היסטוריה קצרה של חותם השעווה

במשך ארבעה מאות שנים, טיפת שעווה אדומה הבטיחה שאיש לא קרא מכתב. איבדנו את זה עם המעבר לעידן הדיגיטלי. זה בר-שחזור.

לפני הנייר

הצורך לתקשר משהו באופן חסוי לאדם רחוק עתיק יותר מהכתב. במסופוטמיה, לוחות טין עם מסרים מנהליים או פרטיים נשלחו בתוך כמוסות העשויות גם הן מטין, שנחתמו לפני האפייה: כל ניסיון לקרוא את התוכן חייב את שבירת המעטפת, והנמען ידע במבט חטוף אם הכמוסה הגיעה שלמה. ברומא הקלאסית, מגילות פרגמנט נקשרו בחוט ונחתמו בשעווה או בעופרת. הרעיון היה תמיד זהה: שכל קריאה בלתי מורשית תשאיר עקבה פיזית בלתי מחיקה.

עידן חותם השעווה

במשך כמה מאות שנים, מסוף ימי הביניים ועד תחילת המאה ה-20, הכלי הקנוני של התכתבות חסויה באירופה היה נייר מקופל וחתום בחותם שעווה. שעווה מותכת נשפכה על חיבור הגיליון והוטבעה בחותם אישי או מוסדי. זה לא היה קישוט. נוטריונים, דיפלומטים, סוחרים ואנשים פרטיים השתמשו בו באותו הגיון: אם חותם השעווה היה שלם וההטבעה הייתה ניתנת לזיהוי, התוכן לא נקרא; אם הוא היה שבור, ההתכתבות הייתה פגומה עוד לפני פתיחתה.

כוחו של חותם השעווה לא היה במחירו היקר או בחגיגיותו. הוא היה בתכונה מבנית מאוד ספציפית: כל ניסיון להסירו ולהחזירו השאיר עקבות גלויים. לא הייתה דרך שקטה לפתוח מכתב חתום. וזה אומר שהחשאיות לא הייתה תלויה בהבטחה של שום מתווך — השליח, העגלון, פקיד הדואר — אלא בעיצוב הפיזי של המעטפת עצמה. זה היה אמון המבוסס על ראיות, לא על מילתו של איש.

המעבר הדיגיטלי

הטלגרף, הטלפון, הדואר האלקטרוני, המסרים הארגוניים. התקשורת האלקטרונית הביאה מהירות, טווח עולמי ועלות כמעט אפסית לכל הודעה. היא גם מחקה את ההבטחה של חותם השעווה. כבירית מחדל, כל הודעה עוברת דרך מתווכים שאת יושרם אנו יכולים לבדוק רק באמצעות הבטחות הכתובות בתנאי שירות, הסמכות טכניות וביקורות עמומות. אין שום דבר המקביל לטיפת שעווה שבורה שתזהיר אותנו.

חותם שעווה דיגיטלי

התכונה שנתנה כוח לחותם השעווה לא הייתה חותם השעווה עצמו, אלא מה שהוא ייצג: יושרה הניתנת לאימות לפי עיצוב, ללא צורך לבטוח בצד שלישי. ניתן לשחזר את התכונה הזו במישור הדיגיטלי, אם כי באמצעות שני אלמנטים במקום אחד. הראשון הוא החותם הקריפטוגרפי — טביעת ה-SHA-256 המופיעה בתחתית כל מאמר בפרסום זה היא, במובן המילולי, חותם שעווה דיגיטלי: כל שינוי בתוכן משנה את טביעת האצבע באופן גלוי, בדיוק כפי ששעווה שבורה חשפה קריאה בלתי מורשית. השני הוא ארכיטקטורת הערוץ: כשאין שרת באמצע בין שני אנשים המתקשרים, אין מתווך שצריך לתת בו אמון. השילוב של שני האלמנטים — יושרה הניתנת לאימות והיעדר מתווך — משחזר, במונחים דיגיטליים, את מה ששעווה אדומה על נייר מקופל עשתה באופן יומיומי במשך ארבע מאות שנים.

השם

פרסום זה נקרא Cuadernos Lacre כיוון שחותם השעווה אינו קישוט היסטורי, אלא תכונה טכנית מוחשית: יושרה הניתנת לאימות על ידי בנייה, ללא הבטחה של מפעיל כלשהו. כל מאמר בסדרה מנתח, בגרסתו הדיגיטלית העכשווית, חלק מאותו רעיון: הצפנה, מטא-נתונים, סודיות מקצועית, ארכיטקטורת תקשורת, מסגרת משפטית אירופית. השם הוא גם דרך לזכור שחשאיות אינה שירות שנרכש, אלא תכונה של הערוץ עצמו שדרכו המידע עובר.

מקורות וקריאה נוספת

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (פרקים על חתימת לוחות ובולות מסופוטמיות).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. פרקים על חותם השעווה ככלי ליושרה ומקוריות.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. ניסוח מודרני של עקרון חותם השעווה: ערבויות בקצוות, לא בערוץ.

הבא → להצפין זה לא להיות פרטי: מה המטא-נתונים אומרים עליכם

קריאות אחרונות

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

קחו את המאמר הזה אתכם לכל מקום שתצטרכו.

Markdown ↓ · טקסט פשוט ↓ · PDF ↓

הקובץ יורד למכשיר שלכם. משם תוכלו לשמור אותו, לייבא אותו ל-Solo2 או לשתף אותו היכן שתרצו. Cuadernos לא מחליטה על היעד עבורכם.

חותם שעווה · SHA-256 3af3e959c9476423e2214ccc5c04c8839eaa71cc3626468cd4efbba8a57682fb

ES

Cuadernos Lacre · פרסום של Menzuri Gestión S.L. ·
נכתב על ידי R.Eugenio · נערך על ידי צוות Solo2.