממצאים שעלו בבדיקות שבוצעו במחשב הנאשם: ה**בדיקה הראשונה,** מיום **1.10.01** שבוצעה על ידי פקד פטרבורג, ראש צוות החקירה. **הבדיקה השנייה,** מיום **8.10.01** שבוצעה על ידי החוקר ניר אלקבץ (**ת/28**). **הבדיקה השלישית,** מיום **17.10.01**, שבוצעה על ידי החוקרים רפ"ק יואל שפנר ביחד עם ראש צוות החקירה אייל פטרבורג. ממצאים אלו מוכיחים מעל לכל ספק סביר, שהנאשם הוא זה שהפיץ את הווירוס, לאור חשיבות ממצאים אלו אביא אותם להלן:

קבצים שקשורים לוירוס שהופץ, קרי "**SUB7**", וספריה שנושאת את השם הזה. מבדיקת קבצים אלו, עלו הממצאים הבאים: חלק מהקבצים היו מוגנים בסיסמה, כמו כן, גודל הקובץ שהכיל את הווירוס שהופץ היה זהה לקובץ שנמצא במחשב הנאשם.

חשיפת הסיסמה: "במוט 786" ובאנגלית "**cnuy786**", המאשימה הוכיחה, שהנאשם השתמש בסיסמה זו למטרות שונות ובמספר תוכניות, כגון:

א. סיסמת הווירוס המקורי שהופץ באינטרנט.

ב. סיסמת הסוס הטוריאני שנמצא במחשב הנאשם.

ג. סיסמת הביוס של מחשב הנאשם, הכוונה היא למערכת ההפעלה הראשונית של המחשב, שלשם כניסה אליה, אפשר להשתמש בסיסמה, אם כי הדבר אינו הכרחי, ובירית המחדל לדברי העד ניר אלקבץ הנה ללא סיסמה. **(ראה עדותו בעמוד 39).**

ד. סיסמת שומר המסך במחשב הנאשם.

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

ה. הסיסמה ששייכת למספר המשתמש של הנאשם בתוכנת ה- "ICQ". יצוין שמספר המשתמש נמסר על ידי הנאשם בעצמו בחקירתו מיום 16.10.01 בעמוד 3. ניסוי הכניסה לתוכנת ה- " ICQ" תוך שימוש בסיסמה, נערך בתחנת המשטרה **(ראה ת/31, וכן עדותו של אלקבץ בעמוד 40).**

ו. סיסמת הסירבר, שהנו מרכיב הוירוס שמותקן במחשב הקורבן.

ז. מציאת מספר ה- "ICQ" ששייך למר כוכבי **(83078987),** במחשב הנאשם, המספר נמסר טלפונית לחוקר יואל שפנר על ידי מר כוכבי **(ראה ת/21)**.

ח. הממצאים שעלו בבדיקה הראשונית שביצע החוקר נסר ז"ל, שכללו, קבצים שהכילו וירוסים **(ת/43 ה' ות/43 ב').**

בבדיקה מיום 17.10.01, עלו שני ממצאים: **הראשון,** הימצאות תוכנה שמטרתה לנקות את המחשב מסוסים טוריאנים. **השני,** מציאת הקבצים שהופצו באינטרנט, לאחר מחיקתם בעזרת התוכנה. **בת/20 ב'** בעמוד 4 מפורטים הקבצים המחוקים ששימשו את הנאשם בהפצת הווירוס.

<u>המסקנה וסיכום ביניים</u>

ממצאים אלו ובמיוחד חשיפת הסיסמה והשימושים שנעשו בה, מוכיחים בוודאות שהנאשם הוא זה שהפיץ את הוירוס והחדירו למחשבו של מר כוכבי, ובכך עבר עבירה של החדרת וירוס בניגוד **לסעיף 6 (ב) לחוק המחשבים**. יחד עם זאת, וכמבואר לעיל, לא מצאתי לנכון להרשיע את הנאשם בעריכת וירוס.

כאמור, שליחת הוירוס שהיה מסוג סוס טוריאני, אפשרה לנאשם לשלוף מסמכים ממחשבו האישי של מר כוכבי ובהמשך לפרסם פרטים מהם בפורום, ועל כן אני מוצא אותו אשם גם בעבירות הבאות שיוחסו לו בכתב האישום, וזאת בהתאם למפורט להלן:

<u>שיבוש או הפרעה למחשב או לחומר מחשב, סעיף 2 לחוק המחשבים קובע:</u>

"העושה שלא כדין אחת מאלה, דינו - מאסר שלוש שנים:

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

(1) משבש את פעולתו התקינה של מחשב או מפריע לשימוש בו; ...".

הוכח שהנאשם גרם לפגיעה במחשבו של מר כוכבי. מר כוכבי מסר בחקירתו במשטרה **(ס/13 עמוד 2 שורה 42)**: "**... אני בעקבות כך שהוא חדר למחשב לא יכולתי לעשות כיבוי מסודר דרך מפעלת (צ.ל. מערכת – כ.ס.) ההפעלה. ולכן בסופו של דבר אני נאלצתי לבצע איתחול (פירמוט) מחדש לכל הכונן הקשיח שלי**". כמו כן, הנאשם ששמר את סיסמת ה- "**ICQ**" של מר כוכבי במחשבו, גרם לבעיות בתוכנה דבר שהביא את מר כוכבי לשנות את הסיסמה שלו.

<u>פגיעה בפרטיות</u>

סעיף 5 לחוק הגנת הפרטיות, קובע:

"הפוגע במזיד בפרטיות זולתו, באחת הדרכים האמורות בסעיף 2(1), (2), (3) עד (7) ו-(9) עד (11) ..."

הפגיעה בפרטיות בענייננו הנה ברורה ובאה לידי ביטוי במספר אופנים: **הראשון,** העתקת המכתבים והמסמכים האישיים שהיו במחשבו של מר כוכובי בניגוד לסעיף 2(5) שקובע: "**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**".

השני, פרסום התכנים של המכתבים, בפורום "**IOL**", ובכך אנשים נוספים נחשפו לתכנים. בהתנהגותו זו, פגע הנאשם בפרטיתו של מר כוכבי כהגדרתה בסעיף 2(10) שקובע:

"פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או (9)".

(בענייננו הפרסום מתייחס לסעיף 2(5)).

אין ספק, שהנאשם היה מודע למעשיו, ועשה זאת בכוונה, שעה ששלף את המסמכים ופרסם תכנים שעלו בהם, ומכאן שגם היסוד הנפשי מתקיים.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

<u>חדירה לחומר מחשב כדי לעבור עבירה אחרת</u>

סעיף 4 לחוק המחשבים דן בעבירה של חדירה לחומר מחשב. הסעיף קובע:

> **"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 ...".**

כפי שקבעתי לעיל, הוכח שהנאשם חדר למחשבו של כוכבי שלא כדין באמצעות השתלת הוירוס, אך הנאשם לא הסתפק בחדירה למחשב, אלא פגע בפרטיתו של מר כוכבי בצורה הקשה ביותר, בניגוד לסעיף 5 לחוק הפרטיות ובכך הוכח שלחדירה נלוותה עבירה נוספות שהנאשם ביצע אותה, ולכן אני מרשיע את הנאשם בעבירה על סעיף 5 לחוק המחשבים שקובע:

> **"העושה מעשה האסור לפי סעיף 4 כדי לעבור עבירה על פי כל דין, למעט על פי חוק זה, דינו - מאסר חמש שנים."**

יסודות אלה מתקיימים בענייננו.

