Leon Battista Alberti (Genova 1404 – Roma 1472) esercitò il proprio genio e rigore scientifico in più campi dello scibile umano. Con Eugenio IV e Niccolò V fu prelato e uomo di Curia Romana. Negli anni tra il 1466 e il 1467 si dedicò alla redazione del trattato "*De Componendis Cyfris*", una breve riflessione circa le modalità attraverso le quali rendere segreta e sicura la corrispondenza degli uomini di Stato.

di Antonio Pizzi

ALLE ORIGINI DELLA CRITTOGRAFIA MODERNA: LEON BATTISTA ALBERTI E IL SUO "*DE CIFRIS*"

Antonio PIZZI lavora all'interno della funzione Affari Legali, Regolamentari e Sicurezza di PosteMobile.

"*Ci sono più cose in cielo e in terra, Orazio, di quante ne possa celare la tua crittografia*"

Così, parafrasando Amleto, potremmo iniziare a percorrere un breve viaggio a ritroso, sino alle origini della moderna crittografia. Il riferimento alla "modernità", che per convenzione e consuetudine rinvia a quel lungo e complesso periodo che va dalla fine del Medioevo sino alla Rivoluzione Francese, serve a definire un preciso perimetro di indagine, entro cui collocare il soggetto e l'oggetto di questa breve riflessione, ovvero Leon Battista Alberti e il suo *De Componendis Cyfris*. **Filosofo, architetto, musicista, pittore e scultore: cinque parole per sintetizzare una personalità poliedrica e vulcanica, un uomo che davvero seppe incarnare lo spirito dell'*homo novus* del Rinascimento italiano**, un paradigma assoluto dello spirito umanistico, assai più di un Brunelleschi, solo per rimanere nel campo architettonico, quello per il quale l'Alberti forse è maggiormente noto.

Infaticabile scrittore di trattati, Leon Battista Alberti (Genova 1404 – Roma 1472) esercitò il proprio genio e rigore scientifico in più e più campi dello scibile umano, interessandosi praticamente a tutte le Arti, spaziando dalla pittura alla scultura, dall'architettura alla letteratura, alla matematica: nulla della cultura e del sapere della sua epoca gli fu estraneo. Né estraneo alla sua personalità fu il tratto umano, tanto che Giorgio Vasari ebbe a definirlo *ammirevole cittadino, uomo di cultura, amico di uomini talentuosi, di mente aperta e gentile con tutti. Visse onorevolmente e da gentiluomo*.
Tuttavia, non si trattò solo di una straordinaria personalità di intellettuale; infatti, il nobiluomo genovese, solo di nascita ma di nobile famiglia fiorentina, fu prelato e uomo di Curia Romana, soprattutto con Eugenio IV e Niccolò V, e vicino a dinastie principesche quali gli Estensi e i Montefeltro, godendo dell'amicizia e della protezione del duca di Urbino Federico III, anche noto come il principe-soldato. Anche le segrete stanze della politica non avevano particolari segreti per lui.

Delineata una siffatta e necessariamente breve biografia ideale, non stupisce che l'interesse dell'Alberti possa essersi indirizzato anche verso la crittografia, una disciplina allora invero assai poco nota, allora come oggi, viene comunque da dire.
Negli anni tra il 1466 e il 1467, si dedicò alla redazione del citato trattatello, definito tale non per la pochezza dell'oggetto, quanto piuttosto per l'esiguità delle pagine, che nella pagina introduttiva ben chiarisce il fine dell'opera, anzi il fine dell'opera in relazione a quello che appare essere il committente: Leonardo Dati, segretario apostolico di Paolo II. In sintesi, il *De Cifris*, come alcuni dei copisti dei 15 manoscritti noti hanno sintetizzato il titolo, altro non è che il frutto della riflessione circa le modalità attraverso le quali rendere segreta e sicura la corrispondenza degli uomini di stato, *qui maximis rebus agendis presunt*, ovvero quanti sono chiamati ad occuparsi di questioni di straordinaria importanza.
Come narra l'Alberti, la suggestione ad indagare gli venne dalle conversazioni intrattenute con il Dati nei giardini vaticani. Il problema prospettato dal nobile segretario fiorentino era così riassumibile: come fosse possibile rendere indecifrabile una comunicazione scritta che malauguratamente dovesse essere intercettata.

