

ה הבטחה הגדולה של טכנולוגיות המידע היא קיומו של שוק גלובאלי של מסחר אלקטרוני. בינתיים, נדמה כי הבטחה זו עדיין לא מומשה, בין השאר בשל העדר תשתית משפטית ראויה להסדרת הסוגיות המורכבות הכרוכות בכך.

מטרת רשימה זו היא להבהיר את מהותן של מערכות מסחר אלקטרוני מנקודת מבטו של המשפטן, ולאפיין את התשתית המשפטית הנדרשת על מנת לסייע ביישומן של מערכות אלו. בעיקר, ידונו מנגנונים לזיהוי צדדים בסחר האלקטרוני באמצעות מנגנוני הצפנה מתוחכמים של "חתימה דיגיטלית" וההסדרים המשפטיים ההולכים ומתגבשים בנושא זה.





## תוכן העניינים

<b>מבוא</b>	<b>.1</b>
<b>מערכות מסחר אלקטרוני</b>	<b>.2</b>
מערכות "סגורות" ומערכות "פתוחות"	1.2
הסוגיות המשפטיות במערכות "פתוחות"	2.2
קטלוג אלקטרוני	1.2.2
חוזה דיגיטלי	2.2.2
קניה מקוונת	3.2.2
עסקה בכסף אלקטרוני	4.2.2
מסחר אלקטרוני מלא	5.2.2
התשתית הטכנולוגית של מסחר אלקטרוני	3.2
<b>זיהוי הצדדים במסחר אלקטרוני</b>	<b>.3</b>
זיהוי באמצעות "חתימה"	1.3
המקבילה האלקטרונית ל"חתימה"	2.3
חתימה דיגיטלית באמצעות הצפנה	3.3
הליכי אישור מפתחות הצפנה	4.3
שטרות דיגיטליים	5.3
<b>הפיקוח על אמצעי הצפנה</b>	<b>.4</b>
פיקוח על העיסוק באמצעי הצפנה	1.4
פיקוח על יצוא טכנולוגיות הצפנה	2.4
הצורך בהקלת הפיקוח על הצפנה	3.4
<b>סיכום ומסקנות</b>	<b>.5</b>





## 1 מבוא

שאלת הבסיס של זיהוי הצדדים לסחר האלקטרוני נדונה בהרחבה.

התשתית הטכנולוגית המרכזית במסחר אלקטרוני היא השימוש באמצעי הצפנה. כפי שיתחוויר להלן, אמצעים טכנולוגיים אלו מאפשרים פתרון אפקטיבי של זיהוי הצדדים בסחר האלקטרוני, באמצעות מנגנון הצפנה מתוחכם של "חתימה דיגיטלית". פתרון טכנולוגי זה הולך ומקבל הכרה חוקית במדינות רבות. הסדרים תחיקתיים אלו ראויים להידון גם במסגרת המשפט הישראלי. בעניין זה, הקריאה ברשימה זו היא להקלת הפיקוח על אמצעי הצפנה בישראל על מנת לאפשר ולהקל את יישומו של מסחר אלקטרוני בישראל.

באמצעותה של מסגרת זו, המטרה היא להביא את העיסוק בהיבטים המשפטיים של המסחר האלקטרוני לשולחן הדיונים של המשפטן הישראלי.

## 2 מערכות מסחר אלקטרוני

כאמור, הגדרה ברורה של התופעה הקרויה "מסחר אלקטרוני", היא תנאי מוקדם לבחינת ההיבטים המשפטיים של תופעה זו. משימת הגדרה זו היא מטרתו של פרק זה. בחינת גדרו של "מסחר אלקטרוני" נערכת מנקודת מבט משפטית. בראשונה, יבחנו מערכות מסחר אלקטרוני ונקודות האבחנה ביניהן אשר יש להן השלכות

נתונים באשר להיקף העסקאות המבוצעות במערכות מסחר אלקטרוני לוקים בחסרון בסיסי: הגדרת "מסחר אלקטרוני" נתונה לפרשנות גמישה. משום כך, אין כל טעם לנסות ולהעריך את היקפי הסחר האלקטרוני. עניין אחד ברור ואין עליו חולק: הסחר האלקטרוני ילך ויתעצם. יתר על כן, סביר להניח כי הגידול בהיקפי הסחר האלקטרוני יתרחש בקצב מואץ ויהפוך לעניין שבשגרה עבור גופים עסקיים קטנים כגדולים, ואף עבור משקי בית ופרטים. בהינתן תרחיש זה, בחינה משפטית של סביבת הסחר האלקטרוני היא מחויבת המציאות.

ואכן, בחינתן של מערכות מסחר אלקטרוני זוכות להתעניינות גדלה והולכת במסודות ממשל 1 ובארגונים בינלאומיים<sup>2</sup>, ואנו עדים לגל חקיקה המיועד לטפל ישירות בסוגיות המשפטיות של מסחר אלקטרוני<sup>3</sup>.

אשר על כן, מבקשת רשימה זו לתרום לבחינה המשפטית דן באמצעות הגדרתם של הסדרי התשתית המשפטית לטיפול במסחר אלקטרוני בישראל<sup>4</sup>.

הגדרתה של התשתית המשפטית למסחר אלקטרוני מחייבת הבהרת גדרו של "מסחר אלקטרוני" מנקודת מבטו של המשפטן. לפיכך, זהו הדיון הפותח רשימה זו. מערכות מסחר אלקטרוני מסווגות לטיפוסי מערכות אשר יש לגביהן שאלות משפטיות אופייניות. מבין אלה,

- 1 ראה: מסמך מקיף מטעם נשיא ארה"ב בנושא מסחר אלקטרוני - The Framework for Global Electronic Commerce http://www.whitehouse.gov/WH/New/Commerce (1 July 1997) גם מוסדות האיחוד האירופאי פעילים מאוד בנושא מסחר אלקטרוני. ראה: The European Ministerial Conference on Global Information Networks: Realising the Potential http://www2.echo.lu/bonn/final.html (6-8 July 1997). כל המקורות במאמר זה מן האינטרנט מצוטטים על-פי כתובות תקפות למועד חיבור המאמר (ספטמבר 1997).
- 2 מסחר אלקטרוני הנו מעצם טבעו חלק מן המסחר הבינלאומי, ולפיכך ארגונים בינלאומיים העוסקים במסחר בינלאומי פועלים בהיקף נרחב בנושא זה. ספריה מרכזית דיגיטלית של הפעילות הבינלאומית בנושא זה מצויה באתר הנורבגי המצויין International Trade Law Monitor : http://ananse.iry.uit.no/trade\_law/nav/electronic.commerce.html
- 3 למשל, חקיקה בנושא "חתימה דיגיטלית" הנדונה להלן.
- 4 בישראל נדון מסחר אלקטרוני בדין וחשבון ועדת הכנסת לתקשוב ומידע אשר פרסמה לאחרונה את ממצאיה. הועדה דן כוננה כועדת משנה של ועדת הכלכלה של הכנסת בנובמבר 1996. בראש הועדה לתקשוב ולמידע כיהן ח"כ מיכאל איתן. דו"ח הועדה פורסם באתר הכנסת באינטרנט: http://www.knesset.gov.il במדור: "כנסת / מדינת ישראל בעידן המידע". ראה בעיקר: דו"ח צוות מסחר אלקטרוני, הפרק במסחר אלקטרוני בדו"ח צוות חוק ומשפט.





סכסוכים.

מערכות מסחר אלקטרוני מסוג זה, קיימות מזה עשרות שנים. הדוגמאות הבולטות ביותר הן מערכות בנקאיות להעברות כספים. מערכות מעין אלו קיימות ברמות שונות. החל, ממערכות סליקה בתוך בנק נתון, וכלה במערכות בינלאומיות של העברת מטבע חוץ. מערכת מסועפת מעין זו, היא מערכת SWIFT<sup>5</sup> להעברות אלקטרוניות של כספים בין בנקים החברים במערכת.

התערבות משפטית במערכות "סגורות", כאמור, מתנהלת בהקשרים מצומצמים יחסית. הואיל, ובסיס ההסדר המשפטי החל על מערכות אלו הוא הסכמי וולונטארי, יכול שמוסדות משפטיים יקבעו הסדרים אופטימאליים לדוגמא, על מנת לעודד את השימוש במערכות אלו, וכן לחסוך בעלויות העסקה של הצדדים המבקשים ליישם הסדר כזה<sup>7</sup>, או לקבוע תקנים מוסכמים ליישום במערכות אלו על מנת לאפשר אחידות בין המערכות. ואכן, בארגוני סחר בינלאומיים מתנהלת פעילות ערה לניסוחם של כללים וסטנדרטים ליישום במערכות אלו<sup>8</sup>.

סוגיות משפטיות הדורשות ליבון מתעוררות במערכות "פתוחות". במערכות מסוג זה, אין הסדר חוזי כולל אליו יש לפנות על מנת לחלץ את הנורמות המשפטיות אשר

משפטיות. בהמשך, יסווגו מערכות המסחר האלקטרוני בהתאם למידת היישום האלקטרוני של שלבים בתהליך המסחר. לבסוף, תינתן סקירה של התשתית הטכנולוגית העומדת בבסיס מערכות המסחר האלקטרוני.

## 2.1 מערכות "סגורות" ומערכות "פתוחות"

אבחנה עקרונית בין מערכות מסחר אלקטרוני, שיש לה השלכות משפטיות, היא האבחנה בין מערכות "סגורות" ומערכות "פתוחות"<sup>5</sup>.

מערכות "סגורות" מאופיינות בכך, שהצדדים המעורבים במסחר האלקטרוני, הם צדדים מזהים ומוכרים זה לזה. כמרכן, הצדדים אשר נערכים לעריכת מסחר אלקטרוני מסוג זה, מגבשים מערכת של הסדרים ונהלים אשר מהווה את הבסיס לקיומו של המסחר ביניהם. מבחינה משפטית, מדובר במערכת מסועפת ומפורטת של תניות חוזיות אשר מסדירות את הסדרי המסחר האלקטרוני בין הצדדים. ברור, כי ניסוח נבון של תניות אלה, ייקח בחשבון תקלות אפשריות בהסדרי המסחר, וכן יקבע מנגנון של יישוב סכסוכים וכללי הכרעה בהם. מכאן, כי מנקודת המבט המשפטית, מערכות אלו מהוות הסדרים וולונטריים על בסיס חוזי, אשר יחתכו בהתאם לדיני החוזים הרגילים. כאמור, בדרך-כלל, יכללו הסדרים אלו גם מנגנונים ליישוב

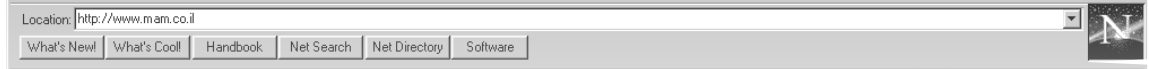
5 המערכות הקרויות כאן "מערכות סגורות", מופיעות בספרות כמערכות EDI - Electronic Data Interchange. הואיל ופעמים רבות, דיונים במערכות EDI או דיונים במערכות Electronic Commerce אינם מבחינים בצורה ברורה באבחנה הנערכת כאן, הטרמינולוגיה כאן היא בין מערכות "סגורות" - ואלה הן מערכות EDI, ובין מערכות "פתוחות", אשר הן המערכות שיאה להן המונח "מסחר אלקטרוני" - Electronic Commerce.

