בס"ד

**בפני הרכב הדיינים הנכבדים**

**אוניברסיטת בר אילן**

תיק מספר: 01/22

**בעניין**

**התובעת:** שמשית חברה לביטוח

מרח' אלנבי 26, תל אביב

טל: 03-7584553

**- נגד -**

**הנתבעת:** SIBI שירותי הגנת סייבר בע"מ

מרח' יהודה הלוי 5, תל אביב

טל: 03-7906222

**כתב הגנה**

**בית הדין הנכבד מתבקש לדחות מכל וכל את תביעתה של התובעת ולחייבה בתשלום הוצאות משפט ונזקי הנתבעת בגין התביעה, כדלהלן:**

**רקע עובדתי**

1. הנתבעת הינה חברה מובילה בשירותי הגנת סייבר.
2. הנתבעת מציעה את שירותיה באופן איכותי ומקצועי לפי טכנולוגיות הסייבר המובילות בעולם, תוך התאמה אישית לכל ארגון על פי צרכיו האישיים והתקציב. כל זאת תוך שמירה על פרטיות הלקוחות ועמידה בתקן ISO הבינלאומי.
3. לאור השירות המקצועי והמהימן אותו מציעה הנתבעת, הנתבעת הפכה לשם דבר בארץ ובעולם.
4. בתאריך 26.12.2020 התקשרה הנתבעת בחוזה עם חברת 'גלגלים' בע"מ (להלן: **"החברה"**) עבור מתן שירותיה למשך 5 שנים. החברה מפעילה קורקינטים שיתופיים במרחב גוש דן ולה אלפי לקוחות המשתמשים בקורקינטים בו זמנית.
5. על פי ההסכם בין הנתבעת לחברה, הנתבעת התחייבה להגן על שרתי החברה מפני חדירת האקרים, להעביר דו"חות אבטחה מקיפים באופן סדיר, לנטר אירועי סייבר בזמן אמת, להגיב באופן מהיר לנטרול האיום, וזאת במקצועיות מקסימלית, על פי אמצעי האבטחה המתקדמים ביותר בשוק הגנת הסייבר.
6. ביום 8.6.21 זיהו מהנדסי הסייבר של הנתבעת פריצת האקרים למערכת השליטה מרחוק של הקורקינטים בבעלות החברה.
7. מהנדס בכיר מטעם הנתבעת הופקד לטפל בבעיה, ותוך דקות ספורות הוא איתר את הפריצה בחומות ההגנה אשר אפשרה חדירה לליבת שרתי החברה, ונטרל את האיום.
8. ביום 1.2.22 פנתה התובעת לנתבעת ועדכנה אותה כי התקבלה במשרדיה תביעה בגין נזקי גוף ורכוש שנגרמו למר אוהד שור, אחד מלקוחות החברה (להלן: 'הלקוח') בזמן הקצר שבו הצליחו ההאקרים לקחת שליטה על מהירות הקורקינטים מרחוק, ולטענתה הנתבעת היא זו שנושאת באחריות בגין נזקים אלה.
9. התובעת פרטה באוזני הנתבעת את טענותיו של הלקוח, כפי שהם פורטו גם בכתב תביעתה שהוגש לבית הדין הנכבד.
10. הנתבעת מקבלת את גרסתו העובדתית של הלקוח באשר להשתלשלות האירועים אשר הובילה לפגיעתו ואת הערכת גובה הפיצוי בגין הנזקים שנגרמו לו, כפי שהועברו לה על ידי התובעת, שכן אין בידיה הכלים לחקור ולהפריך גרסה זו, ועל רקע החקירה שערכו חוקרי התובעת בנוגע להיקף הפגיעות וגובה הפיצויים.
11. יחד עם זאת, הנתבעת מכחישה בתוקף את הטענות בנוגע לרשלנותה ואת אחריותה לנזקי הלקוח.
12. הנתבעת אינה מכחישה את אחריותה להגן על החברה מפני תקיפות סייבר, אך טוענת כי הפריצה לשרתים לא נבעה מהתרשלותה.
13. הנתבעת גם מכחישה את מסקנותיו של ד"ר דני ארכיפלט אשר בדו"ח שסיפק לתובעת טען כי הנתבעת התרשלה בסיפוק ההגנה הנדרשת לשרתי החברה בכך שדו"ח ההגנה שסיפקה לנתבעת לחברה היה חלקי ולא הקיף את פרצת האבטחה בהתחברות לענן של החברה.
14. הנתבעת מספקת הגנה תמידית לכלל שרתי החברה, לרבות לענן החברה שם נמצאת מערכת הבקרה של הקורקינטים, ומספקת דו"חות תקופתיים כנדרש וכמקובל.
15. טרם הפריצה הנתבעת הגישה דו"ח מפורט לחברה על אבטחת כלל שרתיה. דו"ח זה היה מלא ומקיף והצביע על חומות הגנה חזקות דיין כדי למנוע פריצות האקרים רגילות.
16. הנתבעת אינה יכולה לשאת באחריות על פריצות האקרים החורגות מגדר האבטחה הרגילה והסבירה, ואין ביכולתה לחזות כל סוג של פריצה. היא מעניקה אבטחה ברמה הגבוהה ביותר ובכלים הטובים ביותר המצויים בידי מומחי הגנת סייבר בעולם, ומעבר לכך הדברים אינם בשליטתה.
17. יתרה מזו, בעת מתקפת הסייבר, הנתבעת פעלה, כאמור, באופן מיידי ועשתה כל יכולתה כדי לנטרל מתקפה זו תוך זמן קצר ביותר, תוך שימוש בכלים המתקדמים ביותר.
18. לחילופין, גם אם הייתה רשלנות מצד הנתבעת בדו"ח ההגנה שסיפקה לחברה, פריצת ההאקרים הייתה בלתי נמנעת ונבעה מפרצת אבטחה שכוסתה בדו"ח. משכך, הפריצה הייתה מתרחשת בכל מקרה ולא היה ניתן למנוע אותה.
19. **לאור כל האמור מוכחשת בתוקף הטענה כי הנתבעת התרשלה באבטחת שרתי החברה. הנתבעת אינה נושאת באחריות על נזקי התאונה שנגרמו ללקוח.**

