



# לשלים או לא לשלים (כופרה) זאת לא השאלה

תשלום כופרה במתקפות סייבר כהוצאה מוכרת לצרכי מס

מחברים:

עו"ד יעקב עוז עו"ד סיגל אבירם פרופסור אמיר חורי  
עו"ד דני לייבוויץ שטי מהנדס יובל שגב

# לשלם או לא לשלם (כופרה) זאת לא השאלה

תשלום כופרה כהוצאה מוכרת לצרכי מס

## פתח דבר

שלמי תודה לחברי וחברותי שנעתרו לבקשתי והצטרפו אלי לכתיבת חיבור ראשוני זה.

תודה והערכה רבה לפרופסור אמיר חורי, לעו"ד וליוע"מ וחשבונאית סיגל אבירם, למר יובל שגב ועו"ד דנית ליבוביץ שטי.

תשלום כופרה, טרור הסייבר, הסחיטה הכפולה, הפגיעה בפרטיות ומידע אישי ורגיש, התמודדות הרשויות, הארגונים, והחברות ועסקים מעסיקים אותי זמן רב.

הידיעה של משלם הכופרה כי עשה כל שלאיל ידו כדי לפעול על פי הנחיות המחוקק והרגולטורים ובסופו של יום אין ההוצאה הבלתי נמנעת הזאת אינה מותרת בניכוי, יכולים לפגוע באינטרס המוגן שהינו שימור האינטרס המשותף למשלם ולמדינה – המשכיות עסקית המגלמת בתוכה את קידום הפעילות היצרנית במשק, הכנסות, תשלום לכל המשתתפים – המדינה בגביית מיסים, מועסקות ומועסקים מקבלי שכר, ספקים יועצים ועוד.

החיבור ינסה להתמודד עם סימני השאלה, האתגרים היתרונות והחסרונות שבהכרתו של תשלום כופרה כהוצאה המותרת בניכוי.

בשם חברי, חברותי ובשמי הנכם. מוזמנות ומוזמנים להגיב להעיר ולהאיר כמו גם להציע תוספת שתאיר זוויות נוספות לקידום השיח בנושא חשוב זה.

קריאה מהנה.

שלכם,

יעקב עוז

"הידיעה של משלם  
הכופרה כי עשה כל  
שלאיל ידו כדי לפעול על  
פי הנחיות המחוקק  
והרגולטורים ובסופו של  
יום אין ההוצאה הבלתי  
נמנעת הזאת אינה  
מותרת בניכוי, יכולים  
לפגוע באינטרס המוגן  
שהינו שימור האינטרס  
המשותף למשלם  
ולמדינה – המשכיות  
עסקית המגלמת בתוכה  
את קידום הפעילות  
היצרנית במשק, הכנסות,  
תשלום לכל המשתתפים  
– המדינה בגביית  
מיסים, מועסקות  
ומועסקים מקבלי שכר,  
ספקים יועצים ועוד".

## תוכן עניינים

1	פתח דבר
4	מבוא
5	הצידוקים להכרה בתשלום כופרה בשל אירוע סייבר כהוצאה מוכרת
5	רגולציה של אבטחת מידע
6	דו"ח צוות המשנה לוועדת דזידי
7	"שומרי הסף" באבטחת המידע שבדין
8	דגשים מחוק הגנת הפרטיות
8	דגשים מהתקנות
9	תסקיר השפעת הפרטיות
	פערי ידע ומוטיבציה בין נקודת המבט הלאומית לנקודת המבט של הארגון הנתקף היקר
10	התופעה
10	דו"ח מבקר המדינה
11	תשלום דמי הכופרה
12	מדיניות "איסור תשלום" במדינות שונות
14	ניתוח משמעויות "הכרה" בחלופת תשלום דמי הכופרה
15	היבטים נוספים
16	אישור פורנזי – הפרמטרים הטכניים
20	סקירה נורמטיבית של ניכוי הוצאות לצורכי מס
20	הכרה בתשלומי כופרה כהוצאה עסקית
20	מבוא לניכוי הוצאות
20	הוצאה עסקית
21	בין הוצאה פירותית להונית
22	הוצאה לא חוקית, ניכויים שאין להתירם
22	תשלומים לא חוקיים
23	שוחד
23	תשלומי הגנה
24	סחיטה

24.....	כופרה.....
24.....	ניתוח השוואתי.....
24.....	מוטיבציה.....
24.....	כפייה ואיומים.....
25.....	השלכות משפטיות.....
25.....	יישום התרת ניכוי הוצאת תשלומי כופרה.....
25.....	הוצאות רגילות והכרחיות.....
25.....	הפחתת הפסדים.....
26.....	שיקולים רגולטוריים.....
27.....	סיכום.....
27.....	הקריטריונים לקביעת הכרה בהוצאות תשלום כופרה לצרכי מס.....
27.....	ניתוח השלכות ההכרה בתשלום כופרה כהוצאה מוכרת על אוצר המדינה.....
27	התנאים המקדימים להכרה ב הכרה בתשלום כופרה כהוצאה מוכרת על אוצר המדינה
29.....	סוף דבר.....

הפעילות העסקית ואחסון נתונים עסקיים ופרטי מידע במרחב הדיגיטלי מתרחבת. זו הדרך העיקרית כיום שבו נאגר ונשמר מידע. מאגרים אלו, בשל רגישותם, הפכו למטרה בידי גורמים שונים ואנו עדים להתרחבות מתמדת של אירועי סייבר אשר פוגעים או עלולים לפגוע בפעילות זו ובנתונים הנאגרים. לצד התרחבות התופעה של אירועי סייבר מתרחבת גם התופעה שלפיה בעלי פעילות עסקית ומאגרי מידע נדרשים לשלם כופר על מנת לחלץ מידע עסקי ומאגרי מידע אשר נפלו שלא כדין לידי צדדים שלישיים.

העסקים משלמים כופרה לא מתוך כניעה אלא מתוך ניסיון של צמצום והקטנת נזקים. נזקים אלו כוללים לא רק נזקים פרטיים של העסק הנפגע אלא גם נזקים ברמת המקרו כגון הפגיעה באמון של האזרחים כולם במגזר העסקי בישראל. ואכן, תשלום כופרה במקרה כזה נועד להציל עסק מאיבוד נתונים או מחשיפת נתונים אשר פוגע בציבור, וכן חושף עסקים לתביעות במישור דיני הפרטיות ודיני הנזיקין. מבחינה זו, הכופרה המשלום בגין המידע העסקי ומאגרי מידע נועד לשמר פעילות עסקית תקינה של עסק ושמירה על אינטרסים ציבוריים.

הנה כי כן, תשלום הכופרה בשל אירוע סייבר, מהווה למעשה מהלך מתחייב השקול להשקעה בנכס מניב (העסק) לשם המשך תפקודו בצורה נאותה. לפיכך, אך הגיוני הוא שתשלום הכופרה ייחשב כהוצאה מוכרת לצרכי מס, והכל בתנאי שהמשלם עמד במספר תנאים מקדימים לרבות פעולות אקטיביות לשמירה על נכסי ומאגרי המידע על פי דרישות הדין. דבר זה ישפר את רמת ההגנה על מידע ורמת השמירה של עסקים על פרטיות לקוחותיהם, וכן יחזק את מעמדם של עסקים בארץ בעיני שותפים בינלאומיים ולקוחות בחו"ל המבינים מתוך כך שהעסק עושה כל אשר לאל ידיו להגן על פרטיות המידע הנוגע להם והמוחזק על ידו.

אמנם, ההכרה צפויה להטיל נטל על קופת המדינה, ואולם, נראה שהתועלת בצידה של ההכרה, עולה באופן משמעותי, (הן ברמת המקרו והן ברמת המיקרו), על הנטל הצפוי.

ואכן, בנוסף לכל האמור לעיל, קיימם מספר צידוקים להכרה בתשלום כופרה במקרה של אירועי סייבר כהוצאה מוכרת לצרכי מס. להלן רשימה של הצידוקים שאינה בהכרח רשימה סגורה.

## הצידוקים להכרה בתשלום כופרה בשל אירוע סייבר כהוצאה מוכרת

הפעילות העסקית ואחסון נתונים עסקיים ופרטי מידע במרחב הדיגיטלי מתרחבת. זו הדרך העיקרית כיום שבו נאגר ונשמר מידע. מאגרים אלו, בשל רגישותם, הפכו למטרה בידי גורמים שונים ואנו עדים להתרחבות מתמדת של אירועי סייבר אשר פוגעים או עלולים לפגוע בפעילות זו ובנתונים הנאגרים. לצד התרחבות התופעה של אירועי סייבר מתרחבת גם התופעה שלפיה בעלי פעילות עסקית ומאגרי מידע נדרשים לשלם כופרה על מנת לחלץ מידע עסקי ומאגרי מידע אשר נפלו שלא כדין לידי צדדים שלישיים.

העסקים משלמים כופרה לא מתוך כניעה אלא מתוך ניסיון של צמצום והקטנת נזקים. נזקים אלו כוללים לא רק נזקים פרטיים של העסק הנפגע אלא גם נזקים ברמת המקרו כגון הפגיעה באמון של האזרחים כולם במגזר העסקי בישראל. ואכן, תשלום כופרה במקרה כזה נועד להציל עסק מאיבוד נתונים או מחשיפת נתונים אשר פוגע בציבור, וכן חושף עסקים לתביעות במישור דיני הפרטיות ודיני נזיקין. מבחינה זו, הכופרה המשולם בגין המידע העסקי ומאגרי מידע נועד לשמר פעילות עסקית תקינה של עסק ושמירה על אינטרסים ציבוריים.

הנה כי כן, תשלום הכופרה בשל אירוע סייבר, מהווה למעשה מהלך מתחייב השקול להשקעה בנכס מניב (העסק) על מנת שימשיך לתפקד בצורה נאותה. לפיכך אך הגיוני הוא שתשלום הכופרה ייחשב כהוצאה מוכרת לצרכי מס.

