

הנחיות פרקליט המדינה	הנחיה מספר 2.38 – מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב
	ט"ז אלול התשע"ח, 27 אוגוסט 2018

2.38 – מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב

עניינה של הנחיה זו בהתוויית מדיניות התביעה בהעמדה לדין, בניהול התיקים ובטיעון לעונש בעבירה של חדירה לחומר מחשב.

א. המסגרת החוקית

1. חוק המחשבים¹ קובע כי חדירה שלא כדין לחומר מחשב היא עבירה שעונשה שלוש שנות מאסר, להלן לשון סעיף 4 לחוק:

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

2. סעיף 5 לחוק המחשבים קובע נסיבה מחמירה, לפיה חדירה לחומר מחשב שבוצעה כדי לעבור עבירה על חוק אחר (שאינו חוק המחשבים) עונשה חמש שנות מאסר.

3. סעיף 1 לחוק המחשבים מגדיר כי "חומר מחשב" הוא "תוכנה או מידע", כאשר אלה מוגדרים אף הם בסעיף 1 לחוק המחשבים, ובהכללה ניתן לומר כי משמעותה של הגדרה זו היא ש"חומר מחשב" הוא למעשה כל חומר דיגיטלי.

ב. פרשנות עבירת החדירה לחומר מחשב

4. ביום 15.12.2015 ניתח בית המשפט העליון את סעיף 4 הנ"ל, במסגרת פסק הדין בעניין **עזרא**.² מלשון החוק ומרוח פסק דינו של בית המשפט העליון בעניין **עזרא** עולה כי יש לפרש את היסוד ההתנהגותי של "חדירה" באופן רחב הכולל כל גישה או כניסה אל מידע הנמצא במחשב וזאת בכל דרך שהיא, הן בהפעלה, הן בהתחברות (לרבות התחברות מרחוק) והן בהתקשרות אל המחשב.

¹ חוק המחשבים, התשנ"ה-1995, ס"ח 1534.

² רע"פ 8464/14 מדינת ישראל נ' עזרא (15.12.2015). יוער כי בעקבות פסק הדין הוגשה מטעם ההגנה בקשה לדיון נוסף בהלכה שנקבעה בפסק הדין, אך הבקשה נדחתה על ידי בית המשפט העליון במסגרת דני"פ 965/16 עזרא נ' מדינת ישראל, (15.2.2016).

5. כעולה מפסק הדין בעניין **עזרא** אין לדרוש התגברות על מנעול או מכשול טכנולוגי, כגון סיסמה או הצפנה, כתנאי להתקיימות יסוד החדירה שבעבירה. עם זאת, קיימת חומרה יתרה בביצוע עבירה של חדירה לחומר מחשב בדרך של התגברות על מנעול טכנולוגי, והדבר רלוונטי לעניין העונש שיוטל על מבצע העבירה ולעיתים עשוי להיות רלוונטי עוד בשלב בחינת העניין הציבורי בהעמדה לדין.
6. בית המשפט העליון קבע, כי העבירה אינה מוגבלת רק למקרים בהם נעשתה חדירה למידע המבוטא בשפת הקוד של המחשב (שפה קריאת מחשב בלבד) והיא מתקיימת גם במקרים בהם אדם חדר לקבצי מסמכים ולמידע דיגיטלי הקריא בשפת בני האדם.
7. כמו-כן, עולה מפסק הדין כי משמעות הנסיבה "שלא כדין" היא כי החדירה נעשתה בהיעדר הרשאה מאת הבעלים של חומר המחשב הנחדר או מאת כל גורם אחר המוסמך ליתן הרשאה כאמור. הכוונה במונח "הרשאה" היא כי הבעלים של חומר המחשב או גורם מוסמך אחר, נתן הסכמה לגישה אל חומר המחשב. עבירת החדירה מתייחסת למצב של היעדר **הרשאת גישה** להבדיל ממצב של היעדר **הרשאת שימוש**. חריגה מ"הרשאת גישה", קרי גישה לחומר מחשב, כניסה אליו ועיון בו, כשהדבר לא הותר בידי הבעלים או המחזיק כדין במידע – עולה כדי "חדירה שלא כדין" לחומר המחשב. לעומת זאת, חריגה מ"הרשאת שימוש", קרי שימוש במידע שלא למטרה שלשמה הוענקה הרשאת הגישה אליו במקור³ - אינה עולה כדי "חדירה שלא כדין" לחומר מחשב. עם זאת, יובהר כי חריגה מ"הרשאת שימוש" בהחלט עשויה להקים עבירות אחרות, כגון עבירות על סעיפים 2(9) או 16 לחוק הגנת הפרטיות, התשמ"א – 1981 או עבירה על סעיף 284 לחוק העונשין, התשל"ז – 1977, הכל בהתאם לנסיבות העניין.
- ודוק, ייתכנו מצבים שבהם הוענקה לאדם הרשאת גישה אל מחשב מסוים, אולם ההרשאה הוגבלה לתיקיות מסוימות בלבד בתוך אותו מחשב. במקרה שבו האדם חדר שלא כדין לתיקיות אחרות בתוך המחשב, הרי שהגם שיש לו הרשאה לגישה לאותו מחשב לתיקיות מסוימות, החדירה אל התיקיות הנוספות תעלה כדי חריגה מהרשאת גישה ולא רק לכדי חריגה מהרשאת שימוש.
8. הפרשנות של עבירת החדירה, כעולה מלשון החוק ומפסק הדין בעניין **עזרא**, מאפשרת להימנע מפרשנות הקושרת את החדירה לטכנולוגיה ספציפית. נוסחה הרחב יחסית של העבירה מאפשר להימנע ממצב שבו העבירה תהפוך ללא-רלוונטית עם כניסתן של טכנולוגיות חדשות, ולהישאר ברובד נורמטיבי המספק הגנה משפטית הולמת למידע המאוחסן במחשבים, ואכיפה יעילה בעבירות אלה. אולם, בשל היקפה הרחב יחסית של העבירה יש להימנע ממצב של העמדה לדין בשל מעשים של מה בכך. על כך יפורט להלן בסעיף 15.

