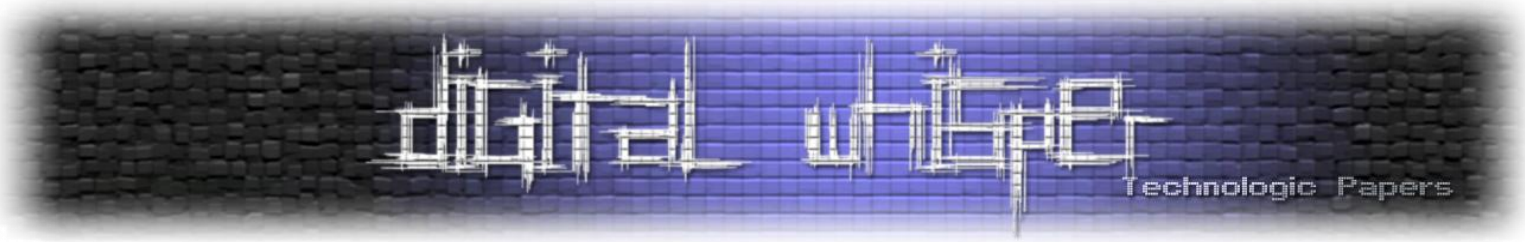

על מקור, עותק והעתק

מאת יהונתן קלינגר

הקדמה

משרד המשפטים מעוניין בשינוי חקיקתי בדיני הראיות שיבטל את כלל הראיה הטובה ביותר ויקדם ארכיבאות דיגיטלית. מטרת הצעת החוק היא לאפשר הגשה של מסמכים לבתי משפט גם כאשר הם העתקים, ובלבד שהם "תוצר המתקבל מתהליך טכנולוגי שבו מיוצרים תוצרים הזהים בתוכנם למקור", ופנה לציבור בבקשה לעמדתו. תמצית זו, שאינה ממצה, מהווה את עמדת התנועה לזכויות דיגיטליות. ואפתח באקדמא קצרה אודות מהו מקור, מהו העתק ומהו עותק.

מקור הינו, בתרגום פשוט, Original, היישות ממנה צמח המסמך; מדובר במסמך בצורתו הטהורה ביותר; אותו מסמך מאפשר, אם מדובר בתוכנת מחשב, את היצירה ממנה ניתן להפיק פלט, או אם מדובר בקובץ מחשב, את קובץ המחשב ממנו ניתן ללמוד על המאפיינים הטכנולוגים של הקובץ.

עותק הינו הביטוי המקובע של המקור. הקיבוע של מקור כלשהוא יוצר עותקים; בחיי היום-יום מדובר על, לדוגמא, הסכמים שנחתמים בשני עותקים: כל צד להסכם מחזיק עותק של ההסכם, אשר חתום בחתימת ידו ובחתימת הצד השני. כל אחד מהעותקים הינו *מקורי* באותה מידה ויכול לשמש כראיה. במצב דברים זה, לא יטען מישהו בבית המשפט כי עותק ההסכם שהצד השני הציג אינו מקורי. במחשבים, עותק של קובץ מחשב יכול לבצע כל מה שקובץ המקור יכול, כיוון שזה לא עבר תהליך כלשהוא. ולכן, כל עותק של קובץ הוא מקורי.

העתק, לעומת זאת, אינו קובץ מקורי, אלא קובץ אשר ביצע קיבוע בלתי הפיך לעותק בנקודת זמן מסוימת. לדוגמא, צילום מסמך במכונת צילום או ייצוא של קובץ Word לפורמאט PDF. המאפיין האי-רברסבילי בקובץ, שמונע ממנו להפוך שנית למקור הוא מה שחשוב; כך, לעניין מקוריות של תוכנה, קוד המקור הוא היצירה המקורית, והגרסאות המהודרות מהוות כל אחת העתק.

העתק נאמן למקור, אם כן, אמור להיות בן-כלאיים בין העותק להעתק, אשר לא ברור אם כלל נדרש בעת שמדובר על ראיות אלקטרוניות.

ההבדלים בין השלושה חושבים ומהותיים כדי להבין מדוע הכלל שמוצע על ידי משרד המשפטים, לאפשר הגעת העתקים (ולא עותקים), כראיות מקוריות, הוא בעייתי. לצורך כך, אסקור קודם כל את שיטת העבודה הרצויה במהלך של עבודה מול קבצי מחשב ולאחר מכן מספר שגיאות שבוצעו, לטעמי, על ידי בתי משפט בישראל בעת שנדרשו לשאלות מסוג זה. לבסוף, אציע מודל חלופי לכלל המוצע על ידי משרד המשפטים, כך שישמר רצון המחוקק, ויאפשר התאמה לעידן דיגיטלי, אך סוגיות הכרוכות באמינות המסמך ואיכותו יאפשרו את העבודה הפורנזית הראויה עליו.

