מסמך עזר מספר 3

להנחיית היועץ המשפטי לממשלה

מספר 1.2500 –

הרחבה וביאור של ההנחיה

ושל מסמכי העזר האחרים

תוכן עניינים למסמך עזר מספר 3

הרחבה וביאור של הנחיית היועץ המשפטי לממשלה מספר 1.2500 ושל מסמכי העזר האחרים שלה:

מבוא 5

1. תקציר מנהלים...5

2. תחולת ההנחיה 8

חלק א׳ – הוראות מנחות 9

פרק א׳– עקרונות יסוד בגיבוש הסדר דיגיטלי 9

1. שקילות פונקציונלית...9

1.1 מהי שקילות פונקציונלית 9

1.2 בעולם הדיגיטלי ניתן לתת מענה מדויק למטרות, שלא חודדו בעולם הפיסי 9

1.3 אופן הפעלת עקרון השקילות הפונקציונלית.......................................10

2. אי עדיפות...11

3. ניטרליות טכנולוגית...12

פרק ב׳ – כללים מנחים לגיבוש הסדר דיגיטלי 13

1. התאמת ההסדר לתכליותיו...13

2. יעילות, פשטות וישימות ההסדר..14

3. הערכת סיכונים והתאמת החשיפה להם לערך הנפגע ולעוצמתו 14

4. הקטנת סיכוני ההסדר וחלוקת הנשיאה בהם במקרה של התממשותם.............16

4.1 שני אופנים להקטנת סיכוני ההסדר – שימוש בטכנולוגיות וקביעת כללים נורמטיביים 16

4.2 השפעה על הסיכונים באמצעות קביעת כללים נורמטיביים :........................17

4.2.1 הדרך הראשונה – כללים שיתמרצו את בעל היכולת הטובה יותר לצמצם את הסיכונים 17

4.2.2 הדרך השנייה – כללים שיטילו את הסיכון על בעל היכולת הטובה ביותר לשאת בסיכון ולפזר אותו 18

4.3 שיקולים שיש לשקול בקביעת חלוקת הנשיאה בסיכונים..........................19

5. הוגנות ההסדר בהתאמתו לאוכלוסייה שעליה הוא נועד לחול :...................21

5.1 התאמת נטלי ההסדר למאפייני האוכלוסייה המושפעת ממנו 21

5.2 סבירותה של קביעת ערוץ דיגיטלי כערוץ יחיד.......................................21

5.3 מתן מענה הולם למי שאינו בעל כישורים או אמצעים לעשות שימוש באמצעים דיגיטליים בעצמו :..23

5.3.1 הכלל – מתן מענה הולם..23

5.3.2 מבחן עזר לקביעה האם המענה המתגבש הוא מענה הולם – הפער באיכות השירות.......... 24
5.4 תמריצים 24
6. חזקות מסירה בהסדרים דיגיטליים.......... 26
6.1 הסבר על חזקות מסירה.......... 26
6.2 כללים לקביעת חזקת מסירה 26
פרק ג'– יישום ההסדר בחקיקה - פרשנות דין קיים ויצירת דין חדש 29
1. פרשנות דין קיים – האם הדין הקיים מאפשר את קיומו של ההסדר? 29
2. יצירת דין חדש – כיצד לעגן את ההסדר בדין כשנדרש שינויו: 31
2.1 אופן ניסוח הדין- תכליות, כללים ומאפיינים במקום כלים וטכנולוגיות, וניתוק מהמימד הפיסי 31
2.2 מדרג נורמטיבי 33
2.3 אי עיגון דרישות טכנולוגיות בחיקוק 33
פרק ד' – הוראות בקשר למושגי יסוד בעולם הדיגיטלי.......... 34
1. קיום דרישת הכתב בעולם הדיגיטלי 34
2. מקור והעתק דיגיטלי: הפעלת כללי ההנחיה על דרישת מסמכי מקור 35
2.1 פיחות במעמדו של המסמך המקורי 35
2.2 שקילת חלופות לדרישת מסמך מקורי נוכח הפיחות במעמדו.......... 35
2.3 פרשנות דין קיים בקשר למסמך "מקור" 36
3. חלופות לחתימה: יישום כלל התאמת התכליות באמצעות "שירותי אמון" 38
4. דרישת חתימה בחיקוק - יישום כללי ההנחיה והוראת סעיף 2 לחוק חתימה אלקטרונית 39
תכליות 40
רמת ודאות מספקת.......... 41
התאמת סוג החתימה שייבחר לרמת הוודאות הנדרשת 41
חלק ב' – יישום ההוראות המנחות: הליך בחינה מומלץ לגיבוש הסדר דיגיטלי 43
1. זיהוי מטרתו הכללית של ההסדר הדיגיטלי 43
2. זיהוי תכליותיו של ההסדר הדיגיטלי על כל היבטיו.......... 44
3. זיהוי הגורמים הנוגעים להסדר 48
4. בחינת סיכוני ההסדר:.......... 49
שלב א' – זיהוי הסיכונים 49
שלב ב' – זיהוי עוצמת הפגיעה במקרה של התממשות הסיכון ורמת ההסתברות להתממשות הסיכון 49
שלב ג' – זיהוי מידת יכולתו של כל גורם לשאת בסיכוני ההסדר וזיהוי הכלים שעומדים לרשותו לשם הקטנת הסיכונים.......... 50
5. ביצוע ניהול סיכונים: התאמת החשיפה לסיכונים לערך הנפגע ולעוצמת הפגיעה ובדיקה האם ניתן להקטינם.......... 51
6. בחינת הנטלים, שבהם יכול לעמוד כל גורם המושפע מההסדר: 51

שלב א׳ – זיהוי הנטלים ומידת השפעתם על כל גורם 52
שלב ב׳ – התאמת הנטלים 52
7. בחירה בין הכלים הקיימים להגשמת כל תכלית 52
8. בחינת התאמת ההסדר לדין והצורך לעגנו בחקיקה 53
חלק ג׳ – מסמכי עזר 54
מסמך עזר 1- תרשים הליך בחינה מומלץ לגיבוש הסדר דיגיטלי 54
מסמך עזר 2– מידע שימושי בנוגע למעבר מעולם הפיסי לעולם הדיגיטלי: 55
1. הסבר על "שירותי אמון" נפוצים 55
1.1. זיהוי אלקטרוני 55
1.2 חתימה אלקטרונית 56
1.3 חותם אלקטרוני 60
1.4 חותמת זמן 62
1.5 דואר אלקטרוני רשום 62
1.6 תעודה אלקטרונית המשמשת לאימות אתר אינטרנט 63
2. סקירת סוגים נפוצים של חתימות אלקטרוניות, מאפייניהן ואופן השימוש בהן בחיי המעשה ומשמעותן הראייתית: 64
2.1 חתימה אלקטרונית מאושרת 64
2.2 חתימה אלקטרונית מאובטחת 65
2.3 חתימה אלקטרונית מאובטחת ב"מערכות סגורות" 66
2.4 חתימה אלקטרונית 68

מבוא

1. תקציר מנהלים:

ככל שחולפות השנים, הקדמה הטכנולוגית מאפשרת פיתוח של יותר ויותר ערוצים דיגיטליים לביצוע פעולות שונות. בהתאם לכך, מתחזקת עם השנים המגמה הקיימת לעבור לתהליכים דיגיטליים ולאפשר ביצוע של פעולות ושירותים – הן ציבוריים והן פרטיים – באופן דיגיטלי.

לשם כך, פורסמה הנחיית היועץ המשפטי לממשלה שמספרה 1.2500 (להלן: "**ההנחיה**"). ההנחיה נועדה לסייע ולתמוך במשרדי הממשלה בביצוע המעבר מן העולם הפיסי אל העולם הדיגיטלי, תוך ניהול סיכונים וקיום התכליות הנדרשות. זאת, הן במסגרת הסדרים הקשורים לשירותים ממשלתיים וציבוריים כדוגמת הגשה מקוונת למדינה, והן במסגרת יצירת הסדרים החלים על השוק הפרטי כדוגמת הסדרת מוצר שנוצר בעולם הדיגיטלי (להלן: "הסדרים דיגיטליים").

המעבר לעולם הדיגיטלי משקף את מדיניות הממשלה, כפי שהובעה בשורה של החלטות ממשלה[1]. הוא מעודד פיתוח והתייעלות ומסייע לממשלה לשפר את השירות לציבור ולשמור על האינטרס הציבורי. יובהר, כי השאלות המשפטיות המתעוררות בהסדרים דיגיטליים אינן שונות במהותן משאלות משפטיות אחרות, והן אינן מעוררות מורכבות מיוחדת. על כן, אין מקום להירתע מגיבוש הסדרים דיגיטליים.

ההנחיה קובעת כללים מנחים ומסבירה כיצד לגבש הסדר דיגיטלי, כך שיעמוד בדרישות הדין ויימצא במתחם הסבירות. כללים אלו נועדו להנחות יועץ משפטי של משרד ממשלתי או של יחידת סמך במתן ייעוץ משפטי, ככל שהוא נדרש לכך, בהיבטים משפטיים של הסדרים דיגיטליים. זאת, בין אם ההסדרים מעוגנים בדין, בנהלים, בכללים, בנוהג או בהסכם. כמו כן, הכללים נועדו להתוות את שיקול דעתו של היועץ המשפטי במסגרת עיגון ההסדר בחקיקה חדשה ובמסגרת פרשנות לגבי חקיקה קיימת.

ההנחיה מבוססת על שני עקרונות יסוד מרכזיים: **שקילות פונקציונלית** – הכלי הדיגיטלי צריך להגשים את מטרות ההסדר; **אי עדיפות** – אין עדיפות עקרונית להסדר פיסי על פני הסדר דיגיטלי, שכן ככלל, אמצעים דיגיטליים אינם נחותים או מסוכנים יותר מאמצעים הקיימים בעולם הפיסי.

---

[1] ראו, למשל, החלטת ממשלה מספר 1046 מיום 15.12.2013 והחלטת ממשלה מספר 2097 מיום 10.10.2014 בעניין הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי "ישראל דיגיטלית". בהמשך להחלטות אלו הובאה החלטה מספר 1008 של הממשלה מיום 17.1.2016, https://www.gov.il/he/departments/policies/2016_dec1008.

על משרד ממשלתי ליישם את הכללים המנחים, המפורטים בהנחיה זו, על בסיס תפישת עולם של ניהול סיכונים. משמעותה של תפישה זו היא כי אין הכרח לבחור בהסדר שמצמצם את סיכוניו לרמה הנמוכה ביותר. ניסיון לצמצם את הסיכונים לרמה הנמוכה ביותר עלול להביא ליצירת הסדר נוקשה, אשר יסכל דה פקטו את ישימותו או יפגע בתועלת הצפויה לנבוע ממנו או בנוחות הגורמים המעורבים בו. זאת ועוד, בעת עיצוב הסדר דיגיטלי, יש לשאוף ליצירת הסדר פשוט, ישים ונגיש לאוכלוסייה שלה הוא נועד.

יובהר, כי הנחיה זו נועדה לפתוח צוהר לעולם של יצירת הסדרים דיגיטליים **בדגש על ההיבט המשפטי**, וככזו, היא אינה מקיפה את כלל ההיבטים שנוגעים להסדרים דיגיטליים. כמו כן, היא אינה מקיפה את כל ההיבטים המשפטיים שנוגעים להסדרים דיגיטליים, אלא מתמקדת כאמור בהיבטים משפטיים הנובעים מההיבטים הדיגיטליים של ההסדרים. על כן, מטבע הדברים, ככל הסדר, הסדר בעל היבטים דיגיטליים עשוי לחייב בחינה משפטית של היבטים נוספים שהנחיה זו אינה עוסקת בהם.

מסמך זה הוא מסמך עזר ממספר 3 של ההנחיה, והוא למעשה מהווה גרסה מפורטת של ההנחיה ושל מסמכי העזר האחרים שלה. מסמך זה חוזר בהרחבה על כל האמור בהנחיה ובמסמכי העזר האחרים שלה ומוסיף דוגמאות רבות להמחשת הדברים.

בדומה למבנה של ההנחיה ושל מסמכי העזר האחרים שלה, מסמך זה בנוי באופן הבא: **בחלק א'** מפורטים עקרונות היסוד והכללים המנחים לגיבוש הסדרים דיגיטליים (פרקים א' ו-ב'); הנחיה לעניין יישום הסדר דיגיטלי בחקיקה (פרק ג'); והוראות בקשר למושגי יסוד בעולם הדיגיטלי כמו, למשל, כתב ומסמך מקורי (פרק ד'). **בחלק ב'** מתואר הליך בחינה מומלץ לגיבוש הסדר דיגיטלי, שבמסגרתו מוסבר כיצד ליישם את ההוראות המנחות המפורטות בחלק א', שלב אחרי שלב. לאחר מכן, מובאת הרחבה לעניין מסמכי העזר של ההנחיה: <u>במסמך עזר מספר 1</u> מובא תרשים גרפי שממחיש את הליך הבחינה המומלץ לגיבוש הסדר דיגיטלי. לנוחות הקריאה, מובא תרשים זה גם בסיפא סעיף זה. <u>במסמך עזר מספר 2</u> מובאים הסברים שימושיים בעניין המעבר מהעולם הפיסי לעולם הדיגיטלי, שעניינם שירותים דיגיטליים, שמקנים אמון בפעולות שונות, כדוגמת חתימה אלקטרונית.

הליך בחינה מומלץ להסדר דיגיטלי

1

זיהוי המטרה הכללית
שיפור השירות? הגברת היעילות?

2

זיהוי תכליות ההסדר
הזדהות? הסכמה לגבי פעולה? תיעוד זמן? הרתעה? שמירה על מהימנות של מידע?

3

זיהוי הגורמים הנוגעים להסדר
מיהם בעלי העניין? הציבור? גורמי מקצוע? גופים ציבוריים? עמותות?

4

בחינת סיכוני ההסדר
אילו סיכונים עלולים להתממש במקרה של אי קיום התכליות ברמה מספקת? מהי עוצמת הפגיעה במקרה של התממשות הסיכון ורמת ההסתברות להתממשותו? מהי מידת יכולתו של כל גורם לשאת בסיכונים? כיצד כל גורם יכול להקטין אותם?

5

ביצוע ניהול סיכונים
יש להתאים את הסיכונים לערך הנפגע ולעוצמת הפגיעה, ולשאוף להקטינם בכלים טכנולוגיים או על ידי קביעת כללים נורמטיביים.

6

בחינת נטלים
מהם הנטלים המוטלים על כל גורם המעורב בהסדר? על ההסדר להיות הוגן וישים, ולהתאים לאוכלוסייה שעליה הוא נועד לחול.

7

בחירה בין הכלים להגשמת כל תכלית
יש ליצור הלימה בין מרכיבי ההסדר והכלים שבשימוש בו לבין רמת הוודאות שבה יש להגשים כל תכלית.

8

בחינת התאמת ההסדר לדין
האם הדין הקיים מאפשר את קיומו של ההסדר הדיגיטלי? האם ניתן להפעיל כללי פרשנות גמישים? האם נדרש תיקון הדין?

2. תחולת ההנחיה:

ההנחיה חלה על משרד ממשלתי, יחידת סמך או יחידה אחרת של המדינה (לעיל ולהלן: "משרד ממשלתי"). היא נועדה להנחות יועץ משפטי של משרד ממשלתי במתן ייעוץ משפטי, ככל שהוא נדרש לכך, בהיבטים משפטיים של הסדרים דיגיטליים. יובהר, כי בחינה משפטית של ההסדרים הדיגיטליים אינה שונה מבחינה משפטית "רגילה" שעל כל יועץ משפטי לעשות ביחס לגיבוש מוצר או שירות שמשרדו מבקש לתת, ומשכך אין לחשוש לבחון הסדרים דיגיטליים בבחינה משפטית מקובלת.

להלן יובאו דוגמאות למקרים שבהם יש לקיים בחינה משפטית לפי הנחיה זו:

- **הסדר דיגיטלי בעל השלכות משפטיות**. ככלל, הסדר דיגיטלי, שבמסגרתו ניתנת האפשרות לקיים חובה או לממש זכות, הוא בעל השלכות משפטיות. כך, למשל, במקרה שבו חלה חובה חוקית על אזרח להגיש מסמך לרשות, יש לענות על השאלה מהן ההשלכות של אי קיום חובה כאמור. ככל שלאי קיום החובה השלכות גדולות יותר על האזרח, כך יש להקנות לו – במסגרת ההסדר הדיגיטלי המתגבש - ודאות גדולה יותר, ולהבטיח שהוא יוכל לקיים הלכה למעשה את חובתו החוקית. כמו כן, במקרה שבו לאזרח קיימת זכות על פי חוק, ועל הרשות חלה החובה לספק את אותה הזכות, יש לבחון כיצד ניתן להבטיח שהאזרח יוכל לממש את הזכות באמצעות ההסדר הדיגיטלי, כך שההסדר לא יגביל את זכותו.
- **קיומם של אילוצים משפטיים, שמשפיעים על גיבושו של הסדר דיגיטלי**. כך, למשל, יש לבחון האם קיימות דרישות בחקיקה לגבי נושא ההסדר, צורניות או מהותיות, כדוגמת חתימה. במסגרת זו, יש לבחון האם ניתן לאפשר במסגרתן את ההסדר הדיגיטלי המתוכנן בדרך של פרשנות, או שמא יש צורך בחקיקה חדשה או בתיקון של חקיקה קיימת.
- **שקילת ליווי ההסדר המתגבש בכללים משפטיים**. כך, למשל, היבטים ראייתיים הנוגעים לעניין כמו חזקות מסירה והסדרי האחריות, שאמורים לחול על המשתתפים בהסדר הדיגיטלי.
- **היבטי אסדרה**. כשמשרדי הממשלה או יחידות בממשלה מבצעות אסדרה, עשויה לעלות השאלה מהו ההסדר הדיגיטלי הראוי במסגרת מערכת היחסים בין המאסדר למפוקחים ובין המפוקחים לציבור.
- **חקיקה**. ככל שההסדר הדיגיטלי נוגע לחקיקה, על היועץ המשפטי לתת דעתו למדרג הנורמטיבי שבו יש לעגן את הוראות ההסדר: חקיקה ראשית, חקיקת משנה או נהלים של הרשות.
- **מידתיות ההסדר וסבירותו**. כשההסדר הדיגיטלי מטיל **נטלים** על הגורמים המושפעים ממנו או עלול לפגוע **בערכים מוגנים**, על היועץ המשפטי לבחון האם הטלת הנטלים והפגיעה האפשרית בערכים עומדות במבחני הסבירות והמידתיות.

<u>חלק א' – הוראות מנחות</u>

<u>פרק א'– עקרונות יסוד בגיבוש הסדר דיגיטלי</u>

התפתחותו המהירה של העולם הדיגיטלי בעידן המודרני הביאה לכך שנעשה שימוש בשירותים דיגיטליים במקומם או בנוסף לשירותים שהיו מקובלים בעבר. התפתחות זו הביאה לגיבוש מספר עקרונות יסוד בתחום, אשר יתוארו בפרק זה, והם: שקילות פונקציונלית, אי עדיפות וניטרליות טכנולוגית. הסדר דיגיטלי יגובש לאורם של עקרונות מנחים אלה.

1. <u>שקילות פונקציונלית</u>:

<u>1.1 מהי שקילות פונקציונלית</u>

אגב המעבר ממסמכים בנייר למסמכים דיגיטליים נבחנו המאפיינים שמסמך דיגיטלי צריך לקיים כדי שייחשב כשקול למסמך בנייר. בחינה זו הביאה לגיבוש הגישה בדבר השקילות הפונקציונלית[2], אשר נהוג להחילה על כל סוגי השירותים והמוצרים הדיגיטליים. לפי גישה זו, מתבצע ניתוח המטרות והשימושים של הדרישה המסורתית בעולם הפיסי (למשל, דרישות של מסמך בנייר), מתוך ניסיון לקבוע כיצד ניתן להשיג מטרות ושימושים אלה בסביבה אלקטרונית.

כך, למשל, אם חיקוק מסוים דורש כי מסמך ייערך בכתב, אזי נדרש, לצורך קביעתו בהסדר דיגיטלי, לשאול מדוע נקבעה הדרישה הזו. ברוב המקרים דרישת הכתב נועדה להבטיח כי ניתן יהיה לשמור את המסמך ולאחזר אותו. לפי השקילות הפונקציונלית, יש להגשים מאפיינים אלה גם בעולם הדיגיטלי.

<u>1.2 בעולם הדיגיטלי ניתן לתת מענה מדויק למטרות, שלא חודדו בעולם הפיסי</u>

גישת השקילות הפונקציונלית מבוססת על ההנחה כי אותם מטרות ושימושים של דרישה בעולם הפיסי צריכים להתקיים גם בעולם הדיגיטלי. **אלא שבעולם הפיסי, במקרים רבים לא חודדו המטרות והשימושים כל צרכם**. כך, ישנם הסדרים בעולם הפיסי שמרכיביהם מגשימים יותר תכליות מהנדרש. לעומת זאת, ישנם הסדרים אחרים בעולם הפיסי שמאפייניהם לא מקיימים ברמה מספקת את כלל תכליות ההסדר בגלל מגבלותיו של העולם הפיסי.

---

[2] גישה זו אומצה במסמך בינלאומי משמעותי בתחום - החוק לדוגמה של האו"ם בעניין מסחר אלקטרוני: Uncitral Model Law On Electronic Commerce (ראו בעמוד 20) (להלן: **"חוק המודל של האו"ם בעניין מסחר אלקטרוני"**).

הסבר על הגישה בעמוד 18 ל http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf :

the "functional equivalent approach" is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.

בהמשך, אומצה הגישה גם בישראל בדו"ח ביניים של הוועדה לבדיקת בעיות משפטיות הכרוכות מסחר אלקטרוני משנת 2004 (ועדה ממשלתית בין משרדית בראשותה של המשנה ליועץ המשפטי לממשלה (משפט אזרחי) דאז טנה שפניץ) (להלן: **"דו"ח מסחר אלקטרוני"**).

שלא כמו בעולם הפיסי, עושרו של העולם הדיגיטלי מאפשר, בחלק מהמקרים, מענה מדויק והולם יותר לאותם המטרות והשימושים. מתן מענה כאמור עשוי להגביר את יעילות ההסדר הדיגיטלי, את ישימותו ואת נוחות השימוש בו.

כך, לדוגמה, חתימה על גבי נייר, שמטרתה המרכזית היא זיהוי החותם, יכולה להיות מוחלפת בעולם הדיגיטלי בשירות של זיהוי דיגיטלי, תוך ויתור על דרישת החתימה.

דוגמה נוספת לדיוק המענה, המתאפשר בעולם הדיגיטלי, היא השירות של "חותמת זמן" דיגיטלית. חותמת זמן עשויה לתת מענה לתכלית הֶעָדָה על זמן ביצוע פעולה, מבלי שמבצע הפעולה יצטרך להיעזר באמצעי תיעוד נוספים, כפי שנהוג היה בעולם הפיסי. כך, למשל, ציון תאריך על מסמך, שאדם מעוניין לשלוח בדואר לרשות מנהלית, על מנת להעיד על זמן כתיבתו ושליחתו, מספק רמה נמוכה של ודאות באשר לזמן כתיבתו. זאת, מאחר שכותב המסמך יכול לציין על המסמך תאריך של יום אחר מיום השליחה. על מנת להביא לרמת ודאות גבוהה יותר באשר למועד כתיבת המסמך, נדרש בעולם הפיסי דבר מה נוסף כמו, למשל, הגעה פיסית אל פקיד הדואר, שמתעד את תאריך הגשת המסמך, במסגרת שירותי הדואר הרשום. לעומת זאת, שימוש ב"חותמת זמן" בעולם הדיגיטלי יכול לספק רמה גבוהה של ודאות באשר לזמן כתיבת המסמך, מבלי להיזקק לגורמים נוספים שיאמתו את הזמן. לדוגמה, צוואה בעדים לפי חוק הירושה, התשכ"ה - 1965 צריכה להיחתם בפני שני עדים ויש לציין עליה את תאריך החתימה. ציון התאריך על גבי הצוואה בעולם הפיסי מספק מידה לא רבה של ודאות לעניין זמן חתימת הצוואה (יצוין, כי הימצאותם של עדים במעמד החתימה מגבירה את הוודאות של זמן ביצוע הצוואה). לעומת זאת, חתימה דיגיטלית במעמד דומה בפני עדים, שאליה מוצמדת "חותמת זמן"[3] דיגיטלית ברמה גבוהה, עשויה לספק רמה גבוהה יותר של ודאות לעניין זמן חתימת הצוואה. לכך יש חשיבות רבה בעולם הצוואות, שבו כשקיימות מספר צוואות, הצוואה המאוחרת בזמן גוברת על קודמותיה.

1.3 אופן הפעלת עקרון השקילות הפונקציונלית

מאחר שכאמור, מטרות הסדרים בעולם הפיסי לא חודדו כל צרכם, בעת הפעלת עקרון השקילות על הסדר מתגבש, יש לבדוק מהם התכליות והשימושים שההסדר נועד להגשים **ולא את אופן יישומם בעולם הפיסי**. כך, למשל, אם בהסדר הפיסי נקבע כי לשם צריכת שירות מסוים נדרשת חתימה על מסמך, אזי יש לשאול כיצד יש להגשים את **מטרת** דרישת החתימה ולא כיצד יש לחתום בעולם הדיגיטלי.

[3] חותמת זמן מצורפת לחתימות אלקטרוניות מסוגים מסוימים. רמת אמינותה של חותמת הזמן תלויה במספר גורמים, ובהם גם תוכנת החתימה שנעשה בה שימוש.

יהיו מקרים שבהם בחינת התכליות תוביל למסקנה כי חלק מהדרישות שהיו קיימות בעולם הפיסי אינן מתאימות לעולם הדיגיטלי. במקרים אלה, לשם הגשמת תכליות ההסדר הדיגיטלי **ניתן לוותר על מימוש חלק מתכונות ההסדר הפיסי**. כך, ההסדר הדיגיטלי עשוי להיות פשוט יותר וקל יותר ליישום. באותו אופן, במקרים שבהם ישנן תכליות שלא היו ניתנות להגשמה בעולם הפיסי או שניתנות להגשמה בו באופן חלקי, יש לבחון **האם ניתן להגשימן בעולם הדיגיטלי**.

יצוין, כי במקרים רבים, אמצעים דיגיטליים יכולים להגשים את המטרות והשימושים ברמת ודאות גבוהה יותר מאמצעים בעולם הפיסי. עם זאת, **אין משמעות גישת השקילות הפונקציונלית כי יש להחמיר את הדרישות בנוגע לשירותים שונים**[4].

☜ **גיבוש הסדר דיגיטלי, יתבצע בהתאם לגישת השקילות הפונקציונלית. לפי גישה זו, ייבחנו המטרות והשימושים של ההסדר ולא הכלים שבאמצעותם הם מושגים בעולם הפיסי.** ☜ **בעת השוואת המטרות והשימושים של העולם הפיסי והעולם הדיגיטלי, תיבחן השאלה, האם המטרות והשימושים בעולם הפיסי חודדו באופן מלא. ככל שאופן היישום בעולם הפיסי מגשים יותר תכליות מהנדרש, אין צורך לקיים תכליות נוספות אלה גם בהסדר הדיגיטלי.**

<u>2. אי עדיפות</u>

עקרון יסוד נוסף בתחום הוא עקרון אי העדיפות, שלפיו לא יישלל תוקפו המשפטי של מסמך אלקטרוני או קבילותו של אותו המסמך רק בשל כך שהוא נוצר או הועבר באופן אלקטרוני[5]. בדומה לכך, לא יישלל גם תוקפה של חתימה או של כל שירות אחר או קבילותם רק בשל כך שהם נערכו באופן אלקטרוני.