³ למשל במקרה של עובד, שהותרה לו גישה למאגר מידע מסוים לצרכי עבודתו, ואותו עובד מעיין במידע ומשתמש בו לצרכים אישיים.

הנחיות פרקליט המדינה

הנחיה 2.38 - מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב

9. יש לזכור כי המחוקק אסר על חדירה לחומר מחשב כשלעצמה, אף אם לא הוכחה תכנית המשך עבריינית (שאז ייתכן וקמה עבירה של חדירה לחומר מחשב כדי לעבור עבירה אחרת, לפי סעיף 5 לחוק המחשבים). זאת בשל הנזק הפוטנציאלי העלול להיגרם מעצם החדירה שלא כדין לחומר המחשב הנמצא במחשב. על כך יפורט להלן בסעיף 14(ב).

ג. דיות ראיות

10. על התביעה רובץ הנטל להוכיח שהחדירה בוצעה ללא הרשאה מאת בעל חומר המחשב או מאת אדם אחר שהוא בעל הרשאת גישה לחומר המחשב. במקרים בהם קיימת עמימות בשאלת ההרשאה שניתנה לחשוד לחדור לחומר המחשב, וקיים ספק סביר ביחס לשאלה האם פעולת החדירה בוצעה בניגוד להרשאה – יפעל הספק לטובת החשוד.

11. במקרים בהם קיימות ראיות לכך שהחשוד התגבר על מנעול או מכשול טכנולוגי לצורך ביצוע החדירה, כגון על ידי ניחוש סיסמה, עקיפתה או פיצוחה, הדבר יעיד על פי רוב, כי החדירה בוצעה ללא הרשאה.

12. תשומת הלב לכך שגם כאשר נכנס החשוד ב"דלת הראשית" – כלומר מקליד את הסיסמה ולא עוקף או מפצח אותה, קיימים מצבים בהם הדבר עשוי, בהתאם לנסיבות, להיחשב כחדירה שלא כדין, כגון מקרה של קבלת הסיסמה במרמה או בתחבולה, השגתה מאתרים באינטרנט בהם פורסמה הסיסמה ללא רשות או השגתה ממשתמשים אחרים שאינם בעלי הרשאה.