שיטת העבודה הרצויה בעבודה מול קבצי מחשב

חשוב לציין כי עותקים יכולים להשתנות בטביעת האצבע הדיגיטלית שלהם; לקבצים יש מאפייני Meta שמוזנים על ידי מערכת ההפעלה כמו מיקום הקובץ ומתי נגשו אליו לאחרונה (R May, Forensic Evidence After Moving a File) ונתונים אלה עשויים להשתנות בכל עת. לכן, חוקרי זיהוי פלילי אשר ניגשים לקבצי מחשב צריכים לבצע את המחקר בצורה סטרילית ומעבדתית ככל האפשר, ובדרך כלל מייצרים עותק של הכונן הקשיח בהעתקה מלאה (על ידי תוכנות כמו EnCase). יצירת עותק מושלם של סיבית לסיבית של הכונן הקשיח.

אולם, יש לזכור כי גם במקרים מסוג זה, ישנם התקנים כגון כרטיסים חכמים שאינם מאפשרים חילוץ של מידע בצורתו המקורית.

אולם, בעוד ששיטה זו נכונה לגבי קבצי מחשב המצויים על מדיה פיסית, לעיתים נדרש החוקר או אוסף הראיות (לעיתים אפילו מדובר על אדם שהופרה זכות היוצרים שלו ונדרש להוכיח כי תמונה אכן פורסמה במקום בו פורסמה) לקבע אתר אינטרנט או קובץ מחשב. לצורך כך, בדרך כלל, נוצר העתק של אתר האינטרנט (בין אם בקובץ תמונה או על ידי הורדת אתר האינטרנט למחשב) אולם, קוד המקור של אתר האינטרנט, בסיס הנתונים שהפעיל אותו או מערכת ההפעלה שהחזיק השרת אינם מועתקים. במצב כזה, הדבר היחיד שיוכל העתק מסוג זה להוכיח הוא כי אכן ביום מסוים כאשר נגשו לאתר ניתן פלט מסוים. יווצר קושי לא מבוטל מלהוכיח כי הפלט הוא רצוי ואותנטי (וראו **חיים רביה**, ראיות אלקטרוניות, חלק א', חלק ב' וחלק ג')

כך, במקרים מסוימים, גם כאשר התקבל פלט (כתוצאה של בחינה מסוימת שמכשיר אלקטרוני ביצע) בתי משפט לא נטו לקבל את הפלט ללא האפשרות לבחון את קוד המקור שיצר את הפלט (לדוגמא, על אף שהטענה נדחתה, State of Florida v. Carol Mae Bjorkland CT 14406 04 וכן Charles Short, Guilt By Machines: The Problem of Source Code Discovery in Florida DUI Prosecutions, Florida Law Review, Vol 6, P. 177). לכן, המאפיין העיקרי של העתקים מסוג זה הינו שהם פלט מחשב, ולא העתק. על כן, בשביל להוכיח שהם אכן אותנטיים, יש לחלץ את הפלט ולשמר אותו בצורה פורנזית הולמת.

ומה היא אותה צורה פורנזית הולמת? אין ציפיה שכל מתדיין בתביעת לשון הרע באינטרנט ידרש להביא מומחה מחשבים על מנת להעיד על אותנטיות הפלט, אלא כל עוד אין טענה אחרת (ובהמשך נדון במה

יש לעשות כאשר יש טענה אחרת) הרי שיצירת העתקים בצורה מקובלת שאינה מייצרת שינוי, כשם שמעוניינת המדינה ליישם, עשויה להיות מקובלת. רצוי לקבע כי קובץ שעל פניו נראה כאילו נוצר במועד מסוים, ומכיל מאפיינים כי אכן נוצר באותו מועד וללא שינוי, יחשב בהעתק של המקור אם בוצע בצורה שאין בה כדי לפגוע ביכולת להתרשם ממקוריותו.

