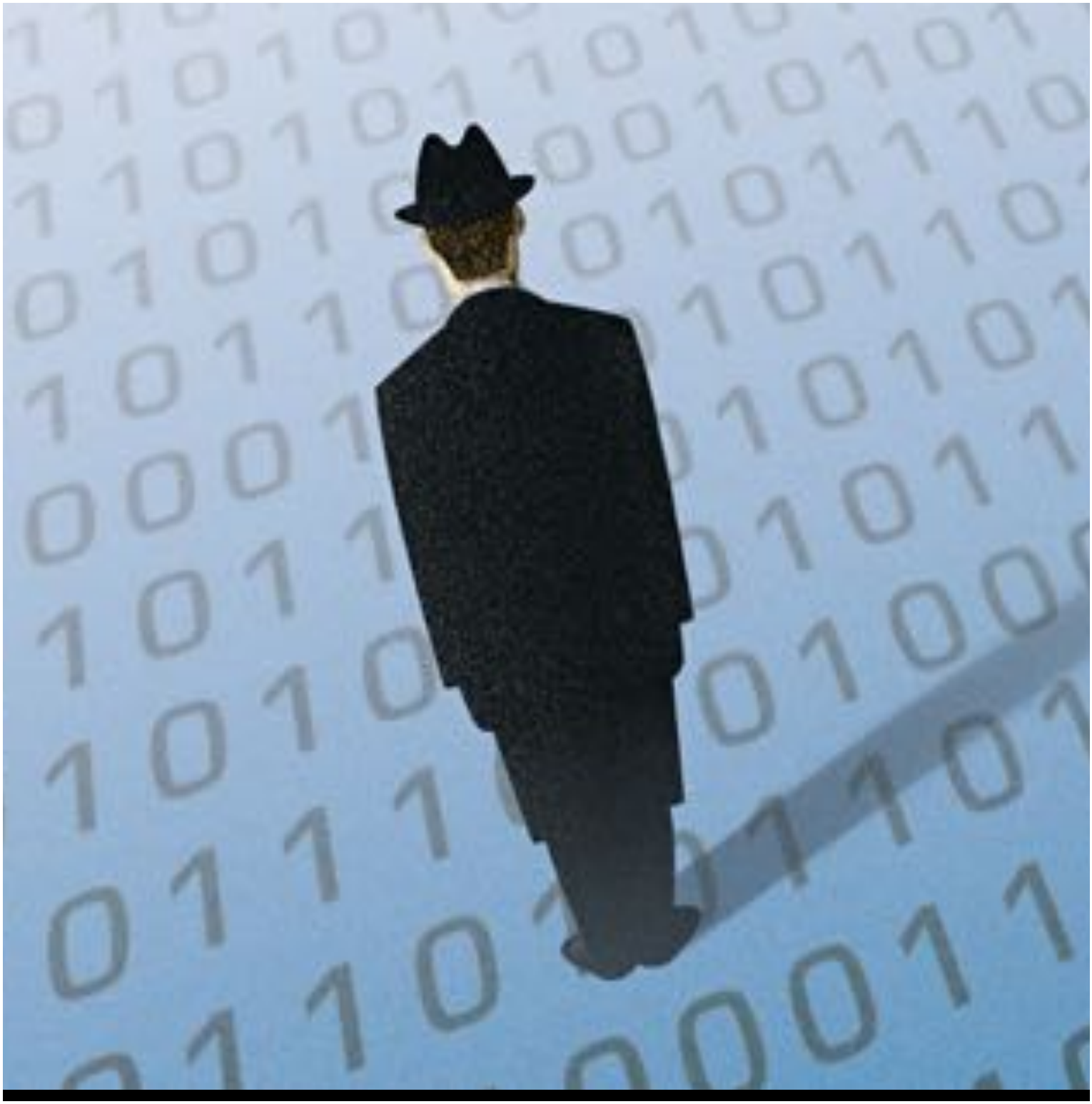

L’informazione come scienza, risorsa e struttura della realtà

Il suo ruolo nella Seconda Guerra Mondiale, nella più moderna tecnologia e nell’ontologia della realtà fondamentale

Marco Rossini – Liceo Scientifico A. Oriani – A.S. 2013/2014

Indice

Introduzione

Questo lavoro si propone di illustrare il significato del concetto di informazione relativamente a come esso risulta definito in campo scientifico. A questa iniziale premessa seguirà un primo approfondimento che vedrà coinvolte alcune delle applicazioni pratiche del concetto di informazione nel campo della comunicazione, e in cui sarà esaminata la loro importanza storica nell'ambito della Seconda Guerra Mondiale. Compiuta questa analisi sul passato, si avrà modo di tornare nel presente, dove verrà illustrato come l'importanza dell'informazione abbia oggi spronato i fisici a giungere alla realizzazione di dispositivi di calcolo straordinari. L'ultima sezione di questo fascicolo cercherà infine di addentrarsi all'interno di un intricato tema filosofico, in cui si esamineranno alcuni tra i principali orientamenti di pensiero che oggi cercano faticosamente di fornire un'ontologia alla realtà fondamentale, e in cui si avrà modo di constatare come il concetto di informazione giochi un ruolo significativo. Sempre in questa sezione, si vedranno alcuni punti di contatto che avvicinano queste posizioni moderne con le speculazioni filosofiche di Friedrich Nietzsche.
Al termine del fascicolo si potrà trovare una sezione conclusiva in cui è riportato un passo di un libro che, nell'opinione dell'autore dell'elaborato, ottimamente si presta a compendiare quanto di fondamentale è straordinariamente connaturato nel concetto protagonista di questo lavoro.

1 – L'informazione come concetto scientifico

*Il termine **informazione** assume nel linguaggio comune una pluralità di significati, talvolta vaghi e poco chiari, ma in ambito scientifico essa corrisponde ad un concetto ben preciso, definito da Claude Shannon nel 1948. Per informazione si intende una quantità di dati associata ad una grandezza chiamata **entropia**, la cui unità di misura è il **bit**. A livello matematico l'informazione è associata ad una **variabile aleatoria** che può essere discreta o continua. Il concetto di informazione trova largo impiego nelle discipline della **crittografia** e della **crittoanalisi**.*

1.1 – Una definizione scientifica di informazione

La notazione scientifica di informazione è stata chiarita da Claude Shannon, matematico e ingegnere americano, nel 1948 come la misura del **numero di alternative possibili** per qualcosa.

Per esempio, se lancio un dado, questo può cadere su 6 facce. Se vedo che è caduto su una faccia particolare, ho una quantità di informazione N = 6, perché sei erano le possibilità alternative. Se non so che giorno sia il compleanno di Pietro, ci sono 365 possibilità diverse. Se Pietro mi dice che giorno è il suo compleanno, ho un'informazione N = 365. E così via.

Invece del numero di alternative N, per indicare l'informazione è più conveniente usare il logaritmo in base 2 di N, chiamato S, che prende il nome di **entropia**.
L'informazione di Shannon, quindi, è:

$$S = log_2 N$$

dove N è il numero di alternative.

In questo modo, l'unità di misura S = 1 corrisponde a N = 2 (perché 1 = $\log_2 2$), cioè all'alternativa minima, che comprende due sulle possibilità.
Questa unità di misura è l'informazione fra due sole alternative ed è chiamata "**bit**".

1.2 – Cos'è un bit?

Il termine **bit**, in informatica e in teoria dell'informazione, assume tre significati molto diversi a seconda del contesto in cui rispettivamente lo si usi.

1) Il bit come quantità di informazione

In questo contesto, un bit rappresenta **l'unità di misura della quantità d'informazione** come è stata definita da Shannon.

Partendo dalla definizione statistica dell'entropia termodinamica, Shannon intuì che l'informazione e questa grandezza termodinamica fossero in qualche modo correlati.

L'informazione viene matematicamente espressa dalla relazione:

$$I = -log_2 P$$

che, utilizzando il logaritmo in base 2 della probabilità P che si verifichi un dato evento, permette di ottenere un valore misurato in bit. Questa quantità prende il nome di **autoinformazione**.

Dall'entropia espressa dalla relazione di Boltzmann, Shannon ricavò l'uguaglianza:

$$S = log_2 P$$

che permette di esprimere l'entropia nella medesima unità di misura dell'informazione, ovvero il bit, e dimostrò che vale la relazione:

$$I = -S$$

che si può enunciare come *"a un aumento di entropia corrisponde una perdita di informazione su un dato sistema, e viceversa"*.

2) Il bit come cifra binaria
In questo contesto, il bit rappresenta **l'unità di definizione di uno stato logico**.

Ciò significa che un bit viene associato a due sole cifre {0,1} in una stringa di codice, ognuna delle quali rappresenta uno specifico stato di qualcosa. Per esempio, l'interruttore della luce spento può essere associato alla cifra 0 e l'interruttore acceso alla cifra 1: in questo modo ognuna delle cifre trasmette 1 bit di informazione, poiché comunica in quale dei due stati l'interruttore si trova.
Nel sistema binario, quindi, i numeri sono formati da sequenze di 0 e 1, che in base alla loro posizione assumono un significato diverso.

Nei computer, per esempio, la presenza o l'assenza di carica sulle piastre di un condensatore rappresenta un bit. A livello atomico si possono usare due stati di eccitazione di un elettrone in un atomo (in cui lo 0 rappresenta lo stato meno eccitato e 1 quello più eccitato).

3) Il bit come qualità di colore
In questo contesto, il bit è l'espressione della **qualità del colore** di un apparecchio elettronico.

Nella computer grafica viene chiamata "profondità di colore" la quantità di bit necessari per rappresentare il colore di un singolo pixel in un'immagine, e la sua unità di misura è il bit per pixel (simbolo bpp). Con l'aumentare del numero di bit per pixel aumenta anche la quantità di colori possibili e, quindi, profondità di colore superiori offrono una gamma più vasta di tonalità distinte.
In questo campo il numero di bit raddoppia sempre (ad esempio 8 bit → 16 bit → 32 bit → 64 bit e così via).

