



**משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר**

תאריך: כ"ח בתשרי התשפ"ג
23 באוקטובר 2022

לכבוד

מר ערן דויד, מנכ"ל משרד המשפטים

שלום רב,

הנדון: ז'ח צוות המשנה בנושא פשיעה והונאות במרחב הדיגיטלי – מתקפות כופרה

תוכן עניינים

2	מבוא
3	תיאור תהליך העבודה של צוות המשנה
6	נתונים על אודות מתקפות כופרה
7	האם ובאילו תנאים יש לאסור על תשלום כופר
8	סקירה משווה
8	ארצות-הברית
11	האיחוד האירופי
12	אוסטרליה
12	ניו-זילנד
12	בריטניה
13	גרמניה
13	צרפת
14	קנדה
14	הדין הישראלי הקיים
15	עמדות שהובעו בפני צוות המשנה
16	איסור פרסום של מתקפת כופרה
17	סקירה משווה
17	ארצות הברית
18	אוסטרליה
19	ניו זילנד
21	האיחוד האירופי
22	בריטניה
23	גרמניה

עמוד 1 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

23	קנדה
25	הדין הישראלי הקיים
25	חובת פרסום
28	איסור פרסום
30	עמדות שהובעו בדיוני צוות המשנה
31	המלצות
31	המלצות בנוגע לאיסור תשלום כופר
32	המלצות בנוגע לאיסור פרסום

מבוא

1. כידוע, ביום 7.12.2021 הורית על הקמת צוות משנה לוועדה להתאמת המשפט לאתגרי החדשנות ולהאצת הטכנולוגיה בראשותך (להלן: "הוועדה"). צוות המשנה נועד לעסוק בנושא **אבחון הבעיות ויצירת דרכי טיפול בנושא פשיעה והונאות במרחב הדיגיטלי** (להלן: "צוות המשנה"). זאת מתוך הכרה בחשיבות הנושא ומאפייניו הייחודיים מתוך כלל הנושאים בהם מתעתדת הוועדה לעסוק. הוחלט כי צוות המשנה יפעל באופן ממוקד לקידום הנושא, למיפוי התופעות במסגרתו איתן נדרש להתמודד, ולבניית תוכנית פעולה.
2. בהתאם לכתב המינוי, כלל צוות המשנה את הגורמים הבאים:
 - א. ד"ר חיים ויסמונסקי, מנהל מחלקת הסייבר בפרקליטות המדינה – יו"ר הוועדה.
 - ב. גב' אניטה יצחק, סגנית הממונה ברשות להגנת הצרכן וסחר הוגן.
 - ג. גב' ליאת גורפינקל, הייעוץ המשפטי למערך הסייבר הלאומי (להלן: "מס"ל").
 - ד. ד"ר שלומית ווגמן, ראש הרשות לאיסור הלבנת הון ומימון טרור (לשעבר).
 - ה. גב' גבי פיסמן, ראש אשכול סמכויות, מחלקת ייעוץ וחקיקה (משפט פלילי).
 - ו. גב' סוריא בשארה, אשכול עונשין ופשיעה חמורה, מחלקת ייעוץ וחקיקה (משפט פלילי).
 - ז. מר שלומי אסטרונגו, מנהל יחידת יהלוי"ם, רשות המיסים.
 - ח. מר שרון ברגר, רכז חוליה בחקירות מס הכנסה, רשות המיסים.
 - ט. תנ"צ דורון יאיר, רח"ט סייבר-סיגינט, משטרת-ישראל.
 - י. נצ"מ זיו שגיב, חטיבת חקירות, משטרת-ישראל.
 - יא. סנ"צ דודי קץ, מפקד יחידת הסייבר בלהב 433, משטרת-ישראל.

עמוד 2 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

תיאור תהליך העבודה של צוות המשנה

3. בעקבות כתב המינוי נערכה במחלקת הסייבר בפרקליטות המדינה עבודת מטה פנים-יחידתית במטרה לאבחן את התופעות המרכזיות בפשיעה והונאות במרחב הדיגיטלי בהן יעסוק צוות המשנה. התופעות שסומנו בעקבות עבודת המטה הן:

א. **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 ההדבקה, דורש התוקף העברת תשלום כופר כתנאי לפתיחת ההצפנה.¹ תופעת מתקפות הכופרה צברה תאוצה בשנים האחרונות, ויש לה השלכות נרחבות על ארגונים ואנשים פרטיים (שהם מושאי תקיפה ולחלופין – המידע האישי שלהם המוחזק בידי ארגונים מצוי בסכנה). כיום אין מדיניות ממשלתית סדורה להתמודדות עם הנושא.

ב. **הונאות פורקס (Forex):** שם "גנרי" לתופעה רחבה של הצעת מוצרי השקעה פיקטיביים ללקוחות, וגניבת כספים מבלי לספק את ההשקעה המוצעת בפועל. הטיפול בתופעה חסר, ונראה כי רשויות האכיפה בישראל בעיקר מגיבות לפנייות לעזרה משפטית המגיעות מחו"ל (גם זאת באופן חלקי).

ג. **הונאות דיוג (פישנינג):** שליחת הודעות בהיקף נרחב לאזרחים (באמצעות SMS, דוא"ל או רשת חברתית) הנחזות לרוב לאתר של גוף לגיטימי (בנק, חברת אשראי, דואר ישראל וכדומה). לעיתים ההודעות כוללות קבצים או קישורים זדוניים שנועדו להדביק את הקורבנות בנוזקות, ולעיתים מטרתן היא לקבל כספים במרמה או גישה בלתי מורשית למידע האישי של מקבל ההודעה.² מדובר בהונאות מתוחכמות בהיקף רחב הפוגעות באנשים רבים, ומטופלות כיום באופן חסר בישראל. כך, בין היתר, לא קיים מנגנון דיווח ייעודי לאזרחים, הדיווחים הקיימים אינם מרוכזים ומקשים על קבלת ההחלטה לחקור את ההונאה (שכן היקפה אינו ברור), אין פעילות ליידוע הציבור לגבי הונאות דיוג קיימות, ולא נעשות כלל פעולות הגנתיות כגון הסרת האתר המתחזה או חסימתו. נוסף על כך, אין כיום פתרון מלא לנפגעים.

4. לאחר מכן, התקיימו שני מפגשי עבודה של צוות המשנה, כדלקמן:

ישראל	משטרת	אתר	כופרה,	מתקפות	1
		https://www.gov.il/he/departments/guides/police_cybercrime_ransomware			
ישראל	משטרת	אתר	דיוג (פישנינג),	הונאות	2
		https://www.gov.il/he/departments/guides/police_cybercrime_phishing			

עמוד 3 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

א. מפגש עבודה ביום 9.1.2022: בפתח הדיון הוצגו לחברי צוות המשנה שלוש התופעות העשויות להיות רלוונטיות לעבודת הצוות שאובחנו בעבודת המטה ותוארו לעיל. במהלך מפגש העבודה, נערך סבב ובו חברי צוות המשנה הציגו את הנושאים שהם מעוניינים לקדם במסגרת עבודת הצוות. כמו כן, רוכזו הצעות החקיקה שהועלו על ידי חברי הצוות ואלו הועברו להתייחסותן של נציגות מחלקת ייעוץ וחקיקה (פלילי) בצוות המשנה, על מנת שתעדכנה בנוגע לסטטוס של כל הצעה.³

ב. מפגש עבודה יום 30.1.2022: בדיון הוצגה סקירה משווה שהוכנה על-ידי מחלקת הסייבר בפרקליטות המדינה הנוגעת לשלושה התופעות. בכלל זה הממצא כי לא אותרה אף מדינה שגיבשה מדיניות הוליסטית להתמודדות עם תופעת מתקפות הכופרה, על אף שמדובר בתופעה נפוצה מאוד הגורמת נזק בהיקף עצום לארגונים רבים; בהמשך לכך, פורטו הסוגיות שנדרש להסדיר בכל הנוגע למדיניות הממשלתית ביחס למתקפות כופרה, וחברי צוות המשנה הביעו את תמיכתם בגיבוש מדיניות ממשלתית סדורה בעניין זה; נציגות מחלקת ייעוץ וחקיקה (פלילי) עדכנו בנוגע לסטטוס הצעות החקיקה הרלוונטיות לעבודת צוות המשנה (שהועלו במפגש העבודה הראשון); הוצג אופן ההתמודדות עם הונאות פורקס בישראל: המצב הקיים, קשיי אכיפה, ופתרונות מוצעים לשם התמודדות עם קשיים אלו.

5. ביום 27.4.2022 התקיימה ישיבה של הוועדה במסגרתה הציג מנהל מחלקת הסייבר בפרקליטות המדינה את פעילותו של צוות המשנה, כפי שפורט עד כה. בהמשך לכך, ביקשת כי צוות המשנה יתמקד בתופעת מתקפות הכופרה, ויפעל לגיבוש מדיניות ממשלתית הוליסטית להתמודדות עם התופעה.

6. בעקבות זאת, ביום 6.6.2022, פרסם צוות המשנה קול קורא לציבור הרחב במטרה לקבל התייחסויות בנושא התמודדות עם מתקפות כופרה, לצורך גיבוש מדיניות ממשלתית הוליסטית להתמודדות עם התופעה (להלן: **"הקול הקורא"**).⁴ במסגרת הקול הקורא פורטו שורה של סוגיות, והן:

³ תיקון התוספת לחוק איסור הלבנת הון, התש"ס-2000 – הוספת עבירות מחשב כעבירת מקור. מדובר בהצעה שהועברה ממחלקת הסייבר בפרקליטות המדינה לבחינת צוות המשנה לענייני חקיקה הפועל תחת המסגרת של הוועדה המתמדת להכוונה ולתיאום הפעילות במאבק בפשיעה החמורה ובפשיעה המאורגנת ובתוצריהן (להלן: **"הוועדה המתמדת"**); תיקון חוק המחשבים, התשנ"ה-1995 – הוספת סעיף עונשי מחמיר של עבירות מחשב בנסיבות מחמירות. ההצעה הועברה ממחלקת הסייבר בפרקליטות המדינה לבחינה במחלקת ייעוץ וחקיקה (פלילי); תיקון חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע"ז-2017 – בדרך של הוספת אתרי דיוג (פישנינג) לרשימת סוגי האתרים שניתן לבקש לגביהם סעדים במסגרת החוק. ההצעה הועברה ממחלקת הסייבר בפרקליטות המדינה למחלקת ייעוץ וחקיקה (פלילי); תיקון הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד-2014 – על דרך של הוספת התייחסות לחדירה לשרתים מרוחקים. ההצעה נבחנת בימים אלה במחלקת ייעוץ וחקיקה (פלילי); הוספת סמכות הקפאה זמנית לרשות לאיסור הלבנת הון לגבי חשבונות שמתנהלת בהם פעילות חשודה. ההצעה נבחנה במקור על-ידי צוות המשנה לענייני חקיקה של הוועדה המתמדת, ונותב לאחרונה לאשכול סמכויות במחלקת ייעוץ וחקיקה (פלילי).

⁴ https://www.gov.il/he/departments/publications/Call_for_bids/ransomware-0622



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

- א. הסדרת הסמכויות בין הגופים והרשויות בישראל (בין היתר, משטרת ישראל, מס"ל ורשות המיסים) תוך הבחנה בין סוגי הגופים המותקפים.
- ב. גיבוש עמדה בנוגע למענה המדינתי שיש לספק לגוף מותקף בזמן אמת, לרבות הכרעות בנוגע להיקף הסיוע ובנוגע לשאלה האם המענה יהיה על בסיס וולונטרי או בכפייה.
- ג. שאלת ה"הפללה" של תשלום הכופר, ומדיניות האכיפה כלפי המשלמים. בהקשר זה, יכולות להיגזר שאלות משנה כגון: מהם התנאים לפטור מאחריות פלילית בגין עבירה של הלבנת הון או מימון טרור? האם יש מקום לחייב את הנסחט לדווח על תשלום הכופר לרגולטורים רלוונטיים (כגון מס"ל, רשות להגנת פרטיות, רגולטור מגזרי רלוונטי)?
- ד. האם נכון להכיר – בתנאים מסוימים – בתשלום כופר כהוצאה מוכרת מבחינת דיני המס?
- ה. האם יש לקבוע במצבים מסוימים איסור פרסום על מתקפת הכופר (למשל אם מדובר בתשתית לאומית קריטית, או אם מדובר במתקפה שפרסומה ברבים והבלטתה יחריף משמעותית את נזקה), או שמא דווקא יש לקבוע חובת פרסום במצבים מסוימים (כאשר מידע אישי של אנשים מצוי בידי הגוף המותקף, כאשר מדובר בחברה ציבורית שהנפיקה ניירות ערך לציבור)?
- ו. האם ובאילו תנאים יכול הגורם הנסחט לקבל שיפוי על נזקיו, לרבות על הנזק הישיר בדמות תשלום הכופר, מחברת ביטוח המעניקה ביטוח סייבר?

7. במקביל לכך, בהמשך לשיח שהתקיים עם מס"ל, סוכם כי לעת הזאת, צוות המשנה יתמקד בנושאים השלישי והחמישי, קרי בשאלת ה"הפללה" של תשלום כופר ובשאלת הפרסום בדבר מתקפת כופר. בהמשך, ובהתאם להנחיותיך, צוות המשנה יוכל להמשיך ללבן ולגבש המלצות באשר ליתר הנושאים שפורטו לעיל.

8. לאחר עיון בהתייחסויות שנתקבלו לקול הקורא, זומנו מספר דוברים להציג את התייחסויותיהם ולהרחיב עליהן בפני צוות המשנה, תוך התמקדות בשני הנושאים שפורטו לעיל. בימים 21.9.2022 ו-28.9.2022, התקיימו שני מפגשי עבודה של צוות המשנה, בהם הציגו הדוברים הבאים: מר טיראן פרטוק, מנכ"ל חברת Yush Capital המספקת שירותי היערכות והתמודדות עם אירועי אבטחת סייבר;⁵ גבי יעל רגב אונגר, מנהלת מחלקת טכנולוגיות מידע וסייבר ברשות שוק ההון, הביטוח והחיסכון (להלן: "רשות שוק ההון") ומר עמית גל, סגן בכיר לממונה על שוק ההון, ביטוח וחיסכון ברשות שוק ההון; מר דורון הדר, שותף מייסד של חברת קריטיקל אימפקט, המספקת שירותי ניהול משברים, לרבות משברי סייבר; פרופ' טל זירסקי, דיקן הפקולטה למשפטים באוניברסיטת חיפה, בשנים האחרונות חוקר את תחום מתקפות הכופר; ומר גלעד בנט, אחראי על אסטרטגיה בתחום פשיעת סייבר במס"ל.