## רגולציה של אבטחת מידע

מידע אישי ומידע רגיש כהגדרתם בחוק הגנת הפרטיות, התשמ"א – 1981 (להלן: החוק) משמשים מושא למרבית מתקפות הסייבר – מתקפות כופרה בארץ ובעולם.<sup>1</sup> מידע זה זכה לכינויים רבים ביניהם "המטבע החדש העובר לסוחר", "הנפט החדש" או "הזהב השקוף".<sup>2</sup>

דיני הגנת הפרטיות ורגולציית אבטחת המידע בישראל, מוסדרים באופן חלקי במספר דברי חקיקה: החל בזכות חוקתית לפרטיות המעוגנת בחוק יסוד,<sup>3</sup> עובר דרך חקיקה ראשית,<sup>4</sup> חקיקת משנה

<sup>1</sup> מתקפות כופרה (Ransomware): "כופרה" היא סוג של נזקה שמטרתה הדבקת מחשב (או רשת מחשבים) של הקורבן, לטובת הצפנתו (נעילתו) או הצפנת הקבצים המאוחסנים בו. לאחר תופעת מתקפות הכופרה, דורש התוקף העברת תשלום כופר כתנאי לפתיחת ההצפנה.  
<sup>2</sup> פרופסור אמיר חורי, מתוך פרסום (פוסט) במדיה החברתית לינקאדין, וכמבוא לפרויקט מחקר מתהווה בתחום.

<sup>3</sup> חוק יסוד: כבוד האדם וחירותו, סעיף 7  
<sup>4</sup> חוק הגנת הפרטיות, התשמ"א – 1981

שהמרכזית בהן עוסקת באבטחת מידע,<sup>5</sup> הנחיות רגולציה ופסיקת בתי המשפט בנושאי פרטיות- שעד כה אינה רבה היא, מבחינה הלכתית. יחד עם זאת, חקיקת הפרטיות ואבטחת המידע בישראל מתפתחת. כך, תיקון חוק הגנת הפרטיות שעבר בקריאה ראשונה צפוי להתקבל בקרוב (לאחר שנים רבות) בקריאה שניה ושלישית.<sup>6</sup> כמו כן, כבר בקרוב יונח תיקון נוסף מקיף וכולל יותר, התואם יותר את הדין הבינ"ל בדגש על המוביל שביניהם ה- GDPR<sup>7</sup> תקנות שהותקנו ב- 2016 ונכנסו לתוקפן ב- 2018. יצוין כי בזמן הקורונה, 2020-2022, מתקפות הסייבר ודרישות הכופרה התגברו בישראל כמו גם בעולם כולו. בעקבות כך, חברות וארגונים רבים עשו ועושים כל שביכולתם על מנת לאבטח ולשמור את המידע מחד ולאפשר משטר העברת מידע ושימוש בו באמצעות נורמות, חקיקה וכללים המהווים שפה מוסכמת – טכנולוגית חדשה, מאידך.

### דו"ח צוות המשנה לוועדת דויד

ביום 7.12.2021, הורה מנכ"ל משרד המשפטים דאז עו"ד ערן דויד, על הקמת צוות משנה לוועדה להתאמת המשפט לאתגרי החדשנות ולהאצת הטכנולוגיה. צוות המשנה נועד לשם עיסוק באבחון הבעיות ויצירת דרכי טיפול בנושא פשיעה והונאות במרחב הדיגיטלי, זאת מתוך הכרה בחשיבות הנושא ומאפייניו הייחודיים.

הוועדה סקרה את הדין הנוהג בישראל ובמספר מדינות בעולם. כבר עתה יודגש, כי בדומה למצב במרבית המדינות שנסקרו בדו"ח, אין בישראל נורמה משפטית ייחודית לעניין תשלום כופרה במסגרת מתקפת כופרה. לצד זאת, ייתכן כי בנסיבות מסוימות תשלום הכופרה יעלה לכדי עבירות פליליות כמתן שירות או העמדת אמצעים לארגון טרור, עבירה לפי סעיף 23 לחוק המאבק בטרור, התשע"ו-2016 (להלן: "חוק המאבק או עבירה של פעולה ברכוש טרור לפי סעיף 32(א) לחוק המאבק בטרור; בטרור"); הפרת חובת דיווח לפי סעיף 33 ביחד עם סעיף 36 לחוק המאבק בטרור; עבירה של מימון פעילות של ארגון פשיעה לפי סעיף 2(א)(1) לחוק המאבק בארגוני פשיעה, התשס"ג-2003; או עבירות מסוימות על חוק איסור הלבנת הון, התש"ס-2000 (להלן: "חוק איסור הלבנת הון") וזאת, כתלות, בין היתר, בזהות הגורם לו מועבר התשלום ובאופן העברת התשלום.

<sup>5</sup> תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן: תקנות או תקנות אבטחת מידע)  
<sup>6</sup> הצעת תיקון (14) בחוק הגנת הפרטיות התשפ"ג – 2023 ותיקון 15 שטרם הונח בפני הכנסת.

ואכן, בשנים האחרונות אירעו מספר מתקפות סייבר מתוקשרות בישראל<sup>8</sup> שתכליתן הצפנת מיזע ודרישת כופרה, בהן התוקפים או ליתר דיוק "קבוצות התקיפה" לא נענו בשל חשד כי הגורמים התוקפים עונים להגדרת הישויות דלעיל.

וכאן ראוי לשאול: מה מעמדו של תשלום לגורם שאינו מוזכר לעיל והאם תשלום זה מותר בניכוי?

הואיל וזוהי השאלה המרכזית בחיבור זה, עוד בטרם נשיב עליה, נניח להלן רשימה חלקית של החובות החלות על בעלי, מנהלי, מחזיקי או בעלי הרשאת גישה למאגרי מידע, ואשר תוצאת אי קיומן של חובות אלו יכולה להוות הפרה ועוולה אזרחית,<sup>9</sup> וכן ישנם סעיפים בחוק שהמפר אותם יחשב כעובר עבירה פלילית.<sup>10</sup> בנוסף, קיימות הנחיות רגולטוריות מגזריים וגורמים מנחים שבמרבית המקרים באות בנוסף לדרישות החוק והתקנות ולא במקומן.<sup>11</sup>

### "שומרי הסף" באבטחת המידע שבדין

הרגולטור – הרשות להגנת הפרטיות במשרד המשפטים (להלן: הרשות), הינה הגורם המרכזי בתחום הגנת הפרטיות ואבטחת המידע אשר לו מוקנות סמכויות האכיפה בחוק. ברשימת הרגולטורים הנוספים לרשות ניתן למצוא את המפקח על שוק ההון, המפקח על הבנקים, משרד הבריאות ומערך הסייבר הלאומי בהיותו הגורם המנחה לתשתיות הקריטיות ומשרדי הממשלה.

להלן מספר דוגמאות מהוראות החוק, התקנות והנחיות הרשות, שהמקיים אותן עשוי להיחשב כמי שסייע ב"צמצום משטח תקיפה" לפי מתודת הסייבר או למקטין הנזק הטוב ביותר בתורת הנזיקין.

<sup>8</sup> ר' לדוג. פרשת שירביט 2020, "אטרף" 2021, הלל יפה 2021, הטכניון 2023.  
<sup>9</sup> ה.ש. 4, סעיף 4.

<sup>10</sup> ה.ש. 4, סעיפים 5,16,31

<sup>11</sup> רשות שוק ההון, ביטוח וחיסכון, המפקח על הבנקים, חוזרי מנכ"ל משרדי ממשלה, מערך הסייבר הלאומי ועוד.



**חובת רישום מאגרי מידע** – ישראל נמנית עם מספר מדינות שעדיין קיימת בהן החובה לרשום מאגרי מידע,<sup>12</sup> בעצם פעולת הרישום, בעלי מאגר מידע מדווחים אודות מידע שנאסף בעניין לקוחות, עובדים, ספקים, כמו גם את מטרות האיסוף ולאיזה צדדים שלישיים המידע מועבר. דע עקא, חובה זו אמורה להצטמצם ואולי אף להתבטל במסגר תיקוני החקיקה הצפויים.

**חובת מינוי ממונה אבטחת מידע** – החוק ומספר חוקים נוספים מחייבים גופים מסוימים למנות ממונה אבטחת מידע,<sup>13</sup> תפקידו של הממונה מוגדר בתקנות<sup>14</sup> ומחוקק המשנה בתקנה זו, מגדיר את כפיפותו למנהל המאגר או לנושא משרה בכיר אחר. במרכז תפקידו של הממונה עומדת חובת הכנת תכנית עבודה ובקרה ולטובת כך קובע מחוקק המשנה שעל בעל המאגר להקצות לממונה את המשאבים הדרושים לצורך ביצוע תפקידו.

**מינוי ממונה הגנת הפרטיות** – הגם שחובה זו אינה קיימת בדברי חקיקה רבים, הרשות להגנת הפרטיות מעודדת מינוי זה, ואכן גופים רבים מעסיקים ממונה הגנת הפרטיות. יצוין כי בתיקוני החקיקה הצפויים להתקבל בישראל, חובה זו תורחב לגופים רבים. מינוי ממונה הגנת פרטיות, אם כך, הופך ל Best Practice המגובה בהמלצת הרגולטור האמון על הפרטיות בישראל, מקובל במדינות רבות בעולם ולפיכך, אי מינוי כזה עלול להיחשב אי מיצוי אמצעי ההגנה המיטביים והמקובלים.

#### דגשים מהתקנות

**חובת קיום תקנות אבטחת מידע** – תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן: התקנות) מסווגות מאגרי מידע ב-4 רמות אבטחה: מאגר ברמת אבטחה של יחיד, אבטחה בסיסית, בינונית וגבוהה. החובות החלות על כל רמת אבטחה קבועות בתקנה 21; ההבדלים בין הרמות מושפעים בין היתר מזהות הגוף שהינו בעל מאגר המידע, מסוג המידע, מספר האנשים בהם עוסק המידע ומספר בעלי הרשאת גישה למידע.<sup>15</sup> בין כלל החובות בהתאם לרמת האבטחה שבתקנות, ישנן כאלה המבוצעות באופן חד פעמי וישנן המעודכנות באופן שוטף ועיתי ובצידן עלויות כספיות. התקנות מחייבות, בהתאם לרמת האבטחה ביצוע פעולות שונות הכוללות, הגדרות למאגר, כתיבת נוהל אבטחה כללי שיעסוק באבטחה פיזית וסביבתית, ביצוע מיפוי מערכות המאגר, ביצוע סקרי

<sup>12</sup> ה.ש. 4, סעיף 8

<sup>13</sup> ה.ש. 4, סעיף 17

<sup>14</sup> ה.ש. 5, תקנה 3

<sup>15</sup> ה.ש. 4, תקנה 21, התוספת הראשונה והשנייה.