<u>החדירה למחשב של גב' קרן איינזברג</u>

גב' קרן איינזברג **(להלן: "העדה" ו/או "קרן")** נחקרה במשטרה ביום 28.10.01 וכן, העידה בביהמ"ש ביום 5.1.04, מעדותה עולים הדברים הבאים:

היא גלשה בפורום "**IOL** " וכן, השתמשה בתוכנת ה- "**ICQ**" בזמנים הרלבאנטיים לכתב האישום, היא אישרה שהיא דיברה בפורום עם מי שכינה את עצמו "**שפלן**" ו- "**איילון**", ואף שאלה אותו אם הוא מיכאל לרמן, אך הוא הכחיש זאת. במהלך הכרות זו הוחלפו מספר קבצים בינה לבין "**שפלן**", להלן אסקור חלק מקבצים אלו, שלגבי חלקם היא טוענת שהם המקור לסוס הטוריאני שגרם לפגיעה קשה במחשבה:

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

תמונות שנשלחו על ידי "שפלן", ונטען שהם תמונותיו שלו **(ראה ת/23)**. תמונות אלו הן של הנאשם, והן הובילו את העדה לחשוב ששם השולח הנו מיכאל לרמן, שכן לתמונה היה לינק שקשור לאתר אינטרנט של הנאשם. תמונות אלו נמצאו במחשבו האישי של הנאשם ע"י החוקר ניר אלקבץ ביום27/11/01, **(ראה ת/32 שכולל את 3 התמונות).**

קבצים של בדיחות ולנקים.

לטענת המאשימה, בהמשך ולאחר התקנת הסוס הטוריאני, שלף הנאשם באמצעתו, מסמכים אישיים של העדה שלפי עדותה לא מסרה אותם לנאשם, להלן רשימה חלקית למסמכים אלו שנמצאו במחשבו האישי של הנאשם: קורות החיים של העדה **(ת/24)**; צילום מסך למחשב שלה; התכתבויות העדה עם חברת "**ערם**" ומסמכים נוספים (ראו **עמוד 32 לפרוטקול**, שם הסתכלה העדה בקבצים אלו באמצעות מחשב נייד, הדיסקט הוגש וסומן **ת/26)**.

העדה ציינה, שהקבצים היו שמורים במחשבה, ושהיא לא שלחה לנאשם כל קובץ מלבד תמונתה (ראה, עמ' 35).

בחקירתה במשטרה היא זיהתה חלק מהקבצים שנמצאו במחשב הנאשם, אשר קשורים אליה, ואף מסרה שהיא חושדת בנאשם:

> **"שאלה: האם את יודעת על איזה חשוד אנחנו מדברים ואם כן כיצד?**
>
> **תשובה: אני ההיתי (צ"ל הייתי – כ.ס.) בטוחה ב 90 אחוזים שמדובר במיכאל לרמן, חוקר פרטי במקצועו, מחיפה, שעושה חקירות על ביטוחים...".**

זה הזמן לציין, שהעדה השתמשה גם במחשב בעלה שהיה ממוקם בקומה השנייה בביתה, מחשב זה נבדק על ידי המשטרה ובו לא נמצא וירוס **(ראה, ס/2)**.

לאור הנתונים הללו, טוענת המאשימה שהוכח שהנאשם הוא האחראי על הפצת הווירוס ועל שליפת המסמכים ממחשבה האישי של העדה.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

ההגנה בסיכומיה **(עמ' 39-40)** חולקת על מסקנה זו, לטענתה לא הוכח שהנאשם החדיר למחשב של גב קרן כל וירוס, וזאת על בסיס מספר נימוקים: **הראשון,** העדר ראיה ביחס להעברת קובץ שמכיל נגיף. **השני,** העובדה שבמחשב בעלה **לא** התגלו וירוסים. **השלישי,** סתירות שהתגלו בעדותה של גב' קרן בעניין חשיפת זהותה ברשת. **הרביעי,** הודאתה שהיא שלחה את התמונה לנאשם, משליכה על האפשרות שהקבצים הנוספים שנמצאו במחשב הנאשם, נשלחו, גם כן, מרצונה החופשי.

לטעמי; אפילו אין בטענות אלו, כדי לעורר ספק בלבי והן נדחות על ידי.

<u>דיון והכרעה</u>

גם על מקרה זה נחיל את המבחנים שהצעתי לעיל, ונבדוק האם המאשימה הביאה ראיות שמוכיחות מעל לכל ספק סביר, שהנאשם החדיר וירוס למחשבה של גב' קרן וביצע עבירות נוספות.

בניגוד למקרה הראשון של מר כוכבי, המאשימה לא הציגה, קובץ או הודעה שבאמצעותם החדיר הנאשם את הווירוס למחשבה של גב' קרן, האם בנסיבות אלו נוכל להרשיע את הנאשם בעבירה של החדרת וירוס? על שאלה זו השבתי באופן חיובי, וקבעתי שייתכנו מקרים בהם על אף שלא נמצא הקובץ שמכיל את הוירוס, ביהמ"ש כן ירשיע בעבירה זו, במקרים אלו יש לנהוג בזהירות, ורק כאשר מובאות ראיות שלא משאירות כל ספק באשר להחדרת הווירוס, ירשיע ביהמ"ש. לאור דברים אלו, אני דוחה את הטיעון **הראשון** של ההגנה. לדעתי, המקרה שבפנינו נופל בגדר מקרים חריגים אלו, שכן הראיות שאמנה להלן מוכיחות שהנאשם אכן החדיר את הוירוס:

<u>הימצאות מסמכים ששייכים לעדה במחשב הנאשם</u>

הימצאות מסמכים אישיים של העדה במחשבו האישי של הנאשם כמפורט לעיל, בלי שיינתן כל הסבר מניח את הדעת מצד הנאשם לעניין פשר המצאות קבצים אלו במחשבו והנסיבות שבהן הוא קיבל אותם, מעלה יותר מחשד כבד ומבוסס שהמסמכים הושגו בדרך לא כשרה, במיוחד לאור דבריה של העדה, לפיהם היא לא העבירה שום קובץ לנאשם, מלבד התמונה שלה **(ת/25)**, שכן אין כל סיבה להעברה זו, הרי למה שהיא תשלח לו קורות חייה או מכתבים אחרים שאין להם כל קשר לעיסוקו או לשיחה שהתנהלה בינם.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

גרסתה הגיונית וסבירה ביותר ובעניין זה העדה השאירה עליי רושם טוב, שכן מלבד העובדה שהסברה הגיוני, העדה ידעה להבחין בין הקבצים השונים ומסרה בגילוי לב ומבלי להסתיר בעדותה בביהמ"ש, שהיא שלחה את תמונתה לנאשם. העדה העידה בחקריתה הראשית בעמ' 33: "**התמונה שאתה מציג בפניי אני חושבת שזו תמונה שאני שלחתי לנאשם יחד עם התמונות של הילדים שלי.**" וגם בחקירתה הנגדית ציינה העדה **בעמוד 35**:

"ש. האם את בטוחה שמיכאל לרמן שלח לך את התמונות בהתנדבות.
ת. את הראשונה כן. אני אמרתי לו שאם ישלח לי תמונה ללא הדבר השחור בפנים שלך, אני אשלח לך גם. הוא שלח ואז שלחתי לו בחזרה. זה היה משא ומתן מצחיק כזה. אני לא הרגשתי מאוימת.
ש. היה מצב שהוא שלח לך תמונה עם פנים גלויות.
ת. אני מאמינה ששלחתי לו תמונה ת/25." (ההדגשות הוספו, כ.ס)

לסיכום, העדה ידעה להבחין בין הקבצים השונים ונתנה הסבר הגיוני, הסבר שמקבל משנה תוקף לאור אי מתן כל הסבר מצד הנאשם להימצאות המסמכים במחשבו. לאור דברים אלו, אני דוחה את טענותיה הנ"ל של ההגנה בעניין הסתירה בין דבריה בביהמ"ש להודעתה במשטרה, שהתרכזה בעניין זהותה ולא בעניין העברת תמונות ספציפיות, גם אם מדובר בסתירה, עדיין מדובר בעניין שולי שאינו פוגע במהימנות העדה.