6 The Society for Worldwide Interbank Financial Telecommunications. ארגון כלל-עולמי שמרכזו בבלגיה, המאגד בנקים ברוב המדינות המפותחות, לשם העברת מטבע באמצעים אלקטרוניים. למבנה הארגון ודרך פעולתו ראה: Hal S. Scott, *Corporate Wire Transfers and the Uniform New Payments Code*, 83 *Columbia Law Review*, 1664 של אירגונים דומים בארה"ב, כגון: CHIPS - The Clearing House Interbank Payment System, מערכת שבסיסה בניו-יורק. כן ראה, בעניין SWIFT: ריקרדו ברואליאל, **דיני בנקאות - חלק כללי** (המכון למחקרי חקיקה ולמשפט השוואתי, ירושלים, 1996) בעמ' 416-7.

7 ראה למשל דו"ח והמלצות להסכם לדוגמא שנערכו על-ידי ועדה של לשכת עורכי-הדין בארה"ב, (ABA) Baum, Boss, McCarthy, Otero & Ritter, *The Commercial Use of Electronic Data Interchange - Areport and Model Trading Partner Agreement*, 45 *The Business Lawyer* 1645 (June 1990)

8 ריכוז המסמכים הנוגעים לתחום זה של EDI ואשר נוסחו במסגרת הפעילות של ארגון האו"ם לסחר בינלאומי (UNCITRAL) בשיתוף פעולה עם ארגונים בינלאומיים אחרים למסחר בינלאומי, ניתן למצוא באתרי האינטרנט <http://ananse.irtl> ITLC ו-<http://www.unece.org/trade/untddid/welcont.htm> UNECE ו-[http://uit.no/trade\\_law/nav/electronic.commerce.html](http://uit.no/trade_law/nav/electronic.commerce.html) וכן:





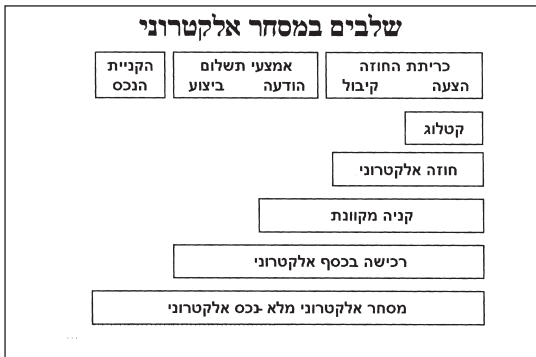
מובחנים, קרי: "הצעה" ר "קיבול".

העברת התמורה מן הקונה אל המוכר. במסחר נהוגים אמצעי תשלום מגוונים להעברת התמורה כאמור. על כן, ההבחנה הנערכת כאן היא בין מתן הודעה על אמצעי התשלום לבין ביצועו בפועל של התשלום. על-כן, ניתן לזהות בשלב זה שני תת-שלבים מוגדרים: "הודעת התשלום" ר "ביצוע התשלום".

הקניית הנכס נשוא חוזה המכר מן המוכר אל הקונה.

סיכומו של דבר, בתהליך המסחר אובחנו חמישה שלבים מוגדרים. שלבים אלו של עסקת המכר, יכול ויבוצעו בצורה אלקטרונית. בהתאם, לשלב ההתפתחות של המערכת הנדונה, מבחינים בחמישה טיפוסים של מערכות מסחר אלקטרוני, המייצגות את מידת היישום האלקטרוני של שלביה של עסקת המכר, כאמור לעיל.

מערכות טיפוסיות של מסחר אלקטרוני, יסווגו על כן, לאחת מבין המערכות כמבואר בתרשים שלהלן. מערכות אלו מאופייניות בכך, שקטעים מסוימים של עסקת המכר מיוצגים דיגיטלית.



יש להן תחולה. אמנם, ייתכן כי מקטעים מסוימים בתהליך יוסדרו בהסדר חוזי, אך שומה עלינו לפנות למערכת המשפטית הכללית על מנת לתת מענה לשאלות משפטיות העשויות להתעורר בסביבה זו. מסחר אלקטרוני מסוג זה, אינו שונה מכל מסחר אחר, בכך שאינו דורש בהכרח קיומו של הסדר חוזי כולל בין צדדים לסחר אשר הנם מזוהים ומוגדרים מראש. באותו אופן, שבו לקוח אקראי פונה לספק כלשהו בשוק על מנת לסחור עמו, כך גם בסביבה האלקטרונית: לקוח מזדמן פונה בשוק אלקטרוני לביצוע עסקאות עם ספקים המצויים בשוק. באשר לשוק הריאלי, מערכות משפט השכילו להסדיר ולעצב את הנורמות המשפטיות אשר חלות על יחסי המסחר בשוק. השאלה הנשאלת כאן היא: האם מערכות נורמטיביות אלו תקפות גם בשוק האלקטרוני - "הוירטואלי", והאם יש צורך בעיצוב כללי משפט חדשים, אם בכלל, על מנת ליתן מענה הולם לסביבה חדשה זו.

במערכות מסחר אלקטרוני, כאמור, מתעוררות אותן שאלות משפטיות המשותפות למשפט החל במערכת התקשורת הגלובאלית דוגמת האינטרנט<sup>9</sup>. שאלות כלליות אלו ראויות לליבון בפני עצמן, והמטרה כאן היא לאפיין את אותן סוגיות משפטיות הייחודיות למערכות המסחר האלקטרוני לסוגיהן.

**2.2 הסוגיות המשפטיות במערכות "פתוחות"**

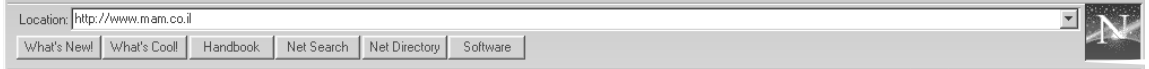
לצורך הדיון כאן, יוגדר "מסחר" כעסקת מכר. מכר אינו אלא "הקניית נכס תמורת מחיר"<sup>10</sup>. בהתאם לכך, תהליך המכר מורכב משלושה שלבים מובחנים:

כריתת חוזה המכר. ככל חוזה, "בדרך של הצעה וקיבול"<sup>11</sup>. על-כן, אפשר לזהות בשלב זה שני תת-שלבים

9 שאלות עקרוניות נובעות ממהותו של האינטרנט כמדיום גלובאלי חסר גבולות גיאוגרפיים, אשר ההתערבות המשפטית האפקטיבית בו מוטלת בספק. ראה דיון מפורט בפסה"ד של ביהמיש העליון בארה"ב לעניין בטלותו של חוק שהתיימר להסדיר הפצת חומרי תועבה באינטרנט: **Reno v American Civil Liberties Union et al.** (US Supreme Court, 26 June 1997). <http://www.aclu.org>. כמרכן, ראה אסופת המאמרים בעניין זה: **Borders in Cyberspace** (edited by Brian Kahin and Charles Nesson, Cambridge: MIT Press, 1997)

10 סעיף 1 לחוק המכר, תשכ"ח ז 1968, ס"ח 529, תשכ"ח עמ' 28.6.1968 [88].





- "ניזילות" המידע המופיע בקטלוג האלקטרוני. זה עשוי להשתנות ואף להתנדף ללא הותיר עקבות.

בהתאם לכך, להלן המערכות הטיפוסיות במסחר אלקטרוני והסוגיות המשפטיות הייחודיות אשר העשויות להתעורר בהן.

## 2.2.2 חוזה דיגיטלי

כאן אנו צועדים צעד נוסף בדיגיטליזציה של תהליך המסחר. החוזה נכרת בסביבה וירטואלית. האפשרויות לביצוע מהלך זה הן מגוונות. הקטלוג האלקטרוני שתואר לעיל, יכול שיאפשר תכתובת אלקטרונית לשכלולו של חוזה המכר בין הצדדים. אפשרות אחרת, שנעשית שכיחה יותר ויותר, הוא מתן אפשרות לקונה לסגור את עסקת המכר, כאשר נושא התשלום נותר לביצוע באחת הדרכים המקובלות במסחר, כגון: משלוח שיק למוכר, או אף מסירת פרטים בדבר דרכי התקשרות, כך שהמוכר יכול ליצור קשר עם הקונה על מנת להשלים את עסקת המכר בהסדרת התשלום.<sup>16</sup>

בטיפול מערכת זו של מסחר אלקטרוני, מצטרפות שאלות נוספות על אלה שכבר נמנו לעיל. לדוגמא:

## 2.2.1 קטלוג אלקטרוני

במערכת זו של מסחר אלקטרוני רק השלב הראשון של עסקת המכר מיוצג באופן אלקטרוני. למעשה, מערכת זו אינה אלא שיטת פרסום העושה שימוש במדיה הדיגיטלית וברשתות התקשוב להפצת המידע אודות המוצרים המוצעים<sup>12</sup>. במבט ראשון נראה, כי במערכת מטיפוס זה הסוגיות המשפטיות המתעוררות בהקשר זה אינן שונות מכל אמצעי פרסום אחרת<sup>13</sup>. ברם, עיון מעמיק יותר יורה שישנן שאלות הייחודיות לאמצעי פרסום זה. מעבר לשאלות הכלליות אשר עולות בכל הקשר של מערכות תקשורת גלובאליות<sup>14</sup> יש לבחון שאלות נוספות כגון:

- אמינות פרטי הזיהוי של האישיות המשפטית<sup>15</sup> (אדם או תאגיד) אשר מתיימרים לפרסם את הקטלוג האלקטרוני.

11 סעיף 1 לחוק החוזים (חלק כללי), תשל"ג צ 1973, ס"ח 694, תשל"ג עמ' 19.4.1973 [18].  
 12 רבים מאתרי הקניות באינטרנט עדיין שייכים לקטגוריה זו. ראה למשל, אתר "המשביר לצרכן": <http://www.hamashbir1a.zarchan.co.il> ואתרים נוספים במדריך "תפוז": <http://www.tapuz.co.il> במדור: "כלכלה ועסקים / קניות".  
 13 למשל: מצג או הבטחה עליך מסתמך הצרכן טטופל במסגרת דיני הניקין ודיני הגנת הצרכן. בתחום דיני החוזים יש מקום לשאלה האם מדובר ב"הצעה" או ב"הזמנה להצעה" וכיו"ב.  
 14 כגון: סמכות השיפוט, כללי ברירת הדין וכיו"ב - שאלות הנובעות מקיומה הגלובאלי של האינטרנט, מבחינת "בכל מקום ובשום מקום". לעיל הערה 9.  
 15 בעולם הריאלי ניתן לאמת על-ניקלה את פרטי הזיהוי הנמסרים בפרסום. למשל, אם מצוינת כתובת גיאוגרפית, אפשר לאמת פרט זה כעניין שבעובדה. אתרים באינטרנט, לפי זה, משולים למודעה אשר מציינת מספר תיבת דואר ותו לא.  
 16 דוגמא לכך הוא אתר הקניות של Israel Online - IOL מייסודו של עיתון "הארץ". באתר זה, ניתנת לקונים האפשרות, לאחר שלכאורה ביצעו את חוזה הרכישה, למסור פרטים למפעילי האתר על מנת שאלה יתקשרו כדי להסדיר את עניין התשלום. נראה שטכניקה זו נקוטה על מנת לנטרל את החששות מפני מסירת פרטים על כרטיסי אשראי באינטרנט. ראה: <http://www.iol.co.il> במדור: "קניות".





