2/3/2026

טכנולוגיות מתקדמות, פרטיות ואתגרי העתיד

עו"ד רבקי דב"ש, עמיתה בכירה, FPF – Israel

במהלך חודשי ינואר-פברואר 2026, קיימנו במסגרת המכון הישראלי למדיניות טכנולוגיה - FPF (Israel סדרה של שלושה וובינרים בנושא "טכנולוגיות מתקדמות, פרטיות ואתגרי העתיד". המפגש הראשון עסק במחשוב קוונטי, השני במידע ומדיה סינתטיים והשלישי בטכנולוגיית בלוקצ'יין. מסמך זה מבקש להציג בקצרה כל אחד מן הנושאים, לא רק כסיכום של הוובינר, אלא תוך הוספת רקע תיאורטי קצר לגבי מצב האסדרה בישראל, לצד התבוננות במסמכי מדיניות מרכזיים שפורסמו בעולם, מתוך רצון לייצר תשתית לשיח מקצועי רחב יותר בכל אחד מן התחומים.

מטבע הדברים, מסגרת הזמן והפורמט של הוובינרים אפשרו הצצה ראשונית בלבד לכל נושא, ואינם מתיימרים להציע סקירה מלאה של המרחב הטכנולוגי, המשפטי והחברתי. בחירת שלושת הנושאים נבעה מן התחושה כי טכנולוגיות אלו אינן זוכות בישראל לדיון מספק דרך הפריזמה של הגנת הפרטיות וזכויות נושאי מידע. נדגיש במיוחד כי סוגיית במידע ומדיה סינתטיים נידונה בהרחבה בהקשרים אחרים כגון טוהר הבחירות, מניפולציות תודעתיות ופרסום ממוקד, ואילו בסדרה זו ביקשנו למקד את הדיון בשאלות היסוד: מהו אופי הפגיעה בפרטיות הנגרמת משימוש בכלים אלו, אילו מודלים של אחריות מתאימים למציאות החדשה, ומהן דרכי ההגנה האפשריות.

אנו מקוות כי הוובינרים, יחד עם מסמך זה, יהוו תשתית ראשונית לשיח מעמיק ומבוסס יותר בישראל, הן בקרב קהילת הפרטיות והטכנולוגיה והן בקרב מקבלי החלטות ומובילי מדיניות בהקשרים דיגיטליים.

תוכן

1 - מפגש ראשון - מחשוב קוונטי 2
רקע 2
תמצית הוובינר 3
2 – מפגש שני - מידע ומדיה סינתטיים 6
רקע 6
תמצית הוובינר 7
3 – מפגש שלישי - בלוקצ'יין 11
רקע 11
תמצית הוובינר 12
4 - לסיום 14

1 - מפגש ראשון - מחשוב קוונטי

רקע

מחשוב קוונטי ניצב כיום על התפר שבין מחקר מדעי מתקדם לבין ניצנים של יישום. בעוד שבשיח הציבורי הוא לעיתים נתפס כהבטחה טכנולוגית רחוקה, הדיון המקצועי כבר מתמקד בשאלות קונקרטיות יותר: אילו מנגנוני הצפנה יוחלשו, מתי האיום יהפוך רלוונטי, וכיצד נכון להיערך כך שזכויות הפרט והאינטרס הציבורי לא ייפגעו.

אנשי הפרטיות נדרשים להערך לעידן הפוסט-קוונטי: להבין את התרחיש התיאורטי, את פוטנציאל הפגיעה שלו ברמת האבטחה של המערכות עליהם הם אמונים, וכן לנהל את הסיכון הנוכחי בהבנה שמתפתחת פרקטיקה של "אוספים היום, מפענחים מחר" (Harvest Now Decrypt Later).

בתחילת 2025 פרסם מערך הדיגיטל הלאומי הנחיה למשרדי הממשלה בדבר "מוכנות להתמודדות עם הצפנה בעידן המחשוב הקוונטי", הקוראת בראש ובראשונה למיפוי הנכסים, המערכות והתקשורות שבהן נעשה שימוש בהצפנה אסימטרית הנחשבת פגיעה למחשוב קוונטי. לצד מערך הדיגיטל, פועלים גם מערך הסייבר הלאומי ורגולטורים נוספים – לרבות שחקנים במגזר הפיננסי ובתחום התשתיות הקריטיות – לגיבוש קווי מדיניות ומסמכי המלצה, הנעים בין העלאת מודעות מקצועית לבין גיבוש תהליכי מעבר מדורגים למנגנוני הצפנה פוסט-קוונטיים במערכות חדשות וקיימות.

ברמה הבינלאומית, העידן הפוסט-קוונטי מקבל כבר ביטוי קונקרטי בסטנדרטים, בהמלצות ובהנחיות רגולטוריות. מכון התקנים האמריקאי (NIST) פרסם באוגוסט 2024 שלושה סטנדרטים ראשונים לקריפטוגרפיה פוסט-קוונטית, הן להצפנה והן לחתימות דיגיטליות, במסגרת פרויקט ה"פוסט-קוונטום קריפטוגרפיה". סטנדרטים אלו נועדו לאפשר לממשלות, ספקי ענן וארגונים גדולים להתחיל במעבר מדורג לפרוטוקולים עמידים למחשוב קוונטי בתהליך רב שנתי.

במסמך TechDispatch #2/2020 על מחשוב קוונטי והצפנה, הפיקוח האירופי על הגנת נתונים (EDPS) מדגיש כי מחשוב קוונטי עתידי עלול לאפשר שבירת הצפנה במפתח ציבורי ולהחליש מנגנוני אבטחה מרכזיים. אי הוודאות לגבי מועד הופעת מחשבים כאלה יוצרת כבר היום סיכון של "אוספים היום, מפענחים מחר" למידע אישי רגיש, במיוחד כזה שיש לו ערך לאורך זמן. לכן ארגונים נדרשים להביא זאת בחשבון במסגרת ניהול הסיכונים תחת ה-GDPR ולהתכונן בהדרגה למעבר לקריפטוגרפיה פוסט-קוונטית, תוך הסתמכות על תהליכי תקינה וניתוח סיכונים קיימים. מסמך זה מתמקד בניתוח הסיכון ובצורך בהיערכות, אך אינו מהווה מפת דרכים מחייבת או תכנית פעולה לתשתיות קריטיות ואבטחת תקשורת.

