



L'informatica giuridica e le tecnologie dell'informazione

Giurisprudenza (Università di Bologna)



Scansiona per aprire su Studocu



Giovanni Sartor

L'INFORMATICA GIURIDICA E LE TECNOLOGIE DELL'INFORMAZIONE

Quarta edizione

CAPITOLO 1: Il diritto e la società dell'informazione	2
CAPITOLO 2: Il calcolatore	10
CAPITOLO 3: Algoritmi e programmi	26
CAPITOLO 4: I dati informatici	53
CAPITOLO 5: Internet	71
CAPITOLO 6: L'intelligenza artificiale	97
CAPITOLO 7: L'IA: tecnologie	109
CAPITOLO 8: L'AI: applicazioni giuridiche	113

CAPITOLO 1: Il diritto e la società dell'informazione

1.1 La società dell'informazione

Con il processo di **industrializzazione** si passa dalla società agricola alla società industriale, il passaggio da società industriale a società dell'informazione si ha con **l'informatizzazione**; l'impiego delle macchine nell'elaborazione delle informazioni, ha determinato la formazione di un nuovo modello sociale. Nella società dell'informazione i calcolatori gestiscono la memorizzazione, *organizzazione e ricerca dell'informazione*, governano le macchine, gestiscono i flussi di lavoro, aumentano la realtà con oggetti e contenuti virtuali.

Floridi ha osservato come la società si va trasformando in un'infosfera popolata da entità computazionali, autonome e intelligenti. Dall'informatica nasce il cibernazio, il mondo virtuale delle reti informatiche, la cui esistenza è il risultato dell'attività dei calcolatori collegati in rete.

1.1.1 Un nuovo paradigma socio-tecnologico

Il sociologo Manuel Castells osserva come la società dell'informazione costituisca un nuovo paradigma socio-tecnologico, caratterizzato da:

- **L'informazione**, il materiale grezzo e materia prima delle nuove tecnologie;
- Gli **effetti** delle nuove tecnologie sono pervasivi; agendo sulle informazioni le tecnologie vanno ad incidere su ogni aspetto della vita individuale e sociale;
- **Interconnessione**; collegano i sistemi tecnologici e organizzativi che ne fanno uso;
- **Flessibilità**, permettono di riorganizzare continuamente i sistemi tecnologici e organizzativi e i loro collegamenti riprogrammando i modi in cui è elaborata, utilizzata e distribuita l'informazione;
- **Convergenza**; tendono a unificarsi in sistemi integrati, una tecnologia fornisce l'input o il supporto per l'impiego dell'altra.

Nella società dell'informazione la produttività dipende dalla tecnologia della generazione di conoscenza, dell'elaborazione dell'informazione e della comunicazione di simboli. La produzione di merci a mezzo di merci diventa produzione di informazione a mezzo di informazione. Lo scambio tra chi produce manufatti e chi fornisce le materie prime tende a essere sostituito dallo scambio tra chi sviluppa la conoscenza e chi fornisce il lavoro necessario per attivare i processi produttivi.

Lo sviluppo delle tecnologie delle informazioni è motore del fenomeno della **globalizzazione**; la nuova *società* viene definita anche *della rete*, un'organizzazione sociale nella quale le attività produttive e culturali si articolano in forme che prescindono le distanze geografiche. La possibilità di inserirsi nei diversi flussi di informazione determina l'inclusione delle persone nei rapporti sociali ed economici; si configurano nuovi rapporti di potere: i **networker**, coloro che determinano i contenuti e i flussi di informazione, si contrappongono ai **networked**, ossia a coloro che accedono passivamente all'infrastruttura tecnologica - informativa.

Si crea una contrapposizione tra chi è in grado di utilizzare le tecnologie dell'informazione e chi non è in grado di farlo, il cosiddetto **digital divide**; la riduzione di questo si può ottenere diffondendo le competenze di base e può accrescere i livelli culturali, la mobilità sociale, la democraticità delle scelte, la capacità di essere soggetti attivi e consapevoli.

1.1.2 Realtà e rappresentazione nella società dell'informazione

La società dell'informazione realizza "esistere e essere percepito"; la percezione è da parte dei sistemi informatizzati e consiste nel rappresentare ogni aspetto naturale e sociale come dati, cioè come strutture informative suscettibile di elaborazione informatica.

Gli eventi della realtà umana e sociale producono conseguenze solo attraverso la loro rappresentazione informatica; vengono rappresentati in sistemi informatizzati determinando processi che possono modificare la realtà stessa. Nella società dell'informazione il rapporto tra gli eventi e le loro rappresentazioni simboliche si pone in modo diverso per due ragioni:

1. l'enorme crescita delle quantità di informazioni disponibili, crescita consentita dall'economicità del trattamento dei dati rispetto al trattamento manuale;
2. possibilità di usare strumenti automatici per acquisire informazioni per la loro registrazione, elaborazione e svolgimento delle attività consequenziali; il compito di prelevare e aggiornare dati, di estrarne conoscenze utili per l'adozione è delegato spesso a strumenti informatici, riducendo l'intervento dell'uomo (es. bancomat).

Le **procedure automatizzate** non comportano la rinuncia all'intervento dell'uomo, che è chiamato a svolgere compiti di supervisione, integrazioni, decisione e controllo operando quasi in simbiosi; ma, riducono i costi della raccolta e della memorizzazione delle informazioni e facilitano l'impiego delle informazioni raccolte.

Alcune esigenze discendono dalla crescente importanza della rappresentazione informatizzata, esigenze che postulano una tutela giuridica cosicché la loro soddisfazione rappresenta il fondamento teleologico del diritto dell'informatica (assicurare all'individuo il controllo sulla propria rappresentazione informatizzata, garantire la sicurezza dei sistemi e dei dati che essi contengono).

1.1.3 Società dell'informazione e trasformazioni sociali

Con il passaggio alla società delle informazioni *l'individuo acquista nuove capacità*; la nostra memoria si espande grazie ai dispositivi di memorizzazione e la capacità di ricercare ed elaborare informazioni si accresce grazie agli strumenti di supporto al lavoro intellettuale; gli strumenti informatici entrano a far parte dei nostri processi cognitivi. Le tecnologie dell'informazione talvolta sostituiscono le interazioni personali; l'individuo acquista nuove opportunità di interazione e di partecipazione sociale, potendo comunicare con altri individui connessi alla rete e partecipando alle comunità virtuali. L'individuo di conseguenza tende a distaccarsi dalle comunità locali di appartenenza, poiché le nuove opportunità possono comportare la perdita delle certezze offerte dal radicamento nel proprio ambiente. Da un lato il ruolo dell'individuo viene enfatizzato, aumentando la sua autonomia nel creare e

comunicare nuovi contenuti; dall'altro sperimenta la propria solitaria impotenza, si vede ridotto a un nodo di una rete sterminata.

Le tecnologie dell'informazione hanno un ruolo nella formazione della nuova economia; nello specifico per il **commercio elettronico** (e-commerce), che consiste nell'effettuazione di scambi commerciali utilizzando reti telematiche. Ma la nuova economia non consiste solo negli scambi telematici, viene anche consentito di condividere informazioni all'interno di strutture produttive decentrate, di analizzare grandi quantità di dati, di adottare con rapidità decisioni complesse; ciò è però anche causa del problema: chi non si adegua alle nuove tecnologie non riesce a restare nel mercato.

La società dell'informazione è caratterizzata da una **trasformazione** che comporta un'ambivalente dialettica tra inclusione ed esclusione, coesione e separazione; molti individui possono cogliere molte opportunità ma molti sono esclusi, il tutto dipende dal contributo che si ha da offrire nel momento in cui viene richiesto.

Le nuove tecnologie si espandono a ogni settore delle attività private e pubbliche:

- back office: l'informatizzazione di un'organizzazione investe le attività produttive e gestionali interne;
- front office: l'informatizzazione di un'organizzazione investe i processi politici e amministrativi interni;
- e-governance: direzione elettronica;
- e-government: governo elettronico;
- e-democracy: democrazia elettronica;
- e-participation: partecipazione elettronica.

1.1.4 L'effetto di rete e l'economia dell'informazione

Nell'economia dell'informazione si manifesta l'**effetto di rete** (network effect), significa che quanto più una rete è ampia e intensamente usata, tanto più quella rete acquista valore; le reti si avviano lentamente ma quando hanno successo la crescita diventa sempre più accelerata. Corollario dell'effetto di rete è la **tendenza monopolistica**: la rete più estesa darà più vantaggi rispetto alle reti meno ampie e tutti tenderanno a passare a essa abbandonando le reti meno estese.

L'effetto di rete si applica alle reti di comunicazione ma anche alla rete che si instaura tra utenti e sviluppatori che adottano certe architetture di software; una volta che un programma elaboratore di testi acquista una diffusione più ampia rispetto ai prodotti concorrenti esso tende a monopolizzare il mercato.

L'effetto di rete è *benefico* ma può ostacolare la diffusione delle migliori soluzioni tecnologiche, a vantaggio di chi riesca a realizzare per primo la rete più ampia; ogni produttore ha interesse ad anticipare il rilascio dei nuovi prodotti, questo perché se il prodotto riesce ad acquisire diffusione sul mercato prima dei prodotti concorrenti l'effetto rete giocherà a suo favore, ciò spiega perché vengano diffusi prodotti prematuri, pieni di errori e imperfezioni.

Le tecnologie dell'informazione sono caratterizzate da *costi fissi* alti e da *costi marginali* bassi; per realizzare la prima copia di un nuovo prodotto bisogna sostenere costi elevati, ma la produzione di ulteriori copie dello stesso prodotto ha prezzi bassi. Di conseguenza, chi controlla una parte più ampia del mercato è avvantaggiato, poiché può suddividere i propri costi fissi tra una base più ampia di utenti e quindi può offrire il prodotto a un prezzo più basso.

1.1.5 Tendenze monopolistiche nell'informatica

Il fatto che tutti gli utenti tendono a convergere nell'uso della stessa soluzione tecnologica per un certo tipo di applicazione viene indicato come **monopolio orizzontale**. Con **monopolio verticale** ci si riferisce invece al fatto che chi domina rispetto a un certo prodotto tende a estendere il proprio controllo anche su altri prodotti.

Le tendenze monopolistiche possono pregiudicare l'interesse dei consumatori di prodotti informatici ma anche la concorrenzialità dei mercati e lo sviluppo tecnologico. Sono messe in atto alcune misure volte ad assicurare l'**interoperabilità dei software**: è importante favorire l'uso di formati di dati aperti che possano essere letti e prodotti da diversi software, cosicché i relativi utenti possano scambiarsi i dati. Per l'interoperabilità verticale è fondamentale la conoscibilità delle interfacce dei software, conoscenza che consente ai concorrenti di sviluppare prodotti compatibili.

Importante nel mercato dell'informatica è l'**asimmetria nell'informazione**, che corrisponde alla differenza tra le conoscenze possedute da chi fornisce un prodotto e da chi lo utilizza; tale asimmetria può pregiudicare i consumatori ma può incidere sul corretto funzionamento dei mercati.

Si parla di **selezione avversa** quando l'utente non è in grado di distinguere servizi buoni e servizi scadenti e i fornitori possono dotarsi di un indice di qualità. Offrendo servizi scadenti tenderanno ad avere un'inferiore reputazione e avranno maggior bisogno di una certificazione per rassicurare i potenziali clienti. Non esistono solo tendenze monopolistiche ma anche tendenze che operano verso la diversificazione e decentralizzazione della produzione e creazione di nuovi modelli economici. La riduzione dei costi di riproduzione e distribuzione consente di realizzare e commercializzare prodotti di nicchia, cui è interessata solo una frazione ristretta del mercato.

Il fenomeno della **coda lunga** fa riferimento al fatto che le poche vendite dei moltissimi prodotti riportati nella coda della curva della domanda può eccedere la somma delle molte vendite dei pochi prodotti di grande successo. Realizzare e commercializzare prodotti destinati a una scarsissima diffusione diventa conveniente solo quando i costi della distribuzione si mantengono molto bassi, come avviene nella distribuzione mediante internet.

Nell'economia dell'informazione gli strumenti di produzione sono in genere accessibili a basso costo: per distribuire prodotti digitali ad esempio basta consentirne lo scaricamento da sito web. Diverso era nell'economia industriale, dove i costi dei macchinari limitavano l'attività produttiva. L'accesso alle reti di informazione e la disponibilità di software per il

lavoro collaborativo facilitano la collaborazione tra individui e organizzazioni, consentendo la realizzazione decentrata di iniziative comuni; progetti di ampie dimensioni possono attuarsi mediante la partecipazione decentrata di individui o piccole unità produttive.

1.2 Il diritto nella società dell'informazione

Le trasformazioni sociali avvenute con la nascita della società dell'informazione generano nuove esigenze, interessi e conflitti che richiedono una nuova disciplina giuridica. Il diritto reagisce a tali trasformazioni e contribuisce a determinare i modi dell'utilizzo di quelle tecnologie diventando esso stesso utilizzatore delle tecnologie informatiche adattandole alle proprie esigenze.

Tra la rivoluzione industriale e quella informazionale si hanno delle **analogie** per ciò che attiene l'impatto sui *temi del diritto*: vengono posti nuovi temi alla disciplina giuridica e alla riflessione del giurista, si tratta di problemi che non riguardano le sole forme di produzione ma anche l'organizzazione sociale e politica e la vita dei singoli; sono assai **diverse** invece per ciò che attiene al loro impatto sui modi in cui si svolge il lavoro del giurista, più profondo e pervasivo quello della rivoluzione informazionale.

Entrambe le rivoluzioni danno vita a nuovi settori del diritto (lavoro, previdenza sociale, industriale, protezione dei dati), altri vennero modificati (commerciale, industriale). Si differenziano poichè la rivoluzione industriale venne disciplinata con autonomia da parte dei diversi ordinamenti mentre la risposta giuridica all'informatizzazione non può essere confinata a un solo ordinamento statale, trattandosi di un fenomeno globale; le soluzioni giuridiche devono coordinarsi e armonizzarsi adeguandosi alla dimensione globale. La rivoluzione industriale non incide sulle modalità di svolgimento lasciando immutati gli strumenti di lavoro del giurista; al contrario quella informazionale incide sull'attività, il giurista acquista nuovi strumenti di lavoro. L'informatizzazione, pur essendo una disciplina unitaria, guarda in due direzioni:

- Verso i problemi giuridici dell'informatica: diritto dell'informatica;
- Verso l'uso dell'informatica nel diritto: informatica del diritto.

1.2.1 L'informatica del diritto

L'informatica del diritto (giuridica) ricopre i seguenti settori:

- **Fonti di cognizione del diritto:** realizza fonti elettroniche di cognizione del diritto; la legislazione, la dottrina e la giurisprudenza sono trasferite in banche di dati, distribuite non solo su grandi sistemi centralizzati ma anche su dischi ottici.
- **Sistemi informativi giuridici:** studiano i modi nei quali le organizzazioni giuridiche possono avvalersi dell'informatica per la conservazione, l'estrazione, l'elaborazione, la condivisione, la circolazione delle informazioni. Si studiano le tecniche per garantire la sicurezza dell'informazione giuridica, la correttezza della sua elaborazione e la permanenza nel tempo della sua conservazione. I moderni sistemi giuridici rendono le informazioni disponibili ai soggetti che operano all'interno delle organizzazioni cui afferiscono i sistemi stessi ma anche ai soggetti esterni a esse.

- **Redazione di documenti:** vengono predisposti software che agevolano la creazione di documenti giuridici, mediante la generazione semi-automatica di parti del testo, la presentazione di informazioni rilevanti, l'aiuto alla verifica, la correzione e la strutturazione dei testi secondo gli standard a essi applicabili.
- **Prove informatiche:** vengono individuate tecniche per gli accertamenti che riguardano oggetti informatici o sono effettuati mediante strumenti informatici.
- **Apprendimento elettronico (e-learning) del diritto:** studia l'uso di tecnologie informatiche nell'insegnamento del diritto;
- **Modelli informatici del diritto:** le strutture della conoscenza giuridica e i metodi per la loro elaborazione vengono tradotti in modelli precisi, elaborabili automaticamente.
- **Determinazioni giuridiche:** si realizzano sistemi informatici che agevolano la qualificazione giuridica di casi concreti, applicando in modo interattivo o automatico conoscenze giuridiche.
- **Deontologia ed epistemologia:** vengono esaminate le condizioni affinché le applicazioni giuridiche delle tecnologie dell'informazione rispettino e promuovano valori giuridici.

Le realizzazioni informatiche sono adattate e integrate in funzione all'ambito dell'esperienza giuridica a cui sono destinate ad operare; possiamo quindi distinguere:

- **Informatica legislativa:** propone sistemi e metodi informatici intesi ad agevolare l'attività degli organi che producono nuove disposizioni normative.
- **Informatica giudiziaria:** propone sistemi e metodi informatici intesi ad agevolare l'attività degli organi che decidono controversie su casi concreti. Studia i sistemi informativi che gestiscono i processi civili, penali e amministrativi.
- **Informatica amministrativa:** propone sistemi e metodi informatici intesi ad agevolare l'attività degli apparati della pubblica amministrazione, ad esempio studiando le tecniche informatiche per la gestione delle procedure amministrative.
- **Informatica delle professioni giuridiche:** sviluppa sistemi e metodi informatici destinati alle diverse professioni giuridiche.

L'informatica giuridica può svolgere diverse funzioni nell'attività del giurista:

1. **Accrescere l'efficienza del lavoro giuridico:** ha avviato il giurista verso l'informatica offrendogli gli strumenti per svolgere prima e meglio il lavoro.
2. **Razionalizzare le attività giuridiche:** integra la prima funzione poichè il pieno utilizzo delle potenzialità dell'informatica richiede la riorganizzazione delle attività giuridiche, strumenti e metodi offerti dall'informatica stessa.
3. **Efficacia assiologica:** la seconda funzione viene tramutata in questa, le tecnologie informatiche contribuiscono efficacemente ad altri valori giuridici.
4. **Autocoscienza del giurista:** il tentativo di impiegare le tecnologie informatiche conduce il giurista ad interrogarsi sulla natura del diritto, sulle componenti della conoscenza giuridica, sui modi in cui avviene la trattazione dei problemi giuridici. Vengono realizzati sistemi in cui il giurista trasferisce il distillato delle proprie conoscenze e delle proprie forme di ragionamento. Questi sistemi che consentono al

giurista di simulare il modo in cui si accosterebbe a casi ipotetici; se il sistema e il giurista danno risposte differenti vi sono due possibili spiegazioni all'errore: nella prima la divergenza è imputabile a un errore del sistema, che ha elaborato le informazioni in modo sbagliato; nella seconda a un errore del giurista, che non è riuscito ad applicare al caso concreto i procedimenti cognitivi che aveva individuato e trasferito nel sistema, la simulazione rivela al giurista i possibili errori e le circostanze che possono indurlo a commetterli.

- 5. Perfezionamento metodologico:** la conoscenza dei procedimenti cognitivi del giurista e delle possibilità offerte dall'informatica conduce a prospettare nuovi e più efficaci modi di elaborare le informazioni giuridiche.

1.2.2 Il diritto dell'informatica

Il diritto dell'informatica dovrebbe: prevenire l'uso delle tecnologie informatiche contro i valori giuridici, risolvere i conflitti di interessi inerenti all'impiego di tecnologie informatiche e promuovere l'uso dell'informatica per realizzare i diritti individuali e le esigenze sociali.

Nel diritto dell'informatica si possono distinguere i seguenti profili:

- **Proprietà intellettuale informatica:** la fruizione dei beni informatici immateriali viene disciplinata nel controverso tentativo di conciliare gli interessi dei produttori e degli utilizzatori di tali beni, di favorire lo sviluppo dell'economia della conoscenza ma anche la diffusione del sapere e del dialogo critico (diritto d'autore).
- **Tutela dei dati:** il trattamento dei dati personali, cioè l'elaborazione delle informazioni che riguardano gli individui, è divenuto oggetto di regolazione giuridica. L'esigenza di tutelare la libertà e la dignità degli interessati e il diritto all'informazione e alla comunicazione ha condotto a una nuova disciplina giuridica.
- **Documenti digitali:** sono state stabilite dal diritto le condizioni per la validità giuridica dei documenti digitali e delle firme elettroniche, dettando le regole volte a prevenire abusi e a individuare responsabilità; disciplina l'uso dei documenti e supporti informatici quali elementi di prova.
- **Presenza virtuale:** il diritto ha cercato di disciplinare la presenza di individui e organizzazioni nel mondo virtuale della rete, al fine di conciliare le esigenze di libertà e interconnessione con la tutela dell'identità personale e la prevenzione di effetti confusori.
- **Commercio elettronico:** viene disciplinata la formazione e l'esecuzione di contratti telematici e lo svolgimento delle attività economico - giuridiche attraverso internet, al fine di favorire la formazione e l'esecuzione di contratti telematici.
- **Governo elettronico:** viene disciplinato l'impiego dell'informatica nelle strutture pubbliche e nei rapporti di queste con i cittadini al fine di accrescere l'efficienza degli apparati pubblici ma anche l'efficacia del loro operato, la trasparenza e la sicurezza delle comunicazioni.
- **Reati informatici:** il diritto penale ha sanzionato i reati che riguardano beni informatici o sono commessi mediante strumenti informatici (frodi informatiche, danneggiamento informatico, pedofilia su internet).

- **Informatica e costituzione:** l'informatizzazione incide sull'esercizio dei diritti fondamentali, sulla relazione tra cittadino e poteri pubblici, sull'equilibrio tra poteri dello stato, sul rapporto stato, regioni ed enti territoriali; è necessario che la regolamentazione giuridica tenga conto dei rischi derivanti dall'informatica.

L'elenco di temi non esaurisce comunque i contenuti del diritto dell'informatica, essendo l'informatica entrata in tutti gli ambiti della vita sociale.

1.3. Breve storia dell'informatica del diritto (pagg. 26 - 34)

1.4 Breve storia del diritto dell'informatica (pagg. 34 - 38)

1.5 Profili tecnologici dell'informatica giuridica

Perché il giurista dovrebbe conoscere i principi dell'informatica? Mentre un tempo chi utilizzava un calcolatore doveva interagire direttamente con la macchina, oggi tra il calcolatore e l'utente si frappongono software sempre più evoluti. L'utente non interagisce direttamente con la macchina, bensì con complessi programmi informatici, specificamente realizzati per svolgere determinate funzioni. Per usare questi programmi non è necessario conoscerne il contenuto, la struttura interna, dal momento che è sufficiente conoscerne l'interfaccia-utente, ossia il modo nel quale il programma si presenta all'utente. Sembra che per usare le tecnologie informatiche non siano necessarie competenze tecnologiche approfondite e tanto meno conoscenze sui principi dell'informatica: basta acquistare un hardware ed un software adeguati ed imparare ad utilizzarli. Di conseguenza, il giurista potrebbe fare a meno di una specifica formazione nell'informatica del diritto.

Secondo l'opinione di chi scrive è vero che lo sviluppo dell'informatica esclude che il giurista debba trasformarsi in un progettista di calcolatori, in un teorico degli algoritmi o in un programmatore. Tuttavia, le tecnologie informatiche non sono limitate ad una specifica funzione né sono destinate ad operare entro un particolare ambito sociale: esse sono le tecnologie caratterizzanti la forma sociale nella quale ci troviamo a vivere ed operare. Di conseguenza, la conoscenza dei metodi e delle tecniche dell'informatica rappresenta il prerequisito per comprendere il funzionamento della società dell'informazione, anche nei suoi profili giuridici. Inoltre, solo tale conoscenza ci consente di capire quali sono le possibilità che ineriscono alla società dell'informazione, sia quelle negative (rischi), sia quelle positive (opportunità). Da un lato, le tecnologie informatiche concorrono a determinare l'interpretazione delle norme vigenti, e quindi a stabilire ciò che è lecito, doveroso o vietato in base al diritto vigente: il contenuto delle norme deve riguardare comportamenti tecnologicamente possibili, che meglio consentano di realizzare i valori giuridici. Dall'altro lato, le tecnologie informatiche concorrono a determinare i possibili progressi giuridici: le nuove norme debbono anch'esse prescrivere comportamenti tecnologicamente possibili ed anzi scegliere quelli che meglio realizzino i valori politico - giuridici perseguiti.

In conclusione, capire come funzionano le tecnologie dell'informatica è il presupposto necessario per capire come funziona la nostra società e quindi per interpretare ed applicare molte delle norme giuridiche che la regolano.

CAPITOLO 2: Il calcolatore

L'artefice dell'informatizzazione è il calcolatore digitale, la macchina dedicata all'elaborazione automatica delle informazioni digitali, dotata di capacità universali in questo ambito.

Tra le capacità delle macchine per l'elaborazione delle informazioni:

- compiere operazioni matematiche ad altissima velocità (calcolatrice);
- registrare enormi quantità di informazioni in spazi ridottissimi e ritrovare i dati richiesti con un'incredibile rapidità;
- trasmettere informazioni a grandi distanze e con enorme velocità;
- governare dispositivi meccanici che compiono operazioni di precisione (i robot);
- eseguire programmi che svolgono compiti molteplici.

I calcolatori sono ormai diffusi in tutte le attività produttive, amministrative e professionali, dove offrono prestazioni sempre più elevate, a costi sempre più bassi. Essi sono componenti essenziali della nostra società. Tale dipendenza si accresce a mano a mano che si compie la transizione verso la società dell'informazione: per quest'ultima uno *sciopero informatico generale* (la contemporanea interruzione di tutti i calcolatori) equivarrebbe alla paralisi totale.

2.1 Macchine e algoritmi per elaborare l'informazione

Il funzionamento del calcolatore è dovuto alla combinazione di due componenti:

- *l'hardware*: l'insieme dei dispositivi materiali che elaborano l'informazione;
- *il software*: l'insieme dei programmi informatici che governano il funzionamento del calcolatore, indicando le elaborazioni da seguire.

Le radici dell'informatica possono trovarsi in due linee: la prima nel tentativo di realizzare macchine capaci di elaborare informazioni e la seconda nel tentativo di definire procedimenti precisi e univoci, gli algoritmi, per elaborare informazioni.

2.1.1 I precursori

L'idea di definire metodi precisi per elaborare informazioni ha una lunga storia. Per esempio, Euclide inventò un famoso algoritmo per il calcolo del massimo comune divisore. Al-Khwârizmi indicò le regole precise, da seguire passo dopo passo, per aggiungere, sottrarre, moltiplicare, dividere i numeri decimali. Si tratta di procedure (algoritmi) che rappresentarono un enorme progresso rispetto alle precedenti tecniche per eseguire calcoli numerici.

Pascal costruì la Pascalina, una macchina per compiere addizioni e sottrazioni. Leibniz perfezionò la Pascalina, costruendo un apparecchio in grado di eseguire anche moltiplicazioni. Tanto la Pascalina, quanto l'apparecchio di Leibniz erano calcolatrici automatiche, ma meccaniche (non elettroniche): esse funzionavano grazie a ingranaggi e ruote dentate, non mediante il passaggio di elettroni. Inoltre potevano eseguire, di volta in volta, solo una delle operazioni rientranti nella loro competenza. Non erano programmabili;

non potevano eseguire automaticamente un'intera combinazione di tali operazioni, secondo indicazioni fornite in anticipo.

Leibniz fu il primo a concepire l'idea dei numeri binari e delle relative operazioni. Egli attribuì alla possibilità di rappresentare tutti i numeri con due sole cifre, lo zero (il nulla) e l'uno, una profonda rilevanza analogica, sia per l'ontologia che per la teologia. Da un lato, la numerazione binaria indicava come la diversità delle cose fosse riducibile ad una sottostante struttura condivisa. Dall'altro lato indicava come l'unico Dio delle religioni monoteiste potesse aver creato il mondo dal nulla.

2.1.2 Macchine programmabili

Jacquard Inventò un nuovo tipo di telaio, che era in grado di tessere da solo diversi tipi di trame. Le trame da tessere si indicavano inserendo nel telaio speciali carte perforate: la posizione dei fori determinava la scelta dei fili e le altre attività della macchina.

Al telaio di Jacquard si sarebbe ispirato il matematico inglese Charles Babbage che, dopo aver progettato una macchina per calcolare i logaritmi, concepì il motore analitico, una macchina dotata di una competenza generale, capace di eseguire qualsiasi calcolo. La peculiarità del motore analitico era la programmabilità: oltre a essere in grado di compiere le operazioni aritmetiche di base, era in grado di eseguire qualsiasi combinazione di tali operazioni. La combinazione delle operazioni da eseguire (il programma) si specificava mediante istruzioni riportate su schede perforate. Le istruzioni indicate nelle schede venivano registrate nella memoria interna al motore analitico, che avrebbe proceduto poi alla loro esecuzione, restituendone il risultato.

Nel motore analitico l'*organo di calcolo* (che effettuava le operazioni aritmetiche) e l'*organo di memoria* (che registrava istruzioni e dati) erano affiancati da un *organo di controllo*, che stabiliva quale dovesse essere la prossima istruzione da eseguire, sulla base delle istruzioni già eseguite e dei risultati ottenuti. Esso anticipava quindi la struttura del moderno calcolatore. Babbage non riuscì a superare i problemi tecnici connessi alla costruzione del suo motore e il suo motore analitico rimase un progetto. Lady Augusta Ada Lovelace scrisse alcuni programmi per la macchina di Babbage diventando la prima programmatrice della storia, immaginò che il motore analitico potesse giocare a scacchi e persino comporre musica (anticipando le ricerche di intelligenza artificiale).

2.1.3 Dalle teorie degli algoritmi delle macchine universali

Negli anni '30 si giunse alla formulazione della tesi di Church/Turing: qualsiasi problema *problema (algoritmico)* per il quale esista una precisa procedura di soluzione può essere risolto utilizzando macchine semplici, capaci di svolgere poche operazioni elementari.

Si stabilì la possibilità di realizzare macchine universali, capaci di elaborare qualsiasi algoritmo. Tali macchine eseguono una procedura esattamente definita, ma tale procedura è astratta (non è finalizzata a un risultato particolare): essa consiste nell'eseguire qualsiasi programma (descrizione di algoritmo) sia fornito alla macchina, applicandolo a dati di input

per tale programma. I moderni calcolatori corrispondono al concetto di macchina universale debbono la loro universalità alla loro capacità di accogliere i dati e i programmi

Si determinò l'equivalenza di tutte le macchine universali: ogni macchina universale (opportunamente programmata) è in grado di eseguire qualsiasi algoritmo; ciascuna macchina universale è in grado di eseguire anche l'algoritmo che determina il funzionamento di qualsiasi altra macchina universale: ogni macchina universale, una volta programmata secondo l'algoritmo che descrive il funzionamento di una diversa macchina universale, è in grado di elaborare anche i programmi scritti per quest'ultima.

Turing ha circoscritto l'ambito dei problemi che ammettono una soluzione algoritmica: vi sono cose che nessun calcolatore può fare, cioè problemi che non sono decidibili, che non sono computabili.

2.1.4 I primi calcolatori

I primi calcolatori furono inventati contemporaneamente (ma indipendentemente) nei paesi belligeranti della seconda guerra mondiale. In Inghilterra, un gruppo di matematici e ingegneri, guidato da Turing, realizzò nel 1941 Colossus, un calcolatore elettronico ma non programmabile, che fu impiegato con successo nel decifrare i codici utilizzati per la comunicazione dall'esercito tedesco. In Germania, Zuse, tra la fine degli anni '30 e l'inizio degli anni '40, realizzò Z-3, il primo calcolatore programmabile basato sul sistema binario, il quale trovò qualche impiego nella progettazione di aeroplani. Negli Stati Uniti, infine, tra il 1941 e il 1945 presso l'università di Pennsylvania, fu realizzato il calcolatore ENTAC (Electronic Numerical Integrator and Computer), elettronico e universale, ma ancora basato sul sistema decimale usato per calcolare traiettorie di proiettili.

2.1.5 La macchina di von Neumann

All'inizio degli anni '50 avvenne il salto tecnologico che consentì di passare ai primi veri calcolatori moderni; viene registrato il programma stesso nella memoria del calcolatore, consentendo di accedere con rapidità alle singole istruzioni da eseguire, e soprattutto di compiere salti condizionati: in base ai risultati già ottenuti potevano essere eseguite o saltate certe istruzioni del programma.

La **memorizzazione interna** del programma caratterizza la macchina di von Neumann. L'*unità di controllo* e l'*unità di calcolo* costituiscono l'**unità centrale di elaborazione**, detta anche processore. Essi attuano una stretta cooperazione: la prima identifica l'istruzione da eseguire e i relativi dati, la seconda esegue l'operazione. Dati e istruzioni vengono prelevati dalla **memoria centrale** nella quale vengono trasferiti i risultati delle elaborazioni; si tratta di un dispositivo di memorizzazione ad alta velocità di lettura e scrittura, che deve essere distinta dalle **memorie di massa**, costituite da dispositivi capaci di contenere permanentemente grandi quantità di informazioni. Affinché le informazioni contenute nelle memorie di massa possano essere elaborate dall'unità centrale di elaborazione, esse debbono essere trasferite nella memoria centrale, la sola direttamente accessibile all'unità centrale.

L'esecuzione di un software residente sul disco di un computer ne comporta la duplicazione: il software deve essere copiato nella memoria centrale.

Il modello di von Neumann è caratterizzato dalla natura sequenziale delle elaborazioni: le istruzioni sono eseguite una alla volta; dopo ogni istruzione si passa alla successiva.

2.1.6 La legge di Moore

L'**unità centrale** di elaborazione di un calcolatore può considerarsi costituita da una complessa *combinazione di "interruttori"*, azionati dal calcolatore stesso, che cambiano posizione nel corso dell'elaborazione, lasciando passare la corrente elettrica o interrompendone il flusso. Per realizzare e connettere tali interruttori si sono utilizzate tecnologie sempre più avanzate, che hanno consentito di ridurre le dimensioni dei calcolatori e di aumentarne la potenza.

Negli esperimenti degli anni '30 si usavano i **relay**, apparecchiature elettromeccaniche che, sotto l'effetto della corrente, muovono una linguetta metallica attivando un contatto; furono sostituiti da **valvole termoioniche** (tubi a vuoto contenenti un elettrodo). Si passò ai **transistor**, dispositivi formati da materiali semiconduttori, che lasciano passare la corrente se magnetizzati in certi modi. Migliaia di transistor, di piccolissime dimensioni, sono stati combinati in circuiti elettronici miniaturizzati, i **circuiti integrati**, inseriti in un chip (frammento) di silicio. In un unico circuito integrato possono essere riunite, a costi molto minori, funzioni in precedenza svolte da molte componenti elettroniche distinte.

Invenzione degli anni '70 fu il **microprocessore**; un circuito integrato che comprende l'intera unità centrale di elaborazione, realizzato in un unico chip. La rapidissima crescita sia nel numero di transistor inclusi in un microprocessore sia nella velocità dei microprocessori stessi ha consentito la realizzazione di **microcalcolatori**, calcolatori la cui unità centrale di elaborazione è costituita da un unico microprocessore, sempre più potenti e sempre meno costosi. I microcalcolatori si sono presto diffusi negli ambienti di lavoro e nelle case, consentendo l'ingresso dell'informatica in tutti gli ambiti della vita individuale e sociale e nelle attività giuridiche.

Il microprocessore, grazie alla sua estrema miniaturizzazione, ha potuto introdursi nei più svariati macchinari e dispositivi tecnologici consentendo l'integrazione dell'informatica con le più diverse tecnologie. Grazie allo sviluppo delle tecnologie biomediche sta entrando anche nel corpo umano, governando dispositivi che rilasciano medicinali o rilevano lo stato di salute, operando in diretto collegamento con il sistema nervoso, sostituendo organi difettosi o integrandone le funzionalità, e così ponendo rimedio ad alcune forme di handicap (difetti dell'udito).

La **legge di Moore** delinea una crescita rapidissima, anzi sempre più accelerata: i calcolatori di oggi sono circa 1.000 volte più potenti di quelli disponibili solo 20 anni fa, e circa 1.000.000 di volte più potenti di quelli disponibili 40 anni fa. Si discute sulla continuazione di tale crescita, che dovrà scontrarsi, prima o poi, con i limiti fisici della miniaturizzazione, poichè si raggiungeranno dimensioni tanto piccole da rendere impossibile la realizzazione o il

funzionamento dei circuiti. Resta aperta peraltro la possibilità che una crescita ulteriore sia consentita dal passaggio a tecnologie completamente diverse da quelle attuali, come quelle ottiche (che sostituiscono la luce agli elettroni) o quantistiche (che sfruttano certi effetti atomici e subatomici).

Anche la cosiddetta **seconda legge di Moore** interviene sullo sviluppo tecnologico nel settore dei microprocessori: il costo dello sviluppo di un circuito integrato raddoppia a ogni nuova generazione di microprocessori. Spiega perché pochissime imprese siano in grado di progettare nuovi microprocessori per microcalcolatore: non più di 3-4 imprese dominano il mercato dei microprocessori, e una di esse (Intel) ne copre circa il 90%.

Lo sviluppo delle prestazioni dei microcalcolatori ha determinato una profonda trasformazione nell'hardware e conseguentemente nell'industria informatica. I microcalcolatori hanno aperto nuove applicazioni all'informatica, ma hanno anche sostituito i calcolatori di maggiori dimensioni in molte delle funzioni già affidate a questi ultimi. Si è avuto un **downsizing** (ridimensionamento), cioè del passaggio delle applicazioni informatiche dai grandi calcolatori a calcolatori di minori dimensioni. I tradizionali produttori di hardware sono stati affiancati e spesso sostituiti da nuove imprese, capaci di produrre microcalcolatori con economicità ed efficienza.

2.1.7 Il personal computer

L'invenzione del microprocessore ha consentito la nascita del **personal computer**, il microcalcolatore destinato all'uso da parte del singolo individuo nella sua attività professionale o domestica. I personal computer per rispondere alle esigenze dei singoli sono diventati sempre più potenti e flessibili, e si sono presentati in forme nuove: dai classici calcolatori da tavolo (**desktop**), si sono aggiunti i portatili (**notebook o laptop**), i palmari (**handheld**), e recentemente i calcolatori indossabili (**apple watch**). Il calcolatore si è arricchito di numerosi dispositivi ausiliari come:

- dispositivi di input o output, per inviare informazioni all'utente o per ricevere dallo stesso (tastiera, stampante, schermo, scanner, proiettore, ecc.);
- dispositivi di memorizzazione secondari, detti memorie di massa, per registrare e conservare dati e programmi (dischi rigidi, nastri, lettore-masterizzatore CD o DVD, dischi rimovibili, ecc.)

Si sono diffusi **smartphone** (telefonini intelligenti) che integrano le funzioni di un palmare e di un telefono cellulare. Un ulteriore esempio di integrazione tra calcolatore e telecomunicazioni è rappresentato dai **netbook**, calcolatori portatili dalle piccole dimensioni e dal costo ridotto, usati soprattutto per il collegamento a Internet e la posta elettronica. L'integrazione si è avuta anche con le "tavolette" (**tablet**), calcolatori dalla forma piatta, destinati soprattutto alla visualizzazione di testi e contenuti multimediali, e alla navigazione sull'Internet.

Il singolo utente ha a disposizione un insieme di sistemi di calcolo in grado di rispondere alle esigenze (un avvocato può usare un calcolatore fisso nello studio quale server per le funzioni

amministrative ma può anche svolgere le proprie attività professionali con il proprio portatile fuori dell'ufficio e consultare atti o riviste sul proprio tablet durante gli spostamenti, possa leggere la posta elettronica sullo smartphone).

2.1.8 Dall'informatica individuale alle reti di calcolatori

Con il personal computer prende vita l'era "**anarchica**" dell'informatica individuale, caratterizzata dalla interazione esclusiva, tendenzialmente monogamica, tra il singolo e il suo calcolatore personale. Prima si poteva accedere a risorse informatiche collegandosi a grandi elaboratori, condivisi da più utenti e gestiti da un centro di calcolo; comportando l'esigenza di inserirsi nell'ambito di una struttura organizzativa e di sottoporsi alle sue regole, avendo la possibilità di accedere a risorse condivise e di comunicare con gli altri utenti del centro di calcolo. Grazie al personal computer ogni individuo dispone in piena **autonomia** delle proprie risorse informatiche, sviluppa liberamente la propria creatività senza incontrare i limiti della volontà altrui; ogni utente si trasforma in una monade isolata, priva della possibilità di condividere risorse e di comunicare con altri.

L'isolamento dei personal computer dovrebbe essere stato superato con i dispositivi di comunicazione di cui si dota il microcalcolatore; questo può collegarsi ad altri calcolatori e dispositivi remoti, diventando capace di colloquiare con altri calcolatori e di inserirsi in reti informatiche via via più ampie. Sono interconnessi i singoli calcolatori pur avendo conservato la propria capacità di elaborazione autonoma e pur essendo il controllo mantenuto da ciascun utente. Si ha un'interazione tra uomo-macchina-uomo, cioè l'interazione tra esseri umani mediata dalla macchina.

2.1.9 Dal modello client-server ai servizi di rete

Lo sviluppo delle reti informatiche è stato favorito dalla crescita accelerata delle prestazioni dei microcalcolatori e dei dispositivi a essi collegati, che ha consentito di impiegare microcalcolatori anche per fornire servizi di rete, come ad esempio accesso ad archivi di dati. Accanto ai microcalcolatori destinati all'utilizzo individuale (i personal computer), si sono quindi diffusi i microcalcolatori destinati a fornire servizi di rete (**i server**). I server offrono prestazioni più elevate per quanto attiene alla potenza di calcolo, alla capacità di memoria, alla sicurezza. Grazie al collegamento dei diversi calcolatori in reti il singolo utente, dal proprio calcolatore, può accedere a risorse disponibili presso altri calcolatori o interagire con altri utenti (posta elettronica). Ogni processo computazionale che l'utente attiva dovrà essere svolto da uno o più calcolatori determinati, ma di ciò l'utente non si occupa; la rete informatica si presenta come un ambiente virtuale, dove sono presenti entità software (sistemi) che mettono a disposizione diverse funzioni e servizi.

Nel mondo dell'Internet, al rapporto uomo-macchina si sostituisce il rapporto uomo-servizi di rete, e le macchine (l'hardware) anziché la diretta controparte dell'uomo appaiono come l'ambiente che offre l'energia vitale (la potenza di elaborazione) e il nutrimento (i dati) alle diverse applicazioni informatiche disponibili, alle entità virtuali con le quali l'uomo interagisce.