סיכונים, הדרכות כוח-אדם, נוהל הקצאת סיסמאות והרשאות, בקרת גישה, תיעוד וביצוע ביקורות פנימיות.

### **חובת דיווח מידי**

כל בעלי המאגרים, בכל הרמות חייבים בתיעוד אירועי אבטחת מידע, בקרות אירוע אבטחה חמור כהגדרתו<sup>16</sup> בעלי המאגרים ברמת אבטחה בינונית וגבוהה חייבים הן בתיעוד, כאמור לעיל והן בדיווח מידי לרשות.

### **תסקיר השפעת הפרטיות**

באוגוסט 2021, פרסמה הרשות להערות הציבור טיוטת מדריך ובו המלצות כיצד לבצע תסקיר.

תסקיר השפעה על פרטיות (Assessment Impact Privacy), המכונה לעיתים "תסקיר השפעה על הגנת מידע" (Assessment Impact Protection Data) (להלן: "התסקיר") מתאר תהליך אשר נועד לסייע לארגון באיתור, הערכה וניהול סיכונים בתחום הפרטיות בפרויקטים או בפעילויות עסקיות וארגוניות אחרות הכוללות עיבוד מידע אישי.

ההערכה היא כי תסקיר זה יובא לאישור הכנסת במסגרת תיקון 15 לחוק כחובה, כפי שנהוג במדינות באירופה, בהן אבטחת המידע עיבוד המידע והגנתו מעוגנים בתקנות ה-GDPR.

יודגש כי בסמכותו של ראש הרשות להגנת הפרטיות בשבתו כרשם מאגרי המידע, להעניק פטור או הקלה במסגרת "הנחיות רשם" מקיום כל או חלק מהתקנות, או לחילופין, להחיל ההוראות כולן או חלקן על מאגר מסוים.<sup>17</sup> אנו סבורים כי קיומן של הוראות הרגולציה השונות עשויות לתרום רבות לצמצום היקף התקיפות, וכן למנוע הקטנת פעילות עסקית – שתשלום מס הוא חלק בלתי נפרד הימנה, וכי באופן כזה, תגבר התועלת שתצמח למשק על הנזק שייגרם למדינה בעצם ההכרה בתשלום כופרה כהוצאה המותרת בניכוי. בחברות וארגונים ישנה הבנה כי התועלת הנובעת מעמידה בהנחיות הרגולציה עשויה לעמוד לזכות החברה, הן באכיפה שגרתית והן בקרות אירוע אבטחת מידע כתוצאה ממתקפת סייבר.

"פרשת שירביט", הינה דוגמה לחברה שלכאורה לא עמדה בדרישות הרגולטור המגזרי – המפקח על שוק ההון, ובשל כך עוד בטרם המתקפה שאירעה בשלהי נובמבר 2020 הוטל עליה קנס בסך

<sup>16</sup> ה.ש. 4 תקנה 1 ותקנה 11 ד'.

<sup>17</sup> ה.ש. 4, תקנה 20

10,940,000 ₪ ע"י המפקח על שוק ההון. זאת ועוד, במהלך חודש יוני השנה התפרסם הסדר הפשרה בשבעה תובענות ייצוגיות שהוגשו כנגדה, ולפיו חברת הביטוח 'הראל' שרכשה את שירביט, תשלם סכום של 4.8 מיליון ₪.

נראה כי הגדרת תשלום כופרה כהוצאה מותרת בניכוי בכפוף לעמידה במבחנים שיוצגו במסמך זה, יהוו תמריץ לעמידה בתנאי הרגולציה, שכאמור, תתרום להקטנת החשיפה שתוארה.

### **פערי ידע ומוטיבציה בין נקודת המבט הלאומית לנקודת המבט של הארגון הנתקף היקף התופעה**

על פי דו"ח פשעי האינטרנט השנתי של 3IC ה-FBI אינו מעודד תשלום כופרה לגורמים פליליים. תשלום כופרה עשוי לעודד את התוקפים לפגוע בארגונים נוספים, לעודד גורמים עבריינים אחרים לעסוק בהפצה של תוכנות כופרה, ו/או לממן פעילויות לא חוקיות. תשלום הכופרה גם אינו מבטיח כי המידע של הנתקף יוחזר.

לא משנה אם אתה או הארגון שלך החלטתם לשלם את הכופרה, ה-FBI קורא לך לדווח על תקריות של תוכנת כופרה ל-3IC. פעולה זו מספקת לחוקרים את הדבר הקריטי מידע שהם צריכים כדי לעקוב אחר תוקפי תוכנות כופרה, להטיל עליהם דין וחשבון לפי החוק האמריקאי ולמנוע התקפות עתידיות".

למעשה, על פי הדו"ח, במהלך שנת 2022 דווחו כ- 2,385 תקיפות כופרה, מתוכן כ- 870 כווננו לארגונים ממגזרים קריטיים בארה"ב.

בישראל, כמו ברוב מדינות העולם, הרשויות נשענות על גופים מסחריים, אשר הסטטיסטיקה שלהן מוטה באופן משמעותי, כתלות בגוף המפרסם. יחד עם זאת, ישנה בהירות לגבי דבר אחד: כיום אין למדינה מקור מקיף ומהימן סטטיסטית לטובת קבלת אומדן אשר יאפשר לקובעי המדיניות, לנתח את היקף התופעה ואת השלכותיה על המשק.

### **דו"ח מבקר המדינה**

ממצא זה, עלה הן בדו"ח מבקר המדינה על פעילות משטרת ישראל ("קיים קושי לקבל מידע מלא לגבי היקף עבירות הסייבר, מאחר שחלקן הגדול אינו מדווח") והן בנתונים של מערך הסייבר הלאומי כפי שהוצגו בוועדת דויד ("בין השנים 2019-2021 התקבלו 413 דיווחים על מתקפות כופרה. על פי ההערכות של חברי צוות המשנה, בפרט של נציגי מס"ל בישיבות צוות המשנה, נתונים אלה נמוכים באופן ניכר מנתוני האמת לגבי מתקפות כופרה שמתרחשות בפועל כלפי אזרחים ותאגידים

ישראליים") ובפרט לאור השונות הגדולה הנובעת מקריאת "כתבות מאיימות" אשר מצטטות דוחות של מספר יצרניות פתרונות האבטחה בינלאומיות.

הפער העצום שבין הערכות גורמים שאינם מסחריים, דוגמת סקר למ"ס בנושא (בשיתוף מערך הסייבר הלאומי), סקר איגוד האינטרנט הישראלי וסקר התאחדות התעשיינים לבין נתוני יצרניות האבטחה וחברות המחקר (דוגמת סופוס ואחרות), מייצר בסיס מוטעה לקביעת מדיניות ציבורית בנושא. אמנם הדו"ח מציין כי "הנזק הכלכלי הכבד שנגרם למשק הישראלי, המוערך כאמור במאות מיליוני ש"ח", אך ניכר לאורך דו"ח הביקורת כי הוא מתבסס לא פעם על נתונים פומביים. כך לדוגמה מציין אותו הדו"ח בדיוק, כי מספר אירועי הכופרה שהתרחשו בעולם בשנת 2020 עומד על 304 מיליון. נתון מופרך, אשר בעקבותיו פניתי הן למשרד מבקר המדינה והן לחוקר מטעם חברת המחקר, שעל בסיס הנתונים שלה התבסס דו"ח המבקר.

עוד מובא בדו"ח המבקר, כי "בסקר בין-לאומי נוסף שנעשה בינואר 2021 ובו השתתפו יותר מ-5,400 מומחי טכנולוגיות מידע מהעולם, ובהם 100 ישראלים, נבדק היקף התופעה של תקיפות כופרה בחברות פרטיות בשנים 2017-2021 נמצא כי כ-54% מבתי העסק שהשתתפו בסקר נפגעו מתקיפת כופרה, וכי 96% מהם שילמו את דמי הכופרה, בסך מיליוני דולרים" בפרסומים משנת 2021, של חברת המחקר סייבריזן, נמצא כי: "רבע מהארגונים שחוו אירוע כופרה נסגרו, 80% עברו תקיפה שנייה ובשליש נרשמו פיטורים או התפטרות של מנהלים בכירים".

כמי ששוחח עם עשרות קובעי מדיניות במדינות שונות בנושא ובחן את הסוגייה באמצעות מאות שיחות עם בעלי עניין שונים (חברות ביטוח, יצרניות אבטחה, מנהלי אבטחה, רגולטורים ועוד), אני יכול לקבוע בוודאות כי נתונים אלו רחוקים משמעותית מהמציאות בשטח.

מתוך הערכות מבוססות, הנשענות בין היתר על הצלבה וניתוח של מידע ממספר גורמים בלתי תלויים, עולה כי היקף התופעה בישראל עומד בסבירות גבוהה מאוד על כמה אלפי אירועי כופרה בשנה בישראל, ועד לכמה עשרות אלפי אירועים בודדים בהערכה מחמירה.

### תשלום דמי הכופרה

במאמר של חברת המחקר גרטנר שדן בסוגיה "לשלם או לא לשלם, זאת השאלה", נאמר כי: "ההחלטה אם לשלם את הכופרה היא החלטה קשה וצריכה להיעשות בזהירות ברמת הדירקטוריון,

לא על ידי מנהלי אבטחת מידע וסיכונים". במאמר זה, מציין מארק האריס, אנליסט ומנהל בכיר בגרטנר כי "ההבנה מה קורה אם אתה משלם, היא המפתח לקבלת ההחלטה הזו".