**טענות משפטיות-הלכתיות**

**שומר שכר**

1. התובעת טוענת כי הנתבעת נחשבת 'שומרת שכר' לעניין ההגנה על שירותי הסייבר של החברה.
2. ראשית יובהר כי לא ניתן להגדיר את הנתבעת כשומרת שכר, שכן במקרה דנן הרכיבים עליהם היא נשכרה להגן (שרתים) כלל אינם נכסים אליבא דהלכתא היות שלא מדובר בנכס מוחשי אלא בנכס וירטואלי.
3. אולם גם אם יוכרע כי מדובר בנכסים ברי שמירה, וכי במסגרת חובותיה של הנתבעת כשומרת שכר, עליה לתת שירות טוב וראוי ביחס להגנה מפני מתקפות סייבר שונות בשרתי החברה, ואף הגנה גבוהה יותר מהנורמה המקובלת לאור העובדה כי היא מקבלת על כך תשלום כספי (פתחי חושן, ג, ב, סע' א-ב), הרי שהנתבעת עמדה בחובותיה כשומרת שכר בהפעילה חומות הגנה לפי תקן ISO הבינלאומי המחמיר ביותר ובמתן מענה מידי לפריצה.
4. לפיכך אף אם נגרם נזק לחברה או מי מעובדיה, הנתבעת פטורה מתשלום הוצאות הנזק לאור העובדה כי נתנה את השירות הטוב ביותר האפשרי לחברה (פתחי חושן, ג, ב, סע' כח).
5. בנוסף, הנתבעת תטען כי הפריצה לשרתי החברה, מוגדרת כאונס. אונס הינו מצב בו לשומר אין יכולת למנוע את הנזק בשעת מעשה, כאשר לא היה צפוי שהמאורע יקרה או שהיתה סבירות נמוכה לכך (הרב ברוך כהנא, דיני שומרים, עמ' 222). הנתבעת אומנם מעניקה שירותי סייבר מעולים בכל קנה מידה, אך לא ניתן לצפות כל סוג של התקפת סייבר.
6. מוכחשת טענת התובעת כי אונס רק חל במקרה של לסטים. כך לדוגמה, בעניין שמירת צאן על ידי רועה מציין השולחן ערוך כי אם שני זאבים טרפו את הצאן המקרה מוגדר כאונס (שו"ע חושן משפט סימן שג ס"ק ד). היינו, כאשר האיום נעשה באמצעות לפחות שני גורמים מאיימים מאוד, מדובר באונס.
7. יתר על כן, מציין השו"ע כי אם שלושה כלבים טרפו את הצאן, המקרה מוגדר כאונס. היינו, כאשר האיום נעשה באמצעות לפחות שלושה גורמים מאיימים פחות, מדובר באונס.
8. בהשוואה למתקפת הסייבר, זו נעשתה בידי קבוצת האקרים איראניים מיומנים ביותר, שמטרתם הינה פגיעה עוינת באזרחי מדינת ישראל. משכך מדובר בגורם מאיים מאוד ולכן הדבר הנחשב כאונס לפי השולחן ערוך והנתבעת פטורה מתשלום נזקי התאונה שנגרמו ללקוח.
9. שומר שכר אינו נושא באחריות לנזק שנגרם באונס (משפט החושן, ב, סימן כד; תוספות ב"מ, ע"א), אף אם היה יכול למנוע את הפגיעה (פתחי חושן, ג, ג, סע' יד). על כן הנתבעת אינה חייבת בתשלום נזקי התאונה שנגרמה מהתקיפה על שרתי החברה, בייחוד שאין בנמצא כל יכולת טכנולוגית למנוע אותה.
