

FIGLI NEL TEMPO. L'EDUCAZIONE

FRANCESCO TONUCCI Psicologo



A Roma un ragazzo di 15 anni si è ucciso perché andava male in matematica. In una lettera spiegava «di essere stato distrutto dalla scuola... Le interrogazioni, i voti, tutto quel clima terribile... Che scuola è mai questa?»

Morire di scuola

ABBIAMO appena parlato di mortalità scolastica, che descrive una morte simbolica e la attualità ci costringe a tornare in modo più drammatico sul grave problema del «mal di scuola». Nei giornali di uno di questi giorni due notizie sconvolgenti. La prima è quella a cui si riferisce la lettera. La seconda appare sui giornali nello stesso giorno e parla di un ragazzo di undici anni di Napoli che organizza un commando di sei suoi amici, più o me-

no coetanei, per entrare nella sala dei professori della sua scuola e far sparire un compito di matematica sbagliato. Poi lo fanno dando fuoco agli armadi e provocano decine di milioni di danni, ma questo è un altro problema. Il fatto sconcertante è la motivazione. Ora si cercherà certamente di indagare sulle debolezze di questi ragazzi, sui loro «precedenti», si sosterrà che se uno si uccide in qualche modo denota fragilità, incapacità di affrontare la vita, che se uno

assalta la scuola per via di un compito denota una abitudine al teppismo, ecc. Ma quelle parole scritte dal ragazzo suicida pesano come macigni. Ci vorrebbe che tutte le scuole d'Italia convocassero consigli di classe, collegi docenti e consigli di circolo e di istituto straordinari, per discutere quelle parole, per analizzare questi due fatti, rispetto ai quali tutti noi adulti, genitori ed insegnanti, siamo ugualmente colpevoli. Tutti contribuiamo a costruire la immagine di una scuola severa, esigente, ostile. Una scuola per la quale lavorare senza avere nulla in cambio, spesso senza capire, per dovere. Tutti ripetiamo ai bambini fin dalla prima elementare:

«Adesso basta giocare, bisogna studiare». Tutti, specialmente noi genitori, ci preoccupiamo se un allievo va volentieri a scuola perché sospettiamo che non stia lavorando seriamente, ma solo divertendosi. Sarebbe bello che in queste riunioni straordinarie si parlasse di come fare in modo che la scuola diventi una esperienza bella, piacevole, divertente, seria come un gioco (non ci sono altre attività umane così alte e così ricche) o un lavoro gratificante e non noioso e avvilente come un lavoro alienante. Che si lavorasse tutti insieme per una scuola nella quale gli studenti vogliano restare più tempo di quello previsto, tornare al pomeriggio, per la quale insomma valga la pena studiare.

FISICA. Potrebbe viaggiare su fotoni il messaggio cifrato veramente inviolabile del futuro

Codice quantistico a prova di spia

Da quando Giulio Cesare si cimentò nell'impresa di creare un codice cifrato per trasmettere messaggi che voleva rimanessero segreti, una folta schiera di scienziati ha cercato di trovare il «codice inviolabile». Senza riuscirci. Ora sembra stia per iniziare l'era della crittografia quantistica: messaggi affidati a fotoni che permettono al decodificatore del messaggio di scoprire qualsiasi intrusione da parte di una spia.



Disegno di Mitra Divshvili

PIETRO GRECO

Il problema è solo quello di trovare un magazzino adatto per conservare fotoni. E poi il grande sogno di Edgar Allan Poe svanirà per sempre. Non appena avremo allestito l'originale magazzino, capace di preservare per lungo tempo l'integrità dei fotoni e delle informazioni che trasportano, saremo in grado di ricevere e di leggere un criptogramma quantistico. Ed allora anche la spia più geniale dovrà arrendersi di fronte alla inviolabilità del primo codice segreto a sicurezza intrinseca. Smentendo non solo la fiducia incrollabile che il principe della letteratura gialla, Edgar Allan Poe, riponeva nella capacità della mente umana di venire a capo di qualsivoglia enigma o mistero (si veda lo *Scarabeo d'oro*, il suo famoso racconto del 1843). Ma anche la fiducia altrettanto incrollabile che il papa della fisica Albert Einstein riponeva nel principio di «località», che è poi l'impossibilità di effettuare azioni istantanee a distanza. Si veda l'articolo *Può essere considerata completa la descrizione quanto-meccanica della realtà?* pubblicato nel 1935 sulla «Physical review», diventato famoso come paradosso Einstein, Podolski, Rosen.

Allestite quel magazzino, assicura Arthur Ekert, fisico della Oxford University e profeta della *quantum cryptography* (New Scientist, 16 gennaio 1993), e saranno proprio le correlazioni istantanee a distanza tra coppie di fotoni a lasciare senza lavoro, una volta e per sempre, tutti gli spioni, rendendo assolutamente inviolabili non solo i messaggi in codice ma anche le loro chiavi di lettura.

