

**Sulla copertina di Science**  
**La storia di Roma antica**  
**ha lasciato l'impronta nel Dna**

La storia di Roma degli ultimi 12 mila anni è stata ripercorsa studiando il Dna degli antichi abitanti della capitale. Una pubblicazione con molti autori italiani si è conquistata la copertina di Science, partendo dall'analisi dei resti genetici di 127

scheletri antichi, ritrovati nella zona attorno alla capitale. Circa 9 mila anni fa una migrazione di coltivatori dall'Anatolia si sovrappose ai cacciatori-raccoglitori locali. Ma è soprattutto durante l'epoca imperiale che il Dna dei romani cominciò a riempirsi di

influssi dal Nord Africa e dall'Asia, proprio come suggerisce la storia cosmopolita della città. Dopo il quarto secolo, con il declino dell'Impero, gli scambi e le migrazioni si impoveriscono. La stessa perdita di diversità si ritrova nel Dna dei romani di quel periodo.



ARTUR MARCINIEC / ALAMY STOCK PH

**Mondi Digitali**  
 di Simone Arcagni

*Una lezione sul confine tra uomini e macchine*

**M**a se le macchine intorno a noi continuano ad aumentare e penetrare in tutti i campi, quale rapporto dovremmo intrattenere con loro? Il professor Francesco Parisi ha dato una risposta, che è poi il titolo del suo ultimo libro: *"La tecnologia che siamo"* (Codice). Chiedo allora a Parisi cosa significa che "siamo la tecnologia"? "Significa che non siamo noi a fare le cose, sono le cose che fanno noi..." Cioè? "Gli occhiali da vista, per esempio, ci rendono osservatori incrementando la nostra vista. Noi facciamo la tecnologia, che ci offre nuove opportunità che conducono alla creazione di nuove tecnologie e così via da migliaia di anni". La cosa interessante è che Parisi non si occupa di tecnologie dal punto di vista dell'ingegneria o della filosofia, ma delle scienze cognitive, cioè quella disciplina che cerca di spiegarci come conosciamo e come apprendiamo. "Le scienze cognitive sono un campo interdisciplinare che prova a capire come funziona la cognizione umana, animale e artificiale". Per questo il campo di ricerca è particolarmente efficace nell'interpretare fenomeni come il rapporto tra uomo e macchina. Studiare l'apprendimento e la conoscenza è la condizione obbligata per poi insegnarla alle macchine, per lavorare sui robot e sulle intelligenze artificiali. Leggendo il denso volume di Parisi iniziamo a capire come funziona il rapporto tra noi e la tecnologia. Parliamo di macchine che magari ci aiutano ad aumentare i nostri sensi, oppure che si imestano per offrirci nuovi strumenti e nuove facoltà, oppure ancora che dispiegano il loro potenziale in simbiosi con noi. Per Parisi è fondamentale capire che "Le tecnologie digitali operano un cambio di paradigma, rappresentano l'ultima frontiera della forza naturale imbrigliata, prima fuoco e vapore ci hanno regalato energia e mezzi per controllare il mondo fisico, ma l'elettricità è qualcosa di diverso: parliamo di una forza che accomuna sia il cervello che lo smartphone, possiamo dire che si tratta della tecnologia paradigmatica dell'ibridazione tra le cose e noi" Nel mondo elettrico vanno ridiscussi i confini tra noi, l'ambiente e le macchine. "La tecnologia che siamo" parla proprio di questo, di come ci estendiamo nell'ambiente con le macchine e di come incorporiamo funzioni che non ci appartengono.

Voleva essere uno strumento a disposizione degli amici, invece è diventato un sito che oggi conta 150 mila visitatori al giorno e tre milioni di iscritti. Il suo nome è Have I Been Pwned e permette agli utenti di controllare se la propria password è finita in un database di credenziali rubate. Un successo che non si aspettava neanche il fondatore, Troy Hunt, ricercatore di sicurezza informatica al lavoro per Microsoft: «È iniziato tutto nel 2013, dopo l'enorme compromissione di Adobe che ha coinvolto milioni di utenti - racconta -. Contemporaneamente circolavano altri file di dati violati in cui vedevo comparire le stesse persone e le stesse password. Così è nata l'idea».

**Di tutte le violazioni che ha analizzato, c'è qualcosa che l'ha particolarmente colpita?**  
 «Mi stupisce la loro portata e il fatto che, in molti casi, sembrano diventare sempre più grandi. Un'altra cosa che trovo particolarmente sorprendente è la quantità di credenziali compromesse appartenenti ai cosiddetti aggregatori di dati, cioè ad aziende che per mestiere si occupano di collezionare le informazioni degli utenti da diverse fonti, per poi rivenderle. Una tendenza che mi preoccupa sia per l'enorme volume di dati che queste imprese hanno a disposizione, sia perché non siamo consapevoli delle informazioni in loro possesso in quanto non gliele abbiamo fornite direttamente».

**Quanti furti di informazioni ha**

L'intervista / Troy Hunt

**"Non usate sempre le stesse"**



**TROY HUNT,**  
 RICERCATORE  
 DI SICUREZZA  
 INFORMATICA  
 PER MICROSOFT

*Per essere sicuri affidatevi a un password manager oppure utilizzate un sistema di autenticazione a due fattori*

**catalogato fino ad ora?**  
 «Oltre 410 per 8.5 miliardi di credenziali compromesse. Ma è solo la punta dell'iceberg».

**Possiamo ancora considerare le password un metodo di autenticazione sicuro?**  
 «Non è una domanda a cui si può rispondere con un sì o un no netti. Le password possono essere usate in maniera molto sicura, sfruttando un password manager: io, ad esempio, utilizzo l'Password. Un ulteriore livello di sicurezza può essere aggiunto con un sistema di autenticazione a due fattori. Il problema è che in molti usano la stessa password, spesso debole, per diversi servizi».

**Finiranno i furti di credenziali?**  
 «No, possono solo aumentare e peggiorare. Basta pensarci: anche attraverso l'internet delle cose condividiamo sempre più dati che ci

riguardano. Inoltre, spesso, salviamo le informazioni in cloud per averle sempre a disposizione ovunque. Molto del materiale presente in Have I Been Pwned arriva da utenti che hanno configurato male i loro servizi cloud».

**C'è gente che vive vendendo i nostri dati?**  
 «Certo, vengono venduti da diversi soggetti, con diversi gradi di legittimazione. C'è chi vende illegalmente le credenziali rubate e poi ci sono i già menzionati aggregatori di dati».

**Gli utenti vengono spesso colpevolizzati per l'impiego di password deboli. Ma c'è qualcosa che le aziende potrebbero fare per migliorare la sicurezza?**

«Penso che la responsabilità sia condivisa. Ad esempio, molte organizzazioni adottano dei pessimi criteri per le password, ovvero chiedono di inserire caratteri speciali e lettere maiuscole. Il risultato? Si sfrutta la vecchia chiave d'accesso, scrivendo la prima lettera in maiuscolo e aggiungendo qualche carattere speciale».

**Lei ha annunciato il "progetto Svalbard", cioè l'intenzione di vendere Have I Been Pwned. Perché e come procede?**

«L'archivio è ormai troppo grande ed è troppo rischioso mantenerne la gestione da solo. Inoltre, vorrei mettere a disposizione degli utenti più servizi, processare più database e raggiungere un'audience più ampia. La trattativa ora è in fase finale. Presto renderemo noti i dettagli».

— R.F.

L'Autore



**Simone Arcagni**  
 insegna alla  
 Università di  
 Palermo, esperto  
 di nuovi media  
 e tecnologie