על פי רוב, דמי הכופרה עומדים על עשרות עד מאות אלפי דולרים לארגון שנתקף. אמנם ישנם חריגים, דוגמת אירוע Acer (דרישה ל- 50 מיליון דולר) וכן דוגמאות בקצה השני, עם דרישה לתשלום של אלפי דולרים בודדים. יחד עם זאת, ניתוח דוחות אשר בוחנים את עלות האירוע הכוללת, לרבות היבטי שיקום, תדמית, כוח אדם ועוד עד להשבת הארגון לשגרה, מראים כי גובה דמי התשלום, מהווים פעמים רבות אחוזים בודדים בהשוואה לעלות האלטרנטיבית והמלאה, קרי לעלות של בחירת האפשרות להתמודדות עם האירוע ללא תשלום לתוקפים.

עלות חזרה מאירוע, עשויה להגיע לעשרות מיליוני שקלים ואף ליותר מכך, כתלות במספר רכיבים אשר משפיעים על החישוב המצטבר. לדוגמא, על פי הנתונים שהועברו על ידי משרד הבריאות, בגין "אירוע הלל יפה" מדובר בסכום של כ-36 מיליון שקל הכולל "הקמה מחדש של תשתיות תקשורת ומערכות מידע, אובדן הכנסות, דחיית ניתוחים לא דחופים, גיוס טכנאים להקמת המחשבים ועוד".

#### **מדיניות "איסור תשלום" במדינות שונות**

המדיניות הרשמית ברוב מדינות העולם, איננה לאסור את תשלום דמי הכופרה. בדו"ח של וועדת דזייד, בפרק שדן בסוגיית הפשעים באינטרנט בכלל ובסוגיית הכופרה בפרט, הוקצה פרק לעניין תשלום דמי הכופרה במדינת ישראל. "בדומה למצב במרבית המדינות שנסקרו לעיל, אין בישראל נורמה משפטית ייחודית לעניין תשלום" נכתב בדו"ח.

"בינתיים, מותר לשלם כופרה להאקרים, בתנאי שמי שמקבל את התשלום לא שייך לגוף שהוא פסול מבחינת הרשימה של גופים כאלה שמפרסמת הרשות לאיסור הלבנת הון ומימון טרור שבמשרד המשפטים, רשימה שכוללת קבוצות טרור ומדינות שנגזרו עליהן סנקציות בינלאומיות (למשל, איראן וצפון קוריאה, גורמים רוסיים וכו'). במקרים האמורים, כשקיים חשד סביר שהאקר או הגוף שמקבל את התשלום עבורו משתייך לישות אסורה, חל איסור מוחלט על העברת תשלום כלשהו". דברים אלו, נאמרו על ידי עו"ד דבורה האוסן-כוריאל.<sup>18</sup>

<sup>18</sup> [https://www.globes.co.il/news/article.aspx?did=1001386674#google\\_vignette](https://www.globes.co.il/news/article.aspx?did=1001386674#google_vignette)

אמנם בשנת 2021, פרסם משרד האוצר של ארה"ב עדכון להנחיית ה-OFAC המחדד את איסור התשלום של דמי הכופרה, אך בפועל בארה"ב, עבור רוב הגופים ובפרט עבור יתר מדינות העולם, עסקים רבים בוחרים בעל כורחם באפשרות של תשלום דמי הכופרה.

בישראל, לא יצא נכון ליום כתיבת מאמר זה, שום חוזר או התייחסות אשר אוסרים במפורש את ביצוע התשלום.

ישנה הבנה סמויה, כי סוגיה זו הינה בבחינת תפוח אדמה לוהט, אשר "נח" לגופים רבים להשאיר אותו במדיניות של עמימות. גופים אשר פנו אל מערך הסייבר הלאומי בשאלת חוקיות התשלום, קיבלו מענה אשר מחדד כי "מערך הסייבר עוסק בתקיפה ובתוקפים, ולא בסוגיות אשר אינן נוגעות ישירות לעצם המתקפה, הכלתה וסילוקה".

נקודת מבט נוספת, שאולי אף מציירת "הסכמה בעקיפין", היא עצם העובדה כי הרשויות השונות במדינה, לרבות המפקח על הבנקים והרשות לאיסור הלבנת הון, לא פסלו את המוצר הביטוחי שנקרא "**פוליסת סייבר**" אשר מאפשר בצורה גלויה לבצע תשלום דמי כופרה לקבוצות התקיפה בתנאים מסוימים. לו רצתה המדינה לאסור את התשלום, הרי שמתבקש היה כי היא תאסור מכירה של פוליסה אשר מצהירה כי כחלק מתכולתה, היא משלמת את דמי הכופרה לתוקף.

בטור דעה שנכתב על ידי לשכת רואי החשבון בישראל בשנת 2022, נאמר כי: "לדעתנו קיימת בישראל אנומליה שנראית מסוכנת בתחום הלבנת ההון. מצד אחד ומבלי לפגוע באסדרה הבנקאית הרלוונטית בישראל, לצורך תשלום הכופרה יש לבצע רכישה של מטבעות קריפטוגרפים מגוף בעל רישיון ישראלי מרשות שוק ההון (או היתר המשך עיסוק) או דרך גוף הממוקם מחוץ לישראל אך מחזיק את הרישיונות המתאימים לכך. מצד שני, אם הרוכש יצהיר בעת רכישת המטבעות הקריפטוגרפים על המטרה האמיתית של הרכישה, הלא היא תשלום כופרה, יהא על הצד המוכר לעצור את הפעולה; וזאת הואיל ולפי הוראות הרשות לאיסור הלבנת הון, מדובר ב"דגל אדום". כך, לא זו בלבד שעל אותו מנהל להתמודד עם מתקפת כופרה, אלא שעליו לשקר לכאורה במילוי שאלון "הכר את הלקוח", אם אין הוא רוצה לגזור גזר דין מוות על הישות שהוא מנהל".

עוד מנמקים רו"ח ועו"ד טל דננברג ורו"ח רועי כץ (יו"רים משותפים בוועדה לחדשנות, פינטק, בלוקצ'יין ומטבעות דיגיטליים בלשכה) כי: "ראוי כי הוצאה בגין כופרה (להבדיל מכופרה) תוכר כהוצאה לצורכי מס הכנסה. מדובר בתשלום המשולם לצורך המשך הפקת הכנסה, אשר הוא הכרחי להמשך ייצור ההכנסה והמשך הפעילות העסקית עד כדי כך שאותה ישות לא יכולה להימנע מלהוציא הוצאה זו.

הכרה בתשלום בגין כופרה כהוצאה אינה אסורה לפי סעיף 32(16) לפקודת מס הכנסה [נוסח חדש]: "תשלומים, בין שניתנו בכסף ובין בשווה כסף, שיש יסוד סביר להניח שנתינתם מהווה עבירה לפי כל דין". אומנם מטבעות קריפטוגרפים עולים כדי שווה כסף וזאת לפי חוזרי רשות המיסים בנושא, אך בניגוד לתפיסה כאילו מדובר בתשלום שמטרתו הימנעות מהעמדה לדין פלילי (קרי: כופרה), שככלל אינו מותר בניכוי כהוצאה, כאן מדובר בתשלום בגין כופרה וזו אינה מהווה עבירה מצדו של המשלם (להבדיל מאשר מצדו של התוקף, מקבל התשלום). משלם הכופרה אינו עובר עבירה כגון שוחד, אלא מבקש לשמור על הקיים ולהשיב את נכסיו המוחשיים והבלתי מוחשיים לקדמותם. לא מדובר בהשגת יתרון מתמיד בדרך המהווה עבירה על החוק אלא להיפך, מדובר בתשלום בלית ברירה על מנת לחזור במהירות האפשרית לפעילות עסקית תקינה. דווקא אי התרת ההוצאה והערמת קשיים בתחום הלבנת ההון פוגעות באיתנותם של העסקים ומגדילות את פוטנציאל הפגיעה במשק בפרט ובמדינה בכלל כתוצאה ממתקפות סייבר התקפי, בין פלילי ובין לאומני".

### ניתוח משמעויות "הכרה" בחלופת תשלום דמי הכופרה

חסרונות	יתרונות	
<ul style="list-style-type: none"> <li>- בעל העסק לא יודע אם התשלום יוביל "לפתרון הבעיה".</li> </ul>	<ul style="list-style-type: none"> <li>- עלות הכלה זולה יותר משמעותית.</li> <li>- העסק לא פועל באזור אפור/שחור של העלמת מידע מבעלי העניין השונים, כגון ספקים, לקוחות, רשויות וכו' (הפעילות מבוצעת בצורה שקופה).</li> <li>- בעל העסק לא נדרש לשקר בעת ביצוע הרכישה של המטבעות הדיגיטליים, כאשר הוא נשאל כחלק מתהליך KYC אודות תכלית רכישת המטבעות.</li> <li>- הארגון מרגיש קורבן ולא אשם. תיקון עוולה של היחס לבעלי העסקים במצב הנוכחי.</li> </ul>	<ul style="list-style-type: none"> <li>נקודת המבט של העסק</li> </ul>
<ul style="list-style-type: none"> <li>- המהלך תורם להגדלת ציר "הביקוש" ומעודד</li> </ul>	<ul style="list-style-type: none"> <li>- המדינה תקבל ויזיביליות טובה יותר בנושא פשיעת הסייבר, ותוכל לבסס</li> </ul>	<ul style="list-style-type: none"> <li>נקודת המבט של</li> </ul>

<p>תוקפים נוספים לפתח ולהתמיד בפשיעה מסוג זה.</p> <p>במידה והדבר ייחשב כהוצאה מוכרת, הרי שיישנה פגיעה מסוימת בטווח המיידני בהכנסות ממיסים.</p> <p>במידה ומדובר בגוף בעל "זיהוי ציבורי", הרי שהדבר עלול להוביל לפגיעה במורל ובתדמית הלאומית (כגון במקרה בו גוף שמזוהה עם הממשל ישלם דמי כופרה).</p>	<p>מדיניות לאומית מבוססת נתונים.</p> <p>- המדינה תסייע להצלה של חלק מהחברות הנתקפות, אשר חלופת אי התשלום עלולה לגזור עליהן "סגירת העסק" (עליית היכולת גביית מיסים, שימור רמת תעסוקה במשק ועוד).</p> <p>- המדינה תוכל לסייע לגופים אחרים, להתגונן מפני מתקפות דומות (באמצעות שיתוף מפתחות, ניתוח דרכי החדירה ועוד).</p>	<p>המדינה</p>
--	--	---------------