במקביל, מסמכים אחרים של מוסדות האיחוד, ובראשם המלצת הנציבות האירופית על יישום קריפטוגרפיה פוסט-קוונטית ועל תיאום מעבר של מדינות החברות, כולל בהקשר של תשתיות קריטיות ורשתות תקשורת, קובעים קווים מנחים אופרטיביים יותר למעבר מתואם, לקביעת

לוחות זמנים, למיפוי נכסים קריפטוגרפיים ולניהול תהליך ההחלפה במערכות קריטיות ברמת מדינה וברמת האיחוד.

הוובינר הראשון בסדרת המפגשים של המכון הישראלי למדיניות טכנולוגיה בנושא טכנולוגיות מתקדמות ופרטיות, הוקדש למחשוב קוונטי ולהשלכותיו על הגנת המידע.

תמצית הוובינר[1]

בוובינר השתתפו פרופ׳ אור דונקלמן ומר יובל ריצ׳לר.

דונקלמן הוא פרופ׳ למדעי המחשב בפקולטה למדעי המחשב והמידע באוניברסיטת חיפה, מומחה לקריפטוגרפיה וקריפטואנליזה. הוא היה מעורב בפרויקט המחקר של האיחוד האירופי PQCRYPTO שעבד על בניית התשתית המדעית להצפנה בטוחה בעידן של מחשבים קוונטים, והיה ממייסדי עמותת פרטיות ישראל.

ריצ׳לר הוא ראש יחידת החדשנות של מערך הדיגיטל הלאומי. ריצ׳לר הוא בעל ניסיון עשיר בפיתוח, ניהול פיתוח ומנהל אופרציה בשוק הפרטי. עם תחילת הקורונה, עבר לשירות הציבורי, ולפני כשלוש שנים הצטרף ליחידת החדשנות.

את הוובינר הנחתה עו״ד רבקי דב״ש, כותבת מסמך זה.

בוובינר ביקשנו לשים במרכז טכנולוגיה שעדיין אינה ״מוצר מדף״, מתוך רצון להסתכל קדימה, ולהערך לעתיד. ביקשנו להבין כיצד מחשב קוונטי מאתגר את עקרונות ההצפנה, האימות והזהות הדיגיטלית, ולמפות מה המשמעויות עבור מדינות, ארגונים ואנשי פרטיות הפועלים היום במערכות שנבנו לעידן טרום-קוונטי.

בחלקו הראשון של המפגש הסביר פרופ׳ דונקלמן, שמחשוב קוונטי צמח במקור מן ההבנה שמערכות קוונטיות מורכבות אינן ניתנות לסימולציה יעילה במחשבים קלאסיים. במקום לעבוד על ערך יחיד המשתנה לאורך זמן, החישוב הקוונטי ״משנה הסתברויות״: הוא מחזיק בו-זמנית מצבי מידע רבים, ומנסה לעצב את ההתפלגות כך שהמדידה תניב בהסתברות גבוהה את התשובה הנכונה. הוא הדגים זאת באמצעות דימוי של בדיקת סיסמאות שבה מחשב קלאסי נדרש לעבור סיסמה-סיסמה, בעוד שמחשב קוונטי מסוגל, ברמה העקרונית, ״להחזיק בידו״ את כל האפשרויות כך שהחישוב יתכנס לפתרון.

עם זאת, פרופ׳ דונקלמן הדגיש שהמרחק בין התיאוריה לבין המציאות ההנדסית עדיין משמעותי. מחשבים קוונטיים בני זמננו סובלים משלוש מגבלות עיקריות:

[1] הכתוב כאן מהווה תקציר של עיקרי הדברים מהוובינר, למבקשים להעמיק בנושא מוצע לצפות בוובינר המלא בקישור הזה.

1. מספר קיוביטים מצומצם יחסית (גם המחשבים המתקדמים ביותר מגיעים לליבות בודדות עד עשרות רבות);
2. זמן קוהרנטיות קצר שבו ניתן לשמור את מצב החישוב לפני שה״רעש״ הפיזיקלי מפריע;
3. מורכבות הנדסית עצומה של קירור, אנרגיה ותפעול.

מאז 2019 נרשמה התקדמות ניכרת ביישימות של מחשוב קוונטי. אולם, להערכתו של פרופ׳ דונקלמן, עדיין נדרשת קפיצת דרך טכנולוגיות על מנת שמחשוב קוונטי יהפוך לאיום מעשי רחב היקף על הצפנה בשימוש יומיומי. גם לאחריה, יחלוף זמן עד שיישומים כאלה יהיו זמינים לצרכים אזרחיים רחבים.

במישור הקריפטוגרפי, דונקלמן הבחין בין השפעת המחשוב הקוונטי על הצפנה סימטרית לבין השפעתו על הצפנה אסימטרית. הצפנה סימטרית (כגון: סיסמאות ומפתחות משותפים), נחלשת במובן של קיצור החיפוש על מרחב המפתחות (באמצעות אלגוריתם גרובר). ניתן לפצות על חולשה זו באמצעות הארכת המפתחות והסתמכות על סטנדרטים שכבר תוכננו מראש לעמידות קוונטית. לעומת זאת, האלגוריתמים האסימטריים הנפוצים כיום (כגון RSA ווריאנטים של דיפי־הלמן), פגיעים הרבה יותר.

המשמעות היא שביום שבו יעמוד לרשות שחקן עוין מחשב קוונטי מתאים, ניתן יהיה לשבור, גם בדיעבד, תקשורות שהוקלטו והוצפנו היום. כאן טמון האיום המובהק ביותר על פרטיות: כל מי שמקליט כיום תעבורה מוצפנת, ושומר אותה, עשוי בעתיד לפענח אותה ולהיחשף למידע אישי שהיה אמור להישאר חסוי לאורך שנים (Harvest Now Decrypt Later).

בנקודה זו חיבר פרופ׳ דונקלמן את הדיון התיאורטי לכלים מעשיים של הגנת פרטיות. הוא הצביע על כך שמנגנונים כמו פרטיות דיפרנציאלית נבנו מלכתחילה כך שיהיו בלתי תלויים בכוח החישוב של התוקף, ולכן הם אינם נחלשים באופן מהותי בפני מחשוב קוונטי, וזאת בניגוד לטכניקות התממה (אנונימיזציה) אחרות, שעלולות להפוך לפגיעות יותר ככל שכוח החישוב גדל. לדבריו, חלק מהאתגר של קהילת הפרטיות הוא להבחין בין כלי הצפנה שתוכננו מראש כעמידים למחשוב קוונטי, ולהימנע מהתפיסה כי מחשב קוונטי ישבור כל הצפנה.