מוגדרים: כרטיסי חיוב מן הסוג הקביל ב"קניון הוירטואלי" שבו עסקינן<sup>19</sup>.

לקניון האלקטרוני יתרונות לא מבוטלים. להצלחה גדולה במיוחד זוכים קניונים לרכישת ספרים ותקליטים<sup>20</sup>. מהירות האיתור, גודל המבחר המוצע, והאפשרות לדגום את המוצר, קרי: לקרוא את תוכן העניינים, או אף קטעים מן הספר, ולחילופין, לשמוע דגימה מן התקליט, ולקרוא אודותיו - כל אלה מתאפשרים באופן עדיף ביותר מאשר בחנויות הספרים או התקליטים.

בקניונים הוירטואליים אף פותחו שיטות מסחר שנתאפשרו אך ורק מתכונות הסביבה האלקטרונית. למשל, אתרים אחדים מציעים מכירות פומביות בשיטה של מכרז פתוח, כאשר ההצעות הזוכות ידועות בכל נקודת זמן עד למועד סגירת המכרז<sup>21</sup>. מודל עסקי אחר, הוא האפשרות הניתנת לצרכן הפוטנציאלי לבצע סקר שווקים מקוון מתוך מגוון חנויות וירטואליות המאוגדות

● האם נכרת חוזה כדת וכדין? האם שיגור ההודעה על-די הצרכן מהווה "קיבול"?!

● האם ניתנה הסכמה לתניות החוזה בעצם ההקשה על מקש "אני מסכים" וכיו"ב<sup>17</sup>?

● מה הדרכים בהן החוק מגן על צרכנים בעסקאות אלה<sup>18</sup>?

היה וישנה דרישת כתב על-פירחוק, האם חילופי המסרים האלקטרוניים מהווים "מסמך בכתב" ?

### 2.2.3 קניה מקוונת

טיפוס מערכת זה, הוא זה אשר נמצא כיום בתנופה הגדולה ביותר. כאן, מאפשרים ללקוח המזדמן לבחון את הסחורה המוצעת, לברור את הפריטים שהוא חפץ בהם ל"יסל הקניות" הוירטואלי שלו, ולבסוף לגשת ל"קופה" ולשלם. אלא, שאמצעי התשלום כאן הם

17 כאן מתעוררת במלוא חריפותה הסוגיה של תקפותן של תניות חוזה המכונים Shrink - Wrap, או "חוזי עטיפת הצלופן". ראה סיכום הד"ר בארה"ב בעניין זה: **Internet**: excerpt from the book *Shrink - Wrap / Point - and - Click Agreements*, Kent Stuckey, <http://www.ljextra.com/internet/excerpt.html> and **Online Law**.

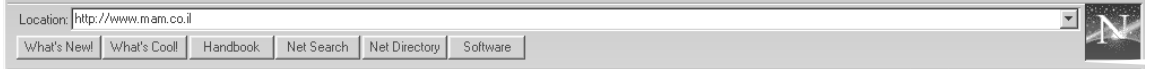
18 קיימת חקיקה עניפה, בעיקר בארצות אירופה, לעניין עסקאות המתבצעות דרך אמצעי תקשורת. לאחרונה, נתקבלה דירקטיבה של מוסדות האיחוד האירופאי המחייבת את מדינות האיחוד להתקין חקיקה בעניין זה, לרבות גילוי נאות של פרטי העסקה על-ידי הספק, וזכות הצרכן לבטל את העסקה בתוך 7 ימים בתנאים מסויימים. ראה: Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, **OJ L 144 (4 June 1997)**. ראה גם: עובדיה שרגאי, "עסקה מרחוק", **הארץ**, 1 דצמבר 1996. בישראל, הצעת חוק הגנת הצרכן (תיקון מס' 5), תשנ"ז - 1996 מאפשרת לצרכן לבטל עסקה בתוך 14 יום, אם העסקה נחתמה "שלא במקום עיסוקו הקבוע של העוסק, או שהעוסק לא נתן לצרכן הזדמנות סבירה לעיין בחוזה לפני חתימתו". מעניין לדון בתחולתו של תיקון זה לעסקאות הנעשות דרך האינטרנט במסחר אלקטרוני. ראה דיון בנושא זה באתר האינטרנט של הכנסת: <http://www.knesset.gov.il> במדור: "קבוצות הדיון בכנסת". מעניין לציין שהצעת חוק זו נבחרה לפתוח מפעל של הכנסת שבו מועמדות הצעות חוק בקבוצת דיון אלקטרונית לתגובות של אזרחים.

19 דוגמאות לטיפוס מערכת זה לא חסרות. בישראל, ראה מדריך "תפוז" שהוזכר לעיל, וכן אתר הקניות של IOL שאף הוא נדון לעיל. בעולם הרחב, קיימים אין ספור קניונים מן הסוג הזה, המציעים סחורות מכל הסוגים.

20 חנויות ספרים: <http://www.amazon.com>; <http://www.booksnow.com>; <http://www.cdnw.com>; <http://www.gemm.com>; חנויות תקליטים: <http://www.gemm.com>.

21 ראה מכירות של ציוד מחשבים ואלקטרוניקה באתר: <http://www.onsale.com>. יש להעיר כי בינתיים, האתר אינו מאפשר שיגור סחורה אל מחוץ לארה"ב גם ישראל נעשה ניסיון ליישם מודל זה, ראה: אתר "מכרז החומרה" בכתובת: <http://www.chip.co.il>.





במאגר מידע משותף<sup>22</sup>.

אלא רצף של אותות מחשב, אשר מייצגים כוח קנייה. מובן שאת ה"מזומנים" הללו יש לרכוש, ואין מטבע אלקטרוני אוניברסלי, אלא יש עסקים אשר מכבדים סוג זה או אחר של כסף אלקטרוני.

בקניות מקוונות עולות כלל הסוגיות אשר נדונו לעיל, ואליהן מתווספות שאלות נוספות כגון אלה שלהלן:

למען האמת, מדובר כאן בשכלול מסוים של שיטת כרטיסי החיוב, אלא שאין "עקבות אלקטרוניים" המשייכים רכישה מסוימת ללקוח מסוים, כפי שאין מנוס מכך בשימוש בכרטיסי חיוב. הצורך לביצוע עסקאות במזומנים הנו צורך נדרש בשוק וישנן עסקאות רבות אשר הצדדים להן מבקשים לשמור בצנעה או שהשתיקה יפה להן. לפיכך, פיתוח מקבילה למזומנים לשם רכישה בקניונים הוירטואליים הוא עיסוק מתפתח באינטרנט<sup>24</sup>.

מה קורה כאשר סחורה לא נתקבלה, או נתקבלה באופן פגום?

מה טיב אחריותם של מתווכים למיניהם המספקים שירותי מידע גרידא, להבדיל מקשר ישיר עם הספק עצמו?

מה בדבר מיסוי, מכסי יבוא וכיו"ב<sup>23</sup>?

#### 2.2.4 עסקה בכסף אלקטרוני

בדומה לכסף האלקטרוני האמור, מתפתחים מודלים של "כרטיסים חכמים" או "ארנקים אלקטרוניים", אשר מהווים יחידות מטבע המאוחסנות בכרטיס אלקטרוני ומאפשרות תשלום, גם של סכומים קטנים, כאמצעי מקובל בשוק האלקטרוני והיראלי כאחד<sup>25</sup>.

אם עד כה נראה שהעולם הוירטואלי לא חידש הרבה, הנה טיפוס מערכת זו נראה כלקוח היישר ממדע בדיוני. כאן מדובר בביצוע עסקה בשלמותה, לרבות תשלום במזומנים. אלא, ש"המזומנים" שבהם עסקינן, אינה

22 האתר GEMM - Global Electronic Music Marketplace מאגד מאות עסקים בתחום המוסיקה, כך שכאשר לקוח מבקש, למשל, לרכוש תקליט, מוצעות לו כל החנויות אשר ברשותן התקליט המבוקש, לרבות פרטים על מחירים, דמי משלוח וכיו"ב. ראה: <http://www.gemm.com>.

23 דו"ח של משרד האוצר בארה"ב אשר ניתח את ההשלכות של מסחר אלקטרוני על מערכת המיסוי הוא: The Department of the Treasury, Selected Tax Policy Implications of Global Electronic Commerce (November 1996) <http://www.ustreas.gov/tax/internet.html>. ראה גם: מיכאל לוי ויוסף בן לוי, "מיסוי עסקאות באינטרנט" מיסים יא (2), עמ' 37- (אפריל 1997). מעניין לציין כי הממשל בארה"ב, בהכירו באופייה הגלובאלי של האינטרנט, ואולי גם מהעדר כלים אפקטיביים לאכיפת מיסוי באינטרנט, מנסה לקדם את הרעיון של איזור סחר חופשי באינטרנט. ראה בעניין זה את נייר העמדה של הבית הלבן (לעיל הערה) והצעת חוק שהוגשה בקונגרס בארה"ב: Internet Tax Freedom Act, HR 1054 (13 March 1997). לפרטים על הצעת חוק זו ונוסח ההצעה, ראה: [http://www.ljextra.com/internet/hr1054\\_105.html](http://www.ljextra.com/internet/hr1054_105.html).

24 האתר של Mark Twain Bank מכריז על עצמו כחלוץ הכסף האלקטרוני. לאחר רכישת Ecash מן הבנק דגן באמצעים מסורתיים, הלקוח מקבל תוכנה מיוחדת, אשר מנהלת עבורו את קופת הכסף האלקטרוני שברשותו וכן מאפשרת ביצוע תשלום לספקים אשר מכבדים אמצעי תשלום זה. רשימת הספקים מרשימה ביותר וכוללת ספקים למוצרים מגוונים החל ממכוניות וכלה בשירותי הצנעה. ראה: מפעילי האתר מבטיחים כי לא נותרים כל רישומים בשימוש ב"כסף" זה, והוא שקול לכל דבר ועניין, מבחינה זו, למזומנים. אתרים רבים נוספים מציעים מודלים דומים. ראה: <http://www.digicash.com>. דרך פעולתו של הכסף האלקטרוני מודגמת גם במאמרם של לוי ובקרלי (לעיל הערה 23) שם, בעמ' 43-44. "מורה נבוכים" בנושא כסף אלקטרוני - <http://www.ex.ac.uk~RDavies/arian/emoney.html> Roy Davies, Electronic Money.