#### היבטים נוספים

- עלות התשלום, בהשוואה לעלות הנזק הכוללת (אשר כוללת בין היתר את השבתת הפעילות העסקית, תשלום לאנשי מקצוע, רכש ציוד ועוד) מהווה חלק קטן מאוד באופן יחסי.
- סוגיית "הלגיטימציה" לתשלום במקרה של כופרה, שונה מהדיון סביב תשלום דמי חסות/פרוטקשיין לעבריינים, הן בשל העובדה כי את דמי החסות לעבריינים מבצע העסק "בשגרה" ולא כאירוע "חד פעמי", הן בשל יכולת גורמי האכיפה לזהות, לשפוט ולצמצם את פעילות העבריינים והן בשל העובדה שתשלום כופרה, הינו משהו שהעסק משלם "בדיעבד" אחרי שכבר נגרם לו הנזק, במטרה להשיב את המצב לקדמותו.
- ניתן להסתכל על הקורבן שחווה אירוע תקיפה, באופן דומה לבעל עסק שהתרשל וכתוצאה מכך נגרם נזק לעסק שלו. לדוגמא, אם אדם השאיר תנור דולק במשרד ונשרף לו כל המשל



על כל תכולת המחשבים והחומר. במקרים בהם בחר בעל העסק שלא לרכוש פוליסת ביטוח, וכעת הוא נדרש להוציא סכום של 100,000 ₪ כדי לקנות מחשבים חדשים ולשחזר את כל המידע. האם גם במקרה זה, הוצאות אלו לא יוכרו לו במס?

- למדינה תפקיד קריטי ביכולת ביצוע זיהוי וייחוס של מתקפה לקבוצת התוקפים ולמדינת היעד. מקורות מידע שימושיים.<sup>19</sup>
- חשוב לזכור, כי להחצנה שלילית יכולה להיות תמונה כפולה/אמביוולנטית. לדוגמא, באירוע קולוניאל פייפליין. האם היה ראוי לשלם (מה שקרה בפועל)? אילו מהאינטרסים הציבוריים גבר על משנהו? אי תשלום לתוקף, או הצורך של האזרחים לקבל שירות חיוני בצורה רציפה? ומה לגבי בתי חולים?
- כיום, לרוב מוחלט של הגופים במשק, אין מוטיבציה לדווח על אירוע סייבר. ברוב מוחלט של המקרים, למדינה אין יכולת לעזור לגוף הנתקף. המצב לא שונה ברוב מדינות העולם וברוב התקיפות.

### אישור פורנזי – הפרמטרים הטכניים

הפורנזיקה הדיגיטלית, כמדע משפטי, פועלת להתאמת ממצאים דיגיטליים כך שיעמדו בדרישות ראייתיות ובהמשך שיוכלו לשמש בהליכים משפטיים. במסגרת פעילות התחקור הטכנולוגי, הפורנזיקה הדיגיטלית הינה המתודולוגיה להפקת ממצאים, הנדרשים להצגה בהתאם לדרישות הרגולטוריות. המתודולוגיה הפורנזית היא חלק מתחום חקירות הזיהוי הפלילי וכוללת עקרונות קשיחים לשמירה על תיעוד ושרשרת ראייתית בנוסף להיבטים המקצועיים הטכנולוגיים שבה. ישנה נטייה להתמקד בקשיים הטכנולוגיים שבאיתור הממצאים הדיגיטליים תוך התייחסות מועטה להיבטים המתודולוגיים של הפורנזיקה. בעוד חקירות טכנולוגיות מפורטות ומקצועיות יכולות להתבצע על ידי בעלי מקצוע שונים, עמידה בדרישות פורנזיות דורשת רקע והבנה בתהליכים ראייתיים, בתיעוד ובהליכים משפטיים.

<sup>19</sup> [/https://www.cbsnews.com/news/ransomware-payments-may-be-tax-deductible](https://www.cbsnews.com/news/ransomware-payments-may-be-tax-deductible)

[https://www.american.edu/kogod/research/cybergov/upload/williamsondon\\_bloombergransomware\\_2017.pdf](https://www.american.edu/kogod/research/cybergov/upload/williamsondon_bloombergransomware_2017.pdf)

<https://fletcher.tufts.edu/news-events/news/hit-cyberattack-your-ransom-payment-hackers-may-be-tax-deductible>

<https://www.irs.gov/about-irs>

במדינת ישראל, לצורך ביצוע חדירה לחומר מחשב ולחקירתו לצרכי הליך פלילי, נדרש מומחה מחשבים בעל תפקיד מיומן<sup>20</sup> וכן בעת הנדרשת, ישנו צורך בצו שופט לביצוע חיפוש בחומר מחשב בהליך אזרחי.<sup>21</sup> מומחיות במחשבים איננה מספיקה בכדי לשמור על הממצאים כראיות וכאשר אנו דנים בתחום המובא לאישור רגולטורי, הרי שעל הארגון להקפיד על תהליכי התקינים.

כדי לעמוד בהיבטים המעשיים להכרה בתשלום כופרה כהוצאה מוכרת ואכן להראות כי הארגון הנתקף אינו יכול להימנע מתשלום הכופרה, יש לבחון את האפשרויות השונות העומדות לפתחו של הארגון בעת ההתמודדות עם ההצפנה ודרישת הכופרה.

בהיבט הטכנולוגי, בעת התמודדות עם אירוע כופרה, נדרשת חקירה מעמיקה לזיהוי ההצפנה, להבנת היקף הפגיעה במערכות הארגון ולבחינת דרכי התמודדות והתאוששות מהירים.

מערך הסייבר הלאומי פרסם בשנת 2019 מדריך להתמודדות עם אירוע כופרה<sup>22</sup> ובו מוצעת מתודולוגיה לבחינת הכופרה, למציאת מפענח ולבחינת אפשרויות שחזור המידע. יובהר כי אין הגדרה רגולטורית להתנהלות באירוע כופרה באופן שיקבע חד משמעית שהארגון התמודד עם האירוע בצורה המיטבית. כיום, אם הרשויות נדרשות לבחינה, זו נעשית באופן פרטני על ידי הרגולטור הרלוונטי ובהתאם לפרקטיקות המקובלות באותה העת.

ארגון NIST האמריקאי פרסם המלצות היערכות ארגוניות וטכנולוגיות לקראת אירוע כופרה,<sup>23</sup> וכן מסמכים נוספים להתמודדות עם אירוע כופרה.<sup>24</sup>

בנייר עמדה זה, אנו ננסה לצייר כמה קווים מנחים כללים, אשר נלמדים מתוכניות התאוששות במקרים של אירועי כופרה ומפרסומים ממשלתיים בנושא.

בהיבט המתודולוגי, כדי להגיע להבנה כי דרך הפתרון הנכונה ביותר לארגון ברגע קבלת ההחלטה הינה תשלום הכופרה, על הארגון לבצע הערכה טכנולוגית ועסקית להערכת הנזק שנגרם ולתוכניות התאוששות אפשריות. כפי שיפורט בהמשך, הדרישות המוטלות על הארגון כדי שיוכל להראות שפעל

<sup>20</sup> ר' סי 23 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969

<sup>21</sup> ר' ת' 116 לתקנות סדר הדין האזרחי, התשע"ט-2018  
<sup>22</sup> <https://www.gov.il/BlobFolder/reports/ransomware/he/RANSOMWARE-CERT-IL-W-980.pdf>

<sup>23</sup> ר' מודל הערכת מוכנות להתגוננות מפני כופרה: NIST IR 8374, Ransomware Risk Management: A Cybersecurity Framework  
Profile <https://csrc.nist.gov/pubs/ir/8374/final>  
וכן: <https://csrc.nist.gov/files/pubs/other/2022/02/24/getting-started-with-cybersecurity-risk-management/final/docs/quick-start-guide--ransomware.pdf>  
<sup>24</sup> <https://cyberreadinessinstitute.org/resource/ransomware-playbook/>

באמצעים טובים להימנע מתשלום הכופרה, כוללות תיעוד רב ופעולות טכנולוגיות מורכבות הדורשות תיעוד אף הן. לרוב מדובר במעמסה משמעותית על ארגון המתמודד עם אירוע בהיקף רחב העוצר את פעילותו ולכן היערכות מוקדמת גם לשלב ההתאוששות תסייע לארגון לפעול על פי הנחיות מתודיות.

לשם כך, ישנם פרמטרים הדורשים בחינה והערכה מצד הארגון על מנת לקבל החלטה מושכלת יותר לתשלום הכופרה:

1. **היקף מניעת הגישה הקיימת בארגון הנתקף** – האם אכן מדובר מבחינה טכנולוגית בהפסקת פעילות מוחלטת של הארגון. יש למפות את כלל המערכות שהוצפנו לרבות רכיבי חומרה ותוכנה ולהעריך את היקף השפעת הרכיבים האלה על עצירת פעילות הארגון.
2. **קיומן המוקדם של תוכניות ומערכות שתפקידן היה למנוע ולמזער התרחשות אירוע מסוג זה.**
3. **קיומה של היערכות ארגונית להתאוששות ממתקפת כופרה** – תוכנית התאוששות המציגה את המערכות הקריטיות הראשונות שיש לשחרר מהצפנה ואת השפעתן על החזרה לפעילות הארגונית.
4. **בוצעו פעולות על ידי הארגון לזיהוי סוג הכופרה ולחיפוש ושימוש במפענח הצפנה.**
5. **תכנית גיבויים קיימת וטיב הגיבויים הקיימים** – להראות שביצע פעולות להחזרת מערכות הארגון לפעילות על בסיס שימוש בגיבויים קיימים. שימוש בגיבוי קיים מחייב בדיקת תקינותו של הגיבוי ואישור טכנולוגי כי רכיבי הכופרה אינם שוכנים גם בגיבוי. במקרה שבו ישנם רכיבי כופרה בגיבוי, הארגון יבחן אפשרות העתקת מידע מתוך הגיבוי לעליה למערכות נקיות תוך שימוש במידע שניתן לחלץ מהגיבוי.
6. **ארגון שאין ברשותו גיבויים קיימים המאפשרים חזרה לפעילות** – יצטרך להציג את מקום הכשל ומדוע אין ברשותו גיבויים, ומדוע אין באפשרותו לשחזר גם מידע חלקי.
7. **חיוניות קונקרטית של המידע שאינו ניתן לשחזור** – על הארגון להראות מדוע המידע שאינו יכול לשחזר קריטי לפעילותו עד כדי הצורך בתשלום הכופרה ולא להתאוששות על בסיס מידע חלקי הניתן לשחזור ממקורות שונים.