בחלקו השני של הוובינר הציג מר ריצ׳לר את זווית הראייה של מערך הדיגיטל הלאומי ונתן הצצה קצרה להערכות הממשלה לעידן הפוסט-קוונטי. ריצ׳לר תיאר את יחידת החדשנות כגוף שעוסק במבט קדימה: זיהוי טכנולוגיות שעשויות להיות רלוונטיות לממשלה בעוד כמה שנים, ובחינה אם ומתי יש הצדקה להתחיל לייצר תנועה ושינוי במערכות מורכבות. לדבריו, לאורך שנים נבחן הנושא מתוך הבנה שמחשוב קוונטי עדיין רחוק ממימוש, אולם בסוף 2024 ותחילת 2025 התגבשה במערך התפיסה שקבועי הזמן מתקצרים, ושיש מקום לעבור משלב של מעקב אקדמי לשלב של הנחיה מסודרת למשרדי הממשלה.

ההנחיה שפורסמה בפברואר 2025 ממוקדת בשני מהלכים עיקריים: העלאת מודעות והכרת האיום, ומיפוי שיטתי של שימושי הצפנה במערכות הממשלתיות. ריצ׳לר הסביר כי ללא מיפוי של

המערכות, הפרוטוקולים, סוגי החתימות הדיגיטליות והנתונים בעלי הערך ארוך הטווח – לא ניתן יהיה בעתיד לתכנן מעבר מדורג לקריפטוגרפיה פוסט-קוונטית, או להחליט היכן יש הכרח להקדים ולהשקיע. ההנחיה משתלבת בעבודת מערך הסייבר הלאומי, שהוציא בעבר מסמכים רחבים יותר לשוק כולו, ובשיח שוטף עם גורמים ביטחוניים, אקדמיים ותעשייתיים, במטרה ליצור תמונה קוהרנטית של האיום ושל אופק ההבשלה הטכנולוגי.

ריצ׳לר השתמש באנלוגיה של באג 2000 כדי להסביר את גישת המוכנות: אז, הוגדר תאריך יעד ברור, בוצעה עבודת מיפוי מסיבית, והמערכות תוקנו מבעוד מועד כך שהאירוע נתפס בדיעבד כ״היסטריה מיותרת״. עם זאת, ההתראות וההערכות, הן אלו שמנעו כשלים חמורים. בעידן הפוסט-קוונטי אין תאריך יעד ידוע, אך ההיגיון דומה: ללא היערכות מוקדמת ומדורגת,

הרגע שבו מחשוב קוונטי יהפוך למשמעותי עלול להפתיע מערכות שלא נערכו בזמן. מכאן נובעת האחריות של גופי מדינה, אבל גם של בעלי תפקידים בארגונים פרטיים. עליהם להתחיל כבר היום בניהול סיכונים קוונטי: לבחון איזה מידע חייב להישאר סודי לאורך שנים, אילו מערכות קריטיות נשענות על הצפנה פגיעה, והיכן נכון לשלב כבר עכשיו פתרונות וסטנדרטים פוסט-קוונטיים.

הוובינר נחתם במסר מאזן - בעת הזו אין הצדקה לפאניקה ציבורית או להקצאת משאבים בלתי מידתית לשדרוג מיידי של כל מערכת, אך גם אין מקום להמתין בשאננות עד הרגע האחרון בו יוודע על יישומו של מחשוב קוונטי. עבור אנשי פרטיות ומדיניות, המשמעות המעשית היא להכניס את המחשוב הקוונטי אל תוך שגרת החשיבה על סיכונים, לשאול שאלות קונקרטיות על פרקטיקות הצפנה, על אורך חיי המידע ולהמשיך לעקוב אחרי סטנדרטים ופרסומי רגולטורים בארץ ובעולם.

---

2 – מפגש שני - מידע ומדיה סינתטיים

רקע

דיסאינפורמציה, מידע ומדיה סינתטיים הפכו בשנים האחרונות לאחד מצירי המתח בין חדשנות דיגיטלית להגנת פרטיות, אמון ציבורי וחוסן דמוקרטי. מצד אחד, אותם כלים עצמם יכולים לשמש להגברת פרטיות - לדוגמה באמצעות יצירת מידע סינתטי לצרכי מחקר והדגמה במקום שימוש במידע אישי מזוהה; מצד שני, אותם מנגנונים בדיוק מאפשרים לייצר בקלות יחסית ובעלויות נמוכות דמויות משכנעות, קמפיינים ממוקדים ותכנים ויזואליים או קוליים שנראים אותנטיים, אך מבוססים על מניפולציה של נתונים ביומטריים, העדפות אישיות ופגיעות חברתיות.

ברמה המושגית ניתן לחלק את הפגיעה הפוטנציאלית הנובעת משימוש בדיסאינפורמציה, מידע ומדיה סינתטיים לשני סוגים עיקריים:

1. **<u>פגיעה בי כנושא המידע</u>** - כאשר נלקחים נתונים אמיתיים אודותיי (תמונה, קול, מידע אישי) ונעשה בהם שימוש לייצר ייצוג שונה של דמותי. במקרה זה נפגעת השליטה העצמית שלי במידע עליי ובאופן שבו אני מוצג/ת בציבור. במספר מדינות כבר מתפתח המושג של "זכות התדמית" כדרך להתמודד עם מורכבות זו[2].
2. **<u>פגיעה בי כמושא המידע</u>** - כאשר נעשה שימוש במידע אישי אודותיי כדי להציע לי פרסום או תעמולה מוכוונת אישית. במקרה זה, הפגיעה אינה רק בעצם השימוש בנתונים, אלא גם באוטונומיה האישית שלי, שהיא אחת ההצדקות המרכזיות לזכות לפרטיות, משום שהיא מקשה עליי לזהות ולהתמודד עם הטיות נסתרות. כך, לדוגמה, שקיפות לגבי מי יצר את המידע (X) ולאיזו מטרה (Y) היא תנאי בסיסי ליכולת הזו.