1.3 – Entropia di una variabile aleatoria

Una **sorgente** di informazione è un'entità che emette *messaggi di informazione*.
Ad esempio, in una comunicazione telefonica, la sorgente di informazione è un essere umano che emette messaggi vocali, mentre in una comunicazione dati la sorgente di informazione è un calcolatore che emette messaggi alfanumerici (caratteri e numeri), tipicamente rappresentati da stringhe di bit.

Le sorgenti dei messaggi possono essere **discrete** o **continue**: una sorgente si dice discreta quando i suoi messaggi sono una sequenza di elementi appartenente a un insieme numerabile, come le sorgenti di numeri interi o di parole scritte; le sorgenti che non sono discrete vengono dette continue, come per esempio le sorgenti di musica e di conversazione.

A livello matematico, l'entropia di una sorgente è associata ad una **variabile aleatoria X** ed è definita come il **valor medio dell'autoinformazione** I(X) della variabile aleatoria:

$$H(X) = M[I(X)] = -M[log_2 P(X)]$$

Se il numero di valori che può assumere X è finito, allora il valor medio si riduce ad una media dell'autoinformazione di ogni simbolo x_i, pesata con la propria probabilità $P(x_i)$:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \cdot \log_2 P(x_i)$$

Se invece X è una variabile aleatoria continua, il valore atteso dell'autoinformazione deve essere calcolato attraverso un integrale:

$$H(X) = -\int P(x) \cdot log_2 P(x) dx$$

1 bit equivale ad esempio all'informazione ottenibile dal lancio di una moneta (P = 0,5), che rappresenta un sistema binario.

Come si può notare dalla **Figura 1**, il massimo dell'entropia di un sistema binario si verifica nelle condizioni di equiprobabilità (P = 0,5) e vale:

$$log_2 2 = 1$$

cioè 1 bit.

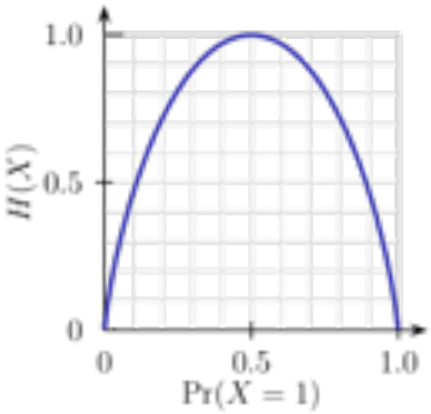

Figura 1 – Grafico dell'entropia di una sorgente binaria (lancio di una moneta).

1.4 – Applicazioni: crittografia e crittoanalisi

Tra le applicazioni della teoria dell'informazione, un ruolo di grande importanza ricoprono le due discipline, tra loro antagoniste, della crittografia e della crittoanalisi.
La **crittografia** è la scienza che studia le tecniche che permettano la manipolazione delle informazioni in modo da renderle incomprensibili alle persone non autorizzate.
La **crittoanalisi** è invece la scienza che studia i metodi per giungere al significato di informazioni cifrate.

2 – Crittografia e crittoanalisi nella Seconda Guerra Mondiale

*Probabilmente in nessun'altra guerra come nella **Seconda Guerra Mondiale** la crittografia ha svolto un ruolo di primo piano. Il secondo conflitto mondiale fu una vera e propria "**guerra dei codici**" combattuta a distanza fra crittografi e crittoanalisti. In questa guerra comparvero diverse macchine a rotori simili nel funzionamento, ma i dispositivi più noti sono sicuramente quelli della macchina **Enigma**, utilizzata dalla **Germania** e decifrata dal **Regno Unito**, e della macchina **Purple**, utilizzata dal **Giappone** e decifrata dagli **Stati Uniti**.*

2.1 – La macchina Enigma

Storia

La macchina Enigma nacque molto prima della Seconda Guerra Mondiale per scopi non militari. Realizzata nel 1918 dall'ingegnere berlinese Scherbius, era stata ideata per proteggere i grandi industriali dell'epoca dal fenomeno dello spionaggio industriale. Diversi esemplari furono acquistati dalla Marina Militare tedesca e, dal 1929, il dispositivo venne acquisito dall'Esercito tedesco.
Durante la guerra, versioni di Enigma furono usate in Germania per quasi tutte le comunicazioni radio, spesso anche per quelle telegrafiche.

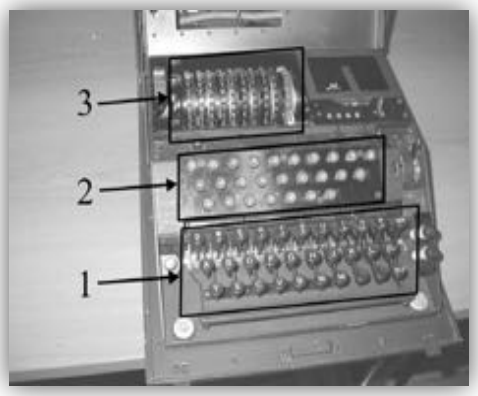

Figura 2 – Una macchina Enigma.
1) tastiera fisica, 2) tastiera luminosa, 3) rotori.

Struttura e funzionamento

La macchina Enigma aveva l'aspetto di una macchina per scrivere con due tastiere, costituita da lettere luminose che si accendevano su una **tastiera luminosa** (2) ad ogni tasto premuto sulla **tastiera fisica** (1). La sequenza delle lettere che si illuminavano dava il messaggio cifrato (o quello in chiaro, se si digitava il testo cifrato). Il suo funzionamento si basava su tre dischi cablati, detti **rotori** (3), che avevano 26 contatti per lato (uno per ogni lettera dell'alfabeto tedesco): i cablaggi dei dischi mettevano in comunicazione ciascuna lettera su un lato con una diversa lettera sull'altro lato. I dischi erano collegati insieme da un particolare meccanismo: il primo disco ruotava di una lettera ad ogni pressione di tasto, il secondo ruotava di una lettera ogni volta che il primo compiva un giro e il terzo ruotava di una lettera quando il secondo finiva un giro. I rotori erano imperniati su un medesimo asse ed era possibile cambiare l'ordine di disposizione dei tre dischi. Inoltre tali rotori erano scelti e riscambiati ogni giorno da un gruppo di cinque esemplari per questioni di sicurezza.

Nella parte anteriore della macchina c'era un'altra sezione, denominata "**pannello dei collegamenti**". Erano disponibili dieci cavi, con uno spinotto a entrambe le estremità, che servivano per scambiare tra loro coppie di lettere prima dell'immissione nel rotore, così da aumentare la sicurezza del codice.

Figura 3 – Pannello dei collegamenti di una macchina Enigma.

Le impostazioni della macchina costituivano la chiave per poter effettuare opportunamente la criptazione e la decriptazione del messaggio.

Il sistema di codifica della macchina Enigma era così sofisticato che nessuno riteneva possibile la decriptazione dei suoi messaggi: il modello base, costituito da soli tre rotori, permetteva già di arrivare a circa 150 milioni di milioni di milioni di combinazioni diverse.

2.2 – La lotta contro Enigma

Una spia tedesca al servizio della Francia

Le prime brecce nel cuore di Enigma poterono aprirsi grazie al contributo di una spia, **Hans Thilo Schmidt**, un funzionario dell'Ufficio Cifra dell'esercito tedesco, che nel 1931 cominciò a consegnare ai servizi segreti francesi i manuali operativi di Enigma. Scoperto nel 1943, si suicidò in carcere per evitare le torture. I manuali di utilizzo, tuttavia, non consentivano da soli di capire la chiave utilizzata per codificare un testo, anche perché le chiavi di cifratura venivano cambiate costantemente, persino più volte al giorno.

Dalla Francia alla Polonia

I servizi segreti francesi decisero quindi di rivolgersi alla Polonia. I servizi segreti polacchi, infatti, erano riusciti ad intercettare una valigia diplomatica contenente un esemplare della macchina Enigma. A Varsavia operava un agguerrito gruppo di crittografi guidati dal matematico **Marian Rejewski**, che nell'agosto 1932 riuscì per la prima volta a violare Enigma. Una volta ricostruita la struttura logica di Enigma, Rejewski progettò e costruì la "**bomba crittologica**", un rudimentale calcolatore in grado di eseguire gradualmente una decodifica dei messaggi. Tuttavia, i successi rimasero limitati: non era sufficiente comprendere le chiavi, ma anche farlo velocemente. Conoscere in tempo reale il senso delle comunicazioni intercettate era di fondamentale importanza, mentre spesso i crittoanalisti polacchi stentavano a capire il senso di messaggi risalenti a mesi o a settimane prima. Inoltre la situazione si aggravò quando tra il 1938 e il 1939 i Tedeschi cambiarono le regole di cifratura, aumentando il numero dei rotori da tre a cinque e rendendo quasi inefficace il metodo polacco.