<u>הפגיעה והתקלות שנגרמו למחשב העדה</u>

גב' קרן העידה שהיא ביצעה בדיקה של המחשב והתברר לה, שהוא נגוע בסוס טוריאני מסוג "SUB7" וכך אמרה: "**עשיתי סריקה באמצעות תוכנה שלא זוכרת את שמה - עלה שם שיש לי סוס טרויאני בשם SAB7.**" **(עמוד 34)**. חששה זה עלה בעקבות, "**קובץ שפוצץ לי את המחשב כל פעם. המסך נהיה שחור ובלגן.....מאותו רגע אני חושבת המחשבים הפכו להיות נגועים, זוהי התוכנה שהכניסה לי את הוירוס למחשב.**" **(עמוד 31)**. ולכן וכמפרוט לעיל, העדה העלתה את חשדה בנאשם ומסרה את השם למשטרה כבר בחקירה הראשונה, תוך שהיא מוסרת פרטים לגביו **(ראו: ס/3)**. עוד הוסיפה העדה **בעמוד 33** בעניין הנזק שנגרם למחשבה: "...**לא אני לא יכולה להעריך, ימים שלמים עשיתי פירמוטים. הבאתי טכנאי שיסביר לי. מדובר בהמון עבודה....**".

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

עדויות אלו מוכיחות שהנאשם שלף את המסמכים בעזרת וירוס ולא בכל דרך אחרת.

הדמיון בין החדירה למחשב כוכבי לחדירה למחשב העדה

מלבד הראיות שקושורת את הנאשם לחדירה לחומר המחשב של גב' קרן, הרי שיש לתת את הדעת גם על הדמיון בין השיטה שבה נהג הנאשם בעניין כוכבי, שיטה שכוללת היכרות בפורום עם הקורבן, ולאחר מכן שליחת קובץ שכולל "סוס טוריאני" ואז שליפת מסמכים אישיים ממחשבו. איני מוצא מקום להרחיב את הדיבור בעניין זה, שכן גם בהעדר דמיון בין שני המקרים, הייתי מרשיע את הנאשם בעבירה של החדרת וירוס וכן בעבירה של חדירה לחומר מחשב, שכן הראיות שהוצגו, לא משאירות כל ספק באשר לזהות מחדיר הווירוס.

בטרם סיום הדיון בפרק זה, אני דוחה את **טענתה השניה** של ההגנה, בעניין אי מציאת וירוסים במחשב בעלה, שכן נימוק זה אינו בעל משקל לעניין עצם החדירה למחשב, אלא הוא רבלאנטי לעניין אינטנסיביות החדירה. שכן, גב' קרן לא טענה שהוירוס פגע רק במחשב בעלה, וכך היא העידה במשטרה **(ס/3)**: **"אני ידעתי שהכניסו לי סוס טוריאני למחשב..... ולא ידעתי שגם למחשב של העבודה של בעלי הכניסו סוס טוריאני".**

האישומים בעבירות הנוספות

לסיכום, אני מרשיע את הנאשם בעבירה של החדרת וירוס למחשב, עבירה בניגוד לסעיף 6 (ב) לחוק המחשבים, וכן בעבירה של הפרעה ושיבוש למחשב בניגוד לסעיף 2 לחוק המחשבים, בעניין זה עדותה של גב' קרן על הנזקים והתקלות שהוירוס גרם למחשבה מהוות ראיה ניצחת להפרעה למחשב. כמו כן, אני מרשיע את הנאשם בחדירה לחומר מחשב לשם ביצוע עבירה, בניגוד לסעיף 5 לחוק המחשבים, כאשר העבירה הנה פגיעה בפרטיות. בענייננו הפגיעה בפרטיות התבטאה אך ורק בשליפת המכתבים האישיים ממחשבה, ועל כן, הפגיעה בפרטיות הנה לפי סעיף 2 (5).

החדירה למחשב של גב' "דניאלה"

המאשימה סומכת את ידיה באישום זה על **ת/29,** שכולל שיחה ארוכה בין **"Daniella"** לבין **"איש"** בעזרת תוכנת ה- "ICQ", במהלך אותה שיחה **(עמ' 10)** כתבה דניאלה ל- **"איש"**: **"שלחת לי וירוס, הקובץ נגוע SOMETHING .....POLY, עשיתי delete פעם ראשונה שזה**

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

קורה לי". ובהמשך באותו עמוד היא מסבירה מה גרם הוירוס למחשב שלה בעת שניסתה לפתוח את הקובץ. המאשימה מציינת את דבריו של "**איש**" בעמוד **18 לת/29** אמר ה- "**איש**": "**וירוס!!! בזה אני מומחה**".

ההגנה טוענת שאין כל יסוד לאישום זה, והיא מעלה מספר טענות: **הראשונה,** המאשימה בעצמה חזרה בה מאישום זה היכן ש**בעמוד 43** לסיכומיה נאמר: "**הסוס הטרויאני כלל לא הופץ באמצעות תוכנת ה-** "ICQ" **אלא באמצעות פורומים באתר** "IOL"". **השנייה,** הרשות החוקרת לא דאגה לברר מי זאת דניאלה, על אף שהיו בפניה די והותר ראיות לבדיקה זו. **השלישית,** "**ת/29 הנו שיחה סתמית או שמא פלרטטנית...**" כמו כן, דניאלה לא האשימה את הנאשם, ואמרה שמשלוח הקובץ היה בלי כוונה.

<u>דיון והכרעה</u>

דין הטענה הראשונה של ההגנה להידחות. אמת, מהדברים שנאמרו, מתקבל הרושם שהמאשימה חזרה בה מהאישום של החדרת הוירוס דרך תוכנת ה- "**ICQ**", אך הסתכלות כוללת על הסיכומים של המאשימה, מראה שהמאשימה לא זנחה טענה זו כלל וכלל, וכנראה הדברים נאמרו בהיסח דעת. מלבד זאת, השימוש בתוכנת ה- "ICQ" לא מוטל בספק, היכן שהדברים הוכחו במשפט והשיחה שהתנהלה בין ה- "**איש**" לדניאלה לא הוכחשה ומכאן שהשאלה הנה, האם על סמך דברים אלו אפשר להרשיע את הנאשם בהחדרת וירוס. לפיכך שתי שאלות מונחות בפנינו: **האחת,** האם "**איש**" הוא הנאשם? דומה שהתשובה חיובית, היכן שגם ההגנה לא חולקת על עובדה זו ובעמוד 38 לסיכומיה, היא אף משתמשת במילה נאשם ולא במילה "**איש**". **השנייה,** האם די בתמלילי השיחות שהוצגו לעיל, בכדי להרשיע בעבירה של החדרת וירוס?

לדעתי התשובה שלילית, ועל כן, יש לזכות את הנאשם מהחדרת וירוס למחשבה של דניאלה. כבר קבעתי לעיל, שבכדי להרשיע את הנאשם בעבירה של החדרת וירוס חייבים להתקיים לפחות שניים מתוך שלושת המרכיבים הבאים: **האחד,** הימצאות הוירוס במחשב הנאשם, **השני** הימצאות הוירוס במחשב הקורבן **והשלישי,** ראיות דיגיטאליות בעניין מסלול העברת הוירוס שקושרות את הנאשם. בענייננו, כל מה שיש הנה שיחה שעולה בה הנושא של החדרת הוירוס, אין בפנינו עדות לקובץ ספציפי שהכיל את הוירוס. בעניין זה לא נוכל לסמוך על דבריה של דניאלה, מהסיבה הפשוטה שאנחנו לא יודעים מי האישיות שעומדת מאחוריה, בעניין זה צודקת ההגנה, בטענתה שהיה על הרשות החוקרת לברר את זהותה של דניאלה, מחדל חקירתי זה יש בו בכדי להביא לזיכוי הנאשם, שכן עלינו לנהוג במשנה זהירות במקרים כאלו וזאת לאור המאפיינים של השיחות בפורום, במה דברים אמורים, הגולשים ברשת חושבים שהם נהנים מפרטיות גבוהה

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

וזהות חסויה ועל כן, הם מרשים לעצמם לעיתים רבות להעביר לבן שיחם, דברים לא מדויקים ואף דברים שקריים, ועל כן רק, אם המאשימה היתה עושה את המאמץ ומאתרת את גב' דניאלה ומביאה אותה לעדות בנוגע לדברים שאמרה, ייתכן ואז היה מקום להרשעה, אך לא כך היה בענייננו.