בישראל, המענה הרגולטורי הישיר לשילוב של דיסאינפורמציה, מידע ומדיה סינתטיים ופרטיות עדיין נמצא בראשית דרכו, והוא מתפצל, דה-פקטו, בין כלים קיימים מתחומי המשפט הפלילי, לשון הרע, הגנת הצרכן והגנת הפרטיות.

נכון למועד זה (פברואר 2026), הרשות להגנת הפרטיות טרם פרסמה מסגרת רגולטורית מקיפה המוקדשת לכל ההיבטים של מידע ומדיה סינתטיים, ודיון זה נשען במידה רבה על ההוראות הכלליות של חוק הגנת הפרטיות, תקנות אבטחת המידע והנחיות הרוחב לגבי מערכות בינה מלאכותית, פרופיילינג ושימוש משני במידע אישי.

עם זאת, הרשות פרסמה בשנים האחרונות שני מסמכים שיש להם חשיבות מיוחדת בנושא זה. הראשון, מסמך מדיניות בנושא "<u>פרטיות ואבטחת מידע בשימוש בטכנולוגיות Deepfake (זיוף עמוק)</u>", בו הבהירה כי הפצה ללא הסכמה של סרטוני ותמונות דיפ-פייק העלולים להיתפס כאותנטיים – במיוחד כאשר מדובר בתוכן משפיל או אינטימי – מהווה פגיעה בפרטיות והפרה של

[2] לדוגמה: בספרד "זכות התדמית" / "הזכות לדימוי עצמי" מעוגנת, בין היתר, <u>בחוקה</u> (סעיף 18.1); בקליפורניה הוכרה הזכות ל-Publicity ב-<u>California Civil Code §3344</u>; ובאיטליה <u>סעיף 10 בקוד האזרחי</u> מגן על הזכות לשימוש בתמונה של אדם ללא הסכמתו.

חוק הגנת הפרטיות. כמו כן נקבע במסמך כי גם מידע מזויף שנחזה להיות מידע אישי אמיתי מחייב כפוף לחובות מכח תקנות אבטחת המידע. השני, הוא התייחסות לנתונים סינתטיים במסגרת "מדריך לטכנולוגיות מגבירות פרטיות (PETs)" שבו הוכרו במפורש נתונים סינתטיים כאחד מכלי הליבה להפחתת סיכוני זיהוי, לצד התממה ופרטיות דיפרנציאלית.

על אף התייחסות ממוקדת זו, ההנחיות הקיימות אינן נותנות בשלב זה מענה מלא למכלול הסוגיות הרחב של קמפיינים תודעתיים, תרגוט פוליטי והאחריות המערכתית של הפלטפורמות.

לצד זאת, גופים מקצועיים, כמו איגוד האינטרנט הישראלי, ממלאים תפקיד הולך וגדל בהפעלת מנגנוני "קו סיוע" ותיווך מול פלטפורמות כגורמי דווח מהימנים כמו גם קידום יוזמות מדיניות להתמודדות מוצלחת יותר עם קמפיינים הונאתיים המבוססים על מדיה סינתטית.

ברמה הבינלאומית, השיח הרגולטורי סביב מידע ומדיה סינתטיים מתחיל להתגבש לכדי מסגרות מחייבות. האיחוד האירופי קבע במסגרת ה- AI Act חובות שקיפות מפורשות לגבי דיפ-פייקים ותוכן שנוצר או עבר מניפולציה באמצעות בינה מלאכותית, לרבות דרישה לסימון ברור של תוכן כמלאכותי, והטלת אחריות הן על המפתחים והן על המפעילים של מערכות אלה. במקביל, חוק השירותים הדיגיטליים (DSA) מחייב פלטפורמות גדולות לזהות ולטפל בסיכונים מערכתיים הנובעים מתוכן כוזב, לרבות דיסאינפורמציה ותוכן סינתטי, ומאפשר הליכי פיקוח ואכיפה רחבים מול חברות להן חשבון בהיקף של מעל 10% מהאוכלוסיה באירופה (לדוגמה: מטא ו-X).

מדינות נוספות, בהן דנמרק, בריטניה, וקוריאה הדרומית, מקדמות תיקוני חקיקה ייעודיים בתחום דיפ-פייקים אינטימיים, תוך שימוש בשילוב של דיני זכויות יוצרים, עבירות מין וחובות הסרה מהירה של תכנים פוגעניים. לאחרונה נכנס תיקון מקיף בהודו, המחייב מהרשתות להסיר את התכנים הפוגעניים בתוך 3 שעות (מה שמעלה גם שאלות של חשש מצנזורה – שלא נרחיב לגביהם כאן). מדינות אלו ממקמות את המידע והמדיה הסינתטיים לא רק כתופעת תוכן, אלא כאתגר ליבה למשפט הפרטיות, להגנת הגוף והזהות הדיגיטלית, תוך ניסיון להוביל באמצעות הרגולציה לפיתוח מנגנוני אחריות של פלטפורמות גלובליות.

תמצית הוובינר[3]

בוובינר השתתפו מר עידן רינג וד"ר אסף וינר, שניהם מאיגוד האינטרנט הישראלי.

עידן רינג הוא סמנכ"ל קהילה וחברה באיגוד, חוקר ומרצה לתקשורת באוניברסיטת בן-גוריון בנגב, שעוסק בפייק ניוז, דיסאינפורמציה והונאות מקוונות ובהשפעת הרשתות החברתיות על אמון ציבורי, על מרחב השיח ועל חוסן דמוקרטי.

[3] הכתוב כאן מהווה תקציר של עיקרי הדברים מהוובינר, למבקשים להעמיק בנושא מוצע לצפות בוובינר המלא בקישור הזה.

ד״ר אסף וינר הוא סמנכ״ל רגולציה ומדיניות ציבורית באיגוד, ומרצה לדיני תקשורת ואינטרנט באוניברסיטת תל-אביב, מומחה למשפט וטכנולוגיה ולמסגרות הרגולציה החדשות שמסדירות פלטפורמות ורשתות חברתיות בעולם.

את הווביינר הנחתה עו״ד רבקי דב״ש, כותבת מסמך זה.

