

Editoriale

Il futuro del lavoro nella nuova società digitale

Un recente saggio di Bryniolfsson e McAfee *The second machine age* ha aperto un grande dibattito a livello mondiale sulla rivoluzione digitale. C'è un punto importante del lavoro di Bryniolfsson e McAfee quando si afferma che mentre la prima età delle macchine ha portato alla sostituzione del lavoro manuale con robot, la seconda età porta alla sostituzione del lavoro intellettuale, dei knowledge workers con nuove forme di robotizzazione.

E questo preoccupa, in particolare perché non si tratta solo di robot al posto di persone, ma di cambiamenti disruptive in tante attività, pensiamo a quanto Amazon sta trasformando il retail con l'offerta online (in Usa si calcola che si potrà ridurre l'occupazione del settore della distribuzione di oltre un milione di posti di lavoro, senza ancora valutare il possibile impatto di Alibaba ed altri nuovi operatori on line).

Gli stessi autori hanno coinvolto eminenti studiosi ed imprenditori americani per sottoscrivere una Lettera aperta sull'economia digitale in cui al di là degli entusiasmi per il grande cambiamento che il digitale sta portando evidenziano alcune delle sfide impegnative che occorre affrontare con riguardo all'impatto sul lavoro e sui modelli organizzativi delle imprese e delle istituzioni, e concludono che *"La creazione di una società basata sulla prosperità condivisa sarà solamente possibile se aggiorneremo leggi, organizzazioni e ricerca per cogliere le opportunità e superare le sfide che la rivoluzione digitale sta ponendo"*. La conclusione del libro



citato è positiva quando afferma che la tecnologia non è il nostro destino. Siamo noi a dare forma al nostro destino.

Ma è sempre più evidente e fonte di preoccupazione il tumultuoso sviluppo dei processi di digitalizzazione, automazione e robotizzazione di tutte le attività. Non vi è dubbio che tali processi portano e porteranno sempre più alla sostituzione di attività lavorative con macchine e robot non solo in attività manuali ripetitive, ma in misura crescente in attività della conoscenza e nei processi decisionali, si pensi solo allo sviluppo di reti di macchine che comunicano con macchine *nell'Internet of things* che diviene ormai *Internet of everything*, costruendo immensi giacimenti di dati e meccanismi di autodecisione human free.

Non vi è dubbio che si crea la necessità di formare nuove conoscenze, nuove competenze e professioni, grazie alle nuove opportunità offerte dalle nuove applicazioni del digitale.

Vi è già ora un gap tra domanda e offerta di lavoro nelle attività trasformate dalla tecnologia e soprattutto nelle nuove attività che stanno sviluppandosi. Uno studio di McKinsey prevede che negli Stati Uniti al 2018 vi sarà un gap tra il 50 ed il 60% tra domanda ed offerta di competenze di superanalisti e sviluppatori di software avanzato. Vi è oggi in USA uno shortage di competenze necessarie per la gestione dei Big Data da parte di industrie come l'aerospazio, le assicurazioni, la farmaceutica e la finanza. Vi è crescente richiesta di una figura complessa definita come il Data Scientist che non viene ancora formata in ambito universitario.

La sfida che abbiamo davanti è gestire questo processo in modo consapevole senza incertezze, gestire la transizione delle attività lavorative verso nuovi contenuti e soprattutto formare e sviluppare le competenze di ciascuna persona in modo permanente senza interruzioni.

Avendo chiaro che non si tratta di un processo di cambiamento transitorio, ma di una mutazione continua senza soste trainata da onde di progresso tecnologico che non si fermano ma si autodeterminano non in forme incrementali lineari ma in forme esponenziali interdisciplinari ed intertecnologiche.

Lo sviluppo delle tecnologie digitali porta radicali trasformazioni ed interdipendenze con l'evoluzione delle biotecnologie e delle tecnologie della vita e della medicina, con le innovazioni in campo energetico, nello sviluppo delle nanotecnologie e dei materiali, nel progresso aerospaziale, ed oltre.

Mai come ora la ricerca scientifica e l'innovazione tecnologica si integrano producendo straordinari effetti di mutazione nelle attività, nel lavoro e nella vita di tutti.

Si tratta di effetti spesso imprevedibili che portano a nuove condizioni che devono divenire *schumpeterianamente*, "distruzione creatrice" e non solo distruzione di attività e di opportunità lavorative.

La velocità di innovazione delle tecnologie digitali porta ad accelerare tutte le altre innovazioni tecnologiche attuando processi innovativi non più lineari, ma

esponenziali, sul modello della *Legge di Moore*, che da decenni conferma il raddoppio ogni anno e mezzo della potenza dei microchips.

Una velocità che si scontra con la difficoltà e la lentezza di adeguamento culturale e organizzativo, determinando ritardi e problemi di transizione nella creazione di nuova occupazione.

Nella storia dell'uomo ed in particolare nella storia degli ultimi due secoli di industrializzazione, l'innovazione tecnologica ha sempre portato straordinari effetti di crescita economica e sociale, assieme a fasi transitorie di crisi occupazionali dovute alla lentezza di adattamento al cambiamento da parte delle organizzazioni e delle persone.

Così rischia di essere ora in modo ancora più accentuato a causa delle caratteristiche trasversali e particolarmente rivoluzionarie del digitale e delle tecnologie ad esso connesse.

Occorre guidare questi processi e non essere guidati, gestire le fasi spesso critiche della transizione attraverso processi riorganizzativi continui e cercare di anticipare l'adeguamento delle attività lavorative alle nuove condizioni determinate dalle innovazioni tecnologiche.

Troppo spesso le imprese e le organizzazioni preferiscono aspettare che la tempesta tecnologica passi, con posizioni inerziali e di business as usual, con risultati quasi sempre molto gravi.

Così la scuola e le università tendono a ritardare cambiamenti negli schemi formativi con effetti altrettanto drammatici sulle prospettive occupazionali dei giovani.

Una attenzione particolare è oggi rivolta a quanto l'innovazione delle tecnologie digitali stia modificando profondamente l'organizzazione, i modelli di business e di gestione della produzione manifatturiera.

Sta iniziando un percorso che intreccia sempre più strettamente i bit e gli atomi e le tecnologie di digital fabrication, additive manufacturing, fast prototyping, Internet of things, cambiando profondamente il volto della "fabbrica" tradizionale.

Nuovi soggetti quali i Fablab, la stampa 3D e i centri di digital prototyping entrano nell'ecosistema della produzione.

Questo cambiamento per costruire la "*fabbrica digitale smart*" o come viene sempre più chiamata *Industria 4.0*, è una sfida di rilevanza fondamentale per le imprese manifatturiere dell'Italia, secondo paese manifatturiero d'Europa dopo la Germania, ma primo in numerosi comparti anche a livello mondiale e grande esportatore di prodotti di qualità.

In AICA è stato avviato con successo un *Osservatorio sulla Fabbrica digitale* mettendo assieme il mondo innovatore dal basso come i Fab Lab o Hub innovativi e startup con artigiani e piccole imprese per dialogare e capire assieme come affrontare le nuove tecnologie, ad esempio l'additive manufacturing, l'Internet of Things, i flussi informativi della value chain. Questa sfida trova davanti a sé alcuni ostacoli.

Ci sono ostacoli legati al sistema economico, per cui le PMI hanno in media una bassa capitalizzazione, si muovono in un contesto di difficoltà burocratiche che frena gli investimenti innovativi.

Ciò che però, in realtà, frena maggiormente la crescita è la carenza di risorse umane qualificate, in particolare di figure dotate di competenze digitali professionali in grado di affrontare il complesso mix di progettazione, programmazione, gestione dei materiali, dei nuovi processi produttivi e di supply chain.

Allo stesso tempo, manca in troppe imprese una capacità di e-leadership, che consenta di comprendere e guidare verso il futuro.

Lo sviluppo di nuove competenze in grado di affrontare la rivoluzione digitale che sta modificando economia e società, scuola, lavoro, imprese e istituzioni, comportamenti sociali non è una opzione che si può o non si può accettare.

E' una strada che deve essere percorsa non rinviando il problema, ma muovendosi come sistema perché l'integrazione delle reti in tutte le attività richiede di operare come sistema.

Se solo alcune parti si convertono si creano inefficienze e sconnessioni.

Il tema delle competenze è divenuto ormai un tema centrale per le imprese italiane : è urgente investire per preparare competenze adeguate da inserire al più presto nel sistema manifatturiero italiano, operando trasformazioni nelle scuole di formazione tecnica, ma anche nei licei con l'effettiva attuazione pratica, non solo annunciata, dell'alternanza scuola-lavoro, così come nel sostegno alla formazione nelle imprese e per chi viene fatto uscire dal lavoro.

Quando parliamo del passaggio dalla società della conoscenza alla società delle competenze non dobbiamo dimenticare che siamo ancora se va bene alla società delle informazioni, non della conoscenza, perché il passaggio dall'informazione alla conoscenza richiede la consapevolezza critica e la gestione dell'informazione finalizzata ad un obiettivo chiaro.

La scuola è la fabbrica di base di questo processo per preparare fin dai primi anni a questa crescita dalla conoscenza alle competenze.

E' una grande sfida che va affrontata unendo le forze, ma soprattutto ponendo al centro dell'azione politica il ruolo strategico dei formatori e la struttura stessa dell'organizzazione scolastica.

Vi sono oggi straordinarie potenzialità formative nelle nuove tecnologie digitali ed elettroniche che consentono di affiancare sviluppo della mente e manualità (oggi in gran parte persa), permettendo la nascita di laboratori didattici a basso costo in tutte le scuole per la costruzione di artefatti fisici (microrobot, sensori, applicazioni su Arduino, stampa 3D) e artefatti virtuali su web da affiancare allo studio del pensiero computazionale ed alla esplicitazione di potenzialità creative da parte dei ragazzi. Ed anche all'educazione all'autoimprenditorialità.

AICA ha avviato da tempo un forte impegno nella individuazione dei profili di competenze per il nuovo scenario digitale, tra cui sono elementi centrali Cloud, BIG Data e Analytics assieme al fondamentale tema della IT Security;

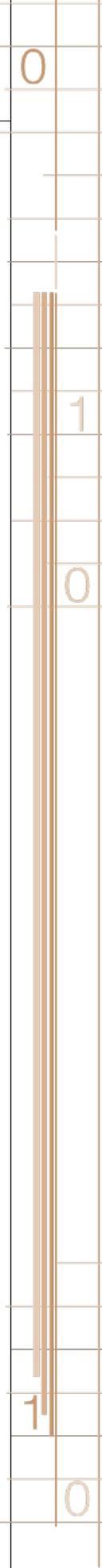
Questo attraverso l'esperienza ormai decennale delle certificazioni professionali, ora basate sull'e-CF (European Competence Framework) dell'Unione Europea che definisce i profili professionali dei professionisti informatici, ma promuove la sua estensione a tutti i livelli manageriali delle imprese e delle istituzioni pubbliche promuovendo l'integrazione delle tecnologie digitali nell'innovazione organizzativa (e-skills e e-leadership).

La sfida della diffusione trasversale delle tecnologie digitali è fondamentale e possibile per il nostro paese che possiede passione creativa, voglia imprenditoriale, il saper fare bene tipico dell'artigiano smart, a cui si unisce la grande esplosione di innovazione che nasce dal basso, le startup, i Fab Lab, gli Hub innovativi, gli acceleratori d'impresa con la scuola (i laboratori, i programmi di alternanza scuola-lavoro, gli ITS) ed il mondo delle piccole e medie imprese e dell'artigianato.

Occorre creare le condizioni per sviluppare ecosistemi innovativi, tanti Hub per accelerare il cambiamento di imprese e istituzioni guidato dalla rivoluzione digitale.

AICA che è stata anche promossa Associazione Digital Champion intende muoversi sempre più in questa direzione, collaborando con tutte le istituzioni interessate.

Bruno Lamborghini
Presidente AICA



Rete Oscura, Rete Profonda, Reti Comunitarie.

Risposte tattiche ai fenomeni di centralizzazione e censura

Carlo Milani, Savino Sasso

Sommario

Deep Web e Dark Net sono termini troppo spesso abusati nella vulgata giornalistica. L'obiettivo primario di questo articolo è fare un po' di chiarezza terminologica e dunque fornire un prontuario minimo per orientarsi nell'oceano della Rete delle Reti, e nelle alternative possibili al modello dominante nella Internet attuale. In secondo luogo, attraverso una rapida ricognizione di quattro progetti di Wireless Community Network, vogliamo mappare in maniera qualitativa un fenomeno in continua crescita e offrire qualche spunto di riflessione concreta per immaginare Reti gestite in maniera condivisa dai loro utenti.

Abstract

Deep Web and Dark Net are terms too often abused in the journalistic clichés. The primary goal of this article is to do some clarity of terminology and therefore provide a minimum handbook to orientate in the ocean of the Network of Networks, and in the alternatives to the current model of the Internet. Second, through a quick survey of four Wireless Community Network, we want to map out with a qualitative approach a growing phenomenon and offer some food for thought to imagine Networks managed in a shared way.

Keywords: Deep Web, Dark Net, Wireless Community Network, Internet Critics, Media Studies



1. Introduzione

In inglese tutto sembra più interessante: Deep Web, Dark Net (Web), (Wireless) Community Network sono termini che circolano con frequenza crescente su Internet; sono oggetto di grande curiosità e di ancor più grandi fraintendimenti. Abbiamo scelto di parlarne in italiano perché siamo consapevoli dell'effetto straniante delle traduzioni, soprattutto in ambito digitale. Riteniamo che per sviluppare uno sguardo critico sia innanzitutto necessario fare un passo indietro rispetto al linguaggio che utilizziamo e considerare le parole non ovvie, bensì cariche di sottintesi. Tale osservazione ci consente di fare un passo in avanti nella comprensione dei meccanismi di articolazione dei significati. L'obiettivo primario di questo articolo è fare un po' di chiarezza terminologica e dunque fornire un prontuario minimo per orientarsi nell'oceano della Rete delle Reti. In secondo luogo, attraverso una rapida ricognizione di quattro progetti di Rete Comunitaria, vogliamo mappare in maniera qualitativa un fenomeno in continua crescita.

Le tre tipologie di Reti elencate si riferiscono a fenomeni affatto eterogenei. Il motivo della crescita spettacolare ed ininterrotta di Internet è già di per sé difficile da descrivere in maniera comprensibile, tanto più se si desidera evitare i tecnicismi specializzati e le semplificazioni da prima pagina. Ancor più complesso risulta quindi discettare di porzioni oscure, profonde o comunitarie di reti variamente connesse (o sconnesse) dalla stessa Internet. Tuttavia, al di là delle difficoltà inerenti alla descrizione di un mondo in perenne divenire, la ragione profonda è che i numeri, spesso utilizzati per trasmettere una parvenza di scientificità, dicono poco dei processi relazionali costitutivi delle dinamiche reticolari. Inoltre vengono spesso usati per fini ideologici non scientifici, ovvero i dati vengono usati come mero strumento di giustificazione di un pensiero ideologico precostituito, spacciato per verità inattaccabile in quanto relativa alla presentazione anodina di numeri.

2. Fare chiarezza

Per districare la matassa, iniziamo da una delle peggiori mistificazioni reperibili su qualsiasi motore di ricerca. Il reportage australiano "Dark Web" di 60 Minutes [1] dichiara di portare lo spettatore in un mondo che nemmeno pensava potesse esistere, chiamato Dark Web, che costituisce "il novanta per cento di Internet". In questo luogo "facile da trovare" sono accessibili "droghe, armi" ed è possibile "persino ordinare un omicidio". In questo luogo impossibile da tracciare gli adolescenti australiani comprano sostanze illecite.

Il riferimento esplicito è a Silk Road, piattaforma di compravendita (in Bitcoin) di beni illegali accessibile tramite Tor (The Onion Router) [2] chiusa nel 2014. Ammettiamo che tale piattaforma facesse parte della Rete Oscura. Ammesso e non concesso che un comune adolescente sia in grado di procurarsi e utilizzare correttamente un browser Tor e un account in Bitcoin (il che implica come minimo che sappia maneggiare chiavi crittografiche in GPG), ebbene, questa Rete Oscura è a sua volta una frazione infinitesima della Rete Profonda, ovvero di quel 90 per cento delle pagine web che non sono indicizzate dai motori di ricerca.

Non c'è nulla di spaventoso in questa mancata indicizzazione. Ogni servizio esposto sul Web che richiede login e password è tendenzialmente parte della Rete Profonda, come accade per conti correnti di vario tipo a cui accediamo quotidianamente, a meno che l'utente del servizio non decida di renderlo pubblicamente disponibile, come accade con le pagine di Facebook accessibili a chiunque. Ogni servizio interno a un'azienda o a un'istituzione accessibile tramite un browser solo dall'interno della rete (Intranet) è altrettanto parte della Rete Profonda. Ogni blogger, ogni Youtuber usa la Rete Profonda: ciò che vede nel suo account non è indicizzato nei motori di ricerca. Persino i servizi che non richiedono procedure di login ma solamente interazioni di ricerca con una base di dati sono parte della Rete Profonda: è il caso banale degli orari dei treni, degli aerei, o ancora delle prenotazioni di stanze d'albergo e molti altri servizi.

2.1 Definizioni

Definiamo **Rete (Web) in chiaro** l'insieme di tutti quei documenti a cui ci si riferisce tramite un link ipertestuale, condivisi tramite Internet e indicizzato dai motori di ricerca pubblicamente accessibili. Internet è l'insieme di interconnessioni globali attive sopra il protocollo IP, una Rete di Reti molto più vasta del solo Web, che è invece distinguibile grazie alla presenza del prefisso di protocollo HTTP/HTTPS (Hyper Text Transfer Protocol / Secure). Tutto ciò che non ha questo prefisso non è parte del Web (es.: FTP, File Transfert Protocol), anche se può essere reso accessibile a normali browser: basti pensare alle caselle di posta elettronica, che usano protocolli non web (SMTP, POP, IMAP) ma possono essere utilizzate attraverso interfacce web.

Definiamo **Rete Profonda (Deep Web)** quella porzione di Internet accessibile tramite Web browser standard ma non indicizzata dai motori di ricerca pubblicamente accessibili. Ecco che i numeri di cui sopra acquisiscono un senso ben diverso: siamo noi utenti comuni di Internet a contribuire massivamente a questa tipologia di Rete. Essa è appropriatamente definita Profonda perché inaccessibile a ogni utente sprovvisto delle specifiche credenziali d'accesso. C'è però un'altra tipologia di soggetti che possono accedere oltre a chi detiene le credenziali d'accesso: coloro che forniscono il servizio. Sembra talmente banale che vale la pena ripeterlo: ogni volta che inseriamo delle credenziali di accesso (login e password) stiamo entrando in casa d'altri (Facebook, Gmail, Twitter, Amazon, ecc.), dove vigono regole scritte ben chiare (benché in continuo aggiornamento), a cui abbiamo aderito la prima volta che ci siamo registrati. Sono i *Termini del Servizio* (TOS, *Terms of Service*). La Rete Profonda non è affatto inaccessibile a chi offre il servizio, anzi, è proprio l'attenta profilazione di quei dati che consente la formulazione di servizi sempre più personalizzati. L'evoluzione si effettua in base al nostro storico di navigazione e interazione con la piattaforma, e al confronto con il comportamento degli altri utenti di quello e di altri servizi.

Definiamo **Rete Oscura (Dark Net)** quella piccola parte della Rete Profonda intenzionalmente nascosta, anonimizzata, decentralizzata [3]. Dal punto di vista tecnico, una Dark Net è un tipo di **Rete Privata Virtuale (VPN)** che presenta misure ulteriori per oscurare gli indirizzi IP dei nodi della rete. In una rete di questo

tipo è difficile non solo risalire all'identità dell'emittente, ma persino sapere se un flusso di informazione su un determinato protocollo è attualmente attivo.

Definiamo invece **Rete Web Oscura (Dark Web)** quella piccola parte della Rete Oscura accessibile tramite strumenti specifici. L'esempio più noto è quello delle Reti web Tor, accessibili tramite un browser Tor, ma ne esistono molte altre, costruite su altri sistemi di anonimizzazione del traffico e degli utenti. Chiunque può visitare un sito nella Web Oscura, a patto che abbia le competenze tecniche necessarie; ciò che può essere davvero difficile da svelare è invece dove si trovi quel sito e da chi sia mantenuto. Il Dark Web è quindi un sottoinsieme delle Reti Oscure.

Definiamo **Rete Comunitaria (CN - Community Network)** una rete di servizi e infrastrutture costruita dagli utenti della rete stessa, cioè da una comunità. La particolarità di queste reti è che invece che dalla logica del profitto (come succede per i normali Internet Service Provider) esse sono guidate dalle necessità dei loro membri.

Definiamo, infine, **Rete Comunitaria Senza Fili (WCN - Wireless Community Network)** una rete comunitaria costruita utilizzando prevalentemente tecnologie di comunicazione radio. In questo caso, invece che creare mondi nascosti all'interno dell'infrastruttura esistente, si tenta di ricostruirla dalle fondamenta, cercando di risolvere alla radice i difetti di progettazione che rendono tanto facili, allo stato attuale, la censura e il controllo.

3. Due opzioni per "aggiustare Internet": una prospettiva storica

L'associazione indebita fra *anonimo* e *illecito* è il punto cruciale per chiarire gran parte delle incomprensioni in campo. Il messaggio ideologico insito nelle comunicazioni propagandistiche che associano l'anonimato all'illecito consiste nel dimenticare volutamente che le Reti Oscure consentono anche la diffusione di comunicazioni in maniera anonima, cioè protetta contro la sorveglianza e la censura [4]. Curioso che non esista un equivalente italiano del termine *whistleblower*, che ha il significato positivo di colui che soffiava il fischietto come un arbitro per attirare l'attenzione del pubblico nei confronti di un fallo, ovvero di una malefatta (all'interno di un'azienda, di un'istituzione e così via), e ha bisogno di essere protetto contro eventuali ritorsioni [5].

Da una prospettiva storica, la rete Internet è la versione civile del progetto di difesa militare statunitense *ARPANET* (1969-1983), la prima rete a commutazione di pacchetto mai realizzata. Una topologia di rete decentralizzata è la caratteristica chiave dal punto di vista difensivo. Questa decentralizzazione è stata interpretata come vocazione all'autonomia da parte di porzioni di reti collegate fra loro fin dai primordi della cultura hacker, negli anni Sessanta [6]. Ma i servizi Web di massa hanno creato immensi serbatoi di dati sensibili, che fanno gola non solo a truffatori e malintenzionati, ma anche a Stati più o meno oppressivi, con le loro Agenzie di Sicurezza più o meno controllate [7]. Sebbene le specifiche tecniche di Internet permettano la decentralizzazione dei servizi e l'implementazione di tecniche utili a mantenere l'anonimato, ovvero ad evitare la

sorveglianza e la censura, gli attori politici ed economici di primo piano si sono da sempre impegnati a trasformarla in un media più facilmente controllabile e censurabile. Lo dimostrano ampiamente gli scandali relativi alla sorveglianza sempre più diffusa ad ogni livello della vita quotidiana, e al ruolo esercitato da agenzie di sicurezza più o meno segrete [8].

In maniera non dissimile dal mercato dei media di massa tradizionali, come la radio e la TV, nel complesso si evidenziano due tendenze: da una parte, massimizzare il numero di spettatori-consumatori-fruitori-utenti (diffusione di dispositivi di connessione a basso costo); dall'altra, mantenere basso il numero di sorgenti da controllare. Si pensi alle tipologie di offerte commerciali disponibili sul mercato civile: le connessioni sono perlopiù asimmetriche. Le utenze domestiche sono generalmente abbastanza veloci nella fruizione di contenuti (accesso a poche sorgenti), ma sono relativamente scarse come emittenti (basse velocità di caricamento-upload). Strutturare una radio via web, per non dire una TV, è praticamente impossibile senza ricorrere a servizi commerciali. D'altra parte, aprire un canale su YouTube non costa nulla, se si passa sotto silenzio la totale delega dei dati (anche di chi accede ai contenuti offerti) a un servizio commerciale formalmente gratuito. L'esaltazione del contributo dei cittadini alla Rete si scontra con la realtà materiale di una Rete pensata per rendere difficile l'allestimento di servizi autogestiti [9].

Se consideriamo la Rete alla stregua di un organismo vivente, possiamo identificare fra le tipologie di Rete di cui sopra alcuni degli anticorpi secreti proprio dalle culture hacker in risposta alle spinte alla centralizzazione e alla sorveglianza, considerate forme degenerative di reticolarità. In questo senso le Reti Oscure e le Reti Comunitarie sono tentativi di "aggiustare la Rete" [26]. Le prime si appoggiano all'infrastruttura esistente, mentre le seconde mirano a ricostruirla in maniera differente.

Infatti le Reti Oscure mirano a costruire reti alternative capaci di vivere nascoste sopra l'infrastruttura di rete esistente, offrendo sia anonimato che accesso a informazioni non disponibili sui canali ufficiali. Le WCN invece mirano alla costruzione di porzioni di Rete autogovernate, eventualmente connesse a Internet, preferendo tecnologie capaci di rendere queste reti resilienti. L'obiettivo è sia di resistere alla censura (es. oscuramento di siti), sia alla distruzione materiale di porzioni dell'infrastruttura di rete. Questo è possibile grazie all'adozione di algoritmi di instradamento delle comunicazioni capaci di adattarsi automaticamente alle modifiche subite dalla topologia di rete.

3.1 Scegliere un metodo, decidere sui dati

Gli autori hanno individuato una decina di esperienze di Reti Senza Fili Comunitarie in Italia. Migliaia nel mondo intero. Alcune si sono estinte da tempo, per le ragioni più varie; d'altra parte ne nascono in continuazione. I dati disponibili sono molti, spesso estremamente dettagliati a proposito dei particolari tecnici (protocolli utilizzati), infrastrutturali (tipologia di apparecchi, monitoraggio dei flussi di dati) e procedurali (installazione di un nuovo nodo, implementazione di un nuovo servizio). Tuttavia, dal momento che le basi dati comunitarie sono spesso compilate a mano in maniera volontaria, sono piene di

errori e non aggiornate. Sono inoltre eterogenee per tipologia di dati raccolti, modalità di raccolta e continuità.

L'automazione della raccolta dati e del monitoraggio (sia dello stato dei nodi che dei flussi di informazione) potrebbe senz'altro aiutare le comunità ad avere una visione più precisa della loro Rete, ad intervenire sui problemi in maniera più tempestiva e anche migliorare le procedure di installazione [10]. Certo, questo potrebbe comportare un avvicinamento sensibile al modello Internet in cui il monitoraggio è delegato a fondazioni e istituzioni, ma soprattutto effettuato da agenzie, governative e non, per scopi di sorveglianza.

3.2 Questionari qualitativi per quattro WCN

Con l'idea di offrire uno spaccato del vibrante e contraddittorio mondo delle WCN comprensibile ad un pubblico non specializzato, ci è sembrato subito evidente che un quantitativo maggiore di dati riguardo alle specificità tecniche di ciascuna, alla tipologia di utenti e all'utilizzo di infrastrutture e servizi, non avrebbe reso i contorni dell'oggetto di studio più distinti. Al contrario, la disomogeneità dei dati era un dato in sé. Inizialmente avevamo immaginato di osservare dall'esterno le diverse WCN, in maniera il più possibile oggettiva e distaccata; ma un lavoro simile rischiava di perdere di vista il pubblico non specializzato, e d'altra parte anche il concetto di "campione rappresentativo", al netto delle disquisizioni statistiche, sfumava in una sequela di grafici e nella scelta dei parametri rilevanti per l'analisi.

La ricerca condotta da Avons, Braem e Blondia in "A Questionnaire based Examination of Community Networks" [11] ci ha convinto della necessità di un'interazione diretta con le comunità, per evidenziare l'importanza fondamentale dell'aspetto relazionale. Il metodo del questionario sottoposto direttamente agli utenti delle WCN era senz'altro interessante, anche perché rendeva evidente il fatto che erano le comunità stesse a rendere disponibili la gran parte dei dati utili per descriverle. D'altra parte, discutendo con persone coinvolte nella costruzione e gestione di WCN, ci sembrava che si potesse dimostrare tutto e il contrario di tutto: che le WCN rappresentavano il futuro, anzi il presente della Rete; viceversa, si poteva ragionevolmente dimostrare che erano assolutamente irrilevanti nell'economia globale delle Reti; si poteva mostrare che erano sostanzialmente prive di intenti ideologici, o al contrario che erano frutto di precise convinzioni politiche e sociali da parte dei membri. Appurato che il punto di vista dell'interlocutore e l'elemento relazionale giocavano un ruolo centrale, abbiamo deciso di farne il criterio di scelta delle WCN. Anche noi diventavamo attori coinvolti.

Abbiamo quindi riformulato un questionario semplificato molto leggero dal punto di vista tecnico (4 domande aperte su dati anagrafici, tecnici, socio-politici e desiderata dei progetti rispetto alle 35 domande suddivise in sei sezioni di [11]) e lo abbiamo sottoposto ai membri di WCN che conoscevamo personalmente, spiegando l'intento divulgativo dell'articolo. Nella richiesta abbiamo specificato che erano bene accette sia risposte collettive che individuali. Le comunità hanno fatto circolare al loro interno i questionari. Nel prosieguo presentiamo i risultati ottenuti in maniera discorsiva, facendo parlare fra loro questionari che

riguardano quattro WCN eterogenee, anche solo per grandezza: Guifi.net in Spagna (decine di migliaia di nodi, 2 questionari compilati) [12]; Tetaneutral.net in Francia (un migliaio di nodi, 1 questionario compilato) [13]; Ninux.org in Italia (centinaia di nodi, 5 questionari compilati) [14]; EigenNet a Pisa (decine di nodi, 1 questionario compilato) [15]. I virgolettati sono tratti dai questionari. L'attenzione si sposta sulle dinamiche della WCN invece che sui numeri che dovrebbero descriverla.

4. Due casi italiani: Ninux.org e EigenNet

Ninux.org nasce a Roma nel 2001 sulla scia di altri progetti internazionali come "Seattle wireless" [16]. Alle prime "isolette" romane se ne aggiunsero altre, e nuove isole continuano a unirsi al progetto in tutta Italia. Si configura quindi come federazione di isole (aggregati di nodi su base locale) in via di collegamento fra loro, priva di statuto collettivo e persino di una forma legale associativa. L'isola romana presenta nodi più fitti e connessi rispetto alle isole più recenti, ad esempio quella fiorentina (una ventina di nodi) e quella bolognese (alcuni nodi solo in parte connessi fra loro). Non solo l'infrastruttura hardware è più solida, ma anche a livello software i servizi offerti sono più stabili man mano che si procede verso Roma (con eccezioni notevoli). Alla base del progetto non vi è un'ideologia né un'affiliazione politica esplicita. Tuttavia, i termini tecnici ricorrenti nelle risposte che abbiamo raccolto, di uso corrente anche nella stampa generalista, sono investiti di forte valenza politica: è il caso di concetti come p2p, privacy, copyleft. Tra le motivazioni ricorrenti per impegnarsi in una WCN, evidenziamo il desiderio di imparare, esprimersi liberamente e di relazionarsi in maniera paritetica. La voglia di sperimentare per alcuni è "senza motivazioni politiche", una curiosità di fondo per la tecnica che diventa una calamita, l'occasione e la "scusa per sperimentare" insieme ad altre persone. Emerge con forza, soprattutto dall'epicentro romano, l'idea che la Rete debba diventare un bene comune, "come l'acqua".

Dal punto di vista tecnico, le WCN ninux sono reti mesh [17], cioè reti a maglie in cui i nodi fungono da ricevitori, trasmettitori e ripetitori. Sono quasi interamente WiFi e usano protocolli standard (prevalentemente 802.11b/g/n) su frequenze di libero uso (2.4GHz e 5Ghz), ma ci sono anche porzioni connesse in rame. Le varie isole sono a loro volta connesse tra di loro tramite una VPN su Internet grazie al protocollo BGP [18] ma per una scelta di impostazione filosofica si preferisce usare questo canale di comunicazione solo per la manutenzione dei nodi o altri motivi tecnici e non per il normale traffico dati. Si tratta di una scelta di capitale importanza per il nostro discorso, perché in questo modo si evita che ninux diventi una mera DarkNet appoggiata sopra l'infrastruttura di Internet.

L'isola romana è quella con l'architettura di rete più complessa visto che comunica, direttamente, con le reti di diversi ISP (Internet Service Provider) oltre ad essere collegata presso il NAP (Neutral Access Point) romano (Namex) una zona franca in cui le diverse reti, che costituiscono Internet, si incontrano fisicamente. Ciò significa che le varie isole ninux sono sottoreti connesse anche ad Internet, ovvero che Ninux **Roma** è riconosciuta come un Sistema Autonomo

che può richiedere l'assegnazione di indirizzi da parte del Registro di Internet Regionale (RIR) (nello specifico il RIR di riferimento è il RIPE NCC) e dunque da parte della Internet Assigned Numbers Authority (IANA). I servizi di queste sottoreti possono quindi essere esposti a membri esterni alla WCN. I servizi disponibili sono gestiti e mantenuti su base volontaria, non sono previste forme di retribuzione monetaria.

EigenNet (attiva dal 2009), come si vede nella mappa dei nodi, è parte dell'arcipelago di ninux. Si trova a Pisa. Si connota come progetto in cui l'elemento tecnico viene importato all'interno di un precedente collettivo studentesco di orientamento "ambientalista e anticapitalista". La spinta iniziale era tesa a rendere più facile la configurazione e il mantenimento delle antenne wireless. EigenNet e Ninux Firenze rappresentano un'eccezione rispetto alla modalità di compilazione delle altre isole Ninux, nelle quali singole persone parlano della loro isola, del loro nodo, e della più ampia comunità. Le due realtà toscane invece hanno risposto entrambe come collettivo, e non si tratta di rappresentanti della comunità che gestiscono la rete, bensì di una compilazione collettiva durante momenti assembleari. In questo sono stati senz'altro facilitati in questo dalle ridotte dimensioni. Da Pisa ci spiegano che i servizi offerti (spazio disco, condivisione file, siti web, ecc.) cercano di venire incontro agli utenti in modo da non disorientarli troppo dal punto di vista dell'interfaccia, delle funzionalità e delle abitudini di utilizzo. Citano come esempio l'uso di OwnCloud, alternativa free e open a Dropbox per le soluzioni cloud. Questo atteggiamento di apertura sembra una risposta concreta alle osservazioni di alcuni ninuxari a proposito delle barriere tecniche in entrata, percepite come il principale ostacolo interno alla crescita e diffusione delle WCN.

In effetti la quantità di informazioni e competenze da acquisire, per un utente di Internet che si avvicini per la prima volta al mondo delle WCN, è enorme. Aprire un contratto con un ISP commerciale e connettersi a Internet è diventato assolutamente banale, mentre entrare a far parte di una WCN può essere molto complicato. Se ci si aspetta che tutto funzioni come sulle reti commerciali, l'esperienza sarà senz'altro frustrante e deludente. Per portare un'analogia semplice, assimiliamo la connettività al cibo. Gli accessi, le Reti e i servizi non sono tutti uguali, così come gli ortaggi industriali non sono uguali ai prodotti di un orto casalingo. Dal punto di vista dell'approvvigionamento, recarsi al supermercato non richiede alcuna competenza particolare [19]. Entrare a far parte di un gruppo d'acquisto solidale, invece, esige una certa disponibilità ad impegnarsi nell'organizzazione del gruppo, nella conduzione degli ordini collettivi, nello smistamento dei prodotti e così via. Le motivazioni economiche possono giocare un ruolo non secondario, perché in gruppo si possono spuntare prezzi migliori, ma chiunque faccia parte di un gruppo d'acquisto sa che in ogni caso la grande distribuzione è una soluzione più comoda, e quasi sempre più a buon mercato. Anche nel caso delle WCN le ragioni di adesione sono principalmente non economiche.

5. L'alternativa comunitaria

L'aspetto economico è un ulteriore punto di criticità interno rilevato dai questionari. I progetti WCN sono considerati utili più che altro per "allenarsi" dal punto di vista tecnico ma non alternative praticabili su larga scala rispetto ai servizi commerciali (da Google a Facebook), "irrilevanti dal punto di vista sociale, economico e politico". Diversi ninuxari vorrebbero che la loro rete "diventasse il substrato di una comunità che gestisce servizi tra pari, alternativi a quelli centralizzati finanziati con la logica della pubblicità". La carenza di fondi e la mancanza di tempo per curare sia lo sviluppo dei nodi sia la comunicazione verso l'esterno vengono indicati come ostacoli principali alla diffusione delle Reti Comunitarie. L'alternativa "indipendente" viene percepita come concreta in scenari come "calamità naturali e censura", cioè in situazioni eccezionali che rendano più difficile o impossibile l'uso di Internet. Per quanto riguarda l'uso di queste tecnologie in situazioni di emergenza si pensi al sistema per la segnalazione dei sopravvissuti sepolti dalle macerie in caso di terremoto in corso di sviluppo presso l'isola di Reggio Calabria o al sistema ideato dai Ninuxer Bolognesi che prevedere palloni aerostatici ancorati al suolo per la copertura Wi-Fi di ampie aree colpite da disastri [20].

5.1 I limiti delle WCN: ostacoli esterni

Sempre riguardo ai limiti nello sviluppo della rete vengono esplicitati anche ostacoli esterni, tra i quali "il terrore delle onde radio": a quanto pare molte persone sono restie a installarsi un'antenna Wi-Fi sul tetto, sul balcone o sul terrazzo perché spaventate dalla nocività delle onde. Non ci sono certezze definitive in merito, né sufficienti dati per sostenere che le onde dei router senza fili siano del tutto innocue, in particolare per bambini e adolescenti. Vale sempre il principio di precauzione, ma alcune considerazioni meritano di essere riportate anche in questa sede.

L'intensità di un segnale Wi-Fi è molto inferiore a quella di altri dispositivi di uso domestico (centomila volta inferiore a quella di un forno a microonde, che è opportunamente schermato); e sono radiazioni di tipo non ionizzanti (a differenza dei raggi X o delle onde radioattive, ad esempio), per le quali non si hanno evidenze scientifiche di pericolosità. Spesso nelle WCN si predilige l'installazione degli apparati sul tetto, non in ambienti di vita quotidiana, e spesso usando antenne direttive, che limitano ancora di più l'irraggiamento. Il dispositivo potenzialmente più dannoso sembra essere il telefono cellulare, che procura una dose ben più alta di microonde molto vicino al cervello. Ci vogliono molti router e computer portatili per generare un irraggiamento pari a quello di un solo telefono cellulare. Infine, in situazioni cittadine, è comune trovarsi immersi in dozzine di reti Wi-Fi private: è soprattutto in casi come questi che una riduzione e razionalizzazione delle sorgenti attraverso accessi condivisi potrebbe senz'altro ridurre la quantità di onde. Gli altri principali ostacoli culturali sono: un'insufficiente diffusione della cultura digitale (competenze tecniche) e della cultura collaborativa (competenze sociali), insieme alla diffusione della "filosofia dello scrocco" (in gergo si parla di *leechers*, persone che non contribuiscono attivamente alla WCN ma ne sfruttano i servizi).

Il desiderio di dar vita a un movimento che si autoalimenta si confronta quindi con ostacoli di vario tipo, non solo di natura tecnica. Anzi, dalle risposte appare chiaro che le questioni più complesse da affrontare sono quelle organizzative. Infatti Ninux si sforza di creare infrastrutture replicabili e distribuite, per consentire a tutte le isole della rete di rendersi autosufficienti, capaci di configurare e gestire in modo autonomo i servizi essenziali della loro comunità. Si sente il bisogno di introdurre delle innovazioni positive che possano essere adottate, "emulate", da tutti i gruppi. Il problema è proprio quello di immaginare e mettere a punto nuove procedure in maniera creativa. Non ci sono problemi nell'eseguire le procedure esistenti, mentre è difficile sperimentare nuove vie, verificare quali opzioni funzionano, limare i dettagli e propagare il modello adeguato alle esigenze individuate.

In merito alla crescita delle comunità, anche EigenNet sottolinea la lentezza e l'impegno profuso. Ma evidenzia che questo accade per una precisa volontà della comunità stessa, che cerca sempre stringere rapporti personali e diretti con gli interessati. Poiché chi installa un nodo entra, a livello logico, in primo luogo nella comunità di persone che gestisce la rete, nella WCN EigenNet questa partecipazione viene considerata possibile solo attraverso "un'effettiva condivisione di principi". In secondo luogo, la conoscenza diretta è un'occasione utile per fornire l'aiuto necessario a installare gli apparati di rete. Questo approccio si discosta notevolmente dalle rilevazioni di [10], secondo cui le tre sfide organizzative primarie (cf. IV-F) sono "trovare fondi per mantenere ed espandere la rete comunitaria", "trovare e mantenere i volontari" e "la crescita della Rete". La volontà di crescita porta con sé un accresciuto bisogno di reperimento fondi, che da una parte plasma la comunicazione in senso pubblicitario, dall'altra vede nelle collaborazioni con strutture commerciali e nell'instaurazione di figure professionali retribuite un sbocco quasi obbligato, magari non auspicato ma che darebbe fiato alla comunità. Ribaltando la prospettiva, le difficoltà interne (barriera tecnica in entrata; irrilevanza socio-politica ed economica delle WCN; carenza di fondi) ed esterne (mancanza di cultura digitale e collaborativa) sembrano derivare a cascata dall'imperativo della crescita. La risposta di EigenNet è non preoccuparsi della crescita ma organizzare seminari e incontri, cioè concentrarsi sull'aspetto qualitativo dei possibili nodi futuri piuttosto che su una comunicazione più ad ampio raggio. La sostenibilità economica rimane un problema irrisolto, ma inquadrato in una prospettiva più ampia di modello sociale e politico proposto dalle WCN.

6. Neutralità, ovvero libertà? Guifi.net e Tetaneutral.net

Un gruppo di persone di varia estrazione ha creato nel 2004 guifi.net, con epicentro Barcellona e la Catalogna, come alternativa agli operatori commerciali. La pagina di Wikipedia relativa al progetto così come il sito stesso ne spiegano bene origini, struttura e obiettivi. Più recente (2011) l'iniziativa di costituirsi come fornitore d'accesso indipendente da parte dell'associazione tetaneutral.net, con sede a Tolosa, la più ampia CN francese. Entrambe utilizzano tutte le tecnologie di rete legalmente disponibili per espandersi: Wi-Fi, doppino di rame, fibra ottica... e mirano a fornire una molteplicità di servizi, dai

più semplici (file sharing) ai più complessi (VOIP, DNS interni). La differenza principale riguarda la taglia: mentre guifi.net è una delle più ampie CN del mondo (si espande con alcuni nodi anche in Africa, America e Asia), tetaneutral.net è decisamente più piccola (poco più di 700 associati) e limitata al sud-ovest della Francia.

Entrambe però si pongono chiaramente come soggetti giuridici, contrariamente alle CN italiane; inoltre hanno contatti e collaborazioni in corso o previste con il mondo imprenditoriale. Si definiscono risolutamente a-politiche, "non governative" e "no-profit". Ribadiscono con forza la volontà di creare alternative comunitarie caratterizzate dalla neutralità del servizio, rispetto all'infrastruttura di rete e ai contenuti. Ci sembra che la neutralità menzionata dalla piccola e politicamente schierata EigenNet non sia esattamente la stessa cosa della neutralità auspicata da queste CN più mature per diffusione e articolazione. La neutralità rimanda però in tutti i casi a un desiderio di libertà dalle pastoie dell'Internet commerciale, considerata controllata e censurata e insicura. Il discorso merita senz'altro maggiore approfondimento. Uno spunto interessante per chiudere ci è offerto dalle riflessioni dedicate alle tecnologie digitali di massa del gruppo Ippolita, secondo cui nessuna tecnologia è neutrale, in quanto ogni strumento presenta "caratteristiche specifiche che vanno analizzate e discusse in maniera specifica. [...] La tecnica è potenza, l'uso di strumenti tecnologici implica l'esercizio di una competenza, frutto di una conoscenza, per cui l'utilizzatore si pone in una dinamica di potere situata, «in relazione a»; nemmeno l'uso di una tecnologia è neutro, perché modifica l'identità dell'utilizzatore." [21]

In effetti porre l'accento sul carattere situato della tecnologia e sul poter-fare attraverso strumenti specifici ci consente di mettere in primo piano, al di là delle incomprensioni terminologiche, la dinamica comunitaria. Se le reti sono considerate "bene comune" (ninux), da ampliare con "sistemi di collaborazione volontaria e autogestita da parte degli utenti" (guifi.net) è chiaro che la libertà agognata si può raggiungere solo attraverso un'organizzazione differente delle reti stesse. Schematizzando, si tratta quindi di una libertà "faticosa", che richiede impegno e sforzo a tutti i livelli, di contro a una libertà "facile", identificata con gli automatismi commerciali.