לאור האמור לעיל, אני מזכה את הנאשם מכל האישומים הקשורים לדניאלה, מאחר והמאשימה לא הרימה את נטל ההוכחה כדרוש במשפט פלילי.

<u>טענת ההשתלטות ע"י אחר</u>

הטענה המרכזית של ההגנה הנה שמישהו אחר השתלט על מחשב הנאשם ומשם, ביצע את העבירות כלפי הקורבנות. לאור כל הדברים שנאמרו לעיל ביחס לחדירה למחשבי הקורבנות האחרים, הדיון בטענה זו מתיתר וזאת לאור הראיות הרבות שקשרו לא רק בין מחשב הנאשם לביצוע העבירות אלא גם את הנאשם עצמו, כוונתי היא לסוגיית הסיסמה וגם להיכרות בין הנאשם לקורבנות, מר כוכבי וגב' קרן. אף על פי כן, ומאחר וההגנה והתביעה השקיעו מלל רב בטענה זו, החלטתי להרחיב מעט את הדיון.

<u>האפשרות הטכנולוגית</u>

המאשימה וההגנה מסכימות שבטכנולוגיה הקיימת כיום, אופציית ההשתלטות מרחוק ע"י אחר אכן קיימת. ראה, סיכומי המאשימה בעמוד 23 שם נאמר: "**לרגע התביעה לא חלקה על אפשרות ערטילאית זו...**" ואף בעמוד 37 לסיכומיה אמרה: "**....המאשימה מעולם לא שללה את הטענה לפיה בהחלט קיימת אופציה לחדור למחשב של אחר ובאמצעותו להעביר וירוסים..**". גם פקד פטרבורג אישר "**...מצב לא פשוט, מסובך וצריך להיות מאוד מאוד מקצועי. אך בהחלט ניתן.**"**(עמוד 78).**

בנוסף לכך, גם מר שמעון גרופר, סמנכ"ל טכנולוגיות אבטחת מידע בחב' אלדין **(להלן, מר שמעון)** אחד העדים המומחים מטעם ההגנה, סקר את אפשרויות ההשתלטות מרחוק בזמן הרלבנטי לכתב האישום, תוך התייחסות ספציפית לתוכנת Windows 95, ולסוגי הווירוסים שמאפשרים שליטה מרחוק.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

יחד עם זאת, המאשימה טוענת שבעינינו לא הובאו כל ראיות שמוכיחות זאת, עוד הוסיפה שלטעמה, הגנה זו הנה ההגנה היחידה האפשרית בעבירות מחשב מהסוג דנן. **(ראה, עמוד 23 לסיכומיה).**

מנגד ההגנה מתרעמת על כך, שכיוון חקירה זה לא זכה להתייחסות ראויה מצד החוקרים ובכך הגנת הנאשם נפגעה קשות. אך לטענתה גם הנתונים הקיימים מצביעים על כך שמישהו אחר השתלט על מחשב הנאשם.

לאור דברים אלו, עלינו להשיב על שתי שאלות: **האחת,** האם הראיות שהובאו מעוררות ספק סביר, שאדם אחר השתלט על מחשב הנאשם וביצע את העבירות? **השנייה,** האם המשטרה בדקה באופן ראוי את טענת ההשתלטות על ידי אחר? ואם התשובה שלילית, מה נפקות מחדל זה?

לדעת המאשימה הראיות שהבואו לעיל בנוסף לראיות שאמנה להלן, לא משאירות ספק סביר בעניין זהות מבצע העבירות:

<u>המיומנות הדרושה לשם השתלטות מרחוק</u>

מר שמעון העיד שאפשרות השימוש במחשב כפלטפורמה, דורשת ידע ומקצוענות: "**אני מכיר הרבה מקרים, שבהם אנשים מקצועניים, בדרך כלל צריך להיות מישהו יותר מקצועי ושמבין את המשמעות של התקפה דרך מחשב מותקף כדי להסוות את העקבות.**" (עמוד 88 לישיבה מיום 31/3/05).

דברים אלו עומדים בניגוד לטענת ההגנה בסיכומיה בעמוד 14 "**שלמחשבו של הנאשם ניתן היה לחדור באופן יחסית קל**".

<u>התאמת זמני השיחות היוצאות מבית הנאשם לבין זמן ביצוע העבירות</u>

מפלט שיחות הטלפון, שהוכן על ידי **העד גיא סוסל** קב"ט חברת בזק וסומן **ת/1 ב'**, עולה כי יש התאמה מלאה בין זמני השיחות היוצאות מבית הנאשם לבין זמני הפצת ההודעות הנגועות בווירוס. מעדותו עולה כי, נתונים אלו נאספים באופן אוטומטי על ידי מחשבים אזוריים ומהם מועברים למחשב מרכזי, ולא קיימת אפשרות מעשית להתחברות או פריצה למחשבים אלו, שכן

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

מדובר במחשב שלא מחובר לרשת. העד הוסיף, שבכדי שרישום שיחה יוצאת ירשם במחשב, יש חובה שאותה שיחה תעבור באותו קו, ואין אפשרות של התחברות מרחוק, הדרך היחידה "לעלות על הקו", היא התחברות לארון הסף של הנאשם, **דבר שלא הוכח בענייננו**.

לטענת ההגנה, לנתונים אלו אין כל משמעות לאור טענתה שמישהו אחר השתלט על מחשב הנאשם, שכן האחר השתמש בשם המשתמש ובקו הטלפון של הנאשם בכדי לבצע את העבירות, ועל כן, אין בנתונים אלו בכדי להוכיח שהנאשם הוא זה שביצע את העבירות. כמו כן, ההגנה חולקת על מסקנת המאשימה, לפיה אם טענת ההשתלטות של ההגנה היא נכונה, כי אז, חברת בזק היתה מגלה זאת, והיא אף מביאה מדבריו של קב"ט בזק:

"ש: אם א' משתמש בביתו עם שם המשתמש והסיסמה שלו וב' חודר אליו דרך האינטרנט ומבצע פעולות דרך המחשב שלו, האם בזק באיזשהי צורה יכולה לדעת זאת? האם זה אך ורק לענייני אינטרנט.

ת: קשור לצורכי אינטרנט בלבד." (עמוד 55 לישיבה מיום 14/10/05)

ראו גם עדותו של עד ההגנה מר שמעון גרופר:

"ש: אם אני התקשרתי מהבית שלי לבזק והמתמחה חודר אליי למחשב דרך סוס טוריאני שהוא עשה, כל הפעולות והתקשרות עם בזק היא אך ורק שלי.

ת: נכון, היא אך ורק שלך. הוא נכנס אליך דרך האינטרנט ואין שום משמעות לבזק". (עמוד 90).

בעניין זה לטעמי נתגלעה מחלוקת בין המומחים, ועל כן, אני מוכן להניח, שלשם ביצוע הבדיקה יש צורך בהצלבת המון נתונים ובעניין זה אני מאמץ את עמדתו של עד ההגנה מר שמעון, בתשובתו לשאלת בית המשפט:

"ת. הוא מתחבר לספק האינטרנט שלו, אתה כב' השופט מתחבר לאינטרנט שלך וזה שקוף לבזק, חודר למחשב שלך ועכשיו התקפות נוספות יהיו מן

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

> **המחשב שלך למחשב אחר. אבל הנקבות יישארו, צריך לסנכרן מתי הוא התקשר לאינטרנט, שיחות הזדהות/תרשומות שיחות של בזק, תרשומת הזדהות לספק האינטרנט של כל אחד מן הצדדים, ולהצליב את שלושתם."** (עמוד 89 – ההדגשות שלי ס.כ)

בעניינינו רוב הנתונים הללו היו קיימים ואף על פי כן, לא הוכחה טענת ההשתלטות על ידי אחר, אך גם אם חלק מנתונים אלו היו חסרים, היתה הדרך פתוחה בפני ההגנה להשלים את החסר; אך היא לא עשתה כן.

