Μια σύντομη ιστορία του βουλοκέριου

Για τέσσερις αιώνες, μια σταγόνα κόκκινου κεριού εγγυόταν ότι κανείς δεν είχε διαβάσει ένα γράμμα. Το χάσαμε με τη μετάβαση στην ψηφιακή εποχή. Μπορεί να ανακτηθεί.

Πριν από το χαρτί

Η ανάγκη να επικοινωνήσουμε κάτι εμπιστευτικά σε κάποιον μακριά είναι παλαιότερη από τη γραφή. Στη Μεσοποταμία, πήλινες πινακίδες με διοικητικά ή ιδιωτικά μηνύματα αποστέλλονταν μέσα σε πήλινες κάψουλες, σφραγισμένες πριν το ψήσιμο: οποιαδήποτε προσπάθεια ανάγνωσης του περιεχομένου απαιτούσε το σπάσιμο του περιβλήματος και ο παραλήπτης γνώριζε με μια ματιά αν η κάψουλα έφτανε άθικτη. Στην κλασική Ρώμη, οι περγαμηνές δένονταν με σπάγκο και σφραγίζονταν με κερί ή μόλυβδο. Η ιδέα ήταν πάντα η ίδια: οποιαδήποτε μη εξουσιοδοτημένη ανάγνωση θα άφηνε ένα ανεξίτηλο φυσικό ίχνος.

Η εποχή του βουλοκέριου

Για αρκετούς αιώνες, από το τέλος του Μεσαίωνα μέχρι τον 20ό αιώνα, το κανονικό εργαλείο της εμπιστευτικής αλληλογραφίας στην Ευρώπη ήταν το διπλωμένο χαρτί σφραγισμένο με βουλοκέρι. Το λιωμένο κερί χυνόταν πάνω στην ένωση του χαρτιού και σφραγιζόταν με μια προσωπική ή θεσμική σφραγίδα. Δεν ήταν διακοσμητικό. Συμβολαιογράφοι, διπλωμάτες, έμποροι και ιδιώτες το χρησιμοποιούσαν με την ίδια λογική: αν το βουλοκέρι ήταν άθικτο και η σφραγίδα αναγνωρίσιμη, το περιεχόμενο δεν είχε διαβαστεί. Αν ήταν σπασμένο, η αλληλογραφία είχε παραβιαστεί πριν καν ανοιχτεί.

Η δύναμη του βουλοκέριου δεν βρισκόταν στο κόστος ή την επισημότητά του. Βρισκόταν σε μια πολύ συγκεκριμένη δομική ιδιότητα: οποιαδήποτε προσπάθεια αφαίρεσης και επανατοποθέτησής του άφηνε ορατά ίχνη. Δεν υπήρχε αθόρυβος τρόπος να ανοιχτεί ένα σφραγισμένο γράμμα. Και αυτό σήμαινε ότι η εμπιστευτικότητα δεν εξαρτιόταν από την υπόσχεση κάποιου μεσάζοντα —του αγγελιαφόρου, του αμαξά, του ταχυδρομικού υπαλλήλου— αλλά από τον ίδιο τον φυσικό σχεδιασμό του περιβλήματος. Ήταν εμπιστοσύνη βασισμένη σε στοιχεία, όχι στον λόγο κανενός.

Η ψηφιακή μετάβαση

Ο τηλέγραφος, το τηλέφωνο, το ηλεκτρονικό ταχυδρομείο, τα εταιρικά μηνύματα. Η ηλεκτρονική επικοινωνία έφερε ταχύτητα, παγκόσμια εμβέλεια και σχεδόν μηδενικό κόστος ανά μήνυμα. Πήρε μαζί της και την εγγύηση του βουλοκέριου. Από προεπιλογή, κάθε μήνυμα περνά μέσα από μεσάζοντες των οποίων την ακεραιότητα μπορούμε να ελέγξουμε μόνο μέσω υποσχέσεων γραμμένων σε όρους χρήσης, τεχνικών πιστοποιήσεων και αδιαφανών ελέγχων. Δεν υπάρχει τίποτα ισοδύναμο με μια σταγόνα σπασμένου κεριού για να μας προειδοποιήσει.