Chi richiede tali servizi non ha in genere alcuna consapevolezza di quali siano la natura, la configurazione, e la collocazione dei calcolatori che svolgono le elaborazioni necessarie a rispondere alle sue richieste: i calcolatori possono essere collocati presso l'organizzazione che svolge il servizio richiesto, ma anche presso imprese che si occupano della manutenzione di calcolatori altrui, e possono essere dislocati in paesi lontani, nei quali la manutenzione è più economica o che offrono condizioni ambientali favorevoli. Chi usa il computer è interessato solo alla possibilità di attivare le funzioni di cui ha bisogno, interagendo con le entità virtuali che offrono tali funzioni: l'architettura nella quale egli opera non è l'architettura fisica della rete dei calcolatori che compiono le elaborazioni, ma l'architettura dello spazio virtuale nel quale egli opera, architettura che definisce le possibilità d'accesso e di utilizzo, le condizioni e i vincoli per realizzarle, i controlli cui sottostare e i costi da affrontare.

2.1.10 Il modello peer-to-peer

Il **modello client-server** ha trovato la propria antitesi nell'idea delle reti peer-to-peer (da pari a pari), frequentemente abbreviato in p2p. Nelle reti peer-to-peer viene meno la distinzione tra server (fornitore di servizi) e client (utilizzatore di servizi). Ogni nodo (calcolatore) della rete svolge entrambe le funzioni: mette a disposizione degli altri nodi una porzione delle proprie risorse e utilizza le risorse analogamente messe a disposizione dagli altri nodi.

Il modello peer-to-peer ha trovato diverse applicazioni, dalla condivisione della potenza di calcolo alla condivisione delle connessioni Internet; importanti realizzazioni si trovano nell'ambito della condivisione di file (**file-sharing**): i nodi di una rete peer-to-peer condividono i file residenti nelle proprie memorie. Ciascun nodo della rete svolge quindi una duplice funzione:

- opera quale file-server quando altri nodi accedono ai file in esso residenti;
- opera quale file-client quando esso accede ai file residenti su altri nodi,

L'idea generale del modello peer-to-peer ha trovato specificazione in diverse architetture software, spesso combinandosi con elementi del modello client-server. Per esempio, nel **sistema Napster** i file da condividere risiedono nei calcolatori dei singoli utenti, mentre in un server centrale è registrato l'indice che specifica gli indirizzi di rete (i nodi) presso i quali sono disponibili i diversi file; secondo questo modello, l'utente interessato ad accedere a un certo contenuto, si rivolge al server centrale per consultare l'indice, legge gli indirizzi dei nodi-peer che contengono quel contenuto, e accede ai file registrati presso uno di quei nodi. Quello stesso utente metterà a disposizione degli altri utenti della rete i file disponibili sul proprio computer, che saranno accessibili da altri nello stesso modo.

Altre reti per il file sharing adottano soluzioni che non richiedono l'utilizzo di un indice centrale; ogni nodo di tali reti possiede le informazioni che gli consentono di accedere ai file di interesse, ovunque questi si trovino.

I sistemi peer-to-peer sono stati oggetto di intense discussioni, e hanno trovato tanto entusiastici sostenitori quanto determinati oppositori. Tra le ragioni a **sostegno** dei sistemi peer-to-peer, il fatto che essi consentono a tutti, anche con risorse limitate, di partecipare

attivamente a Internet; tali sistemi consentono un maggiore utilizzo delle risorse informatiche individuali. I sistemi peer-to-peer sono basati su un'organizzazione egualitaria, ispirata all'idea della reciprocità indiretta, ciò sta alla base delle ragioni politiche che appoggiano tali sistemi. Tali architetture sono apparse come modello di organizzazione sociale e produttiva, capace di unire collaborazione, eguaglianza e libertà,

L'opposizione si basa su ragioni sia tecniche che giuridico-politiche. Dal punto di vista tecnico il file-sharing comporta lo spostamento di grandi quantità di dati, e quindi può condurre al sovraccarico delle reti informatiche. Alcuni fornitori di servizi rete hanno bloccato l'esecuzione delle operazioni di file sharing, ciò contrasta però con il fondamentale principio della neutralità della rete, secondo il quale tutti i contenuti che viaggiano su Internet dovrebbero essere trattati allo stesso modo, indipendentemente dalla loro natura e dall'identità del mittente e del destinatario. Le ragioni politico-giuridiche contro l'uso del peer-to-peer vertono sul fatto che molti documenti nelle reti peer-to-peer sono protetti dal diritto d'autore, e la loro circolazione avviene in violazione dei diritti di proprietà intellettuale. Si afferma di conseguenza che il file-sharing metterebbe a rischio l'attività delle imprese culturali, rendendo non più remunerative le attività creative: potendo accedere gratuitamente ai contenuti condivisi dai loro "pari", gli utenti non sarebbero più disponibili a pagare il prezzo previsto per l'accesso commerciale a quegli stessi contenuti.

I sostenitori del peer-to-peer ribattono che questa tecnologia può essere usata anche per fini leciti, e che anche la condivisione di contenuti protetti da parte di privati non lederebbe eccessivamente gli interessi dei produttori di quei contenuti, al massimo impedisce loro di appropriarsi di rendite monopolistiche. Numerosi *casi giudiziari*, in diversi paesi, hanno affrontato il tema della liceità dei sistemi peer-to-peer, casi conclusi talvolta con decisioni sfavorevoli ai fornitori dei sistemi per il file sharing altre volte con decisioni favorevoli a essi. Di fronte alle enormi dimensioni del fenomeno della condivisione di contenuti protetti on-line, e alla sua diffusa accettazione sociale, diverse tesi si contrappongono:

- chi richiede l'applicazione di sanzioni rigorose, tali da scoraggiare ogni uso non-autorizzato di opere protette dal diritto d'autore;
- chi ritiene che anziché adottare soluzioni repressive bisognerebbe abbandonare o rivedere profondamente il diritto d'autore, privo ormai di un valida funzione economico-sociale, almeno nella sua attuale conformazione giuridica;
- chi ritiene possibili soluzioni di compromesso, quali abbonamenti a modico prezzo, che rendono lecita la condivisione di opere protette in reti peer-to-peer, facendo salvi, tuttavia, gli interessi economici degli autori e dell'industria culturale.

2.1.11 La virtualizzazione e Il cloud computing

La possibilità di realizzare architetture virtuali ha determinato una tendenza verso la centralizzazione. Gli anni '90 avevano visto lo "snellimento" delle apparecchiature hardware, cioè la sostituzione dei macro-calcolatori con mini o **micro-calcolatori** capaci di svolgere, a costi minori, le funzioni già affidate ai macro-calcolatori.

I primi anni del 2000 sono stati caratterizzati dal ritorno dei **macro-calcolatori** nei centri di calcolo più avanzati; si tratta di macchine di enorme potenza, in grado di sostituire decine di server di piccola o media taglia, emulando il funzionamento di ciascuno di essi. I server di piccola o media taglia vengono "virtualizzati": essi hanno un'esistenza virtuale che risulta dai processi computazionali eseguiti dal macro-calcolatore. Quest'ultimo è in grado di emulare (simulare) contemporaneamente il funzionamento di molteplici microcalcolatori, eseguendo tutti i programmi che sarebbero stati eseguiti da questi.

Alla rinascita dei macro-calcolatori si affianca l'emergere dei **computer cluster** (raggruppamenti di calcolatori), infrastrutture informatiche composte di un insieme di calcolatori, collegati da reti locali ad altissima velocità, in grado di operare come se si trattasse di un singolo elaboratore.

Lo sviluppo delle tecnologie per la virtualizzazione ha determinato un'ulteriore evoluzione dei sistemi informatici, il **cloud computing** (elaborazione nella nuvola). Con il termine "nuvola" si fa riferimento alle *risorse informatiche disponibili su Internet*, risorse che nel loro insieme appaiono all'utente quali aspetti di una realtà unitaria, priva di dimensione fisica cui l'utente può accedere ovunque egli si trovi. Nel modello del "cloud computing" l'utente (singolo o impresa) rinuncia al possesso di proprie risorse hardware e software e accede alle infrastrutture hardware e alle applicazioni software acquisendo attraverso Internet, secondo i propri bisogni.

Il *sistema informatico* del fornitore del servizio di cloud-computing si occupa di ottimizzare l'accesso alle risorse condivise, consentendo a più utenti di farne uso secondo le proprie necessità, nell'ambito dei diritti d'accesso che competono a ciascuno. Tale modello dà piena applicazione all'idea del passaggio dalla proprietà ai diritti di accesso, quale modello organizzativo e giuridico atto a governare l'utilizzo delle risorse nell'era digitale, modello valido non solo per i contenuti informativi, ma anche per i servizi e le infrastrutture informatiche: possiamo prelevare capacità e funzionalità informatiche da Internet sulla base di analoghi schemi contrattuali (**utility model**),

La *fornitura di servizi di cloud-computing* è concentrata in poche imprese, che offrono un'ampia gamma di funzioni ai propri clienti, grazie a grandi infrastrutture di calcolo distribuite. [Quando si parla della Amazon's cloud (la nube di Amazon) o della Google's cloud (la nuvola di Google), si fa riferimento alle risorse informatiche messe a disposizione da un particolare fornitore, mediante una rete di calcolatori su cui risiedono tanta i software utilizzati dagli utenti, quanto i dati registrati dagli stessi.] Gli utenti non sanno dove siano collocati i sistemi che essi utilizzano: la nuvola di un grosso fornitore di cloud-computing è il risultato dell'attività numerosi data center tra loro collegati, ciascuno dei quali può consistere di centinaia o migliaia di calcolatori.

Oltre a poter fruire di specifiche applicazioni informatiche (posta elettronica, gestione di documenti, database, ambienti di sviluppo software), gli utenti possono acquistare dal fornitore di servizi di cloud-computing spazi di memoria (acquista la disponibilità di una certa quantità di spazio disco) o Computer virtuali (acquista un computer virtuale da

utilizzare per le proprie elaborazioni, nel quale potrà collocare i propri dati e i software di cui ha bisogno). L'utente potrà accedere ai propri dati o al proprio computer virtuale semplicemente collegandosi a Internet, ovunque egli si trovi, e avrà garanzie di recupero, sicurezza e continuità.

I servizi di cloud-computing possono essere rivolti tanto ai singoli quanto alle organizzazioni; queste trasferiscono nella nuvola una parte crescente delle proprie attività informatiche, rinunciando in tutto o in parte alla creazione di propri centri informatici (accade sempre più spesso che organizzazioni di diverso tipo affidano la propria posta elettronica a un fornitore di cloud-computing; le caselle di posta dei membri dell'organizzazione risiederanno sulla nuvola del fornitore e saranno gestite mediante il software lì presente). La stessa soluzione può essere adottata per spazi di memoria, sistemi software, e computer virtuali dedicati alle funzioni amministrative o anche all'utilizzo individuale da parte dei singoli membri dell'organizzazione. Sono presenti preoccupazioni collegate alla diffusione del modello del cloud-computing:

- il rischio dell'oligopolio: poche imprese offrono i servizi di cloud-computing, che richiedono la disponibilità di enormi attrezzature e risorse umane;
- i rischi per la privacy: da un lato il cloud-computing offre garanzie di sicurezza, grazie all'impiego delle più avanzate tecnologie, dall'altro lato la concentrazione di enormi quantità di dati nell'infrastruttura del fornitore espone gli utenti a gravi rischi, che risulta difficile anticipare e prevenire;
- il passaggio al cloud-computing comporta la perdita del pieno controllo sul proprio sistema di elaborazione da parte degli utenti. Il fornitore del servizio viene a disporre di un potere di fatto (il controllo tecnico sulle macchine e sui programmi) che il fornitore stesso potrebbe usare anche per limitare l'attività degli utenti e piegarla ai propri interessi, e ciò potrebbe compromettere non solo le libertà dei singoli, ma anche la creatività d'Internet.

I difensori delle libertà d'Internet si sono opposti al cloud-computing poiché comporterebbe una nuova dipendenza da pochi grandi fornitori di risorse virtuali, ancor più radicale della dipendenza nei confronti dei fornitori di software proprietario. Altri hanno però osservato che non mancano le iniziative volte a realizzare ambienti per il cloud-computing basati su software libero/open-source e atti a garantire pienamente le libertà degli utenti.

I profili giuridici del cloud-computing sono ancora inesplorati, un'adeguata disciplina è necessaria perché si possa godere dei vantaggi offerti da questa nuova tecnologia, evitando i rischi con essa connessi. Di fronte alle osservazioni critiche circa la possibilità che i dati dei cittadini europei fossero trattati al di fuori dell'Unione europea senza la tutela offerta dalla disciplina comunitaria sulla protezione dei dati, alcune imprese hanno istituito propri data center nell'ambito dell'Unione europea, così da garantire che il trattamento dei dati personali riguardanti cittadini europei siano soggetti alla disciplina comunitaria.

2.1.12 Il calcolatore nell'ambiente

Nei modelli di utilizzo del calcolatore i dispositivi di input e output si limitano a ricevere informazioni dall'utente, e a trasmettere allo stesso i risultati dell'elaborazione: la rilevazione di **informazioni dall'ambiente**, così come le attività di modifica, sono affidate all'iniziativa umana.

Oggi è frequente che queste attività siano affidate a **strumenti automatici**: i sensori del sistema prelevano autonomamente informazioni dall'ambiente fisico, queste vengono elaborate dal calcolatore, che conseguentemente indica agli attuatori di eseguire le operazioni conseguenti alle proprie elaborazioni, anche senza la mediazione dell'uomo.

Ciò vale per i robot ma anche per applicazioni più comuni (un sistema per il controllo di un processo industriale, una volta rilevate condizioni sfavorevoli può attivare automaticamente operazioni intese a prevenire situazioni pericolose). Tra le interazioni automatiche con l'ambiente possiamo comprendere le ipotesi in cui un sistema di elaborazione utilizza dati digitali che estrae da altri sistemi, con o senza l'autorizzazione dei loro titolari, o invia messaggi digitali che hanno conseguenze giuridiche o incidono sul funzionamento di altri sistemi informatici (sistemi per lo spionaggio elettronico).

2.2 I calcolatori quali macchine elettroniche digitali

La storia del moderno calcolatore è stata caratterizzata da uno sviluppo rapidissimo: nel giro di meno di sessant'anni i calcolatori si sono diffusi con estrema velocità, ampliando le proprie capacità di elaborazione e assumendo forme sempre più differenziate.

I calcolatori mantengono immutate le caratteristiche principali; si possono considerare tutti i calcolatori, passati e presenti, quali membri di una stessa specie (il moderno calcolatore). Le caratteristiche principali del moderno calcolatore possono essere così specificati:

- sono **digitali**: elaborano informazioni espresse in numeri e in numeri binari;
- sono **elettronici**: sfruttano il comportamento degli elettroni, particelle che si spostano sui circuiti elettrici e che determinano la creazione di campi magnetici;
- sono **programmabili**: operano seguendo le indicazioni di programmi informatici, i quali esprimono algoritmi (precise specificazioni delle elaborazioni da eseguire);
- sono **universali**: ogni calcolatore è in grado di eseguire (prescindendo dalle limitazioni del tempo e della memoria di cui dispone) ogni algoritmo.

2.2.1 L'era digitale

Nei nostri anni è avvenuto il passaggio dall'analogico al digitale, si tratta di una **trasformazione tecnologica** (nel giro di pochi anni abbiamo ad esempio abbandonato la macchina fotografica analogica a favore della macchina fotografica digitale e stiamo abbandonando il telefono analogico a favore del telefono digitale).

Confrontando un vecchio registratore di cassette (a nastro) e un moderno masterizzatore di CD si può notare che:

- Il registratore è dotato di una testina che percorre il nastro realizzando su di esso una struttura fisica (la traccia) le cui caratteristiche corrispondono alle caratteristiche delle onde sonore riprodotte (rilevate dal microfono o da una testina di lettura); la traccia è analoga alle onde sonore. Il passaggio opposto si compie quando a partire dalla traccia si produce il suono corrispondente: le onde magnetizzate sono trasformate nelle *onde sonore analogiche*. La traccia analogica è continua, come il fenomeno rappresentato: essa non procede per gradini, ma si sviluppa senza soluzione di continuità.
- Il masterizzatore di CD registra il suono in una struttura che non assomiglia al fenomeno sonoro, non ne mima le caratteristiche: il suono è espresso mediante una sequenza di numeri interi. A partire da quei numeri, il lettore (con l'aiuto delle casse) riproduce il suono corrispondente. I valori registrati sono discreti: ciascuno di essi rappresenta un preciso numero, che differisce per un certo numero di unità (per un determinato gradino) dal numero successivo. La registrazione su CD comporta la *digitalizzazione*, la trasformazione di grandezze continue (le caratteristiche fisiche del suono) in quantità digitali (in numeri interi distinti).

Un fenomeno fisico continuo può avere una rappresentazione analogica, che ne mima l'andamento continuo, o una rappresentazione discreta, nella quale l'andamento continuo è sostituito da gradini, ciascuno dei quali è multiplo di una unità di misura determinata. Questi gradini possono essere rappresentati mediante numeri decimali che possono essere sostituiti da numeri binari.

La rappresentazione digitale sembra *più imprecisa e rozza* della rappresentazione analogica: le differenze tra i punti che rientrano in uno stesso gradino spariscono: i punti da uno fino a 1,5 (incluso) sono tutti abbassati al livello 1, mentre i punti tra 1,5 (escluso) e 2 sono tutti innalzati al livello due. Si possono rendere i gradini così piccoli da offrire una rappresentazione sufficientemente precisa per i fini che si perseguono.

La rappresentazione digitale offre due *vantaggi* importanti rispetto alla rappresentazione analogica:

- È **riproducibile** con assoluta precisione (la riproduzione è assolutamente identica all'originale): ogni nuova riproduzione di una rappresentazione analogica comporta una perdita parziale dell'informazione originaria; differenze che si sommano di riproduzione in riproduzione: se la copia ha 10 differenze rispetto all'originale, la copia della copia ne ha 20. Tale perdita non avviene invece nella riproduzione di rappresentazioni digitali: basta riprodurre gli stessi numeri per avere una copia perfetta. Possono presentarsi degli errori nella riproduzione, ma essi sono assai più difficili: affinché un numero binario sia riportato in modo errato bisogna che esso sia completamente stravolto. Esistono tecniche per identificare gli errori nella riproduzione digitale e porre a essi rimedio;
- È direttamente **elaborabile** dal calcolatore: consiste nella possibilità di elaborazione mediante calcolatore: rappresentazione digitale e elaborazione automatica sono complementari.

2.2.2 Il sistema binario

Il sistema di rappresentazione dei numeri da noi comunemente adottato è il **sistema decimale** (0 in base 10), che utilizza le 10 cifre: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Si tratta di un *sistema posizionale*: ogni cifra di un numero rappresenta un valore che dipende dalla posizione della cifra stessa: ogni posizione indica una potenza del 10. Grazie alla sua natura posizionale, il sistema decimale consente di rappresentare qualunque numero, per quanto grande o piccolo, utilizzando sempre gli stessi dieci simboli numerici (numerali). La rappresentazione decimale consente l'effettuazione delle operazioni matematiche di base (addizioni, sottrazioni, moltiplicazioni, divisioni) mediante semplici regole meccaniche (semplici algoritmi)

Il **sistema di numerazione romano**, invece, doveva introdurre nuovi simboli per le nuove quantità, X, L, C, D per il 10, il 50, il 100, il 500, ecc.

Esistono ulteriori sistemi posizionali: nel **sistema ottale** (in base 8) si usano cifre e ogni posizione esprime una potenza dell'8, mentre nel **sistema binario** (in base 2) si usano solo due cifre e ogni posizione esprime una potenza del 2.

Non vi sono ragioni di principio che vietino di adottare nei calcolatori il sistema decimale. Tecnologie decimali erano adottate in macchine calcolatrici meccaniche, che rappresentavano le informazioni numeriche in strutture decimali (ruote metalliche con 10 denti), e la elaboravano manipolando tali strutture (mediante l'azione combinata di ruote e ingranaggi siffatti).

Risulta più facile utilizzare componenti fisiche dotate della capacità di assumere due sole posizioni (un interruttore può essere acceso, lasciando passare la corrente, o spento, interrompendone il flusso). I circuiti binari presentano una maggiore tolleranza al rumore rispetto ai circuiti decimali: nei circuiti i diversi stati logici (le cifre) sono rappresentate mediante diverse tensioni elettriche, e in un circuito binario è più difficile che una variazione di tensione derivate da qualche perturbazione sia interpretata dal circuito come un diverso stato logico, determinando conseguentemente un errore di funzionamento.

Per queste ragioni nei moderni calcolatori le informazioni non sono rappresentate mediante cifre decimali, ma mediante cifre binarie. La singola cifra binaria, o **bit** (binary digit), è l'unità minima dell'informazione registrata od elaborata da un elaboratore. Mentre una singola cifra decimale può assumere uno tra 10 valori (le 10 cifre da 0 a 9), il bit può assumere uno di 2 possibili valori (la cifra 0 o la cifra 1). Una sequenza di 8 bit si chiama **byte**. Il byte ha i seguenti multipli:

- il kilobyte (spesso abbreviato in K), formato da 1.000 bytes (10³ bytes, cioè 1 seguito da 3 zeri);
- il megabyte (o mega), formato 1.000 kilobyte (10⁶ bytes);
- il gigabyte (o giga) formato da 1.000 megabyte (10⁹ bytes);
- il terabyte (o tera) formato da 1.000 gigabyte (10¹² bytes);
- il petabyte formato da 1.000 terabyte (10¹⁵ bytes);
- l'exabyte formato da 1.000 petabyte (10¹⁸ bytes);

- lo zettabyte, formato da 1.000 exabyte (1021 bytes).

Le unità di misura dei gigabyte e terabyte sono utilizzate per specificare la capacità delle odierne unità di memorizzazione; petabyte, exabyte e zettabyte per indicare le quantità di dati registrati o trasmessi su scala globale.

Nel sistema binario (come nel sistema decimale) ciascuna cifra assume un certo valore in funzione della propria posizione: la cifra nella posizione 0 (l'ultima) indica sempre unità, ma la cifra nella posizione 1 (la penultima) non indica decine ma duine; quella nella posizione 2 (la terzultima) non indica centinaia, ma quartine ecc. In un numero binario la cifra x nella posizione n esprime il valore $x * 2^n$.

2.2.3 La codifica dell'informazione nel sistema binario

Nel sistema binario la rappresentazione di un valore numerico richiede un numero di posizioni superiore a quello richiesto nel sistema decimale. Per questo motivo la numerazione binaria non è adatta all'uomo, che non è in grado di memorizzare agevolmente lunghe sequenze di cifre. Il calcolatore non ha tali problemi, essendo dotato di una grande capacità di memoria: esso si occupa di **tradurre i numeri** dalla rappresentazione decimale a quella binaria, quando riceve un input numerico dall'uomo, e dalla rappresentazione binaria a quella decimale, quando trasmette un output numerico all'uomo.

Le cifre binarie possono rappresentare non solo numeri interi, ma anche numeri con una parte decimale (dopo la virgola) e simboli (lettere dell'alfabeto): basta stabilire corrispondenze convenzionali tra i numeri binari e gli oggetti da rappresentare. I caratteri alfabetici e numerici vengono tradotti in numeri binari sulla base di tabelle di corrispondenza (**codifiche**), che stabiliscono un *rapporto biunivoco* tra i caratteri da rappresentare e un insieme di numeri binari (a ogni carattere corrisponde uno e un solo numero binario).

I numeri binari consentono di rappresentare anche altri tipi di informazione: bisogna stabilire una corrispondenza tra cifre binarie e ciò che si intende rappresentare (i suoni possono essere rappresentati in forma binaria, come avviene nei compact disc musicali, e nelle diverse rappresentazioni di contenuti sonori e multimediali adottate nei calcolatori).

2.2.4 Dalla logica all'elettronica: l'algebra di Boole

Un ulteriore vantaggio del sistema binario è costituito dal suo **parallelismo con la logica**: come nel sistema binario una *cifra* può assumere *due soli valori*, tra loro alternativi, 1 o 0, così nella logica classica una *proposizione* può assumere *due soli valori*, tra loro alternativi, essere vera o falsa. Stabiliamo una perfetta corrispondenza tra cifre binarie e proposizioni se conveniamo di denotare la verità con la cifra 1 (anziché dire che una proposizione è vera, diciamo che essa vale 1) e la falsità con la cifra 0 (anziché dire che una proposizione è falsa, diciamo che essa vale 0).

Boole notò che le combinazioni tra proposizioni obbediscono a regole ben definite, di cui si può dare una formulazione precisa, regole simili a quelle che governano le operazioni dell'aritmetica. Tali regole determinano il significato (il funzionamento) degli operatori logici.

I connettivi logici principali, AND, OR, NOT, corrispondono alle congiunzioni italiane "e", "O", "non".

La proposizione congiuntiva "A AND B" risulta vera se A e B sono entrambe vere, altrimenti è falsa (la proposizione "L'Italia è una repubblica" AND "la Gran Bretagna è una monarchia" è vera, poiché sono vere entrambe le proposizioni componenti; la proposizione "L'Italia è una repubblica" AND "la Francia è una monarchia" è falsa, poiché la seconda delle sue componenti è falsa). A AND B vale 1 se e solo se A vale 1 e anche B vale 1: la proposizione A AND B si comporta come una semplicissima macchina; dati gli input 1 per A e 1 per B, l'operatore AND produce il risultato 1. In ogni altro caso AND produce il risultato 0.

Shannon ebbe l'idea di realizzare circuiti elettrici che applicassero le operazioni dell'algebra di Boole. Nel dispositivo elettronico possiamo assumere che 1 e 0 siano rappresentati rispettivamente da un alto e un basso voltaggio elettrico. Quindi, se il voltaggio è alto in entrambi gli input, anche l'output sarà ad alto voltaggio, mentre se in almeno una delle due entrate il voltaggio è basso, anche l'uscita sarà a basso voltaggio.

La proposizione disgiuntiva "A OR B" risulta vera se almeno una tra A e B è vera, risulta falsa se A e B sono entrambe false (la proposizione "La Francia è una repubblica OR "L'Italia è una monarchia" è vera poiché la prima proposizione componente è vera). La proposizione disgiuntiva risulta vera anche quando entrambe le proposizioni componenti sono vere (la proposizione "La Francia è una repubblica" OR "L'Italia è una repubblica" è vera poiché entrambe le proposizioni componenti sono vere). Possiamo esprimere le condizioni di verità di una disgiunzione, dicendo che A OR B vale 1 se e solo se A vale 1 o B vale 1. Anche il connettivo OR può essere tradotto in un dispositivo elettronico.

"OR" può presentarsi anche come *disgiunzione forte*, usando la parola latina aut, e in logica l'operatore XOR. La proposizione A XOR B è vera se e solo se una sola delle proposizioni componenti è vera, essa risulta falsa quando A e B sono entrambe vere (la disgiunzione debole "L'Italia è una repubblica" OR "La Francia è una repubblica", è vera, mentre è falsa la disgiunzione forte "L'Italia è una repubblica" XOR "La Francia è una repubblica").

La negazione di una proposizione è vera se quella proposizione è falsa, e viceversa la negazione è falsa se la proposizione negata è vera: NOT A è vera se e solo se A è falsa (la proposizione negativa "NOT L'Italia è una repubblica", risulta falsa poiché la proposizione negata "L'Italia è una repubblica" è vera).

Combinando porte logiche possiamo ottenere non solo dispositivi capaci di valutare formule complesse (come $[(A \text{ OR } B) \text{ AND } (\text{NOT } (A \text{ AND } B))]$), ma anche dispositivi capaci di compiere le operazioni matematiche elementari, cioè di confrontare, sommare, sottrarre, e dividere cifre binarie: logica proposizionale e matematica binaria appaiono essere due facce di una stessa medaglia.

Le porte logiche possono essere combinate in reti logiche capaci di svolgere tutte le operazioni logico-matematiche di cui ha bisogno un calcolatore universale. Una rete logica

complessa può costituire il microprocessore di un calcolatore (un microprocessore contiene migliaia, o anzi milioni di porte logiche, cioè di transistor, tra loro collegate).

Si parla di **topografia dei prodotti a semiconduttore** per indicare il complesso disegno della rete logica registrata in una piastrina di silicio. Anziché di un microprocessore potrà trattarsi del dispositivo destinato a compiere un'elaborazione specifica, per la quale si richieda una particolare rapidità o che non si voglia far gravare sul microprocessore.

Reti logiche specifiche possono rappresentare un'alternativa rispetto allo sviluppo di programmi software; una medesima elaborazione (i medesimi output, per i medesimi input) si può ottenere sia attraverso l'esecuzione di un programma da parte di un calcolatore universale (un software), sia attraverso una rete logica (una componente hardware). L'elaborazione effettuata mediante una rete logica sarà più veloce di quella effettuata mediante un calcolatore universale guidato da un software, ma lo sviluppo della rete logica comporterà costi maggiori rispetto allo sviluppo del software, e la rete non sarà modificabile.

È interessante osservare che all'affinità funzionale tra hardware e software non corrisponde il medesimo trattamento giuridico. Il disegno di un microprocessore è tutelato, oltre che dal brevetto industriale dalle disposizioni della legge dedicata alla "Tutela delle topografie a semiconduttore"; il software è disciplinato dalla legge sul diritto d'autore..

2.2.5 Computer, dispositivi, reti

L'unità centrale di elaborazione (il processore), che effettua i calcoli logici e matematici, può essere utilmente utilizzata solo se è integrata da numerosi dispositivi ausiliari:

- **dispositivi di input o output**, mediante i quali il calcolatore interagisce con i propri utenti, ricevendo informazioni o comunicandole all'esterno (schermo, tastiera ecc.);
- **dispositivi di memorizzazione**, memorie di massa, che consentono di registrare e conservare permanentemente dati e programmi (dischi rigidi, dischi rimovibili, ecc.);
- **dispositivi di connessione**, mediante i quali il computer interagisce con altri sistemi informatici (modem, scheda di rete ecc.).

Il calcolatore può soddisfare le esigenze dell'utente mediante le proprie risorse hardware e software e i dispositivi accessori a esso collegati. Esso viene sempre più usato per accedere ad altri calcolatori, e ai server che offrono dati e applicazioni informatiche. Nell'era d'Internet il calcolatore dell'utente (che può essere racchiuso all'interno di un cellulare) è sempre più mezzo d'accesso ad altri sistemi di elaborazione: dal proprio dispositivo, l'utente può accedere a informazioni disponibili presso sistemi informatici remoti.

Solitamente i dispositivi automatici collegati al computer si limitano a ricevere o trasmettere informazioni: la rilevazione di informazioni dall'ambiente, e la modifica dell'ambiente stesso sono affidate all'uomo; tuttavia, è sempre più frequente che anche queste attività siano affidate a strumenti automatici: sensori, che prelevano informazioni dall'ambiente fisico (condizioni di calore, umidità, suoni o immagini), e effettori che operano all'esterno (bracci robotici, interruttori, segnalatori acustici, ecc.).

CAPITOLO 3: Algoritmi e programmi

L'informazione è la materia prima (l'input) e il risultato (l'output) dell'elaborazione automatica ma specifica anche lo svolgimento del processo della propria elaborazione, essa governa la macchina che la produce.

3.1 Lo spirito oggettivo della società dell'informazione

Hegel e Marx si sono soffermati sul processo mediante il quale lo spirito umano si oggettiva, estraniandosi (alienandosi) dalla soggettività dell'individuo, e acquisendo una propria esistenza indipendente. Si tratta del lavoro che realizza oggetti materiali, ma anche dell'attività intellettuale. Viene sottolineata l'indipendenza delle creazioni umane rispetto al proprio creatore; esse, una volta realizzate, acquistano un'esistenza autonoma.

Nelle epoche precedenti lo spirito, il contenuto concettuale, una volta espresso in forma linguistica, poteva rivivere solo grazie alla mediazione della mente umana che coglieva e ricreava, mediante la propria interpretazione, i significati espressi in forma linguistica; senza la mediazione dell'uomo, i testi erano privi di operatività.

3.1.1 Testi eseguibili

Nella società dell'informazione i testi possono *vivere*, diventare operanti, *senza la mediazione dell'uomo*, guidando il calcolatore. Solo i contenuti che possano costituire dati o programmi per calcolatore possono acquisire questa forma di vita. I testi sono destinati non solo alla comunicazione umana. Essi sono destinati anche a **governare il funzionamento di un calcolatore**. La possibilità di creare testi suscettibili di esecuzione automatica rappresenta un'evoluzione culturale: lo spirito (il contenuto concettuale) si separa dall'uomo, e diventa capace di autonoma operatività. L'esecuzione del software da parte del calcolatore realizza processi computazionali, che possono originare attività controllate dal calcolatore e possono dar vita ai fenomeni immateriali della realtà virtuale. Sovrapponiamo agli eventi percettibili attivati dal calcolatore le nostre categorie interpretative e costruiamo corrispondentemente un mondo di fenomeni virtuali: alla realtà del mondo fisico si affianca la realtà virtuale prodotta dai processi computazionali.

Ciò comporta un aspetto duplice:

- un **potenziamento delle capacità di creazione-oggettivazione dell'uomo**: le idee dell'uomo, una volta tradotte in un linguaggio comprensibile (eseguibile) da parte del calcolatore, possono trovare realizzazione operativa, ed eventualmente concretizzazione, in una realtà virtuale, senza ulteriore intervento umano e senza la necessità di input materiali. Tale realizzazione può raggiungere risultati che sarebbero difficili e costosi, o addirittura irrealizzabili, se per dar vita alle proprie idee l'uomo dovesse misurarsi con un supporto materiale.
- la **possibilità di creare realtà virtuali** mediante testi eseguibili aumenta l'ambito dell'estraniamento-alienazione. I testi eseguibili, la cui esecuzione automatica dà vita alla realtà virtuale, hanno raggiunto un'enorme estensione: si tratta di istruzioni,

realizzate tramite il lavoro di milioni di persone. Ciascuno di noi sperimenta la realtà virtuale, risultante dal funzionamento dei software, come un ambito di oggettività non modificabile con il proprio intervento individuale.

3.1.2 L'oggettività virtuale: possibilità e necessità

L'ambiente fisico ci offre possibilità d'azione, ma ci presenta anche impossibilità e necessità che restringono le nostre azioni; viviamo in un mondo materiale artificiale, che offre nuove possibilità d'azione agli individui ma ne restringe l'attività nell'ambiente fisico, configurando necessità e impossibilità. Da un lato l'artificiale ci solleva al di sopra della necessità naturalistica, rendendo possibili cose (volare, comunicare a distanza) che erano impossibili nel mondo pre-tecnologico, dall'altro l'artificiale racchiude e indirizza la nostra azione, talvolta in modi che vanno contro l'esigenza del libero sviluppo della nostra personalità.

I processi computazionali (guidati dal software) generano un'oggettività diversa, non fisica ma virtuale, che dischiude alla nostra azione un ambito di possibilità, e al tempo stesso configura necessità e impossibilità. In alcuni casi la cosa può sembrare ovvia e del tutto innocua (quando il sito per il commercio elettronico ci consente di fare acquisti, ma ci impedisce di inviare una richiesta d'acquisto senza aver previamente indicato il nostro indirizzo). In altri casi, la cosa appare problematica, come quando il sito ci impedisce di fare acquisti se non indichiamo anche il nostro codice fiscale e dichiariamo la nostra disponibilità a ricevere pubblicità commerciale, o se il file musicale che abbiamo acquistato on-line non è duplicabile.

In questi casi si tratta di **possibilità e necessità** (impossibilità) che non sono fisiche, (non dipendono dalle leggi naturali, come l'impossibilità di superare la velocità della luce), né tecnologiche (non dipendono dal limitato livello delle tecnologie disponibili). Si tratta di **impossibilità virtuali**, che dipendono dal modo in cui è conformata la realtà virtuale.

3.2 Programmi e algoritmi

L'**hardware** del calcolatore è un esecutore generale di algoritmi: esso è in grado di eseguire qualsiasi manipolazione simbolica, cioè qualsiasi trasformazione che conduca da certi simboli di input a certi simboli di output, una volta fornito di un algoritmo che specifichi come compiere tale trasformazione.

3.2.1 Ricette, programmi e algoritmi

In una prima approssimazione, *un algoritmo è una **procedura** (un piano d'azione) chiara e univoca*, tanto precisa da poter essere attuata da un **esecutore automatico**, senza che a esso debbano essere fornite ulteriori indicazioni.

Per introdurre il concetto di algoritmo possiamo partire da un'attività a tutti nota: la cucina, e dai programmi (1 software) che ci guidano in tale attività, cioè le *ricette*. Si consideri per esempio la seguente ricetta per la mousse di cioccolato:

Input: 250 grammi di cioccolato fondente, 2 cucchiaini d'acqua, 60 grammi di zucchero a velo, 6 uova, rum e vaniglia

Output: Mousse di cioccolato

Algoritmo (procedura, piano d'azione): Fate fondere il cioccolato a bagnomaria con 2 cucchiaini di acqua. Quando è completamente sciolto, unite lentamente lo zucchero a velo e poi il burro, un pezzetto alla volta. Mettetelo da parte e sbattete i tuorli per circa 5 minuti, finché non diventano gonfi e spumosi. Uniteli al cioccolato, che avrete leggermente riscaldato se nel frattempo si fosse rappreso troppo. Aggiungete il rum e la vaniglia. Montate a neve ferma gli albumi, aggiungendo poi due cucchiaini di acqua. Uniteli con delicatezza al composto di cioccolato e tuorli e versate il tutto in coppette individuali. Fate raffreddare per almeno 4 ore e servite con panna montata a piacere. Le dosi bastano per 6-8 persone.

La ricetta specifica le operazioni da eseguire per preparare un certo piatto (la mousse di cioccolato), ed è rivolta a un essere umano, fornito dei consueti strumenti da cucina: questo è l'esecutore autonomo (**l'automa**) al quale si rivolge la ricetta.

La ricetta dà lo spunto per alcune considerazioni generali, che si potranno trasferire in ambito informatico:

1. La prima considerazione riguarda la **distinzione** tra il *testo* della ricetta (la sequenza di parole in cui il testo consiste) e il *contenuto informativo* della stessa. Se il testo fosse tradotto in un'altra lingua o si cambiassero i tempi dei verbi, concordiamo nel ritenere che il testo sia cambiato, ma che il suo contenuto informativo (l'indicazione su come fare la mousse) sia rimasto immutato.
2. La seconda considerazione attiene al fatto che la ricetta appena presentata presuppone un cuoco di media competenza, e presenta il livello di precisione corrispondente alla competenza di tale esecutore. La ricetta dovrebbe essere più dettagliata se il cuoco fosse completamente inesperto. D'altro lato la ricetta potrebbe essere molto più sintetica, se fosse indirizzata a cuochi professionisti, e in particolare a esperti nella preparazione di mousse al cioccolato; in questo caso il cuoco potrebbe offendersi (per la mancanza di fiducia e di rispetto della sua autonomia) di fronte a precisazioni così dettagliate. Per un destinatario esperto, la prima parte della ricetta potrebbe essere sostituita dalla semplice richiesta di preparare una mistura di burro, zucchero e cioccolato. In generale, una **specificazione** deve essere **adeguata** al suo **esecutore**, prescrivendo allo stesso solo azioni che questo è in grado di compiere autonomamente, ma evitando di dettagliare le componenti elementari di azioni complesse che l'esecutore sa già svolgere in modo adeguato.
3. La terza considerazione è che la nostra ricetta non si limita a indicare un insieme di azioni da compiere; essa indica anche l'ordine nel quale quelle azioni debbono essere eseguite e combinate. La struttura di base è la **sequenza**: si assume che le azioni si eseguano nell'ordine in cui sono indicate. Alcune azioni si debbono eseguire qualora risulti vera una certa condizione (la cioccolata si deve riscaldare se si è rappresa);

altre azioni si debbono ripetere finché risulti vera una certa condizione (i tuorli si debbono sbattere finché non sono gonfi e spugnosi).

4. La quarta considerazione riguarda la **distinzione** fra tre *aspetti indicati nella ricetta*. Il dato di partenza o input (gli ingredienti), il risultato da raggiungere o output (la mousse), la procedura (il piano d'azione) da seguire per raggiungere l'output a partire dall'input. La fedele **esecuzione** della procedura consente di passare dall'input al risultato, e se la procedura è corretta ed è fedelmente eseguita, si otterrà il **risultato** desiderato (la mousse).

Un programma per computer svolge una funzione analoga a quella della ricetta da cucina. Entrambi sono *destinati a un esecutore*: come la ricetta richiede l'azione del cuoco, così il programma deve essere messo in atto dal **computer**. Entrambe specificano la procedura da seguire per realizzare un certo output a partire da un certo input: la ricetta indica come realizzare la mousse a partire dagli ingredienti, un programma indica al computer la procedura di calcolo da seguire per realizzare un certo risultato a partire da certi dati di input. Tanto il programma quanto la ricetta indicano quindi una procedura per risolvere un certo problema, caratterizzato nei termini di una certa situazione di partenza e di un certo risultato che si vuole ottenere.

Un algoritmo per un certo esecutore è una **combinazione** precisa e univoca di **azioni**, eseguibili autonomamente da parte di quell'esecutore (senza la necessità di un aiuto da parte di altri), che consentono di risolvere un problema.

Un algoritmo in senso stretto, cioè un algoritmo eseguibile da un **esecutore automatico**, deve possedere rigorosi requisiti di precisione e univocità che mancano in una ricetta di cucina. La ricetta può contenere indicazioni imprecise e in ogni caso contiene istruzioni da applicare con buon senso o comunque con capacità umane. Un algoritmo per computer non riguarda attività materiali ma attività simboliche, l'elaborazione di informazioni.

3.2.2 Algoritmi per la manipolazione dell'informazione

Tra le attività simboliche troviamo l'apprendimento di metodi per compiere le operazioni matematiche di base: si tratta di procedure precise e univoche seguendo le quali, se compiamo ogni passo con esattezza, nell'ordine richiesto, siamo sicuri di arrivare al risultato.

Per esempio, per moltiplicare in colonna due numeri, quali 788 e 89 (i due fattori della moltiplicazione) sappiamo che dobbiamo procedere come segue:

Algoritmo per la moltiplicazione in colonna di numeri interi

Input: due fattori interi

Output: il prodotto dei due fattori

Algoritmo: si proceda come segue:

- si scrivano i due fattori in colonna;

- si parta dalla fine del secondo fattore e finché non si siano considerate tutte le cifre di questo si ripeta quanto segue:
 - si moltiplichi il primo fattore per l'ultima cifra non ancora considerata del secondo fattore (partendo dalla fine di questo);
 - si riporti il risultato di questa operazione sotto al risultato precedentemente ottenuto, spostato di una posizione a sinistra (o immediatamente sotto ai fattori, se si tratta del primo risultato);
- si sommino i risultati così ottenuti.

