

## התוקף ההלכתי של חתימות דיגיטליות

מאת אבן ישראל פוקרוי

מבוא

מאמר זה עוסק בהיבטים ההלכתיים הקשורים לשימוש בחתימה דיגיטלית בשטרות. המאמר עוסק מנושאים הבאים:

1. מקור שסומכים על חתימת העדים בשטרות
2. הבנה בדיני עדות בשטרות
3. תנאים לקיום שטר על פי החתימות
4. מאפיינים של חתימות דיגיטליות
5. בעיות העולות מאפשרות לשכפול דיגיטלי
6. מסקנות

### מקור שסומכים על חתימות העדים של השטר

הכלל הוא שקבלת עדות היא רק בעל פה ולא בכתב. דרשו חז"ל: "על פי שניים עדים או על פי שלושה עדים יקום דבר ולא על פי כתבן ולא על פי תורגמן" (ספרי דברים י"ט:י"ד פסקה קפ"ח).

והיינו, שעדות מתקבלת על ידי שמיעה מפי העדים ולא על ידי קבלת עדות בכתב.

עיין עוד בדברי הרמב"ם: "דין תורה שאין מקבלים עדות לא בדיני ממנות ולא בדיני נפשות אלא מפי העדים" (הלכות עדות ג:ד).

הרמב"ם ממשיך או מביא תקנות חז"ל: "אבל מדברי סופרים שחותכין דיני ממנות בעדות שבשטר אף על פי שאין העדים קיימים כדי שלא תנעול דלת בפני לוויין" (שם).

כלומר, הדין שמקבלים שטר בבית דין כראיה לבעל חוב הוא אך ורק מדברי סופרים. הסיבה לכך היא לשפר היחסים בין מלוה ולוה. ייתכן מצב שהמלוה יצטרך לחפש אחרי העדים לקבל כספו בחזרה. הוא יחשוב שזה טרחה יתרה ולא יסכים לתת הלואה לעני. הרבנן הקלו עליו ועשו מנגנון שאפילו במקרה שהעדים הלכו למדינות הים או מתו, המלוה יכול לקבל את כספו. יש עוד מקום שהנימוק של "שלא תנעול דלת בפני לוויין" מופיע. זה בעדות של דיני ממנות שהרבנן גזר שאין צורך לדרישה וחקירה (סנהדרין ג).



## הבנה בדיני עדות בשטרות

פועל יוצא מהתקנה שמאפשר עדות שבשטר, הוא שהשטר עצמו מהווה עדות. הרמב"ם מחזק את התוקף של העדות בשטר עד כדי כך שהוא פוסק: "עדים החתומים על השטר הרי הם כמי שנחקרה עדותן בבית דין" (רמב"ם עדות ג:ו).

יש כאן שני צדדים של התקנה שניתן לקבל עדות בשטר מפני "שלא תנעול דלת בפני לוויין":

1. ניתן לקבל עדות בכתב ואין את החסרון של "מפיהם ולא מפי כתבם"
2. אין צורך לדרישה וחקירה. הלא העדים לא עומדים לפנינו

יש כאן קשר בין שני הצדדים של התקנה. ההלכה שעדות שבשטר שהיא בעל תוקף בנויה על היותה לדרישה וחקירה. הראיה היא, שכל מקום שעדין יש צורך לדרישה וחקירה כמו בדיני קנסות (סנהדרין ה:ח), לא מועיל חתימת עדים.

העדות שבשטר מקבלת תוקף של עדות גם לגבי ההלכה של "כיוון שהגיד שוב אינו חוזר ומגיד". זה כמו הדין בעדות בעל פה שהוא לא יכול לחזור מעדותו, גם בעדות בשטר הוא לא יחזור מעדותו. וראה הרמב"ם בהלכות עדות (ג:ו) שפוסק כך.