Ένα ψηφιακό βουλοκέρι

Η ιδιότητα που έδινε δύναμη στο βουλοκέρι δεν ήταν το ίδιο το κερί, αλλά αυτό που αντιπροσώπευε: επαληθεύσιμη ακεραιότητα εκ σχεδιασμού, χωρίς την ανάγκη εμπιστοσύνης σε κάποιον τρίτο. Αυτή η ιδιότητα

μπορεί να ανακατασκευαστεί στο ψηφιακό επίπεδο, αν και με δύο στοιχεία αντί για ένα. Το πρώτο είναι η κρυπτογραφική σφραγίδα —το αποτύπωμα SHA-256 που εμφανίζεται στο κάτω μέρος κάθε άρθρου αυτής της έκδοσης είναι, κυριολεκτικά, ένα ψηφιακό βουλοκέρι: οποιαδήποτε τροποποίηση του περιεχομένου αλλάζει ορατά το αποτύπωμα, όπως το σπασμένο κερί πρόδιδε τη μη εξουσιοδοτημένη ανάγνωση. Το δεύτερο είναι η αρχιτεκτονική του καναλιού: όταν δεν υπάρχει διακομιστής στη μέση μεταξύ δύο ατόμων που επικοινωνούν, δεν υπάρχει μεσάζων στον οποίο πρέπει να δοθεί εμπιστοσύνη. Ο συνδυασμός και των δύο στοιχείων — επαληθεύσιμη ακεραιότητα και απουσία μεσάζοντα— αναπαράγει, με ψηφιακούς όρους, αυτό που για τέσσερις αιώνες έκανε καθημερινά το κόκκινο κερί πάνω στο διπλωμένο χαρτί.

Το όνομα

Αυτή η έκδοση ονομάζεται Cuadernos Lacre επειδή το βουλοκέρι (lacre) δεν είναι ένα ιστορικό στολίδι, αλλά μια συγκεκριμένη τεχνική ιδιότητα: επαληθεύσιμη ακεραιότητα εκ κατασκευής, χωρίς υπόσχεση από κανέναν πάροχο. Κάθε άρθρο της σειράς αναλύει, στη σύγχρονη ψηφιακή του εκδοχή, κάποιο μέρος αυτής της ίδιας ιδέας: κρυπτογράφηση, μεταδεδομένα, επαγγελματικό απόρρητο, αρχιτεκτονική επικοινωνιών, ευρωπαϊκό νομικό πλαίσιο. Το όνομα είναι επίσης ένας τρόπος να θυμόμαστε ότι η εμπιστευτικότητα δεν είναι μια υπηρεσία που μισθώνεται, αλλά μια ιδιότητα του ίδιου του καναλιού μέσω του οποίου κυκλοφορούν οι πληροφορίες.

Πηγές και περαιτέρω μελέτη

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (κεφάλαια για τη σφράγιση πινακίδων και bullae στη Μεσοποταμία).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Κεφάλαια για το βουλοκέρι ως όργανο ακεραιότητας και πατρότητας.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Σύγχρονη διατύπωση της αρχής του βουλοκέριου: εγγυήσεις στα άκρα, όχι στο κανάλι.

Επόμενο → Κρυπτογράφηση δεν σημαίνει ιδιωτικότητα: τι λένε τα μεταδεδομένα για εσάς

Πρόσφατα αναγνώσματα

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Πάρτε αυτό το άρθρο μαζί σας όπου το χρειάζεστε.

↓ Markdown ↓ Απλό κείμενο ↓ PDF

Το αρχείο θα ληφθεί στη συσκευή σας. Από εκεί μπορείτε να το αποθηκεύσετε, να το εισαγάγετε στο Solo2 ή να το μοιραστείτε όπου θέλετε. Το Cuadernos δεν αποφασίζει τον προορισμό για εσάς.

Σφραγίδα από βουλοκέρι · SHA-256
76f0522c304ecb3ae27bc118466a1afcea85e5a437764e4bc2e20c587c5c4864
ES

Cuadernos Lacre · Μια έκδοση της Menzuri Gestión S.L. ·
γραμμένη από τον R.Eugenio · επιμελημένη από την ομάδα του Solo2.

JavaScript που απαιτείται για την προτίμησή σας σε φωτεινό/σκοτεινό θέμα. Χωρίς ιχνηλάτες, χωρίς προφίλ, χωρίς κοινή χρήση δεδομένων. Αν θέλετε να μας ακολουθήσετε: RSS.