Questa procedura (algoritmo) per la moltiplicazione è stata espressa nel linguaggio naturale, che le persone usano per comunicare tra di loro. Gli algoritmi per calcolatori debbono essere espressi in linguaggi che il calcolatore può capire (**linguaggi di programmazione**), diversi da quelli usati nella comunicazione tra persone. Il programmatore può trovare conveniente esprimere un algoritmo nel linguaggio naturale, prima di tradurlo in un linguaggio di programmazione. Tale formulazione degli algoritmi si suole chiamare **pseudocodifica**, per indicare che la pseudocodifica di un algoritmo non è ancora un programma per calcolatore.

Questa procedura presuppone che l'esecutore sia in grado di eseguire moltiplicazioni nelle quali il secondo fattore è un numero di una sola cifra ($788 * 9$), e somme di numeri interi. L'esecutore può essere dotato di quella competenza in quanto egli sia in grado di eseguire tali operazioni direttamente, in un unico passo, oppure in quanto egli conosca un algoritmo che gli consente di tradurre le operazioni in questione in operazioni più semplici, che esso è già in grado di eseguire direttamente. Di solito, noi esseri umani non siamo in grado di eseguire direttamente, in un unico passo, moltiplicazioni come $788 * 9$, ma possediamo un algoritmo per eseguire tali moltiplicazioni mediante una combinazione di moltiplicazioni di singole cifre e di semplici addizioni.

Algoritmo per la moltiplicazione intera con secondo fattore di una sola cifra

Input: Due numeri interi, il secondo di una sola cifra

Output: Il prodotto dei due numeri

Algoritmo: si proceda come segue:

- si parta dalla fine del primo fattore;
- finché non si siano considerate tutte le cifre di questo, si ripeta l'operazione seguente:
 - si moltiplichi l'ultima cifra del primo fattore non ancora considerato per il secondo fattore;
 - si sommi al risultato della moltiplicazione del punto precedente l'eventuale riporto (derivante dalla precedente moltiplicazione dello stesso tipo);
 - si scrivano le unità del risultato di questa somma quale cifra componente il risultato finale, a sinistra dell'ultima cifra già scritta;
 - si memorizzi il numero delle decine del risultato della somma quale nuovo riporto;
- si scriva l'eventuale riporto a sinistra dell'ultima cifra già scritta.

I due algoritmi attinenti al calcolo elementare consentono alcune considerazioni.

1. Si osservi che anche l'ultimo algoritmo presuppone alcune **competenze** nell'esecutore, cioè la capacità di moltiplicare tra loro singole cifre, e di aggiungere una cifra a un numero di due cifre. Possiamo assumere che per il nostro esecutore si tratti di competenze **atomiche** (esplica direttamente, con un unico atto, senza scinderne l'attuazione in atti più semplici). Una volta che il nostro esecutore abbia appreso l'ultimo algoritmo, queste competenze atomiche diventano sufficienti a eseguire anche il precedente algoritmo. L'acquisizione di un nuovo algoritmo può comportare un aumento delle competenze dell'esecutore: questi acquista nuove competenze, che possiamo chiamare competenze **molecolari**, risultando dalla combinazione di più atti secondo un determinato algoritmo. Tali competenze consentono all'esecutore di svolgere nuovi compiti, rispetto ai quali le sue competenze atomiche, isolatamente prese, sarebbero insufficienti. Se il nostro esecutore non avesse le competenze atomiche per svolgere l'ultimo algoritmo, bisognerebbe completare la sua competenza mediante la specificazione di un ulteriore algoritmo.
2. Si osservi che i nostri algoritmi **non** riguardano **un solo input**: il primo dei nostri algoritmi numerici può essere applicato a qualsiasi coppia di numeri interi, e il secondo può essere applicato a qualsiasi coppia che consti di un intero qualsiasi e di un intero di una sola cifra. Pertanto tali algoritmi sono generali, nel senso che riguardano una classe di possibili input. Rispetto a tutti gli elementi di tale classe si deve valutarne la correttezza: se i possibili input del nostro algoritmo per la moltiplicazione sono tutti i numeri interi, allora l'algoritmo dovrà darci il risultato corretto per ogni coppia di numeri interi.
3. Si osservi che possiamo **distinguere** tra **l'algoritmo**, cioè la specificazione dell'elaborazione da compiere, e il **processo della sua esecuzione**, cioè la *sequenza* dei passi attraverso i quali l'algoritmo viene eseguito, applicandolo a un input particolare. Il primo algoritmo di calcolo può essere applicato tanto alla coppia $\langle 33;72 \rangle$ quanto alla coppia $\langle 938.478;893.542 \rangle$, ma il processo necessario per eseguire l'algoritmo (ed eseguire il calcolo) sarà diverso; nel secondo caso, l'esecuzione del nostro algoritmo darà luogo a un processo molto più lungo.

3.2.3 Gli errori algoritmici

Consideriamo l'esempio di algoritmo che riguarda **un'elaborazione simbolica** (parole) anziché numeri. Questo esempio illustra come non tutti gli algoritmi siano uguali: alcuni garantiscono di ottenere il risultato desiderato, mentre altri non danno questa garanzia; alcuni sono più efficienti, altri lo sono in misura minore.

Il compito da svolgere consiste nel ricercare in un elenco telefonico il numero corrispondente a un certo nome. Assumiamo che l'elenco comprenda 1.000.000 di abbonati e riporti, per ciascun abbonato, il nome (cognome e nome) e il numero telefonico, e che esso sia ordinato alfabeticamente. Il primo algoritmo è la **ricerca sequenziale**.

Ricerca sequenziale. Prima versione

Input: Un elenco ordinato di abbonati al telefono; il nome dell'abbonato da cercare

Output: Il numero di telefono dell'abbonato cercato

Algoritmo: Si proceda come segue:

- si legga il nome del primo abbonato dell'elenco;
- finché l'ultimo nome letto è diverso a quello cercato, si ripeta l'operazione seguente:
 - si legga il nome dell'abbonato successivo;
- si annoti come output dell' algoritmo il numero di telefono accanto all'ultimo nome letto.

Considerazione rispetto a questo algoritmo:

- **lentezza:** esso funziona in un tempo ragionevole solo quando l'elenco da cercare è abbastanza corto; assumendo che serva mezzo secondo per leggere un nome, e che il nome Rossi Mario si trovi in posizione 600.000 (nel nostro elenco di 1.000.000 di nomi), serviranno 300.000 secondi ($600.000 * 0.5$) per raggiungere Rossi. In media seguendo questo algoritmo si impiegherebbero 250.000 secondi ($500.000 + 0.5$), che corrispondono a circa 70 ore, per trovare un particolare indirizzo. Considereremmo un idiota chi seguisse questo algoritmo per esaminare elenchi di notevole lunghezza, poiché ciò comporterebbe dei tempi eccessivamente lunghi, mentre esistono tecniche di ricerca molto più efficienti per compiere ricerche su elenchi in ordine alfabetico;
- **inefficiente ed è sbagliato:** chiediamoci che accadrebbe se il nome cercato non comparisse nell'elenco. Immaginiamo che il signor Rossini Sergio non posseda telefono (o abbia richiesto di non essere menzionato nell'elenco). Seguendo le indicazioni dell'algoritmo procederemmo fino alla fine dell'elenco e ci arresteremmo a fissare la copertina dell'elenco cercando di leggere il nome di un inesistente abbonato successivo;
- **caso improbabile**, ma che sempre rientra nell'ambito dei problemi che l'algoritmo intende affrontare. Supponiamo che l'elenco sia vuoto: in questo caso l'esecutore cercherà pur sempre di leggere il primo nome dell'elenco, cosa che si rivelerà impossibile.

Questo algoritmo evidenzia un'ovvia verità: *non tutti gli algoritmi sono corretti*. Alcuni algoritmi sono sbagliati: in alcuni casi, rispetto a alcuni loro possibili input, non danno la risposta corretta, non danno alcuna risposta o danno una risposta diversa da quella ci aspettiamo.

Apportiamo delle modifiche all'algoritmo affinché consenta di portarne sempre a termine l'esecuzione. La prima istruzione di questo algoritmo pone che l'ultimo nome letto sia nullo all'inizio del programma, attribuendogli il valore "" (non c'è ancora un ultimo nome letto). L'ultimo nome letto viene a essere una variabile, un oggetto che inizia con il valore "", che muta nel tempo, venendo sostituito dai successivi nomi letti durante l'esecuzione del programma.

Ricerca sequenziale. Seconda versione

Input: un elenco ordinato di abbonati al telefono; il nome dell'abbonato da cercare

Output: il numero di telefono dell'abbonato cercato

Algoritmo: si proceda come segue:

- si ponga l'ultimo nome letto uguale a "";
- finché l'ultimo nome letto è diverso da quello cercato e non si sia raggiunta la fine dell'elenco:
 - si ripeta l'operazione seguente: si legga il nome dell'abbonato successivo;
 - si produca in output il numero di telefono accanto all'ultimo nome letto.

Anche questo algoritmo è errato: quando l'abbonato non compare nell'elenco (com'è il caso per Rossini Sergio) l'esecuzione dell'algoritmo si completa alla fine dell'elenco, ma l'output che ne risulta non è il numero dell'abbonato cercato, ma quello del signor Zuzzurro Zeno, l'ultimo nome dell'elenco. Si riformula l'algoritmo con una terza versione, in modo da evitare quest'ultimo errore.

Ricerca sequenziale. Terza versione

Input: un elenco ordinato di abbonati al telefono; il nome dell'abbonato da cercare

Output: il numero di telefono dell'abbonato cercato

Algoritmo: si proceda come segue:

- si ponga che l'ultimo nome letto sia "";
- finché l'ultimo nome letto è diverso dal nome da cercare e non si sia raggiunta la fine dell'elenco, si ripeta l'operazione seguente:
 - si legga il nome dell'abbonato successivo (che diventa l'ultimo nome letto);
 - se l'ultimo nome letto è uguale al nome da cercare, si produca in output il numero di telefono accanto all'ultimo nome letto;
 - se l'ultimo nome letto è diverso dal nome da cercare, si produca in output la scritta "il nome cercato non compare nell'elenco".

3.2.4 L'efficienza degli algoritmi

Quest'ultimo algoritmo ora funziona rispetto a tutti i suoi input possibili (rispetto a qualsiasi nome da cercare in un elenco alfabeticamente ordinato di abbonati), mentre l'algoritmo precedente funzionava correttamente solo se il nome da cercare era incluso nell'elenco. Questo algoritmo rimane comunque inefficiente; l'efficienza può essere migliorata con qualche modifica minore: è inutile continuare a leggere l'elenco alla ricerca di un nome quando si sia raggiunto un nome successivo nell'ordine alfabetico; per evitare ciò, si potrebbe estendere la condizione che determina la continuazione delle operazioni di lettura come segue: "finché l'ultimo nome letto sia diverso dal nome da cercare, non si sia raggiunta la fine dell'elenco e l'ultimo nome letto non preceda quello cercato". Questo miglioramento, pur significativo, non renderebbe sufficientemente efficiente il nostro algoritmo.

A tal fine è necessario concepire un nuovo algoritmo diverso, che si basa su un'idea completamente diversa rispetto a quella della ricerca sequenziale, che ispirava gli algoritmi

precedenti. Questo algoritmo sarà chiamato **ricerca binaria** poiché procede dimezzando, a ogni lettura di un nome, la lista dei nomi ancora da esaminare.

Ricerca binaria (versione ricorsiva)

Input: il nome Y dell'abbonato cercato: una lista ordinata X di nomi di abbonati, ciascuno affiancato dal relativo numero di telefono

Output: il numero di telefono dell'abbonato cercato

Algoritmo: si proceda come segue:

- se la lista da esaminare non è vuota si proceda nel modo seguente:
 - si legga il nome W dell'abbonato che si trova alla metà della lista X;
 - se il nome Y dell'abbonato cercato è uguale a W, allora si produca in output il numero di telefono di W;
 - se invece il nome Y dell'abbonato cercato segue W nell'ordine alfabetico, allora si esegua l'algoritmo Ricerca binaria (versione ricorsiva) applicandolo all'abbonato da cercare Y e alla seconda metà della lista X;
 - se invece il nome Y dell'abbonato cercato precede W nell'ordine alfabetico, allora si esegua l'algoritmo Ricerca binaria (versione ricorsiva) applicandolo all'abbonato da cercare Y e alla prima metà della lista X.
- se invece la lista da esaminare è vuota, si proceda nel modo seguente:
 - si produca in output la scritta "il nome cercato non compare nell'elenco"

L'esecutore di questo algoritmo, dopo averne iniziata l'esecuzione, esegue nuovamente quello stesso algoritmo, applicandolo ai dati risultanti dalla elaborazione in corso. Le istruzioni di un algoritmo possono quindi comprendere l'indicazione di applicare quello stesso algoritmo a dati risultanti dalla sua esecuzione parziale, senza che ciò comporti un circolo vizioso. Gli algoritmi aventi che richiedono di applicare se stessi ai risultati della propria esecuzione si dicono **ricorsivi**.

Per esemplificare il processo cui dà luogo l'esecuzione di un algoritmo ricorsivo, assumiamo di ricercare il numero di Rossi Mario in un elenco contenente un milione di nomi in ordine alfabetico, usando l'algoritmo della ricerca binaria. Seguendo le indicazioni di tale algoritmo, leggiamo il nome in posizione 500.000. Poiché il nome in posizione 500.000, in ipotesi Marrone Giulia, precede Rossi, allora dobbiamo ricercare Rossi Mario nella seconda metà dell'elenco. A tal fine dobbiamo usare lo stesso algoritmo della ricerca binaria, stavolta applicandolo solo all'elenco costituito dai nomi tra 500.000 e 1.000.000. Seguendo ancora l'algoritmo leggiamo il nome che sta alla metà di tale elenco, cioè il nome in posizione 750.000. Poiché il nome situato in posizione 750.000, in ipotesi Turchese Elena segue Rossi Mario nell'ordine alfabetico, dobbiamo applicare ancora il nostro algoritmo di ricerca, ma stavolta solo alla sezione tra 500.000 e 750.000. Di conseguenza saltiamo alla metà di quella sezione, cioè al numero 625.000.

Procedendo così per una ventina di volte arriviamo a ridurre la lista dei nomi da esaminare alla lista che contiene il solo nome Rossi, cioè alla lista il cui nome in posizione centrale è appunto il nome Rossi, che quindi sarà annotato come output.

Anche quest'ultimo algoritmo dà spunto ad alcune considerazioni. Si può osservare che rispetto all'algoritmo precedente (per la ricerca sequenziale), l'algoritmo per la ricerca binaria è meno semplice; tuttavia esso è più efficiente. Per trovare un nome in un elenco di un milione di abbonati usando la ricerca sequenziale, dobbiamo leggere, in media, 500.000 nomi, per un tempo di 250.000 secondi (circa 7 ore). Seguendo il nuovo algoritmo ci basta leggerne una ventina, cioè ci basta un tempo di 10 secondi. Di conseguenza, il nuovo algoritmo è addirittura circa 25.000 volte ($250.000/10$) più efficiente del precedente, rispetto a un elenco di 1.000.000 di abbonati.

Sarebbe possibile ottenere un algoritmo di ricerca ancora più efficiente. Infatti, quando apriamo un elenco del telefono non ci posizioniamo sempre al centro dell'elenco, ma piuttosto in una posizione che ci aspettiamo si avvicini al nome cercato (ad esempio, se il nome inizia con la lettera "A", apriremo l'elenco verso l'inizio, e se il nome inizia con la "V", verso la fine). Corrispondentemente, potremmo migliorare l'algoritmo di ricerca, specificando che si vada a leggere non il nome collocato nella posizione centrale della porzione della lista ancora da esaminare, ma quello collocato nella posizione nella quale vi è maggior probabilità di trovare il nome cercato, tenendo conto della distribuzione dei nomi tra le diverse lettere dell'alfabeto. Bisogna valutare se il limitato incremento di efficienza che potremmo ottenere in questo modo giustificherebbe lo sforzo richiesto per progettare un algoritmo assai più complicato di quello considerato.

3.2.5 Precisazione del concetto di algoritmo

Non esiste un concetto condiviso di algoritmo: gli studiosi tendono a concordare su alcuni aspetti fondamentali.

Un algoritmo, in un senso molto generico, è *una sequenza di istruzioni che specifica una combinazione di azioni da compiere per risolvere un problema*. Ciò vale tanto per le procedure che riguardano operazioni materiali, quanto per quelli che riguardano elaborazioni simboliche. Nel campo dell'informatica, le azioni da considerare sono solo quelle computazionali.

Ogni azione indicata nell'algoritmo deve essere **eseguibile** da parte dell'esecutore dell'algoritmo, non debbono esserci dubbi per quanto riguarda l'ordine nel quale eseguire le azioni: per qualsiasi azione della procedura, l'algoritmo deve individuare la successiva. La certezza sull'ordine di esecuzione non esclude che l'ordine dipenda da condizioni la cui verifica è affidata all'esecutore stesso; tuttavia, verificate quelle condizioni, l'esecutore deve essere in grado di determinare in modo univoco la prossima azione da eseguire.

Su altri aspetti del concetto di algoritmo non c'è accordo:

- alcuni informatici limitano il concetto di algoritmo alle procedure finite, la cui esecuzione termini sempre in un tempo limitato; altri estendono tale concetto anche a procedure la cui esecuzione, per certi input, possa non avere termine;
- alcuni parlano di algoritmi facendo esclusivo riferimento a manipolazioni simboliche, altri includono anche procedure che includono operazioni materiali;
- alcuni richiedono che gli algoritmi siano ripetibili o deterministici altri ammettono algoritmi non deterministici, che includono aspetti casuali.

A seconda della nozione di algoritmo che si adotta, certe procedure di calcolo potranno rappresentare o non degli algoritmi (la procedura priva di terminazione non rappresenta un algoritmo per chi ritenga che la terminazione sia caratteristica essenziale dell'algoritmo, rappresenta invece un algoritmo per chi adotti un concetto più permissivo).

Un algoritmo è una sequenza finita di istruzioni ripetibili e non ambigue (secondo Sartor). Tale sequenza di istruzioni, se eseguita con determinati *dati in ingresso* (input), produce *in uscita dei risultati* (output), risolvendo una classe di problemi in un tempo finito. L'algoritmo in senso stretto è dotato delle seguenti proprietà:

- *Finitezza*: l'algoritmo deve portare alla soluzione in un numero finito di passi;
- *Generalità*: l'algoritmo non risolve uno solo problema, ma una classe di problemi;
- *Non ambiguità*: le istruzioni indicate sono specificate univocamente, cosicché la loro esecuzione avviene sempre nello stesso modo, indipendentemente dall'esecutore;
- *Ripetibilità*: dati gli stessi dati in input l'algoritmo deve fornire gli stessi risultati in output.

3.2.6 Algoritmi e processi: correttezza e complessità computazionale

Si può dire che è stata trovata una soluzione algoritmica a un problema, quando è stato escogitato un *algoritmo la cui esecuzione produce la soluzione corretta al nostro problema*, per tutti gli input ammissibili (quali possibili casi del problema cui intendiamo dare soluzione).

Dobbiamo **distinguere** l'algoritmo, quale *specificazione dell'elaborazione da eseguire*, dal *processo della sua esecuzione*, cioè dall'attività mediante la quale l'esecutore svolge l'algoritmo. In generale non c'è rapporto tra lunghezza dell'algoritmo e lunghezza del processo della sua esecuzione: anche un algoritmo molto corto può dar luogo a elaborazioni molto lunghe.

Per risolvere un medesimo problema possiamo usare diversi algoritmi, ispirati a diverse idee o invenzioni algoritmiche; inoltre gli algoritmi non sono tutti uguali:

- alcuni algoritmi conducono a soluzioni corrette, altri invece producono risultati errati (per alcuni dei loro possibili input);
- alcuni algoritmi sono più efficienti di altri (producono il proprio risultato con uno sforzo minore, e quindi in un tempo minore).

Quello della **correttezza** è un requisito preliminare e inderogabile. Spesso si assume che i calcolatori siano infallibili, invece i programmi informatici quasi inevitabilmente contengono errori, e il tempo trascorso a individuare e correggere gli errori tende a superare quello impiegato nella stesura dei programmi. Non esiste alcun metodo preciso (algoritmico) che garantisca l'individuazione di ogni errore in qualsiasi programma; non c'è soluzione al problema della terminazione: non esiste, né è possibile realizzare un algoritmo di validità universale (applicabile ad ogni possibile algoritmo) capace di dirci se un algoritmo si interrompe, applicato a un qualsiasi input. A maggior ragione (essendo la non-terminazione un tipo errore) non esiste alcun algoritmo di validità universale capace di dirci se un algoritmo contenga errori. Non è possibile verificare la correttezza di un algoritmo applicandolo preventivamente a ogni input possibile (gli input possibili potrebbero essere infiniti, o comunque troppo numerosi). Un algoritmo può operare correttamente nella maggior parte di casi, ma cadere in errore rispetto a input particolari: finché l'algoritmo non è applicato a uno di quegli input, l'errore può restare inosservato.

[Esempi di errori algoritmici con conseguenze molto gravi. Per esempio alcuni anni fa il razzo Ariane, diretto nello spazio e carico di preziose apparecchiature, dopo pochi chilometri invertì la rotta schiantandosi al suolo. Ciò era dovuto a un banale errore in uno degli algoritmi destinati a guidare la navigazione del razzo, errore in cui il sistema non era mai caduto nel corso dei test effettuati. In ambito sanitario errori negli algoritmi destinati a guidare il funzionamento di apparecchiature delicate possono causare a morte del paziente.]

Anche l'**efficienza** è un aspetto molto importante negli algoritmi. Alcuni algoritmi generano processi molto efficienti, che in breve tempo conducono alla soluzione del problema; altri generano processi molto meno efficienti, che conducono alla soluzione dello stesso problema in tempi lunghissimi. Per misurare l'efficienza di un algoritmo non basta considerare il suo comportamento in relazione a un input particolare; un algoritmo dà vita a diversi processi di diversa lunghezza a seconda dell'input che gli è stato fornito. Tutti gli algoritmi corretti danno risposte sufficientemente rapide se applicati a input di piccola dimensione. Il problema nasce quando l'input diventi di dimensioni notevoli.

Nel valutare l'efficienza degli algoritmi se ne considera la **complessità computazionale**, che fa riferimento al rapporto tra i due termini seguenti:

- l'aumento dell'ampiezza dell'input d'un algoritmo, e
- l'aumento della lunghezza del processo di esecuzione dell'algoritmo stesso.

Negli algoritmi con bassa complessità computazionale l'aumento dell'ampiezza dell'input determina un piccolo aumento della lunghezza del processo d'esecuzione. Negli algoritmi con media complessità computazionale la lunghezza del processo di esecuzione cresce in proporzione all'ampiezza dell'input. Negli algoritmi con alta complessità computazionale l'aumento dell'input determina un aumento più che proporzionale della lunghezza del processo di esecuzione, tanto che a un certo punto diventa impossibile eseguire l'algoritmo in un tempo ragionevole.

Consideriamo un problema: dato un numero di input, si stabilisca se si tratta di un numero primo, e se il numero non è primo, se ne indichi un divisore (con resto 0). Ecco un possibile algoritmo per risolvere questo problema.

Individuazione del minimo fattore

Input: un numero da esaminare

Output: l'indicazione che si tratta di un numero primo o altrimenti, l'indicazione del più piccolo divisore intero del numero in esame

Algoritmo: Si proceda come segue:

- il valore iniziale del divisore si ponga eguale a 1;
- finché la divisione dà un risultato diverso da 0 e il quadrato del divisore è inferiore al numero esaminato si proceda come segue:
 - si ponga quale divisore il successore del divisore presente (in altri termini, si aggiunga 1 al valore del divisore);
 - si divida il numero in esame per il divisore così calcolato;
- se il resto dell'ultima divisione è 0 si annoti che il divisore è un fattore del numero in esame;
- se invece il quadrato del divisore è superiore al numero in esame, allora si annoti che il numero in esame è un numero primo.

Applicando questo algoritmo, per esempio, a 10 e poi a 13, otterremmo le seguenti risposte: 2 è un fattore di 10; 13 è un numero primo. Che accadrebbe se dovessimo operare con un numero molto lungo? Consideriamo l'ipotesi peggiore, cioè l'ipotesi nella quale l'input sia costituito da un numero primo, e che quindi si debbano considerare tutti i possibili divisori, prima di concludere che si tratta, appunto di un numero primo. Si consideri che ogni volta che si aggiungano 2 cifre al numero esaminato, aumenta circa di 10 volte il numero di divisioni da eseguire.

Se dobbiamo fare 10 divisioni per applicare l'algoritmo a un numero di 2 cifre, ne dovremmo fare circa 100 per applicarlo un numero di 4 cifre, circa 1000 per un numero di 6 cifre, e così via. Quando l'input diventa abbastanza lungo (quando il numero di cifre del numero da esaminare diventa abbastanza alto) il numero di divisioni da eseguire diventa elevatissimo. Se il numero di cui estrarre i fattori diventa ancora più lungo, allora il numero di divisioni necessarie supera la capacità di qualsiasi calcolatore esistente o oggi concepibile.

Si dice che l'algoritmo ha una **complessità esponenziale**. Negli algoritmi con complessità esponenziale, al crescere dell'input non solo il processo di esecuzione si allunga, ma lo fa con un'accelerazione sempre maggiore: al crescere dell'input gli algoritmi con complessità esponenziale diventano così esigenti da diventare intrattabili; nemmeno gli esecutori più veloci riescono a eseguirli in tempi ragionevoli. Questo fatto non deve essere considerato come un dato completamente negativo: lo sviluppo di applicazioni informatiche di grande importanza economica e sociale si basa proprio sul fatto che certe elaborazioni algoritmiche sono intrattabili.

Il nostro algoritmo per calcolare i fattori di un numero dato può essere migliorato, ma non in una misura tale rendere trattabile il problema della fattorizzazione: non si è ancora trovato alcun algoritmo efficiente per l'estrazione dei fattori. Proprio su questo fatto si basa il meccanismo della crittografia a chiave asimmetrica, utilizzato per garantire l'autenticità e la segretezza delle comunicazioni. Per **cifrare** un messaggio (trasformarlo in un testo cifrato, incomprensibile al lettore) o per **decifrarlo** (estrarre il messaggio originario dal testo cifrato) si utilizzano, in combinazione, due fattori primi di grande dimensione (circa 150 cifre l'uno), e il loro prodotto. Il prodotto dei due fattori costituisce la chiave pubblica, accessibile a tutti, mentre i due fattori costituiscono la chiave privata, accessibile al solo titolare. Un messaggio cifrato con la chiave pubblica può essere decifrato solo con la chiave privata, mentre un messaggio cifrato con la chiave privata può essere decifrato solo con la chiave pubblica.

Il meccanismo offre sicurezza grazie al fatto che il problema della fattorizzazione è intrattabile: dato un numero di grandi dimensioni non esistono algoritmi capaci di determinarne i fattori con un'efficienza accettabile. Quindi il prodotto può essere reso pubblico pur mantenendo segreti i suoi fattori. Di ciò ci si può avvalere sia per ottenere riservatezza (per far sì che un messaggio possa essere compreso solo dal destinatario cui è rivolto), sia per ottenere sicurezza (per avere la garanzia che un messaggio proviene dal mittente in esso indicato e non è stato manomesso). Chi cifra il messaggio usando la chiave pubblica (il prodotto) sa che solo chi possiede la chiave privata (i fattori) sarà in grado di decifrarlo. Se il messaggio (o una sua parte) è stato invece cifrato usando la chiave privata, chi lo decifra usando la chiave pubblica sa che il messaggio può provenire solo dal possessore della chiave privata corrispondente, e che non è stato alterato.

3.3.1 Gli algoritmi e le competenze degli automi

Nel considerare il rapporto tra i calcolatori e gli algoritmi dobbiamo porci due quesiti:

- quali algoritmi possano essere eseguiti da un calcolatore,
- come dobbiamo esprimere gli algoritmi affinché essi siano eseguibili da parte di un calcolatore.

La prima è la tesi che ogni algoritmo concerne un particolare (tipo di) esecutore, poiché deve consistere di una combinazione di operazioni eseguibili da quell'esecutore. La seconda è la tesi che ogni calcolatore è una macchina algoritmica universale, cioè che esso è in grado di eseguire qualsiasi algoritmo. La conciliazione delle due tesi è che se l'esecutore è capace di eseguire le azioni atomiche e apprende l'algoritmo per combinarle nell'azione molecolare, esso sarà in grado di eseguire anche l'azione molecolare; apprendendo un algoritmo l'esecutore amplia la propria competenza. Acquisendo l'algoritmo in modo permanente (registrandolo nella propria memoria o comunque su un supporto accessibile), l'esecutore acquista la capacità di eseguire da solo, senza l'intervento di terzi, l'azione molecolare, e di risolvere senza aiuti il relativo problema.

Esempio: un cuoco dotato di ricettario e un cuoco privo di ricettario sono entrambi capaci di eseguire le azioni atomiche che si richiedono in cucina, le azioni elementari, che assumiamo possano essere comprese ed eseguite da qualsiasi persona di media capacità culinaria;

entrambi sono capaci di preparare qualsiasi piatto descritto nel ricettario, se assistiti da un istruttore che indichi loro passo dopo passo le azioni atomiche da eseguire. Tuttavia, solo il cuoco fornito di ricettario (o che abbia memorizzato l'intero ricettario) è capace di preparare qualsiasi piatto da solo, senza aiuti esterni. Entrambi sono cuochi universali, ma solo il secondo è più autonomo: per ottenere una mousse al cioccolato, basta dargli l'istruzione "per favore, mi prepari una mousse al cioccolato"; il cuoco privo di ricettario prepara una mousse al cioccolato solo se gli stiamo al fianco, indicandogli, passo dopo passo, tutte le istruzioni contenute nella ricetta. Il sistema (cuoco + ricettario) rappresenta un esecutore diverso e più competente rispetto al sistema consistente del cuoco-in-sé (l'esecutore hardware): grazie all'integrazione delle competenze atomiche del cuoco in sé e delle informazioni contenute nelle ricette, il sistema (cuoco + ricettario) riesce svolgere in autonomia compiti che il cuoco-in-sé riuscirebbe a svolgere solo se gli fossero impartite da un terzo istruzioni dettagliate. Possiamo forse concludere che il sistema (cuoco + ricettario) rappresenta un nuovo cuoco, un cuoco virtuale, che trae origine dall'integrazione del cuoco-hardware (il cuoco-in-sé) e dell'elemento informativo (il ricettario).

Considerando l'hardware di un calcolatore, che è in grado di compiere poche operazioni atomiche con numeri binari; l'insieme delle operazioni atomiche è di solito diverso per diversi modelli di calcolatore. Se un calcolatore ha competenze limitate, come è possibile che mediante elaborazioni informatiche si dia vita alle innumerevoli realtà virtuali? Un calcolatore può acquistare la capacità di eseguire nuove azioni, che non rientrano nella lista delle azioni atomiche a esso innate, qualora gli si forniscono algoritmi opportuni, che realizzino le nuove azioni mediante la combinazione delle azioni atomiche del calcolatore. La competenza di un calcolatore accresce (acquista la capacità di eseguire nuovi compiti) quando il calcolatore abbia accesso ad algoritmi che gli indicano come eseguire azioni molecolari.

3.3.2 Comprensione umana ed esecuzione automatica

Un **programma** è un testo, una sequenza di parole, a loro volte composte di caratteri alfabetici e numerici (non differisce dai testi letterari o scientifici, creati dagli esseri umani per registrare i propri pensieri e comunicarli ad altri). La specificità dei programmi consiste nel fatto che essi sono suscettibili di essere eseguiti automaticamente da parte di un calcolatore. I programmi debbono essere espressi in linguaggi eseguibili da parte del calcolatore.

I programmi per calcolatore sono destinati all'esecuzione automatica, ma anche alla comunicazione umana. Da un lato la comprensione umana del software è preconditione della sua proficua utilizzazione automatica, la comprensione umana del software non si esaurisce con la preparazione dello stesso, ma continua ad accompagnare l'utilizzo, ai fini della correzione e dell'adattamento. D'altro lato, l'esecuzione automatica del software è funzionale alla sua comprensione da parte dell'uomo; solo esaminando questa è possibile coglierne il significato, rilevandone pregi e difetti.

Il software è intermediario tra uomo e macchina, non può essere ridotto a una sola dimensione, né alla mera formula logica o matematica (destinata alla comprensione umana), né al mero dispositivo automatico (destinato alla esecuzione meccanica). Esso è duplice; opera nella comunicazione tra persone e macchine, e nella comunicazione tra le persone che si occupano del medesimo problema informatico, che cooperano alla sua soluzione.

La funzione comunicativa del software trova profili giuridici; ad esso appartengono il codice sorgente, redatto dal programmatore e leggibile da parte dallo stesso, il codice oggetto o eseguibile, risultante dalla traduzione automatica del sorgente in un testo eseguibile da parte della macchina; appartengono le indicazioni accessorie che ne costituiscono la documentazione. Il software è forma di cultura e manifestazione del pensiero, anch'esso ricadrà sotto le garanzie giuridiche che riguardano le manifestazioni dell'ingegno umano e gli oggetti culturali.

La dimensione rappresentativa e comunicativa del software è alla base dello sviluppo dei linguaggi e delle metodologie della programmazione, la cui evoluzione risponde all'esigenza di facilitare la comprensione dei programmi informatici; esigenza che è divenuta più importante in seguito alla formazione e alla crescita della società dell'informazione, che ha condotto alla realizzazione di sistemi informatici sempre più ampi e complessi, costituiti da componenti sempre più eterogenee. Per consentire all'uomo di capire e controllare tali sistemi, si sono dovuti elaborare strumenti (linguistici e metodologici) che consentissero di organizzare questa complessità, di suddividerla e strutturarla in modo da renderla affrontabile da parte della mente umana.

3.3.3 I linguaggi di programmazione

Agli albori dell'informatica chi volesse governare un calcolatore doveva utilizzarne direttamente il linguaggio macchina; le istruzioni prescrivevano operazioni concernenti numeri binari e possono essere analizzate in due segmenti: il **codice dell'operazione**, che indica l'elaborazione da eseguire, e l'**indirizzo dell'operando**, che indica la cella di memoria contenente il dato su cui eseguire l'operazione; solo algoritmi semplici e brevi si possono esprimere in questa forma. Diversi calcolatori sono in grado di eseguire diverse istruzioni atomiche, specificate usando diversi codici binari, un programma in linguaggio macchina può funzionare solo su un particolare tipo di macchina: per eseguire la medesima elaborazione su un diverso calcolatore sarebbe necessario riformulare il programma, trasformandolo in una combinazione di azioni atomiche di tale diverso calcolatore, espresse con i relativi codici binari.

Il superamento dei limiti del linguaggio macchina si ottenne formulando le istruzioni destinate al calcolatore in un linguaggio più facilmente comprensibile all'uomo, e affidando al calcolatore il compito di tradurre tale formulazione nel proprio linguaggio macchina: l'uomo predispose una formulazione algoritmica usando un linguaggio a sé congeniale; tale formulazione diventa l'input di un processo computazionale, eseguito dal calcolatore, seguendo le istruzioni di un programma traduttore; la traduzione ottenuta è eseguita dal calcolatore.

Successivamente sono stati creati dei linguaggi di alto livello, che consentono all'uomo di esprimere in modo sintetico e intuitivo le istruzioni che indicano le elaborazioni da eseguire e al calcolatore di tradurre le istruzioni in univoche combinazioni di istruzioni del suo linguaggio macchina. Il programma informatico espresso in un linguaggio di alto livello può essere tradotto nei diversi linguaggi macchina di diversi calcolatori, e quindi può essere eseguito da ciascuno di quei calcolatori.

Mediante l'**interpretazione**, il programma sorgente è tradotto in linguaggio macchina istruzione per istruzione, con esecuzione di ogni istruzione; a differenza della **compilazione**, l'interpretazione non dà luogo a una versione permanente in linguaggio macchina: le due tecniche di traduzione comportano diversi vantaggi e svantaggi. Il principale vantaggio della compilazione è la maggiore velocità d'esecuzione del programma compilato rispetto al programma interpretato. L'interpretazione permette di modificare il programma interpretato ed eseguirlo immediatamente, così da verificare l'effetto delle modifiche apportate, mentre la modifica del programma compilato richiede la correzione del programma sorgente e una nuova compilazione; i programmi interpretabili hanno il vantaggio di poter essere eseguiti su diversi tipi di calcolatore, grazie all'indipendenza dei linguaggi di alto livello rispetto alla macchina. La compilazione offre un importante vantaggio nella distribuzione commerciale, consentendo di separare il codice oggetto dal codice sorgente; il produttore può scegliere di distribuire solo il codice oggetto (il compilato) mantenendo segreto il sorgente, o di distribuire entrambi i codici a condizioni diverse: mantenendo segreto il sorgente il produttore impedisce a concorrenti e utenti di riutilizzarlo, in tutto o in parte, in nuovi software. Per conciliare i vantaggi commerciali della compilazione con l'esigenza di distribuire un'unica versione del software, funzionante su ogni tipo di macchina, è stata creata una versione intermedia tra codice sorgente e codice oggetto, che come l'oggetto non è comprensibile e modificabile da parte dell'uomo, e come il sorgente può essere utilizzata su ogni tipo di macchina.

3.3.4 Lo sviluppo del software

Lo sviluppo del software è un'attività articolata, la **stesura del programma** rappresenta solo una delle fasi. La parte più importante di un progetto software è l'**analisi**, nella quale si indicano gli obiettivi da realizzare e i modi in cui raggiungerli; all'interno dell'analisi si fa l'**analisi dei requisiti**, nella quale si individuano le funzioni che il sistema deve realizzare, e la **fase della specificazione dei requisiti**, in cui si individuano le caratteristiche del software e le modalità del suo inserimento nell'organizzazione cui è destinato. Successivamente si ha la **fase di progettazione** in cui si decidono l'articolazione del software in moduli e la definizione dei rapporti tra questi. Viene la **programmazione**, la scrittura dei programmi che realizzano i singoli moduli; che può apparire come l'attività principale, realizza il risultato operativo finale in cui culminano le fasi precedenti. Nella **fase di verifica** si accerta che il software sia privo di errori e risponda adeguatamente alle esigenze; fase in cui bisognerà controllare il funzionamento del programma con i più diversi input e casi d'uso, al fine di individuare e correggere gli errori.

La preparazione del software è completata dalla **documentazione**, documenti intesi a illustrare la struttura e il funzionamento del sistema informatico prodotto, necessari per guidare chi utilizza il sistema e per agevolare il compito di chi debba intervenire successivamente su di esso, per correggerne gli errori, aggiornarlo o estenderlo.

Una volta che il software sia entrato in funzione, il lavoro informatico non cessa; ma si entra nella fase di **manutenzione**: si distingue una **manutenzione correttiva**, volta a rimediare agli errori sfuggiti alla fase di verifica, e una **manutenzione integrativa**, volta ad arricchire il software di nuove funzioni. Nella manutenzione integrativa si distinguono le **integrazioni necessarie** o utili perché il software possa svolgere appieno le proprie funzioni, dalle integrazioni che attengono alla realizzazione di funzioni ulteriori rispetto a quelle considerate durante la progettazione.

3.3.5 Componenti e tipologie del software

Nel software si distinguono diverse **componenti**:

- La **componente concettuale** è costituita dagli algoritmi e dall'architettura del software, si distinguono le **idee innovative**, cioè le invenzioni algoritmiche o invenzioni di software capaci di dar luogo ad algoritmi che migliorano rispetto allo stato dell'arte;
- La **componente testuale** è costituita dal programma che esprime la componente concettuale in una forma elaborabile automaticamente. Al programma originale possiamo contrapporre i programmi derivati, che risultano dalla traduzione o dalla modifica del programma originale;
- La **componente materiale** è costituita dalla registrazione della componente testuale su un determinato supporto fisico, cartaceo o informatico;
- La **componente virtuale** è costituita dalla dinamica che risulta dal processo di esecuzione della componente materiale.

Sotto il profilo della **funzione**, si possono distinguere le seguenti tipologie di software:

- **Software di sistema**: offre le funzioni di base per il funzionamento del sistema informatico;
- **Software per la programmazione**: destinato alla realizzazione di applicazioni informatiche, allo sviluppo di nuovi programmi e sistemi; comprende l'interprete o il compilatore, necessari per rendere eseguibile il programma sorgente;
- **Software applicativo**: comprende i programmi che svolgono le diverse funzioni di cui l'utente ha bisogno.

Sotto il profilo del loro **utente**, i software si possono distinguere in:

- **pacchetti standardizzati**, destinati a rispondere alle esigenze di una vasta cerchia di utenti, e offerti a essi in un'unica forma;
- **software su misura**, sviluppati per le esigenze specifiche di uno o più clienti.

Ulteriori distinzioni attengono al regime giuridico al quale il software è assoggettato.

3.4.1 Il software quale bene economico

Il software, sia nella sua componente testuale sia nella sua componente concettuale, è una **realtà astratta** (una configurazione di simboli o idee), e possiede due qualità che lo differenziano dai beni concreti, costituiti da porzioni di materia o energia, e lo assimila agli altri oggetti della proprietà intellettuale (come le opere artistiche o le invenzioni industriali).

Il suo uso è **non-rivale**: più individui possono utilizzare lo stesso software senza che l'utilizzo degli uni diminuisca l'utilità che altri ne traggono. Il suo uso è **non-escludibile**: non si può impedire ad altri di utilizzare un software una volta che essi abbiano accesso a esso, se non adottando misure giuridiche o tecnologiche che limitino l'accesso al bene. (Se io vengo in possesso di un software lo posso usare sul mio computer indipendentemente dalla volontà altrui.)

La disciplina della **proprietà intellettuale**, subordinando il lecito utilizzo di un software al consenso del titolare dei diritti di sfruttamento economico sullo stesso, lo rende **escludibile**: se non vi fosse la proprietà intellettuale sarebbe possibile utilizzare qualsiasi software senza violare la legge, la regolamentazione giuridica rende ciò illecito, e nella misura in cui sia efficacemente applicata, lo rende rischioso o sconveniente. Sul software, attraverso la proprietà intellettuale, viene creato un monopolio temporaneo a favore del titolare dei diritti di sfruttamento economico: il software proprietario può essere usato solo con il consenso del titolare (secondo la disciplina attuale la durata di tale monopolio è estremamente ampia, estendendosi fino a 70 anni dalla morte dell'autore).

Le misure tecnologiche di protezione possono impedire ai terzi gli usi non autorizzati: la distribuzione del solo software compilato impedisce all'utente di modificare il programma per svilupparlo o adattarlo alle proprie esigenze.

