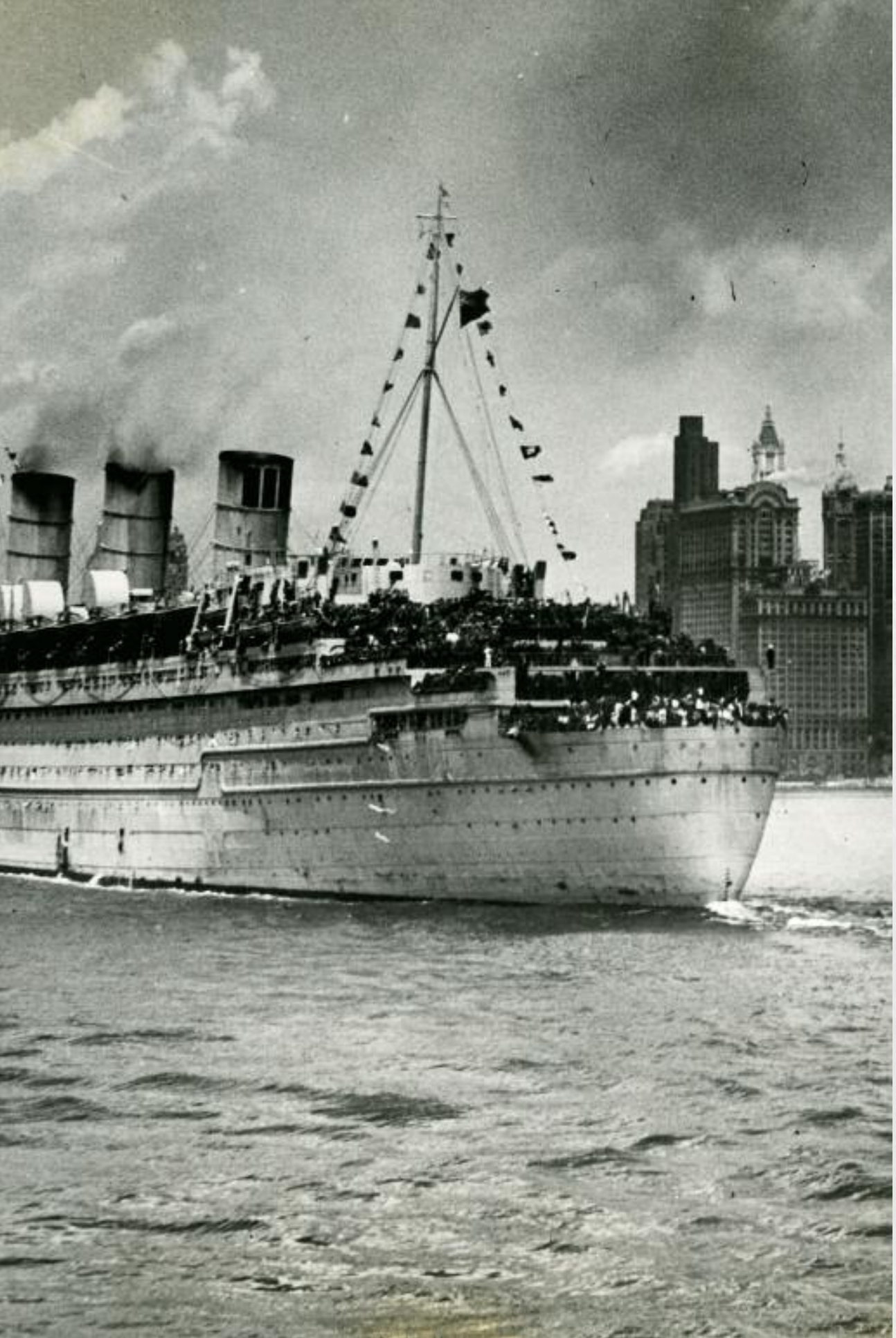

INFORMAZIONE
E INTELLIGENZA 'MECCANICA'
NEGLI SCRITTI DI SHANNON E TURING

Michele Elia

Alan M. Turing e Claude E. Shannon sono quasi coetanei, e fino agli anni Cinquanta hanno avuto vite per molti aspetti parallele. Entrambi hanno ottenuto, in giovane età, risultati sensazionali che hanno cambiato la società e che li hanno resi famosi, peraltro operando in ambienti culturali e scientifici molto diversi: la puritana Inghilterra l'uno, la liberale America l'altro. Entrambi, completata la fase dei grandi contributi scientifici, si sono dedicati ad aspetti difficilmente formalizzabili che concernevano l'intelligenza umana e quella delle macchine, e possono essere considerati come i veri iniziatori dell'Intelligenza Artificiale. È questo contributo, spesso trascurato ma chiaramente riscontrabile nei loro scritti, che s'intende mostrare.

Alla metà del dicembre 1942, il grande matematico inglese Alan Mathison Turing varcò l'Atlantico sulla *Queen Mary*, esponendosi a un grave rischio perché sulle rotte atlantiche gli U-boot attaccavano, con elevata percentuale di successo, tutto il naviglio alleato che riuscivano a intercettare. Vincere la lotta con i sommergibili tedeschi, nota come la «battaglia dell'Atlantico» del Nord, era d'importanza vitale per la Gran Bretagna cui erano indispensabili i rifornimenti di materie prime, armi e prodotti alimentari provenienti dagli Stati Uniti e dal Commonwealth, in una guerra che si prospettava sempre meno breve. E per conseguire il successo, oltre ad adeguati mezzi navali era indispensabile la decrittazione in tempo reale dei messaggi, cifrati con *Enigma*, scambiati tra il comando della Kriegsmarine e le flottiglie di U-boot. Le informazioni così ottenute permettevano di individuare in anticipo e con precisione i tragitti dei battelli nemici e quindi d'interdirne l'attività.
Perché il genio inglese, direttore della stazione Hut 8 a Bletchley Park, e responsabile, per parte britannica, della crittoanalisi dei messaggi cifrati con *Enigma* e *Lorenz* dall'Esercito tedesco[1], si trovava su una nave che avrebbe potuto essere affondata?

1. Baldi – Elia 2015.