Un'anomalia tutta italiana rilevata durante questa ricerca è la forza con cui tutte le isole Ninux si dichiarano non alternative agli ISP commerciali. Tale peculiarità si evidenzia particolarmente nel materiale propagandistico sviluppato in cui la connettività a Internet non viene citata o addirittura ne viene negata la possibilità. Approccio questo radicalmente opposto a quanto accade nella WCN più ampia del mondo, la catalana e quindi spagnola guifi.net, e in tetaneutral in Francia. Difficile capire se l'anomalia sia dovuta a un tentativo di evitare i *leechers*, persone interessate a banda e servizi gratis o a basso costo o ancora anonimizzati piuttosto che a contribuire alla comunità. Si può anche considerare come meccanismo di protezione rispetto alla legislazione vigente, farraginoso e piena di zone grigie per quanto riguarda l'offerta di questo genere di servizi comunitari. Infine, potrebbe intendersi come eredità di un antico "patto fra gentiluomini" fra tecnici, atto a separare in maniera netta il mercato professionale

dal "giocattolo" comunitario. Comunque sia, solo nel caso italiano è possibile individuare una realtà a metà strada tra la WCN e i WISP (wireless ISP) commerciali: i *social ISP*. Si tratta di gruppi che forniscono la connettività a prezzo di costo, avvalendosi di tecnologie identiche a quelle adottate dagli operatori commerciali; si strutturano come soggetti legali (cooperative, associazioni) per contenere i costi e retribuire i professionisti impegnati. Segnaliamo fra i progetti più significativi Noiinet [22] e Progetto Neco [23].

7. Classificare e identificare

Dovrebbe essere chiaro a questo punto che le definizioni proposte nella prima parte non si adattano alle WCN. Tutti gli esempi presi in considerazione comprendono porzioni di Reti normalmente connesse a Internet e pagine web raggiungibili con un normale browser, ma anche Reti Profonde (non indicizzate e che necessitano credenziali di autenticazione) per quanto riguarda alcuni servizi, e persino Reti Oscure in quanto intenzionalmente nascoste, anonimizzate e decentralizzate. Tetaneutral.net si schiera apertamente dalla parte del server indipendente statunitense Riseup, le cui pratiche di protezione e sicurezza sono state oggetto di "criminalizzazione [...] nel quadro di un'inchiesta giudiziaria in Spagna" alla fine del 2014 [24]. Guifi.net promuove su larga scala l'installazione e l'uso di VPN crittografate. La conclusione di questa breve ricognizione è che le due risposte hacker per "aggiustare" Internet, Reti Oscure e Reti Comunitarie, non sono radicalmente opposte. In alcuni casi gli strumenti utilizzati sono pressoché identici, così come le competenze necessarie. Ribadiamo quindi che la costruzione di Reti Oscure non è appannaggio di gruppi criminali. Tutte le WCN prese in considerazione da noi e tutte quelle analizzate nella letteratura consultata [11], [26] dichiarano di porre particolare attenzione nella sicurezza e protezione di reti e dati attraverso l'uso di software libero, strumenti di crittografia e anonimizzazione. La differenza principale tra le due risposte rimane l'esposizione pubblica. Le WCN desiderano farsi conoscere ed espandere il loro modello, anche se non a tutti i costi.

Possiamo quindi ragionevolmente sostenere che sono intrinsecamente una proposta politica, ovvero sono modalità differenti (anche a fra loro) di vivere nello spazio pubblico. Sono proposte politiche perché, in un momento in cui i flussi di dati sono diventati vitali, tanto da poter essere assimilati al cibo, propongono una diversa organizzazione e gestione delle Reti. L'approccio è comunque radicale, perché va alla radice della questione e propone di costruire infrastrutture comunitarie. Per quanto riguarda lo specifico caso italiano analizzato, la struttura estremamente fluida di Ninux.org consente il proliferare di WCN eterogenee legate al suo arcipelago ma non per forza allineate per motivazioni, metodi e obiettivi. Oltre ad abbozzare un discorso sulle tecnologie di rete, abbiamo cercato di considerare queste tecnologie come un discorso, cioè le scelte tecnologiche come decisioni non anodine, ma cariche di implicazioni sociali e politiche.

Diverse questioni rimangono ancora aperte e necessitano senz'altro di ulteriore approfondimento. In primo luogo, le idee ed esigenze di decentralizzazione, anonimato e resistenza alla censura possono trovare concreta attuazione

attraverso gli strumenti scelti dalle comunità WCN? In seconda istanza, i modelli di autogoverno che queste comunità si sono date offrono effettivamente la possibilità di partecipazione libera? Quali sono gli effettivi margini di libertà e autonomia rispetto all'Internet commerciale? Infine, le scelte tecniche delle varie WCN mettono in pratica modelli fedeli all'idea di decentralizzazione oppure corrispondono a scelte di comodo e ricerca delle soluzioni più performanti? Da una simile deriva prestazionale deriverebbero scelte tecnologiche (protocolli e topologie di rete) di fatto esposte ai medesimi rischi di censura e controllo che le WCN correttamente individuano nelle strutture di rete preesistenti. Queste domande, sorte durante la stesura di questo articolo introduttivo, abbisognano di ulteriori indagini e di uno spazio adeguato per essere svolte in maniera non superficiale.

Concludiamo ribadendo una constatazione di base: se gli utenti dell'Internet commerciale sono i costruttori perlopiù inconsapevoli della Rete Profonda, i costruttori di WCN sono utenti e costruttori consapevoli anche di Reti Oscure. Sono diversi fra loro per retroterra socio-politico e culturale. Questa pluralità di soggetti coinvolti nel fenomeno delle DarkNet conduce inevitabilmente alla realizzazione di reti molto diverse fra loro. Fatte salve le domande in attesa di ulteriore elaborazione, questa biodiversità di rete è vitale, costituisce una ricchezza messa in pericolo dalla tensione alla Trasparenza Radicale [25]. Ci auguriamo che preservarla diventi un obiettivo comune.

Riferimenti bibliografici

[1] I virgolettati che seguono sono traduzioni nostre da <http://www.9jumpin.com.au/show/60minutes/stories/2014/september/the-dark-web/> ; per una lettura critica del video, si veda <http://allthingsvice.com/2014/09/15/the-truth-behind-60-minutes-hyperbole-of-the-dark-web/> . L'ultimo accesso effettuato per tutti i link riportati è fine ottobre 2015.

[2] <https://www.torproject.org/>

[3] <http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/>

[4] <http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>

[5] <http://blog.terminologiaetc.it/2013/06/12/significato-traduzione-whistleblower/>

[6] Una ricostruzione ormai classica e in parte agiografica si trova in Levy, S. (2002, 4), Hackers. Gli eroi della rivoluzione informatica, ShaKe.

[7] Lo scandalo noto come DataGate, scoppiato nel 2013 in seguito alla diffusione di documenti sulla sorveglianza di massa da parte dell'ex analista della CIA e dell'NSA Edward Snowden, è solo l'ultimo di una lunga serie. Segnaliamo in particolare la questione Echelon, oggetto di una relazione al Parlamento Europeo nel 2000, del giornalista scozzese Campbell, D. (2003), Il Mondo sotto sorveglianza, Elèuthera. Cryptome segnala e pubblica nel suo archivio materiale analogo fin dal 1996, quindi ben prima di Wikileaks: <https://cryptome.org/>.

[8] Lo spionaggio industriale si confonde sempre più con la sorveglianza istituzionale. Emblematico il caso della società milanese Hacking Team, che per un decennio ha venduto sistemi di intrusione in tutto il mondo (compresi regimi dittatoriali): i suoi dati interni sono stati pubblicati su Wikileaks nel luglio 2015. Un buon osservatorio sulla sicurezza informatica è il blog di Bruce Schneier, <https://www.schneier.com>.

[9] <http://infofreeflow.noblogs.org/post/2008/12/29/info-enclosure-2-0-di-dmtry-kleiner-e-brian-wyrick/>

[10] Il progetto più interessante di monitoraggio europeo, che si esaurirà nell'ottobre 2015, è stato CONFINE <https://wiki.confine-project.eu/>. Una delle ricognizioni più recenti e complete basate sui dati raccolti: BYRUM, G.. "What are Community Wireless Networks For?" **The Journal of Community Informatics**, North America, 11, oct. 2015 <http://www.ci-journal.net/index.php/ciej/article/view/1227/1167>

[11] Avonts, J; Braem, B.; Blondia, C.. 2013 "A Questionnaire based Examination of Community Networks", *International Workshop on Community Networks and Bottom-up-Broadband (CNBuB'2013)* <http://www.computer.org/csdl/proceedings/wimob/2013/9999/00/06673333.pdf>

[12] <https://guifi.net/>

[13] <https://tetaneutral.net/>

[14] <http://ninux.org/>

[15] <https://wiki.eigenlab.org/index.php/EigenNet> <https://eigenlab.org/eigennet/>

[16] Il progetto iniziato nel 2000 sembra essere terminato nel 2014, almeno sul web in chiaro; questo è l'ultimo screenshot reperibile: <https://web.archive.org/web/20140723135945/http://seattlewireless.net/>

[17] Per una prima infarinatura sulle specifiche tecniche relative ai protocolli utilizzati nelle reti mesh si faccia riferimento alla pagina di Wikipedia https://en.wikipedia.org/wiki/Wireless_mesh_network

[18] Approfondimenti relativi a protocolli e acronimi introdotti nel prosieguo ci porterebbero troppo lontano dagli obiettivi di questo articolo; un documento introduttivo sul funzionamento delle Reti è McNamee, J.; Fiedler, K.; Humeau, M.; Maisuradze, M. (2012), *Come funziona internet*, European Digital Rights (EDRi) Papers, trad. it. vari a cura di De Martin, J.C., Centro Nexa <http://nexa.polito.it/nexafiles/ComeFunzionaInternet.pdf>

[19] Per essere più precisi, quelle competenze specifiche sono talmente diffuse da non essere percepite come tali; ma una persona abituata alla piccola drogheria all'angolo non troverà affatto semplice orientarsi nei reparti del supermercato.

[20] http://www.raspibo.org/wiki/index.php/Gruppo_WBEN

[21] Ippolita (2012), *Nell'acquario di Facebook. La resistibile ascesa dell'anarcocapitalismo*, Ledizioni, p. 24. Da un punto di vista accademico, tra gli approcci che da decenni studiano le dinamiche di co-costruzione sociale delle tecnologie, non esclusivamente digitali, ricordiamo SCoT (Social Construction of

Technology) e ANT (Actor-Network Theory), alla quale ci siamo ispirati in questo lavoro. Per un primo approfondimento, si veda: Bruno Latour (1994), Non siamo mai stati moderni, Elèuthera. Un'analisi specifica sul passaggio dalle reti sociali alle tecnologie conviviali: Cabitza, F., Simone, C., Cornetta, D. Sensitizing Concepts for the Next Community-oriented Technologies: Shifting Focus from Social Networking to Convivial Artifacts, *The Journal of Community Informatics*, Vol 11, No 2 (2015).

[22] <http://mappa.italiachecambia.org/scheda/noinet/>

[23] <http://www.progettoneco.org/>

[24] <http://www.fdn.org/fr/article/2015-01-07/la-federation-fdn-soutient-riseup-security-not-crime>

[25] Ippolita, op. cit., pp. 51-58

[26] Maccari, L.; Bailoni, T. Wireless community networks: Una liberation technology per l'Internet del futuro, pp. 5-56, e in particolare 4. *Parte terza: le WCN, un tentativo di aggiustare Internet*, in Caso, R.; Giovannella, F. (2015), Reti di libertà. Wireless Community Networks: un'analisi interdisciplinare (Networks of Freedom. Wireless Community Networks: An Interdisciplinary Analysis), Quaderni della Facoltà di Giurisprudenza; 9. Trento : Università degli studi di Trento.

Biografie

Carlo Milani (PhD) è traduttore, prevalentemente di saggistica. Si è laureato in Lettere all'Università degli Studi di Milano (cyberpunk messicano). All'attività editoriale affianca l'informatica, specialmente lato web, con alekos.net - tecnologie appropriate. Insegna archeologia e validazione delle fonti digitali. Tiene regolarmente conferenze in università italiane ed europee, e formazioni di autodifesa digitale / informatica conviviale in collaborazione con l'autore collettivo ippolita.net.

email: carlo.milani@alekos.net

Savino Sasso è un membro attivo della wireless community network bolognese NinuxBO. Agli studi accademici e all'attività lavorativa come tecnico informatico al servizio della ricerca scientifica, affianca da sempre la passione per la libera circolazione del sapere. È tra i fondatori di RaspIBO, un non-corso di elettronica e informatica libere mirato alla condivisione di conoscenze ed esperienze. Appassionato divulgatore, tiene spesso presentazioni ed è attivo in numerose comunità e associazioni dedicate alla diffusione del software libero e alla riduzione dell'impatto ambientale.

email: savino.sasso@studio.unibo.it

RIQUADRO 4 - I Droni nella Didattica

La riduzione dell'impegno economico necessario ad acquistare un drone o ad affrontarne la realizzazione, grazie alla disponibilità a basso costo di componenti un tempo riservati a impegnativi programmi di ricerca e sviluppo (piattaforme inerziali, processori, sistemi di comunicazione wireless, telecamere, batterie) hanno reso possibile la diffusione di progetti educativi basati sui droni anche nelle scuole.

Un corso pilota è quello messo a disposizione degli studenti presso l'Istituto Tecnico Industriale Statale Galileo Galilei di Arezzo (<http://www.itis.arezzo.it/>), grazie all'impegno pionieristico del prof. Massimo Gallorini. I droni infatti hanno tutte le componenti che vengono studiate nell'istituto: meccanica, elettrotecnica, elettronica, informatica e sono ottimi strumenti per supportare analisi chimico-fisiche-biologiche e riprese per varie applicazioni a bassa quota.

Il programma, denominato "Droni a scuola di Droni", si prefigge di mostrare le possibilità di collaborazione fra la scuola ed il "mondo del



Figura 14
*Il drone realizzato
 dall'ITIS Galileo Galilei di
 Arezzo*

lavoro” nell’innovativo settore delle riprese con i droni ed è articolato su tre tipologie di corsi. Nel corso introduttivo vengono attivati corsi conoscitivi sui principali campi applicativi affini agli indirizzi dell’istituto, ma si parla anche di uso consapevole ed etico, di privacy e delle basilari norme di sicurezza nel volo. Nel corso pratico si affrontano gli aspetti tecnici del funzionamento HW e SW dei droni, approfondendo la sicurezza elettrica e meccanica e la tecnica di volo, con una giornata presso l’aeroporto di Arezzo per una dimostrazione di vari aeromobili adatti a riprese ed analisi di vario tipo. Nel corso teorico di base sulle regole dell’aria, svolto in collaborazione con l’Aeroclub di Arezzo con personale qualificato e abilitato da ENAC (Ente Nazionale Aviazione Civile), vengono approfonditi i temi tecnici e normativi dell’impiego dei droni, compreso

l'esame e il rilascio dell'attestato di pilota di mezzi aerei a pilotaggio remoto.

Nel corso del progetto i ragazzi del quinto anno dell'indirizzo elettronico-informatico hanno realizzato, con il sostegno della Fondazione Arte&Co.Scienza, un prototipo perfettamente funzionante di esacottero, che è stato poi impiegato in numerosi progetti applicativi al fine di insegnare agli studenti, al di là delle nozioni tecniche curriculari, una metodologia di lavoro di squadra in cui molte competenze diverse collaborano alla realizzazione di un obiettivo comune, inclusi gli aspetti di gestione operativa e commerciale, nonché mediatica, dell'attività.

Un esempio è il progetto "Le nostre chiese a volo d'angelo", in cui il drone ha sorvolato la chiesa di Santa Maria della Pieve di Arezzo per documentare lo stato della pietra arenaria utilizzata per costruire l'edificio ed ha effettuato in collaborazione con Davide Mariottini riprese al Santuario di La Verna, sia all'interno che all'esterno del fabbricato, per realizzare un documentario sul luogo di culto francescano. In questo caso sono state coinvolte anche competenze di videoripresa e di video editing, un altro settore di grande interesse per i giovani.

Bibliografia

- [1] Douglas, A. (1897). *The story of the earth's atmosphere*. D. Appleton and Company (volume digitalizzato da Google dalla copia della Harvard University e pubblicato in <https://archive.org/details/storyearthsatmo02archgoog> (ultimo accesso 30 agosto 2015))
- [2] Tesla Memorial Society of New York: <http://www.teslasociety.com/radio.htm> (ultimo accesso 2 settembre 2015)
- [3] Singer, P.W. (2009). *Wired for War. The Robotics Revolution and Conflict in the Twenty-first Century*. The Penguin Press.
- [4] Il brevetto di Nobel aveva come titolo "An Improved Mode of Obtaining Photographic Maps and Earth or Ground Measurements" using a photographic camera carried by a balloon, rocket or missile". In: A. Ingemar Skoog, A. (2010).

“The Alfred Nobel rocket camera. An early aerial photography attempt”, *Acta Astronautica*, Elsevier, 66, Issues 3–4, February–March 2010, 624–635

[5] Sito dell’Aeronautica: http://www.aeronautica.difesa.it/museoVdV/collezione_aeromobili/HangarTroster/Pagine/BI%C3%A9riotXI-II.aspx (ultimo accesso 1 settembre 2015)

[6] “Robot Television Bomber” *Popular Mechanics* June 1940, in https://books.google.it/books?id=19kDAAAAMBAAJ&pg=PA805&dq=Popular+Science+1933+plane+%22Popular+Mechanics%22&hl=en&ei=sXYNTvyADIGLsAK8pbSRCg&sa=X&oi=book_result&ct=result&redir_esc=y#v=onepage&q&f=true (ultimo accesso 1 settembre 2015)

[7] A.J. Lazarski, “Legal Implications of the Uninhabited Combat Aerial Vehicle”. *Aerospace Power Journal*, Summer, 2002, p. 75

[8] Kaplan, F. (2013). “The World as Free-Fire Zone. How drones made it easy for Americans to kill a particular person anywhere on the planet”, *MIT Technology Review*, 31 luglio 2013, <http://www.technologyreview.com/featuredstory/515806/the-world-as-free-fire-zone/>

[9] Goulter, Ch.J.M. (2009). “The Development of UAVs and UCAVs: The Early Years”, in *Air Power UAVs: The Wider Context*, Ed. Barnes O., London: Ministry of Defence Publishing. <https://www.scribd.com/doc/52847466/1/THE-DEVELOPMENT-OF-UAVS-AND-UCAVS-THE-EARLY-YEARS> (ultimo accesso 2° agosto 2015)

[10] Schreiber L., Ostiari E. (2014). “Game of drones: do civilian applications harbour opportunities for sustainable development?”, in *Mirova* http://www.mirova.com/Content/Documents/Mirova/publications/va/studies/MIROVA_Study_Game_of_drones_EN.pdf

[11] Veruggio G, Operto F, “Roboethics: Social and Ethical Implications of Robotics”, in *Springer Handbook of Robotics*, Siciliano, Bruno; Khatib, Oussama (Eds.), 2008, ISBN: 978-3-540-23957-4, pp. 1499-1524.

[12] Normativa del Ministero dello Sviluppo Economico <http://www.sviluppoeconomico.gov.it/index.php/it/commercio-internazionale/import-export/dual-use>

[13] Regolamento delle Camere di Commercio Italiane http://images.ge.camcom.gov.it/f/promozione_economia/sportello_internazionalizzazione/approfondimenti/du/dualuse.pdf

[14] Westin A.F. (1970) *Privacy and Freedom*, by Alan F. Westin, American Bar Association Coverage: 1960-2011 (Vol. 13 - Vol. 63, No. 4)

[15] Quarto Emendamento: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”.

[16] Rodotà S. (2014). *Il mondo della rete*. Quali diritti, quali vincoli. Laterza

- [17] Veruggio G., Operto F. (2014). "A dieci anni dalla nascita della Roboetica", Mondo Digitale, ANNO XIII N. 54 (http://mondodigitale.aicanet.net/2014-6/Relazioni/02_A%20dieci%20anni%20dalla%20nascita%20della%20Roboetica.pdf)
- [18] Springer, P.J (2). Military robots and drones. A reference handbook. ABC-Clio Publisher
- [19] Gogarty, B., Hagger M. (2011). "The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air". Journal of Law, Information & Science, vol 19(1).
- [20] Gregory J Nardi, G.J. (2009). "Autonomy, Unmanned Ground Vehicles, and the U.S. Army: Preparing for the Future by Examining the Past". School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas 10, <http://handle.dtic.mil/100.2/ADA506181> (ultimo accesso 31 agosto 2015).
- [21] Singer, P.W (2009). Brookings Institution. <http://www.brookings.edu/research/opinions/2009/06/27-drones-singer> (ultimo accesso 1 settembre 2015)
- [22] <https://www.thebureauinvestigates.com/?s=drones>
- [23] Cavallaro J., Sonnenberg S., and Knuckey S. (2012). *Living Under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan*. Stanford, Calif. International Human Rights and Conflict Resolution Clinic, Stanford Law School; https://www.law.stanford.edu/sites/default/files/publication/313671/doc/slspublic/Stanford_NYU_LIVING_UNDER_DRONES.pdf (ultimo accesso 1 settembre 2015)
- [24] <http://www.stopkillerrobots.org/>
- [25] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf
- [26] <http://www.unog.ch/80256EE600585943/%28httpPages%29/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument>
- [27] <http://www.unog.ch/80256EE600585943/%28httpPages%29/4F0DEF093B4860B4C1257180004B1B30?OpenDocument>
- [28] Testo pubblicato dalla Radio vaticana http://en.radiovaticana.va/news/2014/11/18/vatican_raises_issue_of_misuse_of_armed_drones_at_un_/1111518
- [29] http://futureoflife.org/AI/open_letter_autonomous_weapons (ultimo accesso agosto 31 2015)
- [30] Rossi P. (2004). "Dedalo e il labirinto: l'uomo, la natura, le macchine". "Rivista di storia economica" n. 3/04, Società editrice il Mulino.
- [31] G. Virone, A. M. Lingua, M. Piras, A. Cina, F. Perini, J. Monari, F. Paonessa, O. A. Peverini, G. Addamo, and R. Tascone, "Antenna pattern verification system based on a micro Unmanned Aerial Vehicle (UAV)," IEEE Antennas and Wireless Propagation Letters, vol. 13, pp. 169-172, Jan 2014.
- [32] G. Pupillo, G. Naldi, G. Bianchi, A. Mattana, J. Monari, F. Perini, M. Poloni, M. Schiaffino, P. Bolli, A. Lingua, I. Aicardi, H. Bendea, P. Maschio, M. Piras, G. Virone, F.

Paonessa,Z. Farooqui,A. Tibaldi,G. Addamo,O.A. Peverini,R. Tascone,S.J. Wijnholds (2015) Medicina array demonstrator: calibration and radiation pattern characterization using a UAV-mounted radio-frequency source. In: EXPERIMENTAL ASTRONOMY, pp. 1-17. - ISSN 0922-6435

[33] AAVV. (2015). *Drones for Disaster Response and Relief Operations* <http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/rims/drones-for-disaster-response-relief-operations-study.pdf>

Biografia

Gianmarco Veruggio: ingegnere elettronico, è Dirigente di Ricerca e Responsabile dell'U.O.S. di Genova presso il CNR-IEIT di Genova.

Specializzato in Informatica e Sistemistica, svolge ricerche nel settore della Computer Graphics applicata alla simulazione e alla realtà virtuale, nel settore della simulazione e controllo delle navi e dei centri di controllo telematico del traffico marittimo. Si dedica poi alla ricerca nel settore della Robotica e Automazione, interessandosi in particolare di architetture distribuite di controllo, sistemi NGC (Navigazione, Guida e Controllo), Internet Robotics.

Nel 2000 è stato co-fondatore della Scuola di Robotica, di cui oggi è Presidente Onorario.

Nel 2002 crea il termine Roboethics (Roboetica) e propone il concetto di un'etica applicata alla robotica. È ideatore e organizzatore del "First International Symposium on Roboethics" (Sanremo, 2004), del "EURON Roboethics Atelier" (Genova, 2006) e degli "ICRA Workshops on Roboethics" (Roma, 14 April 2007; Kobe, 17 maggio 2009; Shanghai, 13 maggio 2011). È stato Corresponding Co-chair del IEEE-RAS Technical Committee on Roboethics.

È autore del libro "Il Mare della Robotica", Di Renzo Editore, 1999.

Nel 2006 gli viene assegnato il Premio Regionale Ligure per l'Innovazione. Nel 2009 riceve l'onorificenza di Commendatore dell'Ordine al Merito della Repubblica Italiana. Nel 2015 la Rotary Foundation lo nomina Paul Harris Fellow.

Email: gianmarco@veruggio.it

Fiorella Operto: dopo gli studi di filosofia, co-fonda una collana di libri di divulgazione scientifica. Ha acquisito un'esperienza specifica nella divulgazione scientifica, lavorando in collaborazione con laboratori scientifici e centri di ricerca in Europa e negli Stati Uniti, partendo dal presupposto che la ricerca scientifica e la divulgazione della conoscenza scientifica debbano andare di pari passo. La sua attività è incentrata sull'introduzione di nuovi mezzi per comunicare le scoperte e le ipotesi scientifiche a un pubblico di lettori non specializzati, utilizzando ogni forma di comunicazione (romanzi, teatro, film, documentari, musica, spot) pur mantenendo le informazioni reali e precise.

Più recentemente, Operto ha cooperato con il Reparto Robotica del Consiglio Nazionale delle Ricerche in Italia per promuovere la conoscenza e la comprensione della nuova scienza robotica.

Nel 2000 è stata co-fondatrice della Scuola di Robotica, di cui oggi è Presidente.

Nel 2004 ha collaborato con il robotico Gianmarco Veruggio nella promozione dell'idea originale della Roboetica, ovvero di un'etica applicata che disciplini la progettazione, produzione e uso dei prodotti robotici.

Nel 2008 ha ricevuto il Blackberry Awards come Tecnovisionaria dell'anno per aver promosso in Italia il progetto Roberta, le ragazze scoprono i robot, ovvero l'uso di kit robotici per promuovere la curiosità e l'interesse scientifici presso le bambine e le ragazze.

Email: fiorella.operto@gmail.com

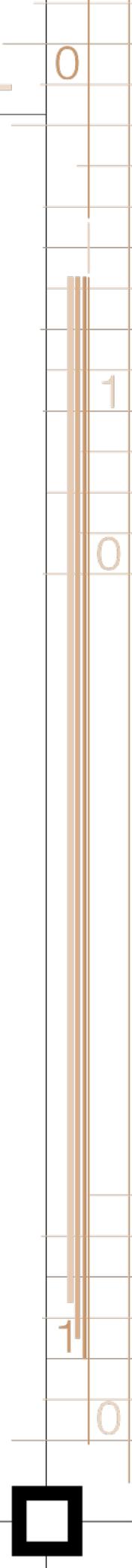
0

1

0

1

0



Internet e le dinamiche dei ruoli degli OTT (“Over The Top”) e Telco nel panorama ICT

Guido Vannucchi

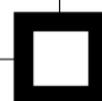
Sommario

L'articolo mette in luce i profondi cambiamenti che hanno rivoluzionato l'intero scenario ICT resi possibili dalla struttura e pervasività delle moderne reti. In particolare, si analizza il travolgente fenomeno della nuova figura di OTT (“Over The Top provider”) che fornisce servizi a livello globale sulle infrastrutture di reti esistenti determinando profonde metamorfosi che investono anche i tradizionali fornitori di servizi di telecomunicazioni (“Telco”) con potenziali rischi di destabilizzazione per l'intero ecosistema ICT. Nell'articolo si delinea l'acceso dibattito in corso sul tema della cosiddetta “Net Neutrality” e, nelle conclusioni, si accenna a possibili evoluzioni dello scenario con l'avvento dell’ “Internet of Things”.

Abstract

The article highlights the deep changes in the ICT ecosystem made possible by the structure and ubiquity of modern networks that have revolutionized the whole scenario of the ICT. Specifically it analyzes the overwhelming phenomenon of the new OTT (“Over The Top provider”) player which provides services at global level on existing network infrastructure. This step bring to a profound metamorphosis which is hitting even traditional telecommunications services providers (“Telco”) with potential risks of destabilization for the entire ICT ecosystem. The article outlines the strong debate in progress on the issue of so-called “Net Neutrality” and, in its conclusion, it hints at possible evolutions of the present scenario with the advent of the “Internet of Things”.

Keywords: IT; TLC; ICT; OTT; ISP; Telco (Telecommunication Company); CP (Content Provider); CDN (Content Delivery Network); Network Paradox; Open Internet; Net Neutrality, All-IP Network; IoT (Internet of Things).



1. Introduzione e quadro di riferimento

Ancora alla fine degli anni 80 - in un panorama in cui era già stato preconizzato il processo di convergenza tecnologica tra Informatica e Telecomunicazioni nell'unico settore ICT (“*Information & Communication Technology*”) - se qualcuno chiedeva agli esperti quali sarebbero state le due aziende più importanti nel panorama ICT degli anni 2000, la risposta unanime era: IBM nel campo della manifattura ed ATT nel campo dei servizi. Questa previsione non si è mai avverata ed è già molto che le due aziende citate non siano scomparse (come molte altre dell'epoca¹) solo a costo di profonde trasformazioni in cui i loro ruoli di manifattura e servizi sono stati largamente stravolti.

Il settore ICT ha così rappresentato, più che in altri campi, la dimostrazione lampante del pensiero di Schumpeter che la vera innovazione è una “distruzione creatrice”.

In particolare, gli OTT (“*Over The Top provider*”) hanno mirato all'innovazione di mercato offrendo “servizi” che traggono il massimo frutto dai nuovi paradigmi di comunicazione (globalità, interconnessione, interattività, larghezza di banda, ecc.) sviluppatasi per merito delle innovazioni tecnologiche che hanno completamente rivoluzionato l'architettura delle reti di telecomunicazione. L'unione, infatti, della digitalizzazione applicata a tutti i tipi di segnali e delle tecniche informatiche utilizzate per il trattamento dei dati ha portato alla nascita di Internet², tratteggiando un risultato straordinario di *cross-fertilization* [1] tra i due settori base dell'ICT. In questo processo non va dimenticato il ruolo fondamentale della Microelettronica che ha reso possibile lo sviluppo vertiginoso, a prezzi *consumer*, di terminali sempre più sofisticati (*notebook, tablet, smarphone, connected TV*, ecc.) che sono causa ed effetto del travolgente aumento dei servizi personalizzati e della rivoluzione dello scenario ICT.

Da metà degli anni 90 il cammino degli OTT è stato irruente ed aggressivo ed ha portato a servizi su scala globale sempre più rivoluzionari e gestiti con modelli di *business* del tutto innovativi. Gli OTT sono definiti “*Over The Top*” per evidenziare che i molteplici servizi da essi forniti sono “disgiunti” dal trasporto dei dati e si “appoggiano” alle reti IP degli operatori di telecomunicazioni (“Telco”). Essi operano pertanto “al di sopra” delle Reti ed il modello di *business* che li caratterizza permette loro di mantenere la completa esclusività dei contenuti inviati e dei relativi *copyright*.

¹ In campo manifatturiero ICT, citando solo le più note, dalla fine degli anni 80 sono scomparse: Acorn, Amdahl, Atari, Bell&Howell, Burroughs, Commodore, Compaq, Control Data, Data General, Digital Equipment, General Electric, Honeywell, ITT Corporation, Marcon Company, Mitsubishi Electronics, Motorola, Nixdorf, Olivetti, Packard Bell, Plessey, RCA Corporation, Sanyo, Siemens Telecommunication, Sperry Rand, Stromberg&Carlson, Tandy, Texas Instruments, Telettra, Xerox, Zenith Data Systems, Western Electric. Con le notizie dello scorso Aprile spariranno a breve anche i nomi Alcatel-Lucent e Nokia-Siemens e rimarrà il solo nome Nokia per le corrispondenti attività.

IBM da grande manifatturiero è diventato oggi fornitore di Servizi ad alto valore aggiunto. AT&T, dal solo mercato USA, si è portata sul mercato globale con offerta molto differenziata di servizi rispetto al passato.

² Il concetto di Internet (abbreviazione di *Internetworking*) nella sua veste di rete di commutazione a pacchetti di dati viene implementato, come ben noto, sulla rete Arpanet a partire dalla metà degli anni '60 ed il primo messaggio spedito con successo sulla rete tra le Università di UCLA e lo SRI (Stanford Research Institute) è dell'Ottobre 1969. La data di nascita di **Internet per il grande pubblico** - dopo l'introduzione del protocollo TCP/IP del 1975 e dell'ipertesto w.w.w. del 1990 sul cui terreno si muoveranno gli OTT - è di molti anni più tardi e viene considerata la **fine Dicembre 1995** quando Bill Gates dopo un lungo periodo di disinteresse alle innovazioni di rete allo studio - pronuncia, in un party natalizio della sua azienda, la frase passata alla storia: “Internet è nel futuro di Microsoft” !

In questo modello di comunicazione viene quindi sfruttata l'innovazione del paradigma Internet che separa il servizio dal trasporto delle informazioni creando una molteplicità di servizi differenziati che possono avere un'incidenza significativa sulla crescita del PIL dei Paesi che utilizzano appieno le potenzialità della rete.

Per quanto riguarda il traffico sulle reti di comunicazioni, una delle più vistose conseguenze è stato il determinante passaggio dalla “centralità della voce” alla “centralità dei dati” [2-3] dal momento che i contenuti di varia natura che gli OTT offrono agli utenti sono tutti implementati nella forma di comunicazioni “dati”. Inoltre, come conseguenza del rapido diffondersi dei nuovi servizi, la velocità di accesso delle reti si è accresciuta di quasi 1000 volte con tassi di crescita annuali a due cifre del traffico *downstream* [4-5] generato dai *server* di pochi grandi OTT e *Content Provider* ciò che, tra l'altro, determina enormi squilibri nei flussi di traffico dati [6].

Storicamente l'inizio della fase di espansione degli OTT è coincisa con il “boom” per le Telco della telefonia mobile e del ricco mercato conseguente: questa circostanza le ha presumibilmente distratte dall'assumere rapidamente una piena coscienza dell'imponente fenomeno OTT in tutti i suoi risvolti anche per l'inaspettata velocità d'espansione dei nuovi attori, impedendo loro di arrivare preparate e adeguatamente sensibilizzate ad alcuni “appuntamenti” critici di evoluzione e sviluppo delle reti conseguenti al nuovo quadro.

In questa situazione mentre da un lato si sono ampliati esponenzialmente - e sempre più con alta remunerazione (diretta o indiretta) - i servizi innovativi forniti dagli OTT, dall'altra le Telco (in particolare europee) hanno visto diminuire le entrate ed i margini di profitto sui servizi di connettività anche per la forte competizione seguita alla liberalizzazione delle telecomunicazioni.

La conseguenza per gli operatori TLC è stata di una scarsa propensione a nuovi investimenti nella rete perché considerati con un ritorno non adeguato nonostante il massiccio aumento del traffico IP. Questi problemi di sostenibilità economica-finanziaria delle Telco [7] mettono pertanto a rischio proprio gli investimenti indispensabili per nuovi accessi, fissi e mobili a banda larga e larghissima.

Nel tempo si è pertanto creata tra OTT e Telco una situazione di confronto scontro. Gli OTT tendono a guardare alle Telco come puri fornitori di connettività - assolutamente vitale per il loro *business* - e naturalmente auspicano prezzi del trasporto dati particolarmente contenuti in modo da poter aumentare la platea dei clienti. Dall'altra, le Telco tendono a vedere gli OTT come gli operatori che, con i loro nuovi servizi, hanno senza dubbio aumentato decisamente l'entità del traffico dati e le richieste di connessione alla Rete ma che, al tempo stesso, traggono il massimo profitto economico dalle nuove possibilità offerte dalle reti con uno sproporzionato sbilanciamento a loro favore.

Le Telco, inoltre, si sono ritrovate con alcuni OTT come nuovi competitori diretti che, “appoggiandosi” alla rete, offrono servizi TLC che gli utenti tendono spesso ad impiegare in quanto più innovativi di altre tipologie di offerte tradizionali.

Come reazione, gli Operatori di telecomunicazione hanno cercato di entrare nella distribuzione dei contenuti ma spesso, in particolare gli europei, solo su scala nazionale o quantomeno su un parco non grandissimo di utenti sottovalutando il fatto che un vero grande punto di forza che caratterizza il

business degli OTT è la loro impostazione di offerta su scala globale anziché verso un parco utenti intrinsecamente limitato.

Il quadro di confronto presenta pertanto delle singolarità che rischiano di destabilizzare l'intero sistema ICT, in particolare nelle aree geografiche in cui gli operatori TLC sono più frammentati, se non si riescono a trovare nuovi equilibri con un miglior bilanciamento di vantaggi e svantaggi tra le diverse componenti.

Il presente articolo si propone, nello specifico, di chiarire la dinamica dei ruoli reciproci di OTT e Telco e di evidenziare le presenti criticità dell'ecosistema ICT che condizionano anche il futuro sviluppo di Internet. A tale proposito, dopo un breve richiamo storico sulla evoluzione degli OTT, vengono analizzate in maggior dettaglio il loro ruolo e la loro natura a confronto delle Telco nonché le interazioni reciproche. L'analisi della evoluzione quantitativa del mercato globale dell'ecosistema ICT a partire dagli inizi degli anni 90 ed il confronto di alcuni dati economici-finanziari delle due famiglie di attori serve a meglio comprendere il quadro di confronto tra OTT e Telco.

Si passano quindi ad esaminare due fondamentali criticità - Il “*Network Paradox*” e la cosiddetta “*Net Neutrality*” - che pesano sull'attuale scenario ed, infine, si cerca di identificare possibili percorsi nell'evoluzione dell'ecosistema ICT per la ricerca di equilibri più stabili.

2. Evoluzione storica e natura degli OTT

La “interconnessione” fra reti era, come è ben noto, gratuita quando Internet serviva per scambiare file fra i calcolatori delle università. La chiusura di NSF-Net³ del 1995 segna l'inizio dello sviluppo commerciale di Internet e lo scenario si evolve rapidamente.

Si espandono inizialmente gli “*Internet Service Provider*”⁴ (ISP) caratterizzati dall'offerta di portali che sviluppano *browser* e potenti motori di ricerca (*Yahoo*, *Excite*, *Google*, ecc.) per “accedere” alle informazioni desiderate. Dopo la “bolla” del 2000 la miriade iniziale di ISP per la fornitura di accessi Internet si concentra in grandi ISP che tendono ad identificarsi con gli operatori Telco che, parallelamente, cominciano ad offrire alcuni tipici servizi Internet.

Successivamente (2003) nascono siti Web con possibilità di scaricare (“*free*” od a pagamento) contenuti (in particolare musica) ed applicazioni complementari alle attività *hardware* delle rispettive aziende (*Apple*, *Samsung*, *HP*, ecc).

A partire da tale epoca iniziano ad affermarsi – come fenomeno di portata planetaria - i “*Social Network*” (*Facebook*, *Twitter*,...) e, verso la fine degli anni 2000, i “*Content Provider*” (CP) propriamente detti (quali ad esempio *Netflix*,...)

³ Val la pena ricordare che la NSFNet (National Science Foundation Network) - creata nel 1986 per collegare a 56 Kbps i centri di supercomputing di Università e Centri di ricerca USA - crebbe sino a diventare un backbone a 45 Mbps, sostituendo anche la famosa ARPANET. Nel 1995 le autorità eliminarono le residue restrizioni al trasporto di traffico commerciale su Internet e NSFNet fu chiusa lasciando il campo ad una pluralità di reti gestite da ISP (Internet Service Provider). A Dicembre 1995 avviene, come già ricordato nella Nota 2, il riconoscimento ufficiale di Microsoft all'importanza potenziale di Internet.

⁴ Storicamente il nome ISP (“Internet Service Provider”) è stato sinonimo di fornitori di accesso ad Internet spesso con una propria rete di backbone che, per l'accesso, si appoggiava in “*unbundling*” alle reti degli Operatori ex-monopolisti. Successivamente il nome si è esteso, purtroppo in modo confuso, anche ai fornitori di “servizi” Internet (spesso coincidenti con i primi).

che forniscono esclusivamente contenuti (“*streaming media on demand*”). Immediatamente a seguire si sviluppano i CDN (“*Content Delivery Network provider*”), quali *Akamai*, *Limelight*, ecc., meno noti al grande pubblico, in quanto contraddistinti dalla fornitura ai *Content Providers* di un sistema distribuito di server che, dislocati strategicamente nei nodi della rete, sono in grado di fornire agli utenti - attraverso algoritmi studiati per ottimizzare la distribuzione dei contenuti - prestazioni elevate ed alta affidabilità.

A partire dal 2006 si diffondono i servizi di navigazione (*Google Maps*, *Waze*,...) e vengono resi disponibili servizi di “*gaming*” in rete (*Nintendo*, *Microsoft*...). Nello stesso periodo si affermano altresì i *Providers* che forniscono veri e propri servizi di comunicazione e messaggistica (*Messenger*, *Skype*, *WhatsApp*, ecc.) in concorrenza con le Telco.

Ed è così che, in pochi anni, i nuovi protagonisti quali *Yahoo* (nata nel 1994), *Apple on line store* (1997), *Google* (1998), *Skype* (nata nel 2003 ed acquisita da Microsoft nel 2011), *Facebook* (2004), *You Tube* (2005 ed acquisita alla fine del 2006 da Google), *Twitter* (2006), *Netflix* (dal 2008 come servizi *on-line*) – si accrescono vertiginosamente sul mercato mondiale, arrivando in alcuni casi, anche attraverso acquisizioni, ad essere veri e propri monopoli⁵ a livello globale e senza soffrire in modo significativo, a differenza delle Telco, di limitazioni legali, fiscali o regolatorie⁶.

In sintesi si può pertanto affermare che la **natura peculiare degli OTT** consiste nell’aver usufruito in modo innovativo dello spazio di condivisione globale creato da Internet: la rete è diventata pertanto il basamento vitale della loro esistenza. Essi, come già detto, **disgiungono l’incombenza del servizio** che offrono dal trasporto/accesso dei pacchetti dati mentre tale conduzione resta completamente affidata alle reti degli operatori Telco in modalità *best-effort*.⁷

Con tale impostazione gli OTT sono in grado di generare un **grande valore economico** appoggiandosi alle infrastrutture di rete esistenti in quanto, ai bordi della rete, sono rigorosi nel mantenere un completo controllo dei propri server e

⁵ In passato i Telco più tradizionali si sono sviluppati come monopoli nazionali in virtù della natura stessa del loro business e dell’alto costo dell’accesso che non era logico raddoppiare (le Authority di regolazione nascono, infatti, molti anni dopo a seguito della liberalizzazione del mercato proprio per garantire l’accesso a questo fondamentale segmento della rete per tutti i concorrenti).

Analogamente, anche se su scala globale, oggi stiamo assistendo a processi di concentrazione degli OTT su determinate tipologie di mercato. In tale campo, infatti, sta valendo la logica che “the winner takes all” (basta menzionare l’esempio di Amazon) il che porta alla creazione di veri monopoli a livello planetario e non solo a livello nazionale come era in passato per le vecchie Telco. Inoltre, un effetto di ulteriore concentrazione nasce dal fatto che gli OTT riescono a trovare sinergie e ulteriore valore aggiunto collegando opportunamente tipologie di servizi nati stand-alone (un esempio tipico, a tale proposito, è quello di Google).

⁶ Questa è anche una delle ragioni del perché, essendo l’USA un Paese con maggiore propensione al rischio, tutti i grandi Provider OTT sono nati e si sono sviluppati in USA che, nel panorama mondiale ICT, può oggi considerarsi un paese “OTT centric” (osservazione da tener presente quando si analizzano le posizioni rispettive di USA ed Europa su questi argomenti).

⁷ Anche i Telco apparentemente hanno in comune con gli OTT il fatto che nell’offrire i loro servizi, nel momento in cui escono dai confini della propria rete nazionale, sono obbligati a transitare su reti d’interconnessione internazionali e, in arrivo al destinatario del servizio (voce, dati, ecc.), sulla rete nazionale di un altro Operatore. A prescindere peraltro dal fatto che il servizio offerto, in particolare in passato, era tipicamente bidirezionale, le interconnessioni (sia su rete fissa che su rete mobile) sono rette da accordi ben precisi che prendono in considerazione la ripartizione del fatturato tra i vari gestori interessati alla comunicazione.

dell'interfaccia utente con la conseguente possibilità di una “**profilazione**” assai precisa dell'utenza per di più non limitata ad un'area geografica ma su scala globale. Queste caratteristiche - aggiunte a **modelli di business** che vanno dalla fornitura gratuita del servizio all'utente finale (con ricavi generati da “*on line advertising*”) fino ad offerte di servizi ed applicazioni completamente a pagamento (“*gaming on line*”, *delivery* di Contenuti *premium* ecc.) - fanno degli OTT attori profondamente diversi rispetto ai tradizionali gestori Telco.