La protezione del software, con misure giuridiche o tecnologiche, si giustifica con *considerazioni economiche* attinenti alle esigenze della produzione. In mancanza di una protezione atta a impedire usi non autorizzati l'autore di un software non potrebbe ottenere guadagni sufficienti a coprire i costi dello sviluppo: i potenziali clienti preferirebbero ottenere copie non-autorizzate (copie "piratate"), a prezzi inferiori, piuttosto che le copie messe in commercio da chi ha creato il software. Chi diffonde copie non-autorizzate potrebbe offrire ai consumatori un prezzo inferiore, non avendo l'esigenza di recuperare i costi sostenuti per lo sviluppo del software.

3.4.2 La tutela del software: diritto d'autore e misure tecnologiche

Il principale modello giuridico per la tutela del software è quello del **diritto d'autore**; il quale rende il software *escludibile*, conferendo a titolo originario all'autore del software una posizione giuridica complessa, che include due fasce di diritti: i **diritti morali** e i **diritti patrimoniali**. I diritti morali (spettano sempre all'autore e sono inalienabili e irrinunciabili) non comportano escludibilità. L'escludibilità deriva dalla componente economica del diritto d'autore, che è costituita da un insieme di diritti esclusivi:

- il titolare dei diritti economici può lecitamente effettuare le utilizzazioni rientranti nei diritti esclusivi;
- il titolare dei diritti economici ha il potere di autorizzare altri a effettuare le utilizzazioni rientranti nei propri diritti esclusivi, nei limiti e nei modi da egli stabiliti;
- quelle utilizzazioni sono precluse a ogni altro soggetto, se non autorizzato dal titolare dei diritti.

Nel caso del software i diritti esclusivi attengono alla duplicazione, e quindi alla stessa esecuzione del programma, e la sua modifica e distribuzione al pubblico: tali attività possono essere compiute lecitamente solo dal titolare del diritto o da chi sia stato autorizzato dallo stesso.

L'autorizzazione all'uso del software viene solitamente conferita ai consumatori mediante un **contratto di licenza d'uso**. *Il titolare del diritto d'autore (licenziante) con tale contratto conferisce alla controparte l'autorizzazione a usare il software entro certi limiti e in certe forme, l'utente (licenziatario) si impegna a rispettare i limiti stabiliti nella licenza, e accetta eventualmente alcune limitazioni di responsabilità.* Il titolare dei diritti può fornire egli stesso una copia del software e ricevere direttamente un corrispettivo dall'acquirente-licenziatario. In altri casi, il titolare dei diritti sarà compensato dal venditore del software, il quale cede copia del software all'acquirente verso un corrispettivo.

Normalmente al licenziatario è trasferita copia del solo **software compilato**, cioè del codice oggetto, e l'autorizzazione comprende solo la facoltà di installare tale codice oggetto sul proprio calcolatore e di eseguirlo. Il software compilato è *chiuso* nel senso che all'utente è preclusa la possibilità di accedere al codice sorgente: egli non è in grado di capire il funzionamento del software dall'interno, né di modificarlo per adattarlo alle proprie esigenze o perfezionarlo in vista di altre utilizzazioni. Tali attività sono **duplicemente impedito**: sono impedito giuridicamente, essendo vietate dalla legge (rientrando nei diritti esclusivi del licenziante e non essendo state autorizzate dallo stesso); sono impedito di fatto, avendo l'utente a disposizione il solo programma compilato.

Il titolare dei diritti può adottare **ulteriori misure tecnologiche** volte a impedire che i possessori di copie del software ne facciano uso in modi non autorizzati e che il software venga illecitamente duplicato. Le misure tecnologiche godono di una protezione giuridica: è vietato compiere attività non autorizzate dopo aver eluso o superato tali misure ed è vietato realizzare o diffondere strumenti atti a superarle.

La disciplina d'autore **delega** ai privati la regolazione dell'uso del software (e delle opere digitali). Tale regolamentazione privata avviene in due forme complementari:

- da un lato mediante i contratti di licenza, che stabiliscono quali utilizzazioni siano giuridicamente consentite agli utenti-licenziatari;
- dall'altro mediante le misure tecnologiche, che determinano quali utilizzazioni siano materialmente possibili agli stessi.

Tale delega ai privati trova un limite solo in poche norme inderogabili, limitate al diritto di effettuare una copia di riserva (backup) quando necessaria, al diritto di tentare di decompilare un software al solo fine di realizzare nuovi prodotti con esso interoperabili, al diritto di correggere un software mal funzionante quando il produttore non risponda alle sollecitazioni in tal senso.

3.4.3 Dal software proprietario al software open source

Nel modello del **software proprietario**, il titolare dei diritti usa una *combinazione di clausole contrattuali e misure tecnologiche* per restringere l'uso del software nei limiti dell'autorizzazione conferita all'utente, autorizzazione che non si estende di regola alla possibilità di duplicare il software.

Il titolare intende conservare a sé il **monopolio**:

- sulla *creazione e distribuzione di nuove copie*, questo gli consente di continuare a ricevere un compenso a fronte della concessione di ulteriori licenze per l'uso del proprio software;
- sulla *modifica e lo sviluppo del proprio software*, monopolio che gli consente di poter trarre ulteriori guadagni dalla vendita delle versioni successive.

Il monopolio dell'autore sulle modifiche e i miglioramenti è protetto dal fatto che il titolare distribuisce il solo *codice oggetto*, che non può essere modificato neppure da esperti programmatori.

Il diritto d'autore interviene a tutela di tale esclusiva vietando la difficile attività consistente nella *decompilazione* del software (il tentativo di risalire dal software compilato al sorgente da cui è stato tratto); tale attività è consentita solo al fine della *interoperabilità*, cioè quando un soggetto cerchi di capire il funzionamento di un programma al fine di realizzare un diverso software con esso compatibile. Viene stabilita la mera liceità della decompilazione, non viene stabilito un diritto di accedere al sorgente, perché nulla garantisce che il tentativo di risalire al sorgente dia il risultato sperato.

Il modello proprietario usa *una combinazione di misure giuridiche* (contratti fondati sul diritto d'autore) *e tecnologiche* (la compilazione), per far sì che il titolare dei diritti possa ottenere un prezzo per il proprio software sufficiente a coprire i costi della riproduzione e di sviluppo.

Tale modello però presenta alcuni aspetti problematici:

- *limita l'uso del software* a quanti abbiamo potuto pagare il prezzo chiesto dal titolare dei diritti. Nel precludere l'uso del software a queste persone si perde l'utilità che esse ne avrebbero potuto trarre senza che alcuno ottenga vantaggi (poiché l'uso è non-rivale, la distribuzione di copie aggiuntive non avrebbe danneggiato gli utenti che hanno pagato il prezzo intero);
- la distribuzione del software solo nella versione compilata comporta una *perdita nella diffusione della conoscenza*. Dalle istruzioni del codice sorgente, l'esperto informatico

è in grado di passare alle operazioni in cui consistono le singole istruzioni, e dalle operazioni prescritte dalle singole istruzioni può risalire alle funzioni svolte dalle combinazioni di istruzioni presenti nel programma e quindi alla funzione svolta dall'intero programma. Il codice oggetto nel suo complesso è inaccessibile dalla mente umana, che è incapace di cogliere la connessione funzionale tra le moltissime istruzioni in linguaggio macchina che compongono un codice oggetto. Un programma è conoscenza, contiene soluzioni a problemi che altri programmatori possono incontrare, idee algoritmiche che essi possono riprendere e sviluppare nel proprio lavoro. Distribuendo il software in versione compilata si impedisce che altri facciano uso di quelle idee. Poiché l'uso delle idee è anch'esso non-rivale (il titolare dei diritti può continuare a usare le idee inglobate nel proprio software anche se esse sono usate da altri) il risultato è una perdita di utilità sociale;

- la distribuzione del solo codice oggetto, in combinazione con la sua protezione mediante il diritto d'autore, comporta *l'impossibilità di sviluppare il software* stesso, di *perfezionarlo* o di *usarne le componenti nello sviluppo* di altri software. Chi fosse interessato a questi usi di un software altrui potrebbe contattare il titolare dei diritti e chiedergli l'autorizzazione a creare software derivati a fronte di un corrispettivo o di una compartecipazione ai guadagni derivanti dalla vendita del software derivato; l'interessato dovrebbe essere certo che il software può essere sviluppato adeguatamente e che il mercato darebbe il risultato atteso, mentre il titolare dei diritti dovrebbe essere certo che l'interessato ha le capacità e l'affidabilità necessaria. In mancanza di tali certezze, e dati i costi della contrattazione, l'affare non si concluderà e le opportunità di sviluppo andranno perdute;
- può comportare una *perdita di libertà e di democraticità*: si tratta della libertà dello sviluppatore e dello studioso di software. Lo specialista di informatica cui sia precluso l'accesso ai software viene privato della libertà di conoscere l'aspetto della sua realtà sociale cui è interessato (libertà di informazione), e della libertà di dare il proprio specifico contributo allo sviluppo culturale (libertà di partecipare alla cultura) e alla discussione delle strutture sociali e politiche (libertà politica). Questa perdita di libertà riguarda anche chi non abbia le competenze per studiare il software, o non sia interessato a farlo, ma può trarre vantaggio dalla conoscibilità del software da parte degli esperti.

Tali problemi hanno determinato la nascita di un modello alternativo, basato su una diversa impostazione giuridica ed economica, il **software open source**. Alle origini del movimento del software open source vi è l'opera di Stallman; il quale si ribellò all'assetto economico-giuridico, che lo privava della libertà di conoscere e modificare i programmi informatici, e di condividere le proprie conoscenze, scoperte, innovazioni: divenne promotore di un diverso regime, che garantisse all'utente, da solo e in collaborazione con altri, le quattro libertà che il regime proprietario gli negava:

- Libertà di eseguire il programma, per qualsiasi scopo;
- Libertà di studiare come funziona il programma e adattarlo alle proprie necessità (l'accesso al codice sorgente ne è un prerequisito);

- Libertà di ridistribuire copie in modo da aiutare il prossimo (libertà 2);
- Libertà di migliorare il programma e distribuire pubblicamente i miglioramenti da voi apportati (e le versioni modificate in genere), in modo tale che tutta la comunità ne tragga beneficio (l'accesso al codice sorgente ne è un prerequisito).

Egli coniò la locuzione **software libero** per designare i programmi informatici ai cui utenti fossero garantite tali libertà, ed elaborò un meccanismo giuridico atto a garantirle, la **licenza GPL** (General Public Licence): il titolare ha il potere di autorizzare altri all'esercizio delle facoltà inerenti ai propri diritti esclusivi e di regolare i modi di tale esercizio. La licenza GPL prevede un'autorizzazione tanto ampia da far venir meno l'esclusività di quei diritti, conferendo irrevocabilmente la pienezza delle quattro libertà al licenziatario del software e ai successivi soggetti cui sia trasferita copia dello stesso.

"Software libero" non vuol dire "non-commerciale" né gratuito. La disciplina del software libero limita le possibilità di guadagno dell'autore (del titolare dei diritti): per la prima copia l'autore può chiedere un prezzo elevato, per le copie successive egli di regola non è più in grado di farlo, perché i potenziali acquirenti possono rivolgersi ai successivi cessionari, i quali possono fornire copia dello stesso software a un prezzo inferiore a quello proposto dall'autore o anche gratuitamente: o l'autore riesce a recuperare tutti i propri costi (e il proprio profitto) con la prima cessione o rischia di lavorare in perdita.

Alle clausole che garantiscono le libertà degli utenti si unisce, nella disciplina della GPL, la clausola del **copyleft** (permesso d'autore): i programmi (le opere derivate) che risultano dalla modifica di un software soggetto a GPL possono essere trasferite ad altri solo se assoggettati anch'essi alla disciplina della GPL (chi ha operato delle modifiche su un software soggetto a GPL non potrà far valere il proprio diritto d'autore sulle modifiche per impedire l'esercizio delle quattro libertà a chi riceva una copia della versione modificata, né potrà distribuire il software solo in versione compilata). Scopo della clausola del copyleft è far sì che il patrimonio del software libero si espanda progressivamente, incorporando perfezionamenti e sviluppi dei programmi liberi. I software disciplinati dalla GPL non sono "di pubblico dominio" (sottratti al diritto d'autore): sono soggetti alla *componente morale del diritto d'autore* e al vincolo del copyleft.

La possibilità di modificare liberamente il software (pur soggetta alla disciplina del copyleft) è **garanzia antimonopolistica** di libertà di impresa: se i partecipanti di un progetto di software libero sono insoddisfatti della direzione presa dal progetto, possono dotarsi di una copia del software e sviluppare un nuovo progetto, anche in concorrenza con quello da cui si sono staccati. Ciò dà luogo alla suddivisione, detta **forking** (biforcazione), del progetto preesistente in rami distinti, che proseguono indipendentemente.

Nel 1984, Stallman fondò la **Free Software Foundation**, allo scopo di promuovere la crescita del **software libero** e iniziò a sviluppare il progetto di un sistema operativo non-proprietario che chiamò **GNU**. Nel 1991 al progetto mancava il nucleo del sistema operativo, indispensabile per il suo funzionamento; nello stesso Torvald pubblicò su Internet il nucleo di un sistema operativo, assoggettando il relativo software alla licenza GPL, e

invitando tutti gli interessati a sperimentarlo e a contribuire al suo sviluppo. Al nucleo fornito da Torvald furono unite alcune componenti di GNU, e grazie alla collaborazione di un crescente numero di sviluppatori, il **Sistema operativo GNU/Linux** fu completato. Fin dalla seconda metà degli anni '90 Linux divenne un concorrente dei sistemi operativi proprietari più diffusi, diffondendosi presso una cerchia sempre più ampia di utenti, sulle più diverse piattaforme hardware. A Linux si affiancarono negli anni successivi, numerosi software soggetti alla disciplina della GPL.

3.4.4 Lo sviluppo del software open source

Lo sviluppo di Linux si basa sulle contribuzioni volontarie e sulla condivisione onnipresente e ricorsiva. Per caratterizzare tale metodo e distinguerlo dallo sviluppo tradizionale, e in particolare dal metodo dello sviluppo a cascata, Raymond contrappone il **bazar** (il variopinto mercato di una città nordafricana o orientale) alla cattedrale.

Nello sviluppo tradizionale si adotta il **metodo della cattedrale**, basato sulla gerarchia, la centralizzazione e la distinzione dei ruoli (progettisti, manager, esecutori); nello sviluppo del software libero si adotta il **metodo del bazar** nel quale coesistono diverse prospettive e iniziative, il progetto è suddiviso in moduli distinti sviluppati in relativa indipendenza e diverse versioni parallele, le decisioni sono decentrate e dinamiche, il coordinamento è fornito dal fatto che tutti rendono disponibili su Internet i risultati del loro lavoro e i commenti sul lavoro altrui.

Nello sviluppo del software open source si procede dal basso verso l'alto (**bottom-up**), anziché dall'alto verso il basso (**top-down**). Gli sviluppatori che partecipano al progetto realizzano moduli che si integrano con quelli già esistenti, secondo la propria percezione e valutazione delle esigenze del progetto, e delle proprie competenze e interessi. Ne risulta uno **sviluppo incrementale-evolutivo** (anziché pianificato), dove la comunità degli sviluppatori e degli utenti stabilisce, con le proprie autonome scelte, quali proposte avranno successo, e quindi incideranno sullo sviluppo e l'articolazione del progetto complessivo.

In un progetto su ampia scala, come Linux, questa dinamica dal basso si combina con il controllo e la revisione effettuati dal gruppo delle persone che coordina il progetto, le quali decidono quali modifiche e quali nuove funzioni includere nelle successive versioni del sistema nel suo complesso. Si tratta di una funzione di guida e controllo che non si basa su gerarchie giuridicamente definite, ma piuttosto sul prestigio dei coordinatori del progetto e sull'aspettativa che il software da essi rilasciato sarà poi generalmente utilizzato e ulteriormente sviluppato (effetto di rete).

Non tutti i tipi di software sono ugualmente suscettibili di essere sviluppati e distribuiti in open source, e i modelli del software proprietario e del software open source non sono necessariamente in conflitto, ma possono svolgere ruoli complementari (numerose imprese sviluppano software con doppia licenza, una versione libera, limitata alle funzioni di base, e una versione proprietaria, arricchita di funzionalità ulteriori, disponibile a pagamento).

3.4.5 Disciplina giuridica e distribuzione del software: classificazioni e terminologia

Per classificare i software sulla base della loro disciplina giuridica dobbiamo distinguere:

- **Software proprietario**, il cui uso è ristretto dalle esclusive del diritto d'autore, e viene conferito secondo una licenza che limita le libertà dell'utente. Tale licenza conferisce al licenziatario la sola facoltà di usare il software, senza poterlo distribuire o modificare. Di regola il software proprietario è chiuso, cioè di esso viene fornito solo il codice oggetto (il compilato), mentre il licenziante trattiene presso di sé il sorgente.
- **Software open source**, il cui uso è concesso con una licenza che conferisce al licenziatario la piena libertà di eseguire, studiare, modificare, distribuire il software. La libertà di distribuire un software open source può essere soggetta alla sola condizione del permesso d'autore (copyleft): cioè all'obbligo di assoggettare a licenza open source anche le modifiche di tale software.

Qualora il titolare dei diritti rinunci irrevocabilmente ai propri diritti economici, e non limiti la distribuzione con la clausola del permesso d'autore (copyleft), chiunque potrà usare, modificare, e distribuire il software, ma potrà rivendicare il proprio diritto d'autore sulle versioni che includano le proprie modifiche, e distribuire tali versioni con licenze proprietarie ed esclusivamente nel codice oggetto: si parla di **software di pubblico dominio**, cioè del tutto sottratto alla disciplina del diritto d'autore per quanto riguarda gli aspetti economici.

Freeware (software gratuito): identifica programmi ottenibili gratuitamente, che possono essere usati e distribuiti dagli utenti, ma non possono essere modificati.

Shareware (software condiviso): fa riferimento al software distribuito gratuitamente, ma solo per un tempo limitato o con funzioni limitate, al fine di indurre l'utente ad acquistare la versione definitiva o completa.

Software-come-servizio (software-as-a-service): il software non è installato nel computer dell'utente ma su un server remoto, cui l'utente accede attraverso Internet. In questo caso fruisce del servizio offerto dal software residente sul sistema informatico del fornitore senza installare il software nel proprio calcolatore.

3.5 Sviluppi della programmazione

Il **programmatore** indica al calcolatore l'algoritmo da eseguire, e il calcolatore lo esegue fedelmente.

3.5.1 La programmazione procedurale: il calcolatore quale esecutore di algoritmi

Secondo il **modello tradizionale**, il calcolatore è un "utile idiota", il fedele esecutore di un algoritmo concepito dall'uomo, ed espresso in un programma informatico: riceve in input il programma che esprime l'algoritmo, accompagnato dai relativi dati, esegue l'elaborazione, consegna i risultati, e resta in attesa di un nuovo input. Il calcolatore elabora i dati secondo il programma e consegna il risultato dell'elaborazione.

3.5.2 La programmazione a oggetti: il calcolatore quale ambiente di oggetti virtuali

I sistemi informatici devono rispondere a tante esigenze e reagire a tanti stimoli provenienti dall'esterno: diventa difficile progettare un software di ampie dimensioni come un oggetto unitario. Si tratterebbe di un'unica combinazione di istruzioni, il cui ordine di esecuzione sarebbe condizionato dalla realizzazione di un elevatissimo numero di condizioni. Il singolo programmatore sviluppa singoli moduli di un progetto complessivo cui partecipano molti altri programmatori, e anche i singoli moduli risultano dalla combinazione di software preesistenti. Il programmatore si limita a integrare i software preesistenti, e a sviluppare le porzioni eventualmente mancanti.

Un software di ampie dimensioni diventa più facilmente comprensibile se concepito e organizzato secondo un'architettura composta da un insieme di oggetti (entità) indipendenti, che interagiscono scambiandosi messaggi. Ciascuno di tali oggetti dispone di piccoli programmi, chiamati **metodi** (diversi per diversi tipi di oggetto), e contiene i propri dati, che rappresentano i valori degli attributi dell'oggetto.

L'**oggetto** attiva i propri metodi sulla base dei valori dei propri attributi, quando ne sussistano le condizioni. Ogni oggetto è chiuso verso l'esterno: la rilevanza e l'effetto dell'input dipende da come esso è valutato all'interno dell'oggetto stesso.

Lo sviluppo di un sistema software consiste nella creazione di un ambiente nel quale i diversi oggetti possano interagire e poi nella definizione di ciascuno di essi, specificandone l'interfaccia verso l'esterno e i programmi e dati che contiene.

Il calcolatore rimane un **esecutore di istruzioni** espresse nel suo linguaggio macchina anche quando esso anima un sistema informatico consistente di molteplici oggetti in interazione: l'esecuzione di tali istruzioni determina il comportamento degli oggetti e la dinamica delle interazioni tra oggetti. Il fatto che le attività degli oggetti risultino, dall'esecuzione dei calcoli binari, non giustifica una prospettiva riduzionista, che consideri oggetti e loro interazioni come una mera apparenza.

Negli ultimi anni, si parla del passaggio da un'architettura basata sugli oggetti, ad un'**architettura basata sui servizi**: l'oggetto software, anziché essere racchiuso nell'ambito d'un particolare sistema, dovrà essere capace di interagire con qualsiasi persona (o programma) ne richieda il servizio, secondo convenzioni (protocolli) condivisi. L'oggetto software diventa quindi il fornitore di un servizio che deve essere ben definito. Le applicazioni informatiche si configurano come configurazioni di reti di sistemi fornitori di servizi, che si sovrappongono e si adattano all'evoluzione della tecnologia e della domanda. All'architettura informatica si affianca un'architettura giuridica, che fissa le regole e le responsabilità secondo le quali i diversi servizi debbono essere forniti e integrati.

3.5.3 I sistemi basati sulla conoscenza: Il calcolatore quale ragionatore automatico

Il calcolatore può acquisire **ulteriori competenze** rispetto alle proprie competenze innate, acquisendo nuovi algoritmi: può essere dotato di *algoritmi per il ragionamento* (che consentano di passare, date certe premesse, alle conclusioni logicamente fondate su tali

premesse). Il calcolatore diventa capace di passare da premesse a conclusioni (**processi di inferenza**): anche quando compie ragionamenti, il calcolatore si limita ad eseguire i semplici calcoli binari, ma combinazioni complesse di quei calcoli, effettuate secondo le indicazioni di un programma ragionatore (tradotto nel linguaggio macchina) danno luogo agli stessi processi di inferenza che effettua anche la nostra mente, quando compie ragionamenti logicamente corretti. L'esecutore algoritmico si è trasformato in un **ragionatore automatico**: la programmazione diventa **programmazione logica**, consistente nell'esprimere la conoscenza (le premesse del ragionamento) in un linguaggio logico, cosicché il sistema possa compiere ragionamenti automatici basati su quella conoscenza.

Sono stati realizzati sistemi informatici in grado di compiere diversi tipi di ragionamento: ragionamenti deduttivi, defeasibile (vincibili da argomenti in contrario, probabilistici, induttivi, abduttivi, ecc). Il tipo di ragionatore automatico maggiormente usato, anche in ambito giuridico, è il più semplice, che si **limita all'applicazione di regole**. Ci possiamo chiedere se sia ancora necessaria la programmazione, cioè, la specificazione di algoritmi in un linguaggio di programmazione, quando il calcolatore sia usato come ragionatore automatico. In un certo senso la risposta è affermativa: le conoscenze (le regole) che forniamo al sistema sono il suo programma, determinando il modo nel quale il sistema svilupperà le proprie inferenze. In un altro senso potremmo negare che si tratti di vera programmazione: le regole non indicano direttamente al calcolatore come esso si debba comportare: esse sono dati forniti al programma ragionatore, che li utilizza autonomamente, secondo il proprio algoritmo per il ragionamento.

3.5.4 Le reti neurali: il calcolatore quale modello del cervello

Le **reti neurali** sono un modello di sistema informatico usato con successo in alcuni ambiti dell'intelligenza artificiale: riproducono il funzionamento delle strutture del nostro cervello, i neuroni e le loro connessioni. Il comportamento intelligente non risulti solo e soprattutto dal ragionamento: **l'intelligenza**, intesa come la capacità di comportamento efficace e flessibile. Le reti neurali artificiali permettono di fornire a un calcolatore una rete neurale, un modello informatico dei neuroni e delle loro connessioni, e algoritmi che determinano l'evoluzione della rete, il suo adattamento all'esperienza. I calcolatori che attivano e modificano le reti neurali continuano a macinare calcoli binari, ma quei calcoli determinano il funzionamento dei neuroni, le loro interazioni, le modifiche della rete, e danno vita al sistema adattivo.

3.5.5 La programmazione ad agenti: il calcolatore quale motore di società virtuali

Il modello della **programmazione ad agenti**: con **agente** si indica un oggetto informatico capace di azione autonoma, e in particolare di azione intelligente, in contesti complessi. Un sistema informatico multiagente (**multiagent system**) comprende entità che comunicano e che inglobano programmi per l'azione intelligente e le informazioni usate da quei programmi. La programmazione in un sistema multiagente consisterà nel realizzare gli agenti, l'ambiente per la loro interazione, gli oggetti a loro disposizione, le procedure e le regole per la loro coordinazione. Un agente potrà accedere ai servizi offerti in rete, e fornire servizi ad altri agenti.

CAPITOLO 4: I dati informatici

I dati informatici sono dati già classificati e interpretati secondo categorie concettuali, e la selezione e l'organizzazione delle informazioni rilevanti secondo determinate forme o categorie è aspetto essenziale delle applicazioni informatiche.

4.1 Dati e modelli concettuali

L'uomo coglie la realtà solo attraverso la mediazione dei propri schemi concettuali. Anche la scienza coglie il mondo alla luce delle proprie categorie e anche la rappresentazione dei dati in un sistema informatico presuppone una **concettualizzazione**: l'individuazione dei concetti da utilizzare per qualificare e ordinare la realtà rappresentata.

4.1.1 Modelli concettuali e rappresentazioni informatiche

L'input di ogni **processo computazionale** è costituito da dati strutturati secondo una particolare **concettualizzazione**. Quando diverse applicazioni informatiche debbano interagire, operando sugli stessi dati, o scambiandosi dati, è necessario che esse posseggano una concezione comune di quei dati, cioè che quei dati esprimano una categorizzazione operata secondo concetti condivisi. Ogni rappresentazione informatica presuppone una **ontologia**, la determinazione di quali tipi di cose (entità) e di quali rapporti tra esse (associazioni) s'intendano rappresentare, e di quali informazioni su tali cose e rapporti si ritengano rilevanti.

4.1.2 Classi, attributi, istanze e associazioni

Nel linguaggio naturale usiamo i nomi comuni per far riferimento a tutte le entità di uno stesso tipo richiamando le loro caratteristiche comuni: associamo al nome un contenuto concettuale.

Quando intendiamo produrre la rappresentazione informatica della realtà corrispondente a un certo termine, è importante avere un'idea precisa del senso in cui stiamo usando quel termine. Nell'informatica un concetto generale usato per denotare oggetti particolari è solitamente denominato **classe**: una volta precisata questa, è necessario stabilire quali informazioni s'intendono fornire circa gli individui appartenenti a tale classe (quali sono le caratteristiche o attributi della classe). Nel determinare gli attributi di una classe selezioniamo gli aspetti della realtà che riteniamo rilevanti, e che saranno riflessi nel nostro sistema informatico; determiniamo il filtro attraverso il quale il nostro software vedrà la realtà, prestabiliamo che cosa esso considererà rilevante e che cosa irrilevante, che cosa potrà influire o non nelle operazioni del sistema. Tali scelte hanno considerevoli implicazioni sia pratiche sia giuridiche.

Hanno **implicazioni pratiche** perché la qualità dei dati informatici può dipendere in modo decisivo dalla scelta degli attributi. Quando si rappresenta una certa classe di entità in un sistema informatico, è opportuno che vi sia un attributo o una combinazione di attributi che individui in modo univoco uno e uno solo degli oggetti rientranti nella classe di riferimento.

L'indicazione di attributi sovrabbondanti rispetto allo scopo perseguito può condurre a violazioni della tutela dei dati, con particolare riferimento al requisito della necessità dei dati stessi, e ai limiti posti al trattamento dei dati sensibili. Specificando valori determinati per gli attributi, si ottiene **un'istanza della classe**, cioè, la rappresentazione di uno degli individui cui fa riferimento il concetto generale.

I dati contenuti in un sistema informatico colgono i rapporti tra entità, solitamente indicati con il termine **associazioni** (relationship).

4.2 L'organizzazione dei dati

La memoria centrale del computer è **volatile** (essa contiene i dati necessari per l'elaborazione in corso, e viene liberata quando tale elaborazione ha termine): per mantenere i dati nel tempo è necessario registrarli su dispositivi di memoria che consentono la registrazione permanente di grandi quantità di dati, detti **memorie di massa**. La registrazione dei dati su tali memorie ha un aspetto logico che riguarda il modo in cui i dati sono materialmente disposti nei supporti fisici utilizzando le tecniche di magnetizzazione o di scrittura ottica su supporti materiali.

Il livello più basso dell'organizzazione logica dei dati consiste nel **file**, una raccolta di dati identificata da un unico nome, il nome del file. Si distinguono due principali tipi di file:

- gli archivi (file strutturati): contengono un insieme di schede dotate della medesima struttura;
- i file di testo libero o resti (file non strutturati): contengono una sequenza non strutturata di caratteri alfabetici e numerici.

4.2.1 Gli archivi (file strutturati)

In un archivio le **istanze** di una certa classe sono registrate in un modo uniforme; a ciascuna istanza è dedicato un **record** (scheda), che a sua volta è suddiviso in **settori** (ciascuno dei quali contiene il valore di un particolare attributo della classe). Si parla di formato di record per indicare la suddivisione di un record in determinati campi.

La registrazione dei record nei supporti fisici dipende dal software utilizzato per creare e aggiornare l'archivio; è necessario distinguere i diversi campi. Si possono adottare diverse tecniche per esprimere la strutturazione della scheda in modo che essa sia riconoscibile da parte della macchina:

- una possibile soluzione consiste nel distinguere i diversi dati in base alla loro posizione all'interno della scheda;
- una tecnica diversa consiste nell'indicare espressamente la natura di ogni dato.

4.2.2 I testi (file non strutturati)

I file di testo consistono di **componenti testuali** (sequenze di parole), accompagnate da indicazioni sulla loro presentazione a video o a stampa (i documenti che realizziamo utilizzando software per la redazione di testi).

Negli elaboratori di testi oggi maggiormente usati le indicazioni attinenti alla presentazione dei contenuti testuali sono registrate dal software; la registrazione avviene in una forma non facilmente leggibile da parte dell'utente, essendo destinata alla elaborazione automatica (elaboratori di testo WYS/WYG).

In alcuni casi **l'illeggibilità è completa**: il tentativo di "leggere" il documento registrato nella memoria del computer richiederebbe uno sforzo enorme. Vi sono anche alcuni formati nel quale si ottiene una maggior leggibilità.

Esistono sistemi per la redazione di testi nei quali l'utilizzatore inserisce all'interno del testo le indicazioni per la presentazione, specificando direttamente le modalità di presentazione delle componenti testuali. Per visualizzare il risultato ottenibile a stampa, bisognerà procedere a una sorta di compilazione: sulla base del file sorgente prodotto dall'autore viene prodotto un file visualizzabile e stampabile: le successive revisioni del testo si dovranno compiere sempre sul file sorgente, dal quale potranno essere tratti nuovi file visualizzabili.

4.2.3 Formati di dati

La **registrazione dei dati** informatici avviene in base a certe regole, che definiscono il formato dei dati stessi. Bisogna stabilire come passare dal formato binario a quello alfabetico o decimale necessario alla lettura dei dati da parte dell'uomo: provvedono particolari tabelle di conversione, che stabiliscono un rapporto biunivoco tra caratteri alfabetici e numerici, e certe sequenze di cifre binarie. Occorrono convenzioni secondo le quali esprimere ulteriori informazioni e altre possono indicare come registrare i dati in modo più compatto o renderli fruibili con maggiore efficienza. L'insieme di tali convenzioni costituisce il **formato dei dati**.

I dati registrati in un certo formato possono essere elaborati solo da software specificamente predisposti in modo da trattare quel formato (chi ha registrato i dati in un certo formato li può condividere con altre persone solo se anche queste utilizzano un software adeguato a quel formato). Utilizzare i dati con altro software richiede una conversione, ciò pone in una posizione di debolezza gli utilizzatori:

- chi abbia accumulato una notevole quantità dei dati in un certo formato è vincolato all'utilizzo dell'unico software predisposto per quel formato, per non dover affrontare i costi e i disagi relativi al trasferimento in altro formato;
- chi intenda condividere dati con altri soggetti è vincolato a predisporre quei dati in un formato accettato dai software impiegati da quei soggetti.

Tali vincoli contribuiscono a determinare l'effetto di rete (la tendenza all'ulteriore diffusione dei formati maggiormente diffusi). Ne risulta un effetto tendenzialmente monopolistico: un formato dati e il software a esso associato tendono a dominare il mercato. Il problema è grave quando si tratti di un formato proprietario, sulla cui evoluzione decide un soggetto privato che detiene il diritto d'autore sui software che producono i testi in quel formato controllandone l'evoluzione e l'utilizzo. Lo sviluppatore del formato può mantenerne occulta la specifica, o può fornirla solo a pagamento o comunque a determinate condizioni.

Per rimediare ai problemi determinati dall'uso di formati proprietari (chiusi), sono nati **formati aperti**.

4.3 Basi di dati e information retrieval

L'elaborazione informatica dei dati offre nuove possibilità:

- di aggregare, disaggregare, combinare, elaborare informazioni;
- registrate su diversi archivi;
- di ricercare elementi testuali compresi all'interno di raccolte documentali.

La prima possibilità è offerta dai sistemi per la gestione di basi di dati, la seconda dai sistemi per l'information retrieval (recupero di informazioni).

4.3.1 Le basi di dati

Il termine **banca di dati** fa riferimento a una qualsiasi raccolta "di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo". Il **sistema per la gestione** di basi di dati funge da Intermediario tra gli archivi di dati e gli utilizzatori dei dati stessi: tali sistemi costruiscono nuove classi, combinando informazioni disponibili nei loro archivi e possono calcolare nuovi attributi sulla base dei dati esistenti.

Il **DBMS** (Database management system) consente di rappresentare i dati in modo indipendente dai programmi destinati a usare quei dati e a facilitare l'accesso ai dati stessi. A tal fine esso mantiene dei **dizionari di dati** (data dictionary), raccolte di metadati che specificano il significato e la struttura dei tipi di dati (classi) registrati nella base di dati, e le convenzioni usate nella loro registrazione,

Un DBMS può contribuire ad assicurare la qualità dei dati stessi, sotto i seguenti profili:

- **Coerenza dei dati:** il DBMS permette a diverse applicazioni di utilizzare gli stessi dati, integrandoli e riducendo le duplicazioni (la ridondanza). La riduzione della ridondanza facilita la coerenza: se un certo dato è registrato una sola volta nella base dei dati, basta modificarlo una sola volta per correggerlo o aggiornarlo;
- **Integrità:** il DBMS contribuisce a far sì che la base di dati sia integra (contenga solo dati corretti);
- **Ripristino:** il DBMS comprende procedure automatiche per il ripristino della base dei dati in caso di errori e malfunzionamenti imputabili all'hardware o al software;
- **Sicurezza:** il DBMS controlla l'intera base di dati e quindi può garantire che ad essa si acceda soltanto secondo certe modalità e procedure e dopo avere ottenuto idonee autorizzazioni;
- **Riservatezza:** l'uso di un DBMS può facilitare il rispetto della riservatezza dei soggetti cui i dati afferiscono, specialmente quando si debbano trattare grandi quantità di dati, rendendoli accessibili a diversi utenti. Il DBMS può fornire ad ogni utente la vista sui dati che corrisponda ai suoi diritti di accesso.

4.3.2 Il modello relazionale

Il **modello relazionale** è un modello di base di dati (insieme al gerarchico, reticolare e a oggetti) composto di tabelle che rappresentano determinate classi di oggetti e i loro rapporti, cioè le associazioni. Una classe indica l'insieme degli oggetti di uno stesso tipo e l'istanza della classe indica uno di tali oggetti. Le associazioni collegano elementi di diverse classi.

Il **modello delle classi** e delle loro associazioni può essere trasferito facilmente in una base di dati relazionale:

- ogni classe e ogni associazione è rappresentata mediante una distinta tabella (relazione);
- ogni riga della tabella rappresenta un'istanza della classe o associazione;
- ogni colonna della tabella riporta i valori di un determinato attributo;
- le associazioni tra diverse tabelle sono rappresentate affiancando le chiavi delle entità associate.

4.3.3 L'information retrieval

I software per **l'information retrieval** (ricerca di informazioni) *recuperano* (retrieve) le *informazioni testuali* estraendole da grandi masse documentali. Un tempo tali masse documentali erano organizzate e gestite in modo unitario e centralizzato, i *sistemi documentali* indicavano i sistemi informatici destinati a raccogliere e organizzare documenti testuali in modo da renderle più facilmente ricercabili. Nell'era di Internet la distinzione tra banche di dati e sistemi per l'information retrieval è divenuta meno rigida: gli strumenti per la ricerca di informazioni testuali estraggono informazioni da banche dati organizzate e da raccolte plurime di documenti eterogenei, memorizzati in formati e luoghi diversi.

La **funzione fondamentale** dei software per l'information retrieval consiste nel *fornire all'utente tutti i documenti di interesse*: l'utente è interessato a tutti i documenti che vertano su un certo tema o concetto; egli dovrà formulare un quesito che specifichi il tema di interesse, e il sistema dovrà rispondere al quesito fornendo i documenti attinenti a quel tema. Il quesito e i documenti a esso pertinenti sono formulati in un linguaggio: la ricerca avviene sul piano sintattico (ricercando tutti i testi che contengano i termini specificati nel quesito). Si passa dalla **ricerca sintattica** a quella **semantica** quando il sistema ricerca i documenti che contengono le parole specificate nel quesito e cerca anche tutti i testi che esprimono il concetto indicato nel quesito, in qualsiasi forma esso sia espresso.

La ricerca automatica di informazioni testuali si avvale di **indici**; tale sistema ha due componenti fondamentali:

- **l'indicizzatore**, per la creazione degli indici. L'indicizzatore estrae le parole dai testi e le inserisce nell'indice, provvedendo a indicare per ogni parola la collocazione dei testi che la contengono; infatti, l'indice elenca tutte le parole contenute nei documenti, e riporta per ogni parola la collocazione dei documenti che la contengono. Si possono utilizzare: *tecniche per lo stemming* che associano ogni parola e i relativi documenti

alla radice da cui tale parola è tratta, o *tecniche di lemmatizzazione*, che unificano in un'unica voce dell'indice le diverse varianti sintattiche dello stesso termine.

- il **motore di ricerca** che, sulla base degli indici, individua ed estrae le informazioni richieste (documenti che corrispondono al quesito dell'utente).

4.3.4 Le prestazioni dei sistemi per l'information retrieval

Nella valutazione delle prestazioni dei sistemi per l'information retrieval vi sono due **parametri fondamentali**, dalla cui combinazione risulta l'accuratezza delle ricerche compiute dal sistema:

- il **richiamo** (recall): la quantità di documenti pertinenti ritrovati, in rapporto a tutti i documenti pertinenti contenuti nella base documentale;
- la **precisione**: la quantità di documenti pertinenti ritrovati, in rapporto a tutti i documenti recuperati.

I fenomeni indicati dai termini "richiamo" e "precisione" possono essere colti dalla **prospettiva complementare**, cioè sotto il profilo dei difetti che risultano dalla mancanza di tali pregi:

- il **silenzio** è il difetto nel richiamo: risulta dalla relazione tra i documenti pertinenti non recuperati (i documenti sui quali il sistema è erroneamente silente), in rapporto a tutti i documenti pertinenti contenuti nel database.
- il **rumore** è il difetto nella precisione: risulta dalla relazione tra la quantità di documenti recuperati non pertinenti (i documenti sui quali il sistema è erroneamente rumoroso), in rapporto a tutti i documenti recuperati.

4.3.5 Le interrogazioni booleane

Nell'informatica troviamo la **logica** nel campo dell'hardware e nel campo del software; si può utilizzare anche per **interrogazioni complesse** mediante un motore di ricerca, formulando **interrogazioni booleane**, consistenti nella combinazione logica di più condizioni.

Prendendo in considerazione la **coniunzione logica AND**: una congiunzione $A \text{ AND } B$ risulta vera se e solo se sono vere entrambe le proposizioni A e B ; la richiesta dei documenti che rispettino (per i quali sia vera) una condizione di ricerca congiuntiva, troverà risposta nel recupero dei documenti presenti nel sistema che rispettano entrambe le condizioni indicate. La risposta a **un'interrogazione congiuntiva $A \text{ AND } B$** consiste *nell'intersezione tra l'insieme dei documenti che rispettano la condizione A e l'insieme dei documenti che rispettano condizione B* . Se denotiamo con A l'insieme degli elementi che rispettano la condizione A e con B l'insieme degli elementi che rispettano la condizione B , il risultato della domanda $A \text{ AND } B$ sarà dato dall'intersezione di A e B . L'operatore AND restringe l'insieme dei documenti recuperati: se la condizione A è soddisfatta da 5 documenti, e la condizione B da 6, ma solo 2 documenti rispettano entrambe le condizioni, solo questi saranno recuperati.

Esaminando le **interrogazioni disgiuntive OR**: una disgiunzione $A \text{ OR } B$ è vera se e solo se è vera almeno una delle proposizioni disgiunte. La richiesta dei documenti che rispettino (per

i quali risulti vera) una condizione di ricerca disgiuntiva, troverà risposta nei documenti che rispettino almeno una delle condizioni indicate. L'insieme dei documenti che rispettano la condizione $A \text{ OR } B$ è costituito dall'*unione dell'insieme degli elementi che rispettano la condizione A e dell'insieme degli elementi che rispettano la condizione B*. Se denotiamo con A l'insieme degli elementi che rispettano la condizione A e con B l'insieme degli elementi che rispettano la condizione B, il risultato della domanda $A \text{ OR } B$ sarà dato dall'unione di A e B ($A \cup B$). L'uso della disgiunzione allarga l'insieme dei documenti: se la condizione A è soddisfatta da 5 documenti, la condizione B da 6, e 2 documenti rispettano entrambe le condizioni, saranno recuperati 9 documenti.