Dalla Polonia alla Gran Bretagna

Con l'invasione della Polonia da parte dei nazisti, la lotta per la violazione di Enigma si spostò in Gran Bretagna. Nell'agosto del 1939 i Britannici costituirono una scuola dei codici e dei cifrari a **Bletchley Park** nel Buckinghamshire, vicino Londra. Qui iniziò una guerra parallela, una vera e propria partita a scacchi, tra gli inglesi che cercavano di decrittare i messaggi dei tedeschi il più velocemente possibile e questi ultimi che cambiavano costantemente le chiavi e perfezionavano le loro macchine. Tra coloro che lavoravano a Bletchley Park c'erano esperti di ogni genere, ma soprattutto ingegneri e matematici, che venivano reclutati tramite un concorso. Inconsapevolmente, gli stessi Tedeschi aiutarono gli Inglesi a decifrare Enigma, infatti i messaggi contenevano spesso le stesse espressioni: molti cominciavano con il medesimo testo di apertura, oppure venivano riportate informazioni di routine e, soprattutto, tutti i messaggi si concludevano con l'espressione "Heil Hitler!". Queste disattenzioni fornirono ai decifratori indizi sul modo in cui era stata impostata Enigma in quel giorno che diventavano fondamentali per risalire

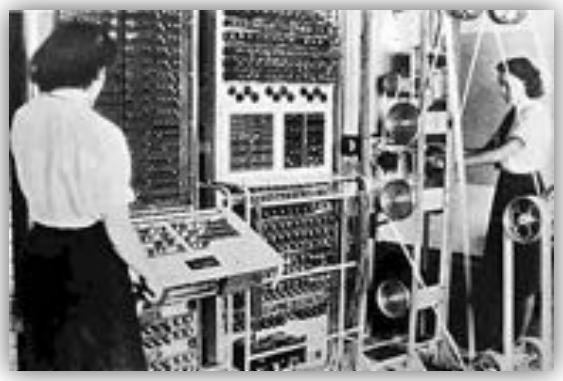

Figura 4 – Il calcolatore "Colossus" progettato da Alan Turing,

all'informazione originale. Le informazioni segretissime ottenute dai britannici vennero denominate informazioni **ULTRA** (o UltraSecret)

Alan Turing
Nella squadra di ricercatori inglesi c'era un giovanissimo matematico di nome **Alan Turing**, che riprogettò la “bomba” polacca dando origine a “**Colossus”**, il primo calcolatore elettronico assemblato a Bletchley Park nel febbraio del 1944. Turing svolse un ruolo fondamentale nel forzare il più complesso cifrario dell’ Enigma navale, denominato shark. Nel 1941, infatti, la guerra aveva cominciato a svolgersi anche nell’Atlantico e il 9 maggio ci fu una battaglia tra il sottomarino tedesco U-Boot 110 e alcune navi inglesi. La squadra inglese vinse lo scontro e riuscì a recuperare un esemplare integro della macchina Enigma, il suo manuale e le tavole per la disposizione dei rotori. Grazie a questo episodio e al lavoro degli uomini di Bletchley Park, gli storici sostengono che la durata del conflitto è stata ridotta di diversi anni. Ad un certo punto della guerra i crittoanalisti britannici divennero così abili nelle decifrazioni in tempo reale al punto da essere in grado, in rari casi, di tradurre gli ordini dei comandanti (e dello stesso Hitler) prima ancora che questi giungessero ai loro destinatari designati.

Curiosità
Per ragioni di sicurezza, il governo britannico decise di mantenere segreto ogni evento accaduto a Bletchley Park fino a trent’anni dopo la fine della guerra, gettando nel dimenticatoio gli sforzi instancabili compiuti dai matematici al servizio del governo inglese.

Alan Turing è rimasto, infatti, a lungo un genio incompreso, e solo nel 2004 l’Inghilterra gli ha dedicato una statua. Turing entrò in depressione e morì, in circostanze non del tutto chiare, nel giugno 1954, a 42 anni. La statua che gli è stata dedicata, a Manchester, lo ritrae con una mela in mano. La versione ufficiale vuole infatti che egli abbia, più o meno volontariamente, ingerito del cianuro accompagnandolo ad una mela. Questo gesto può trovare giustificazione nello stato di terribile depressione in cui Turing era caduto a causa della sua omosessualità, considerata reato dalle allora vigenti leggi inglesi che gli avevano imposto la castrazione chimica.

Vent’anni dopo, nella Silicon Valley californiana, sorgerà una famosa compagnia costruttrice di computer, la "**Apple**", il cui simbolo sarà una mela morsicata proprio in onore di Alan Turing.

2.3 – Il ruolo di ULTRA nelle vicende alleate

Battaglia di capo Matapan (27-29 marzo 1941)
La disfatta della flotta italiana nel sud della Grecia pare abbia avuto origine dal fatto che gli inglesi avessero decrittato alcuni messaggi cifrati della marina tedesca che fornivano l'esatta posizione della flotta italiana.

Sbarco in Normandia (6 giugno 1944)
I generali alleati Eisenhower e Montgomery furono in grado di leggere tutti i messaggi degli alti comandi tedeschi. Ebbero così la conferma che Hitler aveva creduto alla falsa notizia di un imminente sbarco alleato nei pressi della città di Calais, e che aveva per questo concentrato le sue migliori truppe in quella zona. Grazie alle intercettazioni, gli alleati conobbero anche le disposizioni delle truppe tedesche in Normandia e poterono quindi ordinare lo sbarco in territorio francese contro un avversario impreparato che giocava a carte scoperte.

2.4 – La macchina Purple

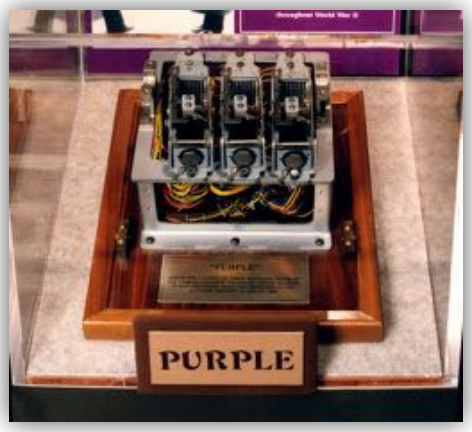

Figura 5 – Il frammento più grande di macchina Purple sopravvissuto al conflitto.

Storia

Negli anni '30 i giapponesi idearono una nuova macchina cifrante che presentava qualche novità significativa rispetto alle molte altre macchine allora in uso: invece di usare i classici rotori come nella macchina Enigma, si usavano dei **commutatori** (o switch) di tipo telefonico, in modo da rendere meno prevedibile la rotazione dei rotori. La macchina, che gli Americani designarono con il nome in codice di **Purple**, aveva inoltre la curiosa caratteristica di dividere l'alfabeto di 26 caratteri in due gruppi distinti, uno di venti lettere e l'altro di sei lettere. I giapponesi, come i tedeschi con Enigma, erano convinti che la macchina fosse inattaccabile, ma ancora una volta non fu così. William Friedman, il massimo crittologo americano, già nel settembre 1940, dopo mesi di sforzi enormi, riuscì a decrittarla.

2.5 – Il ruolo di MAGIC nelle vicende alleate

Meno problematicamente rispetto ad Enigma, il funzionamento di Purple fu scoperto dal *Signals Intelligence Service* (SIS), il gruppo del crittoanalista statunitense **William Friedman**, nel settembre 1940, che riuscì anche a creare una copia della macchina. Così il flusso di decrittazioni, nome in codice **MAGIC**, partì immediatamente.

L'attacco di Pearl Harbor e la teoria della cospirazione (7 dicembre 1941)

L'ex agente segreto statunitense Allen Dulles scrive che:

> « Entro il 1941, che fu l'anno di Pearl Harbor, i nostri crittoanalisti avevano decifrato la maggior parte dei più importanti codici giapponesi diplomatici e navali; di conseguenza, abbiamo avuto spesso le prove di un'imminente azione giapponese nel Pacifico prima che questa avesse luogo ».
>
> (Allen Dulles, L'arte del servizio segreto, Garzanti, Milano, 1963, p. 95)

Questa affermazione sembrerebbe provare la "teoria della cospirazione" di Gore Vidal.
Secondo questo storico americano, gli Stati Uniti, grazie a MAGIC, sapevano in anticipo dell'attacco di Pearl Harbor, ma decisero di non impedirlo; avevano infatti bisogno di un motivo forte per convincere la riluttante opinione pubblica americana della necessità di entrare in guerra, e un attacco a tradimento dei Giapponesi sarebbe stato ideale per questo scopo.

Una teoria più prudente sostiene che gli Americani sapessero che il Giappone era sul punto di attaccare, ma non sapevano esattamente dove. Casualità o meno, sta di fatto che, al momento dell'attacco, nella baia di Pearl Harbor non c'era nemmeno una portaerei, poiché avevano tutte ricevuto l'ordine di portarsi in alto mare nelle settimane precedenti, così che furono affondate solo navi relativamente vecchie e di importanza non fondamentale per la guerra.

Un altro elemento di sospetto, per i sostenitori della teoria della cospirazione, può essere individuato nei misteriosi contrattempi che costrinsero l'ambasciatore giapponese a presentare la dichiarazione di guerra agli americani con qualche ora di ritardo rispetto all'inizio dell'attacco, trasformandolo in un vergognoso attacco a tradimento. I giapponesi, volevano infatti sferrare l'attacco mezz'ora dopo la consegna della dichiarazione di guerra, per beneficiare al massimo del fattore sorpresa, ma una serie di complicazioni nelle

comunicazioni fece si che la dichiarazione venne recapitata solo dopo, causando grande indignazione.

Alla fine della guerra, il generale Marshall ammise che in molti casi di importanza "non vitale" gli alleati dovettero fingere di non conoscere i messaggi cifrati nemici, anche al costo di perdite umane, tale era il timore che tedeschi e giapponesi si accorgessero che i loro cifrari venivano sistematicamente decrittati.
Se l'attacco di Pearl Harbor possa essere annoverato tra questi casi resta un mistero, ed è ben difficile che ciò possa mai essere confermato ufficialmente, considerato che in quell'occasione morirono circa tremila cittadini americani.