לצד זאת, יובהר כי התוקף המשפטי של מסמך, חתימה או רכיב אחר, שנערכו בדרך אלקטרונית, יכול להישלל מסיבות אחרות, שמקורן בקביעות בדין או במגבלה אחרת. כך, למשל, חוזה שנחתם באופן אלקטרוני, אשר יוגש כראיה לבית המשפט, יהיה קביל כראיה, אלא אם כן הוסכם אחרת בידי הצדדים או אם ישנן דרישות ראייתיות מסוימות ששוללות את קבילותו. דוגמה נוספת לכך היא אפשרותו של גוף מאסדר לקבוע, כי מסמך מסוים יוגש אליו בדרך אלקטרונית, המחייבת עמידה בדרישות סף מסוימות או כי מסמך לא יוכל להיות מוגש באופן אלקטרוני כלל.

☜**גיבוש הסדר דיגיטלי יתבצע, ככלל, לאורו של עקרון אי העדיפות.**

[4] הבהרה ברוח דומה נכתבה בחוק המודל של האו"ם בעניין מסחר אלקטרוני בקשר לשקילות הפונקציונלית (ראו סוף פסקה 16 במדריך של חוק המודל).

[5] עקרון זה מעוגן בחוק המודל של האו"ם בעניין מסחר אלקטרוני וכן בסעיף 46 לתקנות REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) (להלן: "תקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון").

3. ניטרליות טכנולוגית

בדומה לעקרון אי העדיפות שתואר בסעיף הקודם, יש לשאוף כי ההסדר הדיגיטלי המתגבש יהיה ניטרלי מבחינה טכנולוגית ככל הניתן[6]. כלומר, כי ההסדר לא יעדיף אמצעי טכנולוגי אחד על פני אמצעי טכנולוגי אחר, אם שניהם מגשימים את השימושים והמטרות של אותו ההסדר. יובהר, כי אין באמור כדי לשלול אפשרות להתייחס לטכנולוגיה מסוימת בגוף ההסדר ואף להקנות לה העדפה כשיש הצדקה לכך, ואולם הסדר ניטרלי טכנולוגית צפוי להישאר עדכני לאורך זמן ולעודד את התפתחות השוק הטכנולוגי. לניטרליות טכנולוגית חשיבות רבה, במיוחד נוכח שינויי הטכנולוגיה התכופים והקושי של המשפט להדביק את קצב שינוי הטכנולוגיה.

☜**גיבוש הסדר דיגיטלי יתבצע, ככלל, לאורו של עקרון הניטרליות הטכנולוגית.**

*להסבר אודות יישום עקרון הניטרליות הטכנולוגית בחקיקה ראו בסעיף 2.3 "אי עיגון דרישות טכנולוגיות בחיקוק" בפרק ג' לחלק א'.

[6] עקרון הניטרליות הטכנולוגית אומץ במסמך בינלאומי משמעותי בתחום – חוק המודל של האו"ם בעניין מסחר אלקטרוני.

פרק ב' – כללים מנחים לגיבוש הסדר דיגיטלי

הסדר דיגיטלי יגובש על פי הכללים המנחים הבאים.

1. התאמת ההסדר לתכליותיו

כלל התאמת ההסדר לתכליותיו הוא כלל המפתח בגיבוש הסדר דיגיטלי, והוא מבוסס על עקרון השקילות הפונקציונלית. לפי כלל התאמת ההסדר לתכליותיו, **על מרכיבי ההסדר הדיגיטלי להתאים לתכליותיו של ההסדר ולקיים אותן ברמת ודאות מספקת ביחס למאפייני ההסדר**. רמת הוודאות שבה כל תכלית צריכה להיות מקוימת תיקבע, בין היתר, לפי סיכוני ההסדר והפגיעה האפשרית במקרה של התממשות הסיכונים, כפי שיפורט בסעיף הבא. ככלל, קיים מתאם חיובי בין הסיכון לבין התכלית, כך שככל שהסיכון גדול יותר, כך יש להגשים את התכלית ברמת ודאות גבוהה יותר.

כך, למשל, הסדר שעוסק במרשם דיגיטלי שנחתם על ידי רופא, צריך להגשים, בין היתר, את התכליות הבאות: הבטחה כי הרופא ששמו כתוב על גבי המרשם הוא אכן מי שחתם עליו (זיהויו) וכי הוא היה מוסמך לחתום על המרשם מתוקף תפקידו כרופא, הבטחה כי המרשם לא שונה לאחר החתימה עליו, והבטחה כי לא ייעשה שימוש במרשם יותר מפעם אחת. אי הגשמת תכליות אלו עלולה לפגוע בבריאות הציבור במקרה של זיוף מרשם, נטילת מינון גבוה יותר של תרופות או סחר בתרופות במקרה של שימוש חוזר באותו המרשם. כמו כן, אי הגשמת התכליות עלולה אף לגרום לנזק כלכלי לקופת החולים, ככל שהיא מסבסדת את עלות התרופה אשר נרכשה שלא כדין. בנסיבות אלו, שבהן עלולה להיפגע בריאות הציבור, נראה שהתכליות האמורות צריכות להתקיים ברמת ודאות גבוהה[7].

☜**על מרכיבי ההסדר הדיגיטלי להתאים לתכליותיהם ולקיים אותן ברמת ודאות מספקת ביחס למאפייניהם.**

[7] ראו ההסדר שנקבע לעניין מרשמים אלקטרוניים בתקנות הרופאים (מתן מרשם), תשמ"א-1981 (תקנה 2א) ונוהל משרד הבריאות בנושא בקישור הבא: https://www.health.gov.il/hozer/DR_107.pdf.

2. יעילות, פשטות וישימות ההסדר

רצוי שהסדר דיגיטלי **יהיה פשוט, יעיל וישים ככל הניתן.** אחרת, ההסדר עלול להיות בלתי סביר. כך, למשל, כשהפגיעה בישימות מכבידה באופן ממשי על האפשרות לממש זכות או לקיים חובה במסגרת ההסדר. כמו כן, הסדר שאינו יעיל או ישים עלול לפגוע בוודאות המשפטית וביכולת לעשות שימוש בכלים משפטיים שונים.[8]

יצוין, כי לעיתים ישנה התנגשות בין השיקול של צמצום הסיכונים לבין השיקול של יצירת הסדר ישים, נוח ויעיל. הסדר דיגיטלי צריך להתגבש על פי תפיסת העולם של ניהול סיכונים, בהתאם לכללים שיפורטו בהמשך. משמעותה של תפישה זו היא כי אין הכרח לבחור בהסדר שמצמצם את סיכוניו לרמה הנמוכה ביותר. ניסיון לצמצם את הסיכונים לרמה הנמוכה ביותר עלול להביא ליצירת הסדר נוקשה, אשר יסכל את ישימותו הלכה למעשה או יפגע בנוחות הגורמים המעורבים בו.[9]

☜**רצוי שהסדר דיגיטלי יהיה פשוט, יעל וישים ככל הניתן.**

3. הערכת סיכונים והתאמת החשיפה להם לערך הנפגע ולעוצמתו

הסדרים דיגיטליים, בדומה להסדרים בעולם הפיסי, טומנים בחובם סיכונים שונים. חלק מהסיכונים בעולם הדיגיטלי שונים במהותם מאלה של העולם הפיסי. זאת, בשל מאפייניו הייחודיים של העולם הדיגיטלי, ובהם הקלות של העברת מידע למספר רב של אנשים בפרקי זמן קצרים, ומבלי שיתקיים מפגש פיסי ביניהם. כך, למשל, במקרה של העברת מסמך הכולל מידע אישי, הפצה לא מורשית שלו עלולה לפגוע בפרטיות האדם שהמידע האישי אודותיו. כמו כן, מאחר שהפצת מידע הפכה להיות פשוטה וקלה יותר בעידן הדיגיטלי, שיעור הנזק שעלול להיגרם מהפצה לא מורשית של המידע גדול לאין ערוך מזה של העולם הפיסי.

---

[8] כך, למשל, הסדר שכולל העברת מסמך מהרשות לאזרח באופן שאינו יעיל או ישים, לא יאפשר לקבוע חזקת מסירה. זאת, מפני שתנאי לקביעת חזקת מסירה הוא הגעת המסר ליעדו ברמת ודאות גבוהה.

[9] כך, למשל, ניתן להניח כי הסדר דיגיטלי, שיחייב את כלל הציבור לרכוש כרטיסים חכמים לצורך ביצוע פעולה חד פעמית, לא ייצא לפועל מסיבות מעשיות. זאת, מפני שבמקרה כזה לא נראה שיהיה תמריץ ממשי לציבור לרכוש כרטיסים חכמים, וכן מאחר שחלק ממנו גם לא יוכל לרכוש אותם או לעשות בהם שימוש (לדוגמה, מסיבות כלכליות, בשל העדר ידע טכנולוגי או מסיבות תרבותיות).

גיבוש הסדר דיגיטלי יתבצע על פי **תפיסת העולם של ניהול סיכונים**. יובהר, כי הנחיה זו עוסקת בניהול סיכונים בהיבט המשפטי ולא בהיבט המקצועי של מדיניות ניהולית,[10] אף שתיתכן חפיפה בין הסיכונים של שני היבטים אלה.[11] ישנם שני סוגים נפוצים של סיכונים **משפטיים**. הסיכון האחד הוא סיכון לפגיעה בערך מוגן. הסיכון השני הוא סיכון ראייתי, אשר בדרך כלל נגרם עקב פגיעה במהימנות מרכיב ממרכיבי ההסדר.

במסגרת ניהול הסיכונים יש לזהות תחילה, בנוגע לכל אחד ממרכיבי ההסדר הדיגיטלי (חתימה, כתב, אופן הגשה, וכד'), את סיכוניו. כך, למשל, שימוש בחתימה אלקטרונית מסוג "חלש" עלול להקל על זיוף חתימה או התכחשות לחתימה; שימוש בהזדהות דיגיטלית ברמה נמוכה עלול להביא לטעות בזיהוי. הערכת הסיכונים תתייחס לסיכונים שעלולים להתממש בנוגע **לכל אחד מהגורמים שעשוי לשאת בסיכון**: הציבור, הגורמים שמעורבים בהסדר במישרין, המשרד הממשלתי שמגבש את ההסדר וכל גורם אחר הנוגע לעניין.

לאחר זיהוי הסיכונים, תיבחנה, בנוגע לכל סיכון, ההשלכות של התממשותו- הן מבחינת הערך שעלול להיפגע והן מבחינת עוצמת הפגיעה. התממשות הסיכונים השונים עלולה לפגוע בערכים מוגנים שונים כמו למשל: זכויות יסוד כדוגמת הגנת הפרטיות, הגנה על קניין, כבוד, זכות לחיים; זכויות כלכליות או כספיות; אינטרסים ציבוריים כדוגמת ביטחון המדינה.

ככלל, ככל שהפגיעה שעלולה להיגרם בשל התממשות סיכון הינה חמורה יותר, מבחינת חשיבות הערך המוגן ועוצמת הפגיעה בו, ושההסתברות להתממשותו גדולה יותר, כך על ההסדר הנבחר להבטיח כי החשיפה לסיכון תהיה קטנה יותר. בהתאם לכך, יש להפעיל את מבחני המידתיות (כשמדובר בזכויות חוקתיות) והסבירות. במסגרת מבחנים אלה, יש לקחת בחשבון, בין היתר, את עלויות הקטנת הסיכון ואת הנטלים שהיא עלולה להטיל.

כך, למשל, הסדר שעניינו בגבייה דיגיטלית של הודעות במשטרה, עלול – אם הכלי הטכנולוגי הנבחר אינו מהימן דיו – לאפשר זיופים, להקל על התכחשות להודעות, וכד'. התממשות סיכון זה עלולה לפגוע בערכים מוגנים משמעותיים כמו חופש התנועה או ביטחון הציבור. במקרה כזה, יש לתת משקל לפגיעה אפשרית זו ובהתאם לעצב הסדר שיצמצם – ככל הניתן – את הסיכון של התכחשות להודעה או זיופה.

יצוין, כי יהיו מקרים שבהם, לאחר ביצוע הבחינה באשר להשלכות התממשותו של כל סיכון כאמור לעיל והיכולת להקטין את סיכוניו כמפורט בסעיף הבא, יתברר שישנם סיכונים, שנטילתם במסגרת ההסדר, תחרוג ממתחם הסבירות או תהיה לא מידתית.

---

[10] גם החלטות מדיניות מתקבלות על בסיס תפיסה של ניהול סיכונים. להסבר והרחבה על ניהול סיכונים **מקצועי** ניתן לעיין במדריך הממשלתי לניהול סיכונים ברגולציה ובמדיניות ציבורית מיוני 2018 (האגף לממשל וחברה, משרד ראש הממשלה, עורך: גיא מור), הזמין בקישור הבא: http://bit.ly/RegRiskManage .

[11] סיכון מקצועי עלול לגרום לסיכון משפטי, אך לא כל סיכון מקצועי עולה בהכרח כדי סיכון משפטי. לדוגמה, סיכון של טעות במערכת שירות ממוחשבת או סיכון של יצירה של מערכת ממוחשבת שאינה נוחה למשתמש ומכבידה עליו הם סיכונים מקצועיים, שיהוו גם סיכון משפטי אם יביאו, למשל, לפגיעה במימוש זכות.

☜**ככלל, ככל שהפגיעה שעלולה להיגרם בשל התממשות סיכון מסיכוני ההסדר הדיגיטלי הינה חמורה יותר, מבחינת חשיבות הערך המוגן ועוצמת הפגיעה בו, ושההסתברות להתממשותו גדולה יותר, כך על ההסדר הנבחר להבטיח כי החשיפה לסיכון תהיה קטנה יותר.**

4. הקטנת סיכוני ההסדר וחלוקת הנשיאה בהם במקרה של התממשותם:

בסעיף זה יתוארו דרכים אפשריות להקטנת סיכוני ההסדר ויוסבר כיצד ניתן לקבוע כללים נורמטיביים בנוגע לחלוקת סיכוני ההסדר ואילו שיקולים יש לשקול בקביעת חלוקת הנשיאה בסיכונים.

4.1 שני אופנים להקטנת סיכוני ההסדר – שימוש בטכנולוגיות וקביעת כללים נורמטיביים

במסגרת ביצוע ניהול סיכונים, נבחנים אופני הטיפול בסיכונים, ובהם האפשרויות להקטין את חומרת הסיכונים ואת ההסתברות להתרחשותם.

טיפול בסיכוני ההסדר יכול להתבצע בשני אופנים מרכזיים. **האחד** הוא קביעה כי בהסדר ייעשה שימוש באמצעים שונים, שיגבירו את מהימנותו, **ויצמצמו את סיכוניו**. זאת, למשל, באמצעות **שימוש בטכנולוגיה מתקדמת** או קביעת **נהלים מסודרים**, שיביאו להגשמת תכליות ההסדר ברמת ודאות גבוהה.

השני הוא קביעת **כללים נורמטיביים**, שיביאו להקטנת הסיכונים או להסטתם ולהטלתם על מי שראוי להטיל עליו אותם. הדוגמה הבולטת לכללים כאלה היא מנגנון של **חלוקת הנשיאה בסיכוני ההסדר** במקרה של התממשותם. חלוקה זו עשויה להקטין את עוצמת הפגיעה או להסיט את הסיכון ולהטילו על מי שראוי יותר שיישא בו. החלוקה תיקבע בהתאם לשיקולים שיפורטו בסעיף 4.3.

יובהר, כי בדרך כלל, קביעת כללים נורמטיביים לא מתאימה להסדרים שכוללים סיכונים הקשורים **לעולם הפלילי** (בדרך כלל מדובר בסיכונים הקשורים לזכויות יסוד כמו, למשל, שמירה על בטחון הציבור או על זכויות חשודים). זאת, מפני שבהסדרים אלה יש צורך ביצירת ודאות גבוהה לכך שתכליות ההסדר תוגשמנה. על כן, בהסדרים שאופיים פלילי, הקטנת הסיכונים על ידי חיוב לעשות שימוש בכלים טכנולוגיים ולקבוע נהלי עבודה מתאימים הם דרך המלך לטיפול בסיכונים. בדומה לכך, כללים נורמטיביים לרוב לא מתאימים להסדרים שעלולים לעורר סיכונים, שהתממשותם תביא לפגיעה באינטרסים ציבוריים בעלי משקל של ממש.

4.2 השפעה על הסיכונים באמצעות קביעת כללים נורמטיביים

קביעת כללים נורמטיביים יכולה להשפיע על הסיכונים בשתי דרכים מרכזיות. **דרך ההשפעה הראשונה** היא על ידי תמרוץ הגורם, שהינו **בעל היכולת הטובה יותר לצמצם את הסיכונים,** לצמצם אותם.[12] **דרך ההשפעה השנייה** היא על ידי הטלת הסיכון על **בעל היכולת הטובה ביותר לשאת בסיכון ולפזר אותו.**[13] להלן יובא הסבר על דרכי השפעה אלה.

על כן, ככלל, בעת קביעת כללים נורמטיביים בעניין סיכוני ההסדר, יש להעדיף את הטלת סיכוניו על הגורם שהינו בעל יכולת טובה יותר לצמצמם או לשאת בהם.

4.2.1 הדרך הראשונה – כללים שיתמרצו את בעל היכולת הטובה יותר לצמצמם את הסיכונים

השפעה על סיכוני ההסדר וצמצומם על ידי תמרוץ בעל היכולת הטובה יותר לצמצם את הסיכונים, לפעול על מנת לצמצמם, יכולה להתבצע במגוון דרכים, ובהן -

- **נהלים ותהליכים**- ניתן להקטין סיכונים באמצעות קביעת נהלים או תהליכים הקשורים להסדר. בדרך כלל גופים גדולים הם בעלי יכולת לקבוע נהלים או לעמוד בהם, וכך באפשרותם לצמצם את הסיכונים או לשאת בהם. על כן, הטלת הסיכונים עליהם עשויה להיות עדיפה, שכן כך הם יתומרצו לקבוע נהלים שיצמצמו את סיכוני ההסדר. כך, למשל, גופים גדולים יכולים להקטין את הסיכונים לזיוף ולשימוש לרעה בכלי דיגיטלי על ידי שליטה על תהליכים: קביעת נהלים, חובות שמירה, מערכות בקרה ומבנה ארגוני מסודר. למשל, עירייה מבוססת שמקבלת מסמך בנייר מתושב וסורקת אותו למחשב, יכולה לבצע סדרה של פעולות לפי נוהל שנקבע מראש. מטרת פעולות אלה היא להגדיל את הסיכוי לכך שהקליטה, השמירה והשימוש החוזר במסמך הסרוק יהיו מהימנים ככל הניתן.

- **טכנולוגיה**- ניתן לצמצם סיכונים על ידי שימוש בטכנולוגיות מתקדמות. כך, גורם בעל יכולת טובה יותר מבחינה טכנולוגית או גורם בעל יכולת כלכלית לרכוש שירותים טכנולוגיים מתקדמים, יכול להקטין את הסיכון על ידי שימוש בכלים דיגיטליים מתקדמים שונים. על כן, נראה שהטלת הנשיאה בהתממשות הסיכון עליו עשויה להיות יעילה יותר. למשל, במקרה שבו הסדר מצריך שימוש בחתימות, גוף גדול יכול לרכוש אמצעים ל"חתימות מאושרות", שמבטחות מהימנות טובה, הן לזהות החותם והן לשלמות המסר, וללמד את עובדיו כיצד לעשות בהן שימוש.

---

[12] למשל, על ידי שליטה ישירה בגורמי הסיכון; מעורבות בעיצוב ההסדר; שימוש בידע טכנולוגי ובאמצעים כלכליים שעומדים לרשותו.

[13] למשל, על ידי פיזור הסיכון או הנזק שנגרם כתוצאה מהתממשותו על מספר רב של גורמים.

- **שליטה על כלי דיגיטלי**- מקרה נוסף שבו לגורם ישנו כלי מעשי מתאים להקטנת הסיכון הוא כאשר יש לו שליטה על כלי דיגיטלי. למשל, בעל אמצעי זיהוי, אשר מזדהה באמצעות סיסמה שידועה רק לו ובאמצעות הטלפון הנייד שלו, עשוי להיות בעל יכולת טובה לשלוט באמצעי הזיהוי שלו. על כן, הטלת האחריות עליו עשויה להיות יעילה, באשר הוא מונע הנזק הזול. יחד עם זאת, יש לשים לב שלצורך הבטחת שליטה כאמור, על בעל אמצעי הזיהוי להיות מודע לצורך לשמור על אמצעי הזיהוי שלו ולהבין מהו האופן שבו עליו לשמור עליו. לדוגמה, כשמדובר באזרחים שמחזיקים בסיסמה לצורך קבלת גישה לאזור אישי באתר אינטרנט ממשלתי, אמנם הסיסמה מצויה ברשות האזרחים, ובאפשרותם להסתיר אותה מפני אחרים באופן הטוב ביותר, אך לפעמים הם אינם מודעים למשמעות של אי שמירת הסיסמה או ששמירה על הסיסמה אינה בהכרח במוקד תשומת לבם.

4.2.2 הדרך השנייה – כללים שיטילו את הסיכון על בעל היכולת הטובה ביותר לשאת בסיכון ולפזר אותו

צמצום סיכונים יכול להתבצע גם על ידי הטלת הסיכון על הגורם שיכולתו **לספוג את הנזק** היא הטובה ביותר. כך למשל, אם לגורם יש אפשרות לפזר את הנזק על מספר רב של אנשים, אזי הפגיעה בכל אחד מהם תהיה קטנה יותר מאשר פגיעה בגורם אחד. לדוגמה, חברות גדולות, שנותנות שירות למספר רב של לקוחות, או המדינה בנותנה שירותים ממשלתיים, יכולות לספוג נזקים ולשאת בהם על ידי פיזור העלות לכלל הלקוחות או האזרחים בהתאמה, במקום שלקוח או אזרח בודד, בהתאמה, ייאלץ לשאת במלוא הנזק לבדו.

4.3 שיקולים שיש לשקול בקביעת חלוקת הנשיאה בסיכונים

פרט לשיקול היכולת לצמצם את הסיכונים או לשאת בהם כמפורט לעיל, בבחינת אופן חלוקת הנשיאה בסיכוני ההסדר, יש לשקול אף את השיקולים הבאים: פערי הכוחות בין הגורמים הנוגעים להסדר[14]; שיקולי צדק[15], ובין השאר שיקולי צדק חלוקתי;[16] שיקולי הוגנות[17], ובין השאר שקילת הטלת האחריות לסיכון על גורם הקשור להסדר, הצפוי ליהנות ממנו, או על גורם הקשור להסדר; שיקולי יעילות וודאות.

ניתן למצוא ביטוי לשיקולים שפורטו לעיל במגוון של דברי חקיקה[18]. כך, למשל, חוק חתימה אלקטרונית כולל הסדר בסעיף 3א, שבו נקבעה חלוקת סיכונים בקשר למערכות יחסים חוזיות, שמתאפיינות בפערי כוחות. ההסדר חל על מקרים שבהם מתבצעת חתימה אלקטרונית על חוזה, כשסוג החתימה מוכתב לצד החותם על ידי הצד השני לחוזה. במקרה כזה, הסיכון במקרה של התכחשות לחתימה מוטל על הצד שהכתיב כיצד תתבצע החתימה, באופן כזה שעליו הנטל להוכיח כי החוזה נחתם, במקרה של התכחשות לחתימה. לדוגמה, חברת סלולר שמחתימה לקוחות על פד דיגיטלי – במקרה של התכחשות הלקוח לחתימה – חברת הסלולר היא זו שתצטרך להוכיח כי הלקוח אכן חתם.

---

14 שיקולים של פערי כוחות באים לידי ביטוי במגוון הקשרים. כך, למשל, ככל שההסדר הדיגיטלי נוגע ליחסים שבין ספק לצרכן, בדרך כלל, יש לקחת בחשבון את העובדה כי הצרכן הוא הצד החלש בעסקה. עוד ראו, למשל, הסדר חלוקת אחריות בסעיף 5(א) לחוק כרטיסי חיוב התשמ"ו-1986 (החוק צפוי להתבטל בשנת 2020 ולהיות מוחלף בחוק שירותי תשלום, התשע"ט-2019, אשר כולל גם הוא הסדר חלוקת אחריות – ראו סעיף 24 לחוק שירותי תשלום).

15 על שקילת שיקולי צדק בפסיקה ראו למשל: פסק דינו של כב' השופט ברנזון בד"נ 22/73 **בן-שחר נ' מחלב**, כח(2) 89, 93-96 (1974); ע"א 10064/02 **"מגדל" חברה לביטוח נ' אבו חנא**, ס(3) 13 פסקה 40,38 לפסק דינו של כבוד השופט ריבלין (2005).

16 על שקילת שיקולי צדק חלוקתי בפסיקה ראו למשל בג"ץ 244/00 **עמותת שיח חדש, למען השיח הדמוקרטי נ' שר התשתיות הלאומיות**, נו (6) 25, פסקה 39 לפסק דינו של כבוד השופט אור (2005). עוד ראו סעיף 196א לחוק התכנון והבניה, התשכ"ה-1965 לעניין היטל השבחה, שתכליתו מבוססת על שיקולי צדק חלוקתי. ראו גם יצחק זמיר "שיקול הצדק בהחלטות מנהליות" **משפט וממשל** כרך ז 623, 662 (תשס"ד-תשס"ה).

17 על שקילת שיקולי הוגנות, ראו למשל: ע"א 5604/94 **חמד נ' מדינת ישראל**, נח(2) 498 פסקה 16 לפסק דינו של כבוד השופט (כתוארו דאז) ברק (2004), ואת קביעת ביהמ"ש בקשר למושג הסבירות: "האדם הסביר אינו רק האדם היעיל. זהו גם האדם הצודק, ההוגן והמוסרי". עוד ראו עח"א 79/1 **מפעלים לניקוי יבש קשת בע"מ נ' היועץ המשפטי לממשלה**, פ"ד לד(3) 365, 374 (1980); ע"א 294/91 **חברת קדישא גחש"א "קהילת ירושלים" נ' קסטנבאום**, פ"ד מו(2) 464, 527 (1992).

