# מדינת ישראל
## משרד המשפטים

**ייעוץ וחקיקה**

ירושלים: ט"ז סיוון תשע"ט
19 יוני 2019
תיקנו: 803-04-2019-000632
סימוכין: 803-99-2019-042475

לכבוד
**<u>משתתפי הישיבה</u>**

שלום רב,

הנדון: **<u>סיכום דיון בנושא דיון טכנולוגיות זיהוי ואימות – עדכון ואימוץ של טכנולוגיות בסקטורים נוספים</u>**

ביום 15/05/19 התקיימה ישיבה במשרד המשפטים, לילך וגנר, ייעוץ וחקיקה פלילי, ראש אשכול פשיעה חמורה ועונשין, בנושא שבנדון.

**<u>משתתפים</u>**: לילך וגנר, דנה רוטשילד, עינת גדעוני, עביר מטאנס, נטע גורי – ייעוץ וחקיקה (פלילי); רעות אופק – ייעוץ וחקיקה (אזרחי); איה גורצקי, עדי טל נוסבאום, אורית חלפון – משטרת ישראל; דרור גולדשטיין, לימור גרובלס – הפיקוח על הבנקים; רונן ניסים – יעוץ משפטי, בנק ישראל; יוני חדד – פרקליטות המדינה מחלקת סייבר; שרון פרידמן – פרקליטות המדינה, אכיפה כלכלית; שרה קנדלר, רוני בקמן, יסמין פרנקל, עדי לדרמן – רשות ניירות ערך; אסף נחמני, יעל צוקרמן בלאו – רשות שוק ההון; עדי פלד – הממונה על נותני שירות עסקי; סבטלנה גרנר, זהבית מלאך – הרשות לאיסור הלבנת הון; לינא כאמל, נעמה גורני, ספיר מנינגר – הרשות להגנת הפרטיות.

**<u>הרקע לדיון</u>**:

כיום ע"פ החוק והצו,[1] הבנקים נדרשים בעת פתיחת חשבון ללקוח, בין היתר, לזיהוי פנים אל פנים וכן לקבלת הצהרת נהנה בחתימת מקור. על פי נוסח הצו, פשיטא, ניתן לקיים דרישות אלה בעת **נוכחות פיזית** של הלקוח בסניף הבנק. לפני מספר שנים יזם בנק ישראל שילוב של טכנולוגיה לזיהוי ואימות מרחוק בתחום הפיננסי, כחלופה לזיהוי פנים אל פנים וחתימת המקור, וזאת בדרך של פרסום הוראת הפיקוח על הבנקים לניהול בנקאי תקין 367. יובהר כי הוראה זו פורסמה כיוזמה עצמאית של בנק ישראל.

[1] צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), תשס"א-2001 (להלן: צו הבנקים).

בעקבות תיקון הוראה 367 בראשית שנת 2018, הבנקים החלו בפועל בתהליך של פיתוח והטמעה של טכנולוגיה **חדשה** המאפשרת פתיחת חשבון בנק מרחוק באמצעות זיהוי בכלים ביומטריים של זיהוי פנים. זאת, תוך ביצוע בקרות שונות על די הבנק כמפורט בהוראה. בחודש אפריל 2019 הפיקוח על הבנקים התיר לחלק מהבנקים להתחיל לפעול באמצעות טכנולוגיה זו, כחלופה לזיהוי ואימות, וזאת כפיילוט מוגבל אשר לאחריו יוסקו מסקנות. היתר זה ניתן לאחר שהתקיימו דיונים שונים בנושא, הרחבה נמצאת במצע לדיון המצורף.

מטרת הישיבה היא לעדכן ולקיים שיח בסוגיות השונות שעלו עד כה במסגרת מתן ההיתרים על ידי בנק ישראל, וזאת הן בשל רצון וצורך של סקטורים פיננסים נוספים לאמץ שימוש בטכנולוגיות דומות והן בשל הצורך לחדד את המשך תהליך העבודה בנושאים אלו.

הוראת הפיקוח על בנקאי תקין 367.pdf | מכתב המלצות בנק - 25-3-2019.pdf | מצע לדיון טכנולוגיות 1305.docx