10. יתרה מזו, שומר שכר שניסה לעשות ככל יכולתו כדי למנוע את הנזק אך נחל אי הצלחה, פטור מתשלום הנזק, שכן גם מקרה זה מוגדר כאונס (שו"ע חושן משפט סימן שג ס"ק ה). הנתבעת הגנה על שרתי החברה טרם התאונה באמצעות ביקורת ודו"חות קבועים, וכן נתנה את המענה המהיר ביותר האפשרי בעת קרות פריצת האבטחה.
11. גם אם נקבל את הטענה שעל הנתבעת מוטלת חובת נטל הראיה, הדו"ח האחרון שהוגש על ידי הנתבעת לחברה, הראה כי כלל ההגנות תקינות וחזקות, ואין צורך בביצוע פעולה נוספת. למרות זאת, האקרים הצליחו לפרוץ את חומות ההגנה החזקות, ללא יכולת שליטה של הנתבעת.
12. השולחן ערוך מציין שבמקרה של אונס, אף אם פעולה בזמן אמת הייתה מונעת את הפגיעה, אין חזקת חיוב על הנזק שנגרם (שו"ע, חושן משפט, סימן שג, סעיף י). הנתבעת ניסתה, כאמור לצמצם ביותר את משכה ועוצמתה של פריצת ההאקרים לשרתי החברה בזמן מתקפת הסייבר, אך לצערה הלקוח נפגע טרם נבלמה הפריצה.
13. לחילופין, גם אם הנתבעת התרשלה בסיפוק ההגנה הנדרשת לשרתי החברה כפי שטוען ד"ר דני ארכיפלט, אין לחייב את הנתבעת בנזק שנגרם ללקוח. זאת משום ששומר שכר מחויב בפיצוי בגין הנזק רק אם נמנע מפעולה שהייתה יכולה למנוע את הנזק (ברוך כהנא, דיני שומרים, עמ' 234).
14. מטענת הרשלנות עולה כי הנתבעת לא דיווחה בדו"ח שלה על פרצת האבטחה, אך לא הוכח כי לו הייתה מדווחת על פרצה זו, היה בכך כדי להשפיע על תוצאות פריצה ההאקרים ולמנוע אותה. סביר יותר כי מתקפת הסיבר הייתה מתרחשת בכל מקרה, שכן מדובר באויב מדינתי עוין אשר בחר לתקוף את מדינת ישראל ואת השוק העסקי שלה. משכך, הנתבעת פטורה מתשלום הנזק.
15. מוכחשת טענת התובעת "תחילתו בפשיעה וסופו באונס, חייב". הנתבעת עמדה בחובתה וסיפקת את ההגנה המיטבית עבור החברה כאמור, ולכן "אין תחילתו בפשיעה".
16. מי שפשע במקרה זה אינה הנתבעת, אלא לכל היותר מדינת ישראל שלא סיפקה התראה מודיעינית מספקת לגבי כוונות תקיפה של אויב עוין, כדוגמת ההאקרים האיראניים הפועלים בשירות מדינת אויב. בהעדר התראה כזו, לא ניתן לצפות מהנתבעת לנקוט אמצעי זהירות יוצאי דופן.
17. מעבר לכך בשו"ת לחם רב (סימן קפ) ישנו דיון בפקיד של סוחר שטעה ברישום סחורה ששלח וכתב י"ג חבילות במקום ט"ו. עולה מפסיקתו שאין לחייב פועל כשומר בגרמא (נזק עקיף – וכפי שיפורט בהרחבה להלן) אלא כשהוא שומר על גוף הממון (פתחי חושן, נזיקין, פרק ג, סעיף כה).
18. במקרה שלנו הנתבעת לא מונתה להיות שומרת על הקורקינטים עצמם, אלא רק על השרתים, ולכן אין לחייבה בנזקי גרמא.
19. לאור כל האמור, בית הדין מתבקש לקבוע כי הנתבעת פטורה מאחריותה לנזק שנגרם ללקוח, גם אם יכריע כי היא מוגדרת כשומרת שכר.