Il viaggio aveva molteplici scopi di considerevole importanza politica e strategica. Dopo l'attacco giapponese del 7 dicembre 1942 a Pearl Harbor, gli Stati Uniti erano entrati in guerra a fianco del Regno Unito contro le nazioni dell'Asse, ed era necessario collaborare con i crittografi americani, condividendo con essi anche le informazioni più delicate. A Washington, Turing doveva incontrare William Friedman, organizzatore e responsabile del centro di crittoanalisi dell'Esercito americano. Questi, emigrato dalla Russia zarista, era assurto rapidamente ai più alti ruoli nei Servizi di sicurezza dell'Esercito statunitense per l'eccezionale abilità con cui, tra l'altro, aveva fornito un determinante contribuito alla decrittazione dei codici usati per cifrare i messaggi tra Tokio e l'ambasciata giapponese a Washington. In particolare, queste attività permisero di conoscere le intenzioni nipponiche con molto anticipo rispetto alla dichiarazione di guerra. Turing doveva poi visitare i Bell Labs di Murray Hill, a New York, con l'evidentemente non dichiarato intento di acquisire ogni informazione possibile sullo stato della crittografia americana. Durante la visita ai laboratori, egli prese visione dei progressi fatti da quella ingegneria delle comunicazioni nella trasmissione della voce sul telefono e nella sua cifratura; apprese del sistema *Sigsaly*[2], cui si stava lavorando in gran segreto e che, nelle intenzioni, avrebbe dovuto proteggere in modo affatto sicuro, senza possibilità d'intrusioni e di decrittazioni, le conversazioni telefoniche; acquisì i particolari sulla codifica digitale della voce col *Vocoder*, inventato, dopo un decennio di studi, dall'ingegnere Homer Dudley degli stessi laboratori Bell e brevettato nel 1939. Il Vocoder (contrazione di *Voice* e *Coder*) è stato il precursore degli attuali sistemi digitali della voce, tra cui LPC-10 (Linear predictive coding) usato nella telefonia cellulare. In Sigsaly, la voce digitalizzata e codificata in forma binaria era cifrata, a bit a bit, secondo lo schema di Vernam. Quasi certamente queste informazioni convinsero Turing che Sigsaly non poteva essere violata perché realizzava la cifratura binaria perfetta one-time-tape, pertanto ne approvò l'uso anche da parte inglese. Questo metodo di cifratura era stato inventato nel 1917 da Gilbert Vernam, brevettato nel 1919, e usato in telegrafia dagli anni Venti[3]. E Sigsaly fu effettivamente impiegato dal Presidente Franklin Delano Roosevelt e dal Primo ministro inglese Winston Churchill nei loro colloqui, durante il periodo più critico del conflitto in Europa, per coordinare le azioni militari con gli alleati e condividere le decisioni sulle operazioni belliche, non ultimo lo sbarco in Normandia del 6 giugno 1944.