Al capitolo terzo, viene fornita una definizione di "cifratura", sulla quale ancora oggi tutti potremmo convenire, ovvero scrivere in modo cifrato significa comporre annotazioni in modo apparentemente arbitrario, ma che acquisiscono reale significato solo tra chi mutualmente abbia definito la reale disposizione delle lettere e delle parole che costituiscono il testo.
Quindi, il trattato prosegue con una vera e propria analisi statistica delle frequenze con le quali le lettere dell'alfabeto latino si ripetono nelle parole: nota che circa ogni otto consonanti si presentano un massimo di sei-sette vocali e la vocale che si presenta con minor frequenza è la lettera O. E ancora, si analizzano tutte le possibili posizioni delle vocali all'interno delle parole, quindi ogni ipotizzabile posizionamento delle consonanti, definendone ogni frequenza teorica.
Dall'analisi lemmatico-strutturale, discende una pressoché logica conseguenza: definire un metodo rigoroso di cifratura attraverso la sostituzione polialfabetica, da realizzarsi attraverso una macchina, il disco cifrante, che troverà applicazioni concrete nei successivi cinque secoli, convenzionalmente e semplicemente fino alla comparsa della **celeberrima Enigma**. Due semplici dischi di rame, di diametro differente, cosicché il maggiore circondi il minore; entrambi fissati su di un perno, affinché entrambi possano

ruotare in modo indipendente. Sui dischi sono incise le lettere dell'alfabeto, in modo tale che ruotando un disco rispetto all'altro si possano far combaciare le lettere sulla base dei criteri di sostituzione precedentemente definiti dal mittente e dal destinatario. **È interessante notare che, nella conclusione, l'Alberti esprime la volontà di tenere segreta la redazione dell'opera**.
La prima edizione a stampa appare solo un secolo dopo, nel 1568 a Venezia, a cura di Cosimo Bartoli, che tra l'altro fu il primo editore e traduttore in lingua italiana del *Corpus* albertiano. Tuttavia ebbe scarsa diffusione e fortuna, fino alla prima metà del Novecento, quando il generale Luigi Sacco, fondatore del primo Ufficio Cifra dell'Esercito Italiano nel 1915 e autore di un fondamentale e ancora celebrato manuale di crittografia, riconobbe all'Alberti di essere stato il progenitore dei metodi polialfabetici e omofonici.

Ad oggi, non è dato ancora sapere se la macchina cifrante sia mai stata realizzata da qualcuno, così come l'Alberti l'aveva progettata, e tuttavia questo non è la questione centrale e appassionante; così come non lo sono le ipotesi avanzate da più studiosi, su tutti David Kahn nella sua fondamentale opera dedicata alla storia della crittografia, circa i progenitori o gli ispiratori della mirabile intuizione albertiana. A riguardo, Kahn ipotizza che il paradigma esemplare da cui prese l'ispirazione siano stati i cerchi concentrici polialfabetici realizzati da Ramon Llull, straordinaria figura di mistico e teologo catalano, vissuto nel XIII secolo; per Lullo, italianizzando dal catalano, i dischi erano funzionali a quella che egli stesso definì *ars magna*, ovvero la trasformazione dei vari concetti filosofici e teologici, in segni geometrici o algebrici, in modo tale che si possano combinare reciprocamente in tutti i modi possibili, allo scopo di ottenere così una specie di mappa o di catasto universale dei concetti. Come si vede, il fine del disco di Lullo è ben diverso, non si tratta di cifrare per ottenere segretezza.

A questo punto, la domanda: perché dopo secoli e secoli, possiamo dire dai tempi dell'Impero Romano, non si è avvertita la necessità di innovare, di migliorare sistemi di cifratura, mentre alla metà del XV secolo tale necessità appare addirittura impellente, tanto da diventare oggetto di invenzione?
Leon Battista Alberti compone il suo trattato negli anni intorno al 1460, come dicevamo sopra, anni che videro succedersi avvenimenti che scossero e squassarono profondamente l'Occidente. Nel 1453, si era consumato l'ultimo atto di quello che era stato il grande Impero Bizantino, l'erede di una tradizione imperiale che da Costantino, dal IV secolo, aveva attraversato, sia pure con alterne fortune, ben undici secoli di storia. Ma, il 29 maggio 1453 il terribile e sanguinoso assedio turco fece crollare le ultime resistenze delle mura, fiaccate dagli incessanti colpi delle artiglierie turche, che da oltre due mesi circondavano la città.
La caduta di Bisanzio non fu priva di conseguenze per il mondo cristiano; ben presto i Turchi dilagarono nei Balcani e in soli tre anni giunsero ad assediare Belgrado. Solo la incredibile determinazione dei Crociati cristiani, per lo più contadini e forse davvero gli ultimi Crociati del Medioevo, radunati per ordine di papa Callisto III da San Giovanni da Capestrano, ebbe ragione delle preponderanti forze turche. Intanto, anche la Guerra dei Cento Anni era giunta al termine, nel 1454: dopo quasi cinque secoli, l'Inghilterra abbandonava definitivamente il suolo continentale e il Regno di Francia poteva consolidarsi.