Analizziamo la **congiunzione NOT**: A è vera se e solo se è falsa la proposizione negata A. La richiesta dei documenti che rispettino (per i quali risulti vera) una condizione di ricerca negativa, troverà risposta nei documenti che non rispettano la condizione negata. L'insieme dei documenti che rispettano la condizione NOT A sono tutti quelli che non rispettano la condizione A. Se denotiamo con A l'insieme degli elementi che rispettano la condizione A, il risultato della domanda NOT A sarà dato dal complemento di A, cioè da tutti gli elementi nel sistema tolti quelli che rispettano A. L'uso del NOT ha senso solo se combinato con l'uso di altri operatori.

Gli operatori booleani (AND, OR, NOT) non esauriscono quelli comunemente disponibili. I motori di ricerca offrono anche la possibilità di specificare che i termini compresenti (richiesti in AND) debbono essere adiacenti, o di fornire termini di ricerca incompleti. L'**operatore di troncamento** consente di indicare solo l'inizio dei vocaboli cercati: si richiedono tutti i documenti che contengano vocaboli che iniziano con l'espressione troncata. La **funzione di mascheramento** consente di sostituire uno o più caratteri della chiave di ricerca con un carattere "jolly", che indica un qualsiasi arbitrario carattere: la ricerca verte su tutti i termini che coincidono con la chiave di ricerca nei restanti caratteri, ogni documento che contenga uno di questi termini soddisfa la condizione specificata mediante il carattere jolly.

4.4 I linguaggi di marcatura

L'uso di linguaggi per la marcatura (**markup language**) consente di individuare le componenti di un documento testuale racchiudendole all'interno di etichette (**tag**) riconoscibili automaticamente, e di inserire ulteriori informazioni (**metadati**) all'interno del documento, distinguendole rispetto al suo contenuto testuale. I testi vengono arricchiti con indicazioni utili per la loro stampa, visualizzazione, catalogazione, strutturazione, per l'estrazione e l'elaborazione delle informazioni in essi stessi contenute.

I linguaggi di marcatura variano in base ai diversi tipi di markup cui danno luogo:

- i markup **proprietary**: definiti e controllati da uno o più produttori di software;
- i markup **non propriety** (pubblici): definiti e controllati da enti imparziali;
- il markup **leggibile**: una persona potrà, senza notevole sforzo, cogliere le indicazioni di marcatura e individuare le porzioni di testo cui si riferiscono;

- il markup **non leggibile**: a differenza del punto precedente sarà impossibile, o richiederà comunque un notevole sforzo;
- il markup **procedurale**: inserimento, nel documento, di istruzioni per la presentazione del testo;
- il **dichiarativo**: caratterizzazione delle porzioni del testo a seconda della loro funzione nel testo stesso, senza specificare come esse debbano essere presentate o elaborate;
- i **linguaggi di marcatura**: specificano le etichette e i comandi da utilizzare nella marcatura di un testo;
- i **metalinguaggi di marcatura**: consentono al loro utilizzatore di definire il proprio linguaggio di marcatura, di definire etichette che corrispondano ai propri bisogni. Offrono il supporto al markup dichiarativo: consentono di definire linguaggi di marcatura che colgano le componenti strutturali e semantiche proprie a particolari tipi di documento.

4.4.1 HTML e XML

Alla base dei linguaggi di marcatura:

- il **linguaggio HTML**: è il linguaggio normalmente utilizzato nella preparazione di pagine web, nella predisposizione di testi destinati a essere visualizzati in rete;
- il **metalinguaggio XML**: è utilizzato per caratterizzare le componenti strutturali e semantiche dei documenti.

I due linguaggi hanno un comune progenitore; infatti condividono alcuni aspetti. Entrambi si basano sull'idea di qualificare gli elementi del testo raccogliendoli entro etichette, racchiuse tra parentesi angolari: un elemento di un documento marcato è rappresentato da un'etichetta di apertura, un contenuto (il frammento del testo da qualificare) e un'etichetta di chiusura. Presentano anche tratti differenziali:

- **HTML** è strumento per **markup procedurale**, in cui si specifica direttamente la presentazione grafica del testo; **XML** consente di realizzare **markup dichiarativi**, nei quali si caratterizza la funzione semantica degli elementi testuali;
- **HTML** è un **linguaggio di marcatura**: la sua sintassi specifica un determinato insieme di etichette da introdurre nel testo da marcare; **XML** è un **metalinguaggio**: la sua sintassi specifica come l'utilizzatore possa creare le proprie etichette, che poi inserirà nei testi da marcare.

XML offre la possibilità di predefinire tutti gli elementi da usare nella marcatura di un testo. Tale definizione si chiama **DTD**: la definizione di una DTD impone di riflettere sulle etichette da impiegare nel testo e di impostarle in modo coerente, consentendo di verificare se il testo presenti la struttura stabilita nella DTD stessa. Il redatto può essere costretto a rispettare la DTD. Il documento che non la rispetti può essere automaticamente respinto dal sistema; viceversa se il documento rispetta la DTD, si dirà che esso è valido rispetto a essa.

4.4.2 L'elaborazione automatica dei dati documentali

All'interno di un **documento XML** sono identificate le **componenti strutturali** del testo riportato nel documento e *altri dati significativi* associati a quel testo; tali dati possono essere utilizzati nella ricerca e per trattare nel modo più opportuno i documenti. Sulla base dell'indicazione della parte da cui l'atto proviene, di quella cui è destinato, e del tipo di atto, si potranno attivare tutte le **attività consequenziali automatiche**; infatti, inserendo opportune informazioni all'interno di un testo legislativo, sarà possibile estrarne indicazioni circa l'iter o ricostruire automaticamente il testo vigente.

La marcatura XML non specifica le modalità della presentazione del testo (non indica quali parti del testo saranno presentate in corsivo, quali in grassetto ecc); se si desidera ottenere un risultato grafico bisogna indicare come i diversi elementi individuati dalla marcatura XML devono essere visualizzati, si avranno quindi differenze secondo le finalità della presentazione o le preferenze del redattore.

4.4.3 XML e gli standard per I documenti giuridici: rinvio

XML è metalinguaggio che consente di creare diversi linguaggi di marcatura per diversi tipi di testi con le caratteristiche che meglio rispondono alla natura di ciascuna classe e alle esigenze da soddisfare. Si deve quindi definire il **modello documentale** (document model) che caratterizza la classe (la struttura comune a tutti i documenti che ne fanno parte); a tal fine è necessario individuare le componenti strutturali dei documenti, specificare l'articolazione del loro contenuto, e scegliere le etichette che le denominano. Definito il modello documentale, si dovranno marcare i documenti, inserendo in essi le etichette del modello, nella sintassi richiesta.

Nel definire modelli documentali XML ciascuno è **libero** di definire e utilizzare la marcatura che preferisce; tale libertà, se consente la massima flessibilità, può compromettere la comunicazione e la condivisione. I testi in formato digitale non sono destinati al solo autore, né a particolari destinatari, ma sono destinati a essere accessibili a una molteplicità di fruitori, umani o informatici, spesso non circoscrivibili in anticipo: per poter essere accessibili e utilizzabili è necessario siano marcati secondo standard condivisi, sulla cui base possano essere sviluppati software da mettere a disposizione di tutti gli interessati.

I **modelli descrittivi** sono tesi a ricoprire tutti (o quasi) i testi di una certa classe, così da consentire la marcatura di ciascuno di quei testi; devono essere flessibili, così da tener conto della diversità di tutte le particolari istanze di documento che appartengono alla classe: ogni istanza di documento della classe deve rientrare in una delle ipotesi alternative previste dal modello.

I **modelli prescrittivi** sono tesi a indicare requisiti strutturali e sintattici che i testi di una certa classe dovrebbero idealmente possedere. Trova impiego nella gestione informatica dei documenti che a esso corrispondono e nella stesura dei testi: strumenti software verificano

automaticamente se il documento marcato corrisponde al modello prescrittivo cui si sarebbe dovuto conformare, e, in caso contrario, invitano il redattore a correggere il documento.

4.5 Indicizzazione semantica

La **ricerca sintattica** (basata sull'estrazione dei testi che contengono le parole specificate nel quesito) pone dei limiti che vengono superati attraverso lo sviluppo di nuove tecnologie: si possono utilizzare lessici strutturati (organizzano i termini da utilizzare nella ricerca specificando i rapporti tra gli stessi).

4.5.1 I soggettari e gli indici per materia

Una delle soluzioni consiste nell'utilizzo di **soggettari**, liste di termini che individuano i temi o argomenti rilevanti, sul modello delle voci che possiamo ritrovare negli indici analitici e sommari dei manuali giuridici. Termini che possono essere utilizzati come **descrittori dei documenti**, associando un termine a un documento ne descriviamo il contenuto, indichiamo che il contenuto del documento afferisce al tema indicato dal termine. Tale associazione può essere compiuta da un documentalista umano (che scorra i documenti in questione, associandoli ai termini che meglio ne esprimono il contenuto) o in modo del tutto o parzialmente automatico (ricorrendo a software in grado di analizzare il contenuto dei testi e di associarlo ai descrittori opportuni).

Il collegamento tra descrittori e documenti può essere espresso in vario modo:

- **Indice inverso di descrittori:** la lista dei descrittori diviene un indice, in cui accanto a ogni descrittore compaiano i riferimenti (gli indicatori) dei documenti cui il descrittore è stato applicato;
- i descrittori vengono inseriti all'interno dei documenti cui essi afferiscono.

Il soggettario diventa maggiormente utile quando viene **strutturato gerarchicamente**, cioè quando indichi che certi termini di portata più ampia (**iperonimi**) sono sovraordinati a certi termini di portata più ristretta (**iponimi**): la materia indicata dal termine più ampio comprende al suo interno la materia indicata termine più specifico. La disponibilità di un soggettario strutturato gerarchicamente può consentire maggiore precisione nella ricerca documentale, poiché offre la possibilità di utilizzare termini più specifici (in modo da restringere l'ambito dei documenti cercati, riducendo il rumore), o anche di estendere automaticamente la ricerca del termine più generale a tutti i termini che ne rappresentino una specificazione (riducendo il silenzio). L'uso del soggettario nella ricerca automatica presuppone che tutti i documenti siano stati indicizzati usando i termini nel soggettario, e che questo sia noto a chi compie la ricerca stessa.

4.5.2 I thesauri

Il termine **thesaurus** fa riferimento al soggettario che comprenda anche una specificazione dei sinonimi; va a specificare rapporti di iperonimia/iponimia, indica quali termini siano sinonimi (esprimano il medesimo contenuto concettuale), e alcuni si estendono a ulteriori

rapporti tra termini (i termini adempimento e inadempimento sono associati al termine contratto, pur non essendo né sinonimi né specificazioni). Il motore di ricerca che utilizzi un thesaurus può estendere la propria ricerca al di là dei documenti che contengono i termini indicati dall'utente.

Un thesaurus è rappresentato da WordNet, il quale stabilisce anche collegamenti tra i diversi lessici WordNet (nelle diverse lingue) e tra i significati lessicali espressi in quei lessici, dando vita a **thesauri multilinguistici**.

4.5.3 Le ontologie

L'**ontologia** viene utilizzata quando il sistema terminologico (la specificazione del significato dei termini e dei loro rapporti) fornisca un vero modello concettuale, che indica quali sono le classi di entità rilevanti, quali classi sono incluse in classi più ampie, quali sono le condizioni per l'appartenenza a una classe, e le relazioni tra diverse classi. L'**ontologia formale** (i cui contenuti siano definiti, almeno in parte, con precisione logica, e siano elaborabili informaticamente) consente di raffinare la ricerca documentale; se disponiamo di essa possiamo:

- individuare con precisione il concetto che ci interessa e chiedere tutti i documenti attinenti a quel concetto o ai concetti che si trovano in particolare connessione semantica con esso;
- far "ragionare" sistemi informatici;
- far comunicare sistemi informatici che utilizzino diverse terminologie.

Nella costruzione di un'ontologia è spesso necessario distinguere diversi significati di un termine, e definire le relazioni concettuali con precisione. Un'ontologia dei contratti potrebbe distinguere diverse nozioni di contratto, il contratto quale evento (le azioni delle parti che realizzano la stipulazione del contratto), il contratto quale contenuto (le clausole pattuite), il contratto quale documento (il testo prodotto dalle parti che riporta il contenuto del contratto), il contratto quale regolamento (insieme di norme prodotte dal contratto quale evento). Tale ontologia potrebbe indicare che la compravendita è un tipo di contratto (quello il cui contenuto è il trasferimento di un bene verso il pagamento di un prezzo), mentre le parti sono gli attori rispetto al contratto quale evento, la proposta è un evento che rappresenta una parte nel più ampio evento costituito dal contratto nel suo complesso, l'adempimento del contratto è un'attività collegata al contratto, ecc. Il thesaurus si limiterebbe a indicare che il termine contratto è un termine più specifico rispetto al termine accordo e più ampio rispetto ai termini compravendita, parti del contratto, proposta, accettazione, adempimento dei contratti, che proposta è sinonimo di accettazione.

4.5.4 Tipi di ontologie

Le presenti ricerche sulle **ontologie** si differenziano dalle antiche per l'uso di moderni metodi logici e per la finalità attinente alla gestione informatica delle informazioni. Si distinguono:

- **ontologie fondazionali:** si occupano dei concetti più astratti che riguardano tutte le regioni dell'essere;
- **ontologie di dominio:** si occupano di particolari ambiti della conoscenza ed esse possono mirare a coprire un intero ambito disciplinare o possono limitarsi a un particolare aspetto della realtà;
- **ontologie del "nocciolo" di un dominio:** per indicare le ontologie che si limitano a rappresentare i concetti più importanti e all'interno di un particolare ambito;
- **ontologie giuridiche di "nocciolo":** rappresentano i concetti giuridici fondamentali o parte di essi;
- **ontologie giuridiche di domini specifici:** si occupano di determinati settori del diritto;
- **ontologie leggere o linguistiche:** mirano a rappresentare i concetti espressi dai termini del lessico corrente, e le connessioni tra concetti.

4.5.5 Le ontologie informatiche e la tradizione giuridica

Lo sviluppo di **ontologie formali** (e informatiche) in ambito giuridico si connette all'opera di tanti giuristi e filosofi del diritto. La giurisprudenza dei concetti attribuì grande importanza alla definizione dei concetti giuridici ordinandoli in piramidi concettuali: relazioni ontologiche tra classi si mescolano alle relazioni tra materie più ampie e materie più ristrette proprie dei soggetti; tipi di leggi vengono collegati a tipi di posizioni giuridiche e a tipi di atti giuridici.

Una rappresentazione più rigorosa (più ontologica) può trovarsi nella dottrina giuridica italiana tradizionale, gli eventi giuridicamente rilevanti vengono classificati seguendo il metodo platonico della divisione (i fatti sono suddivisi in fatti giuridici e fatti giuridicamente irrilevanti, i fatti giuridici sono divisi in fatti in stretto e atti giuridici, gli atti giuridici sono divisi in atti in senso stretto e negozi, i negozi sono divisi in contratti e altri tipi di negozi, ecc.). Le moderne tecniche per la costruzione di ontologie formali possono collegare analisi giuridiche e realizzazioni informatiche, e facilitare la comunicazione tra giuristi e informatici.

4.6 Le nuove frontiere dei dati: big data e open data

Negli ultimi anni si è assistito ad una crescita nella quantità dei dati disponibili in forma digitale, che ha stimolato lo sviluppo di nuove tecnologie per la loro elaborazione.

4.6.1 Big data

La quantità di dati generati dai calcolatori ormai supera di gran lunga i dati prodotti dagli esseri umani. Questa crescita imponente trova diverse spiegazioni:

- diffusione pervasiva di sistemi che acquisiscono informazioni direttamente dagli ambienti fisici e virtuali, senza la necessità di interventi umani: da un lato, il mondo si è riempito di sensori che acquisiscono dati visivi, sonori, radiotrasmessi, o teletrasmessi dagli spazi fisici; dall'altro lato, gli stessi sistemi informatici possono raccogliere tracce digitali di tutte le operazioni effettuate da, o interagendo con essi;

- il costo della memorizzazione dei dati è sceso rapidamente, rendendo economicamente sostenibile la conservazione di grandi masse di dati, anche non immediatamente utili, ma suscettibili di esserlo in futuro;
- nuovi strumenti software, spesso basati sull'intelligenza artificiale, consentono di estrarre informazioni utili da grandi masse di dati, anche non strutturate: la possibilità di utilizzare con profitto grandi quantità di dati stimola la raccolta di quantità sempre maggiori.

Il termine **big data** fa riferimento a cose che si possono fare a una larga scala che non si possono fare ad una scala più piccola, per ottenere nuove comprensioni, o creare nuove forme di valore, in modi che cambiano i mercati, le organizzazioni e il rapporto tra cittadini e governi. Le tecnologie della **data analytics** consentono di estrarre correlazioni probabilistiche inattese dalle grandi masse dati: tra l'acquisto di un bene da parte di una persona e l'interesse della stessa all'acquisto di altri beni in futuro; tra dinamiche dei mercati e successive evoluzioni di domanda, offerta, e prezzi; tra la scelta di un certi "amici" e l'interesse a stabilire contatti con altre persone; tra gli stili di vita delle persone e certe loro patologie presenti o future. L'uso dei big data offre nuove prospettive alla ricerca scientifica, e consente di effettuare scelte individuali, economiche, amministrative, e politiche sulla base di nuove e più ricche informazioni; vi sono però alcuni rischi, rilevanti per il diritto:

- **privacy**: i big data spesso consistono in dati personali (raccolta automatica delle tracce concernenti le nostre attività su Internet, i nostri acquisti, i nostri spostamenti); a questi si aggiungono i dati che noi stessi trasferiamo su internet. Tutti questi dati, grazie alle correlazioni scoperte dalla data analytics, possono indicare ulteriori informazioni personali, anche sensibili. I big data esprimono esigenze in contrasto con due tradizionali principi del trattamento dei dati personali: la limitazione della finalità e la minimizzazione dei dati.
- **posseduti da pochi soggetti**: quelli che grazie alla loro preminenza monopolistica in alcuni settori delle tecnologie dell'informazione sono in grado di prelevare e immagazzinare le enormi quantità di dati necessari per l'esercizio fruttuoso della data analytics. Tali soggetti sono avvantaggiati rispetto ai concorrenti, e delle autorità pubbliche, che dipendono dai possessori dei big data per le informazioni necessarie allo sviluppo delle proprie politiche.

4.6.2 Open data

Il movimento degli **open data** ha l'obiettivo di rendere i dati il più possibile accessibili a tutti. Si propone da un lato di favorire lo sviluppo della ricerca e la diffusione della conoscenza, dall'altro di estendere ad una più ampia cerchia di utenti le opportunità economiche fornite dall'accesso ai dati.

4.7 La crittografia e l'informatica

Le tecnologie informatiche liberano le informazioni dalla loro dimensione fisica, favorendone la conoscibilità e la modificabilità: le informazioni digitali possono essere riprodotte

istantaneamente e trasmesse a distanza, e possono essere modificate entro limiti dettati solo dalla creatività di chi intervenga su di esse. Vi sono dei casi in cui siamo interessati a limitare la conoscibilità di certe informazioni, vogliamo mantenere riservati certi messaggi escludendo i terzi dalla loro conoscenza; viceversa, in altri casi siamo interessati alla autenticità o integrità dei testi elettronici che inviamo o che ci pervengono: esistono tecnologie informatiche per far fronte a tali esigenze.

4.7.1 Cenni sulla crittografia

Le tecniche crittografiche consentono di trasformare un testo leggibile (testo in chiaro) in un testo non più comprensibile al lettore (testo cifrato) e di risalire dal testo cifrato al testo in chiaro. La crittografia esiste da più di 2000 anni, Giulio Cesare usava un semplice metodo crittografico per trasmettere messaggi segreti: un messaggio veniva cifrato spostandone tutte le lettere di un certo numero di posizioni nell'alfabeto; chi fosse venuto in possesso del messaggio avrebbe potuto facilmente determinare, procedendo per tentativi, quale chiave Cesare stesse utilizzando nella cifrazione, e quindi avrebbe potuto decifrare i messaggi segreti.

All'inizio del secolo scorso si cominciò a ricorrere a dispositivi meccanici per la crittografia. I calcolatori consentirono di superare i limiti inerenti alle elaborazioni meccaniche, eseguendo algoritmi per la cifrazione/decifrazione più complessi, compiendo la cifrazione/decifrazione sulla base di certi parametri, detti chiavi.

Si distinguono due tipi di sistemi crittografici:

- **i sistemi a chiave simmetrica**, che usano la stessa chiave sia per la cifrazione sia per la decifrazione del messaggio (il metodo di Cesare); chi è in grado di compiere una delle due operazioni è necessariamente in grado di compiere anche l'altra;
- **i sistemi a chiave asimmetrica**, che usano due diverse chiavi, tra loro complementari, per effettuare con una la cifrazione e con l'altra la decifrazione; le funzioni di cifrazione e decifrazione sono indipendenti: chi conosce solo una delle due chiavi non può svolgere entrambe le funzioni con riferimento allo stesso messaggio. La crittografia asimmetrica consente di realizzare i sistemi a chiave pubblica, nei quali ciascuno dei soggetti che si scambiano informazioni ha la titolarità di una diversa coppia di chiavi.

4.7.2 Crittografia per la riservatezza

Le **tecniche crittografiche** possono essere usate per *l'invio di messaggi segreti*: ciò significa che anche se il messaggio viene intercettato esso non potrà essere letto se non se ne conosce la **chiave di decifrazione**. Alcuni anni fa le tecniche crittografiche più avanzate erano riservate agli usi militari, e ne era anzi vietata la comunicazione al pubblico, le esigenze delle comunicazioni elettroniche e la facile disponibilità di software per la crittografia hanno reso impraticabile il **divieto dell'uso della crittografia**; infatti, oggi potenti sistemi crittografici

sono accessibili a tutti, il che consente a chi lo desidera di ottenere la desiderata riservatezza, ma rende problematiche alcune indagini di polizia.

I sistemi a chiave asimmetrica offrono maggiori **garanzie di sicurezza** rispetto ai sistemi a chiave simmetrica. Nei sistemi a chiave simmetrica è necessario che entrambe le parti posseggano la stessa chiave, prima che le parti possano comunicare usando la chiave condivisa è necessario che esse si scambino tale chiave (chi è in grado di intercettare le comunicazioni tra le parti potrà ottenere la conoscenza della chiave e grazie a essa decifrare le comunicazioni successive). Nei sistemi a chiave asimmetrica, il destinatario del messaggio rende nota una delle sue chiavi e invita il mittente a usarla nell'invio dei messaggi a lui destinatario rivolti (anche se il terzo riesce a intercettare un messaggio diretto al destinatario non potrà decifrarlo: è necessaria la chiave privata del destinatario, che questi ha mantenuto segreta, non comunicandola ad alcuno).

4.7.3 Crittografia per l'autenticità e l'integrità del messaggio: la firma digitale

La **crittografia asimmetrica** può essere usata per garantire l'autenticità e l'integrità del messaggio. In un sistema a chiave pubblica, il mittente può cifrare il proprio testo usando la propria chiave privata, e inviare al destinatario il testo cifrato assieme al testo in chiaro da cui è stato tratto; il destinatario del messaggio può quindi decifrare il testo cifrato usando la chiave pubblica del mittente. Se la decifrazione del testo cifrato dà un risultato identico al testo in chiaro ricevuto, il destinatario può avere due certezze:

- il messaggio è stato inviato dal titolare della chiave privata corrispondente alla chiave pubblica usata per la decifrazione;
- quel messaggio non è stato modificato da terzi: poiché le due chiavi del mittente operano in coppia se il testo cifrato fosse stato ottenuto usando una chiave diversa dalla chiave privata del mittente, dal testo cifrato non si sarebbe potuti risalire al testo originario usando la chiave pubblica del mittente, e se il testo in chiaro fosse stato modificato da terzi esso non coinciderebbe con il risultato della decifrazione del testo cifrato.

La crittografia asimmetrica è impiegata nella **firma digitale**, la tecnologia che meglio garantisce l'autenticità e l'integrità dei documenti elettronici. La tecnologia della firma digitale usa la doppia chiave con un'integrazione: la cifrazione asimmetrica non viene applicata a tutto il testo in chiaro, ma a un'abbreviazione dello stesso, la sua impronta estratta automaticamente dal testo in chiaro. La procedura della formazione della firma digitale si svolge nel modo seguente:

- il mittente crea l'impronta del testo in chiaro utilizzando una procedura informatica (funzione di hash), che garantisce l'univocità dell'impronta (da testi diversi la funzione di hash estrae impronte diverse);
- il mittente cifra l'impronta usando la propria chiave privata, ottenendo la firma digitale del testo in chiaro;
- il mittente spedisce testo e impronta.

Ogni testo cui una persona apponga una firma digitale ha una diversa firma digitale, che risulta dalla codifica dell'impronta di quel testo con la chiave privata del mittente. La verifica dell'autenticità e dell'integrità del messaggio accompagnato da firma digitale si svolge nel modo seguente:

- Il destinatario applica al testo in chiaro ricevuto la funzione di hash estraendone una nuova l'impronta;
- egli decifra l'impronta cifrata ricevuta con il messaggio, mediante la chiave pubblica del mittente;
- infine, il destinatario confronta l'impronta estratta dal testo in chiaro con quella ottenuta attraverso la decifrazione. Se le due impronte sono identiche il messaggio è stato codificato con la chiave privata del mittente, e non è stato modificato da alcuno. Sono quindi garantite la sua autenticità e integrità.

L'obiettivo della firma digitale è fornire al destinatario la garanzia che il messaggio proviene effettivamente da chi appare esserne l'autore. Questo obiettivo può essere frustrato in due circostanze:

- un terzo può essere venuto in possesso della chiave privata del mittente, e può averla apposta senza o contro la volontà di questi;
- un terzo può aver fatto pervenire al destinatario una propria chiave, spacciandola per la chiave pubblica del mittente.

Non esistono soluzioni tecnologiche capaci di prevenire tutti i possibili abusi delle firme digitali, esistono però accorgimenti che riducono il rischio di usi non autorizzati della chiave privata. La garanzia che una firma digitale appartenga a chi appare esserne il titolare può essere fornita da un certificatore, che fornisce al titolare della firma digitale un certificato, cioè un documento elettronico che attesta l'identità del titolare, la chiave pubblica attribuitagli, e il periodo di validità del certificato stesso. Il titolare allega il certificato ai messaggi firmati (assieme alla firma digitale) e sulla base del certificato, il destinatario del messaggio può rivolgersi al certificatore per verificare l'identità del mittente. Solo **certificatori qualificati** possono rilasciare dispositivi di firma atti a produrre firme digitali, dotate di piena efficacia giuridica, assimilabile a quella della sottoscrizione chirografa (a mano), o anzi superiore a essa.

4.7.4 La disciplina giuridica della firma digitale

La disciplina della **firma digitale** è tenuta nel **CAD** all'articolo 1 (codice dell'amministrazione digitale). Si hanno diverse nozioni di firma digitale:

- **firma elettronica:** l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- **firma elettronica avanzata:** insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario

del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

- **firma elettronica qualificata**: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma. Si fa quindi riferimento al **certificato qualificato** che corrisponde al certificato elettronico conforme ai requisiti di cui alla direttiva 1999/93/CE rilasciato da certificatori;
- **firma digitale**: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Il nostro legislatore disciplina l'efficacia giuridica delle firme elettroniche:

- Il documento informatico cui sia apposta una firma elettronica non qualificata, sul piano probatorio è liberamente valutabile in giudizio tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità;
- Il documento informatico cui sia apposta una firma elettronica avanzata ha l'efficacia di scrittura privata (fa piena prova, fino a querela di falso): il titolare potrà sottrarsi all'atto cui sia stata apposta la sua firma avanza, solo provando che il dispositivo di firma è stato usato abusivamente da persona non autorizzata.

Il meccanismo della firma digitale è usato nella **posta elettronica certificata (PEC)**: si tratta di un sistema per inviare messaggi di cui siano certi l'invio e la ricezione:

- il mittente, dopo essersi autenticato, spedisce il messaggio al proprio gestore di PEC, il quale risponde con una ricevuta di accettazione;
- Il gestore appone la propria firma digitale al messaggio e invia il tutto al gestore del destinatario;
- Il gestore del destinatario, verificata l'integrità e la provenienza del messaggio, lo deposita nella casella del destinatario, inviando ricevuta di ricezione al mittente.

4.7.5 La crittografia e gli scambi: bitcoin, e smart contracts

I **bitcoin** sono una moneta elettronica che si basa sul c.d. **blockchain** (catena di blocchi), registro pubblico condiviso di cui esiste una copia in ciascun nodo della rete peer to peer che unisce gli utilizzatori di bitcoin; qui vengono registrati tutti i trasferimenti di bitcoin. Ogni utente della rete bitcoin è identificato da una chiave pubblica, e possiede la corrispondente chiave privata. Il soggetto X intende trasferire 1 bitcoin al soggetto Y. X predisporrà una transazione, cioè un messaggio avente contenuto: "X trasferisce 1 bitcoin a Y". X sottoscrive la transazione usando la propria chiave privata. Quindi diffonde la transazione a tutti i nodi della rete bitcoin. I nodi della rete possono procedere a validare la transazione. Si tratta di

verificare che la firma digitale apposta dal mittente sia corretta (corrisponda alla chiave pubblica del mittente) e controllare se il mittente abbia fondi sufficienti.

Ciascuno nodo, dopo aver validato un numero sufficiente di transazioni, le può riunire e tentare di creare un nuovo blocco della catena. Il tentativo riuscirà se il nuovo blocco sarà accettabile per la rete (avendo le caratteristiche richieste dal sistema) e sarà accettato di fatto dalla rete, anticipando altri tentativi di creare blocchi contenenti le stesse transazioni. Il mantenimento della catena dei blocchi si basa sulla funzione di hash, che genera per ogni blocco una diversa impronta. Ogni nuovo blocco contiene:

- l'impronta dell'ultimo nodo della catena (al quale il nuovo blocco si collega);
- le transazioni raccolte nel blocco;
- un numero detto nonce.

L'impronta del nuovo blocco deve avere una determinata proprietà, cioè contenere un certo numero di bit 0 iniziali. Il numero di 0 richiesti è stabilito per tutta la rete blockchain, e aumenta progressivamente. Il primo nodo che riesca a realizzare un blocco di questo tipo, potrà procedere alla diffusione del blocco sulla rete. Ciascun nodo della rete procederà a validare il blocco, verificando che esso possieda le caratteristiche richieste, e quindi l'aggiungerà alla propria catena. Il nodo che ha realizzato il blocco aggiunto alla blockchain sarà compensato con un certo numero di nuovi bitcoin.

La tecnologia della blockchain consente di effettuare transazioni sicure anche senza che vi sia un'autorità centralizzata: ogni trasferimento porta la firma digitale del mittente, quindi solo il mittente può trasmettere le somme precedentemente ricevute e solo il destinatario può trasmettere successivamente l'ammontare ricevuto dal mittente. La tecnologia della blockchain mostra come sia possibile ottenere certezza negli scambi senza ricorrere alla sanzione giuridica, garantendo la certezza delle transazioni.

I bitcoin sono stati spesso utilizzati per operazioni criminali, grazie all'anonimato da essi consentito: tutte le transazioni sono tracciate, ma sono attribuite a degli indirizzi, senza che risulti l'identità del soggetto che usa l'indirizzo.

Gli ordinamenti giuridici non hanno adottato ancora una linea unitaria rispetto al bitcoin: in alcuni casi i bitcoin sono stati vietati (Islanda e Vietnam); in altri paesi (Stati Uniti), essi sono stati assimilati a beni mobili (i pagamenti in bitcoin si configurano come baratti), e il cambiamento del valore dei bitcoin a fini fiscali come un guadagno. Nel nostro paese manca una regolazione specifica, ma i bitcoin vengono utilizzati nell'incertezza giuridica.

Negli anni più recenti si è sviluppata la **tecnologia degli smart contract** (contratti intelligenti): si tratta di un programma informatico concordato dalle parti, che da un lato esprime il contenuto di un accordo contrattuale e dall'altro, una volta attivato, attua automaticamente quel contenuto. Il contratto si attuerà quindi, senza intervento umano e procederà ad eseguire il regolamento contrattuale, senza che le parti debbano svolgere alcuna attività.

CAPITOLO 5: Internet

5.1 Internet, la rete globale

5.1.1 Le dimensioni di Internet

La parola "**Internet**" fa riferimento a diversi elementi:

- i collegamenti tra calcolatori;
- le macchine che governano il viaggio dell'informazione su tali linee di collegamento;
- le regole (protocolli e altri standard) che stabiliscono come debbano essere formati i dati destinati a viaggiare sulla rete, e come i sistemi della rete debbano interagire;
- i software di rete;
- i calcolatori connessi in rete;
- le entità virtuali esistenti nella rete;
- le persone e le organizzazioni che usano calcolatori della rete;
- le istituzioni che si occupano della gestione e dello sviluppo di Internet.

Tali aspetti hanno contribuito a dar vita alla **rete globale**.

5.1.2 Internet, rete globale e pervasiva

La rete di internet si è rapidamente estesa in dimensione **globale**; infatti, non si limita all'assorbimento passivo delle informazioni ma ogni nodo della rete può essere fruitore e fornitore di informazione. Internet è globale ed è fattore di **globalizzazione**, le distanze diventano irrilevanti nella comunicazione. La rete di Internet è **pervasiva**, riguarda ogni settore dell'attività umana (dupliciamo nel ciber spazio attività che compiamo nello spazio fisico e modifichiamo le modalità nelle quali si svolge ogni tipo di attività).

5.2 L'evoluzione di Internet

5.2.1 Le origini: la rete ARPANet

Fino agli anni '60 i calcolatori erano collegati, mediante cavi, a terminali privi di capacità autonoma di elaborazione e si poteva accedere al solo calcolatore collegato. Vennero create reti di calcolatori per far sì che il singolo utente potesse accedere a più calcolatori (non solo a quello collegato al suo terminale), e che si potessero compiere elaborazioni distribuite, che integrassero risorse di diversi calcolatori.

Nel 1962 è stato elaborato il concetto di **Rete Galattica** (Galactic Network), una rete globale di calcolatori, attraverso la quale chiunque potesse accedere a dati o programmi collocati in qualsiasi parte del mondo; tale studio viene sviluppato da **ARPANet** (la rete progenitrice di Internet). Si sentiva l'esigenza di ampliare l'accesso ai pochi calcolatori allora esistenti, e di ottimizzare l'uso delle scarse risorse informatiche, indirizzando la domanda sui calcolatori di volta in volta disponibili; inoltre la rete doveva essere in grado di mantenere la propria funzionalità anche qualora singoli collegamenti o nodi non fossero operativi. A tal fine era

necessaria una **struttura reticolare distribuita** nella quale ogni nodo fosse capace di elaborazione e fosse collegato ad altri nodi in modi molteplici, direttamente o indirettamente.

5.2.2 La commutazione a pacchetti

ARPANet adottava un nuovo modo per utilizzare le linee di comunicazione, la **tecnica della commutazione a pacchetti**. Tale tecnica consente di utilizzare una linea per più comunicazioni contemporanee; infatti, si distingue dalla **tecnica della commutazione di linea** in cui una linea telefonica rimane a disposizione della sola comunicazione tra i due telefoni collegati, per tutta la durata della chiamata

Il risultato della tecnica a pacchetti si ottiene suddividendo ogni messaggio in pacchetti (che contengono una porzione del messaggio e le indicazioni necessarie per indirizzare il pacchetto a destinazione) e quando tutti i pacchetti sono giunti a destinazione, il messaggio è ricomposto, riunendo i pacchetti nell'ordine appropriato. I pacchetti che viaggiano su Internet vengono chiamati **datagrammi** (datagram). Perché un messaggio suddiviso in pacchetti possa viaggiare dal punto di invio al punto di destinazione e poi essere ricostruito nella sua integrità, bisogna che ogni pacchetto contenga le **indicazioni necessarie** decifrabili automaticamente (l'indicazione del punto di arrivo e di partenza desiderato, la posizione del pacchetto rispetto agli altri pacchetti componenti il messaggio e informazioni di controllo). Affinché tali indicazioni possano essere decifrate automaticamente è necessario che esse siano specificate secondo regole comuni, applicate sia da parte del software mittente, sia da parte del software ricevente: tali regole debbono costituire un **protocollo condiviso**; se tutti si conformano alle regole di comunicazione condivisa viene consentita la comunicazione di macchine e sistemi eterogenei.

5.2.3 Il collegamento delle reti: i protocolli TCP-IP e la neutralità della rete

ARPANet era ancora una singola rete, lo sviluppo di Internet richiedeva che si sviluppasse un modello di "**architettura di rete aperta**", una meta-architettura che consentisse il collegamento tra reti diverse, ciascuna delle quali potesse rimanere autonoma nelle proprie scelte organizzative e tecnologiche. Nei primi anni '70 furono definiti protocolli fondamentali di Internet, chiamati **TCP-IP**, gli elementi principali di tale combinazione di protocolli sono:

- il protocollo TCP che regola lo scambio (invio e ricezione) dei pacchetti;
- il protocollo IP che riguarda l'indirizzamento dei pacchetti nella rete.

Si tratta di uno **strumento tecnico** che include l'idea di ridurre al minimo le operazioni che deve compiere una rete (le apparecchiature che governano il traffico della rete si limitano a far avanzare i pacchetti verso la loro destinazione). Tale scelta risponde a **imperativi tecnologici**: la funzione delle apparecchiature della rete viene semplificata, e la rete acquista una maggiore efficienza. I protocolli TCP-IP definiscono un'**infrastruttura computazionale** dove ogni messaggio può viaggiare da ogni nodo a ogni altro nodo, senza controlli intermedi. Ogni messaggio è suddiviso in pacchetti di bit, racchiusi in una busta digitale che riporta tutte

le informazioni necessarie per trasmettere il pacchetto alla sua destinazione; i pacchetti viaggiano spostandosi di nodo in nodo, seguendo cammini non prestabiliti (il percorso di un pacchetto è determinato dalle condizioni del traffico sulla rete, essendo i pacchetti diretti secondo algoritmi che ottimizzano l'utilizzazione della rete, evitandone la congestione). La trasmissione di un pacchetto da un nodo al successivo è compiuta da calcolatori che si limitano a ricevere il pacchetto inviato dal nodo precedente, e a inviarlo in avanti; quando i pacchetti giungono al calcolatore di destinazione, le buste digitali sono aperte, e i pacchetti sono riuniti e controllati.

L'adiaforia (indifferenza) rispetto ai contenuti veicolati costituisce la **neutralità della rete**, che rappresenta una garanzia di innovazione decentrata, comportando l'assenza di discriminazioni rispetto al contenuto del messaggio veicolato e rispetto alla natura del mittente. Tale neutralità verrebbe meno qualora la rete fosse predisposta in modo da dare precedenza ai messaggi forniti da certe categorie di mittenti o rifiutasse di trasmettere i messaggi che contengono certi contenuti. La neutralità della rete non esclude che la trasmissione di certi contenuti sia vietata dal diritto, né che certi messaggi siano eliminati al punto di arrivo; essa esclude che l'attuazione dei divieti giuridici o delle preferenze di utenti possa essere affidata alla rete stessa.

Recentemente è stata affermata la necessità di superare la neutralità della rete: offrendo a pagamento condizioni preferenziali ai pacchetti che presentano certe caratteristiche si otterrebbero risorse che potrebbero essere utilizzate per potenziare le infrastrutture di Internet. Si otterrebbe un "miglioramento di Pareto", si passerebbe dalla situazione nella quale tutti si debbono accontentare di un servizio modesto, a una nuova situazione nella quale alcuni potrebbero ottenere un servizio migliore, senza che peggiori il servizio offerto agli altri.

Alcuni però sono contrarie all'abbandono della neutralità della rete: si teme che tale abbandono comporterebbe gravi pericoli per lo sviluppo di Internet e per l'economia della rete (potrebbe comportare un peggioramento del servizio per chi non può pagare il prezzo richiesto per prestazioni superiori a pagamento) e metterebbe a rischio la libertà di espressione e la democrazia su Internet (potendo trattare in modo diverso le comunicazioni online a seconda dell'emittente e del contenuto del messaggio, i fornitori di connettività avrebbero la possibilità di controllare l'uso di Internet da parte dei cittadini, di scegliere quali comunicazioni favorire e quali ostacolare).

5.2.4 La nascita della rete delle reti

TCP-IP si propone di governare la comunicazione all'interno di una rete e la comunicazione tra reti eterogenee: i messaggi che viaggiano all'interno di una rete, una volta uniformati al protocollo TCP-IP possono essere trasmessi ad altre reti; con tali protocolli emerge la possibilità di formare una **rete di reti**, che aspira ad accogliere altre reti al suo interno (una volta adottato il protocollo TCP-IP, ARPANet poté essere sostituita da reti distinte).

Una tappa importante nello sviluppo di Internet fu la creazione di una **connessione ad altissima velocità**, afferente a NSFNET, cui poterono collegarsi le reti esistenti: Internet venne ad assumere progressivamente l'attuale **configurazione a più livelli**, nella quale reti locali sono connesse a reti di ampia dimensione, le quali sono connesse alle grandi infrastrutture, dette dorsali (backbone), per i collegamenti intercontinentali. I calcolatori collegati a Internet continuano a far parte di reti locali, impiegate per collegare calcolatori collocati in aree di ridotta dimensione, e per consentire a più calcolatori di condividere i dispositivi di input e output. In una rete locale, alcuni calcolatori, i server, si assumono il compito di offrire certe prestazioni agli altri calcolatori della rete, i client. Le reti locali diventano delle piccole Internet, chiamate **Intranet**, il cui uso è riservato agli utenti della rete locale.

5.2.5 Gli strati di Internet e la pila (stack) dei protocolli

I protocolli TCP-IP assicurano la funzione dell'indirizzamento in rete e del trasporto dei messaggi. I messaggi che viaggiano attraverso Internet sono destinati a svolgere funzioni determinate, dovranno contenere le informazioni necessarie per la particolare applicazione cui afferiscono, e i calcolatori devono trattarli nel modo richiesto da tale applicazione; inoltre, i messaggi, al fine di raggiungere Internet o pervenire ai calcolatori cui sono destinati, debbono compiere un tratto sulle linee telefoniche o su una rete locale.