מוצע כי את כלל הערכת המצב וניהול הסיכונים הארגוניים יבצע גורם חיצוני לחקירה הטכנולוגית המבצעת באירוע, אשר יוכל לבדוק את קיומו של התיעוד הדרוש. זאת, מכיוון שנדרשת נקודת מבט חיצונית, כביקורת, לבדיקת תיעוד ללא היכרות מוקדמת של הפעולות שבוצעו לשם הערכת טיב החומרים וכן החוסרים הקיימים לצורך השלמתם.

הצוות מציע כי השימוש בגורם פורנזי מבקר-חיצוני, המאשר את התיעוד ואת הפעולות שביצע הארגון, יאפשר לרגולטורים לקבע תהליך אחיד ומונחה מקצועית למשק להתמודדות עם אירועי כופרה ולעמידת הארגונים בדרישות הרגולטוריות, באופן שיקל על הרגולטור, תוך התמקדות בתחום האכיפה הרלוונטי ולא בכלל פעולות הארגון ותהליכיו בקבלת ההחלטות בכל אירוע כופרה המתרחש בארגונים.

## סקירה נורמטיבית של ניכוי הוצאות לצורכי מס

### הכרה בתשלומי כופרה כהוצאה עסקית

פרק זה מספק ניתוח של ההבחנות בין תשלום שוחד, תשלומי הגנה וסחיטה, תוך התמקדות בפרספקטיבה של ביטול הוצאה מוכרת לצורכי מס הכנסה. באופן ספציפי, הפרק בוחן את הרציונל להכרה בתשלומי כופרה ששולמו על ידי עסקים כהוצאות הניתנות לניכוי. בפרק יוצג ניתוח השוואתי של הכרה בהוצאות באופן כללי, כדי להבהיר את הסיבות וההשלכות הבסיסיות הקשורות להכרה בהוצאות תשלום כופרה לצורך ניכוי מס.

#### מבוא לניכוי הוצאות

הוצאה המותרת בניכוי – בעלת חשיבות מהמדרגה הראשונה ומהווה בסיס לדיני המס, משמעות הדבר שעסק (עצמאי, חברה או תאגיד) ישלם מס אך ורק על הכנסתו בניכוי הוצאותיו, שאם לא כן אזי אותו עסק בפועל יחויב במס כפול, הן בתשלום מס על ההכנסה, והן בתשלום בגין ההוצאה. יישום עקרון בסיסי זה בדיני המס מוצג בדו"ח השנתי של כל עסק, הכנסות העסק בניכוי הוצאות שעמד בהן העסק לצורך ייצור הכנסותיו ועל פי בסיס זה מחושב ומשולם המס.

מס הכנסה מוטל בישראל, מכוח פקודת מס הכנסה על "ההכנסה החייבת", דהיינו: ההכנסה לאחר הניכויים, הקיזוזים והפטורים שהותרו ממנה לפי כל דין.<sup>25</sup> בהתאם לכך, זכאי נישום לנכות הוצאות שונות, בכפוף לכללים שנקבעו בפקודה. ס' 17 לפקודה קובע כי "לשם בירור הכנסתו החייבת של אדם ינוכו... הוצאות שיצאו כולן בייצור הכנסתו בשנת המס ולשם כך בלבד...".<sup>26</sup> לשון הסעיף טומנת בחובה מספר אבחנות:

#### הוצאה עסקית

הוצאה עסקית מוגדרת כהוצאה שהוצאה כולה לצורך ייצור ההכנסה באותה שנת המס, הוצאות בעסק אלו מסווגות באופן הבא:

- הוצאות שוטפות **שמוכרות במלואן** (כגון: העסקת עובדים, קניות, וכמובן כל הקשור בתחזוקת מערכת המחשבים בעסק).
- הוצאות שוטפות **מעורבות**, הוצאות אלו הוגבלו בשל עירוב השימוש הפרטי והשימוש העסקי (כגון: כיבוד, נסיעה לחוץ-לארץ, הוצאות לינה וארוחת בוקר, מתנות, הוצאות ביגוד, שיחות

<sup>25</sup> י' אדרעי "על ניכוי הוצאות הון, היוון הוצאות שוטפות, ושימוש נאות בשיטות דיווח" הפרקליט לט, 136  
<sup>26</sup> ס' 17 לפקודת מס הכנסה [נוסח חדש]

טלפון, אחזקת רכב ורכישת בגדי עבודה). ככלל, הוצאות מעורבות אינן מותרות בניכוי.<sup>27</sup> למרות זאת, נקבע כי אם ההוצאות ניתנות להפרדה, יש להתיר את ניכוי של החלק שהוצא בייצור הכנסה.<sup>28</sup> מעניין זה ניתן ללמוד כי מערכת המס יודעת לקבוע כללים לאבחנה ולניכוי הוצאות מסויימות,<sup>29</sup> ואף נקבעו תקנות ליישום הכללים.<sup>30</sup> כך בא לידי ביטוי בדיני המס עקרון חיוב במס אמת - משמע כי למרות הקושי הגלום בניכוי הוצאות "מורכבות" - לא ניתן "לוותר" על ניכוי הוצאה "מורכבת" במטרה לחייב את העסק במס על הכנסתו בפועל לאחר הוצאות.

- **הוצאות הוניות** לרכישת נכס, מוכרות בהתאם לאורך חיי השימוש בנכס.
- הוצאות **ענישה**, אינן מוכרות כלל גם אם נעשו במסגרת עסקית (כגון: דוחות, קנסות). הוצאה פרטית זו הוצאה שאינה קשורה לפעילות העסקית ולא הוצאה לשם הפקת הכנסה.<sup>31</sup> לפיכך, היא אינה ניתנת לניכוי כהוצאה מתוך הכנסות העסק.

### בין הוצאה פירותית להונית

שאלה העשויה לעלות במקרה של תשלום כופרה, היא האם מדובר בהוצאה שוטפת (פירותית) או בהוצאה הונית (הפרוסה על פני מספר שנים)

ככל ומדובר בהוצאה עסקית, יש לעמוד על האבחנה שבין הוצאה פירותית – המותרת בניכוי, להוצאה הונית – שמותרת לניכוי כנגד הכנסה הונית או כפריסה על פני מספר שנות השימוש בנכס שנרכש. כך, הוצאה פירותית היא הוצאה שמטיבה מייצרת הכנסה בשנת המס הנוכחית (כגון משכורות לעובדים; מלאי עסקי) בעוד שהוצאה הונית מייצרת הכנסה מעבר לשנת המס (כגון ציוד; מכונות). לצורך ביסוס האבחנה, הפסיקה פיתחה את "מבחן ההשבחה מול שמירה על הקיים", לפיו, הוצאות המוצאות לצורך שמירת הקיים ואחזקת מנגנון הייצור במצב תקין, יותרו בניכוי.<sup>32</sup> מנגד, הוצאה שיש בה כדי להשביח נכס הוני קיים או להעניק לו יתרון תמידי, תסווג כהוצאה הונית המותרת בניכוי אך

<sup>27</sup> ע"א 580/65 א' בן-עזר ובניו בע"מ נ' פקיד השומה למפעלים גדולים, תל-אביב 7, כ(2) 179. (1966)  
<sup>28</sup> אהרן נמדר, מס הכנסה [יסודות ועיקרים] (מהד' רביעית, 2013), 276

<sup>29</sup> סעיף 31 לפקודת מס הכנסה מסמיך קביעת תקנות בדבר ניכוי הוצאות, "שר האוצר רשאי, באישור ועדת הכספים של הכנסת, להתקין תקנות - בין דרך כלל ובין לסוגים של נישומים - בדבר הגבלתו או אי-התרתו של ניכוי הוצאות מסויימות לפי סעיפים 17 עד 27, ובמיוחד בדבר - (1) שיטת החישוב או האומדן של הוצאות; (2) סכומי ההוצאות שיותרו בניכוי, או שיעוריהן; (3) התנאים להתרת ההוצאות; (4) דרכי הוכחת ההוצאות.

<sup>30</sup> תקנות מס הכנסה (ניכוי הוצאות מסויימות), תשל"ב-1972 וכן תקנות מס הכנסה (ניכוי הוצאות רכב), תשנ"ה-1995

<sup>31</sup> יוסף גרוס, דיני המס החדשים (מהדורה שלישית, 2003), 328  
<sup>32</sup> ע"א 735/86 צ' בן שחר זרעים בע"מ נ' פ"ש ת"א, 3 פד"א יח 10

ורק כנגד הכנסה הונית<sup>33</sup> או בפריסה על פני מספר שנות חייו של הציוד הנרכש (באמצעות ניכוי פחת).

כאמור ניתן לפתח במערכת המס מנגנונים להכרה בהוצאות אף אם הן "מורכבות" או הזורשות התאמות וכללים מיוחדים (שיטת חישוב, תנאים ודרכי הוכחה) לצורך הכרה בהן.