ד״ר וינר פתח במיפוי מושגי של השדה: הבחנה בין מיס-אינפורמציה - הפצת מידע שגוי ללא כוונה להטעות, לבין דיס-אינפורמציה - בה מתקיימת כוונה מודעת ליצור נזק, בין אם אישי, ביטחוני או פוליטי. הוא הגדיר ״מידע סינתטי״ כחומר נתונים שנראה כמו תיעוד של המציאות, אך למעשה נוצר באופן מלאכותי על בסיס אלגוריתמים.

הקושי הוא בשרטוט הגבול בין יצירה בדיונית לגיטימית לבין ייצוג שנחווה על ידי הצרכן כעובדתי. החיבור בין דיסאינפורמציה למדיה ומידע סינתטיים, לדבריו, יוצר שכבה חדשה של סיכון: לא רק מידע לא נכון, אלא מציאות מדומה שנראית מדויקת ומותאמת אישית, תוך שימוש בכלים של בינה מלאכותית, קלונינג קולי ודיפ־פייקים.

רינג מיקם את הדיון בהקשר הישראלי המוסדי והחברתי, דרך פעילות איגוד האינטרנט הישראלי. האיגוד, שהחל את דרכו כמנהל שמות המתחם בסיומת ״IL״, התפתח לגוף שמחבר בין תפעול תשתיות אינטרנט לבין הגנה על זכויות משתמשים, חינוך לשימוש מוגן ומחקר על תופעות ברשת.

קו הסיוע לאינטרנט בטוח המופעל על ידי האיגוד, הוכר על ידי פלטפורמות כגורם דיווח מהימן, וטיפל במשך שנים בעיקר בהטרדות, בריונות, התחזות והונאות מקוונות; אולם, מאז ה-7 באוקטובר 2023, הפך גם לזירת התמודדות עם דיס-אינפורמציה, תכנים סינתטיים ואלימות תודעתית כחלק מהחזית הדיגיטלית של המלחמה.[4]

רינג הציג דוגמאות קונקרטיות לשימוש במדיה סינתטית. הוא הדגיש כי חלק משמעותי מהתכנים המזיקים כלל לא ״סינתטי״, אלא תמונות וסרטונים אמיתיים ממקומות וזמנים אחרים שהוצבו בהקשר מטעה - מה שמחדד את הקושי המושגי והמעשי בהבחנה בין ״פייק״ ל״אמיתי״. לצד זאת, הוא תיאר תופעה הולכת ומתרחבת של קמפיינים מסחריים והונאות המתבססים על דמויות סינתטיות, פרופילים מזויפים ותוכן שנועד בעיקר לייצר אנגייג׳מנט ולסמן קהלי יעד לצרכים שיווקיים, פוליטיים ואחרים.

אחד המוקדים המרכזיים בדבריו היה ״AI Slope״, שימוש בתמונות סינתטיות שנועדו להפעיל מניפולציה רגשית ולמשוך לידים, לרוב למטרות מסחריות או הונאתיות. רינג הדגים כיצד תמונות שנראות ״ישראליות״, מקומיות ואותנטיות, משמשות כפיתיון בקבוצות ווטסאפ ופייסבוק קהילתיות, כדי לאסוף מידע על משתמשים ולהכניסם למעגלי פרסום, השקעות מפוקפקות או מיזמים אידאולוגיים. בכך, מדיה סינתטית הופכת לכלי שמבוסס על נתוני פרט מזהים ועל

[4] ראו את המחקר של איגוד האינטרנט הישראלי בנושא ״מייריטים פייקים: דיסאינפורמציה ומאמצי בדיקת עובדות במהלך מלחמת ישראל-איראן״ ניצן יסעור, עידן רינג ויעל רם (2025)

פרופילים פסיכוגרפיים, ומייצר פגיעה כפולה: גם בדמות של מי שעליה מבוסס הקמפיין (גם ללא ידיעתה ובהסכמתה), וגם בפרטיות ובאוטונומיה של מי שמתורגט.

רינג הרחיב גם על שימושים גוברים בבינה מלאכותית ליצירת דיפ-פייקים מיניים והטרדות מגדריות, במיוחד בקרב בני נוער ובחברה הערבית. הוא תיאר כיצד תמונות אמיתיות של נערות, נשים ומורים נאספות מהרשת, מעובדות באפליקציות ייעודיות ליצירת תמונות עירום או תוכן מיני, ומופצות בקבוצות סגורות לשם שיימינג, הכפשה ואף סחיטה. לטענתו, מדובר בהסלמה של תופעות מוכרות של אלימות מגדרית ברשת, אך עם עוצמת נזק חדשה הנובעת משילוב של ביומטריה, בינה מלאכותית והפצה ויראלית, בעוד המערכת המשפטית עדיין מתקשה להדביק את קצב השינוי.

על רקע זה, דיברו רינג ווינר על התרגוט כקשר משמעותי בין מידע ומדיה סינתטיים לפרטיות. נתונים אישיים כגון: גיל, מגדר, מקום מגורים, מצב בריאותי והשקפות פוליטיות, הופכים לחומר הגלם שמאפשר לא רק למכור מוצר, אלא לבנות לכל אדם גרסת תוכן מותאמת: דמות, סיפור, טקסט או סרטון שנראים כאילו הם מדברים בשפתו של הפרט. ד"ר וינר הדגיש שהחידוש אינו בעצם הרצון לשכנע. פרסום ותעמולה תמיד התקיימו. אלא, ברמת הדיוק וחוסר השקיפות: מי שצופה בתוכן אינו יודע שהוא רואה גרסה ייחודית שנבנתה על בסיס נתוניו, ואינו יכול להשוות את המסר לגרסאות אחרות, לבקר אותו או להתגונן מפניו.

בחלק המשפטי הציג וינר את ארגז הכלים הקיים והמתפתח בישראל ובעולם להתמודדות עם מידע ומדיה סינתטיים. הוא הזכיר כי דינים מסורתיים, כגון: הונאה, התחזות, לשון הרע והפרת הפרטיות, ממשיכים לחול, אך מתקשים לעמוד בקצב ההפצה, האנונימיות והבינלאומיות של הפלטפורמות. לכן, חלק גדל מהמאמץ המשפטי מופנה היום כלפי הפלטפורמות עצמן, באמצעות תביעות ייצוגיות, חובות זהירות ורשלנות, והטענה כי החזקת מנגנוני תרגוט, פרסום ותכנים סינתטיים ללא מנגנוני בקרה מספקים מהווה כשלעצמה הפרה של סטנדרט ראוי.