13. במקרים בהם הסתיימו יחסים בין שני צדדים, שכללו הרשאה לשימוש במחשב או ברשת מחשבים, כדוגמת עובד שפוטר מעבודתו, אך עדיין פרטי ההתחברות למחשבי המעסיק ידועים לו ולא שונו ולא נלקחו ממנו, יש לבחון אם עולה בבירור מנסיבות סיום היחסים, מאופי מערכות המידע ומיתר הנסיבות, כי העובד שפוטר אינו רשאי עוד להתחבר למחשבי החברה. מובן כי עמימות בעניין זה עשויה לפעול לזכות החשוד.

ד. שיקולי העמדה לדין בעבירה של חדירה לחומר מחשב

14. הנסיבות המפורטות להלן תישקלנה כנסיבות לחומרה, בבוא הפרקליט לבחון העמדה לדין בעבירה של חדירה לחומר מחשב, כאשר כל נסיבה שמתקיימת תגביר את הנטייה להעמיד את החשוד לדין:

(א) קיומה של נסיבה מחמירה לפי סעיף 5 לחוק המחשבים, כלומר חדירה כדי לעבור עבירה אחרת וכן ביצוע בפועל של עבירות נוספות בעקבות ביצוע החדירה לחומר מחשב (אף ללא הוכחה כי החדירה בוצעה כדי לעבור עבירות אחרות).

הנחיות פרקליט המדינה

הנחיה 2.38 - מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב

(ב) גרימת נזק, ישיר או עקיף, בעקבות החדירה לחומר המחשב, לרבות נזק למוניטין, נזק למידע, פגיעה בביטחון הלאומי, פגיעה בתשתיות חיוניות, פגיעה בפרטיות, אובדן לקוחות של תאגיד שנחדר שלא כדין, הוצאות לתיקון פרצת האבטחה, ירידת שער המנייה של חברה בורסאית שנחדרה, וכן כוונה או פוטנציאל ממשי להביא לאחד מאלה. יובהר כי אין מדובר ברשימה סגורה. מובן כי ככל שהיקף הנזק המוערך או מידת רגישותו של המידע אליו חדר החשוד, גבוהים יותר - יגבר משקלה של נסיבה זו.

(ג) חדירה למחשב שתכליתה הייתה, או שהביאה בפועל, לפגיעה בצנעת הפרט כדוגמת חשיפתן של תמונות אינטימיות או חשיפת עבר מיני.

(ד) הפקת רווח כלכלי כתוצאה מהחדירה או כוונה להפקת רווח כאמור, בין אם הרווח הגיע לידי החשוד ובין אם הגיע לידי אחר. מובן כי ככל שהרווח הכלכלי שהופק או שהייתה כוונה להפיקו היו גבוהים יותר, יגבר משקלה של נסיבה זו.

(ה) ריבוי מחשבים שנחדרו, או חדירה חוזרת ונשנית לאותו מחשב במועדים שונים.

(ו) תחכום והתגברות על מנעולים טכנולוגיים.

(ז) חדירה לחומר מחשב שהתלוותה לה פעולת התחזות של החודר כבעל המחשב או המידע הנחדר, כדוגמת חדירה לחשבון דוא"ל של אדם, ללא ידיעתו או הסכמתו, ושליחת תכתובות בשמו.

15. להלן יימנו שיקולים לקולא, אשר בהתקיימם תגבר הנטייה להימנע מהעמדה לדין של חשוד בעבירת החדירה לחומר המחשב:

(א) כאשר מבוצעות פעולות לאבטחת מידע או להגנה מפני דליפת מידע ממוחשב, ואגב ביצוען מושגת גישה לחומר מחשב ללא ידיעה או ללא הסכמה של המחזיק בו, והדבר נעשה בתום לב, ללא מניעים נוספים, בלא שנעברו עברות נוספות וללא עיון של ממש בתוכנו של המידע הממוחשב – הרי שככלל תגבר הנטייה להימנע מהעמדה לדין של החשוד.

(ב) קיימים מקרים בהם החשוד מורשה להשתמש במחשב, אולם באותו מחשב נמצא גם חומר שהחשוד אינו מורשה לגשת אליו, כדוגמת שותפים לדירה המשתמשים באותו מחשב ומפרידים בין החומרים השייכים לכל אחד מהם, כשאינן ביניהם הסכמה שכל צד רשאי לעיין בחומר של האחר, או עובד שמורשה במסגרת עבודתו לגשת רק לחלק מהחומרים במחשבי מעסיקו, וגם להיפך – עובד אשר שמר במחשב במקום עבודתו תכנים אישיים שלו, שהמעסיק אינו רשאי לעיין בהם.

