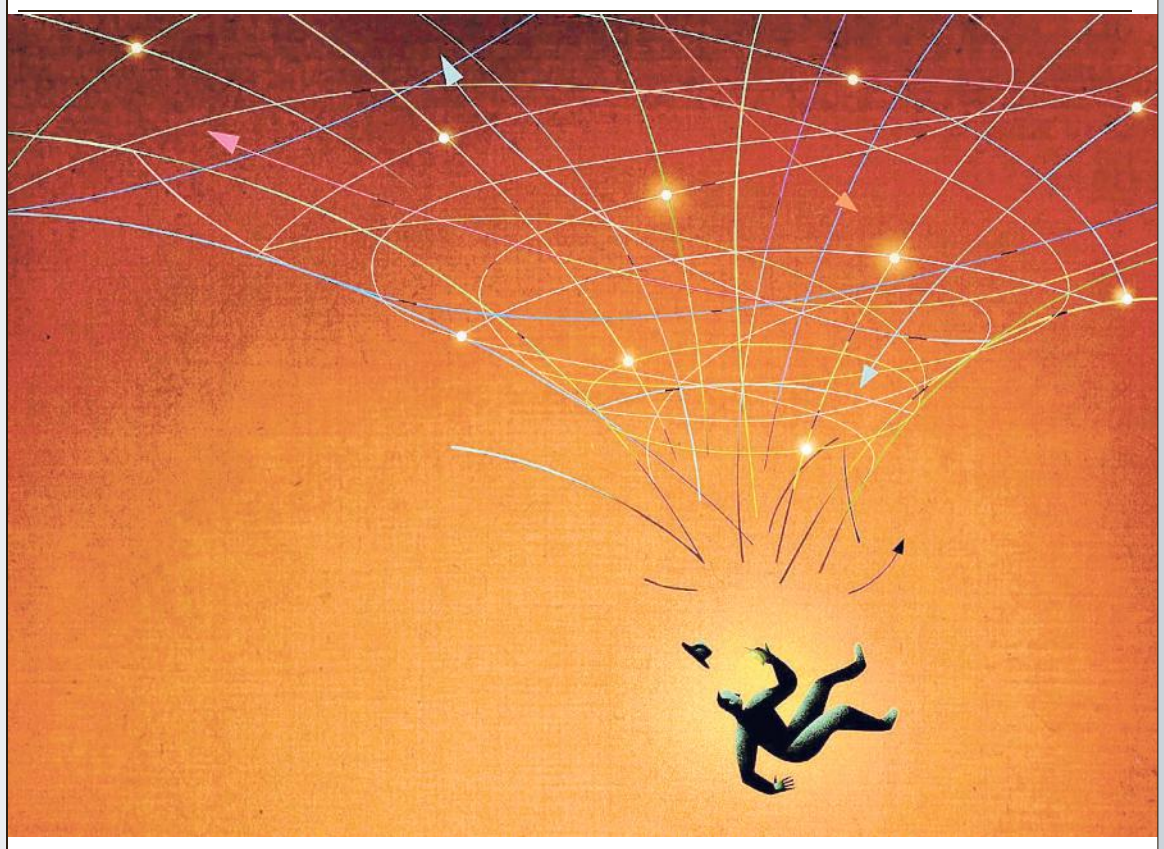
"Quando la Rete era di noi ribelli"

È uno storico scienziato del web, innovatore della crittografia e premio Turing 2015 Ma anche un irregolare che ama i romanzi dei grandi dissidenti sovietici, come Solgenitsin e Kopelev Ed è pensando a loro che rilancia l'allarme sui rischi dell'era digitale



PIERGIORGIO ODIFREDDI

I capelli di Whitfield Diffie sono ormai bianchi, ma la loro lunghezza fin oltre le spalle ricorda che colui che li porta è stato per mezzo secolo un ribelle. Non a caso, la sua storia è raccontata in un libro di Steven Levy intitolato *Crypto: come i ribelli dei codici sconfissero il governo e salvarono la privacy nell'era digitale* (Shake, 2002).
Le armi con cui Diffie e il suo collega Martin Hellmann hanno combattuto la loro battaglia per la privacy contro l'Agenzia per la Sicurezza nazionale (Nsa) statunitense sono state la crittografia a chiave pubblica e la firma digitale, che sono valse ad entrambi il premio Turing per l'informatica nel 2015.