La battaglia delle Midway (4-6 giugno 1942)
Dopo l'entrata in guerra, nel marzo del 1942 gli americani riuscirono finalmente a decifrare completamente il codice usato dalla Marina nipponica. Il 14 maggio dello stesso anno, vennero intercettate e decifrate nuove comunicazioni giapponesi che annunciavano una prossima azione di una poderosa flotta aero-navale nipponica nei pressi di un punto chiamato "AF". Il punto AF creò divergenze d'opinione all'interno della marina militare statunitense, poiché alcuni credevano che esso indicasse le Isole Aleautine, mentre altri lo identificavano con le Midway.
La questione fu risolta il 19 maggio, quando l'ammiraglio Chester William Nimitz, per ingannare i giapponesi, ordinò all'ufficiale Joseph Rochefort di inviare un messaggio in chiaro dalle Midway a Washington in cui si comunicava che l'impianto di desalinizzazione era guasto. Il messaggio fu inviato usando un cifrario che si sapeva essere stato forzato dai giapponesi, e che fu quindi ovviamente intercettato dai loro servizi segreti navali, i quali scrissero a Tokio che AF, dato un guasto all'impianto di desalinizzazione, aveva riserve di acqua di sole due settimane.
Intercettazioni successive confermarono che l'offensiva nipponica sarebbe iniziata tra il 3 e il 4 giugno. Grazie al lavoro di Rochefort, gli Americani non si presentarono impreparati all'appuntamento del 4 giugno e poterono vincere la più grande battaglia aerea della guerra.

Morte dell'ammiraglio giapponese Yamamoto (18 aprile 1943)
Un altro importante risultato favorito dalla crittografia statunitense si ebbe nell'aprile 1943, quando sedici caccia P-38 abbatterono l'aereo personale dell'ammiraglio Yamamoto, comandante in capo della flotta giapponese, e elevato a eroe nazionale in Giappone dopo Pearl Harbor.

Conoscendo ormai completamente il codice giapponese, gli americani furono in grado di decifrare un loro messaggio intercettato il 13 aprile 1943. Il testo in chiaro era stupefacente: erano descritti in modo dettagliato tutti gli spostamenti aerei che il temuto ammiraglio Yamamoto avrebbe tenuto il 18 aprile. L'eliminazione di Yamamoto poteva rappresentare un notevole colpo psicologico per i giapponesi, che non avevano altri militari di simile valore.
Ottenuta l'approvazione del Ministro della Marina americana Frank Knox e del presidente Roosevelt, poté prendere forma il piano per l'eliminazione elaborato dall'ammiraglio Nimitz e da altri miliari statunitensi. Il 18 aprile, dalla base di Guadalcanal, si alzò in volo una squadriglia di P-38 che intercettarono l'aereo di Yamamoto e la sua scorta nei pressi di Bougainville, nelle Isole Salomone. Dopo una breve sparatoria, l'aereo dell'ammiraglio precipitò in fiamme.

Rimane sorprendente il fatto che i Giapponesi non attribuirono l'abbattimento dell'aereo alla scoperta dei loro codici da parte dello spionaggio americano. Così come i Tedeschi credevano inviolabile Enigma, anche i Giapponesi ritenevano i loro messaggi cifrati con la macchina Purple assolutamente sicuri; così il lavoro dei crittoanalisti americani poté proseguire indisturbato fino alla fine del conflitto.

3 – I quantum computer

*Al giorno d'oggi la battaglia tra crittografi e crittoanalisti sembra vedere i primi favoriti, in quanto gli avanzati sistemi di crittografia a cui siamo pervenuti (come l'**algoritmo RSA**) rivelano che decifrare certi codici richieda tempi insostenibilmente lunghi per i calcolatori ordinari. Tuttavia, è già stato costruito un dispositivo chiamato "**quantum computer**", uno speciale calcolatore che, sfruttando i principi della **meccanica quantistica**, sarebbe in grado di eseguire innumerevoli operazioni in breve tempo. Ma ciò non può considerarsi una vittoria per i crittoanalisti, poiché, allo stesso modo di una **crittoanalisi quantistica**, è nata anche una **crittografia quantistica**.*

3.1 – L'algoritmo RSA

La sigla RSA indica uno dei più efficaci algoritmi utilizzati in crittografia.
Semplificando, questo è il suo funzionamento:

Immaginiamo che A debba spedire un messaggio segreto a B.

1) B sceglie due numeri primi molto grandi (per esempio di 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
2) B invia il numero che ha ottenuto ad A. Chiunque può vedere questo numero.
3) A usa questo numero per cifrare il messaggio.
4) A manda il messaggio cifrato a B, chiunque può vederlo, ma non decifrarlo.
5) B riceve il messaggio e, utilizzando i due fattori primi che solo lui conosceva, lo decifra.

A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi con cui si può decifrare il messaggio. Infatti fattorizzare in numeri primi (cioè scomporre un numero nei suoi divisori primi) è un'operazione estremamente lenta, basti pensare che il miglior algoritmo classico conosciuto impiegherebbe circa 5×10^{24} passi per fattorizzare un numero di 300 cifre, ossia circa 150.000 anni alla velocità di un terahertz.

3.2 – Un supercalcolatore

Da anni i matematici sono alla ricerca di una scorciatoia per la scomposizione dei numeri primi, ma tale operazione sembra irrisolvibile dal punto di vista teorico. Tutto ciò che si può fare è velocizzare il processo dal punto di vista tecnologico. Immaginiamo di essere in possesso di un calcolatore con potenza illimitata; esso sarebbe in grado di scomporre un qualsiasi numero nei suoi fattori primi in breve tempo. Al giorno d'oggi il prototipo di un calcolatore simile è già stato costruito: si tratta del quantum computer.

3.3 – L'ostacolo del principio di indeterminazione

Così come i computer tradizionali seguono le leggi della meccanica classica, i quantum computer seguono le leggi della meccanica quantistica.

Prima di procedere ad illustrarne il funzionamento occorre però precisare come l'informazione in senso scientifico, che si è visto essere una quantità precisa e determinata, possa essere inserita in un contesto quantistico noto per essere governato dall'indeterminazione.

Nella fisica dei quanti infatti, il principio di indeterminazione enunciato da Heisenberg rappresenta un limite insuperabile imposto dalla natura, che ostacola la precisione delle misurazioni. Secondo questo principio, non è possibile conoscere con assoluta precisione sia la posizione che la velocità di una particella: se si misura esattamente la posizione di una particella, contemporaneamente questa inizierà a muoversi in un intervallo di velocità; allo stesso modo se si misura la velocità in modo esatto, non si conoscerà con esattezza la posizione della particella. Ciò rende queste variabili inaffidabili per immagazzinare informazioni.

Fortunatamente però, gli scienziati si sono resi conto che questo ostacolo può essere aggirato. Il mondo quantistico è infatti sì dominato dall'indeterminazione, ma non tutte le misurazioni quantistiche sono soggette a questa limitazione. Nei casi in cui posizione e velocità sono indeterminate, altre proprietà, come l'energia, possono essere definite.

Di solito l'energia è infatti una variabile definita, ed è proprio questa sua proprietà a rappresentare la chiave di funzionamento dei computer quantistici.

Come si vedrà tra poco, la variabile definita dell'energia può infatti essere resa, con opportune manipolazioni, indefinita e poi di nuovo definita a piacimento, sfruttando nel suo momento indefinito l'enorme potenziale offerto dalla fisica quantistica.

3.4 – Un sistema binario alternativo

Come si è accennato nel primo capitolo di questo fascicolo, nei computer tradizionali un bit è associato ad un sistema fisico rappresentato dalla presenza o dall'assenza di carica sulle piastre di un condensatore.

Esiste tuttavia un secondo sistema fisico, che obbedisce sempre alle leggi della meccanica classica, a cui può essere associato un bit per costruire le porte logiche dei computer tradizionali. Questo sistema fisico è quello atomico, in cui si possono usare due stati energetici di un elettrone in un atomo, con "0" rappresentato dallo stato di minore energia, e "1" dallo stato di più alta energia.

Per manipolare questa informazione, i fisici inviano impulsi di luce sull'atomo. Un impulso con una data frequenza, durata e ampiezza, noto come impulso π, manda lo stato 0 nello stato 1 e viceversa. I fisici possono regolare questa frequenza per manipolare due atomi interagenti, in modo che uno controlli ciò che accade sull'altro. Questi elementi costituiscono gli ingredienti necessari per costruire porte logiche a uno o due bit, i mattoni dei computer tradizionali.

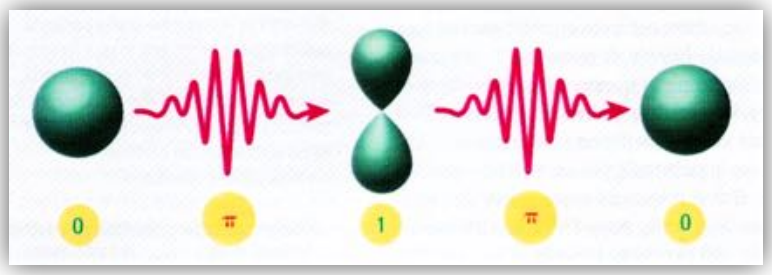

Figura 6 – Un impulso π inverte il valore di un bit. Se l'elettrone era nello stato fondamentale 0 si troverà nello stato 1, e viceversa.
(*Illustrazione tratta da "Le Scienze n°531, novembre 2012, p. 92"*)

3.5 – Un terzo sistema fisico

Se nella meccanica classica un bit può esistere in due stati distinti, in meccanica quantistica può anche esistere in una loro sovrapposizione coerente. Si tratta di un terzo stato, che non ha un analogo nella fisica classica, in cui l'atomo rappresenta entrambi i valori 0 e 1 contemporaneamente.

Infatti, mentre un impulso π scambia gli stati 0 e 1, un impulso della stessa frequenza, ma con una durata o un'ampiezza dimezzata, noto come impulso π/2, manda un elettrone nella sovrapposizione di stati 0 e 1.