2. *Ibidem*.
3. *Ibidem*.

Turing si fermò negli Stati Uniti per ben tre mesi e iniziò l'azzardato viaggio di ritorno in patria su un trasporto truppe, unico civile a bordo, il 16 marzo 1943. Non si sa molto di quest'avventura americana di Turing, ma dal fortunoso ritrovamento di alcune sue note si è appreso che era rimasto insoddisfatto dei colloqui con Friedman, forse perché le geniali caratteristiche del crittografo apparivano poco scientifiche a una mente puramente matematica. Durante le visite ai Bell Labs s'incontrò, forse non per caso, con Claude Elwood Shannon, il quale svolgeva un'attività mai rivelata nei particolari per i Servizi americani. I due, quasi coetanei, trovarono di avere molti punti in comune. Entrambi avevano acquisito molto giovani e rapidamente notevole fama, anche se in ambiti molto diversi e con differenti percorsi formativi. Turing è considerato il fondatore della moderna scienza dei calcolatori e Shannon è il creatore della teoria dell'informazione. Gli argomenti dei colloqui sono sconosciuti ma, quasi come un gossip, corre voce che avessero parlato di macchine per giocare a scacchi e di come riconoscere l'intelligenza umana rispetto a quella 'meccanica' di un calcolatore[4].

Che cos'è l'intelligenza? È una domanda che ricorre da tempi immemori e la risposta è ancora sfuggente. Tuttavia, nell'ultimo secolo sono stati fatti notevoli progressi nella conoscenza della mente umana e del suo funzionamento, e su come imitarla con i calcolatori. Quest'ultima attività è diventata una disciplina nota come Intelligenza Artificiale (AI). Alla sua nascita contribuì direttamente Shannon che con John McCarthy curò il volume *Automata Studies*, pubblicato da Princeton University Press nel 1956, nel quale erano raccolti gli atti della Darmouth Conference svoltasi nello stesso anno, alla quale parteciparono eminenti ricercatori, tra cui John von Neumann, Marvin Minsky e Stefen Cole Kleene, considerata l'evento che dette inizio alla AI come disciplina scientifica, anche se la storia delle sue origini è forse più complessa, come si può arguire da alcuni passaggi importanti.

Nel 1937 Turing pubblicò l'articolo *On computable numbers, with an application to the Entscheidungsproblem* sui Proceedings of the London Mathematical Society, in cui tra l'altro rispondeva in senso negativo a un problema posto dal matematico David Hilbert nel 1928. La questione – tecnicamente formulata in termini di logica formale di primo livello, ma con parole meno tecniche – era se esistesse una procedura generale per decidere se una precisa affermazione logica fosse vera o falsa, utilizzando un numero finito di regole e passi. Turing rispondeva alla questione di Hilbert dopo averne risolto una più generale, ossia cosa sia

4. *Ibidem*.