Una **classificazione** precisa degli OTT risulta difficile e complessa perché - a prescindere dalla difficoltà oggettiva di suddividere gli innumerevoli servizi offerti in classi omogenee - un sempre maggior numero di OTT tende ad operare in più classi di tipologie di offerta. A ciò si aggiunge il fatto che il mondo degli OTT è in continua evoluzione e che alcuni servizi innovativi dovrebbero essere associati a diverse classi di servizi: basta pensare che *WhatsApp*, oltre alla messaggistica su testi e immagini, ha iniziato a fornire servizi voce e video e che *Twitter* ormai fornisce *streaming* video in tempo reale.

Per queste ragioni in **Tabella 1** vengono sintetizzate le caratteristiche peculiari di due sole grandi classi, “puri” e “ibridi”, di **BIG OTT** confrontandole con le specificità delle Telco per meglio chiarire il campo di **incontro/scontro** tra i nuovi attori e gli Operatori di telecomunicazioni. Nella stessa Tabella sono evidenziati i nomi degli OTT e Telco più noti in Europa ed attualmente appartenenti alle tre classi.

	BIG OTT “PURI”	BIG OTT “IBRIDI”	TELCO
ATTORI TIPICI	<ul style="list-style-type: none"> • GOOGLE, YAHOO, FACEBOOK • YOUTUBE*, TWITTER, • SKYPE*, WHATSAPP*,... • NETFLIX, AKAMAI, ... 	<ul style="list-style-type: none"> • APPLE, SAMSUNG, • MICROSOFT, IBM, • AMAZON, ALIBABA, EBAY, ... 	<ul style="list-style-type: none"> • CHINA MOB., AT&T VERIZON.. • DEUTSCHE TLK, TELEFONICA FT-ORANGE, BT, TELECOM ITA • VODAFONE
KEY ASSET	<ul style="list-style-type: none"> • Operatori su scala globale • Applicazioni indifferenziate • Leader nei “<i>Social Networks</i>” • Controllo degli “<i>end points</i>” • Impiego di bande larghissime 	<ul style="list-style-type: none"> • Distribuzione contenuti associate a prodotti hardware • Leaders nella “<i>IT on the Clouds</i>” • Distribuzione di prodotti fisici su scala mondiale 	<ul style="list-style-type: none"> • Oligopoli Locali/Nazionali • Livelli di qualità differenziata • Servizi di “customer care” • Controllo infrastrutture rete
VINCOLI	LIMITATI (grazie ad extraterritorialità legale/fiscale)		FORTI (Regolamentazione)
PARAMETRI ECONOMICI FINANZIARI	<ul style="list-style-type: none"> • Proventi indiretti (pubblicità) • Dinamica crescita altissima • Ridotti livelli Investimenti • Alta generazione cassa • Capacità finanziaria elevata 	<ul style="list-style-type: none"> • Eterogeneità elevata in Ricavi, Dipendenti, Utili; • Crescita differenziata per attività • Generazioni cassa differenziata • Livelli Investimenti differenziati • Buona capacità finanziaria 	<ul style="list-style-type: none"> • Aziende di grandi dimensioni • Crescita limitata o negativa • Margini ridotti per concorrenza • Necessità alti investimenti • Alto indebitamento • Posizione finanziaria indebolita

(*) *YouTube è stata acquistata da Google nel 2006 per 1,65 MILD\$, Skype da Microsoft nel 2011 per 8.5 MLD\$ e Whatsapp da Facebook nel 2014 per 19 MLD\$. e sono ormai incorporate nelle controllanti*

Tabella 1
Caratteristiche dei vari attori dell'ecosistema ICT

Nella Tabella i *player* definiti “puri” sono quelli che sfruttano per il loro *business* la Rete in modo integrale; “ibridi” sono invece quelli caratterizzati dall’affiancare alla loro tradizionale attività manifatturiera (ovvero di distribuzione prodotti) un’attività secondaria, tipicamente OTT, importante (ma concettualmente non indispensabile) per migliorare il loro *core business*.

Di quest’ultima categoria Apple è l’esempio più noto a tutti in quanto da molti anni la vendita *on-line* di prodotti audio ed *Apps*, pur non superando il 10% dei ricavi complessivi, è anche un importante **veicolo** per una maggiore vendita dei prodotti *hardware*. Non sembra tuttavia corretto (e lo stesso si può dire per altri OTT ibridi) assimilare l’intera azienda, come fanno molti analisti finanziari, ad una “*OTT Company*” in quanto Apple avrebbe continuato ad esistere come manifatturiera (*hardware/software*) anche senza la rivoluzione apportata dal *business “Over The Top”*

In altre parole i veri OTT sono solo i “puri” il cui *business*, dall’ordine alla consegna del prodotto, si chiude sulla rete (in questa accezione, per Apple, il solo *business* I-Tunes va considerato OTT).

Esaminando la Tabella 1 si può osservare come, tra i servizi OTT “puri”, molti sono **complementari** rispetto a quelli offerti dalle Telco (ad esempio motori di ricerca, “*Social Networking*”, ecc.) e contribuiscono ad aumentarne le relative entrate mentre altri sono in **diretta competizione** con classi di servizi storicamente tipicamente Telco nel passato (messaggistica, telefonia vocale, “*videophone*”, ecc).

In ambedue i casi è di fondamentale importanza per gli OTT poter fare affidamento su uno sviluppo massiccio delle **reti di accesso broadband** quali i sistemi ADSL per reti fisse ed i sistemi 3G per reti mobili. In aggiunta, per servizi più evoluti (HD o UHD), vi è una forte pressione sui Telco per la realizzazione in tempi rapidi di accessi *ultra-broadband* quali sistemi FTTC (*Fiber To The Cabinet*) o FTTH (*Fiber To The Home*) per le reti fisse nonché sistemi 4G per le reti mobili.

In aggiunta ai sistemi di accesso, occorrono **prestazioni di rete** particolarmente avanzate affinché gli OTT possano erogare i loro servizi con qualità adeguata ad una percentuale sempre maggiore di utenti ma questa esigenza, come si vedrà nel Paragrafo 5, ha creato una nuova categoria di OTT che provvedono a particolari funzioni per ottimizzare la qualità della rete prima che le Telco intuissero tale esigenza.

La classificazione molto semplificata della Tabella 1 deriva anche dal fatto che in campo OTT - come avvenuto per gli Operatori Telco nell’ambito dei servizi di rete fissa e rete mobile - è in corso (vedi Nota 5) un **processo di aggregazione** di servizi diversi sotto un unico gestore. Le più importanti acquisizioni degli ultimi anni - particolarmente utili per chiarire l’evoluzione degli OTT puri ed ibridi - sono citate, con le relative transazioni finanziarie, in calce alla Tabella. Questa tendenza continuerà e porterà a ridurre il numero di *players* OTT aumentando le dimensioni di quelli rimanenti.

3. Scenario di mercato dell'ecosistema ICT

Al fine di comprendere meglio il quadro di confronto tra OTT e Telco e le relative dinamiche è utile esaminare i dati del mercato ICT attuale e della sua evoluzione negli ultimi 25 anni (Figura 1).

La Figura fa riferimento alle **definizioni aggiornate** (a partire dal 2011) dei segmenti del mercato ICT la cui tipologia è stata rivista con l'introduzione - secondo le attribuzioni riportate nel **Riquadro** alla fine dell'articolo - del cosiddetto "**Global digital market**" che, nel seguito, si continuerà per semplicità a denominare mercato dell'ecosistema ICT.

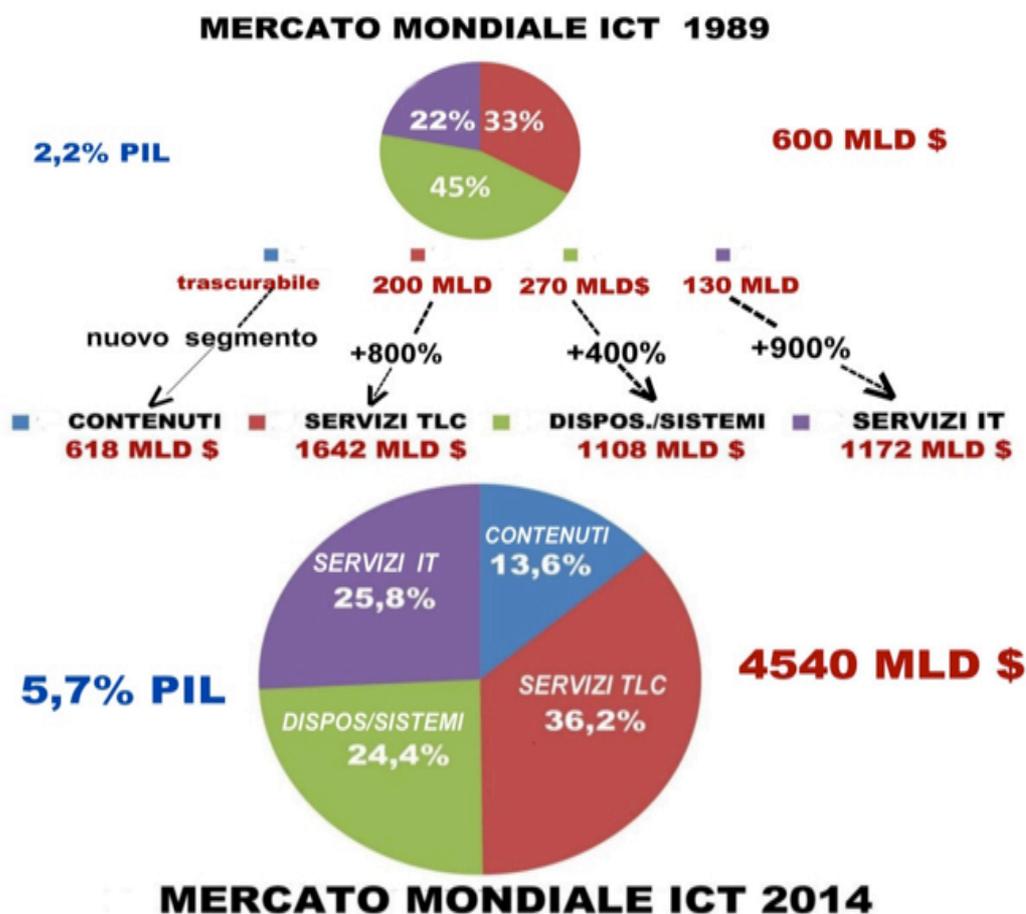


Figura 1
 Evoluzione del mercato ICT in 25 anni (in MLD\$ correnti)
 (I valori del mercato 2014 sono presi del Rapporto Assinform-Net Consult 2015)

Dai dati riportati in Figura 1 si possono fare le osservazioni sotto riportate.

- Il mercato mondiale dell’ecosistema ICT è cresciuto in 25 anni di circa 8 volte ad una percentuale media annua dell’8.5%.
- Il mercato dei “Contenuti digitali e pubblicità *on-line*”, in crescita da anni con ritmi a due cifre, ha oggi un peso di quasi il 14% del mercato globale ICT contro il valore quasi trascurabile di 25 anni fa (se non altro in termini economici).
- Il segmento “Dispositivi e Sistemi” - pur rappresentando nella nuova classificazione l’intera porzione manifatturiera⁸ dell’ecosistema ICT - è decisamente diminuito in questi ultimi 25 anni in peso percentuale, passando da un 45% a poco più del 24% del mercato complessivo. Ciò consegue alla forte decrescita dei prezzi degli apparati professionali non compensata dalla nascita di un sofisticato mercato *consumer* che, peraltro, ha raggiunto oggi un sensibile peso economico, oltre che strategico, in particolare per merito degli *smartphone*.

Un minor peso percentuale dell’*hardware* rispetto al passato è, d’altra parte, in linea con l’ingresso nella “Società dei Servizi” ma - è bene sottolinearlo - il segmento “Dispositivi/Sistemi” è ancora ben lontano dall’essersi trasformato in una *commodity* (basti pensare alla Apple, Samsung ed ai fabbricanti cinesi ed ai margini che si riesce ancora a spuntare su tale mercato!).

- Il complesso dei “Servizi IT” - che include nella nuova definizione allargata anche quello del “*Software*” distribuito in rete ed il nuovo mercato delle *Apps* (anche se ancora alquanto limitato) - ha oggi un peso di circa il 26% del totale incrementando in tal modo di quasi 4 punti la relativa quota del mercato totale ICT.
- I “Servizi TLC” (per rete fissa e mobile) risultano attualmente il segmento di maggior peso nell’ecosistema ICT e si sono accresciuti rispetto al passato di più di 3 punti in percentuale nonostante i prezzi fortemente decrescenti dei servizi di connettività in rete fissa e mobile. La ragione è stata soprattutto legata alla crescita imponente della Cina nel mobile e, più in generale, del mondo asiatico.

In questo segmento i servizi OTT di telecomunicazione hanno oggi un peso del tutto trascurabile mentre, come detto più volte, il traffico generato dagli OTT quali i *Social Network*, Google, Amazon, ecc ha certamente contribuito in modo sostanziale all’attuale entità del segmento.

Le precedenti osservazioni associate ai dati della sottostante **Figura 2**, ci permettono alcune considerazioni relativamente al confronto OTT-Telco.

- A. Il primo **mercato** in cui si muovono gli *Over the Top* è, attualmente, il segmento dei “Contenuti & Pubblicità” (*Google, Facebook, Apple I-tunes, Netflix*) ed è presumibile che, essendo in forte crescita quello legato ad Internet, tale segmento giocherà un ruolo rilevante nell’ecosistema ICT.

⁸ In realtà si ricorda che, già da tempo, il software di sistema degli apparati è considerato parte integrante del segmento manifatturiero a tutti gli effetti.

Inoltre i servizi in cui sarà sempre più forte la presenza degli OTT sono varie tipologie di servizi IT (IBM, HP,...), le Apps (Apple, Google,..), i servizi TLC (WhatsApp, Skype,..) che sono sottosegmenti che si prestano al modello di business ed alla natura degli Over the Top "puri", servizi che, per altro aspetto, contribuiranno ad incrementare sensibilmente il traffico sulla rete.

- B. Come risulta evidente da Fig. 2 - che aggiorna ed amplia i dati 2011 analizzati in [8] - i soli OTT "puri" sono riusciti a creare, senza necessità di forti investimenti, una fonte di ricavi con ingenti margini raggiungendo un'eccezionale capitalizzazione di mercato (MK CAP). In pochi anni essi hanno così potuto dare origine a imponenti generazioni di cassa con una conseguente possente struttura patrimoniale confrontabile con quella dell'intero settore mondiale delle Telco ed in grado, pertanto, di condizionare tutto l'ecosistema ICT.
- C. Nonostante, il grande successo degli OTT e l'invidiabile posizione finanziaria, la **dimensione dei loro ricavi** mondiali è, tuttavia, un ordine di grandezza **inferiore** rispetto all'entità del segmento "Servizi TLC" gestito dalle Telco (si pensi che, attraverso le reti di accesso fisso e mobile dei gestori TLC, Google raggiunge 4 miliardi di clienti distribuiti in tutto il mondo!) e ciò porta all'ultima considerazione.

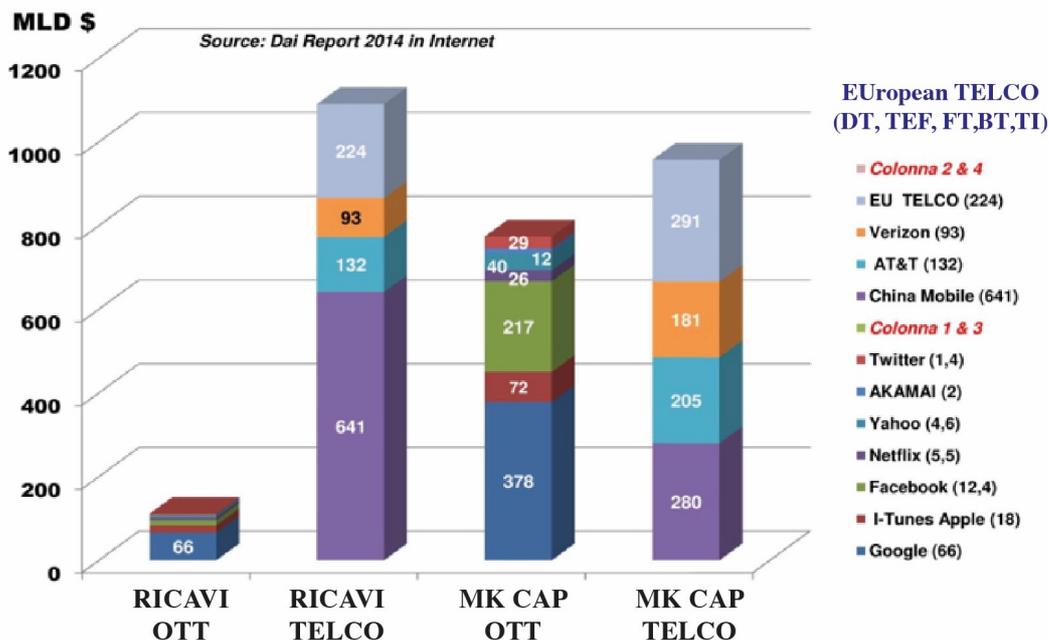


Figura 2
Dati economico-finanziari 2014 dei principali attori OTT/ Telco

D. L'entità e complessità della gestione “fisica” (in particolare per la rete di accesso) non è certo sottovalutata dagli OTT che finora si sono ben guardati dal farsi carico diretto delle reti di accesso⁹. Tuttavia se questo è vero a livello mondiale, il confronto è particolarmente severo nei riguardi delle Telco europee che non sono state in grado di fare evolvere il loro *business* tradizionale, hanno trascurato importanti opportunità e, soprattutto non sono state in grado di costruire una completa offerta di servizi a livello mondiale.

4. Criticità dello scenario: nascita del “Network Paradox” ed i condizionamenti della “Net Neutrality”

I confronti del precedente Paragrafo evidenziano una situazione nel tempo diventata sempre più critica per le Telco europee.

Mentre la remunerazione dei *business* legati ai servizi OTT - grazie ai ricavi dalla pubblicità o direttamente dagli utenti - ha permesso la loro eccezionale affermazione, il *business* legato al trasporto dei pacchetti dati (transiti ed accesso), pur aumentando notevolmente i volumi, ha avuto forti contrazioni di margini sia per effetto della competizione eccessiva che di tariffe *flat* non dipendenti dai volumi di traffico.

In aggiunta i Telco stanno subendo la sfida degli OTT sui modi nuovi di fare servizi TLC (ad es. servizi voce e video con *Skype*, messaggistica con *WhatsApp*, ecc.) che concorre a ridurre sensibilmente alcuni remunerativi mercati tradizionali di nicchia (ad es. gli “sms”).

Si è così verificato il fenomeno che ha preso il nome di “**Network paradox**” (indicato anche come “*Telco Paradox*”) ossia il forte incremento dei volumi di traffico IP associati ad una massiccia riduzione di remunerazione complessiva per i soggetti, quali le Telco europee in diminuzione di ricavi, che sviluppano e gestiscono le reti. Il forte incremento dei costi legati all'entità del traffico rispetto al *trend* dei ricavi ha frenato pertanto gli investimenti sia per la difficoltà di giustificare il loro ritorno sia a causa di una situazione patrimoniale sempre più debole e con flussi finanziari troppo esigui.

Lo spostamento di valore dalle Telco agli OTT si è accompagnato ad una accesa competizione a livello mondiale tra gli stessi OTT per accrescere il proprio *footprint* aumentando sia il numero degli utilizzatori sia la frequenza degli accessi alle applicazioni sui propri *Server Web*. Questo processo ha determinato l'affermazione di pochissimi soggetti Telco che operano a livello sovranazionale - ATT, in particolare, che ha scelto la strada di una fortissima diversificazione di servizi su scala mondiale - dall'altro una crescente necessità di qualità nella connettività IP verso i Clienti finali per supportare i nuovi servizi che richiedono alte velocità a livello applicativo, come si vedrà meglio nel Paragrafo 5 quando si tocca il punto dell'evoluzione delle piattaforme di rete.

Lo stupefacente sviluppo di Internet ha anche reso fondamentali le tematiche relative sia alla “gestione” di Internet sia alla regolamentazione per il suo utilizzo.

⁹ Google ha attivato una propria rete di backbone a livello mondiale ma non sembrerebbe che abbia dato seguito agli annunci di qualche tempo fa di stendere propria fibra ottica nell'area di accesso.

Sino a pochissimi anni fa a nessuno era mai venuto in mente di porre restrizioni allo sviluppo tecnologico ed ai servizi legati ad Internet, né allo sviluppo dei servizi di rete che ne rendono possibile l'utilizzo delle nuove applicazioni con livelli di qualità via via crescenti. In Europa la materia dal 2009 è regolata dal “Regulatory Framework for Electronic Communications” questa normativa riprende principi consolidati, noti come “**Open Internet**”, che hanno guidato la storia di Internet nel Nord America e poi nel resto del mondo (**Figura 3**).

In tempi recenti - quando è apparso chiaro che il trattamento “best effort” del traffico Internet non è sufficiente per i requisiti di qualità nelle nuove Applicazioni - si è assistito a fortissime spinte tese ad impedire lo sviluppo da parte delle Telco di offerte di servizi di trasporto di traffico a qualità differenziata attraverso un'interpretazione forzata del concetto di “**Net Neutrality**”. Si cerca, infatti, di spostare l'attenzione dalla tutela dei diritti delle persone per accedere e scegliere liberamente applicazioni e contenuti a creare vincoli sull'innovazione nelle reti e nei servizi. Lo stato aggiornato del dibattito su tale tematica viene ripreso nel Paragrafo 5.

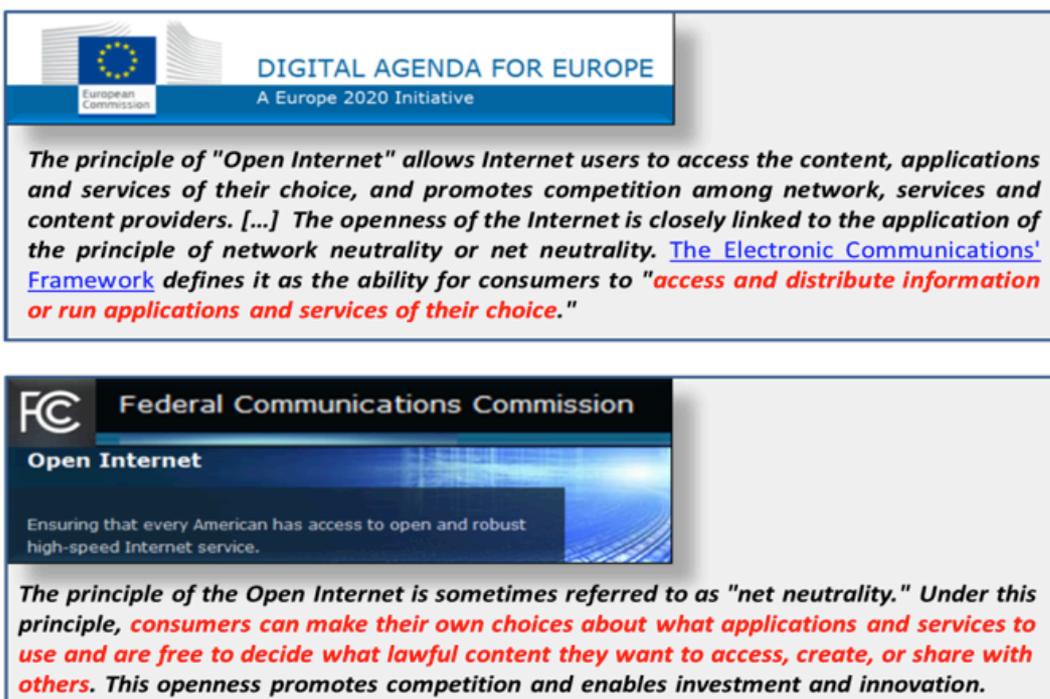


Figura 3
 Due formulazioni di “Open Internet” e di “Net Neutrality” nella “Digital Agenda for Europe” e da parte della FCC americana

5. Come migliorare la stabilità dell’ecosistema ICT

Fra i numerosi fattori di scenario si possono meglio commentare quegli aspetti che si traducono in difficoltà di relazionare il mondo OTT con il mondo Telco e che, se affrontati, possono contribuire a migliorare la stabilità, almeno sul breve-medio termine, dell’ecosistema ICT anche se difficilmente risolutivi sul lungo termine.

Modelli d’interconnessione IP

Come già accennato nel Paragrafo 1 la maggior parte del traffico IP è oggi originato da pochi grandi OTT mondiali (i cosiddetti *HyperGiants*) ed attraversa diversi punti di interconnessione, tra cui quelli con le Telco, prima di giungere ai clienti finali. E’ evidente, pertanto, che le modalità con cui sono realizzate le interconnessioni IP per il traffico del trasporto dati hanno una sensibile importanza sullo sviluppo dell’ecosistema complessivo.

A tale riguardo val la pena ricordare come l’interconnessione per le comunicazioni voce ha avuto da sempre un ruolo fondamentale nello sviluppo dei *business* delle Telco (sia per le comunicazioni “fisse” che “mobili”) mentre per le interconnessioni per comunicazioni dati i Telco hanno fatto l’errore di sottovalutarne la dimensione economica.

In passato, i modelli tradizionali di interconnessione si sono basati, in modalità *best effort*, su accordi di *transito* e “*peering*” (*free* oppure *paid*). La inadeguatezza dei modelli di interconnessione tradizionali, basati storicamente sulla simmetria del traffico, fa emergere la possibilità di affrontare nuovi modelli tra Telco e OTT partendo dalla considerazione che il traffico IP è sempre più caratterizzato non solo dal “volume” ma da un “valore” commerciale che dipende dalla tipologia del traffico, elementi completamente assenti negli attuali modelli di interconnessione.

Il processo di passaggio a nuovi modelli di interconnessione basati sul *delivery* con qualità differenziata è già parzialmente in atto e potrebbe essere accelerato e completato. I nuovi modelli consentono alle Telco/ISP di avere ricavi sia da *end-user*, sia da OTT/CP, in relazione agli specifici benefici che i diversi soggetti ottengono.

I paradigmi per le tariffe di accesso

La competizione tra le Telco è un fenomeno naturale conseguito alla liberalizzazione ed in genere ‘positivo’ (riduzione dei prezzi per i clienti e maggiore efficienza per le Telco) fino a quando, per entrare nel mercato, i *new comers* non offrono servizi di rete sottocosto.

Il fenomeno di una concorrenza troppo spinta tra i Telco è avvenuto, in particolare, in Europa (ed ancor più in Italia) che sta, inspiegabilmente, perseguendo politiche di liberismo eccessivo. Inoltre, ormai a molti anni dalla liberalizzazione, si asseconda un’eccessiva regolamentazione che vincola troppo i *players* TLC ottenendo come risultato la loro capacità d’investimento per margini troppo esigui. Ci si potrebbe infatti chiedere se è giusto che il ruolo della regolamentazione, in ottica esclusivamente di utente, si concentri sulla diminuzione “*sic et simpliciter*” delle tariffe e non piuttosto sia preferibile assumere decisioni regolamentari sulla base di una “*vision*” più allargata che tenga presente

l'intero sistema economico di competenza quali anche i mondi e le strategie degli Operatori e dei Manifatturieri con ritorni alla lunga anche sugli utenti.

Per quanto riguarda le tariffe di accesso, prima che le necessità di banda iniziassero a crescere esponenzialmente, la spinta concorrenziale ha portato a paradigmi **flat** per il traffico dati. Oggi sarà molto difficile od impossibile tornare indietro (a causa delle abitudini del mercato ma anche per possibili interpretazioni della *Net Neutrality*) anche se, nelle reti di accesso, tariffe a “volume”, differenziate nella garanzia del servizio offerto, sarebbero più consone ad un miglior equilibrio di *business* tra gli attori coinvolti.

Evoluzione delle piattaforme di rete

La sfida per le maggiori Telco non si limita all'offerta di bande sempre più larghe nella rete di accesso. La vera sfida, nonostante l'attuale limitata propensione dei Telco agli investimenti, è fare evolvere le reti “tradizionali” di aggregazione e trasporto al fine di permetterne una gestione più avanzata e redditizia.

Più specificatamente va considerato che il traffico IP è ancora essenzialmente trattato in modalità “*best effort*” (con diverse reti e tecnologie in *overlay* in campo da molti anni e spesso superate). E' giunto il momento d'investire per una **rete “All-IP”** altamente flessibile e capace di garantire i **livelli differenziati di qualità** richiesti dalle varie Applicazioni.

La carenza ed i ritardi delle Telco sono state colmati da **nuovi attori globali** OTT che si sono affermati grazie proprio alla loro capacità di fornire il trasporto dei flussi IP con la qualità richiesta dai nuovi servizi. Si tratta degli Operatori CDN (“*Content Delivery Network providers*”), già introdotti nel Paragrafo 2, che hanno conquistato un importante spazio di mercato quando Internet ha cominciato ad essere utilizzata per trasmettere contenuti “pesanti” - quali film, commercio elettronico, distribuzione di cataloghi di prodotti, visitazione di siti di interesse artistico, medico ed altri, ecc. - installando propri apparati (es. *server*, *cache private*) sempre più in prossimità dei clienti finali per ottenere significativi miglioramenti della “**Qualità percepita**”¹⁰ dai clienti.

La stessa esigenza di qualità, a fronte di una eccezionale crescita del traffico, ha spinto aziende di distribuzione di contenuti (come Netflix) a dotarsi di **proprie soluzioni CDN** e Google a realizzare una **propria rete backbone a livello mondiale** per migliorare la qualità del trasporto IP dai propri *Data Center* fino ai punti di interconnessione con gli Operatori di Telecomunicazioni nei diversi Paesi.

Le Telco, se non è troppo tardi, dovrebbero cercare di “recuperare” con investimenti propri quelle soluzioni più strettamente legate alla rete in grado di assicurare i livelli di qualità richiesti ed adeguati ritorni degli investimenti fatti.

Si tratta di realizzare piattaforme *hardware/software* - “al di sopra” del livello di trasporto IP [9] - che consentano di ottenere un sensibile miglioramento della **Qualità percepita** impiegando tecnologie [10] equivalenti a quelle impiegate

¹⁰ Il complesso delle prestazioni serve a migliorare il parametro noto come **QOE (“Quality of Experience”)**. Le prestazioni da curare sono l'**effettiva velocità di trasferimento** delle informazioni (ossia il *Throughput* a livello applicativo) ed il **tempo di scaricamento** (cioè il *Download Time* a livello applicativo). La prima caratteristica dipende dalla *latenza* (ritardo) della rete e dalla perdita di pacchetti nel trasporto; la seconda dall'efficienza del protocollo utilizzato.

dai CDN ma maggiormente integrate con la rete¹¹.

In questa direzione, tuttavia, le Telco trovano difficoltà anche in termini di regolamentazione basate, al solito, su un'interpretazione restrittiva della *Net Neutrality*.

“Open Internet” e regolamentazione

Il passaggio ai nuovi modelli di interconnessione è accompagnato da contenziosi legali/regolatori tra Telco/ISP e OTT, che hanno generato accesi dibattiti, ancora in corso sia in Europa che negli USA, e di cui la “*Net Neutrality*” (vedi Paragrafo 4) è il paradigma.

Negli USA, a fine febbraio 2015 è stato approvato dalla FCC un nuovo testo relativo all'*Open Internet*. Tale regolamentazione appare particolarmente restrittiva a favore degli OTT ed è in linea con la recente presa di posizione del presidente Obama [11].

In tale nuovo testo è riconosciuta l'esigenza di gestire le reti ma **la gestione del traffico** deve essere mirata ad obiettivi di tipo tecnico e non commerciale aumentando i poteri della FCC in relazione alle pratiche di interconnessione.

Le reazioni dell'industria statunitense non sono tardate ad uscire: comunicati stampa della *Broadband Association* e della *Wireless Infrastructure Association* (PCIA) descrivono l'ordinamento FCC come fortemente dannoso per l'innovazione e gli investimenti nel settore TLC e, di conseguenza, per l'intera economia rischiando la conservazione dei posti di lavoro esistenti per non parlare della possibile creazione di nuovi.

Per quanto l'approvazione da parte della FCC costituisca un passo deciso verso regole molto restrittive conseguenti alla *Net Neutrality*, dal punto di vista normativo il confronto sul tema (che ha finito per assumere connotazioni politiche) è ancora in corso e forse un miglior equilibrio è ancora possibile.

In Europa il tema della *Net Neutrality* è analizzato (insieme a quello del *Roaming*) nell'ambito del dibattito in corso al Consiglio UE¹². Una considerazione che può farsi per quanto riguarda le decisioni da prendere da parte del Consiglio è che l'economia americana è oggi *OTT centric* e incentivata dal governo USA per garantire lo sviluppo di questo nuovo settore di mercato (come si può anche notare dalla politica fiscale nei confronti di questi attori, almeno fino ad oggi). Le decisioni europee sulla *Net Neutrality* potrebbero tendere invece a tradursi in un trasferimento di ricchezza dall'Europa verso gli USA, paese in cui, peraltro, la situazione economica delle Telco è notevolmente migliore di quella europea.

Se il complesso dibattito in corso a livello internazionale finisse per far prevalere un'interpretazione “*strong*” della *Net Neutrality*, le reti domestiche delle Telco non potrebbero soddisfare i “*services requirements*” di alcune Applicazioni/Contenuti. Ne conseguirebbe che le Telco sarebbero sfavorite rispetto agli OTT

¹¹ Queste tecnologie adottano paradigmi di **virtualizzazione delle funzioni di rete** denominate NFV (“*Network Function Virtualization*”) e SDN (“*Software Defined Networking*”).

¹² Fra i punti in discussione particolarmente critici appaiono quelli relativi alla possibilità di utilizzo, da parte dei Telco, del *traffic management* e delle soluzioni per il miglioramento della *Quality of Experience*, (definita in Nota 10) e sulla fornitura di servizi con specifici livelli di qualità verso end-users e verso OTT.

avendo limitazioni alle possibilità di un loro recupero di profittabilità economica: difficilmente, come conseguenza, potrebbero avere le risorse da dedicare agli investimenti necessari per diffondere capillarmente la banda larga ed ultralarga con limitazioni allo stesso sviluppo degli OTT.

Si pensi che, nella sola Europa, la differenza fra gli investimenti necessari per raggiungere gli obiettivi di diffusione della banda larga/ultralarga e gli investimenti che, nelle attuali condizioni di mercato e di regolamentazione, possono effettivamente essere sostenuti è stata stimata, per la sola Europa, fra i 110 ed i 170 Miliardi di Euro [12]!

6. Conclusioni ed il possibile ruolo di “Internet of Things”

L'articolo ha cercato innanzitutto di ripercorrere le fasi fondamentali che hanno guidato le grandi evoluzioni nell'ecosistema ICT negli ultimi due decenni che si possono così riassumere:

- il Web 2.0 ha consentito di fornire ‘servizi’ (*streaming video, gaming, cloud, ecc.*) profondamente diversi dai servizi *e-mail* e *file transfer* che hanno caratterizzato la prima fase di Internet ed ha posto le basi per la nascita e l'avvio degli OTT;
- i *Providers* OTT hanno realizzato nuovi tipi di servizi a basso costo, con fantasia e dinamicità, raggiungendo un'utenza *worldwide* senza le limitazioni di mercato degli operatori Telco sviluppatasi, essenzialmente, sulle loro reti nazionali;
- le Telco, in particolare europee, hanno dimostrato incapacità ad entrare nei nuovi *business* dei servizi per limitazioni culturali e dimensioni troppo nazionali;
- una classe di *provider* OTT ha sfruttato le stesse reti Telco per il trasporto di servizi - quali voce, videotelefonata e messaggistica - in diretta competizione con il loro *core business*;
- altri *player*, sempre definibili come OTT “puri”, sono nati operando in *hardware* ai bordi della rete di trasporto con apparati/sistemi aggiuntivi (“*Content Delivery Network*”) che forniscono agli utenti le prestazioni di qualità richieste dai servizi più avanzati.

A partire dal precedente scenario si sono messe in luce le **principali singolarità** che ne sono derivate per i *players* in gioco nell'ecosistema ICT:

- per le Telco il cosiddetto “**Network Paradox**”, ossia minori margini all'aumentare del traffico, scoraggiando le motivazioni per i nuovi investimenti necessari;
- per i *Big OTT*, nonostante le loro estensioni oligopolistiche a livello mondiale, le dimensioni ancora insufficienti per **farsi carico della rete** mondiale (in particolare delle reti di accesso) delle molte Telco distribuite in tante nazioni;
- per le Istituzioni l'attitudine - rincorrendo discutibili interpretazioni dei **principi della Net Neutrality** - a disincentivare nuovi investimenti nel campo delle reti.

Nella parte finale dell'articolo si accenna ad alcune **linee possibili per attenuare le precedenti criticità** attraverso un miglior bilanciamento nelle relazioni OTT-Telco al fine di garantire la stabilità dell'ecosistema ICT attraverso:

- un'ideale evoluzione dei modelli d'interconnessione IP e delle relative tariffe;
- la possibile revisione dei paradigmi tariffari e qualitativi per le reti di accesso;
- uno sforzo d'investimento delle Telco nell'evolvere verso una rete "All IP";
- una maggior attenzione e cautela delle Istituzioni, specie europee, nella regolamentazione per "Open Internet".

Al momento attuale è difficile prevedere se le misure sopra accennate potranno realizzarsi. In ogni caso sono probabilmente troppo segmentate - anche se utili per un transitorio - ed occorre sperare che in modo naturale, e non forzato, si trovi un miglior equilibrio di lungo periodo dell'ecosistema attraverso la sua stessa evoluzione.

Indipendentemente dal destino di ciascuno degli attuali attori è quasi certo che ci si possa attendere un nuovo assetto legato allo sviluppo dell'IoT ("Internet of Things") in cui il modo d'impiego e l'uso delle "cose" sarà molto più importante del loro possesso.

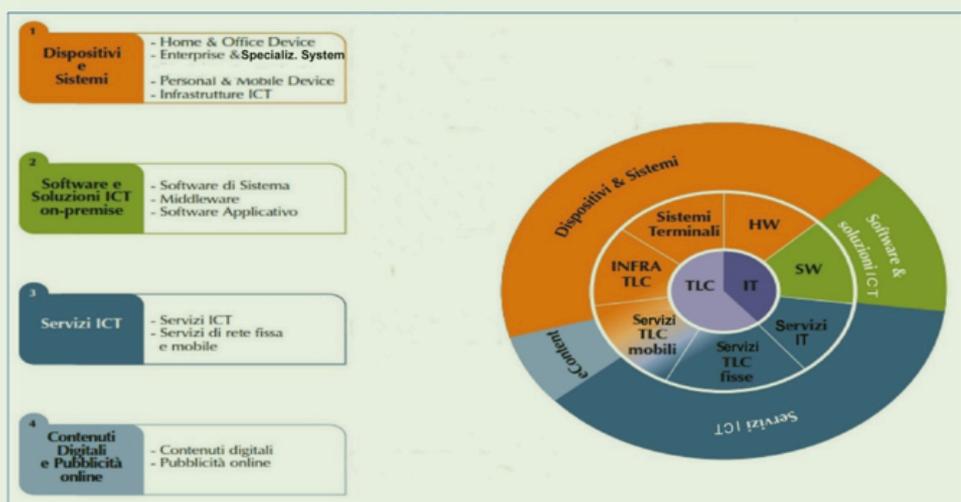
La possibilità, infatti, di mettere "a bordo" di qualunque manufatto una certa quantità d'intelligenza per contribuire al monitoraggio delle prestazioni si sta sempre più estendendo ad un mercato di grandi dimensioni con infinite possibilità di applicazioni (*home automation*, sistemi di sicurezza evoluti, logistica dei magazzini in *real-time*, mezzi mobili "always connected", ecc.) aprendo un mondo di servizi legati a queste applicazioni.

Tutti questi sistemi genereranno una grandissima quantità di dati che dovranno essere in grado di dialogare, attraverso le reti di comunicazioni fisse e mobili, con *Data Center* in cui le informazioni saranno elaborate per generare le informazioni di ritorno.

In questo quadro con interazioni tra telecomunicazioni, logistica ed energia, ci si attende un nuovo forte cambiamento di scenario con la necessità per gli attuali attori di fare evolvere velocemente il loro *business*. Nasceranno così nuovi ecosistemi che porteranno al superamento dei modelli tradizionali e che dovrebbero spingere gli Operatori di telecomunicazioni a trovare alleati a tempi brevi per realizzare tali servizi innovativi. Diversamente, ancora una volta, saranno altri attori ad occupare gli spazi d'innovazione poiché gli spazi attuali diventeranno sempre meno significativi.

RIQUADRO - Classificazione dei segmenti del "Global Digital Market" nell'ecosistema ICT

Facendo riferimento al Rapporto Assinform-Netconsult che ogni anno presenta le evoluzioni di mercato dell'ecosistema ICT, la nuova classificazione (iniziata nel 2012) considera i quattro grandi segmenti indicati in **Figura A1**. Ai tradizionali tre segmenti del mercato ICT viene aggiunto il nuovo segmento dei "Contenuti digitali e pubblicità on-line" mentre per i rimanenti tre segmenti sono stati aggiunti vari sottosegmenti (importanti per individuare i contributi dati al mercato ICT dai nuovi business).

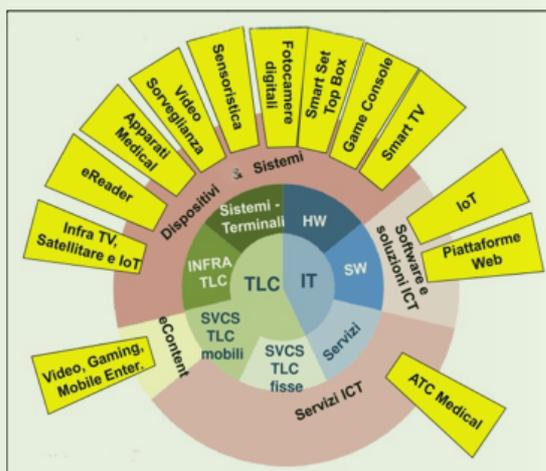


Fonte: Rapporto Assinform-Net Consult 2012

Figura A1 - Classificazione dei segmenti del Global Digital Market

Ci si riferisce, in particolare, al segmento "Dispositivi & Sistemi" che ha aggiunto ai sottosegmenti tradizionali (**Infrastrutture TLC, Infrastrutture IT e Terminalistica**) la **Nuova Terminalistica** (Smart TV, Game console, Smart box, Digital camera, altri dispositivi,) come indicato in Fig.A2.

Inoltre, nell'ambito dei "Servizi ICT", sono stati meglio definiti e differenziati i "Servizi ICT propriamente detti" (quali Outsourcing, System integration, Data Center e Cloud, Consulenza e Assistenza tecnica) ed i "Servizi di Rete". Infine nel tradizionale segmento "Software & Soluzioni ICT" si è aggiunto il nuovo campo di Internet of Things (IOT) e delle Piattaforme Web che confluiscono a formare il segmento "Software & soluzioni ICT".



Fonte: Rapporto Assinform-Net Consult 2012

Figura A2 - Nuovi sottosegmenti reti fissa e mobile)

Bibliografia

- [1] Vannucchi G., *Cinquant'anni di telecomunicazioni digitali ed uno sguardo al futuro: la convergenza Informatica - telecomunicazioni e le nuove architetture di rete fissa - Storia delle Telecomunicazioni*, Firenze “University Press”, 2011, pg. 809-848
- [2] IBM Global Business Services, *Telco 2015: Five telling years, four future scenarios - Executive Report*, 2010
- [3] Ericsson AB, *Ericsson Mobility Report - Interim Report*, August 2013
- [4] Cisco, *Visual Networking Index Forecast and Methodology 2013–2018 - WhitePaper*, June 2014
- [5] Akamai, *State of the Internet*, Q1.2014, Vol7 - Report, 2014 e Q4.2014, 2015
- [6] Sandvine, *Global Internet Phenomena - Report*, 2014
- [7] Telco 2.0 Research, *Your Text is on Fire: OTT's to burn 40% SMS revenue - Report*, Nov. 2011 Communications Magazine, Nov 2013, pp. 24-31
- [8] Patuano M. *Il confronto tra le Telco e gli OTT*, Harvard Business Review, November. 2011
- [9] Bagnasco E. M., Ciccarella G., *Verso la Rete dei Contenuti - Notiziario Tecnico Telecom Italian 2014*, n.2.
- [10] Raj Jain and Subharthi Paul, *Network Virtualization and Software Defined Networking for Cloud Computing - A Survey*, IEEE
- [11] The Washington Post, *Obama to the FCC*, November 2014
- [12] Boston Consulting Group, *Reforming Europe's Telecoms Regulation to Enable the Digital Single Market*, 2013

Ringraziamenti

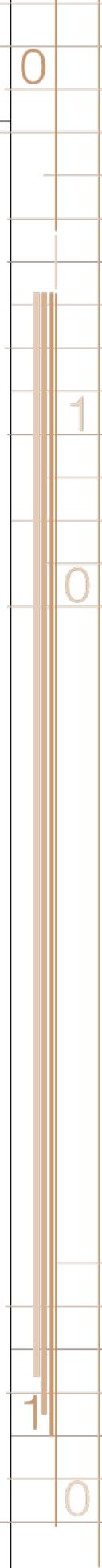
L'Autore desidera particolarmente ringraziare l'ing. Gianfranco Ciccarella per i vari contributi forniti e per le appassionante discussioni a riguardo. Desidera inoltre ringraziare l'ing. Giuseppe Stacchiotti ed il dr. Giuseppe Biassoni per la rilettura critica del testo ognuno con la visione portata dalla rispettiva esperienza professionale. Un ringraziamento infine all'ing. Umberto De Julio che, con le sue molteplici esperienze professionali, ha fornito alcune importanti osservazioni.