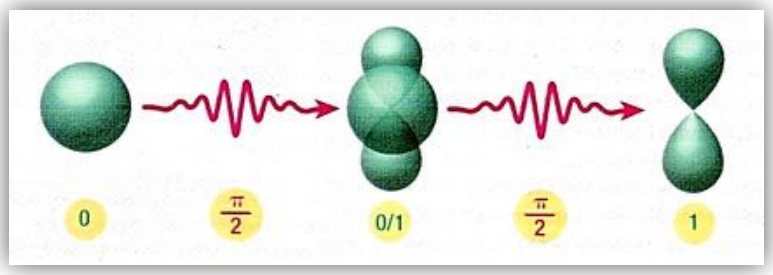

Figura 7 – Un impulso π/2 manda un elettrone dallo stato 0 o 1 in una sovrapposizione dei due stati.
(*Illustrazione tratta da "Le Scienze n°531, novembre 2012, p. 92"*)

3.6 – Dai bit ai qubit

Nel mondo macroscopico la fisica classica fornisce certezze sulle misurazioni e sulle osservazioni che effettuiamo. Il computer "classico" appartiene a questa logica, dove le unità fondamentali dell'informazione, i bit, sono governati da certezze: si sa in ogni momento se un certo bit valga "0", oppure "1".

Ma quando scendiamo nel microscopico la fisica classica va in crisi e lascia spazio a quella quantistica, basata appunto sulla probabilità e mai sulla certezza. La teoria quantistica, dunque, non ci dice mai "il valore è 1" oppure "il valore è 0", ma descrivei sistemi come una sovrapposizione di stati diversi che esistono contemporaneamente.

È per questa ragione che, nei computer "quantistici", non si hanno più dei bit, ma dei **qubit** (quantum bit). I qubit sono unità di informazione quantistica che possono contenere, sovrapposti, tutti i possibili stati compresi tra 0 e 1, ossia infiniti stati. Questi qubit sono rappresentati dagli stati sovrapposti di particelle elementari, come gli stati energetici degli elettroni nell'atomo, lo spin degli elettroni o gli stati di polarizzazione dei fotoni.

Nel mondo classico un elettrone può avere "spin su" oppure "spin giù", mentre nel mondo quantistico lo spin può essere in uno stato di sovrapposizione, ossia in una qualsivoglia combinazione delle due direzioni, per esempio il 70% "spin su" e il 30% "spin giù".
L'intero sistema è, quindi, un aggregato incredibilmente complesso di sovrapposizioni di tutte le possibili combinazioni di spin di ciascuna particella.

3.6 – Un'informazione infinita?

Si sarebbe così tentati di concludere che un solo qubit, almeno in linea di principio, possa tranquillamente

contenere una quantità d'informazione pari a tutto lo scibile umano.
Ma, in termini pratici, non è così, perché interviene un altro poco intuitivo principio della meccanica quantistica: quando si effettua una misura su un sistema quantistico che è in sovrapposizione di stati, questo "collassa" su un solo preciso valore. L'esito della misurazione dello stato di un qubit può infatti essere soltanto 0 oppure 1. Quindi, dalla misurazione di un qubit, è possibile ottenere la stessa quantità di informazione rappresentabile con un bit classico.

Ma se dalla misurazione di un qubit è possibile ottenere la stessa quantità di informazione rappresentabile con un normale bit, perché si afferma che un computer quantistico è enormemente più veloce e potente di un computer classico?

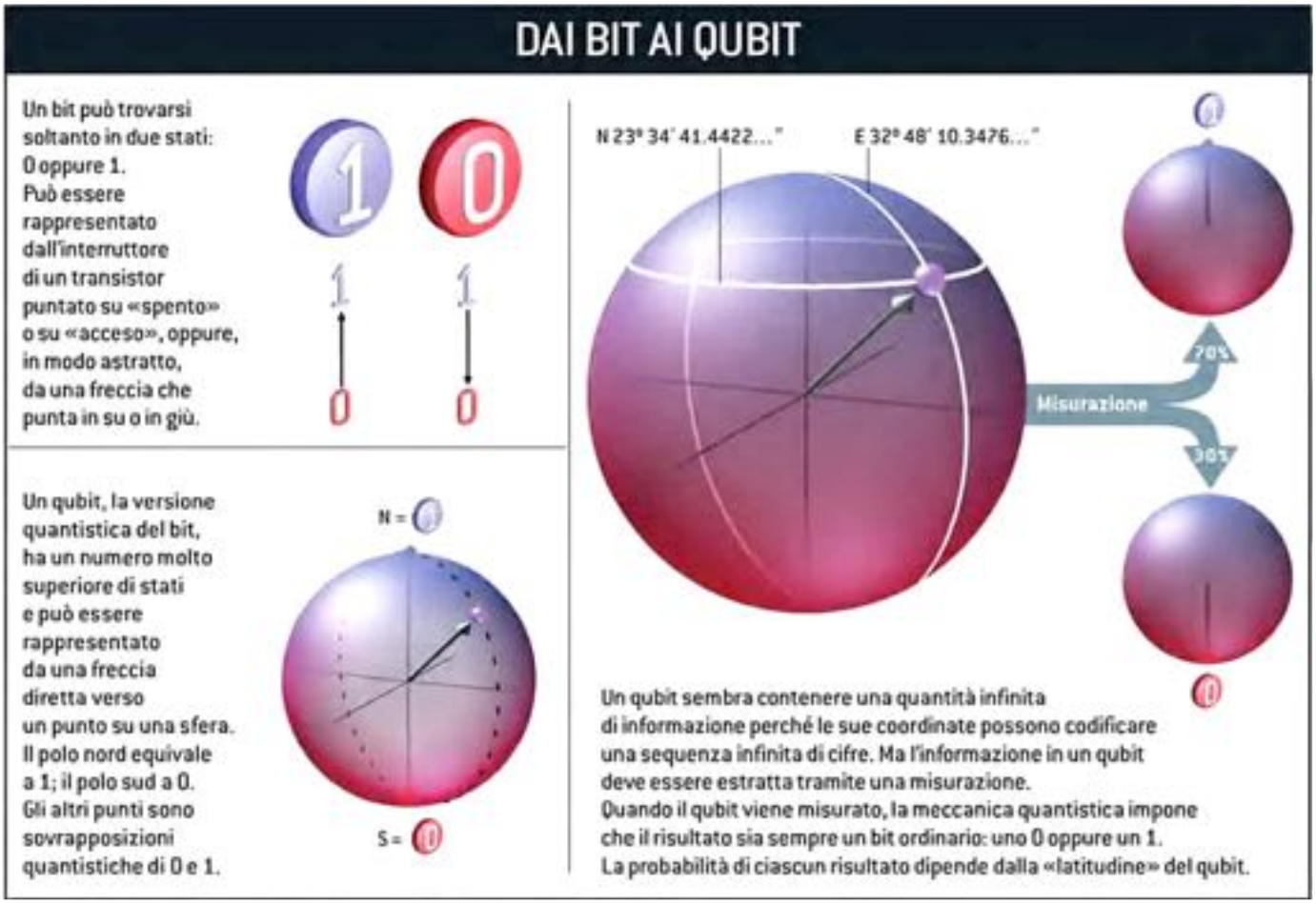

Figura 8 – (*Illustrazione tratta da "Le Scienze n°412, dicembre 2002, pag. 72"*)

3.7 – Sfruttare la sovrapposizione

Effettivamente, a causa di questo principio del collasso, se cercassimo di misurare l'energia dell'elettrone nella sovrapposizione di stati lo troveremmo nello stato di minore energia o di maggiore energia con uguale probabilità, scontrandoci di nuovo con un problema di casualità.

Ma ancora una volta possiamo aggirare questo apparente ostacolo e creare nuove funzionalità.
Colpendo infatti un atomo con un impulso $\pi/2$, come si è visto, l'elettrone entra nella sovrapposizione di stati 0 e 1. Ma colpendolo nuovamente con un altro impulso $\pi/2$, esso ritorna in uno stato definito, che ha la particolarità di negare quello precedente (se si parte da 0 si giunge ad 1, viceversa se si parte da 1 si

giunge a 0).
La soluzione, perciò, non consiste nel misurare l'energia dell'elettrone quando esso si trova nel suo stato

indefinito, ma di lasciarlo inalterato nella sua condizione indeterminata. In questo stato particolare, esso è in grado di compiere in pochi istanti un'operazione richiesta lavorando su innumerevoli valori contemporaneamente, e il risultato di questa operazione può poi tornare a noi sotto forma di informazione precisa e definita.

3.8 – Crittografia e crittoanalisi quantistiche

È evidente come un calcolatore di questo tipo possa costituire una minaccia implacabile per la sicurezza dei sistemi crittografici tradizionali.

Come si è visto infatti, la forza dell'algoritmo RSA risiedeva proprio in un limite di tipo temporale: pur non essendo sicuro da un punto di vista matematico teorico, in quanto si conosce la procedura per decrittare il messaggio, l'enorme mole di calcoli e l'enorme dispendio in termini di tempo necessario a svolgerli faceva di questo algoritmo un sistema di affidabilità pressoché assoluta.
Con l'avvento dei quantum computer, però, questo tipo di sistema non può più offrire alcuna protezione, poiché l'enorme potenza di calcolo di questi dispositivi sarebbe in grado di decifrare un codice RSA in pochi secondi.

Ma questa minaccia sembra però non essere tale.
Insieme alla crittoanalisi quantistica è nata infatti anche una crittografia quantistica, che ad oggi pare totalmente impenetrabile. Essa fonda la propria invulnerabilità sul principio fisico per cui se si cerca di intervenire in qualsiasi modo su un sistema quantistico (per esempio nel tentativo di decifrarlo) esso subisce alterazioni inevitabili e permanenti che vengono notate dalle due parti che comunicano, rivelando la presenza di un intruso.