25 למעשה מדובר בכרטיסים דומים שמונפקים לצרכים מוגדרים ויעודיים, כגון, לשימוש בטלפונים ציבוריים או במכוניות צילום. ההבדל הוא באוניברסליות של היחידות שבכרטיס המהוות, על כן, אמצעי תשלום כמו מזומנים. חברות האשראי הגדולות טורחות בכיוונים אלו. ראה: <http://www.mastercard.com>; <http://www.visa.com>. לאחרונה נתן גם בנק ישראל את דעתו בסוגיה זו, וועדת "הארנק האלקטרוני" הגישה המלצות לנגיד בנק ישראל במאי 1997. דיווח על הוועדה וסיכום המלצותיה ראה: "מצלצלים אלקטרוניים" גלובס, 9 במאי 1997, עמ' 52.







וכיו"ב<sup>29</sup>.

כאשר מבוצעות עסקאות בצורה זו, הצורך באמינות המערכות ומהימנותם מתגבר שבעתיים. לפיכך, על שלל הסוגיות המשפטיות אשר נדונו לעיל מתווספות אחרות, שבעיקרן אבטחת מהימנות העסקאות.

### 2.3 התשתית הטכנולוגית של מסחר אלקטרוני

מבין הטכנולוגיות המהוות את התשתית ליישומו של מסחר אלקטרוני, נודעת חשיבות מיוחדת לאמצעי הצפנה. באמצעות טכנולוגיות מתקדמות של הצפנה, מבקשים לפתור מכשלות בדרך ליישומו של מסחר אלקטרוני מלא. לפיכך, ראוי לעיין בעקרונות טכנולוגיית תשתית זו, על מנת לגזור את ההסדרים המשפטיים המתבקשים.

העיסוק בהצפנת מסרים קיים מקדמת דנה. כבר בתנ"ך אנו מוצאים עדויות לשימוש באמצעי הצפנה. ירמיהו<sup>30</sup> "מצפיף" את המלה "בבל" באמצעות מפתח ההצפנה של שיכול-אותיות האל"ף-בי"ת<sup>31</sup>, שיטה הידועה כשיטת אתב"ש, קרי: האות "א" מקבלת את הערך "תיו", כאשר האות "בי"ת" מקבלת את הערך

השימוש בסוג זה של אמצעי תשלום מעורר שאלות משפטיות ייחודיות בתחומים רבים ומגוונים. כאן נמנה רק מעטים מהן:

האם מדובר בהנפקת כסף ממש? מה בדבר פיקוח ורישוי, וכן מונופול הבנק המרכזי<sup>26</sup>?

האם השימוש בכסף אלקטרוני יכול שיהיה מסוה לפעילות לא חוקית<sup>27</sup> ולהלבנת כספים<sup>28</sup>?

מה הדין במקרה בו "הכסף" שלי אבד, למשל, כאשר המידע במחשבי נמחק?

### 2.2.5 מסחר אלקטרוני מלא

שימוש בכסף אלקטרוני סולל את הדרך למסחר אלקטרוני מלא, כאשר המוצר או השירות ניתן אף הוא להעברה באמצעי תקשורת מחשבים. דהיינו: הנכס אשר מוקנה בטיפוס מסחר זה, אף הוא דיגיטלי. על אף שלכאורה מדובר בתחום מוגבל, נראה שלא כך הוא. בעידן של כלכלת מידע, מוצרים ושירותים רבים ומגוונים אינם אלא מידע. למשל, רכישת תוכנה ומוצרי מידע אחרים; רכישת שירותי תקשורת, שירותי מחשוב

26 מדובר כאן במהפכה מוניטרית של ממש. ראה בכתבת גלובס (לעיל הערה ) בדבר תיאור ההשלכות על המדיניות המוניטריות ועל ממדים מאקר-כלכליים מקובלים.

27 פעילות המקבלת תאוצה לאחרונה הוא עריכתם של הימורים וירטואליים באמצעות כסף אלקטרוני. נסה למשל: <http://www.casinolinks.com>.

28 ראה: 20-21 p. *The Economist*, 26 July 1997, *Money Laundering - Next, Cyberlaundering?*

29 באתרים המנפיקים כסף אלקטרוני כאמור לעיל, יש גם ספקים אשר מוצריהם הם מידע, כגון: תוכנה, ספרות או מוסיקה בפורמט דיגיטלי, או שמספקים שירותים למיניהם, החל משירותי מיחשוב וכלה בשירותי שידוכים...

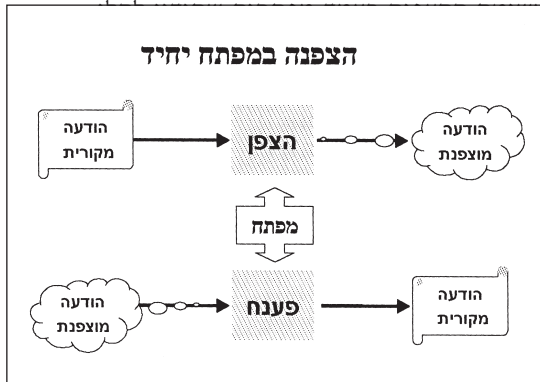
30 ירמיהו, כ"ה:26; נ"א:41.

31 הדרך הפשוטה ביותר ליצור את מפתח ההצפנה הנדון היא לכתוב את אותיות האל"ף-בי"ת כסדרן, ולאחר מכן לכתוב בסדר יורד, מן הסוף אל ההתחלה, את אותיות האל"ף-בי"ת, לשם יצירת האותיות המוחלפות.





באמצעים המבטיחים העברתו בערוץ מאובטח מפני גילוי. שיטת הצפנה זו זוכה בקריפטולוגיה המודרנית לכינוי "הצפנה במפתח יחיד", וזאת על מנת להבחינה



"שייך" וכן הלאה. באופן זה, המילה "בבל" הופכת למילה "ששך". שיטות אחרות של חילופי אותיות אנו מוצאים במקורות, כגון: שיטת אלב"ם<sup>32</sup> או שיטת אטב"ח<sup>33</sup>.

במהלך ההיסטוריה מופיעות עדויות רבות על יישום אמצעי הצפנה, מתוחכמים יותר ומתוחכמים פחות<sup>34</sup>. בהיסטוריה של העת החדשה זכור במיוחד המבצע של בעלות הברית לפענוח מפתח ההצפנה הנאצי במלחמת העולם השנייה. יש המעריכים כי פענוח מפתח ההצפנה הנאצי היווה את אחד היתרונות החשובים שהביאו לניצחון בעלות הברית<sup>35</sup>.

המושג המשותף לאמצעי הצפנה אלה הוא השימוש במפתח הצפנה סודי. מפתח זה נקבע מראש ומוחלף בין הצדדים

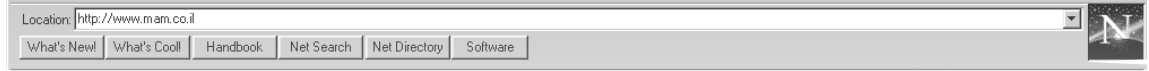
32 שיטת אלב"ם עושה, אף היא, שימוש בחילופי אותיות, אלא שכאן אותיות האל"ף בי"ת מחולקות לשתי קבוצות שוות, המסודרות זו בצד זו. באופן זה, האות אל"ף מקבלת את הערך למ"ד, האות בי"ת מקבלת את הערך מ"ם וכן הלאה. למעשה, השיטה היא של הזחה של אותיות. במקרה זה, הערך של האות הראשונה מקבל את זה של האות ה-13 (קרי" למ"ד); האות השנייה את הערך של האות ה-14 (קרי: מ"ם) וכן הלאה. אחד הפירושים לאמור בישעיהו, ז:6 על "בן טבאל" הוא כי "טבאל" אינו אלא מסר מוצפן בשיטת אלב"ם של "רמלא", כך שבעצם מדובר על ברמלא. במקורות מכונה שיטת פרשנות זו "גימטריה". ראה בעניין זה: ברייתא דשלושים ושתים מידות, מדה כט: גימטריא. כאן, שיטות ההצפנה של שיכול אותיות (בלשון הברייתא: "תמורות האותיות") נדונות בכפיפה אחת עם פירושים המיוסדים על ערכן המספרי של אותיות (בלשון הברייתא: "חשבון האותיות").

33 בשיטת אטב"ח ישנו תחכום מסוים. כאן האותיות המתחלפות מסתכמות בגימטרייה לסכום עגול של עשר או מאה. על-כן, האותיות אל"ף וטי"ת, בי"ת וחי"ת - המשלימות את המספר עשר בגימטרייה - מתחלפות ביניהן. בתלמוד בבלי, סדר מועד, מסכת סוכה נ"ב ע"ב, יש שימוש בשיטה זו לשם גזירה שווה בין "מנון" (משלי, כ"ט:21 "מפונק מנוער עבדו ואחריתו יהיה מנון") לבין "סהדה", ככתוב שם: "באטב"ח של ר' חייא קורין לסהדה מנון", כלומר אין "מנון" אלא "סהדה". ראה גם: מדרש רבה, במדבר, פרשה י"ח, סימן כ"א, סיפא. על-פי פירוש הלוי למדרש רבה, ספר "במדבר", הפסוק ממשלי יתפרש, איפוא: "יצר הרע (קרי: "עבדו" בפסוק דנן) מסיתו לאדם בעולם הזה, ומעיד עליו לעולם הבא" (קרי: "סהדה", עד בארמית, שהוא "מנון" בפסוק זה לפי שיטת אטב"ח) (פירוש א.א. הלוי בהוצאת מחברות לספרות, בעמ' 1775). במובאה דלעיל ממדרש רבה, מובאים בדרך האיכוך כלל המקורות דלעיל, בדבר שיטות אטב"ח, אלב"ם ואטב"ח.