הדבר הזה נכון כשיש הוכחה שזאת חתימתו. כלומר, כשיש עדים שמעידים שזה כתב ידו או שיש חתימה בשטר אחר לבדוק מולה. אבל, אם קיום השטר הוא רק מפי העד עצמו והוא אומר שהוא היה פסול או מוטעה אז הוא נאמן (שם).

אפשר לראות מזה שלפי דעת הרמב"ם, העדות של השטר הוא בדיוק כמו עדות בבית דין. וכמו שהבית דין פוסק לפי העדות, כך כאשר מביאים שטר, הבית דין פוסק לפיו.

## תנאים לקיום השטר על פי חתימות

היסוד שעליו בנוי ההלכה שמקבלים שטרות עם חתימות העדים הוא שיש ראייה שלא ניתנת להכחשה. אנו אומרים שהחתימה היא כמו עדות וברגע שעד מעיד, הוא לא יכול לחזור ולומר שהוא לא העיד. אותה מערכת קיימת בשטרות, אבל קצת שונה. אם יש ספק בחתימה, אפשר להביא עוד שטר עם חתימה של אותו העד או כתב יד אחר שמוכיח שזה הוא כתב ידו. ברגע שעושים כך, אפילו כשהעד עצמו אומר שהוא לא זוכר שחתם או לא זוכר את ההלואה (רמב"ם הל' עדות ח:ד), העדות כשירה.

אז, עיקר הכוח של חתימת העדים בא מזה שכל עוד שאפשר להוכיח שהחתימה היא באמת של העד, השטר קיים אפילו כאשר העד לא קיים.



הדבר שמאפינת חתימה דיגיטלית הוא שזה כמעט בלתי אפשרי לזייף אותה. הדרך לבצע את זה היא על ידי אלגוריתמים חד-סטריים (One Way Hash).

הפונקציה הזאת מבוססת על הצפנה אי-סימטרית שמשמשת ב Public-Private Keys. יש שני מפתחות שאינם זהים אבל יש יחס מתמטי ביניהם. יש פונקציות שכאשר מועבר תוכן מסוים דרכם, מוצאים קיצור של התוכן שהיא ייחודית כלפיו וכלפי דברים אחרים. זאת אומרת, שכאשר בודקים את התוכן הראשוני מול התוצאות, כל שינוי – לא משנה כמה קל – יביא לתוצאה אחרת מהפונקציה. בדרך זאת, אפשר לוודא שלא היה שום שינוי בתוכן המקורי.

במקרה של חתימה דיגיטלית, לוקחים את התוצאות ומעבירים אותם דרך פונקציה אחרת שמשמשת במפתח האישי בתור נתון, ובנויה בצורה שרק עם המפתח הציבורי (Public Key) אפשר להפוך את הפונקציה. יוצא מזה, שכל מי שיש לו את המפתח הציבורי יכול לבדוק עם התוצאה "נחתמה" על ידי המחזיק במפתח האישי. ברגע שהדבר הזה ברור, אפשר להשתמש בתוצאה לוודא שהתוכן לא עבר שום שינוי.

### המערכת הזאת בנויה על ההנחות הבאות:

1. הפונקציות הם חד-סטריים, ואף על פי שקיימת אפשרות לפענח אותם בלי מפתח התהליך הוא כל כך קשה ולוקח כל כך הרבה זמן שהוא הופך להיות בלתי אפשרי. המפתח האישי הוא אישי ובלתי פריץ. יש מנגנונים שמספקים מפתח לא ניתן לגניבה וזיוף, החל מצורך לסיסמא ועד לשימוש בביומטריקה כמו טביעת אצבעות.

2. יש גישה בטוחה למפתח הציבורי. יש צורך למנגנון לוודא שהמפתח לא הוחלף ומישהו אחר יחתום בשמו.

בכל מקרה, הדברים שמאפיינים חתימות דיגיטליות הם אותם הדברים שדורשים ההלכה מחתימה בשטר. האפשרות לזיוף היא כל כך זעירה שאין מקום להתחשב. ברגע שמישהו חותם על שטר דיגיטלית עם חתימה דיגיטלית הוא מעיד בדיוק באותה דרגה כמו שהוא מעיד בחתימה פיזית.