מאפייני הווירוס

הווירוס שהופץ, כלל פקודה שממיסה אותו לאחר שהוא מדביק את מחשב הקורבן, ומכאן שהעובדה שקובץ הווירוס השלם נמצא במחשב הנאשם, מעידה שמקור הווירוס במחשב הנאשם, אחרת הוא היה מומס, וכך העיד החוקר ניר אלקבץ **בעמוד 48**:

> **"ש. אני אומר לך קטגורית, שמישהו השתמש במחשב של מר לרמן שאתה בכלל לא בדקת את זה, כן או לא.**
>
> **ת. לא. הסוס הטרויאני שנמצא במחשב הקורבנות ממיס עצמו לאחר התקנתו. אם המחשב של הנאשם היה מודבק אז הסוס הטרויאני לא היה גלוי, אלא מחוק, מה שלא היה במקרה הזה. לפיכך, הסיטואציה שתיארת שום אחיזה במציאות."**

וכאן עולה השאלה, אם מישהו אחר השתלט על מחשב הנאשם, למה שהוא ישתיל את אותו וירוס ולא יפעיל את פקודת ההמסה, אם הוא באמת רצה לטשטש את עקבותיו.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

מיקום קבצי עריכת הווירוס

קבצי עריכת הווריוס והכנתו גם הם נמצאו במחשב הנאשם, ולכן החוקר ניר אלקבץ, טען שזה מעיד שהווירוס נערך במחשב הנאשם, עוד הוסיף שלא נמצאו אינדיקציות שמראות שהיתה השתלטות על המחשב וכך הוא **מעיד בעמוד 51-52**:

> **"ש. איזה אינדיקציות היו צריכות להימצא במחשב של הנאשם במהלך הבדיקה, כדי לעורר חשד שמישהו אחר חיצוני השתמש במחשבו של הנאשם והחדיר את הוירוס, הסוס הטרויאני למחשב שלו.**
>
> **ת. בגלל שראינו שקובץ עריכת הנגיף נמצא במחשבו של הנאשם וכן קובץ המדביק עצמו, הסרבר נמצא שם וכן קבצים נוספים שהועלו לאינטרנט ובקובץ עריכת הסרבר היה מסומן למיטב זכרוני וי ליד האפשרות של התמוסס מיד לאחר התקנתו, בגלל שהוא שם ולא נמחק, אני הסקתי שהמחשב אינו נגוע בוירוס הזה, בסוס הטרויאני הזה."**

העדר עדות לפגיעה במחשב הנאשם

מקובלת עליי טענת המאשימה בעניין היעדר שיבושים במחשב הנאשם, כי אם באמת המחשב שלו היה נגוע בסוס טוריאני, כי אז היינו מצפים שהנאשם ימסור שהיו לו תקלות ובעיות במחשב, דבר שמאפיין מחשב נגוע. יש לזכור, שגם בעדויות הקורבנות העידו שהווירוס גרם למחשב לנזקים כבדים.

העקבות של ההשתלטות

בעניין זה העיד המומחה מר שמעון: " **בדרך כלל יראו רק את העובדה שיש SUB 7 במחשב הנשלט, לא יראו בדרך שום עקבות של ההשתלטות.**"(עמוד 88 לישיבה מיום 31/3/05).

וכאן עולה השאלה, מניין באו כל הקבצים שנמצאו במחשב הנאשם, שכן לא סביר שנמצא במחשב הנאשם קבצים רבים שקשורים בווירוס, שעה שנטען שמישהו אחר השתלט על מחשב הנאשם. הטענה שכביכול ה"אחר", רצה להפוך את מחשב הנאשם לחשוד, לא יכולה להסביר זאת, שכן מטרת האחר הנה לצמצם את העקבות עד כמה שניתן בכדי להמשיך ולהשתמש במחשב הנתקף והנשלט.

עמדת ההגנה

מלבד דברי ההגנה שהובאו לעיל, מוסיפה היא וטוענת שנטל הראייה להוכחת טענת ההשתלטות על מחשב הנאשם מוטל על כתפי המאשימה, היכן שכל המידע הקשור לטענה זו, מצוי בידיה, כמו כן, תקופת החקירה היתה ארוכה יחסית, דבר שמנע מהנאשם להשיג ראיות רלבאנטיות. הדברים מקבלים משנה תוקף, לאור העובדה שכבר בהזדמנות הראשונה, דבק הנאשם בטענת ההשתלטות על ידי אחר, ואף על פי כן, גורמי החקירה לא בדקו זאת.

היקף תופעת השימוש במחשב כפלטפורמה

העד המומחה מר ברגר גולן (להלן, מר ברגר), התייחס להיקף השימוש במחשבים בתור פלטפורמה לתקיפת מחשבים אחרים. לטענתו, תופעה זו נפוצה מאוד, ובדרך כלל ההאקרים בוחרים במחשב של אדם אחר. העד אף אומר, בעמוד 2 לחוות הדעת המשלימה **(ס/6א'):**

> **"מבדיקות שאני לקחתי בהן חלק באלפי מחשבים בארבע השנים האחרונות, ניתן היה לראות שבכולן החדירות למחשב נעשו דרך טרמינלים, קרי: שלא באופן ישיר, אלא באמצעות מחשבים של אחרים."**

דברים אחרונים אלו אינם מקובלים עלי, שכן על אף שהמומחה טוען שהוא ניתקל באלפי מקרים של שימוש במחשב כבסיס לביצוע עבירות, עדיין הוא לא ביסס זאת על מחקרים או על סטטיסטיקות, הוא אף לא הביא מקרים בהם הטענה נתקבלה (מלבד הזכרת פרטים מעטים על פסק דין מאנגליה) ושהוכח שההשתלטות בוצעה על ידי אחר. המומחה הסתפק באמירה, שהוא בעצמו בשיתוף עם החוקר אייל פטרבורג חקרו מקרה שבו עלתה הטענה של שימוש במחשב כבסיס לתקיפת מחשבים אחרים, כוונתו היא לחקירה בעניין מכון וויצמן.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

המצאות סוס טרויאני במחשב הנאשם

לטענת ההגנה, בחיפוש שנערך במחשב הנאשם, נמצא הקובץ EDITSERVER.EXE, שמאפשר סריקה והתחברות למחשב ה"קורבן", במסך הפתיחה של קובץ זה נמצא כי הדיווח על פעולות הקורבן מועבר למנוי ICQ שמספרו 14438136, לדואר אלקטרוני **mail@mail.com** ולכתובת IP 192.41.3.130. לטענת ההגנה, כתובות אלו לא נבדקו על ידי המשטרה, על אף החשיבות הנעוצה בכך, שכן זה מעיד שהנאשם בעצמו היה קורבן לסוס טרויאני וזה יכול לעזור לו בהגנתו העיקרית, קרי שמישהו אחר השתלט על מחשבו וביצע משם את העבירות.

טענה זו של ההגנה יש בה ממש והיא מתקשרת לנושא של פגמים בחקירה, שאדון בו בפרק הבא.

המאפיינים של ביצוע העבירות

התקופה שבה בוצעו העבירות, קרי מיום 23.12.00 ועד ליום 21.1.01, הנה נקודתית וזמנית, דבר שמעיד, לטענת ההגנה, שאין בפנינו עבריין מחשבים, אחרת היה מדובר בתקופה ארוכה יותר. עוד מוסיפה ההגנה, שהיינו מצפים ממי שעובר עבירות כאלו למחוק את הקבצים אחרי שהוא מסיים, לא כך היה במקרה דנן.