18 ראו, למשל, סעיף 6 לחוק השליחות, התשכ"ה-1965, שלפיו חריגה מהרשאה איננה מחייבת את השולח, אלא אם הצד השלישי ידע או היה עליו לדעת על החריגה מההרשאה (ראו סעיף 18 לחוק זה). השולח רשאי לאמץ את פעולת השלוח, אולם בהיעדר אימוץ כאמור, הרי שהסיכון של היעדר הרשאה מוטל על השולח, אשר בהתנהגותו יצר חזות של הרשאה, ובלבד שכאמור הצד השלישי לא ידע ולא צריך היה לדעת, כי מה שנחזה כהרשאה אינו כזה בפועל. להרחבה ראו ע"א 636/89 **כחולי ואח' נ' בנק ברקליס-דיסקונט ואח'** [3], בעמוד 286 (1991). עוד ראו, למשל, חלוקת הסיכונים שנקבעה בהצ"ח דיני ממונות, התשע"א-2011 (להלן – הקודקס), בסעיפים 21-20, שעניינם ביטול פעולה משפטית של קטין בלי שניתנה הסכמתו לה. ניתן למצוא דוגמה נוספת לחלוקת סיכונים מתוך הקודקס בסעיף 81(ג), שעוסק בביטול חבות במקרה של ריבוי חייבים בשל פגם בכשרות או בייצוג של אחד מהחייבים.

הטעם להסדר זה מבוסס על כך שהצד שהכתיב את אופן החתימה הוא בעל היכולת הטובה יותר להקטין את הסיכון של התכחשות לחתימה: הוא יכול לעשות שימוש בטכנולוגיות חתימה מתקדמות, לקבוע נהלים שיבטיחו שרק לצד החותם תהיה גישה לחתימה; הצד שהכתיב את אופן החתימה הוא הנהנה העיקרי מההסדר, שכן החתימה משרתת את שיקולי הנוחות שלו, ומשכך הוגן להטיל עליו את ההסדר; ישנם פערי כוחות בין הצדדים לחוזה; יהיה יעיל יותר להטיל עליו את החובה, שכן בידיו המידע לגבי הטכנולוגיה שבה נעשה שימוש כדי לבצע את החתימה.

דוגמה נוספת מופיעה בהסדר שנקבע בחקיקה בעניין סליקה אלקטרונית של שיקים. השיק, שמקורו בנייר, נסרק על ידי הבנק למחשב ונסלק באופן אלקטרוני. ככל שהבנק מחליט שלא לשמור את השיק בנייר ולהסתפק בשיק הסרוק, קובע החוק חלוקת אחריות, שלפיה האחריות לנזק שנגרם עקב אי שמירת השיק, תחול על הבנק ולא על הלקוח[19]. הטעמים שעומדים מאחורי הטלת הנשיאה בנזק על הבנק הם היותו מונע הנזק הזול ויכולתו לפזר את הנזק, התועלת הכלכלית שמניב לו ההסדר (כלומר, הנאתו מההסדר), יכולותיו הטכנולוגיות הטובות והכלים המעשיים שברשותו (לדוגמה, קביעת נוהל פנימי לגבי אופן סריקת השיק ושמירת ההעתק הממוחשב), אשר מאפשרים לו לצמצם את הסיכון.

יובהר, כי במקרים שבהם לא נקבע הסדר ספציפי, יחול הדין הכללי, שמבוסס על השיקולים שתוארו לעיל.

☜ **ככלל, עדיף להטיל את סיכוני ההסדר על בעל היכולת הטובה יותר לצמצם אותם או לשאת בהם.** ☜ **בבחינת אופן חלוקת הנשיאה בסיכוני ההסדר, יש לשקול את השיקולים הבאים: מיהו בעל היכולת הטובה ביותר לצמצם את הסיכונים או לשאת בהם; פערי הכוחות בין הגורמים הנוגעים להסדר; שיקולי צדק; שיקולים חלוקתיים; שיקולי יעילות; שיקולי הוגנות; האם למי מהגורמים הקשורים להסדר יש אשם; מי הנהנה העיקרי מההסדר.**

[19] ראו סעיף 5 לחוק סליקה אלקטרונית של שיקים, התשע"ו-2016.

5. הוגנות ההסדר בהתאמתו לאוכלוסייה שעליה הוא נועד לחול:

על הסדר דיגיטלי להיות **הוגן**, וככזה עליו להיות **מותאם לאוכלוסייה שעליה הוא נועד לחול**. כמו כן, עליו להבטיח כי יינתן **מענה הולם** לכל קבוצות האוכלוסייה הנוגעות לעניין, לרבות לקבוצות שעלולות להתקשות בשימוש בכלים דיגיטליים. הכל כמפורט להלן.

5.1 התאמת נטלי ההסדר למאפייני האוכלוסייה המושפעת ממנו

הסדרים דיגיטליים שונים עשויים להטיל מגוון נטלים על הגורמים המעורבים בהם. כך, למשל, הסדר שכולל שימוש בחתימה אלקטרונית מאושרת[20] (להלן: "**חתימה מאושרת**") עשוי להטיל נטל כספי של רכישת אמצעי החתימה ושל מחשוב מתאים, נטל של הקצאת זמן בשל הצורך לנכוח בעת הנפקת אמצעי החתימה ונטל טכנולוגי של בקיאות בשימוש בכלי הטכנולוגי.

על מנת ליצור הסדר הוגן, יש **להתאים את נטלי ההסדר למאפייני הגורמים המושפעים ממנו וליכולתם הצפויה לעמוד בהם**. התאמה זו תסייע גם ביצירת הסדר ישים. כך, למשל, נראה שהסדר המחייב שימוש בחתימה מאושרת לא מתאים להיות מוחל על כלל הציבור, שכיום[21] לא מחזיק באמצעי חתימה המאפשרים ביצוע חתימה מאושרת.[22]

5.2 סבירותה של קביעת ערוץ דיגיטלי כערוץ יחיד

ישנם מקרים שבהם נשקלת החלת הסדר דיגיטלי על הגורמים הנוגעים לו, כך שהם יהיו חייבים לעשות שימוש בכלים דיגיטליים על מנת לקחת חלק בהסדר, ומבלי שתועמד להם חלופה אחרת (להלן גם: "**ערוץ דיגיטלי כערוץ יחיד**"). כך, למשל, קביעה כי צריכת שירות תתבצע רק באופן דיגיטלי תחייב את קהל היעד של השירות לעשות שימוש באמצעים דיגיטליים כדי לצרוך אותו.

קביעת ערוץ דיגיטלי כערוץ יחיד היא נושא מורכב, שמעלה שאלות כבדות משקל בדבר סבירות קביעה זו. במקרים לא מבוטלים, קביעתו של ערוץ דיגיטלי כערוץ יחיד תהיה בלתי סבירה. כדי לבחון האם קביעה זו תהיה סבירה, יש לבחון את נסיבות העניין, ובראשן את מאפייני האוכלוסייה המשופעת מההסדר. מעורבותה של אוכלוסייה מגוונת בהסדר עשויה להשליך על שאלת סבירותו של קביעת ערוץ דיגיטלי כערוץ יחיד. כמו כן, קיומו של מענה הולם, כמפורט בסעיף הבא, עשוי להשליך גם הוא על שאלת הסבירות. **לפיכך, קביעת ערוץ דיגיטלי כערוץ יחיד כפופה לקבלת אישורו של היועץ המשפטי לממשלה או מי מטעמו.**

בבחינת קביעת ערוץ דיגיטלי כערוץ יחיד כאמור יש לשקול מספר שיקולים, ובהם, בין היתר-

---

[20] ראו הגדרתה של חתימה אלקטרונית מאושרת ומאפייניה בסעיף 1 לחוק חתימה אלקטרונית.

[21] נכון לשנת 2019.

[22] יצוין, כי על פי חוק חתימה אלקטרונית, המדינה רשאית להנפיק לאזרחים תעודה שעל גביה אמצעי חתימה אלקטרונית מאושרת, ועל פי סעיף 25 לחוק מרשם האוכלוסין, תעודת הזהות החכמה יכולה לכלול רכיב של חתימה אלקטרונית. על כן, כשהמדינה תספק אמצעי חתימה לכלל האזרחים, חלק מהנטלים שהוזכרו לא יהיו רלוונטיים עוד.

- **האם ההסדר נוגע לאוכלוסיות שעלולות להתקשות בשימוש באמצעים דיגיטליים:** ישנן קבוצות באוכלוסייה שבחלקן לא נוהגות לעשות שימוש באמצעים דיגיטליים בשל כך שאין להן את היכולות או האמצעים לעשות בהם שימוש או מטעמים אחרים. קבוצות אלה עשויות לכלול, בין היתר, אנשים מבוגרים, אנשים שאין להם אמצעים מספיקים לצורך רכישת כלים דיגיטליים או ידע טכנולוגי, ואנשים שאינם עושים שימוש באמצעים דיגיטליים מטעמים תרבותיים או דתיים. רמת האוריינות הדיגיטלית של אנשים הנמנים על קבוצות אלה, או לכל הפחות של חלק מהם, עלולה להיות נמוכה.[23]

על כן, יש לבחון האם הגורמים הנוגעים להסדר כוללים קבוצות באוכלוסייה שעלולות להתקשות בשימוש באמצעים דיגיטליים בשל העדר היכרות וידע, יכולות או אמצעים מתאימים, או מסיבות אחרות.

☜ בנסיבות מסוימות, העמדת שירות דיגיטלי יחיד לאוכלוסיות, שאין להן את היכולות או האמצעים לעשות שימוש באמצעים דיגיטליים באופן עצמאי או היכרות עם אמצעים אלה, **תהיה בלתי סבירה**. נסיבה שעשויה להעיד על חוסר סבירות כאמור היא היותו של ההסדר עוסק בשירות **בסיסי** שניתן **לציבור הרחב**.

- **סוג האוכלוסיות הנוגעות להסדר:** הסדרים דיגיטליים עשויים להתייחס לגורמים הנמנים על קבוצות מסוגים שונים, כמו למשל: גורמים מקצועיים על כל גווניהם כדוגמת בעלי רישיונות (רואי חשבון, עורכי דין או מורי דרך); תאגידים; מגזר שלישי; גורמים עסקיים (עסקים גדולים או עסקים קטנים); הציבור הרחב.

☜ ככלל, ככל שההסדר נוגע לאוכלוסייה מתוחכמת ומקצועית יותר (כמו גורמי מקצוע), כך יהיה סביר יותר להטיל עליה חובות הקשורות לשימוש באמצעים דיגיטליים. באופן דומה, ככל שההסדר נוגע לאוכלוסייה כללית יותר (הציבור הרחב), כך יהיה סביר פחות להטיל חובות הקשורות לשימוש באמצעים דיגיטליים.

יובהר, כי כלל זה **כפוף לבחינה פרטנית** בכל מקרה ומקרה (למשל, אף שמורי דרך ועורכי דין גורמי מקצוע, קיימת שונות רבה במאפייניהם).

---

[23] יובהר, כי גם מבין הקבוצות שנמנו בפסקה זו, עשויים להיות אנשים שנוהגים לעשות שימוש באמצעים דיגיטליים. לכן, יש לבחון בכל מקרה לגופו מהי רמת האוריינות של קהל היעד של השירות ועד כמה הוא בעל נגישות לאמצעים דיגיטליים.

יצוין, כי במקרים שבהם ההסדר נוגע לשילוב של אוכלוסייה מקצועית ואוכלוסייה מהציבור הרחב, ניתן לשקול להבחין בין סוגי האוכלוסיות השונות במסגרת ההסדר. כך, למשל, ראו ההסדר הקבוע בתקנה 14(ד) לתקנות הירושה, התשנ״ח-1998, לעניין הגשת בקשה לצו ירושה. הסדר זה קובע כי בעוד שמבקש רשאי להגיש את בקשתו הן באופן מקוון והן באופן פיסי, אם המבקש מיוצג על ידי עורך דין, אזי על הבקשה להיות מוגשת באופן מקוון בלבד. דוגמה נוספת להבחנה כזו ניתן למצוא בתקנה 76א לתקנות פשיטת הרגל, התשמ״ה-1985 וכן בכללי העמותות (הגשה באופן מקוון), התשע״ט-2019.

- **סוג השירות שההסדר עוסק בו:** סוג השירות או המוצר שבו עוסק ההסדר משפיע גם הוא על סבירות קביעת הסדר כערוץ דיגיטלי יחיד. סוגי השירותים השונים מגוונים, ובהם למשל שירותים בסיסיים כמו קצבאות מביטוח לאומי ושירותים מהתחום העסקי כמו פתיחת חברה ברשם החברות.

☜ ככלל, ככל שהשירות שבו עוסק ההסדר בסיסי או רגיש יותר, ומשפיע על קיום חובה או מימוש זכות, כך יהיה סביר פחות לאפשר לצרוך אותו באופן דיגיטלי בלבד, ולהיפך. זאת, מאחר שהסדר שעניינו בשירות בסיסי עשוי ללמד על כך שקהל היעד שלו כולל אוכלוסייה שעלולה להתקשות בשימוש באמצעים דיגיטליים.

5.3 <u>מתן מענה הולם למי שאינו בעל כישורים או אמצעים לעשות שימוש באמצעים דיגיטליים בעצמו</u>:

5.3.1 <u>הכלל – מתן מענה הולם</u>

בין אם הסדר נקבע במתכונת של ערוץ דיגיטלי יחיד ובין אם לאו, עליו לתת **מענה הולם** לאוכלוסיות שאין להן כישורים או אמצעים לקחת חלק בהסדר הדיגיטלי באופן עצמאי. מענה הולם משמעו כי תינתן **אפשרות סבירה ומעשית לאוכלוסיות אלה, בהתחשב במאפייניהן הייחודיים, לבצע את הפעולות הנדרשות לביצוע במסגרת ההסדר**.

כך, למשל, החלת הסדר של הגשת טופס למוסד ממוסדות המדינה באופן מקוון על אדם מבוגר, מבלי לספק לו מענה הולם כאמור, עלולה למנוע ממנו את האפשרות לבצע הגשה זו באופן עצמאי. החלה כזו עלולה לאלץ אותו להיעזר בקרובי משפחתו או באנשים אחרים שבסביבתו, ובכך למנוע ממנו ליהנות משירות ממשלתי זמין ונוח. **אילוצו להיעזר בסובבים אותו** ולהיות נתון לרצונם הטוב, ככלל, לא מהווה מענה הולם.

מענה הולם כאמור יכול להינתן במסגרת ההסדר הדיגיטלי או על ידי העמדת חלופה שאינה דיגיטלית.[24] כך, למשל, מענה עשוי להינתן באמצעות הדרכה, ליווי השימוש של האדם בהסדר הדיגיטלי על ידי פקיד מטעם המשרד הממשלתי בעמדות שירות עצמי, ביצוע הפעולה הדיגיטלית ע"י נותן השירות עבור מקבל השירות במהלך שיחה טלפונית איתו[25], או על ידי התאמת הממשק הדיגיטלי באופן ייעודי לאוכלוסיית היעד, כך שהיא תונגש לה באופן שתוכל לעשות שימוש בממשק באופן עצמאי.

לעניין העמדת חלופה שאינה דיגיטלית, יש לתת את הדעת גם **לברירת המחדל** לצריכת שירות דיגיטלי ולבחון את סבירותה. דוגמה לברירת מחדל כזו היא קביעה כי שירות יינתן לאדם באופן דיגיטלי, אלא אם הוא יודיע אחרת. בנסיבות מסוימות, מתן שירות דיגיטלי לאוכלוסייה, שמתקשה בשימוש באמצעים דיגיטליים, כברירת מחדל, עלולה לפגוע בה ולהקטין את נגישותה לשירות.

כמו כן, יש להתחשב באוכלוסיות אלה גם במקרה שבו מבצעים שינויים בהסדר הפיסי בנייר, וגם הוא צריך לתת להן מענה הולם.

5.3.2 מבחן עזר לקביעה האם המענה המתגבש הוא מענה הולם – הפער באיכות השירות

במסגרת הבחינה מהו מענה הולם, יש לבחון מהו הפער בין איכות השירות, הניתן לאוכלוסיית היעד הצורכת את ההסדר הדיגיטלי כפי שהוא, לבין איכות השירות, הניתן לאוכלוסיית היעד שנקבע עבורה הסדר חלופי הכולל התאמות. **פער באיכות השירות עלול להעיד** על כך שהמענה אינו הולם, וככזה כחורג ממתחם הסבירות.

ניקח לדוגמה שירות שניתן עד כה מרחוק על ידי שליחת מכתב בדואר, אשר מוחלף בשירות דיגיטלי מרחוק. במקרה כזה, התאמה, שמחייבת אדם להגיע לסניף ולהסתייע בפקיד על מנת לצרוך שירות מסוים, עשויה להצביע על אי הסבירות של המענה לאוכלוסייה זו.

על כן, במקרה שבו העמדת ערוץ דיגיטלי יחיד תביא לביטול אפשרות קיימת לקבל את השירות שלא באמצעות הגעה ללשכת שירות, ככלל, על מענה הולם להיות כזה שלא ידרוש הגעה ללשכת שירות. זאת, ככל שישנה הרעה ברמת השירות עבור אוכלוסיית מקבלי השירות המתקשה לעשות שימוש בכלים דיגיטליים.

5.4 תמריצים

---

[24] יצוין, כי העמדת חלופה שאינה דיגיטלית נובעת בדרך כלל מאילוץ ואינה עולה בקנה אחד עם המגמה הממשלתית של גורמי המקצוע האמונים על תחום התקשוב והדיגיטציה, שהינה כי רצוי לספק מענה הולם בסביבה הדיגיטלית.

[25] ראו, למשל, התייחסות לתוכנית התמיכה הדיגיטלית של ממשלת אנגליה במדריך, שבו מתוארת החובה, בעת יצירת שירות דיגיטלי, לספק סיוע לאדם שזקוק לעשות שימוש בשירות, אך אין לו את הכישורים או הגישה לעשות זאת בעצמו, https://www.gov.uk/service-manual/helping-people-to-use-your-service/assisted-digital-support-introduction.

ישנם מקרים שבהם משרד ממשלתי שוקל את האפשרות לקבוע תמריצים להצטרפות להסדר דיגיטלי. למשל, על ידי קביעת תנאים מיטיבים למי שמגיש מסמך באופן דיגיטלי ביחס לאלו שמגישים את אותו המסמך באופן פיסי.

השיקולים שפורטו לעיל בסעיף 5.2 בעניין סבירותו של ערוץ דיגיטלי יחיד מתאימים להישקל גם בעת בחינת קביעת תמריצים להצטרפות להסדר הדיגיטלי.

במסגרת בחינת קביעת תמריצים כאמור, יש לבחון את מאפייניי האוכלוסיות הנוגעות להסדר ולהתחשב באוכלוסיות שלא נהנות מנגישות לאמצעים דיגיטליים. במקרים שבהם מעורבות אוכלוסיות אלה בהסדר, יש לבחון את מכלול התמריצים הקיימים, ולתת את הדעת לתמריצים **המובנים** בעצם קיומו של ההסדר הדיגיטלי. קיומם של תמריצים מובנים מספקים עשויים לייתר את הצורך בתמריצים יזומים.

כך, למשל, שירות דיגיטלי של משרד ממשלתי שניתן מרחוק, במקום להגיע לסניף של אותו משרד ממשלתי, מייצר כשלעצמו תמריץ הודות לחסכון במשאבים הדרושים לשם הגעה לסניף. על כן, נראה כי כשהשירות הדיגיטלי המוצע איכותי מספיק ומסייע לציבור, הצורך בתמריצים אחרים כדוגמת הנחה באגרות פוחת.

☜ **על נטלי הסדר דיגיטלי להתאים למאפייני הגורמים המושפעים ממנו וליכולתם הצפויה לעמוד בהם.** ☜ **סבירותו של קביעת הסדר כערוץ דיגיטלי יחיד, אשר משמעותה היא כי הגורמים הנוגעים להסדר יהיו חייבים לעשות שימוש באמצעים דיגיטליים, תלויה בנסיבות העניין. בנסיבות מסוימות, העמדת שירות דיגיטלי יחיד לאוכלוסיות, שאין להן את הכישורים או האמצעים לעשות שימוש באמצעים דיגיטליים באופן עצמאי, תהיה בלתי סבירה. קביעת הסדר כערוץ דיגיטלי יחיד כפופה לקבלת אישורו של היועץ המשפטי לממשלה או מי מטעמו.** ☜ **על הסדר דיגיטלי לתת מענה הולם למי שאין לו את הכישורים או האמצעים לקחת חלק בהסדר הדיגיטלי באופן עצמאי.**

6. חזקות מסירה בהסדרים דיגיטליים

6.1 הסבר על חזקות מסירה

אחד מהסיכונים שעשויים להתעורר בהסדרים נוגע להעברת מידע (בסעיף זה: "**מסר**") בין צדדים. קיים מגוון גדול של העברות מסרים כמו, למשל, העברת הודעה מהרשות לאזרח, הגשת מסמך לרשות על ידי אזרח או תאגיד והעברת מסמכים בין צדדים בשוק הפרטי.

במסגרת העברת מסר עלולים להתעורר, הן בעולם הפיסי והן בעולם הדיגיטלי, **שני סיכונים מרכזיים**. האחד, הוא כי הנמען יתכחש לקבלת המסר שהתקבל אצלו, והשני הוא כי מסר שנשלח כלל לא יגיע. במקרה של התממשות אחד מסיכונים אלה, עולה השאלה על מי צריך להיות מוטל הנטל להוכיח כי המסר התקבל או כי נכשלה העברתו.

לשאלה זו עשויה להיות חשיבות רבה בשל המשמעויות שעשויות להיות למסירת המסר או למועד מסירתו. כך, למשל, ישנם מסמכים שנשלחים לאזרח, אשר ממועד קבלתם "מתחיל להיספר" פרק זמן מסוים. במהלך פרק זמן זה, האזרח עשוי להידרש לבצע פעולה כלשהי כמו לדוגמה תשלום לרשות מינהלית. עיכוב בתשלום כאמור עלול לגרור השתת ריביות על האזרח.

על מנת ליצור **ודאות משפטית** לגבי הגעת מסר ליעדו, לפעמים נקבעות בחיקוקים שונים חזקות מסירה, אשר מתנות על כללי הראיות הרגילים. חזקה היא הנחה, שלפיה רואים מסר ככזה שהתקבל אצל נמען בהתקיים תנאים מסוימים, אף שקבלתו לא הוכחה מבחינה עובדתית. הרעיון המונח ביסודן של החזקות הוא, שקיימת הסתברות מספקת לכך שברוב המקרים הן משקפות את המצבים העובדתיים הקיימים למעשה[26]. חזקות עשויות להידרש במקרים שונים כמו למשל כשלנמען המסר יש אינטרס להתכחש לקבלת ההודעה.

חזקות מסירה קיימות בחיקוקים שונים. ראו, למשל סעיף 57ג לפקודת הראיות [נוסח חדש], התשל"א-1971; תקנה 52 לתקנות הירושה, תשנ"ח-1998; תקנה 161 לתקנות סדר הדין האזרחי, התשע"ט-2018.

6.2 כללים לקביעת חזקת מסירה

לנוכח העובדה כי לחזקות המסירה יש משמעות משפטית רבה, ניתן לקבוע חזקות מסירה רק בחיקוק. מאחר שסתירת חזקת מסירה אינה מלאכה פשוטה, ככלל רצוי למעט בקביעת חזקות. הבחינה האם לקבוע חזקת מסירה תתבצע לפי כללי הנחיה זו, ובפרט בהתאם לסעיף 4 "הקטנת סיכוני ההסדר וחלוקת הנשיאה בהם במקרה של התממשותם", לעיל, בפרק זה שעניינו בהקטנת סיכוני ההסדר וחלוקת הנשיאה בסיכוניו במקרה של התממשותם.

---

[26] חיים ה' כהן **המשפט** 273-274 (1992).

כך, למשל, במסרים שמועברים מהמדינה אל הפרט, יש להביא בחשבון כי מערכת היחסים בין המדינה לפרט מתאפיינת בפערי כוחות: מצד אחד, ניצבת המדינה, אשר יכולתה לצמצם את הסיכונים הכרוכים בהגעת מסרים ולשאת בהם היא רבה יותר (למשל, על ידי קביעת נהלי מסירה מתאימים ושימוש בטכנולוגיות מתקדמות). מהצד השני ניצב הפרט, שיכולתו להוכיח, כי לא קיבל מסר שהמדינה טוענת ששלחה אליו, היא בדרך כלל מוגבלת.

ככל שמתקבלת החלטה לקבוע בחיקוק חזקת מסירה, עליה לעמוד בשני הכללים הבאים:

(1) על חזקת המסירה להיות **ניתנת לסתירה.**

(2) קביעת חזקת מסירה צריכה להיות כפופה לכך שהמסר יתקבל אצל הנמען **ברמת ודאות גבוהה.** בבחינת רמת הוודאות כאמור, יש להביא בחשבון את המרכיבים הבאים:

- <u>המען הדיגיטלי</u>- **על המען הדיגיטלי, שאליו נשלח המסר, להיות בשימושו השוטף של הנמען במועד השליחה**. לחלופין, ניתן לבחור במען, שלנמען גישה אליו, ואינו בשימושו השוטף, אם הנמען יודע כי אמור להתקבל מסר במען זה (למשל, על ידי יידוע מראש של הנמען או על ידי שליחת הודעה למען אחר של הנמען כמו, למשל, הודעת טקסט למספר הסלולרי של הנמען, המודיעה על שליחת המסר למען הדיגיטלי) וכי הוא יודע כיצד לעשות שימוש במען הדיגיטלי (למשל, שרמת האוריינות הדיגיטלית שלו מתאימה לקבלת המסר באמצעי הדיגיטלי שנבחר).

  יצוין, כי במקרה שבו המען עשוי להשתנות מעת לעת, יש להבטיח כי קיים **מנגנון עדכון מען**. למשל, במקרה שבו המען הוא דואר אלקטרוני של הנמען, יש להבטיח כי במקרה שבו הנמען מחליף את כתובת הדואר האלקטרוני שלו, השליחה תתבצע לכתובת הדוא"ל העדכנית שלו. מנגנון עדכון מען יכול להתבצע בדרכים שונות. דוגמה לכך היא הטלת חובה על הנמען לעדכן על שינוי במען הדיגיטלי שלו. חובה כאמור כפופה ליידוע של הנמען על חובתו. דרך אחרת לעדכון מען יכולה להיות הטלת חובה על השולח להתעדכן מעת לעת במען הדיגיטלי של הנמען. סוג המנגנון ייקבע על פי נסיבות העניין.

- <u>תהליך השליחה</u> – על שליחת המסר להתבצע תוך שמירה על **שלמותו ועל אי שיבושו או אובדנו** בתהליך העברתו מהשולח לנמען. ניתן לשמור על כך, בין היתר, על ידי קביעת נהלים ושימוש באמצעי אבטחה מספקים[27]. יצוין, כי ישנם אמצעים טכנולוגיים אמינים, ששומרים על שלמות המסר ומבטיחים ברמת וודאות גבוהה את אי שיבושו או אובדנו בתהליך ההעברה. כך, למשל, משלוח הודעת כתובות (SMS) למכשיר סלולרי או משלוח דוא"ל[28].

---

[27] ראו, למשל, אמצעי ההגנה הקבועים בסעיף 36 לפקודת הראיות [נוסח חדש], התשל"א-1971: נקיטה של אמצעי הגנה סבירים מפני חדירה לחומר מחשב ומפני שיבוש בעבודת המחשב באורח סדיר.

[28] כך על פי חוות דעת מקצועית בעניין אמינות מערכות הדואר האלקטרוני והמסרונים מאת ראש רשות התקשוב הממשלתי במשרד ראש הממשלה מיום 19.2.2019. חוות דעת זו מצורפת להנחיה ומסומנת כמסמך עזר 4.