Lo sappiamo. Compattati bancari e fieri militari, vecchi cultori di enigmistica e nuovi teorici delle

autostrade informatiche, insomma tutti coloro che per passione o per professione amano il segreto ed i suoi risvolti, stanno già drizzando le orecchie. Il paradiso (almeno quello della comunicazione criptica) è a portata di mano.

Ma ci conviene andare con ordine. Per cercare di capire se e quando quella fatidica soglia sarà varcata. Tutti i sistemi in codice sono costituiti da una procedura crittografica e da una chiave. La prima procedura per cifrare un messaggio fu ideata da Giulio Cesare in persona. La procedura crittografica del *codice cesareo* era alquanto ingenua. Consisteva nel sostituire ogni lettera del messaggio con un'altra lettera dell'alfabeto. Secondo una regola del tipo: sostituisce ogni lettera con la terza lettera che la segue nell'alfabeto. Così A viene sostituita da D, B da E e così via. La parola Cesare in codice diventa «fhvdoh». Sembra una parola incomprensibile. Ma un bravo criptografo non tarderà davvero molto a trovare la giusta chiave di lettura di un qualsiasi codice cesareo.

Il primo obiettivo dei codificatori è stato quello di superare l'ingenuità di Cesare ed ottenere procedure più complicate da risolvere. C'è riuscito, una volta per tutte, nel 1918 Gilbert Vernam, della *American Telephone and Telegraph Company*, con l'aiuto della matematica e del maggiore Joseph Mauborgne dello *US Army Signal Corp.* Mettendo a punto un codice assolutamente sicuro. Nessuno può decodificare un «cifrarlo Vernam» senza possederne la chiave.

La chiave. Ecco dove si sposta il problema. La chiave di un «cifrarlo Vernam» è una *chiave privata*, lunga quanto il messaggio stesso. Privata, vuol dire che due persone

che vogliono scambiarsi un messaggio segreto devono scambiarsi in segreto anche la chiave per leggerlo. Lunga quanto il messaggio stesso significa che, certo, è una chiave sicura. Ma molto scomoda. Per questo anche dopo il 1918 militari e civili hanno continuato ad usare codici più deboli del «cifrarlo Vernam» pur di avere a che fare con chiavi più brevi. Le chiavi brevi ma statisticamente ben fondate, come quella del sistema DES a rappresentazione binaria (consiste in una successione di 56 zero e uno), sono a prova anche dei più potenti computer. Ma non delle spie. Nessuno infatti può essere sicuro che la chiave privata di un messaggio segreto non cada in mani indesiderate.

Nel 1975 Whitfield Diffie e Martin Hellman propongono un nuovo sistema di crittografia, a *chiave pubblica*. In pratica si utilizzano due chiavi: una per codificare e l'altra per decodificare. La chiave di codificazione è pubblica. In modo che il messaggio possa viaggiare

sui normali mezzi di comunicazione (televisione, radio, giornali, computer). Solo l'utente in possesso della chiave di decodificazione, però, è in grado di leggere il messaggio. Il bello è che ogni singolo utente sceglie la sua chiave di decodificazione (in genere due grandi numeri primi). E non ha necessità di scambiarla. In questo sistema neppure chi invia il messaggio cifrato è poi in grado di decodificarlo. Una brava spia, però, dotata di una felpata indiscrezione potrebbe entrare in momentaneo possesso della chiave segreta costruita dall'utente e senza farsi notare leggere comodamente i messaggi segreti che viaggiano sui mezzi pubblici. D'altra parte l'israeliano Adi Shamir, del Weizmann Institute of Science, già nel 1982 era in grado di forzare uno dei sistemi crittografici a chiave pubblica. Insomma, neppure questo sistema è intrinsecamente sicuro. Così c'è già chi vede un'ondata di «portoghese elettronico» accendere alle autostrade informatiche senza

pagare il pedaggio.

Ma, per la fortuna dei criptoautori, ecco il principio di indeterminazione di Heisenberg venire in soccorso. Già nel 1970 Stephen Wiesner, della Columbia University, proponeva due applicazioni inusuali della fisica dei quanti. Una per produrre banconote non falsificabili. L'altra per codici segreti a sicurezza intrinseca. L'articolo di Wiesner viene rifiutato dalla rivista cui lo ha spedito. Così bisogna attendere il 1979 prima che Charles Bennett della IBM e Gilles Brassard dell'università di Montreal sostengano di poter costruire un sistema crittografico a chiave pubblica assolutamente sicuro affidandolo alla «discrezione delle particelle quantistiche». Dieci anni di duro lavoro e nel 1989 ecco i due presentare trionfanti presso il Thomas Watson Research Center il primo piccolo prototipo funzionante di criptografo quantistico. Fondato, appunto, sul principio di Heisenberg. E sul fatto che nessuno può «misurare» un sistema quantistico