⁵ מר פרטוק היה מעורב, בין היתר, בניהול משברי סייבר בעניינם של בנק לאומי, בנק דיסקונט וחברת שירביט.



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

נתונים על אודות מתקפות כופרה

9. בטרם נרחיב על שני הנושאים בהם דן צוות המשנה, נציין מספר נתונים על אודות היקף התופעה של מתקפות כופרה, וכן נתונים ביחס לנזקים הנגרמים כתוצאה מהן:⁶

א. על-פי ארגון האינטרפול, קיימת מגמת עלייה חדה במספר מתקפות הכופרה (בייחוד נגד בתי חולים), הונאות סייבר ופרצות נתונים (data breaches).⁷ כמו כן, הסוכנות האירופית לאבטחת מידע ורשתות (European Union Agency for Cybersecurity) (להלן: "ENISA") ציינה בדו"ח המסכם לשנת 2021 כי איום הסייבר הנפוץ ביותר במהלך שנת 2021 היה מתקפות כופרה.⁸

ב. על-פי הסקירה השנתית שפרסם המרכז הלאומי לאבטחת סייבר בבריטניה (National Cyber Security Centre) (להלן: "NCSC UK"), ברבעון הראשון של שנת 2021 בוצעו יותר מתקפות כופרה בבריטניה מאשר בשנת 2020 כולה.⁹

ג. במסמך מדיניות של ממשלת אוסטרליה, פורסמה הערכה לפיה ברחבי העולם, כל 11 שניות מתרחשת מתקפת כופרה על עסק, ומשוער כי הנזק הגלובלי ממתקפות כופרה בשנת 2021 יגיע ל-20 מיליארד דולר אמריקני.¹⁰

ד. במסמך המדיניות של המשרד הפדרלי הגרמני לאבטחת טכנולוגיות מידע (להלן: "BSI") משנת 2021, צוין כי אחד האיומים הגדולים בתחום הפשיעה במרחב הסייבר הוא מתקפות כופרה.¹¹

⁶ יודגש כי ישנו קושי אינהרנטי להעריך את היקף הפשיעה וההונאות במרחב הדיגיטלי, לא כל שכן את הנזקים מפשיעה זו. למדינות, לארגונים בינ"ל ולתאגידים יש לרוב אינטרס להסתיר את הנתונים האמיתיים, על מנת לשמר את תדמיתם. מנגד, לחברות המגנות מפני פשיעה במרחב הדיגיטלי יש אינטרס הפוך "לנפח" את הנתונים, וזאת כדי להוכיח את יכולותיהם במניעה ובתגובה לפשיעה.

⁷ [INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes](#) (October 2021).

⁸ [ENISA Threat Landscape 2021 \(October 2021\)](#)

⁹ National Cyber Security Centre, [Annual Review 2021: Making the UK the safest place to live and work](#) (November 2021) [online](#).

¹⁰ Australia's Ransomware Action Plan (Oct. 2021) <https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf>

¹¹ Federal Ministry of the Interior, Building and Community, Cyber Security Strategy for Germany (2021) <https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.html>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

ה. בשנת 2020 התקבלו ב-FBI כ-2,500 דיווחים על מתקפות כופרה, ושיעור הנזק המדווח הכולל בארה"ב - על יסוד דיווחים עצמיים - הוא כ-29 מיליון דולר אמריקני. מדובר בעלייה של כ-300% משנת 2019.¹² עם זאת, הרשות לאכיפת פשעים פיננסיים (Financial Crimes Enforcement Network) דיווחה כי במחצית הראשונה של 2021 סך תשלומי הכופר בארה"ב עמד על 590 מיליון דולר אמריקני, והדבר משקף גידול עצום לעומת כל שנת 2020, שאז סך תשלומי הכופר בארה"ב עמד על 416 מיליון דולר אמריקני.¹³

ו. על פי הערכות של חברות פרטיות,¹⁴ בין 2019 ל-2020 חלה עלייה של למעלה מ-300% בהיקף תשלומי הכופר שבוצעו בפועל על-ידי הנפגעים, כאשר בשנת 2020 שולמו ברחבי העולם למעלה מ-400 מיליון דולר אמריקני.¹⁵ לצד זאת, חלה עלייה של כ-170% בגובה תשלום הכופר הממוצע בארה"ב, בקנדה ובאירופה לכל מתקפה נתונה: מכ-115,000 לכ-312,000 אלף דולר אמריקני.¹⁶

ז. באשר להיקף התופעה בישראל, במוקד 119 המופעל על ידי מס"ל, בין השנים 2019-2021 התקבלו 413 דיווחים על מתקפות כופרה. מפילוח הנתונים לפי שנים עולה כי הייתה עלייה משמעותית בדיווחים בין 2019 ל-2020 (מ-101 ל-148, עלייה בכ-50%), ועלייה נוספת, בין 2020 ל-2021, אך מתונה יותר (מ-148 ל-164, עלייה בכ-10%). 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 ישראלים.¹⁷

האם ובאילו תנאים יש לאסור על תשלום כופר

10. ראשית נסקור את המצב הקיים במדינות שונות ביחס לשאלת ההצדקה לאסור, להגביל או לתמרץ באופן שלילי תשלום כופר. ככלל, במרבית המדינות אין איסור ייחודי וגורף על תשלום כופר במסגרת מתקפת כופרה. לצד זאת, במדינות רבות שנדרשו לסוגיה דן ישנה המלצה (לא-מחייבת) שלא לשלם

¹² FBI, Internet Crime Report (2020) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

¹³ Financial Crimes Enforcement Network, Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 (2021)

https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf. הנתונים מבוססים על דיווחים מגופים פיננסיים לפי חוק איסור הלבנת הון (Anti-Money Laundering Act of 2020).

¹⁴ יצוין כי הערכות אלו פורסמו במסמך הערכת סיכוני פשע מאורגן מקוון לשנת 2021 של היורופול - Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

¹⁵ Chainalysis, Ransomware 2021: Critical Midyear Update, <https://blog.chainalysis.com/reportsransomware-update-may-2021> (2021).

¹⁶ PaloAlto Networks, 2021 Unit 42 Ransomware Threat Report, <https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html> (2021)

¹⁷ בהמשך לה"ש 6, יצוין כי לא קיימת כיום חובת דיווח למס"ל, כך שכל הנראה הנתונים שפורטו אינם משקפים את מלוא התופעה בישראל.



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

דמי כופר. שנית, נפרט על אודות עבירות פליליות בדין הישראלי העשויות לחול במקרה של תשלום דמי הכופר. שלישית, נציג את העמדות השונות שהובעו במהלך דיוני צוות המשנה בעניין זה. לבסוף, נסכם ונציג את המלצות צוות המשנה.

סקירה משווה

ארצות-הברית

11. אין כיום חקיקה פדרלית המטילה איסור בגין תשלום כופר בעקבות מתקפת כופרה.¹⁸ לצד זאת, בספטמבר 2021, מחלקת בקרת נכסים זרים במשרד האוצר (Office of Foreign Assets Control) (להלן: "OFAC")¹⁹ פרסמה מסמך מדיניות בו הודגש כי ממשלת ארצות-הברית מתנגדת נחרצות לתשלום כופר, מאחר שהסכום המשולם עשוי לסייע לתוקף במימון פעולות לא חוקיות נוספות, המפרות את הביטחון הלאומי ומנוגדות למטרות מדיניות החוץ האמריקניות.²⁰ נוסף על כך, תשלום הכופר מעודד ביצוע מתקפות נוספות. כך, חברה שבחרה לשלם עשויה להיות נתונה למתקפה נוספת בעתיד. לבסוף צוין כי אין הבטחה שחברה אשר בוחרת לשלם את הכופר תשיג גישה מחדש לנתונייה, משום שההתקשרות בין הצדדים היא משענת קנה רצוף, מול גורמים עבריינים.

12. בהתאם לכך, קורבן למתקפת כופרה, אשר משלם את דמי הכופר לישות המצויה באחת מרשימות הסנקציות של OFAC, עשוי להפר תקנות של OFAC. במדיניות האכיפה שפרסמה OFAC פורטו השיקולים הרלוונטיים לקביעת פעולת האכיפה המתאימה להפרה, אשר יכולה לנוע מתגובה שאינה פומבית, כמו שיגור מכתב אזהרה לגורם המפר, ועד להטלת קנס כספי אזרחי (civil monetary penalties).²¹ השיקולים שפורטו הם:

¹⁸ ראו סקירה שנערכה על ידי מרכז המחקר של הקונגרס האמריקני, שפורסמה באוקטובר 2021 - Congressional Research Service *Ransomware and Federal Law: Cybercrime and Cybersecurity* p.10 <https://crsreports.congress.gov/product/pdf/R/R46932#:~:text=If%20a%20ransomware%20attack%20or,incident%20response%20and%20damage%20mitigation>

¹⁹ מחלקה זו מוסמכת להטיל סנקציות במטרה להגשים את מדיניות חוץ וביטחון של ארצות-הברית. לרוב OFAC מטילה סנקציות על מדינות או על חבר אנשים (groups of individuals) כגון טרוריסטים או סוחרי סמים; US Department of the Treasury, *Basic Information On OFAC and Sanctions* <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1501>

על אמריקנים חל איסור לשלם או לערוך עסקאות, באופן ישיר או עקיף, עם גורמים המצויים ברשימת הסנקציות של OFAC או מדינות הנתונות תחת אמברגו, לפי International Emergency Economic Powers Act (IEEPA) משנת 1977 ולחלופין לפי Trading with the Enemy Act משנת 1917. איסור זה חל גם במצב בו מתבצעת עסקה המפרה את IEEPA על ידי גורם שאינו אזרח אמריקני, שמובילה אזרח אמריקני להפר איסורים של IEEPA. זאת ועוד, על כל אזרח אמריקני, ללא תלות במיקומו, חל איסור לסייע לאזרח לא-אמריקני לבצע פעולה שאינה יכולה להיות מבוצעת על ידי אזרח אמריקני, תחת מערך הסנקציות האמריקני.

לענייני, רלוונטי הכנסתה של זירת המסחר למטבעות וירטואליים, SUEX, לרשימת הסנקציות של OFAC, מפני ששירות זה זוהה כמספק שירותים פיננסיים עבור גורמים המבצעים מתקפות כופרה. US Department of Treasury, *Treasury Takes Robust Actions to Counter Ransomware* (September 2021) <https://home.treasury.gov/news/press-releases/jy0364>

²⁰ Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (September 2021) https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

²¹ שם.



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

א. פעולות של החברה המותקפת להטמעת תוכנית מבוססת סיכונים שנועדה להפחית את החשיפה לאינטראקציה עם ישויות המצויות באחת מרשימות הסנקציות של OFAC. תכנית מסוג זה צריכה לכלול התייחסות לסיכון שתשלום הכופר יועבר לישות הנתונה תחת סנקציות. על-פי OFAC, שיקול זה נבחן גם בנוגע לחברות הנמצאות באינטראקציה עם קורבנות של מתקפות כופרה, לרבות חברות המספקות ביטוח סייבר וחברות המספקות שירותים פיננסיים ויכולות לסייע בביצוע תשלום הכופר.

ב. נקיטת צעדי אבטחת סייבר כדוגמת אלה המנויים במדריך של הסוכנות לאבטחת סייבר ותשתיות (Cybersecurity and Infrastructure Security Agency) (להלן: "CISA"),²² אימוץ נהלי אבטחת סייבר, ושיתוף פעולה מידי ומתמשך עם גורמי אכיפת החוק ו-CISA.

ג. דיווח באופן יזום ומפורט על אודות תשלום הכופר, ואספקת מידע רלוונטי כמו מידע טכני, גובה הכופר הנדרש לשלם, הוראות הנוגעות לתשלום הכופר.

במסמך המדיניות של OFAC צוין שאם החברה המותקפת נקטה בצעדים כמו אלה המנויים לעיל, OFAC ייטה לבצע פעולת אכיפה שאינה פומבית.

13. מעבר לכך, במדריכים להתמודדות עם מתקפות כופרה, ה-FBI וכן CISA המליצו שלא לשלם תשלום כופר.²³

14. להשלמת התמונה יצוין כי בספטמבר 2021, הוצגה הצעת חוק בקונגרס האמריקאי, במסגרתה הוצע לעגן איסור על גופים פיננסיים לשלם דמי כופר העולים על 100,000 דולר, ללא קבלת אישור של הרגולטור הפדרלי הרלוונטי.²⁴

15. בשונה מהדין הפדרלי, בדין הפנים-מדינתי בארצות-הברית נצפית מגמה של חקיקה האוסרת או לפחות מגבילה תשלום כופר.

²² כגון שמירת גיבוי נתונים לא מקוונים, פיתוח תכניות פעולה, עדכון תדיר של תכניות אנטי-וירוס ועוד. CISA הוקמה בשנת 2018 ותפקידה הוא ניהול והפחתת הסיכונים לתשתיות הסייבר של הממשל האמריקני. CISA מפרסמת מדריכים למניעה ולהתמודדות עם תקריות אבטחת סייבר מסוגים שונים. בספטמבר 2020, CISA פרסמה מדריך למתקפות כופרה (<https://www.cisa.gov/stopransomware/ransomware-guide>) ובנובמבר 2021 פרסמה מדריך כללי לאירועי אבטחת מידע https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf). המדריכים כוללים תיאור של תהליכי קבלת החלטות, שיטות עבודה מומלצות, לקחים מתקריות אבטחת סייבר שאירעו בעבר, ציקליסט להתמודדות בעת התרחשות תקרית ועוד. מטרת פרסום המדריכים היא לסייע לגופים השונים לאמץ שיטות עבודה מומלצות ואחידות וכן לאפשר ל-CISA לעקוב אחר יכולתן של סוכנויות פדרליות להתמודד בהצלחה עם תקריות אבטחת סייבר.