In Italia, a parte il meridione unitario e governato dalla dinastia aragonese, il quadro politico era fortemente frammentato. Sempre nel 1454, la pace di Lodi stipulata tra i cinque maggiori stati della penisola (Ducato di Milano, Repubblica Veneta, Repubblica di Firenze, Stato della Chiesa, Regno di Napoli), sembrava aver garantito stabilità ad un equilibrio fortemente precario. Tuttavia, le rivalità mai sopite si sarebbero potute riaccendere in qualsiasi momento.
Da ultimo, per tornare al contesto politico più vicino a Leon Battista Alberti, la Chiesa stessa era stata profondamente scossa, sino al 1440, da un turbolento susseguirsi di papi e antipapi, ben tre in un certo momento, e di concili lunghi e sostanzialmente inutili. Solo con il Concilio di Firenze, conclusosi nel 1439, la sede pontificia ritroverà pace e unità al proprio interno.
Come si è visto, sia pure molto sommariamente, la situazione geopolitica del Mediterraneo e del continente europeo alla fine del medioevo è fortemente turbolenta, frammentata. È finito il Sacro Romano Impero, anche se formalmente ancora vive; l'Inghilterra è ormai destinata a un futuro sui mari; i Turchi nei Balcani premono per accedere al cuore dell'Europa. La stabilità assicurata dalla diarchia Impero – Chiesa lungo tutti i secoli del medioevo è ormai alle corde.

In questo scenario, sorge allora la necessità di rendere quanto più possibile sicura e impenetrabile la corrispondenza istituzionale; le alleanze sono mutevoli, il rispetto dei trattati mai certo. Di questa preoccupazione Leonardo Dati parla all'amico fidato, confidando che la sua straordinaria cultura, la sua non comune capacità ideativa possano risolvere il problema. Al di là dell'applicazione tecnica ideata dall' Alberti, il disco meccanico cifrante, non può sfuggire un ulteriore elemento di novità, una novità tutta rinascimentale, per così dire: la "passione" per le macchine.
Parlare di Rinascimento e di macchine, fa venire subito alla mente l'immagine di Leonardo da Vinci, è evidente che non fu il solo; tra l'altro Leonardo conobbe personalmente l'Alberti e ne apprezzò le opere e i trattati. Piuttosto, è corretto sostenere che nel Quattrocento si afferma una categoria, quella degli artisti-ingegneri: non più semplice autore, l'artista-ingegnere non si accontenta di operare con efficacia, ma utilizza gli strumenti dei quali dispone o quelli nuovi che sta faticosamente assimilando (il disegno, la capacità di osservazione, la maestrìa meccanica, la competenza geometrica) per interpretare la Natura, per carpirne i segreti e, imitandone le procedure, per piegarla a vantaggio dell'uomo. Se un nuovo mondo si affacciava all'orizzonte, con nuove sensibilità artistiche, filosofiche, scientifiche, tale novità interessò tutte le discipline umane, non esclusa la crittografia, che trasse nuova linfa vitale proprio dai cambiamenti che sopra, sia pure in modo necessariamente sommario, abbiamo delineato.

Il metodo di Leon Battista Alberti non ebbe, quindi, la fortuna che la sua grandezza e la sua potenza innovativa avrebbero meritato. Come è noto ai crittografi, molta e maggior fortuna ebbe il metodo elaborato nel 1586, che va sotto il nome di Cifrario di Vigenère, che costituì la base per successive elaborazioni; ma è interessante notare che proprio il Sacco, a proposito di tale cifrario e in contrapposizione con il metodo albertiano, usa parole molto critiche: *il desiderio di semplificare per ingraziarsi i cifratori ha determinato un progressivo peggioramento dei tipi proposti, fino al massimo* (degrado) *raggiunto con la cosiddetta tavola di Vigenère*.
Così, il *De Computandis Cyfris* e il suo autore possono stagliarsi in tutta la loro grandezza, una grandezza riconosciuta, sia pure in ritardo, ma che ormai è consegnata per sempre non solo alla più definita e perimetrata storia della crittografia, ma alla Storia *tout court*. ©