senza perturbarlo. Nel sistema crittografico di Bennett e Brassard i messaggi quantistici a sicurezza intrinseca sono dei fotoni polarizzati lungo due direzioni. In pratica è come se a ciascun fotone fossero affidati due messaggi complementari. Ma appena una spia riesce a leggerne uno, l'altro viene immediatamente distrutto. L'incauta spia non solo si ritrova tra le mani una informazione incompleta e quindi inutile, ma lascia anche un'impronta indelebile della sua invadente curiosità. Quando arriva al destinatario il fotone porta non solo uno dei due messaggi originali, ma anche l'informazione se è stato spiato o meno. Se non è stato spiato può ricevere, pubblicamente, l'altro mezzo messaggio. Altrimenti interrompe la comunicazione.

La teoria è ben definita. Ma il problema resta quello di far viaggiare i fotoni messaggeri su lunga distanza senza perturbarli. La British Telecom nei mesi scorsi è riuscita a trasmettere un criptomessaggio quantistico su fibre ottiche a 10 chilometri di distanza. L'era delle criptocomunicazioni quantistiche sta dunque per iniziare.

A quest'era Artur Ekert vuole aggiungere un tocco di intrigo in più. Rendendo indefiniti entrambi i messaggi portati dal fotone e soprattutto consentendo di costruire una chiave di decodificazione all'atto stesso della lettura del messaggio. Più segreto di così! L'ipotesi di Ekert si basa sul principio di «non località» o di comunicazione istantanea a distanza tra coppie di fotoni inizialmente correlate. Non appena riuscirà a trovare un magazzino dove «congelare» i fotoni senza perturbarli per un tempo superiore alle poche frazioni di secondo oggi concesse e sufficiente per consentire un'accurata lettura, il fisico inglese non creerà solo un sistema di crittografia a doppia sicurezza intrinseca che rivoluzionerà il sistema di comunicazione planetario. Ma si concederà anche il lusso di smentire, simultaneamente, Edgar Allan Poe, che non credeva agli enigmi insolubili, e Albert Einstein, che non credeva alla comunicazione istantanea a distanza. E se questo vi sembra poco!

Rallenta la lotta contro la morte da morbillo

Il morbillo, la più seria delle malattie infantili, provoca ancora la morte di un milione di bambini, nei 45 milioni di casi registrati ogni anno. In una nota diffusa a Ginevra dall'Organizzazione mondiale della sanità (che ha tenuto in questi giorni la sua annuale conferenza) si rileva che la situazione all'inizio del 1994 mette in pericolo il raggiungimento dell'obiettivo fissato per l'anno prossimo: ridurre del 90 per cento il numero dei casi di morbillo nel mondo. Per evitare tale pericolo - si afferma - sarà necessario un maggiore impegno della comunità internazionale nelle misure per il controllo della malattia. Prima della campagna di vaccinazione contro il morbillo, una trentina di anni fa, la malattia colpiva praticamente tutti i bambini e su circa 130 milioni di casi all'anno i decessi si aggiravano dai 7 agli 8 milioni. Nonostante i successi conseguiti con massicci interventi di vaccinazione, il morbillo è tuttavia ancora responsabile del maggior numero di decessi rispetto a tutte le altre malattie che si possono prevenire con la vaccinazione.

La sonda «sfidata» non incontrerà l'asteroide

La sonda automatica Clementine, che ha portato a termine con successo una cartografia della Luna, non potrà partire - come invece era previsto - per l'incontro con l'asteroide Geographos, che doveva rappresentare il compito finale della sua missione. Il computer a bordo della sonda ha infatti ordinato erroneamente una lunga serie di manovre che hanno diminuito sensibilmente le riserve energetiche della sonda. Questo dispendio di energia impedirà a Clementine di intraprendere il previsto viaggio di alcuni milioni di chilometri verso l'asteroide Geographos. La missione avrebbe fornito immagini senza precedenti di un asteroide. L'incontro avrebbe dovuto avvenire in agosto. Il Pentagono (da cui dipende la sonda che originariamente era parte del programma Guerre stellari) ha modificato i programmi sostituendo la missione scientifica finale con una serie di test militari.

Un odore del passato... e torna la memoria

Cari odori del passato, struggenti e dimenticate fragranze che non esistono più, ma anche fetori di tempi antichi. Questa mescolanza di poesia e durezza è alla base di una nuova e rivoluzionaria terapia che in Gran Bretagna starebbe dando risultati sorprendenti.