²³ לעיל הייש 22; FBI Scams & Safety: Ransomware ; *ransomware guide* September 2020 ; <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware>

²⁴ <https://www.congress.gov/bill/117th-congress/house-bill/5936?s=1&r=35>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

- א. באפריל 2021, צפון קרוליינה אסרה בחוק על ישויות מדינתיות או מקומיות לשלם כופר ואף ליצור קשר עם התוקפים, במסגרת מתקפות כופרה.²⁵ בין הישויות שהחוק חל עליהן מצויים כל הגופים הממשלתיים, רשויות מקומיות, מוסדות חינוך ציבוריים ועוד.²⁶
- ב. בינואר 2022 הסנאט בפנסילבניה אישר הצעת חוק דומה (הצעת החוק מונחת כעת על שולחן בית המחוקקים),²⁷ במסגרתה הוצע לאסור על ארגונים הממונים מכספי מיסים לשלם כופר. כך, הוצע לאסור על תשלום כופר באמצעות כספי מיסים או כספים ציבוריים, למעט מקרים חריגים, בהם המושל יכריז על מצב חירום ויאשר את התשלום.²⁸

N.C. Gen. Stat. § 143-800 <https://casetext.com/statute/general-statutes-of-north-carolina/chapter-143-state-departments-institutions-and-commissions/article-84-various-technology-regulations/section-143-800-state-entities-and-ransomware-payments> ²⁵

ראו גם Spencer Pollock & Kelly Campbell *north Carolina bans state entities from negotiating with hackers – and other states may follow Mcdonald Hopkins* (9.6.22) <https://mcdonaldhopkins.com/Insights/June-2022/NC-bans-negotiating-with-hackers>

עוד יצוין כי במסגרת אותו תיקון חקיקה, הוטלה גם חובת התייעצות עם ה-Department of Information Technology בצפון קרוליינה (להלן: "10NCBIT").

²⁶ שם, (c)(1): "Local government entity. - A local political subdivision of the State, including, but not limited to, a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college"; (c)(2): "State agency. - Any agency, department, institution, board, commission, committee, division, bureau, officer, official, or other entity of the executive, judicial, or legislative branches of State government. The term includes The University of North Carolina and any other entity for which the State has oversight responsibility"; Jonathan Grieg *an inside Look into States Efforts to Ban Gov't Ransomware Payments*, *The Record* (23.8.2022) <https://therecord.media/an-inside-look-into-states-efforts-to-ban-govt-ransomware-payments/>

SENATE BILL NO. 726 ²⁷
<https://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2021&sesSarahCoblePennsylvaniaApproves> : ראו גם: [sInd=0&billBody=S&billTyp=B&billNbr=0726&pn=1326](https://www.infosecurity-magazine.com/news/pennsylvania-ransomware-bill-info-security)

Scott Ikeda ; LEGISCAN <https://legiscan.com/gaits/search?state=PA&bill=726> ; [approves-ransomware-Patchwork Of US State Regulations Becomes More Complex As Florida, North Carolina Ban Ransomware Payments CPO](https://www.cpomagazine.com/cyber-security/patchwork-of-us-state-regulations-becomes-more-complex-as-florida-north-carolina-ban-ransomware-payments) (19.8.2022) <https://www.cpomagazine.com/cyber-security/patchwork-of-us-state-regulations-becomes-more-complex-as-florida-north-carolina-ban-ransomware-payments>

Patricia A. Markus, Gina Ginn Greenwood *Not In My Backyard*: ; Senate Bill No. 726 Article 767 שם, ²⁸ *NC Becomes First State To Prohibit Public Entities From Paying Ransoms Nelson Mullins* (5.4.2022) https://www.nelsonmullins.com/idea_exchange/alerts/privacy_and_data_security_alert/all/not-in-my-backyard-nc-becomes-first-state-to-prohibit-public-entities-from-paying-ransoms



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

ג. ביולי 2022 נכנס לתוקף איסור דומה בפלורידה.²⁹ החוק אוסר על רשויות מדינתיות ומקומיות,³⁰ המצויות תחת מתקפת כופרה, לשלם כופר או להיעתר לדרישות אחרות של התוקפים באופן אחר.³¹

ד. בניו-יורק תלויה ועומדת הצעת חוק האוסרת על תשלום כופר וקובעת קנס אזרחי (Civil penalty) בגין הפרת האיסור.³² אם החוק יעבור במתכונתו הנוכחית, ניו-יורק תהיה המדינה הראשונה שבה האיסור יחול גם על גורמים פרטיים, ובכלל זה אוניברסיטאות,³³ ישויות משפטיות המנהלות עסקים במדינת ניו-יורק, ומוסדות בריאות (בתי חולים, בתי אבות, מתקני בריאות אחרים המוסדרים על ידי משרד הבריאות).³⁴ עם זאת, הענישה המקסימלית היא קנס אזרחי בסך 10,000 דולר, ולכן ייתכן שיהיה בכך כדי לעודד הפרות יעילות.³⁵

האיחוד האירופי

16. ENISA המליצה שלא לשלם כופר ולא לערוך משא ומתן עם התוקפים, מפני שאין הבטחה שהתשלום יחזיר את המצב לקדמותו. שכן מדובר במשא ומתן עם גורמים עברייניים שעשויים להדליף ולמכור את המידע על אף קבלת התשלום המוסכם. כמו כן, תשלום הכופר עשוי לעודד ולממן מתקפות עתידיות.³⁶

17. ב-2017 מועצת האיחוד האירופי קבעה כלים דיפלומטיים בתחום הסייבר ("the Cyber Diplomacy Toolbox") במטרה למנוע, להרתיע ולהגיב לפעילות זדונית במרחב הווירטואלי. בין הכלים מצוי משטר סנקציות הסייבר של האיחוד האירופי, שאומץ בשנת 2019. ביולי 2020, מועצת האיחוד האירופי הטילה לראשונה סנקציות על מספר גורמים בגין מעורבותם במתקפות סייבר. במסגרת

Florida House of Representatives CS/HB 7055²⁹

<https://www.flsenate.gov/Session/Bill/2022/7055/BillText/er/PDF>

defines a state agency as any official, officer, commission, board, authority, council, committee, or³⁰ department of the executive branch of state government; the Justice Administrative Commission; the Public Service Commission; the Department of Legal Affairs; the Department of Agriculture and Consumer Services; and the Department of Financial Services. University boards of trustees and state Alfred Saikali *Florida's New* ; universities do not fall within the definition of a "state agency."
Ransomware And Cybersecurity Requirements/Restrictions JDSUPRA (11.7.2022)

<https://www.jdsupra.com/legalnews/florida-s-new-ransomware-and-8341830>

Elise Elam & Benjamin Wanger *Florida Follows North Carolina in Prohibiting State Agencies from*
Paying Ransoms, Baker Hosteler (19.7.2022) <https://www.bakerdatacounsel.com/cybersecurity/florida-follows-north-carolina-in-prohibiting-state-agencies-from-paying-ransoms/>

Senate Bill S6806A <https://www.nysenate.gov/legislation/bills/2021/s6806>³²

הסנאט במאי 2021, ועדיין נמצאת בתהליכי בחינה וחקיקה.

³³ שם, בהצעת החוק מצוינות הגדרות לגורמים שלגביהם חל החוק: "governmental entity" shall mean any state, city, town or village or local department, board, bureau, division, commission, committee, school district, public authority, public benefit corporation, council of office.

שם.³⁴

Scott Ikeda³⁵, לעיל ה"ש 27.

ENISA Threat Landscape for Ransomware Attacks (July 2022)³⁶

עמוד 11 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

משטר הסנקציות, על תושבי האיחוד האירופי ועל ישויות בו נאסר לשלם לגורמים המצויים ברשימה (בהנחה שזהות התוקף ידועה כמובן).³⁷

אוסטרליה

18. במדריך להתמודדות עם מתקפות כופרה, המרכז האוסטרלי לאבטחת סייבר (Australian Cyber Security Centre) (להלן: "ACSC") המליץ שלא לשלם כופר.³⁸

19. ממסמך מדיניות ממרץ 2021 עולה כי עמדתה של ממשלת אוסטרליה³⁹ היא כי תשלום כופר עשוי לעלות כדי עבירה פלילית. כך, ייתכן שכספי הכופר ישמשו לביצוע עבירה, ולכן העברתם עשויה להקים עבירה של הלבנת הון.⁴⁰ לחלופין ייתכן שכספי הכופר ישמשו ארגוני טרור, והעברתם תעלה כדי עבירה של מימון טרור.⁴¹

ניו-זילנד

20. ה-Computer Emergency Response Team (להלן: "CERT NZ"), צוות חירום לטיפול באירועי סייבר של ניו-זילנד, המליץ שלא לשלם כופר,⁴² מפני שהתשלום לא מבטיח שהקבצים שהוצפנו יחזרו והתשלום עשוי להפוך את המותקף למטרה עתידית.⁴³

בריטניה

21. במכתב משותף של ה-NCSC UK (המרכז הלאומי לאבטחת סייבר בבריטניה), וה-Information Commissioner's Office (להלן: "ICO")⁴⁴ ללשכת עורכי הדין, הובהר שרשויות אכיפת החוק לא מעודדות או תומכות בתשלום כופר. זאת על מנת להניא עורכי דין מלייעץ ללקוחותיהם שנקלעו למתקפת כופרה, לשלם ולהיעתר לדרישות התוקפים.⁴⁵

22. בבריטניה אין חוק המטיל איסור על תשלום כופר. עם זאת, באתר של ה-ICO צוין כי הכופר מועבר לעבריינים ולכן אין הבטחה לכך שהתשלום יביא לכך שהמידע שהוצפן יוחזר. כן, ישנה אזהרה שהתוקפים עשויים לסחוט את הקורבן בשנית. כמו כן, צוין כי תשלום כופר לא עולה בקנה אחד עם

³⁷ European council EU imposes the first ever sanctions against cyber-attacks
<https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks>

³⁸ <https://www.cyber.gov.au/ransomware/what-to-do>

³⁹ Cyber Security Industry Advisory Committee, Locked Out: Tackling Australia's Ransomware Threat (March 2021) <https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf>

⁴⁰ לפי סעיפים 400.3-400.8 לקוד הפלילי האוסטרלי.

⁴¹ לפי סעיפים 103.1-103.2 לקוד הפלילי האוסטרלי.

⁴² CERT NZ *Spotlight On Ransomware* <https://www.cert.govt.nz/it-specialists/news-and-events/spotlight-on-ransomware/>

⁴³ <https://www.cert.govt.nz/business/guides/protecting-from-ransomware/>

⁴⁴ גוף ציבורי ביצועי הכפוף למחלקה לדיגיטל, תרבות, מדיה וספורט, האחראי על רגולציה של הגנת מידע.

⁴⁵ <https://ico.org.uk/media/about-the-ico/documents/4020874/ico-ncsc-joint-letter-ransomware-202207.pdf>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

דרישת שיחזור המידע באמצעים ראויים ("appropriate measures") במקרה של אסון, הקבועה ב- General Data Protection Regulations (להלן: "GDPR"). נוסף על כך, נכתב שגם אם הוחלט לשלם את הכופר, יש לנקוט אמצעים נוספים על מנת להגן על הנתונים ולהפחית את הסיכון לנושאי המידע, מתוך נקודת הנחה שהם עדיין חשובים לפגיעה.⁴⁶

גרמניה

23. במסמך ממרץ 2020, המשטרה הפדרלית (להלן: "BKA"), BSI, והארגון הפדרלי של ארגונים מוניציפאליים, ממליצים שלא לשלם כופר ולדווח על מתקפות כופרה ל-CERT המדינתי או ל-BSI.⁴⁷ יתרה מזו, צוין כי תשלום הכופר יכול להוות עבירה פלילית, אם התשלום יממן פעילות טרור או פעילות של ארגונים עבריינים, בהתאם לחלק 129 בקוד הפלילי הגרמני.⁴⁸ ביחס לתאגידים, מצוין כי BKA במקרים בהם פעילות התאגיד מושבתת לחלוטין בשל המתקפה, ניתן לשקול לשלם כופר. במקרים בהם התאגיד שוקל לשלם את הכופר, BKA ממליץ להתייעץ עם מומחים בתחום, שכן ייתכן שישנן אפשרויות טכנולוגיות להתמודד עם המתקפה (כך למשל אם מפתח ההצפנה של המתקפה הספציפית כבר מוכר).⁴⁹

24. ממסמך של ה-BSI, עולה כי המשרד ממליץ שלא לשלם כופר, ולהשתמש בגיבויים במקום זאת. אולם, אם גם הגיבויים מוצפנים והגורם המותקף שוקל לשלם את הכופר, המסמך מפרט מספר צעדים שעל הגורם המותקף לבצע, למשל: הגורם המותקף מתבקש לדווח על התשלום לגורמי חקירה רלוונטיים ולגורמים העוסקים באבטחת IT, היכולים לסייע במו"מ על גובה הכופר.⁵⁰

צרפת

25. בספטמבר 2020 ה-National Cybersecurity Agency of France (להלן: "ANSSI") פרסם מדריך, יחד עם משרד המשפטים, בעניין מתקפות הכופרה.⁵¹ בו צוין כי מומלץ שלא לשלם כופר שכן, אין

⁴⁶ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/#scenario-7>

⁴⁷ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Ransomware-Kommunen-Empfehlung.pdf?__blob=publicationFile&v=1

⁴⁸ https://www.pinsentmasons.com.translate.google.de-de/out-law/nachrichten/cyber-angriffe-wer-loesegeld-zahlt-kann-sich-strafbar-machen?x_tr_sl=de&x_tr_tl=en&x_tr_hl=en&x_tr_pto=wapp
ראו גם: חלק 129 לקוד הפלילי הגרמני.

⁴⁹ הנחיות אלו פורסמו במסמך ייעודי לתאגידים - https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/ransomwareUnternehmenUndInstitutionen.pdf?__blob=publicationFile&v=2

⁵⁰ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=1

⁵¹ <https://www.dataguidance.com/news/france-anssi-publishes-guide-ransomware-attacks>



משרד המשפטים פרקליטות המדינה מחלקת הסייבר

הבטחה להשגת צופן הפיענוח, התשלום מסייע לעבריינים בהמשך פעילותם הפלילית ועשוי לעודד את הפושעים לתקוף את המשלם שנית.⁵²

קנדה

26. במדריך שפורסם על-ידי ה-Canadian Centre for Cyber Security,⁵³ נכתב כי ההחלטה בדבר תשלום כופר היא בידי הארגון המותקף, אך חשוב שהארגון יהיה מודע לסיכונים הכרוכים בתשלום שכזה. מכאן נראה שבקנדה לא קיימת נורמה אשר אוסרת תשלום כופר.⁵⁴

הדין הישראלי הקיים

27. בדומה למצב במרבית המדינות שנסקרו לעיל, אין בישראל נורמה משפטית ייחודית לעניין תשלום כופר במסגרת מתקפת כופרה. לצד זאת, במצבים מסוימים, ייתכן שתשלום הכופר יעלה כדי עבירה פלילית, כתלות, בין היתר, בזהות הגורם לו מועבר התשלום ובאופן העברת התשלום.⁵⁵ כך למשל, ייתכן – בנסיבות המתאימות – שתשלום הכופר יעלה כדי עבירות של מתן שירות או העמדת אמצעים לארגון טרור, עבירה לפי סעיף 23 לחוק המאבק בטרור, התשע"ו-2016 (להלן: "חוק המאבק בטרור");⁵⁶ עבירה של פעולה ברכוש טרור לפי סעיף 32(א) לחוק המאבק בטרור;⁵⁷ או עבירה של הפרת חובת דיווח לפי סעיף 33 ביחד עם 36 לחוק המאבק בטרור;⁵⁸ עבירה של מימון פעילות של ארגון פשיעה לפי סעיף 2(א)1 לחוק המאבק בארגוני פשיעה, התשס"ג-2003;⁵⁹ או עבירות מסוימות על חוק איסור הלבנת הון, התש"ס-2000 (להלן: "חוק איסור הלבנת הון").