**נזקי גרמא**

1. גם אם יקבע שהנתבעת התרשלה בשמירה על שרתי החברה, הרי שמדובר בנזקי גרמא.
2. במשנה (בבא קמא, נה ע"ב) נאמר: 'הכונס צאן לדיר ונעל בפניה כראוי, ויצאה והזיקה, פטור. לא נעל בפניה כראוי ויצאה והזיקה, חייב. **נפרצה בלילה או שפרצוה לסטים ויצאה והזיקה, פטור. הוציאוה לסטים לסטים חייבים'.**
3. אף אם אכן הנתבעת השאירה פרצה באבטחה כטענת הנתבעת, הרי שההאקרים הם שפרצו והם שהוציאו את המידע הרלוונטי שאפשר להם להשתלט על שרתי החברה, ולכן הנתבעת פטורה מכל חיוב נזיקי.
4. אם תטען התובעת כי מדובר בנזק מסוג גרמי אשר יש לחייב בגינו, תבהיר הנתבעת כי נפסק ברא"ש (שו"ת יז) שהחיוב בדין גרמי הינו רק כאשר האדם עושה בעצמו את ההיזק לממון חבירו, וכן כשהנזק ודאי ('ברי היזקא').
5. במקרה דנן הנתבעת לא עשתה בכוחות עצמה פעולה שגרמה לנזק, אלא לכל היותר התרשלה בשמירה, וכן הנזק לא היה וודאי, שכן הסיכוי שבזמן הקצר בו השתלטו ההאקרים על השרתים יתרחש נזק למי מהנוסעים בקורקינטים היה קלוש.
6. לפי זה אין גם לקבל את טענותיה של התובעת כי הנתבעת נחשבת 'שולחני' ו'שורף שטר חברו', שכן כל אלה חוסות תחת גדר 'דינא דגמרי' ומחייבות רק במקרים של פעולה אקטיבית ונזק וודאי, מה שלא קם בענייננו.
7. בייחוד נכון הדבר בנוגע לעיקר נתח הפיצוי הנוגע לאובדן רווחיו של הלקוח בגין חזרת המשקיעים מהנכונות להשקיע במיזם.
8. נפסק כי אובדן רווח (בניגוד להפסד) מוגדר כגרמא – דהיינו נזק עקיף שלא ניתן לחייב עליו, ולכן גם אם הדבר נבע מעטיה של הנתבעת, אין לחייבה. בעניין זה ראו את דברי המהר"ם (שו"ת, דפוס פראג, סימן תתכא) 'דין הוא דדיינינן דינא דגרמי, היינו במקום שמפסיד חברו על ידי גרימתו. אבל מקום שהיה יכול להרוויח, וגורם לו בגרימתו שאינו מרוויח – פטור'.
9. הנתבעת סיפקה שירותי הגנה המיטביים ודו"ח מקיף על מצב ההגנה על שרתי החברה כאמור, ולכן לא ניתן להגדירה כ'פורצת גדר' חזקה ובריאה.