בנוסף, מערכת הדיוור הדיגיטלי הממשלתי שפותחה ברשות התקשוב, ומשלבת מספר מערכות טכנולוגיות, ובהן פורטל האזור האישי, מהווה פלטפורמה המבטיחה את העברת המסר לנמען בשלמותו, תוך הבטחת צפייתו על ידי הנמען בלבד, ברמת ודאות גבוהה אף יותר משליחה בדוא״ל או במסרון.

- <u>מועד קבלת המסר</u> – מרכיב זה צריך להיבחן רק במקרים שבהם החזקה מבקשת לכלול התייחסות למועד השליחה או הקבלה (אלו המקרים הנפוצים). בעניין מועד קבלת המסר, יש להבטיח כי תהיה **הלימה בין המועד המשוער, שבו התקבל המסר, וככל הניתן בתוספת פרק זמן סביר נוסף לאותו מועד, לבין המועד שנקבע בחזקה**.

  כמו כן, יש להתחשב גם בנסיבות הצפייה הצפויה במסר, ככל שאלה ידועות. כך, למשל, אם המסר נשלח לתיבת דואר אלקטרוני ששייכת למקום עבודתו של הנמען ובקשר לעבודתו, סביר להניח כי הוא יצפה בהודעה רק בימי העבודה ובשעות העבודה שלו. במקרה כזה, לא יהיה סביר לקבוע בחזקה את מועד הקבלה בשעות הערב או בימי מנוחה, אף אם מועד הקבלה המשוער יהיה בשעות או בימים אלה.

  יצוין, כי שליחת מסר במספר דרכים (למשל, באמצעות דוא״ל וגם באמצעות הודעת טקסט למכשיר הסלולרי של הנמען) מעלה את רמת הוודאות כי המסר התקבל אצל הנמען.

לסיום חלק זה יובהר, כי כשנשקלת קביעת חזקת מסירה דיגיטלית לגבי מסמך שקיימת לגביו חזקת מסירה בעולם הפיסי, אין בקיומה של חזקת מסירה בעולם הפיסי כשלעצמו כדי להצדיק את קביעתה של חזקת המסירה הדיגיטלית. בכל מקרה, על חזקת המסירה הדיגיטלית לעמוד בתנאים שפורטו לעיל.

☜ **ככלל, יש למעט בקביעת חזקות מסירה בחיקוקים.**

☜**ככל שנקבעת חזקת מסירה, עליה לעמוד בשני התנאים הבאים:**

1) על החזקה להיות ניתנת לסתירה.

2) קביעת חזקת מסירה צריכה להיות כפופה לכך שהמסר יתקבל אצל הנמען ברמת ודאות גבוהה. לשם כך, יש להביא בחשבון את המרכיבים הבאים: על המען הדיגיטלי, שאליו נשלח המסר, להיות בשימושו השוטף של הנמען במועד השליחה; על שליחת המסר להתבצע תוך שמירה על שלמותו ועל אי שיבושו או אובדנו בתהליך העברתו מהשולח לנמען; ככל שהחזקה כוללת את מועד קבלת המסר, צריכה להיות הלימה בין המועד המשוער, שבו התקבל המסר, וככל הניתן בתוספת פרק זמן סביר נוסף לאותו מועד, לבין המועד שנקבע בחזקה.

פרק ג'– יישום ההסדר בחקיקה – פרשנות דין קיים ויצירת דין חדש

יישום ההסדר הדיגיטלי שגובש מחייב בחינה של השאלה האם הוא תואם את הדין החל או שמא נדרש שינויו או יצירה של דין חדש. בשלב הראשון, יש לבדוק האם קיימת כבר חקיקה שמסדירה את הנושא, ואם כן האם ניתן לאפשר במסגרתה את ההסדר הדיגיטלי המתוכנן בדרך של פרשנות.

כמו כן, יש לזהות את הדינים הכלליים שעשויים לחול על כל הסדר דיגיטלי, לצורך התאמתו אליהם או על מנת להחריג את ההסדר מהם במקרים המתאימים. כך, למשל, על הסדר שכרוך בעיבוד של מידע אישי, חלות ההוראות בעניין מחוק הגנת הפרטיות, התשמ"א-1981.

ככל שישנם אילוצים מכוח הדין ונדרש שינויו, יש לבצע, בשלב השני, את השינויים הנדרשים, בהתאם לאמור להלן.

1. פרשנות דין קיים – האם הדין הקיים מאפשר את קיומו של ההסדר?

נקודת המוצא לבחינה האם הדין מאפשר את קיומו של ההסדר הדיגיטלי המתגבש, מבוססת על עקרון אי העדיפות, אשר תואר בפרק א'. לפיו, במקרה שבו אין סממן בחקיקה ששולל אפשרות לבצע פעולה באופן אלקטרוני, אזי ניתן לקיים אותה באופן אלקטרוני.

כך, למשל, כשנקבע בדין כי יש **להגיש** מסמך לרשות מינהלית, ואין סממן ששולל את הגשת המסמך בדרך מקוונת, ניתן לאפשר הגשה מקוונת במסגרת הדין החל[29]. זאת, בכפוף לכך שלא קיימות סיבות אחרות שעשויות לשלול את ההגשה המקוונת ולכך שהמטרות והשימושים של ההגשה יתקיימו בהגשה המקוונת, בהתאם לעקרון השקילות הפונקציונלית שתואר בפרק א'[30]. כך גם כשהדין קובע שעל הרשות **לפרסם מידע**, הפרסום יכול להתבצע במגוון דרכים המגשימות את התכליות כנדרש, לרבות בדרך של פרסום באופן דיגיטלי, לדוגמה, באתר האינטרנט של הרשות או באמצעי אחר.

---

[29] יצוין, כי שליחת מסר במספר ערוצים כמו למשל דוא"ל והודעת טקסט, עשויה להעלות את רמת הוודאות כי המסר התקבל אצל הנמען.

[30] כך, למשל, אם ההגשה נדרשת בכתב, אז יש לשאול איך יוגשמו מטרות הכתב בעולם הדיגיטלי (לדוגמה, באופן הניתן לאחזור הכתב); אם יש לחתום על המסמך המוגש, יש לשאול כיצד להגשים תכליות החתימה באופן אלקטרוני, וכד'.

דוגמה נוספת היא מקרה שבו קבוע בתקנות **טופס** שאותו יש להגיש לרשות. גם כאן, המונח "טופס" כולל גם "טופס מקוון" ויש לשאול האם הגשה מקוונת של הטופס עולה בקנה אחד עם תכליות הדין. יצוין לעניין זה, כי ייתכנו הבדלים צורניים ותוכניים בין הגשה דיגיטלית של המידע שבטופס לבין הגשה פיסית של הטופס כפי שמופיע בתקנות. כך, למשל, אם בטופס הקבוע בתקנות מופיעה המילה "חתימה" ומעליה מסומן קו תחתון, שנועד להשלמת חתימה, אזי אין בכך כדי לשלול את מילוי הטופס באופן דיגיטלי באמצעות חתימה אלקטרונית. חתימה זו לא חייבת להופיע כחתימה גרפית על גבי הקו התחתון, אלא היא יכולה להתבצע בכל דרך אחרת, העומדת בתכליות הדין (ראו לעניין זה הגדרה "חתימה אלקטרונית" בחוק חתימה אלקטרונית, התשס"א-2001 וסעיף 2(א)(2) לחוק זה).

במקרים שבהם תיתכנה פרשנויות שונות של הדין, אשר אחת מהן מאפשרת את קיומו של ההסדר הדיגיטלי המתבקש, השאלה האם ניתן לבחור בפרשנות זו תיגזר מתכליות הדין. אם תכליותיו עולות בקנה אחד עם ההסדר הדיגיטלי, אזי ניתן לקיים את ההסדר הדיגיטלי במסגרת הדין החל. כך, למשל - המילים "**חתימת יד**" עשויות להעיד על כך שחתימה צריכה להתבצע ב"יד" החותם באופן פיסי, אך אם תכליות הדין מאפשרות זאת, מילים אלה עשויות להתפרש גם כחתימה ביד החותם באופן דיגיטלי. באופן דומה, תפורשנה המילים "**כתב יד**"; המונח "**כרטיס**" עשוי להתפרש ככרטיס נייר אך גם ככרטיס דיגיטלי[31]; כשדין קובע כי מסמך צריך להיות מוגש במספר עותקים, אין להסיק מכך כי ההגשה חייבת להתבצע באופן פיסי[32].

יצוין, כי במקרים רבים, ביצוע תיקונים בדין יארך זמן רב יותר מאשר גיבוש פרשנות גמישה של הדין. לכן, בדרך כלל תהיה עדיפות לפרשנות הדין, בהתאם לכללי הנחיה זו, על פני תיקון הדין. על אף האמור, יהיו מקרים שבהם אף שהדין החל מאפשר את קיומו של ההסדר הדיגיטלי המתבקש, רצוי לבחון האם בכל זאת יש צורך לבצע התאמות בדין על מנת להבטיח כי תכליותיו של ההסדר הדיגיטלי תתקיימנה.[33]

---

[31] ראו לעניין פרשנות המונח "כרטיס" פסקה 12 לפסק דינו של בית המשפט העליון בבג"ץ 8570/14 כן לזקן נ' שר החתבורה ואח' (3.10.2017). בפסק דין זה, התייחס בית המשפט, בדונו בכרטיסי "רב קו" הדיגיטליים שנעשה בהם שימוש בתחבורה הציבורית, לפרשנות הניתנת למונח "כרטיס". בית המשפט הבהיר, שאף שחוק האזרחים הוותיקים, התש"ן-1989, עושה שימוש במונח "כרטיס", שהינו – כך לפי מילון אבן שושן - "פתק, פיסת נייר או קרטון, שרשום עליה דבר מה", אין הכוונה בחוק לפתק הפיזי, אלא לזכות הטמונה בו – הסדר הנסיעה שהכרטיס מייצג. כלומר, בית המשפט התנתק מהמימד הפיסי ופירש את החוק על פי מהותו.

[32] כך, למשל, תקנה 19(א) לתקנות הירושה, התשנ"ח-1998 קובעת כי "הרוצה להגיש התנגדות לבקשה יגיש לרשם לענייני ירושה כתב התנגדות במספר עותקים מספיק עבור בית המשפט ובעלי הדין". אין בנוסח זה כדי לשלול את האפשרות לבצע את ההגשה באופן דיגיטלי.

[33] כך, למשל, ברישיונות שניתנו לחברות הטלפון הסלולרי על ידי משרד התקשורת (נכון לאוגוסט 2017), נקבע כי חוזה ההתקשרות של חברת סלולר עם מנוייה צריך להיות **בכתב**. אף שלפי הדין הכללי, חוזה התקשרות כתוב יכול להתבצע גם באופן אלקטרוני, נקבעה ברישיון הוראה מפורשת בנוגע לכתב בעולם האלקטרוני. "כתב" הוגדר ברישיון כך: "לרבות מסמך אלקטרוני הניתן לשמירה ולאחזור בידי המנוי". כלומר, נקבעו תנאים שעל כתב אלקטרוני לעמוד בהם בשביל שדרישת הכתב תתמלא בעולם האלקטרוני. אם כן, הטעם לכך הוא להבטיח הגנה על לקוחות חברות הסלולר.

מופיע לדוגמה, ברישיון כללי לחברת פלאפון תקשורת בע"מ, למתן שירותי רדיו טלפון-נייד בשיטה התאית (רט"ן).
נוסח משולב נכון לתאריך 22 ביולי 2018 בסעיף 55.3,
https://www.gov.il/BlobFolder/policy/pelephone/he/Pelephone%20-%20License%20-%20integrated%20version%20of%20the%20Internet%20as%20of%2022.7.18.pdf.

זאת ועוד, יש לבחון האם הדין הקיים כולל את כלל הכלים וההוראות הנורמטיביות הנדרשים על מנת לאפשר את ההסדר הדיגיטלי. ישנם מקרים חריגים, שבהם אף אם הדין הקיים מאפשר את קיומו של ההסדר המתגבש, מרכיב ממרכיבי ההסדר חייב להיות מעוגן בדין. מקרים חריגים לדוגמה הם קביעת הסדרי אחריות או התנאה על דיני הראיות (למשל, שינוי נטלי ראיה), אשר חייבים להיות מעוגנים בדין.

☜**במקרה שבו אין סממן בחקיקה ששולל אפשרות לבצע פעולה באופן אלקטרוני, ניתן לקיים אותה באופן אלקטרוני.**

2. יצירת דין חדש – כיצד לעגן את ההסדר בדין כשנדרש שינויו:

2.1 אופן ניסוח הדין- תכליות, כללים ומאפיינים במקום כלים וטכנולוגיות, וניתוק מהמימד הפיסי

בשונה מהעולם הפיסי, העולם הדיגיטלי משתנה במהירות. כמו כן, יש בעולם הדיגיטלי כלים רבים יותר מאלה הקיימים בעולם הפיסי. על כן, תכליות שונות של הסדרים יכולות להיות מוגשמות במגוון רחב יותר של כלים בעולם הדיגיטלי מאשר בעולם הפיסי. כמו כן, אופן הגשמתן עשוי להשתנות בתדירות גבוהה יותר. כך, למשל, תכלית של הזדהות בעולם הפיסי יכולה להיות מוגשמת באמצעות מספר קטן של דרכים כמו זיהוי פנים אל פנים או חתימה ידנית. בשונה מכך, תכלית של הזדהות בעולם הדיגיטלי עשויה להיות מוגשמת במגוון רחב של דרכים כמו באמצעות כרטיס חכם או סיסמה חד פעמית שנשלחת לטלפון הנייד.

בעת ניסוח הדין, שבו מבקשים לעגן את ההסדר הדיגיטלי, יש לתת את הדעת למאפיינים ייחודיים אלה של העולם הדיגיטלי. רצוי, ככלל, לגבש נוסח שיהיה **עדכני לאורך זמן ושיתאים להתפתחויות הטכנולוגיות התכופות**. כמו כן, רצוי ש**הנוסח יאפשר לעשות שימוש במגוון הכלים הטכנולוגיים**, שעשויים להגשים את מטרות ההסדר, לרבות בכאלה שאף לא היו קיימים בעת גיבוש הנוסח. ניסוח כאמור יאפשר לרשות המנהלית גמישות ויצמצם את הצורך בתיקונים תכופים של הדין בשל שינויים טכניים או טכנולוגיים.

לצורך כך, יש לנסח את הדין ברמת הפשטה גבוהה, כך שיכלול התייחסות **לתכליות ההסדר, למאפייניו או לכלליו, ולא לכלים או לטכנולוגיות** שיש לעשות בהם שימוש לשם הגשמת אותן תכליות או לשם קיום אותם כללים. כמו כן, **רצוי שלא לעשות שימוש במונחים הקשורים לעולם הפיסי.**

להלן מספר דוגמאות לאופן ניסוח "ניטרלי" של הדין:

- המילה "טופס" מבטאת את האופן שבו ניתן לקבל או להציג מידע. בעוד שבעולם הפיסי, מילוי טופס היה דרך מקובלת ונפוצה לשם קבלת מידע, בעולם הדיגיטלי יש מגוון דרכים לסדר מידע. טופס דיגיטלי הוא רק דרך אחת מדרכים אלו. על מנת לאפשר את יישומן של מגוון הדרכים הקיימות בעולם הדיגיטלי, נראה שיהיה עדיף לעשות שימוש במילה "מידע" במקום במילה "טופס". כך, למשל, אם אדם צריך להגיש בקשה לרשות, ניתן לקבוע בדין מהם פרטי המידע שיצטרכו להיכלל בבקשה, במקום לקבוע כי הבקשה תיערך בטופס מסוים, שבנוי באופן מסוים. יובהר, כי אין באמור כדי לשלול את האפשרות לפרש את המונח "טופס" בדין קיים, כך שיהיה ניתן למלא אותו באופן מקוון, וזאת אף אם המילוי המקוון אינו זהה לאופן המילוי של טופס הנייר.

- המילה "חתימה" מבטאת כלי להגשמת תכליות שונות כמו, למשל, גמירת דעת, הזדהות או אי שינוי מסמך לאחר החתימה. ניסוח ניטרלי יכלול, במקום את כלי החתימה, את תכליות החתימה או את הכללים שיש לקיים בשביל להגשים תכליות אלה, במנותק מאופן יישומם. ראו, למשל, סעיף 2(ג) לחוק שירותי תשלום, התשע"ט-2019, שקובע כי הסכמת הלקוח לכריתת חוזה שירותי תשלום תינתן במפורש ותתועד בידי נותן שירותי התשלום. כך, הנוסח מתייחס לכלל המהותי שעל נותן שירותי התשלום לעמוד בו ולא **לכלי** שבאמצעותו עליו לממש את הכללים. ראו דוגמה נוספת בתקנה 19ג לתקנות חובת המכרזים, התשנ"ג-1993, המנוסחת ברוח דברים אלו גם היא.

- כשישנה דרישה להגיש או למסור מידע, רצוי שלא לפרט את האמצעי למסירת המידע כמו דוא"ל. כך גם לעניין דרישה לשמור מידע או מסמך, שבעניינה רצוי לבטא את המהות (למשל, תיעוד הניתן לשמירה ולשימוש חוזר) ולא את האמצעי להגשמת הדרישה (למשל, מחברת או פנקס).

☜**בעת ניסוח הדין, שבו מבקשים לעגן את ההסדר הדיגיטלי, יש לתת את הדעת למאפיינים הייחודיים של העולם הדיגיטלי. רצוי, ככלל, לגבש נוסח שיהיה עדכני לאורך זמן ויתאים להתפתחויות הטכנולוגיות התכופות, ושיאפשר לעשות שימוש במגוון הכלים הטכנולוגיים, שמגשימים את מטרות ההסדר. זאת, על ידי ניסוח הדין ברמת הפשטה גבוהה, כך שיכלול התייחסות לתכליות ההסדר, למאפייניו או לכלליו, ולא לכלים או לטכנולוגיות שיש לעשות בהם שימוש לשם הגשמת אותן תכליות או לשם קיום אותם כללים. כמו כן, רצוי שלא לעשות שימוש במונחים הקשורים לעולם הפיסי.**

2.2 מדרג נורמטיבי

במקרה שבו נדרש שינוי בדין לשם מימוש ההסדר הדיגיטלי, יש לבחון באיזו רמה נורמטיבית (כדוגמת חקיקה ראשית או חקיקת משנה) יעוגן השינוי. הכללים שיחולו על חקיקת הסדר דיגיטלי הם אותם כללים שחלים על חקיקה של הסדרים אחרים. כך, למשל, כללי אחריות, נטלים ראייתיים כמו חזקות מסירה, וכן הסדרים הכרוכים בסיכון משמעותי לפגיעה בזכות יסוד, יצריכו הסדרה ולו חלקית בחקיקה ראשית.

☜ **הוראות בנוגע להסדרי אחריות ונטלים ראייתיים יעוגנו בדין.**

2.3 אי עיגון דרישות טכנולוגיות בחיקוק

במסגרת בחירת הרמה הנורמטיבית המתאימה לעיגון ההסדר הדיגיטלי, יש לקחת בחשבון גם את השאלה האם ההסדר מבקש להתייחס לדרישות טכנולוגיות כלשהן. ככלל, ככל שהרמה הנורמטיבית שבה מעוגן ההסדר גבוהה יותר, כך רצוי לקבוע הוראות ניטרליות יותר מבחינה טכנולוגית. זאת, על מנת למנוע מצב שבו שינויי הטכנולוגיה התכופים יהפכו את ההסדר – הלכה למעשה – ללא עדכני. על כן, רצוי שחקיקה ראשית תעסוק בנורמות שמבטאות אמות מידה. לצד זאת, ככל שיש צורך בקביעת דרישות טכנולוגיות, אלה ייקבעו במסגרת הוראות המעוגנות ברמה נורמטיבית נמוכה ככל הניתן[34]. זאת, בשביל שיהיה פשוט יותר לשנותן מעת לעת.

יצוין, כי ככל שנורמה מתייחסת לטכנולוגיה מסוימת, רצוי להתאים אותה לתקנים בינלאומיים בתחום.

☜**ככלל, ככל שהרמה הנורמטיבית שבה מעוגן ההסדר גבוהה יותר, כך רצוי לקבוע הוראות ניטרליות יותר מבחינה טכנולוגית.** ☜**במקרה שבו ההסדר כולל התייחסות לטכנולוגיה מסוימת –** **– יש להעדיף לעגן את ההתייחסות לטכנולוגיה ברמה נורמטיבית נמוכה ככל הניתן;** **– יש להעדיף טכנולוגיה התואמת תקנים בינלאומיים.**

---

[34] כך, למשל, התנאים שעל חתימה מסוג חתימה אלקטרונית מאובטחת לקיים נקבעו ב**חוק** חתימה אלקטרונית כתנאים מהותיים שאינם תלויים בטכנולוגיה מסוימת (למשל, יכולת לזהות שינוי במסר לאחר החתימה), בעוד שטכנולוגיות ספציפיות עוגנו ב**תקנות** חתימה אלקטרונית (אף עיגון זה לא נעשה בדרך של חיוב לעשות שימוש בטכנולוגיה זו או אחרת, אלא בדרך של קביעת חזקות ראייתיות שיקומו בעת שימוש בטכנולוגיה שאליה מתייחסות התקנות).

דוגמה נוספת לקביעת כללים הקשורים להסדר דיגיטלי היא הוראת ניהול בנקאי תקין 367 בעניין בנקאות בתקשורת, שעוסקת, בין היתר, בדרכי זיהוי ואימות. בהוראה זו, ישנם סעיפים שקובעים תנאים שעל הבנקים לעמוד בהם, תוך שמירה על ניטרליות טכנולוגית. כך, למשל, נקבע בסעיף 41, כי הליכים הקשורים לזיהוי הלקוח צריכים לאפשר לוודא כי מידע רגיש לא ייחשף בתהליך זה, ובסעיף 42 נקבע כי פעולות ברמת סיכון גבוה צריכות להתאפשר באמצעות אימות של שני גורמי אימות.

פרק ד' – הוראות בקשר למושגי יסוד בעולם הדיגיטלי

פרק זה עוסק במונחים נפוצים בעולם הדיגיטלי, באופן הפרשנות שלהם לפי הדין הקיים ובהפעלת הכללים בקשר אליהם בעת גיבוש הסדר דיגיטלי חדש.

1. קיום דרישת הכתב בעולם הדיגיטלי

בחוק הפרשנות, התשמ"א- 1981, המונח "כתב" זכה להגדרה רחבה, ולפיה כתב הוא "לרבות בכל דרך אחרת של הצגת אותיות, ספרות או סימנים בצורה הנראית לעין או הניתנת לפענוח חזותי". כלומר, גם הצגת אותיות, ספרות או סימנים בצורה הנראית לעין או הניתנת לפענוח חזותי, **שנוצרה באמצעי אלקטרוני**, נכללת בהגדרת "כתב". כך, למשל, מלל שמוצג בתוכנת דואר אלקטרוני או באתר אינטרנט, נכלל בהגדרת "כתב"[35]. הגדרה זו תואמת את עקרון אי העדיפות.

בדרך כלל נהוג לייחס לכתב שני מאפיינים מרכזיים[36]: נגישות לשימוש נוסף (הכתב נגיש לקריאה חוזרת) ואפשרות לאחזר את המידע (הכתב ניתן לשמירה)[37]. על כן, ככלל, כשנקבעת דרישת כתב בחיקוק, הסדר דיגיטלי שבא ליישם אותה צריך להבטיח קיומם של מאפיינים אלה[38].

יצוין, כי כשהדין עושה שימוש במונח "כתב יד", ניתן לפרשו בשתי דרכים: האחת היא כי פעולת הכתיבה חייבת להתבצע באופן פיסי, ב"יד" הכותב, והשנייה כי היא יכולה להתבצע ביד הכותב גם באופן דיגיטלי. בחירה בין הפרשנויות האפשריות תתבצע לפי תכלית דרישת הכתב בדין, בהתאם לכלל שפורט בפרק שעוסק בפרשנות דין קיים (ראו סעיף 1 "פרשנות דין קיים- האם הדין הקיים מאפשר את קיומו של ההסדר?" בפרק ג' לחלק א' שלעיל).

☜ **כתב יכול להתבצע גם באופן אלקטרוני.**

☜**ככלל, קיום דרישת כתב באופן אלקטרוני יתבצע על די כתב, שהינו נגיש לקריאה חוזרת ולשמירה.**

---

[35] יצוין, כי ישנם דינים שקובעים דרישות מסוימות בתחומים שונים, שעל כתב אלקטרוני לעמוד בהן. במקרים אלה, הדינים המסוימים גוברים על ההגדרה הכללית של "כתב" בחוק הפרשנות. ראו, למשל, הדוגמה של רישיונות הסלולר המוזכרת בה"ש 31.

[36] ניתן למצוא ביטוי למאפיינים אלה בדו"ח מסחר אלקטרוני (ראו סעיף 1 לפרק הראשון בדו"ח), וכן במסמכים בינלאומיים בתחום כמו, למשל, חוק המודל של האו"ם לעניין מסחר אלקטרוני (ראו סעיף 6 לחוק המודל).

[37] יצוין, כי בדרך כלל כתב שניתן לשמירה יהיה נגיש לשימוש נוסף. לעומת זאת, לפעמים כתב שניתן לשימוש נוסף לא יהיה ניתן לשמירה. כך, למשל, מידע שנשמר ביישומון ('אפליקציה') של ספק, נגיש לשימוש ביישומון אך לא בהכרח ניתן לשמירה באופן מקומי אצל הלקוח.

[38] יצוין, כי בעבר נעשה ניסיון להסדיר את דרישות הסף של מסמך אלקטרוני, במסגרת הצעת חוק מסחר אלקטרוני, התשס"ח-2008. הצעת החוק מגדירה מסמך אלקטרוני כמסר שמתקיימים לגביו שני מאפייני הכתב הנפוצים: נגיש לשימוש נוסף וניתן לאחזור.

2. מקור והעתק דיגיטלי: הפעלת כללי ההנחיה על דרישת מסמכי מקור

2.1 פיחות במעמדו של המסמך המקורי

בעבר שררה תפיסה שלפיה מקוריותו של מסמך מגבירה את מהימנותו. כיום, ישנן שיטות העתקה איכותיות, אשר מביאות לכך שמהימנותו של העתק מסמך גבוהה גם היא. על כן, בעולם הפיסי הקשר שבין דרישת מקור לבין רמת המהימנות התרופף. בהתאם לכך, חשיבותה של שמירת המקור ירדה.