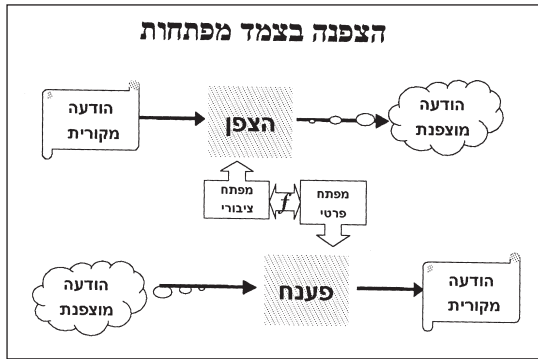
34 ספר מקיף ביותר על ההיסטוריה של ההצפנה: David Kahn, *The Codebreakers - The Story of Secret Writing* (New York: Scribner, 1996) המחבר גם סוקר את המקורות במורשת ישראל, כאמור לעיל, וכן מביא את סיפורו של דניאל, אשר מוכתר על-ידו כמפענח-צפנים כאשר הוא מפרש את הכתובת "תקל תקל מנה ופרסין" (דניאל, ה:25) ראה שם בעמ' 78-9. המחבר תמה מדוע מסר שאינו כתוב בכתב-סתר, נעלם מעיני חכמיו של בלשצאר. מעניין לציין כאן שחז"ל גרסו, שהכתובת לא נתבהרה לחכמים אלו והאיל והיא היתה מוצפנת בכתב סתרים. ראה: סנהדרין, כ"ב ע"א, ד"ה "אמר רב בגימטריא איכתיב להוני". חכמים נחלקו באשר לשיטת ההצפנה שבה נכתבה הכתובת דנן: שיטת אטב"ח (אליבא דרבנן), או שיטת היפוך אותיות (אליבא דשמואל ואחרים); שיטה מפורסמת של הזחת אותיות להצפנת מסרים, המובאת על-ידי Kahn, היא זו של יוליוס קיסר שהשתמש בשיטה שבה ההזחה היא בשלוש אותיות, כלומר: A קיבלה את הערך B; D את הערך E וכן הלאה. ראה: שם, בעמ' 84. בנושא ההיסטוריה של ההצפנה הופיע בעברית ספרו של ברוס נורמן, *מלחמת הצפנים* ("מערכות", 1978).

35 שם, עמ' 9.





סטנפורד בשנת 1976. אך היו אלה שלישיית מדענים מ-MIT שהביאו לגיבושה המעשי של השיטה, ולפיתוח הטכנולוגיה הקרויה על-שמם - טכנולוגיית ההצפנה בשיטת RSA<sup>38</sup>.



העקרונות המתמטיים לפיהם פועלת שיטה זו<sup>39</sup>, הוא קיומו של צמד פונקציות מתמטיות הפוכות זו לזו, שכל אחת מהן היא סוג מסוים של "פונקצית מלכודת חד-כיוונית"<sup>40</sup>. דהיינו, הפונקציות המתמטיות דגן מקיימות שתי תכונות: הפכיות וחד-כיווניות.

לעניין תכונת הפכיות של הפונקציות, פירושו של

בשיטת הצפנה זו, ההודעה המקורית מוצפנת באמצעות מפתח מוסכם על-מנת ליצור את ההודעה המוצפנת. המפתח יכול שיהא שיטה לשיכול או לחילופי אותיות או נוהל מורכב ומתוחכם יותר<sup>36</sup>. אותו המפתח, הוא זה גם שמשמש לפענוח ההודעה, על-ידי ביצוע תהליך הפוך לתהליך ההצפנה על ההודעה המוצפנת על-מנת לחלץ את ההודעה המקורית. שיטות ההצפנה שהודגמו לעיל, כללו מפתח-הצפנה פשוט אשר יישם הליך של חילופי אותיות לפי שיטה קבועה מראש.

שיטת הצפנה במפתח יחיד ישימה בעיקר במערכות סגורות. הואיל, ולפי הניתוח דלעיל נדרש תנאי מקדמי של קשר מוקדם בין הצדדים למסחר אלקטרוני במערכות מעין אלה, הרי שבמסגרת אותו קשר מוקדם אף מוחלפים המפתחות המוסכמים לביצועה של ההצפנה. ברם, כאשר מדובר במערכות פתוחות, ואלה עיקר עניינו של המסחר האלקטרוני העכשווי, כי אז שיטה זו אין בה תועלת רבה, ויש לאתר שיטות חלופיות אשר יתנו מענה לצרכיה של המערכת הפתוחה.

פתרון אפשרי לבעיה זו מושג באמצעות השימוש בטכנולוגיה של צמד מפתחות: מפתח ציבורי ומפתח פרטי, או השיטה האי-סימטרית. השיטה הוצעה לראשונה על-ידי Diffie & Hellman<sup>37</sup> מאוניברסיטת

36 בשפת הקריפטולוגיה: "הודעה מקורית": plaintext; "הודעה מוצפנת": cyphertext; "הצפנה" - encryption; פענוח" - decryption; "מפתח הצפנה" - cypher-key.

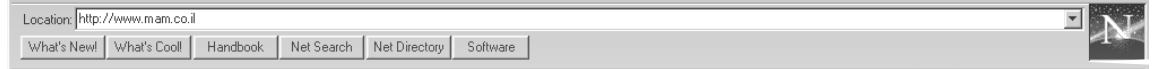
37 המאמר שבו הונחו היסודות לשיטת ההצפנה במפתח ציבורי הוא: W. Diffie and M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22, 6 (1976) pp. 644-654. נראה שהשיטה נולדה אף קודם לכן, במאי 1975, על-פי עדות מפתחיה. ראה תולדות השיטה וסקירת עקרונותיה המתמטיים ב: Albrecht Beutelspacher, *Cryptology (The Mathematical Association of America, 1994)* pp. 97-102. יש להעיר כי על-פי מקור אחר, המאמר דלעיל אינו אלא הפרסום הגלוי הראשון של השיטה, אולם, עקרונותיה נתגלו ונבחנו במעבדות הצבא האמריקאי כעשור קודם לכן. ראה: *The New Encyclopedia Britanica* (15th Edition, 1993) Vol. 16, "Cryptology", at p. 867.

38 RSA הוא ראשיתיות של מפתחי השיטה: Rivest, Shamir & Adleman. השיטה הוצגה במאמר הקלאסי: R. Rivest, A. Shamir and L. Adleman, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM 21 (1978) pp. 1206-1232. שיטה זו אף נרשמה בארה"ב כפטנט מספר 4,405,829 מיום 20 ספטמבר 1983. הפטנט בתוקף עד שנת 2000. אין זה ברור האם ניתן פטנט באירופה ובישראל. כנראה שלא. הפטנט ויישומיו מנוהלים על-ידי חברת RSA Data Security Inc, חברה שנוסדה על-ידי מפתחי השיטה והפועלת מקליפורניה. על השיטה, יישומיה ויישומיה נבוכים" לשיטה (RSA - Frequently Asked Questions - FAQ) ראה אתר האינטרנט של החברה: <http://www.rsa.com>.

39 הביאורים שלהלן מבוססים על ספרו של דוד הראל, **אלגוריתמיקה - יסודות מדעי המחשב** (האוניברסיטה הפתוחה, 1991).

40 one-way trapdoor function





אחר, עליו לאתר את המפתח הציבורי של אותו נמען, ובאמצעותו הוא מצפין את ההודעה המקורית שלו. ההודעה המוצפנת משוגרת לנמען, אשר הוא, ורק הוא, בעל יכולת מעשית לפענחה, הואיל ובידו מצוי המפתח המשלים, הלוא הוא המפתח הפרטי של המפתח הציבורי אותו הפקיד במאגר המפתחות. באופן זה, אנו משיגים את התוצאה של תעבורת מידע מוצפנת בין הצדדים ללא שאלה טרחו להחליף ביניהם מפתח מוסכם מראש. כלומר, פרטיות התעבורה מושגת ללא קשר מקדים.

### 3 זיהוי הצדדים במסחר אלקטרוני

שיטת ההצפנה בצמד מפתחות משיגה תוצאות נוספות והן: זיהוי שולח ההודעה והבטחת שלמותה. אלה מושגים באמצעות הטכניקה הקרויה "חתימה דיגיטלית"<sup>42</sup>. בפרק זה נתחקה אחר תפקידי החתימה במשפט כאמצעי לזיהוי, ונדון באפשרויות ליצור מקבילה אלקטרונית לחתימה כאמצעי לזיהוי הצדדים במסחר אלקטרוני.

#### 3.1 זיהוי באמצעות "חתימה"

לחתימה תפקידים רבים במשפט. יש ומטרתה לאשר תוכנו של מסמך, יש והיא נדרשת על מנת ליתן תוקף למסמך. מכאן, אבחנת היסוד בין תפקיד החתימה כערך ראייתי גרידא<sup>43</sup>, לתפקידה כנושאת אופי

דבר הוא כי צמד המפתחות קשורים מתמטית כך, שהצפנה באחד מהם מאפשרת פענוח במפתח המשלים מבין צמד המפתחות. כלומר, לא רק שתוצאת פענוחה של ההודעה המוצפנת חייבת להיות ההודעה המקורית, אלא שגם הצפנתה של הודעה מפוענחת חייבת להיות ההודעה המקורית.

לעניין תכונת החד-כיווניות, מדובר בכך שפונקציית ההצפנה ניתנת לחישוב יחסית בקלות, בעוד שהפונקציית ההפוכה לה אינה מעשית מבחינה חישובית, במלים אחרות: תהליך ההצפנה הוא יחסית מהיר ונוח, כאשר הפענוח, בהינתן מפתח גדול דיו, דורש משאבי זמן וכוח חישוב בהיקף כזה, ההופך את משימת הפענוח לבלתי אפשרית כמעט, או למצער לבלתי כדאית בעליל.

מטפורה להליך ההצפנה והפענוח האמורים הוא משלוח הודעות בקופסאות הנעולות במנעול מן הסוג אשר ננעל ללא מפתח אלא במעין "קליק", ואשר ניתן לפותחו אך ורק במפתח ייחודי המתאים למנעול המסוים<sup>41</sup>. כלומר, החפץ לשלוח הודעה, מאתר את המנעול של הנמען, והוא יכול להניח את ההודעה בקופסא, שאותה הוא נועל פשוט על ידי "קליק". מכאן ואילך, הקופסא הנעולה יכול שתיפתח על ידי מחזיק המפתח למנעול המסוים, והוא בלבד.

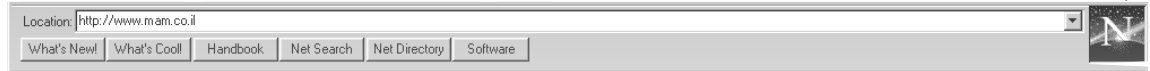
יישום שיטה זו בשוק האלקטרוני הוא פשוט בתכלית. הבה נניח כי כל משתתף בשוק האלקטרוני, מפקיד את המפתח הציבורי במאגר מרכזי הנגיח לכלל המשתתפים. כאשר חפץ מי מהמשתתפים לשלוח הודעה אל משתתף

41 המטפורה המתוארת כאן מבוססת על הסבריו של פרופ' דוד הראל, שם, בעמ' 313 ואילך. במטפורה המתוארת שם הוכנסו שינויים מסוימים.

42 digital signature

43 למשל, לעניין חוזים "חתימה על חוזה יוצרת חזקה בדבר הסכמתו הסובייקטיבית של החותם" הנשיא שמגר בע"א 685/88 קוטרמן נ' קרן תורה ועבודה, פ"ד מז(2) 598, בעמ' 602. ברם, העדרה של החתימה אינה שוללת תוקפו של החוזה, גם כאשר תוקפו של החוזה הוא בקיומו של מסמך בכתב (למשל, בעסקאות במקרקעין, על יסוד ס' 8 לחוק המקרקעין, תשכ"ט - 1969). ראה בעניין זה: ע"א 571/79 זירות מקסים בע"מ נ' ג'רבי ואח', פ"ד לו(1) 589.