**אחריות חברות ביטוח**

1. בשולי הדברים יוער כי, כאמור, בשל כך שמדובר בנזקי גרמא, למעשה גם חברת הביטוח – התובעת, אינה חבה בתשלום ללקוח, ואם הייתה פונה לבית דין הפוסק על פי ההלכה הייתה נפטרת מחבותה.
2. משום כך, אין לאפשר לה לגלגל על הנתבעת שיפוי על פיצוי שבהתנהלות משפטית זהירה ונכונה הייתה אף היא נמנעת ממנו.
3. אמנם מיעוט פוסקים, אותם ציינה התובעת, סוברים שלחברת ביטוח אחריות גם על נזקי גרמא מסויימים, מכח הסכם מכללא ודינא דמלכותא, אך מרבית הפוסקים אינם סוברים כך.
4. גם אליבא דמיעוט הפוסקים שסוברים כן, הרי שעמדתם חלה על חברות ביטוח בלבד, ולא על הנתבעת שאיננה חברת ביטוח, ולכן ההנחות האמורות המצויות בדברי פוסקים אלה, אינן חלות עליה.

**טענות מהמשפט הישראלי-אזרחי**

**דיני חוזים במשפט הישראלי**

1. הסכם ההתקשרות בין הצדדים כלל התחייבות של הנתבעת לתת שירותי הגנה מיטביים על שרתי החברה מפני מתקפות סייבר. ההסכם כלל חיוב על נזק שנגרם במקרה של פריצה שניתן היה לצפות באמצעים טכנולוגים המתקדמים שבידי הנתבעת, אך הוא לא כלל הסדר בגין חיוב על נזק שלא היה ניתן לצפות.
2. על פי סעיף 25(א) לחוק החוזים (חלק כללי) התש"ג-1973, פרשנות החוזה תהיה על פי אומד דעת הצדדים לפי המשתמע מהחוזה ומנסיבות העניין או לפי לשון החוזה. משלא נאמר במפורש בהסכם מהו ההסדר במקרה של תקיפה שלא היה ניתן לצפותה, יש לאמוד את דעת הצדדים.
3. על רקע התחכום הרב של האקרים אירניים, אשר מסתייעים בגיבוי ממשלתם, אין סביר כי הצדדים להסכם התכוונו לכסות גם תקיפה מעין זו בכלל החובות המוטלות על הנתבעת להגנה על המערכת. לפיכך אין לקבוע כי הנתבעת הפרה את מחויבותה על פי ההסכם.
4. בנוסף, על פי ס' 18(א) לחוק החוזים (תרופות בשל הפרת חוזה) התשל"א-1970 (להלן: "חוק התרופות), אם הפרת חוזה נבעה מנסיבות שהמפר לא צפה ולא היה יכול למנען וקיים קשר סיבתי בין האירוע לבין ההפרה, המפר פטור מתשלום פיצויים בגין נסיבות אלו.
5. ברע"א 3126/09 **שאול נאחוסי נ' שלומית סתוי** (נבו 20.2.10), בית המשפט מדגיש כי ס' 18 לחוק התרופות מעגן את 'דוקטרינת הסיכול', ומונה את המבחנים מצטברים שעמידה בהם פוטרת מאכיפת החוזה או ממתן פיצויים בגין ההפרה. בכדי להנות מהגנה זו, על הסיכול להיות בלתי ניתן לצפייה ולהיגרם עקב אירוע חיצוני.