### הוצאה לא חוקית, ניכויים שאין להתירם

סייג נוסף להתרת ניכוי הוצאות הינו ביחס להוצאות שאינן חוקיות או נוגדות את תקנת-הציבור. נקבע כי הוצאה שאינה חוקית, כגון שוחד, אסורה בניכוי. בהקשר זה, בית המשפט מעניק משקל למידת אי-החוקיות. כך, באם העבירה אינצידנטלית להוצאה, ייתכן ותותר בניכוי.<sup>34</sup>

בהציגו כי הוצאה לא חוקית איננה מותרת בניכוי, עולה השאלה באשר לחוקיות תשלום כופרה. מחד, יש הטוענים כי ראוי לסווגו כתשלום שאינו חוקי, שכן הוא מחזק את המודל של התוקפים. בנוסף, הוא מהווה סבסוד לרשת הפלילית.<sup>35</sup> מנגד, יש הטוענים כי סיווג התשלום כתשלום לא-חוקי מעניש את הקורבנות במקום את העבריינים.<sup>36</sup> כמו כן, אי-החוקיות עלולה לספק תמריץ לקורבן להסתיר את מתקפת הכופרה. הסתרה זו מלווה במחיר חברתי כבד בכך שאינה מונעת מאחרים ליפול קורבן לאותה מתקפה ומחלישה את אבטחת הסייבר ככלל.<sup>37</sup> כחלק מהדיון בשאלה, נציג מספר פרקטיקות של תשלומים שאינם חוקיים תוך השוואה והבחנה ביניהם לבין תשלום כופרה, נתייחס להשלכות בדבר סיווג התשלום וכן נציע מספר קריטריונים לצורך הכרה בתשלום כופרה בהוצאה מותרת.

### תשלומים לא חוקיים

שוחד, תשלומי הגנה וסחיטה הינם פרקטיקות בלתי חוקיות הכוללות החלפת משאבים כספיים בנסיבות כפייה. נבקש כעת לעמוד על ההבדלים והדמיון בין פרקטיקות אלו בהקשר של ניכוי מס, תוך שימת דגש מיוחד על הכרה בתשלומי כופרה כהוצאות עסקיות הניתנות לניכוי. הבנה מעמיקה של ההבחנות הללו חיונית להערכת הלגיטימיות של הכרה בתשלומים אלו לצורכי מס.

<sup>33</sup> אהרון נמדר, מס הכנסה [יסודות ועיקרים] (מהד' רביעית, 2013), 270.

<sup>34</sup> עמ"ה (י-ם) 54/84 בתי מלון אלערביה נ' פייש י-ם, פד"א טו 38.

<sup>35</sup> Financial Accounting and Tax Implications of Ransomware.

<sup>36</sup> The Uneasy Case for a Ransom Tax.

<sup>37</sup> Financial Accounting לעיל ה"ש 35.

שׁוּחַד כּרוֹך בּמתן, הצעה, קבלה או שיזול של משהו בעל ערך כדי להשפיע על פעולות או החלטות של אדם בעמדה של כוח. מנקודת מבט מיסויית, תשלומי שׁוּחַד אינם מוכרים כהוצאות עסקיות לגיטימיות, שכן הם נוצרים למטרות בלתי חוקיות ומנוגדים לעקרונות של תחרות הוגנת והתנהגות אתית. מסגרות משפטיות רבות ואמנות בינלאומיות אוסרות בהחלט על ניכוי תשלומים הקשורים לשׁוּחַד. בשונה מכופרה, תשלום שׁוּחַד מאופיין בכך ששני הצדדים נגועים במוטיבציה לעבור על החוק.

תודגש כאן הסתייגות נוספת העשויה להיות רלוונטית לשאלת הבסיס במאמר זה, האם תשלום הכופרה מהווה עבירה על פי דין. בשנת 2009 עניין זה תוקן בפקודת מס הכנסה ונקבע בסעיף 32(16) במסגרת רשימת "ניכויים שאין להתירם", איסור על התרת ניכוי של "תשלומים, בין שניתנו בכסף ובין בשווה כסף, שיש יסוד סביר להניח שנתינתם מהווה עבירה לפי כל דין".

התיקון האמור לפקודה נערך בעקבות פסיקת בית המשפט העליון בעניין תשלום שׁוּחַד. שם נקבע תשלום הוצאה בגין שׁוּחַד אינם מותרים לניכוי, אולם דעותיהם של שלושת השופטים היו חלוקים בדרך בה הגיעו למסקנה זו. השופט רובינשטיין גרס כי אין להתיר את ההוצאה בניכוי בשל כך שמדובר בכספי שׁוּחַד, לעומתו, השופטים א' חיות ו- י' אלון גרסו כי אי התרת ההוצאות בניכוי נובעת עקב כשל ראייתי, כלומר חוסר בהוכחה על ביצוע תשלומים אלו לצורך ייצור ההכנסה. מהלאו ניתן ללמוד על ההן, לא נאמר כי קיים איסור מוחלט לניכוי הוצאה "בלתי חוקית" לכאורה.<sup>38</sup>

### תשלומי הגנה

תשלומי הגנה כוללים מתן כספים ליחידים או לגופים כדי להבטיח הגנה או בטיחות לפעילות העסקית. ככלל, תשלומי הגנה משמשים כאמצעי לשמירה על אינטרסים עסקיים בסביבה בה שחיתות ופשע מאורגן מהווים סיכון משמעותי. כפועל יוצא, חוקיות תשלומי הגנה עשויה להשתנות בהתאם לתחום השיפוט וההקשר. הכרה בתשלומי הגנה כהוצאות הניתנות לניכוי מס אסורה בדרך כלל מאחר והקשר לפעילות בלתי חוקית מרכזי ודומיננטי.

<sup>38</sup> ע"א 6726/05 הירולה בע"מ נ' פקיד שומה ת"א 1 (נבו 05.06.2008)



## סחיטה

סחיטה משקפת פעולה של כפיית יחידים או ארגונים לספק נכסים, לרבות כסף, בכפייה איומים או הפחדה. מנקודת מבט של ניכוי מס, הכרה בתשלומי סחיטה כהוצאות עסקיות לגיטימיות מציבה אתגרים אתיים ומשפטיים משמעותיים. התשלומים נובעים מפעילויות בלתי חוקיות מובהקות, ובכך ניכויים אינו עולה בקנה אחד עם עקרון ההוצאה הלגיטימית של העסק.

## כופרה

כופרה סייבר, המכונה גם "תוכנת כופרה", הינה סוג של תוכנה זדונית שנועדה להצפין או להגביל גישה לקבצים או למערכות הדיגיטליות של הקורבן. העבריינים דורשים תשלום כופרה, בדרך כלל במטבע קריפטוגרפי, בתמורה להחזרת הגישה או מתן מפתח הפענוח. התקפות כופרה סייבר מנצלות נקודות תורפה ברשתות מחשבים, לרוב באמצעות הודעות דיוג, ערכות ניצול או אתרי אינטרנט שנפגעו. הצמיחה של מטבעות קריפטוגרפיים הקלה על האנונימיות והקלות של העסקאות והפכה את כופרה הסייבר לשיטה אטרקטיבית ורווחית יותר. כמו כן, האנונימיות מקשה בהמשך להגיע אל העבריין ולהשיב את התשלום במסגרת הליכים פליליים מקובלים.

## ניתוח השוואתי

### מוטיבציה

בעוד שדמי סחיטה וכופרה סייבר חולקים את המניע של רווח כספי, תשלום שוחד מונע מהרצון להשפיע על תהליכי קבלת החלטות או להשיג יתרונות לא הוגנים. עמלות סחיטה מכוונות לנצל פחד או הפחדה, בעוד כופרה סייבר מנצל את הצורך הדחוף בגישה או שחזור נתונים. כך, ניתן להקביל את המוטיבציה לתשלום בעבור כופרה סייבר להוצאה פירותית הנועדה לשמר את הפעילות העסקית הקיימת בדומה לעקרון "שמירה על הקיים", ולחילופין, ניתן להקביל תשלום ה להוצאה הונית מעין רכישה עצמית של ציוד העסק מחדש, יתרה מזו, אילו העסק לא יעמוד בתשלום זה, הרי שיעמוד בתשלום העלול להיות אף גבוה יותר ברכישת הציוד הנדרש לעסק חדש, תשלום לבעלי מקצוע להתקנת עסק חדש ושחזור העסק הקודם (מאגר לקוחות, נתונים וכו') – שחזור ממקורות חיצוניים העלול לעלות לעסק ולמדינה - עלות גבוהה לאין שיעור.

### כפייה ואיומים

דמי סחיטה מסתמכים על איומים ישירים, הפחדה או אלימות כדי לכפות על קורבנות לעמוד בדרישות. שוחד כרוך לרוב במניפולציה עדינה או בהשפעה עקיפה באמצעות החלפת טובות הנאה או הטבות.

לעומת זאת, כופרה סייבר משתמש באיום של אובדן נתונים או פגיעה במערכת כדי להפעיל לחץ על הקורבנות, מה שהופך אותו למונע יותר מבחינה טכנולוגית.

### השלכות משפטיות

תשלומים בעבור סחיטה ושוחד הם בלתי חוקיים ברוב תחומי השיפוט ותשלומן מקים אחריות פלילית. לכופרה סייבר, כפשע סייבר, יש השלכות משפטיות דומות. עם זאת, האופי האנונימי וחוצה הגבולות של התקפות כופרה סייבר, מציב אתגרים בפני רשויות אכיפת החוק, מה שהופך את האיתור והתביעה למורכבים יותר.

### יישום התרת ניכוי הוצאת תשלומי כופרה

תשלומי הכופרה כאמור שנויים במחלוקת, אולם נוכח המאפיינים הייחודיים של תשלום כופרה, ייתכן כי לא ראוי לסווגה כפעולה בלתי חוקית באופן גורף (בין היתר כי המשלם הוא קורבן ולא העבריין). בעוד שתשלומי כופרה קשורים לרוב לפעילויות לא חוקיות ולכפייה, מספר גורמים משפיעים על הטיעון להכיר בחוקיותן ולהתיר את ניכוי המס שלהם:

#### הוצאות רגילות והכרחיות

לשם זכאות להכרה בניכוי הוצאות לצורכי מס הכנסה, התשלומים חייבים לעמוד בקריטריונים של היותם רגילים והכרחיים. במקרים מסוימים, עסקים עשויים לטעון שתשלומי כופרה נחוצים כדי להגן על הפעילות, הנכסים והנתונים שלהם מפני נזק או אובדן פוטנציאליים, ובכך להצדיק את הניכוי שלהם.