⁵² https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_ranconiciels_tous_concernes-v1.0.pdf

⁵³ גורם ממשלתי, המספק ייעוץ והכוונה של מומחים לאבטחת סייבר לקנדים.

⁵⁴ <https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099>

⁵⁵ וכמובן שעל מנת להקים אחריות פלילית נדרשת לכל הפחות מודעות של המשלם לזהות התוקף, לו מועבר התשלום.
⁵⁶ "הנותן לארגון טרור שירות או המעמיד לרשותו אמצעים, ויש במתן השירות או בהעמדת האמצעים כדי לסייע לפעילות הארגון או לקדמה, דינו – מאסר חמש שנים, אלא אם כן הוכיח שלא היה מודע לכך שהארגון הוא ארגון טרור; לעניין זה, "היה מודע" – לרבות חשד ונמנע מלברר."

⁵⁷ "העושה אחת מאלה דינו – מאסר שבע שנים או קנס פי עשרה מהקנס הקבוע בסעיף 61(א)4 לחוק העונשין: (1) פעולה ברכוש שיש בה כדי לסייע, לקדם או לממן ביצוע של עבירת טרור חמורה או לתגמל בעבור ביצוע של עבירת טרור חמורה גם אם מקבל התגמול אינו מי שביצע את העבירה או התכוון לבצעה; לעניין פסקה זו, די שיוכח כי עושה הפעולה היה מודע לכך שמתקיימת אחת האפשרויות האמורות גם אם לא יוכח איזו מהן; (2) פעולה ברכוש של ארגון טרור או רכוש הקשור לעבירת טרור חמורה; (3) מעביר רכוש לארגון טרור."

⁵⁸ 33. התבקש אדם לעשות פעולה ברכוש במהלך עסקיו או במילוי תפקידו, או בנסיבות שבהן היתה לו אפשרות של ממש לביצוע הפעולה, והיה לאותו אדם חשד סביר שמתקיים האמור בפסקה (1) או (2), או עשה אדם פעולה ברכוש, והיה לו במועד עשייתה או בתוך שישה חודשים מהמועד האמור, חשד סביר כאמור, ידווח על כך למשטרת ישראל [...]; 36. לא מסר אדם דיווח לפי הוראות סעיפים 33 או 34, דינו – מאסר שנה או קנס כאמור בסעיף 61(א)3 לחוק העונשין [...]. והכול אם לא הוכיח כי לא היה מודע שהארגון הוא ארגון טרור; לעניין זה, "היה מודע" – לרבות חשד ונמנע מלברר."
⁵⁹ "מממן במישרין או בעקיפין פעילות של ארגון פשיעה או מקבל מימון לצורך הפעלת הארגון, או מחליט בעניין חלוקת כספים בארגון פשיעה."

עמוד 14 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

עמדות שהובעו בפני צוות המשנה

28. במהלך הדיונים של צוות המשנה, בימים 21.9.2022 ו-28.9.2022, ככלל, הייתה הסכמה בין המשתתפים כי אין מקום להטיל איסור גורף על תשלום כופר במקרה של מתקפת כופרה, כאשר נימוקים שונים הועלו לצורך ביסוס עמדה זו. להלן נפרט נימוקים אלה.
29. מר טיראן פרטוק ציין שכיום התשלום מתבצע, באופן טבעי, בלית ברירה, וכאשר אין פתרון אחר. לכן, הוא מעריך כי הטלת איסור תשלום כופר יביא להתפתחות של שוק "אפור" או "שחור", בו תשלומי הכופר יתבצעו על ידי גופים מפוקפקים.
30. נציגי רשות שוק ההון ציינו כי הם סבורים שטרם בשלה העת לקבוע נורמה משפטית בעניין תשלום כופר. מחד גיסא, ככל שהמניע לתקיפה הוא כלכלי, קביעת איסור תשלום כופר עשויה לסייע בצמצום התופעה, על ידי הקטנת התמריץ לתקיפה. כאשר התוקף הוא ארגון טרור, ייתכן ותשלום הכופר יהיה אסור תחת חוק המאבק בטרור. מאידך גיסא, לעיתים שיקולי יעילות מטים את הכף לעבר תשלום הכופר, שכן עלויות ההתאוששות ממתקפת כופרה עשויות להיות גבוהות בהרבה מהכופר המבוקש, וכן במקרים רבים הגוף המותקף מבוטח, ולכן הוא משופה בגין התשלום. כמו כן, בתור גוף רגולטורי, ציינו נציגי רשות שוק ההון כי הם סבורים שאיסור על תשלום כופר אינו אכיף ואינו ישים. לצד זאת, סייגו ואמרו כי עמדתם נוגעת לגופים פרטיים, ולא לגופי מדינה.
31. נציגת מחלקת ייעוץ וחקיקה (משפט פלילי) ציינה כי מבחינה משפטית, בהיבטים של עקרון האשמה ועקרון שיוריות הדין הפלילי, ביחס לאנשים פרטיים, קיים קושי להטיל אחריות פלילית על משלם הכופר, שהוא – אחרי הכל – קורבן העבירה.
32. נציגי מס"ל ציינו כי אין מקום לאיסור פלילי גורף. לגישתם, הכיוון המתאים הוא הטלת חובת יידוע ודיווח.
33. נציגת הרשות לאיסור הלבנת הון ציינה כי תשלום כופר עשוי להיכלל במסגרת המשטר הקיים של איסור הלבנת הון, במיוחד בשים לב שהמשלם הוא לא תמיד הנפגע עצמו, אלא גוף פיננסי או גוף אחר לניהול משברים. עוד ציינה כי היא תומכת בהסדרת הסוגיה דרך חובות דיווח, אשר כבר קיימות כיום בתחום של איסור הלבנת הון ומימון טרור.
34. מר דורון הדר ציין שישנה חשיבות בשימור מנעד רחב של אפשרויות פעולה באירועי מתקפות כופרה, לרבות תשלום כופר. זאת, בעיקר בשל שיקולי יעילות. מר הדר שיתף מניסיונו האישי כי לעתים מזומנות לקוחותיו מעדיפים לשלם את הכופר כדי שהמידע לא יפורסם וכדי למנוע נזק תדמיתי. מעבר לגוף המותקף עצמו, ציין שיש לקחת בחשבון את האינטרסים של שחקנים נוספים המושפעים ממתקפת הכופרה, ובכלל זה חברות הביטוח של הגופים המותקפים. מר הדר ציין כי לרוב חברות הביטוח של הגופים הגדולים בישראל הן חברות זרות. עוד במסגרת מכלול השיקולים הכלכליים, ציין

עמוד 15 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

כי במספר אירועים לאחרונה, בהם החברה המותקפת בחרה שלא לשלם את הכופר, הוגשו תובענות ייצוגיות עקב דליפת המידע. לכן, לרוב העדיפות של חברות הביטוח תהיה לשלם את הכופר, הן בשל הרצון לגדר את הסיכון ולתחמומו. בהקשר זה התייחס לכך שאחת מחברות הביטוח הגדולות, Lloyd's, פרסמה לאחרונה את עמדתה לפיה פוליסת הביטוח לא תחול על אירוע תקיפה סייבר שבוצעה על ידי גורם מדינתי.⁶⁰ לבסוף סיכם וחזר על כך שהוא סבור שקיים קושי בהחלטה אפריורית בדבר דרך הפעולה הראויה להתמודדות עם מתקפת כופרה, וכי הוא סבור שאמירה גורפת מגבילה את הליך קבלת ההחלטות ולעיתים מייצרת קשיים בכך שלא תמיד ניתן לאכוף את ההנחיה.

35. פרופ' טל ז'רסקי הציג רקע תיאורטי לסוגיה של תשלום כופר, והפנה, בין היתר, למאמריו של פרופ' טום בייקר (Baker) מאוניברסיטת פנסילבניה. ציין שכיום, בשל העובדה שהמדינה לכאורה שותקת בשאלה האם יש לשלם כופר או לא, ההחלטה הזו נופלת לידיהם של גורמים מייעצים או גופי ביטוח. בעבר, משום שסכומי הכופר שנדרשו היו נמוכים יחסית, ההכרעה התרכזה אצל עורכי הדין העוסקים בסוגיות פרטיות ומומחי סייבר. כיום, בשל העלייה העצומה בסכומים הנדרשים, אירועי מתקפות כופרה הם מורכבים יותר, וחברות פונות לגורמים המומחים בניהול מו"מ. הצטרף לדבריו של מר דורון הדר, לפיהם הגופים המותקפים חוששים מפני תביעות, ולכן כאשר מתקבלת ההחלטה על דרך פעולה במסגרת אירוע מתקפת כופרה, היא נבחנת, בין היתר, לפי מבחן סבירות. הציג את עמדתו לפיה מעורבותה של המדינה בהחלטה האם לשלם כופר אם לא צריכה להתמצות בסיוע בזיהוי התוקף ומניעיו ושיתוף הגוף המותקף במידע מודיעיני, על מנת לסייע לו לקבל את החלטתו.

איסור פרסום של מתקפת כופרה

36. ראשית, נסקור את המצב הקיים במדינות שונות ביחס לשאלת איסור פרסום על אודות מתקפות כופרה, בשים לב לזכויות המתנגשות, העשויות לגזור חובות ליידע את נושאי המידע על המידע שדלף בעקבות המתקפה ונוגע אליהם. ככלל, במרבית המדינות יש חובה לעדכן באופן מיידי, בכפוף לחריגים, את נושאי המידע בדבר תקריות אבטחת סייבר הכוללות דלף של מידע אישי. לעיתים, כשלא ניתן לדווח לנושאי המידע באופן אפקטיבי, יש לפרסם הודעה בתקשורת בדבר האירוע. שנית, נפרט על אודות הוראות בדין הישראלי הקיים הנוגעות לאיסורי פרסום היכולות להיות רלוונטיות למתקפות כופרה, הצעת חוק בעניין איסור פרסום זמני של אירוע סייבר, וכן הוראות הנוגעות לחובת יידוע של נושאי המידע שדלף בעקבות המתקפה. שלישית, נציג את העמדות השונות שהובעו במהלך דיוני צוות המשנה בעניין זה. לבסוף, נסכם ונציג את המלצותינו.

⁶⁰ <https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

סקירה משווה

ארצות הברית

37. בנובמבר 2021, משרד המפקח על הסחר במטבע (Comptroller of the Currency), הדירקטוריון של הבנק הפדראלי האמריקני (Board of Governors of the Federal Reserve System) והתאגיד הפדראלי לביטוח פיקדונות (Federal Deposit Insurance Corporation) פרסמו הנחיה פדרלית, המחייבת ארגונים בנקאיים לדווח לרגולטור על תקריות אבטחת סייבר בתוך 36 שעות מרגע זיהוין. כמו כן, ההנחיה מחייבת גופים פיננסיים **לדווח ללקוחותיהם** על תקריות ואירועי סייבר במקרים בהם התקרית הובילה לשיבושים במתן שירותים למשך יותר מארבע שעות.⁶¹ ההנחיה נכנסה לתוקף ב- 62.1.5.2022

38. במסמך מטעם CISA העוסק בהגנה על מידע רגיש ואישי במסגרת מתקפות כופרה, CISA ממליצה שבהינתן גניבה או הדלפה של מידע אשר אוחסן על ידי חברות אחרות, או כאשר מידע אישי נגנב או מודלף, **יש לייצע את בעלי המידע בדבר האירוע.**

39. כאשר מדובר במידע בריאותי של אזרחים, ייתכן שתקום בנוסף חובת דיווח ל-Federal Trade Commission (להלן: "FTC"), ובמקרים מסוימים גם לתקשורת.⁶³ החוק הפדרלי The Health Insurance Portability and Accountability Act of 1996 (להלן: "HIPAA") כולל Notification Rule, לפיו מחזיקים במידע אישי ובריאותי של אזרחים או תושבים אמריקאים חייבים לייצע נושאי המידע הבריאותי, כאשר מתרחש אירוע של הדלפת מידע בריאותי המוגן אלקטרונית (Electronic Protected Health Information – EPHI). במקרה שהדלפה כוללת מידע בריאותי של יותר מ-500 תושבים, קיימת דרישה מצד הגוף הנתקף לייצע את התקשורת ללא דיחוי בלתי סביר, ובכל מקרה לא יאוחר מ-60 יום לאחר גילוי הדלפת המידע. HIPAA קובע את אופן היידוע, את המועד בו יש לייצע ואת תוכן ההודעה.⁶⁴ על-פי חלק 164.412 ל-Breach Notification Rule, ניתן לדחות את חובת היידוע, ההתראה או הפרסום אם גורם אכיפת חוק מצהיר בפני הגוף הנתקף שאלו יסכלו ("impede") חקירה פלילית, או יובילו לפגיעה בביטחון הלאומי. אם ההצהרה ניתנת בכתב ומפרטת את המועד שעד אליו יש לדחות את חובת היידוע, יש להמתין עם היידוע עד למועד הנקוב בהצהרה.