o non sia calcolabile dalla mente umana o da una qualsiasi macchina. Il contenuto dell'articolo è considerato il fondamento teorico dei calcolatori elettronici perché, per sviluppare rigorosamente e in modo indisputabile la sua teoria, Turing introdusse un modello astratto, ma molto semplice, di calcolatore, ora noto come «macchina di Turing». Esso era costituito da una striscia illimitata di carta su cui si potevano scrivere due simboli, 0 e 1, e da un'unità operativa che poteva eseguire poche ben definite operazioni, tra cui muovere in avanti o indietro la striscia di carta, leggervi un simbolo o scriverne sopra uno. Turing sostenne in modo convincente che tutte le elaborazioni, i calcoli numerici o logici, o quant'altro riguardasse l'informazione digitale potessero essere eseguiti da tale apparato. Ossia, qualunque calcolatore può essere descritto per mezzo della «macchina di Turing». È ragguardevole che il riferimento all'informazione discreta, o digitale, ricorra sistematicamente in tutti gli scritti di Turing, anche se egli non s'interessò mai direttamente d'informazione. Tuttavia, è sempre stato sottovalutato che, affinché l'impostazione di Turing portasse a una risposta completa e definitiva su ciò che è calcolabile, come solitamente acclamato, occorreva un concetto sviluppato posteriormente come conseguenza della misura d'informazione introdotta da Shannon. Una delle conclusioni dell'approccio di Shannon, forse quella che più lo rese famoso nell'ingegneria delle comunicazioni, fu una formula che permetteva di calcolare la capacità del canale gaussiano, ossia la massima quantità d'informazione che era possibile trasmettere su un canale disturbato da rumore con statistica gaussiana. Tale risultato comporta che tutta l'informazione scambiata in qualsiasi modo tra esseri umani o comunque utile alla vita, informazione inevitabilmente corrotta da disturbi, è discreta, ossia rappresentabile con un numero finito di simboli.

Questa teoria fu un prodotto delle ricerche sui fondamenti della crittografia e della crittoanalisi condotte dal giovane Shannon nel quinquennio della Seconda guerra mondiale. Per rispondere, in parte, alla domanda metafisica su cosa fosse l'informazione e, in parte, su come recuperare l'informazione dai messaggi cifrati, Shannon, seguendo un'idea del 1928 di Ralph V. Lyon Hartley, utilizzò la probabilità per introdurre una misura dell'informazione in modo assiomatico, e chiamò bit la sua unità di misura, termine non inventato da lui, ma coniato nei laboratori Bell da alcuni colleghi. Il principio seguito da Shannon fu di costruire, su base assiomatica, una teoria matematica delle comunicazioni fondata su un numero finito di postulati ragionevolmente evidenti come quelli della geometria euclidea studiata al liceo. Le ripercussioni sull'evoluzione delle telecomunicazioni hanno determinato, quasi forzato, la telefonia cellulare, internet e i sistemi di memorizzazione digitale di voce e immagini. Tuttavia, i rivoluzionari effetti di questa misura in tutti i settori scientifici – dalla biologia alla fisica, alla meccanica e alla filosofia – sono raramente riconosciuti nella letteratura specializzata. Invece, l'aspetto della teoria dell'informazione universalmente noto agli inizi del terzo millennio è stata la formula «convergenza al digitale», introdotta per indicare il periodo che la comunità scientifica e quella industriale hanno impiegato per far propri i risultati di Shannon sull'informazione, piuttosto che indicare un processo tecnologico che, di fatto, era già completo proprio nei lavori di Shannon degli anni Quaranta. Sembra assai anacronistico parlare ora di convergenza al digitale, se si pensa che l'idea di un calcolatore numerico programmabile comparve con Charles Babbage nell'Ottocento, fu poi seguita dalla teorizzazione di Turing negli anni Trenta, e dotata di concretezza a posteriori dalla teoria di Shannon, sviluppata durante la Seconda guerra mondiale.