**עיקרי הדיון**:

**הצגת פעילות בנק ישראל (ע"י רונן ניסים, בנק ישראל)**: ההליך של פתיחת חשבון מרחוק החל בבנקים עוד בשנת 2014 בדרך של זיהוי באמצעות Video Conference בשילוב כלי זיהוי נוספים, כאשר פקיד בנק זיהה את הלקוח באמצעים אלה. לאור ההתפתחויות בעולם, הוחלט לפני כשנה לפעול על מנת לאפשר את ההליך בעזרת זיהוי טכנולוגי – קרי זיהוי שלא בזמן אמת על יד פקיד, אלא באמצעים טכנולוגיים. הזיהוי הטכנולוגי מתבצע בכך שאדם שחפץ לפתוח את החשבון, יכול להיכנס לאתר הבנק/אפליקציה, להזדהות באמצעות תעודת זהות שנסרקת לאפליקציה וכן צילום של סרטון פנים (המכונה "סרטון חיות"). התוכנה בודקת הן את תעודת הזהות והן את צילום הסרטון מבחינת תעודת הזהות, התוכנה שולפת את פרטי הזיהוי לפי מרשם האוכלוסין ומאמתת אותה מול הצילום.
ההיתר שניתן לבנקים הוא עד הפקת לקחים, שתתבצע בתום פתיחת 1000 חשבונות או חצי שנה, לפי המוקדם. כיום, רק בנק אחד עלה לאוויר (בנק Pepper).

**תיקוף ראייתי (יוני חדד, פרקליטות סייבר)**: בכניסת טכנולוגיה חדשה, בה נעשה שימוש ישיר על ידי גורמי האכיפה, ככלל נעשה הליך של תיקוף ראייתי. עם זאת, במקרה הזה, הוחלט **לקבוע עקרונות** בעיקר מאחר שלבנקים יש כמה טכנולוגיות שונות וכן הן משתנות כל הזמן. לא מדובר גם באמצעים טכנולוגיים שהמדינה עושה בהם שימוש באופן ישיר כגורמי אכיפה. הנחת העבודה היא כי במידה ויעבדו לפי העקרונות המוצעים, הפרקליטות תוכל לעשות בממצאים שימוש ראייתי בעתיד בעת הצורך.
כאשר בוחנים את ההליך החדש, העוסק בזיהוי מרחוק, ניתן לחשוב על סיכונים שונים: **הרתעה פחותה** – כאשר אדם יושב בבית יש פחות פחד לבצע את העבירה; **פיקוח של פקיד** – כאשר מגיע "קוף" שנשלח לפתוח חשבון בנק, הפקיד יכול לזהות את זה; **אפשרות טכנולוגית לזיוף הסרטון** – יכולה להביא לטענת הגנה שאדם אחר הוא זה שפתח את החשבון בעזרת זיוף הסרטון.



רח' צלאח א-דין 29, ת.ד. 49029, ירושלים מיקוד 9149001 ☎ 🖷 @ NetaGu@justice.gov.il

העקרונות שגובשו ניסו להתגבר על הסיכונים, והם פורטו בהרחבה במסמך שהועבר למחלקת יעוץ וחקיקה וצורף כמצע לדיון. בישיבה פורטו מספר עקרונות עיקריים: ראשית, התקשורת צריכה להיות **מאובטחת ומוצפנת**. חשוב כי הנתונים ישמרו בצורה מאובטחת, שגם לעובד בבנק לא תהיה גישה לנתונים, וכך הפרקליטות תוכל לבקש רשומה מוסדית על הנתונים. שנית, על הסרטונים וההליך להיות **מתועדים ולהישמר**. השמירה צריכה להיות בידיעת הלקוח ובהסכמתו, מטעמי פרטיות, אך עדין חייבת להיות שמירה של הנתונים כדי שנוכל להציג לשופט את הסרטונים והוא יוכל להתרשם. הובהר בהקשר זה, כי עולה קושי להסתמך על חוות דעת של גורם מומחה בלבד, נוכח אופי הטכנולוגיה המתבסס על בינה מלאכותית (מדובר במערכת ש"מלמדת את עצמה"). כמו כן, בשל הקושי האמור, לפני ביצוע פעולות בחשבון, יש צורך גם **במעבר אנושי של פקיד בנק** על הליך ההזדהות והסרטון שצולם. שלישית, יש **לזהות את מספר הפלאפון** בעזרת מספר סידורי או כתובת IP. רביעית, יש צורך ב**חוות דעת מומחה** שתבדוק את יכולות המערכת ואת הפוטנציאל לזיהוי שגוי.

**<u>סיכוני הלבנת הון ומשפט משווה (סבטלנה גרנר, הרשות לאיסור הלבנת הון)</u>**: הובהר כי הסטנדרט הבינלאומי הוא מאוד כללי ולא מחייב זיהוי פנים מול פנים, כמקובל בתחום הלבנת ההון מדובר ב**גישה מבוססת סיכון**. בהיבטים של משפט משווה, לאחר בדיקה של הרשות, עולה כי פתיחת החשבון מרחוק מתאפשרת בסינגפור, שוויץ, הונג-קונג ובאנגליה התהליך מתחיל, אך עדין אין חקיקה. הובהר כי במרבית המדינות בעולם הזיהוי מרחוק נעשה בזמן אמת על ידי גורם אנושי, או שנדרשת בקרה של גורם אנושי. כך למשל בשוויץ עדין יש צורך בבדיקה של גורם אנושי, אך ככה"נ יש תיקון חקיקה בנושא. מכל האמור עולה, כי תהליך זה בישראל, כמו גם השאלות שהועלו בו, הוא תקדימי בעולם.