⁶¹ Department of Treasury *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (November 2021) <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf>
⁶² Office of the comptroller of the currency *Information Technology: OCC Points of Contact for Banks* (29.3.22) <https://www.occ.gov/news-Computer-Security Incident Notifications>
⁶³ FDIC *Computer-Security Incident Notification ; issuances/bulletins/2022/bulletin-2022-8.html Implementation* (29.3.22) <https://www.fdic.gov/news/financial-institution-letters/2022/fil2022.html>
⁶⁴ CISA *Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches* https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

לחלופין, אם ההצהרה ניתנת בעל-פה, יש לתעד את ההצהרה ואת זהות הגורם המצהיר, ולדחות את היידוע באופן זמני, ולכל היותר ל-30 ימים מרגע ההצהרה, למעט במצב בו ניתנת הצהרה בכתב במהלך תקופה זו.⁶⁵

40. נוסף על כך, ה-FTC פרסמה Health Breach Notification Rule, המרחיב את תחולת ה-Breach Notification Rule הקבוע ב-HIPAA. מטרת הכלל של ה-FTC הוא לוודא שישויות שאינן מכוסות על-ידי HIPAA ומחזיקות במידע אישי ובריאותי של אזרחים ותושבים אמריקאים יהיו אחראיות לעדכן אזרחים ואת התקשורת (בתנאים המפורטים לעיל), כאשר מידע בריאותי שבאחזקתם דלף.⁶⁶ חלק 318.4, אשר מתייחס לזמני חובת היידוע, מכיל "חריג אכיפת חוק" הדומה לחריג שפורט בפסקה לעיל, לפיו הגוף הנתקף יכול לדחות את מועד היידוע בהתאם להחלטה של גורם אכיפת חוק שהיידוע, ההתראה או הפרסום יסכלו חקירה פלילית או יגרמו נזק לביטחון הלאומי. באשר לאופן בו מעדכן גורם אכיפת החוק את הגוף הנתקף (בכתב או בעל-פה), והדחייה הנגזרת מכך, ההוראות זהות לאלו שפורטו בפסקה לעיל.⁶⁷

אוסטרליה

41. ביוני 2021 הוגשה מטעם השר לאבטחת סייבר הצעת "חוק תשלומי כופר", אשר תחייב גופים ציבוריים ופרטיים (למעט עסקים קטנים) לדווח ולמסור מידע ל-ACSC על תשלומי הכופר שביצעו, בהקדם האפשרי, ולכלול בדיווח ל-ACSC את כל הפרטים המנויים בסעיף 8 לחוק (כגון: סכום התשלום, ארנק מטבעות קריפטוגרפים אליו הועבר התשלום, זהות התוקף וכדומה). עוד הוצע, במסגרת סעיף 9 לחוק, להסמיך את ACSC לרכז את המידע, להעביר את המידע **שנמסר לידי אדם או ציבור רלוונטי** לגבי איום הסייבר הנוכחי, וכן למסור מידע לרשויות המדינה למטרות הנוגעות לאכיפת החוק.⁶⁸ נכון למועד כתיבת שורות אלה, הצעת החוק לא הבשילה לכדי חוק.

⁶⁵ HIPAA Administrative Simplification, Subpart D - Notification in the Case of Breach of Unsecured Protected Health Information

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>

⁶⁶ Part 318 - Health Breach Notification Rule <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>; https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

Federal Trade Commission *Health Breach Notification Rule* <https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule>

⁶⁷ חריג אכיפת החוק אינו מפנה ל-HIPAA, אלא לקוד התקנות הפדרלי (Federal Regulations Code), שהוראותיו זהות לאלו המופיעות ב-HIPAA. ראו גם: Part 318 - Health Breach Notification Rule <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318>

⁶⁸ לדברי ההסבר להצעת החוק ראו: https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6730_ems_d739fac8-4027-422a-ae6a-b4c9af752b4c/upload_pdf/21085EMWatts.pdf;fileType=application%2Fpdf; https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6730_first_reps/toc_pdf/21085b01.pdf;fileType=application%2Fpdf את סטטוס הצעת החוק ניתן למצוא כאן: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bid=s1313



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

42. באוסטרליה, ה-Privacy Act מתווה את אופן הניהול של מידע אישי של פרטים, לרבות אופן השמירה על מידע זה, אופן השימוש בו ועוד.⁶⁹ החוק מטיל אחריות על סוכנויות ממשל אוסטרליות וכן על ארגונים עם מחזור של יותר מ-3 מיליון דולר, בכפוף לחריגים מסוימים.⁷⁰ חוק הפרטיות האוסטרלי מחייב כל גוף שכפוף אליו **לדווח לפרטים** ול-Office of the Australian Information Commissioner (להלן: "OAI") כאשר תקרית של הדלפת מידע ("Data Breach") עשויה להוביל לפגיעה בפרט. התנהלות זו חלה גם במקרים של מתקפות כופרה, כאשר המתקפה משלבת פגיעה במידע רגיש שיכולה להשפיע על פרטים.⁷¹ חוק הפרטיות האוסטרלי מונה חריגים לחובת יידוע זו:⁷² (1) כאשר הדלפת מידע בגוף אחד מהווה בפועל הדלפה של מידע המוחזק גם בידי גופים נוספים, חובת היידוע לא חלה על אותם גופים נוספים.⁷³ (2) כאשר הדלפת המידע מתרחשת בגוף אכיפה, ולראש הגוף (Chief Executive Officer) יש יסוד סביר להניח שקיום חובת היידוע יפגע בפעילות האכיפה של אותו גוף.⁷⁴ (3) כאשר חובת היידוע המפורטת בחוק הפרטיות האוסטרלי אינה עולה בקנה אחד עם הוראות סודיות⁷⁵, חובת היידוע לא תחול על הגוף לגביו מתרחשת הסתירה (אך ורק במידה המתחייבת מאותה סתירה). זאת ועוד, אם מדובר בהוראת סודיות הקבועה בתקנות, ומילוי חובת היידוע יסתור הוראה זו, חובת היידוע לא תחול על הגוף.⁷⁶ (4) כאשר הממונה מחליט שחובת היידוע לא תחול באחת מהנסיבות הבאות: בשל האינטרס הציבורי, בהתאם להמלצה מצד גוף אכיפה או מנהלת האותות האוסטרלית, או לפי כל עניין אחר שהממונה מחשיב כרלוונטי.⁷⁷

ניו זילנד

43. ב-2020 תוקן חוק הפרטיות (Privacy Act) של ניו-זילנד. התיקון מתמקד בהפרות פרטיות שיש לדווח עליהן, ומחייב עסקים וארגונים לדווח לממונה על הפרטיות בניו-זילנד על תקריות של הפרות פרטיות שהובילו לפגיעה באדם, או שסביר שיגרמו לפגיעה כזו. אי-דיווח יכול לעלות לכדי עבירה, ולתשלום של קנס בגובה \$10,000.⁷⁸

⁶⁹ <https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities#OrgAndAgencyPrivacyActCovers>
וגם <https://www.legislation.gov.au/Details/C2021C00452>

⁷⁰ <https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities#OrgAndAgencyPrivacyActCovers>
⁷¹ <https://www.cyber.gov.au/ransomware/what-to-do>

⁷² Australian Privacy Act 1988, Notification of Eligible data breaches, Division, Subdivision B- General Notification Obligations- <https://www.legislation.gov.au/Details/C2021C00452>

⁷³ חלק 26WM לחוק.

⁷⁴ חלק 26WN לחוק.

⁷⁵ "Secrecy Provisions"- הכוונה להוראות המנויות באחד מחוקי חבר העמים הבריטי (ה-Commonwealth), האוסרות או מפקחות על שימוש במידע או על חשיפתו.

⁷⁶ חלק 26WP לחוק.

⁷⁷ חלק 26WQ לחוק.

⁷⁸ <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Act-2020-information-sheets-full-set.pdf>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

44. נוסף על כך, תקרית של הפרת פרטיות **מחייבת ליידע פרטים** שמושפעים מכך, בתנאי שההפרה עשויה לגרום נזק ממשי לפרטים המושפעים. על מנת לבחון האם צפוי להיגרם נזק ממשי יש לקחת בחשבון את רגישות המידע,⁷⁹ זהות הגורם הלא מורשה שבידיו המידע,⁸⁰ סוג הנזק,⁸¹ סבירות התרחשות הנזק ואמצעי האבטחה שנקטו.⁸² באתר הממונה על הפרטיות בניו-זילנד קיים סקר עם שאלות מנחות על מנת לסייע לגופים שהותקפו להעריך האם עליהם לדווח.⁸³

45. לחוק הפרטיות תחולה אקסטרטריטוריאלית, והוא חל על עסקים וארגונים הפועלים בניו-זילנד, גם אם אין להם נוכחות פיזית במדינה. כך למשל, החוק חל גם על גופים כמו פייסבוק וגוגל.

46. הממונה על הפרטיות בניו-זילנד ציין שתיקון זה חל גם על תקריות של מתקפות כופרה, כאשר התוקף משיג גישה למידע אישי, גונב אותו או מונע גישה אליו. חלק 114 לחוק מחייב ארגון ליידע את הממונה על פרטיות על הפרת פרטיות כזו.⁸⁴ חלק 115 לחוק מחייב את הגוף המותקף ליידע את הפרט הנוגע לדבר או ליידע את הציבור בכללותו על הפרת הפרטיות.⁸⁵ החוק קובע כי על הארגון ליידע את הפרט הנוגע לעניין, מהר ככל האפשר מרגע גילוי ההפרה, פרט למקרים בהם לא ניתן ליידע את הפרט באופן סביר ואז יש לפרסם על ההפרה לציבור הרחב. בהמשך לכך, החוק מונה את התנאים בהם יש למסור את ההודעה לציבור הרחב: ההודעה אינה יכולה לפרסם פרטים מזהים של גורם שהושפע מהפרת הפרטיות; על ההודעה להתפרסם בהתאם לתנאים המצויים בחלק 215(1)(a).⁸⁶

47. בחלק 116 מצויים החריגים לכלל המעניקים פטור או עיכוב לחובת היידוע לפרט או לציבור. קיים פטור מחובת יידוע לפרט או לציבור כאשר אלו עשויים לפגוע בביטחון המדינה או ביחסי הבינלאומיים; כאשר ההודעה עשויה לפגוע בחוק אחר שהמגזר הציבורי אמון על ביצועו (מניעה של עבירה, חקירות או זכות להליך הוגן), לחשוף סוד מסחרי, או לסכן שלומו של אדם. ניתן לעכב את היידוע לפרט או לציבור (אך לא לממונה) כאשר אלו עלולים לסכן את אבטחת המידע האישי, והסיכון עולה על יתרונות יידוע נושאי המידע, ורק לתקופה בה הסיכון גובר על היתרונות. ניתן להסתמך על

⁷⁹ Sensitive information can be, for example, about someone's health, political or religious beliefs, or financial information. Context is important. Information that is not sensitive in one situation might be very sensitive in another.

⁸⁰ למשל גורם שעשוי לגרום לנזק, גורם שאינו משתף פעולה, גורם אינו ידוע.
⁸¹ נזק תעסוקתי, התחזות, נזק רגשי, נזק כלכלי, איבוד מידע, נזק פיזי, איומים, פגיעה במוניטין, אובדן הזדמנויות, אפליה או נזק אחר.

⁸² <https://legalvision.co.nz/data-privacy-it/notifiable-privacy-breach>
⁸³ "Do I Need To Notify?" <https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/evaluate>

⁸⁴ חלק 114 – הודעה לממונה על פרטיות <https://www.privacy.org.nz/blog/opc-sends-warnings-to-organisations-to-get-it-right-next-time>

⁸⁵ חלק 115 – הפרטים המושפעים: <https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23504.html>

⁸⁶ שם.



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

החריגים המעניקים פטור או עיכוב בהודעה לפרט או לציבור רק אם יש לה יסוד סביר כי החריג חל או העילה לעיכוב קיימת.⁸⁷

האיחוד האירופי

48. ה-GDPR, רגולציית הגנת הפרטיות של האיחוד האירופי, חלה בתחומי האיחוד וגם על ארגונים מחוץ לאיחוד האירופי, ככל שהם אוספים מידע הנוגע לאזרחים של האיחוד האירופי. סעיף 34 ל-GDPR קובע כי במקרה שהדלפת מידע אישי צפויה לגרום לסיכון גבוה לזכויות ולחירויות של נושאי המידע, על בעל המידע להודיע על הדלפת המידע האישי לנושאי המידע ללא דיחוי מופרז. במקרים הבאים בעל המידע לא נדרש להודיע לנושאי המידע על הדלפת המידע על הדלפת המידע: כאשר בעל המידע יישם אמצעים המגנים על המידע, בפרט כאלו שהופכים את המידע לבלתי מובן לגורם שאינו מורשה (למשל הצפנה); בעל המידע נקט בצעדים לאחר ההדלפה המונעים את התממשות הסיכון לזכויות ולחירויות; ההודעה לנושאי המידע כרוכה במאמץ לא פרופורציונלי. במקרה האחרון, יש להודיע על ההדלפה בתקשורת, או באופן דומה. כאשר בעל המידע טרם הודיע לנושאי המידע על הדלפת המידע, הרשות המפקחת יכולה לדרוש ממנו לעשות כן, ככל שהחריגים שפורטו אינם מתקיימים. זאת לאחר ששקלה את הסבירות שהדלפת המידע האישי תגרום לסיכון גבוה.⁸⁸

49. לפי סעיף 86 ל-GDPR, על הדיווח לנושאי המידע להיעשות בשיתוף פעולה עם הרשות המפקחת, תוך כיבוד הנחיותיה או הנחיות רשות רלוונטית אחרת, כגון רשות אכיפת החוק. אופן הדיווח יהיה תלוי באינטרס הציבורי (למשל, צמצום סיכון מידע, שיצדיק דיווח מהיר, מול הצורך לנקוט בצעדים נגד הפרות דומות, שיצדיק עיכוב).⁸⁹ נוסף על-כך, לפי סעיף 87, ביידוע נושאי המידע ללא דיחוי, יילקח בחשבון טיבה וחומריתה של הדלפת המידע, יחד עם השלכותיה השליליות על נושאי המידע. עוד צוין, כי יידוע שכזה עשוי להביא להתערבותה של הרשות המפקחת בכפוף לסמכויותיה.⁹⁰ זאת ועוד, בסעיף 88 מצוין כי בעת קביעת הכללים לעניין הפורמט והנהלים בדבר יידוע נושאי המידע, יש לקחת בחשבון את האינטרסים של רשויות אכיפת החוק במקרים בהם חשיפה מוקדמת עלולה להקשות שלא לצורך על חקירת נסיבותיה של הדלפת המידע.⁹¹

50. באיחוד האירופי ישנה רשת של (CSIRTs) (Computer Security Incident Response Team), המורכבת מ-CSIRT של מדינות האיחוד. לפי דירקטיבה של הפרלמנט והמועצה האירופיים משנת 2016, על מזכירות ה-CSIRT לפרסם אירועים על תקריות סייבר שהתרחשו במדינות האיחוד

⁸⁷ חלק 116 קובע שורה של נסיבות נוספות בהן קיים פטור מחובת יידוע לפרט או לציבור: כאשר האדם נשוא הפגיעה קטן מגיל 16 והארגון סבור שההודעה תהיה מנוגדת לאינטרסים שלו, כאשר לאחר התייעצות עם רופא הארגון סבור כי ההודעה עשויה לפגוע בבריאותו.