במקרים אלה, ככל שהעדר ההרשאה לגשת לתכנים מסויימים היה ברור לחשוד, ולמרות זאת החשוד נכנס לחומר, מתקיימת, על פניו, עבירה של חדירה לחומר מחשב. עם זאת, סיטואציה שכזו יכול שתשמש שיקול לקולא במסגרת השיקולים אם להגיש כתב אישום בגין עבירת החדירה בנסיבות אלה, וההעדפה תהיה לבחון אפשרות להעמיד את החשוד

לדין בעבירות שבוצעו בעקבות החדירה, ככל שבוצעו, כגון פגיעה בפרטיות, וזאת בשל הקרבה בין החומר המותר לחומר האסור המאוחסנים באותו מחשב.

חריג לאמור לעיל יתקיים במקרים בהם ניצב מנעול טכנולוגי המפריד בין החומר בו הותר לחשוד להשתמש ובין החומר האסור, כדוגמת קבצים ותיקיות שהוצפנו בסיסמה, והתברר בחקירה כי החשוד עקף מנעול טכנולוגי זה.

ה. היחס בין עבירת חדירה לחומר מחשב לעבירות נוספות

16. במקרה בו לאחר חדירה לחומר מחשב בוצעו עקב כך עבירות נוספות, כגון גניבה, פגיעה בפרטיות וכדומה, הוראת החיקוק הרלוונטית עשויה להיות סעיף 5 לחוק המחשבים, הקובע כי חדירה לחומר מחשב כדי לעבור עבירה אחרת (שלא לפי חוק המחשבים) – דינה מאסר חמש שנים. הכוונה לעבור עבירה אחרת יכולה להילמד, בין היתר, מעצם הקרבה ואף החפיפה בזמנים בין ההפעלה, ההתחברות או ההתקשרות הבלתי-מורשות למחשב, לבין העיון, ההעתקה או השימוש במידע המצוי במחשב הנחדר.

17. במקרים בהם לאחר החדירה לחומר המחשב בוצעו עבירות נוספות לפי חוק המחשבים עצמו (ולא לפי חוקים אחרים), הרי שאין תחולה לסעיף 5 הנ"ל, שכן הסעיף, על פי לשונו, חל רק לגבי עבירות נוספות שאינן לפי חוק המחשבים.

18. אם לצורך ביצוע החדירה לחומר מחשב הושגה במחשב הנחדר נזקה כגון וירוס או סוס טרויאני,⁴ בדרך כלל יקים הדבר עבירה נוספת, לפי סעיף 6(ג) לחוק המחשבים, האוסר בין היתר על העברה, החדרה או התקנה של נזקות, ויש לייחס לנאשם את שתי העבירות. זאת, בשים לב לעובדה שמדובר בשתי פעולות אסורות שונות – כשלעתים גם האינטרסים המוגנים נבדלים בכל אחת מהן.

19. עיון במידע אישי האגור במחשב, שאליו בוצעה חדירה שלא כדין, עשוי להקים גם עבירה של פגיעה בפרטיות לפי סעיף 2(5) לחוק הגנת הפרטיות, האוסר על העתקת תוכן של מכתב או כתב אחר, לרבות "מסר אלקטרוני", שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב. סעיף העבירה אוסר על "העתקה" בלתי מורשית או על "שימוש" בלתי מורשה. אף אם המידע בפועל לא הועתק ולא הועבר לאחר, ונמצא כי החשוד עיין בו בלבד, ניתן ואף ראוי לראות בכך משום "שימוש" במידע כמובנו לפי סעיף 2(5) לחוק הגנת הפרטיות.

⁴ "וירוס" הוא כינוי לתוכנת מחשב שסוגלה לחדור אל מחשב ולגרום נזק למחשב, מערכותיו, התוכנות המצויות בו או המידע האגור בו. "סוס טרויאני" הוא כינוי לתוכנת מחשב שסוגלה לחדור אל מחשב, באופן סמוי מפני המחזיק או המשתמש במחשב, ויועדה לבצע פעולות של איסוף או העתקה של המידע האגור במחשב או מתן שליטה מרחוק במחשב הנחדר.