6. כאמור, מוכחשת טענת ד"ר ארכיפלט בדבר פרצת אבטחה בענן החברה שלא מצאה ביטוי בדו"ח האבטחה של הנתבעת. הנתבעת סיפקה שירותי הגנה עקביים על כלל שרתי החברה, לרבות ענן החברה, היא דיווחה באופן מקיף על מצבה העדכני של האבטחה, וככל שידיעתה מגעת על פי האמצעים שבידה, לא היו קיימות פרצות אבטחה בעת מתקפת הסייבר.
7. מכאן, שהנתבעת לא הייתה יכולה לצפות שתתרחש מתקפת סייבר וכן לא יכלה למנוע פריצה זו, על אף האמצעים הטובים ביותר שעמדו לרשותה.
8. יתרה מזו, אף אם יחליט בית הדין הנכבד ליישם גישה מחמירה בדרישת הצפיות ולקבוע כי ניתן לצפות שאיראן תתקוף את מדינת ישראל בממד הסייבר, לא ניתן היה לצפות שאיראן תתקוף דווקא חברה שולית וקטנה כמו הנתבעת, שכן מדובר בחברה עסקית ולא בתשתית קריטית ממשלתית של מדינת ישראל.
9. יש לציין בהקשר זה, כי תקיפת סייבר על ידי מדינה או נציגיה, נחשבת ברף העליון של תקיפות הסייבר, כאשר הספקטרום נע בין יחידים, חברות מתחרות עסקיות, ארגוני טרור וגורמים אנרכיסטיים שונים. כאשר מדינה, כמו איראן, משקיעה את משאביה ביכולות סייבר מקצועי, הכלים בידיה הם עוצמתיים וכמות המשאבים המושקעת בכך היא אין-סופית לעומת כל חברה עסקית באשר היא, וקשה עד בלתי אפשרי לצפות ולתת מענה לסוג כזה של מתקפה.
10. לחילופין, גם אם תתקבל טענת ד"ר ארכיפלט בדו"ח שהציג, כי הנתבעת התרשלה ולא דיווחה בדו"ח על פרצת האבטחה, הרי שגם כך הנתבעת פטורה מתשלום הנזק שנגרם ללקוח לאור דוקטרינת הסיכול, שכן המתקפה הייתה מתרחשת בלאו הכי.
11. על פי ס' 10 לחוק התרופות, קבלת פיצויים עקב הפרת חוזה תעשה רק אם אכן נגרם נזק עקב ההפרה והמפר צפה מראש את הנזק (ע"א 355/80 **נתן אניסימוב בעמ נ' מלון טירת בת שבע בע"מ**, פד לה(2) 800).
12. במקרה דנן, לא הוכח שהנזק נגרם עקב הפרת החוזה דווקא, ויתכן כי גם לו הייתה הנתבעת מדווחת על פריצה האבטחה בדו"ח הפריצה הייתה מתרחשת בכל מקרה, שכן אין גבול לאופני הפריצה האפשריים שהאקרים מסוגלים להמציא ולהפעיל על המערכת.
13. לאור כל האמור עולה, כי גם בהיבט החוזי הנתבעת פטורה מתשלום עבור הנזקים שנגרמו ללקוח.