**<u>שאלות/סוגיות משפטיות שעלו (דנה רוטשילד, ייעוץ וחקיקה):</u>**

ראשית, **שאלת הסמכות** להוצאת נוהל לזיהוי חלופי, שלא בדרך של פנים אל פנים. ישנם צווים חדשים, של רשות שוק ההון, בהם נקבעה סמכות מפורשת לקבוע נהלים לזיהוי חזותי, אך ישנם צווים ישנים הכוללים נוסחים שונים, כאשר לא כולם, ויתכן אף שרובם, אינם מאפשרים לרגולטור להסדיר חלופת זיהוי קבועה בנוהל. הובהר בהקשר זה, שגם ביחס לצו הבנקים, נדרש תיקון של הצו.

שנית, **פרטיות ומאגרי מידע**. כפי שהוצג, מחד, הועלה הצורך בשמירת סרטוני החיות, ומאידך השמירה של סרטונים באיכות גבוהה במאגרים בבנקים מעוררת קושי בהיבטים שונים של פרטיות. הקושי המרכזי שהועלה על ידי גורמי הפרטיות, הוא שהדבר נעשה בהוראת הרשות הציבורית – הרגולטור, נושא אשר לגישתם דורש הסמכה ברורה ומפורשת בחוק לשמירה של תיעוד ביומטרי. נקודת המחלוקת הייתה בשאלה האם די בהסכמה הקיימת בסעיף 7 לחוק איסור הלבנת הון, והצווים מכוחו, הקובע כי גופים פיננסיים ינהלו רישומים, בין היתר לגבי פרטי זיהוי, וישמרו עליהם לתקופה הקבועה בצו. הוצעה גם חלופה אפשרית, והיא בחינת אפשרות טכנולוגית ל"נעילה" של הסרטונים, באופן שלא יאפשר "לחלץ" מהם מידע ביומטרי.



רח' צלאח א-דין 29, ת.ד. 49029, ירושלים מיקוד 9149001 ☎ 🖷 @ NetaGu@justice.gov.il

הנושא הובא בפני רז נזרי, המשנה ליועץ המשפטי לממשלה (משפט ציבורי-חוקתי) אשר הנחה ראשית כל לברר ביחס לאפשרות ה"נעילה" הטכנולוגית, אשר ככל שתהיה אפשרית, מהווה את הפתרון המיטבי.[2] מקום בו לא קיימת אפשרות ריאלית כזו, כפי שהתברר, עמדתו של מר נזרי היא כי על אף הקשיים שהוצגו, לא ניתן לומר כי קיימת מניעה משפטית בשמירת סרטון ה"חיות", וזאת נוכח הוראת סעיף 7(א) לחוק איסור הלבנת הון, כמו גם אלמנט ההסכמה (שיידרש מהלקוחות, בהתאם לדין). יחד עם זאת, במקביל לקידום המתווה המוצע, הנחה מר נזרי לקדם תיקון חקיקה שיכלול סעיף של הסמכה מפורשת כפי שהוצע.

יודגש, מעבר לשאלת ההסמכה ישנם היבטים שונים ושאלות בהקשר של פרטיות העומדות בבסיס ההליך, סוגיות אלו יבוררו בהמשך בהשתתפות הגורמים הרלוונטיים העוסקים בתחום אשר גם לא נכחו בדיון.

שלישית, **תעודת זהות ביומטרית**. הפנו את תשומת ליבנו גם לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, תש"ע-2009. חוק זה אמנם עוסק במידע הנמצא ב"צ'יפ" שבתעודות הביומטריות, ואולם חשוב להכיר שבהיבטים אלו של תעודות ביומטריות עולים קשיים שונים. בין היתר, סעיף 29(ג) לחוק קובע עבירה פלילית על מי שעורך השוואה בין באמצעי הזיהוי הביומטרים בתעודה לבין אמצעי זיהוי ביומטרים שניטלו מאדם, בלא סמכות בחוק. כמובן, כלל הנהלים שיקבעו בהקשרים אלה צריכים להעשות על פי דין.