<https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23506.html#LMS23506>

⁸⁸ [/https://gdpr-info.eu/art-34-gdpr](https://gdpr-info.eu/art-34-gdpr)

⁸⁹ [/https://gdpr-info.eu/recitals/no-86](https://gdpr-info.eu/recitals/no-86)

⁹⁰ [/https://gdpr-info.eu/recitals/no-87](https://gdpr-info.eu/recitals/no-87)

⁹¹ [/https://gdpr-info.eu/recitals/no-88](https://gdpr-info.eu/recitals/no-88)



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

האירופי באתר ייעודי.⁹² דירקטיבה זו חלה על גופים ציבוריים המזוהים כמפעילים שירותים חיוניים. תחת פרק 4, אשר עוסק באבטחת הרשת ואבטחת מערכות המידע של מפעילי שירותים חיוניים, במסגרת סעיף 14, העוסק ביידוע על תקריות סייבר, CSIRT יכול לייצע את הציבור (או לדרוש מהחברה המותקפת לעשות כן) על תקריות שבהן מודעות ציבורית היא הכרחית למניעת תקרית, או לשם התמודדות עם תקרית מתמשכת.⁹³ לכלל זה ישנו חריג לפיו המדינות החברות יכולות לסטות ממועדי היידוע הקבועים במקרים מוצדקים לפי דין ובהסכמה של הרשויות המוסמכות או של ה-CSIRT.⁹⁴

51. במהלך שנת 2020 האיחוד האירופי גיבש דירקטיבה שעתידה להחליף את הדירקטיבה הקיימת מ-2016 שצוינה לעיל. דירקטיבה זו עומדת בפני אישור של מדינות האיחוד האירופי והפרלמנט האירופי.⁹⁵ סעיף 20 לדירקטיבה החדשה פורש את חובת הדיווח של החברות המותקפות,⁹⁶ ומפרט שבמקרים מתאימים, בהם התקרית עשויה להשפיע על מתן השירות, על גוף מותקף לייצע את מקבלי השירות על התקרית.⁹⁷

בריטניה

52. באתר ה-ICO, בלשונית שפונה לארגונים, מצוי מידע על "Personal Data Breach", הדלפה של מידע אישי. באתר נכתב כי לפי ה-UK GDPR (סעיף 34, בדומה לדין החל באיחוד האירופאי) אם ההדלפה עשויה לסכן באופן משמעותי זכויות וחירויות של הפרט, על הארגון לידע את הפרטים נושאי המידע ללא דיחוי. עוד מצוין, כי על מנת להעריך את מידת הפגיעה הפוטנציאלית לפרט יש לבחון את ההשלכות השליליות הפוטנציאליות שיכולות להיגרם לפרט ומידת הסבירות שאלו יתממשו. כך למשל, הסתברות גבוהה של נזק פיזי, אובדן שליטה על הנתונים האישיים, הגבלת זכויות, אפליה, גניבת זהות או הונאה, אובדן כספי, פגיעה במוניטין, אובדן סודיות של נתונים אישיים המוגנים בסודיות מקצועית או כל חיסרון כלכלי או חברתי משמעותי אחר לאדם הנוגע בדבר – תקים עילה לפרט לדרישת יידוע על הדלפת המידע.

53. ה-DPA (The Data Protection Act 2018) מעגן מספר חריגים לחובות המנויות ב-UK GDPR, ביניהן פטור אפשרי מחובת היידוע על הדלפת מידע אישי לסוגים מסוימים של גופים. למשל: (1) חריג פשיעה ומיסוי – כאשר הגוף המותקף מעבד מידע אישי למטרות מניעה וגילוי של פשע, תפיסה או העמדה לדין של עבריינים, שומה או גבייה של מס או חובה בעלת אופי דומה; (2) חריג הגנה על

⁹² <https://eur-lex.europa.eu/eli/dir/2016/1148/oj> - בפס' 40.

⁹³ שם, בסעיף 14.

⁹⁴ שם, בעמוד 47.

⁹⁵ <https://www.technologylawdispatch.com/2022/01/data-cyber-security/cybersecurity-2-0-european-parliament-adopts-new-draft-directive>

⁹⁶ [https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0823/COM_COM\(2020\)0823_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0823/COM_COM(2020)0823_EN.pdf)

– בעמוד 46.

⁹⁷ שם, בעמוד 47.



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

הביטחון הלאומי – כאשר הגוף המותקף מעבד מידע אישי למטרת הגנה על הביטחון הלאומי (איומים ספציפיים מארגוני טרור או מדינות עוינות, הגנה על מטרות פוטנציאליות ושיתוף פעולה עם מדינות אחרות).⁹⁸

54. נוסף על כך, באתר מצוי הסבר על האופן שבו הארגון צריך ליידע את הפרט על ההדלפה. כך, על תיאור ההדלפה להיות בשפה ברורה, עליו לכלול את האופי ההדלפה, איש קשר לקבלת אינפורמציה נוספת, ההשלכות הצפויות מההדלפה, תיאור של הצעדים שנקטים על מנת להתמודד עם ההדלפה מטעם הארגון לצמצום הנזק ועוד. נוסף על כך, מומלץ לתת לפרט המלצות לגבי הצעדים שהוא יכול לנקוט על מנת להגן על עצמו.⁹⁹

גרמניה

55. ה-GDPR מכיל סעיפים "פתוחים" שבאמצעותם חברי האיחוד האירופי יכולים לחוקק חוקי פרטיות, שיסייעו להטמיע את הסטנדרט של ה-GDPR.¹⁰⁰ בגרמניה, נחקק החוק German Federal Data Protection Act (להלן: "BDSG"). לפי סעיף 1(1), החוק חל על גופים ציבוריים המשויכים לפדרציה, גופים פרטיים ועוד. סעיף 66(1) ל-BDSG¹⁰¹ מחיל חובת יידוע על הפרות מידע לפרטים, היכולות לפגוע באינטרסים של אותם פרטים.¹⁰² סעיף 29(1) לחוק הגרמני קובע שחובת היידוע לפרט בגין הפרת מידע אישית, בהתאם לסעיף 34 ל-GDPR, לא תחול, אם חובה זו תוביל להסגרת מידע שלפי חוק או מעצם מהותו, צריך להישמר בסוד, ובפרט בשל אינטרס לגיטימי של גורם צד שלישי.

קנדה

56. ה-Personal Information Protection and Electronic Documents Act (להלן: "PIPEDA") הוא חוק פדרלי, העוסק באופן שבו עסקים מתמודדים עם המידע האישי שברשותם. לפי חוק זה, כל עוד אין איסור לפי חוק אחר, על הארגון להודיע לפרטים נושאי המידע על הפרה של אמצעי אבטחה הנוגעים למידע אישי שבשליטתו. אולם, אין ציפייה שארגון ידווח על כל הפרה, אלא רק כאשר בנסיבות העניין סביר להאמין שההפרה יוצרת סיכון ממשי לפגיעה משמעותית לפרט (בלשון החוק - real risk of significant harm, להלן: "RROSH"). מצוין כי הנזק לא יימדד לפי כמות הפרטים

⁹⁸ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-exemptions>

⁹⁹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa>

¹⁰⁰ <https://www.iltanet.org/blogs/david-tremont/2020/02/06/bdsg-or#:~:text=Basically%2C%20the%20objective%20of%20the,GDPR%20is%20considered%20a%20superior>

¹⁰¹ https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.html

¹⁰² <https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2019/cyber-incident-response-and-data-breach-notification-germany-2019.pdf>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

הנפגעים, ומספיק שקיים נפגע אחד שעלול להיפגע משמעותית.¹⁰³ במסגרת PIPEDA, ארגונים חייבים גם לשמור תיעוד של כל הפרות אבטחת המידע, גם אלו שאינן עומדות בסף הסיכון של "סיכון ממשי לנזק משמעותי".

57. RROSH כולל: פגיעה משמעותית לרבות פגיעה גופנית, השפלה, פגיעה במוניטין או במערכות יחסים, אובדן תעסוקה, הזדמנויות עסקיות או מקצועיות, הפסד כספי, גניבת זהות, נזק לרכוש או אובדן רכוש. על מנת לקבוע האם ההפרה יוצרת סיכון ממשי לפגיעה משמעותית, יש לבחון את **מידת רגישות** המידע האישי הכרוך בהפרה **וההסתברות** שיעשה בו שימוש לרעה.¹⁰⁴ על הארגון ליידע את הפרט בהקדם האפשרי, ההודעה חייבת להינתן באופן ישיר לאדם (בדוא"ל, בטלפון, דואר או צורה סבירה אחרת בכפוף לנסיבות העניין) באופן בולט וברור, למעט בנסיבות מסוימות המתוארות בתקנות שבהן הודעה עקיפה מותרת (למשל, כשהודעה ישירה עשויה לגרום לנזק נוסף לאדם המושפע, הודעה ישירה עלולה לגרום לקושי מיותר לארגון או לארגון אין מידע ליצירת קשר עבור האדם המושפע). על ההודעה לכלול את הפרטים המפורטים בתקנון, בין היתר: תיאור נסיבות ההפרה, מועדה הידוע או המשוער, תיאור המידע האישי ששוא ההפרה, תיאור הצעדים שהארגון נקט להפחתת הסיכון לפגיעה משמעותית ועוד.¹⁰⁵

58. על-פי סעיף 38.13 לחוק הראיות הקנדי (Canada Privacy Act), התובע הכללי (Attorney General) של קנדה רשאי להנפיק תעודה האוסרת על גילוי מידע כאשר המידע הושג באופן סודי מגורם זר, או לצורך הגנה על הביטחון הלאומי.¹⁰⁶ בפרק תחולתו (Application) של ה-PIPEDA מצוין כי במקרה שבו הונפקה תעודה האוסרת על גילוי מידע בהתאם לסעיף 38.13 לחוק הראיות הקנדי, לממונה ולכל מי שפועל מטעמו אסור לגלות מידע החוסה תחת תעודה זו, ועל אותו גורם לנקוט בכל אמצעי זהירות סביר כדי להימנע מחשיפת המידע האסור בגילוי.¹⁰⁷ מכאן שכאשר מידע שדלף מארגון מותקף היה כפוף לתעודה שכזו, הוא יהיה אסור בגילוי, על אף חובת הדיווח הקבועה ב-PIPEDA שפורטה לעיל.

59. כמו כן, לפי חוק הפרטיות הקנדי, ארגון המחזיק במידע אישי חייב להודיע לרשות הממונה ללא דיחוי על כל תקרית הכוללת אובדן של שליטה, גישה בלתי מורשית או גילוי של מידע אישי, כשיש סבירות לקיומו של סיכון לנזק ממשי. בהמשך, הרשות הממונה רשאית לדרוש מהארגון להודיע לאנשים שמתקיים לגביהם סיכון ממשי לנזק. הודעה זו חייבת להינתן ישירות לאדם (אלא אם צוין אחרת על

¹⁰³ https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_1

¹⁰⁴ ש.ס.

¹⁰⁵ https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_1

¹⁰⁶ <https://laws-lois.justice.gc.ca/eng/acts/C-5/page-6.html#docCont>

¹⁰⁷ <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-416934> – סעיף 4 לחוק.



משרד המשפטים פרקליטות המדינה מחלקת הסייבר

ידי הממונה) ולכלול, בין היתר, את תיאור נסיבות אובדן הגישה או חשיפתו הבלתי מורשית למידע האישי, מועד ידוע או משוער, טיב המידע האישי ועוד.¹⁰⁸

60. ב-22.9.2021 ממשלת קוויבק אימצה את הצעת חוק 64, חוק למודרניזציה של הוראות חקיקה בכל הנוגע להגנה על מידע אישי, תוך חקיקת שינויים משמעותיים בדרישות המסדירות את השימוש וההגנה על מידע אישי, לפי החוק המגן על מידע אישי במגזר הפרטי ("חוק המגזר הפרטי")¹⁰⁹ וחוק הגישה למסמכים שבידי גופים ציבוריים והגנת מידע אישי ("חוק המגזר הציבורי")¹¹⁰. החוק מגביר משמעותית את החובות של גופים במגזר הציבורי והפרטי המחזיקים במידע אישי.¹¹¹ החוק דורש מגופים ציבוריים ופרטיים כאחד לדווח ל-Community Associations Institute ולאדם נשוא המידע על "תקריות סודיות", המוגדרות כגישה, שימוש או תקשורת בלתי מורשית של מידע אישי, או אובדן של מידע כזה. זאת אך ורק כאשר התקרית מהווה סיכון לפגיעה חמורה. בין הגורמים שיש לשקול בעת הערכת הסיכון לפגיעה חמורה: רגישות המידע, ההשלכות הצפויות של השימוש במידע והסבירות שישתמשו במידע למטרות מזיקות.¹¹²

הדין הישראלי הקיים

בישראל קיימים מספר נהלים וחוקים המתייחסים לחובת יידוע של אזרחים נשואי מידע אישי במקרים של הדלפת מידע ופגיעה אפשרית בפרטיות המידע. כמו כן, קיימות בדין הישראלי הוראות חוק האוסרות על פרסום בהקשרים אשר יכולים להיות רלוונטיים למתקפות כופרה.

חובת פרסום

61. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 :

א. תקנות הגנת הפרטיות (אבטחת מידע) (להלן: "תקנות הגנת הפרטיות") מגדירות את רמת אבטחת המידע הנדרשת מכל גורם במשק בישראל, ציבורי ופרטי כאחד, המנהל או מעבד מידע אישי דיגיטלי אודות אנשים וקובעות מנגנונים שנועדו להפוך את אבטחת המידע לחלק משגרת ניהול הארגון. מטרת התקנות היא להגביר ולחזק את ההגנה על המידע האישי של אזרחי

¹⁰⁸ <https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=CA>

¹⁰⁹ <https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1>

¹¹⁰ <https://www.legisquebec.gouv.qc.ca/en/document/cs/A-2.1>

¹¹¹ השינויים שהוכנסו בהצעת חוק 64 ייכנסו לתוקף בהדרגה: השינויים הראשונים ייכנסו לתוקף ב-22 בספטמבר 2022, שאר הוראות הצעת החוק אמורות להיכנס לתוקף שנה לאחר מכן, ב-22 בספטמבר 2023, כאשר ההוראות הסופיות ייכנסו לתוקף ב-22 בספטמבר 2024.

¹¹² <https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=CA>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

המדינה, באמצעות דרישות אבטחת מידע ברורות בהן על גופים וארגונים לעמוד, בהתאם לרגישות והיקף המידע האישי שמנוהל או מוחזק על ידם.¹¹³

ב. על-פי תקנה 11(ד) לתקנות הגנת הפרטיות, כאשר אירע "אירוע אבטחה חמור", על בעל מאגר המידע להודיע על כך לרשם (רשם מאגרי המידע) באופן מידי, ולדווח לרשם על הצעדים שנקט בעקבות האירוע (תקנה 11(ד)(1)). כמו כן, הרשם רשאי להורות לבעל מאגר המידע, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר (כיום הרשות הלאומית מוזגה לתוך המס"ל), להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע (תקנה 11(ד)(2)). הוראה זו אינה חלה על בעל מאגר מידע המנוי בסעיף 13(ה) לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**"). בין המאגרים המנויים בסעיף זה: מאגר מידע של רשות ביטחון, מאגר מידע של שב"ס, מאגר מידע של רשות מס, מאגר מידע הנוגע לחקירות ואכיפת החוק של רשות מוסמכת וכדומה.