**דיני נזיקין במשפט הישראלי**

1. על פי סעיף 35 לפקודת הנזיקין, בכדי להקים עילת תביעה המבוססת על עוולת הרשלנות, נדרש להוכיח את יסודות העוולה במצטבר – חובת זהירות, הפרת חובת הזהירות על ידי התרשלות, וקיום קשר סיבתי בין ההתרשלות לבין הנזק שנגרם. במקרה הנדון יסודות עוולת הרשלנות לא מתגבשים לכדי עילה לתביעה כלפי חברת "SIBI" הנתבעת.
2. הנתבעת לא הפרה את **חובת הזהירות** המוטלת עליה מכח החוזה בין הצדדים שכן לא יכלה לצפות את הנזק הספציפי, שנגרם ללקוח בהיותו יזם סטרט-אפ בדרכו לפגישת גיוס משקיעים. הנתבעת, בהיותה ספקית שירותי הגנה בסייבר וחברה טכנולוגית לכל דבר, לא יכלה לצפות את התרחיש הספציפי הזה, אשר מהווה מקרה חריג ובודד, שהסיכויים שיתרחש קלושים.
3. זאת ועוד, הנתבעת לא מחזיקה באחריות להגנה על ציוד הקצה של החברה, כמו הקורקינטים. על חברת "גלגלים" ויצרן הקורקינט שלה חלה האחריות על לוודא את בטיחותו של ציוד הקצה.
4. הנתבעת אף **לא התרשלה** בתפקידה, אלא פעלה במקצועיות וללא דופי למתן השירות המיטבי ללקוחותיה.
5. למרות פעילותה המקצועית ללא רבב של הנתבעת, הפריצה למרבה הצער אכן התרחשה וזאת משום שמדובר בתקיפת סייבר, אשר מאפייניה מעידים, כאמור, כי היא ככל הנראה בוצעה בידי קבוצת האקרים אירנים הנתמכים על ידי איראן עצמה, ולא בידי האקר מזדמן והמטרה הייתה פגיעה פיזית באדם, בצורה עוינת.
6. ישות מדינתית כמו איראן, מחזיקה בידיה אמצעים, אשר מהווים כלים "שוברי שוויון" בתחום הסייבר. האחריות במקרים של תקיפות בין מדינתיות חלה כאמור, על המדינה, שבאחריותה לספק התרעה מקדימה, מניעה ושיבוש של התקיפה. כפועל יוצא מכך, הנתבעת מצדה סיפקה את הכלים להתמודדות סבירה עם תקיפות סייבר ולא אל מול תקיפות המהוות זרוע ארוכה של מדינה עוינת.
7. עוד יודגש, כי בבואנו לבחון את סוגיית איומי הסייבר והסכנות הנובעות מהם, יש לציין כי הם כוללים מידה רבה של **אי-ודאות ומורכבות**. אי הודאות באה לידי ביטוי בחוסר היכולת ליצור מודלים הסתברותיים להערכת הסיכוי להתממשות הסיכון ולהערכת חומרתו של הנזק. בשונה מסיכונים המוגדרים "פשוטים", המוסברים על ידי מודלים של סיבה ותוצאה (למשל תאונות דרכים), סיכוני הסייבר אינם ניתנים להפשטה על ידי מודל הסתברותי ויש אי ודאות באשר למועד הופעתם.
8. נוסף על כך, נזק עקב פגיעה במערכות במרחב הסייבר יכולה להיות כתוצאה מגורמים מגוונים: מטעות אנוש, דרך הגדרות מערכות שאינה תואמת את איום הייחוס ועד לפגיעות בתשתית התוכנה או החומרה. קשה להעריך מראש את השלכותיה של פגיעת סייבר ולכמת את רמת ההגנה הראויה המבטיחה את צמצום הסיכונים במרחב.
9. על רקע כל זאת, יש לקבוע כי הנתבעת העניקה את הגנת הסייבר המקסימלית האפשרית, אל מול שלל האיומים, ובשימוש במערכות, בתכנות ובציוד המתקדם ביותר.
10. יש לקבוע גם כי המקרה הנדון לא עומד ב**מבחן הקשר הסיבתי המשפטי.** בע"א 1639/01 **קיבוץ מעגן מיכאל נ' קרישוב,** פ"ד נח(5) 215 נקבע: "**גורם הכרחי לאירוע משמעו שבלעדי אותו גורם לא היה האירוע מתרחש. תפקידו של הקשר הסיבתי המשפטי הוא לצמצם את המקרים שבהם יוכר קשר סיבתי לאור המטרה של קביעת הקשר הסיבתי במשפט, שהיא הטלת אחריות על אדם (אנגלרד). הקשר הסיבתי המשפטי יוכר רק בדין אותם גורמים עובדתיים שיש הצדקה לחייב אדם באחריות נזיקית בגינם".**
11. לא הוכח שאי הצבעה על פרצה ספציפית בדו"ח שהועבר לחברה מאת הנתבעת, הוא אשר גרם לפריצת ההאקרים. המורכבות הטכנולוגית של הפריצה היא כזו, שלא די בחוות דעתו של המומחה ארכיפלט בכדי להצביע בוודאות על גורמיה. לו הייתה ניתנת לנתבעת ההזדמנות לבדוק את המערכת באופן יסודי, טרם נותקה ממנו בעתיה של הנתבעת, היא הייתה יכולה להצביע על שלל גורמים נוספים שהתרחשו בעת הפריצה ולא היו בשליטתה של הנתבעת שהיו יכולים אף הם להוות גורמים לפריצה.
12. לא מן הנמנע גם, כי לתובעת היה אשם תורם להתרחשות הפריצה והנזק שחוללה, בשל אי יישום המלצותיה של הנתבעת בדו"ח שהעבירה לה, או הפרת אחד או יותר מכללי ההתנהלות המחויבים לצורך מניעת פריצות מעין אלה, כמו פתיחת דוא"ל חשוד על ידי אחד מעובדיה, וכדו'. בהעדר הזדמנות לנתבעת לחקור ולוודא זאת כאמור, לא ניתן לקבוע בוודאות כי הפריצה התרחשה בעתיה, ולהשית עליה את האחריות לקרות הנזק.
13. **לאור האמור לעיל, מוכח מעבר לכל ספק שעוולת הרשלנות לא מתקיימת במקרה הנדון ואין הנתבעת אחראית לנזקים שנגרמו, זאת בשל אי הצטברות התנאים לקיום עוולת הרשלנות**.