זאת, באופן דומה לקביעת בית המשפט העליון כי "הקשבה" להאזנת סתר עולה כדי "שימוש" בה.⁵

20. יובהר כי אם החדירה בוצעה בדרך של הקלדת שם משתמש וסיסמה השייכים לאדם אחר, ללא ידיעתו או הסכמתו של האחר – ככלל אין לייחס לנאשם בשל כך עבירה של מידע כוזב לפי סעיף 3(א)(1) לחוק המחשבים, האוסר על העברת מידע כוזב לאחר, אלא את עבירת החדירה, הגם שטכנית עלול להשתמע כי החשוד העביר מידע שיש בו כדי להטעות.⁶

1. עיון בחומר חקירה, הצגתו לבית המשפט וטיפול בתפוסים

21. ככלל, חומר המחשב אליו חדר הנאשם יועמד לעיון בלבד במשרדי היחידה החוקרת, זאת כדי למנוע מהנאשם אפשרות ליהנות מפירות העבירה בחסות ההליך הפלילי ולמנוע פגיעה נוספת בקורבן העבירה ובפרטיותו, בהתאם להחלטת בית המשפט העליון בעניין **קרוכמל**.⁷ ניתן ליצור עבור הנאשם עותק שיישמר עבורו במשרדי היחידה החוקרת וישמש אותו לבדיקות, אם יש צורך בכך.

22. ככל שנתפסה במסגרת החקירה מדיה מגנטית (כונני מחשב, התקני אחסון ניידים, תקליטורים וכיוב'), בה אגור מידע שהושג בדרך של חדירה שלא כדין לחומר מחשב, יש להתנגד ככלל לבקשות להשבתה לנאשם, זאת משני טעמים:

(א) יש ליעד תפוסים אלה לחילוט בהתאם להוראת סעיף 39 לפקודת סדר הדין הפלילי, בהיותם "חפצים" שנעשתה בהם עבירה.⁸

(ב) אף אם ימחק החומר שהושג בעבירה, כמהלך מקדים להשבתה לידי הנאשם, עדיין לא יהיה בכך כדי לרפא באופן מלא את החשש מפני אפשרות שחזור החומר בשיטות מתקדמות, ובאופן שיביא להמשך שימוש לרעה בחומר.

23. עם זאת, ככלל, יש להתיר לנאשם להעתיק חומר מחשב הדרוש לו מתוך המדיה המגנטית שנתפסה ברשותו, **כל עוד חומר זה לא הושג בעבירה**. הזכות לקבלת העתק מהחומר נובעת מזכותו הקניינית של הנאשם ולכן חלה אף אם החומר אינו בגדר חומר חקירה.⁹

⁵ ע"פ 1497/92 **מדינת ישראל נ' צוברי** פ"ד מז(4) 177, 200-201, פסקה 11 (23.8.1993).

⁶ עוד על פרשנות העבירה על סעיף 3 לחוק המחשבים, ראו "מדיניות העמדה לדין על עבירה לפי סעיף 3 לחוק המחשבים – מידע כוזב או 'פלט כוזב'" **הנחיות פרקליט המדינה** 2.25 (2016).

⁷ בש"פ 6640/06 **קרוכמל נ' מדינת ישראל** (7.9.2006); ראו גם בש"פ 6022/96 **מדינת ישראל נ' מזור**, פ"ד (נ3) 686 (4.9.1996).

⁸ פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969.

⁹ סעיף 32 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969 קובע כלל של מסירת העתק לחשוד כבר בשלב החקירה, בכפוף לסייגים.

ככלל, אין להסכים להעתקה כוללת של כונן קשיח ומחיקת החומר האסור, מהטעמים המנויים בסעיף 22 (ב) לעיל. לצורך ביצוע העתקה כאמור יש לבקש מהנאשם להצביע על קבצים ותכנים שהוא מבקש לקבל לידי את העתקם, ובהתאם לכך היחידה החוקרת תבצע את ההעתקה, בתנאי שהחומר שסומן על ידי הנאשם לא הושג בעבירה.

24. ככלל, ראוי לבקש לחלט גם את יתר חלקי המחשב ששימשו לעבירה (מארו המחשב הכולל את לוח האם, המעבד, ויתר הרכיבים), בהתאם להוראות פקודת סדר הדין הפלילי, ובשים לב לשוויים.