Biografia

Guido Vannucchi, laurea in Ingegneria Industriale all'Università di Bologna nel 1958, “Master Science EE” alla Stanford University nel 1963, Libera Docenza in Comunicazioni Elettriche nel 1971. Direttore Generale Telettra dal 1983 al 1990, “Senior Consultant” di Italtel e di Olivetti Telemidia, Direttore Tecnico e quindi Vice Direttore Generale della RAI dal 1993 al 1998, Consigliere Agenzia Spaziale Italiana nel 2008 e Presidente OTA (organismo AGCOM) dal 2009 al 2012. Membro del Consiglio Superiore delle TLC dal 1990 al 2008 e Presidente Associazione AICT.

Docente al Politecnico di Milano dal 1990 al 2013 in vari corsi. Laurea “*ad honorem*” in Ingegneria delle Telecomunicazioni conferita dall'Università di Padova nel 1998 per i contributi scientifici e manageriali nel campo della trasmissione dei segnali.

E-mail:guido.vannucchi@fastwebnet.it



La crittologia da arte a scienza: l'eredità di Shannon e Turing

Angelo Luvison

Sommario

Gli epocali contributi, sia teorici che pratici, di Claude Shannon – padre della teoria dell'informazione e della segretezza – e di Alan Turing – primo artefice della decrittazione dei messaggi della macchina Enigma – hanno trasformato la crittologia (crittografia + crittanalisi) da pratica artigianale a scienza rigorosa. Poiché le minacce alla sicurezza nel cyberspazio diventano sempre più subdole e tecnologicamente maliziose, la crittografia – oggi contemporaneamente arte e scienza – continuerà a svolgere un ruolo di protezione indispensabile nella sicurezza dei servizi informatici.

Abstract

The seminal contributions, both theoretical and practical, of Claude Shannon – father of the theory of information and secrecy – and Alan Turing – principal codebreaker of the Enigma machine – changed cryptology (cryptography + cryptanalysis) from a mainly hand-crafted work to a mathematical science. As security threats in cyberspace become more and more malicious and technologically smart, cryptography – being at the same time an art and a science – will play an increasing role to cope with high-level trust in digital service security.

Keywords: Milestones in cryptology, Shannon and Turing cryptologists, Enigma breaking, Cybersecurity



1. Introduzione

Strumento tecnico-scientifico fondamentale per la cybersicurezza è la crittologia – dal greco *kryptós* (“nascosto”) e *logos* (“parola”) – scienza che comprende due branche: la crittografia e la crittanalisi [1]. La prima propone nuovi metodi e algoritmi tanto per proteggere i dati e l’informazione quanto per garantire l’autenticità di un messaggio o la sua integrità; mentre la crittanalisi escogita metodi per forzare, illecitamente o a scopo di prova, uno schema cifrato. In realtà, con crittografia molti studiosi intendono sia la crittografia in senso stretto sia la crittanalisi. Il termine crittanalista è entrato nell’uso comune dopo la Seconda guerra mondiale, nel corso della quale la locuzione impiegata dagli anglo-americani era *codebraker* per indicare il solutore non autorizzato di codici cifrati (l’equivalente in italiano era “decrittatore”).

Tuttavia, la crittografia non studia solo la segretezza dell’informazione ma si occupa egualmente dell’autenticità. I due obiettivi speculari, “segretezza” e “autenticità”, spesso, non sono facili da distinguere. Solo recentemente i crittografi ne hanno apprezzato pienamente la differenza, caratterizzabile in questo modo sintetico: una tecnica fornisce “segretezza” se determina chi può “ricevere” il messaggio, fornisce “autenticità” se determina chi “ha inviato” il messaggio.

Il problema della cybersicurezza ha recentemente avuto un revival sotto il profilo sia economico (sicurezza del business) sia della responsabilità etica. Il primo aspetto, in realtà, ha sempre costituito un punto di attenzione per le aziende; il secondo, peraltro, è tornato in auge a causa di parecchie iniziative, non propriamente commendevoli dal punto di vista etico, del governo statunitense, perciò aspramente criticate da molti Paesi.

Oggi, “La crittografia è una questione di diritti umani”, così il fondatore di Wikipedia, Jimmy Wales, ha commentato su Twitter l’annuncio che l’enciclopedia libera adotterà nel prossimo futuro il protocollo HTTPS – quello, per intenderci, usato dai sistemi di transazioni finanziarie e bancarie – per cifrare le comunicazioni da e per i server, rendendo teoricamente impossibile monitorare le abitudini di lettura degli utenti.

Il contrasto tra valori politici e valori etico-sociali non è certamente nuovo. Un gustoso episodio riguarda il Cypher Bureau statunitense, più noto come Black Chamber, che negli Anni Venti del secolo scorso fu l’ente di Signals Intelligence (SIGINT), precursore dell’attuale National Security Agency (NSA). Fondato subito dopo la prima guerra mondiale dal crittanalista Herbert Yardley, questo organismo venne chiuso nel 1929 da Henry Stimson, Segretario di Stato sotto il Presidente Edgar Hoover. L’aneddoto racconta che Stimson si fosse infuriato per la vanteria di Yardley di poter decrittare tutti i cablogrammi diplomatici, compresi quelli del Vaticano. Successivamente, nelle memorie, egli riassunse il suo punto di vista sulla crittografia con frase già allora demodé: “I gentiluomini non leggono la posta l’uno dell’altro” [2]. Questo modo garbato, quasi cavalleresco, corrispondeva ad accettare di buon grado la crittografia tanto nel settore governativo quanto in quello privato, mentre la prassi della crittanalisi era molto meno apprezzata. Il mondo di oggi, più scaltrito, guarda alla crittanalisi come a

un'attività politicamente corretta e prudentiale in ambito governativo, ma vicina allo spionaggio industriale nel privato. In questo secondo caso, essa può, tuttavia, svolgere un ruolo etico oltre che pratico: un crittanalista "amico" è certamente di ausilio per identificare impreviste debolezze di un sistema cifrante, che potrà essere ritirato dal servizio o adeguatamente re-ingegnerizzato.

L'attenzione alla cybersicurezza, o sicurezza nel cyberspazio, è oggi rivolta soprattutto alla difesa dei tradizionali sistemi informatici: PC, server, banche dati, software. Ma, per il continuo sviluppo delle nuove tecnologie – quali il cloud computing e le reti virtuali, l'Internet of Things (IoT) e l'Internet of Everything (IoE), i big data – occorre che la cybersicurezza sia costantemente perseguita e ampliata.

Stante la dipendenza della società da Internet e dalle comunicazioni, il cybercrimine è un problema globale di rilevanza crescente. Diversi studi e analisi valutano il suo costo annuale in circa mille miliardi di dollari: questo dato tiene conto del tempo perduto, delle occasioni mancate negli affari, dei costi per risolvere i problemi tecnici, del danno d'immagine. In parecchi settori dell'economia, si considera molto grave il problema della cybersicurezza e i continui cyberattacchi rafforzano per le imprese più accorte la necessità tanto di maggiori risorse dedicate alla ricerca sulla sicurezza quanto della formazione di figure professionali adeguate. Ogni volta che si usa una carta di credito, si accede a un conto bancario online o si invia un'email, gli algoritmi di cifratura lavorano dietro la scena: quindi, per assicurare la sicurezza dei dati e dell'informazione, nel cloud o nei server di rete, la crittografia svolge un ruolo fondamentale.

Poiché i computer diventano sempre più potenti, la velocità di comunicazione aumenta e la memoria dei dati cresce, i metodi attuali per proteggere l'informazione vengono minacciati o posti sotto attacco da malintenzionati. Per esempio, la capacità dei futuri sistemi di crittografia dovrà superare quella del pur valido Advanced Encryption Standard (AES) adottato dal governo USA nel 2001 per proteggere informazioni "classificate". I crittografi hanno, infatti, tre problemi principali da affrontare: oltre al costo e alla velocità, la sicurezza di lungo periodo.

In questo scenario, possiamo considerare, anche se in modo un po' schematico, Claude Shannon e Alan Turing i padri fondatori, rispettivamente, della crittografia e della crittanalisi contemporanee, per il loro ruolo di attori principali in eventi che hanno permesso l'evoluzione della crittologia da arte a scienza rigorosa, ma pur sempre creativa.

Il contributo di Shannon alla crittografia è la pubblicazione, nel 1949, di un solo ma fondamentale articolo, nel quale approfondisce concetti come "sicurezza teorica" e "pratica", "confusione" e "diffusione", che saranno incorporati in sistemi di cifratura standard.

L'apporto centrale di Turing come solutore di cifrari durante la Seconda guerra mondiale al quartier generale del Government Code and Cypher School (GC&CS) a Bletchley Park, località vicina a Londra, è stato la decrittazione di

Enigma, la formidabile macchina cifrante tedesca. Per decenni i lavori di decrittazione delle comunicazioni dell'Asse da parte di Turing sono stati vincolati al segreto di stato: questa è, quindi, un'occasione per riesaminarne il contributo alla nascita della crittanalisi contemporanea.

Nel 1943, Shannon e Turing ebbero modo di incontrarsi sistematicamente alla mensa dei Bell Telephone Laboratories (BTL) dell'AT&T (American Telephone and Telegraph Corporation), ma – situazione davvero paradossale – non furono autorizzati a scambiarsi informazioni sui rispettivi lavori di intelligence, allora ritenuti assolutamente segreti per la sicurezza dei propri Paesi.

È giusto ricordare anche l'apporto italiano a questa importate disciplina. Infatti, la scienza dei codici e dei linguaggi segreti ha avuto fin dal passato eminenti cultori italiani, fra cui Leon Battista Alberti, Girolamo Cardano e Giovanni Battista della Porta. Ma anche più di recente il nostro Paese ha fornito contributi validi e significativi. Basti pensare al *Manuale di crittografia* (figura 1) del generale Luigi Sacco [3], pubblicato in quattro edizioni (l'ultima del 2014 è stata aggiornata da Paolo Bonavoglia, nipote di Sacco) e considerato da David Kahn nell'*opus magnum* [1]¹ il migliore testo pubblicato – cioè non classificato – di crittografia classica (fino alla metà del Novecento). Il successo del *Manuale* fu notevole tant'è che nel 1941 sarebbe stato tradotto in inglese con il titolo *Manual of Cryptography* e nel 1951 in francese (*Manuel de cryptographie*). Anche in [4], Kahn ha parole di grande stima e rispetto per Sacco, che, dopo la battaglia di Caporetto della Prima guerra mondiale, riuscì a convincere gli alti comandi italiani ad abbandonare i vecchi cifrari, facilmente decrittati dagli austriaci [6], e di adottare nuovi sistemi fino allora rifiutati perché troppo complicati.

Il focus di questo lavoro è principalmente sui contributi di Shannon (paragrafo 3) e Turing (paragrafo 4) alla crittologia come disciplina scientifica. Nel seguito, si ripercorrono alcuni passaggi di fondamentale importanza prima di loro (nel paragrafo 2). Completano la rassegna le conclusioni nel paragrafo 5 e tre



Figura 1
Frontespizio della terza edizione (1947) del Manuale di crittografia di Luigi Sacco.

¹ The Codebreakers [1] è l'opera indispensabile per chiunque desideri penetrare i misteri della crittologia in una prospettiva storica. Tutti i successivi lavori di Kahn sono storicamente pregevoli e raccomandabili, in particolare [4]-[6]. Utile è il volume panoramico [7], purtroppo non esente da pecche o imprecisioni storiche e tecniche. Aggiornatissimo è il recente [8]. Un'encomiabile sintesi dell'intera disciplina si trova in [9], un saggio insolitamente penetrante per una voce enciclopedica (online).

riquadri (curiosità e aneddoti; Shannon e Turing si incontrano ai BTL; misure dell'informazione e delle probabilità) di approfondimento su aspetti particolari appena menzionati nel testo.

La pur estesa bibliografia include solo una modesta parte della sempre più vasta documentazione disponibile in letteratura (o sul Web). Si ritiene, tuttavia, che essa possa risultare già abbastanza orientativa per il lettore desideroso di approfondire uno o più argomenti non sufficientemente dettagliati nel testo. Oggi la crittologia è una disciplina tecnico-scientifica matematicamente fondata e per il suo studio sono in circolazione molti validi manuali universitari, fra i quali gli eccellenti [10]-[13].

Il lessico della disciplina, non sempre uniforme nei lavori tanto scritti direttamente quanto tradotti in italiano, appare spesso ambiguo e incoerente (anche in Wikipedia). Perciò, per assicurare una terminologia con la precisione e la coerenza necessarie in un lavoro di rassegna su una rivista scientifica, si seguirà, con qualche modesto adattamento, quella impiegata in [13], uno dei migliori manuali universitari in italiano su teoria dell'informazione, codici, cifrari. In particolare, è opportuno prestare attenzione a uno dei cosiddetti *false friend* della lingua inglese: *decryption* non corrisponde a "decrittazione"; infatti, *to decrypt* significa decifrare – legittimamente poiché si conosce la chiave – il messaggio cifrato. È quindi, in senso stretto, un *false friend* giacché l'operazione di decrittazione – in italiano – è un'operazione di crittanalisi, cioè di recupero del messaggio originale in chiaro senza possedere la chiave, perciò sostanzialmente non autorizzato. Per questa ragione, la complessità computazionale del processo di decrittazione dovrebbe essere, almeno in linea di principio, significativamente maggiore di quella di decifrazione.

2. I precursori: due pietre miliari

In questo paragrafo si descrivono due importanti eventi – di rilevanza tanto tecnica quanto storica – che hanno caratterizzato le tecniche crittografiche nel passaggio dalla fase classica alla contemporaneità: il principio di Kerckhoffs [14] e il cifrario di Vernam [15].

2.1 Il principio di Kerckhoffs

L'olandese Auguste Kerckhoffs in un articolo in due parti del 1883, *La cryptographie militaire* [14], enunciò una legge generale per i messaggi cifrati: "La sicurezza di un crittosistema dipende solo dalla capacità di tenerne celata la chiave". In base a questo principio, si dà per scontato che il "nemico" sia a conoscenza delle caratteristiche del cifrario o, per dirla in altri termini, che sia a conoscenza dell'algoritmo di cifratura.

Tuttavia, in molte applicazioni crittografiche, tradizionalmente in quelle militari e diplomatiche, il crittografo tende (o, piuttosto, tendeva) a difendere strenuamente la segretezza di tale algoritmo. Potrebbe sembrare, infatti, che il principio di Kerckhoffs sia controintuitivo, e che un progetto, di cui siano mantenute nascoste le specifiche, porti a un sistema intrinsecamente più sicuro: questa è l'idea della "sicurezza mediante oscurità".

Kerckhoff non sarebbe stato contrario all'oscurità di per sé, ma avrebbe ammonito il crittografo a non farvi troppo affidamento. L'esperienza e la storia militare hanno ripetutamente dimostrato che sistemi di questo tipo risultano troppo spesso deboli e che possono essere facilmente forzati non appena il progetto segreto sia stato abilmente "retroingegnerizzato", oppure carpito con altri mezzi più o meno leciti². Un esempio: il Content Scrambling System (CSS) per la protezione del contenuto dei DVD è stato facilmente forzato dopo essere stato opportunamente retroingegnerizzato. Ecco perché uno schema crittografico deve rimanere sicuro anche nel caso in cui la sua completa descrizione sia disponibile a un opponente e perché risulta rischioso affidarsi alla speranza di salvaguardare il progetto della propria cifratura da intrusioni non autorizzate. Come vedremo nel paragrafo 4, anche l'opera di forzatura di Enigma può essere interpretata come un'azione di retroingegnerizzazione.

Il principio di Kerckhoff sarebbe stato riformulato decenni dopo (o, forse, formulato indipendentemente) da Shannon secondo l'enunciato: "Il nemico conosce il sistema", ossia, "Un sistema (di sicurezza) dovrebbe essere progettato assumendo che l'opponente sia in grado di acquisire rapidamente completa familiarità con esso". L'aurea massima di Shannon è oggi condivisa da tutti gli esperti di crittografia.

2.2 Il cifrario a blocco monouso (*one-time pad*) di Vernam

Nel 1926, Gilbert Vernam – ingegnere all'AT&T – pubblicò [15] un importante cifrario da usare con il classico codice Baudot sviluppato nel 1847 e successivamente impiegato nelle telescriventi. L'idea innovativa proposta da Vernam era di utilizzare la chiave una e una sola volta, cioè di cifrare ciascun bit del testo con un bit della chiave scelto in modo completamente casuale. Vernam riteneva – a ragione, sia pur senza dimostrarlo rigorosamente³ – che il cifrario fosse resistente, cioè inviolabile (*unbreakable*), ed era pure consapevole che non sarebbe stato così se i bit della chiave fossero stati successivamente riutilizzati. Vernam nello stesso articolo [15] riferì di prove in campo, condotte dall'U.S. Army Signal Corps, che avrebbero provato l'inviolabilità del cifrario, un obiettivo, peraltro, che nessuna sperimentazione, per quanto estesa, può garantire con certezza assoluta. Il motivo per definire "prescientifica" la crittologia del periodo prima della Seconda guerra mondiale è che fino allora si procedeva per intuizioni e convinzioni non suffragate da dimostrazioni valide. Non fu che allo scoppio di questa guerra che la comunità crittologica comprese appieno il contributo che matematici e ingegneri – fra i quali Shannon e Turing – avrebbero potuto fornire in materia.

Anche se l'articolo è del 1926, già nel 1918 Vernam aveva costruito una macchina elettromeccanica – brevettata l'anno successivo – che automaticamente cifrava le comunicazioni effettuate con telescrivente. Il testo in chiaro alimentava il dispositivo con un nastro di carta, mentre un secondo nastro

² "By hook or by crook" è l'icastica frase idiomatica in inglese.

³ Anche se Vernam era nel giusto, la storia della crittografia è costellata di inventori che erroneamente credono e dichiarano che i loro cifrari siano inviolabili.

in input forniva la chiave. Per la prima volta cifratura e trasmissione venivano automatizzate nello stesso apparato.

Il sistema crittografico di Vernam, oggi è più conosciuto con il nome di *one-time pad*, o blocco monouso, dalla modalità di utilizzazione da parte dello spionaggio internazionale prima, durante e dopo la Seconda guerra mondiale. Gli agenti segreti erano dotati di un blocco di carta contenente la chiave segreta, scelta casualmente e da utilizzare una e una sola volta, cioè monouso. Conseguenza molto importante di questo schema – ed è la ragione per cui la sua ideazione costituisce tuttora una pietra miliare in crittografia – è che fornisce l'unico tipo di crittosistema incondizionatamente sicuro. Ciò sarà, tuttavia, provato quasi trent'anni dopo da un altro ricercatore dell'AT&T: Claude Shannon.

Per completezza di informazione, si può aggiungere che Joseph Mauborgne (U.S. Army Signal Corps) è generalmente considerato co-inventore di Vernam del one-time pad, mentre si è ultimamente accertato [16] che il bancario Frank Miller è stato precursore di entrambi, avendo pubblicato nel 1882 la monografia *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*, in cui già allora proponeva l'uso di questo sistema di cifratura per il servizio telegrafico. Indubbiamente però, la sua prima realizzazione concreta va attribuita a Vernam.

3. Terza pietra miliare: l'articolo di Shannon

Esiste una ormai sterminata aneddotica sull'abitudine di Shannon di lavorare (o giocare) allo stesso tempo con problemi di tipo diverso (figura 2). Oltre a scrivere articoli fondamentali di teoria dell'informazione, Shannon – sempre curioso degli argomenti più eterogenei – ha dato inizio all'era della progettazione dei circuiti logici con la sua tesi di master discussa nel 1937, ha studiato la composizione ottimale di portafogli azionari (si veda, per esempio, [17]), ha coltivato un interesse durevole per le macchine che giocano a scacchi, ai BTL, al MIT, nel garage di casa propria. Tutti i suoi lavori principali sono reperibili in un unico volume pubblicato dall'IEEE Press [18].



Figura 2
Shannon gioca con il suo topo elettromeccanico

Shannon raggiunse i BTL nel 1941 per lavorare nel settore crittografico: i suoi contributi teorici sarebbero stati basilari per sviluppare il sistema SIGSALY del Progetto X, l'imponente apparato di scrambling vocale che avrebbe permesso a Churchill e Roosevelt di parlare da una stanzetta speciale mediante un sistema di codifica vocale d'avanguardia ancora oggi (cfr. § 4 e riquadro 2).

Con la pubblicazione, qualche anno dopo nell'ottobre 1949, del suo fondamentale articolo "Communication theory of secrecy systems" [19] ha definito i principi teorici delle comunicazioni segrete, inaugurando l'era della crittografia scientifica a chiave segreta⁴.

Come anticipato, la versione di Shannon del principio di Kerckhoffs è nella forma "il nemico conosce il sistema". In altri termini, Shannon ipotizza implicitamente che "ogni aspetto progettuale del processo di cifratura sia noto al crittanalista opponente, tranne ovviamente i valori correnti, per esempio, del testo in chiaro e della chiave segreta del messaggio istanziato". In particolare, l'algoritmo di cifratura stesso *non* è segreto.

In una nota a piè di pagina, l'autore avverte che il contenuto dell'articolo [19] era già apparso nel 1945 come un memorandum confidenziale BTL, poi reso pubblico (*declassified*). L'articolo incomincia con la proposizione: "I problemi della crittografia e dei sistemi segreti forniscono un'interessante applicazione della teoria delle comunicazioni"; le comunicazioni segrete, indubbiamente, ne costituiscono l'intento principale.

Anche il titolo è di per sé molto significativo. Gli obiettivi delle tecniche crittografiche sono due: la segretezza e l'autenticazione. Shannon chiarisce che sta considerando solo la segretezza e precisa che vi sono due tipi di sistemi per la segretezza: quelli progettati in difesa da un attaccante ostile in possesso di risorse computazionali illimitate e quelli progettati per proteggersi da un attaccante con capacità computazionale finita. Shannon definisce la prima "segretezza teorica" e la seconda "segretezza pratica" – questi termini sono stati sostituiti nell'uso attuale da "sicurezza incondizionata" (o, talvolta, "sicurezza teorica dell'informazione") e "sicurezza computazionale"; il senso, peraltro, non cambia.

3.1 Sicurezza teorica o pratica

La discussione di Shannon sulla segretezza teorica è concettualmente molto ricca. Shannon fornisce per la prima volta la definizione di *unbreakability* (inviolabilità o inattaccabilità) di un cifrario, dimostrando che lo schema di Vernam, il cifrario a blocco monouso, garantisce la "segretezza perfetta" – termine usato per denotare l'inviolabilità.

Più precisamente, Shannon dimostra che la segretezza perfetta richiede una chiave segreta la cui lunghezza in cifre binarie sia almeno pari al numero di bit di informazione del messaggio cifrato. Diventa con ciò chiaro che la sicurezza pratica è quanto di meglio si possa sperare in situazioni reali dove la chiave segreta è relativamente breve.

Benché i vari circoli di esperti ritenessero da tempo che questo schema di cifratura non potesse essere forzato, fu probabilmente Shannon a pubblicare per primo una conferma teoricamente convincente della congettura ipotizzata. La dimostrazione è molto semplice perché si basa unicamente sull'indipendenza statistica della somma modulo due $c = m \oplus k$ di due processi casuali tempo-discreti statisticamente indipendenti: c è il messaggio cifrato, i

⁴ Questa parte attinge principalmente dall'ottimo saggio [20] di James Massey.

due processi m e k sono, rispettivamente, il messaggio originale in chiaro m e la chiave k .

È da notare che il blocco monouso assicura la segretezza perfetta, non importa quale sia la statistica del testo in chiaro. Proprietà questa molto importante perché non è desiderabile che il sistema di cifratura dipenda dalla statistica della sorgente dei messaggi. Ma il fatto che si richieda un bit di chiave segreta per ogni bit in chiaro rende il sistema poco utilizzabile in pratica – tranne nelle applicazioni dove l'esigenza di segretezza fa premio sul costo e la lunghezza del testo in chiaro è piuttosto limitata: viene subito in mente la “linea calda” tra i capi di stato di Paesi alleati.

3.2 Confusione e diffusione

Secondo Shannon vi sono due operazioni primarie con le quali si possono costruire algoritmi di cifratura robusti e resistenti agli attacchi:

1. **Confusione** è un'operazione di cifratura dove la relazione tra chiave e crittogramma è resa oscura. Un mezzo oggi comunemente impiegato per ottenere confusione è la sostituzione dei bit.
2. **Diffusione** è un'operazione di cifratura dove l'influenza di un solo simbolo del testo in chiaro è spalmata su molti simboli del testo cifrato con l'obiettivo di nascondere le proprietà statistiche del testo in chiaro. Un semplice elemento di diffusione è la permutazione dei bit.

Cifrari che realizzano solo confusione – un esempio è la macchina cifrante tedesca Enigma impiegata durante la Seconda guerra mondiale – non sono sicuri. Né lo sono cifrari basati esclusivamente sulla diffusione. Tuttavia, concatenando le due operazioni, si può costruire un sistema robusto: siamo ancora debitori a Shannon per l'idea di questo artificio. Tecniche di progettazione di sistemi cifranti, che ripetono sui dati le operazioni di “confusione” e “diffusione”, sono oggi utilizzate in tutti gli algoritmi di crittografia a blocchi⁵, quali il Data Encryption Standard (DES) e le sue alternative più recenti: il Triple DES (basato sulla ripetizione del DES per tre volte) e l'Advanced Encryption Standard (AES) [11], 12].

Le cifrature a blocchi moderne posseggono eccellenti proprietà di diffusione, questo significa rendere il testo cifrato (quasi) statisticamente indipendente dall'originale: requisito essenziale nella progettazione dei cifrari a blocchi [11].

4. La rivoluzione nella crittanalisi: Alan Turing

È opinione generalmente condivisa tra gli storici che l'ausilio della crittanalisi per intercettare e decifrare le comunicazioni dell'Asse da parte degli Alleati abbia permesso di abbreviare di almeno due anni la durata della Seconda guerra mondiale, risparmiando quindi milioni di vite umane – queste valutazioni sono di

⁵ Con *cifrario a blocchi* si intende un sistema che trasforma blocchi del messaggio (testo in chiaro) di lunghezza fissa (per esempio, di n bit) in blocchi di crittogramma della stessa lunghezza con il controllo di una chiave (di m bit).

sir Harry Hinsley, lo storico ufficiale dell'intelligence britannica della Seconda guerra mondiale, presentate in varie occasioni e riassunte in [21].

Winston Churchill, forse esagerando, avrebbe detto a Giorgio VI, re del Regno Unito: "È grazie a Ultra⁶ che abbiamo vinto la guerra". E inoltre: "Non direi che Turing ci abbia fatto vincere la guerra, ma oserei dire che l'avremmo perduta senza di lui", dichiarò esplicitamente Irving John (Jack) Gould, altro codebreaker di punta in tempo di guerra [22].

Incontrovertibile rimane il fatto che i crittanalisti alleati con la loro tecnologia abbiano sconfitto i crittografi tedeschi nonostante i loro pur sofisticatissimi sistemi.

4.1 La visione di Turing

Del film di successo *The Imitation Game*⁷ del 2014 sulla vita – alquanto romanizzata – di Alan Turing molti spettatori ricordano, sia pure a grandi linee, l'intuizione visionaria di Turing di costruire una macchina, la *Bombe*, che facesse il lavoro di centinaia di persone per decrittare Enigma, il sistema cifrante impiegato dalle forze armate tedesche. L'apparato Bombe permetteva ai britannici di confrontare un messaggio in chiaro con il messaggio cifrato intercettato e vedere se una qualsiasi configurazione dei rotori di Enigma potesse corrispondere a tale cifratura. Quando e qualora la coincidenza si fosse verificata, essa avrebbe fornito la chiave di decrittazione giornaliera consentendo ai britannici di leggere tutti gli altri messaggi intercettati nella stessa giornata.

A Bletchley Park (il centro era anche chiamato Station X [24]), non tutti erano convinti che Turing ce l'avrebbe fatta: circolava la voce che Alastair Denniston, il primo capo del centro, avesse dichiarato al responsabile della Sezione navale: "I tedeschi non hanno intenzione di farci leggere le loro cose, e dubito che possiate mai riuscirci". Ma Turing e i suoi colleghi ci riuscirono. (In *The Imitation Game*, Denniston appare ancora più categorico: "Enigma non è difficile. È impossibile!").

Questo non fu l'unico grande contributo di Turing in crittanalisi; in effetti, Turing si prodigò anche per risolvere i messaggi tedeschi cifrati con telescrivente *ad hoc* – definita a Bletchley Park con il criptonimo "Tunny" – e negli USA lavorò sul

⁶ Denominazione in codice (o, meglio, "criptonimo") per indicare il lavoro e i risultati di tutte le operazioni del servizio di SIGINT britannico nel periodo bellico, cioè di crittanalisi delle comunicazioni cifrate dell'Asse da parte degli Alleati. Ultra è il nome di un progetto complessivo: l'idea corrente che si riferisse solo a Enigma è imprecisa e parziale. Allo stesso modo, si dovrebbe ricordare – anche se qui non avremo modo di approfondire – che Enigma non fu l'unico sistema cifrato; la stessa Enigma ebbe numerose varianti e fu utilizzata in molti modi nelle reti dei diversi servizi bellici tedeschi. Un altro criptonimo utilizzato, per un breve periodo, per occultare le fonti di informazione provenienti dai canali di intercettazione più disparati fu Boniface.

⁷ Una delle cose migliori del film, diretto da Morten Tyldum, è, probabilmente, l'elogio insistito in ben tre scene della creatività progettuale: "A volte sono le persone che nessuno immagina possano fare certe cose, quelle che fanno cose che nessuno può immaginare", quasi un Leitmotiv della sceneggiatura. In ogni caso, il film – liberamente ispiratosi dalla biografia di Alan Hodges su Turing [23] – è meritevole di plauso per le atmosfere evocative e suggestive del periodo.

sistema SIGSALY di telefonia con voce cifrata. Quest'ultima realizzazione, unica nel suo genere, fu utilizzata regolarmente in importanti comunicazioni d'alto livello su operazioni strategiche, incluse le conversazioni segrete tra il presidente USA Franklin Delano Roosevelt (sostituito da Harry S. Truman prima della fine della guerra) e il premier britannico Winston Churchill (riquadro 2).



Figura 3
La residenza di Bletchley Park

Allo scoppio delle ostilità nel settembre 1939, Turing fu assegnato dal governo britannico al quartier generale del Government Code and Cypher School (GC&CS)⁸ a Bletchley Park (figura 3), dove il suo brillante lavoro avrebbe avuto conseguenze di grande portata. I britannici avevano appena ricevuto i risultati dei tentativi effettuati dai crittanalisti polacchi, aiutati dai colleghi francesi, per forzare il cifrario Enigma (figura 4), in dotazione al settore comunicazioni radio dell'esercito tedesco. Già nel 1932, una piccola squadra di matematici polacchi, guidati da Marian Rejewski, era riuscita a ricostruire – ecco un formidabile esempio di retroingegnerizzazione – il cablaggio interno del modello della macchina Enigma allora in uso.

Nel 1938 i polacchi poi erano poi riusciti a sviluppare una macchina di crittoanalisi [25], dal nome in codice *Bomba* (probabilmente da un termine allora in uso in Polonia per un tipo di gelato). Per funzionare con successo Bomba dipendeva dalle norme operative dei tedeschi, quindi un cambiamento procedurale nel maggio 1940 rese Bomba praticamente inutilizzabile. Durante il 1939 e l'inizio del 1940, Turing con il suo staff progettò una macchina

⁸ Nel 1946, alla fine della guerra, il GC&CS sarebbe diventato il GCHQ (Government Communications Headquarter).

crittanalitica completamente diversa denominata *Bombe*, alla francese e a imitazione dei polacchi (il nuovo termine, invero, indica un ipercalorico dessert inglese, sempre a base di gelato). Con l'ingegnosa macchina di Turing (figura 5), i crittanalisti di Bletchley Park all'inizio del 1942 furono in grado di intercettare e decifrare circa 39.000 messaggi al mese, numero che rapidamente crebbe fino a 84.000 e oltre. Poiché il suo contributo alla vittoria degli Alleati rimase per decenni coperto dal segreto di stato, l'unica onorificenza conferita a Turing fu l'Order of the British Empire, sia pure un riconoscimento di routine e non certo di rango eccezionale.

Ovviamente, i contributi di Turing toccarono più discipline, in ognuna delle quali lo scienziato lasciò impronte memorabili – il titolo del basilare riferimento bibliografico [22]: *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life; Plus the Secrets of Enigma* è indicativo della reale vastità dei suoi interessi.

La descrizione dettagliata dei principi di funzionamento di Enigma, dell'architettura e della sua complicata meccanica a più rotori, non solo nelle numerose varianti, ma già nella versione-base, esula dagli scopi del presente lavoro. Parecchi testi o articoli citati in bibliografia, oltre a molti altri, riportano – con diversi gradi di approfondimento, accuratezza, precisione – i modi di funzionamento di Enigma nonché le tecniche per la sua decrittazione (la *Bomba* polacca, la *Bombe* anglo-americana, ecc.). Per un resoconto di interesse anche storico si rinvia alla fonte primaria [26].

È necessario ribadire un punto: le successive versioni della macchina Bombe britannica non costituivano solamente un miglioramento più veloce della Bomba polacca, molto più piccola e assai meno sofisticata. Bombe, rispetto a Bomba, trovava soluzioni all'Enigma con metodi radicalmente diversi che, infatti, coinvolgevano porzioni di testo in chiaro ed elaborazioni in parallelo nel provare le permutazioni delle possibili connessioni di Enigma. Entrambe però erano elettromeccaniche – solo il successivo (proto)computer Colossus [27] sarebbe stato elettronico.

Dell'esperienza di Turing con Enigma si possono evincere tre aspetti principali:



Figura 4
Una versione della macchina cifrante Enigma

1. L'uso di tecniche probabilistiche, basate su una logica inferenziale bayesiana, e anticipatorie di quella che sarebbe diventata l'analisi statistica sequenziale di Abraham Wald [28] (v. il punto 4.3).
2. La rilevanza di processi *just in time*, cioè la necessità di trovare la chiave giornaliera entro le prime ore del mattino. Tempestività però che si concretizzava non solo nella rapidità ma anche nella perfezione ingegneristica.
3. L'importanza di condividere informazioni in team con competenze interdisciplinari. Benché Turing possedesse un'indole solitaria – “un introverso cronico” lo definì l'amico Max Newman – in realtà, a Bletchley Park non lavorava isolato: vi erano quasi 10.000 dipendenti fra tecnici e amministrativi, di cui circa 2.000 destinati al lavoro di crittanalisi. In tutti i sensi si trattò di un imponente lavoro collettivo, anche se a compartimenti stagni per ragioni di segretezza, durante il quale Turing fu affiancato da collaboratori validissimi.

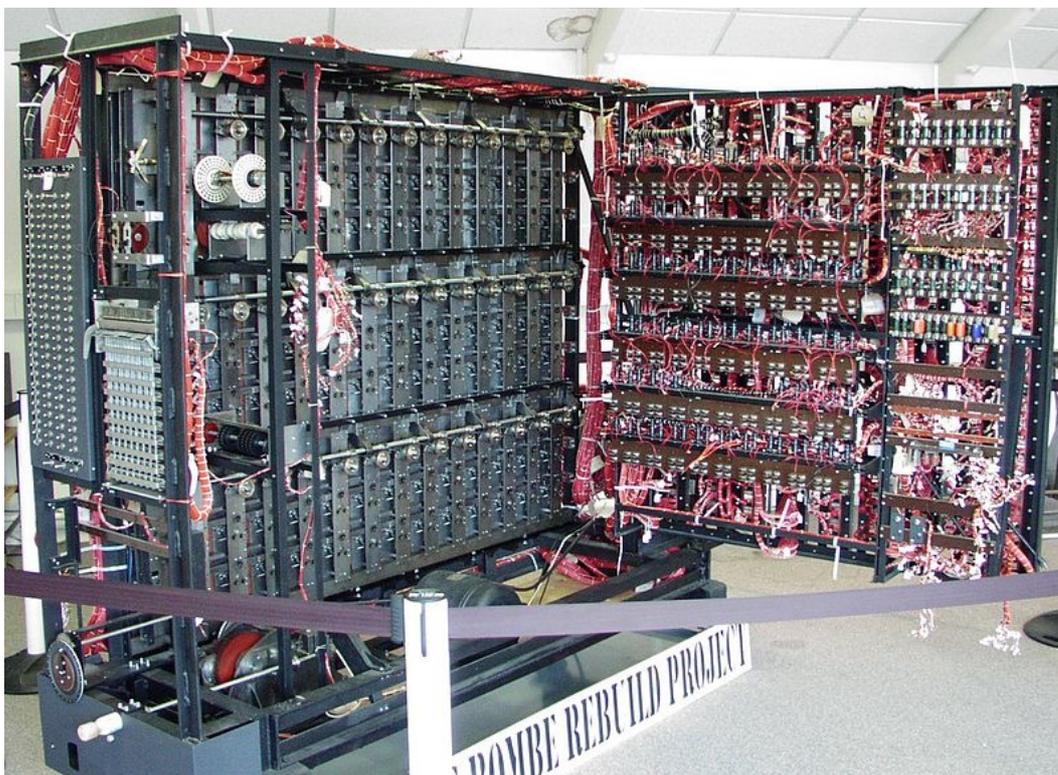


Figura 5

Replica completa e funzionante della macchina Bombe realizzata da Turing a Bletchley Park

4.2 L'illusione di Enigma e il successo di Bombe

Poiché l'unico modo per decrittare i messaggi intercettati di Enigma era di conoscerne il settaggio giornaliero (cioè una tra le 159.000.000.000.000.000.000 combinazioni possibili, come rivela un personaggio nel film citato) e, vista la necessità di cifrare i vari messaggi nel minor tempo possibile, Turing inventò diversi metodi per ridurre drasticamente il numero di settaggi possibili. (In verità, il numero esatto di combinazioni è 158.962.555.217.826.360.000). Per la variante navale di Enigma questo numero deve essere ulteriormente moltiplicato per un altro fattore di variabilità, cioè $26 \times 26 = 676$, il che porta a uno spazio di $1,07 \times 10^{23}$ combinazioni da esplorare [29] (ma il film non lo dice). Come si chiarirà meglio qui di seguito, la sicurezza teorica (o matematica) era di gran lunga maggiore di questi valori numerici, di per sé già impressionanti.

Le tecniche utilizzate da Turing e colleghi furono: 1) i *crib*, 2) il "Banburismo" (*Banburismus*), 3) la meccanizzazione dell'intero processo di decrittazione di Enigma, inclusi i due punti precedenti, mediante le macchine Bombe⁹.

L'individuazione dei *crib* e il Banburismo si basavano entrambi su una metrica logaritmica dell'informazione con logica bayesiana – come per Shannon – denominata "peso dell'evidenza" (riquadro 2). Uno degli assistenti principali di Turing a Bletchley Park, Jack Good, avrebbe sviluppato dopo la guerra il concetto di analisi statistica sequenziale in varie discipline applicative, restando però sempre molto riservato – almeno sino alla fine degli Anni 1970 – sui successi propri e di Turing in Ultra. Come ebbe a dire Good in svariate occasioni: "Il gioco del Banburismo comportava la capacità di mettere insieme un gran numero di pezzi di informazione probabilistica in qualche modo, come nella ricostruzione di sequenze di DNA. Il migliore giocatore, in un gruppetto di dieci, fu Hugh Alexander, il campione di scacchi britannico, che divenne capo della sezione Enigma navale quando Turing incominciò a lavorare sulla segretezza del linguaggio parlato" [28].

Per ridurre il tempo di calcolo necessario a trovare la soluzione di Enigma, i crittanalisti britannici fecero anche ricorso a debolezze pratiche, introdotte inconsapevolmente dai crittografi tedeschi nella fase di cifratura, quali breve frasi di routine che potevano dare origine a congetture sul possibile testo in chiaro, per esempio indicazioni sul tempo atmosferico o espressioni di saluto. Il termine per queste parole probabili era appunto "crib", la quale nel gergo inglese indica l'azione di scopiazzare da altri, azione ben nota agli studenti (particolarmente a quelli italiani). I *crib* erano, in altri termini, locuzioni standard (*Wetter* o "tempo atmosferico", *Keine besondere Ereignisse* o "niente da riferire", ecc.) che ci si aspettava figurassero in posizione fissa nel messaggio in chiaro perché utilizzati sistematicamente e meticolosamente, in accordo con l'ordinata mente teutonica. Un altro elemento indicatore era la frequenza del numero *Eins*,

⁹ Per completezza, occorre dire che vi furono altri due elementi importanti: i *depth* e i *pinch* (cfr., per esempio, [23] e [27]). I primi consistevano nell'ingenua ripetizione di messaggi molto simili con lo stesso settaggio della macchina Enigma da parte dell'operatore tedesco; i secondi denotavano le azioni degli Alleati per la cattura di Enigma e della documentazione pertinente.

o “uno”, scritto in lettere. Una quantità sufficiente di crib rivelati poteva essere molto utile nella ricostruzione delle chiavi giornaliera.

Gli importanti lavori di Miller e Ratcliff [29]-[31] riportano il numero di tutte le possibili impostazioni di Enigma e il numero complessivo delle sue chiavi. Il calcolo rappresenta il trionfo dell'analisi combinatoria – basata su fattoriali, coefficienti binomiali, ecc. – in cui compaiono numeri enormi a esponente com'è tipico delle permutazioni e delle combinazioni. Per esempio, la sicurezza teorica (o matematica) risultava in un astronomico 3×10^{14} , comprensivo di tutte le possibili combinazioni della versione-base di Enigma a tre rotori. Ricorrendo a un paragone suggerito in [29] per sottolineare quanto grande sia questo numero, si potrebbe ricordare che il numero di atomi dell'intero universo osservabile è stimato in 10^{80} . Nessuna meraviglia che l'intelligence tedesca confidasse così tanto nell'inviolabilità assoluta della sua macchina.

Tuttavia la sicurezza informatica non è soltanto puro calcolo matematico, ma significa anche tenere conto di ciò che è noto all'avversario, delle procedure seguite, di come gli operatori abbiano usato le macchine e quali differenti tipi di macchine siano state impiegate. Quindi, a causa di restrizione tecniche e operazionali, il numero effettivo delle possibili configurazioni decresceva drasticamente. Miller [29] ha calcolato questo numero nel già visto $1,07 \times 10^{23}$, un valore pur sempre impressionante perché paragonabile a una chiave lunga circa 77 bit. Anche se oggi per applicazioni commerciali si reputano necessari sistemi di cifratura con chiavi di 128 bit o anche 256 ([9], [11]), il far breccia in Enigma costituiva una sfida formidabile per la tecnologia elettromeccanica di allora.

Oltre a Turing, un altro grande artefice del sistema Bombe per infrangere la sicurezza di Enigma fu il matematico Gordon Welchman (la Bombe da molti studiosi è attribuita tanto a Turing quanto a Welchman), che, lavorando sul cablaggio di Enigma, ne individuò un punto particolarmente debole [32]. Poiché i collegamenti usavano un cavo per connettere una lettera all'altra, la seconda lettera era riportata automaticamente alla prima: se la “A” era inserita nella “E”, la “E”, simmetricamente, era connessa alla “A”. Sfruttando ciò, Welchman propose a Turing di aggiungere a Bombe una tavola che collegava ogni lettera con tutte le altre seguendo uno schema regolare. Combinato con le tre tecniche di Turing sopra indicate, questo espediente ridusse drasticamente il numero delle impostazioni dei rotori facilitando enormemente il compito degli analisti. Dall'agosto 1940 le realizzazioni di Bombe inclusero anche l'artificio di Welchman, noto come “pannello o piastra diagonale” (*diagonal board*).

In definitiva, come già sottolineato al punto 3.1, esiste una differenza cruciale fra sicurezza teorica e sicurezza pratica. La sicurezza teorica può essere data con numeri certi, chiari, trasparenti. I numeri della sicurezza pratica dipendono, invece, da come il sistema di cifratura sia impiegato dal crittografo e dall'abilità del crittanalista. I tedeschi, abbagliati dai puri numeri teorici, non si resero conto di questa distinzione fondamentale. In [30] in forma sintetica e in [31] in forma più particolareggiata, si spiega chiaramente perché i tedeschi abbiano perso non solo la guerra dei codici cifrati ma l'intera guerra: i loro servizi segreti non

seppero mai che gli Alleati ne intercettavano e decrittavano il traffico di messaggi segreti in chiave strategica con regolarità assoluta.