La crittografia è giunta oggi ad punto di arrivo: con il metodo quantistico ha a disposizione una cifratura sicura al 100%. A detta degli scienziati del campo, nessuna geniale intuizione crittoanalitica riuscirà a scalfire minimamente la sicurezza della crittografia quantistica. Ma possiamo davvero esserne sicuri? A loro tempo sia la macchina Enigma che la macchina Purple erano state ritenute impenetrabili, così come lo stesso algoritmo RSA. Ogni volta però i crittoanalisti sono riusciti a provare il contrario, rilevando i punti deboli di queste cifrature. Uno scettico potrebbe quindi supporre che è solo questione di tempo, prima che anche la crittografia quantistica riveli il suo punto debole. In realtà, la situazione odierna è ben diversa da qualsiasi altra: la sicurezza di questo metodo è infatti provata dal punto di vista teorico oltre che pratico. In tutti i casi visti in passato, la sicurezza di una cifratura derivava dalla sua ingegnosità, ma non è mai stata provata matematicamente. La crittografia quantistica è invece costruita su una base teorica: la teoria dei quanti e, se si rivelasse decifrabile, negherebbe la teoria stessa, con conseguenze sconvolgenti per il mondo della fisica.

3.10 – I limiti della computazione quantistica

Per quanto si ritenga che un domani sia destinata a rappresentare una sicura frontiera della tecnologia, la computazione quantistica presenta oggi ancora grossi limiti: tra questi, la necessità di dover innescare i fenomeni a temperature prossime allo zero assoluto che conservino il delicato equilibrio delle particelle e la necessità di dover arginare l'interazione particelle-ambiente che causa una perdita di informazione.

3.11 – Scenari futuri

Quando si approfondisce la conoscenza della realtà, si approfondisce anche la conoscenza nei regni astratti della logica e della matematica, e la meccanica quantistica pare destinata a trasformare anche questi mondi. In fondo, nonostante le verità matematiche siano indipendenti dalla fisica, ne possiamo acquisire una conoscenza attraverso i processi fisici, e quali di queste possiamo conoscere dipende da quali sono le leggi della fisica. Una prova matematica è una sequenza di operazioni logiche, quindi ciò che è dimostrabile e ciò che non lo è dipende da quali operazioni logiche le leggi della fisica permettono di realizzare.
Se diventassero una realtà, i quantum computer consentirebbero ai matematici di guardare oltre la barriera dell’astrazione, permettendo loro di vedere e dimostrare verità che altrimenti sarebbero rimaste nascoste per sempre. Essi potrebbero dimostrare teoremi attraverso metodi che il cervello umano (o un calcolatore classico) non sarebbe in grado nella maniera più assoluta di controllare, perché se la sequenza di proposizioni corrispondente alla dimostrazione intesa nel senso classico venisse stampata, la carta riempirebbe l’universo osservabile per molte volte.

4 – La natura delle cose

*I fisici cercano di descrivere il mondo subatomico ricorrendo ai concetti relativi a due presunti costituenti fondamentali della realtà: le **particelle** e i **campi di forze**. Ma non è chiaro che cosa siano le particelle e i campi di forze in ambito quantistico. Forse a essere veramente importanti non sono le cose in sé, ma le loro **relazioni**. Un'altra idea è che il mondo potrebbe essere composto da **fasci di proprietà**, che fanno essere le cose al loro radunarsi. La filosofia di **Friedrich Nietzsche** trova dei punti di contatto con queste riflessioni sulla realtà.*

4.1 – La ricerca di un'ontologia

Al giorno d'oggi i fisici possono contare su una valida teoria che descrive le leggi del mondo subatomico: la teoria quantistica dei campi. I fisici teorici l'hanno sviluppata tra la fine degli anni venti e l'inizio degli anni cinquanta, unendo la meccanica quantistica con la teoria della relatività ristretta di Einstein. Questa teoria descrive i costituenti fondamentali della materia e le loro interazioni, ed in termini di precisione empirica è la teoria di maggior successo nella storia della scienza. Con a disposizione una teoria così efficace del microscopico può quindi sorprendere che i fisici non siano però ancora sicuri di che cosa sia in realtà il mondo subatomico, di quale sia la sua **ontologia**.

4.2 – Particelle e campi

In questo contesto, i fisici si riferiscono a due descrizioni diverse di un costituente fondamentale: alcuni si riferiscono a "particelle", altri a "campi" in una distinzione che appare artificiale, tanto che spesso i fisici si esprimono in modo da attribuire un ruolo più fondamentale alle une o agli altri.

Il concetto di particella è infatti molto vago, poiché di questi presunti oggetti, secondo la meccanica quantistica, non possiamo dire la posizione precisa. Esse mostrano comportamenti non locali, il loro posizionamento appare diverso a seconda della dinamica degli osservatori, non si possono contare con precisione, nel vuoto appaiono e poi scompaiono. In un fenomeno quantistico enigmatico (chiamato *entanglement*), poi, le particelle possono addirittura perdere la propria individualità: non si sa se siano due, una sola o un "qualcosa" che fa parte di un tutto.
Per queste ragioni risulta difficile sostenere che ciò che chiamiamo "particella" sia quello che il nome evoca. Nel mondo microscopico c'è dunque qualcosa, ma non sembra corrispondere all'idea a priori con il quale lo identifichiamo. Se una "particella" ha una essenza che non coincide con un "qualcosa", allora quel qualcosa non è una particella.

Per quanto riguarda i campi, i problemi sono relativi al fatto che la loro quantizzazione è una operazione matematica che non assegna valori a veri e propri osservabili, ma a probabilità diffuse in un certo spazio. In pratica, la descrizione a campi è produttiva se operata in linguaggio matematico, ma non è traducibile in linguaggio comune.

4.3 – Le proposte della filosofia

L'incapacità della fisica di fornire oggi una sicura ontologia ai concetti fondamentali di particelle e campi cede il passo alla filosofia per la ricerca di un loro fondamento valido.

Il realismo strutturale epistemico

In questo contesto, molti filosofi pensano che siano le relazioni in cui si trovano le cose a essere importanti, non le cose stesse. Questa posizione, detta realismo strutturale, apparve in un primo momento in una

versione moderata, nota come **realismo strutturale epistemico**. Secondo questa concezione, è possibile che non conosceremo mai la vera natura delle cose, ma solo come sono correlate tra loro. Un esempio è il concetto di massa: noi non vediamo la massa in sé, ma vediamo solo le sue relazioni con altri enti o, concretamente, come un corpo dotato di massa interagisce con un altro corpo dotato di massa attraverso il campo gravitazionale.
La constatazione oggettiva di questi comportamenti fisici, indipendentemente dalla descrizione matematica delle loro leggi fisiche, prende il nome di **struttura**.

Il realismo strutturale ontico
Ma qual è la ragione per cui possiamo conoscere solo le relazioni fra le cose e non le cose stesse?
La risposta più semplice è che non esiste altro che le relazioni.

Questo salto fa del realismo strutturale un approccio più radicale, che prende il nome di **realismo strutturale ontico**.
Ciò che fornisce credibilità a questa posizione sono le innumerevoli simmetrie della fisica, consistenti in certi cambiamenti di configurazione del mondo, noti come trasformazioni di simmetria, che non hanno conseguenze empiriche. Queste trasformazioni scambiano i singoli oggetti che compongono il mondo lasciando immutate le loro relazioni. Esse sono analoghe alla trasformazione di simmetria che esercita sul nostro viso uno specchio: esso scambia l'occhio destro con quello sinistro, la narice destra con quella sinistra e così via, ma le posizioni relative di tutti i tratti del viso rimangono identiche. Le particelle e i campi hanno simmetrie più astratte, ma l'idea è la stessa.

Il principio metodologico del rasoio di Occam, ritenuto alla base del pensiero scientifico moderno, suggerisce l'inutilità di formulare più ipotesi di quelle che siano strettamente necessarie per spiegare un dato fenomeno quando quelle iniziali siano sufficienti. In virtù di questo principio, largamente adottato in campo scientifico, è possibile quindi costruire una teoria valida ipotizzando l'esistenza di relazioni specifiche senza ipotizzare anche quella degli oggetti. Per i sostenitori del realismo strutturale ontico, quindi, possiamo fare a meno delle cose e supporre che il mondo sia fatto di strutture e di reti di relazioni.

Nella vita quotidiana sperimentiamo molte situazioni in cui contano solo le relazioni e in cui risulterebbe pleonastico approfondire le caratteristiche degli oggetti stessi. Per esempio, trovandosi davanti alla necessità di compiere un viaggio in treno risulta fondamentale sapere come le stazioni delle varie città sono collegate tra loro, per sapere quando bisogna effettuare un cambio. Il fatto che una certa stazione sia stata ristrutturata di recente non ha nessuna importanza per qualcuno che cerchi di orientarsi tra i collegamenti ferroviari.

Un terzo realismo strutturale
Potrebbe però sembrare strano che siano possibili relazioni senza relati, ossia senza oggetti in relazione. Effettivamente molti fisici e filosofi trovano impossibile ottenere oggetti solidi solo sulla base di questi legami. Esiste infatti una terza posizione che cerca un compromesso tra queste assunzioni, non negando l'esistenza degli oggetti, ma affermando che le relazioni abbiano ontologicamente la precedenza.

L'ontologia dei tropi
Oltre alle posizioni di realismo strutturale, sembra esistere un altro scenario che possa dare significato alla teoria quantistica dei campi.

Anche se i concetti di particelle e campi sono ritenuti diversi tra loro, essi conservano come caratteristica comune l'assunto per cui gli oggetti fondamentali del mondo materiale siano entità dotate di **proprietà**. Per i sostenitori di questa posizione, la distinzione tra oggetti e proprietà può rappresentare il motivo profondo per cui gli approcci basati su particelle e campi hanno entrambi difficoltà, ritenendo sia meglio considerare il concetto di proprietà come l'unica e fondamentale categoria.