25. בעניין הגשת ראיות דיגטליות שהושגו בעבירה לבית המשפט, יש לבקש מבית המשפט להשאירן במשמורת התביעה ולהחזיקן במקום מתאים במשרדי התביעה, תוך התחשבות באופי החומר האגור בהן ובמידת רגישותו.

26. במקרה שחומר החקירה כולל נזקות (וירוסים וסוסים טרויאניים) יש לפתוח את החומר במחשב ייעודי נפרד שמנותק מרשת המשרד ומהאינטרנט, ובמקרה הצורך לבקש מהיחידה החוקרת לדאוג להצגת חומר זה.

ז. הטיעון לעונש

27. יש לראות בשימוש במחשב לביצוע עבירות משום מכפיל נזק ביחס לאותן עבירות, המקשה יותר לתפוס את העבריינים המבצעים פעילות פלילית באמצעות האינטרנט. יש לכך משקל לחומרה לעניין הענישה הראויה לעבירות אלה.¹⁰

28. יש להדגיש את פוטנציאל הפגיעה כתוצאה מעבירות מחשב, בשים לב לתלות של הציבור בשימוש במחשבים (לרבות טלפונים חכמים) ובמידע, מה שמעצים את הצורך בתגובה עונשית מחמירה, שתהלוס את הנזק. זאת, אף אם הנזק אינו מוחשי, ישיר ומיידי. בעניין זה יש להדגיש את הפגיעה בפרטיות, לרבות בסוד השיח, העלולה להיגרם כתוצאה מהחדירה לחומר

¹⁰ בפסק הדין בעניין עזרא הדגיש בית המשפט העליון את הצורך בהחמרת הענישה, יפים לענין זה גם דברי השופטת פרקציה בעניין ע"פ 9893/06 לאופר נ' מדינת ישראל, פסקה 19 לפסק הדין (31.12.2007), שצוטטו בהסכמה בפסק הדין בעניין עזרא:

"הצורך בהגנה על הפרטיות ועל עולמו האינטימי של האדם בעולם המודרני, בצד הקלות הבלתי נסבלת הכרוכה בחדירה לעולמו הפרטי באמצעים טכנולוגיים כאלה ואחרים, מחייבים גישה שיפוטית מחמירה, אשר תיישם אמצעי אכיפה נאותים לצורך הדברת תופעה עבריינית, המהווה סימן היכר ליכולות ההרסניות הטמונות בשימוש לרעה בטכנולוגיה המודרנית. החדירה למידע במחשב שוב איננה מצטמצמת לעניינו של פרט שפרטיות חייו הופרה; עניינה בתופעה כללית ורחבה, העלולה לפגוע בפרטיות חייהם של בני ציבור רחב. קיים, אפוא, אינטרס ציבורי חשוב ומיוחד בהחדרת מסר ברור של אכיפה בסוג עבירות זה, להדברת תופעה הולכת ומתגברת של עבריינות מחשב, המאפיינת את העולם הטכנולוגי המתפתח".

ראו גם ת"פ (מחוזי ת"א) 40250/99 מדינת ישראל נ' בדיר (13.11.2001); ת"פ (מחוזי ת"א) 40061/06 מדינת ישראל נ' האפרתי (27.3.2006); ע"פ (מחוזי ת"א) 71227/01 מדינת ישראל נ' אהוד טננבאום (5.6.2002).

המחשב של הנחדר. נוסף על הפגיעה הפוטנציאלית בבעל המחשב הנחדר, עלולה להיגרם אף פגיעה בפרטיותם של צדדים שלישיים שמידע על-אודותיהם אגור באותו מחשב.¹¹

29. יש להבחין בין שלוש קטגוריות של מתחמי ענישה בנוגע לעבירת החדירה לחומר המחשב: **האחת**, קטגוריית המקרים החמורים ביותר, שבהם חלקו העליון של המתחם יתקרב לעונש המקסימום בגין העבירה. **השניה**, קטגוריית מקרי הביניים, שתצדיק ככלל הטלת מאסר בפועל. **השלישית**, קטגוריית המקרים הקלים, אשר בהעדר נסיבות אחרות לחומרה,¹² רף הענישה בעניינם עשוי לנוע בין מאסר מותנה לבין מספר חודשי מאסר בפועל. זאת, בהתאם למפורט להלן (הרשימות שיובאו אינן רשימות סגורות והמקרים שיפורטו בהן יכולים לעבור מקטגוריה אחת לשניה בהתחשב בנסיבות הענין הקונקרטיות).