Quando ha iniziato a pensare alla rete e ai suoi problemi?
«Era l'agosto del 1973 e stavo chiacchierando con la mia futura moglie Mary, su una panchina di un parco. A un certo punto dissi che in futuro il computer avrebbe permesso alla gente di instaurare profonde relazioni con perfetti sconosciuti. Lei rispose che ero matto. Poi si convinse che avevo ragione e collaborammo insieme a risolvere al problema».

Che problema era, precisamente?
«Che le telecomunicazioni avrebbero presto sostituito molte delle comunicazioni a tu per tu. E questo avrebbe sostanzialmente modificato i meccanismi naturali della privacy, che secondo me costituiscono uno degli aspetti fondamentali della cultura. Bisognava dunque aggiornare questi vecchi meccanismi, per renderli più adatti ai nuovi tipi di comunicazione».

Ma la rete allora non era ancora diffusa.
«Non fra il pubblico. Ma io avevo potuto usare a lungo l'Arpanet del Dipartimento della Difesa, lavorando al Laboratorio di Intelligenza artificiale di Stanford con John McCarthy, uno dei padri dell'intelligenza artificiale, e immaginavo cosa sarebbe successo».

Cioè che, come si dice, Al Gore avrebbe inventato Internet?
«Questo lo dicono i giornalisti, ma è una grossa semplificazione mediatica. Quello che lui fece, e di cui bisogna dargli credito, fu far approvare al Senato nel 1991 la cosiddetta Legge Gore, che aprì la via alla "superstrada dell'informazione". Ma in realtà la rete esisteva ben prima, e serviva a connettere vari laboratori e dipartimenti governativi, direttamente o indirettamente legati ai militari».

La rete fu inventata per motivi strategici?
«Anche questa sembra essere un'invenzione. La realtà è che Bob Taylor, che era direttore dell'Arpa nei primi anni '60, aveva nel suo ufficio vari terminali, ciascuno connesso con un particolare progetto, e gli venne l'idea di farli collegare in qualche modo, in modo che potessero parlarsi fra loro in maniera più efficiente che passando attraverso lui. Ma è certamente possibile che in seguito la cosa sia stata giustificata in termini strategici: soprattutto dopo il cosiddetto Emendamento Mansfield del 1973, che costrinse l'Arpa a lavorare solo a progetti con applicazioni militari».

Tornando a lei?
«La mia preoccupazione era appunto la sicurezza delle comunicazioni. Già nel 1965 un mio amico di nome Bill Mann, che lavorava per la Nsa, mi aveva detto, sbagliando, che le conversazioni telefoniche nell'edificio dove lui lavorava erano criptate. Non era vero, e all'epoca non si sapeva come farlo, ma io cominciai a pensare come si sarebbe potuto fare, e soprattutto che vantaggio ci sarebbe stato a farlo. Ho sempre avuto un atteggiamento antisistema, ed è questa motivazione che mi ha portato alla crittografia a chiave pubblica».

Quando ottenne i suoi primi risultati?
«Alla fine degli anni '60 il mio ufficio era nello stesso edificio in cui si sviluppava il Progetto Multics, il sistema operativo dal quale sono poi nati tutti quelli moderni, da Unix a Windows. Multics conteneva un meccanismo molto elaborato per la protezione dei file, ma la cosa non mi soddisfaceva perché l'amministratore del sistema poteva comunque aggirare le protezioni. La mia idea era che l'unico modo veramente sicuro di proteggere i file fosse che l'utente mantenesse un controllo diretto delle chiavi di accesso».