כך, לדוגמא, עמוד אינטרנט אשר הודפס לתוך קובץ PDF באמצעות תוכנה מקובלת אשר יוצרת חותם מקובל, יחשב כאותנטי אלא אם יתקיימו ראיות אחרות הסותרות זאת, כמו אי התאמה בנתוני ה-Meta Data. הסיבה לכך היא שאותו הקובץ שומר את הטקסט, התמונות והעיצוב מעמוד האינטרנט שהוצג לצופה בצורה זהה, ולא בצורה שמאבדת איכות; כך, העתקה של קובץ הHTML שמהווה את קוד המקור של עמוד האינטרנט שהוצג ללקוח (יחד עם שמירת התמונות המוצגות בו) בתיקיה שתחתם עשוי להחשב כהעתק מהימן, אולם בין השניים עדיף, לשיטתי, קובץ ה-PDF שמעיד גם על אותנטיות העמוד ממנו נשמר הקובץ. מומחה אבטחת המידע **עומר כהן** מוסיף כי פתרון טוב לפתרון הPDF הוא שמירת צילום וידאו שמציג את לכידת המידע: "*אם המטרה היא להציג קיומו של תוכן אינטרנטי, הראיה הטובה ביותר צריכה להיות לכידת מסך בצורת וידאו שבו מוצג תוכן האתר ומאפייני הרשת השונים של המכונה הלוכדת, המוכיחים שבמהלך ההקלטה ניגשים לאתר האמיתי ולא העתק (כמו שינוי DNS למשל), שבדרך זו ניתן לזייף תוכן אינטרנטי בהוצאה לPDF. גם את תוכן הסרטון ואת מאפייני הרשת ניתן לזייף, אבל המאמץ הוא יותר גדול מאשר זיוף תוכן של PDF*".

אולם, ככל שיהיה ניתן לשנות את ההעתק יותר בנקל, וככל שיהיה ניתן לחלץ ממנו פחות ופחות מידע שימושי, כך משקלו הראייתי יהיה נמוך יותר. קובץ JPG, לדוגמא, אשר הינו קובץ תמונה, יחשב פחות מאשר קובץ המציג מסך זהה אך ניתן לחלץ ממנו טקסט בצורה ברורה. ככל שהקרבה לקובץ המקור תהיה גדולה יותר, כך צריך בית המשפט להתרשם כי מדובר בקובץ שמשקף תהליך שימור יותר אותנטי. מעבר לכך, על בית המשפט להיות מסוגל להבין את התהליך שהקובץ עבר עד לצורתו הסופית, ולראות האם ניתן לאבחן שינויים כלשהם שעברו, ומהי האפשרות.

אולם, יש לזכור כי גם במקרה שמתקבל משהו שנחזה להיות מקור, הרי שיכול להיות שמדובר בהעתק משוחזר שהוכנס או אולץ להראות כמקור (ולצורך כך ראו תפ (ת"א) 40156/02 מדינת ישראל נ' ניסים צור),ניתן לזייף קובץ מסוג עותק על ידי נטילת מאפיינים שמצויים בהעתק והפיכתם לבעלי מאפייני Meta פורנזיים.

חשוב להבין שככל שמדובר בקובץ מחשב, ובמיוחד בקבצי מחשב המייצגים פלט מסך כלשהוא, היכולת למניפולציות גבוהה ביותר (וראה חיים רביה, "הראיה הטובה ביותר? אין דבר כזה", 02.12.2003). לכן, ככל שתעלה טענה נגד אותנטיות הפלט, הרי שהפתרון הוא להסתמך על ראיות חיצוניות; אם מדובר על קובץ מחשב שנצרב על מדיה אופטית (CD), הרי שתאריך הצריבה ותאריך יצירת הקבצים במקור ניתנים לאחזור. אולם, בדרך כלל מדובר על קבצים שנשמרו על מחשב; במקרים כאלה, צריך להסתמך על צדדים שלישיים אשר מספקים שירותים בצורה אובייקטיבית על מנת לשמר מהימנות.

לדוגמא, אם אדם מסוים יאחסן קובץ מסוים שהוא עומד להשתמש בו כראיה על שרת אירוח של צד שלישי, ואותו שרת משמר יומנים (Logs) שיוכל להציג בבית המשפט, הרי שאותה ארכיבאות דיגיטלית

תתקיים. כך גם על ידי אחסנת הקובץ בשירות צד ג' כמו YouSendIt או שליחת הקובץ כדואר אלקטרוני לעצמו. מנגד, הדבר היחיד שאותו שירות יספק הינו ראיה שהקובץ נוצר באותו תאריך, לא שאותו קובץ לא עבר מניפולציה.

אם עולה טענה כי פלט של אתר אינטרנט, לדוגמא, עבר מניפולציה, ניתן (לעיתים) להשתמש במנגנונים כמו Google Cache כדי להוכיח שנוצרה תמונה אמינה של אתר האינטרנט במועד מסוים, או להשתמש בארכיון האינטרנט הנמצא ב-Archive.org על מנת להוכיח את הטענה. ניתן גם, במידה והטענה היא כי המסמך זויף, לחייב את הטוען להציג (בהנחה שהוא זה ששלט על אתר האינטרנט) את קוד המקור של האתר בתאריך מסוים (לכן, כאשר מפתחים אתר ישנה חשיבות רבה בשימוש בכלים כמו Subversion על מנת לשמר גרסאות).