30. בגדר קטגוריית **המקרים החמורים** ביותר ייכללו המקרים בהם מתקיימות אחת או יותר מהנסיבות הבאות, הקשורות בביצוע העבירה:

(א) חדירה למחשב שהינו חלק מ"מערכת ממוחשבת חיונית" בגוף שהוא משום תשתית לאומית קריטית (הכוונה לגופים המנויים בתוספת הרביעית והחמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח – 1998).¹³

(ב) חדירה למחשבים ולמידע המוחזקים אצל גופים ביטחוניים.

(ג) חדירה למחשבים ולמידע במטרה לפגוע בביטחון המדינה, אף אם אינם שייכים לגופים ביטחוניים או ל"תשתית לאומית קריטית".

(ד) חדירה על-ידי גורם הפועל מטעם מדינה זרה, אף אם לא הוכחה מטרה לפגיעה בביטחון המדינה.

(ה) חדירה למאגרי מידע של בנקים, חברות אשראי וחברות למתן שירותים פיננסיים.

(ו) חדירה למאגרי מידע הכוללים מעל ל-1,000,000 רשומות של מידע אישי.

31. בגדר קטגוריית **מקרי הביניים** ייכללו מקרים שלא מתקיימות בהם נסיבות המדרג הגבוה לעיל, אך מתקיימות בהם לפחות אחת הנסיבות הבאות הקשורות בביצוע העבירה:

¹¹ ראו בש"פ 6071/17 **מדינת ישראל נ' פישר ואח'**, פסקאות 10-12 לפסק דינו של כבוד השופט עמית (פורסם בנבו, 27.8.2017); ע"פ 8627/14 **דביר נ' מדינת ישראל**, פסקה 7 לפסק דינו של כבוד השופט עמית (פורסם בנבו, 14.7.2015); רע"פ 8873/07 **היינץ נ' מדינת ישראל**, פסקה 17 לפסק דינה של כבוד הנשיאה (בדמי') ביניש (פורסם בנבו, 2.1.2011); ע"פ 9893/06 **לאופר נ' מדינת ישראל**, פסקה 19 לפסק דינה של כבוד השופטת פרוקציה (פורסם בנבו, 31.12.2007).

¹² ראו להלן בסעיף 34 להנחיה.

¹³ בין גופים אלה ניתן למנות את הגופים הבאים: בזק, החברה הישראלית לתקשורת בע"מ; פלאפון תקשורת בע"מ; סלקום ישראל בע"מ; פרטנר תקשורת בע"מ; הרשות לניהול המאגר הביומטרי; בנק ישראל; חברת החשמל לישראל בע"מ; מקורות חברת מים בע"מ; רכבת ישראל בע"מ; רשות שדות התעופה; הבורסה לניירות ערך; חיפה כימיקלים בע"מ; הלשכה המרכזית לסטטיסטיקה; רשות המיסים בישראל; חברת מדיטרניאן נאוטילוס (ישראל) בע"מ; בעלי החזקות במאגרי הגז הטבעי ועוד.

הנחיות פרקליט המדינה

הנחיה 2.38 - מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב

(א) חדירה למחשבים של משרדי הממשלה ומוסדות המדינה, שאינם "תשתית לאומית קריטית" ושאינם של גופים ביטחוניים.

(ב) חדירה למטרות ריגול עסקי.

(ג) חדירה לחשבונות בנק או לחשבונות המאפשרים ביצוע העברות כספיות, כדוגמת ארנקים אלקטרוניים למיניהם.

(ד) חדירה למטרת השגה של מידע פרטי בהיקף ניכר או השגה של מידע פרטי ורגיש, כגון מידע אינטימי, מידע על עברו המיני של אדם או מידע הנוגע לענייניו של קטין.

(ה) חדירה שנעשית עבור תשלום או במסגרת עיסוקו של החודר (לדוגמה אדם המציע שירותי איסוף מידע תמורת תשלום, ובפועל הוא חודר שלא כדין לחומרי מחשב לצורך איסוף המידע).