Di fatto, come sempre avviene in crittanalisi, il successo si basò su una serie di piccoli errori commessi dagli operatori. Piccoli, ma imperdonabili – fra i quali l'uso ripetuto di locuzioni stereotipate – e dipendenti, in larga misura, dalla pigrizia e mancanza di fantasia degli addetti alla macchina, se non da incompetenza o frustrazione. Solo in rari casi, i risultati scaturirono da effettive attività di spionaggio.

Proprio nelle piccole debolezze tecniche e umane si insinua la bravura dell'analista crittografo. La lezione è che ogni schema di cifratura, per quanto studiato ed elaborato presenta sempre minute pecche, crepe, fessure in cui incuneare un grimaldello in modo da allargarle e forzare il sistema apparentemente inviolabile. Come accade con le serrature più sofisticate.

4.3 Probabilità e statistica nel Banburismo

Il cuore del metodo inventato da Turing per ridurre il numero dei test che una macchina Bombe doveva effettuare era una statistica intrinsecamente bayesiana [28], [33], soprannominata appunto Banburismo¹⁰. Il nome era derivato dalla città di Banbury, una cinquantina di chilometri da Bletchley Park, dove venivano prodotte le schede perforate necessarie al processo. Il metodo si basava su un'inferenza logico-statistica per ridurre il numero delle sequenze che Bombe doveva analizzare nella decrittazione finale. Turing, indipendentemente da Shannon, definì anche un'unità di misura dell'informazione su base logaritmica: il “ban” (oppure il suo decimo “deciban” o centesimo “centiban”), termine ancora derivato da Banbury. Poiché i logaritmi erano calcolati su base 10, non è difficile riconoscere che oggi il ban è chiamato “hartley” (per le relazioni di conversione tra le unità di misura dell'informazione, si veda il riquadro 3). Ovviamente un numero di ban per essere espresso in deciban deve essere moltiplicato per 10, o per 100 nel caso dei centiban.

Nel 1940, il termine statistica bayesiana non era ancora stato coniato e, quasi certamente, non sarebbe stato impiegato; la regola (o teorema) di Bayes non godeva, infatti, di buona reputazione tra gli statistici del tempo [28]. Paradossalmente, il fruttuoso ricorso ai metodi bayesiani sarebbe stata assai meno probabile da parte di chi avesse avuto un'educazione standard nei metodi statistici più ortodossi e in uso a quei tempi. Infatti, da decenni l'approccio bayesiano, che Turing avrebbe reso strumento perfetto per attaccare i sistemi di cifratura nemici, era sottoposto ad aspre critiche da parte dei professionisti della statistica.

Ma che si trattasse della regola di Bayes e che Turing ne fosse pienamente consapevole è testimoniato dalla domanda che il suo assistente Jack Good gli fece una volta: “Non stai utilizzando in fondo la regola di Bayes?” “Penso di sì”,

¹⁰ Si rinvia ai lavori [28], [34], [35] per approfondimenti sul teorema di Bayes e la relativa inferenza logico-statistica. In particolare, l'articolo [35] contiene in appendice il riquadro “Una cassetta degli attrezzi di probabilità”, che riporta i principali strumenti di base utili per entrare in argomento.

fu la risposta di Turing [28], [33] (Turing, ovviamente, ne era pienamente consapevole come si evince anche dal lavoro [36] – cfr. dopo e il riquadro 3).

Probabilmente, pochi all'epoca compresero che il Banburismo era bayesianesimo camuffato dietro l'uso del termine "peso dell'evidenza" misurato secondo l'unità del ban e suoi derivati. In estrema sintesi, il metodo consisteva nel sovrapporre due porzioni del testo per individuarne le corrispondenze. Così si riducevano enormemente le possibili configurazioni di Enigma che una macchina Bombe doveva esaminare in un tempo limitato. Si avvaleva inoltre della statistica bayesiana per calcolare le configurazioni iniziali più probabili, ricorrendo alla frequenza di digrammi (coppie di lettere) o trigrammi tipici della lingua tedesca.

Nell'aprile 2012 (l'anno del centenario della nascita dello scienziato), il GCHQ ha autorizzato il rilascio di due preziosi documenti di Turing, non datati, ma risalenti probabilmente alla seconda metà del 1941, come ben argomentato da Sandy Zabell [36]. Il primo di questi, "The applications of probability to cryptography", discute l'uso generale delle probabilità in crittanalisi, ricorrendo a una versione del teorema di Bayes, che Turing chiama *factor principle*. Il secondo "Paper on statistics of repetitions" è una breve nota sulla classica tecnica di crittanalisi, suggerita, per esempio, dal già citato Sacco [3] e da William Friedman¹¹, per stimare l'indice di coincidenza nella ricerca di sequenze ripetute (da cui il successivo test di Good-Turing per la stima statistica dell'evenienza di digrammi, trigrammi ecc. nel linguaggio naturale). In [33], Good menziona il manuale di Sacco nella traduzione francese (1951), sia pure storpiando il cognome in "Saccho".

A chiunque possieda competenze statistiche di base sarebbe possibile, seppure alquanto laborioso, estrarre dai due documenti la sostanza del lavoro di Turing. Tuttavia il saggio di Zabell [36] è davvero prezioso poiché commenta estesamente e con chiarezza l'approccio adottato. Il fatto che i due studi siano stati diffusi soltanto nel 2012 dimostra l'enorme importanza loro attribuita dall'intelligence britannica, non solo nel periodo bellico¹².

Già prima della laurea Turing aveva svolto ricerche originali in teoria delle probabilità, dimostrando una forma generale del teorema del limite centrale per variabili aleatorie indipendenti, non necessariamente identicamente distribuite. Il saggio fu presentato come titolo a supporto della sua candidatura a *fellow* (membro del corpo docente) del King's College a Cambridge nel 1935 [23].

¹¹ Il colonnello William Friedman, che dominò la scena crittologica USA tra le due Guerre, è l'autore della pionieristica monografia *The Index of Coincidence and its Applications to Cryptography* (1920). Il saggio rappresenta il primo importante passo in avanti verso l'analisi quantitativa in crittanalisi [4], proponendo un metodo che abbina le distribuzioni delle frequenze per ricostruire il testo in chiaro.

¹² La versione LaTeX dei due manoscritti di Turing, opportunamente ripuliti e risistemati da Ian Taylor (Università di Oxford) sono anche disponibili, dal maggio 2015, su arXiv, rispettivamente ai link <http://arxiv.org/abs/1505.04714> e <http://arxiv.org/abs/1505.04715>.

4.4 Non solo Enigma

Durante il resto della guerra, il traffico di messaggi cifrati, da entrambi i fronti belligeranti, e i tentativi di decrittazione reciproca furono davvero imponente. Per le successive vicende del Regno Unito che hanno contribuito alla nascita dei primi moderni computer – in parte ispirati direttamente o indirettamente da Turing – si rinvia agli ottimi testi [27] e [37].

Il prodotto tecnico-scientifico più importante di questa azione, che oggi definiremmo di *big science*, fu certamente la realizzazione della serie di dieci (proto)computer Colossus costruiti nel periodo dicembre 1943-giugno 1945 da ingegneri e tecnici britannici. Essi rappresentarono i primi elaboratori elettronici (ovviamente a tubi) programmabili di grosse dimensioni ma, per la solita ossessione alla segretezza dei britannici, furono smantellati a guerra conclusa. Almeno così si riteneva fino a poco tempo fa: lo studioso di Turing Jack Copeland argomenta in [27] che almeno due esemplari di Colossus furono impiegati nel dopoguerra per scopi ancora oggi non rivelati.

4.5 Fine dei segreti di guerra?

Dopo il 1940, il seme bayesiano, piantato da Turing, si sviluppò alquanto rigoglioso presso la comunità dei crittanalisti. Jack Good, che sarebbe diventato uno degli apostoli di questo credo, continuò a lavorare al GHCQ dal 1948 al 1959. Dopo la guerra, Good si prodigò per diffondere i capisaldi statistici del Banburismo [33] con determinazione, ancorché con estrema discrezione perché la maggior parte del lavoro crittanalitico bellico continuava ad essere segreto.

Le autorità britanniche permisero che questo velo di segretezza fosse parzialmente sollevato solo nel 1974, l'anno in cui uno dei partecipanti al progetto Ultra, Frederick W. Winterbotham, pubblicò *The Ultra Secret*. Esistono parecchie versioni sul perché Ultra sia stato mantenuto classificato così a lungo. La più accreditata, propugnata da Kahn [4], è che, dopo la guerra, i britannici abbiano raccolto il maggior numero possibile di macchine Enigma per rivenderle a Paesi del Terzo Mondo, fiduciosi di poterne leggerne i messaggi. Solo all'inizio degli Anni 1970 i vecchi apparati furono sostituiti da nuovi crittosistemi. Di sfuggita, si può menzionare che la recensione di Kahn, ripubblicata in [4], ha contribuito a far diventare *Ultra Secret* un bestseller mondiale.

Negli stessi anni cominciò anche a incrinarsi il silenzio sulle vere funzioni svolte da Bletchley Park e il pieno riconoscimento della sua importanza strategica. Sorprendentemente, in *The Ultra Secret*, il nome di Turing non appare. Compare invece, e frequentemente, in un altro libro – alle volte eccessivamente fantasioso – uscito nello stesso 1974: *Bodyguard of Lies* di Anthony Cave Brown, nel quale, Turing è spesso associato a termini quali *machine* e *Bombe*.

Dopo *Ultra Secret* e *Bodyguard*, fu pubblicata la prima edizione della monumentale e tuttora insuperata biografia su Turing di Hodges [23], cui si aggiunsero con ritmo accelerato resoconti, memoriali, reminiscenze, ricordi dei membri originali del gruppo di crittanalisti, costretti per decenni a un sofferto quanto dignitoso silenzio. Kahn in [6] acutamente osserva che, se il primo più grande segreto della Seconda guerra mondiale fu la bomba atomica, il secondo fu che gli Alleati erano stati in grado di leggere i messaggi cifrati dei tedeschi a loro insaputa.

Negli ultimi decenni Turing è diventato un'icona mediatica su cui si è scatenata la fantasia di scrittori e registi, dal romanzo cult *Cryptonomicon* di Neal Stephenson¹³ al film *The Imitation Game*, che ha dato ulteriore impulso al mito di Turing anche tra chi non lo conosceva affatto.

5. Conclusioni

Quanto detto in precedenza non ha solo un interesse storico, documentario, o aneddotico. Infatti, oggi le violazioni della sicurezza e gli attacchi di pirateria informatica costituiscono un problema diffuso e pervasivo [38] da diversi punti di vista: economico, politico, sociale, etico. Dal momento che i cyberattacchi, in ultima istanza, risultano da intendimenti dolosi condotti sulle configurazioni dei dati disponibili in una rete o in un elaboratore, non si può consentire che sistemi complessi (frutto dei nuovi paradigmi ICT¹⁴ in forte sviluppo quali cloud computing, IoT/IoE, big data, software defined network/radio) siano vulnerabili ai prevedibili attacchi futuri. Il gioco di creare sistemi cifrati e quello di forzarli è sempre più vivo. E trova terreno alquanto fertile nel Web.

La crittografia è certamente uno strumento di sicurezza indispensabile per assicurare che il messaggio non sia letto da nessun altro se non dal destinatario autorizzato. Nel mondo economico – sia privato sia degli affari – i sistemi crittografici sono usualmente impiegati per proteggere i dati trasportati su reti pubbliche di telecomunicazioni e usano algoritmi matematici molto evoluti per “rimischiare” i messaggi (e i testi allegati).

Peraltro, online nulla è protetto, nessuna crittografia, benché strumento di protezione basilare, resiste per sempre, come osserva Cory Doctorow in *Information Doesn't Want to Be Free: Laws for the Internet Age*. Alla lunga gli invasori, ladri, pirati, militari – sempre più scaltri (*smart*) – trovano il Cavallo di Troia o la breccia per entrare nel sistema che si vorrebbe protetto. Identità personali, segreti economici, di stato o impresa, sono a rischio cyberguerra (cfr. Gianni Riotta, *La Stampa*, 21 dicembre 2014). Già Edgar Allan Poe ammoniva saggiamente: “Si può tranquillamente affermare che l'ingegnosità umana non può elaborare un cifrario che la stessa ingegnosità umana non riesca a risolvere”. Così insegnano la violazione ripetuta di Enigma, la previsione eccessivamente ottimistica di Martin Gardner sulla robustezza dei sistemi a chiave pubblica [39], la quotidianità della pirateria informatica.

Peter Drucker, il grande guru del management nel secolo scorso, scrisse “Siamo viepiù consapevoli che la questione principale concernente la tecnologia non è tecnica ma umana”. Parafrasandolo, potremmo quindi dire che stiamo ritornando consapevoli che la questione principale concernente la “sicurezza” non è tecnica ma umana: per una rassegna delle linee-guida di possibili soluzioni a criticità legate al fattore umano si veda il recentissimo [40].

¹³ Una curiosità: il romanzo riporta una conversazione (ovviamente immaginaria) tra Turing e un personaggio fittizio, Lawrence Waterhouse, a riguardo del primo vocoder SIGSALY per comunicazioni vocali segrete (v. il riquadro 2).

¹⁴ *Information and Communications Technology*.

Uno degli esiti principali di questo processo lungo più di settant'anni e del quale Shannon e Turing sono stati protagonisti assoluti è la "matematizzazione" della crittologia (crittografia + crittanalisi) nelle varie branche componenti: logica simbolica e algebra booleana, teoria della complessità, computabilità, probabilità e statistica, ecc. I loro studi hanno permesso di distinguere nettamente quanto in crittologia sia scienza da quanto sia arte (o soluzione ad hoc). Naturalmente, ed è stato prima ricordato, a questo sviluppo hanno cooperato molti altri fra cui il nostro Luigi Sacco e lo statunitense William Friedman. Viene in mente il celeberrimo aforisma di Bernardo di Chartres: "Siamo nani sulle spalle di giganti", ripreso secoli dopo da Isaac Newton, che con sottile perfidia scriveva al nano Robert Hooke: "Se ho visto più lontano è perché stavo sulle spalle di giganti".

Proprio come l'interesse primario di Turing non era nel *code-breaking* ma nella computabilità, così l'interesse precipuo di Shannon non era nell'occultare l'informazione ma nel trasmetterla e nel riceverla nel modo più accurato possibile, cioè (quasi) senza errori. Tuttavia la storia scientifica dei due studiosi dimostra che i loro interessi principali e secondari, strettamente interconnessi, si arricchirono a vicenda.

Tra di loro ci furono però differenze significative. Shannon stabilì i principi fondamentali dei sistemi segreti, cioè della crittografia. Da solo. Non si occupò direttamente delle implicazioni pratiche [41], a parte il contributo allo sviluppo del digital scrambler di SIGSALY. Le imprese di Turing furono piuttosto opera di un *primus inter pares*; tant'è che poté lasciare Bletchley Park per la collaborazione in America (nell'inverno 1942-43). In ruoli allo stesso tempo diversi e complementari, furono due giganti del pensiero, precursori della grande e migliore scienza (big science) in questo XXI secolo. Il lavoro a Bletchley Park è anche un esempio del paradigma universalmente noto come big data, un'etichetta oggi forse già un po' troppo alla moda, quasi un tic culturale.

Né Shannon né, tantomeno, Turing hanno contribuito direttamente agli sviluppi più importanti della disciplina emersi a partire dagli Anni Settanta del Novecento, per esempio, ai sistemi a chiave pubblica, nei quali una chiave segreta condivisa tra le parti comunicanti non è necessaria per garantire la segretezza. Tuttavia, questi e altri contributi – anche quelli più recenti – sono concettualmente debitori agli studi di entrambi.

Così mi pare di poter sintetizzare, al termine della lettura di svariati studi crittologici, in un articolo che più che inseguire un'ambizione di completezza ha cercato di restituire modalità di lavoro e di approccio ai problemi da parte di Shannon e Turing. Il vastissimo materiale sugli argomenti qui sommariamente trattati appare di mole ulteriormente crescente negli ultimi decenni dopo che il velo di segretezza riguardante i documenti dei servizi segreti in vari Paesi è stato parzialmente sollevato. Solo una parte di questi lavori è stata qui utilizzata benché in forma estremamente sintetica e panoramica. Una trattazione sufficientemente dettagliata di tutti gli argomenti, accompagnata da un commento adeguato, riempirebbe un volume di centinaia di pagine. Pertanto, nella rassegna si è accennato solo per sommi capi agli eventi e ai risultati principali, privilegiando l'aspetto tecnico-scientifico pur con qualche

divagazione storica e narrativa. Si rimandano al futuro eventuali approfondimenti su aspetti particolari o più circoscritti.

In conclusione, non sembra inutile sottolineare un'ultima lezione di carattere metodologico nel lascito di Shannon e Turing. Per imparare a gestire scelte sempre più complesse, occorre investire sulla propria intelligenza, sul pensiero logico e critico utilizzando due saperi di base: la teoria della probabilità e la psicologia del rischio. I risvolti pratici di queste competenze – delle quali molti, troppi, sono del tutto digiuni tanto nella mentalità quanto negli strumenti [34], [35] – sono oggetto di ricerche avanzate ben rappresentate da studiosi quali Daniel Kahneman [42] e Gerd Gigerenzer [43]. Beninteso, la razionalità pura deve essere integrata da un'ulteriore competenza basata sull'intuizione che porta all'euristica [43], ossia alla “regola del pollice”, e che solo l'esperienza può insegnare.

In Italia, purtroppo, il vezzo di esibire la propria ignoranza in fatto di tecnoscienza era e resta uno degli esercizi preferiti di certa intelligenza. Di tale ignoranza continua, infatti, a vigere la legittimazione sancita, ormai più di un secolo fa, dal “crocianesimo”, l'idealismo crociano in tutte le sue declinazioni, e ribadita, in anni più recenti, dagli epigoni del pensiero debole e di Heidegger. Quest'ultimo con la sentenza lapidaria “la scienza non pensa” ha autorizzato generazioni di giovani a non impegnarsi nello studio di competenze cruciali per lo sviluppo di un Paese. Gli zelanti campioni nostrani delle cosiddette scienze umane (tutte le altre sono forse “inumane”? [44]) si compiacciono di svilire *in toto* i saperi afferenti alle discipline STEM – acronimo che denota l'insieme di scienza, tecnologia, ingegneria (*engineering*) e matematica [45] – anziché considerarne l'espansione una priorità nazionale, come tradizionalmente avviene negli USA e, in generale, nelle nazioni all'avanguardia culturale, civile, sociale, economica.

Ringraziamenti

Sono sinceramente grato a quanti mi hanno amichevolmente aiutato a reperire l'ampia documentazione di riferimento, rispondendo positivamente alle mie pressanti richieste: Alfredo Biocca, Marina Dambrosio, Letterio Gatto, Pietro Laface, Steven J. Miller, Maurizio Molinaro, Andrea Nicolotti, Giancarlo Pirani, Klaus Pommerening, Laura Porello, Rebecca A. Ratcliff, Dirk Rijmenants, Viola Schiaffonati, Fabrizio Trisoglio, Sandy Zabell. Spero che l'elenco non contenga dimenticanze imperdonabili.

Ringrazio, inoltre, un anonimo revisore le cui acute e pertinenti osservazioni mi hanno permesso di focalizzare i contenuti dell'articolo e di precisare i punti non sufficientemente chiari nella stesura iniziale.

Infine, mi sembra opportuno ricordare i molti strumenti tecnologici e culturali disponibili sul Web, soprattutto Google e Wikipedia, che liberano di continuo risorse altrimenti introvabili con i mezzi tradizionali. E, contrariamente alla vulgata corrente, queste fonti di documentazione – non solo di origine accademica – si sono mostrate, il più delle volte, affidabili e autorevoli.

Riquadro 1 – “1941: l'MI5 cerca la talpa di Agatha Christie”* e altri aneddoti

Nel 1941 la vita dell'ignara Agatha Christie divenne per qualche mese un racconto di Borges, fatto di specchi e allusioni inquietanti, mentre la trama del suo ultimo giallo si rovesciava, ben più temibile, nell'esperienza quotidiana.

I servizi segreti britannici erano infatti convinti che nel suo *N or M*, pubblicato nel novembre 1941, ma tradotto in Italia solo nel 1961 con il titolo *La quinta colonna*, ci fosse un riferimento alle attività del segretissimo centro di decifrazione [decriptazione] di Bletchley Park che era riuscito a trascrivere il codice cifrato tedesco Enigma, con enorme vantaggio per gli inglesi.

Il giallo racconta le avventure di una coppia di detective, Tommy and Tuppence, che danno la caccia a due agenti nazisti, infiltrati in Inghilterra per preparare un'invasione, noti appunto col nome in codice *N e M*. L'MI5, il controspionaggio britannico, rabbrivì quando lesse il nome di un personaggio secondario, il maggiore Bletchley, guarda caso, un “noioso ufficiale” che aveva servito in India e si vantava di conoscere molti segreti della guerra in corso.

I primi sospetti caddero su Dilly Knox uno dei più dotati decifраторi [decriptatori] a Bletchley Park, che era amico della Christie. Fu subito scagionato ed escluse che la scrittrice potesse sapere qualcosa del centro segreto ma accettò di sentirla. Davanti a un vassoio di tè e pasticcini, nella sua casa nel Buckinghamshire le chiese perché avesse proprio scelto quel nome. “Bletchley? – rispose la scrittrice – Mio caro, ero proprio lì, bloccata in treno sulla linea Oxford-Londra, allora mi sono vendicata chiamando così uno dei miei personaggi meno gradevoli.”

È già stato sottolineato che le vicende di Bletchley Park non hanno rappresentato un *one-man show* (cioè Alan Turing da solo), come si potrebbe invece supporre seguendo resoconti mediatici troppo superficiali e mistificanti. In realtà, i ragguardevoli personaggi che si sono occupati di crittanalisi durante la Seconda guerra mondiale sono stati in generale spiriti bizzarri e ameni, spesso dotati di grande creatività.

Assistente di Turing a Bletchley Park fu Jack Good che successivamente, dal 1967 al 1994, insegnò in USA al Virginia Polytechnic Institute and State University. Una sua arguta osservazione fu: “Sono arrivato a Blacksburg alla settima ora del settimo giorno del settimo anno nel settimo decennio, e fui alloggiato nell'Appartamento 7 dell'edificio 7... e tutto per caso”**. Quando si parla di coincidenze fortuite! (Su questo argomento non abbiamo certo nascosto il nostro scetticismo nell'articolo [35]). Good, che fu consulente di Stanley Kubrick per l'intelligente supercomputer HAL 9000 nel film *2001: Odissea nello spazio*, è anche noto per l'ironica

affermazione di avere contato “almeno 46.656 interpretazioni differenti” di teorie bayesiane [28], un numero ben superiore a quello degli statistici professionisti.

Uno dei più giovani colleghi di Turing a Bletchley Park fu Peter Hilton*** il quale, per puro *divertissement*, costruì in una notte insonne il palindromo di 51 lettere: DOC NOTE, I DISSSENT. A FAST NEVER PREVENTS A FATNESS. I DIET ON COD, tuttora il più lungo della lingua inglese. Hilton ha ricordato nelle sue reminescenze di crittanalista [46] l'osservazione invero *tranchant* ma pertinente di Good: “Fortunatamente, le autorità di Bletchley Park non avevano la minima idea che Turing fosse omosessuale; altrimenti, avremmo perduto la guerra”.

Un'altra figura da menzionare è Ian Fleming – il futuro creatore del mitico James Bond – che operò come ufficiale di collegamento tra Bletchley Park e la Naval Intelligence per tutto il periodo bellico. Fleming morì nel 1964, dieci anni prima che il velo di segretezza su Bletchley Park fosse sollevato. Perciò non poté mai svelare il suo coinvolgimento nelle faccende segrete di Enigma e Ultra, nonché i contatti con Turing per l'Operazione *Ruthless* [28], sebbene il suo avvincente lavoro in tempo di guerra abbia ispirato le imprese dell'Agente 007. Anche l'attore Christopher Lee, memorabile nelle sue interpretazioni del conte Dracula e cugino acquisito di Fleming, operò nei servizi segreti britannici durante la guerra.

* È il titolo dell'articolo di Giorgio Gallo (La Stampa, 5 febbraio 2013) dal quale sono ripresi (con adattamenti editoriali) i primi quattro capoversi del riquadro. Il curioso aneddoto sulla Christie è stato svelato dall'esperto di SIGINT Michael Smith [24].

** Cfr. http://en.wikipedia.org/wiki/I._J._Good.

*** Hilton figura anche nel film *The Imitation Game*.

Riquadro 2 – Turing incontra Shannon ai BTL: il sistema X (o SIGSALY)

Alla fine del 1941, con l'entrata degli USA in guerra, i BTL portavano avanti diversi progetti sui sistemi segreti, specialmente sullo *speech scrambling* (mescolamento vocale) per proteggere le comunicazioni da orecchie indiscrete. Uno di questi – denominato Sistema X o SIGSALY* [47] – era probabilmente il più segreto di tutti poiché riguardava lo sviluppo di un sistema radiotelefonico per connettere Churchill a Roosevelt. (Anche SIGSALY sarebbe rimasto fino al 1975 “un sistema del quale non si poteva parlare” [23]).

Shannon lavorò sul progetto benché, per ragioni di segretezza, non avesse accesso a tutti i particolari e fosse vincolato a non interagire con altri sull'argomento. Resta il fatto che si occupava del cuore del sistema, ossia proprio dello schema di cifratura, il blocco monouso di Vernam citato al punto 2.2. Il compito di Shannon era di verificare che nessun dettaglio fosse trascurato e che il metodo fosse veramente imbattibile.

Nel gennaio 1943, Turing andò New York per fornire consulenza su molti aspetti dello speech scrambling e, restando in USA per due mesi, ebbe saltuarie conversazioni con Shannon nella mensa aziendale dei BTL, durante le pause pranzo o del pomeriggio. Fatto abbastanza curioso è che essi non poterono discutere i rispettivi lavori sottoposti al vincolo del segreto militare. Parlarono invece di argomenti di interesse reciproco, allora ritenuti non confidenziali, come la nuova scienza dei computer e l'evenienza di macchine in grado di simulare il cervello umano.

La partecipazione di Turing e Shannon in questo progetto è descritta con abbondanza di particolari aneddotici da Hodges [23], per la verità con un linguaggio che nelle parti tecniche suona un po' datato a chi si occupa oggi di telecomunicazioni nell'ICT.

Lavorando per decrittare i messaggi di Enigma, Turing sviluppò un tipo di misura dell'informazione molto simile a quella pubblicata da Shannon solo nel 1948 [18]. L'unità di informazione di Shannon era il "bit", di Turing il "ban". Non sembra, tuttavia, che lo scienziato britannico abbia contribuito alle intuizioni fondamentali della teoria dell'informazione, infatti, Shannon su queste idee ricevette da Turing "... un bel po' di riscontri negativi" [41].

Volendo sottolineare una differenza tra Shannon e Turing, si può indicare il minor interesse pratico del primo per le applicazioni rispetto ai problemi: "Sembra che [Shannon] abbia preferito lavorare sui problemi allo scopo di comprendere e trovare soluzioni, senza preoccuparsi di applicazioni militari o essere distolto dal suo obiettivo puntando troppo su applicazioni di ogni tipo" [41]. Non è però del tutto vero: cfr. [17] per una descrizione dell'interesse molto pratico e remunerativo, benché non prioritario, di Shannon per l'azzardo e la finanza.

I due scienziati si incontrarono ancora in Inghilterra nel settembre 1950 in occasione di un simposio sulla teoria dell'informazione, nel quale Shannon era l'ospite d'onore. Si confrontarono su una strategia minimax proposta da Shannon per il gioco degli scacchi e sui calcoli di Turing sulla funzione zeta.

In definitiva, anche se le relazioni dirette tra Shannon e Turing furono scarse, peraltro la comunanza di interessi fu straordinaria come dimostra il complesso dei loro lavori, disponibili nei rispettivi *Collected Works* – un unico volume dell'IEEE Press per Shannon, e quattro (costosissimi) tomi della North Holland per Turing.

Tornando al sistema SIGSALY, un cospicuo gruppo di progettisti dei BTL, sotto la direzione di A. B. Clark (che successivamente avrebbe guidato le attività di ricerca e sviluppo della NSA nel biennio 1954-55), sviluppò il

codificatore vocale (vocoder) con particolare attenzione alla qualità della voce. L'articolo di rassegna storica [48] attribuisce al sistema varie priorità di tecnica delle comunicazioni, fra cui:

- la realizzazione della telefonia cifrata
- la quantizzazione del segnale vocale
- la trasmissione della voce in PCM (Pulse Code Modulation)
- l'impiego della modulazione numerica multilivello FSK (Frequency Shift Keying)
- la realizzazione della compressione di banda del segnale vocale
- l'impiego della tecnologia ad "allargamento dello spettro" (Spread Spectrum)

Per le sue peculiarità innovative SIGSALY potrebbe essere considerato addirittura come il primo passo verso la rivoluzione digitale. Le tecniche di spread spectrum avrebbero poi avuto un grande impatto sullo sviluppo delle attuali comunicazioni mobili cellulari (cfr. i contributi di Andrew Viterbi, studioso italiano di famiglia e di nascita).

Kahn in [47] ricorda che Shannon e Turing – insieme con un nutrito gruppo di esperti dei BTL, fra cui Harry Nyquist** – contribuirono alla concezione e allo sviluppo di SIGSALY sia per la parte di comunicazione sia per gli aspetti di sicurezza e riservatezza. Kahn cita anche il curioso episodio di Hedy Lamarr, celebre attrice della prima metà del Novecento, che ottenne nel 1942 il rilascio di un brevetto basato sul *frequency hopping*, un particolare schema di spread spectrum, con applicazione al controllo radio di siluri navali.

Di ritorno dall'America, Turing diede un altro grande esempio delle sue capacità di visione e progettualità creando per il Radio Security Service britannico a Hanslope Park lo scrambler *Delilah*, il primo esempio di sistema portatile e digitale per comunicazioni vocali sicure – realizzato purtroppo troppo tardi per poter diventare operativo.

* Il nome SIGSALY non significava alcunché, era solo un criptonimo somigliante a un acronimo.

** Il suo teorema del campionamento (1928) avrebbe contribuito ad aprire la strada alle comunicazioni numeriche e, subito dopo, all'era dell'informazione digitale.

Riquadro 3 – Teoria dell'informazione e probabilità: terminologia e metriche

In un sistema di trasmissione dell'informazione (trasmettitore + canale + ricevitore), a mano a mano che si riceve l'informazione sul messaggio trasmesso, diminuisce l'incertezza nel ricevitore. Un semplice esempio consente di illustrare questo concetto apparentemente ovvio ma fondamentale. Si supponga di considerare: 1) un canale ideale che non introduce né rumore né distorsione, 2) che i messaggi possibili siano otto, tutti codificati in binario, e 3) che fra questi venga trasmesso il secondo, codificato nella successione 001. La ricezione del primo simbolo 0 elimina una parte dell'incertezza relativa al messaggio trasmesso: infatti, l'informazione rappresentata dallo zero restringe il campo dei messaggi trasmessi a solo quattro. Analogamente la ricezione del secondo 0 restringe il campo di possibili messaggi solo a 000 e 001, finché la ricezione dell'1 elimina ogni dubbio. La probabilità dei singoli messaggi dopo la ricezione di ciascun simbolo si può calcolare applicando la definizione di probabilità condizionata e, quindi, utilizzando la regola di Bayes [28], [34], [35] (non è necessario ipotizzare che la distribuzione di probabilità degli otto messaggi sia uniforme).

L'esempio della logica seguita (un'inferenza bayesiana a tre passi) fornisce il punto di partenza del ragionamento di Shannon, che è anche quello di Turing nel Banburismo, sia pure con una terminologia diversa: fattore bayesiano e peso dell'evidenza. Il fattore di Bayes è definito come la probabilità del dato osservato in una certa ipotesi, divisa per la probabilità in un'altra ipotesi – oggi detto “rapporto di verosimiglianza” (*likelihood ratio*). Il peso, o misura, dell'evidenza – il contenuto informativo secondo Shannon – ne è il suo logaritmo. Su una scala logaritmica, un fattore di soglia decisionale di 50 a 1 (*odds*) è rappresentato da un punteggio di 1,7 ban (oggi Hart), o 17 deciban, infatti, il logaritmo in base 10 di 50 è 1,7. Il peso dell'evidenza è sostanzialmente equivalente alla misura logaritmica dell'informazione, che Turing formulò e usò indipendentemente da Shannon.

Il peso dell'evidenza fu anche usato nel metodo – interamente manuale con carta, matita e gomma – noto come *Turingery* (1942), concepito sempre da Turing per dedurre l'impostazione delle ruote della macchina cifrante soprannominata “Tunny” a Bletchley Park (Tunny era una Lorenz della serie di telescriventi SZ sviluppate dopo Enigma: al volume collettaneo [27] si rinvia per una trattazione aggiornata ed esauriente). Come ricordato in 4.3, il Banburismo consentì a Turing di evitare il metodo computazionale della cosiddetta forza bruta (il tener conto di “tutti i casi possibili”) nella ricerca del messaggio in chiaro. Questo sarebbe stato, infatti, un approccio destinato al fallimento con i mezzi di calcolo allora disponibili. Sostanziale fu la riuscita del processo di meccanizzazione del giudizio attraverso la quantificazione del peso dell'evidenza,

un'anticipazione dei sofisticati programmi inferenziali bayesiani oggi usati nelle applicazioni di intelligenza artificiale. Infine, gli stessi principi del Banburismo – fattori di Bayes e loro logaritmi, in una logica sequenziale, per discriminare tra due ipotesi – sono stati i fondamenti generali della ricerca operativa, a partire dal controllo di qualità.

Nella metrica dell'informazione, la base dei logaritmi determina l'unità impiegata secondo lo standard ISO/IEC [49]:

- shannon (simbolo: Sh) per i logaritmi di base 2
- unità naturale (simbolo: nat) per i logaritmi di base e
- hartley (simbolo Hart) per i logaritmi di base 10

Ne risulta la tabella di conversione:

- 1 Sh = 0,693 nat = 0,301 Hart
- 1 nat = 1,433 Sh = 0,434 Hart
- 1 Hart = 3,322 Sh = 2,303 nat

Benché il “bit” in pratica sia più comune dello “shannon”, anche come misura dell'informazione binaria, diversamente però vorrebbe lo standard [49]: il bit, a stretto rigore, è un termine d'uso generico.

Probabilità e odds. Com'è caratteristico del mondo delle scommesse in Paesi di cultura anglosassone, Turing e i suoi collaboratori a Bletchey Park lavoravano con le *odds* (quote, posta, pronostico) a favore di un evento anziché con la probabilità dello stesso evento*. Odds e probabilità costituiscono due rappresentazioni, o forme, diverse per valutare la possibilità che un determinato evento accada. Si consideri, per esempio, il caso di due assi estratti da un mazzo di 52 carte. La probabilità di questo evento congiunto è $P = 4/52 \times 3/51 = 1/221$: statisticamente, una volta su 221 capita la coppia d'assi. Spesso, soprattutto nell'ambiente delle scommesse, si preferisce indicare che le possibilità contrarie rispetto a quelle favorevoli sono di 221 meno 1, cioè di 220 a 1, o anche che le quote a sfavore sono di 220 : 1. Statisticamente, per ogni 220 casi sfavorevoli ce ne sarà uno favorevole. Le quote a favore sono ovviamente il reciproco, cioè 1 : 200.

In generale, la probabilità $P(A)$ di un evento A è il rapporto tra il numero di casi favorevoli e il numero totale di casi; le quote (odds) a favore $OF(A)$ sono il rapporto tra il numero di casi favorevoli e il numero di casi sfavorevoli. Le relazioni tra probabilità $P(A)$ e odds a favore $OF(A)$ sono: $OF(A) = P(A)/[1 - P(A)]$ e $P(A) = OF(A)/[1+OF(A)]$. Si noti che $OF(A)$, funzione monotona crescente di $P(A)$, tende asintoticamente all'infinito quando $P(A) = 1$. Se $OF(A)$ è esprimibile con il rapporto m/n , la corrispondente probabilità diventa $m/(m + n)$; per esempio, $OF(A) = 1/3$ e $P(A) = 1/4$. Per un evento con probabilità di $2/3$, le quote sono di 2 a 1 (o di 2 : 1), mentre, per un evento di probabilità $3/10$, le quote sono 3 : 7. Una

remunerazione di r a 1 significa che il banco (o l'allibratore) onora la vincita del giocatore con $r + 1$ euro per ogni euro scommesso, altrimenti incamera la posta giocata.

In definitiva, i due termini probabilità e odds, pur esprimendo lo stesso concetto matematico, assumono valori numerici diversi, ancorché legati da semplici relazioni matematiche.

 * Già secoli fa, il concetto di odds era stato efficacemente introdotto, con il termine latino di *proportio*, da Girolamo Cardano nel *Liber de ludo aleae*, opera pubblicata postuma nel 1663. Per un'eccellente ed esauriente trattazione di odds (definizioni, relazioni matematiche, esempi applicativi nei diversi contesti, riferimenti bibliografici), il lettore interessato può ricorrere, in prima istanza, alla voce omonima di Wikipedia (<https://en.wikipedia.org/wiki/Odds>).

Bibliografia

- [1] Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet* (Nuova edizione), Scribner. Prima edizione (1967). Macmillan. Tr. it. parziale della prima edizione (1969). *La guerra dei codici. La storia dei codici segreti*, Mondadori.
- [2] Kahn, D. (2004). *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*, Yale University Press.
- [3] Sacco, L. (2014). *Manuale di crittografia* (Quarta edizione ampliata a cura di Bonavoglia, P.), Apogeo.
- [4] Kahn, D. (1983). *Kahn on Codes: Secrets of the New Cryptology*, Macmillan.
- [5] Kahn, D. (2012). *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Edizione rivista), Frontline Books.
- [6] Kahn, D. (2014). *How I Discovered World War II's Greatest Spy and Other Stories of Intelligence and Code*, CRC Press.
- [7] Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday Books. Tr. it. (1999). *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, Rizzoli.
- [8] Bauer, C.P. (2013). *Secret History: The Story of Cryptology*, CRC Press.
- [9] Simmons, G.J. (Contributore principale) (2012). "Cryptology", *Encyclopedia Britannica Online*, <http://www.britannica.com/EBchecked/topic/145058/cryptology> (ultimo accesso maggio 2015).
- [10] Simmons, G.J. (a cura di) (1992). *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press-Wiley.
- [11] Paar C., Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioner*, Springer.

- [12] Martin, K.M. (2012). *Everyday Cryptography: Fundamental Principles and Applications*, Oxford University Press.
- [13] Fabris, F. (2001). *Teoria dell'informazione, codici, cifrari*, Bollati Boringhieri, 2001.
- [14] Kerckoffs, A. (1883). "La cryptographie militaire", *Journal des sciences militaires*, vol IX, n.1, 5-38 e n. 2, 161-191.
- [15] Vernam, G.S. (1926). "Cipher printing telegraph systems for secret wire and radio telegraph communications", *Journal of the American Institute of Electrical Engineers*, vol. 55, n. 2, 109-115.
- [16] Bellovin, S.M. (2011). "Frank Miller: Inventor of the one-time pad", *Cryptologia*, vol. 35, n. 3, 203-222.
- [17] Luvison, A. (2012). "Teoria dell'informazione, scommesse, giochi d'azzardo", *Mondo Digitale – Rassegna critica del settore ICT*, anno XI, n. 42, 1-16, http://mondodigitale.aicanet.net/2012-2/articoli/05_luvison.pdf (ultimo accesso maggio 2015). Id. (2012). "Quando la teoria dell'informazione gioca d'azzardo", *AEIT*, vol. 99, n. 10, 56-65. (Le due versioni dell'articolo differiscono marginalmente in pochi passaggi). Per un aggiornamento sintetico, cfr. Id. (2015). "L'azzardo di Shannon", *MIT Technology Review* (Edizione italiana), anno XXVII, n. 1, 52-53.
- [18] Sloane, N.J.A., Wyner, A.D. (a cura di) (1993). *Claude Elwood Shannon: Collected Papers*, IEEE Press.
- [19] Shannon, C.E. (1949). "Communications theory of secrecy systems", *Bell System Technical Journal*, vol. 48, n. 4, 656-715, ristampato in [18], 84-143.
- [20] Massey, J.L. (1992). "Contemporary cryptology: An introduction", in [10], 1-39.
- [21] Hinsley, F.H., Stripp, A. (a cura di) (1993, ristampa 2001). *Codebreakers: The Inside Story of Bletchley Park*, New York: Oxford University Press.
- [22] Copeland, B.J. (a cura di) (2004). *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life; Plus the Secrets of Enigma*, Oxford University Press.
- [23] Hodges, A. (1991). *Storia di un enigma. Vita di Alan Turing (1912-1954)*. Nuova edizione (2014). *Alan Turing. Storia di un enigma*, Bollati Boringhieri.
- [24] Smith, M. (2013). *Bletchley Park: The Code-breakers of Station X*, Shire Publications.
- [25] Rejewski, M. (1981). "How Polish mathematicians deciphered the Enigma", *IEEE Annals of the History of Computing*, vol. 23, n. 3, 213-234. (L'articolo contiene due commenti finali – il primo di Cipher Deavorus, esperto crittanalista, il secondo di Jack Good, collaboratore di Turing a Bletchley Park).
- [26] Alexander, C.H.O'D. (circa 1945). *Cryptographic History of Work on the German Naval Enigma*, The National Archives – Government Communications Headquarters GCHQ, Reference HW 25/1, <http://www.ellsbury.com/gne/gne-000.htm> (ultimo accesso maggio 2015).

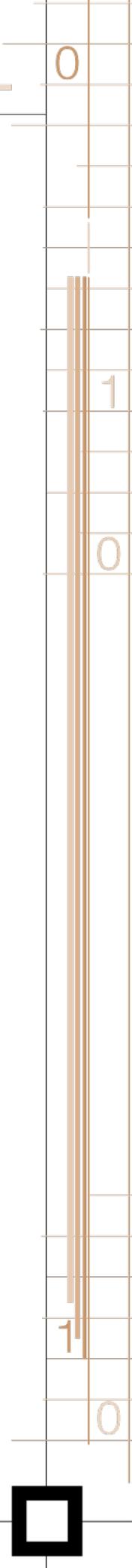
- [27] Copeland, B.J. *et al.* (2010). *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, Oxford University Press.
- [28] McGrayne, S.B. (2012). *The Theory That Would Not Die: How Bayes' Rule Cracked the Enigma Code, Hunted Down Russian Submarine, & Emerged Triumphant from Two Centuries of Controversy*, Yale University Press.
- [29] Miller, A.R. (1995). "The cryptographic mathematics of Enigma", *Cryptologia*, vol. 19, n. 1, 65-80.
- [30] Ratcliff, R.A. (2003). "How statistics led the Germans to believe Enigma secure and why they were wrong: Neglecting the practical mathematics of cipher machines", *Cryptologia*, vol. 27, n. 2, 119-131.
- [31] Ratcliff, R.A. (2006). *Delusions of Intelligence. Enigma, Ultra, and the End of Secure Cyphers*, Cambridge University Press.
- [32] Welchman, G. (1997). *The Hut Six Story: Breaking the Enigma Codes* (Seconda edizione rivista), Classic Crypto Books.
- [33] Good, I.J. (1979). "Studies in the history of probability and statistics: XXXVII A. M. Turing's statistical work in World War II", *Biometrika*, vol. 66, n.2, 393-396. Ristampato, con un ampio commento di Good, in Britton, J.L. (a cura di) (1992). *Collected Works of A.M. Turing: Pure Mathematics*, North Holland, 207-223.
- [34] Luvison, A. (2013). "Apologia della ragione scientifica", *Mondo Digitale – Rassegna critica del settore ICT*, anno XII, n. 45, 1-28, http://mondodigitale.aicanet.net/2013-1/articoli/05_LUVISON.pdf (ultimo accesso maggio 2015).
- [35] Luvison, A. (2014). "Apologia della ragione scientifica – II: strumenti per decidere", *Mondo Digitale – Rassegna critica del settore ICT*, anno XIII, n. 55, 1-32, http://mondodigitale.aicanet.net/2014-7/articoli/03_Apologia_della_ragione_scientifica_II.pdf (ultimo accesso maggio 2015).
- [36] Zabell, S. (2012). "Commentary on Alan M. Turing: The applications of probability to cryptography", *Cryptologia*, vol. 36, n. 3, 191-214.
- [37] Hénin, S. (2014). *Come le violette a primavera. Storia dei molti personaggi e delle molte idee che contribuirono alla nascita dell'innovazione più incisiva del XX secolo: il computer*, AICA.
- [38] Mezzalama, M., Lioy, A., Metwalley, H. (2013). "Anatomia del malware", *Mondo Digitale – Rassegna critica del settore ICT*, vol. XII, n. 47, pp. 1-20, http://mondodigitale.aicanet.net/2013-3/articoli/02_Anatomiadelmalware.pdf (ultimo accesso maggio 2015).
- [39] Gardner, M. (1977). "Mathematical games: A new kind of cipher that would take millions of years to break", *Scientific American*, vol. 237, n. 2, 120-124.
- [40] Winnefeld, J.A., Jr., Kirchoff, C., Upton, D.M. (2015). "Cybersecurity's human factors: Lessons from the Pentagon", *Harvard Business Review*, vol. 93, n. 9, 86-95.