E oggi?
«In linea di principio possiamo proteggere le nostre comunicazioni, anche se da quarant'anni uno dei principali fallimenti in questo campo è la mancata soluzione del cosiddetto "problema del confinamento": come assicurarsi che le informazioni che vengono date a qualcuno non vengano poi passate ad altri. O, più in generale, come evitare che l'esecuzione di un programma produca danni collaterali».

Quindi bisogna trovare il modo di certificare la correttezza di un programma?
«No. Certificare la correttezza è meno di quello che intendo: è come evitare di finire ai servizi sociali, mentre io intendo evitare di finire in prigione. O evitare di finire in quello che Solgenitsin chiamava *Il primo cerchio*, invece che nel vero e proprio *Arcipelago Gulag*. Tra l'altro, il romanzo di Solgenitsin racconta di condannati mandati in un laboratorio di ricerca nei sobborghi di Mosca a fare un lavoro top secret, che guarda caso era in parte crittografico».

Beh, in fondo Solgenitsin era un matematico, e nella sua autobiografia per la Fondazione Nobel dice che la matematica gli ha salvato la vita due volte.
«Ah, non lo sapevo! Lei conosce *Allevia i miei dispiaceri* di Lev Kopelev, che fu l'ispirazione del protagonista di *Il primo cerchio*? Io lo trovo anche più interessante, perché si tratta di memorie, e non solo di un romanzo. Mi sarebbe piaciuto incontrare il dissidente Kopelev: peccato che non mi sia mai capitato».

> È dai lontani anni '60 che la sicurezza della comunicazioni mi preoccupa: sarà forse il mio istinto antisistema
>
> Ancora oggi troppi programmi producono effetti collaterali devastanti: questo è il vero problema

Chi è

Whitfield Diffie (Washington, 1944) è uno scienziato informatico, pioniere della crittografia a chiave pubblica

Estratto avviso accertamenti tecnici non ripetibili procedimento penale n. 2488/2017 R.G.N.R. Mod.21

Procura della Repubblica presso il Tribunale di Paola Avviso di accertamenti tecnici non ripetibili - art. 360 cpp – Proc. pen. n. 2488/2017 R.G.N.R. Mod. 21

Il Sostituto Procuratore della Repubblica, visti gli atti del proc. pen. in oggetto, iscritto nei confronti di... omissis...; per il reato di cui agli arti. 113, 430 e 449 co. 2 del cp - in Paola in data 06/12/2017.

AVVISA

le parti offese, ovvero passeggeri e personale di bordo presenti all'atto dello sviamento dai binari del treno regionale n. 3742, oggetto di indagine; che è stato fissato per le ore 15:00 del decimo giorno successivo alla data di pubblicazione del presente avviso sula Gazzetta Ufficiale della Repubblica Italiana, in Paola, presso il Palazzo di Giustizia, Procura Repubblica, piano 5°, il conferimento dell'incarico diretto agli accertamenti tecnici inerenti i motivi che hanno determinato l'incidente ferroviario di che trattasi, ovvero: 1) estrapolazione e conservazione dei dati informatici presenti nella scatola nera o in altro supporto/sistema informatico atto alla loro conservazione/archiviazione; 2) esame dei luoghi del sinistro occorso in data 06/12/2017, con eventuale raccolta di campioni di materiali e relative analisi; 3) quant'altro utile a fini di giustizia nonché all'esito degli accertamenti prefati;

AVVISA

le persone offese che hanno facoltà di prendere visione degli atti e delle cose trasmesse dall'ufficio del P.M. e presentare memorie/produrre documenti. Paola. 20 dicembre 2017.

IL SOSTITUTO PROCURATORE DELLA REPUBBLICA
Antonio Lepre