**חוק המחשבים**

1. חוק המחשבים תשנ"ה-1995 קובע (סעיף 7) כי 'הפרעה שלא כדין לשימוש במחשב או בחומר מחשב, בכל דרך שהיא....' מהווה עוולה נזיקית.
2. ההאקרים הם אשר נקטו פעולה מפריעה, ואילו הנתבעת לא נקטה בכל פעולה שכזו, אלא להיפך – עשתה כל אשר אל ידה על מנת למנוע פעולות כאלה, ומשום כך אין כל מקום להחיל עליה את העוולות המנויות בחוק זה.
3. אין ספק כי חוק המחשבים עוסק בפריצה ובפגיעה ישירה במחשבים, ומופנה כלפי הפורצים עצמם. טענותיה של התובעת המבקשים להרחיב את העוולה על פי חוק זה גם אל חברות הסייבר בטענה ש'פעולה' כוללת גם מחדל אבטחה, הינן מופרכות מעיקרן.
4. בנוסף, ככל עוולה נזיקית, הוכח כבר כי לא מתקיימים יסודות העוולה, ולכן הם אינם עולים גם לפי חוק המחשבים.

**משפט משווה**

1. פרשת Wengui v. Clark Hill Law Firm עוסקת בתביעה של וונגי - איש עסקים ופליט סיני כנגד פירמת עורכי דין ידועה בארה"ב. הטענה הייתה כי הרשויות הסיניות פרצו לפירמה וגנבו מידע אודות וונגי. בית המשפט המחוזי של ארה"ב, במחוז קולומביה, קבע כי ניתן היה לצפות את הפריצה למערכות המידע והטיל אחריות נזיקית על הפירמה.
2. אולם במקרה שלנו, אין המדובר בגניבת מידע, אלא בהשתלטות על ציוד קצה של החברה, והשתלטות כזו לא ניתן לצפות, כפי שנטען בהרחבה לעיל.
3. לפי מדריך טאלין 2.0 (מדריך רשמי של נאט"ו, הבוחן כיצד ניתן להחיל את המשפט הבין-לאומי על מרחב הסייבר) על מוסדות המדינה מוטלת החובה לנקוט פעולות סבירות העומדות לרשותן כדי שלא לאפשר בשטחן פעולות סייבר מזיקות הננקטות על ידי אורגנים של מדינה אחרת.
4. כך גם במקרה שלנו, על המדינה חלה כאמור, האחריות לספק לגופים פרטיים, ובכללם החברה דנן, הגנה סבירה כנגד פעולות טרור בין מדינתיות המתרחשות בטריטוריה הישראלית, ואין להשית את האחריות בגין כך על הנתבעת.

**סוף דבר**

1. יש לזכור שאנו חיים במציאות גיאו-פוליטית מורכבת שבה מדינות עוינות לישראל, המצוידות ביכולות לביצוע תקיפות סייבר מתקדמות, לא מהססות להפעיל יכולות אלה מול חברות בישראל. ההוכחה לכך היא שבמהלך השנתיים האחרונות הותקפו ונפרצו מאות חברות בישראל.
2. חברת "גלגלים בע"מ" נפלה קורבן לאירוע טרור חמור. מדובר באירוע המהווה חלק מקמפיין מתקפות שמקורו באיראן, שמטרתו זריעת פחד וכניעה במדינת ישראל. כאמור, מטבע הדברים, היכולת להתגונן מפני תקיפה כזו על ידי חברת סייבר פרטית מוגבלת. כאשר מדינה או גורמים מטעמה משקיעים זמן בתקיפה אזרחית שלא נהדפת באמצעות מודיעין מסכל, מערכת ביטחון שמספקת התראה מוקדמת או מטריית הגנה מדינית, נוצרת א-סימטריה מובנית לטובת יכולתו של הגוף התוקף לעומת יכולותיו של הגוף הנתקף. לאור כל זאת לא ניתן לצפות מהנתבעת לספק יכולות שהמדינה עצמה לא תמיד מספקת במקרים מעין אלה.

**הסעד המבוקש**

**לאור כל האמור לעיל, בית הדין הנכבד מתבקש:**

1. לדחות את התביעה.
2. לחייב את התובעת בפיצויים בגין הפגיעה בשמה הטוב ובגין עוגמת הנפש הרבה שגרמה התביעה לנתבעת.
3. להשית על התובעת את הוצאות המשפט ושכר טרחת עורכי-הדין של הנתבעת.
4. מן הדין ומן הצדק להיענות לבקשותיה אלה של הנתבעת.

**\_\_\_\_\_\_\_\_\_\_\_**

**הנתבעת**