- [41] Price, R. (1984). "A conversation with Claude Shannon: One's man approach to problem solving", *IEEE Communications Magazine*, vol. 22, n. 5, 123-126. Estratto da "Oral history: Claude E. Shannon", Interview # 423 conducted by Robert Price for the IEEE History Center, 28 July 1982, http://www.ieeeahn.org/wiki/index.php/Oral-History:Claude_E._Shannon (ultimo accesso maggio 2015).
- [42] Kahneman, D. (2012). *Pensieri lenti e veloci*, Mondadori.
- [43] Gigerenzer, G. (2015). *Imparare a rischiare. Come prendere decisioni giuste*, Cortina.
- [44] De Mauro, T. (2011). "Scienze inumane e scienze inesatte?" in Lingiardi, V., Vassallo, N. (a cura di), *Terza cultura. Idee per un futuro sostenibile*, il Saggiatore, 102-108.
- [45] Temes, G., Solymar, L. (2015). "In defense of engineering education", *Proceedings of the IEEE*, vol. 103, n. 8, 1243-1246.
- [46] Hilton, P. (2000). "Reminiscences and reflections of a codebreaker" in Joyner, D. (a cura di), *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, Springer, 1-8.
- [47] Kahn, D. (1984). "Cryptology and the origins of spread spectrum", *IEEE Spectrum*, vol. 21, n. 9, 70-80. Ristampato in [6], 135-163.
- [48] Bennett, W.R. (1983). "Secret telephony as a historical example of spread-spectrum communications", *IEEE Transactions on Communications*, vol. COM-31, n. 1, 98-104.
- [49] ISO/IEC 2382 – 16 (1996). *Information Technology – Vocabulary – Part 16: Information Theory*.

Biografia

Angelo Luvison è ingegnere elettronico dal 1969 (Politecnico di Torino) con successivi perfezionamenti in teoria statistica delle comunicazioni al MIT e management aziendale all'INSEAD-CEDEP di Fontainebleau. Per oltre trent'anni in CSELT, ha svolto e coordinato ricerche in teoria delle comunicazioni, reti di fibre ottiche ad alta velocità, società dell'informazione. È stato professore di *Teoria dell'informazione e della trasmissione* all'Università di Torino. Ha ricoperto la posizione di segretario generale dell'AEIT. È stato consulente per la formazione permanente dei dirigenti industriali. Detiene sette brevetti ed è autore, o coautore, di quasi 200 articoli, uno dei quali è stato ripubblicato (2007) nel volume celebrativo *The Best of the Best* della IEEE Communications Society. È *Life Member* dell'IEEE. Si occupa tuttora di temi di innovazione e formazione per l'ICT.

Email: angelo.luvison@alice.it



Digital-to-physical

l'evoluzione del marketing per il retail 2.0

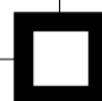
Ilaria Baroni, Marco Nalin, Marco Abitabile,
Francesco Nigro, Marco Mosconi

Sommario

Attraverso lo sviluppo di tecnologie sicure e alla portata di tutti si sta oramai assistendo da anni all'affermazione dello shopping online come l'effettivo strumento di compravendita del futuro. Rispetto al retail tradizionale offre diversi vantaggi, tra i quali la capacità di fornire virtualmente qualsiasi cosa a prezzi abbordabili (accorciando la catena di distribuzione ed i costi in pubblicità e costruzione del marchio) in modo veloce e immediato. I vantaggi oltretutto non sono solo per l'acquirente ma anche per il venditore: la rete dà la possibilità di conoscere meglio i dettagli delle visite dei propri clienti, come il numero di visualizzazioni per oggetto, quali oggetti sono in lista di osservazione, da quali siti proviene il cliente, quanto tempo ha dedicato a valutare l'acquisto, quanto spende in media il cliente, quali sono gli abbinamenti di prodotti più venduti e così via.

Il retail tradizionale attualmente conserva ancora la fetta più grossa del mercato, in parte grazie alla possibilità di vedere e scegliere di persona i prodotti e in parte grazie alla possibilità di relazionarsi con persone reali, perché in caso di problemi il cliente sa che può rivolgersi agli addetti o ai responsabili del negozio. Tuttavia, sul lato informativo, il gap tra retail digitale e fisico è ancora lontano dall'essere colmato.

In questo articolo verranno presentate tecnologie emergenti per l'analisi del comportamento della clientela nel retail tradizionale, che permetteranno nei prossimi anni raggiungere la stessa ricchezza informativa oggi a disposizione solo nel mondo digitale, adattata e ottimizzata per il mondo reale.



Abstract

Through the development of safe and affordable technologies, we are watching from years the consolidation of the shopping online concept, as effective trading way for the future. Compared to the traditional retail, it offers several advantages, including the ability to virtually provide everything fast and affordable (by shortening the supply chain and costs in advertising and brand building). The advantages are not only for the buyer but also for the seller. The networks gives the opportunity to learn more about the details of the visits of each customers (e.g., the numbers of views per object, witch objects are in observation list, from witch site the customer comes, how much time did you take to evaluate the purchase, how much is the average of orders for each customer, which are the best-selling combinations, etc).

The traditional retail still has the lion's share of the market, due to the possibility to see and choose products in a real environment, and to the possibility to be able to talk with real people in case of problems. However, on the information side, the gap between real and digital retail is still far from being bridged.

This article will present the emerging technologies for customer behavior analysis in traditional retail, which will allow in the coming years to reach the same wealth of information that now is available only in the digital world.

Keywords: Retail 2.0, Customer Analytics, Big Data processing, Key Performance Indicators, innovative marketing tools, omni-channel

1. Physical-to-Digital: lo shopping online, strategie e strumenti per conoscere e fidelizzare il cliente

Negli ultimi anni internet ha rivoluzionato profondamente il modo di fare shopping, introducendo modelli di business diversificati e aprendo al mercato globale business che prima erano locali. Con il diffondersi degli smartphone, dei sistemi di pagamento veloce e sicuro, e della connettività disponibile ormai ovunque, molti negozi hanno cominciato a migrare verso lo shopping online, che permette di potersi interfacciare ad un più ampio bacino di utenza rispetto al giro di clientela che passa davanti alle proprie vetrine.

In questo caso i fruitori dei negozi non vengono stimolati dalle classiche insegne, ma esiste un sistema più ampio per incuriosire, interessare e fidelizzare il cliente, partendo dalla pubblicità online, alle offerte personalizzate sui gusti del cliente, all'associazione di servizi e prodotti, e così via.

I percorsi di acquisto degli internauti vengono studiati e registrati, per classificare gli utenti in base alla loro provenienza. Un secondo livello di profilazione viene registrato in base all'analisi del sito di e-commerce stesso: vengono mappati gli articoli o le pagine più viste, i percorsi, gli acquisti, le "wish list", gli oggetti tenuti d'occhio. Un terzo livello di profilazione avviene poi quando l'utente diventa cliente, procedendo all'acquisto: c'è l'effettivo inserimento dati per la creazione del profilo utente, con la relativa acquisizione di informazioni sulla classificazione del cliente (sesso, età, indirizzo e altri dati anagrafici).

L'inquadramento della propria clientela e dei visitatori permette ai negozi online di poter offrire servizi personalizzati ai propri clienti, promozioni e di fare ricerche di mercato più accurate data la vasta disponibilità di dati.

2. Il gap informativo del retail tradizionale

Il retail online e quello tradizionale, nonostante gli scopi simili, hanno attualmente approcci completamente diversi. Il negozio tradizionale riesce sempre ad offrire indubbi vantaggi, come la possibilità di supporto di commessi, toccare e vedere la merce e poter avere immediatamente dei prodotti acquistati. Di contro il commercio tradizionale ha una serie di vincoli piuttosto rigidi che ne regolano il funzionamento [1]:

- Necessita di commessi;
- Opera solo in alcuni orari;
- Richiede un luogo per la compravendita, staff, espositori, inventari, ecc.
- Non condivide informazioni con i competitor;
- Si basa sul business tradizionale, che dipende dalla frequenza della zona da parte di nuovi e vecchi clienti.

Molti negozi "fisici" stanno rivedendo il loro concetto di marketing, procedendo a piccoli passi. Esempi di nuove modalità di contatto con la propria clientela sono messaggi o mail promozionali, il sito internet sempre più social (spesso una pagina di Facebook direttamente), pubblicità online e wifi gratuito.

A prescindere dai cambiamenti in atto nei negozi, il bisogno fondamentale che si deve soddisfare è quello di capire e conoscere la propria clientela, specialmente in periodi di crisi e di cambiamento, quando è fondamentale interpretare e rispondere alle nuove necessità che emergono. In un articolo [2] apparso su KnowThis vengono citate le 7 principali preoccupazioni per i retailers. Al primo posto troviamo proprio la soddisfazione del consumatore: questo vuol dire che anche i commercianti capiscono che il successo del negozio si basa sulla fedeltà del cliente, e che devono tenerne in considerazione il livello di soddisfazione per pianificare strategie e costruire relazioni durature. In seconda e terza posizione ci sono l'acquisizione e la presentazione dei prodotti: saper scegliere la propria merce ed esporla in modo accattivante è indispensabile per il buon funzionamento del negozio. Il quarto punto è lo studio del traffico del negozio, e infine, il layout del negozio e il luogo nel quale viene aperto.

Lo shopping online ormai è in grado di raggiungere e conoscere la propria clientela, anticipandone gusti e desideri. Per sopravvivere lo shopping tradizionale deve fare lo stesso, ma le barriere sono significative in questo senso. Il retail online nasce con una ricchezza informativa già digitalizzata importante, ma lo shopping tradizionale può basarsi solo sui dati del venduto, su contapersone poste agli ingressi dei negozi (che però non discriminano per età, sesso, etnia) e al massimo sulle carte fedeltà o su programmi estemporanei.

Inoltre lo shopping online può beneficiare di strumenti di analisi molto potenti e spesso gratuiti (per es. Google Analytics, Google Ad Words, Google Trends), di cui il retail tradizionale non riesce a beneficiare. Nelle sezioni successive verrà presentato come lo scenario stia cambiando e come tecnologie sempre più usabili e accessibili possano colmare questo gap.

3. L'evoluzione degli strumenti di monitoraggio: dai conta persone ai sistemi di visione artificiale

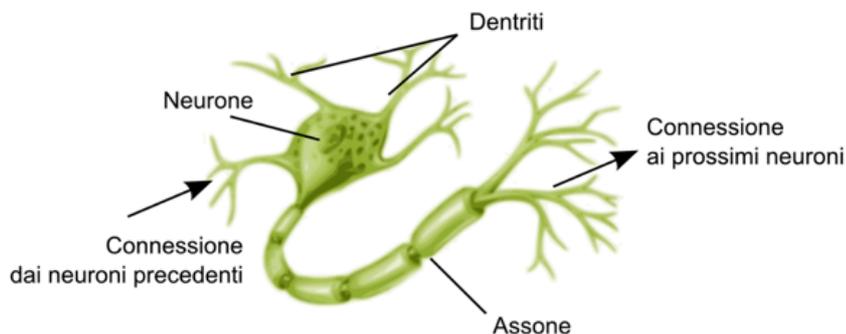
I conta persone posti all'ingresso dei negozi sono ormai una presenza fissa per tutte le catene di abbigliamento, accessori, elettronica, telefonia e molto altro.

Spesso queste soluzioni di monitoraggio sono derivate da sistemi di sicurezza preesistenti, come le barriere anti-taccheggio usate per impedire furti di merce, oppure, sempre ai fini della sicurezza e in conformità dell'Art. 13 del Codice in materia di protezione dei dati personali (d.lgs 196/03), sistemi di videocamere. Questi sistemi di videosorveglianza implementano software per il riconoscimento automatico di comportamenti sospetti, furti, infrazioni in aree vietate.

Un'altra possibilità di monitoraggio degli utenti è offerta dagli smartphone degli acquirenti, i quali possono essere rilevati tramite l'accesso a reti WiFi libere, oppure utilizzando alcuni particolari pacchetti per l'esplorazione di reti wireless necessari per la connessione. Questi sistemi hanno in realtà potenzialità incredibili per quel che riguarda anche l'analisi dei comportamenti dei clienti non solo in termini di sicurezza, ma anche per capirne preferenze, necessità, problemi come eventuali code alle casse, pattern di acquisto e addirittura demografia.

Tali software si basano principalmente sull'uso delle reti neurali artificiali, un modello matematico che trae ispirazione dalla strutturazione fisica della rete neurale che compone il nostro cervello (come rappresentato nella Figura 1). Attraverso la modellizzazione di neuroni, dendriti e assoni è possibile realizzare reti matematiche in grado di apprendere comportamenti, il che permette appunto di riconoscere oggetti all'interno di un'immagine, tracciarne i movimenti, determinarne la natura. In particolare esistono vari modi di far apprendere alla rete come comportarsi davanti a nuovi dati, una delle tecniche maggiormente utilizzate è l'apprendimento per rinforzo, sia positivo sia negativo. Vengono forniti alla rete una grande quantità di campioni di cui si conosce la natura e si invia un rinforzo positivo nel caso in cui la rete sia stata in grado di riconoscere l'oggetto, un rinforzo negativo in caso di errore. Questo permette alla rete di rinforzare o allentare i legami fra i neuroni, in un processo del tutto simile a quello che avviene nel nostro cervello quando facciamo nuove esperienze.

Connessioni neurali nei vertebrati



Rete neurale artificiale

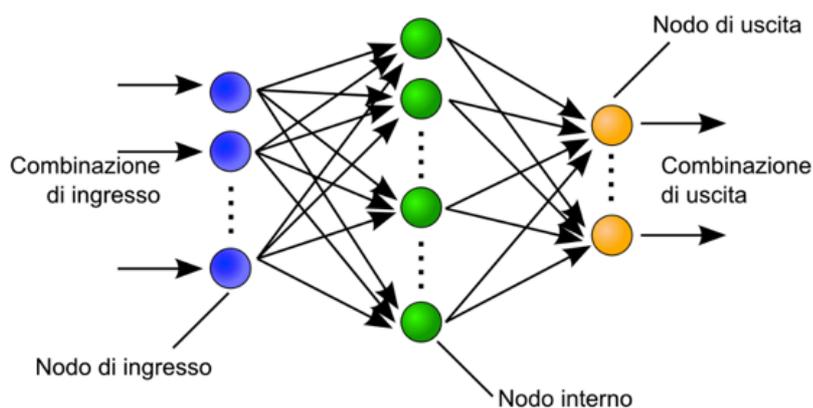


Figura 1

Paragone tra connessione neurale naturale e rete neurale artificiale

Nonostante questo potente strumento matematico, che ci ha permesso di affrontare nuove entusiasmanti sfide, l'argomento del riconoscimento di oggetti e comportamenti da tracce video è ancora oggetto di una intensa ricerca. In un articolo [3] viene fatta una disamina interessante degli sviluppi e delle strategie per l'analisi video in questo campo, descrivendo soluzioni per il tracciamento degli oggetti, l'analisi del movimento, l'analisi del comportamento, la biometria per l'identificazione di soggetti umani e la comprensione del loro comportamento. Nell'articolo vengono elencate anche le principali difficoltà che si trovano quando si realizzano questi algoritmi, tra cui le variazioni nell'illuminazione, il cambio di inquadratura, la dimensione degli oggetti in prospettiva, i cambi di orientamento, e vengono elencate alcune possibili strade utilizzate per risolvere questi problemi.

Un approccio interessante è presentato in una pubblicazione [4], in cui dati raccolti dalle telecamere sono stati usati anche per l'analisi dell'interazione tra clienti e prodotti ed è stato stimato il livello di interesse verso i prodotti stessi.

Kröckel e Bodendorf in un loro articolo [5] propongono alcuni approcci per l'analisi di dati raccolti da telecamere a infrarossi (in particolare è stato utilizzato uno strumento derivato dal mondo videoludico, un controller Kinect di Microsoft, interessante testimonianza di come i videogiochi siano vettore di innovazione tecnologica soprattutto nel campo dell'informatica) per l'analisi di questi comportamenti: per il tracciamento laterale delle persone viene usato un algoritmo proposto da Dalal e Tiggs che usa un istogramma di gradienti orientati; per il tracking dal soffitto, viene proposto l'approccio di Bradski che utilizza un algoritmo di adattamento continuo della media degli spostamenti; per l'analisi degli spostamenti hanno utilizzato un algoritmo chiamato DBSCAN (density-based spatial clustering of applications with noise), mentre i movimenti tra le aree sono stati modellati con catene Markoviane che mostrano la probabilità di transizione e quindi i percorsi più probabili tra le aree di interesse.

Anche Sicre e Nicolas nel loro articolo [6] propongono un confronto tra vari metodi per capire il comportamento umano, in cui le azioni vengono rappresentate con Motion History Image (MHI), Accumulated Motion Image (AMI), Local Motion Context (LMC) e Interaction Context (IC). Nella pubblicazione viene descritto come vengano utilizzate Support Vector Machines (SVM) per classificare le azioni e come la combinazione di LCM e IC sia la migliore per l'identificazione di comportamenti di acquisto in tempo reale, almeno per gli scenari che hanno esplorato.

Chern Hong Lim et al. [7] considerano come le logiche fuzzy possano essere usate per l'analisi dei movimenti delle persone per l'identificazione di azioni di basso livello, medio livello e alto livello. Le logiche fuzzy sono logiche in cui sono espressi più gradi di verità e non solo due (vero o falso) come nella logica classica. In qualche modo possiamo dire che le logiche fuzzy tengano conto che alcune variabili aleatorie possono essere "in parte vere" o "in parte false".

Una volta eseguito correttamente il riconoscimento delle persone e delle loro azioni, rimane il problema di fondo di assegnare un significato a quelle azioni nel contesto nelle quale sono avvenute; questa se possibile, è una sfida ancora maggiore rispetto al semplice riconoscimento e tracciamento degli oggetti in un immagine.

Uno strumento matematico utilizzato per affrontare questo problema è quello della statistica Bayesiana, punta ad includere vari gradi di credibilità rispetto alla veridicità di uno stato.

Tramite esperimenti nel loro shop lab, ricercatori di Philips [8] hanno proposto un modello Bayesiano per i comportamenti degli acquirenti, in cui si distingue tra un livello di sensoristica (che include i dati generati), un livello di caratteristiche (o "features", che includono una astrazione dei dati raccolti, come ad esempio: direzione, velocità, pause, sguardo verso prodotti), e un livello comportamentale (dove si distingue tra i tipi di acquirenti in base ai diversi comportamenti). Le probabilità di ciascun ramo del modello bayesiano è stata calcolata basandosi su una raccolta dati effettuata proprio con soggetti di test nel living lab di Philips.

Un approccio simile di attribuire una semantica ai dati provenienti dalle video camere di un negozio è stato fatto anche da Sicre e Nicolas [9], e anche se il test è stato fatto su video pre-registrati, i risultati sembrano promettenti.

L'analisi dei comportamenti in un negozio non può tenere conto solo dei movimenti o dei gesti identificati, ma deve anche considerare le sfere sociale, affettiva e psicologica delle persone coinvolte nel processo di acquisto. In questo senso una proposta interessante è stata formulata da Cristinani et al. [10], proponendo una teoria chiamata SSP (Social Signal Processing), che investiga principalmente aspetti non verbali, dei quali la maggior parte attuati in modo inconsapevole dagli acquirenti.

L'ultima sfida che ci attende è la ricerca delle correlazione fra tutti i dati ottenibili da questi sensori: infatti riuscire a capire quanto determinate variazioni di uno o più parametri condizionino le abitudini del cliente è ancora delegato all'analisi umana. Tuttavia le più recenti tecniche di data mining ci stanno iniziando a svelare correlazioni fino ad oggi impensabili e siamo solo all'inizio di questo lungo viaggio.

4. L'evoluzione degli strumenti di analisi: dal Cloud Computing all'analisi di Big Data

Uno scenario di afflusso continuo nel tempo di dati provenienti da una quantità elevata di sensori in un numero elevato di negozi fa immediatamente capire quanto l'infrastruttura abilitante un servizio di raccolta ed analisi dati debba essere solida e affidabile. Questo capitolo vuole dare una panoramica di quali siano i più recenti strumenti e termini ricorrenti quando si parla di infrastrutture che sono destinate ad accogliere e gestire grosse moli di dati.

Fino ad una decina di anni fa una tale infrastruttura sarebbe stata difficile e costosa da realizzare, ma nell'ultima decina d'anni è comparso sulla scena informatica il paradigma del Cloud Computing, e negli ultimi anni si parla sempre più di Big Data, intendendo non solo la quantità di dati, ma anche le metodologie per gestirli e analizzarli.

Con Cloud Computing si indica un paradigma di erogazione di risorse e servizi informatici, caratterizzato dalla elasticità di fornitura degli stessi e dal poter essere utilizzati (e configurati) attraverso Internet. Tali risorse sono assegnate grazie a procedure semi-automatizzate, a partire da un insieme di risorse condivise e condivisibili anche da altri potenziali fruitori dei servizi ad esse associate.

Seppur il Cloud Computing abbia penetrato il mercato attraverso la nascita di numerosi servizi ai quali spesso l'ipotetico cliente si è trovato gratuitamente affiliato, tra le più interessanti opportunità offerte da tale servizio non vi è l'erogazione vera e propria del servizio, che piuttosto va considerata come il veicolo che giustifica il vero valore offerto dall'utilizzo di questo modello: la possibilità di raccogliere enormi quantità di dati che rappresentino il cliente, le sue necessità e desideri.

Per comprendere al meglio il sottile legame tra il dato e la profilazione del cliente dal punto di vista di business è necessario volgere l'attenzione a un altro modello che negli ultimi anni ha acquisito molti consensi tra le organizzazioni IT: i Big Data.

La definizione di una base di dati come "Big data" è stata piuttosto varia e mutabile nel tempo; gli approcci che hanno portato a definizioni accettate e comunemente condivise si sono focalizzate prevalentemente su due aspetti:

- dimensione in termini di memorizzazione dei dati;
- approcci all'elaborazione dei dati ed estrazione di conoscenza.

Nonostante questi aspetti risultino fortemente correlati tra loro, in prima battuta i Big Data sono stati considerati [11] come tali soprattutto in funzione del primo; basi di dati così ampie e complesse al punto che i tradizionali approcci per l'elaborazione dei dati risultino del tutto inadeguati.

Successivamente, altre definizioni [12] hanno considerato come determinante la questione più operativa legata ai dati, sottolineando la necessità di utilizzare tecniche di analisi predittive e estrazione di valore, piuttosto che la dimensione dei dati coinvolti, come cernita per la valutazione di un dato come appartenente alla categoria "Big Data".

La dimensione dei Big data risulta comunque essere un parametro di vitale importanza per l'individuazione di questa tipologia di basi di dati; soggetto a costante mutazione, dal 2012 spaziava da poche dozzine di terabytes ad alcuni petabytes di dati.

Questa continua crescita, un trend che pare non destinato ad arrestarsi, ha portato a considerare i Big Data come il principale campo di applicazione di un insieme di nuove tecniche e tecnologie per svelare il valore contenuto all'interno di un data set eterogeneo, complesso e di scala massiva.

Nel 2001, l'analista Doug Laney definì [13] il modello di crescita dei Big Data come tridimensionale (modello delle "3V"), in quanto determinato da 3 differenti caratteristiche:

1. volume;
2. velocità (di generazione dei dati);
3. varietà (intesa come eterogeneità delle fonti -strutturate e non-).

Col tempo tale modello si è esteso, andando ad aggiungere le seguenti caratteristiche:

4. variabilità (inconsistenza nel tempo e dovuta alla varietà);
5. complessità.

Alcune organizzazioni hanno adottato l'utilizzo di una quarta V [14] per indicare la "veridicità" dei dati, ossia la qualità dei dati intesa come potenziale informativo estraibile.

L'utilizzo di un modello del genere (esteso e non) per la definizione dei Big Data ha permesso di evidenziare le differenze [15] con la "business intelligence", per ciò che concerne la natura dei dati e l'utilizzo degli stessi: la business

intelligence utilizza la statistica descrittiva con dati ad alta densità informativa per misurare cose, rilevare tendenze, e così via, quindi fa uso di dataset di dimensione limitata, pulita e il cui comportamento aderisce a modelli predicibili; i big data utilizzano la statistica inferenziale e concetti di identificazione di sistemi non lineari per inferire leggi (regressioni, relazioni non lineari, ed effetti causali) da insiemi enormi di dati scorrelati, rivelarne rapporti e dipendenze ed effettuare previsioni di risultati e comportamenti.

Negli ultimi anni, le organizzazioni IT hanno iniziato a considerare il Cloud Computing come struttura di supporto per i propri progetti Big Data: dalla problematica di cosa e come persistere, i Big Data hanno iniziato a volgere l'attenzione alla valutazione di come ottenere analisi significative dagli stessi, che rispondano a reali esigenze di business.

I modelli di fornitura dei servizi di Cloud Computing, offrendo grande flessibilità, permettono ai sistemi informativi di valutare il migliore approccio per ogni richiesta di business attraverso la crescente maturità dei servizi, sia dal punto di vista infrastrutturale che come qualità del servizio; si è rinnovata quindi la percezione del Cloud Computing come acceleratore [16] del potenziale esprimibile dai Big Data.

5. Digital-to-Physical: la rivoluzione del retail tradizionale

Devin Weng, il direttore di Amazon Marketplace, in una recente intervista sottolinea come il retail tradizionale debba rimettersi completamente in gioco se vuole sopravvivere e come negli ultimi anni la tecnologia abbia destrutturato e talvolta sgretolato questa industria. Nonostante ciò "Shopping vuol dire sia intrattenimento che utilità", afferma, "e alle persone piace fare shopping". Per fornire però alti standard di servizio e mantenere al massimo l'efficienza, non è più possibile appoggiarsi agli attuali modelli di business. Il retail ha voci anche molto onerose nel budget del reparto marketing e avere la possibilità di ottimizzare i flussi di lavoro interni per aumentare l'efficienza, per Wang, è una via verso il successo.

La ricetta di Wang per il retail è composta da 6 ingredienti:

- **Oltre i dispositivi mobili:** nonostante il mercato mobile sia cresciuto (e crescerà) negli ultimi anni, non bisognerebbe concentrare tutti gli sforzi per costruire infrastrutture solo-mobili. Nei prossimi anni vedremo una moltitudine di altri oggetti, personali e non, invadere un negozio tradizionale: camerini intelligenti, touch screen sparsi per il negozio, per non parlare di smart watch e tanti altri gadget tecnologici che possono generare nuovi canali verso il cliente. Non sarà quindi necessaria una "mobile strategy" ma una "omnichannel strategy".
- **Nuove abilità:** costruire esperienze sempre più attrattive è estremamente importante. Molti retailers hanno speso molti dei loro anni a trovare la miglior esperienza attraverso un solo canale (il classico negozio fisico), ma ora capire come connettersi con i clienti attraverso ogni mezzo loro vogliono utilizzare – non il modo in cui il retailer vuole che loro si connettano, ma il modo in cui i clienti vogliono connettersi al retailer – è

tutta un'altra storia, e sono necessarie evidenti nuove capacità che i manager devono iniziare a cercare sul mercato del lavoro.

- **I dati come vantaggio competitivo:** in questo mondo sempre più interconnesso e sempre più ricco di offerte e prodotti, saper governare i propri dati è la chiave verso il successo. Anche se per un venditore poter offrire un vasto catalogo di prodotti può sembrare una grande offerta, l'acquirente può sentirsi travolto da troppa scelta e confondersi. Saper maneggiare i dati per proporre i prodotti giusti alla persona giusta è la chiave per la sopravvivenza.
- **Arte e scienza:** maneggiare dati è sia arte che scienza. Molto si dice sulla scienza, poco sull'arte di maneggiare i dati. Potremmo produrre infinite combinazioni di prodotti che potremmo proporre ai nostri clienti, e potremmo farlo nel modo più scientifico che esista. Nonostante ciò questa non è una strategia efficace. Mettere insieme persone che hanno lavorato direttamente sul campo, nei negozi, a diretto contatto con i clienti, con brillanti matematici, statistici e informatici, che analizzino i dati e sappiano seguire il giusto percorso di analisi, può tirar fuori idee ed intuizioni che si trasformano in azioni vincenti per il retailer.
- **Small Data dai Big Data:** secondo Weng non serve saper manipolare grandi moli di dati, o meglio non basta. Il punto fondamentale per un'azienda è entrare in contatto direttamente con ogni cliente. Deve essere visto come un rapporto 1-1 per il cliente, che non sia intrusivo, fastidioso ed artificiale. Alla fine, si tratta di Small Data.
- **Ispirazione dall' e-commerce:** il vantaggio dell'e-commerce è che puoi sapere di tutto sui tuoi clienti, il mondo è semplificato e ogni attività è tracciata. Ogni processo all'acquisto può essere perfezionato e ottimizzato, esistono strumenti per la ricerca mirata e in pochi istanti sei già al prodotto che cercavi, senza intoppi. Il mondo fisico, dal suo canto, ha un elemento importante: l'incertezza, il caso, quello che consente ad un potenziale cliente di vagabondare per un negozio alla ricerca di qualcosa che ancora di preciso non sa cosa sia, "ci si fa un'idea", poi si acquista. Il futuro del commercio deve poter prendere il meglio dai due mondi.

6. Il confine tra la conoscenza dei propri clienti e la privacy dei cittadini

La gestione della privacy dei consumatori è una tematica attualmente molto discussa, che dev'essere contestualizzata anche in questo settore. La raccolta di dati personali, o la presenza di telecamere in negozi deve seguire la normativa a riguardo e deve rispettare le libertà della persona, per cui di seguito si tratteranno i più comuni esempi di politiche da adottare a riguardo.

Per risolvere i potenziali problemi relativi alla privacy la soluzione più ovvia è dare il controllo al consumatore dei propri dati: la privacy è una delle maggiori preoccupazioni quando si parla di Big Data. Inoltre i media hanno portato alla

luce questa tematica, facendo notare l'eccesso in alcuni metodi di recupero dati, causando inevitabilmente una crescita nella preoccupazione dei consumatori.

Per ovviare alla criticità dell'utilizzo di dati personali, lo studio dei sistemi per il retail viene fatto cercando di anonimizzare il più possibile le informazioni: il dato dev'essere a livello di popolazione o sotto-popolazione (per es. maschi teenagers) e non far riferimento al singolo individuo. Il sistema dev'essere in grado di riconoscere pattern comportamentali, tipologia di utenza (età, sesso, etnia) e le correlazioni degli acquisti con questa, senza entrare nel merito di dati che renderebbero il cliente riconoscibile. Dove invece viene visto fondamentale correlare il dato personale con le altre informazioni, la modalità ideale è quella che prevede un vantaggio di qualche tipo per il cliente (per es. essere punti, sconti, offerte mirate) ed ottenere il suo consenso esplicito all'uso e al trattamento del dato. La gestione della privacy deve evolversi di pari passo con l'evolversi delle tecnologie, non inibendo un processo innovativo in atto, ma neanche violando i diritti fondamentali dei cittadini. Una soluzione definitiva non esiste, ma una buona strada è quella di puntare a dare al consumatore il controllo e la gestione dei propri dati. Le formule "opt-in" o "opt-out" possono venire in aiuto alle aziende, consentendo ai consumatori di decidere se i propri dati debbano essere raccolti per offrire loro servizi a valore aggiunto o no, quali di questi dati lasciare a disposizione, e decidere per cosa possono essere usati. E' importante convincere il consumatore a fidarsi a lasciare i propri dati personali, tramite la trasparenza sulla raccolta dati e i dettagli delle modalità di utilizzo, alimentando la fiducia e la collaborazione e facendo capire che queste informazioni contribuiranno a migliorare l'offerta di prodotti e servizi al cliente stesso [17].

L'approccio del cliente sta in effetti mostrando un'apertura in questo senso, come osservato in un sondaggio di MarketingLand [18], che rileva come i consumatori siano disposti a cedere i propri dati personali in cambio di benefici o se lo ritengono utile.

7. Business Intelligence: le opportunità offerte per il marketing 2.0

Le grandi aziende hanno a disposizione moltissime opzioni per l'analisi dei propri dati, spesso però si paralizzano, scegliendo solo un approccio. E' arrivato oramai il momento di investire del tempo per ricercare il miglior strumento, o insiemi di strumenti, che possa trasformare grandi colossi impacciati in fresche ed agili imprese, pronte a saltare sul prossimo trend che emergerà dal mercato.

E' indubbio che l'offerta sul mercato stia divenendo sempre più vasta per quel che riguarda i prodotti di analisi, e stanno fornendo ai manager di mezzo mondo una potente arma da fuoco per aumentare la crescita e spingere verso MROI (Marketing Return Of Investment) sempre maggiori. Un recente studio condotto su più di 400 aziende [19] in tutto il mondo mostra come avere un sistema di analisi integrato che possa considerare ogni aspetto dell'azienda e, soprattutto, del cliente, possa liberare indicativamente il 15-20% delle spese di marketing, che si traduce in 200 miliardi di dollari che le aziende possono reinvestire o semplicemente risparmiare.

Un altro prerequisito per migliorare il MROI è capire e conoscere i comportamenti d'acquisto dei propri clienti. Il comportamento è cambiato così tanto negli ultimi anni che utilizzare vecchi modelli come il "marketing funnel" (o "teoria dell'imbuto") non genera più gli aspetti desiderati. Mentre la teoria dell'imbuto cerca di concentrarsi sull'esposizione del marchio, ora il cliente deve essere trattato non più come "uno della massa" ma come un preciso individuo che ha il suo proprio "percorso decisionale d'acquisto". Il concetto di percorso decisionale d'acquisto riconosce il fatto che il processo all'acquisto è molto più dinamico e complesso e soggetto a molti differenti momenti di influenza e la semplice esposizione al brand non è sufficiente.

Come già accennato, i dati raccolti sugli acquisti dei clienti nel retail sono molto meno ricchi ed articolati di quelli che si possono raccogliere con gli acquisti online e di conseguenza l'idea che ci si fa del processo decisionale d'acquisto è più vaga e fumosa. Avere uno strumento d'analisi che sia in grado di gestire questa incertezza e sappia integrare informazioni da altre fonti può permettere di maneggiare i dati a disposizione al punto tale che approcci di analisi avanzati - come il MMM (Marketing Mix Model), l'RCQ (euristica Reach-Cost-Quality) e l'Attribution Modeling - possono essere presi in considerazione.

Mentre si pianifica la messa a punto del Marketing Mix per la prossima strategia di marketing, è facile cedere alla tentazione di allocare risorse per iniziative che generano alti ROI (Return Of Investment) in breve tempo, sperando nel fatto che arrivino tanti dati dai clienti quando li si coinvolge in attività brevi ed estemporanee (per esempio registrazione per newsletter, promozioni su smartphone o prodotti in sconto e così via). Tuttavia gli effetti di attività di breve periodo impattano sul 10-20% delle vendite mentre il brand, un valore di lungo termine, attira il rimanente 80-90%. Le scelte di business devono essere fatte consapevolmente e a partire da dati scientificamente stabili per poter produrre un marketing-mix capace di prendere in considerazione tutte e due le facce della medaglia.

Per un retailer "digitalizzare" l'azienda significa mettere in atto il marketing 2.0. Questo però richiede un grande sforzo, non tanto economico, quanto mentale. Pensare in ottica "marketing 2.0" significa cambiare punti di vista, mettersi in discussione e mettere in discussione teorie fino a ieri funzionanti ed efficaci. Utilizzare strumenti di analisi Big Data significa un riassetto dell'azienda. Il reparto marketing inizia sempre più a lavorare con il reparto IT e nuove figure ibride in grado di abbracciare i due mondi iniziano a diventare fondamentali da inserire nell'organigramma aziendale. Non basta rastrellare dipendenti sparsi qua e là per l'azienda: serve creare un vero e proprio "centro d'eccellenza".

White paper e articoli sull'efficacia dei Big Data oramai si trovano ovunque, molti di questi inneggiano ad una vera e propria rivoluzione. Inoltre i primi risultati di alcune grandi aziende (come Google o Amazon) convincono giorno dopo giorno nuovi dirigenti in altri settori e in altre industrie. A seguito di un incontro tra i principali leader dell'analisi di dati, a cavallo fra il 2013-2014 [20], si sono identificati questi punti principali che il nuovo assetto aziendale deve tener presente:

- Big Data e Analytics non sono eccessivamente enfatizzati senza una buona ragione, ma sono troppo semplificati: le prospettive che i senior managers hanno sui Big Data sono un vero problema. I Big Data Analytics possono portare ad un grosso impatto economico all'azienda, ma nonostante ciò le speranze del management cozzano con la realtà dei fatti e le capacità degli applicativi. Questa "poca preparazione" porta facilmente alla crescita di scetticismo qualora i risultati non siano quelli attesi.

Le aziende devono lavorare su due orizzonti: recuperare le piccole "prede" nel breve periodo e creare un volano per aver tempo per le strategie che genereranno valore a medio-lungo periodo. E' bene generare il giusto mormorio all'interno dell'azienda intorno ai risultati nel breve per permettere di acquisire una "fiducia collettiva". Le aziende possono anche trarre beneficio dal mondo degli open data, e trovare nuove correlazioni interessanti, proprio nel paradigma "Big Data".

- Ricercare i talenti e costruire un centro d'eccellenza: questo punto è estremamente valido quando si parla di big data analytics. Devono essere ricercati i migliori talenti e costruire team multidisciplinari che permettano ad ognuno di esprimere il meglio delle proprie capacità. Questi talenti devono essere "coccolati" in un ambiente che possa fornire stimoli a portar avanti il loro lavoro e a generare novità.
- Pensare all'adozione del sistema di analisi: senza una strategia di adozione nessun prodotto decolla. All'interno dell'azienda vige la stessa regola, soprattutto con prodotti complessi come possono essere quelli di big data analytics. Questi sistemi devono essere facili, belli da usare ed estremamente intuitivi. Immense schermate con decine di indici tutti ammassati non fanno altro che generare confusione agli occhi di un manager, che ha bisogno di un sistema pulito, chiaro e che mostri gli indici principali. Il manager più curioso o una persona più operativa devono avere la possibilità di addentrarsi fra le personalizzazioni e le impostazioni per andare oltre al classico cruscotto, ma è indubbio che senza un design intuitivo e funzionalità robuste non si avrà alcuna adozione da parte dei manager e, dunque, il fallimento del cambiamento verso il marketing 2.0.

I dirigenti e gli operatori "più anziani" devono cambiare inevitabilmente il loro approccio all'analisi del dato. Da un mondo guidato dalle intuizioni si sta andando verso un mondo pesantemente guidato dai dati e questo deve portare i dirigenti a porsi domande quali: "Come posso creare nuovo valore?" e "Come faccio a farmi trasportare verso i nuovi risultati che i dati mi segnalano?".

Andare contro questa rivoluzione può solo far del male. L'esperienza giocherà ancora a proprio vantaggio, laddove questa verrà usata come un ingranaggio di un sistema: i dati forniti dai nuovi sistemi di analisi possono far scattare nuove intuizioni e nuove ipotesi che possono essere re-iniettate negli stessi sistemi per creare esperimenti e iniziare a lavorare davvero basato sui dati reali.

Conclusioni

Il mondo digitale sta cambiando e crea ogni giorno nuovi canali e nuovi modelli di business che impattano pesantemente nel mercato del retail. Il consumatore è sempre più difficile da interpretare e da attirare verso un negozio fisico, quando l'online rende sempre più facile ed economico fare tutto da casa. L'articolo ha riportato una panoramica delle tecnologie che sono a disposizione anche del retail tradizionale e che sempre di più vengono usate per colmare il divario informativo tra i due settori.

In futuro non si assisterà alla vittoria dell'uno o dell'altro, ma sempre più i due modi di vendere verranno integrati in un continuum informativo, secondo quello che è il concetto dell'Omni-Channel¹, cioè una conoscenza del cliente attraverso "tutti i canali", dalla conoscenza in prima persona, alla presenza web, social network e così via.

¹ <http://omnichannel.me/what-is-omnichannel/>

Riquadro 1: Le aziende in Italia

Anche in Italia iniziano a comparire le prime aziende che producono le soluzioni di analisi del comportamento della clientela o quelle che le utilizzano. Da molti anni ormai le normali barriere anti-taccheggio fungono anche da contatori di persone entranti o uscenti dal negozio, anche se non tutte sono connesse e salvano questi dati né la loro evoluzione nel tempo. In aggiunta a questo, alcune aziende hanno iniziato a fornire un contatore anche dei passaggi esterni al negozio, per avere un confronto tra traffico passante e traffico entrante nel negozio. Un esempio nel campo dell'intimo è fornito dal gruppo Calzedonia (Calzedonia, Tezenis, Intimissimi, ecc.), che ha adottato già da qualche anno una soluzione del genere, fornita dalla Experian².

Altre aziende hanno iniziato a fornire soluzioni basate su telecamere, come Microlog³ o come la startup PathFlow⁴, che sono in grado di fornire informazioni demografiche e di occupazione degli spazi. Pathflow ha iniziato un progetto pilota⁵ con la catena di negozi di telefonia mobile TIM-Telecom, installando le proprie soluzioni che di fatto aggiungono alle informazioni dette in precedenza le heatmap (mappe "calde", ossia quali zone del negozio sono più frequentate e quali meno) e l'analisi di età e sesso dei clienti nei diversi momenti della giornata.

Un'azienda interessante nel panorama Italiano è DataCream⁶, startup nata ad inizio 2015, ma che fornisce una soluzione tecnologica che integra varie tecnologie diverse come fonti di dati e le aggrega in modo facile e chiaro per il negoziante. Oltre alle tecnologie elencate dalle aziende precedenti, propongono anche l'integrazione di scanner di onde elettromagnetiche nella banda dei 2.4GHz (includendo sia Bluetooth che WiFi) per riconoscere anche le frequenze con cui i dispositivi diventano visibili o "spariscono" dal radar, rilevando di fatto anche tassi di fedeltà dei clienti e stratificando la popolazione del negozio distinguendo i clienti, i dipendenti, i fornitori. DataCream inoltre integra dati provenienti dai software gestionali solitamente usati nei negozi (dai software per le casse a quelli per la gestione del magazzino), nonché sistemi esterni, come meteo, traffico stradale. Il sistema di aggregazione fornisce quindi non solo dati informativi di una certa situazione del negozio e la sua evoluzione nel tempo, ma anche la contestualizzazione dei dati per una loro corretta interpretazione.

Un ultimo tipo di aziende che va menzionato è quello delle aziende di consulenza per i retailer, che propongono soluzioni innovative. Un esempio è l'azienda Temera, che annovera tra i suoi clienti⁷ marchi di prestigio come Dolce&Gabbana, Bulgari, Versace, Gucci, e che di fatto non ha soluzioni proprie, ma interpreta l'esigenza dei clienti e propone loro soluzioni di selezionati partner tecnologici.

² <http://www.footfall.com/case-study/calzedonia-3/?lang=it>

³ <http://www.microlog.it/>

⁴ <http://www.pathflow.co>

⁵ <http://siamosoci.com/pathflow>

⁶ <http://www.datacream.com>

⁷ <http://www.temera.it/clients/>

Riquadro 2: La nuova normalità per l'azienda

E' fine mese. Oggi Giulio, gestore di un negozio di un importante marchio nazionale, come di consueto deve preparare un report da consegnare ai suoi responsabili con la sua valutazione dell'andamento delle attività del suo negozio. La catena di negozi ha da poco acquistato un sistema per l'analisi della clientela. In questo momento, però, solo alcuni negozi stanno beneficiando di questo sistema mentre altri, come il negozio di Giulio, ancora non hanno alcun modo per recuperare informazioni sul comportamento dei clienti, se non un semplice conta-persone all'ingresso. E' per questo che Giulio deve ancora preparare il report mensile in quanto è l'unico modo per responsabili della catena di avere visibilità sulle attività del negozio.

Giulio nel report sottolinea come il reparto donna stia ancora rendendo meno rispetto agli obiettivi e cerca di ipotizzare una soluzione. L'intuizione di Giulio è che, secondo il suo punto di vista, i capi di abbigliamento in esposizione non combaciano con i gusti della popolazione dei clienti. In particolare i prodotti hanno un target d'età molto più alto rispetto all'età media dei passanti. Per cercare di offrire dei dati in supporto a questa sua ipotesi, nel mese precedente Giulio ha chiesto ad un suo collega di sorvegliare l'area donna per un'ora al giorno, ogni giorno in orari differenti per due settimane. Il suo scopo era quello di raccogliere alcune informazioni che potessero sostenere le sue intuizioni. I dati emersi dall'indagine, effettivamente, sembrano dare supporto a Giulio, che decide di inserire nel report stesso queste informazioni.