Il cammino di Shannon nel decennio terminato con la fine del conflitto ha qualcosa di magico nella formazione dello scienziato. Nel 1936, dopo aver conseguito due Bachelor of Science (Laurea di primo livello) in ingegneria elettrica e in matematica all'Università del Michigan, iniziò gli studi di master (Laurea di secondo livello) per ottenere una laurea in ingegneria elettrica al Massachusetts Institute of Technology (Mit), dove lavorò all'importante progetto di Vannevar Bush di un differential analyzer, un tipo di calcolatore analogico idoneo a determinare le traiettorie dei proiettili di cannone o delle bombe lanciate dagli aerei e, più in generale, a risolvere complessi sistemi di equazioni differenziali in molte variabili. Nel 1937, Shannon firmò la tesi di master al Mit in un campo diverso, proprio delle reti telefoniche, A *symbolic Analysis of relay and switching circuits*, i cui risultati furono pubblicati in un articolo apparso su «A.I.E.E. Transactions» (rivista della società americana degli ingegneri elettrici). La storica tesi – che lo «Scientific American» ha definito «la Magna Charta dell'era dell'informazione» – e il relativo articolo resero famoso il giovane Shannon, i cui risultati molto originali sono considerati uno dei più importanti contributi del secolo alla nascente ingegneria dei network per le comunicazioni e per la progettazione dei circuiti digitali che ormai compaiono ovunque, dai telefoni cellulari all'elettronica di consumer, ai satelliti e ai droni, agli aerei e alle navicelle spaziali. L'esperienza maturata sotto la guida del suo relatore di tesi e mentore, Vannevar Bush, nonché il poderoso lavoro nell'ambito delle comunicazioni elettriche e come crittoanalista per i Servizi segreti americani durante la guerra, assicurò a Shannon una preparazione e conoscenze tali da portarlo allo sviluppo, oggi scontato, della teoria matematica dell'informazione.

Nel 1945, licenziato il suo famoso memorandum A M*athematical Theory of Cryptography*, classificato dal Governo americano e pubblicato in più parti dopo essere stato desecretato, negli anni 1948-1949, Shannon si concentrò su apparenti problemi futili, come la teoria dei giochi, le problematiche dei giocolieri (*juggling*), l'istruzione di un calcolatore per giocare a scacchi, o su come far apprendere a un topo elettromeccanico il percorso di un labirinto senza disporre del filo di Arianna. Tutti questi argomenti hanno come denominatore comune il problema dell'intelligenza, qualità che affascinò Shannon al pari di Turing.

Quest'ultimo, nell'articolo C*omputing machinery and intelligence*, pubblicato sulla rivista «Mind» nel 1950, disquisisce su macchine e pensiero, e introduce il concetto di *imitation game* per discutere su come riconoscere l'intelligenza, o meglio, su come distinguere l'intelligenza umana da quella artificiale, in particolare di un calcolatore digitale. A differenza di Shannon, egli sottovaluta il concetto d'informazione e della sua misurazione, dando per scontato che l'informazione sia discreta e rappresentabile da un numero finito di simboli; per lui sono importanti le trasformazioni dell'informazione digitale. Non va però dimenticato che, se l'informazione continua avesse una valenza effettiva, allora per disquisire di computabilità in assoluto sarebbe necessario prendere in considerazione anche le trasformazioni dell'informazione continua, o analogica, come fecero negli Usa con i calcolatori analogici ai quali il giovane Shannon provvidamente lavorò, pur senza convinzione. Va ripetuto che la sua teoria dell'informazione, sviluppata inizialmente come ancillare alla crittografia, ha motivato in modo definitivo le teorie di Turing. Sono stupefacenti le profezie di Shannon sugli sviluppi dei calcolatori, delle macchine per giocare o per imitare l'uomo. Nella memoria T*he potenzialities of Computers* (aprile 1953), preparata per i colleghi dei laboratori Bell, con lucidità e limpidezza di visione, Shannon tenta una previsione sullo sviluppo e sull'impiego dei calcolatori nei successivi trent'anni. La disamina concerne la relazione tra la velocità di calcolo dei calcolatori, la possibilità di programmarli e la capacità di assumere decisioni che a priori il programmatore non conosce perché dipendono dai risultati dei calcoli. In altri termini, i calcolatori elettronici possono imitare il pensiero umano. Dopo un'analisi di quali sinistri sviluppi potrebbero avverarsi, Shannon conclude – siamo nel 1953 – affermando in modo quasi apodittico che il progresso dei calcolatori, per il bene e per il male, non ha punto di ritorno, con implicazioni filosofiche, etiche, sociali ed economiche inquietanti. Termina chiedendosi se l'uomo sarà capace di rivolgere le sue energie mentali a più alti valori culturali e spirituali.