### בעיות העולות משטרות וחתימות דיגיטליות

הבעיה הבולטת ביותר במימוש של שטר דיגיטלי היא באפשרות לשכפל אותה בקלות. אין דבר שמונע ממלווה להעתיק את השטר לדיסק אחר ולתבוע את הלווה שנית. יש שתי דרכים לעקוף את הבעיה הזאת. האפשרות הראשונה היא במסירת השטר. בפירעון החוב, המלווה נותן עותק של השטר ללווה כהוכחה שהחוב נפרע. עצם העובדה שהלווה מחזיק בעותק של השטר מהווה ראיה שהשטר נפרע.

הדרך השניה היא לתת שובר שהוא שטר אחר עם עדים שהחוב נפרע. בשתי האפשרויות, ללווה יש ראייה מובהקת שהוא פרע את החוב כי בלי הפירעון, לא היה לו את השטר. בצד הטכני, קיימות כמה בעיות במימוש תוכנית חתימה דיגיטלית אחיד ובטוח. מצד הביטחוני קיימות בעיות של פריצת מפתחות וכמה סוגים של "הקים" שונים. כמו שהזכרתי לעיל, אפשרות אחת לעקוף את חלק מהבעיות האלה היא לכלול סוג של ביומטריקה במפתח בנוסף לסיסמא. הבעיה עם זה היא העלות, למרות שמצד הטכני זה אפשרי ויעיל.

הבעיה היותר מרכזית לעניות דעתי היא אחידות. אמנם זה לא בהכרח בעיה. אפשר לעשות אוסף מרכזי של מפתחות ציבוריות שישמש את כל בתי הדין.

מלבד הבעיות של אבטחת מידע והעברת מידע לכל הדורש, קיימות בעיות של הכנסת חתימות חדשות. אולי יש פתרון לבעיות האלה במה שלמדנו מהמקורות לעיל. ניתן לקיים חתימה של עד על ידי עדות של מישהו אחר שמכיר את חתימתו. זה דומה לשיטת רשת האימון של PGP. ניתן לקבל חתימת שמעון כי אנחנו מאמינים לראובן שנתן את אימונו בשמעון.

## מסקנות

המסקנה הברורה היא שאין מניעה עקרונית למימוש של חתימות דיגיטליות בשטרי חוב. יש מספר בעיות מעשיות שעדיין הם בתהליך של פתרון על ידי קהילת הבטחת המידע ב-Internet. בעיות אלה הם לאו דווקא בעיות הלכתיות. אם ככה, אפילו בערכאות, יש רק התחלת התהליך של קבלת חתימות דיגיטליות. ברגע שחתימות דיגיטליות יתחילו להיות מקובלות בציבור הרחב, ניתן להתחיל לקבל אותם גם בבתי דינים רבניים.

יליד קייפ טאון, דרום אפריקה, י"ג אב תשל"א. בגיל 3 עבר לגור בארה"ב, קודם ב-סן פרנסיסקו ואחר כך ב-רינו, נבדה. בוגר רינו היי סקול, 1989. מיד אחר כך הגיע ארצה בתוכנית NATIV של בתי הכנסת המאוחדים של ארה"ב. למד חצי שנה באוניברסיטה העברית בירושלים וחצי שנה בקיבוץ סעד ושנה בישיבת המבחר באפרת. חזר לשנה ללמוד ביולוגיה בישיבה יוניבסטי בניו יורק ועלה ארצה להמשיך ללמוד ביולוגיה באוניברסיטת בר אילן. בשתי האוניברסיטאות השתתף בתוכנית הישיבה שלהן. התחתן ועזב את העולם האקדמי וחזר לישיבה בתור אברך בעטרת כהנים בעיר העתיקה, שם למד שנתיים לפני יציאה לעולם ההיי-טק.

נשוי עם 5 ילדים

ב-NDS שנתיים וחצי, מהנדס מערכות ב-DCU.