I responsabili di catena si rendono conto che Giulio ha fatto un ottimo lavoro, e che quel negozio è il prossimo candidato per l'installazione del sistema di analisi dei clienti che il brand ha appena acquistato. Visto che l'area geografica dove è il negozio di Giulio è un'area strategica per il futuro, il mese successivo viene pianificata l'installazione del nuovo sistema di analisi dei clienti anche in quel negozio.

Durante le settimane successive all'installazione, Giulio è entusiasta. Non solo ha dato conferma alle sue intuizioni, ma sta scoprendo tantissime nuove informazioni delle quali lui stesso era completamente ignaro. Ad esempio ora può sapere quanto dura la visita degli acquirenti e dei non acquirenti, quali sono i prodotti più visti dai non acquirenti e quali invece quelli più visti, ma meno acquistati. Ha scoperto che nel reparto donna c'è un'alta percentuale di giovani nei giorni pre-festivi, e che le taglie acquistate non corrispondono alle classiche taglie che quei particolari clienti acquistano, facendo ipotizzare dei regali e rafforzando l'ipotesi che i prodotti in vendita non rispecchino l'età degli avventori.

Nei mesi successivi all'installazione Giulio è sempre più soddisfatto, come del resto lo sono i suoi responsabili. Le nuove prospettive aperte e la maggiore conoscenza dei clienti ha già fatto vedere dei miglioramenti (primo fra tutti nel settore donna, portando subito la direzione a sostituire i prodotti con un target più giovane). Le novità introdotte dal nuovo sistema sono molte e molto efficaci. Con il tempo il sistema ha imparato a riconoscere *come* i visitatori si comportano nel negozio, riconoscendo i pattern di spostamenti degli acquirenti sicuri, da coloro che stanno solo guardandosi intorno e dagli indecisi. Utilizzando un sistema di auricolari senza fili, il sistema in automatico è in grado di avvisare il responsabile che una persona girovaga indecisa in un reparto. Il Manager del negozio può quindi allertare un suo collega che prontamente va a controllare se effettivamente

la persona segnalata ha necessità di un addetto, migliorando così la qualità del servizio al cliente.

Le figure all'interno dell'azienda che possono beneficiare di questo sistema non sono solo il gestore del negozio e il responsabile di catena, ma anche coloro che lavorano al reparto marketing, i visual merchandiser e molti altri.

Laura, ad esempio, è stata incaricata dall'azienda di occuparsi dell'introduzione di una nuova linea di prodotti nei negozi. Laura deve valutare quali, quanti e dove posizionare i prodotti in ogni negozio, con l'obiettivo di fare il tutto esaurito il più velocemente possibile. Con l'aiuto del nuovo sistema di analisi della clientela, Laura seleziona per prima cosa quei negozi che hanno un bacino d'utenza allineato con il target della nuova linea prodotti. Valuta le quantità da inviare a ognuno in base alla vendita di prodotti simili nel periodo indicato e sfruttando il sistema di analisi per avere le proiezioni di vendita delle due settimane successive. Fatto ciò usa nuovamente lo strumento di analisi per modificare la disposizione degli espositori di ogni negozio e valutare l'impatto sulle vendite con l'introduzione del nuovo prodotto. Valuta differenti configurazioni fino a trovare la miglior collocazione per ogni negozio; il sistema ha aiutato Laura facendole vedere come i clienti si muoveranno nel negozio con il nuovo assetto e facendo vedere gli impatti sulle vendite di ogni tipologia di prodotto. Dei negozi selezionati in precedenza ne ha scartati tre, in quanto la simulazione ha dimostrato che l'introduzione della nuova linea avrebbe avuto un impatto negativo su altri prodotti che quei tre negozi vendono. Questo perché la popolazione dei clienti di quei tre negozi ha dei gusti leggermente differenti e con l'introduzione della nuova linea si sarebbe generato un conflitto fra le vendite. Una volta terminata l'analisi ha dato il via alle spedizioni, inviando la quantità corretta di prodotti ai gestori dei singoli negozi e invitando i rispettivi visual merchandiser a collocarli nell'area indicata.

Glossario

Attribution Modeling: è il processo di definizione di un insieme di azioni che contribuiscono in qualche maniera ad un risultato desiderato, nonché alla attribuzione di un valore a ciascuna di queste azioni. Il modello di attribuzione fornirà quindi una comprensione di quale combinazione di azioni ed eseguite in che ordine influenzerà il risultato finale (generalmente l'acquisto da parte di potenziali clienti).

Apprendimento per rinforzo: questa tecnica di programmazione si basa sul presupposto di potere ricevere degli stimoli dall'esterno a seconda delle scelte dell'algoritmo. Quest'ultimo intanto cerca di determinare una politica tesa a massimizzare gli incentivi cumulati ricevuti dall'agente nel corso della sua esplorazione del problema.

Big Data: è un termine sempre più usato che descrive grandi moli di dati, spesso anche eterogenei e destrutturati. Spesso viene usato per indicare non solo i dati stessi, ma anche le metodologie e strategie per gestirli, elaborarli e analizzarli in modo efficace e veloce.

Biometria: in questo caso la si osserva come applicazione al riconoscimento di soggetti. In un particolare tipo di sistema informatico, è la funzionalità che ha lo scopo di identificare una persona basandosi su una o più caratteristiche biologiche o comportamentali, confrontandole con dati e altre informazioni, tramite algoritmi.

Business Intelligence: è un termine molto usato che può riferirsi in generale sia ai processi di raccolta dei dati in un certo contesto o dominio e sia ai processi o tecnologie per analizzare i dati. Nell'articolo viene usato più con la seconda accezione.

Catene Markoviane: sono processi di Markov con spazio discreto, dove il processo di Markov è un processo stocastico nel quale la probabilità di transizione che determina il passaggio da uno stato di sistema dipende unicamente dallo stato precedente, e non da come si è giunti a tale stato.

Cloud Computing: paradigma di erogazione di risorse informatiche sia a livello infrastrutturale (archiviazione, potenza di calcolo, etc.), sia a livello di piattaforma (database remoti, web services, etc.), sia di software (e.g., email, fogli di calcolo, etc.), basato sulla scalabilità, sulla possibilità per l'utente di auto-configurarsi i servizi e sulla modalità di pagamento in base al consumo effettivo di risorse.

Data mining: la disciplina che studia come estrarre nuova conoscenza a partire da grandi quantità di dati.

Euristica Reach-Cost-Quality: è un modello quantitativo per valutare il costo ed il risultato di strategie di marketing, che funziona molto bene nelle predizioni future della spesa del marketing e del ritorno dell'investimento anche quando non ci sono molti dati disponibili.

Istogramma gradienti orientati: è un descrittore di caratteristiche usate in computer vision ed in elaborazione delle immagini per il riconoscimento di oggetti.

Logiche fuzzy: è una logica in cui si può attribuire a ciascuna proposizione un grado di verità compreso tra 0 e 1. Ha la caratteristica di essere polivalente, che la rende un'estensione della logica booleana.

Marketing funnel: tradotto letteralmente vuol dire "imbuto di vendita", ed è un modo (utilizzato sia online che offline) per definire il processo che va dalla visita di un cliente fino ad una vendita. L'immagine dell'imbuto fa capire in modo chiaro che ci sarà una decimazione all'interno dell'imbuto dei clienti, ad ogni step del processo di acquisto. Ad esempio: dato un grosso numero di persone che passano davanti ad un negozio, solo una percentuale entrerà nel negozio; di questi solo una percentuale vedrà un certo prodotto; di questi solo una certa percentuale lo proverà; infine di questi solo una certa percentuale deciderà di acquistarlo.

Marketing Mix Model: termine utilizzato nell'analisi statistica per stimare l'impatto di diverse tattiche di marketing (marketing mix) sulle vendite e di predire l'impatto di tattiche future.

0

1

0

1

0

Neuroni, Dendriti e Assoni: i neuroni sono cellule per lo più dotate di lunghi filamenti, con capacità di eccitarsi se stimolate da un impulso elettrico. Sono composti da un corpo cellulare (detto soma o pirenoforo) dal quale si diramano due tipi di prolungamenti: i dendriti e gli assoni.

Omnichannel strategy: con questo termine si indica un approccio multi-canale alla vendita di servizi e prodotti, che cerca di fornire un'esperienza continua ed uniforme per il cliente attraverso tutti i canali, siano questi siti web tradizionali, applicazioni mobile, applicazioni per tablet, radio, tv, cartellonistica, negozi fisici, etc. L'uniformità ricercata secondo questo approccio è sia nei contenuti che nella veste grafica e nell'esperienza utente.

Opt-in, opt-out: con questi termini si indica la possibilità di essere inseriti o cancellati da un servizio o sistema informatico. In particolare il secondo, opt-out, è utilizzato spesso quando si parla di privacy e della possibilità (non sempre ovvia) per un utente di richiedere la totale cancellazione di tutti i dati che lo riguardano.

Profilazione: come profilazione dell'utente, ci si riferisce all'insieme di attività di raccolta ed elaborazione dei dati relativi a utenti di servizi, per creare gruppi di comportamento, riconoscere abitudini, ecc. In ambito commerciale questa attività viene anche chiamata marketing mirato, usato anche per analisi di potenziali clienti.

Retail digitale: chiamato anche vendita online o online retailing, è il tipo di commercio elettronico utilizzato per raggiungere direttamente il cliente finale tramite internet.

Retail tradizionale: il termine inglese retail corrisponde alla parola italiana "distribuzione al dettaglio" e descrive la vendita di beni e di servizi da parte degli operatori commerciali ai consumatori o utilizzatori finali. Con il termine tradizionale si intende presso il punto vendita (sede fissa), che contiene al suo interno l'assortimento delle merci offerte ai clienti.

Retailer: con questo termine nell'articolo indichiamo qualsiasi negoziante nella vendita al dettaglio, includendo in senso lato anche i proprietari di negozi e i proprietari di catene di negozi.

Reti neurali artificiali: sono modelli matematici creati per rappresentare l'interconnessione tra elementi chiamati neuroni artificiali, ossia costrutti matematici che cercano di imitare le proprietà dei neuroni viventi.

Small Data: questo termine è usato in opposizione al termine "Big Data". Mentre i Big Data hanno una rappresentazione estesa della realtà, comprensibile ai computer, gli Small Data hanno una rappresentazione sintetica (spesso visuale, come grafici, report riassuntivi, etc.) comprensibili agli esseri umani.

Support Vector Machines: sono un insieme di metodi per l'apprendimento supervisionato per la regressione e la classificazione di modelli.

Wish list: termine internazionale per indicare la lista di cose che si vorrebbero comprare, come promemoria.

Bibliografia

- [1] Kaur, G., "Traditional Commerce vs E-Commerce". *International Journal of Management Science and Technology*, Vol 2, No 3, Year 2014. pp 334-340
- [2] Concerns of Retailers (2015). From Retailing Tutorial. KnowThis.com. Retrieved July 06, 2015 from <http://www.knowthis.com/retailing/concerns-of-retailers>
- [3] Ko, T., "A survey on behavior analysis in video surveillance for homeland security applications" *Applied Imagery Pattern Recognition Workshop, 2008. AIPR '08. 37th IEEE*, vol., no., pp.1,8, 15-17 Oct. 2008 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4906450&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D4906450
- [4] Popa, M.C.; Rothkrantz, L.J.M.; Shan, C.; Wiggers, P., "Assessment of customers' level of interest" *Image Processing (ICIP), 2012 19th IEEE International Conference on*, vol., no., pp.41,44, Sept. 30 2012-Oct. 3 2012 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6466790&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D6466790
- [5] Johannes Kröckel, J., Bodendorf, F., "Visual Customer Behavior Analysis at the Point of Sale". *International Journal on Advances in Systems and Measurements*, Vol 5, No 3 & 4, Year 2012. pp 163-168
- [6] Sicre, R.; Nicolas, H., "Shopping scenarios semantic analysis in videos" *Content-Based Multimedia Indexing (CBMI), 2010 International Workshop on*, vol., no., pp.1,6, 23-25 June 2010 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5529913&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D5529913
- [7] Chern Hong Lim, Ekta Vats, Chee Seng Chan, "Fuzzy human motion analysis: A review", *Pattern Recognition*, Volume 48, Issue 5, May 2015, Pages 1773-1796, ISSN 0031-3203, URL: <http://www.sciencedirect.com/science/article/pii/S0031320314004865>
- [8] Popa, M.; Rothkrantz, L.; Zhenke Yang; Wiggers, P.; Braspenning, R.; Caifeng Shan, "Analysis of shopping behavior based on surveillance system" *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*, vol., no., pp.2512,2519, 10-13 Oct. 2010. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5641928&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D5641928
- [9] Sicre, R., Nicolas, H., "Human Behaviour Analysis and Event Recognition at a Point of Sale" *Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on*, vol., no., pp.127,132, 14-17 Nov. 2010 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5673685&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D5673685

- [10] Marco Cristani, R. Raghavendra, Alessio Del Bue, Vittorio Murino, "Human behavior analysis in video surveillance: A Social Signal Processing perspective", Neurocomputing, Volume 100, 16 January 2013, Pages 86-97, ISSN 0925-2312, URL: <http://www.sciencedirect.com/science/article/pii/S0925231212003141>
- [11] Snijders, C.; Matzat, U.; Reips, U.-D. (2012). "Big Data': Big gaps of knowledge in the field of Internet". International Journal of Internet Science 7: 1-5.
- [12] Ibrahim; Targio Hashem, Abaker; Yaqoob, Ibrar; Badrul Anuar, Nor; Mokhtar, Salimah; Gani, Abdullah; Ullah Khan, Samee (2015). "big data" on Cloud Computing: Review and open research issues". Information Systems 47: 98-115.
- [13] Bayer, M.A., Douglas, L., "The Importance of 'Big Data': A Definition" (2012). Gartner. Retrieved 7 July, 2015 from <https://www.gartner.com/doc/2057415/importance-big-data-definition>.
- [14] Coyle, F., " Turning Big Data into Big Benefits ". Villanova University. Volume 25, Numero 10, Ottobre 2012. URL: <http://www85.homepage.villanova.edu/timothy.ay/TOP3090/8%20-%20Analytics/1%20-%20Big%20Data.pdf>
- [15] Delort, P., "Le Big Data, pivot de la transformation numérique et ligne de service de la DSI."(2014) Association Nationale des DSI. URL: <http://www.bigdataparis.com/presentation/mercredi/PDelort.pdf?PHPSESSID=tv7k70pcr3egpi2r6fi3qbjtj6#page=4>
- [16] "Big Data in the Cloud - Converging Technologies", Intel (2015). URL: <http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/big-data-cloud-technologies-brief.pdf>.
- [17] Consumers worry about privacy but still willing to share data (2014). aimia.com. Retrieved July 07, 2015 from <https://www.aimia.com/en/media-center/news-releases/viewer.html/en/consumers-worry-about-privacy-but-still-willing-to-share-data>
- [18] Sterling, G., "Survey: 99 Percent Of Consumers Will Share Personal Info For Rewards, But Want Brands To Ask Permission" (2015). <http://marketingland.com>. Retrieved July 07, 2015 from <http://marketingland.com/survey-99-percent-of-consumers-will-share-personal-info-for-rewards-also-want-brands-to-ask-permission-130786>
- [19] Bhandari, R., Singer, M., van der Scheer, H., "Using marketing analytics to drive superior growth" (2014). Retrieved August 20, 2015 from http://www.mckinsey.com/insights/marketing_sales/using_marketing_analytics_to_drive_superior_growth
- [20] Brown, B., Court, D., McGuire, T., "The data-analytics revolution", Retrieved August 20, from http://www.mckinsey.com/insights/business_technology/views_from_the_front_lines_of_the_data_analytics_revolution

Biografie

Ilaria Baroni è project manager presso Telbios S.R.L., a Milano, da Gennaio 2014. Si occupa di ricerche e sviluppi di nuove tecnologie per la telemedicina, con progetti in ambito Europeo. Coopera anche con il dipartimento di R&D di AB Medica S.p.A. con attività legate alla ricerca robotico-medicale. Si è laureata al Politecnico di Milano in Ingegneria Informatica (specializzazione in Robotica), dal 2010 al 2013 ha lavorato presso l'Ospedale San Raffaele, nell'unità "Innovazione e Ricerca nei Servizi alla Vita e alla Salute", cooperando a progetti di Robotica Cognitiva e Cloud Computing.

Email: ilathea@hotmail.com

Marco Nalin è Program Manager nel reparto di R&D dell'azienda di telemedicina Telbios S.R.L., a Milano. Si è laureato in Ingegneria Elettronica presso l'Università degli Studi di Padova nel 2005. Dal 2004 al 2012 ha lavorato presso l'Ospedale San Raffaele, nell'unità "Innovazione e Ricerca nei Servizi alla Vita e alla Salute", cooperando a svariati progetti legati alla tele-medicina, la maggior parte dei quali co-finanziati dalla Comunità Europea. Le sue competenze includono sistemi di monitoraggio remoto dei pazienti, applicazioni mobili per la salute, robotica cognitiva e Cloud Computing.

Email: marco.nalin@gmail.com

Marco Abitabile è Project Manager e Software Architect Specialist presso Telbios S.r.l. Si occupa dello sviluppo e gestione di progetti innovativi per la cura delle persone. In passato ha collaborato con Asahi Kasei Corporation per lo sviluppo dei sistemi di car-entertainment per Peugeot e Nissan, sviluppandone gli elementi di riconoscimento vocale. Ha lavorato inoltre come ricercatore presso il San Raffaele in progetti legati al Cloud Computing e Chirurgia Robotica. Attento osservatore delle dinamiche sociali, si diverte nello sviluppo di nuove tecnologie al supporto delle aziende per l'analisi Big Data nei settori B2C. Laureato in Ingegneria informatica con grandi passioni per la Robotica, l'Intelligenza Artificiale, Data Mining e il Marketing, crede che per poter mettere in atto un qualsiasi progetto che si trasforma in prodotto si debba intraprendere un percorso olistico e multidisciplinare.

Email: marco.abitabile@gmail.com

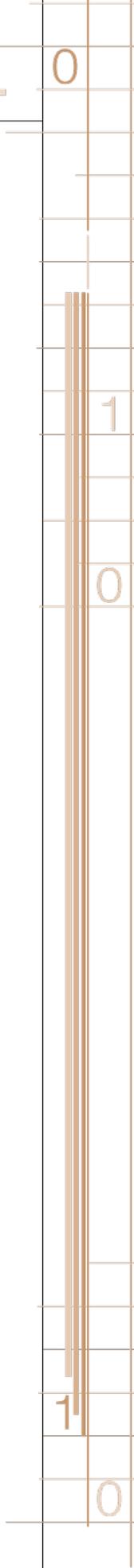
Francesco Nigro è ingegnere Informatico con molteplici esperienze di consulenza nella realizzazione di sistemi di calcolo distribuiti ad alte performance, nella creazione di traduttori e interpreti di linguaggi artificiali e nella progettazione e implementazione di architetture Self*. Coinvolto nella creazione del motore di backend per il provisioning di reti telefoniche/internet Enterprise per Ericsson. Ha realizzato molteplici sistemi di gestione Vending Machine in collaborazione con Ospedale San Raffaele, Rhea Vendor e Barilla. Attualmente impegnato nella realizzazione di architetture distribuite per l'archiviazione e analisi di dati clinici in Telbios S.r.l. Membro attivo della community per la progettazione e implementazione delle standard library in OpenJDK 9. Collaboratore del gruppo Chronicle per la realizzazione di servizi di storage ad alte performance e del progetto Open-Source JCTools per la

realizzazione di meccanismi IPC a basse latenze. Ha collaborato nello sviluppo del binding Java del protocollo di comunicazione per il database Time-Series InfluxDb.

Email: francesco.nigro@datacream.com

Marco Mosconi è Project Manager nell'unità di ricerca eServices4Life dell'azienda Fondazione San Raffaele, a Milano. Si è laureato in Ingegneria Informatica presso il Politecnico di Milano nel 2010. Si occupa di lavorare in progetti cofinanziati in ambito nazionale e internazionale, dove le sue competenze includono applicazioni web e mobile per la salute, robotica cognitiva e Cloud Computing.

Email: brus46@gmail.com



Musei e raccolte di storia dell'informatica in Italia

Silvio Hénin, Luca Cerri

Sommario

In Italia si contano più di cinquanta musei e collezioni di materiale informatico del passato, distribuiti su quasi tutto il territorio, che vanno da piccole collezioni private ai musei nazionali. Oltre alla raccolta e all'esposizione, molti di essi svolgono attività didattica, dimostrativa e di archeologia sperimentale. Con la collaborazione di AICA gli autori hanno svolto un'indagine tramite un questionario a cui hanno risposto 43 istituzioni. Nell'articolo si presentano i risultati e si esaminano alcuni aspetti critici, proponendo la creazione di un network che permetta visibilità, collaborazione e informazione.

Abstract

In Italy there are more than fifty museums and collections of vintage computer equipment, distributed over almost the entire territory and ranging from small private collections to national museums. In addition to collection and exhibition, most of them carry on teaching, demonstrations and experimental archeology. In collaboration with AICA, the authors conducted a survey through a questionnaire answered by 43 institutions. The article presents the results and examines some critical aspects, proposing the creation of a network to improve visibility, collaboration and information sharing.

Keywords: History of Computing, Museum, Vintage computer collections, Survey, Italy



1. Introduzione

"Si dice spesso che la tecnologia disumanizza. Non sono d'accordo, per la semplice ragione che l'uomo è naturalmente tecnologico: ovvero concepisce degli strumenti che a loro volta retroagiscono su di lui cambiandolo", così affermava lo scrittore ed epistemologo Giuseppe Longo in un'intervista rilasciata al quotidiano *Repubblica* nel 2013. Sembra quindi naturale che raccontare la nostra storia di specie umana non possa prescindere dagli oggetti artificiali che abbiamo creato. Se la tecnologia è una delle manifestazioni dell'essere 'uomo' fin dalle origini della specie, è negli ultimi tre secoli che si è assistito ad un suo sviluppo esponenziale. Questo rapido progredire delle conoscenze teoriche e delle tecniche applicative ha creato il bisogno di raccogliere le testimonianze sul suo svolgersi e sono così sorti i musei della scienza e della tecnologia ad affiancare le raccolte dei documenti scritti e quelle delle opere d'arte. Come afferma lo storico R. W. Seidel, «L'uso degli artefatti [storici] come fonte primaria può rispondere a domande cruciali circa il loro sviluppo». [1] Descrivere a parole un meccanismo, anche semplice, è spesso difficile, se non impossibile, mentre poterlo vedere e toccare direttamente, per quanto danneggiato esso sia, aiuta non solo a comprenderlo ma anche a ricostruire il percorso mentale che lo ha prodotto. Per concentrarsi sull'informatica, inoltre, M. M. Burnett, R. M. Supnik sottolineano che "Il costante e veloce progresso della tecnologia informatica provoca la rapida obsolescenza dei sistemi di elaborazione, della loro architettura e delle loro componenti fisiche. Raramente si percepisce il valore dei 'vecchi' sistemi, ma la loro perdita è significativa [...] La comprensione del passato del computer è vitale per la comprensione del suo futuro, e quindi il restauro funzionale dei manufatti storici, oltre alla pura conservazione, è un'attività importante per gli storici dell'informatica". [2]

L'informatica, come altre tecnologie moderne, ha avuto nel nostro paese un esordio piuttosto lento, ma, una volta introdotta, è stata adottata con grande velocità ed ha influenzato la società e l'individuo, l'economia e la politica, le professioni e i passatempi, come in ogni altro paese avanzato. In Italia, come nelle altre nazioni, sono nati musei di storia dell'informatica e molti entusiasti amatori hanno cominciato a collezionare esemplari di vecchie macchine, raccogliendole, conservandole e rimettendole in funzione, evitando la loro scomparsa nei depositi di rottami. A chi scrive è sembrato quindi opportuno raccogliere informazioni su queste piccole e grandi realtà, cominciando dalle semplici domande su quanti sono, dove sono, cosa raccolgono e cosa fanno.

2. Metodo

Nella prima fase di questo progetto si è svolta una ricerca sistematica tramite il motore di ricerca Google, impostando termini come 'museo', 'collezione', 'raccolta', 'computer', 'informatica', 'calcolo', 'calcolatrice', 'calcolatore', 'matematica', al singolare e al plurale, tra loro combinati in vario modo, utilizzando operatori booleani e la ricerca per frasi, come "museo del calcolo" o "museo del computer". Si è poi proceduto ad una prima analisi dei risultati ottenuti, eliminando le ridondanze e ottenendo così un elenco di 35 diverse entità delle quali si è esaminata la pagina web per ottenere maggiori informazioni. Solo in 25

casi si è recuperato un indirizzo postale, per gli altri si è rintracciato solo un indirizzo di posta elettronica. Ai primi è stata inviata una lettera su carta intestata di AICA e, contemporaneamente, a tutti è stato mandato lo stesso testo per email. In entrambe le comunicazioni si invitavano i destinatari a collaborare con l'iniziativa rispondendo ad un questionario. È stata nel frattempo predisposta una sezione del portale di AICA che ripropone il rationale dell'indagine e il questionario, compilabile online¹. Per favorire le risposte e limitare l'impegno chiesto ai partecipanti, il questionario si articola su sole 15 domande, alcune a scelta multipla, alcune a scelta unica e altre a risposta libera. Una prima sezione riguarda i dati anagrafici dell'istituzione. La seconda parte riguarda la collezione degli oggetti hardware e software. La terza sezione concerne le attività svolte in ambito espositivo, didattico, dimostrativo e sperimentale.

Il numero di indirizzi raccolti non era certo elevato e non tutti hanno risposto, ma grazie alle prime adesioni si è generato un 'passa parola' che ha portato gli autori a conoscenza di molte altre realtà che hanno risposto spontaneamente al questionario perché indirizzate da colleghi e amici. Si è così raggiunto un totale di 54 diverse entità, di cui 43 hanno compilato il questionario [vedi Riquadro]. Le rimanenti 11 sono state sollecitate una seconda volta via email, ma generalmente senza risposta; solo in due casi la mancata partecipazione è stata giustificata perché la collezione non riguardava specificatamente il calcolo automatico e/o per mancanza di risorse. Come si vedrà nei risultati, le situazioni sono molto variegate, si va dai grandi musei alle piccole raccolte private e, nel seguito di questo articolo, si è scelto quindi di usare collettivamente il termine 'collezione' per identificarle.

3. Risultati²

Il primo fatto che si evince dall'analisi delle 43 collezioni che hanno partecipato è la loro distribuzione sul territorio nazionale; esse sono presenti in 15 regioni, con una maggiore concentrazione nel Nord (60 %), soprattutto in Piemonte e in Lombardia. Si nota anche un maggiore presenza in località medio-piccole, con più della metà delle collezioni (56%) collocate in centri con meno di 100.000 abitanti. Anche la tipologia fornisce un panorama piuttosto eterogeneo: in più di un terzo dei casi (15/43) si tratta di collezioni private, seguite dalle associazioni (12/43) e, a grande distanza, da altri tipi di istituzioni, come musei, fondazioni, scuole e università. Nella grande maggioranza dei casi, si tratta di realtà di recente istituzione: 31 di esse sono nate dal 2000 in poi. Le attività svolte sono sempre molteplici, ma solo una minoranza (12/43) afferma di essere disponibile a concedere prestiti dei pezzi in collezione. D'altra parte, nel punto 8 del questionario, solo 28 affermano che la collezione è visitabile, mentre 33 dichiarano tra le attività svolte anche l'esposizione. L'apparente contraddizione

¹ Presentazione e questionario sono consultabili sul portale di AICA, alla pagina <http://www.aica.it/newscontestuali/indagine-collezioni-e-musei-italiani-storia-informatica/>

² I grafici dei risultati raccolti sono visibili sul portale di AICA, alla pagina <http://www.aica.it/newscontestuali/indagine-collezioni-e-musei-italiani-storia-informatica/>

(5 casi) potrebbe essere spiegata con la disponibilità a prestare i pezzi per esposizioni estemporanee.

La descrizione del posseduto delle collezioni è stata divisa in 15 diverse categorie di manufatti per quanto riguarda l'hardware e in 4 categorie per il software. Solo in tre situazioni la collezione comprende oggetti di tutte le categorie, mentre nella maggioranza dei casi si concentra su artefatti che vanno dalle calcolatrici meccaniche ed elettromeccaniche ai personal computer. Più di un terzo delle collezioni (16/43) conservano solo minicomputer, personal computer, calcolatrici da tavolo e da tasca e videogiochi, la tecnologia più comune in case ed uffici. Per alcune categorie i risultati sembrano stranamente elevati, ad esempio nel caso dei calcolatori analogici meccanici (12/43) e in quello dei calcolatori elettromeccanici (14/43). E' probabile che ciò sia dovuto all'ambiguità della descrizione che ha confuso i compilatori del questionario. Ad esempio, 'calcolatori analogici meccanici' voleva identificare macchine come gli analizzatori differenziali e 'calcolatori elettromeccanici' le macchine programmabili a relè. Entrambe le categorie erano poco rappresentate in Italia ed è molto improbabile che ne siano rimaste nelle collezioni. Più della metà delle raccolte conservano anche software, soprattutto sistemi operativi e programmi applicativi. Solo 26 collezioni (60,4 %) dichiarano di aver catalogato il posseduto, mentre molte dispongono di una biblioteca o di un archivio di documenti, in 11 casi aperti al pubblico. Altre informazioni interessanti derivano dalle risposte a testo libero. Alla domanda "Attività recenti" quasi la metà dei partecipanti (20/43) elenca corsi, conferenze, esposizioni estemporanee e pubblicazioni a stampa. In 11 casi si dichiarano prestiti temporanei e collaborazioni con eventi organizzati da altri enti o musei e in 8 casi si elencano anche attività di ricostruzione e ripristino di artefatti storici. Alla domanda "elencare artefatti rari o di particolare interesse storico", più della metà (22/43) elencano reperti che possono rispondere ai requisiti.

4. Conclusioni

Da questi primi risultati si evince che nel nostro paese esiste una situazione ricca e variegata: in quasi tutte le regioni italiane vi è almeno una collezione storica di materiale informatico, anche se spesso collocata in piccoli o piccolissimi centri e non sempre visitabile, ma anche quando non aperte al pubblico le collezioni permettono, tramite il prestito, l'organizzazione di mostre temporanee che attraggono visitatori.

A parte i maggiori musei istituzionali, gran parte delle collezioni sono nate dall'iniziativa di privati che hanno cominciato a raccogliere materiale informatico disponibile, a volte aggiungendolo a precedenti raccolte di macchine per ufficio (macchine da scrivere e calcolatrici) o di strumenti elettrici ed elettronici (telefoni, telegrafi, radio e televisori). La maggior presenza di calcolatrici da tavolo e personal computer è giustificabile con la grande disponibilità di questi artefatti, a sua volta dovuta alla loro vasta diffusione e alla rapida obsolescenza della tecnologia. La costante sostituzione di questi economici strumenti ogni pochi anni ha reso disponibile un gran numero di computer, periferiche e accessori (spesso ancora funzionanti) che possono essere acquisiti a costo

quasi nullo. Infine, queste categorie di materiale informatico godono anche del vantaggio di occupare poco spazio e di essere facilmente trasportabili nel caso di prestiti. Per contro, conservare i vecchi mainframe e le loro periferiche comporta problemi di trasporto e di spazio di magazzino che sono affrontabili solo da poche istituzioni.

Non pochi collezionisti si dedicano assiduamente e con passione alla rimessa in funzione dei vecchi computer, organizzando anche pubbliche dimostrazioni e partecipando a eventi internazionali che riuniscono gli 'archeologi sperimentali'. I risultati di questa attività hanno spesso un risvolto didattico di grande interesse che aiuta a penetrare i segreti di una tecnologia che per la maggior parte dei non esperti sembra ammantata di magia inesplicabile. L'archeologia sperimentale è meno critica per i microcomputer e i minicomputer a stato solido ed è facile che macchine degli ultimi 40 anni siano ancora funzionanti. Il limite più serio può essere la reperibilità del software, soprattutto dei sistemi operativi registrati su supporti magnetici (dischi, nastri) che difficilmente sono ancora leggibili: il grave problema noto come 'obsolescenza digitale'. Fortunatamente, la comunità italiana e internazionale degli appassionati è riuscita a recuperare e ha reso disponibile su internet non poco software 'd'annata' che può permettere di rimettere in funzione vecchie macchine il cui hardware sia ancora funzionante.

Degne di lode sono le tante attività didattiche che molte piccole e grandi istituzioni organizzano e offrono a scuole primarie e secondarie o al pubblico generico. Tra gli eventi segnalati nel questionario se ne trovano molti che dimostrano buone capacità organizzative e comunicazionali. In questi casi la collezione di oggetti, come dovrebbe sempre essere, riesce a prendere vita e a diventare spunto per un 'discorso' storico che aiuta le persone a capire il passato per meglio comprendere il presente, superando la nebbiosa banalità dello scontato quotidiano e della pubblicità interessata. Importante è anche la capacità di trasformare quella che può facilmente diventare una sterile 'storia' cronologica in un insieme di 'storie' vive, senza cadere nella tentazione di inventare leggende e miti da scoop giornalistico.

Molte delle entità esaminate sono dotate di biblioteche, emeroteche e archivi di documenti. I documenti scritti, infatti, sono la fonte essenziale per ricostruire la storia di un oggetto, senza la quale esso rimane 'muto' e non può essere apprezzato se non per le sue caratteristiche materiali e/o estetiche. La descrizione dell'artefatto dovrebbe comprendere non solo la sua origine e il nome del suo inventore/costruttore, ma anche la sua destinazione d'uso, il suo costo (un elemento piuttosto rilevante per gli aspetti sociali ed economici), la sua accettazione nell'ambiente lavorativo, il suo inserimento nella struttura organizzativa dove veniva usato, infine il percorso che lo ha portato a far parte della collezione. Certo, questa ricerca non è pensabile per ogni singolo pezzo, ma dovrebbe essere tentata almeno per quelli che sono diventati emblemi di un'epoca e quelli che hanno prodotto un'ondata di innovazione.

Un'altra considerazione che scaturisce dall'analisi dei dati raccolti riguarda la visibilità che le collezioni e le loro attività riescono ad ottenere in ambito nazionale o, almeno, regionale. Come si è visto, la distribuzione geografica

privilegia i piccoli centri con meno di 100.000 abitanti, non sempre raggiungibili con facilità. Oltre a ciò, notizie di manifestazioni, mostre temporanee, eventi didattici trovano una risonanza limitata ai circuiti locali. Queste carenze non possono essere certo imputate a cattiva volontà e neppure a incapacità degli organizzatori (trattandosi di raccolte di strumenti informatici, diamo per scontata la competenza in termini di media digitali di vario tipo), ma spesso sono attribuibili a mancanza di risorse e a difficoltà di relazione con il mondo dell'informazione di massa. Un ulteriore fattore critico, a cui bisognerebbe pensare, riguarda il futuro. La preponderante presenza di piccole collezioni private, gestite da uno solo o da pochi appassionati, fa sorgere una domanda: cosa succederà quando, per un qualunque motivo, questi appassionati non potranno più occuparsene? Le informazioni raccolte ci dicono che non stiamo parlando di poche vecchie calcolatrici e computer obsoleti immagazzinabili in una cantina o nella stanza di un appartamento, ma anche di collezioni che raggiungono le migliaia di pezzi e che necessitano di spazi di dimensioni industriali.

Infine, sembra opportuno ricordare che esistono altre realtà, non ancora esplorate dalla nostra indagine, che potrebbero contribuire a questo salvataggio della memoria storica. Ci riferiamo agli ambienti industriale, commerciale ed amministrativo che a partire dagli anni '50 hanno fatto ricorso alla tecnologia informatica per lo svolgimento delle proprie attività. Proprio in queste aree (manifatture, banche, assicurazioni, amministrazioni locali e nazionali, servizi pubblici) è forse possibile ritrovare altri oggetti da collezione, dimenticati nei magazzini, spesso troppo grandi e complessi per essere acquisiti da singoli privati. La loro esistenza non è certa: un'azienda privata non spreca certo costoso spazio per conservare strumenti obsoleti e questi vengono generalmente rivenduti o inviati alla discarica. Proprio in questi ambienti, però, si potrebbero ritrovare elementi ancor più importanti: i ricordi del loro impiego, le esperienze dell'impatto che i computer hanno avuto sulla vita aziendale e su quella dei lavoratori, i vantaggi conseguiti e le problematiche scaturite dalla loro introduzione. Sarebbe utile ed interessante intervistare, prima che sia troppo tardi, i personaggi che per il loro ruolo hanno vissuto in prima persona i cambiamenti e registrarne i ricordi, da conservare accanto alle macchine e ai documenti a stampa.

Le problematiche sopra esposte non vogliono essere una critica verso le attuali gestioni, che spesso agiscono senza alcuna garanzia di un'assistenza continuativa da parte di enti ed istituzioni, basandosi solo su risorse economiche personali e sull'aiuto di volontari, a tutti loro deve andare il nostro plauso e la nostra gratitudine per quanto hanno fatto e continuano a fare. Le considerazioni esposte vorrebbero piuttosto stimolare una riflessione e un'aperta discussione su quali concreti interventi siano ragionevolmente possibili per ovviare ai problemi più seri. A questo scopo, gli autori si propongono, con l'aiuto e il patrocinio di AICA, di organizzare un incontro nazionale tra tutti coloro che hanno contribuito all'iniziativa, anche al fine di creare una rete di comunicazione per lo scambio di informazioni e idee, la realizzazione di iniziative comuni e una maggiore visibilità presso il pubblico.

Ringraziamenti.

Gli autori desiderano ringraziare AICA, nelle persone di Giulio Occhini e di Franco Filippazzi, per la disponibilità e per il supporto dato a questo studio. Ringraziamo anche tutti i musei e i collezionisti che hanno partecipato all'indagine, non solo per le risposte, ma anche per i consigli dati e per aver fatto conoscere l'iniziativa ai loro colleghi.

Riquadro - Elenco delle collezioni che hanno risposto al questionario.

1977-1987 QUANDO IL COMPUTER DIVENNE PERSONAL, Roma (RM), <http://www.1977-1987.it>

ALL ABOUT APPLE MUSEUM, Savona (SV), <http://allaboutapple.com>

APULIA RETROCOMPUTING, Bari (BA), <http://www.apuliaretrocomputing.it>

ARCHIVIO STORICO E COLLEZIONE DEGLI STRUMENTI DI CALCOLO DELL'ISTITUTO PER LE APPLICAZIONI DEL CALCOLO 'MARIO PICONE', Roma (RM)

ASSOCIAZIONE BINARIO, Venaria Reale (TO), <https://www.facebook.com/associazionebinario>

ASSOCIAZIONE CASA MUSEO FAMIGLIA ALLAIRA, Castellamonte (TO), <http://www.casamuseofamigliaallaira.it/>

ASTUT - ARCHIVIO SCIENTIFICO E TECNOLOGICO DELL'UNIVERSITA' DI TORINO, Torino (TO), <http://www.unito.it/ateneo/strutture-e-sedi/musei-e-archivi/archivio-scientifico-e-tecnologico>

COLLEZIONE GIANGRANDI, Udine (UD)

COLLEZIONE PRIVATA DI CARLO RANDONE, Chivasso (TO),

COMPUTER MUSEUM - MUSEO DIDATTICO DI STORIA DELL'INFORMATICA, Padova (PD), <http://musi.fwtunesco.org/>

ComPVter, Cura Carpignano (PV), <http://www.compvter.it>

DECadence, Pesaro (PS), <http://www.decadence.it>

DIPARTIMENTO DI ELETTRONICA, INFORMAZIONE E BIOINGEGNERIA DEIB - POLITECNICO MILANO, Milano (MI), <http://www.deib.polimi.it>

HCK LUG, Pozzocco Di Bertiole (UD), <http://hckretro.com>

I.T. MUSEUM, Felonica (MN), http://www.itmuseum.it/_web/

KING COMPANY Srl, Gallarate (VA), <http://www.kingsrl.com>

LICEO SCIENTIFICO E CLASSICO STATALE "GIUSEPPE PEANO - SILVIO PELLICO", Cuneo (CN)

COLLEZIONE LUCA PIOTTO, Monfumo (TV)

MALIGNANIMUSEUM, ISIS A. Malignani, Udine (UD)

MATEUREKA - MUSEO DI INFORMATICA E STORIA DEL CALCOLO,
Pennabilli (RI), <http://www.mateureka.it>; www.mathmuseum.eu

MIAI - MUSEO INTERATTIVO DI ARCHEOLOGIA INFORMATICA,
Cosenza (CS), <http://www.verdebinario.org>

MUSEO DEGLI STRUMENTI PER IL CALCOLO, Pisa (PI),
<http://www.fondazionegalileogalilei.it/>

MUSEO DEL CALCOLATORE 'LAURA TELLINI', Istituto Tecnico
Economico e Professionale Statale "Paolo Dagomari", Prato (FI),
<http://museo.dagomari.prato.it>

MUSEO DEL COMPUTER, Camburzano (BI),
<http://www.museodelcomputer.org>

MUSEO DEL DIPARTIMENTO DI MATEMATICA E INFORMATICA,
Università di Parma, Dipartimento di Informatica, Parma (PR),
<http://museo.dmi.unipr.it>

MUSEO DEL PERSONAL ED HOME-COMPUTER, Livorno (LI),
<http://www.museopc.it>

MUSEO DELL'ITIS 'BLAISE PASCAL', Itt Blaise Pascal, CESENA (FC),
<http://www.itis-cesena.it>

MUSEO DELL'INFORMATICA FUNZIONANTE, Palazzolo Acreide (SI),
<http://museo.freaknet.org>

MUSEO DELL'INFORMATICA, Università di Bologna – Dipartimento di
Informatica, Bologna (BO)

MUSEO DI CASA MIA, Fermignano (PU), <http://www.bonasia.info>

MUSEO DI STORIA DELL'INFORMATICA, Verona (VR),
<http://stars.scienze.univr.it:8080/museo/mainpage.jsf>

MUSEO DIDATTICO DEL COMPUTER, Bassano Bresciano (BS),
<http://www.ulisse.bs.it/museo/index.htm>

MUSEO INTERATTIVO DEL CALCOLO - MIC, Sovigliana (FI),
<https://it-it.facebook.com/MIC-Museo-Interattivo-del-Calcolo-516421575105848/timeline/>

MUSEO MATEMATICA "I RACCONTI DI NUMERIA", Roma (RM),
<http://www.apav.it/mat/tempolibero/musei/numeria.htm>

**MUSEO NAZIONALE DELLA SCIENZA E DELLA TECNOLOGIA
"LEONARDO DA VINCI"**, Milano (MI), <http://www.museoscienza.org>

MUSEO PIEMONTESE DELL'INFORMATICA – MuPin, Moncalieri (TO),
<http://www.mupin.it>

MUSEO PUGLIESE DELL'INFORMATICA, Adelfia (BA), h
<http://www.supervinx.com/OnlineMuseum/>

MUSEO SCOLASTICO DELLA SCIENZA E DELLA TECNICA – ITET
Perugia, Perugia (PG), <http://www.itcperugia.it>

MUSEUM INSTRUMENTORUM CALCULI, Carignano (TO),
<http://museostrumenticalcolo.altervista.org/joomla/>

OSTIA BIT, Roma (RM), <http://museosalvacomputer.blogspot.it/>

PERCORSI STORICI DELL'INFORMATICA E DEL CALCOLO – PSIC, I.T.S. 'Alessandro Volta', Trieste (TS)

RETROCAMPUS, Rovato (BS), <http://www.retrocampus.com>

STORIAINFORMATICA.IT, Paternopoli (AV),
<http://www.storiainformatica.it>

Bibliografia

[1] R. W. Seidel, "Reconstruction, Historical and Otherwise: The Challenge of High Tech Artifacts", in: R. Rojas, U. Hashagen (a cura di), *The First Computers. History and Architectures*, MIT Press, 2000.

[2] M. M. Burnett, R. M. Supnik, "Preserving Computing's Past", *Digital Technical Journal*, vol. 8, n. 3, 1996.

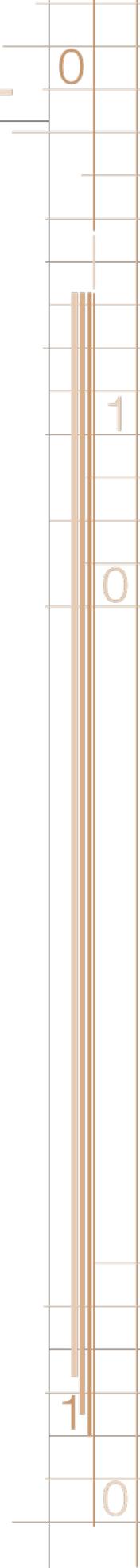
Biografie

Silvio Hénin è uno studioso di storia della tecnologia, in particolare del calcolo automatico. Consulente del Museo Nazionale di Scienza e della Tecnologia 'Leonardo da Vinci' di Milano, collabora con i periodici *Mondo Digitale*, *Le Scienze*, *Annals of the History of Computing* e ha curato numerose voci del *Dizionario Enciclopedico di Informatica, ICT e Media Digitali*, è anche Autore del libro "Come le violette a primavera" (AICA, 2014), una breve storia dell'informatica. E' socio dell'Associazione Italiana Calcolo Automatico e dell'International Federation for Information Processing.