מחשבה של הגב' אסנת אברבנל

אחד ממספרי ה- ICQ שנמצאו במחשב הנאשם שייך לגב' אברבנל וזאת על סמך **ת/66א,** ומכאן היא נחקרה במשטרה ביום 24.1.02, מחשבה נבדק, ונמצאו בו סוסים טרויאניים רבים, אם כי נקבע על ידי המשטרה, שאין קשר בין הקבצים הנגועים הרבים שנמצאו במחשבה לבין הנאשם או מחשבו. החוקר ניר אלקבץ הגיע למסקנה הזו על סמך בדיקת המחשב שלה. עוד הוסיף החוקר, שלא נמצא קשר בין הסוסים שנמצאו במחשב שלה לבין אנשים אחרים, אחרת הוא היה מעדכן את ראש צוות החקירה. **(ראה עמוד 49 לפרוטוקול).**

לטענת ההגנה, מבדיקת המשטרה עולה עוד, שהסוס הטוריאני שהתגלה במחשב העדה שולח הודעות למספר ICQ אחר שלא שייך לנאשם, לפיכך זה מתיישב עם טענת הנאשם בעניין טענת

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

ההשתלטות מרחוק על ידי אדם אחר. גם כאן, הימנעות המשטרה מלחקור את בעל מספר ה-ICQ מהווה כשל חקירה חמור לגישת ההגנה.

מר גולן התייחס בחוות דעתו, לממצאים שהתגלו במחשבה של הגב' אברבנאל, לטעמו ממצאים אלו מתיישבים יותר עם המסקנה שמחשב הנאשם נשלט על ידי אחר, שכן כזכור, הסוס הטוריאני שנמצא שם שלח הודעה למספר ICQ שלא נמצא במחשב הנאשם, ואף גורמי החקירה לא בדקו למי הוא שייך, ועל כן, טוען המומחה שסביר להניח שאחרי שמחשב הנאשם נתפס על ידי המשטרה, ה"אחר" לא יכל לשלוט עוד במחשבה ועל כן, חיפש בסיס אחר שדרכו יוכל להמשיך ולשלוט, לפיכך, טוען המומחה שהימנעות המשטרה מלחקור בעניין זה מהווה פגם חמור.

המאשימה חולקת על התיזה שמעלה המומחה, וטוענת שהעובדה שבמחשב הגב' אברבנאל נמצאו סוסים טרויאניים רבים, מעידה על כך שמחשבה היה פרוץ לכל גולשי האינטרנט.

לטעמי, סברת המומחה בעניין זה הנה השערה תיאורטית שרלבאנטית לשאלה האם הימנעות המשטרה מבדיקת מספר ה-ICQ שהתגלה במחשב הגב' אברבנאל, מהווה פגם בחקירה? תשובה לשאלה זה תינתן בפרק הבא שדן בפגמים בחקירה.

<u>האם אפשר לשנות את הסיסמאות מרחוק?</u>

כזכור, הסיסמה שנמצאה שימשה את הנאשם ב- 6 שימושים שונים. ההגנה טוענת שה"אחר" שחדר למחשב הנאשם יכל גם לשנות את הסיסמה. לעניין סיסמת ה-BIOS, (לוח האם) העיד החוקר ניר אלקבץ, שהוא לא מודע לאפשרות כזו, על אף ניסיונו העשיר בתחום, אך בכנתו הוא הוסיף "**שבמחשבים אפשר הכל**" (עמ' 39 לפרוטוקול). בעוד המומחה מר גולן ציין בחוות דעתו: "**רכיב ה-BIOS ניתן לכתיבה מרחוק במהלך חדירה למחשב**,..." **(ראה ס/6 עמ' 11).**

המאשימה טוענת שההגנה יכלה להוכיח את טענת ההשתלטות על מחשב הנאשם, וכן את טענת אפשרות שינוי סיסמת ה-BIOS מרחוק, בעזרת ניסוי בפני ביהמ"ש שבו ינסה המומחה להשתמש במחשב הנאשם בתור פלטפורמה לביצוע תקיפה למחשב אחר או לשנות את סיסמת ה-BIOS בזמן שהמחשב מחובר לאינטרנט, אך המומחה נמנע מכך.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

בעניין זה, הצדק עם המאשימה, שכן שעה שישנה מחלוקת קשה בין המומחים, האחד אומר שאפשר לשנות את הסיסמה בקלות ובלי כל בעיה, והשני טוען שהוא לא שמע על אפשרות שינוי על אף ניסיונו הרב, נראה לי שהדרך הראויה הנה עריכת ניסוי בפני ביהמ"ש. בעניינינו נראה לי שהמצאות הסיסמה גם בשומר מסך מוכיחיה מעל לכל ספק סביר שלא ה"אחר" קבע את הסיסמה אלא הנאשם במו ידיו.

המסקנה שעולה מכל האמור לעיל הנה, שלא הובאו ראיות שמוכיחות ש"אחר" השתלט על מחשב, הנאשם, אפשרות זו נשארה בחזקת אפשרות תיאורטית, שאינה מקימה ספק סביר, שכן כידוע "**..הספק הסביר צריך להיות מציאותי, ממשי, רציונאלי ומעוגן בעובדות המקרה, ולא תיאורטי והשערתי...**" ראו עמוד 63 לספרו של כבוד השופט בדימוס לינדנשטראוס, **על הספק הסביר**, והפסיקה שמאוזכרת שם. יחד עם זאת, עלינו להשיב על השאלה האחרונה, בעניין מחדלי החקריה ונפקותם.

<u>פגמים בחקירה</u>

ההגנה טוענת שבחקירה נפלו מספר פגמים. ניתן לחלק את הטענות בעניין פגמי החקירה לשתי קבוצות: **הראשונה,** עוסקת בפגמים בניהול החקירה, בין היתר, משך ניהול החקירה, התוכנות ששימושו את החוקרים, אי בדיקת מחשבו של מר כוכבי ועוד.

השנייה, עוסקת **במחדלי החקירה** שהתבטאו באי חקירת טענת הנאשם בעניין השימוש במחשבו בתור פלטפורמה, טענה זו מתרכזת לדעתי בשני עניינים מרכזיים: **הראשון,** אי בדיקת הפרטים שנמצאו במחשב הנאשם לפיהם הוא היה נגוע בסוס טרויאני ששידר פרטים לכתובת דוא"ל מסוימת. **השני,** אי בדיקת פרטים מסוימים שהתגלו במחשבה של גב' אברבנל.

להלן אתייחס בקצרה לטענות ההגנה בעניין הפגמים ששיכים לקבוצה הראשונה, ולאחר מכן אסקור את ההלכה בעניין מחדלי החקירה ואישמה על עובדות המקרה דנן.

<u>הקבוצה הראשונה</u>

ההגנה מלינה על הזמן שלקח למשטרה לחקור את הפרשה, שכן החקירה נפתחה ביום 29.1.2001 בעוד מחשב הנאשם נבדק רק ביום 6.5.2001, לטענתם זמן זה, הנו משמעותי ביותר בעולם

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

המחשבים מבחינת יכולת לפתח תוכנות, להעלים ראיות ועקבות, זאת במיוחד לאור העובדה שבחמשת החודשים לא בוצעה שם עבירה ממחשב הנאשם.

ההגנה סומכת את ידה בעניין מחדלי החקירה גם על עדותו של מר גולן, שעבד בעבר באותו יחידה חוקרת. בחוות דעתו טען החוקר שחקירת המשטרה לקתה בכמה פגמים, למשל: ביצוע העתקת דיסק המקור לדיסק העתק, ניקוי הדיסק שלא בהתאם לנהלים, חוסר תיעוד של חלק מפעולות החקירה כמתחייב מהנהלים, אי נעילת המחשב לאחר תפיסתו, זיהום "זירת הפשע" על ידי הכנסת תוכנות למחשב הנאשם וחיבורו לאינטרנט ומידת האבטחה של חברת ICQ ביחס לפלטי המחשב שהתקבלו על ידה.