ביטוי לכך ניתן למצוא בכרסום ב"כלל הראיה הטובה ביותר". על פי כלל הראיה הטובה ביותר, אין להוכיח את תוכנו של מסמך אלא בדרך של הצגת המקור בבית המשפט. על כן, על פניו, ניתן לסבור כי כשמסמך הקשור להסדר עשוי להיות מוגש לבית המשפט, יהיה צורך לשמור את מסמך המקור. יחד עם זאת, כלל הראיה הטובה ביותר כורסם במהלך השנים על ידי בתי המשפט, כך שבפועל במרבית המקרים הצדדים להליך לא עומדים על הגשת המקור. לכן, המציאות מלמדת שבדרך כלל שמירת מסמכי מקור עבור התדיינויות משפטיות לא תידרש בחיי המעשה, בסופו של יום, לצורך ניהול הליכים משפטיים.[39]

לעניין דרישת המקור במסמך **שנוצר בעולם הדיגיטלי**, מתעוררת שאלה נוספת, והיא מהו המקור. לגבי מסמכים ממוחשבים רבים, ה"מקור" הוא סיביות מחשב שלא ניתן לתופסן בחושים. רק "פלט" של המקור (למשל, הדפסת המסמך במדפסת או הצגתו על גבי מסך מחשב באמצעות תוכנה המעבדת את קובץ המחשב ומקרינה אותו) ניתן לקריאה ולפענוח על-ידי בני אדם. על פניו, הפלט הינו העתק המסמך ולא המקור, אך מאחר שהמקור לא ניתן לתפיסה בחושים, נראה שהשימוש במונח "מקור" עלול שלא להתאים לעולם הדיגיטלי.

כמו כן, בהיבט של מהימנות המסמך, נראה שמסמך ממוחשב "מקורי" (ככל שניתן לזהות אותו) אינו עולה ברמתו על "העתק" ממוחשב, מבחינת התוכן שלו. כך, על פי רוב, כשקובץ מחשב משוכפל לשני קבצים, תוכנו יהיה זהה בשניהם. לעומת זאת, מידע אודות המסמך (מטא דאטה), כמו שעת שמירתו או מועד פתיחתו האחרון, עלול "להיאבד" בהליך העתקה מסוגים מסוימים.

על כן, צורך של שמירת ה"מקור" עשוי לא להיות רלוונטי בעולם הדיגיטלי בשל ההיטשטשות בין מקור להעתקו. בנוסף, בכל הנוגע לתוכן המסמך הדיגיטלי, ככלל, אין עדיפות למקור של קובץ על פני העתקו.

> ☜ **לנוכח הפיחות שחל במעמדם של מסמכי מקור ולאור הטשטוש הקיים בין מסמכי מקור להעתקיהם בעולם הדיגיטלי, במקרים רבים אין עוד עדיפות לשמירת המקור על פני שמירת העתקו.**

2.2 שקילת חלופות לדרישת מסמך מקורי נוכח הפיחות במעמדו

---

[39] יצוין, כי בשנת 2017 פורסם על ידי משרד המשפטים תזכיר חוק לתיקון פקודת הראיות (מקור והעתק כראיה), התשע"ח-2017, שבו מוצע לבטל את כלל הראיה הטובה ביותר.

אחת מתכליותיה המסורתיות של דרישת מסמך מקורי היא הבטחת רמת מהימנות גבוהה של המסמך. נוכח הפיחות במעמדם של מסמכי מקור והטשטוש בין מקורות להעתקיהם, כפי שפורט לעיל, **נראה שבדרך כלל תהיינה דרכים אחרות טובות יותר להבטחת רמת מהימנות גבוהה של מסמך**.

על כן, יש להטיל ספק בצורך במסמך מקורי **ולהעדיף שמירה על מהימנות בדרכים אחרות**. זאת, בהתאם לכלל התאמת התכליות (ראו סעיף 1 "התאמת ההסדר לתכליותיו" בפרק ב' לחלק א' שלעיל).

דוגמה לדרך אחרת לשמירה על מהימנות מסמך מופיעה בהליך שנקבע בתקנות העדות (העתקים צילומיים), התש"ל-1969. תקנות אלה קובעות תהליכים שיש לבצע בעת סריקת מסמכים, אשר עמידה בהם תקנה למסמך הסרוק מעמד של ראיה לכאורה בהליכים משפטיים (ראו סעיף 3א לתקנות). תהליכים אלה מגבירים את מהימנות המסמך.

דרך נוספת להגשמת תכלית המהימנות היא החלפת דרישת מהימנות **המסמך** בדרישת מהימנות **המידע**, שמצוי במסמך. בדרך זו, מתייתר למעשה הצורך בשמירה על מהימנות המסמך עצמו.

כך, למשל, בקשה לקבלת רישיון תיווך במקרקעין כוללת מידע אודות המבקש כמו פרטיו האישיים, האם הוא פושט רגל, האם יש לו רישום פלילי וכד' (ראו ת' 11(א) לתקנות המתווכים במקרקעין, התשנ"ז-1997). נכונותם של פרטים אלה יכולה להיבדק בדרכים שונות מבלי להסתמך על טופס הבקשה (לדוגמה, פרטי המתווך מאומתים מול רשות האוכלוסין, השאלה אם הוא פושט רגל נבדקת מול האפוטרופוס והרישום הפלילי נבדק מול המשטרה). קבלת המידע ממקורות מהימנים אחרים, ככל שאלה מתאפשרים לפי הדין, מחליפה את הצורך במהימנות מסמך הבקשה, כך שאין צורך לדרוש את הגשת מסמך הבקשה המקורי.

דוגמה נוספת לכך היא מקרה, שבו מסמך הדרוש לשם קבלת שירות, אף אם נחתם באופן ידני, מקורו במסמך שהופק במחשב על ידי גוף ציבורי. במקרה כזה, ניתן לרוב לקבל את המידע המצוי במסמך ישירות מהגוף הציבורי שהפיק אותו, ולא באמצעות דרישה לקבל מסמך מקור מהפונה לקבל שירות. הסדר כאמור לא רק שאינו פוגע במהימנות המידע המתקבל, אלא הוא אף מגביר אותה, וזאת תוך הקלת הנטל הבירוקרטי על הציבור.[40]

☜**בשל הפיחות במעמדם של מסמכי מקור, יש לשקול חלופות אחרות להגשמת תכליותיה המסורתיות של דרישת המקור.**

2.3 פרשנות דין קיים בקשר למסמך "מקורי"

[40] לעניין זה ראו החלטת ממשלה 1933 מיום 30.8.2016 בדבר שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור (להלן: "החלטת ממשלה 1933").

פרשנות הדין בנוגע לדרישת מקור (למשל, דין שמסדיר הגשת מסמכים לרשויות או לגופים אחרים) תתבצע לפי כלל התאמת התכליות שפורט בסעיף 1 שעניינו כלל "התאמת ההסדר לתכליותיו" בפרק ב' לעיל, ובשים לב לפיחות במעמדו של המקור, שתואר לעיל. יובהר, כי דרישת מקור בחיקוק לא מונעת שימוש במסמך דיגיטלי. יישום הדרישה לגבי מסמך דיגיטלי נעשה על ידי הגשמת תכליות דרישת המקור במסגרת ההסדר הדיגיטלי.

כך, למשל, כשנדרשת הגשה של מסמך מקור לרשות מינהלית, ניתן לקיים דרישה זו גם באמצעות הגשת העתק סרוק, ובלבד שבהגשת ההעתק הסרוק, ביחד עם הנסיבות האחרות, מתקיימות אותן התכליות שלשמן נדרשה הגשה של מסמך המקור ברמת ודאות מספקת. לדוגמה, כשעל פי הדין, יש להגיש לרשות מינהלית שובר מקורי של תשלום אגרה, ניתן להסתפק בקבלת העתק סרוק של השובר בנסיבות שבהן נבדק ביצוע התשלום ישירות עם הגורם שקיבל את התשלום[41]. זאת, מפני שבדיקה זו מגשימה את תכלית דרישת המקור – וידוא התשלום בפועל.

יובהר, כי מאחר שמושג ה"מקור" מיטשטש בעולם הדיגיטלי, כפי שהוסבר בסעיף 2.1, במקרה שבו הדין כולל דרישת מסמך מקור, **והמסמך נוצר באופן דיגיטלי, ניתן לראות במסמך הדיגיטלי כמקיים את דרישת המקור**.

יצוין, כי במקרים שבהם קיימת דרישת חתימה על מסמך, אין משמעותה של דרישה זו כי המסמך החתום צריך להישמר במקור. שכן, תכליות דרישת החתימה ותכליות דרישת המקור הן תכליות שונות (אף שלפעמים תיתכן חפיפה ביניהן). על כן, בעת הפעלת כללי הפרשנות בקשר למסמך שקיימת לגביו דרישת חתימה, **יש להפריד בין דרישת החתימה ודרישת המקור, ולנתח כל אחת מהדרישות בנפרד, בהתאם לתכליותיה**.

עוד יצוין, כי כשדרישת המקור **אינה מעוגנת בדין**, אלא מבוססת על נוהג, שאלת הפרשנות אינה רלוונטית. החלטת רשות, שאליה אמור להיות מועבר מסמך, האם לדרוש מסמך מקור תתבצע בהתאם לתכליות, לפי כללי הנחיה זו.

☜**פרשנות חיקוק בנוגע לדרישת מסמך מקור תתבצע לפי כלל התאמת התכליות, ובשים לב לפיחות שחל במעמד המקור.**

41 יצוין, כי על פי המדיניות, שאומצה על ידי הממשלה, של קבלת מידע מהציבור פעם אחת בלבד, רצוי לבטל את דרישת הגשת שובר התשלום, ולהסתפק בבדיקה עצמאית של הרשות המינהלית לגבי ביצועו של התשלום. ראו החלטת ממשלה 1933, שאימצה מדיניות זו.

3. חלופות לחתימה: יישום כלל התאמת התכליות באמצעות "שירותי אמון"

חתימה על גבי נייר מתבצעת במרבית המקרים באופן דומה: על ידי שרבוט של אותיות או צורות הקשורות לשם החותם באמצעות כלי כתיבה על גבי נייר. כלומר, בעולם הנייר, נעשה שימוש בעיקר בסוג אחד של חתימה.

בסוג זה של חתימה נעשה שימוש להגשמת מספר מטרות מרכזיות. ראשית, החתימה יכולה להעיד על זהות החותם בזכות צורתה הגרפית, שבדרך כלל ייחודית לחותם. שנית, חתימה עשויה לסייע בבדיקת גמירת דעתו של החותם, כלומר כוונה כלשהי ביחס למסמך הנחתם, כמו, לדוגמה, הסכמה, כוונה להתחייב ומודעות. סוג גמירת הדעת תלוי באופי המסמך הנחתם, בנסיבות החתימה ובמוסכמות חברתיות. למשל, גמירת דעת בנוגע לחוזה בדרך כלל תהיה כוונה להתקשר בחוזה עם צד מסוים, וחתימה תעיד על כוונה זו[42]. שלישית, באפשרות החתימה להעיד על שלמות המסמך הנחתם. כך, למשל, ישנם הסכמים שנהוג לחתום עליהם בתחתית כל עמוד, וכך ניתן להבטיח שלא הוסף עמוד שלא הוסכם עליו בין הצדדים החתומים על ההסכם.

במקרים רבים, דברי חקיקה והנחיות מינהליות, ובמיוחד כאלה שנוצרו לפני העידן הטכנולוגי או בחיתוליו, לא הפרידו בין תכליות החתימה השונות וקבעו דרישת חתימה כברירת מחדל לצורך הגשמת כל תכלית. כך, למשל, ישנם חיקוקים הכוללים דרישת חתימה על מנת להגשים תכלית של הזדהות, מבלי שיש צורך בקיום תכלית של שלמות המסמך הנחתם או בקיום תכליות אחרות כלל.

בשונה מהאפשרויות המצומצמות הקיימות בעולם החתימות על גבי נייר, בעולם הדיגיטלי ישנם סוגים רבים יותר של חתימות, ולצידם קיימים שירותים נוספים, שמספקים רמות שונות של אמון בפעולות דיגיטליות שונות. נהוג לכנות שירותים אלה "שירותי אמון"[43]. מגוון שירותי האמון, ובכללם סוגי החתימות האלקטרוניות, מאפשר ליצור התאמה מדויקת יותר בין האמצעי שנעשה בו שימוש לבין מטרותיו. במסמך עזר 2 בחלק ג' שלהלן יובא הסבר על מספר שירותי אמון: חתימה אלקטרונית, חותם אלקטרוני, זיהוי אלקטרוני, חותמת זמן אלקטרונית, שירותי דואר אלקטרוני רשום ושירותי אימות אתר אינטרנט. לגבי שירותי אמון שלא מוסדרים בדין הישראלי, תתואר במסמך עזר 1 - לשם הרחבת היריעה- ההסדרה האירופאית הקיימת בתחום.

---

[42] ג' שלו, **דיני חוזים - החלק הכללי** (תשס"ה), עמוד 136 (להלן: "**ג' שלו**").

[43] שירות אמון הוא שירות אלקטרוני שכולל, בדרך כלל יצירה, אימות ותיקוף של חתימות אלקטרוניות, חותם אלקטרוני או חותמת זמן אלקטרונית, שירותי משלוחים אלקטרוניים רשומים ותעודות הקשורות לשירותים אלה או יצירה, אימות ותיקוף של תעודות עבור אתרי אימות (ראו הרחבה בסעיף 3(16) לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון.

בעת גיבוש הסדר דיגיטלי, על משרד ממשלתי לקחת בחשבון את כלל שירותי האמון הזמינים לו ולבחור בשירות המתאים ביותר לתכליות ההסדר.

☜**לנוכח קיומם של שירותי אמון מגוונים בעולם הדיגיטלי, יש לבחון – לצד השימוש בחתימות אלקטרוניות או במקומן – גם שימוש בשירותי אמון אחרים על מנת ליצור התאמה מדויקת יותר בין האמצעי שנעשה בו שימוש לבין מטרותיו. על כן, אין מקום לבחור כברירת מחדל שימוש בחתימה דווקא.**

4. דרישת חתימה בחיקוק – יישום כללי ההנחיה והוראת סעיף 2 לחוק חתימה אלקטרונית

סעיף 2 לחוק חתימה אלקטרונית קובע הוראות לגבי החתימה האלקטרונית, שיש לעשות בה שימוש, כשקיימת דרישת חתימה לפי חיקוק. דרישת החתימה יכולה להופיע בחיקוקים באופנים שונים כמו, למשל, כשחיקוק עושה שימוש במילה "חתימה" על הטיותיה השונות, במילים "חתימת יד"[44] או אף כשמצוינת בחיקוק המילה "חתימה" בתחתית טופס שיש למלא. לגבי כל דרישה כזו, על החתימה לעמוד בהוראות סעיף 2 לחוק חתימה אלקטרונית.

יצוין, כי ההוראה הקבועה בסעיף 2 לחוק חתימה אלקטרונית תואמת את כללי ההנחיה וחופפת להם. על כן, בחינה לפי שלבי העבודה המומלצים בהנחיה, תוך הפעלת כלליה בצורה נכונה, תבטיח גם עמידה בהוראות סעיף 2.

סעיף 2(א) לחוק חתימה אלקטרונית קובע כלל גמיש, ולפיו ניתן לקיים דרישת חתימה לפי חיקוק על מסר אלקטרוני (כלומר, מסמך אלקטרוני) באמצעות אחת משתי החלופות הבאות. **החלופה הראשונה** היא חתימה אלקטרונית מאושרת. חתימה זו מקיימת את תכליות החתימה הקלאסיות ברמת ודאות גבוהה. היא מבטיחה את זהות החותם על ידי אימות זהותו בידי גורם שלישי מפוקח (גורם מאשר) וכן מבטיחה כי יהיה ניתן לזהות שינוי במסמך (המסר האלקטרוני) לאחר החתימה עליו.

החלופה השנייה היא חתימה אלקטרונית אחרת, ובלבד שמתקיימות, ברמת ודאות מספקת בנסיבות העניין, התכליות לדרישת החתימה בהתאם לאותו חיקוק (להלן: "מבחן קיום התכליות ברמת ודאות מספקת").

---

[44] יובהר, כי קיום דרישת החתימה באמצעות חתימה אלקטרונית, בהתאם להוראות סעיף 2, עשוי להיות אפשרי גם לגבי חיקוקים שנעשה בהם שימוש במונח "**חתימת יד**" על הטיותיו השונות. כפי שתואר בפרק שעוסק בפרשנות דין קיים (ראו פרק ג' בעמוד 25), במקרים שבהם תיתכנה פרשנויות שונות של הדין, אשר אחת מהן מאפשרת את קיומו של ההסדר הדיגיטלי המתבקש, השאלה האם ניתן לבחור בפרשנות זו תיגזר מתכליות הדין. אם תכליותיו עולות בקנה אחד עם ההסדר הדיגיטלי, אזי ניתן לקיים את ההסדר הדיגיטלי במסגרת הדין החל. במקרה שבו נעשה שימוש במונח "חתימת יד", תיתכנה שתי פרשנויות: האחת היא כי החתימה חייבת להתבצע באופן פיסי, ב"יד" החותם, והשנייה כי היא יכולה להתבצע ביד החותם גם באופן דיגיטלי. בחירה בין הפרשנויות האפשריות תתבצע לפי תכלית דרישת חתימת היד בחיקוק.

כלומר, שיקול הדעת לפי כלל זה מסור לחותם או לגורם שבאפשרותו לקבוע מהו אופן החתימה שבו ייעשה שימוש, בכפוף לקיום תנאי הסעיף. להרחבה על הגורם שמסור לו שיקול הדעת לבחור בין סוגי החתימות כשנדרשת חתימה בחיקוק ראו במסמך עזר 2 בחלק ג׳.

להלן יוסבר כיצד מפעילים את מבחן קיום התכליות ברמת ודאות מספקת, שהינו תנאי לשימוש ב״חתימה אלקטרונית אחרת״ לפי החלופה השנייה שהוזכרה לעיל. יובהר, כי ההסבר שלהלן לעניין אופן הפעלת מבחני סעיף 2 מתאים - מבחינה מהותית - גם למקרה, שבו לאחר הפעלת כללי ההנחיה, נבחר שימוש בכלי החתימה, אף אם לא נדרשת חתימה בחיקוק.

המונח ״חתימה אלקטרונית״ מוגדר בחוק כמידע או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני. כלומר, מדובר במונח רחב מאוד, אשר כולל חתימות מסוגים רבים, החל בהקלדה של שם החותם בתחתית מסמך WORD או בסימון תיבת ״אני מאשר״ על גבי טופס מקוון, עבור לחתימה גרפית על גבי פד דיגיטלי או בחתימה גרפית סרוקה וכלה בחתימה באמצעות ״כרטיס חכם״. כלומר, ״חתימה אלקטרונית אחרת״, המצוינת בחלופה השנייה, כוללת למעשה כל סוג שהוא של חתימה אלקטרונית, ובלבד שמתקיים התנאי הבא: ״**מתקיימות, ברמת ודאות מספקת בנסיבות העניין, התכליות לדרישת החתימה בהתאם לאותו חיקוק**״.

על מנת לבחון כיצד ניתן לקיים תנאי זה, תחילה יש לזהות מהן **תכליות** החתימה באותו חיקוק שבו החתימה נדרשת. לאחר מכן, יש לבדוק מהי **רמת הוודאות** הנדרשת בנסיבות העניין, ולבסוף **להתאים** את סוג החתימה שייבחר לרמת הוודאות הנדרשת. זאת, בדומה לשלבי העבודה המומלצים, המופיעים בהנחיה זו.

<u>תכליות</u>

זיהוי התכליות לדרישת החתימה בחיקוק יתבצע לפי כללי הפרשנות הרגילים.

תכליות החתימה הנפוצות, כפי שהוזכרו בסעיף הקודם, הן –

1. **זיהוי החותם**. בעולם הפיסי, צורתה הגרפית של החתימה, כמו גם נתוניה הגרפולוגיים, הם אלה שעשויים להעיד בדרך כלל על זהות החותם, בעוד שבעולם הדיגיטלי, ישנן דרכים מגוונות ורבות יותר לזיהוי החותם.
2. **אי שינוי המסמך לאחר מועד החתימה**. בעולם הפיסי אופן הגשמתה מוכר לנו, למשל, בנוהג לחתום במקרים מסוימים בתחתית כל דף בראשי תיבות על מנת להבטיח שלא יוכנס למסמך דף נוסף שעליו לא הוסכם. הגשמת תכלית זו יכולה להתבצע בעולם הדיגיטלי בדרכים מגוונות.
3. **גמירת דעת של החותם**, כלומר כוונה כלשהי בנוגע למסמך החתום. תכלית זו היא תכלית משפטית, במובחן מהתכליות האחרות המוזכרות לעיל, שהן תכליות שמוגשמות בהתקיים תנאים טכנולוגיים בעולם הדיגיטלי או תנאים פיסיים בעולם הנייר. ככזו, היא עשויה להילמד מהחתימה, אך גם מנסיבות אחרות (למשל, ההסבר שניתן לחותם עובר לחתימה לגבי

המסמך שעליו הוא עומד לחתום או המוסכמות החברתיות המקובלות באותן נסיבות). כלומר, החתימה היא נסיבה אחת מבין נסיבות שונות שעשויות להעיד על גמירת דעת.

יצוין, כי ישנן תכליות נוספות לדרישות חתימה. כך, למשל, חתימת עורך דין על תצהיר עשויה להגשים, בין היתר, תכלית של אישור לפעולה שמבוצעת על ידי גורם אחר וחתימה על צוואה ע"י המצווה והעדים מייצגת גם הזדהות עם סוג של אירוע טקסי המאפיין עריכת מסמך זה.

רמת ודאות מספקת

לאחר זיהוי התכליות לדרישת החתימה בחיקוק, יש לעבור לבחינת רמת הוודאות שבה כל אחת מהתכליות צריכה להתקיים. רמת הוודאות תיקבע בהתאם לנסיבות העניין ועליה להיות מספקת.

הדרך לקביעה מהי רמת ודאות מספקת בקשר לכל תכלית היא **בחינה של הסיכונים**, שעלולים להתממש במקרה שבו תכליות דרישת החתימה בחיקוק לא תוגשמנה. במסגרת הבחינה, יש לזהות את הסיכונים בקשר לכל אחת מהתכליות שזוהו בשלב הקודם, ולבחון את ההשלכות של התממשותם, ככל שאכן יתממשו. כפי שפורט בכלל בדבר התאמת החשיפה לסיכונים, (ראו סעיף 3 "הערכת סיכונים והתאמת החשיפה להם לערך הנפגע ולעוצמתו" בפרק ב' לחלק א' שלעיל), ככלל, קיים מתאם חיובי בין הסיכון לבין התכלית, כך שככל שהסיכון גדול יותר, כך נדרשת הגשמת התכלית ברמת ודאות גבוהה יותר[45].

ניהול הסיכונים יבוצע בהתאם **לנסיבות העניין**. בין היתר, נסיבות העניין עשויות להיות מאפייניו של החותם, מאפייניו של המסתמך על החתימה, מאפייניי המסמך וסביבת העבודה שבה הוא מצוי[46], סוג מערכת היחסים של החותם והמסתמך, מידת ההיכרות שלהם והסכמות שהגיעו אליהן לגבי סוג החתימה.

התאמת סוג החתימה שייבחר לרמת הוודאות הנדרשת

לאחר זיהוי התכליות ורמת הוודאות שבה הן צריכות להתקיים בנסיבות העניין (כלומר, רמת הוודאות המספקת לקיום תכליות אלה), יש לפנות לבחינת אופן הגשמת התכליות. ניתן להגשים את התכליות כולן באמצעות החתימה האלקטרונית שתיבחר. לחלופין, ניתן לפצל בין התכליות, כך שחלקן תוגשמנה על ידי החתימה האלקטרונית וחלקן בדרך אחרת, במסגרת התהליך הקשור לחתימה. במילים אחרות, **אין הכרח לקיים את כל תכליות דרישת החתימה באמצעות החתימה דווקא.**

[45] יובהר, כי המונח "ברמת ודאות מספקת" לא מכוון לוודאות מוחלטת, אלא לרמת ודאות סבירה בנסיבות העניין בנוגע לחתימה האלקטרונית שנבחרה, שהרי ככלל לא קיים מצב של וודאות מוחלטת.

[46] הסיכונים בקשר לשינוי או זיוף של מסמך, שמנוהל אך ורק ברשת המשרדית, הם על פי רוב קטנים יותר מהסיכונים הקשורים למסמך שעובר על גבי רשת האינטרנט.

כך, למשל, נניח שלחיקוק מסוים שלוש תכליות: זיהוי החותם, הֶעָדָה על גמירת דעתו בנוגע למסמך החתום והבטחה כי המסמך שעליו חתם לא השתנה לאחר מועד החתימה. ניתן להגשים תכליות אלה, כך שרק חלקן תוגשמנה על ידי החתימה האלקטרונית עצמה. לדוגמה, תכלית הזיהוי תוגשם על ידי שימוש בשירות זיהוי דיגיטלי, שבמסגרתו החותם מקיש, למשל, קוד שידוע רק לו בעת כניסה לאזור אישי באתר אינטרנט ייעודי; תכלית הֶעָדָה על גמירת דעת החותם תוגשם על ידי סימון בתיבה, שמעליה מופיע מלל שמבהיר מהי משמעות ביצוע פעולת החתימה (הלחיצה על תיבת הסימון היא למעשה החתימה האלקטרונית, אשר מהווה סימן אלקטרוני שהוצמד למסר אלקטרוני); תכלית אי שינוי המסמך לאחר החתימה תוגשם על ידי "נעילת" המסמך מפני שינויים על ידי היישום הייעודי, שבו נעשה שימוש, באמצעים טכנולוגיים המבטיחים כי המסמך "ננעל".

דוגמה נוספת לשילוב הגשמת התכליות על ידי החתימה עצמה ובדרך אחרת היא **השילוב שבין העולם הפיסי לעולם הדיגיטלי**. כך, למשל, במצב שבו אדם מגיע באופן פיסי לסניף של ספק שירות, הזיהוי יכול להתבצע בעולם הפיסי על ידי פקיד ספק השירות (לדוגמה, השוואת פניו של האדם לתמונה שבתעודה המזהה שלו), והכלים הדיגיטליים (ובהם החתימה האלקטרונית) יוכלו להגשים את יתר התכליות הנוגעות לעניין (למשל, חתימה אלקטרונית על גבי פד דיגיטלי תוכל לסייע בהֶעָדָה על גמירת דעתו של החותם, ותוכנה, שמקיימת דרישות טכנולוגיות מסוימות, תוכל להגשים את תכלית נעילת המסמך מפני שינויים, לאחר ביצוע פעולת החתימה).

מבין החתימות האלקטרוניות אשר מקיימות את התכליות ברמת ודאות מספקת, יש לבחור בחתימה אלקטרונית, שהשימוש בה הוא **ישים** בנסיבות העניין, בהתאם לסעיף 2 "יעילות, פשטות וישימות ההסדר" בפרק ב' שלעיל. כך, למשל, שימוש ב"כרטיס חכם" על מנת לצרוך שירות שניתן לכלל האזרחים, עלול להיות לא ישים, שכן נכון למועד כתיבת שורות אלה, חלק גדול מהאזרחים לא מחזיק בכרטיסים חכמים. כמו כן, יש להבטיח כי במקרה שבו סוג החתימה הנבחר מטיל נטל על החותם, **נטל זה הינו סביר** בנסיבות עניין, בהתאם לסעיף 6 "בחינת הנטלים, שבהם יכול לעמוד כל גורם המושפע מההסדר" בחלק ב' שלהלן.