Email: silvio.henin@aicanet.it

Luca Cerri ha iniziato a lavorare nel settore informatico nel 1974 presso lo stabilimento IBM di Vimercate. Ha poi proseguito la sua esperienza in Olivetti ed in altre multinazionali, dedicandosi al progetto e alla implementazione di sistemi software. Da qualche anno studia le vicende legate alla nascita, allo sviluppo e all'utilizzo del software, con l'obiettivo di documentarne l'evoluzione e l'impatto sulla società moderna. E' consigliere di ARASS-Brera (Associazione per il Restauro degli Antichi Strumenti Scientifici). E' socio di IEEE, di AICA e di ACM (Association for Computing Machinery).

Email: lucacerri@outlook.com



L'insostenibile leggerezza del C.I.O. Chief Information Officer, IT Manager, Digital Innovation Officer: quali profili e competenze per la sanità digitale? L'esperienza della e-HealthAcademy

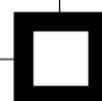
Roberto Bellini, Giuliano Pozza

Cosa emerge dal progetto sviluppato da AICA e AISIS sulla qualificazione dei CIO (Chief Information Officer) della sanità, i cui risultati vengono riportati nel libretto disponibile al seguente link:

http://www.aicanet.it/aica_cio/CIO-eHealthAcademy.pdf/view

Emergono tanti temi, ma ci sembra utile riassumerne tre in particolare:

1. La ricostruzione del contesto in cui si muove il CIO della sanità e di come viene percepito, non solo dal punto di vista organizzativo e istituzionale ma anche da quello dei singoli protagonisti e delle persone intorno a loro. A queste infatti è stato chiesto, durante un sondaggio, di descrivere secondo loro cosa fa un CIO in sanità. Le risposte sono state a volte profonde, spesso involontariamente umoristiche, sempre interessanti;
2. La verifica delle competenze possedute da ciascuno, analizzate nel dettaglio attraverso i questionari e il colloquio di validazione e restituzione. Il colloquio ha fornito ai CIO dei temi di riflessione su se stessi e sulle proprie competenze che, come emerge dalle testimonianze dei protagonisti riportate nel libro, hanno contribuito a una maggior consapevolezza e fatto emergere la necessità di definire un percorso di formazione personale consapevole e mirato;
3. La riflessione di ciascuno sul proprio posizionamento professionale, congiuntamente ai due giorni di formazione strutturata della SDA Bocconi, hanno generato un ulteriore livello di presa di coscienza rispetto alla necessità di mettere in atto scelte concrete che permettano, all'interno del proprio contesto professionale, di "agire" le competenze acquisite durante la formazione.



Potremmo dire che il percorso così articolato ha messo in moto un meccanismo di auto-diagnosi (self-assessment) e di auto-potenziamento (self-empowerment), che auspichiamo resti il vero risultato del percorso, al di là dell'obiettivo contingente della qualificazione. Ciascun candidato ha avuto infatti la possibilità di valutare i propri punti di forza e di debolezza professionali, grazie ad una metodologia da riapplicare in prospettiva per successive verifiche e da considerare come una esemplificazione di quello che ciascuno può fare anche in modo autonomo, nel momento in cui i vari componenti della qualificazione professionale saranno meglio padroneggiati.

Sul piano dell'auto-potenziamento sono emerse come tematiche su cui lavorare:

- La capacità di dominare la tecnologia e non considerarsene asserviti;
- La consapevolezza dei ruoli organizzativi e dei contesti istituzionali da cui si è influenzati e che bisogna imparare a diagnosticare e con cui interagire;
- La necessità di sviluppare obiettivi personali propri, possibilmente convergenti con quelli dell'organizzazione per cui si lavora;
- La misurazione delle proprie prestazioni tramite un'autovalutazione che sia compiuta dal soggetto CIO prima e comunque indipendentemente da quella della struttura organizzativa di riferimento da appoggiare ad una metodologia condivisa come e-CF *plus*. Solo con una misura della prestazione fatta in proprio si pongono le basi per il raggiungimento della piena consapevolezza sul proprio posizionamento, che potrà essere verificato con la direzione e/o con il supporto di un Assessor esterno.

Queste considerazioni presuppongono un'appropriata conoscenza delle proprie competenze secondo uno schema di classificazione condiviso, ottenuto attraverso uno strumento di rilevazione che permette il confronto fra diversi profili professionali e diversi livelli di capacità e prestazioni.

In questo contesto, è emerso chiaramente come il CIO sia sempre più chiamato a svolgere funzioni di "Governance complessiva dei servizi ICT", da erogare tramite infrastrutture sempre più eterogenee, con modelli di sourcing ibridi e in contesti organizzativi sempre più fluidi e complessi.

Cosa si può fare?

Nel concreto, alcune azioni possono e devono essere messe in atto rapidamente o potenziate se esistenti:

- Costruire percorsi di formazione per tutti coloro che hanno un ruolo di leader nei progetti digitali, siano essi appartenenti ai Sistemi Informativi che ad altre organizzazioni aziendali. Si tratta di quelli che vengono definiti gli "e-Leader". Per questi nuovi leader digitali, vanno pensati percorsi di formazione, sia universitari che post-universitari, che aiutino ad impostare e gestire il governo della tecnologia e innovazione digitale come priorità di management aziendale. Il percorso va velocizzato includendo anche facoltà tradizionalmente più caratteristiche del mondo sanitario (medicina, scienze infermieristiche...) e cercando di recuperare con Master o azioni

formative ad hoc i professionisti sanitari che vengono da un percorso "tradizionale", quindi molto distante da questi temi.

- Definizione di percorsi di crescita equilibrata delle componenti di servizio ICT. Uno degli errori più comuni, che in qualche modo è legato ad una carenza di governo o di visione architeturale e strategica, è quello di investire in modo "sbilanciato" solo su alcune componenti dell'architettura. Spesso si investe su nuove applicazioni, senza considerare che una infrastruttura tecnologica sicura ed abilitante è un pre-requisito necessario. In altri casi, si corre il rischio opposto, quello di investire enormemente in grandi "autostrade informatiche", su cui poi non circolano informazioni perché mancano le applicazioni. Dai dati disponibili emerge come i veri leader, ossia coloro che possono dimostrare un percorso di successo, abbiano gestito negli anni un corretto bilanciamento degli investimenti su diversi ambiti, dalle applicazioni ai dati, dalla tecnologia di base alla sicurezza.
- Dal punto di vista culturale e organizzativo, sarà sempre più necessario lavorare in modo integrato sulle competenze digitali, superando la tradizionale divisione tra "utenti" o "key users" che definiscono il bisogno e i requisiti, Direzioni Aziendali (Personale, Direzione Sanitaria, Servizio Qualità...) che intervengono sull'organizzazione e sui processi, manager che finanziano e professionisti ICT che progettano e realizzano le soluzioni tecniche. Questo modello in molti casi non è più applicabile nel contesto attuale.

In quest'ottica si inserisce l'azione di AISIS (Associazione Italiana Sistemi Informativi in Sanità) e AICA (Associazione Italiana per l'Informatica e il Calcolo Automatico), con il supporto di eSanita, Netics e di SDA Bocconi. L'iniziativa è stata denominata e-HealthAcademy: si tratta di un percorso rivolto inizialmente ai Direttori dei Sistemi Informativi o CIO, attuali e futuri, per potenziare le loro capacità di Governo, di Leadership e di Comunicazione. Il percorso attuale porta ad una "qualificazione delle competenze" secondo il framework internazionale e-CF, in coerenza con quanto previsto dalla norma UNI 11506. L'e-HealthAcademy dovrebbe nel prossimo anno svilupparsi con percorsi formativi ad hoc per professionisti e manager sanitari, in collaborazione con organizzazioni di categoria ed università.

Che risultati ci possiamo aspettare

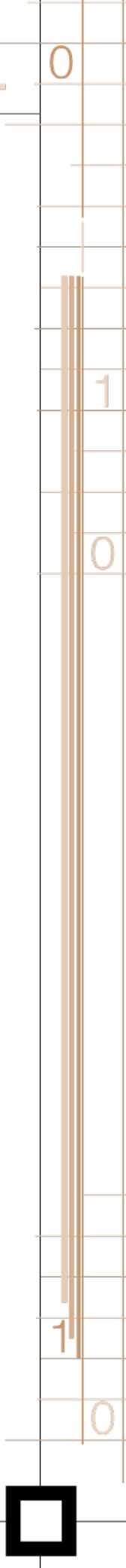
Certamente le possibilità di incidere sulle scelte strategiche della struttura sanitaria di appartenenza potranno non essere immediate, perché il percorso intrapreso è innanzitutto culturale e ogni percorso di questo tipo è un processo di cambiamento complesso che lavora su tempi lunghi.

In ogni caso, il singolo CIO può già da ora innescare tale processo, agendo su diversi fronti:

- Lavorando sulle proprie competenze, sia tramite i percorsi formativi proposti, sia stimolando il contesto professionale in modo che gli permetta di esercitare sul campo le competenze descritte nel profilo del CIO definito da e-CF;

- Aumentando le proprie capacità di comunicazione e di relazione con il top management, sia utilizzando strumenti “digitali” che “analogici” (un incontro e una buona conversazione faccia a faccia sono difficilmente sostituibili con altri strumenti), in quanto queste sono tra le competenze più critiche e spesso più carenti;
- Adottando e facendo entrare nella prassi del proprio team di lavoro metodologie di service management, di project management e di governance dei sistemi informativi;
- Innescando, a partire dai passi precedenti, un dialogo fecondo con il top management aziendale sui temi di IT Governance e di IT Strategy che, giova ricordarlo, non sono attività del CIO, ma una responsabilità del Board Aziendale a cui il CIO dà un contributo fondamentale.

Volendo andare al di là della figura del CIO, che pure ha costituito il focus di questo percorso, crediamo che tutti i professionisti ICT dovrebbero investire sul proprio percorso di costruzione professionale, non solamente a partire dalle competenze tecniche, pure indispensabili. Crediamo infatti che le competenze strategiche, metodologiche, relazionali e di comunicazione, così ben sottolineate dal framework e-CF, siano, seppure in maniera e gradazione diversa, indispensabili per tutti i profili dei professionisti dei sistemi informativi. Questo è forse, in sintesi, il più grande contributo di chiarezza che il percorso della e-HealthAcademy ci ha lasciato.



Cookie e Privacy: Come mettersi in regola?

Antonio Piva, Attilio Rampazzo, Maurizio Sala, Luca Spongano

Sommario

Il 2 giugno 2015 è scaduto il termine per dare attuazione alle prescrizioni del Garante Privacy in materia di cookie, così come contenute nel relativo Provvedimento emesso l'8 Maggio 2014.

È necessario che i gestori dei siti, al fine di determinare correttamente le modalità per adempiere alle nuove prescrizioni normative, individuino e classifichino i cookie utilizzati distinguendoli in base alla Provenienza (cookie di prima o di terza parte), alla loro permanenza sui terminali (cookie di sessione o permanenti) e alla finalità alla base del loro rilascio (cookie tecnici, cookie analitici con/ senza potere identificativo o cookie di profilazione).

È indispensabile poi, a seguito di questa classificazione, avere ben chiari gli adempimenti da mettere in atto, le relative modalità di attuazione ed i razionali che ne sono alla base: predisposizione di banner contenenti l'Informativa breve al fine di informare fin da subito gli utenti sull'utilizzo dei cookie; raccolta di un consenso preventivo all'installazione dei cookie e meccanismi per garantirne la relativa documentabilità; predisposizione di un'Informativa estesa e completa (c.d. Cookie Policy); Notificazione al Garante Privacy per l'utilizzo di talune tipologie di cookie.

Infine, è importante non trascurare l'ambito sanzionatorio, ricordando che la mancata esecuzione dei necessari adempimenti può dare luogo a sanzioni amministrative che possono raggiungere, in taluni casi, il pagamento di somme pari a centoventimila Euro.



Abstract

The final deadline for compliance to the Italian Data Protection Authority (DPA)'s cookie-law 8 May 2014, was the 2nd of June 2015.

In order to determine how to correctly comply to the new measures, website managers have to identify and classify cookies used by their sites according to their origin (first-party cookies or third-party cookies), the duration of stay on the user's terminal equipment (session cookies or persistent cookies) and purposes for which are installed (technical cookies, analytics cookies with/without identification or profiling cookies).

It is essential then, as a result of this classification, have to be clear of the requirements to be put in place, the method of implementation and the underlying rationale: set up banners for provide brief information to inform immediately the data subject about use of cookies; obtain a consent prior installation of cookies and mechanisms to ensure its documentability; prepare an extensive and complete Policy (also called 'Cookie Policy'); the Notification of the processing to the DPA for the use of certain types of cookies.

Finally, it's important to not overlook the scope of sanctions, pointing out that failure to follow the necessary requirements may result in administrative sanctions that can reach, in some cases, payment by a fine amounting to one hundred and twenty thousand Euro.

Keywords: Privacy, Cookie Law, Cookie Policy, Analytics cookies, Profiling cookies

1. Premessa

Preliminarmente ad una trattazione specifica dell'argomento in oggetto, è opportuno ricordare che gli obblighi in materia di cookie derivano da una normativa europea da ultimo modificata nel 2009¹ - e recepita in Italia con un decreto del 25 maggio 2012 - che ha imposto di informare gli utenti per l'utilizzo dei cookie di Internet ed acquisire un loro consenso preventivo. Il Provvedimento dell'Autorità Garante per la protezione dei dati personali (o Garante Privacy) dell'8 Maggio 2014, la cui definitiva adozione è stata preceduta da una consultazione pubblica², ha inteso meglio specificare gli adempimenti previsti dalla norma, lasciando ai relativi destinatari un anno di tempo per adeguarsi. Come previsto dal citato Provvedimento, il 2 giugno 2015 è scaduto il termine per dare attuazione alle prescrizioni del Garante Privacy in materia di cookie.

¹ Direttiva 2009/136/Ce del 25 novembre 2009, del Parlamento europeo e del Consiglio, recante modifica, tra le altre, della direttiva "e Privacy" (2002/58/Ce) relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

² Deliberazione del Garante Privacy recante "Avvio di una consultazione pubblica ai sensi dell'art. 122 volta ad individuare modalità semplificate per l'informativa di cui all'art. 13, comma 3, del Codice in materia di protezione dei dati personali" (Del. n. 359 del 22 novembre 2012, in Gazzetta Ufficiale del 19 dicembre 2012 n. 295).

Il Provvedimento in trattazione si è posto quindi l'obiettivo di individuare le modalità semplificate per rendere l'informativa online agli utenti per l'archiviazione dei c.d. cookie sui terminali da parte dei siti Internet visitati e, contestualmente, fornire idonee indicazioni sulle modalità con le quali procedere all'acquisizione del consenso degli stessi, laddove richiesto dalla legge.

Il presente articolo mira, quindi, a fornire una panoramica riassuntiva e in sintesi di quanto il Garante Privacy ha normato in materia di cookie e indicato nelle F.A.Q. e nei vari chiarimenti che si sono susseguiti successivamente all'emanazione del Provvedimento.

2. Classificazione dei cookie

I cookie (letteralmente "biscotti") sono piccoli file di testo che i siti o, meglio, i *web server* visitati dall'utente inviano al relativo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo terminale. La disciplina relativa all'uso dei c.d. "cookie" è da estendersi anche ad altri strumenti analoghi (a titolo esemplificativo *web beacon*, *web bug* o *clear GIF*³) installati nei terminali utilizzati dagli utenti (personal computer, notebook, tablet pc, smartphone, etc.).

Alcune operazioni non potrebbero essere compiute senza l'uso dei cookie, che, in alcuni casi, sono quindi tecnicamente sostanzialmente necessari: per esempio, l'accesso all'*home banking* e alle attività svolte sul proprio conto corrente online (visualizzazione dell'estratto conto, bonifici, pagamento di bollette, etc.) sarebbero molto più complesse da svolgere e meno sicure senza la presenza di cookie che consentano di identificare l'utente e mantenerne l'identificazione nell'ambito della sessione. I cookie possono poi essere usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni specifiche riguardanti gli utenti che accedono al server e di norma sono presenti in numero molto elevato.

I cookie possono rimanere nel sistema anche per lunghi periodi e possono contenere un codice identificativo unico: questo consente ai siti che li utilizzano di tenere traccia della navigazione dell'utente all'interno del sito stesso per finalità statistiche, pubblicitarie o per creare un profilo personalizzato dell'utente a partire dalle pagine che lo stesso ha visitato e proporre pubblicità mirata (c.d. *Behavioural Advertising*).

Nel corso della navigazione su un sito, l'utente può ricevere sul suo terminale anche cookie di siti o di web server diversi da quello direttamente visitato. Questo accade perché sulla pagina internet visitata possono essere presenti alcuni elementi come immagini, mappe, servizi, suoni, specifici link a pagine web di altri domini che risiedono su server diversi da quello sul quale si trova la pagina visitata. In altre parole, si tratta di cookie che vengono "importati" da un sito web diverso da quello che si sta visitando in quel momento (in questo caso si parla, come vedremo nel seguito, di cookie di "terze parti").

³ *Oggetti incorporati in una pagina web o in una e-mail, che discretamente (solitamente in maniera invisibile) consentono di verificare che un utente abbia avuto accesso al relativo contenuto.*

Esistono, quindi, varie tipologie di cookie che si possono distinguere in base alla Provenienza, alla Durata di permanenza sul terminale e alla Finalità.

In base ad una classificazione focalizzata sulla '**Durata**' si potranno avere:

Cookie temporanei o di sessione

non sono memorizzati in modo persistente, ma limitatamente alla durata della sessione di navigazione. Ciò significa che sono automaticamente cancellati dal terminale dell'utente una volta abbandonato il sito internet visitato e chiuso il browser di navigazione.

Cookie permanenti

sono memorizzati sul dispositivo dell'utente fino a quando non vengono cancellati da parte dell'utente o fino al raggiungimento della loro data di scadenza (se preimpostata). Non vengono quindi cancellati automaticamente dal dispositivo dell'utente quando questo abbandona la pagina internet consultata.

Facendo poi riferimento alla '**Provenienza**' si può parlare di:

Cookie di prima parte

sono i cookie rilasciati dal sito web visitato; il sito è quello corrispondente all'indirizzo digitato dall'utente (ovvero il dominio del sito web visualizzato nella finestra dell'*URL*).

Cookie di terza parte

sono i cookie rilasciati da un sito web diverso rispetto a quello visitato dall'utente e quindi non direttamente riconducibili al dominio indicato nel campo *URL* del *browser*.

Al riguardo è interessante notare come non esista alcuna differenza di tipo intrinseco tra un cookie di prima e di terza parte; la distinzione esiste solo nel contesto di una particolare visita ad un sito. Questo significa che il medesimo cookie può essere di prima parte in un momento e di terza parte in un altro momento. Per esempio, quando si visita *twitter.com*, il browser imposta vari cookie associati con il nome di dominio **.twitter.com*. Nel contesto della visita su Twitter questi sono cookie di prima-parte. Se poi si visita un altro sito o un altro dominio che prevede, per il suo tramite, l'installazione dei cookie da *twitter.com* che ricomprendono gli stessi cookie **.twitter.com*, a questo punto quel medesimo cookie andrà classificato come cookie di terza parte.

Infine, seguendo una classificazione basata sulla '**Finalità**', che, forse, è quella che più ci interessa in quanto si sovrappone alla classificazione di tipo normativo operata dal Garante Privacy, possiamo avere Cookie tecnici (al cui interno possono essere fatti rientrare i cookie analitici di prima parte o di terza-parte senza potere identificativo) e i Cookie di profilazione (al cui interno possono essere fatti rientrare i cookie analitici di terza parte con potere identificativo).

Cookie tecnici

sono definiti come quei cookie essenziali per navigare sui siti internet e per utilizzarne alcune funzionalità specifiche. Possono, a loro volta, essere suddivisi in:

- Cookie di navigazione/indispensabili/di performance/di sicurezza: garantiscono la normale navigazione e fruizione del sito web (permettendo, ad esempio, di realizzare un acquisto o autenticarsi per accedere ad aree riservate); se questi cookie vengono bloccati, i siti che li utilizzano potrebbero non funzionare più correttamente.
- Cookie di funzionalità/preferenze/localizzazione/di stato della sessione: permettono di memorizzare informazioni che modificano il comportamento o l'aspetto del sito (lingua preferita, dimensioni di testi e caratteri, area geografica in cui ci si trova). Se vengono bloccati, l'esperienza di navigazione può essere meno funzionale ma non compromessa. Questi cookie consentono ai siti di memorizzare le scelte che gli utenti operano (come ad esempio, preferenza della lingua) e fornire le funzionalità personalizzate selezionate, in modo da migliorare l'esperienza di navigazione. In alcuni casi, questi cookie possono essere utilizzati anche per offrire servizi on line (es. chat dal vivo) o per evitare che siano offerti agli utenti servizi che hanno rifiutato in passato.
- Cookie statistico/analytics di prima parte o di terza parte senza potere identificativo: sono cookie che generano delle informazioni sull'utilizzo del sito web da parte dei navigatori, tracciandoli in maniera aggregata. Limitatamente a quelli di terza parte possiamo citare i cookie installati per il tramite di *Google Analytics* (piattaforma di web analytics di *Google Inc.* che permette di raccogliere ed analizzare statistiche su come il sito viene "navigato" da parte degli utenti). Questi possono essere assimilati, in linea con la vigente normativa, ai cookie tecnici quando rispettano contestualmente le seguenti condizioni: (i) adozione di misure che riducono il potere identificativo dei cookie tramite il mascheramento di porzioni significative dell'indirizzo IP; (ii) espresso richiamo della terza parte all'impegno ad utilizzare tali cookie esclusivamente per la fornitura del servizio, a conservarli separatamente e a non "arricchirli" o a non "incrociarli" con altre informazioni di cui essa disponga (nell'account amministrativo di Google Analytics esistono, ad esempio, alcune impostazioni di 'condivisione dei dati' che possono essere modificate in tal senso). E' quindi il gestore del sito che deve procedere a settare e configurare l'uso dei cookie (per esempio aggiungendo un certo codice allo script della pagina in uso per procedere alla mascherature dell'IP in caso di utilizzo di Google Analytics). Tale obbligo non può essere evitato da parte dei gestori dei siti per esempio indicando all'utente all'atto dell'Informativa di procedere lui stesso all'attivazione di modalità tecniche tali da disattivare ed impedire l'installazione dei cookie. Si pensi, a titolo esemplificativo, al plug-in messo a disposizione da *Google Inc.* per "bloccare l'installazione di Cookie Analytics"; o, ancora, alle c.d. funzioni "do not track", che consentono all'utente di segnalare a ciascun sito visitato la sua volontà di essere o meno tracciato nel corso della

navigazione. Quest'ultima modalità, ancora oggi in fase di discussione all'interno degli organismi di standardizzazione internazionali, inizia ad essere resa disponibile su alcuni browser di ultima generazione, ma, non essendo per l'appunto standardizzata, non vi è la certezza che attraverso tale funzionalità i segnali e le richieste che l'utente invia ai server siano da questi effettivamente "ascoltate". O, ancora, la possibilità per l'utente di attivare la funzione di "navigazione anonima", ancorché questa non garantisca comunque un anonimato assoluto, utile a non mantenere i dati di navigazione nel browser, che continueranno a restare disponibili ai gestori dei siti web e ai provider di connettività.

Alla luce degli accorgimenti adottati, per l'utilizzo di tali cookie e per i trattamenti di dati personali ad essi connessi non è necessario, in forza di quanto previsto dalla disciplina vigente (art. 122 del Codice Privacy e Provvedimento del Garante dell'8 maggio 2014) richiedere il consenso. Tuttavia, dal momento che l'assenza del consenso riduce la consapevolezza dell'interessato, questa deve essere necessariamente fondata, come vedremo nel seguito, sull'andare a rendere un'Informativa chiara e di immediata comprensione.

A titolo esemplificativo - come chiarito anche dal Gruppo "Articolo 29"⁴ in un parere di qualche anno fa (*Opinion 04/2012 on Cookie Consent Exemption*) - sono cookie per i quali non è necessario acquisire il consenso preventivo e informato dell'utente quelli di sessione utilizzati per "riempire il carrello" negli acquisti online, quelli di autenticazione, quelli che consentono di fruire di contenuti multimediali come *flash player* se non superano la durata della sessione o, ancora, quelli di personalizzazione (che permettono, ad esempio, la scelta della lingua di navigazione).

Cookie di profilazione

Prendendo in considerazione l'altra categoria di cookie basata sulla "Finalità", ovvero quella relativa ai Cookie di profilazione, questi sono raggruppabili in:

- Cookie pubblicitari/ di advertising/ di tracciamento o delle conversioni/ di remarketing (es. utilizzo *Google AdWords*): questi cookie sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete, in base a ciò che è pertinente (annunci personalizzati). I cookie alla base di questa attività vengono quindi utilizzati per raccogliere informazioni sulle abitudini di navigazione dell'utente, al fine di offrire pubblicità rilevante in base alle preferenze e agli interessi dimostrati durante la navigazione. Essi sono inoltre utilizzati anche per limitare il numero di volte in cui viene visualizzata una pubblicità, in modo da rendere la comunicazione più efficace per il promotore e meno invasiva per l'utente. Si pensi a tutte le volte che visitando un sito di servizi, usando la propria *web mail* o accedendo alla propria pagina su un social network, troviamo banner pubblicitari legati

⁴ Il Gruppo, istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione europea.

alle nostre ultime ricerche effettuate sul web o all'ultimo acquisto fatto online. Questo accade perché quegli spazi web sono progettati per riconoscere il terminale collegato ed, eventualmente, indirizzare messaggi promozionali, per l'appunto, "profilati" in base alle proprie ricerche e all'utilizzo di Internet.

- Cookie statistico/analytics di terza parte con potere identificativo: sono cookie che servono a raccogliere informazioni e generare statistiche di utilizzo del sito web, per comprendere come i visitatori interagiscono con il sito. Questi cookie sono considerati ad alto valore identificativo quando non sono messe in atto, in contemporanea, le seguenti condizioni: (i) non sono adottate funzioni tali da ridurre il potere identificativo dei cookie (ad esempio tramite il mascheramento di porzioni significative dell'IP); (ii) la terza parte incroci le informazioni contenute nei cookies con altre di cui già dispone.

Per l'utilizzo di tali cookie (e per i trattamenti di dati personali ad essi connessi) è necessario, in forza di quanto previsto dalla disciplina vigente (art. 122 del Codice Privacy e Provvedimento del Garante dell'8 maggio 2014), la richiesta del consenso.

In sintesi, seguendo le classificazioni sopra individuate potremmo trovarci di fronte a varie "combinazioni". Ciò significa che un medesimo cookie potrà presentare contemporaneamente varie caratteristiche e quindi, per esempio, essere un cookie dalla durata persistente, proveniente da una terza parte e con finalità di profilazione.

3. Ambito di applicazione e soggetti destinatari degli adempimenti

Come visto in precedenza, è necessario precisare che la disciplina relativa all'uso dei cookie si estende anche all'utilizzo di altri strumenti analoghi (come ad esempio *web beacon*, *web bug*, *clear GIF*) che consentono l'identificazione dell'utente o del terminale e che quindi devono essere ricompresi nell'ambito del citato Provvedimento. In questo senso, anche l'utilizzo di alcune tipologie di *App*, è da ritenersi compreso nell'ambito di applicazione della normativa (si pensi, per esempio, ad *App* che si appoggiano su 'web server' o, anche, a quelle che utilizzano sistemi di tracking basati su Google Analytics)⁵.

Resta inteso che quei siti che non consentono l'archiviazione delle informazioni nell'apparecchio terminale dell'utente o l'accesso a informazioni già archiviate, e che quindi non utilizzano cookie, non sono soggetti agli obblighi previsti dalla normativa.

Ciò detto, un ulteriore elemento da considerare ai fini della corretta definizione della materia in esame, è quello soggettivo. E' necessario, cioè, tenere conto e distinguere il differente soggetto che installa i cookie sul terminale dell'utente, a seconda che si tratti dello stesso gestore del sito che l'utente sta visitando (che

⁵ Riguardo al mondo delle *Apps*, per un'analisi più approfondita sugli aspetti in materia di privacy, si consiglia di fare riferimento anche all' "Opinion 02/2013 on apps on smart devices" ad opera del Gruppo "Articolo 29".

il Provvedimento definisce come "editore" o "prima parte") o di un sito diverso che installa cookie per il tramite del primo (c.d. "terze parti"). In taluni casi, per i cookie installati dalle "terze parti", non risulta possibile porre in capo al gestore del sito i medesimi adempimenti che sono previsti per i "propri" cookie di "prima parte". In primo luogo, perché la prima parte non ha sempre la capacità economico-giuridica di farsi carico degli adempimenti delle terze parti e non è nelle sue possibilità poter verificare, di volta in volta, la corrispondenza tra quanto dichiarato dalle terze parti e le finalità da esse realmente perseguite con l'uso dei cookie. Spesso, poi, la prima parte non conosce direttamente tutte le terze parti che installano cookie tramite il proprio sito e, quindi, neppure la logica sottesa ai relativi trattamenti. In ultimo, i cookie di terze parti potrebbero, poi, essere modificati nel tempo dai terzi fornitori. Occorre tenere conto del fatto che spesso i gestori di siti, che comprendono anche persone fisiche come blogger o piccole imprese, sono la parte più "debole" del rapporto.

Analogamente, per quanto concerne l'acquisizione del consenso per i cookie di profilazione, dovendo necessariamente - per le ragioni su esposte - tenere distinte le rispettive posizioni di "titolari del sito" e "terze parti", si ritiene che i primi, con i quali gli utenti instaurano un rapporto diretto tramite l'accesso al relativo sito, assumano necessariamente una duplice veste. Tali soggetti, infatti, da un lato sono titolari del trattamento quanto ai cookie installati direttamente dal proprio sito; dall'altro, non potendo ravvisarsi una contitolarità con le terze parti per i cookie che le stesse installano per il loro tramite, si ritiene corretto considerarli come "intermediari tecnici" tra le terze parti e gli utenti.

4. Gli adempimenti

Come visto, l'individuazione delle attività da attuare è strettamente legata alla tipologia di cookie utilizzato e al soggetto "proprietario" che ne procede all'installazione ("prima parte" e "terza parte").

Nel seguito vengono riassunti gli adempimenti da mettere in atto, specificandone le relative modalità di attuazione ed i razionali che ne sono alla base.

A. **Banner.** Il banner riportante l'Informativa "breve" in forma semplificata, non è obbligatorio nei soli casi di siti internet che facciano uso di cookie tecnici o cookie analitici di prima parte senza potere identificativo (per tale distinzione fare riferimento alla classificazione riportata nei paragrafi precedenti). E' invece adempimento obbligatorio nei casi di utilizzo di cookie di profilazione e di cookie analitici con potere identificativo di terza parte.

Il banner deve essere reso disponibile con una modalità tale da offrire un livello di discontinuità, seppur minima, all'esperienza di navigazione; per esempio con una "tendina" che si presenti "a comparsa" nel momento in cui l'utente accede al sito web, sia nei casi in cui si atterri direttamente sulla home page che in altra pagina appartenente al medesimo dominio.

Il banner deve avere un contenuto minimo di informazioni, ovvero: specificare che il sito utilizza, quando effettivamente lo fa, cookie di profilazione (o analitici di terze parti con potere identificativo) e che

consente di inviare messaggi pubblicitari in linea con le preferenze dell'utente; contenere il link all'Informativa estesa e l'indicazione che, tramite quel link, è possibile negare il consenso all'installazione dei cookie; indicare che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link o anche solo attivando la funzione di "scroll") comporta la prestazione del consenso all'uso dei cookie.

- B. Consenso preventivo e sua documentabilità. Per i trattamenti di dati personali connessi l'utilizzo di cookie di profilazione e di cookie statistici/analytics di terza parte con potere identificativo, è necessario il consenso al trattamento, preliminarmente alla loro installazione sul terminale degli utenti, in forza di quanto previsto dalla disciplina vigente (art. 122 del Codice Privacy e Provvedimento del maggio 2014). Per le modalità di manifestazione, vale quanto indicato dal Provvedimento per il quale "la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie".

Al riguardo, quindi, le soluzioni per l'acquisizione del consenso basate su "scroll", o sulla prosecuzione della navigazione all'interno della medesima pagina web, da molti prospettate e in effetti particolarmente rilevanti nel caso di dispositivi mobili, sono considerate in linea con i requisiti di legge, qualora queste siano chiaramente indicate nell'Informativa (sia nel *banner* sia nell'informativa estesa) e siano in grado di generare un evento qualificabile come azione positiva dell'utente che sia registrabile e documentabile presso il server del gestore del sito (prima parte). Viceversa, non deve e non può essere considerata prestazione al consenso, il *click* da parte dell'utente al *link* dell'informativa estesa riportato nel testo del *banner*.

Per tenere traccia del consenso acquisito, il titolare gestore del sito può avvalersi di un apposito cookie tecnico (sistema non particolarmente invasivo e che non richiede a sua volta un ulteriore consenso).

In presenza di tale "documentazione", non è quindi necessario che il banner sia riproposto alla seconda visita dell'utente/terminale sul medesimo sito, ferma restando la possibilità per l'utente di negare il consenso e/o modificare - in ogni momento e in maniera agevole - le proprie opzioni, ad esempio tramite accesso all'informativa estesa che deve essere quindi linkabile da ogni pagina del sito.

I gestori dei siti hanno, comunque, la possibilità di ricorrere a modalità diverse da quella sopra indicata (e individuata dal Garante Privacy), purché presentino tutti i requisiti di validità del consenso richiesti dalla normativa privacy (in particolare la sua documentabilità).

Per l'installazione dei cookie tecnici non è richiesto il consenso degli utenti ma rimane necessaria fornire adeguata informazione nell'informativa redatta ai sensi dell'art. 13 del Codice privacy e di norma contenuta all'interno delle Privacy Policy già esistenti all'interno del sito.

Con riferimento al tema della responsabilità dei gestori dei siti in tema di raccolta del consenso ed installazione dei cookie di profilazione

provenienti da domini di terze parti, i gestori (di prima parte) svolgono un ruolo di mero intermediario tecnico rispetto all'installazione di tali cookie.

È bene precisare, tuttavia, che per la natura "distribuita" di tali trattamenti - che vedono i siti di prima parte comunque coinvolti nel processo - il consenso all'uso dei cookie di terze parti si sostanzia nella composizione di due elementi entrambi necessari: da un lato la presenza del banner (analizzato nei paragrafi precedenti) che genera l'evento idoneo a rendere il consenso documentabile (a carico della prima parte) e, dall'altro, la presenza dei *link* aggiornati ai siti gestiti dalle terze parti in cui l'utente può effettuare le proprie scelte in merito alle categorie ed ai soggetti da cui ricevere cookie di profilazione.

Si precisa, inoltre, che per quei siti in cui i banner pubblicitari o i collegamenti con i social network sono semplici *link* a siti di terze parti che non installano cookie di profilazione, non vi è bisogno di rendere l'Informativa estesa e di raccogliere il consenso.

- C. Informativa estesa. Tale Informativa deve: contenere tutti gli elementi previsti dalla legge (art. 13 del Codice Privacy), descrivere analiticamente le caratteristiche e le finalità dei cookie installati dal sito (al riguardo è quindi assai consigliabile riportare l'elenco dei cookie distinguendone provenienza, durata e finalità), contenere le richieste di consenso, le quali non devono necessariamente fare riferimento ai singoli cookie installati, ma possono riguardare categorie più ampie o specifici produttori o mediatori con cui i siti di prima parte hanno stabilito rapporti commerciali. Tale documento deve quindi includere il *link* aggiornato alle Informative ed ai moduli di consenso delle terze parti (per garantire all'utente la possibilità di *Opt-Out*) con le quali il titolare gestore del sito in qualità di "intermediario tecnico" ha stipulato accordi per l'installazione di cookie tramite il proprio sito.

In ambito profilazione, la finalità consistente nel creare profili degli utenti al fine di inviare loro messaggi pubblicitari mirati, non potrà essere indicata nell'informativa con il riferimento alla mera finalità pubblicitaria dell'uso dei cookie, ma occorrerà specificare che gli stessi consentiranno al gestore del sito di realizzare, appunto, una profilazione finalizzata alla successiva attività di direct marketing.

E' opportuno, infine, non dimenticare che tale Informativa deve essere linkabile da ogni pagina del sito, per esempio prevedendo un suo accesso tramite *link* riportato nel *footer* di ogni pagina web del medesimo dominio.

- D. Notificazione. L'uso dei cookie rientra tra i trattamenti soggetti all'obbligo di Notificazione (ai sensi dell'art. 37, comma 1, lett. d), del Codice Privacy) laddove questi siano finalizzati a "definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti". Si ricorda che la Notificazione è presentabile solo per via telematica e tramite pagamento dei diritti di segreteria il cui importo è fissato in euro 150,00. Il registro delle Notificazioni è pubblico e consultabile da chiunque senza oneri. Mediante il registro vengono effettuati controlli, dal Garante

Privacy, sui trattamenti oggetto di notificazione, anche verificando le notizie in esse contenute. Per avere alcuni chiarimenti circa le modalità di presentazione della Notificazione, può essere utilizzato come utile supporto quanto riportato nell'Infografica n. 1.

L'uso dei cookie meramente tecnici (es. di navigazione, di funzionalità, di stato della sessione) è, invece, sottratto all'obbligo di notificazione, sulla base di quanto previsto dal provvedimento del Garante Privacy del 31 marzo 2004 (Gazzetta Ufficiale del 6 aprile 2004 n. 81) che ha escluso espressamente quei trattamenti "relativi all'utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet".

Rispetto ai casi in cui vige l'obbligo di Notificazione, si precisa che il gestore di un sito web può effettuare un'unica Notificazione per tutti i diversi ed ulteriori siti web che lo stesso gestisce. In tal caso, nell'atto di Notificazione, andranno indicati tutti i domini nei quali si realizza il trattamento effettuato attraverso i cookie, mantenendone aggiornato – attraverso eventuali modifiche della Notificazione medesima – il relativo elenco.

Al riguardo, infine, è importante precisare che per i cookie di profilazione l'obbligo di Notificazione è a carico al soggetto di terza parte che svolge l'attività di profilazione. Tuttavia, questo non vale per i cookie analitici con potere identificativo di terza parte, in cui l'obbligo di notificazione rimane comunque in capo alla prima parte.



Infografica 1
Notificazione al Garante Privacy
 (documento tratto da <http://www.garanteprivacy.it/cookie>)

5. Alcune conseguenze del mancato rispetto della disciplina in materia di cookie

Per il caso di omessa informativa (nella trattazione in oggetto fare riferimento ai paragrafi relativi alla predisposizione del banner ed alla resa dell'Informativa estesa) o di informativa inadeguata che non presenti i requisiti indicati, oltre che nelle previsioni di cui all'art. 13 del Codice Privacy anche quelle contenute nel Provvedimento del 2014, è prevista una sanzione amministrativa da seimila a trentaseimila euro (art. 161 del Codice Privacy).

L'installazione di cookie sui terminali degli utenti in assenza del preventivo consenso, quando richiesto, può comportare, invece, il pagamento di una sanzione amministrativa da diecimila a centoventimila euro (art. 162, comma 2-bis, del Codice).

L'omessa o incompleta Notificazione al Garante Privacy (ai sensi di quanto previsto dall'art. 37, comma 1, lett. d), del Codice Privacy) è sanzionata con il pagamento di una somma da ventimila a centoventimila euro (art. 163 del Codice).

6. Quadro riassuntivo

L'Infografica n.2 rappresenta una sintesi figurativa che può essere utilizzata per individuare, in maniera veloce ed immediata, gli adempimenti da effettuare.

 GARANTE PER LA PROTEZIONE DEI DATI PERSONALI		Il tuo sito/blog installa cookie? Cosa devi fare		
IMPORTANTE: per una corretta interpretazione degli adempimenti previsti, si raccomanda la consultazione del Provvedimento del Garante dell'8 maggio 2014 e dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie». I documenti sono disponibili su www.garanteprivacy.it/cookie		Segnarli nell'informativa <small>Art. 2, par. 5, Direttiva 2009/136/CE e art. 122, comma 1, Codice privacy</small>	Inserire il banner e richiedere il consenso ai visitatori <small>Art. 2, par. 5, Direttiva 2009/136/CE e art. 122, comma 1, Codice privacy</small>	Notificare al Garante <small>Art. 37, comma 1, lett. d), Codice privacy</small>
CHE TIPO DI COOKIE INSTALLI?		LEGENDA: ✓ adempimento previsto ✗ adempimento non previsto		
	Nessun cookie	✗	✗	✗
	Tecnici o analitici prima parte	✓	✗	✗
	Analitici terze parti <small>(se sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) – vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»</small>	✓	✗	✗
	Analitici terze parti <small>(se NON sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) – vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»</small>	✓	✓	✓
	Di profilazione prima parte	✓	✓	✓
	Di profilazione terze parti	✓	✓	✗ <small>i La notificazione è a carico del soggetto terza parte che svolge l'attività di profilazione</small>

Infografica 2
Quadro riassuntivo degli adempimenti
 (documento tratto da <http://www.garanteprivacy.it/cookie>)

Biografia

Antonio Piva, laureato in Scienze dell'Informazione, Vice Presidente dell'ALSI (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Ispettore AICA presso scuole ed enti di formazione ed Auditor AICA è Coordinatore per la zona Nord Est. Ingegnere dell'Informazione, svolge docenze e collabora con l'Università di Udine su materie di diritto ICT, Privacy, Start UP e Qualità. Consulente su Agenda Digitale ed innovazione nella PA locale, è consulente e valutatore di sistemi di qualità ISO9000, Privacy e Sicurezza presso Enti pubblici e privati. Ispettore AICA presso scuole ed enti di formazione. Membro del Consiglio Nazionale del Forum Competenze Digitali, è Presidente della Sezione Territoriale AICA del Nord Est.

E-mail: antonio@piva.mobi

Attilio Rampazzo, *CISA CRISC, C|CISO CMC* consulente di Sistemi Informativi e Sicurezza delle Informazioni. Ha maturato un'esperienza pluriennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante.

E' CISA Coordinator in ISACA Venice chapter. Svolge attività come Valutatore di Sistemi di Gestione della Qualità, di Sistemi per la Sicurezza delle Informazioni e di Sistemi di Gestione dei Servizi IT (cert. AICQ Sicev) presso CSQA Certificazioni. Trainer accreditato APMG per ITIL, ISO 20000 e Cobit 5.

Docente ai corsi per LA ISO/IEC 27001, LA ISO/IEC 20000-1, LA ISO 22301 riconosciuti AICQ Sicev.

Socio AICA, ISACA Venice chapter, ASSOVAL, ANIP.

e-mail: attilio.rampazzo@gmail.com

Maurizio Sala, avvocato in Milano, fondatore degli studi esteri di Bucarest e Mosca, è componente del Tavolo Tecnico permanente per il Processo Civile Telematico istituito presso l'Ufficio di Gabinetto del Ministro della Giustizia e della Commissione Informatica dell'Ordine degli Avvocati di Milano, Coautore delle specifiche del software per le Note di Iscrizione a Ruolo con codice a barre (NIR) e del Manuale del Diritto di Internet, è autore di pubblicazioni in materia informatico-giuridica, è docente nei corsi di formazione sul Processo Civile Telematico e curatore della sezione sul Processo Telematico della rivista on-line Libera Officina del Diritto (www.lodd.it), dal 2001 al 2009 è stato docente presso l'Università Statale di Milano Bicocca ai seminari sul diritto del CyberSpazio,

E-mail: maurizio@sala.it

Luca Spongano ha conseguito il Master in Diritto delle Nuove Tecnologie ed Informatica Giuridica presso l'Alma Mater Studiorum di Bologna - Facoltà di Giurisprudenza di Bologna (Cirsfid). È certificato ITIL – Foundation. Ha operato, tra gli altri, come esperto legale nel diritto delle nuove tecnologie e diritto dell'informatica, addetto alla gestione della normativa in ambito protezione dei dati personali all'interno del Presidio Privacy della seconda Multiutility italiana, contribuendo alla definizione e mantenimento del Sistema di Gestione Privacy dell'intero Gruppo. È autore sulla rivista telematica informatico/legale Filodiritto. È membro del Consiglio Direttivo e del Gruppo Diritto ICT e Privacy della Sezione Territoriale AICA dell'Emilia Romagna, nonché referente per le tematiche Privacy.

È Privacy Specialist presso VEM Sistemi S.p.A., dove svolge attività di consulenza in ambito privacy e data protection, nei confronti di società di grandi dimensioni, multinazionali e pubbliche amministrazioni.

E-mail: luca.spongano@vem.com