Si possono distinguere **cinque strati nell'architettura di Internet**: lo strato dell'applicazione, lo strato del trasporto, lo strato della rete, lo strato del collegamento dati, lo strato fisico. In conformità ai diversi protocolli che caratterizzano ciascuno strato, specifiche informazioni sono aggiunte ai pacchetti, che possono essere paragonati a una lettera imbustata più volte. Secondo questo modello strutturale, chiamato **incapsulamento**, ogni busta racchiude, come una capsula, la busta dello strato superiore (più intenso), e può essere trattata, in conformità al proprio protocollo, prescindendo dal proprio contenuto. La busta più esterna contiene le indicazioni necessarie affinché il pacchetto giunga da Internet al nostro calcolatore. Tolta la busta del collegamento, troviamo la busta con le indicazioni per l'indirizzamento in rete (IP); tolta anche questa busta, troviamo le informazioni attinenti all'invio del messaggio e al modo in cui deve essere ricevuto (TCP) e agli altri pacchetti afferenti allo stesso messaggio; successivamente troviamo le indicazioni concernenti l'applicazione cui il messaggio è destinato; tolta quest'ultima busta, troviamo il messaggio originario. L'incapsulamento fa sì che gli strati inferiori siano indipendenti dalle funzionalità realizzate ai livelli superiori; il livello inferiore si limita a incapsulare il messaggio da presentare al livello superiore, è neutrale rispetto al contenuto di quel messaggio, non privilegia o discrimina particolari funzionalità, contenuti, o mittenti.

5.2.6 Le culture di Internet

Internet è il luogo in cui coesistono e comunicano diverse culture:

- la cultura tecnico-meritocratica: caratterizzata dai valori della scoperta tecnologica, della competenza e della condivisione della conoscenza;

- la cultura hacker: che unisce ai valori tecnico-meritocratici gli aspetti della creatività e della cooperazione;
- la cultura virtual-comunitaria: caratterizzata dai valori della libertà di comunicazione, associazione e auto-organizzazione;
- la cultura imprenditoriale: basata sui valori del denaro, del lavoro e del consumo.

Queste diverse anime sono potute coesistere e hanno potuto comunicare grazie alla condivisione dei protocolli e delle regole per la comunicazione e per applicazioni condivise. Quando Internet era usata da un numero limitato di persone, spesso implicate nella sua costruzione, le componenti tecno-meritocratiche e hacker erano le principali ispiratrici della rete; in tale ambito che nasce l'**etica hacker** (cioè la prospettiva che enfatizza e premia la creatività tecnologica e la condivisione delle conoscenze) che si intreccia con il modello dello sviluppo del software a sorgente aperta (open source), modello nel quale tutti i membri di un progetto software hanno la possibilità di accedere ai programmi sorgente, di proporre e realizzare modifiche ed estensioni degli stessi, e di distribuire i programmi originali, così come le loro modifiche ed estensioni. Il termine hacker è spesso usato per denotare chi si introduce in sistemi informatici altrui contro la volontà del titolare del sistema, al fine di accedere a informazioni riservate o di compromettere il funzionamento del sistema. La cultura hacker identifica l'hacker in chi si rapporta in modo libertario, creativo e inventivo all'informatica; riservano il termine cracker a chi invece danneggia il funzionamento dei sistemi, o opera nel mondo dell'informatica in modo distruttivo o asociale.

Negli anni successivi, accanto alle comunità incentrate sulla creatività tecnologica crebbero altre comunità virtuali; persone che condividevano certi interessi potevano coltivarli insieme, seppure di regola con flessibilità e con un investimento limitato: si parla di "**individualismo collegato in rete**". L'idea della condivisione e un certo spirito comunitario si sono ripresentati in forme nuove quando si è parlato di **reti di reti**, sono nate nuove forme di collaborazione distribuita che hanno esteso a nuovi ambiti il modello del software open source.

Internet ha rivoluzionato molte attività produttive e commerciali, consentendone l'articolazione su scala globale, e modificandone profondamente lo svolgimento; ma anche le attività economiche hanno modificato profondamente Internet, che si è arricchita di spazi dedicati ad attività commerciali. L'ingresso del commercio nella rete, accanto a problemi, ha effetti positivi, contribuendo alla crescita economica generale e offrendo nuove opportunità sia agli operatori economici sia ai consumatori.

La rete di internet superficie è accompagnata da una più vasta **rete profonda**, che ospita servizi di diverso tipo ad accesso limitato; all'interno della rete profonda possiamo distinguere una **rete oscura**, che include reti e servizi alle quali si può accedere solo con software specifici, intesi a proteggere la segretezza dell'identità dei partecipanti e delle loro operazioni.

5.3 Gli standard e il governo della rete

I protocolli TCP-IP rappresentano il primo livello di standard condivisi per la comunicazione informatica.

5.3.1 La rete e gli standard

Uno **standard di Internet** è una specificazione che è stabile e tecnicamente competente. Il processo della formazione di uno standard consiste di:

- una **fase preparatoria**: sviluppata in diversi stadi, alla comunità di Internet e al giudizio di organi tecnici compete valutare se lo standard abbia raggiunto la maturità necessaria per passare allo stadio successivo);
- **adozione da parte dell'ente competente**, e quindi dalla pubblicazione (i documenti che riportano le versioni dello standard sono pubblici). Con la sua pubblicazione, lo standard è proposto agli sviluppatori di software per Internet, che potranno adottare volontariamente lo standard per la creazione di nuovi software.

La "**vincolatività**" degli standard risulta dalla circostanza che ciascuno ha bisogno di adottare comportamenti coerenti con i comportamenti e le aspettative altrui (se il mio software non corrisponde allo standard sarò io stesso a soffrire, essendo incapace di comunicare in rete; viceversa la mia adozione dello standard sarà tanto più fruttuosa quante più persone utilizzano quello stesso standard); la diffusione dello standard si basa sull'**effetto di rete**. La scelta individuale di seguire un certo standard è giustificata dal vantaggio che il singolo utente trae dal fatto che lo standard sia universalmente adottato: il potere è nelle mani di coloro che, mediante la propria scelta di promuovere uno standard sono capaci di renderlo "saliente" per tutti; l'interesse personale è sufficiente a condurre gli individui a convergere su standard salienti. Questo meccanismo rende possibile la contraddizione tra:

- razionalità collettiva: richiede che tutti gli utilizzatori adottassero congiuntamente lo standard ottimale;
- razionalità individuale: esige che ciascuno segua qualsiasi standard egli preveda sarà adottato dagli altri, a prescindere dal suo valore comparativo.

La corrispondenza tra le razionalità è stata assicurata dai modi nei quali la comunità di Internet è giunta a formulare i propri standard, e in particolare i protocolli. L'adozione di uno standard deriva dalla sua approvazione da parte di comitati di esperti imparziali sulla base della validità tecnica dello standard stesso. La decisione del comitato competente rende lo standard adottato saliente per tutta la comunità di Internet (ogni sviluppatore è indotto ad adottarlo).

La comunità di Internet si sta interrogando su come assicurare, anche in futuro, la qualità e l'imparzialità delle scelte riguardanti Internet, garantendone l'eccellenza tecnologica e proteggendole dalla pressione degli interessi sia economici sia politici: c'è chi ritiene che Internet non possa sfuggire a un controllo politico e chi ritiene che solo mantenendosi

separata rispetto alle istituzioni politiche possa conservare la propria eccellenza tecnologica e la propria imparzialità.

5.3.2 Internet tra norme sociali e norme giuridiche

Agli standard sono affiancate **credenze normative** combinate a **sanzioni informali**, un giudizio negativo della comunità interessata che può condurre nei casi più seri alla stigmatizzazione o anche all'espulsione (ostracizzazione) di chi violi la norma. La combinazione di protocolli convenzionali e di regole sociali è stata sufficiente per governare Internet ai suoi inizi; negli ultimi anni, in seguito alla crescita dell'importanza sociale ed economica di Internet la normatività spontanea è stata affiancata da norme giuridiche. Vi sono opinioni discordi in merito alla necessità della disciplina giuridica:

- **posizioni libertarie o "separatiste"**: Internet crea uno spazio nuovo virtuale e globale, separato rispetto allo spazio oggetto del potere dei governi, fisico e nazionale; quindi alle attività compiute all'interno di Internet non si applicherebbero le discipline giuridiche, questo perchè il cibernazio è dotato di un "codice non scritto" e pertanto non ha bisogno della politica e del diritto: è capace di *autoregolarsi*, di risolvere da solo i propri conflitti, con i propri mezzi;
- alle tesi riportate al punto precedente si oppongono le **richieste di una disciplina giuridica della rete**: *governi*, interessati a controllare la rete a fini di polizia, a censurare alcuni tipi di informazioni, a controllare il dissenso politico e sociale e *comunità degli affari* che hanno richiesto (e ottenuto) facilitazioni per il commercio elettronico, la protezione di marchi e segni distintivi, un'energica tutela della proprietà intellettuale; è stata anche richiesta la garanzia che Internet rimanga un ambiente nel quale esercitare in sicurezza diritti civili, sociali e culturali;
- chi ritiene che gli interventi pubblici e la regolazione autoritativa della rete possano essere controproducenti: per tutelare le libertà dei singoli e favorire lo sviluppo di Internet sarebbe sufficiente il funzionamento libero e pluralistico del mercato, che da solo indirizzerebbe gli operatori e i progettisti verso le soluzioni e le architetture che meglio rispondono agli interessi degli utenti;
- chi ritiene fisiologico un intervento dello Stato nel governo della rete a tutela degli interessi collettivi: l'idea che Internet sia esente dal diritto statale si porrebbe in contrasto con i principi della democrazia e dello stato di diritto;
- chi ritiene che la rispondenza del funzionamento della rete alle esigenze e ai diritti dei suoi utilizzatori possa ottenersi perfezionandone l'autogoverno e rendendolo sensibile ai valori giuridici.

5.3.3 Dagli indirizzi numerici ai nomi di dominio

Secondo i protocolli TCP-IP, ogni calcolatore della rete è identificato da un numero della lunghezza di 4 byte (32 bit), l'**indirizzo IP**; tale numero è espresso in una forma più leggibile e memorizzabile convertendo ogni byte in un numero decimale (le prime cifre del numero identificano la rete cui il calcolatore afferisce mentre le ultime cifre identificano un particolare calcolatore all'interno di quella rete). Un calcolatore può avere un proprio

indirizzo IP permanente o può ricevere, ogni volta che si collega in rete, un diverso **indirizzo IP temporaneo**, che torna disponibile dopo il collegamento e potrà essere assegnato a un nuovo utente. Ogni comunicazione inviata in rete da un particolare calcolatore è etichettata con l'indirizzo del calcolatore mittente: ciò può consentire in molti casi l'individuazione della persona che ha compiuto quella particolare operazione.

Dall'inizio degli anni '80 si ravvisò l'esigenza di usare un diverso sistema di riferimento, che usasse identificatori più facilmente memorizzabili e tali da richiamare la funzione svolta mediante un certo sito o l'identità del suo titolare, nacquero i **nomi di dominio**; un nome di dominio si costruisce combinando più parole separate da punti, nell'analisi del nome si parte dalla fine: l'ultima parola è un suffisso (indica la nazionalità dell'ente cui il nome appartiene, o il tipo di attività svolto dall'ente stesso), preceduto da una parola che solitamente indica l'ente cui fa capo il dominio, che può essere ancora preceduta da ulteriori specificazioni, qualora il dominio afferisca a una ripartizione all'interno di quell'ente.

Un nome di dominio identifica un dominio, cioè un gruppo di indirizzi IP; per identificare un particolare calcolatore appartenente a quel dominio, bisogna anteporre al nome di dominio un'ulteriore specificazione, cioè il nome dell'host che desideriamo contattare. Aggiungendo al nome di dominio il particolare nome di host (che contraddistingue il calcolatore cui vogliamo far riferimento) otteniamo un **nome di dominio completamente qualificato** (nome dominio + nome host) che identifica in modo univoco quel particolare calcolatore.

Esiste un'infrastruttura, chiamata **sistema dei nomi di dominio** che si occupa di tradurre i nomi di dominio completamente qualificati in indirizzi IP. Tale infrastruttura consta di una rete di calcolatori, i server del DSN, i quali fungono da "elenco telefonico di Internet": quando il nostro browser deve accedere a un calcolatore di cui abbiamo indicato il nome di dominio, esso invia il nome di dominio a un server del DSN, che risponde inviando il corrispondente indirizzo IP.

L'innovazione consistente nell'affiancare i nomi di dominio agli indirizzi IP numerici ha un grande impatto giuridico e sociale: i nomi di dominio sono diventati ben presto oggetto di controversie che hanno evidenziato attitudini ben diverse rispetto allo spirito cooperativo delle origini di Internet (la prepotenza di chi, utilizzando un nome quale segno distintivo ne pretendeva l'uso esclusivo anche nel mondo virtuale).

5.3.4 i protocolli delle applicazioni di Internet

Oltre TCP e IP, esistono ulteriori protocolli di Internet; ricordandone alcuni:

- **Il protocollo TELNET:** consente di interagire con un calcolatore remoto nello stesso modo in cui si opererebbe da un terminale dotato di video e tastiera, collegato al calcolatore remoto mediante cavo;
- **Il protocollo FTP:** consente di scambiare e manipolare file. Chi utilizza questo protocollo accede al sistema di file del calcolatore remoto, e può prelevare o depositare file, cancellarli, creare nuove cartelle, ecc.

- **Il protocollo SMTP**: riguarda la posta elettronica. Esso viene di solito utilizzato in combinazione con i **protocolli POP o IMAP**, che integrano SMTP per quanto attiene alla ricezione della posta. Accanto alle funzioni di base della trasmissione e ricezione di messaggi si sono sviluppate alcune importanti funzionalità aggiuntive, come le conferenze virtuali cui possono partecipare tutti gli utenti della rete interessati a determinate problematiche. Esistono due tecniche per la partecipazione a tali conferenze: (1) l'utente, il cui nome è registrato tra i membri del gruppo di interesse, riceve direttamente sulla sua casella postale gli interventi; (2) l'utente contatta archivi elettronici, le news, che raccolgono gli interventi rendendoli disponibili ai partecipanti.

5.3.5 identificazione, e profilazione in rete

Spesso assumiamo che le attività svolte in rete siano **anonime**: la rete non vede il nostro volto (se non ci facciamo riprendere mediante una telecamera) e possiamo accedere alla maggior parte dei siti senza dichiarare la nostra identità: solo in casi particolari ci si richiede di utilizzare una firma digitale o password ottenute al di fuori della rete, come le credenziali per accedere al conto corrente bancario. Il completo anonimato è **un'illusione**: gli utenti della rete sono frequentemente identificati e soggetti a **profilazione** (le persone fisiche possono essere associate a identificativi online che possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle).

Tutte le operazioni compiute in rete sono associate all'IP associato al calcolatore o al cellulare che l'utente utilizza; l'oscuramento di questo richiede l'uso di tecniche di **anonimizzazione**: vi sono sistemi che consentono all'utente di dotarsi di un secondo indirizzo IP temporaneo, diverso da quello che identifica il suo computer, che viene fornito da server dedicati all'anonimizzazione.

Un'identificazione più precisa rispetto a quella risultante dall'IP può essere fornita dai **cookies** e dall'autoidentificazione dell'utente, chiamato a fornire dati personali o a ricollegarsi al sistema usando il nome-utente utilizzato in precedenza; il nome-utente consente di riunire gli accessi effettuati con quel nome, assumendo che siano effettuati da una stessa persona.

La "**profilazione**" consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, consentendo di estrarre nuove correlazioni dalla base di dati disponibili sulla base delle quali estendere la profilazione degli utenti.

5.3.6 I log-file

Quando operiamo su Internet, tutti gli accessi da noi compiuti presso un certo server sono registrati nel **log-file del server** (file che viene aggiornato dinamicamente e che riporta la sequenza delle operazioni compiute su quel server); tale file registra l'indirizzo IP associato al calcolatore che ha effettuato l'accesso, il tempo dell'accesso, la pagina Web visitata, e il

browser utilizzato. Il log-file non consente di collegare la descrizione dell'attività al suo autore ma si limita ad associare quell'attività a un indirizzo IP; infatti non viene considerato dato personale.

5.3.7 I cookie

Le informazioni registrate nel log-file di un sito sono insufficienti a identificare un determinato calcolatore: il meccanismo dell'allocazione dinamica fa sì che uno stesso IP possa essere assegnato a diversi calcolatori in momenti successivi, e che uno stesso calcolatore possa ricevere diversi IP. Ciò impedisce di ricostruire la storia dell'interazione di un determinato utente con il sito, i diversi accessi di una stessa persona essendo normalmente effettuati con diversi IP. La soluzione adottata per raggiungere tali risultati consiste nell'utilizzo dei cosiddetti **cookie**: un insieme di dati inviati dal sito, e memorizzati dal browser in un file che risiede sul calcolatore dell'utente.

Quando un calcolatore si collega per la prima volta a un certo sito, il sito gli invia un cookie, caratterizzato da un proprio identificatore univoco, nell'ambito della directory indicata e del dominio cui afferisce il sito. Ogni qualvolta il calcolatore si ricollega a quel sito, il cookie precedentemente inviato viene rispedito al sito. Il sito quindi sa che il nuovo accesso è stato compiuto proprio dal calcolatore al quale aveva precedentemente inviato il cookie.

I cookie sono semplici dati, non sono virus e non danneggiano il calcolatore; comportano però rischi per la privacy. Infatti, il cookie consente al sito che l'abbia inviato di unire le informazioni concernenti gli accessi al sito stesso compiuti con un certo calcolatore. Se più siti si scambiano i risultati ottenuti con i propri cookies, tutte le informazioni ottenute da quei siti, concernenti lo stesso computer, possono essere unificate. Il sito saprà quindi che un certo computer è stato impiegato per compiere un certo insieme di attività (il sito potrà ipotizzare che l'utente abbia certe caratteristiche e inviare pubblicità mirata o offerte personalizzate, che l'utente potrà gradire o reagire negativamente).

Il Garante distingue, nel provvedimento del 2014, diversi tipi di cookie:

- **i cookie tecnici**: utilizzati al solo fine di effettuare la trasmissione di una comunicazione, o nella misura strettamente necessaria per erogare un servizio esplicitamente richiesto;
- **i cookie di profilazione**: usati per costruire profili degli utenti;
- **i cookie prima parte**: inviati dal gestore del sito cui si accede e provengono dal server cui afferisce la pagina del sito visitato;
- **i cookie terze parti**: inviati da altri soggetti, provengono da altri server, cui il server del sito visitato accede per completare alcuni elementi della pagina stessa o per svolgere particolari operazioni.

Nello stesso provvedimento vengono specificate le condizioni per l'uso legittimo dei cookie:

- per i cookie tecnici si richiede la sola informativa;

- per i cookie di profilazione si richiedono l'informativa, il consenso dell'interessato e la notifica al garante.

Gli obblighi competono al gestore del sito, per i cookie prima parte, e ai terzi da cui proviene il cookie per i cookie terze parti. All'utente viene data la possibilità di scegliere come rapportarsi al cookie: se respingere tutti i cookie o solo quelli di terza parte, e cancellare tutti i cookie che abbiamo già ricevuto o solo alcuni di essi.

5.3.8 La ragnatela globale (World-Wide Web - WWW)

Con la creazione del **World-Wide Web** (WWW - ragnatela globale), un nuovo modello di sistema informatico, si ebbe il cambiamento dell'uso di internet, che diventò una rete globale (aperta a tutti). L'architettura del Web fu definita dal CERN (Centro Europeo per la Ricerca Nucleare) e si tratta di un enorme **insieme di documenti** (non di un software), unificati dagli standard usati per la loro identificazione, creazione e consultazione. I tre standard che hanno consentito l'avvio del Web sono:

- **URL**: un tipo di identificatore per gli oggetti del Web, che designa in modo univoco tali oggetti, specificando come possono essere automaticamente individuati e richiamati (indicano la localizzazione della risorsa da essi identificata e il protocollo da usare per richiamarla). Sono un sottoinsieme degli **URI** (gli identificatori univoci che designano gli oggetti presenti in rete);
- **HTML**: il linguaggio per predisporre documenti ipertestuali;
- **HTTP**: il protocollo che disciplina l'interazione tra il calcolatore client, che richiede pagine Web, e il calcolatore server, che le fornisce.

Grazie al supporto di questi standard sono stati costruiti gli strumenti software per la consultazione e lo sviluppo del Web:

- i software per la navigazione in rete (i browser): consentono di spostarsi dall'una all'altra pagina Web, visitando l'ipertesto globale (una pagina Web può contenere link ad altre pagine Web; tale Link è indicato con una o più parole sottolineate).
- i software per la realizzazione di siti Web. Il Web si ispira al **modello dell'ipertesto** (hypertext); si tratta di un sistema informatico che consente all'utente di visualizzare documenti e di spostarsi automaticamente dal documento visualizzato ad altri documenti a esso collegati, seguendo collegamenti (hyperlink) di diverso tipo.

5.3.9 Il governo (governance) di Internet

Con lo svilupparsi di internet mutano anche le strutture organizzative destinate a coordinare le operazioni, ad assicurare la governance (per sottolineare la differenza tra il coordinamento di Internet e il governo). Da tale trasformazione è emerso un modello che è riuscito a dare risposte alle esigenze della rete.

All'inizio, ARPANet, la progenitrice di Internet, faceva capo all'ARPA (un'unità afferente al Dipartimento della Difesa statunitense); in seguito (anni '80), il coordinamento dello sviluppo

di Internet passò alla NSF (Fondazione nazionale della scienza) e venne offerto il primo collegamento ad alta velocità (**dorsale**) cui altre reti poterono connettersi. Dal 1991, NSFNet fu aperta agli operatori commerciali, che svilupparono proprie reti giungendo a detenere la maggior parte delle infrastrutture di rete. Oggi non esiste un proprietario unico o principale di Internet, ma la proprietà è ripartita tra numerosi enti, pubblici e privati; il governo di Internet è stato affidato a diversi organismi (nati per rispondere a diverse esigenze) autonomi che perseguono interessi collettivi attinenti al funzionamento e allo sviluppo della rete (hanno mantenuto le loro funzioni anche quando si è avuta la globalizzazione della rete). Le strutture per il governo di Internet possono suddividersi in:

- istituzioni finalizzate allo sviluppo tecnologico, alla definizione e al perfezionamento degli standard;
- istituzioni finalizzate alla gestione, all'assegnazione di indirizzi e nomi.

5.3.10 Le istituzioni di Internet: sviluppo tecnologico e standard

Lo sviluppo delle tecnologie di Internet fa capo a **ISOC** (Società di Internet), un'organizzazione senza fini di lucro, fondata per essere guida negli standard, nell'educazione, nelle politiche relative a Internet. La partecipazione a tale società è aperta a tutte le persone interessate a contribuire allo sviluppo di Internet, ma le scelte sono affidate a organi collegiali prevalentemente tecnocratici. A ISOC afferisce **IETF** è un'organizzazione virtuale (che non ha personalità giuridica e sede fisica), comprendente numerosi gruppi di lavoro che si occupano dei diversi standard di Internet; chiunque può associarsi a tali gruppi, iscrivendosi alla relativa lista di posta elettronica, infatti l'iscrizione avviene mediante Internet. L'attività dei gruppi di lavoro è sovrintesa da **IESG** (Gruppo per la direzione dell'ingegneria di Internet) che valuta i progressi nella maturazione degli standard e la validità dei risultati raggiunti; alla definizione degli standard partecipa anche **IAB** (Comitato per l'Architettura di Internet) per ciò che attiene le questioni di carattere più generale. Negli ultimi anni si è aggiunto **W3C** (Consorzio per la ragnatela globale, con struttura associativa e personalità giuridica), che si occupa dello sviluppo di standard per il Word-Wide-Web, finalizzati alla strutturazione, gestione, presentazione delle informazioni disponibili in rete; mira a realizzare un unico Web esteso al mondo intero.

5.3.11 Le istituzioni di Internet: l'assegnazione di nomi e indirizzi

ICANN (Società di Internet per l'assegnazione di nomi e numeri) si occupa del coordinamento delle funzioni riguardanti l'assegnazione di identificatori univoci sia di indirizzi numerici che di nomi di dominio. ICANN svolge attività decentrate; infatti in ogni continente si trova una struttura, il **Registro Regionale di Internet**, competente per l'assegnazione di indirizzi numerici; a tali registri sono affidati grandi quantità di indirizzi, che verranno, dal registro stesso, allocati in blocchi a ciascun fornitore di servizi di Internet, il quale si occuperà di assegnare gli indirizzi ai propri utenti.

L'assegnazione dei nomi generici di dominio (gov., com., org.) è stata delegata alla Network Solutions Inc. (**NSI**), mentre i nomi con suffisso di nazione (it, eu, uk) sono assegnati da enti

situati nelle diverse nazioni interessate: **naming authority**, competenti a definire le regole, e **registration authority**, competenti ad applicarle assegnando i nomi.

ICANN ha definito i criteri uniformi per la risoluzione delle controversie relative all'assegnazione dei nomi di dominio. Per ottenere un nome di dominio generico (privo del suffisso della nazione), bisogna accettare la clausola arbitrale che affida la soluzione di eventuali dispute a un collegio arbitrale che giudicherà applicando la Policy; la procedura dovrà svolgersi presso uno dei fornitori di servizi per la risoluzione amministrativa delle dispute indicati da ICANN, che successivamente applicherà le decisioni. La formazione e l'applicazione delle regole in materia nomi di dominio si manifesta è autonomia della regolazione di Internet rispetto al diritto statale. Anche per i nomi assegnati dalla Registration Authority italiana è possibile attivare una procedura arbitrale, ma la soggezione all'arbitrato è in Italia facoltativa, richiede quindi il consenso di entrambe le parti.

5.3.12 Diritti e governo della rete

L'ONU ha avviato due iniziative sul governo di Internet:

- **Il Word Summit on the Information Society**: il documento finale (2005) enuncia l'impegno a promuovere una società dell'informazione centrata sulle persone, inclusiva e orientata allo sviluppo. Nonostante tale documento non si trovò un accordo sulla struttura giuridica e la localizzazione di ICANN e la scelta fu rinviata al futuro. Il dibattito al riguardo è ancora in corso, anche se gli Stati Uniti hanno dato disponibilità a rinunciare ad ogni posizione giuridica privilegiata rispetto al governo di Internet, e a consentire il trasferimento della sede principale di ICANN in altro paese;
- **L'Internet Governance Forum (IGF)**: creato nel 2006, si tratta di un forum per il dialogo tra molteplici portatori di interessi sulle politiche concernenti il governo di Internet. Durante la conferenza annuale si discute sulla gestione degli indirizzi di Internet e sul superamento della divisione digitale, l'accesso all'informazione, la proprietà intellettuale, la libertà di espressione, la tutela della privacy, la promozione dell'economia di Internet. I diritti umani sono diventati un riferimento nel dibattito del Forum ed è stata sviluppata la **Carta dei diritti e dei principi di Internet**, la quale si propone di "tradurre" i contenuti enunciati nella Dichiarazione Universale dei Diritti dell'Uomo del 1948 in principi per il governo della rete.

5.4 Il Web semantico

Il termine "**Web semantico**" fa riferimento all'inserimento nel Web di informazioni comprensibili al calcolatore, che quindi possono essere elaborate automaticamente attraverso tecnologie informatiche avanzate.

5.4.1 Gli standard del Web semantico

Dello sviluppo del Web semantico se ne occupa W3C, promuovendo la definizione e all'applicazione di standard volti a consentire lo sviluppo di tecnologie per il Web semantico, ai diversi livelli della piramide a gradini.

Lo strato più basso della piramide è costituito da due standard:

- lo **standard Unicode**: che indica come rappresentare, mediante un unico numero binario, ogni carattere di qualsiasi alfabeto oggi in uso;
- lo **standard degli URI**: che indica come denominare in modo non-ambiguo tutte le entità accessibili sul Web.

Gli standard del Web semantico attengono agli strati superiori:

- **XML**: un metalinguaggio che consente di definire etichette per esprimere la struttura dei propri documenti e per includere ulteriori informazioni in tali documenti;
- **RDF**: un linguaggio che consente di includere nei documenti enunciati sugli oggetti rilevanti e le loro proprietà;
- le **ontologie**: consentono di specificare concetti e relazioni concettuali e di compiere le inferenze corrispondenti;
- la **logica** (le regole): permette di esprimere informazioni complesse, utilizzabili nei ragionamenti (inferenze o prove);
- lo strato della **fiducia**: comprende modi per assicurare la riservatezza, l'autenticità, l'integrità e l'affidabilità.

Il Web semantico facilita l'accesso all'informazione e l'effettuazione di varie attività mediante Internet: i documenti potranno essere automaticamente adattati ai bisogni dei loro utilizzatori e potranno includere le informazioni richieste per varie attività che li riguardano, in particolare quelle attinenti al commercio elettronico o al governo elettronico.

5.4.2 Il diritto nel Web semantico

Il Web è diventato la principale fonte di **cognizione del diritto**; tuttavia i documenti giuridici sono disponibili in formati diversi, non sempre leggibili (o non leggibili perfettamente) con il software presente sul nostro elaboratore. Le informazioni, per comprenderle e favorire lo svolgimento delle attività giuridiche, dovrebbero essere arricchite di dati elaborabili mediante strumenti informatici; tali esigenze sono realizzate attraverso il trasferimento delle tecnologie in ambito giuridico, dando luogo alla piramide che comprende:

- standard condivisi per l'identificazione delle risorse giuridiche;
- standard per la strutturazione dei documenti giuridici;
- standard per associare ai documenti giuridici asserzioni di vario genere;
- ontologie giuridiche;
- linguaggi per la rappresentazione delle norme giuridiche in forma logica;
- metodi per assicurare l'affidabilità dell'informazione giuridica e la sua conservazione.

5.5 Il Web 2.0 o Web riscrivibile

La locuzione "**Web 2.0**" fa riferimento al coinvolgimento degli utenti del Web nella creazione del Web stesso e alle infrastrutture informatiche che consentono tale partecipazione; tutti possono partecipare alla dinamica evolutiva. Nell'era del **Web riscrivibile**, Internet è più l'infrastruttura mediante la quale si può accedere alla conoscenza, comunicare, svolgere attività economiche e amministrative, ma è anche il luogo nel quale le persone possono esprimersi, costruire le proprie immagini pubbliche, interagire con amici e conoscenti, impegnarsi nella produzione di conoscenza, partecipare alla cultura e contribuire al dibattito sociale e politico. Infrastrutture e strumenti software rendono possibili le diverse dimensioni del nuovo Web: il nuovo Web riguarda comunità, partecipazione, e collaborazione paritetica, Internet sta evolvendo in un calcolatore globale, vivente, interconnesso che ciascuno può programmare.

5.5.1 I contenuti generati dagli utenti

Nel Web 2.0 gli utenti della rete hanno cominciato a riscrivere la rete stessa, arricchendola con i propri contenuti e le proprie interazioni. Fin dai suoi inizi Internet ha consentito la condivisione di file e la creazione di gruppi di discussione; tuttavia, la predisposizione di pagine Web e la creazione di contenuti digitali e il loro trasferimento on-line presupponevano competenze che la maggior parte degli utenti del Web non possedeva. Il Web 2.0 trova la propria premessa in nuovi strumenti informatici che consentono a tutti gli utenti del Web di contribuire alla rete. Sono disponibili:

- migliori strumenti-accessibili a prezzi ridotti o gratuitamente;
- strumenti per trasferire in rete i contenuti prodotti;
- strumenti per produrre direttamente in rete nuovi contenuti.

La disponibilità di tali strumenti ha favorito la crescita della quantità dei contributi generati dagli utenti. Le iniziative diffuse degli utenti del Web si combinano con l'emergere di funzioni tese a filtrare e organizzare l'informazione prodotta, aggregando le scelte dei singoli in risultati rilevanti per altri.

5.5.2 L'impresa informatica nel Web 2.0: il modello Google

L'innovazione del Web 2.0 consiste nello sfruttare l'**intelligenza collettiva** (gestire, comprendere, e rispondere a quantità di dati prodotti dagli utenti); cambia la natura economica dell'impresa e nuovi tipi di impresa e modelli giuridici acquistano importanza. Imprese tipiche:

- anni '60 e '70: **IBM**, il grande produttore di hardware che vende o noleggia ai propri clienti macchine per il calcolo e i relativi dispositivi periferici;
- anni '80 e '90: **Microsoft**, produttore di programmi informatici;
- Web 2.0: **Google** offre servizi Google; non ha bisogno di adottare misure tecniche o giuridiche atte a prevenire duplicazioni indesiderate poichè il software risiede nei server di Google, dove risiedono anche i dati di cui quel software si avvale. Google

usa il Web per creare i propri indici e compiere le proprie ricerche ma ne estrae anche ulteriori informazioni che le consentono di offrire altri servizi. I proventi di Google derivano dalla pubblicità: agli utenti che compiano una ricerca su Internet utilizzando il motore di ricerca di Google, o che effettuino una ricerca all'interno di una piattaforma fornita da Google (come YouTube), sono fornite due liste di risultati: sul lato sinistro dello schermo compaiono i risultati "naturali" della ricerca, sul lato destro, invece, vengono mostrati link di natura pubblicitaria. Gli inserzionisti interessati a una pubblicità mirata possono acquistare parole per la pubblicità, può indicare le parole il cui utilizzo nella ricerca attiverà la visualizzazione del proprio link pubblicitario e l'ammontare che egli è disposto a pagare quando un utente clicchi su quel link: gli inserzionisti partecipano a un'asta che determina se il loro link sarà visualizzato, e in quale posizione, tale posizione è data anche dalla qualità del messaggio pubblicitario a esso collegato.

5.5.3 Le raccolte di contenuti on-line

La formazione del Web 2.0 è stata resa possibile dalla disponibilità di numerose piattaforme per la condivisione di contenuti, nelle quali l'utente può liberamente e facilmente trasferire i propri contenuti (testi, tracce musicali, filmati), rendendoli accessibili al pubblico; limitiamoci a presentarne due:

- **SSRN**: contiene numerosi sommari (abstract) e contributi nel campo delle scienze giuridiche e sociali, liberamente e gratuitamente scaricabili. Una volta registratosi presso il sito, l'autore può pubblicare online i propri contributi, rendendoli accessibili a tutti; può limitarsi a inserire sul sito il sommario del proprio contributo, ma di solito mette online il testo completo, prima di pubblicarne la versione definitiva su una rivista scientifica. Altri utenti possono inserire indicazioni e commenti utili per completare il proprio articolo.
- **YouTube**: permette di condividere filmati e tracce musicali. Tutti possono accedere ai filmati su YouTube e chi si registra può caricare un numero illimitato di filmati. I filmati non possono essere scaricati (non se ne può trasferire copia sul proprio calcolatore) ma possono solamente essere visualizzati all'interno della piattaforma. Gli utenti possono inserire commenti ed esprimere le proprie valutazioni, segnalare video sconvenienti o illegali, sollecitandone la rimozione.

Le raccolte di materiali online hanno condotto a problemi giuridici, attinenti:

- **al diritto d'autore**: nascono dalla pubblicazione on-line di contenuti protetti senza il consenso del titolare dei diritti;
- **alla protezione dei dati**: nascono in una duplice direzione: trattamento non autorizzato o illegale dei dati concernenti le persone che hanno caricato i filmati online o li hanno visualizzati; e trattamento dei dati afferenti alle persone raffigurate nel filmato;
- **distribuzione di contenuti illeciti**.

5.5.4 Le reti sociali

Un sito di rete sociale (**social network**) può essere definito come un servizio basato sul Web che consente agli individui di (1) costruirsi un profilo pubblico o semipubblico all'interno di un sistema circoscritto, (2) specificare una lista di altri utenti con i quali essi condividono una connessione ed (3) esaminare e attraversare la propria lista di connessioni e le liste fatte da altri all'interno del sistema. Questa caratterizzazione individua le tre funzioni fondamentali dei siti di rete sociali:

- **costruzione del proprio profilo** ('identità): gli utenti della rete creano profili che li rappresentano, grazie alla combinazione di informazioni personali di vario genere; l'interessato esprime e costruisce la propria **identità sociale**;
- **la condivisione delle connessioni**: attraverso il sito si mantengono e si sviluppano contatti con altre persone (che possono preesistere all'utilizzo del sito o essere avviati tramite il sito stesso);
- **l'attraversamento della rete delle connessioni**: gli utenti della rete sociale possono identificare la forma della loro comunità e ruolo che essi stessi hanno al suo interno.

Esistono numerose reti sociali, dotate di finalità parzialmente diverse; la rete maggiormente diffusa su scala globale è Facebook; che ebbe origine nel 2005 presso l'Università di Harvard, esisteva la consuetudine di distribuire ai nuovi studenti un volume che riportava le foto di tutti i nuovi iscritti, Zuckerber ebbe l'idea di informatizzare il volume e realizzò un sito atto a svolgere questa funzione e lo mise a disposizione degli studenti di Harvard. La funzione fondamentale di Facebook è quella di definire il proprio profilo, condividere connessioni, partecipare a comunità; consente a ciascuno di decidere con chi condividere i dati nel proprio profilo.

Rimane irrisolto il **conflitto tra privacy individuale e dinamiche comunicative** nelle reti sociali: una volta che qualcuno abbia aperto il proprio profilo ad altri, diventa difficile controllare l'ulteriore utilizzo che questi facciano delle informazioni cui hanno avuto accesso.

5.5.5 I blog

La parola **blog** (diario di bordo del Web) denota un sito Web caratterizzato dalla rapidità di aggiornamento e dall'interattività con i lettori (possono pubblicare brevi messaggi, essere informati tempestivamente sugli aggiornamenti del sito e di dialogare con l'autore inserendo propri commenti). I blog hanno determinato due innovazioni nell'uso della rete:

- è accresciuta **dinamicità**: anche prima dei blog esistevano siti personali, tendenzialmente statici, nei quali una o più persone presentavano se stesse e mettevano a disposizione del pubblico materiali di vario genere. I blog sono dinamici, in essi nuove informazioni sono pubblicate continuamente (con frequenza giornaliera o più elevata);
- è accresciuta **interattività**: prima dei blog i materiali presentati sul sito personale erano opera del titolare del sito, mentre l'interazione si sarebbe svolta al di fuori

(email). I blog consentono ai lettori di associare commenti alle pagine e ai messaggi dell'autore, commenti che sono visualizzati sul blog e ai quali l'autore o altri lettori possono rispondere: diventa il luogo di un dialogo tra l'autore e i lettori; dialogo che può essere regolato dall'autore limitando alcune persone o esercitando un controllo preventivo sui messaggi.

Il blog può avere destinatari differenti:

- può avere **carattere confidenziale**, ed essere rivolto a una cerchia ristretta di soggetti, una sorta di diario con il quale l'autore condivide le proprie esperienze e i propri interessi con amici e conoscenti;
- rivolgersi a quanti debbano essere aggiornati con riferimento a una certa attività;
- rivolgersi alla generalità degli interessati;
- rivolgersi agli interessati al diritto dell'informatica o ai temi di diritto ed economia, fino a essere un giornale con milioni di lettori;
- blog facenti capo a organizzazioni collettive utilizzati per aggiornare il pubblico sulle proprie iniziative e attività.

I blog creano interconnessioni: vengono inseriti link che conducono alle pagine di altri blog ritenuti significativi e osservazioni o commenti sulla pagina cui è diretto il link. Mediante il meccanismo denominato **trackback** (traccia all'indietro) l'autore del blog viene a conoscenza dell'esistenza di legami rivolti al proprio sito, e può rispondere. L'interconnessione dei singoli blog dà vita alla **blogosfera**, la rete composta dai blog e dalle loro molteplici interconnessioni.

5.5.6 I wiki e Wikipedia

Un **wiki** è un sito Web che permette la facile creazione e modifica di un numero qualsiasi di pagine interconnesse mediante un browser Web che usa un linguaggio di marcatura semplificato o un editore di testi WYSIWY. Si tratta di strumenti elettivi per il lavoro cooperativo, rivolti alla creazione di opere comuni ma possono essere anche strumenti individuali. Le pagine dei Wiki sono redatte usando un linguaggio di marcatura più semplice e limitato dell'HTML; tradotte automaticamente in HTML, e in questo formato inviate al browser che le visualizzerà ai lettori. Alcuni sistemi offrono editor di testi WYSIWYG: il sistema presenta all'autore il risultato che sarebbe presentato al lettore, registrando la corrispondente marcatura. Una funzione essenziale dei wiki è il **controllo delle modifiche**, infatti è possibile esaminare tutte le modifiche subite da un testo, e individuare con precisione chi ha effettuato la modifica e in quale tempo, questo perchè offrono strumenti per la gestione delle versioni di un testo.

Wiki è lo strumento ideale per la collaborazione decentrata di più autori; questi possono intervenire sul medesimo testo, controllandone l'evoluzione nel tempo. Un wiki può essere accessibile solo ad alcune persone ma molti wiki sono aperti al pubblico: qualunque utente registrato può intervenire modificando il contenuto delle pagine. Si potrebbe immaginare che

questa gestione anarchica dovrebbe condurre alla distruzione del contenuto informativo del wiki, ma l'esperienza ha mostrato che gli interventi incompetenti o malintenzionati sono rari.

Wikipedia è un wiki che contiene più di cinque milioni di voci, ed è letta da centinaia di milioni di persone, di cui molti partecipano alla redazione delle voci; tale partecipazione, volontaria e non retribuita, è giustificata dall'interesse per i temi trattati dalle voci. La collaborazione tra i redattori delle voci è facilitata da una regola di neutralità, che prevede la formulazione di tutte le diverse opinioni sulle questioni controverse.

5.5.7 La produzione paritetica di contenuti

La produzione paritetica si realizza mediante **attività cooperative**. Secondo Benkler, la produzione paritetica si distingue sia dal modello degli scambi di mercato sia dal modello gerarchico dell'azienda: chi partecipa a iniziative produttive di questo tipo non segue né i segnali forniti dai prezzi, né le indicazioni dei superiori gerarchici. Si tratta di un settore basato su un ambiente di rete, i cui risultati sono soggetti a un'etica di aperta condivisione, in modo che tutti gli altri possano svilupparli, estenderli, e farli propri.

Questo nuovo modo di produzione faciliterebbe l'individuazione delle persone più adatte a svolgere un certo compito, individuazione che è lasciata agli stessi interessati, evitando difficoltà e costi inerenti alla ricerca dei soggetti cui affidare un certo lavoro. Inoltre, essendo basato sulla condivisione e il libero accesso alle risorse informative, consente alle persone più interessate e competenti nell'usare una certa risorsa senza richiedere il permesso di alcuno. Poiché le risorse da usare in comune sono beni informativi, il loro utilizzo è non rivale e la loro generale accessibilità non ne determina l'eccessivo sfruttamento e il deterioramento. La motivazione per impiegare le proprie energie nello sviluppo di prodotti cui tutti possano accedere liberamente può venire secondo dal piacere derivante dalla creazione e dall'appropriazione indiretta (cioè i vantaggi economici che il creatore può trarre in seguito alla libera accessibilità delle proprie opere).

Non sempre la produzione paritetica può trovare piena applicazione; questo perché altri modelli economici possono meglio soddisfare importanti esigenze: quelle dei creatori (il bisogno di essere retribuiti adeguatamente per il proprio lavoro), quelle dei loro committenti (garanzie di professionalità e disponibilità), quelle proprie di progetti permanenti e di ampia scala (disponibilità di strutture amministrative permanenti e affidabili).