אולם, חייבים לזכור שכאשר מדובר במדיה דיגיטלית היכולת למניפולציה תמיד קיימת, ובית המשפט צריך לשקול שיקולים כמו ראיות חיצוניות. הוא אינו יכול להסתמך יותר על מה שהוא רואה, כיוון שמה שנראה בפניו הוא רק פלט של מסמך, ולא המסמך. הוא לא יכול לקבוע כי מסמך מסוים אכן היה קיים או אותנטי, וצריך לשים עצמו כשסתום למנוע הכנסה של זיופים, אשר אינם מתרחשים מדי יום.

המדרג הראייתי, מהראיה הטובה ביותר ועד הפחות טובה, צריך שיהיה כזה: (1) ככל שניתן להשיג עותק של הקובץ בתאריך הרלוונטי מצד שלישי, שסיפק שירות גיבוי אמין ולא תלוי באחד הצדדים, או עותק של הכונן הקשיח בהעתקה פורנזית, משקל הראיה יהיה גבוה ביותר; (2) ככל שמדובר בפורמאט שהוא LossLess ולא מהודר, אשר משקף את המקור, ואין טענה כי המקור שונה מאותו התאריך, הרי שהקובץ יהיה בחשיבות שניה; (3) בחשיבות שלישית יבוא העתק נאמן של פלט, אשר ישנן ראיות שמבהירות שהפלט לא שונה או טופל בצורה כלשהיא; (4) עותקים באיכות Lossy או תדפיסים יבואו אחרונים.

על מהימנות הפלט שיוגש לבית המשפט (או הקבצים שיוגשו בצורתם המקורית) יעיד איש מחשבים שטיפל וליווה את תהליך שחזור הקבצים לאורך כל הדרך, ויוכל להעיד על מקצועיות התהליך. במיוחד הדבר חשוב כאשר מדובר בראיות אלקטרוניות במשפטים פליליים, אשר משטרת ישראל הראתה כי היא נעדרת כלים פורנזיים להוכחה, וכאשר בחנה תוכן של כונן קשיח עשתה זאת ללא העתקה ולא במצב של קריאה בלבד, תוך שהיא משמידה את הראיות האלקטרוניות הרלוונטיות **(משה הלוי**, "ראיות אלקטרוניות: בדיחה ושמה משטרת ישראל," דואר חשמלי, 22.03.2010) ועושה לעיתים שגיאות הפוגעות ביכולות החקירה שלה. כך, בעוד ש"תכלית החוק מחייבת פירוש זה, וביתר שאת. כפי שנוכחנו לעיל (ראה הקטע המצוטט בסעיף 28 לעיל ממאמרו של ד"ר משגב), הצורך בנוכחות שני עדים חיצוניים נועדה למנוע "השתלת" חומר על ידי המשטרה, והגברת אמון הציבור בעת החיפוש. חשש זה של השתלת חומר נכון שבעתיים כאשר מדובר בתוכנת מחשבים" (בש 1153/02 מדינת ישראל נ' מיכאל אברג'יל), המדינה מנסה לטעון כי החיפוש הנ"ל יגביר את העלויות המוטלות עליה ויפגע ביכולתה לחקור, אולם כב' השופט **משה דרורי**, פסק כי כחלק מההליך הפלילי, יש צורך בהליך הבא בעת חיפוש והעתקת מחשב: "אינני רואה כל קושי, כי כאשר מומחה המחשבים מטעם מז"פ יחדור למחשב ויוציא את הפלט המתאים, יהיה נוכח באותו חדר מומחה מחשבים אחר מטעם האדם שמחשבו נתפס. למותר לציין, כי בדורנו ניתן לבצע העתקות של תוכנה תוך זמן מועט, הניתן למדידה במקרים מסויימים אף בדקות, ועל כן טענת העומס - לאו טענה היא."