#### הפחתת הפסדים

יכול שייטען מצד עסקים כי תשלומי כופרה מהווים אמצעי לצמצום הפסדים כספיים פוטנציאליים הנובעים מהשיבוש, הנזק למוניטין או הפרת המידע כתוצאה ממתקפות סייבר. הטענה גורסת, כי הכרה בתשלומי כופרה כהוצאות הניתנות לניכוי, מסייעת לעסקים להתאושש מתקריות מסוג זה ולשמור על המשכיות. שיקול זה משמעותי במיוחד שעה וישנו חשש שעסקים ייפגעו אנושות ממתקפת סייבר עד כדי סגירתם. בנוסף, בהקשר רחב יותר, גילוי בהכרה בתשלומי כופרה עשוי למנוע הסתרה של מתקפות ולהפחית הפסדים מקורבנות אחרים בהמשך.

האופי המתפתח של איומי הסייבר והשכיחות ההולכת וגוברת של מתקפות כופרה, גרמו למספר רשויות מס וקובעי מדיניות לשקול את ניכוי המס של תשלומי כופרה. בתחומי שיפוט מסוימים, נמשכים דיונים בנוגע לצורך בתקנות או הנחיות ספציפיות שיתייחסו לטיפול המס בתשלומים כאלה.

## הקריטריונים לקביעת הכרה בהוצאות תשלום כופרה לצרכי מס

### ניתוח השלכות ההכרה בתשלום כופרה כהוצאה מוכרת על אוצר המדינה

במידה ותשלום הכופרה יוכר כהוצאה מוכרת, הדבר צפוי להטיל נטל על אוצר המדינה ולמעשה לגרום להפחתה מגביית מס. עם זאת, נראה שהכרה כזו, בשל הנימוקים לעיל, נכונה וצודקת בהיבט של מדיניות כללית ברמה הלאומית, והתועלת בצידה עולה באופן משמעותי על הנטל הצפוי. להלן רשימת נימוקים המצדיקים הכרה בתשלום כופרה באירוע סייבר (כהוצאה מוכרת) כמפורט להלן, ואשר אינם מהווים בהכרח רשימה סגורה:

הכרה בתשלום כופרה בשל אירוע סייבר (בכפוף לכל התנאים לעיל) תעניק למעשה רשת בטחון לעסקים אשר עומדים בתנאים המפורטים לעיל.

ההכרה תעודד עסקים השואפים לקבל הכרה, לנהוג באחריות מרבית בנקיטת פעולות לשמירה ולהגנה על מידע ומאגרי נתונים.

ההכרה תעודד עסקים לפעול כדי להגן בנמרצות על מאגרי מידע ונתוני פרטיות של לקוחות ושל הציבור בכללותו.

ההכרה תעודד עסקים לפעול בשקידה לייעול התנהלותם במרחב הסייבר. דבר זה עשוי גם לשפר את מעמדה של ישראל ברמה של תאימות ואכיפה מול מדינות אחרות לרבות האיחוד האירופי.

ההכרה תעודד יצירת רשת ביטוחית נאותה לעסקים ובכך תמזער חשיפה לתשלום פיצויים ו-נזקים בלתי הפיכים. יצירת רשת ביטוחית פרטית תפזר את הנזקים בקרב כל העסקים העומדים בתנאים לעיל.

ההכרה מהווה, למעשה, אמירה ערכית בדבר רגישות הפגיעה במידע במרחב של המגזר הפרטי בישראל.

### התנאים המקדימים להכרה בתשלום כופרה כהוצאה מוכרת על אוצר המדינה

ככל והוצאה בעבור תשלום כופרה תוכר כהוצאה חוקית ובהמשך כהוצאה המותרת בניכוי, יש להתנות קבלת הטבה זו מקופת המדינה במספר תנאים מצטברים שעל המבקש הכרה לעמוד בכולם מראש, כמו גם לשם מניעת הונאות וניצול ההטבה. להלן תמצית התנאים:

**הערכת סיכוני אבטחה כללית:** קורבנות פוטנציאליים יבצעו הערכת סיכוני אבטחת סייבר כללית בדגש על בחינת סיכונים הקשורים לתוכנת כופרה, תוך סקירת שיטות העבודה המומלצות, תקני אבטחה מקומיים ובהתאם לרגולציה. כך, ניתן יהיה למנוע אחוז מסוים מההתקפות ולמגר את התופעה.

**הודעה לגורמים הרלוונטיים על המתקפה:** שעה שמתחילה מתקפת סייבר, על הקורבן לדווח באופן מיידי על המתקפה ותשלום הכופרה לכל הגורמים הרלוונטיים, לרבות רשויות המס והרשות להגנת הפרטיות כמתחייב על-פי חוק (במקרי אירוע אבטחה חמור כהגדרתו בחוק). קריטריון זה, מלבד היותו ראייה מתועדת למתקפה, עשוי לסייע לקורבן עצמו בכך שמוציא את המו"מ מהמחשכים ומעניק רשת תמיכה. כמו כן, הדבר מסייע למניעת התקפות דומות על קורבנות נוספים.

**קיום הוראות הדין הספציפי:** הגורם המותקף קיים את הוראות החוק והרגולציה החלים עליו בכל הקשור להגנת הפרטיות ולאבטחת מידע לרבות best practice.

**חובת הזהירות של הנפגע/הנישום:** הגורם המותקף פעל לפי סטנדרט הזהירות המקובל בדיני הנזיקין (בין היתר פעל להקטין את הנזקים ולא התרשל בשמירה על המידע).

**ניתוח וניהול משברים:** על הקורבן להכין מסמך הכולל ניתוח וניהול משברים, ממנו ניתן להסיק כי אכן תשלום הכופרה במקרה הספציפי יכול להפחית משמעותית את ההפסדים ולספק תועלת כלכלית לארגון בהשוואה לשחזור המערכת. מסמך זה עשוי להכריע בשאלת יעילות תשלום הכופרה.

39

**לא הייתה דרך אחרת לשחרור המידע למעט באמצעות תשלום הכופרה הנדרש:** הצגת אישור של גורם פורנזי מוסמך המוכיח כי הארגון פעל בשקידה לשחזור המידע המוחזק על ידי הצד התוקף באירוע סייבר ו/או צד אחר שהמידע הגיע אליו שלא כדין וכי תשלום הכופרה הייתה הדרך היחידה לפתרון.

**פוליסת ביטוח:** ביטוח המספק כיסוי לאירועי סייבר. יודגש כי הסכום שהנישום יכול לבקש שיוכר כהוצאה יהיה רק לאחר הקיזוז מכל סכום שיקבל מהמבטח בפוליסת ביטוח סייבר כאמור. במילים אחרות, ההכרה בתשלום כופרה כהוצאה מוכרת, לא תהיה ברירת המחדל של הנישום אלא רק השלמה של הכיסוי הביטוחי שרכש.

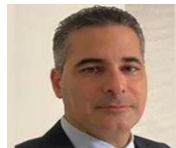
הקושי המרכזי העולה מזרישת הביטוח: מתקפות סייבר הן חדשות יחסית ושוק הביטוחים בהקשר זה טרם מפותח. מסיבה זו, עלות הפרמיה גבוהה כך שהביטוחים עשויים להיות יקרים במיוחד. בנוסף, יש המתנגדים בכלל לביטוח מסוג זה שכן הוא משמר את פרקטיקת תשלומי הכופרה.<sup>40</sup> נראה כי קריטריון הביטוח יעיל רק כאשר הוא מצטרף לשאר הקריטריונים והניסיונות למגר את תופעת מתקפות הסייבר.

## סוף דבר

שוחד, תשלומי הגנה וסחיטה, כרוכים כולם בשיטות לא חוקיות הקשורות להחלפת משאבים כספיים. הכרה בתשלומי כופרה כהוצאות עסקיות הניתנות לניכוי לצורכי מס הכנסה, מעוררת אתגרים ייחודיים בשל ממד הכפייה ומקורם הבלתי חוקי. אמנם ניתן להעלות טיעונים על סמך מושגי הכרח, הפחתה בהפסדים ושיקולים רגולטוריים, אך הקונצנזוס הרחב יותר נוטה לאי ניכוי של תשלומים כאלה. רשויות המס, מחוקקים וארגונים בינלאומיים ממשיכים להתמודד עם המורכבות של נושא זה, ומבקשים להגיע לאיזון בין טיפול בפגיעות עסקיות לבין שמירה על עקרונות אתיים ומשפטיים. לאור הדיון, בספרות מקובל לטעון כי המפתח להתמודד עם תופעות אלו מצוי בהתמקדות במניעה. שכן, כאשר המתקפה בעיצומה, דרכי ההתמודדות מצומצמים במיוחד.

בסיכומי של דבר, ובשקילת מכלול השיקולים, נכון יהיה להכיר בתשלום כופרה בשל אירוע סייבר כהוצאה מוכרת. הכרה כזו, תוביל לחיזוק מעמד ההגנה על מאגרי מידע ודיני הפרטיות, תשפר את מעמדו של המגזר הפרטי בעיני שותפים עסקיים בארץ ובחו"ל, תדרבן נקיטת הליכים אקטיביים להגנה על מאגרי מידע ולמעשה תקטין ותמזער נזקים ברמת המיקרו והמקרו.

## על המחברים:



עו"ד יעקב עוז    עו"ד סיגל אבירם    פרופסור אמיר חורי    עו"ד דנית לייבוביץ שטי    מהנדס יובל שגב

**עו"ד יעקב עוז** – יו"ר ועדת הסייבר והגנת הפרטיות בלהב, מרצה ויועץ בדיני הגנת הפרטיות, מייסד משרד עורכי הדין – יעקב עוז ושות'

**פרופסור אמיר חורי** – פרופסור למשפטים באוני' תל אביב. ראש מכון ש.הורוביץ לקנין רוחני.

**עו"ד ויוע"מ (חשבונאית) סיגל אבירם** – בעלת משרד עריכת דין ויועץ מס, היועצת המשפטית של לשכת היועצים העסקיים והניהוליים בישראל, וכן חברת ועדת מיסים בפורומים שונים.

**מהנדס יובל שגב** - יו"ר פורום סייבר באיגוד הדירקטורים, וחבר בוועדה מייעצת (Advisory Board) במספר ארגונים.

**עו"ד דנית לייבוביץ שטי** - מנכ"לית חברת אלפא פורנזיקס.