5.5.8 Condivisione di contenuti e modelli giuridici: le licenze creative commons

In materia di duplicazione e distribuzione delle opere in formato digitale, il legislatore, in attuazione della normativa comunitaria, ha modificato l'articolo 16 della **legge sul diritto d'autore** specificando che: il diritto esclusivo di comunicazione al pubblico comprende anche la messa a disposizione del pubblico dell'opera in maniera che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente; quindi, chi carica un'opera su una piattaforma accessibile al pubblico (per esempio, YouTube), viola il diritto di comunicazione al pubblico. La disciplina del diritto d'autore stabilisce una durata molto lunga per i diritti di

sfruttamento economico (70 anni dalla morte dell'autore), preveda utilizzazioni libere ristrette, e prevede sanzioni civili, amministrative e penali per l'uso non autorizzato di contenuti protetti.

La disciplina del diritto d'autore sui contenuti digitali (e sul software) è ispirata dall'idea che solo impedendo gli usi non autorizzati si potessero garantire sufficienti profitti all'impresa culturale, e indirizzare gli investimenti verso di essa stimolando la produzione di cultura e conoscenza attraverso i meccanismi del mercato. Nel campo delle opere digitali, numerose opinioni hanno rilevato come una disciplina eccessivamente restrittiva sia scarsamente applicabile e possa favorire gli oligopoli esistenti, limitare l'accesso ai contenuti culturali, e impedire le attività creative. Di qui la richiesta di rivedere la disciplina del diritto d'autore, in particolare riducendo la durata delle esclusive e ampliando le utilizzazioni libere: sono emerse iniziative volte a far sì che lo stesso diritto d'autore possa essere usato per ampliare l'accesso alle opere e il loro uso creativo. Ne è risultato il modello delle **licenze creative commons**: un sistema di licenze semplice e flessibile, che consente all'autore interessato a rendere liberamente accessibili le proprie opere di specificare a quali esclusive egli intenda rinunciare. In tutte le licenze creative commons l'autore autorizza tutti a riprodurre e distribuire l'opera per fini non-commerciali (senza scopo di lucro), e richiede che ogni copia dell'opera (e delle opere derivate tratte da essa) rechi indicazione del suo nome; egli può, se lo desidera:

- ampliare le libertà dei terzi offrendo loro l'ulteriore libertà di modificare l'opera, creando opere derivate basate su di essa;
- assoggettare tale libertà di modifica alla clausola "condividi allo stesso modo" (che corrisponde al copyleft del software libero);
- consentire anche usi commerciali.

Ne risultano sei possibili licenze creative commons:

1. solo riproduzione e distribuzione, solo per fini non commerciali;
2. solo riproduzione e distribuzione, a fini commerciali e non commerciali;
3. riproduzione, distribuzione, e modifica, solo per fini non commerciali, con copyleft ("condividi allo stesso modo");
4. riproduzione, distribuzione, e modifica, a fini commerciali e non commerciali, con copyleft;
5. riproduzione, distribuzione, e modifica, a fini non commerciali, senza copyleft;
6. riproduzione, distribuzione, e modifica, a fini commerciali e non commerciali, senza copyleft.

5.5.9 Contenuti generati dagli utenti e piattaforme commerciali

Le imprese che forniscono le piattaforme del Web impiegano un consistente numero di dipendenti, e operano a scopo di profitto; l'impiego della piattaforma è concesso gratuitamente, ma attività connesse generano reddito: la pubblicità sui siti è fornita a fronte di

un corrispettivo da parte degli inserzionisti, informazioni aggregate risultanti dalle scelte individuali possono essere fornite a pagamento.

L'attività rivolta al profitto dei fornitori delle piattaforme realizza strumenti per la creatività individuale e organizza l'informazione fornita dagli individui in modo che essa divenga conoscenza sociale. Può attuarsi una sinergia: gli individui generano una crescente quantità di contenuti e i fornitori generano migliori servizi per accogliere e aggregare quei contenuti: i bisogni individuali possono realizzarsi in un'economia capace di sostenersi e svilupparsi in un quadro di auto-organizzazione/autoregolamentazione.

Le imprese che offrono servizi e piattaforme per contenuti creati dagli utenti possono utilizzare i dati personali dei propri utenti in forme illecite, e possono adottare strategie commerciali volte a "imprigionare" gli utenti (una volta che le informazioni prodotte dagli utenti siano state trasferite nella piattaforma, gli utenti stessi non sono più in grado di eliminarle); il trasferimento dei dati su una piattaforma online comporta una perdita di controllo da parte dell'utente, anche quando questi abbia la possibilità di rimuovere i dati dalla piattaforma sulla quale sono stati inseriti (quei dati possono essere stati prelevati da altri soggetti). Da tale quadro nasce l'esigenza di elaborare nuove soluzioni tecnologiche e giuridiche che consentano di cancellare i dati dal Web. Il diritto alla cancellazione (**all'oblio**) del soggetto cui si riferiscono i dati si contrappone al diritto all'informazione di chi abbia ottenuto quei dati e li ritenga rilevanti per sé o per altri: adeguate soluzioni richiedono un difficile bilanciamento dei diritti e degli interessi.

Il crescente uso delle piattaforme online può favorire una frammentazione del Web, una divisione in diverse sottoreti; gli utenti tendono a rimanere all'interno della piattaforma, usando i servizi che essa offre piuttosto che i servizi aperti accessibili a tutti gli utenti e i sistemi della rete. La medesima tendenza si verifica nell'accesso al Web mediante dispositivi mobili (chi usa un iPhone non accede ai servizi del Web mediante un motore di ricerca generalista ma mediante App che collegano direttamente ai siti di interesse). Alcuni studiosi della rete temono che questo processo di frammentazione possa pregiudicare la libertà degli utenti e la creatività degli sviluppatori dei software per la rete piegandole alle esigenze di chi controlla le piattaforme. Altri ritengono che le piattaforme chiuse offrano vantaggi in termini di sicurezza e facilità d'uso non altrimenti ottenibili, e che per garantire libertà e creatività basti il mercato (la concorrenza tra i fornitori di piattaforme e servizi).

5.5.10 internet entra nella realtà fisica: servizi di localizzazione, realtà aumentata, Internet delle cose, intelligenza ambientale

L'interazione automatica tra calcolatore e ambiente acquista una nuova dimensione, grazie all'unione di due fattori:

- l'inserimento di calcolatori dotati di sensori in dispositivi di ogni genere;
- il collegamento di quei dispositivi a Internet

L'interazione più diffusa si attua nei servizi basati sulla **localizzazione** (il nostro smartphone è in grado di indicarci il percorso tra due luoghi e ci fornisce anche la nostra posizione nel percorso); se i calcolatori forniti di un sistema di localizzazione sono collegati a Internet, diventa possibile offrire ai loro possessori un insieme di indicazioni e servizi collegati alla posizione, servizi che fanno uso di informazioni disponibili su Internet (dove si trovi nelle vicinanze servizi di un certo tipo).

La **realtà aumentata** indica la visione della realtà ottenuta combinando la raffigurazione di un oggetto tratta dalla realtà con elementi tratti dall'ombra informativa associata a quell'oggetto su Internet (certi smartphone dotati di telecamera possono visualizzare oggetti accompagnandoli con informazioni: il telefono si collega a un sistema che identifica l'oggetto ripreso dalla telecamera e preleva da un database le informazioni che riguardano quell'oggetto; ciò può accadere anche per le persone, grazie allo sviluppo dei sistemi per il riconoscimento facciale, la telecamera del telefonino riprende la faccia di quella persona che viene riconosciuta mediante un confronto con le facce presenti del database).

Il termine **Internet delle cose** indica lo sviluppo di Internet conseguente alla connessione in rete degli oggetti materiali. Tutti gli oggetti potrebbero essere dotati di identificatori univoci e di minuscole etichette radio, capaci di trasmettere un segnale che indica l'identità dell'oggetto. In questo modo sarebbe possibile identificare qualsiasi oggetto, e utilizzare questa possibilità per facilitare gli scambi, i trasporti, l'uso dell'oggetto ecc. Inoltre una quantità crescente di oggetti potrebbe trasmettere la propria identità e compiere elaborazioni e comunicazioni. L'identificazione degli oggetti potrebbe avvenire anche combinando sensori e riconoscimento automatico.

Dotando le cose di capacità di inviare messaggi e di compiere elaborazioni complesse si giunge all'**intelligenza ambientale**, ad ambienti nei quali esistono numerosi dispositivi intelligenti, incorporati nelle abitazioni e negli oggetti di uso in grado di comunicare e di interagire con le persone, adattando gli ambienti alle esigenze di chi ci vive.

Tali sviluppi appena illustrati sollevano problemi giuridici attinenti alla protezione della vita privata e alla tutela delle libertà individuali: emerge la possibilità di realizzare un controllo totale; infatti, ogni nostro comportamento può essere rilevato, classificato, aggiunto ai nostri profili: per prevenire questi sviluppi, è necessario sviluppare un quadro giuridico atto a garantire che la fusione tra mondo virtuale e mondo fisico.

5.5.11 La memoria della rete e il diritto all'oblio

Negli ultimi anni si è assistito ad un ampio dibattito sul **diritto all'oblio** (cancellazione di certi dati personali dopo un certo tempo). Ogni sistema giuridico contiene norme che stabiliscono che certi dati personali, che potrebbero influire negativamente sulla sua reputazione dell'interessato, dopo un certo tempo dovrebbero essere cancellati o resi inaccessibili al pubblico, nell'era pre-informatica tali regole erano limitate a particolari informazioni memorizzate nei registri pubblici (altri dati pregiudizievoli per l'interessato, tipo gli articoli di giornale relativi a reati, sarebbero stati naturalmente "dimenticati" o "oscurati").

Le tecnologie dell'informazione hanno dato luogo a uno scenario diverso: tutti i dati utili possono oggi essere conservati per tempo illimitato e rimanere facilmente accessibili; ciò causa un accrescimento delle conseguenze negative che si possono subire. Da tale situazione emerge un dibattito giuridico sull'esistenza e i limiti di un diritto a che il trattamento di dati personali concernenti eventi passati abbia termine o sia ristretto (anche quando il trattamento fosse in origine legittimo).

Internet è una memoria transattiva, nella quale ognuno può potenzialmente inserire o ricercare informazioni, ciò comporta la difficoltà di eliminare del tutto le informazioni: possono esistere numerose copie dei dati pubblicati in rete e le informazioni rimosse possono essere nuovamente inserite. La dimensione transattiva-comunicativa di Internet fa sì che la cancellazione dei dati possa comportare un conflitto tra interessi: da un lato i diritti alla privacy e all'identità dell'interessato, e dall'altro le libertà di espressione e comunicazione di chi abbia pubblicato online l'informazione e di chi potrebbe accedere ad essa.

La Corte di Cassazione nel 2012 affermò l'obbligo di contestualizzare e aggiornare informazioni pubblicate online, quando dati ulteriori possano completare il significato sociale di tali informazioni, a vantaggio dell'interessato. I giudici stabilirono che un articolo relativo ad un'inchiesta giudiziaria, pubblicato nell'archivio online di una testata giornalistica, doveva essere integrato dai link alla successiva sentenza di proscioglimento. In questo caso si poté superare il conflitto tra il diritto all'oblio e le libertà di espressione e informazione, ampliando l'accesso all'informazione.

La Corte di Giustizia dell'Unione Europea, nella decisione nel caso Google-Spain, ha stabilito che gli interessati hanno un particolare diritto nei confronti dei motori di ricerca, il **diritto alla deindicizzazione**, l'interessato ha il diritto di chiedere che i risultati delle ricerche effettuate usando il suo nome omettano i link a dati personali indesiderati (tale diritto prevale sull'esigenza dell'accessibilità delle informazioni). Il caso sottoposto alla corte riguardava un cittadino spagnolo, il quale aveva chiesto a Google di rimuovere dai propri indici i link ad un articolo di giornale su una vicenda giudiziaria in cui era stato coinvolto ricevendo un diniego. In esecuzione della sentenza Google ha attivato una procedura online mediante la quale gli interessati possono chiedere la deindicizzazione.

5.6 La documentazione giuridica e Internet

5.6.1 La tesi: i sistemi centralizzati degli anni '60 e '70

Tra gli anni '60 e gli anni '70 furono creati sistemi per la documentazione giuridica automatica; negli Stati Uniti tali iniziative furono sviluppate prevalentemente da imprese private, mentre in Europa si attivarono soggetti pubblici. La creazione di tali sistemi si basava sull'idea che si dovesse realizzare in ogni paese un singolo sistema nazionale per la documentazione giuridica, nel quale tutte le fonti del diritto fossero registrate elettronicamente e rese disponibili per la ricerca.

5.6.2 L'antitesi: I molteplici sistemi isolati degli anni '90

Il personal computer consentì l'ingresso dell'informatica nelle attività giuridiche, negli anni '80 la documentazione giuridica si spostò su basi documentali disponibili sul PC, che potevano essere usate senza i costi e i ritardi del servizio telefonico remoto. Ciò fu consentito dal **compact disk**, un nuovo dispositivo di memorizzazione, dotato di capacità superiore, leggibile mediante lettore ottico collegato al PC e consultabile mediante software.

Questa innovazione tecnologica determinò l'entrata degli **editori commerciali** nel campo della fornitura di informazione giuridica; essendo il CD un oggetto materiale facilmente distribuibile, gli editori potevano commercializzare le banche di dati giuridici attraverso i canali esistenti per la vendita di libri e riviste. I cd favorivano l'integrazione dei contenuti; infatti, molti editori realizzarono CD che univano i diversi materiali a loro disposizione.

La diffusione del PC facilita la redazione dei documenti giuridici in forma elettronica. Fino agli anni '70 i calcolatori non erano usati nella redazione dei documenti; ciò comportava una separazione completa tra la fase della preparazione dei documenti giuridici e la loro successiva memorizzazione in sistemi informativi computerizzati. All'inizio degli anni '80 si resero disponibili su PC **elaboratori di testo**, il cui uso si estese alla redazione dei documenti giuridici e favorì la progressiva integrazione tra la produzione dei documenti giuridici e la loro distribuzione in forma elettronica. Ciò ha avuto alcuni effetti:

- si è ampliato l'ambito dei documenti che possono essere resi disponibili al pubblico;
- si è stabilita una connessione tra le procedure intese a produrre il diritto e i sistemi per la documentazione giuridica: la procedura fornisce un documento elettronico, e il documento può essere usato all'interno della stessa procedura, ma può anche essere reso accessibile al pubblico;
- si è rafforzata la posizione delle autorità giuridiche, che possono distribuire direttamente i risultati della propria attività, in forma elettronica, senza doverne affidare a terzi la digitalizzazione.

La versione elettronica della gazzetta ufficiale, grazie alla sua economicità e alla rapidità della sua distribuzione, ha soppiantato la versione cartacea (costituendo in alcuni paesi l'unica versione).

5.6.3 La sintesi: I sistemi universalmente accessibili, ma plurali, degli anni '90

La rivoluzione di Internet, avvenuta negli anni '90, crea la sintesi tra la tesi degli anni '70 (che prevedeva la realizzazione di un unico sistema per la documentazione giuridica) e l'antitesi degli anni '80 (che prevedeva la distribuzione di copie di diverse banche date). Tale sintesi consiste nell'accesso mediante un unico sistema tecnologico distribuito (il Web), a tutte le fonti di documentazione giuridica. La sintesi di Internet ha portato a una grande crescita nella quantità di informazioni giuridiche disponibili sul Web, una crescita da cui hanno tratto profitto gli studiosi del diritto, i pratici e i comuni cittadini.

Per ritrovare sul Web l'informazione giuridica di cui abbiamo bisogno, bisogna estrarre tale informazione da una raccolta di materiali enorme e diversificata: usiamo a tal fine motori di ricerca per Internet e ritroviamo tutti i testi che contengano certe parole o combinazioni di parole, ordinati secondo la loro rilevanza; il risultato è spesso un insieme di documenti che rappresenta solo l'inizio della nostra ricerca: dobbiamo scorrere i documenti ritrovati, e controllare la loro pertinenza rispetto al nostro obiettivo e l'affidabilità della loro fonte. Dopo aver risolto il problema del rumore (i documenti irrilevanti ottenuti come risposta all'interrogazione) dobbiamo affrontare il problema del silenzio (il mancato ritrovamento di documenti rilevanti esistenti sul Web); per risolvere tale problema sarebbe necessaria una ricerca avanzata capace di ritrovare tutti i documenti che parlino del tema che ci interessa. Una volta ritrovati tutti i documenti rilevanti, l'utente deve affrontare il compito di combinare i diversi frammenti di informazione che afferiscono al suo problema.

5.6.4 Una nuova tesi: un sistema informativo giuridico centralizzato per l'era di Internet

L'informazione giuridica su Internet è caratterizzata dalla **frammentazione**: è fornita da enti diversi ed è suddivisa in molti siti (che non seguono standard comuni); porre rimedio a questa frammentazione faciliterebbe la cognizione del diritto, ma al riguardo possiamo distinguere due indirizzi antitetici:

- La tesi consiste in un nuovo modello di sistema di documentazione onnicomprensivo, affidato all'iniziativa pubblica, il cui funzionamento sia integrato con lo svolgimento delle procedure legislative, giudiziarie e amministrative;
- L'antitesi consiste nello sviluppo decentrato di sistemi informativi, al di fuori della pubblica amministrazione, sulla base della libera disponibilità di documenti giuridici in formato elettronico.

Per ciò che attiene la tesi, viene affermato che la direzione da seguire nella documentazione giuridica automatica consiste nel passaggio dalla ricerca documentale alla gestione della normativa. Si tratta di un sistema che consiste in una **base di dati-madre** che contiene tutti i documenti giuridici, di qualsiasi tipo, arricchiti di opportune informazioni mediante marcatura. Tale base di dati dovrebbe essere predisposta e aggiornata mediante un processo editoriale centralizzato, che controlli i documenti di input e inserisca in essi la marcatura richiesta. Dalla base di dati madre si trarranno diversi output in diversi formati (una base di dati per professionisti, che offre prestazioni elevate e più ampi contenuti agli utenti professionali, una gazzetta ufficiale con la nuova legislazione, compilazioni del diritto in vigore, e tutti i testi ufficiali in versione originale, liberamente accessibili).

5.6.5 Una nuova antitesi: l'accesso a risorse giuridiche distribuite

L'antitesi rispetto alla soluzione centralizzata (accesso universale a una base di dati pubblica) consiste nel fornire uno o più punti di accesso a risorse giuridiche condivise, che risiederanno sui sistemi informativi delle autorità che le hanno prodotte e che saranno accessibili in rete. In questo modello Internet fornisce sia i canali attraverso i quali l'informazione è estratta dalle basi di dati originali, sia i canali attraverso i quali l'utilizzatore accede all'informazione. Tale

antitesi si basa sul fatto che paesi di grandi dimensioni, dotati di una pubblica amministrazione distribuita e di ordinamenti giuridici eterogenei, richiedono architetture decentrate: per garantire la conoscibilità del diritto, in un contesto pluralistico (nel quale l'iniziativa privata si affianca a quella pubblica), è necessario fornire libero accesso alle fonti computerizzate dei dati giuridici. Una volta che le autorità pubbliche abbiano reso accessibili i testi giuridici, altri attori (operanti con o senza scopo di profitto) possono occuparsi della distribuzione di quei testi, e del loro arricchimento con informazioni ulteriori.

Entrambi i modelli presentati presentano aspetti positivi. Il modello dell'unico database madre è basato sull'idea che tutte le fonti del diritto dovrebbero essere registrate in formati uniformi, i documenti normativi nella loro versione elettronica originale dovrebbero includere tutta l'informazione necessaria per diverse successive utilizzazioni; questo modello offre affidabilità dell'informazione giuridica e coerenza formale delle diverse fonti. Dei vantaggi sono apportati anche dall'idea di estrarre informazioni da basi di dati giuridici distribuite: nello specifico, la diversità dei servizi di informazione giuridica e concorrenza dei fornitori e la decentralizzazione e l'autonomia.

5.6.6 Una nuova sintesi: l'adozione di standard condivisi

È emersa una sintesi, il cui aspetto unificatore consiste nell'adozione di uno standard comune, che deve specificare come i documenti giuridici possano ricevere degli identificatori nomi univoci e come essi possano essere arricchiti di informazioni elaborabili automaticamente. Tale standard dovrebbe fornire la possibilità di esprimere, in modo riconoscibile dal calcolatore, gli elementi strutturali del testo e i riferimenti normativi e le modifiche.

I provvedimenti giuridici dovrebbero essere registrati in documenti elettronici ufficiali rispettosi dello standard condiviso; tali documenti potrebbero essere memorizzati in database distribuiti o centralizzati, essere riutilizzati ed elaborati con ogni software predisposto in conformità allo standard, essere integrati con ulteriori informazioni previste dallo standard ed elaborati conseguentemente. I documenti ufficiali, prodotti dall'organo autoritativo, dovrebbero essere univocamente identificabili e il loro contenuto determinato. Secondo questo modello, la gestione dei testi legislativi dovrà attuarsi nel modo seguente:

- il testo degli atti approvati dal Parlamento conterrà già tutta l'informazione strutturale e i metadati disponibili in questa fase;
- il Parlamento renderà pubblici tutti i documenti prodotti durante la procedura legislativa che saranno fin dall'inizio creati nel formato richiesto dal relativo standard, e quindi potranno essere immediatamente resi accessibili al pubblico.

In questo modello non si richiede alcun intervento editoriale, i documenti escono dalla procedura parlamentare già nel formato richiesto dallo standard: includeranno in forma interpretabile, automaticamente, informazioni sufficienti affinché software sviluppati sulla base dello standard possano distribuire i documenti all'interno delle istituzioni parlamentari e al pubblico.

CAPITOLO 6: L'intelligenza artificiale

6.1 Il concetto di IA

6.1.1 L'intelligenza

Manca una definizione univoca e condivisa di intelligenza, si conviene che l'intelligenza si rivela nella capacità di svolgere diverse funzioni: l'adattamento all'ambiente, l'apprendimento dall'esperienza, la percezione, l'intuizione, la comunicazione, e così via.

L'IA vuole studiare l'intelligenza, ma si propone anche di costruirla. L'IA trae ispirazione dall'intelligenza naturale, trovando in questa soluzioni appropriate alle proprie esigenze di elaborazione dell'informazione. Tra l'IA ed intelligenza umana vi sono differenze: l'intelligenza umana è realizzata da un hardware di cellule cerebrali e sensoriali, diverso dall'hardware dell'IA (chip di silicio, telecamere e altri sensori). I processi cognitivi umani implicano l'attivazione contemporanea di un elevato numero di neuroni, i sistemi artificiali sono più semplici, ma più veloci, e hanno prestazioni superiori in talune forme di elaborazione dell'informazione (in altre elaborazioni sono inferiori). Il sistema nervoso umano è immerso nel corpo, di conseguenza i processi cognitivi interagiscono in modi complessi con le funzioni biologiche svolte dagli organi e con i processi del metabolismo; nei cervelli artificiali l'integrazione di aspetto corporeo e cognitivo è assente.

6.1.2 Idee di IA

Si distinguono diversi modi di accostarsi all'intelligenza secondo due diverse dimensioni:

- l'idea che l'intelligenza consista prevalentemente nel pensiero si contrappone all'idea che in essa l'interazione con l'ambiente svolga un ruolo preminente;
- l'obiettivo di riprodurre fedelmente le capacità intellettive dell'uomo si contrappone all'obiettivo di realizzare sistemi capaci di razionalità prescindendo dai limiti della razionalità umana.

Viene proposto uno schema che riporta diverse definizioni di IA distinguendole a seconda di come si collocano rispetto alle due dimensioni appena indicate:

- **distinzione tra pensiero e azione:** il comportamento intelligente richiede il collegamento tra il momento epistemico (volto a determinare come stanno le cose, come è fatto il contesto nel quale l'agente si trova e quali dinamiche lo caratterizzano) e il momento pratico (volto a determinare il comportamento più appropriato rispetto agli interessi dell'agente, nel contesto della sua azione): gli interessi epistemici (quali cose un agente desidera conoscere) sono determinati anche dagli obiettivi pratici dell'agente (da che cosa esso intenda realizzare o conservare), e i modi del perseguimento degli obiettivi pratici dipendono dalle nostre conoscenze epistemiche;
- **distinzione tra l'obiettivo** di riprodurre pienamente il pensiero umano e quello di sviluppare procedure cognitive razionali: dipende dall'obiettivo di un'applicazione di IA: simulare l'uomo o affrontare nel modo migliore certi problemi. Scelte che

appaiono irrazionali con riferimento a un concetto ideale di razionalità (non assicurando un risultato ottimale, cioè il migliore risultato possibile) possono apparire appropriate (razionali nella misura in cui ci è possibile esserlo) quando si considerino i limiti delle nostre capacità conoscitive e la complessità dell'ambiente. La nostra stessa ragione ci vieta di sprecare le nostre energie nell'impossibile ricerca della scelta ottimale, e ci richiede di seguire procedure cognitive fallibili, ma rapide ed economiche che conducano a risultati sufficientemente buoni nella maggior parte dei casi. Queste procedure sono chiamate euristiche: ciò che può apparire un difetto della razionalità umana, può rivelarsi una procedura cognitiva appropriata per una razionalità limitata: emulare (copiare) l'intelligenza umana, anche in aspetti apparentemente irrazionali (o solo limitatamente razionali) può condurre a soluzioni efficaci. I sistemi informatici hanno enormi capacità di calcolo e memoria; ma le euristiche diventano necessarie anche per i sistemi informatici, quando i dati accessibili siano limitati, o quando il problema da affrontare presenti un'elevata complessità computazionale.

6.1.3 Un concetto giuridico di IA

L'IA è *la scienza e l'ingegneria del fare macchine intelligenti*, specialmente programmi intelligenti per computer. In ambito giuridico, si è avuta una proposta di **Regolamento sull'IA** (Legge sull'IA), al fine di delimitare il proprio ambito di applicazione; tale regolamento definisce un sistema di IA come un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono. Tre tecnologie che caratterizzano l'IA:

- approcci di apprendimento automatico;
- approcci basati sulla logica e approcci basati sulla conoscenza;
- approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

Una diversa definizione è stata fornita, dall'AI ELEG, nel rapporto predisposto ai fini dell'elaborazione di una strategia europea sull'IA, che ha preceduto la Proposta di Regolamento afferma che: i sistemi di intelligenza artificiale sono sistemi software sviluppati da esseri umani che, dato uno scopo complesso, operano nella dimensione fisica o digitale percependo il loro ambiente mediante l'acquisizione di dati, interpretando le strutture di dati strutturati e non strutturati raccolte, ragionando sulla conoscenza, o elaborando l'informazione, derivata da questi dati e decidendo le migliori azioni da compiere per raggiungere i goal dati. I sistemi di AI possono usare regole simboliche o apprendere un modello numerico, e possono adattare il loro comportamento analizzando come l'ambiente sia influenzato dalle loro azioni precedenti.

Questa definizione elenca molte funzioni nei sistemi di IA: riconoscimento di pattern (analisi di attitudini e sentimenti, ecc.), traduzione (da un linguaggio all'altro), il filtro di informazioni indesiderate (spam, violenza, pornografia, ecc.), selezione di informazioni

(pubblicità o notizie mirate). Alcuni sistemi svolgono solo alcune funzioni, altri combinano diverse capacità, come i veicoli autonomi, che debbono essere in grado di identificare gli oggetti che incontrano, ma anche di pianificare il percorso da effettuare, e autogovernarsi nel viaggio verso la meta.

Le norme più significative del regolamento si applicano solo ai sistemi che il Regolamento classifica come sistemi ad alto rischio, che è ciò che conta ai fini dell'applicazione.

6.2 L'IA nel contesto

6.2.1 Algoritmi

Gli algoritmi sono procedure suscettibili di applicazione automatica, il loro utilizzo si estende oltre i sistemi di IA; non tutti gli algoritmi riguardano l'IA, ma ogni sistema di IA, come ogni sistema informatico, comprende algoritmi. Gli algoritmi dell'IA possono svolgere diverse funzioni epistemiche e pratiche e diverse forme di apprendimento. Un sistema per IA comprende molti algoritmi, dalla cui interazione risulta il funzionamento del sistema stesso; l'AI può essere visto come un singolo algoritmo complesso, che comprende gli algoritmi che risolvono funzioni specifiche.

6.2.2 Big Data

Il termine **Big Data** viene applicato a enormi raccolte di dati che è difficile trattare usando le tecnologie informatiche solitamente impiegate per la gestione dei dati digitali; ciò che caratterizza tali massi sono le cosiddette tre V: enorme **Volume**, alta **Velocità** e grande **Varietà**, altre caratteristiche sono la bassa Veracità (informazioni inaccurate) e l'alto Valore (l'utilità).

I dati che compongono i Big Data possono essere creati dagli umani, ma più spesso sono raccolti automaticamente, da dispositivi che raccolgono informazioni dal mondo fisico o che mediano attività economiche e sociali collegando gli individui facendoli partecipare a organizzazioni socio-tecniche. I Big Data possono riguardare il mondo fisico e digitale non-umano (dati astronomici, ambientali, biologici, industriali, tecnologici), così come gli umani e le loro relazioni (dati sulle reti sociali, la salute, la finanza, i trasporti, ecc.).

Da una prospettiva sociale e giuridica ciò che rende "grande" una massa di dati è una caratteristica funzionalità: la possibilità di usare quei dati per finalità di analitica, per scoprire correlazioni e fare predizioni.

6.2.3 Robotica

L'IA costituisce il nucleo della **robotica**, la disciplina che si occupa di costituire agenti fisici che compiano compiti che richiedono la manipolazione del mondo fisico; la robotica può essere definita come IA in azione nel mondo fisico.

Un **robot** è una macchina fisica che deve affrontare la dinamica, le incertezze e le complessità del mondo fisico. I **robot fisici** sono una macchina, situata nel mondo, che sente, pensa e agisce; un robot deve avere:

- sensori: necessari per ottenere informazioni dall'ambiente, un robot può utilizzare diversi sensori: video-camere o laser per sondare l'ambiente, dispositivi come il GPS per determinare la propria ubicazione, giroscopi o acceleratori per misurare il proprio movimento;
- capacità di elaborazione che emula alcuni aspetti della cognizione: i comportamenti reattivi non richiedono alcuna abilità cognitiva profonda, ma l'intelligenza è necessaria se il robot deve compiere compiti significativi autonomamente;
- attuatori: l'attuazione è necessaria per consentire al robot di esercitare forze sul suo ambiente. Gli effettori o attuatori possono essere avere varie forme e funzioni: gambe, ruote, articolazioni, pinze.

I robot possono essere classificati in tre categorie principali:

- **robot manipolatori:** ancorati fisicamente al proprio posto di lavoro, si presentano tipicamente nella forma di bracci meccanici mobili; infatti, la maggior parte di essi vengono impiegati nelle catene di montaggio;
- **i robot mobili:** si spostano nell'ambiente, con vari strumenti di locomozione (gambe, ruote, eliche, etc.). Molti robot mobili sono usati in ambienti ristretti, dove svolgono funzioni limitate (la pulizia dei pavimenti), altri robot mobili sono dotati della capacità di affrontare missioni di ampio raggio, anche in spazi condivisi con gli esseri umani. Sta avvenendo una progressiva robotizzazione delle automobili (sensori per riconoscere ostacoli, mantenimento della direzione sulla strada), stanno entrando in funzione automobili senza pilota. I *rover*, veicoli di superficie usati nelle esplorazioni extraterrestri (sulla Luna o su Marte) possono muoversi per lungo tempo (anche per più anni) con autonomia, affrontando terreni sconosciuti. Sono numerosi i veicoli aerei senza pilota usati a fini di sorveglianza, nei lavori agricoli o in operazioni militari e profondità marine sono esplorate attraverso l'impiego di Veicoli robotici sottomarini;
- **robot manipolatori mobili:** uniscono manipolazione e movimento (dispositivi robotici usati per disinnescare bombe). A questa categoria appartengono i robot antropomorfi o umanoidi, dotati di un corpo dotato di arti e testa, che mima la struttura fisica degli umani.

Appartengono alla robotica anche:

- **i dispositivi protesici con capacità cognitiva**, destinati a sostituire parti del corpo umano, come gli arti, o l'apparato per l'udito o la visione;
- **robot multicorpo** (multibody), che consistono di gruppi o sciame di dispositivi separati che si autoorganizzano.

6.2.4 Intelligenza ambientale

In riferimento all'**intelligenza ambientale**, si tratta dell'inserimento nell'ambiente fisico di dispositivi automatici dotati della capacità di elaborare informazioni e di esibire comportamenti intelligenti. Tali dispositivi possono assorbire informazioni sia dall'ambiente fisico sia dalla rete informatica; sono destinati a inserirsi nell'ambiente in modo ubiquo e invisibile, governando macchine di vario genere, e facendo sì che l'ambiente stesso si adatti automaticamente alle esigenze dell'uomo; possono comunicare tra loro e con altri dispositivi digitali, ma anche percepire i mutamenti dell'ambiente e reagire agli stessi (casa nella quale la porta si apra automaticamente ogni qualvolta la telecamera riconosca uno degli abitanti, l'impianto stereo proponga brani musicali, tenendo conto dei nostri gusti).

Poiché si tratta di una prospettiva che, accanto agli aspetti positivi, manifesta diversi profili problematici, l'UE ha dedicato uno spazio nei propri progetti all'intelligenza ambientale; si rendono necessarie garanzie giuridiche (tutela dei dati personali, protezione dell'interessato rispetto alle possibilità di sfruttamento).

Lo sviluppo dell'intelligenza artificiale ambientale sembra ricreare un mondo "incantato" nel quale ci accostiamo agli oggetti in modo analogo a quello con cui interagiamo con le persone; in un vicino futuro interagiranno con gli oggetti intelligenti adottando uno stile comunicativo, cioè interrogandoli sulle iniziative che stanno adottando, e indicando a essi i risultati da realizzare o i modi per raggiungerli. Il mondo incantato dell'intelligenza ambientale può diventare un mondo stregato, nel quale gli oggetti (o chi li governa) ci manipolano, ci sfruttano, operano a nostro danno.

6.3 I limiti dell'IA

6.3.1 Intelligenza specifica e intelligenza generale

Le ricerche di IA possono condurre a due risultati distinti, seppure connessi:

- l'intelligenza specifica artificiale: a questa appartengono tutte le applicazioni di IA disponibili, si tratta di sistemi capaci di ottenere risultati utili in attività che richiedono intelligenza, con prestazioni che in alcuni casi sono al livello umano o anche sovrumano. L'IA specifica può essere impiegata con profitto anche in compiti nei quali i sistemi informatici sono ancora inferiori agli umani, ma in cui il loro impiego risulta conveniente per ragioni di costo e rapidità (traduzioni). In molti casi, il risultato migliore può ottenersi combinando intelligenza artificiale e umana. Le applicazioni di intelligenza specifica artificiale sono limitate agli obiettivi ristretti per i quali sono state sviluppate;
- l'intelligenza generale artificiale: un'intelligenza generale artificiale dovrebbe possedere la maggior parte delle abilità cognitive umane, al livello umano, o anche ad un livello sovrumano. In merito alla realizzazione dell'intelligenza generale artificiale si hanno diverse opinioni:

- A. vi è chi esclude che l'intelligenza generale artificiale sia una prospettiva realistica;
- B. altri ritengono che la realizzazione futura di sistemi dotati di intelligenza generale artificiale, sia una probabilità concreta. A questa prospettiva alcuni guardano con preoccupazione, infatti, un sistema dotato di intelligenza generale artificiale potrebbe migliorare sé stesso e presto superare l'intelligenza umana. Grazie alla sua intelligenza sovrumana potrebbe acquisire capacità non più controllabili da parte degli umani, gli umani si troverebbero in una condizione di inferiorità simile a quella degli animali rispetto agli umani. Alcuni importanti scienziati e tecnologi ritengono sarebbe necessario individuare le misure per prevenire la nascita dell'intelligenza generale artificiale, o per dirigerla verso risultati benefici all'umanità, assicurando che tale intelligenza si allinei ai valori umani;
- C. altri guardano favorevolmente allo sviluppo di un'IA che raggiunga e poi superi i limiti dell'intelligenza umana: potrebbe rappresentare il momento magico, a partire dal quale si scatena uno sviluppo accelerato della scienza e della tecnologia, che potrebbe condurre a risolvere i problemi odierni dell'umanità, a superare i limiti biologici dell'esistenza umana (la malattia ecc.) e a distribuire l'intelligenza (umana e artificiale) nel cosmo.

L'intelligenza generale artificiale potrà realizzarsi, in ogni caso, solo tra qualche decennio. Solo sulla base di esperienze più ampie con sistemi avanzati di IA di applicazione progressivamente più generale, sarà possibile comprendere l'ampiezza e la prossimità dei rischi per l'umanità e individuare i modi migliori per affrontarli.

6.3.2 IA forte e IA debole

Un'altra distinzione è quella tra:

- **IA forte:** anche i calcolatori sono capaci di stati cognitivi e di pensiero, si propone di costruire menti artificiali;
- **IA debole:** si propone di realizzare sistemi artificiali capaci di svolgere compiti complessi, sistemi che possono mimare (simulare) aspetti dei processi cognitivi umani, ma che non possono riprodurre quegli stessi processi.

I sistemi di IA oggi disponibili non sarebbero in grado di pensare, non possederebbero una mente.

Il dibattito circa la possibilità di sviluppare forme di IA forte può essere fatto risalire a Turing, che già nel 1936 si interrogava sulla possibilità di sviluppare macchine intelligenti, e su come verificare quando e in quale misura questo risultato potesse considerarsi raggiunto. Turing proponeva un test ispirato a un gioco di società, il "**gioco dell'imitazione**", nel quale una persona interroga due interlocutori di sesso diverso, al fine di determinare chi di questi sia l'uomo e chi la donna; nel gioco di Turing lo scopo dell'interrogante è quello di distinguere l'interlocutore umano e l'interlocutore elettronico, quando un sistema informatico riuscirà a

far credere di essere una persona, l'IA sarà realizzata. Nessun sistema ha ancora superato o si è avvicinato al superamento del test di Turing.

6.3.3 L'AI e la comprensione dei significati

Il test di Turing solleva un problema teorico: se un sistema che riuscisse a superare il test sarebbe una vera IA, o invece sarebbe solo un mero "idiota sapiente"; il test di Turing è comportamentale: per superarlo è sufficiente che la macchina si comporti come un essere umano, non è necessario che esso abbia veramente una mente, dei pensieri.

Vi è stato chi, come Searle, ha affermato l'impossibilità teorica di realizzare sistemi informatici capaci di attività mentale. Per criticare le pretese dell'IA forte Searle ha sviluppato un celebre esperimento mentale, "**l'argomento della stanza cinese**": ci invita a immaginare che una persona capace di parlare solo la lingua inglese (non il cinese) sia chiusa in una stanza dotata di una fenditura verso l'esterno, la stanza contiene dei fogli di carta e un manuale di istruzioni che specifica come, una volta ricevuto un input consistente in una sequenza di caratteri cinesi, si debba produrre un output consistente in un'altra sequenza degli stessi caratteri. Le regole collegano a ogni input l'output appropriato (la risposta che giudicherebbero appropriata in una conversazione tra persone che conoscono il cinese), ma sono formali, fanno riferimento solo alla struttura sintattica della comunicazione prescindendo dal significato dei messaggi: per ogni sequenza di simboli di input tali regole indicano la sequenza di caratteri di output corrispondente e possono essere applicate senza conoscere il significato delle parole formate con quei caratteri. Dalla fenditura viene immesso un foglio di carta che riporta caratteri cinesi (incomprensibili a chi non conosca questa lingua), seguendo le istruzioni del manuale, la persona nella stanza scrive su un foglio bianco la risposta (in caratteri cinesi) che le regole del manuale collegano ai caratteri indicati nei fogli di input, e spinge il foglio attraverso la fenditura. Le risposte che escono dalla camera cinese, sono indistinguibili da quelle che potrebbero essere fornite da una persona capace di parlare il cinese. Di conseguenza la camera cinese riuscirebbe a superare il test di Turing. Searle sostiene però che la persona all'interno della stanza cinese ha solo manipolato simboli a lei incomprensibili: anche se quella persona si comporta come un parlante cinese, le è precluso l'accesso al significato dei simboli che ricopia. La persona nella stanza cinese è il calcolatore, guidato da un software: un calcolatore capace di conversare come un essere umano non è capace di pensieri, non ha una mente, si limita alla cieca manipolazione di simboli.

Numerosi studiosi IA hanno raccolto la sfida di Searle, e hanno contestato il suo argomento. Alcuni hanno obiettato che, anche se l'uomo all'interno della stanza cinese non capisce il cinese, l'intero sistema (la stanza, la persona, e il manuale di regole) è in grado di capire il cinese, possedendo la capacità di rispondere a input in quella lingua producendo output appropriati nella stessa. L'errore di Searle consisterebbe nell'estrarre da tale sistema una sola componente (l'elemento che effettua le trasformazioni simboliche, corrispondente alla persona nella stanza). Sarebbe come chiedersi se la funzione mentale umana consistente nell'effettuazione di operazioni di ragionamento sia sufficiente a comprendere una lingua, una volta separata dalla memoria, dalle conoscenze, dai sensi, ecc. Un'ulteriore critica attiene al

fatto che tanto la mente umana quanto il calcolatore elaborano informazioni con velocità ed efficienza enormemente superiori rispetto all'operatore della stanza cinese. L'impressione che la stanza non capisca il cinese si basa su questa circostanza, non applicabile all'elaborazione informatica. Non sarebbe giustificato estendere ad ogni sistema informatico le conclusioni concernenti la stanza cinese.

Altri hanno osservato che la conclusione che la persona nella stanza (o la stanza nel suo insieme) non comprenda il cinese è determinata dal fatto che la comprensione di un linguaggio richiede la capacità di connettere le parole ai loro referenti reali, il che presuppone l'esperienza degli oggetti di cui parla il linguaggio (o almeno di alcuni di essi). Questo limite di un calcolatore isolato non si applicherebbe però ai sistemi automatici che uniscano capacità percettive (e possibilmente motorie) a quelle attinenti all'elaborazione e alla registrazione delle informazioni. I limiti della stanza cinese non sono limiti dell'IA: essi possono essere superati estendendo il sistema con dispositivi capaci di movimento e dotati di appropriati sensori.