<u>תשובת המאשימה</u>

המאשימה מצדה, דוחה טענות אלו בשתי ידיים, לטענתה העתקת הדיסקים מתבצעת בלי שהחוקר צופה בתוכנו של הדיסק. עוד נטען, שהתוכנות שבהם השתמשו החוקרים ידועות היטב למומחה על אף ששמותיהם לא צוינו בדוחות הפעולה.

לעניין השימוש בדיסק חדש לחלוטין, טוענת המאשימה שלא ברור על מה דרישה זו מבוססת, שכן הפרקטיקה הקיימת במשטרה ובעולם, אינה דורשת שימוש בדיסק חדש. לעניין העתקה החוזרת של מחשב הנאשם, לאחר העברת התיק מהשלוחה הצפונית, טוענת המאשימה שסוגיה זו אינה בתחום מומחיותו של המומחה, מה גם ששיטה זו מלמדת על מקצוענות והיא אף היתה סבירה ביותר בנסיבות העניין. המאשימה טוענת שכל התוכנות ששמשו את צוות החקירה הנן אמינות, קבילות ומקצועיות ביותר, והמומחה בעצמו השתמש בהם בזמן שירותו במשטרה. לעניין, נוכחות עדים בבדיקת המחשב, טוענת המאשימה, שבתקופת החקירה, החוק, הפסיקה או אף הנהלים לא דרשו נוכחות של עדים, עד לב"ש 1153/02 **מדינת ישראל נ' מיכאל אברג'ל,** שם נקבע שיש חובה שיהיו עדים, כיוון שחיפוש במחשב דומה לחיפוש בחצרים.

לעניין אי בדיקת מחשבו של מר כוכבי שמש, טוענת המאשימה, שהסיבה לכך הנה מחיקת הקבצים על ידי מר כוכבי או מי מטעמו, עוד היא מוסיפה שלשם הרשעה בעבירת הפצת ווירוס לא צריכים להוכיח שמחשבים נפגעו, אלא די בהוכחת מקור הפצת הוירוס וכוונת מפיץ הוריוס.

ייאמר מיד, שהמומחה בחוות דעתו יורה חצים לכל הכיוונים, מבלי לתת חלופות, להצביע על בעיות או אף להביא ממצאים משלו, הרי יש לזכור שהמחשב של הנאשם פתוח לבדיקת ההגנה, כל

בתי המשפט

<u>בית משפט השלום חיפה</u> **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

מה שהיה עליו לעשות זה לבצע העתקה לדיסק חדש לחלוטין, בעזרת תוכנת ההעתקה האמינה בעולם ע"פ בחירתו, ואז לבוא לביהמ"ש עם הראיה החותכת, שהתוכנות של המשטרה לא עושות את העבודה.

עוד הוסיף המומחה מר גולן, **בסעיף 4 ז' לחוות דעתו**, שמבדיקה שערך במחשב הנאשם, הוא גילה קובץ שמכיל מידע על תוכנת ה-ICQ, קובץ זה נוצר לטענתו ביום 24.3.2001, קרי כעבור חודשיים אחרי העבירות שמיוחסות לו בכתב האישום, לטענתו בקובץ זה לא נמצאו התכתבויות, אלא קיימים כתובות רבות שמלמדות על מקור ניסיונות חדירה אל המחשב וממנו, לטענת המומחה כתובות אלו לא נבדקו על ידי גורמי החקירה.

המאשימה, דוחה את מסקנותיו של המומחה בעניין זה וטוענת שהמומחה לא ציין את שם הקובץ שהוא בדק, כמו כן, המידע על תוכנת ה-ICQ נמצאים בקבצים שהסיומת שלהם הנה dat, יתרה מזאת לטענת המאשימה למומחה אין ידע בבדיקת קבצים של תוכנת ה-ICQ שכן בתקופת שירותו במשטרה הם לא בדקו תוכנה זו.

לדעתי, ההגנה לא הצביעה על פגמים כלשהם בעבודת צוות החקירה, וגם אם פעילות רשות החקירה לא היתה אופטימלית במספר עניינים כגון משך חקירת התיק, עדיין פעולות אלו היו סבירות ביותר ולבטח לא גרמו לפגיעה ביכולת ההגנה של הנאשם. לא כך הדבר בעניין מחלדי החקירה שאדון בהם להלן:

<u>הקבוצה השנייה- מחדלי החקירה</u>

כאמור לעיל, ההגנה טוענת שנפלו שני מחדלי חקירה בעבודת הרשות החוקרת: **האחד**, אי בדיקת סוס טרויאני שהתגלה במחשב הנאשם שלפי טענת ההגנה שידר נתונים למנוי ICQ שמספרו 14438136, לדואר אלקטרוני **<u>mail@mail.com</u>** ולכתובת IP 192.41.3.130. **השני**, במחשב הגב' אברנבל נמצאו מספר סוסים טרויאניים שאחד מהם שידר למספר ICQ מסוים.

בעניין זה ההגנה צודקת, שכן בנסיבות העניין היה ראוי שהרשות החוקרת תבחן נתונים אלו ותבדוק לאן הם מובילים וכיצד הם משפיעים על החקירה, הדברים אמורים במיוחד לעניין המחדל הראשון.

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

ייאמר מיד, שאין חובה על הרשות החוקרת לבדוק כל קובץ וכל הודעה שמתגלים במחשב הנאשם או הקורבן, דרישה זו אינה סבירה, שכן בכל מחשב קיימים מאות הודעות וקבצים וכל מחשב מוביל לעוד עשרות מחשבים במקרה הטוב, האם ראוי וסביר שנדרוש מהרשות החוקרת לבדוק מסת ראיות כל כך אדירה, שעה שפעילות זו דורשת משאבים רבים והתועלת שלה לחקירה אינה מובטחת.

לדעתי, בעניין זה יש לסמוך על הרשות החוקרת שהיא יודעת לערוך את האיזון הראוי ולבחון את הררי המידע שקיימים במחשב ולבור ממנו את הבר מן המוץ. בעניין תפקיד הרשות החוקרת, יפים הדברים שנאמרו בע"פ 721/80 **תורג'מן נ' מ"י**, פ"ד לה (2) 466, 472: **"מטרת החקירה המשטרתית אינה מציאת ראיות להרשעתו של חשוד, אלא מציאת ראיות לחשיפת האמת, בין אם אמת זו עשויה להוביל לזיכויו של חשוד, ובין אם היא עשויה להוביל להרשעתו".**

על רשות החקירה לפעול בסבירות ובמקצועיות, עד שהיא מגיעה למסקנה שהיא אספה די ראיות בכדי לבסס הרשעה של הנאשם או לחלופין שהראיות אינן מספיקות להגשת כתב אישום. כבר נאמר בע"פ 4384/93 **מליקר נ' מ"י** (לא פורסם),(שהובא בפרשת גולדמן שארחיב עליה את הדיבור בהמשך) ש"**על התביעה להוכיח את המוטל עליה ב'ראיה מספקת' ואין נפקא מינה אם היה לאל ידה להשיג 'טובה' הימנה.**"

כפי שציינתי לעיל, הגעתי למסקנה שאכן היו מחדלי חקירה בעבודת צוות החקירה, לפיכך יש לדון בנפקותם של מחדלים אלו: האם הם מביאים לזיכוי הנאשם או שמא יש לקחת אותם בשכלול מכלול הראיות? סקירה רחבה בעניין מחדלי חקירה ונפקותם ניתנה לא מכבר בעפ 10735/04 **יצחק גולדמן נ' מדינת ישראל** (ניתן ביום 20.2.06 פורסם בתא ביהמ"ש העליון). (להלן, פרשת גולדמן).