ג. יצוין כי "אירוע אבטחה חמור" מוגדר בתקנה 1 לתקנות הגנת הפרטיות כשני סוגים של אירועים. במאגר מידע שחלה עלה רמת אבטחה גבוהה (מאגרי מידע מן הסוגים המפורטים בתוספת השנייה לתקנות הגנת הפרטיות), מדובר באירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה, או שנעשתה פגיעה בשלמות המידע. במאגר מידע שחלה עליו רמת אבטחה בינונית (מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה ואינם מאגר המנוהל בידי יחיד¹¹⁴), מדובר באירוע שנעשה בו שימוש בחלק מהותי מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר. על-פי חוק הגנת הפרטיות, "שימוש" מוגדר גם כ"גילוי, העברה ומסירה". כלומר, גם אם מישהו צפה במאגר, אך לא ביצע בו פעולה אקטיבית אחרת (כמו העתקה), מדובר באירוע אבטחה חמור.

ד. על-פי הנחיית רשם מאגרי המידע מס' 1/2018 "תחולת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 על גופים הכפופים להוראות המפקח על הבנקים, גופים מפקחים הכפופים להוראות המפקח על הבנקים בעניין אבטחת מידע נדרשים לקיים את תקנה 11(ד) אשר פורטה לעיל. אולם, שימוש בסמכות הרשם להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע (לפי תקנה 11(ד)(2)) יעשה בהתאם למסמך הבנות שגובש בין הרשות להגנת הפרטיות לבין בנק ישראל.¹¹⁵

62. הוראות הרשות לניירות ערד:

¹¹³ https://www.gov.il/he/departments/topics/data_security_privacy_protection_authority/govil-landing-page

¹¹⁴ למשל: מאגר מידע שבעליו הוא גוף ציבורי; מאגר מידע הכולל מידע על צנעת חייו האישיים של אדם, מידע רפואי, מידע גנטי, מידע על עבר פלילי של אדם וכדומה.

¹¹⁵ <https://www.gov.il/he/departments/policies/bankdatasecurity>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

- א. ביום 21.10.2018 פרסמה מחלקת תאגידיים ברשות לניירות ערך עמדה משפטית מספר 105-33 בנושא "גילוי בנושא סייבר". במבוא לעמדה צוין כי מטרתה להגביר את מודעות התאגידיים המדווחים לסיכון הפוטנציאלי של מתקפות סייבר, ולתת דגש להיבטים מסוימים שהגילוי לגביהם עשוי להידרש על-פי הוראות דיני ניירות ערך. העמדה אינה יוצרת חובות גילוי חדשות, ואינה גורעת מחובת גילוי החלה על תאגידיים מדווחים מכוח הוראות דין אחרות. העמדה מגדירה "תקיפת סייבר" כ"פעילות שנועדה לפגוע בשימוש במחשב או בחומר מחשב השמור בו".
- ב. עמדתה של הרשות לניירות ערך מפרטת את חובות הגילוי העיקריות החלות על הגופים המדווחים: גילוי בדיווח מידי, גילוי בתשקיף ובדו"ח התקופתי,¹¹⁶ גילוי במסגרת דו"ח הדירקטוריון.¹¹⁷ מאחר שרק חובת הגילוי בדיווח המידי עוסקת ביידוע של הציבור על אודות מתקפת כופרה, חובה זו תפורט להלן.
- ג. **גילוי בדיווחים מידיים**: תקנה 36 לתקנות ניירות ערך (דוחות תקופתיים ומידיים), התש"ל-1970 (להלן: "**תקנות הדוחות**") קובעת כי תאגיד מדווח נדרש לדווח מידי על כל אירוע או ענין החורגים מעסקי התאגיד הרגילים, בשל טיבם, היקפם או תוצאתם האפשרית ואשר יש להם או עשויה להיות להם השפעה מהותית על התאגיד, וכן בדבר כל אירוע או ענין שיש בהם כדי להשפיע באופן משמעותי על מחיר ניירות הערך של התאגיד. בהתאם, כאשר מתרחשת מתקפת סייבר על התאגיד המדווח, נדרש, בין היתר, לבחון את מהותיות האירוע לצורך **דיווח לציבור** ולשם כך לשקלל את מכלול הנזק ופוטנציאל הנזק, הן במישרין והן בעקיפין. הגילוי יכול לכלול פרטים כגון: זהות או סוג התוקפים, נסיבות התקיפה, היקף וסוג הנזק שאירע לרבות השלכות עקיפות, הערכת התאגיד האם אותר מלוא הנזק הישיר, התמודדות התאגיד עם התקיפה, וכן דיווחים משלימים על האירוע.
- העמדה מפרטת דוגמאות לאירועים העשויים לחייב פרסום דיווח מידי מכוח התקנה: פעילותו העסקית של תאגיד הופסקה לפרק זמן; מאגרי מידע נפרצו באופן שעלול להשפיע על פעילות התאגיד במישרין או בעקיפין (ככל שהמאגר מוגן על-ידי דיני הגנת הפרטיות יש להתייחס לכך בנפרד ובנוסף); התאגיד נדרש לשלם כופר בסכום מהותי בעקבות תקיפת סייבר וכדומה.
- ד. ביקורת שנשמעה על עמדה משפטית זו היא שבכל הנוגע לדיווח מידי, התאגיד המדווח אינו נדרש לדווח לציבור באופן מידי, אלא רק לאחר שבחן את מהותיות האירוע ולשם כך שקלל את מכלול הנזק ופוטנציאל הנזק. לפיכך, לתאגיד עצמו עלול להיות תמריץ ממשי לעכב דיווח או לקבוע כי לא מדובר באירוע מהותי, ויקשה לתקוף מהלכים מעין אלה.¹¹⁸

¹¹⁶ על-פי סעיף 1 לתקנות ניירות ערך (דוחות תקופתיים ומידיים), התש"ל-1970 (להלן: "**תקנות הדוחות**"), תקופת הדיווח אינה קבועה, ויכולה להיות רבעון, חצי שנה, או שנת דיווח, לפי העניין.
¹¹⁷ על-פי תקנה 10 לתקנות הדוחות, בשנת דיווח מוגש לרשות לניירות ערך דו"ח הדירקטוריון על מצב ענייני התאגיד, ובו פרטים שונים המפורטים בתקנה 10.
¹¹⁸ <https://www.calcalist.co.il/internet/articles/0,7340,L-3748085,00.html>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

איסור פרסום

63. הצעת החוק "איסור פרסום זמני של מתקפת סייבר", התשפ"ב-2022:

- א. הצעת חוק איסור פרסום זמני של מתקפת סייבר, התשפ"ב-2022 (להלן: "**הצעת חוק איסור פרסום**" או "**הצעת החוק**"), שיזמה באופן פרטי ח"כ מירב בן ארי. הצעת החוק הונחה על שולחן הכנסת ה-24 לקריאה טרומית ביום 16.5.2022.¹¹⁹
- ב. מטרת הצעת חוק איסור פרסום היא לקבוע איסור פרסום זמני של מתקפת סייבר על מנת לצמצם, ככל הניתן, פרסום אודות מתקפת סייבר כאמצעי לחץ והבכה לארגון הנפגע, וכן על מנת לוודא כי ההתמודדות עם האיום נעשית בצורה מיטבית עבור הארגון הנפגע ועבור פרטיות האזרחים. בדברי ההסבר להצעת החוק נכתב כי כלי האיום המרכזי של יוזמי אירועי סייבר הוא התקשורת, כך שללא פרסומים תקשורתיים, התוקפים לא יצליחו לייצר את אפקט הכאוס ולגרום לאיום ממשי.
- ג. סעיף 2 להצעת החוק מגדיר כי "ארגון" הוא עסק או כל מי שמספק שירות לציבור, למעט המדינה ורשות מקומית. כמו כן, "מתקפת סייבר" מוגדרת כשיבוש פעולתו התקינה של מחשב או שיבוש השימוש בו, לרבות בדרך של מחיקה שינוי או הדלפת מידע, אחסון או הצגת מידע או פלט כוזב, מניעה או שיבוש הגישה לרשת תקשורת, מתן גישה לגורם שאינה מורשה, וכן חדירה שלא כדין כמשמעותה בחוק המחשבים, התשנ"ה-1995, כן האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר.
- ד. הצעת חוק איסור פרסום אוסרת על כל אדם לפרסם מידע על מתקפת סייבר החל ממועד התרחשותה ועד שחלפו 30 יום מעת שליחת הדיווח הראשוני עליה לגורם אחראי במשטרת ישראל. דיווח זה מוגדר בהצעת החוק כהודעת ממונה האבטחה בארגון על המתקפה, על הארגון המותקף ועל המידע אשר ברשותו. במקרה שחלפו 30 יום ומומחה¹²⁰ סבור שהטיפול במתקפה לא הסתיים, על הארגון המותקף חובה להגיש דיווח שני על המתקפה, הפעם למס"ל, על אודות מצב ההתמודדות עם המתקפה ועל הפרטים שנתגלו בזמן שחלף. לאחר 14 ימים נוספים, יכול הגוף לפנות לבית משפט שלום לבקשת צו איסור פרסום, שיכול להינתן לפרק זמן מקסימלי של 45 ימים, ולאחר מכן 30 ימים נוספים, ומעבר לכך לא יינתנו צווי איסור פרסום נוספים. מדובר בתקופת זמן של כ-4 חודשים בהם כלי תקשורת לא יוכלו לדווח על מתקפות סייבר. הצעת החוק קובעת שהמפרסם מידע בניגוד לאמור בהצעת החוק דינו מאסר שישה חודשים, ודינו מאסר של

¹¹⁹ <https://main.knesset.gov.il/Activity/Legislation/Laws/Pages/LawBill.aspx?t=lawsuggestionssearch&.awitemid=2191953>

¹²⁰ מומחה מוגדר בהצעת החוק כמי שמופיע ברשימת מומחים שקבע השר לביטחון פנים.

עמוד 28 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

חמש שנים במידה והמידע כולל "חשיפת פרטים שיש בהם כדי לפגוע באינטרס חיוני", מונח שאינו מוגדר בהצעת החוק.

ה. הצעת חוק איסור פרסום זכתה לביקורות. בין היתר, נטען כי מנוגדת לעקרונות יסוד של חופש הביטוי וחופש העיתונאות, ומנוגדת למגמה העולמית שמחייבת גילוי נאות ומידי בדבר מתקפות סייבר. כן נטען שפוגעת בעקיפין בזכות לפרטיות, שכן דיווחים על אירועי אבטחת סייבר מקדמים הגנה על מידע אישי.¹²¹ כך למשל, איסור הפרסום אינו מאפשר לנושאי המידע לנקוט פעולות על-מנת להגן על עצמם ולהקטין את פוטנציאל הנזק של האירוע (החלפת סיסמאות, הפעלת ביטוח, ערנות למתקפות פשינג עתידיות וכדומה). המגמה העולמית לפרסם מידע על אודות מתקפות סייבר נובע מהרצון לאפשר לארגונים אחרים לבצע מהלכים כדי להתגונן ממתקפה דומה או לבדוק האם הם עצמם קרובן למתקפה, למשל על דרך גילוי חולשות האבטחה באמצעותן בוצעה מתקפת הסייבר. הטענה היא שהצעת חוק איסור פרסום אינה מגנה על ארגונים ועל הציבור, אלא מאפשרת לתוקפי הסייבר חלון פעילות שיכול להימשך כ-4 חודשים, במהלכו יכולים לתקוף ארגונים אחרים באותה שיטת פעולה, או לנצל את המידע שחשפו במתקפה כדי לתקוף משתמשים נוספים.¹²²

64. עילות חוק בתי המשפט [נוסח משולב], התשמ"ד-1984:

א. סעיף 70(ד) לחוק בתי המשפט [נוסח משולב], התשמ"ד-1984 (להלן: "חוק בתי המשפט"), קובע כי בית משפט רשאי לאסור כל פרסום בקשר לדיוני בית המשפט, במידה שהוא רואה צורך בכך לשם הגנה על בטחונו של בעל דין, עד או אדם אחר ששמו הוזכר בדיון או לשם מניעת פגיעה חמורה בפרטיות של אחד מהם, לשם מניעת פגיעה בפרטיות של אדם בשל חשיפת מידע רפואי עליו או לשם מניעת פגיעה בפרטיותו של אדם עם מוגבלות שכלית או של אדם עם מוגבלות נפשית, כהגדרתם בחוק הליכי חקירה והעדה של אנשים עם מוגבלות, של אחד מהם.

ב. סעיף 70(ה) לחוק בתי המשפט קובע שבית משפט רשאי לאסור פרסום שמו של חשוד שטרם הוגש נגדו כתב אישום, או פרט אחר מפרטי החקירה, אם הדבר עלול לפגוע בחקירה שעל פי דין; אסר בית המשפט כאמור, יפקע האיסור עם הגשת כתב האישום נגד החשוד, אלא אם כן קבע בית המשפט אחרת.

ג. סעיף 68(ב)(1) לחוק בתי המשפט קובע שבית משפט רשאי לדון בעניין מסוים, כולו או מקצתו, בדלתיים סגורות, אם ראה צורך בכך, בין היתר, לשם שמירה על ביטחון המדינה. סעיף 70(א) לחוק קובע איסור פרסום על דיון שהתנהל בבית משפט בדלתיים סגורות, אלא ברשות בית המשפט.

¹²¹ <https://www.pc.co.il/news/363009>

¹²² <https://www.calcalist.co.il/calcalistech/article/rj325bzpq>



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

ד. סעיפים אלה בחוק בתי המשפט מאפשרים לבתי המשפט לאסור על פרסום חשוד במתקפת כופרה, ככל שנפתחה חקירה במטרה בגין אותה מתקפה. בפעם הראשונה בה פונה היחידה החוקרת במטרה לבית המשפט במטרה להוציא צו הנוגע לחקירת מתקפת הכופרה, יכולה היחידה החוקרת לבקש מבית המשפט איסור פרסום על פרטי החקירה, ככל שסבורה שאיסור הפרסום נדרש לשם שמירה על ביטחון המדינה, או שהפרסום עלול לפגוע בחקירה או לפגוע באופן חמור בפרטיות נושאי המידע.