או ב"חותם" של אדם או אישיות משפטית כשווה-ערך לחתימת שם בכתב יד. בעניין זה, קובעת פקודת השטרות לעניין חתימה על שטרות כדלקמן:

"מסמך או כתב הטעונים לפי פקודה זו חתימתו של אדם, אין צורך שיחותם עליהם בידו הוא אלא די להם בחתימתו שנכתבה בידי אדם אחר או בהרשאתו או על פיה או בחותמו שהוטבע עליהם בידי עצמו או בהרשאתו."

ואם בשטרות, אשר דרישת החתימה היא מהותית לעצם תוקפם, הדין מכיר באמצעים חלופיים שקולים ושווה ערך, קל וחומר, שלעניין מסמכים אחרים אין למצוא מניעה בדין מלתת הכרה לאמצעים שקולים לחתימה. מכאן, הדרך סלולה לקביעתה של המקבילה האלקטרונית לחתימה.

### 3.2 המקבילה האלקטרונית ל"חתימה"

"חתימה" מיועדת להשיג את המטרות של זיהוי החותם ואישור תוכן ההודעה. כלומר, כאשר מסמך נחתם על ידי מאן דהו, הלז אינו יכול להתכחש לאישורו את תוכן המסמך, וכן, בהנחה כי אכן זו חתימתו, כי הוא זה אשר אישר את המסמך. החתימה האלקטרונית

קונסטיטוטית, כלומר שבלעדי החתימה אין כל תוקף למסמך<sup>44</sup>.

מעבר לכך, חתימה מהווה זיהוי של החותם, באופן שאין הוא יכול להתכחש לכך שהוא זה אשר אישר את תוכנו של המסמך או העניק לו תוקף.

לרוב, חתימה נעשית בכתב-ידו של החותם. אולם, אין הדין מחייב שחתימה תהא דווקא שמו של החותם, ולמעשה, הדין מכיר גם ב"סימן" כחתימה<sup>45</sup> כאמור:

"חתימה" - באדם שאינו יכול לכתוב את שמו - לרבות "סימן"

פשוטו של הכתוב הוא כי מדובר במי שאינו יודע קרוא וכתוב, אשר הדין מכיר בסימנו (כגון טביעת אצבע) כשקול לחתימתו. אולם, נראה כי יש כאן פתח לפרשנות הרואה ב"סימן" כשקול לחתימה בנסיבות מתאימות<sup>46</sup>. כך, למשל, הדין מכיר ב"חותם" כממלא תפקיד השקול לחתימה לגבי תאגידים<sup>47</sup>, לרבות חותם המדינה<sup>48</sup>.

נראה, כי על אף שהדרך המקובלת היא חתימה על ידי כתיבת שם בכתב-יד, אין מניעה בדין מלראות ב"סימן"

44 לעניין שטרות נקבע בס' 22 לפקודת השטרות (נוסח חדש) כי אין חבות בלי חתימה. דהיינו: ללא חתימה על השטר אין המסמך עולה לכדי "שטר" כדן. יש מצבים בהן יש מחלוקת לגבי אופייה של החתימה. ראה למשל, לעניין חתימת עד על צוואה: ע"א 127/87 חיים בדיחי ואח' נ' שושנה בדיחי ואח', פ"ד מג(4)341. בעניין זה דעת הרוב סברה כי לחתימת העד אופי קונסטיטוטית בניגוד לדעת המיעוט של השופט ברק (כתוארו אז).

45 ס' 1 לפקודת הפרשנות (נוסח חדש).  
46 בחוק הפרשנות, תשמ"א - 1981 הושמטה ההגדרה של "חתימה". ברם, לפי ס' 1 לחוק, פירושם של ביטויים ומונחים בדין שטרם כניסת החוק לתוקפו, תוסיף לחול פקודת הפרשנות דלעיל.

47 פקודת החברות (נוסח חדש) מעניקה ל"חותם החברה" תפקיד מרכזי באישור תוכנם של מסמכים על-ידי החברה. ראה למשל: ס' 102, 98, 99, 101, 102 וכיו"ב. השווה לעניין שטרות, ס' (ב)92 לפקודת השטרות (נוסח חדש) הקובע כי חתימה של אישיות משפטית היא בהטבעת חותם.

48 חוק חותם המדינה, תשי"ז - 1949. בחוק זה, "חתימת" המדינה היא בעצם הטבעת החותם.





התנאי החמישי הוא התאמת נוהל החתימה האלקטרונית לתקנות המכרזות על טכנולוגיה מוגדרת בקבילה בדיון ליישום נוהל החתימה הדיגיטלית<sup>50</sup>.

המודל התחיקתי המיושם כאן לשם הכרה במקבילה האלקטרונית לחתימה הוא על-ידי קביעת הקריטריונים אשר מגשימים את תכליתיה של החתימה. כאשר נוהל אלקטרוני ממלא אחר קריטריונים אלו, אין מניעה לראות בנהל זה כשקול לחתימה המסורתית. אכן, מודל זה שימש השראה למדינות נוספות לחקיקתן של חוק חתימה אלקטרונית. מבין אלה, יש למנות את ג'ורג'יה<sup>51</sup>, אינדיאנה<sup>52</sup>, ומדינות אחרות<sup>53</sup>.

במודל זה הטכנולוגיה המיושמת נותרה פתוחה, ולעיתים היא נקבעת על-ידי תקנות ביצוע. ברם, כפי שנראה להלן, הטכנולוגיה של הצפנה בצמד מפתחות, או ההצפנה האי-סינכרונית אשר תוארה לעיל, היא הטכנולוגיה המובילה ליישום המקבילה האלקטרונית לחתימה לצורכי זיהוי הצדדים לסחר האלקטרוני.

### 3.3 חתימה דיגיטלית באמצעות הצפנה

ההצפנה האי-סינכרונית בצמד מפתחות, מפתח פרטי סודי ומפתח ציבורי, אשר תוארה לעיל, משמשת בסיס ליישום של נוהל אשר משיג את היעדים של החתימה האלקטרונית, ואשר מגשים את תכליתיה של החתימה כפי שהוגדרו לעיל.

מבקשת ליצור שקילות תפקודית לחתימה המסורתית באמצעות נוהל מתאים המגשים את התפקידים של החתימה כפי שהיא מוכרת לנו, ועל כן יהא שקול לה<sup>49</sup>.

אשר על כן, סימן אלקטרוני אשר מקיים את תכליתיה של "חתימה", יש לתת לו את אותו התוקף אשר ניתן לחתימה בדרך המסורתית של כתב יד וחותם. למעשה, לפנינו "חותם אלקטרוני" המזהה את החותם ומאשר את תוכן המסמך.

ניסיון להגדיר את התנאים לפיהם סימן אלקטרוני יהא שקול לחתימה נעשה בחוק במדינת קליפורניה. בחוק זה נקבעו חמישה תנאים כדלקמן:

it is unique to the person using it; ייחודי לאדם אשר משתמש בו כחתימתו;

it is capable of verification; הסימן ניתן לאימות;

it is under the sole control of the person using it; הסימן נמצא בשליטתו הבלעדית של המשתמש בו;

it is linked to the data in such a manner that data if they are changed, the digital signature is invalidated; החתימה האלקטרונית נפסלת אם שונה התוכן שהחתימה אמורה לאשר. קרי: ישנו קשר בין תוכן ההודעה והחתימה.

49 ההגדרה המוצעת ל"חתימה אלקטרונית" בחוק של קליפורניה: California Digital Signature Act 1995 היא: "An electronic identifier. Created by the party using it to have the same force and effect as the use of a manual signature" נוסח החוק: <http://www.ss.ca.gov/digsig/digsig.htm>.

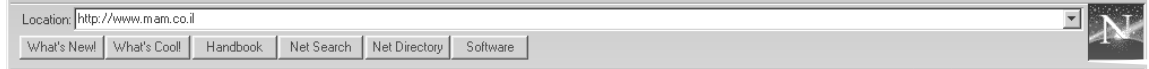
50 בתאריך 23 במאי 1997 פורסם הנוסח המוצע של התקנות, לפיהן, נוהל החתימה הדיגיטלית צריך להתאים לטכנולוגיה מקובלת, כגון: הצפנה בשיטת צמד מפתחות: ציבורי ופרטי, כפי שידון להלן. התקנות, מאפשרות הכרה בטכנולוגיות נוספות מעת לעת, על פי הליך המוגדר בתקנות. ראה נוסח התקנות באתר דלעיל.

51 Georgia Electronic Records and Signatures Act, 1997 Georgia S.B. 103 (Enacted 22 April 1997).

52 Electronic Digital Signature Act, 5 June 1997 ראה סיכום חוק זה וחקיקה נוספת של חתימות אלקטרוניות בכתובת: [הסיכום נערך על-ידי: Thomas J. Smendinghoff ממשרד עורכי-הדין משיקאגו, McBride Baker & Coles - להלן: Smendinghoff]

53 ראה שם אצל Smendinghoff: New Hampshire; Texas Iowa; Kansas; Nebraska; בהתקשרות אל מוסדות יש והיא חלה על כל התקשרות אלקטרונית מסחרית או ציבורית, ויש ותחולתה היא לצרכים מוגדרים, כגון: בהתקשרות אל מוסדות ממשל.

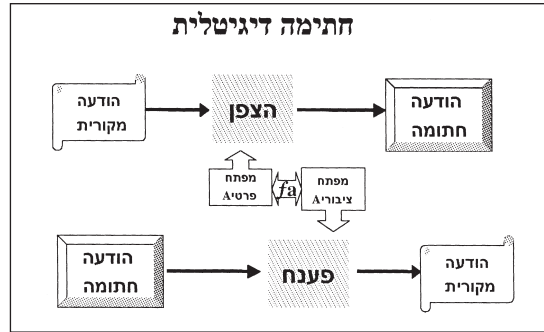




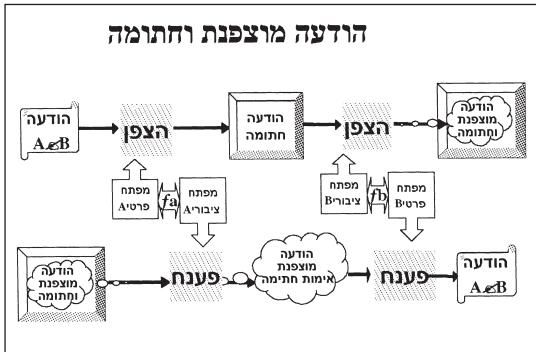
נעולה זו אפשרית אך ורק באמצעות המפתח המתאים הנמצא ברשות הציבור. מכאן, כאשר מפתח מסויים הוא זה אשר מסוגל לפתוח קופסא נעולה זו, כי אז יכולים אנו להיות משוכנעים בדבר זהותו של שולח הקופסא.