ד"ר וינר הציג בקצרה את מגמות ההסדרה באירופה, ה-DSA וה-AI Act, כמסגרות שמנסות לבסס אחריות מערכתית של פלטפורמות ומפתחי מערכות בינה מלאכותית באמצעות ניהול סיכונים, סימון תכנים, מנגנוני דיווח והסרה והטלת סנקציות משמעותיות על אי עמידה בדרישות. הוא הזכיר דוגמאות לפתרונות חדשניים, כמו הצעת דנמרק להעניק זכויות יוצרים על הדמות (likeness) של אדם כדי להקל על הסרה ואכיפה נגד דיפ-פייקים, או הרחבת עבירות מין במדינות שונות כך שיכללו גם יצירה והפצה של דיפ-פייקים אינטימיים ללא הסכמה.[5] בעיניו, אלה אינן פתרונות מושלמים, אך הן מדגימות חשיבה יצירתית על שימוש במנגנונים קיימים (זכויות יוצרים, אחריות פלטפורמות, עוולות נזיקיות) כדי לתת מענה מהיר יחסית לאיומים חדשים.

[5] ראו גם "יוזמות חקיקה נגד דיסאינפורמציה ו-fake news: סקירה בינלאומית" (איגוד האינטרנט הישראלי, 2024)

לקראת סיום, נשאלו הדוברים כיצד נכון לישראל להתקדם רגולטורית, מתוך פרספקטיבה ממוקדת פרטיות. ד״ר וינר הציע להכיר במגבלות הגודל והכוח של השוק הישראלי ביחס לחברות הטכנולוגיה, ולהתמקד בכמה צירים מעשיים:

1. חיזוק האחריות של הפלטפורמות הדומיננטיות בישראל;
2. קידום תביעות פרטיות וייצוגיות ככוח משלים לרגולציה;
3. עידוד שיתופי פעולה בין רגולטורים שונים (פרטיות, הגנת הצרכן, תקשורת, אכיפה פלילית) סביב מטרות משותפות במקום טיפול סקטוריאלי מפוצל.

בה בעת, הוא הצביע על פער בין רמת ההגנה שמקבלים תכנים בתחום זכויות היוצרים לבין הטיפול בתכנים הפוגעים בפרטיות ובכבוד האדם. פער שעלינו לתת עליו את הדעת בבואנו לעצב הסדרים ישראליים לעידן המידע והמדיה הסינתטיים.

הווביינר נחתם בקריאה לאנשי פרטיות, משפט ומדיניות להרחיב את הפריזמה מעבר לשאלת האמת והשקר, אל השאלות כגון: מי מייצר את התוכן, באילו נתונים אישיים נעשה שימוש וכיצד משפיע המודל העסקי של הפלטפורמות על היקף הפגיעה. המשתתפים הדגישו כי ההתמודדות עם דיסאינפורמציה, מידע ומדיה סינתטיים מחייבת להפוך תחומים אלו לחלק אינטגרלי משיח הפרטיות, הזכויות הדיגיטליות והדמוקרטיה, בישראל ובעולם.

3 – מפגש שלישי - בלוקצ'יין

רקע

טכנולוגיית הבלוקצ'יין מציבה את הפרטיות במקום מורכב: היא בנויה על שקיפות קיצונית ויומן עסקאות ציבורי, אך משלבת פוטנציאל טכנולוגי עמוק ליצירת מנגנונים שמגינים על זהות, על תוכן הנתונים ועל האוטונומיה של המשתמשים. מחד, יש כאן תשתית פיננסית-טכנולוגית שמעצם טבעה מאפשרת מעקב אחר דפוסי פעילות, קשרים בין כתובות ושחזור היסטוריית עסקאות, מאידך, אותה תשתית עצמה (ובפרט תשתית העושה שימוש בהוכחות באפס ידיעה), יכולה לשמש כבסיס לעולם שבו ישנה רמת מהימנות גבוהה מבלי לחשוף מידע רגיש - וכך לייצר פרטיות ברמה שלא הייתה אפשרית במערכות ריכוזיות.

ההשלכות הרגולטוריות לאכיפת הסדרים בתחום הגנת הפרטיות, נוגעות לזיהוי "בעל השליטה" במידע, לשאלת קיומו של מאגר (רלוונטי רק לישראל ולמספר מדינות מצומצמות), ולדרך מימוש זכויות נושאי מדע בדגש על זכות התיקון וזכות המחיקה (שטרם הוכרה בישראל). כמו כן, יש לבחון את היכולת של הטכנולוגיה להוות כלי יישומי כטכנולוגיה מקדמת פרטיות (PET).

נכון למועד כתיבת שורות אלו (פברואר 2026), הרשות להגנת הפרטיות בישראל לא פרסמה הנחיה ייעודית או עקיפה לטכנולוגיית בלוקצ'יין, ואכיפת הדין נעשית מכוח ההוראות הכלליות של חוק הגנת הפרטיות, תקנות אבטחת המידע והנחיות רוחב אחרות

עם זאת, בשיח הפרטיות הבינ"ל, בלוקצ'יין מתחיל להשתלב בדיון רחב יותר על (PETs), במיוחד כאשר הוא משולב עם הוכחות באפס ידיעה (ZKP) ופתרונות הצפנה מתקדמים. לצד רגולציה פיננסית ייעודית, מתפתחת גם ספרות רגולטורית ומדיניותית שרואה בבלוקצ'יין תשתית אפשרית לניהול זהויות, תיקים רפואיים ויחסי אמון בין ארגונים – תוך מינימום חשיפה של נתונים אישיים.

בהקשר האירופי, המסמך המרכזי שבוחן את דרך ההטמעה של הוראות ה-GDPR בבלוקצ'יין, פורסם על ידי ה-EDPB באפריל 2025, ומצוי עדיין בגרסת נוסח להערות הציבור. ההנחיות המוצעות שעניינן עיבוד מידע אישי באמצעות טכנולוגיות בלוקצ'יין, מתחילות בהסדר נהיר על הטכנולוגיה, תוך זיהוי הבעיות והאתגרים שהיא מציבה לתחום הפרטיות ובמרכזן רמת השקיפות הגבוהה של הטכנולוגיה, חוסר יכולת למחוק נתונים והצורך להגדיר לצורך הוראות הדירקטיבה, מיהו בעל השליטה.