חלק ב' – יישום ההוראות המנחות:

הליך בחינה מומלץ לגיבוש הסדר דיגיטלי

בפרק זה ייתן הסבר כיצד ליישם את העקרונות והכללים שהובאו בפרקים הקודמים ותינתנה דוגמאות לעניין אופן הטמעתם בעת גיבוש הסדרים דיגיטליים. להלן יתואר תהליך העבודה מוצע לגיבוש הסדר דיגיטלי.

הפעלת שיקול דעת תקין של הרשות המינהלית על פי הליך הבחינה המומלץ, המפורט להלן, יש בו כדי להעיד על כך, שההסדר הדיגיטלי תואם את כללי ההנחיה. זאת, בין היתר, נוכח קיומה של חזקת התקינות המינהלית.

1. זיהוי מטרתו הכללית של ההסדר הדיגיטלי

בשלב הראשון, מוצע לבחון את מטרתו הכללית של ההסדר הדיגיטלי. הבחינה בשלבים הבאים תתבצע לאורה של מטרה זו. כמו כן, זיהוי המטרה הכללית של ההסדר יסייע בהפעלת עקרון השקילות הפונקציונלית וכלל התאמת ההסדר לתכליותיו (וראו בהתאמה סעיף 1 "שקילות פונקציונלית" לפרק א' וסעיף 1 "התאמת ההסדר לתכליותיו" לפרק ב' לחלק א' שלעיל).

להסדר דיגיטלי יכולות להיות מטרות מגוונות. כך למשל -

- אחת מהמטרות הנפוצות של הסדרים דיגיטליים, שעוסקים ביחסי רשות-אזרח, היא **שיפור השירות לציבור**. שיפור השירות יכול להתבצע במגוון דרכים. למשל, ההסדר הדיגיטלי עשוי לשפר את **הנגשת השירותים** והזכויות לאזרחים.[47] כמו כן, ההסדר הדיגיטלי יכול לסייע **בהפחתת הביורוקרטיה** הודות ליכולת של העולם הדיגיטלי להפיץ מידע באופן יעיל ומהימן.[48]
- בנוסף, הסדר דיגיטלי יכול להביא **לחיסכון בעלויות** שונות כמו למשל עלויות של טיפול במסמכים פיסיים ושמירתם והחזקת שטחי אחסון (ארכיבים).

---

[47] כך, למשל, שירותים מקוונים יכולים לאפשר לאזרחים שמתגוררים באזורי פריפריה לעשות שימוש בשירות מהבית ובכך לחסוך מהם את הצורך לנסוע לסניפים המרוחקים מבתיהם.

[48] כך, למשל, הליך דיגיטלי יכול לחסוך לציבור את הצורך להעביר מסמך אחד למספר גופים בשלבים שונים של התהליך. לדוגמה, צו ירושה, שעניינו בזכות בנכס במקרקעין של מוריש, הניתן באופן דיגיטלי, יכול להישלח ישירות לאגף רישום והסדר מקרקעין, לצורך רישום הבעלות בפנקסי המרשם (טאבו). הפחתת הנטל הביורוקרטי יכולה לבוא לידי ביטוי גם בייתור הצורך להגיע פיסית למשרדי הרשות על מנת לבצע פעולה מול פקיד הרשות. ניתן למצוא דוגמה נוספת בתחום העסקים במגזר הפרטי. כך, למשל, פתיחה מקוונת של תיקים של חברות ועמותות ברשות התאגידים, ברשות המסים ובמוסד לביטוח הלאומי, יכולה לייתר את הצורך של העסק המבקש להתייצב במשרדי כל אחד מהגורמים. ראו פירוט בהחלטת ממשלה מספר 1855 מיום 11.8.2016 בעניין שיפור אופן עשיית עסקים בישראל https://www.gov.il/he/Departments/policies/2016_dec1855 .

- מטרה נוספת של הסדרים דיגיטליים היא **הגברת היעילות**. הגברת היעילות יכולה להביא לחסכון בעלויות כספיות (כגון חיסכון בשטחי אחסון) וכן להביא לביצוע טוב יותר של תפקידי הרשות. כך, למשל, מחשוב דיווחים עשוי להעלות את רמת האכיפה של רשות מינהלית על ידי הצלבה ממוחשבת ואוטומטית של נתונים, הדרושים לה לשם ביצוע פעולות אכיפה. הגברת היעילות יכולה להתבצע במספר דרכים. **ראשית**, על ידי הפחתת הטעויות שעלולות להיגרם[49]. **שנית**, הגברת היעילות יכולה להתבצע בזכות **המיידיות שבהעברת מידע** באופן דיגיטלי[50].
- זאת ועוד, הסדר דיגיטלי יכול לשרת מטרה של קידום **מדיניות ירוקה** על ידי הפחתת הניירות הפיסיים שמודפסים ונשמרים.
- מטרה נוספת של הסדר דיגיטלי עשויה להיות **הקטנת סיכונים והגברת הוודאות** ביחס להסדר הקיים. כך, למשל, זיהוי אלקטרוני יכול להגביר את הוודאות בזהות המזדהה.
- בנוסף, לפעמים הסדרים דיגיטליים מגובשים לצורך **עמידה בהתחייבויות בינ"ל**, כמו למשל, עמידה בסטנדרטים של ארגון ה-OECD.

בתום תהליך העבודה, יש לשוב למטרה הכללית שזוהתה בשלב הראשון ולוודא כי ההסדר המתגבש מגשים אותה.

<u>2. זיהוי תכליותיו של ההסדר הדיגיטלי על כל היבטיו</u>

בשלב השני, מוצע לזהות את תכליותיו של ההסדר הדיגיטלי על כל היבטיו. זיהוי התכליות נדרש על מנת להפעיל, בהמשך הבחינה, את עקרון השקילות פונקציונלית (סעיף 1 בפרק א' לחלק א') ואת כלל התאמת ההסדר לתכליותיו (סעיף 1 בפרק ב' לחלק א'). באופן זה, זיהוי התכלית יסייע בגיבוש הכלי שבאמצעותו תוגשם התכלית. להלן מספר דוגמאות של תכליות שונות שעשויות להתעורר.

- **הזדהות**:

  בהסדרים דיגיטליים רבים נדרש זיהויים של גורמים שונים המעורבים בהם. כך, למשל, הסדר שנועד לאפשר לאדם לעיין בנתונים אישיים על עצמו, המופיעים באתר אינטרנט של משרד ממשלתי או של גוף פיננסי, מצריך את זיהויו של האדם ואימות כי הוא אכן מי שהוא טוען שהוא. כשל בזיהוי עלול, לדוגמה, לפגוע בפרטיות האדם, ומכאן חשיבותו. ניתן להגשים את תכלית הזיהוי באמצעות כלים שונים כמו למשל שירות של זיהוי דיגיטלי מסוגים שונים ושירות של חתימה אלקטרונית. הסבר על שירותים אלה מופיע במסמך עזר 2 בחלק ג'.

---

[49] כך, למשל, מילוי של טופס דיגיטלי עשוי להפחית את הטעויות במילוי הטופס על ידי מתן חיווי אוטומטי במקרה של השמטת מילוי של שדה מסוים או במקרה של השלמת פרטים לא מתאימים (למשל, הזנת מספר טלפון בשדה של כתובת).

[50] כך, למשל, מערכת אינטרנט להודעות של הבורסה לניירות ערך (מאיה) מאפשרת, בין היתר, לקבל מידע באופן אלקטרוני על החברות וניירות הערך שנסחרים בבורסה באופן מהיר ומיידי.

יצוין, כי הזדהות יכולה להידרש ביחס לסוגים שונים של גורמים: בני אדם, תאגידים, אתרי אינטרנט, וכד׳.

- **גמירת דעת והֶעָדָה עליה**

ישנם הסדרים שבהם נדרשת גמירת דעת של גורם המעורב בהסדר והֶעָדָה עליה, כלומר הֶעָדָה על כוונה כלשהי מצדו ביחס לפעולה מסוימת שמתבצעת כמו הסכמה, כוונה[51] להתחייב, מודעות או הבנה[52]. יובהר, כי גמירת דעת נלמדת מנסיבות שונות, ועל כן יתכן שלצד שימוש בכלים שונים לצורך הֶעָדָה עליה, יידרש גם קיומן של נסיבות נוספות. כך, למשל, הסתייעות בכלי של חתימה על מנת להעיד על גמירת דעת, עשויה לחייב השלמה של נסיבות נוספות כדוגמת מתן הסבר לגורם שנדרשת הֶעָדָה על גמירת דעתו לפני ביצוע הפעולה על משמעויות הפעולה שהוא מתעתד לבצע. הסבר כאמור עשוי להיות, למשל, הסבר בכתב, הסבר מילולי מאת גורם מוסמך כמו פקיד של רשות מרשויות המדינה או מאת איש מקצוע[53].

- **יצירת הרתעה לפני ביצוע פעולה**

ישנם הסדרים, שבהם מעבר לצורך להבטיח את גמירת דעתו של גורם המעורב בהסדר בקשר לפעולה מסוימת, נדרשת גם יצירת הרתעה, על מנת להגביר את הסיכוי לכך שהפעולה תבוצע באופן מהימן. כך, למשל, בעולם הפיסי, דרך של מסירת מידע בפני דמות סמכותית כמו עורך דין במסגרת חתימה על תצהיר או בפני גורם מוסמך ברשות מינהלית במסגרת התייצבות במקום מושבה של הרשות המינהלית, עשויה להרתיע את מוסר המידע מלמסור מידע שקרי. בעולם הדיגיטלי קיימים כלים אחרים שיכולים לספק הרתעה דומה במקרים רבים. כך, למשל, הצגת הודעה ביישום דיגיטלי, הכוללת אזהרה באותיות גדולות ומודגשות, בטרם ביצוע פעולה של מסירת מידע, עשויה לספק הרתעה מספקת בנסיבות מסוימות.

- **תיעוד זמן ביצוע פעולה והֶעָדָה עליו**

ישנם הסדרים שבהם יש חשיבות למועד המדויק שבו ביצע אחד הגורמים הקשורים להסדר פעולה מסוימת. כך, למשל, עשויה להיות חשיבות לעובדה שמסמך מסוים היה קיים בנקודת זמן מסוימת (תאריך ושעה) ושהוא לא שונה מאז אותה נקודת זמן (למשל, חוזה או צוואה). ניתן להגשים את תכלית הֶעָדָה על זמן ביצוע פעולה ברמות ודאות שונות באמצעות כלים שונים כמו, למשל, שירות של חותמת זמן אלקטרונית, שירות של חתימה אלקטרונית או שירות של חותם אלקטרוני (הסבר על שירותים אלה מופיע בסעיף 1 לחלק ג׳ להלן), ״לוגים״ המתעדים פעילות מערכת או רישום תאריך על גבי מסמך. רמת הוודאות של ההעדה על ביצוע הזמן משתנה מכלי לכלי. כך, למשל, רישום תאריך על גבי מסמך יעיד על זמן כתיבתו ברמת

---

[51] כך, למשל, גמירת דעת בנוגע לחוזה בדרך כלל תהיה כוונה להתקשר בחוזה עם צד מסוים (ראו ג׳ שלו, עמוד 136).

[52] כך, למשל, ישנה חשיבות רבה להבנה במסגרת מתן עדות של חשוד במשטרה.

[53] למשל, מתן הסבר על ידי עורך דין במסגרת ייעוץ משפטי; רופא במסגרת החתמה על טופס הנחיות רפואיות מקדימות לטיפול רפואי עתידי בחולה הנוטה למות לפי חוק החולה הנוטה למות, התשס״ו-2005.

ודאות נמוכה, בעוד שציון מסמך באמצעות חותמת זמן דיגיטלית שמבוססת על מקור זמן חיצוני, יעיד על זמן כתיבתו ברמת ודאות גבוהה.

- **הגנה על מסמך מפני שינויים, יכולת לזהות האם מסמך או נתון שונה ממועד מסוים והֶעָדָה על שינויו או אי שינויו (ככל שקיים מסמך בהסדר המתגבש)**

היכולת לזהות שתוכנו של מסמך או נתון לא שונה החל ממועד מסוים ולהעיד על כך ניתנת למימוש באמצעות כלים מגוונים כמו חתימה אלקטרונית, חותם אלקטרוני, חותמת זמן אלקטרונית (הסבר על שירותים אלה מופיע בסעיף 1 לחלק ג׳ להלן) או מערכת מאובטחת לניהול מידע (לגבי מאגר נתונים).

- **מניעת התכחשות לפעולה שבוצעה**

מניעת התכחשות לפעולה שבוצעה חשובה במיוחד כשמדובר במימוש זכות או במילוי חובה חוקית. בשונה מהתכליות שפורטו לעיל, תכלית זו של מניעת התכחשות בדרך כלל ניתנת להגשמה אגב הגשמת תכליות אחרות. כך, למשל, ניתן למנוע התכחשות לפעולה שבוצעה או לצמצם את הסבירות שלה ככל הניתן על ידי הבטחת זהות מבצע הפעולה והבטחה כי הפעולה התקיימה ושלא נעשה שינוי במידע אודות הפעולה לאחר ביצוע הפעולה.

- **הגעת מסמך שנשלח ליעדו והֶעָדָה על כך שהוא הגיע ליעדו (ככל שקיים מסמך בהסדר המתגבש)**

בהסדרים רבים, שבהם מועבר מידע בין גורמים שונים, עשויה להיות חשיבות לכך, שהמידע, שנשלח משולח מזוהה, התקבל אצל נמען מזוהה וכי המידע הגיע שלם, מבלי שהייתה גישה אל המידע לגורם שאינו מורשה. כמו כן, עשויה להיות חשיבות ליכולת לתעד זאת מבחינה ראייתית. זאת, בין שמדובר בחילופי מידע בין רשות לאזרח ובין שמדובר בחילופי מידע בין אזרחים או גורמים אחרים. חשיבות דומה קיימת להֶעָדָה על זמן השליחה והקבלה.[54] ניתן להגשים תכליות אלה באמצעות שירותים דיגיטליים שונים (ראו הרחבה בסעיף 1 למסמך עזר 2 שבחלק ג׳ להלן "הסבר על "שירותי אמון" נפוצים").

- **שמירה על רמת מהימנות גבוהה של מידע**

תכלית נוספת שעשויה להתעורר בהסדרים שונים היא שמירה על רמת מהימנות גבוהה של מידע או מסמך (לדוגמה, כי מסמך אינו מזויף). כך, למשל, יכולה להיות חשיבות רבה למהימנות של מסמכים, שהם חלק מפעולות משפטיות בעלות רגישות גבוהה, מסמכים שאמורים לשמש ראיה חשובה לפרק זמן ארוך מאד או מסמכים שקשורים לפעולות חד פעמיות ולא שגרתיות.

---

[54] ניתן למצוא פירוט בעניין זה בהקשר של המשפט הפרטי בדו"ח מסחר אלקטרוני, בסעיף 3.1 לפרק השני, שעניינו במועד ומקום משלוח וקבלת מסמך אלקטרוני.

יצוין, כי בעבר שררה תפיסה שלפיה מסמך מקורי מגביר את מהימנותו של המסמך. מאז, חל פיחות במעמדו של המסמך המקורי, ונוספו דרכים להשגת מטרת המהימנות (ראו לעניין זה סעיף 2 "מקור והעתק דיגיטלי: הפעלת כללי ההנחיה על דרישת מסמכי מקור" בפרק ד' לחלק א' שלעיל). על כן, נראה שדרישת קבלת המסמך המקורי (או שדרישה כי המסמך המקורי יישמר) אינה הדרך הבלעדית, ואף לא הטובה ביותר, לשם השגת רמת מהימנות גבוהה שלו. ניתן, ואף רצוי, לעשות שימוש במגוון דרכים אחרות ליצירת רמת מהימנות גבוהה של מסמכים.

- **תיעוד על ביצוע פעולה**

ישנם הסדרים שבהם יש חשיבות לתיעוד פעולה שהתרחשה לצורך שמירת ראיות או מסיבות אחרות. למשל, תיעוד של הוצאת מסמך מארכיון על ידי אדם.

- **הבטחה כי מסמך יהיה קביל בבית המשפט (ככל שקיים מסמך בהסדר המתגבש)**

תכלית ראייתית שעשויה להתעורר בהסדרים שונים היא כי מסמכים שמוגשים לבית המשפט במקרה של התדיינות משפטית הקשורה אליהם יהיו קבילים. על פי "כלל הראיה הטובה ביותר", אשר מקורו במשפט המקובל, אין להוכיח את תוכנו של מסמך אלא בדרך של הצגת המקור בבית המשפט.[55]

לכן, על פניו, כשמסמך הקשור להסדר עשוי להיות מוגש לבית המשפט, לפעמים יהיה צורך לשמור את מסמך המקור. יחד עם זאת, כלל הראיה הטובה ביותר כורסם במהלך השנים על ידי בתי המשפט, כך שבפועל במרבית המקרים הצדדים להליך לא עומדים על הגשת המקור. לכן, חשיבות שמירת המקור ירדה. כמו כן, בעולם הדיגיטלי חל טשטוש בין מקור להעתק לגבי מסמכים שנוצרו באופן דיגיטלי, ועל כן תכלית ראייתית זו של שמירת ה"מקור" עשויה לא להיות רלוונטית בעולם הדיגיטלי בשל מאפייניו הייחודיים. ראו פירוט לעניין הטשטוש בין מקור להעתק במסמכים שנוצרו באופן דיגיטלי בסעיף 2 "מקור והעתק דיגיטלי: הפעלת כללי ההנחיה על דרישת מסמכי מקור" בפרק ד' לחלק א' שלעיל.

- **אחזור מידע ושימוש חוזר בו – דרישת כתב**

תכלית שמתעוררת בהסדרים באופן תדיר הינה כי מידע יהיה ניתן לאחזור (שמירת המידע) ולשימוש חוזר בו בעתיד. תכלית זו בדרך כלל מוגשמת על ידי דרישת כתב, אשר יכול להיות גם אלקטרוני.

---

[55] כפי שצוין בה"ש קודמת, בשנת 2017 פורסם תזכיר חוק מטעם משרד המשפטים, שבו הוצע לבטל את כלל הראיה הטובה ביותר (ראו תזכיר לתיקון פקודת הראיות (מקור והעתק כראיה), התשע"ח-2017).

כך, למשל, האפשרות לשמור חוזה כתוב שנכרת בין צדדים ולקרוא בו בעתיד עשויה להידרש לצרכים ראייתיים; מסרים כתובים שמועברים אל צרכן במסגרת התקשרויות צרכניות לרוב יחייבו שימוש בכתב שניתן לקריאה חוזרת ולאחזור. זאת, על מנת להגן על הצרכן במערכת יחסים שמתאפיינת בפערי כוחות[56].

3. זיהוי הגורמים הנוגעים להסדר

יש לזהות את כלל הגורמים הנוגעים להסדר ואת מאפייניהם. כלומר, יש לשאול מיהם בעלי העניין בהסדר. להלן מספר דוגמאות.

- **המדינה על כלל יחידותיה.** המדינה מתאפיינת בחוסן כלכלי בהיותה הגוף הגדול במדינה, וכן ביכולת להפעיל סמכות שלטונית.
- **הציבור.** ניתן לחלק את הציבור לקבוצות בעלות מאפיינים משותפים, כמו למשל: הציבור הרחב; ציבור בעל מאפיינים משותפים (לדוגמה, חוסכים בקופות גמל); ציבור בשכבות גיל משותפות; ציבור מאותו חתך סוציואקונומי; ציבור המצוי במצב משותף (לדוגמה, הורים, נשים בהריון, משרתי מילואים).

  יצוין, כי הציבור הרחב כולל מגוון גדול של אנשים בעלי מאפיינים שונים. לכן, קשה לייחס לו מאפיינים ייחודיים. משכך, בדרך כלל יש להתחשב במכנה המשותף הרחב ביותר של הציבור, שהינו בדרך כלל המכנה המשותף הנמוך ביותר. כך, למשל, כשבוחנים, בשלבים הבאים את היכולת של "הציבור הרחב" לשאת בנטל מסוים, יש להתחשב במאפייניי החלקים בציבור שיכולתם לשאת בנטל תהיה הקטנה ביותר.
- **תאגידים פרטיים מפוקחים** ברמות פיקוח משתנות, כדוגמת בנקים, חברות ביטוח וחברות סלולר. רמת הפיקוח של גופים משתנה ממגזר למגזר. בדרך כלל, רמת הציות של הגופים, המפוקחים ברמת פיקוח גבוהה, לכללים החלים עליהם נוטה להיות גבוהה נוכח קיומה של מערכת יחסים מתמשכת ומשמעותית עם הגוף המאסדר (רגולטור) שלהם. תאגידים מפוקחים הם בדרך כלל שחקנים מתוחכמים ובעלי אמצעים כלכליים לרכוש טכנולוגיות מתקדמות.
- **אנשים פרטיים בעלי מקצועות מיוחדים** כמו רואי חשבון ועורכי דין. על חלק מבעלי מקצוע חלה חובת רישיון. חלק מהמקצועות כולל אוכלוסייה מתוחכמת.
- **נותני שירותים ועסקים** כדוגמת רשתות מזון. מידת חוסנם הכלכלי ויכולתם לעשות שימוש בטכנולוגיות מתקדמות משתנה בהתאם לגודל הגוף ולמאפייניו. בעניין זה, יש שוני משמעותי בין עסקים גדולים לעסקים קטנים.

[56] ראו הרחבה בעניין דרישת הכתב בחוזים צרכניים בדו"ח מסחר אלקטרוני בסעיף 3 לפרק 3.

- **רשויות ציבוריות, שאינן המדינה**, שמעניקות שירותים לציבור כמו רשויות מקומיות, תאגידי מים וביוב, המוסד לביטוח לאומי. חוסנן הכלכלי של רשויות אלה ויכולתן לעשות שימוש בטכנולוגיות מתקדמות משתנות מרשות לרשות.
- **גופים מהמגזר השלישי**. ישנה שונות גדולה בין גופים אלה בנוגע לחוסנם הכלכלי וליכולת שלהם לעשות שימוש בטכנולוגיות מתקדמות.

זיהוי הגורמים הנוגעים להסדר יסייע בשלב ניתוח סיכוני ההסדר, שבו נבחן את המשמעותיות של נשיאתו של כל גורם בסיכוני ההסדר. כמו כן, זיהויים יסייע גם בשלב בחינת הנטלים, שבו נבדוק באילו נטלים כל גורם הקשור להסדר יכול לעמוד.

4. בחינת סיכוני ההסדר:

בשלב זה, מוצע לבצע סקר סיכונים, שבמסגרתו ייבחנו סיכוני ההסדר, כמפורט להלן. בחינה זו נדרשת כדי להפעיל את כלל ממספר 3 להנחיה זו, שעניינו בהערכת הסיכונים והתאמתם לערך הנפגע ולעוצמתו (ראו סעיף 3 "הערכת סיכונים והתאמת החשיפה להם לערך הנפגע ולעוצמתו" בפרק ב' לחלק א' שלעיל).

שלב א' – זיהוי הסיכונים

סיכוני ההסדר יכולים להיות מגוונים. ניתן לזהות אותם על ידי מענה על השאלה: איזה סיכון עלול להתממש במקרה שתכלית מבין תכליות ההסדר לא תוגשם? כך, למשל, שימוש בחתימה אלקטרונית מסוג "חלש" עלול לאפשר התכחשות לחתימה; שימוש בהזדהות דיגיטלית ברמה נמוכה עלול להביא לטעות בזיהוי.

שלב ב' – זיהוי עוצמת הפגיעה במקרה של התממשות הסיכון ורמת ההסתברות להתממשות הסיכון

עוצמת הפגיעה במקרה של התממשות הסיכון עשויה להיות מושפעת ממספר גורמים, ובהם, בין היתר, הערך הנפגע והיקף הפגיעה.

לצד בחינת עוצמת הפגיעה, יש לבחון גם מהי ההסתברות לכך שהסיכון אכן יתממש, ככל שניתן להעריך זאת בשלב זה של הבדיקה. יצוין, כי יתכנו מקרים שבהם עוצמת הפגיעה עלולה להיות גדולה, אך ההסתברות להתרחשותה תהיה נמוכה.

להלן מספר דוגמאות לערכים מוגנים שעלולים להיפגע:

- **זכויות יסוד** כדוגמת הזכות לפרטיות, למשל כשמדובר במסמך המכיל מידע אישי; הזכות לכבוד, הזכות לחיים ולחופש התנועה, למשל במקרה של שיבוש הליכים פליליים או גביית הודעת חשוד באופן בלתי מהימן, ועוד. עוצמת הפגיעה במקרים אלה עשויה להשתנות ממקרה למקרה.
- **זכויות כלכליות או כספיות**. לדוגמה, במקרה שבו שליחת הודעה דיגיטלית נכשלת מסיבות טכנולוגיות, וכתוצאה מכך הנמען לא יודע על זכות כספית שהוא יכול לממש, עלול להיגרם לו נזק כלכלי בשל אי מימוש הזכות; במקרה של תשלום לרשות מרשויות המדינה בדרך מקוונת, שבמהלכו לא נשמר תיעוד אודות התשלום, המשלם עלול להימצא בהפסד אם לא יצליח להוכיח כי ביצע את התשלום (ככל שנטל ההוכחה מוטל עליו); במקרה של אי קבלת דרישת תשלום מקוונת, עלול להיגרם איחור בתשלום שיגרור ריביות או אף פתיחה בהליכי גביה מינהליים. עוצמת הפגיעה יכולה להשתנות ממקרה למקרה: יהיו מקרים שבהם השפעת התממשות הסיכון תהיה קטנה כמו למשל כשמשלם מצליח להוכיח כי ביצע את התשלום בפועל. במקרה כזה, הפגיעה בו תתמצה בחוסר נוחות, השקעת זמן ומשאבים לצורך ההוכחה, וכד׳. לעומתם, יהיו מקרים שבהם ההשפעה תהיה גדולה יותר כמו למשל במקרה שבו המשלם לא יצליח להוכיח כי ביצע את התשלום, ועל כן ייאלץ לשלם את אותו התשלום פעם נוספת.
- **אינטרסים ציבוריים** כדוגמת ביטחון המדינה. כך, למשל, במקרה שבו הסדר דיגיטלי כולל מסמכים מסווגים, בחירה בטכנולוגיה ״חלשה״ עלולה להביא לכך שהמסמכים יועברו לגורם לא מורשה, למשל עקב תקיפת סייבר. עוצמת הפגיעה במקרה כזה עלולה להיות גבוהה.

<u>שלב ג׳ – זיהוי מידת יכולתו של כל גורם לשאת בסיכוני ההסדר וזיהוי הכלים שעומדים לרשותו לשם הקטנת הסיכונים</u>

בהמשך לזיהוי הגורמים הנוגעים להסדר, יש לבדוק - ביחס לכל גורם כאמור - מהי מידת יכולתו לשאת בסיכון ולפזר אותו וכן מהם הכלים שעומדים לרשותו להקטנת הסיכון האפשרי.

היכולת לשאת בסיכוניו של ההסדר או להקטינם נגזרת ממספר מאפיינים, ובהם, בין היתר, חוסן כלכלי, נגישות לאמצעים דיגיטליים ובקיאות בשימוש בהם, יכולת לעשות שימוש בטכנולוגיות מתקדמות.