65. איסור פרסום כתוצאה מהוראה של הצנזור הצבאי: תקנה 87 לתקנות ההגנה (שעת חירום), 1945 מאפשרת לצנזור הצבאי לאסור פרסום חומר שפרסומו עלול לפגוע, לדעתו, בהגנתה של ישראל או בשלומה של הציבור או בסדר הציבורי. כידוע, בבג"ץ שניצר נקבע כי הצנזור הצבאי מוסמך לפסול פרסומה של ידיעה אם, באופן אובייקטיבי, על יסוד מערכת עובדות נתונה, קיימת ודאות קרובה לכך, כי הפרסום יגרום לפגיעה קשה או ממשית בביטחון המדינה. זאת ועוד, הקביעה, כי אם הפרסום לא ייאסר קיימת ודאות קרובה לפגיעה ממשית בביטחון המדינה, צריכה לבסס עצמה על ראיות ברורות, חד-משמעיות ומשכנעות.¹²³

עמדות שהובעו בדיוני צוות המשנה

66. במהלך דיוני צוות המשנה, נחלקו הדעות באשר להטלת איסור פרסום, או לחלופין חובת פרסום, של מתקפות כופרה. הדעות השונות תפורטנה כדלקמן.

67. מר טיראן פרטוק, אשר תמך בהצעת החוק הפרטית של ח"כ מירב בן ארי בנושא איסור פרסום זמני של מתקפת סייבר (שפורטה לעיל), ציין כי מטרת התוקפים, הן כאלו המונעים ממניע כלכלי והן כאלו המונעים ממניע הנוגע לטרור, אינה בהכרח לפרסם מידע רגיש על אזרחים ישראלים, אלא לחולל כאוס ותהודה תקשורתית, ולכן פרסום פרטי מתקפת הכופרה בתקשורת מאפשר להם להשיג את מטרתם בקלות ובמהירות. כמובן שיש לאזן זאת מול שיקולים דמוקרטיים כגון חופש הביטוי והעיתונות, ועל כן מציע לאסור פרסום באופן זמני, באופן שאינו שולל דיווח ויידוע של הרשויות ושל נושאי המידע על אודות המתקפה והחשש להדלפת המידע. יתר על כן, טען כי לא תמיד זכות הציבור לדעת גוברת על האינטרסים של הגופים שנפגעו ממתקפת הכופרה, ושל האזרחים שהמידע שלהם הודלף, ושרק איסור פרסום זמני יכול להביא לחקירת האירוע באופן שיצמצם את הנזקים הפוטנציאליים כתוצאה מהמתקפה.

68. נציגי רשות שוק ההון ציינו כי לטעמם אין תועלת בחובת פרסום גורפת על אודות מתקפות כופרה, אלא יש לפרסם אך ורק בהתאם לדינים הקיימים בנושאי חובה ואיסור פרסום, למשל על-פי האמור בתקנות הגנת הפרטיות.

¹²³ בג"ץ 680-88 שניצר נ' הצנזור הצבאי הראשי, פ"ד מב(4) 617 (1989).



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

69. מר דורון הדר ציין שההסדר החוקי הקיים בדבר איסור פרסום הוא מספק, ובכל הנוגע לחובת פרסום, אין להטיל חובת פרסום גורפת על גופים שנפגעו ממתקפת כופרה, אלא יש לקבוע אינדיקטורים לפיהם יוחלט האם יש חובה לפרסם. אינדיקטורים אפשריים יכולים להיות: האם המידע שדלף הוא טכני ונוגע לעסקאות בין עסקים, האם יש לקוחות או אזרחים אחרים שהמידע שלהם דלף, סוג המידע שדלף, מה הנזק שנגרם או צפוי להיגרם בפועל כתוצאה מההדלפה, כמות הלקוחות של העסק הנפגע (האם ניתן להודיע להם באופן אישי?) וכדומה.

70. נציגי מחלקת הסייבר בפרקליטות המדינה ציינו כדוגמה מקרה שבו פרסום התקשורת על אודות פריצת קבוצת ההאקרים Black Shadow לשרתי Cyberserve הוביל להישג גדול יותר לתוקפים ולנזק גדול יותר לאזרחים ישראלים. במקרה הנ"ל, קבוצת ההאקרים החלה להדליף מידע מהשרתים על-פי גודל הקבצים, ללא הבנה של טיב המידע המודלף. לאחר שהתקשורת הישראלית חשפה שגם מאגר המידע של אפליקציית ההיכרויות "אטרף" נמצא באותם שרתים, החלה קבוצת ההאקרים להדליף את אותו מאגר מידע, מתוך הבנה שמדובר במידע רגיש העלול לגרום נזק לאזרחים.

71. נציגי מס"ל הסכימו עם העמדה שלפיה קיימים כלים בדין הישראלי לאיסור פרסום של מתקפות כופרה בתקשורת, ככל שנדרש. עם זאת, הביעו הבנה לעמדתו של מר טיראן פרטוק לפיה היכולת לנהל את הפרסומים בתקשורת על אודות מתקפות כופרה היא קריטית.

המלצות

המלצות בנוגע לאיסור תשלום כופר

72. בהמשך לדיונים במפגשי העבודה של צוות המשנה, שפורטו לעיל, הגיעו חברי צוות המשנה לכלל מסקנה כי אין מקום להטיל איסור גורף על תשלום כופר. זאת ועוד, חברי צוות המשנה בחנו את השאלה האם יש לאסור תשלום כופר על גופים מותקפים מסוימים, כגון גופי ממשלה, תשתיות קריטיות, חברות ציבוריות או כדומה. אולם חברי צוות המשנה הגיעו לכלל מסקנה כי גם על גופים ציבוריים או אף ממשלתיים, לא נכון לקבוע כלל גורף של איסור על ביצוע התשלום.

73. עם זאת, תשלום כופר, בין אם על-ידי גופים מדינתיים, בין אם על-ידי תאגידים מסוגים שונים ובין אם על-ידי אנשים פרטיים – הוא בבחינת פעולה בלתי-רצויה. זאת, בין היתר, מהנימוקים הבאים:

א. תשלום הכופר לא מבטיח את החזרת המצב לקדמותו (קבלת צופן הפיענוח, השגת גישה לנתונים וכדומה). מדובר במשא ומתן עם גורמים עברייניים שעשויים להדליף ולמכור את המידע למרות שקיבלו את התשלום המבוקש.

ב. תשלום הכופר עשוי לסייע לתוקפים במימון פעולות לא חוקיות נוספות, ביניהן מתקפות כופרה.

עמוד 31 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

- ג. תשלום הכופר עלול לסמן את המותקף כמטרה עתידית למתקפות כופרה נוספות.
- ד. תשלום כופר לא עולה בקנה אחד עם דרישת שיחזור המידע באמצעים ראויים ("appropriate measures") במקרה של אסון, הקבועה ב-GDPR וכן בתקנה 17(ב) לתקנות הגנת הפרטיות.
74. לאור האמור לעיל, מצאנו לנכון להמליץ על דרכי הפעולה כדלקמן:
- א. המלצה רשמית ופומבית שתופנה לכלל הציבור שלא לשלם כופר תוך הבהרת הטעמים לכך כאמור לעיל, ולדווח על המתקפה וכן על התשלום (ככל שמבוצע תשלום) לאלתר לרשויות המדינה הרלוונטיות, בין היתר: מס"ל, משטרת-ישראל, הרשות להגנת הפרטיות, רגולטורים מגזריים רלוונטיים (כגון המפקח על הבנקים, המפקח על הביטוח, רשות ניירות ערך).
- ב. פרסום הבהרה כללית בדבר הסיכון לגיבוש אחריות פלילית בנסיבות מסוימות של תשלום כופר בגין עבירות כגון מימון טרור או הלבנת הון, כמו גם הסיכון לעבירה על הוראות OFAC במישור הבין-לאומי. ניתן אף לשקול לפרסם פרמטרים או תנאים בהם אותו סיכון יצומצם, למשל במקרה של דיווח מבעוד מועד לרשויות האכיפה, שיתוף פעולה עמו, דיווח מבעוד מועד לרגולטורים רלוונטיים וכדומה.
- ג. בכל הנוגע לגופי מדינה המותקפים במתקפת כופרה, קיים קושי מיוחד להכיר באפשרות שישולמו דמי הכופר, שכן משמעות הדברים יכולה להיות שהמדינה עצמה תהיה מעורבת ב"עסקת העבירה". במקרה כזה, ראוי לטעמנו לשקול לקבוע כי יתקבל אישור מוקדם לכך מאת גורם משפטי בכיר, לאחר התייעצות עם גופי הגנת הסייבר וגופי הביטחון או האכיפה הרלוונטיים.
- ד. מוצע לשקול לקדם את המהלכים הבאים:
- 1) פרסום ההמלצה וההבהרה לציבור הרחב כמפורט לעיל בס"ק א' ו-ב'.
 - 2) חיוב משרדי הממשלה בדיווח לגופים הרלוונטיים במקרה של מתקפת כופרה.
 - 3) עיגון תהליך הבחינה של תשלום כופר – במקרי קיצון – כמפורט לעיל בס"ק ג'.
- כן מוצע לבחון האם המסגרת המתאימה לקדם מהלכים אלה היא החלטת ממשלה או שמא נדרש מהלך הכולל תיקוני חקיקה.

המלצות בנוגע לאיסור פרסום

75. אין ספק שפרסום תקשורתי יכול, בנסיבות מסוימות, להעצים את האפקט שרוצה להשיג התוקף במתקפת כופרה (דהיינו זריעת פחד, בהלה, ייאוש וכדומה), בפרט אם המתקפה נועדה למטרות טרור. לעיתים הפרסום אף עלול להכווין גורמי פשיעה, שאינם התוקפים המקוריים, ליטול את המידע,

עמוד 32 מתוך 34



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

לסחוט את נושאי המידע, למכור אותו וכדומה. מנגד, עומדות זכויות כבודות משקל המתנגשות עם האינטרסים המוגנים, בין היתר: זכות הציבור לדעת, חופש העיתונות, וזכות נושאי המידע להגנה על המידע האישי שלהם.

76. יודגש כי דילמות כאלה הנוגעות לפרסום מתעוררות פעמים רבות בכל הנוגע לאירועים פלייליים או ביטחוניים, חלקם אקוטיים, ולעתים אף מסכני חיים. צוות המשנה הגיע לכלל מסקנה, כי מנגנון איסור הפרסום הקבוע בדין הישראלי מספק תוצאה טובה. זאת, מכיוון שרשויות האכיפה יכולות לפעול להוצאת צווי איסור פרסום, וצווים אלה יכולים להינתן במעמד צד אחד, במהירות יחסית, בהתאם לסמכויות שנקובות כיום. מניסיונו, תהליך הוצאת צו איסור פרסום יכול להיעשות תוך שעות בודדות, מרגע החלטה בדבר הצורך באיסור פרסום עד חתימת הצו או אף הפצתו בפועל.¹²⁴

77. צוות המשנה ער לכך שמנגנון של הוצאת צו איסור פרסום מחייב לערב את רשויות האכיפה למן ההתחלה של אירוע מתקפת כופרה. אולם, מכיוון שידוע מידי של משטרת-ישראל באירוע של מתקפת כופרה הוא בגדר פעולה ראויה ומוצדקת ממילא, הרי ששיתוף משטרת-ישראל לא אמור לשנות את מהלך הדברים הטבעי במקרה של מתקפות כופרה.

78. מעבר לכך, יצוין כי במקרים חריגים, ככל שיהיו כאלה, יוכל גם הצנזור הצבאי לפעול במסגרת סמכויותיו.

79. נוסף על כל האמור, מצאנו לנכון להציע מספר כללים מנחים (GUIDELINES) בנוגע לתהליך הבקשה וההוצאה של צווי איסור פרסום בהקשרנו הנדון:

א. יש לשקול במקרים המתאימים להגביל את הצו, כך שיותר לדווח לכל הרגולטורים הרלוונטיים ללא דיחוי או תוך פרק זמן סביר שייקבע במסגרת הבקשה. לרגולטורים אלה לא יותר לפרסם את המידע הלאה, עד להסרת איסור הפרסום.

ב. יש לשקול לקבוע מגבלות זמן לבקשה לצו איסור הפרסום, וזאת במסגרת ניסוח בקשה לצו. לנוכח השיקולים המתנגשים שצוינו לעיל, יש להיוועץ בפרקליטות בשיתוף כלל הגורמים הרלוונטיים, לגבי משכו של איסור הפרסום.

ג. ככל הניתן, על בסיס המידע הקיים בעת הגשת בקשה לאיסור הפרסום, יש לפרט במסגרת צו איסור הפרסום את הפרטים הבאים: סוג הארגון המותקף; הערכה בדבר היקף המידע אישי המצוי בידי הארגון (בכמה נושאי-מידע מדובר?); סוג המידע האישי המצוי בידי הארגון; קיומם

¹²⁴ לנוכח מסקנתנו זו, לא מצאנו לנכון להיכנס לבחינה לגופו של עניין של הסדרים חוקיים המשנים את המצב הקיים ביחס לאיסורי פרסום, כדוגמת הצעת חוק איסור פרסום שפורטה לעיל.



משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

של משקיעים פרטיים (במידה שמדובר בחברה שהנפיקה ני"ע). מטרתם של כל אלה היא לפרט בפני השופט כמה שיותר שיקולים נוגדים פוטנציאליים לשיקול שמכתיב איסור פרסום.

ד. נוסף על כך, ראוי לבסס את הבקשה לצו איסור פרסום (וכפועל יוצא מכך – גם את ההחלטה), כך שהיא תתייחס לא רק לאיסור פרסום מטעמים של טובת החקירה בנוגע למתקפת הכופרה (סעיף 70(ה) לחוק בתי המשפט, וכן סעיף 70(א) לחוק בתי המשפט, בנסיבות סעיף 68(ב)(1) לחוק בתי המשפט), כי אם גם – ואולי אף קודם כל – לאיסור פרסום מטעמי הגנה על המידע, ובפרט המידע האישי, שנפרץ ונמצא בידי התוקפים (סעיף 70(ד) לחוק בתי המשפט). בהתאם לכך, איסור הפרסום יחול לא רק על פעולותיהם של גורמי הביטחון ורשויות האכיפה, אלא גם באופן ישיר על המידע הפרוץ עצמו. ככל שיוחלט על-ידי מבצעי מתקפת כופרה להפיץ ברבים את המידע שנפרץ במסגרת המתקפה, כולו או חלקו, הרי שפרסומו – ייאסר. כך יימנע הדהוד של המידע באופן שיועיל עם התוקפים.

בכבוד רב,

חיים ויסמונסקי, עו"ד

מנהל מחלקת הסייבר בפרקליטות המדינה

העתק:

חברי צוות המשנה

עמוד 34 מתוך 34