Nella nostra vita quotidiana osserviamo oggetti dotati di particolari proprietà che non possono esistere indipendentemente. Per esempio, quando pensiamo al rosso di solito pensiamo a specifiche cose rosse, non a qualcosa che corrisponde alla rossezza (diversamente da come potrebbe pensare Platone).
Se capovolgessimo questo modo di pensare, potremmo considerare le proprietà come dotate di esistenza, indipendentemente dagli oggetti che le hanno. In questo modo, ciò che chiamiamo "cosa" potrebbe essere solo un fascio di proprietà: colore, forma, consistenza e così via.
All'interno di questa posizione filosofica queste proprietà prendono il nome di **tropi**.

Vedere il mondo per fasci di proprietà non è il modo con cui siamo abituati a concettualizzarlo, ma è possibile risalire a questo modo di vedere la realtà riflettendo sulle percezioni dirette dell'infanzia. Da neonati quando vediamo e sperimentiamo per la prima volta una palla, non percepiamo veramente una palla a pensarci bene. Quello che percepiamo è una forma rotonda, le sfumature dei suoi colori, una certa consistenza elastica. Solo in seguito associamo questo fascio di percezioni ad un oggetto coerente che chiamiamo palla, dimenticando nelle volte successive tutto l'apparto concettuale coinvolto in questa percezione immediata.

L'ontologia dei tropi sfrutta proprio questo modo di vedere la realtà. Nel mondo, le cose non sono altro che fasci di proprietà: non si parte da una palla per attribuirle delle proprietà, si parte dalle sue proprietà e la si chiama palla. Una palla è le sue proprietà.

Applicando questa idea alla teoria quantistica dei campi, l'elettrone è in realtà un fascio di varie proprietà: massa, carica, spin, posizione e velocità. Questa concezione della realtà fornisce un senso alla teoria. Per esempio, la teoria prevede che le particelle elementari possano improvvisamente smettere di esistere, facendo rilevare agli strumenti di rilevazione dei fisici (i contatori Geiger) un valore medio del numero di particelle pari a zero; eppure questi strumenti rivelano che in realtà questo vuoto ribolle di attività, poiché in esso avvengono continuamente numerosi processi che provocano la creazione e la distruzione di particelle di tutti i tipi.
In un'ontologia basata sulle particelle questa attività è paradossale, infatti se le particelle sono fondamentali, come fanno a materializzarsi? Da cosa si materializzano? Nell'ontologia dei tropi la situazione è naturale, poiché il vuoto, anche se privo di particelle, contiene proprietà. Una particella è ciò che si ottiene quando queste proprietà si radunano insieme in un certo modo.

Un bilancio
Facendo un bilancio di queste posizioni filosofiche, il concetto di "cosa" può o venire eliminato (realismo strutturale ontico) o mantenersi (primo e terzo realismo strutturale e filosofia dei tropi).
Laddove mantenuta, però, la "cosa" non sarebbe qualcosa che ha cause, ma sarebbe essa stessa il risultato di una relazione di cause. Ne segue una definitiva distruzione del "**cosale**" in favore di un "**relazionale**".

Il concetto di relazionale avvicina in maniera significativa questi orientamenti di pensiero con la speciale visione del mondo che Friedrich Nietzsche espone ne *"La volontà di potenza"*.

4.4 – L'ontologia della realtà secondo Nietzsche

Per quanto la sua formazione fosse in massima parte filologica e poi votata alla filosofia, nel corso della sua vita Nietzsche aveva saputo prestare un occhio di riguardo anche nei confronti della scienza. L'indagine scientifica, tuttavia, va ad assumere per lui un significato sempre funzionale ad una speculazione filosofica, orientata verso una critica della metafisica tradizionale e della morale. Nei suoi ultimi scritti egli arriva ad abbozzare una vera e propria ontologia della realtà ispirata alle scienze del suo tempo.

Il ruolo della scienza in Nietzsche

Una prima valutazione che Nietzsche riserva alla scienza può essere spiegata facendo riferimento a *Umano, troppo umano* (1878), in cui il filosofo tedesco riflette sulle contraddizioni intrinseche alla forma di vita platonico-cristiana come mortificazione dell'esistenza terrena in nome di una vita ultraterrena. Secondo lui da questo atteggiamento di fondo è nato un "mondo morale" a cui gli uomini hanno affidato la ricerca di un fondamento stabile, di un riparo nei confronti delle incertezze della vita e del sapere. Nietzsche ricercherà l'alternativa a questo mondo morale nella scienza, come scriverà ne *La volontà di potenza*:

> « La scienza è stata finora l'eliminazione della mescolanza totale fra le cose, mediante ipotesi che "spiegano" tutto partendo dalla ripugnanza dell'intelletto per il caos. […] La *fisica* risulta *benefica* per lo spirito; la scienza (come via per la *conoscenza*) riceve un nuovo fascino dopo l'eliminazione della morale. »
>
> (F. Nietzsche, *La volontà di potenza*, Bompiani, Milano, 1992, pp. 331-332)

Una seconda valutazione è quella che è possibile rintracciare ne *La gaia scienza* (1882), in cui Nietzsche dimostra di apprezzare la scienza non in base ad un criterio di verità, ma poiché essa è capace di liberare l'uomo; egli si domanda infatti non se la scienza sia vera o falsa, ma se sia utile o dannosa per la vita, ricavandone una valutazione positiva. In questo periodo, Nietzsche concentra la sua attenzione su studi di natura scientifica, poiché ciò che più lo affascina della scienza è il fatto che essa indaghi sull'origine delle cose; è per questo che la sua attenzione è rivolta alla chimica e alla paleontologia, finalizzate alla ricerca dell'origine degli elementi costitutivi della realtà. In sostanza, per Nietzsche, queste due scienze hanno un atteggiamento "genealogico", ed egli si propone di operare a sua volta, in ambito filosofico, con questo metodo secondo cui si risale all'origine tramite lo smontaggio, ossia tramite il disvelamento degli originari comportamenti etici e delle tendenze umane generatrici della morale. Se infatti la chimica e la paleontologia studiano la natura, Nietzsche vuole invece proiettare la propria indagine sulla morale, demitizzandola.

L'abbozzo di una visione della realtà

La parte più consistente di una teoria, solo abbozzata, a cui Nietzsche affidava la *pars construens* del suo pensiero è contenuta nel testo postumo *La volontà di potenza* (1906). In essa Nietzsche critica i concetti tradizionali di sostanza, causa, spazio e tempo e, d'accordo con l'assunto di base della sua polemica, li pone sul conto di una commistione tra metafisica e morale.

D'accordo con la scienza del suo tempo, Nietzsche sostiene l'idea di una sostanza che funzioni come una sorta di "base di appoggio", di *substratum*, per gli accidenti. Rifacendosi al pensiero di Rudiger Boscovich (1711-1787) secondo cui quando si parla di sostanza ci si riferisce a dei centri di forza, privi di estensione, su cui la forza di gravità esercita l'attrazione a distanza, Nietzsche ritiene che non esista una sostanza estesa, ma soltanto i centri di forza che vengono, essi soli, percepiti dai nostri organi di senso. Tutto il resto, come la nostra idea delle cose e della loro permanenza nello spazio, è frutto di una costruzione mentale.

> « La “cosa” in cui crediamo è solo *inventata*, un fermento aggiunto a diversi predicati. Se la cosa “agisce”, ciò significa: noi comprendiamo *tutte le altre proprietà* presenti ma momentaneamente latenti come una causa del fatto che ora appaia una singola proprietà; ossia, prendiamo la somma delle sue proprietà – x – come *causa della proprietà x*: il che è completamente stupido e folle! »
>
> (F. Nietzsche, *La volontà di potenza*, Bompiani, Milano, 1992, p. 309)

Nella sua prospettiva la forza va quindi a prendere il posto della sostanza. Ma che cosa sarebbe questa forza? Nella ricostruzione nietzschiana la forza è ciò che rimane dopo che il mondo esterno è stato privato della sostanza, la quale non è più l'oggetto diretto delle nostre percezioni, bensì un'utile ipotesi mentale posta dall'uomo. La forza costituisce l'oggetto proprio delle nostre percezioni: nello specifico gli organi di senso entrano in contatto con forze che non forniscono informazioni *qualitative* sugli oggetti, ma che permettono comunque al cervello di elaborare le inferenze che sono alla base delle nostre conoscenze. Le cose, al di là della loro conformazione visibile, sono la risultanza dei rapporti tra queste forze:

> « La “cosa in sé” è un controsenso. Se immagino di abolire tutte le relazioni, le “proprietà”, le “attività” di una cosa, la cosa non rimane: infatti, la cosalità è una nostra finzione, è aggiunta da noi per bisogni logici, allo scopo di definire, di intenderci. »
>
> (F. Nietzsche, *La volontà di potenza*, Bompiani, Milano, 1992, p. 308)

Ne deriva che l'io è interpretabile come un aggregato di forze che tentano reciprocamente di imporsi; nel linguaggio nietzschiano il soggetto è dunque “volontà di potenza”.

Riguardo al concetto di causalità, Nietzsche nega che in natura esista una qualche forma di connessione causale tra gli eventi. Per Nietzsche, infatti, gli esseri umani non sperimentano mai causalità reali, ma soltanto interazioni tra fenomeni che vengono interpretate come cause ed effetti.