(ו) חדירה לחומרי מחשב ממניעים אידיאולוגיים ובמטרה לגרום נזק.

(ז) חדירה למאגרי מידע הכוללים מעל ל-10,000 רשומות של מידע אישי ומתחת ל-1,000,000 רשומות.

(ח) חדירה לחומר מחשב הנגרמת בעקבות חבירה מאורגנת של שני חשודים או יותר.

32. בגדר קטגוריית **המקרים הקלים** ייכללו המקרים שלא נכנסים לשתי הקטגוריות שפורטו לעיל, ככל שאין בהם נסיבות אחרות לחומרה.

33. קיימים בנוסף פרמטרים כלליים אשר עשויים להשפיע על המיקום של כל מקרה בתוך המדרג אליו הוא שייך, **ואף עשויים במקרים מסויימים להביא לשינוי ההתייחסות הראויה למקרה, וסייווגו במדרג אחר**. בין פרמטרים אלה ניתן לציין את הפרמטרים הבאים:

(א) מידת התחכום של מבצע העבירה, שימוש בכלים ייעודיים והתגברות על מנעולים טכנולוגיים מורכבים.

(ב) היקף המאמץ, המשאבים והזמן שהשקיע החודר בביצוע התוכנית העבריינית ובביצוע העבירות.

(ג) מידת הנזק הכלכלי הישיר או העקיף, על כל סוגיו, שנגרמה מהעבירה, לרבות הוצאות אבטחה, ירידת מוניטין, ירידת שער המנייה של חברה בורסאית שנחדרה, עלויות ביטוח וכדומה.

(ד) פוטנציאל הנזק שעלול היה להיגרם כתוצאה מהחדירה, אף אם בפועל לא נגרם, כיוון שהעבירה נחשפה מבעוד מועד, או שמבצע עבירת החדירה לא המשיך להשתמש במידע שהושג כתוצאה מהחדירה.

הנחיות פרקליט המדינה

הנחיה 2.38 - מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב

בהקשר זה יצוין, כי ככל שהרושם העולה מחומר החקירה הוא כי החדירה בוצעה למטרת הוכחת יכולת של החודר בלבד (למשל, כאשר עולה כי החודר לא נטל מידע רגיש בעקבות החדירה לחומר המחשב, לא מחק אותו או שינה אותו ונראה כי גם לא התכוון לעשות כן, ועולה כי מטרתו הייתה להפגין יכולות לפריצה למחשב בלבד), הרי שפוטנציאל הנזק שעלול היה להיגרם כתוצאה מהחדירה כאמור - יהיה נמוך. עם זאת, ייתכן שחדירה לחומר מחשב למטרת הוכחת יכולת בלבד, תסב בפועל נזקים עקיפים ואף במידה ניכרת, ובמקרה כזה יפעל הפרמטר שבס"ק (ג) לעיל לחובת הנאשם.

(ה) היקף ורגישות חומר המחשב שנחשף כתוצאה מהחדירה, מבחינת טיב הפגיעה בפרטיות, בסוד עסקי או כדומה.

(ו) כמות המחשבים שנחדרו ומספר נפגעי העבירה כתוצאה מהחדירה למחשבים (יצוין כי אין חפיפה בין כמות המחשבים הנחדרים לכמות נפגעי העבירה, שכן מחשב אחד יכול לכלול מידע בנוגע למספר אנשים, ולחלופין אדם אחד יכול להחזיק מספר מחשבים).

(ז) עמדת קורבן העברה ומידת הפגיעה הסובייקטיבית בו.

ח. התייעצות

34. בכל הנוגע לעבירה של חדירה לחומר מחשב יכולות להישמע טענות ייחודיות לעולם הסייבר, הן ביחס לשאלת התקיימות העבירה, והן ביחס למידת חומרתה. כך למשל עשוי החשוד להעלות טענה בדבר השתלטות מרחוק על מחשבו ופעולה מתוכו בידי אחר, טענה כי החשוד פעל למטרה טובה של חשיפת נקודות תורפה וחולשות, טענה לקיומה של פרצת אבטחה רחבה המאיינת את פליליות המעשה ועוד. בכל מקרה שמתעוררות שאלות בעקבות טענות אלה ואחרות, יש להיוועץ במחלקת הסייבר בפרקליטות המדינה.