בפרשת גולדמן, דובר בעבירת שוחד. מחדל המשטרה התבטא באי חקירת אחד האנשים שמהם נדרש השוחד. ביהמ"ש קבע שאכן היה מחדל חקירה, אך אף על פי כן, הוא דחה את הערעור והשאיר את ההרשעה בשוחד על כנה וכך קבע:

> **"העדרה של ראיה אשר מקורה במחדלי רשויות החקירה, אם כן, ייזקף לחובת התביעה עת ישקל מכלול ראיותיה, מן הצד האחד, ויכולה היא לסייע בידי הנאשם עת ישקול בית המשפט באם טענותיו מקימות ספק סביר, מן העבר האחר. על כן, אין לקבוע כי מחדל בחקירה מוביל, מניה וביה, לזיכוי**

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

הנאשם. נפקותו של המחדל תלויה בתשתית הראייתית הפוזיטיבית הספציפית שהציגה התביעה, מחד, ובספקות הספציפים אותם מעורר הנאשם, מאידך. השלכות המחדל, איפוא, כפי שנקבע בעניין מליקר האמור, תלויות ב"נסיבות המיוחדות של הענין הנדון" (השוו: ע"פ 277/81 הלוי נ' מ"י, פ"ד לח (2) 369, 385-386; ע"פ 5390/96 אבו מדיעם נ' מ"י, פ"ד נג (4) 29, 45-47; ע"פ 7535/02 עודה נ' מ"י (לא פורסם), פסקה 4; וראו גם: ע"פ 5152/04 אגרונוב נ' מ"י (טרם פורסם), פסקה 4; ע"פ 6858/04 פלוני נ' מ"י (לא פורסם), פסקה 30; רע"פ 8713/04 רצהבי נ' מדינת ישראל (לא פורסם), פסקה 8). עמד על כך בית המשפט לאחרונה:

"מכל מקום חשוב להדגיש, כי התשובה לשאלה אם פגמים ראייתיים שהתגלו מעוררים ספק סביר באשמת הנאשם, תיגזר תמיד מבחינת נסיבותיו המיוחדות של המקרה הנתון" (ע"פ 4855/02 מ"י נ' בורוביץ (טרם פורסם)."

המסקנה מן האמור לעיל, הנה שעלינו לבדוק האם מחדלים אלו מעוררים ספק סביר ביחס להרשעה או שמא הראיות שהוצגו מובילים למסקנה אחת ויחידה לפיה מי שביצע את העבירות הנו הנאשם?

לדעתי, המאשימה הביאה די והותר ראיות שמוכיחות מעל לכל ספק סביר שהנאשם הוא זה שביצע את העבירות, להלן אמנה במעוף הציפור את העובדות המרכזיות שהוכחו במהלך המשפט: במחשב הנאשם נמצא הווירוס שהופץ, קבצים לעריכת הווירוס, קבצים רבים ששייכים לשני קורבנות שהעידו שהם לא שלחו קבצים אלו לנאשם, כתובות ה I.P הובילו לביתו של הנאשם, נמצאה התאמה בין זמן הפצת הווירוס לבין שם המשתמש של הנאשם ומספר הטלפון של ביתו, שני הקורבנות העידו שהם נדבקו מן הווירוס והם חשדו בנאשם, נמצאה סיסמה ששימשה את הנאשם בהרבה שימושים שמוכיחה מעל לכל ספק שהנאשם הוא זה שהפיץ את הווירוס, שכן הסיסמה היתה גם הסיסמה של הווירוס אך גם הסיסמה של שומר המסך במחשב הנאשם.

בטרם סיום אעיר שתי הערות: **האחת,** ההגנה יכלה לבקש צו מביהמ"ש שיורה על חשיפת הפרטים החסרים בעבודת המשטרה, שכן יש לזכור שלא הוכח שהנתונים שקשורים למחדלי

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

החקירה לא קיימים עוד. **השנייה,** התנהגות הנאשם במהלך חקירתו מחזקת את כל הראיות שהובאו לעיל ואף היא הביאה אותי למסקנה שאשמתו הוכחה מעל לכל ספק סביר, להלן אתאר התנהגות זו בקצרה:

בחקירתו השלישית של הנאשם מיום **16.10.01** ע"י רפ"ק אייל פטרבורג, **(ראה, ת/50)** הוא סירב להתייחס לסיסמאות שהוא משתמש בהם במחשבו האישי וטען שהוא לא זוכר אותן, כמו כן, הוא נמנע מלהשיב על שאלות שנוגעות לתוכנית ה- ICQ ,להלן אביא מספר דוגמאות:

"שאלה: איזה סיסמאות יש לך במחשב?
תשובה: אין סיסמאות?
שאלה: למחשב שלך יש סיסמת "שומר מסך", מהי?
תשובה: אני לא זוכר מה שהייתה לי סיסמה בשומר המסך,
וגם אם הייתה אני לא זוכר אותה היום."

בהמשך מסר הנאשם שהוא לא יודע מה זה BIOS וכן לא רצה להשיב על שאלות שנוגעות למחשבו האישי ולתוכנת ה-ICQ וכך השיב בעמוד 3:

"שאלה: האם אתה מכיר או משתמש בתוכנת ICQ?
תשובה: אני לא רוצה לענות לשאלות שקשורות למחשב
שלי יותר, חוץ מזה כן נשאלתי את השאלה הזאת? "

לטעמי לא סביר שהנאשם יישכח את סיסמת שומר המסך שלו, כזכור תפיסת מחשב הנאשם התבצעה ביום **6.5.01** בעוד חקירתו בעניין זה נערכה ביום **16.10.01**, קרי עברו 5 חודשים. כמו כן, יש לזכור שהנאשם כן זכר את מספר ה-ICQ שלו. אך כנראה הנאשם נמנע מלמסור פרטים מחששו להתמודד עם הראיות שהוצגו בפניו, שכן אין לו הסבר שמניח את הדעת.

<u>סיכום</u>

פרשה זו עניינה בגולש אינטרנט שביצע עבירות מחשב כלפי שני קורבנות. בשני המקרים דרך הפעולה זהה, הנאשם שלח הודעה תמימה שהכילה וירוס מסוג סוס טוריאני, הקורבן הוריד את הקובץ, ובכך התאפשרה לנאשם גישה חופשית למחשב הקורבן. בהמשך, הנאשם ניצל את הפרצה

בתי המשפט

בית משפט השלום חיפה **פ 004888/02**

בפני: כב' השופט כ. סעב **תאריך: 28/02/2006**

שנפתחה לנגד עיניו, ושלף קבצים אישיים ששייכים לקורבנות. במהלך המשפט הוצגו ראיות רבות, הן דגיטליות, הן ישירות והן נסיבתיות. ראיות אלו כללו את הקבצים שהופצו באינטרנט, כולל קבצים לעריכת הוירוס, קבצים אישיים של הקורבנות שנמצאו במחשב הנאשם, נתוני תקשורת רבים שמובילים למחשב הנאשם, שיחות שהתנהלו בין הנאשם לקורבנות, כמו כן, התגלתה סיסמת הוירוס שבה עשה הנאשם שימוש רב. נוסף על כך, הקורבנות סיפרו על היכרותם עם הנאשם ועל התקלות שנגרמו למחשבים שלהם בגלל החדרת הוירוס.

סוף דבר

לאור כל האמור לעיל, אני מזכה את הנאשם מהעבירה של עריכת וירוס, עבירה בניגוד לסעיף 6(א) לחוק המחשבים וכן מהעבירה של החדרת וירוס למחשבה של דניאלה. בעוד אני מרשיע את הנאשם ביחס לחדירה למחשבים של מר כוכבי וגב' קרן אייזנברג, בעבירות הבאות:

א. שיבוש או הפרעה למחשב או לחומר מחשב, עבירה בניגוד לסעיף 2 לחוק המחשבים.

ב. חדירה לחומר מחשב כדי לעבור עבירה אחרת - עבירה בניגוד לסעיף 5 לחוק המחשבים.

ג. החדרת נגיף מחשב, עבירה בניגוד לסעיף 6 (ב) לחוק המחשבים.

ד. פגיעה בפרטיות, עבירה בניגוד לסעיף 5 לחוק הגנת הפרטיות, התשמ"א- 1981.

ניתנה היום, ל' בשבט התשס"ו (28 בפברואר 2006) במעמד הצדדים.

כ. סעב, שופט