L'articolo C*omputers and Automata*, apparso nel luglio 1953 su «A.I.E.E. Transactions», è una digressione sul cervello umano e sui calcolatori elettronici in cui è tentato un confronto sotto vari punti di vista, in particolare: complessità, consumo energetico, efficienza, organizzazione strutturale, logica di funzionamento e logica decisionale. La conclusione è che siamo ancora lontani dal costruire macchine che possano competere con la mente umana in quasi tutti gli aspetti, eccezion fatta per i calcoli numerici massivi. Ma la parte più espressiva riguarda la comparazione tra circuiti cerebrali umani e circuiti elettronici nei calcolatori, al cui riguardo è sorprendente questa osservazione: «The brain can operate reliably for decades without really serious malfunctioning (comparable to the meaningless gibberish produced by a computer in trouble conditions) even though the components are probably individually no more reliable than those used in computers» («Il cervello può operare in modo affidabile per decenni senza gravi malfunzionamenti – in confronto alle cose senza senso prodotte da un computer in difficoltà – anche se probabilmente i componenti, a livello individuale, non sono più affidabili di quelli utilizzati nei computer»). In una breve sezione presenta anche un sommario, chiaro nella sinteticità e lucido sull'importanza e sulle conseguenze, del famoso articolo di Turing sull'E*ntscheidungsproblem*.

Le vite di Shannon e Turing sono, per molti aspetti, parallele. Entrambi hanno ottenuto, in giovane età, risultati sensazionali che hanno cambiato la società e che li hanno resi famosi. Ambedue, completata la fase dei grandi contributi matematico-scientifici, si sono dedicati ad aspetti difficilmente formalizzabili che concernevano l'intelligenza umana e quella delle macchine. È innegabile che i due grandi scienziati abbiano operato in ambienti sociali, culturali e scientifici molto diversi: Shannon ha potuto usufruire della forza e liberalità della giovane America, come cantata da Walt Whitman; Turing ha dovuto subire i vincoli di una società vecchia, se non antica, con tutte le limitazioni, anche tragiche, che ne conseguono. Ambedue hanno apprezzato il valore dell'intelligenza e contribuito al sorgere della AI, disciplina che comincia a mostrarsi fruttuosa, anche se non pare possa confondersi con l'intelligenza umana nei suoi aspetti meno tecnici. E neppure con la vita, il cui mistero è tuttora inattaccabile e la cui origine è ancora inesplicabile. Come nel famoso mito della caverna nella R*epubblica* di Platone, noi vediamo le nostre ombre proiettate sulla parete di una caverna (il mondo in cui viviamo) e crediamo che quelle ombre siano la realtà

BIBLIOGRAFIA

M. Baldi – M. Elia, L*a crittografia. Da raffinata arte rinascimentale a moderna scienza*, XXI «Gnosis» (2015) 3, pp. 134-143.
A. Hodges, *Alan Turing: the Enigma*, Burnett Books/Hutchinsons, London 1983.
D.C. Ince (ed.), *Collected Works of* A.M. *Turing. Mechanical Intelligence*, North-Hollande, Amsterdam 1992.
N.J.A. Sloane et al., *Claude Elwood Shannon Collected papers*, Ieee Press, Piscataway 1993.