באמצעות טכניקה זו, ישנו אימות כמעט ודאי בדבר זהותו של שולח ההודעה. מובן, שעל מנת להשיג גם את אבטחת המידע של ההודעה, יש לנקוט בשתי הטכניקות בעת ובעונה אחת. כלומר, ההודעה מוצפנת כמתואר לעיל ואחר נחתמת בהתאם לשיטה המתוארת כאן. כך, משיגים את פרטיות ההודעה, שלמותה, מהימנותה ואימות שולחה. כלומר, מושגת גם המטרה הנוספת של "חתימה דיגיטלית", קרי: שלמות ההודעה. במילים אחרות, לאחר שההודעה נחתמה והוצפנה, אין המוסר יכול להתכחש לה, אבל אין המקבל יכול לפגוע בשלמותה של ההודעה בנוסח המקורי כפי שנקבע על ידי שולחה.

נוהל החתימה הדיגיטלית באמצעות הצפנה זכה להכרה חוקית במדינות רבות. החלוצה מבין אלה היא מדינת יוטה אשר בארה"ב, שקבעה בחוק<sup>54</sup> כבר בשנת 1995 את שקילותו החוקית של נוהל החתימה הדיגיטלית שלהלן לחתימה כדן.



הנוהל האמור מנצל את תכונת ההפכיות של שיטת ההצפנה במפתח ציבורי. כאמור, הודעה שהוצפנה במפתח אחד, ניתנת לפענוח במפתח המשלים. לפיכך, אם וכאשר אדם מצפין את הודעתו באמצעות המפתח הפרטי הסודי השמור עמו, הודעה זו ניתנת לפענוח באמצעות המפתח הציבורי המשלים. הואיל, ומפתח ציבורי זה, והוא בלבד, הוא זה אשר יכול לפענח ההודעה המוצפנת בהליך זה, כי אז ברור למפענח כי השולח הוא הבעלים של המפתח הציבורי, הוא ולא אחר. במילים אחרות, השגנו את זיהויו של השולח ללא עוררין.



טכנולוגיה זו של חתימה דיגיטלית באמצעות הצפנה זוכה להכרה רחבה כאמצעי יעיל ליישום המקבילה האלקטרונית לחתימה לצורכי זיהוי הצדדים בסחר

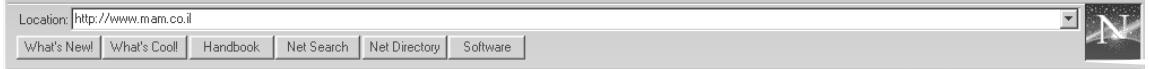
כדי להדגים נוהל זה במטפורה שהוזכרה לעיל, נניח כעת שכל אחד מן המשתתפים הניח גם את המפתח המתאים לפתיחת מנעול ה"קליק" שברשותו<sup>55</sup>. אותו אדם, המבקש לשלוח הודעה, מניחה בקופסא ונועלה באמצעות מנעול ה"קליק" שברשותו. פתיחת קופסא

54 The Utah Digital Signature Act, Utah Code Annotated sec. 46-3-101 to sec. 46-3-504 (1995) code/TITLE46/46\_03.htm)/http://www.le.state.ut.us.

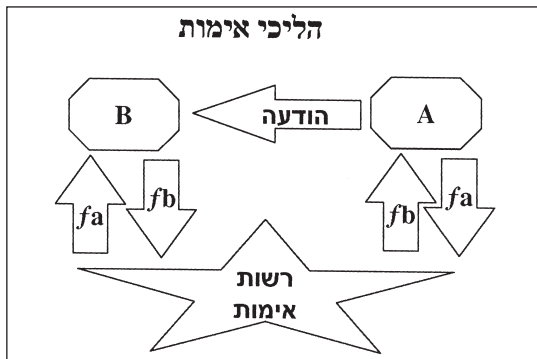
55 קטע הדגמה זה מבוסס על פיתוח המטפורה של פרופ' הראל כאמור. למעשה, המפתח המתואר כאן אינו אלא אותו מנעול "קליק" אשר הונח ברשות הציבור. השימוש באותו אובייקט כאנלוגי למנעול, ובנישימה אחת גם כאנלוגי למפתח נובעת מתכונת ההפכיות המתמטית של הפונקציות שהן עסקין.







מפתח זה נמסר אל כל צד מעוניין החפץ ליצור תקשורת עם אותו אדם. לחילופין, הצד השלישי האמור יוכל לאשר, לפי בקשתו של צד מעוניין, את זהותו של האדם אליו שייך מפתח ציבורי נתון.



אימות חתימות זה, אינו שונה באופן מהותי מאימות לחתימה המסורתית הנערך, למשל, על-ידי נוטריון<sup>61</sup>. ואכן, הצורך באימות, כאמור, הוכרה בחקיקה בעניין "חתימות דיגיטליות". החוק הראשון בעניין זה אשר נחקק במדינת יוטה בארה"ב, אף הסמיך חקיקה זו להסדרים הנוגעים לנוטריונים<sup>62</sup>.

האלקטרוני. מדינות רבות<sup>56</sup> כבר אימצו בחקיקה את המודל הזה, ומדינות רבות אחרות, חקיקה דומה נמצאת בהליכים מתקדמים<sup>57</sup>.

בשלב זה, גל החקיקה בעניין חתימה דיגיטלית שוטף בעיקר את ארה"ב<sup>58</sup>. ראוי לציין את החוק שנתקבל לאחרונה בגרמניה המאמץ חקיקה מקיפה להסדרת שירותי מידע ותקשורת<sup>59</sup>, והכולל גם הסדרים מפורטים בנוגע לחתימה דיגיטלית באמצעות הצפנה<sup>60</sup>.

### 3.4 הליכי אישור מפתחות הצפנה

הבעיות העיקריות ביישומה של טכנולוגיית החתימה הדיגיטלית באמצעות הצפנה, הוא העדר הביטחון בדבר הקשר שבין המפתח הציבורי, ובין אמינות זהותו של מוסר המפתח למאגר הציבורי. לפיכך, אין מנוס משימוש בגורם מתווך אשר יאשר את זהותו של מוסר המפתח. הליכי אימות אלו הם מחויבים על מנת ליצור שוק פתוח ואמין של זהות מוסרי המפתחות למאגר הציבורי. הליכי אימות אלו מבוצעים על ידי רשות אימות, על פי השיטה המתוארת כדלקמן: המפתח הציבורי מופקד בידי צד שלישי אשר גם מבטיח את איהויו של מוסר המפתח והשייך של המפתח לאדם.

Minnesota (19 May 1997); Mississippi (17 March 1997); New Mexico (4 March 1997); Oregon (23 July 1997); 56 Washington (29 March 1996) ראה Smendinghoff לעיל.

57 ראה סיכום מצב החקיקה אצל Smendinghoff לעיל. נכון ליום 17 בספטמבר 1997, מבין מדינות ארה"ב חוקו חוקים או ניסחו הצעות חוק המטפלים בחתימות אלקטרוניות, לרבות באמצעות הצפנה.

58 גם בצרפת, איטליה, קנדה, דנמרק, יפן ועוד שוקלים חקיקה דומה. ראה Smendinghoff לעיל.

59 הגרמני - Budensteg - ביום 13 ביוני 1997. החוק יקבל תוקף סופי לאחר השלמת תהליך חקיקה כמתחייב בחוק הגרמני. ראה פרטים מלאים על תהליך החקיקה ונוסח אנגלי של החוק אשר נערך על-ידי Christopher Kuner ראה: <http://ourworld.compuserve.com/homepages/ckuner>

60 Article 3 לחוק האמור. ראה שם, נוסח החוק והצעה לתקנות הביצוע מיום 7 ביולי 1997.

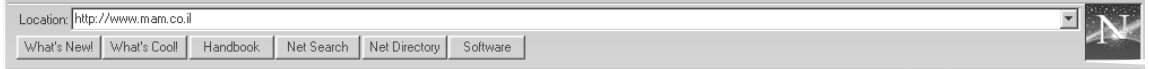
61 נוטריון מוסמך לאמת חתימות על מסמכים על-פי ס' 7 לחוק הנוטריונים, תשל"ו - 1976. הדין מכיר בדרכי אימות חתימה אחרות לפי העניין. ראה, למשל, אימות חתימות במסמכי עסקאות במקרקעין, על-פי: תקנות המקרקעין (ניהול ורישום) תשל"ל - 1969.

62 פרק 46 לקוד של מדינת יוטה, הכולל את החקיקה בעניין חתימה דיגיטלית (לעיל הערה ) דן בנוטריונים; לפיכך מכונה מנגנון אימות זה גם כ־ Cyber-Notary.









## 4 הפיקוח על אמצעי הצפנה

### 4.1 פיקוח על העיסוק באמצעי הצפנה

שר הביטחון, בתוקף סמכותו על-פי חוק הפיקוח על מצרכים ושירותים<sup>67</sup> הסדיר בצו את העיסוק באמצעי הצפנה<sup>68</sup> והכריז על אמצעי הצפנה כשירות בר-פיקוח<sup>69</sup> על-פי החוק דן.

על-פי אכרזת הפיקוח דלעיל, מוגדר העיסוק באמצעי הצפנה<sup>70</sup> בצורה רחבה ביותר בהאי לישנא:

"עיסוק באמצעי הצפנה" - עיסוק בפיתוח, בייצור, בהחזקה, בשימוש, ביבוא, [ביצוא]<sup>71</sup> בהובלה, בהעברה ממקום למקום או מיד ליד, בהפצה, במכירה או ברכישה של אמצעי הצפנה, של שיטת הצפנה, של מפתח הצפנה, או של רשומה המתייחסת להצפנה או טיפול בהם בכל דרך אחרת."

אף המונחים "אמצעי הצפנה", "שיטת הצפנה", "מפתח הצפנה" ו"רשומה המתייחסת להצפנה"

המופיעים בהגדרה דלעיל הוגדרו באורח דומה, כלומר: באופן מרחיב וגורף. לבחינה מיוחדת ראויה ההגדרה של "אמצעי הצפנה". זו כוללת כל התקן, מכשיר, כתב סתרים וכיו"ב אשר:

"... הגורמים או המיועדים לגרום לאי-הבנה מוחלטת או חלקית של מידע למשך תקופת זמן כלשהיא בין על ידי מי שיש בידו ובין מי שאין בידו מפתח הצפנה;"

עינינו הרואות שהמחוקק נתכוון לכך כי העיסוק באמצעי הצפנה בכל צורה ובכל אופן יהיה תחת פיקוח, ויחייב רשיון מן המנהל שמונה על ידי שר הביטחון לעניין צו הפיקוח<sup>72</sup>.