היכן שגו בתי המשפט

ככלל, בתי המשפט לא נדרשו יותר מדי לשאלת מהימנותן של ראיות אלקטרוניות, והתנהגות רשויות חקירה לא היו שערוריתיות במיוחד (בשפ 5837/09 אורטיז נ' מדינת ישראל, לדוגמא). אולם, בהליך תפ (י-ם) 2077/06 מדינת ישראל נ' אליהו אריש נדונה שאלת הליך החיפוש ושמירת הראיות מטלפון סלולרי. באותו המקרה, בית המשפט פסק, בצורה שגויה כי "אף בהנחה כי טלפון סלולארי עונה על הגדרת מחשב, במישרין או בעקיפין, ברור כי לצורך הפקת מידע ממנו, כגון: רשימת שיחות נכנסות ויוצאות, מיסרונים שנשלחו וכו', אין צורך במיומנות מיוחדת מעבר למיומנות של אדם סביר"; כך, בצורה חפוזה, ותוך אי משים לב להבדל בין חומר מחשב לפלט, אפשר בית המשפט המחוזי בירושלים חיפוש בחומר מחשב ולא בעותק של חומר המחשב, אשר צריך להיות הנוהל, ופגע במקוריות החומר.

במקרה אחר, תפ (ת"א) 40156/02 מדינת ישראל נ' ניסים צור בית המשפט לא הצליח להבין מהו מפתח הצפנה, וכתוצאה מכך פסק בצורה שגויה בנושא ראיות אלקטרוניות. המדינה טענה כי **ניסים צור** זייף הסכם השקעה, וכתוצאה מכך הונה חברה אחרת. הנאשם הביא מומחה מחשבים שהעיד לנושא הצפנת הקבצים והיכולת לייחסם למקור, ופסק בחוסר הבנה של מהי הצפנה כי "אין זה ברור מדוע מופיע בסוף הודעת דואר אלקטרוני מפתח הצפנה שאמור להיות מוסתר. תוהה אני, כיצד הגיע לידיו של הנאשם ונמצא, בצירוף מקרים, מיוחד, לקראת עדותו במשפט, דווקא. שנית, שימוש במפתח הצפנה, כך שמענו במשפט, מניב בדרך כלל קבצים מוצפנים, אשר באמצעות הפעלה נוספת של אותו מפתח הצפנה, ניתן לגלות את תוכנם. הנאשם והמומחה מטעמו לקחו קבצים שתוכנם אינו מוסתר, קבצים שאינם מוצפנים. הנתונים ה"מרשיעים", כביכול, התגלו לאחר ההצפנה. גרסת ההגנה, לפיה הנתונים הוכנסו לקבצים באמצעות מפתח ההצפנה, אינה מתיישבת עם עובדת היות הקבצים בלתי-מוצפנים". כאן בית המשפט מפגין חוסר יכולת להבין כי לעיתים מפתח הצפנה לא נועד למנוע מאחרים לקרוא את המסמך אלא דווקא להעיד על אותנטיות המסמך (כמו חתימה אלקטרונית, לדוגמא) (במקרה נוסף,פ 3807/09 מדינת ישראל נ' אלכסנדר פפיסמלוב ואח', בית המשפט ייחס להגדרת קובץ מחשב את הגדרת "מסמך" גם אם אותו מסמך מעולם לא בא לעולם ונותר בתוך המחשב).

כלומר, הבעיה הכללית היא שבית המשפט לא דן בנושאי ראיות אלקטרוניות באותה הרגישות שהוא דן בראיות פיסיות. לבית המשפט קשה עדיין להבדיל בין פלט, עותק, העתק ומקור, וכל עוד שופטי בית המשפט לא יעברו הכשרה פורנזית הולמת, יהיה קשה לטעון לאמינות ראיות דיגיטליות.

המלצות

ההסדר שמוצע על ידי משרד המשפטים אינו הגיוני ואינו מעלה או מוריד כאשר הסוגיה היא אותנטיות הפלט. כאשר מדובר במסמך שהוא מקור, יש לבחון את קבילות המקור על ידי הגשת עותק של המקור, ולא העתק. פתרון זה, לדוגמא, בסוגיות של תוכנה, יאפשרו למומחים לבחון טענות לגבי פגמים בתוכנה, אשר ניתנים לבחינה אך ורק על ידי בחינת קוד המקור והקבצים המהודרים. כאשר מדובר בפלט מחשב, או בראיה שהיא פלט (לדוגמא, יומן שרת שנועד להבהיר כי בוצעה גישה או שינוי במועד מסוים), אזי יש לשמר את הפלט ולהפיק אותו על ידי אדם מוסמך, או אדם שאינו תלוי בצדדים למשפט.

ללא שינויים מסוג זה, ההצעה של משרד המשפטים תאפשר להציג צילומי מסך ולשלול, כמעט, את היכולת לטעון נגדם, ותוכל לפגום ביכולת להסתמך על ראיות אלקטרוניות למסחר אלקטרוני.

תודה לדורון אופק, עומר כהן, עירא אברמוב וצבי דביר על הערותיהם.