נוסף על המשגת התהליך הטכנולוגיה בהגדרות של הדירקטיבה, והקביעה כי שימוש בבלוקצ'יין אינו פוטר מהטמעת ויישום החובות מכח הדירקטיבה, ה-EDPB מציגים את השימוש בבלוקצ'יין העושה שימוש ב-ZKP כטכנולוגיה שעשויה להגביר את הפרטיות – אם כי האמירות שלהם בנושא נכתבות בזהירות ולא בהחלטיות. לשיטתם השימוש ב-ZKP דורש יישום נכון ומבוקר. זהו כלי שיכול לסייע בהגנה על הפרטיות, אולם האחריות היא על controller להוכיח שבפועל מתקיימים עקרונות כמו צמצום המידע, הגבלת תקופת השמירה וזכויות נושאי מידע.

תמצית הוובינר[6]

בוובינר התארח פרופ׳ אלי בן-ששון.

פרופ׳ בן-ששון הוא מייסד-שותף ומנכ״ל של StarkWare תעשיות, ומהדמויות המרכזיות בעולם בפיתוח פרוטוקולי STARK - טכנולוגיות הוכחה קריפטוגרפיות המאפשרות אימות חישובים בקנה מידה רחב, מבלי לחשוף את המידע עצמו. בן-ששון הוא פרופסור לשעבר למדעי המחשב בטכניון, וחוקר למעלה משני עשורים בתחומי קריפטוגרפיה, Zero-Knowledge Proofs (הוכחות באפס ידיעה) ושלמות חישובית. הוא ממפתחי פרוטוקולי STARK ו-FRI, ומהמדענים המייסדים של חברת Zcash - אחד המיזמים הראשונים שהדגימו יישום מעשי של הוכחות אפס-ידע במערכת פיננסית מבוזרת.[7]

את הוובינר הנחתה עו״ד רבקי דב״ש, כותבת מסמך זה.

פרופ׳ בן-ששון פתח במבוא טכנולוגי קצר לבלוקצ׳יין ולשאלות הפרטיות שהוא מעלה. לדבריו, בלוקצ׳יין הוא אוסף פרוטוקולים שרצים על גבי האינטרנט ברשת, peer-to-peer, ללא מתווכים ריכוזיים כמו בנקים או מוסדות ממשל, ומאפשרים לנהל נכסים דיגיטליים. הוא תיאר שלושה עקרונות יסוד של בלוקצ׳יין:

1. כל אחד יכול להצטרף ולהפעיל את הרשת;
2. המערכת מתגמלת את המפעילים כדי לשמר יושרה ויציבות (incentivized integrity);
3. כל מה שקורה על הרשת מתועד באופן שקוף וזמין לכל, כולל היסטוריית טרנזקציות מלאה.

העיקרון השלישי (השקיפות הקיצונית), הוצג כמקור העיקרי לאתגרי פרטיות. פרופ׳ בן-ששון הסביר כי בבלוקצ׳יין ציבורי, כמו ביטקוין או את׳ריום, כל אחד יכול לראות את היסטוריית הפעילות של כל כתובת: כמה נכסים היו בה, למי נשלחו ומתי. אמנם הכתובות אינן מזוהות אלא הן רצפים קריפטוגרפיים, אך בעולם שבו זיהוי בין כתובת לבין אדם יכול להיעשות דרך בורסות, ארנקים מרכזיים או דליפות מידע אחרות, השקיפות הופכת בפועל לכלי למעקב פיננסי רחב היקף.

פרופ׳ בן-ששון סבור שרוב המשתמשים האקטיביים בקריפטו מודעים לרמת הפרטיות (או חוסר הפרטיות) במערכות אלה, אך בפועל רבים מסתפקים בפתרונות חלקיים, כגון: שימוש במספר כתובות, ביצוע ״ערבול״ דרך בורסות מרכזיות, העברת נכסים בין ארנקים שונים וכדומה. פתרונות אלה עשויים להסוות חלקית את מסלול הכסף בפני גורם מזדמן, אך אינם מספקים הגנה משמעותית מפני גורמים בעלי יכולת ניתוח שרשרת מתקדמת. בכך, הדגיש, בלוקצ׳יין הציבורי במתכונתו הבסיסית אינו אנונימי,

[6] הכתוב כאן מהווה תקציר של עיקרי הדברים מהוובינר, למבקשים להעמיק בנושא מוצע לצפות בוובינר המלא בקישור הזה.
[7] גילוי נאות, האורח בוובינר הוא אח של המראיינת.

מכאן עבר הדיון לטכנולוגיות שמנסות להחדיר פרטיות לעולם הבלוקצ'יין, ובראשן הוכחות באפס ידיעה (Zero-Knowledge Proofs), תחום מחקר שבו בן-ששון עוסק מזה למעלה משני עשורים. הוא הסביר באופן אינטואיטיבי כי הוכחת אפס ידיעה מאפשרת לאדם להוכיח טענה, (לדוגמה, "אני מעל גיל 21" או "הייתה לי יתרה מספקת לביצוע העסקה"), מבלי לחשוף את המידע הגולמי שממנו נגזרת הטענה (התאריך המדויק של הלידה, גובה היתרה, זהות הצדדים וכד').

בהקשר של בלוקצ'יין, המשמעות היא שניתן לבנות פרוטוקולים שבהם הרשת מאמתת שכל העסקאות נעשו ביושרה - לדוגמה, שלא בוצעה "הדפסת כסף" ושלא נשלחו סכומים שאין לגביהם יתרה - מבלי שאף אחד מהמשתתפים יודע כמה כסף יש בארנק מסוים, מי העביר למי ובאיזה סכום.

פרופ' בן-ששון הדגים זאת בהקשר רפואי: אפשר לדמיין מערכת שבה קיימים נתונים בעלי רגישות, כמו רצף DNA), יאוחסנו כמעטפות קריפטוגרפיות על גבי בלוקצ'יין. במקרה כזה יוכל האדם להפיק מהן הוכחות שמראות, לדוגמה, שאין לו אחת מעשר מוטציות גנטיות מסוימות, מבלי לחשוף את רצף ה-DNA המלא. חברות ביטוח או גופים אחרים יכולים כך לקבל מידע מספיק לקבלת החלטה (למשל, הנחה בפרמיה), אך לא להחזיק בבסיס הנתונים המלא שחשוף לסיכוני דליפה, שימוש חוזר או פרופיילינג עתידי.