### 4.2 פיקוח על יצוא טכנולוגיות הצפנה

אמצעי הצפנה כפופים גם לדינים מיוחדים שעניינם פיקוח על ייצוא של ציוד לחימה וידע צבאי בתאם לצו אשר הותקן על ידי שר הביטחון<sup>73</sup>. אמצעי הצפנה מוגדרים כ"ציוד לחימה" ושוכנים אחר כבוד בסמיכות

67 תשי"ח - 1957, ס"ח תשי"ב, 24

68 צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) תשל"ה - 1974, ק"ת תשל"ה 15 45 ספטמבר 1974. [להלן: "צו הפיקוח"]

69 אכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) תשל"ה - 1974, ק"ת תשל"ה, 15 46 ספטמבר 1974. [להלן: "אכרזת הפיקוח"]

70 ההגדרה דן שונתה באכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) (תיקון), תשמ"ה - 1984, כך שהמונח "ביצוא" הוצא מגדר ההגדרה כאמור. ברם, אין להבין מכך, שעניין היצוא שוחרר מפיקוח. למעשה, יצוא של אמצעי הצפנה הועבר לפיקוח מיוחד כפי שידון להלן.

71 המילה "ביצוא" הושמטה בתיקון משנת 1984, כאמור לעיל.

72 על פי סעיף 2(א) לצו הפיקוח "לא יעסוק אדם באמצעי הצפנה אלא על פי רשיון מאת המנהל ובהתאם לתנאי הרשיון". הרשיון ניתן לשנה או לתקופה קצרה יותר (ס' 2(ב) לצו) וכרוכה בתשלום אגרה (ס' 7 לצו). למנהל שיקול דעת רחב לעניין מתן הרשיון, ראה סעיף 5 לצו: "המנהל רשאי לתת את הרשיון, לסרב לתיתו, לקבוע תנאים לנתינתו, להתלותו או לבטלו, הכל כפי שימצא לנכון".

73 צו הפיקוח על היצוא (ציוד לחימה וידע צבאי), תשל"ז - 1977 (ק"ת תשל"ז, 1962) [להלן: "צו היצוא"]. הצו הותקן בתוקף הסמכויות שניתנו לשר על-פי מכוח חוק הפיקוח על מצרכים ושירותים, תשי"ח - 1957 ועל-פי פקודת הסמכויות בעניין היבוא, היצוא והמכס (הגנה) 1939; הפקודה דן הוחלפה בפקודת היבוא והיצוא [נוסח חדש], תשל"ט - 1979 (דיני מדינת ישראל, נוסח חדש 32, תשל"ט, 625 מיום 29.3.79). הצו הותקן ביום 15 במאי 1977 ונכנס לתוקף חודשיים מיום פרסומו (הצו פורסם בתאריך 16.6.77, כך שתחילתו היא 16 באוגוסט 1977).





לכלי יריה, חומרי נפץ ומטוסי קרב<sup>74</sup>.

היבטים: הגדרת אמצעי ההצפנה אשר הוטל עליהם פיקוח, והקף העיסוקים אשר עומדים תחת פיקוח. בשני היבטים אלו נוסחו של הצו הוא כה מרחיק לכת, עד אשר יש לתמוה אם בכלל הנו בראיפה במציאות הטכנולוגית דהיום, והאם יש הצדקה מהותית לקיומו בהיקף כה רחב.

טול, דרך משל, את ההגדרה של "אמצעי הצפנה". פרשנות היוצאת ממשוטו של הנוסח בצו, עלולה לגרוס כי שיטות ההצפנה הפשטניות אשר שימשו בתנ"ך, כפי שהודגם לעיל, כגון: שיטת חילופי האותיות של אתב"ש, אלב"ם או אטב"ח הן שיטות הצפנה על-פי אכרזת הפיקוח, ויש צורך באישור מהמנהל על מנת לעסוק בהם...

כך הדבר לעניין גדרו של העיסוק המפוקח. פירוט העיסוקים אשר הצווים דלעיל מתיימרים לפקח עליהם הוא כה גורף עד אשר יש מקום לסברה, כי אף עיון לשמו באמצעי הצפנה ולימוד תורת הקריפטוגרפיה אף הוא בא תחת כנפי צו הפיקוח. היעלה על הדעת, כי הגבלות כה חריפות יוטלו על חופש הלימוד (קרי: חופש הביטוי<sup>78</sup>)!:

נראה כי יש מקום לעדכן את הצו לפי צרכי השעה, כך שתצומצם תחולתו בשני ההיבטים האמורים. ואמנם, עיון בדין הנוהג במדינות אחרות, מלמד שאכן כך

בהתאם לדין הפיקוח על יצוא "ציוד לחימה", כאמור, כל ייצוא של ציוד זה, לרבות, יעוץ או תיווך בקשר ליצוא<sup>75</sup>, מחייבים קבלת היתר מאת המנהל אשר ממונה על-ידי שר הביטחון לעניין זה. חשוב לציין כי היתרים על-פי צו הפיקוח דגן יכול שיהיו על בסיס של עיסקה בודדת<sup>76</sup>, ומתן ההיתר נתון לשיקול דעת רחב של המנהל האמור<sup>77</sup>.

אין חולק כי הסדרי הפיקוח האמורים ראויים לטיפול ב"ציוד לחימה" כמשוטו של מקרא. ברם, שאלה היא האם מידת פיקוח כה הדוקה ראוי כי תחול גם על אמצעי הצפנה.

### 4.3 הצורך בהקלת הפיקוח על הצפנה

השאלה המרכזית היא, איפוא, האם גדרם הרחב של צווי הפיקוח על אמצעי הצפנה אכן הולמים את הצרכים העדכניים של מסחר אלקטרוני. מובן, ששיקולים מכריעים של ביטחון לאומי הם אשר עמדו לנגד עיני מתקיני הצווים. ברם, נראה שההתפתחויות הטכנולוגיות מאז שנות השבעים ועד היום הן כה מהפכניות שיש מקום להעריך מחדש את היקף תחולתם של הצווים דגן.

נראה, כי צווי הפיקוח בנוסחם כיום הנם גורפים בשני

74 התוספת לצו היצוא הנ"ל מפרטת מהו "ציוד לחימה" אשר הנו תחת פיקוח על-פי צו זה. פריט 14 - "אמצעי הצפנה" - הוסף בצו הפיקוח על היצוא (ציוד לחימה וידע צבאי) (תיקון), תשמ"ה - 1984 (ק"ת תשמ"ה, 114).

75 ראה סי' 2 לצו היצוא הנ"ל.

76 סי' 2 (ג) לצו היצוא קובע כי "היתר יכול שיהיה לעיסקה אחת או לשתי עיסקות או יותר".

77 סי' 4 לצו היצוא קובע לאמור: "המנהל רשאי לתת ההיתר, לסרב לתיתו, לקבוע תנאים לנתינתו, ולהתלותו או לבטלו, הכל כפי שימצא לנכון".

78 בפסק דין שניתן ביום 25 באוגוסט 1997 בבית המשפט הפדרלי המחוזי בקליפורניה בעניין Daniel J. Bernstein v US Department of State נקבע כי תוכנת הצפנה מוגנת על פי התיקון הראשון לחוקת ארה"ב בדבר חופש הביטוי, ולפיכך הגבלות לכאורה על פרסום התוכנה, לרבות מחוץ לארה"ב (שם הפיקוח הוא על יצוא אמצעי הצפנה), אינן עומדות במבחן חוקתי. ראה: [http://www.eff.org/pub/Legal/Cases/Bernstein\\_v\\_DoS/Legal/970825\\_decision.html](http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoS/Legal/970825_decision.html).





אמצעים לזיהוי הצדדים למסחר האלקטרוני. נראה, כי טכנולוגיות מתקדמות של אמצעי הצפנה הקרויים "חתימה דיגיטלית" יכול ויתנו מענה נאות לקושיא זו. ואמנם, חקיקה בדבר "חתימה דיגיטלית" זו הולכת ומתגבשת בקרב המדינות המפותחות, ולא מן הנמנע כי גם המשפט הישראלי ראוי כי יאמץ הסדרים ברוח זו.

לעניין מערכת המשפט בישראל, נראה כי יש מקום לעדכן את הפיקוח על אמצעי הצפנה ברוח השעה. עדכון זה ראוי כי יעשה על מנת לאפשר פיתוח ויישום טכנולוגיות התשתית של מסחר אלקטרוני ומנגנוני "חתימה דיגיטלית" בכלל זה.

תגובות, הערות וביקורת יתקבלו בברכה בכתב או בדואר אלקטרוני בכתובות הבאות:

הפקולטה למשפטים, אוניברסיטת חיפה, הר הכרמל,  
חיפה 31905

נעשה<sup>79</sup>. למשל, בארה"ב, היקף העיסוק שהנו בר-פיקוח הוא אך ורק יצוא של אמצעי הצפנה, כאשר גדרם של האמצעים אשר תחת פיקוח מצומצמים לאלה הגדולים מעצמת הצפנה מוגדרת בדן<sup>80</sup>. אף פיקוח מצומצם זה חשוף לביקורת חריפה בארה"ב<sup>81</sup> והקלות בפיקוח נערכות שם מעת לעת.

## 5 סיכום ומסקנות

מסחר אלקטרוני יכול לסייע לפרט, לפירמה העסקית ולחברה. על מנת שיעד זה יושג, אין זה מספיק לפתח את הטכנולוגיות המתאימות, אלא יש צורך גם בהסדרי תשתית משפטיים הולמים. הסוגיות המשפטיות המתעוררות בהקשרי מסחר אלקטרוני הן רבות ומגוונות, ובחלקן הינן שאלות הנובעות מן האופי הגלובאלי של מערכת המסחר האלקטרוני.

כאן נעשה ניסיון ללבן סוגיית יסוד אחת, והיא:

79 בהכרזת בון של שרי האיחוד האירופאי שדנו במסחר אלקטרוני הוכר הצורך בפיתוח אמצעי הצפנה חזקים כתנאי לקידומו של מסחר אלקטרוני. ראה: Ministerial Declaration, The European Ministerial Conference on Global Information Networks: Realising the Potential (Bonn 6-8 July 1997) פרטים על הדיונים ונוסח ההכרזה ראה: <http://www2.echo.lu/bonn/final.html>.

80 תקנות הפיקוח על אמצעי הצפנה בארה"ב הם חלק מתקנות הפיקוח על היצוא של נשק וטכנולוגיות ביטחוניות: Parts 730-774 Export Administration Regulations (EAR) 15 CFR. התקנות ניתנות לאיתור באינטרנט באתרים רבים. ראה למשל: <http://www.jya.com/eartoc.htm> וכן באתר הרשמי של המדפיס הממשלתי האמריקאי - GPO, <http://www.access.gpo.gov> בכתובת:

81 לביקורת חריפה במיוחד זכתה תוכניתו של הממשל ליוזמת הפקדת מפתחות הצפנה אשר זכתה לכינוי - The Clipper Chip. ראה מאמריו של A. Michael Froomkin. בנושא זה באתר הבית של המחבר בכתובת: <http://www.law.miami.edu/~froomkin/> מאמריו פורסמו גם בכתבי עת של נייר, ראה: The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution, 143 University of Pennsylvania Law Review 709 (1995)