I concetti di “spazio” e di “tempo” sono affrontati in modo analogo. Dopo aver eliminato la sostanza, Nietzsche non ha più la necessità di presupporre uno spazio che contenga la materia. Lo spazio dunque, inteso come un contenitore (finito o infinito) degli oggetti, non esiste all'infuori della nostra attività rappresentativa; esiste invece la rappresentazione che ce ne facciamo. É solo per le necessità della nostra organizzazione della realtà che siamo costretti a introdurre il concetto di divisione spaziale, altrimenti le cose verrebbero percepite come un *continuum* indefinito e indistinto. Ne segue la visione del mondo che Nietzsche riassume a chiusura de *La volontà di potenza*:

> « E sapete cosa è per me “il mondo”? Devo mostrarvelo nel mio specchio? Questo mondo è un mostro di forza, senza principio, senza fine, una quantità di energia fissa e bronzea, che non diventa né più grande né più piccola, che non si consuma, ma solo si trasforma […] non è infinitamente esteso, ma inserito come un'energia determinata in uno spazio determinato, e non in uno spazio che in qualche punto sia “vuoto”, ma che è dappertutto pieno di forze, un gioco di forze, di onde di energia che è insieme uno e molteplice, di forze che qui si accumulano e là diminuiscono, un mare di forze che fluiscono e di agitano in se stesse, in eterna trasformazione, che scorrono in eterno a ritroso, un mondo che ritorna in anni incalcolabili, il perpetuo fluttuare delle sue forze, in evoluzione dalle più semplici alle più complesse […]. Questo mio mondo *dionisiaco* che si crea eternamente, che distrugge eternamente se stesso […] senza scopo […] per questo mondo volete un *nome*? Una *soluzione* per tutti i suoi enigmi? Una *luce* anche per voi, i più nascosti, i più forti, i più impavidi, o uomini della mezzanotte? *Questo mondo è la volontà di potenza – e nient'altro!* E anche voi siete questa volontà di potenza – e nient'altro! »
>
> (F. Nietzsche, *La volontà di potenza*, Bompiani, Milano, 1992, p. 561)

Conclusione

Come epilogo a questo breve lavoro di approfondimento sul tema dell'informazione, riporto di seguito un passo tratto da un libro dell'autorevole fisico italiano Carlo Rovelli, che con grande chiarezza ritengo rappresenti la sintesi del percorso affrontato nelle pagine di questo fascicolo.

« Perché la nozione di informazione svolge un ruolo così centrale? Forse perché non bisogna confondere quello che sappiamo di un sistema con lo stato assoluto del sistema stesso. Più precisamente, perché quello che sappiamo è sempre qualcosa che riguarda la relazione fra noi e il sistema. Ogni sapere è intrinsecamente una relazione; quindi, dipende allo stesso tempo dal suo oggetto e dal suo soggetto. Non esistono stati di un sistema che non siano, esplicitamente o implicitamente, riferiti a un altro sistema fisico. […]

Credo che, per comprendere la realtà, sia necessario tenere presente che ciò cui ci riferiamo, quando parliamo della realtà, è strettamente legato a questa rete di relazioni, di informazione reciproca, che tesse il mondo. In fondo, è di questa che parliamo sempre.

Noi, per esempio, spezziamo la realtà tutto intorno in oggetti. Ma la realtà non è fatta di oggetti. È un flusso continuo e continuamente variabile. In questa variabilità, stabiliamo dei confini che ci permettono di parlare della realtà. Pensate a un'onda del mare. Dove finisce un'onda? Dove inizia un'onda? Chi può dirlo? Eppure le onde sono reali. Pensate alle montagne. Dove inizia una montagna? Dove finisce? Quanto continua sotto terra? Sono domande senza senso, perché un'onda o una montagna non sono oggetti in sé, sono modi che abbiamo di dividere il mondo per poterne parlare più facilmente. I loro confini sono arbitrari, convenzionali, di comodo. Sono modi di organizzare l'informazione di cui disponiamo, o meglio, forme dell'informazione di cui disponiamo.

Ma è lo stesso per ogni oggetto, a pensarci bene, e anche per un sistema vivente. Per questo non ha molto senso chiedersi se l'unghia mezzo tagliata sia ancora me o sia già non-me, se il pelo che il mio gatto sta perdendo sul mio divano sia ancora parte del gatto oppure no, oppure quando precisamente inizi a vivere un bambino. Un bambino inizia a vivere il giorno in cui un uomo e una donna pensano a lui per la prima volta, oppure quando dentro di lui si forma la prima immagine di sé, oppure quando respira per la prima volta, o quando riconosce il suo nome, o quando si applichi qualunque altra convenzione: sono tutte interamente arbitrarie. Sono modi per pensare e per orientarsi nella complessità.

Anche la nozione di "sistema fisico", questa astratta nozione sulla quale vive tanta parte della fisica, ovviamente non è che un'idealizzazione, un modo per organizzare la nostra fluttuante informazione sul reale.

Un sistema vivente è un sistema particolare che si riforma in continuazione simile a se stesso, interagendo senza sosta con il mondo esterno. Di questi sistemi non continuano a sussistere che quelli più efficaci nel farlo, e dunque nei sistemi estinti si manifestano le proprietà che li hanno fatti sussistere, le quali si caratterizzano come quelle che rendono la sussistenza possibile. Per questo i sistemi viventi sono interpretabili, e li interpretiamo, in termini di intenzionalità, di finalità.

La finalità nel mondo biologico – questa è l'enorme scoperta di Darwin – è l'espressione o, che è lo stesso, il nome che diamo al risultato della selezione di forme complesse efficaci nel sussistere. Ma il modo più efficace per sussistere in un ambiente è quello di ben gestire le correlazioni con il mondo esterno e cioè l'informazione su di esso, e di saper raccogliere, immagazzinare, trasmettere ed elaborare informazione. Per questo esistono codici del DNA, sistemi immunitari, organi di senso, sistemi nervosi, cervelli complessi, linguaggi, libri, la biblioteca di Alessandria, computer e Wikipedia: per massimizzare l'efficacia della gestione dell'informazione. Cioè della gestione delle correlazioni.

La statua che Aristotele vede in un blocco di marmo esiste, è reale, ed è qualcosa di più del blocco di marmo, ma non è qualcosa che si esaurisca nella statua stessa: è qualcosa che risiede nell'interazione fra il cervello di Aristotele, o il nostro, e il marmo. È qualcosa che riguarda l'informazione che il marmo ha a proposito di qualcos'altro e che è significativa per Aristotele e per noi. È qualcosa di assai complesso che riguarda un discobolo, Fidia, Aristotele e il marmo, e risiede nella disposizione correlata degli atomi della statua e nelle correlazioni fra questi e mille altri nella testa nostra e di Aristotele. […] Noi siamo strutture che si sono selezionate per gestire al meglio (al meglio al fine di sussistere) esattamente questo: informazione.
[…] Il mondo, forse, non va pensato come un insieme amorfo di atomi, ma come un gioco di specchi basato sulle correlazioni fra le strutture formate dalla combinazione di questi atomi.
Come diceva Democrito: non solo quali atomi ci sono, ma anche in che ordine sono disposti. Gli atomi sono come le lettere di un alfabeto: uno straordinario alfabeto così ricco da riuscire a leggere, riflettere e perfino pensare se stesso. Non siamo atomi: siamo ordini in cui si dispongono gli atomi, capaci di specchiare altri atomi e di specchiare noi stessi.
Democrito dà una strana definizione di "uomo": "L'uomo è ciò che tutti conosciamo". Sembra sciocca e vuota, ed è stata criticata per questo, ma non lo è. Salomon Luria, il massimo studioso di Democrito, osserva che non è una banalità ciò che Democrito sta dicendo. La natura di un uomo non è data dalla sua conformazione fisica interna, ma dalla rete di interazioni personali, familiari e sociali in cui esiste. Sono queste che ci "fanno", queste che ci custodiscono. In quanto "uomini", noi siamo ciò che gli altri conoscono di noi, ciò che noi stessi conosciamo di noi e ciò che gli altri conoscono di noi. Siamo complessi nodi in una ricchissima rete di reciproche informazioni. […] »

(Carlo Rovelli, *La realtà non è come ci appare. La struttura elementare delle cose*,
Raffaello Cortina Editore, Milano, 2014, pp. 220-223)

Bibliografia

Manuali

- Abbagnano Nicola e Fornero Giovanni, *La filosofia,* vol. 3A,Paravia, 2009, pp. 394-414, 421-438.
- Cutnell John e Johnson Kenneth, *Fisica*, vol. 3, Zanichelli, 2009, pp. 834-838.
- Giardina A., Sabbatucci G., Vidotto V., *Profili storici*, vol. 3.2, Editori Laterza, 2007, pp. 490-516.

Libri

- De Rosa Catello, *Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografia*, Maggioli Editore, Milano, 2009, pp. 7-11.
- Dulles Allen, *L'arte del servizio segreto*, Garzanti, Milano, 1963, p. 95.
- Ferraris Maurizio, Storia dell'ontologia, Bompiani, Milano 2008, pp. 361-365.
- Nietzsche Friedrich, *La volontà di potenza*, Bompiani, Milano, 1992, pp. 308, 309, 331-332, 561.
- Rovelli Carlo, *La realtà non è come ci appare. La struttura elementare delle cose*, Raffaello Cortina Editore, Milano, 2014, pp. 207-216, 220-223.

Articoli

- Deutsch David e Ekert Artur, *Oltre il limite quantistico*, in *Le Scienze*, n°531, novembre 2012, pp. 88-93.
- Kuhlmann Meinard, *Che cosa è reale?*, in *Le Scienze*, n°542, ottobre 2013, pp. 42-49.
- Nielsen Michael, *Le regole del mondo quantistico*, in *Le Scienze*, n°412, Dicembre 2002, pp. 70-76.

Web

Da "Wikipedia. L'enciclopedia libera", in http://www.it.wikipedia.org, (in data 10 giugno 2014), le voci:

- Alan Turing; Attacco di Pearl Harbor; Bit; Entropia (Teoria dell'informazione); Computer quantistico; Crittoanalisi; Crittografia; Crittografia nella Seconda Guerra Mondiale; Enigma (crittografia); Friedrich Nietzsche; Informatica quantistica; Qubit; RSA; Storia della crittografia; Teoria dell'informazione; Ultra (crittografia).

Da "La crittografia da Atbash a RSA", in http://www.crittologia.eu/, (in data 10 giugno 2014), le voci:

- Il cifrario RSA; La crittografia della II Guerra Mondiale; La disfatta della macchina Enigma; La macchina Enigma; La macchina Purple.