כך, למשל-

- גורמים מתוחכמים או בעלי ממון יכולים בדרך כלל להשתמש בטכנולוגיות שונות. למשל, גורמי מקצוע מבצעים דיווחים לרשות לניירות ערך (מגנ״א) או לרשות המיסים באמצעות כרטיס חכם. לעומת זאת, הציבור הרחב בדרך כלל אינו יכול להשתמש באמצעים טכנולוגיים שהפעלתם מחייבת הבנה, השקעת זמן או כסף (כמו למשל רכישת כרטיס חכם). הציבור

הרחב יכול לעשות שימוש באמצעים העומדים לרשותו כמו, למשל, בתעודת הזהות החכמה[57], בהזדהות באתרים ממשלתיים באמצעות שאלות זיהוי והוכחת זהותו על ידי ביצוע עסקה בכרטיס האשראי שלו, ועוד (שימוש כזה נעשה, למשל, בפרויקט "הר הכסף" של משרד האוצר).

- למדינה בדרך כלל יש אפשרות לעצב את ההסדר. כפי שצוין לעיל, היא נהנית גם מיכולת כלכלית משמעותית, המאפשרת לה לשאת בסיכונים שונים.
- גופים שנותנים שירות לציבור רחב יכולים לפזר את הסיכון על מספר רב של אנשים כמו, למשל, בנקים או יחידות מיחידות המדינה.
- גורמים שמחזיקים ב"שירות אמון" כמו אמצעי חתימה או הזדהות יכולים להקטין את הסיכון על ידי שמירת האמצעי ואי העברתו לאחרים. זאת, ובלבד שהם מודעים לכך שעליהם לשמור את האמצעי ולא להעבירו לאחרים.

ראו פירוט בעניין דרכי השפעה על הסיכוי להתממשות סיכוני ההסדר ועל מידת חומרתם בסעיף 4 "הקטנת סיכוני ההסדר וחלוקת הנשיאה בהם במקרה של התממשותם", בפרק ב' לחלק א' שלעיל.

<u>5. ביצוע ניהול סיכונים: התאמת החשיפה לסיכונים לערך הנפגע ולעוצמת הפגיעה ובדיקה האם ניתן להקטינם</u>

בהתבסס על המאפיינים שזוהו בשלבים הקודמים, יש לפעול בהתאם לכלל ממספר 3 וכלל ממספר 4 להנחיה: יש להתאים את החשיפה לסיכונים לערך הנפגע ולעוצמת הפגיעה, ולהקטין אותם במידת הצורך או להסיט את הנשיאה בהם לגורם שהינו בעל היכולת הטובה יותר להקטין אותם (להסבר והרחבה, ראו סעיף 4 "בחינת סיכוני ההסדר" בפרק ב' לחלק א' שלעיל).

יצוין, כי לאחר בחינת הקטנת הסיכונים, יהיה צורך לבצע הערכת סיכונים פעם נוספת, בהתאם לנסיבות החדשות שתיווצרנה עם השינויים שיגובשו.

<u>6. בחינת הנטלים, שבהם יכול לעמוד כל גורם המושפע מההסדר:</u>

הסדרים דיגיטליים שונים עשויים להטיל מגוון נטלים על הגורמים המעורבים בהם. יש לבחון, בנוגע לכל גורם המעורב בהסדר, אשר זוהה בשלב 3, באילו נטלים כל גורם יכול לשאת במסגרת ההסדר ולהתאים אותם ליכולות אלה. זאת, בהתאם לכלל ממספר 1 להנחיה, הוגנות ההסדר בהתאמתו לאוכלוסייה שעליה הוא נועד לחול (ראו חלק א', פרק ב', סעיף 5 "הוגנות ההסדר בהתאמתו לאוכלוסייה שעליה הוא נועד לחול").

להלן שלבי עבודה מוצעים.

---

[57] יצוין, כי נכון לשנת 2019, טרם חולקו כל תעודות הזהות החכמות לציבור.

שלב א׳ – זיהוי הנטלים ומידת השפעתם על כל גורם

בחינה בנוגע לכל אחד מהגורמים המעורבים בהסדר, שזוהו בשלב 3, באילו נטלים הוא יכול לשאת, מבחינה מעשית, ומהי מידת השפעת הנטל עליו.

להלן מספר דוגמאות לנטלים. יצוין, כי תיתכן חפיפה בין הנטלים השונים.

- **נטל כלכלי** או רכושי. למשל, נטל כלכלי שנוצר בשל רכישת קורא כרטיסים, כרטיס חכם או תוכנת מחשב.
- **נטל טכנולוגי**. למשל, נטל שנוצר בשל הצורך בבקיאות בשימוש במחשב או בכלי דיגיטלי אחר.
- **נטל של השקעת זמן.** למשל, צורך להתייצב בסניף של נותן שירות לצורך רכישת תעודה אלקטרונית או לצורך הזדהות בפני פקיד. דרישות אלה עלולות לפגוע בנוחות הגורם המעורב בהסדר, באיכות השירות הניתן לו ואף להטיל עליו נטל כלכלי.
- **נטל ביורוקרטי**. למשל, צורך להזין נתונים באופן ידני לתוך ממשק ממוחשב. לנטל זה נוסף, במקרים רבים, גם נטל של השקעת זמן (הזנת נתונים במערכת ממוחשבת עשויה לקחת זמן ארוך יותר באופן משמעותי מהזמן שדרוש לשם מילוי טופס בנייר).

שלב ב׳ – התאמת הנטלים

לאחר ניתוח הנטלים שבהם כל גורם יכול לשאת מבחינה מעשית, יהיה ניתן לקבוע אילו נטלים ניתן להטיל עליו. זאת, בהתאם לישימות הטלת הנטל עליו ולהוגנות הטלת הנטל, כמפורט בכלל ממספר 1 להנחיה זו (ראו חלק א׳, פרק ב׳, סעיף 5 ״הוגנות ההסדר בהתאמתו לאוכלוסייה שעליה הוא נועד לחול״).

7. בחירה בין הכלים הקיימים להגשמת כל תכלית

לאחר איסוף הנתונים בשלבים הקודמים, יש לבחור בכלי המתאים למילוי כל אחד מתכליות ההסדר, כך שתהיה הלימה בין מרכיבי ההסדר והכלים שבשימוש בו לבין רמת הוודאות שבה יש להגשים כל תכלית. כלומר, בשלב זה תתבצע התאמת מרכיבי ההסדר לתכליותיו, כך שמרכביו יגשימו את תכליותיו ברמת ודאות מספקת. ניתן לחלק את הכלים הקיימים למילוי התכליות לשתי קבוצות: כלים טכנולוגיים (ראו כלים לדוגמה במסמך עזר 2 שבפרק ג׳, המתאר שירותי אמון שונים) וכלים נורמטיביים (למשל, קביעת כללי התנהגות, הסדרי אחריות[58], קביעת נורמות מפצות במקרה של אי עמידה בכללי התנהגות).

[58] למשל, ראו הסדר של סליקה אלקטרונית של שיקים שתואר בעמוד 15.

הבחירה בין הכלים השונים, בנוגע לכל תכלית, תתבצע בהתאם לכללים המפורטים בפרק ב' לחלק א' להנחיה זו, ובהם: יצירת הסדר הוגן, שנטליו מתואמים לאוכלוסייה הנוגעת לו; התאמת החשיפה לסיכוניו לערך הנפגע ולעוצמתו, הקטנתם וחלוקת הנשיאה בהם בהתאם לכללים.

יצוין, כי ככל שבהסדר הדיגיטלי עולה **תכלית של הזדהות**, בחירת הכלי המתאים להגשמת תכלית זו תתבצע בהתאם למדיניות הלאומית להזדהות בטוחה, אשר אומצה על ידי הממשלה[59] בשנת 2017. להרחבה ראו בסעיף 1.1 "זיהוי אלקטרוני" במסמך עזר 2 שבחלק ג'.

8. בחינת התאמת ההסדר לדין והצורך לעגנו בחקיקה

יש לבחון האם הדין הקיים מאפשר את קיומו של ההסדר הדיגיטלי, בהתאם לכללים המפורטים בסעיף 1 בפרק ג' לחלק א' שלעיל. במסגרת זו, יש לבחון האם ניתן להפעיל כללי פרשנות, כך שיאפשרו את קיומו של ההסדר. כמו כן, יש לוודא כי ההסדר עומד בדינים כלליים שעשויים לחול על כל הסדר דיגיטלי. כך, למשל, על הסדר שכרוך בעיבוד של מידע אישי, חלות ההוראות הנוגעות לעניין מחוק הגנת הפרטיות, התשמ"א-1981.

ככל שהדין אינו מאפשר את קיומו של ההסדר הדיגיטלי, יש לעגנו בדין, בהתאם לכללים המפורטים בסעיף 2 "יצירת דין חדש- כיצד לעגן את ההסדר בדין כשנדרש שינויו" לפרק ג' בחלק א' שלעיל. כך גם במקרה שבו ההסדר לא עולה בקנה אחד עם הדין הכללי, או אז יש לבצע התאמות נקודתיות.

שלב זה של בחינת התאמת ההסדר לדין נועד לאפשר להסדר שגובש לצאת לפועל. יצוין, כי לפעמים בשל אילוצים שונים יהיה יעיל יותר לבחון את התאמת ההסדר לדין בשלב מוקדם יותר (כך, למשל, במקרים שבהם יש קושי לתקן את החקיקה בעניין, כשזו נדרשת). זאת, על מנת להבטיח כי יהיה ניתן לממש את ההסדר שמגובש. יחד עם זאת, דרך המלך היא תחילה לבחון את הרצוי, בהתאם לכללים שפורטו לעיל, ולאחר מכן לבצע התאמות בדין, כשאלה נדרשות, ולהתאים את המצוי לרצוי.

---

[59] החלטת ממשלה 2960 מיום 6.8.2017 בעניין אישור המדיניות הלאומית להזדהות בטוחה, https://www.gov.il/he/Departments/policies/2017_dec2960 .

חלק ג' – מסמכי עזר

מסמך עזר 1 – תרשים הליך בחינה מומלץ להסדר דיגיטלי

הליך בחינה מומלץ להסדר דיגיטלי

1. **זיהוי המטרה הכללית**
שיפור השירות? הגברת היעילות?

2. **זיהוי תכליות ההסדר**
הזדהות? הסכמה לגבי פעולה? תיעוד זמן? הרתעה? שמירה על מהימנות של מידע?

3. **זיהוי הגורמים הנוגעים להסדר**
מיהם בעלי העניין? הציבור? גורמי מקצוע? גופים ציבוריים? עמותות?

4. **בחינת סיכוני ההסדר**
אילו סיכונים עלולים להתממש במקרה של אי קיום התכליות ברמה מספקת? מהי עוצמת הפגיעה במקרה של התממשות הסיכון ורמת ההסתברות להתממשותו? מהי מידת יכולתו של כל גורם לשאת בסיכונים? כיצד כל גורם יכול להקטין אותם?

5. **ביצוע ניהול סיכונים**
יש להתאים את הסיכונים לערך הנפגע ולעוצמת הפגיעה, ולשאוף להקטינם בכלים טכנולוגיים או על ידי קביעת כללים נורמטיביים.

6. **בחינת נטלים**
מהם הנטלים המוטלים על כל גורם המעורב בהסדר? על ההסדר להיות הוגן וישים, ולהתאים לאוכלוסייה שעליה הוא נועד לחול.

7. **בחירה בין הכלים להגשמת כל תכלית**
יש ליצור הלימה בין מרכיבי ההסדר והכלים שבשימוש בו לבין רמת הוודאות שבה יש להגשים כל תכלית.

8. **בחינת התאמת ההסדר לדין**
האם הדין הקיים מאפשר את קיומו של ההסדר הדיגיטלי? האם ניתן להפעיל כללי פרשנות גמישים? האם נדרש תיקון הדין?

מסמך עזר 2 – מידע שימושי בנוגע למעבר מעולם הפיסי לעולם הדיגיטלי:

1. הסבר על "שירותי אמון" נפוצים:

בעולם האלקטרוני קיימים מספר שירותים, שמספקים רמות שונות של אמון בפעולות דיגיטליות שונות. נהוג לכנות שירותים אלה "שירותי אמון"[60]. בסעיף זה יובא הסבר על שירותי האמון הנפוצים: חתימה אלקטרונית, חותם אלקטרוני, זיהוי אלקטרוני, חותמת זמן אלקטרונית, שירותי מסירה ושירותי אימות אתר. לגבי שירותי אמון שלא מוסדרים בדין הישראלי, תתואר - לשם הרחבת היריעה- ההסדרה האירופאית הקיימת בתחום.

1.1. זיהוי אלקטרוני

זיהוי אלקטרוני[61] משמעותו תהליך אלקטרוני, שבו משתמשים במידע, שמאפשר לזהות אדם באופן ייחודי, לצורך זיהויו. הזיהוי יכול להתבצע ביחס לאדם בשם עצמו או בשם אישיות משפטית אחרת (למשל, בשם ארגון)[62], והוא משמש לאימות[63] זהות האדם.

מניסיון שנצבר במשרד המשפטים עולה, כי במקרים רבים שבהם נדרשה חתימה בחיקוק, התכלית המרכזית (ולפעמים גם הבלעדית) של דרישה זו הייתה הזדהות. מכאן, עולה חשיבותו הרבה של הזיהוי האלקטרוני. זאת ועוד, בעולם הדיגיטלי הפעולות נעשות, במקרים רבים, שלא במסגרת מפגש פנים אל פנים. עובדה זו מחזקת את חשיבותו של זיהוי דיגיטלי ברמה הנדרשת. במילים אחרות, ניתן לומר כי שירות הזיהוי הדיגיטלי הינו השירות החשוב ביותר מבין שירותי האמון.

בישראל לא קיים חוק מסגרת, שמסדיר באופן רוחבי את הזיהוי האלקטרוני. עם זאת, ישנם הסדרים ספציפיים שנקבעו בדברי חקיקה שונים, העוסקים באופן הזדהות האזרח לצורך קבלת שירות או קיום חובה.

---

60 ראו הרחבה בסעיף 3(16) לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון.

61 electronic identification

62 ראו ההגדרות הרלוונטיות בסעיף 3 לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון -

'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.

63 authentication

כמו כן, בשנת 2017 החליטה הממשלה[64] לאמץ את המדיניות הלאומית להזדהות בטוחה, שגובשה על ידי צוות בינמשרדי בראשותו של ראש היחידה להזדהות וליישומים ביומטריים. המדיניות מבוססת על תקן בינלאומי בתחום[65] וכוללת התאמות לישראל. המדיניות מגדירה ארבע רמות, אשר מבטאות את מידת הביטחון בזהות של ישות הטוענת לזהות מסוימת. כל רמה כזו מכונה "רמת הבטחת אימות"[66]: רמה 1 מספקת רמת ביטחון נמוכה, רמה 2 מספקת רמת ביטחון בינונית, רמה 3 מספקת רמת ביטחון גבוהה, ורמה 4 מספקת רמת ביטחון גבוהה מאוד.

על פי המדיניות, כל שירות ממשלתי, שכולל הזדהות, יסווג, לאחר ביצוע הערכת סיכונים, לאחת מארבע רמות הבטחת האימות שהוגדרו. בהתאם לסיווג השירות, נותן השירות יוודא כי כלל תהליכי האימות, לרבות בשלב ההרשמה ובשלב ההזדהות בעת צריכת השירות, נותנים מענה לרמת הבטחת האימות המבוקשת. תוצרי המדיניות להזדהות בטוחה כוללים קווים מנחים לסיווג השירות, קווים מנחים לתהליכי הרשמה לשירות, וכן קווים מנחים לאמצעי הזדהות בעת צריכת השירות.

הסדרה נוספת שקיימת בתחום הזיהוי האלקטרוני בישראל היא בחוק מרשם האוכלוסין, אשר מסדיר את תעודת הזהות החכמה. תעודת הזהות החכמה כוללת רכיב של תעודה לאימות[67], אשר מאפשרת לזהות את בעל תעודת הזהות, ברמת הבטחת האימות הגבוהה ביותר המוגדרת במדיניות המתוארת.

הזיהוי יכול להתבצע במגוון דרכים כמו, למשל, באמצעות אימות פרטי המזדהה מול גורם שלישי אובייקטיבי (כמו מרשם האוכלוסין) או שימוש בכרטיס חכם שהונפק למזדהה מבעוד מועד (כמו התעודה לאימות שעל גבי תעודת הזהות החכמה).

1.2 חתימה אלקטרונית

נוכח השימוש הרב שנעשה בחתימה – הן בעולם הנייר והן בעולם האלקטרוני – והתכליות הרבות שהחתימה יכולה להגשים, הוסדר בשנת 2001 מעמדן המשפטי של החתימות האלקטרוניות בחוק חתימה אלקטרונית, התשס"א-2001 (להלן: "חוק חתימה אלקטרונית" או "החוק"). להלן הסבר על ההוראות המרכזיות של החוק.

---

[64] החלטת ממשלה מספר 2960 מיום 6.8.2017 בעניין אישור המדיניות הלאומית להזדהות בטוחה, https://www.gov.il/he/Departments/policies/2017_dec2960 , והמדיניות הלאומית להזדהות בטוחה זמינה בקישור הבא - הקישור הבא https://www.gov.il/he/departments/news/bio_safeidpolicy.

[65] ISO/IEC 29115 – First Edition, Information technology – Security technics – Entity authentication assurance Framework (נכון לדצמבר 2018).

[66] Level of assurance

[67] ראו סעיף 25 לחוק מרשם האוכלוסין.

סוגי החתימות המוגדרים בחוק

החוק מגדיר מהי "חתימה" בעולם האלקטרוני, ומסדיר דרישות סף ותוצאות משפטיות של שני סוגי חתימות: "חתימה מאובטחת" ו"חתימה מאושרת".

חתימה אלקטרונית, בשונה מחתימה על גבי נייר, יכולה להתבצע בדרכים מגוונות: חתימה גרפית על גבי קובץ וורד (WORD) או בתוכנת הצייר (PAINT), חתימה על נייר שנסרקה למחשב, ועוד.

ואכן, ההגדרה הבסיסית של החוק – הגדרת "**חתימה אלקטרונית**"[68] ("מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני") – כוללת כל חתימה שמתבצעת באופן אלקטרוני ללא כל דרישת סף, כדוגמת דרכי החתימה שיתוארו להלן. במילים אחרות, חתימה בעולם האלקטרוני "מתנתקת" מהתפיסה המסורתית של חתימה – שרבוט גרפי – וכוללת סוגים רבים של חתימות כמו למשל הקשת קוד ללא כל סימן גרפי.

לצד ההגדרה הכללית של "חתימה אלקטרונית", מוגדרים בחוק שני סוגי חתימות אלקטרוניות נוספים: "חתימה מאובטחת" ו"חתימה מאושרת". סוגים אלה מבוססים על ההגדרה הכללית של "חתימה אלקטרונית", והם מקיימים דרישות נוספות, שמטרתן להבטיח את הגשמת התכליות הקלאסיות של חתימה.

חתימה אלקטרונית מאובטחת (לעיל ולהלן: "חתימה מאובטחת") מקיימת את הדרישות הבאות: היא ייחודית לחותם, מאפשרת זיהוי שלו, אמצעי החתימה ניתן לשליטתו הבלעדית של החותם וניתן לזהות שינוי במסמך לאחר שנחתם.

קיום דרישות אלה מאפשר להגשים מספר **תכליות** קלאסיות של החתימה: זיהוי (במידה מסוימת) של החותם וקשירתו למסמך החתום, והֶעָדָה על שלמות המסמך ועל כך שלא שונה ממועד החתימה. בנוגע לתכלית של גמירת דעת החותם בדבר ביצוע הפעולה המשפטית או כריתת חוזה, יצוין כי מאפייני החתימה המאובטחת יכולים להיות נסיבה שמסייעת לבחינת גמירת דעת החותם, אך אינם יכולים להגשים תכלית זו לבדם. לצורך הֶעָדָה על גמירת דעת החותם, נדרשות נסיבות נוספות שיעידו עליה, כמו למשל, תוכן המסמך, הסכמות בין צדדים, התנהגות החותם בעת החתימה ותגובות לתהליך יישומי באפליקציית החתימה (כגון לחיצה על אישור במסך שעולה בעיתוי המתאים- pop-up, שמתריע לפני אישור פעולת החתימה ומבקש הסכמה פוזיטיבית של המשתמש לפעולת החתימה), ועוד.

---

[68] לפעמים נעשה שימוש במונח "חתימה דיגיטלית" בשביל לבטא חתימה "גנרית" בעולם הדיגיטלי. המונח שנבחר בחוק חתימה אלקטרונית לתיאור חתימה גנרית בעולם הדיגיטלי הוא "חתימה אלקטרונית". על כן, בהנחיה זו, המונח "חתימה אלקטרונית" יתייחס לחתימה "גנרית" ללא דרישות מיוחדות, כמשמעותה בחוק חתימה אלקטרונית.

במאמר מוסגר יצוין, כי בדברי חקיקה במדינות אחרות, לפעמים המונח "חתימה דיגיטלית" הוא המונח הגנרי המקביל להגדרה "חתימה אלקטרונית" בחוק הישראלי, בעוד שבמונח חתימה אלקטרונית נעשה שימוש לצורך תיאור חתימה שמבוססת על טכניקה של מפתח ציבורי, בדומה לחתימה מאובטחת בדין הישראלי.

חתימה אלקטרונית מאושרת (לעיל ולהלן: "**חתימה מאושרת**") מוסיפה רובד נוסף על החתימה המאובטחת והוא זיהוי חזק של החותם (המכונה זיהוי חד חד ערכי). זיהוי חזק זה מתאפשר הודות לכך שהוא נעשה על ידי גורם שלישי, אשר מפוקח לפי החוק על ידי רשם הגורמים המאשרים ברשות להגנת הפרטיות במשרד המשפטים. גורם שלישי זה, המכונה בחוק "גורם מאשר", מזהה את בעל אמצעי החתימה המאושרת בעת ההנפקה פנים אל פנים. לאחר זיהוי ראשוני זה, ניתן להסתמך על חתימתו של בעל אמצעי החתימה, גם מבלי שהצד המסתמך יפגוש את החותם פנים אל פנים או יכיר אותו.

יצוין, כי גם חתימה מאובטחת יכולה לספק זיהוי חזק, בנסיבות מסוימות. כך, למשל, מרבית עובדי המדינה מחזיקים בכרטיס עובד, שכולל רכיב של חתימה מאובטחת. הזדהות העובד באמצעות החתימה שעל גבי הכרטיס היא הזדהות חזקה, מפני שבעת קבלת כרטיס העובד, עם כניסתו לשירות המדינה, הוא מזוהה באופן חד פעמי פנים אל פנים בהליך פנימי על ידי הגורמים האחראים על זיהוי העובדים ועל חלוקת כרטיסי העובד בכל משרד ממשלתי.

בסעיף 2 למסמך עזר 2 ניתן למצוא סקירה של סוגים נפוצים של חתימות אלקטרוניות, אופן הנפקתן, אופן השימוש בהן בחיי המעשה ומשמעותן הראייתית.

<u>מעמדן הראייתי של חתימות אלקטרוניות</u>

כלל הבסיס הראייתי של החוק הוא כי לא תישלל קבילותה של חתימה רק בשל היותה חתימה אלקטרונית.[69] כלל זה מבוסס על עקרון אי העדיפות, שתואר בסעיף 2, "אי עדיפות", בפרק א' לחלק א' שלעיל.

לעניין חתימה מאושרת וחתימה מאובטחת, נוכח מאפייניהן של חתימות מסוגים אלה, החוק העניק להן **מעמד ראייתי מוגבר**.[70] נקבע, כי מסר, החתום בחתימה מאובטחת, יהיה קביל בכל הליך משפטי ויהווה ראיה לכאורה לכך שהמסר האלקטרוני לא שונה לאחר מועד החתימה ושהמסר האלקטרוני נחתם באמצעי החתימה המתאים לחתימה האלקטרונית. לעניין מסר החתום בחתימה מאושרת, המעמד הראייתי המוגבר ניתן גם לזהות בעל אמצעי החתימה, בנוסף לזהות האמצעי שבאמצעותו בוצעה החתימה (שכן, חתימה מאושרת מבטיחה את זהות החותם ברמה גבוהה יותר).

[69] ראו סעיף 3(א) לחוק חתימה אלקטרונית.

[70] ראו סעיף 3(ב) לחוק חתימה אלקטרונית.

החובות שמוטלות על החותם בחתימה מאושרת או מאובטחת

החוק מטיל על החותם בחתימה מאובטחת או מאושרת **שתי חובות מרכזיות**. ראשית, מוטלת על החותם חובה לנקוט בכל האמצעים הסבירים לשם שמירה על אמצעי החתימה שלו ולשם מניעת שימוש בו ללא הרשאתו. שנית, מוטלת עליו חובה למסור הודעה במקרה שבו נודע לו על פגיעה בשליטתו באמצעי החתימה. החותם בחתימה מאובטחת נדרש למסור הודעה זו לכל מי שסביר שיסתמך על חתימתו האלקטרונית, בעוד שהחותם בחתימה מאושרת נדרש למסור הודעה זו לגורם המאשר שהנפיק עבורו תעודה אלקטרונית. במקרה שבו החותם עמד בחובותיו האמורות, הוא לא יהיה אחראי לנזק שנגרם עקב שימוש באמצעי החתימה שלו ללא הרשאתו[71].

דרישת חתימה לפי חיקוק

כלל היסוד של החוק קבוע בסעיף 2(א), ולפיו כשנדרשת חתימה בחיקוק, ניתן לקיימה באמצעות חתימה מאושרת או חתימה אלקטרונית אחרת, שמקיימת את תכליות דרישת החתימה, ברמת וודאות מספקת בנסיבות העניין. להסבר על אופן יישום כלל זה, ראו בפרק ג' "יישום ההסדר בחקיקה - פרשנות דין קיים ויצירת דין חדש" לחלק א' שלעיל.

למי מסור שיקול הדעת לבחור בין סוגי החתימות כשנדרשת חתימה בחיקוק

כשנדרשת חתימה בחיקוק, סעיף 2(א) מעניק שיקול דעת לבחור בין סוגי החתימות האלקטרוניות הקיימים, בכפוף לתנאיו, אשר פורטו לעיל. שיקול דעת זה מסור לחותם, לגורם שהוא בעל אפשרות לקבוע או להשפיע על סוג החתימה שייעשה בה שימוש, או לגורם המבקש להסתמך על החתימה, לפי העניין. כך, למשל, באשר למסמכים חתומים שהציבור או חלק ממנו נדרש להגיש למשרד ממשלתי, באפשרות אותו משרד ממשלתי לקבוע באיזה אופן יתקבלו מסמכים אלה ומהו סוג החתימה הנדרש לגביהם; גופים מאסדרים (רגולטורים) יכולים לקבוע במסגרת הפיקוח שלהם מהו סוג החתימה שיש לעשות בו שימוש על ידי המפוקחים שלהם או במערכת היחסים בין המפוקחים לציבור; עוסקים מהשוק הפרטי יכולים לקבוע סוגי חתימה שונים שבהם ייעשה שימוש במסגרת התקשרויות חוזיות איתם (לדוגמה, חוזים צרכניים).