Altri hanno osservato che l'intelligenza è un fenomeno emergente da comportamenti meccanici (non intelligenti) anche nel caso del cervello umano: anche l'intelligenza umana nasce da processi non intelligenti, le operazioni "meccaniche" (i processi chimici e fisici) che hanno luogo all'interno dei singoli neuroni del cervello umano e nei contatti (sinapsi) tra gli stessi. Allo stesso modo le operazioni meccaniche che avvengono all'interno del calcolatore programmato potrebbero dare origine all'intelligenza.

Bisogna distinguere due questioni circa l'esperimento mentale della "stanza cinese":

Una prima questione riguarda i sistemi informatici oggi disponibili. Ci possiamo chiedere se questi sistemi siano in grado di comprendere il linguaggio nel modo in cui lo comprendono gli umani, di avere consapevolezza dei significati delle parole e della connessione tra parole e mondo. La risposta al riguardo sembra essere negativa, per ora i sistemi informatici non hanno accesso, se non in misura molto limitata alla dimensione della semantica. Essi si limitano ad un "pensiero cieco" che consiste nell'elaborazione di numeri, o altri simboli, senza avere consapevolezza dei relativi significati. Si tratta di un'elaborazione simile a al nostro ragionamento quando eseguiamo rapidamente dei calcoli matematici, applicando regole prestabilite, senza riflettere sul significato delle regole e dei processi attivati dalla loro esecuzione. Nella comunicazione umana il linguaggio non si limita a combinare parole, esso fa riferimento al mondo fisico e sociale, per capire pienamente che cosa significhi un enunciato non basta collegare tra loro le parole che lo compongono, ed esaminare i rapporti tra quelle parole e altre parole, bisogna anche collegare le parole alle cose cui si riferiscono, e gli enunciati alle situazioni che descrivono, costituiscono o prescrivono: la comprensione piena del linguaggio presuppone infatti l'esperienza del mondo.

I limiti dell'IA di oggi non debbono indurci ad escludere realizzazioni future che includano la progressiva comprensione del linguaggio e del rapporto tra parole e mondo. Sistemi artificiali possono dotarsi di una capacità di "fondare" i significati: essi possono, collegare parole e

immagini, e qualora abbiano una dimensione robotica, anche stabilire connessioni tra parole e interazioni con cose e situazioni.

6.4 Breve storia dell'IA

6.4.1 L'IA prima dell'IA

Il tema del rapporto tra IA e intelligenza umana troverà sviluppo in opere di fantascienza. Nell'opera di Clarke e Asimov, Clarke immaginò il calcolatore HAL, capace di ragionare e di comprendere, acquistando una psicologia umana. L'HAL attiene al disallineamento di valori, il suo comportamento si discosta dai valori umani.

Il comportamento dei sistemi intelligenti deve conformarsi e rimanere conforme ai valori umani: un'IA sovrumano, al fine di raggiungere un obiettivo apparentemente buono, potrebbe realizzare 'istanziamenti perverse'; per evitare che ciò accada dovrebbero perseguire un meta-scopo, preminente su ogni obiettivo specifico loro assegnato, quello di aiutare le persone a raggiungere gli scopi che esse desiderano perseguire.

Asimov analizza il problema del rapporto tra gli uomini e sistemi di IA (robot), i robot sono esseri benevoli, il cui funzionamento si ispira alle tre leggi della robotica:

1. Un robot non può nuocere a un essere umano o consentire, mediante la propria omissione, che un essere umano subisca danno.
2. Un robot deve obbedire agli ordini impartitigli da esseri umani, eccetto che quando questi ordini confliggano con la prima legge.
3. Un robot deve proteggere la propria esistenza fintantoché tale protezione non confligga con la prima o la seconda legge.

Asimov aggiungerà la Legge Zero: un robot non può danneggiare l'umanità o consentire, mediante la propria mancanza di azione, che essa venga danneggiata. Asimov non esclude un aspetto problematico: la disponibilità di servitori robotici, con capacità superiori per molti aspetti a quelle umane, può indurre chi se ne serve a diventare dipendente dai propri schiavi meccanici.

6.4.2 Gli entusiasmi dei pionieri e il paradigma dell'IA simbolica

La ricerca scientifica e tecnologica sull'IA iniziò tra gli anni '40 e gli anni '50 (già nel 1943 venne mostrato come reti di neuroni artificiali potessero elaborare informazioni, dando avvio al tentativo di riprodurre il funzionamento dei neuroni del cervello umano). La nascita dell'IA viene ricondotta a una conferenza che riunì per un mese alcuni pionieri della materia, con lo scopo di studiare l'intelligenza automatica; la tesi fondamentale che ispirava gli studiosi deriva dall'ipotesi che l'intelligenza possa risultare dal funzionamento di un sistema che manipola strutture simboliche: un sistema di simboli fisici consiste di un insieme di entità (simboli), che sono schemi fisici che possono presentarsi come componenti di un altro tipo di entità (espressione o struttura simbolica). Una struttura simbolica è composta di un numero di istanze (o occorrenze) e di simboli correlati in qualche modo fisico; il sistema contiene anche

una collezione di processi che operano sulle espressioni per produrre altre espressioni. Ogni sistema di simboli fisici può essere realizzato mediante una macchina universale, dato che i moderni calcolatori sono macchine universali, l'ipotesi che un sistema di simboli fisici sia capace di intelligenza implica che un calcolatore potrebbe dar vita all'intelligenza.

L'ipotesi del sistema di simboli fisici implica una **teoria computazionale-simbolica dell'intelligenza**: l'ipotesi del sistema simbolico implica che l'intelligenza sarà realizzata da un calcolatore universale. Furono sviluppati calcolatori specificamente dedicati all'IA, le "**macchine per il Lisp**", ma vennero successivamente utilizzati anche calcolatori "a scopo generale" (general purpose). Un sistema capace di risolvere problemi in modo intelligente deve unire due aspetti: una rappresentazione simbolica (in un linguaggio appropriato) delle conoscenze rilevanti e la capacità di trarre conclusioni fondate su tali conoscenze.

McCarthy e Hayes danno la seguente definizione di **intelligenza**, affermando che, un'entità è intelligente se ha un modello adeguato del mondo, se è capace di rispondere a un'ampia varietà di domande sulla base di quel modello, se può trarre informazioni ulteriori dal mondo esterno quando necessario, e può effettuare nel mondo esterno i compiti richiesti dai suoi scopi e consentiti dalle sue capacità fisiche. La nozione di intelligenza comprende due parti:

- la **parte epistemologica**: una rappresentazione del mondo in una forma tale che la soluzione dei problemi derivi dai fatti espressi nella rappresentazione;
- la **parte euristica**: il meccanismo che sulla base dell'informazione risolve il problema e decide che cosa fare.

6.4.3 Sviluppo e crisi delle ricerche di IA

Il programma di ricerca dell'IA simbolica diede origine a risultati: furono sviluppati numerosi sistemi capaci di affrontare compiti tali da richiedere intelligenza negli esseri umani (la soluzione di problemi matematici o fisici) e furono realizzati alcuni strumenti che facilitano la realizzazione di tali sistemi. Alcuni studiosi, dopo tali successi, affermarono che sarebbero state disponibili macchine capaci di raggiungere l'intelligenza umana; ma lo sviluppo delle applicazioni di IA fu lento, e i sistemi di IA non riuscirono a svolgere in modo soddisfacente attività che gli esseri umani compiono spontaneamente e apparentemente senza sforzo.

Negli anni seguenti si cercò di realizzare sistemi esperti capaci di risolvere problemi che richiedessero una particolare competenza specialistica, elaborando tecniche per la rappresentazione della conoscenza in forme tali da renderla elaborabile automaticamente, e procedure per utilizzare ampie basi di conoscenza. Tra tali tecniche ci fu l'uso di metodi per il ragionamento automatico ispirati alla logica; questa, consente di effettuare inferenze e ne garantisce la validità: se le procedure inferenziali di un sistema esperto possono essere ricondotte alla logica (l'insieme dei metodi del ragionamento corretto), allora si può fare affidamento nel funzionamento del sistema stesso (assumendo che anche le premesse del sistema siano corrette): all'inizio degli anni '70 fu inventato il Prolog, un linguaggio logico semplice e intuitivo, basato su una parte della logica predicativa, per il quale furono definite procedure di inferenza molto efficienti. Anche nell'ambito dei sistemi esperti, ai primi

entusiasmi ci fù una delusione: i sistemi realizzati non erano in grado di sostituire la prestazione di un professionista esperto, ma al più di integrarne la competenza. In aggiunta emersero difficoltà inerenti allo sviluppo e alla manutenzione dei sistemi esperti: era difficile e costoso rappresentare la conoscenza nella forma richiesta da un sistema esperto e mantenerla aggiornata; inoltre, non tutte le informazioni potevano essere espresse in questo modo, una volta ridotte in tale forma le informazioni non potevano essere impiegate con la flessibilità di cui è capace l'intelligenza umana, i modelli simbolici apparivano inadatti in talune attività.

6.4.4 Dalla crisi ai primi successi

Nei primi anni '90 vi fu una profonda crisi delle ricerche di IA ("inverno dell'IA"), un clima di sfiducia nei confronti delle prospettive dei sistemi intelligenti. La crisi dell'IA simbolica determinò un'attività di ricerca in direzioni diverse: la ripresa degli studi sui modelli computazionali dell'attività neurale, la creazione di nuovi modelli computazionali simbolici ispirati alle discipline matematiche ed economiche e l'attenzione per le dimensioni dell'azione e della comunicazione.

Vengono ripresi i modelli ispirati all'attività neurale (l'IA simbolica si concentra sulle tecniche per il ragionamento); le reti neurali si ispirano ad un modello biologico: mirano a riprodurre la struttura e la dinamica del cervello piuttosto che una sua funzione (il ragionamento), per l'indirizzo neurale l'essenza dell'intelligenza consiste nell'adattamento all'esperienza. L'elaborazione della conoscenza da parte di una rete neurale è distribuita: l'elaborazione della conoscenza, e l'apprendimento, avverrà mediante elaborazioni numeriche, governate dal calcolo differenziale, che trasformano la rete adattandola all'esperienza. I modelli ispirati all'attività neurale mirano a riprodurre l'aspetto reattivo-intuitivo dell'intelligenza, cioè la capacità di rispondere agli input forniti dall'esperienza e di adattare tale risposta in modo appropriato, senza il tramite del ragionamento e della rappresentazione esplicita della conoscenza.

Le reti neurali (e i modelli connessionistici) hanno offerto una nuova tecnologia per affrontare compiti del senso comune e compiti specialistici attinenti al riconoscimento. I successi ottenuti dai modelli connessionistici hanno forse messo in ombra i progressi nei modelli simbolici. Le elaborazioni simboliche si sono estese all'uso di metodiche formali tratte dalla logica matematica, dalle logiche filosofiche e da discipline quali il calcolo delle probabilità, la teoria della decisione, la teoria dei giochi, le teorie dell'argomentazione. È divenuto possibile utilizzare in misura crescente strumenti di IA per il supporto alla decisione, anche in contesti caratterizzati da incertezza o opinabilità.

L'attenzione per gli aspetti dinamici e relazionali ha consentito di superare l'idea del sistema intelligente quale mero intelletto, privo di iniziativa, che si limita a rispondere alle domande dell'utilizzatore sulla base delle conoscenze registrate al suo interno. Numerose ricerche si sono indirizzate verso la realizzazione di agenti intelligenti, capaci di elaborare informazioni, e di ricercare le informazioni rilevanti. È stato enfatizzato l'aspetto "robotico" dell'IA, cioè la

realizzazione di robot quali entità capaci di azione autonoma, sia nello spazio fisico sia nello spazio virtuale di Internet.

Negli anni '90 le ricerche di IA hanno incontrato Internet, e le sue tecniche hanno trovato impiego in strumenti per la rete (motori di ricerca, sistemi per la costruzione di siti Web).

6.4.5 L'era dell'IA

L'IA ha avuto un enorme successo negli anni più recenti: si è dotata di una solida base interdisciplinare. Una serie di applicazioni di successo sono state sviluppate, e sono entrate nella vita di tutti noi: l'estrazione di informazioni da grandi masse di dati, l'interpretazione degli esami medici e la consulenza medica, la selezione di informazioni rilevanti o l'eliminazione di quelle irrilevanti con tecniche intelligenti, la traduzione automatica, i giochi, la gestione e la logistica, il riconoscimento di immagini, volti, e movimenti, i robot fisici, i sistemi di trasporto autonomi, gli agenti software, la ricerca intelligente di informazioni, l'analisi di documenti, la risposta a domande in linguaggio naturale, transazioni commerciali ad alta velocità, la robotica industriale, i veicoli autonomi, ecc.

CAPITOLO 7: L'IA: tecnologie

7.1 La rappresentazione della conoscenza

Le operazioni che un sistema può fare con i testi dipendono dalle parole che vi compaiono e dalle strutture sintattiche impiegate per collegarle; il sistema ragiona solo sulla base delle forme (non dei contenuti), e in questo senso il suo **ragionamento è formale**.

Chiariamo il concetto di sistema formale applicandolo: dalle premesse (1) "Ogni uomo è mortale", (2) "Socrate è un uomo", deriva la conclusione (3) Socrate è mortale. Per effettuare questa inferenza non abbiamo bisogno di sapere che cosa significa uomo, che cosa significa mortale, che cosa significa Socrate. Ci basta riconoscere la struttura linguistica (la forma) delle premesse, e applicare una regola di inferenza agli elementi racchiusi in quella struttura.

Dall'interazione tra logica ed informatica logica e dell'informatica è nata la **programmazione logica**, che consiste nell'uso della logica simbolica per la rappresentazione esplicita di problemi e delle basi di conoscenza a questi associate, assieme all'uso di inferenze logiche controllate per la soluzione effettiva di tali problemi.

7.1.1 I sistemi basati sulla conoscenza

Nel modello del sistema basato sulla conoscenza, il sistema informatico dispone di due componenti fondamentali: una rappresentazione della conoscenza rilevante, e metodi per il ragionamento automatico applicabili a tale rappresentazione.

7.1.2 Il ragionamento mediante regole

Il ragionamento consiste nel passaggio da certe ragioni a conclusioni giustificate da tali ragioni; passaggio che avviene in generale secondo modelli forniti dalla logica. Si possono distinguere **due tipi di ragionamento**:

- il ragionamento **conclusivo** (deduttivo): la verità delle premesse garantisce la verità delle conclusioni: è impossibile che le premesse siano vere e la conclusione falsa;
- ragionamento **presuntivo** (defettibile): la verità delle premesse fonda solo la presunzione delle conclusioni: se le premesse sono vere, anche la conclusione si assume essere vera a meno che non risulti applicabile un'eccezione.

Il tipo di ragionamento più frequente in ambito giuridico è l'**applicazione di regole**, intese come enunciati condizionali, che collegano un antecedente a un conseguente consentendo di inferire il secondo dal primo. L'antecedente può consistere di una sola proposizione atomica, o di una combinazione di tali proposizioni, dette condizioni, mentre il conseguente consiste di una singola proposizione. Le regole giuridiche collegano una fattispecie astratta a una conseguenza giuridica: la fattispecie astratta è l'antecedente della regola e la conseguenza giuridica astratta ne è il conseguente. Il ragionamento consiste nella derivazione di un effetto giuridico concreto data una fattispecie concreta.

Il **ragionamento concatenamento in avanti**: dato un insieme di fatti noti, il concatenamento in avanti esamina se le condizioni di qualche regola risultino soddisfatte. In caso positivo aggiunge la conclusione della regola ai fatti noti; passa poi a considerare se, grazie alle nuove conclusioni, sia possibile trarre, allo stesso modo, le conclusioni di altre regole (aggiungendo anch'esse ai fatti noti), e così via. Il processo termina quando si sia raggiunta la conclusione desiderata o si sia stabilita l'impossibilità di raggiungerla.

Il **concatenamento all'indietro** procede nel senso opposto: data una conclusione da dimostrare, il ragionamento all'indietro ricerca una regola il cui conseguente coincida con la conclusione cercata. Procede quindi da esaminare se le condizioni di quella regola possano essere a loro volta dimostrate, in quanto conclusioni di altre regole o fatti noti. Il processo termina quando si risale a un insieme di fatti noti dal quale si deriva (mediante una concatenazione di regole) la conclusione cercata, o si sia riscontrata l'impossibilità di rinvenire quei fatti.

Il **ragionamento defeasible**: esistono numerosi modelli logici per trattare le eccezioni e i conflitti tra regole; in uno di questi linguaggi troviamo la "negazione per fallimento": la proposizione "non risulta che A" si considera soddisfatta a condizione che siano falliti tutti i tentativi di dimostrare la proposizione A, sulla base delle informazioni disponibili (quelle incluse nella base di conoscenza).

La correttezza della conclusione tratta da un certo insieme di premesse mediante un'inferenza, è garantita solo dalla compresenza delle seguenti condizioni:

- la correttezza delle premesse;
- la correttezza dello schema di inferenza;
- l'assenza di inferenze prevalenti contro l'impiego delle premesse o contro;
- l'esecuzione dell'inferenza.

7.1.3 Successi e limiti del modello logico

Sistemi esperti furono realizzati in diversi ambiti; il limite nei sistemi esperti era rappresentato dal "collo di bottiglia" della rappresentazione della conoscenza. Tali sistemi applicano la propria base di conoscenza: se la base di conoscenza non include tutte le informazioni rilevanti per risolvere il problema proposto, la risposta sarà inadeguata. Solo in ambiti ristretti i sistemi basati sulla rappresentazione esplicita della conoscenza hanno condotto ad applicazioni di successo.

7.2 L'apprendimento automatico

Nei sistemi basati sull'apprendimento automatico la conoscenza relativa all'ambito di applicazione del sistema è costruita dal sistema sulla base degli esempi forniti dai dati. Grazie a tali metodi, le macchine possono estrarre le informazioni rilevanti dai dati di input e imparare a svolgere in modo adeguato le funzioni a esse affidate.

7.2.1 Indirizzi nell'apprendimento automatico

Si distinguono tre principali indirizzi nell'apprendimento automatico: l'apprendimento supervisionato (supervised), l'apprendimento per rinforzo (reinforcement) e l'apprendimento non-supervisionato (unsupervised) (vedi Figura 7.2).

1. **L'apprendimento supervisionato:** la macchina apprende mediante supervisione, cioè attraverso una fase di istruzione o addestramento in cui le viene fornito un ampio insieme di esempi sulla base dei quali la macchina costruisce un modello generale, applicabile anche a casi nuovi, parzialmente diversi da quelli nell'insieme di addestramento. Il sistema riceve un insieme di coppie, ciascuna della quale combina la descrizione di un problema alla risposta corretta allo stesso.
2. **L'apprendimento per rinforzo:** il sistema apprende dai risultati delle proprie azioni, cioè dalle ricompense o penalità (punti guadagnati o persi) che sono collegati ai risultati a quelle azioni; il sistema osserverà i risultati delle proprie azioni e si autosomministrerà le ricompense e penalità appropriate. Essendo diretto a massimizzare il proprio punteggio complessivo, apprenderà a compiere le azioni che più probabilmente conducono a risultati collegati a ricompense e a evitare le azioni che più probabilmente conducono a risultati collegati a penalità.
3. **L'apprendimento non supervisionato:** il sistema intelligente impara senza ricevere istruzioni, né da fonti esterne (apprendimento supervisionato), né dai risultati delle proprie attività (apprendimento per rinforzo). Le tecniche dell'apprendimento non-supervisionato sono usate in particolare per il raggruppamento, per riunire insiemi di oggetti che presentano somiglianze o connessioni rilevanti.

7.2.2 L'apprendimento supervisionato: addestramento e costruzione di un modello

Nei sistemi per l'apprendimento automatico possiamo distinguere due aspetti: l'**algoritmo discendente** che apprende (costruisce il modello) usando gli esempi forniti al sistema, e l'**algoritmo o modello appreso** (il risultato dell'apprendimento).

Nel processo dell'apprendimento supervisionato l'algoritmo discendente usa l'insieme di addestramento per costruire un modello del compito che il sistema dovrà svolgere. Il modello non si limita a riprodurre gli esempi presenti nell'insieme di addestramento, ma ne offre una generalizzazione: esso può essere applicato anche a nuovi casi, che differiscono in qualche aspetto da ciascuno degli esempi su cui si è basato l'addestramento.

Il modello predisposto dall'algoritmo discendente è usato dall'algoritmo predittore, per fornire risposte sperabilmente corrette a casi nuovi. Se gli esempi più simili al caso nuovo hanno avuto una certa risposta, l'algoritmo predittore potrà proporre la stessa risposta nel caso nuovo.

7.2.3 Predizioni e correlazioni

Le risposte di un sistema basato sull'apprendimento automatico sono solitamente chiamate **predizioni**: in alcuni casi si tratta di anticipazioni del futuro, in altri casi riguarda il presente

o anche il passato; in alcuni casi riguarda un evento suscettibile di verificarsi indipendentemente dalla predizione stessa, in altri casi è un suggerimento, che potrà essere accolto o meno da chi può realizzare l'evento stesso.

Un sistema che effettua predizioni automatiche opera sulla base di correlazioni, cioè di relazioni probabilistiche tra dati di input e esiti possibili. Una correlazione consiste nel fatto che alla presenza di certi dati di input corrisponde una maggiore probabilità di un certo esito (correlazioni positive), o una minore probabilità dello stesso (correlazione negativa). Tali correlazioni sono incorporate nel modello costruito dall' algoritmo di addestramento, che a dati di input correlati positivamente ad un esito favorevole tende a far corrispondere una predizione favorevole, e l'opposto nel caso di correlazione negativa. Gli effetti di tutte le correlazioni rilevanti di cui il sistema può tener conto vengono aggregate in un punteggio (score), che esprime la probabilità che nel caso in esame la classificazione sia positiva anziché negativa.

7.2.4 L'apprendimento supervisionato: Esempi

7.2.5 Le tecnologie per l'apprendimento automatico: sistemi trasparenti e opachi

L'apprendimento automatico usa diversi metodi, che differiscono non solo nelle prestazioni predittive ma anche nella capacità di fornire spiegazioni, e spesso vi è una tensione tra i due obiettivi.

Alcuni dei modelli appresi in modo automatico sono caratterizzati dal fatto che l'attivazione comporta calcoli complessi intesi a riprodurre le correlazioni statistiche tra caratteristiche di input e risultati da predire. Oggi il modello più influente è rappresentato dalle reti neurali, sistemi informatici che consistono di nodi collegati da link ai quali sono assegnati pesi numerici. La struttura informatica utilizzata per riprodurre questo tipo di apprendimento è la rete neurale, una struttura composta da unità chiamate neuroni, e da determinati collegamenti tra le stesse unità. Ogni neurone riceve segnali dai neuroni a esso connessi, segnali che viaggiano seguendo determinati collegamenti. Il neurone, quando riceve determinati segnali, verifica se quei segnali abbiano raggiunto il livello (la soglia) richiesta per la propria attivazione. Se il livello non è stato raggiunto, il neurone rimane inerte; se invece il livello è stato raggiunto, il neurone si attiva, inviando a sua volta segnali ai neuroni con esso connessi.

La tecnica più comune per addestrare una rete neurale consiste nel proporre alla rete una serie di esempi corretti, cioè una serie di coppie < input, output >, dove l'output indica il risultato corretto per l'input corrispondente.

7.2.6 L'integrazione di rappresentazione della conoscenza e apprendimento automatico

In molti settori i modelli logici possono essere complementari all'apprendimento automatico. Questi modelli possono contribuire a spiegare il funzionamento dei sistemi per l'apprendimento automatico, controllare e governare il loro funzionamento secondo standard normativi, validarne i risultati, e sviluppare le implicazioni logiche degli stessi risultati secondo conoscenza concettuale e teorie scientifiche.

CAPITOLO 8: L'AI: applicazioni giuridiche

8.1 Conoscenza e ragionamento

Il tipo di ragionamento più frequente in ambito giuridico è l'**applicazione di regole**. Per "regola" si intende un enunciato condizionale, che collega un antecedente e un conseguente consentendo di inferire il secondo dal primo. Il concetto di regola come condizionale (piuttosto che come obbligo o prescrizione) corrisponde all'idea diffusa che le regole giuridiche colleghino una fattispecie e una conseguenza giuridica: la fattispecie astratta è l'antecedente della regola e la conseguenza giuridica astratta ne è il conseguente.

8.1.1 I sistemi basati su regole nel diritto

I sistemi basati su regole contengono una base di conoscenza costituita da regole, e un motore di inferenza, che applica tali regole ai dati di fatto attinenti a casi concreti. Le informazioni attinenti ai casi possono essere fornite dall'utilizzatore umano del sistema o estratte da archivi informatici. L'importanza di tali sistemi deriva dalla possibilità di applicare un numero elevato di regole, tenendo conto dei collegamenti tra le stesse. Essi possono supplire ai limiti della memoria, dell'attenzione, e della capacità combinatoria dell'uomo.

8.1.2 La scrittura di regole In linguaggio quasi-naturale

La Logical English (un prototipo del sistema è disponibile online, con sorgente aperta) accetta formulazioni vicine al linguaggio naturale e provvede automaticamente a trasformarle in programmi logici, in Prolog o ASP (Answer set programming).

8.1.3 L'uso dei sistemi basati sulla conoscenza giuridica

I sistemi basati sulla conoscenza non sono esperti automatici in grado di sostituirsi al funzionario pubblico, ma piuttosto strumenti che forniscono un aiuto intelligente al richiedente del servizio o al funzionario che lo gestisce.

Si è osservato che l'uso di sistemi basati sulla conoscenza nella pubblica amministrazione può condurre a un'applicazione rigida e iniqua del diritto. Queste critiche possono trovare risposta non tanto nel ribadire che i sistemi basati sulla conoscenza non sminuiscono necessariamente né il ruolo del richiedente un servizio pubblico né quello del funzionario competente. Al contrario l'uso di tali sistemi può accrescere le sfere di iniziativa e di autonomia informata del cittadino e del pubblico funzionario incaricato di provvedere a un'attività regolata dal diritto.

I sistemi basati sulla conoscenza giuridica possono essere utilmente impiegati nella pubblica amministrazione solo all'integrazione delle seguenti attività:

- l'attività dell'esperto informatico-giuridico che si occupa non solo dell'inserimento, ma anche della correzione e revisione delle regole, assicurando che la base di conoscenza non contenga errori di diritto;

- l'attività del cittadino o del funzionario che inseriscono i dati sui casi concreti, sulla base dell'esame delle circostanze di fatto e dell'interpretazione delle regole da applicare;
- l'attività del sistema, che si occupa della derivazione delle conseguenze deducibili dalle regole in esso comprese e dei dati di fatto a esso forniti o cui abbia accesso.

8.1.4 I limiti dell'applicazione deduttiva di regole

I sistemi che applicano automaticamente regole preesistenti trovano le maggiori applicazioni nell'ambito della pubblica amministrazione. Essi non sono in grado di affiancare il giurista nelle attività che formano la parte centrale del suo pensiero.

Secondo alcuni, l'uso di sistemi basati su regole in ambito giuridico presupporrebbe l'accettazione del modello sillogistico del ragionamento giuridico, l'idea che il diritto si riduca a un insieme di regole e che il ragionamento giuridico consista nell'applicazione "meccanica" di tali regole.

I sistemi basati sull'applicazione deduttiva del diritto si limitano a cogliere un aspetto limitato del ragionamento giuridico, ma ciò non postula un errore teorico e non ne determina l'inutilità pratica. Le limitazioni di questi sistemi non ne escludono l'utile impiego, nella piena consapevolezza di tali limitazioni. In un modello simbiotico di interazione uomo-macchina è possibile affidare alla macchina la registrazione delle regole, la loro applicazione logica e il prelievo dei dati fattuali già disponibili in forma elettronica, e affidare invece all'uomo la formulazione delle regole, il controllo sul funzionamento del sistema e l'inserimento e la qualificazione giuridica di nuovi dati fattuali.

8.1.5 La dialettica giuridica: il ragionamento defeasible

Lo sviluppo delle logiche defeasible si basa sull'idea che sia possibile e utile predisporre strumenti logici e informatici capaci di cogliere la dialettica del ragionamento giuridico, superando i limiti del ragionamento sillogistico.

Un'inferenza defeasible è un argomento che si impone alla nostra ragione, ma solo in modo provvisorio, cioè solo a condizione che non emergano eccezioni, contro-esempi, argomenti contrari di importanza preminente. Il fatto che si accolgano le premesse dell'argomento che conduce a una certa conclusione può essere insufficiente a giustificare tale conclusione: bisogna indicare quali controargomenti siano stati considerati, e perché l'argomento prescelto abbia prevalso su di essi.

La struttura interna degli argomenti defeasible. Nella struttura fondamentale degli argomenti basati su regole defeasible si distinguono i dati di partenza dell'argomento (data) e la regola generale (warrant), che consente di passare dai dati alla conclusione che si vuole sostenere (claim). Nel rapporto tra regola generale defeasible e fatti particolari, la regola generale contiene delle variabili (x e y) e la sussunzione della fattispecie concreta nella fattispecie astratta avviene sostituendo, in modo uniforme, le variabili con i nomi di persone o cose particolari.

Gli attacchi tra argomenti. Possiamo distinguere due modi in cui un argomento defeasible può essere attaccato. Il primo è detto **rebutting**, consiste nell'opporre ad a un contro-argomento B che contraddice la conclusione di A: la conclusione di B nega, o è incompatibile con la conclusione di A. Il secondo è detto **undercutting**, consiste nell'opporre ad A un contro-argomento B che nega la forza argomentativa di A: B afferma che le premesse di A sono inidonee a fondarne la conclusione.

Come valutare argomenti in conflitto. L'accoglimento delle premesse (i dati e la regola) di un argomento defeasible non è sufficiente a garantire l'accettabilità della sua conclusione. Solo se tutti i contro-argomenti possono essere superati alla luce di considerazioni ulteriori, la conclusione dell'argomento risulta giustificata. Da ciò discendono due aspetti dell'interazione dialettica tra argomenti contrapposti:

1. consiste nella possibilità di ristabilire un argomento, attaccando gli argomenti che potrebbero sconfiggerlo. Un argomento può essere difeso non solo producendo argomenti ulteriori che vanno nella stessa direzione ma anche cercando di demolire i contro-argomenti che a esso si oppongono;
2. consiste nella possibilità di sostenere un argomento A, contraddetto da un contro-argomento B, adducendo ulteriori argomenti che indichino perché A debba prevalere su B.

Gli argomenti, alla luce delle relazioni con gli altri argomenti presenti nel medesimo contesto argomentativo possono essere suddivisi in tre classi, sulla base in una valutazione che tiene in considerazione tutti e soli gli argomenti presenti in quel contesto:

- argomenti IN, che debbono essere accettati;
- argomenti OUT, che debbono essere respinti;
- argomenti UND, sui quali permane l'incertezza.

Lo status di tali argomenti potrebbero cambiare: ogni argomento potrebbe assumere un diverso status se altri argomenti fossero introdotti nel contesto.

Le logiche degli argomenti. Si tratta di affrontare situazioni nelle quali vi sono numerosi argomenti in gioco. Logiche degli argomenti sono state usate per realizzare sistemi informatici che, anziché limitarsi a fornire una risposta univoca ai quesiti loro proposti, elaborino giustificazioni per la soluzione di punti controversi, suggeriscano argomenti possibili, valutino lo stato degli argomenti alla luce dell'architettura argomentativa complessiva risultante dalle informazioni fornite al sistema.

8.1.6 Il ragionamento basato sui casi

Esempio di sistema per il ragionamento che opera sulla base di rappresentazioni di casi è il sistema HYPO. La base di conoscenza del sistema è costituita da un insieme di precedenti. Ogni caso è descritto con i seguenti dati:

- il suo esito, che può essere a favore dell'attore a, cioè l'accertamento della violazione, o invece a favore della difesa del convenuto c, cioè l'accertamento che non vi è stata violazione;
- un insieme di fattori, cioè di circostanze a favore o contro l'uno o altro esito; individuati con un'analisi giuridica dell'ambito considerato,

8.2 L'apprendimento automatico

8.2.1 Claudette, un sistema basato sull'apprendimento automatico

Il sistema Claudette si propone di applicare metodi di apprendimento automatico per l'analisi giuridica di contratti online e informative privacy, tesa ad identificare e classificare le clausole abusive e illegali, contenute in tali documenti.

Il principale riferimento normativo per l'applicazione di Claudette ai termini di servizio è dato dalla Direttiva 93/13/CEE sui contratti stipulati con i consumatori, che vieta l'utilizzo di «clausole contrattuali abusive» nei contratti unilateralmente redatti da produttori e intermediari. L'Art. 3 della Direttiva 93/13 stabilisce che una clausola è abusiva se: (a) non è stata individualmente negoziata e (b) anche se adottata in buona fede, determina uno squilibrio significativo nei diritti e negli obblighi delle parti, a scapito del consumatore.

La metodologia per l'addestramento del sistema. Il sistema Claudette è stato addestrato a riconoscere le clausole (potenzialmente) abusive mediante metodi di apprendimento automatico supervisionato. Le clausole marcate nell'insieme di addestramento indicano al sistema come a certe forme testuali corrispondano certe classificazioni giuridiche, cioè la determinazione della categoria cui appartiene la clausola e la valutazione della sua vessatorietà.

Gli algoritmi per l'apprendimento "insegnano" al sistema a effettuare determinazioni e valutazioni analoghe a quelle specificate nell'insieme di addestramento. Tali algoritmi generano un "modello" che fornisce al sistema criteri e meccanismi per la classificazione delle clausole. Il sistema, sulla base dell'addestramento, genera un proprio concetto di vessatorietà, che poi applica alla classificazione di nuove clausole. Tale concetto è costruito in modo che, nell'applicarlo, il sistema giunga alle stesse conclusioni cui sono giunti i giuristi che hanno predisposto l'insieme di addestramento, rispetto ai casi contenuti in tale insieme. Applicando modello così costruito il sistema si propone di realizzare due obiettivi:

- categorizzare le clausole di nuovi contratti, cioè determinare l'oggetto;
- valutare le clausole, cioè determinare se esse siano vessatorie.

Per realizzare questi obiettivi sono necessarie due fasi. La prima consiste nella trasformazione delle clausole in strutture di dati che possano essere utilizzate per l'addestramento del sistema. A tal fine è necessario innanzitutto procedere all'analisi lessicale, che consiste nel suddividere il testo negli elementi rilevanti (tipicamente parole e segni di punteggiatura). La fase successiva è quella dell'analisi sintattica, che individua le strutture sintattiche in cui gli elementi sono combinati.

L'apprendimento del sistema consisterà nel costruire un modello che correli la presenza o l'assenza di combinazioni di parole nelle frasi da valutare alle corrispondenti categorizzazioni e valutazioni giuridiche. Sulla base di tale modello, data una nuova frase, il sistema ne indicherà categoria e valutazione giuridica.

In Claudette si sono utilizzati diversi metodi per costruire un modello di questo tipo.

Oltre alle reti neurali si è usata quella della macchina a vettori di supporto. Secondo questo modello, il sistema impara ad assegnare dei pesi alle caratteristiche in considerazione, in modo che venga massimizzata la distanza tra gli esempi positivi e gli esempi negativi, cioè tra le linee parallele che toccano gli esempi positivi e negativi più vicini.

La valutazione delle prestazioni del sistema. Un aspetto essenziale nei sistemi basati sull'apprendimento automatico automatica riguarda la valutazione delle loro prestazioni.

Nel caso di Claudette, addestrato sulla base dell'insieme di addestramento costituito dalle indicazioni di giuristi esperti il criterio di valutazione sarà rappresentato da quelle stesse indicazioni. Si sono sottoposti a Claudette casi non inclusi nel suo insieme di addestramento, e si è verificato se le risposte del sistema coincidessero con quelle che esperti giuridici avevano fornito a quegli stessi casi. Sulla base di tale confronto, le prestazioni del sistema si sono misurate con riferimento alle metriche classiche usate nella classificazione automatica: richiamo, precisione, e media armonica tra precisione e richiamo. La precisione è la valutazione della correttezza delle risposte positive del sistema, cioè dei casi in un cui Claudette classifica correttamente una clausola come abusiva. Essa consiste più esattamente nel rapporto tra le clausole correttamente classificate come abusive (i cosiddetti veri positivi, VP), e l'insieme di tutte le clausole qualificate come abusive, che include tanto i veri positivi quanto i falsi positivi (le clausole erroneamente classificate come abusive, FP).

8.2.2 La previsione di fattori e la previsione basata su fattori

Nei caso di Claudette, il sistema correla direttamente strutture testuali e il risultato giuridico da predire, cioè la categoria e qualità giuridica della clausola. Il sistema svolge un'analisi giuridico: determina se una certa formulazione testuale esprime un contenuto di un certo tipo e se esso sia conforme alla legge.

È possibile utilizzare tecniche per l'apprendimento automatico anche per effettuare predizioni sulla base di una descrizione strutturata degli esempi, piuttosto che sulla base della forma linguistica degli stessi. In questo caso, bisogna associare al documento un insieme di descrittori, che ne esprime le caratteristiche rilevanti. I descrittori sono in generale forniti da esperti umani, che possono però avvalersi di supporti automatici.

Questa soluzione può essere preferibile quando la predizione da effettuare riguarda testi complessi, nei quali è difficile, anche per una rete profonda, individuare connessioni significative tra strutture testuali e l'obiettivo della predizione. L'individuazione degli aspetti giuridicamente rilevanti è utile al fine di fornire una spiegazione significativa.

8.3 La giustizia predittiva

8.3.1 Il concetto di predizione

Nell'ambito dell'apprendimento automatico la predizione può coprire attività molto diverse da una prospettiva teorico-giuridica: la ricerca documentale, la creazione automatica di riassunti o massime, l'associazione di descrittori al testo, l'anticipazione di condotte future di imputati o parti, il supporto alla creazione di documenti, il supporto allo studio empirico del diritto.

La predizione può riguardare il risultato finale di un caso giudiziario o altro evento o circostanza che possa contribuire a determinare quel risultato. Nella prima ipotesi si tratta di anticipare il contenuto della statuizione del giudice. Nella seconda ipotesi si tratta di predire altri eventi rilevanti per la decisione, tipicamente, il comportamento futuro di una parte. Si tratta di previsioni che influiscono sulla determinazione della sentenza, fornendo al giudice indicazioni rilevanti per quantificare la pena da irrogare o da inasprire per il rischio di recidiva in concreto.

Predizioni su eventi presenti o passati. Nella prima ipotesi la predizione si configura come una previsione. Il caso paradigmatico consiste nell'anticipazione dell'esito di una controversia, sulla base di elementi disponibili prima della decisione. Nella seconda ipotesi la previsione dell'esito della controversia si fonda su elementi disponibili solo dopo che la controversia è stata decisa. Per esempio, un sistema potrebbe "predire" l'esito di una controversia sulla base di una porzione della sentenza che ha deciso quella controversia.

Predizioni fondate su ragioni giuridiche o para giuridiche. La predizione può essere fondata su elementi normativamente rilevanti del caso in esame, che il giudice potrebbe considerare nel giustificare la propria decisione o elementi normativamente irrilevanti, che il decisore non dovrebbe prendere in considerazione. Nella prima ipotesi, il sistema automatico fonda le proprie predizioni su elementi giuridicamente significativi, e in particolare sugli aspetti della causa che giustificano l'una o l'altra decisione, secondo il diritto. Tali aspetti possono essere descritti nel linguaggio naturale, o in modo strutturato (elencando le caratteristiche o fattori rilevanti, nella loro combinazione). Nella seconda il sistema basa la propria predizione su aspetti che, pur statisticamente correlati all'esito delle controversie, non forniscono una giustificazione giuridicamente rilevante.

Predizioni spiegate o opache. Il sistema può essere capace di fornire una spiegazione del suo output, adducendo ragioni comprensibili agli umani, o può rimanere opaco, limitandosi a dare la propria indicazione sull'esito finale della controversia. Nella prima ipotesi, il sistema accompagna la propria predizione con l'indicazione degli aspetti giuridicamente rilevanti su cui essa si basa. Nella seconda ipotesi esemplificata dalle reti neurali, manca una spiegazione poiché l'esibizione del processo mediante il quale il sistema, grazie all'attivazione dei neuroni, è giunto alla decisione è privo di significato per gli esseri umani.

Predizioni per giudici e per avvocati/parti. Nel caso prototipico di predizioni concernenti l'esito futuro di una controversia, è importante sottolineare come le indicazioni del sistema

sono suscettibili di essere utilizzate in diverso modo a seconda di chi faccia uso di tali indicazioni, e del modo in cui loro uso è regolato. Giudizi aventi il medesimo contenuto possono avere un significato pragmatico assai diverso. Il prototipico giudizio dell'avvocato o della parte sull'esito di una controversia consiste di una previsione di fatto, che sarà confermata o smentita dal successivo comportamento del giudice. La previsione di come potrebbe essere decisa una futura controversia determina le aspettative e, quindi, il comportamento delle parti, anche prima dell'insorgere della controversia, mentre poi determina il loro comportamento processuale. Il prototipico giudizio del giudicante ha un effetto istituzionale. La predizione fornita da un sistema automatico può avere un effetto diverso a seconda del contesto in cui la predizione viene formulata, e dalle attitudini di chi lo riceve.

Predizione dotate o prive di valore giuridico. La predizione del sistema potrebbe essere dotata di valore giuridico, così da risultare una decisione vincolante per le parti, almeno quando queste non decidano di contestarla.

8.3.2 Obiettivi e proxy delle predizioni

L'obiettivo diretto della predizione automatica si distingue da un possibile obiettivo finale per il quale il sistema viene utilizzato, che può essere diverso dall'obiettivo diretto.

Un sistema destinato a prevedere l'esito delle sentenze può aver l'obiettivo diretto di prevedere la sentenza del giudice medio, obiettivo che si avvicina a quello dell'utilizzatore avvocato o cittadino, solitamente interessati a prevedere il comportamento del giudice della propria causa, così da impostare di conseguenza il proprio comportamento processuale. Nelle applicazioni di giustizia predittiva, va individuato con precisione quale sia l'obiettivo diretto delle predizioni del sistema, per valutarne la rilevanza.

La possibilità di una predizione "oggettiva" non esiste quando, come nel caso della predizione dell'esito di controversie giudiziarie, l'obiettivo da prevedere sia proprio la decisione umana e non vi sia un riscontro obiettivo della correttezza della decisione. In questo caso, il sistema si limiterà a "predire" quale nuova decisione potrà allinearsi alle decisioni passate nel loro complesso, riproducendo le virtù così come i vizi dell'indirizzo prevalente.

Un sistema "predittivo" se sviluppato in modo da fornire indicazioni accurate e accompagnate da spiegazioni adeguate, potrebbe contribuire a migliorare la pratica del diritto, se sviluppato e applicato con piena consapevolezza delle sue funzionalità e dei suoi limiti, nel rispetto di etica e diritto.