**<u>עקרונות בדיגיטל וחתימה דיגיטלית (רעות, ייעוץ וחקיקה אזרחי)</u>**: ככלל, יש לעודד מעבר לעולם הדיגיטלי. כשעוברים לעולם הדיגיטלי, יש לפעול לפי מספר עקרונות מנחים. אחד מהעקרונות הרלוונטיים לענייננו הוא **עקרון הניטרליות הטכנולוגית**. בהקשר דנן, על מנת ליישם עקרון זה, עדיף לקבוע עקרונות שיאפשרו גמישות עם ההתפתחויות הטכנולוגיות ולא לייצר תיקוף של טכנולוגיות ספציפיות (ישנן דרכים שונות להשגת ביטחון בעמידת הטכנולוגיה שנבחרת בעקרונות שנקבעים ע"י הרגולטור. למשל, דרישה לקבל חו"ד טכנולוגית מגורם שלישי, מתן אישור של רגולטור כי טכנולוגיה עומדת בעקרונות על בסיס בקשה, וכד'). עקרון נוסף שמנחה אותנו במעבר לעולם הדיגיטלי הוא **עקרון השקילות הפונקציונלית**, ולפיו יש לבחון מהם המאפיינים והתכליות הנדרשים בעולם הנייר וכיצד ניתן ליישם אותם בעולם הדיגיטלי. נקודת המוצא היא שהעולם הדיגיטלי אינו נחות מהעולם הפיסי ויש לנקוט בגישה גמישה, הבוחנת כיצד להמיר דרישה מהעולם הפיסי לעולם הדיגיטלי.

---

[2] יצוין בהקשר זה שלעמדת הפרקליטות ישנה הבחנה בין אפשרות של "**נעילה**" מפני ניתוח ביומטרי שאין במסגרתה "התעסקות" עם הסרטון, לבין **הפחתה**, **דגרגציה** וכיו"ב אשר אינם נותנים את המענה ועשויים לעורר קשיים להוכחת מהימנותו (ואולי אף קבילותו) של הסרטון. ההתייחסות המבוקשת היא ביחס לאפשרות ה"נעילה". עוד יצוין כי מבירור מול יחידת ההזדהות והיישומים הביומטרים במערך הסייבר הלאומי במשרד ראש הממשלה, עולה כי טכנולוגיות אלו קיימות ומוכרות, אולם הן אינן בשלות מאחר שהן נמצאות בשלבי פיתוח וככל הנראה אינן נמצאות בשלבי ביצוע או משולבות בפרויקטים מסחריים בעולם.



רח' צלאח א-דין 29, ת.ד. 49029, ירושלים מיקוד 9149001 ☎ 🖷 @ NetaGu@justice.gov.il

לעניין המונח "חתימה", בהתאם לעקרונות שפורטו לעיל, יש לבחון אילו כלים דיגיטליים יגשימו את תכליות החתימה במקרה דנן. בדרך כלל, נהוג לייחס לחתימה שלוש תכליות קלאסיות: זיהוי החותם, גמירת דעתו ביחס למסר שעליו חתם ונעילה של המסמך, כך שיהיה ניתן לדעת האם תוכנו שונה לאחר החתימה. ניתן לעשות שימוש בכל חתימה אלקטרונית שתגשים את התכליות הנדרשות, כתחליף לחתימה הפיסית על נייר.

לעניין הגשמת תכלית זיהוי החותם, יצוין כי על פי המדיניות הלאומית להזדהות בטוחה ישנן ארבע רמות מקובלות להזדהות, כאשר רמות 3 ו-4 נחשבות לרמות המספקות זיהוי ברמה גבוהה. יש לבחון בעניינו מהי רמת הזיהוי הנדרשת, בהתאם לסיכונים בנסיבות דנן.

יובהר, לעניין המונח "חתימת מקור", כי בעולם הדיגיטלי משמעות ה"מקור" אינה דומה למקור בעולם הפיסי. לכן, מסר שחתום בחתימה אלקטרונית יכול להיחשב כ"מקור", ובלבד שהסוג הנבחר של החתימה מגשים את תכלית המהימנות, שבדרך כלל מהווה התכלית לדרישת המקור.

**<u>סיכום הדיון</u>**:

לאחר הצגת הסוגיות וההיבטים הרלוונטיים שעלו מכלל הגורמים, בישיבה הבאה נדון בחלק השני, הצופה פני עתיד. הובהר, כי הסוגיה של זיהוי באמצעים טכנולוגיים היא רגישה ומורכבת ולכן יש להתקדם עקב בצד אגודל באימוץ עתידי של טכנולוגיות.

בברכה,
נטע גורי, סטודנטית
ייעוץ וחקיקה (משפט פלילי)

<u>העתק</u>:
המשנה ליועץ המשפטי לממשלה (משפט פלילי), הגב' עמית מררי.



רח' צלאח א-דין 29, ת.ד. 49029, ירושלים מיקוד 9149001 ☎ 🖷 @ NetaGu@justice.gov.il

רח' צלאח א-דין 29, ת.ד. 49029, ירושלים מיקוד 9149001 ☎ 🖷 @ NetaGu@justice.gov.il