«Regalano una nuova vita a chi conduce un'esistenza vuota e priva di sogni», sostiene l'ideatore dell'inconosciuto rimedio al quale nessuno aveva ancora pensato. Fred Dale pensa soprattutto agli anziani sprofondata nell'apatia, condannati all'inattività e alla mestizia: la «terapia degli odori» schiude loro le porte di una «seconda vita» risvegliando memorie sopite, accendendo di splendidi luci ricordi appannati, dando sensazioni nuove e idee palpitanti anche a chi pareva condannato ad una vita priva di un passato interessante.

Basta annusare e torna alla mente un mondo dimenticato, si intrecciano stimolanti rimembranze, si emerge all'improvviso da un

oggi inutile e senza senso che spesso è l'anticamera di malattie senili che conducono a una morte che si poteva evitare.

Per mettere a punto questi terapeutici tuffi nel passato Dale iniziò a collaborare cinque anni orsono con il dottor Mark O'Donnel dell'ospedale Clifton di Blackpool ed ha avviato ora, con risultati assolutamente inattesi, il primo corso ufficiale di «terapia degli odori». «Un successo che neanche io mi attendevo», confessa.

Con l'ausilio di un semplice odore persone che non ricordano che cosa hanno fatto due ore prima sono ora in grado di dire che cosa accadeva quel giorno del 1922 o che cosa disse Churchill alla radio quella tragica notte.

Dale, che «colleziona» odori da molti anni «chiudendoli» in bottiglia, è riuscito anche - ricorrendo a sostanze chimiche - a ricreare molti che egli stesso non aveva mai sentiti: quello della legna che si bruciava nel camino in un determinato periodo, degli ingredienti del

La terapia degli odori potrebbe far tornare la memoria (ma soprattutto la gioia di vivere) a milioni di persone anziane. Ad idearla è stato un inglese, Fred Dale, che da anni colleziona odori chiudendoli dentro bottigliette. Dale ha così ricreato il profumo degli ingredienti di un dolce di Pasqua degli anni '20 o quello degli armadi di

campagna dell'inizio del secolo. Ma anche il tanfo delle stalle vittoriane e il fetore delle trincee della prima guerra mondiale. Le bottigliette «miracolose», una volta annusate, hanno prodotto effetti stupefacenti, a detta di Dale. Nonnine che non parlavano più da anni, improvvisamente hanno cantato le canzoni della gioventù.

STEPHEN BERNARDELLI

dolce di Pasqua degli anni '20, o quello degli armadi di campagna dei primi decenni del secolo. Ma è andato anche oltre: ha «costruito» per un museo il lezzo di una latrina dell'800, il tanfo delle stalle vittoriane e anche il fetore nelle trincee della prima guerra mondiale. E' il lavoro con gli anziani che però lo stimola in modo particolare. Racconta della vecchiaia di un ospizio che ha improvvisamente citato a memoria il numero della sua tessera di raziamento dopo avere annusato l'odore della farina che si

vendeva a Londra durante la guerra. O quello della bisnonna che non parlava da anni e che, dopo avere sentito un odore simile a quello della sua valigia di bambina, un misto di fragranza di mele, panni lavati col sapone di Marsiglia, e cartone bagnato ha iniziato a recitare una poesia di quando andava a scuola.

Annusare e ricordare è, naturalmente, una conseguenza del saper distinguere gli odori. Recentemente, una ricerca della John Hopkins University negli Stati Uniti, ha dimo-

strato che servono tre passaggi fondamentali perché un odore possa essere recepito. Il primo passaggio è quello propriamente chimico: le molecole che «voicollano» l'odore vengono a contatto con gli appositi recettori che si trovano nelle cellule olfattive che sono nel naso. Il secondo passaggio prevede una sorta di amplificazione di ogni segnale all'interno delle cellule: ogni singola molecola dà, infatti, ad una cascata di decine di migliaia di messaggi intercellulari. Il terzo passaggio è la trasformazione di questi messaggi in segnali elettrici che sti-

molano i nervi i quali a loro volta inviano il segnale al cervello. A quel punto è quella che chiamiamo coscienza ad entrare in gioco e noi percepiamo così gli odori.

Secondo il professor Randall Reed, della John Hopkins, la struttura dei recettori olfattivi e del loro sistema di segnalazione è molto simile a quella «incaricata» di recepire la luce.

I recettori molecolari incaricati di «annusare» l'ambiente intorno sarebbero tra i cinquecento e gli ottocento. Secondo il professor Reed, questi recettori sono in grado di «annusare» circa diecimila differenti molecole. Il che non vuol dire distinguere davvero così tanti odori. La capacità di memorizzare e di reagire a certi stimoli chimici consente in media ad ogni persona di distinguere qualche centinaio di odori.

Questo però significa che non tutti siamo in grado di distinguere gli stessi odori. Per esempio, sostiene una ricerca condotta in Gran Bretagna un anno fa, il dieci per