כמענה לשאלה עד כמה בלוקצ'יין משמש כבר היום לתחומים שאינם קריפטו, פרופ' בן-ששון תיאר את ההתפשטות המעשית של השימוש במטבעות יציבים (Stable Coins כמו USDC) לתשלומים יומיומיים, כולל כרטיסי אשראי כך שהסוחר רואה עסקת מאסטרקארד רגילה בעוד שהמשתמש משלם בפועל מכספי הקריפטו שלו. הוא ציין גם שימושים גוברים במסחר בסחורות ובמניות על בסיס בלוקצ'יין, וכן ניסויים בעולמות זהות דיגיטלית (ZK-Identity) ומשחקים, שבהם הטכנולוגיה משמשת הן כבסיס כלכלי והן כמנגנון התחייבות או הוכחת אמינות.

עו"ד דב"ש העלתה את השאלה, מנקודת מבטה של מומחית בתחום הפרטיות: אם בלוקצ'יין והוכחות באפס ידיעה מאפשרים, לפחות בתיאוריה, להחליף מאגרי מידע ריכוזיים ומתווכים אנושיים בפתרונות מבוזרים ומגני פרטיות, מדוע אנחנו עדיין רואים בעיקר שימושים פיננסיים, ולא מוצרי מדף נוספים לפרטיות בתחומי בריאות, זהות ושירותים ציבוריים?

לדעת פרופ' בן-ששון ישנם שני טעמים. הראשון, במישור הטכנולוג-היסטורי - מדובר בתשתית צעירה מאוד, שהיישומים הראשונים שלה, כמו Zcash, יצאו רק באמצע העשור הקודם, ותהליכי הטמעה של תשתיות עמוקות נמדדים לעתים בעשרות שנים; השני, מוסדי - העולם הקיים נשען על מאות שנים של אמון בגורמים מתווכים (בנקים, רואי חשבון, רשויות), והמעבר למודלים שבהם האלגוריתם מחליף את המוסד דורש שינוי תפיסתי עמוק ולא רק פתרון טכנולוגי.

פרופ' בן-ששון הדגים זאת באמצעות השוואה ל- due diligence עסקי. כיום, שתי חברות שנמצאות במו"מ מעבירות את המידע הרגיש לרואה חשבון או בית השקעות שמבצע את הבדיקות ומחזיק במידע. מבט טכנולוגי-קריפטוגרפי היה מאפשר במקום זאת להריץ קוד מוסכם על גבי נתונים

מוצפנים ולהפיק הוכחה שמצביעה על כך שהתנאים הפיננסיים התקיימו, ללא חשיפת הנתונים עצמם. אולם, כל עוד הצדדים רגילים לסמוך על גורם שלישי מהימן, הפיתוי להמשיך במודל הישן גדול, ואימוץ פתרונות אפס הוכחה מצריך היכרות, אמון ויכולת תפעול שאינם טריוויאליים עבור ארגונים מסורתיים.

לקראת סיום, שבו דב״ש ובן-ששון לדון בשאלת הפוטנציאל של בלוקצ׳יין כמקדם פרטיות. מצד אחד, בלוקצ׳יין ציבורי מציב אתגרי פרטיות חריפים: שקיפות מוחלטת, אי־מחיקה וקושי לשרטט גבולות של אחריות ושליטה. מצד שני, בשילוב נכון של פרקטיקות עיצוב פרטיות (PbD), שימוש בהצפנה מתקדמת ובהוכחות באפס ידיעה, ניתן לדמיין מערכות שבהן המשתמש יודע למי הוא נותן גישה, יכול לבחור איזה נתון לחשוף ולאילו מטרות, והמערכת עצמה מוגנת יותר מפני דליפות מסיביות בשל היעדר מאגר יחיד מרכזי.

דב״ש הזכירה לסיום כי האחריות על עמידה בעקרונות פרטיות: שקיפות, צמצום איסוף, הגבלת שימוש וזכויות נושא המידע - לא נעלמת רק משום שהמערכת מבוזרת או רצה על בלוקצ׳יין; להפך, היא מחייבת חשיבה מוקדמת, שפה משותפת בין משפטנים, קריפטוגרפים ומפתחי מערכות, והחלטות מודעות היכן הבלוקצ׳יין מוסיף ערך והיכן עדיפה ארכיטקטורה אחרת.

הווביינר הסתיים בקריאה לקהילת הפרטיות לא ״להתאהב״ בטכנולוגיה, אבל גם לא לוותר על ההזדמנות שהיא יכולה להציע לתחום הפרטיות.

* * *

4 - לסיום

שלושת הנושאים שנדונו - מחשוב קוונטי, מידע ומדיה סינתטיים ובלוקצ׳יין - שונים מאוד זה מזה מבחינת רמת הבשלה טכנולוגית, מודל עסקי ומידת הנראות הציבורית שלהם, אך משותפת להם תכונה אחת: כולם מטשטשים גבולות שהנחו עד היום את דיני הפרטיות והאמון במערכות מידע.

מחשוב קוונטי מערער את הנחת היסוד הבסיסית שלפיה הצפנה חזקה מגנה על מידע לאורך זמן; מידע ומדיה סינתטיים מטשטשים את הגבול בין אמת לבדיה ובין ייצוג אותנטי למניפולציה; ובלוקצ׳יין מערער את ההפרדה בין ריכוזיות למבוזרות, בין שקיפות להגנת נתונים.

מתוך נקודות מוצא שונות, שלוש הטכנולוגיות מחייבות אותנו לחשוב מחדש על שאלות דומות: מי שולט במידע, מהי ״הסכמה מודעת״ במציאות דיגיטלית מתפתחת, היכן עובר קו האחריות של שחקנים פרטיים וציבוריים, ואילו כלים נדרשים כדי להגן על זכויות הפרט בלי לחסום חדשנות.

1. הטכנולוגיות שתוארו כאן עוד יתפתחו, והמסגרת הנורמטיבית סביבן עוד תתעצב ותתפתח. אנו תקווה שהרקע, המיפוי ותמציות הווביינרים ישמשו בסיס לשיח מקצועי רחב

יותר בישראל – בשולחן קבלת ההחלטות, באקדמיה, בקהילה האזרחית ובפרקטיקה היומיומית של מי שאמון על הגנת הפרטיות.