נטל הוכחה בעניין חתימה בקשר למערכות יחסים חוזיות

נוכח שיקול הדעת שמעניק החוק בבחירת סוג החתימה האלקטרונית, נקבעה בסעיף 3א לחוק הוראה, שנועדה להגן על צדדים חלשים להתקשרות חוזית. ההגנה ניתנת על ידי קביעת כלל בנוגע לנטל ההוכחה בקשר לחתימות אלקטרוניות במערכות יחסים חוזיות, שבהן לצד אחד יש עדיפות בעיצוב אופן החתימה. הסעיף לא חל על מערכות יחסים שאינן חוזיות.

---

[71] ראו סעיפים 7-8 לחוק חתימה אלקטרונית.

ניתן להניח כי מערכת יחסים חוזית, שבה צד אחד לחוזה קובע באיזה אופן תתבצע התחימה, מתאפיינות בפערי כוחות. דוגמה למערכת יחסים כזו היא, למשל, מקרה שבו חברת סלולר קובעת באיזה אופן לקוחותיה יחתמו על חוזי ההתקשרות איתה.

לפי הסעיף, במקרים כאלה, אם צד להתקשרות חוזית זו יטען כי החוזה (או מסמך אחר) לא נחתם בידו[72], על הגורם שהייתה לו עדיפות בעיצוב אופן החתימה כאמור (בדוגמה שלעיל – חברת הסלולר), המבקש להסתמך על החתימה ("הגורם המעצב"), להוכיח כי המסמך נחתם על ידי אותו צד. נטל זה יחול על אף האמור בכל חוזה.

באשר להשפעת סעיף זה על משרדי הממשלה, יצוין כי מאחר שהוא חל רק על התקשרויות חוזיות, הוא אינו חל על פעולות המשרד הממשלתי בכובעו המינהלי. זאת ועוד, אף במקרים שבהם משרד ממשלתי הוא צד למערכת יחסים חוזית בכובעו הפרטי (פועל כפיסקוס), שבה יש לו עדיפות בעיצוב אופן החתימה, נראה שהכלל האמור לא צפוי ליצור סיכון משפטי ממשי במקרה של התכחשות לחתימה. הסיבה לכך היא שבמקרה שבו יצטרך המשרד להוכיח כי צד לחוזה חתם על מסמך, הוא יוכל להיעזר בהצגת תהליך החתימה, הטכנולוגיה שנבחרה ונהלי העבודה המקובלים אצלו עם קליטת המסמך החתום. נראה שכל אלה יעניקו למשרד הממשלתי את הוודאות הנדרשת לו בכל הנוגע לאמינות סוג החתימה שנבחר על ידו, וכפועל יוצא מכך יקלו עליו להוכיח כי המסמך נחתם על ידי הצד המתכחש. באופן דומה, גם גופים שאינם ממשלתיים, אשר יפעלו לפי נהלי עבודה מספקים, יצמצמו את הסיכון שלהם.

1.3 חותם אלקטרוני

חותָם אלקטרוני[73] הוא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני על ידי **ישות משפטית שאינה טבעית**. כלומר, חותָם אלקטרוני נכלל בהגדרה הבסיסית של "חתימה אלקטרונית" לפי חוק חתימה אלקטרונית.

בכל הנוגע לחתימה מאושרת לפי חוק חתימה אלקטרונית, ישנו הבדל בין חותָם אלקטרוני לחתימה אלקטרונית: כשמדובר בחתימה מאושרת, החותֵם הוא ישות משפטית טבעית בלבד, כלומר אדם. התעודה האלקטרונית, שעליה מונפקת החתימה המאושרת, יכולה להיות שייכת לתאגיד או למוסד ציבורי, אך החתימה חייבת להתבצע על ידי **אדם**, בשם התאגיד או המוסד. לעומת זאת, פעולה של הטבעת חותָם אלקטרוני יכולה להתבצע גם על ידי התאגיד או המוסד עצמו, מבלי לציין מיהו האדם שביצע את הפעולה בשם התאגיד או המוסד.

---

72 למשל, יתכחש לחתימה בשל כך שהחתימה נעשתה ללא הרשאתו; בשל כך שהמסמך השתנה לאחר החתימה או בשל כך שהחתימה כלל אינה שלו.

73 ראו ההגדרה הרלוונטית בסעיף 3 לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון-

'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

אם כן, שירות אמון מסוג חותָם אלקטרוני מתאים לשימוש כשאין חשיבות לזהות האדם שמבצע את הפעולה בשם התאגיד או המוסד. לעומת זאת, חתימה אלקטרונית של אדם טבעי תידרש כשיש צורך בזיהוי האדם שמבצע את פעולת החתימה עבור התאגיד או המוסד.

מטרתו המרכזית של החותָם האלקטרוני היא לזהות האם מסמך הוא שלם והאם בוצע בו שינוי מאז שהוטבע עליו החותָם. למטרה זו מצטרפות לפעמים מטרות נוספות כמו זיהוי התאגיד או המוסד שעושה שימוש בחותָם האלקטרוני וקשירתו למסמך שעליו הוטבע החותָם. מטרות אלה דומות למטרותיה הקלאסיות של החתימה האלקטרונית.

חותָם אלקטרוני לא מוסדר במפורש בדין הישראלי, אך הוא חופף בחלקו לחתימה אלקטרונית, המוסדרת בחוק חתימה אלקטרונית, כפי שהוסבר לעיל. בשונה מהמצב החקיקתי הקיים בישראל, בתקנות האיחוד האירופאי בנושא, החותָם האלקטרוני מוסדר בנפרד מהחתימה האלקטרונית. לפי תקנות האיחוד, חותָם אלקטרוני שמקיים תנאי סף מסוימים ושהונפק על ידי גוף מפוקח ייהנה מחזקה כי המידע שאליו הוא מקושר הוא שלם ושהוא המידע שנחתם במקור. עוד נקבע בתקנות האיחוד, כי לא יישלל תוקפו של חותָם אלקטרוני רק בשל כך שהוא אלקטרוני או בשל כך שאינו מקיים דרישות סף כלשהן. לצד זאת, תקנות האיחוד מאפשרות למדינות לדרוש קיום תנאי סף מסוימים במסגרת מתן שירותים ממשלתיים. תנאי הסף עשויים ללמד על מאפייניו של החותָם האלקטרוני, והם: החותָם ייחודי ליוצר החותָם; יוצר החותָם ניתן לזיהוי; החותָם הופק באמצעי אשר המשתמש בו יכול, ברמת הסתברות גבוהה, לעשות בו שימוש תחת שליטתו הבלעדית; החותָם מאפשר לזהות שינוי שבוצע במסמך לאחר מועד הטבעת החותָם.

1.4 חותמת זמן:

חותמת זמן אלקטרונית[74] היא מידע אלקטרוני הכולל תאריך ושעה, שנקשר למסמך אלקטרוני, ואשר מוכיח שהמסמך היה קיים באותה נקודת זמן ושהוא לא שונה מאז אותה נקודת זמן.

חותמת זמן אלקטרונית אינה מוסדרת בדין הישראלי, אף שבדרך כלל, תוכנות חיתום שבאמצעותן מתבצעת חתימה אלקטרונית, כוללות גם את שעת החתימה על המסמך (תוכנות החיתום עצמן לא מוסדרות בדין הישראלי).

בדין האירופאי, ישנה הסדרה של חותמת זמן במסגרת תקנות האיחוד בנושא. לפיהן, לא יישלל תוקפה של חותמת זמן רק בשל כך שהיא אלקטרונית או בשל כך שאינה מקיימת דרישות סף כלשהן. לצד זאת, תקנות האיחוד מאפשרות למדינות לדרוש קיום תנאי סף מסוימים במסגרת מתן שירותים ממשלתיים. תנאי הסף יכולים ללמד על מאפייניה של חותמת הזמן, והם: קישור תאריך ושעה למידע באופן ששולל אפשרות לכך שהמידע שונה לאחר מכן מבלי שיהיה חיווי לכך; חותמת הזמן מבוססת על מקור זמן מדויק ועצמאי; חותמת הזמן חתומה על ידי ספק חותמת הזמן בחתימה אלקטרונית או בחותם אלקטרוני שמקיימים תנאי סף מסוימים.

1.5 דואר אלקטרוני רשום

דואר אלקטרוני רשום[75] הוא שירות, המאפשר להעביר מידע בין צדדים באופן אלקטרוני. הוא מספק ראיה בנוגע להעברת המידע, ובכלל זאת ראיה לשליחת המידע ולקבלתו. כמו כן, הוא מגן על המידע המועבר מפני סיכונים של אובדן, גניבה, נזק או שינוי לא מורשה של המידע.

במילים אחרות, שירות זה מספק ראיה למשלוח מידע אלקטרוני והגעתו לנמען ומגן על שלמות המידע, וכן מגן עליו מפני גישה לא מורשית. שירות אלקטרוני זה מקביל במידה מסוימת לשירות של דואר רשום בעולם הפיסי בנייר.

שירותי דואר אלקטרוני רשום אינם מוסדרים בדין הישראלי. בדין האירופאי, שירותים אלה מוסדרים במסגרת התקנות בנושא. לפיהן, לא יישלל תוקפו של מידע שנשלח או התקבל באמצעות שירות דואר אלקטרוני רשום רק בשל כך שהוא נשלח או התקבל בדרך אלקטרונית או בשל כך שאינו מקיים דרישות סף כלשהן.

---

[74] ראו ההגדרה הרלוונטית בסעיף 3 לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון-

'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

[75] ראו ההגדרה הרלוונטית בסעיף 3 לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון -

'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

לצד זאת, התקנות מקנות מעמד ראייתי לשירות דואר אלקטרוני רשום שמקיים תנאי סף המוגדרים בתקנות. לפי התקנות, מידע, שמועבר בשירות דואר ומקיים את תנאי הסף הקבועים בהן, ייהנה מחזקה כי הוא שלם, נשלח על ידי שולח מזוהה והתקבל אצל נמען מזוהה, וזאת ביום ובשעה שצוינה על ידי ספק שירות הדואר האלקטרוני הרשום.

תנאי הסף הינם: השירות מסופק על ידי גוף מפוקח; השירות מוודא ברמת ביטחון גבוהה את זהות השולח; השירות מוודא ברמת ביטחון גבוהה את זהות הנמען לפני שליחת המידע; השליחה והקבלה של המידע מאובטחות באמצעות חתימה מאובטחת או באמצעות חותם אלקטרוני מאובטח של נותן שירות מפוקח, באופן שמונע את האפשרות שהמידע ישונה מבלי שיהיה חיווי לשינוי; ישנו חיווי בנוגע לכל שינוי במידע שנדרש לצורך שליחת המידע או קבלתו, שמוצג לשולח ולמקבל; התאריך והשעה של השליחה והקבלה מוצגים באמצעות חותמת זמן של ספק שירותים מוסמך.

בישראל קיימים שירותים שונים להעברת מסרים. כך, למשל, מערכת הדיוור הדיגיטלי הממשלתי שפותחה ברשות התקשוב שבמשרד ראש הממשלה, משלבת מספר מערכות טכנולוגיות, ובהן פורטל האזור האישי. על פי חוות הדעת של גורמי המקצוע ברשות התקשוב, מערכת זו מהווה פלטפורמה המבטיחה העברת מסרים לנמען בשלמותם, תוך הבטחת צפייתו על ידי הנמען בלבד, ברמת ודאות גבוהה.[76]

1.6 תעודה אלקטרונית המשמשת לאימות אתר אינטרנט

תעודה אלקטרונית לאימות אתר אינטרנט היא תעודה שמאפשרת לאמת אתר אינטרנט ולקשר אותו לבעליו או מפעיליו[77]. תעודה לאימות אתרים אינה מוסדרת בדין הישראלי. בתקנות האיחוד בנושא, נקבעו תנאי סף לתעודה אלקטרונית מוסמכת לאימות. תנאי הסף מלמדים על מאפייניה של התעודה לאימות אתר אינטרנט, ובהם[78]: קיומה של אינדיקציה לכך שהתעודה הונפקה על ידי ספק שירותי אימות אתר מפוקח; פרטי האדם או התאגיד שהונפקה לו התעודה; שמות המתחם (domain) שמופעלים על ידי האדם שהונפקה לו התעודה; פרטים אודות התקופה שבה התעודה בתוקף; מספר סידורי ייחודי של התעודה.

---

[76] כך על פי חוות דעת של ראש רשות התקשוב שבמשרד ראש הממשלה מיום 19.2.2019. חוות דעת זו מצורפת להנחיה ומסומנת כמסמך עזר 4.

[77] ראו ההגדרה הרלוונטית בסעיף 3 לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון -

‘certificate for website authentication’ means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.

[78] לרשימה המלאה, ראו ANNEX IV לתקנות האיחוד האירופי בנושא ניהול זהויות ושירותי אמון.

<u>2. סקירת סוגים נפוצים של חתימות אלקטרוניות, מאפייניהן ואופן השימוש בהן בחיי המעשה ומשמעותן הראייתית:</u>

בסעיף זה תובא סקירה של סוגים נפוצים של חתימות אלקטרוניות, התכליות שהם עשויים להגשים ואופן השימוש בהם בחיי המעשה.

<u>2.1 חתימה אלקטרונית מאושרת</u>

- **הגדרה**: חתימה אלקטרונית מאובטחת, אשר גורם מאשר הנפיק תעודה אלקטרונית מאושרת בדבר אמצעי אימות החתימה המזהה אותה. ההגדרה לקוחה מחוק חתימה אלקטרונית.

- **דוגמאות לשימוש**[79]: הגשות לרשות לניירות ערך באמצעות מערכת מגנ"א; הודעות לפי פקודת המיסים (גביה); נסח טאבו; כתב בי"ד אלקטרוני שמוגש לבתי משפט; מערכת "שער עולמי" של רשות המיסים.

- **תכליות מרכזיות שהחתימה עשויה להגשים**: זיהוי ברמה גבוהה של החותם (רמת אימות 4 על פי המדיניות הלאומית להזדהות בטוחה[80]); יכולת לזהות שינוי במסר החתום לאחר מועד החתימה; הֶעָדָה על זמן ביצוע החתימה (רק בחלק מהחתימות המאושרות). תכליות אלה מתקיימות ברמת ודאות גבוהה. בנוגע לתכלית של גמירת דעת החותם, יצוין כי מאפייני החתימה המאושרת יכולים להיות נסיבה שמסייעת לבחינת גמירת דעת החותם, אך אינם יכולים להגשים תכלית זו לבדם[81].

- **משמעות ראייתית**: מסר אלקטרוני החתום בחתימה מאושרת יהיה קביל בכל הליך משפטי ויהווה ראיה לכאורה לכך שהמסר האלקטרוני לא שונה לאחר מועד החתימה ושהמסר האלקטרוני נחתם על ידי בעל אמצעי החתימה.

- **בחיי המעשה**: שימוש בחתימה מאושרת יכול להתאים במקרה שבו הגורם שמעוניין להסתמך על החתימה לא מכיר את החותם, ועל כן הם נעזרים בצד שלישי, אשר הינו מפוקח על ידי רשם הגורמים המאשרים, שיבטיח את זהותו של החותם.

---

[79] נכון לשנת 2017

[80] עיקרי המדיניות הלאומית להזדהות בטוחה אושרו על ידי הממשלה בהחלטה מספר 2960 מיום 6.8.2017, http://www.pmo.gov.il/Secretary/GovDecisions/2017/Pages/dec2960.aspx.

[81] לצורך הֶעָדָה על גמירת דעת החותם, נדרשות נסיבות נוספות שיעידו עליה, כמו למשל, תוכן המסמך, הסכמות בין צדדים, התנהגות החותם בעת החתימה ותגובות לתהליך יישומי באפליקציית החתימה (כגון לחיצה על אישור במסך שעולה בעיתוי המתאים- pop-up, שמתריע לפני אישור פעולת החתימה ומבקש הסכמה פוזיטיבית של המשתמש לפעולת החתימה), ועוד.

על המבקש לרכוש חתימה מאושרת לפנות לאחד מהגורמים המאשרים לפי חוק חתימה אלקטרונית ולהזדהות בפניו על פי מספר פרטי זיהוי.[82] במסגרת ההנפקה, יתבקש המבקש לבחור סיסמה שידועה רק לו. בתום ההנפקה, יקבל המבקש את אמצעי החתימה. אמצעי החתימה יכול להיות מוטבע על גבי כרטיס חכם, USB, ועוד. השירות ניתן בתשלום[83].

בעל אמצעי חתימה, אשר מעוניין לחתום בחתימה האלקטרונית המאושרת שהונפקה עבורו, צריך להכניס את אמצעי החתימה למחשב (אם למשל אמצעי החתימה הוטבע על גבי כרטיס חכם, עליו להכניס את הכרטיס החכם לקורא הכרטיסים המחובר למחשב), להיכנס לתוכנת חתימה, להקיש את סיסמתו, וכך לחתום את הקובץ הרצוי. ממועד החתימה, יהיה ניתן לזהות שינוי במסמך החתום, ככל שיתבצע.

לאחר החתימה על הקובץ, ניתן לפתוח אותו ולקבל חיווי אודות החתימה כמו למשל האם המסמך שונה ממועד החתימה, זהות החותם, מועד החתימה (בחלק מהחתימות) והאם התעודה ששימשה לביצוע החתימה בתוקף. בדרך כלל החיווי מופיע באופן אוטומטי עם פתיחת הקובץ. ניתן לראות פרטים נוספים על החתימה בעזרת כניסה לסרגל החתימה שמופיע עם פתיחת קובץ.

2.2 חתימה אלקטרונית מאובטחת

- **הגדרה**: חתימה אלקטרונית, שמתקיימים בה כל אלה: היא ייחודית לבעל אמצעי החתימה; היא מאפשרת זיהוי לכאורה של בעל אמצעי החתימה; היא הופקה באמצעי חתימה הניתן לשליטתו הבלעדית של בעל אמצעי החתימה; היא מאפשרת לזהות שינוי שבוצע במסר האלקטרוני לאחר מועד החתימה. הגדרה זו לקוחה מחוק חתימה אלקטרונית.

- **דוגמאות לשימוש**: סעיף 18ב להוראות מס הכנסה (ניהול פנקסי חשבונות), התשל"ג-1973 קובע הסדר, שלפיו ניתן לחתום על חשבונית בחתימה מאובטחת. עוד נקבע בסעיף זה כי כשנעשה שימוש בחתימה מאובטחת, התקבול בשל החשבונית יתקבל בדרך שמאפשרת לזהות את הצדדים לעסקה (למשל, באמצעות כרטיס אשראי). הוספת התנאי בנוגע לתקבול נועדה להבטיח שרמת הוודאות של זהות החותם גבוהה במידה מספקת, וזאת מאחר שרמת הזיהוי של החותם בחתימה מאובטחת עשויה להשתנות מחתימה מאובטחת אחת לאחרת.

- **תכליות מרכזיות שהחתימה עשויה להגשים**: זיהוי של החותם ברמות משתנות (אין פיקוח על אופן ההזדהות ורמתה, ועל כן יהיו מוצרים שבהם הזיהוי יהיה "חזק" ויהיו כאלה שהזיהוי יהיה "חלש" מאוד); זיהוי אמצעי החתימה המסוים (המפתח הפרטי) שבו נעשה שימוש בעת החתימה; יכולת לזהות שינוי במסר החתום לאחר מועד החתימה; הֶעָדָה על זמן

[82] ראו תקנה 10 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.

[83] נכון לשנת 2017, השירות ניתן בשוק הפרטי בתמורה לכמה מאות שקלים אחת לכמה שנים.

ביצוע החתימה (רק בחלק מהחתימות המאובטחות). לאחר שמוכח כי חתימה שנעשה בה שימוש היא אכן חתימה מאובטחת, תכליות זיהוי אמצעי החתימה המסוים שבו נעשה שימוש ויכולת לזהות שינוי במסר לאחר מועד החתימה מתקיימות ברמת ודאות גבוהה. בנוגע לתכלית של גמירת דעת החותם, יצוין כי מאפייני החתימה המאובטחת יכולים להיות נסיבה שמסייעת לבחינת גמירת דעת החותם, אך אינם יכולים להגשים תכלית זו לבדם[84].

- **משמעות ראייתית**: מסר אלקטרוני החתום בחתימה אלקטרונית מאובטחת יהיה קביל בכל הליך משפטי ויהווה ראיה לכאורה לכך שהמסר האלקטרוני לא שונה לאחר מועד החתימה ושהמסר האלקטרוני נחתם על נחתם באמצעי החתימה המתאים לחתימה האלקטרונית (כלומר, אף שלא ניתן מעמד ראייתי מוגבר לזהות החותם, ניתן מעמד ראייתי מוגבר לאמצעי החתימה המסוים – המפתח הפרטי – שבו עשה שימוש החותם). יצוין, כי ישנה אפשרות לפנות אל רשם הגורמים המאשרים לפי חוק חתימה אלקטרונית בבקשה לקבל אישור לכך שטכנולוגיה מסוימת שבה נעשה שימוש – חזקה שהיא חתימה מאובטחת, כלומר היא מוחזקת ככזו שמקיימת את ארבע דרישות החתימה המאובטחת הקבועות בחוק[85].

- **בחיי המעשה**: שימוש בחתימה מאובטחת, שהמסתמך עליה אינו יודע כיצד בוצע אימות זהות החותם, עשוי להיעשות כאשר זהות החותם אינה חשובה או ידועה ממקור אחר.

מאחר שהליך הנפקת חתימה מאובטחת אינו מוסדר בחוק, ניתן לרכוש חתימה אלקטרונית מאובטחת בדרכים שונות וגם מגורמים שאינם מפוקחים לפי החוק. כמו כן, מאחר שרמת ההזדהות הנדרשת בחתימה מאובטחת אינה מוסדרת בחוק, גם ההזדהות לצורך קבלת חתימה מאובטחת יכולה להשתנות מהנפקה להנפקה.

2.3 חתימה אלקטרונית מאובטחת ב"מערכות סגורות"

- **תיאור**[86]: חתימה שנעשה בה שימוש במסגרת מערכות יחסים שבהן הצדדים מכירים זה את זה, והגורם המבקש להסתמך על החתימה הוא מנפיק אמצעי החתימה. למשל, כרטיסי עובד שמנפיק מעסיק במקום עבודה, שבאמצעותם חותמים עובדיו.
- **דוגמאות לשימוש**: מרשם אלקטרוני[87] של רופא על פי נוהל משרד הבריאות[88], אשר עושה שימוש בחתימה אלקטרונית מאובטחת שהונפקה לרופא על ידי קופת החולים. במסגרת נוהל זה, ישנו הסדר אשר יוצר קשר של מעין "מערכת סגורה" בין קופת החולים לבית המרקחת

---

[84] לצורך הֶעָדָה על גמירת דעת החותם, נדרשות נסיבות נוספות שיעידו עליה, כמפורט בה"ש מספר 79 לעיל.

[85] ראו תקנה 9 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.

[86] יובהר, כי לא קיימת הגדרה ייחודית בחוק לחתימה מאובטחת במערכות סגורות.

[87] ראו תקנות הרופאים (מתן מרשם), תשמ"א-1981.

[88] נוהל מספר 107 של משרד הבריאות בשם מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי מחודש יולי 2013, https://www.health.gov.il/hozer/DR_107.pdf.

שבו ניתן לממש את המרשם; חתימה מאובטחת אשר מוטבעת בכרטיס עובד תמו"ז של עובדי המדינה, ומונפקת על ידי יחידת ממשל זמין ברשות התקשוב. זיהוי בעל אמצעי החתימה (במקרה זה, עובד המדינה) מתבצע על ידי אמרכל כל משרד בעת קליטת העובד לעבודה וכרטיס העובד ניתן לו על פי נוהל שהוגדר מראש.

- **תכליות מרכזיות שהחתימה עשויה להגשים**: תכליות החתימה הנפוצות (הזדהות ויכולת לזהות שינוי במסר החתום לאחר מועד החתימה), ככל שהגורם המסתמך הנפיק את החתימה כך שתכליות אלה תוגשמנה.
- **משמעות ראייתית**: חל הכלל הרגיל, שלפיו לא תישלל קבילותה של חתימה רק בשל היותה חתימה אלקטרונית. לא קיימות הוראות ראייתיות מיוחדות בעניינה.
- **בחיי המעשה**: נהוג לעשות שימוש בחתימות אלקטרוניות מאובטחות במערכות יחסים שבהן הצדדים מכירים זה את זה, והגורם המבקש להסתמך על החתימה הוא מנפיק אמצעי החתימה. כך, למשל, חתימות מאובטחות שמונפקות לעובדי המדינה על ידי המדינה באמצעות יחידת ממשל זמין ברשות התקשוב.

2.4 חתימה אלקטרונית

- **הגדרה**: חתימה שאינה נדרשת לקיים תנאי סף כלשהם. חתימה זו מוגדרת בחוק חתימה אלקטרונית כ"חתימה שהיא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני".
- **דוגמאות לשימוש**: חתימה על גבי לוח חתימה דיגיטלי ("פד" דיגיטלי) מסוגים שונים. ראו, למשל, דוגמה לדרישות מהותיות של חתימה גרפית על פד דיגיטלי ברישיונות של חברות הסלולר[89]. יובהר, כי שימוש בחתימה גרפית על פד דיגיטלי אינה פוטרת מהחובה להעניק זכות עיון מוקדם במסמך שעליו מתבצעת החתימה, כשזו קיימת (למשל, מכוח סעיף 5(ב) לחוק הגנת הצרכן, התשמ"א-1981 בנוגע לחוזים בין צרכן לעוסק); "אשרור מקוון" כהגדרתו בתקנות תכנון ובניה (רישוי בניה), התשע"ו-2016- מתן הסכמה מקוונת, לאחר ביצוע אימות זהותו של המבקש אל מול מרשם האוכלוסין; סימון תיבת "אני מאשר" על גבי טופס מקוון; הקלדת שם החותם בתחתית דואר אלקטרוני.
- **תכליות מרכזיות שהחתימה עשויה להגשים**: מאחר שמדובר במנעד גדול של סוגי חתימות שנכללים בקבוצה זו, כך גם התכליות יכולות להשתנות מסוג לסוג.
- **משמעות ראייתית**: החוק לא מקנה העדפה ראייתית לחתימות אלקטרוניות שלא מקיימות תנאי סף כלשהם, וחל עליהן הכלל הכללי, שלפיו לא תישלל קבילותה של חתימה רק בשל היותה חתימה אלקטרונית.
- **בחיי המעשה**: כחתימה שאינה נדרשת לקיים תנאי סף כלשהם, כוללת חתימה אלקטרונית סל רחב של מוצרים בשוק. אופן השימוש בחתימות אלקטרוניות משתנה ממוצר למוצר.

---

[89] ראו סעיף 2.5 לנספח ה' ברישיון פלאפון שמתייחס לאופן מימוש "חתימה גרפית ממוחשבת" ומחיל את ההוראות המהותיות לעניין הזה, הכוללות בין היתר חובות לעניין זיהוי, קיבוע החתימה, נעילת ההסכם ושמירת תיעוד (נכון לשנת 2017), https://www.gov.il/BlobFolder/policy/pelephone/he/Pelephone%20-%20License%20-%20integrated%20version%20of%20the%20Internet%20as%20of%2022.7.18.pdf.